Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE
Diplôme Universitaire de Technologie
Spécialité Réseaux et Télécommunications

Ce rapport est confidentiel

Audit, Perfectionnement et Gestion quotidienne du réseaux informatique de l'unité

Loïc Barbato

OpenEdition Center

Encadrant entreprise : Jean-Christophe Souplet

Encadrant académique : Éric Würbel

2019

Table des matières

Introduction

L'édition numérique ou électronique est quelque chose d'assez récent. Ce n'est qu'en 1971 que la première initiative de numérisation est lancé par Michael hart alors étudiant. Il lance alors le projet Gutenberg qui avait pour objectif de mettre à disposition d'un large public la littérature. C'est dans cette dynamique qu'OpenEdition s'est engagé.

L'entreprise : OpenEdition

OpenEdition est un portail composé de quatre plateformes de publication en sciences humaines et sociales créé par le **Centre pour l'édition électronique ouverte** (**Cléo**). Ce centre, appelé également OpenEdition Center, est une Unité de service et de recherche (USR 2004) sous la tutelle (1) du **CNRS (2)**, de l'**Université d'Aix-Marseille**, de l'**EHESS (3)** et de l'**Université d'Avignon**. Il inscrit son action dans le cadre de la **Bibliothèque scientifique numérique** (**BSN**), initiative du **Ministère de la Recherche français**. Tous ces services sont proposé gratuitement et en accès libre au format html. Un modèle économique a aussi été développé afin de pérenniser les plateformes : le Freemium. Dans ce cadre, une partie des options avancés, telles que le téléchargement en format PDF ou ePub (5), sont payantes . OpenEdition a comme slogan est "***Découvrir le monde. Dans toutes les langues"***.

La construction d'une unité

Tout commence avec la création de la plateforme ***Revues.org*** (devenue ***OpenEdtion Journals*** par la suite) en 1999 par Marin Dacos. On y trouve des centaines de revues en Sciences humaines et sociales. En 2008, la plateforme ***Calenda*** est créé . Elle permet de publier des milliers d'annonces d'événements scientifiques : colloques, journées d'études, séminaires, ainsi que des offres d'emploi et des appels à contribution.

De même, en 2008, la plateforme ***hypothèses.org*** voit le jour, c'est une plateforme de blogging scientifique. Les chercheurs y créent des « carnets de recherches » dans lesquels ils font état des avancées de leurs recherches. La plateforme dispose de diverses instances linguistiques, en allemand et en espagnol, notamment, suite à des partenariats avec la ***Max Weber Stiftung*** pour l'allemand et l'***UNED*** (6) pour l'espagnol.

Enfin en 2013, c'est ***OpenEdition BOOKS*** qui vient compléter ce portail en proposant une publication de livres dont au moins 50 % sont en accès ouvert. Parmi les premiers éditeurs de la plateforme, on dénombre les Éditions de l'***ENS (7)***, les Éditions de l'***EHESS***, les ***Presses universitaires de Rennes***, ***Open Books Publishers***, ***CEU Press (8)***.

À ces plateformes sont adossés des conseils scientifiques afin de définir le périmètre et la qualité scientifique de chaque plateforme.

En parallèle, OpenEdition est devenu une infrastructure de recherche nationale depuis 2016. C'est une initiative publique à but non lucratif soutenue par de grandes institutions de recherche et dont la principale mission est la promotion de l'édition électronique en accès ouvert, OpenEdition inscrit également son action dans le cadre du Comité pour la science ouverte.

Depuis 2016, OpenEdition est lauréat du Plan d'Investissement de l'Avenir (PIA 2 (9)). Pour le PIA 3, l'objectif est la Science Ouverte.

Organisation de l'unité

Comme expliqué précédemment, OpenEdition est passé au fil des années d'une "startup de quelques amis/collègues" à une unité de support et de recherche de près de 60 personnes. Plusieurs réorganisations ont donc eu lieu et des points sont toujours à clarifier (cet audit doit du reste y participer). Actuellement, l'unité est dirigé par une personne entouré de conseils scientifiques (conseils de chercheurs/utilisateurs qui utilisent les plateformes) d'un conseil d'unité (instance représentative des membres de l'unité). Il y a ensuite quatre directeur / trice adjoint / e (Administratif, Informatique, International et Éditorial) qui dirige un secteur (cf. Figure 1 - organigramme de l'unité).

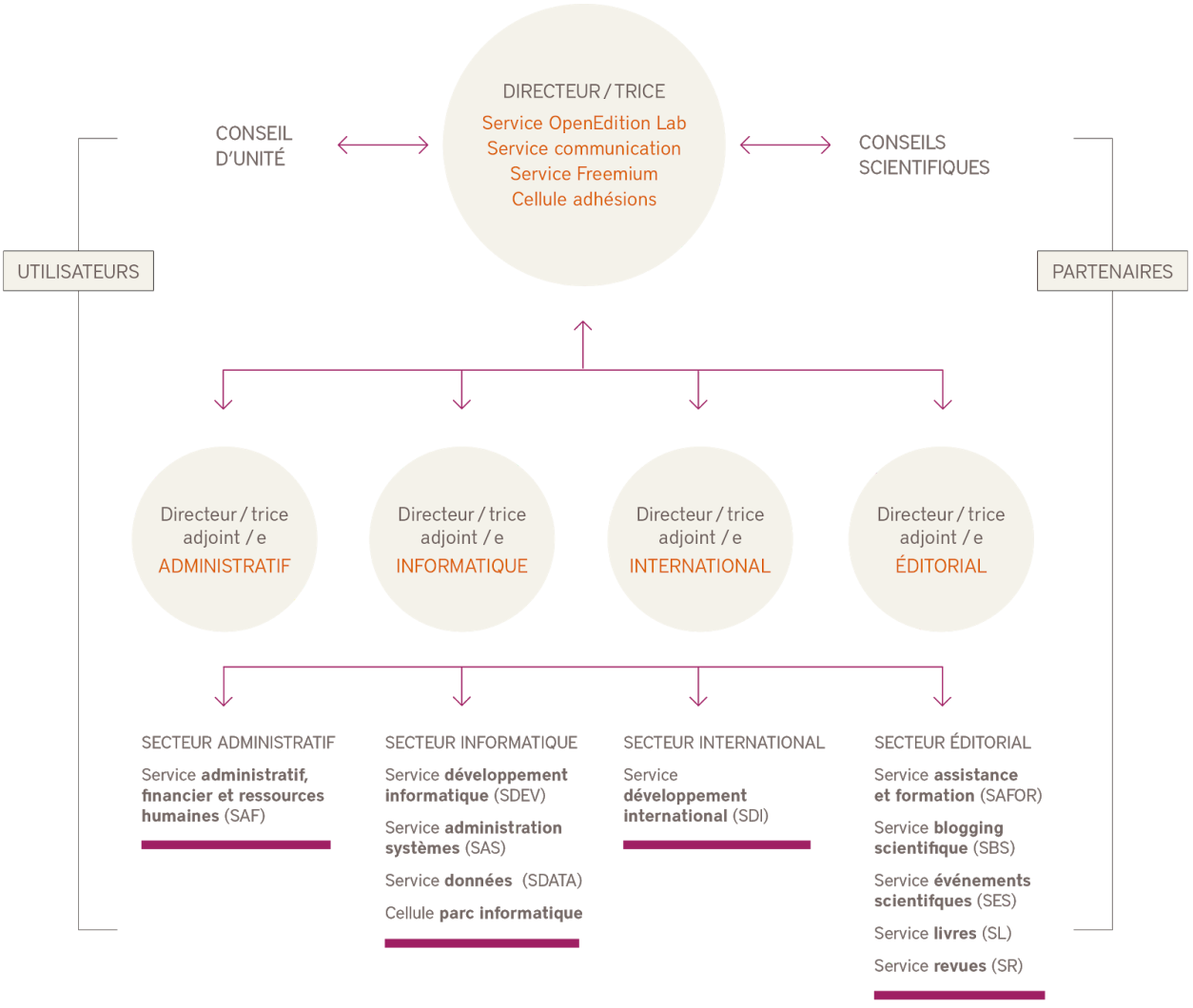


Figure 1 - organigramme de l'unité

Le secteur informatique

Mon stage se déroule au sein du secteur informatique. Comme le montre l'organigramme ci-contre, il est composé de 3 services et d'une cellule :

- le service développement - 4 personnes - développement et maintenance des applications des plateformes, support utilisateurs, développements en réponse au projets nationaux et européens, …
- le service administration systèmes - 1 resp. de service + 1 personne - fiabilité et sécurité du système, garant de la haute disponibilité des plateformes, …
- le service données - 1 resp. de service + 3 personnes - qualité des données, statistiques, respect RGPD (10), ...
- la cellule gestion du parc informatique interne - 1 personne (moi) - inventaire, support utilisateurs, gestion des postes de formation et télétravail, respect consigne CSSI, …

Mon encadrant en est le responsable depuis avril 2019. Ma mission d'audit s'inscrit donc dans le cadre de sa prise de fonction.

Concernant la cellule gestion du parc interne, la personne qui y était en CDD n'a pas pu être renouvelée fin avril 2019.

SECTEUR
INFORMATIQUE

Jean-Christophe Souplet, IR, CNRS
Directeur adjoint pour l'informatique

SERVICE DÉVELOPPEMENT INFORMATIQUE

Yara Delgado-Herrara, IGE, AMU
Développeuse

Roland Haroutiounian, IE, CNRS
Développeur

Hélène Prieto, IR, CNRS
Développeuse

Alexandre Vinogradov, IE, CNRS
Développeur

SERVICE ADMINISTRATION SYSTÈMES

Bruno Cénou, IE, CNRS
Responsable du service

Florentin Clouet, IE, CNRS
Administrateur systèmes et réseaux

SERVICE DONNÉES

Mélanie Carmona, IE, CNRS
Chargée de projets données

Clément Corbin, IGE, AMU
Chargé de referencement

Anne Durand, IR, CNRS
Développeuse

Jean-François Rivière, IE, CNRS
Responsable du service

CELLULE PARC INFORMATIQUE

Poste vacant
Gestionnaire du parc informatique

Mes missions

Problématiques

Avec sa prise de poste et le départ du gestionnaire de parc (en CDD ne pouvant être renouvelé dans l'immédiat), mon responsable a besoin de faire un point sur la situation afin de décider de la conduite à tenir. Tout d'abord, il est important de bien décrire et documenter la situation existante. Il faut ensuite confronter celle-ci à la théorie (dont la formation que j'ai reçue à l'IUT) et aux cadres réglementaires (légaux ou des tutelles de l'unités). Des préconisation pourront alors en découler et un arbitrage pourra être réalisé par la direction en tenant compte également des contraintes (ressources humaines, budgétaires, etc…).

En parallèle avec le départ du gestionnaire précédent, le support quotidien informatique ne peut plus être assuré. Une aide ponctuelle pour les besoins urgent est aussi la bienvenue.

Deux tâches principales

Des problématiques précédentes, 2 tâches ressortent ; en voici, une définition :

Audit du système d'information interne : Un audit permet d'évaluer les risques potentiel dans un environnement, dans notre cas, les environnements informatique peuvent être la sécurisation d'un poste de télétravail ou une vérifications de sécurité (mot de passe, fiabilité d'une application). Il peut viser plusieurs domaines d'étude comme le montre les quelques exemples suivant, la partie physique avec par exemple la vérification des accès d'un bâtiment ou d'une salle, la partie logiciel qui consiste à tester ses limites pour y trouver une faille ou même une partie personnels dans laquelle on retrouve des interrogatoires, des vérifications sur la sauvegarde des mots de passes (pas de papier indiquant le mot de passe sur le poste en question).

Rôles d'un gestionnaire de parc informatique : Le gestionnaire de parc va devoir, comme son nom l'indique, gérer tout le parc informatique. C'est à dire qu'il va avoir pour mission le support utilisateur, la gestion de l'inventaire, des mises à jour, la sécurisation des données ou bien l'ensembles des logiciels et des applications.

Son rôle principal va être de s'assurer du bon fonctionnement de son parc informatique pour qu'aucun événements ne viennent perturber le travail des employés. Si son travail est correctement effectué, il y aura une prévention des défaillances et permettra de réduire les coûts de fonctionnement du système de l'entreprise.

Application dans le cadre d'OpenEdition

La mission principale qui m'a été confiée et pour laquelle j'ai passé le plus clair de mon temps est le confectionnement d'un audit de perfectionnement du réseau informatique de l'unité.

Lors de cette mission, j'ai dû effectuer:

- Un état des lieux, en faisant une vérification du matériel, des licences et des besoins.
- Définir des préconisations d'évolution en prenant en compte les réglementation des tutelles et de lois tel que le RGPD.
- Lors de mon retour dans l'entreprise, je devrai mettre en place certaines de ces préconisations en fonction du temps qu'il me restera.

Mes autres missions ont été de gérer le parc informatique : support utilisateur, inventaire, ...

Enfin et pour avoir une mission plus technique (en attendant la réalisation de préconisations), il m'a été demandé de mettre en place des pages d'affichage d'informations sur un écran d'accueil dans le hall du bâtiment.

I. Audit du système d'information interne

Dans cette partie, nous verrons comment j'ai pu mettre en place l'Audit et quelles ont été les difficultées rencontrées. Par exemple, la réalisation d'un audit était quelque chose de nouveau pour moi. De même, j'ai dû prendre en compte le temps de travail du personnel et travailler sans les gêner. Je vais donc commencer par vous présenter la partie découverte de l'environnement avec la découverte de l'entreprise et ses modes de fonctionnements, puis les préconisations en découlant (définies en plusieurs catégories).

A. Découverte de l'environnement

La découverte de l'environnement fût quelque chose de compliqué pour moi au début, d'une part parce que je devais découvrir comment toute la structure fonctionne et d'autre part car je ne connaissais pas vraiment l'équipe, même s'ils m'ont tous bien accueilli et m'ont permis de m'intégrer très rapidement.

J'ai donc commencé avec le gestionnaire de parc, la personne en CDD sur le poste de gestionnaire de parc (avant moi) et avec qui j'ai pu échanger lors des deux premier jours de mon stage avant la fin de son contrat. Il m'a expliqué globalement comment était effectué son travail, à quelles missions quotidiennes il pouvait avoir à faire. Il m'a présenté les quelques logiciels qu'il utilisait puis il m'a présenté le serveur d'affichage dynamique Xibo (Annexe 1) qu'il a mis en place. Par la suite j'ai effectué mes propres recherches pour étudier les autres points. Pour se faire, j'ai été amené à poser des questions au personnel, passer dans leur bureau et étudier le matériel (Annexe 2).

A la suite de quelques semaines, quelques rendez-vous et de mes premiers retours, j'ai fixé avec mon encadrant les points d'étude suivants :

1. Postes Informatiques

Dans cette partie j'ai traité tout ce qui concerne les ordinateurs. Je vais vous présenter ces éléments, en les complétant par ce qui pour moi fait défaut.

a) Postes fixes

Concernant les Postes Fixes, il y a pour la plupart de ces postes deux comptes minimum, un compte utilisateur et le compte admin CLEO. Malheureusement, ces postes ne sont pas dans un domaine ce qui ne permet une sauvegarde des sessions utilisateurs. Pour contrer ce problème, un système de redirection du dossier "Mes documents" a été mis en place.
Point positif la session admin permet la gestion du poste sans avoir d'impact négatif pour l'utilisateur, ni de besoin d'accès au mot de passe de l'utilisateur pour accéder au poste, ce qui renforce la protection des mots de passe.

Autre point à aborder c'est le compte administrateur, il permet à un administrateur d'accéder à la session sans avoir besoin du mot de passe de l'utilisateur. Maintenant, il faut aussi savoir que chaque utilisateur possède actuellement tous les droits administrateurs sur le poste. Ce qui implique l'installation de logiciel et un control total de son poste, il pourrait par exemple enlever la session admin. Autre possibilité, l'installation non voulue d'un logiciel malveillant qui pourrait impacter tous les autre postes (ex : ransomware).

b) Postes de formations

Pour les Postes Formations, se sont des postes qui ne sont pas nettoyé et dans lesquels on peut y retrouver toute sorte de choses comme des comptes Gmail (de formation précédente ou du personnel), des photos ou bien des documents de travail du personnel. Ces Postes ne sont pas toujours mis à jour et le mot de passe censé être le même pour tous, n'est lui non plus, pas actualisé. De plus ces PC étant en accès autorisé pour le personnel dans le cadre du télétravail, des besoins de dernière minutes et des conférences, ils sont vite modifiés, adaptés par l'utilisateur (personnel). La configuration des PC est alors modifiée et, ils perdent leur "base" propre (être identique) pour les formations. Ils ne possèdent qu'une seule session qui sert pour toutes ces utilisations, ce qui d'un point de vue sécuritaire ne devrait pas être le cas.

c) Postes de télétravail

À propos des Postes de Télétravail, que ce soit des postes appartenant aux employés ou à l'entreprise, des ordinateurs fixes ou portable, ils sont configurés avec l'accès au VPN de l'entreprise et la messagerie instantané.

2. Réseaux

Concernant l'administration du réseaux informatique, tout est géré par Aix-Marseille Université et plus précisément son service informatique la DOSI (Direction Opérationnelle des Systèmes d'Information).
Les quelques points suivants sont donc concernent donc la partie "visible" chez OpenEdition.

a) Wifi

Il y a 5 bornes Wifi disposé dans le bâtiment, quatre de ces bornes sont des Linksys E2000 et la dernière est une Linksys WRT54GL (cf images ci-contre). Elles sont placées chacunes à une vingtaine de mètres l'une de l'autre et réparties sur les deux étages. Elles ne sont pas cachées dans le faux plafond mais posées sur le sol ou sur des tables. Chaque borne est indépendante et proposent un Wifi différent de l'autre. Mise à part le mot de passe (scotché sur chaques bornes et dans certaines pièces), il n'y a aucune sécurité, aucun vlan ou aucun autre moyen de control sur les personnes présentent sur le Wifi.

b) Ethernet

Il y a actuellement aucune restriction sur le réseau, ce qui signifie qu'une personne qui connecte un ordinateur sur une prise RJ45 peut accéder librement à internet et au réseau de l'entreprise.

c) Vlan

Le manque de Vlan pour pouvoir segmenter et contrôler l'entreprise reste quelque chose de problématique. En effet, si une personne accède au réseau par Wifi ou par une connection direct, elle aura un accès total sur celui-ci. Cela peut engendrer des problèmes de sécurité si une personne mal intentionné y accède lors d'une formation par exemple ou, autre cas de figure, suite à l'infection d'un PC portable (télétravail par exemple), une personne ou un virus pourrait se propager sur tout le réseau. Il faut aussi prendre en compte les différents besoins de chaque services, le secteur informatique ne devrait pas avoir de limite sur le téléchargement. C'est à eux d'effectuer des mises à jour ou des installation tandis que le service livre, par exemple, n'a pas de besoin particulier. Selon moi, il faudrait donc pouvoir effectuer, en fonction des besoins de chaque service, un ajustement de la bande passante (ceci reste à discuter avec mon encadrant). Actuellement pour effectuer une mise à jour de windows, le temps peut-être de 2 à 5 minutes de téléchargement ou d'une heure.

De plus, si on prend en compte les besoin de l'administration, il faut pouvoir les séparer du reste de l'entreprise par sécurité.

d) Wifi Eduroam

La question concernant la non présence du service Eduroam est à se poser. Ce service permettrait un accès sans fil sécurisé à l'Internet aux personnels de la communauté enseignement supérieur et /recherche. Le mettre en place au sein d'OpenEdition serait donc un plus. Ce point sera à aborder avec la DOSI.

3. Informations générales

a) Informations liées au personnel

Au niveau de la gestion du personnel, nous avons pu voir avec l'arrivé de stagiaires (y compris mon arrivé), le départ du gestionnaire de parc et l'arrivé de nouveaux membres du personnel que certaines procédures étaient déjà en place. Elles ont des avantages comme des inconvénients.

Dans le cadre de l'arrivée d'un nouveau membre du personnel ou d'un stagiaire, la procédure est que le/la chef de service prévient deux semaines à l'avance le service RH pour que la création de son compte Google, la mise en place d'un poste de travail et la création de son compte LDAP soit lancés. Le compte LDAP lui permettra un accès au serveur de fichier interne et une connection aux différents services comme Redmine (Annexe 3).

Dans le cadre du départ d'une personne, la procédure devient un peu plus floue, cela prend un peu de temps avant la suppression complète des données concernant cette personne. C'est à dire que son compte Google n'est pas supprimé immédiatement et son espace personnel sur le serveur de fichier non plus, il faut récupérer les données et vérifier qu'aucun documents en cours, importants soit perdu. Pour son poste de travail, il en revient au gestionnaire de parc de faire une vérification avant de le réinitialiser.

b) Informations liées au gestionnaire de parc

Ce point était une demande de mon encadrant, il visait à participer à la réflexion sur l'avenir de la cellule "gestion du parc" au sein d'OpenEdition.

Après avoir passé presque deux mois dans l'unité, j'ai du passer au moins la moitié de mon temps à m'occuper de support utilisateur, avec la préparation de formations (mise en place de la salle et du câblage), des problèmes internes tel que l'installation de logiciel (ex : Geslab) ou le renouvellement de licences, la mise en place du télétravail et de son support, … . Il faut en plus de ces opérations ajouter la gestion de l'inventaire et du matériel, la préparation de nouveaux postes de travail et de demandes tel que la conférence Elpub (11). Il est donc, pour moi, nécessaire que cette cellule soit maintenue pour éviter des problèmes technique, de plus la perte de ce poste provoquerait une augmentation de travail pour les autres services du secteur informatique.

Si la cellule perdure, on pourrait par contre lui confier de nouvelles responsabilités avec la coordination du système d'information interne à l'entreprise : mise en place d'un serveur de domaine, coordination des création de compte ldap, mail, … .

4. Sécurité

Dans cette section, nous verrons la partie sécurité. C'est à dire tout ce qui concerne la protection contre le vol du matériel, le cryptage du matériel selon le Règlement Général de la Protections des Données (RGPD) et les réglementation du CNRS et la sécurité physique.

a) Chiffrement / Cryptage (RGPD et règlement du CNRS)

Selon des notes et des mails interne du CNRS, leur réglementation concernant le chiffrement des postes est sans appel, tous les postes (PC fixes, PC portables, Smartphone et autres) qui contiennent des fichiers professionnels doivent être chiffré. Cette directive semble très peu respecté, en effet si l'on prend la totalité des ordinateurs fixes présent dans le bâtiment, il doit y avoir moins de 10 postes qui sont actuellement protégés par BitLocker ou VeraCrypt sur un total d'environ 75 postes. Cela représente, dans le meilleur des cas, seulement 13% d'ordinateurs cryptés, on est bien loin des 100%. Maintenant, si on regarde la partie des ordinateurs portables, on obtient un score presque égal, sur la totalité des postes portables, il n'y en a qu'une quinzaine qui sont chiffré sur environ 65 postes soit au mieux 23% des ordinateurs.En ce qui concerne le RGPD, les données du personnel sont sécurisées. Il y a par exemple une vérification effectuée sur les mail à risque.

b) Gestion et protections des mots de passe

On peut observer différents problèmes concernant les mots de passe et leurs divulgations. Les deux types de divulgations de mots de passe suivant sont des exemples que j'ai pu trouver :

- La première par sauvegarde d'un fichier contenant des mots de passe (Annexe 4).
- La deuxième les mots de passe écrit sur l'ordinateur ou à côté (écran, bureau, Post-it).

Au delà de ces problèmes, la connaissance par toute l'entreprise du mot de passe administrateur le rend inutil et surtout donne l'accès à certaines fonction dont les utilisateurs ne devrais pas disposer.

c) Sécurité en cas d'intrusion dans le bâtiment (vols de matériels)

À l'heure actuelle, seul l'ordinateur de mon encadrant est protégé par des câbles de sécurité. Selon moi, on s'aperçoit donc que sur l'ensemble des postes, la question de la sécurité du matériel n'a pas été pris en compte. De plus, il faut aussi savoir que lors de la conférence Elpub, aucun kits de sécurité n'a été déployé sur place pour la protection des ordinateurs portables, la simple précaution prise a été leur stockage dans une pièce fermé à clef. Concernant cette conférence, nous en avions discuté mais l'absence de ces kits nous a limité.

B. Préconisations définies suite à l'état des lieux

Dans cette partie, nous verrons les préconisations que j'ai pu effectuer suite à l'état des lieux, mes connaissances personnel et des recherches effectuées pour valider des points à améliorer comme pour le RGPD ou le chiffrement.

1. Postes Informatiques

Concernant les postes, la préconisation principale est de mettre en place sur les ordinateurs où ce n'est pas le cas, le compte administrateur CLEO ce qui permettra une totale gestion des postes sans avoir besoin des mots de passe du compte local de l'utilisateur.

Je pense aussi qu'il faut mettre en place un serveur de mises à jour à distance tel que le rôle WSUS (Windows Server Update Services) qui permet d'effectuer les mises à jour de Windows de ses logiciels (ex : Word, Excel, …). Maintenant pour avoir quelque chose de plus complet et pour pouvoir effectuer les mises à jour de tous les logiciels utilisés (Adobe Creative Cloud, …), Windows propose des outils tel que :

- Remote Desktop Services (RDS) il a comme inconvénients de ne pas supporter tous les logiciels et les applications doivent être d'abord installées sur le serveur avant d'être distribué malgré tout, il ne nécessite pas de matériel haut de gamme pour son utilisation.

- GPO (Group Policy) qui est une extension du Windows Server permettant de mettre en place ces installations ou mises à jour pour un groupe d'utilisateur, c'est un moyen sécurisé de déploiement sur le réseau mais reste compliqué à organiser et gérer pour un grand nombre de GPO. Il peut aussi être lié avec Active Directory (AD), un domaine ou une unité d'organisation (UO).

- System Center Configuration Manager (SCCM) qui permet de gérer de grand parcs d'ordinateurs, il offre aussi de nombreuses autres options comme la prise en main à distance, la possibilité d'un inventaire matériel et logiciel ou le déploiement de systèmes d'exploitation complets. Ce logiciel de gestion de système à un prix, 1323 $ (1 177 €) pour un achat de licence System Center et pour deux serveurs.

Les autres solutions sont externes à Microsoft :

- Citrix Managed Desktop est un des nombreux services proposé par Citrix, il convient pour un grand nombre d'applications mais il est très coûteux et le produit peut arriver en fin de vie ce qui veut dire qu'à un moment, il n'y aura plus de support.

- PDQ Deploy est un outil de déploiement de logiciels qui peut, en étant installé sur un ordinateur (celui du gestionnaire de parc par exemple) déployer à distance des applications ou des correctifs mais il peut aussi permettre de planifier des tâches ou exécuter des scripts. Il est gratuit et payant (pour accéder à toute les fonctions il faudra débourser 500 $ (445 €) par administrateur) et malheureusement certaines options tel que la planification ou la gestion automatique ne sont pas disponible dans la version gratuite.

Je préconiserais donc l'utilisation de SCCM qui apporte pour moi le plus d'avantage, maintenant son prix peut être un obstacle. C'est pourquoi l'utilisation de l'extension GPO sur un Serveur Windows me paraît convenir à l'entreprise. De plus cela permettrait l'implantation d'un contrôleur de domaine qui pourrait, en plus d'offrir plus d'options, permettre de ne plus passer par un prestataire concernant l'annuaire LDAP et réduire les coûts dans le temps.

2. Réseaux

Pour le réseau, il faut pour commencer, prendre rendez-vous avec la DOSI (12) pour un explication plus détaillé de leur infrastructure. Ensuite, il faut mettre en place une attribution d'adresse IP par adresse MAC pour verrouiller les entrées sur le réseau. Puis il faudra mettre en place des VLANs pour pouvoir administrer le réseau et définir les droits d'accès, la bande passante, …; nous pouvons prendre l'exemple des postes de formation, ils ne devraient pas être dans le même réseau que le secteur administration. Il en va de même pour leurs besoins, une utilisation pour les formations peut avoir pour conséquence un simple accès WEB et bloquer le reste.

Pour les bornes WIFI, elles ne devront former qu'un seul et même réseau pour éviter la déconnection ou la perte du signal en traversant le bâtiment. De plus il faudrait pouvoir les cacher dans le faux plafond ou un endroit qui éviterait le débranchement involontaire ou une connection au port console.

En ce qui concerne le service Eduroam, il faudrait aussi pouvoir le mettre en place pour proposer accès sans fil sécurisé à l'Internet aux personnels et aux étudiants de la communauté enseignement supérieur/recherche.

3. Informations générales

Pour le personnel, il est donc évident, selon moi, qu'il faut mettre en place une manière plus efficace le traitement des données lors du départ d'un membre du personnel ou d'un stagiaire. La mise en place de cette procédure pourrait réduit les coûts des comptes Google et permettre de régler au plus vite la partie données utilisateur lié au RGPD concernant les adresses mail (prénom.nom@entreprise.com) et les numéro professionnel attribué au personnel. L'ajout du traitement de l'ancien poste (mise en place d'une image d'un poste vierge) pourrait aussi permettre l'effacement des données utilisateur et être utilisation pour les postes de formations à la fin de chaque formation.

De mon point de vue, la cellule gestionnaire de parc doit perdurer pour pouvoir assurer une aide permanente aux utilisateurs qui peuvent avoir à tout moment un problème technique. De plus elle est essentielle pour assurer la gestion de l'inventaire, des mises à jour et de l'achat ou du renouvellement des licences, une tâche qui est effectuée toute au long l'année. Il ne faut pas oublier que cette cellule doit aussi s'occuper des installations de postes (stagiaire ou personnel) et de la mise en place du télétravail. Sans cette cellule, toutes ces missions devront être réaffectées. Or le reste du personnel a déjà ses propres missions et il faudra donc que chacun (secteur informatique ou non) participe. C'est donc pour éviter cela qu'il me semble indispensable que la cellule "gestion du parc informatique" soit conservée.

4. Sécurité

Du point de vue de la sécurité, de gros progrès sont à fournir. Respecter les règles du CNRS et du RGPD est dans les priorités. Il faut au plus vite mettre en place le chiffrement de tous les postes utilisé par le personnel.

Pour la sécurisation des mots de passe, il faut évidemment supprimer le mot de passe administrateur et en définir un nouveau et éviter de le divulguer au personnel. Une demande au membre du personnel doit être effectué afin de ne laisser aucun mots de passe visible à côté de leur poste et bien sûr éviter de les stocker dans un simple fichier Word.

Le matériel doit lui aussi être sécurisé de manière physique pour éviter les vols lors d'évènements (comme déjà arrivé) ou dans le bâtiment. L'entreprise doit donc acquérir un grand nombre de câble de sécurité pour pouvoir protéger ses écrans et ses postes.

II. Gestionnaire de parc informatique

Dans cette partie, nous verrons le travail quotidien que j'ai effectué auprès des employés, avec dans un premier temps le support utilisateur avec les interventions journalière, les problèmes rencontrés … , puis un point plus approfondi sur l'inventorisation et la gestion du parc avec les contraintes que cela engendre.

A. Support utilisateur

En tant que gestionnaire de parc, j'ai dû faire face à plusieurs problèmes concernant les utilisateurs. Nous allons voir, dans cette partie, comment j'ai pu effectuer cette mission quelles ont été les difficultées rencontrées, comment elles ont été surmontées et quelles sont les différentes tâches sur lesquelles je suis intervenu.

Comme expliqué précédemment, à mon arrivé chez OpenEdition, j'ai pu profiter de deux jours avec le gestionnaire de parc qui était le gestionnaire du parc informatique avant moi, il finissait son contrat fin avril. Il m'a donc présenté son métier qui, pour moi, était une première. Ma mission était simple, récupérer le plus d'information auprès du gestionnaire de parc tel que les mots de passe d'administration ou ceux des appareils (imprimantes, serveur d'affichage ,…). Lors de mon deuxième jour, le gestionnaire de parc m'a confié la configuration de deux postes de télétravail.

1. Préparation de postes de télétravail

La mise en place du télétravail chez OpenEdition est assez récent. Qui dit quatre tutelles, dit quatre entités pouvant mettre en place le télétravail avec chacune ses employés et ses modalités. Il faut donc pouvoir respecter les demandes et leurs conditions (en sécurité pour les données, …).

Toutes les demandes sont effectuées dans un ordre précis, la demande est faite par l'agent (l'employé voulant effectuer du télétravail) auprès de sa hiérarchie (son/sa responsable de service) grâce à une fiche de demande de télétravail qui va ensuite la faire remonter à l'administration de l'entité de l'agent pour que cette demande soit étudiée. Puis après sa validation, un ticket sur Redmine est alors créé par son/sa responsable qui va indiquer le(s) jour(s) de télétravail. Dès ce moment, mon travail est de préparer le pc, qu'il appartienne à l'agent ou à l'entreprise.

Les deux ordinateurs que j'ai du préparer lors de mon deuxième jour sont des ordinateurs "formation" c'est à dire que ce sont des postes portables utilisés lors des formations qui se déroulent dans nos locaux. Il a fallu effectuer un chiffrement de ces ordinateurs, pour cela j'ai utilisé Veracrypt (Annexe 5) qui est une demande du CNRS. Le chiffrement d'un ordinateur permet de sécuriser les données qui sont à l'intérieur, vous pouvez choisir plusieurs possibilitées, le chiffrement complet du disque qui permet de bloquer l'accès (la demande du mot de passe se fait au démarrage), le chiffrement partiel d'un disque qui peut être représenté par le chiffrement d'une partition (mot de passe demandé pour l'accès à cette partition), le chiffrement d'un dossier ou d'un fichier (mot de passe demandé pour l'accès au fichier ou dossier).

Nous avons donc choisi un chiffrement complet pour pouvoir tout sécuriser, cela prend, selon la quantité de données à chiffrer, plus ou moins de temps, dans notre cas environ 45 minutes même si ces ordinateurs ne contenaient que peu de données (± 60 Go). Une fois le chiffrement fini, je me suis occupé de la création des sessions du personnel puis, une fois cette tâche effectué, il reste l'installation des logiciels. Dans les logiciels utilisé, on retrouve une partie commune à tous les employés, elle est composée de la suite office (Word / PowerPoint / …) de la messagerie instantanée (Pidgin Annexe 6) et du client VPN (13) (OpenVPN Annexe 7). Une fois ces installations terminé, il reste les demandes spécifique au personnel (Financier / Développement / …). Pour finir, j'ai du effectuer, auprès des deux personnes concerné, une démonstration concernant la connection au VPN, puis vers le serveur de fichiers et présenter les raccourcis.

Par la suite, j'ai effectué d'autres demandes de télétravail ou de modification de poste de télétravail en raison de soucis technique sur un macbook pro par exemple. Il faut savoir gérer ces demandes en avance pour ne pas être pris au dépourvu la veille du jour de télétravail de l'agent.

2. Support quotidien

En règle générale, il y a au moins une personne qui passe demander de l'aide par jour. Les demandes sont toutes différentes. Il faut donc se préparer à tout. Dans la majorité des cas, la demande peut être traité en moins de 30 minutes, mais il arrive que la demande prenne plus de temps et qu'il faille s'en occuper au plus vite pour éviter tout dérangement ou alors il faut mettre en place une solution temporaire pour que la personne puisse continuer de travail (ex : prêt d'un ordinateur portable).

Parmis les demandes les plus fréquentes, on retrouve les installations de logiciels, cela prend en général une dizaine de minutes. J'ai aussi eu des utilisateurs qui ne pouvait pas se connecter à leur session à cause d'une demande de renouvellement du mot de passe qui ne voulais pas s'effectuer. Dans ce cas, la solution était simple car deux choix sont possibles (en passant par le compte administrateur) :

- Soit on effectue le changement de mot de passe par le panneau de configuration et donc avec une interface graphique.
- Soit on utilise la console Cmd (Command prompt ou invite de commandes) en administrateur et on rentre la commande net user "***Nom d'utilisateur***" "***Nouveau mot de passe***"

Après avoir changer le mot de passe l'utilisateur peut se reconnecter.

On peut être aussi confronté à des problèmes plus "complexe" comme lors des mises à jour des postes de formations, une des mises à jour Windows, sur l'un des postes n'a pas voulu s'effectuer. À ce moment là, il suffit de contourner le service de mise à jour en la récupérant directement sur le site de microsoft et en effectuant l'installation manuellement.

3. Installation en tout genre

Au sujet des installation, j'ai été confronté à différentes demandes d'installations. Il y avait des installations classique avec la mise en place d'un nouveau poste utilisateur lors de l'arrivé d'un nouveau membre du personnel et les installations pour les formations.

Dans le cadre d'une installation de poste, il faut simplement mettre en place le compte administrateur CLEO, puis le compte de l'utilisateur. Enfin, il reste les logiciels de base (Word, Adobe, …) puis Kaspersky (Annexe 8) (l'antivirus fournit par le CNRS).
Le chiffrement du disque dur doit aussi être effectué pour se conformer au règlement du CNRS.

Dans le cadre de l'installation de la salle de formation, il faut préparer les ordinateurs (remise à zéro des données utilisateur), puis il faut mettre en place le câblage électrique et mettre en place la connection au réseau.

B. Inventaire et gestion du parc informatique

Dans cette partie, je vais vous expliquer en quoi consiste la gestion de l'inventaire et du parc informatique.

1. Vérification du matériel

Pour commencer l'audit, j'ai dû effectuer une vérification du matériel. Pour cela, il fallait commencer par vérifier le matériel en stock, une chose rapidement effectué car tout était dans la même pièce. En suite, il m'a fallu faire une vérification de chaque poste, j'ai commencé par les ordinateurs portables en faisant, en plus d'un check up sur l'inventaire déjà effectué, une vérification de chaque poste pour savoir s'il était à jour, quels logiciels étaient installés dessus et si l'antivirus était mis à jour. Puis en effectuant mes passages liés au support utilisateur et en échangeant avec mes collègues, j'ai pu approfondir cet inventaire.

Le problème auquel j'ai dû faire face était la vérification du matériel de Paris, en effet des personnes sont en postes dans l'école de l'EHESS à Paris et ont du matériel sur place mais pour le vérifier et en apprendre plus sur les procédures (installation, dépannage, …) j'ai dû effectuer une réunion avec eux par visioconférence avec Hangouts (un service de Google).

2. Achats et renouvellement de licences

Concernant les licences, je suis tombé face à un véritable problème. Pour commencer, je devais savoir si certaines demandes de renouvellement avaient traité ou non. Puis après plusieurs réunions, nous avons dû déterminer si les licences à renouveler avait une utilitées, je me suis donc penché sur le sujet et j'ai effectué une "enquête" auprès des utilisateurs de ces licences. Sur les quatre types de licences, nous avons décidé d'en renouveler deux avec le même contrat, pour un type un autre contrat a été prévu pour mieux s'adapter à nos besoins (et, par la même occasion, faire une légère économie), et pour le dernier type de licences, elle n'a pas été renouvelé car jugé inutile.

3. Commandes de matériels

À propos des commandes de matériels, nous n'en avons pas effectué une seule. Nous voulions éviter le surplu de commandes et pouvoir mettre en place des prioritées pour les achats de matériel. En effet, le gestionnaire de parc s'occupait de cela et le personnel venaient le voir pour lui demander de commander tel ou tel chose. Malheureusement, le budget n'étant pas illimité, il faut dès à présent mettre en place une procédure d'achat pour éviter le surplus de matériel ou la commande d'objets de peu d'importance.

Mon travail fut donc d'établir une liste d'achat avec les besoins nécessaires (comme les câbles de sécurité) puis après avoir préparé cette liste, prendre en compte les demandes du personnel et les noter pour en étudier l'intérêt. Une fois la liste établie validé, nous pourrons alors lancer la commande du nouveau matériel.

III. Conclusion et poursuite du stage

J'ai donc pu, dans ces deux mois, réaliser un bonne partie des mission qui m'ont été attribuées. J'y suis arrivé grâce avec mes collègues et mes connaissances. J'ai ainsi effectué un état des lieux, et rédiger mes premières préconisations.
Mon objectif étant de permettre une évolution aussi bien matériel que dans les pratiques chez OpenEdition. Les améliorations que j'ai préconisées seront, selon moi, bénéfiques pour les employés et pourront être durables. Lors de leur mises en place, je veillerai à les détailler le plus possible et à ne pas gêner les autres employés.

Malgré les quelques problèmes rencontrés, j'ai pu apprendre après avoir effectué des recherches et être bien entouré pour l'exécution de mes missions.

J'ai donc, par ce stage, appris beaucoup de choses tant sur le savoir que sur le savoir-faire. ceci a été permis grâce au connaissances acquises au sein de l'IUT Réseaux et Télécommunications.

Suite à ces deux mois, j'ai également pu découvrir le fonctionnement d'une unité de service et de recherche et découvrir ce milieu qu'est la recherche.

Actuellement, il me reste encore cinq semaines à passer au sein d'OpenEdition. Mes objectifs vont être de finir mon rapport d'audit et mes préconisations. Il faudra ensuite présenter ce travail en interne et obtenir un classement des préconisations à mettre en place. Selon le temps restant, je pourrai alors mettre en place ces préconisations.

Enfin et en écrivant les dernières lignes de ce rapport, j'apprends qu'OpenEdition me propose de poursuivre avec eux l'an prochain et d'y faire mon année d'apprentissage de licence, ce que j'ai accepté. Ceci me paraît donc être la meilleure conclusion de ce stage.

IV. Remerciements

Je tiens à remercier toutes les personnes qui m'ont permis de réaliser avec succès mon stage. Plus particulièrement, je voudrais remercier l'équipe pédagogique de l'IUT ainsi que Marie Pellen, Directrice d'OpenEdition.

Je tiens à remercier mon encadrant de stage, **Jean-Christophe Souplet, Directeur Adjoint et Responsable du Secteur Informatique au sein OpenEdition**, pour son accueil, son aide tout au long du stage, de sa confiance et du temps qu'il a pu m'accorder.

Pour finir, je tiens à remercier toute l'équipe d'OpenEdition pour leur accueil et la bonne humeur.

V. Glossaire

(1) Tutelle, Une unité de recherche ou un laboratoire peut être affilié à une ou plusieurs tutelle. Ce sont des établissements d'enseignement supérieur ou des organisme de recherche comme le CNRS. Ils sont alors responsable des comptes bancaire, des locaux et ont un fort pouvoir de décision.

(2) CNRS, Centre National de la Recherche Scientifique

(3) EHESS, l'École des Hautes Études en Sciences Sociales

(4) Freemium, C'est un mot valise qui combine "free" (gratuit) et premium (prime). C'est une stratégie commercial qui vise à attirer des utilisateur par des services gratuits ou en libre accès, pour leur proposer des options payantes.

(5) ePub, Electronic publication (publication électronique) format pour les livres numérique.

(6) UNED, Universidad Nacional de Educación a Distancia
(Université Nationale d'Enseignement à Distance)

(7) ENS, l'École Normale Supérieur

(8) CEU Press, Central European University Press
(Presse universitaire de l'Europe centrale)

(9) PIA, Plan d'Investissement de l'Avenir est un programme d'investissement de l'État français. Il regroupe plusieurs domaine comme la recherche et l'enseignement supérieur.

(10) RGPD, Règlement général sur la protection des données, c'est un règlement Européen pour la protection des données à caractère personnel. Il est en vigueur depuis le 24 mai 2016.

(11) Elpub, Elpub est une Conférence internationale de l'édition électronique. Cette année la 23ème édition c'est déroulé à Marseille au palais du Pharo et a célébré la diversité culturelle dans tous les aspects de la transmission et de la perception du mot écrit, parlé et illustré.

(12) DOSI, Direction Opérationnelle des Systèmes d'Information

(13) VPN, Virtual Private Network

VI. Sitographie

Comission Européenne / en ligne / visité le 1er mai / https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations_fr

CNRS / en ligne (pdf) / visité le 1er mai / http://www.dr2.cnrs.fr/IMG/pdf/chiffrement_agssiv3.pdf

CNIL / en ligne / visité le 1er mai / https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-un-guide-pour-accompagner-les-sous-traitants

CNIL / en ligne / visité le 1er mai / https://www.cnil.fr/fr/comprendre-le-rgpd

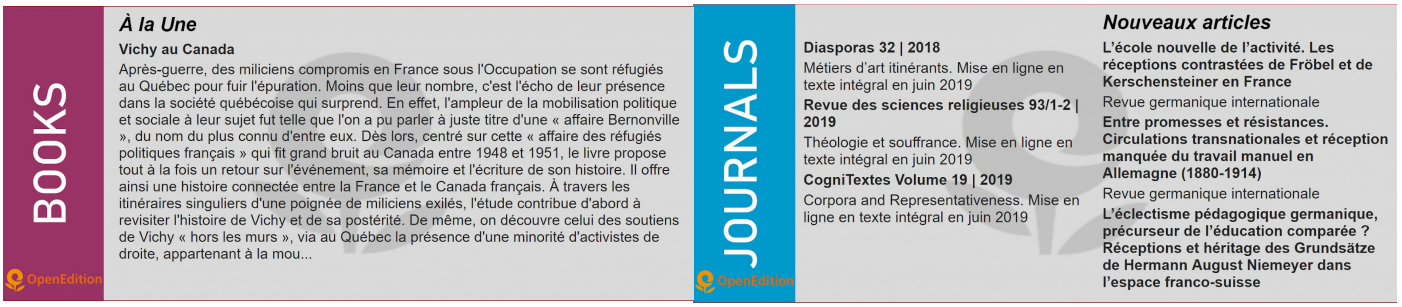
CNRS / en ligne / visité le 15 mai / http://www.insu.cnrs.fr/institut_insu/fr/reglement-general-sur-la-protection-des-donnees-rgpd

ResInfo / en ligne / visité le 15 mai / https://resinfo.org/Les-NewsLetters-de-RESINFO/Newsletter-6/Le-RGPD-au-CNRS

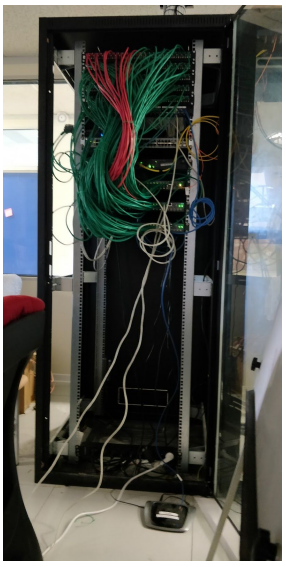
Min 2 rien / en ligne (pdf) / visité le 15 mai / https://www.min2rien.fr/wp-content/uploads/2014/02/Mohammed_Khabzaoui_13022014_Chiffrement.pdf

VII. Annexes

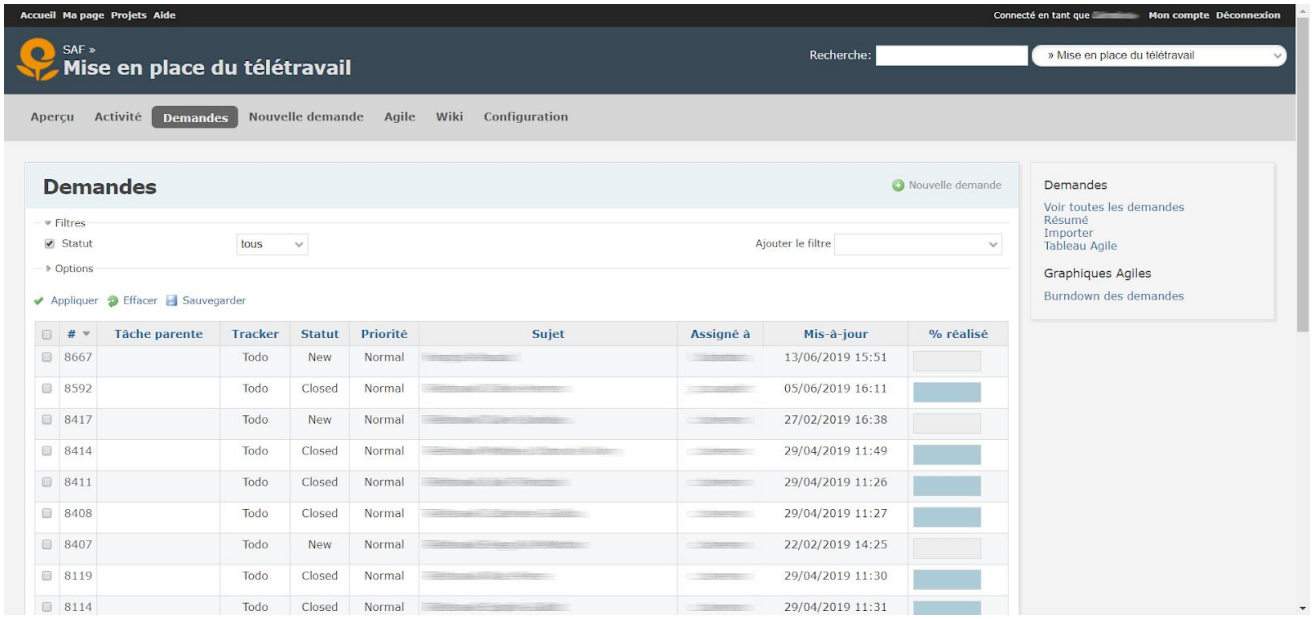
Annexe 1 : Xibo est est une solution Open Source d'affichage dynamique. Il peut être utilisé lors d'évènement dans une entreprise pour une diffusion en interne d'actualité pour les employés ou pour présenter au visiteur l'entreprise.
Voici quelques capture de mon travail :

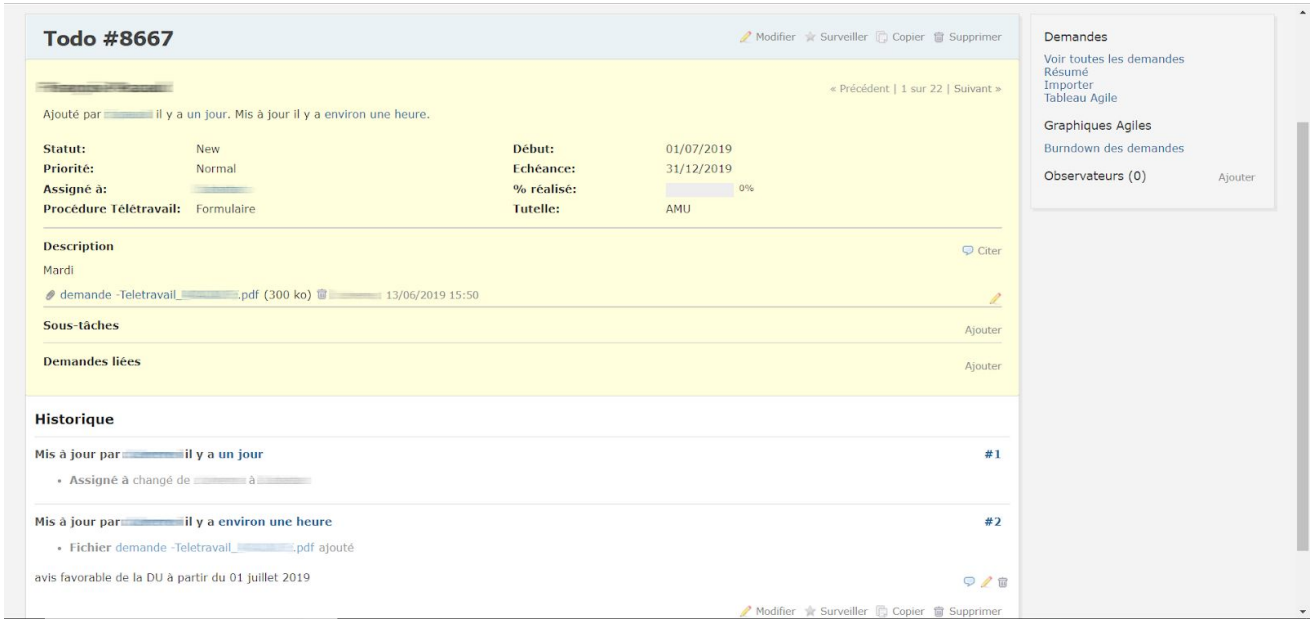


Annexe 2 : Voici quelques exemple de matériels :

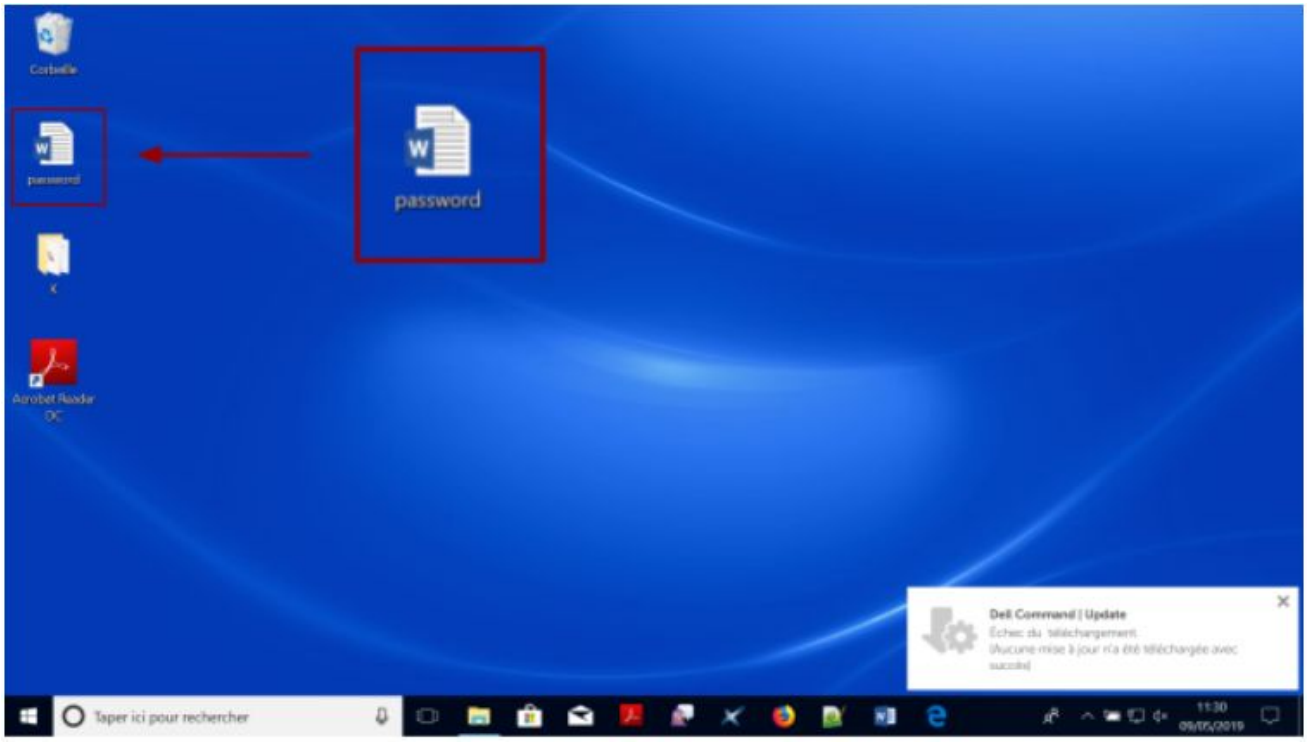


Annexe 3 : Redmine est une application web libre de gestion de projets complète en mode web, développée en Ruby. Le langage Ruby est un langage de programmation libre (standardisé au Japon). Grâce à cette application, on peut mettre en place un projet (dans mon cas le projet existait déjà) puis le suivre avec une barre d'avancement et des modifications.
Voilà donc le projet télétravail et une exemple de demande à traiter.





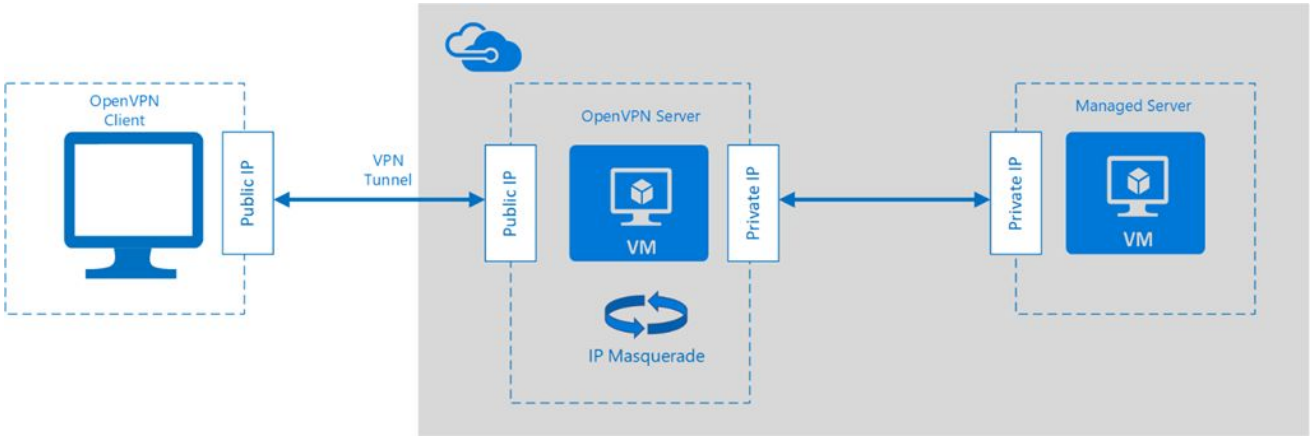
Annexe 4 : Photo d'un des postes de formation contenant un fichier avec des mots de passe.



Annexe 5 : VeraCrypt est un logiciel utilitaire de chiffrement qui utilise cinq système de chiffrement. Il fait suite au projet TrueCrypt et est sortie en 2013. Ces système sont AES, Camellia, Kuznyechik, Serpent et Twofish. Il est développé par une société française IDRIX, de plus il est gratuit et sous licence libre.
Il n'est pas validé par l'ANSSI (l'Agence Nationale de la Sécurité des Systèmes d'Information) mais reste très efficace.

Annexe 6 : Pidgin est une messagerie instantané. Elle vous permet de vous connecter simultanément à des comptes sur plusieurs réseaux de discussion. C'est une application qui fonctionne sur Linux, Windows et UNIX. Elle est compatible avec beaucoup de réseaux de discussions tel que Google Talk, Jabber / XMPP, Bonjour.

Annexe 7 : OpenVPN est un logiciel libre permettant la création d'un Virtual Private Network. Son créateur James Yonan a sortie la première version en 2001. Le logiciel fonctionne avec des clés privée partagé au préalable entre le client et le serveur. Il utilise des certificats électroniques ou de couples de noms d'utilisateur / mot de passe. Disponible sur presque tous les OS, il offre de nombreuses solution de sécurité et de contrôle.



Annexe 8 : Kaspersky est un anti-virus qui a été créé par une société privée multinationale spécialisée dans la sécurité des systèmes d'information. Créé en 1997, la société est maintenant implanté dans 32 pays. Elle propose aussi des logiciels anti-spyware, anti-spam et d'autre outils de sécurité.

Voici un mail destiné aux employés pour activer la nouvelle licence valable jusqu'en juin 2020 :

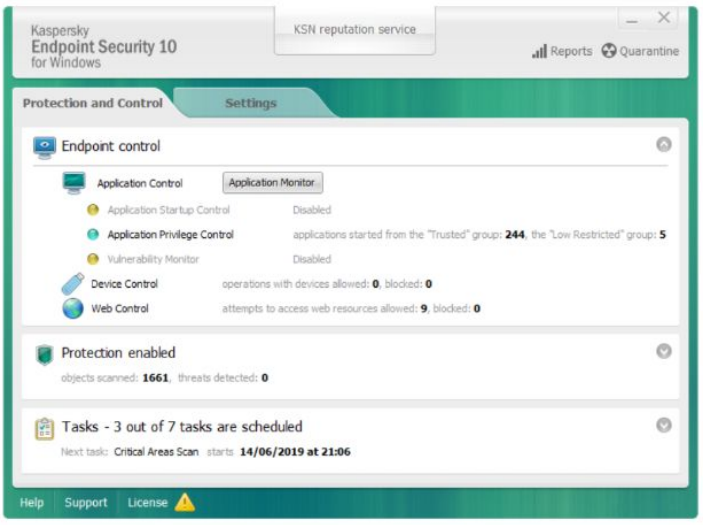
Loïc Barbato <loic.barbato@openedition.org> ven. 14 juin 21:47 (il y a 4 jours)
À vie-du-cleo

Bonsoir à tous,

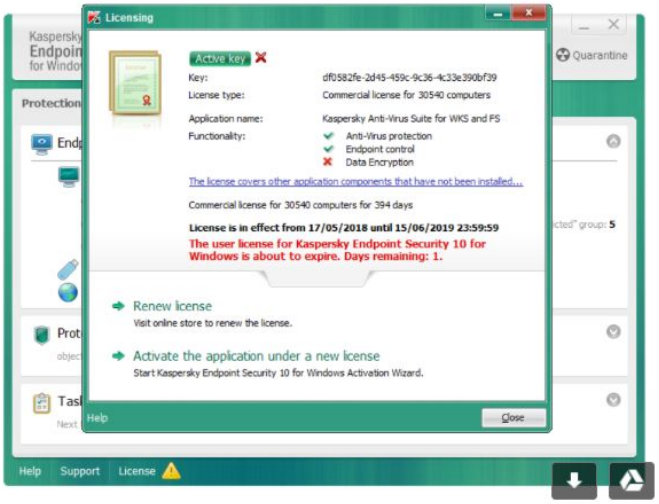
Dès demain (15/06/19), la licence Kaspersky arrivera à sa date limite, ce mail a donc pour but de vous expliquer étape par étape comment activer la nouvelle licence.

Pour commencer, il vous faudra ouvrir Kaspersky, rien de plus simple.
Dans votre barre de taches, il y a une flèche qui va vers le haut, elle vous permet de vous montrer les icônes des logiciels en cours.

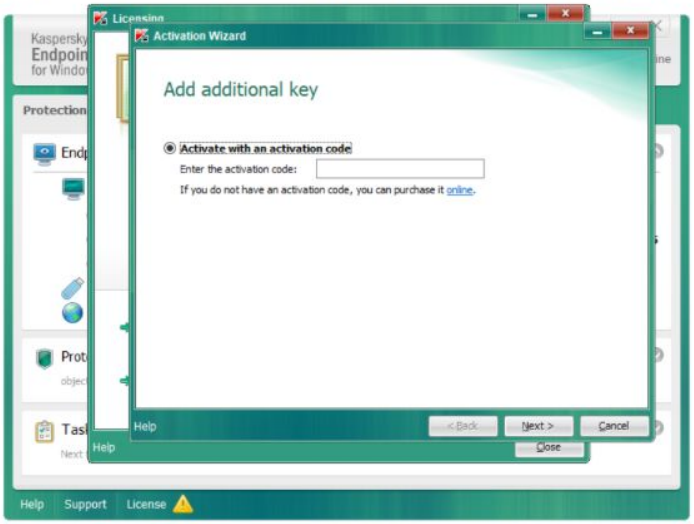
Il vous suffira de cliquer sur le "K" rouge et noir (icône de Kaspersky).
Cela va vous ouvrir cette fenêtre.



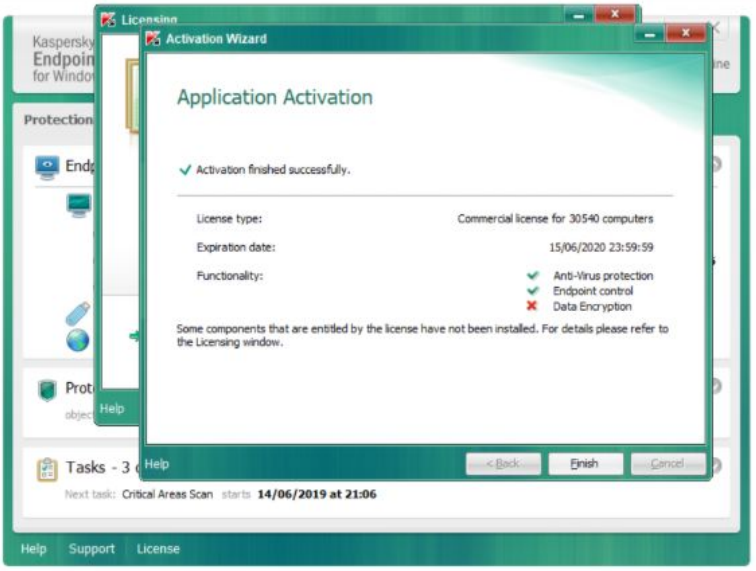
En bas à gauche, vous remarquerez l'onglet "Lincense", cliquez dessus pour pouvoir accéder au menu de renouvellement.
La fenêtre suivante va donc s'ouvrir pour vous demander de choisir, soit de racheter une licence, soit de la renouveler.



Ce choix est bien "Activate the application under a new license" (Activer l'application sous une nouvelle licence).
Une fois que vous aurez cliquez sur cette option, une nouvelle fenêtre apparaît pour vous demander de rentrer la nouvelle licence (son code).



Le code à rentrer est le suivant : W
Une fois ce code copié, cliquez sur "Next", la dernière fenêtre s'ouvre pour vous indiquer que vous avez bien rentré la nouvelle licence.



Vous pouvez donc cliquer sur "Finish" et fermer les autres fenêtre.

Si vous avez une quelconque difficulté pour effectuer ce renouvellement de licence, je serais disponible dès lundi pour vous aider.

Je vous souhaite une bonne soirée et un bon weekend,
Cordialement, Loïc