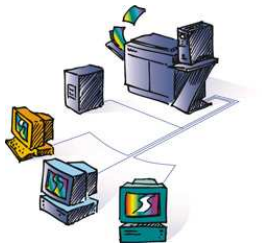
Les services et la sécurité des réseaux



1 Les équipements périphériques en réseau

Dans un réseau, on voit des ordinateurs, connectés entre eux par hub/switch ou routeur.

Mais le reste ?

En réalité, on peut rencontrer divers équipements directement connectés et accessibles par le réseau comme :

Périphérique d'entrée/sortie : imprimante, vidéo projecteur, scanner, caméra …

Périphérique de stockage : disque dur en réseau, unité de lecture/gravure de disque, unités de sauvegarde sur bande, disque.

Ces périphériques doivent disposer d'une carte réseau interne.

2 Les services de réseau

2.1 Notion de client/serveur

On appelle :

- client, l'ordinateur qui réclame et reçoit un service (données d'un fichier, usage d'un périphérique)
- serveur, l'ordinateur qui fournit le service demandé

Serveur et micro-ordinateur sont deux frères ennemis enchaînés sur le même réseau.

Le serveur, objet de toutes les attentions de l'administrateur du réseau, représente l'informatique lourde et centralisée.

Lorsqu'il devient serveur d'applications, le micro-ordinateur se voit réduit au rang de simple terminal.

Le micro-ordinateur, par contre, représente l'informatique libre, créatrice, économique et décentralisée -- mais il a besoin du serveur pour utiliser un périphérique commun ou accéder à une base de données.

A l'heure où les discussions font rage sur le rôle respectif du client et du serveur, rappelons-nous le proverbe de la sagesse paysanne : à chacun son métier, et les vaches seront bien gardées.

2.2 Types de serveurs

Les services rendus par un serveur peuvent être très variés, c'est pourquoi on distingue :

- le serveur de fichiers, de base de données, qui gère une ou plusieurs bases de données
- le serveur d'impression, qui gère la file d'attente des imprimantes du réseau
- le serveur d'applications
- le serveur web, qui met à disposition les pages d'un site web (ou intranet) et tout ce qu'elles contiennent
- le serveur de messagerie (mail), qui stocke les messages entrants, et les tient à disposition des ordinateurs clients
- les serveurs propres à Internet : ftp, Proxy, DNS, etc.

Ces services peuvent être regroupés sur une même machine, ou assurés par des machines distinctes. Dans les arts et industries graphiques, le serveur **OPI** (Open Prepress Interface) est un serveur de fichiers un peu particulier : il stocke les images dans leur version haute résolution pour les envoyer à l'imageuse (imprimante de très haute définition, spécialisée pour la production d'images, prototypes de pub, …), après que le travail de mise en page ait été effectué avec les images en basse résolution.

2.3 Autres services et fonctions diverses

Authentification, Gestion des utilisateurs : service de gestion des droits d'accès aux ordinateurs, aux serveurs, au réseau. Il enregistre les différents mots de passe.

DHCP : attribution automatique d'adresses IP.

Afin de se simplifier le travail et les connexions des postes mobiles, il existe un serveur d'adresses IP pour les postes qui se connectent occasionnellement.

(Par exemple : les commerciaux qui sont toujours en vadrouille sauf le lundi pour le café et le vendredi pour le pot, et sui en profitent pour mettre à jour les données de leur PC en se connectant au réseau. - Ils en profitent, d'ailleurs, pour introduire des virus au passage !!! ;-)

DNS : conversion d'adresses IP en URL

Ce service facilite la connexion à internet aux utilisateurs oublieux que nous sommes tous.

Le serveur de nom de domaine converti les adresses web (comme www.lemeilleurdessites.fr) en adresse IP pour se connecter (10.100.64.13)

Proxy/cache : service d'accélération des accès au web en mémorisant les pages les plus recherchées, sur le serveur web

Pare feu / firewall : logiciel servant à limiter les intrusions en provenance de l'extérieur de la zone protégée (ou zone démilitarisée : DMZ), sur le serveur web.

Cette protection n'est pas toujours suffisante et ne concerne pas les virus !!

3 Sécuriser un système d'information

Pour sécuriser un système d'information, il faut d'abord prendre quelques précautions.

Les maîtres mots sont les suivants :

Confidentialité, intégrité, disponibilité

Ils sous entendent aussi :

L'authentification des utilisateurs et autres acteurs,

La garantie de la vérité portée par ces données,

L'étanchéité des communications aux personnes non autorisées,

La transparence des renseignements fournis

Les actions à mener prendront donc différentes directions :

La sensibilisation des utilisateurs

La sécurité logique des données (logiciel, système d'exploitation, données)

La sécurité des communications

La sécurité physique du matériel

3.1 Sensibilisation des utilisateurs

3.1.1 Sécurité contre les intrusions : confidentialité des données

L'accès aux données doit être réservé aux seules personnes autorisées.

Cet accès peut être défini sur la machine (mot de passe machine) mais il est peu fiable et très localisé.

Serveur d'authentification : on utilisera un logiciel de service de gestion des utilisateurs qui permettra de mettre en place toute une stratégie d'accès aux données, au réseau, aux communications (internet).

Attention, avec ce type de logiciel, vous pouvez aussi espionner vos collègues (ou être par) : heures d'accès au système, pages web visitées, volume de courrier, voire contenu.

Ce genre de pratiques est réprouvé (partiellement) par la loi !...

3.1.2 Sensibilisation

De proche en proche, de connaissance en connaissance, il faut au maximum 14 personnes pour allez de n'importe qui en France, jusqu'au président de la république.

Donc si vous diffusez votre mot de passe, rien n'empêchera quelqu'un de mal attentionné de l'utiliser pour détruire vos données, se servir de votre compte sans votre accord pour des actions répréhensibles par la loi, voire d'effectuer des transaction à votre nom…

Un secret partagé n'est plus un secret.

Pour éviter cela, il est possible de mettre en place une stratégie de mots de passe où, à intervalles régulier, les utilisateurs doivent changer le mot de passe, avec la possible interdiction de réutiliser un ancien mot de passe.

Par ailleurs, comme une montre mécanique est sensible aux champs magnétiques, une disquette, cartouche de sauvegarde y sont également sensibles. Par extension tout matériel informatique est fragile. Noter que statistiquement, un ordinateur meurt plus souvent par coups et blessure infligés par l'utilisateur que d'un virus ou de son obsolescence après de nombreuses années de service…

3.2 Sécurité des données sur les disques : RAID

Il existe différents dispositifs internes aux machines afin de sécuriser les données. Ces dispositifs sont appelés RAID (Redundant array of inxpensive/independent disks / enesmble redondant de disque non extensibles/indépendants).

Raid	Nom	Description
0	Stripping	Disques (3) dont chacun héberge une partie des données
1	Mirroring	Duplication des données sur plusieurs disques (cher en disques)
2	Stripping	Idem Raid0, avec gestion d'un code erreur. Obsolète
3		Les octets sont répartis sur 3 disques, un quatrième stock un code de contrôle de parité (cher)
4		Idem 3 avec des block de données
5		Idem 4 mais les codes de contrôle ne sont pas forcément sur le disque 4 (3 disques au mini). Le plus utilisé
6		Idem 5 avec 2 codes de contrôle. Nécessite au moins 4 disques : cher

Les solutions les plus employées sont Raid1 et 5 qui ont des caractéristiques différentes mais les meilleurs rapports capacité/coût et temps de lecture/écriture.

Elle sont mises en œuvre avec des solutions logicielles ou matérielles (contrôleurs de disques spécialisés) sur des machines serveurs, souvent avec des disques SCSI ou SATA.

3.3 Sécurité des données, sauvegardes

La sécurité des données concerne non seulement celle de leur disques, mais aussi leur maintien et leur restauration, si la machine qui les héberge se crash totalement.

Pour cela, il existe différentes solutions qui ont leurs avantages et leurs inconvénients.

On utilise différents critères de choix qui sont (liste non exhaustive) :

- le degré de sécurité de conservation,
- la disponibilité des données sécurisée,
- la validité des sauvegardes : délai entre la sauvegarde et son rechargement restaurées en cas de crash,
- le volume des données et
- la criticité des données à sécuriser.

On sécurisera les données comptables, pas les pages web du proxy.

Solution	Degré de sécurité	Disponibilité	Validité des données	Fréquence
Réplication sur une autre machine	Moyen à mauvais selon les causes de la perte de données.	Très rapide, immédiate, transparent pour l'utilisateur	Excellent	permanente
Sauvegarde sur cartouche (bande magnétique)	Bon	Moyen, compter au moins une heure de rechargement	Moyen à bon, dépend de fréquence de sauvegarde et de rapidité de modification des données	Journalier, hebdo, mensuelles, annuelle
Sauvegarde su CD, …	Bon	Moyen, Délai un peu meilleur.		Idem (support perdu !)
Coffre à données local	Bon, si le coffre est ignifugé	Bon		N/A
Coffre à données en banque	Très bon	Moyen à passable		N/A
Extériorisation des données. (entreprise de sauvegarde)	Bon, selon le fournisseur	Très variable selon la fiabilité du fournisseur de stockage. A TESTER	Selon la fréquence de sauvegarde, selon le contrat	Selon le contrat

On utilisera, par ailleurs, des systèmes d'exploitation spécialisés pour assurer les fonctions de serveur : Windows NT, 2000 server, 2003, Unix, Novell, OS/400

IMPORTANT : Tester et contrôler les procédures de reprise. Au besoin, effectuer des exercices (comme des exercices incendie) pour vérifier que les procédures sont viables.

Procédures d'archivage à + ou – long terme (une sauvegarde annuelle permet de vider la base de données de toutes les données antérieures).

Choix des données archivées

Temps de sauvegarde (une sauvegarde bloque souvent le système complet, attention aux applications en temps réel)

3.4 La sécurité des communications

Les communications sont le seul moyen de partager l'information. C'est aussi une porte ouverte aux intrusions et aux virus.

On a monté son joooli réseau, on l'a segmenté et on a oublié la sécurité :

- pas de mots de passe réseau : intrusion possible ;
- pas d'anti-virus : attention aux disquettes et aux épidémies ;
- l'accès de l'extérieur est libre (internet, peer to peer, telnet) : bonjour les pirates fouineurs ;

Il faut donc installer des filtres contre toutes ces agressions en

- segmentant le réseau de façon à limiter les accès entre les sous-parties,
- en installant des logiciels de contrôle de transit (firewall) aux nœuds et aux portes du réseau,
- en programmant les routeurs de façon à orienter les intrus vers des zones publiques sans possibilité d'accès aux zones privées (DMZ : demilitarized Zone),
- en cryptant les communications avec les machines distantes sans possibilité d'intrusion ou d'écoute parasite (VPN : virtual private network).

3.5 Sécurité contre les virus

3.5.1 Risques

Les virus sont de différents types :

Les attaques logicielles : détruisent ou altèrent le fonctionnement de logiciels ou les données

Le chevaux de Troie, expions : virus ouvrant des portes aux intrusions ou exportant des données

Les intrusions : logiciels permettant de s'introduire dans des systèmes privés

3.5.2 Mesures

Première consigne : éviter d'en introduire dans le système en limitant l'utilisation et l'échange de disquettes, en installant un anti-virus (AV) qui contrôlera tous les fichiers qui entrent ou sortent du système d'information.

Secundo : ne pas ouvrir les pièces jointes aux mails dont on ne connaît pas la source.

Tertio : mettre en place des contrôles AV sur les services de messagerie, sur les accès externes – surtout Internet.

Utiliser des systèmes d'exploitation différents entre les serveurs de données et d'application et les postes client peut être une très bonne stratégie anti-virus, ces derniers étant généralement spécifiques.

De plus, il existe plus de virus pour les systèmes d'exploitation Microsoft (99%) que pour Linux ou Unix. Il n'en n'existe aucun (ou quasiment) pour l'AS/400.

3.6 Sécurité du matériel

3.6.1 Risques

Les risques existent à différents niveaux

Le bâtiment

Feu, tremblement de terre (si, si, surtout à Ribeauvillé …), foudre, vols

L'alimentation électrique

Feu, micro coupures, coupure franche, parasites, baisse de tension ou surtension, foudre, eau, …

3.6.2 Mesures

Protection Thermique (feu, chaleur).

On concentre souvent les serveurs dans une pièce spécialisée, la salle machine, où les serveurs sont protégés contre diverses agressions.

Dans cette salle, les moyens anti-feu ne sont JAMAIS de l'eau (OH ! gloup !)

(donc pas de sprinkler ici !!!)

Les machines ne supportent pas les températures élevées (interruption du fonctionnement ou combustion du processeur). Il faut donc assurer une température de dépassant pas 35 à 40°, l'optimum se situant à 20°. Prévoyez une climatisation.

Protection électrique

Les alimentations (220V) doivent être munies d'une prise de terre, si possible avec une protection contre la foudre.

Ajouter un onduleur qui assurera la fourniture d'un courant régulier, voire, assurera l'alimentation durant un court laps de temps en cas de coupure importante (env. 5 à 15' selon le matériel et la consommation)

On voit souvent des onduleurs centralisés, associé à des prises munies d'un détrompeur (rouge) pour éviter de brancher une lampe de bureau sur l'onduleur.

Les câbles de communication seront sécurisés en étant placés en altitude ou souterrains, hors du passage de véhicules, hors de portée des parasites électriques dus aux câbles de puissance (machines, ateliers)

Tremblement de terre

Sans penser que les bâtiments risque de s'effondrer, auqel cas, l'entreprise risque fort d'avoir autre chose à sauver que son matériel, il ne faut pas négliger les vibrations provoquées par outil de production (machines outil, véhicules, presses, …)

Un plancher souple ou monté sur silent-blocks constituera une bonne protection contre les vibrations parasites.

Protection du matériel (Vol, intrusion, dégradation, malveillance)

Regrouper les serveurs dans une salle machine et limitez en l'accès aux seules personnes habilitées. La salle machine sera souvent accessible en passant par un voire plusieurs bureaux mais rarement depuis un couloir, jamais depuis l'extérieur.

Les armoires de distribution, de répartition du réseau seront verrouillées et anonymes, les câbles seront placés dans des gaines hors de portée du personnel.

4 Conclusion

En entreprise, un réseau local simple est facile à mettre en place (un peu de câble, quelques composants réseaux et un système d'exploitation dédié aux serveurs) et stratégique pour la circulation des informations au sein de l'organisation (partage des données, travail de groupe, confidentialité).

Il sert surtout à partager des ressources de travail (ERP, Compta, paye, logistique) mais aussi à communiquer avec l'extérieur (mails, EDI).

Voilà.

Sans être apte à créer un grand réseau, vous pouvez en comprendre les principes et participer sans crainte à une discussion stratégique sur le sujet.

Bibliographie :

- Technologie des ordinateurs et des réseaux ; Pierre-Alain Goupille, Dunod
- Réseaux ; Andrew Tanenbaum, Dunod
- http://stm01.free.fr/download/reseaux.pdf
- www.01net.com
- http://www.foo.be/cours/cisco/html/node2.html
- http://cerig.efpg.inpg.fr/ICG/Formation/En-ligne/Exposes/Connectivite/default.htm
- www.commentcamarche.net