

Propos rassurants des uns, discours alarmistes des autres, sans oublier la dernière marotte des journalistes: la sécurité sur Internet est un sujet complexe.

Sécurité sur Internet: vrais et faux problèmes

Si le problème est bien réel, la sécurité sur Internet ne doit ni être un sujet tabou ni une affaire de spécialistes. Il convient d'informer correctement les acteurs et les utilisateurs sur la réalité des dangers.

PASCAL THONIEL



PASCAL THONIEL

PDG de NTX Research, société spécialisée dans la sécurité réseau des systèmes d'information.

C'EST À PARTIR de cette prise de conscience générale que l'on peut mettre en œuvre une politique de sécurité claire et efficace. Internet est un gigantesque système d'information ouvert à l'échelle de la planète. C'est en quelque sorte une ressource commune dont la conception, la gestion et l'utilisation sont partagées. Internet est donc à la disposition de tous pour le meilleur... comme pour le pire.

Dans ce contexte, on peut dire qu'Internet pose des problèmes de sécurité. L'importance de la sécurité est la conséquence directe du succès d'Internet, de son déploiement et de la multiplicité de ses applications. En général, les problèmes de sécurité sont toujours liés aux enjeux et cela est aussi vrai pour Internet. A l'origine, on trouve les accidents, les erreurs (par incompétence ou par maladresse) ainsi que la malveillance. A la malveillance, par exemple, les enjeux peuvent

être définis comme un gain potentiel obtenu en cas d'attaque.

Peut-on sécuriser Internet?

De même qu'il est possible de sécuriser et de protéger un système d'information d'entreprise, il existe des solutions pour sécuriser et protéger Internet – à condition bien sûr de concevoir et de mettre en œuvre une véritable politique de sécurité suivie dans le temps. Cette politique doit s'appliquer aux informations elles-mêmes mais aussi au système informatique qui les supporte (infrastructure). Il est cependant faux de penser qu'il existe ou qu'il existera une solution universelle de sécurité pour Internet.

D'abord, parce que le système couvre toute la planète et qu'une réglementation mondiale est illusoire. Ensuite, parce qu'Internet est à la fois multiforme et terriblement complexe avec de nombreux acteurs et utilisateurs aux intérêts divergents qui interagissent entre eux. Enfin, par-

ce qu'Internet est un système qui évolue sans cesse. Impossible donc de mettre Internet dans une bulle surtout si les attaques peuvent aussi venir de l'intérieur.

Alors... Vrai ou faux?

► *Les virus, mythe ou réalité?*

Réalité. Les virus informatiques existent bel et bien. Ils s'en créent de nouveaux chaque jour même si ce ne sont bien souvent que des variantes des grandes catégories existantes. Les attaques virales sont souvent systématiques, aveugles et la contamination se diffuse rapidement sur Internet.

► *Les logiciels anti-virus sont des moyens de protection efficaces.*

Vrai. Les grands éditeurs de logiciels anti-virus utilisent des réseaux pour détecter rapidement toute nouvelle apparition de virus sur la toile et «fabriquent» les parades nécessaires. Le vrai problème réside plutôt dans l'administration de ces logiciels à grande échelle. Une fois votre solution anti-virus correctement déployée (c'est-à-dire de ma-

Les ruses sont nombreuses et les victimes crédules. Une fois mis en place, le cheval de Troie permet à l'attaquant de prendre ni plus ni moins le contrôle de votre machine!



nière exhaustive), il est nécessaire de mettre à jour régulièrement vos bases virales (les fameuses parades) disponibles chez l'éditeur sous peine de devenir rapidement vulnérable.

► *Les éditeurs de logiciels anti-virus fabriquent leurs propres virus pour mieux vendre leurs solutions.*

Faux. L'imagination, l'inventivité et l'activité débordante des créateurs de virus est largement suffisante pour occuper à temps plein toutes leurs équipes de recherche.

► *Les chevaux de Troie, mythe ou réalité?*

Réalité. Ces armes logiques sont redoutables. Toute la difficulté pour l'attaquant est d'arriver à implanter à votre insu ces points d'accès illicites à l'intérieur de votre système. Les ruses sont nombreuses et les victimes crédules lorsqu'elles ne sont pas bien informées. Une fois mis en place, le cheval de Troie permet à l'attaquant de prendre ni plus ni moins le contrôle de votre machine!

► *Il est facile de se protéger à*

l'avance contre les attaques par saturation (deni de service).

Faux. Les attaques par saturation sont concertées et de multiples attaquants font converger leurs efforts sur une même cible. Avec des moyens convenables, la réussite de l'opération est presque garantie. La solution réside dans la détection et le diagnostic rapide de ce type d'attaque afin de mettre en œuvre immédiatement des ressources de remplacement. Dans ces conditions, la gêne est de courte durée pour les utilisateurs légitimes.

► *Le firewall protège mon réseau interne de l'Internet...*

Vrai. Le firewall est un poste de contrôle qui opère un cloisonnement des réseaux. Il est l'agent central de la sécurité des réseaux informatiques. Concrètement, le firewall est une ressource matérielle et logicielle possédant des interfaces de communication: généralement un ordinateur est équipé de cartes réseau et sur lesquels s'exécute un logiciel de contrôle des flux informatiques. Le firewall ou garde-barrière se place entre un réseau privé d'entreprises et un réseau public ou entre deux réseaux privés au sein d'une même entreprise. Le garde-barrière contrôle les données entrantes et sortantes du réseau privé d'entreprise vers les autres réseaux extérieurs. Suivant les règles de sécurité établies au sein du réseau privé de l'entreprise, le garde-barrière filtre les entrées-sorties et ne laisse passer que celles qui ont été autorisées.

► *... je peux donc dormir tranquille.*

Attaques possibles et fonctions de sécurité

CINQ sortes d'attaques ont été retenues:

1. Attaque par saturation provoquant un déni de service (limitation de la capacité du système informatique à pouvoir être utilisé dans de bonnes conditions);
2. Accès non autorisé aux ressources du système limitant l'accès des données aux personnes et aux processus autorisés (authentification, contrôle d'accès et confidentialité);
3. Attaque sur l'intégrité des données et des processus limitant le système à permettre la modification des données par les

- personnes ou par le processus habilités;
4. Attaque par répudiation (négation) des actions effectuées limitant le système à prouver que des actions ou des transactions ont bien eu lieu, à des fins de traçabilité, de preuve, de contrôle ou d'audit;
5. Attaque sur la continuité, la durabilité, la fiabilité, la convivialité et la sûreté de fonctionnement du système informatique qui limite la capacité de ce système à exécuter les actions et à rendre les services que l'on attend de lui dans des conditions de performance et d'utilisation adéquates, tout au long de sa durée de vie. ■

Si vous souhaitez payer vos achats en ligne, assurez-vous que le site marchand accepte bien le paiement par carte bancaire protégé par le protocole sécurisé SSL (Secure Socket Layer).

Faux. Le firewall est une pièce maîtresse de la sécurité des réseaux comme la Reine peut l'être pour le jeu d'échec. Cependant, le firewall ne peut constituer à lui tout seul une protection suffisante comme il est quasiment impossible de gagner une partie d'échecs sans se servir intelligemment des autres pièces. Placé aujourd'hui au centre de l'intérêt médiatique, le firewall est considéré parfois par certains décideurs comme une solution miracle aux problèmes de sécurité informatique. Il est essentiel pour les responsables de la sécurité de donner à cet outil sa juste valeur et d'en faire prendre conscience aux principaux intéressés. Rien n'est plus dangereux en effet de se croire en sécurité retranché derrière une défense en forme de «ligne Maginot». Il est également illusoire de penser que l'achat d'un firewall et sa mise en route procèdent d'une promenade de santé. L'architecture du firewall et sa place au sein des réseaux doivent être mûrement réfléchies et le paramétrage de ses règles effectué avec soin, le tout conformément à la politique de sécurité choisie.

► *Les écoutes de ligne sont monnaie courante sur Internet et sur les réseaux.*

Vrai. Les sondes, les analyseurs de trafic et les logiciels renifleurs permettent de «photographier» toutes les données qui transitent sur les réseaux, Internet compris. Ces logiciels sont faciles à mettre en place, quasiment indétectables et faciles à utiliser. Ils permettent de récupérer les identifiants, les mots

de passe et autres codes d'accès envoyés par les utilisateurs légitimes circulant des postes clients aux serveurs. Il en est de même si vous communiquez votre numéro de carte bancaire sur Internet. Ces logiciels sont équipés d'analyseurs syntaxiques et de filtres capables de trier les informations intéressantes (par exemple les seize chiffres de votre carte bancaire) parmi les flots de données.

► *Les gouvernements, les puissantes organisations privées et le crime organisé sont impliqués dans la guerre électronique de l'information.*

Vrai. Les enjeux de la maîtrise de l'information sont considérables, ce qui implique un avantage décisif pour celui qui en possède la clé avant les autres.

► *Je suis impliqué et menacé directement par cette guerre.*

Faux. A moins que vous ne représentiez à vous seul un enjeu considérable pour un de ces acteurs majeurs, vous ne risquez rien car vous ne présentez pas d'intérêt réel et vos informations personnelles seront noyées dans la masse. Mais rien ne vous empêche d'appliquer les consignes simples de sécurité pour être à l'abri d'accidents et de banales tentations.

► *La technique cryptographique protège efficacement mes informations.*

Vrai. Certains algorithmes de chiffrement de données sont à la fois sûrs, solides et la longueur des clés secrètes utilisées suffisantes.

► *La longueur des clés symétriques de 128 bits (seize caractères) est insuffisante.*

Faux. Aujourd'hui et pour les

vingt années à venir, cette longueur de clé sera suffisante pour empêcher une attaque par le test exhaustif de toutes les clés possibles (attaque dite à force brute). A moins que les ordinateurs quantiques ou biologiques ne voient le jour d'ici là...

► *La sécurité sur Internet est une affaire de technique et de techniciens.*

Faux. C'est avant tout une affaire de méthode, de clarté, d'information et de formation des utilisateurs. Ce ne sont pas les outils de sécurité qui manquent mais leur adéquation au problème posé, la qualité de leur implémentation et de leur administration engendrant des contraintes et donc des failles.

La sécurité du paiement en ligne est relative

Pour terminer, voici un sujet qui nous regarde tous personnellement: le commerce électronique grand public et le paiement en ligne qui sont globalement sûrs.

Ceci est en partie vrai pour le commerce électronique, mais pas pour le paiement en ligne. A savoir: si vous souhaitez payer vos achats en ligne, assurez-vous que le site marchand accepte bien le paiement par carte bancaire, protégé par le protocole sécurisé SSL (Secure Socket Layer). Etablissez automatiquement une liaison sécurisée SSL de votre navigateur vers le site Web marchand et communiquez votre numéro de carte bancaire qui sera alors chiffré pendant sa transmission. C'est à la fois simple et efficace. Mais le consommateur/payeur est-il effectivement

La vérité est que les plaintes se multiplient et que les trois-quart de ces plaintes portent sur l'utilisation abusive de numéros de cartes bancaires sur Internet.

bien protégé? Certains détracteurs vous diront que le chiffrement opéré sur le numéro de carte bancaire est insuffisant compte tenu de la longueur maximale des clés limitées aujourd'hui à quarante bits (cinq caractères). Je rappellerai à toutes fins utiles que les décrets d'application concernant l'extension de cette limite à 128 bits (seize caractères) ne sont pas encore parus au journal officiel. Ils ont raison car un test exhaustif de l'ensemble des clés «quarante bits» possibles est plutôt facile à mettre en œuvre et permet ainsi de décrypter le message. Pourtant, c'est un faux problème car il suffira d'étendre effectivement la longueur des clés autorisées et d'utiliser un algorithme de chiffrement sûr pour déjouer les attaques par l'écoute de ligne... Alors où est le problème? Le problème est que les commerçants en ligne et leurs banques acceptent aujourd'hui des paiements par cartes bancaires sans exiger la signature manuscrite (ce qui est bien normal sur Internet), le code confidentiel ou le code PIN (ce qui est beaucoup plus grave). En effet, cela veut dire qu'un numéro de carte bancaire valide, quel qu'il soit, est un sésame suffisant pour vous ouvrir toutes grandes les portes du paiement. Or tout le monde sait qu'un numéro de carte bancaire n'est plus un secret. Il existe toutes sortes de moyens pour se le procurer:

- Par écoute de ligne bien sûr mais aussi et surtout...
- Par de petits logiciels capables de générer des numéros valides (en téléchargement

libre et gratuit sur Internet aux bonnes adresses);

► Par la récupération en masse des bases «client» des grands sites marchand où sont enregistrés les numéros (ce type d'attaque a déjà touché les grands noms du commerce en ligne et ce sont quelques centaines de milliers de numéros qui circulent désormais dans la nature sans le contrôle de leur propriétaire légitime);

► Par des filières classiques: de petits délinquants qui récupèrent les factures avec la complicité de caissiers indelicats (la police est effrayée par l'importance de ce trafic).

Donc, s'il vous est facile de payer en ligne avec votre numéro de carte bancaire, vous comprendrez aisément qu'il est tout aussi facile pour quelqu'un de malhonnête qui utilise un numéro valide et peut-être, pourquoi pas le vôtre! En fait, le système «SSL/carte bancaire» n'authentifie pas le possesseur de la carte: à l'autre bout du réseau n'importe qui peut se faire passer pour le détenteur légitime de la carte à l'autre bout du réseau... Dernier argument parfois invoqué pour rassurer notre consommateur/payeur: la législation vous protège. En cas de problème, vous disposez de quelques jours pour dénoncer un achat auquel vous n'avez pas pris part, votre compte est recredité et tout le monde est content. C'est la loi. La réalité est plus terre à terre: la plupart des gens ne tiennent pas une comptabilité stricte d'où la porte ouverte à de nombreux abus avant de s'en apercevoir, mais trop tard. D'autre part, les banques

ne facilitent pas forcément les procédures de dénonciation des transactions, loin s'en faut, c'est même plutôt le parcours du combattant. La vérité est que les plaintes se multiplient et que les trois-quart de ces plaintes portent sur l'utilisation abusive de numéros de cartes bancaires sur Internet. Si vous n'en entendez pas encore parler c'est que le paiement en ligne est encore peu développé. Qu'en sera-t-il alors? Pour les numéros valides qui n'appartiennent à aucun compte réel, ne vous réjouissez pas trop vite car les impayés des commerçants en ligne vous seront bientôt refacturés sur les prix à vous, bons payeurs. En tout état de cause, tant que le consommateur/payeur ne pourra pas véritablement s'authentifier lors de la transaction, le risque est bel et bien présent.

Existe-t-il des solutions?

Les solutions sûres existent, mais elles ne sont pas forcément celles que l'on veut nous faire croire et elles ne sont peut-être pas aussi faciles à mettre en œuvre qu'on le prétend. Gardons-nous enfin de croire que des solutions universelles vont venir régler tous les problèmes de sécurité comme par enchantement. Premièrement, parce que vous n'aurez jamais le temps de les déployer sur l'ensemble d'Internet et qu'il y aura toujours une brèche qui permettra à des petits malins de passer. Deuxièmement, parce qu'Internet est un système en perpétuelle évolution et qu'on ne peut sécuriser et protéger qu'un système statique. ■