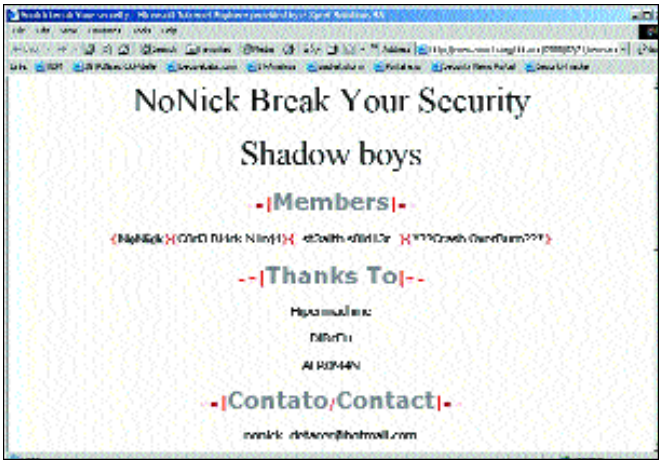
La sécurité des applications web

Les firewalls applicatifs HTTP

DANGER. Les chiffres sont éloquents : 90% des applications web sont vulnérables. Et leur nombre ne cesse d'augmenter de façon drastique. Un article de e-Xpert Solutions.



Les problèmes de sécurité sont incontestablement un motif de préoccupation, un frein important au déploiement des applications et services web. Cet article a pour ambition d'explorer les outils, classiques ou plus avant-gardistes, qui peuvent être mis en œuvre pour réduire tout ces risques.

Les applications web

Une application web est une application qui n'a besoin que du protocole HTTP pour être pilotée par un utilisateur. Celui-ci a alors besoin d'un simple navigateur web ou d'une application propriétaire utilisant le protocole HTTP.

La plupart des applications web sont accessibles depuis Internet. Un grand nombre d'entre elles se trouvent également sur des intranets. Or, ceux-ci ne peuvent pas non plus être considérés comme des réseaux sûrs.

Les applications web sont généralement basées sur une architecture en trois tiers :

1. Pr sentation

Le premier tiers est responsable de la présentation des informations entre le client et le serveur. Cette partie est composée du navigateur et d'un serveur web, auxquels s'ajoute généralement un générateur de pages (JSP, ASP, Java Script, HTML, etc.).

2. Application

Le deuxième tiers est le «moteur» de l'application. Il est responsable de la logique de l'application, du traitement des données, de la prise de décision, etc. Cette partie est généralement basée sur une application serveur (WebLogic, WebSphere, Jakarta, JBoss, etc.) et a recours à des technologies comme Java, .Net, PHP, CGI, etc.

3. Donn es

Enfin, le dernier tiers assure l'interfaçage et le stockage des informations nécessaires au fonctionnement de l'application web. Plusieurs méthodes d'accès peuvent être utilisées, telles que XLM, SQL, JDBC, etc. Naturellement, il existe des applications web beaucoup plus simples, qui ne fonctionnent pas sur ce modèle. Elles nécessitent toutefois autant de précautions en termes de sécurisation.

L'approche classique

Différentes manières de protéger les applications web peuvent être mises en œuvre. L'approche classique consiste à sécuriser le périmètre, les communications et les systèmes d'exploitation qui hébergent les applications web.

Sécurité du périmètre – firewall

Le but de la sécurisation du périmètre est de protéger l'accès réseau aux applications web et plus particulièrement au serveur web frontal (Apache, IIS, IPlanet, etc.). Cette protection est généralement mise en place à l'aide d'un firewall. Son rôle principal est de filtrer les accès et de n'autoriser que les protocoles réseaux nécessaires au bon fonctionnement de l'application web.

Dans la plupart des cas – s'il s'agit d'une application web publique – le serveur web est placé sur une DMZ (zone publique du firewall). Le firewall n'autorise alors que le protocole HTTP (port 80), voire le protocole HTTPS (SSL port 443). Tous les autres sont par contre bloqués.

Sécurisation des communications – SSL

Dans certains cas, il est nécessaire de sécuriser l'accès entre le navigateur et l'application web. SSL est une solution très intéressante à cet égard. Elle offre :

la confidentialit , qui permet de chiffrer les communications entre le navigateur et le serveur web par des algorithmes cryptographiques du type 3DES, RC4, etc. Il devient alors extrê-

mement difficile pour des «hackers» de déchiffrer les informations transitant sur le réseau;

l'int grit , qui propose un mécanisme capable de détecter d'éventuelles modifications des informations transitant entre le navigateur et le serveur web. Il est dès lors très difficile de modifier les informations sans laisser de traces;

l'authentification des communications. Avec la technologie des certificats numériques (PKI, X509), tout navigateur qui se connecte à un serveur web SSL peut obtenir la preuve qu'il est bien en train de communiquer avec le serveur de son choix. Le certificat numérique permet en effet d'attester l'appartenance d'un site web à telle ou telle société. A noter que ce mécanisme propose une authentification à sens unique : l'utilisateur peut authentifier le serveur web, mais pas l'inverse.

Avec SSL, il est toutefois possible de disposer de l'authentification mutuelle. Cela signifie que le serveur web peut, lui aussi, identifier avec certitude la personne utilisant le navigateur. Pour cela, il est nécessaire de délivrer un certificat numérique à l'utilisateur lui-même. Le certificat sera alors utilisé par le navigateur web.

Sécurisation des systèmes d'exploitation – FIA

Malgré la multiplication des firewalls, il est entré dans les mœurs de sécuriser les systèmes d'exploitation qui hébergent les applications web et plus particulièrement le serveur web. Qu'il s'agisse d'une plate-forme Unix/Linux ou Windows, l'approche reste la même.

L'idée est de blinder l'OS. Différentes mesures peuvent être prises à cet effet :

- restriction des services, blindage du «stack» IP;
- sécurisation de la méthode d'administration (SSH, Remote contrôle sécurisé);
- authentification forte pour l'administration (*SecurID, Token USB*, carte à puces, etc.);
- mise en place de mécanismes d'alerte;
- mise en place de procédures de backup;
- application des patchs de sécurité;
- etc.

Afin de garantir l'intégrité des systèmes d'exploitation, il peut s'avérer très utile de mettre en œuvre une solution de contrôle d'intégrité. Il s'agit alors de surveiller, grâce à des mécanismes de signature digitale, les fichiers sensibles. La technologie FIA (*File Integrity Assesment*) – dont le produit le plus utilisé est Tripwire – permet de déceler le moindre changement intervenant sur une machine. Elle est ainsi très efficace pour détecter et lutter contre les intrusions (technologie IDS).

Limites de l'approche classique – le port 80

L'approche classique est nécessaire, mais elle ne répond pas au principal problème de sécurité des applications web. En dépit de tous les mécanismes mis en place, il est nécessaire de laisser le port 80 ou 443 traverser le firewall pour atteindre le serveur web frontal. Dans ce cas, le rôle du firewall est donc d'autoriser ou non le port 80 ou 443. Il n'est toutefois pas en mesure d'analyser les informations transportées par le protocole. Cela revient à laisser des camions passer la douane sans regarder le contenu de leur cargaison!

Pourquoi le port 80 pose-t-il problème?

Les statistiques le démontrent largement : la plupart des applications web sont vulnérables aux attaques applicatives. Ces vulnérabilités sont essentiellement dues à des failles dans leurs différents composants logiciels. Un «hacker» a dès lors tout loisir d'exploiter ces failles par l'intermédiaire du protocole HTTP (port 80/443). Le firewall classique n'est donc pas en mesure de bloquer de telles attaques.

Quelle solution? Le firewall applicatif HTTP

Une autre solution consiste à protéger les applications web des attaques externes. Cette protection se comporte comme un firewall classique, à cette différence près qu'elle se concentre exclusivement sur le protocole HTTP et son contenu (XML, SOAP, HTML, etc.). Cette technologie, appelée firewall applicatif HTTP, est à même de filtrer toutes les requêtes HTTP, de manière à ne laisser passer que les informations nécessaires et considérées comme non dangereuses. Il est ainsi possible de se prémunir contre des attaques de type : Buffer Overflow, Directory Traversal, Cross Site Scripting (XSS), SQL Injection, Meta caractères, Back Door, Cookies Poisoning, Brute force, Manipulation d'URL, etc.

Déploiement

La mise en œuvre d'une solution de sécurisation des applications web peut s'effectuer de plusieurs façons :

- installation d'un agent sur le serveur web frontal;
- installation d'une machine relais (reverse proxy) devant le serveur web.

La première approche est intéressante en termes de coûts, mais elle est très intrusive. La seconde offre une architecture plus robuste, dans la mesure où la machine relais est pensée pour être très sécurisée.

Nécessaire mais pas suffisant

Encore trop d'entreprises pensent que dès lors qu'elles ont mis en place un firewall classique, elles sont à l'abri de menaces externes. Certes, le firewall classique est un élément nécessaire. Il ne peut cependant protéger, à lui seul, les applications web. Il est dès lors recommandé, pour sécuriser vos applications web stratégiques, de recourir à un firewall applicatif HTTP. ●

Sylvain Maret
Directeur
veille technologique
e-Xpert Solutions SA

Contact : e-Xpert Solutions SA
Route de Pré-Marais 29
1233 Bernex
Tél : +41 22 727 05 55
info@e-xpertsolutions.com
http://www.e-xpertsolutions.com

e-Xpert Solutions SA

Au bénéfice d'une longue expérience dans les secteurs financier et industriel, e-Xpert Solutions SA propose à sa clientèle des solutions «clés en main» dans le domaine de la sécurité informatique des réseaux et des applications. Des solutions qui vont de la sécurité d'architecture – tel le firewall, VPN, IDS, FIA, le contrôle de contenu, l'antivirus – aux solutions plus avant-gardistes comme la prévention des intrusions (approche comportementale), les firewalls applicatifs HTTP, l'authentification forte, la biométrie, les architectures PKI ou encore la sécurisation des OS Unix et Microsoft et des postes clients (firewall personnel).

Article paru dans IB com, avril 2003

IBcom