Sécurité VPN, sans-fil

Durée : 2 jours Référence : SVPNSF

Cette formation établit la liste des menaces et des vulnérabilités concernant les moyens d'accès aux données et applications de l'entreprise via l'Internet, Wifi, Bluetooth et terminaux mobiles (notebook et Smartphone) et apporte des solutions concrètes pour s'en prémunir.

Contenu

- Menaces et vulnérabilités
- Les attaques sur l'utilisateur
- Les attaques sur les postes clients
- Sécurité des réseaux privés virtuels (VPN)
- Sécurité des réseaux sans-fil
- Sécurité des Smartphones

Participants

Responsables sécurité, Consultants, Techniciens, Administrateurs et Ingénieurs réseaux/système.

Pré-requis

Connaissances de base sur les systèmes et réseaux.

Programme

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

- Attaques ciblées 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.
- Les principales lacunes sécuritaires des OS clients.
- Amélioration de la sécurité dans Windows.

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 ?
  - Le VPN avec DirectAccess sous Windows 7.

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.
- Les principales attaques : Bluebug, BlueSmack, BlueStack...

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). Accès au SI en VPN SSL avec authentification forte. Protection des données par le chiffrement (EFS, Bitlocker et Bitlocker to go).