Partie 3

Fiche 7

Que faire, face aux comportements déviants ?

Sommaire

Introduction

L'accroissement du volume d'e-mail est un fait avéré. Toutes les messageries électroniques se remplissent avec des e-mails que l'on peut faire entrer dans 2 ou 3 grandes catégories :

- les e-mails non sollicités, et dont la réception peut être associée à une perturbation de l'activité normale ou à une pollution ;
- les e-mails non sollicités, mais dont la réception peut légitimement se justifier ;
- les e-mails qui correspondent à une activité que l'on pourrait qualifier de "normale".

La facilité d'utilisation et de diffusion des e-mails peut aussi devenir un fléau lorsqu'ils sont utilisés mal à propos.
Nombreuses sont les entreprises dont les salariés voient leur messagerie professionnelle se remplir et être polluée par des e-mails qui ne correspondent en rien à leurs attentes ou à leur activité professionnelle. Et il en est de même avec les messageries personnelles.
L'e-mail est ainsi victime de sa facilité d'utilisation, de son faible coût et finalement, de son succès.

Cette fiche fait le point sur ces différents types d'e-mails :

- le SPAM, qui est constitué d'e-mails non sollicités ;
- le PHISHING, méthode notamment basée sur des e-mails et qui vise à leurrer les destinataires afin de leur soustraire certaines de leurs informations confidentielles ;
- le HOAX, ou canular, version moderne des chaînes fondées sur la crédulité humaine ;
- les VIRUS, véhiculés par les e-mails comme des pièces jointes malveillantes ;
- avec l'une des conséquences possibles, les BOTNET, qui sont des réseaux de machines compromises pouvant être contrôlées à distance.

L'objectif de cette fiche est, pour chacun de ces

types, de le décrire succinctement, d'en montrer un exemple, et d'émettre quelques préconisations pour l'utilisateur et pour le décideur afin de faire changer les comportements.

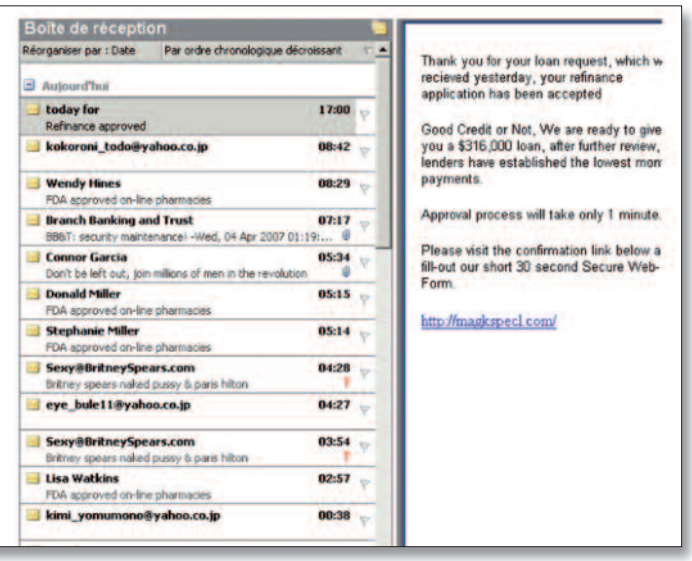
Le SPAM

Le SPAM est un e-mail non sollicité, envoyé massivement et souvent de manière répétitive, à vocation le plus souvent commerciale, à des destinataires dont l'adresse électronique a été collectée sans leur consentement explicite. Il est appelé également pourriel au Canada ou pollupostage en France. Le terme SPAM a été repris suite à un célèbre sketch des Monthy Python dans les années 70 et à sa lancinante réplique "spam, spam, spam, …".

Les chiffres varient selon les sources, mais pour la plupart elles estiment que le pourcentage de SPAM qui transite sur l'Internet serait supérieur à 75% du total des e-mails.
Les contenus de ces SPAM vantent souvent les mérites de soi-disant produits naturels ou miraculeux aux vertus rajeunissantes, aux effets miraculeux, ou capables de renforcer les performances physiques, le tout, bien entendu à des prix bien plus faibles qu'ailleurs. Parfois, il s'agit de produits pharmaceutiques d'autres natures, de montres prétendument de luxe ou de logiciels bureautiques dont on est censé pouvoir faire l'acquisition avec d'incroyables réductions.

Un exemple d'e-mail de SPAM :

Cette boîte aux lettres est envahie de SPAM



Recommandations

Pour l'utilisateur :

1) Vivre avec les SPAM

De plus en plus souvent, il est proposé dans le texte de l'e-mail, de suivre un lien ou de se connecter sur un site pour demander à être retiré de la liste de diffusion.
La première recommandation est de ne pas le faire ! En effet, cela risque surtout de produire l'effet inverse : demander à être retiré d'une liste de diffusion démontre l'utilisation réelle de l'adresse e-mail, ce qui incitera encore plus à l'inonder de nouveaux SPAM ! Donc, si vous ne connaissez pas l'expéditeur d'un e-mail, supprimez le message sans lire son contenu.

2) Disposer d'un anti-virus à jour

L'une des fonctions de l'anti-virus est de détecter les tentatives d'utilisation illicite d'un logiciel de messagerie. Si le poste de travail se trouve être infecté par un code malveillant, ce dernier peut être à l'écoute d'un ordre provenant d'Internet, et extraire des bases locales de destinataires ou d'expéditeurs pour collecter de nouvelles adresses d'e-mail, ou utiliser de façon furtive le logiciel de messagerie pour diffuser à son tour de nouveaux SPAM. Un anti-virus avec une signature anti-virale à jour permettra dans la plupart des cas, de détecter et d'éradiquer ce type de code malveillant.

Pour le décideur

3) Utiliser des filtres anti-SPAM

Aussi bien sur les passerelles, sur les relais et les serveurs de messagerie il est possible d'installer des logiciels qui vont détecter puis filtrer ces SPAM, mais une telle possibilité est aussi offerte pour les postes de travail. Ainsi, la plupart des logiciels clients de messagerie permettent aux utilisateurs de définir des filtres basés sur des mots clés ou sur des noms ou domaines émetteurs. D'autres solutions spécifiques sont vendues pour jouer le rôle de filtre de détection et de suppression de SPAM. Outre les performances et les caractéristiques techniques de ces produits, la granularité et la finesse de la détection et du filtrage sont des critères de choix importants avec le mécanisme de mise à jour des filtres.
Attention cependant aux messages identifiés comme SPAM alors qu'ils n'en sont pas (ce que l'on appelle des "faux positifs"). Il est aussi recommandé d'au moins en parcourir la liste avant de les effacer. Enfin, certains filtres anti-spam ajoutent devant le titre du message le marqueur "**SPAM**" et le délivre ainsi, laissant au destinataire le soin de choisir le mode de traitement à faire pour l'e-mail litigieux.

4) Suivre l'évolution de la législation

Devant l'ampleur du phénomène du SPAM, une directive européenne publiée en juillet 2002 oblige l'émetteur d'un e-mail à solliciter la permission de son interlocuteur avant de lui présenter son produit. Les Etats-Unis, tout en autorisant a priori l'émission d'un message publicitaire, obligent l'émetteur à avertir le récepteur de son droit de demander à être retiré de sa liste de distribution.

Les législations diffèrent donc d'un pays à l'autre, il est intéressant d'en suivre les évolutions. Dans le cas d'une entreprise internationale, il convient aussi de respecter les différentes législations locales.

Le PHISHING

Le phishing, aussi appelé "hameçonnage" au Canada et "filoutage" en France, est une tentative de récupération de données confidentielles basée sur la tromperie et le leurre, afin de les utiliser à des fins frauduleuses.

Le mot "phishing" vient de la contraction des mots "phreakers", un "ancien" mot qui désigne des fraudeurs des réseaux téléphoniques qui y accèdent et l'utilisent sans payer, et "fishing", l'action de pêcher, qui dans ce contexte se transforme en une pêche aux naïfs !

Son principe est simple et repose sur trois mécanismes :

- Un e-mail est reçu semblant provenir d'une autorité dont la réputation est grande et dont l'identité ne peut pas être mise en doute : une banque, avec utilisation du logo, des polices de caractères, des couleurs, et du style, un site de vente en ligne, un site de partage et d'échange... Tout alors semble conforme et rassurant. Il est généralement demandé au destinataire de l'e-mail de ressaisir les informations permettant de l'identifier de façon formelle. Le prétexte n'est pas toujours crédible (une banque ayant perdu les coordonnées de ses clients par exemple !). Un lien est généralement proposé et permet à l'utilisateur de se connecter sur le soi-disant site.

- Une fois connecté sur le site, il est donc demandé de donner les réponses aux quelques questions dont, les codes d'accès en ligne, le numéro de carte bleue avec bien entendu son code secret, le ou les mots de passe, ….

- Une fois les éléments d'identification recueillis, il ne reste plus au phisher qu'à tirer profit concrètement de son butin.

La messagerie électronique n'est donc qu'un véhicule pour des attaques de type phishing, mais sa combinaison avec une usurpation d'identité d'un prétendu émetteur rend le tout crédible… à première vue.

Le taux de phishing est en constante augmentation. Même si les banques anglo-saxonnes et nord-américaines ont été les premières à faire les frais de ces tentatives d'extorsion de fonds, plusieurs sociétés françaises ont aussi été affectées.

Les auteurs de phishing jouent aussi parfois sur les noms de domaines, ou même parfois sur les similitudes entre les caractères.

Prenons par exemple une organisation française dont le nom serait CNPF (sic), le nom de domaine complet « cnpf.fr » et le site Web « www.cnpf.fr ». Il y aurait ainsi au moins deux types d'attaques de phishing dont elle pourrait être victime :

- des personnes malveillantes pourraient vouloir faire croire que cette organisation dispose d'une interface « en ligne » pour les membres et déposer le nom de domaine « cnpf-enligne.fr » ou « cnpf-online.fr ». Il leur suffirait alors d'envoyer des e-mails en prétendant qu'un nouveau site dédié vient de s'ouvrir, de demander aux destinataires de s'y connecter, et de remplir les questionnaires en ligne, pour un motif fallacieux.

- Si de tels noms de domaines sont déjà déposés, ils pourraient envoyer des e-mails demandant aux destinataires de se connecter, en cliquant sur un lien directement fournit dans le corps de l'e-mail. Ils pourraient ainsi écrire « www. cnpf-enligne.fr » (le « l minuscule » est remplacé par un « I majuscule », ou WWW.CNPF-0NLINE.FR (le « O majuscule » est remplacé par « zéro ».

Dans la réalité, on trouve de nombreux autres exemples de « jeux » sur les caractères, et pas seulement contre des institutions financières ou bancaires.

À la date de rédaction de cet ouvrage, les premiers noms de domaines avec des caractères accentués font leur apparition (« IDN » ou « Internationalised Domain Names » pour noms de domaines internationalisés). L'accentuation de certaines lettres de la langue française alliée à l'imagination débordante des personnes malveillantes incite donc à la méfiance.

Exemple d'un faux message bancaire :

Recommandations

Pour l'utilisateur

1) Connaître les habitudes "Internet" de ses partenaires financiers (banque, assurances, …)

Il n'arrive quasiment jamais qu'une banque communique directement avec ses clients par e-mail pour leur demander d'aller se connecter sur un site pour mettre à jour ses coordonnées. Et il est encore bien plus rare que cette même banque, qui a délivré une carte de crédit par exemple, demande à ses clients de lui communiquer des informations secrètes qu'elle n'est pas censée avoir !

2) Ne jamais cliquer sur un hyperlien Web contenu dans un e-mail

Un hyperlien trouvé dans un e-mail est une facilité donnée à l'utilisateur pour aller sur une page Web sans avoir à en saisir l'adresse sur son navigateur, surtout si cette adresse est longue et compliquée.
En cas de doute sur la légitimité d'un e-mail ou sur le site cible proposé, il est préférable de ne rien faire, et de contacter sa banque par téléphone pour vérification !
De façon générale, pour aller sur des sites connus, autant les conserver dans sa liste de liens privilégiés au sein du navigateur Internet.

3) Se méfier quand on donne des renseignements confidentiels

Dans la mesure où il s'avère nécessaire de fournir des informations confidentielles, il est recommandé de vérifier que le site en question offre au moins un mode de raccordement sécurisé en HTTPS (avec un pictogramme de cadenas sur lequel on peut cliquer pour connaître quelle autorité a signé le certificat authentifiant le site),

Pour le décideur

4) Eduquer les utilisateurs

Les attaques en phishing reposant essentiellement sur la crédulité et le manque de recul des utilisateurs, un effort d'éducation sur la connaissance de la cybercriminalité et la manière de la contrer est la première des défenses.

De plus, les solutions de filtrage des accès Web proposent souvent une catégorie "Phishing" composée de sites reconnus comme étant des sites servant au phishing. Il faut bien sûr interdire l'accès aux pages Web de cette catégorie.

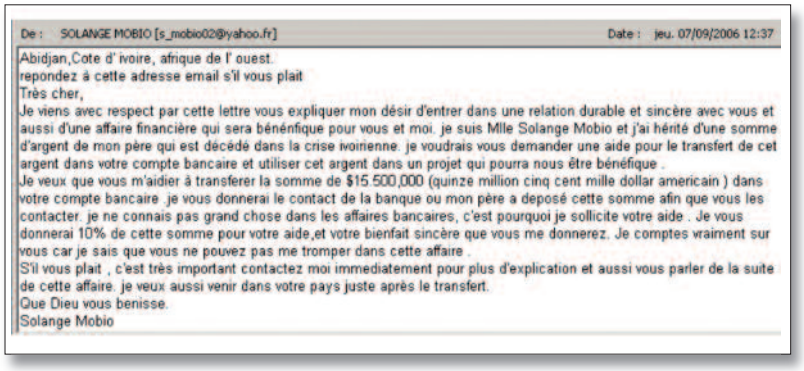
Les HOAX, ou contenus malveillants

Certains e-mails véhiculent des contenus qui jouent sur la naïveté, l'ignorance ou la peur du destinataire pour l'inciter à se situer dans un contexte de crise ou pour lui extorquer de l'argent. A titre d'exemple on peut citer, le "hoax" et la fraude nigériane.
Ces e-mails malveillants, appelés HOAX ou canulars, cherchent soit à saturer Internet (principe des chaînes), soit à porter directement préjudice (incitation de l'e-mail à supprimer un fichier système indispensable en faisant croire que c'est un virus).

Le HOAX, déclinaison moderne des lettres chaînées, est un phénomène né pratiquement avec la messagerie électronique. Il en tourne plusieurs milliers en permanence sur l'Internet, et ils parviennent à leurs destinataires au hasard des listes de distribution.

La fraude nigériane, censée donner une commission sur des transferts de fonds … suspects, cherche à obtenir des renseignements sur le compte bancaire de sa victime. Elle est l'œuvre de mafias, très organisées et expertes dans l'art d'agir sur les comptes en banque !

Exemple de « fraude nigériane » :



De : SOLANGE MOBIO [s_mobio02@yahoo.fr] Date : jeu. 07/09/2006 12:37

Abidjan,Cote d' ivoire, afrique de l' ouest.
repondez à cette adresse email s'il vous plait
Très cher,
Je viens avec respect par cette lettre vous expliquer mon désir d'entrer dans une relation durable et sincère avec vous et aussi d'une affaire financière qui sera bénénfique pour vous et moi. je suis Mlle Solange Mobio et j'ai hérité d'une somme d'argent de mon père qui est décédé dans la crise ivoirienne. je voudrais vous demander une aide pour le transfert de cet argent dans votre compte bancaire et utiliser cet argent dans un projet qui pourra nous être bénéfique .
Je veux que vous m'aidier à transferer la somme de $15.500,000 (quinze million cinq cent mille dollar americain) dans votre compte bancaire .je vous donnerai le contact de la banque ou mon père a deposé cette somme afin que vous les contacter. je ne connais pas grand chose dans les affaires bancaires, c'est pourquoi je sollicite votre aide . Je vous donnerai 10% de cette somme pour votre aide,et votre bienfait sincère que vous me donnerez. Je comptes vraiment sur vous car je sais que vous ne pouvez pas me tromper dans cette affaire .
S'il vous plait , c'est très important contactez moi immediatement pour plus d'explication et aussi vous parler de la suite de cette affaire. je veux aussi venir dans votre pays juste après le transfert.
Que Dieu vous benisse.
Solange Mobio

Recommandations

Pour l'utilisateur :

1) Vivre avec les contenus malveillants

Le meilleur conseil est surtout de ne pas devenir complice d'un HOAX en le transmettant à d'autres destinataires. Il ne faut évidemment pas répondre aux sollicitations des hoax et de la fraude nigériane. Avec un peu d'habitude, il devient facile de détecter l'arnaque et de ne pas tomber dans le piège.

2) Signaler hoax et fraude nigériane auxquels vous êtes confrontés

Il existe des sites Internet sur lesquels on peut signaler ce type d'e-mails malveillants, par exemple www.hoaxbuster.com pour les HOAX, ou même quelques sites étatiques.

Pour le décideur

3) Sensibiliser les salariés

La messagerie électronique est un outil mis à disposition du salarié uniquement à des fins professionnelles. Un message provenant d'une source inconnue, dont la teneur sort de l'ordinaire, n'a pas à être traité. Le chef d'entreprise est par ailleurs responsable des actions de ses employés durant leurs heures de travail, avec les outils qu'il leur a fournis, conformément à la politique de sécurité que l'entreprise doit avoir publiée.

Interdiction de participer à la transmission d'un HOAX durant les heures de travail, éducation aux dangers du piège d'une fraude nigériane sont des éléments pouvant être portés dans la charte de sécurité de l'entreprise.

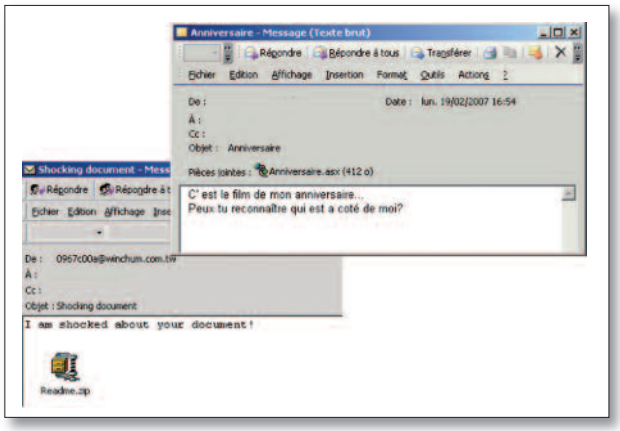
Les VIRUS véhiculés par les pièces jointes malveillantes

Un e-mail accompagné d'un ou de plusieurs fichiers attachés présente une probabilité non négligeable que ces fichiers soient infectés. Cela est particulièrement le cas avec des fichiers exécutables '.exe', de fichiers de liaison '.pif', Mais cela est parfois aussi vrai avec des fichiers bureautiques en ".doc", ".xls", ou même en ".zip".

Un virus est un code qui s'installe sur un poste de travail, après ouverture d'un fichier joint contaminé, et exécute sa « charge utile », pour détruire certaines catégories de fichiers du disque ou espionner l'utilisation de l'ordinateur à des fins de recueil d'informations secrètes.

On compte 60.000 souches de virus référencées et il s'en crée chaque mois entre 300 et 500. Jadis un anti-virus les identifiait assez facilement par leur signature spécifique et les éradiquait. Aujourd'hui les virus mutent, changent de signature, changent d'emplacement disque et se jouent des antivirus et parfois même les empêchent de fonctionner. Un poste de travail connecté à l'Internet sans protection est visité, voire contaminé, dans l'heure par l'extérieur.

Exemple d'e-mails véhiculant sans doute un virus



Recommandations

Pour l'utilisateur

1) Protéger le poste de travail par un antivirus à jour

La meilleure contre-mesure à opposer à un virus est de disposer sur son poste de travail d'un bon logiciel anti-virus tournant en tâche de fond avec sa base de signature fréquemment mise à jour. Cette mise à jour ne peut être réalisée que dans la mesure où un contrat a été souscrit auprès de l'éditeur du logiciel anti-virus ! Il s'agit donc d'une action qui doit être

menée en amont, puis renouvelée régulièrement.
En amont, une infrastructure de réception des e-mails peut être constituée avec d'autres logiciels anti-virus couplés aux serveurs de messageries comme mentionné ci-après.

2) Prendre garde aux pièces jointes attachées aux e-mails
Si on ne connaît pas l'émetteur ou la provenance d'un e-mail, il est particulièrement déconseillé d'exécuter un fichier qui lui est attaché, compte tenu du très fort risque de contamination. De même, avant d'envoyer un fichier en attachement à un e-mail, contrôlez le par votre anti-virus. Il est ainsi recommandé de privilégier un envoi de fichiers dans un format "passif", par exemple au format Acrobat PDF, plutôt que dans un format potentiellement "actif" car pouvant contenir des codes actifs, comme par exemple avec les logiciels de la suite bureautique Office (Word, Excel …) pouvant contenir des macro qui s'exécutent lors de l'ouverture du fichier.

Pour le décideur
3) Protéger l'entreprise
Un antivirus mutualisé sur le serveur de messagerie de l'entreprise est capital pour le contrôle systématique des messages entrants et sortants. De plus, il ne sera efficace que si sa base de signature est le plus à jour possible.

Il semble indispensable de mettre en place une solution de filtrage et d'éradication des codes malicieux dès l'entrée sur le réseau de l'entreprise, mais il l'est tout autant en sortie du réseau de l'entreprise, car la contamination des clients, partenaires et prospects rend le chef d'entreprise civilement responsable des dommages commis à l'extérieur par les e-mails de ses employés.

Le concept de BOTNET et de prise de contrôle à distance des machines…

Le BOTNET est un réseau de machines infectées par un type de virus particulier (le BOT) permettant d'en prendre le contrôle à distance, à l'insu de son propriétaire. Bien que semblant fonctionner normalement, le poste de travail est prêt à exécuter les ordres envoyés par un serveur maître, situé quelque part sur l'Internet, le plus souvent dans un pays étranger à législation généralement différente, voire inexistante. Ce serveur de commande, en général aux mains de mafias, en monnaye l'utilisation, par le biais de location ou d'un « service clé en main » par exemple pour bloquer un site marchand en réalisant une attaque massive en déni de service.

À ce jour, les plus grands réseaux de BOTNET répertoriés par les éditeurs de logiciels anti-virus comptent plusieurs centaines de milliers de postes compromis et potentiellement actifs

Cette contamination peut avoir deux sources potentielles :
- le téléchargement de fichiers (exécutables, utilitaires, jeux, musique, films,…) à partir de sites ou de réseaux peu fiables : sites de téléchargements « gratuits », réseaux de Peer-To-Peer ;
- exécution d'une pièce jointe attachée à un e-mail.

Recommandations

Pour l'utilisateur :
1) Vérifier fréquemment la configuration de votre machine
Les anti-virus ont une certaine efficacité pour détecter et éradiquer ces BOTS, petits logiciels qui infectent les PC. Il existe également des utilitaires (payants ou en mode freeware) qui analysent en détail la configuration de la machine et proposent de la nettoyer. Ne pas hésiter à y avoir recours souvent, en prenant garde, lors de la phase de nettoyage.

2) Écouter les plaintes contre des agissements dont vous n'êtes pas au courant
Si vous êtes l'objet de plaintes (pour envoi de SPAM vers une messagerie dont vous n'avez jamais entendu parler, pour une attaque en déni de service,…), ces accusations sont peut-être réellement fondées du fait de la contamination de votre machine. Procédez à une vérification, et à son éventuel nettoyage.

Pour le décideur :
3) Dans le cadre de l'entreprise, portez plainte si vos machines sont compromises
En France, une agression sur un système d'information constitue un délit, et est puni par la loi. Si vous pensez que votre réseau et ses postes de travail ont été agressés ou contaminés, vous pouvez notamment porter plainte auprès des autorités et organismes compétents tels que la BEFTI à Paris, et l'OCLCTIC. Le possesseur du serveur maître pourra alors être inquiété par la justice, surtout s'il réside dans un pays où la loi est répressive concernant les agressions sur les systèmes d'information.