PRA - Plan de reprise d'activité (informatique)

Définition :

Un plan de reprise d'activité (PRA) est un ensemble de procédures (techniques, organisationnelles, sécurité) qui permet à une entreprise de prévoir par anticipation, les mécanismes pour reconstruire et remettre en route un système d'information en cas de sinistre important ou d'incident critique.

En cas de sinistre, Le PRA permet de reconstruire les serveurs en leur affectant les données répliquées et ainsi de redémarrer les applications sous quelques minutes ou quelques heures, suivant les solutions retenues. Il existe plusieurs niveaux de capacité de reprise, et le choix doit dépendre des besoins exprimés par l'entreprise.

Les entreprises actuelles dépendant de plus en plus de leur informatique, elles ne peuvent donc plus se permettre de ne pas avoir une solution face à un incident informatique, qui pourrait leur être fatal ou entraîner une paralysie de l'activité professionnelle. Le plan de reprise d'activité a alors un rôle majeur pour assurer le redémarrage structuré des systèmes d'information.

Le PRA est comme une assurance, tant qu'il n'y a pas d'accident, on ne voit pas l'intérêt.

Voici quelques chiffres clés pour comprendre la mise en place du plan :

- 76 % des entreprises déclarent la perte de données informatiques sur les deux dernières années.
- 82 % des PME non préparées à un sinistre ne survivent pas à un important crash informatique.

Le PRA décrit hiérarchiquement l'ensemble des mesures qui doivent être mises en place lors de la survenue d'un sinistre ou d'un incident majeur ayant entraîné une interruption de l'activité. Le PRA définit les architectures, les moyens et les procédures nécessaires à mettre en œuvre pour assurer la protection des applications qu'il couvre.

Objectifs et détermination des besoins

L'objectif d'un PRA est de minimiser les temps morts et la perte de données lors d'un sinistre. Le but premier est de protéger l'organisation dans l'éventualité qu'une partie ou la totalité de ses opérations et services informatiques soit inutilisables. Le PRA minimise la perturbation des opérations et assure un certain niveau de stabilité organisationnelle et le rétablissement de ces données sera prioritaire après le sinistre.

Un système de reprise peut être coûteux à mettre en place et à maintenir au sein de l'organisation. Il est donc essentiel de définir convenablement les attentes du système de reprise. Les besoins de l'organisation sont mesurés à l'aide de deux concepts :

- **Durée maximale d'interruption admissible (Recovery Time Objective : RTO3) :** C'est le délai de rétablissement d'un processus, à la suite d'un incident majeur, pour éviter des conséquences importantes associées à une rupture de la continuité d'activité. Il définit le temps alloué pour faire le basculement vers le nouveau système.
- **Perte de données maximale admissible (Recovery Point Objective : RPO)** : Le RPO commence à s'exprimer à l'instant où l'incident majeur arrive et peut être exprimé en secondes, minutes, heures ou jours. Il s'agit donc de la quantité maximale acceptable de perte de données. C'est la durée des fichiers ou des données dans le stockage de secours exigé par l'organisation pour reprendre des opérations normales après l'incident. Ce critère définit l'état dans lequel doit se trouver le nouveau système après basculement.

Les 3 types de sinistres informatiques et leurs conséquences

Il y a 3 grandes catégories de sinistres pouvant causer la perte totale ou partielle de votre système d'information. Certains d'entre eux impliquent une perte de données ne pouvant être récupérées que par une sauvegarde externalisée.

Catastrophes naturelles :

Le terme « catastrophe naturelle » évoque un événement soudain qui expose les habitants d'une ville et leurs infrastructures à de lourds dégâts. Elles peuvent être de différentes formes : tempêtes, inondations, cyclones, tremblements de terre, sécheresses ou encore grandes chaleurs.

Les conséquences de ces sinistres peuvent être :

- Perte d'un immeuble ou d'un local : elle peut être causé par une coupure électrique, un feu, une tempête, un cyclone, un tsunami ou bien une inondation. Elle peut entraîner la perte d'un centre de données, qui est une conséquence dramatique pour l'entreprise.
- Désastre à grande échelle (ville, région, pays) : Ce sont des sinistres avec une très faible probabilité mais qui nécessite d'être évoqué de par leurs conséquences. Les cyclones ou les tremblements de terre peuvent interrompre l'ensemble des activités informatiques d'une zone géographique.

Il faut prendre en considération les risques naturelles qui concernent la ou les régions d'implantation. Si l'entreprise a son siège dans une région A mais qu'elle a des antennes dans plusieurs autres régions, il faut prendre en compte les risques naturels de toutes les zones d'implantation.
Dans ce cas, plusieurs PRA peuvent être mis en place.

Sinistres sur les installations :

Ce sont des sinistres, d'origines variées qui peuvent impacter les installations. Ils peuvent être intentionnels (vol, attentat, sabotage) ou non intentionnel (incendie, dégâts des eaux).
Un sinistre dans une salle serveurs peut mettre à plat toute la société. C'est pour cela qu'il faut prévoir des solutions, même en mode dégradé, pour faire repartir les services.

Cybercriminalité et malveillance :
Les attaques sont variées : virus, cyberattaque, piratage informatique, logiciels malveillants. Le sabotage d'installations industrielles est une autre alternative. Dans certains cas, ces attaques peuvent paralyser l'activité professionnelle, ou encore entraîner une perte de données conséquente

Les conséquences de ces incidents peuvent être diverses, notamment entraîner une coupure des communications, ainsi les systèmes reliés ne peuvent plus échanger de données et on assiste alors à une perte d'informations, une saturation, une panique système ou un arrêt des activités. Une entreprise peut aussi subir la perte des applications installées.

C'est pour cela qu'il faut mettre en œuvre la stratégie de protection la plus complète possible et former les utilisateurs sur les bonnes pratiques et les pièges à éviter.

Autres causes :
Les autres causes de pertes de services ou de données sont dues à des facteurs internes aux organisations ou à leur partenaires proches :

- pertes de services essentiels (électricité, communications)
- erreurs de manipulation (saisies, erreurs de programmation, de configuration de l'infrastructure)
- vols de matériel
- pannes matérielles

Ces causes de panne n'est pas à sous-estimer.
En effet, une rupture de fibre ou une panne électrique sont des risques plus que probables. Dans le cadre d'une gestion full cloud, la rupture de fibre condamne l'accès aux données.
Dans le cadre d'une panne électrique prolongée, les ordinateurs seront coupés et les serveurs (même avec onduleur) s'arrêteront.

Types de mesures

Le Plan de Reprise d'Activité idéal n'existe pas. Il n'existe pas un modèle template qui marche pour toutes les organisations.
En effet, suivant la typologie de métier, suivant la taille de l'entité et son niveau de maturité IT, les contraintes sont radicalement différentes.
Le PRA doit être fait sur mesure tout en suivant une méthodologie commune.

Il y a trois stratégies de base qui figurent dans tous les plans de reprise :

- **Mesures préventives**

Les mesures préventives vont tenter de prévoir l'occurrence d'incidents. Ces mesures cherchent à identifier et réduire les risques. Elles sont créées pour atténuer ou prévenir la fréquence des sinistres ou des désastres.
Les mesures préventives peuvent inclure:

- des sauvegardes de données très régulières.
- de prévoir un plan de reprise d'activité précis et testé régulièrement.
- d'installer des générateurs et de conduire des inspections du quotidien.

- **Mesures détectives**

Les mesures détectives sont prises pour détecter la présence d'éléments indésirables dans le système d'information de l'organisation. Leur but est de découvrir de nouvelles menaces potentielles. Elles peuvent mettre en avant des événements non-désirés. Ainsi, l'organisation doit mettre en œuvre des mesures :

- Installer des logiciels anti-virus à jour et les renouveler
- Mettre en place des sessions de formation des salariés pour diminuer le phénomène de shadow IT
- Installer des logiciels de contrôle/surveillance des serveurs et des réseaux

- **Mesures correctives**

Les mesures correctives visent à restaurer un système après un événement indésirable (sinistre, désastre). Ces mesures portent sur la fixation ou la restauration des systèmes d'information après l'incident.

Elles peuvent inclure la tenue de documents critiques dans le plan de reprise d'activité ou la souscription à des polices d'assurance adaptées à l'organisation. Dans toutes les organisations, un Plan de Reprise d'Activité doit permettre de répondre aux interrogations suivantes :

- Quel est son objectif et son but ?
- Quelles sont les personnes ou équipes responsables si des perturbations surviennent ?
- Que feront ces personnes quand l'incident surviendra ?

Méthodologie

Un Plan de reprise d'activité se déroule en 9 étapes. Suivant la taille de la société et le temps mobilisable pour le PRA, certaines étapes seront plus ou moins poussées.

Étape 1 : Obtenir l'engagement de la direction

Pour qu'un plan de reprise d'activité soit réussi, la responsabilité centrale du plan doit dépendre de la direction.
Celle-ci est responsable de coordonner le plan de reprise d'activité et d'assurer son efficacité dans l'organisation. Elle est aussi chargée de répartir le temps et les ressources nécessaires, à la fois financières et relatives à l'effort que tout le personnel concerné doit fournir.

Étape 2 : L'établissement d'un comité de planification

La direction générale de l'entreprise nomme un comité de planification pour surveiller le développement et la mise en œuvre du plan. Il inclut des représentants de tous les services fonctionnels de l'organisation et il compte aussi habituellement le directeur du service informatique. Le comité définit aussi la portée du plan.

Étape 3 : Procéder à une évaluation des risques

Le comité de planification prépare une analyse de risque et une analyse d'impact sur l'activité qui inclut une gamme d'incidents possibles, y compris des menaces naturelles, technologiques et humaines.
Chaque service de l'organisation est analysé pour déterminer la conséquence potentielle et l'impact associé à plusieurs scénarios de désastre. Le processus d'évaluation des risques évalue aussi la sécurité des documents importants.

Traditionnellement, le feu a constitué la menace la plus importante pour une organisation. Cependant on devrait aussi considérer la destruction humaine intentionnelle. L'entreprise doit prévoir un plan minutieux présentant comme situation « le pire cas », c'est-à-dire la destruction du bâtiment principal. Il est important d'évaluer les impacts et les conséquences résultant de la perte d'informations et des services.

Étape 4 : Établir des priorités pour traiter l'incident
À ce point, les besoins critiques de chaque département de l'organisation sont évalués pour établir un ordre de priorités. L'établissement de priorités est important car aucune organisation ne possède des ressources infinies.

Une méthode utilisée pour déterminer les besoins critiques d'un département est de documenter toutes les fonctions exécutées par chaque département. Une fois que les fonctions principales ont été identifiées, les opérations et les processus sont alors classés par ordre de priorité : élément essentiel, important et non essentiel.

Étape 5 : Déterminer les stratégies de récupération
Pendant cette phase, des recherches sur les alternatives les plus pratiques de traitement en cas de désastre sont faites et évaluées.
On considère tous les aspects de l'organisation, y compris:

- les installations physiques
- le matériel informatique et les logiciels
- les lignes de communication
- les fichiers de données et les bases de données
- les services clients
- les opérations d'utilisateurs
- les systèmes d'information de gestion
- la structure
- les systèmes d'utilisateur final
- les autres traitements

Étape 6 : Organiser et documenter un plan écrit
Ensuite, un plan est préparé pour guider le développement des procédures détaillées. La direction générale passe en revue et approuve le plan proposé. Le plan est utilisé pour la table des matières après la révision finale.
D'autres avantages de cette approche sont :

- Il aide à organiser les procédures détaillées.
- Il identifie tous les étapes majeures avant que le processus d'écriture réel ne commence.
- Il identifie des procédures superflues qui doivent être écrites seulement une fois.
- Il fournit une feuille de route pour développer les procédures.

On le considère souvent comme la meilleure pratique pour développer un format standard du plan de reprise d'activité.

L'équipe de direction est particulièrement importante car elle coordonne le processus de reprise. L'équipe évalue l'incident, active le plan de reprise et contacte les directeurs d'équipe. Elle surveille aussi les documents et contrôle le processus de reprise.

Étape 7 : Le développement de critères et procédures d'essai
Les plans doivent être testés et évalués sur une base régulière. Il faut une documentation avec les procédures pour tester le plan.
Les tests fourniront à l'organisation l'assurance que toutes les étapes nécessaires sont incluses dans le plan.
Il existe aussi d'autres raisons de tester le plan de reprise d'activité :

- Déterminer la faisabilité et la compatibilité des installations de secours et des procédures.
- Identifier les zones du plan qui doivent être modifiées.
- Former les managers et les membres des équipes.
- Montrer la capacité de l'organisation à reprendre l'activité.
- Fournir une motivation pour maintenir et mettre à jour le PRA.

Étape 8 : Tester le plan
Après que le test de procédures ait été effectué, "une répétition" initiale du plan est exécutée. Le test fournira des informations supplémentaires quant aux nouvelles étapes qui devront être incluses, aux changements des procédures qui ne sont pas efficaces et aux autres rajustements appropriés. Ceux-ci ne peuvent pas devenir évidents à moins qu'un réel test d'essai ne soit exécuté. Le plan est par la suite mis à jour pour corriger n'importe quel problème identifié pendant le test.

Les différents types de tests sont : tests de liste de contrôle, tests de simulation, tests parallèles et interruption complète.

Étape 9 : Obtention de l'approbation du plan
Une fois que le PRA a été écrit et testé, le plan est alors soumis à la direction pour approbation. Celle-ci doit donner son accord pour la mise en place d'un PRA.

Comme vous l'avez compris, le PRA peut s'inscrire dans une stratégie globale car il intègre des éléments de sécurité informatique, de gestion de sauvegarde…
Lorsque l'on construit un SI, il faut avoir en tête un PRA afin de penser la meilleure architecture matériel et logiciel pour ce prémunir des risques et, le cas échéant, répondre à ces derniers.

Source originale : https://fr.wikipedia.org/wiki/Plan_de_reprise_d%27activit%C3%A9_(informatique)

Si l'on fait un PRA dédié au domaine informatique, les étapes peuvent être légèrement différentes. On peut décomposer en 11 étapes préalables et essentielles :

1. **Faire un audit de tous les risques de pannes possibles** sur le système d'information et identifier les causes probables : panne matérielle, panne logicielle, cyberattaque, coupures électriques, incendie, catastrophe naturelle, erreur humaine, etc.
2. **Détecter et évaluer chaque risque pour identifier les applications métiers qui ne pourront pas fonctionner en mode dégradé**. Il faut donc bien appréhender et mesurer la tolérance aux pannes de l'ensemble du système d'information.
3. **Définir la criticité des environnements applicatifs et les besoins de sauvegarde et réplication ainsi que de restauration** qui devront s'appliquer. Devront être définis ici le RTO (Recovery Time Objective) et le RPO (Recovery Point Ojective).

4. **Prévoir des sauvegardes automatiques** à une fréquence correspondant au besoin de l'organisation.
5. **Faire du « Crisis Management »**, c'est-à-dire attribuer des rôles et des tâches à des personnes précises qui auront la responsabilité d'intervenir le moment venu. En d'autres termes, il faut organiser et mobiliser ses équipes pour agir efficacement lors du sinistre.
6. **Définir des priorités et un coût de reprise d'activité** : évaluer des seuils d'indisponibilité des services et les prioriser afin de définir le coût de remise en service de l'infrastructure.
7. **Définir le choix de l'équipement de sauvegarde et de reprise d'activité ainsi que le budget** qui y sera consacré.
8. **Tester régulièrement le plan de reprise d'activité** : bien que le coût d'un test de PRA informatique soit conséquent, il est impératif d'évaluer régulièrement sa fiabilité à minima deux fois par an.
9. **Faire évoluer le plan de reprise d'activité en fonction des changements apportés au système d'information** : le SI d'une entreprise évoluant constamment, il est essentiel de répercuter ces changements sur le PRA informatique construit initialement afin d'en assurer sa fiabilité.
10. **Documenter précisément le PRA**: il faut encourager le retour d'expériences des acteurs garants de la fiabilité du PRA en le documentant précisément. Le partage de la connaissance du SI va directement impacter les performances d'un PRA informatique. Ainsi, les phases de tests ou les remontées d'échecs doivent être systématiquement documentées, ce qui est généralement peu souvent le cas.
11. **Prendre en compte les contraintes réglementaires** auxquels certaines typologies d'organisations doivent se conformer dans l'exécution de leurs activités.

Source originale : https://www.cyres.fr/blog/plan-de-reprise-activite-11-etapes-essentielles/