E3. Utiliser des supports amovibles de façon sécurisée

Le support amovible, s'il permet de transporter facilement des données, peut être compromis par un logiciel malveillant susceptible d'agir sur la machine ou le réseau auquel il sera connecté. La perte d'un support amovible signifie, bien évidemment, la perte des informations qu'il contient.

ORGANISATIONNEL

➤ Interdire la connexion, à des postes reliés au système d'information de l'entreprise, d'équipements et de supports amovibles personnels (clés USB, disques durs externes, lecteurs MP3, etc.).

➤ Sensibiliser les collaborateurs, notamment au moyen de la charte informatique, à cette règle importante souvent perçue comme une contrainte.

TECHNIQUE

➤ Désactiver l'exécution automatique des périphériques.

COMPORTEMENTAL

➤ En cas d'utilisation d'un support amovible, par exemple pour échanger des données sensibles, choisir un support réservé à cet usage.

➤ Avant de l'utiliser, analyser avec un outil adapté, tout support amovible qui a été connecté à l'extérieur du réseau de l'entreprise.

➤ Chiffrer les supports amovibles pour limiter tout risque de fuite d'information en cas de perte ou de vol.

➤ Ne pas prêter ses supports amovibles. Ne pas les laisser accessibles sans surveillance.

Mots clés

Chiffrement : procédé de cryptographie grâce auquel on rend la compréhension d'un document impossible à toute personne qui ne possède pas la clé de (dé)chiffrement.

Pour aller plus loin

➤ Agence nationale de la sécurité des systèmes d'information (Anssi)

- Guide des bonnes pratiques de l'informatique
- Guide d'hygiène informatique
- Passeport de conseils aux voyageurs
- Guide d'élaboration d'une charte d'utilisation des moyens informatiques et des outils numériques
- Liste de logiciels de chiffrement que vous pouvez utiliser en toute confiance

➤ Service du Haut fonctionnaire de défense et de sécurité (SHFDS) du ministère de l'Économie, des Finances et de la Relance.