

Clés USB et supports amovibles : petits objets, gros risques

Vecteur d'infection, fuite de données ambulante et objet piégé : les règles d'usage des supports qui passent de main en main.

7 min de lecture · Niveau Essentiel · cyberionis.fr/ressources/usb-supports-amovibles

La clé USB semble inoffensive — c'est précisément sa force. Elle traverse les défenses réseau sans les toucher : branchée à l'intérieur, elle y apporte ce qu'elle contient. Infections historiques, clés « perdues » sur les parkings d'entreprises ciblées, données confidentielles baladées sans chiffrement : le petit objet cumule les grands classiques. Quelques règles simples le remettent à sa place.

1. Les trois risques distincts

- L'infection entrante : une clé contaminée (souvent à l'insu de son propriétaire) introduit un malware directement sur le poste — le canal favori pour toucher les systèmes isolés d'Internet
- La fuite sortante : la clé qui se perd avec le fichier clients dessus, non chiffrée — une violation de données au sens RGPD, notification à la clé
- L'objet piégé : plus rare mais réel, du matériel conçu pour attaquer (fausses clés qui simulent un clavier et tapent des commandes) — d'où la règle absolue sur les clés trouvées

ATTENTION

Une clé USB trouvée — sur le parking, dans une salle de réunion, reçue par courrier « cadeau » — ne se branche JAMAIS, nulle part, « juste pour voir à qui elle est ». C'est un scénario d'attaque documenté et éprouvé : la curiosité est exactement le mécanisme exploité. Elle se remet au référent informatique, qui sait quoi en faire.

2. Les règles d'usage en entreprise

- Le chiffrement obligatoire pour tout support qui sort des locaux : clé chiffrée matériellement ou via BitLocker To Go — la clé perdue devient alors un non-événement
- Des supports fournis par l'entreprise, identifiés, plutôt que la collection personnelle de chacun
- L'analyse antivirus automatique à l'insertion (l'EDR le fait) et l'exécution automatique désactivée
- Les échanges avec l'extérieur (clients, prestataires, imprimeurs) privilégient les liens de partage sécurisés — la clé qui circule de main en main est le pire canal
- Sur les postes sensibles : le blocage pur et simple des ports USB pour le stockage, géré centralement

3. Le disque dur externe : mêmes règles, plus de données

Tout ce qui précède vaut au carré pour les disques externes : plus de capacité, donc plus de dégâts en cas de perte — et un usage sauvegarde qui a ses propres exigences (voir notre guide sauvegardes) : un disque de sauvegarde se chiffre, se débranche après usage, et ne reste pas connecté en permanence à portée d'un ransomware. En fin de vie, tout support s'efface sérieusement ou se détruit — la corbeille et le

formatage rapide ne suppriment rien.

4. Les autres « supports » qu'on oublie

- Les cartes SD des appareils photo et drones : elles contiennent les images du chantier ou du client — mêmes règles de chiffrement et d'effacement
- Les téléphones branchés en USB « pour charger » sur un poste : préférer le chargeur secteur, ou refuser le transfert de données proposé
- Les gadgets promotionnels (clés, câbles, chargeurs reçus en salon) : sympathiques et invérifiables — pas sur les postes de l'entreprise
- Les photocopieurs avec port USB : un canal d'entrée-sortie souvent oublié des règles

L'essentiel à retenir

01 Interdire absolument le branchement des supports trouvés ou inconnus

02 Chiffrer tout support qui sort des locaux

03 Fournir des supports d'entreprise identifiés

04 Activer l'analyse à l'insertion et bloquer l'exécution automatique

05 Privilégier les liens de partage sécurisés pour les échanges externes

06 Effacer sérieusement ou détruire les supports en fin de vie

Questions fréquentes

Comment chiffrer une clé USB simplement ?

Sous Windows Pro : clic droit sur la clé ! BitLocker To Go, un mot de passe, c'est fait — la clé se lit sur les autres Windows avec le mot de passe. Alternative multiplateforme : les clés à chiffrement matériel (clavier de saisie intégré), plus chères mais utilisables partout. Dans les deux cas, le mot de passe rejoint le gestionnaire d'entreprise.

Un client nous remet ses documents sur une clé. On fait quoi ?

On ne la refuse pas — on la traite : branchement sur un poste à jour avec analyse antivirus active (jamais sur un poste critique), copie des fichiers nécessaires, analyse, puis restitution. Et pour la suite de la relation, proposez un lien de dépôt sécurisé : plus simple pour tout le monde, et plus sûr.

Faut-il vraiment bloquer les ports USB ?

Pas partout — le blocage total gêne plus qu'il ne protège dans la plupart des PME. La gradation raisonnable : règles claires + chiffrement + analyse automatique pour tous ; blocage du stockage USB sur les postes réellement sensibles (comptabilité, serveurs, postes exposés au public). Les outils de gestion de parc le paramètrent finement.

Pour aller plus loin

Cybermalveillance.gouv.fr — les supports amovibles — www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/appareils-mobiles

ANSSI — Guide d'hygiène informatique — cyber.gouv.fr/publications/guide-dhygiene-informatique

Besoin d'aide pour le mettre en place ?

Audit, durcissement, accompagnement : Cyberionis sécurise les TPE, PME et collectivités, à Nancy, Lure et à distance.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr