



FORMATION DÉCOUVERTE À LA SÉCURITÉ DES SYSTÈMES D'INFORMATIONS

OBJECTIFS

Ce stage permet aux participants d'acquérir le vocabulaire du domaine et de comprendre les principes essentiels de la sécurité des systèmes d'information.

À l'issue de la formation, les stagiaires seront capables de :

- comprendre les différentes menaces internes / externes du monde IP
- définir la terminologie
- décrire les concepts du domaine de la sécurité des systèmes d'information,
- décrire les principes des outils de protection (firewall, authentification, VPN, chiffrement, outils de surveillance, détection d'intrusion et de vulnérabilité et en appréhender les technologies,
- définir les avantages et limites de chaque technologie
- identifier les principaux éléments de l'offre du marché

MÉTHODE

Les exposés théoriques sont illustrés d'exemples concrets et de représentations schématiques accessibles. Le formateur restera disponible aux questions de la salle, et y répondra immédiatement dans la mesure du possible. Tout au long de la formation, du temps sera consacré à des jeux de questions réponses, permettant d'intégrer les notions de base et de les manipuler en groupe.

PERSONNES CONCERNÉES, PRÉREQUIS

DSI, nouvellement chargé de la sécurité des SI, toute personne nouvellement en charge de la sécurité des SI. Aucun pré requis n'est nécessaire pour cette formation d'introduction, de bonnes bases informatiques sont nécessaires.

DURÉE

Deux jours de formation en intra-entreprise pour 3 à 10 participants.

Sécurité du système d'information

- utilisateurs fixes et itinérants, administrateurs

Les systèmes informatiques

- les systèmes d'exploitation
- les services Internet
- les services de stockage et de sauvegarde
- architecture des réseaux LAN et WAN, les VPN
- sécurité physique et logique, statistiques
- certificat, coûts d'immobilisation, évaluation

Risques et attaques

- indisponibilités, altération, écoute, etc.
- intrusion et injection de codes : virus, cheval de Troie, ver, etc
- attaques structurées et non structurées
- attaques composites
- usurpation d'identité,
- types d'attaques et de risques : passive et active

Les services de sécurité

- filtrage, chiffrement, contrôle d'accès, authentification, confidentialité, intégrité, disponibilité, facilité d'utilisation

Les technologies

- les firewalls et les proxies, serveurs d'authentification
- la détection d'intrusion (IDS)
- chiffrement, PKI, certificat, authentification, Radius
- protocoles sécurisés : S-HTTP, SSL, S/MIME

Les solutions

- architecture, DMZ, et DMZ étendue
- solutions génériques : routeur, firewall, carte à puce, etc
- VPN : IPSec et VPN SSL

La démarche de sécurité

- politique de sécurité, standard ISO 17799 ou BS 7799
- les certifications IPSec, Critères Communs
- audits : les différentes méthodes
- le plan de secours, la gestion de crise