

CLOUD : GOUVERNANCE ET SÉCURITÉ

CODE STAGE : ACF101

OBJECTIFS

Comprendre les éléments fondamentaux de la sécurité du Cloud
Identifier et analyser les risques liés au Cloud
Comprendre les contrats Cloud
Mettre en oeuvre les bonnes pratiques de sécurité dans le Cloud
Connaître les techniques de sécurisation réseau du Cloud.

DURÉE

3 jours

PUBLIC

Architectes, chefs de projets, ingénieurs informatique (réseau, système, développement...).

PRÉ-REQUIS

Avoir des connaissances minimales sur le Cloud (caractéristiques, modèles de services, modèles de déploiement) et des bases en sécurité informatique et réseaux. Avoir également des notions de management de projet.

PROGRAMME

Introduction

En quoi la sécurité du Cloud est-elle différente de celle dans l'entreprise ?

Retour sur les aspects fondamentaux de la sécurité : confidentialité, intégrité, disponibilité, traçabilité

Principes généraux de sécurité : SMSI, PSSI

La sécurité des infrastructures virtuelles aujourd'hui

La gestion de la sécurité des environnements virtuels « traditionnels »

L'impact de l'hyperviseur et de la virtualisation du réseau

Les risques actuels et les techniques de sécurisation associées

Introduction à la sécurité du Cloud

Les organismes aux différentes échelles : CNIL, ANSSI, ENISA, Cloud Security Alliance, ISO

Les grandes réglementations : HDS, Directives européennes, Privacy Shield

Les certifications : ISO 27001, 27002, 27005, 27018

Exercice

Présentation d'une architecture virtuelle de la société X : comment la sécuriser avec les techniques traditionnelles ?

Les risques identifiés

Introduction

Identification et classification des données externalisables

Données, métadonnées, données d'authentification et sauvegardes

Données de production, financières et des parties prenantes (clients, fournisseurs, personnels)

Processus de gestion des risques ISO 27005

Approches qualitatives et quantitatives

Les risques critiques avec un très fort impact métier

Perte de gouvernance

Les défis de la conformité

Les risques de changement des règles juridiques

Les risques critiques avec une forte vraisemblance

Echec d'isolation

Compromission interne du Cloud provider

Suppression de données non sécurisées

Gestion du réseau

Traitement et réduction des risques

Actions liées aux risques et opportunités ISO27001

Traitement et réduction des risques

Risques résiduels

PDCA

Et audit

Actions de réduction organisationnelle des risques

Actions de réduction techniques des risques

Aspects juridiques : le contrat Cloud



Introduction

Les différences entre les contrats d'infogérance et les contrats Cloud

Gérer et garantir la localisation, le transfert et la sécurité des données, la confidentialité

La dilution des responsabilités

Les contrats : généralités

Les clauses clés du contrat

SLA

Support

Sécurité

Facturation

Les clauses d'auditabilité

Les Cloud auditor et les APM

La réversibilité ou comment changer de provider ?

L'interopérabilité du Cloud

Les SLA

Les SLA techniques

Les SLA opérationnels

Exemples de SLA de contrats Cloud

La tarification et les licences

Vers un nouveau modèle de coûts

Capex / Opex

L'impact sur les licences logicielles de l'entreprise

L'exemple du SPLA de Microsoft

Comment gérer les licences en environnement hybride ?

Analyse des coûts cachés

Les outils des providers (Amazon, Azure) et les outils spécifiques (RightScale)

Etudes de cas

Le contrat de Microsoft Office 365

Le contrat SaaS et son audit pour une société de services financiers

Les bonnes pratiques de sécurité dans le Cloud



Sécurisation de l'infrastructure du Cloud
La sécurité physique et environnementale
Contrôle d'accès et gestion des identités
La sécurité des données : chiffrement
La gestion des mots de passe : cryptologie

Opération et exploitation des SI
Gestion des changements
Séparation des environnements
Sauvegarde des environnements
Journalisation des évènements
Sécurisation
Gestion
Exploitation

Continuité d'activité
Les normes de Data Center : uptime institut et tier I à IV
PRA / PCA et/dans le Cloud
Redondance des ressources et des équipements

Acquisition, développement et maintenance des SI
Politique de développement
Développement externalisé

Tiers et ressources humaines
Procédures d'entrée et de sortie
La rupture contractuelle

Etude de cas
L'évolution d'un infogéreur traditionnel sans politique de sécurité vers un Data Center HDS

La sécurité du réseau dans le Cloud

Sécurité des accès
L'impact de la multiplication des applications SaaS
La fédération des identités : SAML



Le cas d'ADFS et de Azure AD

L'évolution vers le Identity as a Service

Sécurité des flux

L'impact de la virtualisation du réseau

La micro-segmentation

Distributed firewall

Le cas de Vmware NSX

La sécurité entre les Clouds

Les offres de VPN des providers

Les possibilités d'interconnecter vos équipements à ceux du Cloud provider

L'interconnexion des applications SaaS avec des données situées dans l'entreprise

Etudes de cas

La fédération d'identités avec Office 365

La sécurisation des accès à AWS

