



Article de Jacques Bourdeau
Ingénieur en sécurité
ESI Technologies

Gare aux crimes informatiques, ils peuvent être commis de mille et une façons.

L'omniprésence des technologies de l'information n'a pas que des effets positifs. En matière de crime, par exemple, à peu près tous les délits connus dans les annales judiciaires peuvent être commis avec l'apport de l'informatique.

Le plus courant d'entre tous, le vol, se rencontre sous diverses formes car de tous les temps, les cambrioleurs se sont efforcés d'aller chercher le butin là où il se trouve. Aujourd'hui, par conséquent, ils se tournent vers le vol de données puisque toute information a une valeur. C'est d'ailleurs la raison pour laquelle on stocke des données.

Le vol

Le type de vol informatique le plus fréquent met en scène un employé qui quitte une organisation pour se joindre à une autre ou pour lancer sa propre affaire. En vidant son bureau, il prend soin de faire une copie de données stratégiques qu'il pourra refiler à ses nouveaux patrons ou conserver pour son usage personnel. Ce petit manège peut coûter très cher à une entreprise et même l'acculer à la faillite.

C'est pourquoi il est important d'établir en priorité des mesures de sécurité interne, avant même de se protéger contre les menaces externes. Évidemment, un employé pourra toujours emporter avec lui l'information à laquelle il devait nécessairement avoir accès pour accomplir son travail. Dans ce cas, il devient très difficile, voire impossible, de se protéger grâce à des solutions technologiques. Et, si de nombreux voleurs ont pu consulter des données sans autorisation d'accès, il est intéressant de noter que les enquêtes informatiques, conduites au sujet d'un vol, permettent parfois de mettre au jour d'autres vols qui ont été perpétrés antérieurement par les mêmes suspects.

L'espionnage

L'histoire suivante est tirée d'un fait vécu – c'est d'ailleurs le cas de tous les exemples présentés dans cet article. Imaginé le scénario suivant : un employé qui quitte son entreprise est de connivence avec un autre qui, lui, demeure à l'emploi de celle-ci afin d'agir comme taupes. Les deux complices bénéficient ainsi d'un flux continu d'informations vitales qui permettent à l'employé démissionnaire de suivre ou de précéder son ex-employeur chez un client, afin de torpiller ses efforts grâce aux renseignements confidentiels qu'il détient. Il s'agit là d'espionnage et les enquêteurs ont pu retracer les coupables, en examinant leurs communications électroniques.

La fraude

Une autre variation du scénario de l'employé qui démissionne est qu'il emporte avec lui des informations confidentielles afin de fonder une entreprise et lui donner un nom pratiquement semblable à celui de l'organisation qu'il vient de quitter. Ceci lui permet de se faire passer pour son ex-employeur et de détourner à son profit des chèques qui lui sont destinés puisque la banque ne voit pas la subtile différence. Dans ce cas, les enquêteurs n'ont eu qu'à remonter la piste des malfaiteurs en fouillant les dossiers de comptabilité électroniques de l'entreprise frauduleuse.

L'usurpation d'identité

L'usurpation d'identité représente une autre forme fréquente de crime informatique. Relativement facile à réaliser, ce délit peut s'avérer très lucratif, car il suffit de connaître quelques renseignements de base pour prendre l'identité de quelqu'un d'autre. Ainsi, il est possible avec le nom, l'adresse, la date de naissance et le numéro d'assurance sociale d'un individu de contracter une hypothèque en son nom.

Puisque c'est trop souvent à l'aide du numéro d'assurance sociale que ces fraudes sont commises, on multiplie les mises en garde aux particuliers. On cible ceux qui remplissent leur rapport d'impôt en ligne et qui stockent ce numéro dans leur ordinateur, car en l'absence de mesures de protection adéquates, un pirate pourrait aisément s'y introduire et extraire les neuf chiffres précieux.

Le viol

D'étranges motifs sont aussi à l'origine de l'usurpation d'identité, comme dans l'histoire sinistre où un homme, qui convoitait une femme, intercepte la correspondance épistolaire qu'elle entretient avec sa soeur dans le but de parvenir à modifier, à leur insu, les échanges qu'ils entretiennent et ensuite réussir à attirer la femme dans ses filets. Pour y arriver, il se dote d'une adresse de courrier électronique appartenant au même service de messagerie publique qu'utilisent les deux soeurs et qui ressemble à s'y méprendre à l'adresse de l'une d'elles.

De cette façon, il est en mesure d'envoyer à chacune des messages apparentés à ceux qu'a véritablement écrits l'autre, mais qui en réalité contiennent les modifications et les ajouts du malfaiteur. En anglais, on appelle ce type d'intrusion dans une correspondance privée *Man in the middle attack* (MITM).

Au début, le stratagème fonctionne, mais rapidement les victimes constatent que quelque chose ne tourne pas rond et ils demandent une enquête. Celle-ci permet d'identifier que le réseau d'entreprise à partir duquel opère le scélérat est aux États-Unis. Ce qui complique malheureusement l'enquête car l'organisation à laquelle il appartient refuse de prêter son aide afin de coincer le coupable. Des mesures de sécurité spéciales sont alors mises en place pour protéger la soeur. Juste à temps, puisque le malfaiteur s'apprêtait à aller cueillir sa victime à un moment et en un endroit précis.

L'extorsion et le chantage

Les TI peuvent aussi conduire à l'extorsion, comme l'illustre l'histoire suivante où un administrateur de réseau exige de l'argent de son employeur, faute de quoi il publiera à son sujet de l'information confidentielle à laquelle il a facilement accès dans ses fonctions. L'employeur contacte les enquêteurs et pendant qu'il est convoqué par la direction, qui veut lui annoncer son congédiement, les enquêteurs s'introduisent dans le système qu'il est chargé d'administrer et changent les mots de passe. Ils se consacrent ensuite à établir des mesures de sécurité qui empêcheront le maître chanteur d'accéder de nouveau au système. Une démarche qui s'avérera judicieuse, puisqu'il tentera effectivement de briser la sécurité pour accéder aux systèmes.

Le harcèlement

Dans ce cas de harcèlement, c'est un employeur peu scrupuleux qui emmagasine du matériel pornographique dans le poste de travail d'un employé afin de le congédier. Mais une enquête demandée par l'employé, permet de découvrir qu'un volume très important de matériel a été stocké sur le disque dur à une vitesse qu'il aurait été impossible d'atteindre s'il avait été téléchargé depuis le Web. En définitive, c'est l'absence de traces de navigation sur un site mal entretenu, la présence de nombreux doublons dans les fichiers répertoriés et d'autres signatures qui ont permis d'écarter l'hypothèse voulant que l'employé se divertisse pendant les heures de travail. Ce cas présente une particularité par rapport aux autres histoires : c'est la défense et non la poursuite qui a sollicité l'aide des enquêteurs.

Le vandalisme et le comportement non-professionnel

Il existe aussi de nombreux cas de vandalisme électronique perpétré par plaisir ou défi, par des pirates qui s'introduisent dans les systèmes informatiques d'une entreprise. Le vandalisme peut aussi provenir de membres du personnel qui, souvent, en veulent à leur employeur. Dans ce cas, les dégâts causés varient énormément et on les classe de facilement réparables à irrémédiables.

Les enquêteurs informatiques sont également appelés à élucider des cas de comportement non-professionnel impliquant des personnes qui se servent de l'ordinateur de leur employeur pendant les heures de travail, afin de se consacrer à un autre emploi. Il arrive également que des travailleurs naviguent exagérément sur Internet dans d'autres buts que ceux qui sont prévus dans le cadre de leur travail.

Nécessité de prendre les mesures appropriées

Bien sûr, il ne s'agit pas là d'une liste exhaustive des types de crimes ou de méfaits qui sont commis avec le concours de l'informatique. Il en existe bien d'autres et il faut retenir que de tels problèmes surviennent beaucoup plus souvent qu'on ne le pense. Les gestionnaires ne doivent pas croire que cela n'arrive qu'aux autres. Tous les délits évoqués dans cet article ont été commis au Québec et ont tous fait l'objet d'une enquête. Les organisations et les individus soucieux de conserver secrète l'information leur appartenant doivent impérativement adopter des mesures efficaces de protection.