

La sécurité physique des locaux : le maillon qu'on oublie

Visiteurs, écrans ouverts, serveur dans le placard à balais : la meilleure cybersécurité tombe si la porte est ouverte.

7 min de lecture · Niveau Essentiel · cyberionis.fr/ressources/securite-physique-locaux

On chiffre, on filtre, on authentifie — et le serveur trône dans un local ouvert, les écrans restent allumés à l'accueil, et n'importe qui en gilet fluo circule sans question. La sécurité physique est le socle silencieux de la cybersécurité : un accès physique à une machine, c'est potentiellement tous les contrôles logiques contournés. L'état des lieux se fait en une visite de vos propres locaux — avec les yeux d'un intrus.

1. Le tour des locaux, avec les yeux d'un intrus

- Que voit-on depuis l'accueil et les zones visiteurs ? Écrans, documents, tableaux blancs stratégiques, post-it...
- Où sont serveur, NAS, baie réseau ? Local fermé à clé, ou placard ouvert entre les ramettes et le café ?
- Qui circule sans être questionné ? Le livreur, le « technicien », le costume assuré traversent la plupart des PME sans un mot
- Que trouve-t-on dans les poubelles et sur les imprimantes ? Devis, listings, courriers — le papier fuit autant que le numérique
- Les prises réseau des salles de réunion et zones publiques sont-elles actives ? Un câble branché = un accès au réseau interne

2. Les mesures de base (peu coûteuses)

- Verrouillage automatique des sessions (5 minutes) partout, et le réflexe Windows+L en se levant — surtout aux postes visibles du public
- Le local technique fermé à clé, clés recensées — serveur, baie, sauvegardes n'ont rien à faire en libre accès
- Écrans orientés, filtres de confidentialité aux postes exposés (accueil, guichets)
- Le broyeur près de l'imprimante, et la règle : tout document nominatif ou commercial se broie
- Impressions sensibles récupérées immédiatement — ou l'impression à badge/code si le copieur le permet
- Bureaux « propres » le soir dans les zones accessibles : les documents sensibles dorment dans des tiroirs fermés

CAS CONCRET

Le test d'intrusion physique le plus classique réussit dans la majorité des PME : un gilet de chantier, une échelle ou un carton, un « c'est pour la clim » — et l'auditeur se retrouve seul dans les locaux, voire dans le local serveur. Aucun logiciel ne protège de la politesse française face à un gilet fluo. La parade : la culture du « je peux vous aider ? » systématique envers tout inconnu.

3. Encadrer les visiteurs et intervenants

- Tout visiteur est accueilli, accompagné, raccompagné — la règle vaut pour le commercial comme pour le technicien
- Les interventions techniques s'annoncent : un « dépanneur » non prévu se vérifie par un appel au prestataire supposé (au numéro connu — le faux support se déplace aussi)
- Les intervenants réguliers (ménage, maintenance) : encadrés par contrat, sensibilisés, et les zones sensibles restent fermées en leur présence hors accompagnement
- L'alarme et le contrôle d'accès à la mesure des enjeux : badges ou codes individuels (révocables !) plutôt que LA clé universelle dupliquée depuis dix ans

4. Protéger les machines elles-mêmes

- Le chiffrement des disques rend le vol de machine muet — c'est la jonction entre sécurité physique et logique (voir notre guide)
- Les câbles antivol pour les portables en zone de passage, la fixation pour les équipements exposés
- Les prises réseau inutilisées désactivées, le Wi-Fi visiteurs séparé — l'accès physique au réseau se mérite aussi
- La vidéosurveillance là où elle se justifie, dans les règles CNIL (zones, information, conservation)

L'essentiel à retenir

- | | |
|----|--|
| 01 | Faire le tour des locaux avec les yeux d'un intrus |
| 02 | Fermer le local technique à clé et recenser les accès |
| 03 | Généraliser verrouillage automatique et réflexe Windows+L |
| 04 | Installer broyeur et règle du bureau propre en zone accessible |
| 05 | Instaurer l'accompagnement systématique des visiteurs |
| 06 | Chiffrer les disques et neutraliser les prises réseau libres |

Questions fréquentes

Nos locaux sont petits, tout le monde se connaît. Est-ce vraiment un sujet ?

C'est justement le contexte où le gilet fluo marche le mieux : « on se connaît » signifie qu'un inconnu est supposé être légitime (« il doit être là pour quelque chose »). Les mesures de base coûtent presque rien et ne gênent personne — et le local serveur fermé protège aussi de l'accident bête : la fuite d'eau, le radiateur, le coup de balai dans le câble.

Un intrus peut-il vraiment faire quelque chose en deux minutes sur un poste ?

Sur une session ouverte : lire et copier des documents, envoyer un email « de vous », brancher une clé préparée qui installe un accès en secondes. Sur une machine verrouillée mais accessible : brancher un enregistreur discret entre clavier et PC. Le verrouillage systématique et le contrôle des inconnus ferment l'essentiel de ces scénarios.

La vidéosurveillance des locaux est-elle recommandée ?

Pour les accès et zones de valeur, elle a du sens — dans le cadre CNIL strict : on filme les accès et les biens, pas les salariés au travail en continu ; panneaux d'information, conservation limitée (un mois max en général), accès aux images restreint. Et les caméras elles-mêmes se sécurisent : ce sont des objets connectés comme les autres.

Pour aller plus loin

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

CNIL — la vidéosurveillance au travail — www.cnil.fr/fr/la-videosurveillance-videoprotection-au-travail

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