Sensibilisation sur la sécurité SI

Durée : 1 jour Référence : SESSI

Cette formation vous fera connaître les risques et les conséquences d'une action utilisateur, portant atteinte à la sécurité du système d'information. Présentation des principales techniques mises en place dans l'entreprise.

Contenu

- Introduction
- La sécurité informatique : comprendre les menaces/risques
- Vers une utilisation responsable et sécurisée
- Implication dans la sécurité du SI
- Agir pour une meilleure sécurité

Participants

Tous les utilisateurs du SI.

Pré-requis

Aucune connaissance particulière.

Programme

Introduction

- Cadre général : qu'entend-on par sécurité informatique (menaces, risques, protection).
- Comment une négligence peut créer une catastrophe. Quelques exemples. La responsabilité.

La sécurité informatique : comprendre les menaces/risques

- Les composantes d'un SI et leurs vulnérabilités
    - Systèmes d'exploitation client et serveur…

  - Réseaux d'entreprise (locaux, site à site, accès par Internet). Réseaux sans fils et mobilité.
  - Les applications à risques : Web, messagerie ...
  - Base de données et système de fichiers.
- Menaces et risques
  - Sociologie des pirates. Réseaux souterrains. Motivations.
  - Typologie des risques. La cybercriminalité en France.
  - Vocabulaire (sniffing, spoofing, smurfing, hijacking...).

Vers une utilisation responsable et sécurisée

- La protection de l'information
  - Vocabulaire.
  - Confidentialité, signature et intégrité.
  - Comprendre les contraintes liées au chiffrement.
  - Schéma général des éléments cryptographiques.
- La sécurité du poste de travail
  - Windows, Linux ou MAC OS : quel est le plus sûr ?
  - Gestion des données sensibles.
  - La problématique des ordinateurs portables.
  - Menace sur le poste client.
  - Comprendre ce qu'est un code malveillant.
  - Gestion des failles de sécurité.
  - Le port USB : fuite, attaque et confidentialité.
  - Le rôle du firewall client.
- L'authentification de l'utilisateur
  - Contrôles d'accès : authentification et autorisation.
  - L'importance de l'authentification.
  - Le mot de passe traditionnel.
  - Authentification par certificats et token.
- Les accès depuis l'extérieur
  - Accès distant via Internet. Comprendre les VPN.
  - De l'intérêt de l'authentification renforcée.

Implication dans la sécurité du SI

- Analyse des risques, des vulnérabilités et des menaces.
- Les contraintes réglementaires et juridiques.
- Pourquoi mon organisme doit respecter ses exigences de sécurité.
- Les hommes clés de la sécurité : comprendre le rôle du RSSI et du Risk manager.

Agir pour une meilleure sécurité

- Les aspects sociaux et juridiques. La CNIL, la législation.
- La cyber-surveillance et la protection de la vie privée.
- La charte d'utilisation des ressources informatiques.
- Conclusion.
    - Les bons réflexes.
    - Construire un plan de traitement des risques à partir de la matrice des risques et des autres sources (audits, incidents).
    - Que contient le plan : les objectifs et les mesures, les indicateurs d'avancement et de qualité.
    - Les risques résiduels.
    - La gestion et les usages du plan de traitement des risques.
    - Etude de cas
    - Réalisation d'un plan de traitement des risques.