Sécurité des SI Risques et Protection initiation

Durée : 3 jours Référence : SECSI1

Cette Formation présente les problèmes de sécurité des SI. Elle vise à apporter aux participants les connaissances de bases indispensables pour :

- Apporter des réponses pratiques à la question : comment sécuriser mon Système d'information
- Comprendre les enjeux et les risques sécurité ainsi que leurs éventuels impacts sur le SI
- Se familiariser avec les notions et les concepts sécurité des réseaux et du SI en général
- Contribuer au choix des équipements, outils et mécanismes de sécurité

Contenu

- Concepts fondamentaux de la sécurité des SI
- Natures et types d'attaques
- Techniques de Firewalling
- Principes de la cryptographie
- Le cloisonnement et le zonage
- Les VPN
- Management de la SSI

Participants

Responsable sécurité, ingénieur et administrateur sécurité, Chef de projet sécurité, architecte, développeur et Responsable informatique.

Pré-requis

Très bonnes connaissances du fonctionnement des protocoles TCP-IP. Connaître les principes fondamentaux et les concepts réseaux.

Programme

Concepts fondamentaux de la sécurité

- Définitions : sécurité informatique, sécurité du système d'information, sécurité de l'information,
- Périmètre et domaines de sécurité (physique, logique, réseaux, systèmes, Transactions,..)
- Problèmes de sécurité liés à IP (réseaux et applications),
- Définitions Menaces, risques, vulnérabilités

Nature et types d'attaques

- Services et Critères DICP de la sécurité :
- Analyse de risques.
- Attaques de type écoutes frauduleuses : man-in-the-middle, ARP Spoofing, MAC flooding, MAC Duplicating, IP spoofing, , hijacking,
- Attaques de type de services : SYN Flooding, Buffer Overflow, Cross Site Scripting, SQL Injection

Techniques de Firewalling

- Principes de filtrage,
- Niveaux de filtrage : réseaux, applications, données,
- Les équipements FireWall, Firewall personnel, proxy, Reverse proxy

Principes de Cryptographie

- Confidentialité : Algorithme chiffrement symétrique asymétrique (DES, 3DES, RSA, AES…)
- Intégrité : Algorithme de hachage (MD5, SHA-1, …)
- Authentification : usage des clés publiques et privées (Certificat x.509)
- Le masquage, le hachage, le scellement
- Le HMAC
- Infrastructure des clés publiques (PKI)

Le cloisonnement et le zonage

- Architecture réseaux : VLAN, DMZ, DMZ étendue,

- Les VPN (niveau 2 : PPTP, L2TP- niveau 3 : IPsec , autres : VPN-SSL)
- Contrôle des accès et notamment les accès distants

Les VPN-IPsec & les VPN-SSL

- Présentation de deux technologies
- Comparatif selon cahier des charges
- Choix de la solution adaptée aux besoins

Management de la sécurité des SI

- Élaborer une Politique de sécurité réseau,
- Chartes et aspects juridiques,
- Sensibilisation des utilisateurs