Guides de sécurité pour les petites entreprises

Qui représente la plus grande menace ?
Le personnel ou les cybercriminels

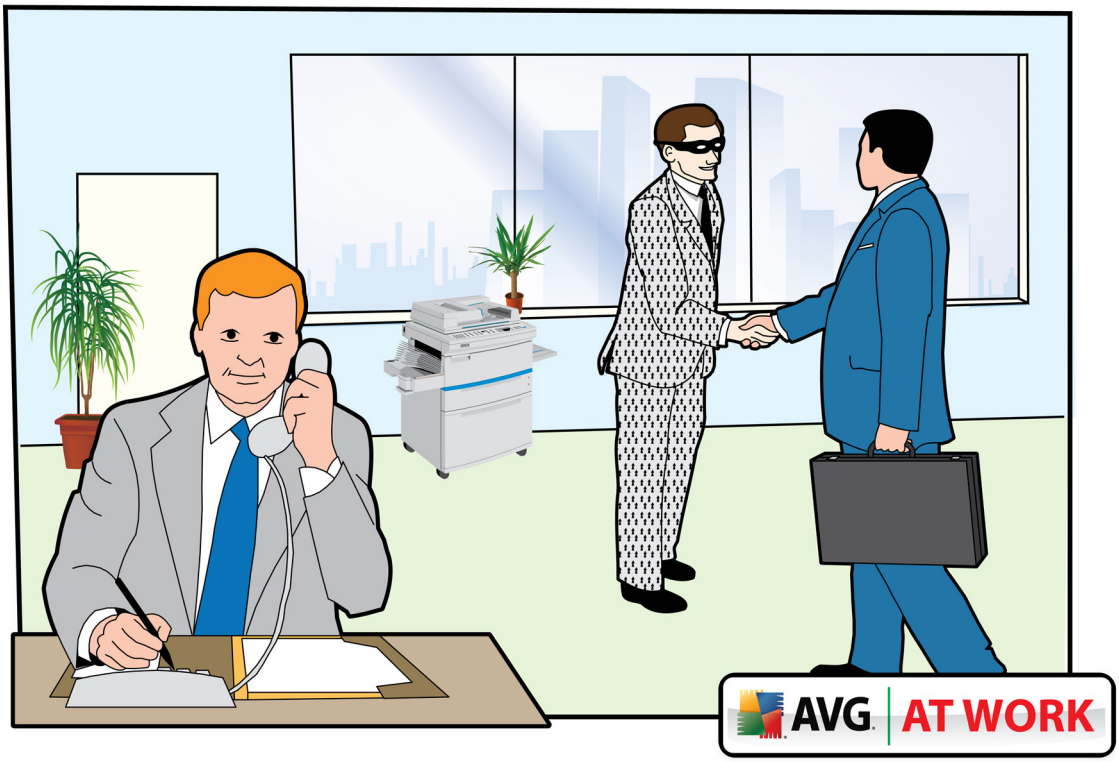
AVG AU TRAVAIL

Qui représente la plus grande menace ? Le personnel ou les cybercriminels

Le personnel interne est traditionnellement considéré comme représentant une menace plus importante pour la sécurité des entreprises que les pirates externes. Cela reste-t-il vrai compte tenu du perfectionnement croissant des cybercriminels ?

Le saviez-vous ?

- Il y a une dizaine d'années, les virus et autres formes de logiciels malveillants étaient principalement produits par de jeunes codeurs amateurs en mal de célébrité
- Les recherches effectuées par Verizon indiquent que soixante-quatorze pour cent des brèches de données proviennent de sources externes
- Les chiffres cités par le Forum Économique Mondial révèlent que les vols en ligne à eux seuls représentaient environ mille milliards de dollars en 2009.



La sagesse populaire considère que la principale menace pour la plupart des réseaux informatiques d'entreprise est posée par des employés mécontents plus que par d'obscurs cybercriminels. Les employés ont accès aux mots de passe et, dans le cas du service informatique, aux droits d'administrateur. De plus, ils savent généralement ce qu'ils cherchent et la valeur que peuvent avoir ces informations pour un concurrent.

Le concept de ce que l'on appelle « menace interne » existe depuis longtemps dans les cercles de sécurité informatique et semble basé en partie sur une étude réalisée par le FBI au début des années 1990 et qui a conclu que 80 pour cent des attaques de sécurité informatiques étaient perpétrées en interne. Toutefois, les choses ont bien changé en vingt ans : c'est l'équivalent d'un millénaire en temps Internet. Alors qu'autrefois, les pirates et les auteurs de virus étaient souvent des gosses qui voulaient s'amuser, la cybercriminalité s'est bien développée et est devenue une véritable industrie. Les chiffres cités par le Forum Économique Mondial indiquent que les vols en ligne à eux seuls représentaient environ mille milliards de dollars en 2009.

Cette « industrialisation » efficace de la cybercriminalité pourrait bien avoir eu un effet sur la perception de la « menace interne » : faut-il toujours la considérer comme la principale priorité en termes de sécurité informatique ? Des groupes criminels organisé qui cherchent à s'infiltrer dans les réseaux d'entreprise, comme d'autres pourraient viser la salle des coffres d'une banque, peuvent sembler plus dangereux qu'un employé licencié ou mécontent. Un rapport AVG, intitulé « Why Traditional Anti-Malware Solutions Are No Longer Enough » explique pourquoi les entreprises pourraient être amenées à reconsidérer l'essentiel de l'affectation de leurs ressources de sécurité.

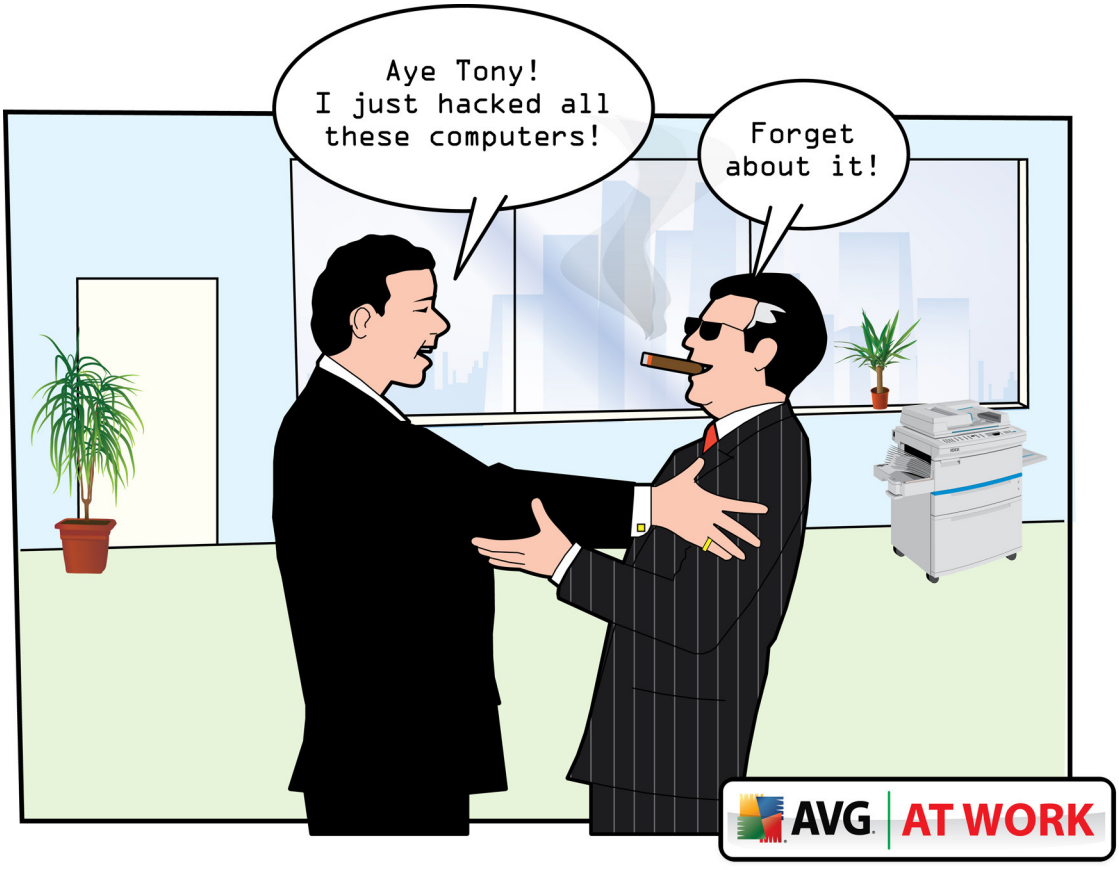
« Il y a une dizaine d'années, les virus et autres formes de logiciels malveillants émanaient principalement de jeunes codeurs amateurs en quête de célébrité qui voulaient se faire un nom dans les communautés underground de pirates », explique le rapport, qui ajoute que : « Toutefois, le paysage de la sécurité a bien changé depuis quelques années ». Les groupes de criminels organisés ont compris qu'il y avait de l'argent à gagner dans les logiciels malveillants et ont recruté des programmeurs de talent pour créer des programmes malveillants. Ces programmes n'avaient pas pour but de provoquer des perturbations, mais de permettre le vol d'argent, de

données ou des deux. Cela a abouti à la création d'une économie souterraine dans laquelle les criminels peuvent acheter et vendre des données et les programmes utilisés pour voler ces données ».

Toutefois, même si les menaces externes semblent s'être organisées avec le soutien de réseaux criminels, cela signifie-t-il nécessairement qu'elles dépassent les risques posés par des employés mécontents ? Les experts semblent partagés sur cette question ; c'est dû en partie à la définition de ce qui constitue une menace interne, par opposition à une menace externe. Même si la nature de la cybercriminalité a peut-être changé au cours des vingt dernières années, il en va de même pour l'entreprise moyenne. Les entreprises sont de plus en plus fragmentées et comptent de plus en plus sur des consultants et des experts externes. D'autres facteurs, tels que les fusions et acquisitions en nombre croissant, ont rendu floues les limites autrefois stables de certaines grandes entreprises après leur fusion avec des concurrents dont elles conservaient le personnel.

Dawn Cappelli, responsable expérimentée du personnel technique de l'équipe de CERT Computer Emergency Response Team (réponse aux urgences informatiques) de l'université Carnegie Mellon, a récemment expliqué comment l'entreprise avait dû modifier sa définition du mot interne pour suivre le rythme des pratiques professionnelles. « Notre définition de la menace interne fait référence à un employé, sous-traitant ou partenaire actuel ou antérieur », a-t-elle expliqué. « Nous avons récemment ajouté le terme partenaire à cette définition en raison des tendances récentes auxquelles nous assistons ».

De son côté, le CERT, l'un des plus importants organismes de sécurité informatique aux États-Unis, soutient toujours l'idée selon laquelle les entreprises devraient concentrer toute leur attention en termes de sécurité informatique vers les menaces internes. L'une des sections du site Web de cet organisme se consacre à la « Recherche des menaces internes ». « Les pirates internes, grâce à leur accès légitime aux informations de leur entreprise, à ses systèmes et réseaux, présentent un risque considérable pour les employeurs. Certains employés qui connaissaient des problèmes financiers ont alors eu l'idée d'utiliser les systèmes qu'ils côtoient chaque jour à leur bureau pour commettre des fraudes », explique l'organisme dans un rapport intitulé « L'image globale » du sabotage informatique interne. (www.cert.org/archive/pdf/08tr009.pdf)



Toutefois, si des organismes comme le CERT connaissent bien les menaces que représentent les employés, d'autres entreprises considèrent que le raffinement et l'organisation croissants des cybercriminels ont irrémédiablement transformé les règles du jeu. La société de télécommunications Verizon est convaincue que les entreprises devraient se concentrer sur les menaces externes. Le rapport d'enquête sur les brèches de données professionnelles Verizon réalisé en 2009 (www.verizonbusiness.com/fr/Products/security/dbir/) révélait en effet que soixante-quatorze pour cent des brèches de données provenaient de sources externes et que 32 pour cent émanaient de partenaires commerciaux. « Seules 20 pour cent d'entre elles ont eu lieu en interne, un résultat qui pourrait aller à l'encontre de nombreuses idées reçues largement répandues », précisait le rapport.

Le rapport Verizon reconnaît également que de nombreuses brèches de sécurité internes ne sont pas signalées par les entreprises, lesquelles s'efforcent de contenir la publicité négative qui pourrait résulter de la publication d'un tel incident. Toutefois, l'entreprise conclut malgré tout que même si certains incidents internes ne sont pas

signalés, les recherches effectuées au fil de plusieurs années soutiennent son argument selon lequel les attaques externes présentent une menace plus importante. « Les résultats de 600 incidents enregistrés sur une période de cinq années vont largement à l'encontre de l'idée très répandue selon laquelle la plupart des brèches sont le fait des employés », explique l'entreprise.

Cependant, même si certains spécialistes de la sécurité se concentrent sur la distinction entre menaces externes et internes, d'autres spécialistes pensent qu'une concentration excessive sur l'origine des attaques pourrait s'avérer être une distraction dangereuse. « Tout ce débat interne contre externe a toujours été une question de sémantique plus qu'autre chose », déclare le gourou de la sécurité Bruce Schneier dans son blog. « Si on compte les attaques, celles qui proviennent de l'extérieur sont nettement plus nombreuses, simplement parce que les agresseurs externes sont plus nombreux. En revanche, si on dénombre les incidents, les chiffres sont plus proches : dans ce cas, on obtient une proportion de 75 pour cent contre 18 pour cent. Enfin, si on calcule les préjudices, les attaques internes sont généralement les plus dangereuses, surtout parce que les agresseurs possèdent des informations beaucoup plus détaillées qui leur permettent de mieux cibler leurs attaques ».
(http://www.schneier.com/blog/archives/2008/06/it_attacks_insi.html)

Schneier pense que les entreprises feraient mieux d'adopter un point de vue plus holistique vis-à-vis de la sécurité informatique et de penser en termes de sauvegarde de leurs données et de leurs systèmes contre les attaques, d'où qu'elles viennent.
« Qu'elles soient d'origine interne ou externe, les attaques constituent un risque pour la sécurité et il faut se défendre contre les deux. Il n'est pas particulièrement utile d'essayer de les comparer », précise-t-il.

Il semble finalement que, même si le danger que présentent les cybercriminels de plus en plus perfectionnés a sans doute augmenté depuis quelques années, la nature de plus en plus fragmentée de nombreuses entreprises signifie que le personnel, les partenaires et même les clients représentent également des cibles éventuelles pour les pirates dits internes. Certes, les entreprises feraient bien de tenir compte des différentes tactiques utilisées par les deux groupes (les cybercriminels et les employés), mais la meilleure approche globale consiste à mettre en place une stratégie de sécurité solide et adaptative afin de pouvoir suivre les évolutions de la sécurité Internet.

Robert Gorby

AVG SMB group :
bit.ly/AVGSMB

Devenez fan d'AVG :
facebook.com/avgfree

Lisez nos blogs :
blogs.avg.com

Suivez-nous sur :
twitter.com/
officialAVGnews

Devenez un affilié Avg:
avg.com/gb-en/
affiliate

Regardez notre chaîne :
youtube.com/user/
officialAVG

AVG Technologies France
1, Place de la Chapelle
64600 Anglet
France
www.avg.fr

AVG Technologies CZ, s.r.o.
Lidická 31, 602 00 Brno
République Tchèque
www.avg.cz

AVG Technologies USA, Inc.
1 Executive Drive, 3rd Floor
Chelmsford, MA 01824
États-Unis
www.avg.com/us-en/
homepage

AVG Technologies UK, Ltd.
Glenholm Park, Brunel Drive
Newark, Nottinghamshire,
NG24 2EG
Royaume-Uni
www.avg.co.uk

AVG Technologies GER GmbH
Bernhard-Wicki-Str. 7
80636 München
Allemagne
www.avg.de

AVG Technologies CY Ltd.
Arch. Makariou III.
2-4 Capital Centre
1505, Nicosie, Chypre
www.avg.com

AVG AU TRAVAIL