

Sécurité des réseaux informatiques

1. Généralités

L'envie de se faire connaître du grand public national et international devient monnaie courante chez les entreprises des pays en voie de développement. Les entreprises utilisent le réseau Internet comme média de communication pour résoudre ce problème crucial, mais ils sont régulièrement exposés aux attaques provenant de l'extérieur (pirates, arnaques, virus...). Il serait donc nécessaire de sécuriser le réseau et le système informatique. La suite de notre exposé portera sur l'enjeu de la sécurité des réseaux informatiques pour les entreprises.

2. Qu'entendons-nous par enjeux de la sécurité des réseaux?

Nous entendons par enjeux de la sécurité réseau tout ce qu'on risque de gagner ou de perdre dans une entreprise en sécurisant les données et le matériel. Il est nécessaire de s'assurer du bon fonctionnement des machines et de l'authentification des utilisateurs qui devront travailler avec les droits qui leur ont été attribués, en empêchant les utilisateurs non autorisés de réaliser une tâche, de prévoir des pannes qui peuvent être causées par des intrus ou même par le personnel de cette entreprise.

3. Sécurité du réseau dans le cas généralité

Les entreprises connectés au réseau Internet haut débit bénéficient généralement de certains services tels que la téléphonie sur IP, la visioconférence, des mises à jour de sécurité gratuites... Certains pirates exploitent généralement les failles de sécurité de ces services pour attaquer ces entreprises. Ces pirates sont parfois motivés par l'argent (en attaquant des banques); ou bien par le désir d'être populaire (pour impressionner des amis); et l'envie de causer du tort à l'entreprise. Ils sont parfois attirés par tout ce est interdit.

Il faudra donc définir une politique de sécurité informatique en faisant des mises à jour; en sécurisant les serveurs de l'entreprise; en sécurisant le réseau sans fil (s'il existe dans l'entreprise); en sécurisant la voix sur IP. La liste est longue.

3.1. Les mis à jour

Les entreprises doivent effectuer régulièrement des mises à jour afin d'améliorer le fonctionnement des machines et de veiller à leur sécurité. Deux modes de mises à jour peuvent être employés:

3. Le mode manuel: Ici l'utilisateur effectue lui-même la mise à jour en téléchargeant un logiciel exécutable depuis le réseau Internet
4. Le mode automatique: Ici l'équipement effectue sa mise à jour lui-même depuis un site distant à une période définie par l'administrateur ou le fabricant.

3.2. Sécuriser les serveurs de l'entreprise

Il est recommandé d'effectuer les différentes actions suivantes pour sécuriser efficacement les postes serveurs:

- Activer le mot de passe de protection BIOS
- Activer le mot de passe de démarrage BIOS
- Booter sur le disque dur en premier
- Désactiver le lecteur de disquette et de CD-ROM
- Ne pas faire un multiboot
- Configurer le délai d'affichage du boot à zéro
- Désactiver la touche F8 au démarrage
- Utiliser un mot de passe robuste
- Modifier les permissions sur les répertoires et les fichiers systèmes
- Utiliser les permissions avancées pour interdire explicitement les suppressions

Il faudra noter que toutes ces actions doivent être réalisées par un administrateur averti.

3.3. Sécuriser le réseau sans fils

Certaines entreprises sont parfois dotées d'un réseau sans fil pour faciliter l'accès à leur réseau aux ordinateurs portables nomades. Comme méthode de sécurité on peut citer:

- La non-annonce de l'identification de réseau SSID (Service Set Identifier)
- Le contrôle des adresses MAC afin de sélectionner les machines

- L'authentification par chiffrement WEP (Wired Equivalent Privacy)

Mais deux vulnérabilités se présentent dans le réseau sans fil:

- L'écoute du canal: Les données sont diffusées par ondes radios en point multipoint par le point d'accès et il est impossible d'empêcher cette propagation dans l'air libre (il est donc facile pour le pirate d'écouter la communication)
- les connexions illicites: n'importe qui peut se connecter au réseau et avoir accès aux informations

3.4. Sécuriser la voix sur IP

Certaines entreprises utilisent la téléphonie sur IP donc la tarification est moins onéreuse celle opérateurs locaux. Dans la voix sur IP on peut noter:

- Au niveau IP: L'interception des communications (écoute des appels)
- Au niveau des protocoles: La surfacturation des appels
- L'usurpation d'identité (la piraterie)

4. La sécurité dans les entreprises Camerounaises

De façon générale la sécurité réseau dans les entreprises se fait sur deux niveaux :

- La sécurité virale
- La sécurité des données

4.1. La sécurité virale

Un virus est logiciel écrit dans langage de programmation ayant pour objectif de nuire les systèmes d'exploitation, les fichiers, et parfois même le matériel (disque, carte graphique....).

On entend par sécurité virale, l'ensemble des méthodes nécessaires pour palier aux attaques des virus et des intrus (cheval de Troie).

Ce type de sécurité est observé dans toutes les entreprises Camerounaises ainsi que chez les particuliers. Ceci pour plusieurs raisons : les anti-virus sont disponibles gratuitement sur Internet, ainsi que leur mise à jour. Nous pouvons citer comme antivirus les plus utilisés : AVG, VirusScan MC Afee, Norton etc.... Il est conseillé de scanner et mettre à jour régulièrement son poste de travail afin d'obtenir les dernières bases virales.

4.2. Sécurité des données

Ce type de sécurité n'est pas pratiqué par toutes les entreprises. On les observe généralement dans les grandes boîtes (BEAC, CRTV, Ringo...). La sécurité des données se fait sur deux niveaux :

- A l'intérieur du réseau : Il est conseillé que les manipulations des fichiers et répertoires au niveau du serveur de données ne soient réalisés que par l'administrateur du réseau et le responsable du service informatique. Nul ne peut avoir accès au serveur de données que s'il a les autorisations nécessaires (lecture – écriture – exécution). Il faut noter que le matériel réseau (serveur, routeurs, ponts d'accès...) doit être conservé dans des salles à température ambiante adéquate et connectés sur des onduleurs.
- A l'extérieur du réseau : Ici la sécurité est beaucoup plus effectuée au

Fichier téléchargé gratuitement sur www.mongosukulu.com - Téléchargement & Cours gratuits
niveau du pare feu qui nécessite une bonne configuration afin de bloquer
des attaques venant de l'extérieur telles les attaques des sniffer, des
hackers... et des prises en main à distance.

Conclusion

Au terme de notre analyse force est de constater que la sécurité de haut niveau n'est pas observée dans la plus part de nos entreprises. La majorité des entreprises Camerounaise n'ont pas assez de fonds à consacrer pour leur sécurité. Car les entreprises Africaines (cas du Cameroun) ne sont les cibles privilégiées des hackers. Ce qui ne les encourage pas à sécuriser efficacement leur réseau.

Les entreprises Camerounaises qui sécurisent efficacement leur réseau gagnent énormément dans l'intégrité et la confidentialité de leurs données. ***Bien qu'il n'existe pas de sécurité absolue.***

Puisque la sécurité des données demande de gros investissements financiers, matériels et logistiques, les PME (Petites et Moyennes Entreprises) qui ne disposent pas assez de capitaux ne s'intéressent pas à leur sécurité, d'où la perte régulière des données.

Les entreprises des pays en voie de développement (Cameroun) doivent protéger leur réseau informatique afin de ne pas être amèrement surprises par des attaques provenant de l'extérieur (Internet ou par des concurrents) ou de l'intérieur, afin d'améliorer le rendement de l'entreprise.