Sécurité des réseaux

Introduction

Lors de la mise en place d'un réseau informatique, il est nécessaire de penser la sécurité dans son ensemble :

- dangers liés à l'usure ou aux défauts matériels (destructions, pannes, obsolescence…)
- dangers liés à l'utilisation de l'outil informatique par les utilisateurs (destruction, diffusion, fuite, virus, …)
- dangers liés à l'ouverture du réseau sur l'extérieur (piratage, blocages, destructions, …)

Si quelques règles de base sont impératives pour limiter les risques, il n'est pas de solution universelle. Le seul bon investissement dans un système de sécurité est celui qui répond à la question : « si le risque encouru venait à se réaliser, cela coûterait-il moins cher que l'achat préalable d'un système de sécurité ? ». C'est pourquoi il est important de connaître les risques potentiels et les solutions du marché pour s'en protéger.

I Préambule : Les risques et les parades

Les dangers de l'informatique sont innombrables, mais ils relèvent de quelques principes toujours identiques pour lesquels les solutions offertes sont assez circonscrites. Nous allons évoquer les différents risques et lister (de manière non exhaustive) les parades possibles.

1.1 Destruction de données

L'information produite par l'entreprise, qu'elle soit du domaine comptable et financier, commercial, productif, technologique ou analytique, est aujourd'hui un élément vital souvent dématérialisé sur un support de stockage.

Enjeux Assurer une sauvegarde fiable des informations répond à plusieurs objectifs : une obligation juridique exige la conservation de certaines informations sur des périodes plus ou moins longues ; l'information construite au fur et à mesure de l'évolution de l'entreprise constitue une histoire, une mémoire qui permet d'envisager l'avenir en s'appuyant sur le passé ; enfin, la disponibilité de l'information aux différents niveaux de la hiérarchie permet une communication élaborée, un suivi immédiat, une capacité d'analyse dont l'entreprise ne peut se passer. Source de risque

Aussi est-il indispensable de se prémunir contre les dangers d'une disparition de l'information, due :

- aux événements climatiques (inondation, tempête, …) ou autres catastrophes (incendie, effondrement de bâtiment, …)
- aux manipulations malencontreuses des utilisateurs (« oups ! j'ai supprimé le répertoire au lieu d'un fichier »)
- aux attaques extérieures visant à nuire au fonctionnement de l'entreprise

Parades

La première des mises en œuvre impérative est la sauvegarde des informations sur un support qui sera stocké en dehors du lieu de leur production. Cette sauvegarde sera associée à une politique adaptée aux besoins (périodicité, rotation, contenu, ...).

On s'assurera aussi de limiter les accès des utilisateurs en fonction de leur profil et de leur besoin, qu'il s'agisse de l'exploitation de fichiers dans un répertoire (permissions et ACL) ou d'accès aux tables des bases de données (GRANT).

On protègera les accès externes en limitant au maximum les possibilités d'intrusion sur le réseau et en limitant les portes ouvertes sur l'extérieur au strict nécessaire (Filtrage).

Enfin, on pourra assurer une duplication à chaud de l'information pour pallier sa destruction (RAID, Cluster).

1.2 Défaut de fonctionnement du système

Si l'informatique a été mise en place dans l'entreprise, l'objectif est bien que les utilisateurs puissent travailler en collaboration, avec les outils adaptés, tant dans la production et l'enregistrement de données utiles que dans l'accès aux outils de communication interne et externe.

Enjeux

La panne d'un service réseau, d'une application, d'une machine, peut aller de la simple immobilisation temporaire de quelques individus à la paralysie totale de l'activité. Il est donc nécessaire de s'assurer que l'entreprise dispose de la capacité à réagir et réparer promptement une panne, qu'elle ne soit pas totalement dépendante de l'outil informatique ou qu'elle dispose d'un système redondant permettant de basculer sur un service de secours.

Source de risque

Il peut s'agir de la simple panne d'un disque dur ou d'un matériel (serveur, matériel réseau), d'un défaut de fonctionnement électrique, de l'effondrement d'un matériel par manque de capacité, ou d'une attaque visant à rendre un service indisponible (déni de service) en procédant par des envois massifs d'informations (*flooding* ou *inondation*), par le blocage d'un programme en lui adressant des messages mal formés (*ping de la mort*) ou par la saturation des matériels réseau.

Parades

La sécurité minimum consiste à mettre en place des systèmes à tolérance de panne ou à redondance :

- Onduleur pour l'électrique
- RAID pour les données
- Multiprocessing pour les capacités de traitement
- Serveurs secondaires pour les fonctions de base (authentification, DNS, sauvegarde, etc)
- Liens redondants ou de liens de secours pour les accès inter-site (ADSL + RNIS).
- Clustering de serveur pour les fonctions lourdes (base de données, gestion, exploitation, etc)

Ensuite, on veillera à dimensionner les composants en fonction des besoins et à assurer la surveillance de leur bon fonctionnement (SNMP, sondes, ...) et à segmenter les réseaux.

On se protègera aussi des accès malveillants en établissant une politique de sécurité (filtrage,

paramétrage des matériels d'interconnexion,...) , de veille technologique (nouveaux virus, failles, etc) et de surveillance (analyseurs, scanners de port, anti-spyware,...).

Anticipation

Dans l'éventualité d'une destruction du système, les entreprises peuvent entreprendre une démarche d'inventaire préalable et de mise en place de procédures pensées à l'avance. On parlera d'un Plan de Reprise d'Activité (PRA), qui identifiera les sources de risque et les classifiera des plus anodines aux fonctions critiques. Pour les risques les plus dangereux, on définira les systèmes de prévention qui empêchent leur survenue (redondance, isolation, etc), et les procédures de réaction urgentes à mettre en place le cas échéant (relance d'un système distant, restauration de données, etc).

On parle même de Plan de Continuité d'Activité qui vise à empêcher toute interruption des services, quel qu'en soit le coût et quitte à fonctionner en mode dégradé. Ce document précisera alors toutes les situations de crise possible, les éléments de redondance à prévoir et les procédures de basculement sur le système de secours.

Dans certains secteurs (santé, banque, etc), les assurances exigent que de telles pratiques soient mises en place sous peine de ne pas rembourser l'entreprise insouciante.

1.3 Espionnage

La plus grande vulnérabilité est à l'intérieur de l'entreprise, volontairement ou non. Mais l'extérieur n'est pas exempt de danger. On parlera notamment du social engineering (Ingénierie sociale qui consiste à acquérir des données privées en manipulant des personnes, par tromperie...) ou de l'espionnage industriel.

Enjeux

Si l'information de production est sensible, elle ne l'est pas autant que toute l'information stratégique (plans d'actions, courriers internes, objectifs, ...), technologique (brevets, recherche, savoir-faire,...) ou financière (bénéfice ou pertes, plans d'investissement, salaires,...) qui pourrait intéresser aussi bien la concurrence que les partenaires de l'entreprise.

Source de risque

On pourra parler de choses triviales comme la diffusion des salaires des dirigeants, des tentatives d'accès à des données non autorisées ou de la diffusion des mots de passe entre utilisateurs et aller jusqu'à l'espionnage organisé (Business intelligence), tentatives d'introduction sur le système, d'accès à des informations confidentielles par vol de mot de passe ou de matériels mobiles, d'analyse des échanges réseau (internet)...

L'usurpation d'identité d'un utilisateur (mail), afin de recevoir des informations destinées à un autre, ou l'usurpation d'adresse IP (machine) dans le but de s'introduire sur le réseau en se faisant passer pour un autre matériel, sont des pratiques courantes dans le monde industriel.

La technique du *phishing*, répandue autour des sites bancaires notamment, consiste à rediriger un utilisateur vers un site fictif ayant toute l'apparence du site officiel mais ayant pour but de capturer des informations d'identification.

Les *keyloggers* sont des logiciels de type cheval de Troie qui s'installent sur une machine et se

chargent de capturer toutes les frappes de touches au clavier dans le but d'intercepter des mots de passe.

Parades

La première étape est la sensibilisation des utilisateurs aux dangers de l'utilisation des outils, de la diffusion de l'information, de la diffusion des mots de passe et de la vérification des sites visités ou des mails reçus qui installeront les logiciels espions.

On pourra aussi mettre en œuvre des techniques de filtrage (sur des mots-clés sensibles, sur des services particuliers type mail ou FTP, sur les autorisations d'accès en entrée ou en sortie) et de log en enregistrant les échanges produits par les utilisateurs grâce à un proxy.

L'utilisation de techniques de cryptage et de signature électronique permettront de s'assurer de la confidentialité des échanges et de l'identité des individus.

L'isolement de l'adressage interne par le recours à un adressage privé et au NAT (Network Address Translation) permet de se prémunir contre l'usurpation d'IP.

Pour les attaques plus sournoises, de type phishing, on pourra former les utilisateurs à l'utilisation des navigateurs internet, notamment dans le repérage des sites sécurisés (cadenas et https).

Bien entendu, les antivirus et antispyware seront mis à contribution pour la prévention de l'introduction d'outils malveillants (malware).

1.4 Virus

Dernières des fragilités du système, elle est aujourd'hui la plus souvent mise à mal car c'est par son biais que se font la plupart des attaques extérieures citées plus haut.

Enjeux

La protection contre les virus s'est largement accrue depuis l'avènement de la messagerie et des accès internet. Les virus, plus ou moins malveillants, peuvent aller d'un simple message d'infection ou d'activités anormales (affichages intempestifs, modification de l'environnement, etc) jusqu'à l'immobilisation complète du système, voire la destruction de données.

S'en protéger ne vise plus à simplement éviter quelques nuisances mais à assurer le fonctionnement normal, permanent d'un système.

Source de risque

INTERNET !!!! Si auparavant la disquette était le point le plus surveillé, c'est aujourd'hui de l'internet qu'arrivent les innombrables versions de virus, que ce soit à travers les sites malveillants introduisant des *spywares* (portes dérobées), les *vers* qui se propagent par la messagerie, les macro-commandes dans les fichiers bureautique, etc.

Les clés USB sont une nouvelle source d'introduction de pollution informatique.

Parades

En plus de la mise en place d'un antivirus centralisé avec des mises à jour régulières et distribuées

sur les postes clients, il faudra aussi :

- Sensibiliser les utilisateurs au bon usage du mail, à la prudence avec les pièces attachées.
- Interdire ou limiter l'utilisation de la messagerie, ou l'introduction de pièces attachées.
- Désactiver les macro-commandes dans les outils bureautiques.
- Surveiller les ports en activité sur les machines, interdire les ports d'attaque standard.
- Désactiver éventuellement les ports USB pour interdire les ajouts de périphériques externes (clés, lecteurs divers)
- Mettre en place des outils de type *anti-spyware*.

II Le problème des accès distants

Enjeux

Si les consignes précédentes s'appliquent indifféremment dans le réseau local ou dans son ouverture vers l'extérieur, ce sont les accès distants qui exposent le plus le système informatique à des dangers incontrôlés. On peut en effet plus facilement limiter les fonctions réseau mises en place dans une infrastructure locale maîtrisée qu'empêcher l'utilisation de ces fonctions par l'extérieur.

En outre, les éléments utiles mis à disposition des utilisateurs externes (site web, messagerie, etc) peuvent devenir des sources potentielles d'attaque et d'intrusion.

On devra d'une part se protéger des entrées cherchant à :

- s'approprier l'information de l'entreprise par capture de contenu, intrusion ou espionnage
- détruire l'information de l'entreprise par les intrusions et les virus
- rendre impossible l'utilisation des ressources réseau par déni de service
- s'approprier les identités machine ou utilisateur par usurpation

Il faudra aussi se prémunir des utilisations internes frauduleuses risquant :

- d'engendrer une fuite d'information par diffusion de mots de passe ou transmission de données confidentielles
- de gaspiller le temps de travail pour des utilisations extra-professionnelles (sites internet, jeux, messagerie personnelle et instantanée, etc)

TCP/IP : le cœur du problème

Avec l'utilisation du standard TCP-UDP/IP, les entreprises ont gagné en simplicité et en pérennité dans la mise en place des réseaux locaux et étendus.

Aujourd'hui, toutes les offres permettent en effet la compatibilité ou l'encapsulation du flux IP de manière à garantir une communication sur un protocole unique de bout en bout, quels que soit le chemin et les réseaux empruntés, y compris jusqu'au transport de la voix.

Rançon du succès, ce protocole universel et ouvert est, comme Windows pour les systèmes d'exploitation, la cible privilégiée des pirates, hackers, crackers et autres fouineurs. IP est en effet un protocole non sécurisé qui permet à un espion à peine compétent de lire en clair les adresses IP des émetteurs et destinataires, d'en usurper l'utilisation ou d'étudier le contenu complet du datagramme (donc les mots de passe de haut niveau).

Parades et modèle OSI

Les techniques complémentaires à IP permettant d'assurer la sécurité du réseau vont intervenir sur les différentes couches du modèle OSI, de 3 à 7 :

- en modifiant les adresses internes au réseau (translation d'adresses),
- en opérant une surveillance du trafic (proxy)
- en limitant la communication avec l'extérieur (filtrage par port)
- en autorisant ou non les échanges pour des adresses IP déterminées (filtrage IP),
- en autorisant des types de communication par les ports TCP/UDP correspondant aux services de la couche application (filtrage par port),
- en interdisant certains contenus illicites (filtrage par mot clé),
- en appliquant toutes ces restrictions pour des utilisateurs identifiés (authentification)
- en cryptant le contenu de la trame

En fonction du niveau du modèle OSI auquel ils interviennent, les matériels ou logiciels porteront des dénominations allant du routeur filtrant au pare-feu (firewall).

Conclusion

L'avantage même du réseau par sa capacité à mettre en communication les utilisateurs et rendre l'accès aux données possible indépendamment de l'organisation et la localisation des personnes est aussi son point de vulnérabilité. Une fonction essentielle de l'administrateur est donc de s'informer des failles existantes et de mettre en place les outils de protection et une surveillance complémentaire pour s'assurer que ses outils remplissent bien leur fonction. La sécurité ne s'arrête pas après la mise en place des outils, elle est activité permanente qui nécessite actualisation et veille technologique de la part de l'administrateur.