Compte Rendu Détaillé du Projet : Gestion de Crise Cybersécurité

Date de rendu : 04/04/2025

Durée du projet : 10/2024 – 12/2024

**1. Contexte et Objectifs**

Objectif principal : Préparer l’organisation à faire face à une attaque ransomware via une simulation réaliste, valider le Plan de Reprise d’Activité (PRA), mettre à jour les politiques de sécurité, et auditer l’efficacité des sauvegardes.

Livrables attendus :

- Rapport de simulation d’attaque ransomware avec scénario et résultats.

- PRA mis à jour et testé.

- Politiques de sécurité révisées (charte utilisateur, procédures d’urgence).

- Audit des sauvegardes et preuve de restauration réussie.

Contraintes :

- Minimiser l’impact sur les opérations quotidiennes pendant la simulation.

- Conformité aux réglementations (RGPD, ISO 27001).

**2. Méthodologie et Organisation**

2.1. Rôles de l’Équipe

- Responsable de la Gestion de Crise : Coordination des actions, communication interne/externe.

- Expert Cybersécurité : Simulation de l’attaque, analyse des vulnérabilités.

- Administrateur Système : Activation du PRA, restauration des sauvegardes.

- Juriste/DPO : Vérification de la conformité légale des actions.

- Responsable Communication : Gestion des messages aux parties prenantes.

2.2. Outils Utilisés

- Metasploit/Cobalt Strike : Simulation de l’attaque ransomware.

- Veeam/Backup : Audit et restauration des sauvegardes.

- SIEM (ex: Splunk) : Analyse des logs pour détecter l’attaque.

- Tableau de Bord de Crise : Outil collaboratif (ex: Microsoft Teams + Trello).

**3. Phases du Projet**

3.1. Phase 1 : Préparation (2h)

Objectif : Définir le scénario de crise et préparer les ressources.

Tâches réalisées :

- Scénario d’attaque :

- Vecteur : Phishing avec pièce jointe Excel malveillante (macro).

- Propagation : Chiffrement des fichiers via LockBit 3.0 simulé.

- Checklist PRA :

- Priorité des systèmes critiques (ERP, serveurs de base de données).

- Contacts d’urgence (hébergeur, prestataire de sauvegarde).

3.2. Phase 2 : Simulation d’Attaque Ransomware (3h)

Objectif : Tester la détection et la réponse de l’équipe.

Tâches réalisées :

- Lancement de l’attaque :

- Envoi d’emails de phishing à 10 collaborateurs (testés).

- Exécution d’un script PowerShell simulant le chiffrement.

- Réponse immédiate :

- Isolation des machines infectées (déconnexion réseau).

- Activation du plan de communication de crise.

3.3. Phase 3 : Activation du PRA (4h)

Objectif : Restaurer les opérations critiques.

Tâches réalisées :

- Restauration des sauvegardes :

- Utilisation de Veeam pour récupérer les VM critiques (temps cible : 4h).

- Vérification de l’intégrité des données (checksums).

- Basculement vers le site de secours :

- Réactivation des services cloud (AWS S3, Office 365).

3.4. Phase 4 : Mise à Jour des Politiques de Sécurité (2h)

Objectif : Corriger les faiblesses identifiées.

Tâches réalisées :

- Révision de la charte utilisateur :

- Interdiction des macros Excel sans autorisation.

- Obligation de MFA (Microsoft Authenticator) pour tous les accès distants.

- Procédures d’urgence :

- Délai maximal de déclenchement du PRA : 1h après détection.

3.5. Phase 5 : Audit des Sauvegardes (3h)

Objectif : Garantir la fiabilité des sauvegardes.

Tâches réalisées :

- Tests de restauration :

- 5 sauvegardes aléatoires restaurées (taux de succès : 100%).

- Mesure du RTO (Recovery Time Objective) : 3h45.

- Vérification des sauvegardes hors ligne :

- 2 sauvegardes air-gapped stockées hors site (non accessibles via le réseau).

3.6. Phase 6 : Documentation et Retour d’Expérience (2h)

Objectif : Capitaliser sur les leçons apprises.

Tâches réalisées :

- Rapport de simulation :

- Chronologie de l’attaque, temps de réponse, points de blocage.

- Atelier de rétrospective :

- Succès : Détection rapide via le SIEM.

- Améliorations : Former les utilisateurs aux emails de phishing.

**4. Résultats et Livrables**

4.1. Crise Gérée avec Succès

- Temps de restauration : Respect du RTO fixé à 4h.

- Données récupérées : 100% des données critiques restaurées.

4.2. Documentation

- Nouvelle charte utilisateur : Intégrée au contrat de travail.

- Checklist PRA : Incluant les étapes post-crise (analyse forensique).

**5. Défis Rencontrés et Solutions**

- Problème : Sauvegarde partiellement chiffrée par le ransomware simulé.

- Solution : Ajout de sauvegardes immuables (ex: AWS S3 Object Lock).

- Problème : PRA incomplet pour les applications métier.

- Solution : Ajout de procédures spécifiques dans le PRA (ex: restauration de la base de données SAP).

**6. Bilan et Améliorations Futures**

- Points forts : Coordination efficace de l’équipe, restauration rapide.

- Axes d’amélioration :

- Exercices de phishing réguliers pour les utilisateurs.

- Simulation de scénarios complexes (ex: attaque double extorsion).

**Annexes**

Annexe 1 : Capture d’écran du SIEM pendant l’attaque

Légende : Alertes de connexions suspectes et fichiers chiffrés.

Annexe 2 : Extrait de la Charte Utilateur Révisée

Article 5 : Sécurité des Emails

- Tout email suspect doit être signalé via le bouton "Report Phishing".

- Les macros Excel/Word sont interdites sans validation de la DSI.

```

Annexe 3 : Checklist de Test de Sauvegarde

| Système | RTO Visé | RTO Atteint | Statut|

|--------------------|--------------|------------------|------------|

| Serveur ERP | 4h | 3h45 | ✅ |

| Base de données | 2h | 1h50 | ✅ |

| Fichiers partagés | 6h | 5h20 | ✅ |

Équipe Projet

Membres : Axel