Formation état de l'art de la sécurité des Systèmes d'Information

Pour faire face à la montée en puissance des menaces qui pèsent sur nos systèmes d'information, le monde de la sécurité doit s'adapter, et est de fait en perpétuelle évolution aussi bien sur le plan des technologies que des méthodes et modèles conceptuels sous-jacents. Ce séminaire de 3 jours dresse un état de l'art complet des outils organisationnels et techniques de maîtrise du risque informatique

Objectifs

- Identifier les différents domaines de la sécurité et de la maîtrise des risques liés aux informations
- Connaître les principes et les normes de chaque domaine de la SSI
- Disposer d'informations sur les tendances actuelles, que ce soit dans les menaces ou dans les solutions à notre disposition
- Connaître les principaux outils et acteurs du marché (y compris logiciels libres), avec pour chaque, une présentation des forces et des faiblesses des solutions existantes

Public concerné

- Directeurs du système d'information ou responsables du service informatique souhaitant analyser les risques liés au SI
- Responsables et chefs de projet en charge de la mise en place d'une politique de sécurité
- Chefs de projet sécurité et toute personne so

Prérequis

- Ce séminaire ne nécessite pas de pré-requis

Une formation de 3 jours

Caractéristiques
Tarif : 2160 euros HT par personne
Numéro de formateur : 11754730575
Nombre d'heures : 21
Référence : SEM54
Contact : Jean JUILLET
Telephone : 01.42.62.91.86
Email : contact@kaptive.com

Paris
10/02/2014
14/04/2014
30/06/2014
15/09/2014
01/12/2014

Lyon
17/02/2014
10/06/2014
27/10/2014

Description des modules

1ère partie : Introduction

Tendances des menaces et risques

- Statistiques sur la sécurité
- Tendances dans l'évolution des menaces
- Profil des attaquants
- Architecture générale SSI
- Solutions du marché

2ème partie : Sécurité des réseaux et des systèmes

Sécurité périmétrique

- Fonctionnalités proposées
- Logiciels, appliances et UTM
- Mise en cluster, scalabilité

Solutions antivirales

- Tendances du risque viral
- Protection des postes et serveurs
- Sécurité des flux et protection des passerelles

Solutions anti-spam

- évolution du spamming (chiffres et technologies)
- Solutions de lutte anti-spam

Détection et prévention d'intrusion

- Principes et concepts
- Différence entre IDS et IPS, avantages comparés

Network Access Control

- Concept de NAC
- Limites des technologies

Sécurité des contenus

- Principes et concepts
- Sécurité des flux applicatifs (messagerie, messagerie instantanée, VoIP...)

Qualité de service et supervision

- Principes et concepts
- Security Information Management

Haute disponibilité

- Haute disponibilité des réseaux et des liens
- équilibrage, routage dynamique
- Haute disponibilité des systèmes, clusters, virtualisation
- Haute disponibilité des données, SAN et sauvegardes

3ème partie : Nomadisme

Sécurité des postes nomades

- Problèmes de sécurité liés au nomadisme
- Protection d'un poste vs. solutions spécifiques
- Mise en quarantaine

Accès distants, VPN SSL

- Concept et standards de VPN sécurisé
- Intérêts du VPN SSL
- Contrôle du point d'accès

4ème partie : Gestion des identités et des accès

Gestion des identités

- Gestion du cycle de vie des utilisateurs
- Problématique organisationnelle
- Problématique technique
- Gestion des identités vs. SSO

Authentification forte

- Systèmes cryptographiques
- Tokens
- Systèmes biométriques

Authentification LDAP et SSO

- Urbanisation de l'authentification
- Architectures à base d'annuaire LDAP
- SSO

Fédération d'identités

- Enjeux de la fédération d'identités
- Concepts et normes

Infrastructures de clés publiques

- Cryptographie à clé publique, certificats de clés
- Autorités de certification et d'enregistrement
- Révocation et gestion des urgences

5ème partie : Produits et services du marché sécurité applicative

Applications web et web services

- Architecture des applications web
- Normes et standards de sécurité des web services

Développement sécurisé

- Principes de développement sécurisé
- Tests et analyse de code
- Méthodes et outils

6ème partie : Risk Management, normes

Méthodes d'audit et d'analyse des risques

- Normes et méthodes d'audit
- état des méthodes d'analyse des risques informatique

Normes de sécurité

- ISO27000 : système de management de la sécurité de l'information
- BS25999 : continuité des activités
- Autres normes internationales de sécurité des SI

Outils d'audit et de test de sécurité

- Typologie des audits et outils d'audit
- Typologie des tests de sécurité