

COMMENT METTRE EN PLACE DES SYSTEMES DE SECURISATION?

Les systèmes d'information sont devenus complexes et hétérogènes : des serveurs Unix de constructeurs différents y côtoient des serveurs WNT, ainsi que des routeurs et des commutateurs. Tous ces équipements fonctionnent avec des systèmes d'exploitation de plus en plus variés et complexes et les réseaux viennent interconnecter tous ces éléments entre eux. C'est ainsi que dans chaque élément, chaque système et chaque réseau, se posent de nombreux problèmes de sécurité : il est donc très difficile d'avoir rapidement une vue claire des risques encourus.

■ C'est pour cette raison qu'à l'heure de la mise en place d'un système de sécurisation, il est nécessaire de prendre en compte un certain nombre de règles de base.

D'abord, **prendre son temps**. La mise en place d'une solution de sécurisation d'un système d'information ne s'improvise pas. Il est très important de prendre le temps de comprendre son système, de repérer où sont les failles de sécurité, quels sont les services ou les éléments à protéger, etc. Ces opérations sont le fruit d'un travail soigneux d'analyse des risques : cette tâche ne peut être bâclée. La mise en place d'un système de sécurisation d'un système d'information nécessite donc, en premier lieu, de prendre son temps.

■ **Devancer le besoin**. Comme la mise en place d'un système de sécurisation prend du temps, il est important de devancer les besoins. Attendre le dernier moment met en danger le système d'information. La mise en place d'un système de sécurisation oblige donc les responsables à adopter vis-à-vis du système d'information, une attitude prospective, plus que réactive.

■ **Se former**. La sécurité est une spécialité, elle couvre plusieurs domaines : les droits dans les systèmes d'exploitation, les applicatifs, les règles d'accès dans les routeurs, etc. Une bonne maîtrise des aspects sécuritaires de ces équipements et systèmes est indispensable.

■ **Rester critique**. Le marché de la sécurité présente une offre de produits et de services variés et en constante évolution. Les éditeurs de logiciels ont parfois tendance à créer artificiellement des besoins pour nourrir le marché (le cas des PKI est un bon exemple). Il est donc très important de rester critique vis-à-vis du marché et ne retenir que les produits ou

services dont votre système d'information a réellement besoin.

Autant dire que la mise en place d'un système de sécurisation est un projet sensible qui mérite d'être conduit avec le plus grand soin.

Les deux sens de la sécurité

■ Le premier réflexe, quand une entreprise parle de sécuriser son système d'information, consiste à le protéger contre des attaques provenant de l'extérieur. Elle sait qu'un concurrent ou un simple pirate peut vouloir attaquer son système d'information à partir d'Internet : il est donc important de se protéger contre l'extérieur.

■ En revanche, l'entreprise a moins tendance à se protéger contre l'intérieur. Il est surprenant de constater à quel point les serveurs internes sont exposés, sans protection, à l'ensemble des utilisateurs du système d'information. S'il est vrai que l'écrasante majorité des utilisateurs est honnête, il n'en est pas moins vrai que certaines populations sont susceptibles de porter atteinte aux serveurs internes. Les exemples les plus courants sont les stagiaires, les personnels temporaires ainsi que certains utilisateurs mécontents. Le système d'information doit donc être protégé tant vis-à-vis de l'intérieur que de l'extérieur.

■ Les besoins de services sont également dans les deux sens. Les utilisateurs internes ont besoin d'accéder aux services qui sont à leur disposition sur Internet ou sur l'Intranet d'un partenaire. En même temps, le système d'information doit fournir des services aux utilisateurs d'Internet, à des partenaires dans le cadre d'un Intranet ou encore, à des utilisateurs en déplacement.

■ Si nous descendons plus concrètement au niveau des flux, nous retrouvons une fois de plus cette notion de bidirectionnalité : les protocoles fonctionnent en effet dans les deux sens. Le dialogue entre le client et le serveur est toujours bidirectionnel. Quel que soit le sens d'établissement du dialogue et quel que soit le sens des communications des données, nous voyons que la sécurité du contenu s'applique dans les deux sens de la liaison.

- En conséquence, il faut éviter les solutions qui ne cherchent à protéger qu'un seul côté de la liaison entre le client et le serveur.

Les deux niveaux de la sécurité

- Les systèmes de sécurité agissent à deux niveaux : d'abord au niveau du réseau, ensuite au niveau applicatif.

Le filtrage :

Il consiste à analyser au niveau IP si un datagramme doit passer ou non. C'est une fonction au niveau réseau, qui dans un système d'exploitation est généralement dans le noyau du système. Cette fonctionnalité de filtrage est notamment fournie dans les routeurs et les commutateurs. Le filtrage protège et contrôle tout ou partie du réseau. Il a l'avantage d'être indépendant des utilisateurs et, par ailleurs, il n'est pas nécessaire de connaître totalement le parc des systèmes à protéger pour mettre en place un filtre. Le filtrage peut être en traversée : c'est le cas le plus classique. Dans ce cas, c'est un routeur et/ou un firewall qui remplit cette mission de filtrage. Le filtrage peut aussi être en bout : dans ce cas, il est assuré par un serveur pour contrôler l'accès au serveur lui-même. Les exemples les plus courants sont ceux de TCP_Wrappers sur un serveur Unix, Netfilter sous Linux, IPFilter sous OpenBSD ou le filtrage intégré dans Windows 2000, qui sera plus facile à utiliser dans Windows XP.

- Lors du choix d'un produit de filtrage, il faut vérifier qu'il permet :

• De filtrer :

- Les datagrammes IP en entrée comme en sortie,
- Sur plusieurs interfaces, séparément par interface,
- Sur l'accès à lui-même,
- En fonction des adresses MAC ou X25,
- En fonction des adresses IP sources et destinations,
- En distinguant les datagrammes d'établissement de connexion des autres,
- En fonction du type de protocole au-dessus de IP (ICMP, TCP, UDP, etc.)
- En fonction des numéros de port source et destination, c'est-à-dire des services client/serveur
- En groupant des adresses IP et des n° de port
- En fonction des numéros de service RPC
- En fonction des commandes dans les protocoles

- De permettre des filtres dynamiques
- De ne pas être biaisé par l'optimisation des filtres
- D'être lui-même protégé et sécurisé
- De journaliser :

- Avec une sélection par ligne de filtre
- Avec plusieurs niveaux d'importance
- Une session complète.

- De comptabiliser les datagrammes
- De convertir et traduire les adresses IP
- De détourner les datagrammes
- De dupliquer les datagrammes
- De filtrer sur la session avec des automates d'état
- De créer des tunnels (VPNs) conformes à IPSEC.

Le relaying applicatif :

Un relais se place entre une application cliente et une application serveur. Il est souvent implémenté comme un programme résident en mémoire (démon). Il se comporte comme serveur vis-à-vis du client et comme client vis-à-vis du serveur. Il permet également d'insérer dans le dialogue entre client et serveur une phase d'identification et d'authentification de l'utilisateur. Un bon service de relaying ne doit jamais exiger l'installation d'un logiciel client (ou serveur) spécifique. L'utilisateur doit en effet pouvoir se servir de son logiciel client pour accéder au serveur via le relais. Ceci est également vrai pour le serveur. Le relaying permet aussi de s'assurer que le flux entre le client et le serveur correspond bien à l'application qui est sensée être fournie, par exemple en filtrant au niveau applicatif.

- Lors du choix d'un produit de relaying, il faut vérifier qu'il permette notamment :

• De supporter tous les services demandés par les utilisateurs, ainsi que ceux qui seront demandés dans le futur

- SQLNet v2 et Net8,
- Services audio/vidéo.

• D'authentifier les utilisateurs :

- Systématiquement,
- Pour tous les protocoles relayés, en entrée comme en sortie,
- Sans utiliser une authentification ou identification basée à l'intérieur du réseau,
- Indépendamment de la base de données d'authentification propre au système du serveur de relaying,
- En choisissant le type d'authentification en fonction de la source et de la destination,
- En supportant des authentificateurs de qualité,
- En authentifiant la session cliente et non en identifiant l'adresse IP de la machine source.

• De fabriquer des autorisations avec une granularité permettant l'application de la politique de sécurité :

- Utilisateur authentifié (ou groupe),
- Service demandé,

- Commandes dans le service,
- Machines ou réseaux source,
- Machines ou réseaux destination,
- Heures de connexion,

- **D'être totalement indépendant vis-à-vis des logiciels utilisés par les utilisateurs, côté client comme côté serveur.**

- D'être transparent dès que l'utilisateur est authentifié.
- D'être accessible de manière transparente.
- De s'adapter à des protocoles nouveaux ou spécifiques.

- **De permettre une comptabilité de la consommation Internet pour chaque utilisateur, indispensable à la refacturation en interne.**

- **De ne pas provoquer une perte de performance.**

- **De contrôler les types des documents relayés :**

- Word, PDF, etc
- Code mobile : Java,
- Binaires Intel : ActiveX,
- Archives (zip, etc).

- **De contrôler les contenus des documents relayés.**

- **Macros dans Word, Excel, etc.**

- **Javascript et VBscript dans HTML.**

- **Virus.**

Une solution complète de sécurisation de système d'information se doit d'assurer ces fonctionnalités de filtrage et de relayage. Il faut rejeter toute solution qui ne reposerait que sur une seule de ces deux fonctionnalités.

Choix des équipements

- On trouve sur le marché, deux types de produits qu'on appellera boîtes noires et blanches.

- **Les boîtes noires** sont des systèmes préconfigurés, voire autoconfigurés. Ce sont des systèmes qui ne nécessitent pas, ou peu, d'intervention de la part de l'utilisateur. Ils fonctionnent tout seuls et semblent être des systèmes complets.

En fait, les boîtes noires sont rarement des systèmes complets : elles ne font en général que du filtrage IP sans sécurité au niveau utilisateur. Par ailleurs, il est souvent indispensable de placer un routeur devant elles.

Les produits boîtes noires ne sont généralement qu'un composant d'une solution complète dans laquelle ils doivent être intégrés.

Malgré leur prétention de transparence, les boîtes noires imposent toujours une exploitation et donc, un administrateur compétent. Au bout du compte, elles peuvent revenir beaucoup plus chères à l'usage car

elles ne dispensent pas d'installer et de gérer un routeur en amont, un relais applicatif en aval et d'administrer l'ensemble.

Le cas où les boîtes noires peuvent se justifier est celui des toutes petites structures.

- **Les boîtes blanches** : en opposition aux boîtes noires, on peut parler de boîtes blanches. Il s'agit ici de choisir des produits ouverts, que l'on intègre et administre soi-même.

Ce principe permet de maîtriser la technique et l'architecture conceptuelle de la solution de sécurité. Si l'on choisit par exemple, de configurer soi-même une machine en y installant le système d'exploitation puis un relais applicatif, on garde la maîtrise totale de ce relais. Il est alors possible de le configurer finement en fonction de ses besoins et les modifications d'architecture sont rendues possibles.

Il est important dans ce cas de choisir un fournisseur accessible et que l'on peut influencer pour faire évoluer le produit en fonction des besoins.

Le choix d'un distributeur repose sur sa connaissance du produit. Il est bon de savoir s'il l'utilise lui-même pour ses propres besoins, s'il possède les codes sources et s'il a le pouvoir d'influencer le fabricant.

Il faut par ailleurs que le fournisseur propose des services et qu'il possède la compétence pour les services proposés.

Enfin, il faut dissocier le choix de la sécurité IP avec d'autres choix comme celui de l'opérateur IP : à chacun sa spécialité.

La possession du code source est la seule solution pour être indépendant du vendeur. Elle permet de s'affranchir de la pérennité du fabricant, d'avoir une idée de la qualité de conception et d'écriture du logiciel. La possession du code source permet aussi de s'assurer qu'il n'y a pas de trappe cachée dans le logiciel.

Posséder le code source n'est pas réservé à un petit groupe de sociétés possédant des compétences pointues en C et Unix : les logiciels de relayage sont en effet relativement concis et lisibles. Il est alors possible de contrôler les fonctions du logiciel et la qualité d'écriture.

Architecture d'ensemble

- L'architecture est la combinaison des routeurs et des machines. Il est important de vérifier que le produit a la capacité :

- **De se configurer à l'aide d'un outil interactif et**

convivial, permettant :

- l'écriture de règles de filtrage dans un langage simple (adresses IP et utilisateurs),
- la génération automatique des filtres IP,
- le contrôle des règles de filtrage,
- la surveillance,
- en conservant toujours des fichiers de configuration humainement lisibles.

• De journaliser avec détail :

- en exploitant les journaux produits,
- en générant des alarmes,
- en s'interfaçant avec les outils existants d'administration ou de gestion de réseau,
- en protégeant la journalisation,

• De permettre une gestion à distance en toute sécurité.

D'autres critères sont également à vérifier, notamment la capacité du produit à :

• Supporter une forte croissance en termes de :

- nombre de connexions simultanées,
- nombre d'utilisateurs,
- débit du réseau.

• Supporter des adresses IP privées (RFC 1918).

• Permettre la gestion de plusieurs domaines (exemple : `societe.ca` et `ca.societe.com`).

• Permettre des échanges dans des tunnels sécurisés entre deux passerelles Internet de la même organisation (VPN).

• Ne pas imposer une configuration particulière sur un routeur externe à la solution, comme un routeur télécom ou le routeur de l'opérateur Internet.

Tous les éléments d'un système de sécurisation de système d'information doivent être administrés. Il peut être utile de recourir à des systèmes de configuration et d'administration.

Au moment de choisir un de ces outils, il est recommandé de vérifier qu'ils ont la capacité :

• D'apporter un plus vis-à-vis de l'édition de fichiers texte

• De conserver la possibilité d'éditer des fichiers texte

• De permettre une configuration par des scripts automatiques

• D'authentifier les administrateurs individuellement

• De journaliser les actions des administrateurs

• D'aider l'exploitant

• De fonctionner à distance

Par ailleurs, leur champ d'action doit couvrir :

- **Le filtrage IP,**
- **Le relayage applicatif,**
- **Les services Internet,**
- **Les journaux,**
- **La configuration des authentificateurs.**

Compétence humaine

- Quelle que soit l'architecture retenue pour le système de sécurisation du système d'information, il est indispensable d'en maîtriser tous les éléments.

La surveillance du système est un aspect stratégique de la sécurité. Il est tout à fait inutile d'investir des sommes considérables si, une fois le système mis en place, personne ne le surveille.

Il est donc nécessaire que les administrateurs aient les connaissances suffisantes pour configurer, administrer et surveiller chaque élément (routeur, système d'exploitation, relais applicatif etc.).

Les procédures de sauvegarde et d'analyse des journaux doivent être clairement formalisées et testées. En fait, le niveau de sécurité dépend avant tout :

- **de la compétence des administrateurs,**
- **de la disponibilité réelle et garantie des administrateurs,**
- **de la rigueur de travail des administrateurs,**
- **de leur travail de veille,**
- **de leur capacité à s'auto-former,**
- **du formalisme de leur travail,**
- **du contrôle du niveau d'administration et du respect des règles de sécurité dans le temps.**

Conclusion

- Nous avons vu que la mise en place d'un système de sécurisation est un projet sensible. Une fois opérationnel, ce système doit être administré par un personnel compétent. Il faut en tout état de cause, préférer les solutions que l'on maîtrise complètement, aux solutions opaques. Un système de sécurisation doit être régulièrement remis en cause et mis à jour en fonction de l'évolution des services. En fait, un système de sécurisation de système d'information est un système vivant : il faut l'installer, l'administrer puis le faire évoluer.