Télétravail et cybersécurité

Accroissement des cybermenaces à l'ère du télétravail

Le **télétravail** implique une connexion aux systèmes et aux données de l'entreprise via des réseaux externes qui **peuvent ne pas être sécurisés**. Cette tendance augmente la **surface d'exposition** des entreprises aux cyberattaques, entraînant ainsi la nécessité de **renforcer les mesures de sécurité.**

Quels sont les risques SSI associés au télétravail ?

Plusieurs risques SSI peuvent être associés au télétravail, notamment :

- **L'utilisation d'appareils personnels non durcis** ce qui rend le risque d'exposition à des attaques potentielles plus élevé et met en péril la sécurité des données sensibles.
- **Risques d'interception de données** en raison de l'utilisation de réseaux Wi-Fi publics ou peu sécurisés.
- **Contamination des environnements SI** de l'entreprise via des failles de sécurité sur les ordinateurs utilisés par les employés permettant aux attaquants d'accéder au réseau de l'entreprise ou au travers l'installation de logiciels vulnérables non mis à jour.
- **Fuites de données potentielles** dues à un stockage ou un partage inapproprié d'informations sensibles (ex : stockage des données sensibles sur des appareils personnels, utilisation de services cloud non approuvés, etc.) ou de la perte d'un appareil mobile. Le risque est d'autant plus grand si l'appareil n'est pas chiffré.

Quelles sont les bonnes pratiques cyber à adopter dans le cadre du télétravail ?

Pour diminuer les risques associés au télétravail et garantir la protection des données et des opérations contre d'éventuelles menaces, il est essentiel de mettre en place certaines mesures :

- **Travailler depuis chez soi ou depuis un lieu sûr** et éviter les connexions Wi-Fi publiques non sécurisées.
- **Encouragez l'utilisation de réseaux privés virtuels (VPN)** pour établir des connexions chiffrées entre les appareils et le réseau de l'entreprise.
- **Mettre à jour régulièrement** tous les logiciels, systèmes d'exploitation et applications avec les derniers correctifs.
- **Restreindre l'accès des collaborateurs** aux seules données et ressources nécessaires à leurs rôles et activités.
- **Mettre en place des outils de surveillance** pour détecter les activités suspectes ou les cybermenaces potentielles
- **Intégrer la MFA** pour renforcer la protection de l'accès des utilisateurs au SI.
- **Protéger les données en chiffrant tous les terminaux** afin de réduire les risques de fuite de données en cas de perte ou de vol d'équipements.

Ressources pertinentes

- Des recommandations sur la sécurité au télétravail publié sur la plateforme **Cybermalveillance.gouv** [Site web]
- Des recommandations sur le Nomadisme numérique publié par **l'ANSSI** [PDF]
- Des bonnes pratiques cybers à adopter dans le cadre du travail à distance publiées par **l'ENISA** [Site web]