Sécurité des systèmes d'informations
Université Paris 8
Amir AHMADI

Identifier les piliers techniques et non techniques de la sécurité de réseau

La sécurité des réseaux repose sur plusieurs piliers, à la fois techniques et non techniques. Voici un aperçu des principaux piliers de la sécurité réseau :

Globalement :

1. **Piliers Techniques** :
    - **Renforcement des points d'extrémité** : Il s'agit de protéger les périphériques tels que les postes de travail, les serveurs et les appareils mobiles contre les attaques.
    - **Résilience des points d'extrémité** : Assurer la capacité d'auto-rétablissement des périphériques en cas d'incident.
    - **Définition de priorités sur le réseau** : Identifier les éléments critiques du réseau et leur accorder une attention particulière en matière de sécurité.
    - **Résilience du réseau** : Garantir la capacité du réseau à se rétablir après une perturbation.
2. **Piliers Non Techniques** :
    - **Prévention** : Mettre en place des mesures pour éviter les incidents de sécurité.
    - **Détection** : Surveiller le réseau pour détecter toute activité suspecte ou intrusion.
    - **Réaction** : Avoir des procédures en place pour réagir rapidement en cas d'incident de sécurité.

En détails :

Piliers techniques :

1. **Pare-feu (Firewall)** :
    - Filtrage des paquets entrants et sortants.
    - Contrôle d'accès basé sur des règles.
    - Détection et prévention d'intrusion (IDS/IPS).
2. **Cryptographie** :
    - Chiffrement des données sensibles.
    - Protocoles sécurisés (SSL/TLS, IPsec).
    - Signature numérique pour l'authentification.
3. **Systèmes de détection et de prévention des intrusions (IDS/IPS)** :
    - Surveillance du trafic réseau pour détecter les activités suspectes.
    - Blocage automatique ou notification d'événements suspects.
4. **Authentification et contrôle d'accès** :

    - Utilisation de l'authentification à deux facteurs.
    - Gestion des identités et des accès (IAM).
    - Contrôles d'accès basés sur les rôles.
5. **Sécurité des points d'accès sans fil (Wi-Fi)** :
    - Chiffrement des données Wi-Fi (WPA2/WPA3).
    - Contrôle d'accès basé sur les adresses MAC.
6. **Sécurité des protocoles réseau** :
    - Mise à jour et sécurisation des protocoles (ex: DNSSEC pour DNS).
    - Utilisation de VPN pour sécuriser les communications.
7. **Gestion des vulnérabilités et des correctifs** :
    - Surveillance des failles de sécurité.
    - Application rapide des correctifs.

Piliers non techniques :

1. **Politiques de sécurité et sensibilisation** :
    - Élaboration et application de politiques de sécurité.
    - Formation des utilisateurs sur les meilleures pratiques de sécurité.
2. **Gestion des risques et conformité réglementaire** :
    - Évaluation continue des risques liés à la sécurité.
    - Respect des réglementations et normes de sécurité (ex: GDPR, PCI DSS).
3. **Plan de réponse aux incidents** :
    - Développement d'un plan de réponse aux incidents de sécurité.
    - Formation du personnel pour réagir rapidement et efficacement aux incidents.
4. **Surveillance et audit** :
    - Surveillance continue des activités réseau.
    - Audits réguliers pour identifier les vulnérabilités et les faiblesses.
5. **Gestion des fournisseurs et partenaires** :
    - Évaluation de la sécurité des tiers et partenaires.
    - Contrats de sécurité pour garantir la conformité aux normes de sécurité.
6. **Gestion de la confidentialité des données** :
    - Protection des données sensibles conformément aux réglementations.
    - Utilisation de mesures de confidentialité telles que l'anonymisation et la pseudonymisation des données.
7. **Sécurité physique** :
    - Protection physique des équipements réseau et des serveurs.
    - Contrôles d'accès aux locaux et aux installations sensibles.

Ces piliers sont essentiels pour maintenir un réseau sécurisé et opérationnel.

Références :

1. https://www.itpro.fr/piliers-securite-reseau/
2. https://www.centre-formation-informatique.net/prevention-detection-et-reaction-les-trois-grands-piliers-de-la-cybersecurite/
3. https://www.icsi-eu.org/mag/3-pilier-securite-industrielle
4. https://lightpdf.com/fr/resume-un-pdf.html