4

Bien sécuriser son réseau sans-fil Wi-Fi domestique

CENTRE DE RECHERCHE
SUR L'INFORMATION
SCIENTIFIQUE ET TECHNIQUE
cerist

Bien sécuriser son réseau sans-fil Wi-Fi domestique

Le Wi-Fi (Wireless Fidelity) est une technologie permettant de créer avec aisance des réseaux informatiques sans fil. Sa portée varie de quelques dizaines de mètres à plusieurs centaines de mètres, ce qui en fait une technologie de premier choix pour le réseau domestique avec connexion internet. Elle est de plus en plus utilisée par divers matériels informatiques :
ordinateur, Assistant personnel (PDA), Smartphone, console de jeux, portable, etc. La Sécurité de ce type de réseau, souvent négligée et toujours source de problème, vient du fait qu'il est facile de monter un réseau Wi-Fi mais qu'il est un peu plus difficile de le sécuriser.
Parmi les risques liés à cette technologie, on trouve : l'écoute ou le vol d'informations personnelles, l'intrusion au réseau local, l'utilisation de la connexion Internet à l'insu de son propriétaire.
Plusieurs mécanismes existent pour assurer un niveau de sécurité acceptable, on parle toujours de filtrage d'adresse MAC, WEP, WPA, etc.

Bonnes pratiques pour sécuriser son réseau Wifi:

- **Désactiver la diffusion du SSID :** Le SSID identifie le réseau. C'est un nom qui est utilisé pour différencier votre réseau sans-fil des autres. Si vous désactivez sa diffusion, celui-ci n'apparaitra pas dans la liste des connexions possibles de vos voisins.

- **Utiliser le chiffrement :** Le WEP (Wired Equivalent Privacy) et WPA (Wi-Fi Protected Access) sont deux possibilités pour chiffrer (donc pour protéger) les données qui circulent sur votre réseau. Comme vous ne pouvez pas savoir qui est à l'écoute, le

chiffrement de vos données permet d'en assurer la confidentialité. Cela se fait à l'aide de ce que l'on appelle une clef. Si on ne connaît pas cette clef, il devient impossible de lire ou de transmettre des données valides.
Le système WPA est plus efficace que le système WEP. Privilégiez donc WPA si votre Point d'accès/carte sans fil le supporte.

• **Utiliser le filtrage d'adresse MAC :** Chaque carte réseau possède un identifiant unique pour la reconnaître, c'est l'adresse MAC. Dans l'utilitaire de configuration de votre modem/routeur Wifi, il vous faut activer l'option de filtrage puis saisir les adresses MAC de chacune des machines qu'on autorise à se connecter à votre réseau.

• **Désactiver Le Serveur DHCP :** DHCP (Dynamic Host Configuration Protocole) est un mécanisme qui permet d'affecter automatiquement des paramètres nécessaires à la communication sur le réseau (adresse IP, masque de sous-réseau, passerelle, DNS). C'est très pratique d'utiliser le DHCP mais un pirate n'aura pas alors à deviner la configuration de votre sous-réseau. Donc, autant se mettre en configuration fixe : vous choisissez votre IP et vous la conservez.

• **Combiner les mécanismes de sécurité :** Chacun des mécanismes de sécurité cités peut être contourné d'une façon ou d'une autre. Pour avoir un bon niveau de sécurité utilisez une combinaison de ces mécanismes. Le minimum étant d'utiliser WEP et un filtrage par adresse MAC.

WPA2 est supporté dans les nouvelles cartes/points d'accès Wi-Fi. WPA2 permet d'avoir un niveau de sécurité supérieur à celui de WPA. Il est conseillé de l'utiliser quand c'est possible.


Stat
Attn
DDR
Stat
Attn
DDR
Stat
Attn
DDR
Stat
Attn
DDR
Stat
Attn
DDR