Comparaison des différents protocoles de sécurité wifi

La sécurité des réseaux sans fil vise à empêcher les utilisateurs non autorisés de se connecter à un réseau Wi-Fi spécifique. Elle permet également de protéger vos données, en s'assurant qu'elles ne peuvent être consultées que par les utilisateurs autorisés à se connecter à votre réseau.

Quels sont les différents types de sécurité Wi-Fi ?

Pour garantir cette sécurité, plusieurs protocoles ont été développés par la Wireless Alliance. Parmi eux, on trouve le Wired Equivalent Privacy (WEP), le Wi-Fi Protected Access (WPA), le Wi-Fi Protected Access 2 (WPA2) et le Wi-Fi Protected Access 3 (WPA3). Il est essentiel de connaître ces différents protocoles et de savoir lequel est utilisé par votre réseau pour assurer une protection optimale.

WEP :

Le WEP, ou Wired Equivalent Privacy, est un protocole de sécurité pour les réseaux sans fil, apparu en 1997. Il chiffre les données pour les rendre illisibles aux pirates, mais utilise une clé statique de 64 ou 128 bits, ce qui le rend vulnérable. Malgré des révisions, des failles de sécurité ont été découvertes, et la Wi-Fi Alliance a retiré le WEP en 2004. Aujourd'hui, il est considéré comme obsolète, bien qu'il soit encore parfois utilisé sur des appareils anciens ou non mis à jour.

WPA :

Le WPA, ou Wi-Fi Protected Access, a été introduit en 2003 pour remplacer le WEP. Contrairement au WEP, qui utilise une clé statique, le WPA utilise le protocole TKIP pour changer dynamiquement les clés, rendant plus difficile pour les intrus de pirater le réseau. Plus tard, le TKIP a été remplacé par l'Advanced Encryption Standard (AES) pour une sécurité encore meilleure. Le WPA inclut également des contrôles d'intégrité des messages pour détecter les modifications des paquets de données. Malgré ces améliorations, des failles ont été découvertes, menant à l'introduction du WPA2. Une clé WPA est simplement le mot de passe utilisé pour se connecter à un réseau sans fil, souvent imprimé sur le routeur ou fourni par le gestionnaire du réseau.

WPA2 :

Le WPA2, ou Wi-Fi Protected Access 2, a été introduit en 2004 comme une version améliorée du WPA. Il fonctionne en deux modes : le mode personnel (WPA2-PSK) pour les environnements domestiques et le mode entreprise (WPA2-EAP) pour les usages professionnels. Les deux modes utilisent le protocole CCMP basé sur l'algorithme AES, offrant une meilleure sécurité que le TKIP du WPA. Cependant, le WPA2 présente des vulnérabilités, notamment aux attaques, mais reste plus sûr que le WEP ou le WPA.

WPA3 :

Le WPA3, introduit en 2018, améliore la sécurité Wi-Fi avec des fonctionnalités avancées. Il permet d'autoriser les appareils via des étiquettes NFC ou des codes QR, au lieu d'un mot de passe partagé. Le protocole d'authentification simultanée d'égaux crée une connexion sécurisée, même avec un mot de passe faible. De plus, le WPA3 protège mieux contre les attaques par force brute en limitant les tentatives de deviner le mot de passe hors ligne. Les appareils WPA3, disponibles depuis 2019, sont compatibles avec ceux utilisant le WPA2.