RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

LES ESSENTIELS

SÉCURISATION DES RÉSEAUX WI-FI

Le Wi-Fi est une technologie de communications radiofréquences destinée au déploiement de réseaux locaux sans-fil. Cette technologie présente de nombreux risques tels que l'interception ou la modification du trafic réseau.

Retrouvez, en une vingtaine de bonnes pratiques, les ressources essentielles de l'ANSSI pour déployer et utiliser le Wi-Fi de manière sécurisée en milieu professionnel.

1/ UTILISER LE WI-FI AVEC SON TERMINAL PROFESSIONEL

→ **Désactiver l'interface Wi-Fi et le partage de connexion Wi-Fi** quand ils ne sont pas utilisés.

→ **Désactiver la connexion automatique** aux réseaux Wi-Fi connus.

→ **Se connecter uniquement à des réseaux Wi-Fi maîtrisés ; si cela est impossible** (par exemple dans les gares, aéroports ou les cafés), **utiliser un VPN maîtrisé par l'entité.**

→ **Configurer le pare-feu local des ordinateurs portables** afin de bloquer les connexions entrantes, notamment via l'interface Wi-Fi.

→ **Supprimer les réseaux connus et les secrets associés** sur les terminaux avant reconditionnement, cession ou mise au rebut.

→ **Aller plus loin** en consultant l'état de la menace sur les téléphones mobiles.

2/ DÉPLOYER DES RÉSEAUX WI-FI MAÎTRISÉS PAR L'ENTITÉ

→ **Désactiver systématiquement la fonction *Wi-Fi Protected Setup* (WPS) des points d'accès.**

→ **Désactiver la fonction *Universal Plug and Play* (UPnP)** si non utilisée.

→ **Autoriser uniquement les points d'accès Wi-Fi maîtrisés par l'entité** sur le réseau. L'utilisation de points d'accès **Wi-Fi personnels en environnement professionnel est à proscrire**.

→ **Utiliser les modes de sécurité robustes et éprouvés :** WPA3-Enterprise, WPA2-Entreprise (sous condition) ou WPA3-Personal :

> en mode WPA3-Enterprise**, utiliser uniquement les suites EAP** (*Extensible Authentication Protocol*) supportant l'authentification par certificats. S'assurer de la validité et de la légitimité des certificats utilisés avant toutes connexions (Infrastructure de gestion de clés) ;

> en mode WPA2-Enterprise, **activer la protection des trames de gestion (PMF)** ;

> éviter le mode mixte WPA3/WPA2 ou les configurations de transition. Cela peut entraîner le partage des secrets entre les modes WPA2 et WPA3, ainsi qu'une dégradation de sécurité pour les terminaux supportant WPA3.

→ **Contrôler la diffusion des secrets d'authentification :**

> diffuser les secrets au seul personnel autorisé ;

> changer régulièrement les secrets de connexion et les modifier sans délais suite à une compromission ou suspicion de compromission.

V1.0 (08/26)

www.cyber.gouv.fr / conseil.technique@ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

→ **Cloisonner les réseaux par usage** :

> **cloisonner chaque Wi-Fi dans un VLAN distinct les uns des autres ainsi que des réseaux filaires. Contrôler les communications nécessaires entre ces réseaux** à l'aide d'équipements de filtrage (pares-feux) ;

> **utiliser des noms de réseau (SSID) distincts pour chaque mode de sécurité**, notamment si plusieurs configurations coexistent. Par exemple :

- un réseau nommé *Postes de travail* utilisant le mode WPA3-Enterprise ;
- un second réseau nommé *IoT* utilisant le mode WPA2-Enterprise pour les objets connectés de l'entité, tels que les automates ou Interface Homme Machine ne supportant pas WPA3. Ces équipements sont souvent plus vulnérables et ne supportent pas toujours les dernières normes de sécurité, c'est pourquoi il est important de leur dédier un réseau.

→ **Ne pas cacher le SSID** lors de la configuration des réseaux Wi-Fi. Il est inutile de masquer son SSID car un terminal précédemment connecté à un Wi-Fi au SSID caché diffusera le nom dudit réseau.

→ **Modifier le SSID proposé par défaut.** Éviter tout libellé trop explicite pouvant révéler une activité professionnelle ou des informations personnelles.

→ **Bloquer par défaut la connexion de terminaux non maîtrisés** (par exemple : téléphones personnels) avec l'enrôlement exclusif des terminaux maitrisés. Dans le cas d'un réseau Wi-Fi invité, celui-ci est dédié et cloisonné des autres réseaux.

3/ ADMINISTRER DES RÉSEAUX WI-FI SÉCURISÉS

→ **Journaliser les connexions des points d'accès et des contrôleurs Wi-Fi** :

> configurer les points d'accès et les contrôleurs pour que les évènements de sécurité puissent être collectés. Il est préférable de rediriger l'ensemble des évènements générés par les points d'accès et les contrôleurs vers une infrastructure centrale de supervision (cf. les Recommandations de sécurité pour l'architecture d'un système de journalisation) ;

> respecter la réglementation sur la conservation des données techniques de connexion pour les offres de Wi-Fi public (voir à ce sujet les ressources de la CNIL).

→ **Configurer, lorsque qu'une IGC existe, l'auto-enrôlement des certificats** par les stratégies de groupe Windows (GPO) afin que les postes reçoivent automatiquement le certificat nécessaire à leur authentification sur le réseau Wi-Fi. Restreindre ensuite l'accès au SSID concerné aux seules connexions authentifiées par certificat.

→ **Sécuriser l'administration des points d'accès et des contrôleurs Wi-Fi** :

> **modifier les éléments de connexions présents par défaut.** Cela inclut les secrets, tels que les mots de passe de connexion Wi-Fi et les certificats, mais aussi les mots de passe d'administration. Les secrets doivent être robustes, conformément aux Recommandations relatives à l'authentification multifacteur et aux mots de passe ;

> utiliser des protocoles d'administration sécurisés (TLS, SSH) ;

> connecter l'interface d'administration à un réseau d'administration dédié, sécurisé et cloisonné – cf. les Recommandations relatives à l'administration sécurisée des SI ;

> **déployer systématiquement et dans les meilleurs délais les mises à jour** des systèmes d'exploitation, des pilotes, des points d'accès, des contrôleurs et des terminaux.