

Sécuriser l'informatique de l'entreprise : Aspects Techniques et Juridiques

1 jour

SEC200

OBJECTIF

Apprendre les notions fondamentales pour sécuriser l'informatique de l'entreprise dans tous ses aspects Techniques et Juridiques.
Evaluer les risques, garantir la fiabilité et la sécurité des données.
Concevoir une stratégie de gestion de la sécurité.

PUBLIC CONCERNÉ

Administrateurs systèmes et réseaux.

PRÉ-REQUIS

Notions de base de l'administration des systèmes d'information.

PROGRAMME

Matin : Aspects Techniques

INTRODUCTION

- Les challenges de la sécurité informatique
- Connaître les menaces potentielles
- Stratégies, méthodologie et procédures
- Comment se déroule une attaque ?

SECURISER

> Sécuriser le réseau

- Les concepts de base des réseaux
- Les pare-feu
- Cryptage et sécurisation des protocoles Internet
- Identification et cryptage du mot de passe
- Les Réseaux Privés Virtuels (RPV/VPN)
- Protection des réseaux sans fil (Wi-Fi)

> Sécuriser les systèmes d'exploitation et les applications

- Les niveaux de complexité des mots de passe
- Autres techniques d'identification
- Les mesures à prendre application par application

> Sécuriser les paiements électroniques

- Les paiements par carte bancaire en ligne
- Côté utilisateur : comment protéger son numéro de carte ?
- Les autres modes de paiement en ligne

> Virus et antivirus

- Les antivirus
- Les principales voies d'infection
- La protection du serveur de messagerie
- La protection du logiciel client messagerie
- Protéger les autres voies d'infection
- Choix de l'antivirus
- Se tenir informer de l'actualité des virus
- EICAR - Virus de test
- Comment limiter et détecter une infection ?
- Comment désinfecter une machine déjà infectée ?

- Qu'est-ce que les cookies ? Sont-ils une menace ?

SURVEILLER

> Détection d'intrusion

- Systèmes de détection d'intrusions (IDS/IPS)
- Honeypot
- Contrôle d'intégrité
- Enregistrement du trafic réseau
- Analyse du trafic réseau à l'aide d'un sniffeur
- Analyse des logues

> Administration de la sécurité - tests d'intrusions

- Politique de sauvegarde
- Comment agir en cas de sinistre ?
- Détection de vulnérabilité
- Tests d'intrusion
- Feuille de route de la sécurité
- Veille technologique
- Check-list

> Risque humain et approche sociale

- L'ingénierie sociale
- Sécurisation des accès physiques
- Comment identifier vous-même le pirate ?
- Les mesures à prendre

Sécuriser l'informatique de l'entreprise : Aspects Techniques et Juridiques

1 jour

SEC200

Après-midi : Aspects Juridiques

INTRODUCTION

LES ACTEURS DE L'INTERNET : RESPONSABILITES

> La responsabilité des intermédiaires techniques

- Opérateurs
- Fournisseurs d'accès
- Fournisseurs d'hébergement

> La responsabilité des fournisseurs de contenus

- Fournisseurs de contenus
- Fournisseurs de liens hypertextes
- Gestionnaires de forum de discussion
- Blogueurs

INFRACTIONS PENALES & INTERNET

> Présentation de la loi Godfrain

> Atteintes aux systèmes d'information

- Accès et maintien frauduleux
- Atteinte à l'intégrité du système
- Atteinte à l'intégrité des données
- Renforcement de la loi Godfrain
- Autres infractions relatives aux SI
- Sanctions encourues

> Les autres infractions

- Infractions de presse
- Atteintes à l'ordre public
- Atteintes aux mineurs

INFORMATIQUE ET LIBERTES

> La problématique des données personnelles pour les administrateurs techniques

> Présentation de la CNIL et de la loi Informatique et Libertés

- La CNIL
- La CNIL en action
- La loi et ses principes
- Les différents régimes (déclaration, autorisation, avis)
- Les droits des personnes

> La vie privée en entreprise et la cybersurveillance

- Contrôle de l'employeur sur l'outil de travail
- Le contrôle de l'utilisation d'Internet
- Le contrôle de l'utilisation de la messagerie
- Autres situations concrètes

> Les règles spécifiques

- Cookies, spamming
- Données de connexion
- Sites web, annuaires professionnels

> La biométrie en entreprise

DROIT D'AUTEUR & NUMERIQUE

> Les droits de l'auteur

- Les droits de l'auteur
- Les exceptions en bref

> L'exception de copie privée

> Lutte contre la copie numérique illicite

> Typologie et protection des œuvres numériques

- Bases de données
- Liens hypertextes
- Logiciels libres

LA SECURITE DES ECHANGES

> La preuve, la signature et l'archivage électroniques

- Admission de la preuve électronique
- Signature électronique
- Archivage électronique

> La cryptologie

SECURISER NORMATIVEMENT UN SYSTEME D'INFORMATION

> Les normes

- Variété des normes

> Utilité et conséquences