Analyse des menaces cyberattaques identifiées

Réseau inter-sites (Site A ↔ Site B)

Projet : Identifier les menaces courantes en matière de cyberattaque pour ce type de configuration réseau conçu sur Packet Tracer.
Date : Octobre 2025
Réalisé par : PEREIRA Lucas

Après avoir configuré le réseau sur Packet Tracer avec deux sites en 192.168.1.0/24 et 192.168.2.0/24 reliés par un routeur ISR4331, j'ai identifié trois menaces courantes en termes de cyberattaques pour ce type de réseau :

1. Man-in-the-Middle (MITM)

Description : Un attaquant se positionne entre deux machines pour intercepter leurs communications. Il peut lire et modifier les données sans que les victimes s'en rendent compte. L'attaquant se positionne secrètement entre l'émetteur et le récepteur.

Vulnérabilités liées à ce réseau : Le routeur ISR4331 est le point de passage obligé entre le Site A et le Site B. Sans tunnel VPN ou chiffrement, toutes les données circulent en clair. Un attaquant qui compromet le routeur ou se positionne sur cette liaison peut intercepter l'intégralité du trafic inter-sites (mots de passe, fichiers, emails...).

Mesures de prévention :

- Mettre en place un VPN IPsec entre les sites pour chiffrer les communications.
- Utiliser uniquement des protocoles sécurisés (SSH, HTTPS, SFTP).
- Sécuriser l'accès au routeur avec des mots de passe forts et des ACL.

2. Accès non autorisé aux équipements

Description : Un attaquant prend le contrôle du routeur ou des switchs en exploitant des faiblesses de configuration tels que les mots de passe par défaut, Telnet activé, et accès physique non sécurisé.

Vulnérabilités liées à ce réseau : Les équipements Cisco sont livrés avec des configs par défaut. Lors de mes recherches, j'ai constaté que l'accès à l'administration peut être facile si Telnet est activé avec un faible mot de passe. Un attaquant qui contrôle le routeur est capable d'observer l'ensemble du trafic, modifier des routes, ou couper des connexions. L'accès physique non protégé permet également une prise de contrôle via le port console : avec un simple câble console (RJ45 vers USB), n'importe qui peut se connecter directement au routeur et accéder au mode privilégié si aucun mot de passe console n'est configuré. Dans un bureau non sécurisé, cela représente un risque majeur.

Mesures de prévention :

- Changer tous les mots de passe par défaut immédiatement.
- Désactiver Telnet et utiliser uniquement SSH.
- Configurer des ACL pour limiter les accès admin.
- Sécuriser physiquement les équipements.
- Configurer un mot de passe sur le port console (line console 0 / password).
- Activer les logs pour tracer les connexions.

3. Propagation de malware

Description : Un logiciel malveillant (virus, ransomware) infecte une machine et se propage à l'ensemble du réseau. Les ransomwares chiffrent toutes les données et demandent une rançon.

Vulnérabilités liées à ce réseau : Il n'y a pas de segmentation visible - tous les PCs sont sur un réseau plat par site. Si un utilisateur ouvre une pièce jointe infectée, le malware peut scanner le réseau local et infecter tous les postes en quelques minutes. Ensuite, il peut traverser vers l'autre site via le routeur. Sans segmentation, une seule infection peut paralyser toute l'entreprise.

Les ransomwares sont particulièrement préoccupants : en 2023-2024, des attaques comme LockBit ou BlackCat ont paralysé des entreprises entières en quelques heures. Ces malwares modernes se propagent automatiquement via les partages réseau, chiffrent non seulement les fichiers locaux mais aussi les sauvegardes accessibles, et certains exfiltrent les données avant de les chiffrer pour faire du double chantage. Dans notre configuration, sans segmentation entre les sites, un ransomware pourrait atteindre les deux sites en moins de 30 minutes.

Mesures de prévention :

- Segmenter le réseau avec des VLANs (postes, serveurs, imprimantes séparés).
- Installer un antivirus/EDR à jour sur tous les postes.
- Mettre en place des sauvegardes régulières sur un système isolé.
- Configurer un pare-feu entre les sites pour filtrer le trafic.
- Sensibiliser les utilisateurs aux bonnes pratiques.
- Désactiver les partages réseau inutiles.
- Limiter les droits administrateurs des utilisateurs.

Conclusion

Ces trois menaces exploitent des vulnérabilités à divers niveaux du réseau : la connexion inter-sites (MITM), les équipements eux-mêmes (accès non autorisé) et les postes utilisateurs (malware). La sécurité repose sur plusieurs niveaux de protection : VPN, mots de passe renforcé, segmentation, sauvegardes et sensibilisation. Une seule solution ne suffit pas, il est nécessaire d'adopter une stratégie globale.

Document rédigé par : Identifier les menaces courantes en matière de cyberattaque pour ce type de configuration réseau conçu sur Packet Tracer.
Date : Octobre 2025
Réalisé par : PEREIRA Lucas