Sécurité du Cloud Computing

Durée : 2 jours Référence : SECC

Cette Formation présente les problèmes de sécurité au sein du Cloud. Elle expose les connaissances essentielles permettant de se présenter au passage de la certification CCSK de la Cloud Security Alliance.

Contenu

- Introduction
- Sécurité des environnements virtuels
- Sécurité des accès réseaux au Cloud
- Travaux de la Cloud Security Alliance (CSA)
- Sécurité du Cloud Computing selon l'ENISA
- Recommandations du NIST pour la sécurité
- Contrôle de la sécurité du Cloud
- Aspects juridiques

Participants

Responsables sécurité, chefs de projets, consultants, administrateurs, techniciens.

Pré-requis

Connaissances de base sur la virtualisation.

Programme

Introduction

- Définition du Cloud Computing.
- Les principaux fournisseurs et les principales défaillances déjà constatées. SecaaS (Security as a Service) : les services de sécurité dans le Cloud.
- Les points clés d'une architecture sécurisée dans le Cloud : authentification, gestion des habilitations, cloisonnement des services, contrôle d'intégrité des configurations,

confidentialité, clés de chiffrement, sauvegarde, haute disponibilité, PRA/PCA, traçabilité, non-répudiation et imputabilité des actions utilisateurs.

Sécurité des environnements virtuels

- Les apports de la virtualisation pour la sécurité
- Menaces et vulnérabilités spécifiques.
- Trois modèles d'intégration de la sécurité : Virtual DataCenter, Appliance matérielle et Appliance virtuelle.
- Les solutions de sécurité dédiées à la virtualisation.

Sécurité des accès réseaux au Cloud

- Vulnérabilités et les enjeux de la sécurité d'accès au Cloud.
- La sécurité native dans IP v4, IPsec et IP v6.
- Les protocoles : PPTP, L2TP, IPsec et VPN SSL.
- L'accès au Cloud via le Web sécurisé (https).
- Les vulnérabilités des clients du Cloud (PC, tablettes, smartphones) et des navigateurs.

Travaux de la Cloud Security Alliance (CSA)

- Le référentiel Security Guidance for Critical Areas of Focus in Cloud Computing. Les treize domaines de sécurité. Les sept principales menaces.
- La suite intégrée GRC (CloudAudit, Cloud Controls Matrix, Consensus Assessments Initiative Questionnaire, Cloud Trust Protocol).
- La certification CCSK (Certificate of Cloud Security Knowledge).

Sécurité du Cloud Computing selon l'ENISA

- Evaluation et gestion des risques du Cloud par la norme l'ISO 27005. Les trente-cinq risques identifiés par l'ENISA.
- Les recommandations ENISA pour la sécurité des Clouds gouvernementaux.

Recommandations du NIST pour la sécurité

- Les lignes directrices pour la sécurité et la confidentialité dans le Cloud Computing public.
- Analyse des standards NIST 800-144 et NIST 800-146.

Contrôle de la sécurité du Cloud

- Quel label de sécurité pour les fournisseurs : Cobit, ISO2700x, Critères communs ISO 15401 ?
- Comment auditer la sécurité dans le Cloud ?
- Les outils de contrôle de sécurité orientés Cloud (Metasploit & VASTO, openVAS, xStorm, etc.).

Aspects juridiques

- Du Cloud privé au Cloud public : conséquences juridiques. Responsabilités des différents acteurs.
- La conformité réglementaire (PCI-DSS, CNIL, SOX, ...).
- Les précautions pour la rédaction d'un contrat.