bioMérieux

Rapport de Stage

Gestion de la sécurité des machines et serveurs dans un environnement Recherche et Développement

ALVES Brandon
17/05/2022

Table des matières

Contexte

bioMérieux SA est une entreprise française de biotechnologie spécialisée dans le diagnostic in vitro. Son siège se situe à Marcy-l'Étoile et la compagnie est présente dans 44 pays comme les Etats-Unis, la Chine, le Japon, l'Espagne ou encore le Brésil. Elle fournit des solutions de diagnostic dans plus de 160 pays. Ces solutions permettent aux professionnels de santé d'identifier une pathologie de manière rapide et fiable, ainsi que de déterminer la source d'une contamination. Ses produits sont utilisés pour le dépistage des maladies infectieuses et le suivi des cancers et les urgences cardiovasculaires. Ils sont également utilisés pour la détection de micro-organismes dans les produits agroalimentaires, pharmaceutiques et cosmétiques.

L'objectif de ce stage est de comprendre la particularité de la gestion de la Cybersécurité dans un environnement Recherche et Développement (R&D). Dans un premier temps nous étudierons différentes politiques de sécurité qui s'appliquent au sein de l'entreprise bioMérieux. Nous partirons de normes de sécurité qui définissent les bonnes pratiques et comment les mettre en place. Nous étudierons également plus précisément les politiques de sécurité propres à BioMérieux comme la Politique de Sécurité des Systèmes d'Information (PSSI) de l'entreprise. Nous verrons les écarts et les ajustements entre les standards définis dans les normes et les politiques de l'entreprise. Ensuite, nous nous pencherons sur les contraintes métiers liées à la R&D et pourquoi il est important d'adapter la sécurité à cet environnement. Nous mettrons en évidences les éléments qui rentrent en dissonance avec les politiques de sécurité de BioMérieux. Enfin, nous proposerons et étudierons une solution qui n'entrave pas l'activité des départements R&D tout en garantissant un niveau de sécurité optimal du système d'information.

Normes et Politiques de sécurité

Dans son rapport d'activité 2021 [1], cybermalveillance.gouv.fr constate une hausse importante des demandes d'assistance en ligne. Cette plateforme d'aide aux victimes de cybercriminalité a enregistré plus de 173 000 demandes en 2021, soit plus de 65% par rapport à l'année précédente. De son côté, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a également publié un "Panorama de la menace informatique" qui fait état de 1 082 intrusions avérées dans des systèmes d'information en 2021, contre 786 en 2020 (+37%). Ces nombreuses cyberattaques ont des finalités diverses : gains financiers, espionnage, déstabilisation, sabotage... Pour une entreprise comme BioMérieux, les conséquences d'une fuite de données peuvent être très dommageables sur le plan financier et sur le plan de la réputation. C'est pourquoi, aujourd'hui, un Système de Management de la Sécurité de l'Information devient de plus en plus un élément fondamentale dans la sécurité de l'information d'une entreprise.

Normes ISO/CEI 27000

Les normes internationales ISO/CEI 2700x ont pour objet les technologies de l'information, les techniques de sécurité et les systèmes de management de la sécurité de l'information. Cette suite de normes sont composées d'une trentaine de normes. Parmi elles, les plus connues sont :

- La norme ISO/CEI 27001 qui définit un système de management de la sécurité de l'information ;
- La norme ISO/CEI 27002 qui décrit des mesures de sécurité à mettre en œuvre pour le management de la sécurité de l'information.

Ces normes sont mises à jour tous les 5 ans. Celles-ci étant payantes, je me suis appuyé sur les versions de 2013 [2] accessibles gratuitement.

Norme ISO/CEI 27001

Par définition, un SMSI doit garantir les principes suivants :

- Disponibilité : garantir le fonctionnement des outils pour la continuité des services aux utilisateurs ;
- Intégrité : garantir l'exactitude, l'exhaustivité et la cohérence des données.
- Confidentialité : garantir que l'information n'est accessible qu'aux personnes autorisées, pour un besoin spécifique, c'est le principe du « besoin d'en connaitre ».

La première étape dans l'établissement d'un SMSI est la compréhension par l'Organisation de son contexte. Elle doit déterminer les enjeux internes et externes relatifs à son activité. Elle doit ensuite identifier les parties intéressées concernées par le SMSI et les exigences en termes de management de la sécurité de l'information par ces dernières. Enfin, elle doit établir le domaine d'application du SMSI.

La norme ISO/CEI 27001 insiste sur la qualité de leadership dont doit faire preuve la Direction et sur son engagement en faveur du SMSI. Pour ce faire l'Organisation doit par exemple s'assurer que les ressources nécessaires au SMSI soient disponibles. Les rôles et les responsabilités de chaque individu concerné par le SMSI doivent être clairement définis et communiqués au sein de l'Organisation.

Après avoir clairement déterminé les enjeux et exigences s'exerçant sur l'Organisation, celle-ci peut alors déterminer les risques et opportunités liés au système d'information dans le but de les traiter. Pour ce faire, l'Organisation doit définir un processus d'appréciation des risques de sécurité de l'information puis un processus de traitement de ces risques. Des objectifs mesurables en terme de sécurité de l'information doivent également être définis et communiqués au sein des différentes parties intéressées.

La norme ISO/CEI 27001 insiste sur la sensibilisation des risques de la sécurité de l'information au sein de l'Organisation ainsi que sur la documentation des informations exigées par la norme internationale.

Enfin l'Organisation doit surveiller, mesurer, analyser et évaluer les performances de sécurité de l'information ainsi que l'efficacité du SMSI. Pour ce faire, elle peut réaliser des contrôles et des audits. Les contrôles et audits sont des analyses qui permettent d'évaluer un fonctionnement particulier. La différence entre un audit et un contrôle réside dans le fait qu'un contrôle est une procédure qui intervient de manière régulière alors qu'un audit est fait de manière ponctuelle. De plus un audit doit suivre des exigences et être documenté. Si des éléments de non-conformités sont relevés, l'Organisation doit agir pour maitriser et corriger l'élément au sein d'un processus d'amélioration continue.

Norme ISO/CEI 27002

La norme internationale ISO/CEI 27002 est un ensemble de 114 mesures dites « bonnes pratiques » destinées à être utilisées par tous les responsables de SMSI afin de sécuriser leur système d'information. A noter qu'en 2022, la norme ISO/CEI 27002 a été mise à jour. Ces mesures concernent :

- Politiques de sécurité de l'information ;
    - Orientations de la direction en matière de sécurité de l'information ;
- Organisation de la sécurité de l'information ;
    - Organisation interne ;
    - Appareils mobiles et télétravail ;

- Sécurité des ressources humaines ;
    - Avant l'embauche ;
    - Pendant la durée du contrat ;
    - Rupture, termes ou modification du contrat de travail ;
- Gestion des actifs ;
    - Responsabilités relatives aux actifs ;
    - Classification de l'information ;
    - Manipulation des supports ;
- Contrôle d'accès ;
    - Exigences métier en matière de contrôle d'accès ;
    - Gestion de l'accès utilisateur ;
    - Responsabilités des utilisateurs ;
    - Contrôle de l'accès au système et à l'information ;
- Cryptographie ;
    - Mesures cryptographiques ;
- Sécurité physique et environnementale ;
    - Zones sécurisées ;
    - Matériels ;
- Sécurité liée à l'exploitation ;
    - Procédures et responsabilités liées à l'exploitation ;
    - Protection contre les logiciels malveillants ;
    - Sauvegarde ;
    - Journalisation et surveillance ;
    - Maîtrise des logiciels en exploitation ;
    - Gestion des vulnérabilités techniques ;
    - Considérations sur l'audit des systèmes d'information ;
- Sécurité des communications ;
    - Gestion de la sécurité des réseaux ;
    - Transfert de l'information ;
- Acquisition, développement et maintenance des systèmes d'information ;
    - Exigences de sécurité applicables aux systèmes d'information ;
    - Sécurité des processus de développement et d'assistance technique ;
    - Données de test ;
- Relations avec les fournisseurs ;
    - Sécurité dans les relations avec les fournisseurs ;
    - Gestion de la prestation du service ;
- Gestion des incidents liés à la sécurité de l'information ;
    - Gestion des incidents liés à la sécurité de l'information et améliorations ;
- Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité ;
    - Continuité de la sécurité de l'information ;
    - Redondances ;
- Conformité ;
    - Conformité aux obligations légales et réglementaires ;
    - Revue de la sécurité de l'information ;

Politique de Sécurité des Systèmes d'Information (PSSI) bioMérieux

La PSSI est le document de référence de la sécurité du système d'information de l'Organisation. Elle définit les objectifs à atteindre et les moyens accordées pour y parvenir. La démarche de réalisation

de cette politique est basée sur une analyse des risques de la sécurité des systèmes d'information. La PSSI permet à l'entreprise de faire valoir son investissement en termes de sécurité du système d'information auprès de ses clients. De plus, si par exemple l'entreprise est victime d'un vol de données, la PSSI peut faire référence lors d'un conflit juridique pour démontrer que l'entreprise avait investi en moyen humain et technique sur la sécurisation de son système d'information.

La PSSI de bioMérieux [3] reprend la démarche préconisée par les normes internationales ISO/CEI 27 001/002. Cette PSSI s'applique à l'ensemble des ressources humaines du système d'information bioMérieux. Ce document est validé par le Directeur Général du groupe, Alexandre Mérieux. Ce dernier délègue au Directeur des Systèmes d'Information (DSI), Marc BONNET, la gestion du SI. Le Directeur des Systèmes d'Information quant à lui, délègue la gestion de la sécurité du système d'information au Responsable de la Sécurité du Système d'information (RSSI). Le RSSI est assisté dans la définition des stratégies et le suivi des mesures opérationnelles par le responsable de l'équipe Cybersécurité, Thierry VALLET.

La PSSI définie une stratégie d'évaluation des risques. Au cours de cette démarche, elle définit une cartographie des assets en fonction de leurs importances en termes de disponibilité, d'intégrité et de confidentialité. Elle définit l'unique propriétaire de toute ressource informatique appartenant à son système d'information comme étant bioMérieux. La PSSI définit également le SMSI de bioMérieux comme étant la structure qui, au sein d'un processus d'amélioration continue :

- Définit les exigences en termes de sécurité ;
- Définit les solutions opérationnelles de remédiation ;
- Contrôle la bonne application des mesures de sécurité ;
- Sensibilise les différents acteurs concernés par les enjeux de sécurité du système d'information.

La PSSI de bioMérieux stipule également que des audits de sécurité doivent ponctuellement permettre de vérifier la conformité des exigences de sécurité de l'entreprise avec ses enjeux stratégiques et avec ses mesures opérationnelles. Enfin la PSSI de bioMérieux définit des politiques techniques de sécurité (PTS). Ce sont des mesures de sécurité spécifiques aux ressources du système d'information. Ces PTS reprennent les différents domaines d'application de la norme internationale ISO/CEI 27002.

Nous voyons ici que la PSSI de bioMérieux tente le plus possible de suivre les recommandations des normes ISO/CEI 27 001/002. La démarche dans l'établissement de son SMSI suit les préconisations de la norme avec une définition claire des enjeux de sécurité de l'entreprise, l'identification du domaine d'application du SMSI, la répartition des rôles et des responsabilités des différents acteurs, la démarche d'identification et de classification des risques, la sensibilisations aux risques des différents acteurs et le contrôle continue des performances de sécurité et de la cohérence des exigences de sécurité avec les enjeux de l'entreprise au sein d'un processus d'amélioration continue.

Charte informatique bioMérieux

La charte informatique de bioMérieux [4] définit le bon usage des éléments du SI par ses utilisateurs. Ces règles s'appliquent, entre autre, à l'utilisation du poste de travail, l'accès à la messagerie interne et externe ainsi qu'à l'accès d'Internet et de son utilisation. Cette charte stipule que :

- Il est interdit de faire des modifications sur les ordinateurs qui pourraient porter atteinte à l'intégrité et à la sécurité du poste de travail ;
- L'employé ne doit jamais connecter de supports amovibles tels clés USB et disques durs externes autres que ceux disponibles sur la plateforme d'achats de bioMérieux ;

- les codes d'accès au système d'information sont personnels et ne doivent pas être partagés ;
- L'utilisation des ressources informatiques à des fins privées est tolérée pour répondre aux nécessités de la vie courante et familiale ;
- L'usage des ressources de bioMérieux par l'employé doit toujours être adapté à ses missions professionnelles.

Afin d'assurer la sécurité de son système d'information, bioMérieux met en place et utilise certains outils de surveillance. Parmi eux :

- Filtrage des accès Internet ;
- Filtrage des mails ;
- Monitoring par Security Operation Center (SOC) ;
- Analyse de comportement des postes et serveurs (EDR) ;
- Analyse des flux firewalls ;
- Analyse des flux sur les réseaux de production.

Les informations collectés sont conservées pendant plusieurs mois en fonction des outils.

Règles de sécurité pour les machines bioMérieux

Ne sont autorisés à être connectés au réseau de l'entreprise que les équipements appartenant et fournis par bioMérieux. Pour les machines qui seront connectées plus de 15 jours au réseau de l'entreprise, ces dernières doivent respecter 4 règles de sécurités importantes :

- Être protégé par la solution antimalware de l'entreprise. L'antivirus doit être actif et à jour de ses signatures antivirales
- Être à jour de ses patch critiques par la solution d'entreprise
- Être enregistrées dans la base de données de gestion de configuration (CMDB) de l'entreprise ;
- Suivre la convention de nommage établie par l'IS.

L'antivirus utilisé pour les stations de travail est *Symantec ou MDE* et *Trend Micro* pour les serveurs. Le patch manager est *SCCM* pour les stations de travail et *WSUS* pour les serveurs. La CMDB utilisée par bioMérieux est *ServiceNow*. Ces machines sont gérées et fournies par l'IS. La convention de nommage est définie suivant le format suivant :

- une première chaîne de caractères indique la localisation de la machine ;
- une seconde chaîne de caractères indiquent le type de machine ;
- une troisième chaîne de caractères numérique qui permet de rendre le nom de la machine unique.

Par exemple le nom d'une machine pourrait être FRL012345 :

- FR pour être situé en France;
- L pour avoir une machine « laptop »;
- 012345 qui permet de rendre unique le nom de la machine.

Recherche et Développement chez bioMérieux

Cartographie des entités Recherche et Développement

La R&D chez bioMérieux est composée de 1740 employés. L'effectif global de l'entreprise étant de 13747 employés, la R&D représente à peu près 13% de l'effectif global. L'activité de bioMérieux est divisée en 2 pôles d'activité : l'industrie (industry) et le médical (clinic). Les affaires médicales sont

divisées en plusieurs sous pôles d'activité comme l'immunoessais, la microbiologie, le moléculaire ou encore les solutions IT. Les affaires industrielles sont divisées en 2 pôles : l'agroalimentaire (food) et le pharmaceutique (pharma).

Le tableau ci-dessous liste les différentes unités de départements R&D chez bioMérieux. Pour chacun d'eux, le manager y est associé ainsi que sa localisation.

Départements	**Localisations**
Clinic	
Immunoassays	FR/MAR
Regulatory & Clinical Affairs	FR/MAR
Molecular Argene	FR/VER
IT Solutions & System Development	FR/BAL
Portfolio & Open Innovation	FR/CDE
Microbiology	US/STL
AQ Clinic	US/STL
Immunoassays Astute	US/SND
Program & Marketing	US/SLM
Molecular BioFire	US/SLC
Medical Affairs	US/DUR
Industry	
Food	FR/CRA
AQ Industry	FR/CRA
Pharma	US/HMN

Dans le cadre de ce stage, le périmètre auquel nous nous limitons est la R&D IT Solutions & System Development (R&D SD). L'objectif est dans un premier temps d'identifier les contraintes liées à l'activité de la R&D SD. Une fois ces contraintes clairement identifiées, il s'agira alors de proposer une solution qui n'entre pas en conflit avec ces contraintes tout en garantissant une protection des machines de la R&D SD. Enfin la solution trouvée pourra ensuite être communiquée et déployée sur l'ensemble des machines R&D de bioMérieux.

Définition des machines « produits » de Recherche et Développement

Parmi les machines non standards, on retrouve les machines « produits » de R&D. Ces machines peuvent être divisées en 3 familles :

- Famille A : Ce sont des machines gérées et fournies par l'IS. Elles possèdent une image d'OS de l'IS. Elles ont donc un antivirus installé ainsi qu'un patch manager. Elles sont enregistrées dans la CMDB et suivent la convention de nommage de l'IS. Elles sont connectées au domaine.
- Famille B : Ces machines sont semblables aux machines de la famille 1 à l'exception du fait qu'elles ont une image d'OS de la R&D. De plus, elles sont gérées par la R&D. Enfin, elles suivent une convention de nommage de l'IS mais spécifique pour la R&D (en FRRD ou en USRD).
- Famille C : Ces machines ne sont pas connectées au domaine contrairement aux autres. Elles sont dans des workgroups. Elles ne sont pas gérées par l'IS mais par la R&D. Elles ont Windows Defender comme Antivirus. Elles n'ont pas de patch manager et ne sont pas enregistrées dans la CMDB. Elles ne respectent pas la convention de nommage de l'IS.

On résume ces informations dans le tableau ci-dessous.

Famille	A	B	C
Géré par	IS	R&D	R&D
OS	IS	R&D	R&D
Antivirus	oui	oui	Oui, Windows Defender Antivirus
Patch Manager (SCCM / WSUS)	oui	oui	Non
CMDB	oui	oui	non
Convention de nommage de l'IS	oui	Oui, en FRRD/USRD	non
Connecté au domaine	oui	oui	non

Contraintes liées aux activités de Recherche et Développement

La recherche et développement au sein de bioMérieux est soumise à certaines contraintes. Ces contraintes sont quelques fois en contradiction avec la politique de sécurité de bioMérieux. L'objectif de ce stage est alors de trouver un moyen de concilier ces contraintes avec la politique de sécurité de bioMérieux. J'ai pu m'entretenir avec le R&D System Manager chez bioMérieux afin d'évoquer ces contraintes. Premièrement, il faut distinguer 2 types de machines : les machines standards et les machines non-standards. Parmi les machines standards, on retrouve les laptops personnels. Ces machines peuvent être spécialisées dans le développement comme pour les membres des départements R&D. Ces machines ont par exemple plus de CPU. Cela leur permet de faire fonctionner des logiciels nécessitant beaucoup de CPU comme des IDE par exemple. Ces machines sont remplacées tous les 3 ans (avant la fin d'expiration de la garantie). Enfin ces machines sont connectées au domaine de l'entreprise. Parmi les machines non-standards, on retrouve les machines de production, qui sont nécessaires à l'activité de l'entreprise, ou encore les machines « produits » R&D. Ces dernières sont utilisées à des fins de test. Elle simulent l'environnement du client avec le produit logiciel vendu.

Premièrement, une nécessité au sein du département R&D est de pouvoir disposer de privilèges « administrateur », au moins ponctuellement. En effet ces privilèges sont nécessaires pour :

- Installer des environnements de développement comme Eclipse ou IntelliJ IDEA;
- Installer d'anciennes ou de nouvelles versions de logiciels;
- Installer un client de gestion de version sur les nouvelles machines comme Git ;
- Installer des logiciels de diagrammes;
- Lancer des scripts;
- Installer, lancer, arrêter, supprimer des services comme les services web ou de bases de données;
- Ouvrir des ports logiciels;
- Ajouter une règle dans le firewall d'un LAN;
- Pouvoir écrire sur le disque.

Les machines « produits » ont également des besoins particuliers en termes d'antivirus. En effet, un antivirus trop restrictif ne peut pas convenir. Ce qui était par exemple le cas avec Symantec. Symantec mettait en quarantaine certains fichiers exécutables qu'il considérait comme potentiellement dangereux. Symantec se basait sur la réputation des logiciels. Ces nouveaux logiciels ayant une réputation inconnue, Symantec les considérait comme potentiellement dangereux.

De plus ces machines ne peuvent pas toujours être connectées au domaine de l'entreprise. En effet, les machines connectées au domaine sont soumises à des stratégies de groupe (GPO). Ces stratégies peuvent limiter certaines fonctionnalités des machines auxquelles elles s'appliquent. Il n'est pas non plus envisageable de joindre ces machines au domaine en leur appliquant une politique d'exception. En effet ces machines auraient accès aux ressources du domaine alors qu'elles n'en n'ont peut-être pas l'utilité et seraient de plus moins bien protégées que les machines sur lesquels les GPO s'appliquent. BioMérieux a choisi de laisser hors du domaine les machines « produits » lorsque cela est possible.

Les contraintes évoquées précédemment sont liées au développement. Il existe d'autres contraintes, notamment celles liées aux produits commercialisés par l'entreprise. Par exemple, l'utilisation, encore une fois, d'un antivirus peut poser problème. La signature de certains logiciels peut être reconnue par l'antivirus et empêcher leur exécution. Il existe également des contraintes de performances pour ces produits. En effet, l'utilisation d'un antivirus peut impacter de manière significative les performances, ce qui n'est pas souhaitable.

Nous voyons donc ici que les entités R&D ont des contraintes particulières. L'application stricte de la politique de sécurité de bioMérieux sur les postes de travail R&D n'est pas souhaitable d'un point de vue Business. Celle-ci perturberait le travail des équipes de R&D. La solution adoptée par l'entreprise est d'appliquer des règles de sécurité différentes sur ces postes de travail. Il faut pour cela un outil qui sécurise tout en assurant le bon fonctionnement du service R&D.

Gestion actuelle de la sécurité dans les entités Recherche et Développement

Dans un premier temps, il a été décidé d'évaluer la gestion de la sécurité dans les entités R&D au sein du département R&D SD. J'ai eu l'occasion de discuter avec deux membres de cette équipe, l'un situé à Saint Louis, l'autre situé à La Balme-les-Grottes. Ces discussions m'ont permis de comprendre leur fonctionnement actuel. Une première discussion s'est structurée autour des points suivants :

- l'utilisation d'antivirus;
- l'utilisation de patch manager;
- l'enregistrement dans la CMDB;
- le respect de la convention de nommage.

Les solutions antivirales utilisées par la R&D SD est Symantec et Windows Defender. La fonctionnalité d'analyse de réputation est désactivée dans Symantec afin de ne pas mettre en quarantaine l'exécution de nouveaux logiciels. Les machines de la famille C activent la protection Windows Defender. La plupart de ces machines ne sont pas connues de SCCM. Pour les machines des familles A et B, toutes ne possèdent pas un client SCCM non plus. La majorité des machines de la famille C ne sont pas enregistrées dans la CMDB. Afin de maintenir un inventaire au niveau local, celles-ci sont listées dans des documents (de type feuille de calcul). Encore une fois toutes les machines des familles A et B ne sont pas non plus enregistrées dans ServiceNow. Enfin, la R&D SD de Saint Louis utilise sa propre convention de nommage. Celle-ci ne respecte pas les règles de l'IS. Ces machines ainsi nommées ne sont donc pas connectées au domaine de l'entreprise. Chez la R&D de La Balme-les-Grottes, les équipes utilisent un outils nommé RDVMTools. Cet outil attribue automatiquement un nom de machine en [FR/US]RD[PH/VM] au nouvelles machines déployées.

Solution choisie par bioMérieux

Comme évoqué précédemment, la solution cherchée par bioMérieux doit permettre d'appliquer sa politique de sécurité tout en garantissant le bon fonctionnement des métiers de la R&D. Un antivirus classique est une solution difficilement compatible avec les contraintes métiers de la R&D :

- les antivirus utilisant des signatures ont tendances à bloquer trop souvent l'installation et l'utilisation de nouveaux logiciels.
- Ces antivirus ne sont pas obligatoirement ceux utilisés par les clients de bioMerieux.

La solution trouvée est fondée sur une analyse comportementale plutôt qu'une comparaison de signature. Cette solution doit également permettre d'installer les mises à jours sur les machines comme le fait SCCM. Enfin cette solution doit permettre d'inventorier les différentes machines.

La solution qu'a choisi bioMérieux est Microsoft Defender for Endpoints (MDE). MDE a également l'avantage d'être embarqué par défaut sur les machines Windows 10. Cela est un élément très important pour la R&D. En effet, la R&D doit souvent reproduire les environnements des clients bioMérieux avec les machines « produits ». Or ces clients n'ont pas, a priori, obligatoirement les mêmes solutions antivirales installées sur leur machines. Cependant, ils ont généralement un système d'exploitation Windows 10 avec MDE de préinstallé dessus.

Déploiement de MDE sur les machines Recherche et Développement non-standards

Phase de recensement des machines Recherche et Développement non-standards

La première étape préalable au déploiement de MDE sur les machines non-standards est le recensement de ces dernières. Pour les machines R&D des catégories A et B, il n'y a normalement pas de problème particulier à les inventorier. En effet, ces machines sont connectées au domaine et recensées dans la CMDB. Le problème se pose pour les machines R&D de la catégorie C. En effet, la visibilité sur ces machines est très réduite. Comme évoqué précédemment, ces machines ne sont pour la plupart pas connues de la CMDB. La méthode afin de recenser ces machines a été de contacter les différents responsables au sein du département R&D System Development pour leur demander la liste de leurs machines de la catégorie C. Ces différents contacts possédaient tous une liste des machines qu'ils utilisaient dans leurs périmètres. Cela a facilité le travail d'inventaire.

Phase de création des profils standards et non standards

Afin de pouvoir appliquer des politiques d'exception sur les machines non-standards, il a fallu créer des groupes particuliers dans lesquels placer ces machines. Ces différents profils doivent être créés dans un autre outil : Microsoft Endpoint Manager (MEM). MEM est un gestionnaire de parc informatique. Il permet de gérer l'ensemble des utilisateurs, applications machines sans interrompre les processus existants. La première étape a donc été de créer un profil pour les machines non-standards. Les machines connectées à l'AD, elles, sont associées au profil standard.

Phase de déploiement de MDE sur les machines R&D non-standards

La phase d'enrôlement des machines dans MDE est organisées en plusieurs vagues. Les vagues sont classées en fonction de la criticité des postes qui y sont associés. Les machines les plus critiques sont les machines associées à la production. En effet, un incident sur ces machines pourrait entraîner une perte d'activité pour l'entreprise. C'est pourquoi ces machines seront enrôlées en dernier.

L'enrôlement des machines dans MDE est différent selon la catégorie de la machine. Pour les machines des catégories A et B, c'est-à-dire connectées au domaine, l'enrôlement se fait via SCCM. La machine est dans un premier temps associée au profil non-standard dans Intune, puis dans un second temps enrôlée dans MDE.

Pour les machines de la catégorie C, la procédure est différente. En effet ces machines n'étant pas connectées au domaine, il n'est pas possible de passer par SCCM. Pour enroler ces machines, MDE met à disposition un script. Ce script, une fois exécuté sur la machine cible, enrôle cette dernière

dans MDE. Une option sur MDE permet alors d'enregistrer les machines connues de MDE dans Intune. Le profil non-standard est ensuite associé à ces machines.

Conclusion

Ce stage a été une belle opportunité dans mon parcours d'ingénieur. Celui-ci m'a permis d'évoluer dans une entreprise internationale, notamment au sein de son équipe cybersécurité, hétérogène en profils. En effet, j'ai pu côtoyer des profils assez variés. Certains étaient plutôt orientés gouvernance, c'est-à-dire avec une approche décisionnelle de la cybersécurité, tandis que d'autres étaient plutôt orientés opérationnel, c'est-à-dire avec une approche technique de la cybersécurité. J'ai ainsi pu comprendre que les deux approches étaient complémentaires et indissociables l'une de l'autre. En effet, la partie gouvernance comprend la définition et l'établissement de règles de sécurité, la mise en place des contrôles appropriés ainsi que la gestion de risques. La partie opérationnelle, consiste en la mise en pratique de ces règles de sécurité et des outils de contrôles.

J'ai également pu observer et prendre part aux interactions entre la cybersécurité et la R&D. J'ai trouvé intéressant de voir comment ces deux entités ont pu trouver une solution commune qui répondait à leur problème respectif :

- Du côté de la cybersécurité, le problème était le faible niveau de sécurité sur les machines R&D en workgroup, liée à l'application approximative des règles de sécurité sur ces machines (pas toujours inventoriées dans la CMDB, pas toujours de connu du gestionnaire de patch) ;
- Du côté de la R&D, le problème était la difficulté d'utilisation de certains outils qui étaient régulièrement bloqués par l'outil antiviral Symantec.

Ainsi, l'EDR de Microsoft a pu améliorer le niveau de sécurité de l'entreprise sans bloquer l'activité des équipes R&D qui sont soumises aux différentes contraintes que nous avons évoquées. De plus cet outil a permis aussi bien à la R&D et à la cybersécurité d'avoir une meilleure vue sur l'ensemble des machines en workgroup.

Cette expérience chez BioMérieux m'a également permis de comprendre l'organisation au seins d'une grande entreprise. J'ai pu par exemple me rendre compte qu'il existe plusieurs niveaux de décision lorsqu'une action est envisagée. Cette action doit être validée par ces différents niveau ce qui peut prendre du beaucoup de temps quelques fois.

Définitions

Antivirus

Un antivirus ou antimalware est un logiciel conçu pour détecter, alerter et neutraliser des logiciels ou fichiers malveillants. Ces antivirus peuvent être classer en deux catégories : les antivirus « classiques » et les antivirus de « nouvelle génération ». Nous nous intéressons ici aux logiciels classiques et nous nous intéresseront dans un second temps aux antivirus de nouvelle génération.

Le mode opératoire de ces antivirus pour détecter des programmes malveillants est simple. Ce mode opératoire se base sur les signatures virales. Une signature virale est une information qui caractérise et identifie un virus. Par exemple une signature virale peut être une chaîne binaire d'un exécutable qui installe, à partir d'un adresse internet public, un rançongiciel sur le système. La liste des signatures virales sont accessibles par ces antivirus. Les antivirus analysent alors l'ensemble des fichiers présent sur le système d'information et compare leur contenu aux signature virales. Si une

concordance apparaît, une alerte est déclenchée et une action peut être prise par l'antivirus comme la mise en quarantaine du programme malveillant par exemple.

Patch Manager

Un patch manager est un logiciel qui permet de détecter, analyser et déployer des mises à jours de sécurité logicielles. Celui-ci référence le parc informatique existant et conserve l'historique des installation de patchs. Il peut donc localiser précisément sur quelles machines doivent être installées les patchs de sécurité. Il permet également à tout instant de revenir en arrière après l'installation d'un correctif. La force d'un patch manager réside dans sa base de données qui référence l'état de mises à jour des machines. Ces logiciels facilitent ainsi la détection d'incompatibilités logicielles ou matérielles avec un correctif de sécurité spécifique. Les correctifs installés sont ceux des éditeurs et dépendent donc de leurs délais de publication.

Obsolescence

L'obsolescence est le fait de devenir désuet. L'obsolescence est un risque que les systèmes d'information doivent considérer. Les logiciels ont souvent une durée de support limité. Au-delà de cette période, le support de l'outil ne sera plus assuré. Si des failles apparaissent au-delà de cette période de support, celles-ci ne pourront être corrigées. Cela correspond donc à un risque important en terme de sécurité.

Base de données de gestion de configuration (CMDB)

Une CMDB est une base de données répertoriant les informations relatives à un SI. Ces informations portent sur les composant qui forment le SI. Ces élément sont appelés « éléments de configuration ». Ces éléments peuvent être n'importe quel composant informatique comme par exemple des logiciels, du matériel, ou encore du personnel. La CMDB fournit également une vue organisée de ces éléments de configuration et des relations entre eux. Un élément de configuration dispose d'attributs modifiables, configurables.

Au fur et à mesure que l'infrastructure du SI devient de plus en plus importante, la compréhension de l'information devient de plus en plus difficile. C'est alors l'intérêt d'utiliser une CMDB.

Domaine, Active Directory (AD) et Workgroup

Dans l'environnement Microsoft, un domaine est un ensemble de machines partageant des informations d'annuaire. Le domaine permet à l'administrateur du domaine de gérer les ressources au sein de son entreprise de manière plus efficace car centralisées dans une même base e données. Cette base de données est stockée sur des serveurs particuliers, appelés Domain Controller.

L'Active Directory (AD) est la mise en œuvre par Microsoft des services d'annuaire LDAP de ressources pour les systèmes d'exploitation Windows. Ces ressources peuvent être des utilisateurs, des postes clients, des imprimantes, des dossiers partagés, des domaines, des groupes, etc… L'AD permet l'identification (identifiant), l'authentification (mot de passe) et l'autorisation (permissions) de ces ressources. Ces ressources sont appelées des objets. Ces objets sont organisés de manière hiérarchique. L'objet de top niveau est appelée Forêt. Les objets sont regroupés au sein d'un domaine. Au sein d'un domaine, c'est Le Domain Controller (DC) qui assure l'identification et l'authentification des objets du domaine. L'AD permet d'avoir un fort niveau de sécurité avec l'identification, l'authentification et les autorisations. Il permet également de localiser un objet au sein d'un domaine. L'AD permet également de gérer les privilèges des objets grâce à des politiques de groupes (objets du même groupe ont les mêmes droits).

Un workgroup est un ensemble de machines dans lequel chaque machines gère la sécurité de l'accès à ses ressources partagées. Le workgroup est un réseau pair-à-pair. Il n'existe pas d'authentification centralisée dans un workgroup contrairement au domaine.

La sécurité de l'AD est critique pour un système d'information. En effet, si un individu malveillant parvient à s'introduire dans l'AD, par exemple en utilisant des informations de connexion dérobés, ce dernier aura accès aux ressources que lui octroient les privilèges du compte usurpé. Si les privilèges sont importants, il pourra agir en conséquence et il y pourra alors y avoir un risque de vol d'information ou encore un risque d'arrêt de l'activité de l'entreprise (si l'AD est neutralisé par exemple). Si les privilèges ne sont pas assez élevés il pourra toujours essayer d'infecter les dossiers partager pour infecter quelqu'un avec des privilèges suffisants.

L'utilisation de workgroups soulève des problématiques en terme de sécurité. Premièrement, ces machines sont beaucoup moins traçables car non connectés à l'AD et ne bénéficient donc pas non plus de la sécurité déployé sur le domaine. De plus, ces machines, n'étant pas soumises aux politiques de groupes, les utilisateurs sont administrateurs de leur propre machine, ce qui peut poser des problèmes en terme de sécurité. Néanmoins, si ces machines sont bien isolées, le fait de ne pas être reliées à l'AD peut permettre de contenir certaines menaces et de ne pas les propager sur le domaine.

Les règles de nommage sont un enjeu important au sein d'un réseau de machines. Le nom d'hôte d'une machine permet d'identifier celle-ci de manière unique sur le réseau. Contrairement à l'adresse IP qui peut être attribuée de manière dynamique et donc évoluer, le nom de machine n'a pas vocation à changer. Ainsi, ne pas suivre les conventions de nommages peut engendrer d'introduire des doublons au sein du réseau. Cela pose alors problème pour l'identification des machines et la cohérence de l'AD.

Stratégie de Groupe (GPO)

Une stratégie de groupe (GPO) est un ensemble de paramètres qui s'appliquent à des groupes d'utilisateurs ou de machines. L'utilité des GPO est d'avoir une configuration homogène sur des machines ou des utilisateurs d'un même groupe. Ces configuration peuvent par exemple être :

- Bloque l'invite de commande ;
- Définir un fond d'écran ;
- Déployer un logiciel ;
- Désactiver la télémétrie de Windows 10 ;
- Préconfigurer la suite Office ;
- …

Il existe des stratégies de groupe locale et des stratégies de groupe Active Directory. Les stratégies de groupes locales s'appliquent sur des machines en workgroup. La configuration doit être faite sur chaque machine du workgroup. Pour les GPO AD, les configuration sont faites à l'aide d'un gestionnaire de stratégie de groupe. Les GPO peuvent s'appliquer à différents niveaux :

- Workgroup (stratégie de groupe locale) ;
- Site ;
- Domaine ;
- Unité d'organisation.

C'est la GPO la plus proche de l'objet (utilisateur ou machine) qui s'applique en cas de conflit.

Intune

Microsoft Intune est un service basé sur le cloud qui se concentre sur la gestion des périphériques mobiles (MDM) et la gestion des applications mobiles (MAM). Il permet de contrôler la façon dont les appareils d'une organisation sont utilisés, y compris les téléphones mobiles, les tablettes et les ordinateurs portables. Il permet également de définir des stratégies spécifiques pour contrôler les applications. Par exemple, il est possible d'empêcher l'envoi d'e-mails à des personnes extérieures à l'organisation. Intune permet également aux utilisateurs de se servir de leurs appareils personnels à l'école ou au travail. Sur les appareils personnels, Intune permet de garantir que les données restent protégées et peut isoler les informations professionnelles des données personnelles.

Extended Detection and Response (XDR)

Un XDR est un outil de sécurité qui collecte et met en corrélation des données provenant de plusieurs couches de sécurité :

- Email ;
- Gestion des vulnérabilités ;
- Points de terminaison ;
- Identité ;
- Applications pour le cloud ;

Un XDR permet une détection, grâce à la mise en corrélation des données qu'il reçoit, de détecter plus rapidement les menaces et permet donc également des réponses plus rapides. La solution XDR choisie par bioMérieux est Microsoft 365 Defender.

Endpoint Detection and Response (EDR)

La solution EDR choisie par bioMérieux est Microsoft Defender for Endpoints (MDE).

Références

[1] vie-publique.fr, «Les cybermalveillances en forte hausse en 2021,» 30 03 2022. [En ligne]. Available: https://www.vie-publique.fr/en-bref/284654-les-cybermalveillances-en-forte-hausse-en-2021. [Accès le 08 07 2022].

[2] ISO/CEI, Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences, ISO/CEI, 2013.

[3] P. PELONI, Politique de sécurité des systèmes d'information bioMérieux, 2007.

[4] bioMérieux, Charte de bonne conduite pour l'utilisation des outils informatiques, 2022.