Introduction à la sécurité informatique

Cours Synthèse de 1 jour - 7h
Réf : ISI - Prix 2024 : 950CHF HT

Avec l'évolution d'Internet, la sécurité des SI devient de plus en plus importante aussi bien dans un cadre privé que professionnel. Cette introduction à la sécurité des SI, vous présentera les risques et les menaces portant atteinte à la sécurité du système d'information.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Comprendre les risques et les menaces qui peuvent atteindre le SI

Les conséquences possibles d'une attaque informatique

Identifier les mesures de protection de l'information

Apprendre les actions nécessaires à la sécurisation de son poste de travail

Favoriser la conduite de la politique de sécurité SI de l'entreprise

LE PROGRAMME

dernière mise à jour : 10/2018

1) Les menaces et les risques

- Qu'est-ce la sécurité informatique ?
- Comment une négligence peut-elle créer une catastrophe ?
- Les responsabilités de chacun.
- L'architecture d'un SI et leurs vulnérabilités potentielles.
- Les réseaux d'entreprise (locaux, distantes, Internet).
- Les réseaux sans fil et mobilité. Les applications à risques : Web, messagerie...
- La base de données et système de fichiers. Menaces et risques.
- La sociologie des pirates. Réseaux souterrains. Motivations.

2) La sécurité du poste de travail

- La confidentialité, la signature et l'intégrité. Les contraintes liées au chiffrement.
- Les différents éléments cryptographiques. Windows, Linux ou MAC OS : quel est le plus sûr ?
- Gestion des données sensibles. La problématique des ordinateurs portables.
- Les différentes menaces sur le poste client ? Comprendre ce qu'est un code malveillant.
- Comment gérer les failles de sécurité ?
- Les ports USB. Le rôle du firewall client.

3) Le processus d'authentification

- Les contrôles d'accès : l'authentification et l'autorisation.
- L'importance de l'authentification.
- Le mot de passe traditionnel.
- L'authentification par certificats et par token.
- La connexion à distance via Internet.
- Qu'est-ce qu'un VPN ?
- Pourquoi utiliser une authentification renforcée.

PARTICIPANTS

Tous les utilisateurs souhaitant se former aux fondamentaux de la sécurité informatique.

PRÉREQUIS

Connaître le guide d'hygiène sécurité de l'ANSSI.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

4) Le cadre juridique et les bons réflexes à avoir

- Quelles sont les contraintes réglementaires et juridiques.
- Pourquoi on doit respecter ces exigences de sécurité ?
- Agir pour une meilleure sécurité : les aspects sociaux et juridiques.
- La CNIL (Commission Nationale de l'Informatique et des Libertés) et la législation.
- Qu’est-ce qu’une analyse des risques, des vulnérabilités et des menaces ?
- Comprendre le rôle du RSSI et du Risk Manager.
- La cybersurveillance et la protection de la vie privée.
- La charte d'utilisation des ressources informatiques. La sécurité au quotidien et les bons réflexes à avoir.

LES DATES

CLASSE À DISTANCE
2024 : 17 juin, 30 sept., 25 nov.