Bulletin Valeur Ajoutée

BVA

Protéger votre site

Selon les spécialistes en sécurité informatique, les pare-feu n'offrent pas une protection absolue contre les pirates qui sévissent sur Internet.

Richard Reiner, responsable technologique principal et **Karen McNeil,** directrice de projet principale, Assurent Software, Inc.

Une fois qu'elle a établi une présence en ligne, une entreprise a besoin de savoir si la sécurité de ses applications est bien assurée.

M. Richard Reiner souhaiterait d'ailleurs que plus de chefs d'entreprises y fassent attention. M. Reiner, responsable technologique principal de la firme Assurent Software Inc., est reconnu dans le monde comme une autorité dans le domaine de la sécurité informatique, de la sécurité des applications et de la protection des renseignements personnels. Selon lui, la diversité des applications actuellement ouvertes sur Internet (sites de services bancaires au détail, systèmes de réservation, portails personnalisés, outils d'accès à distance et même sites Web de marketing) fait qu'il est devenu moins évident pour les entreprises de défendre leurs systèmes informatiques contre les pirates.

« Avec la migration des applications des gros ordinateurs vers les interfaces Web, il est devenu plus difficile d'assurer l'intégrité des serveurs et des systèmes informatiques, en raison des risques accrus, explique M. Reiner. Depuis trois ou quatre ans, les pirates informatiques s'intéressent moins au cœur des systèmes, qui restent relativement à l'abri derrière les pare-feu, pour s'attaquer aux points d'entrée que représentent les applications auxquelles les entreprises permettent d'accéder par Internet. »

En s'en prenant aux applications, qui résident en surface, les pirates peuvent arriver à pénétrer encore plus profondément à l'intérieur des processus internes, et à causer plus de tort. Comme les applications ouvertes sur Internet ont avec le temps pris une importance croissante pour les entreprises, elles tendent à être de plus en plus intégrées aux systèmes internes. Une transaction effectuée par un client à partir d'une interface Web peut donc, en déclenchant une réaction en chaîne au niveau des données, se ressentir au niveau de la base d'information de l'entreprise elle-même.

Il importe par conséquent de s'assurer que les applications Internet des entreprises soient dotées des caractéristiques de sécurité intégrées dès le départ, affirme M. Reiner, car il y a des limites à ce qu'on peut faire pour améliorer la sécurité des applications à l'étape du déploiement.

« En matière de sécurité des applications, l'approche actuelle consiste à verrouiller les applications au niveau du code source. »

« Malheureusement, il arrive souvent que des vulnérabilités subsistent au niveau du code sans qu'on les détecte. Le processus de validation du code est onéreux, et il n'y a pas assez de développeurs suffisamment bien formés pour régler les problèmes de sécurité. »

Printemps 2005 • Numéro 25

Banque Scotia[MC]

44, rue King Ouest
Toronto (Ontario) M5H 1H1
Courriel : businessproducts@scotiabank.com
www.banquescotia.com/bva

[MC] Marque de commerce de La Banque de Nouvelle-Écosse.
Tous les autres noms de produits et de services sont des marques de commerce ou des marques déposées de leurs propriétaires respectifs.
La mention de marques de commerce dans cette publication n'implique pas la concession d'une licence.
© Banque Scotia, 2004. Tous droits réservés.

Bien que des produits de sécurité aient été mis au point pour tenter de reconnaître les signatures d'attaques ayant déjà touché des applications, ou «documentées», les pirates conçoivent souvent au cas par cas des attaques non reconnues comme des attaques s'étant déjà produites.

« L'Open Web Application Security Project a répertorié 135 possibilités d'attaque différentes sur des applications Web, fait remarquer M. Reiner. Souvent, on ne se rend compte qu'on a été attaqué que quand on s'aperçoit que des données de l'entreprise se sont volatilisées ou sont tombées en de mauvaises mains. »

M. Reiner ajoute que beaucoup trop d'entreprises ont une fausse impression de sécurité quand il s'agit de leurs applications ouvertes sur Internet.

Et d'ajouter : « Il y a bien des gens dans les entreprises qui se laissent bercer par l'idée qu'un pare-feu empêchera l'utilisation non autorisée ou abusive de leurs applications Web. Or, un pare-feu ne constitue en fait que la première ligne de défense d'un réseau. Pour une protection complète, il faut ajouter un système de protection de deuxième ligne. »

L'isolation des processus, un développement positif

Un pare-feu permet d'établir une ligne de front, mais il y a maintenant également de nouveaux logiciels pour protéger les applications elles-mêmes, à l'intérieur du périmètre protégé.

Au lieu d'essayer d'intercepter les activités suspectes en repoussant les attaques détectées, la protection de deuxième ligne consiste à déterminer les interactions légitimes entre l'utilisateur et l'application et à arrêter les autres. Dans cette logique, toute tentative d'accès ne cadrant pas avec les modes d'utilisation permis sera considérée comme une attaque et traitée en conséquence.

Connaître les risques pour investir dans les meilleures technologies

Comme on peut l'imaginer, les institutions financières canadiennes ne sont pas les dernières à se soucier de défendre leurs réseaux et leurs applications. En fait, les spécialistes des TI de toutes les grandes banques échangent régulièrement de l'information sur les moyens d'assurer la sécurité en ligne et les derniers outils développés dans ce but. Cette coopération rend l'ensemble du système bancaire canadien plus sûr et permet de mieux combattre la fraude.

Glenn Blair, directeur général adjoint, Sécurité informatique de la Banque Scotia déclare :

« Nous sommes à l'avant-garde pour ce qui est d'intégrer de nouveaux dispositifs de sécurité à nos systèmes. Sachant que la Banque Scotia fait beaucoup pour promouvoir les solutions Web de gestion de la trésorerie, nous prenons notre responsabilité très au sérieux. Il s'agit pour nous de combiner les technologies de détection et d'isolation de manière à atteindre ou à dépasser les normes d'exploitation que nous nous fixons tout en évitant à la Banque de s'exposer à des risques indus. »

Selon M. Reiner, toutes les entreprises se doivent d'évaluer le degré de risque auquel elles s'exposent afin de déterminer si elles doivent investir davantage en vue de renforcer la sécurité de leurs applications.

Optimiser la sécurité des systèmes informatiques d'une entreprise revient somme toute à une question d'argent, c'est-à-dire : combien est-on prêt à mettre?

Comme l'exprime M. Reiner, « il peut être plus facile de prévoir les pertes financières à comptabiliser en fin d'exercice que de mesurer l'impact possible sur la réputation de la Banque d'une brèche dans la protection des informations confidentielles. Or, c'est cela qui devrait guider les décisions prises en ce domaine. »

Printemps 2005 • Numéro 25

Banque Scotia[MC]

44, rue King Ouest
Toronto (Ontario) M5H 1H1
Courriel : businessproducts@scotiabank.com
www.banquescotia.com/bva

[MC] Marque de commerce de La Banque de Nouvelle-Écosse.
Tous les autres noms de produits et de services sont des marques de commerce ou des marques déposées de leurs propriétaires respectifs.
La mention de marques de commerce dans cette publication n'implique pas la concession d'une licence.
© Banque Scotia, 2004. Tous droits réservés.