Contactez-nous Tél. : +33 (0)1 83 35 34 40
Email inscription@lepont-learning.com
Site web www.lepont-learning.com

TENDANCES

Sécurité du cloud computing

REF : SICO004

DUREE : 14h

Présentiel Classe virtuelle

PUBLIC

Directeurs du système d'information ou responsables du service informatique souhaitant analyser les risques liés à l'utilisation d'une solution Cloud Responsables et chefs de projet en charge de la mise en place d'une politique de sécurité lié à un projet Cloud Chefs de projet et toute personne en charge de la sécurité du Cloud Computing

Modalités et délais d'accès : les inscriptions sont fernées 24h avant la 1ére journée de formation.

Accessibilité : Si vous avez des contraintes particulières liées à une situation de handicap, veuillez nous contacter au préalable afin que nous puissions, dans la mesure du possible, adapter l'action de formation.

PREREQUIS

Ce séminaire nécessite une connaissance sommaire de l'informatique

MODALITES PEDAGOGIQUES

1 poste et 1 support par stagiaire

8 à 10 stagiaires par salle

Remise d'une documentation pédagogique papier ou numérique pendant le stage

La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience

MODALITES D'EVALUATION

Auto-évaluation des acquis par le stagiaire via un questionnaire en ligne Attestation de fin de stage remise au stagiaire

OBJECTIFS PEDAGOGIQUES

Cette formation Sécurité du Cloud Computing vous permettra de :

- Comprendre comment s'appuyer sur des référentiels de normes et de standards pour sécuriser le Cloud
- Connaître les moyens génériques de la sécurité du Cloud
- Être en mesure de s'inspirer des solutions et des démarches des opérateurs de Cloud pour sécuriser son approche
- Comprendre comment éviter la mise en place d'une sécurité coûteuse et laborieuse pouvant dégrader la performance du réseau global

PROGRAMME

Introduction

- Rappel des éléments matériels et logiciels de l'architecture Cloud selon les organismes de standardisation NIST (National Institute of Standards and Technology)
- Complexité du contexte de l'utilisation en tout lieu avec tout type de terminaux de connexion

Déceler les points de vulnérabilité du Cloud

- Solutions et architectures du Cloud proposées par des grands acteurs du secteur (OS Cloud, virtualisation, stockage, Datacenter, réseaux...)
- Points de vulnérabilité du terminal d'accès au Datacenter du Cloud
- Problèmes de sécurité spécifique aux Clouds ouverts et interconnectés
- Quatre niveaux de sécurité (technologique, organisationnel, contractuel et de conception d'architectures techniques)

S'inspirer des recommandations d'organismes officiels CSA (Cloud Security Alliance) et ENISA (European Network and Information Security Agency) pour sécuriser le Cloud et gérer les risques

- Protection d'accès à distance au Cloud et Datacenter (firewall multifonctions)
- Sécurité des transactions en ligne par la cryptologie (PKI)
- Authentification des accès : NAC, RBAC, portail captif, authentification forte
- IAM (Identity and Access Management)
- Surveillance des activités anormales (IDS/IPS, NIDS/NIPS)
- SIEM (Security Information and Event Management)
- Lutte contre le vol de données (DLP : Data Lost Prevention)
- 35 types de risques selon ENISA
- Traitement des 5 risques majeurs et fréquents en s'appuyant sur les recommandations d''ENISA

S'appuyer sur les solutions techniques de sécurité du Cloud, proposées par les constructeurs et opérateurs Cloud

- Synthèse des approches, matériels et logiciels de sécurité adoptés par des fournisseurs de Cloud
- Solutions de sécurité offertes par les opérateurs de Cloud

public
- Internalisation des dispositifs privés dans le Datacenter du Cloud
- Cloud intermédiaire de sécurité (SecaaS : Security as a Service)
- Avantages et inconvénients de chaque solution

Sécuriser le Cloud par l'organisation des processus et le contrat de sla

- Classification des applications éligibles pour le Cloud
- Évaluation des risques et mise en place de leur gestion
- Plan de reprise d'activité
- Choix entre les Clouds souverains et ouverts
- Définir les critères de SLA de sécurité
- Responsabilité de l'entreprise : terminaux d'accès et réseaux locaux et distants
- Responsabilités partagées des parties prenantes (entreprise cliente et son fournisseur des services du Cloud) en cas de problèmes liés à la sécurité

Sécuriser le Cloud par la conception des architectures

- Isolement et étanchéité des solutions impliquées (Virtualisation, Stockage, orchestration, API, connecteurs...) et des applications
- Association des moyens de protection, en fonction du niveau de sécurité nécessaire des éléments du Cloud
- Cloud hybride
- Cryptage de la transmission au niveau des réseaux locaux du Datacenter
- Firewall local au sein du Cloud
- Sécuriser les accès locaux et distants au Cloud en tout lieu pour des terminaux mobiles : VPN SSL, VPN IPSec et IEEE802.11i
- Dispositifs Outband de sécurité et de Firewall d'identité pour les accès mobiles en local
- Impact des solutions incohérentes de sécurité et métriques de qualité indispensable
- Ingénierie du trafic IP et des flux de données pour le bon fonctionnement des applications

Sécuriser l'utilisation des périphériques personnels des employés pour accéder au Cloud (BYOD: Bring Your Own Device)

- Choix des solutions sécurisées d'accueil des terminaux (VDI, TS-WEB, RDP, PCoIP...)
- Sélection des périphériques : tablettes, Smartphone, OS, navigateurs.... et leurs contraintes
- Étude des vulnérabilités pour fixer les règles d'utilisation d'accès au Cloud
- Affectation des droits selon des critères techniques et organisationnels

Version du : 16/12/2021