Cybersécurité
La défense du système et du réseau

1 – Sécurité physique

Objectif : protéger physiquement l'accès à l'équipement réseau en limitant l'accès aux locaux.

- Clôtures, gardes, vidéo surveillance.
- Badges, RFID, carte magnétique, authentification biométrique. Le critère de précision est le plus important. Il s'exprime en **types** (**I** ou **II**) et en taux d'erreur.
  - Une erreur de Type I rejette un utilisateur autorisé (Problème de capteur, doigt sale, …).
  - Une erreur de Type II accepte un utilisateur non autorisé => c'est grave pour la sécurité.
  - Taux d'erreur : c'est le taux auquel un système accepte des individus non-inscrits ou des imposteurs comme des utilisateurs authentiques.

2 – Sécurité des applications

Objectif : protéger les applications, les sites web et les services en ligne.

Sécurisation d'une application lors du :

Développement	Vérification des champs d'un formulaire (mail, âge, numéro téléphone, …), masquage des données d'origine avec des caractères ou des données aléatoires.
Phase de test	Vérification des failles.
Déploiement	Utiliser le hachage (MD5, SHA-1, SHA-256, SHA-512, etc)

3 – Sécuriser les réseaux (les protocoles)

Détection ➔ scan des ports pour repérer les services ouverts et les protocoles utilisés.

Les principaux protocoles à protéger

- **DHCP (Dynamic Host Configuration Protocol)** : Les hackers peuvent cibler les serveurs DHCP pour refuser l'accès aux périphériques sur le réseau.
  Solution : DHCP snooping empêchent les serveurs DHCP non autorisés de fournir des adresses IP.

Le snooping DHCP
Utilisé pour prévenir les attaques de déni de service (DoS) et les attaques de type "man-in-the-middle" qui exploitent le processus d'attribution d'adresses IP par DHCP.
Le "snooping DHCP" consiste à surveiller le trafic DHCP sur le réseau au niveau des commutateurs (switches). Le commutateur analyse le trafic DHCP qui traverse le réseau, maintient une table des associations entre adresses IP et adresses MAC basée sur les informations fournies par les serveurs DHCP légitimes.
Si le commutateur détecte des paquets DHCP provenant de sources non autorisées, il peut les rejeter.

- **DNS (Domain Name System) :** Les hackers peuvent cibler les serveurs DNS afin de rediriger le trafic vers des sites web non autorisés.
  Solution : DNS Security Extensions (DNSSEC) qui utilise des signatures numériques pour renforcer l'authentification.

- **ICMP (Internet Control Messaging Protocol) :** La commande Ping envoie des messages ICMP à l'hôte et attend une réponse. Les cybercriminels peuvent modifier l'utilisation d'ICMP pour exécuter des attaques de reconnaissance, par déni de service (DDoS).
  Solution : filtrage des requêtes ICMP.

- **NTP (Network Time Protocol) :** Le protocole NTP synchronise les horloges des systèmes informatiques sur des réseaux de données. Les cybercriminels attaquent les serveurs NTP pour perturber les communications sécurisées qui dépendent de certificats numériques et pour masquer les informations d'horodatage sur les attaques.

Quelques protocoles vulnérables

- **HTTP (Hypertext Transfer Protocol – port 80) :** une solution consiste à chiffrer les communications avec SSL/TLS. L'utilisateur voit HTTPS dans le champ URL d'un navigateur au lieu de HTTP.

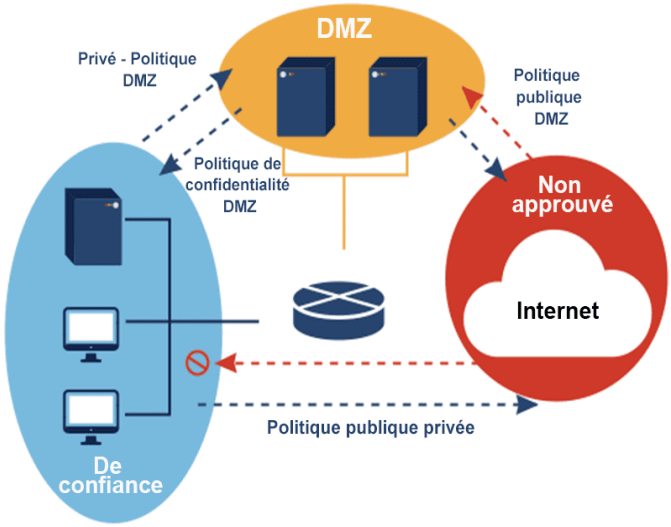
Secure Sockets Layer (SSL)
Il gère le chiffrement en utilisant une poignée de main SSL au début d'une session pour assurer la confidentialité et empêcher les écoutes et les falsifications.

Transport Layer Security (TLS) : plus sécurisée que le protocole SSL.

- **FTP :** nom d'utilisateur et mot de passe en clair pour se connecter. FTPS est plus sécurisé, il prend également en charge TLS et SSL.

4 – Segmentation du réseau pour renforcer la sécurité

Une première solution consiste à utiliser un VLAN. Il peut séparer les groupes d'appareils qui hébergent des données sensibles du reste du réseau, ce qui réduit les risques de violation des informations confidentielles.



En général la plupart des réseaux ont deux à quatre zones de risque :
- **Le LAN** privé (Réseau fiable).

- **La DMZ** (serveurs exposés) : Une DMZ est un petit réseau isolé du réseau interne (LAN). Il héberge des serveurs accessibles depuis internet.

- **Internet.**

Modèle Zéro-trust
Le réseau zéro-trust surveille en permanence tous les utilisateurs (autorisations) sur le réseau, quel que soit leur statut ou leur rôle. Sa mise en place s'effectue sur le pare-feu.

5 – Sécurité Wi-Fi

Les protocoles sans fil

- **WEP (Wired Equivalent Privacy)** a été le premier protocole de sécurité (obsolète).
- **WPA (Wi-Fi Protected Access)** version 3. Elle utilise des clés de 256 bits. WPA-PSK (Pre-Shared Key) est la configuration WPA la plus courante.

- **WPS (Wi-Fi Protected Setup)** permet de configurer un réseau domestique sans fil sécurisé. Un code PIN est utilisé pour connecter les appareils au réseau sans fil.
  Vulnérabilité : attaque par force brute. WPS ne doit pas être utilisé.

Méthodes d'authentification

Wifi pour des systèmes ouverts : pas d'authentification.

Wifi avec authentification par clé partagée EAP (Protocole d'Authentification Extensible) qui fonctionne avec un nom d'utilisateur et un mot de passe.

6 - Sécurité des mobiles

Cas d'un terminal mobile appartenant à l'entreprise ou celui d'un personnel utilisé à des fins professionnelles.

Les menaces	Les mesures de protection
• Vol • Perte • Accès non autorisé	• Code PIN, biométrie • L'effacement à distance supprime les données en cas de vol ou de perte. • Le chiffrement complet de l'appareil.

7 – Résilience en matière de cybersécurité

L'objectif de la résilience, c'est d'éviter que les systèmes tombent en panne, ce qui peut avoir un impact sur la productivité et le chiffre d'affaires.

Haute disponibilité

Systèmes conçus pour éviter autant que possible les temps d'arrêt. Les trois principes de conception :

- Élimination des points de défaillance uniques : remplacement du matériel à chaud, avoir des connexions et des composants redondants.
- Alimentations redondantes.
- Surveillance active des systèmes afin de détecter les défaillances avant qu'elles ne surviennent.

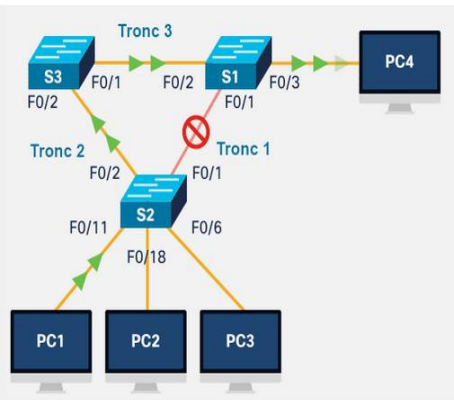
Redondance du matériel

On ajoute du matériel redondant (switch, routeur, …) pour anticiper la défaillance d'un périphérique du réseau.

Lorsqu'on intègre une redondance physique dans un réseau (un switch de plus), des boucles et des trames dupliquées se produisent. Celles-ci entraînent des conséquences désastreuses : latence, surcharge, débit dégradé.
Solution : Le protocole Spanning Tree (STP)

Spanning Tree Protocol (STP)

Le protocole STP (Spanning Tree Protocol) est implémenté sur les switches. Sa fonction de base est d'empêcher les boucles sur un réseau lorsque les commutateurs s'interconnectent via plusieurs chemins.

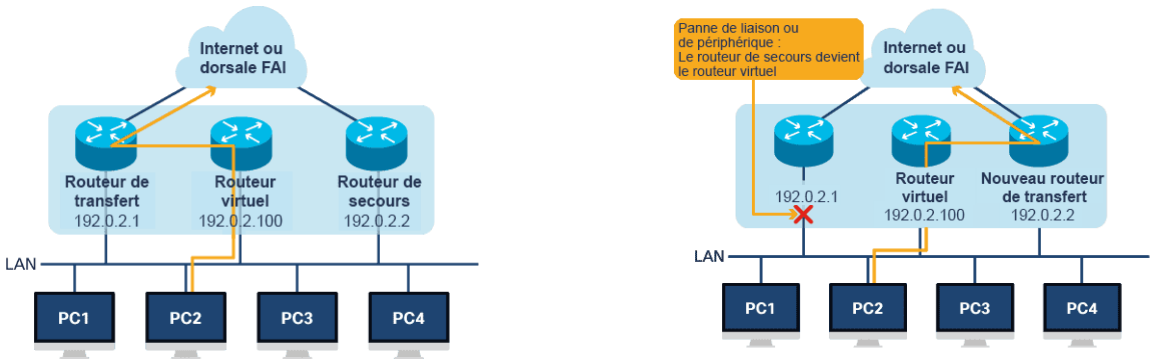


Les étapes STP en cas de panne.

- PC1 envoie une trame de diffusion sur le réseau.
- La liaison entre S1 et S2 tombe en panne, ce qui se traduit par une perturbation du chemin d'origine.
- S2 débloque le port (F0/2) précédemment bloqué et permet au trafic d'emprunter un chemin alternatif.
- Si la liaison entre S2 et S1 est rétablie, le protocole STP bloque de nouveau la liaison entre S2 et S3.

Redondance des routeurs

Si un seul routeur sert de passerelle par défaut, il constitue un point de défaillance unique. L'entreprise peut choisir d'installer un routeur de secours supplémentaire.



Si le routeur 1 (192.0.2.1) tombe en panne le routeur 2 (192.0.2.2) prend le relais. Le problème c'est qu'il faudrait indiquer à tous les hôtes du réseau que la nouvelle passerelle est 192.0.2.2. Pour éviter de changer la passerelle, on définit un routeur virtuel avec une passerelle fixe que le routeur 1 ou 2 soit en panne.

8 – IoT et systèmes industriels

Une cyberattaque peut entraîner la panne ou l'interruption d'installations vitales comme les télécommunications, les services financiers, les systèmes de transport ou les centrales électriques. Leur protection est essentielle pour protéger l'économie d'un pays.

Stuxnet

Stuxnet est un ver informatique qui a été découvert en 2010. Ce logiciel malveillant fut conçu pour cibler les systèmes de contrôle industriels (SCADA) utilisés dans les installations nucléaires iraniennes (centrifugeuses). Il est considéré comme l'un des premiers exemples de "cyber-arme" en raison de sa sophistication et de son ciblage spécifique. Le ver exploitait plusieurs vulnérabilités dans les systèmes Windows et se propageait via des clés USB. L'origine exacte de Stuxnet est attribuée aux États-Unis et à Israël.

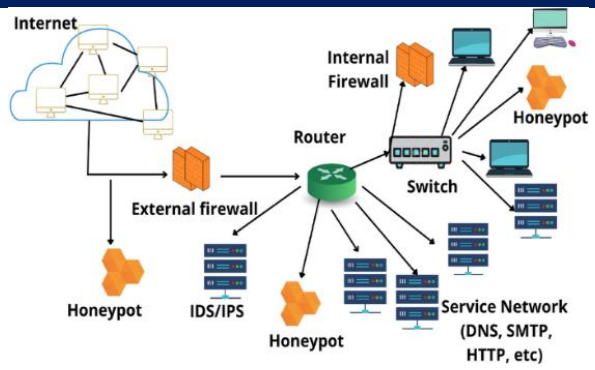
Pour éviter les attaques sur ces systèmes, vous devez séparer les réseaux internes et externes afin de séparer le réseau SCADA (machines industrielles) du LAN de l'entreprise.

9 – VoIP (Voix par IP)

Les cybercriminels ciblent ces systèmes afin de bénéficier de services téléphoniques gratuits, de pratiquer des écoutes clandestines ou encore de nuire aux performances et à la disponibilité.

- Usurpation d'identité (l'hackeur récupère tous les appels entrants)
- Usurpation d'identité du proxy (la victime est amenée à communiquer via un proxy malveillant).
- Le détournement d'appel (interception et réacheminement des appels vers un autre chemin avant d'atteindre leur destination).

10 – Défense active : Honeypot (tromperie)



Pot de miel (Honeypot)

C'est un système configuré pour imiter un serveur du réseau de l'entreprise. Il est délibérément exposé, pour attirer les attaquants. Lorsqu'un hacker s'attaque au pot de miel, ses activités sont consignées et surveillées en vue d'un examen ultérieur.