



Nos experts ont la parole

## **Easybourse.com**

2 juin 2009

Laurent Gobbi, Associé KPMG

Christophe Ternat, Manager KPMG



Avec l'aimable autorisation de Easybourse.com :

[www.easybourse.com](http://www.easybourse.com)



**L. Gobbi et C. Ternat**  
**Associé KPMG\* et Manager KPMG\***  
**«Une menace croissante sur les systèmes d'information»»**  
**(Easybourse.com)**

Dans un contexte économique difficile où la concurrence est exacerbée, les attaques cybercriminelles contre les acteurs économiques sont en très nette augmentation, selon notre dernière étude internationale sur la cybercriminalité.

En effet, ces actes qui pouvaient, il y a peu, être considérés comme du vandalisme sont aujourd'hui liés à des intérêts économiques. Les cybercriminels attaquent directement les flux financiers ou revendent les données dérobées à leurs victimes.

Dans ce cadre, nous avons réalisé, en collaboration avec le cabinet AKJ Associate, une étude sur la cybercriminalité. Entre le 3 février et le 13 mars 2009, nous avons interrogé plus de 300 personnes en charge de l'audit, la gestion des risques ou la sécurité des systèmes d'information dans des organisations de types et de tailles diverses à l'échelle mondiale.

### **Des ressources jugées insuffisantes pour la sécurité des systèmes d'information des entreprises**

La sécurité, tout comme l'informatique, est souvent perçue dans les entreprises comme un centre de coût. Souvent, les investissements dans la sécurité ne permettent pas d'accroître directement la performance ou les revenus de l'entreprise et le retour sur investissements est difficilement mesurable.

**Les ressources accordées à la sécurité jugées insuffisantes pour 62% des professionnels interrogés**

L'enquête révèle que les vecteurs de décision permettant de lancer des actions relatives à la sécurité proviennent essentiellement de l'environnement extérieur : un incident majeur chez un concurrent, la volonté de se mettre en conformité réglementaire, ou un incident ayant influé sur l'image de l'entreprise.

Pour 67% des personnes interrogées, le budget est la principale limite à la mise en place de systèmes de sécurité efficaces contre la cybercriminalité. Les responsables de la sécurité des systèmes d'information confirment qu'il est difficile pour eux de légitimer ces dépenses auprès du management en démontrant l'impact de potentiels incidents de sécurité sur le business.

En conséquence, les entreprises adoptent souvent des postures défensives, car leur priorité est de répondre aux menaces visibles. Ces ressources insuffisantes rendent difficile la mise en place d'une organisation proactive qui permettrait

d'anticiper les menaces et de réduire les risques associés.

## **50% des responsables de la sécurité informatique estiment que les entreprises sont insuffisamment protégées contre les « malware ».**

Les « malwares », ou « codes malveillants », sont des programmes nocifs introduits sur un ordinateur à l'insu de l'utilisateur tels les virus, vers, logiciel espion, etc. Les antivirus et autres outils de protection contre les malwares s'appuient principalement sur une base de signatures pour les détecter.

**79% des personnes interrogées affirment que les logiciels de sécurité construits sur des bases de signatures n'offrent pas un niveau de sécurité suffisant.**

Néanmoins, de plus en plus de codes malveillants sont capables de se présenter sous des formes différentes, déjouant totalement leur détection par les outils s'appuyant sur une base de signature.

L'une des personnes interrogées lors de notre étude nous a déclaré : « Nous avons dernièrement subi une attaque par l'intermédiaire d'un code malveillant dormant installé sur nos serveurs. Ce malware n'avait pas été détecté pendant 10 mois ! Combien d'autres malwares de ce type contaminent aujourd'hui notre informatique ? »

Si des méthodes d'analyses comportementales apparaissent dans les antivirus, elles restent aujourd'hui encore trop timides. En effet, le principe de « blacklist » (bloquer seulement certaines opérations) reste prépondérant. Une approche par « whitelist » (autoriser seulement certaines opérations) représente la prochaine étape dans l'amélioration de la maturité de ces logiciels.

## **Les sites Internet infectés par des malwares et les téléchargements constituent les principales difficultés rencontrées par les professionnels de la sécurité pour protéger leurs infrastructures**

Si par le passé les « hackers » cherchaient à faire parler d'eux par le biais de messages laissés sur la page de garde des sites Internet qu'ils avaient pu pirater, aujourd'hui leur ego est bien moins mis en valeur. En effet, les attaques actuelles des sites Internet s'attachent, pour une grande partie d'entre elles, à mettre en place des malwares qui ne modifient en rien l'esthétisme de ces sites. Plutôt ingénieuses, ces attaques profitent de la fréquentation des sites infectés pour contaminer leurs visiteurs : chaque internaute visitant le site infecté se fait infecter à son tour.

Les entreprises sont donc confrontées à deux problématiques : augmenter le niveau de détection des attaques afin d'identifier rapidement tout type d'attaques de leurs sites Internet, et protéger les postes de leurs utilisateurs pour éviter la diffusion des malwares présents sur les sites infectés.

Par ailleurs, les téléchargements de fichiers restent une menace d'actualité. Les antivirus de flux (proxy) et les antivirus de poste (antivirus installés sur les postes de travail et les serveurs) se doivent d'être maintenus à jour tant sur les moteurs de détection que sur les bases de signatures utilisées.

## **Les applications accessibles depuis Internet, des zones sensibles de l'infrastructure informatique**

Particulièrement visées, elles présentent deux opportunités importantes pour les organisations cybercriminelles.

D'une part, elles proposent un service depuis Internet. Il est donc aisé d'attaquer ce service depuis n'importe quel endroit du monde (accessibilité) pendant une période de temps non contrainte. De plus, leur anonymat est quasiment garanti.

D'autre part, ces services sont fréquentés par des visiteurs de toute nature. Plus ces sites infectés sont fréquentés plus la propagation des malwares installés est importante.

Il faut aussi noter que les terminaux mobiles (PDA) représentent également un vecteur important compte tenu du faible niveau de maturité en termes de sécurité liée à la jeunesse de ces technologies.

### **La crise et la cybercriminalité**

La crise actuelle tend à augmenter les risques liés à la cybercriminalité. En effet, les facteurs amenant les employés à commettre des actes de fraudes sont intensifiés par les conséquences de la crise :

- ▶ leur motivation : peur de la perte d'emploi, bonus revus à la baisse, pressions financières,
- ▶ l'occasion : la suppression de poste peut entraîner des terrains favorables à la fraude comme le non-respect du principe de séparation des fonctions,
- ▶ la rationalité économique : désir de prendre ce que les employés croient comme dû et qui n'a pas été accordé à cause du contexte économique défavorable.

De plus, la connaissance des faiblesses des systèmes et des processus de l'entreprise ainsi que leur facilité d'accès aux ressources dont les données (informations financières, clients,...) de l'entreprise présentent des risques importants. Le personnel informatique représente un risque particulier, car il possède souvent des droits étendus ainsi qu'une bonne connaissance des forces et des faiblesses du système d'information de l'entreprise.

**Deux professionnels sur trois (66%) estiment que les informaticiens, susceptibles d'être licenciés du fait de la crise, pourraient être amenés à mettre leurs compétences et leurs connaissances au service de l'économie cybercriminelle.**

Enfin, la concurrence exacerbée par le climat de crise actuelle accentue la valeur des données clients dont le vol devient le premier risque cité par les personnes ayant répondu à l'enquête.

Ces risques peuvent toutefois être limités en mettant en place ou en renforçant les processus de l'entreprise tels que la gestion des départs. Ce processus particulier doit être généralisé à tous les utilisateurs (employés, stagiaires, personnels intérimaires, prestataires et partenaires) et à tous les composants du système d'information. Il se doit également d'inclure la suppression systématique de l'ensemble des accès informatiques de l'utilisateur ainsi que la récupération du matériel mis à sa disposition.

**Publié le 02 Juin 2009**

Copyright © 2009 **easy**BOURSE

\* Laurent Gobbi est Associé au sein du cabinet KPMG en charge des activités de conseil et d'audit des systèmes d'information

\* Christophe Ternat, est Manager au sein du cabinet KPMG, responsable de la ligne de service sécurité des systèmes d'information

### ► **Méthodologie de l'étude**

Présentée lors du 7ème congrès international sur la cybercriminalité qui s'est tenu à Londres les 24 et 25 mars 2009, cette étude réalisée par KPMG en collaboration avec AKJ Associates, a été menée entre le 3 février et le 13 mars 2009 auprès de 307 collaborateurs majoritairement européens (78%) et issus de différents métiers : sécurité informatique, détection de fraude, sécurité des entreprises, audit et risque.

Plus de la majorité des professionnels interrogés (80%) travaillent dans le secteur privé aussi bien dans la distribution, les télécommunications, l'énergie, les jeux d'argent, les médias, l'industrie, les transports, la logistique et des établissements financiers. Les secteurs non-marchand et public sont également représentés.