Sécurité de l’accès Wi-Fi

Risques associés à l’accès à un Wi-Fi non sécurisé

Lorsque l’on se connecte à un réseau Wi-Fi non sécurisé, les données peuvent être facilement interceptées. C’est le cas des :

- **Mots de passe :** Des cyberattaquants créent de faux réseaux Wi-Fi imitant les réseaux Wi-Fi légitimes afin de récupérer votre mot de passe via un faux formulaire de connexion (portail captif, boite mail, réseaux sociaux, etc.).
- **Données de navigation :** Les données qui circulent sur un réseau Wi-Fi ne sont pas protégées. Un réseau Wi-Fi ouvert peut donc permettre à des tiers de consulter vos données de navigation (historique, cookies, données envoyées ou reçues…).

Par ailleurs, se connecter à un Wi-Fi non sécurisé vous expose potentiellement à des malwares ayant pour conséquence :

- **Le piratage de l’appareil :** Des cyberattaquants chargent un point d’entrée malveillant d’un logiciel malveillant (malware) qui compromet votre appareil. Cela leur donne accès à l’ensemble des données qu’il contient.
- **L’usurpation d’identité :** La compromission de votre appareil peut permettre à des cyberattaquants de le réutiliser à des fins frauduleuses en votre nom.
- **L’attaque par rebond de l’entreprise :** Votre appareil professionnel peut représenter un point d’entrée du système d’information de l’entreprise, exposant cette dernière à des cyberattaques aux conséquences potentiellement sévères.

Ressources pertinentes

- Recommandations de l’**ANSSI** sur la sécurité relative aux réseaux Wi-Fi (PDF)

Bonnes pratiques de sécurité Wi-Fi

- **Utilisez un réseau Wi-Fi connu et sécurisé :** Connectez-vous uniquement aux réseaux Wi-Fi autorisés et sécurisés mis en place par l'entreprise et évitez de vous connecter à des réseaux publics non sécurisés.
- **Limitez l’usage de réseaux Wi-Fi publics :** Le cas échéant, réservez l’usage de Wi-Fi publics à des usages en consultation de données non confidentielles uniquement.
- **Bloquez les connexions automatiques aux points d’accès publics :** Désactivez par défaut la connectique Wi-Fi de votre appareil et ne l’activez qu’en cas de besoin. Cela permet d’une part d’empêcher la connexion automatique à un point d’accès malveillant et d’autre part d’empêcher un tiers de savoir quels réseaux votre appareil recherche automatiquement pour créer des répliques visant à vous tromper.
- **Soyez vigilants aux réseaux en « doublon » :** N’hésitez pas à vérifier auprès de l’entité dont il émane le nom du réseau légitime.
- **Désactivez le partage de fichier :** En cas de connexion sur un réseau Wi-Fi public non sécurisé, désactivez les paramètres de partage de fichiers sur votre appareil pour protéger vos données locales.
- **Mettez à jour votre appareil :** Maintenez à jour le système d’exploitation et les pilotes Wi-Fi de votre appareil afin d’appliquer les derniers correctifs de sécurité.
- **Utilisez un VPN :** En cas de mobilité, dotez-vous de mesures de protections supplémentaires comme un réseau privé virtuel (VPN) préconisé par l’entreprise, permettant de vous isoler du reste du trafic et de protéger vos données de navigation d’un éventuel cyberattaquant.