Sarah KOMBAR
Ahmad ZIAB
Mohamed Amine EL BAH
Cyril TILHOU-TRIEP

CESI
ÉCOLE D'INGÉNIEURS

Livrable 2 :

Administration du Système d'Information

Novembre 2023

Sommaire

I. Résumé

Lors du dernier livrable, nous avons étudié le réseau de l'entreprise ABSTERGO afin de tirer nos conclusions sur l'état du système. Nous avons aussi suggéré des améliorations possibles au Système d'Information existant.

II. Introduction

Contexte

Dans le cadre de la modernisation et de la sécurisation de son infrastructure, ABSTERGO envisage de refondre son Système d'Information (SI). Ce processus implique l'adoption de nouvelles technologies et pratiques pour renforcer la sécurité, améliorer l'efficacité et garantir la conformité avec les normes de qualité et les meilleures pratiques de l'industrie. Le Livrable 2 se concentre sur la proposition d'une infrastructure révisée qui aborde les aspects critiques du SI, notamment l'authentification, la virtualisation, la supervision, la sauvegarde, la maintenance, la continuité des activités, et la sécurité intégrée.

Contenu détaillé :

1. **Authentification :**
    - Discussion sur les différentes techniques d'authentification disponibles, telles que l'authentification à deux facteurs (2FA), l'authentification multifacteur (MFA), les certificats numériques, l'authentification biométrique, etc.
    - Analyse des avantages et des inconvénients de chaque méthode en fonction du contexte d'ABSTERGO.
    - Recommandations pour une solution d'authentification robuste qui protège les identités et les accès.
2. **Virtualisation/Conteneurisation :**
    - Comparaison des options de virtualisation et de conteneurisation, en mettant en évidence les différences en termes de performance, d'isolation des ressources, de gestion, etc.
    - Évaluation de la pertinence de chaque technologie pour le nouveau SI.
    - Recommandations sur la solution la mieux adaptée pour ABSTERGO, en tenant compte des besoins futurs et actuels.
3. **Supervision :**
    - Importance de la supervision proactive pour la santé du SI et la détection précoce des problèmes.
    - Proposition d'une solution de supervision qui couvre les exigences spécifiques d'ABSTERGO.
4. **Politique de sauvegarde :**

- Élaboration d'une politique de sauvegarde qui reflète les exigences du métier d'ABSTERGO, en incluant les types de données, la fréquence de sauvegarde, et les protocoles de restauration.
- Présentation des meilleures pratiques en matière de sauvegarde et de restauration.

5. **Pare-feu :**
    - Importance des pares-feux dans la protection du SI d'ABSTERGO.
    - Analyse des différents pares-feux sur le marché.
    - Proposition d'une solution de pare-feu qui couvre les exigences spécifiques d'ABSTERGO.
6. **Cryptographie :**
    - Importance de la cryptographie dans la protection des données transmises sur le réseau.
    - Présentation de diverses méthodes de cryptographie.
    - Choix de la méthode de cryptage des données.
7. **Relations d'approbation :**
    - Cas d'utilisation des relations d'approbation.
    - Différentes caractéristiques des relations d'approbation.
8. **Schéma de l'infrastructure intégrant la sécurité :**
    - Présentation d'un schéma détaillé du nouveau SI, mettant en évidence les mesures de sécurité intégrées à chaque niveau.
9. **Contrat de maintenance :**
    - Description de l'importance d'un contrat de maintenance solide pour assurer une performance optimale et une gestion efficace des pannes.
    - Points clés qui devraient être inclus dans le contrat d'ABSTERGO pour garantir la couverture des aspects critiques.
10. **Plan de reprise d'activité/Plan de continuité :**
    - Définition et différenciation du Plan de Reprise d'Activité (PRA) et du Plan de Continuité d'Activité (PCA).
    - Stratégies pour la mise en œuvre de ces plans chez ABSTERGO, en mettant l'accent sur la minimisation des temps d'arrêt et la préservation de l'intégrité des données.

Ce livrable servira de feuille de route pour les décisions stratégiques concernant la refonte de l'infrastructure SI d'ABSTERGO, en mettant l'accent sur la robustesse, la résilience, et la conformité.

Problématique

Comment présenter la nouvelle infrastructure, démontrer sa viabilité, et mettre en avant la sécurité, tout en intégrant les notions vues en cours et les recommandations précédentes ?

III. Renforcement de la Sécurité du S.I.

Dans l'état actuel, nous avons constaté que le système d'information (S.I) d'ABSTERGO possède un niveau de sécurité très faible.

Plusieurs problèmes ont été identifiés : par exemple, l'historique a révélé que l'entreprise utilisait un seul mot de passe pour toutes ses machines, sans option de double authentification, le rendant vulnérable aux attaques de type "man-in-the-middle" ou aux intrusions directes, donnant accès à toutes les machines.

Pour remédier à ces problèmes, nous identifierons dans cette partie les méthodes d'authentification les plus appropriées, les comparerons et les recommanderons. Ensuite, nous mettrons en place des solutions de cryptographie pour sécuriser le S.I contre les attaques physiques et à distance.

1. Authentification

Définition

L'authentification est le processus de vérification de l'identité d'une personne, d'un système informatique ou d'un appareil électronique pour garantir qu'ils sont qui ils prétendent être. C'est une étape essentielle dans la sécurité des systèmes et des données, car elle permet de contrôler l'accès aux ressources sensibles et de protéger contre les utilisateurs non autorisés.

Techniques d'authentification

Il existe de nombreux types d'authentifications, chacun adapté à des besoins spécifiques en matière de sécurité et de commodité. Voici certains des types d'authentifications les plus courants :

- **Authentification par nom d'utilisateur et mot de passe** : L'utilisateur doit fournir un nom d'utilisateur et un mot de passe pour accéder à un système ou un compte. C'est l'une des méthodes les plus répandues, bien qu'elle puisse être vulnérable aux attaques par force brute si les mots de passe sont faibles.
- **Authentification à deux facteurs (2FA)** : En plus du nom d'utilisateur et du mot de passe, l'utilisateur 8 doit fournir une deuxième forme d'authentification, comme un code généré par une application sur son smartphone ou une clé de sécurité matérielle.
- **Authentification à trois facteurs (3FA)** : Outre le nom d'utilisateur et le mot de passe, cette méthode exige trois formes d'authentification, généralement quelque chose que l'utilisateur sait (mot de passe), quelque chose que l'utilisateur a (comme un smartphone), et quelque chose que l'utilisateur est (comme une empreinte digitale).
- **Authentification biométrique** : Elle se base sur les caractéristiques physiques ou comportementales uniques de l'utilisateur, telles que les empreintes digitales, l'iris, la reconnaissance faciale, la reconnaissance vocale, etc.
- **Authentification par carte à puce** : L'utilisateur insère une carte à puce ou une carte intelligente (comme une carte d'identité électronique) dans un lecteur de carte pour s'authentifier.
- **Authentification par certificat numérique** : L'utilisateur possède un certificat numérique délivré par une autorité de certification. Ce certificat est utilisé pour prouver l'identité de l'utilisateur.
- **Authentification basée sur le protocole RADIUS** : Utilisée principalement dans les réseaux, l'authentification RADIUS (Remote Authentication Dial-In User Service) permet aux utilisateurs de s'authentifier à distance, souvent utilisée dans les connexions sans fil et les connexions VPN.

- **Authentification basée sur le protocole Kerberos** : Il s'agit d'un protocole de sécurité qui permet l'authentification mutuelle entre les utilisateurs et les services dans un environnement de réseau.
- **Authentification sociale** : L'utilisateur s'authentifie en utilisant des informations provenant de services de médias sociaux, tels que se connecter avec son compte Facebook ou Google.
- **Authentification par code PIN** : L'utilisateur doit entrer un code PIN (numéro d'identification personnel) pour accéder à un système ou un compte.
- **Authentification par l'appareil** : L'authentification est basée sur les propriétés uniques de l'appareil utilisé, comme l'adresse 0MAC de l'appareil.
- **Authentification par clé de sécurité** : Les clés de sécurité matérielles, telles que les clés USB de sécurité, génèrent des codes à usage unique pour l'authentification.
- **Authentification sans mot de passe** : Des méthodes émergentes telles que l'authentification sans mot de passe utilisent des informations comportementales, des données biométriques ou des informations contextuelles pour authentifier les utilisateurs sans avoir besoin de mots de passe traditionnels.

Choix de la méthode d'authentification :

Au regard des différentes techniques disponibles, il est impératif d'évaluer la méthode la plus adaptée pour ABSTERGO.

L'implémentation d'une authentification à deux facteurs, dont au moins un des facteurs serait physique, semble être l'alternative optimale pour ABSTERGO. Parmi les nombreuses méthodes applicables, l'authentification biométrique ainsi que l'utilisation de cartes à puce sont des options pertinentes.

Authentifications biométriques :

Pour l'authentification biométrique, celle-ci est naturellement intégrée via Windows, mais a un certain coût. En effet, l'authentification biométrique par scanner d'empreinte digitale peut coûter entre 20 et 30€ par poste. Cependant, cette méthode d'authentification représente un investissement uniquement dédié à la reconnaissance de l'utilisateur. Si le budget est une contrainte pour l'entreprise, il serait plus judicieux d'envisager une solution offrant une double fonctionnalité malgré un prix potentiellement plus élevé. Une telle option pourrait être des webcams compatibles avec Windows Hello, permettant une reconnaissance faciale rapide et efficace. Windows Hello, utilisant un système de scan 3D du visage, est très difficile à tromper. Le fait qu'il soit intégré aujourd'hui à des caméras à 70€ le rend attractif, offrant à chaque poste une capacité de communication en ligne en plus de l'authentification, réalisant ainsi une économie.

Pour l'accès à distance, de nombreux ordinateurs portables modernes sont équipés d'un capteur d'empreintes intégré et d'une caméra Windows Hello, les rendant compatibles avec les deux méthodes d'authentification.

Authentification par carte à puce :

En ce qui concerne les cartes à puces, cette méthode d'authentification offre un avantage majeur car elle est, par défaut, intégrée à AD/DS et pourrait être utilisée pour remplacer le mot de passe de

l'utilisateur. Cela permettrait à ce dernier de s'authentifier très rapidement sur n'importe quel poste, éliminant ainsi les problèmes d'oubli de mot de passe.

Cette méthode ne peut cependant pas être utilisée seule. En effet, le vol d'une carte est une tâche assez aisée. La combiner avec Windows Hello pourrait rendre le système extrêmement robuste.

Toutefois, ce système engendre également un coût qui pourrait s'avérer élevé pour l'entreprise, dépendant du budget disponible et du nombre de postes à moderniser. En effet, il est possible de trouver des lecteurs de cartes à des tarifs variant entre 20 et 40€ par poste.

Pour ce qui est de l'accès à distance, rares sont les ordinateurs portables équipés de lecteurs de cartes d'accès. Il faudra donc se tourner vers des offres professionnelles, qui sont souvent moins attractives en termes de rapport puissance/coût.

Tableau récapitulatif du niveau de risque et couts pour les méthodes d'authentification identifiées :

Afin d'identifier quelle méthode était la plus juste à l'utilisation pour le cas d'ABSTERGO, nous avons dressé un tableau permettant de calculer le niveau de sécurité, pondérer par la facilité d'utilisation et de mise en place, le tout mettant en avant le prix et la versatilité.

Tableau 1: Récapitulatif des méthodes d'authentification

Méthodes d'authentification	Prix/postes	Utilité double ?	Score risque (plus bas = mieux)
Mot de passe uniquement	0	Non	2
Reconnaissance faciale uniquement	70 €	Oui	-2
Carte à puce uniquement	30 €	Oui	1
Empreinte digitale uniquement	20 €	Non	-2
Reconnaissance faciale + mot de passe	70 €	Oui	-5
Carte à puce+ Mot de passe	30 €	Oui	-1
Empreinte digitale + Mot de passe	30 €	Non	-2
Carte à puce + Empreinte digitale	50 €	Oui	-5
Carte à puce + Reconnaissance faciale	100 €	Oui (2)	-8
Empreinte digitale + Reconnaissance faciale	90 €	Oui	-6

Ce tableau est une version simplifiée de celui que vous trouverez dans le document complémentaire « risques cout autentification.xlsx » où les critères utilisés pour cette étude sont détaillés en profondeur.

De cette étude, nous concluons que les méthodes sans mot de passe sont généralement les plus sûres et les plus agréable pour les utilisateurs.

Les mots de passe, bien qu'ils soient une contrainte pour les utilisateurs et vulnérables à plusieurs types d'attaques (phishing, force brute, keylogging), présentent des avantages. Ils sont purement logiciels et n'entraînent pas de coûts supplémentaires, à l'exception de la gestion des oublis de mots de passe par l'équipe informatique. Les mots de passe sont facilement intégrables à tous les systèmes et simples à déployer. Ils sont également non discriminatoires ; certaines personnes peuvent avoir des empreintes digitales endommagées ou un visage non identifiable par les caméras Windows Hello.

Il ressort également que les cartes à puce ne sont pas aussi sécurisées qu'on le pense. Elles peuvent être volées et combinées avec du keylogging (dans le cas d'un 2FA avec mot de passe) pour accéder aux machines en l'absence de l'utilisateur. Toutefois, elles offrent l'avantage de réguler l'accès aux bureaux, assurant un suivi des mouvements et améliorant la sécurité physique et logicielle de l'environnement de travail.

L'association d'une carte à puce et de la reconnaissance faciale offre une authentification efficace, rapide, simple à mettre en œuvre, polyvalente et sécurisée. Pourquoi préférer la reconnaissance faciale aux empreintes digitales ? Si un voleur s'empare de la carte d'accès, il lui est plus facile de copier l'empreinte digitale que de tromper la reconnaissance faciale.

Windows Hello n'est pas seulement une méthode d'authentification, mais aussi un standard exigeant que les caméras puissent scanner la forme du visage, ce qui garantit une authentification efficace malgré des changements mineurs tels qu'une barbe ou une coiffure. L'unique façon de s'authentifier serait de posséder un modèle 3D exact du visage de l'utilisateur.

Le choix le plus logique semble donc être de choisir cette méthode. Et pourtant, ce n'est pas forcément le choix le plus judicieux

Choix final de méthode d'authentification :

Notre choix final c'est tourner sur la mise en place de la reconnaissance faciale + mot de passe : cette méthode d'authentification est extrêmement robuste et pourrait facilement être mise en place pour 30% d'économie par postes comparer au combo Carte à puce + Windows hello.

2. Virtualisation/Conteneurisation

HYPERVISEURS :

Définition

Un hyperviseur, également connu sous le nom de moniteur de machine virtuelle, est un logiciel ou un matériel qui permet la virtualisation. Il permet de créer et de gérer des machines virtuelles (VM) sur un serveur physique, ce qui permet à plusieurs systèmes d'exploitation et applications de fonctionner indépendamment les uns des autres sur le même matériel.

Isolation des VM : Les hyperviseurs offrent une isolation forte entre les machines virtuelles (VM).

Utilisation des ressources : Les hyperviseurs consomment généralement plus de ressources car chaque VM nécessite un système d'exploitation complet. Cela peut entraîner une utilisation moins efficace des ressources matérielles.

Taille des images : Les images de VM sont généralement plus grandes que les conteneurs, car elles incluent un système d'exploitation complet.

Temps de déploiement : Le déploiement de VM peut prendre plus de temps en raison de la nécessité d'installer et de configurer un système d'exploitation complet.

Compatibilité : Les hyperviseurs sont capables de virtualiser divers systèmes d'exploitation, y compris des systèmes invités Windows et Linux.

Isolation de l'environnement : Les hyperviseurs offrent une isolation plus robuste, ce qui les rend adaptés aux charges de travail nécessitant une isolation stricte.

Mise en réseau : Les hyperviseurs nécessitent souvent une configuration de réseau plus complexe pour connecter les VM au réseau.

CONTENEURISATION :

Définition

La conteneurisation se réfère à un environnement logiciel légère et isolée qui encapsule une application et ses dépendances pour faciliter le déploiement sur différentes plateformes et pour mieux gérer et manipuler les applications par les autres sans avoir des obstacles de dépendances ou des erreurs.

Isolation des conteneurs : Les conteneurs partagent le même noyau de système d'exploitation sous-jacent, ce qui signifie qu'ils ne sont pas aussi isolés que les VM. Cependant, ils offrent une isolation suffisante pour la plupart des cas d'utilisation.

Utilisation des ressources : Les conteneurs sont plus efficaces en termes d'utilisation des ressources, car ils partagent le noyau du système d'exploitation. Donc mieux que le VM.

Taille des images : Les images de conteneurs sont plus petites, car elles ne contiennent que les dépendances nécessaires à l'application.

Temps de déploiement : Les conteneurs se déploient rapidement car ils n'ont pas besoin d'installer un système d'exploitation complet. Ils sont prêts à l'emploi une fois que les dépendances sont configurées.

Compatibilité : La conteneurisation est principalement orientée vers les applications basées sur Linux, bien qu'il existe des solutions pour exécuter des conteneurs Windows.

Isolation de l'environnement : Les conteneurs offrent une isolation plus légère, ce qui les rend adaptés aux charges de travail où l'isolation est moins critique.

Mise en réseau : Les conteneurs partagent souvent le même réseau que l'hôte, ce qui simplifie la configuration du réseau.

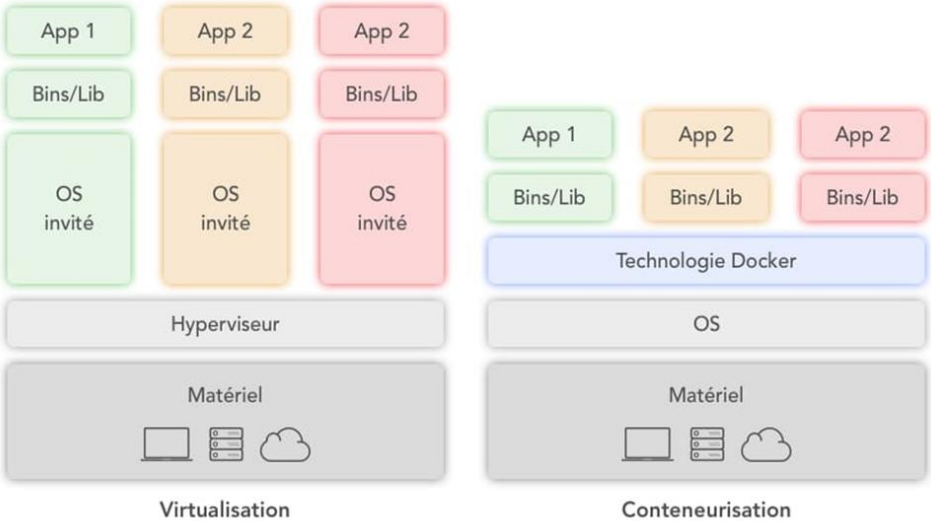

Figure 1: Comparaison Virtualisation et Conteneurisation | Source : BigInt [1]

Nous allons donc mettre en place une plateforme d'orchestration de conteneurs. Avant de faire ceci, nous allons comparer les systèmes d'orchestration les plus connus, d'où [2] :

Tableau 2 2: Etude comparative des systèmes d'orchestration

	Avantages	***Inconvénients***
Docker Swarm	○ Rapide à installer et à configurer ○ Déploiement et évolutivité rapide des conteneurs en grands clusters ○ Haute disponibilité fournie par la réplication des conteneurs ○ Fonctionne avec d'autres outils Docker existants	○ Limité par l'API Docker ○ N'offre pas d'outils intégrés pour gérer le logging ou le monitoring ○ Tolérance aux pannes limitée
Kebernets	○ Fournit de solides garanties aux états du cluster ○ Haute disponibilité fournie par la réplication des conteneurs ○ Organisation de service facile avec pods	○ Grand nombre de configurations manuelles ○ Difficile de changer de plateforme (définitions YAML à réécrire) ○ Déploiement lent
Apache Mesos	○ Flexibilité de personnalisation et d'implémentation de contraintes plus complexes ○ Supporte de très grandes échelles	○ Installation et configuration complexe
Cloud Foundry	○ Prise en main facile ○ Mise à l'échelle instantanée ○ Déploie en utilisant des images docker et des buildpacks	○ Impossible de personnaliser ses déploiement

D'après nos études, Docker Swarm semble être plus adapte à nos besoins. En effet, c'est facile à installer et à configurer et nous n'avons pas besoin d'aller à grand échelle.

3. Supervision des Systèmes

Définition

La supervision des systèmes consiste en l'observation continue d'une infrastructure par un responsable IT. Elle englobe le contrôle des processeurs, de la mémoire des serveurs, des routeurs, des commutateurs, de la bande passante et des applications, mais aussi la supervision des performances et de la disponibilité des périphériques réseau les plus importants.

La supervision permet d'éviter les erreurs qui se produisent dans le système d'information. Sans elle, les problèmes ne peuvent être traités qu'après qu'ils se soient produits. Ceci présente bien-sûr des risques et la résolution peut prendre du temps. D'autre part, la supervision par petits outils dédiés ne fournit pas une vue d'ensemble sur les éléments à surveiller. Le système de supervision permet donc de gagner du temps, épargner des dépenses tout en offrant une solution effective.

Afin de pouvoir garder un œil sur le système d'information, il faudra mettre en place un système de supervision. Ce dernier est un logiciel qui supervise les périphériques système, le trafic et les applications, et donne l'alerte en cas de dysfonctionnement ou de perturbation. Son utilisation nécessitera de le centrer sur le processus, la mémoire, le stockage et les connections réseaux puis d'établir un protocole de résolution de problème. [3]

- ***Systèmes de supervision***

Il existe plusieurs logiciels de supervision dont nous noterons les avantages et les inconvénients des plus populaires [4] [5] [6]:

Tableau 3 3: Etude comparative des systèmes de supervision

	Avantages	***Inconvénients***
Centreon	○ Interface Web facile à utiliser ○ Permet de faire une configuration personnalisée ○ Diffusion en temps réel des informations sur le tableau de bord (processeur, RAM, espace disque dur…) ○ Richesse des plugins	○ Difficile à faire évoluer ou à faire maintenir par des tiers (plugins) ○ Certains modules sont payants (ex : MAP) ○ Problèmes de compatibilité : trop de versions
Nagios	○ Large variété de représentation visuelles et rapports des résultats ○ Possibilité de hiérarchiser les résultats et les données ○ Richesse des plugins	○ Interface Web complexe ○ Configuration de bout en bout et fastidieuse, nombre important de fichiers de configuration ○ Difficile à faire évoluer ou à faire maintenir par des tiers (plugins) ○ Pauvre dans la gestion SNMP
	○ Logiciel libre	○ Performance diminue à partir de plus de mille nœuds de réseau

Zabbix	○ Facile à configurer ○ Couvre la surveillance des états et les performances du S.I. ○ Affichage personnalisable à l'utilisateur	○ Pas de rapports en temps réel ○ Difficile de créer et de définir des modèles d'alerte et de rapport ○ Mauvais traitement des déroutements
Ganglia	○ Spécialisé pour les systèmes de calcul haute performance (S.I., grappes et réseaux hauts performance) ○ Utilisé par Cray, MIT, NASA et Twitter/X	○ Mode opératoire spécifique et complexe ○ Tableau de bord difficile à prendre en main
Zenoss	○ Rapports très pertinents sur les nœuds de réseau ○ Tableau de bord personnalisable, flexible et puissant ○ Capacité de surveiller plusieurs plateformes ○ Grande capacité de gestion d'évènement	○ Moins performant que les autres ○ Version libre très limitée ○ Complexité d'installation et des éléments à surveiller ○ Ne peut pas être intégré à d'autres bases de données ○ Manque de clarté dans les cartes topologiques

D'après les informations reçues, nous pouvons voir que Centreon semble être la meilleure solution de supervision.

4. Politique de Sauvegarde

Définition

Afin d'assurer la sécurité des données, il est nécessaire de faire des sauvegardes régulières.

Ces sauvegardes vont servir, en cas de problème, à restaurer les bases de données dans un état le plus proche possible du moment où le problème est survenu.

Cependant, le jour où une restauration sera nécessaire, il est possible que la personne qui a mis en place les sauvegardes ne soit pas présente. C'est pour cela qu'il est essentiel d'écrire et de maintenir un document qui indique la mise en place de la sauvegarde et qui détaille comment restaurer une sauvegarde.

En effet, suivant les besoins, les outils pour sauvegarder, le contenu de la sauvegarde, sa fréquence ne seront pas les mêmes.

Par exemple, il n'est pas toujours nécessaire de tout sauvegarder. Une base de données peut contenir des données de travail, temporaires et/ou faciles à reconstruire, stockées dans des tables standards. Il est également possible d'avoir une base dédiée pour stocker ce genre d'objets. Pour diminuer le temps de sauvegarde (et du coup de restauration), il est possible de sauvegarder partiellement son serveur pour ne conserver que les données importantes.

La fréquence peut aussi varier. Un utilisateur peut disposer d'un serveur PostgreSQL pour un entrepôt de données, serveur qu'il n'alimente qu'une fois par semaine. Dans ce cas, il est inutile de

sauvegarder tous les jours. Une sauvegarde après chaque alimentation (donc chaque semaine) est suffisante. En fait, il faut déterminer la fréquence de sauvegarde des données selon :

- Le volume de données à sauvegarder et/ou restaurer.
- La criticité des données.
- La quantité de données qu'il est « acceptable » de perdre en cas de problème.

Le support de sauvegarde est lui aussi très important. Il est possible de sauvegarder les données sur un disque réseau (à travers SMB/CIFS ou NFS), sur des disques locaux dédiés, sur des bandes ou tout autre support adapté. Dans tous les cas, il est fortement déconseillé de stocker les sauvegardes sur les disques utilisés par la base de données.

Ce document doit aussi indiquer comment effectuer la restauration. Si la sauvegarde est composée de plusieurs fichiers, l'ordre de restauration des fichiers peut être essentiel. De plus, savoir où se trouvent les sauvegardes permet de gagner un temps important, qui évitera une immobilisation trop longue.

De même, vérifier la restauration des sauvegardes de façon régulière est une précaution très utile.

Objectif

L'objectif essentiel de la sauvegarde est la sécurisation des données. Autrement dit, l'utilisateur cherche à se protéger d'une panne matérielle ou d'une erreur humaine (un utilisateur qui supprimerait des données essentielles). La sauvegarde permet de restaurer les données perdues. Mais ce n'est pas le seul objectif d'une sauvegarde. [8]

Une sauvegarde peut aussi servir à dupliquer une base de données sur un serveur de test ou de préproduction. Elle permet aussi d'archiver des tables. Cela se voit surtout dans le cadre des tables partitionnées où l'archivage de la table la plus ancienne permet ensuite sa suppression de la base pour gagner en espace disque.

Différentes approches de la sauvegarde

La sauvegarde au niveau système de fichiers permet de conserver une image cohérente de l'intégralité des répertoires de données d'une instance arrêtée. C'est la sauvegarde à froid. Cependant, l'utilisation d'outils de snapshots pour effectuer les sauvegardes peut accélérer considérablement les temps de sauvegarde des bases de données, et donc diminuer d'autant le temps d'immobilisation du système.

La sauvegarde logique permet de créer un fichier texte de commandes SQL ou un fichier binaire contenant le schéma et les données de la base de données.

La sauvegarde à chaud des fichiers est possible avec le Point In Time Recovery.

Suivant les prérequis et les limitations de chaque méthode, il est fort possible qu'une seule de ces solutions soit utilisable. Par exemple :

- Si le serveur ne peut pas être arrêté, la sauvegarde à froid est exclue d'office ;

- Si la base de données est très volumineuse, la sauvegarde logique devient très longue ;
- Si l'espace disque est limité et que l'instance génère beaucoup de journaux de transactions, la sauvegarde PITR sera difficile à mettre en place.

RTO/RPO

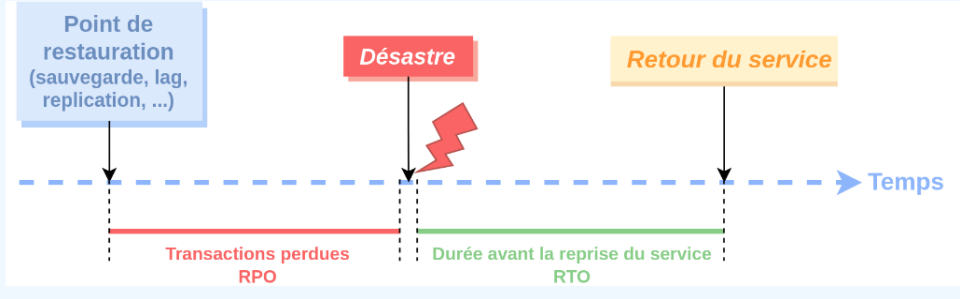

Figure 2: Principe du RTO/RPO [8]

La politique de sauvegarde découle du :

- **RPO** (*Recovery Point Objective*): Perte de Données Maximale Admissible faible ou importante ?
- **RTO** (*Recovery Time Objective*): Durée Maximale d'Interruption Admissible courte ou longue ?

Le RPO et RTO sont deux concepts déterminants dans le choix des politiques de sauvegardes. La RPO (ou PDMA) est la perte de données maximale admissible, ou quantité de données que l'on peut tolérer de perdre lors d'un sinistre majeur, souvent exprimée en heures ou minutes. Pour un système mis à jour épisodiquement ou avec des données non critiques, ou facilement récupérables, le RPO peut être important (par exemple une journée). Ils peuvent alors s'envisager des solutions comme :

- Les sauvegardes logiques (dump) ;
- Les sauvegardes des fichiers à froid.

Dans beaucoup de cas, la perte de données admissible est très faible (heures, quelques minutes), voire nulle. Il faudra s'orienter vers des solutions de type :

- Sauvegarde à chaud ;
- Sauvegarde d'instantané à un point donnée dans le temps (PITR) ;
- Réplication asynchrone, voire synchrone.

La **RTO** (ou DMIA) est la durée maximale d'interruption du service.

Dans beaucoup de cas, les utilisateurs peuvent tolérer une indisponibilité de plusieurs heures, voire jours. La durée de reprise du service n'est alors pas critique, on peut utiliser des solutions simples comme :

- La restauration des fichiers ;
- La restauration d'une sauvegarde logique (dump).

Si elle est plus courte, le service doit très vite remonter. Cela nécessite des procédures avec un minimum d'acteurs et de manipulation :

- Réplication.
- Solutions HA (Haute Disponibilité).

Politique 3-2-1

Une politique de sauvegardes « 3-2-1 » est une appellation mnémonique pour un système basé sur les principes suivants :

- 3 copies au moins des données protégées, les données primaires et deux sauvegardes.
- 2 médias & systèmes, parce que chaque support (disque dur / bande) ou système (SAN / NAS) peut être un point de défaillance unique ; la première sauvegarde se trouve sur site, pour une capacité de reconstruction rapide.
- 1 site externe pour la deuxième sauvegarde afin de disposer d'une ressource ultime, même si un événement catastrophique touchait le premier site.

Si le nom est facile à mémoriser, la mise en œuvre demande du soin pour éviter des « découvertes douloureuses » comme :

- Des ensembles RAID ne constituent pas un original et une copie de sauvegarde, même en mode miroir ; des ensembles RAID forment un procédé qui améliore la disponibilité et les performances en lecture mais les défaillances de disques ne sont pas indépendantes (en particulier pour les systèmes à parité qui sollicitent soudainement et fortement les disques quand un premier disque est détecté comme défaillant).
- Les sauvegardes chaînées (original, sauvegarde sur site, sauvegarde hors site) sans contrôle d'intégrité à chaque étape ne font que propager les erreurs

Formaliser la politique de sauvegardes

Les obstacles à des sauvegardes systématiques ne sont donc pas ni la faisabilité, ni la disponibilité des technologies mais un manque d'organisation opérationnelle. C'est pourquoi la première étape pour une entreprise ou organisation, consiste à formaliser une politique de sauvegardes standardisée. Cette politique indique les moyens et garanties apportées par la politique de sauvegardes :

- Protection contre les défaillances de sites ou de supports : plan de sauvegardes « 3-2-1 »
- Protection contre les corruptions techniques : contrôle d'intégrité et notification
- Protection contre les corruptions lentes : historique sur plusieurs mois
- Protection contre les divulgations de données par l'accès aux sauvegardes : chiffrement par la source
- Protection contre les erreurs de manipulation des utilisateurs : réduction du délai entre sauvegardes successives (de 1j à 1h pour les espaces de documents) et historisation « d'instantanés » [9]

Amélioration du système d'information Abstergo avec les politiques de sauvegarde

Pour améliorer notre système d'information Abstergo avec des politiques de sauvegarde nous devons tout d'abord mettre en place un cahier d'évaluation de notre système pour identifier les données essentielles les bases de données, les documents et les placer en ordre de priorité. [10]

1. CONSTRUIRE ET PROTÉGER

- Définissez une politique de sauvegarde en identifiant les données critiques pour l'activité de votre entreprise et en précisant la fréquence à laquelle il est important de les sauvegarder.
- Considérez les opérations de sauvegarde et de restauration comme des opérations sensibles d'administration devant bénéficier des protections adéquates : poste d'administration durci, flux dans un réseau d'administration, etc.
- Rendez indépendante votre infrastructure de sauvegarde vis-à-vis de vos annuaires de production (Active Directory, etc.).
- Assurez-vous du contrôle d'accès à vos sauvegardes pour garantir qu'elles ne seront ni modifiées ni altérées et toujours disponibles, en particulier dans le cadre de l'utilisation d'offres de sauvegarde Cloud.
- Soyez vigilant sur la sensibilité des données sauvegardées en cas de solution hors-site, dans un cloud public ou chez un prestataire externe. Chiffrez les sauvegardes au préalable par vos propres moyens si nécessaire.
- Faites évoluer continuellement votre infrastructure de sauvegarde au même rythme que l'évolution de vos SI (virtualisation, cloud, etc.) et en fonction de l'évolution de la menace. Ne conservez pas une infrastructure obsolète en production

2. ANTICIPER ET RÉAGIR

- Définissez une stratégie de restauration, en lien avec votre PRA et en tenant compte des principaux scénarios d'attaque identifiés sur vos SI (rançongiciels, espionnage, etc.). Réalisez régulièrement des tests de restauration. Impliquez la direction sur les modes dégradés acceptables en cas de crise Cyber.
- N'oubliez pas d'inclure les médias d'installation et les configurations de vos applications métier dans vos sauvegardes.
- Réalisez régulièrement et impérativement des sauvegardes hors-ligne (déconnectées du SI).
- Prévoyez une procédure d'isolation d'urgence du système de sauvegarde (serveurs, médias, etc.) en cas de suspicion de compromission ou d'attaque en cours.
- Après un incident, tenez compte du fait que vos sauvegardes peuvent contenir les vecteurs de compromission. Restaurez à partir de sources de confiance (images officielles, binaires d'installation signés), contrôlez la conformité des configurations, faites un scan antivirus des données.

Pour notre système d'information Abstergo on va utiliser un type de sauvegarde basé sur plusieurs critères qui sont :

- La fréquence des sauvegardes
- Les méthodes de sauvegarde soit incrémentielle ou complète
- Les périodes de rétention des données
- Les méthodes de stockage

- Sécurité des données soit par le chiffrement ou l'authentification
- Les tests de restauration
- Catalogue de donnés pour bien décrire les données et ces emplacements

Dans notre projet on va faire un serveur de backup (Windows Server 2019) et on va le connecter au serveur principal.

On va utiliser la politique de sauvegarde 3-2-1 pour la sauvegarde et on va suivre ces éléments clés pour assurer le fonctionnement de sauvegarde.

Type de données : documents, images, tableaux Excel, rapports, documents contiennent des règlementations, contrats, confidentialité de société

Importance des données : critique, il Ya des documents sensibles

Fréquence de sauvegarde : chaque semaine, lors de fin de semaine le vendredi

Type de sauvegarde : complète

Périodes de rétention : 4 semaines

Méthodes de stockage : stockage sur site et stockage distant (cloud)

Chiffrement :

Toutes les sauvegardes devraient être chiffrées pour protéger la confidentialité des données par un algorithme RSA.

Test de restauration :

Planifiez des tests de restauration réguliers pour vous assurer que vous pouvez effectivement récupérer les données en cas de besoin.

RTO (Recovery Time Objective) :

RPO (Recovery Point Objective) :

Conformité réglementaire :

L'assurance que les politiques de sauvegarde sont conformes légalement aux règlementations, C'est comme vérification juridique.

Budget :

5. Pare-feu

Définition

Les pares-feux permettent de filtrer le contenu et la communication malveillante ou potentiellement indésirable avant d'arriver sur le réseau de la société. Ceux-ci fonctionnent comme un contrôleur d'accès entre les réseaux interne et externe. Les pares-feux peuvent être un système logiciel ou matériel.

L'utilisation d'un pare-feu est essentielle dans un système d'information puisqu'il permet d'empêcher de renforcer sa sécurité. En effet, le pare-feu constitue un premier cordon de sécurité et empêche les menaces externes d'accéder au système en détectant le trafic potentiellement dangereux et en filtrant les informations. Le pare-feu empêche les hackeurs de pénétrer dans le système, mais également de s'approprier les données sensibles de la société sans y être autorisés. De plus, si l'entreprise possède un réseau composé de plusieurs terminaux connectés à Internet, le pare-feu crée un point d'entrée unique dans lequel les menaces éventuelles peuvent être identifiées et atténuées. [11]

Nous allons donc chercher à mettre en place un pare-feu pour protéger le système d'information ABSTERGO. Nous allons donc comparer les pares-feux les plus utilisés [12] [13] [14] :

Tableau 4 : 4Etude comparative des pares-feux

	Avantages	***Inconvénients***
Pfsense	○ Installation relativement simple ○ Bonne stabilité et évolutivité ○ Bonne détection des intrusion, protection et inspection du contenu ○ Nécessite moins de matériel ○ Logiciel libre	○ Peut nécessiter des services proxy supplémentaires ○ Configuration efficace nécessite de compétences élevées
Untangle	○ Interface simple à utiliser ○ Fournit des droits de gestion de la bande passante ○ Tableau de bord simplifié qui permet suivre et de surveiller facilement les menaces	○ Fonctionnalités très basiques ○ Pas beaucoup de documents d'assistance ○ Peu flexible
USG	○ Bonne évolutivité ○ Facile à gérer ○ Beaucoup de fonctionnalités	○ Problèmes de performances liés au filtrage du contenu des chaînes en direct ○ Ne fonctionne pas quand le trafic est intense
Cisco Secure Firewall	○ Installation relativement simple ○ Support excellent ○ Bonne stabilité et évolutivité ○ Fonctionnalités d'accès a distance, VPN et ACL	○ Interface peut être mieux ○ Droits de licence et extensions trop chers ○ Peu de fonctionnalités

D'après les capacites de ABSTERGO, nous proposerons d'utiliser le système Pfsense comme pare-feu.

6. Cryptographie

Définition :

La cryptographie est l'art et la science de sécuriser les communications et les informations en utilisant des techniques de chiffrement, de déchiffrement et de protection des données. Elle vise à rendre les données illisibles pour toute personne non autorisée, tout en permettant aux parties légitimes de déchiffrer et d'accéder aux informations de manière sécurisée.

Chiffrement :

Le chiffrement est le processus de transformation des données en un format illisible et inintelligible, appelé texte chiffré, à l'aide d'un algorithme mathématique et d'une clé. Le but du chiffrement est de protéger les données contre l'accès non autorisé ou la lecture par des tiers indésirables. Lorsque des données sont chiffrées, elles ne peuvent être lues que par des personnes ou des entités possédant la clé de déchiffrement appropriée.

Comment le chiffrement fonctionne :

Le chiffrement est un processus de protection des données en les transformant en un format illisible à l'aide d'un algorithme et d'une clé. Imaginez que vous avez un message que vous souhaitez garder secret. Vous utilisez une formule mathématique (l'algorithme de chiffrement) et une clé spéciale pour brouiller ce message et le transformer en un jargon incompréhensible (le texte chiffré). Vous pouvez partager ce texte chiffré en toute sécurité, car il est impossible à déchiffrer sans la clé appropriée. Une fois que le destinataire possède la clé, il peut utiliser l'algorithme de déchiffrement pour retrouver le message original. Le chiffrement est essentiel pour sécuriser les communications, protéger les données et garantir que seules les personnes autorisées peuvent accéder aux informations. C'est une méthode cruciale pour préserver la confidentialité et la sécurité des données dans le monde numérique.

Les types des chiffrements :

Il existe différents types de chiffrement, chacun ayant ses caractéristiques et ses utilisations spécifiques :

- **Chiffrement symétrique :** Dans ce type de chiffrement, la même clé est utilisée pour à la fois le chiffrement et le déchiffrement des données. Cela signifie que la personne qui chiffre les données et celle qui les déchiffre doivent partager la même clé secrète. Le chiffrement symétrique est généralement plus rapide que le chiffrement asymétrique, mais il pose le défi de sécuriser la clé partagée. Des exemples de chiffrement symétrique incluent AES (Advanced Encryption Standard) et DES (Data Encryption Standard).
- **Chiffrement asymétrique** : Aussi appelé chiffrement à clé publique, ce type de chiffrement utilise deux clés distinctes : une clé publique et une clé privée. La clé publique est utilisée pour chiffrer les données, tandis que la clé privée est utilisée pour les déchiffrer. La clé publique peut être partagée librement, tandis que la clé privée doit être conservée secrète. Le chiffrement asymétrique est couramment utilisé pour des tâches telles que la signature numérique et l'échange sécurisé de clés. RSA et ECC (Elliptic Curve Cryptography) sont des exemples de chiffrement asymétrique.

- **Chiffrement de bout en bout** : Il s'agit d'une application du chiffrement asymétrique où les données sont chiffrées par l'expéditeur et ne sont déchiffrées qu'à destination, en garantissant que même le fournisseur de services intermédiaire n'a pas accès aux données en clair. Des services de messagerie sécurisée comme Signal et WhatsApp utilisent le chiffrement de bout en bout.
- **Chiffrement de disque** : Il consiste à chiffrer l'intégralité d'un disque dur ou d'un volume de stockage. Toutes les données stockées sur ce disque sont automatiquement chiffrées, ce qui garantit leur sécurité en cas de vol ou d'accès non autorisé. BitLocker pour Windows et FileVault pour macOS sont des exemples de chiffrement de disque.
- **Chiffrement de fichiers** : Plutôt que de chiffrer un disque entier, le chiffrement de fichiers permet de chiffrer des fichiers ou des dossiers individuels. Les fichiers chiffrés nécessitent une clé pour être lus. Des outils comme VeraCrypt et 7-Zip offrent des options de chiffrement de fichiers.
- **Chiffrement de communications** : Il est utilisé pour sécuriser les communications entre deux parties. Le chiffrement SSL/TLS est couramment utilisé pour sécuriser les connexions Internet, tandis que le chiffrement de courrier électronique (comme S/MIME et PGP) permet de chiffrer les e-mails.
- **Chiffrement homomorphique** : C'est un type spécial de chiffrement qui permet de traiter des données chiffrées sans avoir besoin de les déchiffrer. Cela a des applications dans le calcul sécurisé en préservant la confidentialité des données.

Comparaison entre chiffrement et cryptage :

Le terme "chiffrement" et le terme "cryptage" sont souvent utilisés de manière interchangeable, mais il y a une différence subtile entre les deux.

Chiffrement

Le chiffrement est un processus de transformation des données en un format illisible en utilisant un algorithme mathématique et une clé. Le but est de protéger les données en rendant difficile leur lecture par des tiers non autorisés.

Il est généralement associé à la protection des données, de la confidentialité et de la sécurité. Le chiffrement est utilisé pour sécuriser les données sensibles et empêcher leur accès non autorisé.

Le terme "chiffrement" est souvent utilisé dans le contexte de la sécurité de l'information et des communications.

Cryptage (en anglais "encryption")

Le terme "cryptage" est parfois utilisé de manière interchangeable avec "chiffrement", mais il peut également être utilisé pour décrire le processus de conversion des données en un format chiffré.

Bien que le terme "cryptage" soit moins courant que "chiffrement", il est néanmoins correct du point de vue technique.

Dans de nombreux cas, le terme "cryptage" est utilisé de manière informelle ou dans des contextes moins techniques.

Des méthodes de chiffrements :

CHIFFREMENT DE HILL

Le chiffrement de Hill est une technique de chiffrement par substitution polygraphique, ce qui signifie qu'elle remplace des groupes de lettres (ou des paires de lettres, appelées "digrammes") par d'autres groupes de lettres en utilisant une matrice mathématique. Le chiffrement de Hill a été inventé par Lester S. Hill en 1929 et est considéré comme l'un des premiers chiffrements à clé publique.

Le chiffrement de Hill fonctionne en utilisant ces éléments :

- **Matrice de clé** : Pour chiffrer un message à l'aide du chiffrement de Hill, une matrice de clé est utilisée. Cette matrice est généralement une matrice carrée, et sa taille dépend de la longueur de la clé. Par exemple, si la matrice de clé est de taille 2x2, elle ressemblera à ceci :
  [a b]
  [c d]
  Les valeurs a, b, c et d sont des nombres entiers qui composent la clé de chiffrement.
- **Chiffrement** : Pour chiffrer un message, il est d'abord divisé en groupes de lettres, généralement par paires (digrammes). Chaque digramme est converti en une matrice colonne correspondante en utilisant un système d'affectation de nombres aux lettres. Par exemple, dans un système basé sur l'alphabet anglais, "A" pourrait être égal à 0, "B" à 1, "C" à 2, et ainsi de suite. Les lettres sont généralement converties en nombres en utilisant la numérotation de l'alphabet (A=0, B=1, C=2, etc.).
- **Multiplication matricielle** : Chaque matrice colonne représentant un digramme est multipliée par la matrice de clé. Le résultat est une nouvelle matrice colonne, qui représente le digramme chiffré.
- **Conversion en texte chiffré** : Les matrices colonnes chiffrées sont converties en lettres en utilisant la correspondance inverse des numéros aux lettres. Le message chiffré est ainsi obtenu.

Le processus de déchiffrement consiste à effectuer l'inverse des opérations de chiffrement en utilisant la matrice d'inversion de la matrice de chiffrement.

CHIFFREMENT CESAR

Le chiffrement de César, également connu sous le nom de chiffrement par décalage, est l'une des méthodes de chiffrement les plus simples et les plus anciennes. Il a été utilisé par Jules César pour protéger les communications militaires. Le principe du chiffrement de César est de déplacer chaque lettre d'un texte original d'un certain nombre fixe de positions dans l'alphabet pour obtenir le texte chiffré.

Le chiffrement de César fonction de cette manière :

- **Choix du décalage** : Tout d'abord, vous choisissez un nombre, appelé "décalage" ou "clé de chiffrement". Ce nombre détermine combien de positions chaque lettre du texte original sera décalée dans l'alphabet. Par exemple, si vous choisissez un décalage de 3, "A" serait chiffré en "D", "B" en "E", et ainsi de suite.
- **Chiffrement** : Pour chiffrer un message, vous prenez chaque lettre du texte original et appliquez le décalage. Les lettres restent inchangées si elles ne sont pas alphabétiques. Par exemple, si le message original est "HELLO" et le décalage est de 3, le message chiffré sera "KHOOR".

- **Déchiffrement** : Pour déchiffrer le message, vous utilisez le décalage inverse. Si le décalage était de 3, vous décalez chaque lettre de 3 positions dans la direction opposée pour retrouver le message original.

LE HACHAGE

Une fonction de hachage cryptographique, souvent simplement appelée "fonction de hachage", est un outil essentiel en cryptographie et en sécurité informatique. C'est une fonction mathématique qui prend en entrée des données de taille variable (par exemple, un fichier, un mot de passe ou un texte) et renvoie une valeur de hachage, une chaîne de caractères généralement de longueur fixe, qui est une représentation unique et condensée des données en entrée. Les fonctions de hachage ont plusieurs caractéristiques importantes :

- **Déterminisme** : Pour une entrée donnée, une fonction de hachage donnée renverra toujours la même valeur de hachage. Cela garantit la reproductibilité du hachage.
- Rapide à calculer : Les fonctions de hachage doivent être efficaces à calculer, même pour de grandes quantités de données.
- **Principe du "one-way"** : Il doit être difficile (idéalement impossible) de revenir des valeurs de hachage aux données d'origine. En d'autres termes, il doit être difficile de retrouver les données d'origine à partir de la valeur de hachage.
- **Diffusion** : Une petite modification dans les données d'entrée doit entraîner une grande différence dans la valeur de hachage résultante. Deux ensembles de données très similaires ne doivent pas avoir des valeurs de hachage similaires.
- **Résistance aux collisions** : Une collision se produit lorsque deux ensembles de données différents produisent la même valeur de hachage. Les fonctions de hachage cryptographiques sont conçues pour minimiser la probabilité de collisions.

Les fonctions de hachage ont de nombreuses applications en sécurité informatique, notamment :

- **Stockage sécurisé de mots de passe** : Les mots de passe ne sont pas stockés en texte clair, mais plutôt sous forme de hachages. Lors de l'authentification, le hachage du mot de passe entré par l'utilisateur est comparé au hachage stocké.
- **Intégrité des données** : Les valeurs de hachage des fichiers ou des messages peuvent être utilisées pour vérifier si les données ont été modifiées ou altérées pendant la transmission.
- **Tables de hachage** : Les fonctions de hachage sont utilisées pour accéder rapidement aux données dans les tables de hachage.
- **Signature numérique** : Les fonctions de hachage sont utilisées pour créer des empreintes numériques pour les documents. Une modification du document entraîne une modification de l'empreinte, indiquant que le document a été altéré.
- **Sécurité en matière de cryptomonnaie** : Les fonctions de hachage sont utilisées pour sécuriser les transactions et les portefeuilles de cryptomonnaie.

Les fonctions de hachage cryptographiques sont conçues pour résister aux attaques et sont un élément essentiel de la sécurité informatique moderne. Des exemples courants de fonctions de hachage cryptographiques comprennent SHA-256 (Secure Hash Algorithm 256 bits) et MD5 (Message Digest 5).

Cependant, MD5 est obsolète et vulnérable aux attaques, et il est recommandé d'utiliser des fonctions plus sécurisées comme SHA-256.

Nous allons alors utiliser les fonctions de hachage RSA-SHA512 avec OpenVPN sur Pfsense afin de chiffrer les données sensibles partagées au sein du réseau.

7. Relations d'approbation

Définition

Une relation d'approbation est un lien de confiance (Trust Relationship) établie entre deux domaines Active Directory, voir même entre deux forêts Active Directory. Ces relations permettront de faciliter l'accès aux ressources entre les domaines concernés, ce qui permet de mutualiser les accès bien que les domaines disposent d'une base de données Active Directory différente.

On crée les relations d'approbations par l'intermédiaire de la console « Domaines et approbations » intégrée à Windows Server.

Cas d'utilisation des relations d'approbations

Les relations d'approbations peuvent s'avérer utiles et sont utilisées dans plusieurs cas de figure :

- Une entreprise dispose de plusieurs filiales avec des noms différents, donc des domaines différents, elle pourra créer des relations de confiance entre ses domaines
- Une multinationale, qui scindera son infrastructure en plusieurs domaines, on peut imaginer un par zone géographique (Europe, Asie, Amérique, etc), il faudra là aussi créer des relations de confiance pour faciliter l'accès aux ressources.
- La fusion de deux entreprises existantes, qui utilisent à la base chacune leur domaine. La relation d'approbation permettra de faciliter la fusion au niveau du système d'information (avant une éventuelle restructuration complète).

Direction et transitivité

Lorsque l'on parle de relations d'approbations, on ne peut pas échapper à la notion de direction et de transitivité, il va falloir s'y faire. Définissons ces termes :

DIRECTION

Dans le cadre d'une relation d'approbation, la direction peut être unidirectionnelle c'est-à-dire uniquement dans un sens, ou bidirectionnelle c'est-à-dire dans les deux sens. Qu'est-ce que cela signifie ?

Une relation d'approbation unidirectionnelle signifie qu'un domaine A approuvé un domaine B, sans que l'inverse soit appliqué. De ce fait, un utilisateur du domaine B pourra accéder aux ressources du domaine A, alors que l'inverse ne sera pas possible !

Pour que cela soit possible, il faut que la relation d'approbation soit bidirectionnelle pour que les deux domaines s'approuvent mutuellement. Un utilisateur du domaine A pourra alors accéder aux ressources du domaine B, et inversement.

TRANSITIVITE

Une relation d'approbation, en plus d'être unidirectionnelle ou bidirectionnelle, peut être ou ne pas être transitive.

La transitivité signifie que si un domaine A approuvé un domaine B, et que ce domaine B approuve un domaine C, alors le domaine A approuvera implicitement le domaine C. Autrement dit, « comme A approuvé B et que B approuve C, alors A approuvé C ».

LES APPROBATIONS PREDEFINIES

Les approbations prédéfinies sont des relations d'approbations créées automatiquement lorsque l'on étend une forêt ou un domaine. J'entends par là le fait d'ajouter un domaine enfant à un domaine existant, par exemple :

Si l'on dispose d'un domaine « principal.local » et que l'on ajoute le domaine enfant « second.local », il y aura automatiquement une relation de confiance entre ces deux domaines. Une relation d'approbation transitive et bidirectionnelle sera créée entre ces deux domaines. On parlera d'approbation « parent/enfant ».

LES APPROBATIONS EXTERNES

Il est possible de réaliser des relations d'approbations externes, c'est-à-dire entre des domaines situés dans des forêts différentes. Ces relations sont unidirectionnelles et non transitives.

Pour que l'approbation soit réciproque, il faut que chaque domaine effectue une relation vers le domaine cible, ce qui permettra d'arriver indirectement à une relation bidirectionnelle. [15]

Nous voulons établir une relation entre le site principal et le site secondaire R&D à Lyon. Le premier doit être le contrôleur du domaine. Nous devons donc établir une relation unidirectionnelle du site principal au site secondaire.

IV. Schématisation du Nouveau Système d'Information

En effectuant ces améliorations, nous obtenons ce Système d'Information :

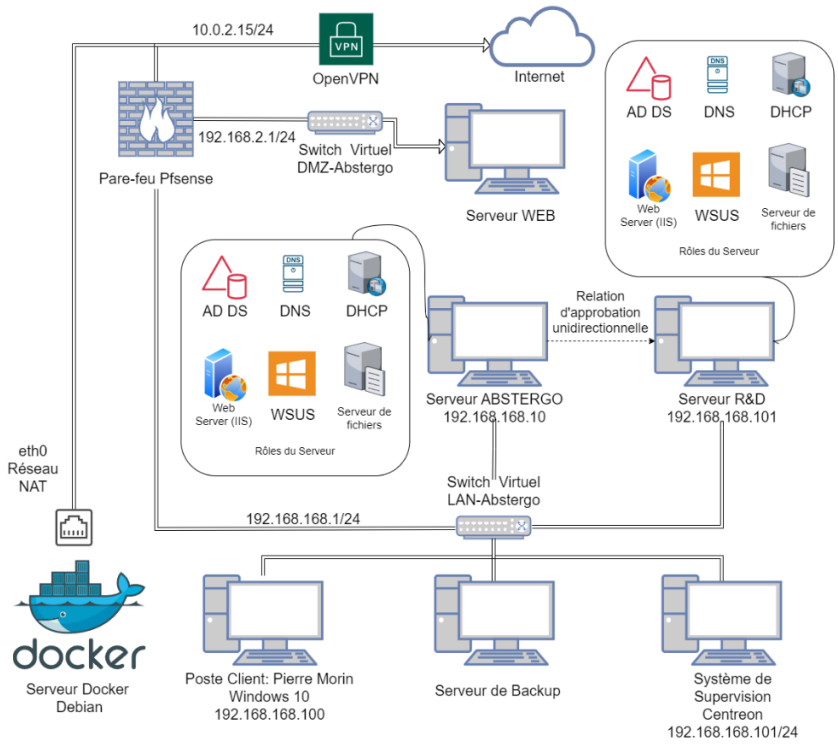

Figure 3: Schématisation du nouveau S.I.

V. Gestion de la Continuité Opérationnelle

1. Contrat de Maintenance

Définition

Le contrat de maintenance informatique est la convention par laquelle une entreprise de service informatique s'engage auprès de son client à entretenir son parc informatique contre rémunération.[16]

La maintenance informatique consiste à assurer le bon fonctionnement du matériel, des logiciels et des réseaux informatiques. Elle comprend des tâches telles que l'installation de mises à jour et de correctifs, la sauvegarde des données et la mise en place de mesures de sécurité. La maintenance informatique comprend également le dépannage des problèmes lorsqu'ils surviennent et la réparation ou le remplacement des équipements cassés. Elle peut être confiée à une équipe interne ou à un prestataire de maintenance informatique.

Types de contrat

Il existe plusieurs types de maintenance informatique, chacune répondant à un objectif précis :

1. LA MAINTENANCE INFORMATIQUE PREVENTIVE

La maintenance préventive est l'ensemble des actions permettant de détecter et de corriger les défaillances potentielles avant qu'elles ne se manifestent. Elle vise à éviter les pannes et les pertes de données en assurant le bon fonctionnement des équipements et des logiciels.

La maintenance préventive implique des tâches programmées régulièrement, comme l'installation de mises à jour et de correctifs, la sauvegarde des données et la mise en œuvre de mesures de sécurité.

La maintenance préventive informatique est une activité essentielle pour toute entreprise qui souhaite protéger ses investissements et garantir la disponibilité de ses services. Elle permet notamment d'éviter de nombreux problèmes informatiques courants avant qu'ils ne surviennent.

Elle doit être réalisée par une équipe qualifiée et expérimentée afin de garantir un niveau de service optimal.

2. La maintenance informatique corrective

La maintenance corrective est l'activité consistant à identifier et corriger les défaillances d'un système informatique et à le remettre dans un état opérationnel. Elle comprend des tâches telles que le dépannage du problème, la réparation ou le remplacement de l'équipement et la restauration des données. Elle s'applique aux logiciels et aux hardwares et est réalisée la plupart du temps par le personnel d'assistance informatique.

La maintenance corrective est généralement effectuée après la mise en production d'un système ou d'une application, mais elle peut être nécessaire à tout moment si des défaillances sont identifiées.

3. La maintenance informatique curative

La maintenance curative est un type de maintenance qui va plus loin que la maintenance corrective. Elle vise à remédier aux défaillances en recherchant l'origine du problème afin d'apporter une solution sur le long terme.

La maintenance curative informatique est généralement déclenchée lorsqu'une panne ou un dysfonctionnement intervient sur un équipement ou un système.

4. La maintenance informatique evolutive

Alors que la maintenance préventive et corrective vise à assurer le bon fonctionnement des systèmes informatiques, la maintenance évolutive permet de les faire évoluer pour répondre à des besoins changeants.

La maintenance évolutive est un processus continu de suivi et de mise à jour d'une application ou d'un système existant afin de répondre aux besoins changeants des utilisateurs. Ce type de maintenance est nécessaire pour garantir que le logiciel continue de fonctionner correctement et reste compatible avec les autres applications et systèmes. Elle peut également impliquer des améliorations mineures du code ou du design, afin d'améliorer l'expérience utilisateur ou les performances du logiciel.

En raison de sa nature itérative, la maintenance évolutive exige une communication étroite entre les développeurs et les utilisateurs, afin que tous les changements apportés au logiciel soient documentés et testés avant d'être mis en production.

La maintenance évolutive est généralement effectuée par le personnel informatique avec l'aide de développeurs et d'autres spécialistes. [17]

2. Plan de Continuité

LE PLAN DE CONTINUITÉ D'ACTIVITÉ (PCA)

Le PCA vise à garantir la haute disponibilité du système informatique de l'entreprise, particulièrement en cas de crise. Il ne s'agit ni plus ni moins que de s'assurer que toutes les applications critiques nécessaires à l'activité de l'entreprise soient disponibles, même en cas de sinistre.
La conception de l'architecture du système informatique de l'entreprise est au centre du PCA. Il faut mettre en place des équipements redondants (réseau, système de stockage de données, serveurs, datacenters), capables de prendre automatiquement le relai si l'un des éléments principaux venait à tomber en panne ou à être mis hors service. De cette façon, les utilisateurs continuent à bénéficier du même service, quoi qu'il se passe.
Naturellement, une architecture redondante nécessite que les données de l'entreprise soient à jour en permanence à la fois sur le réseau primaire (utilisé tous les jours) et sur le réseau secondaire (utilisé comme secours en cas d'incident). Les données doivent donc être répliquées entre le primaire et le secondaire de façon automatique et transparente. Seules les applications et les données critiques sont généralement incluses dans le PCA. [18]

- **Identification des activités critiques** : Identifiez et classez les activités critiques d'ABSTERGO afin de déterminer les priorités en cas de perturbation.
- **Planification de la continuité** : Établissez des plans détaillés pour chaque activité critique, y compris des procédures d'urgence, des stratégies de repli, et des solutions de travail à distance.
- **Redondance des ressources** : Mettez en place des redondances pour les ressources essentielles, telles que les serveurs, les connexions Internet et l'alimentation électrique, afin de réduire les points de défaillance uniques.
- **Tests réguliers** : Effectuez des exercices de simulation de crise pour évaluer l'efficacité de vos plans PCA et identifiez les domaines nécessitant des améliorations.

LE PLAN DE REPRISE D'ACTIVITÉ (PRA)

Opter pour un PCA est une excellente solution, mais qui peut être très coûteuse. Les entreprises n'ayant pas les moyens financiers de mettre en place un PCA peuvent opter pour le PRA.
Contrairement au PCA qui est là pour empêcher tout arrêt de l'activité de l'entreprise, le PRA est là pour gérer ce risque. Si le système d'informations de l'entreprise n'est plus disponible (panne matérielle, cyberattaque…), le PRA va décrire l'ensemble des procédures nécessaires à un redémarrage au plus vite du système informatique.
Ce redémarrage ne peut pas être fait de n'importe quelle façon, et le PRA est là pour définir la nature et l'ordre des actions à mettre en place pour remettre le système et les données dans l'état dans lequel ils étaient avant l'incident.
Les procédures décrites dans le PRA n'ont qu'un objectif, assurer un redémarrage rapide et sûr du système informatique et de l'activité de l'entreprise, et vérifier qu'aucune perte de données n'est à déplorer. Il est donc nécessaire de mettre en place un système de sauvegarde, et de restauration des données à partir d'un site de secours. [18]

- **Sauvegarde et restauration** : Mettez en place des politiques de sauvegarde régulières pour toutes les données critiques, avec des mécanismes de chiffrement. Assurez-vous que les procédures de restauration sont bien documentées et testées.
- **Haute disponibilité** : Utilisez des solutions de haute disponibilité pour vos systèmes critiques, telles que la virtualisation, la répartition de charge et la redondance des serveurs.

- Stockage de données hors site : Gardez des copies de sauvegarde des données essentielles dans un emplacement distant et sécurisé pour éviter la perte en cas de sinistre.
- **Planification des interventions** : Identifiez les procédures de récupération et les étapes pour restaurer les systèmes informatiques de manière rapide et efficace.
- **Formation et sensibilisation** : Formez votre personnel aux procédures de PRA et organisez des sessions de sensibilisation régulières pour qu'ils sachent comment réagir en cas d'incident.

Figure 4: Plans PCA/PRA [18]

VI. Conclusion

Notre projet approfondi du système d'information d'ABSTERGO a conduit à des recommandations clés pour renforcer la sécurité et améliorer l'efficacité opérationnelle. Nous avons proposé des solutions pratiques, telles qu'une authentification robuste, la virtualisation adaptée, une supervision proactive, une politique de sauvegarde solide, un pare-feu approprié, et l'utilisation de la cryptographie pour sécuriser les données.

Le schéma détaillé illustre comment ces éléments s'intègrent pour créer une infrastructure informatique sécurisée. Le contrat de maintenance souligne l'importance de la gestion proactive des équipements.

En conclusion, en adoptant ces recommandations, ABSTERGO peut renforcer sa sécurité, améliorer son efficacité, et être prête pour les défis futurs, affirmant ainsi sa position en tant que leader dans son secteur.

Bilan de groupe

En ce qui concerne ce livrable, notre groupe a travaillé sur le système d'information d'Abstergo et sur les points pouvant être améliorés pour obtenir un système d'information équilibré et sécurisé. Les améliorations que nous proposons sont des points que nous avons déjà abordés en cours et lors d'ateliers tout au long de ce bloc. De plus, nous avons ajouté d'autres propositions visant à renforcer davantage notre système d'information. Nous avons également proposé une nouvelle cartographie, élaborée grâce aux nouveaux points que nous avons identifiés, parmi lesquels on peut citer le pare-feu, le VPN et Docker.

Bilan Personnel

Sarah KOMBAR :

Ce livrable m'a permis de bien reconnaitre les différentes options disponibles en ce qui concerne l'authentification, la virtualisation, la surveillance, la sauvegarde, la sécurité réseau, et la cryptographie. Nous avons également pu évaluer laquelle d'entre elles est plus adaptée en fonction de nos besoins.

Ahmad ZIAB :

Ce livrable m'a permis d'approfondir mes connaissances sur la sécurité des systèmes d'information, en particulier en ce qui concerne l'authentification, la virtualisation, la surveillance, la sauvegarde, la sécurité réseau, et la cryptographie. La proposition d'une infrastructure révisée pour ABSTERGO a renforcé ma compréhension des meilleures pratiques en matière de sécurité informatique, et la résolution des problèmes identifiés a enrichi mon expérience dans la conception de solutions robustes et conformes aux normes de l'industrie.

Mohamed Amine EL BAH :

Ce livrable m'a aidé à faire les choix des points d'amélioration du système d'information Abstergo. Il m'a également aidé à comprendre plusieurs notions théoriques, notamment en matière de sécurisation de système, de conteneurisation et d'automatisation, ainsi que de surveillance et de politiques de sauvegarde.

Cyril TILHOU-TRIEP :

Ce livrable m'a permis de mettre une bonne base de réflexions sur les méthodes que nous allons utiliser dans le livrable 3, de plus réfléchir sur la manière d'améliorer un système de SI apporte des réflexions tout a fait passionnante sur son fonctionnement qui malheureusement n'on pas pu figurer dans celui-ci, mais ont contribué a mon développement personnel.

VII. Table de Figures

Figures

Tableaux

VIII. Bibliographie

[1] « Docker, une technologie de conteneurisation qui séduit et s'affirme », Entreprise informatique - ESN - SSII - Toulouse, Albi & Rodez. Consulté le: 3 novembre 2023. [En ligne]. Disponible sur: https://inforsud-technologies.com/ressources/focus/docker-une-technologie-de-conteneurisation-qui-saffirme/

[2] Rvewelle, « Kubernetes vs d'Autres Plateformes d'Orchestration de Conteneurs », Medium. Consulté le: 3 novembre 2023. [En ligne]. Disponible sur: https://medium.com/@rewelle/kubernetes-vs-dautres-plateformes-d-orchestration-de-conteneurs-233a1568e571

[3] « Supervision des systèmes – définition, exemples et conseils ». Consulté le: 30 octobre 2023. [En ligne]. Disponible sur: https://www.paessler.com/fr/system-monitoring

[4] C. Technologies, « 10 meilleures solutions de supervision informatique », Supervision Clever. Consulté le: 1 novembre 2023. [En ligne]. Disponible sur: https://supervision-clever.fr/meilleures-solutions-de-supervision-informatique/

[5] « fetch.pdf ». Consulté le: 1 novembre 2023. [En ligne]. Disponible sur: https://xstra.u-strasbg.fr/lib/exe/fetch.php?media=doc:sem2012:sem2012-nagios.pdf

[6] P. F. team, « Découvrez les 16 meilleurs outils de supervision réseau », Pandora FMS Monitoring Blog. Consulté le: 1 novembre 2023. [En ligne]. Disponible sur: https://pandorafms.com/blog/fr/outils-supervision-reseau/

[7] « SolarWinds Service Desk », Capterra. Consulté le: 13 novembre 2023. [En ligne]. Disponible sur: https://www.capterra.fr/software/129478/solarwinds-service-desk

[8] « Politique de sauvegarde ». Consulté le: 3 novembre 2023. [En ligne]. Disponible sur: https://public.dalibo.com/exports/formation/manuels/modules/i0/i0.handout.html

[9] P. Jean-Philippe, « Politiques de sauvegardes ».

[10] « Les règles d'or de la sauvegarde », ANSSI. Consulté le: 3 novembre 2023. [En ligne]. Disponible sur: https://www.ssi.gouv.fr/les-regles-dor-de-la-sauvegarde/

[11] « La nécessité d'installer un pare-feu sur le SI de votre société par votre prestataire informatique », Synoméga. Consulté le: 4 novembre 2023. [En ligne]. Disponible sur: https://www.synomega.com/2020/12/necessite-dinstaller-pare-feu-systeme-dinformation-de-societe-prestataire-informatique/

[12] « Which One Should You Choose pfSense or Untangle? » Consulté le: 4 novembre 2023. [En ligne]. Disponible sur: https://www.knowledgenile.com/blogs/pfsense-vs-untangle
[13] « Compare Cisco Secure Firewall vs Netgate pfSense », PeerSpot. Consulté le: 4 novembre 2023. [En ligne]. Disponible sur: https://www.peerspot.com/product_comparisons/19146-22829
[14] G. Inc, « Unified Security Gateway (USG) vs Sangfor Next-Generation Firewall 2023 | Gartner Peer Insights », Gartner. Consulté le: 4 novembre 2023. [En ligne]. Disponible sur: https://www.gartner.com/market/network-firewalls/compare/product/huawei-security-gateway-usg-vs-sangfor-next-generation-firewall
[15] « Les relations d'approbations | IT-Connect ». Consulté le: 7 novembre 2023. [En ligne]. Disponible sur: https://www.it-connect.fr/chapitres/les-relations-dapprobations/#google_vignette
[16] « Contrat de maintenance informatique : que doit-il contenir ? » Consulté le: 2 novembre 2023. [En ligne]. Disponible sur: https://www.legalstart.fr/fiches-pratiques/relations-commerciales/contrat-maintenance-informatique/
[17] « Les différents types de maintenance informatique - FC MICRO ». Consulté le: 3 novembre 2023. [En ligne]. Disponible sur: https://fcmicro.net/differents-types-de-maintenance-informatique/
[18] « Quelle différence entre PRA et PCA (plan de reprise et plan de continuité) ? » Consulté le: 3 novembre 2023. [En ligne]. Disponible sur: https://www.advancia-itsystem.com/site/fr/news_details.php?id_article=19&id_news=138