Nomadisme numérique

Qu'est-ce que le nomadisme numérique ?

Le nomadisme numérique désigne toute forme **d'utilisation des technologies de l'information** permettant à un utilisateur **d'accéder au SI depuis des lieux distants**, ces lieux n'étant pas **maîtrisés par l'entité.**

Dans ces lieux de travail non contrôlés par l'entité, les risques suivants sont accentués : **perte ou vol** de matériel, **compromission du matériel et des informations** qu'il contient, **accès non autorisé au SI** de l'entité, **interception ou altération des informations** entraînant une perte de confidentialité et/ou d'intégrité. Afin de réduire ces risques, il est nécessaire de mettre en place des mesures de **protection physique et logique.**

Les points de vigilance :

La connexion **aux réseaux non maîtrisés & non sécurisés** (Wi-Fi public, objet connecté, etc.) peuvent permettre à un attaquant d'accéder aux données confidentielles d'un équipement. Afin de limiter la surface d'exposition, il est conseillé de **ne pas mutualiser des usages personnels et professionnels** sur un même appareil.

Ressources mises à disposition :

- ANSSI – Recommandations sur le nomadisme numérique (PDF) ;
- ANNSI – Bonnes pratiques à l'usage des professionnels en déplacement (PDF) ;
- CNIL – Perte ou vol de matériel informatique nomade : les bons réflexes à avoir ! (Site web) ;
- ANS – Maîtrisez-vous le risque numérique lié au nomadisme des professionnels? (PDF) ;

Les bonnes pratiques et mesures de sécurité :

- **Sensibilisation :** Les utilisateurs nomades doivent être **conscients des risques** liés à ce mode de travail. Des formations sur les **comportements à adopter** doivent être mis en œuvre.
- **Sécurisation physique :** Dans les lieux publics, il est important de protéger la confidentialité des terminaux, en prenant par exemple les mesures suivantes : **banaliser les terminaux nomades**, utiliser un **filtre écran de confidentialité**, des **verrous de ports** USB et RJ45, un **câble antivol**, ou encore un **support externe** (carte à puce ou un jeton USB).
- **Sécurisation des connexions :** Afin de limiter l'exposition des services de l'entité, il est recommandé d'établir un **tunnel VPN IPsec** entre le poste nomade et le SI de la structure.
  Pour prévenir la réutilisation d'identifiants en cas de vol ou de perte, il est préférable d'utiliser une **authentification forte** (exemple : mécanisme de mot de passe à usage unique par exemple, CPS / eCPS, etc.).
- **Adoption de politiques de sécurité dédiées : limiter la liste des applications** pouvant être installées sur les terminaux nomades, et **bloquer les périphériques amovibles** permet de réduire la surface d'exposition.
- **Chiffrement des données :** Il est conseillé de commencer par un **chiffrement complet du disque** avant d'envisager le chiffrement d'archives ou de fichiers (Outil recommandé par l'ANSSI : Cryhod).