Cahier des charges détaillé de l'évolution de l'infrastructure

Aperture COntr Ol Management Engineering

Fournisseur de solutions innovantes & inattendues

PORCHER Samuel, BELLANGER Quentin, BATARD Clément – 19/03/2024 – POEC Développeur Cybersécurité

EPSI l'École d'ingénierie informatique

SOMMAIRE

I. Mise en contexte

A. Introduction

Ce cahier des charges a pour objectif de répondre au besoin exprimé par l'entreprise ACME de faire évoluer son système d'information.

Après avoir été la victime de plusieurs accès non autorisés à son réseau informatique ainsi qu'à ses applications, la direction de l'entreprise envisage l'évolution de son Système d'Information (SI) et demande donc au service support informatique de faire une proposition afin de renforcer la sécurité informatique du réseau et de leurs outils de travail. Cette demande s'inscrit également dans l'évolution des pratiques de l'entreprise avec la création d'un CRM (Customer Relationship Management) afin de gérer les interactions et les relations avec les clients.

Ce cahier des charges va détailler les enjeux de cette évolution ainsi qu'une présentation de l'infrastructure actuelle et les évolutions à apporter pour répondre à ces enjeux.

B. Description de l'entreprise

Aperture Science est une entreprise innovante et leader dans le domaine de la technologie des portails, connue pour avoir développé le célèbre Aperture Science Handheld Portal Device, communément appelé "Portal Gun". Fondée par le visionnaire Cave Johnson, l'entreprise a connu une croissance rapide et emploie aujourd'hui 250 salariés, répartis dans divers départements et pôles d'expertise et situés dans des installations souterraines massives et ultra-modernes s'étendant sur plusieurs kilomètres carrés.

Aperture Science est organisée en plusieurs pôles d'expertise, chacun dédié à un aspect spécifique de la technologie des portails et de ses applications. Parmi ces pôles, on retrouve la recherche et développement, l'ingénierie, la production et une équipe commerciale. Les commerciaux d'Aperture Science jouent un rôle essentiel dans la promotion et la vente des produits et services de l'entreprise, en veillant à ce que les solutions de portail révolutionnaires d'Aperture Science soient accessibles aux clients du monde entier.

L'obsession pour l'innovation, le manque de supervision, la dépendance à l'IA, la détérioration des infrastructures et le manque de transparence contribuent aujourd'hui à la vulnérabilité de l'entreprise.

II. Analyse de l'infrastructure actuelle[1]

A. Présentation

Le SI actuel de l'entreprise ACME est disposé au sein d'un seul et même réseau local.

Les postes de travail fonctionnent sous Windows 10 professionnel[2] sans configuration spécifique avec une absence de gestion de parc. En ce qui concerne les serveurs, l'entreprise dispose d'un serveur abritant la base de données sous Ubuntu 12.04 et de serveurs complémentaires sous Windows pour la gestion des courriels, des fichiers et des applications Web.

La base de données sur laquelle va venir s'appuyer le CRM a été réalisé avec une technologie MySQL en version 5.1 qui n'est aujourd'hui plus maintenue. Les employés disposent de licences logicielles correspondant à leur besoin métier. Pour le développement du Customer Relationship Management. La version de Java utilisée est la 21.

B. Etat actuel des équipements d'ACME

- Ordinateurs de bureau : 150
- Ordinateurs portables : 50
- Serveurs : 4
- Imprimantes réseau multifonctions : 5
- Commutateurs (switches) : 10
- Routeurs : 1
- Points d'accès Wi-Fi : 5
- Câblage réseau (câbles Ethernet, prises murales)
- Support de stockage externe (Disque dur et clé USB)
- Téléphones IP : 150

C. Analyse des points faibles et des besoins de sécurité

C1. Réseau local de l'entreprise non sécurisé

Manque d'éléments de sécurité du réseau

A ce jour, le réseau de l'entreprise ACME ne dispose pas d'éléments de sécurité du réseau et est donc vulnérable à de nombreuses problématiques.

Tout d'abord, cela rend le SI plus vulnérable aux menaces externes, car aucun filtrage du trafic entrant et sortant n'est effectué. Ensuite, sans certains éléments de sécurité, il est

1 Nous partons du principe que tout ajout dans le SI de l'entreprise passe obligatoirement par le service informatique pour la configuration.

2 Il n'est pas fait mention du type de licence dans la consigne. Nous nous permettons ici d'imaginer.

difficile de contrôler et de gérer l'accès aux ressources du réseau, ce qui peut entraîner des accès non autorisés et des fuites de données.

Sans éléments de sécurité du réseau, le SI a beaucoup plus de mal à détecter des activités suspectes ou malveillantes au sein du réseau, ce qui rend la réponse aux incidents plus lente et moins efficace. Il n'y a également pas de prévention des intrusions, car aucune mesure n'est prise pour bloquer ou empêcher les activités malveillantes en temps réel.

Enfin, en l'absence de ces dispositifs de sécurité, les logiciels malveillants et les attaques peuvent se propager plus facilement au sein du réseau, mettant en péril l'intégrité et la confidentialité des données.

Architecture monolithique du réseau

L'architecture réseau de l'entreprise ACME est actuellement monolithique, c'est-à-dire que l'ensemble du parc se trouve dans le même réseau.

Cela comporte plusieurs inconvénients. Sur le plan sécuritaire, tout d'abord, l'absence de segmentation du réseau facilite la propagation des menaces et des attaques, car un intrus peut accéder à l'ensemble du réseau une fois qu'il y a pénétré. En l'absence de VLAN, la gestion du trafic est moins efficace puisque le réseau peut être surchargé et mal réparti entrainant des problèmes de performances. Enfin, sur le plan de la gestion, un réseau unique et non segmenté est plus complexe à gérer et à maintenir, car les modifications apportées à une partie du réseau peuvent entraîner des répercussions sur l'ensemble du réseau.

C2. Manque de sécurité de la base de données et du serveur

Les informations contenues dans le serveur de base de données d'ACME sont aujourd'hui vulnérables à de potentielles actions malveillantes.

En ce qui concerne la base de données, l'utilisation de la version MySQL 5.1 présente plusieurs risques. Tout d'abord, étant une version ancienne, elle est officiellement non prise en charge depuis 2013 et ne reçoit plus de mises à jour de sécurité. Ensuite, plusieurs vulnérabilités semblent connues sur cette version de MySQL et sans mises à jour, ces vulnérabilités restent non corrigées, exposant les données à des risques de compromission. Enfin, nous retrouvons des problématiques de supports qui n'est plus assuré sur cette version ainsi que des soucis de performance en raison de l'absence d'optimisations et d'améliorations apportées aux versions ultérieures.

Cette base de données est actuellement contenue sur un serveur qui évolue sous une version d'Ubuntu qui ne dispose plus de support de sécurité créant ainsi plusieurs failles. Le matériel serveur ne pourra peut-être pas supporter les évolutions proposées et nous devrons donc proposer également une évolution sur ce plan.

C3. Absence de sauvegardes automatique des données

Les informations contenues dans les serveurs d'ACME et notamment, celui de la base de données, sont uniquement contenues en local. Cette méthode provoque une absence totale de résilience en cas d'intrusion au sein du réseau local et de compromission des données.

C4. Mauvaise gestion du parc de machines

Plusieurs problèmes se posent vis-à-vis du SI d'ACME quant à la gestion, actuellement inexistante du parc.

En effet, ACME ne dispose pas d'outils permettant d'automatiser les mises à jour de sécurité obligeant les administrateurs à les effectuer sur chaque machine augmentant ainsi les possibles erreurs de manipulation et les oublis. Cette automatisation sera par la suite essentielle puisque à court terme, le système d'exploitation devra évoluer vers Windows 11 pour obtenir l'ensemble des mises à jour mises à disposition de Microsoft. Ces mises à jour sont d'autant plus cruciales qu'elles apportent au fur et à mesure des corrections de failles de sécurité connues notamment des pirates informatiques.

Ce manquement de mises à jour est visible particulièrement sur les serveurs. Certains tournant comme mentionné précédemment sous des versions très anciennes d'Ubuntu ne disposant plus de support de sécurité.

L'absence d'une gestion centralisée du parc informatique de l'entreprise ACME empêche l'encadrement des pratiques des utilisateurs en matière de sécurité. Ces pratiques impactent des éléments très sensibles comme la gestion des mots de passe, les restrictions de connexions ou la configuration des navigateurs web, ouvrant la porte à de nombreuses pratiques risquées.

C5. Questionnements sur l'accès à l'application

L'accès au réseau d'ACME n'est aujourd'hui pas centralisée permettant ainsi plusieurs failles de sécurité et empêchant une bonne gestion des identités au sein du réseau.

La volonté de l'entreprise de créer un CRM doit être intégrée à cette réflexion afin de filtrer les différentes connexions et d'avoir un niveau de sécurité suffisant, mais ne limitant pas les logiques métiers des utilisateurs.

A cela, vient s'ajouter le besoin d'une connexion à distance notamment pour être utilisé par les commerciaux en déplacement. Afin de leur permettre d'accéder aux différentes ressources du réseau local et d'internet de manière sécurisé, il sera nécessaire d'envisager des outils permettant de sécuriser la connexion en dehors du réseau local.

III. Propositions de solutions

A. Propositions principales

A1. Sécurisation du réseau local de l'entreprise

Restructuration de l'architecture réseau

L'infrastructure réseau en bloc tel qu'elle est proposée aujourd'hui dans l'entreprise ACME est amenée à évoluer pour des raisons de sécurité. La création de sous-groupes réseaux logiques (et non physiques) passera par une analyse des systèmes ayant des besoins de sécurité homogènes (regroupement des serveurs infrastructures ente eux, les postes de travail administrateur, ...).

Chacune de ces zones se caractérisera par des VLAN et des sous-réseaux IP dédiés. Après la division en zone, des mesures de cloisonnements seront à prendre telles qu'un filtrage IP à l'aide d'un pare-feu peuvent être mises en place entre les différentes zones.

Segmenter le réseau en plusieurs VLAN pourra également permettre d'isoler certaines parties sensibles de ce même réseau comme les serveurs ou encore les ordinateurs se connectant en tant qu'administrateur, tout en renforçant particulièrement la sécurité sur ces points sensibles du réseau.

Un routage inter VLAN sera à mettre en place afin de permettre la communication entre les différents sous-réseaux avec des règles de sécurité limitant les interconnexions au strict nécessaire.

Eléments de sécurité du réseau

L'utilisation d'Internet, devenue essentielle, exposent les utilisateurs à des risques considérables tels que les sites Web hébergeant du code malveillant, les téléchargements de fichiers néfastes, la prise de contrôle des terminaux et la fuite de données sensibles. Afin de sécuriser le réseau local de l'entreprise, il est crucial d'empêcher les ordinateurs des utilisateurs d'avoir un accès au réseau direct à Internet.

Pour ce faire, il est recommandé de déployer une passerelle sécurisée d'accès à Internet, comprenant au minimum certains éléments de sécurité :

Un pare-feu tout d'abord, positionné au plus près de la connexion Internet est indispensable pour une bonne défense périmétrique. Ce pare-feu aura pour fonction de sécuriser le réseau en définissant les connexions autorisées ou interdites. Il viendra donc interconnecter des réseaux de niveaux de sécurité différents. Il permettra de filtrer les communications entre les zones que ce soit en entrée ou en sortie pour les analyser puis les autoriser ou les rejeter en fonction des règles de sécurité en vigueur (origine destination du paquet, la fragmentation des données, les données, ...). Cet élément de sécurité aura également pour but de créer une DMZ (zone démilitarisée) afin d'isoler le réseau local d'une zone qui serait en lien direct avec Internet.

Le réseau local ne sera jamais exposé directement sur internet et inversement, les utilisateurs n'auront pas accès directement à internet depuis le réseau local de l'entreprise, tout transitera soit par la DMZ soit par une connexion VPN (Virtual Private Network) qui sera détaillée plus loin dans ce cahier des charges.

Cela veut aussi dire qu'en cas d'intrusion le pirate n'aura accès qu'aux machines dans la DMZ mais en aucun cas au réseau local. Cette DMZ hébergera des machines du réseau interne ayant besoin d'être accessibles depuis l'extérieur comme notre relais de mail, notre concentrateur VPN ou encore notre « Forward proxy ».

Ce « Forward proxy », aura pour objectif de jouer le rôle d'intermédiaire entre l'utilisateur, le réseau local et internet en filtrant tout flux sortant et en anonymisant le réseau local. L'utilisateur devra d'abord se connecter au serveur proxy et lui envoyer sa requête qui à son tour transmettra le message au serveur distant. Ce faisant le serveur proxy viendra masquer le réseau interne sur internet.

Nous proposons de compléter ces éléments par la mise en place d'une capacité de supervision de la sécurité via un Security Operation Center (SOC). Combiner ce SOC à des outils tels qu'IPS/IDS mais encore des XDR (Extended Detection and Response) permettant de collecter et analyser les données de sécurité provenant de différentes sources (réseau, équipements finaux, courriels, etc.) permettront d'anticiper et de réagir aux menaces.

L'utilisation d'un IDS aura pour objectif de repérer les le trafic malveillant comme les tentatives d'intrusion, les attaques virales, les débits importants, ...Il sera en mesure de lancer des alertes selon les informations qu'il recevra en temps réel. Il sera complété par un IPS qui pourra stopper directement les activités suspectes (par exemple en bloquant les ports). Le rôle de cet IPS sera aussi de détecter les attaques sur le réseau d'ACME à partir d'une base de données de signature d'attaque.

Afin de mettre en place ces outils nous proposons de passer par une entreprise externe disposant des compétences et des outils pour réaliser ce type de prestation. De nombreuses entreprises proposent ces services comme ITrust ou SYD Apps.

Protocoles de sécurité

Un travail sur l'utilisation de protocoles de sécurité est obligatoire. Sur le volet internet, l'utilisation du protocole HTTPS (HyperText Transfer Protocol Secure) est obligatoire. Sachant que nous privilégions ici un hébergement en local de notre CRM[3], il est nécessaire de configurer le service SSL (Secure Sockets Layer) sur notre serveur :

En effet, lorsqu'on met en place un serveur web, le site par défaut qui est actif utilise le protocole non-sécurisé HTTP et écoute sur le port 80. Pour des soucis de sécurité et de

[3] *Pour des raisons pratiques la mise en place d'un protocole HTTPS n'a pas pu être fait, cela reste une amélioration possible à notre projet.*

confidentialité de l'information, il peut être intéressant de passer ce site en HTTPS qui écoute quant à lui sur le port 443 via l'activation du module SSL.

L'activation de ce certificat SSL également sur le serveur mail permettra l'utilisation du protocole SMTPs (Simple Mail Transfer Protocol Secure) et IMAPs (Internet Message Access Protocol) pour sécuriser les échanges entre tous nos collaborateurs.

Nous préconisons également l'utilisation de clés SSH (Secure Shell) pour renforcer la sécurité en ce qui concerne les échanges d'informations entre machines et notamment celles jugées comme critiques pour la sécurité du SI. Pour ce faire il sera nécessaire de les générer via l'outil OpenSSH disponible sur l'ensemble des OS (Systèmes d'exploitations) qui composent notre parc informatique. Nous préconisons l'utilisation de clés SSH réalisées avec l'algorithme ED-25519 pour plus de sécurité. Seront concernés par cette mesure les serveurs ainsi que les ordinateurs ayant une autorité plus importante comme le poste de l'administrateur, mais également ceux pouvant se connecter à la base de données d'ACME.

A2. Sécurisation de la base de données et de son serveur hébergeant les données de l'application

Nous avons mentionné précédemment que des vulnérabilités de notre base de données étaient en grande partie dues au manque de mise à jour logicielle mais également matérielle. C'est donc une évolution de cette base de données via des mises à jour ainsi qu'une sécurisation physique de celle-ci que nous proposons.

Pour faire évoluer la base de données, il sera nécessaire d'effectuer une exportation de celle-ci pour la faire passer sur la dernière version MySQL (8.0.36). Une autre possibilité serait d'utiliser MariaDB en version LTS 10.11.

Une telle évolution de la base de données devra être accompagnée d'une évolution du serveur l'abritant, actuellement sous Ubuntu 12.04. Il s'agira donc non seulement de mettre à jour cette version pour passer à la version 22.04.4, mais également d'investir dans un nouveau serveur pouvant s'adapter à cet écart d'OS.

Les échanges de données entre le serveur Web et le serveur contenant la base de données s'effectueront via le protocole SSH (voir « protocoles de sécurité » mentionnés plus haut).

L'utilisation d'un pare-feu d'application Web (WAF) aura également pour conséquences de réduire le risque d'injections SQL, de détournements de session, ...

Enfin, contrôler l'accès aux salles serveurs et aux locaux techniques est indispensable pour empêcher les intrusions physiques et garantir l'intégrité des infrastructures critiques de l'entreprise et notamment de la salle contenant le serveur de base de données. L'accès à la base de données via MySQL s'effectuera via un compte User qui devra obtenir une élévation de privilèges en tant que root pour effectuer toutes les modifications.

A3. Mise en place d'une sauvegarde automatique des données sur un site tiers

Nous prévoyons la mise en place d'un serveur de sauvegarde hébergé par une entreprise tierce (ScaleWay, OVH, ...) pour les bases de données de l'entreprise. Pour s'y connecter en cas de pannes une connexion type VPN IPsec sera faite entre notre réseau et notre hébergeur de confiance. Cette solution aura également pour but d'héberger les sauvegardes des données vitales au bon fonctionnement de l'entité que détiennent les postes utilisateurs.

Les sauvegardes devront être vérifiées de manière périodique pour empêcher une compromission de ces éléments qui s'avérerait fatale en cas d'attaque informatique. Un plan de continuité d'activité (PCA) et de reprise d'activité (PRA) devront également être rédigés pour permettre à ACME d'être résiliente en cas de cyberattaque.

A4. Amélioration de la gestion du parc de machines de la société en automatisant la configuration des machines

En soulignant les problèmes posés quant à la gestion actuellement inexistante du parc, nous souhaitons proposer non seulement une solution pour automatiser les configurations, mais également une protection homogène des postes de travails des collaborateurs.

WSUS (Windows Server Update Services)

Tout d'abord, afin de maintenir à jour le parc des composants terminaux du SI, nous proposons d'utiliser la solution de Windows WSUS. Cette solution permettra en effet de maintenir à jour les composants du parc via un service installé sur un Windows serveur 2022 qu'il conviendra d'acquérir pour rendre l'entreprise plus efficiente dans son fonctionnement.

Serveur Ubuntu

En ce qui concerne le serveur sous Ubuntu, une mise à jour automatique sera envisagée via l'outil "unattended-upgrades" qui installera automatiquement les mises à jour de sécurité et les correctifs importants.

Active Directory

Nous souhaitons proposer également l'utilisation d'un Active Directory, auquel il s'agira d'inclure le plus grand nombre d'équipements informatiques possible. Ce service de gestion des identités et des ressources informatiques centralisé permettra d'organiser, d'authentifier et de contrôler l'accès des utilisateurs au sein du réseau informatique. Les postes de travail et les serveurs sont concernés par cette mesurer. Ainsi, des politiques de durcissement du système d'exploitation ou d'applications pourront facilement s'appliquer depuis un point central tout en favorisant la réactivité attendue en cas de besoin de reconfiguration.

Protection des postes utilisateurs

De manière à sécuriser le réseau, la sécurisation des postes utilisateurs ne doit pas être négligée. Quelques bonnes pratiques sont donc à mettre en œuvre au sein d'ACME via une gestion du parc informatique.

- limiter les applications installées et modules optionnels des navigateurs web aux seuls nécessaires ;

- doter les postes utilisateurs d'un pare-feu local et d'un anti-virus (ceux-ci sont parfois inclus dans le système d'exploitation) ;

- chiffrer les partitions où sont stockées les données des utilisateurs.

- désactiver les exécutions automatiques.

- protéger contre les supports amovibles (Applocker sous Windows).

A5. Simplification de l'accès à l'application en relation avec la gestion du parc

Avec le travail de centralisation mentionné plus haut, l'Active Directory permettra aux utilisateurs déjà connectés depuis peu à leur ordinateur de se connecter à l'application sans remettre les identifiants mots de passes propre à l'application.

A6. Accès distant sécurisé à l'application

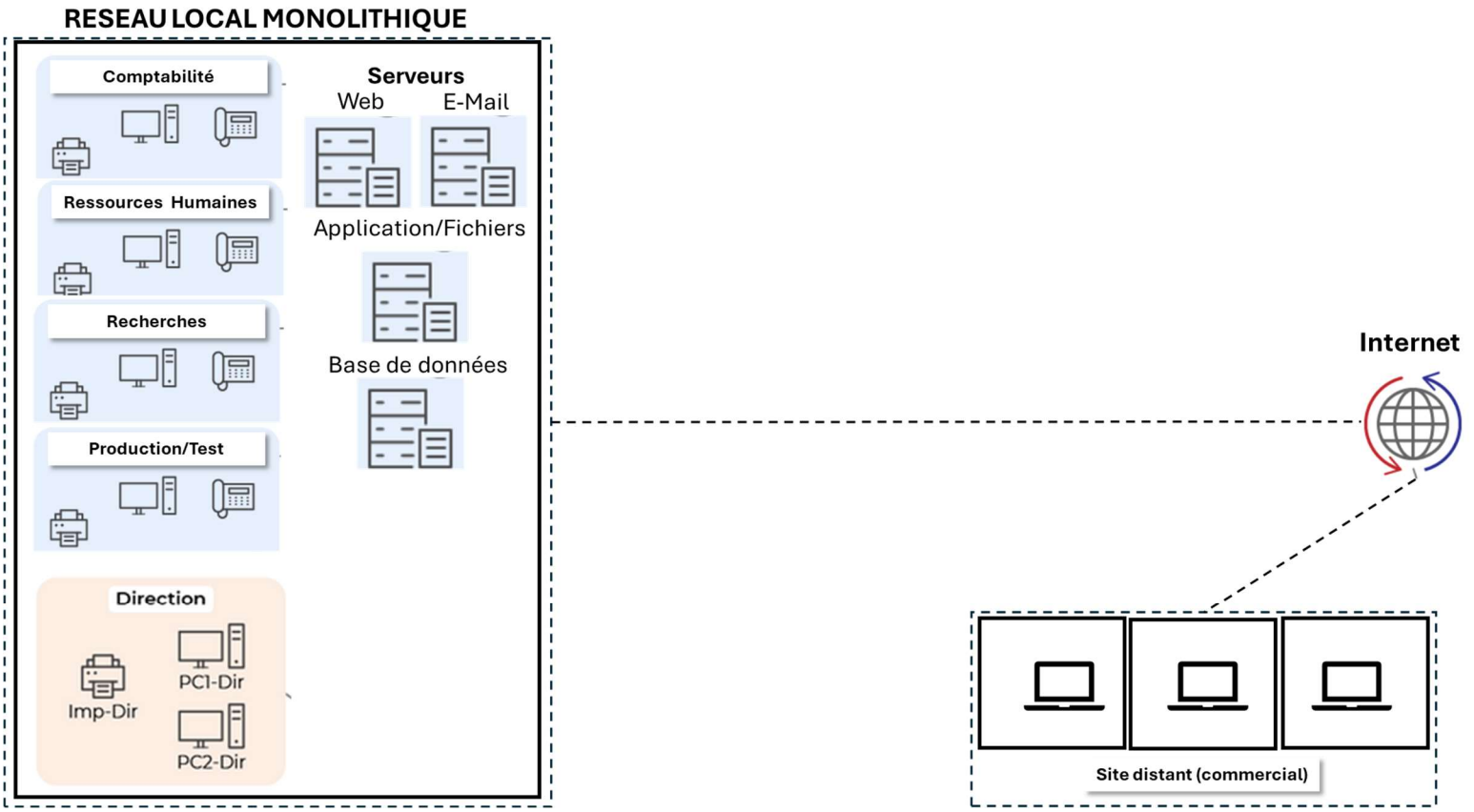
Afin de protéger notre parc utilisé en situation de mobilité, nous préconisons un chiffrement du matériel. Bitlocker est une solution que nous proposons puisqu'elle est intégrée à Windows ce qui correspondrait aux OS dont disposent nos commerciaux sur le terrain. Nous pensons également qu'il est important de créer des GPO (Group Policy Object) pour configurer les appareils en mobilité utilisés par les commerciaux. Nous pourrons ainsi impacter et limiter l'utilisation de l'ordinateur (verrouillage du terminal, lancement d'application au démarrage de l'ordinateur, ...).

En plus de leurs outils, nous souhaiterions sécuriser les connexions des commerciaux via deux solutions.

L'utilisation d'un VPN IP type IPsec protégera les commerciaux lors de leur déplacement en cas de connexion à d'autres ressources qui ne seraient pas situés dans le réseau local et donc protégé par les outils interne à l'entreprise. Cet outil pourra via un tunnel crypté, protéger la connexion internet des utilisateurs assurant la confidentialité des données échangées, ainsi que l'accès à des ressources réseau privé, même à distance.

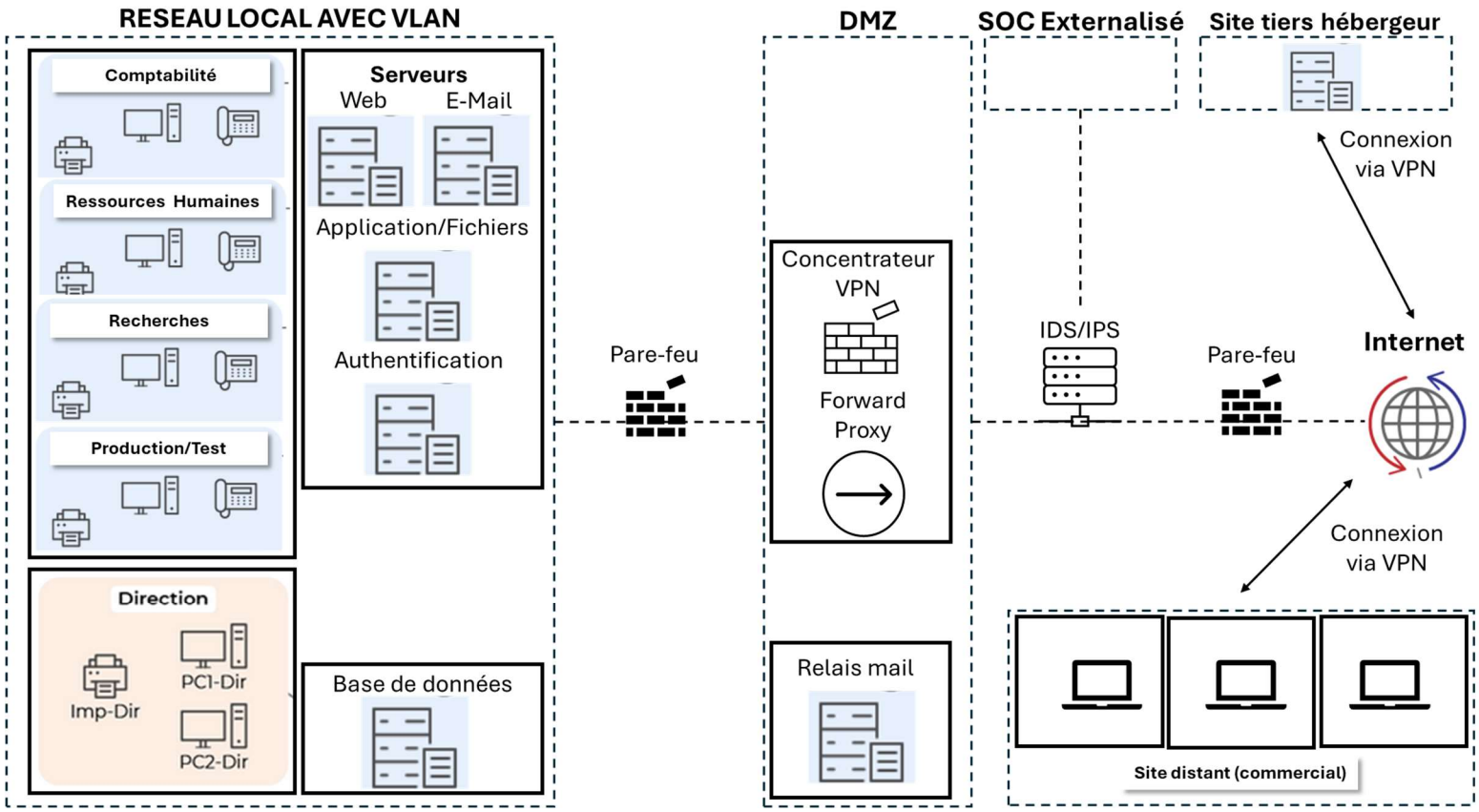
Le déblocage de l'ordinateur des commerciaux sera conditionné via GPO à l'authentification via VPN. L'entreprise devra donc investir dans du matériel adéquat pour mettre en place cette solution. Ce type de matériel est proposé par exemple par l'entreprise Cisco.

A7. Proposition de l'évolution de l'infrastructure de l'entreprise



Ancienne infrastructure

Nouvelle infrastructure



B. Pour aller plus loin :

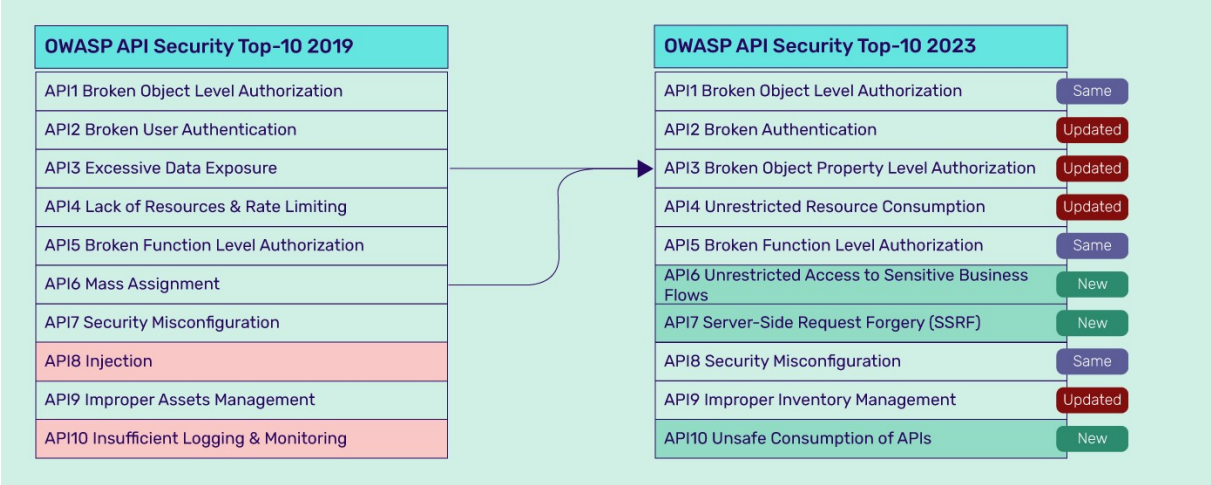
Les prochaines remarques ne vont pas porter sur les critères détaillés dans les besoins du cahier des charges, mais sont néanmoins importantes si l'on souhaite renforcer la protection de son SI.

B1. Maintenir une bonne connaissance du système d'information

Tout d'abord, il nous semble essentiel de continuer à consigner l'ensemble des nouveautés arrivant au sein de notre système d'information afin de toujours garder à jour les informations dont nous disposons.

B2. Prise en compte du top 10 OWASP

Afin de satisfaire les exigences actuelles en matière de sécurité il est important de rester à jour sur les potentielles menaces qui peuvent impacter l'activité de l'entreprise. Nous proposons donc de nous caler sur le top 10 OWASP répertoriant les 10 menaces les plus courantes dans le monde et qui est renouvelé chaque année. L'évolution de notre SI devra donc pouvoir répondre à ce standard de sécurité informatique.



Faire appel à une entreprise pouvant réaliser des tests de pénétration après sécurisation du SI nous permettrait de tester les principales attaques pouvant subvenir sur le réseau en nous basant sur le top 10 OWASP, et de tester les différentes mesures qui seront détaillées ci-après.

B3. Prise en compte du RGPD

Qu'il s'agisse des données clients stockés dans le CRM ou celles des différents employés d'ACME la prise en compte du RGPD[4] est à la fois une obligation réglementaire mais

[4] *LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles*

également un point d'attention dans la future mise en place de notre SI et du déploiement de nos nouveaux outils.

B4. Politique du Zero-Trust

S'imposant comme un nouveau standard dans l'application des principes de sécurité, la politique du Zero-Trust est également recommandé par l'ANSSI pour ses garanties d'accès aux ressources des structures de manières sécurisées. Cela s'appuie sur trois piliers fondamentaux que sont la vérification explicite, l'accès selon le privilège minimum et la prise en compte des violations. L'entreprise ACME devra se rendre conformer à cette politique si elle souhaite rentrer dans les standards de l'ANSSI et donc limiter le nombre des cyberattaques et leurs importances.

B5. Respect de la norme ISO 27001

La conformité à ISO 27001 signifie qu'une organisation ou une entreprise a mis en place un système pour gérer les risques liés à la sécurité de ses données ou des données qu'elle est amenée à traiter, et que ce système est conforme aux bonnes pratiques et principes énoncés dans cette norme internationale. Se conformer à ces bonnes pratiques confirmera à l'entreprise sa capacité en matière de cybersécurité.

B6. Privilégier l'usage de produits et de services qualifiés par l'ANSSI

Toujours dans le cadre des exigences générales, l'utilisation de matériel qualifié par l'ANSSI nous procure une sécurité supplémentaire de notre SI. Pour ce faire elle dispose d'un référentiel avec de nombreux outils matérielles et logiciels considérés comme plus sécurisés.[5]

B7. Solutions logicielles de sécurité.

Le risque de sécurité est accru, car les dispositifs de l'entreprise deviennent plus vulnérables aux attaques de logiciels malveillants tels que les virus, les vers et les chevaux de Troie. Cela peut compromettre la confidentialité des données, la disponibilité des systèmes et l'intégrité des informations.

De surcroit, en l'absence de logiciels de sécurité des réseaux, les infections peuvent se propager plus facilement à travers le réseau de l'entreprise, affectant potentiellement plusieurs systèmes.

L'installation de solutions anti-malwares sur les postes de travail semble être quelque chose de basique, mais d'extrêmement efficace permettant de contrer certaines menaces.

[5] https://cyber.gouv.fr/produits-services-qualifies

B8. Capacité du réseau

La capacité du réseau ne devra pas être oubliée dans cette future évolution qui doit à la fois être sécurisé mais également efficiente dans les logiques métiers qui caractérisent l'entreprise.

Tout d'abord, le réseau doit être suffisamment dimensionné avec des commutateurs, des routeurs et des points d'accès sans fil capables de gérer le nombre d'utilisateurs et le trafic réseau prévu (sans oublier la marge de croissance pour anticiper les futurs besoins). Il faudra également s'assurer que la bande passante Internet et les liens entre les différents segments du réseau sont suffisants pour supporter le trafic généré par les 250 salariés, en prenant en compte les applications et services utilisés.

Enfin la segmentation décrite plus haut nous aidera dans cette tache de capacité du réseau notamment pour des questions de répartition du trafic et la facilitation dans la gestion du réseau.

B9. Comptes administrateurs

Pour sécuriser le SI de l'entreprise ACME un travail doit être fait au niveau des comptes administrateurs.

Tout d'abord il va être question de restreindre fortement l'accès à Internet depuis les postes ou serveurs utilisés pour l'administration du système d'information. Ces postes pourront ainsi intervenir sur certains éléments du réseau mais seront extrêmement limités quant à la navigation sur internet et au téléchargement de logiciels. Cela passera aussi par la configuration des postes via des règles de GPO.

Cette mesure ira de pair avec la nécessité de dédier les comptes administrateurs à des machines préalablement identifiées comme telles. Pour la connexion à ces machines spécifiques l'authentification sera à renforcer avec notamment une connexion à double facteur.

De plus, il faudra faire en sorte d''utiliser un réseau dédié et cloisonné pour l'administration du système d'information ainsi que surveiller son activité au travers une lecture des journaux d'évènements. L'utilisation de VLAN mentionnés précédemment va en ce sens. Il sera également possible de demander au prestataire externe s'occupant du SOC d'analyser de manière quotidienne les logs sur les comptes des administrateurs systèmes.

L'utilisation de clés SSH pourra être envisagée pour chiffrer les communications entre les postes d'administrations et le reste du SI d'ACME.

Enfin, limiter au strict besoin opérationnel les droits d'administration sur les postes d'administration permettra de cerner de manière basique la question de la sécurité des comptes administrateurs. Ces droits doivent être attribués uniquement aux administrateurs en charge de l'administration des postes d'administration.

Annexes

Bibliographie

https://www.ionos.fr/digitalguide/serveur/know-how/fondamentaux-vlan/

https://cyber.gouv.fr/sites/default/files/2017/01/guide_hygiene_informatique_anssi.pdf

https://openclassrooms.com/fr/

https://www.youtube.com/

https://wiki.lidstah.info/

https://www.ibm.com/fr-fr/topics/network-security