Les etapes de la mise en securite

B. Boutherin

sommaire

L'Informatique Professionnelle n° 220 janvier 2004

DOSSIER SPÉCIAL SÉCURITÉ

L'INFORMATIQUE PROFESSIONNELLE

Mensuel publié par Gartner
Tél. 01 71 01 31 00
Fax 01 71 01 32 32

COMITÉ ÉDITORIAL :
Jean-Pierre Corniou
Olivier Le Gendre
Catherine Leloup
Jean-Claude Maury
Christian Morfouace
Jacques Pantin
Pierre Lora-Tonet
André Schwob
Serge Yablonsky

DIRECTEUR DE LA PUBLICATION :
Norbert Miconnet

RÉDACTEUR EN CHEF :
Jean-Marc Berlioux (1502)

RÉDACTEUR EN CHEF DELEGUE :
Jean-Michel Atzel

GESTION DES ABONNEMENTS :
OCIFAM
34 quai de l'aisne
93500 Pantin
Tel. : 01 41 83 52 78

SIEGE SOCIAL :
Gartner
Immeuble Triangle de l'Arche
9-11, cours du Triangle
92937 Paris La Défense cedex
Tél : 01 71 01 31 00
Fax : 01 71 01 32 32

TARIFS ABONNEMENTS :
France 410 € (tva 2,10 %)
Hors France 430 €

ISSN 0750-1080
Commission Paritaire 61050
RC 350 624 102
SARL au Capital de 162 000 €

IMPRIMEUR :
Imprimerie Moderne de Bayeux
7 rue de la Résistance
BP 133
14401 Bayeux cedex
Tél. 02 31 51 63 20

CRÉDIT PHOTO :
Man sneaking with top secret bri
Photodisc collection

Edito

J.M. Atzel

Tous coupables !

Signe des temps, la sécurité sera encore en 2004, la priorité numéro un des organisations en général et des Directions des Systèmes d'Information en particulier. On voit mal d'ailleurs comment, dans un monde troublé où la violence fait quotidiennement la une de nos journaux, il pourrait en être autrement.

Omniprésents et accessibles de partout, les systèmes d'information, qui sont devenus essentiels à l'activité économique voire à la survie des entreprises, constituent bel et bien une cible de choix pour tous les terroristes en herbe et leurs aînés, pirates et brigands professionnels.

Attaqués de toutes parts par jeu, par défi ou par vengeance et volonté de nuire, les systèmes d'information doivent ainsi se prémunir contre les attaques rangées des hackers, spammers et autres cyberterroristes du monde entier, qui profitent des failles des réseaux et du manque de vigilance des gardiens de l'intégrité pour porter leurs coups.

Pourtant, malgré les dégâts causés et les effets médiatiques redoutables de ces agressions commises par les ennemis de l'extérieur, c'est bien du sein même des entreprises que peuvent surgir les attaques les plus dangereuses. La criminalité la plus répandue, la plus pernicieuse et la plus efficace vient en effet de l'intérieur, du collègue désœuvré, dégoûté, anéanti... malade qui préfère nuire à tous que souffrir isolé.

On comprend dès lors que les politiques de sécurité qui ont conduit tout d'abord à créer des enceintes fortifiées à coup de firewalls ou des lignes Maginot enterrées pointées sur l'ennemi de l'extérieur, se retrouvent inopérantes face à des salariés perturbés ou désenchantés.

Que faire alors ?

La réponse, on le sait, est multiple, difficile et intellectuellement peu satisfaisante. Il faut multiplier les contrôles et surveiller. Mais il faut aussi et surtout recréer les conditions d'une effervescence professionnelle collective dirigée vers un même but : le succès de l'organisation grâce à la réussite des femmes et des hommes qui la compose. C'est certes plus difficile à faire que d'installer des firewalls ou des zones démilitarisées mais c'est certainement beaucoup plus efficace.

Ainsi, la sécurité d'une entreprise passe par une appropriation collective des principes et des règles de sûreté. Pour y parvenir, il faut créer les conditions d'une appropriation collective de la stratégie et des objectifs de l'entreprise. C'est à ce prix que l'on pourra faire baisser significativement les risques et les dommages causés.

Dans ce combat collectif, les hommes de la sécurité, les directeurs des systèmes d'information et l'ensemble des responsables au plus haut niveau sont forcément parties prenantes. Certes, le voleur peut être pris et condamné, mais tous ceux qui n'auront pas pris la mesure des dangers finiront, qu'on le veuille ou non, sur le banc des accusés, coupables de négligence, voire d'incompétence. Nous serons donc tous forcément coupables. Mais avant d'être accusés, il faudrait aussi que nous prenions conscience de notre propre responsabilité.

Jean-Michel Atzel

RESEAU LINUX

Les étapes de la mise en sécurité

Linux a atteint une maturité suffisante pour être l'un des éléments clefs sur lequel repose la sécurité des réseaux. Une large panoplie d'outils disponibles dans le monde du logiciel libre existe. Ces outils peuvent répondre aux exigences les plus fortes en matière de sécurité.

Bernard Boutherin

Responsable Sécurité Informatique IN2P3
Service Informatique LPSC

S'il n'y avait pas de pirate ou pas de vulnérabilité dans les systèmes, il ne serait pas nécessaire de faire de la sécurité. Malheureusement, il suffit de laisser quelques heures une machine vulnérable connectée sans restriction à Internet pour voir cette machine compromise et toucher ainsi du doigt l'ampleur du risque (1).
Il en est de même en regardant les logs du routeur en entrée d'un réseau.

Les scans y sont permanents ! Ces scans peuvent être attribués à la propagation de vers ou à des pirates à la recherche de machines vulnérables. Le scan permet en effet au pirate de déterminer l'existence d'un service vulnérable. Ce service pourra alors être compromis à l'aide d'un exploit trouvé sur Internet (2). Notez au passage que les pirates qui nous attaquent sont rarement des experts de la programmation système comme les hackers. La plupart du temps, ce sont des gamins qui téléchargent un exploit et l'exécutent sans bien comprendre ce qu'ils font!

> « Les systèmes ont été écrits sans vraiment prendre en compte la sécurité »

Quant aux vers, ce sont des automates qui se propagent de manière autonome en enchaînant le scan d'un réseau dont l'adresse a été choisie aléatoirement avant l'attaque proprement dite des machines vulnérables. Sur chaque machine compromise, le vers s'exécute de nouveau pour attaquer un nouveau réseau. La propagation de ces vers augmente donc de façon combinatoire et ils peuvent ainsi contaminer des milliers de machines chaque minute !
Dans ce contexte, malgré l'existence bien réelle des pirates, s'il n'y avait pas de vulnérabilité dans les systèmes (ni dans leur configuration), il serait quand même possible de dormir tranquille. Mais les systèmes sont souvent très imparfaits et ont en général été écrits (ou configurés) en pensant aux fonctionnalités et sans vraiment prendre en compte la sécurité. Résultat : il existe des défaillances dans la plupart des services. La plus commune est l'incapacité à gérer le débordement de mémoire (3).

1/ 1 De plus en plus de sites mettent en place des leurres (honey pot) à l'attention des pirates. Leur objectif est de mieux connaître les outils, les rootkits, utilisés par ces derniers, voire d'en récupérer les sources afin de les analyser. Cela est également un bon moyen pour être au courant des attaques du moment afin de focaliser son attention sur les services sensibles. 2/ L'exploit est un programme, écrit par un hacker (programmeur système de haut niveau) permettant d'utiliser une vulnérabilité présente dans un système, afin de prendre le contrôle de celui-ci. Les exploits sont souvent diffusés sur Internet sur des sites dont c'est la spécialité. 3/ Débordement de mémoire (en anglais buffer overflow). Imaginez un service qui reçoit un argument beaucoup plus long que ce qu'avait prévu le programmeur. Cet argument va écrire dans un endroit imprévu : une zone de mémoire où se trouvait du code. Quand ce code - fourni dans l'argument par le pirate - sera exécuté, un peu plus tard, la machine passera sous le contrôle du pirate!

Linux et les vulnérabilités

Comme pour tout système ouvert, les sources du code de Linux sont à la disposition de tous et en particulier des pirates. On comprend facilement qu'il leur est beaucoup plus facile de trouver des possibilités de buffer overflow dans un code disponible sans restriction que dans un système dont le code source n'est pas public.

Mais ce qui a été la faiblesse de Linux dans ses débuts fait aujourd'hui sa force, car les développeurs de Linux sont désormais très attentifs à cet aspect et nombre de vulnérabilités mises en évidence ont été corrigées au fil des versions. Aujourd'hui Linux est devenu un système qui mérite la confiance des plus exigeants en matière de sécurité.

De plus, un grand nombre de distributions orientées vers la sécurité sont maintenant disponibles sous Linux. Elles proposent des configurations où la sécurité est particulièrement soignée (voir le site http://www.linux.org/dist).

Cloisonner le réseau

En fait, il n'est plus possible de maintenir, avec un effort raisonnable, des machines complètement visibles sur Internet. Cloisonner le réseau devient donc indispensable. Cloisonner, c'est, dans un premier temps, élever une protection en périphérie de l'entreprise ; puis, dans un deuxième temps, entre les différentes zones qu'il aura été possible d'identifier à l'intérieur de l'entreprise. Ces zones seront isolées les unes des autres par des firewalls (boîtes noires qui isolent deux réseaux). La première étape de la restructuration du réseau consiste à identifier les zones et les flux réseau utiles entre celles-ci. Parmi les zones, il y aura toujours une DMZ (DeMilitarized Zone) qui accueillera les machines offrant des services à l'extérieur (voir **figure 1**).

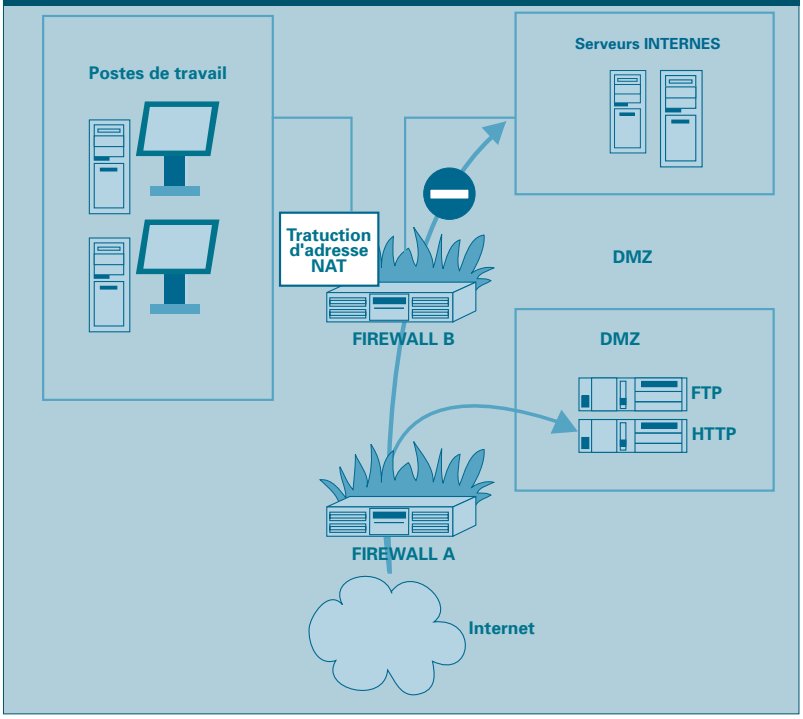
> **Un grand nombre de distributions orientées vers la sécurité sont maintenant disponibles sous Linux**

Visibles depuis l'extérieur, ces machines seront plus exposées et donc potentiellement plus vulnérables. Il sera donc prudent de mettre en place des outils de surveillance efficaces dans la DMZ et de soigner particulièrement la configuration et les mises à jour des services présents dans cette zone.

Le firewall, ne laisse passer que certains services à destination de certaines machines. A partir du noyau 2. 4 Linux intègre Netfilter un outil de choix pour construire un firewall. Netfilter offre toutes les fonctionnalités nécessaires (filtrage avec états, suivi de connexion, traduction d'adresse), pour faire du filtrage réseau.

- Le filtrage avec états. Le pare-feu enregistre les connexions qui le traversent et il est ainsi capable d'accepter un paquet en fonction de son histoire (par exemple retour d'une connexion ouverte depuis l'intérieur) et non pas seulement en fonction de l'état des bits SYN et ACK (4) contenus dans le paquet.
- Le suivi de connexion. Cette technique pousse un peu plus loin le principe du filtrage avec état. Le pare-feu est capable de savoir qu'une ouverture de connexion ftp-data, par exemple, est reliée à une connexion ftp initialisée de l'intérieur.

Figure 1 • Les services accessibles de l'extérieur doivent être placés dans la DMZ



4/ Bits SYN et ACK : l'entête de tout paquet TCP/IP contient 8 bits de statut qui donnent des informations sur l'état de la connexion correspondante. Parmi eux, SYN est positionné en cas d'ouverture de connexion, tandis que ACK (acknowledgment) est positionné si le paquet est une réponse à une connexion précédemment ouverte.

• La traduction d'adresse (NAT). Le NAT (5) permet de masquer la structure interne du réseau à l'extérieur de celui-ci.

La configuration de Netfilter est effectuée à l'aide de la commande iptables. Le site de référence sur le sujet est : http://www.netfilter.org

L'administration des systèmes et des services

Le système d'exploitation est le dernier rempart contre les attaques. Un service bien configuré, à jour dans sa version n'introduira pas de faille de sécurité dans le réseau. Il est très important de soigner tout particulièrement la configuration des machines situées dans la DMZ car elles sont accessibles de l'extérieur.

Les règles de base de la bonne administration système relèvent du bon sens :

• il faut automatiser, chaque fois que cela est possible, les installations et les mises à jour pour avoir un parc homogène et facile à administrer ;

• il faut identifier et arrêter les services inutiles (il est même recommandé de les désinstaller).

Se protéger avec le chiffrement

Les techniques de chiffrement permettent de sécuriser les échanges entre les machines à l'intérieur même d'un réseau local ou de faire circuler de manière sécurisée des informations sensibles sur Internet.

> “ Le système d'exploitation est le dernier rempart contre les attaques ”

Les algorithmes de chiffrement peuvent être classés en deux catégories : les symétriques et les asymétriques :

• Le chiffrement symétrique. La même clef est utilisée pour chiffrer et pour déchiffrer les informations transmises. Les algorithmes de chiffrement symétrique sont caractérisés par leur rapidité, ils seront utilisés pour échanger des volumes importants de données. Parmi les algorithmes de chiffrement symétrique on trouve DES, 3DES, Blowfish, AES. Quand il est disponible, il faut choisir l'algorithme AES qui est le plus efficace.

• Le chiffrement asymétrique. Chaque utilisateur (ou plus généralement chaque acteur) possède un couple de clefs, l'une est publique (elle sera diffusée le plus largement possible), l'autre est privée (elle sera gardée secrète). Ce qui est chiffré avec la clef publique ne peut être déchiffré qu'avec la clef privée et réciproquement. Cela permet d'assurer : la confidentialité d'un message en le chiffrant avec la clef publique du destinataire ; et la signature en chiffrant avec sa clef privée personnelle. L'intérêt du chiffrement asymétrique est qu'il limite le nombre de clefs nécessaires. Son inconvénient est sa lenteur. En conséquence, ce type de chiffrement est souvent utilisé pendant les phases d'authentification pour permettre l'échange d'une clef de session symétrique.

Les techniques de chiffrement peuvent être implémentées à plusieurs niveaux dans les couches du modèle OSI.

• Au niveau applicatif. C'est le cas par exemple de l'application client/serveur SSH.

• Au niveau réseau. C'est ce que fait le protocole IPsec, interdisant ainsi les possibilités d'écoute, quelle que soit l'application utilisée. IPsec est couramment mis en œuvre quand on déploie un VPN entre un site et un autre ou entre un site et un utilisateur nomade. Il est plus rare de voir un réseau complet où IPsec est déployé sur chaque poste.

Conseils

- **Impliquer les dirigeants.** Le déploiement de la sécurité risque souvent d'entrer en conflit avec la quête de fonctionnalités, qui est perpétuelle en informatique. Les responsables fonctionnels ne sont pas toujours biens placés pour arbitrer entre des besoins en terme de fonctionnalités et les exigences de la sécurité. C'est pourquoi il est important que la direction d'un site soit impliquée dans la sécurité de celui-ci. En effet, il incombe à la direction d'effectuer les arbitrages nécessaires ainsi que d'assumer les risques encourus.
- **Mettre en place des procédures.** Il est également important que l'entreprise définisse un certain nombre de protocoles pour que les informations nécessaires circulent : identification du ou des responsables ; appartenance à un CERT (voir le site du CERT Coordination Center : http://www.cert.org); diffusion d'avis de sécurité ; reporting des incidents ; mise en place de conventions telle que l'adresse " abuse@ma.petite.entreprise ".
- **Sensibiliser les utilisateurs.** Le maillon faible d'un système informatique est souvent l'utilisateur, dont le comportement peut mettre en péril tout système de sécurité. Il est important que chaque utilisateur soit sensibilisé au risque informatique et ait la connaissance des enjeux de la sécurité pour son entreprise.

5/ NAT : Network Address Translation, la traduction d'adresse consiste à modifier les adresses source ou destination contenues dans un paquet au moment ou il traverse un routeur ou un firewall. Cette technique permet par exemple à un pool de machines d'utiliser une unique adresse IP (celle du routeur) pour sortir sur Internet.

• Au niveau matériel. A ce niveau, on voit apparaître des cartes Ethernet et des modems qui supportent le chiffrement.

Il faut noter que la plupart des attaques sur des outils de chiffrement se font sur leur implémentation (par la recherche de débordement de mémoire par exemple) et non sur le protocole lui-même. Il est donc très important pour un site qui déploierait le chiffrement, par exemple avec l'utilisation de SSH pour ses échanges sur Internet, de mettre à jour ses serveurs régulièrement, en fonction des avis de sécurité en provenance des CERTs (Computer Emergency Response Team). Le déploiement des technologies WIFI est un exemple où la mise en place de solutions de chiffrement (VPN ou SSH par exemple) est indispensable pour limiter les possibilités d'écoute frauduleuse du réseau. Pour en savoir plus, une introduction aux techniques de chiffrement est disponible sur : http://www.rsasecurity.com/rsalabs/faq/index.html

L'authentification forte

Il arrive malheureusement assez fréquemment qu'une intrusion sur un site puisse avoir lieu avec un vrai mot de passe utilisé sur un compte valide. Il suffit pour cela qu'un collaborateur de l'entreprise se soit fait sniffer (6) son mot de passe ou que sa machine personnelle soit compromise.
L'authentification forte permet de se protéger contre cela en associant au mot de passe la nécessité de posséder un objet matériel (carte à puce ou token) sans lequel la connexion ne sera pas possible. Même si le mot de passe de l'utilisateur venait à être écouté, celui-ci ne sera plus utilisable pour une prochaine session. C'est le principe du mot de passe à usage unique (One Time Password).
Les systèmes les plus classiques permettant la génération de mots de passe à usage unique utilisent une séquence pseudo aléatoire, initialisée avec la même souche, sur la calculette que possède l'utilisateur et sur le serveur. Le mot de passe fourni par l'utilisateur et sa calculette est donc compatible avec celui généré par le serveur. D'autres systèmes commencent à se développer permettant de stocker la clef privée d'un utilisateur dans un équipement matériel : le token. Il est doté d'une puce qui effectue les opérations de chiffrement nécessaires pour répondre au challenge proposé en utilisant la clef privée. Cette dernière n'est donc pas vulnérable puisqu'elle n'est jamais chargée dans la mémoire de l'ordinateur hôte ni sur son disque (voir sur ce sujet le site de référence : http://www.ealladin.com/etoken).
L'intérêt de ces tokens est qu'ils peuvent aussi être utilisés pour s'authentifier de façon plus large que les calculettes, par exemple pour signer ou chiffrer des messages électroniques ou encore s'authentifier sur des serveurs Web accessibles par certificat.

> « La plupart des attaques sur des outils de chiffrement se font sur leur implémentation et non sur le protocole lui-même »

Surveiller le réseau

Il est nécessaire d'ajouter aux protections décrites ci-dessus un mécanisme de surveillance permettant de détecter les tentatives d'intrusion réussies ou non sur le réseau. Il faut également être capable de mesurer la robustesse de la politique de sécurité afin de la faire évoluer. La surveillance peut commencer avec une bonne gestion de l'ensemble des traces fournies par les éléments du réseau : logs routeur, logs système et applicatif (syslog sous Unix/Linux).
La mise en place d'un outil de métrologie réseau (par exemple MRTG : http://www.mrtg.org ou RDDtool : http://people.ee.ethz.ch/~oetiker/webtools/rrdtool) est également une étape fondamentale de la mise en sécurité d'un site. Un système de prise d'empreinte système, tel que Tripwire (http://www. tripwire.org), pourra être déployé, en particulier dans la DMZ, afin de réagir très vite en cas d'intrusion. Des outils d'audit tel que Nessus (http://www.nessus.org) pourront être utilisés régulièrement sur les machines sensibles pour valider leur configuration. Enfin, un système de détection d'intrusion (NIDS - Network Intrusion Detection System) permettra de reconnaître la signature réseau d'une intrusion, de la propagation d'un ver, d'un comportement anormal ou même d'un simple scan, et de générer un message d'alerte. Voir le site de snort : http://www.snort.org.

Bernard Boutherin

Bibliographie

Bernard Boutherin, Benoit Delaunay,
Sécuriser un réseau Linux
Paris, Editions Eyrolles, Septembre 2003.

6/ Snif (écoute) réseau : En l'absence de chiffrement, c'est le cas par exemple avec telnet, ftp ou http, les mots de passe circulent en clair sur le réseau. Il est donc facile pour un utilisateur malveillant de prendre connaissance de ceux-ci. Tout logiciel d'analyse réseau, tel que ethereal disponible en standard sous Linux, lui permettra de voir le contenu des paquets qui circulent sur le réseau et donc les mots de passe qu'ils contiennent. Quant aux pirates, ils possèdent des sniffers, logiciels permettant d'extraire uniquement les couples utilisateur/mot de passe !