Formation Mettre en oeuvre la sécurité réseaux

La protection des données de l'entreprise passe par une politique de sécurité capable de résister à toutes menaces extérieures. Loin d'être un domaine spécifique, la sécurité doit être prise en compte aussi bien pour les équipements réseaux que pour les systèmes. Même s'il n'est pas un expert, l'administrateur ne doit pas ignorer les risques encourus et doit être capable de mettre en oeuvre une architecture de sécurité répondant aux exigences de l'entreprise

Objectifs

- Savoir concevoir et réaliser une architecture de sécurité adaptée
- Mettre en oeuvre les principaux moyens de sécurisation des réseaux
- Disposer d'une première approche sur la sécurisation des serveurs
- Découvrir les obligations légales inhérentes à la sécurité

Public concerné

- Toute personne en charge de la sécurité d'un système d'information ou intervenant sur le réseau ou la mise en place de serveurs d'entreprises

Prérequis

- Utilisation courante de Windows et des équipements constitutifs d'un réseau, connaissances couvertes par les stages Pratique des réseaux (SR200) et Soyez autonome avec TCP/IP (SR230)

Une formation de 5 jours

Caractéristiques
Tarif : 2650 euros HT par personne
Numéro de formateur : 11754730575
Nombre d'heures : 35
Référence : SR211
Contact : Jean JUILLET
Telephone : 01.42.62.91.86
Email : contact@kaptive.com

Paris
10/02/2014
14/04/2014
23/06/2014
01/09/2014
20/10/2014
24/11/2014

Lyon
24/02/2014
19/05/2014
13/10/2014
15/12/2014

Description des modules

L'environnement

- Le périmètre (réseaux, systèmes d'exploitation, applications)
- Les acteurs (hacker, responsable sécurité, auditeur, vendeur et éditeur, sites de sécurité)
- Les risques
- La protection
- La prévention
- La détection

Les attaques

- Les intrusions de niveau 2 : au niveau du commutateur d'accès ou du point d'accès sans-fil
- Les intrusions de niveau 3 (IP) : IP spoofing, déni de service, scanSniffer, man-in-the-middle, les applications stratégiques (DHCP, DNS, SMTP), les applications à risques (HTTP)
- Les attaques logiques : virus, ver, cheval de troie, spyware, phishing, le craquage de mot de passe
- Les attaques applicatives : sur le système d'exploitation ou sur les applications (buffer overflow)

Les protections

- Au niveau des commutateurs d'accès : port sécurisé sur mac-adresse, utilisation du protocole 802.1x, VLAN Hopping, DHCP Snooping, IP source guard, ARP spoofing, filtre BPDU, root guard
- Au niveau sans-fil : mise en place d'une clé WEP, de WPA, de WPA 2 (802.1i)
- Au niveau IP : les pare-feux applicatifs, spécialisés, sur routeur, state full (inspection des couches au dessus de 3), les UTM, les proxys
- Protection des attaques logiques : les anti-virus, les anti spyware, le concept NAC
- Protection des attaques applicatives : hardening des plates-formes Microsoft et Unix, validations des applicatifs

La sécurisation des accès distants

- établissement d'un VPN
- Choix cryptographique
- VPN IPsec : serveur ou boîtier spécialisé ou UTM ?
- Client logiciel ou matériel ?
- VPN SSL : serveur - Appliance spécialisée ou UTM ?
- Principe du NAC

Monitoring et prévention

- Sondes IDS
- SysLog Serveur
- Exploitations des logs
- IPS : boîtiers dédiés, fonctionnalité du routeur

Exemples d'architectures

- Exemple d'une entreprise mono-site
- Connexion des nomades
- Exemple d'entreprise multi-site