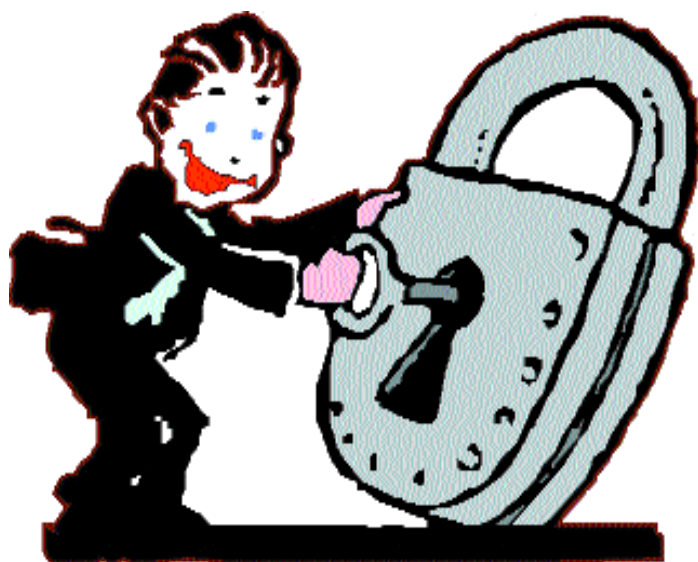


Sécurisation du port 80. Un article d'e-Xpert Solutions

Sécurisation des flux HTTP pour les postes clients

PROTOCOLE. Qu'ont en commun le Peer-to-Peer, l'Internet Surfing, la Backdoor, l'Instant Messaging, le Soap, le Tunneling HTTP ou encore les codes mobiles? Tous font appel au port 80.



Sécurité Il faut veiller à ce que l'entreprise soit bien «verouillée» par rapport aux virus.

Article paru dans IBcom, fév. 2004

IBcom

De plus en plus, le port 80 (HTTP) est utilisé comme protocole de transport universel. Il est devenu un des moyens les plus aisés pour échanger des informations, car généralement autorisé par la plupart des firewalls. Initialement conçu pour transporter des informations liées à HTTP/HTML, il est désormais le protocole de prédilection d'un nombre croissant d'autres applications, tels que le Peer-to-Peer, les codes mobiles, la messagerie instantanée, le transfert de fichiers, les services web (Soap), etc.

Cet état de fait a toutefois son revers. Dès lors que le port 80 devient en quelque sorte la couche transport, la plupart des firewalls ne sont plus en mesure de le filtrer correctement. Cela

pose des problèmes de sécurité, notamment pour ce qui est de la protection des applications ou des services web, mais surtout pour celle des entreprises autorisant leurs employés à surfer sur Internet.

Le but de cet article est de se focaliser sur ce dernier point. Soit d'évoquer les mesures techniques qu'il est possible de mettre en œuvre au sein d'une entreprise pour assurer une protection réellement efficace des systèmes. Outre les aspects techniques de la sécurité, il est possible d'avoir recours à toute une série de mesures plus «organisationnelles» pour répondre à la politique de sécurité de l'entreprise. On peut penser au filtrage d'URL, à l'accès ou non à Internet, etc. Ces points ne seront toutefois pas traités dans cet article.

Votre firewall périmétrique est-il suffisant?

La plupart des entreprises connectées à Internet ont aujourd'hui mis en place un firewall, voire un système de détection et/ou de prévention d'intrusions réseau. Ceci constitue la «protection périmétrique» et c'est sans conteste une très bonne approche. Mais qu'en est-il du système de sécurité relatif aux accès internet des postes clients? Peut-on sans autre laisser le port 80 traverser le firewall périmétrique sans contrôle spécifique? La

réponse dépend bien entendu du risque qu'une entreprise est prête à accepter, sachant que le port 80, s'il est mal contrôlé, peut ouvrir la porte à un grand nombre d'attaques : virus, Malware, Spyware; Tunneling HTTP; fuite d'informations; exécution de codes malicieux; portes dérobées (Backdoors; vol de données; etc.).

Plusieurs axes de contrôle

Outre la mise en application d'un antivirus local sur tous les postes clients, on peut faire ressortir plusieurs axes de contrôle : l'authentification; le contrôle du contenu; le filtrage des URL; la journalisation des accès. Il existe plusieurs approches pour sécuriser le port 80. L'une d'entre elles consiste à traiter le problème par l'installation de logiciels spécialisés (FW personnels, HIDS, HIPS, etc.) sur tous les postes clients. Une autre est de mutualiser ces contrôles en un point unique.

Contrôle du port 80 par la technologie proxy

Pour mettre en place les différents axes de contrôle, l'idée est de faire transiter tous les flux du port 80 à travers un proxy. Celui-ci est généralement placé en amont du firewall périmétrique. Avec une telle architecture, il devient impossible de «sortir» sur Internet sans un passage par cet outil de contrôle.

L'authentification : une des mesures de base

Une des premières mesures de sécurité à appliquer réside dans l'authentification soit de l'utilisateur, soit du poste de travail pour pouvoir utiliser le proxy. Toute communication non authentifiée est rejetée par le proxy. Cette mesure a pour effet de contrôler de façon très granulaire qui ou quel poste est autorisé à surfer sur Internet et avec quels droits d'accès.

Il existe plusieurs façons de faire. Une des plus simples est de recourir à l'existant, tel un annuaire d'entreprise (AD Microsoft, Novell, etc.). La plupart des proxies sont aujourd'hui capables de travailler avec des mécanismes d'authentification tels que LDAP, NTLM, Radius, Kerberos, certificats numériques, etc.

Le contrôle de contenu

Le terme de contenu utilisé ici est générique. Il définit les contrôles possibles sur les flux, entrants et sortants, du port 80 : les virus, les codes mobiles, les flux chiffrés (SSL), le Peer-to-Peer et la messagerie instantanée, le Tunneling HTTP.

Les virus

Au même titre que pour la messagerie internet, le contrôle des virus pour les flux web est un des éléments de base de la sécurité informatique. Il est recommandé, dans la mesure du possible, d'utiliser un logiciel antivirus différent de celui des postes de travail. Le but est en effet d'offrir une complémentarité pour mieux lutter contre les virus. Du point de vue de l'architecture à retenir avec un proxy, une des meilleures approches est celle du protocole ICAP : il permet une intégration fiable et performante avec le proxy.

Les codes mobiles

ActiveX, VBScript, Java, JavaScript sont de plus en plus

utilisés par les applications web. Ces langages apportent un réel plus. Il n'en demeure pas moins qu'employés à mauvais escient ils deviennent redoutables et peuvent compromettre les postes clients. Un moyen efficace de les contrôler est alors de recourir à un logiciel spécialisé dans l'analyse des codes mobiles, couplé au proxy, pour analyser les flux en temps réel. Du point de vue de l'architecture, le protocole ICAP est, là encore, une des meilleures solutions.

Les flux chiffrés SSL – «Man in the Middle»

Comme déjà évoqué ci-dessus, il est fortement recommandé d'analyser les flux avec un antivirus et un logiciel d'analyse des codes mobiles. Mais comment faire avec un flux chiffré (HTTP over SSL)? Celui-ci pose un réel problème dans la mesure où il n'est normalement pas possible d'inspecter son contenu. Alors, que faire? Ne pas examiner ces flux? Les interdire? Ou chercher un mécanisme permettant de les contrôler?

Ce mécanisme, c'est le SSL – «Man in the Middle». Il permet d'analyser un flux chiffré au même titre qu'un flux HTTP en clair. Ce logiciel joue le rôle d'intermédiaire entre un poste client et le serveur SSL : il permet de déchiffrer le flux pour en analyser le contenu et de le rechiffrer ensuite pour l'envoyer au serveur. Cette technique fonctionne très bien et peut facilement s'interfacer avec un proxy, par exemple en utilisant le protocole ICAP.

Le Peer-to-Peer et la messagerie instantanée

De plus en plus, les logiciels Peer-to-Peer et ceux de messagerie instantanée s'appuient sur le port 80 pour communiquer. Cela pose la question de la propagation des virus ou des codes malicieux, mais aussi de

la fuite d'informations au sein de l'entreprise. Dès lors qu'il s'agit de filtrer les communications – afin de les bloquer ou de les restreindre –, le proxy est un outil très efficace, pour autant qu'il soit à même d'analyser de façon très granulaire le contenu du port 80. C'est le cas des proxies de la nouvelle génération qui autorisent, par exemple, l'utilisation des messageries instantanées, tout en bloquant la fonctionnalité du transfert de fichiers.

Le Tunneling HTTP

La technique du Tunneling HTTP consiste à faire passer d'autres applications, telle qu'une «Backdoor», dans le port 80 : un utilisateur mal intentionné ou un attaquant externe peut ainsi faire transiter des informations entre une entreprise et l'extérieur (et inversement). Là encore, un proxy de la nouvelle génération est capable de détecter ce genre de trafic parasite et de le stopper.

L'URL filtering

Un système de filtrage est souvent utilisé pour bloquer l'accès à certaines catégories de sites. Il se peut aussi qu'il soit installé dans l'optique d'une meilleure productivité des collaborateurs. Mais on peut le voir sous l'angle d'un outil de protection, au même titre qu'un antivirus. En effet, certains systèmes de filtrage d'URL sont capables d'empêcher l'accès aux sites susceptibles de contenir des virus ou des codes malicieux pouvant compromettre l'entreprise. Cette méthode est complémentaire à l'approche plus classique de l'antivirus et de l'inspection de codes mobiles.

La journalisation des accès

Enfin, il est recommandé de mettre en place un système de journalisation des accès transitant par le proxy. Utiles pour effectuer des statistiques, ces informations constituent éga-

lement une source importante de renseignements. Ces logs peuvent en effet être utilisés pour détecter des intrusions, retracer une fuite d'informations, etc.

Conclusion

On le voit de plus en plus, le port 80 est et deviendra un des moyens de transport les plus utilisés pour faire transiter de l'information sur Internet. Or, les firewalls classiques ne sont plus à même de le gérer correctement. Il devient ainsi urgent de mettre en œuvre des outils adaptés au port 80, d'instaurer des mécanismes de sécurité offrant une réelle protection pour les entreprises connectées à Internet. Les proxies répondent en grande partie à ce nouveau défi. ●

**Sylvain Maret-Directeur
veille technologique
e-Xpert Solutions SA**

e-Xpert Solutions SA

Au bénéfice d'une longue expérience dans les secteurs financiers et industriels, 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 – tels le firewall, VPN (SSL, IPSEC), 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.

e-Xpert Solutions SA

Chemin du Creux 3,
1233 Bernex-Genève
Tél. : +41 22 727 05 55
info@e-xpertsolutions.com,
www.e-xpertsolutions.com