Configuration sécurisée de l’accès Wi-Fi

Risques associés à un Wi-Fi non sécurisé

La mauvaise configuration d’un réseau Wi-Fi ou un dysfonctionnement ponctuel peuvent être exploités par des cyberattaquants pour :

- **La récupération des données de navigation des utilisateurs du réseau :** Différentes méthodes peuvent être utilisées pour accéder au Wi-Fi de l’entreprise et récupérer des informations et des données potentiellement sensibles et/ou confidentielles. En particulier, les données reçues et envoyées par l’utilisateur sont exposées et peuvent être interceptées par des cyberattaquants si le réseau n’est pas chiffré à l’état de l’art.
- **La réutilisation du matériel / de la bande passante :** Un cyberattaquant peut accéder de manière illégitime au réseau et utiliser la connexion Wi-Fi du dispositif afin d’en faire une utilisation frauduleuse.
- **Le rebond vers le reste du SI :** Le réseau peut être utilisé pour réaliser dans un second temps des attaques plus sophistiquées, par le biais de diverses techniques comme l’ingéniérie sociale par exemple, afin d’infecter plusieurs postes de l’entreprise (voire l’ensemble du système d’information). Cela expose indirectement d’autres informations et données sensibles présentes sur le SI et rend ce dernier vulnérable aux cyberattaques.
- **La création de points d’accès malveillants (Evil Twin) :** Des cyberattaquants imitent le réseau légitime pour inciter les utilisateurs à s'y connecter et récupérer via de faux formulaires de connexion des informations comme des mots de passe par exemple.

Bonnes pratiques de configuration Wi-Fi

- **Utilisez un chiffrement robuste :** Assurez-vous que le réseau Wi-Fi de l'entreprise utilise un protocole de chiffrement robuste tel que WPA3 ou WPA2.
- **Utilisez des mots de passe forts :** Si vous configurez un réseau Wi-Fi, utilisez des mots de passe forts et uniques pour empêcher l'accès non autorisé (voire utilisez de la MFA).
- **Mettez en place un filtrage réseau :** Isolez le réseau-Wifi du réseau filaire et mettez en place des équipements de filtrage (par exemple un filtrage des adresses MAC) afin de limiter l’accès au réseau à des dispositifs sécurisés ou préalablement approuvés.
- **Activez la détection d'intrusion :** Configurez des systèmes de détection d'intrusion pour surveiller les activités suspectes sur le réseau Wi-Fi de l'entreprise. Cela permet de détecter rapidement les tentatives d'accès non autorisé.
- **Isolez le réseau Wi-Fi « Visiteurs » :** Dédiez une infrastructure réseau distincte pour les accès des simples visiteurs afin de ne donner accès à aucune ressource du réseau interne.
- **Mettez à jour régulièrement les matériels :** Assurez-vous que les routeurs, les points d'accès et les périphériques Wi-Fi sont régulièrement mis à jour avec les derniers correctifs de sécurité pour combler les vulnérabilités potentielles.

Ressources pertinentes

- Recommandations de l’**ANSSI** sur la sécurisation des accès Wi-Fi (PDF)