Plan de Reprise d'Activité (PRA)

Entreprise FINPLUS

TABLE DES MATIERES

Introduction

Dans le monde dynamique des services financiers, l'entreprise FINPLUS reconnaît l'importance stratégique d'anticiper et de réagir de manière efficace face à d'éventuelles interruptions majeures. Le Plan de Reprise d'Activité (PRA) élaboré pour FINPLUS est conçu pour être une feuille de route proactive, détaillant les actions spécifiques à entreprendre afin de restaurer rapidement les opérations normales après un incident majeur. Face aux risques potentiels tels que les cyberattaques, les pannes matérielles, et les catastrophes naturelles, ce PRA assure la résilience de l'entreprise, préservant ainsi la confiance de ses clients et la stabilité de ses activités financières.

Responsabilités Assignées

Responsable Global du PCA :

- Le Directeur de la Sécurité Informatique, est désigné comme le responsable global du PCA, assurant la coordination et la supervision du processus de continuité d'activité.

Responsable de la Communication :

- Le Responsable de la Communication, est chargé de la diffusion d'informations aux employés, aux clients et aux partenaires pendant une interruption, assurant une communication transparente.

Identification des Actifs Critiques

1.1. **Serveurs Physiques Haute Performance :**

- Systèmes hébergeant les applications bancaires en ligne, les services de gestion de portefeuille, les systèmes de paiement électronique, etc.

- Mesures de redondance et de clustering pour garantir la disponibilité.

1.2. **Systèmes de Stockage Dédiés :**

- Stockage des données financières avec capacités de redondance et de sauvegarde automatisée.
- Utilisation de technologies avancées de stockage.

1.3. **Réseau Redondant :**

- Architecture réseau avec des chemins multiples pour assurer une disponibilité constante.
- Pare-feu sophistiqué pour filtrer le trafic entrant et sortant.

1.4. **Serveurs d'Applications Web Sécurisées :**

- Hébergent des applications bancaires en ligne avec des mécanismes de chiffrement SSL/TLS.
- Garantir la sécurité des transactions et des opérations bancaires.

1.5. **Terminaux de Paiement Électronique :**

- Infrastructure dédiée avec des protocoles sécurisés de traitement des transactions.
- Assurer la sécurité des transactions électroniques.

1.6. **Bases de Données Clients :**

- Bases de données distribuées stockant et gérant les informations clients.
- Sauvegardes régulières pour prévenir la perte de données.

1.7. **Centre de Données de Secours :**

- Site distant avec serveurs et systèmes de stockage redondants.
- Mécanismes de réplication des données en temps réel pour assurer la continuité.

Évaluation des Risques

2.1. **Cyberattaques :**

- Risque de compromission des données financières.
- Mesures de sécurité : pare-feu nouvelle génération, détection et prévention des intrusions, chiffrement des données.

2.2. **Panne Matérielle :**

- Risque d'interruption des services dus à des défaillances matérielles.
- Mesures de sécurité : serveurs redondants, sauvegardes régulières.

2.3. **Catastrophes Naturelles :**

- Risque lié aux catastrophes naturelles (inondations, tremblements de terre).
- Mesures de sécurité : centre de données de secours avec réplication des données.

Définition des Objectifs de Récupération

3.1. **Serveurs Physiques Haute Performance :**

- RTO : 4 heures
- RPO : 2 heures

3.2. **Systèmes de Stockage Dédiés :**

- RTO : 8 heures
- RPO : 4 heures

3.3. **Réseau Redondant :**

- RTO : 2 heures
- RPO : 1 heure

3.4. **Serveurs d'Applications Web Sécurisées :**

- RTO : 4 heures
- RPO : 2 heures

3.5. **Terminaux de Paiement Électronique :**

- RTO : 6 heures
- RPO : 3 heures

3.6. **Bases de Données Clients :**

- RTO : 8 heures
- RPO : 4 heures

3.7. **Centre de Données de Secours :**

- RTO : 12 heures
- RPO : 6 heures

Mesures pour Maintenir des Opérations Minimales

1. Serveurs Physiques Haute Performance :

1.1. Identification de l'Incident : L'identification de la défaillance des serveurs physiques peut être réalisée à l'aide de systèmes de surveillance automatisés qui détectent des signes de dégradation des performances, d'alertes de sécurité, ou de perte de connectivité. Par

exemple, des outils de surveillance des performances peuvent signaler une augmentation anormale du temps de réponse ou des erreurs fréquentes.

1.2. Activation du Plan de Reprise d'Activité (PRA) : Dès la confirmation de l'incident, la cellule de crise doit être activée. Cela implique la notification immédiate des membres de l'équipe technique, du responsable de la continuité d'activité et d'autres parties prenantes clés. Les canaux de communication d'urgence, tels que les alertes SMS et les appels téléphoniques, peuvent être utilisés pour garantir une mobilisation rapide.

1.3. Mobilisation des Équipes : L'équipe technique doit se réunir rapidement pour évaluer l'étendue de la défaillance. Des outils de gestion des incidents peuvent être utilisés pour créer un ticket d'incident, attribuer des responsabilités et suivre l'avancement de la résolution. Par exemple, le responsable de l'équipe peut être chargé d'évaluer l'impact sur les applications bancaires en ligne, tandis qu'un expert en infrastructure examine les serveurs physiques eux-mêmes.

1.4. Sélection du Serveur de Reprise : Le choix du serveur de reprise dépendra de plusieurs facteurs, y compris la disponibilité des serveurs de secours, leur capacité à gérer la charge de travail prévue, et la géo-redondance si cela est pertinent. Une évaluation rapide des serveurs de reprise disponibles peut être effectuée pour déterminer le plus adapté à la situation.

1.5. Restauration des Données : Utiliser les sauvegardes pour restaurer les données sur le serveur de reprise. Les sauvegardes doivent être régulièrement testées pour garantir leur intégrité et leur disponibilité. Les procédures automatisées de restauration peuvent être mises en œuvre pour accélérer le processus.

1.6. Configuration des Paramètres de Redondance : Mettre en place les paramètres de redondance sur le serveur de reprise pour garantir une disponibilité continue. Cela peut inclure la configuration de clusters, la mise en œuvre de solutions de basculement automatique, et la synchronisation des données en temps réel avec le serveur principal.

1.7. Tests de Fonctionnement : Effectuer des tests approfondis du serveur de reprise et des applications. Cela implique de simuler des charges de travail réalistes, de vérifier la

connectivité réseau, et de s'assurer que toutes les fonctionnalités critiques sont opérationnelles. Les résultats des tests doivent être documentés pour évaluer l'efficacité du PRA.

1.8. Basculement : Une fois que la reprise a été validée par les tests, le basculement vers le serveur de reprise peut être effectué. Cela peut être réalisé en redirigeant le trafic vers le serveur de reprise, en mettant à jour les enregistrements DNS, ou en utilisant d'autres mécanismes de redirection. Les utilisateurs doivent être informés du basculement et des instructions éventuelles pour reprendre leurs activités.

2. Systèmes de Stockage Dédiés :

Lorsqu'une défaillance majeure est détectée dans les systèmes de stockage dédiés, la première étape consiste à identifier l'incident de manière précise. Cela peut être réalisé à l'aide d'outils de surveillance qui signalent des anomalies, telles que des erreurs de lecture/écriture ou des pannes matérielles.

Une fois l'incident identifié, le plan de reprise d'activité (PRA) est immédiatement activé. Cette activation doit être rapide et efficace pour minimiser l'impact sur les opérations. Les membres de l'équipe technique responsables de la gestion des systèmes de stockage sont immédiatement alertés et mobilisés.

L'étape suivante consiste à évaluer l'étendue de la défaillance. L'équipe technique doit analyser les journaux d'événements, les rapports d'erreur, et effectuer des tests de diagnostic pour comprendre la nature et la portée de la défaillance. Par exemple, si un disque dur a échoué, il est essentiel de déterminer s'il s'agit d'une défaillance isolée ou si d'autres disques sont également susceptibles de tomber en panne.

La restauration des données intervient ensuite, en utilisant les capacités de redondance préalablement mises en place et les sauvegardes régulières. Par exemple, si les données sont stockées de manière redondante sur plusieurs disques, le système peut automatiquement reconstruire les données perdues à partir des copies existantes.

Dans le cadre de la configuration des paramètres de redondance, des ajustements peuvent être apportés pour renforcer la robustesse du système de stockage. Cela pourrait inclure l'ajout de nouveaux disques, la mise en place de nouvelles stratégies de redondance, ou la correction de configurations susceptibles de causer des défaillances.

Les tests de fonctionnement sont cruciaux pour s'assurer de l'intégrité des systèmes de stockage restaurés. Des scénarios de test, tels que la simulation de charges de travail élevées, doivent être exécutés pour garantir que les systèmes peuvent fonctionner de manière optimale dans des conditions normales.

Enfin, une fois que la reprise a été validée par des tests rigoureux, le basculement vers les systèmes restaurés peut être effectué. Cela signifie que l'infrastructure revient à son état opérationnel normal, et les utilisateurs peuvent reprendre leurs activités habituelles sans interruption significative.

3. Réseau Redondant :

En cas de défaillance affectant l'architecture réseau, l'identification rapide de l'incident est cruciale. Les outils de surveillance du réseau, tels que les systèmes de détection d'intrusion et les alertes automatiques, sont utilisés pour détecter les anomalies. Dès qu'une défaillance est confirmée, l'activation du Plan de Reprise d'Activité (PRA) est immédiate, impliquant la mobilisation de l'équipe technique dédiée.

Une fois l'incident confirmé, l'équipe technique évalue l'étendue de la défaillance en analysant les journaux d'événements, en effectuant des tests de connectivité, et en collaborant avec les fournisseurs de services réseau. Cette évaluation permet de déterminer la meilleure approche pour la reprise d'activité.

La configuration des chemins réseau redondants intervient à ce stade. Cela implique l'activation des liens réseau de secours et la redirection du trafic vers des chemins alternatifs. Par exemple, si l'incident concerne la connexion principale à Internet, la bascule vers une connexion de secours peut être effectuée en ajustant la configuration des routeurs et des pares-feux.

Des tests de fonctionnement sont essentiels pour garantir la stabilité du réseau redondant. Cela peut inclure des simulations de trafic, des tests de charge, et la vérification de la disponibilité des services critiques. Les résultats des tests orientent les ajustements nécessaires pour optimiser les performances du réseau redondant.

Une fois la reprise validée par des tests concluants, le basculement vers les chemins réseau redondants est effectué. Cette étape doit être soigneusement orchestrée pour minimiser les interruptions de service. Les équipes de communication doivent informer les parties prenantes de la transition, tandis que les mécanismes de surveillance continuent à être opérationnels pour détecter toute anomalie après le basculement.

4. Serveurs d'Applications Web Sécurisées :

Communication d'Urgence : La cellule de crise est immédiatement informée de l'incident. Des exemples de canaux de communication peuvent inclure l'utilisation de messagerie instantanée, de notifications push et d'e-mails d'alerte. Les parties prenantes, y compris les responsables IT et les membres de la direction, sont notifiées de manière transparente.

Mobilisation des Équipes : La cellule de crise prend en charge la coordination des efforts de reprise. Par exemple, le responsable de la sécurité informatique pourrait être chargé de surveiller les activités malveillantes pendant que l'administrateur système se concentre sur la restauration des serveurs.

Récupération d'Urgence : L'utilisation des sauvegardes les plus récentes est cruciale. Par exemple, si une base de données est compromise, la restauration à partir d'une sauvegarde récente minimise la perte de données. La mise en place rapide des mécanismes de chiffrement SSL/TLS, avec des certificats valides, assure la sécurité des transactions.

Tests de Fonctionnement : Les tests de fonctionnement incluent la vérification approfondie des applications web restaurées. Par exemple, en simulant des transactions réelles, on peut s'assurer que toutes les fonctionnalités, telles que la gestion de compte et les paiements en ligne, sont opérationnelles. Les tests de sécurité, tels que des analyses de vulnérabilité, garantissent l'efficacité des mécanismes de chiffrement.

Activation des Services : Le processus d'activation doit être progressif. En commençant par les fonctionnalités essentielles, comme l'accès aux comptes, et en étendant progressivement aux services complets, on minimise les risques potentiels liés à une reprise complète. Par exemple, les services critiques sont rétablis en priorité, suivi par les fonctionnalités moins sensibles.

Surveillance Continue : Une fois les services activés, une surveillance continue est cruciale. Des outils de surveillance en temps réel détectent toute anomalie, et les configurations de sécurité sont ajustées en conséquence. Par exemple, des outils d'IDS/IPS peuvent être utilisés pour surveiller les activités réseau suspectes.

Communication de la Fin de Crise : La cellule de crise informe les parties prenantes de la reprise complète des opérations normales. Cette communication peut inclure des rapports détaillés sur les mesures prises, les leçons apprises et les actions préventives pour l'avenir.

5. Terminaux de Paiement Électronique :

Activation du PRA : Lorsqu'une interruption affecte les terminaux de paiement électronique, le PRA est déclenché immédiatement. Par exemple, en cas d'une panne matérielle ou d'une attaque ciblée, l'équipe de sécurité informatique doit être alertée pour initier le processus de reprise.

Communication d'Urgence : La cellule de crise, composée de membres préalablement désignés, est immédiatement informée de l'incident et de l'activation du PRA. Les parties prenantes, y compris les responsables des services concernés, sont notifiées de manière transparente et rapide.

Mobilisation des Équipes : La cellule de crise prend en charge la coordination des efforts de reprise. Par exemple, le responsable des terminaux de paiement électronique supervise le processus, travaillant en étroite collaboration avec les équipes techniques responsables de la maintenance des terminaux.

Récupération d'Urgence : La restauration des configurations des terminaux de paiement électronique commence en utilisant les sauvegardes récentes. Les protocoles sécurisés de

traitement des transactions sont rétablis pour garantir la sécurité des opérations. Par exemple, les configurations logicielles et les clés de chiffrement peuvent être restaurées à partir de sauvegardes validées.

Tests de Transactions : Des transactions de test sont effectuées pour vérifier l'intégrité et la sécurité des terminaux. Cela peut inclure la simulation de transactions avec des cartes de test pour s'assurer que les protocoles de chiffrement et les processus de traitement des paiements fonctionnent correctement.

Activation Graduelle des Terminaux : Les terminaux sont activés de manière progressive, en commençant par des zones ou services spécifiques. Par exemple, les terminaux dans une succursale spécifique peuvent être réactivés avant d'étendre la reprise à l'ensemble du réseau. Cette approche graduée permet de surveiller attentivement chaque étape de la reprise.

Surveillance Continue : Une surveillance constante est établie pour détecter toute activité anormale. Des outils de détection d'intrusion et de surveillance des transactions sont utilisés pour assurer la sécurité continue. En cas d'activité suspecte, des mesures correctives sont prises immédiatement.

Réajuster les Configurations de Sécurité : Au besoin, les configurations de sécurité sont réajustées pour renforcer la protection contre de nouvelles menaces potentielles. Cela peut inclure des mises à jour logicielles, des changements de clés de chiffrement, ou des ajustements dans les politiques de sécurité.

Communication de la Fin de Crise : Une fois la reprise complète des opérations normales assurée, les parties prenantes sont informées de manière formelle. Une communication transparente sur la résolution de l'incident, les mesures de sécurité prises, et la normalisation des opérations est essentielle pour restaurer la confiance des clients et des partenaires.

6. Bases de Données Clients :

Activation du PRA *:* En cas d'incident touchant les bases de données clients, le PRA est déclenché pour minimiser l'impact. Par exemple, en cas de corruption de données après une cyberattaque, le PRA est activé pour rétablir rapidement les services.

Communication d'Urgence *:* La cellule de crise est notifiée immédiatement, et les parties prenantes sont informées de l'incident et de la mise en œuvre du PRA. Un exemple serait l'envoi de notifications automatisées aux responsables de la sécurité et aux équipes informatiques.

Mobilisation des Équipes *:* La cellule de crise, composée de spécialistes des bases de données et de la sécurité, coordonne la récupération. Les équipes ont des rôles prédéfinis, par exemple, un responsable de la restauration des données et un spécialiste des tests.

Récupération d'Urgence *:* Les sauvegardes régulières sont utilisées pour restaurer les bases de données. Des outils automatisés, tels que des scripts de restauration, peuvent accélérer le processus.

Vérification de l'Intégrité des Données *:* Une validation minutieuse est effectuée pour garantir que les données restaurées sont intègres. La comparaison avec des copies de sauvegarde précédentes permet de détecter toute altération.

Tests de Fonctionnement *:* Des tests sont exécutés pour s'assurer que les bases de données sont fonctionnelles. Par exemple, la simulation de transactions bancaires peut être effectuée pour vérifier la cohérence des données.

Activation Graduelle des Services : Les services dépendant des bases de données sont activés progressivement, en commençant par les plus critiques. Par exemple, les transactions en ligne peuvent être restaurées avant les fonctionnalités moins essentielles.

Surveillance Continue : Une surveillance constante est mise en place pour détecter tout problème émergent. Les paramètres de sécurité et de sauvegarde sont ajustés au besoin.

Communication de la Fin de Crise : Une fois la reprise d'activité réussie, une communication officielle est diffusée aux parties prenantes, indiquant que les services liés aux données clients sont entièrement disponibles.

7. Centre de Données de Secours

Détection de l'Incident *:* Les outils de surveillance détectent toute défaillance majeure au centre de données principal, par exemple, une panne de serveur critique.

Activation du Plan de Reprise : Dès la confirmation de l'incident, le PRA est déclenché pour assurer une transition rapide vers le centre de données de secours.

Communication d'Urgence *:* Les responsables de la cellule de crise et les parties prenantes sont notifiés immédiatement du basculement vers le site distant.

Mobilisation des Équipes *:* La cellule de crise active les équipes responsables du centre de données de secours, avec des spécialistes du réseau et de la virtualisation.

Basculement vers le Centre de Données de Secours *:* Les serveurs et systèmes de stockage redondants sont activés sur le site distant, et le trafic est dirigé vers le centre de données de secours.

Réplication des Données en Temps Réel *:* La réplication des données en temps réel est vérifiée pour garantir une continuité sans perte significative.

Tests de Fonctionnalité *:* Des tests opérationnels sont réalisés pour s'assurer que tous les systèmes du centre de données de secours fonctionnent correctement, y compris des simulations de charge.

Communication de la Reprise *:* Une annonce officielle est faite pour informer toutes les parties prenantes du succès du basculement vers le centre de données de secours, avec des détails sur la continuité des opérations depuis le site distant.

Conclusion

En conclusion, ce Plan de Reprise d'Activité de FINPLUS va permettre la continuité de son activité.