

**LIVRABLE 01**

**PROJET**

**ABSTERGO**

**GROUPE 01**

**BROCHOT Florian**

**BERRACHED Hana**

**LAPLACE Hugo**

# INTRODUCTION

## RECAPITULATIF

Créée en 1981, la PME ABSTERGO se spécialise dans la création de capteurs et de solutions IoT. Elle a des partenariats avec de grands noms de l'industrie automobile. Récemment, pour s'adapter aux nouvelles dynamiques du marché, elle a choisi de fusionner avec ANIMUS, un géant des télécommunications multi-niveaux. L'acquisition s'est faite rapidement, vue la tendance d'ANIMUS à racheter d'autres entreprises. Une équipe a été formée pour étudier, documenter, et optimiser l'infrastructure d'ABSTERGO, avec un audit prévu en moins de deux mois.

## REQUETE

Nous avons été sollicités pour cartographier le système d'information d'ABSTERGO et faire un diagnostic sur la gestion des identités et des accès aux données.

## EXAMEN INITIAL DU SI

Dans le paysage actuel des affaires, la compétitivité est primordiale. Pour maintenir sa position, une entreprise doit harmoniser ses ressources. C'est ici que le Système d'Information (SI) joue un rôle crucial. Le SI, grâce aux technologies IT, englobe des dispositifs et des logiciels comme les CRM ou les ERP. Une entreprise se subdivise en deux systèmes principaux : le système de pilotage et le système opérant. Le SI agit comme un pont entre ces deux, assurant l'efficacité opérationnelle. Il collecte, stocke, et diffuse les informations, les transformant en stratégies concrètes.

# RECUPERATION DES MDP KEEPASS

Il fallait dans un premier temps analyser le fichier « ABSTERGO\_Database.kdbx » en s'aidant de KeePass qui est un gestionnaire de mots de passe qui dispose de nombreuses fonctionnalités permettant ainsi aux utilisateurs d'enregistrer sur un même support, c’est-à-dire un seul fichier entièrement protégé, Ieurs différents mots de passe utilisés sur internet.

Ce qu'il faut retenir par rapport à tout ça est qu'après avoir défini un mot de passe pour pouvoir accéder à une base de données, en l'occurrence le « Master Password » et l'unique mot de passe dont nous aurons à nous rappeler il sera alors possible d'enregistrer en toute sécurité autant de mots de passe que l’on souhaite par la suite

Gestionnaire de mots de passes dans lequel nous avons trouvé les différentes données d'authentifications nous permettant d'accéder à l'ensemble des machines virtuelles d’ABSTERGO.

# EXPLORATION DES SERVEURS

On devrait avoir accès à une machine virtuelle spécifique après s'être connecté au DigitaLab. la machine est nommée « A3 Administration SI »

https://digitaIab.cesi.fr

En se connectant à cette dernière. nous aurons accès à la première VM qui désigne un serveur Windows Serveur 2019

On continue nos recherches sur le gestionnaire de serveur :

# DNS



# DHCP



# APACHE

# Active directory

Problèmes identifiés :

1. Uniformité des mots de passe pour tous les utilisateurs.
2. Manque de groupements, rendant impossible la centralisation des comptes.
3. Présence d'un unique contrôleur de domaine.
4. Absence de connexion internet.
5. Pas de serveurs de redondance pour la sauvegarde des données en cas d'incident.
6. L'absence d'unités organisationnelles complique la délégation administrative et les droits dans Active Directory.
7. Des difficultés d'accès au serveur Filezilla pour les utilisateurs hors du réseau local.
8. Manque de GPO pour gérer les restrictions nécessaires.
9. L'absence de service DHCP dans Active Directory.
10. Rien gérer les mises à jour de Microsoft dans Active Directory.
11. Manque de sécurité dans les transferts de fichiers.

Solutions proposéees :

1. Augmenter la sécurité en attribuant un mot de passe unique à chaque utilisateur, éventuellement via un gestionnaire de mots de passe.
2. Implémenter la gestion des groupes GPO pour une administration optimisée des données et de l'infrastructure.
3. Ajouter des contrôleurs de domaine supplémentaires pour garantir la continuité des services d'annuaire et la protection de la base d'annuaire.
4. Restaurer la connectivité internet.
5. Installer le service DHCP.
6. Établir des serveurs de redondance pour éviter la perte de données et garantir l'accès aux backups.
7. Structurer Active Directory avec des unités organisationnelles (OU) pour faciliter la gestion et l'administration des comptes.
8. Assurer la disponibilité du serveur Filezilla à tous les utilisateurs, y compris ceux hors réseau.
9. Déployer des GPO adaptés pour une meilleure gestion des restrictions.
10. Intégrer une solution pour des transferts de données sécurisés.

# SCHEMA DE L'INFRASTRUCTURE DU SYSTEME D'INFORMATION D’ABSTERGO :

A partir de l'étude établie ci-dessus nous avons pu en déduire l'architecture du SI d’ABSTERGO, comme le montre la figure l'ensemble des serveurs et les ordinateurs sont reliés au commutateur qui lui est relié au routeur afin d'avoir accès à internet :



# PROCEDURES DE MIGRATION (RELATION D'APPROBATION) :

Sachant qu’ANIMUS a racheté l'entreprise ABSTERGO, il est nécessaire de relier les systèmes d'information pour permettre l'accès aux ressources. Pour cela nous proposons de faire des procédures de migration de données avec des relations approbations.

Définition d'une relation d'approbation :

Une relation d'approbation est une liaison établie entre deux domaines d'Active Directory, permettant aux utilisateurs de l'un des domaines d'accéder aux ressources de l'autre. Elle détermine comment l'authentification des utilisateurs est traitée entre les deux domaines et peut être configurée selon différents paramètres, tels que la directionnalité et la transitivité, pour répondre aux besoins de sécurité et d'administration des entreprises.

Types de relations d’appprobation :

Il existe plusieurs types de relations d'approbation dans Active Directory :

Relation d'approbation unidirectionnelle : Dans ce type de relation, les utilisateurs d'un domaine (disons domaine A) peuvent accéder aux ressources de l'autre domaine (domaine B) mais pas l'inverse.

Relation d'approbation bidirectionnelle : Ici, les utilisateurs des deux domaines peuvent accéder aux ressources de l'autre domaine. C'est-à-dire que les utilisateurs de A peuvent accéder à B et vice versa.

Relation d'approbation transitive : Si le domaine A a une relation d'approbation avec le domaine B, et le domaine B a une relation d'approbation avec un domaine C, alors par transitivité, A aura une relation d'approbation avec C.

Relation d'approbation non transitive : Cette relation est le contraire de la transitive. Si A a une relation d'approbation avec B, et B avec C, cela ne signifie pas que A a une relation d'approbation avec C.

Relation d'approbation externe : Cette relation est établie entre deux domaines qui appartiennent à des forêts différentes et qui ne partagent pas de relation d'approbation de forêt. Elle peut être unidirectionnelle ou bidirectionnelle.

Relation d'approbation de forêt : C'est une relation d'approbation transitive entre deux forêts. Les utilisateurs d'une forêt peuvent accéder aux ressources de l'autre forêt.

Relation d'approbation à sens unique entrant : Dans cette relation, le domaine de confiance peut accéder aux ressources du domaine approuvant, mais l'inverse n'est pas vrai.

Relation d'approbation à sens unique sortant : Ici, le domaine approuvant peut accéder aux ressources du domaine de confiance, mais pas l'inverse.

.

# CONCLUSION

Une fois l'analyse du SI d'ABSTERGO faite, nous avons pu trier toutes les informations disponibles dans le système, ce qui nous a amené à notifier quelques incohérences ou erreurs au sein du système qui réduire les performances de l'entreprise ABSTERGO nous nous devons donc de corriger les erreurs et penser à une bonne stratégie de sécurité.