**Sécurité réseau :**

Lorsque l’on installe un réseau sans fil généralement nous le sécurisons aussi car installer un réseau sans fil sans le sécuriser peut permettre à des personnes non autorisées d’écouter, de modifier de d’accéder à ce réseau. Il est donc primordial de sécuriser les réseaux sans fil dès leur installation. Il existe plusieurs moyens de sécuriser son réseau de façon plus ou moins forte selon les ressources et leur importance.

Nous pouvons par exemple changer les mots de passe par défaut comme par exemple celui de l’administrateur, modifier la configuration par défaut, désactiver les services disponibles non utilisés ou régler la puissance d’émission du point d’accès au minimum nécessaire.

Il faut faire les mises à jour dès que celle-ci sont possibles. Nous pouvons aussi changer le SSID par défaut car il est plus judicieux de ne pas choisir un SSID attractif.

Pour sécuriser correctement ces données qui transitent sur un réseau y ajouter un chiffrement. L’absence de chiffrement dans un réseau sans fil laisse l’ensemble des données qui transitent sur ce réseau à la merci d’une personne munie d’une carte Wi-Fi.

Le protocole initialement proposé pour le chiffrement des communications entre éléments d’un réseau sans fil est le WEP. Ce protocole WEP utilise une clé d’une longueur de 64 à 256 bits dont 24 ne sont pas utilisés pour le chiffrement. Cela fait une clé, si on la compare à un mot, d’une longueur de 5 à 29 caractères. La majorité des clés est composée de 13 caractères. L’algorithme utilisé dans le chiffrement possède une grande faiblesse qui est exploitée. Le WEP est rapidement incapable d’offrir un niveau de sécurité suffisant pour la plupart des utilisateurs car il est possible en surveillant une quantité de trafic suffisante de casser une clef WEP en seulement quelques secondes. De plus, le chiffrement WEP introduit des problèmes de gestion de clefs qui dégradent rapidement la sécurité du réseau.

Le protocole WPA offre une protection d’un niveau bien supérieur à WEP. Il utilise le même algorithme de chiffrement et est basé sur le même principe. En revanche le TKIP (Temporal Key Integrity Protocol ou Protocole d’intégrité par clé temporelle) a été ajouté, permettant ainsi une permutation plus importante des clés sans que le vecteur d’initialisation ne puisse être reconstitué de manière utile. Le protocole WPA2 quant à lui utilise un algorithme de chiffrement beaucoup plus puissant, utilisé dans le cryptage des documents sensibles et possédant une clé très forte. Il s’agit de la dernière norme du protocole WPA permettant de protéger votre réseau WLAN.