



CASES articles

Tout le monde les connaît, mais que sont-ils réellement ?

Les spams et leur coût

Pour plus de sécurité, adoptez les réflexes CASES !

Le comportement de l'utilisateur constitue la base de sa protection

Plus de 70 % des e-mails transmis à travers le monde n'ont pas été sollicités par leurs destinataires, c'est ce qu'on appelle communément des spams. Chaque année, les collaborateurs d'une entreprise passent environ 1200 minutes à identifier et à effacer des e-mails. Les filtres anti-spam peuvent réduire les coûts liés à ces manipulations de près de 35 %. L'efficacité des mécanismes de filtrage dépend toutefois de la quantité d'e-mails reçus, du comportement des utilisateurs d'Internet et des connaissances dont disposent ces mêmes utilisateurs à propos de ces mails indésirables. Le comportement de l'utilisateur est en tout cas primordial dans le but de les endiguer.

« Les spammeurs ayant des motivations criminelles tentent d'exploiter à leurs fins la crise des crédits actuelle. Ils essaient ainsi de tirer profit des inquiétudes des consommateurs en envoyant un nombre bien plus important d'e-mails proposant des produits de services financiers directs ou en étroite relation avec le thème de l'argent. Il peut s'agir de tentatives de phishing, de jeux malhonnêtes, d'offres de crédits et d'emplois ou de toute autre forme d'incitatif financier ». Telle était l'interprétation de MessageLabs (société active dans le domaine de la sécurité de l'information) de la vague de spams observée en janvier 2008.

Mais qui est responsable du spamming ? Comment un utilisateur devient-il victime de spams ? Les filtres anti-spam permettent-ils de réduire les coûts pour les entreprises ? Et



comment peut-on éviter ces fameux spams ?

Les spammeurs

Outre les cybercriminels décrits précédemment, ce sont également les utilisateurs et les départements marketing des entreprises qui contribuent au spamming. Qui n'a, par exemple, jamais renvoyé de chaînes de lettres par e-mail ? Bon nombre de sociétés utilisent toujours les e-mails afin de faire de la publicité pour leurs produits ou d'attirer les usagers d'Internet sur leur page web. Il est bien sûr nécessaire d'établir une distinction entre spams publicitaires ou d'information et spams utilisés à des fins criminelles. Les effets préjudiciables de ces derniers peuvent évidemment être bien plus graves.

Comment un utilisateur devient-il victime de spams ?

Dès 2004, Bill Gates recevait quelque quatre millions de spams par jour. Les spammeurs disposent de divers moyens afin de se procurer les adresses e-mail des usagers d'Internet. Des logiciels spécifiques, appelés « robots », scrutent par exemple l'Internet à la recherche d'adresses e-mail et les stockent dans des banques de données.

Il est également possible que le fournisseur d'accès à Internet revende sa liste d'adresses e-mail à des tiers et que ceux-ci les communiquent à leur tour. Une multitude d'entreprises et de personnes privées peuvent ainsi entrer en possession de l'adresse e-mail d'un utilisateur. Ce procédé est légal, sous réserve que l'utilisateur ait accepté que son adresse puisse être communiquée.

De nombreux utilisateurs divulguent également leur adresse e-mail, par

exemple, sur des forums de discussion ou la font apparaître sur leur page personnelle. Les robots mentionnés ci-dessus sont alors en mesure de les enregistrer automatiquement.

Un utilisateur communique obligatoirement son adresse e-mail lorsqu'il effectue une commande sur une page d'e-commerce, lorsqu'il s'inscrit sur une liste de distribution d'e-mails ou lorsqu'il s'abonne à des services sur une page Internet. À ces occasions, l'utilisateur d'Internet devrait veiller à indiquer clairement qu'il n'autorise pas la divulgation de son adresse e-mail.

Les adresses e-mail peuvent également être générées. À cette fin sont combinés de toutes les façons possibles les noms et prénoms usuels ainsi que la liste des fournisseurs d'accès à Internet connus. Il en résulte la génération de centaines de milliers d'adresses e-mail, dont une bonne partie existe réellement.

Les filtres anti-spam réduisent les coûts pour les entreprises

L'Institut de recherche sur l'avenir du travail (« Forschungsinstitut zur Zukunft der Arbeit ») a étudié ce que peuvent coûter les spams par collaborateur. L'analyse se basait alors sur une université et son centre hospitalier. Lors de cette étude, l'Institut de recherche a également considéré l'utilisation d'une solution de filtrage anti-spam.

En 2006, les 5000 collaborateurs de l'université recevaient un total quotidien de 170 000 e-mails, dont environ 90 % étaient des spams. Il a été établi que durant l'année 2006, chaque collaborateur a ainsi passé en moyenne deux jours de travail à identifier et à effacer des spams. Au niveau d'une seule personne, ce chiffre peut sembler négligeable, mais il en va tout autrement lorsque l'on considère les 5000 collaborateurs de l'université.

Les coûts liés à l'installation et à la maintenance d'une solution de filtrage anti-spam pour 5000 collaborateurs s'établissaient à 15 120 EUR pour la

première année. En moyenne et par personne, cette solution a permis de réduire de 439 minutes le temps de travail nécessaire pour la détection et l'effacement de spams. Pour chaque collaborateur, le temps consacré aux spams a ainsi été diminué en moyenne d'environ 35 %, ce qui correspond à d'importantes réductions de coûts. Ces effets n'étaient toutefois sensibles que pour les utilisateurs qui recevaient un grand nombre de spams et qui disposaient de connaissances modestes relatives à ceux-ci, ou qui n'appliquaient pas les réflexes de protection adéquats afin de les éviter. Pour les utilisateurs bien informés en matière de spams, qui appliquaient des réflexes de protection adéquats pour les éviter ou qui étaient peu exposés à leur réception en raison de leur fonction, le filtre anti-spam n'a pas généré de diminution des coûts.

Les réflexes de protection pour éviter les spams

Il est déconseillé de répondre à des spams. D'une part, parce que l'expéditeur mentionné est bien souvent faux et, d'autre part, parce que cela confirmerait à un éventuel réel expéditeur que l'adresse à laquelle il a envoyé le spam est bien active, ce qui se traduirait par un nombre encore plus important de spams pour le destinataire.

Il est généralement recommandé de ne pas divulguer publiquement son adresse e-mail privée ou l'adresse e-mail de son lieu de travail. L'adresse e-mail privée devrait être réservée à un cercle restreint d'amis ou de collègues de travail. Il devrait s'agir de personnes de confiance. Les adresses e-mail sur le lieu de travail devraient être utilisées exclusivement à des fins professionnelles.

Lorsqu'il s'avère nécessaire de communiquer son adresse e-mail, l'utilisateur devrait veiller à ce que celle-ci ne puisse être divulguée « sans son autorisation formelle ». À défaut, fournisseurs d'accès et prestataires de services peuvent par exemple faire figurer l'adresse e-mail de l'utilisateur dans des listes publicitaires.

Conseil de sécurité :

De plus amples informations relatives au thème des spams et à leur identification peuvent être consultées sur le portail de la sécurité de l'information www.cases.lu. Une fiche thématique correspondante est ainsi disponible dans la rubrique Publications. Une excellente page web traitant des spams peut être consultée sur :

<http://spam.abuse.net/>.

Jusqu'au 26.10.2008, les collaborateurs du portail de la sécurité de l'information CASES ainsi que ceux de deux partenaires (Luxembourg Safer Internet et le Service National de la Jeunesse) répondent directement aux questions posées sur le thème de la sécurité de l'information. Il suffit pour cela de se rendre au stand d'exposition CASES (A03) lors de la Foire d'automne qui se tient à Luxembourg-Ville.

Informations sur la foire : du 18.10. au 21.10.2008, CASES a enregistré quelque 2000 téléphones mobiles dont l'interface Bluetooth était activée autour de son stand d'exposition. Les appareils dont la fonction Bluetooth est activée sont détectables dans un rayon de deux kilomètres grâce à des antennes spéciales. Les criminels peuvent exploiter la fonction Bluetooth activée par exemple pour accéder aux données contenues dans un téléphone mobile ou pour téléphoner à l'aide de celui-ci. Les visiteurs de la Foire d'automne peuvent suivre l'affichage des noms des téléphones mobiles ainsi détectés sur deux écrans sur le stand CASES. Lorsque la fonction Bluetooth n'est pas utilisée, il est recommandé de la désactiver par mesure de sécurité. Le projet commun de CASES et du Service National de la Jeunesse s'est poursuivi jusqu'à la fin de la Foire d'automne.

Les utilisateurs devraient également éviter de communiquer leur adresse e-mail privée ou professionnelle sur des forums ou des pages Internet.

Pour l'inscription sur des sites ne semblant pas dignes de confiance, l'utilisateur devrait disposer d'une ou de plusieurs adresses e-mail « poubelle ». Sur l'Internet, des prestataires de services tels que Hotmail, Yahoo, web.de, gmx.de ou freenet.de proposent des adresses e-mail gratuites.

Des mesures anti-spam permettent d'identifier les e-mails indésirables et de les juguler. À cette fin, des règles doivent être établies et adaptées au comportement de l'utilisateur.

Des programmes anti-spam installés au niveau des serveurs permettent de filtrer les e-mails avant leur distribution aux destinataires. Ceci donne la possibilité d'intercepter très tôt ceux qui sont indésirables. Les fournisseurs d'accès à Internet proposent par exemple ce genre de solutions à leurs clients. La boîte mails de l'utilisateur ne se retrouve ainsi pas submergée par les spams et les réseaux sont également moins encombrés.

Description : **spam**

Le terme de « spam » désignait initialement une marque commercialisant de la viande en conserve. Ce terme a par la suite été répété à outrance dans un sketch bien connu, ce qui lui a valu de devenir synonyme de réprobation. Il n'existe pas de définition officielle pour le « spam ». Le terme désigne aujourd'hui généralement tous les e-mails envoyés en masse à de nombreux destinataires, ceux-ci n'ayant alors pas sollicité leur réception. Pour les destinataires, ces e-mails signifient une perte de temps, car il faut les identifier et les extraire du courrier électronique légitime. Ils génèrent également des frais supplémentaires, sous forme de connexions Internet plus longues et de volumes de données plus conséquents à acheminer. De nombreux e-mails de spam contiennent également des malwares ou sont exploités pour d'autres actes criminels au détriment des usagers d'Internet. Pour les destinataires, les spams constituent une nuisance, un danger et un préjudice. En raison de la forte concurrence sur ce secteur, les coûts liés à l'envoi de spams sont très bas pour l'expéditeur. En 2006, plusieurs millions d'adresses e-mail valides ne valaient ainsi qu'un peu moins de 50 dollars.

Définition : **phishing**

Le phishing qualifie les agissements visant à obtenir les données d'utilisateurs par le biais de pages Internet falsifiées.

Les programmes anti-spam au niveau client mettent en œuvre des règles de filtrage. Ces règles doivent être définies par l'utilisateur et adaptées à son comportement. Les programmes anti-

spam installés au niveau des serveurs sont toutefois plus efficaces.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu