Alerte Rouge

Est-ce que votre périmètre est sécuritaire?

Nelson Ruest, directeur des Entreprises Résolutions - nruest@reso-net.com
Danielle Ruest, directrice adjointe des Entreprises Résolutions - danrue@reso-net.com

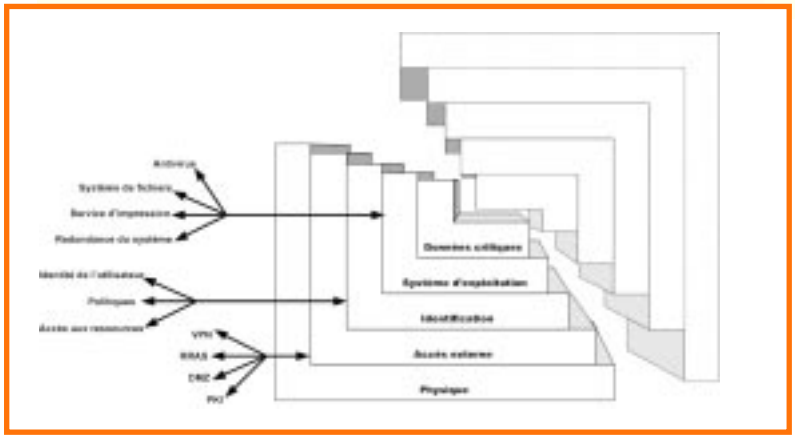
Non, ce n'est pas le nom d'un film populaire. Non, il faut faire l'alerte! L'alerte rouge! Car la sécurité informatique est devenue tellement importante que son manque commence à tous nous affecter.

Prenons, par exemple, le virus « Code Red ». Depuis la mi-juillet, la lumière indiquant la réception clignote sans arrêt sur notre modem câble personnel même quand tout poste est arrêté complètement. Pourquoi? Parce qu'il transige présentement sur Internet un nouveau virus de type « vers » qui infecte les serveurs Web utilisant Internet Information Server de Microsoft. Ce virus infecte les systèmes non-protégés et s'y installe comme si c'était son chez-soi. À partir de ce moment, il commence à rechercher d'autres endroits qu'il peut appeler chez lui.

Alors, il choisit des adresses Internet au hasard et vérifie s'il peut, premièrement entrer, ensuite trouver un habitat accueillant (le serveur IIS de Microsoft), vérifie si la porte est verrouillée et, si elle est ouverte, s'y installe tout bonnement comme si c'était l'enfant prodige tant attendu.

Pourtant, s'il y a un virus bien connu sur l'Internet, c'est bien Code Red. Depuis les tous premiers jours de son annonce, les firmes et les organismes spécialisés en sécurité informatique ont donné l'alerte. Plusieurs manufacturiers d'anti-virus ont annoncé de nouvelles signatures permettant sa détection et son élimination. Tout le monde aurait dû être bien au courant des méfaits de ce vers.

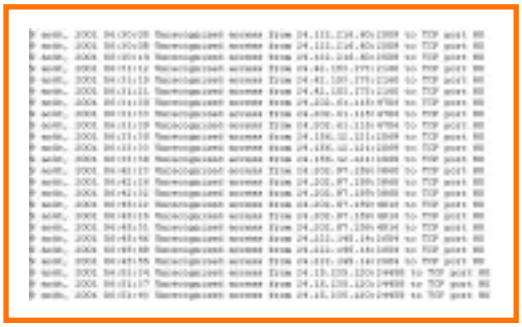
Autre point important du dossier, le virus a un comportement régulier basé sur un horaire mensuel. Au début du mois, il essaie d'infecter d'autres systèmes par l'entremise d'adresses aléatoires et entre le 20 et le 28, il attaque le site de la Maison Blanche à Washington (www.whitehouse.org). Pis encore, il a la capacité de se métamorphoser.



Le rapport d'un garde-barrière personnel démontre que Code Red est très actif, même chez soi.

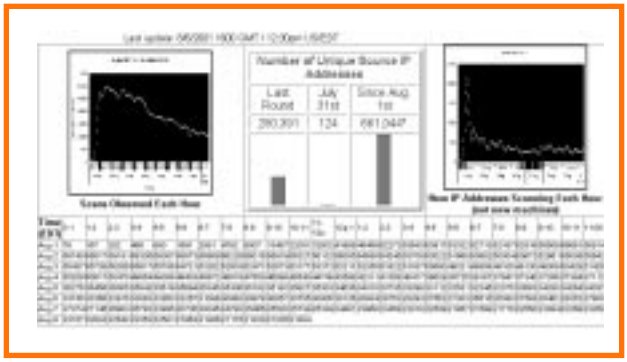
À date, ce virus a infecté de 150 000 à 175 000 systèmes. Et, ce ne sont que les systèmes connus. Un rapport complet est disponible au site Web de Digital Island (www.digitalisland.net/codered/). Ce qui est à déplorer des méfaits de ce virus, c'est que l'alerte a belle et bien été donnée et que les solutions ont rapidement été disponibles. Microsoft avait un correctif dès le 18 juillet et nombre de revues, de journaux, de stations de radio, même télévision, de courriers électroniques, de bulletins électroniques, ont lancé l'alerte. Aucune personne responsable de système informatique, quelle que soit son envergure, aurait dû être ignorante du fait que ce virus était à la recherche de proies. De plus, le correctif ne prend que quelques minutes à installer et selon les instructions du site de Digital Island, le virus est très facile à éliminer.

Alors, pourquoi la lumière de notre modem câble? Parce que 175 000 systèmes balaient l'Internet avec des adresses aléatoires pour en infecter d'autres; c'est beaucoup et c'est trop. C'est trop quand un fournisseur Internet tel Vidéotron, se sent obligé d'avertir sa clientèle. Dans un communiqué à ses clients daté du 6 août, Vidéotron annonça et expliqua le pourquoi du clignotement de la lumière de réception. C'était bel et bien Code Red.

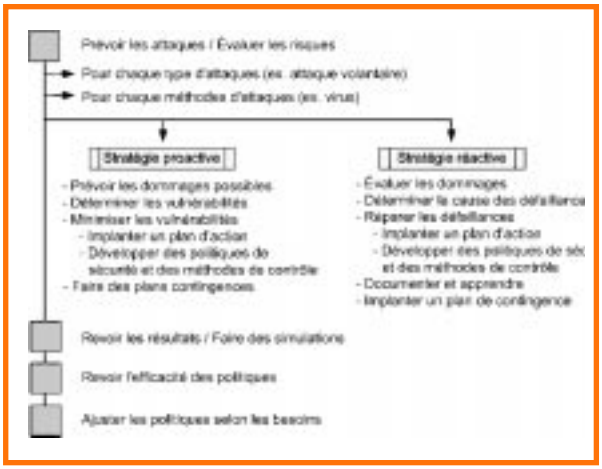


Digital Island affiche les activités de Code Red.

La sécurité peut être vue comme une série de blocs ou de murs protégeant des données critiques.



Quand il s'agit de sécurité, toute organisation se doit d'être proactive et réactive.



Le problème de sécurité

La sécurité est importante pour tous, que nos systèmes soient domestiques ou corporatifs. Plusieurs utilisent les technologies Windows de Microsoft et ainsi, plusieurs utilisent IIS car il y est compris (dans les versions serveurs de Windows) et il s'installe par défaut. Mais le problème ne s'arrête pas à Windows. Tous les systèmes ayant accès à Internet ont des failles quelconques.

L'institut SANS (www.sans.org), un organisme publique dédié à la diffusion d'informations et de formation sur la sécurité informatique et aussi dédié au combat contre les intrusions et autres attaques électroniques, produit un bulletin hebdomadaire sur les failles connues des systèmes informatiques. Chaque édition inclut des informations sur les systèmes de type Linux, IBM, Sun, Oracle et bien d'autres. Le domaine informatique est vaste et les failles possibles le sont aussi.

La sécurité est un problème qui affecte tous et toutes en informatique. Mais aujourd'hui, elle affecte aussi les individus qui se dotent de systèmes domestiques. La venue des sites Web personnels propage l'utilisation des technologies informatiques. Pour vous, les utilisateurs individuels, tout comme pour les informaticiens, nos conseils sont les suivants :

- Abonnez-vous à un service d'informations de sécurité! Pour les informaticiens dédiés, utilisez le service de SANS (http://server2.sans.org/sansnews). Pour les amateurs, utilisez au moins le service fournit par votre manufacturier de système d'exploitation. Pour les utilisateurs de Microsoft IIS, voici l'adresse : http://www.microsoft.com/security/default.asp.
- Utilisez aussi un garde barrière (« firewall » en anglais). Les utilisateurs domestiques peuvent maintenant se procurer de petits gardes-barrières personnels aux environs de 350 $. Ceux-ci sont disponibles des sociétés D-Link, Linksys, Intel et autres. Ces petits outils sont des merveilles car ils bloquent tout accès à votre environnement interne, automatiquement. Les utilisateurs corporatifs ont accès à des solutions de sécurité qui sont beaucoup plus complètes et c'est leur responsabilité de se doter des outils appropriés.

Des personnes, des procédures et des PCs

Mais, la sécurité ne s'arrête pas à la technologie. En fait, les éléments les plus importants de la sécurité sont souvent le personnel et les procédures. Une organisation qui priorise la sécurité doit se doter d'une politique de sécurité. Celle-ci établit les grandes lignes et les responsabilités nécessaires pour protéger les informations qui sont les acquis de l'organisation.

Une des méthodes les plus efficaces pour faciliter un comportement sécuritaire est d'utiliser un modèle de sécurité. Ce modèle est représenté sous forme de blocs concentriques. Chaque bloc forme une couche de sécurité. Celle-ci inclut : la sécurité physique, les accès externes, l'identification, le système d'exploitation et les données critiques. Ce sont ces dernières que la sécurité vise à protéger, donc chaque couche forme un bouclier protégeant ces données.

Les éléments physiques incluent des salles informatiques verrouillées, des gardiens de sécurité, des systèmes d'alarme. Les accès externes protègent le réseau des accès électroniques provenant de sources externes à votre réseau. L'identification assure l'authenticité des intervenants et leur accorde les permissions appropriées. Le système d'exploitation permet la mise en place de mesures de sécurité informatisées telles l'anti-virus, le système de fichiers et la relève automatique. Chaque couche assiste la protection de la couche adjacente.

La politique de sécurité contient une expression d'actions disciplinaires si elle est ignorée. Elle couvre toutes les couches énumérées, mais doit aussi inclure une communication régulière avec les utilisateurs, un programme de formation, des processus de vérification, des agents de sécurité désignés, et un plan réactif ainsi qu'un plan de récupération. La communication et la formation assureront que le point d'appui d'un environnement sécuritaire, le personnel, sera au fait des choses. Souvent, tout repose sur les processus utilisés et le degré d'importance qui sera accordé à la sécurité par le personnel de l'organisation. Ce sont les piliers de la sécurité interne.

Tout organisme se doit d'avoir un élément de sécurité en informatique. Tous ont le choix : être proactifs et prévenir, ou être réactifs et réagir.

Être maître chez soi

Code Red est un virus dangereux. Il affecte non seulement les organismes utilisant l'informatique, mais aussi le rendement que les individus attendent de l'Internet. Soyez proactifs ou réactifs, le choix est le vôtre; 90 % de la solution a un problème, c'est de savoir qu'il existe. La sécurité, c'est un élément essentiel de l'informatique.