CESI

Livrable 2

Projet Administration du Système d'Information

Groupe 1 : Hugo Breniaux – Arnaud Hittinger – Arthur Lambert
18/10/2021

Table des matières

Contexte

La société ANIMUS, leader mondial dans les télécommunications multi-niveaux, ne cesse de s'accroître du fait des besoins croissants sur ce marché.

Elle procède régulièrement à des rachats d'entreprises et notamment des PME. Elle avait entendu parler récemment des difficultés d'une entreprise nommée ABSTERGO qui s'est spécialisée dans les protocoles Bluetooth nouvelle génération.

Cette opportunité n'était pas à rater et, rapidement, la vente de la société s'était conclue.

Comme à chaque fois, il est prévu d'intégrer le Système d'Information de l'entreprise rachetée dans celui d'ANIMUS.

Le procédé est toujours le même :

- L'environnement système est rattaché à celui d'ANIMUS
- Les paramètres de sécurité sont configurés sur le modèle défini par ANIMUS
- Les dernières vérifications d'optimisation sont faites et les procédures sont mises à jour

Malheureusement, cette fois-ci, un gros problème se pose : l'administrateur système de l'entreprise a démissionné peu de temps avant le rachat et celui-ci n'est pas localisable malgré les recherches.

Il semblerait que, cette fois-ci, la tâche ne soit pas aussi facile ...

Dès que l'administrateur système aura été contacté, un accès au système d'information d'ABSTERGO vous sera donné.

LIVRABLE 2 : Avant toute autre action de migration, il conviendra de vérifier que la sécurité est conforme aux attentes du S.I.. Après une longue étude, il a été décidé de fixer le rendu du rapport de sécurité au mercredi 3 novembre. Bien qu'il ne vous est demandé qu'un rapport, il est prudent de mettre en place certains aspects techniques qui, de toute façon, feront partie de la maquette à présenter le mardi 9. En plus de l'infrastructure sécurisée avec DMZ, filtrage et VPN pour les nomades, il faudra également s'assurer que les données circulant sur le réseau soient parfaitement protégées et fiables et que la gestion des éventuels certificats est rigoureuse. Bien évidemment, l'authentification via l'Active Directory est le dernier élément indispensable. Libre à vous de compléter par des préconisations supplémentaires ...

Sécurité actuelle du SI

Cryptographie

Les données transitant sur le réseau ne semblent pas chiffrées. Cela signifie donc que les serveurs ne possèdent pas de certificats permettant le chiffrage et la sécurisation des données en transit sur le réseau entre client-serveur. Néanmoins la machine Windows possède un protocole Kerberos permettant une authentification mutuelle entre un client et un serveur, il utilise un chiffrement par clé secrète (permettant aussi le déchiffrement) pour le trafic d'authentification du client.

Pour ce qui est des mots de passes, ils sont stockés dans un fichier chiffré (KeePass), mais ce sont tous les mêmes mots de passes, cela créé une faille de sécurité. De plus les mots de passes sont actuellement un point majeur de la sécurité d'un système et doivent donc être traités avec grande attention.

L'organisation ne possède pas non plus de services SSO pour l'authentification des utilisateurs sur plusieurs applications.

Sécurité

Il ne semble pas y avoir de campagnes de sensibilisation concernant la sécurité, confidentialité et intégrité des données. On peut prendre comme exemple le phishing, ou des pièces jointes malicieuses dans des mails.

La hiérarchie au sein de l'entreprise ne semble pas non plus être pris en compte de manière sérieuse, en démontre la gestion des mots de passe, et des périphériques sur le réseau (annuaire AD).

Communication

En termes de communication, les messages de maintenance sont affichés sur de simple feuilles, et ne sembleraient pas être communiqués par des moyens numériques (tel que les courriels) permettant de garder la trace de différents évènements / informations déplacées au sein de l'organisation. Ils ne permettent pas non plus d'assurer la bonne transmission des informations aux employés visés.

Optimisation

Concernant les applications et services dans l'entreprise, ils ne sont pas déployés de manière optimisé, ni même maintenu convenablement (backups, …). Il y a possibilité d'utiliser docker et/ou des scripts PowerShell pour un déploiement optimisé des applications et des services, mais aussi de leurs maintenances tout un assurant un versioning et une isolation adapté.

Sauvegardes

Il ne semble pas y avoir de politique de sauvegardes au sein de l'entreprise.

Réseau

Le réseau ne possède pas de DMZ (avec un pare-feu, un proxy, …) permettant de filtrer les accès et requêtes au réseau, ainsi que permettre l'accès à différents services (par exemple des pages Web) ce qui ajouterais une couche de sécurité supplémentaire s'il était présent dans le réseau.

Le réseau de l'organisation n'est pas divisé en plusieurs sous-réseaux (invités, comptabilité, …) permettant la gestion, l'organisation et la séclusion des flux de données et des différents services et/ou parties de l'entreprise.

Les machines linux ne possèdent pas de service **VPN** permettant la connexion en dehors du réseau local (depuis l'extérieur), contrairement à la machine Windows (disposant du **Secure Socket Tunneling Protocol Service**[1] et du **Remote Access Connection Manager**[2]), mais qui n'est pas paramétré (fonctionnel).

Des services **SSH** permettant la gestion des serveurs à distance sont actifs sur les machines linux, il ne semblerait pas y en avoir sur la machine Windows.

[1] *Un type de tunnel VPN qui fournit un mécanisme pour transporter PPP ou L2TP à travers un canal SSL 3.0. SSL fournit une sécurité au niveau transport avec une négociation de clés, le chiffrement, et le contrôle de l'intégrité des données.*

[2] *Gère les connexions d'accès à distance et VPN de l'ordinateur à Internet ou à d'autres réseaux distants.*

Hypothèses sur l’entreprise ABSTERGO

- Le nombre d’employés sera de : 100.
- On fixe à 20 le nombres d’employés « nomade »
- Des sous-traitant devrons pouvoir accéder à certaines ressources de l’entreprise.

Mise en place d'une sécurité conforme aux exigences du SI

Filtrage

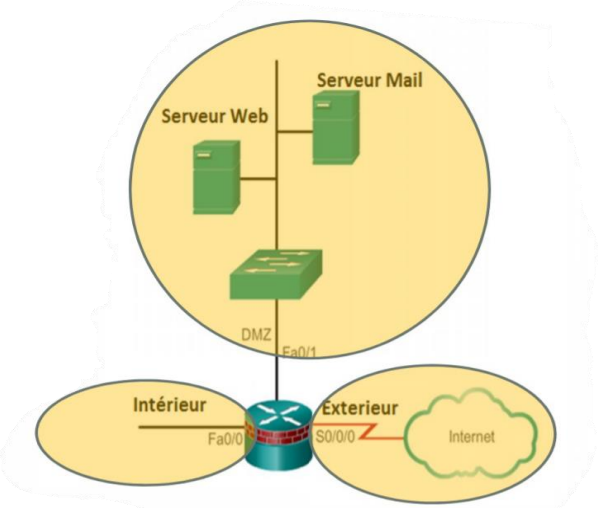
Le pare feu :

Un **pare-feu** (de l'anglais *firewall*) est un logiciel et/ou un matériel permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique. Il surveille et contrôle les applications et les flux de données (paquets).

Sa fonction de base est de réaliser une inspection sur le trafic transitant, vérifier qu'il est conforme aux règles, laisser passer le « bon » trafic, bloquer, signaler, jeter le « mauvais » trafic.

Il permet de séparer le réseau en trois zones :

- **Le LAN (l'intérieur)**
- **Le WAN (l'extérieur)**
- **La DMZ**
    - **Zone démilitarisée**
    - **Zone spéciale autorisant un accès public de l'extérieur**



Types de pare-feu

Un pare-feu peut être un :

- **Pare-feu logiciel**
    - Un poste de travail avec un logiciel pare-feu
- **Pare-feu matériel**
    - Une boite noire spécial qui contient un logiciel
- **Pare-feu Proxy**

Un firewall matériel ou logiciel ?

Un pare-feu logiciel hérite de toutes les vulnérabilités du système d'exploitation sur lequel ils s'exécutent. L'architectures du pare-feu logiciel est connu, donc c'est souvent plus facile d'y exploiter ses vulnérabilités.

Pare-feu Proxy :

Il sert de relais entre deux réseaux en s'interposant et en effectuant une validation fine du contenu des paquets échangés. Le proxy représente donc un intermédiaire entre les machines du réseau interne et le réseau externe, subissant les attaques à leur place. De plus, le filtrage applicatif permet la destruction des en-têtes précédant le message applicatif, ce qui permet de fournir un niveau de sécurité supplémentaire.

Il s'agit d'un dispositif performant, assurant une bonne protection du réseau, pour peu qu'il soit correctement administré. En contrepartie, une analyse fine des données applicatives requiert une grande puissance de calcul et se traduit donc souvent par un ralentissement des communications, chaque paquet devant être finement analysé.

Les principes de base

- **Moindre privilège**
- **Défense en profondeur**
- **Goulot d'étranglement**
- **Interdiction par défaut**
- **Participation de l'utilisateur**
- **Simplicité**

Le moindre privilège :

Ne pas accorder aux utilisateurs du réseau protégé par le pare feu des droits dont ils n'ont pas besoin.

Exemple :

- Interdire le P2P dans une entreprise
- Limiter la taille du téléchargement
- Les utilisateurs réguliers ne doivent pas être des administrateurs
- Les administrateurs doivent également utiliser des comptes utilisateurs

Défense en profondeur :

Utiliser les moyens de protection à tous les niveaux possibles, ce qui permet d'évite de laisser entrer des communications indésirables. Des moyens autres que le firewall comme les antivirus, antispam, etc...

Exemple :

- Installer des Anti-virus à plusieurs niveaux.
- Sur les PC, sur les Serveurs, sur un hyperviseur
- Sécuriser les machines même celles qui sont protégées par le pare feu

Goulot d'étranglement :

Toutes les communications entrant ou sortant du réseau doivent transiter par le pare feu. Il ne faut pas avoir plusieurs points d'entrée sur un réseau.

Exemple :

- Eviter l'utilisation des modems sur le LAN

Interdiction par défaut :

En première règle → il faut tout interdire. Ensuite autoriser explicitement le trafic « conforme », ce qui permet d'éviter tout transit involontairement accepté (Oublie de certaines menaces).

Participation de l'utilisateur :

- Les utilisateurs doivent être impliqués dans la mise en place du pare feu.
- Ils doivent exprimer leurs besoins
- Ils recevront en échange les raisons et les objectifs de la politique de sécurité

Les contraintes du pare feu seront acceptées

- Moins d'objections
- Comprendre les besoins de l'utilisateur
- S'assurer que les raisons de restrictions sont bien comprises

Simplicité :

Les règles de filtrage du pare feu doivent être les plus simples

- Pour assurer qu'elles compréhensibles
- Eviter toutes les erreurs de conception
- Il serait plus facile de vérifier le bon fonctionnement

Dans notre situation

Dans notre situation, nous allons utiliser un **pare-feu logiciel** qui sera installé sur une machine virtuelle. Le logiciel de pare-feu que nous allons utiliser sera **PfSense**.

Filtrage

Un pare-feu permet de mettre en place un ensemble de règles sur les données qui transite par lui. C'est ce qu'on appel le filtrage, et c'est règles sont définit par les administrateurs réseaux qui suivent la politique de sécurité de l'entreprise.

Il existe plusieurs méthodes de filtrages :

- **Le Filtrage simple de paquets**
- **Le Filtrage dynamique**
- **Le Filtrage applicatif**

Le filtrage simple de paquets

Le principe du filtrage simple de paquets et le filtrage de base d'un pare-feu. Il analyse les en-têtes de chaque paquet de données échangé entre une machine du réseau interne et une machine extérieure.

Ainsi, les paquets de données échangée entre une machine du réseau extérieur et une machine du réseau interne transitent par le pare-feu et possèdent les en-têtes suivants, systématiquement analysés par le firewall :

- adresse IP de la machine émettrice ;
- adresse IP de la machine réceptrice ;
- type de paquet (TCP, UDP, etc.) ;
- numéro de port (rappel : un port est un numéro associé à un service ou une application réseau).

Les adresses IP contenues dans les paquets permettent d'identifier la machine émettrice et la machine cible, tandis que le type de paquet et le numéro de port donnent une indication sur le type de service utilisé.

Le tableau ci-dessous donne des exemples de règles de pare-feu :

Règle	Action	IP source	IP dest	Protocol	Port source	Port dest
1	Accept	192.168.10.20	194.154.192.3	tcp	any	25
2	Accept	any	192.168.10.3	tcp	any	80
3	Accept	192.168.10.0/24	any	tcp	any	80
4	Deny	any	any	any	any	any

Les ports reconnus (dont le numéro est compris entre 0 et 1023) sont associés à des services courants (les ports 25 et 110 sont par exemple associés au courrier électronique, et le port 80 au Web). La plupart des dispositifs pare-feu sont au minimum configuré de manière à filtrer

les communications selon le port utilisé. Il est généralement conseillé de bloquer tous les ports qui ne sont pas indispensables (selon la politique de sécurité retenue).

Le port 23 est par exemple souvent bloqué par défaut par les dispositifs pare-feu car il correspond au protocole Telnet, permettant d'émuler un accès par terminal à une machine distante de manière à pouvoir exécuter des commandes à distance. Les données échangées par Telnet ne sont pas chiffrées, ce qui signifie qu'un individu est susceptible d'écouter le réseau et de voler les éventuels mots de passe circulant en clair. Mieux vaut utiliser le protocole SSH, réputé sûr et fournissant les mêmes fonctionnalités que Telnet.

Le filtrage dynamique

Le filtrage simple de paquets ne s'attache qu'à examiner les paquets IP indépendamment les uns des autres, ce qui correspond au niveau 3 du modèle OSI. Or, la plupart des connexions reposent sur le protocole TCP, qui gère la notion de session, afin d'assurer le bon déroulement des échanges. D'autre part, de nombreux services (le FTP par exemple) initient une connexion sur un port statique, mais ouvrent dynamiquement (c'est-à-dire de manière aléatoire) un port afin d'établir une session entre la machine faisant office de serveur et la machine cliente.

Ainsi, il est impossible avec un filtrage simple de paquets de prévoir les ports à laisser passer ou à interdire. Pour y remédier, le système de **filtrage dynamique de paquets** est basé sur l'inspection des couches 3 et 4 du modèle OSI, permettant d'effectuer un suivi des transactions entre le client et le serveur. Le terme anglais est « **stateful inspection** » ou « *stateful packet filtering* », traduisez « *filtrage de paquets avec état* ».

Un dispositif pare-feu de type « stateful inspection » est ainsi capable d'assurer un suivi des échanges, c'est-à-dire de tenir compte de l'état des anciens paquets pour appliquer les règles de filtrage. De cette manière, à partir du moment où une machine autorisée initie une connexion à une machine située de l'autre côté du pare-feu ; l'ensemble des paquets transitant dans le cadre de cette connexion seront implicitement acceptés par le pare-feu.

Si le filtrage dynamique est plus performant que le filtrage de paquets basique, il ne protège pas pour autant de l'exploitation des failles applicatives, liées aux vulnérabilités des applications. Or ces vulnérabilités représentent la part la plus importante des risques en termes de sécurité.

Le filtrage applicatif

Le filtrage applicatif permet de filtrer les communications application par application. Le filtrage applicatif opère donc au niveau 7 (couche application) du modèle OSI, contrairement au filtrage de paquets simple (niveau 4). Le filtrage applicatif suppose donc une connaissance des protocoles utilisés par chaque application.

Le filtrage applicatif permet, comme son nom l'indique, de filtrer les communications application par application. Le filtrage applicatif suppose donc une bonne connaissance des applications présentes sur le réseau, et notamment de la manière dont elle structure les données échangées (ports, etc.).

Un firewall effectuant un filtrage applicatif est appelé généralement « passerelle applicative » (ou « proxy »), car il sert de relais entre deux réseaux en s'interposant et en effectuant une validation fine du contenu des paquets échangés. Le proxy représente donc un intermédiaire entre les machines du réseau interne et le réseau externe, subissant les attaques à leur place. De plus, le filtrage applicatif permet la destruction des en-têtes précédant le message applicatif, ce qui permet de fournir un niveau de sécurité supplémentaire.

Il s'agit d'un dispositif performant, assurant une bonne protection du réseau, pour peu qu'il soit correctement administré. En contrepartie, une analyse fine des données applicatives requiert une grande puissance de calcul et se traduit donc souvent par un ralentissement des communications, chaque paquet devant être finement analysé.

Par ailleurs, le proxy doit nécessairement être en mesure d'interpréter une vaste gamme de protocoles et de connaître les failles afférentes pour être efficace.

Enfin, un tel système peut potentiellement comporter une vulnérabilité dans la mesure où il interprète les requêtes qui transitent par son biais. Ainsi, il est recommandé de dissocier le pare-feu (dynamique ou non) du proxy, afin de limiter les risques de compromission.

Dans notre situation

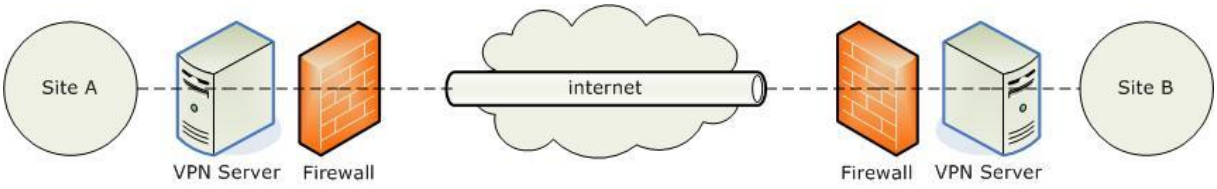
Dans notre situation, nous allons mettre en place **un filtrage simple de paquets** grâce au pare-feu **PfSense**.

VPN

Un VPN (Virtual private network) est un système permettant de créer un lien direct entre des ordinateurs distants, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics.

L'objectif est de créer un lien virtuel entre deux points, par exemple entre deux réseaux d'entreprise, ou entre un PC client et un réseau d'entreprise. Au sein de ce lien, les données seront sécurisées et isolées du reste du trafique, c'est là tout l'intérêt du VPN et cette notion de "privé". Le VPN permet de créer une extension virtuelle de votre réseau local jusqu'à un autre réseau (site) ou jusqu'à un poste de travail distant.

Le VPN va chiffrer les données de bout-en-bout, c'est-à-dire de l'équipement qui ouvre le tunnel jusqu'à son point de terminaison. Grâce à cela, il renforce la confidentialité des échanges au travers de réseaux non sécurisés (exemple : hotspot public).



Il existe plusieurs Protocoles permettant d'utiliser un VPN :

- GRE (*Generic Routing Encapsulation*) développé au départ par Cisco, à l'origine protocole transportant des paquets de couche 3, mais pouvant désormais aussi transporter la couche 2
- PPTP (*Point-to-Point tunneling Protocol*) est un protocole transportant des trames de couche 2 (du PPP) développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics.
- L2F (*Layer Two Forwarding*) est un protocole transportant des trames PPP (couche 2) développé par Cisco Systems, Nortel et Shiva. Il est désormais obsolète.
- L2TP (*Layer Two Tunneling Protocol*) est l'aboutissement des travaux de l'IETF (RFC 3931) pour faire converger les fonctionnalités de PPTP et L2F. Il s'agit ainsi d'un protocole transportant des sessions PPP (couche 2).
- IPsec est un protocole transportant des paquets (couche 3), issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP. Il est associé au protocole IKE pour l'échange des clés.
- L2TP/IPsec est une association de ces deux protocoles (RFC 3193) pour faire passer du PPP sur L2TP sur IPsec, en vue de faciliter la configuration côté client sous Windows.
- SSL/TLS, déjà utilisé pour sécuriser la navigation sur le web via HTTPS, permet également l'utilisation d'un navigateur Web comme client VPN. Ce protocole est notamment utilisé par OpenVPN.

- SSH permet, entre autres, d'envoyer des paquets depuis un ordinateur auquel on est connecté.
- MPLS permet de créer des VPN distribués (VPRN) sur un nuage MPLS, de niveau 2 (L2VPN) point à point, point à multipoint (VPLS), ou de niveau 3 (L3VPN) notamment en IPv4 (VPNv4) et/ou IPv6 (VPNv6 / 6VPE), par extension et propagation de VRF (*Virtual routing and forwarding* – tables de routage virtuelles) sur l'ensemble du réseau MPLS.

Tableau 1 Différents protocole

	Pour	Contre
PPTP	Rapide. Client intégré sur presque toutes les plateformes. Facile à configurer.	Craqué par la NSA. Pas entièrement sûr.
L2TP	Considéré comme habituellement fiable. Disponibles sur tous les appareils modernes et systèmes opératoires. Facile à configurer.	Plus lent qu'un OpenVPN. Il est possible que la NSA le craque. Soucis possibles avec firewall restrictif. La NSA a peut-être volontairement fragilisé ce protocole.
OpenVPN	Peut contourner la plupart des firewalls. Hautement configurable. Puisque c'est un open source, on peut facilement vérifier la présence de backdoors. Il est compatible avec de nombreux algorithmes de cryptage. Hautement sécurisé.	Peut-être un peu dur à configurer. Nécessite des logiciels tiers. Parfait sur ordinateur, a besoin d'améliorations sur mobile.
SSTP	Peut contourner la plupart des firewalls. Le niveau de sécurité dépend du cryptage, mais il est habituellement sûr. Complètement intégré au système d'exploitation Windows. Prise en charge Microsoft.	Puisque c'est une norme propriétaire appartenant à Microsoft, on ne peut pas vérifier la présence de backdoors. Marche seulement sur plateforme Windows
IKEv2	Extrêmement sécurisé : nombreux cryptages pris en charge, comme 3DES, AES, AES 256. Prend en charge les appareils BlackBerry. Stable, surtout quand il se reconnecte après avoir perdu la connexion ou changé de réseau. Facile à configurer, du moins pour l'utilisateur. Un peu plus rapide que L2TP, PPTP et SSTP.	Peu de plateformes pris en charge. Port 500 UDP plus facile à bloquer que les solutions SSL, comme SSTP ou OpenVPN. Pas de solution open source Installation difficile côté serveur, ce qui cause des problèmes.

VPN Client-to-site

On parle de VPN Client-to-site, lorsque le tunnel VPN est établi entre un PC client et un réseau d'entreprise.

Par exemple, pour des employés travaillant hors du site mais nécessitant d'avoir accès à des ressources internes à l'entreprise.

On ne peut ouvrir les ports sur le pare-feu de l'entreprise pour obtenir un accès sur chaque serveur. D'une part, ce n'est pas pratique. D'autre part, ce serait catastrophique en matière de sécurité informatique. On ne peut pas non plus installer un logiciel de prise en main à distance (Teamviewer, AnyDesk, etc.) sur chaque serveur.

La solution la plus sûre est l'utilisation du VPN, parfaitement adapté à cet usage.

Ce type de VPN s'applique également pour donner accès à des partenaires à une ressource de notre réseau interne.

Pour l'utiliser, il nécessite généralement que l'utilisateur se connecte par l'intermédiaire d'un client VPN. Soit celui intégré au système, comme Windows, ou en fonction du protocole utilisé, d'un logiciel spécifique.

Dans notre situation

Dans notre situation, nous devons pouvoir garantir un accès à distance aux ressources de l'entreprise aux différents **employés nomades** de l'entreprise (les employés travaillant hors du site) et un **VPN Client To Site** remplirait tous c'est besoin. De plus **PfSense** permet d'utiliser le protocole **OpenVPN** permettant d'établir une connexion distante de façon sécurisée grâce au chiffrement.

DMZ

Dans les réseaux informatiques, une DMZ, où zone démilitarisée, est un sous - réseau physique ou logique qui sépare un réseau local (LAN) d'autres réseaux non fiables, généralement l'Internet public. Les DMZ sont également appelées réseaux de périmètre ou sous- réseaux blindés.

Tout service fournit aux utilisateurs sur l'Internet public doit être placé dans le réseau DMZ. Les serveurs, ressources et services externes y sont généralement situés. Certains des services les plus courants incluent le Web, la messagerie électronique, le système de noms de domaine, le protocole de transfert de fichiers et les serveurs proxy.

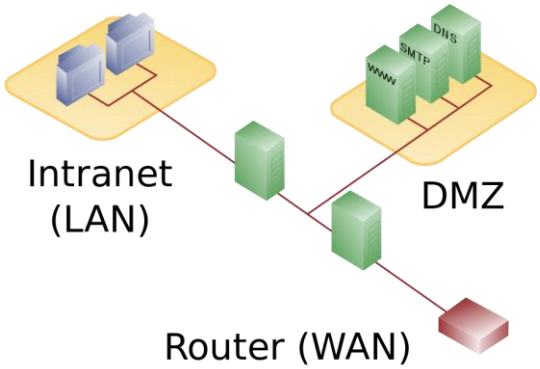
Les serveurs et les ressources de la DMZ sont accessibles depuis Internet, mais le reste du réseau local interne reste inaccessible. Cette approche fournit une couche de sécurité supplémentaire au réseau local car elle restreint la capacité d'un pirate à accéder directement aux serveurs internes et aux données à partir d'Internet.

Les pirates et les cybercriminels peuvent atteindre les systèmes exécutant des services sur des serveurs DMZ. Ces serveurs doivent être renforcés pour résister aux attaques constantes.

Pourquoi les DMZ sont-elles importantes ?

Les DMZ offrent un niveau de segmentation du réseau qui aide à protéger les réseaux d'entreprise internes. Ces sous-réseaux restreignent l'accès à distance aux serveurs et ressources internes, ce qui rend difficile l'accès des attaquants au réseau interne. Cette stratégie est utile à la fois pour un usage individuel et pour les grandes organisations.

Les entreprises placent les applications et les serveurs exposés à Internet dans une DMZ, les séparant du réseau interne. La DMZ isole ces ressources de sorte que, si elles sont compromises, il est peu probable que l'attaque cause une exposition, des dommages ou des pertes.



Architecture et conception de réseaux DMZ

Un seul pare-feu avec au moins trois interfaces réseau peut être utilisé pour créer une architecture réseau contenant une DMZ. Le réseau externe est formé en connectant l'Internet public - via une connexion de fournisseur de services Internet - au pare-feu sur la première interface réseau. Le réseau interne est formé à partir de la deuxième interface réseau et le réseau DMZ lui-même est connecté à la troisième interface réseau.

Différents ensembles de règles de pare - feu pour surveiller le trafic entre Internet et la DMZ, le LAN et la DMZ, et le LAN et Internet contrôlent étroitement quels ports et types de trafic sont autorisés dans la DMZ à partir d'Internet, limitent la connectivité à des hôtes spécifiques dans le réseau interne et empêcher les connexions non demandées à Internet ou au réseau local interne à partir de la DMZ.

Dans notre situation

L'ajout d'une DMZ à notre SI est essentiel étant donner la présence de serveurs Web et d'autres services nécessitant d'être accessible depuis Internet. On va pouvoir en mettre une en place grâce au **pare-feu PfSense** qui permet la mise en place d'une DMZ.

Sécurisation des données circulant sur le réseau

Chiffrement des données

Pour la mise en place de la sécurisation des données circulant sur le réseau, on va d'abord s'atteler au chiffrement de ce mêmes données. Cela va permettre dans le cas d'une interception du flux, d'éviter la lecture en « toute lettre » des informations (les données étant chiffrées, elles ne sont pas lisibles sans une clé de déchiffrement). De ce fait un potentiel acteur malveillant ne pourras pas lire les données sans posséder la clé secrète. Pour cela on va pouvoir utiliser les protocole TLS (anciennement SSL), HTTPS, SFTP ainsi que des certificats et un VPN.

Certificats

Ces certificats vont certifier (comme leur nom l'indique) de la légitimité des périphériques, tel qu'un serveur. Ainsi lorsqu'un client souhaite accéder ou communiquer avec un serveur, le certificat lui permettra de vérifier qu'il parle bien au bon destinataire, mais aussi que les informations ne pourront être déchiffrées et lues seulement par le destinataire (et inversement depuis le serveur).

Pour ce faire plusieurs solutions sont possibles, nous allons dans notre cas mettre en place des paires de clés RSA (avec OpenSSL par exemple), et ainsi de créer des certificats, et chiffrer les données en fonction de ces clés.

Signatures

En plus des certificats, on va aussi pouvoir utiliser des signatures, cela est utile pour prouver l'identité de l'émetteur, mais aussi pour garantir l'intégrité des données. Ces signatures sont par exemple généralement utilisées dans les échanges via courriel.

Sécurité des échanges

La messagerie électronique ne constitue pas un moyen de communication sur pour transmettre des données personnelles, sans mesures complémentaire. Une simple erreur de manipulation peut conduire à divulguer à des destinataires non habilités des données personnelles et à porter ainsi atteinte au droit à la vie privée des personnes. En outre, toute entité ayant accès aux serveurs de messagerie concernés (notamment ceux des émetteurs et destinataires) peut avoir accès à leur contenu.

Précautions sur la sécurité des échanges

L'un des meilleur moyen (mais celui le plus extrême aussi est le chiffrement des données avant leur enregistrement sur un support physique à transmettre à un tiers (via par exemple un DVD, une clé USB, ou un disque dur portable). Il faut tout de même veiller à rester vigilant avec ce dispositif car vous branchez directement un dispositif vulnérable qui peut être infecté et infecter votre ordinateur provoquant des dommages importants.

Lors d'un envoi via un réseau :

- Chiffrer les pièces sensibles à transmettre, si cette transmission utilise la messagerie électronique.
- Utiliser un protocole garantissant la confidentialité et l'authentification du serveur destinataire pour les transferts de fichiers, par exemple SFTP ou HTTPS, en utilisant les versions les plus récentes des protocoles.
- Assurer la confidentialité des secrets (clé de chiffrement, mot de passe, etc.) en les transmettant via un canal distinct (par exemple, envoi du fichier chiffré par e-mail et communication du mot de passe par téléphone ou SMS).

Dans le cas d'un fax :

- Installer le fax dans un local physiquement contrôlé et uniquement accessible au personnel habilité.
- Faire afficher l'identité du fax destinataire lors de l'émission des messages.
- Doubler l'envoi par fax d'un envoi des documents originaux au destinataire.
- Préenregistrer dans le carnet d'adresse des fax (si la fonction existe) les destinataires potentiels.

Il ne faut absolument pas transmettre des fichiers contenant des données personnelles en clair via des messageries grand public.

CNIL Sécurisation des échanges : https://www.cnil.fr/fr/securite-securiser-les-echanges-avec-dautres-organismes

Sous-traitance

Précautions sur la sous-traitance

Concernant la sous-traitance, étant donné que les données communiquées il faut faire appel uniquement à des sous-traitants présentant des garanties suffisantes (notamment en termes de connaissances spécialisées, de fiabilité et de ressources), et exiger la communication par le prestataire de sa politique de sécurité des systèmes d'information.

Pour plus d'assurance sur les garanties, il est conseillé de prendre et documenter les moyens (audits de sécurité, visite des installations, etc.) permettant d'assurer l'effectivité des garanties offertes par le sous-traitant en matière de protection des données. Ces garanties incluent notamment :

- Le chiffrement des données selon leur sensibilité ou à défaut l'existence de procédures garantissant que la société de prestation n'a pas accès aux données qui lui sont confiées si cela n'est pas nécessaire à l'exécution de son contrat.
- Le chiffrement des transmissions de données (ex : connexion de type HTTPS, VPN, etc.).

- Des garanties en matière de protection du réseau, de traçabilité (journaux, audits), de gestion des habilitations, d'authentification, etc.

CNIL sous-traitance : https://www.cnil.fr/fr/securite-gerer-la-sous-traitance

Réseau

Précautions au niveau du réseau en général

Plusieurs précautions sont à prendre au niveau du réseau, notamment accès autour du wifi.

Il va falloir gérer les réseau Wi-Fi. Ils doivent utiliser un chiffrement à l'état de l'art (WPA2 ou WPA2-PSK avec un mot de passe complexe et non pas WEP) et les réseaux ouverts aux invités doivent être séparés du réseau interne.

Le VPN doit être imposé pour les accès à distance ainsi que, si possible, une authentification forte de l'utilisateur (carte à puce, boitier générateur de mots de passe à usage unique (OTP), etc.). Pour la connexion aux équipements du réseau (pare-feu, routeurs, passerelles...) il faudra privilégier le protocole SSH ou un accès physique direct à l'équipement plutôt qu'au protocole telnet.

Et bien évidemment il va falloir limiter les flux réseau au strict nécessaire en filtrant les flux entrants/sortants sur les équipements (pare-feu, proxy, serveurs, etc.). Voir par exemple les précautions pour l'accès à un site web.

Précautions sur l'accès à un site web (peut s'appliquer à d'autres serveurs)

Le mieux est de rendre l'utilisation de TLS (en remplacement de SSL) obligatoire pour toutes les pages d'authentification, de formulaire ou sur lesquelles sont affichées ou transmises des données à caractère personnel non publiques. Il ne faut pas non plus faire transiter des données à caractère personnel dans une URL telles que identifiants ou mots de passe.

Comme cela on va mettre en œuvre le protocole TLS sur tous les sites web, en utilisant uniquement les versions les plus récentes et en vérifiant sa bonne mise en œuvre. On va aussi limiter les ports de communication strictement nécessaires au bon fonctionnement des applications installées. Si l'accès à un serveur web passe uniquement par HTTPS, il faut autoriser uniquement les flux réseau IP entrants sur cette machine sur le port 443 et bloquer tous les autres ports.

*Certaines des informations présentent dans le rapport sur la sécurisation des données sont tirées du guide de la sécurité des données personnelle de la CNIL : https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles

Gestion rigoureuse des certificats

Plusieurs bonnes pratiques pour la gestion des certificats peuvent êtres énoncés :

Bonne pratique n°1 : Utilisez une plateforme de gestion MPKI

Les solutions Managed PKI (MPKI) permettent aux entreprises de gérer et commander leurs certificats, sans les coûts associés à la gestion d'une Autorité de Certification en interne.

Nombreuses sont les entreprises qui optent pour cette solution, notamment en raison des avantages financiers. Certaines Autorités de Certification réputées offrent même des solution MPKI.

Grâce à une solution MPKI, une grande partie des efforts liés au maintien d'une infrastructure PKI interne sont délégués à une Autorité de Certification externe, sans aucune concession sur votre sécurité.

Cela permet de simplifier tous les aspects de la gestion du cycle de vie des certificats (allant de l'émission, l'inspection à la résolution de problèmes et le renouvellement), en gagnant du temps pour se concentrer sur le suivi des détails importants des certificats, tels que :

- Dates d'expiration
- Erreurs sur les terminaux SSL/TLS
- Demandes de certificats émises par vos collègues
- Révocations éventuelles
- Autorités de Certification émettrices

La solution MPKI permet l'automatisation du suivi des détails et de la gestion des demandes de certificats, réduisant du même coup le risque d'erreur humaine.

Bonne pratique n°2 : misez sur les API pour automatiser

Les API facilitent l'automatisation et la personnalisation des opérations pour les équipes IT pour la gestion des certificats. Elles donnent accès à une multitude de technologies pour les développeurs.

Si l'interface utilisateur d'un outil de gestion SSL/TLS peut convenir aux petites entreprises, les grandes structures ont pour leur part besoin d'une solution plus personnalisée. En ce sens, certains outils de gestion PKI donnent accès à une API permettant de personnaliser les workflows et fonctionnalités, mais aussi d'automatiser les processus pour réduire le nombre d'interventions manuelles. Une API peut donc se révéler extrêmement utile pour adapter l'administration SSL/TLS en fonction des besoins.

Cette automatisation permet de réduire le risque d'erreur humaine et de pannes liées à des problèmes de certificats, avec à la clé un niveau de sécurité renforcé. Elle fait aussi économiser du temps sous bien des aspects du cycle de vie des certificats SSL/TLS. Par exemple :

- Demandes de certificats
- Approbation de demandes de certificats
- Refus de demandes de certificats

- Téléchargement de certificats
- Renouvellement de certificats
- Révocation de certificats
- Réémission de certificats

Enfin, le recours à une API réduit la complexité de la gestion de certificats émis par diverses Autorités de Certification, et permet l'amélioration de la maîtrise du processus de renouvellement. Une API est donc le meilleur moyen d'économiser du temps en automatisant et en personnalisant la gestion des certificats.

Bonne pratique n°3 : décelez les certificats oubliés

La présence des certificats oubliés s'explique par un triple phénomène : l'augmentation générale du nombre de certificats en circulation, la multiplication des personnes habilitées à commander et installer des certificats, et la rotation des effectifs au sein des entreprises. Ces certificats « sauvages » posent problème dans la mesure où ils passent inaperçus.

L'outil d'inspection, permet de faire bénéficier à la fois d'une visibilité générale et d'une analyse granulaire du portfolio de certificats. Cet outil recense tous les certificats déployés sur votre réseau, quelle que soit l'Autorité de Certification émettrice, permettant d'éviter toute erreur due à un suivi manuel, sans compter qu'il accélère aussi considérablement la tenue des inventaires.

Il est recommandé d'effectuer au moins une fois par semaine ces analyses offrant une visibilité complète sur les certificats actifs et facilitant la détection précoce d'éventuels problèmes, y compris des certificats oubliés menaçants.

Bonne pratique n°4 : organisez votre équipe

Pour parfaire à la bonne gestion des certificats, il faut passer par une bonne gestion des collaborateurs en charge de l'infrastructure PKI.

Il est ici recommandé de répartir en équipes (ou départements) les employés, avec des droits adaptés pour chaque.

On appelle ça la segmentation de l'entreprise. Les demandes seront ainsi réparties en fonction de leur provenance, leur adresse IP ou tout autre critère de classement.

Bonne pratique n°5 : accélérez votre processus d'approbation

L'émission d'un large volume de certificats impose une parfaite maîtrise de l'infrastructure PKI pour permettre l'accélération et la simplification du processus d'approbation. Dès lors qu'il y a collaboration avec une Autorité de Certification très prompte à valider les demandes, le seul point de blocage se situe généralement au niveau de l'administrateur chargé de l'approbation en interne.

Pour cela il suffit de la contacter directement en lui envoyant les e-mails de vérifications. Les certificats seront donc déployés dans la foulée de leur validation.

Bonne pratique n°6 : soyez attentifs aux notifications

Les notifications sont importantes pour les administrateurs SSL/TLS. Sans elles, certains certificats risquent de ne pas être renouvelés, avec les problèmes de sécurité que cela entraîne. Les notifications les plus importantes sont celles signalant les certificats sur le point d'expirer. Mais attention à ne pas négliger le reste du cycle de vie des certificats. D'autres notifications pourront notamment être très utiles pour les demandes de certificats en attentes, les révocations récentes ou encore les certificats à réémettre.

Il est également important d'établir des procédures en cas de problèmes spécifiques. Si la notification arrive à temps, il sera possible d'agir avant qu'il ne soit trop tard. Grâce à ce genre de précautions, il est possible d'éviter les expirations de certificats inopinées pouvant entraîner la paralysie d'un serveur.

Bonne pratique n°7 : surveillez votre réseau et générez des rapports

Les analyses réseau sont importantes et permettent de dresser un tableau de bords des détails de tous les certificats, voir même de pousser plus loin les inspections tout en permettant l'évaluation de l'état du réseau.

Cette surveillance de tous les instants est sans doute la meilleure garante d'une visibilité totale sur l'environnement. En effet, la combinaison des fonctions de recherche et de reporting peut considérablement améliorer la compréhension et la maîtrise du portfolio de certificats.

Pour en exploiter le plein potentiel plusieurs conseils sont donnés :

- Déployez un agent pour l'analyse de votre réseau et la création d'un rapport au moins une fois par mois
- Si possible, automatisez vos analyses à l'aide d'un script
- Intervenez sur les terminaux vulnérables après chaque analyse
- Approuvez les demandes de certificats aussi vite que possible
- Optez pour des renouvellements automatiques pour éviter les pannes

En surveillant ainsi le réseau cela permet une inspection continue, indispensable à la gestion du cycle de vie des certificats.

Bonne pratique n°8 : utilisez un outil de détection des vulnérabilités

Un certificat ne vous protégera que partiellement si vous utilisez un chiffrement obsolète ou des versions SSL/ TLS vulnérables. Et même si tout est à jour, une nouvelle vulnérabilité peut se déclarer à tout moment. D'où l'importance de pouvoir résoudre les problèmes rapidement.

Un outil permettant d'analyser le réseau, rechercher des vulnérabilités et fournir des informations sur les points faibles du réseau/infrastructure va permettre de gérer ces vulnérabilités plus sereinement.

Lorsqu'il repère une vulnérabilité, on peut donc intervenir sûrement et rapidement.

Bonne pratique n°9 : choisissez une plateforme tout-en-un

Le plus simple est d'opter pour une plateforme de gestion des certificats qui réponde à tous les besoins :

- Solution MPKI
- Tableau de bord complet
- Automatisation à l'aide d'API
- Recherche de certificats
- Segmentation et attribution de rôles utilisateur
- Configuration de notifications et procédures d'escalade en cas de problèmes
- Détection des vulnérabilités

La plateforme est l'instrument qui vous permet de garder le contrôle sur votre infrastructure PKI et de gérer le cycle de vie des certificats.

DIGICERT Gestion des certificats : https://www.digicert.com/resources/certificate-management-ultimate-guide-datasheet-fr-2019.pdf

Authentification via l'Active Directory

Afin de permettre aux utilisateurs de se connecter à différents services, nous allons recourir à une solution d'authentification unique : Kerberos

Ce protocole permet de s'authentifier une seule fois grâce à des liens de confiance et est donc une bonne solution pour s'authentifier. Il nous faudra simplement un mot de passe maître. Ce mot de passe maître devra répondre à un certain nombre de critères (longueur minimum, utilisation de caractères spéciaux, chiffre) afin d'obtenir une bonne entropie. Quant à leur renouvellement de récente recommandation de l'ANSII, le tende à dire que nous devrions limiter le renouvellement de mot passe utilisateur.
https://www.ssi.gouv.fr/guide/recommandations-relatives-a-lauthentification-multifacteur-et-aux-mots-de-passe/

Pour continuer avec Active directory, nous allons devoir le modifier celui actuelle afin de créer des groupes d'utilisateur et des unités d'organisation qui vont permettre de mieux organiser les utilisateurs. Cela va également nous permettre de limiter leur droit. Exemple, ils ne pourront pas installer n'importe quelle logicielle, il faudra impérativement le compte administrateur pour l'installer et passerons donc systématiquement par nous a chaque installation ce qui nous permettra de vérifier la source.

Politique de sauvegarde

De nombreuses menaces, existent sur nos données et il est de notre devoir que de prévoir un plan en cas d'incident sur celle-ci. Pour cela, je vais me baser sur 10 conseille proposée par le gouvernement français. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/sauvegardes

1. Effectuez des sauvegardes régulières de vos données.

La première recommandation est sur le fait de réaliser des sauvegardes régulières de nos données. Dans notre cas, les sauvegardes devront s'effectuer automatiquement quand un utilisateur ajoute des données à notre SI.

2. Identifiez les appareils et supports qui contiennent des données.

Dans notre cas, nous disposons de :
- 3 Serveurs qui contiennent tous des espaces de stockage.
- Des postes utilisateur sur lequel nous ne savons pas pour le moment ce qu'il y a.
- Potentiellement, des disques durs externes afin de disposer de backup.

3. Déterminez quelles données doivent être sauvegardées.

Nous allons avoir plusieurs types de sauvegarde à gérer.

Dans un premier temps, nous allons avoir le travail des collaborateurs a enregistré sur notre serveur de fichier, et ce, dès qu'un utilisateur effectue une sauvegardée.
Et dans un second temps les données qui concernent les utilisateurs, c'est-à-dire les données de notre Active directory, les mails ect…

4. Choisissez une solution de sauvegarde adaptée à vos besoins.

Dans notre cas, la sauvegarde va s'effectuer dans un premier temps sur les disques durs de nos serveurs qui seront configurés en RAID. (Le RAID est un ensemble de techniques de virtualisation du stockage permettant de répartir des données sur plusieurs disques durs afin d'améliorer soit les performances, soit la sécurité ou la tolérance aux pannes de l'ensemble du ou des systèmes.)
Mais il faudra également prévoir un plan de sauvegarde autre que nos disques durs dans notre cas nous préconisons des disques durs externe de type HDD.

5. Planifiez vos sauvegardes.

Afin d'assurer ces sauvegardes, il va falloir établir un planning de sauvegarde et du type de

sauvegarde à effectuer.
Différents types de sauvegardes
• La sauvegarde complète est une copie de la totalité de vos données.
• La sauvegarde incrémentale ou incrémentielle ne copie que les fichiers qui ont été créés. ou modifiés depuis la dernière sauvegarde.
• La sauvegarde différentielle est une copie complète des fichiers qui ont été créés ou modifiés depuis la dernière sauvegarde complète.
Dans notre cas, la sauvegarde différentielle semble la plus adaptée.
En ce qui concerne le planning de sauvegarde, il faudra effectuer une sauvegarde différentielle sur deux disques (ou plus, mais reparti sur deux personnes) qui tourne jour après jour.

Exemple

	Lundi	Mardi	Mercredi	Jeudi	Vendredi	Samedi
Semaine	Personne A	Personne B	Personne A	Personne B	Personne A	Personne B

En parallèle de cela, le patron disposera également de disque qui devra ramener tous les 3 mois afin d'être actualisé avec les dernières données essentielles. Ce qui permet également en cas de problème (Physique type disque corrompu.) de posséder des disques sans délai d'attente pour les personnes qui effectuent les sauvegardes quotidiennes.

6. Déconnectez votre support de sauvegarde après utilisation.

Il est difficilement envisageable de déconnecter les disque no serveur après utilisation. Cependant les Disque dur externe eu seront déconnecter systématiquement après utilisation.

7. Protégez vos sauvegardes.

Au même titre que nos données, nous chiffrerons les données les plus sensibles sur nos sauvegardes.

8. Testez vos sauvegardes.

Afin de vérifier le bon déroulement de notre script de sauvegarde, il faudra régulièrement vérifier qu'il fonctionne correctement à raison de 2 fois par an et plus si nous nous apercevons que des incidents surviennent régulièrement.

9. Vérifiez le support de sauvegarde.

Les HDD ont une durée de vie de 5 à 10 ans. Comme ces disques seront souvent manipulée

et transportée, il faudra à l'occasion du point numéro 8 effectuer une analyse de la qualité de nos disques et prévoir de les renouveler tous les 5 ans Il est à noter qu'au moment de l'achat de ces disques il faudra varier les constructeurs en effet il est possible que certaines séries soient victime de souci physique le fait de posséder plusieurs constructeurs nous permet de minimiser les problèmes du a une mauvaise série.

10. Sauvegardez les logiciels indispensables à l'exploitation de vos données.

Dans notre cas, il faudra par la suite déterminer une liste avec les utilisateurs de logicielle indispensable au fonctionnement de nos données.

Conclusion

Pour conclure sur notre politique de sauvegarde, nous allons devoir mettre en place un système de backup (PCA/PRA). Ce système sera la plupart du temps déconnecté, mais en cas d'incident il nous permettra de restaurer nos données.

Préconisations supplémentaires

Sensibilisation

Malgré toutes les mesures mise en place une faille reste toujours ouverte. Cette faille, c'est l'humain en effet une employée pourrais très facilement ouvrir une faille dans notre SI, et ce, involontairement. Du a une non-connaissance des risques de piratage. Pour remédier à cela, il faudrait prévoir une « Journée de sensibilisation » afin de les avertir des différents risques qui peuvent exister et dont ils devraient se méfier. Dans cette journée, nous évoquerons différent vecteur d'attaque auquel les employer peuvent être confrontée, telle que le phishing, les clefs USB mal veillant ect … Nous profiterons également de ce moment pour répondre aux questions.

Contrôle d'accès

Le contrôle d'accès à un réseau (et à internet) va permettre de le sécuriser, en évitant des intrusions, et en limitant les accès à que ce qui est essentiel. Cette limitation va laisser lieu à une centralisation de la surveillance des différents échanges et des points d'accès. La sécurisation du wifi est un point important dans le contrôle d'accès au réseau car il est facilement accessible, devenant un point sensible du réseau.

Cela peut se faire via un pare-feu filtrant les données transitant entre le réseau et internet, mais aussi en limitant le nombre de points d'accès à surveiller et en restreignant l'accès au réseau aux appareils internes à l'entreprise car des appareils personnels (si présent sur le réseau) peuvent engager des failles de sécurité (virus, vers, …).

Sécurisation des ports

Pour éviter tout risque d'intrusion sur le réseau depuis l'intérieur du site, il serait plus sûr de verrouiller tous les ports non utilisés des différents périphériques. De cette maniérer, l'accès non autorisé ou non voulu sera évité.

Mise à jour

Il est important de respecter la mise à jour des services, des systèmes d'exploitation et des applications pour sécuriser l'infrastructure et ajouter des nouvelles fonctionnalités.

Conclusion

La sécurité du système d'information est un point à ne pas négliger dans une entreprise. En effet cela pourrait amener à compromettre l'entreprise et ses employés.

Cela passe par plusieurs points clés :

- Installation d'un pare-feu au sein du S.I
- Mise en place d'une DMZ
- Configuration d'un VPN
- Chiffrement des données sensibles
- Gestion des sauvegardes
- Gestion des utilisateurs
- Gestion des périphériques
- Maintient d'une infrastructure à jour
- Bonnes pratiques élémentaires

Ce livrable nous a permis de prendre conscience de l'ensemble des points critiques de sécurité au sein d'une entreprise auxquels nous nous devons de porter une attention particulière.