# RÉCAPITULATIF DES ENJEUX ET DE LA MISE EN PLACE D'UNE POLITIQUE DE SÉCURITÉ DANS UN RÉSEAU INFORMATIQUE

**Richard CHBEIR**

Aucun réseau informatique n'est à l'abri d'une attaque (volontaire ou non) à sa sécurité (Orange book [1]). Installer uniquement un logiciel de sécurité, souvent nommé *firewall* ou pare-feu, qui a pour objectif de protéger notre réseau de l'extérieur n'est pas suffisant. Les statistiques montrent que 60 % des incidents d'attaques et d'intrusions viennent de l'intérieur du réseau (dont 20 % non volontaires et 40 % volontaires) et 40 % de l'extérieur. Cela dit, la protection contre les attaques informatiques doit englober la totalité du réseau. L'objectif de ce papier n'est pas de proposer une nouvelle solution de sécurité, mais plutôt de vous soumettre une étude sur les principaux éléments à prendre en compte lors de la mise en place d'une politique de sécurité contre les intrusions informatiques. Le papier s'articule autours de 3 axes principaux :

- L'identification des enjeux, des risques et des techniques de piratage utilisées.
- Les mesures de sécurité dans un réseau : pour pouvoir se défendre contre les dangers omniprésents. *L'authentification des utilisateurs, leurs droits d'accès, les ports et les services, les outils de sécurité, les audits et les sauvegardes* seront abordés.
- Les principales opérations à effectuer avant et/ou après les attaques.

1. Le livre Orange (Orange Book) est le nom commun de tous les critères d'évaluation de la sécurité des systèmes du département de défense des États-Unis.

## LES ENJEUX ET LES RISQUES

Pour se protéger des pirates❖, il faut connaître les possibilités d'attaques. Aussi, pour se défendre d'elles, il faut commencer par accepter le danger. La mise en place d'une politique (ou plan) de sécurité consiste en :

**L'identification des éléments à protéger** (matériels, logiciels, données, personnes, etc.).

**L'identification des attaques éventuelles** des pirates dont :

- **La dégradation** qui consiste à perturber le réseau informatique via une panoplie de programmes parasites tels que les virus❖, les chevaux de Troie❖, les vers (WORM)❖, les bombes❖, les bactéries❖, etc.
- **L'altération des données** qui s'effectue soit pendant la transmission des données sur un réseau, soit avant leur émission, soit pendant le passage sur un nœud❖ du réseau.
- **L'écoute** qui consiste à surveiller et à intercepter des données soit sur un poste (cheval de Troie❖), soit sur une ligne de communication (sniffer et probe❖).

**Le choix d'une approche de sécurité :** détermine si la sécurité du réseau nécessite de : *ne rien autoriser*, *n'autoriser que*, *autoriser tout sauf, ou tout autoriser*.

**Le choix des moyens nécessaires pour pallier aux défaillances de sécurité** : il s'agit d'acheter le matériel et les logiciels appropriés aux besoins et à la politique adoptée.

## LES MESURES DE SÉCURITÉ

La politique de sécurité doit englober l'ensemble du réseau informatique. La plupart des tentatives d'intrusions peuvent provenir (volontairement ou non) des utilisateurs autorisés. Pour cela, les mesures de sécurité doivent prendre en considération le réseau local, appelé LAN (Local Area Network), et le réseau externe connu sous le nom WAN (Wide Area Network).

❖ Voir annexe pour plus de précisions.

### L'authentification des utilisateurs

Le premier niveau de sécurité à prendre en compte dans un LAN est **l'utilisateur**. Pour accéder aux ressources locales et réseaux, il devra s'identifier grâce à un nom d'utilisateur et à un mot de passe. Chaque utilisateur doit être unique dans son contexte et appartenir à au moins un groupe d'utilisateurs. Certaines règles sont à respecter :

**Le nom d'utilisateur (Login)** doit être significatif pour pouvoir identifier toutes les personnes. Plusieurs méthodes d'identification sont possibles. L'une d'entre elles consiste à associer la première lettre du prénom au nom complet de la personne. Par exemple, le nom d'utilisateur « rchbeir » est utilisé par l'utilisateur Richard CHBEIR. Par ailleurs, chaque système d'exploitation propose des comptes administrateurs (admin sous Novell, root sous Unix [2], et administrator sous Windows) capable de gérer les utilisateurs (création, attribution des droits et des fichiers, etc.).

**Le mot de passe (Password)** doit être personnel et incessible. Certaines consignes peuvent rendre difficiles voire inefficaces les tentatives de connexion des pirates :

- le mot de passe doit contenir au moins 8 caractères dont 2 numériques ;
- le renouvellement périodique (mensuel si possible) du mot de passe ;
- le cryptage des données pour rendre l'interception et la surveillance moins efficaces ;
- la déconnexion et le blocage du système après un certain nombre de tentatives de connexion ;
- l'interdiction de se connecter avec des comptes administrateurs sur des postes non sécurisés.

### Les permissions d'accès

Afin de rendre votre politique de sécurité plus efficace, il faut établir convenablement les droits d'accès des utilisateurs et des groupes. L'installation standard des systèmes d'exploitation (Unix, Windows NT, Novell, etc.) n'est pas sécurisée en soi. Elle nécessite certaines manipu

2. Nous sous-entendons par Unix tous les systèmes qui exploitent la logique Unix (Linux, AIX, etc.).

lations. Quelques points fondamentaux cités ci-dessous peuvent apporter un niveau minimal de sécurité :

**Sécurité des fichiers contenant les mots de passe :** sous les systèmes Unix, deux fichiers sont à prendre en compte : le fichier des utilisateurs et leurs mots de passe : « /etc/passwd », et celui des groupes : « /etc/groups ». Les deux fichiers cryptés sont accessibles à tous les utilisateurs, même « guest » ou « anonyme », sans quoi ces derniers ne pourraient pas se connecter. Ce qui les rend, malgré le cryptage, faciles à pirater. En effet, certains outils permettent de les décrypter. Pour remédier à cela, l'administrateur (root) peut exécuter la commande *« shadow »* permettant de transférer le contenu de ces deux fichiers dans un autre fichier inaccessible aux utilisateurs. D'autre part, sous Windows, la base de registre contenant les paramètres cryptés du système (system.dat) et des utilisateurs (user.dat) doit être protégée. Microsoft propose deux outils : « poledit » et « regedit » qui permettent de manipuler et de personnaliser entièrement le système. A l'aide de ces deux outils, vous pouvez minimiser les risques d'intrusions :

1. En interdisant l'exécution de l'Explorateur Windows, des commandes MS-DOS et les outils de la base de registre (Poledit et regedit).
2. En autorisant l'exécution d'une liste d'applications comme Winword, Excel, etc.
3. En interdisant les modifications des paramètres de configuration (panneau de configuration, imprimante, etc.).

**Attribution convenable des droits d'accès :** dans un LAN, chaque utilisateur doit pouvoir créer et gérer des fichiers et des répertoires dans son espace de travail. Les autorisations d'accès (lecture, écriture, listage, exécution, etc.) aux fichiers et programmes doivent être parfaitement étudiées et installées. Dans une politique standard de sécurité, un simple utilisateur possède, d'une part, son répertoire de travail où il a tous les droits d'accès, et, d'autre part, des répertoires plus restreints appropriés à son activité. Il faut en principe éviter de donner le droit d'installation des programmes, de sauvegarde des fichiers système, de création de compte, d'ouverture des sessions sur le terminal du serveur, aux utilisateurs non autorisés.

**Les ports et les services**

Les ports utilisés par un ordinateur sont aussi des portes ouvertes aux pirates (LAN et WAN). Un port sur un serveur est un point d'entrée logique permettant à un client d'utiliser une application (ou un service). Par exemple, pour afficher la page d'accueil du site « TF1 » sur un navigateur WEB, l'utilisateur se met en contact avec le port 80 du serveur http://www.tf1.fr. D'autres ports existent tels que le port 21 pour le service ftp, 23 pour le service Telnet, 25 pour le SMTP, 53 pour le DNS, 80 pour le HTTP, 110 pour le POP3, etc. Les pirates peuvent entrer en contact avec les applications qui « écoutent » les ports associés à chaque service. Les techniques actuelles de piratage utilisées sont multiples :

**Plantage du serveur** : en exécutant des applications non prévues (Telnet sur le service Ftp), ou en exécutant un nombre de demandes qui dépassent la capacité du serveur.

**Accès indirect** : en se servant de la faiblesse de certains protocoles. Par exemple, le protocole réseau NetBios sous Windows permet d'accéder au disque local de la machine. En effet, cela s'avère dangereux puisque l'accès à la base de registre est ouverte.

**Contourner les applications :** en exécutant des applications non prévues, ou en accédant aux privilèges (droits) administrateurs nécessaires pour faire tourner tel service.

Pour remédier à cela, quelques manipulations sont primordiales :

- suppression des services non utilisés,
- audit des connexions sur les ports utilisés,
- attribution des privilèges appropriés aux services (pour éviter qu'ils fonctionnent avec des privilèges d'administrateur ou d'invité).

**Les outils de sécurité**

L'achat des moyens de sécurité est dépendant de la politique de sécurité envisagée. Il peut s'agir, d'une part, de l'achat de matériel pour l'interconnexion de réseaux (LAN et WAN) comme les routeurs❖, les passerelles❖ et les ponts❖. Il peut s'agir également de l'achat de logiciels de différents types tels que les relais de connexion❖, les relais d'applications❖, les firewall❖, etc. Vous pouvez consulter le site Web

❖ Voir annexe pour plus de précisions.

(http://www.fwl.dfn.de/eng/fwl/fw/fw-prod.html) pour en savoir plus sur les apports de chaque produit et pouvoir les comparer. L'installation de ces produits nécessite des compétences spécifiques.

**Les audits**

La mise en place d'un système de sécurité nécessite la réalisation des audits dans le but de détecter ses éventuelles vulnérabilités. Cela consiste à collecter et à analyser plusieurs informations : login (connexion) et logout (déconnexion), tentatives de prises de droits de l'administrateur, accès aux ports, serveurs demandés, changements de droits, accès invité (guest) et anonyme (anonymous), modifications des services, login échoué, etc. Sous Unix, les commandes **syslogd**, **COPS, audit, ac,** et **sa** permettent de mettre l'écoute sur les processus et les connexions. Sous Windows NT, plusieurs outils d'audits existent, parmi lesquels : « Audit Policy » accessible par « User Manager/Policies/Audit ».

**La sauvegarde**

La sauvegarde de votre système est l'élément le plus important dans la mise en place d'une politique de sécurité. Elle permet de reconstruire votre installation en cas d'intrusion. Il est préférable qu'elle soit effectuée sur des supports variés (cartouche, cédérom, disque dur amovible, etc.). La commande **tar**, sous Unix, est utilisée pour sauvegarder des fichiers sur bandes ou cassettes. Sous Windows, plusieurs outils existent sur le marché (Arcserve, Seagate, Computer Associate, etc.) permettant une sauvegarde automatique sur des supports multiples. Il est très important de vérifier que **le produit choisi soit capable non simplement d'effectuer la sauvegarde du système mais également de le reconstruire entièrement.**

## QUE FAIRE APRÈS L'INSTALLATION ?

La mise en place d'une politique de sécurité ne s'arrête pas à l'installation du système de protection (ou garde-barrière). Il faut : paramétrer votre système, choisir une stratégie de sécurité, acheter le matériel approprié, installer les logiciels avec les compétences pertinentes, tracer les évènements, et sauvegarder les données. Mais cela n'est pas tout. Votre politique de sécurité doit prendre en compte le suivi des mises à jour de(s) logiciel(s). Il est également important de s'informer de l'évolution des nouvelles technologies et des techniques de piratage à travers les publications (news et journaux). En cas d'incident, il faut

prendre plusieurs dispositions. En résumé : décider qui prévenir, évaluer et gérer les dégâts, sauvegarder votre configuration actuelle et reconstruire votre système, remettre en cause et réorganiser votre politique de sécurité, enfin, attribuer les responsabilités.

Richard CHBEIR

**ANNEXE**

- **Pirate :** tout utilisateur qui tente volontairement de contourner un système.
- **Virus :** programme qui se recopie tout seul à l'intérieur d'un autre programme et qui s'exécute dans le but de perturber ou de détruire le système.
- **Cheval de Troie** : programme qui se réfugie dans un autre programme. Il est conçu pour faire croire à l'utilisateur que son programme habituel fonctionne normalement, alors que son objectif est radicalement détourné. Certains chevaux de Troie (comme NetBus) sont conçus pour écouter d'une façon transparente toutes les commandes de l'utilisateur, y compris la saisie de son mot de passe.
- **Ver :** programme solitaire qui se reproduit via le réseau, d'un ordinateur à un autre pour encombrer le système.
- **Bombe :** identique au virus mais qui déclenche son exécution lors d'un évènement particulier et à une date donnée.
- **Bactérie :** programme qui se recopie dans l'ordinateur afin d'exploiter le maximum de ressources matérielles (espace disque, processeur et mémoire).
- **Probe (testeur de réseau) :** logiciel qui émet différentes données (trames et paquets) sur le réseau vers les ports d'une machine afin de trouver ses vulnérabilités. Plusieurs logiciels existent sur le marché (SATAN et ISS) et sont utilisés aussi bien par les pirates que par les administrateurs.
- **Sniffer (analyseur de réseau) :** logiciel qui observe les informations véhiculées sur le réseau. Par exemple : RealSecure, Netmon, et Readsnmb sous Windows, et Tcpdump sous Unix.

- **Pont** : matériel destiné à interconnecter deux réseaux physiques de même type.
- **Passerelle** : matériel destiné à interconnecter deux réseaux physiques de types différents. Elle est souvent nommée *convertisseur de protocoles* car elle permet de traduire des trames différentes (X25 et Ethernet par exemple).
- **Routeur** : passerelle qui se charge aussi de gérer l'acheminement (le routage) d'informations entre les machines de plusieurs réseaux (à condition de connaître leurs adresses).
- **Relais de connexion** : passerelle *logicielle* permettant de filtrer les trames entre deux réseaux. Il permet au réseau LAN d'être invisible de l'extérieur. En effet, une seule adresse (IP) est visible de l'extérieur, souvent celle de la machine, où le relais de connexion est installé. Cela permet à plusieurs machines de se cacher derrière cette même adresse officielle.

  Par exemple, socks, UDP, et Wingate sont des logiciels qui existent sur le marché.
- **Relais d'application ou Proxy :** passerelle *logicielle* entre deux réseaux qui prétend être une application particulière (comme le Proxy Telnet prétend être le serveur Telnet). Le relais d'application de la messagerie électronique, par exemple, stocke les messages sur le disque et un autre processus va retransmettre ces messages à leur destination.

  Par exemple, Microsoft Proxy, W3C HTTP, Internet Gauntlet et Netscape Proxy.
- **Firewall :** installé sur un poste dédié appelé *bastion*, il regroupe les fonctionnalités du relais de connexion et d'application. Il permet aussi de filtrer les adresses entre deux réseaux.

  Par exemple : FireWall-1 (Check Point), Netasq, F100 Lancop F10, et ULTIMATELY Secure Firewall.
- **Nœud** : tout matériel informatique (pont, passerelle, routeur, PC, etc.) capable d'agir sur les données transmises sur un réseau.