

## « Le facteur humain est souvent à l'origine de problèmes de sécurité »

Une attaque informatique ne se présente pas uniquement sous la forme d'un virus. Et contrairement aux idées reçues, le premier du genre – Elk Cloner – a été détecté sur un ordinateur Macintosh Apple II en 1982. La sécurité n'est plus seulement dépendante des barrières techniques, mais aussi de facteurs humains. Décryptage avec un spécialiste de la sécurité des réseaux.



Michel Rueger : « L'envoi de code par SMS représente un risque lors de la transmission de celui-ci, car les réseaux mobiles ne sont pas imperméables, le standard GSM datant quelque peu ».

### Monsieur Rueger, quels sont les moyens existants pour assurer la sécurité sur le web et dans les réseaux des technologies IT ?

Il n'y a pas de solution miracle lorsque l'on parle de sécurité ! Le meilleur moyen est celui qui est adapté au risque lié. Chaque entreprise doit établir une stratégie en fonction de sa présence et de son utilisation

d'Internet. Avec l'arrivée de services « Web 2.0 », interactifs avec l'utilisateur, l'accès au web mérite d'être géré de manière approfondie pour éviter que l'interaction n'aille pas au-delà de ce que l'entreprise ne souhaite. Avec certains logiciels de communication VoIP (voix sur IP) et chat, il est par exemple possible de donner le contrôle de votre ordinateur à un correspondant. Ce genre de

fonction peut rapidement se trouver en désaccord avec la politique d'accès aux informations de l'entreprise, lorsque du côté de la réception on demande à chaque visiteur de s'inscrire et de porter un badge...

### Les fabricants d'anti-virus ont-ils su évoluer et s'adapter aux attaques exponentielles des pirates ?

Les éditeurs font un énorme travail et ce sur deux niveaux : ils doivent continuellement s'adapter pour découvrir et bloquer les nouvelles menaces, tout en proposant des solutions qui sont utilisables par la plupart des réseaux. Mais une attaque informatique ne se présente pas uniquement sous la forme d'un virus. C'est pourquoi certains éditeurs intègrent des fonctions de prévention d'intrusions (IDP), ainsi qu'une surveillance des processus du système. Ensuite, l'efficacité de l'antivirus sur l'ensemble d'un parc informatique dépend énormément des paramètres avec lesquels il a été déployé, et comment il est surveillé. Certains éditeurs sont parfois plus réactifs que d'autres pour la découverte de virus, mais ce n'est pas l'unique critère : il faut aussi que l'antivirus puisse supprimer correctement le virus qu'il a découvert, et se protéger lui-même contre des menaces inconnues (au risque de se faire à son tour piloter par un virus).

### Comment un jeune hacker peut-il encore de nos jours s'introduire dans une base de données de la NASA ou du Pentagone, avec toutes ces barrières ?

Probablement pour les mêmes raisons qu'une attaque terroriste est toujours possible, même dans les pays dont la défense est bien organisée. Preuve que la sécurité informatique n'est pas qu'une question de budget (en partant du principe que le budget IT Security de la NASA est adéquat). Les entreprises et collectivités peuvent tirer profit de ces faits et en déduire qu'une bonne solution de sécurité repose sur une stratégie (non seulement sur du matériel/logiciel) et qu'une solution de sécurité doit être surveillée afin de détecter les activités suspectes à temps.

**Pourquoi les utilisateurs des ordinateurs Mac sont-ils moins vulnérables aux virus ? Est-ce une raison technique ou par désintérêt des pirates ?**

Les deux sont probables. La raison technique est due à l'architecture du système d'exploitation MacOSX, reposant sur un noyau UNIX qui a été développé en tenant compte de la gestion des droits sur les processus. A l'inverse des PC sous Microsoft Windows, les applications sous UNIX ne s'exécutent (normalement) pas avec les privilèges administrateur. Cette stratégie rend la propagation des virus difficile. Pour mémoire, l'un des premiers virus informatiques qui a touché le grand public est Elk Cloner, en 1982. Il s'activait lors de la 50<sup>ème</sup> partie du jeu dans lequel il avait été intégré. Et ce jeu fonctionnait sous... Macintosh Apple II, un ordinateur assez répandu à cette époque. Il faudra attendre 4 ans pour trouver le premier virus sur IBM PC, (c)Brain. La raison du désintérêt des pirates pourrait devenir une motivation à l'avenir, la stratégie d'Apple étant de contrôler tout ce qui s'installe sur les plates-formes mobiles telles que iPhone et iPad, ce qui ne plait pas forcément, sans parler de leur grande influence sur le marché du multimedia et des contenus.

**Quel est le rôle de l'autorité de certification dans un certificat d'entreprise ?**

D'une manière générale, il s'agit d'un processus de validation. Pour tous les certificats (d'entreprise ou non), l'autorité de certificat signe, émet et maintient les certificats ainsi que les listes de révocation. La vérification de l'identité de l'entreprise ou de la personne se fait soit directement par l'autorité de certificat, soit par une autorité d'enregistrement, sur la base de papiers d'identité et d'extraits du registre du commerce pour les entreprises. L'autorité de certification opère elle-même ou peut déléguer l'hébergement de la clé privée du certificat à un opérateur de certification ou autorité de dépôt. En Suisse, nous avons la chance de bénéficier d'une preuve d'identité électronique sécurisée, reconnue par la loi : SuisseID. Les autorités de certifications sont ainsi des organismes accrédités pour l'émission du certificat SuisseID. Il s'agit en l'occurrence de Quo Vadis, SwissSign, Swisscom, et l'Office Fédéral de l'Informatique et des Télécommunications (OFIT).

**Qu'est-ce qu'une identité numérique et, vu la prolifération des réseaux sociaux, peut-elle être vraiment sécurisée ?**

L'identité numérique est l'ensemble des informations placées dans divers profils tels que Facebook, LinkedIn, ainsi que des contributions dans des blogs, formant ainsi une entité virtuelle rattachée à un individu. On pourrait

imaginer joindre un certificat (par exemple SuisseID) afin de s'assurer que le profil correspond vraiment à la personne recherchée, et non à un homonyme ou un imposteur. Mais un certificat, s'il identifie son détenteur, ne va pas régler la problématique de l'utilisation des informations placées dans un profil Facebook, que ce soit par l'éditeur du site ou les membres qui vont le consulter. Aussi,

**« Une réelle défense étatique modifiera notre appréciation de liberté dans le monde virtuel »**

mis à part le nom, le prénom, l'âge et le sexe de l'individu, la véracité des informations que l'individu aura placées dans ses profils tient uniquement à sa bonne foi.

**Quelle est la meilleure méthode d'identité pour gérer son compte bancaire ? La technique des mots de passe aléatoires (liste) n'est-elle pas dépassée ?**

La liste de codes aléatoires est théoriquement moins sécurisée car elle est générée par avance, stockée chez le détenteur du site, imprimée, envoyée à l'utilisateur puis stockée chez l'utilisateur. Elle peut être simplement copiée par une personne qui la trouverait. Elle laisse donc beaucoup de probabilité à une erreur humaine. Le token (petit générateur de codes aléatoires) ou le lecteur de carte sont plus fiables car le code aléatoire est généré lors de l'utilisation, parfois après l'introduction d'un mot de passe, et sa validité est limitée dans le temps. Ce code unique étant généré aléatoirement sur une base de temps ou d'événement, il reste très difficilement prédictible.

**Et la méthode du SMS ?**

Le SMS est une évolution du token ou du lecteur de carte : dans ce cas le code aléatoire est généré du côté du serveur, puis il est transmis à l'utilisateur via SMS. Un risque lors de la transmission du code existe, car les réseaux mobiles ne sont pas imperméables, le standard GSM datant quelque peu. Cependant ce système a un avantage : il ne nécessite pas de token ou de lecteur de carte (sur lesquels bien des utilisateurs inscrivent leurs noms d'utilisateurs et mots de passe, réduisant à néant les efforts de sécurité). Il met en jeu un appareil avec lequel les utilisateurs ont une relation particulièrement intime : leur téléphone portable.

**Ok, mais combien de personnes prennent-elles la peine de dissimuler leur token et leurs informations de login bancaire dans des endroits différents ?**

Très peu, pour des questions de commodité. Combien de personnes laissent-elles leur téléphone portable sans surveillance ? Très

peu, car il contient des informations personnelles, l'utilisateur y est donc naturellement attentif. Il est probable que si l'on arrive à garantir une sécurité technique dans les méthodes d'identification faisant intervenir le téléphone portable, on aura un système bien sécurisé car il comprend un lien émotionnel avec l'utilisateur, ce qui n'est pas le cas avec une liste à biffer ou un token. Il est encore

utile de rappeler que la cause première de piratage bancaire est la présence de programmes espions ou de virus sur l'ordinateur de l'utilisateur, permettant au hacker de le contrôler en arrière-plan une fois le login réalisé.

**Quelle est alors la meilleure méthode pour atteindre la sécurité au maximum ?**

Rester déconnecté et n'échanger aucune donnée !

**Que se passerait-il si Internet tombait en panne pendant une semaine ? Accessible a-t-elle prévu ce genre de scénario et comment s'en sortir ?**

Ce serait une question à poser à un opérateur. Si les ordinateurs de la planète sont déconnectés d'Internet, la problématique de la sécurité informatique s'en verrait allégée.

**Que conseillez-vous à une entreprise pour se sécuriser au mieux ?**

La base de la sécurité est organisationnelle. La première démarche est de faire l'inventaire des fonctions informatiques vitales, et de définir quels risques sont acceptables et lesquels ne le sont pas. Ensuite il faut définir un cahier des charges pour le responsable informatique. Le facteur humain étant souvent à l'origine de problèmes de sécurité, il convient de définir les conditions dans lesquelles les systèmes informatiques de l'entreprise peuvent être utilisés et d'expliquer ces règles aux utilisateurs qu'ils devront ensuite approuver. Ensuite, des solutions techniques pourront être évaluées en fonction des besoins, puis mises en place. En ce qui concerne la protection de base au niveau de la connexion Internet, je recommande dans tous les cas de mettre en place une solution de filtrage permettant d'analyser le contenu du trafic sur les couches 4 à 7 du modèle OSI, en plus du filtrage « statefull » au niveau 3 réalisé par les firewalls conventionnels. Cette analyse en profondeur permet une meilleure prévention d'intrusions, la détection de virus et programmes espions et le blocage du trafic qu'ils génèrent. L'administrateur pourra aussi choisir d'autoriser

ou non les nombreux flux multimedia et réseaux d'échange, qui peuvent se fondre dans la masse du trafic utilisant le protocole http. Un filtrage plus avancé encore permet d'intercepter les connexions cryptées (https), et d'appliquer un filtrage similaire au trafic non crypté.

**Comment voyez-vous le développement de la sécurité informatique – technique, stratégique et sociale – ces dix prochaines années ?**

A court terme, l'identification des intervenants devrait se généraliser. Il est encore trop simple de pouvoir écrire un email en utilisant une adresse d'expéditeur quelconque. Pour être clair, rien ne l'empêche. Les certificats combleront ce problème, et dans un 2<sup>ème</sup> temps, des services IdP (Identity Provider) spécialisés pourront donner une preuve de fonction, par exemple le droit de signature pour une entreprise sur la base du registre du commerce, ou l'appartenance à un registre des notaires, des fiduciaires, etc.


Au niveau technique, la capacité à analyser en temps réel le trafic des données, à corréler les informations pour en déduire un éventuel risque permettra d'utiliser

efficacement le trop grand nombre d'alertes généré par les systèmes de surveillance actuels. Sur le plan de l'infrastructure, on en parle depuis bientôt dix ans, le protocole IPV6 devrait s'imposer prochainement.

**Pourquoi la migration vers IPV6 est-elle inévitable ?**

L'explosion des connexions mobiles nécessite de plus en plus d'adresses IP : en août 2010, on estime que l'Internet Assigned Numbers Authority (IANA) assignera le dernier bloc de 16,7 millions d'adresses IP libres à un registre Internet régional (RIR) en juin 2011. Et que les RIR épuiseront les dernières adresses IPV4 en février 2012. Ce nouveau protocole permettra de nouvelles fonctions de sécurité et d'authentification. Mais la plus grande évolution sera probablement au niveau des états. Il y a peu de frontières dans le monde virtuel et un contrôle quasi inexistant sur les échanges : des informations, des produits virtuels et des taxes échappent aux gouvernements. La mise en place d'une réelle défense étatique modifiera probablement notre appréciation de liberté dans le monde virtuel.

**Un souhait ou conseil particulier ?**

Qu'Internet se développe en tenant compte des expériences du monde réel et des analogies qu'il convient de mettre en évidence. 

Interview :  
Roland Keller  
Rédacteur responsable  
SWISS ENGINEERING RTS

**regard sur**

**Michel Rueger**

Avec son associé Laurent Meuwly, Michel Rueger a fondé en 2001 Accessible Sàrl, une entreprise spécialisée dans la sécurité informatique et le développement d'applications web. Ce jeune chef d'entreprise de 36 ans a suivi le développement d'Internet dès 1994 en tant que « Network Designer » pour le compte d'un des premiers fournisseurs d'accès en Suisse, auprès duquel il a créé le département de sécurité IT. En 2010, sa société fribourgeoise sise à Givisiez compte pas moins de 15 employés et met ses compétences au service de plusieurs projets du Pôle scientifique et technologique du canton de Fribourg.

# Anti-virus : l'embaras du choix

Qu'ils soient gratuits ou payants, les logiciels anti-virus sont d'emblée efficaces en fonction des versions choisies. Les éditeurs offrent leurs outils plutôt dans le but de générer d'énormes quantités de clients afin de mieux les sensibiliser sur la sécurité et accroître leurs ventes.

Parmi la panoplie existante sur le marché, quel anti-virus faut-il choisir ? En principe, tous les fabricants offrent les barrières suffisantes pour empêcher la plupart des virus d'infecter nos ordinateurs. Chacun y apporte ses pare-feux ou ses solutions plus ou moins efficaces selon la mise à jour des virus traqués. Avira, un développeur peu populaire, propose par exemple des statistiques de hameçonnage permanentes. En tant que spécialiste allemand de premier rang en matière de sécurité, ce dernier, dont le siège est situé à Tettngang, près du Lac de Constance, annonce qu'il compte environ 100 millions de clients pour 300 employés.

**De Panda à Symantec**

Panda Security, qui fête par ailleurs cette année son 20<sup>ème</sup> anniversaire, vante son système d'« Intelligence collective » contre les malwares. Celui-ci fonctionne comme une base de données en ligne et en temps réel qui stocke la plupart des fichiers de

signature, gardant seulement l'essentiel sur les postes des clients. Chaque utilisateur fait office de capteur de nouveaux virus et autres malwares, en envoyant à l'entreprise de Bilbao (fief de la fondation de Panda), via Internet, les données sur les nouvelles menaces détectées sur son poste. Cette nouvelle approche diminue la consommation de la bande passante sur les PC des utilisateurs et fournit une protection plus rapide, plus complète et toujours à jour. Kaspersky Lab, avec son siège à Moscou, dispose aussi d'outils étoffés : ce groupe international de plus de 1'700 spécialistes hautement qualifiés a mis au point bon nombre des standards technologiques de l'industrie des antivirus, comme par exemple : des solutions à échelle complète pour environnements Linux, UNIX et NetWare. L'entreprise californienne Symantec, plus connue sous le nom de son produit Norton, est une grosse firme qui compte pas moins de 17'500 employés

dans le monde. Ses atouts : ses ingénieurs et développeurs. Ils sont plus de 3'500 dans le monde. Symantec dépend obligatoirement de normes très fonctionnelles, ouvertes et interoperables.

**Les gratuits**

McAfee offre pour sa part un processus de distribution de ses logiciels via Internet (home.mcafee.com), un site payant où plus de deux millions d'abonnés actifs seraient enregistrés. L'éditeur californien argue que ses produits sont soutenus par des organisations respectées dans le domaine de la recherche antivirus, comme McAfee AVERT. Celles-ci protègent les clients McAfee des attaques de virus les plus récentes et les plus complexes. Sachez aussi qu'il existe des logiciels gratuits tels qu'avast, Antivir, AVG, Microsoft Security, Comodo, Secuser.com, etc. Tous sont efficaces, mais à un moment donné, certains deviennent payants pour avoir davantage de protection. (rke) 