

Objets connectés au bureau : caméras, imprimantes & co

Chaque appareil « intelligent » branché au réseau est un petit ordinateur — souvent jamais mis à jour, jamais surveillé.

9 min de lecture · Niveau Essentiel · cyberionis.fr/ressources/objets-connectes

Caméras IP, imprimantes, badgeuses, écrans connectés, capteurs, machine à café « smart » : le bureau moderne héberge des dizaines de petits ordinateurs que personne n'administre. Livrés avec des mots de passe d'usine, rarement mis à jour, souvent bavards vers Internet, ils sont devenus une porte d'entrée favorite des attaquants — précisément parce qu'on ne les regarde pas.

1. Pourquoi c'est un vrai sujet

- Un objet connecté EST un ordinateur : processeur, système, réseau — mais sans antivirus, sans supervision et avec un support fabricant souvent inexistant
- Une fois compromis, il sert de tête de pont : depuis la caméra, l'attaquant scanne le réseau, rebondit vers les postes et serveurs
- Les identifiants d'usine (admin/admin) sont publics : des moteurs de recherche spécialisés listent les appareils exposés, mot de passe inclus
- Les caméras posent en plus un problème RGPD : images de salariés et de clients, durées de conservation, information des personnes

CAS CONCRET

Le botnet Mirai a marqué l'histoire en enrôlant des centaines de milliers de caméras et enregistreurs livrés avec des mots de passe d'usine, pour lancer certaines des plus grosses attaques jamais vues. Les héritiers de Mirai recrutent toujours — et la caméra du parking fait un excellent soldat.

2. Les règles pour chaque appareil

- Changer le mot de passe d'usine à l'installation — LA règle numéro un
- Mettre à jour le firmware à l'installation, puis régulièrement ; préférer les marques qui publient encore des mises à jour
- Désactiver ce qui ne sert pas : accès depuis Internet, UPnP, services cloud du fabricant non utilisés, Telnet
- Se demander avant d'acheter : cet appareil a-t-il vraiment besoin d'être connecté ? Le grille-pain Wi-Fi peut rester bête
- Inscrire chaque appareil dans l'inventaire, avec son responsable et sa date de fin de support

3. Le cas de l'imprimante — l'oubliée universelle

L'imprimante-copieur de bureau mérite une mention spéciale : elle a un disque dur (qui garde copie des documents numérisés), une interface d'administration (souvent au mot de passe d'usine), des fonctions d'envoi d'emails, et un accès complet au réseau. C'est un serveur déguisé.

- Mot de passe administrateur changé, interface accessible uniquement depuis le réseau interne
- Firmware mis à jour lors des visites de maintenance — l'exiger du prestataire
- Effacement du disque avant restitution en fin de leasing (les contrats sérieux le prévoient — vérifiez)
- Numérisation vers email : configurée proprement, pas via un compte générique au mot de passe faible

4. Isoler : la défense qui pardonne tout

On ne pourra jamais garantir la sécurité intrinsèque de chaque gadget — la vraie réponse est l'isolement : un réseau (VLAN ou à défaut le réseau invité) dédié aux objets connectés, sans accès aux postes et serveurs. La caméra compromise n'atteint alors... que les autres caméras. Combiné à l'inventaire et aux mots de passe changés, ce cloisonnement transforme un parc d'objets incontrôlable en risque maîtrisé.

L'essentiel à retenir

- 01 Inventorier tous les objets connectés de l'entreprise
- 02 Changer chaque mot de passe d'usine
- 03 Mettre à jour les firmwares, écarter les appareils abandonnés par leur fabricant
- 04 Couper l'accès Internet des appareils qui n'en ont pas besoin
- 05 Isoler les objets connectés sur un réseau dédié
- 06 Traiter l'imprimante comme un serveur : mot de passe, mises à jour, disque effacé en fin de vie

Questions fréquentes

Comment savoir si un de nos appareils est déjà compromis ?

Signes évocateurs : appareil qui redémarre seul, devient lent, trafic réseau inhabituel, paramètres modifiés. Mais la plupart des compromissions sont silencieuses — d'où l'approche pragmatique : réinitialisation d'usine, mot de passe fort, firmware à jour et isolement réseau remettent les compteurs à zéro sans analyse coûteuse.

Les caméras « made in ailleurs » à bas prix sont-elles un risque ?

Le prix bas se paie souvent en sécurité : mots de passe codés en dur, mises à jour inexistantes, flux qui transitent par des serveurs dont vous ignorez tout. Certaines marques sont même interdites dans les administrations de plusieurs pays. Pour une entreprise, privilégiez les marques établies avec un vrai suivi de sécurité — et isolez-les quand même.

Et la vidéosurveillance côté RGPD ?

Règles CNIL : les caméras filment les biens et les accès, pas les salariés à leur poste en continu ; information par panneaux visibles ; conservation limitée (un mois maximum sauf circonstance particulière) ; accès aux images restreint et tracé. Une caméra mal positionnée ou des images conservées des années sont des motifs de sanction récurrents.

Pour aller plus loin

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

Cybermalveillance.gouv.fr — sécuriser les objets connectés — www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/securite-objets-connectes

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