Zeitschrift: Reihe Kriminologie / Schweizerische Arbeitsgruppe für Kriminologie = Collection criminologie / Groupe suisse de travail de criminologie

Herausgeber: Schweizerische Arbeitsgruppe für Kriminologie

Band: 17 (1999)

Artikel: Criminalité informatique : quels risques pour l'entreprise?

Autor: Reigner, Jacqueline

DOI: https://doi.org/10.5169/seals-1051179

JACQUELINE REIGNER

CRIMINALITÉ INFORMATIQUE, QUELS RISQUES POUR L'ENTREPRISE?

Introduction

Sur l'écran de votre ordinateur, la réalité virtuelle. Courant, se faufilant par les réseaux informatiques interconnectés, la criminalité informatique, est bien réelle et les risques qui menacent vos entreprises ou vos organisations sont tous aussi réels. Les dommages que vous subissez se chiffrent en heures de travail et en millions de francs.

Exemple: le vol

Un cabinet de services juridiques et fiscaux se fait voler pendant la nuit la quasi totalité de son parc micro-informatique. Dommages matériels: 500 000 FF. Dommages immatériels évalués à 300 000 FF à quoi s'ajoutent 2 millions de FF en responsabilité civile.

Statistiques

En France, le CLUSIF, une association à but non lucratif édite chaque année les statistiques des sinistres informatiques dans le secteur non-gouvernemental. En 1996, les pertes causées par des sinistres informatiques sont évalués à près de 13 millions de FF:

- 62% par acte de malveillance
- 24% par accident
- 14% par erreurs

Les chiffres de l'évaluation du CLUSIF sont publiés chaque année depuis 1983. Chaque année les résultats montrent une augmentation des sinistres causés par *malveillance.*

De nombreuses études au Royaume Uni ou aux Etats-Unis confirment cette tendance.

Exemple: la fraude

Parmi les actes de malveillance, nous avons déjà vu un exemple de vol. Autre cas de malveillance: la fraude, autrement dit l'utilisation non autorisée des ressources du système d'information, qui conduit à un préjudice financier pour la victime, essentiellement formé par le détournement de biens au profit du criminel.

Dans une banque, un cadre, ayant autrefois travaillé au service informatique, entre sur écran une série d'écritures, dont le compte d'origine est «Réserves» et le compte d'aboutissement est un numéro de compte personnel dans une banque étrangère. Les opérations sur réserves sont rejetées en anomalies dans un fichier d'attente, afin d'être ultérieurement recyclées. Le fraudeur utilise alors une chaîne de recyclage batch, normalement employée en mode dégradé dans le cadre du plan de secours. Cette chaîne, ancienne, n'est pas à jour, et les écritures passent. Ce n'est que le lendemain, lors du contrôle quotidien, que l'anomalie est identifiée. Les mouvements de fonds ont déjà été réalisés pour 7,5 millions de FF.

Exemple: le sabotage

Le sabotage est un autre type de malveillance. Il peut prendre la forme d'un attentat, de vandalisme ou de toute action malveillante conduisant à un sinistre matériel.

Dans une banque: Sabotage physique d'une trieuse de chèques très spécialisée d'une valeur de 5 millions de FF. Le retard de traitement (transfert vers un centre régional) a entraîné environ 2 millions de FF de pertes supplémentaires.

Exemple: l'attaque logique

Encore un type d'action malveillante, l'attaque logique. C'est l'utilisation non autorisée des ressources du système d'information, conduisant à un préjudice pour la victime, se traduisant essentiellement par une perte d'intégrité et/ou de disponibilité, entraînant le plus souvent un profit indirect pour le criminel et/ou le commanditaire éventuel. Dans cette catégorie se trouve: sabotage immatériel, infection informatique, programme «simple», bombe logique, cheval de Troie, sabotage «manuel», programme auto-reproducteur, ver, virus.

Les attaques logiques se subdivisent en deux catégories:
- les attaques non ciblées (comme les virus) qui représentent l'immense majorité des attaques en nombre, mais avec un impact modéré,
- les attaques ciblées vers une entreprise (bombe logique, manipulation de données ou de programmes, etc.) dans le but de la paralyser au moins momentanément. Ces attaques sont très peu nombreuses, mais leur impact est très élevé.

L'écoute du flux d'information sur le réseau entre le siège et l'usine principale a permis de détecter une importante transaction commerciale en cours. Le pirate a inoculé un programme d'écoute, puis grâce aux clés d'accès détectées un programme perturbateur. L'entreprise qui n'a pu sortir à temps la proposition détaillée avec la nomenclature des pièces a perdu un marché dont la marge prévue était de 10 millions de FF.

Exemple: la divulgation

Ici, l'utilisation non autorisée des ressources du système d'information entraîne la divulgation à des tiers d'informations confidentielles.

Distribution: Copie du fichier fournisseur au profit d'un concurrent (collusion d'un informaticien de la société avec un concurrent). Ce dernier a pu obtenir des fournisseurs avec lesquels il avait de moins bonnes conditions une mise à niveau. Il a pu alors pratiquer une attaque de son concurrent sur les produits pour lesquels celui-ci était moins bien placé. La perte en un an est estimée 45 millions de FF.

Exemple: autres malveillances

Il existe encore d'autres types de malveillance:
Industrie: Suite à un conflit avec la direction, départ de la presque totalité de l'équipe informatique d'un petit centre. Les pertes d'exploitation dues à l'impossibilité d'exploiter et de corriger les programmes par manque de documentation, même avec l'aide de personnes compétentes extérieures, ont été évaluées à plus de 2 millions de FF, soit le budget informatique annuel de cette entreprise.

Sécurité informatique

Le système d'information de votre entreprise ou votre organisation en est le centre vital, l'outil stratégique et en même temps son point le plus sensible. La malveillance informatique – avec sa part de 62% des cas – est en passe de devenir le risque industriel et économique numéro un. Peu médiatisée, cette information n'est pas familière. C'est pourquoi, elle paraît incroyable, exagérée... «on a encore jamais vu ça!» Plus difficile à croire encore est le constat suivant: dans plus de 80% des cas, l'auteur du délit est en relation contractuelle avec la victime, soit il fait partie du personnel de l'entreprise soit il agit avec la complicité d'un membre de l'entreprise ou encore il fait pression sur ce dernier.

Pourquoi est-il si difficile de croire aux risques informatiques? Quelques éléments de réponses se trouvent dans l'approche psychologi-

que du risque informatique. D'une part, la désinformation par des rapports insuffisants peut amoindrir la gravité apparente d'un problème. De plus les estimations de la fréquence ou de la gravité d'une brèche sont souvent en dessous de la vérité. En effet parmi tous les délits qui surviennent, seule une part est détectée. En outre, les coûts sont difficiles à évaluer. Quant aux délits détectés, seule une faible portion est signalée à la police (6–15%). Au contraire. la victime cherche souvent à étouffer l'affaire. «Assurez-vous que toutes les personnes au courant de ce qui s'est passé auront été averties de ne pas en parler. La presse recherche désespérément une grosse entreprise touchée. La moindre fuite pourrait faire un tort immense au nom de l'entreprise.» citation du manager d'un entreprise victime. D'autre part, la sous-inquiétude: 30% des personnes interrogées lors d'une enquête pour Data Processing and Communications Security déclarent que la direction générale se sent peu concernée par la sécurité informatique, voire pas du tout. Une étude déjà ancienne réalisée par Coopers & Lybrand dans les assurances révèle que 48% des entreprises n'avaient aucun plan anti-catastrophe et que seules 4% avaient testé leur plan. Ces chiffres sont-ils vraiment différents aujourd'hui?

En 1990, une étude en Allemagne de l'ouest souligne que parmi 871 ordinateurs centraux et 40 000 micro-ordinateurs:

- 20% utilisent des antivirus
- 23%incluent les micro-ordinateurs dans les plans de sécurité
- 27% pourchassent les logiciels piratés
- 46% ont des plans de secours et de reprise
- 56% ont rédigé des consignes pour la sécurité des informations
- 58% utilisent des procédures de sauvegardes.

La révolution informatique a rendu la gestion des informations plus efficace. Puisque les utilisateurs travaillent si dur pour générer des informations utiles, comment se fait-il qu'ils ne se sentent pas plus concernés par la protection de ce travail? Un autre facteur explique, lui aussi, la difficulté de prendre en compte les risques informa-

tiques: la compréhension des événements rares. Il est plus facile de comprendre les événements fréquents mais pas trop graves que les événements rares aux conséquences très graves. Tous les jours, vous composez avec un micro-ordinateur qui ne démarre pas, une imprimante récalcitrante ou une sauvegarde perdue, mais les conséquences en sont relativement faibles, mise à part la contrariété qu'elles génèrent. Bien au contraire en cas de sinistres qui perturbent gravement le système d'information: saturation de service qui rend impossible une activité stratégique, perte irrémédiable d'un serveur, etc, vous perdez alors tout ou partie de votre instrument de travail et c'est votre production, votre chiffre d'affaire et votre emploi qui en sont l'enjeu.

Catalogue des risques

Imaginez que demain matin vous arrivez à votre bureau. Vous allumez votre micro-ordinateur, vous lisez votre messagerie, vous répondez aux messages les plus urgents. Vous jetez un coup d'oeil aux tableaux de bord de l'application principale et vous vous attelez à la rédaction du rapport important pour le prochain conseil. Afin de compléter vos informations vous recherchez des documents sur votre Intranet et effectuez plusieurs requêtes sur Internet.

Avez-vous déjà énuméré les risques informatiques d'un tel système d'information en réseau? Sans vouloir en faire une liste exhaustive, essayons d'en citer les principaux:

- Votre micro-ordinateur Windows 95, 98 ou NT est la cible d'un nouveau type de virus baptisé peu élégamment Backorifice (développé par le groupe «Cult of the Dead Cow») ou de Netbus. Sans que vous le sachiez un espion veille sur votre micro-ordinateur, il peut lire votre écran à distance en même temps que vous, il peut lire, modifier ou effacer vos fichiers, changer vos répertoires et s'amuser à faire sauter la flèche de votre souris ou ouvrir

et fermer votre lecteur CD. Il a la mainmise totale sur votre micro-ordinateur.

- Votre boîte à lettre peut être saturée comme celles des journalistes, qui ne plaisant pas à un lecteur, ont été saturées de messages orduriers les empêchant d'utiliser leur messagerie pendant plusieurs heures.
- Le «flood» est l'envoi rapide de données inutiles sur une victime. Ici l'ordinateur est inutilisable.
- 25 millions de personnes sont abonnées à ICQ, un outil de communication utilisé sur Internet pour discuter avec quelqu'un où qu'il se trouve. Dans certains cas on dénombre un contact toutes les 30 secondes.
- L'espionnage d'entreprise est une réalité même si beaucoup de chef d'entreprise et de responsables informatiques ne veulent pas y penser. Il y a quelques années, Hitachi ne s'est pas gênée de s'introduire dans les profondeur du système d'information d'IBM.
- Pendant que vous utilisez Internet pour envoyer des messages à vos partenaires, d'autres s'activent sur des sites WEB sataniques ou pornographiques.
- Le vol d'information passe totalement inaperçu. Le vol peut se faire simplement par l'interception des données en un point quelconque, qu'elles soient stockées ou en transit.
- En 1998, une PME typique a subit 1100 incidents de sécurité sur son Firewall parmi lesquels 202 attaques sérieuses.
- Les premières informations recherchées par les pirates sont les mots de passe: dans les cas les plus faciles, le pirate découvre un compte sans mot de passe, parfois il s'agit d'un compte administrateur aux privilèges très élevés. D'autres cas faciles sont des mots de passe identiques à l'identifiant. Un peu plus difficile: des mots de passe différents mais qui existent dans un dictionnaire. Pour les décoder le pirate dispose de logiciels dits de «brute force attack». Finalement les mots de passe les plus difficiles à trouver sont formées de lettres et de chiffres d'une longueur importante (une phrase vaut mieux qu'un mot), et mieux encore changé ré-

gulièrement. Mais, est-ce que ce mot de passe est crypté ou bien passe-t-il en clair sur le réseau?

- Avec un banal sniffer, tout pirate en herbe peut lire à livre ouvert tous les identifiants et les mots de passe non cryptés qui circulent sur le réseau.
- Si le mot de passe est crypté, le pirate utilisera un logiciel dit de «craquage» et la qualité du chiffrement exigera un temps de «craquage» plus long.
- Sur Internet, vos messages sont transparents ainsi que vos accès aux serveurs que vous préférez. La transparence d'Internet offre à tous les indiscrets la possibilité de lire, le plus simplement du monde, le courrier des autres. Et sans beaucoup plus de peine, d'entrer dans les systèmes personnels de chacun et d'aller y feuilleter à livre ouvert des données qui auraient dû rester confidentielles.
- Votre entreprise possède un serveur WEB, vitrine virtuelles destinée à soutenir l'image de marque et montrer votre compétitivité, votre dynamisme et consolider des relations privilégiées avec vos clients. Etes-vous certain qu'il est suffisamment protégé et qu'il ne risque pas d'être modifié à votre insu? A témoin, le site du département de la justice transformé en département de l'injustice et quelques croix gammées retrouvées à la place du logo de gouvernement.
- Imaginez que votre nom, votre adresse IP, votre identité soient usurpés sur Internet à des fins criminelles. Comment organisez-vous votre défense pour prouver que vos coordonnées électroniques ont été utilisées à votre insu?

Des exemples classiques de délits informatiques:

- Zboralsky, un pirate exceptionnel, aurait usurpé en 1995 l'identité d'un patron du FBI et utiliser ses cartes de communication afin d'accéder à son propre compte.
- Les phreacker sont ceux qui volent les codes d'accès afin de téléphoner gratuitement en utilisant le standard informatique d'une entreprise.

Il est étonnant de constater avec quelle facilité un pirate peut recevoir des informations confidentielles par téléphone.

- Mitnick dès 1992 a provoqué de nombreux dégâts d'un volume financier important. Il est entré dans les systèmes informatiques de certaines entreprises afin de relever les 20 000 numéros de carte de crédit des fournisseurs de services on line. Un autre jour, il transfert l'intégralité de la note de téléphone de l'hôpital sur la facture privée d'une de ses relations.

Conclusion

La pratique de la sécurité informatique est imposée par la force des choses dès que l'entreprise ou l'organisation est connectée et accessible par des réseaux publics, par exemple Internet.

Dès ce moment, les responsables prennent conscience que leur activité dépend étroitement de leur système d'information. En même temps, ils prennent conscience de la vulnérabilité de ce dernier.

Les 3 caractéristiques de la sécurité informatique sont:

- Disponibilité: vous désirez utiliser vous-même vos informations.
- Intégrité: vous ne désirez probablement pas que d'autres personnes les modifient.
- Secret: vous ne désirez probablement pas que d'autres connaissent vos données confidentielles.

Afin de disposer d'un système d'information intègre et confidentiel, il est utile d'approfondir les points suivants:

1 La sensibilisation aux risques: les directions générales et les responsables informatiques ne sont actuellement pas tous conscients des risques.
2 Les risques proviennent en majorité de l'intérieur de l'entreprise.
3 Il existe bel et bien un risque d'intrusion – de l'intérieur du réseau ou de l'extérieur – des systèmes d'information qui court-cir-

cuite totalement la gestion des accès et qui profite des vulnérabilités nombreuses et connues des systèmes. Pour s'en protéger il ne suffit pas d'installer un firewall. Une réduction complète des vulnérabilités des systèmes est nécessaire.

4 La sécurité exige une approche globale qui analyse les risques et qui prenne en conséquence un ensemble de mesures cohérentes dans les domaines techniques (gestion des accès, sauvegardes, firewall, filtrages, cryptage, réseau virtuel privé, etc.) et organisationnels, ainsi que par un processus d'amélioration continue.

Références

D. Brent Chapman et Elizabeth D. Zwicky, La sécurité sur Internet. Firewall. Ed. O'Reilly International Thomson, Paris, 1996

Tom Sheldon, Guide pratique de la sécurité sous windows NT, International Thomson publishing France, Paris, 1997

Karanjit Siyan & Chris Hare, Internet. Sécurité & Firewalls, Simon & Schuster Macmillan (France), Paris, 1996

David J. Stang et Sylvia Moon, Sécurité réseaux, Dunod, Paris, 1996

Terry Bernstein, Anish B. Bhimani, Eugene Schultz et Carol A. Siegel, Sécurité Internet pour l'entreprise, International Thomson publising France, Paris, 1997

John Vacca, Sécurité sur Internet, Sybex, 1997