Exercice : CFA Numérique – Haute Disponibilité et PRA

KOUASSI GLOHNDY JEAN-MARIE

Sommaire

1. Introduction

Le CFA Numérique est un centre de formation spécialisé dans les métiers du numérique, comptant 100 salariés et proposant des formations 100% à distance. Son infrastructure informatique est donc critique pour assurer la continuité pédagogique et administrative.

Suite à une cyberattaque ayant compromis le serveur Active Directory, tous les fichiers ont été chiffrés. Cette situation met en évidence la nécessité d'un Plan de Reprise d'Activité (PRA) afin de garantir la haute disponibilité (HA) et la résilience du système d'information.

2. Analyse de l'existant et identification des risques

L'infrastructure actuelle comprend :
- Un serveur Active Directory centralisant l'authentification et la gestion des utilisateurs.
- Des serveurs applicatifs et bases de données pour les plateformes pédagogiques.
- Des services cloud et de communication.

Risques identifiés :
- Cyberattaques (ransomware, phishing, déni de service).
- Pannes matérielles (serveurs, stockage, alimentation électrique).
- Erreurs humaines (mauvaises configurations, suppressions accidentelles).
- Sinistres physiques (incendie, inondation, panne électrique majeure).

Impacts potentiels :
- Interruption de l'enseignement à distance.
- Perte de données sensibles (dossiers étudiants, documents administratifs).
- Atteinte à la réputation de l'établissement.
- Blocage des activités administratives et pédagogiques.

3. Composants du PRA et priorisation des services

Un PRA efficace repose sur plusieurs composants techniques et organisationnels :

- Sauvegardes régulières : locales et externalisées.
- Sites de secours : cold site, warm site, hot site selon les moyens.
- Redondance des serveurs et réseaux.
- Procédures documentées de restauration.

Priorisation des services (selon criticité et RTO/RPO) :
1. Active Directory et authentification (essentiel pour accès aux ressources).
2. Plateformes pédagogiques (accès aux cours et examens en ligne).

3. Serveurs administratifs et bases de données.
4. Services de communication (email, outils collaboratifs).
5. Services secondaires (intranet, communication externe).

4. Procédure en cas de cyberattaque sur l'Active Directory

Étapes techniques :
- Isoler immédiatement le serveur compromis pour éviter la propagation du malware.
- Identifier la nature de l'attaque et vérifier l'étendue de la compromission.
- Restaurer le contrôleur de domaine depuis une sauvegarde saine.
- Mettre en place un serveur Active Directory de secours (redondant) pour assurer la continuité.
- Réinitialiser les mots de passe utilisateurs et renforcer les politiques de sécurité.

Étapes organisationnelles :
- Informer la direction, les équipes IT et les utilisateurs des mesures en cours.
- Suivre une procédure documentée avec rôles et responsabilités clairs.
- Communiquer aux apprenants et partenaires les délais de rétablissement prévus.

Bonnes pratiques :
- Effectuer des tests réguliers de restauration.
- Mettre en place un PRA automatisé (bascule rapide sur serveur de secours).
- Renforcer la cybersécurité (EDR, segmentation réseau, mises à jour régulières).

5. Conclusion

La cyberattaque survenue au sein du CFA Numérique démontre l'importance vitale d'un Plan de Reprise d'Activité adapté. La mise en place de sauvegardes fiables, de redondance et de procédures de restauration garantit la continuité pédagogique et administrative même en cas de sinistre. Enfin, la sensibilisation des équipes et les tests réguliers du PRA sont des éléments clés pour assurer la haute disponibilité et la résilience de l'infrastructure informatique.