

POURRIELS

Gros intrus, petites cuirasses

■ Huit courriers électroniques sur dix ne font qu'engorger les boîtes aux lettres.
 ■ Le filon pour s'en débarrasser prend de nombreuses formes, assez coûteuses.

Le spam (message électronique non désiré ou pourriel) réduit la productivité des utilisateurs, contraints de trier, un à un, des centaines de messages non sollicités par semaine. L'administrateur de la messagerie enregistre les plaintes, puis fait de son mieux pour filtrer les e-mails à l'aide d'outils encore imparfaits.

Précautions d'usage. Difficile de mettre en place une sécurisation globale lorsque des millions de messages sont déversés par des robots chaque jour plus malins que la veille. À partir d'adresses d'expédition usurpées, l'émetteur de courriels en masse fabrique des adresses aléatoires puis teste sans cesse les routeurs de messages. Il génère ainsi un trafic colossal de requêtes indésirables avant d'émettre tous azimuts ses flots de publicités, de virus et de programmes espions.

Des réseaux de robots esclaves sont formés à partir de simples micro-ordinateurs connectés à haut débit, sans pare-feu. Ces PC « zombies » propagent le spam à grande échelle, à l'insu de leur utilisateur. Ils contribuent à troubler les boîtes aux lettres des organi-

sations qui éprouvent toutes les peines du monde à se protéger efficacement.

Un nombre croissant d'entreprises perdent confiance dans l'usage de la messagerie électronique. La télécopie et le courrier postal, quoique plus lents, sont remis au goût du jour. Les cuirasses actuelles pour stopper le spam prennent la forme de logiciels, d'équipements dédiés ou de services loués à l'entreprise. Mais les filtres mis en œuvre sont vite contournés par les pollueurs. « Pour éviter de transformer des ressources universitaires en réseau "zombie", nous avons testé les parades Open Source, puis finalement investi dans un boîtier Iron Port à 30.000 euros pour contrôler 2.000 boîtes aux lettres électroniques », précise Patrice Garnier de l'université de Tours.

Former une ligne de défenses superposées limite les dégâts mais devient vite onéreux. L'industrie informatique cherche une parade plus efficace. Microsoft vient ainsi d'acquiescer l'éditeur Sybari Software pour ses combinaisons antispams accolées aux serveurs de messagerie d'entreprise. Car les « spameurs » n'hésitent pas, notamment, à piller l'annuaire d'une société.

Quelques précautions d'usage s'imposent aux professionnels désormais, comme le chiffrement des adresses électroniques publiées sur le Web. On peut aussi se doter d'autant d'e-mails que l'on a d'abonnements en ligne, mais cela permet surtout de tracer la provenance des fuites éventuelles.

Olivier Bouzereau

LES GESTES QUI SAUVENT

Une formation pour combattre la négligence des salariés

■ La mise en place de solutions complexes ne suffit pas à sécuriser une infrastructure.
 ■ L'accompagnement des collaborateurs est indispensable.

Pour reprendre une célèbre expression, « la sécurité informatique est l'affaire de tous », contrairement à ce que l'on croit trop souvent, la mise en place de solutions même complexes ne suffit pas à sécuriser une infrastructure.

Il est indispensable de faire respecter un certain nombre de consignes dans toutes les strates de l'entreprise pour les rendre efficaces. Avant tout, il faut savoir informer les collaborateurs des risques et des mesures à prendre. Attention, il n'est pas question du tout de semer la panique mais de leur expliquer ce qu'ils doivent faire, et pourquoi ils doivent le faire, pour les responsabiliser.

Miser sur la formation. Les différentes études réalisées sur la sécurité des systèmes d'information montrent qu'une grande partie des sinistres est d'origine humaine.

Certains sont volontaires (destruction de fichiers, vols...) et ont un but délibéré de nuisance (espionnage industriel, vengeance à la suite d'un licenciement...). Mais une grande partie est due à de la négligence (fichiers non sauvegardés, ma-

nipulations hasardeuses...) car, très souvent, les salariés n'ont pas été formés.

Sauvegarder et se méfier. Or les professionnels de la sécurité tirent la sonnette d'alarme. Une étude réalisée par le cabinet Ernst & Young montre que le principal obstacle à la mise en œuvre d'une sécurité des systèmes d'information efficace est la « faible prise de conscience des utilisateurs ». Un état qui est lié en particulier au fait que le « formateur » n'est pas clairement désigné.

Administrateur de la sécurité informatique, DSI, responsable de la sécurité générale ou PDG – dans le cas des PME : chaque entreprise, quelle que soit sa taille, doit désigner la personne qui ira présenter auprès de tous les collaborateurs les gestes essentiels.

En premier lieu, il faut sauvegarder régulièrement et systématiquement tous les documents de travail (textes, fichiers de tableur, éléments graphiques et visuels...). D'un point de vue économique, les pertes consécutives à cet oubli peuvent être considérables.

Au niveau de l'entreprise, la sauvegarde des éléments critiques sera dupliquée sur plusieurs supports et si possible entreposée en différents lieux géographiques.

L'autre élément clé consiste à ne pas ouvrir les e-mails dont on ne connaît pas l'expéditeur ou dont l'inti-

tulé semble louche. Au mieux, il s'agit d'un spam, en français un « pourriel ». Au pire, c'est un virus qui a traversé les couches de protection du système et qui risque d'infecter tout le réseau.

Si le courriel a été ouvert, il ne faut bien sûr jamais ouvrir la pièce jointe. L'e-mail doit être détruit et les responsables de la sécurité prévenus.

Généralement, au moment où commencent à se propager les virus, les éditeurs ont déjà envoyé les antidotes à leurs clients. Mais ceux-ci n'ont pas forcément achevé la mise à jour de tous les postes.

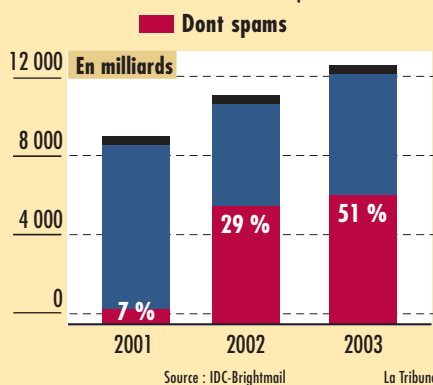
Ces recommandations contre les attaques extérieures valent aussi pour tous les éléments qui peuvent être introduits dans l'ordinateur comme la disquette, la clé USB ou les mini-disques durs.

Enfin, quand un collaborateur quitte une entreprise, il est fortement recommandé de bloquer immédiatement tous les accès (informatiques et physiques) dont il disposait.

Florence Puybareau

PLUS DE LA MOITIÉ DES COURRIELS SONT DES SPAMS

L'évolution du nombre total de courriers électroniques



focus LA SOLUTION D'UNE PME

Créer des listes blanches pour authentifier les expéditeurs

■ Fondateur et PDG de Mail in Black, Régis Novi propose une solution antispam fondée sur le principe d'authentification de l'expéditeur et non sur le filtrage de contenus. « Nous enregistrons 75 % de spams chez nos clients et 10 % de virus en moyenne. Le filtrage classique repose sur l'analyse de l'objet et du contenu des messages. Or le "spameur" contourne ces règles très vite. »

Une technique imparable. L'approche classique est loin d'être la panacée, démontre le jeune Marseillais, surtout lorsqu'elle exige un travail fastidieux à l'administrateur ou lorsqu'elle bloque à tort certains messages pertinents. « Le temps gagné par

utilisateur est perdu en recherche de faux positifs. »

Sous la forme d'un abonnement annuel de 40 euros par an et par poste de travail, Mail in Black recueille les messages pour le compte de l'entreprise, établit une liste blanche d'émetteurs, puis aiguille ainsi les seuls mémos désirés. L'expéditeur doit répondre une fois pour toutes à un défi en ligne. « Une technique imparable car seul un œil humain peut détecter le code aléatoire demandé. »

En cas d'absence de réponse au défi, l'abonné reçoit un récapitulatif de tout ce qui a été bloqué la veille pour récupérer ponctuellement, par exemple, la confirmation de son billet d'avion commandé sur Internet. O. B.

