



Votre intervention compte

Pour plus de sécurité, adoptez les réflexes CASES !

Installez vous aussi un portier : le firewall

Les médias ne cessent de le rappeler : des milliers voire des millions d'ordinateurs privés sont entre les mains de tiers malintentionnés.

1 656 227 nouveaux programmes malveillants rien qu'en 2008. Comment couper l'herbe sous le pied des criminels ? C'est très simple. De plus en plus de propriétaires d'ordinateur sont bien informés et ne permettent pas à leur ordinateur de mener une vie propre. Un portier les y aide : le firewall.

À votre avis, combien valez-vous pour les cybercriminels ? Pascal Steichen, collaborateur de CASES et intervenant dans la mise au point de méthodes et instruments nationaux pour analyser et bloquer les cyberattaques, connaît la réponse : « Les informations sur les cartes de crédit se négocient entre 0,06 et 30 dollars sur le marché de la cybercriminalité. Les données d'accès aux comptes sont bien plus chères, entre 10 et 1 000 dollars. Les informations qui permettent l'accès au compte e-mail d'un utilisateur varient entre 0,10 et 100 dollars et les données relatives à l'identité d'une personne peuvent aller jusqu'à 60 dollars. Les bons clients bénéficient naturellement d'une remise », ajoute-t-il.

Jamais auparavant un nombre aussi important d'utilisateurs n'a pu accéder à tant d'informations. Chacun, où qu'il soit sur Terre, peut apporter sa contribution à cette société de la connaissance. Les services dans des domaines tels que la santé, l'économie, l'État, la formation, les loisirs sont à notre portée en un simple clic. Internet compte plus d'un milliard d'utilisateurs. Cet immense potentiel doit-il tomber entre les mains de cybercriminels ? Faut-il se



résoudre à surfer sur Internet la peur au ventre ?

Le modèle économique des pirates semble avoir le vent en poupe tant leur intérêt pour les ordinateurs des utilisateurs et leurs informations personnelles est grand. Le chantage, l'espionnage industriel ou le terrorisme pour détruire les structures publiques ou les services économiques font aussi partie des machinations criminelles. Attirés par des gains qui se comptent en millions, les cybercriminels sont structurés à la manière d'une profession, actifs dans le monde entier et bien cachés derrière les ordinateurs kidnappés d'utilisateurs privés. Il est légitime de se demander combien de temps nous accepterons encore d'exposer nos ordinateurs aux accès non autorisés et au détournement à des fins criminelles.

De plus en plus d'utilisateurs développent des réflexes de protection, coupant ainsi l'herbe sous le pied des cybercriminels. Les pirates

tendent toutefois de mettre en place leur modèle économique en toute discrétion via des logiciels malveillants de plus en plus sophistiqués. Le firewall est un outil offrant aux utilisateurs une bonne protection contre les cybercriminels.

Un portier au service de l'utilisateur

La présence d'antivirus mis à jour régulièrement se généralise sur les ordinateurs luxembourgeois. Les utilisateurs comprennent le fonctionnement de ce programme et maîtrisent son application, pour le plus grand plaisir des formateurs du portail luxembourgeois de la sécurité de l'information CASES.

« Une protection non comprise et non maîtrisée est inefficace. Si on ne comprend pas la raison d'attacher sa ceinture en voiture ou si on ne sait pas comment l'attacher, on ne sera pas en sécurité dans la voiture malgré la présence de la ceinture. Ceci est également vrai pour Internet. C'est

pourquoi nous sommes très satisfaits de voir de plus en plus d'enfants, âgés même de neuf ou dix ans, connaître le fonctionnement et l'utilisation d'un antivirus. Ce n'était pas le cas il y a à peine deux ans », explique Monsieur Steichen.

L'expert en sécurité espère un succès semblable auprès des utilisateurs pour un deuxième programme de protection indispensable à tout ordinateur, le firewall. « Les cybercriminels tentent de pénétrer dans votre ordinateur. S'ils y parviennent, ils seront bien cachés. Ils observeront vos faits et gestes, seront à l'affût des informations pouvant être monnayées. Pendant que vous surfez sur Internet avec votre ordinateur, les pirates se serviront en outre de la puissance de calcul de votre machine à des fins criminelles. Un va-et-vient de données et de programmes se produira sur votre ordinateur. En tant que profane, vous ne remarquerez rien », ajoute M. Steichen sur le professionnalisme des pirates.

« Mais si l'ordinateur d'un utilisateur dispose d'un antivirus et d'un firewall, la tâche des pirates sera plus ardue. La fonction d'un firewall est comparable à celle d'un portier », explique M. Steichen. Tout le monde ne peut pas entrer et tout le monde ne peut pas sortir : c'est précisément ainsi que vont les choses avec un firewall. Ce ne sont toutefois pas les personnes qui sont contrôlées, mais les programmes et les données. Tous les logiciels ne peuvent accéder à votre ordinateur depuis Internet et tous les programmes ne peuvent pas quitter votre ordinateur à destination d'Internet ! Une protection simple mais efficace que les enfants luxembourgeois participant aux formations CASES découvrent dès la troisième année d'école. Pour que le portier puisse décider qui peut entrer ou sortir du bâtiment, il doit savoir quelles personnes disposent de quels droits ou qui est digne de confiance. Sinon, il n'y aurait pas de protection malgré la présence du portier. Ceci est également valable pour le firewall. Il faut donc veiller à ce que le celui-ci soit correctement configuré.

Est-il possible d'avoir une protection suffisante sans firewall ?

Les attaques d'utilisateurs ont essentiellement eu lieu via des sites Internet en 2008. Les pirates exploitent les faiblesses des sites courants. La société Symantec active dans le domaine de la sécurité de l'information a pu identifier 12 885 sites Internet compromis en 2008. Si un utilisateur visite un de ces sites, les criminels tentent de télécharger des logiciels malveillants sur son ordinateur et de prendre le contrôle de la machine sans que l'utilisateur ne remarque rien. Les pirates échouent rarement en raison du manque de connaissances, du manque de fonctions de protection et des points faibles existants.

Trois chevaux de Troie et deux vers figuraient en 2008 au top 10 des familles de nouveaux programmes malveillants dangereux. Une fois installé sur l'ordinateur d'un utilisateur, un cheval de Troie ouvre une porte de l'ordinateur de l'utilisateur vers Internet. Les données et programmes peuvent alors aller et venir sur l'ordinateur infecté dans que l'internaute ne remarque rien. L'utilisateur n'est plus le maître de sa machine.

Les vers sont également sans merci comme l'a prouvé récemment Conficker. S'il est installé sur l'ordinateur via un point faible de

celui-ci, ce ver se propage de lui-même à partir de cette machine, prend contact avec d'autres ordinateurs, permet la prise de contrôle de la machine par des tiers et désactive seul les mécanismes de protection de l'ordinateur infecté.

Un firewall correctement configuré évite que des programmes s'installent sur l'ordinateur ou accèdent à Internet à partir de la machine. Il met ainsi fin aux agissements des vers et chevaux de Troie. Comme une voiture sans freins, une protection suffisante d'un ordinateur n'est pas pensable sans firewall.

Importance de la compréhension de base du mécanisme de protection

Tous les systèmes d'exploitation actuels possèdent un firewall de base. Sur Windows Vista et Ubuntu GNU/Linux, ce firewall est déjà automatiquement activé. Les utilisateurs de Windows XP, par exemple, peuvent activer ce firewall en quelques clics, via Démarrer, Contrôle du système, Centre de sécurité, Firewall.

Les utilisateurs doivent cependant savoir que ce firewall de base n'analyse que les données entrantes.

Conseil de sécurité : vérification de sécurité et firewall gratuit

Un ordinateur peut être comparé à un immeuble de bureaux avec 65 535 portes, appelées « ports ». Comme les portes de bureau, chaque port possède son propre numéro. Des informations peuvent entrer dans l'ordinateur ou en sortir vers Internet via chacun de ces ports. Les cybercriminels tentent d'obtenir l'accès à l'ordinateur d'un utilisateur via les ports. Un firewall correctement configuré complique ces tentatives d'intrusion.

Un firewall est donc devenu indispensable sur un ordinateur, au même titre que l'antivirus. À cet effet, l'industrie met même à la disposition des utilisateurs privés des firewallx gratuits. La société Zonealarm propose gratuitement à l'utilisateur privé son firewall du même nom sur le site www.zonealarm.com. Il suffit de cliquer sur « Télécharger et acheter » et ensuite sur « Téléchargements gratuits ». Les utilisateurs doivent se familiariser avec la fonction de protection du firewall pour garantir une protection optimale à leur ordinateur.

Définition : firewall

Un firewall est un dispositif physique (matériel) ou logique (logiciel) servant de système de protection pour un ordinateur ou un réseau informatique. Il permet de bloquer et de traquer les attaques ou connexions suspectes pouvant être utilisées pour propager des vers ou chevaux de Troie. Il permet aussi d'empêcher la transmission incontrôlée de données vers l'extérieur.

Ce modèle simple ne surveille pas les données sortantes. C'est comparable à un portier qui ne contrôlerait que les personnes désirant entrer dans le bâtiment mais pas celles qui le quittent.

L'utilisation d'un firewall nécessite une compréhension de base de la part de l'utilisateur. C'est la condition pour garantir une protection optimale. L'utilisateur doit commencer par dire

au firewall quels programmes bénéficient de quels droits d'accès. Ensuite, le firewall informera l'utilisateur lorsqu'il rencontrera un comportement de programme inhabituel sur l'ordinateur ou des demandes d'accès de programmes. L'utilisateur doit alors décider s'il autorise l'accès d'un programme sur Internet, par exemple.

« Le manque de compréhension de base de ce mécanisme de protection entraîne des erreurs de paramétrage et de mauvaises décisions de la part de l'utilisateur. Le résultat est un faux sentiment de sécurité. Les utilisateurs doivent donc se familiariser avec cette fonction de protection. Cela évitera à l'ordinateur de vivre sa propre vie », conclut M. Steichen.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu