SECURITE
et
INTERCONNEXION

D’après les notes de cours de Manel Ayari

Plan du cours

- **Chapitre 1– Introduction à la sécurité**
- **Chapitre 2 – Introduction à la cryptographie**
- **Chapitre 3– la protection informatique**
  - **Sécurité physique du système informatique.**
  - **Sécurité logique du système d'information.**
  - **Sécurité des systèmes d'exploitation.**
- **Chapitre 4 – les solutions de sécurité pour les réseaux d'entreprise**

CHAPITRE 1
Introduction à la sécurité Informatique

Remarque

- Les outils mis à disposition ne doivent être utilisés qu'à des fins de tests et pour augmenter la sécurité de réseau cible;
- Il est illégal de les mettre en œuvre pour modifier, ajouter, supprimer ou prendre connaissance d'informations non déclarées comme publiques;

La sécurité absolue n’existe pas

On ne peut jamais être sûr d’être parfaitement en sécurité, mais on peut:

1- Améliorer la sécurité par rapport à ce qu’elle était avant

2- Comparer et estimer létat de sécurité par rapport à quelqu’un d’autre.

3- S’assurer que toutes les précautions raisonnables ont été prises pour optimiser la protection des données

4- La sécurité étant dynamique dans le temps, évaluer les processus mis en place pour entretenir la sécurité à long terme.

Concepts de la sécurité

Ensemble de méthodes, techniques et outils chargés de protéger les ressources d'un système afin d'assurer :

- la disponibilité : les services (ordinateurs, réseaux, périphériques, applications…) et les informations (données, fichiers…) doivent être accessibles aux personnes autorisées quand elles en ont besoin en un temps acceptable.
- l'intégrité : les services et les informations ne peuvent être modifiés que par les personnes autorisées (administrateurs, propriétaires…).
- la confidentialité : les informations n'appartiennent pas à tout le monde. seuls ceux qui en ont le droit peuvent y accéder.

- la non-répudiation :aucun des correspondants ne pourra nier la transaction.
- l'authentification : vérifier l'identité annoncée et à s'assurer la non usurpation de l'identité d'une entité

Critères fondamentaux

- Fonctions:
  - Contrôle d'accès
  - Procédures de sauvegarde
  - Tests de montée en charge et dimensionnement
  - Chiffrement
  - Détection et prévention d'intrusion et de virus

- Critères
  - La disponibilité
  - L'intégrité
  - La confidentialité

Critères fondamentaux

- D’autres critères sous-jacents:
  - Imputabilité: Affectation certaine d’une entité à une action ou à un évènement;
  - Traçabilité: Possibilité de trouver l’origine d’un évènement et ses différentes phases;
  - Auditabilité: Capacité de garantir la présence des informations nécessaires à une analyse ultérieure d’un évènement.

Quand l’information est-elle sensible?

- Quand de réels renseignements sont en cause;
- Quand leur divulgation peut porter préjudice aux personnes concernées, même théoriquement;

Comment évaluer la probabilité d’une atteinte?

- Se méfier des effets déformants de l’inconnu;
- Moins on a l’impression d’être en contrôle de la situation, plus on a tendance à exagérer le risque.
- On doit donc s’employer à dissiper l’inconnu et à garder la tête froide.

Quelques statistiques

- Après un test de 12 000 hôtes du département de la défense américaine, on retient que 1 à 3% des hôtes ont des ouvertures exploitables et que 88% peuvent être pénétrés par les relations de confiance.
- Enfin, le nombre de voleurs d'informations a augmenté de 250% en 5 ans,
- 99% des grandes entreprises rapportent au moins un incident majeur
- les fraudes informatiques et de télécommunication ont totalisés 10 milliards de dollars pour seuls les Etats-Unis.
- 1290 des plus grandes entreprises rapportent une intrusion dans leur réseau interne et 2/3 d'entre elles à cause de virus.

Domaines d’application de la sécurité

- Sécurité physique;
- Sécurité de l’exploitation;
- Sécurité logique;
- Sécurité applicative;
- Sécurité des télécommunications.

Domaines d’application

Sécurité physique	Normes de sécurité, protection des ressources énergétiques, protection de l’environnement, redondance physique, plan de maintenance préventive et corrective…
Sécurité de l’exploitation	Plan de secours, plan de continuité, plan de tests, inventaire régulier/dynamique, gestion des incendies, gestion du parc, analyse des fichiers, journalisation, séparation des environnements (dev, indus, appli), gestion des contrats de maintenance …
Sécurité logique	Réalisation de mécanisme de sécurité par logiciel
Sécurité applicative	Robustesse des applications, contrôles programmés, intégration de mécanisme de sécurité, plan d’assurance sécurité, gestion des contrats d’achat de logiciels…
Sécurité des télécoms	Connectivité fiable et de qualité, protocoles sécurisés,…

Domaines d'application de la sécurité

- Plan de sauvegarde
- Gestion rigoureuse des clés d'accès aux locaux
- Validation et audit des programmes
- Antivirus
- choix des protocoles réseaux
- Marquage des matériels
- Gestion des configurations et des mises à jour
- Méthodologie de développement
- Cryptographie

- Physique
- Exploitation
- Logique
- Applicative
- Télécommunication

Contraintes de sécurité

Technologies Internet	Technologie grand public, n'intègre pas en natif des mécanismes de sécurité, disponibilité des outils de gestion de réseau, d'analyse de trafic, d'audit…
Système	Permissivité des configurations, attractivité des systèmes (failles connues), gestion inadpatée, approche partielle de la sécurité…
Réseau	Connectivité entendue, multiplicité et distribution des éléments constructifs, absence de contrôle global, dimensionnement insuffisant
Personnes	Différentes catégories et modes d'usage, différents points d'accès au réseau, nombre croissant, formation et compétences variables, caractère imprévisible…