01 INFORMATIQUE
26 RUE D'ORADOUR SUR GLANE
75504 PARIS CEDEX 15 - 01 44 25 30 01

7 NOV 2003
Hebdomadaire Paris
OJD : 73618

Technologies & services | Testé en entreprise

Dans la peau d'un pirate pour mieux voir les vulnérabilités de son réseau

Auditer la sécurité de son réseau depuis internet n'est pas la panacée. Mais cela permet d'identifier les failles les plus évidentes et les plus aisément exploitables.

EN RÉSUMÉ

En marge des tests d'intrusion, l'audit en ligne de vulnérabilités dévoile les failles d'un réseau telles qu'elles peuvent être vues par un internaute hostile. L'entreprise lance, via internet, un scan sur les adresses IP de son choix. L'outil d'audit, hébergé par l'éditeur, scrute les machines. Un rapport liste l'ensemble des lacunes des systèmes et fournit des préconisations quant aux corrections à effectuer. Ces rapports sont à prendre avec précaution.

La sécurité du système d'information est d'autant plus délicate à contrôler dans le temps que l'infrastructure évolue. La tâche qui incombe aux responsables de la sécurité est donc double. Elle se partage entre la mise en place d'une architecture fiable et son contrôle fréquent. Ce dernier exige un audit des systèmes. En marge des prestations humaines réalisées par des SSII ou des cabinets de consultants en sécurité, les entreprises peuvent avoir recours à des audits en ligne. Une technologie qui a vu le jour à la fin des années 90 afin de compléter le travail de détection d'intrusions. « *J'utilisais un outil d'audit interne, qui me rassurait sur le fait que nos machines semblaient parfaitement étanches* », explique Laurent Muller, directeur général et directeur informatique de la société Alban Muller, fournisseur des industries pharmaceutiques et cosmétiques. L'apport de l'audit en ligne est la vue du réseau depuis internet. « *Un seul scan d'essai de l'outil de Qualys a suffi pour révéler que nos machines n'étaient pas si étanches que cela* », reconnaît Laurent Muller.

L'audit en ligne joue le rôle d'un juge de paix

A la suite du scan, le responsable de sécurité obtient un rapport des vulnérabilités dévoilées. En fait, ce document qualifie l'état de ce qu'un « *internaute hostile peut déceler depuis internet, et donc les failles potentielles qu'il pourrait exploiter* », précise Stéphane Kersulec, directeur télécoms, réseaux et bureautique du Club Méditerranée. Ce dernier utilise l'audit en ligne de la société d'origine rennaise Intranode, à la fois pour tester son accès internet et pour mesurer la qualité de service du prestataire d'hébergement de ses sites institutionnels. Stéphane Kersulec compte toutefois en priorité sur son expertise et sur celle de ses équipes d'ingénieurs : « *Le service d'Intranode joue le rôle d'un juge de paix.* » Les différents rapports des outils d'audit en ligne livrent des préconisations sur les correctifs à appliquer aux failles détectées.

Tous ceux qui les utilisent préviennent qu'il ne faut pas les prendre au pied de la lettre. « *J'obtiens des commentaires très précis et très*

01 INFORMATIQUE
26 RUE D'ORADOUR SUR GLANE
75504 PARIS CEDEX 15 - 01 44 25 30 01

pertinents sur les vulnérabilités, qui me permettent de bien appliquer un patch », tempère Laurent Muller. Avant de reconnaître que son goût personnel pour la sécurité et sa formation d'ingénieur en électronique l'aident dans sa tâche. « *L'analyse consolidée est indispensable. C'est-à-dire que nous croisons les données du rapport avec la réalité de notre infrastructure et les données obtenues auprès des fournisseurs* », insiste Stéphane Kersulec, qui voit surtout dans l'audit le moyen de s'assurer que les systèmes sont à l'état de l'art.

Des faux positifs à surveiller

Une opinion et un recul partagés par Olivier Pantaléo, directeur de l'activité consulting chez Cyber Networks, société spécialiste des architectures de communication sécurisées, et utilisatrice du service d'Intranode. « *Ces outils restent des automates. Un important traitement humain doit donc venir compléter leur veille.* » Et l'on retrouve les mêmes travers que dans le domaine de la détection d'intrusions : un nombre important de faux positifs. « *Le souci est que ces outils n'effectuent pas de tests intrusifs. Ils ne forcent pas les vulnérabilités. Par exemple, sur la base d'une information récupérée sur la version d'un système d'exploitation ou d'un logiciel, ils vont se contenter de lister l'ensemble des vulnérabilités afférentes. Mais combien seront réellement applicables à l'entreprise cliente ?* » s'interroge Olivier Pantaléo. Seule l'expertise humaine distingue le faux positif. D'ailleurs, ces outils n'ont pas servi, dans les cas présents, à remettre en cause l'infrastructure. Notamment en ce qui concerne le Club Méditerranée, une structure qui dispose en interne de compétences pour sécuriser suffisamment en amont son réseau. D'ailleurs, d'une fréquence hebdomadaire, l'entreprise est rapidement passée à des scans mensuels, entrecoupés d'interventions ponctuelles du personnel en charge de la sécurité des zones démilitarisées. La PME Alban Muller a, quant à elle, revu la configuration de certaines machines. Et elle réserve particulièrement ses scans aux modifications opérationnelles de l'infrastructure. « *C'est alors un bon garde-fou* », résume Laurent Muller.

Christophe Dupont

STÉPHANE KERSULEC, directeur télécoms, réseaux et bureautique du Club Méditerranée

« Le dernier patch à la mode est une tendance dont il faut se méfier »

▸ CLUB MÉDITERRANÉE

- **Activité :** groupe de tourisme.
- **Localisation :** 330 sites dans une quarantaine de pays.
- **Effectif :** 22 000 salariés.
- **Chiffre d'affaires 2002 :** 1,74 Md€.
- **Technologie :** Activesentry Web

OLIVIER PANTALÉO, directeur de l'activité consulting de Cyber Networks

« Il faut valider l'information que remonte l'audit »

▸ CYBER NETWORKS

- **Activité :** intégration et conseil en architectures de communication sécurisées et en environnement collaboratif.
- **Localisation :** Suresnes, Lyon, Nantes.
- **Effectif :** 85 personnes.
- **Chiffre d'affaires 2003 :** 13 M€.
- **Technologie :** Activesentry Web pour des prestations d'audit auprès de ses clients.

01 INFORMATIQUE

7 NOV 2003
Hebdomadaire Paris
OJD : 73618

26 RUE D'ORADOUR SUR GLANE
75504 PARIS CEDEX 15 - 01 44 25 30 01

LAURENT MULLER, directeur général et directeur informatique d'Alban Muller International

« L'audit m'assure que les failles les plus évidentes sont corrigées »

► ALBAN MULLER INTERNATIONAL

- **Activité :** conception de produits pour les industries de la beauté et de la santé.
- **Localisation :** Vincennes, Montreuil et Chartres.
- **Chiffre d'affaires 2002 :** 20 M€.
- **Technologie :** Qualysguard, de l'Américain Qualys pour auditer une douzaine de serveurs et un réseau de cent postes.