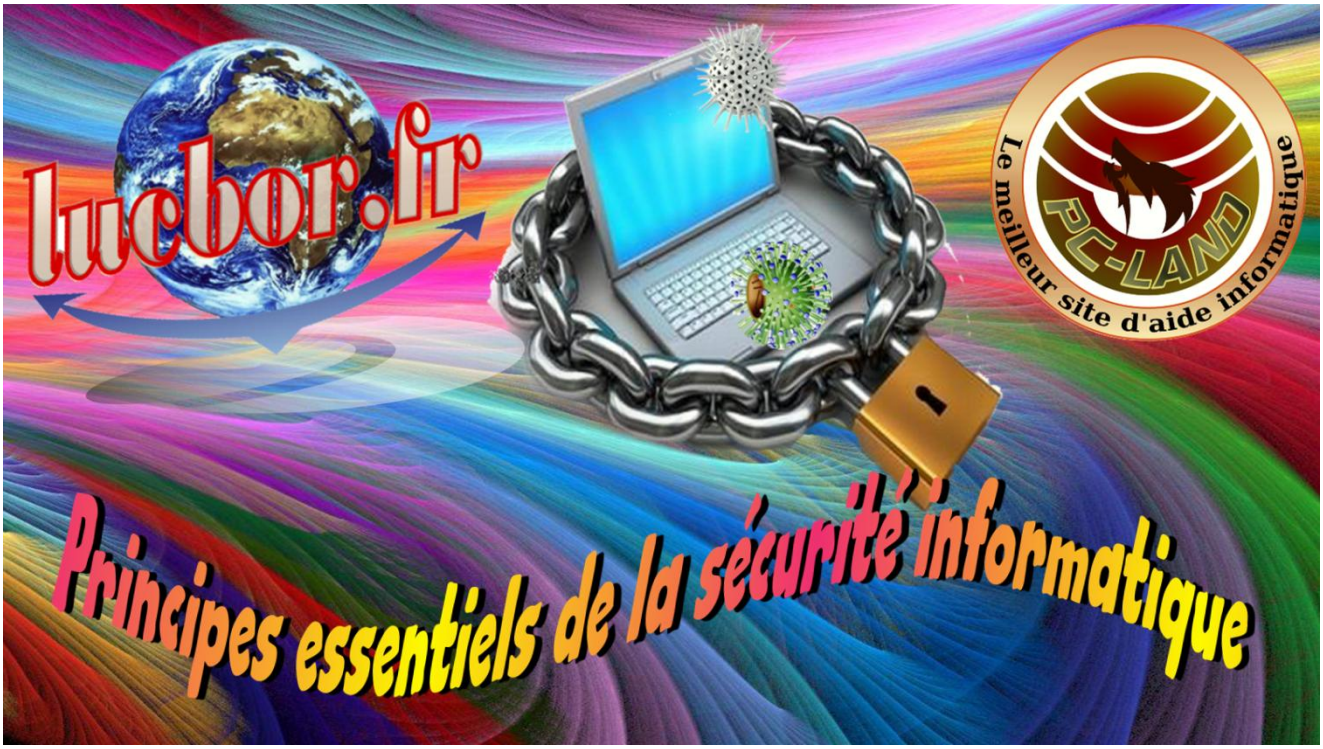


La sécurité d'un système d'information peut être comparée à une chaîne de maillons plus ou moins résistants. Elle est alors caractérisée par le niveau de sécurité du maillon le plus faible. Ainsi, la sécurité du système informatique doit être abordée dans un contexte global :

- la sensibilisation des utilisateurs aux problématiques de sécurité.
- la sécurité de l'information.
- la sécurité des données, liée aux questions d'interopérabilité, et aux besoins de cohérence des données en univers réparti.
- la sécurité des réseaux.
- la sécurité des systèmes d'exploitation.
- la sécurité des télécommunications.

Choisir un bon mot de passe

Dans un système d'information, un mot de passe est souvent l'élément dont l'efficacité repose le plus sur l'utilisateur. Il est donc très important de savoir choisir plusieurs mots de passe dits forts, c'est-à-dire difficiles à déchiffrer. La force d'un mot de passe dépend de sa longueur et du nombre de possibilités existantes pour chaque caractère le composant.

Ainsi, un mot de passe composé de caractères minuscules, majuscules, chiffres et caractères spéciaux sera de meilleure qualité qu'un mot de passe composé uniquement de minuscules. Difficile à retrouver à l'aide d'outils automatisés, et difficile à deviner par une tierce personne. Un mot de passe long et ne comportant pas de mots du dictionnaire peut être difficile à retenir, et sera souvent inscrit sur un bout de papier à côté du poste, ce qui pourrait compromettre la sécurité de celui-ci dans un environnement partagé. Il faut donc trouver des moyens mnémotechniques pour fabriquer et retenir facilement de tels mots de passe.

Méthodes d'attaques sur les mots de passe :

La plupart du temps, seule une empreinte du mot de passe est stockée sur l'ordinateur. Celle-ci résulte d'une fonction de hachage, qui est à sens unique (c'est-à-dire, qu'on ne peut pas retrouver le mot de passe à partir de son empreinte unique).

Une attaque sur un mot de passe peut soit se faire sur son empreinte, soit sur l'authentification elle-même.

Dans le premier cas, l'attaquant va appliquer la fonction de hachage sur différents mots et les comparer avec l'empreinte dérobée, jusqu'à trouver une équivalence.

Dans le deuxième cas, il va directement essayer les mots dans le programme jusqu'à obtenir une authentification réussie. Dans le cas où le nombre de tentatives est limité, cette deuxième attaque devient quasi-impossible.

Le choix des mots que le programme d'attaque essaye définit le type d'attaque : force brute, dictionnaire, compromis temps / mémoire...

Attaque par force brute :

Une attaque par force brute tente d'utiliser tous les mots de passe possibles. Plus il y a de caractères et plus leur espace de départ (types de caractères) est grand, plus cette attaque mettra de temps à aboutir. Un mot de passe long (au moins 10 caractères) et utilisant des types de caractères différents ne peut ainsi être trouvé en un temps raisonnable par un attaquant ayant des moyens conventionnels.

Attaque par dictionnaire :

L'attaque par dictionnaire consiste à utiliser des mots issus d'une liste, le but recherché étant de retrouver des mots de passe utilisant des mots communs (de différentes langues). Plusieurs techniques sont utilisées pour augmenter le nombre de combinaisons testées, notamment :

- ajout d'un ou plusieurs chiffres ("password01") ; changement des minuscules ou majuscules ("pAssword") ;
- remplacement des caractères par des chiffres ("pa55w0rd").

Le choix d'un mot de passe ne faisant aucune référence à un mot connu du dictionnaire rendra cette attaque inutile.

Ingénierie sociale :

Cette méthode consiste simplement à deviner le mot de passe, en fonction d'éléments que l'attaquant aura pu obtenir sur le propriétaire du mot de passe et de ses proches (nom, prénom, date de naissance...). Ceux-ci peuvent être ajoutés manuellement dans un dictionnaire, pour que le programme utilise diverses techniques citées précédemment pour optimiser des combinaisons

Faire les mises à jour de sécurité :

La plupart des attaques tentent d'utiliser les failles d'un ordinateur (failles du système d'exploitation ou des logiciels).

En général, les agresseurs recherchent les ordinateurs dont les logiciels n'ont pas été mis à jour afin d'utiliser la faille non corrigée et ainsi parviennent à s'y introduire. C'est pourquoi il est fondamental de mettre à jour tous ses logiciels afin de corriger ces failles.

Les logiciels, comme toute création humaine, comportent des défauts appelés bogues.

Parmi ces défauts, on trouve des défauts portant atteinte à la sécurité. C'est ce que l'on appelle des vulnérabilités. Les éditeurs de logiciels ayant découvert un défaut effectuent des campagnes de correction des problèmes ; il suffit de télécharger une "rustine" logicielle pour réparer le défaut de sécurité. Cela s'appelle une mise à jour de sécurité, ou un correctif de sécurité ou un patch de sécurité.

Si une vulnérabilité a été découverte sur un des logiciels que vous utilisez, une personne malintentionnée pourrait essayer d'en tirer profit pour essayer de prendre le contrôle de votre ordinateur, vous voler des

informations, provoquer le dysfonctionnement ou l'arrêt de votre machine, propager un ver, installer du contenu illicite, etc.

Il est donc primordial de toujours maintenir à jour vos logiciels en appliquant systématiquement toutes les mises à jour de sécurité au fur et à mesure qu'elles sont publiées.

Les logiciels modernes disposent de fonctions de mises à jour automatiques qui permettent de télécharger et d'installer les correctifs dès qu'ils sont disponibles.

Pour les logiciels qui ne disposent pas de fonctions de mises à jour automatiques, vous pouvez vous tenir informés en vous abonnant à des services d'alerte.

Ces services vous permettront non seulement d'être alerté en cas de sortie d'une mise à jour qui n'est pas distribuée automatiquement mais aussi d'être averti des solutions de contournement lorsqu'un correctif n'est pas encore disponible pour contrer une nouvelle menace, en attendant la publication d'un correctif (attaques dites du jour zéro).

Effectuer des sauvegardes régulières

Un des premiers principes de défense est de conserver une copie de ses données afin de pouvoir réagir à une attaque ou un dysfonctionnement. La sauvegarde de vos données est une condition de la continuité de votre activité.

Sauvegarder, c'est mettre en lieu sûr des informations pour les récupérer en cas de besoin.

Le meilleur moyen de ne pas perdre ses données est d'avoir toujours au moins une copie en lieu sûr, appelée sauvegarde. Il est primordial d'effectuer régulièrement des sauvegardes. La fréquence des sauvegardes dépend de la quantité de données que vous acceptez de perdre en cas de destruction de vos données.

En plus des données, vous pouvez sauvegarder votre système et vos logiciels, mais en général, ils sont fournis avec des moyens de réinstallation qui rendent cette sauvegarde moins importante que celle des données.

Pour effectuer une sauvegarde, vous pouvez utiliser soit un outil spécialisé soit faire de la simple copie de fichiers.

Il est recommandé, une fois la sauvegarde effectuée, d'entreposer les supports loin de l'ordinateur qui contient les données. Cette précaution évite que la destruction des données d'origine ne puisse s'accompagner de la destruction de leur copie de sauvegarde (ce qui pourrait arriver en cas d'incendie ou d'inondation).

Le support externe utilisé pour stocker la sauvegarde peut être un CD, un DVD enregistrables, un disque dur externe, une bande magnétique (DAT, DLT)... en fonction de l'équipement que vous possédez (interface USB, graveur, lecteur de bande) et de la quantité de données que vous avez à sauvegarder.

Attention

Bien trop souvent, la sauvegarde n'est pas réalisée sur les données importantes et il est trop tard une fois qu'elles sont perdues pour faire quoi que soit. Faites donc vos sauvegardes régulièrement, par exemple en vous mettant un rappel dans votre calendrier ou en programmant une tâche automatisée. N'oubliez pas non plus que si vous avez chiffré des données, il faut sauvegarder les clés qui permettront de déchiffrer les données, sinon vos données seront illisibles en cas de perte de la clé.

Écrire sur un morceau de papier une information importante permettra certes de s'en souvenir mais il ne faut pas perdre le papier ! Ainsi sauvegarder c'est bien, mais l'important c'est de pouvoir récupérer les données (les restaurer). Il est donc nécessaire de s'entraîner à la restauration des données ou des systèmes

afin de s'assurer que tout fonctionne, et aussi permettre de limiter le stress le jour où la restauration sera nécessaire.

Bien configurer son navigateur :

Ce qui est vrai pour un système d'exploitation, l'est également pour les logiciels qui y sont installés. Avant toute utilisation d'un navigateur, quel qu'il soit, il convient de s'assurer le plus tôt possible que celui-ci est à jour Les navigateurs les plus récents proposent tous une fonctionnalité de mise jour automatique.

Tous les navigateurs récents proposent le support de langages exécutables par votre navigateur afin d'enrichir le contenu des pages affichées par le navigateur. Cependant, toutes ces technologies peuvent être des moyens pour des personnes malveillantes de faire exécuter sur votre machine et à votre insu des codes malveillants.

Les ActiveX

Les ActiveX ou plus précisément les contrôles ActiveX sont une technologie propre à Internet Explorer. Ils permettent l'exécution de programmes sur votre machine par l'intermédiaire de votre navigateur. Un contrôle ActiveX malveillant que vous auriez accepté d'installer sur votre machine a potentiellement accès à tout ou partie de votre ordinateur. Il est recommandé de les désactiver par défaut dans Internet Explorer et d'en limiter l'utilisation aux sites de confiance.

Les Applets Java

Les appliquettes (applet) sont relativement rares et leur support peut être désactivé par défaut. Si toutefois, il vous est indispensable d'activer le support de ces composants, il conviendra de s'assurer que la machine java de votre ordinateur est bien mise à jour.

Pourquoi ? Les appliquettes sont des programmes téléchargés et exécutés dans le contexte de votre navigateur. Ils ont la particularité de ne pas être exécutables en tant que tel. Ils nécessitent la présence d'une machine virtuelle Java sur votre système pour fonctionner correctement. Internet Explorer utilise par défaut la machine virtuelle livrée avec Windows. Les autres navigateurs, quant à eux, requièrent l'installation d'une machine virtuelle tierce.

Les scripts JavaScript

Bien que cela soit de plus en plus délicat, il convient de désactiver autant que faire se peut les scripts JavaScript dans votre navigateur et ne les activer que sur des sites de confiances et lorsque cela est réellement nécessaire.

Pourquoi ? Le JavaScript est un langage très utilisé permettant l'intégration de programmes directement dans les pages des sites. Il est présent dans de nombreuses pages et sites internet. On peut le trouver également dans certaines interfaces d'administration d'imprimantes ou d'équipements en réseau. Il peut être le vecteur de certaines attaques visant à utiliser des fonctionnalités de votre navigateur à votre insu ou à récupérer des informations sur votre ordinateur.

Gérer les extensions de navigateur :

Une bonne pratique consiste à n'installer que des extensions dont vous avez besoin et dont l'origine est de confiance.

Il existe des extensions disponibles pour les navigateurs permettant le support de nouvelles fonctionnalités ou de nouvelles technologies. Il conviendra à chaque ajout de prendre en compte le fait que celui-ci peut être à l'origine d'une nouvelle vulnérabilité sur votre ordinateur. Il est donc nécessaire de ne les installer qu'au cas par cas.

Naviguer prudemment sur l'internet :

Une fois votre navigateur et votre machine correctement configurés et à jour, il convient encore de prendre quelques précautions d'usage lorsque vous naviguez sur des sites internet.

Ne donnez pas d'informations personnelles et confidentielles (vos coordonnées personnelles, vos coordonnées bancaires, etc) sur un site marchand ou un site bancaire, sans avoir vérifié au préalable que le site est sécurisé par l'emploi d'un certificat électronique qui garantit que le site est authentique, et qui va servir à protéger la confidentialité des informations échangées. Pour cela, il y a deux informations affichées par le navigateur qui doivent être vérifiées :

- l'adresse URL du site doit commencer par "https://" et le nom du site doit correspondre à l'attente de l'utilisateur ;
- un petit cadenas fermé doit figurer à droite de l'adresse du site, ou en bas à droite de la barre d'état (selon la version et le type de votre navigateur) ; il symbolise une connexion sécurisée. En cliquant dessus, on peut afficher le certificat électronique du site, et visualiser le nom de l'organisme.
- il est toujours possible à un agresseur d'intervenir en amont (sur votre machine) ou en aval (sur le site consulté ou en vous aiguillant sur un site frauduleux au nom très voisin) afin d'obtenir des informations sensibles.
- Dans tous les cas, il est important de ne jamais donner d'informations personnelles sur des forums , blogs, sites communautaires (adresse physique, de messagerie...).
- Il est important de prendre en compte, lorsque l'on veut déposer un message sur ce genre de site, que le contenu de vos écrits pourra être analysé par des programmes appelés robots. Ceux-ci sont capables de récupérer facilement les adresses de messageries ou les identifiants de messageries instantanées présents dans le texte.
- Or ces informations pourront très bien être utilisées afin de propager du pourriel. Aujourd'hui, il n'est pas rare après avoir déposé son adresse personnelle de messagerie électronique sur un forum de se voir inondé de pourriels les heures ou jours suivants. De plus ces informations communiquées dans ces sites resteront publiques et non maîtrisables pour une très longue période.
- Lorsque que vous décidez de faire des achats sur internet, assurez-vous du caractère sérieux du site marchand et qu'il offre toutes les garanties de sécurité lorsque vous allez payer (chiffrement, possibilité de rétractation...).
- Il convient également d'être prudent sur la nature des données bancaires demandées lors d'un paiement en ligne. Un site ne doit jamais vous demander de saisir votre code secret associé à votre carte bancaire.
- L'utilisateur d'un ordinateur dispose de privilèges ou de droits sur celui-ci. Ces droits permettent ou non de conduire certaines actions et d'accéder à certains fichiers d'un ordinateur.
- On distingue généralement les droits dits d'administrateur et les droits dits de simple utilisateur. Dans la majorité des cas, les droits d'un simple utilisateur sont suffisants pour envoyer des messages ou surfer sur l'internet. En limitant les droits d'un utilisateur on limite aussi les risques d'infection ou de compromission de l'ordinateur.

Télécharger prudemment :

L'internet met à disposition des utilisateurs une grande source de données :

- documents bureautiques (fichiers Office, PDF, etc.), données multimédia (musique, vidéos, animations),
- des applications gratuites ou payantes.

Il existe plusieurs méthodes pour échanger toutes ces données :

- par messagerie (pièces jointes à des courriers électroniques),
- par des liens sur les sites internet ;
- par réseau pair-à-pair (P2P) ;
- par client/serveur FTP.

Avant le téléchargement, voici quelques questions à se poser :

- Ai-je le droit de télécharger ce genre de données ?
- Est-ce que je peux faire confiance à la source ?
- Est-ce que mon ordinateur contient des données professionnelles, et suis-je prêt à installer n'importe quoi dessus ?

Télécharger, c'est introduire un élément inconnu sur l'ordinateur. En installant une application, ou en ouvrant un document, le risque d'avoir sa machine compromise est possible.

Un cheval de Troie (trojan) peut être introduit dans l'ordinateur :

Il peut installer à l'insu de l'utilisateur :

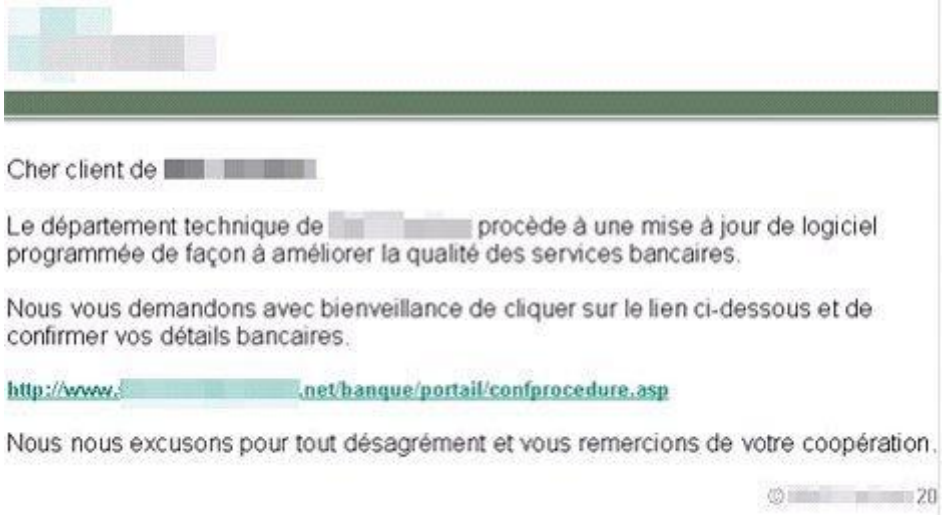
- des espiogiciels, ces logiciels ou modifications de logiciels qui espionnent les actions faites sur l'ordinateur (sites visités, applications utilisées, frappes tapées au clavier, documents ouverts, etc.),
- des "publiciels", ces logiciels ou modifications de logiciels qui font apparaître de façon pernicieuse de la publicité sur l'ordinateur, que ce soit au niveau des barres du navigateur internet, par des fenêtres surgissantes (popup), ou par des messages système,
- des outils qui transforment la machine en machine zombie : elle obéit à distance à d'autres personnes, qui l'utilisent ensuite pour lancer des attaques ou dérober des informations confidentielles, etc.

Se méfier du filoutage (phishing) :

Une des attaques classiques visant à tromper l'internaute pour lui voler des informations personnelles, consiste à l'inciter à cliquer sur un lien placé dans un message. Ce lien peut-être trompeur et malveillant. Plutôt que de cliquer sur celui-ci, il vaut mieux saisir soi-même l'adresse du site dans la barre d'adresse du navigateur. De nombreux problèmes seront ainsi évités.

Généralement la victime reçoit dans sa messagerie électronique un courriel, semblant provenir de sa banque ou d'un organisme de confiance, lui indiquant qu'un problème est survenu sur son compte. Le contenu du mail est vraisemblable, il utilise le logo de l'organisme bancaire et invite la victime à cliquer sur le lien contenu dans le courrier afin de résoudre ce soi-disant problème. Le lien affiché est d'ailleurs celui de la banque (quand le message est affiché au format HTML).

Exemple : Courriel de filoutage envoyé à des clients d'une banque


Cher client de

Le département technique de procède à une mise à jour de logiciel programmée de façon à améliorer la qualité des services bancaires.

Nous vous demandons avec bienveillance de cliquer sur le lien ci-dessous et de confirmer vos détails bancaires.

http://www. .net/banque/portail/confprocedure.asp

Nous nous excusons pour tout désagrément et vous remercions de votre coopération.

Le lien internet masqué, contenu dans le mail, conduit en fait à un site ressemblant à s'y méprendre au site de la banque ou de l'organisme de confiance. Cette imitation du site bancaire a été déposée par une personne malintentionnée sur un autre site internet compromis. Dès qu'une victime saisit des informations

personnelles (coordonnées bancaires, identifiants, mots de passe), celles-ci sont immédiatement envoyées à la personne malveillante qui s'empressera de les utiliser pour vider le compte bancaire de sa victime.
Remarque

Ces courriers frauduleux ne sont généralement pas ciblés mais envoyés à des milliers d'adresses.

Contrôler la diffusion d'informations personnelles :

L'internet n'est pas le lieu de l'anonymat et les informations que l'on y laisse échappent instantanément !

Dans ce contexte, une bonne pratique consiste à ne jamais laisser de données personnelles dans des forums, à ne jamais saisir de coordonnées personnelles et sensibles (comme des coordonnées bancaires) sur des sites qui n'offrent pas toutes les garanties requises. Dans le doute, mieux vaut s'abstenir...

Ne jamais relayer les canulars par messagerie (hoax):

Ne jamais relayer des messages de type chaînes de lettres, porte-bonheur ou pyramides financières, appel à solidarité, alertes virales, etc. Quel que soit l'expéditeur, rediffuser ces messages risque d'induire des confusions et de saturer les réseaux.

Ce type de canular peut être réalisé sur différents supports :

- la messagerie ;
- les forums de discussions.

En participant, ou en étant victime de ces canulars, vous vous exposez, ou vous exposez votre entreprise à certains risques :

- participation à votre insu à une attaque en déni de service ;
- recommandations de fausses mesures de sécurité pouvant causer des dégâts ;
- divulgation de l'organisation interne de votre entreprise, voire de la liste des personnes les plus crédules ;
- déni de service sur les outils de messagerie ;
- banalisation du risque sur la sécurité.

Pour inciter les lecteurs à faire suivre le message au maximum de personnes, celui ci joue généralement sur les sentiments du destinataire. Les leviers les plus couramment utilisés sont l'estime de soi, en faisant valoir au destinataire qu'il réalise une "bonne action" (aider un enfant malade, bloquer la prochaine épidémie de virus informatiques...), et l'argent, en lui faisant croire qu'il peut acquérir à bon compte certains objets intéressants (un téléphone portable, une image attrayante,...).

Pour convaincre de la véracité du message, il est souvent fait appel à divers éléments :

- des arguments d'autorités : le message prétend, par exemple, ne pas être un canular (ou hoax en anglais), ou que l'information a été vérifiée par une autorité reconnue (FBI, éditeur d'antivirus, hôpital, fournisseur d'accès à internet, le service informatique, Microsoft ou tout autre grand éditeur de logiciel, etc.) ;
- le message est présenté comme le témoignage direct d'une personne impliquée ;
- des éléments d'actualité sont cités : le destinataire sera d'autant plus incité à accorder sa confiance si il peut rattacher le message à un contexte d'évènements qu'il connaît ;
- le message provient d'une connaissance, elle-même victime de la rumeur : cette situation tend à faire baisser votre niveau de vigilance. "Puisque je reçois une invitation à propager un message de la part de quelqu'un que je connais, je suppose qu'il s'est assuré du bien fondé de la démarche et je me dispense de le faire".

Afin d'augmenter l'efficacité du message, le destinataire est souvent placé en situation d'urgence afin de limiter son analyse. Il est incité à prendre une décision rapide concernant l'envoi du message et a considéré qu'il vaut mieux diffuser une fausse nouvelle plutôt que de laisser arriver une catastrophe.

Danger de ce type de messages :

Le premier risque concerne la surcharge de vos réseaux et de vos serveurs de messagerie.

Il est également possible de déclencher systématiquement l'envoi d'un message à la réception du canular. Cette fonctionnalité peut être obtenue :

- automatiquement, par le biais d'une inclusion malicieuse dans le code source de la page lorsque le texte du message est exprimé en HTML ;
- manuellement en invitant le destinataire à ajouter une adresse particulière à la liste de diffusion (l'argumentaire du message vise à justifier pourquoi il est nécessaire d'ajouter ce destinataire).

Cet envoi peut avoir différentes utilités pour la personne à l'origine du canular :

- lorsque le destinataire de ce message est une victime, il est noyé sous un flot de messages. Dans ce cas, le fait de lire le message et de le faire suivre s'apparente à de la complicité dans une opération de déni de service sur un tiers
- lorsque le destinataire de ce message envoyé automatiquement est la personne malicieuse, elle obtient la liste de vos correspondants, ce qui lui permet d'imaginer la structure de votre entité et les réseaux de personnes à l'intérieur. De surcroît, elle reçoit la liste des personnes les plus crédules (celles qui font suivre les courriels). Cette information pourrait être exploitée ultérieurement pour obtenir, à moindre risque, des informations plus sensibles.

Il existe également une variante, demandant d'envoyer vos cartes de visite à un enfant gravement malade qui les collectionne et dont c'est la seule passion. Une personne malintentionnée dispose ainsi des informations lui permettant de prétendre vous connaître et avoir travaillé avec vous, voire de se faire passer pour vous. Elle est également en mesure d'en déduire l'organigramme de votre entité.

Parfois le message vous demande de réaliser des actions supposées être les seules pertinentes étant donné l'urgence. Cependant elles sont dangereuses. Par exemple, vous êtes invités à :

- débrancher l'ordinateur sans l'éteindre proprement pour éviter d'être contaminé par un virus ;
- effacer tous vos documents bureautiques probablement déjà contaminés.

Solution :

Il ne faut jamais chercher à savoir si de telles rumeurs, véhiculées par la messagerie, sont fondées ou non. C'est une fausse piste. La décision doit se prendre de façon objective sur ce que le message vous incite à faire.

Dès que vous recevez un message :

- avec beaucoup de destinataires ;
- dont le texte véhicule une forte charge émotive ;
- qui inspire un sentiment d'urgence ;
- qui vous invite à faire quelque chose que vous ne faites pas spontanément ;

Vous devez supposer que vous êtes en présence d'un canular.

Que la rumeur soit fondée ou non, la diffusion massive d'un message par tous les usagers de la messagerie, ne constitue jamais la bonne démarche.

Les virus informatiques :

Fléau majeur de l'informatique, les virus sont aussi présents sur internet. Qu'ils s'attaquent au secteur d'amorce de vos disques, aux fichiers exécutables ou aux documents incluant des macros, leur but est toujours le même : proliférer en cachette, se faire subitement remarquer, puis souvent détruire vos données. La meilleure protection reste la prévention : méfiez-vous des disquettes introduites dans des ordinateurs peu sûrs, et des fichiers douteux téléchargeables sur internet ou reçus en pièce jointe d'un courrier.

Les virus sont un fléau majeur de l'informatique, et pas seulement sur internet : un simple échange de disquettes entre copains ou collègues de travail peut contaminer votre disque dur, sans même éveiller vos soupçons. Car la bestiole est souvent rusée. Autopsie.

Qu'est-ce qu'un virus?

Un virus est un petit programme conçu pour se cacher dans votre ordinateur, puis se multiplier, se répandre de par le monde et enfin déclencher une action (message, destruction, petite musique, etc.). On dénombre plusieurs catégories de virus, en fonction de la cible visée dans l'ordinateur.

Les différentes familles de virus

La première catégorie regroupe les **virus de secteur d'amorce** (= virus de "boot sector", c'est-à-dire affectant la zone du disque qui est lue en premier au démarrage) tels que Form, jack the ripper, french boot, parity boot... Ces virus remplacent le secteur d'amorce du disque infecté par une copie d'eux-mêmes, puis déplacent le secteur original vers une autre portion du disque. Le virus est ainsi chargé en mémoire bien avant que l'utilisateur ou un logiciel ne prenne le contrôle de l'ordinateur.

Les **virus d'applications** infectent les fichiers exécutables, c'est-à-dire les programmes (.exe, .com ou .sys). Pour simplifier, disons que le virus remplace l'amorce du fichier, de manière à ce qu'il soit exécuté avant le programme infecté, puis il lui rend la main, camouflant ainsi son exécution aux yeux de l'utilisateur.

Les **virus macro** sont des virus qui infectent uniquement des documents (Word, Excel...), en utilisant le langage Visual Basic pour Application. Ces virus se propagent actuellement dans de fortes proportions et peuvent malheureusement causer de grands dégâts (formatage du disque dur par exemple).

Enfin, il y a les **virus de mail**, également appelés **vers**. Ces virus se servent des programmes de messagerie (notamment Microsoft Outlook) pour se répandre à grande vitesse, en s'envoyant automatiquement à tout ou partie des personnes présentes dans le carnet d'adresses. Leur premier effet est de saturer les serveurs de messagerie, mais ils peuvent également avoir des actions destructrives pour les ordinateurs contaminés. Ils sont particulièrement redoutables, car le fait de recevoir un mail d'une personne connue diminue la méfiance du destinataire, qui ouvre alors plus facilement le fichier joint contaminé.

A noter que certains virus sont des virus polymorphes. A chaque fois que l'un d'eux infecte un fichier, il se crypte différemment. Résultat, il faut que l'antivirus analyse la technique d'encryptage de chaque virus pour déceler, dans les fichiers contaminés, une sorte de "manie" caractéristique, une constante.

Il ne faut pas confondre les virus avec les troyens ou les emails bombs. Contrairement à son cousin le virus, qui profite de toute occasion pour se multiplier, le troyen véritable ne se reproduit pas (pour plus d'informations, consultez le dossier Secuser.com sur les troyens). Par ailleurs, plusieurs vulnérabilités dans les logiciels Internet Explorer / Outlook font que certains virus peuvent infecter votre ordinateur à la simple ouverture du message ou lors de sa lecture dans la fenêtre de visualisation voire en consultant une page web si Internet Explorer n'a pas été patché contre cette vulnérabilité.

Fonctionnement d'un virus

Quel que soit le type de virus, aucun ne contamine - pour l'instant - les fichiers compressés. Cela ne garantit pas qu'un fichier compressé soit exempt de virus : il peut très bien avoir été infecté avant compression, et se révélera donc dangereux une fois décompressé.

Pour bien comprendre le mode de fonctionnement d'un virus, il faut se souvenir de l'analogie avec le virus biologique. Comme lui, le virus informatique essaie de contaminer tout ce qu'il peut, de se dissimuler aux yeux de l'organisme infecté, et de se répandre le plus largement possible. Les virus infectent un maximum de fichiers puisqu'ils demeurent en mémoire dès le démarrage de l'ordinateur. Ils interceptent les commandes du Bios, et agissent ainsi selon leur humeur...

Règles générales de protection

La prévention paie toujours. Quelques règles simples peuvent être appliquées :

- ne téléchargez pas des programmes d'origine douteuse, qui peuvent vous être proposés sur des sites persos ou des chats eux-mêmes plus ou moins douteux;
- méfiez-vous des fichiers joints aux messages que vous recevez : analysez avec un antivirus à jour tout fichier avant de l'ouvrir, et préférez détruire un mail douteux plutôt que d'infecter votre machine, même si l'expéditeur est connu;
- fuyez les disquettes d'origine douteuse (ou ayant transité dans des lieux publics vulnérables comme les salles de cours ou TP des écoles ou universités), et protégez les vôtres en écriture;
- créez dès maintenant, si ce n'est pas déjà fait, une disquette de boot saine contenant un antivirus (la plupart des antivirus le proposent) pour une désinfection d'urgence;
- procédez régulièrement à des sauvegardes du contenu important de votre disque dur après avoir vérifié l'absence de virus : cela peut paraître fastidieux, mais en cas d'infection (ou même simplement en cas de crash de disque dur), ça vous sauvera la mise...
- tenez-vous au courant des apparitions de nouveaux virus. Secuser.com vous offre ce service en émettant des alertes lorsqu'un virus connaît une diffusion importante. Les informations (nom du virus, mode de transmission connu, etc.) sont alors consultables en ligne dans sur le site, ou par abonnement gratuit à la lettre hebdomadaire Secuser News, ou encore en temps réel via la liste Secuser Alerte. Connaître l'existence du virus, c'est déjà le tuer à moitié...

En complément de ces règles de prévention, la meilleure protection - et le principal remède en cas de contamination - consiste à installer un antivirus (certains sont gratuits, voir les liens utiles en fin d'article). Une solution qui reste toute relative, car aucun produit ne détecte 100% des virus, 100% du temps : d'où l'importance de la prévention. Par ailleurs, de nouveaux virus apparaissant chaque jour, il faut veiller à régulièrement actualiser la base de données virales du logiciel : la plupart des éditeurs proposent une mise à jour au minimum mensuelle, mais pas toujours gratuite...

Comment savoir si mon ordinateur est contaminé ?

Tout comme les troyens, les virus sont le plus souvent repérés trop tard, par les conséquences potentiellement désastreuses de leur activité : affichage de messages intempestifs, émission de sons ou de musiques inattendus, mais aussi plantage de l'ordinateur, formatage du disque dur, etc.

Pourtant, de nombreux indices peuvent mettre la puce à l'oreille de l'internaute vigilant : mémoire système disponible inférieure à ce qu'elle devrait être, changement du nom de volume d'un disque, programmes ou fichiers subitement absents, apparition de programmes ou de fichiers inconnus, ou encore comportement anormal de certains programmes ou fichiers.

Que faire en cas de contamination ?

La solution la plus simple reste de vous procurer un logiciel antivirus. La plupart propose une procédure permettant de désinfecter le contenu du disque avant d'installer le logiciel, mais le mieux est d'installer

l'antivirus avant toute contamination afin de bénéficier de l'ensemble de ses fonctionnalités (surveillance des transferts de fichiers ou de l'accès aux fichiers sensibles, inoculation des fichiers pour repérer tout changement de taille suspect, etc.).

Vous pouvez également utiliser un antivirus gratuit en ligne pour procéder immédiatement à l'analyse ainsi qu'à l'éradication de virus éventuellement présents sur vos disques.

En cas de doute ou d'infection avérée, demander de l'aide sur un forum d'aide informatique comme *PC-Land*

http://pcland.easyforum.fr/

La sécurité de transmission :

Le Wifi

Le Wifi est une technologie permettant de créer des réseaux informatiques sans fil (Wireless). Il s'agit d'une norme de l'IEEE baptisée 802.11.

Sa portée varie d'un appareil à l'autre entre quelques dizaines de mètres à plusieurs centaines de mètres, ce qui en fait une technologie de premier choix pour le réseau domestique avec connexion internet.

Il est de plus en plus utilisé par divers matériels informatiques, ordinateurs, organiseurs (PDA), consoles de jeux portables voire des imprimantes utilisent elles aussi le Wifi pour simplifier leur connexion.

Sécurité

Voici le point le plus important, souvent négligé et cause de problème. Il est facile de monter un réseau, mais il ne faut pas oublier de fermer la porte, que vous soyez ou non dans votre appartement.

Diverses possibilités : WEP, WPA, MAC, etc.

Le SSID ou "nom du réseau" identifie le réseau, donne un nom pour le différencier des autres. Si vous ne le diffusez pas, vous serez le seul à le connaître et c'est tout de suite plus difficile de se connecter à votre réseau.

Le WEP/WPA, ce sont deux possibilités d'encrypter les données qui circulent sur le réseau. Le problème du WIFI est que vous n'avez aucun contrôle de médium sur lequel circulent les données contrairement aux réseaux filaires. Donc vous ne savez pas qui est à l'écoute. Encrypter les données permet d'en assurer la confidentialité. Cela se fait à l'aide de ce que l'on appelle une clef. Cette clef permet également de sécuriser l'accès au réseau car, si on ne la connait pas, impossible de communiquer, donc incapable de lire les trames et/ou d'en envoyer au bon format.

Eviter les valeurs par défaut

Lors de la première installation d'un point d'accès, celui-ci est configuré avec des valeurs par défaut, y compris en ce qui concerne le mot de passe de l'administrateur. Un grand nombre d'administrateurs en herbe considèrent qu'à partir du moment où le réseau fonctionne il est inutile de modifier la configuration du point d'accès. Toutefois les paramètres par défaut sont tels que la sécurité est minimale. Il est donc impératif de se connecter à l'interface d'administration (généralement via une interface web sur un port spécifique de la borne d'accès) notamment pour définir un mot de passe d'administration.

D'autre part, afin de se connecter à un point d'accès il est indispensable de connaître l'identifiant du réseau (*SSID*). Ainsi il est vivement conseillé de modifier le nom du réseau par défaut et de désactiver la diffusion (*broadcast*) de ce dernier sur le réseau. Le changement de l'identifiant réseau par défaut est d'autant plus

important qu'il peut donner aux pirates des éléments d'information sur la marque ou le modèle du point d'accès utilisé.

Le bluetooth :

Dans les années à venir, le système Bluetooth équipera de plus en plus de périphériques de communication, augmentant par là-même l'ergonomie des équipements, mais facilitant en contrepartie l'accès des attaquants à une masse toujours croissante de données personnelles.

S'il peut s'avérer difficile, voire aléatoire de contrôler les agissements de certaines personnes malhonnêtes, il n'en reste pas moins qu'il est tout à fait possible et même fortement conseillé, d'assurer soi-même, et ce très simplement, la sécurité de son matériel. (Entre autres, ne pas divulguer ses mots de passe, ne coupler son périphérique qu'avec des appareils connus, le placer en mode non détectable, utiliser les patchs de mise à jour du système d'exploitation de l'équipement, etc.).

Voir le dossier pdf sur le lien suivant :
http://www.cases.public.lu/fr/publications/dossiers/bluetooth/bluetooth-insecurite.pdf

Sources utilisées :

http://www.securite-informatique.gouv.fr/

http://www.secuser.com/

http://www.hoaxbuster.com/

http://www.cases.public.lu/fr/publications/outils/index.html

http://pcland.easyforum.fr/