28/11/2022

Livrable 2 :

Maquette :

Luc BARRETO Alexandre MILHAS Valentin OBERT
CESI

Table des matières

I) Introduction :

Nous avons lors de notre analyse de l'existant remarqué qu'il y avait beaucoup de failles de sécurité, et ainsi que de problèmes notamment liés à la fiabilité du Système d'informations d'Abstergo. Nous allons passer ici en revue tous les correctifs qui seront appliqués aux parties défectueuses du Système d'Information.

En parallèle de l'analyse de l'existant, nous avons pris en compte les demandes des collaborateurs de l'entreprise, ce qui a mis en exergue dans le nouveau Système d'informations :

Dans un premier temps, plusieurs employés nous ont remonté des problèmes de permissions avec les comptes utilisateurs. En effet, certaines personnes avaient accès à des données sensibles normalement inaccessibles. Nous avons donc reconfiguré l'Active Directory et refait l'ensemble des comptes utilisateur ainsi que l'ensemble des permissions attribuées à chacun.

Nous avons de plus appliqué un ensemble de règles à l'ensemble des employés. Cela a pour but l'harmonisation et la sécurisation de l'ensemble des postes. On peut par exemple penser à l'attribution automatique des fonds d'écran.

Nous avons aussi été informés que les services fournis par l'Active Directory étaient régulièrement hors service que qui empêchait les personnels de travailler. Pour éviter cela, nous avons mis en place des redondances et étudié les charges auxquelles était soumis le serveur pour adapter les redondances.

II) Management du projet :

Pour organiser correctement les ressources humaines de ce projet, nous avons réalisé un OBS, WBS et un diagramme de Gantt que vous trouverez ci-dessous :

Diagramme WBS :

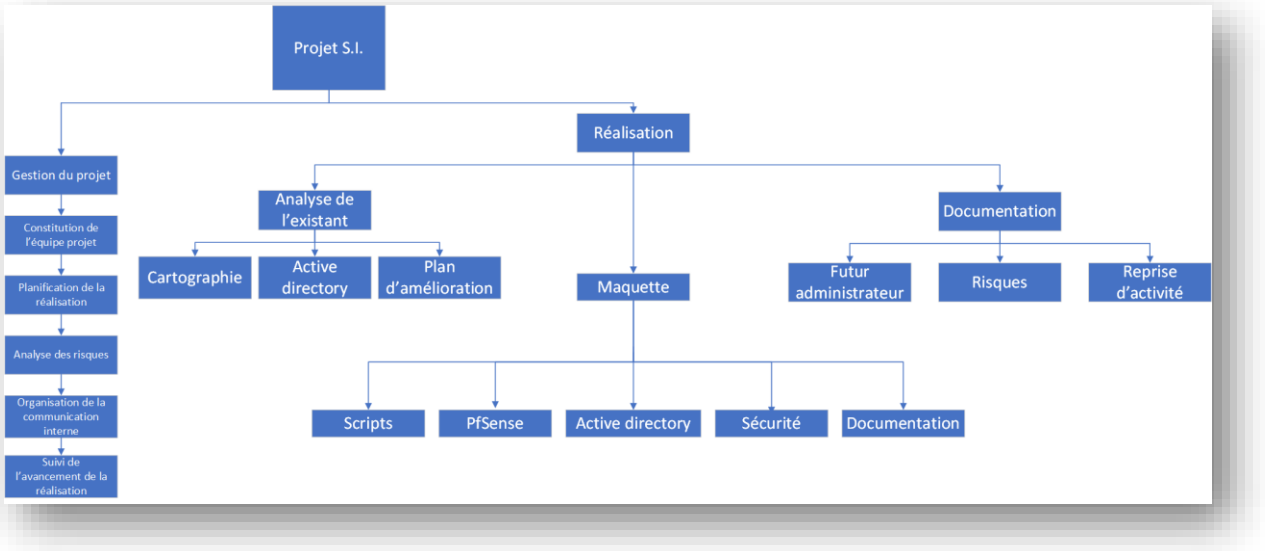


Diagramme OBS :

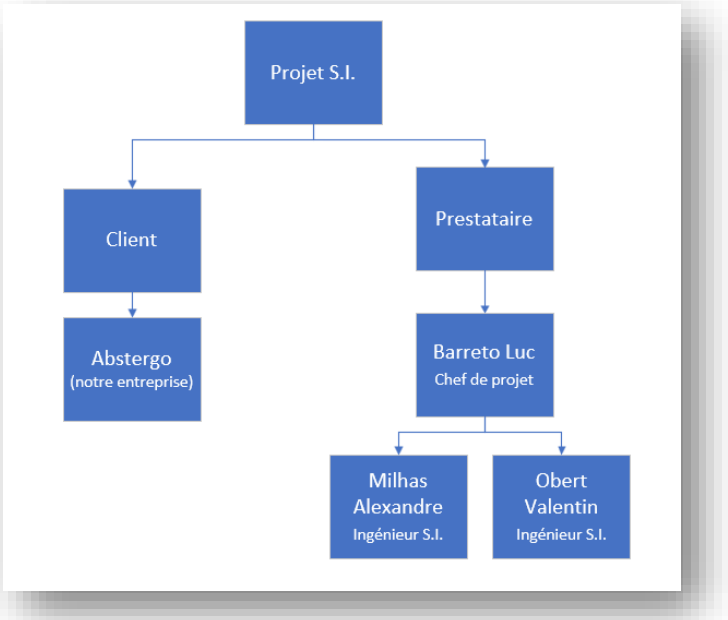
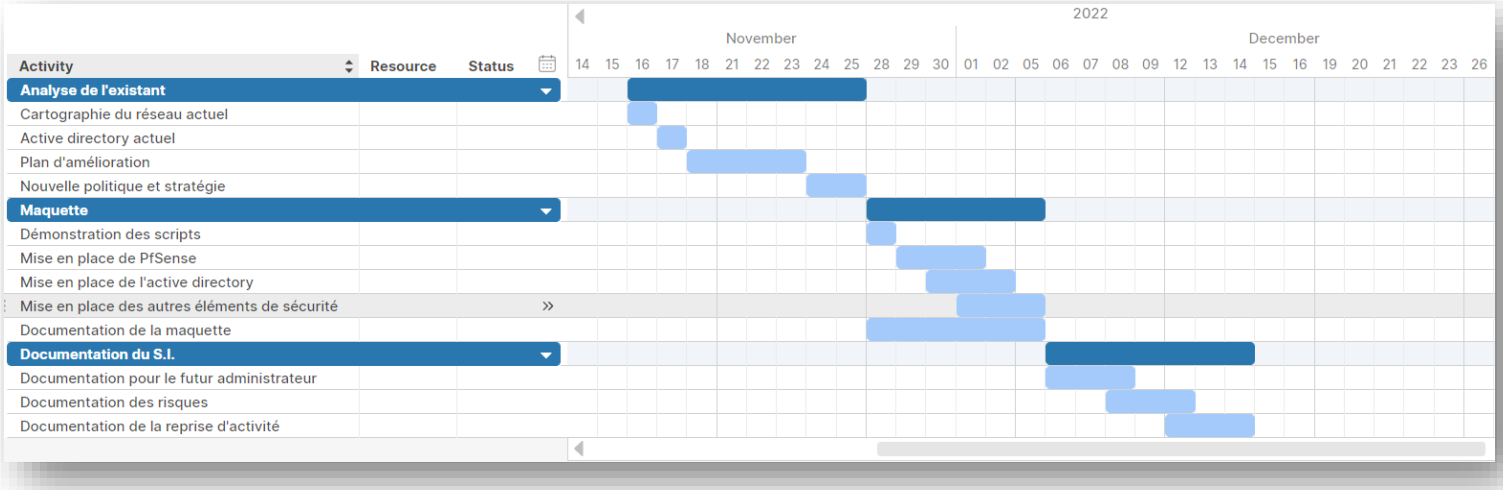


Diagramme de Gantt :



III) Scripts de découverte et d'automatisation :

Pour effectuer une analyse de l'existant le plus rapidement possible, nous nous sommes aidés de commandes, script de découverte et d'automatisation Powershell. En effet, Powershell nous permet d'accéder à de nombreuses informations dans l'ensemble du système d'information de la société, en particulier les données relatives à l'Active Directory actuellement configurée en en fonction.

Ci-dessous les scripts et les commandes Powershell utilisées :

```
PS C:\Users\Administrateur> ipconfig /all

Configuration IP de Windows

   Nom de l'h"te . . . . . . . . . . . : SRV-WIN-01
   Suffixe DNS principal . . . . . . . : ABSTERGO.INTERNAL
   Type de noeud. . . . . . . . . . . . : Mixte
   Routage IP activ, . . . . . . . . . : Oui
   Proxy WINS activ, . . . . . . . . . : Non
   Liste de recherche du suffixe DNS. : ABSTERGO.INTERNAL

Carte Ethernet LAN-Abstergo :

   Suffixe DNS propre … la connexion. . . :
   Description. . . . . . . . . . . . . . : Microsoft Hyper-V Network Adapter
   Adresse physique . . . . . . . . . . . : 00-15-5D-10-3C-02
   DHCP activ,. . . . . . . . . . . . . . : Non
   Configuration automatique activ,e. . . : Oui
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.68.1(pr,f,r,)
   Masque de sous-r,seau. . . .ÿ. . . . . : 255.255.255.0
   Passerelle par d,faut. . . .ÿ. . . . . :
   Serveurs DNS. . .  . . . . . . . . . . : 127.0.0.1
   NetBIOS sur Tcpip. . . . . . . . . . . : Activ,

Carte Ethernet WAN-Abstergo :

   Suffixe DNS propre … la connexion. . . :
   Description. . . . . . . . . . . . . . : Microsoft Hyper-V Network Adapter #2
   Adresse physique . . . . . . . . . . . : 00-15-5D-10-3C-01
   DHCP activ,. . . . . . . . . . . . . . : Oui
   Configuration automatique activ,e. . . : Oui
   Adresse d'autoconfiguration IPv4 . . . : 169.254.68.125(pr,f,r,)
   Masque de sous-r,seau. . . .ÿ. . . . . : 255.255.0.0
   Passerelle par d,faut. . . .ÿ. . . . . :
   NetBIOS sur Tcpip. . . . . . . . . . . : Activ,
```

```
PS C:\Users\Administrateur> Get-ADUser -Filter *


DistinguishedName : CN=Administrateur,CN=Users,DC=ABSTERGO,DC=INTERNAL
Enabled           : True
GivenName         :
Name              : Administrateur
ObjectClass       : user
ObjectGUID        : 71022eb8-81b9-43d1-8925-471980b4e621
SamAccountName    : Administrateur
SID               : S-1-5-21-3297936115-407780048-1493146685-500
Surname           :
UserPrincipalName :

DistinguishedName : CN=Invité,CN=Users,DC=ABSTERGO,DC=INTERNAL
Enabled           : False
GivenName         :
Name              : Invité
ObjectClass       : user
ObjectGUID        : 08695362-eb88-42e9-9936-a9b6253928bc
SamAccountName    : Invité
SID               : S-1-5-21-3297936115-407780048-1493146685-501
Surname           :
UserPrincipalName :

DistinguishedName : CN=krbtgt,CN=Users,DC=ABSTERGO,DC=INTERNAL
Enabled           : False
GivenName         :
Name              : krbtgt
ObjectClass       : user
ObjectGUID        : 76802823-9785-43d6-b705-52384ab43707
SamAccountName    : krbtgt
SID               : S-1-5-21-3297936115-407780048-1493146685-502
Surname           :
UserPrincipalName :
```

```
PS C:\Users\Administrateur> Get-ADDefaultDomainPasswordPolicy -Current LoggedOnUser


ComplexityEnabled           : True
DistinguishedName           : DC=ABSTERGO,DC=INTERNAL
LockoutDuration             : 00:30:00
LockoutObservationWindow    : 00:30:00
LockoutThreshold            : 0
MaxPasswordAge              : 42.00:00:00
MinPasswordAge              : 1.00:00:00
MinPasswordLength           : 7
objectClass                 : {domainDNS}
objectGuid                  : 36453ee4-5c4a-44bc-941d-a743fc9388ff
PasswordHistoryCount        : 24
ReversibleEncryptionEnabled : False



PS C:\Users\Administrateur> Get-ADDefaultDomainPasswordPolicy -Current LocalComputer


ComplexityEnabled           : True
DistinguishedName           : DC=ABSTERGO,DC=INTERNAL
LockoutDuration             : 00:30:00
LockoutObservationWindow    : 00:30:00
LockoutThreshold            : 0
MaxPasswordAge              : 42.00:00:00
MinPasswordAge              : 1.00:00:00
MinPasswordLength           : 7
objectClass                 : {domainDNS}
objectGuid                  : 36453ee4-5c4a-44bc-941d-a743fc9388ff
PasswordHistoryCount        : 24
ReversibleEncryptionEnabled : False
```

```
DistinguishedName : CN=Pierre Morin,OU=Comptabilité,OU=UtilisateursAbstergo,DC=ABSTER
                    GO,DC=INTERNAL
Enabled           : True
GivenName         : Pierre
Name              : Pierre Morin
ObjectClass       : user
ObjectGUID        : de457ce3-4c50-4997-b0a1-996f917cffd4
SamAccountName    : pmorin
SID               : S-1-5-21-3297936115-407780048-1493146685-1605
Surname           : Morin
UserPrincipalName : pmorin@ABSTERGO.INTERNAL
```

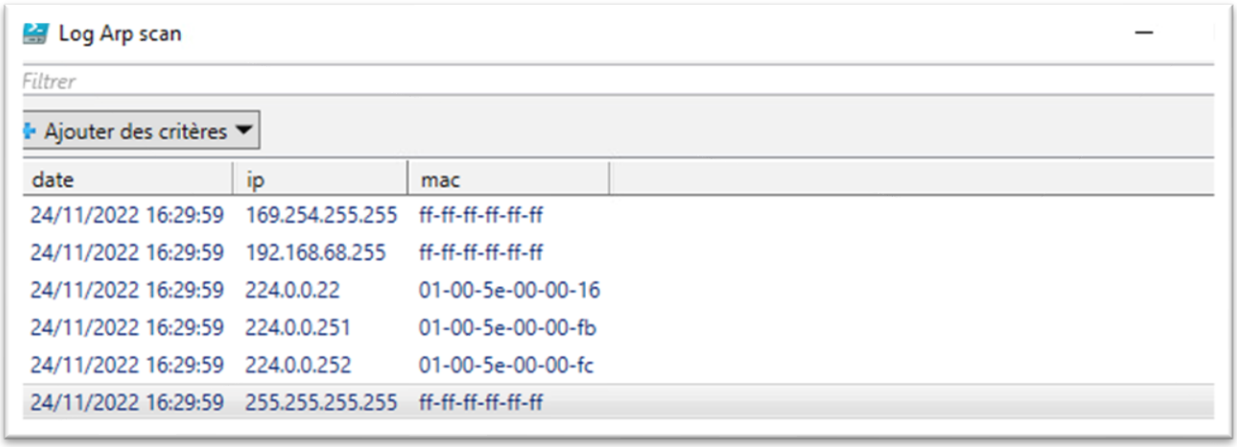
```
PS C:\Users\Administrateur> (Get-ADForest).Domains | %{ Get-ADDomaincontroller -Filter * -Server $_}


ComputerObjectDN           : CN=SRV-WIN-01,OU=Domain
                             Controllers,DC=ABSTERGO,DC=INTERNAL
DefaultPartition           : DC=ABSTERGO,DC=INTERNAL
Domain                     : ABSTERGO.INTERNAL
Enabled                    : True
Forest                     : ABSTERGO.INTERNAL
HostName                   : SRV-WIN-01.ABSTERGO.INTERNAL
InvocationId               : ef626046-8a0a-4a63-8a1b-2cb24ffc7996
IPv4Address                : 169.254.68.125
IPv6Address                : ::1
IsGlobalCatalog            : True
IsReadOnly                 : False
LdapPort                   : 389
Name                       : SRV-WIN-01
NTDSSettingsObjectDN       : CN=NTDS Settings,CN=SRV-WIN-01,CN=Servers,CN=Default-Fir
                             st-Site-Name,CN=Sites,CN=Configuration,DC=ABSTERGO,DC=IN
                             TERNAL
OperatingSystem            : Windows Server 2019 Datacenter
OperatingSystemHotfix      :
OperatingSystemServicePack :
OperatingSystemVersion     : 10.0 (17763)
OperationMasterRoles       : {SchemaMaster, DomainNamingMaster, PDCEmulator,
                             RIDMaster...}
Partitions                 : {DC=ForestDnsZones,DC=ABSTERGO,DC=INTERNAL,
                             DC=DomainDnsZones,DC=ABSTERGO,DC=INTERNAL,
                             CN=Schema,CN=Configuration,DC=ABSTERGO,DC=INTERNAL,
                             CN=Configuration,DC=ABSTERGO,DC=INTERNAL...}
ServerObjectDN             : CN=SRV-WIN-01,CN=Servers,CN=Default-First-Site-Name,CN=S
                             ites,CN=Configuration,DC=ABSTERGO,DC=INTERNAL
ServerObjectGuid           : dd360b85-24b8-444f-aa49-e116b4935dee
Site                       : Default-First-Site-Name
SslPort                    : 636
```

```
PS C:\Users\Administrateur> Get-ADForest -Current LocalComputer


ApplicationPartitions : {DC=DomainDnsZones,DC=ABSTERGO,DC=INTERNAL,
                        DC=ForestDnsZones,DC=ABSTERGO,DC=INTERNAL}
CrossForestReferences : {}
DomainNamingMaster    : SRV-WIN-01.ABSTERGO.INTERNAL
Domains               : {ABSTERGO.INTERNAL}
ForestMode            : Windows2016Forest
GlobalCatalogs        : {SRV-WIN-01.ABSTERGO.INTERNAL}
Name                  : ABSTERGO.INTERNAL
PartitionsContainer   : CN=Partitions,CN=Configuration,DC=ABSTERGO,DC=INTERNAL
RootDomain            : ABSTERGO.INTERNAL
SchemaMaster          : SRV-WIN-01.ABSTERGO.INTERNAL
Sites                 : {Default-First-Site-Name}
SPNSuffixes           : {}
UPNSuffixes           : {}
```

```powershell
Clear
#Fichier de logs
$logfile='d:\arp.log'
$logs=@()
$cmd=@()
#Récupération du contenu du fichier de logs existant
if(Test-Path -Path $logfile)
{
    $logs+=Import-CSV -Path $logfile
}
$date=Get-Date
#Balayage par pin du réseau 192.168.1.0/24
For($i=1;$i -lt 255;$i++)
{
    $ping =ping 192.168.68.$i -n 1 -w 5
    #Récupération de la commande arp -a toutes les 60 secondes
    if($date.AddSeconds(60) -lt (Get-date))
    {
        $cmd+=arp -a
        $date=Get-Date
    }
}
$cmd+=arp -a
#Elimination des doublons du fait de l'exécution régulière de arp -a
$cmd=$cmd|Sort -Unique
#Récupération des adresses ip et mac
ForEach($row in $cmd)
{
    if($row -match '^ +([0-9\.]+) +([0-9a-f\-]+) +[a-z]+ +$')
    {
        $ip=$Matches[1]
        $mac=$Matches[2]
        $logs+=[PSCustomObject]@{date=$date;ip=$ip;mac=$mac}
    }
}
#Sauvegarde des données de la table arp dans le fichier de logs
$logs| Export-Csv -NoTypeInformation -Path $logfile
#Falcultatif : affichage des résultats si vous exécutez le script en mode interactif
$logs|Out-GridView -Title 'Log Arp scan'
$logs=$null
```



IV) Plan d'amélioration :

A) Cartographie du système d'information :

Pour obtenir un SI plus sécurisé, il est essentiel de mettre en place un pare-feu et un proxy, avec des règles de filtrage ACL strictes.

Nous avons donc choisi de mettre en place un pare-feu logiciel et un proxy logiciel via PfSense.

Le pare-feu sera en mode « State Full » ce qui permet de vérifier que chaque paquet est conforme à une connexion en cours. Il s'assure donc que le paquet est bien la suite d'un précédent paquet, et la réponse à un paquet dans le sens inverse.

Nous avons choisi de virtualiser les pare-feux et proxys via PfSense et donc de ne pas les avoir en physique pour faciliter leur administration, mais surtout pour réduire les coûts élevés des solutions matérielles.

De plus, comme ils sont virtualisés et donc que les coûts sont plus faibles, pour obtenir un SI plus stable, on peut se permettre de rajouter un deuxième PfSense, ce qui permettra d'avoir un proxy, un pare-feu et un routeur logiciel de secours. Cependant, il faudra tout de même compter dans le budget un deuxième serveur PfSense. C'est ce qu'on a représenté dans la nouvelle cartographie avec la seconde branche.

PfSense permet également de mettre en place une DMZ via son routeur logiciel intégré. Nous recommandons de mettre en place une zone déminéralisée (DMZ) et d'y placer tous les éléments qui sont directement reliés à Internet pour améliorer la sécurité du réseau.

Pour ce qui est des serveurs, nous en avons mis 3 principaux et 2 de backup. Dans les 3 principaux, nous avons :

1 serveur sous Linux qui est dans la DMZ et qui contiendra le Wiki et le site vitrine.

1 autre serveur sous Linux dans le LAN qui contiendra les serveurs NFS, IPBX, TFTP, de données et l'ERP.

1 serveur sous Windows dans le LAN qui contiendra les services de l'active directory, de WSUS, de DHCP, de DNS, de partage SMB et le serveur d'impression.

De plus, nous recommandons également de rajouter des serveurs de backup virtualisé dans 2 serveurs un sous Windows et l'autre sous Linux, ils sont dans le LAN :

Dans le cas où l'Active Directory du Windows serveur principal viendrait à ne plus fonctionner rendant l'authentification du personnel impossible, il est prévu de mettre en place un Active Directory redondant (donc un deuxième serveur active directory) sur un Windows serveur lui-même redondant afin de permettre aux employés de travailler malgré un dysfonctionnement du Windows serveur. Le deuxième AD serait en lecture seule (RODC) afin qu'il ne soit pas possible de modifier la configuration du domaine puisque si le serveur principal est attaqué il ne faudrait pas que l'attaquant soit en mesure de s'octroyer des droits ou de prendre le contrôle des contrôleurs du domaine.

Un autre serveur WSUS pour continuer de pouvoir distribuer des mises à jour en cas de problème sur le premier. Ce serveur est virtualisé sur le serveur de backup Windows.

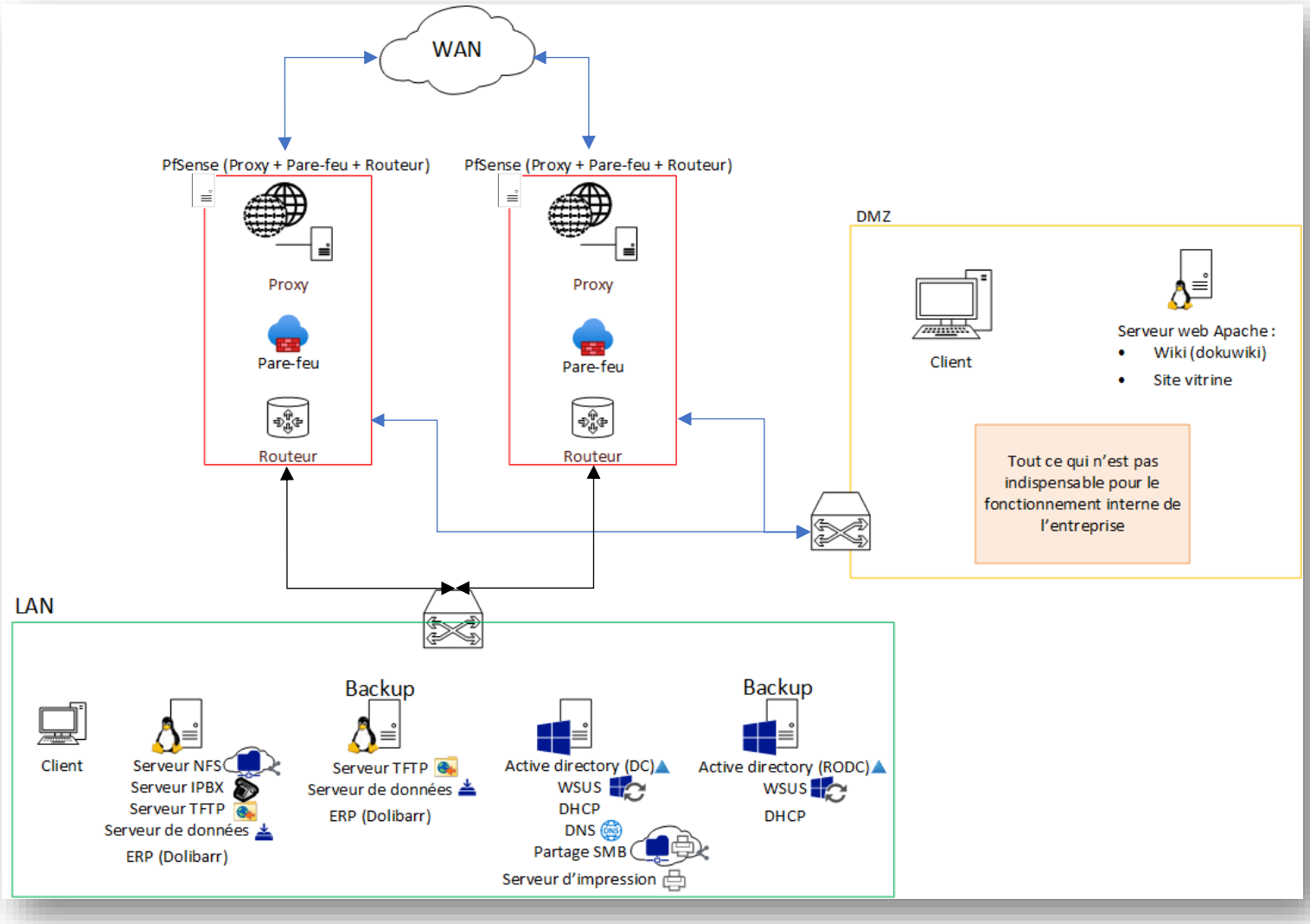
Un deuxième serveur DHCP pour l'attribution automatique des IP. Ce serveur est virtualisé sur le serveur de backup Windows.

Un deuxième serveur TFTP pour le transfert de fichier qui est important pour continuer l'activité de l'entreprise. Ce serveur est virtualisé sur le serveur de backup Linux.

Un autre serveur de données pour ne pas perdre notre travail en cas de problème sur le premier. Ce serveur est virtualisé sur le serveur de backup Linux.

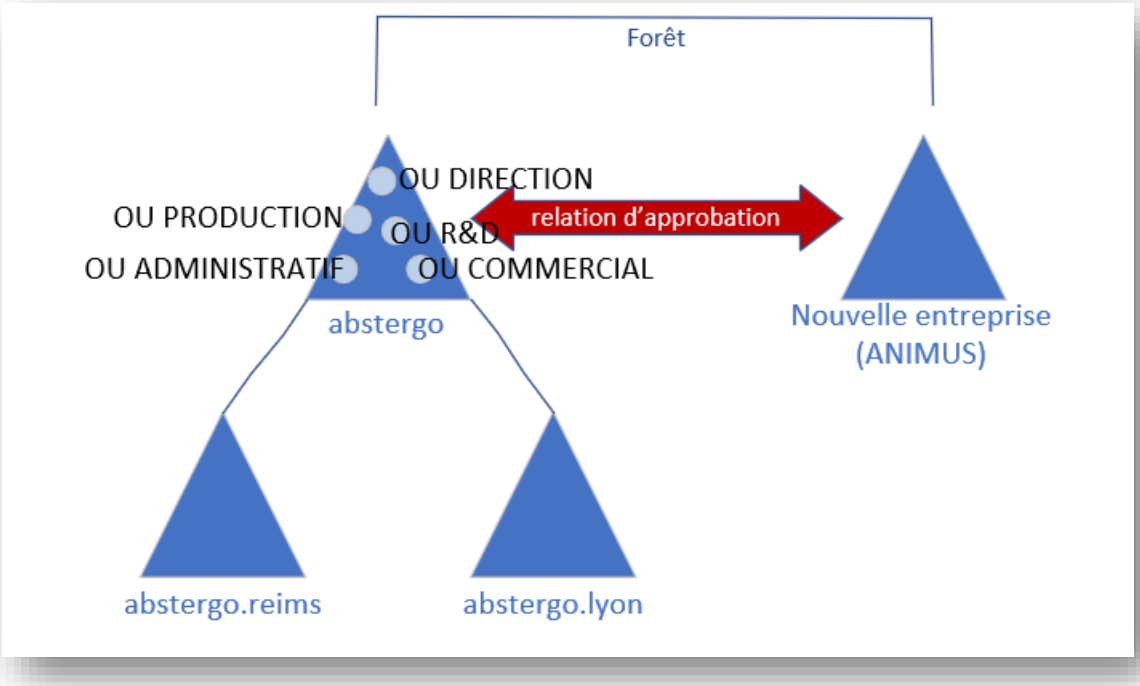
Et un deuxième serveur contenant le service d'ERP afin de s'assurer que cela ne paralyse pas l'entreprise si le premier rencontre un problème. Ce serveur est virtualisé sur le serveur de backup Linux.

Cartographie du nouveau S.I. :



B) Gestion des identités et l'accès aux données (active directory) :

Pour faciliter les mises à jour, la gestion des machines et le respect des stratégies et politiques de l'entreprise, nous vous recommandons de suivre ce nouveau plan d'active directory :



Chaque zone géographique de l'entreprise est un sous-domaine, les unités organisationnelles se trouvent dans le domaine d'Abstergo. De plus, le tout se trouve dans une forêt composée de deux arbres, le premier est notre entreprise et le second sera la nouvelle entreprise qui nous rachète. Ces arbres seront reliés entre eux grâce à une relation d'approbation bidirectionnelle. Cela permettra aux employés d'Animus de se connecter chez Abstergo et vice versa.

C) Virtualisation :

Nous avons décidé de virtualiser certains serveurs pour éviter de nous retrouver avec trop de serveurs. Cela permettra de faire des économies et de faciliter la gestion des serveurs.

Note : Pour la maquette tous les serveurs seront virtualisés dans hyper-v pour faciliter la démonstration, donc sur le même serveur. Dans la réalité il y aura bien plusieurs serveurs physiques.

Voici un résumé des virtualisations effectué :

Aux totales dans la réalité, nous aurons 3 serveurs.

Il y aura un premier serveur principal dans le LAN avec dedans un hyper-v qui contiendra 3 serveurs virtualisés, un PfSense, un Windows serveur et un Linux. Le PfSense s'occupera de faire le proxy, le pare-feu, le routage des sous-réseaux (WAN, LAN, DMZ), le DHCP. Le Windows serveur s'occupera de

faire l'active directory, le WSUS, le DNS, le partage SMB, le serveur d'impression. Le serveur Linux s'occupera de faire le NFS, le IPBX, le TFTP, le serveur de données et l'ERP.

Le deuxième serveur sera secondaire (de backup) dans le LAN avec dedans un hyper-v qui contiendra 3 serveurs virtualisés, un PfSense de secours identique au principal, un Windows serveur de secours différent du principal (il aura uniquement l'active directory (en RODC) et le WSUS) et un Linux qui sera aussi différent du principal (il aura uniquement le TFTP, le serveur de données et l'ERP de secours).

Et enfin le troisième serveur qui sera dans la DMZ, ce sera un serveur web Apache qui contiendra le site vitrine et le Wiki.

D) Sécurité :

Vecteurs d'attaques :

En termes de sécurité, nous avons vu précédemment que l'élément principal qu'il fallait corriger était la politique de mot de passe de l'entreprise. Le mot de passe était le même partout, ce qui rend l'intrusion aisée. Il faut donc remédier à cela en priorité. Pour y remédier, nous pouvons nous baser sur les règles de mot de passe éditées par la CNIL et le RGPD. On a par exemple pour un mot de passe très sécurisé une base obligatoire d'un minimum de 12 caractères, avec majuscules, minuscules, et caractères spéciaux. Il nous sera possible d'imposer cette politique par le biais de l'Active Directory.

Pour continuer, nous allons nous pencher sur les différents vecteurs d'attaque possibles en adoptant une approche de sécurité par les risques.

Les risques sur le système d'information peuvent se diviser en 4 grandes catégories, 4 grands vecteurs :

-Le vecteur humain : Dans ce vecteur, nous retrouvons tout ce que l'on pourrait appeler vulgairement « la bêtise humaine ». Nous identifions des menaces telles que le phishing ou encore des manipulations accidentelles et non voulues sur le poste. Nous sommes aussi ici confrontés aux problèmes des données de chaque employé que nous ne pouvons pas contrôler. Pour remédier à ces problèmes humains, il est possible d'utiliser l'Active Directory pour administrer et bloquer certaines tâches critiques, mais le principal axe de progrès est l'éducation des gens vis-à-vis de l'outil informatique.

-Le vecteur réseau : Pour ce vecteur, la principale cause serait une mauvaise mise en place de l'ensemble du réseau. Tout d'abord, un accès Internet avec un débit faible est problématique, mais ce débit dépend souvent du fournisseur d'accès à Internet et nous n'avons donc pas de levier direct sur ce point. Néanmoins, il est toujours possible de configurer les appareils de la façon la plus optimale possible pour gérer le réseau. D'un point de vue de la menace sécuritaire, la principale menace serait une attaque par déni de service distribué (DDoS) ou encore de Ransomware. Pour contrer un DDoS, des configurations et des pare-feux sont disponibles. Pour l'autre type d'attaque, c'est la sécurité globale du réseau qui sera mise à mal. Cela rejoint donc notre ajout d'un proxy et d'une zone démilitarisée sur le réseau.

-Le vecteur logiciel : D'un point de vue du logiciel, on peut se rapprocher des dangers réseau, spécialement si le logiciel est connecté à Internet. Il faut donc veiller à contrôler les logiciels utilisés,

d'autant plus si certains logiciels sont développés en interne. À part cela, la prochaine menace évoquée se rapproche du facteur humain. En effet, il faut pouvoir contrôler les installations et désinstallations de logiciels sur les ordinateurs des utilisateurs. À but de contrôle, on peut penser à l'utilisation d'un centre logiciel qui permet de contrôler les logiciels installables et éviter l'installation de logiciels inutiles ou pirates. On peut aussi finalement penser à interdire l'utilisation de fichiers avec extension .exe.

-Le vecteur physique : Pour le vecteur physique, on se rapproche beaucoup du côté hardware de l'informatique. On peut par exemple citer des restrictions sur les postes individuels des employés comme des restrictions sur les ports USB ou encore la caméra. On peut penser à ce vecteur encore de manière localisée. En effet, des accès aux différentes salles dans les locaux de l'entreprise doivent être contrôlés pour éviter d'éventuelles intrusions qu'elles émanent d'individus externes ou interne à la société. On peut retrouver des problèmes comme des vols, des dégradations ou encore des accès à des salles serveur ou il serait possible de se connecter directement sur le serveur ou de pouvoir les débrancher.

Audits :

Pour renforcer la sécurité, nous recommandons de passer des audits de sécurité aux employés et aux équipements afin de s'assurer que les normes de sécurité soient respectées. Un audit de qualité 9001 est déjà en cours, mais nous pouvons en rajouter comme la 27001 qui est la sécurité.

Politique et stratégie de l'entreprise :

Nous avons bientôt un audit qualité ISO 9001, il nous faut donc nous préparer à cet audit.

ISO 9001 :

Afin d'améliorer nos performances opérationnelles et de qualité, mais surtout de prouver nos compétences en qualité, nous avons entamé des démarches afin d'être audité ISO 9001 d'ici quelques semaines. Nous avons déjà commencé à prendre des actions correctives, mais voici pour rappel les points importants à retenir pour pouvoir être agrégés ISO 9001.

-Orientation client

-Leadership

-Implication du personnel

-Approche processus

-Amélioration continue

-Prise de décision fondée sur des preuves

-Management des relations avec les parties intéressées

-Approche risques et opportunité

De plus, afin d'améliorer l'image de notre entreprise, nous pensons pouvoir nous pencher sur la norme ISO 27001 qui permettrait d'attester de la qualité de notre Système de Management de la Sécurité et de l'Information (SMSI).

ISO 27001 :

Premièrement, cette norme internationale est peu répandue en France, car non obligatoire. Elle s'applique au niveau des systèmes de management de la sécurité de l'information. Malgré son caractère non obligatoire, elle fait de plus en plus souvent partie des nouveaux référentiels de sécurité, ce qui explique son évocation dans ce dossier.

Dans les faits, la norme a pour objectif de protéger et défendre l'entreprise des risques de vol, perte ou détérioration de données. Elle s'applique aussi bien au niveau informatique, hardware et software, mais aussi au niveau organisationnel et managérial.

Son processus d'application est le traitement de la sécurité par les risques. Afin de mettre en place et respecter cette norme, on commence par une analyse des risques susceptibles de peser sur les données. On réalise cette étude à tous les niveaux de l'entreprise afin de prendre en compte le maximum de paramètres.

À l'issue de cette étude, les risques identifiés vont être analysés pour établir un ratio entre leur probabilité de réalisation et l'impact de l'évènement.

C'est à l'issue de cette analyse que l'on va pouvoir commencer à regarder du côté des actions de protection et de prévention. Toutes les actions possiblement applicables sont détaillées dans la norme ISO 27002 et classées par importance : « doit », « peut », « est conseillé de ». Ce sera ensuite à la direction de l'entreprise de déterminer si les solutions conviennent selon un traitement réservé à chacun des risques :

-Réduction du risque en réduisant son impact.

-Prévention du risque, en réduisant la probabilité qu'il se produise.

-Partage du risque avec un prestataire.

-Acceptation du risque, par exemple si la mesure à mettre en place coûte trop cher par rapport au risque et aux bénéfices.

Finalement, la direction devra établir et signer une Déclaration d'Applicabilité pour certifier leur engagement et leur volonté d'appliquer et maintenir cette norme dans le temps. En effet, il faudra à la suite des opérations précédentes établir un plan d'action, l'appliquer et surtout suivre et contrôler les équipements pour s'assurer de la bonne mise en place et du bon maintien des actions liées à la norme.

Gouvernance :

Concernant les mots de passe, nous avons découvert que la stratégie de mots de passe était inexistante et toutes les installations étaient sécurisées par le même mot de passe. Les mots de passe étant un élément essentiel dans la sécurisation du Système d'information, nous comptons mettre en place une importante politique de mots de passe.

Tout d'abord, nous allons appliquer des règles au contenu du mot de passe. En effet, nous allons imposer une durée minimale de 12 caractères (comme suggéré par l'ANSSI) ainsi que l'utilisation d'au moins une majuscule, une minuscule, un caractère spécial ainsi qu'un chiffre. Ces restrictions de types de caractères rentrent dans la règle des exigences de complexité des mots de passe.

En parallèle de cela, seront ajoutées des règles de blocage de compte en cas de mauvaise entrée de mot de passe. La session utilisateur pourra se bloquer pendant un temps donné si l'utilisateur rentre trop de fois un mot de passe erroné. Dans le cas où un compte utilisateur viendrait à être bloqué, il sera nécessaire à l'utilisateur de contacter son administrateur système pour permettre un déblocage.

Finalement, il est possible de limiter la vie du mot de passe dans le temps et d'obliger l'utilisateur à changer de mot de passe à intervalle de temps régulier. Nous comptons mettre cet intervalle de temps à 3 mois.

GPO :

En lien avec la gouvernance présentée plus tôt, nous nous basons sur les stratégies de groupe ici afin de garantir de hauts standards de sécurité, mais aussi permettre d'uniformiser le SI pour rendre son maintien plus simple.

Nous les utilisons dans un premier temps pour éditer des stratégies de mots de passe. Nous avons donc pu configurer certains paramètres pour forcer les utilisateurs à utiliser des mots de passe forts. Nous avons donc défini une longueur minimale obligatoire. Cela s'ajoute à l'activation de la règle des exigences de complexité du mot de passe. En effet, cette règle permet d'obliger à utiliser une minuscule, une majuscule, un caractère spécial ainsi qu'un caractère numérique.

En lien avec les mots de passe, nous avons défini des stratégies de blocage de compte. Le compte utilisateur auquel l'utilisateur essaye de se connecter pourra automatiquement se bloquer en cas d'un nombre trop important de tentatives infructueuses.

Maintenant que l'accès au compte utilisateur est sécurisé, il nous faut sécuriser « l'intérieur » du compte. C'est ainsi que nous avons choisi d'appliquer la stratégie de restriction d'installation de logiciels. Dans les faits, cette stratégie va bloquer l'utilisation de fichiers exécutables comme les fichiers .exe, .bat, .msi ainsi que les scipts de l'invité de commande Windows.

La prochaine étape est la modération de l'accès au panneau de configuration. Les utilisateurs n'auront donc pas accès à l'entièreté des fonctionnalités du panneau de configuration afin d'éviter que les utilisateurs puissent modifier en profondeur leur environnement de travail.

Dans le même objectif, nous souhaitons restreindre l'accès aux périphériques de stockage amovibles. Cela va permettre d'éviter d'avoir à faire face à des problèmes d'intrusion par le biais de périphériques externes que des utilisateurs pourraient brancher.

Il est possible grâce aux GPO de monitorer les mises à jour de Windows et des autres applications Microsoft. En effet, nous pouvons gérer le service Windows Update et choisir à quel moment nous allons lancer les mises à jour sur l'ensemble de nos postes, ajouter des délais avant les mises à jour ou encore choisir d'utiliser un serveur WSUS ou non. Cette GPO est utile à un but sécuritaire, car elle évite que des utilisateurs puissent changer ou refuser de changer de version de système d'exploitation. C'est en plus un fantastique outil de gestion qui permet d'éviter à devoir mettre manuellement à jour l'ensemble des postes.

Toujours dans la maîtrise de l'environnement utilisateur, on peut citer la GPO d'Installation de logiciels. En effet, en configurant cette GPO, il est possible d'automatiser l'installation et la diffusion de logiciel sur les postes. L'installation s'effectue automatiquement dès lors que le poste rejoint le domaine ou une Unité d'Organisation. La liste des applications à installer est à paramétrer dans le menu des GPO. Il est donc possible de fournir à un employé un ordinateur équipé de tous les logiciels nécessaires pour débuter son installation et ses activités.

E) Procédure de migration et retours en arrière :

Procédure de migration :

Une migration de S.I. est une étape extrêmement délicate. Elle demande un certain savoir-faire afin de surmonter les difficultés régulièrement rencontrées, et préserver la sécurité et l'intégrité de données de l'entreprise.

C'est pourquoi nous avons décidé d'expliquer la procédure à appliquer afin d'éviter de mauvaise surprise :

- Client et entreprise :

La première étape consiste à alerter en amont les clients et les collaborateurs de l'entreprise qu'une migration du S.I. va être effectuée et donc qu'ils n'auront pas accès à certains services de l'entreprise pendant ce temps (c'est pourquoi nous recommandons d'effectuer la migration la nuit pour impacter le moins de personnes possible).

- Sauvegarde :

Une fois l'alerte lancée et que les acteurs soient informés, on commencera l'opération de sauvegarde. Il s'agit de faire un backup du S.I. actuel afin de pouvoir revenir en arrière en cas de problème.

- Migration principale :

Lorsqu'on est sûr que la sauvegarde est opérationnelle, nous commencerons par ajouter le serveur PfSense principales et nous transférons les différents services (comme l'active directory) dans leurs nouvelles zones (LAN ou DMZ). Puis nous activerons les différentes règles de sécurité (comme le pare-feu via un filtrage ACL).

- Validation du début de la migration :

Une fois la migration principale effectuée, nous vérifierions que les services soient tous opérationnels et intègres.

- Ajout de la redondance :

En suit, il faudra ajouter les différentes redondances afin de s'assurer que le réseau soit stable dans le temps.

- Retour des acteurs du nouveau S.I. :

Enfin, nous nous assurons que les retours des clients et des collaborateurs sur le nouveau S.I. soient positifs, le cas échéant, il faudra remédier au potentiel problème rencontré.

Retour en arrière :

Pour anticiper une erreur dans la migration ou une intrusion malveillante dans notre S.I. visant à détruire nos services, configurations et données, il est important de sauvegarder ces derniers sur des serveurs isoler du SI afin de pouvoir y accéder après une attaque qui aurait réussi. Pour les configurations de nos éléments informatiques une nouvelle backup est nécessaire à chaque mise à jour de la configuration, pour les données il vaut mieux faire une backup selon un temps défini au vu de la quantité d'actions qu'il y a sur le SI en même temps, par exemple une backup des données présente dans les bases de données tous les jours avant que les employés arrivent sur site.

Conclusion

Nous avons donc ici exposé notre plan de remédiation pour la remise à niveau du système d'information d'Abstergo. L'analyse de l'existant ainsi que les échanges avec nos nouveaux collègues ont permis d'identifier rapidement les points critiques et de mettre en place des actions correctives.

Le système d'information a été amélioré pour répondre aux exigences opérationnelles requises pour le bon fonctionnement de l'entreprise et donc permettre le rachat par Animus. Nous n'avons pas oublié la norme ISO 9001 pour laquelle nous serons audités dans les jours à venir.

Nos objectifs ont été l'amélioration des performances, de la sécurité, mais aussi de la fiabilité et de la facilité d'administration. C'est dans ce cadre la que nous avons mis en place une gouvernance de données et une politique de sécurité pour les mots de passe afin d'assurer de bons niveaux de sécurité. L'Active Directory et les GPO nous on permit de mettre en place les stratégies de sécurité, mais aussi de centraliser le contrôle sur les différents postes et comptes utilisateurs.

De plus, nous avons voulu faire attention aux coûts des nouvelles infrastructures et avons donc décidé de virtualiser certains services pour éviter une explosion des dépenses au niveau informatique.