



Direction Informatique Express

édition du 2 novembre 2007

2 novembre 2007

Pleins feux sur la sécurité informatique

02/11/2007 - Halloween a inspiré plusieurs fournisseurs et firmes de recherche qui ont publié des études ayant pour thème la protection des données sensibles.

Alain Beaulieu

CA Security Management

- Solution globale et complète
- Evolutivité inégalée
- Intégration et modularité

ca Transforming IT Management

► Cliquez ici pour accéder au livre blanc intitulé « Gestion de la sécurité : aligner la sécurité sur l'activité de l'entreprise »

En cette semaine d'Halloween où la peur et le danger sont à l'honneur, la sécurité informatique a beaucoup attiré l'attention des entreprises de TI et des firmes d'analyse de marché qui ont publié plusieurs études sur le sujet.

Parmi celles-ci il y a [Fusepoint](#) qui a révélé les conclusions d'un sondage canadien sur la sécurité des données, que [Léger Marketing](#) a réalisé pour elle, cet été, auprès de 1 200 employés canadiens, dont 495 cadres supérieurs. Établie à Montréal, Fusepoint fournit aux entreprises des services applicatifs et des services d'infogérance d'infrastructure informatique.

Ce sondage souligne le sentiment d'insécurité qui règne dans les entreprises, alors que les employés et les cadres supérieurs pensent que les renseignements confidentiels dont dispose leur entreprise sont mal protégés. Le sondage indique plus précisément que 48 % des cadres supérieurs canadiens craignent pour la sécurité des renseignements confidentiels, même si 71 % de ces renseignements sont protégés par des politiques et des procédures spécifiques. C'est seulement deux cadres supérieurs sur cinq (37 %) qui affirment se sentir vraiment en sécurité et seulement un sur quatre (24 %) qui soutiennent pouvoir décrire, avec précision, les mesures de sécurité de leur entreprise.

Qui plus est, plus des deux cinquièmes (42 %) des cadres supérieurs n'ont aucune idée de la valeur monétaire qu'une atteinte à la sécurité pourrait avoir pour leur entreprise, et ce, bien que 62 % de ceux-ci croient qu'une telle atteinte nuirait à la réputation de leur entreprise. Quoi qu'il en soit, ils semblent vivre assez bien avec ce sentiment d'insécurité, puisque 81 % d'entre eux se sentent personnellement responsables de la sécurité des données de leur entreprise...

Le sentiment d'insécurité des employés est encore plus grand que celui des cadres, puisque 85 % d'entre eux ne croient pas que les renseignements personnels conservés dans les bases de données en ligne sont en sécurité. Le fait que 12 % d'entre eux aient été victimes d'un vol d'identité ou connaissent quelqu'un qui l'ait été explique le peu de confiance qu'ils ont à l'égard de la sécurité des bases de données en ligne. Par ailleurs, un employé sur six (17 %) affirme que son entreprise a déjà subi une atteinte à la sécurité de ses ressources informationnelles.

En outre, les cadres supérieurs croient que la menace provient autant de l'interne, alors que des employés n'ont pas un comportement très sécuritaire et téléchargent virus et logiciels espions sans le savoir, que de l'externe, et ce, bien que ces mêmes cadres croient que les attaques provenant de l'extérieur aient crû depuis 2005. Malgré cela, un cadre supérieur sur cinq affirme que son entreprise n'utilise pas d'antivirus et un sur quatre, que son entreprise fonctionne sans coupe-feu. D'une manière générale, la moitié de cadres et des employés interrogés sont d'avis que leur entreprise ne fait pas tout ce qu'elle devrait pour protéger adéquatement les consommateurs.

Revirement de situation à venir

Tout n'est pas perdu, puisqu'un prochain revirement de situation est plausible. C'est du moins ce que conclut la firme [Astaro Corporation](#), qui a réalisé un sondage mondial plus tôt cette année auprès de 2 800 professionnels de TI, dont les deux tiers (67 %) se disent préoccupés par la fuite d'informations confidentielles. Or, seulement 22 % de ceux-ci ont recours au cryptage des courriels. La firme américaine spécialisée dans les systèmes de gestion unifiée des menaces s'attend donc à ce que les investissements en ce sens augmentent prochainement.

Ce sont toutefois la protection des réseaux étendus, l'évaluation des vulnérabilités et la protection des applications Internet qui domineront les investissements en sécurité des entreprises au cours des cinq prochaines années. En fait, 65 % des professionnels interrogés ont indiqué qu'ils allaient investir dans ce domaine.

Aujourd'hui, la totalité des spécialistes ont dit s'en remettre principalement à un pare-feu pour se protéger des attaques externes, suivi d'un antivirus (91,5 %), d'un antipourriel (90 %), d'une solution de réseau privé virtuel ou VPN (81 %) et d'un système de protection contre les intrusions (74 %).

Finances et zombies

Dans le domaine particulier des services financiers, la gestion des risques qui pèsent sur les informations confidentielles détenues par les institutions bancaires serait en tête des priorités des décideurs qui y oeuvrent, selon une récente étude européenne réalisée par [Datamonitor](#) à la demande du fournisseur de solutions de sécurité [RSA](#). En fait, 75 % des responsables de la sécurité informatique interrogés affirment comprendre les avantages qu'offre une gestion intégrée de l'ensemble du cycle de vie des informations.

Cela étant dit, les actions entreprises sont plutôt timides, dans la mesure où moins du tiers des responsables ont adopté une approche intégrée de gestion des informations. À titre d'exemple, 47 % des responsables interrogés ne se préoccupent pas de la sécurité du périmètre et préfèrent s'en tenir à la seule protection des informations. On a donc tendance à appliquer, dans ce secteur, une approche de gestion par silos.

[IBM](#) a aussi réalisé une étude mondiale sur le secteur financier, qui montre que les entreprises sont mal préparées pour faire face aux conséquences d'un événement à risque majeur. En fait, 42 % des entreprises ayant connu un tel événement reconnaissent qu'elles étaient mal préparées (62 % des entreprises affirment avoir connu au moins un tel événement). Ce sont seulement 52 % des entreprises qui ont mis en place un programme officiel permettant de faire face à un tel événement. Menée auprès de 1 200 dirigeants financiers, l'étude conclut que ce sont les organisations de finance intégrées, qui appliquent des normes et des procédures communes à l'ensemble de l'entreprise, qui sont les mieux préparées.

[Finalement, Symantec](#) a, quant à lui, publié un rapport de sécurité sur les réseaux de zombies (*botnets*), c'est-à-dire une armée d'ordinateurs contrôlés à distance par un pirate, menant des attaques coordonnées dont l'objectif est de paralyser des réseaux et des systèmes informatiques. Les ordinateurs sont contrôlés via un logiciel malicieux (bot) qui y est téléchargé. Les attaques menées par les réseaux de zombies, qui constituent actuellement la plus importante menace provenant d'Internet, selon Symantec, peuvent aussi servir au vol d'identités.

Or, il s'avère que le Canada est le deuxième pays affichant le plus fort taux d'attaques par utilisateur, après Israël, juste avant les États-Unis. Le Canada est, plus précisément, la cible de 6 % de toutes les attaques provenant d'Internet, mondialement. Le fait que durant la première moitié de l'année, le Canada ait affiché le plus fort taux d'utilisation d'Internet, en termes de nombre d'heures par citoyen, n'est pas étranger à cela.

Quoi qu'il en soit, espérons que le climat morbide qui prévalait le soir d'Halloween ait poussé quelques responsables à remettre en question l'approche qu'applique leur entreprise pour protéger les données sensibles. Car la solution au problème que pose la protection des ressources informationnelles passe avant tout par l'instauration de méthodes de travail sécuritaire. On a beau avoir les meilleurs outils disponibles sur le marché, mais si on fait preuve de négligence, les « zombies » et autres vampires finiront par avoir le dernier mot.

Alain Beaulieu est adjoint au rédacteur en chef au magazine Direction informatique.

Fermez la fenêtre