1 Définition d'une politique de sécurité

- Protection humaine.
- Protection organisationnelle.
- Protection physique.
- Protection technique.

1.1 Protection humaine

Sensibiliser et former.

1.2 Protection organisationnelle

- **Contrôle d'accès administratif** : Préciser les droits d'administrations des utilisateurs sur les postes de travail.
- **Mise en œuvre d'une charte éthique** : Définir les politiques de sécurité et préciser les rôles et les responsabilités.
- **Mettre en place les plans** :
  - PRA : Plan de reprise d'activité.
  - PCA : Plan de continuité d'activité.
- **Gérer les appareils des utilisateurs**
  - BYOD (Bring your own device) : les gérer ou les interdire.
  - CYOD (Choose your own device) : les appareils autorisés sont présélectionnés.
  - COPE (Company Owned and Provided Equipment).
- **Maintenir à jour le SI**
- **Superviser, auditer, réagir**
- **Définir des bonnes pratiques du travail**
  - l'utilisation des mots de passe forts.
  - Controler / interdire l'utitlisation de l'internet.
  - Installation de logiciels à partir du réseau du SI.

1.3 Protection physique

- Contrôle d'accès physique : contrôler l'accès aux locaux (badges..etc) et detetcter les accès non-autorisées (caméras...etc).
- Protection physique des locaux/équipements (panne électrique...etc).
  - Protéger contre les incidents environnementaux.
  - Protéger contre le vol.

1.4 Protection technique

- **Identification** : Reconnaissance d'une entité a travers un indetifiant (ID,email...etc).
- **Authentification** : Vérification de l'identité annoncé (mot de passe, une empreinte biométrique...etc)
- **Autorisation** : Vérification des droits d'accès.

2 Authentification

- **Techniques biométriques** : Physique (visage,Empreinte digitale...etc), Comportementale (la voix, Dynamique de la frappe clavier...etc).
- **Protocoles courants** :
  - Niveau Applications : HTTPs,FTP.
  - Niveau transport :
    * SSL (Secure Socket Layer),
    * SSH (Secure shell),
    * SET (Secure Electronic Transaction),
    * S/MIME (Secure Multipurpose Internet Mail Extension).
    * RADIUS (Remote Authentication Dial-In User Service) : permet de centraliser les données d'authentification.
    * Kerberos : utilisé pour se connecter sur une machine
  - Niveau Réseaux : IPSec.
- **Autres méthodes** :
  - SSO (Single Sign-On) : Par example avec le compte Google.
  - OTP (One Time Password).

3 Chiffrement

- **Chiffrement symétrique** : Une même clé est utilisée pour crypter et décrypter le message,Example : DES, AES.
- **Chiffrement asymétrique (à clé publique)** : Chaque utilisateur dispose deux clés : privée et publique,Example : RSA, ElGamal.
- **Protocoles courants** : PGP (Pretty Good Privacy).
- **PKI (Public Key Infrastructur)** : PKI utilise le chiffrement asymétrique, où le détenteur des clés utilise un certificat numérique, qui joue le rôle comme une signature numérique et contient la clé publique ainsi que des informations sur l'identité.

4 Antivirus

- **Définition** : Un logiciel capable de détecter la présence de virus et dans certain cas les neutraliser en suppriment le code correspondant au virus, du fichier infecté ou La mise en quarantaine du ficher infecté.
- **Fonctionnement** :
  - En utitlisant une base virale à jour (a base du signature virale).
  - En utitlisant contrôleur d'intégrité : detecter les modifications.
  - L'analyse heuristique (analyser le comportement des applications).

5 Pare-feu (Firewall)

- **Définition** : un ensemble de composants matériels et/ou logiciels qui filtrent le flux entrant/sortant entre deux ou plusieurs zones réseaux.
- **Fonctionnement** :
  - contrôler les connexions sortantes à partir du réseau local.
  - Sécurité.
  - surveiller le trafic entre le réseau local et internet.

- **Firewall filtrant (Packet filtering firwall)**

  Permet :

  - Analyse (les entêtes) des paquets : @IP, Numéro de port source et destination,protocole,taille de données...etc.
  - Enregistre les évènements.
  - Translation d'adresses (NAT).

- **Filtrage dans IPtables de Linux**

  - Input chain (la chaine d'entrée) : contient des règles qui filtrent le trafic entrant.
  - Output chain (la chaine de sortie) : contient des règles qui filtrent le trafic sortant.
  - Forward chain (la chaine FORWARD) : contient des règles qui filtrent le routage via la boîte Linux.

```
# iptables -A <CHAIN> -s <@IP_SRC> -d <@IP_DST> -p <PROTOCOL> -icmp_type <ICMP_TYPE>
-sport < NUM_PORT_SOURCE > -dport <NUM_PORT_SOURCE> -i <INPUT_INTERFACE> -o <OUTPUT_INTERFACE>
-m state --state <STATE {NEW|ESTABLISHED|RELATED|INVALID}> -j <ACTION {ACCEPT,DROP}>
```

Exemple :

- Permission de connexions sortantes WEB (HTTP : tcp/80) à toute destination :

```
# iptables -A OUTPUT -p tcp --dport 80 -m state --state NEW -j ACCEPT
```

Protocole	Protocole de transport/port
SSH	tcp/22
HTTP	tcp/80
DNS	udp/53
FTP	tcp/21
Telnet	tcp/23
HTTPS	tcp/443
SMTP	tcp/25

Table 1: Protocoles et leur protocole de transport et numéro de port correspondants

6 Traduction d'adresses (NAT)

- **Définition** : utitlisé pour traduire une adresse IP en une autre,utilisé généralement pour connecter à Internet les réseaux IP privés,cette traduction est réalisée par un dispositif qui connecte le réseau à l'extérieur, par example : un routeur.
- **Types** :
  - NAT Basic : translate seulement les adresses IP.
  - NAPT (Network Adress/Port Translation).

7 Proxy

Un proxy est un intermédiaire dans une connexion entre le client et le serveur,nécessaire pour chaque protocole d'application (HTTP,FTP...etc).

8 DMZ (Demilitarized Zone Network)

Une DMZ est un sous-réseau placé en passerelle entre un réseau à protéger et un réseau externe non protégé,utilisé pour rendre des machines accessible à partir de l'extérieur.

9 Systèmes de détection d'intrusion (IDS)

- **Définition** : Un appareil ou une application logicielle qui surveille le réseau ou le système dans le but de détecter les activités malveillantes.
- **Méthodologies** : Bassée sur signature,le comportement.
- **Types**
  - N-IDS (Network - Based IDS).
  - H-IDS (Host - Based IDS).
  - IDS Hybrides : (N-IDS + H-IDS).
- **Système de Prévention d'Intrusions (IPS)** : IDS + la possibilité d'arrêter des incidents éventuels,en bloquant les paquets malveillantes.

10 Virtual Private Network (VPN)

Un VPN crée un tunnel privé sur Internet en établissant un chemin virtuel entre l'émetteur et le destinataire, puis en chiffrant et acheminant les données via ce chemin sécurisé, utilisant des protocoles comme **IPSec** ou **SSL**.

11 Internet Protocol Security (IPSec)

IPSec est un ensemble de mécanismes de sécurité commun à IPv4 et IPv6, visant à sécuriser les échanges de données au niveau de la couche réseau.

12 Acess Control List (ACL)

- **Définition** : les ACL sont utilisé pour filterer les accées entre deux réseaux,selon @ source,@ destination,protocole et numéro de port.
- **Types** :
  - ACL standard : prent un numéro de 1 à 99 ou de 1300 à 1999,permet le filtrage par @ source seulment.
  - ACL étendue : prent un numéro de 100 à 199 ou de 2000 à 2699,permet le filtrage par @ source,numéro de port ou service.

```
# access-list {acl_number | acl_name} {permit|deny} {protocol} {source_address source_wildcard|any}
[operator [port [port]]] {destination_address destination_wildcard|any} [operator [port [port]]]
```

Exemple :

```
# acess-list 105 deny tcp host 192.168.1.5 any neq http
```