Mémoire de fin d'étude

Thème : Analyse des risques résiduels aux mécanismes et stratégies de protection du système d'information du groupe AG2R LA MONDIALE face aux pertes de données

Mémoire rédigé et présenté par : **Borel TAMETCHOP TEMKOU**

Tuteur entreprise : **Yannick LAFOUCRIERE**

Tuteur école : **Abdelhadi MIFDAL**

Document confidentiel

Année universitaire 2021 – 2022

Dédicaces

Ce mémoire de fin de cycle est dédié à toute ma famille pour son soutien indéfectible et à toutes les personnes qui de près ou de loin ont participé à la réussite de ce travail.

Remerciements

Je tiens à remercier toutes les personnes qui ont contribués au succès de mon apprentissage et qui m'ont aidé pendant la rédaction de ce mémoire de fin de cycle.

Je voudrais dans un premier temps remercier mon tuteur professionnel M. Yannick LAFOUCRIRE et M. Jean-Francois NERON chef de l'équipe Ressources IT et Orchestration, pour leurs patiences, leurs disponibilités et surtout les conseils, qui ont contribué à alimenter ma réflexion.

Je remercie également toute l'équipe pédagogique du Groupe 3IL et les intervenants, pour avoir assuré la théorie et la pratique en cours.

Je tiens à témoigner toute ma reconnaissance aux personnes suivantes, pour leur aide précieuse :

M. Abdelhadi MIFDAL mon tuteur académique qui m'a guidé et poussé ma réflexion dans la réalisation de ce mémoire.

M. Adrien YVANOFF, M. Bertrand MONNIRIEL, M. Remy IBACH, Jean Pierre BELMOND qui ont partagé leurs connaissances et expériences.

Enfin ma famille, pour leur soutien indéfectible et leurs encouragements.

Résumé

Ce mémoire est le fruit de mon parcours d'apprentissage au sein de l'entreprise AG2RLM. Il s'inscrit dans un contexte où les cybers attaques visant l'intégrité des systèmes d'information sont de plus en plus récurrentes. A cet effet, il est exigé aux entreprises qui fournissent des services nécessaires à l'activité économique et sociale de mettre en place des mécanismes et stratégies de protection pour assurer la résilience de son système d'information. J'ai étudié les règles sur la protection des systèmes d'information applicables aux OSE pour analyser celles implémentées au sein de l'entreprise AG2RLM. Ces recommandations concernent l'administration sécurisée des plateformes, le maintien en condition opérationnel, la sauvegarde et la gestion des droits d'accès. De ces recommandations, j'ai émis des critiques et par la suite des axes d'amélioration. Les critiques émises portent sur le partage de la station de travail pour l'administration des plateformes et les usages récurrents (messagerie, navigation sur internet, traitement de document). Les axes d'amélioration que j'ai proposés englobent la mise en place d'une infrastructure VDI dédiée à l'administration des plateformes avec une authentification centralisée multi facteur, la sauvegarde des données NAS dans la plateforme de sauvegarde inaltérable. Certains axes d'amélioration tels que la réduction de la durée de conservation des données de la plateforme inaltérable doivent encore être réévalués, car elle entre en conflit avec certains principes du RGPD et la cohérence en cas de restauration.

Abstract

This brief is the result of my learning journey at AG2RLM. It takes place in a context where cyber attacks on the integrity of information systems are increasingly recurring. In this case, compagnies providing services necessary for economic and social activity are required to put in place protective mechanisms and strategies to ensure the resilience of their information systems. I have studied the rules on the protection of information systems applicable to OSE to analyze those implemented within the AG2RLM company. These recommendations concern the secure administration of platforms, the maintenance in operational condition, the safeguarding and management of access rights. From these recommendations I have expressed criticism and subsequently areas for improvement. The criticisms raised concern the sharing of the workstation for the administration of platforms and recurring uses (messaging, internet browsing, document processing). The areas for improvement that I have proposed include the establishment of a VDI infrastructure dedicated to the administration of the platforms with centralized multi-factor authentication, the backup of NAS data in the unalterable backup platform. Some areas for improvement such as the reduction of the retention period of the data of the unalterable platform must still be reassessed because it conflicts with certain principles of the GDPR and consistency in the event of restoration

Glossaire

AG2RLM : ag2r la mondiale

ANSSI : agence nationale de la sécurité des systèmes d'information

IP : internet protocole

NAS : network area Storage

NIS : network system information and Security

PSI : plan de secours informatique

PSI CYBER : plan de secours informatique cyber

OSE : operateur de services essentiels

RGPD : règlement générale sur la protection des données à caractère personnelle

RPO : recovey point objective

SI : système d'information

SAN : Storage area network

SSL : sécure socket layer

VDI : Virtual desktop infrastructure

VSA : Virtual server agent

WAN : wide area network

Sommaire

Introduction générale

Les données, représentent pour chaque entreprise l'actif élémentaire permettant d'alimenter en permanence son unité organisationnelle. L'intégration des technologies numériques dans le traitement de ces données, est un enjeu stratégique pour le développement de son activité, puisqu'elle favorise la compétitivité, l'efficacité et l'amélioration des conditions de travail. Tout ceci est possible grâce aux nouvelles technologies de l'information et de la communication qui garantissent disponibilité, scalabilité et performance. Face aux avantages que tirent les entreprises des technologies numériques, se trouve un risque pouvant mettre en péril l'entreprise : la perte des données.

En effet, une étude réalisée par Hiscox Assurance France montre que « En moyenne, 80% des entreprises qui perdent leurs données informatiques font faillite dans les 12 mois qui suivent » [1]. Cette perte de données peut découler d'une catastrophe naturelle, d'une cyberattaque, d'une panne matérielle, ou par le sabotage d'un employé malveillant.

Pour les entreprises opérateurs de services essentiels, à l'instar d'AG2R LA MONDIALE, la mise en place des mécanismes de protection du système d'information et des données stockées est un objectif élémentaire visant à assurer la résilience face aux pertes de données et garantir la pérennité de l'entreprise.

Toutefois, les mécanismes mis en œuvre peuvent être perfectibles au regard des nouvelles vulnérabilités qui plane sur les systèmes d'information. Dans une démarche d'amélioration continue, il nous revient de répondre aux questions : quelles sont les failles à la stratégie de résilience face aux pertes de données ? et quels peuvent êtres des axes d'amélioration ?

Pour ce faire, nous allons confronter les préconisations l'union européenne et des services publics Français en matière de protection des systèmes d'information et ceux implémentés au sein du groupe AG2RLM. Mon travail, s'articule autour de deux parties, en premier plan, état de l'art qui présente les opérateurs de services essentiels, les règles auxquelles ils sont soumis en matière de protection des systèmes d'informations. En second plan, l'analyse crique qui présente les mécanismes et stratégies de protection du système d'information implémentés au sein de notre entreprise ainsi que les critiques pour proposer des solutions ou axes d'amélioration.

Première Partie : État de l’art

- Chapitre 1 : Les opérateurs de services essentiels
- Chapitre 2 : La protection du système d’information des opérateurs de services essentiels

Chapitre 1 : Operateurs de services essentiels

Ce chapitre présente les opérateurs de services essentiels et les obligations auxquelles ils doivent se conformer.

1. Les services essentiels

L'union européenne, pour assurer la sécurité des activités économiques et sociales critiques des pays membres face aux risques cyber, a mis sur pied la directive européenne NIS (Network and information system Security) qui définit un cadre règlementaire visant à renforcer la cybersécurité au sein des pays membre. Elle a été transposée en droit nationale par l'état Français, et est sous la supervision de l'agence national de la sécurité des systèmes d'information qui accompagne et contrôle les opérateurs de services essentiels dans la mise en place de ces prescriptions. [2]

2. Les opérateurs de services essentiels

Les opérateurs de services essentiels (OSE) sont des structures publiques ou privées, fournissant des services, nécessaires au fonctionnement économique et sociale de la nation, dont la continuité pourrait être affectée par des incidents sur son système d'information, nécessaire à la fourniture des dits services. En raison de leurs activités, les structures OSE traitent et stockent des données extrêmement variées dans leur nature, leur usage et leur sensibilité au quotidien. Une altération de ces données, c'est-à-dire un défaut d'intégrité, peut avoir un impact immédiat, comme dans le cas des données de prévoyance santé, qui peuvent être essentielles au traitement de l'assurance santé d'un patient et dont l'altération peut impacter significativement la qualité et les délais de traitement. La modification d'autres types de données présentes dans le SI, comme les systèmes d'exploitation informatiques et les applications métiers, ou encore les paramétrages des équipements, peuvent entraîner des dysfonctionnements importants des systèmes essentiels et priver les personnels des outils informatiques nécessaires à leurs activités, ou engager la responsabilité de la structure dans des litiges avec des tiers ou avec l'Etat. [2]

2.1 Les Obligations des opérateurs de services essentiels

Désigner par le premier ministre sur recommandation des ministres des secteurs d'activité concernés et l'agence national de la sécurité des systèmes d'information, les OSE sont tenus de :

- Identifier un représentant auprès de L'ANSSI ;
- L'identification du ou des services essentiels ;
- Déclarer à l'ANSSI tout incident susceptible d'avoir un impact sur la continuité des services ;
- Participer aux contrôles de sécurité de l'ANSSI ou des prestataires qualifiés sous la demande du premier ministre ;
- Appliquer dans un délai imparti des règles de sécurité. [2]

2.2 Les règles de sécurité

Elles font partie des obligations auxquelles doivent se conformer les OSE et se regroupent autour de 4 quatre principes du management des risques :

- La gouvernance de la sécurité des réseaux et système d'information : elle concerne la mise en œuvre d'une politique de sécurité et l'homologation des réseaux et systèmes d'information ;
- La protection et la sécurité des réseaux et système d'information : elle concerne la sécurité de l'architecture, l'administration et le contrôle d'accès des réseaux et système d'information, la sécurité physique et environnementale ;
- La défense et la sécurité des réseaux et système d'information : elle couvre la détection, le traitement des incidents affectant les réseaux et système d'information ;
- La résilience et la sécurité des réseaux et système d'information : elle porte sur la gestion de crises en cas d'incidents de sécurités. [2]

Ce mémoire analyse les règles sur la protection des systèmes d'information.

Chapitre 2 : La Protection des systèmes d'information des OSE

Ce chapitre, met en lumière les règles et préconisation définies par l'agence nationale de la sécurité des systèmes d'information, la directive Network and information Security system pour assurer la protection des systèmes d'informations essentiels.

1. La Protection des SI

De nous jours, aucune entreprise n'est à l'abris d'une attaque visant son système d'information, quel que soit son domaine d'activité ou sa taille. Cependant, l'impact dépend des données qui y sont stockées. Une attaque désigne un acte malveillant visant à endommager, voler ou détruire les données d'un système d'information. Pour faire face aux attaques, les entreprises implémentent des mécanismes de sécurité ayant la capacité de prévenir, identifier et réagir contre les menaces. Malgré tous ces mécanismes, les attaques cybers ne cessent d'augmenter avec la découverte de nouvelles failles de sécurité, le développement de nouvelle technique attaque et l'augmentation des surfaces d'attaques, rendant les entreprises de plus en plus vulnérables. Toutefois, les entreprises doivent accepter les principes selon lesquels, elles peuvent être victimes d'une attaque, et doivent donc mettre en place des stratégies de protection résiliente pour limiter l'impact et relancer le système d'information après l'incident.

La résilience est la capacité pour une entreprise à assurer la reprise de son activité après un incident malveillant ou involontaires ayant causé une interruption totale pour partielle de son système d'information. Mettre en place une stratégie de protection résiliente revient pour les entreprises à passer de mesures passives que propose la cybersécurité à des mesures proactives pour minimiser les pertes de données et garantir la reprise d'activité.

1.1 La protection des SI des OSE

Une des particularités des OSE est le fait qu'ils collectent et traitent les données à caractère personnel pour mener à bien leurs activités. Ces opérations sur les données sont réalisées par le biais du SI afin de permettre une meilleure interaction entre les différents acteurs de son unité organisationnelle et de faciliter le processus décisionnel. Protéger ce SI, c'est garantir la continuité des services sur lesquels il repose. Pour protéger la vie privée et liberté des populations, l'union européenne à instaurer le règlement général sur la protection des données à caractère personnelle (RGPD) qui définit un cadre règlementaire pour la collecte et le

traitement des données personnelles sur son territoire. Il vise à renforcer les droits des personnes dont les données sont collectées et à responsabiliser les responsables du traitement.

Pour se conformer au RGPD, les OSE doivent intégrer dans leur processus de traitement, des dispositifs permettant à une personne d'exercer ses droits sur ses données. Ils doivent s'assurer de la sécurité des locaux et des SI pour empêcher que les données ne soient déformées, endommagées ou que des tiers non autorisés y aient accès. Ces mesures doivent être prises en considération dès la conception de son SI.

Nous allons nous concentrer dans ce mémoire sur les mécanismes mis en place pour assurer la protection du système d'information et les données qu'il contient.

1.2 Les menaces pesant sur un système d'information

Il s'agit des incidents pouvant entrainer l'interruption totale ou partielle :

- Les défaillances matérielles et logiciels ;
- Les erreurs de manipulation commises par les utilisateurs ou les exploitants du SI ;
- Les tentatives de nuisance (vengeance par « sabotages » ou « vandalisme » des données) qui impliquent généralement des personnes ayant ou ayant eu un lien avec la structure (employé, fournisseur…), ou tentatives de déstabilisation de l'entreprise par le piratage ;
- La cybercriminalité ciblée qui grâce au ransomware bloque l'accès aux données en leurs chiffrant pour réclamer une rançon à la victime.

1.3 La finalité de la protection d'un système d'information

Pour répondre aux contraintes que peuvent engendrer les menaces ci-dessus, des mécanismes doivent être mise en œuvre afin :

- Assurer la disponibilité du SI
- Détecter les modifications anormales des données stockées
- Être en possession d'une copie des données en cas d'altération des originaux.
- Relancer le système d'information de l'entreprise en cas de cyberattaque.
- Assurer la protection et l'intégrité des applications et des données.

2. Les stratégies et mécanismes de protection des SI pour une résilience aux pertes de données

Elles s'inspirent des règles de sécurité de la directive network and information system Security et de la commission européenne visant à améliorer la résilience numérique des entreprises opérateurs de service essentiels et acteurs du secteur financier européen.

2.1 La sauvegarde des données

La sauvegarde est une technique qui permet de garder une copie des données à un instant T. Des sauvegardes régulières, de l'ensembles des données de l'infrastructure, des applications métier et des serveurs de fichier, doivent être réalisées enfin d'avoir en sa possession qui copie des données sur laquelle on peut s'appuyer pour réaliser une restauration en cas de défaut d'intégrité des originaux.

2.1.1 Les types de sauvegarde

- La sauvegarde complète : elle représente la copie complète de tout données présentes dans le support d'un système de traitement.
- La sauvegarde différentielle : C'est la copie des données modifiées depuis la dernière sauvegarde complète.
- La sauvegarde incrémentale : c'est la copie des données modifiées depuis la dernière sauvegarde.

2.1.2 Le périmètre de la sauvegarde

Il est propre à chaque entreprise et identifie le champ d'application de la sauvegarde. On l'établit en fonction de :

- La criticité des données,
- La vitesse d'évolution des données,
- Le volume des données,
- La durée de conservation
- La périodicité de la sauvegarde

2.1.3 Fréquence de la sauvegarde

Elle est fonction du RPO (recovery point objective) et permet de définir la durée qui s'écoule entre deux sauvegardes que nous pouvons exploiter pour restaurer les données. Moins il y a d'écart de temps entre les sauvegardes plus il y a de chance de récupérer les données récentes.

2.1.4 Stratégie de sauvegarde

Afin de prévenir les risques de pertes ou de compromissions totales des données, il est important de mettre en place une stratégie de sauvegarde reposant sur la règle de 3-2-1. Cette règle préconise :

- Réaliser Trois copies des données dont Une originale et Deux copies.
- Stocker ses Deux copies sur Deux supports distincts pour réduire les pertes de données dues à la défaillance du support en cas d'utilisation d'un support unique.
- Stocker une copie de ses données hors site pour prévenir la perte totale des données en cas d'incendie, d'attaque physique ou de cyberattaque. [3]

2.1.5 Contrôle et vérification des sauvegardes

En cas de pertes ou de compromission des données de production, la sauvegarde est le seul recours que peut utiliser les entreprises pour assurer un retour d'activité. Il est primordial pour les entreprises d'effectuer des vérifications de chaque processus de sauvegarde et réaliser des tests de restauration des données sauvegardés pour s'assurer qu'ils disposent d'une source fiable pour assurer la continuité de l'activité de l'entreprise après un sinistre.

2.2 Les mises à jour des plateformes

Appliquer régulièrement les mises à jour des composants du système d'information permet de corriger les vulnérabilités présentent sur les dits systèmes, qui peuvent être source d'attaque ou propagation des infections. Ces mises à niveau doivent être signées par l'éditeur des plateformes en question et installer dès sa publication avec un processus maîtrisé. Une veille des plateformes doit être effectuée en permanence pour rester informé de la découverte des vulnérabilités et la disponibilité des différents patchs ou mises à jour proposé par l'éditeur pour les correctifs.

2.3 Cloisonnement

Séparer les différents éléments d'un système d'information sans impacter le service rendu permet de limiter la surface d'attaque, Contenir ou de ralentir un éventuel attaquant en l'empêchant d'accéder à des éléments du système d'information, aussi bien depuis l'extérieur (intrusion) que depuis l'intérieur (déplacement latéral)

2.3.1 Le cloisonnement physique

Elles définies de quelle manière les différents sous-systèmes d'un SI sont séparés. Les connexions entre équipements doivent être uniquement ceux nécessaires au bon fonctionnement. Elle concerne les connexions réseau, mais aussi les possibilités de communication au sein d'un même composant physique à l'instar des échanges inter processus au sein d'un système d'information ainsi que les communications entre plusieurs machines virtuelles à travers leur hyperviseur commun.

2.3.2 Le cloisonnement logique

Il s'agit de l'isolation intégrée à l'équipement, permettant de séparer les différents sous-systèmes intérieurs. Par ce mécanisme, la communication latérale entre sous système est impossible, chaque sous-système est indépendant l'un de l'autre.

2.4 L'administration sécurisée

L'administration désigne tout action d'installation, de modification ou de suppression d'un composant d'un SI susceptible de modifier son fonctionnement ou sa sécurité. Ces actions doivent être identifiés et protéger car elle représente les vecteurs d'attaque utilisés pour compromettre le fonctionnement d'un système d'information. Une bonne administration sécurisée passe par :

- Une meilleure gestion des comptes d'administration : les administrateurs doivent disposer d'un ou plusieurs comptes dédiés distincts pour chaque système, ce compte doit disposer uniquement des droits lui permettant de réaliser son travail sur son périmètre d'action ;
- Un annuaire doit être dédie pour gérer les comptes d'administration et les accès aux ressources administrées ;
- Une authentification renforcée des comptes administration avec l'utilisation des mots de passe complexes et le double facteur d'authentification ;

- Chiffrer les secrets d’authentification lorsqu’ils sont en transit ou stockés.

2.5 La sécurité physique et environnementales

Elle concerne toutes les procédures et les méthodes mises en place pour assurer la sécurité physique et environnementale des infrastructures qui héberges les systèmes d’information essentiels. Cette sécurité doit prendre en compte :

- La protection contre les risques environnementaux (les catastrophes naturelles, incendie)
- Le contrôle des accès physique à l’infrastructure
- Le contrôle des employés internes et externes qui peuvent accéder à l'infrastructure.

Deuxième Partie : Analyse critique

❖ Chapitre 3 : La protection du système d'information chez AG2RLM

❖ Chapitre 4 : Critiques et suggestions d'amélioration des mécanismes et stratégies de protection du système d'information

Chapitre 3 : La protection du système d'information et ses données chez AG2RLM

Ce chapitre présente les stratégies et mécanismes mis en place pour assurer la protection SI et les données stockées au sein du groupe AG2RLM.

1. Présentation du SI

Le groupe AG2LM en tant qu'opérateur de services essentiels et acteur du secteur financier en France et dans l'union européenne, traite et stocke un très grand volume de données dont l'intégrité et la disponibilité garantie la pérennité de son activité. Pour assurer cette pérennité, il dispose d'une architecture convergée qui permet d'assurer la tolérance aux pannes et au désastre de site, procurant ainsi un niveau de protection de son SI. Cette infrastructure est organisée autour de deux data center dont l'un est le site de production et l'autre le site de secours. Voir l'étude de l'existant dans le rapport du projet de sauvegarde inaltérable

Le système d'information du groupe AG2RLM, étant essentiel pour la continuité des services fournis et la pérennité de son activité, se doit être disponible et intègre. Pour cela plusieurs mécanismes et technologies sont déployés pour assurer la protection du système d'information. [4]

2. La protection du système d'information

Elle résulte de l'ensemble des mécanismes et stratégies mis en place pour assurer la disponibilité, l'intégrité et la sécurité.

2.1 La tolérance aux pannes

Au sein de ses infrastructures, le premier niveau de protections du SI réside dans sa capacité à tolérer les pannes. Elle est assurée par les mécanismes suivants :

2.1.1 La redondance

Pour éviter les pertes de données ou interruption des services suites à l'indisponibilité d'un équipement ou la rupture d'une liaison, Alimentations électriques, disques, contrôleurs de stockage sont doublés au sein de l'infrastructure. Le raccordement d'un équipement aux sources d'énergie ou aux réseaux de communication (réseau local ou réseau de stockage) est toujours doublé, en mode actif/passif (failover)ou actif/actif (répartition de charge). Les réseaux de

stockage SAN sont tous en mode dual fabric actif/actif (deux chemins redondants), quel que soit le protocole utilisé.

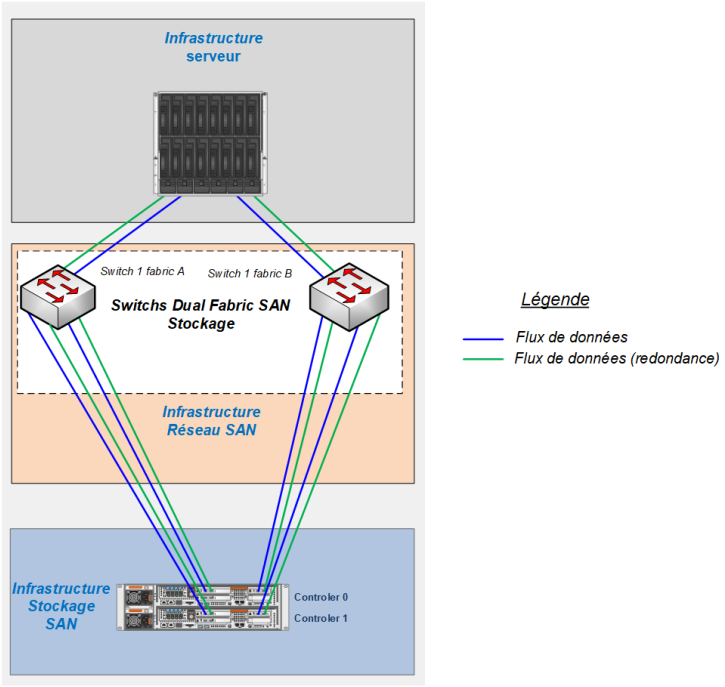

Figure 1: redondance des liaisons de données

2.1.2 La virtualisation des environnements

Elle occupe prêt de 80% de l'infrastructure, favorisant la création des clusters de serveurs (hyperviseurs) en fonction des environnements, pour faciliter la migration d'une machine virtuelle d'une infrastructure à une autre sans interruption de service ou de redémarrer une machine virtuelle en cas de perte de son hyperviseur sur un autre.

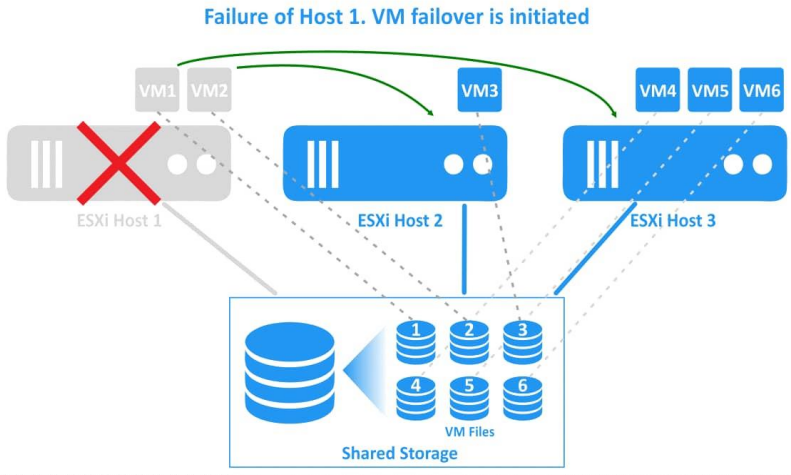

Figure 2 : mécanisme de failover dans un cluster de serveurs *[4]*

2.2 Le cloisonnement

il permet d'isoler les sous-systèmes d'un SI afin de réduire la surface d'attaque ou de propagation d'une attaque.

2.2.1 Cloisonnement physique

C'est l'infrastructure principale est subdivisée en deux régions pour assurer une isolation des composants afin de limiter la zone de propagation d'une erreur humaine ou logique. Aucun composant ou équipement n'est partagé entre les régions, et seuls des flux IP assurent la communication d'une région à une autre. [5]

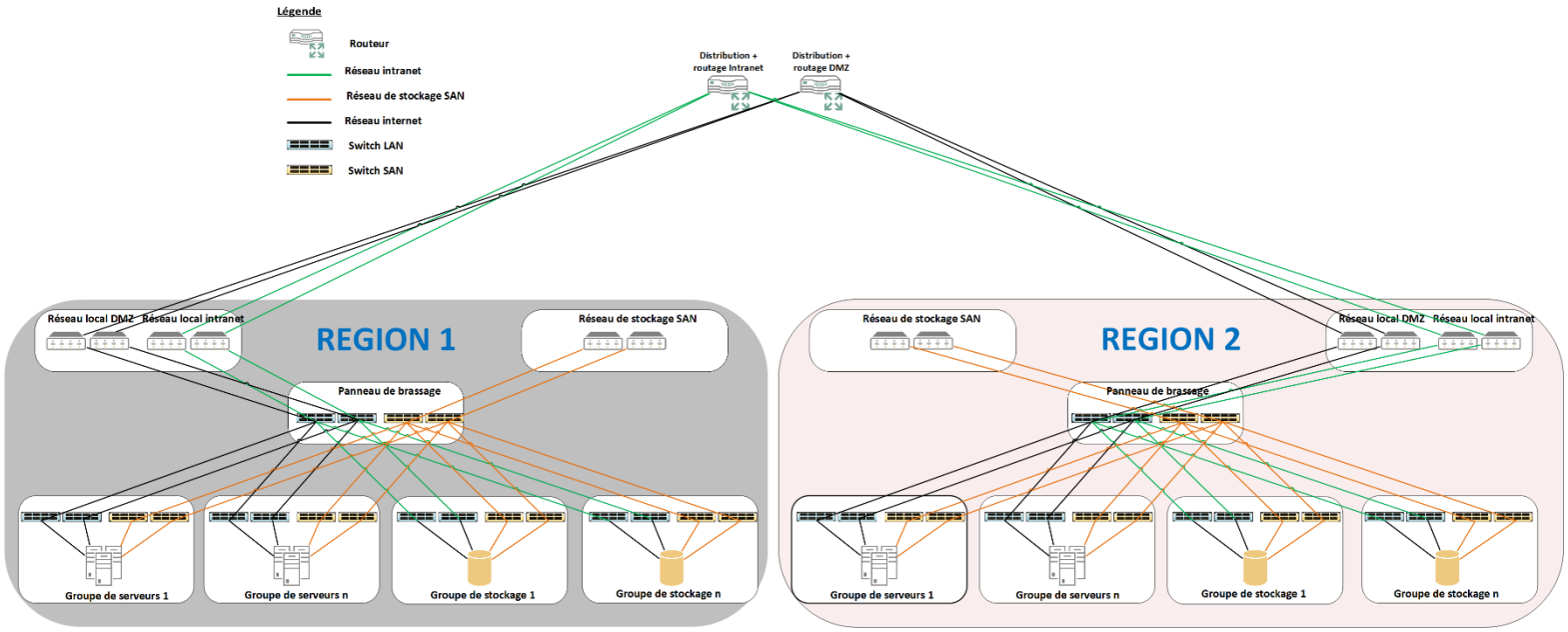

Figure 3 : cloisonnement des infrastructures du data center

2.2.1 Le Cloisonnement du réseau par zone de confiance

Les réseaux datacenter sont sur une instance de routage distincte des réseaux utilisateurs, et les partenaires sont sur un WAN distinct des sites du Groupe. Une action sur un cœur réseau n'affecte pas les autres. Le réseau de flux IP entre les deux zones du data center sont isolé.

2.2.3 Cloisonnement Logique SAN

Sur les systèmes de stockage SAN les deux mécanismes de cloisonnement utilisés sont les suivants :

2.2.3.1 Le zoning

Est un mécanisme configuré sur les switches d'une fabric SAN et permet de déterminer si un hôte à l'autorisation de communiqué avec une baie de stockage ou pas et de séparer la communication entre deux ou plusieurs hôtes connectés sur la même fabrique SAN.

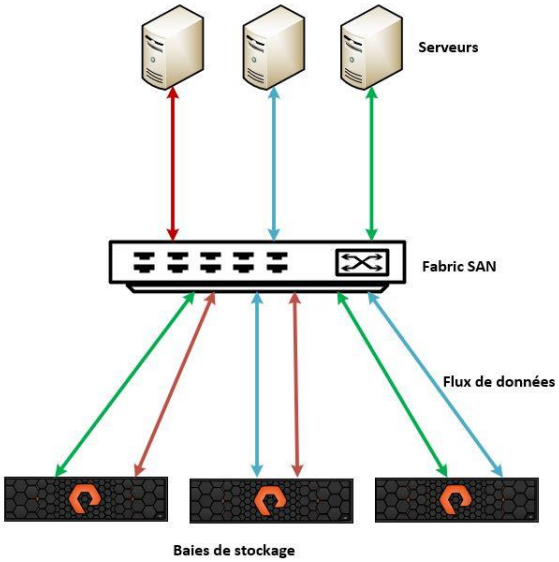

Figure 4 : le mécanisme de zoning SAN

2.2.3.2 Le Lun Masking

Les baies étant composé d'unité de stockage appelé Lun ou volume, ce mécanisme permet d'associer un volume à un hôte ou groupe de hôtes. Cela permet de protéger et isole les données de plusieurs hôtes connectés sur une même baie de stockage.

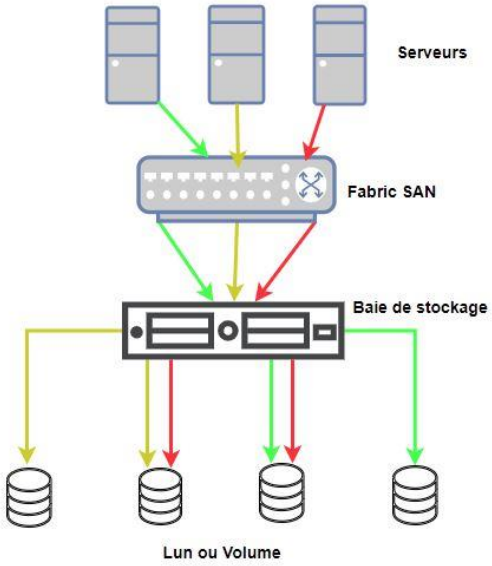

Figure 5 : mécanisme de Lun masking

2.3 Mécanisme et stratégie de protection des données

Pour éviter une perte totale des données au niveau de la production, les mécanismes suivants ont été mis en place :

2.3.1 La sauvegarde des données des systèmes de production

Cette sauvegarde concerne tous les serveurs critiques de production et est réalisée par la solution Commvault. En fonction du type de serveur et des données à sauvegarder, on a deux méthodes de sauvegarde :

- La sauvegarde applicative : qui nécessite l'installation de l'agent applicatif Commvault iDataAgent sur le serveur pour la sauvegarde des données applicatives.
- La sauvegarde serveur : qui nécessite l'installation du Virtual serveur agent (VSA) dans l'hyperviseur et permet de sauvegarder les disques virtuels des machines.

Une sauvegarde incrémentale des données modifiées depuis la dernière sauvegarde complète est réalisée du lundi au vendredi en fin de journée et une sauvegarde complète des données est réalisée le weekend.

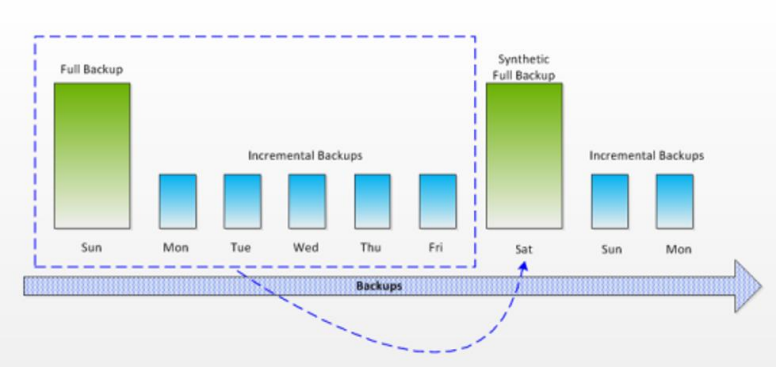

Figure 6 : typologie des sauvegardes du site de production

Ces sauvegardes sont stockées sur les infrastructures dédiées à Commvault du site de production. Les sauvegardes incrémentales et complètes sont conservées pendant 5 semaines minimum et la dernière sauvegarde complète du mois peut être conserver jusqu'à 12 mois pour les applications les plus critiques.

2.3.2 Les snapshots

C'est l'enregistrement à un instant T des données. Il est réalisé sur les baies de stockage de production, les volumes de données destinés aux applications sensibles sont regroupés en groupe de protection, un snapshot est réalisé chaque jour sur chaque groupe de protection et conserver sur les baies pendant une semaine. En cas de défaut d'intégrité, la restauration des données peut être réaliser à travers le snapshot.

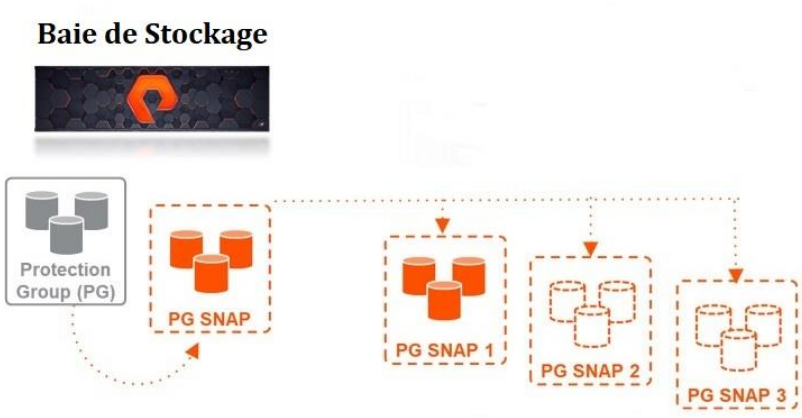

Figure 7 : snapshot des protections groupes

2.3.3 Réplication asynchrone des données des systèmes de stockages

Les volumes de données critiques au sein des baies de stockage de production sont regroupés en protection groupes. Un snapshot de chaque protection groupe est réalisé chaque jour, une copie est stockée sur la baie et une autre est transférée vers les baies de stockage de l'infrastructure de secours via le mécanisme de réplication asynchrone.

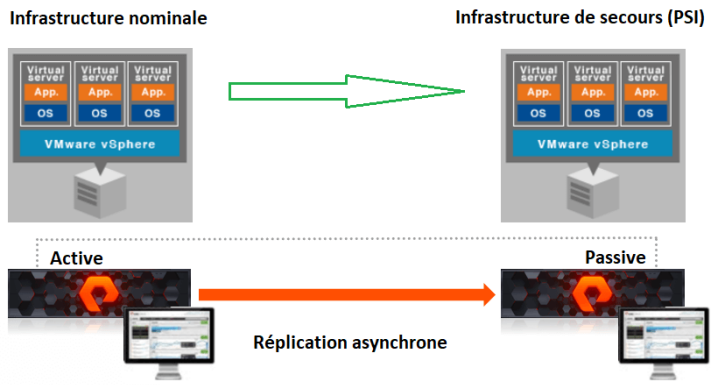

Figure 8 : réplication asynchrone des données de productions vers le site de secours

2.3.4 Réplication asynchrone des données des systèmes de sauvegarde

Les données des serveurs critiques sont sauvegardées de manière hebdomadaires sur les sur des infrastructures dédiées au sauvegarde. Une copie est stockée dans la zone de production et une copie est transférée aux infrastructures de sauvegarde de secours par le mécanisme de réplication Dash copy. Ces données sauvegardées sont conservées dans les l'infrastructure de secours pendant 5 semaines.

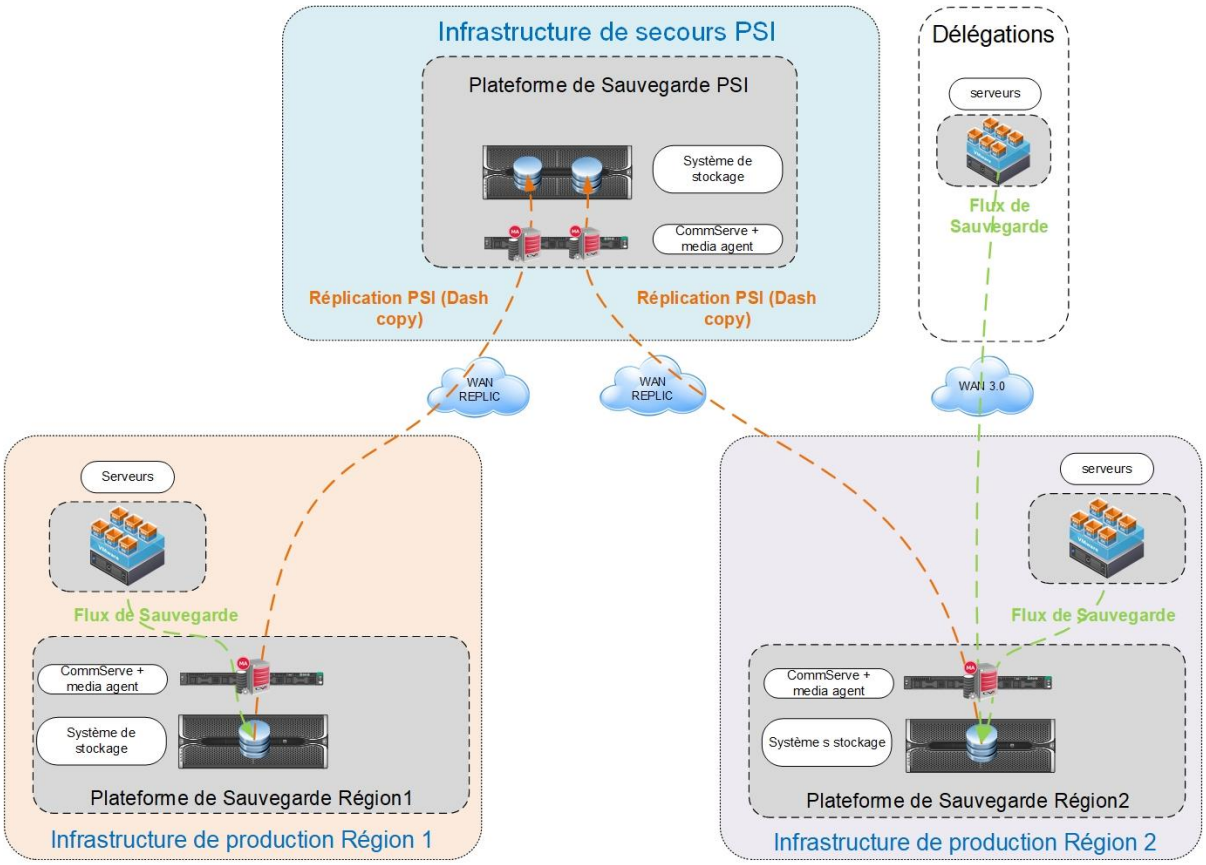

Figure 9 : réplication des sauvegardes de l'infras de production vers l'infras de secours

2.4 Administration et exploitation

L'administration et la gestion des serveurs et systèmes de stockage n'est autorisé qu'aux personnes habilitées. Les droits d'administration sur ces équipements sont définis en fonction des prérogatives du profil d'un utilisateur sur les dit systèmes. L'authentification des comptes administrateur est réalisé par un annuaire central qui gère les équipes infrastructures du groupe du groupe et auquel est rattaché les hyperviseurs et systèmes de stockages. Les connexions aux interfaces d'administration sont chiffrées via un certificat SSL délivré par l'autorité de certification du groupe et accessible uniquement depuis le réseau interne.

2.5 Maintien en condition opérationnelle

Pour assurer le bon fonctionnement de ses infrastructures, une évolution logicielle de l'infrastructure est effectuée régulièrement afin de conserver une infrastructure à un niveau de version supporté par le constructeur tout en bénéficiant de nouvelles fonctionnalités ou amélioration de fonctions existantes. Les opérations de maintenance sur l'infrastructures sont

réalisées par le mainteneur Stordata selon un contrat de maintenance signé avec AG2RLM en cas de découverte d'une vulnérabilité sur un système, le système peut être isolé ou les accès peuvent être restreint jusqu'à ce que le constructeur mette à disposition un patch correctif ou mise à niveau.

3. Le plan de continuité informatique

En temps de fonctionnement normale, les données de l'infrastructure de production sont répliquées quotidiennement vers le site de secours PSI. Les données de PSI sont répliquées chaque mois vers la plateforme de PSI CYBER. Cela permet de garantir la reprise du système d'information en cas d'indisponibilité totale de l'une de ces infrastructures et assurer un retour à la normale après résolutions des incidents ayant créés l'indisponibilité.

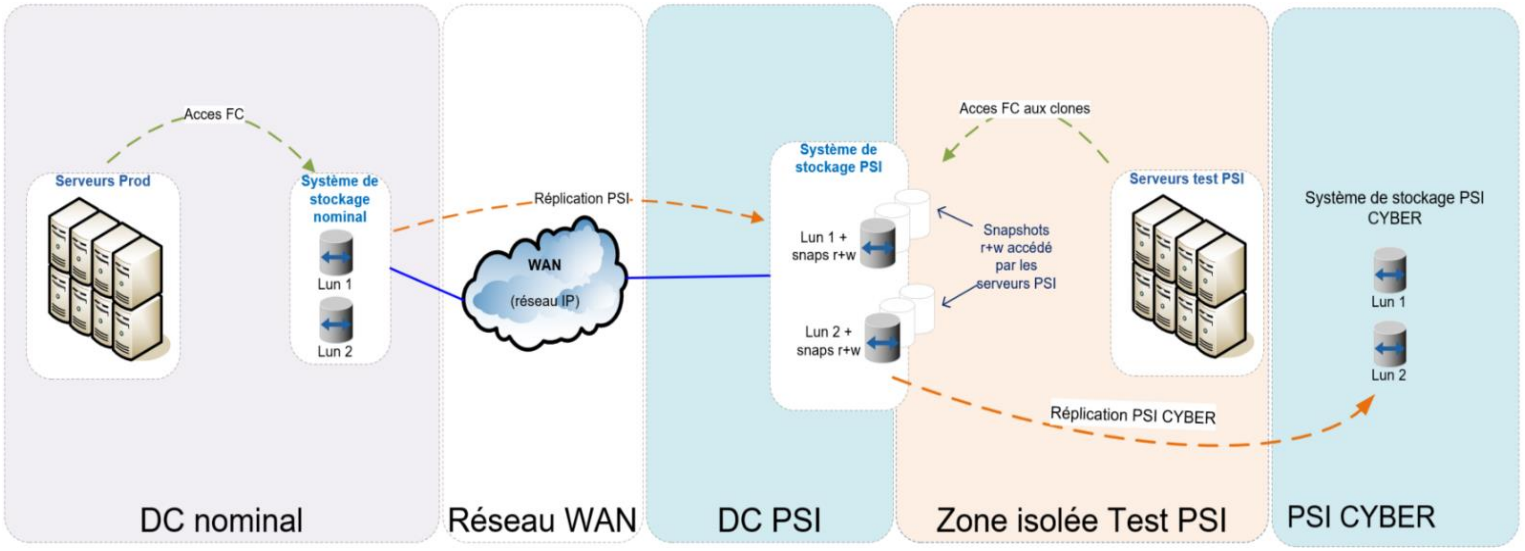

Figure 10 : plan de continuité informatique

Le plan de continuité informatique, est planifié de manière suivante :

3.1 Indisponibilité de l'infrastructure de production

En cas d'indisponibilité totale ou prolongée de l'infrastructure de production, le PSI ou plan de secours informatique est activé. Il consiste à connecter les serveurs physiques (hyperviseurs) aux systèmes de stockages de l'infrastructure de secours PSI pour redémarrer les serveurs virtualisés et les applications qu'ils hébergent.

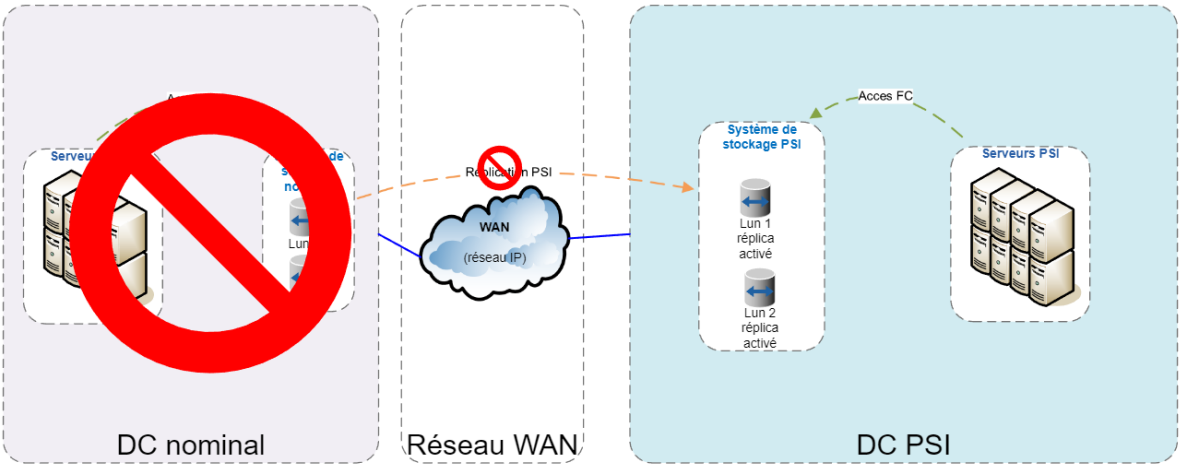

Figure 11 : activation du plan de secours informatique

3.2 Rétablissement du site de production

Pour assurer un retour à la normale, de l'infrastructure de production à la suite d'une indisponibilité totale ou prolongée, le processus de réplication des données sera inversé. Les données, collectées au sein de l'infrastructure de secours PSI, seront répliqué vers les systèmes de stockages de l'infrastructure de production afin rétablir le site de production et désactiver le plan de secours informatique.

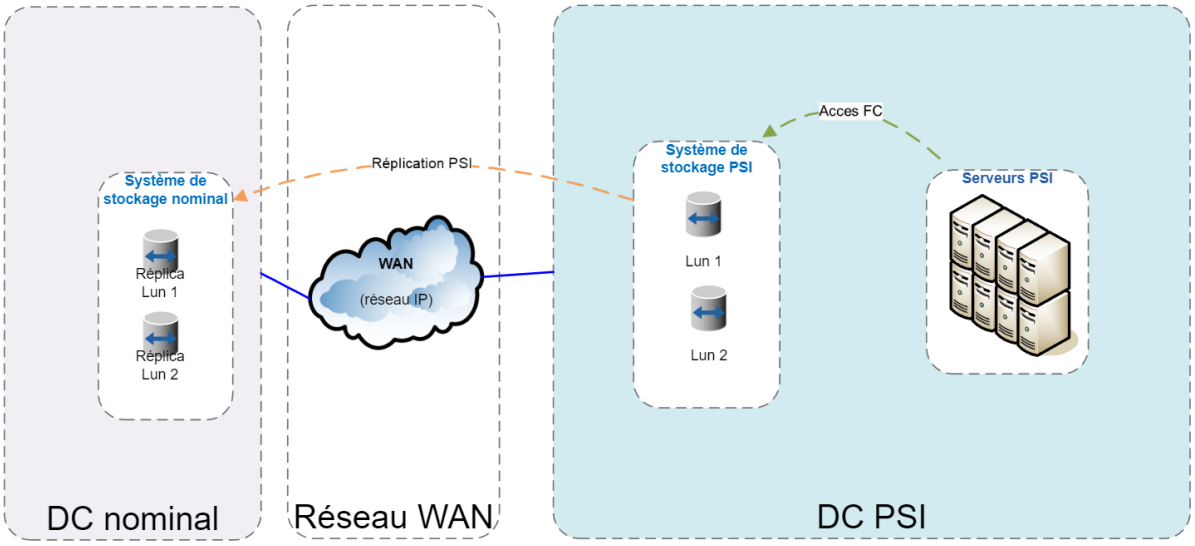

Figure 12 : Rétablissement du site de production après activation PSI

3.3 Indisponibilité de l'infrastructure de production et de PSI

C'est le scénario le plus envisageable par suite d'une cyberattaque ayant compromis les données de production et la réplication. Le seul recours pour redémarrer le système d'information est la sauvegarde hors connexion hébergée par la plateforme PSI CYBER.

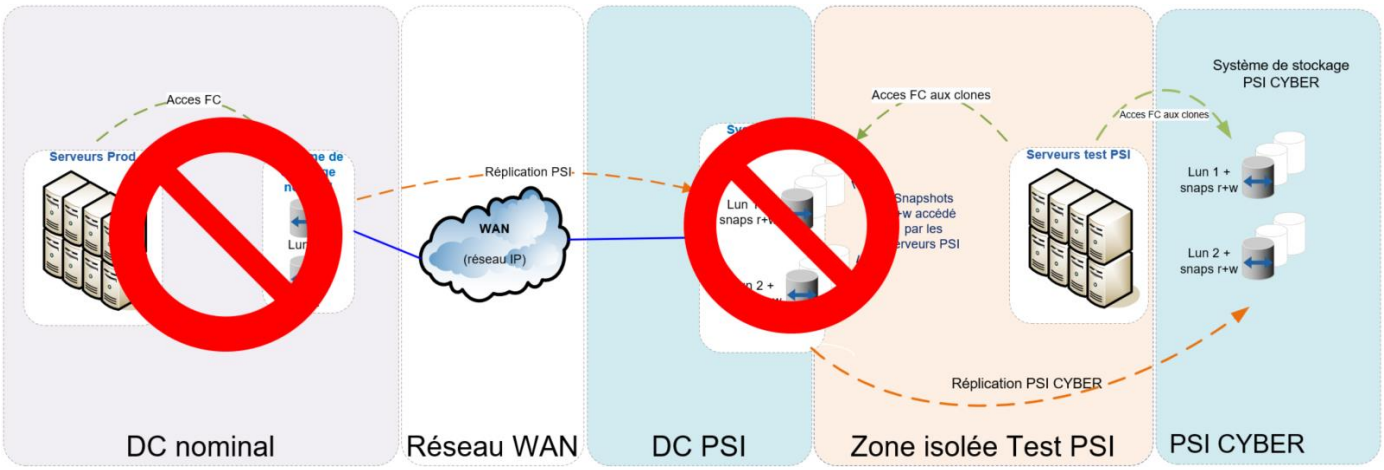

Figure 13 : activation du plan de secours PSI CYBER

Chapitre 4 : Critiques et suggestions face aux mécanismes et stratégies de protection des systèmes d'information du groupe AG2RLM

Après avoir présenté de manière synthétique, les mécanismes et stratégies implémentés pour assurer la protection du système d'information du groupe AG2RLM, il sera question de diagnostiquer les risques résiduels et si possible, de proposer des axes d'améliorations.

1. Les critiques et suggestions

Pour donner suite à notre analyse des stratégies et mécanismes implémentées pour assurer la protection et disponibilité du SI, j'ai relevé quelques points d'ombre et les axes d'amélioration pour les mitiger.

1.1 Améliorer le cloisonnement physique des systèmes de secours

Du point de vue du cloisonnement physique, l'infrastructure de PSI et celui de PSI Cyber est séparé par un grillage, ce qui laisse vulnérable les infrastructures de secours. En cas d'incendie toutes les données qu'elle contient seront perdues.

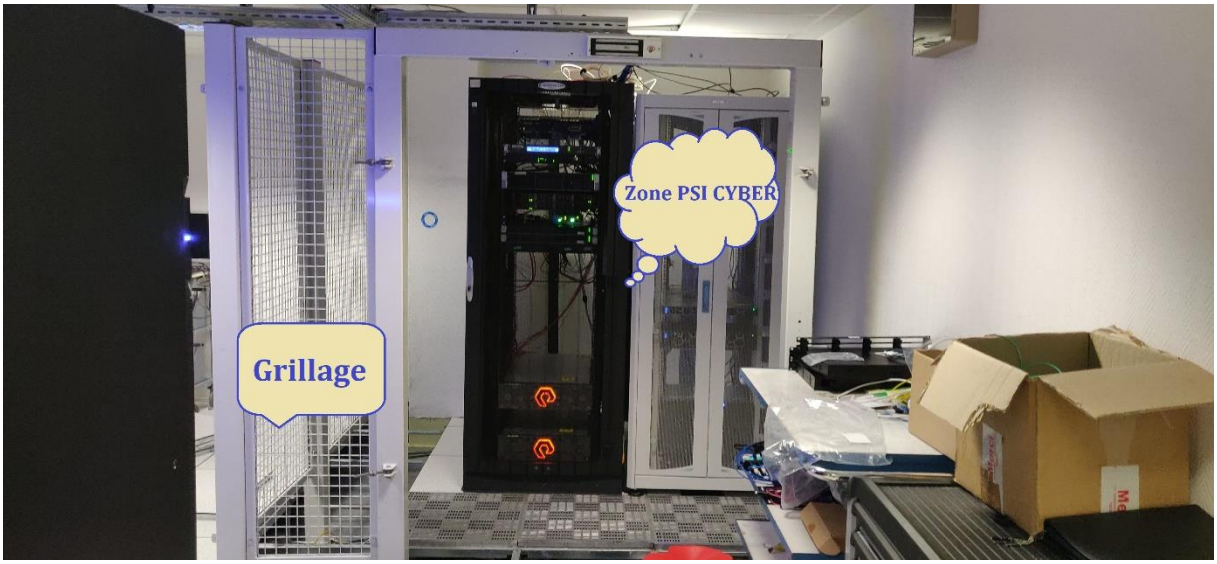

Figure 14 : installation du grillage pour la protection de la zone PSI CYBER

Suggestion : déplacer l'infrastructure de PSI CYBER vers une autre salle du bâtiment et restreindre les accès uniquement aux opérations de maintenance pour protéger les données quelle contient de toute attaque physique. Le groupe possède déjà des salles informatiques en

cours de décommissionnement dans le même bâtiment, cette proposition peut être réalisée à moindre frais.

1.2 Améliorer les stratégies de protection des données

1.2.1 l'exhaustivité des données stockées

La plateforme inaltérable ne conserve que les données applicatives critiques des serveurs de production. Cependant d'autres types de données sensibles et indispensables à l'activité des services métiers et aux équipes gérant le système d'information doivent être protégés pour assurer la continuité des services fournis en cas de compromission ou suppression de ceux de production. Ces données sont hébergées sur les systèmes de stockages de type NAS et ne sont pas protégées d'une altération par le PSI CYBER.

Suggestion : Dans un contexte d'évolution de la plateforme de sauvegarde inaltérable, ajouter de nouvelles extensions de stockage pour héberger des copies de données des systèmes de stockages NAS.

1.2.2 Protection des hyperviseurs pour le plan de secours

Pour assurer la relance des applications critiques après une indisponibilité involontaire, avec les données de PSI CYBER, il est primordial de reconstruite à l'identique l'environnement dans lequel les données ont été collectées et sauvegardées. Cet environnement est géré par le système d'exploitation hôte installé sur le matériel serveur. Ce système d'exploitation est représenté au sein de nos infrastructures pas les hyperviseurs de niveau 1 qui permettent de virtualiser les serveurs applicatifs. Il est installé sur un disque dur attaché directement au serveur. En cas de dégradation du système d'exploitation de ces serveurs le recovery time objective (RTO) du plan de secours informatique pourrait être fortement affecté, ou encore des virus rootkit pourraient être installés sur ces machines. Il devient critique de reconstruire les serveurs applicatifs virtuelles sans le système d'exploitation hôte.

Suggestion : protéger les systèmes d'exploitation des hyperviseurs nécessaires à la restauration des serveurs applicatifs virtuels. Je recommande la création des volumes « boot from SAN » dans les baies de PSI dédiés au système hyperviseur afin de les répliquer régulièrement vers les baies stockage de PSI CYBER. En cas de redémarrage des serveurs applicatives virtuels de puis la plateforme de PSI CYBER, les hyperviseurs pourront être démarrés à partir des leurs volumes boot from SAN directement dans les baies de stockage SAN.

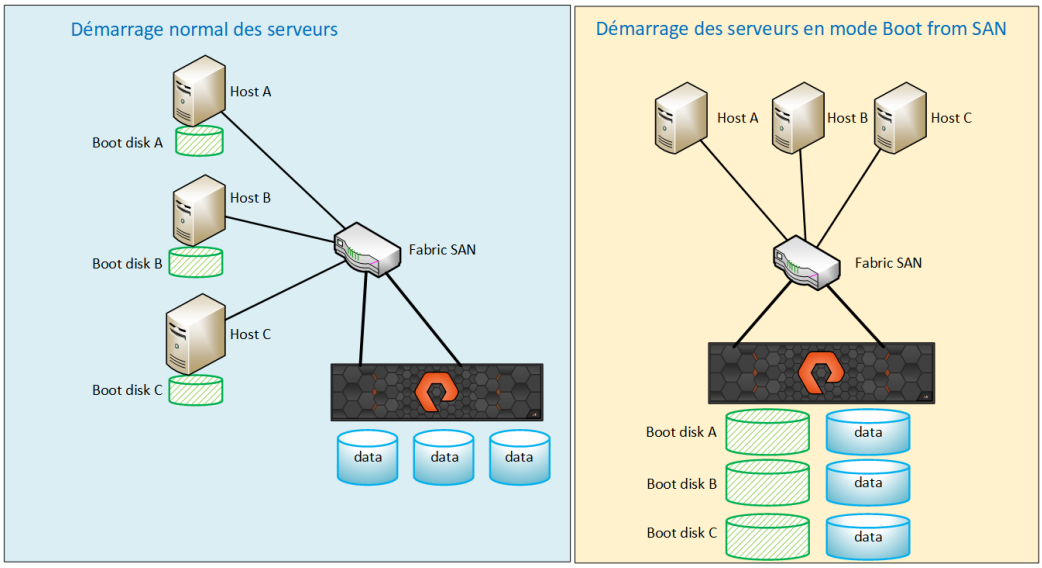

Figure 15 : mode boot from SAN des serveurs

1.2.3 Risque de conflit entre la stratégie de sauvegarde et le RGPD

Bien que la plateforme de sauvegarde inaltérable apporte une nouvelle couche de protection au données critiques du groupe, elle peut entrer en conflit avec les principes du règlement général sur la protection des données à caractère personnelle du fait de la rétention de ces données et les droits des personnes dont les données sont collectées. Dans le cas où une personne veut exercer son droit en demandant la suppression ou modification de ses données, celles-ci seront traitées sur les plateformes de productions mais aucun traitement ne sera opéré sur les copies de ses données présentes dans la plateforme inaltérable durant les 9 prochains mois. Si une restauration des plateformes de productions est réalisée à partir d'une sauvegarde de moins de 9 mois en PSI cyber, les modifications appliquées aux données après la réalisation de cette sauvegarde ne seront pas prises en compte.

Suggestion : je préconise une réflexion autour de la réduction du délai de rétention des données dans la plateforme de sauvegarde inaltérable, puisque cette copie des données de productions

est réalisée chaque mois. Cette réflexion devra prendre en compte les risques inhérentes à la sécurité cyber par rapport au risque du non-respect de la règlementation RGPD

1.2.4 Amélioration du cloisonnement de l'infrastructure de PSI CYBER

La plateforme de PSI cyber est isolé du réseau du réseau de production, cependant les serveurs CommVault de PSI CYBER et les leurs hyperviseurs restent eux joignables depuis le réseau de production pour la synchronisation des bases de données entre le serveur CommVault de PSI et celui de PSI CYBER, ouvrant ainsi un vecteur d'attaque par le biais du réseau SAN.

Suggestion : Je préconise une déconnexion des serveurs CommVault et ses hyperviseurs dans les périodes d'inactivité des réplications de données des systèmes de PSI vers celui de PSI CYBER.

1.2.5 Critique sur la fréquence de réplication et la durée de rétention des données par la plateforme de sauvegarde inaltérable

La plateforme de sauvegarde inaltérable permet de garder une copie des données des applications critiques chaque mois. Cette ultime copie des données est conservée pendant une période de 9 mois. Cet écart d'un mois entre les données de production et celles stockées par la plateforme de PSI CYBER créent une différence de version entre les données et augmentent la quantité maximale de données perdues en cas de destruction des données de production. La conservation de ces données, pendant 9 mois, entraîne une consommation du volume des baies de stockage avec des données qui, dans le cadre d'une restauration, créeront un énorme problème de cohérence au sein de nos services métiers.

Suggestion : je recommande, une nouvelle réflexion par les services métiers et l'équipe pilotage sur la fréquence des réplications des sauvegardes et la durée de rétention de ces données en zone PSI CYBER.

1.2.6 Critique sur la viabilité des sauvegardes de la plateforme de PSI CYBER

L'intérêt de sauvegarde de PSI CYBER est d'être en possession d'une ultime copie des données de productions sur lesquels l'entreprise peut s'appuyer pour restaurer son système d'information en cas de destruction ou compromission des systèmes nominaux et de secours. Ces sauvegardes, ne peuvent être utiles uniquement si elles sont viables. Toutefois, aucun processus ou mécanisme de relecture et de vérification de la viabilité n'a été défini.

Suggestion : planifier un test de la plateforme de PSI CYBER durant lequel on va présenter les baies de stockage de PSI CYBER aux serveurs de test pour relancer le système d'information à partir des données sauvegardées. Ce test doit être conforme à celui réalisé sur les données de PSI.

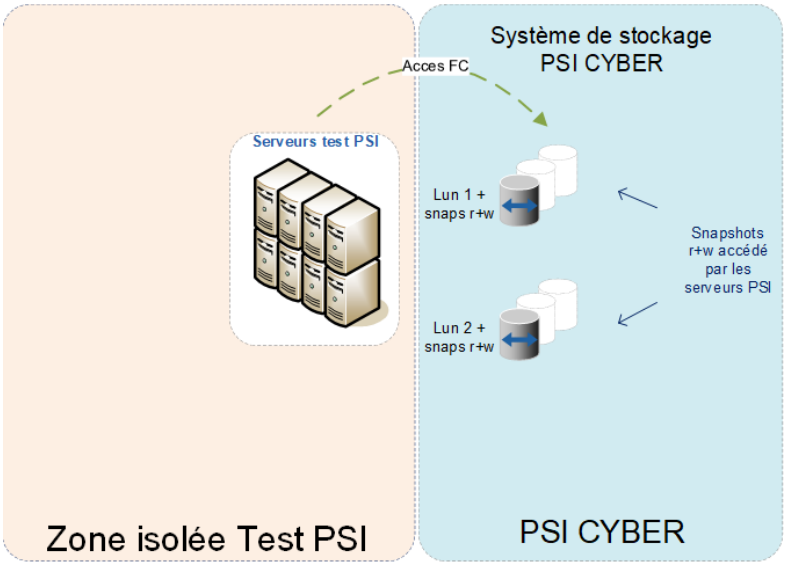

Figure 16 : test de viabilité des données de l'infrastructure de PSI CYBER

1.3 Critique sur l'administration des infrastructures

Les stations de travail utilisées par les équipes d'administration, conservent une grande quantité de renseignements (clés de chiffrements, fichiers de configurations, identifiant, etc..) nécessaires à l'administration. Ces stations de travail sont particulièrement sensibles et doivent être protégées en conséquence. Cependant, elles sont aussi utilisées pour accéder aux environnements de travail usuels (messagerie, gestion documentaire, outils de communication, internet, etc…) engendrant ainsi un faible niveau de sécurité puisqu'elles sont en permanence connectée à un réseau non fiable comme internet. Cela crée une surface d'attaque importante et expose les systèmes administrés par ces stations. Si les postes de travail sont compromis, un attaquant peut causer de graves dommages à l'intégrité et à la stabilité du système d'information.

Suggestion : à défaut d'allouer une station de travail dédié à l'administration pour chaque membre de l'équipe d'administration, ce qui est laborieux pour un collaborateur d'avoir deux stations de travail pour un même poste, on pourrait mettre sur pied une infrastructure de poste de travail virtuel (VDI) connecté sur le réseau de management des infrastructures du système

d'information. Une infrastructure VDI représente un poste de travail virtuel hébergé par un serveur sur un hyperviseur de niveau 1, elle est accessible depuis le terminal d'un utilisateur grâce à un client installé sur le terminal du client ou depuis un navigateur. Elle doit permettre de centraliser l'administration de l'infrastructure et augmenté la sécurité des plateformes critiques, car aucun n'échange de données entre le terminal physique de l'utilisateur et la station virtuelle ne sera possible.

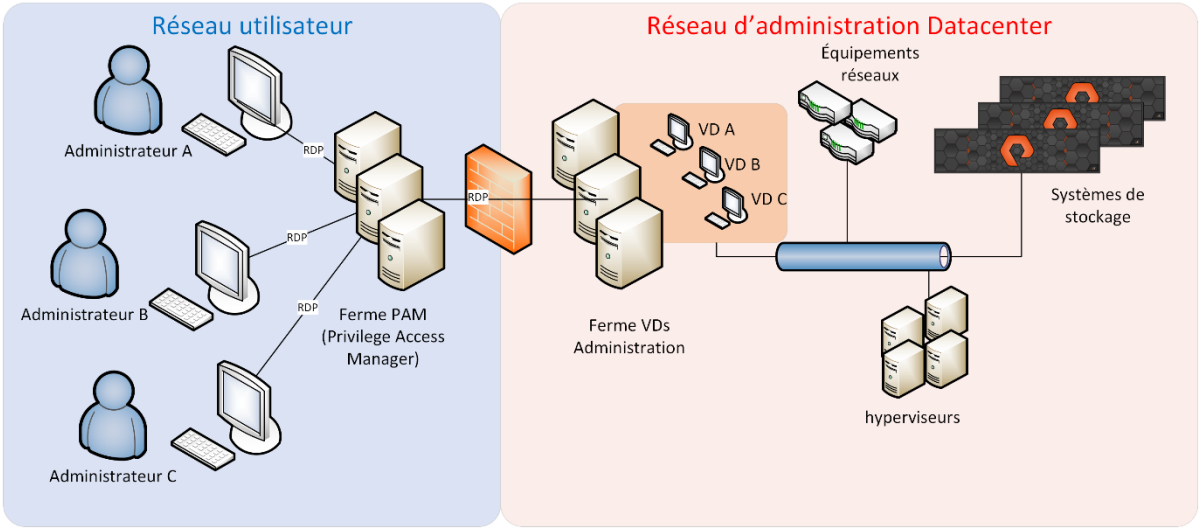

Figure 17 : Architecture VDI dédié à l'administration

1.4 Critique sur la procédure de maintenance de la plateforme de PSI CYBER

Pour assurer la sécurité de la plateforme et des éléments qu'elles contiennent, des opérations de maintenance doivent être réalisées pour la maintenir opérationnelle. Cependant, ces équipements sont isolés du réseau de l'entreprise, aucun accès à distance n'est possible. De plus, les seules informations de contrôles sont les logs et les scripts d'inventaire des baies de stockage, aucune vérification des manipulations effectuées sur ces équipements n'est contrôlée depuis le réseau de productions. Le fait qu'une personne, peut se retrouver seule auprès de ces données sensibles constitue un risque de sabotage ou hacktivisme.

Suggestion : Tout accès à cette plateforme dans l'optique de réaliser une opération qui peut affecter partiellement ou totalement son fonctionnement doit faire l'objet au préalable d'une demande auprès du service pilotage du SI. Cette demande doit présenter de manière explicite les manipulations à effectuer au sein de cette infrastructure et les équipements cibles. Après validation de la demande l'équipe pilotage SI doit affecter un responsable de AG2LM pour assister le technicien dans la réalisation de ses manipulations.

Conclusion

La protection des SI reste un enjeu de taille sur lequel chaque entreprise doit veiller pour assurer la pérennité de son activité. Elle résulte d'un processus d'amélioration continue composée de mécanismes et de stratégies nécessaires au maintien en condition opérationnelle des différents composants du SI.

Dans ce mémoire, j'ai examiné les règles de protection des réseaux et des SI auxquelles sont assujettis les opérateurs de services essentiels, pour exprimer des critiques à l'égard de ces applications au sein de notre entreprise ainsi que les pistes d'amélioration. Ces règles d'administration, de sécurité de l'architecture et de contrôle des accès ont été définies par la directive NIS pour protéger les SI nécessaires à la continuité des activités économiques et sociales des pays de l'union européenne.

Au cours de mon analyse, j'ai relevé des écarts sur la mise en place de ces règles de protection. Ces écarts peuvent être considérés, d'une part, comme des risques résiduels qui ne sont pas pris en compte dans le présent règlement et, d'autre part, comme des pistes d'amélioration. Les solutions proposées, ne permettent pas toutes de mitiger les écarts, car l'implémentation de certaines d'entre elles à l'exemple du temps de conservation des données de la plateforme de sauvegarde inaltérable et son impact sur le règlement RGPD, qui doit faire l'objet d'une étude préalable par les directions métiers et des risques dans la meure ou ils mettent directement en péril la stratégie de sécurité des données actuellement définie.

Enfin, l'intégration de ces différentes critiques et des axes d'amélioration dans le processus d'amélioration continue de protection des données et son SI, permettrait au groupe AG2RLM de renforcer sa politique de résilience. Toutefois, les mécanismes et stratégies décrits ici ne sont pas exhaustifs en ce qui concerne la protection des SI.

Bibliographie

[1] Hiscox Assurances, «Rapport sur la gestion des cyber risques,» 2020.

[2] ANSSI, «UN DISPOSITIF DE CYBERSÉCURITÉ POUR LES OPÉRATEURS DE SERVICES ESSENTIELS,» [En ligne]. Available: https://www.ssi.gouv.fr/administration/reglementation/directive-nis/nis-un-dispositif-de-cybersecurite-pour-les-operateurs-de-service-essentiel/. [Accès le MAI 2020].

[3] légifrance, *Arrêté du 14 septembre 2018 fixant les règles de sécurité et les délais mentionnés à l'article 10 du décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de,* 2018.

[4] Marsh, «Cyber résilience : 12 points de controles pour renforcer votre sécurité,» 2021.

[5] A. L. MONDIALE, «architecture de sauvegarde et stockage,» 2020.

[6] M. Bose, «nakivo.com,» 30 Novembre 2021. [En ligne]. Available: https://www.nakivo.com/blog/wp-content/uploads/2021/11/One-ESXi-host-fails-and-vSphere-HA-initiates-VM-failover.jpg. [Accès le 18 aout 2022].

[7] AG2R LA MONDIALE, «convergence des data center,» 2018.

[8] ANSSI, «Recommandations pour la protection des systemes d'information essentiels,» 18 12 2020. [En ligne]. Available: https://www.ssi.gouv.fr/uploads/2020/12/guide_protection_des_systemes_essentiels.pdf.

[9] A. F. d. l. S. Numérique, «Guide des mécanismes de protection de l'intégrité des données stockées,» 2017.

Liste des figures