

# 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

## Pré requis

- 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	Paris	Lyon
Tarif : 2650 € HT par personne	21/03/2011	16/05/2011
Numéro de formateur : 11753687675	20/06/2011	05/09/2011
Nombre d'heures : 35	22/08/2011	
Référence : SR211	17/10/2011	
Contact : Patrick LE GOFF	12/12/2011	
Telephone : 01.76.60.66.10		
Email : <a href="mailto:contact@kaptive.com">contact@kaptive.com</a>		

## Description des modules

num	Module
<b>1</b>	<b>L'environnement</b>
<b>Détails</b>	<ul style="list-style-type: none"> <li>- Le périmètre (réseaux, systèmes d'exploitation, applications)</li> <li>- Les acteurs (hacker, responsable sécurité, auditeur, vendeur et éditeur, sites de sécurité)</li> <li>- Les risques</li> <li>- La protection</li> <li>- La prévention</li> <li>- La détection</li> </ul>
<b>2</b>	<b>Les attaques</b>
<b>Détails</b>	<ul style="list-style-type: none"> <li>- Les intrusions de niveau 2 : au niveau du commutateur d'accès ou du point d'accès sans-fil</li> <li>- 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)</li> <li>- Les attaques logiques : virus, ver, cheval de troie, spyware, phishing, le craquage de mot de passe</li> <li>- Les attaques applicatives : sur le système d'exploitation ou sur les applications (buffer overflow)</li> </ul>
<b>3</b>	<b>Les protections</b>
<b>Détails</b>	<ul style="list-style-type: none"> <li>- 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</li> <li>- Au niveau sans-fil : mise en place d'une clé WEP, de WPA, de WPA 2 (802.1i)</li> <li>- Au niveau IP : les pare-feux applicatifs, spécialisés, sur routeur, state full (inspection des couches au dessus de 3), les UTM, les proxys</li> <li>- Protection des attaques logiques : les anti-virus, les anti spyware, le concept NAC</li> <li>- Protection des attaques applicatives : hardening des plates-formes Microsoft et Unix, validations des applicatifs</li> </ul>
<b>4</b>	<b>La sécurisation des accès distants</b>
<b>Détails</b>	<ul style="list-style-type: none"> <li>- Établissement d'un VPN</li> <li>- Choix cryptographique</li> <li>- VPN IPsec : serveur ou boîtier spécialisé ou UTM ?</li> <li>- Client logiciel ou matériel ?</li> <li>- VPN SSL : serveur - Appliance spécialisée ou UTM ?</li> <li>- Principe du NAC</li> </ul>
<b>5</b>	<b>Monitoring et prévention</b>
<b>Détails</b>	<ul style="list-style-type: none"> <li>- Sondes IDS</li> <li>- SysLog Serveur</li> <li>- Exploitations des logs</li> <li>- IPS : boîtiers dédiés, fonctionnalité du routeur</li> </ul>
<b>6</b>	<b>Exemples d'architectures</b>
<b>Détails</b>	<ul style="list-style-type: none"> <li>- Exemple d'une entreprise mono-site</li> <li>- Connexion des nomades</li> <li>- Exemple d'entreprise multi-site</li> </ul>
<b>7</b>	<b>Cadre législatif</b>
<b>Détails</b>	<ul style="list-style-type: none"> <li>- Rappel sur le cadre légal</li> <li>- Rappel sur l'application de la LSF</li> </ul>