CONCEPTION D'INFRASTRUCTURES

PROXMOX

Avant de commencer …

RESSOURCES

Les ressources disponibles sont multiples :

- Echanges entre les stagiaires,

- INTERNET, consultez les sites spécialisés,

VOUS AVEZ DES QUESTIONS ?

Notez-les, puis ...

N'hésitez pas à poser des questions à votre formateur :)

PRISE DE NOTE

Pensez à prendre des notes de ce que vous lisez, de vos questions, à faire des schémas ...

Prendre des notes c'est apprendre et retenir !

Conception d'Infrastructures

Objectifs:

- Ce module vise à fournir une compréhension approfondie des principes fondamentaux de la conception d'infrastructures, y compris la **sécurisation**, la **virtualisation** et le **cloud computing**.
- Les apprenants seront capables d'analyser les besoins pour concevoir des **infrastructures performantes** et **sûres**, tout en planifiant pour la capacité et la **continuité**. Enfin, ils apprendront à optimiser et maintenir des architectures adaptées aux besoins actuels et futurs.

Sommaire

CHAPITRE 5 : Sécurité des Infrastructures

Sécurité des infrastructures

Objectifs:

- Intégrer la sécurité dès la conception des infrastructures.
- Identifier les risques et menaces potentiels liés aux infrastructures.
- Mettre en place des bonnes pratiques de sécurité pour les infrastructures.
- Comprendre les enjeux de la conformité réglementaire dans la conception d'infrastructures.
- Appréhender les stratégies de protection des infrastructures contre les attaques.

Sécurité des infrastructures

Définition:

- **Sécurité dès la conception (Security by Design)**
- C'est une approche qui consiste à intégrer la sécurité comme un élément fondamental dès les premières phases de conception d'un système ou d'une infrastructure IT.

Sécurité des infrastructures

Objectifs:

- Réduction des coûts liés à la remédiation post-déploiement.
- Renforcement de la posture de sécurité globale.
- Prévention proactive plutôt que réactive.
- Meilleure conformité aux réglementations (RGPD, ISO 27001, NIS2, …).

Sécurité des infrastructures

Principes fondamentaux:

- Principe du moindre privilège : chaque composant ou utilisateur doit avoir uniquement les accès nécessaires.
- Séparation des responsabilités : cloisonnement fonctionnel (séparation DMZ / LAN).
- Redondance de sécurité : sécurité en couches (defense-in-depth).
- Surveillance dès le design : prévoir des outils de supervision dès l'architecture initiale.

Sécurité des infrastructures

Exemple

- Prévoir des VLANs segmentés avec des ACLs dès la phase de design réseau.
- Intégrer un système de journalisation centralisé (ex : SIEM) dès l'installation des serveurs.

Les risques et menaces potentiels liés aux infrastructures:

- **Les types de risques:**

Type de menace	Exemples
Physique	Incendie, vol de matériel, coupure de courant
Logique	Malware, attaques DDoS, ransomware
Humain	Erreur humaine, ingénierie sociale, abus de privilèges
Environnemental	Inondation, surchauffe des serveurs

Sécurité des infrastructures

Méthodes d'identification:

- Analyse de risque (EBIOS, OCTAVE, MEHARI).
- Cartographie des actifs critiques.
- Matrice de risques (Impact x Probabilité).
- Scénarios d'attaque (kill chain, MITRE ATT&CK).

Outils utiles

- Scanner de vulnérabilité : Nessus, OpenVAS.
- SIEM : Splunk, ELK, Wazuh.
- Gestion des configurations : Ansible, Terraform.

Sécurité des infrastructures

Bonnes pratiques de sécurité:

A. Sécurité réseau:

- **Segmentation réseau** : usage des VLAN, DMZ, et zones sécurisées.
- **Pare-feu et ACLs** : contrôler les flux inter-segments.
- **VPN/IPSec :** pour l'accès distant sécurisé.
- **Surveillance réseau (IDS/IPS)** : Snort, Suricata, Zeek.

Bonnes pratiques de sécurité:

B. Sécurité des serveurs:

- Harden des systèmes (désactivation des services inutiles, restriction des ports).
- Mise à jour régulière avec gestion de patching (WSUS, YUM, APT).
- Authentification forte (MFA, LDAP, Kerberos).
- Utilisation de systèmes de fichiers chiffrés (LUKS, BitLocker).

Sécurité des infrastructures

Bonnes pratiques de sécurité:

C. Sécurité physique:

- Contrôle d'accès biométrique ou badge.
- Onduleurs + générateurs de secours.
- Systèmes de détection incendie/gaz.

Sécurité des infrastructures

Bonnes pratiques de sécurité:

D. Bonnes pratiques générales:

- Principe de moindre privilège.
- Sauvegardes régulières (3-2-1).
- Journalisation + supervision.
- Tests de pénétration réguliers (Pentest).

Les enjeux de la conformité:

Norme / Réglementation	Description
ISO 27001	Système de management de la sécurité de l'information
RGPD	Règlement général sur la protection des données
NIS2 (UE)	Directive sur la sécurité des réseaux et systèmes d'information
PCI-DSS	Norme pour la sécurité des paiements par carte bancaire
HDS	Hébergement de données de santé (France)

Sécurité des infrastructures

Objectifs de conformité:

- Protéger les données personnelles et sensibles.
- Garantir la disponibilité, l'intégrité et la confidentialité des infrastructures.
- Éviter les sanctions financières ou pénales.

Exemple:

- Un datacenter hébergeant des données médicales doit être HDS certifié en France, avec des logs centralisés, un plan de reprise d'activité (PRA) et des accès strictement contrôlés.

Sécurité des infrastructures

Stratégies de protection:

A. Approche en couches (Defense-in-Depth): Met en place plusieurs couches défensives :

- **Physique** : Contrôle d'accès au bâtiment.
- **Réseau** : Firewall, IDS/IPS.
- **Systèmes** : Bastion, antivirus, patching.
- **Applications** : WAF, authenticité des requêtes.
- **Données** : Chiffrement.
- **Utilisateurs** : Sensibilisation, MFA.

Stratégies de protection:

B. Automatisation et orchestration:

- Utilisation d'outils comme Ansible, Puppet, ou Terraform pour appliquer des configurations sécurisées.
- Réponse automatisée aux incidents avec SOAR (Security Orchestration, Automation, and Response).

Stratégies de protection:

C. Gestion des identités et des accès:

- Mise en œuvre de RBAC (Role-Based Access Control).
- Intégration avec AD, LDAP, SSO.
- Audit régulier des droits.

Stratégies de protection:

D. Surveillance et détection proactive:

- Supervision avec SIEM.
- Analyse de comportements (UEBA).
- Threat Intelligence (CTI) : MISP, VirusTotal, Shodan.

Stratégies de protection:

Exemple:

Pour protéger un système e-commerce :

- WAF sur l'interface web.
- IDS en amont de la base de données.
  Accès VPN + MFA pour l'administration.
- Données sensibles chiffrées au repos et en transit.

Sécurité des infrastructures

Exercice: Élaboration d'une Politique de Sécurité

- Entreprise : MedData Santé: Une entreprise fictive spécialisée dans la gestion des données de santé (hébergement de dossiers médicaux électroniques).
- Mission : Fournir une plateforme sécurisée pour :
  - Le stockage et l'accès aux dossiers médicaux électroniques (DMP).
  - L'hébergement des résultats d'analyses médicales, ordonnances numériques.
  - La téléconsultation, la prescription électronique, etc.
- Infrastructure : Hybride (on-premise + cloud privé certifié HDS).
- Effectif : 150 employés.
- Clients : Hôpitaux, cliniques, laboratoires, professionnels de santé libéraux.
- Contraintes réglementaires : RGPD, HDS (Hébergeur de Données de Santé), ISO 27001.

Exercice: Élaboration d'une Politique de Sécurité

- En tant que responsable de la sécurité des systèmes d'information, votre mission est de créer une politique de sécurité pour la nouvelle infrastructure de l'entreprise. Vous devez :
  - Identifier cinq risques liés à la sécurité de l'infrastructure.
  - Établir des bonnes pratiques pour sécuriser les composantes de l'infrastructure contre ces risques.
  - Définir des mesures de conformité réglementaire que l'entreprise doit respecter.
  - Proposer une stratégie pour protéger l'infrastructure contre les attaques, incluant des solutions de détection et de réponse aux incidents.

CONCLUSION DE LA SEANCE

FÉLICITATIONS !!!

Vous savez maintenant pourquoi il faut sécuriser les infrastructures et quelles sont les solutions à mettre en place