Sécurité - PCA, PRA et DRP

Difficulté : Novice

Notions : PCA, PRA, stratégies de survie.

I. Introduction

Dans certains secteurs d'activité (médicaux, bancaires, défense, etc...), une simple coupure de service peut avoir des conséquences graves. Et même pour des secteurs moins sous tensions, cela peut avoir des conséquences financières directes.

(*exemple : dans le secteur de l'agroalimentaire ou du médicament, le moindre doute sur la gestion de la chaîne du froid peut signifier une destruction de la production*).

Afin d'assurer la pérennité du service informatique de l'organisation, Il est nécessaire d'anticiper ces problèmes et de prévoir des solutions.

La sauvegarde, bien que répondant en partie à ces points, doit être intégrée dans des plans plus larges.

On distingue 2 scenarii principaux dans la gestion de crise :

- **La continuité d'activité** : un problème survient (matériel par exemple), comment l'on s'assure de poursuivre l'activité avec pas ou peu de rupture de service.

- **La reprise d'activité** : un problème a eu pour conséquence l'arrêt de tout ou partie de l'activité de l'entreprise et il faut repartir.

II. Notions fondamentales

Lors de l'établissement de ces plans, un certain nombres de points sont à retenir :

La résilience : Il s'agit de la capacité de l'organisation à résister à un incident qui pourrait entraîner une rupture d'activité.

La disponibilité (Availability) : Il s'agit du temps de disponibilité du service. Certaines entreprises (opérateurs télécom, datacenters, doivent assurer une disponibilité et garantissent souvent celle-ci. Elle est défini en pourcentage de disponibilité sur 1 année (par exemple, un datacenter peut assurer une disponibilité de 98% ce qui signifie que sur une année de 365 jours, ce qui signifie que l'entreprise garantit que sur une année, il n'y aura jamais plus de 7jours d'indisponibilité cumulés, consécutifs ou non)

La récupération (recovery) : En cas d'incident, la capacité à repartir en production et de récupérer les données de l'entreprise.

La continuité (continuity) : La continuité de l'activité ou du service. La capacité à assurer la fourniture de celui-ci même en cas d'incident.

Ces points seront étudiés, définis et des solutions seront apportées pour atteindre les objectifs fixés.

III. Le PCA

3.1 But du PCA

Le PCA (**P**lan de **C**ontinuité d'**A**ctivité) est un ensemble de mesures prises pour s'assurer de la continuité des services essentiels et minimiser au maximum l'impact d'un dysfonctionnement ou d'un incident.

Cela se réalise à tous les niveaux de votre infrastructure.

Sur la couche matérielle par exemple, on trouve sur les serveurs 2 alimentations électriques indépendantes, deux processeurs, des contrôleurs RAID pour s'assurer que le serveur continue de fonctionner même en cas de défaillance matérielle.

Sur la couche réseau, un certain nombres de protocoles permettent une redondance des équipements (STP, RSTP, LACP sur les switch, HSRP, VRRP pour les routeurs). Cela permet de palier à la perte d'un équipement réseau ou la défaillance d'une interface.

Ou sur des couches plus haute, des mises en place de redondances de services (2 AD, 2 filers, hébergés sur des nodes différents).

Ainsi, grâce à la combinaison de toutes ces mesures, on assure un certain niveau de fiabilité et de continuité.

Le service peut continuer à fonctionner malgré un problème ou une situation de crise.

3.2 Méthodologie de mise en place

Basés sur une étude de risque (voir Sécurité - Analyse de risque (méthode Ebios)), l'on devra suivre le schéma de réflexion suivant :

1. Définir les points critiques à protéger. Les "fonctions vitales" de l'entreprise.
2. Etablir les scénarii qui entraineraient une rupture de service.
3. Proposer, pour chaque point, une solution adaptée pour y répondre
4. Définir les responsabilité et rôles dans la mise en œuvre et le suivi du PCA
5. Rédiger les process
6. Effectuer des test réguliers après mise en œuvre

Exemple : Une société agroalimentaire fabrique des tourtes à la viande, elle doit gérer des stocks de matières première et s'assurer du bon fonctionnement de la chaîne du froid. Dans ce cadre là,

elle a déployé une solution de supervision à travers un réseau de capteurs dans les frigo et les entrepôts, ainsi que des outils de traçabilité des stocks et du temps passé hors stockage.

Scénario 1 : un dysfonctionnement suite à une coupure de courant, à mis HS certains équipements réseaux. Cela empêcherai la lecture des capteurs, ce qui ferait que l'entreprise n'aurai plus de moyen de remonter les données, ni d'être avertie en cas de problème. La chaîne de production devrait être bloquée et l'ensemble des stocks vérifiés. En cas de doute, cela entrainerai une destruction des stocks. Donc pertes financières directes, délai d'approvisionnement pour renouveler le stock.

> *Solutions proposées : Adopter une topologie réseau full mesh, redonder les équipements critiques, mettre en place des onduleurs afin de palier aux futures coupures électriques. Cela permettra en cas de rupture d'un chemin réseau, de panne d'un équipement ou d'une coupure électrique, de continuer à assurer la traçabilité des informations.*

Scénario 2 : Les données des capteurs sont enregistrés dans une base de donnée, suite à une corruption système due à un disque plein, celle-ci est mise à l'arrêt. De fait, les données ne sont plus enregistrées et les conséquences seraient les mêmes que dans le scénario d'avant.

> *Solutions proposées : Séparer les données de la bases du système en les mettant sur des disques séparés. Cela réduira les pertes et empêchera une production future. Superviser l'espace disque afin de pouvoir entreprendre des actions préventives. Redonder le serveur de base de donnée sur un second nœud de la ferme de serveurs. Si l'un des serveurs tombe en panne, le second prendra le relai, assurant la continuité de l'enregistrement des mesures.*

3.3 Bonne pratiques

Tout comme pour la sauvegarde, Il faut s'assurer que le PCA sera fonctionnel le jour où celui-ci doit servir.

Il faut donc tester régulièrement celui-ci, valider les process et/ou les faire évoluer.

Il faut également mettre en place un plan de communication interne, s'assurer que les personnes qui sont responsables de ces points sont informées.

Vérifier la conformité avec les standards ISO 22301 et 27001.

IV. Le PRA

4.1 But du PRA

Le PRA (**P**lan de **R**eprise d'**A**ctivité) est un ensemble de mesures visant à reprendre le plus rapidement possible une activité normale suite à un incident majeur ayant entrainé une rupture de l'activité.

Cela peut consister à disposer d'équipements de rechange, d'un site où les machines virtuelles sont répliquées, de locaux déportés.

Contrairement au PCA où le but est d'éviter la rupture, le PRA part du principe que cette rupture est survenue et qu'il faut donc faire reprendre l'activité.

4.2 Méthodologie de mise en place

Basés sur une étude de risque (voir Sécurité - Analyse de risque (méthode Ebios)), l'on devra suivre le schéma de réflexion suivant :

1. Définir les points critiques à rétablir en priorité. Les "fonctions vitales" de l'entreprise.
2. Etablir les scénarii qui entraineraient une rupture de service.
3. Proposer, pour chaque point, une solution adaptée pour y répondre
4. Définir les responsabilité et rôles dans la mise en œuvre et le suivi du PRA
5. Rédiger les process
6. Effectuer des test réguliers après mise en œuvre

Exemple : Une société de gestion d'autoroute dispose d'un centre de contrôle assurant la surveillance du réseau autoroutier et la coordination des interventions de maintenance et le

contact avec les services d'urgences.

Scénario 1 : Suite à un accident, un incendie s'est déclenché à côté du site du PC. L'incendie se propage jusqu'aux locaux du PC. Une évacuation est demandée.

> *Solutions proposées : Construire un second bâtiment de PC de l'autre côté du réseau autoroutier géré et y disposer tout l'équipement nécessaire au fonctionnement du PC. Répliquer l'ensemble des serveurs et baies de stockages sur le site de secours. La procédure de démarrage est lancée au moment de l'ordre d'évacuation. Quand le personnel investit le site de secours, les équipements sont démarrés, fonctionnels, les données sont accessibles. La reprise de l'activité normale peut reprendre.*

Scénario 2: Suite à une compromission des serveurs, un cryptolocker à infecté le réseau informatique et a chiffré les données. Le système est hors service.

> *Solutions proposées : Mettre ne place un système de sauvegarde hors ligne éprouvé et testé régulièrement. Disposer de réseaux isolés permettant une reprise de l'activité sans risquer une nouvelle compromission. Mettre en place un plan, au moins partiellement automatisé, de reconstruction des services et de récupération de la donnée.*

4.3 Bonne pratiques

Tout comme pour la sauvegarde et le PCA, Il faut s'assurer que le PRA sera fonctionnel le jour où celui-ci doit servir.

Il faut donc tester régulièrement celui-ci, valider les process et/ou les faire évoluer.

Il faut également mettre en place un plan de communication interne, s'assurer que les personnes qui sont responsables de ces points sont informées.

Les outils principaux du PRA à mettre en place et valider sont :

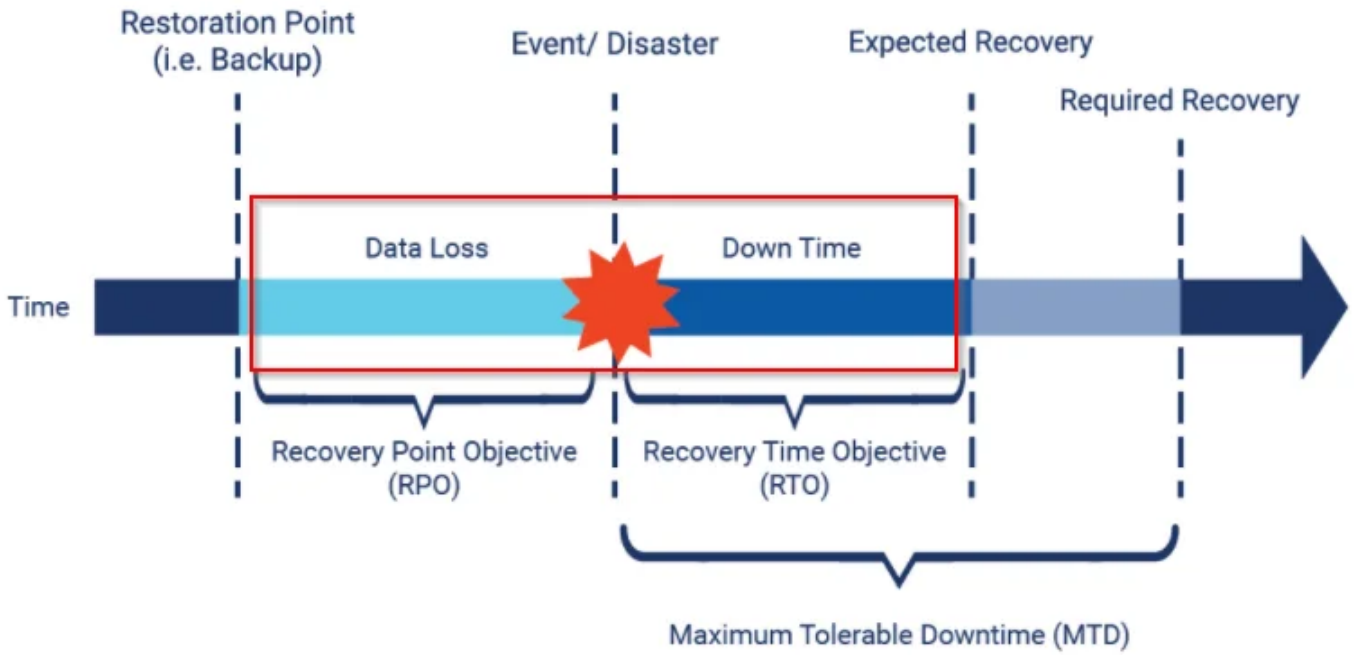
- Sauvegardes
- DRP (Disaster Recovery Procedure)

>

> **Info** : Là où auparavant, les efforts du PRA se concentraient sur la réplication des machines, une sauvegarde complète des VM et de leur contenu, l'évolution des menaces en terme de cybersécurité fait qu'aujourd'hui on aura plus tendance à partir du principe que les réplicas et les sauvegardes du système sont potentiellement corrompu(e)s.

> **Astuce** : Découlant du constat ci-dessus, la méthode aujourd'hui privilégiée est une reconstruction complète du système et de l'infrastructure. Suivi d'une restauration des données conservées à part. Une bonne partie de la reconstruction est partiellement, voire entièrement automatisée.

Définir correctement le RTO et le RPO.



Si il y a une possibilité lors de la conception de choisir le placement du site de PRA.

Table des distances - risques naturels et anthropiques

Dans la conception d'un centre de données, le choix du site est l'une des étapes les plus cruciales et constitue la toute première étape. Nous nous concentrons principalement sur deux sous-domaines : les risques naturels et anthropiques.

Objet fabriqué par l'homme	Distance minimale (KM)
Stations-service/carburant	1.6

Lignes de transmission à haute tension	1.6
Les fugues des aéroports	1.6
Petits lacs et zones de débordement	1.6
Chemins de fer	1.6
Grand complexe de magasins	1.6
Tours de stockage d'eau	1.6
Canaux	3.2
Ports et ports	3.2
Lacs et barrages	3.2
Carrières	3.2
Stations radar	5
Laboratoires de recherche	5
Stations de radio/télévision	5
Ambassades	5
Aéroports	8
Usines chimiques et électriques	8
Stations et installations militaires	13
centrales nucléaires	80

Distance entre deux sites

Distance	Buts et considérations	Sources
1-5 km	Protection contre les menaces locales (feu, explosion, crash aérien, etc...)	Internal safety design
50-160 km	Compromis entre un temps de latence correct et une distance optimale prévenant les risques régionaux.	,
320+km	Assure une dépendance régionale (Grille énergétiques différentes, régions sismiques différentes, etc...) mais peut probablement introduire de la latence.	

V. Conclusion

Pour des stratégies efficaces, il faudra mettre en place à la fois un PCA et un PRA. Car les deux n'adressent pas les mêmes problèmes.

Voici un cours comparatif entre les deux :

Fonction	pca	pra
timing	Pendant et immédiatement après incident	Après incident, en réponse.
focus	Continuité des opérations vitales	Restauration de l'ensemble des opérations.
nature	Proactive	Réactive
exemple	Garder un portail client accessible.	Restaurer un service après une cyberattaque.

Et évidement, le tout devra être documenté, testé et amélioré.

Complétés avec des études de nouveaux scenarii.

Revision #2
Created 2026-07-17 20:41:30 UTC by Olivier
Updated 2026-07-17 20:43:23 UTC by Olivier