Extrait du OSI

http://www.osi-ngo.org/centre-de-ressources/services/guichets/service-informatique/points-de-securite-a-respecter-en-tant-que-membre-osi/article/securite-en-ligne

Sécurité en ligne

- Centre de Ressources - Services - Guichets - Service Informatique - Points de Sécurité à Respecter en tant que Membre OSI -

Date de mise en ligne : vendredi 22 janvier 2010

Description :

E-finance, Email, usurpation d'identité... prévenez au lieu de devoir guérir... ou de ne pas y arriver quand le mal est fait !

Comment bien gérer ses mots de passe

La gestion des mots de passe est une affaire délicate. Celui qui ne gère pas attentivement ses mots de passe risque d'être la victime d'escrocs informatiques. Heureusement, il existe quelques règles simples qui sécurisent les mots de passe et leur emploi.

Règle n° 1 : utilisez des mots de passe appropriés

En matière de qualité, il y a de grandes différences. Les mots complets ou les noms, par exemple, dans une langue quelconque offrent une protection insuffisante. Il faudrait donc éviter d'inclure des passages de votre nom d'utilisateur dans votre mot de passe. Un mot de passe uniquement constitué de chiffres est également tabou. Il vaut mieux opter pour une combinaison arbitraire de majuscules et de minuscules ainsi que de chiffres et de caractères spéciaux. Finalement, un mot de passe devrait compter au moins six caractères. Sur Internet, vous trouvez une multitude de générateurs qui peuvent vous aider à trouver le bon mot de passe.

Règle n° 2 : conservez les mots de passe en sécurité

Les mots de passe complexes décrits précédemment sont malheureusement difficiles à mémoriser. Il est cependant déconseillé de les noter. Il faut les conserver à un endroit sûr. De plus, il faut absolument éviter de sauvegarder ces mots de passe et autres éléments de sécurité sur l'ordinateur. Lorsque le navigateur demande s'il faut enregistrer le mot de passe et le nom de l'utilisateur, vous devriez refuser.

Règle n° 3 : utilisez différents mots de passe

Même si cela implique un surcroît de dépenses, vous devriez disposer de différents mots de passe. Si jamais un des mots de passe tombe entre de mauvaises mains, les dégâts restent minimes. En outre, les mots de passe devraient être renouvelés à des intervalles réguliers. Celui qui se perd dans cette multitude de mots de passe devrait les noter et les conserver dans un endroit sûr.

Règle n° 4 : ne dévoilez jamais vos mots de passe

Les mots de passe ne doivent jamais être mentionnés, ni dans un e-mail, ni par fax ni au téléphone. Si vous deviez recevoir une demande d'indiquer votre mot de passe, il s'agit probablement d'une tentative de piratage. Ne répondez donc jamais à ces demandes.

Règle n° 5 : tapez votre mot de passe uniquement si la connexion est cryptée

Si vous travaillez avec des données confidentielles sur Internet, veillez à ce que le flux d'informations soit crypté. Cela empêche en général les pirates informatiques de lire ces données et de les utiliser à leurs fins. On reconnaît une connexion cryptée grâce à l'indication https:// devant l'adresse Internet au lieu de http://. Dans ce cas, le « s » signifie « secure ». En outre, dans le cas d'une connexion sécurisée, un petit cadenas apparaît en bas de la fenêtre.

Règle n° 6 : ne laissez jamais votre ordinateur entre les mains d'autrui

Un autre risque est le fait de laisser votre ordinateur sans surveillance, sans prendre de mesures de sécurité, lorsque ce dernier est accessible à d'autres personnes. Dans ce cas, vous devez fermer votre ordinateur, même pour de courtes absences, sinon toutes les mesures de sécurité électroniques ne servent à rien.

Alex Hämmerli (Swisscontent Corp, trad. m.r) / 05.09.2008

Surfer sur Internet sans surprise coûteuse

Celui qui surfe sur Internet doit se protéger contre divers dangers. Un navigateur actualisé et sûr constitue un équipement de base pour surfer sur Internet.

Internet recèle de nombreux dangers. Les pirates informatiques parviennent toujours plus facilement à provoquer des dégâts considérables auprès d'Etats, d'entreprises et de personnes privées. Jusqu'à présent, les cybercriminels sévissaient surtout sur les pages pornographiques et de téléchargement illégal. Ils se servaient d'offres louches afin de télécharger des logiciels dangereux sur l'ordinateur du visiteur. Selon les experts en sécurité, un PC peut aussi attraper des virus sur des sites Web sûrs. Ainsi, on a par exemple découvert une bannière publicitaire Flash qui, par une simple visite sur le site blick.ch, provoquait l'installation de chevaux de Troie sur l'ordinateur de l'utilisateur et causait ainsi des dégâts considérables.

Plus c'est actuel, mieux c'est

Le programme, c'est-à-dire le navigateur Internet qui indique les sites Web, constitue souvent une porte d'entrée pour ces malwares, surtout si vous surfez sur Internet avec des vieux navigateurs. C'est pourquoi un navigateur devrait toujours être actualisé. A cet effet, il faut activer les fonctions d'actualisation automatique. Du point de vue de la sécurité se profilent actuellement les programmes gratuits « Internet Explorer » (minimum version 6.0 avec Service Pack 1) de Microsoft ou le programme concurrentiel « Firefoy » de Mozilla (minimum version 1.5). Pour les utilisateurs de Mac, les navigateurs « Safari » à partir de la version 1.3 ou « Firefox » à partir de la version 1.5 sont relativement sûrs. Les spécialistes se disputent toutefois quant à savoir quel programme offre le plus de sécurité. Les résultats des études varient en fonction des mandants.

Installer des actualisations pour le navigateur

Les fonctions de navigateur étendues telles que JavaScript, Java, ActiveX et autres exigent l'installation d'un code étranger sur le PC du visiteur. Il existe certes divers mécanismes de protection censés éviter qu'un tel code de programme provoque des dégâts, mais on détecte sans cesse des lacunes de sécurité qui suppriment ces restrictions. Bon nombre de ces lacunes sont basées sur des erreurs de programmation et peuvent donc être écartées via l'installation automatisée des patches actuels de navigateur. Certains risques peuvent uniquement être évités en désactivant les options correspondantes dans les paramètres du navigateur Internet.

Mon navigateur est-il sûr ?

La meilleure arme contre les malwares du navigateur est le savoir ainsi qu'une méfiance saine face à tout ce qui provient de la Toile. Celui qui clique sur tout et n'importe quoi finit tôt ou tard par attraper un malware, indépendamment du fait que le navigateur ou le système d'exploitation soient neufs.

Conseils de sécurité

- Toujours travailler avec la version du navigateur la plus récente. Les navigateurs disposent de fonctions d'actualisation automatique qui se trouvent facilement dans le menu d'aide. Ainsi, les lacunes de sécurité dans le navigateur peuvent être rapidement comblées.
- Les navigateurs Internet modernes ont la capacité de reconnaître les sites Internet peu sûrs. S'il visite un tel site, l'internaute reçoit un avertissement.
- Les internautes qui ne sont pas dépendants de Windows ont la possibilité d'opter pour Mac ou Linux, car ces systèmes disposent d'une structure nettement plus difficile à attaquer.
- Limitez autant que possible l'installation de java scripts (Active Scripting) en passant par les paramètres du navigateur ou autorisez uniquement l'accès de sites fiables.
- Limitez autant que possible l'installation d'éléments de contrôle ActiveX en passant par les paramètres du navigateur. Augmentez les paramètres de sécurité du Internet Explorer à « élevé ».

Bernhard Bircher-Suits (Swisscontent Corp., trad. m.r) / 05.09.2008

Virus et vers : connaître ses ennemis !

Presque tous les jours et tant au bureau qu'à domicile, nous sommes bombardés de courriels douteux qui, s'ils sont ouverts, peuvent causer de sérieux problèmes. Afin de se protéger contre ce danger, il faut connaître ses ennemis.

Les malwares (« mal- » vient de l'anglais « malicious », malicieux, et « -ware » vient de « software ») sont classés en trois types de logiciels malveillants : les chevaux de Troie (voir dossier spécial) ainsi que les virus et les vers.

Les virus

Les virus informatiques sont la forme de malware la plus ancienne : ils se multiplient en s'autocopiant et en s'infiltrant dans des programmes, des documents et des supports de données encore sains. Les virus prennent beaucoup de formes différentes et engendrent des modifications incontrôlables dans le système d'exploitation, dans certains logiciels ainsi que des hardwares, par exemple en manipulant les connexions ou la carte graphique. Ainsi, les virus peuvent altérer la sécurité des données et des programmes se trouvant sur le PC et provoquer des interférences ainsi que des pertes de données.

Les vers

De nos jours, les vers informatiques ont quasiment évincé les virus. Les vers ressemblent aux virus, mais ils se répandent dans les réseaux de manière indépendante, par exemple via l'envoi de courriels infectés, la messagerie instantanée ou des programmes peer-to-peer tels que « Kazaa », « Morpheus » ou des systèmes BitTorrent. Les vers n'ont donc pas réellement besoin d'hôte pour se répandre. Ils utilisent les listes de distribution existantes. Etant donné que presque tous les ordinateurs sont connectés à un réseau, les vers se propagent à une vitesse incroyable.

Comment puis-je me protéger ?

En général, les vers sont automatiquement activés lorsqu'ils sont téléchargés sur le disque dur. Soyez donc particulièrement prudent lorsque vous ouvrez les pièces jointes : ouvrez uniquement les données que vous estimez totalement sûres, mais surtout pas les fichiers « .exe ». La terminaison du document indique que c'est un programme. Même les expéditeurs connus ne garantissent pas des pièces jointes propres. Les vers se propagent grâce aux comportements négligents, à l'excès de confort et à l'ignorance des utilisateurs. Utilisez donc avec précaution la messagerie instantanée ainsi que l'e-mail et les programmes peer-to-peer.

N'oubliez jamais : les vers sont les maîtres du camouflage. Faites particulièrement attention aux extensions de noms de fichiers telles que « .jpg.exe » ainsi qu'aux noms de fichier longs qui induisent en erreur quant au véritable caractère du fichier. Il est également dangereux de télécharger des données dont la fonction d'application reste méconnaissable pour les amateurs. Voici quelques exemples : .dll, .ax, .ini, .com, .pif, ou .bat.

Utilisez un programme antivirus

Avant d'ouvrir un fichier provenant d'Internet, vous devriez faire contrôler le document par un programme antivirus. Bon nombre de scanners de virus font cela automatiquement de nos jours. Il est toutefois nécessaire que le programme soit toujours actualisé, faute de quoi de nouveaux malwares pourraient passer entre les mailles du filet. Les programmes antivirus sont particulièrement essentiels pour Microsoft Windows : pour ce système d'exploitation, il existe une multitude de virus et de nouveaux s'y ajoutent presque chaque jour. Pour les Mac, la sécurité est entretemps devenue aussi nécessaire, car de plus en plus de virus s'y attaquent.

Alex Hämmerli (Swisscontent Corp, trad. m.r) / 05.09.2008

Le PC, une véritable forteresse

Celui qui surfe occasionnellement sur Internet et installe parfois des programmes doit protéger son ordinateur des virus, des chevaux de Troie et autres malwares. Dans ce cadre, les programmes de protection téléchargeables gratuitement sont généralement tout aussi efficaces que les programmes en vente et souvent très chers.

Il y a un moment dans la vie de tout PC ou portable encore vierge et à peine reconfiguré que tous les virus, vers et autres programmes espions (spyware) attendent avec impatience : le moment où l'ordinateur entre pour la première fois en contact avec Internet. Sans protection efficace, des malwares peuvent envahir un PC connecté à Internet en l'espace de 20 minutes. C'est ce qu'a constaté le centre américain Internet Storm Center (ISC).

Points d'accès et remèdes

Comment un programme infecté arrive-t-il sur un PC ? C'est très simple : pour aller sur Internet, l'appareil se voit attribuer une adresse IP grâce à laquelle chaque PC peut être identifié sur la Toile. Les logiciels de piraterie raffinés essaient sans cesse de trouver des adresses IP sur Internet. S'ils en trouvent, un virus, un ver ou un cheval de Troie peut être lancé sur l'ordinateur de manière ciblée. Un autre point d'accès est le courriel. Lorsqu'un ver transmis par courriel est introduit et installé sans qu'on ne le remarque, il esquive les mesures de sécurité du système et se propage. Les attaques sur les PC sont de plus en plus raffinées et lancées à des intervalles de plus en plus courts. C'est pourquoi les fournisseurs de services dans le secteur de la sécurité doivent souvent perfectionner leurs mécanismes de protection en un temps record. Pour garantir un niveau de protection élevé, chaque PC devrait compter trois différents outils de protection : un pare-feu contre les attaques IP sur la Toile, un logiciel antivirus et un logiciel espion contre les programmes d'espionnage. Il est également conseillé d'acquérir un logiciel permettant de surfer anonymement sur Internet.

Alternatives similaires et moins chères

Celui qui ne veut pas chaque année dépenser une fortune pour des logiciels de protection peut miser sur les programmes gratuits. Selon diverses études, ils ne sont en général pas moins efficaces que les alternatives payantes de fabricants renommés. Dans le domaine de l'antivirus, les programmes Avira Antivir (www.free-av.de [http://www.free-av.de]) et Avast Home (www.avast.com [http://www.avast.com]) sont convaincants. Néanmoins, l'application est uniquement gratuite pour les utilisateurs privés. Dans le domaine des logiciels gratuits, les paquets complets de sécurité sophistiqués ne sont jusqu'à présent pas disponibles. Cela signifie qu'en général, pour chaque type de danger, il faut installer un logiciel de protection particulier.

Programmes payants avec surface d'opérateur

Les paquets de sécurité payants protègent l'ordinateur privé de manière assez efficace et peuvent être, grâce à une surface d'opérateur homogène, facilement remplacés. Ils ne sont toutefois pas complets, contrairement à ce qu'aiment à prétendre les fabricants. Le magazine d'informatique allemand « c't » a comparé divers paquets de logiciels de sécurité Internet et constaté que dans tous les cas, au moins une composante de protection était faible. Dans le pire des cas, l'antivirus coupe entièrement la connexion à Internet ou illusionne l'utilisateur. Aucun programme testé par ce magazine ne constitue une véritable protection complète, indique « c't ». L'installation de logiciels de sécurité est toutefois indispensable. Les cybercriminels ayant beaucoup d'imagination, il est néanmoins conseillé de garder une certaine mesure de méfiance dans toutes les activités sur Internet, en plus des logiciels de protection, surtout lorsqu'il s'agit de transmettre des données personnelles.

Bernhard Bircher-Suits (Swisscontent Corp., trad. m.r) / 05.09.2008

Chevaux de Troie - logiciels présumés utiles

Si vous installez régulièrement sur votre ordinateur des logiciels gratuits présumés utiles depuis Internet, vous devez

protéger votre PC contre les pièces jointes des courriels et les dangereux chevaux de Troie.

Cheval de Troie (en anglais, « Trojan Horse »), appelé aussi troyen, désigne un logiciel d'apparence légitime, mais conçu pour subrepticement exécuter des actions nuisibles sur l'ordinateur de l'utilisateur. Souvent, les programmes gratuits téléchargés d'Internet ou de bourses de téléchargement sont infectés par ces logiciels malveillants. Les troyens appartiennent à la famille des programmes indésirables ou nuisibles appelés « malware ». La plupart du temps, ils s'introduisent dans l'ordinateur de la victime de manière ciblée et clandestine, mais peuvent aussi y parvenir par hasard. En général, ils sont camouflés sous l'apparence d'un programme utile en utilisant par exemple le nom d'un fichier utile, ou présentent une fonctionnalité utile outre leur fonction nuisible dissimulée.

Moyen de transport à des fins criminelles

Bon nombre de chevaux de Troie sont utilisés pour installer subrepticement des programmes nuisibles sur l'ordinateur de l'utilisateur. Ces programmes nuisibles fonctionnent de manière autonome sur l'ordinateur, ce qui signifie qu'on ne peut pas les désactiver en terminant ou même en effaçant le troyen. La fonction effective du fichier installé peut être de n'importe quel type. Ainsi, les programmes espions comme par exemple « Keylogger » peuvent s'introduire dans l'ordinateur. Ces programmes traquent les touches saisies du clavier et transmettent les données collectées aux criminels. L'installation clandestine de programmes contenant des portes dérobées est donc possible. Ces logiciels permettent de commander l'ordinateur à distance par Internet et mener des actions malfaisantes sans que l'utilisateur ne puisse le contrôler.

Les points d'accès

Les chevaux de Troie peuvent atteindre un ordinateur par les mêmes points d'accès que ceux utilisés pour la transmission de données électroniques, soit par tous les supports de données ou les connexions de réseau comme Internet. Les bourses d'échanges de fichiers et les sites manipulés « Drive-by-Download » ainsi que l'envoi de fichiers ou de pièces jointes par courriel constituent les accès les plus fréquemment utilisés pour l'introduction de troyens. La diffusion vers d'autres ordinateurs se fait ensuite depuis le PC de l'utilisateur qui ne se doute de rien. Souvent, les pirates utilisent un ver informatique comme vecteur transportant le cheval de Troie.

Protection avec les programmes antivirus

Afin de vous protéger efficacement contre les chevaux de Troie, renoncez à utiliser des programmes provenant de sources inconnues ou peu fiables. Les fournisseurs de programmes ou de services à la limite de la légalité sont particulièrement dangereux. Une autre mesure de protection est l'installation d'un logiciel antivirus. Pour combattre les intrus malveillants, de nombreux programmes antivirus tels que Panda Internet Security (www.pandasoftware.ch [http://www.pandasoftware.ch]), Norton Internet Security (www.symantec.com/de/ch/index.jsp [http://www.symantec.com/de/ch/index.jsp]) ou Eset Smart Security (www.eset.com/smartsecurity [http://www.eset.com/smartsecurity]) sont disponibles sur le marché. Si un cheval de Troie est détecté par un logiciel antivirus avant que l'utilisateur ne le diffuse, ce programme antivirus offre une protection efficace. Toutefois, une fois qu'un cheval de Troie a entamé sa mission destructive, ces programmes antivirus ne pourront les supprimer du système que jusqu'à un certain point. Si un troyen déjà installé est détecté, il est vivement conseillé de nettoyer le PC en sauvegardant la dernière image « propre » du disque dur. Un scanner de virus tend à effectuer partiellement cette tâche de manière fiable. En règle générale, un brin de méfiance est conseillé lorsque vous téléchargez des logiciels d'Internet ou installez des programmes à partir de supports de données sur votre ordinateur.

Bernhard Bircher-Suits (Swisscontent Corp., trad. mfp) / 05.09.2008

Phishing : la prudence est de rigueur

Prudence et méfiance sur Internet : si l'on vous demande par courriel des données confidentielles relatives à votre compte bancaire, effacez immédiatement ce courriel.

L'objectif du hameçonnage (phishing) est d'obtenir des renseignements personnels d'internautes crédules en utilisant des adresses Internet frauduleuses. Il s'agit, par exemple, d'informations sur votre compte de sites de ventes aux enchères en ligne (p. ex. eBay ou ricardo) ou de données d'accès pour l'e-banking. Les escrocs utilisent la crédulité et la bonne foi de leurs victimes en leur adressant des courriels avec des adresses d'expéditeur falsifiées. Dans ces messages, il est par exemple indiqué que les informations sur le compte ou sur les données d'accès (nom d'utilisateur et mot de passe) ne sont plus sécurisées ou actuelles et qu'elles devraient être changées ou confirmées via un lien mentionné dans le courriel. Le lien n'est pas dirigé sur le site original du fournisseur de services en question (p. ex. la banque), mais sur un site Internet contrefait par l'escroc. Avec les données obtenues de manière frauduleuse, un escroc peut, par exemple, effectuer des transactions bancaires au nom de la victime (utilisateur Internet) ou placer une offre sur un site de vente aux enchères.

Se protéger en faisant preuve de vigilance

Il est impératif de rester méfiant lorsque l'on surfe sur Internet. Seule une vigilance accrue peut éviter le pire. En effet, une falsification parfaite n'existe pas. Une banque sérieuse ne demandera jamais de changer des mots de passe ou autres données sensibles par courriel. Souvent, le destinataire sera abordé par une formule générale telle que « Cher client » au lieu de par son nom, encore un signe de falsification puisque la banque connaîtrait le nom du client. Une grammaire ou une orthographe déficiente peut aussi constituer un indice d'attaque par hameçonnage. Ces courriels doivent être immédiatement effacés. Il est judicieux d'utiliser un mot de passe pour chaque application.

En outre, il est conseillé de toujours saisir manuellement l'adresse Internet de la banque. Il ne faut en aucun cas cliquer sur des liens contenus dans le courriel ou sur des pages Internet de tierces personnes afin d'arriver sur le site Web souhaité. Si vous deviez malgré tout atterrir sur le site de « votre banque » via un hyperlien, vous devez impérativement et immédiatement vérifier l'authenticité de ce site Internet à l'aide du certificat d'authenticité. Le cryptage de la connexion doit également être vérifié. Pour ce faire, double-cliquez sur le symbole « cadenas fermé » dans la partie inférieure de la fenêtre du navigateur et les caractéristiques du certificat apparaissent à l'écran. Il doit être au nom de la banque. Si le « Fingerprint » du certificat correspond à celui publié sur la page d'accueil de la banque, il s'agit bien d'une connexion cryptée sécurisée sur le bon site.

Se protéger par des logiciels

Outre la prudence requise, les logiciels peuvent également contribuer à la sécurité en matière d'Internet. Selon le logiciel installé, le filtre du courriel du programme antivirus reconnaît les courriels de hameçonnage, les bloque et les efface, à condition que le logiciel antivirus soit constamment mis à jour. Les navigateurs comme Internet Explorer ou Mozilla Firefox alertent aussi contre les pages de hameçonnage. Les navigateurs et filtres e-mail qui se basent sur des listes noires publiées sur Internet dépendent de l'actualité de celles-ci. Ceci constitue un grand inconvénient dans les nouvelles formes d'attaque par hameçonnage, car ni le procédé ni la défense ne sont connus.

Dajan Roman (Swisscontent Corp., trad. mfp) / 05.09.2008

Bloquer les accès malintentionnés avec un routeur

Si l'on souhaite protéger son ordinateur contre les connexions entrantes malintentionnées, un routeur NAT offre au moins une protection partielle. Un routeur coupe en fait le réseau mondial de votre ordinateur personnel. Un routeur doté d'un pare-feu intégré permet en outre de définir les services Internet autorisés.

Lorsque vous êtes connecté à Internet, vous courez le risque que des programmes ou des personnes pénètrent dans votre ordinateur via des points faibles ou des failles de sécurité et lisent, manipulent ou effacent des fichiers. Outre le logiciel antivirus habituel et un logiciel pare-feu, il existe une autre méthode qui offre une première protection avant qu'un intrus ne puisse s'introduire dans votre ordinateur.

Connexion entre l'ordinateur et Internet

Les routeurs de la plupart des opérateurs sont équipés de NAT. L'abréviation NAT signifie « Network Address Translation ». Le procédé NAT connecte l'ordinateur du réseau privé local à Internet. En théorie, tout ordinateur connecté à Internet a besoin d'un numéro de code unique pour l'identification, c'est-à-dire l'adresse IP. Cette adresse est en général attribuée à un seul ordinateur par le fournisseur de services Internet. Lorsque vous installez un routeur, il reste toutefois le support de l'adresse IP. Les ordinateurs connectés au réseau local à domicile reçoivent séparément du fournisseur de services Internet des adresses indépendantes.

Réseau privé invisible à l'extérieur

Grâce à un routeur, plusieurs ordinateurs peuvent être exploités sur une même connexion Internet. Du point de vue de la stratégie de sécurité, ce système présente aussi l'avantage de séparer le réseau international du réseau local. En effet, les adresses IP privées du routeur ne sont pas visibles depuis la Toile, ce qui rend les accès malintentionnés à l'ordinateur difficiles.

Limiter le courant de données

Si le routeur dispose d'un pare-feu intégré, vous pouvez en outre définir les services Internet pour lesquels un débit de données est autorisé. Dans la liste correspondante de l'interface utilisateur du routeur, sélectionnez uniquement les applications dont vous avez vraiment besoin, de façon à bloquer les courants de données indésirables venant de l'extérieur du routeur. Si une application ne fonctionne pas sur l'ordinateur à cause du pare-feu, le problème peut être résolu par le déblocage du port. Ceci est possible grâce aux options « Port-Forwarding », « Virtual Server » ou « Static Routing », se trouvant généralement dans les paramètres avancés de l'outil de configuration du routeur. Le manuel ou le site Internet du producteur de logiciel permet de déterminer le port de chaque application.

Pas de substitution pour le logiciel pare-feu

Il ne faut cependant pas surestimer cette limitation globale des accès extérieurs. Elle ne peut remplacer un logiciel pare-feu efficace. Un bon pare-feu offre également une protection adéquate pour le courant de données interne vers l'extérieur et comprend en outre d'autres possibilités pour la réglementation de certains accès qu'un routeur n'offre pas. Pour optimiser la sécurité, il est recommandé d'installer un logiciel pare-feu sur l'ordinateur, en plus du routeur. Si vous utilisez un simple modem USB, un logiciel pare-feu s'avère impératif. Cela vaut aussi pour tout utilisateur disposant d'une connexion Internet d'un câblo-opérateur sans routeur connecté. A partir de Windows XP, un pare-feu comprenant quelques fonctions de base est déjà intégré dans le système.

Routeurs/modems des différents fournisseurs Internet (Exemple de la Suisse)

Fournisseur	Appareils avec NAT	Appareils sans NAT
Swisscom	Tous les appareils	Aucun
Cablecom	Aucun	Tous les appareils
Sunrise	Tous les appareils (ZyXEL)	Aucun
Solnet	Tous les appareils (ZyXEL, AVM et Draytek)	Aucun
Tele 2	Tous les appareils	Aucun
QuickLine	Abonnements sans appareils	Aucun
Backbone (seulement pour entreprises)	Tous les appareils (ZyXEL et Cisco)	Aucun

Source : données des fournisseurs Internet sélectionnés

Christian Iten (Swisscontent Corp., trad. mfp) / 05.09.2008

E-banking : sécurité élevée à peu de frais

En observant quelques mesures de sécurité élémentaires, vous pouvez effectuer vos paiements en ligne sans problème. Il s'agit de sécuriser votre ordinateur et de rester vigilant pendant vos sessions d'e-banking.

Beaucoup de personnes restent sceptiques quant à l'utilisation de l'e-banking. Craignant que leur compte soit vidé, elles n'ont aucune confiance dans les systèmes et préfèrent effectuer leurs opérations bancaires avec papier et courrier, mais tout le monde peut forcer une boîte aux lettres. En revanche, pour pénétrer dans un PC, il faut un minimum de connaissances informatiques. Le risque peut en outre être minimisé très simplement en suivant quelques conseils (www.melani.admin.ch [http://www.melani.admin.ch]).

Protection de l'ordinateur

Pour effectuer votre e-banking en toute sécurité, il est vivement conseillé d'utiliser uniquement un ordinateur doté d'un programme pare-feu et d'un logiciel antivirus. L'important est d'effectuer régulièrement les mises à jour des logiciels et d'utiliser les versions les plus actuelles du navigateur et des différents programmes. Si elle est disponible, il est conseillé d'activer la fonction de mise à jour automatique. Cela vaut surtout pour les logiciels antivirus. Lorsque le pare-feu est activé, il empêche l'établissement de connexions Internet indésirables. N'ouvrez jamais des courriels d'origine inconnue et n'installez jamais des programmes non fiables.

Avant d'ouvrir une session

Avant de vous connecter sur la plate-forme d'e-banking, vous devez fermer toutes les fenêtres du navigateur. Pour ouvrir une session d'e-banking, vous devez rouvrir le navigateur et toujours saisir l'adresse manuellement. Pendant la session, toutes les autres connexions doivent rester fermées et aucun autre site Internet ne peut être sélectionné. Il est aussi impératif d'observer les règles du mot de passe. Les établissements financiers demandent à leurs clients en ligne un procédé d'authentification à plusieurs niveaux (p. ex. numéro de contrat, liste à biffer et mot de passe ou similaire). La plupart du temps, le client peut choisir librement son mot de passe. Choisissez un mot de passe difficile à deviner composé de lettres, de chiffres et de caractères spéciaux (minimum 8 caractères) et modifiez-le régulièrement. Ces mots de passe ainsi que tous les autres ne peuvent être communiqués à personne, même pas à la banque. La banque ne vous demandera jamais de lui communiquer votre mot de passe. N'écrivez jamais votre mot de passe et ne le sauvegardez surtout pas sur votre ordinateur.

Pendant la session d'e-banking

Vérifiez l'authenticité du site Internet à l'aide du certificat d'authenticité, ainsi que le cryptage de la connexion (voir article sur le « phishing »). Les éventuels messages d'erreurs ou d'alarme devraient être pris au sérieux et respectés. Si vous avez le moindre doute, contactez immédiatement votre banque.

Terminer la session d'e-banking

Il est important de se déconnecter et de terminer correctement la session d'e-banking. Toutes les interfaces des banques disposent d'une fonction prévue à cet effet, intitulée « terminer », « logout » ou « quitter ». En général, une nouvelle page apparaît sur le navigateur vous confirmant la fin de session correcte. Après avoir quitté la session d'e-banking, il est conseillé d'effacer les fichiers Internet temporaires se trouvant dans le cache du navigateur afin d'effacer de votre ordinateur la « mémoire » et toute trace de votre session en ligne.

- Internet Explorer : Extras/options Internet/effacer cookies/OK.
- et : Extras/options Internet/effacer fichiers/effacer tous les contenus hors ligne/OK
- Firefox : Extras/réglages/protection des données/effacer tout
- Safari : Safari/vider cache

Dajan Roman (Swisscontent Corp., trad. mfp) / 05.09.2008

Sécurité W-LAN

L'internaute qui surfe sans fil sur Internet ou qui échange des données via un réseau sans fil encourt le danger de rencontrer des pirates informatiques peu scrupuleux dans le réseau. Quelques simples réglages sur le routeur W-LAN suffisent à optimiser la sécurité.

Il est très pratique de surfer sans fil sur Internet avec un PC ou un portable ou d'échanger des données entre

différents terminaux dans un réseau sans fil. Toutefois, lors de l'utilisation du W-LAN (Wireless Local Area Network), souvent désigné dans la publicité par le terme technique Wi-Fi, la prudence est de rigueur. Si le réseau radio n'est pas assez sécurisé, des intrus peuvent utiliser la connexion Internet pour des activités illégales, voire espionner les données sauvegardées sur l'ordinateur. Quelques simples réglages sur le routeur W-LAN permettent de minimiser le risque.

Protéger l'accès au routeur avec un mot de passe

Pour maintenir l'installation du routeur confidentielle, il vaut mieux connecter l'ordinateur par câble. La première règle est de choisir un mot de passe personnel pour l'accès au routeur. Mais attention, si vous oubliez le mot de passe, vous n'avez pas accès à une nouvelle configuration ; vous devez alors réinitialiser l'ordinateur manuellement, et toutes les installations effectuées sont perdues !

Cryptage, la mesure essentielle

La mesure la plus importante en matière de protection du W-LAN est le cryptage. Pour ce faire, plusieurs méthodes sont généralement disponibles dans les interfaces de configuration. La méthode la plus sûre se nomme Wi-Fi Protected Access (WPA ou WPA2). Tous les routeurs actuels supportent cette méthode. Les composants W-LAN plus anciens ne supportent pas encore le WPA2. Ensuite, jeter un coup d'oeil sur le site Internet du fournisseur du routeur peut également s'avérer utile. Une mise à jour du logiciel y est peut-être déjà disponible, prête à être téléchargée et transmise au routeur.

Accepter uniquement des terminaux connus

Pour améliorer la sécurité de son réseau W-LAN, il existe ce que l'on appelle le filtrage MAC : si les adresses MAC des périphériques que vous souhaitez autoriser sont saisies dans la liste correspondante du routeur, seules ces dernières ont un accès au réseau W-LAN. L'adresse MAC, représentée par 12 chiffres, est unique et permet l'identification. Elle ne peut être modifiée. Toutefois, la sécurité n'est pas garantie à 100%. Les pirates chevronnés réussissent à contrefaire les adresses MAC. En essayant systématiquement avec des adresses aléatoires, il devient possible d'avoir accès au réseau W-LAN.

Activer le pare-feu et modifier le nom du réseau

En général, un routeur W-LAN possède un pare-feu intégré. Lorsque l'ordinateur propose cette option dans le menu de configuration, il vaut la peine de l'activer. Une autre mesure de protection est la modification du SSID saisi par défaut dans le routeur en une description générale permettant l'accès au Wi-Fi, sans association avec le propriétaire ou le lieu du réseau sans fil. Ce SSID n'est autre que le nom du réseau W-LAN.

Christian Iten (Swisscontent Corp., trad. mfp) / 05.09.2008

Ingénierie sociale : vol d'identité avec répercussions

néfastes

L'ingénierie sociale est l'une des formes les plus dangereuses et les plus efficaces de cybercriminalité. Le plus grand risque est le facteur humain.

L'« ingénierie sociale » est une technique qui a pour but d'extirper des informations, des données confidentielles ou des services non autorisés à des personnes en exploitant leur confiance. Les mesures de sécurité sont manipulées. L'ingénierie sociale peut être divisée en trois domaines : basée sur l'approche personnelle, basée sur l'informatique et l'ingénierie sociale inverse.

Ingénierie sociale basée sur l'approche personnelle

Dans cette forme d'ingénierie sociale, les criminels essaient de parvenir directement aux informations en se faisant passer pour des autorités ou des personnes de confiance. Ainsi camouflés, ils obtiennent frauduleusement des données sensibles. La tactique de la fouille des poubelles est aussi un procédé d'ingénierie sociale. Les poubelles d'entreprises ou de personnes privées sont passées en revue en quête de mots de passe, de dossiers, de photos et d'autres informations. Ces éléments sont directement utilisés, par exemple en tant que moyen de pression en cas de chantage, ou indirectement, en livrant des informations à l'agresseur avec lesquelles il peut se créer une fausse identité.

Ingénierie sociale basée sur l'informatique

Avec cette forme d'ingénierie sociale, des identités sont simulées à l'aide de moyens techniques comme les e-mails ou les sites Web afin d'obtenir les données souhaitées. Le « phishing », ou hameçonnage, est l'exemple par excellence de ce type de fraude. Lisez à ce sujet d'autres articles dans ce dossier. Bon nombre de tirages au sort ou de jeux de gains figurent également dans cette catégorie d'ingénierie sociale. L'objectif est d'obtenir des données personnelles, utilisées ensuite de manière abusive à des fins publicitaires.

Ingénierie sociale inverse

L'objectif de l'ingénierie sociale inverse est de leurrer la victime en tant que prétendu sauveteur dans l'urgence, de manière à ce qu'elle livre des informations sensibles ou soit entraînée vers des actions nuisibles. La plupart du temps, ce type d'attaque crée une situation problématique qui provoque du stress ou des craintes chez la victime. Les pirates d'ingénierie sociale inverse simulent, par exemple, une attaque informatique ou une panne de système qui exige immédiatement l'accès au compte d'utilisateur d'un présumé technicien.

Protection contre l'ingénierie sociale

La protection contre l'ingénierie sociale ne peut guère être garantie par une solution technique, étant donné que cette dernière est contournée. C'est pourquoi seule la victime peut contribuer le plus en matière de sécurité en s'assurant de la vraie identité et de la légitimité de l'interlocuteur, et c'est uniquement ensuite qu'elle peut fournir des données sensibles. En cas de doute, il est impératif de demander le nom, le numéro de téléphone et l'endroit où se trouve le correspondant téléphonique afin de vérifier ensuite toutes ces coordonnées. Des informations apparemment anodines comme un message d'absence ne devraient pas être transmises de bonne grâce à tout le monde, car elles pourraient servir à un pirate pour créer une fausse identité. Dans ce cas, il faut tout particulièrement veiller à ce que le pirate ne parvienne pas, par tâtonnements, grâce à des questions habiles et des recoupements, à l'information recherchée. En

outre, les vieux fichiers, papiers, disques durs et autres documents sensibles devraient soigneusement être détruits.

Alex Hämmerli (Swisscontent Corp., trad. mfp) / 05.09.2008

Liste de contrôle : comment optimiser la sécurité en ligne

Internet recèle de nombreux dangers : les visiteurs de sites Internet sérieux peuvent aussi infecter leur PC comme le font les cybercriminels en téléchargeant, par exemple, des logiciels dangereux d'offres Internet douteuses. L'utilisateur de PC n'est cependant pas désarmé face à ces attaques informatiques. En connaissant les invasions possibles et en suivant quelques simples conseils, l'internaute peut aisément s'en protéger.

Pour protéger votre ordinateur, votre comportement sur Internet est essentiel. Cela commence par la bonne utilisation de mots de passe qui doivent être appropriés, conservés de manière sûre, être différents et cryptés. Les mots de passe devraient en outre être uniquement saisis dans des connexions de réseau cryptées garantissant la transmission cryptée des informations confidentielles. Un ordinateur en marche ne devrait pas rester sans surveillance, sans être sécurisé par un mot de passe correspondant ; des intrus pourraient sinon accéder de manière incontrôlée aux données confidentielles.

Si vous surfez sur Internet, votre navigateur devrait toujours être sécurisé et mis à jour en permanence. Les navigateurs Internet obsolètes affichant les sites Internet constituent souvent un point d'accès pour les programmes nuisibles. Quelques simples conseils peuvent vous aider à améliorer la sécurité de votre navigateur.

Si vous surfez sans fil sur Internet ou échangez des données sur un réseau sans fil, vous encourez le risque que des pirates malintentionnés ne s'y introduisent. Quelques simples réglages sur le routeur W-LAN suffisent à optimiser la sécurité.

Lorsqu'il s'agit de sécuriser son ordinateur contre d'éventuelles attaques extérieures malintentionnées, un routeur NAT offre au moins une protection partielle. En effet, un routeur sépare le réseau mondial de l'ordinateur à domicile. Avec un routeur doté d'un pare-feu intégré, vous pouvez en outre définir les services Internet auxquels vous souhaitez autoriser l'accès.

Les programmes de sécurité sont aussi essentiels. Sans ces logiciels, des parasites virtuels peuvent rapidement planter un ordinateur non sécurisé. Pour une protection sans faille, quatre outils de sécurité devraient être installés sur chaque PC : un pare-feu contre les attaques du réseau, un logiciel antivirus contre les programmes malveillants, un logiciel contre les programmes espions et un bon navigateur.

Les virus, les vers et les chevaux de Troie sont dangereux. Les virus et les vers sont souvent diffusés via des courriels douteux que l'utilisateur ouvre sans rien suspecter. Les chevaux de Troie sont des logiciels camouflés sous l'apparence d'applications informatiques utiles, mais qui remplissent une autre fonction à l'arrière-plan sans que l'utilisateur ne le sache. Souvent, les programmes gratuits provenant d'Internet ou des bourses de téléchargement sont infectés avec ces vermines. Vous pouvez vous protéger contre ces logiciels malveillants (malware) en n'ouvrant

aucun fichier dont le contenu n'est pas clairement identifiable comme inoffensif, ou en refusant d'utiliser des programmes d'origine inconnue ou peu fiable.

Un autre risque pour l'internaute consiste en ce que l'on nomme « phishing » ou hameçonnage. Son objectif consiste à obtenir des données confidentielles d'utilisateurs crédules par le biais d'adresses falsifiées. Pour éviter cela, méfiance et grande vigilance sont de rigueur.

L'une des formes les plus dangereuses et les plus efficaces de cybercriminalité est certainement l'ingénierie sociale. Le plus grand facteur risque est le facteur humain. Il s'agit d'une technique qui a pour but de soutirer des informations, des données confidentielles ou des services non autorisés à des personnes en exploitant leur confiance. Les mesures de sécurité sont manipulées. C'est pourquoi seule la victime peut contribuer le plus en matière de sécurité en s'assurant de la vraie identité et de la légitimité de l'interlocuteur.

Jeannette Schläpfer (Swisscontent Corp., trad. mfp) / 05.09.2008