Sécurité des Systèmes d'Information, synthèse organiser la sécurité de votre SI : de l'analyse des risques à la mise en œuvre des solutions de sécurité

Séminaire de 3 jours - 21h
Réf : SSI - Prix 2024 : 2 890CHF HT

Avec l'explosion du digital qui a multiplié les opportunités de développement, le management de la sécurité des Systèmes d'Information est devenu un enjeu majeur pour toutes les entreprises. Ce séminaire très riche vous présentera l'ensemble des actions et des solutions permettant d'assurer la sécurité de votre SI : de l'analyse des risques à la mise en œuvre optimale de solutions de sécurité.

OBJECTIFS PÉDAGOGIQUES

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

Maîtriser le processus de gouvernance de la sécurité

Utiliser les référentiels métiers et les normes associées de la série ISO 27K

Connaître le cadre juridique français et européen (LPM, NIS, RGPD, …)

Planifier un plan d'actions pour atteindre les objectifs de la politique de sécurité

Elaborer une riposte adéquate et proportionnée pour réduire les risques cyber

LE PROGRAMME

dernière mise à jour : 12/2019

1) Les fondamentaux de la sécurité du système d'information

- La définition des actifs processus/information et actifs en support (informatique).
- La classification DICT/P : Disponibilité, Intégrité, Confidentialité et Traçabilité/Preuve.
- La définition du risque SSI et ses propriétés spécifiques (vulnérabilités, menaces).
- Les différents types de risques : accident, erreur, malveillance.
- L'émergence du cyber risque, les APT, se préparer à une cyber crise.
- Les sources d'information externes incontournables (ANSSI, CLUSIF, ENISA, etc.).

2) La task force SSI : de multiples profils métiers

- Le rôle et les responsabilités du RSSI / CISO, la relation avec la DSI.
- Vers une organisation structurée et décrite de la sécurité, identifier les compétences.
- Le rôle des "Assets Owners" et l'implication nécessaire de la direction.
- Les profils d'architectes, intégrateur, auditeurs, pen-testeurs, superviseurs, risk manager, etc.
- Constituer un équipe compétente, formée et réactive aux évolutions du cyber espace.

3) Les cadres normatifs et réglementaires

- Intégrer les exigences métiers, légales et contractuelles. L'approche par la conformité.
- Un exemple de réglementation métier : PCI DSS pour protéger ses données sensibles.
- Les mesures de sécurité pour atteindre un objectif de confidentialité, intégrité des données.
- Un exemple de réglementation juridique : directive NIS/ Loi Programmation Militaire.
- Les 4 axes de la sécurité vue par l'Europe et l'ANSSI : Gouvernance, Protection, Défense et Résilience.
- Les mesures de sécurité pour atteindre un objectif de disponibilité, intégrité des processus.

PARTICIPANTS

Ingénieurs prenant les fonctions de RSSI, directeurs ou responsables informatiques, ingénieurs ou correspondants sécurité, chefs de projet intégrant des contraintes de sécurité.

PRÉREQUIS

Aucune connaissance particulière.

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.

- La norme ISO 27001 dans une démarche système de management (roue de Deming/PDCA).
- Les bonnes pratiques universelles de la norme ISO 27002, la connaissance minimale indispensable.
- Les domaines de la sécurité : de la politique à la conformité en passant par la sécurité informatique.
- Elaborer un Plan d'Assurance Sécurité dans sa relation client/fournisseur.

4) Le processus d'analyse des risques

- Intégration de l'Analyse des risques au processus de gouvernance de la sécurité.
- Identification et classification des risques, risques accidentels et cyber risques.
- Les normes ISO 31000 et 27005 et la relation du processus risque au SMSI ISO 27001.
- De l'appréciation des risques au plan de traitement des risques : les bonnes activités du processus.
- Connaitre des méthodes pré définies : approche FR/EBIOS RM, approche US/NIST, etc.

5) Les audits de sécurité et la sensibilisation des utilisateurs

- Les catégories d'audits, de l'audit organisationnel au test d'intrusion.
- Les bonnes pratiques de la norme 19011 appliquées à la sécurité.
- Comment qualifier ses auditeurs ? – exemple avec les PASSI en France.
- Sensibilisation à la sécurité : Qui ? Quoi ? Comment ?
- De la nécessité d'une sensibilisation programmée et budgétisée.
- Les différents formats de sensibilisation, présentiel ou virtuelle ?
- La charte de sécurité, son existence légale, son contenu, les sanctions.
- Les quiz et serious game , exemple avec le MOOC de l'ANSSI.

6) Le coût de la sécurité et les plans de secours

- Les budgets sécurité, les statistiques disponibles.
- La définition du Return On Security Investment (ROSI).
- Les techniques d'évaluation des coûts, les différentes méthodes de calcul, le calcul du TCO.
- La couverture des risques et la stratégie de continuité.
- Plans de secours, de continuité, de reprise et de gestion de crise, PCA/PRA, PSI, RTO/RPO.
- Développer un plan de continuité, l'insérer dans une démarche sécurité.

7) Concevoir des solutions techniques optimales

- Structurer sa protection logique et physique. Savoir élaborer une défense en profondeur.
- Les trois grands axes de la sécurité informatique (réseaux, données, logiciels).
- Cloisonner ses réseaux sensibles, les technologies firewall réseaux et applicatif.
- Rendre ses données illisibles pendant le stockage et le transport, les techniques cryptographiques.
- Sécuriser ses logiciels par le durcissement et une conception secure.
- Gestion des vulnérabilités logicielles, savoir utiliser CVE/CVSS.

8) Supervision de la sécurité

- Indicateurs opérationnels de gouvernance et de sécurité.
- Le pilotage cyber : tableau de bord ISO compliant.
- Préparer sa défense (IDS, détection incidents, etc.).
- Traitement des alertes et cyber forensics, le rôle des CERT.

9) Les atteintes juridiques au Système de Traitement Automatique des Données

- Rappel, définition du Système de Traitement Automatique des Données (STAD).
- Types d'atteintes, contexte européen, la loi LCEN. Le règlement RGPD.
- Quels risques juridiques pour l'entreprise, ses dirigeants, le RSSI ?

10) Recommandations pour une sécurisation "légale" du SI

- La protection des données à caractère personnel, sanctions prévues en cas de non-respect.
- De l’usage de la biométrie en France.
- La cybersurveillance des salariés : limites et contraintes légales.
- Le droit des salariés et les sanctions encourues par l’employeur.

LES DATES

CLASSE À DISTANCE
2024 : 04 juin, 09 sept., 17 déc.