Réseaux & Télécoms

5 RUE CHANTECOQ
92808 PUTEAUX CEDEX - 01 41 97 61 61

NOVEMBRE 2003
Mensuel
OJD : 26312

Tester et traiter les vulnérabilités : pas simple !

Premiers pas pour se protéger des attaques : connaître ses points faibles. C'est le rôle des outils et des méthodes d'audit de vulnérabilité. Est-il raisonnable de leur faire confiance à 100 % ? Faut-il automatiser les politiques de sécurité ou les faire à la main ? Quelle est la robustesse de la sécurité ainsi «fabriquée» ?

Les méthodes sérieuses d'audits de vulnérabilité accompagnent toujours leurs actions automatisées (scan de port…) de tentatives «manuelles» d'intrusion dans le système d'information et comptent sur des spécialistes «humains» pour optimiser les tests en les adaptant, à la volée, au profil de l'entreprise auditée. Mais, dans la majorité des cas, c'est plutôt le prêt-à-porter qui est préconisé et utilisé : des outils d'audit automatisés tels ceux de Qualys, ISS ou Vigilante.

Qualys s'est tout d'abord penché sur la façon dont les problèmes de vulnérabilité sont résolus. Quatre points en ressortent. Tout d'abord, une entreprise met environ trente jours pour qu'une vulnérabilité critique soit corrigée sur 50 % de ses systèmes ; il se passe environ soixante jours pour que le code d'exploitation soit mis sur Internet pour tous. Ensuite, il faut compter avec l'arrivée de nouvelles machines au sein de tout parc micro – des machines installées de façon «brute», possédant à peine un niveau adéquat de «service pack». S'ajoute à cela la reconfiguration d'autres systèmes, ceux que l'on réforme et que l'on réaffecte à une autre fonction… autant de mouvements qui rendent immortelles certaines vulnérabilités. Dernier point, l'extrême rapidité à laquelle se succèdent les problèmes : la liste des dix vulnérabilités les plus critiques à un moment précis est, en moins de douze mois, remplacée à moitié par d'autres défaillances.

C'est ainsi que la tendance de l'audit de vulnérabilité pousse aujourd'hui les acteurs à proposer de nouvelles fonctions (en plus des listes de systèmes «à corriger», «non corrigés» et «en cours de correction») pour les aider à pallier les vulnérabilités détectées par leurs produits. Qualys a inséré une sorte de *workflow* qui permet de tracer le traitement de la vulnérabilité, mais aussi de prévenir au sujet de ladite vulnérabilité et du temps imparti pour la résoudre.

L'outil d'audit, un lien pour les correctifs

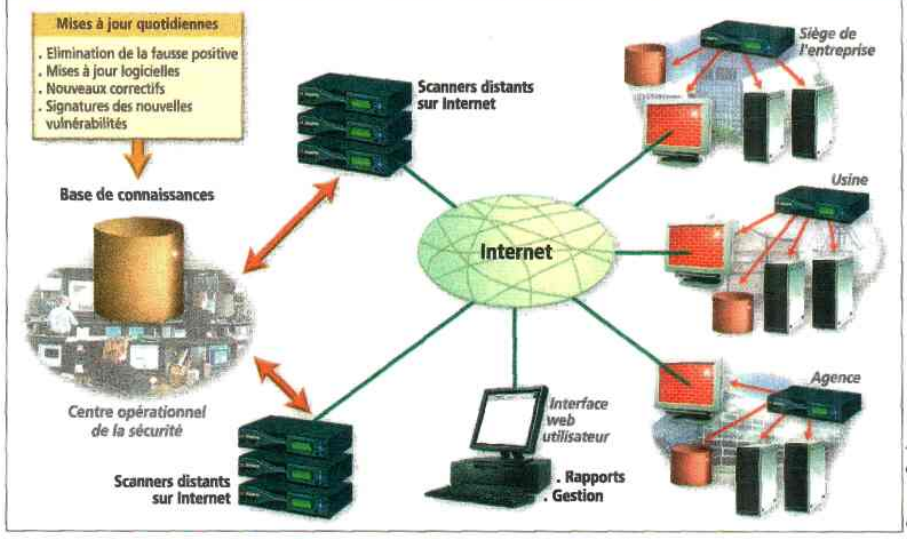
Sinon, dans le domaine de la prévention, il peut arriver que le correctif ne soit pas encore émis. C'est généralement l'outil d'audit de vulnérabilité qui fait le lien avec le fournisseur de déploiement de correctifs. Il en existe un bon nombre sur le marché, outre ceux proposés par les fournisseurs de systèmes d'exploitation eux-mêmes comme Microsoft ou Novell. On retrouve également les éditeurs de plates-formes d'administration, tels Computer Associates, Tivoli/IBM, Openview d'HP, aux côtés de ceux qui se sont spécialisés dans ce segment, tels Landesk ou Marimba. Les éditeurs d'outils d'audit de vulnérabilité fournissent en général à ces derniers les informations nécessaires pour effectuer le déploiement mais ne prennent en aucun la responsabilité de l'effectuer.

On détecte d'abord, on déploie ensuite, mais entre ces deux phases doit se dérouler une étape d'une importance capitale : le test de non-régression ou, en termes plus simples, vérifier si le correctif à bug ne comporte pas de bug lui-même ou n'entre pas en conflit avec une configuration particulière que n'aura pas su voir l'éditeur-auteur de rustine.

Cette «gestion de *patches*» est aujourd'hui un grand sujet de polémiques. Il est en effet quasiment impossible d'automatiser cette tâche.

"Prévenir au sujet de la vulnérabilité et du temps imparti pour la résoudre"

LE TRAITEMENT DES VULNÉRABILITÉS ET "PATCHES" SELON QUALYS

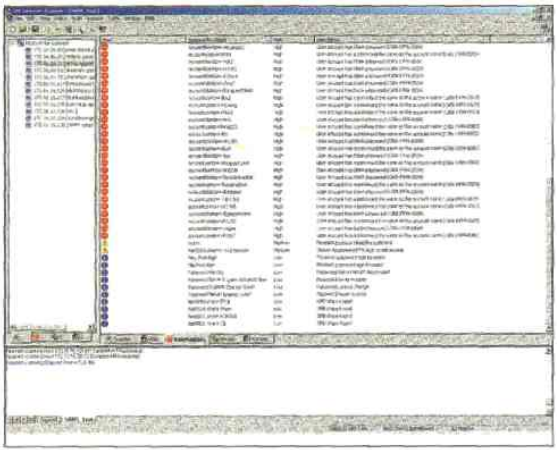


Une base de connaissance externalisée permet de gérer au quotidien les informations de sécurité.

Réseaux & Télécoms

5 RUE CHANTECOQ
92808 PUTEAUX CEDEX - 01 41 97 61 61

NOVEMBRE 2003
Mensuel
OJD : 26312



D.R.

Internet Scanner, d'ISS. La détection de vulnérabilités est une première phase. Suit en général le déploiement des *patches* adéquats… ce qui crée d'autres soucis.

Microsoft a beaucoup été critiqué pour le manque de fiabilité de son OS, mais également pour sa politique de gestion de *patches*, jugée trop compliquée, comprenant parfois autant de méthodes de déploiement qu'il existe de familles de logiciels ou de tailles de réseau : exécutables ou fichiers MSI, Windows Update ou serveurs SUS… la solution unique promise, tant au niveau de la «normalisation» des correctifs que des automates d'application, se fait encore attendre.

Cela laisse la part belle à d'autres acteurs tel Shavlik, dont Microsoft a d'ailleurs diffusé une version «limitée» de son principal outil. Shavlik propose HFNetChkPro4, qui n'exige ni installation d'agent, ni partie cliente sur le poste destinataire.

Egalité dans l'imperfection

Sur le territoire français, on retrouve aussi Marimba. Comme certains de ses concurrents, Marimba contrôle l'intégrité du poste de travail après le déploiement. Il se sert des protocoles HTTP et HTTPS pour effectuer la distribution. C'est le client, une fois n'est pas coutume, qui prend contact avec le serveur le plus proche géographiquement. Il peut être de n'importe quel type, PC, PDA…, et peut utiliser des lignes RTC comme les réseaux sans fil.

Quel que soit l'OS considéré, il est susceptible de comporter des trous de sécurité, et l'actuelle campagne d'opinion qui vise Microsoft ne doit pas faire oublier que la faille existe aussi chez ses concurrents : Linux, Oracle, Cisco… tout le monde publie chaque semaine un bulletin d'alerte. Cette égalité dans l'imperfection implique autre chose : le marché des *assessment tools* et des diffuseurs de correctifs ne peut se contenter des outils «propriétaires» d'un Microsoft, d'un Oracle ou d'un Novell, capable de ne diffuser que les correctifs d'un Microsoft, d'un Oracle ou d'un Novell. Dès que le réseau devient un peu complexe – c'est le cas de celui d'une PME de deux cents postes –, il faut avoir recours à des offres d'éditeurs spécialisés, qui seuls proposent des outils généralistes ou capables de s'adapter parfaitement à la topologie du réseau de leurs clients. Pourtant, malgré les alertes de ces derniers mois, le «succès» rencontré par des virus exploitant des failles connues prouve que l'indispensable outil à déployer du *patch* est loin d'être aussi populaire que l'antivirus.

Solange Belkhayat-Fuchs