



RAPPORT DE STAGE

AISSA Quentin

Du 30 Mai au 07 Juillet 2022

Tuteur de stage : David DEBLIQUY
Enseignant référent : Madame ARGAUD

Etablissement : Saint-Aspais Melun
Entreprise d'accueil : Eau de Paris – Siège social

SOMMAIRE

Introduction.....	3
Etude de l'existant.....	3
Cahier des charges.....	4
Mise en place de station de décontamination.....	4
Conclusion.....	6

Introduction

If I was accepted in the company « Eau de Paris », it is to answer a problematic, the safety with regard to the peripherals of external storages. I will have to find a solution, implement it and inform the employees. First of all I had to find out how the security of this system currently works, the company uses « A Totem of decontamination » (Appendix 1) which allows the analysis of USB media, which is present at the headquarters as well as on primary remote sites. The decontamination station is simple, you insert a USB device like a USB key, the device scans it and it can be used on any computer for a limited time. The company's headquarters being particularly large, a single device is not enough for the entire structure, so we had to opt for a solution, that of extending the decontamination station system to the entire structure with their new version, the « A Satellite of decontamination » (Appendix 2) more compact and with more configuration, it will allow a better integrity of the security system for the users of the company. On top of that I will have the opportunity to take care of the company's network on the industrial side and to help the users to solve their problems.

Appendix 1 :



Appendix 2 :



Etude de l'existant

Eau de Paris est une entreprise Public local à caractère industriel ou commercial, elle est en charge de capter, traiter et distribuer l'eau aux parisiens. Eau de Paris a pour Directeur Général Benjamin Gustin, appuyé par une directrice générale adjointe, Estelle Desarnaud. Ils pilotent huit directions distinctes, respectivement chargées de la production, de la qualité de l'eau, de la distribution, du patrimoine, des systèmes d'information, des relations extérieures, du secrétariat général et des ressources humaines et financières (Annexe 3). Pour ma part je me situe dans le service opération et sécurité au sein de la direction du système d'information, celui-ci est composé de plusieurs sous services, je me situe dans le service pole opération et sécurités (Annexe 4). L'entreprise comportant un effectif d'environ 900 salariés, il est important de pouvoir fournir à l'ensemble de nos collaborateurs les moyens nécessaires pour travailler dans les meilleures conditions et ceux, en toute sécurité. La DSI offre à l'ensemble des collaborateurs et services de la régie une gamme complète de prestations. Dans une démarche soucieuse de la qualité du service, la DSI propose un catalogue de services évolutifs. Il permet de connaître la définition, le niveau de service et les conditions d'accès pour chacune des prestations.

Au quotidien, la DSI travaille à faire fonctionner ces services dans des conditions optimales. En cas de problème, les utilisateurs peuvent faire appel à la « Eautline » via l'Intranet (Eautline). L'équipe en charge du support à la DSI est ainsi la seule d'Eau de Paris à travailler en prise direct, sans intermédiaire hiérarchique, avec l'ensemble des collaborateurs de la régie Le Service Infrastructures et Opérations assurent la définition, la maîtrise d'œuvre et la maintenance des infrastructures informatiques ainsi que le support de l'ensemble des utilisateurs du SI d'Eau de Paris.

Le pôle « Opérations et Sécurité » est garant de l'architecture technique des différentes infrastructures, du plan d'évolution de ces infrastructures et de l'intégration des applications livrées par les services « Etudes et Projets » et « SIG Data et Industriel » au sein des infrastructures SI. Ce pôle s'assure aussi que le SI et ses infrastructures

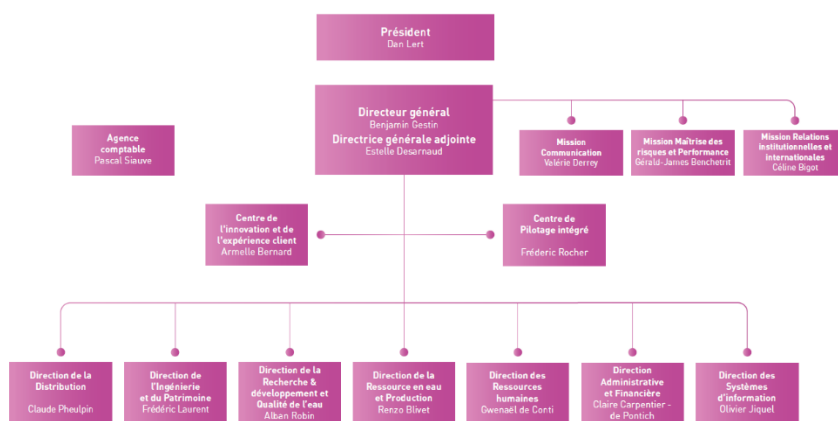
fonctionnent en permanence en opérant des contrôles réguliers et en assurant la maintenance des systèmes.

Le pôle « Support et environnement utilisateurs » est quant à lui le point d'entrée unique de la DSI pour tous les utilisateurs qu'il s'agisse de dotation de matériel et/ou logiciel, ou encore de questions ou problèmes relatifs à leur usage.

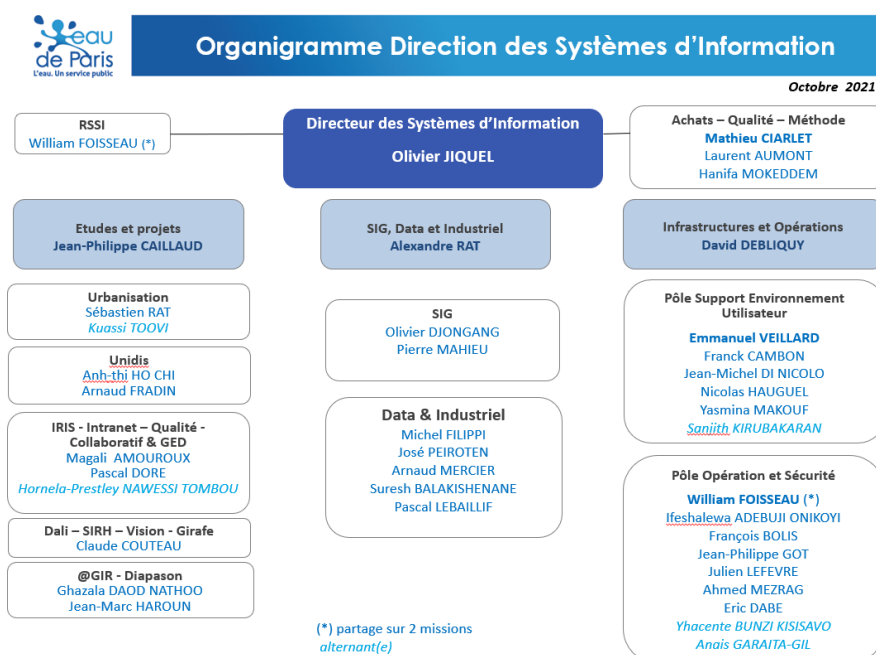
Eau de Paris est aussi acteur de la cyber sécurité. Les attaques informatiques et leurs conséquences sur les entreprises et les organisations font régulièrement la une de l'actualité. Comme toute entreprise, Eau de Paris est exposée à ces risques et il est de leurs responsabilités collectives d'y faire face.

La réduction du risque passe par des dispositifs de sécurité gérés par les équipes en charge du Système d'information mais aussi par une sensibilisation et un comportement responsable de chaque utilisateur.

Annexe 3 :



Annexe 4 :



Cahier des charges

L'entreprise Eau de Paris m'a donc recruté dans le but d'améliorer, de mettre à jour et d'étendre la sécurité par rapport aux stockages amovibles de l'entreprise. Dans un premier temps il faudra analyser le système actuel et le fonctionnement général de la sécurité au sein de l'entreprise, savoir comment l'entreprise se protège pour savoir où et comment mieux la sécurisée. Dans un second temps il faudra mettre en place le système, le configurer pour être facile de compréhension et d'utilisation par les utilisateurs et le tester pour s'assurer de sa fonctionnalité de plus, le système physique devra fonctionner en Wi-Fi afin d'être utilisable partout. Dans un troisième temps il faudra développer ce système dans la structure, l'amener à être disponible pour tous et partout. Dans un dernier temps il faudra établir une communication pour faire comprendre aux utilisateurs les nouveaux ajouts de sécurités et comment s'en servir au quotidien pour assurer la sécurité de l'entreprise notamment en les sensibilisant.

Il s'agit alors d'installer un dispositif appelé « Station de décontamination » permettant de scanner des supports USB et ainsi savoir s'ils sont ou non affecté par un virus, cela afin d'autoriser ou refuser n'importe quels périphériques à pouvoir se connecter à un poste informatique durant une période donnée. Il y a un total de 7 stations à configurer soit 4 pour le siège, 2 encore non définies et une station d'ancienne génération à déplacer sur un autre site et donc à reconfigurer. Ensuite il faudra les installer à des endroits stratégiques pour qu'ils soient disponibles pour tous et toutes. Pour finir il faudra réaliser un support de communication par l'intermédiaire de mail, message et affiches pour faire comprendre à quoi servent ces stations, comment l'utiliser et sa nécessité pour l'entreprise.

Annexe à cela, je réaliserai un schéma de liaison du réseau industriel, j'assisterai la reconfiguration de pare feu, l'installation de nouveau pare feu, l'installation de routeur et de serveur sur des sites distants.

Mise en place de station de décontamination

Après avoir passé une semaine à découvrir le fonctionnement d'un service informatique au sein d'une entreprise et d'avoir pu échanger avec chacun de mes collègues, il fallait commencer à mettre en place un système de sécurité et de vérification des stockages amovibles (clés USB, disque dur, smartphone...). J'ai donc commencé à m'intéresser à la sécurité utilisée dans l'entreprise, celle-ci utilise en grande majorité une solution d'end point et des firewalls de nouvelles générations (les deux provenant du même fournisseur). Les solutions d'end point de l'entreprise sont de haute technologie, elles représentent des points d'entrée vulnérables clés pour les cybercriminels. Les end point sont l'endroit où les attaquants exécutent du code et exploitent les vulnérabilités, ainsi que les ressources à chiffrer, exfiltrer ou exploiter. La solution d'End point est donc un anti-virus à type comportementale, aussi appelé technologie EDR, elle permet de bloquer les logiciels malveillants, les exploits et les attaques avancées sans fichier avec le stack technologique de sécurité des terminaux la plus complète du secteur. L'agent bloque les menaces grâce à la protection contre les menaces comportementales, à l'IA et à l'analyse dans le Cloud. Pour résumer la

technologie EDR est capable de s'adapter et d'analyser l'exécution des programmes et de les bloquer si nécessaire.

La première question à se poser est alors ; Pourquoi utiliser une solution de vérification des stockages amovibles pour l'entreprise alors que celle-ci possède un anti-virus à la pointe de la technologie moderne ? La réponse fut longue à trouver mais simple, les stations de décontamination des supports de stockages amovibles ne sont pas vitales pour l'entreprise mais représentent une sécurité supplémentaire permettant aux utilisateurs de s'assurer eux même de leurs propres sécurités cela les mettant en confiance avec leur environnement de travail.

J'ai donc dû mettre en place ce système de station de décontamination, l'objectif est de mettre à disposition des utilisateurs une borne permettant de scanner n'importe quel support de stockages amovibles afin d'avoir une porte de sécurité supplémentaire dans la structure. L'entreprise a déjà par le passé utilisé des stations de décontamination qui ont été mises en place sur plusieurs sites distants dont un au siège où je me situe, cette première génération de station s'appelle des « Totems », ils sont imposants et coûtent relativement chers, ils sont au total de 13. Mon responsable m'informe alors de l'arrivée d'une nouvelle génération plus compacte et moins chère, l'on appelle ce nouvel appareil « Satellite ».

Ma tâche est alors de configurer ces Satellites, afin de les déployer un étage sur deux dans le siège. L'on m'a alors fourni des accès privilégiés afin de pouvoir configurer les Satellites dans leur intégrité.

Afin de configurer une station de décontamination j'ai eu accès à plusieurs documentations, celle de configuration de la station, celle de configuration de l'agent pour les postes informatiques et une documentation réalisée par l'entreprise pour savoir quels paramètres utiliser. Une station a alors besoin de deux configurations :

- La première permet d'identifier la station, de la nommer et de lui apporter des modifications.
- La deuxième permet de lui affecter une configuration réseau, si celle-ci se connecte en Ethernet ou en Wi-Fi, le certificat, etc.

Cependant la documentation de configuration de l'entreprise n'a jamais configuré ses stations en Wi-Fi, il va alors falloir mettre à jour le document et trouver comment réaliser la configuration en Wi-Fi.

Tout d'abord je réalise la configuration d'identification, je me connecte alors au panel prévu pour l'utilisation des stations je nomme ainsi ma station sur l'interface, note son numéro de série et l'ajoute au groupe de l'entreprise. Je peux maintenant créer une configuration relative au modèle de la station, je configure alors (Annexe 5) :

- L'adresse ip (en dhcp)
- Le masque
- Le DNS

La configuration sera alors faite par Ethernet. J'exporte de cela un fichier qui ira ensuite sur une clé USB à insérer à la station, celle-ci pourra alors obtenir la configuration réalisée.

Après cela la station doit être branché en Ethernet afin d'être d'une part fonctionnel et identifiable sur le panel, l'on peut ainsi aisément configurer visuellement l'interface pour les utilisateurs comme rajouter un texte explicatifs et le logo de l'entreprise.

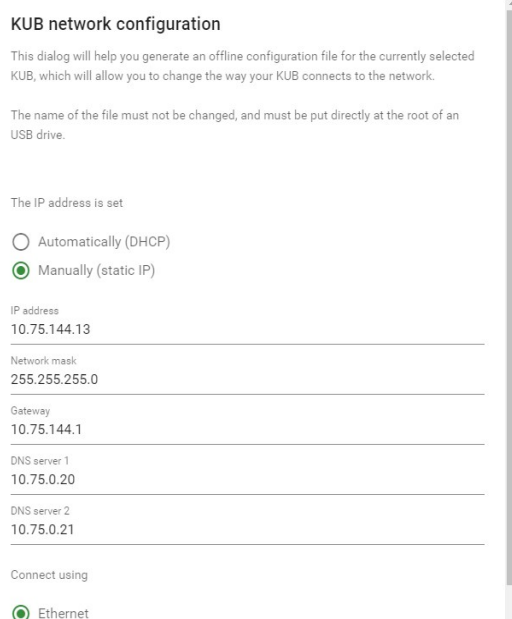
Cependant un problème se pose, celui de le configurer en Wi-Fi, il aura fallu plusieurs jours après de multiple échange avec le support afin d'obtenir une License permettant cette configuration, elle est similaire mais relativement plus longue, elle permet donc l'utilisation des stations sans utiliser de prise Ethernet. J'ai ainsi ajouté à la documentation comment les configurer (Annexe 6).

Enfin 6 nouvelles stations ont pu être configurées, la moitié seront installé au siège et l'autre moitié seront envoyé dans des sites distants tel que des usines. A la suite des installations dans le siège j'ai réorganisé l'inventaire des stations en créant un nouveaux plus organisé et simple contenue des mesures à prendre (Annexe 7). Celui-ci contient les informations sur les lieux, emplacements et état des stations, j'ai aussi du renseigner les anciennes stations afin de rendre le document complet et unique pour l'inventaire.

Ainsi je prends l'initiative de réaliser des affiches permettant aux employer de comprendre comment utiliser les stations. Je le réalise facilement via Word et le rend sobre afin de rendre compréhensible pour tous et toute le guide d'utilisation (Annexe 8). De plus je réalise deux messages visant à informer le personnel via l'intranet de l'entreprise ainsi que par mail (Annexe 9).

Afin que l'agent puisse être fonctionnel il faut déployer et mettre en place un agent sur les postes des utilisateurs, cet agent permet de vérifier la signature réaliser par la station et ainsi lui refuser ou lui autorisé l'accès, sans cela les bornes n'ont aucun intérêt. Un autre service est en charge de déployer directement sur les postes cette solution, je me serai simplement contenté d'informer les salariés de ce dont il s'agit et de quand cela sera mis en place.

Annexe 5 :



KUB network configuration

This dialog will help you generate an offline configuration file for the currently selected KUB, which will allow you to change the way your KUB connects to the network.

The name of the file must not be changed, and must be put directly at the root of an USB drive.

The IP address is set

☐ Automatically (DHCP)

☒ Manually (static IP)

IP address
10.75.144.13

Network mask
255.255.255.0

Gateway
10.75.144.1

DNS server 1
10.75.0.20

DNS server 2
10.75.0.21

Connect using

☒ Ethernet

Annexe 6 :

<p>Vous pouvez également la configurer en <u>wi-fi</u> de la manière suivante</p> <p>Sélectionner <u>wifi</u> et <u>dhcp</u></p> <p>Ajouter les DNS et spécifier le Wifi utilisé, activer le WPA2 entreprise</p>	<p>Connect using</p> <p><input type="radio"/> Ethernet</p> <p><input checked="" type="radio"/> Wi-Fi</p> <p><input type="radio"/> LTE Modem</p> <p>The IP address is set</p> <p><input checked="" type="radio"/> Automatically (DHCP)</p> <p><input type="radio"/> Manually (static IP)</p> <p>Hostname ("host-name" DHCP field) KUB</p> <p>DNS server 1 (empty to use DHCP DNS) [redacted]</p> <p>DNS server 2 (empty to use DHCP DNS) [redacted]</p> <p>Access point SSID [redacted]</p> <p>Security [redacted]</p> <p>Security</p> <p><input checked="" type="checkbox"/> Use 802.1X Authentication</p> <p>Authentication Secure EAP (PEAP)</p>
--	--

Annexe 6 :

<p>Spécifier l'utilisateur et le mot de passe (trouvable dans le coffre-fort)</p> <p>Bien spécifier l'utilisateur dans l'<u>Anonymous identity</u> et l'<u>Username</u></p> <p>Ajouter un certificat et générer le fichier de <u>conf</u></p>	<p>Authentication Secure EAP (PEAP)</p> <p>Anonymous identity User</p> <p>CA Certificate</p> <p>Click here to upload a CA certificate CANCEL</p> <p>Inner authentication MSCHAPv2</p> <p>Username User</p> <p>Password Indiquer le MDP</p>
---	---

Annexe 7 :

Numéro de sér	Inventair	Nom	Typ	Emplacement	Détails	Projet d'installatio
K-3000-191	19117	Satellite_M19_8	Satellite	Module 19 - Etage 8	Sud - Reprographie	Installé
K-3000-190	19118	Satellite_M19_4	Satellite	Module 19 - Etage 4	Nord - Reprographie	Installé
K-3000-192	19119	Satellite_M19_6	Satellite	Module 19 - Etage 6	Nord - Reprographie	Installé
K-3000-193	19120	Satellite_M19_2	Satellite	Module 19 - Etage 2	Nord - Reprographie	Installé
K-3000-189	19121	Satellite_???	Satellite	Stock		Remplacement à Berger
K-3000-194	19122	Satellite_Berger	Satellite	Berger - Etage 1	Au niveau de l'imprimante près des bureaux	HS à réparer
K-5000-445	???	Totem_Haxo	Totem	Haxo		Installé
K-5000-446	08859	Totem_???	Totem	Stock		Usine de Maillot
???	???	Totem_Hay-les-Roses	Totem	L'hay les roses		Installé
???	???	Totem_Joinville-BAT_Administrati	Totem	Usine de Joinville		Installé
K-5100-271	???	Totem_Joinville-BAT_ATELIER	Totem	Usine de Joinville		Installé
???	???	Totem_Labo	Totem	Laboratoire d'Ivry		Installé
K-5000-444	???	Totem_Montmartre	Totem	Montmartre		Installé
K-5000-447	???	Totem_Montreuil-Sur-Eure	Totem	Montreuil-Sur-Eure		Installé
???	???	Totem_Orly	Totem	Orly		Installé
K-5000-448	???	Totem_Pyrénées	Totem	Pyrénées		Installé
???	???	Totem_Saint-Cloud	Totem	Saint-Cloud		Installé
???	???	Totem_Sorques	Totem	Sorques		Installé
???	???	Totem_Wallace	Totem	Wallace - Etage 1	En face de l'atelier dans les bureaux	Installé

Conclusion

En conclusion ce stage m'a permis de découvrir les bases de la cyber sécurité en entreprise ainsi que le fonctionne de celle-ci dans le cadre technique et opérationnel. J'ai pu échanger et communiquer avec beaucoup de personnes différentes ainsi que développer et mettre en avant mes compétences acquissent au cours de cette année pour structurer et mettre en place un projet. J'ai sus donné suite à mon travail en l'accompagnement de taches annexes permettant une meilleure introduction de celui-ci et une meilleure compréhension de la part des salariés et de mes responsables. Cela fut enrichissant pour moi et me permettra à l'avenir de mieux comprendre toutes les fonctions d'un projet d'entreprise, d'une part l'ajout ou l'amélioration d'un système mais aussi son déploiement, la communication lié à celui-ci et les compétences qui requière d'autre services afin d'accomplir à bien une mission.