OPENCLASSROOMS

[redacted]

RAPPORT DE STAGE

Nom et prénom : **FAIVRE Mickaël**

Formation : **Technicien informatique**

Date de formation : **Juin 2023 — Mars 2024**

Abréviations

- **AD** : Active Directory
- **TCP/IP** : Transmission Control Protocol / Internet Protocol
- **DSI** : Direction des Systèmes d'Informations
- **SI** : Systèmes d'Informations
- **RSI** : Responsable des Systèmes d'Informations
- **MFA** : Multi-Factor Authentification
- **VoIP** : Voice Over Internet Protocol
- **VPN** : Virtual Private Network
- **PC** : Personnal Computer
- **PDF** : Portable Document Format
- **NAS** : Network Attached Storage
- **SAN** : Storage Area Network
- **GLPI** : Gestion Libre de Parc Informatique
- **RAID** : Redundant Array of Independent Disk
- **VM** : Virtual Machine
- **DNS** : Domain Name System
- **DHCP** : Dynamic Host Configuration Protocol
- **PVE** : Proxomox Virtual Environment
- **KVM** : Kernel-based Virtual Machine
- **PHP** : PHP Hypertext Preprocessor
- **IP** : Internet Protocol
- **URL** : Uniform Resource Locator
- **GPO** : Group POlicy
- **PSO** : Password Setting Objects
- **AGDLP** : Account, Global, Domain Local, Permissions
- **UO** : Unité Organisationnelle
- **VLAN** : Virtual Local Area Network
- **LAN** : Local Area Network
- **WAN** : Wide Area Network
- **WDS** : Windows Deployment Services
- **ITIL** : Information Technology Infrastructure Library
- **RGPD** : Règlement Général sur la Protection des Données
- **ANTS** : Agence Nationale des Titres Sécurisés
- **EFA** : Email Filter Appliance

Glossaire

- **Active Directory** : Annuaire de gestion des accès et des utilisateurs mis en place par Microsoft.
- **Domaine Active Directory** : Organisation regroupant des utilisateurs, de machines et des ressources sous un même ensemble ayant le même nom.
- **ITIL** : Ensemble de conseils relatifs à la gestion et à la bonne conduite d'un système d'information afin d'optimiser son fonctionnement et son organisation.
- **Script** : Programme informatique permettant de réaliser une tâche précise.
- **GPO ou Stratégie de sécurité** : Possibilité offerte par Active Directory afin d'appliquer des règles à un ensemble d'éléments.
- **Unité organisationnelle :** Élément d'un domaine permettant d'y ranger d'autres éléments (utilisateurs, machines) et d'éventuellement y appliquer des stratégies de sécurité.
- **Problème :** Incident répété qui nécessite de trouver une solution définitive.
- **Load balancing :** Répartition automatique de la charge entre plusieurs serveurs afin d'équilibrer la charge d'utilisation.
- **Cluster :** Groupe de serveurs, aussi appelé grappe, qui permet à plusieurs serveurs de travailler de façon synchrone.
- **Hyperviseur :** Logiciel ou système d'exploitation permettant de créer des machines virtuelles sur une machine physique hôte. Les ressources de l'hôte sont alors partagées virtuellement entre les différentes machines virtuelles.
- **Failover :** Basculement automatique d'un service sur un autre serveur en cas de panne.
- **Markdown :** Langage de balisage simple permettant la mise en page et la syntaxe d'un texte facilement.
- **Modèle OSI :** Norme de communication pour les appareils d'un réseau informatique. Il segmente la communication en plusieurs couches. Chaque couche ayant une fonction et une capacité bien définies.
- **L1 à L7 :** Diminutif de Layer (couche, en français). Fais référence aux différentes couches du modèle OSI. En réseau, nous parlons de L2 pour les switchs ne transmettant que des trames Ethernet et L3 pour les appareils capables de faire du routage.
- **Switch :** Aussi appelé commutateur réseau. Relie plusieurs câbles (RJ45 ou fibre) et propage les trames Ethernet sur ses différents ports. Il en existe deux types : L2, ne transmet que les trames Ethernet. L3, capable de router les paquets IP.
- **Routeur :** Appareil pouvant transmettre les paquets IP à d'autres appareils identifiés sur le réseau.
- **Bruteforce :** Méthode consistant à essayer de milliers de mots de passe en quelques secondes dans l'espoir de trouver celui utilisé par un service ou un utilisateur.

Table des matières

1 — Introduction

Mon stage s'est effectué au sein de [redacted] (1) durant la période du 27/11/2023 au 23/02/2024. Cette entreprise est intéressante de par la diversité des missions effectuées au sein de sa DSI. Nous couvrons ainsi le bon fonctionnement de l'ensemble des services absolument essentiels pour que [redacted] se passe au mieux. Outre ces missions cruciales, le SI propose également un support aux utilisateurs afin de les former sur l'outil informatique. Que ce soit pour l'usage dans leurs vies quotidiennes ou afin de faire leurs démarches en ligne [redacted] Pour terminer, les utilisateurs peuvent également être accompagnés dans un « point Cyber » qui met à leur disposition une connexion internet fibrée, des ordinateurs portables et une imprimante en réseau.

J'ai souhaité rejoindre cette entreprise justement pour la variété de ces missions, mais aussi afin d'avoir un poste qui a un réel impact sur la vie des utilisateurs. Le SI étant omniprésent dans l'administration, si un service est impacté par une panne, cela a de graves conséquences. [redacted]

De plus, [redacted] est réputée pour ce « point Cyber » et la qualité des formateurs. Le RSI est également la personne qui a mis en place l'ensemble des serveurs et du réseau. Il connait ainsi parfaitement son fonctionnement et son architecture, ce qui me permet de pouvoir avoir des informations de première main quant à la configuration du SI.

Les missions demandées lors de ce stage consisteront à apporter un support aux employés [redacted] qui pourraient rencontrer des problèmes liés à la SI, animer des cours afin de former les usagers pour qu'ils puissent être autonomes sur un ordinateur ou les aider lors de leurs démarches administratives en ligne.

J'ai également proposé plusieurs idées afin d'améliorer la qualité des services proposés aux utilisateurs, tout comme j'ai suggéré des solutions afin de résoudre les problèmes que le service prouvait rencontrer dans son fonctionnement quotidien.

J'ai donc souhaité apporter des solutions techniques afin d'automatiser l'inventaire du parc informatique, qui jusqu'à présent était fait manuellement. Il m'a semblé également pertinent de proposer l'utilisation d'un gestionnaire de mot de passe, voire l'usage de la MFA, ce qui permettrait de sécuriser davantage le réseau de la collectivité à travers une identification renforcée par le biais de mots de passe fort ou d'une double authentification.

La fulgurante augmentation des cyber attaques tournées contre les [redacted] est un sujet critique (2). Il est inenvisageable qu'une [redacted] puisse être paralysée suite à une attaque ou que les données personnelles et confidentielles des [redacted] puissent se retrouver en vente sur le dark web.

Ainsi, la sécurité du système d'information et l'amélioration de son utilisation seront les maitres mots de mon stage. Soucieux d'apporter de nouvelles idées et les compétences acquises lors de ma formation, à travers l'ensemble des projets.

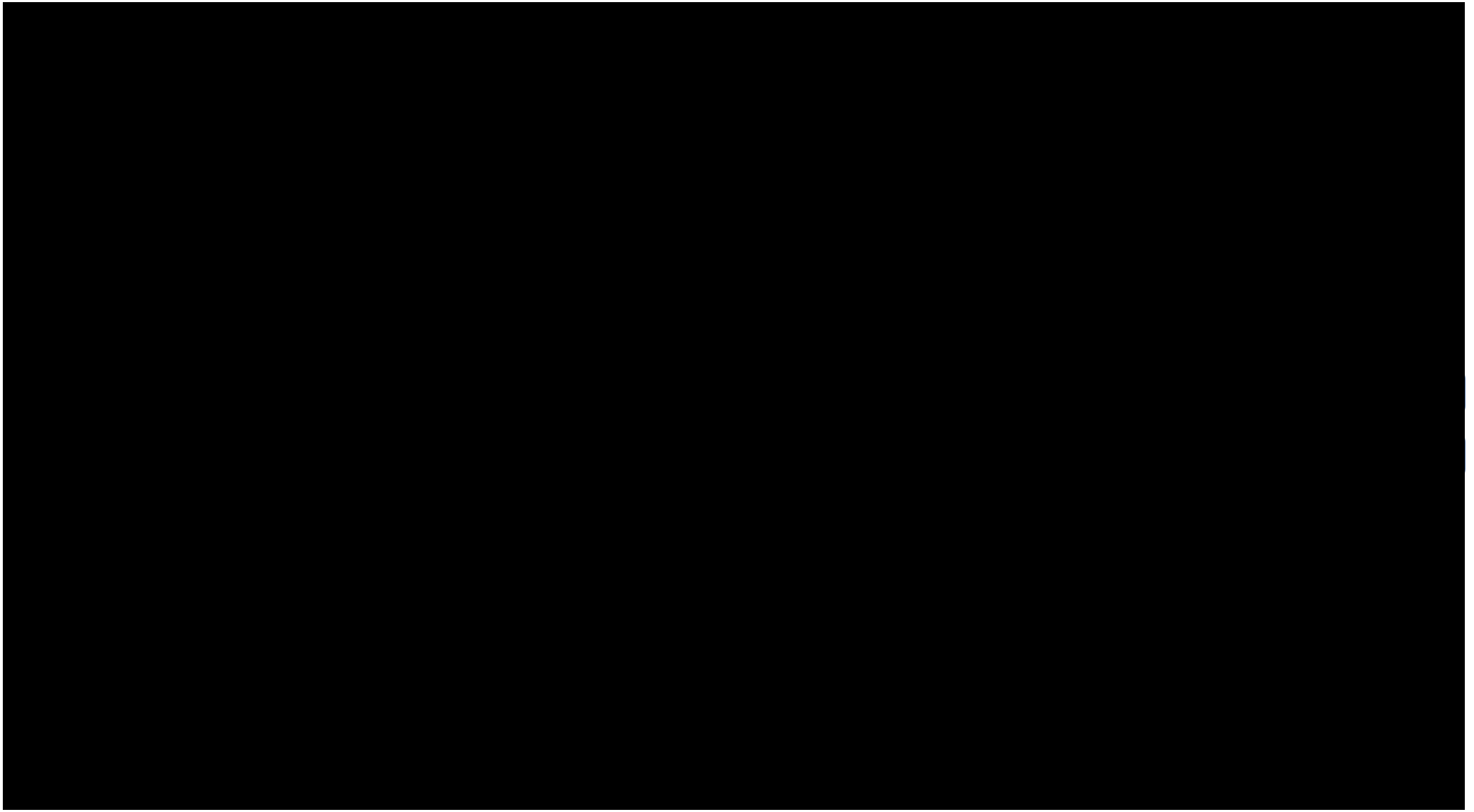
1.1 - Présentation entreprise :

[redacted]

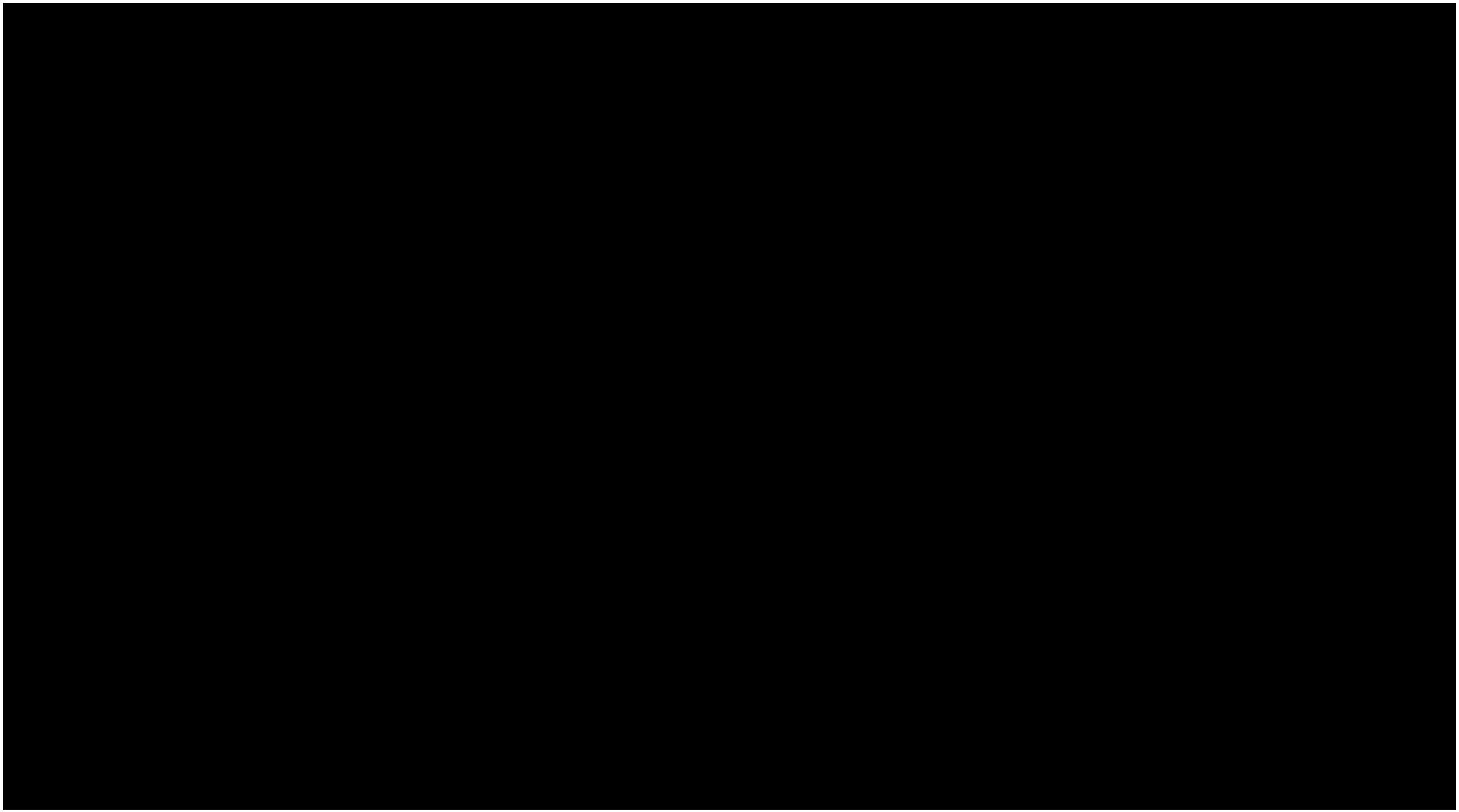
[redacted]

[redacted]

[redacted]



1.3 - Organigramme du système d'information



1.4 - Mission du service et missions personnelles :

La mission principale du service informatique est d'installer et de maintenir le parc informatique présent dans l'ensemble de la [redacted].

Cela peut aller de la configuration d'une imprimante dans un service de [redacted] à l'installation d'une nouvelle salle en vue d'une augmentation des effectifs.

Les locaux principaux étant actuellement en travaux, il est aussi nécessaire de déplacer des services entiers vers de nouveaux bureaux. Cela demande de réinstaller les postes utilisateurs, les téléphones VoIP et les imprimantes, mais ça nécessite aussi de refaire la connexion des câbles RJ45 du réseau.

En tant que stagiaire, mes missions principales sont, dans un premier temps, de me renseigner sur l'infrastructure du réseau et la configuration des différents services proposés aux utilisateurs (Active Directory, partage de fichiers, VPN, etc.).

Une fois cette première étape terminée, il m'est demandé d'apporter mon aide aux différents salariés de [redacted], mais aussi de faire des cours aux administrés qui souhaitent apprendre à mieux maitriser l'outil informatique.

Il y a également un inventaire à gérer concernant les PC portables qui peuvent être utilisés par les [redacted] qui se présentent au « point Cyber » : vérifier que les PC possèdent bien le chargeur adapté, qu'une souris est présente, les inventorier en cas de matériel absent et gérer les mises à jour des différents systèmes d'exploitation (les PC de prêt étant sous Windows 10 ou Windows 11).

1.5 — Présentation mission :

La DSI s'occupe principalement du support utilisateur des personnes travaillant dans les différents services de [redacted]. Nous nous occupons aussi de l'installation de nouveau poste client ou lors des besoins de visioconférence pour les [redacted].

En plus de cela, la mairie étant en pleins travaux de rénovation, nous devons aussi gérer l'installation des nouveaux bureaux et de l'espace ouvert à tous nommé « point Cyber ». Dans cet espace, nous avons dû installer de nouvelles tables, de nouveaux bureaux, de nouveaux écrans tactiles qui servent à diffuser du contenu destiné aux [redacted]. Ces écrans tactiles servent également pour afficher en très grands des PDF ou des images afin d'illustrer les cours d'informatique qui sont donnés aux personnes qui le souhaite.

1.6 — Contexte :

La DSI est composée de trois personnes à temps plein.

Un RSI, responsable du système d'information, travaillant à [redacted] depuis plus de 20 ans. Ce dernier [redacted] pendant des années, puis a évolué pour devenir RSI lors de la transition vers le numérique entamé par [redacted] il y a plusieurs années.

À ses côtés, il y a deux [redacted], issus de la campagne faite par le gouvernement afin de créer un véritable accompagnement, dans les [redacted], pour les usagers devant s'adapter au fait que l'ensemble des services de l'État (passeport, carte grise, impôts, etc.) sont dorénavant disponibles sur internet. Le but premier étant d'accompagner les personnes vers une autonomie numérique, les [redacted] ne sont pas des techniciens spécialisés dans la gestion et l'administration d'un parc informatique.

[redacted]

À savoir que [redacted] accepte beaucoup de stagiaires. Il est donc assez courant de devoir créer de nouveaux comptes sur le serveur Active Directory avec des accès restreints.

L'ensemble des données qui transitent dans les bureaux et est stockée sur les serveurs sont sensibles, car personnelles et destinées à [redacted]. Les données sont stockées sur trois serveurs NAS différents. Deux de ses serveurs sont dans les [redacted], dans la même baie serveur. Le troisième serveur est lui installé dans les locaux de [redacted].

Lors des interventions dans les locaux de [redacted], il est très courant qu'un [redacted] soit en rendez-vous. Il est donc fondamental de savoir rester discret et d'intervenir de façon transparente, sans devenir une gêne pour la personne.

1.7 — Technologies utilisées :

1.7.1 — Serveurs :

Je vais diviser les technologies utilisées au sein de [redacted] en trois parties distinctes. Cette découpe sera une simplification du modèle OSI afin de présenter l'essentiel du matériel et logiciel.

Par la suite je vais détailler l'architecture de chaque couche.

- **Couche physique :** Cette couche comprend les câbles, switch, routeur, serveur physique, prise RJ45, imprimantes, etc.
- **Couche système :** Mets les ressources des couches physiques à disposition des applications
- **Couche applicative :** Mets les différents services à disposition des utilisateurs

Présentation de l'architecture globale de [redacted]

Couche applicative	Active Directory, TSE, serveur de fichiers, Suite office, applications métiers, …	Rôles Windows, logiciels, …
Couche système	Windows, Linux	Système d'exploitation
	Proxmox	Virtualisation
Couche physique	Serveurs — Ressources à mutualiser	
	SAN — Stockage des données	Disques durs, SSD
	LAN — Liaison des données	Câbles téléphone, fibre optique, switch, routeur, firewall

1 — Présentation de proxmox

Proxmox est un hyperviseur de type 1. C'est-à-dire que celui-ci se substitue au système d'exploitation. Cela permet de laisser une plus grande part des ressources matérielles disponibles aux futures machines virtuelles qui seront installées.

Voici quelques fonctionnalités disponibles (4) :

- **QEMU :** Pour Quick EMUlation. Permets de paravirtualiser certains composants d'une machine virtuelle afin d'améliorer les performances de la VM sans avoir à modifier le système d'exploitation émulé, contrairement à d'autres méthodes de paravirtualisation.
- **Proxmox VE Cluster Manager :** Cela permet de mutualiser les ressources des trois serveurs présents dans la baie serveur et d'apporter une plus grande résilience aux différents systèmes installés sur l'hyperviseur.

- **Pile logicielle « ha-manager » :** Supervise la haute disponibilité. Celle-ci gère automatiquement les erreurs qui peuvent se présenter sur un serveur et propose un failover afin de pouvoir basculer, si le logiciel n'arrive à redémarrer le service en défaut, sur un second serveur virtuel du cluster.
- **Backup/Restore :** Sauvegarde et restauration des données qui prend en compte la bande passante de stockage disponible ainsi que la protection des dossiers qui peuvent être marque comme « protégé » afin d'éviter une suppression accidentelle. Elles peuvent être automatisées et/ou faites manuellement.
- **Ceph :** Permets, sur un même nœud physique, de faire du stockage répliqué et d'avoir les machines virtuelles.

2 — Présentation SAN

Le SAN (Stockage Area Network) met à disposition un espace de stockage massif sur le réseau LAN. Cet espace peut être composé de plusieurs types de disques (lents, rapides …) selon les besoins. Ainsi, les disques de backup pourront être plus lents, le backup se faisant sur une plage horaire hors de celle de travail. Le temps n'est pas une contrainte dans ce cas précis.

À contrario, les disques utilisés pour le stockage du partage de fichiers seront des disques rapides, les utilisateurs ayant besoin de pouvoir interagir avec les données de façon rapide.

Avoir des disques lents pour le backup permet également une réduction des couts non négligeables, les disques rapides étant plus chers à l'achat. Une bonne répartition du type de disque est donc nécessaire et cela doit se réfléchir en amont, avant l'installation des serveurs physiques. Cela afin d'optimiser le coût d'installation et de maintenance et le d'avoir un système adapté aux besoins de l'entreprise.

3 — Cluster :

La grappe serveur est composée de trois serveurs (nœuds) ayant des configurations identiques :

[redacted]

Proxmox se charge de répartir la charge (load-balancing) entre les différents nœuds de la grappe tout comme il se charge de répartir les services en cas de perte d'un nœud de la grappe.

Les services présents sont les suivants :

[redacted]

4 - Sécurité

Deux firewalls logiciels sont en place. Il s'agit du logiciel OPNsense, qui est une version open-source et gratuite de pfsense. Un premier firewall s'occupe du filtrage des accès vers [redacted] quand le second se charge du filtrage des accès extérieurs.

Les mises à jour du serveur se font manuellement, lorsque les horaires de bureau sont terminés. Cela évite d'impacter le travail des [redacted] sur place. Ces mises à jour sont gérées directement par le responsable du SI.

Les mises à jour des postes utilisateurs n'ont aucune gestion et se font au cas par cas, automatiquement, par le système d'exploitation de la machine. Bien que cela ait déjà posé problème : des [redacted] se sont retrouvés dans l'incapacité de travailler suite à de grosses mises à jour, le responsable ne juge pas utile de mettre en place un serveur WSUS pour optimiser cela.

1.7.2 — Parc utilisateur

1 — Matériel

Le parc informatique des utilisateurs est relativement vari. Suite à la pandémie de COVID-19 et aux confinements ayant été mis en place à l'époque, la plupart des services ont été obligés de passer au télétravail. Par conséquent, beaucoup d'utilisateurs ont des ordinateurs portables.

Il faut également ajouter des services, comme [redacted] est nomade et que les déplacements sont très courants dans leur secteur. Essentiellement pour se rendre dans [redacted].

Tous les ordinateurs portables des [redacted] sont de marques ASUS, mélangeant les modèles ExpertBook [redacted].

D'autres services, notamment les [redacted], ne sont pas compatibles avec le télétravail. Ces postes sont des ordinateurs fixes. Il n'y a aucune marque dominante parmi l'ensemble des postes présents. Ceux-ci étant montés par une tierce entreprise qui les vend ensuite, montés[redacted].

Cela dépend aussi du besoin des postes. Quand une puissance de calcul supérieure à la moyenne est requise pour le travail de l'[redacted] (la création d'affiches via Photoshop, par exemple), alors la machine proposée est proportionnée aux besoins.

Depuis plusieurs mois maintenant, les postes de travail sont petit à petit migrés sur des disques de stockages SSD. Mais cela peut se faire uniquement quand l'agent n'est pas présent sur son poste, afin de ne pas impacter son travail.

Pour la copie des disques et des partitions, nous utilisions le logiciel Paragon Hard Disk Manager. Ce logiciel permet de faire de copie de partitions de tailles différentes. Ce qui nous permet de faire une copie d'un disque HDD de 1To vers un disque SSD de 240Go. L'unique prérequis est que le volume des données présent ne doivent pas dépasser la taille de la partition du disque receveur.

Mais cela ne pose jamais problème. Le partage de fichiers et le serveur Active-Directory sont configurés de telle manière que toutes personnes se connectant à sa session voient ses données enregistrées directement sur le serveur et non sur l'ordinateur local. Les disques locaux ne sont donc que très rarement sollicités.

2 — Logiciel

La suite Office (Word, Excel, etc.) est présente sur l'ensemble des postes utilisateurs. La gestion des licences se fait par nos soins, directement sur l'interface administrateur Web de Microsoft.

Nous possédons des licences basiques et des licences business. La principale différence est l'accès complet à la suite Office, à la possibilité d'avoir un compte Exchange d'entreprise et de pouvoir installer Teams pour l'entreprise.

Noter que Teams est quotidiennement utilisé pour les échanges entre les services ou les échanges informels entre les [redacted]. Il est venu remplacer mattermost que le personnel ne trouvait pas suffisamment ergonomique.

Teams sert aussi pour les visioconférences, que ce soit en interne ([redacted] disposant de services qui ne sont pas tous localisés au même endroit) ou externe. Il arrive très régulièrement que le service des ressources humaines procède à des visioconférences pour des entretiens d'embauche. [redacted] en ont également besoin pour communiquer avec des [redacted]. Si je prends l'exemple des budgets, ils sont définis par [redacted] et c'est ensuite par visioconférence avec les [redacted] que les fonds sont attribués aux services en ayant besoin.

Exchange a été choisi comme solution mail étant donné que le service est directement intégré dans l'environnement Microsoft. Nous avons une cohérence entre les services et les logiciels utilisés. Cette cohérence et l'uniformité dans l'ergonomie des différents logiciels permettent aux utilisateurs de s'y retrouver plus facilement et de prendre des habitudes d'usage.

La configuration des mails professionnels de [redacted] se fait en jonction avec un serveur mail local. Le fait de passer par un serveur Exchange permet de libérer du temps au responsable qui n'a ainsi pas besoin de se préoccuper de la configuration du serveur mail et de la réputation de notre adresse IP publique.

La configuration d'un mail auto-hébergé peut-être très chronophage (5) et poser de très nombreux problèmes. Si un fournisseur mail (Gmail, Laposte, etc.) décide unilatéralement que notre configuration mail et/ou que la réputation de notre adresse IP publique n'est pas assez bonne, alors les mails envoyés par [redacted] peuvent se retrouver bloqués ou être envoyés dans les spams sans raison valable.

Nous créons donc un mail sur les serveurs Exchange de Microsoft et nous faisons ensuite une redirection vers le mail créé en local sur nos serveurs. Un mail envoyé fait donc un rebond entre notre serveur mail, est envoyé vers le serveur Exchange et est ensuite envoyé au destinataire final. Dans le cas de la réception d'un mail, le principe est exactement le même, mais en sens inverse.

Le serveur Exchange change l'entête du mail afin de remplacer les parties (IP, DKIM, SPF, etc.) qui pourraient poser problème si les entêtes d'origine lui semblaient suspects.

3 – Support utilisateur

Les utilisateurs disposent de trois moyens principaux pour nous signaler un problème :

1 GLPI
2 Téléphone
3 Contact direct (oralement)

Le plus souvent, ce sont les tickets GLPI qui sont utilisés. Bien que cela puisse dépendre du problème rencontré et de son urgence. Effectivement, il est courant que les utilisateurs rencontrant un grave problème viennent plutôt nous voir directement plutôt que d'ouvrir un ticket.

Pour les aider, nous prenons généralement la main à distance grâce au logiciel Anydesk. Mais quand il s'agit d'une intervention dans des services géographiquement proches, nous n'hésitons pas à intervenir physiquement sur la machine. Il nous arrive aussi de devoir intervenir par téléphone, tout en ayant pris la main à distance pour éviter que les utilisateurs interviennent durant le dépannage. De plus, cela peut les rassurer de nous avoir au téléphone pendant que nous intervenons. Le fait de leur expliquer les étapes de dépannage fait aussi en sorte qu'en cas de problème similaire, l'utilisateur saura comment corriger le souci. Bien que cela dépende essentiellement du niveau de panne rencontré.

Nous faisons très peu de formation des utilisateurs sur leurs logiciels métiers, ces derniers existant depuis de très nombreuses années. Néanmoins, nous les formons quand de nouveaux services sont mis en place ou que de nouveaux appareils sont branchés.

Généralement, la formation se fait en présentiel : nous expliquons et montrons le fonctionnement devant [redacted]. Un document au format papier ou PDF est également mis à leur disposition pour éviter les oublis et les erreurs. Le document papier est remis au directeur de service et est en libre accès pour les agents dudit service. Le PDF est quant à lui disponible sur le serveur de fichiers [redacted] afin que n'importe qui puisse y accéder en cas de problème ou de besoin.

A noter qu'il n'existe pas de charte informatique dans [redacted]. Le responsable n'en voyant pas nécessairement le besoin.

4 - Sécurité

Les postes utilisateurs sont protégés par Windows Defender. Ce dernier étant nativement présent sous Windows, cela nous évite de devoir déployer des logiciels additionnels sur le parc.

Les utilisateurs n'interviennent que très rarement pour des problèmes de sécurité. Leurs comptes n'ayant pas les droits requis pour l'installation de nouveaux logiciels, nous devons intervenir nous-même pour qu'un nouveau logiciel soit installé.

Malheureusement, aucune GPO n'existe sur le serveur AD de [redacted]. Il n'y a donc aucune restriction sur l'utilisation des ports amovibles, par exemple.

1.8 — Formulation du besoin :

Les services [redacted] dépendent de notre SI et les servies [redacted] sont essentiels au bon fonctionnement [redacted]. Par conséquent, les services se doivent d'être sécurisés et d'avoir un taux de disponibilité élevé.

Toute lenteur sur un service impactera nécessairement la qualité de vie [redacted].

Cela requiert donc d'avoir un service réactif et d'anticiper les éventuels pannes et problèmes.

Sur la partie serveur, nous devons donc procéder à un moniroting régulier et proactif des services informatiques afin de déceler une faiblesse matérielle sur un serveur qui pourrait se transformer en panne. Nous devons également faire une veille importante sur les mises à jour logiciel et se renseigner de l'impact qu'elles pourraient avoir sur le bon fonctionnement des services du SI.

Quant à la partie poste utilisateur, nous devons être attentifs aux demandes [redacted] qui rencontreraient des lenteurs ou des problèmes afin d'être surs que cela n'est pas le signe avant-coureur d'une panne matériel.

Nous anticipons également les pannes et autres problèmes en remplaçant régulièrement le matériel qui devient obsolète.

1.9 — Cadrage de la mission :

1.9.1 Enjeux

Nous devons impérativement maintenir un SI fonctionnel malgré la diversité des usages [redacted] dus aux différents services présents [redacted] et en externe. Nous devons également veiller à la sécurité des données ainsi qu'à leur sauvegarde tout comme nous devons sécuriser les serveurs afin de nous prémunir contre toute attaque cyber.

En cas de problème, dû à une attaque ou à une panne généralisée, l'ensemble de [redacted] serait paralysée, ce qui n'est pas envisageable.

1.9.2 — Planning

Le planning peut varier en fonction du service, mais les horaires d'ouverture de la mairie au public sont les suivants :

[redacted]

[redacted]

[redacted]

[redacted]

1.9.3 — Effectifs de la DSI

La DSI est composée d'un responsable et de deux [redacted]. Durant un an, ils sont également accompagnés d'un alternant en BTS RISC (Réseaux Informatiques et Systèmes Communicants).

Il arrive très régulièrement que des stagiaires, de différents niveaux, intègrent l'équipe. Les stages peuvent soient être d'une durée de quelques semaines pour les étudiants en BAC pro ou en BTS ou de plusieurs mois dans le cas d'un étudiant faisant une formation professionnalisante.

1.9.4 — Budget

Généralement, le budget annuel du SI est de 25 000€ HT.

Une enveloppe fixe de 10 000€ HT est prévue chaque année, mais n'est pas suffisante pour subvenir aux besoins imprévus : pannes, casse matérielle, etc. C'est pourquoi cette première enveloppe est souvent sous-dimensionnée et que le budget annuel est plutôt de 25 000€ HT.

Exceptionnellement, pour l'année 2023-2024, le budget du SI était de 93 000€ HT, essentiellement dû aux travaux de rénovation et à la modernisation de la salle : ajout d'écrans connectés pour les cours, rénovation totale de la salle, installation d'une baie dans la salle connectée.

2 — Projets :

2.1 — Projet 1 :

Il m'a été demandé de réfléchir à une évolution du serveur GLPI afin de le mettre à jour et de permettre une remontée automatique des postes clients présents sur le domaine de [redacted].

Pour mener à bien ce projet, un serveur de la baie informatique a été mis à ma disposition. C'est un serveur Primergy RX100 S7 qui dispose d'un RAID matériel. Le serveur ayant été totalement remis à neuf pour l'occasion, j'ai dû, dans un premier temps, reconfigurer le RAID en créant une nouvelle grappe de disques et de nouveaux disques logiques. Il m'a fallu également configurer l'interface réseau du serveur afin de pouvoir y brancher mon ordinateur portable.

Une fois cette première manipulation faite, j'ai installé un hyperviseur de type 1 – Proxmox VE – ce qui me permettra de mutualiser les ressources du serveur et d'installer l'ensemble des VM dont j'ai besoin sur un seul et même serveur physique. Il m'a fallu également configurer une nouvelle carte réseau virtuelle sur Proxmox VE afin que l'ensemble des VM puissent communiquer entre elles, tout en étant isolées du reste du réseau de la mairie.

L'hyperviseur installé, j'ai mis en place une VM Debian qui servira de serveur Web pour accueillir GLPI.

Avant d'installer Apache2, j'ai reconfiguré l'interface réseau de la distribution afin qu'elle puisse communiquer avec PVE et l'ensemble des VM qui y seront présentes. Ensuite j'ai installé Apache2, MySQL et PHP et tous les paquets nécessaires au bon fonctionnement de GLPI.

GLPI étant pleinement fonctionnel et configuré, je suis passé à l'installation d'une seconde VM qui permettra d'accueillir Windows Server 2022. Cette machine sera le contrôleur de domaine de test et servira également de serveur DNS et DHCP. Afin de faciliter l'installation des logiciels et de rendre l'ensemble de l'installation plus réaliste, le partage de fichiers a été configuré.

DHCP fournira les IP pour les machines du domaine via la configuration d'une étendue primaire avec la plage IP 10.10.0.0/24.

DNS me permettra de configurer une entrée de type A, pour pouvoir accéder à GLPI via une URL, sans avoir à taper une adresse IP.

Pour automatiser la remontée des ordinateurs du domaine dans l'inventaire de GLPI, j'ai décidé passer par une GPO qui sera effective sur l'ensemble du domaine.

L'agent GLPI étant au format .msi, il m'a fallu configurer la GPO afin d'exécuter « msiexec.exe » au démarrage des postes client en ajoutant les paramètres en ligne de commande pour que l'agent se configure correctement pour communiquer avec le serveur situé sur la VM Debian.

Dans l'idée de faire un projet qui se rapproche au maximum de la réalité et des objectifs de sécurité requis dans un environnement de production, plusieurs UO ont été créés dans l'AD et les groupes globaux et locaux ont été mis en place en respectant les principes d'ADGLP (6).

L'utilisateur de test que j'ai créé a donc été ajouté à une UO « DSI », enfant de l'UO « [redacted] ». L'UO « DSI » contient un groupe global nommé « GG_DSI ». Ce groupe global est membre de deux groupes locaux :

« GLP_DSI_RO » et « GLP_DSI_RW », ces groupes étant ceux qui disposeront des droits de lecture seule ou d'écriture dans l'ensemble des fichiers de partages. L'utilisateur de test a donc seulement été ajouté au groupe global.

Ce projet n'aura pas dépassé le stade de test dû à la trop courte durée de mon stage.

Une application dans les conditions réelles n'aurait pas été possible en l'état actuel du serveur AD, ce dernier ne possédant aucune UO. Un déploiement par GPO lié directement à la racine du domaine aurait impliqué que toutes les machines du domaine, y compris les serveurs, se voient touchées par le déploiement. Or, à des fins de sécurité, il est préférable de ne pas installer des logiciels non nécessaires sur un serveur.

Pour pallier à ce problème, il aurait fallu créer des UO sur le serveur AD, ce qui n'est pas possible sans l'approbation de tous les directeurs de service. Une réunion est bien prévue à cet effet, mais elle n'aura lieu qu'au milieu du mois de mars. Mon stage se terminant fin février, il est trop tard pour que je puisse y participer.

2.2 — Projet 2 :

Le point Cyber ouvert [redacted] ayant besoin d'un ordinateur ou d'une connexion internet ne disposait pas d'imprimante leur permettant de pouvoir repartir avec leurs documents personnels.

Au lieu de pouvoir simplement imprimer les documents, il fallait les envoyer par mail à l'ordinateur du secrétariat afin de pouvoir les sortir sur une imprimante du domaine.

Pour pallier ce problème et rendre l'impression plus facile, j'ai procédé à l'installation et à la configuration d'une distribution Debian sur un ordinateur portable dédié uniquement à cette tâche.

J'ai utilisé le serveur d'impression Cups ainsi que les pilotes libres proposés par HP. Afin de pouvoir maintenir et dépanner le serveur sans avoir besoin de se rendre sur le PC serveur, j'ai configuré un serveur SSH sur l'ordinateur portable pour pouvoir prendre la main à distance. Les accès SSH et à l'espace admin du serveur d'impression sont restreints par un couple login/mot de passe.

J'ai récupéré un vieil ordinateur portable qui n'avait plus aucune utilité dans les locaux de la DSI. Après avoir essayé à de nombreuses reprises à configurer une imprimante partagée sur le système d'exploitation en place sur le PC (Windows 10), j'ai très vite rencontré un problème.

L'imprimante était visible sur le réseau, mais lorsqu'un utilisateur voulait s'en servir pour imprimer un document, l'erreur suivante apparaissait : « Impossible de terminer cette opération (erreur 0x00000709). Vérifiez que le nom de l'imprimante est correct ou que l'imprimante est connectée au réseau. » (7). D'après mes recherches, il s'agit d'une erreur courante et d'un bug répertorié par Microsoft lorsque l'on souhaite partager une imprimante en réseau. Diverses solutions sont proposées afin de corriger ce bug. Allant de la modification du registre du système d'exploitation à la modification des GPO locales de l'ordinateur. S'agissant d'un vieil ordinateur qui n'était plus utilisé depuis des années

par la DSI et après avoir essayé l'ensemble des solutions proposées sans succès, j'ai soumis l'idée de changer le système d'exploitation afin de contourner le problème rencontré par Windows.

Bien entendu, j'ai pris soin de vérifier si ce dernier contenait des documents personnels et/ou importants avant de supprimer le système d'exploitation en place. Quand j'ai constaté que rien d'important ne persistait le PC, j'ai procédé à l'installation d'une distribution GNU/Linux (Debian 12) via l'utilisation d'une clé USB bootable (8).

Le serveur d'impression ne sera disponible que pour les PC connectés au point d'accès wifi dédié au point Cyber.

Pour installer un serveur d'impression, j'ai procédé à une mise à jour complète du système via la commande :

```
sudo apt-get update &&  apt-get updgrade
```

Une fois le système mis à jour, j'ai ensuite installé les paquets nécessaires au bon fonctionnement de l'imprimante partagée : cups – sera le serveur d'impression, qui propose une interface web pour la configuration. hplip — qui contient les pilotes, développés par HP, qui sont obligatoires pour faire fonctionner l'imprimante.

```
sudo apt-get install -y hplip cups
```

Il a ensuite fallu installer, via l'interface Web de cups, renommer l'imprimante explicitement et lui attribuer les pilotes dédiés.

Quand le serveur d'impression est entièrement fonctionnel, je suis passé à la configuration des postes utilisateurs afin d'installer la bonne imprimante réseau. Cela se fait en passant par les paramètres de Windows, dans le menu « Bluetooth et appareils » puis « Imprimantes et scanneur ». En cliquant sur « Ajouter un appareil », l'imprimante apparait. En cliquant sur « Ajouter », cette dernière s'installe automatiquement.

Ainsi, chaque utilisateur du point cyber de la mairie peut imprimer des documents personnels, sans avoir besoin de l'intervention d'un technicien informatique ou d'un conseiller numérique. Cela ajoute également un service extrêmement utile pour l'ensemble des administrés. À noter que durant les deux premières semaines de mon stage, un nombre conséquent de personnes ont demandé à ce qu'une impression soit disponible. Leur permettant ainsi d'acquérir une plus grande autonomie et de ne plus dépendre d'un membre de la famille ou d'un magasin possédant une imprimante pour avoir une version physique de leur document personnel et/ou administratif.

2.3 — Projet 3 :

Ce projet concerne les ordinateurs du « point Cyber » qui sont mis à disposition des [redacted] le souhaitant.

Ces ordinateurs sont de marque ASUS, modèle ExpertBook 1500. Ce sont donc des ordinateurs assez récents qui peuvent suffire dans la plupart des besoins nomades (navigation, bureautique, etc.).

Deux ordinateurs sont disponibles en permanence et réservés [redacted]. Pour s'en servir, les utilisateurs peuvent soit réserver un créneau horaire depuis le site de la mairie, soit venir à l'improviste.

Au début de mon stage, il n'existait que très peu de restrictions quant à la durée d'utilisation. Alors que le règlement intérieur limitait explicitement la durée des sessions à une heure. Si un usager souhaitait rester deux heures, techniquement, rien ne l'en empêchait. Quand bien même cela allait à l'encontre du règlement. Point de vue restriction d'usage, les sessions se font sur un compte local de l'ordinateur, avec un niveau simple utilisateur. Des limitations ont été mises en place via les GPO locales : les ports USB sont bloqués, l'accès au gestionnaire de tâche est interdit, tout comme l'accès aux paramètres de l'ordinateur.

Il m'a été demandé de mettre en place, sans contrainte sur la méthode employée, une limitation de durée afin que les sessions démarrées avec le compte spécifiquement créé pour les usagers du « point Cyber » soient automatiquement coupées au bout de 60 minutes.

Afin que mon projet soit le plus adapté à l'usage fait en mairie et au fonctionnement actuellement mis en place, je me suis renseigné auprès des [redacted] et du secrétariat de l'accueil afin de connaitre leurs méthodes actuelles :

- Comment les usagers ont-ils accès au règlement intérieur du « point Cyber » ?
- Doivent-ils renseigner des informations personnelles avant de pouvoir utiliser un ordinateur ?
- Ces informations sont-elles obligatoires ?
- Les informations personnelles données servent-elles à générer des statistiques ?
- Comment sont gérées ses statistiques ?
- Ses statistiques sont-elles uniquement à usage interne ?

Ceci m'a permis de cibler très précisément les attentes et les besoins nécessaires à ce projet et de pouvoir également adapter mon travail aux différentes contraintes et de savoir quels seraient les moyens que j'allais utiliser pour parvenir à mes fins.

Actuellement, pour accéder à un ordinateur du « point Cyber » les usagers doivent se présenter à l'accueil général de la mairie. La secrétaire leur donnera une fiche d'informations à remplir ainsi qu'une copie du règlement intérieur. Les informations demandées sont : nom, prénom, adresse, âge.

Ce n'est qu'une fois cette fiche papier complétée que les usagers peuvent se connecter sur un ordinateur de prêt.

Après en avoir discuté avec mon tuteur de stage, [redacted], j'ai pu constater que la fiche d'informations actuellement en place ne correspond plus réellement à leurs besoins. En effet, les [redacted] doivent transmettre ces informations à [redacted], via la plateforme développée [redacted], afin que des statistiques nationales soient effectuées. Or, les informations demandées par [redacted] ne correspondent pas à celles présentes sur la fiche papier actuellement présentée aux usagers. Il est donc évident que la fiche d'informations doit être mise à jour pour que les statistiques soient justes.

Les [redacted] souhaitent aussi, à partir des informations collectées dans cette fiche, générer des statistiques internes afin de se faire une idée des besoins de la population et de l'évolution des usages. Ils peuvent également ajuster le budget en fonction du nombre d'administrés passant par le « point Cyber ».

À la suite de mon enquête, il s'avère que ces informations doivent obligatoirement être collectées à chaque nouvelle session et que les données doivent être stockées un an durant (les statistiques internes se faisant annuellement).

Comme nous pouvons le constater, la méthode actuelle peut s'avérer terriblement chronophage : une secrétaire donne une fiche à remplir. L'usager remplit la fiche. Une seconde secrétaire est chargée, chaque année, de reprendre les fiches une par une pour les saisir dans un tableur excel. Les [redacted] doivent saisir manuellement les informations sur le site des [redacted]. Il peut s'avérer parfois difficile de relire les personnes.

Suite à ce constat, il m'a semblé essentiel de réfléchir à la mise en place d'un formulaire électronique, que les usagers devront remplir directement sur l'ordinateur de prêt attribué. Ce formulaire devra impérativement afficher ou proposer d'afficher le règlement intérieur du « point Cyber ». Ce formulaire devra automatiquement enregistrer les données dans un tableur excel. Et, si possible, une nouvelle feuille de calcul devra être créée à chaque changement d'années pour correspondre aux besoins de statistiques annuelles de la mairie.

Cette simple transition d'une fiche papier à un formulaire électronique fera gagner énormément de temps pour les différents agents de [redacted] devant gérer les papiers et cela simplifiera les démarches pour l'usager. Ce dernier sera dorénavant redirigé directement au « point Cyber », sans devoir remplir de fiche [redacted]. De facto, cela fluidifiera les passages à l'accueil et évitera les files d'attente, la secrétaire pouvant difficilement aiguiller des personnes tout en vérifiant les informations personnelles données par l'usage souhaitant se rendre au « point Cyber ».

Concernant le blocage de session après une heure, il est absolument nécessaire que l'usager soit informé régulièrement du temps restant. Si une session doit se déconnecter au bout d'une heure, il faut que l'usager ne soit pas surpris et/ou perde des données suite à cette fin de session.

Cette information du temps passé doit se faire automatiquement. Il ne serait pas confortable et pratique de demander aux [redacted] de chronométrer le temps d'une session ou de faire aveuglément confiance à la bonne foi des usagers, certains n'hésitant pas à rester plusieurs heures sans rien dire.

À partir des besoins donnés et des éléments d'informations récoltés, je me suis penché sur une solution nativement présente sous Windows. Mais rien ne correspond.

Concernant des logiciels tiers qui pourraient être adaptés, soit ce sont des solutions gratuites, mais qui ne sont plus maintenues depuis des années et qui, bien souvent, ne conviennent pas parfaitement aux besoins, soit ce sont des solutions payantes, parfois extrêmement chères. Or, il n'est pas possible de payer une licence plusieurs milliers d'euros uniquement pour limiter des sessions utilisateurs dans le temps.

J'ai donc opté, dans un premier temps, pour un script Powershell que je développerai moi-même. Mais après plusieurs tentatives, il semblait compliqué, en Powershell, de créer des interfaces graphiques correctes et viables. Étant donné que je dois mettre en place un formulaire pour collecter les informations personnelles, il apparait que ce langage n'est pas adapté à ce besoin.

Powershell ne permet pas non plus de gérer plusieurs timers (minuteurs) pour la gestion des fenêtres informatives sur le temps restant et/ou le temps déjà écoulé de la session.

Je souhaitais également que le programme soit le plus simple à porter d'une machine à l'autre, sans que les [redacted] aient besoin de créer une entrée dans le planificateur de tâches. La solution qui semblait la plus adaptée était de convertir le code source en exécutable. Une fois le code source compilé, il n'y aura plus qu'à copier les programmes d'un PC à un autre pour l'installer sur un nouvel ordinateur.

Après recherches, j'ai pu constater que le langage Python pouvait correspondre : il permet de créer des interfaces graphiques grâce à la librairie Qt (9) qui est multiplateforme et est spécifiquement conçue pour développer des interfaces graphiques complexes. PyQt (10), un module Python qui permet d'interagir avec la librairie Qt simplement. Il est donc possible de mettre en place, assez facilement, des interfaces graphiques avec Python.

Ce langage étant aussi plus adapté que Powershell, il sera plus facile de gérer des minuteurs afin de gérer les fenêtres informatives sur les temps de session restants.

Pour débuter, j'ai programmé une version dite « BETA ». Il s'agit d'un premier jet, qui m'a surtout permis d'apprivoiser Python, de connaitre les possibilités offertes par ce langage ainsi que ses limitations.

Cette version BETA était fonctionnelle, mais ne remplissait pas l'ensemble des besoins. En particulier, je n'étais pas parvenu à faire en sorte qu'une fenêtre plein écran s'affiche en début de session afin d'y afficher un formulaire pour les informations de l'usager présent.

Le fonctionnement de ce programme était le suivant :

Un premier programme nommé configuration.py permettait de paramétrer et personnaliser la limitation de session. Toutes les informations de configuration étaient enregistrées dans un fichier de type JSON (JavaScript Object Notation). Ceci permet d'enregistrer des données structurées facilement et qui à l'avantage d'être facilement lisible pas un être humain en cas de problème.

Ensuite un second programme nommé session_manager.py récupérait les données de configuration via le fichier JSON. Session_manager était le programme exécuté à l'ouverture de session et c'est ce programme qui s'occupait de déconnecter la session au bout de 60 minutes et d'afficher les fenêtres infomatives en fonction du temps de session déjà écoulé.

L'ensemble était relativement sommaire, mais fonctionnait. Hormis la fiche à remplir par l'usager, les besoins étaient quasiment comblés. Cela confirmait que mon choix était le bon, mais qu'un travail d'approfondissement était encore nécessaire pour parvenir à corriger l'absence de fiche d'entrée.

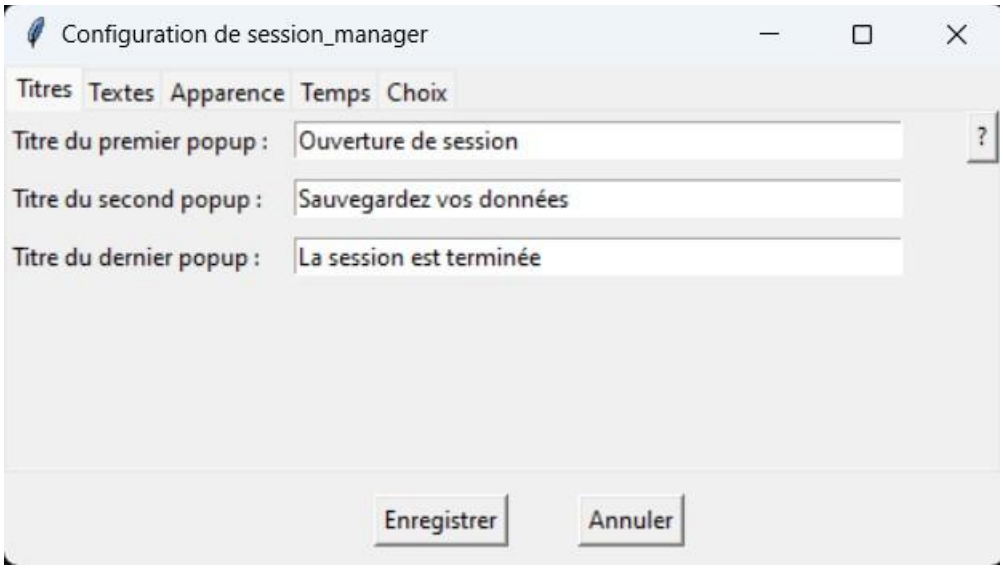


Fig. 1 : configuration.py — Organisé en onglets pour permettre différents paramétrages

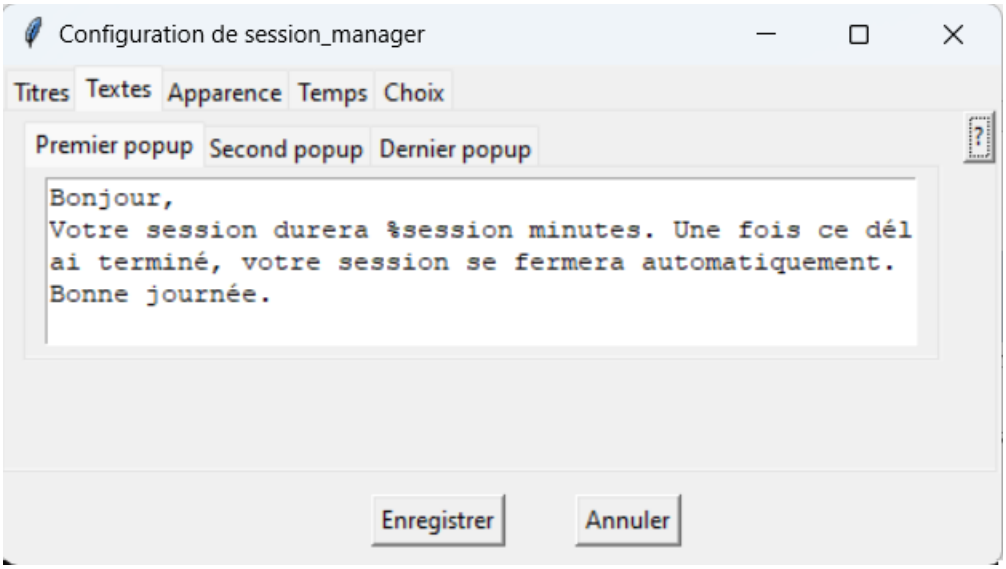


Fig. 2 : L'onglet « texte » de configuration.py permet de modifier le texte affiché dans les fenêtres informatives

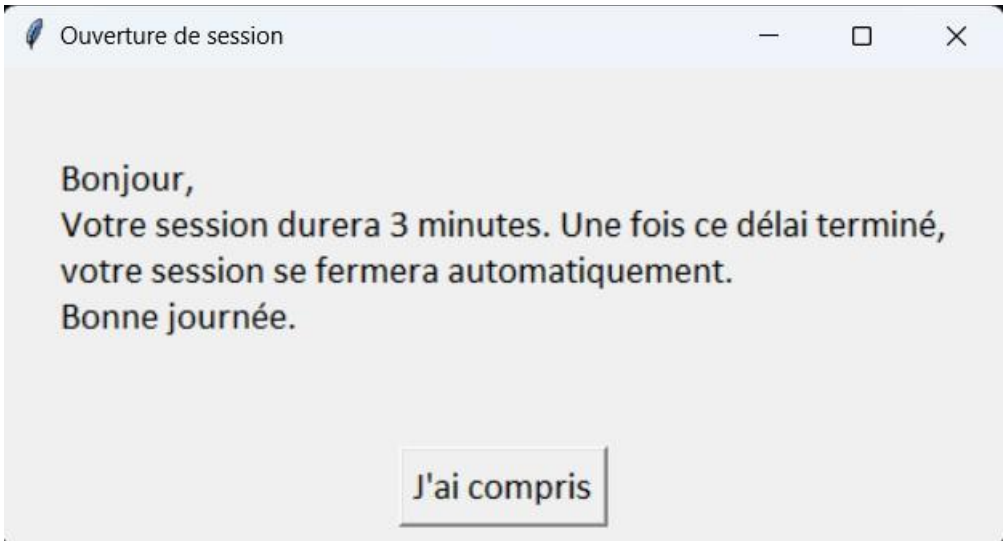


Fig. 3 : session_manager.py, quand un timer donné est atteint, la fenêtre informative s'affiche durant la session invitée

Les timers (minuteurs) étaient personnalisables, tout comme le titre des fenêtres et leurs textes. Une gestion des variables était présente, de telle façon que dans la configuration, nous pouvions mettre « %session » et ce texte était remplacé par sa valeur numéraire du fichier JSON. Cela permettait une plus grande souplesse de personnalisation et évitait d'entrer des données « en dur » dans le paramétrage.

Cet ensemble de programmes, que j'ai sobrement décidé d'appeler « Session Manager » a été installé sur un ordinateur de prêt du « point Cyber ». Il a parfaitement fonctionné. Mais l'absence de fiche d'entrée pour que les usagers entrent leurs informations personnelles me gênait. Sans parler du fait que les fenêtres informatives avaient un aspect très sommaire, pour ne pas dire basique.

Il était donc temps pour moi de passer à une version plus complète.

N'étant pas un spécialiste de Python, j'ai trouvé le logiciel Qt Designer qui permet de créer des interfaces graphiques avec la méthode de glisser-déposer et de WYSIWYG (What You See Is What You Get (= ce qui vous voyez est ce que vous obtenez)). C'est une méthode très simple et très pratique pour manipuler des interfaces graphiques sans avoir à les coder manuellement. Qt Designer dispose, comme précisé précédemment, d'un mode de glisser-déposer. Un menu présente les différents éléments (appelés Widgets) existants dans la librairie Qt, et il suffit de glisser l'élément du menu vers la fenêtre de création et l'élément est ajouté à l'interface graphique que je veux.

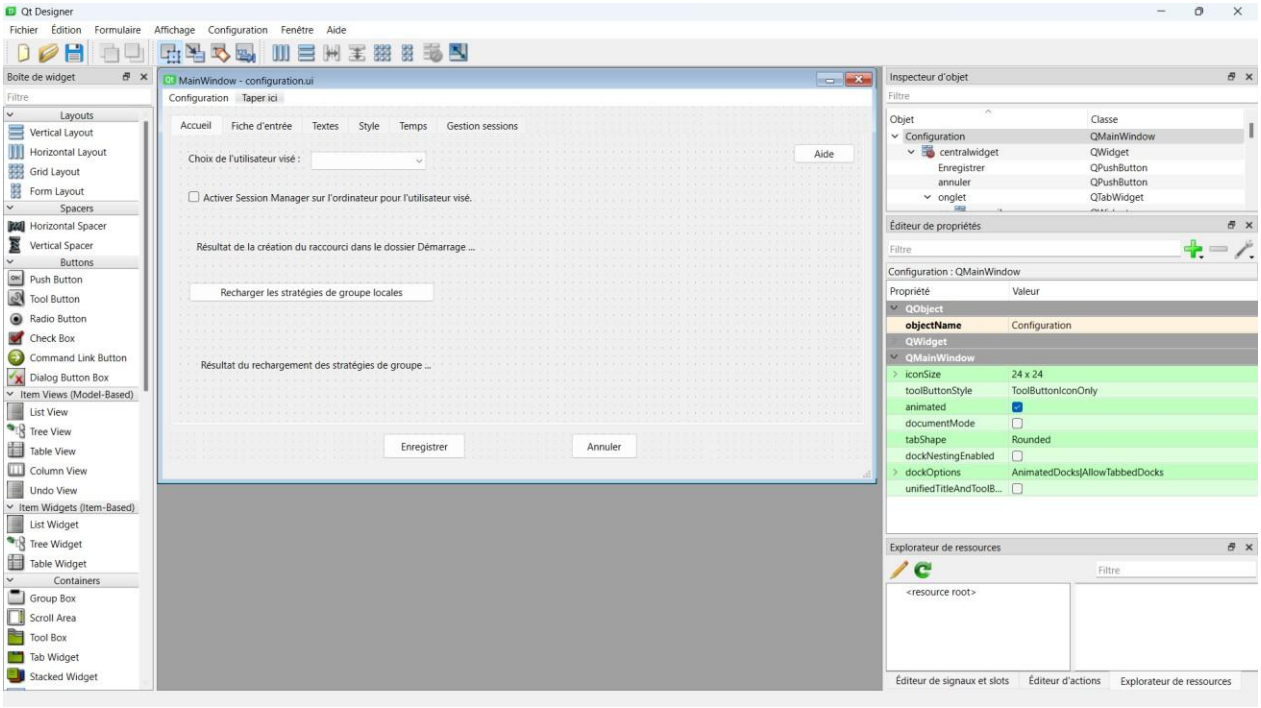


Fig 4 : L'interface utilisateur de Qt Designer, avec la liste des Widgets à gauche. L'interface graphique développée au centre. Les paramètres des Widgets à droite.

Ce logiciel va me permettre de gagner énormément de temps, n'ayant pas besoin de programmer, à la main, une interface graphique dans un langage que je ne maitrise que très peu. Je pourrais également proposer des options beaucoup plus poussées et, par conséquent, un logiciel qui sera plus durable.

J'ai ensuite creusé le sujet pour éviter d'avoir un programme au format Python, en « .py ». Cela oblige à installer un interpréteur python sur toutes les machines devant utiliser ce logiciel. Ce n'est ni pratique ni « user-fiendly ». C'est une source d'éventuels problèmes en cas de conflit de version, d'oubli d'installation de l'interpréteur, etc.

Pour résoudre ce problème et après m'être beaucoup renseigné, j'ai appris qu'il était possible de pseudo-compiler un programme Python en un exécutable. Cet exécutable (au format .exe) n'a pas besoin d'un interpréteur Python installé sur la machine, car l'interpréteur est intégré directement dans l'exécutable lors de la pseudo-compilation. Ce qui rend le programme beaucoup plus portable et simple d'utilisation. Supprimer une contrainte est toujours une bonne chose.

Pour écrire mon code, j'ai utilisé Visual Studio Code. Un éditeur de code gratuit et très efficace. Il est utilisé avec beaucoup de langage grâce aux modules existants qui permettent d'adapter complètement l'éditeur à mes besoins.

L'avantage de Visual Studio Code est qu'il propose également un module nommé « Github Copilot ». Il s'agit d'une intelligence artificielle spécifiquement conçue pour la programmation. Il propose, entre autres, des outils d'auto-complétions du code intelligent (l'IA arrive à deviner le code que l'on veut écrire en fonction du code déjà écrit), on peut également lui parler directement via l'onglet « Conversation » de Visual Studio Code pour lui poser des questions spécifiques au code affiché. Je pourrais donc apprendre à développer avec Python, tout en ayant l'opportunité d'apprendre à utiliser Copilot.

Afin de pouvoir travailler depuis mon PC portable dans les locaux [redacted] ou depuis mon PC fixe chez moi, j'ai hébergé mon code source sur la plateforme Github (11). Cette plateforme permet d'avoir accès à son code de n'importe où et de la synchroniser d'une machine à l'autre.

Par exemple, si je développe sur le PC portable, une fois ma journée terminée, j'envoie (push) mon code depuis le module Github de Visual Studio Code sur le site de Github. Puis quand j'arrive chez moi, je télécharge (pull) le code depuis la plateforme. Je peux ainsi travailler n'importe où sans avoir de problème de versions et en plus je peux avoir une plateforme sur laquelle héberger mon code source pour qu'il soit facilement accessible.

Une fois tous ces outils en main, je me suis mis au travail pour la nouvelle version de Session Manager avec plein d'idées en tête pour créer un programme complet, paramétrable et qui répond parfaitement aux besoins de [redacted], tout en essayant d'être le plus évolutif possible.

Pour commencer, avec l'aide de Qt Desiger, j'ai créé l'interface graphique de mon programme de configuration.

Ce logiciel est très puissant et efficace, on peut faire énormément de choses avec lui une fois que les concepts de bases ont été acquis. Le plus important pour la suite est de bien nommer les différents widgets positionnés dans l'interface pour interagir avec eux facilement dans le reste du script.

Une fois mon interface de configuration terminée, il faut convertir le fichier Qt (au format .ui) en interface compréhensible par Python. Sur mon environnement de développement, j'ai donc installé le paquet PyQt, qui permet cette manipulation. Pour cela, une fois Python installé sur mon environnement, je passe par l'invite de commande de Windows et je tape la commande suivante :

```
pip install PyQt6
```

Une fois le paquet PyQt installé, je convertis mon interface .ui en .py grâce à la commande suivante, toujours dans l'invite de commande Windows :

```
pyuic6 – O configuration.ui Ui_configuration.py
```

Par la suite, je dois importer mon interface de configuration convertie dans le programme qui va interagir avec. À l'heure actuelle, mon interface n'enregistre rien et ne sert à rien. C'est juste une coquille vide. Il faut ensuite que je programme toutes les fonctions qui vont permettre d'enregistrer ou de réagir avec les interactions de l'utilisateur sur l'interface graphique.

Pour importer mon fichier dans mon script qui va permettre les interactions, je saisis le code suivant au début de mon script :

```
from Ui_configuration import Ui_Configuration
```

Ceci me permet d'importer, depuis (from) *Ui_configuration* la classe *Ui_Configuration*. Et pour faire interagir mon code avec les éléments de l'interface, je construis la classe principale de mon programme puis je crée une instance de ma classe *Ui_Configuration* que j'associe à *self.ui*

Ce qui me donne le code suivant :

```
# Classe principale de l'application
class MainWindow(QMainWindow):

    # Constructeur de la classe
    def __init__(self, parent=None):
        super().__init__(parent) # Appelle le constructeur de la classe parente
        self.ui = Ui_Configuration() # Crée une instance de Ui_Configuration
```

Ainsi, si je veux interagir avec les widgets de *Ui_Configuration*, j'utilise le code suivant :

```
self.ui.Enregistrer.clicked.connect(self.enregistrer_conf) # Enregistrement de la
configuration
```

Ce code se traduit de la façon suivante :

self.ui est l'instance de classe de *Ui_Configuration*. *Enregistrer* est le nom que j'ai donné au bouton « Enregistrer » de mon interface graphique. *Clicked* est la méthode de PyQt qui permet de capter les clics sur des éléments graphiques. *Connect* est la méthode qui permet de lier l'évènement *clicked* au bouton *Enregistrer*. Puis, entre parenthèses, nous faisons appel à une fonction nommée *enregistrer_conf()* qui appartient à ma classe *MainWindow*, d'où la présence du préfixe *self*

Pour résumer, ce code fait appel à la fonction *enregistrer_conf()* quand l'utilisateur va cliquer sur le bouton éponyme.

Le code complet de configuration.py, qui permet d'enregistrer les interactions avec mon interface graphique représente plus de 900 lignes de code.

Le fonctionnement reprend celui de ma version BETA : configuration.py permet le paramétrage du programme principal nommé session_manager.py. La configuration est enregistrée dans un fichier JSON sous la forme d'un dictionnaire complexe. Voici une partie de config.json :

```
{
    "text": {
        "text_popup_1": "Un texte d'avertissement",
        "text_popup_2": "Un second texte d'avertissement",
        "text_fermeture": "Le texte de fermeture de session
    },
    "timer": {
        "delai_fermeture": "15",
        "duree_session": "3",
```

```
        "timer_popup_1": "1",
        "timer_popup_2": "1",
        "timer_popup_3": "10"
    },
    "fiche": {
        "fiche_log": true,
        "fiche_activation": true,
        "fiche_duree_session": true,
        "fiche_15min": true,
        "fiche_30min": true,
        "fiche_1h": true
    },
```

Session_manager.py se contentera donc d'adapter son fonctionnement selon les valeurs des différentes variables présentes.

J'ai souhaité que le programme soit le plus complet possible et puisse être personnalisable possible. L'objectif est double ; que [redacted] puissent le configurer comme ils le souhaitent, sans avoir besoin de modifier le code source du programme, afin de simplifier leur travail et faire en sorte que le programme puisse être utilisé le plus longtemps possible. Si certaines limitations existent, [redacted] pourraient, en cas d'évolution de leurs besoins, être obligés de trouver une nouvelle solution. Ce qui n'est pas le but. Une très grande personnalisation me permet d'anticiper les futurs besoins.

Mon programme de configuration dispose des fonctionnalités suivantes :

- Fonctions générales
    - Activer ou désactiver Session Manager
    - Choisir le compte qui sera concerné par la gestion de session
    - Recharger les GPO locales
- Gestion de la fiche d'entrée
    - Activer ou désactiver la fiche d'entrée
    - Activer ou désactiver le stockage des données utilisateurs dans un document Excel
    - Définir le temps de session voulu (donnée à usage statistique)
    - Gestion des champs présents dans la fiche d'entrée
        - Ajouter ou supprimer des champs (texte simple ou texte et champ de saisie)
        - Modifier l'ordre d'affichage des données à remplir
        - Afficher une prévisualisation de la fiche d'entrée
- Définir les textes qui seront affichés dans l'ensemble des popups
    - Possibilité d'utiliser des variables pour remplacer les valeurs dynamiques
- Personnaliser l'apparence des popups :
    - Taille de la fenêtre (largeur et hauteur)
    - Choix de la police de caractère et de sa taille
    - Choix des couleurs utilisées
        - Couleur de fond du popup
        - Couleur de la police de caractère
        - Couleur du bouton
        - Couleur du texte du bouton

        - Couleur du bouton au survol
        - Texte du bouton
    - Prévisualisation du popup
- Définir les différents timers (minuteurs) utilisés :
    - Durée globale d'une session
    - Délai avant affichage du premier popup de rappel
    - Délai avant affichage du second popup
    - Durée d'affichage des popups avant leur fermeture automatique
    - Durée d'affichage de la fenêtre avant la déconnexion de la session
- Type de fermeture de session (déconnexion ou verrouillage de session)
- Activer ou désactiver la fenêtre de fermeture de session
- Personnalisation des fichiers d'aide (format markdown)

Très régulièrement, au cours du développement du programme, j'ai fait appel à l'avis des [redacted] afin d'être sûr de ne pas dévier et de respecter leurs besoins et ce qu'ils aimeraient avoir en termes de fonctionnalités. D'autant qu'en fonction de l'avancée du développement du programme, leurs besoins ont aussi évolué en voyant les possibilités.

J'ai rencontré certaines difficultés en programmation n'étant pas spécialiste de python. Il a fallu que je cerne les limites techniques de python et les restrictions de sécurité de Windows. Devant interagir, dans mon programme de configuration, avec la liste des utilisateurs, les déconnexions de sessions, l'activation du programme, etc. Cela demandait des interactions bas niveau avec Windows. Or, certaines de ces interactions ne sont pas permises, pour des raisons de sécurité. Ou il faudrait utiliser un langage de plus bas niveau que python.

Par exemple, lors du développement, j'ai souhaité, via mon programme de configuration, que l'activation de Session Manager soit gérée par le planificateur de tâche. Mon souhait était que si l'utilisateur coche une case dans le programme, alors une tâche est ajoutée au planificateur. Mais cela n'est pas possible en python, à cause des restrictions.

Pour contourner le problème, il a fallu trouver une alternative. Les stratégies de groupe locales ne sont pas non plus accessibles en python, ou cela devient extrêmement complexe et risqué en cas de mauvaise manipulation.

La solution a été d'ajouter un raccourci vers mon programme session_manager dans un répertoire particulier. Ce répertoire permet, en ajoutant un raccourci vers un programme, de faire en sorte que le programme soit exécuté à l'ouverture de la session utilisateur. Python permettant facilement de créer des raccourcis, cela convenait parfaitement à mon besoin. Le répertoire en question est le suivant :

```
C:\Users\{user}\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup\session_manager.lnk
```

{user} étant dans ce cas une variable qui est égale au nom de l'utilisateur pour lequel on souhaite activer le programme session_manager.

Une seconde difficulté rencontrée est que je voulais permettre aux [redacted] de modifier l'ordre d'affichage des champs de saisie de la fiche d'entrée. Pour que la fiche puisse être dynamique au maximum et s'adapter aux futurs besoins. Le problème est que les informations sont enregistrées au moment où la fenêtre de configuration est fermée. Si un [redacted] ajoutait un champ et souhaitait, dans la foulée, modifier son ordre d'affichage,

il lui aurait fallu ajouter le champ, fermer la fenêtre du programme, ouvrir à nouveau le programme et enfin modifier l'ordre d'affichage. Ce qui n'est absolument pas pratique ni ergonomique.

Pour pallier ce problème, j'ai dû créer des fonctions qui, à chaque nouvelle modification faite dans l'interface graphique de la configuration, va chercher en temps réel les nouvelles informations saisies.

J'ai voulu que la fiche d'entrée soit visuellement agréable. En me renseignant sur divers forums spécialisés, j'ai pu voir qu'il était possible, avec PyQt, d'utiliser certaines propriétés de CSS (12) (Cascading Style Sheets) qui sont des feuilles de style pour définir les priorités graphiques d'une page web (html). Toutes les propriétés ne sont pas disponibles, mais cela me permettra au moins d'avoir un aspect visuel plus travaillé et agréable qu'une fenêtre Windows.

Il est ainsi possible de choisir la police de caractère, la taille de la police, la couleur de fond de l'image, la couleur de la police, idem pour les éléments composant le bouton qui ferme la fenêtre.

Autre détail que je souhaitais : les utilisateurs étant sur le PC de prêt ne devaient pas pouvoir fermer la fiche d'entrée, ni pouvoir la masquer et utiliser le PC temps que les champs n'étaient pas remplis. La solution fut relativement simple à trouver, les paramètres de PyQt permettant d'afficher une fenêtre plein écran, de désactiver le bouton de fermeture d'une fenêtre (la fameuse croix blanche en haut à droite) et de faire en sorte que la fenêtre revienne en permanence au premier plan sur l'écran. Cela correspond parfaitement à mes besoins.

Les utilisateurs n'ayant pas accès au gestionnaire de tâche, il leur est donc impossible de fermer et/ou masquer la fiche d'entrée. Ils ne peuvent donc pas utiliser l'ordinateur sans avoir pris le temps de lire et de compléter les informations demandées.

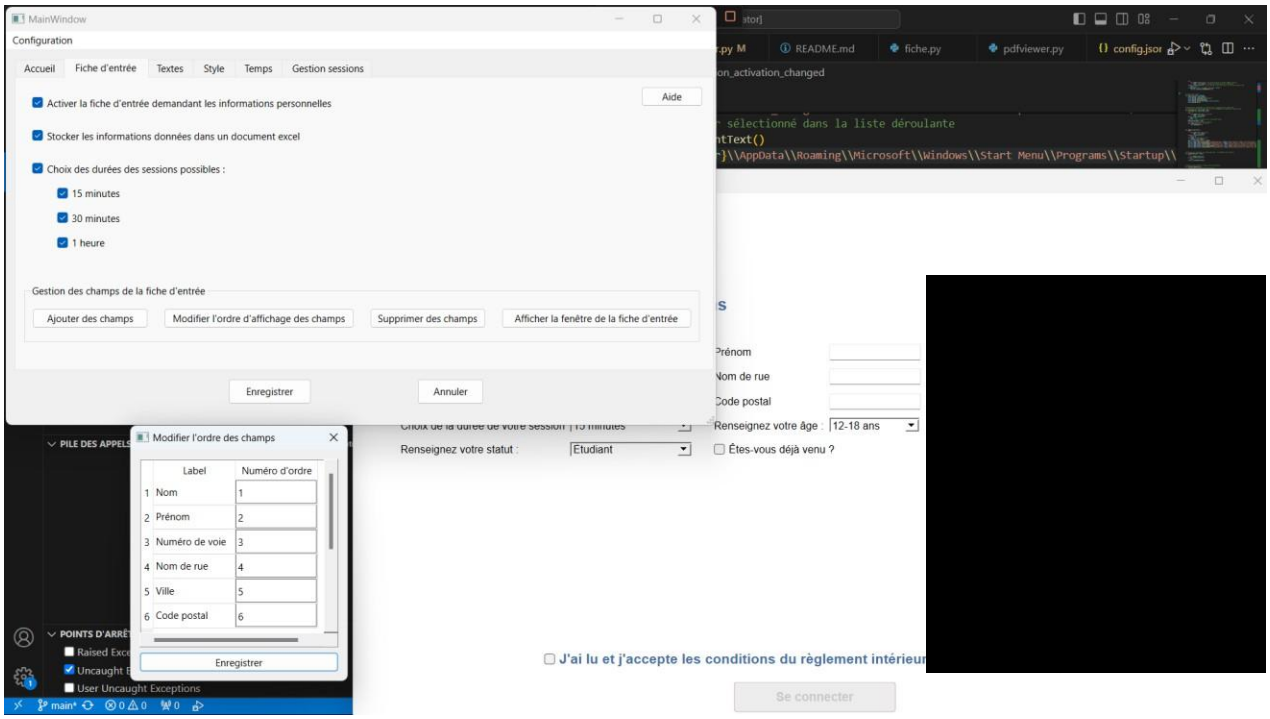


Fig. 5 : L'onglet de personnalisation de la fiche d'entrée. Un aperçu de la fiche d'entrée (qui sera en plein écran lors de l'ouverture de la session invitée) et la fenêtre permettant de modifier l'ordre d'affichage des champs de la fiche d'entrée

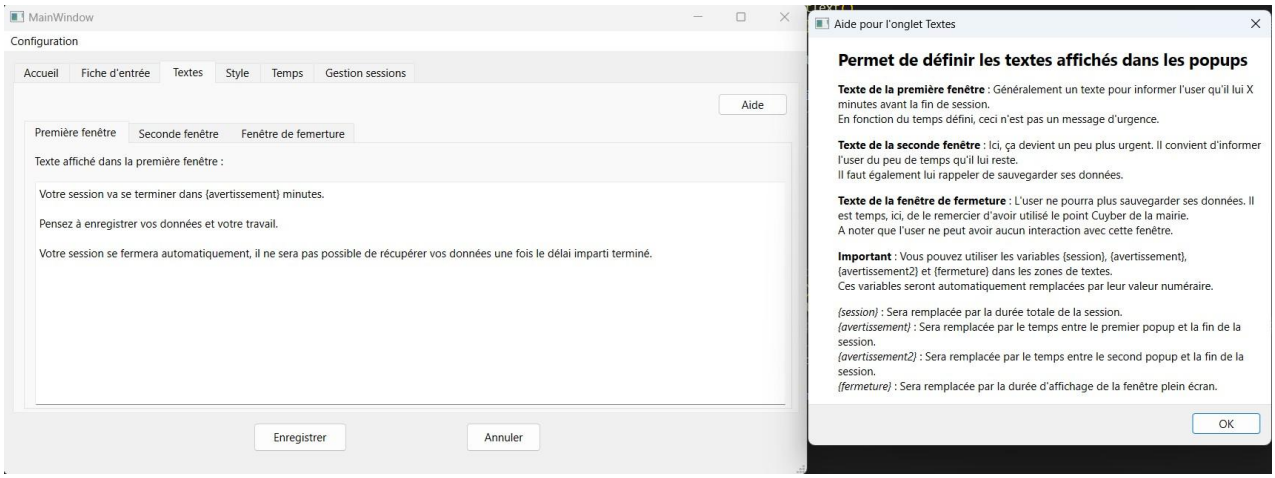


Fig. 6 : L'onglet permettant la personnalisation des fenêtres qui s'afficheront au fur et à mesure du temps restant sur la session invitée. À droite, la fenêtre d'aide pour aider les conseillers numériques à comprendre comment fonctionne cet onglet

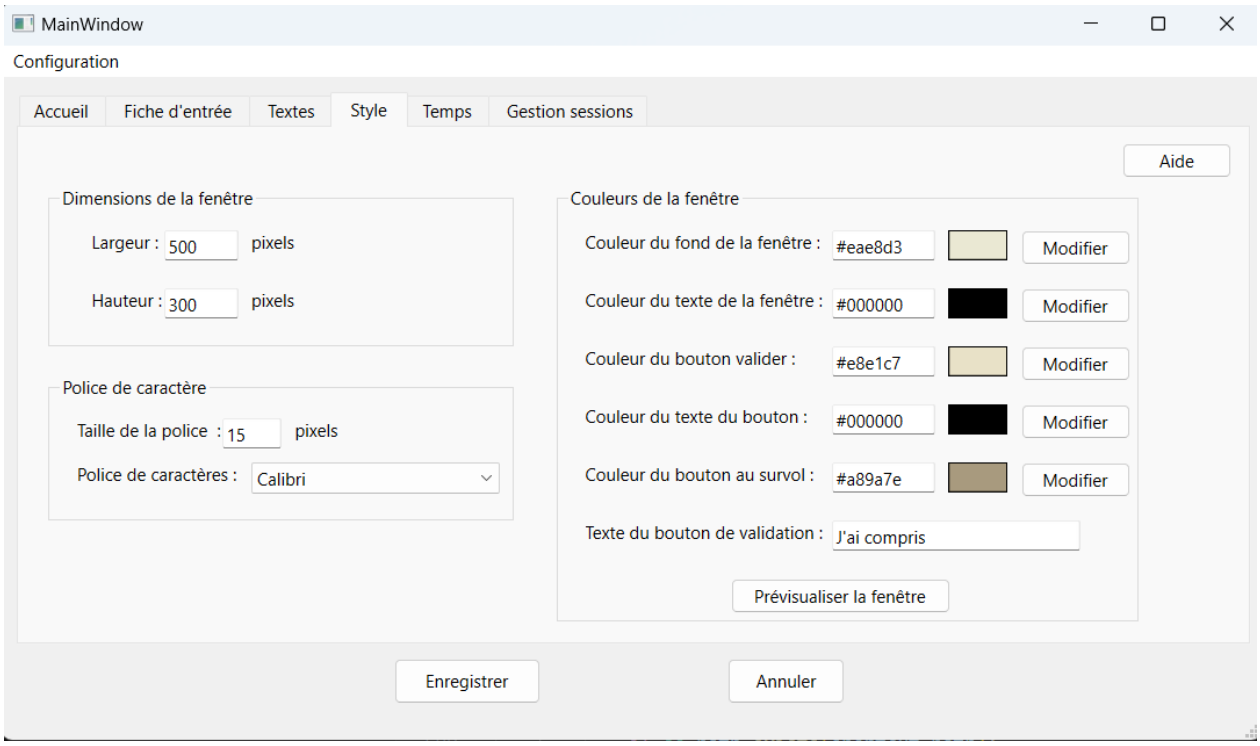


Fig. 7 : L'onglet permettant de personnaliser l'affichage des fenêtres d'avertissement.Les boutons « Modifier » ouvrent une palette de couleur. « Prévisualiser » affiche la fenêtre en prenant en compte les modifications en temps réel.

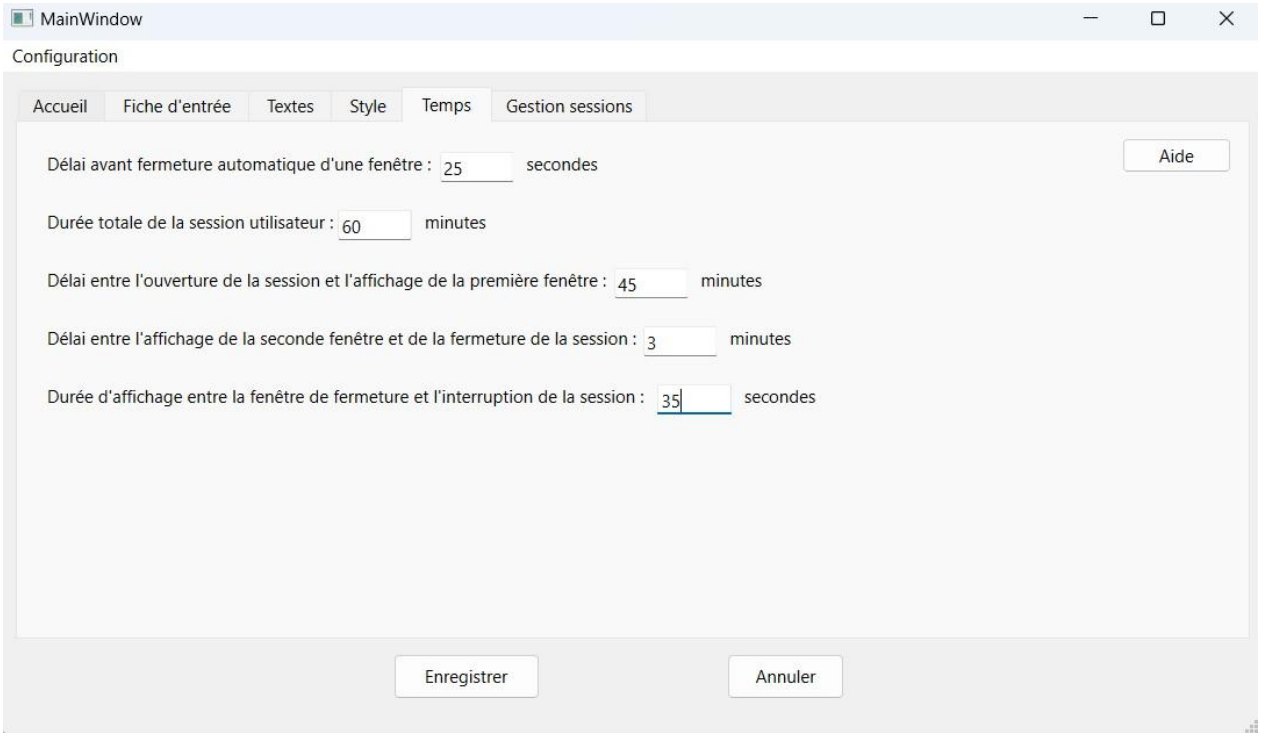


Fig. 8 : L'onglet Temps afin de personnaliser la durée d'une session, les délais d'affichage des différentes fenêtres d'avertissement

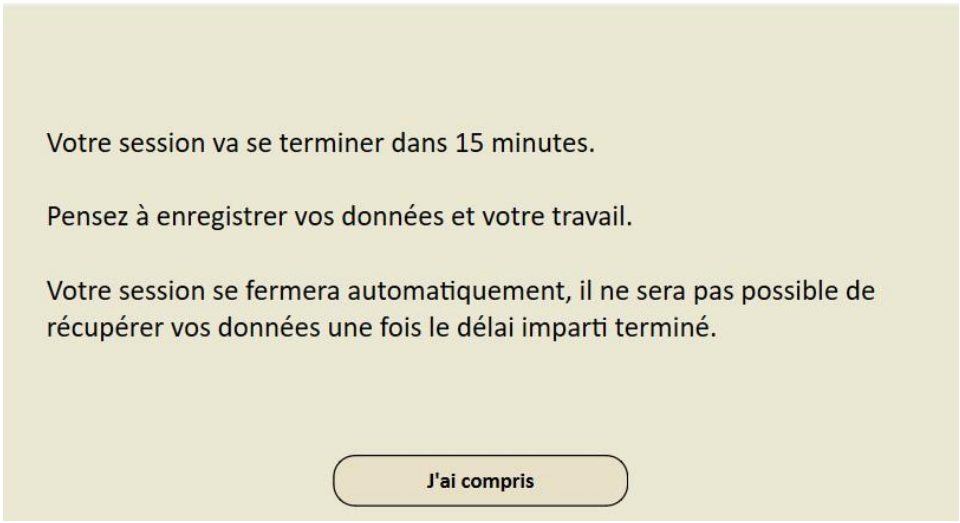


Fig. 9 : Une fenêtre d'avertissement, avec les paramètres définis dans l'onglet Style et le texte saisi dans l'onglet Texte

Les données enregistrées dans la fiche d'entrée sont enregistrées dans un fichier excel. Une colonne portant le nom du champ est automatiquement créée si un champ est ajouté depuis le programme de configuration.

Le script génère une nouvelle feuille chaque année, de façon à correspondre aux besoins statistiques.

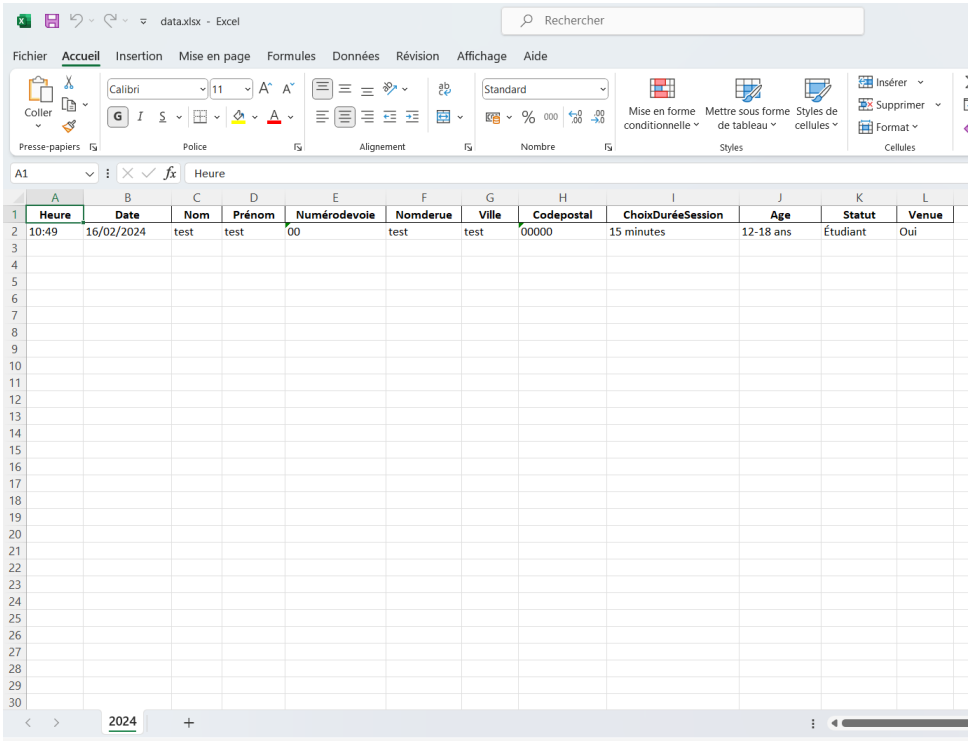


Fig. 10 : Un exemple du fichier excel généré. On peut constater les données saisies et la feuille correspondant à l'année en cours.

La largeur des colonnes est ajustée automatiquement en fonction de la taille du titre de la colonne. Cela se fait assez facilement en python et permet d'améliorer la lisibilité du document.

Si un champ est supprimé, la colonne reste présente dans le document excel mais la cellule restera vide. Idem si un champ est ajouté : une colonne sera créée, mais les lignes précédentes seront vides.

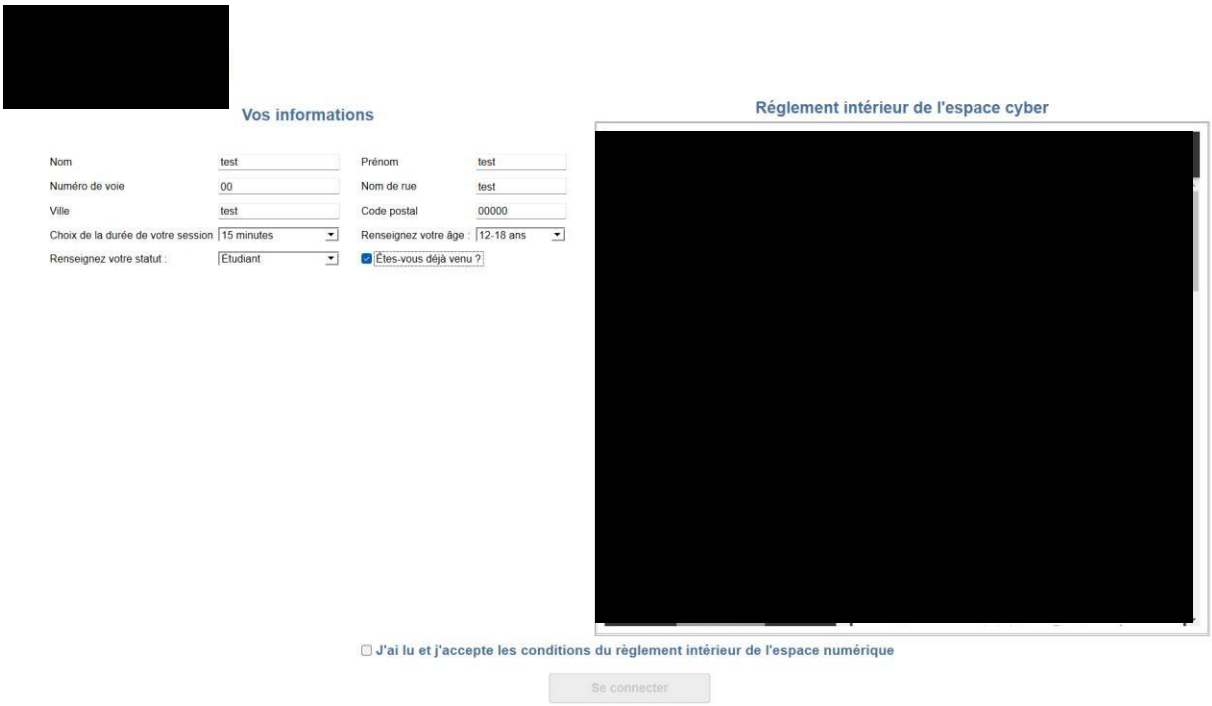


Fig. 11 : La fiche d'entrée, en plein écran, telle qu'affichée à l'ouverture d'une session

Le règlement intérieur affiché est présent dans le dossier courant du script. Si les [redacted] souhaitent le changer, il leur suffit de modifier le fichier PDF nommé reglement.pdf.

Le logo est également modifiable facilement : il suffit de remplacer le fichier image logo.png présent dans le dossier img, dans le répertoire courant du script.

En cas de changement des besoins, les [redacted] peuvent désactiver l'enregistrement des données de la fiche d'entrée en décochant simplement une case dans le programme de configuration. Il est aussi possible de désactiver l'affichage de la fiche d'entrée à l'ouverture de la session. Cela afin d'anticiper la future évolution des besoins [redacted].

Quand j'ai eu terminé de programmer mes applications j'ai dû réfléchir à un moyen de convertir mes fichiers .py en exécutable afin de ne pas installer l'interpréteur Python sur les PC hôtes. Pour cela j'ai utilisé le programme PyInstaller (13) qui permet de créer une pseudo-compilation de programmes python en exécutable.

Il faut passer par l'invite de commande Windows et entrer la commande suivante :

```
pyinstaller --onedir --noconsole configuration.py
```

Le paramètre —*onedir* sert à ajouter les dépendances du programme dans un dossier à part sans qu'elles soient compilées afin d'améliorer le temps d'exécution du programme.

--*noconsole* fait en sorte que, lors de l'exécution du programme, la console de l'interpréteur python ne sont pas affichée en arrière-plan. Si tel était le cas, alors il suffirait aux utilisateurs de fermer la console de l'interpréteur pour terminer le programme. De plus cela ne serait pas ergonomique : une fenêtre resterait présente en permanence le temps de la session utilisateur et ces derniers pourraient ne pas comprendre pourquoi cette fenêtre est là.

Pour terminer ce projet, j'ai configuré les navigateurs internet pour que l'historique, les mots de passe, les identifiants, les cookies, etc., soient supprimés quand le navigateur est fermé. Dans le cas contraire, une personne mal intentionnée pourrait récupérer les mots des précédents utilisateurs qui, par mégarde, auraient enregistré leur mot de passe dans le navigateur.

Le répertoire courant du script comporte aussi un fichier README.md (14) (fichier texte au format markdown (15)) qui explique le fonctionnement du programme en détail. Le langage et les programmes utilisés. Les détails techniques pour la compilation. Les fonctionnalités. Et mon adresse mail.

Ce document a pour but d'apporter tous les détails nécessaires à la compréhension du programme pour une personne qui ne connait pas du tout ce logiciel. Il est composé d'un peu plus d'une centaine de lignes de texte et j'ai tenté d'être le plus explicite et le plus précis possible afin qu'en cas de problème, les [redacted] puissent avoir les clés en main pour trouver une solution.

Chaque onglet du programme de configuration contient un bouton d'aide. L'aide affichée est enregistrée au format markdown aussi. J'ai mis cette aide dans un format éditable afin que les [redacted] puissent la modifier en fonction de leur besoin, ou pour éventuellement s'en servir de pense-bête, voire pour ajouter un détail que j'aurais oublié.

Le code source est également disponible su Github et le lien présent dans le fichier README. J'ai également laissé le code source à mon tuteur de stage. En cas de besoin ou s'ils souhaitent y apporter des modifications, ils pourront modifier le programme et le compiler. Toutes les informations nécessaires étant données dans le fichier README.

2.4 — Projet 4

Des travaux ont été effectués dans [redacted] afin de la rénover. Une attention toute particulière a été apportée au SI afin de permettre aux administrés de pouvoir suivre des cours d'informatique, de recevoir une aide pour leurs démarches en ligne, ou encore afin de leur proposer un « point Cyber » disposant d'un ordinateur portable récent, d'une imprimante en réseau et d'une connexion fibrée.

Cette première salle propose une surface de 70m². Elle accueille les deux [redacted] et le « point Cyber ». Elle dispose d'une baie informatique 19 pouces recevant les divers éléments nécessaires au bon fonctionnement du réseau.

[redacted]

Dans un second temps, et dans une optique de modernisation de la mairie, la salle recevant le [redacted] a été entièrement refaite à neuf. Cette seconde salle, de 130m², accueillera [redacted].

Cette salle dispose d'enceintes encastrées au plafond. D'un réseau de communication filaire dans le sol. D'une baie serveur de 19 pouces pour y placer les différents éléments informatiques permettant de gérer l'ensemble du système de la salle.

La connexion Internet de cette salle est apportée par la baie informatique de salle du « point Cyber ».

Une contrainte nous a été imposée pour connecter l'ensemble des deux salles. Un [redacted] devait se tenir dans la nouvelle salle le 8 février 2024. Or les travaux ont pris beaucoup de retard et nous ne disposions plus que de trois jours pour faire le câblage, configurer le réseau, procéder aux contrôles de bon fonctionnement et faire un test grandeur nature avec [redacted]

L'annonce ayant été faite officiellement lors des [redacted] au mois de janvier, cette date limite ne pouvait être repoussée. De plus, des journalistes avaient été conviés pour couvrir l'évènement afin de mettre en avant la modernisation de [redacted].

Une fois les travaux de gros œuvres terminés dans ces salles, il nous a fallu procéder au câblage des différents éléments propres au réseau de communication (prises murales RJ45 pour la VoIP et le réseau internet, bornes Wi-Fi, switch, routeur, etc.). L'électricien chargé des travaux a seulement tiré les câbles. Mais il n'a procédé à aucune connexion ni aucun branchement de prise.

Avant de pouvoir câbler le réseau, nous avons dû repérer les différents câbles RJ45 et définir une topologie du réseau afin d'organiser notre travail.

Les connectiques filaires ont été faites par nos soins, en respectant la norme T568B (16). Cette norme définit comment les différentes paires de fils d'un câble RJ45 doivent être assemblées dans un connecteur terminal (prise, noyau, etc.). La norme B est recommandée dans les installations dites commerciales tandis que la norme A aura plutôt tendance à être utilisée dans un réseau domestique. Il faut toutefois noter que la norme A se fait vieille et est de moins en moins utilisée. Cette dernière permettant des débits inférieurs à la norme B.

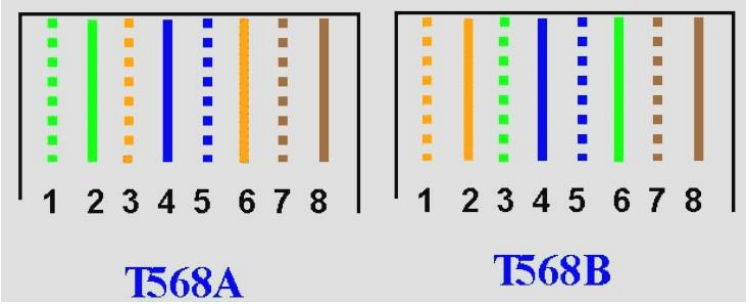


Fig 1 : schéma de câblage d'un connecteur 8P8C (également nommé RJ45)

Comme le montre le schéma, la différence entre les deux normes A et B se situent au niveau des paies vertes et oranges. Il est impératif que l'ensemble des connecteurs soit câblé de la même façon afin d'avoir un câblage droit (la paire verte est sur les connecteurs 1 et 2 sur les deux extrémités du câble).

Un croisement dans les connexions rendrait la communication impossible entre les deux terminaux branchés.

Pour la salle du « point Cyber », cela représente 18 câbles RJ45 :

- 10 prises RJ45 pour Internet dans des trappes au sol.
- 4 prises RJ45 murales pour les bureaux des conseillers numériques
- 3 prises murales pour brancher les écrans servant pour les cours informatiques
- 1 câble permettant d'acheminer la connexion Internet vers la salle du conseil municipal

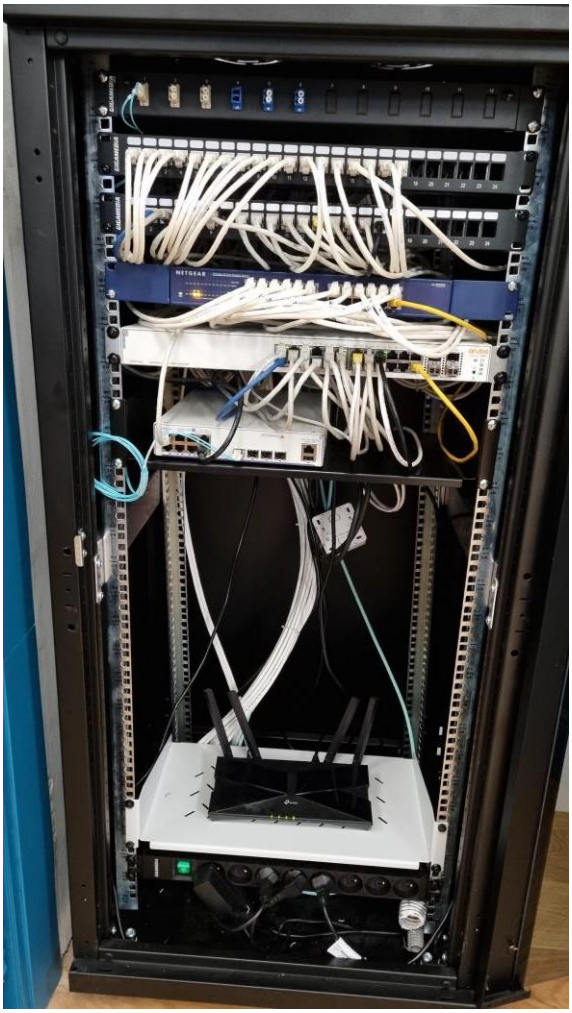


Fig. 1 : La baie informatique du SI que nous avons brassé

La connexion Internet du « point Cyber » est acheminée depuis un câble fibre directement depuis la salle des serveurs de la mairie.

Concernant la salle du [redacted], cela représente 25 câbles :

- 21 prises RJ45 dans des trappes au sol
- 3 prises murales pour les écrans servant à afficher les infographies lors du conseil municipal
- 1 câble provenant de la salle du « point Cyber ».

Fig. 2 : la baie informatique de la salle du conseil

Pour faire l'essentiel de ce travail de câblage, nous étions deux : l'alternant de la SI et moi.

Nous avons commencé par brancher les câbles RJ45 dans la baie informatique du « point Cyber ». Ces câbles sont les départs permettant de propager le réseau dans la salle.

Les 18 câbles ont été connectés à un noyau RJ45. Puis l'ensemble des noyaux sont clipsés dans un support modulaire dans la baie informatique. Afin de pouvoir les repérer plus facilement. Chaque câble desservant une prise. Il peut être utile, en cas de panne future, de savoir précisément quel câble correspond à quelle prise.

Fig 3 : Un noyau RJ45 utilisé dans les baies

Les noyaux sont utilisés afin de permettre une organisation plus propre de la baie informatique et une plus grande modularité. Quand l'ensemble des câbles sont connectés à un noyau et que tous les noyaux sont rangés dans leur support, il nous a fallu installer un switch L3.

Quand l'ensemble des noyaux des deux salles ont été mis en place, nous sommes passés au branchement de l'ensemble des prises réseaux présentent dans les deux salles. Cela représente 41 prises RJ45 à connecter.

Cette étape terminée, nous avons relié les noyaux au switch, dans les baies informatiques, via des câbles RJ45 de 50 centimètres. Un routeur est également présent dans la baie informatique de salle du « point Cyber » afin de mettre en place un VLAN pour le réseau Wi-FI mis à disposition des usagers venant dans [redacted]. Cela a pour but de créer deux réseaux distincts ne communiquant pas entre eux. Il est alors impossible pour une personne connectée sur le Wi-Fi de se connecter aux serveurs de [redacted]. Ceci permet de sécuriser le réseau informatique permettant le bon fonctionnement des services [redacted].

Le switch est relié au routeur. Routeur qui fait la liaison avec le réseau WAN et le réseau LAN grâce à un câble optique relié à un switch optique dans la salle serveur de la mairie.

Notre réseau LAN est basé sur l'adresse IP 192.168.1.0/24. Le VLAN Wi-Fi est basé sur l'adresse IP 192.168.20.0/24.

Une seconde contrainte est apparue avec le temps : les adresses IP disponibles sur notre réseau LAN principal (192.168.1.0/24) arrivent à saturation. L'étendue DHCP du serveur AD est 192.168.1.50 à 192.168.1.200. Les adresses hors de cette étendue sont réservées pour les différents services existants et les services qui pourraient être mis en place lors d'une évolution du réseau. La salle du [redacted] pouvant accueillir 30 à 40 simultanément, cela pourrait finir par tarir les adresses IP disponibles sur le serveur DHCP. Les [redacted] étant tous équipés de Chromebook qui seront connectés sur un réseau Wi-Fi. Réseau Wi-Fi différent de celui mis à disposition des usagers. Les [redacted] ayant besoin de pouvoir accéder aux différents services [redacted] (services de fichiers partagés en premier lieu).

Afin de résoudre cette problématique, le responsable du système d'information m'a chargé de mettre en place un routeur Wi-Fi spécifique pour la salle [redacted]. Le routeur devant être relié au réseau interne [redacted], mais devant fournir une étendue DHCP différente de celle du serveur Active-Directory.

Pour ce faire, j'ai configuré le routeur Wi-Fi de la façon suivante :

L'adresse de la passerelle WAN est 192.168.1.254/24. Cette adresse correspondant à la passerelle du réseau principal interne.

Les serveurs DNS du routeur Wi-Fi sont 192.168.1.6/24 et 192.168.1.9/24, ce qui correspond aux DNS configurés dans le serveur Active-Directory.

La passerelle LAN est 192.168.30.1/24. Le routeur Wi-Fi sera donc sa propre passerelle pour le réseau local.

L'étendue du serveur DHCP du routeur Wi-Fi est 192.168.30.20/24 à 192.168.30.200/24. Ceci afin de permettre la mise en place d'éventuels futurs services sur ce réseau tout en ayant 180 adresses IP disponibles pour les personnes présentes dans la salle du conseil municipal. Cela couvre très largement les besoins, la salle ne pouvant accueillir plus de 100 personnes simultanément.

Ainsi, j'ai pu solutionner le problème rencontré et soulager l'étendue DHCP du serveur Active-Directory, tout en reliant les deux réseaux entre eux. Il est donc parfaitement possible, grâce à la configuration de l'IP de la passerelle WAN du routeur Wi-Fi, d'être connecté sur le réseau 192.168.30.0/24 et de communiquer avec le réseau principal 192.168.1.0/24.

Fig. 4 : La salle du conseil avec les écrans sur lesquels partager les documents et les micros. Le micro [redacted] permet de couper tous les autres micros qui seraient activés.

Cette salle nous a demandé environ une matinée de travail pour repérer les câbles, connecter les noyaux et les prises. L'installation du système audio-visuel a été faite par une entreprise extérieure, étant donné qu'il fallait configurer des amplificateurs, régler l'effet Larsen (17) des micros, etc.

Fig. 5 : La salle connectée, appelée « point Cyber » dans laquelle nous travaillons. La baie informatique se situe derrière les deux portes bleues.

La salle connectée est l'open-space dans lequel travaille les [redacted] et les différents stagiaires. Elle accueille également les personnes souhaitant profiter d'un ordinateur de prêt. Les prises réseaux et électriques sont cachées dans des trappes au sol, présentent sous les tables. Les ordinateurs de prêt sont en permanence sur les tables, à disposition des usagers. Les écrans sont pilotables en réseau et sont tactiles et sont utilisés pour les cours informatiques en groupe. Ils peuvent afficher des visuels type PowerPoint

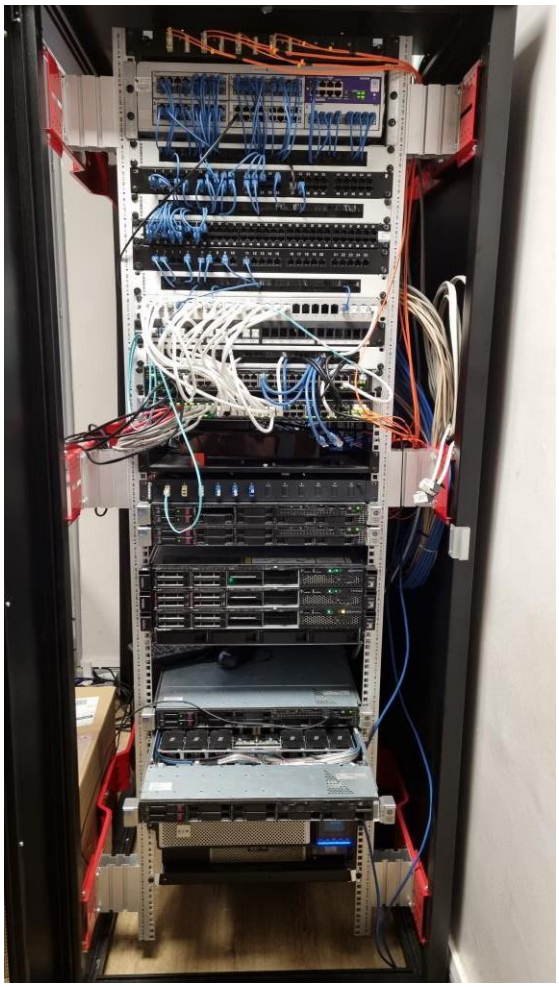


Fig. 6 : La baie principale, située dans une salle fermée à clé et climatisée.

La baie principale, située dans la salle serveur, contient :

- Les IPBX : pour gérer les réseaux téléphones IP LAN & WAN. Le logiciel utilisé dans notre cas est Alcatel-Lucent OmniPCX Entreprise.
- Les firewalls : ce sont des firewalls logiciels utilisant OPNsense

3 — Axes d'amélioration

3.1 — Gestionnaire de mot de passe

Il y a actuellement aucune politique de sécurité concernant les mots de passe dans [redacted]. Les mots de passe n'ont aucune restriction quant à leur longueur, leur complexité et leur réutilisation. De plus, de très mauvaises habitudes en matière de sécurité ont été prises lors de la définition d'un mot de passe par défaut d'un service ou d'un compte utilisateur : les nouveaux services se voient tous attribuer le même mot de passe, qui n'est jamais changé. Les nouveaux utilisateurs (AD, GLPI, etc.) se voient également tous attribuer le même mot de passe.

Il est donc très courant de voir plusieurs utilisateurs ayant le même mot de passe et ne le changer qu'un cas de besoin. Les mots de passe attribués sont également très sensibles aux attaques par dictionnaire (18). En effet, il existe pléthore de listes disponibles facilement sur internet qui contiennent les mots de passe les plus couramment utilisés (19). La vulnérabilité du système est donc très importante.

Notons que ces pratiques ne respectent pas les standards de sécurité recommandés par le Gouvernement (20).

Afin de remédier à ceci, je proposerai le déploiement, systématique, d'un gestionnaire de mot de passe par une GPO qui toucherait l'ensemble des ordinateurs du domaine.

Mon choix de gestionnaire de mot de passe se portera sur KeePass (21) pour plusieurs raisons :

1. Le logiciel est gratuit, ce qui ne demande donc pas d'allouer un budget à son déploiement
2. KeePass est certifié CSPN (Certification de Sécurité de Premier Niveau) par l'ANSSI (22)
3. Une version existe pour les téléphones Android et iOS
4. Il est possible d'y intégrer une traduction française validée par KeePass (23)

Concernant le déploiement, il sera fait par le biais d'une GPO ajoutée sur le serveur AD de [redacted]. Cette GPO touchera l'ensemble des ordinateurs du domaine afin que le logiciel soit installé automatiquement à chaque nouvelle machine reliée au réseau.

Néanmoins, afin de pouvoir accompagner au mieux et configurer KeePass en fonction de nos besoins en sécurité, le logiciel sera déployé service par service. Par exemple, lundi nous le déploierons dans le [redacted], le mardi dans le service comptabilité, etc.

Le déploiement sur les téléphones se fera au bon vouloir des usagers. Bien que, lors de la transition vers l'utilisation du gestionnaire, nous procèderons à une explication et une formation des utilisateurs, les téléphones étant, dans la plupart des cas, des téléphones personnels, nous ne pourrons intervenir directement dessus. Néanmoins, nous constaterons à l'usage que les utilisateurs finissent par installer l'application, essentiellement pour se faciliter la vie.

Le déploiement se déroulera donc en deux étapes :

- Une première phase de test ou le déploiement ne se fera que sur les ordinateurs du SI
- Une fois le test validé, le déploiement se fera sur toutes les machines du domaine, service par service

Cette phase de test a un double objectif : permettre aux [redacted] de s'habituer à l'usage du gestionnaire de mot de passe, ils pourront ainsi plus facilement aider ou dépanner les utilisateurs rencontrant un problème avec. Puis cela permettra de voir si le déploiement se passe bien tout en vérifiant que la solution est adaptée aux besoins et si cela ne pose aucun souci dans le fonctionnement actuel des services et des usages.

Afin d'avoir le recul nécessaire quant à l'impact du déploiement et laisser le temps aux [redacted] de prendre leurs marques sur ce nouvel outil, la phase de test durera un mois. En fonction des retours, à l'issue de ce mois, KeePass sera déployé globalement.

Pour cette première étape de test, il sera nécessaire de créer une UO ne contenant que les machines de la DSI. Pour ce faire, je procèderai, en accord avec le responsable, à la création d'une UO dans laquelle je déplacerai les ordinateurs du SI. Ma GPO ne sera appliquée que sur cet UO durant la période de test.

Aucune autre GPO n'est présente sur le serveur, le déplacement des ordinateurs n'a donc aucun impact sur l'architecture en production.

Durant cette première phase, le plus long sera sans doute d'accompagner les [redacted] dans l'utilisation et le fonctionnement de ce logiciel tout en prenant le temps d'expliquer l'importance d'une bonne hygiène en matière de sécurité informatique tout en expliquant et détaillant l'intérêt des recommandations de l'ANSSI.

Ce délai me permettra également de rédiger la documentation pour accompagner les utilisateurs durant cette transition. La documentation sera imprimée et mise à disposition à l'accueil et dans les bureaux des différents services et sur le partage de fichiers. Ce document est à but didactique : il contient essentiellement des captures d'écran du logiciel ainsi que des textes explicatifs.

Un second document afin d'expliquer les besoins d'une telle transition sera créé. Ceci a pour but de faire comprendre les enjeux de ce changement à l'ensemble des utilisateurs. L'information est capitale dans le cadre d'un changement d'habitude : les usagers vont plus facilement se plier à ce changement et l'accepter s'ils comprennent de quoi il en retourne. Dans ce document, il sera essentiel d'insister sur le besoin d'améliorer la sécurité informatique en accompagnant mon texte de diverses statistiques sur l'augmentation du nombre de cyber attaques. Je pourrais très largement m'inspirer par celui que j'ai créé lors du projet numéro 4 de la formation, où nous devions faire un slide de 6 pages expliquant les bonnes pratiques à avoir en sécurité informatique.

Ce mois sera donc l'occasion de faire de la pédagogie auprès des employés de [redacted] afin d'anticiper les récalcitrances [redacted] et leur expliquer pourquoi nous faisons cela.

En tout, l'installation de KeePass sur l'ensemble du parc devrait se faire sur deux mois :

- Un premier mois de test
- Un mois pour déployer sur le reste du parc, en prenant le temps d'accompagner les agents des différents services

Concernant le coût, il reste difficile à estimer précisément. Bien que le logiciel soit gratuit, le temps imparti au déploiement, à la rédaction des documents et à l'accompagnement risque d'être onéreux. Un moyen efficace de réduire le coût du au temps serait d'attribuer cette tâche à l'alternant présent. Eventuellement, un stagiaire pourrait l'accompagner pour la partie explicative des documents.

De cette manière, les [redacted] n'auront pas besoin de participer au déploiement, pourrons se focaliser sur le support et les cours numériques de leur planning tout en ayant acquis les compétences et connaissances nécessaires pour le support futur sur KeePass.

La gestion sur le serveur AD peut se faire très simplement puisque la GPO sera déjà créée.

3.2 - Création d'UO sur le serveur Active-Directory

A mon arrivé à [redacted], le serveur AD ne contenait aucune UO (Unité Organisationnelle) permettant de structurer la hiérarchie sur le serveur et de sécuriser les partages de fichiers.

En effet, la gestion des partages de fichiers et d'accès à ces fichiers se faisait en donnant les droits directement à l'utilisateur. Cette méthode, en plus d'être contraire au principe du « moindre privilège » (24) en sécurité informatique est va également à l'encontre des recommandations de Microsoft sur la méthode AGDLP (25).

Outre ces problèmes liés à la sécurité, la maintenance d'un tel système est extrêmement compliquée : il faut, manuellement, vérifier les accès de chaque dossier, de chaque fichier, ne pas faire d'erreur dans l'attribution des droits, etc. Cette méthode est chronophage et la maintenance, en cas de changement d'équipe par exemple, est tout simplement catastrophique.

Pour résoudre ce problème, j'ai proposé la création d'Unité Organisationnelle par service. Les utilisateurs ne seront plus dans le dossier utilisateur présent, de base, sur un serveur AD, mais seront placés dans leur UO respective.

Chaque UO contiendra également un groupe de sécurité global et deux groupes de sécurités locales.

Les utilisateurs seront membres de groupe de sécurité global, puis le groupe de sécurité global sera membre des groupes de sécurité local, selon les besoins d'accès aux fichiers partagés. Deux groupes locaux sont créés : un groupe avec les droits en lecture seule, un groupe avec les droits en lecture/écriture.

Lors de la discussion avec le responsable SI, ce dernier m'a proposé de participer à une réunion regroupant l'ensemble des directeurs des différents pôles. Cette réunion a pour objectif de définir leurs besoins d'accès aux différents dossiers.

Cela nécessitait également une restructuration complète du serveur de fichiers. L'arborescence actuellement en place n'était pas adaptée à une gestion des accès par groupes locaux. Une telle restructuration a bien été commencée, mais les habitudes des droits d'accès par utilisateur et non par groupe a été utilisée. Ce qui fait que, in fine, cette nouvelle arborescence ne présente aucun intérêt pour ce projet.

Pour réellement mettre en place la méthode AGDLP, il faudrait commencer par créer l'ensemble des UO correspondant aux services [redacted]. Puis créer les groupes globaux et locaux nécessaires. Une fois ceci terminé, il faudrait déplacer les utilisateurs existants dans leur UO respectives puis les ajouter en tant que membre de leur groupe global.

Il faudrait également procéder à une refonte du serveur de partage afin que les droits soient donnés aux groupes locaux et non aux utilisateurs. Pour cela, une approche possible serait de dupliquer le dossier de partage existant en le purgeant des droits déjà attribués. Il faudrait ensuite refaire les droits manuellement, pour l'ensemble du dossier, tout en appliquant les mêmes droits à tous les sous-dossiers et fichiers.

Une étape nécessaire et contraignante serait de former les [redacted] à la bonne utilisation d'un fichier de partage : leur apprendre qu'un fichier doit être placé dans le bon dossier pour ne pas qu'ils rencontrent de problème de droits d'accès.

Il existe la possibilité de « mapper » certains dossiers automatiquement pour les utilisateurs faisant partant de tel ou tel service. Cela afin de simplifier l'accès aux dossiers et d'éviter aux utilisateurs de devoir naviguer en aveugle dans un dossier de fichier partagés qui peut être assez conséquent.

Cela nécessite plusieurs mois de travail. Le simple fait de devoir organiser une réunion avec l'ensemble des directeurs de pôle peut prendre deux mois. Chacun n'étant pas disponible quand les autres le sont. De plus, il faut que les directeurs réfléchissent bien à leurs besoins spécifiques. Un important travail de réflexion est indispensable en amont afin de rencontrer le minimum de problèmes quand viendra le temps de créer la nouvelle structure de fichiers.

Une documentation devra également écrite afin d'expliquer très clairement le nouveau fonctionnement. Les utilisateurs auront probablement un temps d'adaptation nécessaire, le fonctionnement n'étant plus le même qu'auparavant : avant, les agents concernés se contentaient d'envoyer un mail au SI pour demander les accès à tel ou tel dossier/fichier, puis nous devions nous connecter sur le serveur AD, aller dans le dossier concerné et attribuer les droits nécessaires sur un ou plusieurs dossiers. Maintenant, cela ne sera plus possible. Pour que les droits soient respectés au mieux, ce sera à la charge de l'utilisateur de bien placé son document s'il veut que les personnes ayant accès puissent le lire et/ou le modifier. Cela peut paraître contraignant, mais c'est obligatoire si nous voulons suivre les recommandations de Microsoft et améliorer la sécurité et la maintenance des utilisateurs du serveur AD.

Une fois ceci terminé, nous pourrons procéder à une sauvegarde de l'ancien système de partage de fichiers, par précaution. La nouvelle structure du partage devra également faire gagner de l'espace disque sur le serveur car beaucoup de doublons existent actuellement. Les gens ayant tendance à toujours copier les dossiers dans plusieurs répertoire différents.

4 — Données et RGPD

Le respect au règlement général sur la protection des données est une obligation légale pour [redacted]

[redacted] a été obligée, de par la nature même du RGPD (26), de désigner un DPO (Délégué à la Protection des dOnnées). Ce DPO doit procéder à un audit global de la protection des données tous les ans. Pour le cas de [redacted] dans laquelle j'ai effectué mon stage, le DPO est l'entreprise [redacted]. Le cabinet [redacted] est géré par Mr [redacted], Expert de Justice en informatique et télécommunication. De fait, il est donc rattaché directement au Ministère de la Justice.

Les procédures de gestion des données et de leur traitement ont été décidées par [redacted].

5 — Conclusions

Ce stage [redacted] fut une très bonne première expérience. Outre l'ambiance générale qui est excellente, la grande diversité des missions et le fait d'arriver lors des travaux de rénovation et de modernisation furent de bonnes surprises.

J'ai ainsi pu apprendre à câbler entièrement une salle en respectant les normes réseau existantes, brasser des baies informatiques complètes. Le responsable m'a également laissé une grande marge de manœuvre et m'a autorisé à faire la configuration des switchs L3 utilisés dans notre salle connectée ainsi que celui de la [redacted]. Bien que les configurations ne soient pas complexes (aucun VLAN, par exemple), cela m'a permis de voir en conditions réelles les attentes et besoins d'une entreprise. Configurer un routeur Wi-Fi fut également une très bonne expérience. Le responsable m'a défini les besoins en amont puis m'a laissé le champ libre sur la façon de faire. Là aussi, il s'agit d'une configuration mise en place pour un usage réel. Il faut donc réfléchir aux différentes sécurités à mettre en place (clé WPA, mot de passe du portail de configuration fort, etc.), à la plage IP et à la façon dont on va attribuer les IP : doit-on mettre un DHCP en place directement sur le routeur Wi-Fi ou doit-on laisser le serveur DHCP de l'Active-Directory s'en occuper ? Le DHCP principal dispose-t-il d'une plage assez étendue ? Quelle adresse devrais-je utiliser en tenant compte des différents réseaux déjà existants ?

Toutes ces questions ont été très stimulantes et mes doutes quant à ma capacité à réussir de telles configurations ont très vite été dissipés grâce à la confiance de mon tuteur et du responsable du SI. Sans compter le plaisir de faire quelque chose qui nous passionne.

Les challenges ont été nombreux et j'ai pu découvrir et apprendre énormément de choses.

Bien que n'étant pas développeur et ne comptant pas le devenir, avoir un projet lié à la programmation fut très intéressant. J'ai ainsi pu redécouvrir un nouveau pan de l'informatique et un langage de programmation qui m'était jusqu'à présent inconnu.

Savoir que le logiciel développé sera quotidiennement utilisé, y compris lorsque j'aurais terminé mon stage, a été une motivation supplémentaire. Lors de ce projet, j'ai vraiment voulu faire quelque chose de fonctionnel, d'évolutif et qui ne semble pas graphiquement daté et les différents retours que j'ai eus de mes collègues ont été très encourageants.

Ces différentes expériences, le fait que j'ai également pu passer du temps avec le technicien extérieur pour parler de configuration réseau, VLAN, etc., m'a conforté dans mon choix de vouloir évoluer vers un poste d'administrateur système & réseau.

Bibliographie

[En ligne]

2. [En ligne] https://www.cobalt.io/blog/cybersecurity-statistics-2024.

3. [En ligne]

4. [En ligne] https://www.proxmox.com/en/proxmox-virtual-environment/features.

5. [En ligne] https://www.fastmail.com/blog/pros-and-cons-of-hosting-your-own-email/.

6. [En ligne] https://en.wikipedia.org/wiki/AGDLP.

7. [En ligne] https://learn.microsoft.com/fr-fr/troubleshoot/windows-client/printing/errors-connect-to-shared-printer-cname-record.

8. [En ligne] https://www.ventoy.net/en/index.html.

9. [En ligne] https://fr.wikipedia.org/wiki/Qt.

10. [En ligne] https://pypi.org/project/PyQt6/.

11. [En ligne] https://github.com/impli-osx/session_manager.

12. [En ligne] https://developer.mozilla.org/fr/docs/Web/CSS.

13. [En ligne] https://pyinstaller.org/en/stable/index.html.

14. [En ligne] https://recherche.data.gouv.fr/fr/categorie/33/guide/modele-de-readme.

15. [En ligne] https://docs.framasoft.org/fr/grav/markdown.html.

16. [En ligne] https://cableorganizer.fr/learning-center/article/quelle-est-la-difference-entre-t568a-and-t568b.html.

17. [En ligne] https://www.shure.com/fr-FR/conferences-reunions/ignite/astuces-pour-viter-l-effet-larsen-des-syst-mes-audio-en-salle-de-reunion.

18. [En ligne] https://www.lemagit.fr/definition/Attaque-par-dictionnaire.

19. [En ligne] https://github.com/danielmiessler/SecLists.

20. [En ligne] https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe.

21. [En ligne] https://keepass.info/.

22. [En ligne] https://cyber.gouv.fr/sites/default/files/IMG/cspn/anssi-cspn_2010-07fr.pdf.

23. [En ligne] https://keepass.info/translations.html.

24. [En ligne] https://www.cyberark.com/fr/what-is/least-privilege/.

25. [En ligne] https://en.wikipedia.org/wiki/AGDLP.

26. [En ligne]