L'importance du facteur humain dans la sécurité informatique

L'ART DE LA SUPERCHERIE

KEVIN D. MITNICK
& William L. Simon

Les révélations du plus célèbre hacker de la planète

L'ART DE LA SUPERCHERIE

Préface de Steve Wozniak
Cofondateur d'Apple

WILEY

CampusPress

L'ART DE LA SUPERCHERIE

KEVIN MITNICK
ET WILLIAM L. SIMON

CampusPress a apporté le plus grand soin à la réalisation de ce livre afin de vous fournir une information complète et fiable. Cependant, CampusPress n'assume de responsabilités, ni pour son utilisation, ni pour les contrefaçons de brevets ou atteintes aux droits de tierces personnes qui pourraient résulter de cette utilisation.

Les exemples présents dans cet ouvrage sont fournis pour illustrer le propos du livre. Ils ne sont en aucun cas destinés à être reproduits.

CampusPress ne pourra en aucun cas être tenu pour responsable des préjudices ou dommages de quelque nature que ce soit pouvant résulter de l'utilisation de ces exemples.

Tous les noms de produits ou autres marques cités dans ce livre sont des marques déposées par leurs propriétaires respectifs.

Cet ouvrage est une version française de *The Art of Deception*, publiée et vendue à travers le monde avec l'autorisation de John Wiley & Sons, Inc.

Publié par CampusPress
47 bis, rue des Vinaigriers
75010 PARIS
Tél. : 01 72 74 90 00

Mise en pages : Hekla

ISBN : 2-7440-1976-3
Copyright © 2005 CampusPress
Tous droits réservés

CampusPress est une marque de
Pearson Education

Titre original : The Art of Deception

Traduction : Daniel Garance
et Raymond Debonne
Avec la collaboration technique
d'Arnold McDonald (A McD)

ISBN original : 0-471-23712-4
Copyright © 2002 by John Wiley
& Sons, Inc.
Tous droits réservés

Wiley Publishing, Inc.
Indianapolis, Indiana
USA

Aucune représentation ou reproduction, même partielle, autre que celles prévues à l'article L. 122-5 2° et 3° a) du code de la propriété intellectuelle ne peut être faite sans l'autorisation expresse de Pearson Education France ou, le cas échéant, sans le respect des modalités prévues à l'article L. 122-10 dudit code.

La manipulation (*social engineering*)[1]

On dit d'une personne qu'elle a recours à la manipulation lorsqu'elle utilise l'influence et la persuasion pour duper les gens en se faisant passer pour quelqu'un qu'elle n'est pas. *In fine*, le manipulateur sait exploiter autrui afin d'obtenir des renseignements, en s'aidant ou non de moyens technologiques.

1. N.D.T. : Dans le cadre de cet ouvrage, nous avons choisi le terme *manipulation* pour traduire l'expression anglo-saxonne *social engineering*. Nous aurions pu adopter la traduction littérale, "ingénierie sociale", que l'on rencontre par ailleurs, mais dont le sens ne recouvre pas exactement celui de *social engineering*.

Sommaire

Préface 1

Avant-propos 3

Introduction 9

Partie 1 Dans les coulisses 11

Chapitre 1 Le plus faible maillon de la sécurité 13

Partie 2 L'art de l'attaquant 25

Chapitre 2 Quand une information anodine ne l'est pas 27

Chapitre 3 L'attaque directe : il suffit de demander 43

Chapitre 4 Instaurer la confiance 53

Chapitre 5 Laissez-moi vous aider 67

Chapitre 6 Pouvez-vous m'aider ? 89

Chapitre 7 Faux sites et liaisons dangereuses 105

Chapitre 8 Exploiter la compassion, la culpabilité et l'intimidation 119

Chapitre 9 L'arnaque par inversion 149

Partie 3 Menaces d'intrusion 165

Chapitre 10 L'intrusion physique 167

Chapitre 11 Manipulation et technologie 193

Chapitre 12 Les attaques visant le salarié de base 215

Chapitre 13 Les stratagèmes sophistiqués 231

Chapitre 14 L'espionnage industriel 247

Partie 4 Stratégies de prévention 267

Chapitre 15 Programme de formation et d'information des salariés 269

Chapitre 16 Les règles de sécurité à appliquer dans l'entreprise 283

Annexe Consignes de sécurité 357

Sources 367

Index 369

Préface

Les êtres humains que nous sommes ont une propension innée à explorer leur environnement. Quand nous étions jeunes, Kevin Mitnick et moi étions extrêmement curieux de découvrir le monde, et impatients de faire nos preuves. Nous avons souvent été récompensés lorsque nous avons tenté d'apprendre de nouvelles choses, de résoudre des énigmes et de gagner. Mais, en même temps, dans le monde qui nous entoure, il faut suivre des règles de conduite qui réfrènent notre profond désir de découverte totale. Pour les hommes de science et les entrepreneurs les plus hardis, de même que pour les gens comme Kevin Mitnick, satisfaire ce profond désir procure les plus vives émotions et permet d'accomplir des choses que d'aucuns considèrent comme impossibles.

Kevin Mitnick est l'une des personnes les plus nobles que je connaisse. Si vous l'interrogez, il vous répondra franchement que ce qu'il avait coutume de pratiquer, le *social engineering* (à savoir la manipulation), cela revient à arnaquer les gens. Mais Kevin n'est plus un manipulateur. Et même quand c'était le cas, son but n'a jamais été de s'enrichir ou de porter atteinte à autrui. Cela ne veut pas dire qu'il n'existe pas de criminels dangereux et nuisibles qui ne tirent pas parti de leurs capacités de manipulation pour réellement nuire à autrui. En fait, c'est exactement pour cette raison que Kevin a écrit ce livre : pour vous apprendre à vous méfier de ce genre de personnes.

Cet ouvrage montre à quel point nous sommes tous vulnérables — le gouvernement, le monde des affaires, les entreprises publiques, privées et chacun d'entre nous — aux attaques des manipulateurs. Dans une époque qui a pris conscience de l'importance de la sécurité, nous consacrons des sommes énormes à développer des techniques destinées à protéger nos

réseaux informatiques ainsi que nos données. Ce livre souligne combien il est facile de contourner toutes ces protections technologiques.

Que vous travailliez dans le secteur privé ou dans l'administration publique, ce livre constitue un guide efficace qui vous aidera à comprendre comment les manipulateurs procèdent, et comment vous pouvez contrecarrer leurs plans. Par le biais d'histoires romancées à la fois amusantes et instructives, Kevin et son coauteur Willian L. Simon mettent en avant les techniques employées par les manipulateurs.

Les technologies mises en place en matière de sécurité laisse des failles importantes que des gens comme Kevin peuvent nous aider à combler. Lorsque vous aurez lu cet ouvrage, vous admettrez peut-être enfin que nous avons tous besoin des conseils d'un Mitnick.

Steve Wozniak

Avant-propos

Certains hackers détruisent les fichiers ou les disques durs entiers d'autres personnes : il s'agit des *crakers*. Les hackers débutants qui ne s'embarrassent pas de connaissances techniques et se contentent de télécharger les outils des hackers pour s'introduire dans des systèmes informatiques sont des *script kiddies*. Il existe également des hackers, plus expérimentés et compétents en programmation, qui développent des programmes de piratage puis les mettent sur le Web. Enfin, d'autres individus, nullement intéressés par la technologie, se servent de l'ordinateur comme d'un simple outil pour voler de l'argent, des biens ou des services.

Contrairement au mythe Kevin Mitnick créé par les médias, je ne suis pas un hacker malveillant.

Voici mon histoire.

POUR COMMENCER

Ma voie a certainement été tracée très tôt. J'étais un garçon insouciant, mais je m'ennuyais. Lorsque mon père est parti, alors que j'avais trois ans, ma mère a pris un travail de serveuse afin de subvenir à nos besoins. Enfant unique élevé par une mère dont les longues journées de travail étaient harassantes et dont l'emploi du temps était irrégulier, j'étais pratiquement livré à moi-même. J'étais ma propre baby-sitter.

Le fait de grandir dans une commune de la vallée de San Fernando m'a offert tout San Francisco à explorer, et à l'âge de douze ans, j'ai découvert un moyen de voyager gratuitement dans tout Los Angeles et ses environs. Un jour, en prenant le bus, je me suis rendu compte que la validité du billet que j'avais acheté dépendait d'un modèle inhabituel de poinçon que les chauf-

feurs utilisaient pour indiquer le jour, l'heure et la route sur les tickets. Répondant à une question que j'avais astucieusement posée, un chauffeur sympathique m'a indiqué où acheter ce type particulier de composteur.

Ce système avait été conçu pour pouvoir changer de bus et poursuivre un voyage jusqu'à sa destination finale, mais j'ai cherché comment m'en servir pour voyager gratuitement partout où je voulais aller. Se procurer des billets vierges était un jeu d'enfant. Les corbeilles à papier des stations de bus étaient toujours pleines de carnets partiellement utilisés dont les chauffeurs se débarrassaient à la fin de leurs rotations. Avec un bloc vierge et le composteur, je pouvais poinçonner mes propres tickets et voyager partout où les bus de Los Angeles voulaient bien me mener. En peu de temps, j'avais appris par cœur les horaires du réseau presque tout entier (exemple précoce de ma surprenante mémoire pour certains types d'informations ; je suis encore capable aujourd'hui de me souvenir de numéros de téléphone, mots de passe et autres détails apparemment sans importance qui remontent à mon enfance).

L'une de mes autres passions, dont j'ai fait de bonne heure la découverte, est ma fascination pour la pratique de la magie. Dès que j'avais appris le fonctionnement d'un nouveau tour, je pratiquais, pratiquais et pratiquais encore jusqu'à le maîtriser totalement. Dans une certaine mesure, c'est à travers la magie que j'ai découvert la joie que l'on éprouve à apprendre des secrets.

Du pirate téléphonique au hacker

Ma première rencontre avec un manipulateur a eu lieu pendant mes années de lycée, lorsque j'ai fait la connaissance d'un étudiant totalement accaparé par un hobby appelé *phreaking* (le piratage téléphonique). Il s'agit d'un type de *hacking* qui permet d'explorer le réseau téléphonique en exploitant les réseaux et les employés des opérateurs téléphoniques. Cet étudiant m'a montré les astuces qu'il pouvait mettre en pratique avec un téléphone : par exemple, obtenir n'importe quel renseignement qu'un opérateur téléphonique détenait sur un client ou utiliser un numéro de test confidentiel pour passer gratuitement des appels longue distance. (En fait, ils n'étaient gratuits que pour nous. J'ai découvert beaucoup plus tard qu'il ne s'agissait nullement d'un numéro confidentiel, et que les appels étaient en réalité facturés à une innocente entreprise.)

Voilà mes premiers pas dans le milieu de la manipulation — mon école maternelle, pour ainsi dire. Mon ami, ainsi qu'un autre *phreaker* rencontré peu de temps après, m'ont fait écouter des appels *bidons* qu'ils effectuaient auprès de l'opérateur téléphonique. J'ai écouté ce qu'ils disaient et analysé ce qui les rendait crédibles ; j'ai appris à connaître les différents services de ces entreprises, leur jargon et leurs procédures. Mais cet "apprentissage" n'a pas duré pas longtemps ; ce n'était pas nécessaire. Rapidement, j'ai su tout faire moi-même, en apprenant à mon rythme et en faisant encore mieux que mes premiers maîtres.

Le chemin qu'allait prendre ma vie au cours des quinze années qui allaient suivre était tout tracé.

Au lycée, l'un de mes tours favoris consistait à obtenir un accès *a priori* non autorisé au commutateur téléphonique et à changer la "catégorie de service" d'un camarade phreaker. Lorsqu'il tentait de passer un appel de chez lui, il entendait un message qui lui demandait d'insérer une pièce, car le commutateur de l'opérateur téléphonique avait reçu une information indiquant qu'il appelait d'un téléphone payant.

Je me suis rapidement passionné pour tout ce qui concernait le monde des téléphones, pas seulement l'électronique, les commutateurs et les ordinateurs, mais également l'organisation de la profession, ses procédures et sa terminologie. En peu de temps, j'en savais probablement plus sur les opérateurs téléphoniques que n'importe quel employé. Et j'avais développé mes propres capacités de manipulation, à tel point qu'à dix-sept ans, j'étais capable de converser avec la plupart des employés des télécoms sur à peu près n'importe quel sujet, par téléphone ou même en personne.

À cette époque, nous employions le terme *hacker* pour désigner toute personne qui consacrait beaucoup de temps à bidouiller le matériel informatique et les logiciels, soit pour développer des programmes plus efficaces, soit pour contourner des étapes inutiles et terminer un travail plus rapidement. Le sens de ce terme est devenu négatif, véhiculant la notion de "criminel malveillant". Dans ces pages, je l'emploierai comme je l'ai toujours fait, c'est-à-dire dans son sens premier, plus neutre.

Après le lycée, j'ai étudié l'informatique au Computer Learning Center de Los Angeles. Au bout de quelques mois, le responsable informatique de l'école s'est aperçu que j'avais trouvé une faille dans le système d'exploitation et acquis les privilèges d'administration complets sur son ordinateur IBM. Les meilleurs experts en informatique de l'équipe enseignante n'arrivaient pas à comprendre comment j'avais fait. Et voilà ce qui pourrait constituer l'un des premiers exemples d'"embauche de hacker". Je me suis vu proposer une offre que je ne pouvais refuser : réaliser un projet de licence pour améliorer la sécurité informatique de l'école ou risquer la suspension pour

avoir piraté le système. Naturellement, j'ai choisi le projet de licence et finalement obtenu mon diplôme avec les honneurs.

Devenir un manipulateur

Certains se lèvent tous les matins en appréhendant la routine de leur journée de travail. Pour ma part, j'ai toujours eu la chance d'aimer mon travail. Vous n'imaginez pas les défis, les récompenses et le plaisir que j'ai eus pendant la période où j'étais détective privé. J'ai développé mes talents dans cet art que l'on appelle le "social engineering", la manipulation (qui consiste à obtenir des gens qu'ils fassent ce qu'ils ne feraient normalement pas pour un étranger) et ai été rémunéré pour cela.

Je n'ai eu aucune difficulté à devenir un manipulateur compétent. La branche paternelle de ma famille ayant évolué dans le commerce depuis des générations, l'art de la supercherie et de la persuasion ont dû faire partie des dons que j'ai hérités. Lorsque vous combinez ce don à une inclination à tromper les gens, vous obtenez le profil type du manipulateur.

On peut dire que le "métier" d'expert en persuasion comprend deux spécialités. Celui qui escroque et vole l'argent d'autrui appartient à la catégorie de l'*escroc*. Celui qui use de supercherie, de persuasion et de son pouvoir d'influence à l'encontre des entreprises, en visant généralement leurs informations, appartient à l'autre catégorie, celle du *manipulateur*. Dès l'époque de mes trajets gratuits en bus, alors que j'étais trop jeune pour savoir que ce que je faisais était mal, je m'étais reconnu un certain talent pour découvrir des secrets que je n'étais pas censé détenir. J'ai développé ce talent en utilisant la supercherie, en apprenant le jargon et en acquérant de solides compétences en manipulation.

L'une des méthodes que j'ai employées pour développer les techniques de mon métier, si je puis l'appeler un métier, a consisté à choisir des informations qui ne m'importaient pas vraiment, et à voir si je pouvais amener quelqu'un à l'autre bout du fil à me les fournir, juste pour améliorer ma technique. De la même façon que je pratiquais mes tours de magie, je m'exerçais au prétexte. Grâce à ces exercices, j'ai rapidement constaté que j'étais capable d'obtenir pratiquement toutes les informations que je souhaitais.

Comme je l'ai indiqué, des années plus tard, lors d'un témoignage au Congrès devant les sénateurs Lieberman et Thompson :

J'ai obtenu un accès non autorisé aux systèmes informatiques de certaines des plus grandes entreprises de la planète, et ai réussi à m'introduire dans certains des systèmes informatiques les plus résistants jamais développés. Je me suis servi à la fois de moyens techniques et non techniques pour obtenir le code source de divers systèmes d'exploitation et de dispositifs de télécommunication pour étudier leurs vulnérabilités et leur fonctionnement interne.

Toute cette activité n'a eu pour seul but que de satisfaire ma curiosité personnelle, pour voir ce dont j'étais capable et pour découvrir des informations secrètes sur les systèmes d'exploitation, les téléphones cellulaires et tout ce qui aiguisait ma curiosité.

DERNIÈRES RÉFLEXIONS

J'ai reconnu, depuis mon arrestation, que les actes que j'avais commis étaient illégaux, et que je violais la vie privée d'autrui.

Mes méfaits ont été dictés par la curiosité. J'ai voulu en savoir le plus possible sur le fonctionnement des réseaux téléphoniques et connaître dans les détails ce qui se rapportait à la sécurité informatique. Je suis passé du garçonnet qui aimait faire des tours de magie au hacker le plus célèbre du monde, redouté des entreprises et de l'administration. Lorsque je regarde les trente dernières années de ma vie, je reconnais que j'ai fait certains choix très malheureux, guidé par la curiosité, le désir d'approfondir mes connaissances techniques et le besoin de vrais challenges intellectuels.

Aujourd'hui, je suis différent. J'ai développé des talents et acquis de nombreuses connaissances sur la manière de sécuriser les informations et sur les tactiques de manipulation. Je les utilise maintenant pour aider l'administration, les entreprises et les individus à prévoir, détecter et répondre aux attaques dirigées contre la sécurité de leurs informations.

Ce livre est une autre façon de faire bénéficier les autres de mon expérience, de les aider à échapper aux attaques des voleurs d'informations malintentionnés qui sévissent sur la planète. J'espère que vous trouverez ces histoires distrayantes, instructives et pédagogiques.

Introduction

Cet ouvrage contient une mine de renseignements sur la sécurité des informations et la manipulation. Pour vous aider à vous y retrouver, voici un rapide aperçu de son organisation :

Dans la partie I, je révélerai quel est le maillon le plus faible de la sécurité et vous montrerai en quoi vous et votre entreprise êtes menacés par des attaques de manipulateurs.

Dans la partie II, vous verrez comment les manipulateurs jouent avec votre confiance, votre désir d'aider les autres, votre compassion et votre crédulité pour obtenir ce qu'ils veulent. Des histoires romancées mettant en scène des attaques classiques permettront de voir que les manipulateurs peuvent porter de nombreuses casquettes et prendre différents visages. Si vous croyez n'en avoir jamais rencontré, vous vous trompez certainement. Reconnaîtrez-vous un scénario vécu dans ces histoires et vous demanderez-vous si vous avez déjà été manipulé ? Cela se pourrait fort bien. Mais après avoir lu les Chapitres 2 à 9, vous saurez comment prendre le dessus au prochain appel d'un manipulateur.

La partie III du livre présente également des histoires inventées destinées à vous montrer comment le manipulateur atteint son but : comment il peut s'introduire dans les locaux de votre entreprise, dérober des secrets du type de ceux qui peuvent faire ou défaire une entreprise, et déjouer vos mesures de sécurité hautement sophistiquées. Ces scénarios vous donneront des informations sur différentes sortes de menaces, qui vont de la simple vengeance d'un employé au cyber-terrorisme. Si vous tenez aux informations qui permettent à vos affaires de durer, ainsi qu'au secret de vos données, lisez entièrement les Chapitres 10 à 14.

Il est important de noter que, sauf indication contraire, les anecdotes de ce livre sont purement fictives.

Dans la partie IV, je traite du discours d'entreprise à tenir pour faire échec aux attaques par manipulation lancées contre votre société. Le Chapitre 15 propose un plan détaillé de programmes de formation à la sécurité. Enfin, le Chapitre 16 pourrait simplement vous sauver la vie : il s'agit d'un ensemble complet de règles de sécurité que vous pouvez adapter à votre organisation et instaurer sur-le-champ afin de protéger votre entreprise et vos informations.

Pour finir, je propose une section intitulée "Identification des attaques", qui comprend des listes récapitulatives, des tableaux et des diagrammes résumant les informations essentielles susceptibles d'aider vos employés à déjouer l'attaque d'un manipulateur. Ces outils fournissent également des informations importantes pour l'élaboration de votre propre programme de formation à la sécurité.

Tout au long de ce livre, vous trouverez également plusieurs sections particulières : les rubriques Jargon donnent des définitions de termes employés dans le milieu de la manipulation et des hackers informatiques ; les Messages de l'auteur proposent des conseils concis pour renforcer votre stratégie en matière de sécurité ; enfin, les notes et les encadrés fournissent des données ou des explications supplémentaires.

Partie 1

Dans les coulisses

Chapitre 1

Le plus faible maillon de la sécurité

Une société qui achète les meilleures technologies de sécurité disponibles dans le commerce, qui forme son personnel à verrouiller tous ses secrets avant de quitter l'entreprise le soir et qui engage des vigiles auprès de la meilleure entreprise de gardiennage, n'en reste pas moins vulnérable. Le personnel peut appliquer toutes les mesures de sécurité possibles recommandées par les experts, installer méthodiquement tous les produits de sécurité conseillés et respecter scrupuleusement la bonne configuration des systèmes et l'application des mises à jour, il n'en reste pas moins vulnérable.

LE FACTEUR HUMAIN

En témoignant récemment devant le Congrès, j'ai expliqué que j'aurais souvent pu obtenir des mots de passe et d'autres informations sensibles d'entreprises en prétendant être quelqu'un d'autre et *en les demandant tout simplement.*

Il est naturel d'aspirer à un sentiment de sécurité absolue, ce qui conduit beaucoup de gens à avoir une fausse impression de tranquilité. Considérons le propriétaire d'un appartement qui équipe la porte d'entrée d'une serrure à gorge réputée inviolable, afin de protéger sa femme et ses enfants. Il se sent plus rassuré maintenant qu'il a mis sa famille à l'abri des intrus. Mais qu'en est-il de l'intrus qui brise une fenêtre ou trouve le code de la porte du garage ? Même si le père de famille installait un système de sécurité plus robuste, ce serait mieux, mais pas sûr à 100 % : verrous coûteux ou pas, le propriétaire reste vulnérable.

Pourquoi ? Parce que le véritable maillon faible de la sécurité, c'est le facteur humain.

La sécurité n'est trop souvent qu'une simple illusion, une illusion parfois encore accentuée lorsque la crédulité, la naïveté ou l'ignorance s'en mêlent. "Seules deux choses sont infinies, l'univers et la stupidité de l'homme, et je n'en suis pas certain pour la première", a ainsi déclaré le scientifique du XX^{e} siècle le plus respecté au monde, Albert Einstein. Finalement, les attaques des manipulateurs peuvent réussir lorsque les gens sont stupides ou, plus souvent, lorqu'ils ignorent simplement les bonnes mesures à prendre en matière de sécurité. De nombreux professionnels travaillant dans les technologies de l'information s'en tiennent à l'idée, fausse, qu'ils ont largement protégé leurs entreprises contre les attaques, parce qu'ils ont déployé des produits de sécurité standard — pare-feu, systèmes de détection d'intrusions ou dispositifs d'authentification plus robustes comme les cartes biométriques. Quiconque pense que les systèmes de sécurité offrent à eux seuls une vraie sécurité accepte l'*illusion* de sécurité. C'est un fait réel dans un monde utopique : inévitablement, tôt ou tard — mais généralement assez tôt —, cette personne connaîtra un incident en relation avec la sécurité.

Comme l'affirme l'éminent expert en sécurité Bruce Schneier, "la sécurité n'est pas un produit, c'est un processus". Qui plus est, la sécurité n'est pas qu'un problème de technologie, c'est un problème de personnes et de gestion.

À mesure que les développeurs continueront d'inventer de meilleures mesures de sécurité, rendant l'exploitation des failles techniques de plus en plus difficile, les agresseurs se tourneront davantage vers l'exploitation de l'élément humain. Percer le pare-feu humain est souvent facile, ne requiert aucun investissement (si ce n'est en appels téléphoniques) et implique un risque minimum.

UN CAS CLASSIQUE DE DUPERIE

La plus grande menace pour la sécurité des actifs professionnels est incarnée par le manipulateur, un magicien sans scrupule qui vous montre sa main gauche pendant que sa main droite vole vos secrets. Cette personne est souvent si amicale, charmante et obligeante que vous êtes heureux de l'avoir rencontrée.

Afin de mieux nous rendre compte de ce qu'est la manipulation, nous allons en étudier un exemple. Peu de gens se souviennent encore aujourd'hui d'un jeune homme nommé Stanley Mark Rifkin et de sa petite aventure avec la désormais défunte Security Pacific National Bank de Los Angeles. Comme les récits de son escapade varient et que Rifkin n'a jamais raconté son histoire, ce qui suit repose uniquement sur des rapports publiés.

Rupture de code

Nous sommes en 1978. Un jour, Rifkin va faire un tour dans la salle des virements électroniques de la Security Pacific National Bank, salle réservée au personnel autorisé, d'où sont envoyés et reçus des virements totalisant des milliards de dollars chaque jour.

Rifkin travaille au développement d'un système destiné à sauvegarder les données de la salle des virements, pour le cas où l'ordinateur principal tomberait en panne. Ce rôle lui permet d'accéder aux procédures de transfert, et notamment de connaître la façon dont les préposés de la banque opèrent pour faire un virement. Il apprend que les préposés autorisés à ordonner des virements électroniques se voient attribuer chaque matin un code étroitement surveillé, qu'ils utilisent pour appeler la salle des virements.

Dans cette salle, les employés se dispensent de retenir leur code quotidien : ils l'écrivent sur un bout de papier qu'ils collent à un endroit d'où ils peuvent facilement le lire. En ce jour précis de novembre, Rifkin a une bonne raison d'effectuer sa visite : il veut jeter un coup d'œil à ce papier.

En arrivant dans la salle des virements, il prend quelques notes sur les procédures de fonctionnement, prétendument pour s'assurer que le système de sauvegarde est bien coordonné avec les systèmes classiques. En même temps, il lit subrepticement le code de sécurité sur le morceau de papier d'un employé et l'apprend, puis sort quelques minutes plus tard. Comme il le dira par la suite, il a l'impression, à ce moment-là, qu'il vient de gagner au loto.

Il y a ce compte en Suisse...

En quittant la pièce vers quinze heures, il se rend directement à la cabine téléphonique située dans le hall en marbre de l'immeuble, d'où il appelle la salle des virements. Il change de casquette, laissant celle de Stanley Rifkin, consultant de la banque, pour prendre celle de Mike Hansen, membre du service international de la banque.

Voici approximativement la teneur de la conversation :

"Bonjour, ici Mike Hansen de l'international", dit-il à la jeune femme qui répond au téléphone.

Elle demande le numéro du bureau. C'est la procédure standard, et il le sait : "286", répond-il.

Son interlocutrice s'enquiert alors du code.

Rifkin a raconté plus tard que son rythme cardiaque, propulsé par l'adrénaline, a repris son rythme normal à cet instant. Il répond calmement "4789". Puis il donne des instructions de virement : "dix millions deux cent mille dollars exactement" à la Irving Trust Company à New York, afin de créditer la Wozchod Handelsbank de Zurich, en Suisse, où il a déjà un compte.

"Très bien, je l'ai. Et à présent, j'ai besoin du numéro de convention inter-établissement", répond la femme.

Rifkin se met à transpirer ; cette question n'était pas prévue, elle était passée à travers les mailles de ses recherches. Il parvient cependant à tenir son rôle, agit comme si tout était normal, mais enchaîne sur-le-champ, sans laisser de répit à son interlocutrice : "laissez-moi vérifier ; je vous rappellerai". Il change à nouveau de casquette pour appeler un autre service de la banque, en prétendant cette fois être un employé de la salle des virements électroniques. Il obtient le numéro et rappelle la femme, qui note ce dernier et le remercie. (Vu les circonstances, ce remerciement peut être considéré comme très amusant.)

Conclusion

Quelques jours plus tard, Rifkin s'envolait vers la Suisse, récupérait son argent et remettait huit millions de dollars à une agence russe en échange d'une poignée de diamants. Il faisait ensuite le chemin inverse et passait la douane américaine avec les pierres cachées dans une ceinture à billets. Il venait de réussir le plus gros casse de banque de l'Histoire, sans avoir utilisé d'arme, ni même d'ordinateur. Bizarrement, son hold-up l'a finalement mené dans les pages du Livre Guinness des records du monde, dans la catégorie de "la plus grosse fraude informatique".

Stanley Rifkin a exploité l'art de la supercherie, à savoir les compétences et techniques que l'on regroupe aujourd'hui sous le terme de *social engineering*. Un plan minutieux et du bagout, c'est tout ce qu'il a suffi.

Il s'agit précisément de ce que nous traitons dans ce livre : les techniques de manipulation (dans lesquelles votre serviteur excelle) et la façon d'éviter qu'elles ne soient utilisées dans votre entreprise.

NATURE DE LA MENACE

L'histoire de Rifkin nous éclaire parfaitement sur la façon dont on peut tromper notre sentiment de sécurité. Des épisodes comme celui-là se reproduisent *tous les jours* — d'accord, il ne s'agit pas toujours de casse à dix millions de dollars, mais d'incidents tout de même pernicieux. Peut-être perdez-vous de l'argent en ce moment même ou quelqu'un est-il en train de vous voler les plans d'un nouveau produit. Si cela n'est pas encore arrivé à votre entreprise, la question n'est pas de savoir *si* ça lui arrivera, mais *quand*.

Une préoccupation croissante

Dans une étude menée aux États-Unis en 2001 sur la criminalité informatique, le Computer Security Institute a indiqué que 85 % des organisations qui ont répondu à l'enquête ont détecté des brèches dans la sécurité de leurs ordinateurs au cours des douze derniers mois. Ce chiffre est renversant. Et seules 15 % d'entre elles ont pu déclarer n'avoir eu aucun problème de sécurité dans l'année. Le nombre d'entreprises qui ont indiqué avoir subi des pertes financières à cause de failles informatiques, soit 64 %, est tout aussi ahurissant. Plus de la moitié des sociétés ont donc subi des pertes financières, en *une seule année*.

Mon expérience personnelle me conduit à penser que les nombres indiqués dans de tels rapports sont quelque peu exagérés. Je me méfie de la manière dont ces enquêtes sont menées. Mais cela ne veut pas dire que les dommages ne soient pas considérables ; ils le sont. Les gens qui ne prévoient pas un incident de sécurité planifient un échec.

Les outils de protection vendus dans le commerce et déployés dans la plupart des entreprises protègent essentiellement les systèmes informatiques contre les intrus amateurs tels que les *script kiddies* (littéralement, les "gamins du script"). En réalité, ces simili-hackers, qui rêvent de célébrité et pensent l'atteindre en utilisant des logiciels téléchargés, ne sont généralement qu'ennuyeux. Les pertes les plus importantes, les véritables menaces, viennent d'attaquants sophistiqués qui ont des objectifs bien définis et sont motivés par l'argent. Ces personnes visent une cible à la fois, contrairement aux amateurs qui tentent d'infiltrer le plus de systèmes possible. L'intrus amateur est attiré par la quantité, le professionnel vise les informations de qualité et de valeur.

Les technologies telles que les dispositifs d'authentification (pour prouver une identité), de contrôle d'accès (pour gérer l'accès aux fichiers et aux ressources d'un système) et les systèmes de détection des intrusions (l'équivalent électronique des alarmes antivol) sont indispensables à un programme de sécurité d'entreprise. Toutefois, il est courant, encore aujourd'hui, qu'une entreprise dépense plus d'argent en café que dans la mise en œuvre de mesures de protection contre les attaques de sécurité.

Tout comme le criminel est incapable de résister à la tentation, le hacker s'emploie à trouver des failles dans les systèmes de protection.

Des pratiques trompeuses

On entend souvent dire qu'un ordinateur sûr est un ordinateur éteint. Cela peut paraître judicieux, mais c'est faux : un manipulateur peut persuader quelqu'un d'entrer dans un bureau et d'allumer l'ordinateur. Un adversaire qui veut vos informations les obtiendra, généralement par différents moyens. Ce n'est qu'une question de temps, de patience, de personnalité et d'obstination. C'est là que l'art de la supercherie entre en scène.

Pour déjouer des mesures de sécurité, un attaquant, un intrus ou un manipulateur doit trouver un moyen pour amener un utilisateur de confiance à lui révéler des informations ou à lui fournir un accès. Lorsque des employés fiables sont dupés, influencés ou manipulés au point qu'ils révèlent des informations sensibles ou que leurs actes débouchent sur une faille dans la sécurité, ce qui permet à l'attaquant de se glisser dans l'entreprise, aucune protection au monde n'y peut rien. De même que les cryptanalystes sont parfois capables de révéler le texte d'un message codé en trouvant une faiblesse qui leur permet de court-circuiter la technologie du codage, les manipulateurs manipulent vos employés pour court-circuiter les mesures de sécurité en vigueur.

ABUS DE CONFIANCE

Le plus souvent, les manipulateurs qui réussissent sont très conviviaux. Ils sont charmants, polis et attachants. Toutes ces caractéristiques sociales sont nécessaires pour établir rapidement un contact et gagner la confiance de leur interlocuteur. Un manipulateur expérimenté est capable d'obtenir l'accès à pratiquement n'importe quelle information en exploitant les stratégies et les tactiques du métier.

Les experts informatiques les plus compétents se sont efforcés de développer des solutions de sécurité de l'information afin de réduire au minimum les risques inhérents à l'utilisation des ordinateurs, mais ils ont négligé la vulnérabilité la plus importante : le facteur humain. Malgré notre intelligence, nous, les hommes — vous, moi, et tous les autres — demeurons la menace la plus forte pour la sécurité d'autrui.

Où il est question d'atavisme

Nous oublions ce qu'est la menace, en particulier dans le monde occidental. Aux États-Unis plus qu'ailleurs, nous ne sommes pas formés à nous méfier des autres. On nous enseigne qu'il faut aimer notre prochain et nous avons confiance et foi envers autrui. Voyez combien il est difficile pour les sociétés de surveillance de quartiers d'obtenir des habitants qu'ils ferment leurs portes et leur voiture à clé. Cette forme de vulnérabilité est évidente, mais elle semble ignorée par beaucoup, qui préfèrent vivre dans un monde imaginaire et jouer avec le feu, jusqu'au jour où ils se brûlent.

Nous savons que tout le monde n'est pas bon et honnête, mais trop souvent, nous vivons comme si c'était le cas. Cette aimable innocence a été le creuset des vies des Nord-Américains et il est pénible d'y renoncer. En tant que nation, nous avons introduit dans notre concept de liberté la notion que les meilleurs lieux de vie sont ceux où les verrous et les clés sont le moins nécessaires.

La plupart des gens continuent de penser qu'ils ne se feront pas duper par d'autres, et jugent la probabilité de l'être très faible. Les attaquants se servent donc de cette croyance courante : pendant tout le temps qu'ils exploitent la confiance de leurs victimes, leurs comportements et leurs demandes sont si raisonnables qu'ils ne soulèvent aucune suspicion.

Naïveté organisationnelle

Cette innocence, qui est l'une des caractéristiques des Américains, était évidente lorsque les ordinateurs ont commencé à être connectés à distance. Souvenez-vous que l'ARPANET (*Advanced Research Projects Agency Network*) du ministère de la Défense, le prédécesseur d'Internet, a été conçu pour que les institutions gouvernementales, de la recherche et de l'enseignement puissent partager des informations sur leurs études. L'objectif était la liberté de l'information et le progrès technique. Par conséquent, de nombreux établissements d'enseignement ont installé les premiers systèmes informatiques avec peu ou pas de sécurité. Un libertaire notable de l'informatique, Richard Stallman, a même refusé de protéger son compte par un mot de passe.

Mais aujourd'hui, Internet est utilisé pour le commerce électronique et les dangers liés à un faible niveau de sécurité dans notre monde connecté ont considérablement évolué. Et ce n'est pas en employant davantage de technologies que l'on va résoudre le problème de la sécurité lié au facteur humain.

Regardez seulement nos aéroports aujourd'hui. Bien que la sécurité soit devenue primordiale, nous apprenons parfois dans les médias que des voyageurs ont pu court-circuiter la sécurité et passer les points de contrôle avec

des armes. Comment cela est-il possible à une époque où les aéroports se trouvent dans un tel état d'alerte ? Les détecteurs de métaux ont-ils failli ? Non. Le problème ne se situe pas au niveau des machines. Le problème, c'est le facteur humain, ce sont les personnes qui manœuvrent les machines. Les responsables de l'aéroport auront beau aligner la garde nationale et installer des détecteurs de métaux et des systèmes de reconnaissance faciale, il est vraisemblablement beaucoup plus important que l'équipe de sécurité principale soit formée de façon à filtrer correctement les passagers.

Le même problème existe à l'intérieur des institutions gouvernementales, des entreprises et dans les établissements d'enseignement, partout dans le monde. Malgré les efforts déployés par les experts en sécurité, les informations restent vulnérables et continueront à être considérées comme une cible privilégiée par les attaquants doués pour la manipulation tant que le maillon le plus faible de la chaîne de sécurité, à savoir le maillon humain, n'aura pas été renforcé.

À présent plus que jamais, nous devons cesser de prendre nos désirs pour des réalités ; nous devons mieux nous informer sur les techniques utilisées par ceux qui essaient de s'en prendre à la confidentialité, à l'intégrité et à la disponibilité des informations présentes sur nos systèmes et nos réseaux informatiques. Nous avons accepté l'idée que nous devons nous protéger ; il est maintenant temps d'admettre l'importance d'une informatique défensive et d'apprendre à la pratiquer.

La menace d'une attaque qui viole votre intimité, votre pensée ou les systèmes informatiques de votre entreprise peut paraître improbable tant qu'elle ne se présente pas. Pour éviter que cela se produise, nous devons tous être informés, rester vigilants et protéger farouchement nos données, nos informations personnelles et les infrastructures critiques de notre pays. Et nous devons mettre en place ces protections aujourd'hui.

TERRORISTES ET DUPERIE

Naturellement, la supercherie n'est pas le seul outil du manipulateur. Le terrorisme physique crée les événements les plus importants, et nous en sommes venus à réaliser comme jamais auparavant que le monde est dangereux. La civilisation n'est, après tout, qu'un mince vernis.

Les attaques de New York et de Washington, en septembre 2001, ont apporté tristesse et peur dans le cœur de tous, non seulement des Nord-Américains, mais également de tous les gens bien intentionnés de toutes les nations. Nous savons désormais que des terroristes bien entraînés sont disséminés sur tout le globe et qu'ils attendent de lancer d'autres attaques.

Les efforts déployés récemment par le gouvernement américain ont élevé le niveau de conscience sécuritaire. Dans les pays occidentaux, la population doit rester vigilante et sur ses gardes envers toutes les formes de terrorisme. Elle doit comprendre comment les terroristes se fabriquent traîtreusement de fausses identités, composent des rôles d'étudiants et de voisins, et se fondent dans la foule. Ils cachent leurs véritables desseins tout en complotant et utilisent des mécanismes de supercherie semblables à ceux que vous découvrirez dans cet ouvrage.

Pour autant que je sache, les terroristes n'ont pas encore exploité de ruses par manipulation pour s'infiltrer dans les entreprises, les usines de traitement des eaux, les installations de production d'électricité ou d'autres lieux vitaux pour l'infrastructure d'un pays. C'est simplement trop facile ! Il n'est jamais trop tôt pour qu'émergent une conscience sécuritaire et une politique de sécurité, et j'espère que ce livre incitera la direction des entreprises à la mettre en place et à la renforcer.

À PROPOS DE CE LIVRE

La sécurité d'une société est une question d'équilibre. Si la sécurité pèche par défaut, votre entreprise est vulnérable ; si elle pèche par excès, cela conduit plutôt à délaisser les affaires courantes, paralysant la croissance et la prospérité de l'entreprise. Le défi consiste à atteindre un équilibre entre sécurité et productivité.

Nombre de livres sur la sécurité des entreprises insistent sur la technologie matérielle et logicielle, et ne traitent pas correctement la menace la plus sérieuse de toutes : la duperie humaine. À l'inverse, l'objectif de cet ouvrage est de vous aider à comprendre comment vous, vos collègues et d'autres personnes dans votre entreprise êtes manipulés, et de vous faire connaître les barrières que vous pouvez ériger pour arrêter d'être des victimes. Ce livre met principalement l'accent sur les méthodes non techniques auxquelles les intrus malveillants ont recours pour voler des informations et compromettre l'intégrité des données — que l'on suppose être sûres mais qui ne le sont pas —, ou détruire le produit du travail de l'entreprise.

Ma tâche est rendue plus difficile par le simple fait que chaque lecteur a été dupé par les plus grands experts en manipulation de tous les temps : ses parents. Vos parents ont trouvé les moyens d'obtenir, "pour votre bien", que vous fassiez ce qu'ils estimaient être le mieux. Les parents deviennent de grands menteurs tout comme les manipulateurs développent habilement des histoires, des raisons et des justifications pour parvenir à leurs fins. Oui, nous

avons tous été façonnés par nos parents, qui sont des manipulateurs bienveillants (mais parfois pas aussi bienveillants que cela).

Conditionnés par cette formation, nous sommes tous devenus vulnérables à la manipulation. Notre vie serait difficile si nous devions toujours être sur nos gardes, méfiants et soucieux à l'idée que nous pourrions devenir la dupe d'une personne qui tenterait de profiter de nous. Dans un monde parfait, nous ferions implicitement confiance aux autres, puisque les gens seraient honnêtes et dignes de confiance. Mais comme nous vivons dans un monde imparfait, nous devons conserver un certain niveau de vigilance afin de repousser les efforts de manipulation de nos adversaires.

Les parties principales de ce livre, les Parties 2 et 3, sont constituées d'histoires qui montrent les manipulateurs à l'œuvre. Vous y découvrirez :

- Une méthode habile à laquelle les pirates du téléphone ont eu recours il y a des années pour obtenir des numéros de téléphone non répertoriés auprès d'un opérateur téléphonique.
- Différentes méthodes utilisées par les attaquants pour convaincre même les employés vigilants et suspicieux de révéler le nom d'utilisateur et le mot de passe de leur ordinateur.
- Comment le dirigeant d'un centre opérationnel a coopéré avec un attaquant, lui permettant de voler des informations sur le produit le plus secret de son entreprise.
- La façon dont un attaquant a amené une femme à télécharger un logiciel qui espionnait à chaque fois qu'elle appuyait sur une touche de son clavier et qui lui en envoyait les détails par e-mail.
- Comment les détectives privés obtiennent des informations sur votre entreprise et sur vous-même, informations qui, je peux pratiquement l'affirmer, vous feraient froid dans le dos.

Lorsque vous prendrez connaissance de certaines histoires des Parties 2 et 3, vous penserez peut-être qu'elles sont impossibles, que personne ne peut vraiment se tirer de tous les mensonges, sales tours et intrigues qui y sont décrits. Dans tous les cas, la réalité est que ces récits décrivent des événements qui peuvent survenir et qui surviennent ; nombre d'entre eux se produisent chaque jour quelque part dans le monde, peut-être même dans votre entreprise au moment où vous lisez ce livre.

Le contenu de cet ouvrage vous ouvrira vraiment les yeux lorsque vous aurez à protéger votre entreprise, mais aussi à déjouer personnellement les propositions d'un manipulateur et à protéger l'intégrité de votre vie privée.

Dans la Partie 4 de ce livre, mon objectif est de vous aider à établir des règles commerciales indispensables, ainsi qu'un programme de formation destiné à favoriser la prise de conscience des employés afin de minimiser les risques qu'ils soient un jour trompés par un manipulateur. Connaître les stratégies, méthodes et tactiques du manipulateur vous aidera à mettre en place des contrôles adéquats et à sécuriser vos données informatiques sans saper la productivité de votre entreprise.

En résumé, j'ai rédigé cet ouvrage pour vous aider à prendre davantage conscience de la sérieuse menace que constitue la manipulation. Je veux aussi vous aider à vérifier que votre entreprise et vos employés sont moins sujets à être abusés de cette façon. Ou peut-être devrais-je dire beaucoup moins sujets à être *encore* abusés *à l'avenir.*

Partie 2

L'art de l'attaquant

Chapitre 2

Quand une information anodine ne l'est pas

Que pensent la plupart des gens de la véritable nature de la menace que représentent les manipulateurs ? Que devez-vous faire pour vous tenir sur vos gardes ?

Si l'on imagine que des manipulateurs peuvent chercher à s'emparer d'éléments de grande valeur — qui sont par exemple vitaux pour le capital intellectuel de l'entreprise —, il faudra probablement prévoir de consolider son système de défense et d'augmenter le nombre de gardiens fortement armés.

En réalité, une personne malveillante peut mettre à mal la sécurité d'une entreprise simplement en se procurant certains renseignements ou documents : il s'agit généralement d'informations qui paraissent tellement anodines, tellement courantes et sans importance que la plupart des employés ne voient aucune raison de les protéger ou d'en contrôler la diffusion.

LA VALEUR CACHÉE D'UNE INFORMATION

La plupart des informations apparemment banales qui circulent dans une entreprise sont prisées par les attaquants qui utilisent des techniques de manipulation, car elles peuvent leur être très utiles pour paraître crédibles.

Dans ce chapitre, nous allons voir comment les manipulateurs procèdent en laissant les personnes "assister" aux attaques dont elles sont victimes. Je présente parfois l'action du point de vue de la victime — ce qui vous permet de vous mettre à sa place et d'évaluer comment vous (ou l'un de vos

employés ou collègues) auriez pu réagir —, mais aussi du point de vue du manipulateur.

La première histoire concerne une faille dans le monde de la finance.

CreditChex

Pendant longtemps, les Britanniques ont eu un système bancaire très "vieux jeu". Un Britannique typique, c'est-à-dire honnête, n'aurait pas pu rentrer dans une banque pour y ouvrir un compte. Il aurait été impensable pour une banque de vous accepter comme client si vous n'aviez pas été présenté par un client déjà connu avec une lettre de recommandation.

Quelle différence, évidemment, avec le monde bancaire apparemment égalitaire d'aujourd'hui ! Et dans notre monde moderne, la facilité à faire des affaires n'est nulle part ailleurs plus évidente qu'en Amérique du Nord, démocratique et bienveillante, où presque tout le monde peut entrer dans une banque et ouvrir facilement un compte courant, pas vrai ? Eh bien… pas exactement. En vérité, les banques sont peu disposées, et on les comprend, à ouvrir un compte à une personne qui a peut-être déjà émis des chèques sans provision — ce qui serait presque aussi malvenu que d'avoir un casier judiciaire suite à un vol ou d'être poursuivi pour détournement de fonds. Par conséquent, il est de pratique courante, dans de nombreuses banques, de mener une petite enquête sur le client potentiel avant de l'accepter… ou de le rejeter.

L'une des principales entreprises qui fournissent des informations aux banques est un établissement que nous appellerons CreditChex. Elle offre un service de qualité à ses clients mais, comme de nombreuses entreprises, elle peut également, et sans le savoir, rendre service aux manipulateurs malins.

Premier appel : Kim Andrews

"National Bank, ici Kim."

"Bonjour. Voilà, j'ai besoin d'un renseignement. Utilisez-vous CreditChex ?"

"Oui."

"Lorsque vous téléphonez à CreditChex, comment appelez-vous le numéro d'identification que vous leur donnez — est-ce un 'Merchant ID' ?"

Pause ; elle réfléchit à la question, se demandant de quoi il s'agit et si elle doit répondre.

Oscar enchaîne rapidement, sans lui laisser de répit :

"Voyez-vous, Kim, je travaille sur un livre, et ce livre traite d'enquêtes privées."

"Oui", dit-elle, répondant à la question avec assurance, heureuse d'aider un écrivain.

"Ainsi, on appelle ça un Merchant ID, n'est-ce pas ?

"Hmm hmm."

"OK, très bien. Je voulais être sûr d'employer le bon jargon. Pour le livre. Merci pour votre aide. Au-revoir, Kim."

Deuxième appel : Chris Talbert

"National Bank, nouveaux comptes, ici Chris."

"Bonjour Chris. Alex à l'appareil. Je représente le service client chez CreditChex. Nous réalisons une étude pour améliorer nos services. Pouvez-vous m'accorder deux minutes ?"

Chris répond qu'elle le fera volontiers et Alex poursuit :

"Très bien. Quelles sont les heures d'ouverture de votre bureau ?" Elle répond à cette question, puis au flot de questions qui suivent :

"Combien d'employés de votre bureau utilisent notre service ?"

"À quelle fréquence nous appelez-vous pour un renseignement ?"

"Lequel de nos 800 numéros vous a-t-on affecté pour nous appeler ?"

"Quel est notre délai de réponse ?"

"Depuis combien de temps travaillez-vous à la banque ?"

"Quel Merchant ID utilisez-vous actuellement ?"

"Avez-vous déjà trouvé des inexactitudes dans les informations que nous vous avons fournies ?"

"Si vous aviez des suggestions pour améliorer notre service, quelles seraient-elles ?"

Et enfin :

"Accepteriez-vous de remplir régulièrement des questionnaires si nous vous les envoyions au bureau ?"

Elle accepte, ils discutent un peu, Alex raccroche et Chris reprend son travail.

Troisième appel : Henry McKinsey

"CreditChex, Henry McKinsey, en quoi puis-je vous aider ?"

Mark dit qu'il fait partie de la National Bank. Il fournit le bon numéro d'identification puis le nom et le numéro de sécurité sociale de la personne sur laquelle il sollicite des renseignements. Henry demande la date de naissance, que Mark lui donne également.

Après quelques instants, Henry lit le listing qui apparaît sur son écran d'ordinateur.

"Wells Fargo déclaré NSF en 1998, une fois, montant de 2 066 dollars." NSF (fonds insuffisants) est le sigle habituel employé par les banques américaines pour indiquer que des chèques ont été émis alors qu'il n'y avait pas assez d'argent sur le compte pour les honorer.

"D'autres activités depuis ?"

"Aucune activité."

"Y a-t-il eu d'autres requêtes ?"

"Voyons. Eh bien, deux, le mois dernier. Third United Credit Union de Chicago." Il bute sur le nom suivant, Schenectady Mutual Investments, et doit l'épeler. "C'est dans l'État de New York", ajoute-t-il.

Un détective privé à l'œuvre

Ces trois appels ont été passés par la même personne : un détective privé que nous appellerons Oscar Grace. Grace avait un nouveau client. Encore policier quelques mois auparavant, il pensait qu'une partie de son nouveau métier irait de soi mais qu'une autre allait représenter un défi pour son inventivité. Cette mission tombait résolument dans cette seconde catégorie.

Tout comme les privés de la fiction — les Sam Spade et autres Philip Marlowe —, les vrais détectives privés attendent de longues heures dans leur voiture, la nuit, à essayer d'attraper des épouses infidèles. Ils accomplissent également un travail tout aussi important, bien qu'on le remarque moins, lorsqu'ils surveillent les épouses en conflit avec leur mari par exemple. Ce travail repose plus sur des compétences en manipulation que sur une résistance à l'ennui qui sévit lors des attentes nocturnes.

La nouvelle cliente de Grace était une femme qui semblait disposer d'un budget confortable pour sa garde-robe et ses bijoux. Elle était venue un jour à son bureau et avait pris place dans le fauteuil en cuir, le seul qui ne soit pas encombré par une pile de dossiers. Après avoir posé son grand sac à main Gucci sur le bureau, le symbole de la marque tourné vers Grace, elle avait annoncé qu'elle envisageait d'informer son mari de son intention de divorcer. Seulement "il y avait un tout petit problème"...

Il apparaissait que son mari avait pris une longueur d'avance. Il avait déjà retiré l'argent de leur compte d'épargne et une somme encore plus importante de leur P.E.A. Elle voulait savoir où avaient été entreposés leurs biens, et son avocat ne lui était d'aucune aide. Grace devinait que l'homme de loi était l'un de ces avocats haut placés des quartiers résidentiels qui ne voulait pas se salir les mains avec des problèmes d'argent de ce genre.

Grace pouvait-il l'aider ?

Il lui assure que ce sera un jeu d'enfant, indique ses tarifs, estime le montant de ses dépenses, et ramasse un chèque d'acompte.

Puis il regarde le problème en face. Que faire lorsque vous n'avez jamais été confronté à un travail comme celui-ci et ne savez absolument pas comment vous y prendre pour retrouver une somme d'argent ? Vous avancez à tout petits pas. Voici, selon nos sources, l'histoire de Grace.

"Je connais CreditChex et sais comment les banques utilisent cet établissement, car mon ex-femme a travaillé dans une banque. Mais je ne connais pas le jargon et les procédures, et essayer de joindre mon ex serait une perte de temps."

Première étape : obtenir la terminologie exacte et trouver comment formuler ma demande afin de donner l'impression d'avoir déjà quelques connaissances. À la banque que j'appelle, la première jeune femme, Kim, se montre méfiante lorsque je lui demande comment ils s'identifient lorsqu'ils appellent CreditChex. Elle hésite ; elle ne sait pas si elle doit me répondre. En suis-je déconcerté ? Pas le moins du monde. En fait, son hésitation me fournit un indice important, c'est le signe que je dois fournir une raison qui lui semble crédible. Lorsque j'affirme que j'effectue des recherches pour un livre, cela lève ses doutes. Vous dites que vous êtes auteur ou scénariste, et tout le monde vous répond sans rechigner.

Kim possédait d'autres informations susceptibles de m'aider, comme les renseignements demandés par CreditChex pour identifier la personne au sujet de laquelle vous appelez, les informations que vous pouvez solliciter et, surtout, le Merchant ID. J'étais prêt à poser ces questions, mais son hésitation a levé le drapeau rouge. Elle a avalé l'histoire des recherches pour un livre, mais elle a encore quelques soupçons. Si elle s'était montrée mieux disposée, je lui aurais demandé de révéler davantage de détails sur leurs procédures.

Il faut progresser à l'instinct, écouter attentivement ce que la victime d'une manipulation dit et comment elle le dit. Cette femme paraissait suffisamment intelligente pour tirer la sonnette d'alarme si je lui avais posé trop de questions inhabituelles. Et même si elle ne savait pas qui j'étais ou de quel numéro j'appelais, il n'en reste pas moins que dans ce business, on ne veut pas que le personnel soit accaparé par un individu qui demande des informations précises. C'est pourquoi il ne faut pas "brûler sa source" : on peut être amené à rappeler le même bureau plus tard.

Jargon

Brûler sa source
Un attaquant a brûlé sa source lorsque la victime s'est rendu compte de l'attaque. Dès que la victime a connaissance de l'attaque et qu'elle avertit les autres employés ou la direction, il devient extrêmement difficile d'exploiter cette même source lors d'attaques ultérieures.

Je suis toujours à l'affût de petits signes qui m'indiquent le niveau de coopération d'une personne, sur une échelle allant de "Vous me paraissez convenable et je crois tout ce que vous me dites" à "Appelez la police, ce type prépare un mauvais coup".

Comme je trouve que Kim est à la limite, j'appelle quelqu'un dans un autre bureau. Lors de mon deuxième appel, avec Chris, l'astuce de l'enquête joue comme un charme. Là, la tactique consiste à glisser les questions importantes dans un tas d'autres questions sans conséquence qui servent à apporter de la crédibilité. Avant de lâcher la question sur le numéro d'identification avec CreditChex, j'exécute un dernier petit test en lui posant une question personnelle sur son ancienneté dans la banque.

Une question personnelle comme celle-là est comme une mine. Par conséquent, si je pose une question personnelle et si elle y répond sans que sa voix ait changé, cela signifie qu'elle n'est pas soupçonneuse quant à la nature de la question. Je peux sans danger poser la question voulue sans éveiller ses soupçons, et elle me fournira certainement la réponse que j'attends.

Autre chose connue de tout bon détective privé : ne jamais terminer la conversation après avoir obtenu le renseignement clé. Deux ou trois autres questions, une petite conversation, et on peut dire au revoir. Plus tard, si la victime se remémore ce que vous lui avez demandé, il s'agira probablement des dernières questions. Les autres seront généralement oubliées.

Ainsi, Chris m'a indiqué leur Merchant ID et le numéro de téléphone qu'ils appellent pour poser leurs questions. J'aurais été plus satisfait si j'avais pu poser quelques questions sur la quantité d'informations qu'il est possible d'obtenir de CreditChex. Mais il était préférable de ne pas y aller trop fort.

C'était comme avoir un chèque en blanc de CreditChex. Je pouvais désormais appeler et obtenir des informations quand je le voulais. Je n'avais même pas besoin de payer. En l'occurrence, le représentant de CreditChex était heureux de me fournir exactement les informations que je voulais : deux établissements auxquels le mari de ma cliente s'était récemment adressé pour ouvrir un compte. Par conséquent, où se trouvaient les biens que sa future ex-femme recherchait sinon dans les institutions bancaires que m'avait indiquées ce quidam de chez CreditChex ?

Analyse de l'arnaque

Toute la ruse est fondée sur l'une des tactiques fondamentales de la manipulation, qui consiste à avoir accès à des informations qu'un employé de l'entreprise considère anodines, alors qu'elles ne le sont pas.

Le premier employé de la banque a confirmé la terminologie qui permet de décrire le numéro d'identification utilisé pour appeler CreditChex : le Merchant ID. La deuxième employée a fourni le numéro de téléphone pour appeler CreditChex, ainsi que le renseignement essentiel, à savoir le Merchant ID de la banque. Toutes ces informations lui paraissaient insignifiantes. Après tout, cette employée savait qu'elle s'adressait à quelqu'un de chez CreditChex, par conséquent il n'y avait pas de mal à divulguer le numéro !

Toutes ces démarches servaient à préparer le troisième appel. Grace disposait de tout ce dont il avait besoin pour téléphoner à CreditChex, se faire passer pour un représentant de l'une de leurs banques clientes, National, et demander simplement les renseignements qui l'intéressaient.

Aussi habile pour extorquer des informations que l'est un bon escroc pour voler de l'argent, Grace était très doué pour cerner les gens. Il connaissait la tactique courante qui consiste à cacher les questions clés parmi des questions anodines. Il savait qu'en posant une question personnelle à la deuxième employée, il testerait sa bonne volonté à coopérer, et qu'il pourrait ensuite lui demander innocemment le numéro d'identification.

L'erreur commise par la première employée, en confirmant la terminologie du numéro d'identification de CreditChex, était presque impossible à éviter. Ce terme est si largement répandu dans le monde bancaire qu'il apparaît sans importance : c'est le modèle même de ce qui est anodin. Mais la seconde

employée, Chris, n'aurait pas dû répondre aux questions sans vérifier précisément que son interlocuteur était vraiment celui qu'il prétendait être. Elle aurait dû, pour le moins, prendre son nom et son numéro de téléphone et le rappeler ; ainsi, si la moindre question s'était posée plus tard, elle aurait gardé une trace du numéro de téléphone utilisé par le correspondant. Dans ce cas, il aurait été plus difficile pour l'attaquant de se faire passer pour un représentant de CreditChex.

Le message de Mitnick

Dans cette situation, un Merchant ID équivaut à un mot de passe. Dans votre entreprise, existe-t-il un code ou un numéro interne que les gens ne traitent pas avec suffisamment de précautions ?

Il aurait été encore préférable d'appeler CreditChex en utilisant un numéro déjà répertorié par la banque — et non communiqué par l'interlocuteur —, ce qui aurait permis de vérifier que celui-ci travaille effectivement pour l'entreprise et qu'il réalise bien une enquête auprès des clients. Toutefois, dans la pratique, et vu que la plupart des gens manquent toujours de temps, ce type de vérification d'appels téléphoniques demande beaucoup trop de temps, excepté lorsqu'un employé suspecte qu'une attaque est en cours.

LE PIÈGE DU MANIPULATEUR

Il est bien connu que les chasseurs de têtes utilisent des tactiques de manipulation pour recruter les talents d'une entreprise. Nous en présentons ci-après un exemple.

À la fin des années quatre-vingt-dix, un service d'embauche assez peu moral accepte un nouveau client, une entreprise qui recherche des ingénieurs en électricité ayant une expérience dans l'industrie du téléphone. La tête pensante du projet est une femme enjôleuse, dotée d'une voix gutturale qu'elle a appris à utiliser pour inspirer immédiatement confiance et sympathie au téléphone.

Elle décide d'organiser un raid sur un fournisseur de services téléphoniques cellulaires, afin de voir si elle peut localiser quelques ingénieurs tentés de traverser la rue pour un concurrent. Elle ne peut évidemment pas appeler directement la standardiste en lui demandant de la mettre en contact avec un ingénieur ayant cinq ans d'expérience. Pour des raisons qui s'éclaireront par la suite, elle commence donc son attaque en demandant des renseignements qui paraissent dénués de tout intérêt et que le personnel de l'entreprise donne à quiconque, ou presque, les sollicite.

Premier appel : la réceptionniste

La femme, utilisant le nom de Didi Sands, appelle le siège de la société de services téléphoniques cellulaires. La conversation se déroule approximativement comme suit :

La réceptionniste : "Bonjour. Marie à l'appareil, que puis-je faire pour vous ?"

Didi : "Pouvez-vous me mettre en relation avec le service Transport ?"

R : "Je ne suis pas sûre que nous en ayons un, je regarde dans mon répertoire. De la part de qui ?"

D : "Didi."

R : "Êtes-vous dans l'immeuble ou... ?"

D : "Non, je suis à l'extérieur."

R : "Didi comment ?"

D : "Didi Sands. J'avais le poste du Transport, mais j'ai oublié le numéro."

R : "Un instant."

Pour dissiper les soupçons, Didi pose alors une question anodine "juste pour établir la connexion", et destinée à indiquer qu'elle connaît bien l'entreprise.

D : "Dans quel immeuble êtes-vous : Lakeview ou Main Place ?"

R : "Main Place. (*Pause.*) C'est le 805 555 6469."

Pour assurer ses arrières au cas où l'appel au Transport ne donnerait pas ce qu'elle recherche, Didi indique qu'elle veut aussi parler au service Immobilier. La réceptionniste lui en fournit également le numéro. À la demande de Didi, la réceptionniste essaie de lui passer le service du Transport, mais la ligne est occupée.

Didi demande alors un *troisième* numéro de téléphone, celui des Comptes clients, situé dans un établissement de l'entreprise, à Austin, au Texas. La réceptionniste lui demande de patienter un instant et pose le téléphone. Pour indiquer à la Sécurité qu'elle a un appel téléphonique suspect et qu'elle pense qu'il se trame quelque chose ? Pas du tout, cette attente n'a rien à voir avec Didi. Elle est bien un petit peu casse-pieds, mais pour la réceptionniste, cela fait partie de la routine. Après une minute environ, la réceptionniste revient, cherche le numéro des Comptes clients, appelle le service et le met en relation avec Didi.

Deuxième appel : Peggy

La conversation suivante se déroule ainsi :

Peggy : "Comptes clients, Peggy."

Didi : "Bonjour, Peggy. Ici Didi, à Thousand Oaks."

P : "Bonjour Didi."

Didi emploie alors un terme habituel dans le monde de l'entreprise, le code du compte de charge sur lequel sont affectées les dépenses par rapport au budget :

D : "J'ai une question à vous poser. Comment puis-je trouver le centre des coûts d'un service particulier ?"

P : "Vous devez obtenir une autorisation de l'analyste budgétaire du service en question."

D : "Sauriez-vous qui est l'analyste budgétaire du siège social de Thousand Oaks ? J'essaie de remplir un formulaire et je ne sais pas quel est le centre des coûts."

P : "Je sais juste que quand vous avez besoin d'un numéro de centre des coûts, vous appelez votre analyste budgétaire."

D : "Avez-vous un centre des coûts pour votre service, ici au Texas ?"

P : "Nous avons notre propre centre des coûts, mais ils ne nous donnent pas leur liste complète."

D : "Combien de chiffres compte le centre des coûts ? Par exemple, quel est votre centre des coûts ?"

P : "Eh bien, par exemple, avez-vous 9WC ou SAT ?"

Didi n'a aucune idée des services ou des groupes auxquels cela fait référence, mais cela n'a pas d'importance. Elle répond :

D : "9WC."

P : "Alors en général, c'est quatre chiffres. Vous avez dit que vous étiez avec qui ?"

D : "Au siège social, Thousand Oaks."

P : "Bien, en voilà un de Thousand Oaks : c'est 1A5N, N comme Nancy."

En passant simplement assez de temps avec une personne disposée à aider, Didi obtient le numéro du centre des coûts dont elle a besoin, et qui fait partie de ces renseignements que personne ne songe à protéger puisqu'ils n'ont *a priori* aucune valeur pour un profane.

Troisième appel : un mauvais numéro bien utile

Didi appelle le service Immobilier, prétextant qu'elle a fait un mauvais numéro. Elle commence par "Désolée de vous déranger, mais...", et prétend être une employée qui a perdu le répertoire téléphonique de son entreprise. Elle demande donc qui elle doit contacter pour s'en procurer un nouvel exemplaire. L'homme lui dit que la version imprimée n'est plus à jour, mais que le répertoire est disponible sur le site intranet de l'entreprise.

Didi déclare qu'elle préfère utiliser un exemplaire papier et son interlocuteur l'invite à appeler Publications puis, sans qu'elle le sollicite — peut-être simplement pour rester un peu plus longtemps au téléphone avec cette femme à la voix enjôleuse —, cherche le numéro et le lui donne.

Quatrième appel : Bart chez Publications

Chez Publications, elle tombe sur un employé nommé Bart. Didi annonce qu'elle fait partie de Thousand Oaks, et qu'un nouveau consultant a besoin d'un exemplaire du répertoire de l'entreprise. Elle précise qu'un exemplaire papier conviendrait mieux au consultant, même s'il n'est pas vraiment à jour. Bart lui répond qu'elle doit remplir un formulaire de demande et le lui envoyer.

Didi indique qu'elle n'a plus de formulaires, que c'est urgent et que Bart serait un amour s'il voulait bien remplir un formulaire pour elle. Il accepte avec un enthousiasme révélateur et Didi lui fournit les détails. Pour l'adresse du fournisseur fictif, elle indique le numéro d'une *boîte aux lettres*, du type boîte postale d'entreprise (sa société loue des boîtes pour ce genre de situations).

Il pourrait y avoir des frais pour le prix et l'envoi du répertoire. "Bien. À présent, indiquez-moi le centre des coûts de Thousand Oaks."

"1A5N, N comme Nancy."

Quelques jours plus tard, lorsque Didi reçoit le répertoire de l'entreprise, elle constate que l'investissement est encore plus rentable que prévu : le répertoire fournit non seulement les noms et les numéros de téléphone, mais il indique également qui travaille pour qui, c'est-à-dire qu'il donne la structure complète de l'entreprise.

La femme à la voix grave a extorqué les informations dont elle avait besoin pour lancer son raid, grâce à un bagout et à des manières typiques du manipulateur expérimenté. Elle est maintenant fin prête pour chasser les têtes par téléphone.

Analyse de l'arnaque

Dans cette attaque avec manipulation, Didi commence par se procurer les numéros de téléphone de trois services de l'entreprise visée. Cela lui est facile car les numéros qu'elle demande ne sont pas secrets, d'autant moins pour les employés. Un manipulateur apprend à se faire passer pour un initié, et Didi est experte à ce jeu. L'un des numéros de téléphone la conduit au numéro d'un centre des coûts, qu'elle utilise ensuite pour se procurer un exemplaire du répertoire des employés de l'entreprise.

Le message de Mitnick

Comme les pièces d'un puzzle, chaque information, si elle est prise tout seule, peut sembler insignifiante. Par contre, lorsque les éléments sont rassemblés, une image claire apparaît. Ici, pour le manipulateur, l'image est celle de la structure interne complète de l'entreprise.

Dans cet exemple, il a suffi au manipulateur de paraître aimable, d'employer un peu du jargon du métier et, avec la dernière victime, de glisser quelques mots en guise de clin d'œil.

Mais il a également fallu un élément essentiel et que l'on acquiert difficilement, à savoir une capacité à manipuler, perfectionnée par une pratique intensive et par l'application de leçons transmises par de nombreuses générations de confidents.

D'AUTRES INFOS "SANS IMPORTANCE"

Outre les numéros de téléphone et de postes internes d'un centre des coûts, quelles autres informations apparemment sans valeur peuvent s'avérer extrêmement intéressantes pour votre ennemi ?

Appel téléphonique de Peter Abels

"Bonjour", dit la voix à l'autre bout du fil. "Ici Tom, de Parkhurst Travel. Vos billets pour San Francisco sont prêts. Voulez-vous que nous vous les envoyions ou souhaitez-vous venir les chercher vous-même ?"

"San Francisco ?" interroge Peter. "Je ne vais pas à San Francisco."

"Vous êtes bien Peter Abels ?"

"Oui, mais je n'ai prévu aucun voyage prochainement."

"Eh bien, répond Tom avec un rire sympathique, vous êtes sûr que vous ne voulez pas aller à San Francisco ?"

"Si vous pensez pouvoir en persuader mon patron..." dit Peter, en poursuivant le jeu de la conversation amicale.

"Cela m'a tout l'air d'un malentendu", indique Tom. Sur notre système, nous enregistrons les prévisions de voyages sous le numéro des employés. Quelqu'un a peut-être employé un mauvais numéro. Quel est votre numéro d'employé ?

Peter indique obligeamment son numéro. Et pourquoi pas ? Il figure sur pratiquement tous les formulaires personnels qu'il remplit, et un grand nombre de personnes dans l'entreprise y ont accès : les ressources humaines, la paie et, naturellement, l'agence de voyage extérieure. Personne ne traite un numéro d'employé comme un secret. Quel danger cela pourrait-il bien représenter ?

La réponse est facile à imaginer. Deux ou trois éléments d'information pourraient être suffisants pour usurper une identité, c'est-à-dire pour que le manipulateur revête lui-même l'identité d'un autre. En se procurant le nom d'un employé, son numéro de téléphone et son numéro d'employé — et, éventuellement, pour faire bonne figure, le nom et le numéro de téléphone de son directeur —, un manipulateur à peu près compétent détient l'essentiel des données nécessaires pour que son identité paraisse authentique à la prochaine personne qu'il va appeler.

Si une personne prétendant appartenir à un autre service de votre entreprise avait appelé hier, pour une raison plausible, et avait demandé votre numéro d'employé, auriez-vous eu la moindre hésitation à le lui donner ?

Et à propos, quel est votre numéro de sécurité sociale ?

Le message de Mitnick

Morale de l'histoire : ne donnez aucune information personnelle ou interne à l'entreprise à qui que ce soit, à moins que sa voix ne vous soit connue ou que vous sachiez précisément de qui il s'agit.

EMPÊCHER LES ARNAQUES

L'entreprise a la responsabilité d'informer les employés sur la manière dont une erreur sérieuse peut survenir lorsque des informations non publiques ne sont pas traitées correctement. Une politique de sécurisation des informations bien conçue, associée à une formation adéquate, permettront aux employés d'améliorer considérablement leurs connaissances sur la bonne

gestion des informations commerciales de l'entreprise. Une politique de classification des données vous aidera à mettre en place des contrôles appropriés sur la divulgation des informations. Si une telle politique n'existe pas, toutes les informations internes doivent être considérées comme confidentielles, sauf indication contraire.

Pour protéger votre entreprise contre la fuite d'informations apparemment anodines, il faut prendre les mesures suivantes :

- Le service de sécurisation des informations doit dispenser une formation qui détaille les méthodes utilisées par le manipulateur, afin d'aider les employés à en prendre conscience. Comme nous venons de le voir, une des méthodes consiste à obtenir des renseignements apparemment anodins et à les exploiter pour mettre rapidement en confiance son interlocuteur. Chaque employé doit être averti que lorsqu'une personne qui appelle connaît les procédures de l'entreprise, son jargon et des informations internes, en aucun cas cela ne permet de l'identifier ni ne l'autorise à demander des renseignements. Il peut s'agir d'un ancien employé ou d'un fournisseur qui dispose des informations requises. En conséquence, chaque entreprise a la responsabilité de déterminer la méthode d'authentification appropriée qu'un employé doit appliquer lorsqu'il est en contact avec des gens qu'il ne connaît pas.
- Les personnes qui sont chargées de mettre en place une politique de classification des données doivent examiner le type de détails qu'un manipulateur peut exploiter pour atteindre des employés, détails apparemment anodins mais qui peuvent mener à des informations sensibles. Il est évident que vous ne dévoileriez jamais le code secret de votre carte bancaire, mais indiqueriez-vous le serveur dont vous vous servez pour développer les logiciels de votre entreprise ? Ces informations pourraient-elles être utilisées par une personne qui prétend avoir légitimement accès au réseau de l'entreprise ?
- Parfois, le simple fait de connaître le vocabulaire interne à l'entreprise peut faire apparaître le manipulateur comme autorisé et bien informé. Les attaquants s'appuient souvent sur cette confusion courante pour convaincre, par duperie, leurs victimes... complaisantes malgré elles. Par exemple, le Merchant ID est un numéro d'identification dont le personnel du service des nouveaux comptes d'une banque se sert quotidiennement. Mais un tel numéro équivaut à un mot de passe. Si les employés comprenaient l'importance de cet identifiant, qui est utilisé pour identifier précisément un demandeur, ils y accorderaient une plus grande attention.

- Très peu d'entreprises — voire aucune — donnent le numéro d'appel direct de leur P.-D.G. Cependant, la majorité ne voient aucun inconvénient à donner les numéros de la plupart de leurs services, en particulier à quelqu'un qui est ou paraît être un employé. Une des contre-mesures possibles consiste à mettre en place une politique qui interdit de donner aux étrangers les numéros de téléphone internes des employés, fournisseurs, consultants et intérimaires. Plus important encore : il faut mettre en place une procédure afin de déterminer précisément si la personne qui appelle pour demander des numéros de téléphone est vraiment employée dans l'entreprise.

Le message de Mitnick

Comme le dit le vieux proverbe — même les vrais paranoïaques ont probablement des ennemis. Nous devons donc supposer que toute entreprise a également des ennemis : par exemple, des attaquants qui visent l'infrastructure du réseau pour compromettre des secrets commerciaux. Ne laissez pas votre entreprise alimenter les statistiques de la criminalité informatique ! Il est largement temps de consolider les défenses nécessaires en mettant en œuvre des contrôles adaptés, *via* une politique de sécurité et des procédures bien conçues.

- Les codes de comptabilité des services, de même que les copies du répertoire de l'entreprise (qu'il s'agisse de supports papier, de fichiers de données ou de répertoires téléphoniques électroniques sur l'intranet) sont des cibles courantes pour les manipulateurs. Concernant la divulgation de ce type d'informations, il faut que chaque entreprise ait un règlement écrit et qu'elle le diffuse largement. Il faut notamment garantir l'existence d'un document qui enregistre les cas où une information sensible a été dévoilée à une personne étrangère à l'entreprise.
- En lui-même, un renseignement tel que le numéro d'un employé ne devrait pas pouvoir servir à une authentification, quelle qu'elle soit. Chaque employé doit être formé afin de vérifier non seulement l'identité de la personne qui demande des informations, mais également pourquoi elle a besoin de ces informations.
- Dans tout programme de formation à la sécurité, les employés doivent apprendre à respecter la marche à suivre. À chaque demande de renseignement émanant d'un étranger, il faut d'abord refuser

poliment de répondre, jusqu'à ce que la requête puisse être vérifiée. Ensuite, et avant de satisfaire cette requête, il faut suivre le règlement et les procédures de l'entreprise relatives à la vérification et à la divulgation des informations non publiques. Cette façon de procéder peut aller à l'encontre de notre inclination naturelle à aider les autres, mais un brin de paranoïa peut se révéler nécessaire pour vous éviter d'être la prochaine dupe d'un manipulateur.

Comme nous l'avons vu par le biais des histoires de ce chapitre, une information apparemment anodine peut servir de clé pour accéder aux secrets les plus prisés de votre entreprise.

Chapitre 3

L'attaque directe : il suffit de demander

Les attaques par manipulation sont parfois très compliquées, impliquant l'élaboration d'un plan en plusieurs étapes, combinant manipulation et savoir-faire technique.

Mais je suis toujours frappé par le fait qu'un manipulateur expérimenté arrive souvent à atteindre son but grâce à une simple attaque directe. Comme vous allez le constater, il suffit parfois de demander directement un renseignement…

OBTENIR UN NUMÉRO QUI EST SUR LISTE ROUGE

Vous voulez connaître le numéro de téléphone d'une personne sur liste rouge ? Un manipulateur est capable de vous indiquer une demi-douzaine de méthodes pour y parvenir (et vous en trouverez quelques-unes dans certaines des histoires présentées au fil de ces pages), mais le scénario le plus simple est probablement celui dans lequel un seul appel téléphonique suffit, comme nous allons le voir ci-après.

Le numéro, s'il vous plaît

Un attaquant compose le numéro de la compagnie de téléphone privée du MLAC (*Mechanized Line Assignment Center*, centre d'affectation de lignes automatiques). Voici ce qu'il dit à la femme qui décroche :

"Bonjour, Paul Anthony à l'appareil. Je raccorde les câbles. Voilà, ici, un terminal a grillé dans un incendie. La police pense qu'un saligaud a essayé d'incendier sa propre maison pour toucher l'assurance. Je suis ici tout seul pour essayer de raccorder ce terminal de deux cents paires de fils. J'aurais vraiment besoin d'aide. Vous pouvez me dire quels établissements travaillent au 6723 South Main ?"

Dans d'autres services de la compagnie de téléphone, tout employé qui répond saurait que les informations concernant des numéros non publiés ne sont censées être données qu'au personnel de l'entreprise qui en a reçu l'autorisation. Mais *a priori*, seuls les employés connaissent le MLAC. Et tant qu'ils ne donnent jamais de renseignements au public, qui refuserait un peu d'aide à un membre de l'entreprise qui se retrouve tout seul pour régler un problème ? L'employée se sent désolée pour lui, elle-même a connu de mauvaises journées de travail ; elle ferait bien quelque chose pour aider un collègue embarrassé. Elle lui indique donc le câble, les paires et chaque numéro opérationnel affecté à l'adresse.

Analyse de l'arnaque

Comme vous le remarquerez souvent dans les histoires d'arnaques, la connaissance du jargon d'une entreprise et de sa structure professionnelle — ses divers bureaux et services, ce que chacun y fait et les informations que chacun possède — fait partie de l'arsenal d'astuces indispensables au succès du manipulateur.

Le message de Mitnick

Il est dans la nature humaine de croire nos semblables, en particulier lorsqu'ils formulent des demandes qui paraissent raisonnables. Les manipulateurs utilisent ce point faible pour exploiter leurs victimes et atteindre leurs buts.

LE JEUNE HOMME EN FUITE

Un homme que nous appellerons Frank Parsons, recherché par le gouvernement fédéral pour avoir fait partie d'un groupe de pacifistes clandestin dans les années soixante, était en fuite depuis des années. Dans les restaurants, il s'asseyait toujours face à la porte et regardait de temps en temps par-dessus son épaule, d'une façon qui pouvait paraître déconcertante. Il déménageait régulièrement après quelques années.

Un jour, Frank débarque dans une ville qu'il ne connaît pas et se met à chercher du travail. Pour quelqu'un de son niveau, extrêmement compétent en informatique (et en manipulation, même s'il ne le mentionne généralement pas dans son curriculum vitæ), trouver un bon poste n'est généralement pas un problème. Excepté pendant les périodes de difficultés économiques, les personnes qui possèdent un bon bagage informatique sont très recherchées. Frank trouve donc rapidement un poste bien rémunéré, avec des responsabilités, dans une grosse entreprise près de chez lui.

"Le gros lot", pense-t-il. Mais lorsqu'il remplit son formulaire d'embauche, il tombe sur un os : l'employeur demande au candidat de fournir une copie de son casier judiciaire, qu'il doit se procurer lui-même auprès de la police d'État. La pile des papiers d'embauche comprend d'ailleurs un formulaire demandant ce document, ainsi qu'une petite case destinée à recevoir l'empreinte digitale du candidat. Même si on lui demandait seulement l'empreinte de son index droit, il suffirait de la comparer à celle de la base de données du FBI pour qu' il se retrouve rapidement dans un établissement pénitentiaire.

Néanmoins, il apparaît à Frank qu'il pourrait peut-être — peut-être seulement — s'en tirer une nouvelle fois. Peut-être ces empreintes digitales se sont-elles pas réellement envoyées au FBI ? Comment le savoir ?

Frank est un manipulateur : comment *pensez-vous* qu'il le saura ? Il appelle la patrouille d'État : "Bonjour. Nous réalisons une étude pour l'antenne locale du ministère de la Justice. Nous collectons des informations pour mettre en place un nouveau système d'identification d'empreintes digitales. Puis-je parler à une personne connaissant bien ce que vous faites, et qui pourrait peut-être nous aider ?"

Quand l'expert local prend le téléphone, Frank lui pose une série de questions sur les systèmes qu'ils utilisent, ainsi que sur les possibilités de recherches et de stockage des données d'empreintes digitales. Ont-ils des problèmes d'équipement ? Sont-ils reliés au service de recherches d'empreintes digitales du centre national de renseignements sur les criminels (le NCIC, *National Crime Information Center*) ou seulement à celui de cet État ? Est-il facile pour tout le monde d'apprendre à utiliser l'équipement

Frank a habilement noyé la question clé parmi les autres.

La réponse sonne comme une douce musique à ses oreilles : non, ils ne sont pas reliés au NCIC.

Le message de Mitnick

> Les escrocs du renseignement n'éprouvent aucune crainte à téléphoner aux forces de l'ordre ou aux pouvoirs publics pour obtenir des informations sur les procédures d'application des lois. Avec de tels éléments en main, les manipulateurs sont capables de contourner tous les contrôles de sécurité standard de votre entreprise.

C'est tout ce dont Frank avait besoin. Comme il n'est pas fiché dans cet État, il envoie sa demande et est embauché. Il n'a jamais vu personne entrer dans son bureau pour lui dire : "Ces messieurs sont du FBI et voudraient avoir une petite conversation avec vous".

SUR LE PAS DE LA PORTE

Le bureau sans papier est un mythe : les entreprises continuent d'imprimer des pages et des pages de papier tous les jours. Or les informations imprimées dans votre entreprise peuvent se révéler vulnérables, même lorsque vous prenez des précautions et les classez comme étant confidentielles.

Voici une histoire qui illustre la façon dont peuvent procéder les manipulateurs pour obtenir vos documents les plus secrets.

Supercherie du bouclage

Chaque année, l'opérateur téléphonique dont nous allons parler ici publie un volume intitulé "Répertoire des numéros de tests" — ou du moins il le faisait, mais comme je suis toujours en liberté surveillée, je ne vais pas me risquer à le lui demander. Ce document est très prisé des pirates car il indique tous les numéros de téléphone étroitement surveillés qui sont utilisés par les ouvriers qualifiés de l'entreprise, techniciens ou autres, pour contrôler, par exemple, les numéros qui sonnent toujours occupé.

L'un de ces numéros de tests, que l'on appelle "bouclage" (*loop-around*) dans le jargon, est particulièrement utile. Ainsi, les pirates s'en servent pour trouver d'autres pirates avec qui bavarder gratuitement. Ils l'utilisent également comme numéros de rappel qu'ils fournissent, par exemple, aux banques. Un manipulateur peut indiquer à un employé de banque que ce numéro de téléphone est celui où il est joignable au bureau. Lorsque la banque rappelle le numéro de test, le pirate est en mesure de recevoir l'appel, mais il est protégé puisqu'il a indiqué un numéro de téléphone à partir duquel il est impossible de remonter jusqu'à lui.

Ce type de répertoire fournit de nombreuses informations précises exploitables par n'importe quel pirate en quête de renseignements. Ainsi, de nombreux gamins dont le violon d'Ingres est d'explorer le réseau téléphonique convoitent les nouveaux répertoires édités chaque année.

Le message de Mitnick

> Il faut toujours dispenser une formation aux règles de la sécurité à tous les employés de l'entreprise, et cette formation doit être conforme au règlement de l'entreprise.

L'arnaque de Stevie

Naturellement, comme les opérateurs téléphoniques ne fournissent pas facilement ces informations, les pirates doivent se montrer inventifs pour se les procurer. Comment font-ils ? Une personne déterminée monterait un scénario tel que celui que je présente ci-après.

C'est l'automne, en Californie du sud. Tard un soir, un type que j'appellerai Stevie téléphone au bureau central d'une petite compagnie de téléphone, bâtiment d'où partent toutes les lignes de sa zone.

Lorsque le standardiste de service répond, Stevie annonce qu'il appartient à la division de l'entreprise téléphonique qui édite et distribue les travaux imprimés. "Nous avons votre nouveau répertoire de numéros de tests" dit-il. "Mais pour des raisons de sécurité, nous ne pouvons pas vous l'envoyer tant que nous n'avons pas récupéré l'ancien. Et le gars qui les livre est en retard. Si vous voulez bien laisser le vôtre à votre porte, il peut faire un détour, le prendre, laisser le nouveau et continuer."

Le standardiste ne se doute de rien et trouve cela sensé. Il fait exactement comme indiqué. Sur le pas de porte de l'immeuble, il place son exemplaire du répertoire, dont la couverture avertit clairement, en lettres rouges : "**CONFIDENTIEL ENTREPRISE** — APRÈS USAGE, CE DOCUMENT DOIT ÊTRE DÉTRUIT".

Stevie arrive en voiture et scrute attentivement les alentours, afin de s'assurer que des policiers ou des employés de l'entreprise ne se sont pas en train de l'observer, cachés derrière des arbres ou dans des voitures. Personne en vue. Il prend négligemment le répertoire et s'en va.

Ce nouvel exemple montre avec quelle facilité un manipulateur peut se procurer ce qu'il veut en appliquant le principe élémentaire de la "simple demande".

ATTAQUE À LA DEMANDE

Dans un scénario de manipulation, les biens d'une entreprise sont exposés, mais c'est parfois également le cas des clients.

Travailler dans un service clients apporte son lot de frustrations et de rires, mais aussi son lot d'erreurs involontaires, dont certaines peuvent avoir des conséquences malheureuses pour les clients.

L'histoire selon Janie Acton

Depuis plus de trois ans, Janie Acton s'occupe d'un standard en tant que représentante d'un service clients pour Hometown Electric Power, à Washington. Elle est considérée comme l'une des meilleures employées, intelligente et consciencieuse.

C'est Thanksgiving lorsque Janie reçoit cet appel. Voici ce que lui dit son interlocuteur :

"Ici Eduardo, du service facturation. J'ai une dame en attente, une secrétaire de l'un des vice-présidents de l'entreprise, et qui me demande des informations, mais je ne peux pas utiliser mon ordinateur. J'ai reçu un e-mail d'une fille des ressources humaines dont le sujet était "ILOVEYOU", et lorsque j'ai ouvert le fichier joint, je n'ai plus été capable d'utiliser ma machine. Un virus. Je me suis fait avoir par un stupide virus. Pourriez-vous rechercher quelques informations sur des clients pour moi ?"

"Bien sûr" répond Janie. "Il a planté votre ordinateur ? C'est terrible."

"Ouais."

"Que puis-je faire pour vous ?" demande Janie.

Pour être crédible, l'attaquant demande alors des renseignements en se fondant sur ses recherches antérieures. Il a appris que les informations qu'il cherche sont stockées dans ce que l'on appelle le système d'information de facturation clients et il a trouvé comment les employés s'y référaient. "Pouvez-vous appeler un compte sur le système d'information de facturation clients ?", demande-t-il.

"Oui, quel est le numéro du compte ?"

"Je ne l'ai pas ; il faut que vous me donniez son nom."

"Très bien, quel est le nom ?"

"Heather Marning." Il épelle le nom et Janie le tape.

"OK. Je l'ai."

"Parfait. Est-ce un compte courant ?"

"C'est bien un compte courant."

"Quel est son numéro ?" demande-t-il.

"Vous avez un crayon ?"

"Je suis prêt."

"Compte numéro BAZ6573NR27Q."

Il relit le numéro puis demande l'adresse du service, qu'elle lui donne.

"Et le téléphone ?"

Janie lui lit également cette information.

Le manipulateur la remercie, prend congé et raccroche. Janie passe à l'appel suivant, sans plus jamais penser à cette conversation.

Le projet de recherche d'Art Sealy

Art Sealy avait cessé de travailler comme éditeur freelance pour de petites maisons d'édition lorsqu'il s'est rendu compte qu'il pourrait gagner plus d'argent en faisant des recherches pour des auteurs et des entreprises. Il a vite découvert que les honoraires qu'il pouvait demander étaient proportionnels à son éloignement de la frontière parfois imprécise entre le légal et l'illégal. Sans jamais en prendre conscience, et certainement sans jamais l'avoir verbalisé, Art est devenu un manipulateur ; il utilisait des techniques qui étaient familières à tout professionnel du renseignement. Il s'est avéré qu'il possédait un talent naturel pour cela, car il trouvait de lui-même des techniques que la plupart des manipulateurs devaient apprendre auprès de tiers. Peu de temps après, il franchissait le pas sans le moindre sentiment de culpabilité.

"Un homme me contacte, indiquant qu'il écrit un livre sur les années Nixon et qu'il recherche un informateur susceptible de lui fournir un scoop de source sûre sur William E. Simon, qui a été ministre des Finances sous Nixon. M. Simon est décédé, mais l'auteur connaît le nom d'une femme qui a fait partie de son équipe. Il est presque certain qu'elle vit toujours à Washington, mais il n'a pas réussi à se procurer son adresse. Elle ne possède

pas de ligne de téléphone à son nom, ou alors sur liste rouge. Voilà la situation lorsqu'il m'appelle. Je lui dis, bien sûr, qu'il n'y a aucun problème pour que je l'aide."

C'est le genre de job que vous pouvez réussir en un coup de téléphone ou deux... si vous savez ce que vous faites. On peut généralement compter sur n'importe quelle entreprise de services locale pour révéler ce type d'information.

J'aime suivre une approche différente à chaque fois, juste pour que les choses restent intéressantes. Mais "Ici Monsieur Untel, de la direction" a toujours bien marché pour moi. Cette fois-ci, "J'ai quelqu'un en ligne, du bureau du vice-président", a aussi fonctionné.

Le message de Mitnick

> Ne croyez jamais que toutes les attaques de manipulation sont forcément des ruses élaborées et complexes au point qu'on puisse les détecter avant qu'elles soient menées à leur terme. Certaines attaques consistent simplement, pour les manipulateurs, à entrer et sortir, à frapper et disparaître, etc. : des cas dans lesquels les manipulateurs se limitent à formuler une demande.

Vous devez développer votre instinct de manipulateur et évaluer le niveau de coopération que la personne que vous avez au bout du fil est prête à vous accorder. Cette fois, j'ai eu de la chance avec une dame bienveillante et serviable. En un seul appel, j'ai obtenu l'adresse et le numéro de téléphone. Mission accomplie.

Analyse de l'arnaque

Janie savait certainement que les informations concernant les clients étaient sensibles. Jamais elle n'aurait discuté d'un compte d'un client avec un autre client, ni donné d'informations privées au public.

Mais naturellement, dans le cas d'un appel en interne, des règles différentes s'appliquent. Avec les collègues, il s'agit de s'entraider. L'employé du service de facturation aurait pu rechercher les données lui-même si son ordinateur n'était pas tombé en panne à cause d'un virus, et Janie était contente d'avoir pu aider un collègue.

Art a reconstitué graduellement l'information clé qu'il recherchait, en demandant en cours de route des renseignements qui ne l'intéressaient pas vraiment, comme le numéro de compte. Cela dit, en ayant le numéro de compte, il disposait d'une solution de secours : si l'employé s'était méfié, Art aurait rappelé et aurait eu de meilleures chances de réussite, car le fait de connaître le numéro de compte l'aurait rendu encore plus crédible auprès d'un autre employé.

Janie n'aurait jamais pensé qu'on puisse lui mentir à ce point, qu'un soi-disant employé ne fasse pas du tout partie du service facturation. Naturellement, la faute n'est pas imputable à Janie. Elle n'a pas été correctement formée au principe qui veut que l'on s'assure de savoir à qui l'on parle avant de révéler des informations sur un fichier de clients. Personne ne l'avait prévenue du danger d'un appel téléphonique comme celui d'Art. Ce n'était pas dans le règlement de l'entreprise, cela n'a pas fait partie de sa formation, et son chef de service ne le lui avait jamais signalé.

EMPÊCHER L'ARNAQUE

Élément à inclure dans votre formation à la sécurité : le simple fait qu'un appelant ou un visiteur connaisse le nom de certaines personnes de l'entreprise, un peu de jargon ou des procédures ne signifie pas qu'il est celui qu'il prétend être. Et cela ne le désigne absolument pas comme une personne autorisée à recevoir des informations internes, ou à accéder à votre réseau informatique.

Les formations à la sécurité doivent mettre l'accent sur ce type de cas : en cas de doute, vérifiez !

Dans le temps, le fait de pouvoir accéder à des informations internes à l'entreprise était une marque de rang et de privilège. Les employés chargeaient les fourneaux, faisaient fonctionner les machines, tapaient les lettres et classaient les rapports. Le contremaître ou le patron leur disaient que faire, quand et comment. C'était le contremaître ou le patron qui savait combien d'éléments chaque ouvrier devait produire dans un roulement, qui connaissait les couleurs, les tailles et le nombre d'éléments que l'usine devait produire pour la semaine en cours, la semaine suivante, et ainsi de suite jusqu'à la fin du mois.

Les ouvriers manœuvraient les machines, les outils et les matériaux, et les patrons géraient les informations. Les ouvriers n'avaient besoin que de renseignements spécifiques à leurs travaux.

Le tableau est un peu différent de nos jours, n'est-ce pas ? De nombreux ouvriers en usine utilisent un ordinateur ou une machine pilotée par ordinateur. Dans notre environnement actuel, presque tout ce que font les employés implique le traitement d'informations.

C'est pourquoi il est nécessaire de diffuser un règlement sur la sécurité à l'échelle de l'entreprise, quel que soit le niveau hiérarchique. Chacun doit comprendre que les patrons et les contremaîtres ne sont pas les seuls à détenir des informations susceptibles d'intéresser un attaquant. Aujourd'hui, les ouvriers, à tous les niveaux, même ceux qui n'utilisent pas d'ordinateur, peuvent être visés. Le maillon faible qu'un manipulateur exploitera pour atteindre son objectif peut tout simplement être un représentant nouvellement embauché dans le groupe du service clients.

Chapitre 4

Instaurer la confiance

Certaines des histoires de cet ouvrage pourraient vous faire penser que je prends tous les gens du métier pour de sombres idiots, prêts, voire disposés, à divulguer tous les secrets en leur possession. Le manipulateur sait que cela n'est pas vrai. Pourquoi les attaques par manipulation réussissent-elles si bien ? Non pas parce que les gens sont stupides ou manquent de bon sens mais parce qu'en tant qu'êtres humains, nous sommes tous vulnérables ; et certaines techniques de manipulation peuvent nous amener à accorder notre confiance à la mauvaise personne.

Le manipulateur anticipe la suspicion et la résistance, et il est toujours prêt à transformer la méfiance en confiance. Un bon manipulateur imagine son attaque comme une partie d'échecs, en prévoyant les questions que sa cible est susceptible de lui poser, afin de préparer les bonnes réponses.

L'une des techniques couramment employées repose sur l'instauration d'un climat de confiance chez la victime. Comment un arnaqueur peut-il nous amener à lui faire confiance ? Faites-moi confiance, il sait comment faire !

LA CONFIANCE : LA CLÉ DE L'ARNAQUE

Plus un manipulateur peut faire passer ce qu'il fait comme une démarche professionnelle ordinaire, plus il endort les soupçons. Lorsque les gens n'ont aucune raison de se méfier, il est facile pour un manipulateur de gagner leur confiance.

Note

Vous aurez remarqué que dans la plupart des histoires que je présente, je me réfère à tout manipulateur, pirate téléphonique ou arnaqueur en employant le pronom personnel "il". Il ne s'agit pas de sexisme : en réalité, la plupart des experts dans ce domaine sont des hommes. Cependant, bien que le nombre de manipulatrices soit peu élevé, il est en augmentation. Il y a en tout cas assez de manipulatrices pour qu'on ne baisse pas notre garde lorsqu'on entend une femme à l'autre bout du fil. En fait, les manipulatrices possèdent un net avantage : elles peuvent jouer de leurs charmes pour nous faire coopérer. Je présente donc dans cet ouvrage un petit nombre d'histoires qui mettent en scène des représentantes de ce que l'on appelle le "sexe faible".

Premier appel : Andrea Lopez

Andrea Lopez répond au téléphone du magasin de location de vidéos où elle travaille et, d'emblée, se met à sourire : c'est toujours agréable lorsqu'un client prend la peine de dire qu'il est satisfait du service fourni. Le client en question annonce qu'il a eu d'excellents rapports avec ce magasin, et il souhaite en informer le directeur par écrit.

Il demande donc le nom et l'adresse postale du directeur ; Andrea lui dit qu'il s'agit de Tommy Allison et communique son adresse au client. Alors qu'il est le point de raccrocher, une nouvelle idée lui vient : "Je voudrais également écrire au siège de votre société. Quel est le numéro de votre magasin ?" Elle lui donne également cette information. Il la remercie, ajoute un mot agréable pour lui dire combien son aide lui a été utile et prend congé.

"Avec des appels comme celui-là, pense-t-elle, la journée paraît toujours passer plus vite. Ce serait vraiment bien si les gens faisaient ça plus souvent."

Second appel : Ginny

"Studio Vidéo, bonjour. Ginny à l'appareil, que puis-je faire pour vous ?"

"Bonjour, Ginny" répond son interlocuteur avec enthousiasme, donnant l'impression qu'il a souvent affaire à elle. Je suis Tommy Allison, directeur du magasin 863. Nous avons un client qui veut louer *Rocky V* et nous sommes en rupture de stock. Pouvez-vous vérifier si vous avez des copies ?"

Elle reprend la ligne au bout d'un moment et dit : "Oui, nous en avons trois".

"Très bien, je vais voir si le client veut bien se rendre chez vous. Merci beaucoup ! Et si notre magasin peut vous rendre un quelconque service, n'hésitez pas à appeler et demandez Tommy. Je serai content de faire mon possible pour vous aider."

Au cours des deux semaines suivantes, Ginny reçoit trois ou quatre appels de Tommy pour un service ou un autre. Il s'agit toujours de demandes légitimes et il paraît toujours très sympathique. En outre, Tommy ne donne pas l'impression de s'intéresser à elle. Il est également un peu plus bavard chaque fois : "Vous êtes au courant pour le grand incendie de Oak Park ? On a plein de routes coupées, par ici", etc. Ces appels font une petite coupure dans la routine quotidienne, et Ginny est toujours contente de l'entendre.

Un jour Tommy appelle, apparemment stressé : "Est-ce que vous avez eu des ennuis avec vos ordinateurs ?"

"Non" répond Ginny. "Pourquoi ?"

"Un type est entré dans un poteau téléphonique avec sa voiture et le réparateur de la compagnie des téléphones dit qu'une partie entière de la ville va perdre ses liaisons téléphoniques et ses connexions Internet jusqu'à ce qu'ils aient tout réparé."

"Oh, non ! L'homme est-il blessé ?"

"On l'a emmené en ambulance. En tout cas, j'ai besoin d'un petit service. J'ai ici l'un de vos clients qui veut *Le Parrain II* et il n'a pas sa carte avec lui. Pourriez-vous vérifier pour moi les informations à son sujet ?"

"Bien sûr."

Tommy donne le nom et l'adresse du client. Ginny le trouve sur l'ordinateur et indique le numéro de compte à Tommy.

"Aucun retard ni reliquat ?" demande Tommy.

"Non, apparemment il n'y a rien."

"OK. Je vais enregistrer l'opération manuellement et je la rentrerai dans notre base de données plus tard, quand les ordinateurs fonctionneront de nouveau. Il veut payer avec sa carte Visa, mais il ne l'a pas avec lui. Quels sont le numéro et la date d'expiration de la carte ?"

Ginny les lui donne et Tommy prend congé : "Merci pour votre aide. À bientôt au téléphone !" puis il raccroche.

L'histoire de Doyle Lonnegan

Lonnegan n'est pas un jeune homme que vous aimeriez voir sonner chez vous. Autrefois spécialisé dans le recouvrement de dettes de jeu, il est encore prêt à rendre service s'il ne doit pas pour autant trop s'exposer. Dans le cas

présent, il s'est vu offrir un assez belle somme en liquide pour passer quelques coups de téléphone à un magasin de vidéos. Cela paraît pourtant assez simple, mais aucun de ses "clients" ne savait comment s'y prendre pour mener cette arnaque ; ils avaient besoin du talent et du savoir-faire de Lonnegan. Voici son histoire .

Les joueurs ne font pas de chèques pour tenir leurs paris quand ils sont malchanceux ou pèchent par bêtise à la table de poker. Tout le monde sait cela. Alors pourquoi mes amis ont-ils continué à jouer avec un tricheur sans pognon sur la table ? Allez savoir... Peut-être sont-ils un peu faibles au niveau du QI, mais ce sont mes amis !

Le type n'avait pas de liquide, alors ils ont accepté un chèque. Je vous demande un peu ! L'accompagner à un distributeur automatique, voilà ce qu'ils auraient dû faire. Mais non, ils prennent un chèque de 3 230 dollars.

Naturellement, il a été refusé. Il fallait s'y attendre. Alors ils m'appellent : est-ce que je pourrais les aider ? Je n'ai plus pour habitude de menacer physiquement les gens. Du reste, il existe de meilleurs moyens, de nos jours. Je leurs dis donc que je prends 30 % de commission et que je vais voir ce que je peux faire. Ils me donnent son nom et son adresse, et je saute sur l'ordinateur pour voir quel est le magasin vidéo le plus proche de chez lui.

Je n'étais pas très pressé. Quatre appels téléphoniques pour me mettre dans les petits papiers de la responsable du magasin, et bingo, j'obtenais le numéro de la carte Visa du tricheur.

Un autre de mes amis tient un bar où les serveuses ont les seins nus. Pour cinquante dollars, il a accepté de faire passer comme une dépense au bar, *via* la carte Visa, la somme d'argent que le type du poker devait. Vous voyez le tricheur expliquer ça à sa femme ? Vous pensez qu'il peut essayer de convaincre Visa que ce n'est pas lui qui a fait cette dépense ? En plus, il sait que nous savons qui il est. Et si nous avons pu obtenir son numéro Visa, il va s'imaginer que nous pourrons obtenir plus encore. Pas de doute là-dessus.

Analyse de l'arnaque

Les premiers appels de Tommy étaient simplement destinés à instaurer la confiance. Lorsque l'heure de la véritable attaque est venue, Ginny a baissé sa garde et considéré Tommy comme ce qu'il prétendait être, à savoir le directeur d'un autre magasin de la chaîne.

Et pourquoi *ne l'aurait*-elle *pas* vu comme tel ? Elle le connaissait déjà. Elle ne le connaissait qu'au téléphone, bien sûr, mais ils avaient établi une amitié professionnelle, fondée sur la confiance. Dès lors qu'elle l'avait accepté comme une personne ayant autorité, un autre responsable de la même entreprise, la confiance avait été établie et le reste n'avait plus été qu'un jeu d'enfants.

Le message de Mitnick

La technique d'arnaque qui repose sur la mise en confiance est l'une des tactiques les plus efficaces des manipulateurs. Il faut toujours se demander si l'on connaît vraiment la personne à qui l'on parle. Dans de rares cas, elle peut ne pas être celle qu'elle prétend. En conséquence, nous devons tous apprendre à observer, à réfléchir et à nous poser des questions sur la légitimité de la personne en question.

VARIATION SUR UN THÈME : VOL DE CARTE

L'instauration d'un sentiment de confiance n'implique pas qu'il faille à chaque fois passer une série d'appels téléphoniques à la victime, comme dans l'histoire précédente. Je me souviens d'un incident dont j'ai été témoin, où cinq minutes ont suffi.

Surprise, papa !

Je suis assis à une table de restaurant avec Henry et son père. Dans la conversation, Henry reproche à son père de donner son numéro de carte de crédit comme s'il s'agissait de son numéro de téléphone. "C'est vrai que tu dois le fournir quand tu achètes quelque chose" dit-il. "Mais le donner à un magasin qui classe ton numéro dans ses dossiers, c'est de la bêtise pure !"

"Le seul endroit où je l'ai fait, c'est chez Studio Vidéo", dit M. Conklin, désignant la chaîne de magasins vidéo. "Mais j'examine mon relevé de carte Visa tous les mois. S'ils prélevaient des sommes indues, je le saurais."

"OK" dit Henry, "mais une fois qu'ils ont ton numéro, il est très facile que quelqu'un le vole !"

"Tu veux dire un employé malhonnête ?"

"Non, *n'importe qui*, et pas seulement un employé."

"Tu parles à tort et à travers", dit M. Conklin.

"Je peux appeler immédiatement et faire en sorte qu'ils me donnent le numéro de ta Visa" lui assure Henry.

"Non, tu ne *peux pas*", rétorque son père.

"Je peux le faire en cinq minutes, ici, devant vous, sans même quitter la table."

M. Conklin paraissait sûr de lui, bien qu'il ne voulait pas le montrer. "Je dis que tu ne sais pas de quoi tu parles" aboie-t-il, en sortant son portefeuille et en flanquant un billet de cinquante dollars sur la table. "Si tu peux faire ce que tu prétends, c'est à toi."

"Je ne veux pas de ton argent, papa" dit Henry.

Il sort son téléphone portable et demande à son père dans quel magasin vidéo il est client. Il appelle le service des renseignements pour connaître le numéro de téléphone de ce magasin et celui du magasin vidéo le plus proche de Sherman Oaks.

Puis il appelle le magasin de Sherman Oaks. En suivant pratiquement la même méthode que celle décrite dans l'histoire précédente, il obtient rapidement le nom du directeur et le numéro du magasin.

Il appelle ensuite le magasin où son père possède un compte. Il applique la vieille ruse qui consiste à se faire passer pour un directeur, en utilisant le nom du directeur et le numéro du magasin qu'il vient d'obtenir. Puis il exploite la même méthode que celle que nous avons vue précédemment : "Vos ordinateurs fonctionnent-ils bien aujourd'hui ? Les nôtres, non". Il écoute la réponse et annonce : "Bien, j'ai un de vos clients, ici, qui veut louer une vidéo, mais nos ordinateurs sont en panne. J'ai besoin que vous recherchiez le compte de ce client et que vous vous assuriez que c'est un client de votre magasin."

Henry lui donne le nom de son père et lui demande alors de lui lire toutes les données concernant le compte (légère variante par rapport à la technique de Lonnegan) : adresse, numéro de téléphone et date d'ouverture du compte. Mais il se ravise et dit : "En fait, vous voyez, j'ai beaucoup de clients qui attendent. Quels sont le numéro et la date d'expiration de la carte de crédit ?"

Henry tient son mobile d'une main et, de l'autre, écrit sur une serviette en papier. Après avoir raccroché, il glisse la serviette devant son père, qui la fixe bouche bée. Le pauvre homme paraît totalement stupéfait, comme si tout son système de confiance venait de s'écrouler.

Analyse de l'arnaque

Pensez à votre propre attitude lorsqu'un inconnu vous demande quelque chose. Si un étranger miteux frappe à votre porte, vous n'allez certainement pas le laisser entrer. Mais si un étranger se présente, bien habillé, souliers cirés, coiffure parfaite, poli et souriant, vous serez probablement moins méfiant. Peut-être s'agit-il en réalité de Jason, du film *Vendredi 13*, mais vous serez enclin à faire confiance à cette personne tant qu'elle paraîtra normale et qu'elle ne brandira pas un couteau de boucher.

Cela est moins évident, mais nous jugeons les gens au téléphone de la même façon. Est-ce que cette personne semble vouloir me vendre quelque chose ? Est-elle agréable et sociable, ou est-ce que je ressens une sorte d'hostilité ou de tension ? Emploie-t-elle un vocabulaire soutenu ? Nous jugeons toutes ces choses et peut-être une dizaine d'autres inconsciemment et en un éclair, souvent dans les tout premiers instants de la conversation.

Le message de Mitnick

Il est dans la nature de l'homme de penser qu'il est peu probable qu'on le trompe dans une transaction quelconque, du moins jusqu'à ce qu'il ait une raison de croire le contraire. Nous pesons les risques et, le plus souvent, laissons aux gens le bénéfice du doute. C'est le comportement naturel des gens civilisés, en tout cas des gens civilisés qui n'ont jamais été trompés, manipulés ou "délestés" d'une grosse somme d'argent.

Enfants, nos parents nous ont appris à ne pas faire confiance aux étrangers. Peut-être devrions-nous tous tenir compte de ce vieux principe sur notre lieu de travail.

Au travail, nous sommes sollicités en permanence. Avez-vous l'adresse e-mail de M. Untel ? Où est la dernière version de la liste de clients ? Qui est le sous-traitant de cette partie du projet ? S'il vous plaît, envoyez-moi la dernière mise à jour du projet. J'ai besoin de la dernière version du code source. Etc.

Et vous savez quoi ? Parfois, ceux qui formulent ces demandes sont des gens que vous ne connaissez pas personnellement, qui travaillent pour un autre service de l'entreprise, ou le prétendent. Mais les informations qu'ils donnent tiennent debout, et ils semblent appartenir à notre "sphère" ("Marianne a dit..." ; "C'est sur le serveur K-16..." ; "...révision 26 des nouveaux plans du produit"). Nous étendons alors notre cercle de confiance pour les y inclure et leur donnons allègrement ce qu'ils demandent.

Bien sûr, nous pouvons hésiter un peu et nous demander pourquoi quelqu'un de l'usine de Dallas aurait besoin de consulter les plans du nouveau produit ou quel mal il y aurait à donner le nom du serveur sur

lequel se trouvent ces plans. Alors nous posons une ou deux autres questions à notre interlocuteur. Si ses réponses nous paraissent raisonnables et ses manières rassurantes, nous baissons notre garde, notre inclination naturelle à croire notre semblable revient au galop, et nous faisons, dans les limites du raisonnable, ce qui nous est demandé.

Et ne croyez pas un instant que l'attaquant visera uniquement les personnes qui utilisent les systèmes informatiques de l'entreprise ! Et le gars qui s'occupe du courrier ? "Pourriez-vous me rendre un petit service : glisser ceci dans la sacoche du courrier interne ?" Est-ce que l'employé de la salle du courrier sait qu'il s'agit d'une disquette contenant un petit programme spécial pour la secrétaire du P.-D.G. ? Désormais, l'attaquant reçoit sa propre copie des e-mails du P.-D.G. Eh oui ! Vous vous demandez si cela pourrait vraiment arriver dans votre entreprise ? Ma réponse est que c'est certain.

LE TÉLÉPHONE MOBILE À UN CENT

Si beaucoup de gens s'ingénient à chercher les meilleures affaires, les manipulateurs, eux, ne "cherchent" pas une meilleure affaire, ils "trouvent" le moyen d'en faire une. Par exemple, les entreprises lancent parfois des campagnes de marketing tellement alléchantes que l'on peut difficilement les ignorer : dans ce cas, les manipulateurs étudient l'offre et se demandent comment ils peuvent conclure l'affaire.

Récemment, un opérateur téléphonique d'envergure nationale faisait une importante campagne publicitaire en offrant pour un cent un téléphone flambant neuf à qui souscrirait l'un de ses abonnements.

Une grand partie des acheteurs ont découvert, mais trop tard, qu'un client prudent se devait de poser un certain nombre de questions avant de s'engager dans un abonnement de téléphonie mobile : il faut savoir si le service est analogique, numérique, ou les deux ; quel est le nombre de minutes utilisables chaque mois ; etc., etc. Il était particulièrement important de comprendre à l'avance ce que recouvrait le terme du contrat "d'engagement", à savoir le nombre de mois ou d'années d'abonnement obligatoire.

Imaginez qu'un manipulateur, qui se trouve par exemple à Philadelphie, soit attiré par un modèle de téléphone mobile bon marché proposé par une entreprise de portables, mais que l'abonnement obligatoire ne lui convienne pas. Pas de problème. Voici comment il pourrait gérer la situation.

Premier appel : Ted

Tout d'abord, le manipulateur appelle un magasin d'une chaîne d'électronique, sur West Girard.

"Electron City. Ici Ted."

"Bonjour Ted. Adam à l'appareil. Voilà, il y a quelques nuits, j'ai parlé avec un vendeur d'un téléphone mobile. Je lui ai dit que je le rappellerai quand j'aurai choisi l'abonnement, et j'ai oublié son nom. Qui est le gars qui travaille de nuit dans ce service ?"

"Il y en a plusieurs. Peut-être William ?"

"Je n'en suis pas sûr. Peut-être bien. Comment est-il ?"

"Grand. Plutôt maigre."

"Je pense que c'est lui. Quel est son nom de famille, déjà ?"

"Hadley. H-A-D-L-E-Y."

"Ouais, ça m'a l'air d'être ça. Quand va-t-il arriver ?"

"Je ne connais pas son emploi du temps, cette semaine, mais le personnel de nuit arrive vers 17 heures."

"Très bien. Alors j'essaierai ce soir. Merci, Ted."

Second appel : Katie

L'appel suivant est adressé à la même chaîne, sur North Broad Street.

"Bonjour, Electron City. Katie à l'appareil, que puis-je faire pour vous ?"

"Katie, bonjour. Ici William Hadley, du magasin de West Girard. Comment ça va aujourd'hui ?"

"Doucement, que se passe-t-il ?"

"J'ai un client qui est venu pour cette offre de téléphones mobiles à un cent. Tu vois lesquels ?"

"Oui. J'en ai vendu deux la semaine dernière."

"Il te reste des téléphones qui vont avec cet abonnement ?"

"J'en ai eu beaucoup."

"Parfait. Parce que je viens d'en vendre un à un client. Le type a fait un crédit ; nous l'avons signalé dans le contrat. J'ai vérifié ce maudit stock et il ne nous reste plus de téléphones. Je suis très embêté. Peux-tu me rendre un service ? Je vais l'envoyer à ton magasin pour qu'il prenne un téléphone. Peux-tu lui vendre le téléphone pour un cent et lui donner un reçu ? Il est convenu qu'il me rappelle quand il aura l'appareil pour que je lui indique comment l'utiliser."

"Oui, bien sûr. Envoie-le."

"Très bien. Son nom est Ted. Ted Yancy."

Lorsque le gars qui prétend s'appeler Ted Yancy se présente au magasin de North Broad Street, Katie rédige une facture et lui vend le téléphone mobile pour un cent, exactement comme le lui a demandé son "collègue". Elle a tout avalé.

Au moment de payer, comme le client n'a pas le moindre argent sur lui, la vendeuse prend un cent dans une petite boîte où il y a toujours du liquide, et elle donne la pièce à la caissière. Yancy obtient le téléphone sans même avoir payé l'unique cent qu'il devait !

Il est alors libre d'aller voir une autre entreprise de téléphones mobiles qui utilise le même modèle et de choisir l'abonnement qu'il veut : de préférence mensuel, et sans engagement obligatoire...

Analyse de l'arnaque

Il est naturel que nous ayons un haut niveau de confiance en quiconque *prétend* être un collègue, et qui connaît les procédures et le jargon de l'entreprise. Le manipulateur de cette histoire a profité de cela en se servant d'une offre promotionnelle, en se présentant comme un employé de la société, et en demandant un service à un autre magasin. Cela se produit fréquemment entre succursales de chaînes et entre services de sociétés, où les gens sont physiquement séparés et traitent avec d'autres employés qu'ils n'ont en réalité jamais rencontrés.

HACKER LES FLICS

Certaines personnes ne peuvent s'empêcher de réfléchir aux informations que leur entreprise rend accessible à tous *via* le Web. Ainsi, le producteur de mon émission hebdomadaire sur KFI Talk Radio à Los Angeles a effectué des recherches en ligne et trouvé une copie d'un manuel d'instructions pour accéder à la base de données du centre national de renseignements sur les criminels (NCIC, *National Crime Information Center*). Plus tard, il a également eu accès par ce biais au manuel du NCIC proprement dit, un document sensible qui fournit toutes les instructions permettant de récupérer des informations de la base de données nationale des criminels du FBI.

Ce manuel est un guide destiné aux organismes gouvernementaux chargés de l'application de la loi ; il fournit le formatage et les codes qui permettent de récupérer les informations sur les criminels à partir de la base de données nationale. Les organismes de tout le pays peuvent interroger cette base de données pour obtenir des informations susceptibles d'aider à résoudre des crimes dans leur propre juridiction. Le manuel contient les codes qui servent à décrire tous les éléments de la base de données, depuis les différents types de tatouages aux différentes coques de bateaux, en passant par l'argent ou les bons volés.

Quiconque a accès au manuel peut y rechercher la syntaxe et les commandes grâce auxquelles on extrait des informations de la base de données nationale. Ensuite, en suivant les instructions du guide de procédures, et avec un petit peu de sang-froid, n'importe qui peut extraire des informations de la base de données. Le manuel fournit également les numéros de téléphone à appeler pour obtenir de l'aide pour l'utilisation du système. Vous avez peut-être des manuels comparables dans votre entreprise, qui proposent des codes de produits ou des codes pour récupérer des informations sensibles ?

Le FBI n'a très probablement jamais découvert que son manuel confidentiel et ses instructions de procédures sont accessibles à tous en ligne ; et je ne pense pas qu'il serait content de l'apprendre. Une copie a été mise en ligne par un service gouvernemental de l'Oregon, l'autre par un organisme gouvernemental chargé de l'application de la loi au Texas. Pourquoi ? Dans les deux cas, il est probable qu'on a pensé que les informations étaient sans valeur et que les rendre accessibles ne prêtait pas à conséquence. Peut-être les a-t-on mises sur un intranet pour simplifier la tâche aux employés, sans penser que les informations devenaient disponibles pour quiconque — y compris le curieux, le hacker —, sur Internet, avait accès à un bon moteur de recherche tel que Google.

À l'écoute du système

Qu'il s'agisse d'utiliser de telles informations pour tromper un fonctionnaire du gouvernement ou un employé d'une entreprise, le principe est le même : comme le manipulateur arrive à accéder à des bases de données ou à des applications particulières, ou qu'il connaît les noms des serveurs informatiques d'une entreprise, par exemple, il est crédible. Et la crédibilité amène la confiance.

Dès lors qu'un manipulateur possède de tels codes, il lui est facile d'obtenir des informations. Dans cet exemple, il pourrait commencer par appeler un employé d'un bureau x de la police d'État, et l'interroger sur l'un des codes du manuel, par exemple, sur le code agression. Il pourrait dire quelque chose comme "Quand j'effectue une requête OFF dans le NCIC, j'obtiens une erreur "Système arrêté". Recevez-vous la même chose quand vous faites une requête OFF ? Pourriez-vous essayer pour moi ?" Il pourrait aussi dire qu'il

essaie de remonter jusqu'au fichier d'une personne recherchée (un WPF, *Wanted Person's File*, dans le jargon de la police).

Le préposé à l'autre bout du fil relèverait que son interlocuteur est au courant des procédures d'utilisation et des commandes utilisées pour interroger la base de données du NCIC. Qui d'autre qu'une personne formée à l'utilisation du NCIC pourrait connaître ces procédures ?

Après que l'employé a confirmé que son système fonctionne bien, la conversation pourrait s'engager ainsi :

"J'aurais besoin d'un peu d'aide."

"Qu'est-ce que vous recherchez ?"

"J'ai besoin que vous me passiez une commande OFF sur Reardon, Martin. Date de naissance 18/10/66."

"Quel est son numéro de sécurité sociale ?"

"700-14-7435."

Après avoir parcouru la liste, l'employé pourrait dire, par exemple, "Il a obtenu un 2 602."

Il ne resterait plus à l'attaquant qu'à jeter un coup d'œil au NCIC en ligne pour trouver la signification du numéro : le casier judiciaire de l'homme contient un cas d'escroquerie.

Analyse de l'arnaque

Un manipulateur accompli ne passerait pas une minute à réfléchir aux moyens de pénétrer dans la base de données du NCIC. En effet, pour obtenir les informations qu'il veut, il lui suffit de passer un simple appel au service de la police locale et de discuter aimablement de façon à paraître de la maison. La fois d'après, il appellera simplement un autre bureau de la police en se servant du même prétexte.

Vous vous demandez peut-être s'il n'est pas risqué d'appeler un service de police, le bureau d'un shérif, ou le bureau d'une patrouille d'autoroute. L'attaquant ne court-il pas un grand risque ?

La réponse est non... Et pour une raison bien particulière : tout comme les militaires, les employés chargés de l'application des lois ont, profondément enraciné en eux, et ce depuis le premier jour, le sens de la hiérarchie. Tant que le manipulateur se pose en tant que sergent ou lieutenant — c'est-à-dire qu'il prend un grade plus élevé que celui de son interlocuteur —, le système fonctionne bien car la victime a bien appris que l'on ne pose pas de question à un supérieur. Autrement dit, le grade confère des privilèges, et notamment celui de ne pas être remis en cause par les personnes de grade inférieur.

Mais il ne faut pas penser pour autant que les domaines précités soient les seuls où ce respect de la hiérarchie puisse être exploité par le manipulateur. Comme le montrent certaines histoires présentées dans cet ouvrage, les manipulateurs utilisent souvent l'autorité ou la hiérarchie comme arme dans leurs attaques d'entreprises.

EMPÊCHER L'ARNAQUE

Quelles initiatives peut prendre votre entreprise pour réduire le risque que des manipulateurs profitent de la propension naturelle de vos employés à faire confiance aux gens ? Voici quelques conseils.

Protéger vos clients

À l'ère de l'électronique qui est la nôtre, de nombreuses entreprises commerciales conservent les numéros de cartes de crédit de leurs clients dans un fichier. Néanmoins, cette pratique devrait être déconseillée.

Si vous devez conserver des numéros de cartes de crédit dans un fichier, les procédures concernées doivent être accompagnées de précautions de sécurité encore plus importantes que le cryptage ou le contrôle d'accès. Il faut former les employés de sorte qu'ils reconnaissent les arnaques des manipulateurs comme celles que nous avons décrites dans ce chapitre. Ce collègue que vous n'avez jamais rencontré en personne mais qui est devenu un ami au fil des appels téléphoniques peut fort bien ne pas être celui qu'il prétend. Il peut ne pas avoir le "besoin de savoir" pour accéder aux informations sensibles d'un client. Il se peut que son "besoin de connaître" certaines informations sensibles concernant un client ne soit pas légitime, car il peut très bien ne pas travailler pour l'entreprise.

Le message de Mitnick

Chacun devrait être averti du *modus operandi* du manipulateur : il rassemble le plus d'informations possible sur la cible et les utilise pour inspirer confiance au même titre qu'un initié. Puis il attaque tous azimuts.

Faire confiance, mais de façon avisée

Les gens qui ont accès à des informations manifestement sensibles — les ingénieurs logiciel, le personnel de la recherche et du développement (R&D), etc. — ne sont pas les seuls à devoir être sur la défensive vis-à-vis des intrusions. Si vous voulez protéger votre entreprise contre les espions industriels et les voleurs d'informations, pratiquement chaque employé doit recevoir une formation.

En premier lieu, il faut commencer par étudier les informations à l'échelle de l'entreprise, en considérant séparément les informations qui sont sensibles, celles qui sont capitales et celles qui sont précieuses, et en s'interrogeant sur les méthodes qu'un attaquant pourrait utiliser pour s'en emparer *via* des tactiques de manipulation. Les réponses à ces interrogations doivent servir à mettre en place la formation appropriée pour les personnes qui ont un accès autorisé à ces informations.

Lorsqu'une personne que vos employés ne connaissent pas personnellement sollicite des renseignements ou un document, ou qu'elle leur demande de faire une manipulation sur leur ordinateur, ils doivent se poser des questions. Si je donne ce renseignement à mon pire ennemi, peut-il s'en servir pour me nuire, à moi ou à mon entreprise ? Est-ce que je connais tous les effets potentiels des commandes que l'on me demande d'entrer dans mon ordinateur ?

Bien sûr, nous ne voulons pas vivre en soupçonnant toute nouvelle personne que nous rencontrons. Pourtant, plus nous sommes confiants, plus il est probable que le prochain manipulateur dans les parages sera capable de nous amener à dévoiler des informations qui appartiennent à notre entreprise.

Qu'avez-vous sur votre intranet ?

Certaines parties de votre intranet peuvent être ouvertes au monde extérieur, d'autres doivent être réservées aux employés. Votre entreprise s'assure-t-elle comme il faut que les informations sensibles ne sont pas accessibles à un public dont elle voulait les écarter ? Quand, pour la dernière fois, un employé de votre entreprise a-t-il vérifié si des informations sensibles de votre intranet n'avaient pas été involontairement rendues disponibles *via* les zones d'accès public de votre site Web ?

Si votre entreprise a installé plusieurs serveurs proxy pour être protégée contre les menaces d'attaques électroniques, ces serveurs ont-ils été récemment contrôlés afin de s'assurer qu'ils sont correctement configurés ?

En fait, quelqu'un a-t-il *déjà* vérifié la sécurité de votre intranet ?

Chapitre 5

Laissez-moi vous aider

Lorsque nous sommes confrontés à un problème, nous sommes reconnaissants envers la personne qui, possédant la connaissance, la compétence et la bonne volonté nécessaires, nous tend la main. Le manipulateur comprend cela et sait en tirer parti.

Il sait également comment vous *causer* un problème, puis vous rendre reconnaissant envers lui lorsqu'il le résout… et enfin, jouer sur votre gratitude pour vous extorquer des informations ou vous demander une petite faveur qui laissera votre entreprise (ou vous-même, personnellement) dans une situation bien pire que celle qui précédait votre rencontre. Et vous ne saurez peut-être jamais que vous avez perdu quelque chose de précieux. Voici quelques méthodes typiques que les manipulateurs emploient pour "aider" leurs victimes.

LA PANNE DE RÉSEAU

Date et heure : lundi 12 février, 15 h 25.

Lieu : bureaux de Starboard Shipbuilding.

Premier appel : Tom Delay

"Tom Delay, service Comptabilité".

"Bonjour Tom, ici Eddie Martin du Service Assistance. Nous essayons de résoudre un problème de réseau informatique. Savez-vous si un membre de votre équipe a eu un problème en étant en ligne ?"

"Euh, pas à ma connaissance."

"Et vous, vous n'avez pas de problème non plus ?"

"Non, tout semble normal."

"Très bien. Voilà, nous appelons des gens susceptibles d'être touchés par le problème, car il est important que nous sachions immédiatement si vous perdez votre connexion réseau."

"Ça n'annonce rien de bon. Vous pensez que ça pourrait arriver ?"

"Nous espérons que non, mais appelez si c'est le cas. D'accord ?"

"Vous pouvez compter sur moi."

"Il semble qu'une panne de connexion réseau serait désastreuse pour vous..."

"Et *comment* !"

"... alors pendant que nous travaillons là-dessus, je vous donne mon numéro de téléphone portable. Vous pourrez me joindre directement en cas de besoin.

"C'est très gentil, allez-y."

"C'est le 00 0867 5309."

"00 0867 5309. C'est noté. Merci. Quel est votre nom, déjà ?"

"Eddie. Autre chose : j'ai besoin de vérifier le port auquel votre ordinateur est connecté. Regardez si votre machine porte quelque part une étiquette indiquant quelque chose comme 'numéro de port'."

"Un instant... non, je ne vois rien de tel."

"Très bien, alors derrière l'ordinateur, vous voyez le câble réseau ?"

"Oui."

"Remontez-le jusqu'à son branchement. Regardez s'il y a une étiquette sur sa fiche de connexion."

" Attendez une seconde, ou plutôt une minute ; il faut que je m'accroupisse pour m'approcher suffisamment et la lire. Voilà : elle indique 'Port 6-47'."

"Bien. Ce sont les données que nous avions, c'était juste pour vérifier".

Deuxième appel : le type de l'informatique

Deux jours plus tard, un appel arrive au Centre des Opérations Réseau de la même entreprise.

"Bonjour, ici Bob ; je suis dans le bureau de Tom Delay. Nous essayons de résoudre un problème de câblage. J'ai besoin que vous désactiviez le port 6-47."

Le gars de l'informatique indique que ce sera fait dans quelques minutes et qu'il le préviendra lorsqu'il pourra le reconnecter.

Troisième appel : obtenir de l'aide de l'ennemi

Une heure plus tard environ, le type qui se présente comme Eddie Martin fait ses achats à Circuit City lorsque son mobile sonne. Il voit que l'appel provient de Starboard, et se précipite dans un endroit calme avant de répondre.

"Service assistance, Eddie."

"Oh, bonjour Eddie, nous avons un écho, où êtes-vous ?"

"Je suis, euh, dans une armoire de câblage. Qui êtes-vous ?"

"Tom Delay. Je suis content de vous avoir. Vous vous souvenez m'avoir appelé l'autre jour ? Ma connexion réseau vient de tomber en panne comme vous l'aviez prévu, et je suis un peu paniqué."

"Ouais, nous avons pas mal de gens en panne en ce moment. Nous devrions nous en occuper d'ici ce soir. Ça ira ?"

"NON ! Pas du tout ! Je vais prendre du retard si je suis en panne tout ce temps. Quel est le mieux que vous puissiez faire pour moi ?"

"Quelle est votre urgence ?"

"Je pourrais faire autre chose en attendant... Une demi-heure, par exemple ?"

"UNE DEMI-HEURE ! Rien que ça ! Écoutez, je laisse tomber ce que je fais et je regarde si je peux m'attaquer à votre problème."

"J'apprécie vraiment, Eddie."

Quatrième appel : ça y est

Quarante-cinq minutes plus tard...

"Tom, ici Eddie. Allez-y, essayez votre connexion réseau."

Après quelques instants :

"Oh, très bien, ça marche : c'est formidable !"

"Bon, content d'avoir pu vous aider."

"Merci beaucoup."

"Écoutez, si vous voulez être certain que votre connexion ne tombera plus en panne, je peux vous indiquer un logiciel que vous devriez lancer. Ça prend seulement deux minutes."

"En ce moment, ce n'est pas l'idéal."

"Je comprends... Mais il pourrait nous éviter à tous les deux une grosse migraine la prochaine fois que ce problème de réseau se produira."

"Bon... si c'est seulement quelques minutes !"

"Voilà ce que vous devez faire..."

Eddie guide alors Tom pour télécharger une petite application depuis un site Web. Une fois le programme téléchargé, Eddie demande à Tom de double-cliquer dessus. Celui-ci essaie puis indique :

"Ça ne marche pas. Il ne se passe rien."

"Ah, mince, le programme doit avoir un problème. Débarrassons-nous en, nous referons un essai une autre fois." Puis il engage Tom à supprimer le programme afin que celui-ci ne puisse être récupéré.

Temps total écoulé : douze minutes.

L'histoire de Bobby Wallace

Cela amusait toujours Bobby Wallace qu'on lui confie une bonne mission comme celle-là et que le client n'aborde pas vraiment la question, non formulée mais évidente, concernant les raisons pour lesquelles il voulait ces informations. Dans le cas présent, Bobby ne pouvait penser qu'à deux raisons. Peut-être le client représentait-il une organisation intéressée par le rachat de l'entreprise ciblée, Starboard Shipbuilding, et voulait-il connaître sa véritable situation financière, notamment tout ce que la cible aurait voulu cacher à un acheteur potentiel. Ou peut-être représentait-il des investisseurs qui soupçonnaient une gestion financière douteuse et qui cherchaient à découvrir si certains dirigeants n'étaient pas mouillés.

Mais il était également possible que ce client ne veuille pas lui révéler la véritable raison, car si les informations avaient de la valeur et que Bobby l'ait su, il aurait certainement demandé plus d'argent pour faire ce travail.

Il existe de nombreuses façons de fracturer les fichiers les plus secrets d'une entreprise. Bobby a passé quelques jours à les passer en revue et à faire quelques vérifications avant de décider d'un plan. Il en a choisi un qui repose sur une approche qu'il apprécie particulièrement, lorsque la cible est dans une situation telle qu'elle demande de l'aide à l'attaquant. Pour commencer, Bobby s'est procuré un téléphone mobile à carte prépayée de 39,95 dollars auprès d'un magasin spécialisé. Prétendant appartenir au service assistance de l'entreprise, il a appelé l'homme qu'il a choisi pour cible et a fait en sorte que celui-ci lui télépone sur son portable en cas de problème avec sa connexion réseau.

Après une pause de deux jours pour ne pas se faire remarquer, il a appelé le Centre des Opérations Réseau (le COR) de l'entreprise. Il a prétendu être en train de dépanner Tom, la cible, et a demandé que la connexion de Tom soit débranchée. Bobby savait qu'il s'agissait là de la partie la plus délicate de toute la ruse : en effet, dans de nombreuses entreprises, le personnel du service assistance travaille étroitement avec le COR ; en réalité, il savait que le service assistance fait souvent partie de l'organisation informatique. Mais la personne du COR à laquelle il a parlé a considéré l'appel comme banal, n'a pas demandé le nom de la personne du service assistance qui était supposée travailler sur le problème de réseau, et a accepté de débrancher le port réseau de la cible. Cela fait, Tom était totalement isolé de l'intranet de l'entreprise, incapable de recevoir des fichiers du serveur, d'échanger des fichiers avec ses collègues, de télécharger ses e-mails ou même d'envoyer une page de données à l'imprimante. Dans le monde d'aujourd'hui, cela revenait à vivre dans une caverne.

Comme Bobby l'escomptait, il n'a pas fallu longtemps pour que son téléphone mobile sonne. Naturellement, il est venu en aide à ce pauvre collègue qui était bien embêté. Il a appelé le COR et a fait rétablir la connexion réseau. Enfin, il a appelé l'intéressé et l'a manipulé à nouveau, cette fois pour qu'il se sente coupable de lui opposer un refus, après la faveur que Bobby lui avait faite. Tom a donc accepté de télécharger un logiciel sur son ordinateur. Évidemment, la nature de son acte n'était pas exactement celle qu'il pensait. Le logiciel que Bobby lui avait préconisé, et qui était censé empêcher sa connexion réseau de tomber en panne, était en réalité un *cheval de Troie*, une application logicielle qui a fait avec l'ordinateur de Tom ce que la supercherie originale a fait avec les Troyens : introduire l'ennemi à l'intérieur du camp. Tom a indiqué que rien ne s'était passé lorsqu'il a double-cliqué sur l'icône du logiciel ; le fait est que, par conception, il ne pouvait rien voir, pas même que la petite application installait un programme secret qui permettrait à un inquisiteur d'accéder à son ordinateur.

Une fois le logiciel lancé, Bobby disposait du contrôle complet de l'ordinateur de Tom, manipulation que l'on désigne sous le terme *shell de commande à distance*. En accédant à l'ordinateur de Tom, Bobby a pu rechercher les fichiers des comptes intéressants et les recopier. Puis il les a examinés tout à loisir pour collecter les informations voulues par ses clients.

Jargon

Cheval de Troie
Programme qui contient du code malveillant ou dangereux, conçu pour endommager l'ordinateur ou les fichiers de la victime, ou pour obtenir des informations à partir de l'ordinateur ou du réseau de la victime. Certains chevaux de Troie sont conçus pour être cachés à l'intérieur du système d'exploitation de l'ordinateur et espionner chaque frappe au clavier et chaque action, ou pour recevoir des instructions à partir d'une connexion réseau et effectuer certaines fonctions, tout cela à l'insu de la victime.

Et ce n'était pas tout. Il pouvait à tout moment parcourir les e-mails et les notes de service privées des cadres de l'entreprise, ou lancer une recherche textuelle sur des mots susceptibles de révéler le moindre indice intéressant.

Jargon

Shell de commande à distance
Ce terme désigne une interface non graphique qui accepte des commandes de type texte pour effectuer certaines fonctions ou exécuter des programmes. Un attaquant qui exploite des failles techniques ou qui est capable d'installer un cheval de Troie sur l'ordinateur de sa victime peut ensuite obtenir un accès distant à un shell de commande.

Tard dans la nuit qui a suivi l'installation du cheval de Troie, Bobby a jeté le téléphone mobile dans une benne à ordures. Naturellement, il a d'abord pris soin d'effacer la mémoire et de retirer la batterie : il ne voulait surtout pas que quelqu'un appelle par erreur le numéro du mobile et que celui-ci se mette à sonner !

Analyse de l'arnaque

L'attaquant tisse une toile pour convaincre sa cible qu'elle connaît un problème qui, en fait, n'existe pas ou, comme ici, qui ne s'est pas encore produit mais qui se *produira immanquablement*, puisque c'est l'attaquant lui-même qui va le créer. Il se présente donc comme la personne capable de fournir la solution.

Ce type d'attaque est particulièrement rentable pour l'attaquant : comme la graine est semée à l'avance, lorsque la cible découvre un problème, c'est elle-même qui téléphone pour demander de l'aide. L'attaquant se contente d'attendre que le téléphone sonne, ce que l'on appelle dans le métier la *manipulation par inversion*. Un attaquant qui peut convaincre sa cible de l'appeler acquiert une crédibilité instantanée : si j'appelle une personne que je crois appartenir au service assistance, je ne lui demande pas de prouver son identité.

Jargon

Manipulation par inversion
Il s'agit d'une attaque par manipulation dans laquelle l'attaquant fait en sorte que la victime soit confrontée à un problème et soit contrainte de le contacter pour lui demander son aide. Une autre forme de manipulation par inversion retourne la situation contre l'attaquant : la cible reconnaît l'attaque et utilise des procédés psychologiques fondés sur l'influence pour tirer autant d'informations que possible de l'attaquant, afin que l'entreprise soit en mesure de protéger les actifs visés.

Dans une arnaque comme celle-ci, le manipulateur choisit une cible dont la connaissance en informatique est limitée. Plus la victime a des connaissances poussées, plus elle se méfiera ou s'apercevra facilement qu'elle est manipulée. Celui que je nomme parfois *l'employé aux prises avec l' informatique*, qui est peu au fait des technologies et des procédures, est plus enclin à obéir. Il est plus susceptible de tomber dans un piège où on lui demande de "télécharger simplement ce petit programme", car il n'a aucune idée des dommages potentiels de certains logiciels. En outre, il y a peu de chance qu'il estime la valeur des informations qui se trouvent sur le réseau.

AIDONS UN PEU LA PETITE NOUVELLE

Les employés récemment arrivés représentent une cible idéale pour les attaquants. Ils ne connaissent pas encore beaucoup de gens, ni les procédures, ni ce qu'il faut faire ou pas dans l'entreprise. Et dans l'espoir de faire bonne impression, ils s'empressent de montrer combien ils savent être coopérants et prompts à répondre.

Serviable Andrea

"Ressources Humaines, Andrea Calhoum."

"Andrea, bonjour, ici Alex de Corporate Security."

"Oui ?"

"Comment allez-vous aujourd'hui ?"

"Bien. Que puis-je faire pour vous ?"

"Voilà, nous mettons au point un séminaire sur la sécurité pour les nouveaux employés et nous avons besoin de quelques personnes pour le tester. Je voudrais le nom et le numéro de téléphone de tout le personnel embauché au cours du dernier mois. Pourriez-vous m'aider ?"

"Je ne pourrai pas avant cet après-midi. Ça vous ira ? Quel est votre numéro de poste ?"

"Bien sûr, ça ira, c'est le 52... Oh, mais je serai en réunion une grande partie de la journée. Je vous appellerai quand je serai de retour à mon bureau, certainement après seize heures."

Lorsque Alex appelle vers 16 h 30, Andrea tient une liste prête et lui donne les noms et les numéros de poste.

Un message pour Rosemary

Rosemary Morgan est enchantée de son nouvel emploi. Elle n'a jamais travaillé pour un magazine et les gens sont plus sympathiques qu'elle ne le pensait, ce qui est surprenant, du fait de la pression sans relâche que subit la plupart de l'équipe pour boucler le numéro chaque mois. L'appel qu'elle reçoit ce jeudi matin confirme une nouvelle fois cette impression de bienveillance.

"Vous êtes bien Rosemary Morgan ?"

"Oui."

"Bonjour Rosemary. Ici Bill Jorday du groupe Sécurité des Informations."

"Oui ?"

"Quelqu'un de notre service vous a-t-il informée quant aux pratiques de sécurité ?"

"Non."

"Voyons. Nous ne permettons à personne d'installer un logiciel apporté de l'extérieur de l'entreprise. En effet, nous ne voulons avoir aucun problème lié à l'utilisation de logiciels sans licence. De plus, cela évite tout problème avec des logiciels susceptibles de contenir un ver ou un virus."

"D'accord."

"Êtes-vous au courant de nos règles d'utilisation du courrier électronique ?"

"Non."

"Quelle est votre adresse e-mail actuelle ?"

"Rosemary@ttrzine.net."

"Vous ne vous connectez pas sous le nom d'utilisateur Rosemary ?"

"Non, c'est R-Morgan."

"Bien. Nous voulons que tous nos nouveaux employés soient conscients qu'il peut être dangereux d'ouvrir un fichier joint qu'ils n'attendent pas. Nombre de virus et de vers arrivent dans des messages qui proviennent apparemment de gens que vous connaissez. Donc, si vous recevez un e-mail avec un fichier joint que vous n'attendez pas, vous devez toujours vérifier si c'est bien la personne listée comme expéditeur qui vous l'a envoyé. Vous comprenez ?"

"Oui, j'ai entendu parler de cela."

"Bien. Et notre règlement précise que vous devez changer de mot de passe tous les quatre-vingt-dix jours. Quand avez-vous changé votre mot de passe pour la dernière fois ?"

"Je suis ici depuis trois semaines seulement ; j'utilise toujours le premier que l'on m'a fourni."

"Très bien. Vous pouvez attendre la fin des quatre-vingt-dix jours. Mais nous avons besoin de nous assurer que les mots de passe utilisés ne sont pas trop faciles à deviner. Utilisez-vous un mot de passe constitué à la fois de lettres et de chiffres ?"

"Non."

"Nous devons régler cela. Quel mot de passe utilisez-vous actuellement ?"

"C'est le nom de ma fille : Annette."

"C'est un mot de passe vraiment peu sûr. Vous ne devez jamais choisir un mot de passe en lien avec un événement familial. Voyons un peu... Vous pourriez faire comme moi. Vous pouvez utiliser votre mot de passe actuel comme première partie, mais ensuite, à chaque fois que vous le modifiez, il serait bien d'ajouter un nombre correspondant au mois en cours."

"Ainsi, si je le fais maintenant pour mars, je devrais utiliser trois."

"C'est à vous de voir. Qu'est-ce qui serait le mieux pour vous ?"

"Annette-trois, je pense."

"Très bien. Voulez-vous que je vous indique comment effectuer la modification ?"

"Non, je le sais."

"Parfait. Encore une chose dont il nous faut vous parler. Votre ordinateur est équipé d'un logiciel antivirus et il est important de le maintenir à jour. Vous ne devez jamais désactiver la mise à jour automatique, même si votre ordinateur ralentit de temps en temps. D'accord ?"

"Bien sûr."

"Très bien. Et avez-vous notre numéro de téléphone à votre portée pour nous contacter en cas de problème informatique ?"

Elle ne l'a pas. Il lui communique le numéro qu'elle note soigneusement, puis elle reprend son travail, une nouvelle fois heureuse de toute l'attention dont elle est l'objet.

Analyse de l'arnaque

Cette histoire met en relief un principe sous-jacent que vous rencontrerez tout au long de ce livre : les renseignements les plus courants qu'un manipulateur souhaite obtenir d'un employé, indépendamment de son objectif ultime, sont les informations sur l'identification de la cible. Avec le nom du compte et le mot de passe d'un seul employé appartenant au bon service de l'entreprise, l'attaquant dispose de tout ce dont il a besoin pour s'introduire et localiser les éléments qu'il recherche. Posséder ces informations équivaut à trouver les clés du royaume : il peut alors se déplacer librement dans le domaine de l'entreprise et trouver le trésor convoité.

Le message de Mitnick

Avant que les nouveaux employés ne soient autorisés à accéder à n'importe quel système de l'entreprise, ils doivent recevoir une formation afin de respecter les bonnes procédures de sécurité, en particulier ne jamais dévoiler son mot de passe.

PAS AUSSI SÛR QUE VOUS LE PENSEZ

"L'entreprise qui ne fait pas l'effort de protéger ses informations sensibles est tout simplement négligente." Nombre de personnes seraient d'accord avec cette affirmation. Et le monde serait meilleur si la vie était aussi évidente et simple. Mais la vérité est que même les entreprises qui s'efforcent de protéger des informations confidentielles peuvent être exposées à de sérieux risques.

Voici une histoire qui illustre une fois de plus la façon dont les entreprises se trompent elles-mêmes quotidiennement, lorsqu'elles croient que leurs mesures de sécurité, conçues par des professionnels expérimentés et compétents, ne peuvent être contournées.

L'histoire selon Steve Cramer

Ce n'est pas une grande pelouse, de celles que l'on sème à grand coût. Elle ne rend personne jaloux. Et elle n'est assurément pas assez grande pour qu'il achète une tondeuse électrique, ce qui est une bonne chose puisque de toute façon, il ne l'utiliserait pas. Steve aime tondre avec une tondeuse mécanique : il met plus de temps, mais cela lui donne un prétexte commode pour se concentrer sur ses propres pensées au lieu d'écouter Anna lui raconter les histoires du personnel de la banque où elle travaille, ou lui énumérer les courses qu'il doit faire. Il hait ces tâches qui font partie intégrante de ses week-ends. Il lui vient à l'esprit que Pete, son fils de 12 ans, a sacrément bien fait de rejoindre l'équipe de natation : désormais, comme il doit se trouver à un entraînement ou à une compétition tous les samedis, il échappe aux corvées du samedi.

D'aucuns peuvent penser que le travail de Steve, qui consiste à concevoir de nouveaux appareils pour GeminiMed Medical Products, est ennuyeux ; mais Steve sait qu'il sauve des vies. Il pense qu'il exerce un métier créatif. Artistes, compositeurs, ingénieurs : dans l'esprit de Steve, tous sont confrontés au même type de défi que lui, à savoir créer quelque chose de nouveau. Et sa dernière invention, un nouveau type de stimulateur cardiaque curieusement intelligent, serait son plus bel aboutissement.

Il est presque 11 h 30 ce samedi, et Steve est contrarié parce qu'il a presque terminé de tondre la pelouse mais il n'a pas vraiment avancé dans sa réflexion : il cherche la façon de réduire l'énergie demandée par le stimulateur cardiaque, son dernier obstacle. Un sujet idéal à ressasser pendant qu'il tond, mais aucune réponse ne lui est encore venue.

Anna apparaît à la porte, les cheveux recouverts d'un foulard de cow-boy en cachemire rouge qu'elle porte toujours lorsqu'elle fait les poussières. "Téléphone !", lui lance-t-elle. "Quelqu'un du travail."

"Qui ?" demande Steve.

"Ralph quelque chose je crois."

Ralph ? Steve ne connaît aucun Ralph à GeminiMed, qui soit susceptible de l'appeler le week-end. Mais Anna a sans doute mal compris.

L'appel téléphonique de Ralph

"Steve, ici Ramon Perez du support technique." Ramon ! Steve se demande comment Anna a fait pour confondre un nom hispanique avec Ralph.

"Je vous appelle juste pour vous prévenir..." dit Ramon. "Trois des serveurs sont en panne, nous pensons que cela peut être dû à un ver. Nous devons nettoyer les disques et effectuer des restaurations de sauvegarde. Vos fichiers devraient pouvoir être rétablis et en mesure de fonctionner mercredi ou jeudi. Si nous avons de la chance."

"C'est absolument inacceptable !" dit Steve, en essayant de ne pas se laisser emporter. *Comment ces gens peuvent-ils être aussi stupides, pensent-ils vraiment qu'il peut se débrouiller sans accéder à ses fichiers tout le week-end et la plus grande partie de la semaine ?* "Pas question. Je vais travailler sur mon ordinateur chez moi dans moins de deux heures et j'aurai besoin d'accéder à mes fichiers. Est-ce bien clair ? "

"Oui, oui, tous les gens que j'ai appelés veulent être en haut de la liste. J'ai sacrifié mon week-end pour travailler là-dessus et ce n'est pas drôle de voir que tous ceux à qui je parle sont en rogne contre moi."

"Je suis sur la corde raide, l'entreprise compte sur mon travail ; je dois le terminer cet après-midi. Ne comprenez-vous pas cela ?"

"J'ai encore beaucoup de personnes à appeler avant même de commencer", dit Ramon. "Disons que vous aurez vos fichiers vers mardi ?"

"Pas mardi, pas lundi, aujourd'hui. MAINTENANT !" dit Steve.

"Bien, bien", dit Ramon ; Steve l'entend pousser un soupir de mécontentement. "Voyons ce que je peux faire. Vous utilisez le serveur RM22, c'est cela ?"

"Le RM22 et le GM16. Les deux."

"OK. Je peux gagner du temps. J'aurais besoin de votre nom d'utilisateur et de votre mot de passe."

Oh oh, pense Steve, *que se passe-t-il ? Pourquoi a-t-il besoin de mon mot de passe ? Pourquoi le personnel informatique ou quiconque en aurait besoin ?*

"Comment avez-vous dit que vous vous appeliez ? Et qui est votre supérieur ?"

"Ramon Perez. Écoutez, lorsque vous avez été embauché, vous avez dû remplir un formulaire pour obtenir votre compte d'utilisateur et indiquer un mot de passe. Je pourrais aller voir et vous montrer que nous l'avons dans un fichier ici. D'accord ?"

Steve réfléchit un moment puis accepte. Il attend de plus en plus impatiemment pendant que Ramon essaie de retrouver des documents dans un dossier. Quand il reprend enfin le téléphone, Steve l'entend qui fouille dans une pile de papiers.

"Ah, le voilà !" dit enfin Ramon. "Vous avez mentionné le mot de passe Janice."

Janice ? C'est le prénom de sa mère, et il l'a, en effet, parfois utilisé comme mot de passe. Il se peut très bien qu'il l'ait indiqué comme mot de passe lorsqu'il a rempli son formulaire d'embauche.

"Oui, c'est cela", admet-il.

"OK, nous perdons du temps en ce moment. Vous savez que je suis sérieux, vous voulez que je fasse au plus vite pour récupérer rapidement vos fichiers, alors il faut que vous m'aidiez."

"Mon nom d'utilisateur est s, d, cramer — c-r-a-m-e-r. Le mot de passe est 'pelican1'."

"Je vais y arriver" dit Ramon, paraissant finalement serviable. "Accordez-moi deux heures."

Steve termine la pelouse, déjeune, et le temps de se rendre à son ordinateur, constate que ses fichiers ont bien été restaurés. Il est satisfait d'avoir traité aussi énergiquement ce type de l'informatique peu coopérant et espère qu'Anna a entendu combien il est autoritaire. Il serait bon de féliciter cet homme ou son patron, mais cela fait partie des choses qu'il ne prend jamais le temps de faire.

L'histoire selon Craig Cogburne

Craig Cogburne était vendeur dans une entreprise de haute technologie, et il obtenait de bons résultats. Au bout d'un certain temps, il a commencé à réaliser qu'il avait une réelle aptitude pour deviner un client, comprendre ses résistances et détecter certaines de ses faiblesses ou vulnérabilités, ce qui lui permettait facilement de réaliser la vente. Il a pensé à d'autres façons d'utiliser ce talent, et cela l'a conduit vers un domaine beaucoup plus lucratif, celui de l'espionnage industriel. Voici comment il raconte ce qui s'est passé.

Cette mission-là est une sacrée mission. J'ai l'impression qu'elle ne va pas me prendre beaucoup de temps et qu'elle va être assez rentable pour me payer un voyage à Hawaii, ou peut-être à Tahiti !

Le gars qui m'a embauché ne m'a pas désigné le client, naturellement, mais son entreprise semble vouloir rattraper la concurrence d'un seul coup, rapidement et

facilement. Tout ce que j'aurai à faire, c'est me procurer les plans et les spécifications d'un nouveau gadget baptisé "stimulateur cardiaque", quel que soit cet appareil. L'entreprise s'appelle GeminiMed. Jamais entendu parler d'elle, mais c'est un établissement classé parmi les 500 premières entreprises et qui possède des succursales dans une demi-douzaine d'endroits. Cela facilite la tâche car, dans des entreprises plus petites, il y a de grandes chances pour que la personne à qui l'on s'adresse connaisse celle que l'on prétend être et découvre la supercherie. Ce qui peut ruiner toute l'opération.

Mon client m'a fait parvenir un fax, un extrait de magazine médical indiquant que GeminiMed travaille sur un stimulateur cardiaque de conception radicalement nouvelle, le STH-100. Pour dire la vérité, le journaliste a déjà effectué une grande partie de mon travail. Avant même de commencer, j'ai déjà le nom du nouveau produit, qui m'est indispensable.

Premier problème : obtenir le nom des personnes de l'entreprise qui travaillent sur le STH-100 ou qui peuvent avoir besoin des plans. J'appelle donc la standardiste et dis : "J'ai promis à quelqu'un de votre groupe de le contacter et je ne me souviens plus de son nom, mais son prénom commence par un S". Elle répond : "Nous avons un Scott Archer et un Sam Davidson." Je prends alors un gros risque. "Lequel travaille dans le groupe STH-100 ?" Elle ne le sait pas ; je choisis Scott Archer au hasard, et elle me met en relation avec son poste.

Lorsqu'il décroche, je lui dis : "Bonjour, ici Mike de la salle du courrier, nous avons ici un paquet de la FedEx destiné à l'équipe du projet STH-100. Vous n'avez aucune idée du destinataire ?" Il me donne le nom du chef de projet, Jerry Mendel. J'obtiens même qu'il recherche pour moi son numéro de téléphone. J'appelle. Mendel est absent mais un message sur son répondeur dit qu'il est en vacances jusqu'au 30 — il dispose donc encore d'une semaine pour skier ou faire autre chose —, et qu'en cas de besoin pendant son absence, on doit appeler Michelle au 9137. Très serviables, ces gens, vraiment.

Je raccroche, appelle Michelle et l'obtiens au téléphone : "Ici Bill Thomas. Jerry m'a dit de vous appeler lorsque j'aurais la spécification qu'il veut faire relire à ses collaborateurs. Vous travaillez sur le stimulateur cardiaque, c'est bien cela ?" Elle répond que oui.

À présent, nous abordons la partie délicate de l'arnaque. Si jamais elle commençait à paraître méfiante, j'étais prêt à jouer la carte de la simple faveur faite à Jerry. Je lui demande sur quel système ils sont.

"Système ?"

"Quels serveurs informatiques utilise votre équipe ?"

"Oh, dit-elle, le RM22. Et certains membres se servent aussi du GM16."

Très bien. J'avais besoin de cette information et j'ai pu l'obtenir sans éveiller les soupçons de mon interlocutrice. Cela l'a amadouée pour la demande suivante, que je formule sur le ton le plus indifférent possible : "Jerry m'a dit que vous pourriez me donner la liste des adresses e-mail des membres de l'équipe de développement", en retenant mon souffle.

"Bien sûr. Mais la liste est trop longue à lire, puis-je vous l'envoyer par e-mail ?

Oups. Toute adresse e-mail qui ne finirait pas par GeminiMed.com serait comme un énorme drapeau rouge. "Cela ne vous dérangerait pas de me le faxer ?"

Elle n'y voit aucun inconvénient.

"Notre fax est en panne. Je dois obtenir le numéro d'un autre, je vous rappelle dans un instant" lui dis-je. Puis je raccroche.

À présent, vous pensez peut-être que je me trouve devant un problème insoluble, mais il ne s'agit que d'une autre astuce courante du métier. J'attends un peu pour que ma voix ne paraisse pas familière à la réceptionniste, puis je l'appelle : "Bonjour, Bill Thomas à l'appareil. Notre fax ne fonctionne pas, puis-je faire envoyer un fax sur votre machine ?" Elle répond que c'est possible et me donne le numéro.

Et j'irais simplement retirer le fax, c'est cela ? Bien sûr que non. Première règle : ne jamais se rendre sur les lieux, sauf absolue nécessité. Vous êtes très difficilement identifiable si vous n'êtes qu'une voix au téléphone. Et si l'on ne peut pas vous identifier, on ne peut pas vous arrêter. Il est difficile de passer les menottes à une voix. Je rappelle donc la réceptionniste peu après pour lui demander si mon fax est arrivé. "Oui" répond-elle.

"En fait, je dois le transmettre à un consultant que nous employons. Pourriez-vous l'envoyer pour moi ?" Elle accepte. Et pourquoi pas ? Comment une simple réceptionniste pourrait-elle reconnaître des données sensibles ? Pendant qu'elle envoie le fax au consultant, je fais mon sport de la journée en me rendant à la papeterie qui est proche de chez moi, et dont l'enseigne indique "Envoi/Réception de fax". Mon fax était supposé arriver avant moi et c'est bien le cas. Je possède la liste complète des noms et adresses e-mail de l'équipe.

S'introduire

Donc, jusqu'à présent, j'ai été en contact avec trois ou quatre personnes différentes en seulement quelques heures et j'ai fait un pas de géant qui va bientôt me permettre de m'introduire dans les ordinateurs de l'entreprise. Mais il me faut d'abord d'autres éléments.

La priorité est le numéro de téléphone qui me permettra d'appeler le bon serveur de l'extérieur. J'appelle GeminiMed une dernière fois et demande le service informatique à la réceptionniste, puis une personne susceptible de m'aider en informatique. Elle me passe quelqu'un et j'affecte d'être confus et très ignorant de tout ce qui est technique. "Je suis à la maison, je viens d'acheter un nouveau portable, et j'ai besoin de le configurer pour pouvoir me connecter de l'extérieur."

La procédure est évidente, mais patiemment, je le laisse me guider jusqu'à ce qu'il arrive au numéro de téléphone d'appel entrant. Il me donne le numéro comme s'il s'agissait d'une information banale. Je lui demande d'attendre pendant que j'essaie. Parfait.

À présent, j'ai franchi l'obstacle de la connexion au réseau. J'appelle et découvre que le service est équipé d'un serveur de terminaux permettant à toute personne de se connecter à n'importe quel ordinateur du réseau interne. Après quelques essais, je tombe sur l'ordinateur d'une personne, qui possède un compte d'invité sans mot de passe obligatoire. Certains systèmes d'exploitation, lors de leur première installation, demandent à l'utilisateur de mettre en place un identifiant et un mot de passe, mais fournissent également un compte d'invité. L'utilisateur est supposé fournir son mot de passe personnel pour le compte d'invité ou désactiver celui-ci, mais la plupart des gens ne le savent pas ou ne s'en préoccupent pas. Ce système venait sûrement d'être installé et le propriétaire n'a pas pris la peine de désactiver le compte d'invité.

Grâce au compte d'invité, j'ai désormais accès à un ordinateur, qui s'avère fonctionner sur une ancienne version du système d'exploitation UNIX. Sous UNIX existe un fichier de mots de passe qui renferme les mots de passe cryptés de toutes les personnes autorisées à accéder à l'ordinateur. Ce fichier contient le *hachage* unidirectionnel (c'est-à-dire une forme de cryptage irréversible) du mot de passe de chaque utilisateur. Avec un hachage unidirectionnel, un mot de passe réel comme "justdoit" devrait être représenté par un hachage crypté ; dans ce cas, UNIX devrait convertir le hachage en treize caractères alphanumériques.

Le message de Mitnick

Hachage de mot de passe
Il s'agit d'une chaîne de charabia qui résulte du traitement d'un mot de passe *via* un processus de cryptage unidirectionnel. Le processus est censé être irréversible, c'est-à-dire que l'on considère qu'il est impossible de reconstruire le mot de passe à partir du hachage.

Lorsqu'un utilisateur lambda veut transférer des fichiers sur un ordinateur, il doit s'identifier en indiquant un nom d'utilisateur et un mot de passe. Le programme du système qui contrôle cette autorisation encode le mot de passe saisi puis compare le résultat au mot de passe crypté (le hachage) contenu dans le fichier de mots de passe ; si les deux concordent, il autorise l'accès.

Comme les mots de passe du fichier sont cryptés, ce fichier est à la disposition de n'importe quel utilisateur puisque, en théorie, il n'existe aucun moyen de décrypter les mots de passe. Je télécharge donc le fichier, le soumets à une attaque de dictionnaire (voir le Chapitre 12 pour de plus amples informations sur cette méthode) et découvre que l'un des ingénieurs de l'équipe de développement, un certain Steven Cramer, possède un compte sur l'ordinateur, et que son mot de passe est "Janice". À tout hasard, j'essaie d'ouvrir ce compte avec ce mot de passe sur l'un des serveurs de développement : si cela fonctionne, j'économiserai du temps et des risques. Mais ce n'est pas le cas.

Cela signifie que je dois amener la personne à me dévoiler son nom d'utilisateur et son mot de passe. Et pour cela, je dois attendre le week-end.

Vous connaissez déjà la suite. Le samedi, j'appelle Cramer et invente une histoire de ver et de serveurs à restaurer à partir de sauvegardes, afin de déjouer ses soupçons.

Quant à l'histoire que je lui ai racontée concernant le fait qu'il avait indiqué un mot de passe en remplissant ses papiers à l'embauche, je comptais sur le fait qu'il ne se rappellerait pas que cela ne s'était jamais produit. Un nouvel employé remplit tant de formulaires que des années plus tard, comment s'en rappellerait-il ? Et de toute façon, s'il m'avait coincé, il restait bien d'autres noms sur la longue liste que je possédais.

Avec le nom d'utilisateur et le mot de passe de Cramer, je me suis introduit dans le serveur, fureté ici et là, et j'ai enfin localisé les fichiers des plans du STH-100. Ne sachant pas lesquels étaient essentiels, j'ai transféré tous les fichiers vers un site FTP gratuit situé en Chine, où ils pouvaient être stockés

sans éveiller les soupçons de quiconque. Le client n'avait plus qu'à trier pour trouver ce qu'il cherchait.

Analyse de l'arnaque

Pour ce Craig Cogburne, comme pour quiconque excelle dans les arts tortueux mais pas toujours légaux de la manipulation, la mission présentée ici représente un défi presque banal. Le but est de localiser et de télécharger des fichiers stockés sur un ordinateur d'entreprise sécurisé, protégé par un pare-feu et par toutes les technologies sécuritaires habituelles.

La plus grande partie du travail a été un jeu d'enfant. Il s'est d'abord fait passer pour un employé de la salle du courrier et a créé un sentiment d'urgence en prétendant qu'un paquet de la FedEx attendait d'être livré. Cette ruse lui a permis de récupérer le nom du responsable de l'équipe d'ingénieurs qui travaillaient sur le stimulateur cardiaque. Ce responsable était en vacances mais, élément très utile pour tout manipulateur qui souhaite voler des informations, il avait laissé le nom et le numéro de téléphone de son assistante. En appelant celle-ci, Craig a écarté tout soupçon éventuel en prétendant qu'il répondait à une demande du chef d'équipe. Le chef d'équipe étant parti en vacances, Michelle n'avait aucun moyen de vérifier auprès de lui les dires de Craig. Elle l'a donc cru et a fourni sans problème la liste des membres du de l'équipe : pour Craig, il s'agissait d'une information nécessaire et capitale.

L'assistante ne s'est même pas méfiée lorsque Craig lui a demandé d'envoyer la liste par fax plutôt que par e-mail, ce qui est pourtant plus commode pour l'expéditeur et le destinataire. Pourquoi tant de crédulité ? Comme de nombreuses employées, elle ne voulait pas que son patron découvre, à son retour, qu'elle n'avait pas répondu comme il fallait à une personne qui essayait simplement de satisfaire une demande que lui-même avait formulée. Par ailleurs, selon cet interlocuteur, le patron n'avait pas seulement autorisé cette requête, il avait également requis son assistance. Une fois encore, cet exemple met en situation une personne qui souhaite fortement se montrer coopérative ; or, la plupart des personnes qui ont cette propension se font plus facilement duper.

Ensuite, Craig ne se risque pas à pénétrer physiquement dans le bâtiment pour récupérer le fax : il obtient de la réceptionniste qu'elle le lui envoie, sachant qu'elle est disposée à coopérer. Après tout, les réceptionnistes sont généralement choisies pour leur amabilité et leur capacité à faire bonne impression. Rendre de petits services comme recevoir et envoyer un fax relève du travail d'une réceptionniste, fait que Craig était capable d'exploiter.

Quiconque aurait connu la valeur des informations qui lui passaient entre les mains aurait tiré la sonnette d'alarme, mais ce n'était pas le cas de la réceptionniste.

En utilisant un style de manipulation différent, Craig a joué l'ignorant et le naïf pour amener l'expert en informatique à lui fournir le numéro qui permettrait d'accéder de l'extérieur au terminal de l'entreprise, matériel qui sert de point de connexion aux autres systèmes informatiques du réseau interne.

Craig a pu se connecter facilement en essayant un mot de passe par défaut, qui n'avait jamais été changé : les mots de passes non modifiés constituent l'une des grandes failles les plus évidentes que l'on trouve sur de nombreux réseaux internes protégés par pare-feu. En fait, les mots de passe par défaut de nombreux systèmes d'exploitation, routeurs et autres types de produits, sont disponibles en ligne. N'importe quel manipulateur, hacker, ou espion industriel, de même que le simple curieux, peut trouver la liste sur http://www.phenoelit.de/dpl/dpl.html. (Il est incroyable de voir à quel point Internet facilite la vie de ceux qui savent où chercher.)

Cogburne s'est ensuite arrangé pour amener un homme prudent et soupçonneux ("Comment avez-vous dit que vous vous appeliez ? Qui est votre supérieur ?") à lui donner son nom d'utilisateur et son mot de passe, ce qui lui a permis d'accéder aux serveurs utilisés par l'équipe de développement du stimulateur cardiaque. Cela revenait à ouvrir la porte à Craig pour qu'il passe en revue les secrets les plus étroitement surveillés de l'entreprise et télécharge les plans du nouveau produit.

Que se serait-il passé si Steve Cramer avait continué à se méfier de l'appel de Craig ? Il était peu probable qu'il fasse part de ses soupçons avant son arrivée au travail le lundi matin, et il aurait été trop tard pour empêcher l'attaque.

Élément clé pour comprendre la dernière partie de la ruse : Craig s'est d'abord montré apathique et indifférent aux soucis de Steve, puis il a changé de ton et a paru vouloir l'aider. En effet, la plupart du temps, si la victime pense que vous essayez de l'aider ou que vous lui faites une faveur, elle livre des informations confidentielles qu'elle aurait sinon soigneusement protégées.

EMPÊCHER L'ARNAQUE

L'une des astuces les plus puissantes du manipulateur consiste à retourner la situation. C'est ce que nous avons vu dans ce chapitre. Le manipulateur crée un problème puis le résout magiquement, amenant la victime à fournir l'accès aux secrets les mieux gardés de l'entreprise. Vos employés tomberaient-ils dans ce

type de panneau ? Vous êtes-vous soucié de rédiger et de diffuser des règles de sécurité spécifiques pouvant contribuer à l'empêcher ?

Instruire, instruire et instruire encore

Il existe une vieille histoire au sujet d'un touriste en visite à New York qui arrête un passant dans la rue et lui demande "Comment va-t-on à Carnegie Hall ?" Le passant répond "Il faut pratiquer, pratiquer, pratiquer encore". Tout le monde est si vulnérable aux attaques des manipulateurs que la seule défense efficace consiste à instruire et à former ses employés, en les entraînant comme il faut pour qu'ils sachent repérer un manipulateur, puis en entretenant régulièrement leurs réflexes par rapport à ce qu'ils ont appris lors de la formation, car ils les perdent trop facilement.

Chaque membre de l'entreprise doit apprendre à montrer un degré de suspicion et de prudence approprié quand il est contacté par quelqu'un qu'il ne connaît pas personnellement, en particulier lorsque ce dernier demande d'une manière ou d'une autre l'accès à un ordinateur ou à un réseau. Il est dans la nature humaine de vouloir croire autrui, mais comme le disent les Japonais, "les affaires, c'est la guerre". Or vous ne pouvez pas vous permettre de baisser votre garde dans vos affaires. Les règles de sécurité de l'entreprise doivent clairement définir ce que sont les comportements appropriés et inappropriés.

La sécurité n'est pas la même pour tous. Ainsi, le personnel commercial a généralement un rôle et des responsabilités très différents, et à chaque poste correspondent des vulnérabilités particulières. Il est souhaitable de mettre en place une formation de base que tout le personnel de l'entreprise doit suivre, puis que chacun doit compléter en fonction de son profil professionnel afin de réduire les risques de devenir un jour une cible. Les employés qui gèrent des informations sensibles ou occupent des postes de confiance devraient recevoir une formation spécialisée complémentaire.

Protéger les informations sensibles

Tout employé approché par un étranger qui lui propose de l'aide, comme nous l'avons vu dans les histoires de ce chapitre, doit suivre les règles de sécurité de l'entreprise, qui sont élaborées en adéquation avec les besoins commerciaux, la taille et la culture de ladite entreprise.

Il ne faut jamais coopérer avec un étranger qui vous demande de rechercher des informations pour lui, d'exécuter des commandes inhabituelles sur un ordinateur, de modifier la configuration de logiciels ou encore d'ouvrir un

fichier joint à un e-mail ou de télécharger un logiciel non contrôlé, ces derniers cas étant potentiellement les plus nuisibles de tous. Tout logiciel — même un programme qui semble ne rien faire — peut ne pas être aussi anodin qu'il y paraît.

Le message de Mitnick

Personnellement, je pense qu'une entreprise ne doit autoriser aucun échange de mots de passe. Il est plus facile d'instaurer une règle stricte qui interdit au personnel de partager ou d'échanger des mots de passe confidentiels. C'est également plus sûr. Mais lorsqu'une entreprise opte pour cette solution, elle doit le faire en fonction de sa propre culture et ses propres besoins en matière de sécurité.

Avec le temps, et quelle que soit l'excellence de notre formation, nous finissons par négliger certaines procédures. Nous oublions alors cette formation au moment critique, c'est-à-dire précisément au moment où nous en avons besoin. On pourrait penser qu'à peu près tout le monde sait (ou devrait savoir) qu'il ne faut pas donner son nom d'utilisateur et son mot de passe. Mais en réalité, il est nécessaire de rappeler fréquemment à chaque employé que s'il révèle le nom d'utilisateur et le mot de passe de l'ordinateur de son bureau, de son domicile ou même de la machine à affranchir de la salle du courrier, c'est un peu comme donner le code secret de sa carte de crédit.

Il existe occasionnellement — *très* occasionnellement — des circonstances dans lesquelles il est nécessaire, voire important, de fournir à autrui des informations confidentielles. Pour cette raison, on ne peut pas faire du mot "jamais" une règle absolue. Encore une fois, vos règles et procédures de sécurité doivent être très précises quant aux situations dans lesquelles un employé est autorisé à donner son mot de passe et, plus important encore, quant aux personnes autorisées à demander des informations.

Tenir compte de la source

Dans la plupart des entreprises, la règle devrait être que toute information dont la divulgation est susceptible de nuire à l'entreprise ou à un employé ne peut être donnée qu'à une personne connue et déjà vue, ou dont la voix est reconnue sans problème. Dans des situations où la sécurité est très importante, les seules demandes pouvant être satisfaites sont celles qui sont formulées en personne ou en utilisant un puissant moyen d'authentification.

Les procédures de classification des données doivent stipuler que les services de l'entreprise impliqués dans des travaux sensibles ne fourniront *aucune* information à tout individu non connu ou dont personne ne se porte garant d'une manière ou d'une autre.

Ainsi, comment traitez-vous une demande d'informations apparemment légitime — concernant par exemple la liste des noms et adresses e-mail du personnel de votre équipe —, qui provient d'un employé d'une autre entreprise ? Comment faire prendre conscience que des informations comme celles-ci, dont la valeur est moins évidente, par exemple, que celle d'une page de spécification d'un produit en cours de développement, doivent uniquement être utilisées en interne ? Élément clé de la solution : dans chaque service, il faut désigner des employés chargés de traiter toutes les demandes d'informations à transmettre à l'extérieur du groupe. Une formation approfondie à la sécurité doit alors être dispensée aux employés désignés afin qu'ils connaissent les procédures spéciales à suivre.

N'oublier personne

N'importe qui peut rapidement dresser une liste des services internes de l'entreprise qui ont besoin d'une haute protection contre des attaques malveillantes.

Mais nous oublions souvent d'autres endroits moins évidents, bien que très vulnérables. Ainsi, quand Craig Cogburne a demandé qu'on envoie un fax à un numéro de téléphone interne de l'entreprise, cela semblait inoffensif et suffisamment sûr, mais l'attaquant a profité de cette faille. La leçon à tirer de cela est la suivante : chacun des secrétaires et employés administratifs, cadres de l'entreprise et dirigeants doit recevoir une formation spécifique à la sécurité afin d'être sensibilisé à ce type d'astuces. N'oubliez pas de protéger la porte d'entrée : les réceptionnistes sont souvent des cibles privilégiées et doivent connaître les méthodes de duperie que peuvent utiliser les attaquants qui se présentent ou qui appellent.

En matière de sécurité, les entreprises devraient déterminer un point de contact unique qui joue le rôle de comptoir central pour les employés qui pensent avoir été la cible d'une manipulation. Le fait de disposer d'un service unique auquel rapporter les incidents de sécurité fournit un système d'alerte rapide et efficace, qui permet d'établir si une attaque coordonnée est en cours, et de réparer immédiatement le moindre dommage.

Chapitre 6

Pouvez-vous m'aider ?

Nous venons de voir comment les manipulateurs abusent les gens en leur proposant leur aide. Une autre forme d'approche consiste à inverser les rôles : le manipulateur prétend avoir besoin de l'aide de la personne qu'il sollicite. Nous pouvons tous nous apitoyer sur une personne qui se trouve dans le pétrin et cette approche a prouvé son efficacité maintes et maintes fois, permettant ainsi au manipulateur d'atteindre son objectif.

L'ÉTRANGER

Au Chapitre 3, nous avons présenté une histoire qui illustre la façon dont un attaquant peut amener une victime à dévoiler son numéro d'employé. Dans l'histoire qui suit, l'approche est différente mais elle aboutit au même résultat ; elle montre comment l'attaquant peut tirer profit de certaines informations.

Continuons avec les Jones

Dans la Silicon Valley réside une entreprise de réputation mondiale que nous ne nommerons pas. Ses bureaux de vente et ses installations, disséminés dans le monde, sont tous connectés au siège par l'intermédiaire d'un WAN (*Wide Area Network*). L'intrus, un garçon intelligent et plein d'entrain nommé Brian Atterby, sait qu'il est presque toujours plus facile de pénétrer dans un réseau *via* l'un de ses sites distants, dont on peut pratiquement affirmer que la sécurité est plus relâchée qu'au siège.

Il téléphone au bureau de Chicago et demande à parler à M. Jones. La réceptionniste demande s'il connaît le prénom de M. Jones. Il dit :

"Combien de Jones avez-vous ?" Elle répond qu'il y en a trois et l'interroge sur le service dans lequel travaille ce monsieur.

L'attaquant : "Si vous me donnez les prénoms, je vais peut-être le reconnaître." Elle énumère alors : "Barry, Joseph, Gordon."

"Joseph. Je suis pratiquement sûr que c'est lui, et il est dans... quel service ?"

"Développement commercial."

"Parfait. Pouvez-vous me le passer, s'il vous plaît ?"

Elle le met en relation. Lorsque Joseph Jones répond, voici ce que l'attaquant lui annonce : "M. Jones ? Bonjour, ici Tony, de la paie. Nous venons juste de faire aboutir votre demande pour que le règlement de votre salaire soit directement viré sur votre compte de l'Union de Crédit."

"QUOI ???!!! Vous plaisantez ! Je n'ai rien demandé de tel. Je n'ai même pas de compte à l'Union de Crédit."

"Oh non ! C'est déjà fait !"

Monsieur Jones n'est pas qu'un peu contrarié à l'idée que son salaire va peut-être arriver sur le compte d'une autre personne, et il commence à penser que le type à l'autre bout du fil doit être un peu lourd. Avant même qu'il ait pu répondre, l'attaquant indique : "Je ferais mieux de voir ce qui s'est passé. Les changements de salaires sont saisis par numéro d'employé. Quel est votre numéro d'employé ?"

Jones indique son numéro et le soi-disant Tony affirme : "Non, tout est en ordre, la demande ne vient pas de vous, alors." *Il sont de plus en plus stupides chaque année !*, se dit Joseph Jones.

"Je vérifie si on en a tenu compte et rectifie immédiatement l'erreur. Ne vous inquiétez pas, vous recevrez votre prochain salaire sans problème", le rassure le type.

Un voyage d'affaires

Peu de temps après, l'administrateur système du bureau des ventes d'Austin, au Texas, reçoit un appel téléphonique : "Ici Joseph Jones, je suis du service Développement commercial, au siège. Je serai en ville pendant la semaine, à l'Hôtel Driskill, et j'aimerais pouvoir accéder à mon e-mail. Pouvez-vous me créer un compte provisoire ?"

"Redonnez-moi votre nom, et votre numéro d'employé", répond l'administrateur système. Le faux Jones décline alors son nom."

"Restez en ligne, je vérifie si vous êtes dans la base de données", puis, un instant après : "Très bien, Joseph. Dites-moi, quel est le numéro de votre immeuble ?" L'attaquant ayant fait ses devoirs du soir, tient la réponse prête.

Le message de Mitnick

> Ne vous fiez pas aux protections et aux pare-feu pour protéger vos informations. Surveillez les points les plus vulnérables. Vous constaterez souvent que c'est votre personnel qui constitue le maillon faible.

"Parfait, lui dit l'administrateur système, ça roule."

Ce n'est pas plus compliqué que cela. L'administrateur système a vérifié le nom de Joseph Jones, le service et le numéro d'employé, et Joseph a fourni la bonne réponse à la question piège. "Votre nom d'utilisateur sera le même qu'à votre bureau, "jbjones", indique l'administrateur système, et je vais vous donner "changemoi" comme mot de passe initial."

Analyse de l'arnaque

Après deux appels téléphoniques et une quinzaine de minutes, l'attaquant a obtenu l'accès au WAN de l'entreprise. Cette entreprise ressemble à certains fameux bonbons, à savoir qu'elle a "une enveloppe croquante et dure avec un corps tendre et mou". L'enveloppe extérieure, le pare-feu, n'est pas une protection suffisante, car dès qu'un intrus réussit à la contourner, les systèmes informatiques internes possèdent une sécurité tendre et molle. Le plus souvent, ils sont donc mal protégés.

Et cela correspond à l'histoire que nous venons de voir. En se procurant un numéro d'appel et un compte, l'attaquant n'a même pas eu besoin de franchir un pare-feu Internet et, une fois à l'intérieur, il pouvait facilement compromettre la plupart des systèmes du réseau interne.

Je sais de source sûre qu'une ruse semblable a fonctionné chez l'un des plus grands éditeurs de logiciels informatiques de la planète. Vous pensez peut-être que les administrateurs système de telles entreprises reçoivent une formation afin de détecter ce genre de ruses. Mais d'après mon expérience, personne n'est en totale sécurité face à un manipulateur suffisamment intelligent et persuasif.

Jargon

Sécurité bonbon
Expression inventée par Bellovin et Cheswick, des Laboratoires Bell, pour décrire un dispositif de sécurité dans lequel le périmètre extérieur — un pare-feu, par exemple — est solide, mais l'infrastructure qui se trouve derrière est "molle", c'est-à-dire vulnérable.

SÉCURITÉ CLANDESTINE

À l'époque des bars clandestins — du temps de la prohibition —, pour être autorisé à entrer, un client potentiel devait d'abord se présenter à la porte et frapper. Après quelques instants, un petit volet s'ouvrait dans la porte et un visage sévère et intimidant scrutait l'extérieur. Si le visiteur connaissait la procédure, il donnait le nom d'un client habituel de l'endroit ("Je suis envoyé par Joe" suffisait généralement), après quoi le videur ouvrait la porte et le laissait entrer.

Mais le vrai truc consistait à savoir où se trouvait le bar clandestin, car la porte n'était pas signalée et les propriétaires n'accrochaient évidemment pas d'enseigne lumineuse pour indiquer leur présence. En général, il suffisait de se présenter au bon endroit pour entrer. Malheureusement, le même niveau de protection est largement appliqué dans le monde actuel de l'entreprise, ce qui génère un degré de non-protection que je désigne sous le terme de *sécurité clandestine*.

Jargon

Sécurité clandestine
Sécurité qui repose sur le principe que l'on sait où se trouve l'information recherchée, et que l'on utilise un mot ou un nom pour obtenir l'accès à cette information ou à un système informatique.

Vu au cinéma

Voici l'extrait d'un film que beaucoup de gens connaissent. Dans *Les trois jours du Condor*, le personnage principal, Turner (joué par Robert Redford), travaille pour une petite société qui dépend en fait de la CIA. Un jour, il revient de son déjeuner pour constater que tous ses collègues ont été abattus. Il ne lui reste plus qu'à essayer de deviner qui a fait ça et pourquoi, tout en sachant que ces individus, quels qu'ils soient, le recherchent.

Plus tard dans l'histoire, Turner arrive à obtenir le numéro de téléphone de l'un des sales types. Mais qui est-il, et comment Turner peut-il le localiser ? Il a de la chance : grâce au scénariste David Rayfiel, Turner a reçu une formation dans le corps des transmissions de l'armée, ce qui l'a mis au fait des techniques et des pratiques des entreprises de téléphonie. Comme il a le numéro de téléphone du type, Turner sait exactement quoi faire. Dans le scénario, la scène se déroule ainsi :

L'appel de Turner

Turner décroche de nouveau le téléphone et compose un autre numéro.

Dring ! Dring ! Puis,

Voix de femme (*filtrée*) :

"CNA, Mme Coleman à l'appareil."

Turner :

"Ici Harold Thomas, Mme Coleman. Service Clients.
CNA au 202-555-7389, s'il vous plaît."

Voix de femme (filtrée) :

"Un instant, s'il vous plaît."

(*Presque immédiatement.*)

"Leonard Atwood, 765 MacKensie Lane, Chevy Chase, Maryland."

Le scénariste associe par erreur un code de la zone de Washington avec une adresse du Maryland, mais peu importe : comprenez-vous ce qui s'est passé ici ?

Turner, grâce à sa formation, savait quel numéro appeler pour joindre le bureau de la compagnie de téléphone CNA. Ce service était réservé aux installateurs et à d'autres membres autorisés du personnel. Ainsi, un installateur pouvait appeler la CNA et lui indiquer un numéro de téléphone. L'employée lui répondait en lui fournissant le nom et l'adresse du titulaire de la ligne.

Duper la compagnie de téléphone

Dans la réalité, de tels numéros de téléphone sont gardés secrets. Même si les entreprises de téléphonie fournissent aujourd'hui moins généreusement les informations, elles fonctionnaient à l'époque sur une variante de la sécurité clandestine, que les professionnels de la sécurité appellent la *sécurité par obscurité*. Elles supposaient alors que quiconque appelait l'équivalent de la

CNA et connaissait le bon jargon ("Service clients. CNA au 202-555-7389, s'il vous plaît", par exemple) était une personne autorisée à recevoir l'information qu'elle sollicitait.

Jargon

Sécurité par obscurité
Ce terme désigne une méthode de sécurité informatique inefficace fondée sur le fait de garder secrets les détails de fonctionnement du système (protocoles, algorithmes et procédures internes). La sécurité par obscurité repose sur la supposition erronée qu'aucun individu ne pourra contourner le système s'il n'appartient pas à un groupe de personnes spécifique.

Le message de Mitnick

La sécurité par obscurité n'a *aucun* effet sur le blocage des attaques de manipulation. Chaque ordinateur dans le monde est utilisé par au moins un être humain. Par conséquent, si l'attaquant peut manipuler la personne qui utilise le système, l'obscurité du système ne sert à rien.

Nul besoin de vérifier, d'identifier, de fournir un numéro d'employé ou un mot de passe changé quotidiennement. Si vous connaissiez le numéro à appeler et paraissiez crédible, on supposait qu'il était légitime de vous donner les informations.

Cette hypothèse n'était pas très solide. La seule action entreprise en matière de sécurité consistait à changer régulièrement le numéro de téléphone, au moins une fois par an. Même ainsi, le numéro en cours était très largement connu des pirates téléphoniques, enchantés de pouvoir profiter de cette commodité et de la partager avec leurs amis pirates. L'existence d'un bureau de type CNA est l'une des premières choses que j'ai apprises lorsqu'on m'a parlé du passe-temps favori des adeptes du piratage téléphonique, alors que j'étais adolescent.

Partout dans le monde des affaires et au gouvernement, la sécurité par obscurité domine encore. Ainsi, il est probable que n'importe quel intrus semi-expert pourra se faire passer pour une personne autorisée en rassemblant simplement suffisamment d'informations sur les services, le personnel et le jargon de votre entreprise. Voire moins que cela : parfois, il suffit d'un numéro de téléphone interne.

UN DIRIGEANT INFORMATIQUE NÉGLIGENT

Même si les employés de nombreuses entreprises sont négligents, indifférents ou ignorants quant aux risques liés à la sécurité, on s'attend en tout cas à ce qu'une personne telle que le directeur du centre informatique d'une boîte qui figure parmi les 500 premières entreprises soit parfaitement informée des meilleures pratiques en matière de sécurité.

On ne s'attend pas à ce qu'une telle personne, notamment parce qu'elle fait partie du service informatique, soit la victime d'une manipulation simpliste et évidente. Mais ces suppositions peuvent parfois se révéler fausses.

Écoute des fréquences secrètes

Jadis, un passe-temps qui amusait beaucoup de gens consistait à régler une radio sur la fréquence des pompiers ou de la police, afin d'écouter les conversations parfois très tendues sur l'évolution d'une attaque de banque, de l'incendie d'un immeuble ou d'une course-poursuite. On pouvait trouver les fréquences radio utilisées par les forces de l'ordre et les pompiers dans certains livres vendus chez le libraire du coin. Aujourd'hui, des listings sur le Web vous fournissent, aux U.S.A., les fréquences locales, celles du comté, de l'État et parfois même celles des agences fédérales.

Naturellement, les curieux n'étaient pas les seuls à écouter. Les voleurs en train de dévaliser un magasin en pleine nuit pouvaient se régler sur la fréquence adéquate et savoir ainsi si une voiture de police était dépêchée sur les lieux. Les vendeurs de drogue gardaient un œil sur les activités des agents locaux de la DEA (*Drug Enforcement Agency*, l'agence chargée de lutter contre le trafic de drogue). Un incendiaire pouvait démultiplier son plaisir morbide en allumant un incendie et en écoutant tout le trafic radio qu'il générait pendant que les pompiers s'acharnaient à éteindre l'incendie.

Ces dernières années, les progrès informatiques ont permis de crypter les messages vocaux. À mesure que les ingénieurs ont découvert des moyens d'introduire de plus en plus de puissance de calcul dans une seule micropuce, ils ont commencé à fabriquer de petites radios cryptées pour les représentants de la loi, ce qui empêche les malfrats et les curieux d'écouter.

Danny l'oreille indiscrète

Passionné par les antennes et hacker compétent, Danny a décidé de chercher un moyen de se procurer le logiciel de codage hyper secret — le code source — de l'un des plus importants fabricants de systèmes radio sécurisés. Il espérait que l'étude du code lui permettrait d'écouter les forces de l'ordre,

et éventuellement d'utiliser la technologie de sorte que même les agences gouvernementales les plus puissantes éprouveraient des difficultés à surveiller ses conversations avec ses amis.

Les Danny du monde secret des hackers appartiennent à une catégorie particulière, située entre le purement curieux mais totalement anodin, et le dangereux. Les individus comme Danny possèdent les connaissances de l'expert, associées au désir malicieux du hacker d'entrer dans des systèmes et des réseaux pour le défi intellectuel et le plaisir de voir de l'intérieur le fonctionnement de la technologie. Mais leurs effractions électroniques ne sont que des tours de force. Ces hackers inoffensifs pénètrent illégalement les sites pour le pur plaisir et la joie de prouver qu'ils en sont capables. Ils ne volent rien et ne retirent pas d'argent de leurs exploits ; ils ne détruisent aucun fichier, n'interrompent aucune connexion réseau et ne plantent aucun système informatique. Mais le simple fait qu'ils piègent des copies de fichiers et recherchent des mots de passe dans des e-mails à l'insu des administrateurs réseau et de la sécurité casse les pieds des personnes chargées de protéger les systèmes. Le fait de se montrer supérieur aux autres représente une grande part de leur satisfaction.

Dans cette optique, notre Danny voulait examiner en détail le produit le plus étroitement surveillé de son entreprise cible, afin de satisfaire simplement sa brûlante curiosité personnelle et admirer les innovations réalisées par le fabricant.

Les plans du produit étaient, inutile de le préciser, des secrets de fabrication soigneusement gardés, aussi précieux et protégés que pratiquement n'importe quel bien de l'entreprise. Danny le savait. Et il ne s'en souciait pas. Après tout, ce n'était jamais qu'une grosse entreprise inconnue.

Mais comment obtenir le code source du logiciel ? En l'occurrence, s'emparer des joyaux de la couronne du service des communications sécurisées de l'entreprise s'est avéré très facile, même si l'entreprise utilisait une méthode d'authentification à deux facteurs, selon laquelle les personnes doivent prouver leur identité à l'aide de deux identifiants différents au lieu d'un seul.

Voici un exemple déjà courant dans certains pays. Lorsqu'une carte de crédit est renouvelée, la personne concernée doit appeler la banque émettrice pour lui signaler que la carte est bien en la possession de son titulaire et non de quelqu'un qui l'aurait dérobée dans le courrier. De nos jours, les instructions jointes à la carte indiquent généralement que la personne doit appeler *de son domicile*. Le cas échéant, un logiciel situé chez l'émetteur de la carte de

crédit analyse le numéro d'identification (ANI, *Automatic Number Identification*) fourni par le central téléphonique.

Un ordinateur prend le numéro du client et le compare à la base de données de la société émettrice. Le temps que l'employé prenne la ligne, son écran affiche les informations de la base de données qui concernent le client. Ainsi, l'employé sait déjà que l'appel provient du domicile d'un client ; il s'agit d'une forme d'authentification.

L'employé choisit alors l'un des éléments affichés à l'écran — le plus souvent le numéro de sécurité sociale, la date de naissance ou le nom de jeune fille de la mère du client — et interroge la personne sur cette information. L'exactitude de sa réponse constitue une seconde forme d'authentification, puisque ce sont des informations qu'il est censé connaître.

Jargon

Authentification à deux facteurs
Procédure qui utilise deux éléments de type différent pour vérifier une identité. Par exemple, il se peut qu'une personne doive s'identifier en appelant à partir d'un certain endroit identifiable et en donnant un mot de passe.

Dans l'entreprise de fabrication de systèmes radio sécurisés de notre histoire, chaque employé qui a accès à un ordinateur possède un nom de compte et un mot de passe classiques, et a en plus un petit appareil électronique, appelé SID (pour Secure ID). C'est ce que l'on appelle un jeton temporel (*time-based token*). Il en existe deux types : le premier fait environ la moitié de la taille d'une carte de crédit mais est un peu plus épais, l'autre est suffisamment petit pour que les gens l'attachent à leur porte-clés.

Ce gadget, qui provient du monde de la cryptographie, possède une petite fenêtre affichant une série de six chiffres. Toutes les soixante secondes, l'affichage change et indique un nombre différent. Lorsqu'une personne non autorisée a besoin d'accéder au réseau depuis l'extérieur, elle doit d'abord s'identifier comme utilisateur autorisé en saisissant son code secret et les chiffres affichés sur son SID. Après vérification par le système interne, elle s'authentifie avec son nom de compte et son mot de passe.

Pour que le jeune hacker Danny parvienne au code source tant convoité, il devait donc non seulement se procurer le nom d'utilisateur et le mot de passe d'un employé (pas très difficile pour un manipulateur expérimenté) mais également échapper au jeton temporel.

Passer à travers l'authentification à deux facteurs d'un jeton temporel associé au code PIN secret d'un utilisateur relève d'un défi digne de *Mission impossible*. Mais pour les manipulateurs, ce challenge est semblable à celui d'un joueur de poker qui a un talent hors du commun. Avec un peu de chance, en s'asseyant à la table, il sait déjà s'il est susceptible de rafler une grosse somme d'argent.

La forteresse prise d'assaut

Danny commence par les travaux préparatoires. En peu de temps, il réussit à rassembler suffisamment d'éléments pour se faire passer pour un employé. Il connaît le nom de l'employé, son service, son numéro de téléphone et son numéro d'employé, ainsi que le nom et le numéro de téléphone du directeur.

À présent, c'est le calme avant la tempête. Au sens littéral du terme. Selon le plan qu'il a établi, Danny a encore besoin d'un élément pour passer à l'étape suivante, élément qu'il ne peut absolument pas contrôler : il a besoin d'une tempête de neige ! Il faut que Dame Nature l'aide un peu, et que le temps devienne mauvais au point que les employés ne puissent pas se rendre à leur bureau.

Justement, l'usine de fabrication en question se trouve dans le Dakota du Sud et, l'hiver, quiconque espère du mauvais temps n'a pas longtemps à attendre. Un vendredi pendant la nuit, une tempête arrive. La neige se transforme rapidement en pluie verglaçante, de sorte qu'au matin, les routes sont recouvertes d'une dangereuse couche de glace bien lisse. Pour Danny, il s'agit d'une excellente opportunité.

Il téléphone à l'usine, demande la salle informatique et joint l'un des employés, un opérateur du nom de Roger Kowalski.

Danny se présente en se faisant passer pour l'employé dont il s'est procuré le nom : "Ici Bob Billings. Je travaille au service des communications sécurisées. Je suis à la maison et je ne peux pas venir à cause de la tempête. Le problème, c'est que j'ai besoin d'accéder à ma station de travail et au serveur depuis la maison, et j'ai laissé mon SID au bureau. Pourriez-vous aller le chercher ? Vous ou quelqu'un d'autre ? Puis lire mon code quand j'aurai besoin d'entrer ? Mon équipe a des délais très serrés et je ne peux pas achever mon travail. Et il n'est pas possible que je me rende au bureau, les routes sont beaucoup trop dangereuses sur mon trajet."

À quoi l'opérateur répond : "Je ne peux pas quitter le centre informatique."

Dany saute sur l'opportunité : "Avez-vous vous-même un SID ?"

"Il y en a un ici, au centre informatique", dit-il. "Nous en gardons un pour les opérateurs, en cas d'urgence."

"Bien" dit Danny. "Pouvez-vous me rendre un grand service ? Quand j'aurai besoin d'appeler le réseau, pourrez-vous me permettre d'emprunter votre SID ? Jusqu'à ce que je puisse reprendre la voiture."

"Qui êtes-vous, déjà ?" demande Kowalski.

"Bob Billings."

"Pour qui travaillez-vous ?"

"Pour Ed Trenton."

"Ah, oui, je le connais."

Lorsqu'il est susceptible de se trouver dans une position délicate, un bon manipulateur fait plus que le nécessaire : "Je suis au premier étage, ajoute-t-il, près de Roy Tucker."

L'opérateur connaît également ce nom. Danny revient sur son travail. "Il serait beaucoup plus facile d'aller simplement à mon bureau et d'y récupérer mon SID."

Danny est presque certain que le gars ne va pas accepter. En tout premier lieu, il ne voudra pas abandonner son poste au beau milieu de son astreinte pour traîner dans les couloirs et les cages d'escalier d'une partie éloignée de l'immeuble. Il ne voudra pas non plus toucher au bureau d'une autre personne et violer son espace personnel. Non, on peut facilement parier qu'il ne voudra pas faire cela.

Kowalski ne veut pas dire non à un employé qui sollicite son aide, mais il ne veut pas non plus dire oui et que ça lui apporte des ennuis. Il évite donc de prendre la décision : "Je dois demander à mon patron. Patientez." Il pose le téléphone et Danny l'entend prendre un autre appareil, appeler et expliquer la demande. Kowalski fait alors une chose inexplicable : il se porte garant de l'homme qui dit s'appeler Bob Billings. "Je le connais", dit-il à son directeur. "Il travaille pour Ed Trenton. Pouvons-nous lui permettre d'utiliser le SID du centre informatique ?" Danny, qui patiente au bout de l'autre ligne, n'en revient pas de recevoir une aide aussi extraordinaire et inattendue. Il ne peut en croire ses oreilles, ou sa chance.

Après quelques instants, Kowalski reprend la ligne et lui indique que son directeur veut lui parler lui-même, puis lui donne le nom et le numéro de portable du directeur.

Danny appelle le responsable et reprend une nouvelle fois toute l'histoire, en ajoutant des précisions sur le projet sur lequel il travaille et la raison pour laquelle son équipe de production doit tenir des délais serrés. "Il serait plus

facile que quelqu'un aille récupérer ma carte" dit-il. "Je ne crois pas que le bureau soit fermé à clé, elle devrait se trouver dans mon tiroir en haut à gauche."

"Bien" dit le responsable. "Juste pour le week-end, je pense que nous pouvons vous laisser utiliser celle du centre informatique. Je demanderai aux employés de service de vous lire le code d'accès aléatoire lorsque vous appellerez."

Pendant tout le week-end, chaque fois que Danny a voulu entrer dans le système informatique de l'entreprise, il lui a suffi d'appeler le centre et de demander qu'on lui lise les six chiffres affichés sur le jeton temporel du centre informatique…

Un travail de l'intérieur

Et une fois à l'intérieur du système informatique de l'entreprise, comment Danny allait-il retrouver le serveur qui héberge le logiciel recherché ? Il avait anticipé cela.

De nombreux utilisateurs d'ordinateurs fréquentent les groupes de discussion, ce vaste ensemble de pages électroniques où les gens peuvent poser des questions auxquelles d'autres répondent, où ils peuvent rencontrer des compagnons virtuels qui partagent un même intérêt en musique, informatique, ou sur des centaines d'autres sujets.

Mais peu de gens savent, lorsqu'ils mettent un message dans un groupe de discussion, que leur message reste disponible en ligne pendant des années. Par exemple, le moteur de recherches Google gère actuellement des archives de sept cent millions de messages, dont certains datent de vingt ans ! Danny commence donc par se rendre à l'adresse Web : http://groups.google.com.

Comme requête de recherche, Danny saisit "encodage radio communications" et le nom de l'entreprise. Il trouve un message vieux de plusieurs années sur ce sujet, émis par un employé lorsque l'entreprise a commencé à développer le produit, certainement bien avant que les services de police et les agences fédérales envisagent de brouiller les signaux radio.

Le message contient la signature de l'expéditeur, qui indique non seulement son nom, Scott Baker, mais aussi son numéro de téléphone et même le nom de son service, les communications sécurisées.

Danny décroche le téléphone et compose le numéro. Travaille-t-il toujours au même endroit, des années plus tard ? Est-il au travail par un tel week-end de tempête ? Le téléphone sonne, une fois, deux fois, trois fois, et une voix se fait entendre : "Ici Scott."

Prétendant appartenir au service informatique de l'entreprise, Danny amène Baker (par l'une des méthodes qui vous sont désormais familières) à révéler le nom des serveurs qu'il a utilisés pour ses travaux de développement. Ces serveurs sont susceptibles d'héberger le code source renfermant l'algorithme d'encodage et le microcode propriétaires utilisés pour les produits de radio sécurisés de l'entreprise.

Danny se rapproche de plus en plus du but, et son excitation grandit. Il anticipe le sentiment de grande supériorité qu'il ressent toujours lorsqu'il réussit une chose dont peu de gens sont capables.

Mais il n'y est pas encore arrivé. Jusqu'à la fin du week-end, il peut entrer dans le réseau de l'entreprise chaque fois qu'il le souhaite, grâce à ce responsable coopérant du centre informatique. Il connaît les serveurs auxquels il doit accéder. Mais lorsqu'il appelle, le serveur de terminaux auquel il se connecte ne lui permet pas d'accéder aux systèmes de développement des communications sécurisées. Il doit y avoir un pare-feu ou un routeur interne qui protège les systèmes d'ordinateurs de ce groupe. Il doit trouver un autre moyen.

L'étape suivante requiert du sang-froid : Danny rappelle Kowalski et se plaint que son serveur ne l'autorise pas à se connecter. "J'ai besoin que vous m'installiez un compte sur l'un des ordinateurs de votre service afin que j'utilise Telnet pour me connecter à mon système."

Le directeur a déjà accepté de dévoiler le code d'accès affiché sur le jeton temporel, aussi cette nouvelle demande ne paraît-elle pas déraisonnable. Kowalski crée un compte et un mot de passe provisoires sur l'un des ordinateurs du centre des opérations et dit à Danny : "Rappelez-moi quand vous n'en aurez plus besoin pour que je le supprime."

Un fois qu'il est connecté *via* le compte provisoire, Danny est en mesure de se connecter à travers le réseau aux ordinateurs du service des communications sécurisées. Après avoir cherché en ligne pendant une heure une faille qui pourrait lui donner l'accès à un serveur de développement principal, il décroche le gros lot. Apparemment, l'administrateur système ou réseau n'a pas pris soin de se renseigner sur les derniers bogues de sécurité du système d'exploitation qui permettent un accès à distance. Mais Danny l'a fait.

En peu de temps, il localise les fichiers de code source recherchés et les transfère sur un site de e-commerce qui propose un espace de stockage gratuit. Si les fichiers sont un jour découverts sur ce site, ils ne pourront jamais mener jusqu'à lui.

Il lui reste une dernière tâche à accomplir : effacer soigneusement ses traces. Danny pense que le week-end a été productif. Et il n'a jamais été

obligé de prendre des risques. L'expérience a été enivrante, bien plus que celles qu'il ressent à faire du ski ou du parachutisme.

Danny s'enivre cette nuit-là, non pas de whisky, de gin, de bière ni de saké, mais de cette puissance et de cette sensation d'accomplissement qu'il éprouve à mesure qu'il se noie dans les fichiers qu'il a dérobés et qu'il se rapproche de l'insaisissable logiciel de radio si secret.

Analyse de l'arnaque

Comme dans l'histoire précédente, la ruse n'a fonctionné que parce qu'un employé de l'entreprise s'est montré trop bien disposé à prendre pour argent comptant ce que lui racontait son interlocuteur au téléphone. D'un côté, l'empressement dont témoignent les employés pour aider des collègues à régler des problèmes est un élément qui contribue au bon fonctionnement de l'industrie, et qui fait qu'il est plus agréable de travailler avec les employés de telle entreprise plutôt qu'avec ceux de telle autre. D'un autre côté, cette serviabilité peut constituer un point faible majeur qu'un manipulateur essaiera d'exploiter.

Une partie de la manipulation employée par Danny est savoureuse : lorsqu'il demande si quelqu'un peut récupérer son SID dans son bureau, il ne cesse d'employer l'expression "aller chercher", qui sert aussi à donner des ordres à son chien. Personne n'aime qu'on lui demande d'aller chercher quelque chose. Avec ces simples mots, Danny est d'autant plus certain que sa requête sera refusée et la solution de remplacement acceptée, ce qui est exactement le but recherché.

L'opérateur du centre informatique, Kowalski, s'est laissé tromper par Danny lorsqu'il a cité des noms de personnes que Kowalski connaît. Mais pourquoi le *directeur* de Kowalski — un directeur informatique, pas moins — permet-il à un étranger d'accéder au réseau interne de l'entreprise ? Tout simplement parce que l'appel à l'aide peut être un outil de persuasion puissant dans l'arsenal du manipulateur.

Le message de Mitnick

Cette histoire montre que les formes d'authentification telles que celles qui font appel aux jetons temporels ne constituent pas une défense contre le manipulateur astucieux. La seule défense repose sur des employés consciencieux qui respectent les règles de sécurité et savent de quelle façon les autres peuvent influencer malicieusement leur comportement.

Une histoire comme celle-là pourrait-elle se produire dans *votre* entreprise ? S'est-elle déjà produite ?

EMPÊCHER L'ARNAQUE

Un élément récurrent apparaît dans ces histoires : l'attaquant s'arrange pour appeler le réseau informatique de l'entreprise de l'extérieur, sans que la personne qui l'aide prenne les mesures suffisantes pour vérifier qu'il est bien l'employé qu'il dit être et qu'il est autorisé à bénéficier de cet accès. Quelle raison me fait aussi souvent revenir sur ce thème ? C'est parce que la confiance est un facteur présent dans un très grand nombre d'attaques de manipulation. Pour le manipulateur, il s'agit du moyen le plus simple d'atteindre son but. Pourquoi un attaquant passerait-il des heures à essayer de rentrer par la force lorsqu'il peut y parvenir *via* un simple appel téléphonique ?

Du point de vue du manipulateur, l'une des méthodes les plus puissantes pour mener à bien ce type d'attaque consiste à prétendre qu'il a besoin d'aide, et cette approche est fréquemment utilisée par les attaquants. À l'évidence, vous ne voulez pas que vos employés arrêtent d'aider leurs collègues ou les clients : vous devez donc les armer de procédures de vérification spécifiques qu'ils appliqueront lorsque quiconque demandera un accès à un ordinateur ou à des informations confidentielles. Ainsi, ils continueront d'aider ceux qui le méritent tout en protégeant les informations et les systèmes informatiques de l'entreprise.

Les procédures de sécurité de l'entreprise doivent expliquer clairement et en détail le type de système de vérification qui doit être utilisé dans les diverses circonstances. Voici quelques conseils généraux à prendre en compte :

- Un bon moyen de vérifier l'identité d'une personne qui formule une requête consiste à appeler le numéro de téléphone de cette personne, tel qu'indiqué dans le répertoire de l'entreprise. Si la personne est en réalité un attaquant, l'appel de vérification vous mettra en contact avec la vraie personne pendant que l'imposteur sera en attente, ou vous joindrez la boîte vocale du véritable employé de sorte que vous serez en mesure d'écouter le son de sa voix et le comparer à celui de l'attaquant.
- Si, pour vérifier les identités, votre entreprise utilise des numéros d'employés, ces numéros doivent être traités comme des informations sensibles qu'il faut surveiller étroitement et ne pas dévoiler à des étrangers. Ce principe s'applique également à tous les autres

types d'identifiants internes comme les numéros de téléphone internes et les adresses de courrier électronique.

- Les formations données par l'entreprise doivent attirer l'attention de chacun sur le fait qu'il est courant de considérer les inconnus comme des employés légitimes simplement parce qu'ils paraissent autorisés ou informés. Qu'une personne connaisse les pratiques d'une entreprise ou emploie la terminologie interne ne dispense pas de vérifier son identité.
- Les responsables de la sécurité et les administrateurs ne doivent pas limiter leur attention à la prudence que les *autres* manifestent. Ils doivent également s'assurer qu'eux-mêmes respectent les mêmes règles, procédures et pratiques.
- Les mots de passe et autres identifiants du même genre ne doivent naturellement jamais être partagés, mais la restriction concernant le partage est encore plus importante avec les jetons temporels et les autres formes d'authentification sécurisées. Il doit relever du bon sens que le partage de l'un de ces éléments viole la globalité de l'installation des systèmes de sécurité développés par l'entreprise. Si un incident de sécurité survient, ou si quelque chose fonctionne mal, vous ne pourrez pas désigner de responsable.
- Comme je le répète tout au long de ce livre, les employés doivent se familiariser avec les stratégies et les méthodes de manipulation, afin d'être en mesure d'analyser dans leur intégralité les requêtes qu'ils reçoivent. Il est bon que les jeux de rôles fassent partie intégrante des formations à la sécurité : si vous y avez recours, ils aideront vos employés à mieux connaître la façon de démasquer des manipulateurs.

Chapitre 7

Faux sites et liaisons dangereuses

Un vieux proverbe dit que l'on n'a jamais rien sans rien. Pourtant, le stratagème qui consiste à offrir quelque chose gratuitement continue d'être appliqué aussi bien dans les affaires légitimes ("Mais attendez, il y en a encore ! Appelez immédiatement et nous ajouterons une série de couteaux !") que dans celles qui le sont moins ("Achetez un hectare de terrain sur la Côte d'Azur et recevez-en un autre gratuit !").

Et la plupart d'entre nous sommes si avides de recevoir quelque chose de gratuit que nous pouvons devenir aveugles et ne plus voir la réalité de l'offre ou de la promesse. Nous connaissons l'avertissement habituel : "Acheteur, prends garde", mais il est maintenant temps de tenir compte d'un autre conseil : il faut faire attention aux fichiers joints, aux e-mails ainsi qu'aux logiciels gratuits. Un attaquant astucieux exploitera tous les moyens possibles pour s'introduire dans le réseau d'une entreprise, notamment notre satisfaction bien naturelle à recevoir des cadeaux. Nous en présentons quelques exemples dans ce chapitre.

VOULEZ-VOUS UN CADEAU ?

À l'image des virus, véritables fléaux pour les médecins et pour l'humanité en général, le bien-nommé "virus informatique" représente un fléau comparable dans le monde de l'informatique. Les virus informatiques qui accaparent le plus l'attention et font le plus parler d'eux — et ce n'est pas fortuit — sont ceux qui créent le plus de dégâts. Ce sont des produits de gens malintentionnés.

Les petits voyous de l'informatique essaient de montrer aux autres leur savoir-faire. Parfois, leurs actes ressemblent à un rite d'initiation, destiné à impressionner les hackers plus anciens et expérimentés. Ils veulent créer un ver ou un virus capable d'infliger des dommages. Si leur travail détruit des fichiers, envoie à la corbeille des disques durs entiers et se propage par e-mail en infectant les systèmes informatiques de milliers de personnes qui ne se doutent de rien, ces individus se vantent alors avec fierté de leur réalisation. Lorsque le virus cause suffisamment de dégâts pour que la presse en parle et que les journaux télévisés relaient des avertissements à ce propos, c'est encore mieux.

On a beaucoup écrit sur les virus informatiques. Des livres et des programmes logiciels ont été rédigés, des entreprises se sont créées pour offrir des protections. Nous n'aborderons pas ici les défenses mises au point en fonction des techniques d'attaque. Nous nous intéressons moins aux actes destructeurs du petit voyou informatique qu'aux efforts plus ciblés de son lointain cousin, le manipulateur.

C'est arrivé par e-mail

Vous recevez certainement chaque jour des e-mails qui véhiculent des messages ou des offres gratuites dont vous n'avez ni besoin, ni envie. Vous connaissez le principe. On vous promet des conseils pour vos investissements, des réductions sur le prix des ordinateurs, télévisions, appareils photos ou voyages, on vous propose des cartes de crédit dont vous n'avez pas besoin, des conseils qui vous permettront de regarder gratuitement des chaînes de télévision payantes, des moyens d'améliorer votre santé ou votre vie sexuelle, etc.

De temps en temps, une offre destinée à retenir votre attention apparaît dans votre boîte aux lettres électronique. Il peut s'agir d'un jeu gratuit, d'une photo de votre star préférée, d'un programme de calendrier gratuit ou d'un shareware bon marché qui protégera votre ordinateur contre les virus. Quelle que soit l'offre, l'e-mail vous demande de télécharger le fichier qui contient le cadeau que le message vous a convaincu d'essayer.

Vous pouvez également recevoir un message dont l'objet indique "Sam, tu me manques" ou "Sophie, pourquoi ne m'as-tu pas écrit ?", ou encore "Salut, Tom, voici la photo sexy que je t'ai promise". Il ne peut pas s'agir d'un courrier publicitaire de pacotille, pensez-vous, car mon nom y figure et il est si personnel… Alors vous ouvrez le fichier joint pour voir la photo ou lire le message.

Toutes ces actions — télécharger un logiciel dont vous avez eu connaissance *via* un e-mail publicitaire, cliquer sur un lien qui vous mène à un site dont vous n'avez jamais entendu parler, ouvrir un fichier joint provenant d'un inconnu — sont susceptibles de vous donner bien des soucis. Bien sûr, le plus souvent, vous avez exactement ce à quoi vous vous attendiez, ou au pire quelque chose de décevant ou de choquant, mais en tout cas inoffensif. Mais parfois, ce peut être l'œuvre d'une personne malintentionnée.

L'envoi de code malveillant sur votre ordinateur ne constitue qu'une petite partie de l'attaque. L'attaquant doit vous persuader de télécharger le fichier joint pour qu'elle réussisse.

Note

Un type de programme, baptisé *RAT* (*Remote Access Trojan*) dans le monde clandestin de l'informatique, fournit à l'attaquant un accès complet à votre ordinateur, exactement comme s'il était assis devant votre clavier !

Les formes les plus dommageables de code malveillant — les vers tels que Love Letter, Sir Cam, et Anna Kournikova, pour n'en citer que quelques-uns — reposent toutes sur des techniques de duperie et exploitent, pour se propager, le désir qu'ont les personnes d'obtenir quelque chose gratuitement. Le ver arrive sous forme de fichier joint à un e-mail, qui propose quelque chose d'alléchant, comme une information confidentielle ou l'accès gratuit à des espaces pornographiques. Le message peut aussi indiquer — ruse particulièrement subtile — que le fichier joint est le reçu d'un élément coûteux que vous êtes supposé avoir commandé. Ce dernier stratagème vous conduit à l'ouvrir pour vérifier que votre carte de crédit n'a pas été débitée pour un article que vous n'avez pas commandé.

Il est étonnant de voir le nombre de personnes qui tombent dans ces pièges ; même en ayant été avertis maintes fois des dangers qu'il y a à ouvrir des fichiers joints aux e-mails, notre conscience du danger diminue avec le temps et nous expose à ce type de risque.

Repérer un logiciel malveillant

Un autre type de *malware* — abréviation de *malicious software*, logiciel malveillant — place sur votre ordinateur un programme qui fonctionne sans que vous en ayez connaissance ou que vous soyez d'accord, et qui effectue des

tâches à votre insu. Un malware peut paraître anodin : ce peut être un document Word ou une présentation PowerPoint, ou tout programme doté d'une fonctionnalité de macro, mais qui installera secrètement un programme interdit. Par exemple, il peut s'agir d'une version du cheval de Troie décrit au Chapitre 6. Une fois installé sur votre machine, ce logiciel peut indiquer à l'attaquant toutes les touches du clavier sur lesquelles vous appuyez et lui fournir vos mots de passe et vos numéros de cartes de crédit.

Deux autres types de logiciels malveillants sont également terribles. Le premier peut transmettre à l'attaquant chaque mot que vous prononcez devant votre micro, *même lorsque vous croyez que celui-ci est coupé*. Pire, un attaquant peut utiliser une variante de cette technique si votre ordinateur est équipé d'une Webcam : il pourra voir tout ce qui se trouve devant votre terminal, même lorsque vous pensez que la caméra est éteinte, de jour comme de nuit.

Jargon

Malware
Terme argotique qui désigne un logiciel ou un programme informatique malveillant, comme un virus, un ver ou un cheval de Troie, dont les actions sont dommageables.

Le message de Mitnick

Méfiez-vous des individus qui offrent des cadeaux, sinon votre entreprise pourrait connaître le même sort que la cité de Troie. En cas de doute, pour éviter une infection, protégez votre ordinateur.

Un hacker doté d'un sens de l'humour particulier et malicieux peut essayer de déposer sur votre ordinateur un petit programme qui peut méchamment vous empoisonner la vie. Par exemple, il peut faire en sorte que votre lecteur de CD n'arrête pas de s'ouvrir, ou que la fenêtre sur laquelle vous travaillez soit constamment réduite, ou qu'un fichier audio émette un cri perçant à plein volume au milieu de la nuit. Rien de plus drôle quand vous essayez de dormir ou de terminer un travail… Mais au moins, ce type de programmes ne créent aucun dommage permanent.

MESSAGE D'UN AMI

Les scénarios peuvent se révéler pires encore, même si vous prenez des précautions. Imaginez : vous avez décidé de ne plus prendre de risque. Vous ne téléchargez plus de fichiers sauf s'ils proviennent de sites sûrs que vous connaissez et auxquels vous faites confiance (Amazon par exemple). Vous ne cliquez plus sur des liens ou des e-mails de provenance inconnue. Vous n'ouvrez plus les fichiers joints d'e-mails que vous n'attendiez pas. Et vous vérifiez que la page Web qui s'affiche possède bien le symbole d'un site sécurisé lorsque vous faites des achats en ligne ou que vous échangez des informations confidentielles.

Puis un jour, vous recevez un e-mail d'un ami ou d'une collègue, qui contient un fichier joint. Il ne peut donc rien contenir de malveillant puisqu'il provient de quelqu'un que vous connaissez bien. Et ce, d'autant plus que vous sauriez qui accuser si les données de votre ordinateur venaient à être endommagées.

Vous ouvrez le fichier joint et… BOUM ! Vous voilà avec un ver ou un cheval de Troie. Pour quelle raison une personne que vous connaissez vous ferait-elle cela ? En fait, les apparences sont trompeuses. Vous connaissez l'histoire : le ver s'introduit dans l'ordinateur, puis se propage par e-mail à toutes les personnes qui figurent dans le répertoire d'adresses. Par conséquent, chacune de ces personnes reçoit un courrier de quelqu'un qu'elle connaît et ne se méfie pas, alors que chaque e-mail contient le ver, qui peut ensuite se propager, comme le ricochet d'une pierre sur un étang immobile.

Si cette technique est si efficace, c'est qu'elle fait "d'une pierre deux coups" : non seulement elle se propage pour infecter d'autres victimes non méfiantes, mais en outre on pense qu'elle provient d'une personne de confiance.

Le message de Mitnick

L'homme a inventé quantité de choses merveilleuses qui ont changé nos modes de vie et le monde. Mais si la technologie — qu'il s'agisse de l'ordinateur, du téléphone ou d'Internet — est utile aux personnes bienveillantes, il se trouvera toujours des individus malveillants qui en détourneront l'usage.

Triste réalité que le contexte technologique que nous connaissons : même si l'on reçoit un e-mail d'un proche, on peut encore se demander s'il est prudent de l'ouvrir !

VARIATIONS SUR UN THÈME

Il existe un type de fraude qui consiste à vous diriger sur un site Web autre que celui que vous escomptiez. Cela se produit régulièrement, sous des formes différentes. L'arnaque suivante, qui a réellement eu lieu sur Internet, en est un exemple représentatif.

Joyeux Noël...

Un retraité nommé Edgar, qui était représentant en assurances, reçoit un jour un e-mail de PayPal, une entreprise proposant un moyen commode et rapide d'effectuer des paiements en ligne. Ce type de services est particulièrement pratique lorsqu'une personne située dans un pays quelconque, quel que soit le pays ou le continent, achète un article à un individu qu'elle ne connaît pas. PayPal débite la carte de crédit de l'acheteur et vire l'argent directement sur le compte du vendeur.

En tant que collectionneur de poteries anciennes, Edgar fait beaucoup d'affaires par l'intermédiaire de l'entreprise de ventes aux enchères en ligne eBay. Il utilise souvent PayPal, et il arrive que ce soit plusieurs fois par semaine. Il est donc intéressé lorsqu'il reçoit un e-mail qui semble provenir de PayPal et lui offre une récompense pour la mise à jour de son compte PayPal. Voici ce que dit le message :

> Cher client de PayPal, nous vous souhaitons de bonnes fêtes de fin d'année ;
>
> Alors que la nouvelle année approche et que nous nous y préparons tous, PayPal aimerait, en guise de cadeau, créditer votre compte de 5 dollars !
>
> Pour recevoir ces 5 dollars, il vous suffit de mettre à jour les données vous concernant sur notre site PayPal sécurisé. Toute année apporte son lot de changements ; en actualisant vos informations chez nous, vous nous permettrez de continuer à offrir, à vous et à notre estimé service clients, un excellent service, tout en gardant nos renseignements à jour !
>
> Pour mettre à jour maintenant les données qui vous concernent et recevoir instantanément 5 dollars sur votre compte PayPal, cliquez sur le lien suivant :
>
> http://www.paypal-secure.com/cgi-bin
>
> Merci d'utiliser Paypal.com et de nous aider à croître et à devenir les premiers de notre catégorie !
>
> Nous vous souhaitons un joyeux Noël et une très bonne nouvelle année !
>
> L'équipe de PayPal.

À propos des sites Web de commerce électronique

Vous connaissez sans doute des gens peu disposés à effectuer des achats en ligne, même auprès d'entreprises largement connues comme Amazon et eBay, ou de sites Web tels que Nike. Dans un sens, ils ont raison de se méfier. Si votre navigateur utilise le standard actuel de cryptage sur 128 bits, les informations que vous donnez sur un site sécurisé sortent cryptées de votre ordinateur. Avec beaucoup d'efforts, ces données pourraient effectivement être décryptées, mais elles ne sont certainement pas cassables en un temps acceptable, sauf peut-être par la NSA (*National Security Agency*, l'agence américaine chargée d'intercepter les communications), qui, à notre connaissance, n'est pas intéressée par le vol de numéros de cartes de crédit, ni par le fait de savoir qui commande des cassettes vidéo pornographiques ou des sous-vêtements sexy.

Ces fichiers cryptés pourraient assurément être cassés par quiconque dispose du temps et des ressources nécessaires. Mais en réalité, il faudrait être fou pour déployer tous ces efforts afin de dérober *un seul* numéro de carte de crédit lorsque de nombreuses entreprises spécialisées dans le commerce électronique commettent l'erreur de stocker les données financières non cryptées de tous leurs clients dans leur base de données ! Et il y a pire : un certain nombre de ces entreprises utilisent un logiciel de base de données SQL spécifique et elles n'ont jamais changé le mot de passe par défaut de l'administrateur système. Lorsqu'elles ont installé le logiciel, le mot de passe était "null", et c'est toujours "null" aujourd'hui. Par conséquent, le contenu de la base de données se trouve à la disposition de quiconque, sur Internet, décide de se connecter au serveur d'une telle entreprise. Ces sites sont sans cesse attaqués et des informations leur sont dérobées, à l'insu de tout le monde.

Par ailleurs, ces mêmes personnes qui ne veulent pas faire d'achats sur Internet de crainte qu'on utilise les données de leur carte de crédit n'éprouvent aucune réticence à se servir de leur carte dans un magasin, ou pour régler un déjeuner, un dîner ou autre — même dans un bar ou un restaurant situés dans un quartier malfamé où elles n'emmèneraient pas leur mère !

Des reçus de carte de crédit sont continuellement volés ou récupérés au milieu des détritus alors qu'ils ont pourtant été jetés à la poubelle. Et de nombreux vendeurs ou maîtres d'hôtel indélicats peuvent noter votre nom et les renseignements concernant votre carte de crédit, ou utiliser un gadget que l'on trouve facilement sur Internet : un périphérique qui permet d'extorquer et de stocker les données de n'importe quelle carte de crédit et les utiliser ultérieurement.

Les achats en ligne présentent quelques risques, mais pas plus que ceux qui sont réalisés dans les petites boutiques. Aux États-Unis, les sociétés de cartes de crédit vous offrent la même protection lorsque vous utilisez votre carte en ligne (par exemple, si des frais sont débités de votre compte à la suite d'une fraude, vous n'êtes redevable que des 50 premiers dollars).

Par conséquent, selon moi, la crainte de régler des achats en ligne est injustifiée.

Edgar ne remarque aucun des signes qui révèlent que quelque chose ne colle pas dans cet e-mail (par exemple, le point-virgule qui termine la première ligne et la mauvaise formulation "à notre estimé service clients, un excellent service"). Il clique sur le lien, saisit les renseignements demandés — nom, adresse, numéro de téléphone, informations sur la carte de crédit — puis attend que le crédit de cinq dollars apparaisse sur son prochain relevé de carte de crédit. Mais au lieu de cela, il voit apparaître toute une liste de frais concernant des articles qu'il n'a jamais achetés.

Analyse de l'arnaque

Edgar s'est fait avoir par une arnaque courante sur Internet, et qui se présente sous diverses formes. Une autre arnaque de ce type (voir Chapitre 9) fait appel à un faux écran de connexion, créé par l'attaquant et identique à l'écran réel. La différence est que le faux écran ne donne pas accès au système informatique que l'utilisateur essaie d'atteindre, mais fournit le nom d'utilisateur et le mot de passe au hacker.

Dans l'arnaque dont a été victime Edgar, les escrocs ont créé un site Web baptisé "paypal-secure.com", qui semble être une page sécurisée du site officiel de PayPal, mais qui n'en est pas une. Lorsque Edgar a saisi les renseignements sur ce site, les attaquants ont obtenu exactement ce qu'ils voulaient.

Le message de Mitnick

Chaque fois que vous visitez un site qui vous demande des renseignements que vous considérez comme privés, vérifiez systématiquement que la connexion est authentifiée et cryptée, même si cela ne suffit pas toujours (aucun système de sécurité n'est parfait). Plus important encore : ne cliquez jamais automatiquement sur Oui dans une boîte de dialogue qui signale un problème de sécurité (par exemple un certificat numérique invalide, venu à expiration ou révoqué).

VARIATIONS SUR LA VARIATION

Combien existe-t-il de façons d'abuser les internautes afin de les conduire sur un faux site Web et de les amener à fournir des informations confidentielles ? À mon avis, personne ne peut fournir une réponse exacte, mais on ne se trompera pas en disant qu'il en existe "des tas et des tas".

Le lien manquant

Une ruse courante consiste à envoyer un e-mail proposant une bonne raison de visiter un site et qui fournit un lien pour s'y rendre directement. Sauf que le lien ne vous conduit pas au site indiqué : il ressemble juste au lien qui mène réellement à ce site. Voici un autre exemple d'une astuce qui a effectivement été employée sur Internet et qui implique, elle aussi, l'utilisation détournée du nom PayPal :

```
www.PayPai.com
```

À première vue, cela semble bien désigner PayPal. Même si la victime le remarque, elle pensera qu'il s'agit d'un léger défaut qui fait que le "l" de Pal ressemble à un "i". Et qui remarquerait au premier coup d'œil que dans :

```
www.PayPal.com
```

Le chiffre 1 est mis à la place de la lettre "l". Il y aura toujours trop de gens qui ne feront pas attention aux fautes d'orthographe ou à d'autres indications erronées. Lorsque ces personnes se rendent sur le faux site, comme il ressemble à celui qu'elles connaissent, elles saisissent allègrement les données de leur carte de crédit. Pour mettre en place une telle arnaque, un attaquant a seulement besoin d'enregistrer le nom de domaine factice, d'envoyer des e-mails et d'attendre que les "candides" se manifestent, prêts à être escroqués.

Au milieu de l'année 2002, j'ai reçu un e-mail qui, apparemment, faisait partie d'un mailing et provenait de "Ebay@ebay.com". Ce message est présenté dans la figure ci-après.

msg : Cher utilisateur eBay,

Il apparaît très clairement qu'un tiers a corrompu votre compte eBay et a violé les règles de notre convention d'utilisation concernant les enchères et achats :

4. Enchères et achats

Vous êtes tenu d'exécuter la transaction avec le vendeur si vous achetez un article par l'intermédiaire de nos formats de prix fixés ou êtes le dernier enchérisseur tel que décrit ci-après. Si vous êtes le dernier enchérisseur (tant que l'enchère minimum applicable ou les obligations de réserve sont respectées) et si votre enchère est acceptée par le vendeur, vous êtes tenu d'effectuer la transaction avec le vendeur, sinon la transaction est interdite par la loi ou par la présente convention.

Vous avez reçu cette notification d'eBay parce qu'il a été porté à notre attention que votre compte actuel a interrompu des enchères avec d'autres membres eBay et eBay demande une vérification immédiate de votre compte. Si vous ne le faites pas, celui-ci deviendra invalide.
Cliquez ici pour vérifier votre compte : http://error_ebay.tripod.com.

****

Les marques citées appartiennent à leurs propriétaires respectifs.
eBay et le logo eBay sont des marques de eBay Inc.

Les victimes qui cliquaient sur ce lien arrivaient sur une page Web qui ressemblait vraiment à une page eBay. La page était bien conçue, on y trouvait un authentique logo eBay, les rubriques "Acheter" et "Vendre", ainsi que d'autres liens de navigation qui conduisaient le visiteur au site eBay réel. Un logo de sécurité était également présent au coin inférieur droit de la page. Afin de décourager des victimes éventuellement méfiantes, le concepteur avait même employé un cryptage HTML pour cacher la destination des informations fournies par l'utilisateur.

Il s'agit d'un excellent exemple d'attaque par manipulation reposant sur l'informatique. Et encore, il n'est pas sans défaut.

Le texte du courrier n'est pas bien écrit : notamment, le paragraphe qui commence par "Vous avez reçu cette notification" est maladroit (les responsables de ces canulars ne louent jamais les services d'un professionnel pour rédiger leurs textes, et cela se voit toujours). De même, quiconque prêtait attention aurait eu des soupçons car eBay demandait au visiteur des informations concernant PayPal ; il n'y avait aucune raison pour qu'eBay demande à un client des données personnelles concernant une autre entreprise.

Et quiconque connaissait bien Internet aurait certainement vu que l'hyperlien renvoyait non pas au domaine d'eBay mais à tripod.com, qui est un service d'hébergement Web gratuit. Cela en disait long quant à l'illégitimité de l'e-mail. Néanmoins, je parie que de nombreuses personnes ont saisi sur cette page les informations qui leur étaient demandées, y compris leur numéro de carte de crédit.

Note

Pourquoi est-on autorisé à enregistrer des noms de domaine qui peuvent abuser les gens ou prêter à confusion ? Parce que d'après la législation et les règlements actuels qui concernent Internet, tout le monde a le droit d'enregistrer n'importe quel nom de site tant que celui-ci n'est pas déjà employé.
Les entreprises essaient de lutter contre l'utilisation de ce type d'adresses, mais imaginez contre quoi elles se battent ! General Motors a ainsi intenté un procès à une entreprise qui avait enregistré le nom "fuckgeneralmotors.com" et qui faisait pointer l'URL sur le site Web de General Motors. Mais General Motors a perdu.

Vigilance !

En tant qu'internaute, nous nous devons d'être vigilants, et de décider en toute conscience des circonstances dans lesquelles il est opportun de saisir des renseignements personnels, des mots de passe, numéros de compte, etc.

Combien de personnes de votre connaissance pourraient vous dire si la page Internet qu'elles sont en train de lire remplit les conditions qui font qu'une page est sécurisée ? Combien d'employés de votre entreprise savent ce à quoi il faut faire attention ?

Quiconque utilise Internet devrait connaître le petit symbole qui figure souvent sur les pages Web et représente un cadenas. Et savoir qu'un cadenas

fermé indique que le site a été certifié comme sécurisé. Lorsque le cadenas est ouvert ou qu'il est absent, cela signifie que le site Web n'est pas certifié authentique et que les informations ne sont pas cryptées.

Toutefois, un attaquant qui sait s'approprier des privilèges d'administrateur sur un ordinateur d'entreprise est également capable de modifier le code du système d'exploitation afin de duper l'utilisateur quant à sa perception de la réalité. Ainsi, pour contourner le problème du contrôle de certification, il est possible de modifier les instructions de programmation d'un navigateur qui indiquent que le certificat numérique d'un site Web est invalide. On peut aussi modifier le système avec ce que l'on appelle un *rootkit*[1], en installant une ou plusieurs *portes dérobées*, plus difficiles à détecter, au niveau du système d'exploitation.

Les connexions sécurisées certifient les sites comme authentiques et cryptent les informations qui sont diffusées, de sorte que les attaquants ne peuvent utiliser les informations qu'ils interceptent. Mais il se peut que le propriétaire du site sécurisé n'applique pas tous les patchs de sécurité nécessaires, ou qu'il n'oblige pas les utilisateurs ou les administrateurs à respecter les bonnes pratiques en matière de gestion des mots de passe. Par conséquent, on ne peut prétendre qu'un site apparemment sécurisé est invulnérable à une attaque.

Jargon

Porte dérobée (*backdoor*)
Point d'entrée caché qui fournit un passage secret pour pénétrer à l'intérieur de l'ordinateur d'un utilisateur, à l'insu de celui-ci. Les portes dérobées sont également utilisées par les programmeurs quand ils développent un logiciel : elles leur permettent d'accéder au programme pour corriger des problèmes.

Les protocoles HTTP (*HyperText Transfer Protocol*) et SSL (*Secure Socket Layer*) fournissent un système automatique qui utilise les certificats numériques non seulement pour crypter les informations transmises au site distant, mais aussi pour assurer une authentification (garantie que vous communiquez bien avec le site Web authentique). Cependant, ce système de protection ne fonctionne pas pour les utilisateurs qui ne vérifient pas avec soin si le nom du site affiché dans la barre d'adresse est bien celui auquel ils accèdent.

1. N.D.T. : Logiciel qui, en se substituant à des programmes système de la machine attaquée, permet à un attaquant de dissimuler ses activités. Le principe consiste à délivrer de fausses informations pour faire croire à l'utilisateur que tout va bien… Alors que l'attaquant contrôle le système !

Un autre aspect de la sécurité, auquel on prête rarement attention, est lié aux messages d'avertissement qui indiquent, par exemple : "Ce site n'est pas sûr ou le certificat de sécurité a expiré. Êtes-vous sûr de vouloir continuer ?" Nombre d'internautes ne comprennent pas ce message et, lorsqu'il apparaît, cliquent simplement sur OK ou Oui et poursuivent leur tâche, sans se douter qu'ils se trouvent peut-être sur des sables mouvants. Un homme averti en vaut deux : sur un site Web qui n'utilise pas de protocole sûr, vous ne devez jamais saisir de données confidentielles telles que votre adresse, votre numéro de téléphone, vos numéros de cartes de crédit ou de comptes bancaires, et toutes les informations que vous souhaitez garder privées.

Jargon

Secure Socket Layer
Protocole développé par Netscape, qui authentifie à la fois le client et le serveur dans une communication sécurisée sur Internet.

Thomas Jefferson a dit un jour que le maintien de notre liberté nécessitait une "vigilance éternelle". Il en va de même de notre sécurité et de la protection de notre vie privée, dans une société qui utilise l'information comme une valeur marchande.

Être bien informé sur les virus

Remarque particulière concernant les logiciels antivirus : ils sont essentiels pour l'intranet de l'entreprise, comme pour tout employé qui se sert d'un ordinateur. Non seulement les utilisateurs doivent avoir un logiciel antivirus installé sur leur machine, mais encore faut-il qu'il soit activé (ce qu'un grand nombre de personnes n'aiment pas car cela ralentit inévitablement certaines fonctions de l'ordinateur).

Pour utiliser au mieux les logiciels antivirus, il ne faut jamais oublier une procédure importante, qui consiste à mettre régulièrement à jour les définitions de virus. Si votre entreprise ne diffuse pas les logiciels ou les mises à jour par l'intermédiaire du réseau. Chaque utilisateur doit télécharger lui-même le dernier ensemble de définitions de virus. Selon moi, chacun devrait configurer son logiciel antivirus de sorte que les nouvelles définitions de virus soient automatiquement actualisées chaque jour.

Autrement dit, vous êtes vulnérable si les définitions de virus ne sont pas mises à jour régulièrement. Et même ainsi, vous n'êtes toujours pas à l'abri des vers ou des virus que les entreprises qui développent des antivirus ne connaissent pas encore ou pour lesquels elles n'ont pas encore publié de fichier de détection.

Tous les employés qui ont des privilèges d'accès à distance depuis leur portable ou leur ordinateur personnel doivent avoir au minimum un logiciel antivirus à jour et un pare-feu individuel sur leur machine. Tout attaquant chevronné recherchera le maillon le plus faible, et c'est par là qu'il attaquera. Il relève donc de la responsabilité de l'entreprise de rappeler régulièrement aux personnes équipées d'ordinateurs avec accès distant qu'elles doivent disposer d'un pare-feu personnel et d'un logiciel antivirus à jour et activé : on ne peut attendre de chaque ouvrier, directeur, vendeur ou employé qui travaille à distance qu'il ait toujours à l'esprit les dangers qu'il y a à laisser son ordinateur sans protection.

Outre ces procédures, je recommande vivement l'utilisation de logiciels moins courants, mais non moins importants, qui protègent des attaques des chevaux de Troie, à savoir les logiciels anti-cheval de Troie. Au moment où je rédige ce livre, les deux programmes les plus connus sont The Cleaner (www.moosoft.com) et Trojan Defence Suite (www.diamondcs.com.au).

En résumé, le principe de sécurité certainement le plus important pour les entreprises est celui-ci : comme nous avons tous tendance à nous montrer négligents avec ce qui semble accessoire pour la bonne réalisation de notre travail, ou à l'oublier, il est nécessaire de rappeler aux employés, et de façons diverses, qu'il ne faut pas qu'ils ouvrent de fichiers joints à des e-mails, à moins qu'ils soient certains que l'expéditeur est une personne ou une entreprise auxquelles ils peuvent faire confiance. La direction doit également rappeler à son personnel qu'il doit utiliser un logiciel antivirus et un logiciel anti-cheval de Troie, qui fournissent une réelle protection contre des e-mails apparemment inoffensifs mais qui sont susceptibles de contenir une charge destructrice.

Chapitre 8

Exploiter la compassion, la culpabilité et l'intimidation

Les manipulateurs utilisent l'influence pour amener leur cible à agir comme ils le souhaitent. Lorsqu'ils sont expérimentés, ils sont très habiles à mettre au point des ruses destinées à activer des sentiments comme la crainte, l'émotion ou la culpabilité. Ils utilisent pour cela des déclencheurs psychologiques, c'est-à-dire des mécanismes automatiques qui poussent les gens à satisfaire aux requêtes qui leur sont faites sans analyser de façon approfondie toutes les informations qui sont à leur disposition.

Nous souhaitons tous éviter les situations difficiles, pour nous comme pour les autres. En se servant de ce ressort, l'attaquant peut jouer sur la compassion d'une personne, culpabiliser sa victime ou utiliser l'intimidation comme une arme.

Nous verrons dans ce chapitre quelques tactiques courantes qui jouent sur les émotions.

UNE VISITE AU STUDIO

Avez-vous déjà remarqué comme certaines personnes peuvent s'approcher, par exemple, du gardien de l'entrée d'un hôtel où se déroule une réunion, une réception privée ou une dédicace de livres, et passer tout simplement devant lui sans qu'il leur demande leur billet ou leur invitation ?

De la même façon, un manipulateur peut s'introduire dans des lieux où cela paraît impossible. Vous allez le constater avec l'histoire suivante, qui se déroule dans le monde de l'industrie cinématographique.

L'appel téléphonique

"Bureau de Ron Hillyard, ici Dorothy."

"Bonjour Dorothy. Je m'appelle Kyle Bellamy. Je viens d'arriver pour travailler dans l'équipe d'Animation Development de Brian Glassman. Vous faites des choses bien différentes ici !"

"C'est possible. Je n'ai jamais travaillé dans un autre studio de cinéma, alors je ne sais pas vraiment. Que puis-je pour vous ?"

"Pour vous dire la vérité, je me sens un peu stupide. Un auteur vient me voir cet après-midi pour un lancement et je ne sais pas où m'adresser pour l'amener au studio. Les gens du bureau de Brian sont vraiment charmants, mais je déteste les ennuyer avec des "comment puis-je faire ceci, comment puis-je faire cela ?". C'est comme si j'avais ma première cuite et que je ne retrouve plus la salle de bains, vous voyez ce que je veux dire ?"

Dorothy rit.

"Vous voulez la sécurité. Composez le 7, puis 6138. Si vous obtenez Lauren, dites-lui que Dorothy lui demande de prendre bien soin de vous."

"Merci Dorothy. Et si je ne trouve pas les toilettes des hommes, je vous rappelle !"

À cette idée, elle rit avec lui, puis raccroche.

Le point de vue de David Harold

J'aime le cinéma et lorsque j'ai emménagé à Los Angeles, j'ai pensé que j'allais rencontrer toutes sortes de gens appartenant au milieu du cinéma et qu'ils allaient m'inviter à des réceptions et m'emmener déjeuner aux studios. Bon, je suis ici depuis un an, j'ai presque 26 ans et le mieux que j'aie pu faire, c'est visiter les studios Universal avec tous les braves touristes. Alors pour finir, je me dis que puisqu'ils ne veulent pas m'inviter, je vais m'inviter moi-même !

J'achète un exemplaire du *Los Angeles Times*, lis la page des spectacles pendant plusieurs jours et note les noms de certains producteurs de divers studios. Je décide d'essayer d'abord l'un des studios les plus importants.

J'appelle donc la standardiste et lui demande le bureau du producteur dont j'ai trouvé le nom dans le journal. La secrétaire qui répond paraît maternelle, et je me dis que j'ai de la chance ; s'il s'était agi d'une jeune fille dont la présence ici était uniquement motivée par l'espoir d'être remarquée, elle ne m'aurait même pas donné l'heure.

Mais cette Dorothy est du genre à recueillir les chats perdus, elle a l'air désolée pour ce jeune débutant qui semble écrasé par son nouvel emploi. C'est sûr, j'ai eu de la chance de tomber sur elle. Ce n'est pas tous les jours que la personne que vous essayez de duper vous donne plus que ce que vous demandez. En plus, compatissante, elle m'a non seulement donné le nom de l'un des employés de la sécurité, mais m'a également conseillé de me recommander d'elle auprès de la femme supposée m'aider.

Naturellement, j'avais de toute façon prévu d'utiliser le nom de Dorothy. Mais cela est encore mieux. Lauren ouvre immédiatement et ne se donne même pas la peine de vérifier si le nom que je lui donne figure dans la base de données des employés.

Lorsque j'arrive au portail, ce même après-midi, non seulement mon nom figure sur la liste des visiteurs, mais je dispose d'une place de parking. Je profite d'un long déjeuner puis me balade dans le studio jusqu'à la fin de la journée. Je vais même jeter un œil dans quelques studios d'enregistrement et assiste à des tournages. Je reste jusqu'à 19 heures. Voilà l'une de mes journées les plus passionnantes !

Analyse de l'arnaque

Tout le monde a un jour été un nouvel employé. Nous nous souvenons tous de ce qu'a été cette première journée, en particulier lorsque nous étions jeunes et inexpérimentés. Ainsi, lorsqu'un nouvel employé demande de l'aide, il peut escompter que de nombreuses personnes — notamment celles qui se trouvent au bas de l'échelle — se souviennent de leurs propres impressions de nouveaux venus et viennent au-devant de lui pour lui tendre la main. Le manipulateur le sait et comprend qu'il peut en user pour jouer sur la compassion de ses victimes.

Nous permettons trop facilement aux étrangers de se déplacer à leur guise dans les bâtiments et bureaux de notre entreprise. Même si l'on fait garder l'entrée et que l'on dispose de procédures d'enregistrement pour les visiteurs, un intrus peut utiliser de nombreuses variantes de la ruse que nous venons de voir pour obtenir un badge de visiteur et entrer. Et si votre entreprise demande que les visiteurs soient escortés ? Cette règle est excellente, mais n'est efficace que si vos employés se montrent vraiment consciencieux, qu'ils arrêtent et interrogent les personnes qui, avec ou sans badge de visiteur, se promènent seules. Et si leurs réponses ne sont pas satisfaisantes, vos employés doivent avoir le réflexe de contacter la sécurité.

Le fait que des étrangers puissent se déplacer si facilement dans vos établissements met en danger les informations sensibles de votre entreprise. Dans le

contexte actuel, vu les risques d'attaques terroristes qui planent sur notre société, ce sont bien plus que de simples informations qui peuvent être en danger.

"FAITES-LE TOUT DE SUITE !"

Tous les individus qui utilisent des tactiques de manipulation ne sont pas des manipulateurs distingués. Quiconque possède les connaissances d'un salarié d'une entreprise peut devenir dangereux. Et le risque est encore plus grand pour une entreprise qui conserve dans ses fichiers et ses bases de données les informations personnelles de ses employés, ce que font naturellement la plupart des entreprises.

Lorsque les employés n'ont pas reçu de formation pour reconnaître les attaques par manipulation, certaines personnes telles que la jeune femme abandonnée de l'histoire qui suit peuvent mener des actions que la plupart des gens honnêtes penseraient impossibles.

Le point de vue de Doug

De toute façon, les choses n'allaient pas si bien que cela avec Linda, et dès que j'ai rencontré Erin j'ai su qu'elle était faite pour moi. Linda est, comment dire, un petit peu… Euh, une personne pas exactement instable mais qui peut d'une certaine manière s'emporter lorsqu'elle est contrariée.

Je lui ai dit, aussi gentiment que j'ai pu, qu'elle devait déménager, je l'ai aidée à faire ses valises et ai même laissé prendre quelques CD qui m'appartenaient. Immédiatement après son départ, je suis allé dans un magasin d'outillage acheter un verrou pour ma porte d'entrée et l'ai posé le soir même. Le matin suivant, j'ai appelé l'opérateur téléphonique pour lui demander de changer mon numéro et de m'inscrire sur liste rouge. J'étais ainsi libre pour Erin.

Le point de vue de Linda

J'étais prête à partir de toute façon, simplement, je n'avais pas décidé du moment. Mais personne n'aime se sentir rejeté. Par conséquent, la question se résumait seulement à savoir ce que je pourrais faire pour qu'il comprenne quel crétin il était.

Il ne m'a pas fallu longtemps pour trouver. Il devait y avoir une autre fille, sinon il ne m'aurait pas demandé de faire mes bagages aussi rapidement. Alors j'attendrai un peu et commencerai à l'appeler tard le soir. Vous savez, à l'heure où on aime le moins être appelé.

J'ai attendu le week-end suivant et l'ai appelé vers 23 heures le samedi soir. Mais il avait changé de numéro de téléphone et le nouveau était sur liste rouge. Cela montre bien combien ce type est un salaud.

Mais ce n'était qu'un contre-temps. J'ai commencé à fouiller dans les papiers que j'avais réussi à rapporter chez moi juste avant de quitter mon travail, chez l'opérateur téléphonique. Et j'ai trouvé ce que je cherchais : Doug avait fait réparer la ligne téléphonique suite à un problème et j'avais conservé le reçu correspondant, qui indiquait le câble et la paire de son téléphone. Voyez-vous, vous pouvez modifier votre numéro de téléphone à votre guise, mais vous gardez toujours les mêmes fils entre votre domicile et le central téléphonique. Le jeu de fils en cuivre qui sort de chaque maison ou appartement est identifié par des numéros que l'on appelle "câble et paire". Et si vous savez comment procède l'opérateur et ce qu'il faut faire, il vous suffit de connaître le câble et la paire de la cible pour trouver son numéro de téléphone.

Je possédais la liste de tous les centraux téléphoniques de la ville, avec leurs adresses et numéros de téléphone. J'ai recherché le numéro du central situé à proximité de l'endroit où j'ai vécu avec cet idiot de Doug, et l'ai appelé. Naturellement, il n'y avait personne. Où est l'opérateur lorsque vous avez vraiment besoin de lui ? Il m'a fallu environ vingt secondes pour élaborer un plan. J'ai appelé d'autres centraux téléphoniques et finalement localisé un type. Mais il était à des kilomètres de là, probablement assis sur sa chaise avec les pieds sur le bureau. J'ai compris qu'il n'accepterait pas facilement de faire ce que je voulais. Mais mon plan était au point.

"Ici Linda, du centre de dépannage" ai-je dit. "Nous avons une urgence, le service d'une unité paramédicale est en panne. Un technicien essaie de réparer mais ne trouve pas le problème. Nous avons besoin que vous vous rendiez immédiatement au central téléphonique du Webster afin de vérifier s'ils ont une tonalité."

Puis je lui ai indiqué que je le rappellerais quand il y serait parce que, naturellement, je ne tenais pas à ce qu'il appelle le centre de dépannage et me demande.

Je savais qu'il n'aurait pas envie de quitter le confort du bureau central en plein hiver, de s'emmitoufler pour aller racler la glace de son pare-brise et conduire dans la neige à moitié fondue en pleine nuit. Mais comme il s'agissait d'une "urgence", il ne pouvait pas dire qu'il était trop occupé.

Lorsque je l'ai joint, quarante-cinq minutes plus tard, au central téléphonique du Webster, je lui ai dit de vérifier le "câble 29 paire 2481", ce qu'il a fait : "Oui, il y a une tonalité". Évidemment, je le savais déjà.

Je lui ai ensuite demandé de procéder à une LV, c'est-à-dire une vérification de ligne, à savoir identifier le numéro de téléphone. Il a appelé pour cela un numéro spécial qui indique le numéro à partir duquel on appelle. Il ne savait pas si le numéro était sur liste rouge ou récemment attribué ; il a donc fait ce que je lui demandais et j'ai entendu l'annonce du numéro sur son appareil de test. Merveilleux ! Tout avait fonctionné comme un charme.

"Bien, le problème doit être ailleurs, à l'extérieur", lui ai-je dit, puisque je connaissais maintenant le numéro. Je l'ai remercié et lui ai dit que nous continuerions à travailler dessus, puis je lui ai souhaité bonne nuit.

Le message de Mitnick

Dès qu'un manipulateur connaît le fonctionnement interne de l'entreprise ciblée, il lui est facile d'utiliser cette connaissance pour entretenir des rapports avec les employés. Les entreprises doivent se préparer aux attaques par manipulation provenant d'employés, anciens ou actuels, qui agissent pour un quelconque intérêt personnel. Des contrôles peuvent se révéler utiles pour se débarrasser des individus susceptibles d'adopter ce type de comportement. Mais le plus souvent, ces personnes sont extrêmement difficiles à repérer. La seule façon de se protéger correctement contre ce type de manipulation consiste à appliquer et à contrôler l'application des procédures de vérification des identités. Il faut notamment vérifier le statut de la personne avant de dévoiler quelque information que ce soit à quiconque n'est pas identifié comme faisant toujours partie de l'entreprise.

Et voilà pour ce Doug, qui essayait de se protéger de moi en se cachant derrière un numéro sur liste rouge ! La plaisanterie allait pouvoir commencer…

Analyse de l'arnaque

La jeune femme de cette histoire a pu obtenir les informations qu'elle voulait pour assouvir sa vengeance car elle connaissait le fonctionnement interne de l'opérateur téléphonique : les numéros de téléphone, les procédures et le jargon. Grâce à cela, elle a non seulement pu se procurer un numéro de téléphone récent sur liste rouge, mais elle l'a fait en outre au beau milieu de la nuit, en plein hiver, et en faisant traverser la ville à un dépanneur.

"UNE DEMANDE DE M. LE DIRECTEUR GÉNÉRAL"

Une forme d'intimidation très efficace, et répandue — essentiellement parce qu'elle est simple — consiste à influencer le comportement d'autrui en jouant sur l'autorité.

La seule évocation de "l'assistant du directeur général" peut être inestimable. Ainsi, les détectives privés, et même les chasseurs de tête, s'en servent tout le temps. Ils appellent la standardiste et indiquent qu'ils veulent être mis en relation avec le bureau du directeur général. À la secrétaire ou à l'assistante qui répond, ils disent qu'ils ont un document ou un paquet pour le directeur général. Ils peuvent aussi lui demander d'imprimer le fichier joint au mail qu'ils ont prévu d'envoyer. Ou encore quel est le numéro de fax ? Et au fait, quel est votre nom ?

Puis ils appellent la personne suivante : "Jeannie, du bureau du directeur général, m'a dit de vous appeler car vous pourriez m'aider."

Cette technique, qui consiste à "lâcher un nom", est habituellement utilisée pour établir rapidement des rapports en faisant en sorte que la cible croie que l'attaquant est en contact avec une personne hiérarchiquement importante. Une cible sera plus encline à accorder une faveur à quelqu'un qui fait référence à une personne qu'elle-même connaît.

Si l'attaquant a des vues sur une information très sensible, il peut utiliser ce type d'approche afin d'éveiller chez la victime des émotions exploitables, comme la peur d'avoir des ennuis avec ses supérieurs.

En voici un exemple.

L'histoire de Scott

"Scott Abrams à l'appareil."

"Scott, ici Christopher Dalbridge. Juste avant, j'étais en communication avec Monsieur Biggley et il est plutôt mécontent. Il dit qu'il a envoyé une note, il y a dix jours, indiquant que votre personnel devait nous faire parvenir des copies de toutes vos recherches concernant la pénétration du marché, afin que nous les analysions. Nous n'avons toujours rien reçu."

"Des recherches sur la pénétration du marché ? Personne ne m'en a parlé. Dans quel service êtes-vous ?"

"Nous sommes une entreprise de consultants dont il loue les services, et nous sommes déjà en retard."

"Écoutez, je suis en route pour une réunion. Donnez-moi votre numéro de téléphone et…"

À présent, l'attaquant ne paraît pas loin d'être excédé :

"C'est cela que vous voulez que je dise à Monsieur Biggley ?! Écoutez, il attend notre analyse demain matin et nous devons travailler dessus cette nuit. Maintenant, voulez-vous que *je* lui dise que nous ne pouvons pas parce que nous n'avons pas reçu votre rapport, ou voulez-vous le lui dire vous-même ?"

Un directeur général en colère, ça peut vous ruiner la semaine. La cible commence à penser qu'elle ferait mieux de s'en préoccuper avant d'aller à cette réunion. Une fois encore, le manipulateur a appuyé sur le bon bouton pour obtenir le résultat qu'il voulait.

Analyse de l'arnaque

Le procédé qui vise à intimider la cible en faisant référence à la hiérarchie fonctionne particulièrement bien auprès des employés qui occupent des postes relativement bas dans l'entreprise. Le fait d'utiliser le nom d'une personne importante non seulement efface la suspicion, mais incite également souvent l'employé à faire son possible pour rendre service : la tendance naturelle de tout un chacun à se rendre utile est décuplée lorsqu'on pense que la personne que l'on aide est importante ou influente.

Toutefois, le manipulateur sait qu'il est préférable, dans ce type de supercherie, d'utiliser le nom d'un supérieur hiérarchique plutôt que celui du patron. Mais cela est délicat à mettre en œuvre dans les petites entreprises : l'attaquant ne veut pas que sa victime en parle, par hasard, au responsable du marketing. "J'ai transmis le plan marketing du produit au type auquel vous avez demandé de m'appeler" peut trop facilement produire une réponse comme : "Quel plan marketing ? Quel type ?" Et cela pourrait mener l'entreprise à découvrir qu'elle est victime d'une manipulation.

Le message de Mitnick

L'intimidation peut créer la peur d'une punition, ce qui pousse les gens à coopérer. L'intimidation peut également faire naître la peur d'avoir des ennuis ou de voir disparaître une bonne occasion de recevoir une nouvelle promotion.

Les gens doivent savoir non seulement qu'on accepte, mais également qu'on attend d'eux qu'ils remettent l'autorité en question lorsque la sécurité est en jeu. Les formations dispensées en matière de sécurité des informations doivent inclure un enseignement sur la façon de contester l'autorité avec courtoisie, sans que les relations inter-personnelles en pâtissent. En outre, cela doit être soutenu à tous les niveaux hiérarchiques. Si un employé n'a pas de soutien lorsqu'il remet la légitimité de personnes en question, quel que soit leur statut, la réaction normale est de ne plus agir de la sorte ; or, c'est exactement l'inverse de ce qui est attendu.

CE QUE LA SÉCURITÉ SOCIALE SAIT DE VOUS

Nous aimons croire que les pouvoirs publics qui possèdent des fichiers nous concernant gardent ces informations soigneusement à l'abri des personnes qui n'ont pas besoin de les connaître. La réalité est que même le gouvernement fédéral des États-Unis n'est pas à l'abri des intrusions.

L'appel téléphonique de May Linn

Heure : 10 h 18, jeudi matin.

Lieu : un bureau de la Sécurité sociale.

"May Linn Wang à l'appareil."

La voix à l'autre bout du fil semble contrite, presque timide.

"Mademoiselle Wang, ici Arthur Arondale, du bureau de l'Inspecteur Général. Nous avons ici un nouvel employé qui ne dispose pas encore d'ordinateur, donc il utilise le mien car il a un projet urgent. Nom d'une pipe, nous faisons partie de l'administration des États-Unis, et on nous dit que notre budget ne permet pas d'acheter un ordinateur à cet employé ! Et maintenant, mon responsable voit que je prends du retard dans mon travail et ne veut rien entendre !"

"Je vois parfaitement ce que vous voulez dire."

"Pourriez-vous me rendre service en faisant une petite recherche, sur MCS, à ma place ?" demande-t-il, en utilisant le nom du système informatique qui permet de rechercher des renseignements sur les contribuables.

"Bien sûr, de quoi s'agit-il ?"

"La première chose dont j'ai besoin est que vous fassiez un *alphadent* sur Joseph Johnson, né le 4 avril 1969." (Cela signifie que l'ordinateur fait une recherche alphabétique à partir du nom du contribuable, identifié en outre par sa date de naissance.)

Après une petite pause, elle demande :

"Que voulez-vous savoir ?"

"Quel est son numéro de dossier ?" demande-t-il, en utilisant le raccourci dont se servent les initiés pour désigner le numéro de sécurité sociale. Elle le lui lit.

"Très bien, pouvez-vous effectuer une identification numérique sur ce dossier ?", dit-il.

Cela signifie qu'elle doit lui lire les renseignements concernant le contribuable ; May Linn lui indique donc le lieu de naissance, le nom de jeune fille de la mère et le nom du père du contribuable. Le manipulateur écoute patiemment pendant qu'elle lui donne également le mois et l'année d'émission de la carte ainsi que le bureau qui l'a émise.

Il souhaite ensuite qu'elle fasse un DEQY — prononcer "DECK-oui" (abréviation de *detailed earnings query*, demande de revenus détaillée).

"Pour quelle année ?", demande-t-elle. "L'année 2001."

May Linn annonce alors : "La somme est de 190 286 dollars, le payeur est Johnson MicroTech."

"Autres revenus ?"

"Non."

"Merci", dit-il. "Vous êtes très aimable".

Puis il essaie de convenir qu'à chaque fois qu'il aura besoin d'informations et qu'il ne pourra pas se servir de son ordinateur, il fera appel à ses services. Il s'agit là encore de l'astuce préférée des manipulateurs, qui consiste toujours à tenter d'établir de bons rapports avec une personne, pour éviter de devoir trouver une nouvelle cible à chaque appel.

"Pas la semaine prochaine" lui dit-elle,"car je dois assister au mariage de ma sœur, mais une autre fois, je ferai ce que je pourrai."

L'histoire de Keith Carter

Si l'on en juge par les films et les romans policiers à succès, les détectives privés prennent des libertés avec la morale et en savent long sur la façon de découvrir des détails croustillants sur la vie des gens. Ils utilisent pour cela des méthodes parfaitement illégales tout en s'arrangeant comme ils peuvent pour ne pas être arrêtés. Dans la réalité, naturellement, la plupart des détectives privés exercent des activités parfaitement légales. Dans la mesure où nombre d'entre eux, aux États-Unis, ont commencé leur vie professionnelle comme officiers assermentés de l'ordre public, ils savent très bien ce qui est légal et ce qui ne l'est pas, et la plupart ne sont pas tentés de franchir la frontière.

Il existe cependant des exceptions. En effet, certains détectives — et il y en a plus d'un — collent assez bien au moule des types que l'on trouve dans les histoires criminelles. Ces types savent qu'ils peuvent exécuter beaucoup plus facilement et rapidement une mission en prenant quelques raccourcis. Que ces raccourcis se trouvent être des félonies potentielles qui peuvent les conduire derrière les barreaux pour quelques années ne semble pas dissuader les moins scrupuleux.

En général, les détectives les plus renommés — ceux qui travaillent dans de jolies suites de bureaux loués dans les beaux quartiers — ne font pas ce type de travail eux-mêmes. Ils se contentent d'employer un intermédiaire qui le fera à leur place.

L'homme que nous appellerons Keith Carter fait partie des privés qui ne s'embarrassent pas de morale.

Il s'agit d'un cas typique, du genre "où cache-t-il l'argent ?" Parfois, d'ailleurs, c'est aussi "où cache-t-elle l'argent ?". Bref, une riche dame veut savoir où son mari a caché son argent. (Pour quelle raison une femme riche se marie-t-elle avec un type pauvre ? C'est une question que Keith Carter se pose de temps en temps, mais à laquelle il n'a jamais trouvé de réponse satisfaisante.)

Ici, c'est le mari, Joe Johnson, qui garde l'argent bien au chaud. C'est un homme brillant, qui a lancé, avec dix mille dollars empruntés à la famille de son épouse, une SSII dont il a fait une entreprise qui vaut à présent cent millions de dollars. D'après l'avocat qui défend la femme dans le divorce, l'époux aurait énormément œuvré pour dissimuler ses avoirs et l'avocat en veut un état détaillé et complet.

Keith pense qu'il faut commencer par voir du côté de la Sécurité sociale. Les dossiers sur Johnson devraient révéler des informations extrêmement utiles dans une telle situation. Grâce à ces informations, Keith se ferait passer pour sa cible et obtiendrait des banques, des maisons de courtage et des institutions offshore qu'elles lui révèlent tout.

Il passe son premier appel téléphonique à un bureau local de la Sécurité sociale[1], en composant le 800, numéro indiqué dans le bottin local et que tout un chacun peut utiliser.

Un employé prend l'appel et Keith lui demande de le mettre en relation avec le service des réclamations. Une autre attente, puis une voix. À présent, Keith passe la vitesse supérieure : "Bonjour, commence-t-il, ici Gregory Adams, du bureau 329. Voilà, j'essaie de joindre la personne des réclamations qui gère un numéro de dossier se terminant par 6363, mais le numéro que j'ai est celui d'un fax."

Son correspondant recherche le numéro et le donne à Keith.

1. N.D.T. : L'équivalent d'une Caisse Primaire d'Assurance Maladie.

Lorsque May Linn répond, Keith change de casquette et reprend le baratin habituel : il prétend appartenir au bureau de l'Inspecteur Général et explique son problème (un autre employé qui monopolise son ordinateur). Elle lui donne l'information qu'il cherche et promet de faire ce qu'elle pourra lorsqu'il aura besoin d'aide à l'avenir.

Analyse de l'arnaque

Le manipulateur a rendu son approche efficace en se servant de la compassion de l'employée, en racontant que son collègue utilise son ordinateur et que son patron "n'est pas très content" de lui. Comme les gens montrent rarement leurs émotions au travail, lorsqu'ils le font, cela peut totalement retourner leurs défenses ordinaires. Le stratagème émotionnel que l'on peut résumer par "J'ai un problème, voulez-vous m'aider ?" lui a suffi pour obtenir ce qu'il voulait.

Note

Insécurité sociale

Aussi incroyable que cela puisse paraître, la Sécurité sociale américaine a mis sur le Web des informations qui sont utiles pour son personnel, mais également d'une valeur inestimable pour les manipulateurs. On y trouve les abréviations et le jargon employés, ainsi que des instructions sur la façon de formuler des demandes, comme nous l'avons vu dans notre histoire.

Vous voulez en savoir plus sur la Sécurité sociale des États-Unis ? Il suffit de faire une simple recherche sur Google de ou saisir l'adresse suivante dans votre navigateur : http://policy.ssa.gov/poms.nsf. Si l'administration n'a pas encore lu cette histoire et supprimé le manuel, vous trouverez des instructions en ligne qui fournissent même des informations détaillées sur les données qu'un employé de la Sécurité sociale est autorisé à communiquer à l'ensemble des représentants de l'ordre. Cette communauté peut évidemment comprendre n'importe quel manipulateur capable de convaincre un employé de la Sécurité sociale qu'il appartient aux pouvoirs publics ou à l'administration.

L'attaquant n'aurait pas réussi à obtenir ces informations auprès de l'un des employés qui traitent les appels téléphoniques du public. Le type d'attaque utilisé par Keith ne fonctionne que lorsque le numéro de la personne qui reçoit l'appel n'est pas disponible au public, ce qui laisse supposer que la personne qui appelle ne peut être que de la maison — autre exemple de sécurité clandestine.

Voici les éléments qui ont facilité cette attaque :

- La connaissance du numéro de téléphone.
- La connaissance de la terminologie utilisée — alphadent et DEQY.
- Le fait d'affirmer faire partie du bureau de l'Inspecteur Général. Tout fonctionnaire américain sait qu'il s'agit d'une agence d'investigations gouvernementale dotée de larges pouvoirs. Cela donne à l'attaquant une aura d'autorité.

Autre considération intéressante : les manipulateurs semblent savoir formuler leurs requêtes de sorte que personne ne se demande "Pourquoi est-ce *moi* qu'il appelle ?", même lorsque, logiquement, il aurait été plus sensé que l'appel soit destiné à une autre personne d'un tout autre service. Le fait d'aider l'appelant permet peut-être de briser la monotonie quotidienne au point que la victime en oublie le caractère inhabituel de l'appel.

Enfin, dans cette histoire, l'attaquant voulait non seulement obtenir des informations concernant le cas en cours, mais également s'assurer d'avoir un contact qu'il pourrait rappeler régulièrement. Sinon, il aurait pu utiliser un autre stratagème courant de l'attaque qui exploite la compassion : "J'ai renversé du café sur mon clavier". Cela n'aurait pas fonctionné ici, car un clavier peut être remplacé dans la journée. À la place, il a imaginé qu'une personne se servait de son ordinateur, histoire qu'il pouvait ressortir raisonnablement pendant plusieurs semaines : "Hé, je pensais qu'il aurait son propre ordinateur hier, il y en a un qui vient d'arriver, mais c'est un autre employé qui l'a obtenu. Ainsi, cet individu vient toujours", etc.

UN SIMPLE APPEL

L'une des principales difficultés pour un attaquant consiste à faire en sorte que sa requête paraisse *raisonnable*, qu'il s'agisse d'une requête classique parmi celles que reçoit la victime pendant sa journée de travail, quelque chose qui ne dérange pas trop. Et de même que bien d'autres aspects dans la vie, cela peut relever du défi un jour, mais être du gâteau le lendemain.

L'appel téléphonique de Mary H.

Date et heure : lundi 23 novembre, 7h49.

Lieu : Mauersby & Storch Comptabilité, New York.

Pour la plupart des gens, la comptabilité consiste à effectuer des calculs. Heureusement, tout le monde ne voit pas ce travail de cette façon. Ainsi, Mary Harris trouve son travail de chef comptable passionnant, et c'est l'une des raisons pour lesquelles

elle est l'une des employées les plus impliquées du service comptabilité de son entreprise.

Ce lundi, Mary arrive de bonne heure pour prendre de l'avance sur une journée qui s'annonce longue, et elle est surprise d'entendre son téléphone sonner. Elle décroche et donne son nom.

"Bonjour, ici Peter Sheppard. Je suis d'Arbuckle Support, l'entreprise chargée de l'assistance technique de votre société. Nous avons reçu plusieurs plaintes, pendant le week-end, de personnes ayant eu des problèmes avec des ordinateurs. Je pensais procéder au dépannage ce matin, avant l'arrivée du personnel. Avez-vous eu des problèmes avec votre ordinateur ou en vous connectant au réseau ?"

Elle lui répond qu'elle ne sait pas encore. Elle allume son ordinateur et pendant qu'il démarre, Peter explique ce qu'il attend d'elle.

"J'aimerais faire quelques tests avec vous. Je peux voir sur mon écran les touches que vous tapez au clavier et je veux m'assurer que cela circule correctement sur le réseau. Par conséquent, à chaque fois que vous appuierez sur une touche, je veux que vous me disiez laquelle et je verrai si la même lettre ou le même chiffre apparaît bien ici. D'accord ?"

Devant l'évocation cauchemardesque de son ordinateur en panne et d'une journée frustrante qui lui interdirait le moindre travail, elle est plus que contente que cet homme lui apporte de l'aide. Après quelques instants, elle annonce : "Je suis devant l'écran de connexion et je vais saisir mon nom d'utilisateur ; je le tape maintenant, M...A...R...Y...D".

"Jusque-là, c'est parfait", dit-il. "Je vois cela ici. À présent, continuez et tapez votre mot de passe mais ne me le dites pas, vous ne devez jamais l'indiquer à quiconque, pas même à l'assistance technique. Je verrai simplement les astérisques, puisque votre mot de passe est protégé pour que je ne puisse pas le voir". Rien de cela n'est vrai, mais tout paraît logique à Mary. Puis il lui demande de le prévenir lorsque son ordinateur aura démarré."

Lorsque c'est fait, il lui fait lancer deux de ses applications et elle lui indique qu'elles ont démarré impeccablement.

Mary est soulagée de constater que tout semble fonctionner normalement. "Je suis content, j'ai pu m'assurer que vous pouvez utiliser votre ordinateur" dit Peter, et il poursuit : "Ah, sinon, nous venons d'installer une mise à jour qui permet aux utilisateurs de changer leur mot de passe. Voulez-vous me consacrer quelques minutes pour que je voie si elle fonctionne correctement ?"

Elle lui est reconnaissante de l'aide qu'il vient de lui apporter et accepte volontiers. Peter lui montre comment lancer l'application qui autorise l'utilisateur à changer de mot de passe, un élément standard de Windows 2000. "Allez-y, entrez votre mot de passe" lui dit-il. Mais souvenez-vous qu'il ne faut pas le prononcer tout haut."

Lorsqu'elle a terminé, Peter indique : "Juste pour ce test rapide, lorsqu'on vous demande votre nouveau mot de passe, saisissez "test123" une première fois, puis une nouvelle fois dans la case Vérification et cliquez sur Entrée".

Il l'amène jusqu'au processus de déconnexion du serveur. Il la fait attendre quelques minutes puis lui demande de se reconnecter, cette fois avec son nouveau mot de passe. Tout fonctionne à merveille, Peter semble très content et il lui montre comment reprendre son mot de passe d'origine ou en choisir un nouveau — en la prévenant encore de ne pas prononcer le mot de passe à haute voix.

"Bien Mary", dit Peter. "Nous n'avons trouvé aucun problème, et c'est parfait. Mais si un problème quelconque survenait, n'hésitez pas à nous appeler. Je m'occupe généralement de projets spéciaux, mais n'importe qui ici peut vous aider." Elle le remercie et lui dit au revoir.

Le point de vue de Peter

La nouvelle concernant Peter avait circulé : plusieurs personnes qui étaient allées à l'école avec lui avaient entendu dire qu'il était devenu une sorte de génie de l'informatique, capable de trouver des informations que personne n'arrivait à obtenir. Lorsque Alice Conrad vient lui demander un service, il commence par refuser. Pourquoi l'aiderait-il ? Lorsqu'il lui a demandé un rendez-vous, un jour, elle l'a éconduit.

Mais son refus ne semble pas la surprendre. Elle lui dit que de toute façon elle pensait bien qu'il ne pourrait pas réussir ce qu'elle voulait. C'est un défi pour Peter car, naturellement, il est certain d'y parvenir. Et c'est ainsi qu'il est amené à accepter.

Alice s'est vu proposer un contrat de consultant pour une entreprise de marketing, mais les termes du contrat ne lui semblent pas satisfaisants. Avant de demander de meilleures conditions, elle veut connaître le contenu des contrats des autres consultants.

Voici comment Peter raconte l'histoire.

"Je ne l'aurais pas dit à Alice, mais j'expédiais les gens qui me demandaient un service en doutant de mes capacités, lorsque je savais que ce serait facile. Enfin, pas si facile que cela, cette fois. Cela demanderait une certaine habilité. Mais c'était d'accord.

Je pourrais lui montrer combien j'allais mener cela brillamment.

Peu après 7h30 ce lundi matin, j'appelle les bureaux de l'entreprise de marketing et obtiens la standardiste ; je lui dis que j'appartiens à l'entreprise qui gère les plans de pension et que j'ai besoin de parler à quelqu'un de la comptabilité. A-t-elle remarqué si des employés de la comptabilité étaient déjà arrivés ? Elle répond : "Je crois avoir vu Mary entrer il y a quelques minutes. Je vais essayer de vous la passer."

Lorsque Mary décroche le téléphone, je lui raconte ma petite histoire sur les problèmes d'ordinateur, destinée à lui donner la frousse et à la faire coopérer. Immédiatement après lui avoir montré comment changer son mot de passe, je me connecte au système avec le mot de passe provisoire que je lui ai demandé d'utiliser, "test123".

C'est là qu'intervient la maîtrise : j'installe alors un petit programme qui me permet d'accéder aux systèmes informatiques de l'entreprise dès que je le veux, en utilisant un mot de passe secret personnel. Lorsque je raccroche, l'étape suivante consiste à effacer l'historique de mes opérations afin que personne ne puisse même savoir que je me suis trouvé sur le système. C'est facile. Après m'être accordé davantage de privilèges système, je peux télécharger un petit programme, baptisé *clearlogs*, que j'ai trouvé sur un site Web relatif à la sécurité (www.ntsecurity.nu).

C'est là que commence le vrai travail. Je recherche tous les documents contenant le mot "contrat" et télécharge les fichiers. Puis je fouille un peu plus et arrive au répertoire qui contient tous les bulletins de rémunération des consultants. Je rassemble alors tous les fichiers de contrats et une liste des règlements.

Alice pourra ensuite étudier soigneusement les contrats et voir combien les autres consultants sont payés. Pour la consultation de tous ces fichiers, je lui laisse le plus gros du travail. Ma tâche est terminée."

Le message de Mitnick

Il est stupéfiant de constater à quel point il est facile pour un manipulateur d'obtenir certaines choses des gens, selon la manière dont il structure sa requête. Le principe consiste à déclencher une réponse automatique, en fonction de principes psychologiques, et à compter sur les raccourcis mentaux que les personnes utilisent lorsqu'elles considèrent l'appelant comme un allié.

Analyse de l'arnaque

L'appel téléphonique que Peter a passé représente la forme la plus basique de la manipulation : il s'agit d'une entreprise simple qui nécessite peu de préparation, qui réussit du premier coup et qui aboutit après quelques minutes seulement.

Mieux encore, Mary n'avait par la suite aucune raison de penser qu'elle avait été victime d'un stratagème ou d'une ruse, aucune raison de rédiger un rapport ou de faire du foin.

Le plan de Peter a fonctionné grâce à l'utilisation de trois tactiques de manipulation. Tout d'abord, il a obtenu la coopération de Mary en provoquant chez elle un sentiment de peur, en lui faisant croire que son ordinateur était susceptible de tomber en panne. Puis il a pris le temps de lui faire ouvrir deux de ses applications afin qu'elle se rende compte que celles-ci fonctionnaient parfaitement ; cela permettait également à Peter de renforcer leurs rapports, d'établir un sentiment de confiance. Enfin, il a obtenu une plus grande coopération, encore — et cela correspondait à la partie essentielle de la tâche qu'il devait accomplir —, en jouant sur le fait qu'elle lui était reconnaissante de l'aide qu'il lui avait apportée en s'assurant que son ordinateur n'avait pas de problème.

En lui disant qu'elle ne devait jamais révéler son mot de passe, même à lui, Peter a réalisé un travail subtil et en profondeur pour la persuader qu'il se préoccupait de la sécurité des fichiers de son entreprise. Elle avait donc d'autant plus confiance en Peter, puisqu'il la protégeait, ainsi que son entreprise.

LA DESCENTE DE POLICE

Imaginez la scène : les autorités américaines essaient de tendre un piège à un homme nommé Arturo Sanchez qui diffuse gratuitement des films sur Internet. En effet, les studios d'Hollywood disent qu'il viole la législation sur les copyrights. Mais lui répond qu'il essaie simplement de les forcer à reconnaître l'existence d'un marché inévitable, afin qu'ils réagissent et qu'ils permettent aux internautes de télécharger les nouveaux films sur le Web. Il fait remarquer, à juste titre, que cela pourrait être une énorme source de revenus dont les studios ne semblent pas du tout conscients.

Mandat de perquisition, s'il vous plaît

Une nuit qu'il rentre tard chez lui, Arturo observe les fenêtres de son appartement depuis l'autre côté de la rue et remarque que les lumières sont éteintes, alors qu'il les laisse toujours allumées lorsqu'il s'absente.

Il frappe à la porte d'un voisin jusqu'à ce que celui-ci se réveille, et apprend que l'immeuble a fait l'objet d'une descente de police. Mais ils ont demandé aux voisins de sortir et il n'est pas sûr de l'appartement qu'ils ont visité. Il sait juste qu'ils ont emmené certains objets lourds, seulement ils étaient emballés et il n'a pas pu voir ce que c'était. Ils n'ont procédé à aucune arrestation.

Arturo vérifie son appartement. Mauvais augure : il trouve un papier émanant de la police, qui lui demande d'appeler immédiatement un poste de police afin de fixer un rendez-vous pour une convocation dans les trois jours. Mais il y a un augure pire encore : l'absence de ses ordinateurs.

Arturo se rend dans la nuit chez un ami, mais l'incertitude le ronge. Que sait la police ? L'ont-ils enfin trouvé, mais en lui laissant une dernière chance de s'enfuir ? Ou s'agit-il d'une tout autre chose qu'il pourrait éclaircir sans devoir quitter la ville ?

Avant de poursuivre votre lecture, prenez un moment pour réfléchir : pouvez-vous envisager une seule façon de découvrir ce que sait la police à votre sujet ? En supposant que vous n'ayez aucun contact politique, ni ami dans les services de police ou au bureau du District Attorney[1], pouvez-vous concevoir qu'il existe un moyen pour que vous, citoyen ordinaire, vous procuriez ces informations ? Ou que même une personne douée en manipulation le puisse ?

Arnaquer la police

Arturo, lui, sait comment faire : pour commencer, il se procure le numéro de téléphone d'une boutique de photocopies proche de chez lui, l'appelle et lui demande son numéro de fax. Puis il téléphone au bureau du District Attorney et demande le service des procès-verbaux. Lorsqu'il est en communication avec ce service, il se fait passer pour un détective de Lake County et dit qu'il a besoin de parler à l'employé qui enregistre les mandats de recherches en cours.

Le stratagème d'Arturo

Une fois en communication avec ce service, Arturo se fait passer pour un détective de Lake County et dit qu'il a besoin de parler à l'employé qui enregistre les mandats de recherches en cours.

"C'est moi", répond la femme. "Oh, très bien", dit-il. "Nous avons fait une descente chez un suspect la nuit dernière et j'essaie de localiser la déclaration écrite sous serment."

"Nous les classons par adresse", indique-t-elle.

Lorsqu'il donne son adresse, elle semble presque excitée. "Oh, oui, bouillonne-t-elle, je le connais *celui-là*. "L'affaire des copyrights"."

"C'est celui-là. Avez-vous la déclaration par écrit et sous serment, ainsi que la copie du mandat ?"

"Oh, je l'ai justement ici."

"Parfait" dit-il. "En fait, je suis sorti et j'ai rendez-vous avec un représentant des forces de l'ordre à ce sujet dans quinze minutes. Je suis très distrait ces derniers temps et j'ai oublié le dossier à la maison. Or je n'ai plus le temps de faire l'aller-retour. Pourriez-vous m'en faire des copies ?"

"Bien sûr, aucun problème. Je vais faire des copies, vous pouvez passer les prendre."

"Parfait", dit-il, "c'est parfait, mais en fait, je suis de l'autre côté de la ville. Vous serait-il possible de me les faxer ?"

Cela posait un petit problème, mais pas insurmontable. "Nous n'avons pas de fax ici, aux procès-verbaux" répond-elle. "Mais il y en a un en bas, dans le bureau des greffiers, et je suis autorisée à l'utiliser."

"Laissez-moi appeler le bureau des greffiers et les mettre au courant", dit-il.

L'employée du bureau des greffiers dit qu'elle serait contente de l'aider mais veut d'abord savoir qui va payer. Elle a besoin d'un numéro de compte. "Je me procure le numéro et vous rappelle", indique Arturo.

Puis il appelle le bureau du District Attorney, en se faisant de nouveau passer pour un officier de police et demande simplement à la réceptionniste le numéro de compte du bureau. Elle le lui donne sans hésiter.

Son deuxième appel au bureau des greffiers pour indiquer le numéro lui fournit un prétexte pour manipuler encore un peu l'employée : il s'arrange pour qu'elle se rende à l'étage supérieur pour prendre les copies à faxer.

Effacer ses traces

Arturo a encore quelques étapes à franchir. Il est toujours possible que quelqu'un sente que c'est louche ; il se peut aussi que deux détectives, habillés normalement, fassent semblant de s'occuper dans le magasin de photocopies en attendant que quelqu'un arrive pour demander ce fax. Il patiente donc un peu puis rappelle le bureau des greffiers pour vérifier que l'employée a bien transmis le fax. Jusqu'ici, tout s'est bien déroulé.

1. N.D.T. : L'équivalent de notre Procureur de la République.

Note

Comment un manipulateur connaît-il en détail tant de procédures — les services de police, le bureau du District Attorney, les pratiques des opérateurs téléphoniques ainsi que l'organisation d'entreprises spécifiques dont les secteurs d'activité sont utiles à ses attaques, comme les télécommunications et l'informatique ? Parce que chercher est son travail. Pour le manipulateur, ces informations constituent un stock de connaissances qui peuvent l'aider.

Arturo appelle alors un autre magasin de photocopie de la même chaîne et utilise une ruse que nous connaissons bien maintenant : il dit combien il est satisfait de leur travail et indique qu'il veut écrire une lettre de félicitations à la directrice, il lui faut donc son nom. Avec cette information essentielle, il rappelle le premier magasin de photocopie et dit qu'il veut parler au directeur. Lorsque celui-ci décroche, Arturo dit : "Bonjour, ici Edward du magasin 628 à Hartfield. Ma directrice, Anna, m'a demandé de vous appeler. Nous avons un client très contrarié : quelqu'un lui a donné un mauvais numéro de fax, qui est en fait celui de votre agence, et il est ici à attendre un fax important. Le directeur promet qu'un de ses employés va s'occuper du fax et l'envoyer immédiatement au magasin de Hartfield.

Arturo attend déjà dans le second magasin lorsque le fax arrive. Dès qu'il l'a en main, il rappelle le bureau des greffiers pour remercier la femme qui le lui a envoyé et il précise : "Il n'est pas nécessaire de rapporter ces copies à l'étage supérieur, vous pouvez simplement les jeter". Puis il appelle le directeur du premier magasin et lui demande également de jeter l'exemplaire du fax. De cette façon, il n'y aura plus la moindre trace de ce qui s'est passé, au cas où quelqu'un se présenterait ensuite pour poser des questions. Les manipulateurs savent que l'on n'est jamais trop prudent.

En s'organisant de cette façon, Arturo n'a même pas eu à payer quoi que ce soit au premier magasin pour avoir reçu le fax et l'avoir renvoyé au second. Et s'il s'avérait que la police se présente au premier magasin, Arturo aurait déjà son fax et se serait évanoui depuis longtemps dans la nature avant qu'elle ait pu l'intercepter au deuxième endroit.

Fin de l'histoire : la déclaration écrite sous serment et le mandat indiquent que la police a bien mis en évidence qu'Arturo se livre à la copie de films. C'est ce qu'il voulait savoir. Vers minuit, il avait franchi la frontière de l'État et entamé une nouvelle vie, quelque part, avec une nouvelle identité, prêt à reprendre sa campagne.

Analyse de l'arnaque

Le personnel qui travaille dans le bureau d'un District Attorney est en contact permanent avec les représentants de la loi : il répond à des questions, prend des dispositions, reçoit des messages. En l'occurrence, il est vraisemblable que quiconque est assez maître de soi pour appeler en se faisant passer pour un policier, un représentant de l'État, etc., sera cru sur parole. Sauf s'il est évident qu'il ne connaît pas le jargon, ou s'il se montre nerveux et butte sur ses mots, ou encore ne paraît pas crédible, il se peut qu'on ne lui pose même pas la moindre question pour vérifier son titre. C'est exactement ce qui s'est produit dans ce cas, avec deux employés différents.

Le message de Mitnick

La vérité est que personne n'est à l'abri des techniques de duperie dont peuvent user les bons manipulateurs. En raison du rythme de la vie quotidienne, nous ne prenons pas toujours le temps de mûrir nos décisions, même dans le cas de sujets importants pour nous. Les situations compliquées, le manque de temps, l'état émotionnel ou la fatigue mentale peuvent facilement nous distraire. Nous utilisons alors un raccourci mental et prenons des décisions sans analyser soigneusement et complètement les informations : ce processus mental est connu sous le nom de *réponse automatique*. Cela est également vrai pour les représentants de la loi ; nous sommes tous des êtres humains.

Il a fallu un seul appel téléphonique à Arturo pour obtenir un code de facturation obligatoire. Puis il a joué la carte de la compassion en racontant son histoire de rendez-vous quinze minutes après : "Je suis très distrait et j'ai oublié le dossier à la maison". Son interlocutrice s'est naturellement sentie désolée pour lui et a cherché à l'aider.

Puis en ayant recours, non pas à un, mais à deux magasins de photocopies, Arturo a pris le maximum de précautions pour récupérer son fax. Il existe une variante de cette ruse, qui rend encore plus difficile toute action éventuelle pour remonter jusqu'au manipulateur : au lieu de faire envoyer le document à un autre magasin de photocopies, l'attaquant peut fournir, en guise de numéro de fax, l'adresse d'un service Internet gratuit qui recevra le

fax pour lui et le fera suivre automatiquement sur son adresse e-mail. De cette façon, l'attaquant peut le télécharger directement sur son ordinateur, sans avoir besoin de montrer son visage à un endroit où il pourrait être identifié plus tard. L'adresse e-mail et le numéro de fax électronique pourront être abandonnés une fois la mission accomplie.

INVERSION DES RÔLES

Un jeune homme que j'appellerai Michael Parker fait partie de ces gens qui se rendent compte, mais un peu tard, que les métiers les mieux rémunérés sont généralement exercés par des personnes diplômées. Il a la possibilité de s'inscrire à mi-temps dans une université, avec un prêt étudiant, mais cela signifie qu'il devra travailler de nuit et les week-ends pour payer son loyer, sa nourriture, son essence et l'assurance de sa voiture. Michael, qui a toujours aimé trouver des raccourcis, pense alors qu'il existe peut-être un autre moyen, un moyen qui lui permettra d'y arriver plus vite et avec moins d'efforts. Comme il a commencé à jouer avec les ordinateurs à l'âge de dix ans et qu'il est depuis fasciné par la manière dont ils fonctionnent, il décide de voir s'il peut "créer" son propre diplôme accéléré de licencié ès informatique.

Le diplôme, avec ou sans mention ?

Il aurait pu s'introduire dans les systèmes informatiques de l'université, trouver l'enregistrement d'un diplômé avec une jolie mention ("bien" ou "très bien", par exemple), copier l'enregistrement, y placer son propre nom et l'ajouter aux enregistrements de l'année en question. Mais en y pensant bien, il n'est pas sûr que ce soit une bonne idée. En effet, il se dit qu'il doit également exister d'autres enregistrements relatifs à la vie des étudiants sur le campus, et qui concernent le paiement des cours, le logement, etc. Par conséquent, s'il se contente de créer un enregistrement indiquant les cours suivis et les niveaux universitaires, cela risque de ne pas suffire.

En se triturant les méninges, il lui vient à l'esprit qu'il pourrait voir si l'université a accueilli un diplômé du même nom que lui, qui aurait obtenu un diplôme d'informatique dans une fourchette d'années appropriée. Si tel était le cas, il lui suffirait d'indiquer le numéro de sécurité sociale de l'autre Michael Parker sur ses formulaires d'embauche ; ainsi, toute entreprise qui vérifierait son nom et son numéro de sécurité sociale auprès de l'université s'entendrait dire que oui, il avait bien le diplôme prétendu. (Il était évident pour lui, même si cela ne l'était pas pour la plupart des gens, qu'il pouvait indiquer un numéro de sécurité sociale dans un formulaire de candidature puis, s'il était embauché, indiquer son propre numéro dans les formulaires destinés aux nouveaux employés. La plupart des entreprises ne pensent jamais à vérifier si un nouvel embauché a utilisé un numéro différent lors la procédure d'embauche.)

Se connecter

Comment localiser un Michael Parker dans les enregistrements de l'université ? Voici comment il y parvient :

Il se rend à la bibliothèque principale du campus, s'assied devant un terminal informatique, se connecte à Internet puis accède au site Web de l'université. Il appelle ensuite le bureau des inscriptions. À la personne qui lui répond, il utilise l'un des classiques du manipulateur : "J'appelle du centre informatique, nous apportons quelques modifications à la configuration du réseau et nous voulons nous assurer que nous n'allons pas interrompre votre accès. À quel serveur êtes-vous connecté ?"

"Qu'entendez-vous par 'serveur' ?" lui demande-t-on.

"À quel ordinateur vous connectez-vous lorsque vous avez besoin de rechercher des renseignements universitaires sur les étudiants ?"

La réponse, "admin.rnu.edu", lui indique le nom de l'ordinateur sur lequel les enregistrements concernant les étudiants sont sauvegardés. C'est la première pièce du puzzle : il connaît maintenant sa machine cible.

Il saisit cette URL sur l'ordinateur et n'obtient aucune réponse : comme il s'y attendait, un pare-feu bloque l'accès. Il lance alors un programme afin de voir s'il peut se connecter à un autre service de cet ordinateur et trouve un port ouvert avec un service Telnet actif, qui permet à un ordinateur de se connecter à distance à un autre et d'y accéder comme s'il était directement connecté à un *terminal muet*. Pour obtenir un accès, il lui suffit de connaître le nom d'utilisateur et le mot de passe d'une personne lambda.

Il appelle de nouveau le bureau des inscriptions, en écoutant d'abord la voix pour être sûr qu'il s'adresse à une autre personne. Il obtient une femme et prétend encore appartenir au centre informatique de l'université. Il lui dit qu'ils installent un nouveau système de production d'enregistrements administratifs. Il lui demande de se connecter au nouveau système, en mode test, pour voir si elle peut accéder aux enregistrements universitaires des étudiants. Il lui donne l'adresse IP à laquelle se connecter, puis la guide dans la procédure.

Jargon

Terminal muet
Terminal qui ne contient pas de microprocesseur propre. Les terminaux muets peuvent uniquement accepter des commandes simples et afficher des caractères et des chiffres sous forme de texte.

En fait, l'adresse IP la conduit à l'ordinateur devant lequel Michael est assis dans la bibliothèque du campus. Il a réussi à créer un simulateur de connexion qui ressemble exactement à celui qu'elle est habituée à voir lorsqu'elle rentre dans le système des enregistrements des étudiants. "Cela ne fonctionne pas", indique-t-elle. "Je reçois toujours 'Login incorrect'."

Pendant ce temps, le simulateur de connexion a enregistré sur le terminal de Michael les touches de clavier sur lesquelles elle a appuyé pour saisir son nom de compte et son mot de passe ; mission accomplie. Il lui explique que certains comptes n'ont pas encore été transférés sur cette machine. "Je crée votre compte et je vous rappelle", dit-il. Attentif à régler les derniers détails, comme doit l'être tout bon manipulateur efficace, il la contacte ultérieurement pour lui dire que le système de test ne fonctionne toujours pas et que, si cela lui convient, on la rappellera, elle ou quelqu'un d'autre, lorsque la cause du problème aura été découverte.

Un registre utile

À présent, Michael connaît le système informatique auquel il doit accéder et dispose d'un nom d'utilisateur et d'un mot de passe. Mais de quelles commandes va t-il avoir besoin pour rechercher, parmi les fichiers de renseignements, un licencié en informatique dont le nom et la date d'obtention du diplôme conviennent ? La base de données des étudiants devait être propriétaire et avoir été créée sur le campus pour satisfaire les besoins spécifiques de l'université et du bureau des inscriptions ; par conséquent, il ne devait être possible d'accéder aux informations de la base de données que d'une seule et unique façon.

Première étape pour éliminer cet obstacle : trouver la personne susceptible de le guider à travers les mystères de la recherche dans la base de données des étudiants. Il appelle de nouveau le bureau des inscriptions et a une autre personne au bout du fil. Il dit à l'employée qu'il appartient au bureau des Doyens des Ingénieurs et demande : "Qui est censé nous aider lorsque nous avons des problèmes d'accès aux fichiers universitaires des étudiants ?"

Quelques minutes plus tard, il est au téléphone avec l'administrateur de la base de données de l'université et joue sur la compassion : "Je suis Mark Sellers, du bureau des inscriptions. Désolé de vous déranger, mais tout le monde est à une réunion cet après-midi, et il n'y a personne pour m'aider. J'ai besoin de retrouver la liste de tous les licenciés en informatique entre 1990 et 2000. Il nous la faut pour la fin de la journée et si je ne me la procure pas, je ne vais pas garder ce poste longtemps. Vous êtes disposé à aider quelqu'un dans l'embarras ?" Aider les gens fait partie du rôle de l'administrateur de la base de données, aussi explique-t-il le processus à Michael, pas à pas.

Lorsqu'il raccroche, Michael a téléchargé toute la liste des licenciés en informatique de ces années-là. En quelques minutes, il trouve deux Michael Parker, en choisit un et récupère son numéro de sécurité sociale ainsi que d'autres informations pertinentes stockées dans la base de données. Il devient alors "Michael Parker, diplômé en informatique avec mention, 1998."

Analyse de l'arnaque

Dans cette supercherie, l'attaquant a utilisé une ruse que je n'avais pas encore évoquée : il a demandé à l'administrateur de la base de données de le conduire à travers un processus informatique qu'il ne connaît pas. Une inversion des rôles puissante et efficace, qui équivaut à demander à un propriétaire de magasin de vous aider à transporter jusqu'à votre voiture un carton plein d'articles que vous venez de lui voler.

Le message de Mitnick

Les utilisateurs d'ordinateurs ignorent parfois complètement les menaces que représente la manipulation, ainsi que les vulnérabilités qui lui sont associées, et qui existent pourtant dans notre monde dominé par la technologie. Ils ont accès à des informations mais n'ont pas la moindre idée de ce qui pourrait se révéler être une menace pour la sécurité. Un manipulateur préférera cibler un employé possédant une faible connaissance de la valeur des informations en question car celui-ci sera plus enclin à répondre à ses demandes.

EMPÊCHER L'ARNAQUE

Compassion, culpabilité et intimidation sont trois déclencheurs psychologiques très couramment utilisés par le manipulateur, et ces histoires ont montré comment on les met à l'œuvre. Mais que pouvez-vous faire, votre entreprise et vous-même, pour éviter ces types d'attaques ?

Protéger les données

Certaines histoires de ce chapitre soulignent le danger que représente l'envoi d'un fichier à une personne que l'on ne connaît pas, même s'il s'agit (ou s'il semble s'agir) d'un employé et si le fichier est transmis *en interne*, à une adresse e-mail ou à un fax de l'entreprise.

Les règles de sécurité de l'entreprise doivent être très précises quant aux mesures de protection à mettre en œuvre lorsqu'il s'agit de délivrer des données de grande valeur à une personne que l'on ne connaît pas personnellement. Il faut définir des procédures pour le transfert de fichiers contenant des informations sensibles. Il faut également définir clairement les étapes à suivre pour effectuer une vérification lorsque la requête émane d'une personne inconnue, en distinguant différents niveaux d'authentification suivant le degré de confidentialité de l'information.

Voici quelques procédures à prendre en compte :

- Définir à quel point l'information est importante (ce qui peut obliger à demander une autorisation au propriétaire de l'information en question).
- Conserver un journal de ces transactions, par employé ou par service.
- Établir une liste des personnes qui ont été spécialement formées aux procédures et qui sont autorisées à divulguer des informations sensibles. Exiger que seules ces personnes soient autorisées à envoyer des informations aux individus extérieurs à l'équipe ou au service.
- Pour les demandes de données effectuées par écrit (e-mail, fax ou courrier), instaurer des mesures de sécurité supplémentaires afin vérifier que la requête a bien été formulée par la personne en question.

À propos des mots de passe

Tout employé qui a accès à des informations confidentielles — et aujourd'hui, cela signifie presque tout employé qui utilise un ordinateur — doit savoir qu'un acte aussi simple qu'un changement de mot de passe, même pour quelques instants, peut provoquer une brèche importante dans la sécurité.

Les formations en matière de sécurité doivent traiter le sujet des mots de passe et mettre l'accent sur le moment où il faut les changer et sur la façon de le faire, définir ce qui constitue un mot de passe acceptable, et insister sur les dangers auxquels on s'expose en laissant n'importe qui faire partie du processus. Il faut notamment que les formations amènent tous les employés à comprendre qu'ils doivent se montrer soupçonneux devant *n'importe quelle* demande impliquant leurs mots de passe.

On pourrait penser qu'il suffirait de diffuser un simple message parmi les employés. Or ce n'est pas le cas car, pour mesurer la portée du message, les employés doivent saisir combien une action simple telle que celle qui consiste à changer un mot de passe peut conduire à compromettre la sécurité. Vous pouvez dire à un enfant qu'il doit regarder des deux côtés avant de traverser la route, mais tant que l'enfant n'en comprendra pas l'importance, vous ne pourrez compter que sur son obéissance aveugle. Et les règles qui s'appuient sur une obéissance aveugle sont généralement ignorées ou oubliées.

Note

Les mots de passe sont à ce point au centre des attaques par manipulation que nous leur consacrons une section particulière au Chapitre 16, dans laquelle vous trouverez des conseils spécifiques quant à leur gestion.

Centraliser les rapports

Il vous faut instaurer une règle de sécurité qui consiste à désigner une seule personne ou un seul groupe auxquels les employés signaleront les activités suspectes qui leur semblent être des tentatives d'infiltration de votre entreprise. Tous les employés doivent savoir qui contacter chaque fois qu'ils suspectent une tentative d'intrusion électronique ou physique. Ils doivent toujours avoir à leur portée le numéro de téléphone de l'endroit à appeler pour rapporter ce type de faits, afin de ne pas perdre de temps à le chercher lorsqu'ils soupçonnent qu'une attaque est en cours.

Protéger votre réseau

Les employés doivent comprendre que le nom d'un serveur informatique ou d'un réseau n'est pas une information anodine, mais qu'il peut constituer pour un attaquant une donnée essentielle qui l'aidera à gagner la confiance des personnes qu'il contactera ou à localiser les informations qu'il souhaite.

En particulier, les salariés tels que les administrateurs de bases de données, qui travaillent avec des logiciels spécifiques, appartiennent à la catégorie du personnel la plus au fait des nouvelles technologies ; pour cette raison, ils doivent opérer selon des règles spéciales et très restrictives quant à la vérification de l'identité des personnes qui appellent pour obtenir des informations ou des conseils.

Il faut que les employés auxquels on fait régulièrement appel pour tout problème informatique soient bien formés quant aux types de requêtes qui doivent éveiller leurs soupçons, c'est-à-dire qui peuvent révéler que l'appelant est peut-être en train de tenter une attaque par manipulation.

Toutefois, il est important de noter que, du point de vue de l'administrateur de base de données de la dernière histoire de ce chapitre, l'appelant respectait les critères de légitimité : il appelait d'un campus et se trouvait manifestement sur un site qui exigeait un nom de compte et un mot de passe. Cela souligne une fois de plus l'importance qu'il y a à utiliser des procédures standardisées pour vérifier l'identité de quiconque demande des informations, en particulier dans un cas comme celui-ci, où l'appelant souhaitait qu'on l'aide à accéder à des enregistrements confidentiels.

Tous ces conseils doivent être encore plus suivis dans les lycées et les universités. Il n'est pas nouveau que le piratage informatique est le passe-temps favori de nombreux étudiants, ni surprenant que les données informatiques concernant les étudiants — et parfois également le corps enseignant — constituent une cible attrayante. Cette activité abusive est tellement importante que certaines entreprises considèrent actuellement les campus comme des environnements hostiles et mettent en place des règles de pare-feu qui bloquent l'accès aux établissements dont les adresses se terminent par *.edu*.

En tout état de cause, tous les types d'enregistrements qui concernent les étudiants et le personnel doivent être considérés comme des cibles d'attaque privilégiées, et être parfaitement protégés en tant qu'informations sensibles.

Conseils pour les formations

La plupart des attaques par manipulation sont très faciles à contrecarrer… pour quiconque sait ce à quoi il faut faire attention. Du point de vue de l'entreprise, il est fondamental de dispenser de bonnes formations en matière de sécurité, et il est également fondamental d'employer diverses méthodes pour *rappeler* aux gens ce qu'ils ont appris.

Utilisez des fenêtres dynamiques qui s'affichent lorsque l'utilisateur allume son ordinateur, et qui indiquent un message de sécurité différent chaque jour. Le message doit être conçu de telle sorte qu'il ne disparaisse pas automatiquement, mais que l'utilisateur soit obligé de cliquer sur un objet pour accuser réception de sa lecture.

Une autre approche que je recommande consiste à établir un programme de rappels en matière de sécurité. Il est important que les messages de rappel soient fréquents : un programme de sensibilisation doit être continu et sans fin. S'agissant du contenu, les rappels doivent être formulés différemment à chaque fois. Des études ont montré que l'efficacité de ces messages est d'autant plus grande lorsque leur formulation varie ou qu'ils sont utilisés dans des exemples différents.

L'utilisation de courtes annonces dans le bulletin d'information de l'entreprise constitue également une excellente approche. On ne consacrera pas une page entière à la sécurité — cela en vaudrait pourtant certainement la peine — mais plutôt un encart de deux ou trois colonnes, comme pour une petite publicité dans le journal local. Dans chaque nouveau bulletin, on rappellera ainsi, de façon brève et frappante, un élément relatif à la sécurité.

Chapitre 9

L'arnaque par inversion

Le film *L'arnaque*, cité par ailleurs dans ce livre (et, d'après moi, certainement le meilleur film jamais tourné au sujet d'une arnaque), déploie son stratagème rusé avec un luxe de détails fascinants. Le film décrit exactement la façon dont les escrocs de premier rang tirent les ficelles. Si vous voulez savoir comment une équipe de professionnels réussit une arnaque en extorquant une grosse somme en une seule soirée, il n'existe pas de meilleur manuel.

Mais les arnaques traditionnelles, quel que soit leur degré de subtilité, suivent un modèle. Parfois, la ruse se déroule en sens inverse, c'est ce que l'on nomme une *arnaque par inversion*. Il s'agit d'un cas intéressant dans lequel l'attaquant met en place une situation pour faire en sorte que la victime l'appelle à l'aide, ou qu'un collègue formule une demande, à laquelle l'*attaquant* répond.

Comment fonctionne ce type d'arnaque ? C'est ce que vous allez découvrir.

L'ART DE LA PERSUASION AMICALE

Lorsqu'un individu moyen dresse le profil d'un hacker informatique, il pense généralement à l'image peu flatteuse d'un abruti introverti et solitaire dont le meilleur ami est l'ordinateur, et qui éprouve des difficultés à suivre une conversation, excepté par messagerie instantanée. Le manipulateur, qui a souvent des dons de hacker, possède également des talents tout à fait différents, comme une forte capacité à exploiter et à duper les gens. Ces facilités lui permettent d'obtenir des informations en suivant des voies qu'on n'imaginerait même pas.

Le pseudo-client d'Angela

Lieu : Banque Fédérale de l'Industrie, agence de Valley.

Heure : 11 h 27.

Angela Wisnowski répond à un appel téléphonique émanant d'un homme qui, étant sur le point de recevoir un héritage important, souhaite obtenir des renseignements sur les différents types de comptes d'épargne existants et sur tout investissement sûr et aux intérêts décents. Elle explique qu'il existe un certain nombre de possibilités et lui demande s'il pourrait venir à l'agence pour en discuter avec elle. Il a prévu de partir en voyage dès que l'argent serait arrivé, et il a beaucoup de dispositions à prendre. Elle commence donc à lui faire quelques suggestions et lui donne des détails sur les taux d'intérêt, tout en essayant de connaître ses objectifs d'investissement.

Elle pense qu'elle est en train de marquer des points, quand il annonce : "Oh, je suis désolé, je dois prendre un autre appel. Quand pourrons-nous terminer notre conversation afin que je puisse me décider ? À quelle heure prenez-vous votre pause déjeuner ?" "À 12 h 30", répond-elle. Il lui dit qu'il essaiera de rappeler avant cette heure-là ou demain dans la matinée.

L'interlocuteur de Louis

Les banques importantes utilisent des codes de sécurité internes qui changent chaque jour. Lorsque l'employé d'une agence a besoin de renseignements d'une autre agence, il prouve qu'il est habilité à obtenir ces informations en donnant le code de la journée. Pour disposer d'un niveau de sécurité et d'une souplesse plus importants, certaines grandes banques émettent plusieurs codes chaque jour. Dans un établissement de la côte ouest des États-Unis que j'appellerai la Banque Fédérale de l'Industrie, les employés trouvent chaque matin, sur leur ordinateur, une liste de cinq codes pour la journée, identifiés de A à E.

Lieu : le même.

Heure : 12 h 48 le même jour.

Louis Halpburn ne se doute de rien lorsqu'il reçoit un appel cet après-midi-là, un appel identique à ceux qu'il traite régulièrement plusieurs fois par semaine.

"Bonjour, dit l'appelant. Ici Neil Webster, de l'agence 3182 à Boston. Angela Wisnowski, s'il vous plaît."

"Elle est partie déjeuner. Puis-je vous aider ?"

"Eh bien, elle a laissé un message nous demandant de lui faxer certains renseignements sur l'un de nos clients."

L'appelant semble avoir passé une mauvaise journée.

"La personne qui s'occupe normalement de ces demandes est malade", dit-il. "J'en ai toute une pile à traiter, il est presque seize heures de ce côté-ci des États-Unis et j'ai rendez-vous chez le médecin dans une demi-heure."

La manipulation, ici, qui consiste à indiquer toutes les raisons pour lesquelles l'autre personne devrait se sentir désolée pour le manipulateur, est destinée à amadouer la cible. Il poursuit : "Pour quiconque écoute son répondeur téléphonique, le numéro de fax est inaudible. J'ai compris "123", mais après ?"

Louis donne le numéro de fax et son interlocuteur lui dit : "Très bien, merci. Avant que je puisse faxer cela, j'ai besoin de vous demander le Code B."

"Mais vous m'avez appelé", répond-il avec juste ce qu'il faut de froideur pour que l'homme de Boston perçoive le message.

Parfait, pense l'attaquant. *C'est chouette quand les gens ne tombent pas tout de suite dans le piège ! S'ils ne résistaient pas un peu, le travail serait trop facile et je pourrais devenir paresseux.*

Il répond : "Mon directeur d'agence est simplement devenu paranoïaque ; il veut que nous fassions des vérifications avant d'envoyer quoi que ce soit. C'est tout. Mais si vous n'avez pas besoin que nous vous faxions les renseignements, c'est parfait. Pas besoin de vérifier."

"Attendez, dit Louis, Angela sera de retour dans une demi-heure environ. Je peux lui demander de vous rappeler."

"Je lui répondrai simplement que je n'ai pas pu envoyer le renseignement aujourd'hui parce que, en ne me donnant pas le code, vous n'avez pas autorisé ma requête. Si je ne suis pas malade demain, je la rappellerai."

"Très bien."

"Le message mentionne 'Urgent'. Tant pis, sans vérification, je suis coincé. Vous lui direz que j'ai essayé de l'envoyer mais que vous ne m'avez pas donné le code, d'accord ?"

Louis abandonne sous la pression. Un soupir audible de contrariété descend le long de la ligne du téléphone.

"Bien, dit-il, attendez une minute ; je dois aller à mon ordinateur. Quel code voulez-vous ?"

"Le B," répond le manipulateur.

Il place la ligne en attente puis la reprend rapidement. "C'est 3184."

"Ce n'est pas le bon code."

"Si ça l'est : le B, c'est 3184."

"Je n'ai pas dit B, j'ai dit C."

"Oh ! Attendez une minute."

Une autre pause, le temps de regarder une nouvelle fois les codes.

"Le C, c'est 9697."

"9697, c'est bon. Le fax ne va pas tarder. D'accord ?"

"Merci."

L'appel de Walter

"Banque Fédérale de l'Industrie, Walter à l'appareil."

"Bonjour, Walter, ici Bob Grabowski à Studio City, agence 38" dit l'interlocuteur. "J'ai besoin de la photocopie de la *sig card*[1] d'un client. Pouvez-vous me la faxer ?" Aux États-Unis, la sig card comporte bien plus que la signature du client : elle inclut également des données d'identification comme le numéro de sécurité sociale, la date de naissance, le nom de jeune fille de la mère, et parfois même un numéro de permis de conduire. Très commode pour un manipulateur.

"Pas de problème. Quel est le code D ?"

"Un autre guichetier utilise mon ordinateur en ce moment", dit l'appelant. "Mais je viens d'employer le B et le C, et je m'en souviens. Demandez-moi l'un d'eux."

"D'accord, le C ?"

"9697."

Quelques minutes plus tard, Walter faxait la photocopie de la carte comme convenu.

L'appel de Donna Plaice

"Bonjour, M. Anselmo à l'appareil."

"En quoi puis-je vous aider ?"

"Quel est le numéro 800 que je suis supposé appeler quand je veux voir si un virement a bien eu lieu sur mon compte ?"

"Vous êtes client de la banque ?"

"Oui, je n'ai pas utilisé le numéro depuis un certain temps, et je ne sais plus où je l'ai noté."

"Le numéro est 800-555-8600."

"Très bien, merci."

1. N.D.T. : L'équivalent de notre carte bleue.

L'histoire de Vince Capelli

Le fils d'un flic de Spokane, Vince, savait depuis son plus jeune âge qu'il ne passerait pas sa vie à travailler dur pour un salaire ridicule. Ses deux principaux objectifs dans la vie étaient de quitter Spokane et de se mettre à son compte. Les sarcasmes de ses camarades de classe, pendant toute la période du lycée — ils trouvaient risible qu'il soit si pressé de monter une affaire sans savoir laquelle —, n'avaient fait que le décider davantage.

En secret, Vince savait qu'ils avaient raison. Il n'était bon qu'au poste de receveur de l'équipe de baseball du lycée. Mais pas assez bon pour obtenir une bourse du lycée, pas assez bon pour le baseball professionnel. Alors quelle affaire pouvait-il monter ?

Il y avait une chose que les copains proches de Vince n'avaient jamais vraiment comprise. Quoiqu'ils aient de nouveau (un couteau à cran d'arrêt, une paire de gants bien chauds, une petite amie sexy), il ne fallait pas longtemps pour que Vince s'approprie la "nouveauté" s'il la convoitait. Il ne volait ni ne chapardait pas dans le dos des autres ; ce n'était même pas nécessaire. Le détenteur la lui donnait volontairement et se demandait ensuite comment cela s'était produit. Et il n'aurait servi à rien de demander une explication à Vince : il ne savait pas lui-même pourquoi. Les gens semblaient tout bonnement lui donner ce qu'il voulait.

Vince Capelli était un manipulateur précoce, même s'il n'avait jamais entendu ce terme.

Ses amis ont arrêté de rire quand ils ont eu leurs diplômes en main. Pendant que les autres parcouraient péniblement la ville à la recherche d'emplois qui demandaient d'autres compétences que celles de savoir servir des frites, le père de Vince avait envoyé son fils parler à un vieux copain flic qui avait quitté la police pour lancer sa propre affaire de détective privé à San Francisco. Ce dernier a rapidement remarqué que Vince était doué pour ce travail et l'a embauché.

C'était il a six ans de cela. Il détestait les missions où il devait espionner des épouses infidèles, ce qui impliquait de rester assis de longues heures à surveiller, mais il se sentait toujours émoustillé quand il devait effectuer des recherches approfondies dans des affaires financières pour des procureurs qui essayaient de savoir si une misérable crapule était assez riche pour qu'il vaille la peine de la poursuivre en justice. Ces missions lui offraient toutes les chances d'utiliser son intelligence.

Comme cette fois où il a fouillé dans les comptes bancaires d'un type nommé Joe Markowitz, qui avait peut-être arnaqué un ami occasionnel. Lequel ami voulait maintenant savoir, au cas où il intenterait un procès à

Markowitz, si celui-ci avait suffisamment de fonds pour payer des dommages et intérêts.

Vince devait tout d'abord se procurer au moins un, mais de préférence deux des codes de sécurité journaliers de la banque. Cela paraissait presque impossible : pour quelle raison un employé de banque creuserait-il une crevasse dans son propre système de sécurité ? Posez-vous la question : si vous vouliez faire cela, auriez-vous la moindre idée de la façon d'y parvenir ?

Pour les gens comme Vince, c'est trop facile.

Les gens ont confiance en vous lorsque vous connaissez le jargon de leur métier et de leur entreprise. C'est comme appartenir à leur cercle d'intimes. C'est en quelque sorte une poignée de main secrète.

Dans ce cas, l'affaire était simple. Tout ce qu'il fallait pour commencer, c'était un numéro d'agence. Lorsque Vince a appelé le bureau de Bacon Street à Buffalo, l'employé qui lui a répondu semblait être un guichetier.

"Ici Tim Ackerman" dit Vince. N'importe quel nom ferait l'affaire, il n'allait pas le noter sur un papier. "Quel est le numéro de votre agence ?"

"Numéro de téléphone ou numéro d'agence ?" voulut savoir le guichetier, ce qui était plutôt stupide dans la mesure où Vince venait juste de composer son numéro de téléphone.

"Numéro d'agence."

"3182" dit-il. Comme cela. Pas de question telle que "C'est pour savoir quoi ?". Comme ce ne sont pas des informations sensibles, elles sont écrites sur pratiquement n'importe quel bout de papier que les employés utilisent.

Deuxième étape : appeler l'agence dont la cible était cliente, obtenir le nom de l'un des employés et savoir à quelle heure il partait déjeuner. Angela s'absente à 12h30. Jusque-là, c'est parfait.

La troisième étape du plan consistait à rappeler la même agence pendant la pause déjeuner d'Angela et à prétendre appeler de telle agence de Boston. Il suffisait ensuite d'affirmer qu'Angela avait besoin que des informations lui soient faxées, et que, pour ce faire, l'employé devait donner à Vince un des codes de la journée. C'est là qu'était le point délicat. Si Vince devait un jour concevoir un "permis" pour manipulateurs, il prévoirait un problème de la sorte, où la victime devient soupçonneuse — à juste titre — et où le manipulateur est coincé tant qu'il n'a pas surmonté le problème. On ne peut pas y arriver en récitant un texte ou en jouant un numéro répété à l'avance, il faut pouvoir deviner sa victime, saisir son humeur, jouer avec elle comme lorsqu'un poisson a mordu : on laisse un peu de mou, on le remonte, on laisse un peu de mou, on le remonte. Jusqu'à ce qu'on le récupère dans l'épuisette pour le laisser tomber dans le bateau.

C'est ainsi que Vince a obtenu l'un des codes de la journée. Un grand pas ! Comme la plupart des banques n'en utilisent qu'un, le problème aurait pu être résolu. Mais la Banque Fédérale de l'Industrie en utilise cinq, et un contre cinq est une forte cote. Avec deux contre cinq, Vince avait de meilleures chances de passer à l'acte suivant de cette petite pièce. Il aimait bien le moment où il avait répondu : "Je n'ai pas dit B, j'ai dit C." Lorsque cela marche, c'est beau. Et cela marche la plupart du temps.

En obtenir un troisième aurait été encore mieux. En réalité, il avait prévu d'en obtenir trois en un seul appel : "B", "C" et "D" se ressemblent tellement qu'il aurait pu prétendre à chaque fois que son interlocuteur l'avait mal compris. Mais pour cela, il fallait tomber sur un adversaire facile, et cet employé n'en était pas un. Vince se contenterait donc de deux codes.

Les codes du jour seraient son atout pour obtenir les informations de la sig card. Vince appelle et l'employé demande un code. Il veut le D, et Vince n'a que le B et le C. Mais ce n'est pas la fin du monde. Dans une telle situation, il faut se maîtriser, paraître confiant, continuer comme si de rien n'était. Vince a alors rusé avec un "Quelqu'un utilise mon ordinateur, demandez-moi un des codes que j'ai."

"Nous sommes tous employés de la même entreprise, nous sommes tous unis, nous ménageons notre interlocuteur" : c'est ce qu'on espère que pensera la victime à un moment comme celui-là. En l'occurrence, l'employé a bien joué son rôle. Il a choisi entre B et C, et Vince lui a fourni la bonne réponse. L'employé a ensuite envoyé le fax de la carte.

La manipulation était presque terminée. Un autre appel lui a permis d'obtenir le numéro commençant par 800 que les clients utilisent pour appeler le service automatique de la banque, qui indique, *via* une voix électronique, les renseignements que l'on demande. Grâce à la carte, Vince disposait de tous les numéros de compte. Un crayon à la main, Vince a appelé le numéro 800 et, après avoir appuyé sur quelques touches, il avait obtenu le dernier solde des quatre comptes de la personne, ainsi que le détail de ses derniers dépôts et retraits.

Vince avait tout ce que son client lui avait demandé, et même davantage. Il est toujours agréable d'offrir un petit extra pour faire bonne impression, pour satisfaire les clients. Après tout, c'est en répétant des coups comme celui-là que l'on arrive à garder son business.

Analyse de l'arnaque

La clé de cet épisode consistait à obtenir les codes du jour, dont le rôle était capital, et pour cela, l'attaquant a utilisé plusieurs techniques.

Il a commencé par un petit bras de fer verbal, quand Louis s'est montré réticent à lui donner un code. Louis avait raison de se méfier, puisque les codes sont conçus pour être utilisés dans le sens inverse. Il savait que normalement, c'est son interlocuteur inconnu qui devait *lui* fournir un code de sécurité. C'était le moment critique pour Vince, la charnière dont dépendait le succès de ses efforts.

Devant la méfiance de Louis, Vince en a simplement rajouté sur le plan de la manipulation, en faisant appel à la compassion de Louis ("je dois aller chez le docteur"), à l'urgence ("j'ai une tonne de boulot, il est presque 4 heures") et à l'influence ("dites-lui que vous ne m'avez pas donné le code"). La menace que Vince brandissait était habile puisqu'elle n'était que sous-entendue : si vous ne me donnez pas le code de sécurité, je n'envoie pas les renseignements que votre collègue attend, et je lui dirai que je les lui aurais bien envoyés mais que vous n'avez pas voulu coopérer.

Mais ne blâmons pas trop vite Louis. Après tout, l'homme qui était au bout du fil savait (ou du moins *paraissait* savoir) qu'Angela avait demandé un fax. Il était au courant des codes de sécurité et savait qu'ils étaient désignés par une lettre. Il n'y avait donc aucune raison de ne pas lui fournir la vérification qu'il demandait.

Louis n'est pas seul dans ce cas. Des employés de banque transmettent des codes de sécurité à des manipulateurs tous les jours. Cela paraît incroyable, mais c'est vrai.

Il existe une frontière où les techniques utilisées par les détectives privés cessent d'être légales pour devenir illégales. Vince est resté dans la légalité lorsqu'il a obtenu le numéro d'agence. Même lorsqu'il a persuadé Louis de lui donner deux des codes de sécurité du jour. Il a franchi la frontière lorsqu'il a obtenu que des renseignements confidentiels sur un client de la banque lui soient faxés.

Mais pour Vince et son employeur, les risques liés à ce crime sont faibles. Quand vous volez de l'argent ou des biens, on remarquera toujours qu'ils ont disparu. Mais quand vous volez des informations, le plus souvent, personne ne s'en aperçoit car ces informations restent en la possession de leur propriétaire.

Le message de Mitnick

Les codes de sécurité verbaux sont comme des mots de passe : ils fournissent un moyen commode et fiable de protéger les données. Mais les employés doivent être avertis des astuces dont usent les manipulateurs, et ils doivent apprendre à ne pas livrer ces informations si précieuses.

LES FLICS DUPÉS

Pour un détective privé véreux ou un manipulateur, la connaissance du numéro de permis de conduire[1] de quelqu'un peut s'avérer bien commode : elle peut par exemple servir à s'approprier l'identité de la personne afin d'obtenir des informations sur ses soldes bancaires.

Si on ne peut dérober le portefeuille de ladite personne ou risquer un coup d'œil au-dessus de son épaule au moment opportun, obtenir son numéro de permis de conduire s'avère presque impossible. Mais pour quiconque possède même de modestes compétences en manipulation, le défi n'est pas bien difficile à relever.

Un manipulateur, que je nommerai Éric Mantini, a régulièrement besoin de disposer de numéros de permis de conduire et de numéros d'immatriculation de véhicules. Il se rend compte qu'il multiplie inutilement les risques en appelant le DMV (*Department of Motor Vehicule*, le service d'immatriculation des véhicules à moteur) et en employant la même ruse à chaque fois qu'il a besoin de ces renseignements. Il se demande donc s'il n'y aurait pas une possibilité de simplifier les choses.

Il est probable que personne n'y a songé auparavant, mais il imagine un moyen d'obtenir les informations en un clin d'œil et à volonté. Il profite pour cela d'un service offert par le DMV de son État. Les DMV de nombreux États (ou quel que soit le nom qu'on leur donne) mettent à la disposition des compagnies d'assurance, des détectives privés et de certains autres groupes que le corps législatif fédéral a habilités en ce sens, des renseignements sur les citoyens — renseignements par ailleurs protégés.

Naturellement, le DMV a ses propres règles quant aux types de données à dévoiler. Ainsi, le secteur des assurances peut avoir accès à certains fichiers, mais pas à d'autres. Des restrictions de même type concernent les détectives privés, et ainsi de suite pour chaque corps de métier.

1. N.D.T. : Aux États-Unis, le permis de conduire fait office de carte d'identité.

Pour les personnes chargées de l'application de la loi, une règle différente s'applique généralement : le DMV fournit n'importe quelle information enregistrée à n'importe quel officier assermenté qui s'identifie correctement. Dans l'État où vit Éric, un officier doit, pour s'identifier, fournir un Code du demandeur, qui est attribué par le DMV, ainsi que son numéro de permis de conduire. Lorsqu'il procède à la vérification, un employé du DMV doit toujours rapprocher le nom de l'officier et son numéro de permis de conduire, de même qu'un autre élément d'information — généralement la date de naissance — avant de donner le moindre renseignement.

Et Éric n'envisage rien de moins que de revêtir l'identité d'un représentant de la loi.

Comment s'y prend-il ? En exécutant une arnaque par inversion sur les flics !

L'arnaque d'Éric

Tout d'abord, Éric appelle les renseignements téléphoniques et demande le numéro du siège du DMV. On lui indique le 503 555 5000 ; il s'agit naturellement du numéro destiné aux appels du grand public. Il appelle alors un poste de shérif tout proche et demande le Télétype, à savoir le bureau qui traite les communications en provenance et à destination d'autres organismes qui représentent la loi, de la base de données nationale de la criminalité, des mandats locaux, etc. Lorsqu'il est en contact avec le Télétype, il annonce qu'il cherche le numéro de téléphone que les forces de l'ordre utilisent pour appeler le siège fédéral du DMV.

"Qui êtes-vous ?" demande le policier du Télétype.

"Je suis Al. J'appelais le 503 555 5753", dit-il. Il n'a qu'en partie inventé ce numéro : il est en effet probable que le bureau spécial du DMV qui prend les appels des représentants de la loi possède le même code de zone que celui du numéro pour le grand public. Il est presque aussi certain que les trois chiffres (555) suivant le préfixe (503) sont également identiques. Ce dont il a vraiment besoin, ce sont des quatre derniers chiffres.

Le bureau du Télétype d'un shérif ne reçoit pas les appels du public. Et l'appelant possède déjà la plus grande partie du numéro. Manifestement, il est habilité.

"C'est le 503 555 6127", dit l'officier.

Ainsi, Éric connaît désormais le numéro de téléphone spécial que les représentants de la loi appellent. Mais ce seul numéro ne le satisfait pas ; le bureau doit posséder bien plus de numéros que cette ligne unique, et Éric a besoin de connaître le nombre de lignes existantes, ainsi que le numéro de téléphone de chaque ligne.

Le commutateur

Pour mener à bien son plan, Éric doit accéder au commutateur téléphonique qui gère les lignes des représentants de la loi au sein du DMV. Il appelle le service des télécoms de l'État et prétend qu'il fait partie de Nortel, le fabricant du DMS-100, l'un des commutateurs commerciaux les plus répandus : "Pouvez-vous me passer, s'il vous plaît, un technicien qui travaille sur le DMS-100 ?".

Quand il a le technicien au bout du fil, il annonce qu'il travaille au centre d'assistance technique de Nortel au Texas (le *Nortel Technical Assistance Support*), et explique qu'il est en train d'y créer une base de données centrale afin d'appliquer les dernières mises à jour logicielles à tous les commutateurs. Comme tout sera fait à distance, les techniciens n'ont pas à intervenir. Mais il a besoin du numéro d'appel entrant du commutateur pour effectuer les mises à jour directement depuis le centre d'assistance technique.

Cela paraît parfaitement plausible, et le technicien indique le numéro à Éric. Celui-ci peut désormais appeler directement l'un des commutateurs téléphoniques de l'État.

Pour se défendre contre les intrus extérieurs, les commutateurs commerciaux de ce type sont protégés par des mots de passe, exactement comme les réseaux informatiques des entreprises. Tout bon manipulateur qui a quelque connaissance en piratage téléphonique sait que les commutateurs Nortel proposent un nom de compte par défaut pour les mises à jour de logiciels : NTAS (sigle de *Nortel Technical Assistance Support* ; ils ne sont pas allés chercher bien loin !). Mais le mot de passe ? Éric essaie plusieurs fois, en choisissant à chaque fois parmi les mots de passe les plus couramment utilisés, ou qui sembleraient évidents en l'occurrence. "NTAS", comme pour le nom de compte, ne marche pas. Pas plus que "helper" ou "patch".

Puis il essaie "update"[1]… et ça marche. Classique ! Utiliser un mot de passe évident, facile à deviner, est à peine mieux que de ne pas en utiliser du tout.

Le fait d'être à la pointe dans son domaine facilite les choses, et Éric en sait probablement autant sur ce commutateur et sur la façon de le programmer et de le dépanner que le technicien lui-même. Maintenant qu'il est à même d'accéder au commutateur en tant qu'utilisateur autorisé, il dispose d'un

1. N.D.T. : Mise à jour.

contrôle total sur les lignes téléphoniques qu'il ciblait. Depuis son ordinateur, il interroge le commutateur sur le numéro de téléphone du DMV réservé aux représentants de la loi, à savoir 555 6127. Il découvre l'existence de dix-neuf autres lignes dans le même service. À l'évidence, on y traite un gros volume d'appels.

À chaque appel entrant, le commutateur est programmé pour trouver une ligne non occupée parmi les vingt lignes utilisées.

Éric choisit la ligne numéro dix-huit dans la série, et il saisit le code qui ajoute un renvoi d'appel vers cette ligne. En guise de numéro de renvoi d'appel, il indique le numéro de téléphone de son nouveau téléphone mobile à carte… et bon marché, du type de celui que les dealers affectionnent particulièrement, car ils sont suffisamment bon marché pour être jetés une fois le travail accompli.

Maintenant que le renvoi d'appel est activé sur la dix-huitième ligne, dès que les dix-sept lignes seront occupées, l'appel entrant suivant ne sonnera pas dans le bureau du DMV mais sera relayé vers le téléphone mobile d'Éric. Il s'assied et attend.

Un appel au DMV

Peu avant 8 heures, ce matin-là, le téléphone sonne. C'est cette partie qui est la meilleure, la plus savoureuse… Voici Éric parlant avec un policier, c'est-à-dire quelqu'un qui a autorité pour venir l'arrêter, ou pour obtenir un mandat de perquisition et organiser une descente pour rassembler des preuves contre lui.

Et cet appel est suivi de toute une série d'appels de policiers, auxquels Éric répond, l'un après l'autre. Un jour qu'il déjeunait avec des amis dans un restaurant, il lui est même arrivé de recevoir un appel toutes les cinq minutes ou presque, et d'écrire les informations qu'on lui transmettait sur une nappe en papier avec un stylo d'emprunt. Encore aujourd'hui, il trouve vraiment cet épisode hilarant.

Mais s'entretenir avec des officiers de police ne déconcerte aucunement tout bon manipulateur. En fait, les frissons que ressent Éric à abuser ces représentants de la loi ajoutent encore certainement à son plaisir.

Aux dires d'Éric, les appels se déroulaient à peu près comme suit :

"DMV, en quoi puis-je vous aider ?"

"Ici le détective Andrew Cole."

"Bonjour, détective. Que puis-je pour vous ?"

"J'ai besoin d'un *Soundex* pour le permis de conduire 0005602789" disait-il, en employant un terme courant dans les forces de l'ordre pour demander une photo. Ce service est utile pour les policiers, par exemple, qui s'apprêtent à arrêter un suspect et qui veulent savoir à quoi il ressemble.

"Bien sûr, donnez-moi quelques instants pour trouver l'enregistrement" répondait Éric. "À propos, détective Cole, quelle est votre agence ?"

"Jefferson County". Puis Éric posait les questions importantes : "Quel est votre code de demandeur ? Votre numéro de permis de conduire ? Votre date de naissance ?".

Le détective donnait alors tous les renseignements qui permettaient de l'identifier et Éric faisait semblant de vérifier les informations. Il lui annonçait ensuite qu'elles étaient correctes et lui demandait ce qu'il voulait exactement que le DMV recherche pour lui. Il faisait semblant d'entamer la recherche, en tapotant sur son clavier de sorte que son interlocuteur l'entende, puis disait à peu près ceci : "Oh, non, mon ordinateur vient encore de tomber en panne. Désolé, détective, mon ordinateur a fait des siennes toute la semaine. Pourriez-vous rappeler afin de joindre un autre employé ?"

Ainsi, il mettait fin à l'appel sans éveiller le moindre soupçon quant à son incapacité à satisfaire la requête de son interlocuteur. Entre-temps, Éric avait dérobé une identité dont il pourrait se servir pour obtenir des informations confidentielles auprès du DMV chaque fois qu'il en aurait besoin.

Après avoir pris des appels pendant quelques heures et obtenu des dizaines de codes de demandeurs, Éric a appelé le commutateur et a désactivé le renvoi d'appels.

Par la suite, et ce pendant de nombreux mois, il a pu remplir les missions que lui confiaient des sociétés d'investigation totalement légales mais qui ne voulaient pas savoir comment il se procurait ses informations. Dès qu'il en avait besoin, il rappelait le commutateur, activait le renvoi d'appels et collectait des informations sur une autre série de policiers.

Analyse de l'arnaque

Revenons sur les ruses qu'Éric a employées avec différentes personnes pour que sa supercherie fonctionne. Il obtient d'abord d'un adjoint du shérif employé au Télétype qu'il fournisse un numéro de téléphone confidentiel du DMV à un parfait inconnu, qu'il croit être un officier mais auquel il ne demande aucune justification.

Ensuite, un employé du service des télécoms de l'État fait de même : il ne met pas en cause les dires d'Éric, qui se présente comme l'employé d'un fabricant d'équipements, et il lui fournit un numéro de téléphone pour appeler le commutateur qui dessert le DMV.

Si Éric peut se servir du commutateur, c'est dans une large mesure grâce à la faiblesse des pratiques de sécurité mises en place par le fabriquant, puisque le même nom de compte est utilisé sur tous les commutateurs. Cette négligence ouvre une voie royale au manipulateur qui cherche à deviner les mots de passe puisque, une fois encore, les techniciens qui s'occupent des commutateurs, comme presque tout le monde, choisissent des mots de passe faciles à retenir.

Maintenant qu'il a accès au commutateur, Éric met en place le renvoi des appels de l'une des lignes téléphoniques entre les représentants de la loi et le DMV vers son propre téléphone portable.

Vient alors la partie la plus savoureuse : l'un après l'autre, il amène les représentants de la loi à lui révéler non seulement leurs codes de demandeur, mais également leurs propres données d'identification, ce qui permet ensuite à Éric de se faire passer pour eux.

Même si Éric possédait certaines connaissances techniques nécessaires pour mener à bien ce tour de force, il n'aurait pas réussi sans l'aide de cette série de personnes qui ignoraient qu'elles s'adressaient à un imposteur.

Cette histoire illustre à nouveau le fait que les gens ne se demandent pas : "Pourquoi cette personne s'adresse-t-elle à moi ?". Pourquoi l'officier du Télétype donne-t-il cette information à une personne qu'il ne connaît pas — ou, ici, un étranger qui *se fait passer* pour un adjoint du shérif — au lieu de suggérer qu'il s'adresse à un autre adjoint ou à son propre supérieur ? Une fois de plus, la seule réponse que je puisse apporter est que les gens posent rarement cette question. Il ne leur vient pas à l'esprit de la poser ? Ils ne veulent pas paraître méfiants et peu serviables ? Peut-être. Une explication plus poussée ne serait que conjecture. Et les manipulateurs ne s'en soucient guère ; seul leur importe que cet état de fait facilite l'obtention d'informations qui, sans cela, auraient été très difficiles à se procurer.

Le message de Mitnick

Si votre entreprise est équipée d'un commutateur téléphonique, que fera la personne qui en a la charge si le vendeur de cet équipement l'appelle et lui demande le numéro d'appel entrant ? Et au passage, cette personne a-t-elle déjà changé le mot de passe par défaut du commutateur ? Ce mot de passe est-il un mot tout bête que l'on trouve dans le dictionnaire, et par conséquent facile à deviner ?

EMPÊCHER L'ARNAQUE

Correctement utilisé, un code de sécurité offre une protection supplémentaire précieuse. En revanche, une mauvaise utilisation d'un code de sécurité peut être même pire que l'absence de code, car cela donne l'illusion d'une sécurité. Quel intérêt d'avoir des codes, si vos employés ne les gardent pas secrets ?

Toute entreprise qui a besoin de codes de sécurité verbaux doit indiquer clairement à ses employés quand et comment les utiliser. Si elle avait suivi une formation appropriée, la personne de la première histoire de ce chapitre n'aurait pas eu besoin de se fier à son instinct — dont le manipulateur est d'ailleurs facilement venu à bout — lorsqu'un étranger lui a demandé de lui fournir un code de sécurité. Elle a senti qu'on ne devait pas lui demander ce renseignement dans de telles circonstances, mais en l'absence d'un règlement de sécurité clair — et de bon sens —, elle l'a donné.

Les directives en matière de sécurité devraient également définir la procédure qu'un employé doit suivre lorsqu'il flaire une demande louche concernant un code de sécurité. Tous les employés doivent savoir qu'il leur faut signaler immédiatement la moindre demande relative à des données d'authentification, tels le code ou le mot de passe du jour, si elle est formulée dans des circonstances douteuses. Lorsqu'une tentative de contrôle d'identité d'un demandeur échoue, ils doivent également le signaler.

L'employé doit au minimum noter le nom, le numéro de téléphone et le bureau ou le service de l'appelant, puis raccrocher. Avant de rappeler ce dernier, il doit vérifier que l'entreprise compte effectivement un employé à ce nom, et que le numéro de téléphone fourni par l'interlocuteur correspond à celui indiqué dans le répertoire (papier ou en ligne) de l'entreprise. Le plus souvent, cette tactique simple suffira pour s'assurer que l'appelant est bien celui qu'il prétend être.

Les vérifications deviennent un peu plus complexes lorsque le répertoire téléphonique de l'entreprise est imprimé plutôt qu'en ligne. Des personnes sont embauchées, certaines démissionnent, d'autres changent de service, d'emploi, de numéro de téléphone. Le répertoire papier est déjà obsolète le lendemain de son édition, avant même d'être distribué. Même les répertoires en ligne ne sont pas toujours fiables car les manipulateurs savent comment les modifier. Si un employé ne peut pas vérifier un numéro de téléphone par le biais d'une source indépendante, il doit pouvoir le faire en utilisant d'autres moyens, par exemple en contactant son directeur.

Partie 3

Menaces d'intrusion

Chapitre 10

L'intrusion physique

Pourquoi est-il si facile, pour quelqu'un qui vient de l'extérieur, de se faire passer pour un salarié de l'entreprise de manière si convaincante que même des personnes tout à fait conscientes des problèmes de sécurité s'y laissent prendre ? Pourquoi est-il si facile de tromper des employés qui sont parfaitement informés des procédures de sécurité, qui sont soupçonneux vis-à-vis de personnes qu'ils ne connaissent pas personnellement et qui cherchent à protéger les intérêts de leur entreprise ?

Réfléchissez à ces questions tout en lisant les témoignages de ce chapitre.

L'AGENT DE SÉCURITÉ EMBARRASSÉ

Date et heure : mardi 17 octobre, 2 h 16 du matin.

Lieu : Skywatcher Aviation Inc., une usine dans la banlieue de Tucson, Arizona.

Le point de vue de l'agent de sécurité

Leroy Greene se sentait beaucoup mieux quand il entendait claquer ses talons de cuir sur le sol du hall de l'usine déserte que lorsqu'il passait sa nuit devant les écrans vidéo du bureau de la sécurité. Au bureau, à part observer les écrans, il n'avait rien le droit de faire, pas même de lire un magazine. Il devait rester assis à observer les images fixes affichées sur les moniteurs, où rien ne bougeait jamais.

Une ronde dans les halls lui permettait au moins de se dégourdir, et quand il pensait à balancer ses bras et ses épaules en rythme, ça lui faisait même un peu d'exercice. Et encore, ce n'était pas vraiment de l'exercice pour quelqu'un

qui avait été plaqueur dans l'équipe de football américain de son lycée. Enfin, un boulot, c'est un boulot.

Un soir, alors qu'il tourne à l'angle sud-ouest et s'engage sur la coursive qui surplombe l'immense hall d'assemblage, son regard tombe soudain sur deux personnes qui longent la rangée d'hélicoptères en cours de montage. Les deux personnes s'arrêtent et semblent se montrer mutuellement des détails sur les appareils. Étrange, à cette heure de la nuit. "Je ferais mieux d'aller voir", pense-t-il.

Leroy se dirige vers un escalier qui le mène directement derrière les deux personnes, et celles-ci ne prennent conscience de sa présence que lorsqu'il est à leurs côtés. "Bonjour. Je peux voir vos badges, s'il vous plaît ?" Leroy essaye toujours de garder une voix douce en de telles circonstances ; il sait que sa carrure est suffisamment impressionnante.

"Bonjour, Leroy", dit l'un d'eux, lisant le nom qui se trouve sur le badge. "Je suis Tom Stilton, du service marketing du siège, à Phoenix. Je suis en ville pour des réunions et je voulais montrer à mon ami comment on construit les meilleurs hélicoptères du monde."

"Très bien. Votre badge, s'il vous plaît." Leroy ne peut s'empêcher de les trouver très jeunes. Le type du marketing semble sortir tout droit du lycée, et l'autre, dont les cheveux lui descendent jusqu'aux épaules, ne doit pas avoir plus de quinze ans.

Le garçon aux cheveux courts met la main dans sa poche pour y chercher son badge, puis commence à tapoter ses autres poches. "Bon sang, dit-il, j'ai dû le laisser dans la voiture. Je peux aller le chercher — j'en ai pour dix minutes pour aller jusqu'au parking et revenir."

Leroy a sorti son bloc-notes. "Comment avez-vous dit que vous vous appeliez ?" demande-t-il, et il note soigneusement la réponse. Puis il leur demande de les suivre jusqu'au bureau de la sécurité. Dans l'ascenseur qui les mène au deuxième étage, Tom se met à bavarder, racontant qu'il n'est dans l'entreprise que depuis six mois, et qu'il espère ne pas avoir d'ennuis à cause de ça.

Dans le bureau de la sécurité, les deux autres veilleurs de nuit se joignent à Leroy pour questionner le duo. Stilton donne son numéro de téléphone, dit que sa supérieure hiérarchique est Judy Underwood et indique son numéro de téléphone ; l'ordinateur confirme ces informations. Leroy prend à part les deux autres veilleurs de nuit pour discuter de la marche à suivre. Aucun ne veut prendre de risques ; tous trois considèrent qu'il vaut mieux appeler la supérieure, même s'il faut pour cela la réveiller au milieu de la nuit.

C'est Leroy qui appelle Judy Underwood ; il explique qui il est et demande si un certain Tom Stilton travaille bien pour elle. Elle paraît à moitié endormie. "Oui", dit-elle.

"Eh bien nous l'avons trouvé sur la chaîne de montage à 2 h 30 du matin sans badge d'identité."

"Je vais lui parler", répond Judy Underwood.

Stilton prend le combiné et s'excuse : "Judy, je suis vraiment désolé que ces types te réveillent au milieu de la nuit. J'espère que tu ne m'en voudras pas pour ça."

Il écoute quelques instants, puis il dit : "Je devais être ici ce matin de toute façon, pour la réunion à propos du nouveau communiqué de presse. Au fait, tu as eu l'e-mail concernant le contrat Thompson ? Il faut qu'on se voie avec Jim lundi pour en reparler. Et on déjeune toujours ensemble mardi, non ?"

Il écoute quelques instants de plus, puis lui souhaite une bonne nuit et raccroche.

Leroy est surpris : il pensait qu'il récupérerait le combiné pour que la dame lui confirme que tout allait bien. Il envisage un moment de la rappeler, mais change d'avis. Il l'avait déjà dérangée une fois au milieu de la nuit ; s'il appelait une deuxième fois, elle finirait peut-être par en avoir assez et pourrait se plaindre à son chef. Il préfère ne pas faire de vagues.

"Ça va si je montre le reste de la chaîne de montage à mon ami ?" demande Stilton. "Vous voulez vous joindre à nous pour nous surveiller ?"

"Allez-y, dit Leroy, faites votre tour. N'oubliez pas votre badge la prochaine fois. Et informez la sécurité si vous voulez visiter l'usine en dehors des heures de bureau — c'est la règle."

"Je m'en souviendrai", dit Stilton. Et ils partent.

Dix minutes à peine après leur départ, le téléphone sonne dans le bureau de la sécurité. C'était Judy Underwood. "C'était qui, ce type ?" demande-t-elle. Elle dit qu'elle a essayé de lui poser des questions, mais qu'il n'arrêtait pas de parler de leur déjeuner commun, et qu'elle n'avait aucune idée de qui il était.

Les agents de sécurité appellent l'entrée de l'usine et le surveillant du parking. Tous deux confirment que les deux jeunes sont partis quelques minutes plus tôt.

Quand il raconte cette histoire, Leroy termine toujours en disant : "Je me suis fait passer un sacré savon par mon patron. J'ai eu de la chance d'avoir gardé mon boulot."

L'histoire vue par Joe Harper

Depuis plus d'un an, Joe Harper, âgé de dix-sept ans, s'amusait à pénétrer dans des bâtiments surveillés, parfois de jour, parfois de nuit, juste pour voir jusqu'où il pouvait aller. Fils d'un musicien et d'une serveuse qui travaillaient tous deux de nuit, Joe n'avait pas trouvé de meilleure occupation pour tuer le temps. Son récit fournit des informations intéressantes sur les tenants et les aboutissants de l'affaire.

"J'ai un ami qui s'appelle Kenny et qui veut devenir pilote d'hélicoptère. Il m'a demandé si je pouvais le faire entrer dans l'usine Skywatcher pour voir la chaîne de montage où sont assemblés les hélicoptères. Il sait que j'ai déjà réussi à m'introduire dans d'autres bâtiments. Ce qui me procure des sensations fortes, c'est d'arriver à entrer dans un endroit interdit.

Mais on n'entre pas comme ça dans une usine ou dans les locaux d'une entreprise. Il faut réfléchir au préalable, tout planifier et effectuer une reconnaissance complète de la cible. Vérifier sur le site Web de la société les noms et fonctions, l'organigramme et les numéros de téléphone. Parcourir les communiqués de presse et les articles des magazines. Mes recherches préliminaires sont ma meilleure mesure de sécurité : quand je suis confronté à quelqu'un, je dois pouvoir montrer que ma connaissance de l'entreprise vaut celle de n'importe lequel de ses salariés.

Où commencer ? J'ai d'abord cherché, sur Internet, où l'entreprise était établie, et j'ai vu que leur siège social était à Phoenix. J'ai appelé sur place et ai demandé le service marketing. Toutes les entreprises ont un service marketing. Une femme a répondu ; j'ai dit que je représentais Blue Pencil Graphics, que je voulais proposer les services de ma société à Skywatcher, et j'ai demandé à qui je devais m'adresser. Elle m'a dit qu'il fallait voir avec Tom Stilton. J'ai demandé son numéro de ligne directe ; elle n'a pas accepté de me le donner, mais elle m'a mis en communication avec son poste. C'est sa boîte vocale qui a décroché, et le message disait : "Tom Stilton, service graphique, poste 3147, laissez votre message après le bip". La standardiste ne donnait pas les numéros de poste, mais lui l'indiquait sur sa boîte vocale. Tout allait bien : je disposais maintenant de son nom et de son numéro de poste.

Un deuxième appel au même endroit : "Bonjour, je cherche à joindre Tom Stilton, mais il est absent. J'ai une petite question à poser à son chef". Sa chef était également absente, mais une fois mes appels terminés, je connaissais son nom ainsi que son extension, qu'elle avait elle aussi obligeamment laissé sur sa boîte vocale.

L'agent de surveillance du hall d'entrée de l'usine ne posait pas de problème, mais je suis passé à côté de l'usine et j'ai vu que le parking était entouré d'un grillage. Quand il y a un grillage, il y a un gardien qui vérifie votre identité à l'entrée. Et la nuit, il est probable qu'il note aussi les numéros de la plaque d'immatriculation. Il fallait donc que j'achète une vieille paire de plaques au marché aux puces.

Mais auparavant, il fallait que j'obtienne le numéro de téléphone de la guérite du gardien. J'ai attendu un peu. Ainsi, si je tombais sur la même standardiste, elle ne reconnaîtrait pas ma voix. J'ai donc appelé en demandant : "Nous avons eu des informations comme quoi le téléphone du poste situé Ridge Road fonctionnait mal ; est-que le problème est réglé ?". Elle dit qu'elle n'en savait rien, mais qu'elle me mettait en communication.

Le gardien a répondu : "Poste de Ridge Road, ici Ryan". J'ai dit : "Bonjour Ryan, ici Ben. Vous avez eu des ennuis avec vos lignes de téléphone ?". Ryan est un agent de sécurité mal payé, mais il a dû suivre une formation sur la sécurité, parce qu'il a demandé : "Ben comment ? Quel est votre nom de famille ?". J'ai continué à parler comme si je n'avais rien entendu : "Quelqu'un a signalé un problème concernant votre ligne de téléphone".

Je l'ai entendu éloigner le combiné de l'oreille et demander : "Bruce, Roger, il y a eu un problème avec le téléphone ?". Il m'a ensuite répondu : "Non, il n'y a pas eu de problème, à notre connaissance".

"Combien de lignes de téléphone avez-vous ?"

Entre-temps, il avait oublié qu'il n'avait pas obtenu mon nom de famille. "Deux", m'a-t-il répondu.

"Et là, nous sommes sur quelle ligne ?"

"La 3140."

Le tour était joué. "Et toutes les deux fonctionnent sans problème ?"

"Apparemment."

"Bon, écoutez, Ryan. Si vous avez le moindre problème avec le téléphone, appelez-nous au service des télécoms, à tout moment. Nous sommes là pour vous aider."

Mon ami et moi avons décidé de visiter l'usine le soir même. En fin d'après-midi, j'ai appelé le gardien du parking : "Bonsoir, ici Tom Stilton, du marketing. Nous sommes sur un projet avec des délais très serrés, et il y a deux collègues qui vont passer chez vous. Ils ne seront sans doute pas là avant une ou deux heures du matin. Vous serez encore là ?".

Il était heureux de pouvoir dire que non, qu'il finissait son service à minuit.

J'ai dit : "Dans ce cas, vous voulez bien laisser une note pour celui qui vous remplace ? Quand mes deux collègues arriveront et qu'ils diront qu'ils viennent voir Tom Stilton, laissez-les entrer, d'accord ?".

Il m'a répondu qu'il n'y avait pas de problème. Il a noté mon nom, mon service, ainsi que mon numéro de poste, et a indiqué qu'il s'en occuperait.

Nous sommes arrivés à l'entrée du parking un peu après deux heures, j'ai donné le nom de Tom Stilton, et un gardien à moitié endormi nous a indiqué par où passer et où se garer.

Lorsque nous sommes entrés dans le bâtiment, il y avait un autre agent de surveillance dans le hall d'entrée, ce qui est normal en dehors des heures ouvrables. J'ai dit au gardien que j'avais à terminer un rapport pour le lendemain matin, et que l'ami qui m'accompagnait voulait visiter l'usine. "C'est un fana des hélicoptères, ai-je dit, il veut apprendre à les piloter." Il m'a demandé mon badge. J'ai mis la main dans ma poche, puis tapoté mes autres poches ; j'ai raconté que je l'avais laissé dans la voiture et que j'allais le chercher. "Il y en a pour dix minutes", ai-je dit. "Ça ira, a-t-il répondu, donnez-moi juste votre nom et votre signature."

La visite de l'usine, c'était super ! Du moins jusqu'à ce que ce colosse de Leroy nous arrête.

Dans le bureau de la sécurité, je me suis dit que quelqu'un d'extérieur à l'entreprise aurait l'air nerveux et inquiet. Par conséquent, j'ai commencé à prendre un air agacé, comme si j'étais vraiment celui que je prétendais être, et qu'il était énervant qu'on ne veuille pas me croire.

Lorsqu'ils ont commencé à dire qu'ils allaient appeler la femme qui était censée être mon supérieur hiérarchique, je me suis dit que ce serait peut-être le bon moment pour essayer de fuir. Mais il restait le poste de garde du parking : même si nous parvenions à sortir du bâtiment, il leur suffirait de fermer la grille d'entrée pour nous coincer.

Quand Leroy a appelé la chef de Stilton et m'a passé le combiné, la dame a commencé à crier : "Qu'est-ce qui se passe ? Qui êtes vous ?". J'ai continué à parler en simulant une discussion tranquille, puis j'ai raccroché.

Combien de temps faut-il pour trouver quelqu'un qui peut donner un numéro de téléphone de l'entreprise au milieu de la nuit ? J'estimais que nous disposions de moins de quinze minutes pour sortir avant que cette femme ne parvienne à rappeler le bureau de la sécurité pour l'informer du problème.

Nous sommes sortis en allant aussi vite que possible sans avoir l'air pressés. Et nous avons été soulagés quand le gardien, à l'entrée du parking, nous a fait signe de passer."

Analyse du stratagème

Il est intéressant de noter que cette intrusion est effectivement l'œuvre d'adolescents. En l'occurrence, ceux-ci n'avaient aucune intention criminelle : pour eux, il s'agissait de voir s'ils pouvaient réussir un coup de ce type. Mais si deux adolescents y sont parvenus si aisément, des cambrioleurs, des espions ou des terroristes y seraient parvenus encore plus facilement.

Comment se fait-il que trois agents de sécurité expérimentés aient permis à deux intrus de repartir ? Et pas n'importe quels intrus : deux adolescents assez jeunes pour que n'importe quelle personne sensée ait des soupçons à leur égard.

Leroy a effectivement eu des soupçons, dans un premier temps. Il a eu raison d'accompagner les deux intrus jusqu'au bureau de la sécurité, d'interroger celui qui disait être Tom Stilton et de vérifier son nom et son numéro de téléphone. Il a également eu raison d'appeler le supérieur hiérarchique de Tom Stilton.

Mais en définitive, il a été abusé par l'assurance et l'indignation du jeune homme. Ce n'était pas le comportement d'un intrus ou d'un voleur : seul un véritable salarié se serait comporté de cette manière — du moins Leroy le pensait-il alors. On aurait dû apprendre à ce dernier à se fonder sur des méthodes d'identification sûres, pas sur des impressions.

Pourquoi n'a-t-il pas été plus soupçonneux quand le jeune homme a raccroché sans lui rendre le combiné afin que Judy Underwood puisse confirmer que Tom Stilton avait bien une raison de se trouver dans l'usine à cette heure tardive ?

Leroy a été dupé par une ficelle si grosse qu'il aurait dû la détecter tout de suite. Mais plaçons-nous maintenant de son point de vue : celui d'un jeune à peine sorti de l'école, qui craint de perdre son emploi et d'avoir des ennuis s'il dérange une deuxième fois un chef de service en pleine nuit. Si vous aviez été à sa place, auriez-vous passé ce deuxième appel ?

Bien entendu, le deuxième appel n'était pas la seule alternative possible. Qu'est-ce que l'agent de sécurité aurait pu faire d'autre ?

Avant même son premier appel, il aurait pu demander aux deux adolescents un quelconque papier d'identification comportant une photo. Dans la mesure où ils étaient venus en voiture, au moins l'un d'entre eux devait posséder un permis de conduire. Comme ils avaient donné de faux noms, ils auraient été immédiatement démasqués (des professionnels se seraient quant à eux munis de faux papiers). Leroy aurait donc dû vérifier leur identité et

noter les informations correspondantes. S'ils avaient prétendu tous deux ne pas avoir de papiers, il aurait dû les accompagner jusqu'à leur voiture afin de retrouver le badge que le faux Tom Stilton aurait laissé.

Le message de Mitnick

Les manipulateurs ont généralement une personnalité agréable. Ils réfléchissent vite et bien. Par ailleurs, ils savent interrompre la continuité des pensées de leurs victimes afin de s'assurer de leur coopération. S'imaginer qu'on n'est pas vulnérable vis-à-vis de ce type de manipulation, c'est sous-estimer les capacités et "l'instinct de tueur" du manipulateur.

Le bon manipulateur, lui, ne sous-estime jamais son adversaire.

Après l'appel téléphonique, l'un des agents de sécurité aurait dû rester avec le duo jusqu'à ce qu'ils quittent le bâtiment et retrouvent leur voiture. L'agent aurait alors pu noter le numéro d'immatriculation. S'il avait été observateur, il aurait constaté que les plaques (achetées au marché aux puces) étaient dépourvues de sceau officiel — raison de plus pour ne pas laisser repartir les deux adolescents.

LA FOUILLE DES POUBELLES

Rares sont ceux qui accordent une grande importance à la nature de ce qu'ils jettent à la poubelle chez eux : factures de téléphone, facturettes de carte bancaire, emballage de médicaments, relevés de banque, papiers se rapportant à leur travail, etc.

Au travail, les employés doivent prendre conscience que certaines personnes fouillent les poubelles pour y trouver des informations utiles.

Lorsque j'étais au lycée, je fouillais dans les déchets des compagnies de téléphone locales, souvent seul, parfois accompagné par des amis qui voulaient comme moi se renseigner davantage sur une compagnie. Avec l'expérience, on apprend toutes sortes d'astuces, par exemple qu'il faut tout faire pour éviter les sacs qui proviennent des toilettes, et qu'il est indispensable de porter des gants.

Ce type d'occupation n'était pas particulièrement agréable en soi, mais sa contrepartie était extraordinaire : on récupérait des répertoires téléphoniques internes, des manuels d'utilisation d'ordinateurs, des listes de salariés, des documents indiquant comment programmer les commutateurs, et bien plus encore ! Le tout était accessible à quiconque voulait bien se baisser pour le ramasser.

En arrivant, je choisissais quelques boîtes en carton, les sortais de la pile et les mettais de côté. Si quelqu'un venait me demander ce que je faisais, je disais qu'un de mes amis allait déménager et que je cherchais des cartons pour emballer ses affaires. Jamais aucun agent de sécurité n'a remarqué que les cartons contenaient des documents que je m'apprêtais à rapporter chez moi. Parfois, il me demandait de partir, auquel cas je m'attaquais au siège social d'une autre compagnie de téléphone.

Je ne sais pas ce qu'il en est aujourd'hui, mais à l'époque, il était facile de repérer les sacs pouvant contenir des documents intéressants. Tout ce qui avait été balayé par terre et tout ce qui venait de la cafétéria se trouvait dans de grands sacs, alors que les corbeilles des bureaux étaient toutes garnies de sacs poubelle blancs, que les équipes de nettoyage sortaient un à un, puis attachaient ensemble.

Lors d'une recherche avec des amis, j'ai trouvé des morceaux de papier déchirés à la main. Quelqu'un s'était donné la peine de transformer les feuilles en morceaux à peine plus grands que des confettis, tous regroupés dans un unique sac poubelle. Nous avons emporté le sac dans un café voisin, l'avons vidé sur une table, puis nous sommes mis à assembler les morceaux.

Nous aimions tous les casse-tête, et ces feuilles étaient pour nous comme un puzzle géant, mais la récompense est allée bien au-delà de la satisfaction d'avoir reconstitué le puzzle : une fois que toutes les feuilles ont été reconstituées, nous disposions de tous les noms d'utilisateurs et de tous les mots de passe de l'un des systèmes d'ordinateurs cruciaux de la compagnie.

Les résultats de nos fouilles valaient-ils la peine, vu le risque encouru ? Assurément, et ce d'autant plus que le risque était nul. Ce qui était vrai jadis l'est encore aujourd'hui : tant qu'on ne se trouve pas illégalement sur une propriété privée, la fouille des poubelles n'a rien d'illégal aux États-Unis[1].

Bien entendu, les phreakers et les hackers ne sont pas les seuls à mettre leur nez dans les poubelles. La police les fouille fréquemment, et toute une série de malfrats, du petit escroc au parrain de la Mafia, doivent en partie leur condamnation aux preuves trouvées par la police dans leurs déchets. Les services de renseignements de tous les pays utilisent depuis longtemps cette méthode.

Ce type de techniques ne sont peut-être pas de celles qu'utiliserait James Bond : les spectateurs préfèrent le voir se battre avec le méchant et aller au lit

1. N.D.T. : En France et en Belgique, en revanche, elle est généralement interdite par arrêté municipal ou par règlement communal.

avec une jeune beauté plutôt que de fouiller dans les poubelles. Mais les "vrais" espions sont moins difficiles quand ils sont susceptibles de trouver des informations parmi les épluchures de bananes, le marc de café, les journaux et les listes de courses, d'autant plus que ces recherches présentent peu de risques.

Le prix des poubelles

Les entreprises jouent également à ce jeu. En juin 2000, les journaux ont annoncé qu'Oracle, dont le président, Larry Ellison, est sans doute le plus farouche adversaire de Microsoft, avait fait appel aux services d'une agence d'investigation qui s'était fait prendre la main dans le sac.

Apparemment, les enquêteurs avaient cherché à obtenir le contenu des poubelles d'une organisation de lobbying soutenue par Microsoft, l'ACT. D'après la presse, l'agence d'investigation aurait envoyé une femme offrir 60 dollars à l'équipe de nettoyage en échange des déchets de l'organisation. Le personnel a refusé. Lorsque la femme a offert 500 dollars à l'ensemble de l'équipe et 200 dollars à son responsable, ils ont à nouveau refusé et ont dévoilé l'affaire au grand jour.

Analyse du stratagème

En fonction de ma propre expérience et de celle d'Oracle, vous vous demandez peut-être pourquoi quiconque prendrait le risque de voler les détritus de quelqu'un.

Pour moi, la raison est que le risque est nul et que les bénéfices peuvent être importants. Bien sûr, on prend plus de risques quand on tente de soudoyer le personnel d'entretien, mais pour qui n'a pas peur de se salir un peu, les pots-de-vin sont inutiles.

Pour le manipulateur, la fouille des poubelles offre un intérêt particulier. Il peut obtenir assez d'informations pour monter son attaque contre l'entreprise ciblée à partir des mémos, des plannings, des lettres, etc., qui dévoilent les noms des personnes, des services, des fonctions et des projets. Les poubelles peuvent également fournir des organigrammes hiérarchiques de l'entreprise, des informations sur sa structure, le calendrier des congés prévus, et ainsi de suite. Tous ces détails peuvent sembler insignifiants pour ceux qui travaillent dans l'entreprise, mais ils peuvent s'avérer précieux pour un manipulateur.

Mark Joseph Edwards, dans son livre *Internet Security with Windows NT*, mentionne des rapports entiers jetés à cause de la présence de quelques coquilles, des mots de passe notés sur des bouts de papier, des messages "En votre absence" avec des numéros de téléphone confidentiels, des chemises comprenant des dossiers complets, des disquettes et des bandes n'ayant été ni effacées ni détruites — autant d'informations qui peuvent aider un assaillant éventuel.

Edwards met ensuite l'accent sur la question suivante : "D'où vient le personnel d'entretien de l'entreprise ? Vous avez peut-être décidé que l'équipe de nettoyage n'aurait pas accès à la salle des ordinateurs de l'entreprise, mais n'oubliez pas les autres corbeilles. Si les agences fédérales considèrent qu'il est nécessaire de vérifier les antécédents des personnes qui ont accès à leurs corbeilles et à leurs destructeurs de documents, vous devriez sans doute en faire autant."

Le message de Mitnick

> Nous n'accordons pas une grande importance à ce que nous jetons chez nous ; pourquoi devrait-il en être autrement sur notre lieu de travail ? Or, vos déchets peuvent constituer un trésor pour vos ennemis. Il est donc essentiel que les salariés d'une entreprise prennent conscience du danger (personnes sans scrupule qui recherchent des informations) et de la vulnérabilité (informations confidentielles non détruites ni effacées).

LE PATRON HUMILIÉ

Personne ne s'est posé de questions quand Harlan Fortis s'est présenté comme tous les lundis matin à son travail, au service des transports du comté, en disant qu'il était parti en hâte de chez lui et qu'il avait oublié son badge. Depuis deux ans qu'elle travaillait dans l'entreprise, l'agent de sécurité avait vu Harlan entrer et sortir du bâtiment tous les jours. Elle lui a donc fourni un badge provisoire, lui a demandé de signer pour en accuser réception, et l'a laissé passer.

L'affaire a éclaté deux jours plus tard et l'histoire s'est répandue dans le service comme une traînée de poudre. La moitié de ceux qui l'ont entendue n'ont pas voulu y croire, et ceux qui y ont cru ont été partagés entre le rire et la compassion pour le pauvre homme.

Après tout, George Adamson était quelqu'un de compréhensif et d'aimable, le meilleur chef de service qu'ils aient jamais eu. Il ne méritait pas ce qui lui arrivait — pour peu que l'histoire fût vraie, bien sûr.

Le problème avait commencé quand, le vendredi soir précédent, George Adamson avait appelé Harlan Fortis dans son bureau pour l'informer aussi gentiment que possible qu'à partir du lundi suivant, Harlan changerait de poste. Il était muté au service des égouts. Pour Harlan, c'était pire qu'être renvoyé : c'était humiliant. Mais il ne se laisserait pas faire.

Le soir-même, il s'assoit sous son porche en observant les gens qui rentrent chez eux après leur journée de travail. Il finit par repérer l'individu qu'il cherche, un garçon du voisinage nommé David, qu'on surnomme le petit génie de l'informatique. Il l'arrête, lui offre un coca acheté spécialement pour l'occasion, puis lui propose un marché : la dernière console de jeu et six cartouches en échange d'un peu d'aide en informatique et la promesse de tenir sa langue.

Harlan détaille son plan sans fournir de détails compromettants, et David accepte. Il explique à Harlan ce qu'il doit faire. Harlan suit les instructions : il achète un modem, pénètre dans l'entreprise, trouve un ordinateur avec une prise de téléphone libre à proximité et branche le modem. La phase suivante est la plus risquée : il s'assoit devant l'ordinateur, installe le logiciel de contrôle à distance et le met en route. L'occupant habituel du bureau aurait pu entrer à tout moment, et n'importe qui, passant à proximité, aurait pu voir qu'il ne se trouvait pas dans son propre bureau. Harlan est tellement tendu qu'il arrive à peine à lire les instructions que David a notées sur un bout de papier. Finalement, la tâche effectuée, il parvient à sortir du bâtiment sans se faire remarquer.

Mise en place du traquenard

David passe le soir même à l'heure du dîner et ils s'installent tous deux devant l'ordinateur de Harlan. Quelques minutes plus tard, David s'est connecté au modem, a accédé à l'ordinateur distant, puis à celui de George Adamson, ce qui n'était pas très difficile puisque George n'avait jamais le temps de prendre des mesures de précaution, notamment en changeant de mot de passe. En outre, comme il demandait sans cesse à telle ou telle personne de télécharger un fichier ou d'envoyer un e-mail à sa place, tout le monde avait fini par connaître son mot de passe.

Après quelques recherches, ils dénichent un fichier nommé PrésentationBudget2002.ppt, que David télécharge sur l'ordinateur de Harlan. Celui-ci demande au garçon de rentrer à la maison et de revenir quelques heures plus tard.

Quand David est de retour, Harlan lui demande de se reconnecter à l'ordinateur du service des transports et de remettre le fichier à l'endroit où il l'avait trouvé, en remplaçant l'ancienne version. Harlan montre la console de jeux à David et lui dit que si tout va bien, il l'aura le lendemain.

Une surprise pour George

On pourrait croire que les séances du conseil du comté consacrées au budget sont trop rébarbatives pour attirer beaucoup de monde mais, en réalité, la salle du conseil était ce jour-là pleine à craquer : journalistes, représentants de différents groupes d'intérêts, citoyens ordinaires et même deux équipes de télévision étaient présents.

Pour George Adamson, ces séances représentaient toujours un enjeu considérable. C'était le conseil du comté qui tenait les cordons de la bourse, et si la présentation de George n'était pas convaincante, le budget des transports serait réduit. Tout le monde commencerait alors à se plaindre des nids de poule, des feux hors service et des carrefours dangereux, on le rendrait responsable, et il passerait une très mauvaise année. Mais lorsque son tour est venu ce soir-là, il était confiant. Il avait travaillé sur cette présentation PowerPoint pendant six semaines, et il l'avait essayée en présence de sa femme, de ses subordonnés directs et de quelques amis proches. Tout le monde s'accordait à dire que c'était la meilleure présentation qu'il ait jamais faite.

Les trois premières images PowerPoint étaient très encourageantes. Pour changer, tous les membres du conseil étaient attentifs, et son message passait bien.

Et soudain, tout se détraque. La quatrième image devait comprendre la photo de la section d'autoroute qui venait d'être construite, devant un coucher de soleil ; à sa place, George Adamson voit apparaître la photo d'une jeune femme provenant d'un magazine tel que *Playboy* ou *Penthouse*. Il entend la réaction de surprise du public et se hâte d'appuyer sur la touche de son ordinateur portable pour passer à l'image suivante.

Mais l'image suivante est pire. Sur celle-là, plus rien n'est laissé à l'imagination.

Alors qu'il essaye de faire disparaître l'image, quelqu'un coupe l'alimentation du projecteur tandis que le président de la séance, après un violent coup de marteau, crie dans le vacarme ambiant que la séance est ajournée.

Analyse du stratagème

En utilisant les connaissances informatiques d'un adolescent, un employé mécontent est parvenu à accéder à l'ordinateur du chef de son service, à télécharger une présentation PowerPoint importante et à remplacer une

partie des images par des photographies destinées à mettre son ancien patron dans une situation très embarrassante.

Le modem étant connecté d'une part à une prise de téléphone, d'autre part à l'un des ordinateurs de l'entreprise, le jeune hacker a pu se connecter. Une fois le logiciel de contrôle à distance en place, l'adolescent a pu accéder à n'importe quel fichier du système. Comme l'ordinateur était connecté au réseau, et que le nom d'utilisateur et le mot de passe du patron étant connus, l'accès à ses fichiers a été un jeu d'enfant.

En comptant le temps nécessaire pour scanner les images, l'opération entière n'a pris que quelques heures. En revanche, il a fallu plusieurs années pour que les dommages causés à la réputation de la victime disparaissent.

Le message de Mitnick

La très grande majorité des employés mutés, renvoyés ou licenciés ne posent pas de problème. Toutefois, il suffit d'un seul pour qu'une entreprise prenne conscience, mais trop tard, des mesures qui auraient dû être appliquées pour éviter un désastre.

L'expérience et les statistiques prouvent que le principal danger, pour une entreprise, vient de l'intérieur. Ce sont les salariés de l'entreprise qui savent le mieux où se trouvent les informations importantes, et où frapper pour causer les dégâts les plus importants.

UNE JEUNE FEMME AMBITIEUSE

Par une belle matinée d'automne, Peter Milton pénètre dans le hall d'entrée des bureaux de Honorable Auto Parts à Denver, un grossiste en pièces détachées d'automobiles. Il attend son tour tandis que la réceptionniste fait entrer un visiteur, renseigne quelqu'un au téléphone et réceptionne un colis, tout cela plus ou moins en même temps.

"Où avez-vous appris à faire autant de choses à la fois ?" demande Peter quand elle peut enfin se consacrer à lui. Elle sourit, visiblement flattée qu'il ait remarqué ses talents. Il explique qu'il travaille au service marketing à Dallas, et il vient rencontrer Mike Talbott du service commercial d'Atlanta. "Nous devons rendre visite ensemble à un client cet après-midi, explique-t-il. Je vais attendre ici."

"Le marketing..." Elle a prononcé le mot sur un ton presque rêveur, et Peter lui sourit en attendant la suite. "Si j'avais pu aller à l'université, c'est ce que j'aurais fait, dit-elle. J'adorerais travailler au service marketing."

Il sourit de nouveau. "Kaila, dit-il en lisant le nom indiqué sur le bureau, à Dallas, une de mes collègues était secrétaire. Elle a été transférée au service marketing, et maintenant, elle est chef de projet adjointe et gagne deux fois plus qu'avant."

Les yeux de Kaila se mettent à briller. Il poursuit : "Vous savez utiliser un ordinateur ?".

"Bien sûr", dit-elle.

"Que diriez-vous si je proposais votre nom pour un travail de secrétaire au service marketing ?"

Elle fait un grand sourire. "Pour un poste comme ça, je suis prête à m'installer à Dallas !"

"Dallas vous plaira beaucoup, dit-il. Je ne peux pas vous promettre de poste dans l'immédiat, mais je vais voir ce que je peux faire."

Elle se dit que cet homme séduisant, avec son costume-cravate et sa coupe de cheveux soignée, incarne peut-être un tournant dans sa carrière professionnelle.

Peter s'assoit dans le hall d'entrée, ouvre son ordinateur portable et se met à travailler. Après dix à quinze minutes, il s'approche de nouveau du bureau de la réceptionniste et dit : "Écoutez, j'ai l'impression que Mike a dû prendre du retard. Y a-t-il une salle de réunion où je puisse m'asseoir et vérifier mon courrier électronique, en attendant ?".

Kaila appelle la personne qui gère les salles de réunion, et elle fait en sorte que Peter puisse utiliser l'une de celles qui sont inoccupées. L'entreprise suit une mode qui provient de la Silicon Valley (sans doute lancée par Apple) et qui consiste à donner des noms originaux aux salles de réunion : personnages de bandes dessinées ou de dessins animés, chaînes de restaurants ou vedettes du cinéma. En l'occurrence, la salle attribué à Peter se nomme Minnie Mouse. Kaila lui fait signer le registre puis lui indique comment s'y rendre.

Il trouve la salle, s'installe et connecte son ordinateur portable au port Ethernet.

Vous avez peut-être compris ce qui s'est produit : il est maintenant connecté au réseau *derrière le pare-feu de l'entreprise*.

Le point de vue d'Anthony

On pourrait dire qu'Anthony Lake était un homme d'affaires paresseux. A moins que "véreux" ne soit un qualificatif plus exact.

Plutôt que de travailler pour d'autres, il avait décidé de s'installer à son propre compte. Il voulait ouvrir une boutique où il pourrait rester toute la journée au lieu d'avoir à courir sans cesse à gauche et à droite. Mais il voulait aussi que son entreprise soit rentable.

Quel genre de boutique ? Il n'a pas été long à se décider. Il s'y connaissait en réparation automobile ; il allait donc ouvrir un magasin de pièces détachées.

Et comment faire pour être sûr de gagner de l'argent ? Il a eu une inspiration soudaine : il fallait convaincre Honorable Auto Parts, le grossiste, de lui vendre au prix d'achat la marchandise dont il avait besoin.

Bien entendu, Honorable Auto Parts n'y consentirait pas de plein gré. Mais Anthony avait du bagout, son ami Mickey savait comment pénétrer les systèmes informatiques, et à eux deux, ils ont donc mis un plan au point.

En ce jour d'automne, il avait donc réussi à se faire passer pour un employé de la société nommé Peter Milton, à pénétrer les locaux de Honorable Auto Parts et à connecter son ordinateur portable au réseau de l'entreprise. Mais ce n'était que la première étape. Ce qui restait à faire n'était pas simple, d'autant plus qu'Anthony s'était fixé un temps maximum de quinze minutes, après quoi il considérait que le risque de se faire repérer devenait trop important.

Il avait téléphoné au préalable en se faisant passer pour un technicien du fournisseur d'ordinateurs de l'entreprise, et il avait débité son histoire : "Votre société a souscrit à un plan de support technique de deux ans. Nous sommes en train de vous enregistrer dans notre base de données, et nous avons besoin de savoir quels logiciels vous utilisez, afin de vous prévenir quand de nouvelles versions ou des patches sont disponibles". Il avait obtenu en réponse une liste de logiciels, et un ami comptable avait identifié le logiciel MAS 90 comme étant la cible : c'était ce logiciel qui gérait la liste des clients du grossiste, ainsi que les remises et les conditions de paiement pour chacun d'entre eux.

Le message de Mitnick

Répétez à vos salariés que l'habit ne fait pas le moine : le fait que quelqu'un ait une apparence soignée ne le rend pas plus crédible pour autant.

Avec cette information essentielle, il s'est servi d'un logiciel pour identifier tous les hôtes du réseau, et il ne lui a pas fallu longtemps pour trouver le serveur utilisé par le service comptable. Il a lancé l'un des nombreux logiciels de piratage qui se trouvaient sur son ordinateur portable afin d'identifier tous les utilisateurs autorisés du serveur cible. Avec un autre logiciel, il a appliqué une liste de mots de passe couramment employés, tels que "*blank*" (vierge) et "*password*"(mot de passe). C'est ce dernier qui a fonctionné, ce qui n'est pas surprenant : peu de gens sont créatifs lorsqu'il s'agit d'inventer un mot de passe !

Six minutes seulement s'étaient écoulées, et les carottes étaient presque cuites. Il avait pénétré le serveur.

Seules trois minutes ont été nécessaires pour ajouter très soigneusement à la liste des clients le nom de sa nouvelle société, son adresse, son numéro de téléphone et le nom du contact. Et surtout l'élément crucial, celui qui ferait toute la différence, et qui indiquait que toutes les pièces lui seraient vendues avec une marge de 1 % par rapport au prix auquel Honorable Auto Parts les achetait.

En un peu moins de dix minutes, il en avait fini. Il s'est arrêté assez longtemps pour remercier Kaila, lui dire qu'il avait vérifié son courrier et que finalement, il allait directement retrouver Mike Talbot chez le client. En outre, il n'oublierait pas de la recommander pour le poste de secrétaire à la division marketing.

Analyse du stratagème

Le manipulateur qui a dit s'appeler Peter Milton a employé deux techniques psychologiques distinctes, l'une planifiée, l'autre improvisée sur le moment.

Il s'est habillé comme un cadre bien payé. Costume, cravate et coupe de cheveux : on pourrait croire que ce ne sont que des détails, mais ils peuvent faire la différence. J'en ai pris conscience moi-même par accident. Au cours de ma courte carrière de programmeur chez GTE California, une importante compagnie de téléphone aujourd'hui disparue, je me suis rendu compte que si j'arrivais sans badge et habillé correctement mais de manière décontractée (polo, pantalon de coton et mocassins), on m'arrêtait et on me questionnait : où est votre badge, qui êtes-vous, où travaillez-vous ? Parfois, au contraire, j'arrivais, toujours sans badge, mais avec un complet-cravate, l'air très "professionnel". Je m'intégrais à un groupe de personnes au moment où elles entraient dans le bâtiment et je discutais avec elles comme si je les connaissais. Même quand les gardes remarquaient mon absence de badge, ils ne me

dérangeaient pas parce que je semblais faire partie des cadres de l'entreprise et parce que ceux qui m'accompagnaient, eux, avaient leurs badges.

Cette expérience m'a fait comprendre à quel point l'attitude du personnel de sécurité est prévisible. Comme tout le monde, il juge d'après les apparences, une vulnérabilité sérieuse que les manipulateurs apprennent à exploiter.

La deuxième arme psychologique de l'assaillant est entrée en jeu quand il a remarqué les efforts inhabituels que déployait la réceptionniste. Tout en gérant plusieurs personnes à la fois, elle parvenait à rester aimable et à donner l'impression à chacun qu'elle s'occupait de lui. Il a interprété son attitude comme étant celle de quelqu'un qui cherchait à prouver sa valeur et à aller de l'avant. Lorsqu'il a dit travailler pour le service marketing, il a observé sa réaction et a constaté qu'il avait réussi à établir un contact avec elle. Il pouvait donc la manipuler en lui faisant miroiter un meilleur poste. Bien entendu, si elle avait dit préférer travailler pour le service comptable, il aurait prétendu y avoir des contacts lui permettant d'y trouver un emploi pour elle.

Autre arme psychologique à laquelle l'assaillant a eu recours ici : l'établissement d'un climat de confiance, et ce en deux étapes. Il a d'abord commencé par bavarder avec la réceptionniste à propos d'un poste possible au marketing, et il a cité le nom d'un collègue, qui était celui d'un salarié existant, de même qu'il avait utilisé pour lui-même le nom d'un employé de l'entreprise.

Il aurait pu conclure sa première conversation en demandant directement une salle de réunion. Il a préféré s'asseoir pendant un moment et faire semblant de travailler en attendant son collègue : autre moyen de dissiper les soupçons, dans la mesure où un intrus ne se serait pas éternisé. Il ne s'est pas attardé très longtemps, toutefois : les manipulateurs savent qu'il est préférable de ne pas rester plus longtemps que nécessaire sur le lieu de leurs méfaits.

À titre d'information, aux États-Unis, ni l'usurpation d'identité commise par Anthony, ni le fait d'avoir obtenu l'accès de la salle de réunion, ni même le fait de se connecter au réseau Ethernet de l'entreprise n'est un délit en soi. Seule l'intrusion dans le réseau informatique constitue un délit. C'est plus ou moins le même cas dans la plupart des autres pays occidentaux.

Le message de Mitnick

Le fait de laisser un étranger pénétrer en un endroit d'où il peut accéder au réseau de l'entreprise représente un risque pour la sécurité du réseau. On peut tout à fait admettre qu'un salarié, en particulier un salarié provenant de l'extérieur, puisse vérifier son courrier électronique à partir d'une salle de réunion. Toutefois, si le visiteur n'est pas identifié de manière formelle, ou si le réseau n'est pas segmenté pour éviter les connexions non autorisées, il peut s'agir d'un maillon faible pour l'accès aux fichiers de l'entreprise.

KEVIN MITNICK ESPIONNÉ

Il y a très longtemps, j'ai travaillé dans le service informatique d'une petite entreprise, service qui était composé de quatre personnes et d'un unique bureau. À un moment donné, j'ai remarqué qu'à chaque fois que j'entrais dans le bureau, l'un de mes collègues, que j'appellerai Joe, passait brusquement à une autre fenêtre sur son écran. Cette attitude m'a parue suspecte, et quand elle s'est de nouveau produite à deux reprises au cours de la même journée, j'ai décidé de tirer l'affaire au clair.

L'ordinateur de Joe fonctionnait comme un terminal du mini-ordinateur de l'entreprise. J'ai donc installé sur le mini-ordinateur VAX un logiciel de surveillance. Ce logiciel me permettait de voir exactement ce qu'il faisait, comme si je disposais d'une caméra qui filmait par-dessus son épaule ce qui se passait sur son écran.

Mon ordinateur était adjacent à celui de Joe. Je me suis arrangé pour positionner mon moniteur de telle manière que Joe ne voie pas ce qui se passe sur mon écran, mais il aurait pu tourner la tête à tout moment et voir que je l'espionnais. Ces précautions se sont révélé inutiles : il était bien trop captivé par ce qu'il faisait pour me prêter la moindre attention.

J'ai alors constaté, médusé, que mon collègue avait obtenu l'accès à ma feuille de paye, et qu'il s'intéressait à mon salaire.

Je n'étais dans l'entreprise que depuis quelques mois, et sans doute Joe ne supportait-il pas l'idée que je puisse être mieux payé que lui.

Quelques minutes plus tard, j'ai vu qu'il téléchargeait des outils de hacker qui ne sont employés que par les pirates peu expérimentés, qui ne savent pas en programmer eux-mêmes. Joe ne savait donc pas que l'un des hackers les plus expérimentés des États-Unis était assis à côté de lui.

Il connaissait déjà mon salaire ; il était donc trop tard pour intervenir. Du reste, n'importe qui ayant accès aux ordinateurs de l'administration fiscale ou de la Sécurité sociale pouvait en faire autant. Et je ne voulais pas me trahir en lui faisant comprendre que je savais qu'il savait. À l'époque, je cherchais à garder un profil bas. Un bon manipulateur reste discret sur ses capacités et ses connaissances : il cherche à être sous-estimé, non à être perçu comme une menace.

Je n'ai donc pris aucune mesure, me consolant en me disant que Joe pensait qu'il connaissait l'un de mes secrets, alors que c'était l'inverse : c'était moi qui en savait plus sur Joe qu'il n'en savait sur mon compte.

Je me suis aperçu petit à petit qu'en réalité, mes trois collègues du service informatique s'amusaient à vérifier le salaire de telle ou telle jolie secrétaire (ou beau garçon, en ce qui concernait notre unique collègue féminine) sur lesquels ils avaient des vues. Ils pouvaient à tout moment connaître les salaires et les primes de n'importe quel employé de la société, y compris de ses dirigeants.

Analyse du stratagème

Cette histoire illustre un problème intéressant. Les fichiers des feuilles de paies étaient accessibles à tous ceux qui avaient la charge de gérer les systèmes informatiques de l'entreprise. Il s'agit donc d'une question de personnes, et de savoir à qui on peut faire confiance. Il peut être difficile pour les salariés d'un service informatique de résister à la tentation de fouiller dans certains fichiers. Et ils ont accès à ces fichiers parce qu'ils disposent de privilèges particuliers au niveau du système informatique.

Une protection envisageable consisterait à effectuer un audit des accès aux fichiers particulièrement sensibles tels que les feuilles de paies. Bien entendu, toute personne disposant des privilèges requis pourrait désactiver cet audit ou effacer *a posteriori* les traces de son passage, mais chaque mesure supplémentaire rend les intrusions plus difficiles à dissimuler.

MESURES DE PRÉVENTION

Qu'il fouille dans les poubelles ou qu'il trompe un agent de sécurité ou une réceptionniste, le manipulateur peut envahir l'espace de votre entreprise de différentes manières. Mais vous serez sans doute heureux d'apprendre qu'il existe différentes mesures préventives efficaces.

Protection des locaux en dehors des heures de travail

Tous les employés qui viennent travailler en dehors des heures de travail habituelles doivent avoir l'obligation de s'arrêter à la réception ou au bureau de la sécurité pour obtenir un badge provisoire pour la journée. L'incident de la première histoire de ce chapitre se serait sans doute terminé autrement si les agents de sécurité avaient eu à suivre une procédure précise lorsqu'ils rencontrent une personne sans badge.

Pour les entreprises et les secteurs d'activité où la sécurité n'est pas un élément prioritaire, il n'est peut-être pas indispensable que chaque salarié laisse son badge visible en permanence. Dans les secteurs sensibles, en revanche, ce doit être une obligation respectée de manière stricte. Les salariés doivent être formés et encouragés à exiger le port du badge de la part des collègues, et les salariés de plus haut niveau hiérarchique doivent apprendre à accepter sans contestation ce type d'exigence, même lorsqu'elle vient d'un subordonné.

Le règlement de l'entreprise doit prévoir des sanctions pour les salariés qui oublient de porter leur badge de manière répétée. Dans certaines entreprises, les sanctions sont échelonnées de manière progressive, du rapport au supérieur hiérarchique jusqu'à l'avertissement formel.

Par ailleurs, lorsqu'il y a des informations sensibles à protéger, l'entreprise doit établir des procédures pour les visites en dehors des heures de travail. Une solution consiste à obliger les visiteurs à prendre rendez-vous par l'intermédiaire du personnel de sécurité ou de tout autre groupe défini. Ce groupe aurait l'obligation de vérifier l'identité des visiteurs potentiels au moyen d'un appel téléphonique auprès du supérieur hiérarchique des visiteurs, ou en suivant toute autre méthode d'identification sûre.

Du respect pour les déchets

L'histoire des fouilleurs de poubelles a permis de présenter les différentes manières dont une personne malveillante peut profiter du contenu de vos poubelles. Les huit points à retenir en ce qui concerne les déchets sont les suivants :

- Classifiez toutes les informations en fonction de leur degré de confidentialité.
- Mettez en place, pour l'ensemble de l'entreprise, des règles définissant de quelle manière les salariés doivent se débarrasser des documents confidentiels.
- Faites en sorte que tous les documents confidentiels soient détruits de manière sûre et définitive. N'utilisez pas de destructeurs de documents d'entrée de gamme : les bandes de papier qu'ils produisent peuvent être exploitées par des assaillants pour peu qu'ils soient assez patients. Choisissez des destructeurs de documents offrant une coupe croisée, et dont le niveau de sécurité soit donc de 4 ou 5 (sur une échelle de 5).
- Mettez au point une méthode pour rendre inutilisable ou effacer *entièrement* le contenu des supports informatiques : disquettes, disques Zip, CD-ROM, DVD-ROM, bandes magnétiques, vieux disques durs et autres. Rappelez-vous que le fait de placer un document dans la Corbeille, à partir du système d'exploitation, ne

supprime pas réellement le document, comme les dirigeants d'Enron l'ont appris à leurs dépens. Le simple fait de jeter un support informatique dans une poubelle est une incitation pour le fouilleur de poubelles local (voyez le Chapitre 16 pour des informations plus précises sur la destruction des supports informatiques).

- Effectuez un minimum de contrôles quant aux membres de vos équipes de nettoyage, en vérifiant éventuellement leurs antécédents.
- Rappelez régulièrement aux salariés qu'ils doivent penser à la nature des informations qu'ils jettent dans leur corbeille.
- Verrouillez vos poubelles.
- Utilisez des poubelles séparées pour les informations confidentielles et faites enlever ces poubelles par des sociétés fiables et spécialisées dans ce type de travail.

Mesures en cas de départ

Nous avons déjà mentionné plus haut le fait que le départ d'un salarié doit s'accompagner de mesures extrêmement rigoureuses en ce qui concerne l'accès de ce salarié aux informations confidentielles, aux mots de passe, etc. Vos procédures de sécurité doivent permettre de déterminer qui a l'autorisation d'accéder à quoi. Il peut être difficile pour un manipulateur venant de l'extérieur d'échapper à vos mesures de sécurité : ne facilitez pas pour autant la tâche aux anciens salariés.

Autre mesure qu'on néglige couramment : certains salariés ont accès aux bandes de sauvegarde stockées par une société extérieure. Cette société doit donc être informée immédiatement afin que le nom de l'ancien salarié soit ôté de la liste des personnes autorisées.

En fonction des mesures mises en relief par les anecdotes de ce chapitre, et même si le Chapitre 16 revient plus en détail sur ce sujet essentiel, il peut être utile de mentionner ici certaines des principales mesures de sécurité à mettre en place :

- Une liste complète des procédures à suivre lors du départ d'un salarié, avec des mesures spécifiques pour les salariés ayant accès à des données sensibles.
- Une procédure pour empêcher *immédiatement* l'accès du salarié à son ordinateur, de préférence avant même qu'il ait quitté le bâtiment.
- Une procédure pour récupérer le badge d'identification du salarié ainsi que tout autre moyen d'accès tel que clés, systèmes d'accès électroniques, etc.

- L'obligation pour les agents de sécurité de demander aux personnes sans badge une pièce d'identité avec photo, et de vérifier que leur nom figure bien sur la liste des personnes salariées par l'entreprise.

Certaines mesures supplémentaires seront trop onéreuses pour certaines entreprises, mais utiles pour d'autres. Parmi les mesures de sécurité les plus strictes, on peut citer :

- Des badges d'identification électroniques associés à un lecteur de badges à l'entrée de l'entreprise, ce qui permet de confirmer immédiatement qu'une personne donnée fait partie de l'entreprise et qu'elle est autorisée à entrer dans le bâtiment. Notez toutefois que les agents de sécurité doivent prêter attention à la technique consistant, pour une personne non autorisée, à s'introduire dans l'entreprise en même temps qu'une ou plusieurs personnes autorisées.
- L'obligation de changer de mot de passe pour tous les membres du groupe de travail de la personne sur le départ, surtout quand ce départ n'est pas volontaire. Cette mesure peut sembler excessive. Toutefois, à titre d'anecdote, le personnel de sécurité de la compagnie de téléphone Pacific Bell a trouvé très drôle que General Telephone, autre compagnie de téléphone, m'ait engagé en tant qu'informaticien. Mais lorsque la première a appris qu'un hacker connu avait travaillé pour eux, ils firent changer les mots de passe de *tous les salariés de l'entreprise* !

Le lieu de travail ne doit pas se transformer en prison, mais en même temps, il est nécessaire de se défendre contre le salarié qui vient d'être renvoyé et qui veut se venger.

N'oublier personne

Lorsqu'on établit des règles de sécurité, il est courant d'oublier les salariés "de base" qui n'ont pas accès aux informations sensibles. Nous avons vu dans les chapitres précédents que les réceptionnistes étaient une cible facile pour les assaillants, et l'histoire du grossiste en pièces détachées en est une autre illustration : un personnage sympathique, bien habillé et prétendant venir d'une autre branche de la même société peut ne pas être qui il prétend. Les réceptionnistes doivent être formés à demander poliment une identification interne à la société quand c'est nécessaire, et cette formation doit également s'appliquer à tous ceux qui sont susceptibles de remplacer les réceptionnistes pendant l'heure du déjeuner ou les pauses.

Pour des visiteurs extérieurs à l'entreprise, les réceptionnistes doivent demander une pièce d'identité comprenant une photo et noter les informations qu'elle comporte. Il est bien sûr possible de se procurer une fausse pièce d'identité, mais le fait de l'exiger complique néanmoins la tâche pour l'assaillant potentiel.

Dans certaines sociétés, il peut être utile d'exiger que tout visiteur reste accompagné dès son entrée et entre deux réunions. Les procédures doivent également spécifier que l'accompagnateur, lorsqu'il présente le visiteur à la personne avec laquelle elle a rendez-vous, précise bien si le visiteur fait partie ou non de l'entreprise. Pourquoi ? Parce que, comme nous l'avons vu dans les récits précédents, l'assaillant se fera souvent passer pour untel auprès de la première personne rencontrée, puis pour un autre auprès de la suivante. Il n'est pas difficile pour l'assaillant de convaincre le réceptionniste qu'il a un rendez-vous avec un ingénieur, par exemple. Une fois dans le bureau de l'ingénieur, il pourra prétendre être un commercial qui souhaite proposer un quelconque produit à l'entreprise. Et une fois sorti du bureau de l'ingénieur, il pourra librement accéder à tout le bâtiment.

Avant de laisser entrer un salarié venant d'un autre site, il faut respecter des procédures spécifiques pour s'assurer que la personne fait effectivement partie de la société. Les réceptionnistes et les agents de sécurité doivent être conscients des méthodes que les assaillants utilisent pour prendre l'identité d'un salarié afin d'obtenir l'accès aux locaux.

Quelle protection envisager contre un individu qui parvient à entrer dans un bâtiment et à brancher son ordinateur portable sur un port situé derrière le pare-feu de l'entreprise ? Étant donné l'évolution technologique actuelle, il s'agit d'un vrai défi. Les ports des salles de réunion, de formation et des autres lieux de ce type doivent être protégés par des pare-feu ou des routeurs. Mais il est préférable de mettre en place une méthode pour authentifier tout utilisateur qui tente d'accéder au réseau.

Service informatique et sécurité

Mieux vaut le savoir : dans votre propre entreprise, tous ceux qui font partie du service informatique savent ou peuvent savoir à tout moment quel est votre salaire et combien gagne le président, ou qui utilise le jet de l'entreprise pour partir en vacances de ski.

Dans certaines entreprises, le personnel du service informatique peut même augmenter ses propres salaires, payer des fournisseurs inexistants, faire disparaître des mentions négatives de leur dossier personnel et ainsi de suite. Parfois, seule la peur de se faire prendre les empêche de passer à l'action, jusqu'au jour où survient quelqu'un que la cupidité ou la malhonnêteté foncière fera agir au mépris du danger pour parvenir à ses fins.

Il existe bien sûr des solutions. Les fichiers sensibles peuvent être protégés par un système de contrôle d'accès de telle manière que seules les personnes autorisées puissent y accéder. Certains systèmes d'exploitation disposent d'un système d'audit qui peut être configuré pour garder la trace de certains événements, comme le nom des personnes qui ont accédé à un fichier protégé, que cet accès ait été ou non couronné de succès.

Si votre entreprise est consciente de ce problème et a mis en place des contrôles d'accès et un système d'audit pour les fichiers sensibles, elle aura fait un grand pas dans la bonne direction.

Chapitre 11

Manipulation et technologie

Les manipulateurs exploitent pleinement leur talent pour obtenir de leurs victimes une coopération involontaire, mais souvent, leur réussite dépend également de leur connaissance des systèmes téléphoniques et informatiques.

Voici un échantillon de situations où le manipulateur fait largement appel à la technologie pour parvenir à ses fins.

PIRATAGE DERRIÈRE LES BARREAUX

Quelles sont les installations qui sont les mieux protégées contre toute intrusion, qu'elle soit physique, téléphonique, informatique ou de toute autre nature ? Fort Knox, la Maison blanche ou le Pentagone sont de bons exemples, mais on peut aussi citer les prisons américaines. Il est rare qu'on s'en échappe, et les fugitifs sont généralement presque immédiatement repris. On pourrait croire que de telles institutions seraient invulnérables aux attaques des manipulateurs. Il n'en est rien : il n'existe pas de système de sécurité qui soit absolument sûr.

Il y a un certain nombre d'années, deux escrocs professionnels ont connu de sérieux problèmes après avoir délesté un juge local d'une importante somme d'argent. Le duo était dans le collimateur de la justice depuis des années, mais à la suite de cette affaire, les autorités ont commencé à s'intéresser à eux de beaucoup plus près. Elles ont mis la main sur l'un des deux escrocs, Charles Gondorff, et l'ont placé en détention préventive dans une prison à proximité de San Diego.

Johnny Hooker, son collègue, savait que Gondorff aurait besoin d'une importante somme d'argent pour rémunérer les services d'un bon avocat.

Mais comme la plupart des escrocs, il avait toujours dépensé sans compter pour s'offrir des vêtements, des voitures et des femmes, et il lui restait à peine de quoi vivre.

Hooker devait donc monter une nouvelle escroquerie afin de trouver assez d'argent pour l'avocat, mais il ne savait pas comment faire. C'était toujours Charlie Gondorff qui avait mis au point les arnaques. Hooker n'osait pas rendre visite à Gondorff en prison pour lui demander que faire, d'autant moins que la police fédérale savait qu'elle avait affaire à deux escrocs qui chercheraient à communiquer l'un avec l'autre. Obstacle supplémentaire : seuls les membres de la famille étaient autorisés à rendre visite aux prisonniers, ce qui signifiait qu'il devrait falsifier des papiers d'identité en prétendant être un parent de Gondorff. L'utilisation de faux papiers d'identité dans une prison fédérale ne lui paraissait pas être une bonne idée.

Il fallait donc qu'il trouve un autre moyen de contacter Gondorff.

Ce n'était pas tâche facile. Aucun détenu d'une prison fédérale, d'État ou locale n'avait le droit de recevoir des appels téléphoniques. Les téléphones des prisonniers, dans les prisons fédérales, portaient tous une mention du type : "Les détenus sont informés que toutes les conversations passées à partir de ce téléphone sont écoutées par les autorités, et que l'utilisation du téléphone vaut consentement implicite de cette mise sur écoute". Le fait de préparer un délit par téléphone en laissant les autorités suivre les conversations représentait donc sans nul doute un bon moyen de prolonger son séjour en prison.

Hooker savait toutefois que, en vertu de la Constitution américaine, certains appels n'étaient pas mis sur écoute, à savoir ceux qui sont établis entre un détenu et son avocat. En fait, la prison où se trouvait Gondorff disposait de téléphones directement reliés au bureau des avocats de la défense, le PDO (*Public Defender's Office*). Les compagnies de téléphone appellent ce service une "connexion directe". Les autorités considèrent ce système comme sûr dans la mesure où les appels sortants sont automatiquement mis en communication avec le PDO et que les appels entrants sont bloqués. Même si quelqu'un devait découvrir le numéro des téléphones situés à l'intérieur de la prison, les appels ne pourraient aboutir dans la mesure où les appareils sont programmés pour refuser les appels entrants.

Hooker se dit qu'en tant qu'escroc professionnel, il devait pouvoir trouver une solution à son problème. Gondorff avait déjà essayé d'utiliser l'un des téléphones reliés au PDO en disant : "Bonjour, ici Tom, du centre des dérangements téléphoniques de la compagnie de téléphone. Nous effectuons un test sur la ligne ; est-ce que vous pouvez composer le neuf, double zéro ?" Le neuf aurait permis d'accéder à l'extérieur, et le double zéro à un opérateur. Mais la tentative avait échoué : la personne qui répondait au PDO connaissait l'astuce.

Son comparse avait eu plus de succès : il avait appris que la prison était divisée en dix quartiers d'habitation, chacune munie de sa ligne de téléphone connectée directement au bureau des avocats. Mais il restait beaucoup à faire. Après quelques nuits de réflexion, Hooker avait mis au point un plan en cinq étapes. Pour un individu moyen, chacune de ces étapes aurait représenté un obstacle insurmontable ; pas pour un manipulateur professionnel.

La première étape consistait à trouver les numéros des dix téléphones reliés au PDO.

Dans la deuxième, il fallait modifier la programmation des téléphones afin qu'ils acceptent les appels entrants.

La troisième étape consistait à identifier le quartier dans lequel était détenu Gondorff.

En quatrième lieu, Hooker devait trouver le numéro de téléphone de l'appareil du quartier de Gondorff.

Enfin, il fallait convenir d'un rendez-vous téléphonique avec Gondorff sans mettre la puce à l'oreille des autorités.

Contacts avec la compagnie de téléphone

Johnny commence par appeler les bureaux de la compagnie de téléphone, en se faisant passer pour un fonctionnaire de l'Administration des Services Généraux, l'agence responsable des achats de biens et de services pour le compte du gouvernement fédéral. Il dit qu'il est en train de rédiger une commande pour des services supplémentaires, et qu'il a besoin de connaître les données de facturation pour tous les services de connexion directe actuellement en service, et en particulier les numéros de téléphone et les factures mensuelles concernant les postes du centre de détention de San Diego. À l'autre bout du fil, son interlocutrice est enchantée de pouvoir l'aider.

Pour confirmer ses informations, Hooker appelle l'un de ces numéros de téléphone ; il entend alors un message préenregistré du type "Cette ligne n'est plus en service actuellement", qui signifie en réalité que la ligne a été programmée pour ne plus recevoir d'appels, exactement ce à quoi il s'attendait.

Hooker connaît bien le fonctionnement des compagnies de téléphone, et il sait qu'il doit contacter un service nommé RCMAC (*Recent Change Memory Authorization Center*), qui est chargé des modifications de statut apportées aux lignes. Il appelle d'abord les bureaux centraux de la compagnie de téléphone, dit qu'il fait partie d'une équipe de réparation et qu'il a besoin de

connaître le numéro du RCMAC pour tel et tel préfixe, en l'occurrence celui qui correspond aux téléphones de la prison. C'est une demande courante de la part de techniciens en cours de mission, et l'employé, à l'autre bout du fil, lui fournit le numéro demandé sans hésitation.

Il appelle ensuite le RCMAC, donne un faux nom et prétend à nouveau faire partie d'une équipe de réparation.

L'appel au RCMAC

Il demande à la personne qui lui répond de consulter l'un des numéros de la prison, qu'il a obtenu quelques appels plus tôt. Une fois qu'elle a obtempéré, il lui pose la question suivante :

"La ligne est-elle programmée pour refuser les appels entrants ?"

"Oui", répond-elle.

"Ça explique pourquoi le client n'arrive pas à recevoir d'appels, dit Hooker. Pouvez-vous me rendre service et réactiver les appels entrants pour cette ligne ?" Il attend quelques instants pendant que sa correspondante vérifie sur un autre ordinateur qu'un ordre a été passé pour autoriser la modification. Elle indique : "Cette ligne n'est pas censée recevoir d'appels entrants. Je n'ai ici aucun ordre concernant une modification du statut de la ligne".

"Exactement, c'est ça l'erreur. L'ordre aurait dû passer hier, mais l'attaché de clientèle qui est en charge de ce client est rentré à la maison parce qu'il était malade, et il a oublié de dire à quelqu'un d'autre de s'occuper de l'ordre de changement de statut. Et maintenant, bien sûr, le client est fou furieux."

Après une courte pause pendant laquelle la correspondante de Johnny Hooker réfléchit à cette demande, qui est inhabituelle et va à l'encontre des procédures standard, elle dit : "D'accord". Il l'entend taper sur son clavier et, quelques instants plus tard, la modification est effectuée.

Il a réussi à briser la glace et à établir entre eux une sorte de complicité. Interprétant correctement l'attitude de sa correspondante et sa bonne volonté, il n'hésite pas à aller plus loin : "Auriez-vous quelques minutes de plus pour m'aider ?"

"Oui, répond-elle. Qu'est-ce que je peux faire pour vous ?"

"J'ai là plusieurs autres lignes qui appartiennent au même client, et qui ont toutes le même problème. Je vais vous lire les numéros pour que vous puissiez vérifier qu'elles ne sont pas configurées pour refuser les appels, d'accord ?". Elle accepte.

Quelques minutes plus tard, le statut des dix lignes était "corrigé" de manière à accepter les appels entrants.

À la recherche de Gondorff

Étape suivante : déterminer dans quel quartier de la prison se trouve Gondorff. Il s'agit d'une information que les responsables des centres de détention préfèrent évidemment garder secrète. Une fois de plus, Hooker doit s'appuyer sur ses talents de manipulateur.

Il appelle une prison fédérale située dans une autre ville (Miami en l'occurrence, mais n'importe quelle prison aurait fait l'affaire) et prétend appeler depuis le centre de détention de New York. Il demande à parler à quelqu'un qui a accès au système informatique central des prisons : ce système, nommé *Sentry*, regroupe les informations concernant tous les détenus du pays.

L'appel d'Hooker

Quand il a la personne correspondante au bout du fil, Hooker prend son meilleur accent de Brooklyn.

"Bonjour, dit-il. Ici Thomas, du centre de détention fédéral de New York. Notre connexion avec Sentry fonctionne très mal en ce moment. Pouvez-vous retrouver un prisonnier pour moi ? Il devrait se trouver dans votre établissement." Il donne le nom et le numéro de Gondorff.

"Non, il n'est pas ici, répond son correspondant. Il est au centre correctionnel de San Diego."

Hooker feint d'être surpris. "À San Diego ? Il aurait dû être transféré par avion jusqu'à Miami la semaine dernière ! Et c'est bien la même personne ? Quelle est sa date de naissance ?"

"Le 12 mars 1960."

"Oui, c'est bien lui. Dans quel quartier se trouve-t-il ?"

"Le quartier Dix Nord", répond le correspondant — alors qu'il n'y a aucune raison qu'un membre de l'administration pénitentiaire de New York ait besoin de connaître une telle information.

Hooker a fait modifier les lignes de téléphone de manière à ce qu'elles acceptent les appels entrants et il sait dans quel quartier se trouve Gondorff. Il faut maintenant qu'il sache à quel numéro de téléphone correspond le quartier Dix Nord.

Cette partie de son projet est plus difficile à réaliser. Hooker essaie d'appeler l'un des numéros ; il sait que la sonnerie des téléphones est désactivée et que personne ne peut savoir qu'il appelle. Laissant le combiné décroché, il s'assoit et prend un livre, tout en écoutant la sonnerie diffusée par le haut-parleur de son téléphone. Le détenu qui finit par décrocher, à l'autre bout, cherche bien sûr à parler à son avocat. Hooker sait comment répondre : "Bureau des avocats", annonce-t-il.

> Lorsque le détenu demande à parler à son avocat, Hooker dit : "Je vais voir s'il est disponible. De quel quartier appelez-vous ?". Il note la réponse, met son correspondant en attente puis reprend la ligne après quelques instants et dit : "Il est en audience. Rappelez plus tard". Puis il raccroche.
>
> Il attend presque toute la matinée, mais il aurait pu être plus malchanceux : son quatrième appel l'a mis en communication avec le quartier Dix Nord. Hooker sait maintenant quel numéro utiliser pour accéder au téléphone non surveillé du quartier de Gondorff.

Synchronisation des montres

Avant-dernière étape : faire savoir à Gondorff à quel moment il doit décrocher le téléphone qui relie directement les détenus au bureau des avocats. C'est plus simple qu'on pourrait le penser.

Hooker appelle le centre de détention en prenant sa voix "officielle", s'identifie en tant que membre de l'administration pénitentiaire et demande à être mis en contact avec le quartier Dix Nord. L'appel est aussitôt transféré. Lorsque le gardien décroche, Hooker se présente : "Ici Tyson, du R et D". "R et D" est l'abréviation de *Receiving and Discharge*, l'unité responsable de l'admission et des départs des détenus. L'utilisation d'une abréviation qui n'est employée que par le personnel pénitentiaire suffit à éviter que son interlocuteur ne se pose des questions. "J'ai besoin de parler au détenu Gondorff. Nous avons des affaires à lui, ici, et nous voulons savoir à quelle adresse les expédier. Pouvez-vous le faire venir au téléphone ?"

Hooker entend le gardien appeler Gondorff. Après quelques minutes qui lui paraissent interminables, une voix familière résonne dans le combiné.

"Ne dis rien avant que je t'explique de quoi il s'agit", dit Hooker. Il lui dit sous quel prétexte il a appelé, afin que Gondorff puisse donner l'impression qu'il indique à quelle adresse ses affaires doivent être envoyées. Hooker poursuit : "Si tu peux accéder au téléphone du bureau des avocats à une heure cet après-midi, ne dis rien. Sinon, dis-moi à quelle heure tu peux y être". Gondorff ne répond pas. Hooker continue : "Bien. Sois là à une heure. Je t'appellerai, et tu décrocheras. Si c'est le bureau des avocats qui répond, raccroche et réessaie toutes les vingt secondes, jusqu'à ce que ce soit moi qui réponde."

À une heure, Gondorff décroche le téléphone, et Hooker est à l'autre bout de la ligne. Ils peuvent discuter tranquillement et en toute impunité, et organisent une série d'autres appels de même nature, qui leur permettent de planifier l'escroquerie qui pourra fournir la somme nécessaire pour payer l'avocat de Gondorff.

Analyse du stratagème

Cet épisode montre comment un manipulateur est capable de mener des actions qui, *a priori*, paraissent impossibles, et ce en manipulant successivement plusieurs personnes dont chacune n'accomplit qu'une seule tâche, laquelle semble sans conséquences en soi. C'est en associant toutes ces actions que le manipulateur parvient à ses fins.

La première salariée de la compagnie du téléphone a cru fournir des informations à un fonctionnaire de l'Administration des Services Généraux.

La deuxième savait qu'elle n'était pas censée changer le statut de la ligne sans un ordre correspondant, mais a néanmoins aidé son interlocuteur. Ainsi, les dix téléphones de la prison sont devenus accessibles de l'extérieur.

La requête adressée au fonctionnaire de la prison de Miami du fait d'un problème informatique a paru parfaitement raisonnable. Et même s'il n'existait aucune raison pour que l'interlocuteur ait besoin de connaître le quartier où se trouvait le détenu, pourquoi refuser de répondre à la question ?

Quant au gardien du quartier Dix Nord, qui pensait que l'appel venait de l'intérieur de la prison, pourquoi aurait-il refusé de répondre à la demande qu'on lui faisait ? Celle-ci n'avait rien d'extraordinaire, aussi a-t-il fait venir Gondorff au téléphone.

TÉLÉCHARGEMENT RAPIDE

Dix ans après avoir terminé ses études de droit, Ned Racine constate que ses camarades de promotion vivent dans de belles maisons avec pelouse et piscine, et vont jouer au golf une à deux fois par semaine tandis que lui plaide toujours des affaires mineures pour des clients qui n'ont jamais assez d'argent pour le payer. Mais la jalousie est mauvaise conseillère et, un jour, Ned en a assez.

Le seul bon client qu'il ait jamais eu est un cabinet comptable spécialisé dans les fusions et acquisitions. Ils n'ont pas fait appel à lui pendant très longtemps, mais assez toutefois pour qu'il comprenne que la publication de certaines affaires traitées par cette société peut avoir des répercussions sur les cours de certaines entreprises cotées en bourse. Ce ne sont pas de grosses entreprises, non. Mais dans un sens, c'est préférable : une augmentation, même faible, du prix de leurs actions peut représenter des gains importants en pourcentage. Si seulement il pouvait savoir sur quelles affaires ils travaillent…

Il connaît quelqu'un qui connaît quelqu'un qui a de l'expérience dans certains domaines… particuliers. Cet homme écoute Racine exposer son plan et accepte de l'aider. En échange d'une partie des gains que Racine allait

réaliser en bourse, il lui indique comment procéder. Il lui fournit également un petit appareil très pratique qui vient d'apparaître sur le marché.

Pendant quelques jours, Racine surveille l'aire de stationnement du petit parc d'activités économiques où se trouvent les modestes bureaux de l'entreprise. La plupart des employés partent entre 17 h 30 et 18 h. À 19 h, l'aire de stationnement est vide, et l'équipe de nettoyage arrive vers 19 h 30.

Le lendemain soir, quelques minutes avant 20 h, Racine se gare un peu à l'écart de l'aire de stationnement. Comme prévu, le parking est vide, à l'exception de la camionnette du service de nettoyage. Racine appuie son oreille contre la porte et entend le ronronnement de l'aspirateur. Il frappe d'un coup sec à la porte et attend, dans son costume-cravate, et sa serviette fatiguée sous le bras. Il n'y a pas de réponse, mais il est patient. Il frappe de nouveau. L'un des membres de l'équipe de nettoyage ouvre. "Bonjour !" crie Racine à travers la porte vitrée, en montrant la carte de visite de l'un des associés, qu'il a obtenue quelque temps auparavant. "Ma voiture est fermée à clé. Il faut que je retourne à mon bureau pour prendre mes clés."

L'homme déverrouille la porte, la referme derrière Racine et allume les lumières du couloir afin que Racine puisse voir où il va. Pourquoi agirait-il autrement ? Il rend service à l'une des personnes qui lui fournissent son salaire. Ou du moins a-t-il toutes les raisons de le penser.

Racine s'assoit devant l'ordinateur de l'un des associés et le met en route. Pendant son démarrage, il installe sur le port USB de l'ordinateur le petit gadget qu'on lui a fourni. L'objet est assez petit pour ressembler à un porte-clés, mais il peut contenir plus de 120 mégaoctets de données. Racine accède au réseau en utilisant le mot de passe de la secrétaire de l'associé, qui a obligeamment laissé un Post-it sur l'écran. En moins de cinq minutes, Racine a téléchargé toutes les feuilles de calculs et tous les documents stockés sur l'ordinateur de l'associé et les autres ordinateurs du réseau, et il a quitté les lieux.

Le message de Mitnick

> Les espions industriels et les pirates informatiques pénètrent parfois physiquement dans les locaux de l'entreprise visée. Plutôt que de recourir à un pied-de-biche pour entrer, le manipulateur utilise son talent pour inciter la personne qui se trouve de l'autre côté de la porte à lui ouvrir d'elle-même.

ARGENT FACILE

La première fois que j'ai eu accès à un ordinateur, au lycée, nous devions nous connecter *via* un modem à un mini-ordinateur central PDP-11 de DEC, qui se trouvait dans le centre de Los Angeles, et auquel étaient connectés tous les autres lycées de la ville. Le système d'exploitation de cet ordinateur se nommait RSTS/E ; c'est le premier avec lequel je me suis familiarisé.

À l'époque, en 1981, DEC finançait un salon annuel pour ses produits et, une année, le salon devait se tenir à Los Angeles. Un magazine pour utilisateurs de ce système d'exploitation avait annoncé le lancement d'un nouveau système de sécurité nommé LOCK-11. La promotion du produit était assurée par une campagne publicitaire ingénieuse, dont l'argument ressemblait peu ou prou à ceci : "Il est 3 h 30 du matin et Johnny, qui habite dans le voisinage, vient de trouver le numéro pour se connecter à votre ordinateur : 555-0336 ; il lui a fallu 336 essais. Si vous ne voulez pas que cela vous arrive, il vous faut LOCK-11". La publicité suggérait que le produit était impossible à pirater. Et il serait en démonstration au salon.

J'étais moi-même curieux de voir le produit. Un camarade de lycée, Vinny, qui pendant plusieurs années a été mon partenaire de *hacking* (et qui, plus tard, est devenu un informateur pour le compte du FBI et s'est retourné contre moi), s'intéressait également au nouveau produit de DEC, aussi nous sommes-nous rendus ensemble au salon.

Des billets de banque au bout de la ligne

Lorsque nous sommes arrivés au salon, nous avons constaté que le LOCK-11 intéressait une grande partie des visiteurs. Apparemment, les développeurs du produit étaient prêts à parier une certaine somme que personne ne parviendrait à pirater leur produit. C'était là un défi auquel je ne pouvais résister.

Nous nous sommes dirigés tout droit vers le stand du LOCK-11 et avons vu que les trois développeurs du produit tenaient le stand. Je les ai reconnus et ils m'ont reconnu : adolescent, j'avais déjà une certaine réputation comme *phreaker* et *hacker* parce que le *Los Angeles Times* avait publié un long article sur mes premiers démêlés avec les autorités. Cet article indiquait que j'avais réussi à pénétrer en pleine nuit dans les locaux de la compagnie Pacific Telephone et que j'en étais ressorti avec des manuels d'ordinateurs sous les bras, au nez et à la barbe du personnel de surveillance. (Apparemment, le *L. A. Times* voulait faire dans le sensationnel, et cela les arrangeait de publier mon nom. Mais comme j'étais mineur à l'époque, l'article allait à l'encontre des

règles de la profession, et sans doute de la loi, qui interdisait de publier les noms de mineurs accusés de délits.)

Notre arrivée au stand a suscité de la part des développeurs un certain intérêt, qui était réciproque. Ils étaient curieux à mon égard parce qu'ils me connaissaient en tant que hacker, par ouï-dire, et qu'ils étaient un peu surpris de me voir sur place. De notre côté, l'intérêt venait du billet de 100 dollars qu'ils avaient tous trois glissé dans leur badge. C'était la prime offerte à quiconque parviendrait à pirater le système ; 300 dollars représentaient une belle somme pour deux adolescents. Nous étions impatients de commencer.

Le LOCK-11 se fondait sur un principe établi faisant appel à deux niveaux de sécurité. L'utilisateur devait disposer, classiquement, d'un nom d'utilisateur et d'un mot de passe ; de plus, le nom d'utilisateur et le mot de passe ne fonctionnaient que s'ils étaient saisis à partir d'un terminal autorisé. Pour pirater le système, le hacker devait non seulement connaître un nom d'utilisateur et un mot de passe, mais également entrer ces informations à partir du bon terminal. Les développeurs du LOCK-11 étaient convaincus que cette manière de procéder suffisait pour empêcher toute intrusion. Nous avons donc décidé de les prendre en défaut, et de gagner un peu d'argent de poche par la même occasion.

Un homme que je connaissais, et qui était considéré comme un gourou du RSTS/E, était arrivé avant nous au stand. Plusieurs années auparavant, il m'avait mis au défi de pénétrer l'ordinateur interne de développement de DEC, après quoi ses collègues m'avaient poursuivi en justice. Depuis cette époque, il était devenu un programmeur respecté. Une fois au stand, nous apprîmes qu'il avait essayé de pirater le système de sécurité LOCK-11 peu avant notre arrivée, mais qu'il avait échoué. Cet incident rendait les développeurs encore plus confiants quant à l'invulnérabilité de leur produit.

Le pari était simple : celui qui pénétrait le système gagnait la somme en jeu. Une bonne publicité pour le produit, sauf bien sûr si quelqu'un devait parvenir à pirater le système. Les développeurs étaient tellement sûrs d'eux qu'ils avaient affiché sur le stand des noms d'utilisateur et des mots de passe pour une partie des comptes du système. Et ce non seulement pour des comptes normaux, mais aussi pour des comptes privilégiés.

En réalité, ils prenaient moins de risques qu'on pourrait le croire : je savais que dans ce type de système, chaque terminal est connecté à l'un des ports de l'ordinateur lui-même. Il ne fallait pas être très malin pour deviner qu'ils avaient connecté les cinq terminaux du hall d'exposition de telle manière que les visiteurs ne puissent ouvrir de session qu'en tant qu'utilisateurs non privilégiés ; autrement dit, il n'était possible d'ouvrir des session que pour des comptes ne disposant pas de privilèges administrateur. Deux approches étaient envisageables : soit tenter de contourner le logiciel de sécurité, ce que le système LOCK-11 était censé empêcher ; soit échapper au système de sécurité d'une manière qui n'avait pas du tout été prévue par les développeurs.

Le défi relevé

Vinny et moi nous sommes éloignés du stand et j'ai conçu un plan. Nous nous sommes promenés innocemment, surveillant le stand de loin. À l'heure du déjeuner, quand les allées du salon ont été moins fréquentées, les trois développeurs ont décidé de prendre une pause et d'aller déjeuner, laissant sur le stand une jeune femme qui était sans doute l'épouse ou la petite amie de l'un d'eux. Nous nous sommes approchés du stand et j'ai engagé la conversation avec la jeune femme, en lui posant des questions telles que "Depuis combien de temps travaillez-vous pour cette société ?", "Quels autres produits propose l'entreprise ?", etc.

Pendant ce temps, Vinny, hors de son champ de vision, s'était mis au travail, se servant d'une compétence que nous avions développée tous les deux. En plus de notre fascination pour les ordinateurs et de mon propre intérêt pour la prestidigitation, nous avions tous deux appris à crocheter les serrures. Enfant, j'avais écumé les rayons d'une librairie *underground* de la région de Los Angeles, qui proposait des ouvrages montrant comment crocheter des serrures, se libérer de menottes, créer des faux papiers, toutes choses qu'un enfant n'est pas censé connaître.

Vinny, tout comme moi, s'était exercé à crocheter les serrures, et il avait acquis une relative rapidité avec les serrures conventionnelles. À une époque, j'aimais faire des farces avec les serrures ; ainsi, quand quelqu'un utilisait deux serrures pour plus de sécurité, je m'amusais à les crocheter toutes deux, à les démonter et à les remettre en place en inversant leur position. Le propriétaire des serrures ne comprenait pas ce qui lui arrivait lorsqu'il tentait d'ouvrir chacune des serrures avec la mauvaise clé.

Sur le stand, je continuais à distraire la jeune femme tandis que Vinny, accroupi derrière le stand de manière à ne pas être vu, crochetait la serrure du meuble qui renfermait le mini-ordinateur PDP-11 et le branchement des câbles. Le crochetage du meuble n'a posé aucun problème : il était muni d'une serrure dite à paillettes, que même des crocheteurs amateurs tels que nous parvenions à crocheter facilement.

Il n'a fallu qu'une minute environ à Vinny pour crocheter la serrure. Dans le meuble, il a trouvé exactement ce à quoi il s'attendait : une série de ports

pour la connexion des terminaux utilisateur, et un port particulier pour ce qu'on appelle le *terminal console*. C'est ce terminal qui est utilisé par l'opérateur ou l'administrateur système pour accéder à tous les ordinateurs. Vinny a branché le câble du port console sur l'un des terminaux du stand.

L'un des terminaux était maintenant reconnu en tant que terminal console. Je me suis installé devant le terminal recâblé et ai ouvert une session en utilisant l'un des mots de passe que les développeurs avaient gentiment fourni. Le logiciel LOCK-11 a vu que j'ouvrais une session à partir d'un terminal autorisé et m'a permis de me connecter avec des privilèges d'administrateur. J'ai ensuite modifié les paramètres du système d'exploitation de manière à pouvoir ouvrir une session administrateur à partir de tous les terminaux du stand.

Une fois ma modification effectuée, Vinny s'est remis au travail : il a rétabli les connexions initiales des câbles, puis a crocheté à nouveau la serrure, cette fois pour refermer le meuble.

J'ai affiché le contenu du répertoire pour savoir quels fichiers se trouvaient sur l'ordinateur. J'ai cherché le programme LOCK-11 et les fichiers associés, et j'ai trouvé quelque chose de plus surprenant : un répertoire qui n'aurait pas dû se trouver sur cette machine. Les développeurs étaient si sûrs d'eux-mêmes et de l'invulnérabilité de leur système qu'ils n'avaient pas cru bon de supprimer le code source de leur nouveau produit ! Je suis passé au terminal d'impression adjacent et ai commencé à imprimer une partie du code source sur les bandes de papier continu dont on se servait à l'époque.

Vinny venait tout juste de verrouiller la serrure et de me rejoindre quand les développeurs sont arrivés de leur déjeuner. Ils m'ont trouvé assis devant le terminal, en train de tapoter tandis que l'imprimante continuait à travailler. "Qu'est-ce que tu fais, Kevin ?" m'a demandé l'un d'entre eux.

"J'imprime juste votre code source", ai-je répondu. Bien entendu, ils ont pensé que je plaisantais, du moins jusqu'à ce qu'ils jettent un coup d'œil à l'imprimante, et qu'ils voient qu'il s'agissait bien de leur précieux code source.

Ils ne pouvaient croire que j'avais ouvert une session en tant qu'utilisateur privilégié. "Appuie sur Contrôle+T", m'a demandé l'un des développeurs, ce que j'ai fait. L'affichage de l'écran a confirmé mes dires. Le développeur s'est frappé le front, tandis que Vinny a dit : "Trois cents dollars, s'il vous plaît".

Le message de Mitnick

Encore un exemple de personnes très intelligentes qui sous-estiment leur adversaire. Qu'en est-il de vous ? Seriez-vous prêt à parier trois cents dollars (ou euros) sur le fait que votre système informatique est inviolable ? Parfois, la méthode utilisée pour contourner une protection technologique n'est pas celle qu'on attend.

Ils ont payé, et Vinny et moi avons parcouru le salon avec les billets de cent dollars glissés dans notre badge. Tout le monde savait ce que signifiaient ces billets.

Bien entendu, Vinny et moi n'étions pas venus à bout du logiciel, et si les développeurs avaient établi de meilleures règles pour leur pari, s'ils avaient employé une serrure plus sûre ou avaient mieux surveillé leur équipement, il n'auraient pas été humiliés par un duo d'adolescents ce jour-là.

J'ai appris par la suite que les développeurs ont dû passer à la banque pour retirer de l'argent : ces billets de cent dollars étaient tout ce qu'ils avaient initialement prévu pour leurs dépenses.

LE DICTIONNAIRE, UN MOYEN D'ATTAQUE

Lorsqu'un assaillant parvient à se procurer un mot de passe, il peut accéder au système de la victime. Dans la plupart des cas, la victime n'est même pas consciente de l'intrusion.

Un jeune pirate informatique que j'appellerai Ivan Peters avait pour objectif d'obtenir le code source d'un nouveau jeu électronique. Il n'a eu aucune difficulté à accéder au réseau étendu (WAN, *Wide Area Network*) de l'entreprise parce qu'un de ses amis hackers avait déjà réussi à pénétrer l'un de ses serveurs Web. Après avoir découvert que le serveur Web présentait une faille qui n'avait pas été corrigée, son ami a failli tomber de sa chaise en s'apercevant que la machine avait également été configurée en tant que *hôte à double réseau (ou réseau double)*, ce qui voulait dire qu'il disposait d'un point d'entrée pour le réseau interne de l'entreprise.

Mais une fois qu'Ivan a été connecté, il a dû faire face à un problème qui est à peu près celui de quelqu'un qui se trouve au musée du Louvre et cherche la Joconde. En l'absence de plan, la recherche pouvait durer pendant des semaines. En l'occurrence, il avait affaire à une très grosse société, avec des centaines de bureaux et des milliers de serveurs, et bien entendu, le plan du réseau n'était pas fourni.

Plutôt que d'avoir recours à une approche technique pour savoir quel serveur il devait cibler, Ivan a fait appel à ses dons de manipulateur. Il a passé quelques appels téléphoniques en utilisant des méthodes comparables à celles décrites dans les autres chapitres de ce livre. Il a d'abord appelé le support informatique, dit qu'il était un salarié et qu'il avait un problème d'interface avec un des produits conçus par son groupe, puis a demandé le numéro de téléphone du chef de projet chargé du jeu qui l'intéressait.

Il a ensuite appelé ce chef de projet en faisant croire qu'il faisait partie du département informatique. "En cours de soirée, dit-il, nous allons installer un nouveau routeur et nous voulons éviter que vous perdiez votre connexion avec vos serveurs. Pour cela, nous devons savoir quels serveurs vous utilisez." Les mises à jour du réseau étaient fréquentes. Et le nom d'un serveur ne pouvait pas servir à grand-chose, n'est-ce pas ? Il était protégé par mot de passe ; tout seul, le nom du serveur ne permettait donc à personne d'y accéder. Le chef de projet a donc donné le nom du serveur, sans prendre la peine de rappeler son interlocuteur pour s'assurer de la véracité de ses dires, ni même noter ses nom et numéro de téléphone. Les serveurs s'appelaient ATM5 et ATM6.

Attaque du mot de passe

Ivan est alors passé à une méthode plus technique pour obtenir les informations d'authentification. Sur les systèmes qui permettent un accès à distance, la première étape de la plupart des attaques techniques consiste à identifier un compte au mot de passe faible, qui fait office de point d'entrée initial dans le système.

Lorsqu'un assaillant se sert d'outils logiciels pour tenter d'identifier des mots de passe à distance, il doit généralement rester connecté au réseau de l'entreprise pendant un certain temps, parfois pendant des heures. C'est un risque pour lui : plus il reste connecté longtemps, plus il est susceptible d'être détecté.

Pour Ivan, la première étape a donc consisté à effectuer une énumération, qui dévoile des détails sur le système cible. Là encore, Internet permet d'accéder facilement à toutes sortes de logiciels utiles à cette fin (à l'adresse http://ntsleuth.0catch.com ; le caractère avant "catch" est un zéro). Ivan a trouvé plusieurs logiciels d'énumération en téléchargement, qui lui ont évité d'effectuer ce travail à la main, ce qui aurait pris plus de temps et augmenté ses risques d'être repéré. Sachant que sa cible se servait principalement des serveurs Windows, il a téléchargé NBTEnum, un utilitaire d'énumération NetBIOS (*Network basic input/output system*, interface de programmation réseau bas niveau). Il a saisi l'adresse IP (Internet) du serveur ATM5, puis a lancé l'utilitaire. Celui-ci a rapidement identifié plusieurs comptes sur le serveur.

Jargon

Énumération
Processus qui permet de dévoiler les services disponibles sur le système cible, le système d'exploitation utilisé et une liste des noms de comptes grâce auxquels on peut accéder au système.

Une fois les comptes identifiés, le même outil d'énumération permet de lancer une attaque du système par dictionnaire. L'attaque par dictionnaire est une technique bien connue des spécialistes de la sécurité informatique et des hackers, mais dont l'existence peut surprendre la plupart des gens. Cette attaque consiste à identifier le mot de passe des utilisateurs d'un système en se fondant sur des mots courants.

Tout le monde est paresseux dans ce domaine, mais je suis toujours étonné de constater à quel point, lorsque la plupart des utilisateurs choisissent leurs mots de passe, créativité et imagination semblent entièrement leur faire défaut. La majorité des utilisateurs choisissent un mot de passe qui offre une certaine protection mais qui est également facile à retenir ; il doit donc s'agir de quelque chose qui leur est proche : les initiales de la personne ou son surnom, le nom du conjoint, la chanson, le film ou la bière préférée, par exemple. Ou encore le nom de la rue où on habite, le modèle de voiture qu'on utilise, le village où l'on passe ses vacances d'été ou le ruisseau où on va pêcher… Qu'est-ce que tous ces mots ont en commun ? Il s'agit principalement de noms de personnes, de lieux ou de noms communs. Une attaque par dictionnaire consiste à essayer très rapidement, pour un ou plusieurs comptes d'utilisateurs, une série de mots courants.

Ivan a exécuté son attaque par dictionnaire en trois étapes. Pour la première étape, il a utilisé une liste contenant 800 des mots de passe les plus courants, parmi lesquels on trouve *secret*, *work* (travail) et *password* (mot de passe). Le logiciel a également effectué des permutations, en ajoutant à chaque mot un chiffre ou le nombre correspondant au mois en cours, et tous ces mots ont été essayés pour chacun des comptes identifiés. Sans résultat.

Pour son essai suivant, Ivan a recherché les termes "*wordlists dictionaries*" (listes de mots, dictionnaires) *via* le moteur de recherche Google. Il a trouvé des milliers de sites comprenant des listes de mots complètes pour l'anglais et

plusieurs langues étrangères. Il a téléchargé un dictionnaire anglais complet et l'a complété avec plusieurs listes de mots téléchargés à partir du site www.outpost9.com/files/WordLists.html.

Sur ce site, dont l'accès est gratuit, les mots sont regroupés par listes spécialisées : noms et prénoms de personnes, noms des députés et sénateurs américains, noms d'acteurs et mots tirés de la Bible, par exemple. Ces mêmes listes de mots sont accessibles par l'intermédiaire du serveur FTP de l'Université d'Oxford, à l'adresse ftp://ftp.ox.ac.uk/pub/wordlists.

D'autres sites proposent des listes de noms tirés de dessins animés, de mots utilisés dans l'Odyssée, dans Star Trek, dans le domaine des sciences ou de la religion, ou encore dans les œuvres de Shakespeare, de Tolkien, etc. Une société en ligne propose une liste contenant 4,4 millions de mots et de noms pour la modique somme de 20 dollars. On peut également configurer le logiciel pour qu'il essaie les anagrammes des mots du dictionnaire — autre méthode fréquemment employée par les utilisateurs pour augmenter la sécurité de leurs mots de passe.

Plus vite qu'on le pense

Une fois qu'Ivan a eu décidé de la liste de mots à employer et que l'attaque a été lancée, il a pu se consacrer à d'autres tâches. C'est probablement ce qui peut paraître le plus incroyable : on pourrait penser qu'après avoir lancé une telle attaque, l'assaillant pourrait aller se coucher en attendant et, à son réveil, constater que la situation n'a pas beaucoup évolué. En réalité, en fonction de la plate-forme attaquée, de la configuration de la sécurité du système et de la connexion réseau, il est possible d'essayer tous les mots de la langue anglaise en moins de trente minutes ![1]

Pendant que sa première attaque suivait son cours, Ivan a lancé, à l'aide d'un deuxième ordinateur, une attaque sur l'autre serveur utilisé pour le développement du jeu, ATM6. Vingt minutes plus tard, le logiciel avait réussi ce que beaucoup d'utilisateurs croient impossible à réaliser : la découverte d'un mot de passe. L'un des utilisateurs avait choisi le mot de passe "Frodon", le nom de l'un des hobbits du *Seigneur des anneaux*.

Ivan a alors pu ouvrir une session sur le serveur ATM6 avec le nom d'utilisateur et le mot de passe qu'il avait trouvés.

Il a constaté deux choses, l'une bonne, l'autre mauvaise. La bonne chose était que le compte pour lequel il disposait du nom d'utilisateur et du mot de passe était un compte administrateur, ce qui allait être essentiel pour la prochaine étape. En revanche, le code source ne se trouvait nulle part ; il devait donc être sur l'autre serveur, ATM5, dont Ivan savait déjà qu'il résistait aux attaques par dictionnaire. Mais il n'abandonnait pas encore : il lui restait quelques trucs à essayer.

Sur certains systèmes d'exploitation Windows et UNIX, les empreintes (*hashes*) des mots de passe sont à la disposition de quiconque a accès à l'ordinateur sur lequel elles sont stockées, suivant le raisonnement que l'empreinte ne peut être "cassée" et qu'elle ne nécessite par conséquent aucune protection. Or ce raisonnement est faux. À l'aide d'un autre utilitaire nommé pwdump3, également disponible sur Internet, Ivan est parvenu à trouver les empreintes des mots de passe du serveur ATM6 et à les télécharger.

Un fichier typique d'empreintes de mots de passe ressemble à ceci :

```
Administrator:500:95E4321A38AD8D6AB75E0C8D76954A50:2E48927A0
B04F3BFB341E26F6D6E9A97:::
akasper:1110:5A8D7E9E3C3954F642C5C736306CBFEF:393CE7F90A8357
F157873D72D0490821:::
digger:1111:5D15C0D58DD216C525AD3B83FA6627C7:17AD56414430 8B4
2B8403D01AE256558:::
ellgan:1112:2017D4A5D8D1383EFF17365FAF1FFE89:07AEC950C22CBB9
C2C734EB89320DB13:::
tabeck:1115:9F5890B3FECCAB7EAAD3B435B51404EE:1F0115A72844721
2FC05E1D2D820B35B:::
vkantar:1116:81A6A5D035596E7DAAD3B435B51404EE:B933D36DD12258
946FCC7BD153F1CD6E:::
vwallwick:1119:25904EC665BA30F4449AF42E1054F192:15B2B7953FB6
32907455D2706A432469:::
mmcdonald:1121:A4AED098D29A3217AAD3B435B51404EE:E40670F936B7
9C2ED522F5ECA9398A27:::
kworkman:1141:C5C598AF45768635AAD3B435B51404EE:DEC8E827A1212
73EF084CDBF5FD1925C:::
```

Une fois les empreintes sur son ordinateur, Ivan a eu recours à un outil différent pour passer à un autre type d'attaque de mots de passe, une attaque dite *par force brute*. Ce genre d'attaque consiste à utiliser toutes les combinaisons de caractères alphanumériques et la plupart des caractères spéciaux.

Ivan a fait appel à un utilitaire nommé L0phtcrack (prononcer "loftcrack"), disponible sur le site www.atstake.com (www.elcomsoft.com est une autre très bonne source d'outils de récupération de mots de passe). Les administrateurs système se servent de cet utilitaire pour identifier les mots de passe faibles ; les assaillants l'utilisent pour les casser. La fonction force brute de L0phtcrack teste toutes les combinaisons possibles de toutes les lettres et de tous les chiffres, ainsi que certains caractères spéciaux (!@#$%^&, entre

1. N.D.T. : Et le français compte beaucoup moins de mots que l'anglais.

autres). Notez toutefois que L0phtcrack ne permet pas de casser un mot de passe contenant des caractères non imprimables.

L0phtcrack est extrêmement rapide : il peut essayer jusqu'à 2,8 millions de combinaisons par seconde sur une machine équipée d'un processeur à 1 GHz. Toutefois, même à cette vitesse, et si l'administrateur a correctement configuré Windows (en désactivant l'utilisation des empreintes LANMAN), le temps nécessaire pour casser un mot de passe peut être considérable.

Jargon

Attaque par force brute
Technique de détection de mot de passe qui consiste à essayer toutes les combinaisons possibles de caractères (lettres, chiffres et symboles).

De ce fait, l'assaillant télécharge généralement les empreintes et exécute l'attaque sur sa propre machine (ou sur une autre) plutôt que de rester connecté au réseau de l'entreprise et de risquer de se faire repérer.

Pour Ivan, l'attente n'a pas été très longue. Quelques heures plus tard, le logiciel avait découvert les mots de passe de chacun des membres de l'équipe de développement. Mais ces mots de passe concernaient les utilisateurs de la machine ATM6, et il savait déjà que le code source du jeu ne se trouvait pas sur ce serveur.

Et maintenant ? Il n'avait toujours pas de mot de passe pour un compte du serveur ATM5. Il lui restait encore une possibilité : connaissant les mauvaises habitudes de la plupart des utilisateurs en matière de sécurité, il se dit que l'un des membres de l'équipe avait peut-être choisi le même mot de passe pour les deux machines.

Et c'était le cas. L'un des membres de l'équipe utilisait le mot de passe "gamers" sur les deux serveurs, ATM5 et ATM6.

Les portes lui étaient maintenant grandes ouvertes. Il a cherché un moment avant de trouver le code source en question, l'a téléchargé puis a effectué une dernière opération, classique pour les pirates informatiques : il a modifié le mot de passe d'un compte inutilisé disposant de droits d'administrateur, ce qui lui permettrait d'accéder à une version mise à jour du logiciel à l'avenir.

Analyse du stratagème

Le principe de cette attaque se fonde sur des vulnérabilités à la fois humaines et techniques. L'assaillant a d'abord réussi, en téléphonant sous un faux prétexte, à localiser et à identifier les noms d'hôtes des serveurs qui contenaient les informations recherchées.

Il a ensuite fait appel à un utilitaire pour identifier les noms d'utilisateur de tous les comptes des serveurs qui l'intéressaient. Il a alors lancé deux attaques sur les mots de passe, la première étant une attaque par dictionnaire, qui consiste à utiliser tous les mots courants d'une langue, et éventuellement une liste de noms propres : noms, prénoms, lieux, etc.

Les outils de *hacking*, commerciaux ou gratuits, sont à la disposition de quiconque, que ses intentions soient bonnes ou mauvaises. Il est donc essentiel d'être vigilant en ce qui concerne la protection des systèmes informatiques de l'entreprise et de son infrastructure réseau.

Le message de Mitnick

> Pour reprendre la terminologie du Monopoly, si vous utilisez un mot du dictionnaire comme mot de passe, vous allez directement en prison. Vous ne passez pas par la case Départ et ne touchez pas 20 000 dollars. Vous devez apprendre aux salariés à choisir des mots de passe qui protègent réellement votre système.

L'importance de cette menace est largement sous-estimée. À ce propos, le magazine *ComputerWorld* a publié les étonnants résultats d'une analyse portant sur les fonds de placement Oppenheimer, basés à New York. Le vice-directeur du département de la sécurité réseau de ces fonds a lancé une attaque sur les mots de passe des salariés de l'entreprise en utilisant un logiciel en vente libre. En *trois minutes*, il avait cassé le mot de passe de 800 salariés !

MESURES DE PRÉVENTION

Les attaques des manipulateurs deviennent encore plus dangereuses lorsqu'ils s'aident de moyens technologiques. Pour prévenir ce type d'attaques, il est nécessaire de prendre des mesures à la fois sur le plan humain et sur le plan technique.

Apprendre à dire non

Dans le premier récit de ce chapitre, l'employée du RCMAC n'aurait pas dû modifier le statut des dix lignes pour leur permettre de recevoir des appels entrants en l'absence de tout ordre officiel. Les salariés ne doivent pas seulement *connaître* les règles et les procédures de sécurité ; ils doivent comprendre à quel point ces règles sont importantes pour éviter tout acte de malveillance.

Le respect des règles de sécurité peut être obtenu par un système de récompenses et de contraintes. Bien entendu, ces règles doivent rester réalistes et ne pas inclure de procédures trop astreignantes pour être appliquées. Par ailleurs, des programmes de sensibilisation aux problèmes de sécurité doivent convaincre les salariés que s'il est important d'accomplir ses tâches dans les délais impartis, l'utilisation de raccourcis, s'ils contreviennent aux procédures de sécurité, peuvent mettre en péril les collègues et l'entreprise tout entière.

Les mêmes règles de prudence s'appliquent quand on fournit des informations à un inconnu au téléphone. Même si la personne se présente de manière très convaincante, quel que soit son statut ou son niveau hiérarchique dans la société, *aucune* information autre que les informations accessibles au public ne doit être fournie tant que l'identité de la personne n'a pas été établie de manière formelle. Si ces règles avaient été suivies, la manipulation décrite dans la première partie de ce chapitre aurait échoué et le détenu Gondorff n'aurait pas pu planifier une nouvelle escroquerie avec son complice Hooker.

C'est là un point si important que je le répète tout au long de ce livre : il faut vérifier, vérifier, vérifier. Toute demande qui n'est pas faite en personne ne doit pas être acceptée tant que l'individu n'a pas été formellement identifié, point final.

Nettoyage

Pour toutes les sociétés qui ne peuvent s'offrir les services d'un agent de sécurité permanent, la possibilité qu'un intrus pénètre dans les locaux en dehors des heures de travail représente un vrai problème. En général, les équipes de nettoyage sont respectueuses vis-à-vis de toute personne qui semble faire partie de l'entreprise. Après tout, cette personne pourrait leur causer des ennuis, voire les faire renvoyer. Pour cette raison, le personnel d'entretien, qu'il soit interne à l'entreprise ou recruté par l'intermédiaire d'une agence spécialisée, doit être formé aux questions de sécurité physique.

Pas besoin de baccalauréat ni même de parler la langue du pays pour effectuer un travail de nettoyage. La formation, quand formation il y a, consiste généralement à expliquer quel produit de nettoyage utiliser dans quelle situation. Il est exceptionnel qu'on explique au personnel que quand quelqu'un veut accéder aux bureaux en dehors des heures de travail, il faut lui demander le badge de la société, puis appeler les bureaux de la compagnie de nettoyage, expliquer la situation et attendre une autorisation.

Toute entreprise doit prévoir le type de situation décrit dans ce chapitre et former son personnel en conséquence. Mon expérience personnelle est que la plupart, voire toutes les entreprises du secteur privé sont très laxistes dans ce domaine de la sécurité physique. Il peut aussi être utile d'avoir une approche inverse du problème et de responsabiliser les salariés de l'entreprise plutôt que le personnel d'entretien. Ainsi, l'entreprise pourra exiger de ses salariés qu'ils viennent systématiquement avec leurs propres clés ou cartes d'accès pour accéder aux bureaux en dehors des heures de travail, et qu'ils n'obligent jamais le personnel d'entretien à les laisser entrer. Le personnel d'entretien, quant à lui, doit obéir à une règle simple : ne jamais ouvrir à personne, sous aucun prétexte. Cette règle peut même faire l'objet d'une clause lors de l'établissement du contrat avec la société de nettoyage.

Par ailleurs, les équipes d'entretien doivent connaître la technique qui consiste, pour un intrus, à se mêler à un groupe de personnes autorisées pour accéder à des zones sensibles de l'entreprise. Elles doivent également apprendre à refuser l'entrée à des personnes qui les suivraient dans le bâtiment, même si ces personnes semblent être des salariés de l'entreprise.

Réalisez ensuite des tests à intervalles réguliers (trois ou quatre fois par an, par exemple) afin d'évaluer l'efficacité des mesures que vous avez prises. Demandez à un salarié de se présenter à l'entrée de l'entreprise en dehors des heures de travail et d'essayer de convaincre le personnel d'entretien de le laisser entrer. Vous pouvez également faire appel à une société spécialisée dans ce type de test de vulnérabilité.

Protéger ses mots de passe

Les entreprises ont de plus en plus tendance à recourir à des moyens techniques pour renforcer leur sécurité, en configurant les systèmes d'exploitation de manière à imposer l'utilisation de mots de passe et en limitant le nombre de mots de passe qui peuvent être saisis avant de verrouiller un compte donné. En fait, les systèmes Microsoft Windows dédiés aux entreprises incluent cette fonction de verrouillage. Du fait que les clients sont souvent agacés par les fonctions qui requièrent des efforts supplémentaires de leur

part, lors de l'installation des logiciels, les fonctions de sécurité sont souvent désactivées par défaut. Il serait temps que les éditeurs de logiciels changent d'attitude et activent par défaut les fonctions de sécurité ; je pense d'ailleurs qu'ils y viendront bientôt.

Bien entendu, les règles de sécurité de l'entreprise doivent obliger les administrateurs système à utiliser tous les moyens techniques à leur disposition pour renforcer la sécurité des systèmes informatiques, l'objectif étant de dépendre le moins possible des individus, plus susceptibles de commettre des erreurs. À l'évidence, quand on limite le nombre de mots de passe erronés successifs pour un compte donné, on rend les choses nettement plus difficiles pour les assaillants potentiels.

Toutes les entreprises doivent trouver un équilibre entre sécurité et productivité ; certains salariés ont tendance à tout miser sur le second facteur au détriment du premier, n'acceptant pas l'importance des mesures de sécurité pour la protection de l'intégrité des informations confidentielles de l'entreprise.

Quand les règles de l'entreprise sont muettes sur un sujet donné, les salariés risquent de prendre la voie de la moindre résistance et d'agir d'une manière qui les arrange et qui simplifie leur travail. Certains salariés pourront s'opposer à tout changement et ignorer ouvertement les règles de base en matière de sécurité. Vous avez peut-être déjà eu affaire à ce type de personnes, qui respectent les règles concernant la longueur et la complexité du mot de passe, mais qui notent ensuite ce mot de passe sur un Post-it qu'elles collent sans vergogne sur leur moniteur.

Le choix de mots de passe difficiles à identifier et l'activation des fonctions de sécurité de votre système informatique sont des éléments essentiels pour la protection de votre entreprise.

Pour plus de détails sur la manière de choisir des mots de passe, reportez-vous au Chapitre 16.

Chapitre 12

Les attaques visant le salarié de base

Comme le montrent de nombreuses anecdotes de ce livre, l'attaque du manipulateur expérimenté porte souvent sur des salariés situés aux niveaux inférieurs de la hiérarchie. Il est souvent facile de manipuler ces personnes pour obtenir une information apparemment sans valeur, mais qui rapproche le manipulateur de son but, à savoir l'obtention d'informations plus confidentielles.

L'assaillant attaque souvent le "salarié de base" parce qu'il est fréquent que celui-ci ignore la valeur d'une information donnée au niveau de l'entreprise, ou les conséquences possibles de certaines actions. Par ailleurs, il se laisse souvent influencer par certaines techniques courantes chez les manipulateurs, comme le fait de se prévaloir d'un niveau hiérarchique plus élevé, d'être sympathique et chaleureux, de donner l'impression de connaître des collègues de la victime, de faire jouer l'urgence de la situation ou de laisser croire à la victime qu'elle pourra tirer un bénéfice de son rapport avec le manipulateur.

Voici quelques exemples d'attaques qui visent le salarié de base.

L'AGENT DE SÉCURITÉ SERVIABLE

Les escrocs savent que les personnes cupides sont des victimes toutes désignées parce qu'elles se laissent plus facilement duper que les autres. Quand ils ciblent un membre d'une équipe de nettoyage ou de surveillance, les manipulateurs recherchent plutôt quelqu'un de sympathique et de

serviable, qui sera le plus susceptible de les aider, comme le montre le récit qui suit.

Le point de vue d'Elliot

Date et heure : 21 h 30, un mardi du mois de février 1998.

Lieu : Les bureaux de Marchand Microsystems, à Nashua, dans le New Hampshire.

Elliot Stanley savait qu'il n'avait pas le droit de sortir du bureau de la sécurité en dehors de ses heures de ronde. Mais on était au milieu de la nuit, et il n'avait vu personne depuis qu'il avait pris son service. Et puis il était presque l'heure d'effectuer ses rondes. Le pauvre type, au bout du fil, avait vraiment l'air désespéré. Et ça fait toujours tellement plaisir de pouvoir rendre un petit service.

Le point de vue de Bill

Bill Goodrock avait un objectif simple, qu'il s'était fixé à l'âge de douze ans et dont il ne s'était jamais départi : prendre sa retraite à vingt-quatre ans, sans toucher à un seul centime de l'héritage que son père avait placé dans un *trust fund*. Il allait montrer à son père, ce puissant banquier, qu'il pouvait réussir seul.

Il ne lui restait que deux ans, et il était clair, maintenant, qu'il ne ferait pas fortune dans les vingt-quatre mois en se transformant en homme d'affaires brillant ou en requin de la finance. Il envisage brièvement de braquer des banques, mais il sait que c'est une solution illusoire : le risque est bien trop élevé pour le bénéfice qu'il peut en retirer. Il rêve donc de réaliser un "Rifkin", c'est-à-dire un vol de banque électronique.

La dernière fois que Bill avait été en Europe avec ses parents, il avait ouvert un compte à Monaco où il avait déposé 100 francs. Le solde du compte n'était toujours que de 100 francs, mais il avait un plan qui allait lui permettre d'atteindre rapidement un montant à sept chiffres, voire huit avec un peu chance.

La petite amie de Bill, Anne-Marie, travaille au département fusions-acquisitions d'une grande banque de Boston. Un soir, pendant qu'il attend dans les locaux de la banque qu'elle sorte d'une réunion, il cède à la curiosité et branche son ordinateur portable sur le port Ethernet de la salle de réunion où il se trouve. Bingo ! Il est connecté au réseau interne de la banque, derrière son pare-feu. Ce qui lui donne une idée.

Il associe ses compétences avec celles d'un camarade de classe qui connaît une jeune fille nommée Julia, une brillante étudiante en informatique qui effectue un stage chez Marchand Microsystems. Julia semble être une excellente source d'informations sur des sujets sensibles. Ils lui racontent qu'ils écrivent le scénario d'un film, et elle les croit. Elle trouve amusant d'inventer une histoire avec eux et de leur donner tous les détails sur la manière dont il serait possible de réaliser le coup qu'ils décrivent. En fait, elle trouve l'idée brillante et ne cesse d'insister pour faire partie du générique du film. Ils la mettent en garde contre le plagiat de scénarios et lui font jurer de ne jamais en parler à personne.

Une fois que Julia a fourni toutes les informations nécessaires, Bill exécute lui-même la partie risquée de l'opération, sans jamais douter de son succès.

"J'appelle en cours d'après-midi et j'apprends que le responsable de la sécurité, pour la nuit, est un homme du nom d'Isaiah Adams. À 21 h 30 ce soir-là, j'appelle l'agent de surveillance situé à l'entrée du bâtiment. L'histoire que je lui raconte repose sur le fait que la situation est urgente, et j'essaye de donner l'impression de paniquer un peu. "Ma voiture est en panne et je ne peux pas venir jusqu'au bureau, dis-je. J'ai quelque chose d'urgent à faire, et j'ai vraiment besoin de votre aide. J'ai essayé d'appeler le responsable de la sécurité, Isaiah, mais il n'est pas chez lui. Pourriez-vous me rendre ce petit service ?"

Les locaux sont vastes, et les bureaux sont identifiés par des codes courrier. Je lui indique donc le code courrier du laboratoire d'informatique et lui demande s'il sait où il se trouve. Il me répond que oui et accepte de s'y rendre pour moi, mais dit qu'il lui faudra plusieurs minutes pour y arriver. Je lui dis que je l'appellerai directement au laboratoire, en prétextant que je ne dispose que d'une seule ligne de téléphone et que je suis en train de l'utiliser pour essayer de me connecter au réseau afin de résoudre le problème.

Il est dans le labo quand j'appelle, et je lui dis où trouver la console qui m'intéresse, celle qui comporte une banderole en papier avec le nom "elmer". Julia m'a dit que c'est l'hôte qu'elle utilise pour compiler les versions publiques du système d'exploitation commercialisé par la société. Lorsqu'il me dit l'avoir trouvé, j'ai la confirmation que Julia m'a fourni des informations exactes, et mon cœur s'arrête de battre pendant un instant. Je lui fais appuyer deux ou trois fois sur la touche Entrée, et il me dit voir s'afficher le symbole de la livre. Cela signifie que l'ordinateur est connecté en tant que root, le compte superutilisateur qui dispose de tous les privilèges système. L'agent de

sécurité n'est pas un professionnel du clavier, et il n'est pas loin de paniquer lorsque je lui énonce ce que je veux qu'il tape :

```
echo 'fix:x:0:0::/:/bin/sh' >> /etc/passwd
```

Il y parvient finalement, et je dispose alors d'un compte avec le nom fix. Je lui fais ensuite taper :

```
echo 'fix::10300:0:0' >> /etc/shadow
```

J'ai ainsi défini le mot de passe chiffré, qui se trouve entre les deux deux-points. Le fait de ne rien mettre entre les deux-points indique que le mot de passe du compte est nul. Ces deux commandes suffisent pour ajouter au fichier de mots de passe le compte fix avec un mot de passe nul. Et ce compte a des privilèges de superutilisateur.

Je lui fais ensuite exécuter une commande de répertoire récursive afin d'imprimer une longue liste de noms de fichiers. Puis je lui dis de faire avancer le papier dans l'imprimante, de le détacher et de le ramener avec lui jusqu'à son bureau, sous prétexte que j'aurais peut-être besoin par la suite qu'il me lise ce qui avait été imprimé.

Le plus beau est que l'agent de sécurité ne sait absolument pas qu'il a créé un nouveau compte. L'impression des répertoires de fichiers est nécessaire pour faire disparaître les commandes qu'il a tapées auparavant. Ainsi, l'administrateur système ou l'utilisateur, le lendemain matin, ne verraient pas que la sécurité de leur système a été compromise.

Je dispose à présent d'un compte, d'un mot de passe et de tous les privilèges. Un peu avant minuit, je me connecte et je suis les instructions que Julia a soigneusement tapées "pour le scénario". En quelques instants, j'ai accès à l'un des ordinateurs de développement qui contient le code source de la nouvelle version du système d'exploitation de la société.

Je télécharge alors dans cet ordinateur un *patch* écrit par Julia, qui d'après elle modifie une instruction dans l'une des bibliothèques du système d'exploitation. En pratique, ce patch crée un *backdoor* (une "entrée de service") caché qui permet d'accéder à distance au système à l'aide d'un mot de passe secret.

Note

Le type de backdoor employé ici ne modifie pas le programme d'ouverture de session du système d'exploitation. Dans le cas présent, une fonction spécifique qui fait partie d'une bibliothèque dynamique utilisée par le programme d'ouverture de session est remplacée pour créer un point d'entrée secret. Habituellement, les pirates remplacent ou modifient le programme d'ouverture de session lui-même, mais les administrateurs système avertis peuvent détecter cette modification en comparant le programme avec celui fourni sur son support initial (un CD-ROM ou tout autre moyen de distribution).

Je suis soigneusement les instructions qu'elle a notées, installant d'abord le patch, puis supprimant le compte fix ainsi que les entrées des *logs* (journaux) pour y faire disparaître les actions que je viens d'effectuer. J'efface mes traces derrière moi, en quelque sorte.

Bientôt, l'entreprise va diffuser la mise à jour de son système d'exploitation à ses clients, des institutions financières du monde entier. Et chaque exemplaire de la mise à jour contiendra le backdoor que j'ai inséré dans la distribution avant qu'elle soit terminée. Je pourrai donc accéder à toutes les banques et maisons de courtage où la mise à jour sera installée.

Jargon

Patch
Il s'agit généralement d'une petite quantité de code qui permet de régler un problème particulier quand il est placé dans un exécutable. Se dit parfois "programme rustine" en français.

Bien entendu, j'ai encore du travail. Il faut que je parvienne à accéder au réseau interne de toutes les institutions financières auxquelles je veux "rendre visite", à déterminer quel ordinateur est utilisé pour les transferts de fonds, puis à installer un logiciel de surveillance pour connaître le détail des opérations effectuées et la manière dont les fonds sont transférés.

Mais tout cela, je peux le réaliser à distance, à partir de n'importe quel ordinateur. Sur une plage de Tahiti, par exemple.

Je rappelle l'agent de sécurité, le remercie pour son aide et lui dit qu'il peut jeter ce qu'il a imprimé.

Analyse du stratagème

L'agent de sécurité avait des instructions quant aux tâches qu'il devait effectuer, mais même des instructions complètes et bien conçues ne peuvent couvrir toutes les situations possibles. Personne ne lui avait dit qu'il pouvait causer des dégâts en tapant deux lignes sur un ordinateur pour une personne qu'il pensait être un salarié de l'entreprise.

Avec l'aide de l'agent de sécurité, il était facile d'accéder à un ordinateur particulièrement sensible, celui qui contenait la version maître de la mise à jour du système d'exploitation. Le fait que cet ordinateur se trouve derrière une porte fermée à clé ne servait ici à rien, puisque l'agent de sécurité disposait de la clé.

Même un salarié de base foncièrement honnête (ou dans le cas présent, une stagiaire étudiante en informatique) peut parfois être amené, volontairement ou involontairement, à fournir des informations cruciales qui permettent de mettre au point une attaque, comme l'emplacement de l'ordinateur cible ou, élément capital ici, la date à laquelle la nouvelle version du logiciel allait être compilée. Ce facteur est important parce qu'une modification apportée trop tôt aurait eu plus de risques d'être détectée ou d'être sans effet parce que la compilation aurait été effectuée à partir d'une autre source.

Le fait que le garde ait ramené les feuilles imprimées jusqu'à son bureau, puis les ait détruites, est également une étape importante. Sans cette mesure, les programmeurs, en arrivant le lendemain matin, auraient pu trouver les traces du piratage dans l'imprimante ou éventuellement dans la poubelle. Le fait de fournir à l'agent de sécurité une raison plausible pour qu'il emporte avec lui les feuilles imprimées permettait d'éviter ce risque.

Le message de Mitnick

> Lorsque l'assaillant ne peut accéder lui-même physiquement à un système informatique ou à un réseau, il essaie de manipuler quelqu'un pour qu'il le fasse à sa place. Quand l'accès physique est nécessaire pour une attaque, l'utilisation d'une victime en tant qu'exécutant est même préférable pour l'assaillant, qui risque ainsi beaucoup moins de se faire repérer et appréhender.

LE PATCH URGENT

On pourrait croire que quelqu'un qui travaille pour le support informatique d'une entreprise est conscient des risques qu'il y a à fournir à un étranger un accès au réseau. Mais quand cet étranger est un manipulateur qui fait croire qu'il appelle de la part d'un éditeur de logiciels, il obtient parfois des résultats inespérés.

Assistance à distance

L'interlocuteur veut savoir qui s'occupe des ordinateurs, et le standardiste le met en communication avec le responsable du support technique informatique, Paul Ahearn.

L'attaquant s'identifie en tant que "Edward, de SeerWare, l'éditeur de votre logiciel de base de données. Apparemment, toute une série de clients n'ont pas reçu l'e-mail concernant la mise à jour urgente, alors nous en appelons quelques-uns pour vérifier que personne n'a de problème avec l'installation du patch. Vous avez déjà installé la mise à jour ?"

Paul dit qu'il est à peu près sûr qu'il n'a rien vu de tel.

Edward répond alors : "Eh bien, il arrive occasionnellement que des quantités importantes de données se perdent à cause d'un bug, alors nous vous conseillons de l'installer aussi vite que possible." Ce que Paul est tout à fait prêt à faire. "Bien, dit son interlocuteur, nous pouvons vous envoyer une bande ou un CD-ROM avec le patch ; je voulais juste vous dire que c'est vraiment une mise à jour capitale. Deux sociétés ont déjà perdu plusieurs journées de données. Vous devriez donc vraiment l'installer dès qu'il arrive avant que quelque chose de similaire ne se produise chez vous."

"Je ne peux pas le télécharger à partir de votre site Web ?" demande Paul.

"Il sera bientôt disponible ; pour le moment, l'équipe technique est occupée à limiter les dégâts. Si vous voulez, notre service clientèle peut l'installer pour vous à distance. Nous pouvons le faire par Telnet (utilitaire TCP/IP qui permet d'ouvrir une session sur un hôte distant), si votre système le permet."

"Non, pas de Telnet chez nous, surtout par Internet, c'est trop risqué, répond Paul. Par contre, si vous pouvez utiliser le SSH, ça serait possible." Le SSH (*Secure SHell*) est un protocole qui permet de transférer des fichiers sécurisés.

"Oui, nous pouvons utiliser le SSH. Quelle est l'adresse IP ?"

Paul lui donne l'adresse IP, et quand son interlocuteur demande quels nom d'utilisateur et mot de passe il doit employer, il les lui fournit également.

Analyse du stratagème

Bien entendu, cet appel aurait effectivement pu provenir de l'éditeur de logiciels. Mais si c'était le cas, cette histoire n'aurait pas eu sa place dans ce livre.

Ici, le manipulateur a influencé la victime en créant un sentiment d'urgence et en jouant sur la crainte d'une perte de données tout en offrant une solution immédiate qui résoudrait le problème.

Quand un manipulateur a pour cible quelqu'un qui connaît la valeur de l'information, il doit disposer d'arguments particulièrement convaincants pour obtenir un accès distant. Le sentiment d'urgence peut alors agir en tant que diversion, la victime obéissant avant d'avoir réellement pris conscience de ce qu'on lui demande.

LA PETITE NOUVELLE

Quelles données sont utiles pour un assaillant potentiel ? Parfois, il s'agit d'informations qu'on ne pense pas du tout à protéger.

La conversation de Sarah

"Ressources humaines, Sarah à l'appareil."

"Bonjour Sarah, ici George, du parking. Vous voyez les cartes d'accès que vous utilisez pour entrer dans le parking et accéder aux ascenseurs ? Nous avons eu un problème, ici, et nous devons reprogrammer les cartes de tous ceux qui sont arrivés depuis moins de quinze jours."

"Vous voulez donc connaître leurs noms ?"

"Oui, et leurs numéros de téléphone."

"Je vais consulter la liste et je vous rappelle. À quel numéro puis-je vous joindre ?"

"Au 73... Attendez, il faut que je prenne ma pause. Je peux vous rappeler dans une demi-heure ?"

"Bon, d'accord."

Lorsqu'il rappelle, elle annonce :

"Il n'y a que deux nouveaux : Anna Myrtle, aux finances. Elle est secrétaire. Et notre nouveau vice-directeur, M. Underwood."

"Et les numéros de téléphone ?"

"Un instant... 6973 pour M. Underwood, et 2127 pour Anna Myrtle."

"Merci, vous m'avez rendu un grand service."

La conversation d'Anna

"Finances, ici Anna."

"Heureusement que j'ai trouvé quelqu'un qui soit encore au travail. Bonjour Anna, je suis Ron Vittaro ; je suis le responsable éditorial du département des livres d'entreprise. Je ne crois pas que nous ayons été présentés. Bienvenue dans la société."

"Merci."

"Écoutez, je suis à Los Angeles et j'ai un problème. J'ai besoin que vous me consacriez environ dix minutes de votre temps."

"Bien sûr. Qu'est-ce que je peux faire pour vous ?"

"Allez dans mon bureau. Vous savez où c'est ?"

"Non."

"C'est le bureau qui fait le coin, au quinzième étage ; le numéro 1502. Je vous y appelle dans quelques minutes. Quand vous serez dans mon bureau, appuyez sur la touche de renvoi, sinon la messagerie se mettra automatiquement en route."

"D'accord, j'y vais."

Dix minutes plus tard, elle est dans son bureau et a annulé le renvoi vers la messagerie. Elle décroche quand le téléphone sonne. Il lui dit de s'asseoir devant l'ordinateur et de lancer Internet Explorer. Quand il c'est fait, il lui demande de taper l'adresse suivante : www.geocities.com/ron_insen/manuscript.doc.exe.

Une boîte de dialogue apparaît, et il lui dit de cliquer sur Ouvrir. L'ordinateur semble télécharger le manuscrit, puis l'écran devient noir. Lorsqu'elle l'informe du problème, il répond : "Oh non, ça recommence. Nous avions souvent des problèmes de téléchargement à partir de ce site, mais je croyais que c'était réglé. Tant pis, je me débrouillerai pour obtenir le fichier autrement plus tard." Il lui demande ensuite de redémarrer l'ordinateur pour être sûr qu'il fonctionne encore correctement après le problème qu'elle a eu. Il lui indique les étapes à suivre pour relancer le système.

Une fois l'ordinateur de nouveau en fonction, il la remercie chaleureusement et raccroche. Anna retourne au service financier pour finir le travail qu'elle a commencé un peu plus tôt.

Le point de vue de Kurt Dillon

Les éditions Millard-Fenton étaient ravies de l'auteur avec lequel elles étaient sur le point de signer, un dirigeant d'une entreprise du *Fortune 500*, qui était à la retraite et dont les mémoires étaient passionnants. Quelqu'un avait suggéré à l'auteur de se tourner vers un chef de département pour la négociation du contrat. Le chef de département ne voulait pas admettre qu'il n'y connaissait rien en contrats d'édition, aussi avait-il engagé un vieil ami pour qu'il lui indique ce qu'il devait savoir. Malheureusement, ce vieil ami n'était pas un très bon choix. Kurt Dillon utilisait pour ses recherches des méthodes qui n'étaient pas tout à fait orthodoxes, et qui en fait étaient même à la limite de la légalité.

Dillon a souscrit à une offre d'hébergement gratuit chez Geocities sous le nom de Ron Vittaro, puis a placé sur le site nouvellement créé un logiciel espion (*spyware*). Il a changé le nom du logiciel en *manuscript.doc.exe* afin de faire croire qu'il s'agissait d'un document Word, donc moins suspect. Cette astuce a fonctionné encore mieux que prévu parce que Vittaro n'avait jamais changé un des paramètres par défaut de Windows, nommé "Masquer les extensions des fichiers dont le type est connu". De ce fait, le fichier s'est affiché en tant que "manuscript.doc".

Il a ensuite demandé à une amie d'appeler la secrétaire de Vittaro. Suivant les consignes de Dillon, elle a dit : "Je suis l'assistante de Paul Spadone, le président de Ultimate Bookstores, à Toronto. M. Vittaro a rencontré M. Spadone au cours d'un salon, il y a un moment de cela, et il lui a demandé de l'appeler pour discuter d'un projet commun éventuel. Comme M. Spadone est souvent absent, il m'a demandé de vous appeler pour savoir quand M. Vittaro serait présent dans vos bureaux."

Quand elles ont eu comparé les plannings, l'amie disposait d'un nombre suffisant de dates pour pouvoir indiquer à Dillon à quel moment Vittaro serait présent au bureau. Ce qui voulait dire qu'il savait également quand il serait *absent*. Il n'avait pas fallu discuter pendant longtemps pour apprendre que la secrétaire de Vittaro profiterait de son absence pour partir au ski. Pendant une brève période, tous deux seraient donc absents du bureau.

Jargon

Logiciel espion (*spyware*)
Logiciel qui permet de surveiller secrètement les activités d'un ordinateur. L'une des formes de ce logiciel sert à suivre les déplacements des utilisateurs sur Internet afin de mieux cibler la publicité qui leur est destinée. L'autre a une fonction analogue à celle d'une écoute téléphonique, à ceci près que la cible est l'ordinateur et non le téléphone. Le logiciel intercepte toutes les activités de l'utilisateur, y compris les mots de passe qu'il saisit et les touches qu'il presse, son courrier électronique et ses séances de *chat* ou de messagerie instantanée, les sites Web visités, et il peut également effectuer des captures d'écran.

Jargon

Installation silencieuse (*silent install*)
Installation d'un logiciel sans que son utilisateur en ait conscience.

Le premier jour où Vittaro et sa secrétaire doivent être absents tous les deux, pour plus de sécurité, il appelle Vittaro en prétextant une urgence ; la standardiste lui répond que M. Vittaro et sa secrétaire sont tous deux absents, et que leur retour n'est pas prévu avant trois jours.

La première tentative de Dillon pour inciter une salariée nouvellement arrivée à l'aider dans son projet est couronnée de succès : la secrétaire ne semble pas avoir le moindre scrupule à l'aider à télécharger le "manuscrit", qui est en réalité un logiciel espion du commerce que Dillon a modifié de telle manière que l'installation soit silencieuse. En procédant ainsi, l'installation ne serait pas détectée par un logiciel antivirus. Pour une raison mystérieuse, les fabricants d'antivirus ne commercialisent pas de produits susceptibles de détecter la présence de logiciels espions du commerce.

Dès que la jeune femme a téléchargé le logiciel sur l'ordinateur de Vittaro, Dillon est retourné sur le site de Geocities et a remplacé le fichier doc.exe par le manuscrit d'un livre qu'il avait trouvé sur Internet. Ainsi, si jamais quelqu'un avait vent de quelque chose et retournait sur le site pour savoir ce qui s'était passé, il trouverait le manuscrit innocent d'un livre mal écrit et impubliable.

Une fois le spyware installé et le système redémarré, le logiciel était automatiquement activé. Ron Vittaro, une fois de retour, se remettrait au travail,

et le logiciel espion enregistrerait le détail de toutes ses actions, y compris les courriers électroniques et des captures d'écran montrant ce qu'affichait le moniteur. De temps en temps, ces informations seraient envoyées à une adresse électronique d'un service de courrier électronique gratuit ukrainien.

Quelques jours après le retour de Vittaro, Dillon s'est mis à explorer les informations qui s'accumulaient sur son compte de courrier ukrainien, et il a bientôt trouvé les e-mails confidentiels qui indiquaient jusqu'où les éditions Millard-Fenton étaient prêtes à aller pour signer un contrat avec l'auteur. Avec ces informations à sa disposition, l'agent de l'auteur n'a eu aucune difficulté à négocier des conditions très supérieures à celles qui avaient été initialement proposées. Ce qui signifiait bien sûr que la commission de l'agent serait plus importante.

Analyse du stratagème

Ici, l'assaillant a augmenté ses chances de succès en faisant agir à sa place un salarié qui venait d'arriver dans l'entreprise. Il a spéculé sur le fait qu'un employé récent serait plus enclin à coopérer et moins bien informé sur l'entreprise, sur ses collègues et sur les procédures de sécurité qui auraient pu compromettre sa tentative.

En se faisant passer pour un chef de département lors de sa conversation avec Anna, Dillon savait que son autorité ne serait sans doute pas mise en doute. Au contraire : elle penserait peut-être que le fait d'aider un chef de département pourrait lui valoir des avantages en retour.

Les opérations qu'il a fait réaliser à Anna, et qui ont provoqué l'installation du logiciel espion, n'avaient *a priori* rien de suspect. Anna ne se doutait pas que ces quelques actions, innocentes en l'apparence, pouvaient permettre à un assaillant d'obtenir des informations importantes susceptibles d'être employées au détriment de l'entreprise.

Pourquoi a-t-il choisi une boîte aux lettres ukrainienne comme boîte de destination des messages envoyés par le logiciel espion ? Pour plusieurs raisons. D'une part, le choix d'un pays lointain rend plus difficile la détection de l'origine de l'intrusion. D'autre part, les délits qui impliquent le réseau Internet sont souvent considérés comme non prioritaires dans des pays tels que l'Ukraine, ce qui diminue la probabilité d'une coopération judiciaire avec les États-Unis.

MESURES DE PRÉVENTION

De préférence, le manipulateur choisit toujours un salarié peu susceptible de s'apercevoir que la demande du manipulateur est suspecte. La tâche de ce dernier est ainsi plus facile, mais également moins risquée, comme le montrent les récits de ce chapitre.

Le message de Mitnick

> Il est courant de demander des services à des collègues, et les manipulateurs savent comment exploiter la tendance naturelle à l'entraide. L'assaillant utilise ce côté positif de la nature humaine pour inciter des salariés à effectuer des actions qui le rapprochent de ses objectifs. Il est important de comprendre ce concept simple, afin d'être plus à même de se rendre compte des tentatives de manipulation exercées à votre encontre.

Des salariés plus prudents

Dans les chapitres précédents, j'ai insisté sur le fait qu'il fallait informer les salariés des problèmes de sécurité de telle manière qu'aucun inconnu ne parvienne à les convaincre d'exécuter ses instructions. Ils doivent également savoir qu'il peut être dangereux de réaliser quelque opération que ce soit sur l'ordinateur d'un autre. Le règlement de l'entreprise doit l'interdire, sauf quand un responsable l'autorise expressément. Parmi les situations envisageables, on peut citer :

- une demande effectuée par une personne connue du salarié, quand la demande est effectuée *de visu* ou par téléphone, à condition que la voix de l'interlocuteur puisse être identifiée de manière sûre ;
- une demande effectuée par une personne identifiée de manière formelle au moyen de procédures approuvées ;
- une action autorisée par le supérieur hiérarchique ou n'importe quelle autre autorité supérieure connaissant personnellement la personne à l'origine de la requête.

Les salariés doivent apprendre à ne pas rendre service à des personnes qu'ils ne connaissent pas personnellement, même quand elles disent faire partie des dirigeants de l'entreprise. Une fois que les règles de sécurité sont en place, l'encadrement doit encourager les salariés à s'y tenir, même si cela implique pour un salarié de s'opposer à l'un des dirigeants de l'entreprise qui lui demande d'ignorer, en sa faveur, l'une des règles de sécurité.

Chaque société doit également élaborer des règles et des procédures concernant les requêtes en matière de manipulation des ordinateurs. Dans le stratagème qui implique la société d'édition, le manipulateur a visé une nouvelle salariée qui n'avait pas été informée des règles et des procédures de sécurité. Pour éviter ce type d'attaque, tout salarié, récent ou non, doit respecter une règle simple : ne jamais effectuer sur un ordinateur une action quand c'est un inconnu qui en fait la demande, point final.

Rappelez-vous que tout salarié qui dispose d'un accès physique ou électronique à un ordinateur (ou à tout équipement informatique) est susceptible d'être manipulé à partir de l'extérieur.

Les salariés, en particulier ceux du département informatique, doivent savoir que le fait de laisser un étranger accéder au réseau informatique de l'entreprise équivaut, d'un point de vue personnel, à laisser traîner dans la rue une facturette de carte bancaire comprenant le numéro de ladite carte. La décision de communiquer des informations sensibles ou qui peuvent compromettre la sécurité du système informatique ne doit jamais être prise à la légère et sans réflexion préalable.

Le département informatique doit également se méfier de tout inconnu qui dit appeler de la part d'un éditeur de logiciels ou d'un fabricant de matériel. En général, il est préférable de choisir un ou plusieurs correspondants pour chaque éditeur ou fabricant, la règle étant qu'aucun autre salarié n'accepte de fournir des informations ou de procéder à des modifications du matériel informatique ou téléphonique. Ainsi, les correspondants désignés peuvent se familiariser avec leurs homologues chez le fabricant ou l'éditeur et risquent moins d'être abusés par un imposteur. Un appel provenant d'un éditeur ou d'un fabricant en l'absence de tout contrat d'assistance est suspect en soi.

L'ensemble des salariés de l'entreprise doivent être conscients des menaces et des vulnérabilités au niveau de la sécurité de l'information. Les agents de sécurité doivent être formés non seulement dans le domaine de la sécurité en soi, mais aussi dans celui de la sécurité de l'information. Comme les agents de sécurité disposent souvent d'un accès physique à l'ensemble des locaux de l'entreprise, ils doivent être capables d'identifier les types de manipulations qu'on est susceptible d'utiliser à leur encontre.

Attention aux logiciels espions

Les logiciels espions commerciaux étaient autrefois principalement utilisés par les parents pour surveiller l'activité de leurs enfants sur Internet, ou par les employeurs pour (soi-disant) vérifier quels employés passaient leur temps à surfer sur le Web. Une utilisation plus sérieuse consistait à identifier les sources potentielles de vol d'informations ou d'espionnage industriel. Les développeurs présentent leurs logiciels espions comme un moyen de protéger ses enfants, alors que leur vrai marché est composé de personnes qui veulent espionner d'autres personnes. De nos jours, ceux qui achètent des logiciels espions sont très souvent des personnes qui cherchent à savoir si leur époux(se) ou petit(e) ami(e) les trompe.

Peu avant que je rédige l'histoire de ce chapitre consacrée aux logiciels espions, la personne qui recevait mon courrier électronique à ma place (je n'étais pas autorisé à utiliser Internet à l'époque) a trouvé un message publicitaire vantant les mérites d'une série de logiciels espions. L'un de ces logiciels était décrit comme suit :

- **Un must !** Ce puissant logiciel de surveillance, qui fonctionne secrètement en arrière-plan, enregistre secrètement dans un fichier texte toutes les touches saisies par l'utilisateur ainsi que le titre de toutes les fenêtres Windows et l'heure de leur ouverture. Les logs peuvent être cryptés et automatiquement envoyés à l'adresse électronique de votre choix ou être simplement enregistrés sur le disque dur. L'accès au logiciel est protégé par mot de passe et il peut être masqué dans le Gestionnaire des tâches (qui s'affiche avec Ctrl+Alt+Suppr).
- Utilisez-le pour surveiller les adresses Web tapées par l'utilisateur, les sessions de chat, les courriers électroniques et plus encore (mots de passe ;-)).
- Vous pouvez l'installer discrètement sur n'importe quel ordinateur et vous faire envoyer les sessions enregistrées !

Un autre logiciel, dans le même courrier, disait pouvoir effectuer des captures d'écran de l'ordinateur cible, ce qui équivaut à disposer d'une caméra vidéo pour filmer l'écran de l'utilisateur. Certains de ces logiciels n'ont même pas besoin d'un accès physique à l'ordinateur de l'utilisateur. Ils peuvent être installés et configurés à distance, et le mouchard informatique est en place ! Des organisations comme le FBI sont sûrement ravies du développement de la technologie.

Comme les logiciels espions sont d'un accès très facile, votre entreprise doit établir deux niveaux de protection. Vous devriez installer un système de détection des logiciels espions tel que SpyCop (www.spycop.com) sur tous les postes de travail et exiger des salariés qu'ils l'utilisent à intervalles réguliers pour vérifier l'absence de ces logiciels. Par ailleurs, vous devez apprendre aux

Une défaillance des antivirus ?

Les logiciels antivirus ne détectent pas les logiciels espions commerciaux, car ils ne les considèrent pas comme hostiles alors que leur but est d'espionner les actions de l'utilisateur. De ce fait, l'équivalent informatique de l'écoute téléphonique est indétectable, et n'importe qui parmi nous pourrait être illégalement surveillé à tout moment. Bien entendu, les développeurs des logiciels antivirus peuvent prétendre que les logiciels espions sont destinés à être utilisés de manière légitime et ne doivent donc pas être considérés comme hostiles. Pourtant, certains outils dont se servait jadis la communauté des *hackers* et qui sont aujourd'hui distribués librement ou vendus en tant que logiciels de sécurité sont considérés comme hostiles par ces mêmes logiciels antivirus. Il y a donc ici deux poids, deux mesures, et je me demande pourquoi.

salariés qu'il peut être dangereux de télécharger un logiciel à la demande de quelqu'un et d'ouvrir la pièce jointe d'un e-mail.

Mesure supplémentaire pour éviter qu'un logiciel espion puisse être installé en l'absence du salarié (pause café, déjeuner ou réunion) : rendez obligatoire l'utilisation du mot de passe de l'économiseur d'écran ou d'une technique similaire. Ainsi, aucune personne non autorisée qui s'introduirait dans le bureau du salarié ne pourrait accéder à ses fichiers, lire son courrier électronique ou installer un logiciel espion ou tout autre logiciel de ce type. Cette mesure de protection n'implique aucun investissement supplémentaire, et ses bénéfices potentiels sont très importants.

Chapitre 13

Les stratagèmes sophistiqués

Vous savez maintenant que lorsqu'un inconnu appelle en demandant des informations sensibles ou tout élément qui pourrait profiter à un assaillant, la personne qui répond doit avoir appris à demander le numéro de téléphone de son interlocuteur et à le rappeler pour vérifier qu'il est bien la personne qu'il prétend : salarié de l'entreprise ou d'un partenaire commercial, ou encore membre du personnel de l'assistance technique de l'un des fournisseurs, par exemple.

Même quand une société dispose d'une procédure d'identification des appelants et que cette procédure est scrupuleusement respectée par les salariés, certains assaillants utilisent des astuces sophistiquées pour convaincre leurs victimes qu'ils sont bien qui ils prétendent être. Et même des salariés qui ont conscience des problèmes de sécurité peuvent être dupés par certains stratagèmes, que nous décrivons dans ce chapitre.

LES DANGERS DE L'IDENTIFICATION DE L'APPELANT

Aujourd'hui, tout le monde est familiarisé avec le système d'identification de l'appelant, à savoir l'affichage sur le combiné du numéro de téléphone ou du nom de la personne qui appelle. Dans l'entreprise, l'intérêt de cet affichage est qu'il permet de savoir immédiatement si un appel vient de l'intérieur ou de l'extérieur de l'entreprise.

Il y a de nombreuses années, quelques *phreakers* ambitieux ont exploité ces possibilités d'identification avant même que ce service ne soit offert au

public. Leur plus grand plaisir était de saluer par leur nom les personnes qui les appelaient avant que celles-ci aient prononcé un mot.

On pourrait penser que ce type de procédé représente un moyen sûr d'identifier son interlocuteur téléphonique. Parfois, c'est justement ce sur quoi comptent les assaillants.

L'appel de Linda

Date et heure : Mardi 23 juillet, 15 h 12.

Lieu : Les bureaux du service financier de Starbeat Aviation.

Le téléphone de Linda Hill sonne alors qu'elle est en train de rédiger un mémo pour son chef. Elle regarde l'écran du téléphone, qui indique que l'appel vient des bureaux de New York ; le nom qui s'affiche, Victor Martin, lui est inconnu.

Pendant un moment, elle est tentée de laisser la messagerie prendre le relais afin de pouvoir terminer son mémo sans être interrompue. Mais la curiosité est plus forte et elle décroche le téléphone. Son interlocuteur se présente, disant qu'il travaille aux relations publiques et qu'il prépare un dossier pour le président de la société. "Il est en route pour Boston pour un rendez-vous avec l'un de nos banquiers et il a besoin des principaux résultats financiers pour le trimestre en cours. Autre chose : il a aussi besoin des projections financières pour le projet Apache", dit Victor en utilisant le nom de code d'un produit qui, au printemps prochain, serait l'une des principales mises sur le marché de la société.

Elle lui demande son adresse électronique, mais il dit avoir des problèmes pour recevoir son courrier en ce moment ; ne lui serait-il pas possible d'envoyer un fax ? Elle répond que cela ne pose pas de problème et lui donne l'extension interne de son fax.

Elle envoie le fax quelques minutes plus tard.

Mais Victor ne travaille pas pour les relations publiques de l'entreprise. En fait, il ne travaille pas du tout pour l'entreprise.

Le point de vue de Jack

Jack Dawkins a commencé très jeune sa carrière professionnelle de pickpocket au cours des matches au Yankee Stadium, sur les quais bondés du métro et dans la foule des touristes noctambules de Times Square. Il était si doué qu'il parvenait à ôter la montre du poignet d'un homme sans que celui-ci ne s'en aperçoive. Mais au cours de son adolescence, il était devenu malade et s'était fait prendre. Dans le centre de détention pour mineurs, il avait appris un nouveau métier où les risques de se faire prendre étaient bien moindres.

La dernière mission qu'il avait acceptée consistait à obtenir les résultats et les données comptables trimestriels d'une entreprise avant que ces données soient transmises à la SEC (*Securities and Exchange Commission*), la commission des opérations de bourse américaine, et qu'elles soient rendues publiques. Son client était un dentiste qui ne voulait pas dire pourquoi il avait besoin de ces informations. Jack trouvait cette prudence déplacée, il en avait vu bien d'autres ! Le dentiste avait sans doute un problème de dettes, ou peut-être une maîtresse aux goûts de luxe. Ou peut-être s'était-il vanté auprès de sa femme de ses talents de boursicoteur, et il avait perdu une forte somme qu'il espérait regagner en misant à coup sûr. Pour cela, il avait besoin de savoir dans quel sens évolueraient les cours de l'action d'une entreprise lorsque celle-ci annoncerait ses résultats trimestriels.

On sera surpris de voir le peu de temps qu'il faut à un manipulateur pour trouver une solution à un problème auquel il n'a jamais été confronté. Lorsque Jack est rentré chez lui après son entretien avec le dentiste, il avait déjà conçu un plan. Son ami Charles Bates travaillait pour une société, Panda Importing, qui disposait de son propre central téléphonique.

En termes techniques, ce central téléphonique, ou PABX (*Private Automatic Branch eXchange*), était de type RNIS (ISDN en anglais). Ce type de PABX permet de spécifier, pour chaque poste raccordé, le numéro de téléphone du poste appelant. Ce numéro, ainsi que d'autres informations, est transmis *via* le canal de données RNIS (le canal D) au central téléphonique de l'opérateur téléphonique, puis au téléphone du destinataire.

Charles Bates était toujours prêt à aider son ami Jack Dawkins, moyennant rétribution, et il savait comment reprogrammer le PABX de son entreprise pour que les appels émis à partir d'un poste particulier de Panda Importing semblent, sur l'écran du téléphone appelé, provenir du numéro interne de Victor Martin, de Starbeat Aviation.

Peu de gens savent qu'il est possible de faire apparaître n'importe quel numéro sur un poste équipé pour identifier les appelants ; de ce fait, Linda n'a eu aucun scrupule à faxer les informations demandées par la personne qu'elle croyait être un collègue travaillant aux relations publiques.

Après que Jack a raccroché, Charles Bates a reprogrammé le PABX de sa société de manière à rétablir le "vrai" numéro de poste.

Analyse du stratagème

Certaines entreprises ne souhaitent pas que leurs clients ou leurs fournisseurs voient s'afficher les numéros de téléphone de leurs salariés. Ainsi, Ford pourra faire en sorte que les appels en provenance de son service d'assistance affichent le numéro vert du centre d'assistance, et non le numéro de poste du téléopérateur qui effectue l'appel. De cette manière, l'entreprise protège la confidentialité de ses numéros internes.

Mais cette possibilité de reprogrammation du numéro d'identification de l'appelant peut être exploitée par des plaisantins ou, bien sûr, par des individus malveillants.

VARIANTE : UN APPEL DU PRÉSIDENT DES ÉTATS-UNIS

En tant que co-animateur d'une émission de radio nommée *Darkside of the Internet* (le côté obscur d'Internet) sur KFI à Los Angeles, je travaillais sous les ordres du directeur de programmes de la station, David. Je connais peu de personnes travaillant aussi dur que David, et il est toujours impossible à joindre au téléphone du fait de ses plannings surchargés. Il fait partie de ces personnes qui ne répondent pas aux appels, sauf si l'identification de l'appelant lui indique qu'il s'agit de quelqu'un à qui il doit parler.

Lorsque je l'appelais de mon téléphone fixe (je n'avais pas le droit d'utiliser mon téléphone portable), mon numéro ne s'affichait pas sur son téléphone[1]. Je devais alors laisser un message sur sa boîte vocale, ce qui était toujours frustrant.

J'ai discuté de la situation avec un vieil ami qui avait créé une société spécialisée dans la location de bureaux pour entreprises de haute technologie, et nous avons élaboré un plan. Il avait accès au PABX de sa société et il pouvait donc programmer le numéro qui devait s'afficher sur le poste de la personne appelée. À chaque fois que j'avais besoin d'appeler le directeur de programmes et que je tombais sur sa messagerie, je demandais à mon ami de programmer le numéro que je voulais faire apparaître sur l'écran du téléphone de David. Parfois, l'appel semblait provenir de l'assistant de David, d'autres fois, de la société propriétaire de la station de radio.

Mais ce que je préférais, c'était lui faire croire que l'appel venait de son propre domicile, parce que j'étais sûr qu'il décrocherait. Je dois dire, au crédit de David, qu'il prenait toujours avec humour le fait que je le dupe une fois de plus avec cette technique. Et surtout, il restait en ligne assez longtemps pour s'intéresser au problème que je lui soumettais et le résoudre.

1. N.D.T. : L'identification des interlocuteurs téléphoniques est peu répandue aux États-Unis pour les téléphones fixes de particuliers.

Au cours d'une autre émission de radio, j'ai fait la démonstration de cette technique en faisant s'afficher le numéro de téléphone du FBI de Los Angeles sur le poste de mon correspondant. Cela a choqué l'animateur de l'émission, Art Bell, qui m'a reproché d'avoir commis un acte illégal. Je lui ai fait remarquer qu'en réalité, ce que j'avais fait n'avait rien d'illégal tant qu'aucune tentative d'escroquerie ou de tromperie n'y était associée. Après cette émission, j'ai reçu plusieurs centaines d'e-mails dont les expéditeurs me demandaient comment j'avais fait. Maintenant, vous le savez aussi.

C'est là l'outil parfait pour le manipulateur qui cherche à se prévaloir d'une fausse identité. Si, lors de la phase de recherches préliminaires, le manipulateur apprend que la victime utilise ce procédé d'identification, il peut se faire passer pour un salarié de l'entreprise en faisant apparaître le numéro de ce dernier.

Les possibilités du manipulateur sont alors multiples. Un pirate informatique pourra téléphoner à votre domicile en prétendant faire partie du service informatique de l'entreprise, et dire qu'il a besoin d'urgence de votre mot de passe pour restaurer vos fichiers à la suite d'un crash du serveur. Ou le numéro affiché pourra être celui de votre banque, et une jeune femme à la voix agréable aura uniquement besoin de vérifier vos numéros de compte et le nom de jeune fille de votre mère. Pour faire bonne figure, elle vous demandera également le numéro, voire le code de votre carte bancaire, en raison d'un problème quelconque du système. Des propositions d'investissement douteuses seront beaucoup plus convaincantes si l'appel semble provenir d'une banque établie. Une personne qui en veut à une entreprise pour une raison quelconque pourra appeler en se faisant passer pour un représentant du fisc ou du FBI.

Si vous avez accès à un PABX et quelques connaissances en programmation — que vous pouvez généralement acquérir à partir du site du fournisseur du matériel du site d'un fournisseur de matériel —, vous pouvez vous servir de cette technique pour jouer des tours à vos amis. Si l'une de vos relations a de grandes ambitions politiques, par exemple, vous pouvez faire en sorte que votre appel semble provenir du 202 456 1414, et votre correspondant verra s'afficher "WHITE HOUSE" sur l'écran de son téléphone !

La morale de cette histoire est simple : on ne peut se fier à l'identification de l'appelant, sauf pour des appels internes aux locaux de l'entreprise. Au domicile comme sur son lieu de travail, tout le monde doit être conscient du

fait que l'identification de l'appelant peut être falsifiée, et qu'elle ne peut être employée pour une identification formelle[1].

LA SALARIÉE INVISIBLE

Shirley Cutlass a trouvé un nouveau moyen de gagner rapidement beaucoup d'argent. Finies les journées de travail harassantes : elle fait maintenant partie du club sans cesse grandissant de ceux qui s'adonnent au crime de la décennie, l'usurpation d'identité.

Aujourd'hui, elle a décidé d'extorquer des informations confidentielles au service des relations clientèle d'une société de cartes de crédit. Après les démarches préliminaires habituelles, elle appelle la société qu'elle vise et indique à la standardiste qu'elle souhaite être mise en communication avec le service des télécoms. Aux télécoms, elle demande l'administrateur des boîtes vocales.

Utilisant des informations qu'elle s'est procurées lors de ses recherches préliminaires, elle indique qu'elle se nomme Norma Todd, et qu'elle appelle des bureaux de Cleveland. Elle recourt à une ruse qui doit maintenant vous être familière : elle dit qu'elle doit être présente au siège social de l'entreprise pendant une semaine et qu'elle a besoin d'y disposer d'une boîte vocale afin d'éviter les appels à travers les États-Unis pour consulter sa messagerie. Elle n'a pas besoin d'une ligne téléphonique, dit-elle, juste d'une boîte vocale. Son interlocuteur répond qu'il s'en occupe et qu'il la rappelle dans une heure pour lui fournir les informations nécessaires.

Prenant sa voix la plus séduisante, elle demande : "J'ai une réunion qui commence, je peux vous rappeler dans une heure ?"

Quand elle rappelle, la boîte vocale est en place ; il lui donne son numéro d'extension et son mot de passe provisoire. Il lui demande ensuite si elle sait modifier ce mot de passe, et elle accepte de se laisser expliquer la procédure, bien qu'elle la connaisse sans doute au moins aussi bien que lui.

"Au fait, dit-elle, quel numéro dois-je appeler pour accéder à mes messages à partir de mon hôtel ?" Il lui fournit le numéro.

1. N.D.T. : Ce qui est vrai pour les États-Unis l'est dans une large mesure pour la France et la plupart des autres pays. En France, le réseau Numéris (RNIS) transmet deux numéros au destinataire : le NDS (numéro programmé par l'utilisateur) et le NDI (numéro de l'installation, généré par l'opérateur). Selon la programmation du central téléphonique de l'entreprise qui reçoit l'appel, c'est l'un ou l'autre numéro (ou aucun) qui s'affiche sur le poste du correspondant. Dans le cas d'une ligne analogique (non RNIS), le numéro généralement affiché est le NDS. Même le NDI n'offre pas une sécurité absolue, mais il est difficile à falsifier. Une bonne programmation du central téléphonique de l'entreprise est donc cruciale. Par ailleurs, quelle que soit la technique utilisée par l'assaillant, il est toujours possible de remonter jusqu'à lui, ce qui représente un risque non négligeable pour lui, si la malveillance est découverte.

Shirley appelle ce numéro, modifie le mot de passe, puis enregistre le message d'accueil de la boîte vocale.

L'attaque de Shirley

La mise en place était facile. Shirley est maintenant prête à mettre en œuvre son art de la supercherie.

Elle appelle le service des relations avec la clientèle de la société. "Je suis du service des encaissements, à Cleveland", dit-elle avant de se lancer dans une variante du prétexte habituel. "Le support technique est en train de réparer mon ordinateur, et j'ai besoin de votre aide concernant certaines informations sur un client." Elle donne le nom et la date de naissance de la personne dont elle veut usurper l'identité, puis indique les informations dont elle a besoin sur cette personne : adresse, nom de jeune fille de la mère, numéro de carte de crédit, limite de crédit, crédit disponible et historique des paiements. "Rappelez-moi à ce numéro", dit-elle en mentionnant le numéro d'extension interne que l'administrateur des boîtes vocales lui a fourni. "Et si je suis absente, laissez les informations sur ma boîte vocale."

Elle s'occupe à droite et à gauche pendant le reste de la matinée, puis, dans l'après-midi, vérifie le contenu de sa boîte vocale. Toutes les informations qu'elle a demandées s'y trouvent. Avant de raccrocher, Shirley efface le message d'accueil : elle sait qu'il serait imprudent de laisser subsister des traces de sa voix enregistrée.

Et l'usurpation d'identité, le délit qui connaît aux États-Unis la croissance la plus rapide, va faire une nouvelle victime. Avec les informations qu'elle vient de récolter sur l'identité et la carte de crédit de sa victime, Shirley peut commencer à faire des dépenses sur le compte de quelqu'un d'autre.

Analyse du stratagème

Ici, l'assaillante a d'abord trompé l'administrateur des boîtes vocales de la société en lui faisant croire qu'elle était l'une de ses collègues afin d'obtenir une boîte vocale provisoire. Et à supposer qu'il se soit avisé de vérifier, il aurait constaté que le nom et le numéro de téléphone fournis par Shirley correspondaient à une salariée réelle de l'entreprise.

Il suffit ensuite à Shirley de fournir une excuse raisonnable concernant un problème d'informatique et de demander à ce que les informations requises soient laissées sur sa boîte vocale. Pourquoi un salarié refuserait-il de fournir ces informations à une collègue ? Après tout, le numéro fourni par Shirley

était celui d'un poste interne ; il n'y avait donc aucune raison d'être suspicieux.

Le message de Mitnick

Appelez de temps à autre votre propre boîte vocale ; si le message d'accueil n'est pas le vôtre, vous avez été victime d'un manipulateur.

LA SECRÉTAIRE OBLIGEANTE

Le pirate informatique Robert Jorday avait fréquemment fait des intrusions dans le réseau d'une entreprise internationale, Rudolfo Shipping. Celle-ci a fini par prendre conscience du fait que quelqu'un s'infiltrait dans un serveur terminal, et à partir de ce serveur dans tous les autres serveurs de l'entreprise. Pour protéger la société, l'entreprise a décidé d'imposer l'utilisation d'un mot de passe pour toutes les connexions à distance avec les serveurs terminaux.

Robert appelle le centre de gestion du réseau, se fait passer pour un avocat du service juridique et dit qu'il ne parvient pas à se connecter au réseau. Son interlocuteur, un administrateur réseau, lui explique qu'ils ont connu récemment quelques problèmes de sécurité, et que tous les utilisateurs qui se connectent à distance doivent demander à leur chef de service un mot de passe valable pour un mois. Robert demande quelle méthode est employée pour communiquer le mot de passe au chef de département, et comment il doit faire pour l'obtenir. La réponse est que le mot de passe pour le mois à venir est envoyé dans un mémo interne à chaque chef de service.

À partir de là, les choses étaient simples. Robert fait quelques recherches, appelle la société en début de mois et parvient à contacter la secrétaire de l'un des chefs de service, une dénommée Janet. "Bonjour Janet, dit-il. Ici Randy Goldstein, du service de recherche et développement. Je sais que j'ai reçu le mémo pour le mot de passe qui me permet de me connecter à distance au serveur terminal, mais je ne le trouve plus. Est-ce que vous avez reçu votre mémo pour ce mois-ci ?"

Elle l'a en effet reçu.

Il lui demande si elle peut le lui faxer, et elle accepte. Il lui donne le numéro de fax du réceptionniste du hall d'entrée d'un autre bâtiment de l'entreprise, où il s'est arrangé pour qu'on mette de côté les fax qui lui sont destinés ; il aurait donc pu demander à ce que le mot de passe lui soit transmis après réception. Cette fois-là, cependant, il utilise une autre

méthode de transmission : il donne au réceptionniste un numéro auquel renvoyer le fax, et qui correspond à un service de fax virtuel auquel il a souscrit. Les fax adressés à ce numéro sont envoyés en tant qu'e-mails à l'adresse électronique de l'abonné.

Le nouveau mot de passe arrive dans la boîte aux lettres que Robert a établie auprès d'un service de courrier électronique gratuit en Chine. Ainsi, toute tentative de remonter jusqu'à lui serait compromise, les autorités chinoises étant notoirement peu enclines à porter assistance à des enquêteurs américains pour ce type d'affaire. Et Robert n'a même pas eu à se présenter en personne à l'endroit où se trouve le fax.

Le message de Mitnick

Un manipulateur expérimenté sait comment influencer les gens pour qu'ils lui rendent de petits services. Le fait de recevoir un fax et de le transmettre semble si anodin qu'il n'est pas difficile de faire en sorte qu'un réceptionniste ou une autre personne accepte une requête de ce type. Apprenez à refuser tout service impliquant des informations, dès lors que le demandeur ne peut pas être formellement identifié.

COMMENT ÉCHAPPER AUX CONTRAVENTIONS

Toute personne qui a reçu une contravention pour excès de vitesse a sans doute rêvé de trouver un moyen d'échapper à la sanction. Il n'est pas question de réaliser des travaux d'intérêt collectif, de payer l'amende ni de compter sur un détail technique tel que la non-conformité du radar, mais plutôt de se montrer plus malin que le système.

Le stratagème

Je ne recommanderais pas d'utiliser cette méthode pour échapper à une contravention, néanmoins cet exemple illustre bien la manière dont l'art de la supercherie peut être exercé par un manipulateur.

Un automobiliste, que nous appellerons Paul Durea, s'est fait verbaliser pour excès de vitesse.

Première étape

Police de Los Angeles, Division Hollenbeck.

"Bonjour, je voudrais parler au policier qui s'occupe des convocations."

"C'est moi."

"Parfait. Je suis John Leland, du cabinet d'avocats Meecham, Meecham et Talbot. Je voudrais faire convoquer un policier pour une affaire."

"Oui, quel policier ?"

"Est-ce que l'officier Kendall travaille chez vous ?"

"Quel est son numéro de matricule ?"

"21349."

"Oui. Quand avez-vous besoin de lui ?"

"Au cours du prochain mois, mais je dois faire convoquer plusieurs autres témoins dans cette affaire et informer ensuite le juge des dates qui nous conviennent. Y a-t-il des jours au cours du prochain mois où l'officier Kendall ne sera pas disponible ?"

"Voyons... Il a des congés du 20 au 23, et il est en formation le 8 et le 9."

"D'accord. C'est tout ce que j'ai besoin de savoir pour le moment. Je vous rappellerai quand la date de l'audience aura été fixée."

Tribunal municipal, bureau du greffier

Paul : "Je souhaite que soit établi un acte d'accusation pour cette contravention."

Greffier : "Vous voulez un acte d'accusation ?"

"Oui."

Bon. "L'acte d'accusation peut être établi demain matin ou demain après-midi. Qu'est-ce que vous préférez ?"

"Demain après-midi."

"Présentez vous demain à 13 h 30 à la salle d'audience numéro six."

"Merci. J'y serai."

Tribunal municipal, salle six

Date : Jeudi, 13 h 45

Juge : "Monsieur Durea, vous connaissez vos droits en la matière ?"

Paul : "Oui, monsieur le président."

"J'ai vérifié dans votre dossier. Vous avez la possibilité de commuer votre contravention en stage de sensibilisation. Dans ce cas, votre contravention sera annulée après huit heures de stage."

"Non, monsieur le président. Je demande à être jugé. Et il y a autre chose, monsieur le président. Je serai en voyage d'affaires en Europe ces prochaines semaines, mais je serai présent le 8 et le 9. Mon cas peut-il être jugé l'un de ces deux jours ?"

"Très bien. Vous serez jugé le 8 juin à 8 h 30, en salle quatre."

"Merci, monsieur le président."

Tribunal municipal, salle quatre

Paul arrive tôt à la salle d'audience le 8 au matin. Lorsque le juge entre, le greffier lui remet une liste des affaires pour lesquelles les officiers de police ne se sont pas présentés. Le juge appelle les accusés à la barre, Paul y compris, et leur fait savoir qu'ils sont relaxés.

Analyse du stratagème

Lorsqu'un agent établit une contravention, il indique son nom et son numéro de matricule. On peut alors facilement savoir à quel commissariat il appartient. Une fois le commissariat identifié, il n'est pas difficile non plus de trouver le policier responsable des convocations pour la zone géographique concernée.

Aux États-Unis, il est courant de convoquer les policiers au tribunal. Quand un représentant du ministère Public ou de la défense a besoin de faire témoigner un policier, il vérifie au préalable que le policier sera disponible le jour de l'audience. Il lui suffit pour cela d'appeler le policier responsable des convocations.

Habituellement, l'avocat demande si le policier en question est disponible tel ou tel jour. Paul a dû, quant à lui, imaginer un stratagème pour obtenir l'information inverse, à savoir les jours d'absence du policier.

Lors de sa première visite au tribunal, pourquoi Paul n'a-t-il pas simplement demandé au greffier la date qu'il voulait pour le jugement ? Parce qu'en général, les accusés ne peuvent pas la choisir librement. Si la première date proposée par le greffier ne convient pas, il en propose une, voire deux autres, mais pas plus.

En demandant l'établissement d'un acte d'accusation[1], Paul passait devant le juge, et il savait qu'il aurait ainsi plus de chances d'obtenir la date de jugement de son choix. Il a donc demandé des dates correspondant aux jours où le policier était en formation, sachant que pour l'État, la formation des policiers est prioritaire sur leur présence au tribunal municipal. Et en l'absence de policier au cours du procès, Paul était automatiquement relaxé[2].

Le message de Mitnick

L'esprit humain est quelque chose de merveilleux. Il est fascinant d'observer à quel point certaines personnes se montrent inventives pour obtenir ce qu'elles veulent ou se tirer d'embarras. Et il faut faire montre de cette même créativité et de cette même inventivité pour protéger les informations et les systèmes informatiques, que l'on se trouve dans le secteur privé ou public. En conclusion : quand vous mettez en place des règles de sécurité, soyez créatif et n'hésitez pas à utiliser des méthodes peu orthodoxes.

LA VENGEANCE DE SAMANTHA

Samantha Gregson était furieuse.

Elle avait travaillé dur pour obtenir le diplôme de son école de commerce et elle avait dû s'endetter lourdement pour payer ses études. On lui avait toujours répété que le diplôme était ce qui faisait la différence entre un petit boulot et une carrière, et que c'était le moyen de gagner beaucoup d'argent. Et une fois diplômée, elle n'avait réussi à trouver aucun emploi convenable.

Finalement, elle avait été contente de recevoir l'offre de Lambeck Manufacturing. Bien sûr, il était humiliant d'accepter un poste de secrétaire, mais M. Cartright lui avait dit combien ils tenaient à la recruter, et que sa situation de secrétaire serait un bon tremplin dès lors qu'un poste non administratif se libérerait.

1. N.D.T. : Une procédure spécifique aux États-Unis.
2. N.D.T. : Ce stratagème ne peut fonctionner qu'aux États-Unis et au Canada. En France, c'est le procès-verbal de contravention qui fait foi, et le policier n'a pas besoin de se rendre au procès.

Deux mois plus tard, elle apprend que l'un des chefs de produits junior de Cartright quitte l'entreprise. Elle peut à peine dormir cette nuit-là, s'imaginant déjà au quatrième étage, dans un bureau avec une porte, assistant à des réunions et prenant des décisions.

Le lendemain matin, elle va voir M. Cartright. Il dit qu'elle devrait se familiariser encore un peu avec les activités de l'entreprise avant de pouvoir prétendre à un poste de ce type. Puis ils recrutent un jeunot qui en sait beaucoup moins qu'elle sur les activités de l'entreprise.

C'est à ce moment qu'elle commence à prendre conscience du fait que l'entreprise emploie beaucoup de femmes, mais que presque toutes sont secrétaires, et que tant qu'elle travaillera pour eux, elle ne se verra jamais confier aucune responsabilité.

La monnaie de la pièce

Il lui a fallu presque une semaine pour mettre au point sa vengeance. Un mois plus tôt, un journaliste d'un magazine spécialisé l'avait baratinée lorsqu'il était venu pour le lancement d'un nouveau produit. Quelques semaines plus tard, il l'avait appelée au travail et lui avait promis un bouquet de fleurs en échange de quelques informations concernant le prochain produit de la société, le Cobra 273. Pour des informations plus confidentielles qu'il pourrait utiliser dans son magazine, il était même prêt à faire un saut à Chicago et à l'inviter à dîner.

Peu après cet appel, elle s'était rendue dans le bureau du jeune Johannson au moment où il se connectait au réseau de l'entreprise. Sans réfléchir, elle avait observé ses doigts taper le mot de passe, qui était "marty63".

Son plan prenait forme. Elle se souvenait avoir tapé un mémo peu après avoir été embauchée. Elle en retrouve une copie et en tape une nouvelle version en utilisant les mêmes tournures que dans l'original. Voici ce qu'elle tape :

> À : C. Pania, service informatique
> DE : L. Cartright, développement produits
> Martin Johannson travaillera auprès de l'équipe des projets spéciaux dans mon service.
> Je l'autorise par la présente à accéder aux serveurs utilisés par l'équipe de développement. Veuillez lui attribuer les mêmes droits d'accès qu'un développeur produit.
>
> Louis Cartright

À l'heure du déjeuner, lorsque les bureaux sont presque vides, elle découpe la signature de Cartright dans l'original du mémo, la colle sur la nouvelle

version et met du correcteur autour des bords. Elle fait une photocopie du résultat, puis une copie de la copie. Les contours sont à peine visibles.

Elle envoie le fax depuis la machine située à proximité du bureau de monsieur Cartright.

Trois jours plus tard, elle se trouve assez de travail pour rester dans l'entreprise alors que tout le monde est parti. Elle entre dans le bureau de Johannson et se connecte au réseau avec son nom d'utilisateur et son mot de passe, marty63.

Quelques minutes plus tard, elle a trouvé les spécifications du produit Cobra 273 et les a copiées sur une disquette Zip.

La disquette se trouve dans son sac à main tandis qu'elle traverse le parking dans l'air frais de la nuit. Elle va la transmettre au journaliste le soir même.

Analyse du stratagème

Une salariée mécontente, une recherche à travers des dossiers, un petit mémo, un couper-coller et un fax. C'est tout ce qu'il a fallu pour accéder à des informations confidentielles.

Et quelques jours plus tard, un magazine spécialisé publiait un scoop : toutes les spécifications et les plans marketing d'un nouveau produit qui ne devait être commercialisé que plusieurs mois plus tard. Le magazine serait lu avec beaucoup d'intérêt par ses abonnés, tous des professionnels qui disposaient ainsi de plusieurs mois pour développer des produits concurrents et pour mettre en place des campagnes publicitaires dénigrant le Cobra 273.

Bien entendu, le magazine ne révèlerait jamais la source de ses informations.

MESURES DE PRÉVENTION

Les salariés d'une entreprise doivent être conscients du fait que l'identification de l'appelant n'est pas une méthode d'identification sûre et que, par conséquent, ils ne doivent pas s'y fier pour transmettre à un tiers des informations sensibles. Il faut employer un autre moyen : vérifier auprès du supérieur hiérarchique de la personne que la demande est justifiée et que la personne est autorisée à obtenir cette information, par exemple.

Pour établir ses processus de vérification, chaque entreprise doit trouver elle-même un compromis entre sécurité et productivité. Quelle priorité faut-il accorder au maintien des mesures de sécurité ? Les salariés risquent-ils de rechigner à mettre en œuvre les procédures de sécurité, voire de les ignorer entièrement pour mieux accomplir leurs tâches ? Il faut répondre à ces questions avant de mettre en place des règles de sécurité basées sur la culture et les besoins de l'entreprise.

La plupart des gens perçoivent comme une gêne tout ce qui peut entraver l'exécution de leurs tâches et sont susceptibles d'ignorer toute mesure de sécurité qu'ils considèrent comme une perte de temps. Motiver les salariés à travers la formation et l'information est essentiel pour qu'ils considèrent la sécurité comme une de leurs responsabilités quotidiennes.

On peut noter que plusieurs fabricants de modems ont doté leurs produits d'une fonction d'identification de l'appelant. Cela permet de protéger le réseau de l'entreprise en interdisant les connexions à distance à tout numéro qui ne fait pas partie des numéros autorisés. Dans un environnement où les risques de sécurité sont faibles, cette méthode d'identification est acceptable. Mais, comme nous l'avons vu, il n'est pas très difficile de falsifier l'identification de l'appelant, et cette méthode n'est donc pas fiable dans un environnement où les risques de sécurité sont élevés.

Pour éviter les usurpations d'identité, comme dans l'histoire où l'administrateur crée une boîte vocale sur le système téléphonique de l'entreprise, établissez la règle suivante : les créations de lignes téléphoniques, de boîtes vocales et d'entrées dans l'annuaire de l'entreprise, qu'il soit imprimé ou en ligne, doivent être demandées par écrit au moyen d'un formulaire spécifique. Le supérieur hiérarchique du demandeur doit approuver la demande et l'administrateur des boîtes vocales doit vérifier la signature.

La création de comptes d'utilisateur et l'extension des droits d'un utilisateur ne doivent être autorisées qu'après une identification formelle du demandeur, qui peut se faire au moyen d'un appel téléphonique auprès du gestionnaire ou de l'administrateur système ou de son représentant. C'est le numéro indiqué dans l'annuaire de l'entreprise qui doit être appelé. Si l'entreprise utilise le courrier électronique sécurisé, qui permet aux salariés de signer leurs messages numériquement, cette méthode peut également être employée.

Rappelez-vous que n'importe quel salarié, qu'il ait accès ou non aux ordinateurs de l'entreprise, peut être dupé par un manipulateur. Les formations aux problèmes de sécurité doivent donc être dispensées à tous. Assistants administratifs, réceptionnistes, standardistes et agents de sécurité doivent être sensibilisés aux types de manipulations les plus couramment employés afin d'être plus susceptibles d'y parer.

Chapitre 14

L'espionnage industriel

La menace que représentent les attaques contre les institutions publiques, les entreprises et les universités n'est pas une fiction. Presque chaque jour, les médias annoncent l'arrivée d'un nouveau virus, une attaque visant à déstabiliser Internet ou un vol d'informations de carte bancaire à partir d'un site de commerce électronique.

On apprend ainsi que Borland accuse Symantec de s'être livré à de l'espionnage industriel à ses dépens ou que Cadence Design Systems poursuit un concurrent en justice pour vol de code source. Nombreux sont ceux qui s'imaginent que leur propre entreprise ne pourrait pas être victime de ce type d'attaque. Pourtant, de nouveaux cas sont recensés chaque jour.

VARIATIONS SUR UN MÊME THÈME

La ruse décrite dans l'histoire qui suit a sans doute été utilisée très souvent avec succès, même si elle donne l'impression de sortir d'un roman de John Grisham ou d'un film hollywoodien tel que *Révélations*.

Action en justice

Supposons qu'un procès majeur soit en cours contre un laboratoire pharmaceutique, Pharmomedic. D'après l'accusation, les dirigeants de cette entreprise savaient que l'un de leurs médicaments les plus vendus avait des effets secondaires mais qui n'apparaissaient qu'après plusieurs années de traitement. Et ces dirigeants, bien que disposant de plusieurs études qui montrent les risques que présente le médicament, n'auraient jamais informé les autorités comme ils étaient tenus de le faire.

William Chaney, l'avocat du cabinet new-yorkais qui représente les parties civiles dans cette affaire, dispose des témoignages de deux médecins ayant travaillé pour Pharmomedic qui confirment ces accusations. Mais les deux médecins sont retraités et aucun des deux ne possède de document qui appuie ses dires ; de plus, leur personnalité n'en fait pas des témoins très convaincants. Chaney sait que sa position était délicate : à moins d'obtenir une copie de l'une de ces études, ou un mémo ou une autre communication interne concernant l'affaire, il n'aura aucune chance lors du procès.

Il fait donc appel à une société dont les services lui ont déjà été utiles : Andreeson and Sons, agence d'investigation. Chaney ne sait pas comment Pete Andreeson et ses hommes obtiennent leurs informations, et il ne veut pas le savoir. Il sait seulement que Pete Andreeson est un bon détective.

Pour Andreeson, dans ce type de mission, la première règle est que les cabinets d'avocats et les entreprises qui le recrutent ne doivent jamais savoir comment il obtient les informations, afin qu'ils ne puissent pas être incriminés par la suite. C'était lui, Andreeson, qui se trouvait en première ligne, mais vu les montants qu'il demandait pour ce type de mission délicate, il considérait que le risque en valait la chandelle. Et puis il éprouvait une satisfaction personnelle à se montrer plus malin que ses adversaires.

Si les documents que recherche Chaney existent et qu'ils n'aient pas été détruits, ils doivent se trouver quelque part dans les fichiers de Pharmomedic. Mais ce serait une tâche titanesque que de les rechercher parmi les dizaines de millions de fichiers d'une grande multinationale. D'un autre côté, il n'était pas impossible qu'ils aient transmis des copies de ces fichiers à leur cabinet d'avocats, Jenkins and Petry. Si les avocats de l'entreprise connaissaient l'existence de ces documents et qu'ils aient omis de les transmettre aux autorités au cours de l'enquête, ils auraient agi à l'encontre des règles de leur profession et commis un acte illégal. Ce qui, pour Andreeson, justifiait les méthodes qu'il allait utiliser à leur encontre.

L'attaque d'Andreeson

Andreeson met ses hommes au travail et, quelques jours plus tard, il sait à quelle société Jenkins and Petry confie le stockage de ses sauvegardes hors site. Il sait aussi que cette société de stockage dispose d'une liste de noms correspondant aux personnes qui sont autorisées par le cabinet d'avocats à retirer les bandes de sauvegarde auprès de la société de stockage. Il sait enfin qu'à chacun de ces noms correspond un mot de passe. Il envoie deux de ses hommes effectuer une petite incursion.

La nuit suivante, à 3 heures du matin, les hommes d'Andreeson entrent dans les bureaux de la société de stockage après avoir fracturé la serrure à l'aide d'un outil de crochetage, le pistolet américain commandé sur le Web à l'adresse www.southord.com. Ils mettent en route un ordinateur et sourient en voyant apparaître le logo de Windows 98 : cette version de Windows ne nécessite aucune authentification, leur tâche sera aisée. Après quelques recherches, ils trouvent une base de données Access contenant la liste des personnes autorisées par chacun des clients de la société à retirer des bandes de sauvegarde. Ils ajoutent un faux nom à la liste du cabinet Jenkins and Petry, un nom correspondant à un permis de conduire que l'un des hommes d'Andreeson a en sa possession. Bien entendu, ils auraient pu forcer la porte menant à la zone de stockage des bandes et essayer de trouver de cette manière les bandes demandées par leur client. Mais dans ce cas, tous les clients de la société de stockage auraient été avertis de l'incident, et les assaillants auraient perdu un avantage : les professionnels préfèrent toujours garder la possibilité de revenir à la charge si nécessaire.

Les intrus réalisent également une copie du fichier contenant la liste des autorisations, suivant en cela une pratique courante des espions industriels. Cette liste ne leur est d'aucune utilité pour le moment, mais on ne sait jamais à quoi elle pourrait servir à l'avenir, et cela ne coûte rien d'effectuer la copie.

Le lendemain, l'un des deux hommes appelle la société de stockage et utilise le nom et le mot de passe qu'ils ont ajoutés à la liste. Il demande les bandes du cabinet Jenkins and Petry datant du mois précédent et dit qu'un coursier passera les prendre. En milieu d'après-midi, Andreeson a les bandes à sa disposition. Ses hommes ont pu restaurer les données sur leur propre système informatique et se lancer dans leurs recherches en toute tranquillité. Andreeson constate avec satisfaction que le cabinet d'avocats ne crypte pas ses données sauvegardées, se montrant dans ce domaine aussi imprudent que la plupart des autres entreprises.

Les bandes sont restituées à la société de stockage le lendemain, sans que personne ne soupçonne quoi que ce soit.

Le message de Mitnick

Les informations importantes doivent être protégées, quel que soit leur support ou leur emplacement. La liste des clients d'une entreprise a la même valeur, qu'elle soit imprimée sur papier ou qu'elle ait la forme d'un fichier stocké dans vos bureaux ou dans une entreprise extérieure. Les manipulateurs choisissent toujours le point d'entrée le plus vulnérable, et la société de stockage d'une entreprise est souvent considérée comme

telle, mais elle présente l'avantage supplémentaire que le risque de s'y faire repérer est moindre. Toute entreprise qui stocke des données sensibles auprès de sociétés tierces doit crypter ses données pour les protéger.

Analyse du stratagème

L'intrusion dans les locaux de la société de stockage n'a pas posé de problème du fait de la faiblesse des mesures de sécurité, pas plus que l'accès à l'ordinateur ni la modification de la liste des personnes autorisées à retirer les bandes de sauvegarde. Ensuite, l'assaillant a pu obtenir les bandes de sauvegardes simplement en les demandant ; le contenu de ces bandes n'a pas posé de problème non plus parce que le cabinet d'avocats ne se donnait pas la peine de crypter les données.

Cet incident montre comment un sous-traitant qui ne prend pas de mesures de précautions suffisantes peut compromettre la sécurité des informations de ses clients.

LE NOUVEAU PARTENAIRE COMMERCIAL

Les manipulateurs ont un avantage par rapport aux escrocs : il n'ont pas besoin de se trouver face à leur victime. Les escrocs, quant à eux, se retrouvent tôt ou tard en présence de leur cible, ce qui permet à cette dernière de dresser leur portrait après coup, voire d'appeler la police si elle évente la ruse assez tôt.

Les manipulateurs sont généralement allergiques à ce type de risque. Toutefois, il arrive que l'enjeu justifie qu'ils s'exposent de cette manière.

Le point de vue de Jessica

Jessica Andover est très contente d'avoir trouvé un poste au sein de cette entreprise spécialisée dans la robotique. Bien sûr, ce n'est qu'une start-up qui ne peut pas la payer très cher, mais l'entreprise est petite, ses collègues sont sympathiques, et elle a l'espoir de s'enrichir grâce aux stock-options qu'elle touche. Elle ne deviendra peut-être pas millionnaire comme les créateurs de la société, mais tout de même suffisamment riche.

C'est pour toutes ces raisons que Rick Daggot est accueilli par un sourire chaleureux quand il franchit les portes de la société en ce matin d'août. Avec son costume Armani, sa montre Rolex President et sa coupe de cheveux soignée, il a cette attitude virile et confiante qui faisait déjà tourner la tête des filles quand Jessica était au lycée.

"Bonjour, dit-il, je suis Rick Daggot et je viens pour mon rendez-vous avec Larry."

Le sourire de Jessica s'évanouit. "Larry ? dit-elle. Il est en vacances pour la semaine."

"J'avais rendez-vous avec lui à treize heures. Je suis venu exprès de Louisville pour le rencontrer," répond Rick en sortant son PDA (*Personal Digital Assistant*, assistant numérique personnel), qu'il allume et montre à Jessica.

Elle regarde l'écran et secoue la tête : "C'est le 20, la semaine prochaine." Il reprend son PDA et y jette un coup d'œil. "Oh non ! gémit-il. Je n'arrive pas à croire que j'aie pu faire une erreur aussi stupide."

"Je peux peut-être vous réserver un vol pour le retour ?", demande-t-elle, se sentant désolée pour lui.

Pendant qu'elle téléphone, Rick lui confie que Larry et lui étaient sur le point de mettre en place une alliance commerciale stratégique. La société de Rick fabrique des produits pour les chaînes d'assemblage, produits qui complètent parfaitement le prochain modèle de la société de Larry, le C2Alpha. Ensemble, le C2Alpha et les produits de Rick formeraient une solution très compétitive qui ouvrirait des marchés importants pour les deux sociétés.

Une fois que Jessica a fini d'effectuer la réservation pour un vol en fin d'après-midi, Rick dit : "Bon, je pourrai au moins parler à Steve, s'il est là." Mais Steve, le cofondateur et vice-président de l'entreprise, n'est pas là non plus.

Rick, dont l'amabilité vis-à-vis de Jessica est à la limite de la séduction, suggère alors que puisqu'il est là et qu'il doit attendre la fin de l'après-midi pour son vol de retour, il pourrait emmener déjeuner quelques-uns des principaux collaborateurs de Larry. Et il ajoute : "Vous aussi, bien entendu. Y a-t-il quelqu'un qui puisse vous remplacer à l'heure du déjeuner ?"

Flattée à l'idée de déjeuner avec Rick, Jessica demande : "Qui d'autre souhaitez-vous voir ?". Il tapote sur son PDA et nomme quelques personnes : deux ingénieurs du service de recherche et développement, le nouveau commercial et le responsable financier du projet. Rick demande à Jessica de contacter chacune de ces personnes et de leur dire qui il est. Il mentionne ensuite le meilleur restaurant des environs, où Jessica a toujours voulu manger, dit qu'il réservera lui-même une table pour 12 h 30 et qu'il rappellera en fin de matinée pour s'assurer que tout se passe comme prévu.

Lorsque les quatre employés et Jessica arrivent au restaurant, leur table n'est pas encore prête, aussi s'installent-ils au bar, et Rick fait comprendre que l'addition sera pour lui. Rick a du style, et c'est le genre de personne avec qui

on se sent immédiatement à l'aise, comme si on le connaissait depuis des années. Il semble toujours avoir le mot juste, a toujours une remarque à faire ou une anecdote intéressante à raconter quand la conversation faiblit et, d'une manière générale, est d'une compagnie très agréable.

Il mentionne juste assez de détails concernant les produits de son entreprise pour que ses interlocuteurs puissent se faire une bonne idée de l'offre commerciale conjointe qu'ils vont proposer. Il cite plusieurs très grosses sociétés qui sont clientes de son entreprise et, au bout d'un moment, tous ses interlocuteurs sont convaincus que leur produit sera un succès commercial dès son lancement.

Puis Rick se lance dans une discussion à part avec Brian, l'un des ingénieurs. Tandis que les autres discutent entre eux, Rick partage en privé quelques idées avec l'ingénieur, insistant sur les particularités du C2Alpha qui le distinguent de la concurrence. Il apprend ainsi que la société se montre volontairement discrète sur certaines de ces particularités, particularités dont Brian est fier et qu'il qualifie de "top".

Rick bavarde ainsi discrètement avec chacun. Le commercial est content de pouvoir discuter de la date de sortie et du plan marketing. Le responsable financier tire une enveloppe de sa poche et note en détail les frais liés aux matières premières et à la fabrication, les prix de vente et la marge prévue, ainsi que les contrats qu'ils espèrent passer avec chacun des revendeurs, dont il n'oublie pas de préciser les noms.

Quand leur table est prête, Rick a échangé des idées avec tout le monde et gagné un cercle d'admirateurs. À la fin du repas, tout le monde serre la main de Rick et le remercie. Il échange des cartes de visite avec chacun et mentionne en passant à Brian, l'ingénieur, qu'il aimerait avoir une discussion plus approfondie avec lui dès que Larry serait de retour.

Le lendemain, Brian décroche son téléphone et constate que c'est Rick qui l'appelle ; celui-ci lui dit qu'il vient de s'entretenir avec Larry. "Je repasse lundi pour régler quelques détails avec lui, dit Rick, et en attendant, il voudrait que j'aie plus de détails sur votre produit. Il m'a dit que vous pourriez m'envoyer les derniers plans et les dernières spécifications. Il choisira les informations qui doivent m'être communiquées."

L'ingénieur dit que cela ne posera pas de problème. "Bien", répond Rick. Et il poursuit : "Larry m'a dit de vous dire qu'il avait des problèmes pour récupérer son courrier électronique. Il s'est donc arrangé pour créer à partir de son hôtel un nouveau compte de courrier Yahoo. Il a dit que vous deviez envoyer les fichiers à l'adresse larryrobotics@yahoo.com."

Le lundi matin suivant, quand un Larry bronzé et détendu arrive dans les locaux de son entreprise, Jessica ne peut s'empêcher de mentionner Rick. "C'est vraiment quelqu'un de sympa. Il nous a invités à déjeuner, moi et quelques autres." Larry paraît déconcerté. "Rick ? Quel Rick ?"

"Comment, quel Rick ? Ton nouveau partenaire commercial !"

"Quoi ?"

"Et tout le monde a été très impressionné par les questions qu'il a posées."

"Je ne connais personne du nom de Rick."

"Qu'est-ce que tu racontes ? C'est une blague, Larry, tu me fais marcher !"

"Convoque-moi tous les chefs de département, et tout de suite. Toutes affaires cessantes. Et aussi tous ceux qui étaient présents à ce déjeuner, toi comprise."

L'ambiance autour de la table de réunion est sombre ; personne ne dit mot. Larry entre, s'assoit et prend la parole : "Je ne connais personne du nom de Rick. Je n'ai pas de nouveau partenaire commercial dont je vous aurais caché l'existence. Et je pensais que cela allait de soi. Si cette histoire est une plaisanterie, j'aimerais que la personne qui en est responsable se dénonce."

Un silence pesant lui répond, et l'atmosphère s'assombrit d'instant en instant.

Finalement, Brian parle : "Pourquoi est-ce que tu n'as rien dit quand je t'ai envoyé l'e-mail avec les spécifications du produit et le code source ?"

"Quel e-mail ?"

Brian se raidit. "Oh, bon sang !"

Cliff, l'autre ingénieur, intervient : "Il nous a donné des cartes de visite à nous tous. Il n'y a qu'à l'appeler pour exiger des réponses."

Brian sort son PDA, y affiche une entrée puis fait glisser l'appareil au travers de la table en direction de Larry. Contre toute vraisemblance, tous caressent encore un faible espoir tandis que Larry compose le numéro. Après quelques instants, il appuie sur la touche du haut-parleur du téléphone et tout le monde entend que la ligne est occupée. Après avoir essayé le même numéro pendant vingt minutes sans rien obtenir d'autre que ce même signal, Larry, énervé, appelle une opératrice pour obtenir plus d'informations.

L'opératrice de la compagnie de téléphone lui demande, sur un ton méfiant : "Où avez-vous obtenu ce numéro, monsieur ?" Larry répond qu'il se trouve sur la carte de visite d'un homme qu'il doit contacter d'urgence. L'opératrice répond : "Je suis désolée. Il s'agit d'un numéro utilisé par nos techniciens pour effectuer des tests, et qui sonne toujours occupé."

Larry fait la liste de toutes les informations qui ont été communiquées à Rick. Le bilan n'est pas réjouissant.

Deux policiers viennent enregistrer les dépositions. Après avoir écouté l'histoire, ils font remarquer qu'aucun crime n'a été commis au niveau de l'État, et qu'ils ne peuvent rien faire. Ils conseillent à Larry de contacter le FBI, qui est compétent pour les litiges commerciaux impliquant plusieurs États. Quand Rick Daggot a employé une fausse identité pour se faire envoyer les caractéristiques du produit, il a peut-être commis un crime fédéral, mais il faudrait que Larry en parle avec le FBI pour en être sûr.

Trois mois plus tard, Larry prend son petit déjeuner dans sa cuisine en lisant son journal lorsqu'il manque renverser son café. Ce qu'il craignait depuis qu'il avait entendu parler de Rick, son pire cauchemar, est arrivé. En première page de la section économie du journal, une société dont il n'a jamais entendu parler annonce la sortie d'un produit qui ressemble point pour point au C2Alpha que sa propre entreprise développe depuis deux ans.

Des inconnus lui ont volé son produit et l'ont commercialisé avant lui. Son rêve est détruit. Les millions de dollars investis en recherche et en développement sont perdus. Et il ne pourrait sans doute jamais rien prouver à leur encontre.

Le point de vue de Sam Sanford

Sam Sanford aurait été assez malin pour obtenir un poste bien payé dans n'importe quelle entreprise, mais il préférait gagner sa vie en escroquant son prochain, ce qui lui réussissait bien. Il a fini par attirer l'attention d'un espion qui avait été mis à la retraite de manière anticipée à cause de ses problèmes de boisson. Aigri et vindicatif, ce dernier avait trouvé un moyen de tirer profit des talents qu'il avait développés au service du gouvernement. Il était toujours à la recherche de personnes qu'il pourrait employer, et il a repéré Sam dès leur première rencontre. À ses côtés, Sam a constaté qu'il était aussi facile, et au moins aussi profitable, de soutirer des informations aux sociétés que de soutirer de l'argent à des particuliers. Voici comment il raconte son histoire.

"Il faut du cran pour faire ce que je fais. Quand on essaie de tromper les gens par téléphone, ou *via* Internet, on n'a aucun risque de se faire repérer. Mais un bon arnaqueur traditionnel, du genre qui travaille en face à face avec sa victime (et c'est un métier qui est loin d'avoir disparu, croyez-moi), est capable de vous regarder droit dans les yeux, de vous raconter des salades et de faire en sorte que vous le croyiez. Certains procureurs appellent cela un délit. Pour moi, c'est un don.

Mais il ne faut pas s'aventurer à l'aveuglette : il faut d'abord s'informer. Un escroc qui travaille dans la rue peut prendre la température de quelqu'un avec un brin de conversation et quelques suggestions prudentes. Si la personne fournit les bonnes réponses, l'escroc s'est trouvé un pigeon.

Quand la cible est une société, il y a un travail de préparation à faire. Savoir comment elle fonctionne, ce qu'elle veut et de quoi elle a besoin. Être patient. Choisir le rôle qu'on va jouer et apprendre ses répliques. Et ne pas se lancer avant d'être prêt.

J'ai mis plus de trois semaines à préparer ce coup-là. Le client m'a formé pendant deux jours sur ce que "ma" société produisait et sur les raisons pour lesquelles cette alliance commerciale serait aussi lucrative.

Ensuite, j'ai eu de la chance. J'ai appelé la société et j'ai prétendu représenter une société de capital-risque qui souhaitait fixer un rendez-vous ; j'essayais de trouver un moment, au cours des prochains mois, où tous nos partenaires seraient disponibles : y avait-il une période à éviter, où Larry serait absent ? On m'a répondu que oui, qu'il n'avait pas pris de vacances depuis la création de sa société, mais que sa femme l'avait obligé à prendre des vacances au cours de la première semaine d'août.

C'était dans deux semaines. Je pouvais attendre.

Entre-temps, un magazine spécialisé m'avait fourni le nom de l'agence de relations publiques de la société. J'ai appelé l'agence et leur ai dit que j'appréciais la couverture médias qu'ils fournissaient pour leur client, la société de robotique ; je souhaitais donc que la personne qui s'occupait de ce compte prenne en charge ma société. La personne en question était une jeune femme dynamique qui voyait d'un bon œil la possibilité d'obtenir un nouveau compte. Au cours d'un repas onéreux et un tout petit peu trop arrosé, la jeune femme a fait son possible pour me convaincre que son agence gérait extrêmement bien les problèmes de relations publiques de ses clients. J'ai fait celui qui en avait vu d'autres. J'avais besoin de plus de détails. En la poussant un petit peu, à la fin du repas, j'en avais appris plus que je n'espérais sur le nouveau produit et sur les problèmes internes de la société.

Le reste de l'opération s'est déroulé exactement comme je l'avais prévu. La réceptionniste a avalé sans le moindre soupçon mon histoire selon laquelle je m'étais trompé d'une semaine pour le rendez-vous, et que je voulais néanmoins en profiter pour rencontrer les membres de l'équipe. Elle a même été désolée pour moi. Le déjeuner m'a coûté 150 dollars, pourboire compris.

Mais j'avais les informations qu'il me fallait : les numéros de téléphone, les noms des postes, et un homme clé qui croyait que j'étais bien la personne que je prétendais être.

J'admets que Brian m'a bien eu pendant un moment. Il semblait être le genre de personne prête à m'envoyer n'importe quoi pourvu que je le lui demande. Mais quand j'ai indiqué ce que je voulais qu'il m'envoie, il a semblé un peu sur ses gardes. C'est là qu'on voit qu'une bonne préparation est essentielle. J'avais gardé en réserve le compte de courrier électronique au nom de Larry, juste au cas où. Les responsables de la sécurité, chez Yahoo, attendent sans doute encore que quelqu'un utilise le compte de courrier afin de pouvoir le retrouver. Ils peuvent attendre longtemps. L'oiseau s'est envolé. Je suis maintenant sur un autre projet."

Analyse du stratagème

Dans un stratagème qui implique un face à face, le manipulateur doit avoir une apparence adaptée au rôle qu'il veut jouer. Il aura tel aspect sur un champ de courses, tel aspect au café du coin, tel autre encore au bar d'un hôtel de luxe.

Il en va de même dans le domaine de l'espionnage industriel. Dans certains cas, le manipulateur privilégiera le costume-cravate s'il cherche à se faire passer pour un cadre dirigeant d'une grosse entreprise, pour un consultant ou pour un commercial. Dans d'autres cas, lorsqu'il cherchera à se faire passer pour un analyste programmeur, un technicien ou le responsable du courrier, les vêtements, l'uniforme, bref toute son apparence sera très différente.

Pour infiltrer la société, l'homme qui dit s'appeler Rick Daggot sait qu'il doit projeter une image de confiance en soi et de compétence, qu'il s'appuie sur des connaissances approfondies du produit développé par la société et du secteur d'activité en général.

Il ne lui a pas été très difficile de trouver au préalable les informations dont il avait besoin. Une petite ruse lui a permis de savoir quand le grand patron serait absent. En revanche, il était un peu plus délicat d'obtenir assez de détails sur le projet pour pouvoir donner l'impression d'être un "initié" par rapport aux produits de la société. Souvent, ces informations sont connues de différents partenaires de la société : investisseurs, sociétés de capital-risque contactées par le passé pour financer l'entreprise, banquier, cabinet d'avocats. L'assaillant doit toutefois se montrer prudent : il peut être difficile de trouver quelqu'un qui soit prêt à fournir des informations internes à l'entreprise, et en essayant deux ou trois sources potentielles d'informations, on risque de tomber sur quelqu'un qui aura des soupçons et fera capoter toute l'affaire. Les manipulateurs doivent choisir leurs victimes avec soin et n'essayer qu'une seule fois chaque piste.

Le déjeuner était un autre moment risqué. Il fallait qu'il passe quelques instants avec chacune des personnes invitées sans que les autres n'entendent la conversation. Il a dit à Jessica qu'ils allaient déjeuner dans un restaurant chic à 12 h 30, mais il a réservé la table pour 13 heures. Il espérait que cela les obligerait à attendre au bar pendant un moment, et c'est exactement ce qui s'est passé. Il a ainsi eu la possibilité de passer de l'un à l'autre et de bavarder avec chacun.

Rick pouvait toutefois encore se trahir de bien des manières : une mauvaise réponse ou une remarque imprudente auraient suffi. Seul un espion industriel très astucieux et très sûr de lui aurait pris le risque de s'exposer de cette manière. Mais Rick avait des années d'expérience acquises dans la rue et il avait confiance en ses capacités : même s'il commettait une erreur, il serait capable de se rattraper et de gommer les soupçons éventuels. C'était le moment le plus dangereux et le plus difficile de l'opération, et la poussée d'adrénaline qu'il a ressentie à ce moment-là lui a fait comprendre qu'il n'avait pas besoin de conduire une voiture de sport, de faire du vol libre ou de tromper sa femme : son travail était sa vraie source de plaisir. Il s'est demandé combien de personnes auraient pu en dire autant.

Le message de Mitnick

La plupart des manipulations sont perpétrées par téléphone ou Internet, mais ne comptez pas sur le fait qu'un assaillant n'oserait jamais se présenter en personne dans votre entreprise. Dans la plupart des cas, l'imposteur utilisera une forme quelconque de manipulation pour accéder au bâtiment après avoir falsifié un badge de salarié à l'aide d'un simple logiciel du commerce tel que Photoshop.

Qu'en est-il des cartes de visite qui indiquent un numéro qu'un opérateur téléphonique utilise pour des tests ? La série télévisée *The Rockford Files*, dont le personnage principal était un détective privé, illustrait l'utilisation de cette technique. Rockford, qui était joué par l'acteur James Garner, disposait dans sa voiture d'une machine à imprimer les cartes de visite qu'il employait pour obtenir des cartes correspondant à ses besoins du moment. Aujourd'hui, un manipulateur peut faire imprimer des cartes de visite en moins d'une heure ou les imprimer lui-même avec une imprimante laser.

Note

John Le Carré, l'auteur de *L'espion qui venait du froid*, de *Un pur espion* et de nombreux autres livres remarquables, est le fils d'un aventurier doublé d'un escroc. Enfant, Le Carré a été frappé de constater que même si son père parvenait facilement à tromper qui il voulait, il était lui-même fréquemment victime d'autres escrocs. Ce qui montre que personne n'est à l'abri d'une manipulation, pas même un manipulateur.

Qu'est-ce qui amène un groupe d'hommes et de femmes intelligents à se faire avoir par un imposteur ? Pour porter un jugement sur une situation donnée, nous utilisons à la fois notre instinct et notre intellect. Quand, d'une part, une histoire est plausible (et donc que notre intellect l'accepte) et que, d'autre part, l'imposteur projette une image vraisemblable, nous avons tendance à baisser notre garde. C'est la vraisemblance de l'image projetée qui fait la différence entre un imposteur ou un manipulateur qui réussit et celui qui se retrouve rapidement derrière les barreaux.

Demandez-vous si vous seriez entièrement imperméable à une histoire telle que celle de Rick. Si vous êtes sûr que oui, demandez-vous si vous avez *jamais* été trompé par personne. Si cela s'est produit, il est probable que la vraie réponse à la première question est non.

SAUTE-MOUTON

Dans l'histoire qui suit, il n'est pas question d'espionnage industriel, mais en la lisant, vous comprendrez pourquoi elle a sa place dans ce chapitre.

Harry Tardy était de retour au bercail, et il était amer. Il espérait pourtant que les Marines seraient une porte de sortie, mais le camp d'entraînement s'était avéré beaucoup trop dur pour lui. Et maintenant, il était à nouveau dans son petit patelin qu'il détestait, prenait des cours d'informatique pour adultes dispensés par l'université locale et cherchait un moyen de se venger de ce qu'il subissait.

Il a fini par le trouver. En buvant des bières avec un camarade de son cours, il s'est plaint de leur formateur, un monsieur je-sais-tout méprisant, et, ensemble, ils ont mis au point un plan pour le compromettre : ils allaient obtenir le code source utilisé dans l'un des modèles de PDA les plus vendus, l'envoyer sur l'ordinateur du formateur et laisser des traces de manière à faire croire que ce dernier était le coupable.

Le camarade en question, Karl Alexander, dit à Harry qu'il "connaissait quelques trucs" et qu'il lui expliquerait comment procéder. Sans se faire pincer.

Travail préliminaire

En commençant ses recherches, Harry a appris que le produit avait été développé dans un centre situé à proximité du siège social à l'étranger. Mais il existait également un laboratoire de recherche et développement aux États-Unis. Selon Karl, c'était une bonne chose : pour qu'ils puissent parvenir à leurs fins, il fallait qu'un site quelconque aux États-Unis ait également besoin d'avoir accès au code source.

Harry était alors prêt à appeler le laboratoire de développement à l'étranger. Il devait lancer un appel au secours, du type "j'ai un problème, aidez-moi s'il vous plaît". Bien entendu, l'appel au secours devait être un peu plus subtil que cela. Karl a rédigé un script, mais Harry ne paraissait absolument pas crédible quand il le lisait. Il a donc dû s'entraîner pendant un moment avec Karl pour pouvoir dire son texte sur un ton naturel.

Ce que Harry a fini par dire, avec Karl à ses côtés, ressemble plus ou moins à ceci :

"J'appelle du centre de recherche et développement de Minneapolis. Notre serveur a été infecté par un ver qui s'est répandu dans tout le département. Nous avons dû réinstaller le système d'exploitation et quand nous avons voulu utiliser les sauvegardes pour récupérer les données, toutes les sauvegardes étaient corrompues. Et devinez qui était censé vérifier l'intégrité des sauvegardes ? Moi. Et maintenant, mon chef me crie dessus, et la direction est furieuse que les données aient été perdues. J'aurais besoin de la dernière version du code source aussi vite que possible. Est-ce que vous pourriez me *gzipper* le code et me l'envoyer ?"

À ce moment, Karl lui a écrit une petite note, et Harry a dit à son interlocuteur qu'il avait juste besoin d'un transfert interne du fichier vers le centre de recherche et développement de Minneapolis. C'était un point essentiel : lorsque le correspondant de Harry a su qu'on lui demandait d'envoyer le fichier en interne, il n'a plus eu de scrupules ; après tout, quel mal pouvait-il y avoir à cela ?

Jargon

Gzipper
Réunir des fichiers en un seul fichier compressé à l'aide d'un utilitaire Linux GNU nommé gzip.

Il a donc accepté de gzipper et d'envoyer les fichiers. Étape par étape, avec l'aide de Karl, Harry a expliqué à son interlocuteur la procédure à suivre pour transformer l'énorme code source en un seul fichier compact. Il lui a également indiqué le nom à donner au fichier compressé, "newdata" (nouvelles données), expliquant qu'il éviterait ainsi toute confusion avec les anciens fichiers corrompus.

Karl a dû expliquer deux fois l'étape suivante à Harry avant qu'il ne la comprenne, et qui était un élément essentiel du petit jeu de saute-mouton qu'avait imaginé Karl. Harry devait maintenant appeler le centre informatique de Minneapolis et raconter une histoire du type : "Je vais vous envoyer un fichier, pouvez-vous le réexpédier ailleurs pour moi ?", le tout bien sûr habillé de motifs plausibles. Harry avait du mal à comprendre pourquoi il fallait dire que c'était lui, Harry, qui envoyait un fichier, alors que le fichier ne venait pas de lui, mais de quelqu'un à l'étranger.

"Le type du centre de recherche et développement sert d'intermédiaire, a expliqué Karl. Il doit croire qu'il ne fait que rendre un service à un collègue ici aux États-Unis, et que ce service consiste à recevoir un fichier qui vient de toi et à le réexpédier à ta place."

Harry a fini par comprendre. Il a appelé le centre de recherche et développement, où il a demandé à la standardiste de le mettre en contact avec le centre informatique, puis il a demandé à parler à un technicien. L'homme qui a décroché semblait aussi jeune que Harry lui-même. Harry l'a salué et lui a expliqué qu'il appelait du département de production de Chicago, et qu'il essayait depuis un moment d'envoyer un fichier à un partenaire commercial avec lequel il travaillait sur un projet commun, mais qu'à cause d'un problème de routeur, il ne parvenait pas à atteindre son réseau. "Est-ce que je peux vous transférer le fichier ? Quand vous l'aurez reçu, je vous appellerai pour que vous le transfériez sur l'ordinateur du partenaire commercial."

Harry a ensuite demandé au jeune homme si le centre informatique disposait d'un service de *FTP anonyme*, une configuration qui permet de transférer des fichiers en provenance et à destination d'un dossier sans qu'aucun mot de passe ne soit nécessaire. Oui, ils disposaient d'un FTP anonyme, et le technicien a donné à Harry l'adresse IP interne pour y accéder.

Jargon

FTP anonyme
Programme qui permet à des utilisateurs distants d'accéder aux dossiers d'un ordinateur sans avoir besoin de disposer d'un compte. Le transfert de fichiers se fait à l'aide du protocole FTP (*File Transfer Protocol*). En principe, lorsqu'un ordinateur est configuré de cette manière, seuls certains dossiers sont rendus accessibles.

Une fois qu'il a eu cette information, Harry a rappelé le centre de recherche et développement à l'étranger. Le fichier compressé était prêt, et Harry a fourni les instructions pour qu'il soit transféré sur le serveur FTP anonyme. En moins de cinq minutes, le code source compressé était parvenu à destination au centre informatique de Minneapolis.

Le piège se referme

Le plus dur était fait. Avant de continuer, Harry et Karl devaient maintenant attendre pour être sûrs que le fichier était arrivé. Pendant ce temps, ils se sont installés devant l'ordinateur du formateur et ont effectué deux opérations indispensables. La première consistait à installer un serveur FTP anonyme sur la machine afin que celle-ci puisse accueillir le fichier transféré.

La seconde permettait de résoudre un problème délicat. À l'évidence, ils ne pouvaient demander au technicien du centre informatique d'envoyer le fichier à une adresse telle que warren@rms.ca.edu, par exemple. Le domaine ".edu" dévoilerait immédiatement la supercherie, puisque n'importe quel technicien informatique le reconnaîtrait immédiatement comme l'adresse d'une école ou d'une université, ce qui ferait échouer tout le stratagème. Pour contourner ce problème, ils sont allés dans Windows sur l'ordinateur de l'instructeur et ont noté l'adresse IP de la machine, qui n'est composée que de chiffres.

Entre-temps, le moment était venu de rappeler le technicien du centre informatique. Harry lui a indiqué qu'il venait de transférer le fichier dont il lui avait parlé. "Pouvez-vous vérifier que vous l'avez reçu ?" Oui, il était arrivé. Harry lui a alors demandé d'essayer de l'envoyer et lui a fourni l'adresse IP relevée sur l'ordinateur du formateur. Il est resté en ligne tandis que son interlocuteur effectuait la connexion et lançait le transfert, puis il a

eu un large sourire quand la diode du disque dur de l'ordinateur du formateur s'est mise à clignoter — signe qu'il était en train de recevoir le fichier.

Harry a échangé quelques généralités avec le technicien sur le fait qu'un jour peut-être, les ordinateurs et les périphériques seraient plus fiables, l'a remercié et a raccroché.

Ils ont copié le fichier depuis la machine du formateur vers des disquettes Zip de manière à disposer chacun d'une copie du code source. Ce serait un peu comme une peinture volée dans un musée, qu'on peut admirer soi-même, mais qu'on n'ose pas montrer à ses amis. Sauf que dans le cas présent, ils avaient une copie, l'original se trouvant toujours dans le musée.

Karl a indiqué à Harry comment désinstaller le serveur FTP de l'ordinateur du formateur et supprimer les fichiers d'audit afin qu'il ne reste pas de traces de ce qu'ils avaient fait, à l'exception du fichier volé, placé à un endroit où il serait facile à repérer.

Pour finir, ils ont envoyé directement sur Usenet[1] une partie du code source à partir de l'ordinateur du formateur. Une partie seulement afin de ne pas causer trop de tort à la société, mais ils laissaient ainsi des traces visibles qui menaient jusqu'au formateur. Celui-ci allait se trouver dans une situation extrêmement embarrassante.

Analyse du stratagème

Il a fallu la conjonction d'un certain nombre d'éléments pour que ce plan fonctionne, mais il repose principalement sur un (faux) appel à l'entraide de la part d'un collègue qui a son patron sur le dos. Combiné avec des explications précises sur la manière dont son interlocuteur pouvait l'aider à résoudre le problème, cet argument s'est avéré suffisamment convaincant. Il a fonctionné dans la situation que nous venons de décrire, et il a fonctionné dans de nombreux autres cas.

Deuxième élément crucial : le premier interlocuteur d'Harry connaissait la valeur du fichier. Par conséquent, Harry lui a demandé de l'envoyer à une adresse *interne* de l'entreprise.

Troisième pièce du puzzle : le technicien pouvait constater que le fichier lui avait été envoyé depuis l'intérieur de l'entreprise. Cela pouvait uniquement signifier, du moins en apparence, que la personne qui lui avait transmis le fichier aurait pu l'envoyer elle-même pour peu que sa connexion réseau externe ait fonctionné. Il n'y avait donc aucune raison de refuser de l'aider.

1. N.D.T. : Réseau décentralisé qui gère les groupes de nouvelles (discussion).

Le fait de demander de renommer le fichier compressé peut paraître un détail mineur. Il n'en est rien. L'assaillant ne pouvait prendre le risque de faire transférer un fichier qui serait immédiatement identifiable en tant que code source (ou dont le nom ferait apparaître un rapport avec le produit), et qui aurait donc éveillé la suspicion. Il était donc essentiel que le fichier ait un nom neutre. De fait, le jeune technicien n'a eu aucun scrupule à envoyer à l'extérieur de l'entreprise un fichier dont le nom, *newdata*, ne fournissait aucune information quant à son contenu.

Vous avez compris pourquoi cette histoire a sa place dans ce chapitre : ce qui n'a été qu'une plaisanterie de potaches aurait aussi bien pu être une tentative d'espionnage menée par un professionnel travaillant pour un concurrent ou un pays étranger, par exemple. Dans tous les cas, les dégâts causés à l'entreprise auraient pu être énormes, car si un produit concurrent était arrivé sur le marché, cela aurait fortement réduit les ventes du produit de l'entreprise victime de la manipulation.

Votre propre entreprise est-elle vraiment à l'abri d'une telle attaque ?

Le message de Mitnick

> La règle sous-jacente que chaque salarié doit connaître et appliquer sans exception est la suivante : en l'absence d'autorisation de la part de la hiérarchie, ne jamais transférer de fichier à une personne qu'on ne connaît pas personnellement, même si l'adresse de destination semble être interne au réseau de l'entreprise.

MESURES PRÉVENTIVES

L'espionnage industriel, qui représente depuis longtemps une menace pour les entreprises, est maintenant devenu le gagne-pain de nombreux espions traditionnels qui se sont reconvertis après la fin de la Guerre froide. Ces espions peuvent être tant à la solde d'entreprises concurrentes du même pays que d'entreprises ou de gouvernements étrangers. Du fait de leur expérience passée, ils sont à même de détecter la moindre faille dans les systèmes de protection érigés par les entreprises.

Sécurité hors site

Qu'aurait pu faire l'entreprise dont la société de stockage s'est fait dérober des documents ? La menace aurait pu être évitée si l'entreprise avait crypté ses données. Le cryptage (ou *chiffrement*, pour utiliser le terme technique) repré-

sente un coût supplémentaire en temps et en argent, mais c'est une mesure de sécurité indispensable. Il faut par ailleurs vérifier à intervalles réguliers que les opérations de chiffrement et de déchiffrement s'effectuent sans problème.

Il reste toujours le risque que les clés de chiffrement se perdent ou que la seule personne qui les connaisse soit renversée par un bus. Quoi qu'il en soit, faire sous-traiter le stockage d'informations sensibles par une société extérieure sans utiliser de chiffrement est à mon avis de l'inconscience pure et simple.

Le stockage de données sensibles à l'extérieur de la société, à un endroit où des tiers peuvent accéder, est une faille de sécurité courante. Voici plusieurs années, j'étais employé par une entreprise qui aurait pu être plus prudente dans la protection des données de ses clients. Les techniciens informatiques laissaient les bandes de sauvegarde de l'entreprise à *l'extérieur* de la salle d'ordinateurs fermée afin que des coursiers puissent passer les prendre quotidiennement. N'importe qui aurait pu emmener ces bandes, qui contenaient tous les documents écrits de la société sous une forme non chiffrée. La perte de bandes de sauvegarde chiffrées est déjà, en soi, ennuyeuse ; mais si ces données ne sont pas chiffrées, leur perte peut être une catastrophe de grande ampleur pour l'entreprise.

Les grandes entreprises n'ont pas d'autre choix que de stocker les sauvegardes hors site. Mais les procédures de sécurité de l'entreprise doivent prévoir des vérifications auprès de la société de stockage pour s'assurer que celle-ci prend au sérieux la sécurité de ses clients. S'ils ne prennent pas au moins autant de précautions que votre propre entreprise, tous vos efforts en matière de sécurité peuvent être compromis.

Pour les sociétés de plus petite taille, il existe une alternative intéressante : l'envoi quotidien par Internet des fichiers nouveaux ou modifiés, à destination d'une société proposant un stockage en ligne. Ici encore, il est essentiel de chiffrer les données. Sinon, les informations sont accessibles non seulement à tout employé peu scrupuleux de la société de stockage, mais également à tout pirate informatique capable de pénétrer dans le système informatique ou le réseau de cette société.

Bien entendu, lors de la mise en place d'un système de chiffrement pour la protection des fichiers sauvegardés, il faut également établir des procédures sûres pour le stockage des clés de chiffrement ou des mots de passe qui permettent de déverrouiller les fichiers. Les clés secrètes utilisées pour chiffrer les données doivent être stockées dans un coffre-fort ou une chambre forte. Dans les procédures, il faut également prévoir la disparition soudaine du salarié qui gère ces données (départ, accident, etc.). Les codes, leur lieu de stockage ainsi que les procédures de chiffrement et de déchiffrement doivent toujours être connus d'au moins deux personnes, de même que les procédures indiquant quand et comment ces clés doivent être changées. Il faut indiquer dans ces procédures que les clés doivent être immédiatement modifiées si l'un des salariés qui y avait accès quitte l'entreprise.

L'illustre inconnu

L'histoire de ce chapitre dans laquelle un imposteur malin séduit des salariés pour leur soutirer des informations sur l'entreprise montre l'importance que l'on doit accorder à la vérification des identités. La deuxième histoire, dans laquelle le manipulateur demande à ce qu'un fichier soit réexpédié vers un site FTP, montre également à quel point il est important de savoir qui formule la demande.

Vous trouverez au Chapitre 16 des règles précises à suivre pour vérifier l'identité d'un inconnu qui souhaite obtenir des informations ou demande à ce que soit effectuée une opération quelconque. Nous avons parlé de vérification tout au long de ce livre ; le Chapitre 16 vous montrera comment procéder.

Partie 4

Stratégies de prévention

Chapitre 15

Programme de formation et d'information des salariés

Un manipulateur a reçu pour mission d'obtenir les plans de votre nouveau produit, dont la sortie est prévue dans quelques mois. Qu'est-ce qui va l'arrêter ?

Votre pare-feu ? Non.

Des méthodes d'authentification sophistiquées ? Non.

Des systèmes de détection d'intrusions ? Non.

Le chiffrement ? Non.

La limitation des numéros de téléphone pouvant obtenir un accès par modem ? Non.

Des noms de codes pour les serveurs, afin que la nature des informations qui s'y trouvent soit plus difficile à déterminer pour les intrus ? Non.

La vérité est qu'aucune technologie au monde n'est capable d'empêcher l'attaque d'un manipulateur.

LA SÉCURITÉ GRÂCE À LA TECHNOLOGIE, À LA FORMATION ET AUX PROCÉDURES

Les sociétés qui effectuent des tests de pénétration pour vérifier la sécurité de leur entreprise signalent que les tentatives effectuées par des manipulateurs pour pénétrer leurs systèmes informatiques ont un taux de réussite de *presque 100 %*. Les moyens technologiques mis en œuvre peuvent rendre plus difficile ce type d'attaque dans la mesure où ils réduisent le nombre de personnes impliquées dans le processus de prise de décision. Toutefois, le seul moyen

efficace pour réduire le danger que représentent les manipulateurs consiste à mettre en place *à la fois* un programme de sensibilisation des salariés, des règles définissant l'attitude que doivent adopter les salariés dans différentes situations, et une formation aux problèmes de sécurité.

Le seul moyen de protéger les plans de vos produits est de faire en sorte que vos salariés soient formés et conscients du danger, et qu'ils appliquent les consignes. Cela implique de mettre en place une formation portant sur les règles et les procédures, mais surtout un programme de sensibilisation permanent. Certains professionnels recommandent d'utiliser 40 % du budget de sécurité d'une entreprise pour les programmes de sensibilisation.

La première étape consiste à faire prendre conscience à tous les salariés qu'il existe des personnes sans scrupules susceptibles de les tromper pour les manipuler psychologiquement. Les salariés doivent savoir quelles informations doivent être protégées et comment elles doivent l'être. Une fois qu'on sait de quelle manière on est susceptible d'être manipulé, on a beaucoup plus de chances de prendre conscience du fait qu'une attaque est en cours.

La sensibilisation à la sécurité suppose aussi qu'il faut informer tout le monde des procédures et des règles de sécurité de l'entreprise. Comme vous le verrez au Chapitre 16, il est nécessaire d'établir des règles pour guider les salariés dans certaines situations afin de protéger les systèmes informatiques et les informations sensibles de l'entreprise.

Vous trouverez dans ce chapitre et dans le suivant les mesures que vous devez prendre en matière de sécurité afin d'éviter les attaques. Si vos salariés ne sont pas bien entraînés et bien formés et s'ils ne suivent pas des procédures soigneusement conçues, la question n'est pas de savoir *si*, mais *quand* votre entreprise sera la victime d'une attaque d'un manipulateur. N'attendez pas qu'une attaque se produise pour mettre en place ces règles : les dégâts causés par un assaillant pourraient toucher à la fois l'entreprise elle-même et les emplois de vos salariés.

COMMENT LES ASSAILLANTS PROFITENT DE LA NATURE HUMAINE

Pour développer un programme de formation efficace, vous devez d'abord comprendre pourquoi les personnes sont exposées aux attaques. L'identification de ces tendances au cours de vos formations — sur lesquelles vous pourriez attirer l'attention à l'aide de jeux de rôles, par exemple — aidera vos salariés à comprendre pourquoi nous pouvons tous être manipulés par des imposteurs.

La manipulation est étudiée par les scientifiques depuis au moins cinquante ans. Dans le numéro de février 2001 du magazine *Scientific American*, Robeft B. Cialdini a publié un article qui résume ces recherches. Cet article parle de six "tendances primaires de la nature de l'homme" qui jouent un rôle dans les tentatives que l'on fait pour obtenir une réponse favorable à une demande.

Ces tendances sont celles sur lesquelles se basent consciemment ou, le plus souvent, inconsciemment, les manipulateurs.

L'autorité

La plupart des gens obéissent aveuglément quand une demande provient d'une personne qui dispose d'une quelconque autorité, ou d'une personne censée être habilitée à effectuer cette demande.

Dans son livre, *Influence*, le Dr. Cialdini parle d'une étude menée dans trois hôpitaux du Middle West, où vingt-deux postes d'infirmières ont été contactés par une personne qui prétendait être un médecin de l'hôpital et qui a donné des instructions pour administrer à un patient un médicament qui n'est délivré que sur ordonnance. Les infirmières qui ont reçu cet appel ne connaissaient pas leur interlocuteur. Elles n'avaient aucune preuve qu'il était médecin (et il ne l'était pas). Les instructions leur ont été données par téléphone, ce qui allait à l'encontre des règles de l'hôpital. Le médicament n'était pas censé être administré dans la partie de l'hôpital où se trouvaient les infirmières, et la dose qu'on leur avait demandé d'administrer représentait le double de la dose quotidienne maximale, ce qui aurait pu mettre en danger la vie du patient. Pourtant, Cialdini indique que dans 95 % des cas, l'infirmière est allée chercher la dose indiquée du médicament à la pharmacie de l'hôpital, puis a pris la direction de la chambre du patient (avant d'être interceptée par un observateur et informée de l'expérience).

Exemple d'attaque : le manipulateur peut se prévaloir d'une certaine autorité, en prétendant par exemple faire partie du service informatique ou travailler pour la direction de l'entreprise.

La sympathie

La victime a davantage tendance à répondre à une demande quand l'interlocuteur lui apparaît comme quelqu'un de sympathique ou qui a des intérêts, des croyances ou des attitudes analogues aux siennes.

Exemples d'attaques : au cours de la conversation, l'assaillant parvient à déterminer l'un des centres d'intérêt de la victime et fait semblant de

s'intéresser lui aussi au même sujet. Il peut aussi prétendre venir de la même région ou de la même université, ou avoir les mêmes objectifs. Le manipulateur pourra également tenter d'imiter les comportements de sa cible afin de donner l'impression d'une ressemblance.

La réciprocité

Nous acceptons plus facilement de rendre service si nous avons au préalable obtenu une faveur ou la promesse d'une faveur. Il peut s'agir d'un objet matériel, d'un conseil ou d'une aide. Quand quelqu'un nous rend un service, on a tendance à vouloir lui rendre la pareille, même quand le service n'a pas été sollicité.

Les membres de la secte Hare Krishna savaient très bien exploiter cette tendance de l'être humain. Ils donnaient un livre ou une fleur aux gens, et quand ceux-ci tentaient de le leur rendre, ils refusaient en disant : "C'est un cadeau que nous vous faisons". La tendance naturelle à la réciprocité faisait qu'ils obtenaient ainsi quantité de dons.

Exemple d'attaque : un salarié reçoit un appel d'une personne qui dit qu'elle fait partie du service informatique. L'interlocuteur explique que certains ordinateurs de la société ont été infectés par un virus, non reconnu par les logiciels antivirus et capable de détruire tous les fichiers de l'ordinateur. Il indique ensuite quelles mesures prendre pour éviter le problème. Après cela, l'interlocuteur demande à la personne de tester un utilitaire récemment mis à jour qui permet aux utilisateurs de changer de mot de passe. Le salarié a du mal à refuser parce que son interlocuteur vient de l'aider à se protéger d'un virus, il lui rend donc la pareille en acceptant de tester l'utilitaire.

La cohérence

Lorsqu'on s'engage ouvertement à faire quelque chose, il est difficile par la suite de se désister. En effet, un désistement pourrait nous faire passer pour quelqu'un de peu fiable, d'où notre tendance à aller jusqu'au bout une fois que nous avons pris un engagement.

Exemple d'attaque : l'assaillant contacte une nouvelle recrue et l'informe que l'utilisation des systèmes informatiques de l'entreprise est soumise à l'acceptation des règles et des procédures de sécurité. Après avoir énoncé quelques règles de sécurité, l'interlocuteur demande à l'utilisateur de lui indiquer son mot de passe, afin de vérifier qu'il respecte bien les règles de sécurité en ce qui concerne la complexité des mots de passe. Lorsque l'utilisateur a dévoilé son mot de passe, l'interlocuteur lui recommande d'en créer un autre, et ses conseils mènent l'utilisateur à choisir un mot de passe que l'assaillant pourra deviner facilement. La victime obéit parce qu'elle a, au préalable, accepté de se conformer aux règles de sécurité de l'entreprise et qu'elle suppose que son interlocuteur n'a fait que vérifier qu'elle suivait bien ces règles.

La validation sociale

L'être humain a tendance à obéir plus facilement quand ses actions se conforment à celles de son entourage. Les actes des autres sont validés si le comportement est correct et l'action appropriée.

Exemple d'attaque : l'assaillant explique qu'il réalise une étude et cite les noms de plusieurs personnes du service qui y auraient déjà participé. Pour la victime, la participation de ses collègues valide l'authenticité de la requête, elle accepte donc d'y prendre part. Son interlocuteur lui pose alors une série de questions au cours desquelles il l'amène à dévoiler son nom d'utilisateur et son mot de passe.

La rareté

Un individu aura tendance à répondre plus facilement à une demande s'il croit que l'objet recherché est rare et que d'autres sont en concurrence avec lui pour l'obtenir, ou qu'il est disponible uniquement pendant une durée limitée.

Exemple d'attaque : l'assaillant envoie des e-mails qui annoncent que les 500 premières personnes qui s'enregistreront auprès d'un nouveau site Web recevront des places de cinéma. Quand un visiteur s'enregistre sur le site, on lui demande de fournir son adresse électronique professionnelle et de choisir un nom d'utilisateur et un mot de passe. Nombre d'utilisateurs, pour se simplifier la vie, tendent à employer systématiquement le même mot de passe ou des mots de passe similaires. L'assaillant peut ensuite tenter de compromettre la sécurité de l'ordinateur personnel ou professionnel de la victime en se servant du nom d'utilisateur et du mot de passe fournis.

CRÉATION D'UN PROGRAMME DE SENSIBILISATION ET DE FORMATION

Le fait de diffuser une brochure indiquant les règles de sécurité à respecter ou d'inciter les salariés à se rendre sur une page de l'intranet où sont expliqués les risques de sécurité ne suffit pas à réduire les risques. Chaque entreprise doit non seulement définir des règles de sécurité et les fixer par écrit, mais

également inciter *toute personne* ayant accès à des informations internes ou au système informatique à apprendre et à suivre ces règles. De plus, il faut s'assurer que chacun comprend bien les raisons de l'existence de chacune des règles, afin que personne ne soit tenté de les ignorer par paresse ou pour gagner du temps. Sinon, le salarié aura toujours l'excuse de l'ignorance, et c'est justement cette vulnérabilité qu'exploitent les manipulateurs.

L'objectif central de tout programme de sensibilisation à la sécurité est d'inciter les participants à modifier leur attitude de telle manière qu'ils veuillent eux-mêmes jouer un rôle dans la protection de l'entreprise. Un argument très motivant consiste à leur faire comprendre que leur participation ne profitera pas seulement à l'entreprise, mais aussi à eux-mêmes. Comme l'entreprise dispose d'informations confidentielles sur tous ses salariés, le fait de protéger les informations ou les systèmes de l'entreprise contribue également à protéger les informations personnelles de chacun.

Tout programme de formation à la sécurité nécessite un véritable engagement. Les efforts en ce sens doivent viser toute personne qui a accès à des informations confidentielles ou au système informatique de l'entreprise. La formation doit être continue et son contenu doit être mis à jour en permanence, afin de prendre en compte les changements de personnel et l'apparition de nouvelles menaces et vulnérabilités. Les salariés doivent voir que les dirigeants de l'entreprise s'impliquent, et cette implication doit être réelle : il ne doit pas s'agir d'un simple mémo du type "nous approuvons ces mesures". Enfin, il faut que des moyens suffisants viennent compléter le programme, de façon qu'il puisse être développé, communiqué à tous et testé, et que ses résultats puissent être évalués.

Objectifs

Le premier principe à prendre en compte lors du développement d'un programme de formation et de sensibilisation à la sécurité est que les salariés doivent être amenés à prendre conscience du fait que leur entreprise peut être attaquée à tout moment. Ils doivent apprendre que chaque salarié a un rôle à jouer dans la défense de l'entreprise contre les tentatives de vol d'informations ou d'intrusion dans le système informatique.

Dans la mesure où de nombreux aspects de la sécurité des informations dépendent de la technologie, il est facile de développer une certaine complaisance et d'imaginer que les problèmes seront tous réglés par les pare-feu et autres systèmes de sécurité. La formation doit avoir comme objectif principal de faire prendre conscience à chaque salarié qu'il se trouve en première ligne quand la sécurité de l'entreprise est en jeu.

La formation à la sécurité ne doit pas se limiter à l'énonciation de règles. Le concepteur du programme de formation doit tenir compte du fait que les salariés, lorsqu'ils exécutent leurs tâches quotidiennes sous pression, ont tendance à oublier ou à ignorer leurs responsabilités dans le domaine de la sécurité. La connaissance des tactiques de manipulation et des manières grâce auxquelles on peut s'en défendre est importante, mais elle n'aura d'effet que si la formation met l'accent sur la *motivation* des salariés à mettre leurs connaissances en pratique.

L'entreprise peut considérer qu'un programme a atteint son objectif principal si toutes les personnes formées sont fondamentalement convaincues d'une notion essentielle, à savoir que la sécurité de l'information fait partie de leur travail, et si elles sont motivées pour agir en conséquence.

Les salariés doivent accepter le fait que la menace d'une attaque par un manipulateur est réelle, et que la perte d'informations confidentielles peut représenter une menace pour la survie même de l'entreprise et de ses emplois, ainsi que pour les informations personnelles de chacun. D'une certaine façon, ne pas prendre de précautions vis-à-vis de la sécurité de l'information au travail équivaut à ne pas prendre de précautions vis-à-vis de son propre numéro ou code de carte bancaire. Ce type d'analogie peut d'ailleurs être exploité pour inciter les salariés à respecter les règles de sécurité.

Mise en œuvre du programme de sensibilisation et de formation

Le responsable de la conception du programme d'information sur la sécurité doit être conscient du fait que le projet ne peut s'appliquer de manière identique à toute l'entreprise. La formation doit être adaptée aux besoins précis des différents groupes dans l'entreprise. Bien qu'une grande partie des règles de sécurité décrites au Chapitre 16 puissent s'appliquer à tous les salariés, beaucoup d'autres sont spécifiques. Lors de l'élaboration du programme de formation, il faut au minimum distinguer les groupes suivants : dirigeants, personnel informatique, utilisateurs d'ordinateurs, assistants administratifs, réceptionnistes et standardistes, et agents de sécurité (le Chapitre 16 présente une répartition des règles de sécurité selon les fonctions des salariés).

Dans la mesure où les agents de sécurité d'une entreprise ne sont généralement pas supposés utiliser un ordinateur, et ne sont en contact qu'exceptionnellement et de manière très limitée avec les ordinateurs de l'entreprise, ils ne sont généralement pas pris en compte lors de la conception d'un tel programme de formation. Toutefois, les manipulateurs peuvent inciter un agent de sécurité à les laisser pénétrer dans un bâtiment ou un bureau, ou à

effectuer une action qui aurait pour conséquence une intrusion informatique. Si les membres du personnel de sécurité n'ont pas besoin du même niveau de formation que ceux qui utilisent quotidiennement des ordinateurs, ils ne doivent cependant pas être ignorés lors de l'élaboration du programme de formation.

Dans le monde de l'entreprise, il n'existe probablement que peu de sujets qui concernent tous les salariés et qui soient à la fois aussi importants et aussi peu intéressants *a priori* que la sécurité. Un programme de formation et de sensibilisation bien conçu doit donc viser à informer les participants, mais aussi à les motiver et à susciter leur intérêt.

L'objectif doit être de transformer la formation et la sensibilisation à la sécurité en une expérience distrayante et interactive. Différentes techniques peuvent être mises en œuvre : jeux de rôle montrant les techniques employées par les manipulateurs ; études de comptes rendus médiatiques qui concernent des attaques ayant affecté d'autres entreprises, et discussions sur la manière dont elles auraient pu être évitées ; projection de vidéos sur la sécurité, qui soient à la fois informatives et distrayantes.

Note

Pour les entreprises qui ne disposent pas des moyens de mettre en place en interne un programme de formation à la sécurité, il existe des sociétés de formation proposant leurs services dans ce domaine. Aux États-Unis, le salon Secure World Expo (www.secureworldexpo.com) réunit les principaux prestataires de ce domaine.

Les histoires relatées dans ce livre peuvent également servir de support pour expliquer les méthodes et les tactiques des manipulateurs, pour rendre les participants plus conscients du danger et pour faire la démonstration des vulnérabilités du comportement humain. Vous pourriez envisager d'utiliser ces scénarios comme base pour des jeux de rôle. Ils peuvent aussi servir à lancer des discussions sur la manière dont les victimes auraient dû réagir pour empêcher le succès des attaques.

Les concepteurs de cours et les formateurs constateront que la formation à la sécurité représente un vrai défi, mais qu'il existe aussi de nombreuses possibilités de créer des cours vivants et animés, et donc d'impliquer les participants dans les problèmes de sécurité.

Structure de la formation

La première composante de la sensibilisation à la sécurité doit prendre la forme d'un module de base obligatoire pour tous les salariés. En outre, les nouvelles recrues doivent suivre ce module dès leur arrivée dans l'entreprise. Je conseille d'interdire tout accès aux ordinateurs de l'entreprise tant que cette séance de base n'a pas été effectuée.

La séance de base doit de préférence être assez précise pour retenir l'attention et assez courte pour que les concepts essentiels puissent être mémorisés. La quantité des sujets à aborder justifient bien sûr une formation plus longue, mais les objectifs principaux en l'occurrence sont la motivation et la sensibilisation. Ils seront d'autant mieux atteints que la séance sera courte ; des séances d'une demi-journée, voire d'une journée, risquent de saturer les participants.

Ces séances doivent aider les employés à prendre conscience des dégâts que peuvent subir l'entreprise et chacun des salariés en l'absence de bonnes pratiques en matière de sécurité. Plus que des séances dans lesquelles on donne des informations spécifiques sur les règles à suivre en matière de sécurité, ces séances sont destinés à amener les salariés à accepter qu'ils sont personnellement responsables de la sécurité.

Pour les salariés qui ne peuvent participer directement aux séances, l'entreprise pourra envisager de développer des cours de sensibilisation sur différents supports : vidéos, logiciels, cours en ligne ou manuels.

À la suite de la séance initiale, des séances plus longues doivent être conçues pour informer les salariés sur les vulnérabilités et les techniques d'attaque spécifiques à leur fonction dans l'entreprise. Des cours de recyclage doivent être obligatoires au moins une fois par an. La nature du danger et les méthodes employées pour tromper les gens sont en évolution constante, ce qui implique une mise à jour constante du programme. Par ailleurs, la vigilance des personnes formées a tendance à diminuer avec le temps, ce qui nécessite de réitérer la formation selon une fréquence raisonnable. Là aussi, l'accent doit être mis, non pas tant sur des menaces et des méthodes de manipulation spécifiques que sur l'importance pour les salariés d'appliquer les consignes de sécurité et sur leur motivation.

Les supérieurs hiérarchiques doivent fournir à leurs subordonnés le temps nécessaire pour apprendre les règles et les procédures de sécurité et pour participer au programme de sensibilisation. Il ne faut pas attendre des salariés qu'ils se familiarisent avec les problèmes de sécurité ou qu'ils assistent à des cours pendant leur temps libre. Les nouvelles recrues doivent disposer d'un

temps suffisant pour étudier les règles et les procédures de sécurité avant de commencer à exercer les responsabilités de leur fonction.

Un salarié qui accède pour la première fois à des informations sensibles ou au système informatique, à la suite d'un changement de poste, doit bien sûr suivre une formation complète sur la sécurité conçue spécifiquement pour ses nouvelles fonctions. Ce sera par exemple le cas d'un technicien informatique qui devient administrateur système ou d'un réceptionniste qui devient assistant administratif.

Contenu de la formation

À la base, les attaques des manipulateurs ont toutes un élément en commun : elles trompent leur victime sur la véritable identité de leur interlocuteur. L'assaillant se fera par exemple passer pour un collègue ou une autre personne habilitée à accéder aux informations sensibles, ou autorisée à donner à la victime des instructions concernant l'utilisation d'un équipement informatique. Presque toutes ces attaques peuvent être déjouées si le salarié ciblé procède à deux vérifications simples :

- Vérification de l'identité de l'interlocuteur : celui-ci est-il vraiment celui qu'il prétend être ?
- Vérification des autorisations : l'interlocuteur a-t-il vraiment besoin de ces informations/est-il autorisé à effectuer cette demande ?

Note

La formation à la sécurité n'étant pas infaillible, à chaque fois que c'est possible, reposez-vous sur des mesures faisant appel à la technologie et non sur le personnel de l'entreprise. En d'autres termes, et à titre d'exemple, vous pourriez configurer le système d'exploitation pour éviter tout téléchargement de logiciel à partir d'Internet, ou empêcher la possibilité de choisir des mots de passe courts et faciles à deviner.

Si les séances de sensibilisation pouvaient modifier le comportement des salariés et que ceux-ci appliquent systématiquement les critères ci-dessus lors de toutes les requêtes, le danger que représentent les manipulateurs serait considérablement réduit.

En pratique, un programme de sensibilisation et de formation à la sécurité prenant en compte les comportements humains et les techniques des manipulateurs indiquera :

- Les façons dont les manipulateurs procèdent pour tromper leurs victimes.
- Les méthodes utilisées par les manipulateurs pour atteindre leurs objectifs.
- Comment reconnaître une éventuelle attaque par manipulation.
- La procédure à suivre en cas de requête suspecte.
- À qui signaler les tentatives, réussies ou non, de manipulation.
- L'importance de s'opposer à toute personne qui fait une demande suspecte, quelle que soit la position hiérarchique prétendue de la personne.
- Le fait qu'il faut éviter de faire confiance à quelqu'un sans vérification préalable, même quand la tendance naturelle est de lui donner le bénéfice du doute.
- L'importance de vérifier l'identité d'une personne et le bien-fondé de sa requête (voir "Procédures de vérification et d'autorisation" au Chapitre 16 pour des méthodes de vérification d'identité).
- Des procédures de protection des données sensibles, incluant une familiarité avec un système de classification des données.
- L'indication de l'emplacement "physique" des règles et des procédures de sécurité de l'entreprise, et leur importance quant à la protection des informations et des systèmes informatiques de l'entreprise.
- Un résumé des principales règles de sécurité et une explication de leur signification. Ainsi, chaque salarié devra savoir comment concevoir un mot de passe difficile à casser.
- L'obligation pour chaque salarié de respecter les règles de sécurité, et les sanctions en cas de non-respect.

Par définition, la manipulation implique une interaction humaine quelconque. L'assaillant utilisera très souvent une grande variété de méthodes et de techniques de communication pour atteindre son objectif. Pour cette raison, un programme de sensibilisation bien conçu et complet tentera de couvrir tout ou partie des domaines suivants :

- règles de sécurité en matière de mots de passe d'ordinateur ou de boîtes vocales ;
- procédures pour la communication d'informations sensibles ;
- règles d'utilisation du courrier électronique, y compris des mesures de protection à l'encontre d'attaques de virus, de vers (*worms*) et de chevaux de Troie (*Trojan Horses*) ;

- obligations en matière de sécurité physique, telles que le port du badge ;
- obligation d'exiger le port du badge de la part de toute personne à l'intérieur des locaux ;
- pratiques de sécurité concernant les boîtes vocales ;
- méthodes de classification des informations et mesures de protection des informations sensibles ;
- méthodes de destruction des documents sensibles et des supports informatiques contenant ou ayant contenu par le passé des informations confidentielles.

Par ailleurs, si l'entreprise prévoit de faire réaliser des tests de pénétration pour déterminer l'efficacité de ses défenses contre les tentatives de manipulation, les salariés doivent en être informés. Faites savoir aux salariés qu'à un moment ou à un autre, dans le cadre d'un tel test, ils sont susceptibles de recevoir un appel téléphonique (ou toute autre forme de communication) utilisant les techniques de manipulation à propos desquelles ils ont été formés. Les résultats de ces tests doivent être employés, non pour punir les salariés, mais pour définir les axes des formations supplémentaires à dispenser.

Vous trouverez plus de détails sur tous les points cités plus haut au Chapitre 16.

VÉRIFICATION DES CONNAISSANCES

Il peut être souhaitable de vérifier que les salariés maîtrisent bien les connaissances acquises lors du programme de formation avant de les laisser accéder au système informatique de l'entreprise. Si vous créez des tests en ligne, il existe des logiciels d'évaluation qui permettent d'analyser les résultats des tests et de déterminer les domaines où la formation doit être renforcée.

Vous pourriez également envisager de délivrer un certificat à l'issue d'une formation effectuée avec succès, afin d'encourager et de motiver les salariés.

Nous recommandons de compléter le programme en faisant signer aux salariés un document dans lequel ils s'engagent à respecter les règles et les principes de sécurité qu'ils ont appris. Des études montrent que la probabilité qu'une personne s'efforce à respecter les procédures est plus grande lorsqu'elle signe ce type d'engagement.

SUIVI

La plupart des gens savent que de nouveaux acquis, même quand ils concernent un sujet important, tendent à être progressivement oubliés s'ils ne sont pas renforcés à intervalles réguliers. Dans la mesure où il est essentiel que les salariés soient toujours à jour quant au danger que représentent les manipulateurs, il est essentiel d'effectuer un suivi du programme de formation.

L'un des moyens de s'assurer que les salariés gardent à l'esprit les problèmes de sécurité est de faire en sorte que la sécurité de l'information soit prise en compte par tous les salariés de l'entreprise comme faisant spécifiquement partie de leur travail. Les salariés prennent ainsi conscience qu'ils jouent un rôle crucial dans la sécurité de l'entreprise en général (par défaut, ils pourraient considérer que "ce n'est pas leur rôle").

Alors que la responsabilité générale des programmes de sécurité de l'information repose généralement sur une personne qui fait partie du service de la sécurité ou du service informatique, le développement des programmes de sensibilisation à la sécurité de l'information sera de préférence assuré conjointement avec le service de formation.

Le programme de sensibilisation continue devra être créatif et exploiter tous les supports disponibles pour communiquer les messages de sécurité de telle manière que les salariés gardent en permanence les consignes de sécurité à l'esprit. Tous les supports traditionnels peuvent être utilisés, et il ne faut pas hésiter non plus à exploiter des supports moins traditionnels. Comme dans la publicité classique, l'humour et l'imagination peuvent être d'un grand secours. La formulation des messages doit être variée, de manière à ce qu'ils ne deviennent pas familiers au point d'être ignorés.

Parmi les possibilités exploitables pour un programme de sensibilisation continu, on peut citer :

- La distribution d'un exemplaire de ce livre à chacun des salariés.
- L'insertion d'informations dans la lettre de l'entreprise : articles, encadrés (courts de préférence) ou bandes dessinées, par exemple.
- L'affichage de la photo du salarié du mois pour la sécurité.
- L'accrochage d'affiches dans les zones de repos des salariés.
- L'envoi de brochures imprimées en même temps que le bulletin de paie.
- L'envoi de rappels par e-mail.
- L'utilisation d'économiseurs d'écran rappelant les règles de sécurité.
- La diffusion de messages de sécurité par l'intermédiaire du système de boîtes vocales.

- L'impression d'autocollants pour le téléphone avec des messages tels que "Votre interlocuteur est-il bien la personne qu'il prétend être ?",
- L'affichage au démarrage de l'ordinateur de messages tels que "Si vous envoyez un courrier électronique confidentiel, cryptez-le".
- L'inclusion de la prise en compte des problèmes de sécurité dans la notation ou l'évaluation annuelle des salariés.
- La diffusion *via* l'intranet de rappels quant aux problèmes de sécurité. On pourra par exemple leur donner une forme humoristique pour inciter les salariés à les lire.
- L'utilisation, dans la cafétéria, d'un panneau d'affichage électronique pour rappeler les consignes de sécurité, en changeant fréquemment le message.
- La distribution de brochures.
- L'utilisation de moyens alternatifs : des "fortune cookies", distribués gratuitement à la cafétéria, et qui contiennent un message relatif à la sécurité plutôt qu'une prédiction de l'avenir.

La menace est constante ; par conséquent, les rappels doivent eux aussi être constants.

LE POINT DE VUE DU SALARIÉ

En plus des programmes de sensibilisation et de formation, je conseille aux entreprises de mettre en place un programme de récompenses actif et dont les salariés doivent être bien informés. Vous devez montrer de la reconnaissance envers les salariés qui ont détecté et fait échouer l'attaque d'un manipulateur, ou qui ont d'une manière quelconque contribué au succès du programme de sécurité de l'information.

Inversement, les brèches dans la sécurité doivent également être rendues publiques en interne, de même que les sanctions prévues pour le non-respect des règles de sécurité, que ce soit par négligence ou par paresse. Tout le monde fait des erreurs, mais la violation répétée des procédures de sécurité ne doit pas être tolérée.

Chapitre 16

Les règles de sécurité à appliquer dans l'entreprise

A en croire les résultats d'un sondage mené par le FBI et publié par Associated Press en avril 2002, neuf grandes entreprises et administrations fédérales sur dix auraient fait l'objet d'une attaque informatique. Il est intéressant de constater que seule une entreprise sur trois environ signalait ou reconnaissait publiquement que des attaques avaient eu lieu. Cette réticence est justifiée. Les entreprises cherchent à préserver la confiance de leurs clients et à éviter d'autres attaques de la part d'assaillants qui auraient été informés de leur vulnérabilité. De ce fait, elles restent très discrètes sur les attaques qu'elles subissent.

En réalité, il n'existe pas de statistiques sur les attaques des manipulateurs, et même si on cherchait à en établir, elles seraient très peu fiables parce que, dans la plupart des cas, les entreprises n'ont pas conscience du vol d'informations dont elles sont victimes.

Des mesures de prévention efficaces peuvent être mises en place contre la plupart des types d'attaques des manipulateurs, mais il faut être réaliste : si tous les membres du personnel de l'entreprise ne sont pas convaincus que la sécurité est importante, et qu'ils ne font pas tous l'effort de connaître et de respecter les règles de sécurité, alors les attaques de manipulateurs représenteront toujours un grave danger pour l'entreprise.

En fait, grâce au développement de moyens technologiques efficaces qui permettent de lutter contre les failles de sécurité, les voleurs d'informations auront sans doute de plus en plus souvent recours à la manipulation et à l'exploitation des faiblesses humaines pour accéder à des informations sensibles

ou pénétrer les réseaux d'entreprise. À l'évidence, un espion industriel tentera d'atteindre son objectif en utilisant la méthode la plus facile et où les risques de détection sont les plus faibles. En réalité, une société qui protège ses systèmes informatiques et son réseau à l'aide de technologies dernier cri risque d'être plus vulnérable vis-à-vis d'assaillants qui utilisent des techniques de manipulation pour atteindre leurs objectifs.

Ce chapitre présente des règles conçues pour minimiser les risques qu'encourt une entreprise par rapport aux attaques par manipulation. Ces règles sont faites pour répondre à des attaques qui n'exploitent pas directement des failles technologiques. Elles concernent les méthodes qui consistent, pour les manipulateurs, à faire appel à une ruse ou un prétexte quelconque pour inciter un salarié à leur fournir des renseignements ou à accomplir des tâches qui leur donneront la possibilité d'accéder à des informations confidentielles ou au système informatique de l'entreprise.

COMMENT DÉFINIR DES RÈGLES DE SÉCURITÉ

Les règles de sécurité sont des instructions explicites indiquant aux salariés comment se comporter pour assurer la protection des informations ; elles sont un élément essentiel pour la mise en place d'une protection efficace de l'entreprise. Ces règles ont encore plus d'importance dans le contexte de la détection et de la prévention des attaques de manipulateurs.

La mise en place des mesures de sécurité se fait en formant les salariés aux règles et aux procédures de sécurité. Toutefois, il est important de noter que même si les salariés suivent scrupuleusement ces règles, elles ne représentent pas une garantie absolue contre les attaques des manipulateurs. L'objectif doit être de réduire les risques jusqu'à un niveau acceptable.

Les règles présentées ici comprennent des mesures qui, même si elles n'ont pas toutes un rapport direct avec les techniques des manipulateurs, ont au moins avec celles-ci un rapport indirect. Ainsi, les règles concernant l'ouverture des pièces jointes du courrier électronique, qui peuvent contenir un cheval de Troie, un "troyen", ou un autre logiciel grâce auquel l'assaillant peut prendre le contrôle de l'ordinateur du salarié, permettent de prévenir une technique fréquemment employée par les pirates informatiques.

Les étapes du développement d'un programme

Un programme complet de sécurité de l'information commence généralement par une évaluation des risques qui sert à déterminer :

- quelles informations de l'entreprise doivent être protégées ;
- quelles menaces spécifiques existent à l'encontre de ces informations ;
- quels dommages pourraient être causés à l'entreprise si ces menaces potentielles venaient à se réaliser.

L'objectif principal de l'évaluation des risques consiste à définir quelles informations doivent être protégées en priorité, et si oui ou non la mise en place de mesures de protection peut être rentable au regard d'une analyse coûts-bénéfices. Ou en termes plus simples : quelles informations doivent être protégées en premier, et combien d'argent est-il raisonnable de dépenser pour protéger ces informations ?

Il est essentiel que le personnel dirigeant de l'entreprise soutienne le développement des règles de sécurité et du programme de sécurité de l'information, et qu'il s'y implique. Comme pour tout autre programme d'entreprise, le succès d'un programme de sécurité est conditionné par l'implication personnelle des dirigeants. Les salariés doivent avoir conscience du fait que les cadres dirigeants considèrent eux-mêmes que la sécurité de l'information a une importance capitale pour le fonctionnement de l'entreprise, que la protection des informations de l'entreprise est indispensable pour sa survie et que l'emploi de chacun des salariés peut dépendre de la réussite du programme.

La personne qui aura pour tâche de rédiger les règles de sécurité doit éviter tout jargon technique et utiliser un style pouvant être compris par tous, techniciens et non-techniciens. Il faut aussi que ce document explique pourquoi chacune des règles est importante, sans quoi les salariés les considéreront comme une perte de temps et les ignoreront. Un premier document concernera les règles, et un second les procédures de sécurité : en effet, les règles changeront sans doute beaucoup moins fréquemment que les procédures, puisque celles-ci sont la mise en application des règles.

Par ailleurs, le rédacteur devra connaître les moyens technologiques susceptibles d'aider à mettre en place de bonnes pratiques en matière de sécurité. Ainsi, la plupart des systèmes d'exploitation permettent d'exiger de la part des utilisateurs qu'ils choisissent des mots de passe respectant certaines spécifications, en ce qui concerne leur longueur par exemple. Dans certaines entreprises, il sera possible d'interdire le téléchargement de programmes par l'intermédiaire de paramètres globaux ou locaux des systèmes d'exploitation. Les règles de sécurité doivent imposer l'utilisation de systèmes technologiques de sécurité là où leur présence se justifie financièrement et où ils remplacent avantageusement les décisions humaines.

Il faut que les salariés soient informés des conséquences que peut avoir le non-respect des règles et des procédures. Par ailleurs, un système de récompenses doit être créé pour les salariés qui respectent strictement les consignes de sécurité ou qui font échouer une attaque. Dans ce dernier cas, l'événement et la récompense du salarié pourront être rendus publics, par exemple par l'intermédiaire de la lettre d'information de l'entreprise.

L'un des objectifs du programme de sensibilisation à la sécurité est de faire prendre conscience de l'importance des règles de sécurité et des dommages qui peuvent être causés par un non-respect de ces règles. La nature humaine est ainsi faite qu'occasionnellement, les salariés ignoreront ou contourneront des règles qui semblent dépourvues d'objet ou représenter une perte de temps. C'est au personnel dirigeant de l'entreprise de faire en sorte que les salariés comprennent l'importance de ces règles et soient décidés à les appliquer plutôt que de les considérer comme des obstacles à éviter si possible.

Il est important de noter que les règles de sécurité de l'information ne sont jamais définitives. Au fur et à mesure du développement de l'entreprise, de l'apparition de nouvelles technologies de sécurité et de l'évolution des vulnérabilités, les règles devront être modifiées et complétées. Rendez disponibles à tous les règles et les procédures de sécurité en les diffusant sur l'intranet de l'entreprise ou en les plaçant dans un dossier librement accessible. Vous augmenterez ainsi la probabilité que ces règles soient régulièrement consultées, et vous fournirez aux salariés un moyen d'obtenir une réponse rapide aux questions en rapport avec la sécurité.

Enfin, il est conseillé d'effectuer à intervalles réguliers des tests de pénétration et de vulnérabilité au moyen de différentes techniques de manipulation, afin de mettre à jour des faiblesses éventuelles ou l'absence de prise en compte des règles et des procédures de sécurité. Les salariés devront être prévenus de la mise en œuvre périodique de ces tests avant que ceux-ci soient réalisés.

Comment utiliser ces règles

Les règles détaillées présentées dans ce chapitre ne sont qu'un sous-ensemble des règles de sécurité que je considère comme nécessaires pour éviter tout risque pour l'entreprise. Par conséquent, la liste qui suit ne doit pas être considérée comme exhaustive, mais plutôt comme une base pour la création d'un ensemble de règles adaptées aux besoins spécifiques de votre entreprise.

Les rédacteurs de la charte de sécurité devront choisir les règles en fonction de différents facteurs spécifiques à l'entreprise : environnement, objectifs commerciaux, obligations légales, culture d'entreprise, systèmes informatiques utilisés, etc. Les autres règles pourront être ignorées.

Par ailleurs, dans chaque catégorie, il faudra choisir le degré de rigueur avec lequel les règles seront appliquées. Une petite entreprise dont toutes les activités sont regroupées dans les mêmes locaux et où tous les salariés se connaissent ne craindra pas grand-chose de la part d'un assaillant cherchant à se faire passer pour un salarié de l'entreprise au téléphone (mais il pourra toujours essayer de se faire passer pour l'un de ses fournisseurs). De manière similaire, dans une société où la culture d'entreprise encourage une attitude plus détendue, seule une partie des règles sera adoptée, même si c'est au détriment de la sécurité de l'entreprise.

CLASSIFICATION DES INFORMATIONS

Il est essentiel d'élaborer un système de classification des informations sous forme de catégories qui détermineront dans quelle mesure les informations peuvent être diffusées. Ce système permet de créer un cadre pour la protection des informations de l'entreprise en indiquant à tous les salariés le degré de confidentialité de chaque information.

En l'absence de classification des données (c'est ainsi que fonctionnent la plupart des entreprises aujourd'hui), c'est le salarié qui doit prendre la plus grande partie des décisions quant à leur diffusion. Bien entendu, ces décisions sont prises de manière subjective et non en fonction de facteurs objectifs tels que la confidentialité, l'importance ou la valeur des informations. Par ailleurs, certaines informations sont diffusées parce que le salarié ignore qu'en répondant à une demande d'information, il met peut-être celle-ci dans les mains d'un assaillant.

Le système de classification des données détermine des règles de classement des données selon plusieurs niveaux. En procédant ainsi, les salariés peuvent suivre une série de procédures de traitement des informations qui évitent que des données confidentielles soient diffusées par erreur ou par inadvertance, et qui réduisent le risque que des données confidentielles soient communiquées à une personne non autorisée.

Une formation concernant le système de classification des données doit être dispensée à tous les salariés, y compris à ceux qui n'utilisent habituellement pas les systèmes informatiques ou de communication de l'entreprise. Dans la mesure où chaque membre du personnel a potentiellement accès aux informations de l'entreprise, qu'il fasse partie du personnel de nettoyage ou de surveillance, ou qu'il soit consultant, sous-traitant ou même stagiaire, n'importe qui peut faire l'objet d'une attaque.

La direction de l'entreprise doit définir un *responsable de l'information* qui sera responsable pour toute information employée au sein de l'entreprise. Habituellement, le responsable de l'information est celui qui décide du niveau de classification d'une information donnée, qui réévalue périodiquement les niveaux de classification et qui décide si des changements sont nécessaires ou non. Il peut également déléguer une partie de ses responsabilités à un ou plusieurs autres membres du personnel.

Catégories et définitions pour la classification

Les informations doivent être classées selon différents niveaux en fonction de leur confidentialité. Une fois qu'un système de classification est en place, un changement de méthode de classification coûte cher en temps et en argent. Ici, j'ai choisi quatre niveaux de classification, qui correspondent à la plupart des besoins des entreprises de moyenne et grande taille. En fonction de la quantité et de la nature des informations confidentielles, il pourra être nécessaire d'ajouter des catégories supplémentaires pour des types spécifiques d'informations. Inversement, dans une entreprise de plus petite taille, une classification à trois niveaux pourra être suffisante. Rappelez-vous que plus un système de classification est complexe, plus il représente de frais du point de vue de sa mise en œuvre et de la formation des salariés.

Confidentielles. Il s'agit des informations les plus sensibles. Les informations confidentielles ne doivent pas être diffusées à l'extérieur de l'entreprise ; en général, elles ne seront communiquées qu'à un nombre très limité de personnes, à savoir celles qui doivent en disposer à tout prix. La nature des informations confidentielles est telle que leur diffusion non autorisée pourrait avoir un impact sérieux sur l'entreprise, ses actionnaires, ses partenaires commerciaux et ses clients. Les informations confidentielles font généralement partie de l'une des trois catégories suivantes :

- informations concernant des secrets commerciaux, du code source propriétaire, des spécifications techniques ou toute information sur un produit qui pourrait représenter un avantage pour des concurrents ;
- informations commerciales et financières non publiques ;
- tout autre type d'informations essentielles pour le fonctionnement de l'entreprise, par exemple les stratégies commerciales futures.

Privées. Ce sont les informations de nature personnelle qui ne sont destinées à être employées qu'à l'intérieur de l'entreprise. La diffusion non autorisée d'informations privées peut avoir un impact sérieux sur les salariés, voire sur l'entreprise si ces informations devaient parvenir entre des mains malintentionnées (manipulateurs, en particulier). Parmi les informations privées, on peut citer les données de comptes bancaires, de salaires ou toute autre information personnelle qui n'est pas destinée à être rendue publique.

Internes. Ces informations peuvent être diffusées librement auprès du personnel de l'entreprise. En principe, la diffusion non autorisée d'informations internes n'est pas susceptible de nuire à l'entreprise, ses actionnaires, ses partenaires commerciaux, ses clients ou ses salariés. Toutefois, un manipulateur sera susceptible d'exploiter ce type d'information pour se faire passer pour un salarié, un fournisseur ou un sous-traitant de l'entreprise et obtenir un accès non autorisé au système informatique de l'entreprise.

Un accord de confidentialité doit être signé avant que des informations internes soient communiquées à des tiers, qu'il s'agisse des salariés d'un fournisseur, d'un sous-traitant, ou d'un partenaire commercial, par exemple. Les informations internes comprennent les informations qui font partie du quotidien de l'entreprise et qui ne doivent pas être communiquées à l'extérieur : organigramme de l'entreprise, numéros de téléphone pour la connexion à distance, noms internes des ordinateurs, procédures d'accès distant, codes des centres de facturation, etc.

Note

La catégorie "interne" est souvent nommée "sensible" par les spécialistes de la sécurité. J'ai choisi le terme "interne" parce qu'il définit mieux l'audience visée. J'utilise le terme "sensible" pour me référer indifféremment aux informations confidentielles, privées ou internes, en bref toutes les informations qui ne sont pas spécifiquement désignées comme "publiques".

Publiques. Il s'agit des informations spécifiquement conçues pour être diffusées auprès du public. Ce type d'informations peuvent être librement publiées, que ce soit sous forme de communiqués de presse, de renseignements fournis par le service technique ou de brochures publicitaires. Notez que toute information non spécifiquement définie comme publique doit être considérée comme sensible.

Terminologie de l'information classifiée

En fonction de leur classification, les informations ne doivent être distribuées qu'à certaines catégories de personnes. Dans le reste de ce chapitre, nous

nommerons *personne non vérifiée* une personne que le salarié ne connaît pas personnellement, ni en tant que salarié actif, ni en tant que salarié ayant le droit d'accéder aux informations demandées, ni en tant que salarié pour lequel un tiers s'est porté garant.

Une *personne de confiance* est une personne que le salarié connaît de vue en tant que collègue, client ou consultant de l'entreprise et qui a le droit d'accéder aux informations demandées. Une personne de confiance peut être un salarié d'une entreprise "amie" : fournisseur, sous-traitant ou partenaire commercial ayant signé avec l'entreprise un accord de confidentialité.

Une personne de confiance peut se *porter garante* d'un tiers en ce qui concerne son droit à accéder à des informations données. Dans certains cas, les règles de sécurité peuvent exiger au préalable que la personne de confiance soit toujours salariée par l'entreprise avant d'accepter une demande d'informations pour laquelle la personne de confiance se porte garante.

Un *compte privilégié* est un compte, d'ordinateur ou autre, qui nécessite des autorisations plus étendues que celles d'un compte d'utilisateur de base. Ce sera par exemple un compte d'administrateur, grâce auquel on peut modifier les privilèges d'utilisateur et utiliser différentes fonctions système.

Une *boîte vocale générique* est une boîte vocale qui répond aux appels avec un message générique pour l'ensemble du service. Ce type de boîte vocale est employé pour protéger les noms et les extensions de numéros de téléphone des salariés d'un service donné.

PROCÉDURES DE VÉRIFICATION ET D'AUTORISATION

Pour voler des informations, le manipulateur se fait souvent passer pour un salarié, un fournisseur, un sous-traitant ou un partenaire commercial de l'entreprise. Pour assurer la sécurité des informations, un salarié à qui on demande de fournir une information ou d'exécuter une action doit, avant de satisfaire à la requête, identifier son interlocuteur de manière sûre et vérifier que celui-ci a le droit d'obtenir les informations qu'il requiert.

Demandes provenant de personnes de confiance

Lorsqu'une personne de confiance demande qu'on lui fournisse un renseignement ou qu'on accomplisse une tâche, il peut être nécessaire de vérifier :

- Que la personne est bien salariée par l'entreprise, ou que le lien qui existe entre l'entreprise et la personne justifie l'accès au type d'information demandé. Cela permet d'éviter que des salariés licenciés ou que des clients, des fournisseurs, des sous-traitants, etc., qui n'ont plus de rapports commerciaux avec l'entreprise puissent se faire passer pour du personnel autorisé.
- Que la personne a besoin de connaître les informations demandées, et qu'elle est autorisée à y accéder ou à requérir telle ou telle action.

Demandes provenant de "personnes non vérifiées"

Quand une requête provient d'une personne non vérifiée, il faut suivre une procédure d'identification scrupuleuse afin d'identifier de manière sûre la personne comme étant habilitée à obtenir les informations demandées, en particulier quand la requête est en rapport avec les ordinateurs ou tout autre type de système informatique. Cette procédure est fondamentale pour contrer les tentatives de manipulation ; si elle est systématiquement observée, la menace que représentent les attaques des manipulateurs sera très fortement réduite.

Toutefois, il faut veiller à ce que cette procédure ne soit pas complexe au point de provoquer des coûts excessifs ou d'être dissuasive pour les salariés.

La procédure de vérification, qui est détaillée ci-après, consiste à vérifier :

- que la personne est bien celle qu'elle prétend être ;
- qu'elle est actuellement salariée par l'entreprise, ou par un partenaire commercial de l'entreprise ;
- qu'elle est habilitée à obtenir les informations demandées, ou qu'elle est en droit d'exiger que l'on accomplisse la tâche qu'elle sollicite.

Première étape : vérification de l'identité

La liste ci-après décrit différentes méthodes d'identification, classées par ordre croissant d'efficacité. J'indique également les faiblesses de chaque méthode, c'est-à-dire le ou les moyens que peut utiliser un manipulateur pour tromper un salarié qui fait appel à cette méthode.

1. **Identification de l'appelant** (si les téléphones de l'entreprise disposent de cette fonction). L'affichage du téléphone permet de déterminer si l'appel vient de l'intérieur ou de l'extérieur de l'entreprise, et si le nom ou le numéro de téléphone affiché correspond à celui de l'interlocuteur.

   Faiblesse. Les informations d'identification de l'appelant peuvent, dans certains cas, être falsifiées par toute personne ayant accès à un PABX (central téléphonique) connecté au réseau téléphonique.

2. **Rappel de la personne.** Le salarié vérifie dans l'annuaire de l'entreprise que la personne en fait partie, et rappelle son interlocuteur en composant l'extension indiquée dans l'annuaire.

   Faiblesse. Un assaillant qui dispose de connaissances suffisantes peut faire effectuer un transfert d'appel de telle manière que l'appel réalisé ensuite par le salarié soit automatiquement transféré sur le téléphone (extérieur) de l'assaillant.

3. **Garantie.** Une personne de confiance qui se porte garante de l'identité de l'appelant vérifie l'identité de l'appelant.

   Faiblesse. Les assaillants parviennent souvent à convaincre un autre salarié de leur identité et à l'inciter à se porter garant pour eux.

4. **Secret commun.** Utilisation d'un secret spécifique à l'entreprise, mot de passe ou code, par exemple.

   Faiblesse. Si de nombreuses personnes connaissent ce secret, il sera facile pour l'assaillant de le découvrir.

5. **Supérieur hiérarchique du salarié.** Appel auprès du supérieur hiérarchique de l'interlocuteur afin de vérifier l'identité de ce dernier.

   Faiblesse. Si l'appelant fournit lui-même le numéro de téléphone de son supérieur hiérarchique, l'interlocuteur du salarié pourra être non pas le véritable supérieur hiérarchique, mais un complice de l'assaillant.

6. **Courrier électronique signé numériquement.** Le courrier électronique est signé numériquement par une personne de confiance.

   Faiblesse. Si l'assaillant a réussi au préalable à s'introduire dans l'ordinateur d'un salarié et à y installer un logiciel d'enregistrement des touches saisies, il pourra envoyer un e-mail signé numériquement qui semblera provenir d'une personne de confiance.

7. **Reconnaissance de la voix de l'interlocuteur.** La personne à qui s'adresse la demande a déjà été en contact avec son interlocuteur, de préférence en face à face ; elle sait que son interlocuteur est une personne de confiance et le connaît assez bien pour être en mesure de reconnaître sa voix au téléphone.

   Faiblesse. Cette méthode est sûre et il n'existe pas pour le manipulateur de moyen simple de la contourner. Toutefois, elle n'est utile que lorsque la personne à qui est faite la demande connaît son interlocuteur.

8. **Mot de passe dynamique.** La personne qui formule la requête s'identifie par l'intermédiaire d'un système de mot de passe dynamique tel que celui proposé par ActivCard, une société spécialisée dans les produits de gestion et d'authentification d'identités.

   Faiblesse. Pour contourner cette protection, il faudrait que l'assaillant obtienne un support d'identification (appareil ou carte à puce) ainsi que le code PIN du salarié auquel appartient ce support ; il pourrait également essayer d'inciter le salarié à fournir les informations affichées sur le support ainsi que son code PIN.

9. **En personne, avec un support de vérification d'identité.** Le manipulateur se présente en personne et fournit un badge de l'entreprise ou tout autre moyen d'identification sûr, de préférence muni d'une photo.

   Faiblesse. Les manipulateurs parviennent souvent à voler des badges ou à en créer de faux ; toutefois, ils évitent généralement cette approche parce qu'ils s'exposent ainsi à être identifiés et appréhendés.

Deuxième étape : vérification du statut actuel de l'interlocuteur

La principale menace, en ce qui concerne l'information, ne vient pas du manipulateur professionnel, ni du pirate informatique expérimenté, mais de bien plus près : il s'agit du salarié à peine licencié qui veut se venger ou qui espère monter sa propre affaire à l'aide d'informations volées à l'entreprise. Notez qu'une version modifiée de cette procédure peut servir à vérifier qu'une personne est toujours en relation commerciale avec l'entreprise, qu'il s'agisse d'un fournisseur, d'un consultant ou d'un sous-traitant (entre autres).

Avant de fournir des informations sensibles à quelqu'un ou de suivre ses instructions lorsqu'il demande d'exécuter une opération quelconque sur du matériel informatique, vérifiez que l'individu est toujours salarié de l'entreprise en utilisant l'une des méthodes suivantes :

Annuaire de l'entreprise. Si l'entreprise dispose d'un annuaire en ligne des salariés et qu'il est fréquemment mis à jour, il est possible d'y vérifier que la personne fait toujours partie de l'entreprise.

Vérification auprès du supérieur hiérarchique de la personne. L'appel auprès du supérieur hiérarchique doit se faire à l'aide du numéro indiqué dans l'annuaire de l'entreprise, et non avec celui fourni par le correspondant.

Vérification auprès du service de la personne. Un appel auprès du service de l'interlocuteur permet de déterminer si la personne fait effectivement encore partie de l'entreprise.

Troisième étape : vérification de l'habilitation à obtenir les informations demandées

Dernier point à vérifier : la personne doit être habilitée à obtenir les informations qu'elle demande, ou à faire effectuer sur les systèmes informatiques les actions demandées.

Pour vérifier cette habilitation, plusieurs méthodes peuvent être employées :

Vérification par l'intermédiaire de la liste des fonctions, des services ou des responsabilités. L'entreprise peut définir des listes indiquant quelles informations peuvent être communiquées à quels salariés. Ces listes peuvent être organisées par fonction ou poste, par service, par responsabilité ou selon une combinaison de ces éléments. De telles listes doivent être placées en ligne pour pouvoir être fréquemment actualisées et rapidement accessibles. Généralement, la création et la gestion de ces listes seront confiées aux responsables de l'information.

Note

La simple existence de telles listes peut être une aubaine pour un manipulateur. Si un assaillant apprend l'existence de listes de ce type au sein de l'entreprise visée, il cherchera probablement à l'obtenir par tous les moyens. Une fois dans ses mains, une telle liste peut lui ouvrir de nombreuses portes et compromettre sérieusement la sécurité de l'entreprise.

Autorisation d'un supérieur hiérarchique. Le salarié contacte son supérieur hiérarchique ou celui de la personne qui a formulé une demande, pour obtenir l'autorisation de répondre à cette requête.

Autorisation du responsable de l'information ou de l'un de ses délégués. Le responsable de l'information est celui qui décide en dernier recours si, oui ou non, la demande d'une personne peut être satisfaite. Dans le cas d'une vérification informatique, la procédure consiste, pour le salarié, à contacter son supérieur hiérarchique immédiat afin d'obtenir l'autorisation de répondre à la demande, autorisation basée sur le profil du poste du correspondant. Si ce profil est inexistant, le supérieur hiérarchique doit contacter le responsable de l'information approprié pour obtenir son autorisation. Cette chaîne de commandement doit être respectée afin que les responsables de l'information ne soient pas submergés de demandes.

Autorisation à l'aide d'un logiciel spécifique. Pour une grande entreprise dont le domaine d'activité est très concurrentiel, il peut être utile de développer un logiciel propriétaire fournissant aux salariés les informations nécessaires. Ce logiciel serait une base de données comprenant les noms des salariés et les privilèges d'accès aux informations sensibles. Les utilisateurs ne pourraient pas consulter les droits d'accès de chacun, mais à chaque requête, ils pourraient saisir le nom de la personne qui formule la demande et le code d'identification correspondant au type d'information demandé. Le logiciel répondrait ensuite en autorisant ou en refusant la requête. En suivant cette méthode, on évite le risque que représente une liste des salariés qui indique l'habilitation de chacun à accéder aux informations confidentielles, privées ou internes, liste qui peut être subtilisée.

RÈGLES CONCERNANT LE PERSONNEL DIRIGEANT

Les règles qui suivent concernent les cadres et le personnel dirigeant de l'entreprise. Elles sont divisées en quatre catégories : classification de l'information, diffusion de l'information, utilisation du téléphone et règles diverses. Les catégories et les règles sont numérotées pour faciliter l'identification de chacune des règles.

Règles de classification de l'information

Cette catégorie de règle définit la manière dont l'entreprise classe la sensibilité des informations et détermine qui a accès aux différents niveaux d'information.

1-1 Définition de la classification des informations

Règle. Toute information de valeur, confidentielle ou essentielle pour le fonctionnement de l'entreprise, doit être classifiée dans l'une des catégories prédéfinies par le responsable des informations correspondant ou l'un de ses délégués.

Notes/explication. Le responsable des informations ou l'un de ses délégués affecte un niveau de classification à tout type d'information couramment employé pour le fonctionnement de l'entreprise. Le responsable détermine également qui est habilité à accéder à ces informations et comment elles peuvent être utilisées. Il peut réévaluer sa classification à tout moment et définir un délai à partir duquel un type d'information change automatiquement de classification.

Les informations confidentielles sous forme électronique (fichiers informatiques, e-mails) peuvent être communiquées :

- Dans le corps d'un message électronique crypté.
- En tant que pièce cryptée jointe à un message électronique.
- Par transfert électronique vers un serveur faisant partie du réseau interne de l'entreprise.
- Par fax à partir d'un ordinateur, à condition que seul le destinataire prévu utilise la machine de destination ou qu'il se trouve à côté de la machine de destination lors de l'expédition du fax. Il est également possible d'envoyer un fax en l'absence de son destinataire, à condition de faire appel à une transmission cryptée et, pour la réception, d'utiliser un serveur de fax protégé par mot de passe.

Les discussions concernant les informations confidentielles peuvent être conduites en face à face, par téléphone à l'intérieur de l'entreprise, par téléphone crypté à l'extérieur de l'entreprise, par transmission satellite cryptée, par visioconférence cryptée et par Voix sur IP (VoIP) cryptée.

Pour une transmission par fax, la méthode recommandée consiste à envoyer la première page du fax ; le destinataire accuse réception de la page en envoyant lui-même une page par fax, prouvant ainsi qu'il se trouve à proximité de l'appareil. L'expéditeur envoie ensuite le reste du fax.

Les moyens de communication suivants ne doivent pas être employés pour s'échanger des informations confidentielles ou les diffuser : courrier électronique non crypté, message de boîte vocale, courrier normal ou toute méthode de communication sans fil (GMS, SMS, téléphone fixe sans fil).

2-4 Communication d'informations privées

Règle. Les informations "privées", c'est-à-dire les informations concernant les salariés et qui, si elles étaient rendues publiques, pourraient nuire au personnel de l'entreprise, ne peuvent être communiquées qu'à des personnes de confiance habilitées à les obtenir.

Notes/explication. Les informations privées qui ont un support physique (document imprimé ou support informatique amovible) peuvent être communiquées :

- en personne, en face à face ;
- par courrier interne scellé et marqué avec le niveau de classification "Privé" ;
- par courrier normal.

Les informations privées sous forme électronique (fichiers d'ordinateur, e-mails) peuvent être communiquées :

- Par courrier électronique à l'intérieur de l'entreprise.
- Par transfert électronique vers un serveur faisant partie du réseau interne de l'entreprise.
- Par fax, à condition que seul le destinataire prévu utilise la machine de destination ou qu'il se trouve à côté de la machine de destination lors de l'expédition du fax. Il est également possible de l'envoyer à destination d'un serveur de fax protégé par mot de passe.

Les discussions concernant les informations privées peuvent être conduites en face à face, par téléphone, par transmission satellite, par visioconférence, et par Voix sur IP cryptée.

Les moyens de communication suivants ne doivent pas être employés pour s'échanger des informations privées ou les diffuser : courrier électronique non crypté et message de boîte vocale.

2-5 Communication d'informations internes

Règle. Les informations internes ne doivent être communiquées qu'au personnel de l'entreprise ou à des personnes de confiance ayant signé un accord de confidentialité. Il est nécessaire d'établir des règles pour la diffusion des informations internes.

Notes/explication. Les informations internes peuvent être diffusées sous n'importe quelle forme à l'intérieur de l'entreprise ; pour une diffusion à l'extérieur de l'entreprise sous forme de courrier électronique, celui-ci doit être crypté.

2-6 Conversations téléphoniques traitant de sujets sensibles

Règle. Avant de communiquer par téléphone quelque information que ce soit autre que celles de type public, le salarié doit reconnaître personnellement la voix de son interlocuteur grâce aux contacts antérieurs qu'il a eus avec celui-ci, ou le système téléphonique de l'entreprise doit identifier l'appel comme venant d'un numéro interne qui a été affecté à l'appelant.

Notes/explication. Si la voix de l'interlocuteur n'est pas reconnue, le numéro interne de celui-ci peut être appelé pour vérifier que la voix du message de la boîte vocale correspond bien à la voix de l'appelant ; il est également possible d'appeler le supérieur hiérarchique de la personne pour vérifier l'identité et l'habilitation de cette dernière.

2-7 Procédures concernant le personnel d'accueil

Règle. Le personnel d'accueil (à l'entrée des locaux) doit demander un moyen d'identification comprenant une photo avant de remettre quelque document ou paquet que ce soit à une personne qui n'est pas un salarié actif de l'entreprise. Le nom, le numéro de la pièce d'identité, la date de naissance, la nature de l'objet remis et la date et l'heure de la remise doivent être consignés.

Notes/explication. Cette règle s'applique aussi à tout objet remis à un service de courrier tel que Chronopost, EMS Taxipost, UPS, etc.

2-8 Transfert de logiciels à des tiers

Règle. Avant tout transfert ou communication de logiciel, programme ou code informatique, l'identité de la personne qui en a fait la demande doit être établie de manière sûre, ainsi que son habilitation à obtenir le logiciel. En général, le code source développé par une entreprise est considéré comme une information très importante, et il est donc classifié comme confidentiel.

Notes/explication. L'habilitation est généralement déterminée par le fait que l'interlocuteur a besoin ou non d'accéder au logiciel pour accomplir son travail.

2-9 Habilitation des contacts et prospects

Règle. Le personnel des ventes et du marketing doit vérifier l'identité réelle de ses contacts et prospects avant de leur fournir des numéros de téléphone internes, les plans de produits ou d'autres informations sensibles.

Notes/explication. Une tactique courante des espions industriels consiste à contacter un commercial et à lui faire croire qu'il est susceptible d'effectuer un achat important. Afin de ne pas manquer la vente, le commercial sera enclin à lui fournir des renseignements qui pourront être employés par l'espion pour accéder par la suite à des informations confidentielles.

2-10 Transfert de fichiers et de données

Règle. Les fichiers et autres données électroniques ne doivent pas être transférés sur un support amovible, à moins que la demande ne provienne d'une personne de confiance dont l'identité a été vérifiée et qui a besoin des données dans ce format.

Notes/explication. Un manipulateur parviendra facilement à abuser un salarié en lui fournissant un prétexte plausible de la raison pour laquelle il a besoin qu'on lui copie des informations sensibles sur une disquette Zip, une bande ou un CD-ROM, et qu'on mette ensuite ce support à sa disposition à l'entrée de l'entreprise où il pourra le retirer.

Utilisation du téléphone

Les règles d'utilisation du téléphone permettent de s'assurer que les salariés peuvent vérifier l'identité de leurs interlocuteurs et protéger leurs propres informations des appels extérieurs à l'entreprise.

3-1 Transferts d'appels

Règle. Aucun transfert d'appel vers un numéro de téléphone extérieur n'est autorisé dans l'entreprise pour les lignes de fax ou d'accès à distance au réseau de l'entreprise.

Notes/explication. Un assaillant déterminé pourra tenter de tromper le personnel de l'opérateur téléphonique ou du service interne des télécommunications et obtenir le transfert d'une ligne de téléphone interne vers une ligne externe contrôlée par l'assaillant. Celui-ci pourra ainsi intercepter des fax, demander que des informations confidentielles soient faxées vers le numéro qu'il contrôle (mais qui sera considéré comme sûr par le personnel de l'entreprise) ou obtenir le nom d'utilisateur et le mot de passe du compte d'un salarié en lui faisant accéder à distance à un ordinateur que l'assaillant contrôle, et qui simule le processus d'ouverture d'une session.

Suivant les services de téléphonie employés par l'entreprise, la fonction de transfert d'appel pourra se trouver sous la responsabilité de l'opérateur téléphonique et non du service des télécommunications de l'entreprise. Dans ce cas, on demandera à l'opérateur téléphonique de refuser la mise en place d'un transfert d'appel pour les lignes de téléphone utilisées pour le fax et l'accès à distance.

3-2 Identification de l'appelant

Règle. Le système téléphonique de l'entreprise ou son opérateur doivent fournir une identification de l'appelant pour tous les postes téléphoniques internes, et si possible générer une sonnerie différente selon que l'appel est interne ou externe. Par ailleurs, en cas d'utilisation d'un central téléphonique (PABX), celui-ci doit être configuré de manière à assurer le plus haut niveau de sécurité en ce qui concerne l'identification de l'appelant pour les appels externes.

Notes/explication. La vérification de l'origine des appels extérieurs peut permettre de faire échouer une attaque ou d'identifier l'appelant.

3-3 Téléphones à accès libre

Règle. Pour éviter qu'un visiteur puisse se faire passer pour un salarié de l'entreprise, les appels en provenance de téléphones à accès libre situés à l'intérieur de l'entreprise seront clairement identifiés comme tels ("Accueil", par exemple).

Notes/explication. Si l'identification de l'appelant se présente simplement comme un numéro d'extension, des mesures de sécurité appropriées doivent être prises en ce qui concerne les appareils mis à la disposition du public et situés à l'intérieur de l'entreprise. Il ne doit pas être possible pour un assaillant de téléphoner à partir de l'un de ces appareils et de faire croire à son interlocuteur qu'il utilise le téléphone de l'un de ses collègues.

3-4 Mots de passe par défaut des systèmes téléphoniques

Règle. Le responsable des boîtes vocales doit modifier tous les mots de passe par défaut du système téléphonique avant que celui-ci soit utilisé par le personnel de l'entreprise.

Notes/explication. Les manipulateurs sont susceptibles d'obtenir une liste des mots de passe par défaut employés par les fabricants et de les utiliser pour accéder à des comptes administrateur.

3-5 Boîtes vocales

Règle. Une boîte vocale générique doit être mise en place pour chacun des services de l'entreprise en contact avec le public.

Notes/explication. La première étape de la manipulation consiste à obtenir des informations sur l'entreprise ciblée et son personnel. Plus l'accès aux noms et aux numéros de téléphone des salariés est difficile, moins un manipulateur sera susceptible d'identifier des cibles potentielles dans l'entreprise ou de se faire passer pour l'un de ses salariés.

3-6 Vérification de l'identité des prestataires de services téléphoniques

Règle. Aucun technicien extérieur ne peut être autorisé à intervenir à distance sur le système téléphonique de l'entreprise sans avoir été préalablement identifié de manière sûre et autorisé à intervenir.

Notes/explication. Les pirates informatiques qui parviennent à accéder au système téléphonique de l'entreprise peuvent ensuite créer des boîtes vocales, intercepter des messages destinés à d'autres utilisateurs ou passer des appels gratuits aux frais de l'entreprise.

3-7 Configuration du système téléphonique

Règle. Le responsable des boîtes vocales en assure la sécurité en configurant de manière appropriée le système téléphonique.

Notes/explication. En ce qui concerne les boîtes vocales, le système téléphonique peut être configuré de manière plus ou moins sûre. Le responsable des boîtes vocales doit être conscient des questions de sécurité et coopérer avec les responsables de la sécurité pour configurer le système téléphonique afin de protéger les données sensibles.

3-8 Traçage des appels

Règle. Si les prestations proposées par l'opérateur téléphonique le permettent, un système de traçage des appels sera mis en place pour toute l'entreprise, afin qu'il soit possible, en cas d'appel suspect, de retrouver l'origine de l'appel.

Notes/explication. Il faut apprendre aux salariés à utiliser le traçage d'appels et à savoir dans quelles circonstances il doit être employé. Ce sera par exemple le cas lorsque la personne qui appelle tente d'obtenir un accès non autorisé aux systèmes informatiques de l'entreprise ou demande des informations confidentielles. Lorsqu'un salarié active la fonction de traçage d'appels, les responsables de la sécurité doivent immédiatement en être informés.

3-9 Systèmes téléphoniques automatiques

Règle. Si l'entreprise dispose d'un système téléphonique transférant automatiquement les appels vers le service ou le poste demandé, il doit être programmé de telle manière que les extensions téléphoniques n'apparaissent pas lors du transfert de l'appel.

Notes/explication. Un assaillant peut utiliser le système téléphonique automatique d'une entreprise pour retrouver les numéros de téléphone de chacun des salariés. Ces connaissances peuvent ensuite lui servir à convaincre ses interlocuteurs qu'il fait partie de l'entreprise et qu'il est habilité à obtenir des informations sensibles.

3-10 Désactivation des boîtes vocales après plusieurs tentatives d'accès infructueuses

Règle. Le système téléphonique de l'entreprise doit être programmé de manière à verrouiller un compte de boîte vocale dès lors qu'un certain nombre de tentatives d'accès infructueuses ont eu lieu.

Notes/explication. Le responsable des télécommunications doit faire en sorte qu'une boîte vocale se verrouille automatiquement après cinq tentatives d'accès infructueuses. Les boîtes vocales verrouillées doivent être déverrouillées manuellement par le responsable.

3-11 Restriction de l'accès à certains numéros

Règle. Les numéros de téléphone internes de services qui, en principe, ne reçoivent pas d'appels de l'extérieur (assistance technique interne, salle des ordinateurs, etc.) doivent être programmés de manière à ne pouvoir être appelés que de l'intérieur de l'entreprise. Une autre solution consiste à les protéger par mot de passe ; ainsi, les personnes autorisées à téléphoner de l'extérieur doivent fournir un mot de passe pour pouvoir effectuer un appel entrant.

Notes/explication. Cette règle empêchera la plupart des manipulateurs amateurs d'entrer en contact avec leur cible. Toutefois, un assaillant déterminé parviendra parfois à convaincre un salarié de l'entreprise d'appeler un numéro à accès restreint, l'utilisateur de ce numéro rappelant ensuite l'assaillant. Il pourra aussi convaincre un salarié d'activer une conversation à trois en incluant le numéro à accès restreint. Lors de la formation à la sécurité, ces subterfuges doivent être évoqués afin que les salariés en aient connaissance.

Règles diverses

4-1 Conception des badges des salariés

Règle. Les badges doivent comprendre une grande photo que l'on peut reconnaître de loin.

Notes/explication. Si elles sont standard, les photos des badges d'entreprise sont d'une utilité très limitée en ce qui concerne la sécurité. La distance entre la personne qui entre dans le bâtiment et l'agent de sécurité (ou le réceptionniste) qui a pour charge de vérifier les identités est généralement trop grande pour qu'une petite photo sur un badge lui soit d'une aide quelconque. Pour que la personne soit identifiable d'après sa photo, celle-ci doit être assez grande, et le badge doit être modifié en conséquence.

4-2 Mise à jour des droits d'accès lors d'un changement de poste ou de responsabilités

Règle. Lorsqu'un salarié change de poste ou que ses responsabilités augmentent ou diminuent, le supérieur hiérarchique du salarié doit en informer le service informatique afin que le profil de sécurité de la personne soit modifié en conséquence.

Notes/explication. La gestion des droits d'accès du personnel est indispensable pour limiter la diffusion d'informations sensibles. La règle qui s'applique est celle du *plus petit privilège*. Les droits d'accès attribués aux utilisateurs sont aussi réduits que possible mais doivent leur permettre d'accomplir correctement leurs tâches. Il faut que toute demande de modification qui doit aboutir à des droits d'accès de niveau plus élevé respecte les règles établies en la matière.

Le supérieur hiérarchique du salarié ou le service des ressources humaines a la responsabilité d'informer le service informatique de la modification des droits de l'utilisateur.

4-3 Identification du personnel extérieur à l'entreprise

Règle. L'entreprise doit fournir un badge spécial comprenant une photo à tout le personnel ne qui ne fait pas partie de l'entreprise mais qui doit fréquemment pénétrer dans les locaux.

Notes/explication. Le personnel qui entre fréquemment dans l'entreprise sans en faire partie (pour effectuer des livraisons à la cafétéria, réparer des photocopieuses ou installer des téléphones, par exemple) peut représenter une menace. En plus de diffuser des badges, il est nécessaire d'apprendre aux salariés de l'entreprise à repérer les visiteurs dépourvus de badges et à réagir en conséquence.

4-4 Désactivation des comptes des sous-traitants

Règle. Quand un sous-traitant ou un consultant auquel a été attribué un compte d'utilisateur a terminé sa mission ou quand son contrat expire, le responsable du sous-traitant dans l'entreprise doit immédiatement en informer le service informatique afin que tous ses comptes soient désactivés, y compris les comptes utilisés pour les accès aux bases de données, l'accès à distance ou l'accès par Internet.

Notes/explication. Lorsque le contrat d'un sous-traitant ou d'un consultant extérieur expire, il existe toujours le risque qu'il utilise ses connaissances des systèmes informatiques et des procédures de l'entreprise pour accéder à des informations sensibles. Tous les comptes d'utilisateur que le sous-traitant utilisait ou dont il avait connaissance doivent être désactivés ou supprimés.

4-5 Comptes rendus d'incidents

Règle. L'entreprise doit mettre en place un groupe ou désigner au moins une personne auxquels seront signalés tous les incidents de sécurité, et qui auront pour mission de diffuser les informations concernant les alertes de sécurité en cours.

Notes/explication. La centralisation des comptes rendus d'incidents de sécurité supposés offre la possibilité de détecter des attaques qui, autrement, seraient passées inaperçues. Si des attaques systématiques portant sur l'ensemble de l'entreprise sont identifiées et signalées, la cible des attaques peut parfois être déterminée, et l'on peut prendre des mesures pour protéger en particulier les informations concernées.

Les salariés auxquels sont signalés les incidents doivent être familiarisés avec les méthodes et tactiques des manipulateurs afin qu'ils puissent évaluer les rapports qui leur sont faits et qu'ils puissent reconnaître une attaque en cours.

4-6 Numéro de téléphone pour le compte rendu d'incidents

Règle. L'entreprise doit mettre en place un numéro de téléphone spécial pour de joindre le groupe ou la personne auxquels sont signalés les incidents de sécurité. Il s'agira de préférence d'une extension facile à retenir.

Notes/explication. Lorsqu'un salarié a l'impression d'être victime d'une manipulation, il doit avoir la possibilité d'alerter immédiatement la personne ou le groupe responsable des informations sur les incidents de sécurité. Pour que cette alerte soit rapide, tous les opérateurs téléphoniques et tous les réceptionnistes de l'entreprise doivent pouvoir accéder immédiatement à ce numéro, et il doit être largement diffusé dans l'entreprise.

Un système d'alerte précoce peut contribuer de manière significative à la détection des attaques qui visent l'entreprise et à une réaction rapide face à ces attaques. On doit avoir suffisamment bien formé les salariés pour qu'ils utilisent le numéro de téléphone spécial dès lors qu'ils ont l'impression d'avoir été la cible d'une manipulation. Conformément à des procédures préétablies, le ou les responsables des informations sur les incidents de sécurité doivent immédiatement signaler aux groupes visés qu'une attaque pourrait être en cours, afin que le personnel soit sur ses gardes.

4-7 Sécurisation des zones sensibles

Règle. L'entrée des zones sensibles doit être gardée par un agent de sécurité, et deux formes d'authentification seront demandées.

Notes/explication. L'une des formes d'authentification acceptables est un verrou électronique qui s'ouvre quand le salarié passe son badge dans un appareil et entre un code d'accès. Le meilleur moyen de sécuriser une zone est de poster à son entrée un agent de sécurité qui surveille le déroulement de l'authentification. Dans les entreprises où le coût d'un agent de sécurité supplémentaire serait trop élevé, deux formes d'authentification doivent être employées pour permettre l'entrée. En fonction des risques et du coût, il est conseillé d'utiliser une carte d'accès associée à une identification biométrique.

4-8 Armoires du système informatique et de télécommunications

Règle. Toutes les armoires et pièces contenant des interconnexions réseau ou de télécommunications, ou encore des points d'accès au réseau, doivent être sécurisées en permanence.

Notes/explication. Seul le personnel autorisé doit avoir la permission d'accéder aux armoires et pièces qui renferment des interconnexions réseau ou de télécommunications. Les techniciens qui ne font pas partie de l'entreprise doivent être identifiés de manière sûre en suivant les procédures définies par le service en charge de la sécurité de l'information. L'accès aux lignes téléphoniques, hubs, centraux, routeurs ou autres matériels de ce type peut être exploité par un assaillant pour compromettre la sécurité des réseaux de l'entreprise.

4-9 Points de dépôt du courrier interne

Règle. Les points de dépôt du courrier interne à l'entreprise ne doivent pas se trouver dans des locaux accessibles au public.

Notes/explication. Les espions industriels ou les pirates informatiques ayant accès aux points de dépôt du courrier interne de l'entreprise peuvent s'en servir pour envoyer de fausses lettres d'autorisation ou des formulaires internes qui demandent aux salariés de fournir des informations confidentielles ou d'exécuter une action qui fera progresser l'assaillant. Un assaillant pourrait aussi envoyer un CD-ROM ou un autre support électronique, en y associant des instructions — pour mettre à jour un logiciel ou ouvrir un fichier contenant en réalité une macro, par exemple — qui lui donneront la possibilité de s'approcher de son objectif. Toute demande passant par un courrier distribué en interne est spontanément considérée par son destinataire comme authentique.

4-10 Tableaux d'affichage de l'entreprise

Règle. Les tableaux d'affichage destinés à l'information des salariés ne doivent pas être placés dans des locaux accessibles au public.

Notes/explication. La plupart des entreprises disposent de tableaux d'affichage où des informations internes à l'entreprise, privées ou personnelles, sont rendues publiques : notes aux salariés, listes de salariés, mémos internes, petites annonces avec les numéros de téléphone personnels des salariés, etc.

Les tableaux d'affichage sont souvent situés à côté de la cafétéria, de la salle fumeurs ou de la salle de repos, auxquelles les visiteurs ont généralement accès. Ce type d'information ne doit pas être exposé à la vue des visiteurs ou du public.

4-11 Entrée de la salle informatique

Règle. La salle ou le centre informatique doivent toujours être verrouillés, et seules des personnes habilitées doivent pouvoir y pénétrer.

Notes/explication. Il peut être utile de mettre en place un système de contrôle d'accès électronique par badge afin que toutes les entrées puissent être enregistrées.

4-12 Comptes auprès de fournisseurs

Règle. Les salariés qui réalisent des achats auprès des fournisseurs de l'entreprise doivent mettre en place un compte protégé par mot de passe afin d'empêcher des personnes non autorisées de passer des commandes au nom de l'entreprise.

Notes/explication. Certains fournisseurs offrent la possibilité, aux clients qui en font la demande, de protéger leur compte par mot de passe. L'entreprise doit établir un mot de passe pour tous les fournisseurs qui offrent des services ayant une importance essentielle pour son fonctionnement. Cette règle est particulièrement fondamentale dans le domaine des télécommunications et d'Internet. Dès lors que les services fournis sont essentiels pour l'entreprise, il faut se servir d'un secret commun préalablement établi pour vérifier que l'interlocuteur est autorisé à formuler sa demande. On notera que, pour l'identification, des données telles que le numéro de sécurité sociale, le numéro de TVA, le nom de jeune fille de la mère ou tout autre renseignement de même nature ne doivent pas être employés.

Un manipulateur pourra par exemple appeler l'opérateur téléphonique et demander la mise en place d'un transfert d'appel pour une ligne qui procure une connexion à distance à partir d'un modem. Il pourra aussi demander au centre d'enregistrement de modifier les données d'adresses IP de manière à opérer une redirection vers un nom de domaine

4-13 Personne de référence pour chaque service

Règle. L'entreprise peut demander à chaque service de désigner une personne de référence qui fera office de point de contact afin que n'importe qui dans l'entreprise puisse facilement vérifier l'identité d'une personne inconnue prétendant faire partie de ce service. Ainsi, le service d'assistance de l'entreprise contactera la personne de référence pour vérifier l'identité d'un salarié qui demande un service.

Notes/explication. Cette méthode de vérification d'identité réduit le nombre de salariés autorisés à se porter garants pour les employés de leur service lorsque ceux-ci formulent une demande, concernant la réinitialisation d'un mot de passe, par exemple.

Les attaques des manipulateurs réussissent en partie parce que le service d'assistance technique est généralement débordé et ne prend pas la peine de vérifier l'identité des interlocuteurs. Dans le cas d'une grande entreprise, qui emploie évidemment un grand nombre de salariés, les membres du service d'assistance ne peuvent généralement pas identifier personnellement tous les employés. Le fait de désigner quelqu'un comme référence permet de limiter le nombre de personnes que les employés du service d'assistance doivent connaître personnellement à des fins de vérification.

4-14 Mots de passe des clients

Règle. Les commerciaux et le service clients n'auront pas accès aux mots de passe des comptes des clients.

Notes/explication. Il est courant pour les manipulateurs d'appeler le service clients d'une entreprise et, sous un prétexte quelconque, de tenter d'obtenir les informations d'authentification de l'un des clients, le mot de passe, par exemple. Cette information lui servira ensuite à appeler un autre salarié du service clients, à se faire passer pour un client et à obtenir des informations ou à passer des commandes frauduleuses.

Pour empêcher ce type d'attaque de réussir, les logiciels du service clients doivent être conçus de telle manière que les commerciaux ne puissent saisir que les informations d'authentification fournies par l'appelant, suite à quoi le logiciel indiquera si le mot de passe est correct ou non.

4-15 Tests de vulnérabilité

Règle. Lorsqu'ils recevront leur formation en matière de sécurité ou lors de leur phase d'orientation, les salariés seront informés du fait que l'entreprise procède à des tests de vulnérabilité afin de vérifier le respect des consignes de sécurité.

Notes/explication. En l'absence d'avertissement préalable, les tests de pénétration peuvent embarrasser, gêner ou mécontenter les salariés du fait de l'utilisation à leur encontre de tactiques "déloyales". Ce type de conflit sera évité si, dès leur arrivée, les recrues sont informées de l'existence de ces tests.

4-16 Affichage des informations sensibles

Règle. Les informations de l'entreprise qui ne sont pas destinées au public ne seront affichées dans aucune zone accessible au public.

Notes/explication. À l'évidence, les informations confidentielles concernant les produits et les procédures ne doivent pas être affichées publiquement. Il en va de même pour les coordonnées internes, telles que les numéros de téléphone internes des salariés ou les plans des lieux qui indiquent les responsables de chaque service de l'entreprise.

4-17 Sensibilisation à la sécurité

Règle. Tous les salariés de l'entreprise doivent suivre un cours de sensibilisation à la sécurité lors de leur phase d'orientation. Par ailleurs, des cours de recyclage doivent être dispensés à intervalles réguliers au moins une fois par an, en fonction des décisions du service responsable de la formation à la sécurité.

Notes/explication. Un grand nombre d'entreprises n'accordent aucune importance à la sensibilisation des utilisateurs finaux. Dans une étude sur la sécurité menée aux États-Unis en 2001, seules 30 % des entreprises qui ont répondu dépensent de l'argent pour former leurs utilisateurs finaux. Or, la sensibilisation à la sécurité est un facteur essentiel pour contrer les attaques de manipulateurs.

4-18 Formation à la sécurité avant l'accès aux ordinateurs

Règle. Tout salarié doit suivre avec succès un cours de formation à la sécurité avant de pouvoir accéder au système informatique de l'entreprise.

Notes/explication. Les manipulateurs choisissent souvent pour cible les nouvelles recrues qui, au sein de l'entreprise, sont généralement celles qui sont le moins bien informées à propos des règles de sécurité et de gestion des informations sensibles.

La formation doit permettre aux salariés de poser leurs propres questions à propos des règles de sécurité. Après la formation, tout titulaire d'un compte d'utilisateur doit signer un document attestant qu'il connaît les règles de sécurité et qu'il accepte de les respecter.

4-19 Code de couleurs pour les badges

Règle. Les badges d'identification doivent se conformer à un code de couleurs grâce auxquelles on pourra distinguer les salariés, les sous-traitants, les intérimaires, les fournisseurs, les consultants, les visiteurs et les stagiaires.

Notes/explication. La couleur du badge est un excellent moyen d'identifier de loin le statut d'une personne. L'alternative consisterait à placer une grande lettre sur le badge, mais le codage par couleur est plus sûr.

Une technique courante de manipulation pour s'introduire dans des locaux consiste à se faire passer pour un livreur ou un technicien de maintenance. Une fois à l'intérieur, le manipulateur prétend alors être un collègue ou ment à propos de son statut pour obtenir la coopération des salariés. L'objectif de cette règle est d'empêcher qu'une personne puisse s'introduire de manière légitime dans les locaux, puis accéder à des zones qui lui sont interdites. Avec le code de couleurs, une personne qui accède aux locaux en tant que réparateur ne pourra pas se faire passer ensuite pour un salarié, car la couleur de son badge la trahirait.

RÈGLES CONCERNANT LE SERVICE INFORMATIQUE

Le service informatique de chaque entreprise doit mettre en place des règles particulières visant à protéger l'information. J'ai divisé cette partie en quatre sections (qui correspondent au type de structure le plus courant dans les services informatiques) : Général, Service d'Assistance, Administration et Exploitation/Production.

Général

5-1 Coordonnées des salariés du service informatique

Règle. Les numéros de téléphone et adresses électroniques des salariés du service informatique doivent être communiqués uniquement aux personnes qui ont besoin de les connaître.

Notes/explication. L'objectif de cette règle est d'éviter que des coordonnées puissent être exploitées par des manipulateurs. Si l'entreprise fournit un seul numéro de téléphone et une seule adresse électronique au public pour

son service informatique, les personnes extérieures à l'entreprise ne pourront pas contacter directement le personnel informatique. L'adresse électronique à utiliser pour les questions administratives et techniques doit avoir un format générique, tel que "admin@nomdelasociete.com" ; le numéro de téléphone public doit correspondre à une boîte vocale générique pour le service, et non à un ou plusieurs salariés.

Quand des coordonnées directes sont disponibles, l'assaillant peut plus facilement joindre directement un salarié du service informatique et l'inciter à fournir des informations qui pourront servir à une attaque. Il peut aussi se faire passer pour un membre du personnel informatique dont il utilisera le nom et les coordonnées.

5-2 Demandes d'assistance technique

Règle. Seul le service d'assistance est habilité à fournir une assistance technique.

Notes/explication. Un manipulateur pourra cibler un membre du personnel informatique qui, habituellement, n'effectue pas de missions d'assistance technique et qui ne connaît peut-être pas les procédures de sécurité à suivre pour traiter ce type de demande. Par conséquent, le personnel informatique doit savoir qu'il doit refuser ce type de demande et orienter la personne qui en est à l'origine vers le service d'assistance.

Service d'assistance

6-1 Procédures d'accès distant

Règle. Le personnel du service d'assistance ne doit fournir aucun détail ni aucune instruction concernant l'accès à distance, y compris les points d'accès extérieurs au réseau et les numéros d'appel pour l'accès à distance, tant que l'individu qui en fait la demande n'a pas été identifié à la fois :

- En tant que personne habilitée à obtenir des informations internes.
- En tant que personne habilitée à se connecter au réseau de l'entreprise comme utilisateur externe. À moins d'être connue à titre personnel, cette personne doit être identifiée de manière sûre à l'aide des procédures de vérification et d'autorisation décrites au début de ce chapitre.

Notes/explication. Le service d'assistance interne de l'entreprise est souvent une cible prioritaire pour les manipulateurs, d'une part parce que la nature de son travail est d'aider les utilisateurs qui ont des problèmes informatiques, d'autre part parce que son personnel dispose habituellement de privilèges système importants. Tout le personnel du service d'assistance doit être entraîné de manière à faire office de pare-feu humain afin d'éviter la diffusion d'informations sensibles qui pourraient être exploitées par des personnes non autorisées pour accéder à des ressources de l'entreprise. La règle à observer est de ne jamais dévoiler les procédures d'accès distant à aucun individu, tant qu'on n'en a pas établi l'identité de manière sûre.

6-2 Réinitialisation de mots de passe

Règle. Le mot de passe d'un compte d'utilisateur ne peut être réinitialisé qu'à la demande du propriétaire du compte.

Notes/explication. La technique la plus courante utilisée par les manipulateurs consiste à se faire passer pour un utilisateur et à demander une modification ou une réinitialisation du mot de passe sous prétexte que celui-ci a été perdu ou oublié. Pour contrer ce type d'attaque, le membre du personnel informatique qui reçoit une demande en ce sens doit rappeler son interlocuteur avant d'agir. Pour ce faire, il ne faut pas utiliser un numéro de téléphone fourni par l'interlocuteur mais le numéro qui figure dans l'annuaire. Voir "Procédures de vérification et d'authentification" pour plus de détails à ce sujet.

6-3 Modification des privilèges d'accès

Règle. Toute demande concernant l'augmentation des privilèges ou des droits d'accès d'un utilisateur doit être approuvée par écrit par le supérieur hiérarchique de l'utilisateur du compte. Une fois la modification apportée, une confirmation doit en être envoyée au supérieur hiérarchique par courrier interne. Par ailleurs, on vérifiera l'authenticité de ces requêtes à l'aide des procédures de vérification et d'autorisation.

Notes/explication. Lorsqu'un pirate informatique parvient à accéder à un compte d'utilisateur, l'étape suivante consiste à augmenter ses privilèges afin d'obtenir un contrôle complet sur le système. Un assaillant qui connaît les procédures d'autorisation peut falsifier une demande d'autorisation lorsque celle-ci est transmise par courrier électronique, fax ou téléphone. L'assaillant pourra par exemple appeler le support technique ou le service d'assistance et tenter de persuader un technicien de lui attribuer des privilèges supplémentaires pour le compte auquel il a accès.

6-4 Autorisation de création d'un compte d'utilisateur

Règle. Toute demande de création d'un compte d'utilisateur pour un salarié, un sous-traitant ou une autre personne autorisée, doit être soit

rédigée puis signée par le supérieur hiérarchique de la personne concernée, soit envoyée par courrier électronique signé numériquement. Ce type de demande doit également être vérifié par l'envoi d'une confirmation *via* le courrier interne de l'entreprise.

Notes/explication. Dans la mesure où les mots de passe et les autres données qui permettent de pénétrer les systèmes informatiques sont les cibles prioritaires des manipulateurs, il faut prendre des précautions spéciales. L'objet de cette règle est d'empêcher qu'un pirate informatique puisse se faire passer pour une personne autorisée ou falsifier une demande de nouveau compte. Par conséquent, toute demande de ce type doit être vérifiée de manière sûre à l'aide des procédures de vérification et d'autorisation.

6-5 Communication de nouveaux mots de passe

Règle. Les nouveaux mots de passe doivent être traités comme des informations confidentielles et leur communication ne doit se faire que par des méthodes sûres : en personne et en face à face, ou par courrier recommandé avec accusé de réception, entre autres. Voir les règles concernant la communication d'informations confidentielles.

Notes/explication. Le courrier interne peut également être utilisé, mais dans ce cas, il est conseillé d'utiliser des enveloppes spéciales qui masquent le contenu du courrier. Il est conseillé de désigner dans chaque service une personne de référence pour l'informatique ; cette personne aura à charge de communiquer les données relatives aux nouveaux comptes et de se porter garante de l'identité de ceux qui perdent ou oublient leur mot de passe. Ainsi, le service d'assistance ne sera en communication qu'avec un nombre restreint de personnes qui seront facilement identifiées.

6-6 Désactivation d'un compte

Règle. Avant de désactiver un compte d'utilisateur, il est nécessaire de vérifier que la requête a été effectuée par une personne autorisée.

Notes/explication. L'objectif de cette règle est d'empêcher un assaillant de demander la désactivation d'un compte, puis d'appeler l'utilisateur de ce compte en se faisant passer pour un technicien pouvant résoudre le problème d'accès au compte. Dans une telle situation de "dépannage", la victime révélera plus facilement son mot de passe.

6-7 Désactivation d'un port ou d'un périphérique réseau

Règle. Aucun port ni périphérique réseau ne doit être désactivé par qui que ce soit, sauf un technicien dont l'identité a été vérifiée.

Notes/explication. L'objectif de cette règle est d'empêcher un assaillant de demander la désactivation d'un port ou d'un périphérique réseau, puis d'appeler l'utilisateur de l'ordinateur correspondant en se faisant passer pour un technicien qui peut résoudre le problème d'accès au réseau. Dans une telle situation de "dépannage", la victime révélera plus facilement son mot de passe.

6-8 Communication des procédures d'accès sans fil

Règle. Aucun salarié ne doit communiquer à des tiers non autorisés les procédures grâce auxquelles on peut accéder au réseau par l'intermédiaire d'un équipement d'accès sans fil.

Notes/explication. Il faut toujours vérifier qu'une personne est autorisée à se connecter au réseau de l'entreprise en tant qu'utilisateur externe avant de lui fournir des informations sur les procédures de connexion au réseau sans fil. Voir les procédures de vérification et d'autorisation.

6-9 Noms des utilisateurs rencontrant des problèmes

Règle. Les noms des salariés signalant qu'ils sont confrontés à un problème informatique ne doivent pas être communiqués à l'extérieur du service informatique.

Notes/explication. Une attaque classique consiste, pour le manipulateur, à appeler le service d'assistance et à demander le nom des personnes qui ont signalé des problèmes d'informatique. La personne qui appelle prétendra être un collègue, un fournisseur ou un technicien de l'opérateur téléphonique. Une fois informé des noms des personnes qui ont signalé un problème, le manipulateur contacte ces personnes en se faisant passer pour un technicien qui appelle pour résoudre le problème. Au cours de la conversation, l'assaillant amène alors sa victime à lui fournir les renseignements qu'il souhaite ou à exécuter une action grâce auxquels l'assaillant pourra s'approcher de son objectif.

6-10 Exécution de logiciels ou de commandes

Règle. Les personnes qui font partie du service informatique et disposent de comptes privilégiés ne doivent exécuter aucun logiciel ni aucune commande à la demande de tiers qu'ils ne connaissent pas personnellement.

Notes/explication. Une méthode courante employée par les assaillants pour installer un "troyen" (*Trojan horse*, cheval de Troie) ou un autre logiciel de piratage consiste à modifier le nom et le contenu d'un logiciel existant, puis à appeler le service d'assistance en se plaignant qu'un message d'erreur

s'affiche à chaque exécution d'un programme. L'assaillant convainc alors le technicien du service d'assistance d'essayer d'exécuter le programme lui-même. Quand le technicien obtempère, le logiciel de piratage hérite des privilèges de l'utilisateur qui exécute le programme, et il modifie le système de telle manière que l'assaillant dispose des mêmes privilèges que le technicien. L'assaillant dispose ensuite de droits étendus sur le système informatique de l'entreprise.

Cette règle permet de contrer cette tactique en exigeant du personnel d'assistance qu'il vérifie l'identité et le statut de la personne qui émet la requête avant d'y satisfaire en exécutant un logiciel.

Administration

7-1 Modification des droits d'accès globaux

Règle. Toute demande de modification des droits d'accès globaux associés à un type de poste déterminé doit être approuvée par le groupe qui a la responsabilité de la gestion des droits d'accès du réseau de l'entreprise.

Notes/explication. Le personnel autorisé analysera toute requête de ce type pour s'assurer qu'une telle modification ne représente pas une menace pour la sécurité de l'entreprise. Si c'est le cas, avant de prendre une décision quant aux modifications à effectuer, le responsable discutera du problème avec la personne qui a formulé la demande.

7-2 Demandes d'accès distant

Règle. Les demandes d'accès distant ne peuvent être accordées qu'aux employés qui peuvent prouver qu'ils ont besoin d'accéder au système informatique de l'entreprise à partir de l'extérieur. La requête doit être formulée par le supérieur hiérarchique de la personne qui est à l'origine de la demande, et elle doit être vérifiée à l'aide des procédures de vérification et d'autorisation.

Notes/explication. Une partie du personnel peut avoir besoin d'accéder au réseau à partir de l'extérieur de l'entreprise, mais le fait de limiter le nombre de personnes disposant d'un tel accès réduit de manière considérable les risques et la gestion de ce type de connexion. Plus le nombre de personnes qui peuvent se connecter à distance est réduit, moins un assaillant a de victimes potentielles. Il ne faut pas négliger le fait qu'un assaillant peut aussi attaquer *via* Internet un utilisateur qui a le droit de se connecter à l'entreprise à distance, ou se faire passer pour un tel utilisateur lors d'un appel téléphonique à l'entreprise.

7-3 Réinitialisation des mots de passe des comptes privilégiés

Règle. Toute demande de réinitialisation du mot de passe d'un compte privilégié doit être approuvée par l'administrateur système responsable de l'ordinateur sur lequel est utilisé le compte en question. Le nouveau mot de passe doit être expédié par courrier interne ou communiqué en face à face.

Notes/explication. Les comptes privilégiés permettent d'accéder à toutes les ressources système et à tous les fichiers stockés sur un système donné. Par conséquent, ces comptes doivent être particulièrement bien protégés.

7-4 Accès distant du personnel d'assistance externe

Règle. Aucun membre du personnel d'un service d'assistance externe (fournisseur de matériels ou de logiciels) ne doit obtenir d'informations concernant l'accès à distance ni accéder aux systèmes informatiques de l'entreprise sans que l'on vérifie au préalable son identité et son autorisation. Si le fournisseur a besoin d'un accès privilégié pour fournir des services d'assistance, le mot de passe du compte utilisé par le fournisseur doit être modifié immédiatement après que le fournisseur a terminé sa tâche.

Notes/explication. Un pirate informatique pourra se faire passer pour un fournisseur afin d'accéder au réseau informatique ou de télécommunications de l'entreprise. Par conséquent, il est essentiel de vérifier à la fois l'identité du fournisseur et le fait qu'il est autorisé à exécuter les opérations demandées. Par ailleurs, dès lors que sa tâche est terminée, on doit de nouveau lui interdire l'accès au système en modifiant le mot de passe qui lui a été temporairement attribué.

Le fournisseur ne doit jamais être autorisé à choisir lui-même un mot de passe pour son compte d'utilisateur, même si ce compte est provisoire. Certains fournisseurs ont tendance à utiliser les mêmes mots de passe pour différents clients. Ainsi, il est arrivé qu'un fournisseur de services de réseaux ait mis en place chez tous ses clients des comptes privilégiés avec des mots de passe identiques, et pour aggraver encore son cas, avec un accès Telnet activé !

7-5 Authentification forte pour l'accès distant aux systèmes de l'entreprise

Règle. Tous les points de connexion vers l'intérieur du réseau de l'entreprise doivent être protégés à l'aide de techniques d'authentification forte, mots de passe dynamiques ou biométrie, par exemple.

Notes/explication. Nombre d'entreprises se servent de mots de passe statiques comme unique moyen d'authentification pour les utilisateurs distants.

Cette manière de procéder est dangereuse parce qu'elle n'est pas sûre : les pirates informatiques s'attaquent à tout point d'accès distant susceptible d'être le maillon faible du réseau de l'entreprise ciblée. N'oubliez pas qu'on ne peut jamais savoir si quelqu'un d'autre connaît le mot de passe qu'on utilise.

De ce fait, les points d'accès distants doivent être protégés par des techniques d'authentification forte tels que les jetons temporels, les cartes à puces ou la biométrie, afin que des mots de passe éventuellement interceptés ne puissent être d'aucune utilité à un assaillant.

Lorsqu'il n'est pas possible de faire appel à une authentification forte, les utilisateurs doivent respecter scrupuleusement les règles concernant les mots de passe difficiles à deviner.

7-6 Configuration des systèmes d'exploitation

Règle. Les administrateurs système doivent faire en sorte que, lorsque c'est possible, les systèmes d'exploitation soient configurés de manière à imposer le respect des règles de sécurité.

Notes/explication. La conception et la diffusion de règles de sécurité sont des étapes essentielles qui contribuent à réduire les risques, mais dans la plupart des cas, c'est l'attitude du salarié qui est déterminante pour le respect de ces règles. Néanmoins, il est parfois possible d'imposer ce respect au travers de moyens informatiques, par exemple en ce qui concerne la longueur minimale des mots de passe. L'automatisation des règles de sécurité par l'intermédiaire de la configuration des paramètres des systèmes d'exploitation évite que le salarié ait à prendre la décision et réduit ainsi les risques de sécurité pour l'entreprise.

7-7 Expiration obligatoire

Règle. Tous les comptes d'utilisateur doivent expirer au bout d'un an.

Notes/explication. Cette règle a pour but de faire disparaître les comptes inemployés, dans la mesure où les pirates informatiques ciblent souvent ce type de comptes. Avec cette règle, on a l'assurance qu'un compte appartenant à d'anciens salariés ou sous-traitants qui aurait été laissé en place par erreur sera automatiquement supprimé.

La direction de l'entreprise pourra également décider que lors de l'expiration de leur compte, les salariés assistent à un cours de recyclage ou relisent les règles de sécurité et consignent par écrit leur engagement à les respecter.

7-8 Adresses de courrier électronique génériques

Règle. Le service informatique doit créer une adresse électronique générique pour chacun des services qui est en contact avec le public.

Notes/explication. L'adresse électronique générique peut être diffusée auprès du public par l'intermédiaire de la standardiste ou du site Web de l'entreprise. Les salariés ne doivent communiquer leur propre adresse électronique qu'aux personnes qui ont véritablement besoin de la connaître.

Lors de la première phase d'une attaque par manipulation, l'assaillant tente souvent d'obtenir les numéros de téléphone, les noms et les intitulés de postes des salariés. Dans la plupart des cas, ces informations peuvent être obtenues sur simple demande ou en se rendant sur le site Web de l'entreprise. Lorsqu'une entreprise utilise des boîtes vocales et des adresses électroniques génériques, il est plus difficile d'associer le nom d'un salarié à une fonction ou un service particulier.

7-9 Coordonnées pour l'enregistrement des noms de domaines

Règle. Lors de l'enregistrement d'un nom de domaine, les coordonnées fournies ne doivent mentionner nommément aucune personne : elles doivent uniquement indiquer des adresses électroniques génériques et le numéro du standard de l'entreprise.

Notes/explication. Le but de cette règle est d'éviter qu'un assaillant exploite des coordonnées. Quand ces informations mentionnent le nom et le numéro de téléphone d'un individu, les manipulateurs peuvent en profiter pour contacter l'individu en question et l'abuser de manière à lui faire révéler des informations système. Ils peuvent aussi lui faire exécuter une action qui leur permettra de s'approcher de leur objectif. Un manipulateur peut également se faire passer auprès d'un tiers pour la personne mentionnée dans les coordonnées.

Plutôt que de mentionner le nom d'un salarié, les coordonnées électroniques doivent avoir un format tel que "administrateur@societe.com". Le personnel du service des télécommunications pourra mettre en place une boîte vocale générique pour les contacts administratifs ou techniques afin de limiter la quantité d'informations qui peuvent être exploitées dans une attaque.

7-10 Mises à jour de sécurité et de système d'exploitation

Règle. Tous les correctifs (*patchs*) de sécurité disponibles pour le système d'exploitation et les logiciels doivent être installés dès qu'ils sont disponibles.

Si cette règle ne peut être appliquée parce qu'elle risquerait de compromettre des systèmes cruciaux pour le bon fonctionnement de l'entreprise, les mises à jour doivent être appliquées dès que possible.

Notes/explication. Lorsqu'une faille est identifiée, il faut immédiatement contacter l'éditeur de logiciels pour savoir si un correctif ou un remède provisoire a été mis au point pour remédier à cette vulnérabilité. Un système non mis à jour représente l'une des failles de sécurité les plus graves qui soient pour l'entreprise. Quand l'administrateur système repousse l'installation des correctifs, il ouvre une voie royale aux assaillants pour pénétrer le réseau de l'entreprise.

Des dizaines de failles sont identifiées chaque semaine, et les informations qui leur sont relatives sont publiées sur Internet. Si le personnel du service informatique de l'entreprise ne prend pas la peine d'appliquer les correctifs de sécurité dès que leur installation peut se faire sans nuire au fonctionnement de l'entreprise, la présence de pare-feu ne suffira pas à protéger les systèmes informatiques. Que ce soit pour le système d'exploitation ou pour tout logiciel utilisé dans l'entreprise, il est essentiel de se tenir informé des failles qui sont régulièrement identifiées.

7-11 Coordonnées sur le site Web

Règle. Le site Web externe de l'entreprise ne doit pas dévoiler les détails de l'organigramme de l'entreprise ni citer le nom d'aucun salarié.

Notes/explication. Les informations concernant la structure de l'entreprise telles que les organigrammes hiérarchiques, les listes de salariés, les intitulés des fonctions ou des postes, les coordonnées téléphoniques internes, les numéros de téléphone des salariés et tout autre renseignement employé en interne ne doivent pas être divulgués sur un site Web accessible au public.

Les pirates informatiques parviennent souvent à obtenir des informations très utiles à partir du site Web de l'entreprise ciblée. L'assaillant utilise ces informations pour donner l'impression qu'il connaît l'entreprise de l'intérieur, ce qui augmente sa crédibilité lorsqu'il se fait passer pour un salarié, par exemple. Par ailleurs, l'assaillant peut analyser ces informations pour identifier des cibles potentielles ayant accès à des informations sensibles.

7-12 Création de comptes privilégiés

Règle. Aucun compte privilégié ne peut être créé et aucun privilège système ne peut être accordé sans l'autorisation de l'administrateur système.

Notes/explication. Les pirates informatiques se font souvent passer pour des représentants du fabricant des ordinateurs utilisés par l'entreprise ou des représentants de l'éditeur de ses logiciels, afin d'obtenir la création de comptes d'utilisateur. L'objet de cette règle est de bloquer ces attaques en établissant un contrôle plus strict quant à la création de comptes privilégiés. L'administrateur système doit approuver toutes les demandes de création de comptes disposant de privilèges élevés.

7-13 Comptes Invité

Règle. Tous les comptes Invité de tous les ordinateurs et autres appareils en réseau doivent être désactivés ou supprimés, à l'exception des comptes FTP anonymes agréés par l'administrateur système.

Notes/explication. La fonction des comptes d'invités est de fournir un accès provisoire à des personnes n'ayant pas besoin de disposer de leur propre compte. Certains systèmes d'exploitation présentent par défaut un compte Invité lors de leur installation. Les comptes Invité doivent être désactivés parce que leur existence va à l'encontre du principe de la traçabilité des utilisateurs. Le service informatique doit être à même de suivre toute activité informatique et de l'associer à un utilisateur spécifique.

Les manipulateurs parviennent facilement à exploiter les comptes Invité pour obtenir des accès non autorisés, soit directement, soit indirectement en incitant des salariés autorisés à les utiliser.

7-14 Cryptage des données stockées hors site

Règle. Les données de l'entreprise qui sont stockées hors site doivent être systématiquement cryptées.

Notes/explication. Le personnel de la division d'exploitation doit s'assurer que toutes les données peuvent être rétablies en cas de besoin. Pour cela, il procédera à intervalles réguliers à des tests portant sur un échantillon aléatoire de données cryptées. Par ailleurs, les clés qui servent à crypter les données doivent être déposées auprès d'une personne de confiance pour le cas où elles seraient perdues ou indisponibles par ailleurs.

7-15 Accès des visiteurs aux connexions réseau

Règle. Tous les points d'accès Ethernet accessibles au public doivent se trouver sur une partie du réseau segmentée afin d'empêcher tout accès non autorisé au réseau interne.

Notes/explication. L'objet de cette règle est d'empêcher des personnes extérieures à l'entreprise de se connecter au réseau interne lorsqu'elles se trouvent dans les locaux de l'entreprise. Les prises Ethernet situées dans les salles de réunion, la cafétéria, les salles de formation ou d'autres lieux accessibles

aux visiteurs doivent être filtrées afin d'empêcher des accès non autorisés au système informatique de l'entreprise.

L'administrateur du réseau ou de la sécurité pourra choisir de mettre en place un réseau local virtuel (VLAN), si cette option est disponible, pour limiter l'accès au réseau interne à partir de ces emplacements.

7-16 Modems pour les connexions à distance

Règle. Les modems qui donnent la possibilité de se connecter à distance à partir de l'extérieur de l'entreprise ne doivent pas répondre avant la quatrième sonnerie.

Notes/explication. Comme le montre le film *War Games*, les hackers utilisent une technique nommée *WarDialing* pour trouver des lignes de téléphone auxquelles sont connectés des modems. La première étape consiste, pour le hacker, à identifier les préfixes téléphoniques de la zone où se trouve l'entreprise. Ensuite, un programme de scan permet d'essayer chacun des numéros de téléphone de ce préfixe afin de détecter les lignes auxquelles sont connectés des modems. Afin d'accélérer le processus, ces types de programmes sont configurés pour laisser sonner une ou deux fois en attendant une réponse du modem, avant de passer au numéro suivant. Lorsqu'un modem est configuré pour ne répondre qu'après quatre sonneries, les programmes de scan ne peuvent pas identifier la ligne correspondante comme étant reliée à un modem.

7-17 Logiciels antivirus

Règle. Une version récente d'un logiciel antivirus doit être installée et activée sur chacun des ordinateurs de l'entreprise.

Notes/explication. Dans les entreprises où l'installation des logiciels antivirus et des fichiers de définition de virus sur les postes des utilisateurs n'est pas automatique, c'est à chacun des utilisateurs d'installer et de mettre à jour les logiciels sur son propre système, y compris sur les ordinateurs utilisés pour accéder au réseau à distance.

Si possible, ces logiciels doivent être configurés pour une mise à jour quotidienne des fichiers de définition de virus. Quand cette mise à jour n'est pas automatique, elle doit être réalisée par les utilisateurs au moins une fois par semaine.

Ces règles s'appliquent à tous les ordinateurs, portables et de bureau, qui sont utilisés pour accéder aux systèmes informatiques de l'entreprise, y compris les ordinateurs dont l'utilisateur est lui-même propriétaire.

7-18 Pièces jointes de courriers électroniques (dans un contexte de sécurité élevée)

Règle. Quand une entreprise doit imposer des contraintes de sécurité élevées, il faut que le pare-feu de l'entreprise soit configuré de manière à supprimer systématiquement les pièces jointes des courriers électroniques.

Notes/explication. Cette règle ne s'applique qu'aux entreprises qui doivent imposer des contraintes de sécurité élevées ou à celles qui n'ont pas besoin de recevoir de pièces jointes par courrier électronique.

7-19 Authentification des logiciels

Règle. Tout nouveau logiciel, toute mise à jour et tout correctif, qu'ils soient fournis sur un support physique ou téléchargés *via* Internet, doivent être authentifiés avant installation.

Notes/explication. Cette règle s'applique à tous les logiciels ainsi qu'aux composants de système d'exploitation, *patchs* et correctifs, mises à jours logicielles, etc. De nombreux éditeurs de logiciels ont mis au point un système grâce auquel le client peut vérifier l'intégrité du logiciel qui lui parvient, généralement au moyen d'une signature numérique. Quand cela est impossible, il faut contacter l'éditeur pour vérifier l'authenticité du logiciel.

Il est arrivé que des pirates informatiques envoient à leur victime un logiciel dans son emballage pour donner l'impression qu'il est fourni par l'éditeur. Avant d'installer un logiciel envoyé à l'entreprise, il est essentiel de vérifier son authenticité, en particulier si ce logiciel est parvenu à l'entreprise sans que celle-ci en ait fait la demande.

Notez qu'un assaillant déterminé pourra apprendre que votre entreprise a commandé un logiciel auprès d'un éditeur ; il pourra alors annuler la commande de l'entreprise puis commander le logiciel lui-même. Il le modifiera ensuite en fonction de ses besoins, puis le fera livrer à l'entreprise, sous emballage scellé si nécessaire. Une fois le logiciel installé, l'assaillant pourra prendre le contrôle de l'ordinateur.

7-20 Mots de passe par défaut

Règle. Tout composant du système d'exploitation et tout matériel qui sont initialement livrés avec un mot de passe par défaut doivent être reconfigurés de manière à respecter les règles de l'entreprise en matière de mots de passe.

Notes/explication. Différents composants de systèmes d'exploitation et appareils sont livrés avec des mots de passe par défaut, autrement dit avec des mots de passe qui sont identiques pour tous les appareils ou logiciels vendus.

Le fait de ne pas modifier ces mots de passe constitue une erreur grave qui peut menacer la sécurité de l'entreprise.

Les mots de passe par défaut sont connus et largement distribués sur le Web. Lorsqu'il lance une attaque, le premier mot de passe qu'essaie un assaillant est le mot de passe par défaut.

7-21 Verrouillage après des tentatives d'accès infructueuses (dans un contexte de sécurité faible ou moyenne)

Règle. Dans une entreprise où les exigences en matière de sécurité sont peu ou moyennement élevées, il est particulièrement important de verrouiller un compte pour une durée déterminée après un nombre donné de tentatives d'accès infructueuses.

Notes/explication. Il est nécessaire de limiter le nombre de tentatives d'accès infructueuses pour tous les serveurs et ordinateurs de l'entreprise. Cette règle est indispensable pour éviter qu'un mot de passe puisse être découvert par le biais d'essais de connexions successifs, d'attaques par dictionnaire ou par force brute.

L'administrateur système doit configurer les paramètres de sécurité de telle manière qu'un compte soit verrouillé dès lors qu'un certain nombre de tentatives d'accès infructueuses ont été effectuées. Il est conseillé de verrouiller le compte pendant au moins trente minutes après sept tentatives d'accès infructueuses.

7-22 Verrouillage après des tentatives d'accès infructueuses (dans un contexte de sécurité élevée)

Règle. Dans une entreprise où les exigences en matière de sécurité sont élevées, un compte doit être verrouillé après un nombre donné de tentatives d'accès infructueuses et ne doit être déverrouillé que suite à une demande adressée au groupe responsable de la gestion des comptes d'utilisateurs.

Notes/explication. Il est nécessaire de limiter le nombre de tentatives d'accès infructueuses pour tous les serveurs et ordinateurs de l'entreprise. Cette règle est indispensable pour éviter qu'un mot de passe puisse être découvert par le biais d'essais de connexion successifs, d'attaques par dictionnaire ou par force brute.

L'administrateur système doit configurer les paramètres de sécurité de telle manière qu'un compte soit verrouillé dès lors que cinq tentatives d'accès infructueuses ont eu lieu. Une fois le compte verrouillé, le propriétaire du compte devra appeler l'assistance technique ou le groupe responsable des comptes utilisateurs pour déverrouiller le compte. Avant le déverrouillage, le personnel responsable devra identifier de manière sûre le propriétaire du compte en respectant les procédures de vérification et d'autorisation.

7-23 Modification périodique des mots de passe des comptes privilégiés

Règle. Tout propriétaire de compte privilégié doit changer de mot de passe au moins une fois par mois.

Notes/explication. L'administrateur système pourra faire respecter cette règle en configurant en conséquence les paramètres du système d'exploitation, si celui-ci le permet.

7-24 Modification périodique des mots de passe des utilisateurs

Règle. Tout utilisateur doit changer le mot de passe de son compte au moins une fois tous les deux mois.

Notes/explication. L'administrateur système pourra faire respecter cette règle en configurant en conséquence les paramètres du système d'exploitation, si celui-ci le permet.

7-25 Mots de passe des nouveaux comptes

Règle. Tout nouveau compte doit être muni d'un mot de passe expirant après un délai défini, afin d'obliger l'utilisateur à choisir un nouveau mot de passe.

Notes/explication. Cette règle permet de s'assurer que seul le propriétaire du compte connaît son mot de passe.

7-26 Mot de passe au démarrage de l'ordinateur

Règle. Tous les ordinateurs doivent être configurés de manière à ce qu'il soit obligatoire de saisir un mot de passe au démarrage.

Notes/explication. Il faut configurer les ordinateurs afin d'obliger la saisie d'un mot de passe dès leur démarrage, avant le lancement du système d'exploitation. Cela évite qu'une personne non autorisée puisse mettre en route et utiliser l'ordinateur d'un tiers. Cette règle s'applique à tous les ordinateurs de l'entreprise.

7-27 Règles relatives aux mots de passe pour les comptes privilégiés

Règle. Tous les comptes privilégiés doivent être protégés par un mot de passe sûr. Ce mot de passe doit respecter les critères suivants :

- ne pas faire partie du dictionnaire de quelque langue que ce soit ;
- contenir à la fois des majuscules, des minuscules, au moins un symbole et au moins un chiffre ;
- avoir une longueur d'au moins douze caractères ;
- n'être lié en aucune façon à l'entreprise ou à l'utilisateur.

Notes/explication. Dans la plupart des cas, les pirates informatiques ciblent les comptes disposant de privilèges système. À l'occasion, le hacker est susceptible d'exploiter une vulnérabilité pour prendre le contrôle d'un système.

Les premiers mots de passe qu'essaiera un attaquant sont les plus simples, à savoir ceux des dictionnaires. Le choix d'un mot de passe sûr renforce la sécurité en réduisant la probabilité qu'un assaillant découvre un mot de passe à l'aide d'une attaque par essais successifs, par dictionnaire ou par force brute.

7-28 Points d'accès sans fil

Règle. Tous les utilisateurs qui se connectent *via* un réseau sans fil (*wireless* ou *Wi-Fi*) doivent faire appel à une technologie de réseau privé virtuel (VPN, *Virtual Private Network*) pour protéger le système informatique de l'entreprise.

Notes/explication. Ces réseaux sans fil peuvent être attaqués à l'aide d'une technique appelée *WarDriving*, qui consiste à se déplacer avec un ordinateur portable équipé d'une carte réseau 802.11b, ce qui donne la possibilité de détecter les réseaux sans fil et d'y pénétrer.

Nombre d'entreprises ont déployé des réseaux sans fil sans même activer le protocole WEP (*Wired Equivalent Privacy*), qui offre une certaine protection. Toutefois, à l'heure actuelle (début 2003), ni le 802.11b avec WEP, ni même le nouveau protocole 802.1X n'offrent un niveau de confidentialité suffisant.

Par conséquent, il est essentiel de compléter le protocole utilisé (802.11b ou 802.1X) par le déploiement d'un réseau privé virtuel (VPN).

7-29 Mise à jour des fichiers de définition de virus

Règle. Tous les ordinateurs doivent être programmés pour une mise à jour automatique des fichiers de définition de virus.

Notes/explication. Cette mise à jour doit être réalisée régulièrement, et au moins une fois par semaine. Dans les entreprises où les ordinateurs restent sous tension en permanence, il est conseillé de le faire tous les soirs.

Les logiciels antivirus sont inefficaces s'ils ne sont pas mis à jour régulièrement pour détecter toutes les nouvelles formes de code qui représentent une menace. Dans la mesure où la menace d'une contamination par des virus, des vers ou des troyens est nettement plus grande quand les fichiers de définition ne sont pas régulièrement mis à jour, il est essentiel de procéder à des mises à jour fréquentes de ces fichiers.

Exploitation et production

8-1 Exécution de commandes et de programmes

Règle. Aucun salarié du service d'exploitation/production de la direction informatique ne doit exécuter de commande ni lancer de programme à la demande d'une personne qu'il ne connaît pas. Dans une situation où une personne non vérifiée semble avoir une bonne raison de formuler cette demande, le salarié devra au préalable obtenir l'approbation d'un supérieur hiérarchique.

Notes/explication. Les salariés du service d'exploitation/production sont des cibles de choix pour les manipulateurs dans la mesure où leurs fonctions leur donnent généralement un accès privilégié aux systèmes informatiques. Par ailleurs, les assaillants comptent sur le fait qu'il soient moins expérimentés et moins bien informés des procédures de l'entreprise que d'autres membres du personnel informatique. L'objet de cette règle est d'ajouter un niveau de contrôle afin d'éviter que le personnel informatique ne soit dupé par des manipulateurs.

8-2 Salariés disposant d'un compte privilégié

Règle. Les salariés qui disposent d'un compte privilégié ne doivent fournir ni aide ni information à des personnes dont l'identité n'a pas été vérifiée. Cela vaut pour l'assistance informatique (aide à l'utilisation d'un logiciel, par exemple), l'accès aux bases de données, le téléchargement de logiciels ou la communication du nom de salariés ayant la possibilité de se connecter à distance.

Notes/explication. Les manipulateurs ciblent souvent les salariés qui disposent de comptes privilégiés. L'objet de cette règle est de faire en sorte que les membres du personnel informatique gèrent correctement les appels susceptibles d'être des attaques par manipulation.

8-3 Informations sur le système informatique

Règle. Le personnel de la division de production/exploitation ne doit fournir aucune information concernant les équipements et les systèmes informatiques de l'entreprise sans avoir au préalable vérifié de manière sûre l'identité de son interlocuteur.

Notes/explication. Les pirates informatiques contactent souvent le personnel de la division de production/exploitation du service informatique et tentent d'obtenir des informations telles que les systèmes procédures d'accès au système ou les procédures et numéros d'accès distant qu'ils peuvent exploiter ensuite.

Dans les entreprises qui emploient des personnes au support technique, les demandes de renseignements concernant le système informatique qui sont adressées au personnel de la division de production/exploitation doivent être considérées comme inhabituelles. Il faut examiner toute demande en fonction des règles de classification des informations afin de déterminer si l'individu à l'origine de la requête est autorisé à obtenir les renseignements demandés. Quand on ne peut déterminer la catégorie de l'information, on la considérera comme "Interne".

Dans certains cas, le service technique d'un fournisseur aura besoin de communiquer avec des personnes qui ont accès aux systèmes informatiques de l'entreprise. Des correspondants doivent être désignés dans l'entreprise afin que les fournisseurs traitent toujours avec les mêmes personnes et puissent identifier leurs interlocuteurs.

8-4 Communication des mots de passe

Règle. Le personnel de la division de production/exploitation ne doit jamais communiquer ses mots de passe ni aucun mot de passe dont il a connaissance sans l'approbation préalable d'un supérieur hiérarchique.

Notes/explication. D'une manière générale, la communication d'un mot de passe à un tiers doit être formellement interdite. Cette règle concerne le cas où le personnel de la division de production/exploitation doit communiquer un mot de passe dans une situation d'urgence. Dans ce cas exceptionnel, l'approbation d'un supérieur hiérarchique doit être obtenue au préalable. Pour plus de sécurité, la responsabilité de la communication des mots de passe à des tiers doit être limitée à un groupe restreint d'individus qui a reçu une formation spéciale concernant les procédures de vérification.

8-5 Supports numériques

Règle. Tous les supports numériques contenant des informations qui ne sont pas destinées au public doivent être conservés sous clé.

Notes/explication. L'objet de cette règle est d'empêcher le vol d'informations sensibles stockées sur des supports numériques.

8-6 Données sauvegardées

Règle. Le personnel de la division de production/exploitation doit stocker les données sauvegardées dans le coffre-fort de l'entreprise ou dans un autre lieu sûr.

Notes/explication. Les données sauvegardées sont une autre cible de choix pour les pirates informatiques. Un assaillant ne perdra pas de temps à tenter de trouver une faille dans le système informatique ou le réseau d'une entreprise quand les données sauvegardées et non protégées constituent le maillon le plus faible de la chaîne. Une fois que les données sauvegardées ont été dérobées, l'assaillant peut accéder à toutes les informations qui s'y trouvent, sauf si ces données sont cryptées. Par conséquent, la protection physique des données sauvegardées sur un support est essentielle pour assurer la confidentialité des informations de l'entreprise.

RÈGLES CONCERNANT TOUS LES SALARIÉS

Quel que soit le service dans lequel ils travaillent, il existe des règles de sécurité que tous les salariés doivent connaître. Nous les avons réparties dans les catégories suivantes : Général, Utilisation des ordinateurs, Utilisation du courrier électronique, Utilisation du téléphone, Utilisation du fax, Utilisation des boîtes vocales, Mots de passe.

Général

9-1 Comptes rendus d'appels suspects

Règle. Les salariés qui ont le sentiment d'avoir subi une tentative de manipulation, notamment lors de demandes portant sur la communication d'informations ou l'exécution de certaines actions sur l'ordinateur, doivent immédiatement signaler cette tentative au groupe responsable des informations sur les incidents de sécurité.

Notes/explication. Quand un manipulateur ne parvient pas à faire en sorte que sa cible réponde à sa demande, il fera presque toujours une seconde tentative auprès de quelqu'un d'autre. Lorsque l'on rend compte d'un appel ou d'un événement suspect, cela permet à l'entreprise d'être alertée du fait

qu'une attaque est peut-être en cours. Les employés constituent donc la première ligne de défense contre les attaques des manipulateurs.

9-2 Gestion des appels suspects

Règle. Lorsqu'un salarié reçoit un appel téléphonique qui lui semble être une tentative de manipulation, il doit, dans la mesure du possible, prolonger l'appel afin d'apprendre le maximum d'informations sur les objectifs de l'assaillant et noter les détails ainsi obtenus.

Notes/explication. Lorsqu'un compte rendu comprend de tels détails, il est plus facile de déterminer l'objectif ou la méthode de l'attaque.

9-3 Communication des numéros d'accès à distance

Règle. Les salariés ne doivent pas communiquer les numéros des modems de l'entreprise. Ils doivent diriger l'individu qui formule une telle demande au service d'assistance.

Notes/explication. Les numéros de téléphone qui donnent un accès à distance doivent être considérés comme une information interne et ne doivent être communiqués qu'aux salariés ayant effectivement besoin de les connaître dans le cadre de leur travail.

Les manipulateurs ciblent souvent les salariés ou les services qui sont les moins susceptibles de se montrer réticents à fournir ce type d'information. Un assaillant appellera par exemple le service comptable en se faisant passer pour un employé de l'opérateur téléphonique qui tente de résoudre un problème de facture. Il demandera ensuite les numéros de fax ou de modems de l'entreprise en expliquant que la connaissance de ces numéros l'aidera à résoudre son problème. Le manipulateur visera souvent un salarié qui n'a pas conscience de l'importance des informations qu'il fournit, ou qui n'est pas assez formé en ce qui concerne les règles et les procédures de communication d'informations de l'entreprise.

9-4 Badges d'identification

Règle. Excepté quand ils se trouvent dans leurs propres bureaux, tous les membres du personnel de l'entreprise, cadres et dirigeants inclus, doivent porter leur badge en permanence.

Notes/explication. Il faut dispenser une formation à tous les salariés, y compris aux dirigeants de l'entreprise, afin de les aider à accepter et à comprendre qu'il est indispensable de porter son badge où qu'on se trouve dans l'entreprise, sauf dans ses propres bureaux et dans les zones ouvertes au public.

9-5 Attitude vis-à-vis des salariés ne portant pas de badge

Règle. Tous les salariés doivent systématiquement exiger le port du badge de la part de personnes qu'ils ne connaissent pas personnellement et qui se trouvent dans les locaux de l'entreprise.

Notes/explication. Bien entendu, l'objectif ne doit pas être de transformer tous les salariés de l'entreprise en agents de sécurité, mais il reste que toute entreprise qui accorde de l'importance à la protection de ses informations doit prendre au sérieux la menace que représente un manipulateur qui peut circuler librement à l'intérieur des locaux. La diligence des salariés quant au respect de cette règle devra être encouragée par des contreparties ; différents types de récompense sont envisageables.

9-6 "Passagers clandestins" (entrée dans des locaux sécurisés)

Règle. Les salariés qui pénètrent dans un bâtiment ne doivent laisser personne entrer en même temps qu'eux en tant que "passager clandestin" lorsque cette entrée est sécurisée (avec carte magnétique, par exemple).

Notes/explication. Les salariés ne doivent pas considérer qu'il est malpoli de demander à un inconnu de s'identifier avant de l'aider à entrer dans les locaux de l'entreprise ou dans une zone sécurisée.

Les manipulateurs font souvent appel à la technique du "passager clandestin", qui consiste à attendre que quelqu'un s'apprête à pénétrer dans les locaux ou dans une zone sécurisée pour se joindre à la personne et entrer avec elle. La plupart des gens se sentent mal à l'aise lorsqu'ils doivent exiger d'une personne qu'elle s'identifie avant de la laisser entrer avec eux, dans la mesure où ils la considèrent *a priori* comme un collègue. Autre technique de ce type utilisée par les manipulateurs : les bras encombrés de cartons, ils attendent qu'un "collègue" serviable leur ouvre ou leur tienne la porte.

9-7 Destruction de documents sensibles

Règle. Les documents sensibles doivent être détruits au moyen d'une coupe croisée ; les supports informatiques ayant jamais contenu des informations sensibles, y compris les disques durs, doivent être détruits selon les procédures définies par le groupe responsable de la sécurité de l'information.

Notes/explication. Les destructeurs de documents standard ne suffisent pas à détruire les documents de manière sûre ; une coupe croisée est nécessaire. La meilleure manière de procéder consiste à partir du principe que les principaux concurrents de l'entreprise fouilleront dans les poubelles pour y chercher des documents qui pourront les intéresser.

Les espions industriels et les pirates informatiques trouvent souvent des informations sensibles à partir de documents jetés à la poubelle. Il est également arrivé que des concurrents tentent de soudoyer le personnel de nettoyage afin d'obtenir le contenu des corbeilles d'une entreprise. Ainsi, dans un cas récent, un salarié de la banque d'affaires Goldman Sachs a découvert dans une corbeille des documents prouvant l'existence d'un délit d'initiés.

9-8 Méthodes d'identification

Règle. Des données telles que le numéro de sécurité sociale ou de carte d'identité du salarié, ses date et lieu de naissance ou le nom de jeune fille de sa mère ne doivent jamais être employées pour vérifier une identité. Ces données ne sont pas secrètes et peuvent être obtenues de diverses manières.

Notes/explication. Pour peu qu'il y mette le prix, un manipulateur parviendra toujours à obtenir les données personnelles d'un tiers. Pourtant, malgré le peu de garanties qu'elles offrent, ces données continuent à servir de méthodes d'identification pour les banques, les services publics et autres services. C'est pour cette raison que l'usurpation d'identité est le délit dont le taux de croissance est le plus rapide à l'heure actuelle.

9-9 Informations sur la structure de l'entreprise

Règle. Les détails de la structure d'une entreprise ne doivent être communiqués à personne d'autre qu'aux salariés de l'entreprise.

Notes/explication. Les informations sur la structure de l'entreprise peuvent être présentées sous forme d'organigrammes, de listes de salariés par service, de listes d'intitulés de postes ou de fonctions dans l'entreprise, de numéros de téléphone internes, etc.

La première phase d'une attaque consiste généralement à obtenir des informations sur la structure interne d'une entreprise. Ces informations sont ensuite analysées pour mettre au point un plan d'attaque. L'assaillant peut également analyser cette structure pour déterminer quels salariés sont susceptibles d'avoir accès aux informations qu'il cherche. Lors de l'attaque, les informations dont dispose l'assaillant lui permettent plus facilement de se faire passer pour un collègue auprès de sa victime, ce qui augmente ses chances de succès.

9-10 Informations privées sur les salariés

Règle. Toute demande concernant des informations privées sur un salarié doit être transmise au service des ressources humaines.

Notes/explication. Une exception possible à cette règle est le numéro de téléphone d'un salarié qui doit être fréquemment contacté pour des raisons professionnelles, comme dans le cas des télétravailleurs. Toutefois, il est toujours préférable de s'enquérir du numéro de téléphone de la personne qui formule la demande et de la rappeler à ce numéro.

Utilisation des ordinateurs

10-1 Saisie de commandes sur un ordinateur

Règle. Aucun salarié de l'entreprise ne doit exécuter de commandes sur un ordinateur ou un autre système informatique à la demande d'un tiers, sauf s'il s'agit d'un employé du service informatique dont l'identité a été vérifiée.

Notes/explication. Il est courant pour les manipulateurs de demander à un salarié d'exécuter une commande qui provoque un changement dans la configuration du système : ainsi, l'assaillant peut s'introduire sans authentification dans l'ordinateur de la victime ou obtenir des informations dont il pourra se servir dans le cadre d'une attaque technique.

10-2 Noms internes des systèmes informatiques

Règle. Les salariés ne doivent pas dévoiler les noms internes des systèmes informatiques ni des bases de données sans vérifier au préalable que la personne qui en fait la demande appartient bien partie de l'entreprise.

Notes/explication. Les manipulateurs tenteront parfois de se faire communiquer les noms des systèmes informatiques de l'entreprise ; la connaissance de ces noms leur permettra ensuite d'appeler l'entreprise et de se faire passer pour un salarié qui a des problèmes pour utiliser l'un des systèmes ou y accéder. La connaissance des noms internes des systèmes augmente la crédibilité du manipulateur.

10-3 Demande d'exécution de programmes

Règle. Aucun salarié de l'entreprise ne doit exécuter de programme sur un ordinateur à la demande d'un tiers, sauf s'il s'agit d'un salarié du service informatique dont l'identité a été vérifiée.

Notes/explication. Toute demande d'exécution d'un programme ou d'une application doit être refusée, à moins que la personne qui formule une requête soit identifiée de manière sûre comme faisant partie du service informatique de l'entreprise. Si la demande implique de révéler des informations confidentielles (qui se trouvent par exemple dans un message électronique ou dans un fichier), la réponse à cette demande doit respecter les règles en

matières de communication d'informations confidentielles. Voir la section Communication d'informations confidentielles.

Les pirates informatiques peuvent inciter un interlocuteur à exécuter des programmes qui leur donnent accès au système informatique. Le programme exécuté par le salarié peut donner la possibilité à l'assaillant de prendre le contrôle de l'ordinateur de sa victime. Ce programme peut aussi enregistrer chacune des actions de la victime et envoyer ces informations à l'assaillant. Le manipulateur peut inciter une personne à exécuter sur son ordinateur des instructions qui peuvent causer des dégâts. De même, une attaque qui utilise des moyens techniques peut faire en sorte que le système d'exploitation de l'ordinateur exécute des instructions qui peuvent causer des dégâts similaires.

10-4 Téléchargement et installation de logiciels

Règle. Aucun salarié de l'entreprise ne doit télécharger ni installer de logiciels sur un ordinateur à la demande d'un tiers, sauf s'il s'agit d'un salarié du service informatique dont l'identité a été vérifiée.

Notes/explication. Les salariés doivent se tenir sur leurs gardes quand on leur demande d'effectuer une opération inhabituelle sur leur ordinateur (ou celui d'un autre).

Une tactique courante, pour les manipulateurs, consiste à inciter leur victime à télécharger et à installer un logiciel qui leur donnera ensuite les moyens de pénétrer les défenses du système informatique visé. Dans certains cas, le logiciel pourra également espionner le salarié à son insu ou permettre au manipulateur de prendre le contrôle de l'ordinateur à distance.

10-5 Envoi de mots de passe par courrier électronique

Règle. Aucun mot de passe ne sera envoyé par courrier électronique sans cryptage du message.

Notes/explication. L'envoi de mots de passe par courrier électronique est à éviter ; il peut cependant être employé par des sites de commerce électronique dans certaines circonstances précises :

- envoi de mots de passe à des clients qui se sont enregistrés auprès du site ;
- envoi de mots de passe à des clients ayant perdu ou oublié leur mot de passe.

10-6 Logiciels de sécurité

Règle. Aucun salarié ne doit désinstaller ni désactiver les pare-feu, les logiciels antivirus et de protection contre les "troyens", ni aucun autre logiciel de sécurité sans accord préalable du service informatique.

Notes/explication. Certains utilisateurs désactivent d'eux-mêmes les logiciels de sécurité en pensant améliorer ainsi les performances de leur ordinateur.

Par ailleurs, un manipulateur pourra tenter d'inciter un salarié à désinstaller ou désactiver des logiciels qui servent à protéger son ordinateur contre des attaques.

10-7 Installation de modems

Règle. Aucun modem ne doit être connecté à aucun ordinateur sans accord préalable du service informatique.

Notes/explication. Il est important de prendre conscience du fait que des modems raccordés à des postes de travail représentent une grave menace pour la sécurité, surtout s'ils sont connectés au réseau de l'entreprise. Pour cette raison, il est nécessaire de respecter les règles en matière de connexion de modems.

Les pirates utilisent une technique nommée *WarDialing* pour tenter d'identifier les modems actifs d'une plage de numéros de téléphone donnée. La même technique peut être employée pour détecter quels numéros, parmi ceux attribués à une entreprise, sont raccordés à un modem. Un assaillant peut facilement compromettre la sécurité du réseau de l'entreprise s'il parvient à identifier un modem qui utilise un logiciel d'accès distant vulnérable configuré avec un mot de passe facile à deviner, ou sans mot de passe du tout.

10-8 Modems et réponse automatique

Règle. Tous les employés dont le poste dispose d'un modem agréé par le service informatique doivent désactiver la fonction de réponse automatique pour éviter que quiconque puisse se connecter au modem à partir de l'extérieur.

Notes/explication. Lorsque c'est possible, le service informatique doit mettre en place une série de modems partagés pour les salariés qui doivent se connecter à des systèmes informatiques extérieurs *via* un modem.

10-9 Outils de piratage

Règle. Aucun salarié ne doit télécharger ni utiliser un programme destiné à contrer les mécanismes de protection des logiciels.

Notes/explication. Internet comprend des centaines de sites dont la vocation est de proposer des programmes qui permettent de "cracker" les protections des logiciels *shareware* et commerciaux. L'utilisation de tels logiciels va à l'encontre des droits de copyright des auteurs de logiciels, mais surtout, elle est extrêmement dangereuse. Dans la mesure où ces logiciels proviennent de sources inconnues, ils peuvent contenir du code malveillant caché qui peut endommager l'ordinateur de l'utilisateur ou faire office de "troyen" et permettre à une personne extérieure de prendre le contrôle de l'ordinateur de l'utilisateur.

10-10 Diffusion en ligne d'informations sur l'entreprise

Règle. Les salariés ne doivent diffuser sur aucun forum public ni aucune liste de diffusion des informations concernant les logiciels ou l'équipement informatique de l'entreprise, et ne fournir aucune coordonnée contrevenant aux règles de sécurité.

Notes/explication. Les messages envoyés sur des forums (qu'il s'agisse de forums Web ou Usenet) ou sur des listes de diffusion peuvent être exploités par les assaillants lors de la phase de recherche d'informations. Au cours de cette phase, l'assaillant explore Internet pour y chercher tout renseignement utile sur l'entreprise, ses produits ou ses salariés.

Certains messages peuvent contenir des informations très utiles aux assaillants. Imaginons qu'un administrateur système pose par exemple une question portant sur la configuration des filtres d'un pare-feu d'une marque ou d'un type particulier. Un assaillant qui découvre ce message est susceptible d'en déduire des informations importantes sur le pare-feu de l'entreprise et éventuellement d'imaginer un moyen de le contourner afin d'accéder au réseau interne de l'entreprise.

Une solution à ce problème consiste à mettre en place une règle autorisant les salariés à poster des messages sur les forums à partir de comptes anonymes qui ne permettent pas d'identifier l'entreprise dont ils sont issus. Bien entendu, cette règle devra également exiger que les messages soient dépourvus de toute coordonnée par laquelle on pourrait identifier l'entreprise.

10-11 Disquettes et autres supports électroniques

Règle. Un support électronique tel qu'une disquette ou un CD-ROM trouvés dans les locaux de l'entreprise et d'origine inconnue ne doit être inséré dans aucun système informatique.

Notes/explication. L'une des méthodes employées par les assaillants pour installer du code malveillant sur un ordinateur de l'entreprise consiste à copier des programmes sur des disquettes ou des CD-ROM et à noter sur leurs étiquettes des noms incitant à la curiosité (par exemple "Salaires - confidentiel"). Ils en laissent ensuite "traîner" plusieurs exemplaires dans l'entreprise. Il suffit alors qu'un seul salarié insère la disquette ou le CD-ROM dans son ordinateur pour que le code malveillant de l'assaillant soit exécuté et crée par exemple un *backdoor* (une "porte dérobée") qui donne la possibilité de pénétrer le système, ou qu'il cause des dégâts sur le réseau.

10-12 Élimination des supports électroniques amovibles

Règle. Avant de jeter tout support électronique ayant jamais contenu des informations sensibles, il faut le démagnétiser ou le rendre définitivement inutilisable, même si les informations ont été effacées au préalable.

Notes/explication. Même si la destruction de documents est aujourd'hui appliquée de manière courante, les salariés négligeront peut-être la menace que représente le fait de jeter simplement des supports électroniques à la poubelle alors qu'ils ont contenu par le passé des informations sensibles. Les employés peuvent supposer que le fait d'effacer des fichiers suffit à empêcher qu'ils puissent être récupérés. Cette supposition est erronée et peut mener à des fuites d'informations. Par conséquent, tout support électronique contenant ou ayant contenu des informations sensibles doit être effacé ou détruit en respectant les procédures définies par le groupe responsable.

10-13 Protection des économiseurs d'écran par mot de passe

Règle. Tous les salariés doivent définir un mot de passe pour leur économiseur d'écran, ainsi qu'un délai d'inactivité après lequel l'ordinateur passe en mode économiseur d'écran ou veille.

Notes/explication. Tous les salariés doivent mettre en place un mot de passe pour leur économiseur d'écran et configurer leur ordinateur pour que l'économiseur d'écran soit activé après dix minutes d'inactivité. L'objet de cette règle est d'empêcher toute personne non autorisée d'utiliser l'ordinateur de quelqu'un d'autre. Elle empêche aussi les personnes qui se seraient introduites dans les locaux de se servir des ordinateurs des salariés en leur absence.

10-14 Engagement écrit sur la non-communication des mots de passe

Règle. Avant d'obtenir un compte d'utilisateur, tout salarié ou fournisseur doit s'engager par écrit à ne jamais révéler à personne le mot de passe qu'il utilise.

Notes/explication. Cet engagement doit également mentionner les sanctions disciplinaires auxquelles s'expose le salarié au cas où il communiquerait son mot de passe à un tiers.

Utilisation du courrier électronique

11-1 Pièces jointes de messages électroniques

Règle. Les pièces jointes de messages électroniques ne doivent jamais être ouvertes, sauf si le salarié avait prévu d'en recevoir ou qu'elles proviennent d'une personne de confiance.

Notes/explication. Toutes les pièces jointes de messages électroniques doivent être traitées avec prudence. Vous pourriez exiger que tout envoi de pièce jointe soit précédé par la notification d'un tel envoi par une personne de confiance, sans quoi la pièce jointe ne devra pas être ouverte. Vous réduisez ainsi le risque que représentent les manipulateurs qui parviennent à convaincre leurs interlocuteurs d'ouvrir une pièce jointe.

L'une des méthodes qui permettent de compromettre la sécurité d'un système informatique consiste à inciter un salarié à exécuter un programme malveillant qui crée une vulnérabilité et offre la possibilité à l'assaillant de pénétrer dans le système. Un courrier électronique avec une pièce jointe contenant du code ou une macro malveillants peut donner à l'assaillant le contrôle de l'ordinateur du destinataire.

Un manipulateur pourra envoyer à sa victime un courrier électronique comprenant une pièce jointe, puis inciter la victime à ouvrir la pièce jointe.

11-2 Transfert automatique de courrier électronique

Règle. Le transfert automatique du courrier électronique à destination d'une adresse externe est interdit.

Notes/explication. L'objet de cette règle est d'empêcher des personnes extérieures à l'entreprise de recevoir du courrier envoyé à une adresse électronique de l'entreprise.

Il arrive que des salariés mettent en place le transfert du courrier entrant vers une adresse électronique extérieure pendant les périodes où ils sont absents. Il peut également arriver qu'un assaillant parvienne à convaincre un salarié de mettre en place une adresse électronique interne qui transfère les messages vers une adresse externe. L'assaillant se fera ensuite passer pour un membre du personnel de l'entreprise et demandera qu'on lui envoie des informations sensibles à l'adresse interne de l'entreprise, informations qui seront automatiquement transférées à l'extérieur de l'entreprise.

11-3 Transfert de courrier électronique

Règle. Pour toute demande de transfert d'un message électronique de la part d'une personne non vérifiée et à destination d'une autre personne non vérifiée n'a pas été vérifiée non plus, il faut au préalable confirmer l'identité de la personne qui formule la requête.

11-4 Vérification du courrier électronique

Règle. Tout message électronique qui semble provenir d'une personne de confiance et demande la communication d'informations sensibles ou l'exécution d'une action sur un ordinateur nécessite une authentification supplémentaire. Voir les procédures de vérification et d'autorisation.

Notes/explication. Un assaillant peut facilement falsifier un message électronique et son en-tête pour donner l'impression qu'il provient d'une autre adresse que la sienne. Un assaillant peut également envoyer, à partir d'un système qui a déjà été forcé, un message électronique qui autorise soi-disant à divulguer une information ou à exécuter une action. L'examen de l'en-tête d'un message électronique ne permet pas de déterminer de manière sûre son origine.

Utilisation du téléphone

12-1 Participation aux questionnaires téléphoniques

Règle. Les salariés ne participeront à aucun questionnaire téléphonique provenant de l'extérieur de l'entreprise. Toute demande de ce type sera transmise au service des relations publiques.

Notes/explication. Une méthode utilisée par les manipulateurs pour obtenir des informations consiste à appeler un salarié d'une entreprise et à prétendre qu'ils réalisent une étude. La proportion de salariés qui sont prêts à fournir des informations sur l'entreprise et sur eux-même pour les besoins (supposés) d'une étude est surprenante. Entre deux questions innocentes, l'assaillant insérera toujours des questions concernant les informations qu'il souhaite obtenir. Ces informations seront ensuite exploitées pour compromettre la sécurité du réseau de l'entreprise.

12-2 Communication des numéros de téléphone internes

Règle. Lorsqu'une personne non vérifiée demande le numéro interne d'un salarié, ce dernier doit se demander si son interlocuteur a véritablement besoin de le connaître.

Notes/explication. L'objet de cette règle est de faire en sorte que la communication d'un numéro de téléphone direct à un tiers non identifié soit un acte réfléchi. Lorsque l'interlocuteur n'a pas véritablement besoin de connaître le numéro de la ligne directe du salarié, mieux vaut lui demander de passer par le standard.

12-3 Mots de passe sur les boîtes vocales

Règle. Il est interdit de laisser un message qui contient des informations concernant un mot de passe sur quelque boîte vocale ou répondeur que ce soit.

Notes/explication. Les manipulateurs parviennent souvent à accéder aux boîtes vocales des salariés parce que celles-ci sont en général uniquement protégées par un code facile à deviner. Un type d'attaque possible consiste, pour l'assaillant, à créer une fausse boîte vocale à son nom, puis à convaincre un salarié de l'entreprise de laisser un message qui contient des informations concernant un mot de passe. Cette règle empêche l'utilisation de ce genre de stratagème.

Utilisation du fax

13-1 Transmission de fax

Règle. Aucun fax ne doit être reçu puis transmis à un tiers sans vérification préalable de l'identité de la personne qui formule la requête.

Notes/explication. Un manipulateur parviendra parfois à convaincre un salarié de faxer des informations sensibles à destination d'un fax situé dans les locaux de l'entreprise. Auparavant, il aura prévenu un autre salarié situé à proximité du fax de destination, généralement une secrétaire ou un assistant administratif, qu'un fax doit lui parvenir à ce numéro et qu'il passera le chercher. Ensuite, une fois le fax arrivé à destination, l'assaillant demandera au salarié de le lui réexpédier sous un prétexte quelconque (réunion urgente, par exemple). Le salarié, qui n'aura généralement pas conscience de l'importance des informations que contient le fax, obtempérera.

13-2 Vérification des autorisations faxées

Règle. Avant d'exécuter quelque instruction que ce soit qui est reçue par télécopie, le destinataire du fax doit s'assurer que l'expéditeur est un salarié ou une personne de confiance. Pour cela, il suffit généralement de téléphoner à l'expéditeur.

Notes/explication. Les salariés doivent être prudents quand ils reçoivent des requêtes inhabituelles par fax (on leur demande par exemple de fournir

certains renseignements ou d'exécuter certaines opérations sur leur ordinateur). Les données contenues dans l'en-tête du fax peuvent être falsifiées ; il suffit pour cela de modifier les paramètres de l'appareil émetteur. L'en-tête d'un fax ne doit donc pas servir à vérifier une identité ou une autorisation.

13-3 Envoi d'informations sensibles par fax

Règle. Avant de transmettre des informations sensibles par fax à destination d'une machine située dans une zone accessible à d'autres personnes, l'expéditeur enverra la première page du fax seule. À la réception de cette page, le destinataire lui répondra en envoyant une autre page, afin de prouver qu'il se trouve à proximité du fax. Ce n'est qu'ensuite qu'il pourra recevoir le reste du fax.

Notes/explication. On utilise cette procédure pour vérifier que le destinataire est physiquement présent à proximité de l'appareil de destination. De plus, elle permet de s'assurer que la ligne du fax n'a pas été configurée pour transférer l'appel vers une destination tierce.

13-4 Interdiction d'envois de mots de passe par fax

Règle. Un mot de passe ne pourra sous aucun prétexte être envoyé par fax.

Notes/explication. L'envoi d'informations d'authentification par fax n'est pas sûr. En général, différents salariés peuvent accéder aux appareils de télécopie. De plus, les fax dépendent du réseau téléphonique commuté, qui peut être manipulé de sorte que les appels à destination d'un appareil de télécopie soient transférés vers un autre numéro contrôlé par l'assaillant.

Utilisation des boîtes vocales

14-1 Mots de passe des boîtes vocales

Règle. Les mots de passe des boîtes vocales ne doivent sous aucun prétexte être communiqués à des tiers. Par ailleurs, il faut modifier ces mots de passe tous les trois mois au moins.

Notes/explication. Les messages laissés sur les boîtes vocales peuvent contenir des informations confidentielles. Pour protéger ces informations, les salariés doivent modifier fréquemment leur mot de passe et ne jamais le divulguer. Par ailleurs, ils ne doivent pas employer de mots de passe identiques ou similaires sur une période de douze mois consécutifs.

14-2 Mots de passe sur différents systèmes

Règle. Les utilisateurs de boîtes vocales ne doivent pas utiliser le même mot de passe sur aucun autre système téléphonique ou informatique, qu'ils soient internes ou externes.

Notes/explication. L'utilisation de mots de passe similaires ou identiques sur plusieurs systèmes, ordinateur et boîte vocale, par exemple, facilite le travail du manipulateur qui pourra aisément deviner tous les mots de passe d'un utilisateur lorsqu'il en aura identifié un.

14-3 Configuration des mots de passe des boîtes vocales

Règle. Les utilisateurs de boîtes vocales doivent créer des mots de passe difficiles à deviner. Il faut que ceux-ci ne soient liés en aucune façon à leur utilisateur et qu'ils ne correspondent pas à une structure facilement identifiable.

Notes/explication. Les mots de passe ne doivent pas être composés de séries de chiffres ou de chiffres répétés (1111, 1234, 1010), ne doivent pas être identiques à l'extension du numéro de téléphone ni semblables à celui-ci, et ne doivent être liés ni à l'adresse, ni à la date de naissance, ni à la plaque d'immatriculation, ni au numéro de téléphone, ni à aucune autre donnée personnelle de l'utilisateur.

14-4 Messages marqués comme "anciens"

Règle. Quand, dans la boîte vocale, des messages non écoutés ne sont pas signalés comme étant nouveaux, l'administrateur des boîtes vocales doit en être avisé et le mot de passe de la boîte vocale doit immédiatement être changé.

Notes/explication. Les manipulateurs disposent de nombreux moyens pour accéder à une boîte vocale. Un salarié qui s'aperçoit que des messages qu'il n'a encore jamais entendus ne sont pas signalés comme nouveaux peut supposer qu'un tiers a obtenu un accès non autorisé à la boîte vocale et a écouté ses messages.

14-5 Messages d'annonce des boîtes vocales

Règle. Les informations fournies par le message d'annonce de la boîte vocale des salariés doivent être limitées. En particulier, elles ne doivent pas indiquer les horaires de travail du salarié ni ses dates de congé.

Notes/explication. Les messages d'annonce des boîtes vocales ne doivent présenter ni le nom de famille, ni l'extension du numéro, ni la raison de l'absence du salarié (voyage d'affaires, congé, horaires de travail…). Un assaillant pourra utiliser ces informations pour mettre au point une histoire plausible qui lui donnera la possibilité de tromper d'autres salariés.

14-6 Structure des mots de passe des boîtes vocales

Règle. Les salariés ne doivent pas choisir pour leur boîte vocale un mot de passe dont une partie reste constante tandis que l'autre change selon un modèle prévisible.

Notes/explication. Il sera par exemple interdit d'utiliser des mots de passe tels que 743501, 743502, 743503, les deux derniers chiffres correspondant au numéro du mois.

14-7 Informations privées et confidentielles

Règle. Aucune information privée ni confidentielle ne devra être communiquée sous forme de message sur une boîte vocale.

Notes/explication. Le système téléphonique de l'entreprise est généralement plus vulnérable que son système informatique. Les mots de passe sont fréquemment constitués d'une série de chiffres, ce qui restreint fortement le nombre de possibilités que l'assaillant doit envisager. De plus, dans certaines entreprises, les mots de passe des boîtes vocales sont connus des secrétaires ou d'autres membres du personnel administratif qui ont pour tâche de réceptionner les messages destinés à leur supérieur hiérarchique. De ce fait, aucune information sensible ne doit être communiquée sous forme de message sur une boîte vocale.

Mots de passe

15-1 Mots de passe au téléphone

Règle. Les mots de passe ne doivent jamais être communiqués au téléphone.

Notes/explication. Des assaillants sont susceptibles d'épier la conversation téléphonique, soit en personne, soit par l'intermédiaire de moyens technologiques.

15-2 Communication des mots de passe d'ordinateurs

Règle. Le mot de passe d'un compte d'utilisateur ne doit être communiqué à un tiers sous aucun prétexte sans un accord écrit préalable du personnel du service informatique responsable de ce type de décision.

Notes/explication. Dans nombre d'attaques par manipulation, l'objectif est d'inciter des utilisateurs à divulguer leur nom d'utilisateur et leur mot de

passe. Cette règle est cruciale pour réduire le risque que représentent les attaques par manipulation contre l'entreprise. En conséquence, elle doit être scrupuleusement respectée dans toute l'entreprise.

15-3 Mots de passe Internet

Règle. Les salariés de l'entreprise ne doivent jamais utiliser sur Internet un mot de passe identique ou analogue à celui employé sur les systèmes informatiques de l'entreprise.

Notes/explication. Les opérateurs de sites Web malveillants peuvent mettre en place un site qui offre un "cadeau" de valeur ou permet prétendument de gagner un prix. En contrepartie, le visiteur doit s'enregistrer en fournissant une adresse électronique, un nom d'utilisateur et un mot de passe. Dans la mesure où beaucoup d'internautes utilisent des mots de passe et des noms d'utilisateur identiques ou similaires sur différents systèmes, l'opérateur du site Web tentera d'utiliser ces informations pour s'introduire dans le système informatique de l'utilisateur à son domicile ou à son travail. L'ordinateur dont se sert le visiteur sur son lieu de travail peut parfois être identifié grâce à l'adresse électronique qu'il a saisie lorsqu'il s'est enregistré sur le site Web.

15-4 Mots de passe sur différents systèmes

Règle. Les salariés ne doivent jamais utiliser les mêmes mots de passe ou des mots de passe analogues sur différents systèmes. Cette règle est valable quel que soit le système (ordinateur ou boîte vocale, routeur ou pare-feu) et son emplacement (à domicile ou sur le lieu de travail), et s'applique également aux logiciels (bases de données et applications).

Notes/explication. Pour tenter de pénétrer les réseaux informatiques, les assaillants exploitent les faiblesses humaines. Ils savent que pour éviter d'avoir à retenir plusieurs mots de passe, beaucoup d'utilisateurs ont recours à des mots de passe identiques ou similaires pour chacun des systèmes auxquels ils accèdent. Par conséquent, les assaillants commenceront par tenter d'obtenir le mot de passe utilisé par la cible sur l'un des systèmes auxquels elle a accès. Ce mot de passe, ou l'une de ses variantes, leur donnera presque à coup sûr la possibilité d'accéder à d'autres appareils et systèmes dont se sert le salarié.

15-5 Réutilisation de mots de passe

Règle. Aucun utilisateur n'emploiera à plusieurs reprises le même mot de passe ou un mot de passe analogue dans un délai de dix-huit mois.

Notes/explication. Le fait de changer fréquemment de mot de passe permet de réduire les dommages potentiels que pourrait causer un assaillant ayant découvert le mot de passe d'un utilisateur. Quand le nouveau mot de passe est sans rapport avec l'ancien, l'assaillant ne peut pas le deviner aussi facilement.

15-6 Mots de passe conçus sur un même modèle

Règle. Les salariés ne doivent pas choisir un mot de passe dont une partie reste identique tandis que l'autre change de manière prévisible.

Notes/explication. Il sera par exemple interdit d'utiliser des mots de passe tels que thomas01, thomas02, thomas03, les deux derniers chiffres correspondant au numéro du mois.

15-7 Règles pour la création des mots de passe

Règle. Les mots de passe choisis par les utilisateurs doivent respecter certains critères, qui sont les suivants :

- Avoir une longueur d'au moins huit caractères pour les comptes d'utilisateurs standard et d'au moins douze caractères pour les comptes privilégiés.
- Contenir à la fois des majuscules, des minuscules, au moins un symbole ($, _, ! ou &, par exemple) et au moins un chiffre, pour peu que ces caractères soient possibles.
- Ne pas faire partie du dictionnaire de quelque langue que ce soit et n'être lié en aucune façon à l'entreprise ou à l'utilisateur : famille du salarié, loisirs, voiture, plaque d'immatriculation, numéro de sécurité sociale, adresse, numéro de téléphone, nom d'animaux familiers, etc., sont donc exclus.
- Ne pas être une variante d'un mot de passe précédemment employé, une partie du mot de passe étant identique tandis que l'autre change : seront donc interdits de mots de passe tels que thomas, thomas2, thomas3 ou thomasjanv, thomasfevr, thomasmars.

Notes/explication. Quand les critères ci-dessus sont respectés, l'assaillant peut difficilement deviner le mot de passe. Une technique pour générer des mots de passe plus faciles à mémoriser consiste à faire alterner voyelles et consonnes dans le mot, selon le modèle "CVCVCVCV", ce qui donnera des mots de passe tels que MIXOCASO ou CUSOJENA.

15-8 Mots de passe notés sur papier

Règle. Les salariés ne doivent noter un mot de passe sur papier que s'ils le gardent ensuite en lieu sûr, et jamais à proximité de l'ordinateur ou de l'appareil protégé par mot de passe.

Notes/explication. Il est conseillé de dissuader les salariés de noter leurs mots de passe sur papier. Dans certaines situations, toutefois, il ne sera pas possible de faire autrement, par exemple dans le cas d'un utilisateur qui dispose de plusieurs comptes sur plusieurs systèmes. Les mots de passe notés sur papier doivent être stockés en lieu sûr, toujours à l'écart de l'ordinateur. Un mot de passe ne devra sous aucun prétexte être collé sur le moniteur ou placé sous le clavier.

15-9 Mots de passe stockés en clair sur un ordinateur

Règle. Les mots de passe ne doivent jamais être stockés en clair sur un ordinateur, ni sous la forme d'un texte qui apparaît quand on appuie sur une touche de fonction. Lorsqu'il est nécessaire de stocker un mot de passe sur un ordinateur, il faut pour cela recourir à un utilitaire de cryptage agréé par le service informatique afin d'empêcher toute divulgation non autorisée.

Notes/explication. Un assaillant peut facilement retrouver un mot de passe stocké sur un ordinateur dès lors qu'il n'est pas crypté, que ce mot de passe soit stocké en tant que fichier texte, fichier *batch*, touche de fonction de terminal, fichier d'ouverture de session, macro, script ou fichier quelconque contenant les mots de passe qui donnent accès à des serveurs FTP.

RÈGLES CONCERNANT LES TÉLÉTRAVAILLEURS

Les télétravailleurs se trouvent à l'extérieur du pare-feu de l'entreprise et sont par conséquent plus vulnérables aux attaques. Les règles ci-après permettront d'éviter que des manipulateurs utilisent des télétravailleurs en tant que point d'accès à vos données.

16-1 Clients légers

Règle. Tout personne employée par l'entreprise et qui est autorisée à se connecter au réseau de l'entreprise au moyen d'un accès à distance doit utiliser à cette fin un client léger.

Notes/explication. Quand un assaillant élabore une stratégie d'attaque, il tente d'identifier des utilisateurs qui ont accès au réseau de l'entreprise à partir de l'extérieur. Les télétravailleurs sont par conséquent des cibles privilégiées. Leurs ordinateurs sont généralement moins bien protégés et ils peuvent constituer le maillon faible qui donnera la possibilité de pénétrer le réseau de l'entreprise.

Tout ordinateur connecté à un réseau protégé peut être "piégé de l'intérieur" à l'aide d'un logiciel furtif qui enregistre les frappes au clavier ; la ligne elle-même peut être piratée. Une solution possible à ces problèmes consiste à faire appel à un client léger. Un client léger est assimilable à un poste de travail sans disque ou à un terminal : l'ordinateur distant ne dispose d'aucune possibilité de stockage et le système d'exploitation, les applications et les données se trouvent toutes sur le réseau. L'accès au réseau par l'intermédiaire d'un client léger réduit de manière significative le risque que représentent les systèmes non patchés ou trop anciens et un code malveillant éventuellement installé sur l'ordinateur de l'utilisateur. La gestion du problème de sécurité que représentent les télétravailleurs est plus simple quand elle peut être centralisée. Plutôt que de faire dépendre de télétravailleurs inexpérimentés la protection du réseau de l'entreprise, il est préférable de déléguer ce type de responsabilité aux administrateurs système ou réseau qui ont reçu une formation.

16-2 Logiciels de sécurité pour télétravailleurs

Règle. Tout ordinateur extérieur que l'on connecte au réseau de l'entreprise doit être équipé de logiciels antivirus et anti-troyens, ainsi que d'un pare-feu (logiciel ou matériel). Les fichiers de définition de virus et de troyens doivent être mis à jour au moins une fois par semaine.

Notes/explication. Les télétravailleurs ne sont généralement pas expérimentés en matière de sécurité, et ils ne mettent pas toujours en œuvre des moyens suffisants pour protéger leur ordinateur, ce qui peut permettre à un assaillant d'accéder au réseau de l'entreprise. Les télétravailleurs représentent donc un danger potentiel s'ils ne sont pas formés. En plus des logiciels antivirus et anti-troyens, il est nécessaire d'installer un pare-feu pour empêcher des utilisateurs malveillants d'avoir accès à des services qui seraient activés sur l'ordinateur du télétravailleur.

Une anecdote concernant Microsoft vous convaincra peut-être de la nécessité de prendre au sérieux le risque potentiel que représentent les télétravailleurs. Un ordinateur appartenant à un télétravailleur employé par Microsoft a été infecté par un troyen. Le ou les assaillants ont ensuite réussi à utiliser la connexion de ce télétravailleur pour se connecter au réseau de développement de Microsoft et y dérober une partie du code source d'un produit en cours de développement.

RÈGLES CONCERNANT LE SERVICE DES RESSOURCES HUMAINES

Le service des ressources humaines a une responsabilité particulière : celle de protéger les informations personnelles des salariés de l'entreprise. Une autre de ses responsabilités est de protéger l'entreprise des actes d'anciens salariés mécontents.

17-1 Salariés quittant l'entreprise

Règle. Lorsqu'un salarié quitte l'entreprise, de son plein gré ou non, le service des ressources humaines doit immédiatement :

- supprimer l'enregistrement concernant la personne dans le répertoire en ligne des salariés et désactiver ou faire transférer sa boîte vocale ;
- informer le personnel d'accueil, à l'entrée des locaux ;
- ajouter le nom du salarié à la liste des salariés qui quittent l'entreprise, laquelle doit être envoyée à tous les salariés au moins une fois par semaine.

Notes/explication. Le personnel d'accueil, qui se trouve à l'entrée des locaux, doit être informé quand des employés quittent l'entreprise, afin d'éviter que d'anciens salariés puissent entrer librement dans l'entreprise. Par ailleurs, le fait d'informer les autres salariés permet d'éviter qu'un ancien salarié puisse prétendre faire partie de l'entreprise afin d'essayer d'inciter d'anciens collègues à agir d'une manière qui soit dommageable pour la société.

Dans certaines circonstances, il peut être nécessaire de demander à chacun des utilisateurs de l'entreprise de changer de mot de passe (ce qu'a décidé de faire la direction de l'opérateur téléphonique GTE après m'avoir licencié au seul prétexte que j'étais un hacker connu…).

17-2 Notification auprès du service informatique

Règle. Lorsqu'un salarié quitte l'entreprise, de son plein gré ou non, le service des ressources humaines doit immédiatement le signaler au service informatique afin que celui-ci désactive tous les comptes de ce salarié, y compris ceux employés pour l'accès aux bases de données, l'accès à distance, etc.

Notes/explication. Il est essentiel de désactiver l'accès d'un salarié à tous les systèmes informatiques dès son départ. Un ancien salarié mécontent dont les comptes n'auraient pas été désactivés pourrait accéder aux réseaux de l'entreprise et y causer de sérieux dommages.

17-3 Informations confidentielles utilisées lors du recrutement

Règle. Les petites annonces et les autres formes que peuvent prendre les offres d'emploi doivent, dans la mesure du possible, être rédigées de telle manière que le matériel et les logiciels informatiques utilisés dans l'entreprise n'y soient pas mentionnés.

Notes/explication. En ce qui concerne l'équipement informatique de l'entreprise, les recruteurs ne doivent divulguer que les informations strictement nécessaires pour attirer les candidats qualifiés.

Les pirates informatiques lisent les journaux ainsi que les communiqués de presse et visitent les sites Web en y cherchant les offres d'emploi. Souvent, pour attirer des candidatures, les entreprises dévoilent trop d'informations sur le matériel et les logiciels qu'elles utilisent. Une fois que l'assaillant connaît les systèmes informatiques de sa cible, il peut passer à la phase suivante de son attaque. Par exemple, si un assaillant sait qu'une entreprise utilise le système d'exploitation VMS, il peut, sous un prétexte quelconque, se faire indiquer le numéro de version utilisé dans l'entreprise, puis envoyer un faux correctif à installer d'urgence qui semblera provenir de l'éditeur. Une fois le correctif installé, l'assaillant aura accès aux ordinateurs de l'entreprise.

17-4 Informations personnelles sur les salariés

Règle. Le service des ressources humaines ne doit jamais divulguer d'informations personnelles concernant un salarié ou ex-salarié, sous-traitant, consultant, intérimaire ou stagiaire, sauf accord écrit spécifique du directeur des ressources humaines.

Notes/explication. Les chasseurs de têtes, les détectives privés et les usurpateurs d'identité ciblent toujours des informations telles que les numéros de sécurité sociale, les dates de naissance, l'historique des salaires, les coordonnées bancaires, etc. Les manipulateurs se font en effet passer pour l'individu auquel ces informations sont relatives. Par ailleurs, les noms des nouvelles recrues sont particulièrement intéressants pour les voleurs d'informations. Les nouvelles recrues sont plus susceptibles de satisfaire à des demandes qui proviennent de soi-disant supérieurs hiérarchiques ou de personnes qui prétendent faire partie du personnel de sécurité de l'entreprise.

17-5 Vérification des antécédents

Règle. Une vérification des antécédents doit être obligatoire pour tous les candidats recrutés, ainsi que pour les consultants, travailleurs intérimaires ou stagiaires avant la signature d'un contrat de travail.

Notes/explication. Pour des questions de coût, les recherches détaillées portant sur les antécédents d'une recrue pourront être limitées aux postes à responsabilité. Notez toutefois que n'importe quelle personne ayant physiquement accès aux locaux de l'entreprise représente un danger potentiel. Ainsi, le personnel d'entretien a accès aux bureaux du personnel et par conséquent aux ordinateurs qui s'y trouvent. Un assaillant qui dispose d'un accès physique à un ordinateur peut y installer en moins d'une minute un utilitaire capable d'enregistrer tout ce qui est saisi par l'utilisateur, et par conséquent les mots de passe.

Les pirates informatiques vont parfois jusqu'à se faire embaucher pour accéder aux systèmes informatiques et au réseau de l'entreprise ciblée. Un assaillant pourra facilement obtenir le nom de la société de nettoyage en appelant la société ciblée et en prétendant faire partie d'une autre société de nettoyage qui cherche de nouveaux clients.

RÈGLES CONCERNANT LA SÉCURITÉ PHYSIQUE

Bien que les manipulateurs cherchent à éviter de se présenter en personne dans l'entreprise qu'ils visent, il arrive qu'ils aillent jusqu'à pénétrer dans vos locaux. Les règles qui suivent vous aideront à empêcher les intrusions physiques.

18-1 Identification du personnel extérieur à l'entreprise

Règle. Les livreurs et autres personnes extérieures à l'entreprise qui ont régulièrement besoin d'entrer dans les locaux doivent être munis d'un badge spécial ou d'une autre forme d'identification en accord avec les règles de sécurité.

Notes/explication. Les personnes extérieures à l'entreprise qui ont régulièrement besoin d'entrer dans les locaux (pour des livraisons de boissons ou de nourriture à la cafétéria, pour réparer des photocopieuses ou installer des téléphones, par exemple) doivent être munies d'un badge d'identification spécifique. Celles qui ne sont présentes qu'à titre occasionnel doivent être traitées comme des visiteurs et ne doivent jamais être laissées seules.

18-2 Identification des visiteurs

Règle. Tout visiteur doit présenter une pièce d'identité en règle comprenant une photo avant de pouvoir pénétrer à l'intérieur des locaux.

Notes/explication. L'agent de sécurité ou le réceptionniste doit faire une photocopie du papier d'identité du visiteur avant de lui fournir un badge, et cette copie doit être rangée avec le nom et la signature fournis par le visiteur. Une autre solution consiste à faire noter par le réceptionniste les données présentes sur la pièce d'identité du visiteur ; celles-ci ne doivent pas être notées par le visiteur lui-même.

Les manipulateurs qui cherchent à pénétrer dans un bâtiment indiqueront toujours de fausses données quant à leur identité si on leur en laisse la possibilité. Il n'est pas très difficile pour un manipulateur d'obtenir de faux papiers ainsi que le nom d'un salarié avec lequel il peut prétendre avoir rendez-vous, mais le fait de noter les coordonnées d'une personne d'après ses papiers d'identité ajoute un niveau de sécurité.

18-3 Accompagnement des visiteurs

Règle. Les visiteurs doivent être accompagnés en permanence lorsqu'ils se trouvent dans les locaux de l'entreprise.

Notes/explication. Une astuce courante utilisée par les manipulateurs consiste à obtenir un rendez-vous avec un salarié de l'entreprise pour une raison quelconque. À la fin de son entrevue avec ce salarié, le manipulateur dira qu'il trouvera lui-même le chemin de la sortie. Il sera alors libre de se déplacer à sa guise dans les locaux et éventuellement d'accéder à des informations sensibles.

18-4 Badges provisoires

Règle. Les salariés qui viennent d'un autre site et ne sont pas munis de leur badge personnel doivent présenter une pièce d'identité comportant une photo et être munis d'un badge provisoire.

Notes/explication. Les assaillants se font souvent passer pour des salariés d'un autre bureau ou d'un autre bâtiment de la même société afin de pouvoir entrer dans les locaux.

18-5 Évacuation d'urgence

Règle. En cas d'évacuation d'urgence ou d'exercice d'évacuation, le personnel de sécurité doit s'assurer que plus personne ne se trouve à l'intérieur des locaux.

Notes/explication. Le personnel de sécurité doit vérifier l'absence de retardataires dans les bureaux ou les salles de repos. Avec l'autorisation des pompiers de l'entreprise (ou des responsables de la sécurité), le personnel de sécurité doit prêter attention aux personnes qui pourraient quitter les locaux longtemps après l'évacuation.

Les espions industriels et même les pirates informatiques sont capables de provoquer une diversion pour accéder à un bâtiment ou à une zone sécurisée. Les techniques utilisées peuvent consister à diffuser un gaz inoffensif, le butyl mercaptan, dont l'odeur rappelle celle du gaz naturel, ou à déclencher des fumigènes. Une fois que le personnel commence les procédures d'évacuation, l'assaillant utilise cette diversion pour voler des informations ou accéder aux systèmes informatiques de l'entreprise. Une autre technique est de se cacher dans les toilettes ou dans un placard lors d'un exercice d'évacuation planifié et d'attendre que le personnel ait quitté les locaux.

18-6 Visiteurs dans la salle du courrier

Règle. Aucun visiteur non accompagné n'est autorisé à se rendre dans la salle du courrier.

Notes/explication. L'objet de cette règle est d'empêcher un intrus de dérober, d'envoyer ou de substituer du courrier interne à l'entreprise.

18-7 Numéros de plaque d'immatriculation

Règle. Si l'entreprise dispose d'un parc de stationnement surveillé, le personnel de surveillance notera les numéros de plaque de tous les véhicules qui entrent dans le parking.

18-8 Poubelles

Règle. Les poubelles doivent toujours rester à l'intérieur de l'entreprise et ne doivent jamais être accessibles au public.

Notes/explication. Les poubelles sont une excellente source d'informations pour les pirates informatiques et les espions industriels. Selon les pays et les villes, la législation tolère ou non la fouille dans les poubelles mais dans tous les cas, les poubelles doivent rester à l'intérieur de l'entreprise.

RÈGLES CONCERNANT LES RÉCEPTIONNISTES

Les réceptionnistes et les standardistes sont souvent en première ligne quand il s'agit de faire face aux manipulateurs. Pourtant, il est rare qu'ils soient suffisamment formés pour identifier un intrus et l'empêcher de pénétrer dans les locaux. Les règles ci-après permettront aux réceptionnistes de mieux protéger votre entreprise et ses informations.

19-1 Annuaire interne

Règle. Les données de l'annuaire interne de l'entreprise ne doivent être divulguées qu'aux salariés de l'entreprise.

Notes/explication. Les noms, fonctions, numéros de téléphone et adresses de l'annuaire interne de l'entreprise doivent être considérés comme des informations internes et n'être divulgués qu'en respectant les règles correspondantes.

Par ailleurs, toute personne qui appelle doit citer le nom ou l'extension de la personne qu'elle cherche à contacter. Le standardiste peut transférer l'appel quand l'appelant ne connaît pas l'extension, mais dans ce cas, il ne doit pas citer le numéro d'extension.

19-2 Numéros de téléphone d'équipes et de services spécifiques

Règle. Aucun salarié ne doit divulguer le numéro de la ligne directe du service d'assistance interne de l'entreprise, du service de télécommunications, de la division d'exploitation du service informatique ou des administrateurs système, sans avoir vérifié au préalable que l'appelant a des raisons valables de contacter ces groupes ou personnes. Lorsqu'un standardiste transfère un appel vers l'un de ces numéros, il doit annoncer le nom de l'appelant.

Notes/explication. Certaines entreprises considéreront cette règle comme trop restrictive, mais elle permet d'éviter qu'un manipulateur puisse se faire passer pour un salarié en demandant un nouveau transfert d'appel vers l'intérieur de l'entreprise (dans certaines sociétés, l'appel semblera alors venir de l'intérieur de l'entreprise), ou qu'il puisse faire la démonstration de sa connaissance de l'entreprise en citant le numéro d'extension d'un salarié.

19-3 Transmission d'informations

Règle. Les standardistes ne doivent pas prendre de messages ou transmettre des informations à la demande de personnes qui ne sont pas identifiées en tant que salariés actifs de l'entreprise.

Notes/explication. L'une des ruses des manipulateurs consiste à obtenir que des tiers se portent garants pour eux à leur insu. Ainsi, un manipulateur qui connaît le numéro de téléphone d'un standardiste demandera dans un premier temps à celui-ci de prendre des messages pour lui. Il appellera ensuite la victime, se fera passer pour un collègue, demandera des informa-

tions sensibles et fournira comme numéro de téléphone celui du standard. Pour finir, il ne lui restera plus qu'à appeler le réceptionniste un peu plus tard en lui demandant si quelqu'un a laissé des messages pour lui.

19-4 Objets déposés pour être emportés

Règle. Avant de donner un objet à un coursier ou à toute autre personne non vérifiée, le réceptionniste ou l'agent de sécurité doit demander une pièce d'identité comportant une photo et noter les informations présentées sur le document en question.

Notes/explication. L'une des techniques employées par les manipulateurs consiste à demander à un salarié de fournir des documents sensibles à un autre salarié — en principe habilité à les recevoir — en les déposant à l'accueil de l'entreprise. Le personnel à l'accueil, quant à lui, croira que ces documents peuvent être confiés à des tiers. Le manipulateur pourra donc ensuite se faire remettre les documents en personne ou demander à un coursier de les prendre pour lui.

RÈGLES CONCERNANT LE GROUPE D'INFORMATION SUR LES INCIDENTS

Chaque entreprise doit mettre en place un groupe ou une équipe qui doivent être informés dès qu'une attaque contre l'entreprise est identifiée. Les règles qui suivent permettront de définir la mise en place et le fonctionnement de ce groupe.

20-1 Groupe d'information sur les incidents

Règle. Il faut désigner une personne ou un groupe en tant que responsable de l'information sur les incidents, et c'est à cette personne ou à ce groupe que les salariés doivent signaler tout incident lié à la sécurité. Tous les salariés doivent disposer des informations nécessaires pour contacter cette personne ou ce groupe.

Notes/explication. Les salariés doivent savoir identifier les menaces pour la sécurité de l'entreprise et avoir appris à signaler ces menaces au groupe d'information sur les incidents. Il est également important que l'entreprise mette en place pour ce groupe des procédures et des habilitations spécifiques afin qu'il puisse réagir lorsqu'une menace est signalée.

20-2 Attaques en cours

Règle. Dès qu'une attaque par manipulation est signalée au groupe d'information sur les incidents, ce dernier doit immédiatement déclencher les procédures prévues pour alerter tous les salariés concernés.

Notes/explication. Le groupe d'information peut également envisager d'alerter l'ensemble de l'entreprise. Une fois que la personne ou le groupe responsable est convaincu qu'une attaque est en cours, sa priorité doit être de réduire autant que possible les dommages potentiels et donc d'avertir le personnel de l'entreprise qu'il doit se tenir sur ses gardes.

Annexe

Consignes de sécurité

Les listes et graphiques qui suivent vous serviront de référence pour consulter rapidement les méthodes de manipulation dont il a été question aux Chapitres 2 à 14, ainsi que les procédures de vérification décrites au Chapitre 16. Adaptez ces informations en fonction de votre entreprise et mettez-les à disposition de vos salariés afin qu'ils puissent s'y référer lorsque se pose une question concernant la sécurité.

IDENTIFICATION DES ATTAQUES

Ces listes vous aideront à identifier une attaque par manipulation.

Cycle de la manipulation

ACTION	DESCRIPTION
Recherche	Peut porter sur des sources publiques telles que les informations déposées auprès de la Commission des Opérations en Bourse, les rapports annuels, les brochures publicitaires, les demandes de brevets, les communiqués et articles de presse, les magazines spécialisés, le contenu du site Web. Autre source possible : les poubelles.
Mise en place d'un rapport de confiance	Le manipulateur montre qu'il est "dans le coup", usurpe une identité, mentionne des noms de collègues, appelle à l'aide ou fait valoir son autorité.

ACTION	DESCRIPTION
Exploitation de la confiance	Le manipulateur demande à la victime de lui fournir des informations ou d'agir à sa place. Ou inversement, la victime est parfois manipulée de telle manière qu'elle demande de l'aide à l'assaillant.
Utilisation des informations	Si les informations obtenues ne sont qu'une étape pour atteindre l'objectif final, l'assaillant répète les manœuvres précédentes du cycle jusqu'à ce que le but soit atteint.

Méthodes de manipulation courantes

Les méthodes de manipulation suivantes sont les plus courantes :

- se faire passer pour un collègue ;
- se faire passer pour un salarié d'un fournisseur, d'un partenaire commercial ou pour un représentant des forces de l'ordre ;
- se faire passer pour un supérieur hiérarchique ;
- se faire passer pour un nouveau salarié ayant besoin d'aide ;
- se faire passer pour un fournisseur de matériel ou de logiciel proposant un correctif ou un *patch* ;
- proposer de l'aide en cas de problème, puis provoquer le problème afin que la victime fasse appel au manipulateur ;
- envoyer un logiciel gratuit ou un correctif que la victime est censée installer ;
- envoyer un virus ou un "troyen" en tant que pièce jointe d'un message électronique ;
- afficher une fausse fenêtre qui demande à l'utilisateur d'entrer de nouveau ses données d'ouverture de session ;
- enregistrer au moyen d'un utilitaire les touches sur lesquelles la victime a appuyé ;
- déposer sur les lieux de travail de la victime des disquettes ou des CD-ROM contenant un logiciel malveillant ;
- utiliser une terminologie et un jargon spécialisés pour gagner la confiance de l'interlocuteur ;
- offrir un cadeau sur un site Web afin que la victime fournisse un nom d'utilisateur et un mot de passe ;
- déposer un document ou un fichier dans la salle du courrier de l'entreprise afin qu'il semble provenir de l'intérieur de l'entreprise ;
- modifier les informations d'un en-tête d'un fax afin qu'il semble provenir de l'intérieur de l'entreprise ;
- demander au réceptionniste ou au standardiste qu'il transfère un fax ;
- demander le transfert d'un fichier vers une destination qui semble être interne à l'entreprise ;
- mettre en place une boîte vocale afin que les personnes qui rappellent l'assaillant aient l'impression de téléphoner à l'intérieur de l'entreprise ;
- demander un accès local distant au courrier électronique sous prétexte de se trouver à l'extérieur du site.

Signes pouvant indiquer qu'une attaque est en cours

Une attaque est peut-être en cours lorsque l'interlocuteur :

- refuse de fournir un numéro où on puisse le rappeler ;
- formule une demande inhabituelle ;
- fait valoir son autorité ;
- fait valoir l'urgence de la situation ;
- menace d'exercer des représailles si le correspondant ne s'exécute pas ;
- semble mal à l'aise lorsqu'il est questionné ;
- cite des noms de collègues ;
- fait des compliments ou flatte son correspondant ;
- utilise la séduction.

Cibles courantes pour des attaques

TYPE DE CIBLE	EXEMPLES
Individu qui ne connaît pas la valeur des informations	Réceptionniste, standardiste, assistant administratif, agent de sécurité

Type de cible	Exemples
Individu qui a des privilèges spéciaux	Employé du service d'assistance technique, administrateur système, opérateur de saisie, responsable télécoms
Fabricant/ fournisseur	Fabricant de matériel, éditeur de logiciels, fournisseur de systèmes de boîtes vocales
Service spécifique	Comptabilité, ressources humaines

Facteurs augmentant la vulnérabilité aux attaques

- nombre important de salariés ;
- existence de plusieurs sites ;
- messages de boîtes vocales qui fournissent des informations sur les salariés ;
- divulgation des numéros d'extensions téléphoniques ;
- absence de formation en matière de sécurité ;
- absence de système de classification des informations ;
- absence de rapports systématiques sur les incidents.

CLASSEMENT DES INFORMATIONS ET VÉRIFICATION

Ces tableaux et graphiques vous permettront de réagir de manière adéquate aux demandes susceptibles d'être des tentatives de manipulation.

Procédure de vérification d'identité

Action	Description
Identification de l'appelant	Vérifier que l'appel est interne et que le nom ou le numéro d'extension correspondent à l'identité de l'appelant
Rappel	Rechercher l'appelant dans l'annuaire de l'entreprise et le rappeler au numéro indiqué dans l'annuaire

Action	Description
Demande de garantie	Demander à une personne de confiance de se porter garante de l'identité de la personne qui formule la requête
Partage d'un secret commun	Demander à l'interlocuteur de fournir une information secrète interne à l'entreprise, par exemple le mot de passe ou le code du jour
Contact du supérieur hiérarchique	Contacter le supérieur hiérarchique immédiat de l'individu et vérifier auprès de lui l'identité et le statut de ce dernier
Demande de signature électronique	Demander un message électronique signé numériquement
Reconnaissance de la voix	Si l'interlocuteur est connu, l'identifier grâce à sa voix
Utilisation de mots de passe dynamiques	Effectuer une vérification à l'aide d'un système de mot de passe dynamique ou d'un autre système d'authentification fort
Présentation en personne	Demander à l'interlocuteur de se présenter en personne avec un badge de salarié ou un autre moyen d'identification

Procédure de vérification du statut d'un salarié

Action	Description
Vérification dans le répertoire de l'entreprise	Vérifier que le correspondant se trouve dans le répertoire en ligne de l'entreprise
Vérification auprès du supérieur hiérarchique de l'interlocuteur	Appeler le supérieur hiérarchique correspondant en utilisant le numéro de téléphone du répertoire ou de l'annuaire de l'entreprise

ACTION	DESCRIPTION
Vérification auprès du service du correspondant	Appeler le service du correspondant pour s'assurer qu'il fait encore partie de l'entreprise

Procédure de vérification de l'habilitation de l'interlocuteur

ACTION	DESCRIPTION
Vérification dans la liste des fonctions/postes/services	Vérifier dans les listes existantes que l'interlocuteur est habilité à obtenir les informations qu'il demande
Demande d'autorisation auprès du supérieur hiérarchique	Demander au supérieur hiérarchique (le sien ou celui du correspondant) l'autorisation de fournir les informations demandées
Demande d'autorisation auprès du responsable de l'information ou l'un de ses délégués	Demander au responsable de l'information si l'interlocuteur est habilité à obtenir les informations
Demande d'autorisation à l'aide d'un logiciel	Utiliser une base de données propriétaire pour vérifier que l'interlocuteur est habilité à obtenir les informations

Critères de vérification des non-salariés

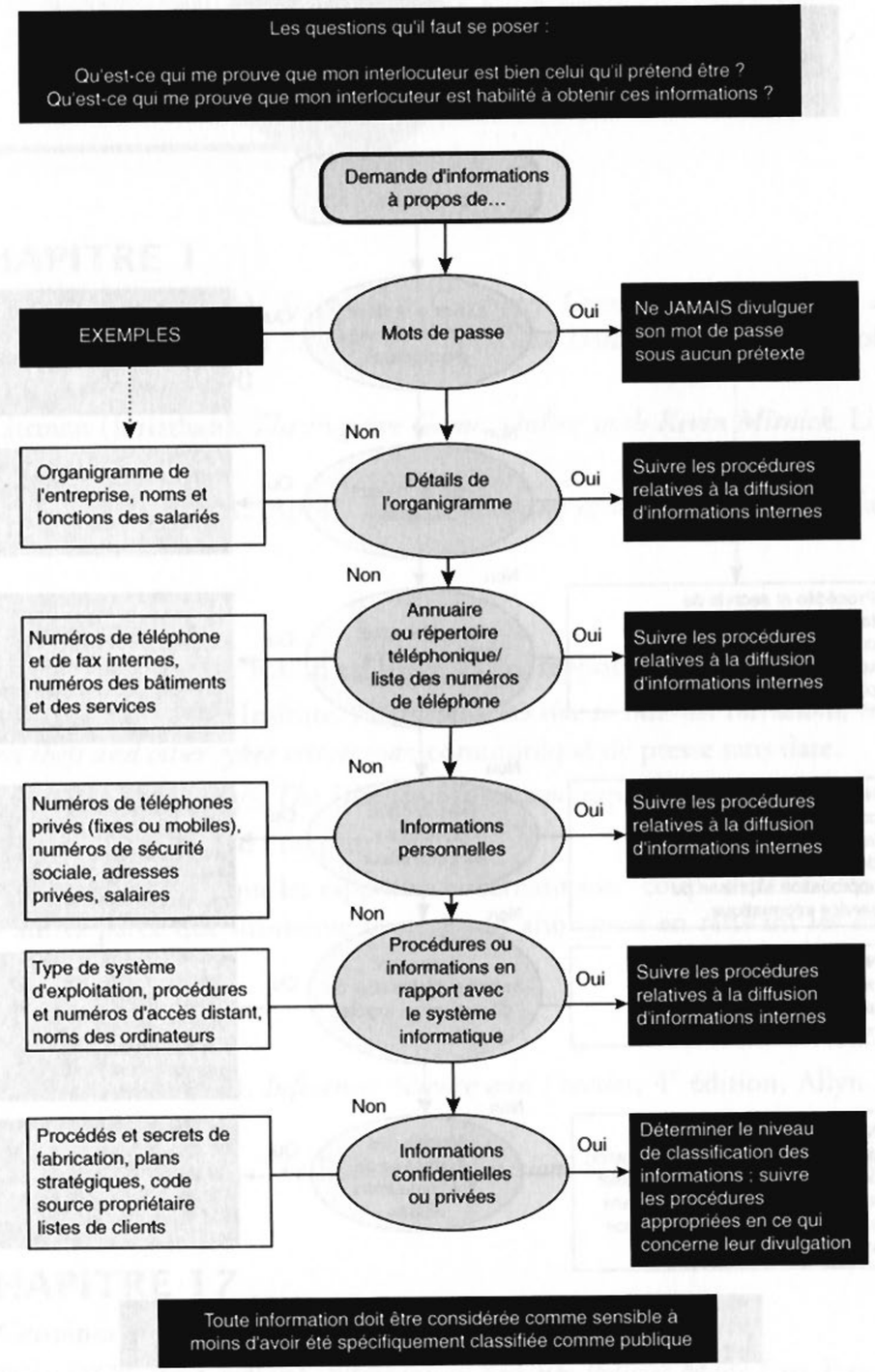
CRITÈRE	ACTION
Relation	Vérifier l'authenticité de la relation avec l'entreprise du correspondant : fournisseur, partenaire commercial ou autre
Identité	Vérifier l'identité de l'interlocuteur et son statut dans l'entreprise partenaire ou chez le fournisseur
Accord de confidentialité	Vérifier que l'interlocuteur a signé un accord de confidentialité
Accès	Transmettre la demande aux supérieurs hiérarchiques quand le niveau de classification de l'information est supérieur à "Interne"

Classification de l'information

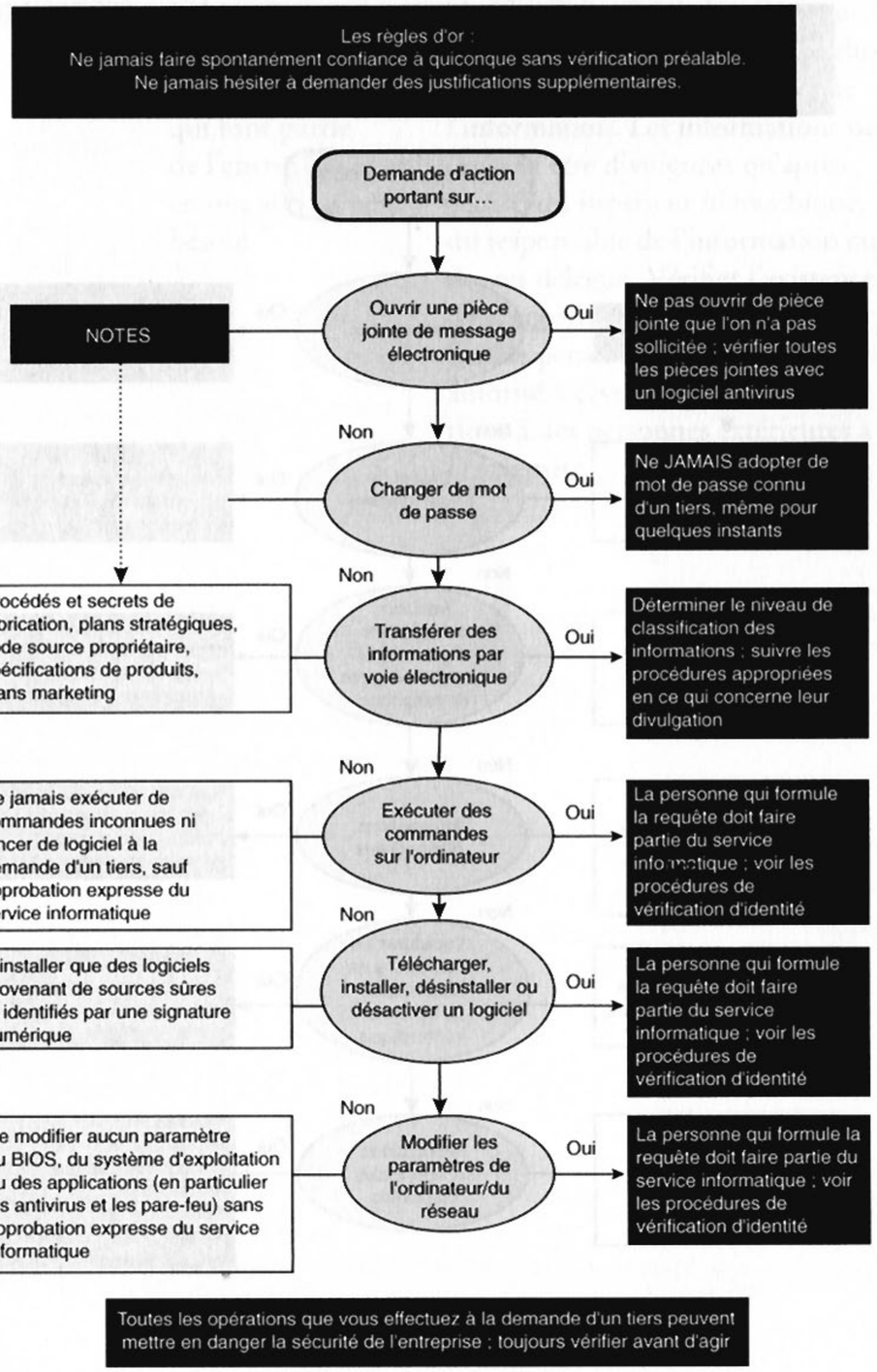
CLASSIFICATION	DESCRIPTION	PROCÉDURE
Public	L'information peut être librement diffusée	Aucune vérification n'est nécessaire
Interne	Diffusion à l'intérieur de l'entreprise seulement	Vérifier que la personne qui formule la requête est actuellement employée par l'entreprise, ou s'assurer de l'existence d'un accord de confidentialité et de l'autorisation des supérieurs hiérarchiques si la personne est extérieure à l'entreprise.
Privé	Informations concernant le personnel de l'entreprise ; diffusion à l'intérieur de l'entreprise seulement	Vérifier que la personne qui formule la requête est actuellement employée par l'entreprise ou qu'elle a l'autorisation d'obtenir les informations qu'elle demande. Vérifier également auprès des ressources humaines que ces informations peuvent être transmises.

Classification	Description	Procédure
Confidentiel	Informations à ne divulguer qu'aux personnes qui font partie de l'entreprise et qui en ont absolument besoin	Vérifier l'identité de la personne qui formule la requête et son habilitation auprès du responsable de l'information. Les informations ne doivent être divulguées qu'après accord du supérieur hiérarchique, du responsable de l'information ou de son délégué. Vérifier l'existence d'un accord de confidentialité. Seul le personnel dirigeant est autorisé à divulguer ces informations à des personnes extérieures à l'entreprise.

Réponse à une demande d'informations



Réponse à une demande d'action



Sources

CHAPITRE 1

BloomBecker (Buck), *Spectacular Computer Crimes: What They Are and How They Cost American Business Half a Billion Dollars a Year*, Irwin Professional Publishing, 1990

Littman (Jonathan), *The Fugitive Game: Online with Kevin Mitnick*. Little Brown & Co, 1997

Penenberg (Adam L. April), *The Demonizing of a Hacker*, Forbes Magazine, 19 avril 1999

CHAPITRE 2

L'histoire de Stanley Rifkin est basée sur les rapports suivants :

Computer Security Insitute, *Financial losses due to Internet intrusions, trade secret theft and other cyber crimes soar*, communiqué de presse sans date.

Epstein (Edward Jay), *The Diamond Invention*, rapport inédit

Holwick, Rev. David : rapport inédit

M. Rifkin a admis que les rapports concernant son "coup" diffèrent les uns des autres parce que lui-même protège son anonymat en refusant les interviews.

CHAPITRE 16

Cialdini (Robert B), *Influence: Science and Practice*, 4e édition, Allyn and Bacon, 2000.

Cialdini (Robert B), *The Science of Persuasion*, Scientific American, février 2001

CHAPITRE 17

Certaines des règles de ce chapitre sont inspirées de :

Wood (Charles Cresson), *Information Security Policies Made Easy*, Baseline Software, 1999

Index

Numerics

802.11b, carte réseau 326

A

Abonnement de téléphonie mobile 60
Abus de confiance 18
Accès
  à des informations confidentielles 103
  à distance 312, 322
    demandes 316
    numéros d'accès 330
  à un ordinateur 103
  à une base de données 63
  aux fichiers 186
  aux ordinateurs (formation) 310
  contrôler 65
  physique 220
  sans fil 315, 326
Accueil 300
Administrateur
  de base de données 142, 143
  système 90
Adresse
  e-mail 59, 74
  IP 141, 261
Agence d'investigations 131
Agent de sécurité 218, 220
Aide 358
  de l'ennemi 69
  émanant d'un étranger 86
  informatique 139
Aider
  les nouveaux venus 73
  un manipulateur 89
Algorithme 94
Anna Kournikova 107
Annuaire interne 353
Anodine, information 27, 33
Antécédents des salariés 350
Antivirus 117, 230, 322, 347
  fichiers de définition de virus 326
Antivol 17
Appels
  prétextes 3
  suspects
    compte-rendu 329
    gestion 330
  vérifier 34
Archive, groupe de discussion 100
Armoires du système informatique 307
Arnaque par inversion 149
ARPANET 19
Assistance technique 132, 311
Assurance automobile 157
Astérisques, pour mot de passe 132
Attaquant
  catégories 17
  créant le problème 72
Attaque
  directe 43
  en cours 355
  par manipulation 115
  prétendre un besoin d'aide 103
Audit 186, 191
Authentification
  à deux facteurs 87, 96, 97
  des logiciels 323
  forte 317
  méthode 40
Autorité 271

B

Backdoor 218
Badge 184, 350
  absence 330
  code de couleur 311
  conception 304
  d'identification 330
  électronique 189
  port 187
  provisoire 351

Bancaire, compte 15
Bandes de sauvegarde 249
Banque
  code de sécurité interne 150
  compte 15
  enquête sur client 28
Base de données
  accès 63
  de détenteurs de carte de crédit 97
  du centre national d'informations criminelles 62
  du FBI 45
  SQL, mot de passe 111
Bellovin, Steve 92
Bibliothèque dynamique 219
Biométrie 318
Boîte
  aux lettres 37
  vocale 237, 238, 302
    générique 290
    messages d'annonce 342
    mots de passe 340, 341
Borland 247
Brevets 357
Brochures 357

C

Câble
  de réseau 68
  et paire 123
Cadenas en bas de page Web 115
Capital intellectuel 27
Cartes
  à puce 297, 318
  de crédit 40, 87, 108, 110
    vol 57
  de visite 257
  Visa 55
Cas
  classique de supercherie 14
  descente de police 135
  panne de réseau 67
Casier judiciaire 45
Casquette, changement 130
CD-ROM 336
Central téléphonique 233
Centraliser les rapports 145
  d'incidents de sécurité 88
Certificat numérique 116
Changement de mot de passe 132
Charte de sécurité 286
Chercher, travail du manipulateur 138
Cheswick, Steven 92
Cheval de Troie 107, 109
Chiffrement 263
CIA 92
Cialdini, Robert 271
Cible, connaissance en informatique limitée 73
Classification
  des données 40, 88
  des informations 287, 295
    confidentielles 288
    internes 289
    publiques 289
Clés
  de cryptage 264
  renseignement 32
Clients légers 346
Climat de confiance 53, 184
Cliquer sur un lien 107
Code
  de protection 163
  de sécurité
    interne de banque 150
    verbal 157
  journalier 154
  malveillant 107
  rupture 15
  source 204
Commerce électronique sur Internet 19
Communiqués de presse 357
Commutateur 159
  mise à jour logicielle 159
  téléphonique 162
Compte
  bancaire
    d'épargne 150
    ouverture 28
  d'invité 82
  d'utilisateur
    création 245, 313
    désactivation 305, 314
    expiration 318
    Invités 321
    mots de passe 325
    privilégiés 320
  en Suisse 15
  privilégié 290
  provisoire 90
Compte rendu d'incidents 306, 329
Conditionnement des parents 21
Confiance 9, 184
  abus 18
  création d'un sentiment de 53
  prudente 66
Confidentiel (niveau de classification) 288
Connaissance du fonctionnement interne 124
Connexions
  à distance 322
  à un réseau d'entreprise 82
  réseau 69, 132
  sécurisée 116
Conseils
  d'investissement 106
  de formation 163
Consultant 125, 133
  numéro de téléphone 41
Contacts 300
Contraventions 239
Contribuable 127
Contrôle
  à distance 180
  complet d'un ordinateur 71
  d'accès 65, 191
Coopération
  niveaux de 32
  par la peur 135
  par la reconnaissance 135
Copie illégale de films 138
Copyright, viol 135
Corbeille à papier 175
Correctif 319, 358
Courrier
  électronique
    adresse générique 319
    cryptage 297
    pièces jointes 323, 338
    signature numérique 292
    transfert automatique 338
    vérification 339
  interne, dépôt 307
Crédulité 9
Criminalité informatique 17
Critères de légitimité 146
Crochetage 203
  pistolet américain 249
Cryptage 65, 263, 321
  clés 264
  de messages vocaux 95
  HTML 114
  standard actuel 111
  unidirectionnel 83
Cyber-terrorisme 9

D

d 103
Déclenchement de réponse automatique 134
Déclencheur psychologique 119
Défi
  de l'autorité 126
  intellectuel 96
Définir les comportements 86
Définitions de virus, mise à jour 117
Démarrage de l'ordinateur, mot de passe 325
Départ d'un salarié 188
Destruction
  documents 187, 330
  supports électroniques 337
Détective privé 22, 30, 128, 153
Dictionnaire (attaque par) 207
Diplôme, création accélérée 140
Diriger sur un faux site 113
Discours d'entreprise 10
Disquettes 336
DLL 219
Document
  destruction 330
  secret 46
Données
  classification 40
  protection 264
Droits d'accès 243
  mise à jour 304
  modification 316

E

Échange de mots de passe 87
E-commerce 111
Économiseurs d'écran 230, 337
Écoute des forces de l'ordre 95
Effacer
  mémoire d'un téléphone mobile 72
  traces 101, 137
Effraction, menace 20
E-mail
  adresse 59, 74
  d'un ami 109
  fichier joint 106
Embauche
  formulaire 45
  service 34
Employé
  ancien 124
  mutation 180, 188
  nouveau 121, 127
  numéro 39
    authentification 41
    téléphone 41
Empreinte
  de mots de passe 209
  digitale 45
Enchères en ligne 110
Engagement écrit 280

Ennemi, aide 69
Enquête sur client des banques 28
Énumération 207
Équipe de nettoyage 188
Espionnage
  industriel 66, 79, 247, 256
  traditionnel 84
Évacuation d'urgence 351
Expiration des comptes d'utilisateur 318
Exploration du réseau téléphonique 47
Extensions de fichiers 224

F

Facteur humain 13, 20
  maillon faible 13, 52, 118
Fausse identité 21
Faux site 113
Fax 137, 151, 239, 244, 340
  en panne 81
  envoi d'informations sensibles 341
  mauvais numéro 138
FBI 62
  base de données 45
Fichiers
  d'empreintes 209
  de définition de virus 326
  de mots de passe 82
  de numéros de cartes de crédit 65
  joints d'un e-mail 105
  transfert 263
Film, copie illégale 138
Force brute (attaque par) 209
Formation à la sécurité 10, 41, 47, 51, 274, 275
  accès aux ordinateurs 310
  mise en œuvre 275, 281
  programme 88
  structure 277, 278
  suivi 281
  vérification des connaissances 280
Formulaire d'embauche 45
Formuler une demande 31
Fouille des poubelles 174
Fréquences radio de la police 95
Frontière entre le légal et l'illégal 49
FTP
  anonyme 261
  site 83

G

Garantie 290, 292
Groupe
  d'information sur les incidents 354
  de discussion 100
Gzipper 259

H

Hachage de mot de passe 83
Hacker
  dangereux 96
  informatique 85
Hacking 3
  de la police 62
  passe-temps d'étudiants 146
Hare Krishna (secte) 272
Heures de travail, visites hors des 187
Hors site 263, 321
Hôte à double réseau 205
HTML, cryptage 114
HTTP (Hypertext Transfer Protocol) 116
Hyperlien 115

I

IBM 3
Identification 227
  d'empreintes digitales 45
  de l'appelant 231, 244, 291, 300
  méthodes 332
  personnel extérieur à l'entreprise 350
  visiteurs 351
Identité 278
  fausse 21
  usurpation 39
  vérification 296
ILOVEYOU, virus 48
Incidents, compte rendu 306
Inconnu, déplacement dans l'établissement 121
Influence 271
Information
  anodine 27, 33
  confidentielle 144
    divulgation 297
  des employés 39
  mesures de protection 40
  sensible 66
    protection 86
  sur l'entreprise, diffusion en ligne 336
  valeur 73, 143
Informatique, criminalité 17
Ingénieur logiciel 66
Inspirer confiance 56
Installation
  de production d'électricité 21
  silencieuse 225
Intellectuel
  capital 27
  défi 96
Interne (niveau de classification) 289
Internet
  commerce électronique 19
  fraude 110
Intranet 41, 63, 286
  domaine d'appartenance 66
  être isolé 71
Intrusion
  physique 167, 200
Invité, compte 82
ISDN 233

J

Jargon 29
Journal de transactions 144
Judiciaire, casier 45

K

Keylogger 132

L

L0phtcrack 209
LANMAN (empreintes de mots de passe) 210
Le Carré, John 258
Légal ou illégal, frontière 49
Licence de logiciel 74
Licenciement d'un salarié 180, 188
Lien ressemblant 113
Liste rouge 43, 122
Locaux, intrusion 167
Logiciels
  anti-Troyen 118
  antivirus 117, 230, 322, 347
    mise à jour 75
  authentification 323
  de codage 95
  de contrôle à distance 180
  de sécurité 335, 347
  espions 224, 225
  exécution 315
  gratuits 105
  installation 358
  malveillants, repérage 107
  téléchargement ou installation 334
Login incorrect 142
Love Letter 107

M

Macro 108
Maillon faible 13, 52
Maison blanche 235
Malware, malicious software 107
Manipulateur 3
  aide 67
  caractéristiques sociales 18
  modus operandi 65
  précoce 153
Manipulation
  attaque 43
  des parents 21
  par inversion 73
  techniques 16
Marlowe, Philip 30
Mauvais numéro 37
Menace
  effraction 20
  nature 16
  sous-entendue 156
Message
  d'annonce des boîtes vocales 342
  d'avertissement 117
Méthode d'authentification 40
Microsoft 176
Mise à jour 319
  antivirus 75, 117
  automatique 75
  logicielle de commutateur 159
Modem 178, 180, 322
  installation 335
  réponse automatique 335
Monotonie quotidienne 131
Mots de passe 78, 96, 108, 144, 183, 213, 358
  acceptables 145
  astérisques 132
  attaque
    par dictionnaire 207
    par force brute 209
  au téléphone 343
  boîtes vocales 340, 341
  changement 75, 132, 189
  communication 314
  composition 75
  comptes privilégiés 326
  cryptés 82
  d'ordinateurs 343
  démarrage de l'ordinateur 325
  des clients 308
  divulgation 328
  dynamiques 292, 361
  échange 87
  économiseur d'écran 337
  empreintes 209
  envoi par courrier électronique 334
  Internet 344
  modification périodique 325

non obligatoires 82
nouveaux comptes 325
par défaut 85, 302, 323
par fax 341
partage 104
règles pour la création 344
réinitialisation 313, 317
réutilisation 344
stockés sur ordinateur 346
Moyens technologiques 285

N

Nature humaine 44, 59
Navigateur 116
NBTEnum 206
NetBIOS 206
Niveau de coopération 32
Nom
d'utilisateur 75, 78
de compte par défaut 159
de domaine
informations de contact 319
trompeur 113
Nouvel employé 52, 73, 121, 127, 226
Numéro
communiqué par l'appelant 34
d'employé 39, 103
dévoilé 89
d'immatriculation de véhicule 157
de carte
de crédit 57, 65, 108
Visa 55
de compte 155
de fax 138
de port 68
de poste interne 38
de téléphone
identification 128
interne 41, 339
liste rouge 43, 122
mobile 68
non disponible pour le public 130
rappeler 34
mauvais 37
PIN 293
répertorié 34

O

Oracle 176
Ordinateur, panne 132
Organigramme 332
Ouverture
de compte bancaire 28
de fichier joint 107

P

PABX 233
Page
sécurisée 115
Web, cadenas 115
Paiements en ligne 110
Panne
d'ordinateur 132
de fax 81
de réseau 67
de serveur 78
Papier d'identité 173
Paraître aimable 38
Paranoïa salubre 42
Pare-feu 85, 91, 118, 141, 181, 190, 347
Partage de mot de passe 87, 104
Passagers clandestins 184, 189, 330
Patch 218, 221, 319, 358
Personne
ayant autorité 125
de confiance 290
de référence 308
non vérifiée 290
Personnel
autorisé d'une entreprise de téléphonie 44
d'accueil 300
d'entretien 188, 212
vulnérabilité 91
Persuasion 6
amicale 149
Phreaking 3
Pièces jointes 323, 338
Piratage téléphonique 3, 54, 94
Pistolet américain 249
Plaque d'immatriculation 352
Points de contrôle, aéroports 19
Police
fréquences radio 95
hacking 62
tromper 136
Port
du badge 187
numéro 68
Poubelles 174, 187, 331, 352, 357
Pratiques trompeuses 18
Prison 193
Privé (niveau de classification) 288
Privées 288
Privilèges d'accès, modification 313
Problème
créé par l'attaquant 72
de câblage 68
Procédures
accès à distance 312
d'une entreprise 40
de sécurité 103, 163
standardisées 146
Procès-verbaux 136
Programme
de piratage 3
de sécurité de l'information 284
rustine 219
Propriétaire de bases de données 142
Prospects 300
Protection
contre la fuite d'informations 40
du réseau 347
Protocole 94
Public (niveau de classification) 289

Q

Question
clé
enfouie dans questions anodines 33
noyée dans d'autres questions 45
personnelle, test 33
piège 91
Questionnaires téléphoniques 339

R

Raccourcis mentaux 134
Rachat d'entreprise 70
Radio
cryptée 95
sur fréquences de la police 95
Raisonnable, requête 131
Rappel 292
Rappeler un numéro de téléphone 34
Rapports, centralisation 145
Rareté 273
Rayfiel, David 93
RCMAC 195, 212
Recherche
de mot dans fichiers 134
de numéros non publiés 44
et développement 66
Réciprocité 271
Reconstitution graduelle d'information 50
Recrutement 348
de talents 34
Référence à l'autorité 126
Règles de sécurité 144, 283
définition 284
rédaction 285
Renseignement
clé 32
demande 41
financier 153
Répertoire
d'entreprise 37, 41
téléphonique, édité ou en ligne 163
Requête raisonnable 131
Réseau
connexion 67
étendu 205
panne 67
privé virtuel 326
protection 347
segmentation 185
téléphonique, exploration 47
Responsable de l'information 288
Ressemblance de liens 113
Ressources humaines 348
Restauration des sauvegardes 78
Retrait bancaire 155
Rifkin, Stanley Mark 14
RNIS 233
Routeur 190
Rupture de code 15
Ruse
lettre de félicitations au directeur 138
montrer un processus informatique 143
Rustine 219

S

Salaire 186
Salarié
antécédents 350
de base 189, 215
départ 188
informations privées 332
licencié 180
quittant l'entreprise 348
récent 226
statut 293
Salle
du courrier 352
informatique 308
Sauvegardes 249, 264
stockage 329
Savoir-faire, technique 43
Schneier, Bruce 14
Se faire passer pour un initié 38
Secret commun 292
Secure Socket Layer 117
Secure World Expo 276
Sécurité

bonbon 92
clandestine 92
des informations 9
par obscurité 94
relâchée 89
sociale 127
technologies 13
Segmentation du réseau 185
Sensation de puissance 102
Sensibilisation à la sécurité 273, 310
mise en œuvre 275
suivi 281
Sensibles (informations) 289
Sentiment de confiance 135
Serrure 203
à paillettes 203
pistolet américain 249
Serveur
en panne 78
proxy 66
Shareware bon marché 106
Signature numérique 292
Silent install 225
Silicon Valley 89
SirCam 107
Site
de groupe de discussion 100
faux 113
FTP 83
Web 320
Situation financière 70
Solde
bancaire 157
de compte 155
Soupçons, endormir 53
Source, identifier 87
Spade, Sam 30
Spyware 224, 225
SSH 221
SSL (Secure Socket Layer) 116
Stallman, Richard 19
Standard de cryptage 111
Station de travail 98
Stockage hors site 249, 264
Stratagème émotionnel 130
Supercherie classique 13
Supérieur hiérarchique 292
Superutilisateur 217
Supports numériques 329
Suspicion 53
Symantec 247
Sympathie 271
Syntaxe de commandes pour extraire des informations 63
Systèmes
d'exploitation, configuration 318
informatiques, effraction 20

T

Tableaux d'affichage 308
Tactique émotionnelle 119
Technique
de manipulation 16
savoir-faire 43
Technologie
logicielle 21
matérielle 21
sécurité 13
Télécharger des fichiers 85, 106
Télécopie 239, 244, 340
Téléphone
central téléphonique 233
configuration 303
de courtoisie 302
mobile
abonnement 60
jeté 72
numéro 68
règles de sécurité 300
traçage des appels 303
Télétravailleurs 346
Telnet 141, 221
Tests
de pénétration 269, 280, 286
de vulnérabilité 310
The Cleaner 118
Thompson, sénateur 6
Tokens 318
Traçage des appels 303
Traces, effacer 101, 137
Transfert
d'appels 300
de fichiers 263, 300
Trojan Defence Suite 118
Troyens 315, 335, 347, 358

U

UNIX 82
Update, mot de passe par défaut 159
Usenet 262
Usurpation d'identité 39, 184, 236, 245

V

Valeur des informations 63, 73, 143
Validation sociale 273
VAX 185
Ventes aux enchères 110
Ver 74, 106, 107
Vérification
appel téléphonique 34
d'identité 103, 265, 278, 291, 296
de l'habilitation 294
de ligne 123
des autorisations 278
du statut du demandeur 293
Viol de copyright 135
Virus 48, 74, 326, 358
informatique 106
se tenir informé 117
Visa, carte 55
Visiteurs
accès au réseau 321
accompagnement 351
identification 351
salle du courrier 352
Voix non familière 81
Vol de carte de crédit 57
VPN 326
Vulnérabilité du personnel 91

W

WAN (Wide Area Network) 89, 205
War Driving 326
Webcam 108
Wi-Fi 326
Wireless 326
Wordlists 207

Z

Zones sensibles, sécurisation 306

Dépôt légal : août 2005
IMPRIMÉ EN FRANCE

Achevé d'imprimer le 12 août 2005
sur les presses de l'imprimerie «La Source d'Or»
63200 Marsat
Imprimeur n° 9891

L'ART DE LA SUPERCHERIE

KEVIN D. MITNICK
& William L. Simon

Dans cet ouvrage, Kevin Mitnick vous propose de découvrir des scénarios réalistes d'arnaques et d'escroqueries, tous basés sur l'art de la persuasion et de la manipulation.

Mitnick démontre que l'homme doit être au centre de la politique de protection des données : aucun pare-feu ou protocole de cryptage ne sera jamais assez efficace pour arrêter des individus déterminés à pénétrer un réseau ou à obtenir une information confidentielle. L'élément humain est donc la clé, mais c'est aussi le principal point faible des systèmes de sécurité : un personnel peu ou mal formé, ou qui ne respecte pas les consignes, constituera une cible privilégiée pour tout hacker digne de ce nom.

Raconté à la fois du point de vue de l'attaquant et de la victime, *L'art de la supercherie* explique pourquoi certaines attaques par imposture réussissent, et indique comment elles auraient pu être déjouées. Ce livre donne également des conseils précis aux entreprises afin que les investissements qu'elles réalisent pour sécuriser leurs systèmes donnent des résultats probants.

« Alors que la plupart des livres sur le piratage traitent de l'aspect technique, celui-ci - original - se focalise sur un sujet habituellement négligé : l'homme. [...] De façon romancée et pratique, Kevin Mitnick révèle des exemples d'impostures, et explique comment s'en protéger. » Pirates Magazine

CampusPress

WILEY

CampusPress est une marque de
Pearson Education France
47 bis, rue des Vinaigriers
75010 Paris
Tél. : 01 72 74 90 00
Fax : 01 42 05 22 17
www.pearsoneducation.fr

A propos de l'auteur...

Kevin Mitnick, cyber-criminel recherché par le FBI, a purgé une peine de cinq ans de prison. Remis en liberté en 2000, il est devenu depuis l'un des plus brillants experts en sécurité informatique. Consultant et cofondateur de *Defensive Thinking*, une société-conseil basée à Los Angeles, il a rédigé des articles de presse pour plusieurs magazines d'information et journaux spécialisés, et participe à de nombreux salons et conférences.

Catégorie : Sécurité/Actualités
Titre original : The Art of Deception

ISBN : 2-7440-1976-3

1976 0805 14,90 €
9 782744 019760