AIDE-MÉMOIRE

PROTÉGER SON RÉSEAU SANS FIL

Objectif du document

Procéder à un paramétrage robuste et sécurisé d'une borne de réseau sans fil.

Les réseaux sans fil ou Wi-Fi sont souvent vulnérables et accessibles à des personnes malveillantes cherchant à intercepter des données sensibles (informations personnelles, codes de cartes de paiement, données d'entreprise, etc.).

Force est de constater que la problématique de sécurisation des réseaux sans fil n'est pas toujours bien comprise et que les risques courus sont souvent méconnus.

Destinataire du document : Administrateur de réseau

Date de la dernière modification : 2017-06

Les fondamentaux

La technologie sans fil repose sur un lien radio dont les ondes sont sujettes à l'interception et aux interférences (brouillage accidentel ou intentionnel des ondes). Plusieurs contextes justifient l'utilisation de connexions filaires. À défaut, la confidentialité des informations doit être assurée par l'utilisation de moyens de chiffrement complémentaires tels que l'IPsec ou TLS.

La sécurité et la robustesse d'un réseau sans fil dépendent en général :

- de l'accessibilité du réseau, c'est-à-dire de la portée des signaux électromagnétiques qui propagent le signal sans fil;
- des mécanismes d'authentification utilisés afin d'identifier les utilisateurs du réseau de manière univoque et sûre;
- des mécanismes cryptographiques mis en place afin de protéger les communications sans fil, lesquels sont souvent dérivés des mécanismes d'authentification;
- des mécanismes d'administration et de supervision des points d'accès du réseau et des terminaux utilisant le réseau;
- d'autres éléments de configuration des points d'accès sans fil.

La mise en place et l'utilisation du réseau sans fil doivent être encadrées par une politique de sécurité elle-même validée par la direction de l'organisation.

Recommandations

Sur tout type de terminal :

- N'activer l'interface sans fil que lorsqu'elle celle-ci doit être utilisée.
- Désactiver systématiquement l'association automatique aux points d'accès sans fil configurés dans le terminal afin de garder le contrôle sur la connectivité du terminal.
- Maintenir à jour le système d'exploitation et les pilotes du réseau sans fil du terminal.
- Éviter autant que possible de se connecter à des réseaux sans fil inconnus ou qui ne sont pas dignes de confiance.
- Bloquer, par configuration du pare-feu local, les connexions entrantes via l'interface sans fil.

Sur un terminal à usage professionnel :

- Respecter la politique de sécurité de l'entité, en particulier lorsqu'il s'agit de moyens cryptographiques d'authentification ainsi que de protection de la confidentialité et de l'intégrité.
- Ne pas brancher de borne personnelle sur le réseau de l'entité.
- En situation de mobilité, lors de toute connexion à des points d'accès sans fil qui ne sont pas dignes de confiance (ex. : à l'hôtel, à la gare ou à l'aéroport) et préalablement à tout échange de données, utiliser systématiquement des moyens de sécurité complémentaires (ex. : VPN IPsec).
- Mettre en place un protocole de sécurité spécifique tel que TLS ou IPsec lorsque des données sensibles doivent être véhiculées via un réseau sans fil.

Sur les points d'accès sans fil :

- Configurer le point d'accès pour utiliser un chiffrement robuste. Le mode WPA2 avec l'algorithme de chiffrement AES-CCMP est fortement recommandé. Pour les points d'accès personnels, utiliser le mode d'authentification WPA-PSK (WPA personnel) avec un mot de passe long (ex. : une vingtaine de caractères) et complexe, d'autant plus que ce dernier est enregistré et n'a pas besoin d'être mémorisé par l'utilisateur.
- Lorsque l'accès n'est protégé que par un mot de passe (WPA-PSK), il est primordial de changer régulièrement ce dernier, mais également de contrôler sa diffusion. En particulier, il convient de :
    - ne pas communiquer le mot de passe à des tiers non autorisés (ex. : prestataires de services)
    - ne pas écrire le mot de passe sur un support qui pourrait être vu par un tiers non autorisé
    - changer le mot de passe régulièrement et lorsque sa sécurité a été compromise.
- Pour les réseaux sans fil en environnement professionnel, mettre en place le mode WPA2 avec une infrastructure d'authentification centralisée en s'appuyant sur le mode WPA entreprise (standard 802.1x et protocole EAP), ainsi que des méthodes d'authentification robustes.
- Configurer le VLAN privé invité en mode *isolated* lorsque le point d'accès sans fil prend en charge cette fonctionnalité.
- Ne pas conserver un nom de réseau (SSID) générique et proposé par défaut. Le SSID retenu ne doit pas être trop explicite par rapport à une activité professionnelle ou une information personnelle.
- Désactiver systématiquement la fonction WPS (Wifi Protected Setup) des points d'accès.
- Sécuriser l'administration du point d'accès sans fil en :
    - utilisant des protocoles d'administration sécurisés (ex. : HTTPS)
    - connectant l'interface d'administration à un réseau filaire d'administration sécurisé, au moins en y empêchant l'accès aux utilisateurs sans fil
    - utilisant des mots de passe d'administration robustes.

- Configurer le point d'accès pour que les évènements de sécurité puissent être supervisés. En environnement professionnel, il est préférable de rediriger l'ensemble des évènements générés par les points d'accès vers une infrastructure centrale de supervision.

L'architecture réseau

- La couverture des réseaux sans fil doit être limitée aux zones nécessitant cette couverture.
- En environnement professionnel, isoler le réseau sans fil du réseau filaire et mettre en place des équipements de filtrage réseau permettant l'application de règles strictes et en adéquation avec les objectifs de sécurité de l'organisation. Comme pour le point d'accès, l'équipement de filtrage doit être paramétré pour que puissent être supervisés les évènements de sécurité.
- Si un réseau sans fil « visiteurs » doit être mis en place, il est recommandé de déployer une infrastructure dédiée à cet usage, isolée des autres et ne donnant accès à aucune ressource du réseau interne. Ce réseau doit par ailleurs avoir sa propre politique de sécurité beaucoup plus restrictive.

L'environnement *Active Directory*

- Mettre en place les objets de stratégies de groupe nécessaires à l'application de stratégies de sécurité verrouillant les configurations sans fil des postes clients Windows, de manière à appliquer techniquement différentes recommandations indiquées dans ce document.
- Afin de ne pas les communiquer aux utilisateurs, déployer sur les postes Windows les informations de connexion au réseau sans fil par objet de stratégie de groupe (nom de réseau, clé d'accès, certificats éventuels si la méthode EAP le nécessite, etc.).