Les crimes informatiques explosent

- Informatique - Sécurité Informatique -

Date de mise en ligne : jeudi 1er octobre 2009

Entreprises privées, cotées en Bourse et gouvernements du Canada partagent un très gros problème, les brèches de sécurité et les dépenses qui y sont liées ont explosé en 2009.

C'est l'inquiétant constat effectué par une étude conjointe publiée aujourd'hui par le le géant des télécoms Telus et son partenaire Rotman School of Management de l'Université de Toronto.

Le sondage mené auprès de 600 spécialistes en sécurité des technologies de l'information signale que le nombre moyen de brèches a augmenté de 276% par organisation.

Conséquemment, les dépenses connexes ont bondi de 97% pour une moyenne de 834 000 $ en 2009.

Les organismes gouvernementaux sont la cible la plus fréquente des malfaiteurs en informatique. Leurs dépenses moyennes en la matière ont plus que triplé pour atteindre 1 M$. Les société fermées paient 807 000 $ - un chiffre plus que doublé - alors que les sociétés cotées en Bourse ont enregistré une variation haussière de seulement 6%.

Parmi les principaux problèmes, les accès non autorisés à des renseignements par des employés ont grimpé de 112%. Les vols de renseignements confidentiels ont monté de 75% et les vols d'ordinateurs portables ou autres appareils portatifs ont augmenté de 56%.

La brèche la plus fréquente, soit 62% des cas, se fait par l'intermédiaire de virus ou de logiciel espion. Le hameçonnage constitue 27% des brèches. Les attaques qui visent à empêcher un réseau de répondre aux demandes s'élèvent à 17%. Les actes commis par les employés à l'interne représentent eux aussi 17% des cas.

Comment réagir au problème ? L'étude Rotman-Telus signale que les organisations qui dépensent plus de 5% de leur budget techno pour la prévention en récoltent les fruits. Cela se fait surtout sentir dans la protection des communications sans fil, des mots de passe, dans le blocage des attaques par applications Web et dans le vol d'identité.

Un problème de prévention

Un autre aspect frappant qui ressort de cette étude, c'est la fréquence d'évaluation des risques. Environ 68% des organismes gouvernementaux se penchent sur la question au mieux une fois par année.

Environ 60% des compagnies cotées en Bourse font ce travail aux six mois ou plus souvent. Enfin, les entreprises au capital fermé se divisent également entre ces deux catégories de fréquence.

Toutefois, un fait inquiétant demeure : 42% des entités sondées n'ont pas de plan formel d'évaluation des risques.

« Nos recherches indiquent que les règles sur la conformité représentent un des facteurs ayant contribué à cette flambée des pertes liées à la sécurité informatique », dit Walid Hejazi, professeur d'économie de l'entreprise à la Rotman School of Management.

« Bien que la conformité ne puisse expliquer dans tous les cas la hausse du nombre de brèches de sécurité, ajoute M. Hejazi, il faut souligner qu'elle est devenue un facteur beaucoup plus déterminant pour les sociétés fermées et les

organismes gouvernementaux en 2009, ce qui fait que les capacités qui permettent de détecter les menaces à la sécurité et d'y réagir se sont considérablement améliorées. »

« Ainsi, poursuit le professeur, les organisations détectent maintenant plus de menaces qu'auparavant et elles doivent, par conséquent, consacrer une plus grande part de leur budget pour intervenir de manière appropriée. »

Alan Lefort, directeur général des Laboratoires de sécurité Telus, déplore que la gestion des risques technologiques est souvent mal planifiée. « Sans une gestion qui tient compte des menaces et qui évalue les capacités de bout en bout, elles sont souvent prises au dépourvu lorsqu'un nouveau type d'attaque ou de vulnérabilité devient le centre d'attention. »

Post-scriptum :

http://argent.canoe.ca/lca/affaires...