Avenue des Facultés
80000 Amiens

Plan de Reprise d'Activité(PRA)

SAE Semestre 5

Liam TARGET, Justin LARGILLIÈRE Malcolm WALTER, Lucas GONTHIER, Lorenzo VATRIN, Victor DA SILVA LOURENCO MARQUES.

BUT3 Informatique
Tous parcours

Année 2024 - 2025

Plan de Reprise d'Activité(PRA) v1.1

Plan de Reprise d'Activité (PRA) v1.1

Le Plan de Reprise d'Activité (PRA) est un document stratégique et opérationnel qui décrit les mesures à mettre en œuvre pour assurer la reprise des activités critiques d'une organisation après un incident majeur ou une crise. L'objectif principal du PRA est de minimiser les impacts sur l'entreprise et de rétablir les services essentiels dans un délai prédéfini et réagir en cas de panique.

Identification des risques
Comme mentionné dans le document *Analyse des risques*, nous allons traiter les principaux risques afin de disposer d'une solution en cas de problème.

Tout d'abord, il est impératif de **prévenir les utilisateurs avant de couper les services** du jeu pour éviter qu'ils ne soient surpris et pour préserver l'image du jeu.
Ensuite, il faut résoudre le problème tout en **restant transparent** si une communication est nécessaire. Enfin, une fois le problème résolu, il est important de vérifier le bon fonctionnement avant la mise en production en réalisant **une série de tests**.

Précautions :

- **Sauvegardes :**
  Disposer d'une sauvegarde fonctionnelle et sécurisée de l'ensemble du jeu, stockée localement, pour restaurer rapidement les données en cas de problème, ainsi qu'une sauvegarde externalisée hors du serveur principal.
- **Protection :**
  Installer des antivirus et des pare-feu pour protéger le système contre les virus, bien que cela ne garantisse pas une sécurité absolue.
  Maintenir le système à jour pour éviter les failles de sécurité.
  Prévoir une alimentation de secours et garantir la stabilité du réseau pour éviter les interruptions.
- **Forum :**
  Mettre en place un forum dédié aux joueurs pour signaler rapidement les bugs.
- **Environnement physique :**
  Contrôler la température des équipements, veiller à une bonne ventilation et éviter la surchauffe.

Mises en situation :

- Effectuer des simulations de conditions réelles, comme des catastrophes naturelles, des pertes d'électricité, des intrusions dans les locaux ou des attaques sur le système de sécurité.
- Le PRA est conçu pour gérer des problèmes graves ou non résolus par le Plan de Continuité d'Activité (PCA).

Marche à suivre pour certaines situation grave :

- Bug et instabilité des serveurs si le PCA ne suffit pas.
    - Prévenir et arrêter les services.
    - Identifier la source du problème.
    - Isoler le problèmes afin d'avoir l'étendu de celui-ci.
    - Résoudre le problème.
    - Vérifier la stabilité si cela ne convient pas de faire de même avec le serveur.
    - Vérifier si tout fonctionne.
    - Faire des tests du jeu.
    - Et relancer les services du jeu avec une patchNote.

- Catastrophe naturelle grosse fuite d'eau et d'électricité.
    - Pour éviter cela réfléchir à l'architecture du bâtiment et où on positionne le matériel sensible.
    - L'accès à la zone réservée.
    - Avoir un backup récent et fonctionnel.
    - Arrêter les matériels exposés si possibilité d'essayer de remettre les services en route via d'autres matériels.
    - Sinon essayer de remettre les services en route dans les meilleurs délais avec les moyens que nous avons donc prévoir une marge dans les imprévus.

- Intrusion dans nos locaux pour avoir des informations et demander une rançon soit un ransomware.
    - Avoir une zone sécurisée autour du bâtiment avec un contrôle d'accès et des droits spécifiques à chaque personne.
    - Avoir mis en place un système d'alerte pour une activité suspecte sur le réseau ou autre en mode super admin afin d'être prévenu rapidement et surtout automatiquement.
    - Impératif une fois identifier le problèmes et l'importance de celui-ci bloqué les accès sensible au données comme principalement au données bancaire et à la base de données.
    - Identification exacte du problème et isolation de celui-ci, prévenir les personnes en charge de la sécurité.
    - Afin de bloquer l'attaquant à l'endroit où il se trouve et pouvoir récupérer les données en cas de failles si l'attaquant arrive à s'introduire plus loin dans le système, prévenir les médias et être transparent sur les informations et les rassurer sans donner de promesse.
    - Minimiser au plus la fuite et perte de données, bloquer au mieux l'attaquant sur le réseau ou sur site afin de neutraliser la menace.
    - En cas de problème majeur, carte blanche et ne jamais payer la rançon.
    - Remise en service du jeu.