Animus

Plan de reprise d’activité

09/11/2020

VARLET Timothée, DESROUSSEAUX Gabriel, GUYOT Erwan, TERRIER Antoine

Table des matières

Architecture

1- Eléments implémentés

Au cours de ce projet, plusieurs points ont été mis en place pour concevoir notre architecture :

- Une DMZ avec un firewall permettant à notre LAN d'être moins exposé.
- Un Active Directory.
- Un système d'authentification chiffré avec un PKI.
- Un accès à distance à notre réseau grâce à un VPN.
- Une architecture réseau permettant de réduire les impacts d'une panne d'un matériel réseau.
- Une politique de sauvegarde quotidienne fiable.
- Une sensibilisation des utilisateurs permettant de réduire le risque d'intrusions causées par une erreur humaine.
- Un switch supplémentaire en cas de panne d'un de nos switches utilisés.

2- Durée maximale admissible du dernier enregistrement des données.

Notre durée maximale du dernier enregistrement des données est écrite sous la forme de RPO. Ayant défini que tous les matins 1h avant le début des heures de travail notre serveur effectuerait une sauvegarde incrémentale, permettant de sauvegarder toutes les modifications opérées sur les données de l'entreprise durant les dernières 24h. Car la durée maximale admissible pour une perte de données sera de 1 jour, afin que le temps de travail perdu soit limité.

Nous pouvons aussi mettre en place un cloud permettant de récupérer les données à distance et en cas de problème de serveurs avoir un backup en ligne permettant d'avoir une plus grosse prévention en cas de perte de données.

Plan de reprise d'activité (PRA)

Un PRA se divise en 7 principales catégories pour chaque incident possible.

1. Criticité

La criticité d'un incident se définit en fonction de son impact sur le fonctionnement de l'entreprise. Elle est composée de 3 catégories.

Basse : Impact peu handicapant pour l'entreprise, aucun impact réel sur celle-ci.

Moyenne : Impact handicapant sur une certaine branche de l'entreprise ou sur un certain type de matériel menant à son utilisation impossible. Mais matériel ou branche facilement réparable ou remplaçable.

Haute : Impact très handicapant pour l'entreprise menant à l'inactivité de plusieurs branches de l'entreprise ou de l'entreprise entière.

Pour chaque catégorie de criticité cela mène à un RTO (Recovery Time Objective) plus ou moins long en fonction du niveau de catégorie. Au plus l'impact est critique, au plus le RTO et donc le temps de service inactif sera élevé. Nous pouvons monter par exemple à une journée entière d'inactivité lors d'une panne de courant, rendant le cas de panne de courant en criticité maximale.

2. Action immédiate

La catégorie action immédiate est la partie expliquant les premières actions à faire lors de la détection d'un problème permettant d'éviter l'aggravation d'un événement. Il expliquera comment réagir à cette situation et comment empêcher le problème de persister.

3. Action durable

L'action durable explique comment résoudre le problème dans les détails et réparer l'erreur pour que celle-ci ne soit plus un handicap au service et que le fonctionnement de l'activité revienne à la normale.

4. Effets sur utilisateurs

En cas de panne d'un service cela peut avoir des répercussions sur les utilisateurs. Cette partie nous détaillera quel service peut être dégradé et qui va être le plus touché par le cas de cette panne.

5. Prévention

Pour s'adapter et ne pas subir chaque problème auquel nous sommes confrontés, nous pouvons en rencontrant des problèmes éviter qu'ils se reproduisent. Cette catégorie nous permet aussi d'éviter les problèmes prévisibles en mettant en place des stratégies avant que le problème se produise et ainsi avoir une plus forte stabilité de nos services.

Par exemple pour éviter une erreur d'origine humaine nous pouvons sensibiliser les employés permettant d'éviter d'avoir ce type de problème tout en sécurisant leurs comptes. Cela nous permet alors d'avoir une forte prévention de ce genre de problème.

6. RPO

Partant du principe qu'une sauvegarde sera effectuée tous les matins 1 heure avant l'arrivée des employés, notre durée de RPO maximale sera fixée à 1 journée. L'horaire d'une heure avant l'arrivée des premiers employés étant le plus optimal, car en cas de problème de sauvegarde ou autre, la sauvegarde ne restera au maximum 1 seule heure non résolue.

7. RTO

Le temps maximum acceptable de l'interruption d'un service est défini en fonction de l'importance du service. Ce temps est défini en fonction de l'activité de l'entreprise et du temps de réparation et de détection du problème

Par exemple pour un ordinateur en panne. Il est plus acceptable que celui-ci soit inopérant plus longtemps qu'un serveur. Car un ordinateur portable en panne n'impacte qu'un employé, là où un serveur en panne peut impacter tout un service, voire même l'entreprise entière.

Pour notre PRA nous avons mis en place beaucoup de méthodes permettant de réduire l'impact d'un problème. Comme pour nos 4 switches montés en redondance permettant la prise en charge d'un switch déjà branché en cas de panne du switch principal, nous avons aussi décidé d'avoir un switch non-branché de secours permettant sa mise en place rapide en cas de plusieurs problèmes sur nos différents switches. Le fait d'avoir un switch de remplacement nous permettra de le mettre en place très rapidement en cas de panne, et ainsi d'avoir un temps d'inactivité minime.

Une mise en place de sauvegarde quotidienne, permet d'avoir une perte de données s'élevant au maximum à une journée ou moins. Ce qui nous permettra de régler énormément de problèmes, comme par exemple en cas de crash d'un pc ou d'une panne nous pouvons récupérer sa sauvegarde de la veille et restaurer cette sauvegarde sur un nouveau pc ou sur le pc réparé permettant à l'employé de pouvoir continuer à travailler sans avoir perdu plus d'une journée de travail.

Tableau PRA

Après l'analyse de chaque problème possible et de comment les résoudre. La mise en place d'un tableau répertoriant chaque incident possible mais aussi de comment réagir étape par étape à cet incident.

Description	Criticité	Detection	Action immédiate	Action durable	Effet sur utilisateurs	Prévention	RPO	RTO	Personne à contacter	Comment le contacter
Utilisateurs compromis	Basse	Actions opérées par utilisateur Inaccès à son propre compte	Bloquer l'utilisateur	Supprimer toutes les actions opérées par l'utilisateur, et supprimer son compte pour lui en recréer un de zéro.	Compte bloqué Nouveau compte	Windows Defender	24	1	Mr DESROUSSEAUX Gabriel	e-mail ou téléphone
Faille disque dur unique	Basse	Avertissement du système	Remplacer le disque dur Par un DD virtuel Restorer celui-ci par une sauvegarde	Acheter un nouveau disque dur. Remplacer le disque dur compromis.	Aucun effet	Garder des disques durs de secours	24	1	Mr DESROUSSEAUX Gabriel	e-mail ou téléphone
Faille de plusieurs disques durs	Basse	Avertissement du système	Remplacer le disque dur Par un DD virtuel Restorer celui-ci par une sauvegarde générale	Acheter un nouveau disque dur. Remplacer le disque dur compromis.	Aucun effet (Car basculement auto)	Mettre en place une sauvegarde générale de routine	24	1	Mr DESROUSSEAUX Gabriel	e-mail ou téléphone
Modification de contenu non-autorisé	Basse	Vérification des logs d'utilisateurs périodique	Restauration du contenu modifié	Réparer la brèche de sécurité	Changement pour utilisateurs	Réparer les vulnérabilités	1	0	Mr DESROUSSEAUX Gabriel	e-mail ou téléphone
Perte de données	Basse	Avertissement du système	Restaurer les données grâce à une backup	Aucune action supplémentaire nécessaire	Utilisateurs n'auront plus accès à leurs données	Mettre en place une sauvegarde générale de routine	24	1	Mr DESROUSSEAUX Gabriel	e-mail ou téléphone
Lieu de travail compromis	Haute	Détecteur de fumée...	évacuation du batiment Sauvegarde des données sur cloud (backup)	Mise en place de télétravail	Risque de dégât	Respect des normes (incendies, sismiques)	1	24	Mr DESROUSSEAUX Gabriel	e-mail ou téléphone
Panne de plusieurs postes de travail	Basse	Avertissement du système	Remplacer / réparer machines grâce à une sauvegarde	Remplacer / réparer machines grâce à une sauvegarde	Perte de performance de travail	Surveiller l'état des machines	24	1	Mr DESROUSSEAUX Gabriel	e-mail ou téléphone
Panne de serveur	Haute	Avertisement	Mettre en place un nouveau serveur grâce à une backup	Réparer l'ancien serveur pour plus que ca ne se reproduise	Grosse perte de perfomance de travail	Surveiller l'état des serveurs et que leurs capacités ne soient pas surchargés.	24	5	Mr DESROUSSEAUX Gabriel	e-mail ou téléphone
Panne logicielle	Moyenne	Avertissement du système	Mise à jour Réparation logiciel	Mise à jour Réparation logiciel	Aucun accès temporairement aux logiciels	Faire les mises à jour sur les versions les plus stables	1	12	Mr DESROUSSEAUX Gabriel	e-mail ou téléphone
Panne d'internet	Moyenne	Avertissement du système	Switch sur une connexion plus stable / boitier 4G	Changer de box internet	Aucune connexion temporairement	Avoir une connexion supportant le nombre de connexion. Limiter débit en fonction d'activité Faire les mise à jour et installation logicielles le soir	0	1	Mr DESROUSSEAUX Gabriel	e-mail ou téléphone
Panne switch	Faible	Problème de connexion aux serveurs	Prise en charge par l'autre switch de topo Changement de switch (switch de secours)	Vérifier les paramètres de l'ancien switch Bien paramétrer le nouveau switch	Aucun effet	Comprendre et appréhender le/les problème(s) Garder plusieurs switchs de secours	0	1	Mr DESROUSSEAUX Gabriel	e-mail ou téléphone
Coupure électrique	Haute	Extinction de toutes les machines	Prise en charge par générateur de secours Sauvegarde immédiate de toutes les données	Télétravail Migration appel client sur téléphone portable	Inapte au travail	Aucune prévention possible	0	24	Mr DESROUSSEAUX Gabriel	e-mail ou téléphone

Tableau du plan de reprise d'activité. Ce tableau est joint à ce rapport au format PDF

Plan de Reprise d'Activité manuscrite (PRA) :

Utilisateurs compromis :

Ce sinistre a un niveau de **criticité bas** car on peut facilement réagir et si ce n'est qu'un utilisateur simple il ne pourra faire trop de dégât au système d'information ou aux données.

L'**action immédiate** dans le cas où ce sinistre viendrait à se produire est qu'il faut **immédiatement bloquer le ou les utilisateurs en question** pour qu'ils ne puissent pas faire quoique ce soit qui puisse nuire à l'activité ou à l'entreprise.

À la suite de ce sinistre il faudrait en **action durable**, **rollback toutes les actions effectuées par le ou les utilisateurs compromis**, **supprimer le ou les comptes compromis** pour en **recréer de nouveaux** derrières pour éviter tout problèmes au cas où le hacker a installé des choses invisibles sur le ou les comptes compromis.

Ce sinistre a pour **effet sur l'utilisateur** qu'il verra son **compte bloqué, supprimé puis recréé par la suite** donc qu'il va perdre un petit peu de temps de travail et devoir refaire certaines choses sur le nouveau compte.

Pour la **prévention** d'un futur évènement similaire il faudrait **utiliser Windows Defender** pour que les comptes soit mieux protégés.

Le **RPO** de ce sinistre est de **24 heures** car en moyenne les sauvegardes de données utilisateurs dans les serveurs se font une fois par jour.

Le **RTO** de ce sinistre est de **1 heure** car si on réagit directement on n'a besoin que d'une heure pour bloquer le compte, rollback les actions du compte, supprimer le compte et en recréer un derrière.

Faille de disque dur unique :

Ce sinistre a un niveau de **criticité basse** car une faille de disque dur est facilement détectable et facilement remplaçable. Un problème de disque dur n'impact qu'une seule machine donc cela ne pénalisera pas un service entier.

L'**action immédiate** dans le cas où ce sinistre viendrait à se produire est qu'il faut **remplacer le disque dur qui a une faille par un disque dur virtuel** en attendant et ensuite **restaurer le disque dur virtuel** avec une sauvegarde récente et fonctionnelle du disque dur compromis.

À la suite de ce sinistre il faudrait en **action durable**, **racheter un nouveau disque dur** et **remplacer le disque dur compromis** en le restaurant avec une sauvegarde récente et fonctionnelle.

Ce sinistre n'a **pas d'effet sur l'utilisateur.**

Pour la **prévention** d'un futur évènement similaire il faudrait **avoir plusieurs disques durs de secours** pour pouvoir directement remplacer le disque dur plutôt que de devoir passer par un disque dur virtuel.

Le **RPO** de ce sinistre est de **24 heures** car en moyenne les sauvegardes de données dans les serveurs se font une fois par jour.

Le **RTO** de ce sinistre est de **1 heure** car on peut mettre en place le disque dur virtuel et/ou remplacer le disque dur compromis en 1 heure.

Faille de plusieurs disques durs :

Ce sinistre a un niveau de **criticité basse** car le fait d'avoir plusieurs disques durs en panne peut un handicap sévère pour une simple machine mais cet incident peut être facilement résolu sans pour autant impacter un service entier grâce au backup.

L'**action immédiate** dans le cas où ce sinistre viendrait à se produire est qu'il faut **remplacer les disques durs qui a une faille par des disques durs virtuels** en attendant et ensuite **restaurer les disques durs virtuels** avec une sauvegarde récente et fonctionnelle générale.

À la suite de ce sinistre il faudrait en **action durable**, **racheter des nouveaux disques durs** et **remplacer les disques durs compromis** en les restaurant avec une sauvegarde récente et fonctionnelle générale.

Ce sinistre n'a **pas d'effet sur l'utilisateur** car le basculement sur les disques durs virtuels se font automatiquement.

Pour la **prévention** d'un futur évènement similaire il faudrait **avoir plusieurs disques durs de secours** pour pouvoir directement remplacer le disque dur plutôt que de devoir passer par un disque dur virtuel et **mettre en place une sauvegarde générale journalière.**

Le **RPO** de ce sinistre est de **24 heures** car en moyenne les sauvegardes de données dans les serveurs se font une fois par jour.

Le **RTO** de ce sinistre est de **1 heure** car le basculement sur les disques durs virtuels se fait automatiquement et que le changement et que la restauration peut se faire en 1 heure.

Modification de contenu non-autorisé :

Ce sinistre a un niveau de **criticité bas** car la modification de contenu non-autorisé ne va pas forcément impacter gravement l'activité et la mise en place d'un backup est facilement réalisable grâce aux sauvegardes récentes qui sont détectables avec les logs.

L'**action immédiate** dans le cas où ce sinistre viendrait à se produire est qu'il faut **utiliser les backups** pour modifier ce qui a été modifié pour le faire redevenir comme il était avant la modification non-autorisé.

À la suite de ce sinistre il faudrait en **action durable**, **repérer et réparer la brèche de sécurité** pour ne plus que ça se reproduise.

Ce sinistre a pour **effet sur l'utilisateur** que **certaines données ou certains fichiers peuvent revenir à un état précèdent** pour contrer les modifications non-autorisés.

Pour la **prévention** d'un futur évènement similaire il faudrait **réparer la ou les brèches de sécurité**.

Le **RPO** de ce sinistre est de **1 heure** car en moyenne un utilisateur va sauvegarder le fichier sur lequel il travaille toutes les heures.

Le **RTO** de ce sinistre est de **0 heure** car le fichier ça ne prend que très peu voire presque pas de temps pour revenir à un état précèdent à partir de backups ou d'anciennes sauvegardes ou simplement en faisant Ctrl + Z.

Perte de données :

Ce sinistre a un niveau de **criticité bas** car grâce aux backups quotidienne nous avons un accès immédiat et facile à nos données de la veille ce qui permet de ne pas reprendre le travail à 0 mais de repartir sur nos anciennes sauvegardes de la veille.

L'**action immédiate** dans le cas où ce sinistre viendrait à se produire est qu'il faut **restaurer les données avec les backups de données.**

À la suite de ce sinistre il faudrait en **action durable**, **faire attention** à ce que ça ne se reproduise plus et **toujours avoir des backups** sous le coude en cas de problème.

Ce sinistre a pour **effet sur l'utilisateur** que **les utilisateurs n'auront plus accès aux données** le temps que les données soit restaurés depuis le backup.

Pour la **prévention** d'un futur évènement similaire il faudrait **mettre en place une sauvegarde générale journalière.**

Le **RPO** de ce sinistre est de **24 heures** car en moyenne les sauvegardes de données se font tous les jours.

Le **RTO** de ce sinistre est de **1 heure** car il suffirait d'une heure pour pouvoir restaurer les données à partir du backup.

Lieu de travail compromis :

Ce sinistre a un niveau de **criticité haut** car en fonction de la catastrophe qui se produit et de sa gravité il peut y avoir des dégâts conséquents pour le matériel de l'entreprise, mais aussi l'innaccès aux locaux peut empêcher la production de certains services pour les clients par l'entreprise Animus

L'**action immédiate** dans le cas où ce sinistre viendrait à se produire est qu'il faut **évacuer le bâtiment** (dans le cas d'un incendie) **ou se mettre à l'abris** (dans le cas d'un tremblement de terre ou d'inondations). Il faudrait aussi **sauvegarder toutes les données possibles sur un cloud** pour pouvoir toujours y avoir accès au cas où les serveurs de données internes venaient à être endommagés.

À la suite de ce sinistre il faudrait en **action durable**, **mettre en place du télétravail** dans le cas du possible en fonction des dégâts matériels.

Ce sinistre a pour **effet sur l'utilisateur** qu'il y a un **risque de dégâts sur le matériel et sur les personnes** présentes dans le bâtiment à ce moment.

Pour la **prévention** d'un futur évènement similaire il faudrait **respecter au mieux les normes anti-catastrophe** comme les normes incendiaires et sismiques.

Le **RPO** de ce sinistre est de **1 heures** car il faut environ 1 heure pour enregistrer les données sur un cloud.

Le **RTO** de ce sinistre est de **24 heure** car l'indisponibilité causée par la catastrophe est variable entre 1 et 24h en moyenne.

Panne de plusieurs postes de travail :

Ce sinistre a un niveau de **criticité bas** car ce n'est pas bien grave si certaines personnes ne peuvent pas travailler sur le moment et ce genre de problème peut se résoudre relativement rapidement.

L'**action immédiate** dans le cas où ce sinistre viendrait à se produire est qu'il faut **remplacer ou réparer le poste inapte** à travailler avec une sauvegarde récente.

À la suite de ce sinistre il faudrait en **action durable**, **repérer le problème** pour que cela ne se reproduise pas dans le futur et **réparer ou remplacer le poste** si cela n'est pas déjà fait.

Ce sinistre a pour **effet sur l'utilisateur** que **l'utilisateur ne pourra pas travailler** pendant un certain donc on aura une perte de performance.

Pour la **prévention** d'un futur évènement similaire il faudrait **surveiller l'état des machines** régulièrement.

Le **RPO** de ce sinistre est de **24 heures** car en moyenne les sauvegardes des données se font tous les jours.

Le **RTO** de ce sinistre est de **1 heure** car il faut environ une heure pour pouvoir changer un utilisateur de poste de travail.

Panne de serveurs :

Ce sinistre a un niveau de **criticité haut** car si un serveur venait à tomber une panne ce serait un très gros problème pour l'activité en fonction de l'utilité du serveur.

L'**action immédiate** dans le cas où ce sinistre viendrait à se produire est qu'il faut **mettre un place un nouveau serveur** en mettant dessus le backup du serveur qui vient de tomber en panne.

À la suite de ce sinistre il faudrait en **action durable**, **repérer le problème** et **réparer l'ancien serveur** en conséquence.

Ce sinistre a pour **effet sur l'utilisateur** qu'il y aura une **grosse perte de performance** étant donné que l'un des serveurs sera down pendant un moment.

Pour la **prévention** d'un futur évènement similaire il faudrait **surveiller l'état des serveurs** et **surveiller la capacité des serveurs** pour éviter qu'ils ne soient pas surchargés.

Le **RPO** de ce sinistre est de **24 heures** car les sauvegardes de données serveur se font une fois par jour.

Le **RTO** de ce sinistre est de **5 heures** car il faut en moyenne 5 heures pour mettre en place un nouveau serveur en utilisant le backup de l'ancien serveur.

Panne logicielle :

Ce sinistre a un niveau de **criticité moyen** car en fonction du logiciel la gêne occasionnée peut être plus ou moins importante.

L'**action immédiate** dans le cas où ce sinistre viendrait à se produire est qu'il faut **mettre à jour** ou **réparer le logiciel** en question.

À la suite de ce sinistre il faudrait en **action durable**, qu'il faut **mettre à jour** ou **réparer le logiciel** en question.

Ce sinistre a pour **effet sur l'utilisateur** que le logiciel en question ne sera pas disponible pendant un moment.

Pour la **prévention** d'un futur évènement similaire il faudrait **vérifier que les pilotes, applications et logiciels** soient souvent **mis à jour**.

Le **RPO** de ce sinistre est de **1 heure** car grâce aux backups quotidiennes nous pouvons récupérer les données de la veille si elles sont corrompues à cause du logicielle, il suffit alors de réinstaller le logiciel ou le mettre à jour sur une version plus stable.

Le **RTO** de ce sinistre est de **12 heures** car pour diagnostiquer un logiciel et le réparer et/ou le mettre à jour il faut environ une journée de travail complète soit 12 heures.

Panne d'internet :

Ce sinistre a un niveau de **criticité moyen** car une panne d'internet peut empêcher la plupart des activités qui ont besoin d'une connexion internet mais ne va pas forcément tout bloquer.

L'**action immédiate** dans le cas où ce sinistre viendrait à se produire est qu'il faut **se reporter vers une connexion plus stable fonctionnelle** ou passer sur un **boitier 4g**.

À la suite de ce sinistre il faudrait en **action durable**, **trouver la source du problème et être plus sensible** à ce niveau-là et **changer de routeur ou de fournisseur internet**.

Ce sinistre a pour **effet sur l'utilisateur** que la connexion internet sera indisponible pendant un moment.

Pour la **prévention** d'un futur évènement similaire il faudrait **s'assurer que la connexion peut tenir un certain nombre de connexions simultanées**, **limiter le débit** en fonction de l'activité de l'utilisateur et **faire les tâches lourdes** en connexion comme les mises à jours et téléchargements **la nuit.**

Le **RPO** de ce sinistre est de **0 heure** car une coupure d'internet nous permet d'au minimum sauvegarder en local et de ne perdre aucune donnée et attendre que la connexion revienne pour récupérer toutes les fonctionnalités.

Le **RTO** de ce sinistre est de **1 heure** car il faut en moyenne une heure pour pouvoir connecter tous les utilisateurs à un nouveau point de connexion.

Panne de switch :

Ce sinistre a un niveau de **criticité bas** car dans notre topologie si un switch venait à tomber en panne, un autre switch prendrait immédiatement le relai ce qui fait que ça n'a presque aucun impact.

L'**action immédiate** dans le cas où ce sinistre viendrait à se produire est qu'il faut **remplacer le switch défaillant** par un switch de secours pendant que **l'autre switch en redondance prendra automatiquement le relai**.

À la suite de ce sinistre il faudrait en **action durable**, **vérifier les paramètres de l'ancien switch** et **trouver le problème** pour ne plus que cela se reproduise et **bien paramétrer le nouveau switch** en conséquence.

Ce sinistre n'a pas d'**effet sur l'utilisateur**.

Pour la **prévention** d'un futur évènement similaire il faudrait **comprendre et appréhender le problème** survenu et **avoir plusieurs switchs de secours**.

Le **RPO** de ce sinistre est de **0 heure** car ayant un switch de secours la route passera automatique sur notre switch de secours étant paramétré déjà comme le premier qui est tombé en panne.

Le **RTO** de ce sinistre est de **1 heure** car il faut en moyenne une heure pour pouvoir remplacer le switch défaillant par le switch de secours.

Coupure électrique :

Ce sinistre a un niveau de **criticité haut** car une coupure électrique va, dans la plupart des cas, couper plusieurs services comme la connexion internet, certains serveurs physiques, certains postes de travails si ce sont des ordinateurs fixes.

L'**action immédiate** dans le cas où ce sinistre viendrait à se produire est qu'il faut **prendre en charge par un générateur de secours** qui servira à tous les **utilisateurs de faire les sauvegardes nécessaires** avant que le générateur de secours ne soit vide.

À la suite de ce sinistre il faudrait en **action durable**, **proposer du télétravail** et faire une **migration des appels client sur téléphone portable** pour être moins dépendant de source électrique.

Ce sinistre a pour **effet sur l'utilisateur** que dans la plupart des cas l'utilisateur sera inapte à travailler.

Ce genre d'évènement n'est **pas vraiment prévisible** donc on ne peut **pas** proposer de **prévention** à cela.

Le **RPO** de ce sinistre est de **0 heures** car ayant mis en place un générateur permettant de tenir au maximum une heure notre système informatique ou du moins les parties où la sauvegarde de données est le plus important cela laissera le temps à tout le monde d'enregistrer toutes ses données et ne pas les perdre avec une coupure brutale de leurs travails sans avoir l'occasion de sauvegarder.

Le **RTO** de ce sinistre est de **24 heure** car en moyenne on trouve une solution ou le problème est résolu au bout de 24 heures.