

## SECURITE RESEAUX/INTERNET

**Durée: 5 Jours / 35h**

### Pré requis :

- Aucun

### Objectifs de la formation :

- Acquérir une nouvelle méthode de relance de factures au téléphone tout en préservant la relation commerciale.
- Mettre en place une organisation efficace du recouvrement par téléphone.

### Modalité de formation :

- Formation sur le site de l'entreprise ou en centre de formation, individuelle ou en groupe.

### Moyens pédagogiques :

- Les exercices pratiques sont basés sur des cas concrets. Ils peuvent également être fournis par le(s) participant(s).
- Supports de cours et/ou fiches pratiques

### Evaluation formation :

- Grille d'évaluation soumise au(x) stagiaire(s) en fin de parcours.

### Evaluation des acquis :

- Contrôle continu avec évaluation régulière des acquis

### Dispositif de suivi :

- Assistance téléphonique
- E-mail

### PROGRAMME

#### • Introduction : qui fait quoi et comment ?

Concepts et principes de sécurité : risque, menaces, vulnérabilité, politique de sécurité...

Evolution de la cybercriminalité en France et dans le monde.

Typologie des risques, le top 20 des attaques sur Internet.

Les failles de sécurité dans les logiciels (évolution et cycle de vie).

Nouvelles techniques d'attaque et contre-mesures associées.

#### • Outils et méthodes d'intrusion par TCP-IP

Les attaques par le stack IP

(IP Spoofing, TCP-flooding, SMURF, etc.).

Les attaques applicatives (DNS, HTTP, SMTP, etc.).

Utilisation d'un code mobile malveillant (conception, diffusion, propagation).

Comprendre les techniques des hackers

(sniffing, tapping, smurfing, hi-jacking, flooding, cracking...).

Les sites majeurs de la sécurité (CERT, Security focus/bugtraq, CVE...).

#### • Sécurité des postes clients

Comprendre les menaces orientées postes clients (backdoor, virus, worm, spyware, rootkit, keylogger...).

Le rôle du firewall personnel et ses limites.

Les logiciels anti-virus/anti-spyware

(comparatif et déploiement).

Comment gérer les correctifs de sécurité sur les postes clients ?

Linux et Open Office bien mieux sécurisés que Microsoft Windows et MS Office ?

Quels sont les apports réels de Vista en matière de sécurité ?

Comment sécuriser les périphériques amovibles (disques externes, clés USB, DVD, etc.).

Le contrôle de conformité du client Cisco NAC, Microsoft NAP.

Toute reproduction sans autorisation, même partielle, est interdite.

## SECURITE RESEAUX/INTERNET (suite)

Toute reproduction sans autorisation, même partielle, est interdite.

### • Sécurité Wifi

Technologies de réseaux sans fil (Standards IEEE 802.11).

Attaques spécifiques (Wardriving, failles WEP, failles EAP).

Mécanismes de sécurité des bornes

Vulnérabilités WEP. Faiblesse de l'algorithme RC4.

Description des risques (interception du trafic, man in the middle, DoS, ...).

Le standard de sécurité IEEE 802.11i (WPA et WPA2).

Architecture des WLAN (segmentation des réseaux, flux).

Authentification des utilisateurs (EAP, passphrase, certificats, token...).

Les différentes méthodes Cisco LEAP, EAP-TLS...

Audit et surveillance du réseau.

Recherche des réseaux « sauvages ».

Outils d'audit, logiciels libres, Netstumbler, WifiScanner...

### • Technologie firewall/proxy

Les serveurs proxy, reverse proxy, le masquage d'adresse.

Le filtrage : comment identifier pour filtrer une application.

Firewall et proxy : quelle complémentarité ?

Les firewalls dédiés/non dédiés.

Principe des firewalls, périmètre fonctionnel.

La mise en place de solutions DMZ (zones démilitarisées).

Sécurité liée à l'adressage : adressage privé (RFC 1918), fonctions NAT et PAT.

Les firewalls de type "Appliance", l'approche SOHO.

Comment sélectionner le firewall le mieux adapté à vos contraintes.

Produits et principaux acteurs du marché.

Les solutions à haute disponibilité (Stonesoft, Radware, Alteon...).

### • Techniques cryptographiques

Historique, terminologie, principaux algorithmes connus, cryptanalyse.

Législation et principales contraintes d'utilisation en France et dans le monde.

Algorithmes à clé publique : Diffie Hellman,

RSA, schémas à apport nul de connaissance.

Scellement et signature électronique : MD5, MAC, MAA, SH.

Mots de passe, token, carte à puce, certificats et biométrie

Authentification forte : logiciels (S/key), cartes à puces, calechettes d'authentification.

Préserver la confidentialité des mots de passe.

## SECURITE RESEAUX/INTERNET (suite et fin)

Toute reproduction sans autorisation, même partielle, est interdite.

### • Architectures de sécurité pour l'Intranet/Extranet

Les architectures à clés publiques (Public Key Infrastructure)  
Le standard SSL, la version 2, la version 3, TLS,  
40 ou 128 bits.

Un serveur de certificat interne ou public ?

En France ou aux USA ? À quel prix ?

Comment obtenir des certificats serveurs et clients.

Comment faire gérer ces certificats : de la création  
à la révocation.

Annuaire LDAP et sécurité.

Architectures "3A" (authentification, autorisation, audit) :  
concept de SSO, Kerberos,

Normes OSF/DCE et ECMA Tacacs.

### • Sécurité des applications

Comment bien architecturer son application

(front-office/back-office) ?

Comment réaliser un filtrage d'URL efficace ?

Liste blanche et/ou liste noire.

La sécurité intrusive/non intrusive.

Le pare-feu applicatif ou reverse proxy filtrant.

L'authentification renforcée et la gestion SSO.

Le hardening et les vérifications d'intégrité en temps réel.

L'authentification des services distants :

comment la renforcer ?

Comment améliorer les performances et assurer  
une haute disponibilité ?

### • Gestion et supervision active de la sécurité

L'apport des normes ISO 27001 et ISO 27002 dans  
le management de la sécurité.

Les tableaux de bord Sécurité. La norme ISO 27004.

Les missions du RSSI dans le suivi de la sécurité.

Les audits de sécurité (technique ou organisationnel).

Le contrôle de sécurité périmétrique par scanner.

Les tests de vulnérabilité ou tests d'intrusion,

les contraintes des lois (LCEN, LSQ, etc.).

Les outils spécialisés Sondes IDS, Scanner VDS,

Firewall IPS.

Comment répondre efficacement aux attaques ?

Comment consigner les éléments de preuve et mettre

en oeuvre un plan de riposte efficace ?

Mettre en place une solution de SIM (Security Information M

La veille technologique : comment se tenir toujours informé  
des nouvelles vulnérabilités ?