La sécurité Wifi

La formation « Sécurité Wifi » vous permettra d'apprendre à mettre en place et gérer un réseau Wifi et sa sécurité. Le programme est donné à titre indicatif et sera adapté à vos besoins et votre niveau après audit. N'hésitez pas à nous contacter pour toute demande spécifique.

Pré-requis

Les connaissances des concepts, de la terminologie et des solutions réseaux sont supposées acquises.

Public concerné

Toute personne qui gère, utilise, contrôle ou met en place des réseaux sécurisés.

Durée et tarif de la formation

La durée de la formation varie en fonction des besoins et des objectifs déterminés après audit. Les tarifs sont disponibles sur devis.

Contenu de la formation

Principes des réseaux sans fil

Introduction aux réseaux sans fil Comparaison avec le fixe.

Les diverses générations de réseaux sans fil. Les PAN, les WPAN, les LAN, les WLAN

Les performances attendues.

Wi-Fi : IEEE 802.11

Wi-Fi et ses particularités.

Les équipements Wi-Fi : cartes et points d'accès.

Les bandes de fréquences.

L'intégration dans le monde Ethernet.

Les architectures.

Les débits et les performances.

La technique d'accès au support physique.

Le mode d'économie d'énergie.

La qualité de service.

La gestion des réseaux Wi-Fi.

Mise en place d'un réseau Wi-Fi

Les contraintes.

Le choix des équipements.

Le coût de l'installation.

Configuration d'un réseau Wi-Fi.

Politique de sécurité dans un réseau Wi-Fi.

Sécurité WiFi

Faiblesses intrinsèques des réseaux sans fil Est-il possible de se protéger des attaques de type déni de service ?

Comment contrôler la zone d'émission ? Peut-on éviter le vol des informations ?

Le rôle du SSID en matière de sécurité.

Les faiblesses des solutions d'authentification. Fonctions élémentaires : SSID et MAC Filtering

Wired Equivalent Privacy – WEP

Détails du fonctionnement et présentation des faiblesses.

Problématique d'échange des clefs.

Méthode d'authentification et de chiffrement.

WiFi Protected Access – WPA

Détails du fonctionnement.

Les principaux avantages de WPA sur WEP.

Extensible Authentication Protocol – EAP.

Temporal Key Integrity Protocol – TKIP.

Message Integrity Check – MIC.

Les points sensibles et les risques résiduels. WPA v2 et norme 802.11i.

L'architecture réseau, interconnexion des LAN et des WLAN

Contrôle de la zone de couverture.

Segmentation du réseau.

Firewall et zones démilitarisées.

Protection du poste client.

Utilisateurs nomades, VPN et réseaux sans fil.