PARIS PANTHÉON-ASSAS UNIVERSITÉ

Projet Cloud :

TechTrendz AWS architecture

Réalisé par:

Redwane Zaghouini

Rabab Soleiman

Mohamed Anouar Bouachour

PARIS PANTHÉON-ASSAS UNIVERSITÉ

Analyse de Risques

Scénario 1: Accès Non Autorisé aux Bases de Données

Vraisemblance : Faible

Impact : Très élevé

Mitigation :

Chiffrer les données en transit et au repos.

Utiliser des groupes de sécurité stricts pour limiter l'accès.

Surveiller les accès via CloudWatch et CloudTrail.

Scénario 2 : Compromission des Clés IAM

Vraisemblance : Moyenne
Impact : Élevé
Mitigation *:* Activer MFA pour toutes les actions critiques. Utiliser des rôles IAM avec des permissions minimales nécessaires. Surveiller et gérer les clés d'accès avec rotation régulière.

Scénario 3 : Compromission des S3 Buckets Publics

Vraisemblance : Moyenne
Impact : Élevé
Correction : on doit configurer les politiques des buckets S3 avec des permissions minimales,activer "Block Public Access" pour les buckets sensibles etutiliser AWS Config et CloudTrail pour surveiller les modifications.

Scénario 4 : Exploitation d'une Vulnérabilité dans le Code Lambda

Vraisemblance : Faible
Impact : Élevé
Mitigation : Limiter les permissions IAM associées aux fonctions Lambda. Mettre en place des tests de sécurité continus (CI/CD).

Scénario 5 : Attaque par Déni de Service Distribué (DDoS)

Description :

Une attaque DDoS vise à rendre un service indisponible en inondant les systèmes, les réseaux ou les applications avec un trafic excessif.

Vraisemblance :

Modérée. (Les attaques DDoS sont fréquentes et peuvent cibler n'importe quelle organisation)

Impact :

Élevé. (Une attaque DDoS réussie peut rendre votre application ou service indisponible, affectant les utilisateurs et entraînant des pertes financières)

Mitigation :

Utilisation d'AWS Shield : on doit activer AWS Shield Standard (inclus) ou Advanced pour protéger vos applications contre les attaques DDoS.

Mise en Place de WAF (Web Application Firewall) : on doit Configurer AWS WAF pour filtrer le trafic et bloquer les requêtes malveillantes.

Auto-scaling : on doit Configurer l'auto-scaling pour absorber les pics de trafic.

Scénario 6 : Exploitation de Vulnérabilités Logicielles

Description :

Les attaquants peuvent exploiter des vulnérabilités dans les logiciels et les services que vous utilisez pour obtenir un accès non autorisé ou exécuter du code malveillant.

Vraisemblance :

Moyenne (Les vulnérabilités logicielles sont courantes et doivent être régulièrement corrigées)

Impact :

Élevé. L'exploitation réussie d'une vulnérabilité peut conduire à une compromission totale du système.

Mitigation:

Implémenter un processus de gestion des patches pour corriger rapidement les vulnérabilités.

Utiliser des outils de scan de vulnérabilités pour identifier et corriger les failles.

Adopter des pratiques de développement sécurisé et effectuer des tests de sécurité réguliers.

Scénario 7 : Exposition de Données Sensibles

Description :

Des données sensibles peuvent être accidentellement exposées via des S3 buckets mal configurés.

Vraisemblance :

Élevée. Les erreurs de configuration des S3 buckets sont fréquentes.

Impact :

Très élevé. L'exposition de données sensibles peut entraîner des violations de la vie privée, des sanctions réglementaires et une perte de confiance des clients.

Mitigation :

Configuration des Politiques S3 : Utilisez des politiques strictes pour contrôler l'accès aux S3 buckets.

Activation de la Sécurité des S3 Buckets : Activez les contrôles de sécurité comme le chiffrement par défaut, les journaux d'accès et la surveillance des objets publics.

Outils d'Audit : Utilisez AWS Config et Amazon Macie pour détecter et signaler les configurations incorrectes et les données sensibles.

Scénario 8 : Mauvaise Configuration des Groupes de Sécurité

Vraisemblance : Élevée
Impact : Élevé
Mitigation:

Effectuer des audits réguliers pour identifier et corriger les règles de sécurité excessivement permissives.

Création des modèles de groupes de sécurité pour garantir des configurations cohérentes et sécurisées.

Utilisation des outils comme AWS Trusted Advisor ou des solutions tierces pour analyser automatiquement les configurations des groupes de sécurité et signaler les problèmes potentiels.

Scénario 9 : Compromission des Instances EC2 (Web Servers)

Vraisemblance : Moyenne
Impact : Élevé

Mitigation : Utiliser un WAF pour filtrer les requêtes malveillantes. Appliquer des correctifs de sécurité régulièrement. Restreindre les permissions IAM pour limiter les actions des instances EC2.

Scénario 10 : Compromission de Compte Administratif

Description :

Un compte administratif compromis peut donner à un attaquant un accès complet à votre infrastructure, permettant des modifications destructrices ou le vol de données.

Vraisemblance :

Moyenne. Les comptes administratifs sont des cibles privilégiées pour les attaquants.

Impact :

Élevé. La compromission d'un compte administratif peut entraîner une perte complète de contrôle sur votre infrastructure.

Mtigation :

Authentification Multi-Facteur (MFA) : on doit exiger l'utilisation de MFA pour tous les comptes administratifs.

Limitation des Droits : il faut appliquer le principe du moindre privilège et créer des rôles administratifs spécifiques avec des permissions minimales nécessaires.

Surveillance et Journaux : il faut activer la journalisation AWS CloudTrail et surveiller les activités suspectes.

Evaluation des risques :

Scénario 1 : Accès Non Autorisé aux Bases de Donnée :

Probabilité : faible

Criticité : élevée

Impact : élevé

Scénario 2 : Compromission des Clés IAM

Probabilité : moyenne

Criticité : Élevée

Impact : Élevé

Scénario 3 : Compromission des S3 Buckets Publics

Probabilité : faible

Criticité : Élevée

Impact : Élevé

Scénario 4 : Exploitation d'une Vulnérabilité dans le Code Lambda

Probabilité : faible

Criticité : Élevée

Impact : élevée

Scénario 5 : Attaque par Déni de Service Distribué (DDoS)

Probabilité : moyenne

Criticité : Élevée

Impact : Élevé

Scénario 6 : Exploitation de Vulnérabilités Logicielles

Probabilité : élevée

Criticité : Élevée

Impact : Élevé

Scénario 7 : Exposition de Données Sensibles

Probabilité : élevée

Criticité : élevée

Impact : élevé

Scénario 8 : Mauvaise Configuration des Groupes de Sécurité

Probabilité : moyenne

Criticité : Élevée

Impact : moyenne

Scénario 9 : Compromission des Instances EC2 (Web Servers)

Probabilité : moyenne

Criticité : Élevée

Impact : Élevé

Scénario 10 : Compromission de Compte Administratif

Probabilité : moyenne

Criticité : élevée

Impact : élevé

Matrice :

Impact / Probabilité	Faible	Moyen	Élevé
Faible			S4 , S1,S3
Moyen		S8	S10,S9, S2,S5
Élevé			S7,S6

Plan D'action de continuité :

Stratégies de Continuité des Opérations

Redondance et Réplication :

Utilisation des régions et des zones de disponibilité multiples pour déployer des services.

Réplication les données critiques entre différentes régions avec AWS RDS Multi-AZ et Amazon S3 Cross-Region Replication.

Sauvegardes et Restauration :

Automatisation des sauvegardes régulières des données avec AWS Backup.

Tester régulièrement les procédures de restauration pour garantir l'intégrité et la disponibilité des sauvegardes.

Plans de Réponse aux Incidents

Détection et Surveillance :

Implémenter AWS CloudTrail et CloudWatch pour la surveillance des activités et la détection des incidents.

Configuration des alarmes pour les comportements anormaux et les violations potentielles de sécurité.

Équipe de Réponse aux Incidents :

Formation d'une équipe dédiée à la réponse aux incidents avec des rôles et des responsabilités définis.

Établissement un plan de communication pour informer les parties prenantes en cas d'incident.

Plans de Reprise après Sinistre

Définition les RTO et RPO :

Détermination des objectifs de temps de récupération (RTO) et les objectifs de point de récupération (RPO) pour chaque service critique.

Scénarios de Reprise après l'incident :

Perte de données critiques (utiliser les sauvegardes pour restaurer les données).

Défaillance de la région AWS (basculer les opérations vers une autre région).

Tests et Exercices :

Faire des tests de reprise après sinistre régulièrement pour valider les procédures et identifier les améliorations nécessaires.

Sécurité et Conformité

Gestion des Accès :

Implémentation une gestion stricte des accès avec IAM, MFA obligatoire et politique de moindre privilège.

Effectuation des audits réguliers des permissions et des accès.

Chiffrement :

Chiffrement des données en transit et au repos avec AWS KMS.

Utilisation des certificats SSL/TLS pour sécuriser les communications réseau.

Conformité Réglementaire :

Maintien de la conformité avec les réglementations pertinentes (RGPD HIPAA) en utilisant des services certifiés AWS.

Plans de Formation et Sensibilisation

Formation Continue :

Formation régulièrement les employés aux meilleures pratiques de sécurité et aux procédures de continuité des opérations.

Simulations d'Incidents :

Organisation des exercices de simulation d'incidents pour tester la préparation et la réactivité des équipes.