



À votre tour ! Activez le firewall !

Pour plus de sécurité, adoptez les réflexes CASES !

Un petit guide pour l'usage quotidien

Mystérieux firewall – un mécanisme de protection qui effraie encore bon nombre d'utilisateurs, sans raison. Ce portier s'active et se configure correctement en quelques clics. Qu'il soit écolier, étudiant, travailleur, femme au foyer ou retraité, chaque internaute est en mesure de maîtriser les fonctions et paramètres d'un firewall. Une colonne de journal suffit pour décrire les principales choses à savoir sur cette protection et les appliquer avec succès sur un ordinateur.

Un ordinateur équipé du système d'exploitation Windows XP, mais dont le firewall était inactif, est passé entre les mains de pirates en moins de quatre minutes en 2004. En 24 heures, la machine de test dépourvue de firewall a subi à cette époque plus de 8 000 attaques, selon une étude d'USA Today et Avantgarde. Surfer en toute décontraction sur Internet ? Sans firewall, cela n'est plus possible depuis de nombreuses années.

Mais que cache ce mécanisme de protection ? Les firewalls s'utilisent dans des routeurs, ordinateurs et réseaux informatiques, les trois pouvant se retrouver aujourd'hui dans les foyers luxembourgeois. Quasiment tous les ménages possèdent un ordinateur et un routeur DSL pour surfer à grande vitesse sur Internet. Le routeur est généralement un boîtier rectangulaire placé dans le garage, à la cave ou dans une pièce spécifique. Il analyse les paquets de données entrants puis les bloque ou les transmet à l'adresse de destination.

Comprendre rapidement et facilement le concept du firewall

Pour mieux comprendre le concept du firewall, il est utile de savoir qu'un ordinateur possède 65 535 portes, appelées « ports » dans le jargon

informatique. Des informations peuvent entrer dans l'ordinateur ou en sortir vers Internet via chacun de ces ports. Un routeur est une sorte d'ordinateur spécial qui analyse les paquets de données entrants en fonction de leur adresse de destination.

Le firewall a le rôle d'un gardien. Comme pour la surveillance d'un immeuble de bureau, tout le monde ne peut pas entrer ou sortir. Ce ne sont toutefois pas les personnes qui sont contrôlées, mais les programmes et les données. Cette vérification est très importante pour les routeurs. Pour en bénéficier, ils doivent disposer d'un firewall standard. Chaque ordinateur devrait aussi être protégé par un firewall. Les programmes ne peuvent alors plus accéder indépendamment à l'ordinateur via Internet, à l'insu de l'utilisateur. Il en va de même pour les programmes installés sur l'ordinateur. Ils ne peuvent plus quitter l'ordinateur vers Internet sans que l'utilisateur n'en ait connaissance.

Qu'est-ce que cela signifie ? La tâche de programmes malveillants comme les vers qui tentent seuls de pénétrer dans l'ordinateur se complique. Un cheval de Troie qui se trouve peut-

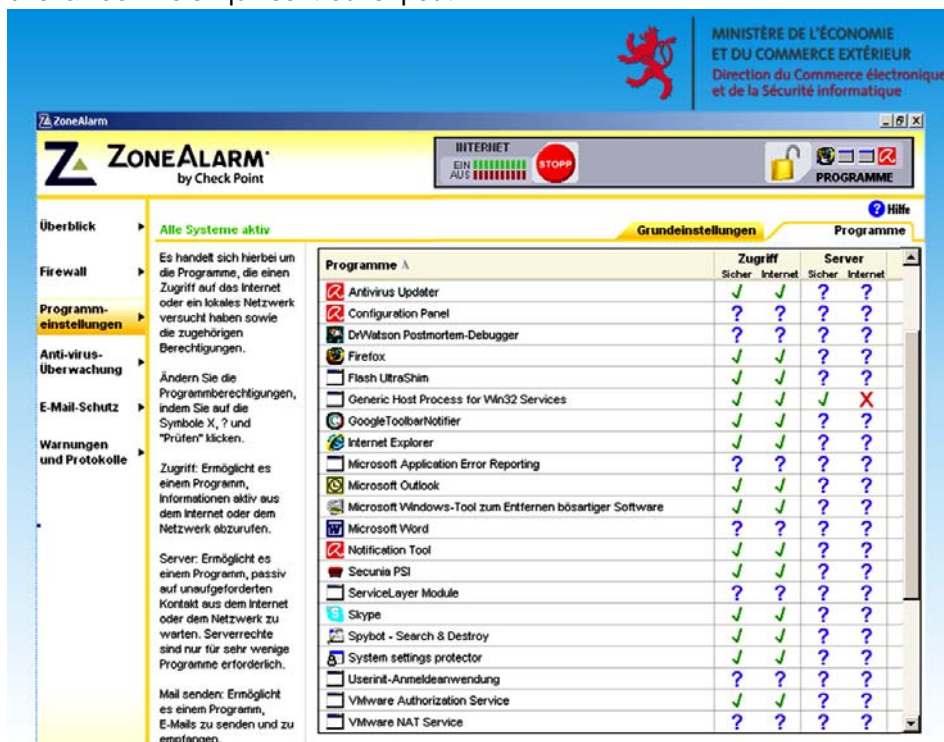
être déjà sur l'ordinateur et via lequel des pirates souhaitent entrer en contact sur Internet est également stoppé par le firewall. La sécurité est ainsi renforcée. C'est particulièrement vrai quand l'utilisateur surfe sur Internet directement depuis l'ordinateur, sans utiliser le routeur mais au moyen d'autres technologies comme l'UMTS.

Comme dans le cas du gardien d'un immeuble de bureau, il faut signaler au firewall les programmes qui peuvent accéder à l'ordinateur depuis Internet et ceux qui sont autorisés à aller sur Internet depuis l'ordinateur.

La protection de base en quatre clics

Tous les systèmes d'exploitation actuels possèdent un firewall de base. Pour les utilisateurs des systèmes d'exploitation Windows Vista ou Ubuntu GNU/Linux, ces firewalls sont activés automatiquement. Mais, attention, le firewall de base n'analyse que les données entrantes ! Il en résulte certes une meilleure protection contre les intrusions potentielles, mais les programmes et données peuvent toujours quitter l'ordinateur sans contrôle.

Un firewall de base est cependant



préférable à l'absence de protection et il est recommandé aux utilisateurs de Windows XP de vérifier la configuration de leur firewall s'ils ne possèdent pas de firewall spécial. C'est très simple, quatre clics suffisent : « Démarrer », suivi de « Contrôle du système », « Centre de sécurité » et « Firewall Windows ». Il faut cliquer ici sur la fonction « Actif » sous « Généralités ». Si ce n'est pas le cas, le paramétrage correspondant peut être réalisé aussitôt. Un firewall non activé sera signalé dans le centre de sécurité par un symbole de couleur rouge et « inactif ».

La meilleure protection consiste toutefois en l'installation d'un firewall qui assumera toutes les fonctions d'un gardien, c'est-à-dire vérifier les flux de données entrants et sortants. Les utilisateurs qui installent un tel firewall seront d'abord étonnés du nombre de programmes qui demandent une autorisation pour aller sur Internet ou pour accéder à l'ordinateur. Ce n'est qu'à ce stade que beaucoup d'utilisateurs réalisent les allées et venues transitant par leur ordinateur.

À côté des programmes de protection payants qui offrent une protection intégrale, l'industrie propose aux utilisateurs privés des produits gratuits moins complets assurant une bonne protection. La section suivante explique les principaux paramétrages d'un tel produit gratuit, en prenant l'exemple du firewall ZoneAlarm.

Exemple – bien configurer un firewall

Sur le site www.zonealarm.com, les utilisateurs privés utilisant le système d'exploitation Windows peuvent télécharger et installer une version gratuite du firewall Zonealarm en cliquant sur « Télécharger et acheter », puis sur « Téléchargements gratuits ». Selon la puissance de l'ordinateur et la connexion Internet, le téléchargement et l'installation peuvent prendre de quelques minutes à une demi-heure. Après l'installation, l'utilisateur peut configurer le firewall en ouvrant le programme ZoneAlarm Security.

Dans le programme, rubrique « Firewall », il convient de régler les « Paramètres de base » au moins sur « Moyen ». Les utilisateurs doivent veiller à ce que le paramètre ne soit pas sur « Éteint ». Attention ! Si ce paramètre est désactivé, il n'y a plus

de protection assurée par le firewall, même par le firewall de base de Microsoft. Les utilisateurs peuvent le vérifier sous Windows via « Démarrer », « Contrôle du système », puis « Centre de sécurité ». Si l'utilisateur souhaite laisser le paramètre « Désactivé » de ZoneAlarm, il est nécessaire de réactiver manuellement le firewall de base du centre de sécurité via « Firewall Windows », « Actif ».

Si les paramètres de base du firewall ZoneAlarm sont sur « Moyen », il faut déterminer quels programmes ont quels droits. Nous utiliserons ici

l'exemple d'un ordinateur ne faisant partie d'aucun réseau. Un internaute moyen qui surfe, lit ses e-mails, téléphone via l'ordinateur et joue à des jeux peut configurer rapidement et facilement la version gratuite du firewall ZoneAlarm.

Les utilisateurs doivent savoir qu'il est généralement préférable que les programmes de l'ordinateur accèdent à Internet pour y puiser les informations. Les spécialistes parlent ici d'une fonction « pull ». Il faut, par contre, éviter que des programmes d'Internet aient accès à l'ordinateur pour y puiser des informations.

Conseil de sécurité : vérification de la sécurité des ports d'un ordinateur ou d'un routeur

Les cybercriminels tentent d'obtenir l'accès à l'ordinateur d'un utilisateur via les ports. Les utilisateurs privés peuvent faire vérifier gratuitement la sécurité des principaux ports de leur routeur. La société de sécurité de l'information Security Metrics propose un tel test en ligne : <http://www.securitymetrics.com/portscan.adp>. Le test est accompagné d'explications et de recommandations de sécurité. Cette vérification peut être effectuée aussi pour l'ordinateur. Mais, pour que le test ne se limite pas aux ports du routeur DSL et vérifie réellement ceux de l'ordinateur, ce dernier doit se connecter à Internet directement via une autre technologie comme l'UMTS. Attention ! Surfer directement sur Internet sans firewall actuel et bien configuré revient à s'exposer à un risque accru d'attaque. Si les utilisateurs privés de Windows peuvent compter sur des firewalls comme ZoneAlarm, mis à disposition gratuitement par l'industrie, les utilisateurs de Mac OS X peuvent utiliser le firewall gratuit WaterRoof. Sur www.cases.lu, les utilisateurs trouveront en outre sous la rubrique « Publications », « Dossiers », « Dossier DSL » les résultats du test de sécurité des routeurs DSL courants du commerce au Luxembourg.

Définition : système d'exploitation

Un système d'exploitation est un logiciel permettant le fonctionnement d'un ordinateur. Le système d'exploitation administre par exemple la mémoire, les unités d'entrée et de sortie ainsi que l'exécution de programmes.

Définition : UMTS

L'Universal Mobil Telecommunications System (UMTS) permet un débit nettement plus rapide qu'avec la norme GSM. On parle aussi de la norme de téléphonie mobile de troisième génération, 3G.

Définition : firewall

Un serveur est un logiciel spécial mettant à la disposition d'autres programmes un accès à des services spécifiques. Le logiciel communique pour cela avec d'autres programmes appelés clients dans le jargon informatique. Le matériel est aussi appelé serveur. Il s'agit ici d'un ordinateur sur lequel tourne au moins un logiciel serveur.

Définition : navigateur

Les navigateurs sont des programmes utilisés pour consulter des sites Internet.

Dès l'installation, le programme de protection procède seul au réglage pour les programmes courants. L'utilisateur peut toutefois modifier ces paramètres sous la rubrique « Paramètres du programme », « Paramètres de base ».

Tous les programmes de l'ordinateur mis à jour automatiquement nécessitent un accès à Internet. La mise à jour régulière de programmes est une fonction de protection très importante et ne peut en aucun cas être interdite. Ces programmes demanderont donc un accès Internet au firewall, lequel transmettra la demande à l'utilisateur. Pour que des programmes comme le système d'exploitation, l'antivirus, le navigateur ou le programme de téléphonie restent à jour, il faut accorder ici l'autorisation d'accès à Internet.

Pour que des programmes de messagerie électronique comme Outlook puissent aller chercher les e-mails sur Internet, il faut aussi autoriser leur accès à Internet. Si ce point est négligé, l'utilisateur s'étonnera de ne plus recevoir d'e-mails. Pour éviter ces soucis, les programmes comme l'application d'e-mails peuvent être ajoutés à la liste de programmes ZoneAlarm et libérés pour Internet via « Paramètres de programme », puis « Ajouter ».

En général, les utilisateurs peuvent constater que presque aucun des programmes n'a besoin d'une autorisation du serveur. Si certaines fonctions disparaissent après l'installation du firewall, il suffit de vérifier les paramètres du programme.

Les messages envoyés par le firewall doivent toujours être lus attentivement.

Seuls les programmes connus de l'utilisateur devraient obtenir un accès vers Internet. Il en va de même pour les accès à l'ordinateur. L'utilisateur doit s'informer sur les programmes inconnus, par exemple sur le programme « Generic Host Process for Win32 Services ». Il s'agit d'un programme Windows que l'on peut sélectionner dans la liste de programmes en cochant les domaines « Accès sûr », « Accès Internet » et « Serveur sûr ».

CASES, le portail luxembourgeois de la sécurité de l'information du Ministère de l'Économie et du Commerce extérieur, www.cases.lu, met à disposition des utilisateurs une assistance par e-mail pour répondre aux questions relatives au firewall.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu