Chapitre II :

Concepts de base de la sécurité

Ramzi Ouafi
Technologue à ESPRIT
e-mail : **Ramzi.ouafi@esprit.tn**

Introduction

- Avec l'ouverture des entreprises vers l'extérieur, les ressources de l'entreprise sont exposées a divers "dangers".
- Se connecter a Internet n'est pas sans danger. Et les machines connectées en réseau sont encore plus exposées si le niveau de sécurité n'est pas élevé.
- **Pas de risque ZERO !!!!!.**
- Restons modestes :
  - Sécurité est un sujet énorme
  - De nouvelles attaques pirates contre les réseaux informatiques censés être les mieux sécurisés du monde.
  - Complexe car connaissance très pointue dans différents domaines
    - Système
    - Réseau
    - Cryptographie
    - Base de données
    - Administration

Terminologie de sécurité

La sécurité informatique vise généralement les principaux objectifs suivants

- – **La confidentialité** : a rendre l'information inintelligible à d'autres personnes que les seuls acteurs de la transaction.
- – **L'intégrité**: Vérifier l'intégrité des données consiste a déterminer si les données n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle).
- – **L'authentification** : consiste a assurer l'identité d'un utilisateur (signature), garantir a chacun des correspondants que son partenaire est bien celui qu'il croit être.
- – **La non répudiation**: du message = l'émetteur nie avoir envoyé le message
- – **La disponibilité** : est de garantir l'accès à un service ou à des ressources.

Terminologie de sécurité

- **Autres termes de sécurité**

- **– Vulnérabilité : *faiblaisse / faille susceptible de nuire dans l'absolu,***

– Menace:

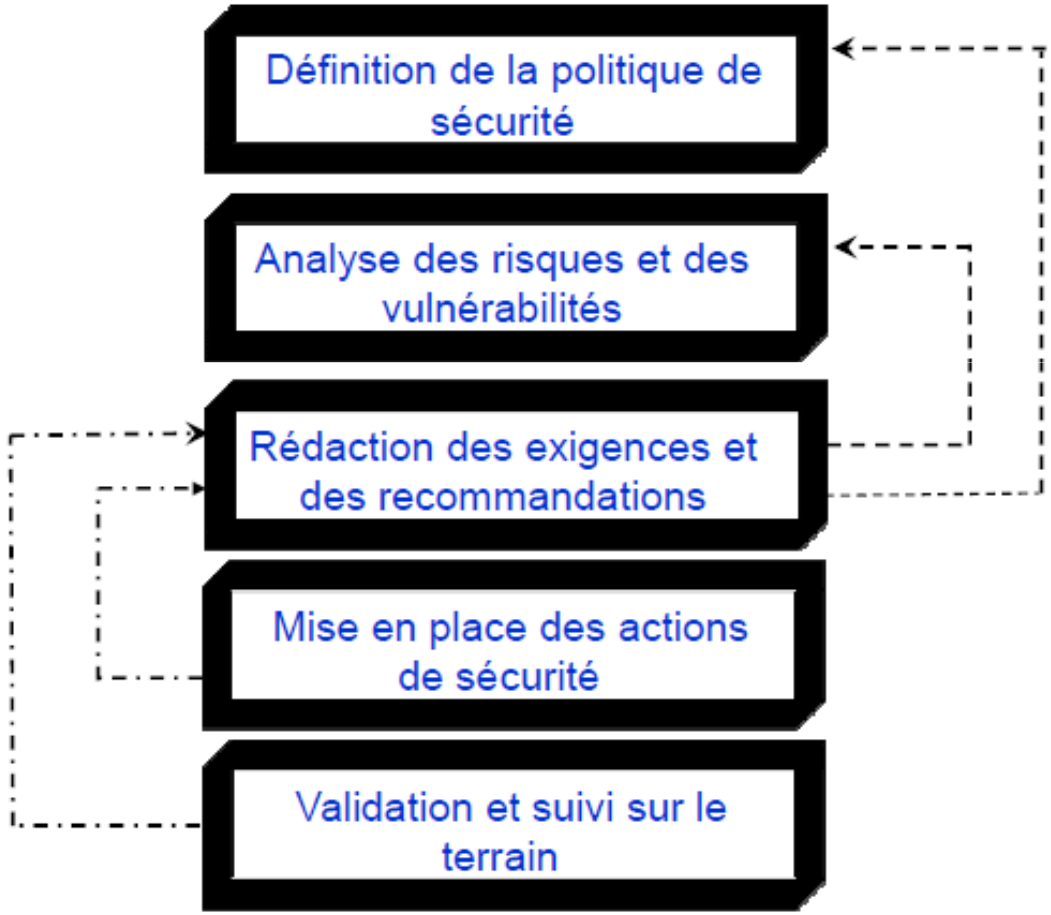
- Source de risque *interne / externe.*
- Concerne aussi bien le *hardware / software.*
- Visant les *données / les utilisateurs / la documentation.*

– Contre-mesures :est l'ensemble des actions mises en œuvre en prévention de la menace

– Impact : représente la conséquence du risque sur l'organisme et ses objectifs

- Peut être qualifie en termes de niveau de sévérité (ou de gravite) exemple : *faible / moyen / fort .*

La méthodologie de sécurité



Politique de Sécurité

- **Développer une politique de sécurité:** l'ensemble des modèles d'organisation, des procédures et des bonnes pratiques techniques permettant d'assurer la sécurité du SI.
  - Répondre à la question :
    - Qui ?
    - Peut, Doit, ne doit pas ?
    - Connaître, Modifier, Communiquer ?
    - Quoi ?
  - Quelle sécurité à apporter au Système d'information? Comment le faire Quels moyens pour atteindre cet objectif ?
- **Contenu du document « Politique de Sécurité »**
  - **1.** But de la politique
  - **2.** Périmètre /domaine d'application
  - **3.** Utilisation des ressources informatiques et accès des utilisateurs.
  - **4.** Contrôles
  - **5.** Mesures en cas de violation
  - **6.** Communication
  - **7.** Rôles et responsabilités

Analyse des risques & des vulnérabilités

- **Risque informatique :** En sécurité informatique, le risque est lié à l'éventualité d'une menace informatique volontaire ou involontaire, interne ou externe au système d'information.

- **Analyse ses risques: Gestion & Maîtrise**
  - **Méthode :** un ensemble plus ou moins structuré de principes, référentiel, base de connaissances de bonne pratiques.
  - **Plusieurs méthodes :**
    - MARION, MEHARI, (Clusif)
    - OCTAVE (Université de Carnegie Mellon).
    - ISO17799, ISO 27005 (ISO)
  - **Comment ? Selon la méthodologie**
    - **Identification de la thématique :** Sécurité physique, Sécurité des applications, etc.
    - **Identification des Menaces :** Erreur d'exploitation, Attaque logique du réseau, Carence de personnel, etc.
    - **Evaluation de la potentialité** (gravité): faible, Moyen, Fort.

- **Critères de choix de la méthodologie :**
  - la qualité de la documentation
  - l'existence d'outils logiciels en facilitant l'utilisation
  - la compatibilité avec une norme nationale ou internationale, etc.

Analyse des risques & des vulnérabilités

- **Vulnérabilité :** Définit toute faille de sécurité présentée par un système informatique pouvant être exploitées par des menaces à des fins malveillantes

- **Différents types de vulnérabilités**

  - **Protocoles de communication**: arpspoof, synflood, dnsspoof, etc.
  - **Défauts de configuration** : comptes, services, privilèges, par défauts ➔check lists
  - **Erreurs de programmation**: Buffer Overflow,

- **Identification des vulnérabilités: des scanners de vulnérabilités**

  - Système et réseaux : Nessus, GFI LANGUARD, Internet Security Scanner.
  - Base de données : Database scanner (IBM), McAfee Security Scanner for Databases, …
  - Applications Web **:** Acunetix Web Vulnerability Scanner,

Rédaction des exigences & recommandations

- **Plan d'actions de sécurité**: décrit les tâches liées à la mise en œuvre de
- Le plan d'action sécurité est ordonné en fonction des priorités:
  - Prioritaire.
  - Urgente.
  - Normale.
- Proposition au niveau organisationnel
  - Création d'unité responsable de la sécurité su SI.
  - Définition des rôles : Conception, Réalisation, Contrôle
  - Nommer les responsables et ressources internes et externes en charge.
  - Financement du plan.
  - Etc.
- Au niveau technique
  - Développement des scénarii du schéma sécurisé du réseau.
  - Conception de la structure d'annuaire pour la gestion des profils utilisateurs.
  - Conception du plan d'adressage (segmentation logique + routage inter-domaine)
  - Etc.

Mise en place des actions de sécurité

- **Sécuriser**
  - Déploiement des actions de sécurité.
  - Actions correctifs dégagés par les outils de scan de vulnérabilités.
  - Mise en place des outils de sécurité (configuration et intégration).
  - Mise en place des outils de suivi et de reporting
- **Exemples**
  - Cloisonner les réseaux de l'entreprise VLAN.
  - Mise en place d’un annuaire LDAP
  - Création de tunnel virtuel privé (VPN) pour sécuriser des accès distants.
  - Etc.

Règles de base de la sécurité

- **Interdiction par défaut :**
  - o Tout ce qui n'est pas autorise explicitement est interdit
- **– Moindre privilège :**
  - o N'autoriser que le strict nécessaire
- **– Défense en profondeur :**
  - o Protection au plus tôt et a tous les niveaux : Cela implique d'avoir ces défenses en série et non en parallèle.
- **– Goulet d'étranglement :**
  - o Point de sortie unique permettant le contrôle
- **– Simplicité :**
  - o Filtrage le plus simple possible
- **– Concertation :**
  - o Acceptation des contraintes par les utilisateurs

Les attaques réseaux

- Une attaque peut être:
  - ***Passive:*** ne modifie pas l'état de communication ou du réseau**.**
    - Exemple de mécanismes: l'observation par sonde et l'analyse de trafic.
  - ***Active:*** dangereuse, car elle modifie l'état d'un serveur ou l'état d'une communication.
    - Exemple de mécanismes: connexion frauduleuse a un équipement, prise de contrôle d'un serveur, l'altération des messages qui circulent sur le réseau.
- Aussi une attaque peut être *interne / externe.*
  - **Interne** : Audit de vulnérabilités
  - **Externe** : Test intrusif

Les attaques réseaux

- Les principales classes d'attaques
  - Les attaques d'accès ou ***Sniffing***
  - Les attaques de modification
  - L'usurpation ou le ***Spoofing***
  - Le Déni de service (Deny of Service, DoS)

Les éléments de sécurité

- **Techniques de Cloisonnement des réseaux**
  - Segmenter votre réseau pour une meilleure sécurité et performance : les VLANs
- **Techniques de Contrôle d'accès** : Fonction principale de filtrage:
  - ACL.
  - Firewall
- **Les mécanismes cryptographiques**
  - Outils de chiffrement
  - Infrastructure PKI ou SSL, ….
- **Les solutions VPN**
  - IPSec, PPTP, L2TP
- **Les systèmes d'authentification**
  - Les serveurs **AAA.**
  - Radius, TACACS+, Kerberos ou Carte a puce ?

Les éléments de sécurité

- **Techniques de Détection d'intrusion**: IDS / IPS
  - Sur les équipements réseaux et système.
- **Les Outils de protection virale**
  - Sur postes de travail, serveur web, réseau
- **Les Outils d'audit technique** (réseau, Base de données, web)
  - Examen et évaluation des vulnérabilités des systèmes (Sécurité Proactive)
- **Outils de Journalisation et d'audit des activités**
  - La confiance n'exclut pas le contrôle !
- **Outils de sauvegarde et de continuité d'activité** (Redondance, clustering, etc.)
  - Comment peut-on assurer la continuité d'activité en cas de pannes ou de défaillances matérielles ?