13/11/2023

PCA – PRA

Membres du groupe

* + Chef de projet : Hugo la place
  + Florian Brochot
  + Hana Berrached

Contexte du projet

La société ANIMUS, un leader dans les télécommunications multi-niveaux, est en expansion constante, répondant à une demande croissante sur le marché. Sa stratégie d'expansion comprend l'acquisition d'entreprises, notamment des PME. Récemment, Animus a acquis Abstergo, spécialisée dans les protocoles Bluetooth de nouvelle génération.

Chaque acquisition par Animus implique l'intégration du système d'information de l'entreprise acquise. Ce processus standardisé comprend :

* L'annexion de l'environnement système de l'entreprise acquise à celui d'Animus.
* La configuration des paramètres de sécurité selon les normes d'Animus.
* Les vérifications finales d’optimisation et la mise à jour des procédures.

Dans le cadre de l'évaluation des risques pour le Plan de Reprise d'Activité (PRA) et le Plan de Continuité d'Activité (PCA) nous avons effectué :



PRA / PCA

A. Evaluation des risques

* **Physiques** :

La société possède des serveurs physiques donc nous devons prendre en compte les risques des catastrophes naturelles ou les risques causés par des humains tels que les attentats, vols, masse électrique, mauvais branchement.

* **Informatiques :**

La société est une société informatique et il faudra en compte les menaces informatiques dues aux cybers attaques, virus, panne des routeurs, internet, mauvaise configuration…

B. Stratégie de sauvegarde et de récupération

1. **Application de la règle 3-2-1 :**

Cette stratégie consiste à réaliser trois copies des données qui doivent être stockées sur deux supports différents avec une copie située à l’extérieur de l’entreprise



1. **Trois données de nos données :**

Cela signifie que nous avons deux copies et une original, ce qui va nous permettre de diminuer les chances de perdre des données si l’un des équipements de stockage rencontre un problème.

1. **Deux supports de stockage différents :**

Ces trois copies de nos données pourraient être stockées sur un seul équipement. Cependant, si notre équipement rencontre un problème on perdra toutes nos données, pour diminuer la probabilité de perdre les données, il est préférable de stocker sur deux supports en privilégiant différents types de stockage ( disques durs internes et tout type de support amovibles comme le cloud ou des disques durs externes..)

1. **Une copie hors site**

Si l’entreprise subis une catastrophe naturelle telle qu’une inondation ou un incendie et que toutes les données ont été stockées dans le même emplacement, toutes les copies seraient détruites, rendant ainsi le Plan de Reprise d’Activité complètement inutile.

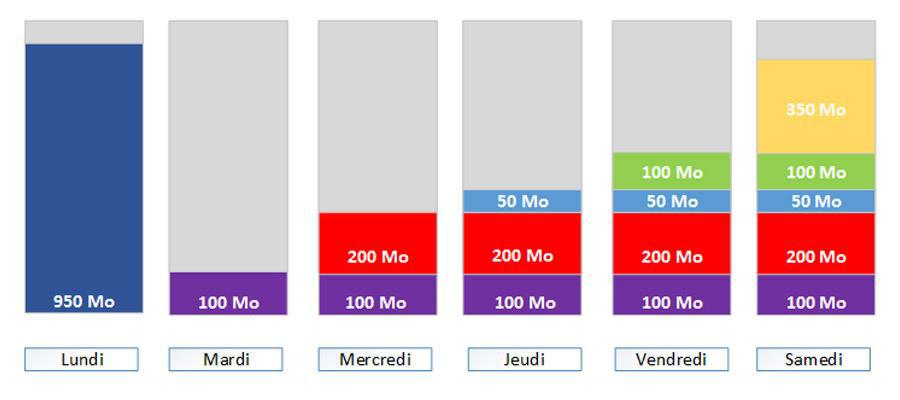
Les systèmes cloud permettent de mettre en œuvre rapidement et simplement l’externalisation de la sauvegarde.



C. Méthode de sauvegarde

Les systèmes de sauvegarde permettent d’appliquer différentes méthodes, voici les plus courantes :

* Sauvegarde complète : Cette Méthode permet de copier toutes les données indépendamment des modifications depuis la précédente sauvegarde.
* Sauvegarde différentielle : Cette méthode permet de conserver toutes les modifications depuis la sauvegarde complète, quel que soit le type de modification.
* Incrémentale : Cette méthode permet de conserver toutes les modifications depuis la précédente sauvegarde. Ce qui signifie que la préservation des données est effectuée depuis les sauvegardes incrémentale précédentes.



La sauvegarde incrémentielle est souvent considérée comme la méthode la plus appropriée pour de nombreux environnements informatiques, en raison de ses avantages en termes d'efficacité et d'économie de ressources. Contrairement à la sauvegarde complète, qui copie l'intégralité des données à chaque fois, la sauvegarde incrémentielle ne sauvegarde que les fichiers qui ont été créés ou modifiés depuis la dernière sauvegarde, qu'elle soit complète ou incrémentielle.

Cette approche est particulièrement pertinente dans les contextes où les modifications des données ne sont ni fréquentes ni massives. En conséquence, elle permet une économie significative de temps et d'espace de stockage. Par exemple, dans un cycle hebdomadaire de sauvegarde, une sauvegarde complète pourrait être effectuée au début de la semaine. Dans les jours suivants, seules les modifications ou les nouveaux fichiers depuis cette sauvegarde complète seraient sauvegardés. Cette méthode réduit la charge sur les systèmes de stockage et améliore l'efficacité du processus de sauvegarde, tout en assurant que les données les plus récentes sont toujours sauvegardées.

En conclusion, la sauvegarde incrémentielle est souvent privilégiée pour sa capacité à fournir une protection des données efficace et actualisée sans engendrer les coûts en temps et en espace associés aux sauvegardes complètes répétées.



D. Procédure de reprise d’activité :

1. **Identification et Analyse des Risques :**
   * Dresser une liste exhaustive des risques potentiels (catastrophes naturelles, cyberattaques, défaillances techniques, etc.).
   * Évaluer les conséquences potentielles de chaque risque sur l'activité de l'entreprise, y compris les impacts sur les opérations, la réputation et les finances.
2. **Évaluation de la Criticité des Systèmes et des Données :**
   * Examiner et classer les applications et les données selon leur importance pour l'entreprise.
   * Déterminer quelles données et systèmes sont essentiels pour maintenir les opérations minimales lors d'une interruption.
3. **Définition des Objectifs de Temps de Reprise (RTO) et de Point d'Objectif de Reprise (RPO) :**
   * Établir la durée maximale acceptable d’interruption de service (RTO) pour chaque composant critique du système.
   * Fixer le RPO, ou la quantité maximale de données acceptables à perdre en cas de crash.
4. **Mise en Place de Solutions de Sauvegarde et de Restauration :**
   * Sélectionner et installer les solutions de sauvegarde et de restauration adaptées aux besoins identifiés.
   * Assurer que ces solutions sont capables de répondre aux RTO et RPO définis.
5. **Rédaction des Procédures de PRA/PCA :**
   * Documenter en détail les étapes à suivre en cas d'interruption.
   * Définir clairement les rôles et responsabilités de chaque membre de l'équipe en cas de crise.
   * Préciser les procédures de communication interne et externe.
6. **Planification Budgétaire et Priorisation des Ressources :**
   * Allouer un budget spécifique pour les activités de reprise d'activité.
   * Prioriser les investissements en fonction de la criticité des systèmes et des données.
7. **Tests et Mises à Jour Réguliers du Plan :**
   * Organiser des tests réguliers du PRA/PCA pour vérifier son efficacité et identifier les domaines d'amélioration.
   * Mettre à jour le plan en fonction des changements dans le système d'information et des nouvelles menaces potentielles.

Plan de sauvegarde

Afin d’être parés à toute éventualité, nous devons faire des sauvegardes nos serveurs et de nos routeurs Pfsense

