



Nathan



Arthur



MEHMETI FAÏK



MAHMOUD CHARIF

Yannick



Système automatisée

Livrable final

PROJET ANIMUS EXTENDUS 06/12/2023

Table des matières

[0. Contexte Livrable 3](#_Toc153880040)

[1. Role de la documentation 3](#_Toc153880041)

[2. Mise en place de l’active directory 3](#_Toc153880042)

[2.0. Déploiement de l’ADDS et réplication en lecture seule 3](#_Toc153880043)

[2.1. Déploiement d’un serveur DHCP 4](#_Toc153880044)

[2.2. Déploiement d’un serveur WSUS 5](#_Toc153880045)

[2.3. Mise en place des unité d’organisation et des groupes 5](#_Toc153880046)

[2.4. Mise en place des Group policy object 5](#_Toc153880047)

[2.4.1. Fond D’ecran pour les utilisateurs 5](#_Toc153880048)

[2.4.2. Limite des formats de fichiers et de leur taille 5](#_Toc153880049)

[2.4.3. Restrictions sur les ports USB 5](#_Toc153880050)

[2.5. Mise en place du Serveur de Fichiers 5](#_Toc153880051)

[2.6. Mise en place des accès VPN IPSec Site à site 5](#_Toc153880052)

[2.7. Mise en place des accès VPN OpenVPN client à site 6](#_Toc153880053)

[2.7.1. Authentification par certificats 6](#_Toc153880054)

[2.7.2. Infrastructure a clés publiques (PKI) 6](#_Toc153880055)

[2.7.3. Accés au gestionnaire de certificats 6](#_Toc153880056)

[2.7.4. Gestion de l'autorité de certification 6](#_Toc153880057)

[2.7.5. Création et gestion des certificats 6](#_Toc153880058)

[2.7.6. Mise en place du serveur VPN 6](#_Toc153880059)

[2.7.7. Export des certificat client OPENVPN (.ovpn) 7](#_Toc153880060)

[3. Utilisation des scripts 8](#_Toc153880061)

[4. Gestion des Risques 9](#_Toc153880062)

[5. Maintenance du S.I. 11](#_Toc153880063)

[5.0. Stratégies de Maintenance 11](#_Toc153880064)

[5.0.1. Maintenance préventive : 11](#_Toc153880065)

[5.0.2. Maintenance corrective : 11](#_Toc153880066)

[5.0.3. Maintenance évolutive : 11](#_Toc153880067)

[6. Axes d’amélioration du S.I. 11](#_Toc153880068)

[7. Sensibilisation à la Sécurité 11](#_Toc153880069)

[8. Conclusion 12](#_Toc153880070)

[8.0. Valeur de la documentation pour la sécurité à long terme. 12](#_Toc153880071)

[8.1. Engagement envers l'amélioration continue. 12](#_Toc153880072)

[9. Table des illustrations 13](#_Toc153880074)

[10. Lexique 14](#_Toc153880075)

# Contexte Livrable

Dans le cadre de notre projet pour ABSTERGO, il est primordial de fournir une documentation complète au futur administrateur. Celle-ci inclura les diverses procédures et scripts que nous avons mis en œuvre. Par ailleurs, il est essentiel de conscientiser la direction aux risques informatiques en identifiant dix menaces potentielles et en détaillant les solutions spécifiques que nous avons développées pour les contrer, garantissant ainsi une sécurité optimisée et une réponse proactive face aux vulnérabilités du système d'information.

# Role de la documentation

Cette documentation vise à fournir une référence concise et facile à suivre pour les administrateurs système responsables de la mise en place, de la gestion et de la maintenance d'un environnement de réseau informatique d'entreprise. Elle traite de l'installation de services critiques, de la gestion des utilisateurs, de la sécurisation du réseau et de la préparation aux différents risques IT.

# Mise en place de l’active directory

## Déploiement de l’ADDS et réplication en lecture seule

Une image contenant texte, Appareils électroniques, capture d’écran, Police

Description générée automatiquement

Figure 1 Script d'installation de l'AD DS et du Serveur DNS

La réplication de l’AD DS pour le site distant est RODC (Lecture seule)

## Déploiement d’un serveur DHCP

Une image contenant texte, capture d’écran, affichage, logiciel

Description générée automatiquement

Une image contenant texte, Police, ligne, capture d’écran

Description générée automatiquement

Une image contenant texte, Police, capture d’écran

Description générée automatiquement

## Déploiement d’un serveur WSUS

L’installation et la configuration de Windows Server Update Services (WSUS) sert à gérer la distribution des mises à jour de sécurité et des correctifs pour les systèmes Windows dans l'entreprise.

Les mises à jour sont stockées dans un lecteur dédié.

## Mise en place des unité d’organisation et des groupes

Créer une structure d'unités d'organisation (OU) dans AD pour refléter l'organisation de l'entreprise et faciliter la gestion des politiques de groupe et des permissions.

## Mise en place des Group policy object

### Fond D’ecran pour les utilisateurs

Une politique de groupe pour standardiser le fond d'écran sur tous les postes de travail des utilisateurs.

### Limite des formats de fichiers et de leur taille

Les GPO pour restreindre les types de fichiers (médias) pouvant être sauvegardés sur le réseau d'entreprise et appliquer des quotas de taille de fichier.

### Restrictions sur les ports USB

GPO pour désactiver l'utilisation des ports USB pour les périphériques de stockage non autorisés afin de protéger contre la fuite de données.

## Mise en place du Serveur de Fichiers

Le serveur de fichiers est déployé sur le Windows Server pour un stockage centralisé. Il y’a une configuration des permissions appropriées et des quotas d'espace disque pour les utilisateurs et les groupes.

## Mise en place des accès VPN IPSec Site à site

La configuration d’un accès VPN via IPSec de type Site à Site permet de connecter le réseau interne au réseau R&D de Lyon. (Voir schéma de la nouvelle infrastructure du Livrable 2).

## Mise en place des accès VPN OpenVPN client à site

La configuration d'un accès VPN via OpenVPN de type client à site permet aux utilisateurs distants de se connecter de manière sécurisée au réseau de l'entreprise comme s'ils étaient sur place. Cela permet l'accès sécurisé aux ressources de l'entreprise depuis n'importe où.

### Authentification par certificats

OpenVPN utilise des certificats numériques pour authentifier le serveur VPN et les clients qui tentent de se connecter. Cette méthode est basée sur une infrastructure à clés publiques (PKI).

### **Infrastructure a clés publiques (PKI)**

Une PKI est nécessaire pour créer, gérer, distribuer, utiliser, stocker et révoquer les certificats numériques. Dans le contexte d'OpenVPN, elle assure que seuls les clients possédant un certificat valide et émis par l'autorité de certification (CA) de confiance peuvent établir une connexion avec le serveur VPN.

### Accés au gestionnaire de certificats

* Dans l'interface PfSense, allez dans le menu System (Système).
* Sélectionnez Cert. Manager (Gestionnaire de certificats) sous la section Cert Manager.

### Gestion de l'autorité de certification

* Dans l'onglet CAs (Autorités de certification), vous pouvez créer une nouvelle CA, visualiser ou éditer les CA existantes.
* Pour créer une nouvelle CA, cliquez sur (Ajouter) et remplissez les informations nécessaires telles que le nom descriptif, la clé privée, le type d'algorithme de signature, etc.

### Création et gestion des certificats

* Dans l'onglet Certificates (Certificats), vous pouvez voir tous les certificats existants.
* Pour créer un nouveau certificat, cliquez sur (Ajouter/Signer).
* Vous devez fournir les détails requis tels que le nom descriptif, l'autorité de certification associée, le type de certificat, et d'autres options de configuration.

### Mise en place du serveur VPN

Une fois que vous avez votre CA et vos certificats en place, vous pouvez les utiliser pour configurer votre serveur VPN dans PfSense en allant dans VPN > OpenVPN > Servers (Serveurs) et en configurant les paramètres correspondants avec les certificats appropriés.

### Export des certificat client OPENVPN (.ovpn)

Une image contenant texte, logiciel, capture d’écran, Page web

Description générée automatiquementExporter les ficher de connexion OpenVPN grâce au package OPENVPN qu’il faut installer dans le package manager puis une fois installé allez dans VPN > OpenVPN > Client Export Utility

# Utilisation des scripts

Nous aurons besoin de 3 fichiers qui devront obligatoirement être dans le même dossier USERS.ps1 , OU.ps1 et USERS.csv

Pour créer une OU nous devons juste ajouter le nom du domaine dans la liste $ouNoms dans le script OU.ps1

Pour ajouter un utilisateur supplémentaire, il faut ajouter une ligne dans le csv comme suit :

prénom;nom;SAM;MDP;groupes;domaine1;domaine2

prenom : le prénom de l’utilisateur

nom : le nom de famille de l’utilisateur

SAM **:** Les identifiants des utilisateurs sont formés des trois premières lettres du nom de famille suivies du prénom complet.

MDP : Chaque mot de passe se compose de 11 caractères, incluant trois majuscules, sept minuscules et un caractère spécial choisi parmi les suivants : @, !, ?, & et %.

groupes : la syntaxe pour mettre les groupes est OU.Sous-Ou.groupe, si vous voulons ajouter plusieurs groupes en même temps, il suffit de les séparer avec un « / » sans espaces.

domaine1 : la partie gauche du domaine

domaine2 : la partie gauche du domaine

# Gestion des Risques

**Cyberattaques :**

Mettre en place des règles de pares-feux dans l’infrastructure, sensibiliser les membres du S.I. aux différentes menaces d’attaque (comme les tentatives d’hameçonnage). Surveiller le réseau pour détecter des éventuelles intrusions, et avoir une bonne gestion des accès aux données aux utilisateurs, isolée les données sensibles des attaques.

**Pertes de données :**

Mettre en œuvre des politiques de sauvegarde régulières, utiliser le chiffrement des données sensibles, et sensibiliser les utilisateurs à l'importance de la protection des données.

**Défaillance matérielle :**

Mettre en place une infrastructure redondante, effectuer des sauvegardes régulières, et maintenir un plan de reprise après sinistre.

**Mauvaise gestion des identités et des accès** :

Mettre en place des processus de gestion des identités robustes, appliquer le principe du moindre privilège, et effectuer des audits réguliers des droits d'accès.

**Catastrophes naturelles :**

Mettre en place un plan de sauvegarde 3-2-1 pour que les données ne soient pas perdues à la suite de la dégradation ou perte de matériel (avoir une copie des données du S.I. à des endroits distincts). Elaborer un plan de continuité des activités du S.I. afin de réagir plus rapidement et efficacement, puis effectuer des tests régulièrement pour améliorer et rendre efficace ce plan.

**Non-conformité réglementaire :**

Établir des politiques de conformité claires, mettre en place des mécanismes de suivi et de rapport, et former le personnel sur les réglementations en vigueur.

**Divulgation de données/renseignements sensibles :**

En cas de divulgation de renseignements ou données sensibles sur le S.I., les actifs de l’entreprise peuvent être compromis. Pour s’en prémunir, il convient de protéger l’entreprise à l’aide d’une clause de confidentialité, une charte d’utilisation du SI et de la sensibilisation du personnel.

**Panne de courant :**

Identification de l’étendue de la panne et mettre en place une stratégie de sauvegarde redondante pour éviter toute perte d’informations au niveau du S.I. On pourrait également s’équiper d’onduleurs supplémentaires ou des solutions alternatives afin que ce ne soit pas l’entièreté du système qui est impacté. Finalement, redémarrer séquentiellement les systèmes pour éviter une surcharge électrique et mettre en place un plan de reprise.

**Espionnage Industriel :**

Afin de se prémunir de cette menace, le S.I. doit être surveillé en permanence grâce à un logiciel de supervision pour détecter toute activité suspecte et chiffrer les données, surveiller les locaux pour éviter l’accès aux personnes tiers au S.I., et enfin surveiller la sécurité des fournisseurs et faire en sorte qu’ils respectent les normes du S.I.

**Ingénierie sociale :**

En cas d’attaque par ingénierie sociale une personne tierce, pour obtenir des informations ou manipuler certains employés. Pour s’en prémunir, il convient de mettre en place des procédures afin d’éviter ce type d’arnaque et une sensibilisation ou encore une chaîne d’alerte.

# Maintenance du S.I.

La maintenance du S.I. vise à garantir la fiabilité, la performance et la sécurité des services informatiques. Elle doit s'aligner avec les objectifs stratégiques d'ABSTERGO et s'assurer que le S.I. soutient efficacement les opérations de l'entreprise.

## Stratégies de Maintenance

### Maintenance préventive :

* Mises à jour régulières des logiciels et du matériel pour corriger les failles de sécurité et améliorer les performances.
* Audits de sécurité périodiques pour identifier et corriger les vulnérabilités.
* Nettoyage physique des serveurs et des équipements réseau pour prévenir les défaillances matérielles.
* Analyse des journaux et des performances pour anticiper les problèmes.

### Maintenance corrective :

* Procédures de dépannage pour résoudre les pannes et les erreurs système rapidement.
* Remplacement des composants défectueux ou obsolètes.
* Mise en place de patches ou de correctifs en réponse aux incidents de sécurité.

### Maintenance évolutive :

* Amélioration continue des systèmes pour prendre en charge de nouvelles fonctionnalités métier.
* Intégration de nouvelles technologies pour rester compétitif.
* Mise à échelle des ressources pour répondre aux exigences de croissance de l'entreprise.

# Axes d’amélioration du S.I.

* Mettre un place une stratégie de sauvegarde 3-2-1, pour offrir une protection robuste face aux pertes de données.
* Mettre en place un accès VPN pour les utilisateurs travaillant à distance. Cela permettra de chiffrer les échanges lors de la connexion au S.I.
* Mise en place d’un PCI et PRI pour faire face aux différents risques et menaces sur le S.I.

# Sensibilisation à la Sécurité

La sécurité informatique est importante dans notre monde connecté. Garder les informations confidentielles, intactes et disponibles est essentiel pour protéger les entreprises et les utilisateurs. Les menaces comme les cyberattaques sont partout, ce qui montre pourquoi il est crucial de sensibiliser à la sécurité de l’infrastructure et en informatique en général. Des choses simples comme avoir des mots de passe robustes, mettre à jour les programmes régulièrement, et apprendre aux employés à reconnaître les arnaques en ligne sont des actions essentielles.

# Conclusion

## Valeur de la documentation pour la sécurité à long terme.

La documentation approfondie du système d'information revêt une importance cruciale pour les administrateurs système. Elle représente une source essentielle d'informations sur l'architecture, la configuration et le fonctionnement du SI, permettant aux administrateurs de développer une compréhension approfondie de l'environnement informatique. Cette documentation facilite la gestion quotidienne en fournissant un guide détaillé pour les tâches de maintenance, de résolution des problèmes et de mise à jour du système.

Elle joue également un rôle vital dans le transfert des connaissances au sein de l'équipe, accélérant l'intégration des nouveaux membres et assurant une continuité opérationnelle. En outre, la documentation contribue à la planification de la capacité en offrant une vue claire des ressources actuelles et en aidant à anticiper les besoins futurs. Pour les incidents de sécurité ou les pannes, une documentation précise permet une réponse rapide, réduisant ainsi les temps d'arrêt et les impacts sur l'organisation. En favorisant la conformité aux normes, la documentation renforce également la sécurité et la gouvernance du SI. Enfin, elle sert d'outil d'amélioration continue en permettant l'analyse des performances passées et l'identification des opportunités d'optimisation. Ainsi, un administrateur bien documenté est mieux équipé pour assurer la stabilité, la sécurité et l'efficacité des opérations informatiques au sein de l'organisation.

## Engagement envers l'amélioration continue.

L'amélioration continue des équipements et infrastructures du système d'information est impérative pour assurer la performance optimale, la sécurité et la durabilité de l'environnement informatique d'une organisation. En investissant dans des technologies plus récentes, les entreprises peuvent bénéficier des dernières avancées en matière de traitement de données, de stockage et de connectivité, garantissant ainsi une exécution plus rapide et efficace des processus informatiques.

De plus, la mise à niveau régulière contribue à réduire les vulnérabilités de sécurité en s'adaptant aux nouvelles menaces et en évitant les risques associés aux équipements obsolètes. Cette approche proactive permet également une intégration fluide de nouvelles fonctionnalités, favorisant l'innovation et la compétitivité de l'entreprise sur le marché.

Sur le plan financier, bien que les coûts initiaux des mises à niveau puissent être significatifs, les économies à long terme résultant d’une meilleure efficacité opérationnelle et de la réduction des coûts de maintenance justifient ces investissements. En outre, le respect des normes et réglementations en constante évolution, ainsi que la contribution à la durabilité environnementale grâce à l’utilisation d’équipements plus écoénergétiques, renforcent la position et la responsabilité de l’organisation dans un monde numérique en constante mutation.

L’amélioration continue du SI est une stratégie incontournable pour rester agile, sécurisé et compétitif dans le paysage technologique dynamique d'aujourd'hui.

# Table des illustrations

Figure 1 Script d'installation de l'AD DS et du Serveur DNS 3

# Lexique

**Architecture** : La conception structurale du réseau informatique, y compris les composants hardware et software et leurs interrelations.

**Mises à jour régulières** : L'installation de nouvelles versions de logiciels ou de firmware pour corriger des bugs ou des failles de sécurité.

**Audits de sécurité périodiques** : Des évaluations régulières des systèmes pour détecter des vulnérabilités potentielles.