

Sécuriser le Wi-Fi et le réseau de l'entreprise

Séparer les usages, verrouiller les équipements : les fondations d'un réseau sain.

9 min de lecture · Niveau Intermédiaire · cyberionis.fr/ressources/wifi-reseau

Le réseau est le système nerveux de l'entreprise. Un Wi-Fi mal configuré ou une box laissée avec ses réglages d'usine offrent un accès direct à tout ce qui y est connecté : postes, serveurs, imprimantes, caméras.

1. Le Wi-Fi

- Chiffrement WPA2 minimum, WPA3 si vos équipements le permettent
- Un mot de passe long et unique — changez celui inscrit sous la box
- Un réseau invité séparé pour les visiteurs et les appareils personnels
- Désactiver le WPS, vulnérable par conception
- Renommer le SSID sans y mettre le nom de l'entreprise si possible

2. Les équipements réseau

- Changer tous les mots de passe administrateur par défaut (box, routeur, NAS, imprimantes, caméras)
- Mettre à jour le firmware des équipements régulièrement
- Désactiver l'administration à distance quand elle n'est pas nécessaire
- Fermer les ports et services inutilisés

3. Aller plus loin : la segmentation

Séparer le réseau en zones (VLAN) — bureautique, serveurs, invités, objets connectés — limite la propagation d'une compromission : une caméra IP piratée ne doit pas pouvoir atteindre votre serveur de fichiers. C'est le type de chantier qu'un audit réseau permet de dimensionner correctement.

4. Savoir ce qui est connecté

On ne protège pas ce qu'on ignore. La plupart des réseaux de PME hébergent des appareils que personne n'a recensés : la caméra installée par un prestataire, le NAS d'un ancien projet, la prise connectée de la machine à café.

- Faire l'inventaire des appareils connectés (l'interface de la box ou du routeur les liste) et identifier chaque inconnu
- Débrancher ou isoler ce qui ne sert plus
- Refaire ce tour d'horizon deux fois par an — les appareils s'accumulent en silence
- En PME, un audit réseau professionnel cartographie tout cela et révèle les expositions involontaires vers Internet

CAS CONCRET

Cas réel récurrent : une caméra IP à 40 €, installée avec son mot de passe d'usine et accessible depuis Internet pour « voir le magasin de chez soi ». Elle apparaît dans les moteurs de recherche spécialisés (Shodan) en quelques jours — et offre un point d'entrée directement branché sur le réseau du magasin.

L'essentiel à retenir

- 01 Passer le Wi-Fi en WPA2/WPA3 avec un mot de passe robuste
- 02 Créer un réseau invité séparé (visiteurs et appareils personnels)
- 03 Changer les mots de passe par défaut de tous les équipements
- 04 Mettre à jour les firmwares (box, routeur, NAS, imprimantes)
- 05 Inventorier les appareils connectés deux fois par an
- 06 Étudier la segmentation du réseau avec un professionnel

Questions fréquentes

WPA2 ou WPA3, quelle différence concrète ?

WPA3 corrige les faiblesses connues de WPA2 (attaques par dictionnaire hors ligne notamment) et chiffre mieux les échanges. Activez le mode mixte WPA2/WPA3 si vos appareils anciens ne suivent pas. Le vrai danger est ailleurs : le WEP et le WPA d'origine, cassables en minutes, et les mots de passe d'usine jamais changés.

Faut-il cacher le nom du réseau (SSID) ?

C'est une protection illusoire : le réseau reste visible pour n'importe quel outil d'analyse Wi-Fi, et cela complique la vie des utilisateurs légitimes. Un chiffrement solide et un bon mot de passe protègent réellement ; un SSID caché, non.

Le réseau invité est-il vraiment utile pour une petite équipe ?

Oui, et pas seulement pour les visiteurs : il accueille aussi les téléphones personnels des collaborateurs et les objets connectés non critiques. Tout ce qui s'y connecte ne peut pas atteindre vos postes, serveurs et imprimantes — c'est une segmentation gratuite, incluse dans la plupart des box et routeurs.

Un VLAN, c'est indispensable pour une TPE ?

Pas forcément : pour une petite structure, un réseau invité bien utilisé couvre l'essentiel. Les VLAN se justifient dès qu'il y a des serveurs, des équipements sensibles (caisse, production, vidéosurveillance) ou des dizaines d'appareils — leur mise en place demande du matériel adapté et un professionnel.

Pour aller plus loin

Cybermalveillance.gouv.fr — sécuriser son réseau Wi-Fi — www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/reseaux-wifi

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