

Sommaire

1. Introduction

- Importance de la sécurisation des architectures informatiques

2. Évaluation des risques

- Identification des menaces
- Analyse d'impact

3. Contrôle d'accès

- Mécanismes d'authentification
- Authentification multi-facteurs (MFA)

4. Chiffrement des données

- Chiffrement au repos
- Chiffrement en transit

5. Mise à jour et correctifs

- Importance des mises à jour régulières
- Gestion des vulnérabilités

6. Sécurité des réseaux

- Pare-feu et IDS
- Utilisation des VPN

7. Formation et sensibilisation

- Programmes de formation pour les employés
- Sensibilisation aux menaces courantes

8. Plan de continuité d'activité

- Élaboration d'un plan de reprise après sinistre
- Stratégies de continuité

9. Surveillance et audits

- Outils de surveillance
- Audits de sécurité réguliers

10. Segmentation du réseau

- Importance de la segmentation
- Mise en œuvre de la segmentation

11. Gestion des incidents

- Plan de réponse aux incidents
- Récupération après une cyberattaque