



Menaces et vulnérabilités de 2009

Pour plus de sécurité, adoptez les réflexes CASES !

Enquête réalisée auprès de plus de 60 experts en sécurité de 16 pays

Automne 2009. Plus de 150 experts en sécurité et hackers du monde entier se réunissent à Luxembourg. Une occasion de les interroger sur les plus grosses failles et menaces de 2009. Les résultats sont étonnants. Ils mettent l'accent sur les applications actuelles et les utilisateurs.

Les médias ne cessent de parler des risques sur Internet, sur l'ordinateur et dans le réseau. Mais qu'est-ce qu'un risque ? Comment le terme se définit-il ? Si on suit attentivement le cours dans une classe de troisième, le risque se définit par une équation : $\text{risque} = \text{point faible} \times \text{danger} \times \text{conséquence}$.

L'enseignante s'efforce d'expliquer cela aux enfants en établissant des analogies avec la vie réelle : la clé cachée sous le paillason constitue un point faible ; le voleur est le danger ; les objets de valeur volés ou endommagés sont les conséquences possibles.



De façon générale, il est malheureusement difficile d'agir seul contre le danger « voleur ». Mais il en va tout autrement pour les vulnérabilités. Une clé de maison ne se cache ni sous un paillason ni sous un pot de fleurs. Cela augmente énormément le risque de cambriolage car les voleurs connaissent les soi-disant cachettes. L'analogie avec la clé et le voleur permet de faire comprendre aux internautes que connaître les vulnérabilités et les menaces d'Internet contribue à réduire les risques.

Pour qu'un utilisateur puisse réduire son risque d'être victime d'attaques, il convient de s'interroger sur les grands dangers et les principaux

vulnérabilités du monde numérique cette année.

Les principaux dangers de 2009

Les participants de la conférence sur la sécurité hack.lu qui se tient chaque automne à Luxembourg travaillent comme physiciens, ingénieurs de logiciels, informaticiens, testeurs de systèmes de sécurité, policiers, professeurs, chercheurs ou consultants en sécurité de l'information.

Ils viennent du Luxembourg et des pays limitrophes, mais également de contrées aussi lointaines que les États-Unis ou l'Inde. Ils ont une chose en commun : ils s'occupent tous des vulnérabilités et des

dangers du monde numérique ainsi que des conséquences possibles des attaques. CASES, le portail luxembourgeois de la sécurité de l'information du Ministère de l'Économie et du Commerce extérieur, a donc demandé leur avis de spécialiste sur les plus grands dangers de 2009.

« Les vulnérabilités de 2008 et des années précédentes continuent de représenter un danger important. La plupart de ceux-ci ne sont pas encore éliminés. Les cybercriminels les exploitent toujours », explique un chercheur français. Les experts en sécurité et les hackers insistent en effet souvent pendant des mois, voire des années, sur les failles des programmes et systèmes sans être entendus. Si des solutions sont mises à disposition par l'industrie, l'utilisateur final est le maillon faible suivant de la chaîne. Connaît-il le point faible ? L'utilisateur appliquera-t-il la solution proposée pour supprimer le point faible ? Il faut malheureusement souvent répondre par la négative à ces questions.

L'ordinateur et Internet sont complexes. Les cybercriminels travaillent avec des astuces et ruses, ce qui peut rapidement dépasser un internaute. Les experts en sécurité en sont conscients. Mais un expert sur trois estime que l'utilisateur lui-même était le plus gros danger en 2009.

Point faible du côté d'Internet : les experts en sécurité accusent les nombreux sites Internet mal développés. Ceux-ci offrent aux cybercriminels une foule de vecteurs d'attaque. C'est pourquoi le portail luxembourgeois de la sécurité de l'information CASES met un guide à la disposition des entreprises, organisations, associations et tout site Internet. Cette publication reprend les exigences de sécurité minimales pour un site Internet. Le guide contenant des check-lists est disponible sur www.cases.lu, rubrique Publications / Dossiers sous le nom « Référentiel de sécurité pour applications web ».

Manque de masquage ou de vérification des métadonnées. Les sites Internet présentant des failles au niveau des champs de saisie sont facilement victimes d'injections SQL. Les criminels tentent d'intégrer leurs propres commandes de base de données via l'application donnant accès à cette base de données pour prendre le contrôle sur le serveur, par exemple.

Les téléphones mobiles, des appareils polyvalents aux nombreuses vulnérabilités. L'iPhone est devenu très populaire. Ses propriétaires sont intéressés par les nombreuses applications et l'accès pratique à Internet offert par cet appareil. Mais les applications ne manquent pas de failles de sécurité. Les utilisateurs doivent savoir que plus le nombre d'utilisateurs d'un logiciel ou d'un appareil spécifique est grand, plus il est intéressant pour les criminels d'exploiter une faille. Les experts en sécurité conseillent donc de se tenir au courant des failles de sécurité de l'iPhone et de mettre régulièrement à jour les programmes. Ceci est d'ailleurs également vrai pour les appareils similaires.

Son journal intime sur le Net. Un expert en sécurité suisse avertit aussi les membres de Twitter : « Certains utilisateurs détaillent leur emploi du temps sur cette application. Ils pensent que cela n'intéresse personne de toute façon. Ils se trompent lourdement : les voleurs de données et les cambrioleurs sont leur premier public. »

Le fumeur, un point faible ? Les experts présentent aux entreprises une faille de sécurité simple mais très concluante et dangereuse : « les fumeurs ». « Ils sortent pour fumer en laissant la porte ouverte », explique un expert. Des tiers ont ainsi facilement accès aux bâtiments d'une entreprise.

Un fournisseur de solutions de sécurité explique à ce sujet :

d'utilisateurs pensent que ça ne peut arriver qu'aux autres ! Ils ne pensent pas être une cible intéressante. Cette

mauvaise évaluation de la situation réelle et l'ignorance génèrent de grosses vulnérabilités du côté de l'utilisateur qui devient ainsi un danger général. » « Des formations continues des utilisateurs sont nécessaires. Les utilisateurs évitent ainsi de cliquer aveuglément sur tout ce qui bouge et ne téléchargent pas de logiciels inconnus sur leur ordinateur », ajoute un autre expert. « La naïveté des utilisateurs ouvre grand la porte aux cybercriminels pour un vaste spectre de formes d'attaque à la fois bon marché et lucratives comme le phishing ou le vol d'identité », conclut un autre participant.

Un expert sur quatre incrimine les données publiées sur Internet. Les réseaux sociaux, un danger ? Oui, répondent les experts. Ils sont inquiets car la divulgation volontaire d'informations personnelles dans des réseaux sociaux facilite le vol d'identité. Personne ne peut encore dire quelles répercussions un dossier numérique établi sur 50 ou 60 ans aura sur la vie d'un utilisateur. Les utilisateurs doivent en général être prudents et vigilants avec la publication de données privées.

Le classement des autres dangers

12 experts réagissent aux lois sur l'obligation pour les entreprises de conserver des données pendant une certaine période et aux tentatives d'interdire certains contenus d'Internet aux utilisateurs. Ils parlent de leur crainte d'une censure possible d'Internet et des traces de données numériques de l'utilisateur. Ce qui était imaginé à l'origine pour protéger l'utilisateur pourrait se retourner contre lui à l'avenir.

Plusieurs experts citent aussi les vulnérabilités des programmes actuels. Ils pensent notamment aux applications comme Flash qui permettent de réaliser des graphiques et animations ou au format de fichier universel PDF d'Adobe. Tous deux se trouvent sur pratiquement tous les ordinateurs. Ne pas mettre ces programmes régulièrement à jour revient à donner aux cybercriminels une clé pour placer des logiciels malveillants sur l'ordinateur.

Mais les experts considèrent aussi les grandes entreprises et leurs applications comme des menaces. « Google occupe une position de monopole des moteurs de recherche sur Internet. Si aucun concurrent de taille n'arrive, il pourrait bientôt couvrir 100 % du marché. Les monopoles ne favorisent généralement pas les évolutions », argumente un universitaire luxembourgeois. « Comme Google continue

de s'étendre, ce moteur de recherche et l'entreprise qui se cache derrière auront bientôt le contrôle sur tout l'Internet et sur ses utilisateurs », commente un professeur de l'Université du Luxembourg.

Même les systèmes d'exploitation Windows et leurs failles sont cités par quelques experts. Un informaticien spécialisé dans les tests logiciels classe les systèmes d'exploitation comme suit : Windows 7 suivi de Vista et XP. Mais attention, même les systèmes d'exploitation d'Apple et Linux comportent des failles. Les utilisateurs qui pensent être à l'abri avec ces systèmes se trompent. Ce faux sentiment de sécurité constitue précisément une grande menace car les utilisateurs négligent les réflexes de sécurité. Le directeur d'un département de recherches déclare : « La sécurité n'est pas inhérente au produit mais commence dans la tête des utilisateurs. »

D'autres experts en sécurité citent au rang des menaces le vers Conficker et, de façon générale, les vers propagés par les e-mails. Les mots de passe préconfigurés par défaut, dans les routeurs par exemple, sont également mentionnés. Les chevaux de Troie qui permettent un accès direct à l'ordinateur d'un utilisateur ou les injections SQL qui permettent l'exploitation des failles de

sécurité en relation avec des bases de données SQL font partie comme en 2008 des plus grandes menaces de l'année 2009.

Recherche des principales vulnérabilités de 2009

Experts et utilisateurs se posent la même question : quel sera le plus grand point faible lié à l'ordinateur et Internet cette année ? Les participants à la conférence hack.lu qui citent ensemble plus de 25 vulnérabilités importantes pointent à l'unanimité le point faible « navigateur Internet ».

Les petits programmes comme Mozilla Firefox, Internet Explorer ou Opera servant à visualiser des sites web ou des documents et données représentent un point faible de taille. Les

erreurs de programmation dans ces logiciels et leurs plug-ins offrent de nombreux angles d'attaque aux criminels. Les plug-ins sont des programmes informatiques qui s'intègrent dans le navigateur pour étendre ses fonctionnalités.

Mais ce point faible est suivi de près par l'utilisateur. Déjà classé parmi les plus grandes menaces, les experts sont unanimes ici aussi. « Notre esprit n'est pas conscient de la complexité des applications que nous utilisons tous les jours. Au lieu de nous informer, nous préférons masquer les avertissements et messages de sécurité » commentent un expert en sécurité français et son homologue suisse.

En troisième position, les experts citent les failles du protocole réseau SSL,

Secure Sockets Layer, utilisé pour le transfert des données en toute sécurité. « SSL est une infrastructure de sécurité importante d'Internet. Des certificats faux mais valables aux yeux des utilisateurs peuvent compromettre le commerce électronique. Ils permettent les attaques de type Man-in-the-middle », argumente un testeur de logiciels allemand. Le criminel se trouve ici entre les deux partenaires de communication. Il a le contrôle total du trafic de données entre deux ou plusieurs participants du réseau qui ne sont pas conscients de sa présence. Le criminel peut visualiser et manipuler à l'envi les informations. Il peut se faire passer pour leur interlocuteur auprès des partenaires de la communication.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu