Cybersécurité réseaux/Internet, synthèse
protégez votre SI et vos communications d'entreprise

Séminaire de 3 jours - 21h
Réf : SRI - Prix 2024 : 2 890€ HT

Ce séminaire vous montre comment répondre aux impératifs de sécurité des entreprises et intégrer la sécurité dans l'architecture d'un Système d'Information. Il comprend une analyse détaillée des menaces et moyens d'intrusion ainsi qu'un panorama des principales mesures de sécurité disponibles sur le marché. Vous disposerez des éléments techniques et juridiques pour assurer et superviser la sécurité de votre SI.

OBJECTIFS PÉDAGOGIQUES

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

Connaître l'évolution de la cybercriminalité et de ses enjeux

Maîtriser la sécurité du Cloud, des applications, des postes clients

Comprendre les principes de la cryptographie

Gérer les processus de supervision de la sécurité SI

LE PROGRAMME

dernière mise à jour : 01/2020

1) Sécurité de l'information et cybercriminalité

- Principes de sécurité : défense en profondeur, modélisation du risque Cyber.
- Les méthodes de gestion de risques (ISO 27005, EBIOS RM).
- Panorama des normes ISO 2700x.
- Évolution de la cybercriminalité.
- Les nouvelles menaces (APT, spear phishing, watering hole, Crypto-jacking,...).
- Les failles de sécurité dans les logiciels.
- Le déroulement d'une cyberattaque (Kill Chain).
- Les failles 0day, 0day Exploit et kit d'exploitation.

2) Firewall, virtualisation et Cloud Computing

- La protection périmétrique basée sur les firewalls et les zones DMZ.
- Différences entre firewalls UTM, enterprise, NG et NG-v2.
- Produits IPS (Intrusion Prevention System) et IPS NG.
- Les vulnérabilités dans la virtualisation.
- Les risques associés au Cloud Computing selon le CESIN, l'ENISA et la CSA.
- Les solutions CASB pour sécuriser les données et applications dans le Cloud.
- Le Cloud Controls Matrix et son utilisation pour l'évaluation des fournisseurs de Cloud.

3) Sécurité des postes clients

- Comprendre les menaces orientées postes clients.
- Les logiciels anti-virus/anti-spyware.
- Comment gérer les correctifs de sécurité sur les postes clients ?
- Ransomware : mesures préventives et correctives.
- Comment sécuriser les périphériques amovibles ?
- Les vulnérabilités des navigateurs et des plug-ins.
- L'attaque Drive-by download.

PARTICIPANTS

RSSI, DSI, architectes, développeurs, chefs de projets, commerciaux avant-vente, administrateurs système & réseau.

PRÉREQUIS

Des connaissances générales sur l'informatique et le réseau Internet sont nécessaires.

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.

- Les menaces via les clés USB (BadUSB, rubber ducky,…).

4) Fondamentaux de la cryptographie

- Les techniques cryptographiques.
- Les algorithmes à clé publique et symétriques.
- Les fonctions de hachage simple, avec sel et avec clé (HMAC).
- Les architectures à clés publiques (PKI).
- Certification CC et qualification ANSSI des produits cryptographiques.

5) Authentification et habilitation des utilisateurs

- L'authentification biométrique et les aspects juridiques.
- L'authentification par challenge/response.
- Les différentes techniques d'attaque (brute force, keylogger, credential stuffing,…).
- L'authentification forte à facteurs multiples (MFA).
- Authentification carte à puce et certificat client X509.
- Les standards HOTP et TOTP de l'OATH.
- Les standards UAF et U2F de l'alliance FIDO (Fast ID Online).

6) La sécurité des flux réseaux

- Crypto API SSL et évolutions de SSL v2 à TLS v1.3.
- Les attaques sur les protocoles SSL/TLS.
- Les attaques sur les flux HTTPS.
- Le confinement hardware des clés, certifications FIPS-140-2.
- Évaluer facilement la sécurité d'un serveur HTTPS.
- Le standard IPsec, les modes AH et ESP, IKE et la gestion des clés.
- Surmonter les problèmes entre IPSec et NAT.
- Les VPN SSL. Quel intérêt par rapport à IPSec ?
- Utilisation de SSH et OpenSSH pour l'administration distante sécurisée.
- Déchiffrement des flux à la volée : aspects juridiques.

7) Sécurité Wi-Fi

- Attaques spécifiques Wi-Fi.
- Comment détecter les Rogue AP ?
- Mécanismes de sécurité des bornes.
- Description des risques.
- Le standard de sécurité IEEE 802.11i.
- Attaque KRACK sur WPA et WPA2.
- Les apports de WPA3 et les vulnérabilités DragonBlood.
- Authentification des utilisateurs et des terminaux.
- L'authentification Wi-Fi dans l'entreprise.
- Outils d'audit, logiciels libres, aircrack-ng, Netstumbler, WiFiScanner...

8) Sécurité des Smartphones

- Les menaces et attaques sur la mobilité.
- iOS et Android : forces et faiblesses.
- Virus et codes malveillants sur mobile.
- Les solutions de MDM et EMM pour la gestion de flotte.

9) Sécurité des applications

- Application du principe de défense en profondeur.
- Applications Web et mobiles : quelles différences en matière de sécurité ?
- Les principaux risques selon l'OWASP.
- Focus sur les attaques XSS, CSRF, SQL injection et session hijacking.
- Les principales méthodes de développement sécurisé.
- Quelle clause de sécurité dans les contrats de développement ?
- Le pare-feu applicatif ou WAF.

- Evaluer le niveau de sécurité d'une application.

10) Gestion et supervision active de la sécurité

- Les audits de sécurité (scope et référentiels : ISO 27001, RGPD, ….).
- Les tests d’intrusion (black box, gray box et white box).
- Les plateformes de "bug Bounty".
- Comment répondre efficacement aux attaques ?
- Mettre en place une solution de SIEM.
- Mettre en œuvre ou externaliser son Security Operation Center (SOC) ?
- Les technologies du SOC 2.0 (CASB, UEBA, Deceptive Security, EDR, SOAR, machine learning, ...).
- Les labels ANSSI (PASSI, PDIS & PRIS) pour l’externalisation.
- Les procédures de réponse à incident (ISO 27035 et NIST SP 800-61 R2).

LES DATES

CLASSE À DISTANCE
2024 : 18 juin, 09 oct., 04 nov.

PARIS
2024 : 12 juin, 23 sept., 10 déc.