Réaliser un Plan de

Reprise d'Activité

Exemple Label Cyber-Safe

Avertissement : le présent document est fourni dans le cadre de la labellisation Cyber-Safe et nécessite d'être adapté à votre situation. Son usage ne garantit pas la conformité aux exigences du Label.

1 Introduction

Entre les pannes, les incendies, les inondations, les virus informatiques ou les épidémies, il existe de nombreux risques et incidents potentiels qui peuvent affecter la vie (et la survie) d'une entreprise.

De plus, avec des entreprises de plus en plus digitalisées, les conséquences de l'indisponibilité d'un système informatique et de la perte de données peuvent être désastreuses.

1.1 Définition

Le **PRA (Plan de Reprise d'Activité)** est une procédure de réponse aux événements inattendus pour assurer la continuité des opérations de l'organisation.

Le **RPO (Recovery Point Objective)** est le moment de la dernière sauvegarde complète effectuée. Plus il est éloigné de l'incident, plus vous êtes susceptible de perdre des données. C'est donc l'intervalle de sauvegarde des données que votre activité peut tolérer.

Le **RTO (Recovery Time Objective)** est le temps qu'il vous faudra pour rétablir vos systèmes et retrouver une activité normale après un incident majeur.

Plus vous pouvez minimiser l'impact potentiel d'un incident avec le bon Plan de Reprise d'Activité, plus tôt vous pourrez reprendre les opérations. Ces indicateurs (RPO/RTO) vous aident à définir vos besoins pour la sauvegarde de vos données et de votre infrastructure.

Pour approfondir le sujet, des liens vers des articles pour compléter cette procédure sont disponibles en appendice 1.

1.2 Périmètre

Chaque plan de reprise d'activité est unique puisqu'il s'adapte à votre entreprise et à ses spécificités. Il n'existe donc pas de modèle parfait : il s'agit d'anticiper tous les risques et d'obtenir une vision complète et exhaustive afin d'être en mesure de maîtriser les imprévus.

L'annexe 1 est un exemple de Plan de Reprise d'Activité pour Cyber-Safe. Ce document peut service d'exemple à votre démarche, mais vous devez avant tout réfléchir à votre situation en particulier.

L'annexe 2 « Checklist Résilience » est un document qui définit les contacts et les opérations à réaliser en cas d'interruption. Pour éviter toute redondance, il est conseillé de faire référence à cette liste de contrôle si certaines informations du PRA y sont déjà présentes.

1.3 Objectif

Pour faire face aux incertitudes conjoncturelles et aux risques (qu'ils soient économiques, financiers ou sanitaires), le plan de reprise d'activité repose sur l'anticipation.

Il consiste à adopter une posture agile pour s'adapter à un environnement changeant. Les enjeux sont importants et multiples pour la société :

- Garantir un niveau de chiffre d'affaires minimum en assurant la reprise d'une activité (même partielle) et assurer la survie de l'entreprise ;
- Satisfaire ses clients, même en période de crise, et les fidéliser pour améliorer son image ;
- Fidéliser les collaborateurs et fluidifier l'organisation interne de l'entreprise en garantissant la bonne gestion et le bon fonctionnement de la structure.

2 Rôles et responsabilités

Les responsabilités doivent être définies pour élaborer, maintenir à jour, tester et exécuter le PRA.

Une liste des acteurs du plan de reprise définit les rôles et les responsabilités et les informations nécessaires pour les contacter.

Un PRA doit pouvoir être activé en toute circonstance et à tout instant, il est donc essentiel que :

- L'accès au document soit garanti ;
- La liste contienne les coordonnées (privées si besoin) nécessaires pour garantir l'information des responsables ;

3 Ressources et activités critiques

Les systèmes sont de plus en plus complexes et interconnectés, il faut définir avec précision les priorités en fonction de la criticité des données et des activités.

Les indicateurs RTO, la durée maximale d'interruption que votre entreprise peut supporter avant que la situation ne devienne critique, et RPO, la durée de perte de données maximale admissible par l'entreprise doivent être évaluées pour chaque activité pour prioriser la restauration des outils et des données.

Pour ce faire, il est nécessaire de lister :

- Les outils nécessaires à la bonne marche de l'entreprise (ERP, CRM, Site web, interface clients, …) ;
- Les données, leur emplacement et leur criticité ;

4 Scénarios

Peu importe votre activité professionnelle, il est important de prendre conscience des risques et de les cartographier. Ensuite, vous serez en mesure de classifier les services et les actions indispensables au fonctionnement optimal de votre entreprise.

Pour définir les scénarios, les risques encourus par l'organisation doivent être évalués selon la liste non exhaustive de critères ci-dessous :

- Risque humain : une grève ou un accident d'un travailleur.
- Risque naturel : des intempéries ou une pandémie.
- Risque logistique : un délai de livraison ou la faillite d'un fournisseur.
- Risque technique : une panne électrique, d'internet ou de machines.
- Risque data security : un piratage, un vol de données ou un bug.
- Risque matériel : un vol ou un incendie.
- Risque client : un délai de paiement ou une créance douteuse.

Le PRA vous aide à vous adapter rapidement dans l'organisation du travail (activité partielle, télétravail, etc.) : Il garantit la résilience et la pérennité de votre entreprise face à ces scénarios. L'impact de la crise, quelle qu'elle soit, est ainsi atténué.

5 Procédure

Pour chaque type de données et/ou chaque type de serveur, étudiez les étapes à effectuer pour retourner à un mode de fonctionnement dégradé (minimum) et un mode fonctionnel complet.

5.1 Exemple : Reprise des fichiers administratifs en cas de rançongiciel

Temps nécessaire (à affiner avec les résultats des tests) : 6h pour dégradé et 15 h pour fonctionnel.

1. Déterminer la date d'infection : X
2. Créer un nouvel environnement totalement isolé de l'environnement de travail actuel et effectuer toutes les actions suivantes dans ce nouvel environnement.
3. Réactiver la VM vsphere à une date antérieure à X
4. Réactiver la VM veeam à une date antérieure à X
5. Démarrer veeam et restaurer l'AD à une date antérieure à X
6. Vérifier certains éléments sur l'AD
7. Restaurer la VM « fileserver » à une date antérieure à X
8. Restaurer les PC des employés suivants à une date antérieure à X
9. ======== MODE DEGRADE ATTEINT ==========
10. Restaurer les autres PC
11. Restaurer le monitoring
12. ….
13. ======== MODE FONCTIONNEL ATTEINT ========

5.2 Reprise des données ERP en cas de disques défectueux

Temps nécessaire (à affiner avec les résultats des tests) : 10h pour dégradé et 20h pour fonctionnel.

1. Détection du non-fonctionnement de l'ERP
2. Validation de la panne généralisée, information des collaborateurs
3. Intervention du prestataire IT pour diagnostic → Disques à remplacer
4. Remplacement du matériel (SLA)
5. Récupération du dernier support disponible
6. Vérification de l'intégrité de la base de données SQL
7. Intervention du prestataire ERP
8. Restauration du dernier backup ERP disponible
9. ======== MODE DEGRADE ATTEINT ==========
10. Reprise des activités finances
11. État des lieux des données perdues
12. Reprise manuelle des données manquantes
13. …
14. ======== MODE FONCTIONNEL ATTEINT ========

6 Priorités

Pour chaque élément au point 5, les mettre dans l'ordre de reprise selon les besoins de l'entreprise :

- 5.1 en dégradé (6h)
- 5.3 en dégradé (4h)
- 5.4 en fonctionnel (9h)
- 5.2 en dégradé (10h)
- ….

7 Tests et fréquence

Définissez à quelle fréquence la procédure doit être testée et quels sont les points à vérifier impérativement.

Pour réduire l'impact économique des tests, profitez des évènements habituels ou imposés pour définir et tester votre processus de reprise, par exemple :

- Un changement de serveur
- Le confinement lors de la crise COVID
- La mise à jour d'un logiciel ERP

La simulation d'un scénario, avec les acteurs du plan de reprise, permet d'échanger sur les responsabilités de chacun. Documentée par un PV ou un rapport, cette une approche est très efficace et plus simple à mettre en place que des tests complets.

8 Mots de passe et accès physiques

Lors des tests, vérifiez que vous arrivez à remettre en route les services les plus importants et que vous avez accès aux codes et mots de passe même sans l'information (papier dans le coffre, clé USB….).

De même les accès physiques doivent être possibles.

9 Annexes

9.1 Annexe I

Plan de reprise d'activité Cyber-Safe (version pdf, version docx)

9.2 Annexe II

Checklist Résilience

10 Appendices

10.1 Appendices 1

Wikipédia – Plan de reprise des activités

https://fr.wikipedia.org/wiki/Plan_de_reprise_d%27activité_(informatique)

https://fr.wikipedia.org/wiki/Plan_de_reprise_d%27activité

Wikipédia – Plan de continuité

https://fr.wikipedia.org/wiki/Plan_de_continuité_d%27activité_(informatique)

https://fr.wikipedia.org/wiki/Plan_de_continuité

Infomaniak News – Plan de reprise d'activité (PRA)

https://news.infomaniak.com/plan-de-reprise-activite/

Secrétariat général de la défense et de la sécurité nationale (FR)

Guide pour réaliser un plan de continuité