Sécurité VPN, sans-fil et mobilité, synthèse
identifier les menaces et appliquer les solutions les plus efficaces

Séminaire de 2 jours - 14h
Réf : VPN - Prix 2024 : 2 090CHF HT

Aujourd'hui, les technologies de communication sans fil et les terminaux mobiles facilitent grandement l'accès aux applications de l'entreprise. Afin de préserver la sécurité de ces accès, ce séminaire dresse un panorama complet des menaces et des vulnérabilités, et apporte des solutions concrètes pour s'en prémunir.

OBJECTIFS PÉDAGOGIQUES

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

Evaluer les risques de sécurité dans un contexte de mobilité

Connaître les types d'attaque

Comprendre la solution VPN

Sécuriser les réseaux sans-fil et les Smartphones

EXEMPLE

Approche théorique et pratique avec démonstration, avantages et inconvénients des solutions, retours d'expérience.

LE PROGRAMME

dernière mise à jour : 01/2018

1) Menaces et vulnérabilités

- Evolution de la cybercriminalité en France.
- Statistiques et évolution des attaques.
- Evaluation des risques dans un contexte de mobilité.

2) Les attaques sur l'utilisateur

- Les techniques d'attaques orientées utilisateur.
- Les techniques de Social engineering.
- Codes malveillants et réseaux sociaux.
- Les dangers spécifiques du Web 2.0.
- Attaque sur les mots de passe.
- Attaque "Man in the Middle".

3) Les attaques sur les postes clients

- Risques spécifiques des postes clients (ver, virus...).
- Le navigateur le plus sûr.
- Rootkit navigateur et poste utilisateur.
- Quelle est l'efficacité réelle des logiciels antivirus ?
- Les risques associés aux périphériques amovibles.
- Le rôle du firewall personnel.
- Sécurité des clés USB.
- Les postes clients et la virtualisation.

4) Sécurité des réseaux privés virtuels (VPN)

- Les techniques de tunneling. Accès distants via Internet : panorama de l'offre.
- Les protocoles PPT, LTP, L2F pour les VPN.

PARTICIPANTS

DSI, RSSI, responsables sécurité, chefs de projets, consultants, administrateurs.

PRÉREQUIS

Connaissances de base de l'informatique.

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.

- Le standard IPsec et les protocoles AH, ESP, IKE.
- Les solutions de VPN pour les accès 3G.
- Quelles solutions pour Blackberry, iPhone... ?
- VPN SSL : la technologie et ses limites.
- Le panorama de l'offre VPN SSL. Critères de choix.
- IPsec ou VPN SSL : quel choix pour le poste nomade ?

5) Sécurité des réseaux sans-fil

- La sécurité des Access Point (SSID, filtrage MAC...).
- Pourquoi le WEP est dangereux ? Qu'apportent WPA, WPA2 et la norme 802.11i ?
- L'authentification dans les réseaux Wi-Fi d'entreprise.
- Technologies VPN (IPsec) pour les réseaux Wi-Fi.
- Comment est assurée la sécurité d'un hotspot Wi-Fi ?
- Les techniques d'attaques sur WPA et WPA2.
- Les fausses bornes (Rogue AP).
- Attaques spécifiques sur Bluetooth.

6) Sécurité des Smartphones

- La sécurité sur les mobiles (Edge, 3G, 3G+...).
- Les risques spécifiques des Smartphones.
- Failles de sécurité : le palmarès par plateforme.
- Virus et code malveillants : quel est le risque réel ?
- Protéger ses données en cas de perte ou de vol.

Démonstration : Mise en oeuvre d'un accès Wi-Fi fortement sécurisé avec IPsec et EAP-TLS. Attaque de type "Man in the Middle" sur une application Web en HTTPS via un Smartphone (sslsnif et sslstrip).

LES DATES

CLASSE À DISTANCE
2024 : 17 oct.