Etatdel'art

Sécurité des SI

SSI — 3 JOURS

Description

La sécurité des informations est une problématique constante des systèmes d'information pour les entreprises. Comment protéger les données dans la société ? en dehors de la société ? contre quels risques ?

Déroulement

Notre formation vous permet en 3 jours d'avoir un état de l'art des techiques, technologies et méthodes pour assurer la sécurité de vos données et services.

Protéger le poste client (virus, ver, logiciels espions, mauvaises manipulation...), protéger les serveurs (tolérance aux pannes, vols d'informations), protéger les accès au réseau (Wireless, VPN, connexion Internet), protéger les accès aux services (éviter les dénis), se protéger contre le social engineering...autant de points clés à surveiller et sécuriser pour garantir une pérennité des données dans le réseau et lors de leur transit.

Public

- Responsable informatique
- Administrateur systèmes et réseaux
- Chefs de projet
- RSSI

Pré-requis

- Culture générale du fonctionnement d'un système d'informations
- Notions de base de la sécurité

Certifications

- Certification par l'Institut Européen de Management des entreprises

Programme

Analyse des risques

- Connaître son SI
- PC final et serveur
- Quelles sont les données externalisées (cloud) ?
- Méthodes d'accès aux réseaux
- Gestion des autorisations
- Risques de piratage
- Risques de perte d'information
- Risques de vols d'information
- Risques naturels
- Les risques d'ingénierie sociale

Mise en oeuvre d'une politique de sécurité

- La sécurité physique
- Sécurité des installations (incendies, inondations, vols...)
- Prévision d'un plan de continuité et de reprise
- Contrôler les accès
- La sécurité des services
- Sécuriser les applications
- Technologies VPN
- Utilisation d'une DMZ
- Comment intégrer la disponibilité et la mobilité des collaborateurs

Management de la sécurité

- Les méthodes
- Marion, Melissa, Méhari, EBIOS
- Les limites de ces méthodes
- Les audits de sécurité
- Mener un audit dans une entreprise multisites
- Expliquer les enjeux de la sécurité aux utilisateurs finaux et aux directions
- Mise en oeuvre technique de la sécurité
- Stress du système
- Amélioration de la sécurité
- Savoir protéger les investissements au meilleur coût pour les meilleures raison
- Comunications sur la politique de sécurité
- Comment réagir à une attaque (en interne, en externe)
- Les limites du plan de sécurité et les dispositions juridiques
- Définition et rôle du RSSI

Vous serez capable de...

Evaluer les menaces matérielles et immatérielles sur votre système d'information et connaître les techniques de remédiation

- Comprendre les menaces sur les équipements de l'infrastructure
- Mettre en place une politique interne (technologique et humaine) de sécurité des informations
- Choisir les dispositifs et emplacements de sécurité
- Concevoir le Plan de Sécurité

egilia®