Formation Sécurité VPN, sans-fil et mobilité, synthèse

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

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.

Référence	VPN
Durée	2 jours (14h)
Tarif	1 990 €HT
Repas	repas inclus

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 17 au 18 octobre 2024

VOIR TOUTES LES DATES

Objectifs

| Evaluer les risques de sécurité dans un contexte de mobilité
| Connaître les types d'attaque
| Identifier la solution VPN
| Sécuriser les réseaux sans-fil et les Smartphones

Public

| DSI
| RSSI
| responsables sécurité
| chefs de projets
| consultants
| administrateurs

Prérequis

| Connaissances de base de l'informatique.

Programme de la formation

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

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".

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.

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.
| 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 ?

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.

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).

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

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne

fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.