



CASES articles

Un pare-feu permet de bloquer les attaques ou les connexions suspectes

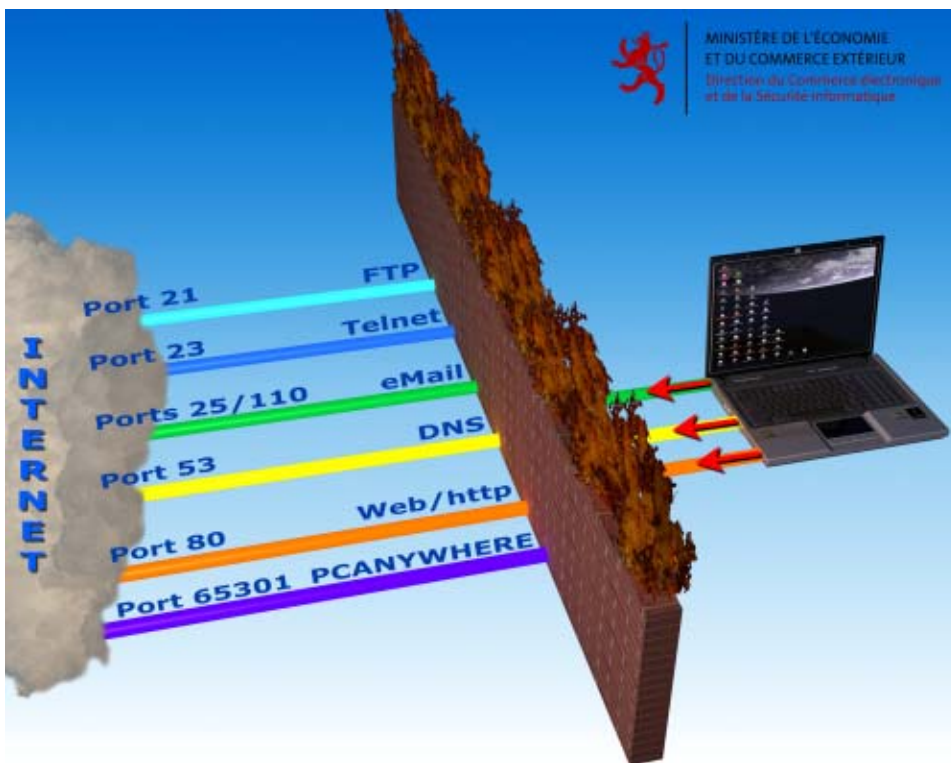
Les ordinateurs sans pare-feu peuvent être piratés en quelques minutes

Pour plus de sécurité, adoptez les réflexes CASES !

Simple et efficace – Un pare-feu correctement paramétré fait partie des règles d'or de la sécurité informatique

Surfer sur Internet soumet l'ordinateur à toute une série de tentatives illicites d'accès par des cybercriminels. Les pirates tentent ainsi de manipuler la machine afin d'en obtenir le contrôle. Une étude réalisée dès 2004 par le quotidien USA Today, en collaboration avec la société de technologie Avantgarde, a démontré qu'un ordinateur sous Windows, non protégé par un pare-feu, est attaqué en moyenne toutes les dix secondes depuis Internet. Ce nombre important d'attaques permet de mieux comprendre l'absolue nécessité de l'utilisation de mécanismes de protection sur un ordinateur, en particulier d'un pare-feu. Un pare-feu correctement paramétré permet de bloquer les attaques dirigées contre l'ordinateur ou les connexions suspectes. Les systèmes d'exploitation Windows, MAC et Ubuntu disposent d'un pare-feu basique intégré. Les utilisateurs peuvent néanmoins avoir recours à une vaste gamme d'autres pare-feu, performants et conviviaux.

Un pare-feu établit un mur de protection autour de l'ordinateur. Il peut être constitué d'un logiciel ou d'un matériel et analyse les flux de données ainsi que les informations que ceux-ci contiennent. L'analyse de ces flux lui permet de bloquer les attaques dirigées contre un ordinateur ou les connexions suspectes pouvant être utilisées afin de propager des virus, vers ou chevaux de Troie. Un pare-feu de bonne qualité empêche éga-



lement la transmission incontrôlée de données de l'ordinateur vers l'extérieur.

Dès 2004, plus de 8000 attaques recensées par jour

Une étude réalisée par USA Today et Avantgarde dès 2004 a démontré qu'un ordinateur test sous Windows ne disposant pas de pare-feu subissait plus de 8000 attaques en une journée. Cet ordinateur test faisait office de leurre pour attirer les pirates et a été connecté à Internet sur une période de deux semaines. Pendant cette période, 9 attaques ont abouti, du point de vue du pirate. À chaque fois, les cybercriminels ont pu obtenir le contrôle de l'ordinateur. D'autres ordinateurs sous Windows, servant également de leurres pour les pirates, mais équipés d'un pare-feu basique, n'ont subi qu'un dixième de ces attaques quotidiennes. Les pare-feu basi-

ques installés sur ces machines procédaient à l'analyse des flux de données entrants. Au cours de la durée de l'étude, aucune des attaques menées sur les ordinateurs disposant d'un pare-feu basique n'a abouti.

Le fait qu'un ordinateur relié à Internet subisse une attaque quelques minutes seulement après la connexion, a également été établi dès 2004. Il s'agissait alors d'attaques aveugles, dont l'objectif était de détecter les points faibles de l'ordinateur – faiblesses liées par exemple à un système d'exploitation non mis à jour. À cet effet, les cybercriminels utilisent les adresses IP disponibles pour le grand-public. Ces adresses sont mises à disposition par les fournisseurs d'accès à Internet pour les connexions à large bande. Ces domaines d'adresses connus sont systématiquement scannés par les pira-

tes afin de détecter les ordinateurs vulnérables et d'en prendre le contrôle.

La rapidité et le nombre des attaques indiquent clairement que les cybercriminels travaillent avec des outils automatisés.

Dès qu'un pirate a réussi à prendre le contrôle d'un ordinateur, celui-ci est utilisé pour lancer des attaques contre d'autres PC. À l'insu de son propriétaire, l'ordinateur devient ainsi un robot télécommandé, également appelé « bot » ou zombie.

Pour des raisons d'efficacité, les cybercriminels se concentrent sur les ordinateurs disposant des systèmes d'exploitation les plus usuels lors de leurs attaques. Outre de nouvelles failles de sécurité, ils utilisent alors des faiblesses bien connues. Les pirates savent parfaitement que de nombreux usagers d'Internet ne procèdent pas à la mise à jour de leur PC et que leurs machines disposent de moyens de protection insuffisants. Les cybercriminels mettent les négligences des utilisateurs à profit, de manière ciblée.

Les pirates sont d'ailleurs en concurrence les uns avec les autres. Il a ainsi été constaté que les cybercriminels ayant réussi à prendre le contrôle d'un ordinateur en éliminent les points faibles initiaux, ce qui empêche leur détection par d'autres pirates. Les attaques des autres pirates, visant à prendre le contrôle de la machine, sont ainsi évitées.

Les données recueillies confirment qu'un système d'exploitation et des programmes actualisés ainsi qu'un pare-feu correctement paramétré sont indispensables pour la sécurité d'un ordinateur. L'installation et le bon paramétrage d'un pare-feu font ainsi partie des règles d'or de la sécurité informatique et doivent absolument être entrepris avant de connecter un ordinateur à Internet.

Comment fonctionne un pare-feu ?

« Un pare-feu fonctionne sur la base de règles définies par l'utilisateur. Dans ce cadre s'applique l'adage communément admis, disant que tout ce qui n'est pas expressément autorisé doit être interdit. Mais qu'est-ce que cela signifie ? En règle générale,

Exemple concret : étapes de la prise de contrôle d'un ordinateur par un pirate

En 2004, un ordinateur équipé du système d'exploitation Windows XP, mais ne disposant pas de pare-feu, a été relié à Internet via une connexion large bande. Ce PC devait servir de leurre pour attirer les pirates. La machine a ensuite été observée afin d'identifier les attaques, leurs modes opératoires ainsi que leurs répercussions. Les attaques ainsi que les différentes étapes ont été consignées par ordre chronologique dans un registre :

10:52:08

Moins de quatre minutes après le début du test, un des pirates réussit à s'introduire dans le PC équipé de Windows XP. Le point faible exploité est le même que celui utilisé par le ver SASSER au cours de sa propagation en mai 2004.

11:03:30

Onze minutes après l'intrusion du premier pirate, un second cybercriminel obtient l'accès à la même machine. Ce pirate utilise alors le même point faible que celui déjà exploité en juillet 2003 par le ver BLASTER.

11:04:04

Un troisième pirate lance une attaque. Il utilise un ordinateur infecté afin de s'introduire dans le PC sous Windows XP. Une nouvelle fois, c'est le point faible déjà exploité par le ver SASSER qui est utilisé.

20:21:44

Un peu plus de 10 heures plus tard, un quatrième pirate réussit à s'introduire dans l'ordinateur. Tout se passe bien pour ce cybercriminel : il commence le chargement de fichiers en utilisant des commandes upload et tente à plusieurs reprises d'établir une liaison avec un serveur. Le pirate est ainsi en mesure de se créer une interface conviviale lui permettant de transmettre ses ordres à l'ordinateur touché.

20:22:49

Le quatrième pirate réussit à intégrer l'ordinateur à un chatroom présent sur un serveur ; il dispose ainsi d'une interface lui permettant de transmettre facilement d'autres commandes à la machine corrompue.

20:23:05

Le cybercriminel prend le contrôle de l'ordinateur. Il tente d'accéder à une page Internet ; celle-ci est très probablement hébergée sur une autre machine, également manipulée par le pirate. Le but est de télécharger des malwares sur l'ordinateur cible.

20:23:11

La machine désormais sous contrôle du quatrième pirate commence à scanner Internet. Il est probable que cela soit lié au téléchargement et à l'installation des malwares mentionnés précédemment. Le but du scanning est de détecter d'autres ordinateurs vulnérables et de les corrompre. À cet effet, le pirate utilise les mêmes points faibles que ceux qui lui ont permis de prendre le contrôle de la première machine.

En moins de deux minutes, le quatrième pirate a réussi à prendre le contrôle de l'ordinateur test et à l'utiliser pour lancer des attaques contre d'autres PC. Simultanément, il a éliminé les points faibles de l'ordinateur détourné afin de rendre impossible toute prise de contrôle de celui-ci par d'autres pirates. Le propriétaire d'un ordinateur manipulé de la sorte (ou zombie) n'est pas conscient du téléguidage que subit sa machine.

une action ou un flux de données doit être expressément autorisée afin qu'une liaison puisse être établie avec un réseau. L'Internet fonctionne par le biais de l'envoi et de la réception de blocs de données, que l'on qualifie de « paquets ». Le pare-feu analyse ces paquets sur la base des règles prédéfinies et les autorise ou les refuse », explique François Thill, responsable du portail de la sécurité de l'information CASES du Ministère de l'Économie et du Commerce extérieur.

En fonction de la qualité du pare-feu, ce dernier peut également offrir le filtrage et l'analyse des données faisant partie des différents paquets. Le téléchargement de fichiers ou de logiciels malveillants sur Internet peut ainsi être évité. La consultation de pages web interdites peut également être bloquée, tout comme l'envoi ou la réception d'e-mails potentiellement dangereux.

Conseils relatifs à l'utilisation d'un pare-feu

Dans certains cas, un pare-feu peut entraîner des restrictions d'accès à un réseau comme Internet, par exemple lorsque le paramétrage est trop strictif. D'un autre côté, un réglage incorrect peut générer une impression trompeuse de sécurité. Afin d'utiliser un pare-feu au meilleur de ses possibilités, il est nécessaire de bien définir les règles et de le paramétrer correctement. La convivialité de la majorité des produits proposés rend cet exercice accessible aux utilisateurs même inexpérimentés. Ceux-ci devraient tenter de trouver le bon équilibre entre sécurité et fonctionnali-

Conseils de sécurité :

Pare-feu gratuits

La société de logiciels ZoneAlarm propose gratuitement (pour l'utilisateur privé) le pare-feu *ZoneAlarm* au téléchargement sur son site www.zonealarm.com. En suivant ce lien : [Download & Buy] suivi de [More free Downloads] puis en cliquant sur [Free ZoneAlarm® Firewall] [DOWNLOAD NOW] [ZoneAlarm® Firewall], tout utilisateur privé peut aisément télécharger et installer ce pare-feu sur son PC.

Vérification de sécurité gratuite par Computerports

Un ordinateur peut être comparé à un immeuble possédant 65 535 portes, les « ports ». Chaque porte est identifiée par un numéro spécifique et permet l'entrée de données vers l'ordinateur ou la sortie de données à partir de celui-ci. Si ces ports ne sont pas protégés, les cybercriminels peuvent obtenir l'accès à la machine concernée. Un pare-feu correctement paramétré protège les ports contre toute intrusion et tout flux de données indésirable. La société SecurityMetrics, active dans le domaine de la sécurité de l'information, propose une vérification de sécurité gratuite des principaux ports pour les ordinateurs utilisés à des fins privées. Le lien <http://www.securitymetrics.com/portscan.adp>, Home Office / Personal Firewall Test, permet de lancer un simple test de sécurité. Des explications et des conseils en matière de sécurité pour bien paramétrer son pare-feu sont communiqués au cours du test.

Définition : adresse IP

L'adresse IP (Internet Protocol) identifie un ordinateur ou tout autre appareil au sein d'un réseau. Elle permet d'identifier sans équivoque un PC. Les adresses IP sont utilisées sur Internet, une adresse précise est ainsi attribuée à chaque ordinateur. Une adresse IP peut être comparée à un numéro de téléphone dans un réseau téléphonique.

tés. Le pare-feu doit ainsi fournir un degré de protection adéquat tout en évitant une trop grande restriction des fonctions mises à la disposition de l'utilisateur. En principe, le nombre d'utilisateurs pouvant modifier les règles et les paramètres du pare-feu devrait être limité. S'ils n'ont pas pro-

cedé à l'installation de leur propre pare-feu sur l'ordinateur, les utilisateurs devraient vérifier le fonctionnement et le paramétrage du pare-feu basique accompagnant leur système d'exploitation respectif.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu