Ville de Renens
Une différence créative

MUNICIPALITÉ

PRÉAVIS N° 33-2023

AU CONSEIL COMMUNAL

Changement de l'infrastructure informatique, de ses composants matériels, logiciels et sécuritaires au sein de l'administration communale - Demande de crédit d'investissement

Date et lieu proposés pour la séance de la Commission :

Le mardi 7 février 2023 à 19h00

Lieu : Salle de municipalité

Préavis déposé au Conseil communal du jeudi 2 février 2023

PRÉAVIS N° 33-2023

Changement de l'infrastructure informatique, de ses composants matériels, logiciels et sécuritaires au sein de l'administration communale – Demande de crédit d'investissement

Table des matières

Renens, le 23 janvier 2023

AU CONSEIL COMMUNAL DE RENENS,

Monsieur le Président,
Mesdames les Conseillères communales, Messieurs les Conseillers communaux,

1. Préambule

L'infrastructure informatique (IT) de la Ville de Renens, qui date de 2015, est de plus en plus en souffrance face à la demande légitime du personnel de la Ville de Renens, notamment en matière de performance et d'usage. La garantie de l'infrastructure s'éteindra à la fin de l'année 2023, ce qui pourrait avoir des conséquences importantes en cas de pannes (indisponibilité des pièces, plus de pièces neuves mais uniquement d'occasion, etc.).

Au-delà de l'infrastructure serveurs, il est important de dresser également l'ensemble des thématiques qui gravitent autour et qui composent l'écosystème IT de la Ville de Renens, ceci afin d'assurer une cohérence de renouvellement et d'orientation pour le futur de l'informatique.

Afin de traiter cet écosystème, une liste des différentes thématiques a été élaborée comme suit :

- la connectivité et le centre de calculs ;
- la place de travail (Workplace) ;
- l'infrastructure serveurs ;
- le réseau ;
- la sécurité ;
- la gestion des sauvegardes & archives ;
- l'amélioration de l'environnement de travail.

Chacune des thématiques a été traitée en fonction d'une situation existante et des solutions idéalement souhaitées. Tous ces éléments ont été abordés en tenant compte des faiblesses du système actuel qui sont notamment :

- le manque de simplicité et de mobilité pour les collaboratrices et les collaborateurs ;
- la gestion des données qui doit être améliorée ;
- le manque de sécurité de l'infrastructure ;
- le manque de stabilité et les performances qui ne sont pas à la hauteur de nos enjeux ;
- le manque de pérennité sur le moyen terme.

Dans cet objectif de refonte majeure de l'informatique de l'administration communale, notamment par des changements profonds de fonctionnement ainsi que l'ajout de nouveaux concepts et équipements, l'attribution d'un crédit d'investissement est demandée au Conseil communal.

Conscients qu'il s'agit d'un préavis technique pouvant être relativement complexe à lire, un glossaire a été élaboré pour en faciliter la compréhension. Il se trouve dans l'annexe 1 du présent préavis.

2. Objectifs du changement d'infrastructure

Le changement de l'infrastructure est nécessaire dans la mesure où cette dernière ne répond plus aux exigences actuelles en termes de stabilité et de performances notamment. De plus, elle ne sera bientôt plus sous garantie (fin 2023) et chaque jour qui passe accroît le risque d'un problème majeur.

Au-delà de l'infrastructure IT, d'autres enjeux sont à prendre en compte comme la transformation numérique de l'administration publique, les processus qui se digitalisent, la traçabilité, la sécurité ainsi que le cycle de vie des données.

Cette refonte se définit selon les objectifs suivants :

- assurer la continuité opérationnelle informatique de l'activité de l'administration ;
- sécuriser et maintenir l'intégrité des données et des systèmes ;
- améliorer les processus et les systèmes informatiques pour en faciliter l'usage et l'évolution ;
- fournir un outil de travail adapté qui soit : facile, mobile, performant et pérenne.

Un autre facteur d'un tel changement réside dans l'amélioration significative de l'efficience et la simplification des connexions au système informatique.

Disposer de cette nouvelle infrastructure informatique, c'est permettre au service informatique, en plus des tâches quotidiennes, d'accentuer son travail sur deux aspects essentiels :

- être un facilitateur ente les parties prenantes et les usagères et usagers (notamment dans les projets transverses) ;
- être un levier de transformation numérique.

3. Contexte et historique

Dès 2015, la ligne directrice était de minimiser le nombre de périphériques physiques à maintenir au sein du parc informatique de la Ville de Renens, notamment les PC fixes et portables. C'est pour cette raison que le concept de mise à disposition de machines virtuelles (VDI) a été introduit. En effet, le principe était d'avoir un minimum de composants (écrans, postes légers notamment) et ainsi offrir aux usagères et usagers des postes Windows virtuels prêts à l'emploi.

Ces machines à disposition sont toutes identiques dans leur configuration (même logiciel, même mémoire vive, même CPU). Pour certaines tâches (comme le dessin), de par la puissance de calcul requise, la VDI n'était et n'est toujours pas adaptée. Par conséquent, les personnes travaillant dans ces contextes métiers disposaient déjà de stations de travail (postes fixes) offrant plus de puissance.

Actuellement, c'est une solution qui n'est plus viable, car elle coûte cher en maintenance sur les composants matériels. Elle est également plus que limitée dans son évolution de par son prix et par les ressources internes qu'elle nécessite. Cette technologie provoque aussi de nombreux blocages et ralentissements dans le travail journalier.

Enfin, elle n'est plus du tout adaptée au mode de travail actuel avec le déploiement du télétravail et des séances à distance (visio-conférences).

Pour toutes ces raisons, il devient indispensable de repenser l'entier du réseau et de l'infrastructure de l'informatique de Renens.

4. Thématiques globales

L'objectif de ce préavis est de créer et disposer d'une informatique qui se veut à la fois pérenne, stable et performante. Il est question également d'améliorer l'équipement informatique des collaboratrices et des collaborateurs pour leur offrir plus de flexibilité par l'introduction de PC portables.

La refonte de cette infrastructure informatique repose notamment sur un remplacement complet des équipements du réseau. Les technologies choisies permettront une simplification de la gestion et une meilleure stabilité.

À ceci viennent s'ajouter les aspects sécuritaires quant au trafic interne, externe (internet) et aux postes de travail au travers des produits/technologies qui permettent de sécuriser et contrôler les accès aux différents sites et services de la Ville.

En complément, la rétention des données traitées au sein de l'administration a été révisée, afin d'améliorer les sauvegardes et l'archivage.

4.1 Poste de travail

L'ensemble des postes de travail utilisés par les employé·e·s seront remplacés. Actuellement, les collaboratrices et les collaborateurs travaillent avec des machines virtuelles (VDI) ou des postes fixes. Ce préavis propose d'équiper chaque poste des éléments suivants :

- un PC portable ;
- une station d'accueil permettant de connecter un ou des écrans et d'autres périphériques (ex. : téléphone, clavier, souris, etc.) ;
- un ou deux écrans (la configuration pourrait être choisie en fonction des besoins du personnel).

Les informations sont détaillées dans l'annexe 2, au chapitre 2.2.

4.2 Serveurs

L'infrastructure actuelle est en fin de vie et ne sera plus sous garantie. Il devient donc urgent et nécessaire de remplacer l'entier de ces serveurs par une technologie plus moderne (hyperconvergence), qui est à la fois plus simple à gérer et qui offre de meilleures performances.

De plus, le système de secours électrique (UPS/Onduleurs) sera remplacé et amélioré afin d'avoir une plus grande autonomie (maintien du réseau). Le déplacement de notre infrastructure dans un centre de données de la région lausannoise (Brainserve) est également prévu.

Les informations sont détaillées dans l'annexe 2, aux chapitres 2.1 et 2.3.

4.3 Sécurité

Afin de garantir la sécurité du réseau de la Ville de Renens, qui est un maillon essentiel, il est prévu de remplacer plusieurs composants, voire d'en acquérir de nouveaux :

- remplacement des pare-feux (ceux actuellement en fonction sont en fin de vie et de garantie) ;
- acquisition d'un Bastion : système qui sécurise et contrôle l'accès à nos serveurs pour des fournisseurs ;
- acquisition d'un WAF : outil qui permet de centraliser les demandes de connexion aux différentes applications web ;
- acquisition d'un système NAC : système de contrôle des prises réseaux (WiFi compris) qui se trouvent dans les bâtiments communaux ;
- remplacement de l'anti-spam : système de filtrage des courriels avant réception et envoi ;
- remplacement de l'antivirus : remplacement de la solution actuelle (Kaspersky) par une solution plus moderne et plus évoluée (Microsoft).

En complément, le système d'archivage sera amélioré par l'introduction d'une solution permettant d'augmenter la fréquence, la durée de vie et la taille des sauvegardes.

Les informations sont détaillées dans l'annexe 2, aux chapitres 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.12 et 2.13.

4.4 Réseau

Les équipements réseaux - routeurs et switchs - sont en fin de vie et ne seront plus sous garantie. Par conséquent, il est nécessaire de les remplacer par une technologie simplifiée et qui permettra une meilleure gestion.

Les informations sont détaillées dans l'annexe 2, au chapitre 2.4.

4.5 Logiciels bureautiques

En vue d'harmoniser et de bénéficier des nouvelles technologies pour le travail au quotidien au sein de l'administration, Office 365 sera mis en place pour l'ensemble du personnel avec une adresse électronique pour chacun·e.

De plus, une nouvelle solution d'archivage de courriels sera introduite, qui permettra ainsi à chacun·e une recherche plus rapide et la garantie d'un archivage légal. Pour certaines données sensibles, un système de cryptage pourra être utilisé.

Les informations sont détaillées dans l'annexe 2, aux chapitres 2.11, 2.14 et 2.15.

5. Calendrier

Comme évoqué dans les précédents chapitres, la mise en place de tous les éléments se fera pas à pas, sur l'année 2023 et à début 2024. Il est très difficile de faire une planification temporelle, dans la mesure où les délais de livraison sont très fluctuants, allant de quelques jours à plusieurs semaines, voire plusieurs mois.

Néanmoins, le principe de déroulement sera le suivant :

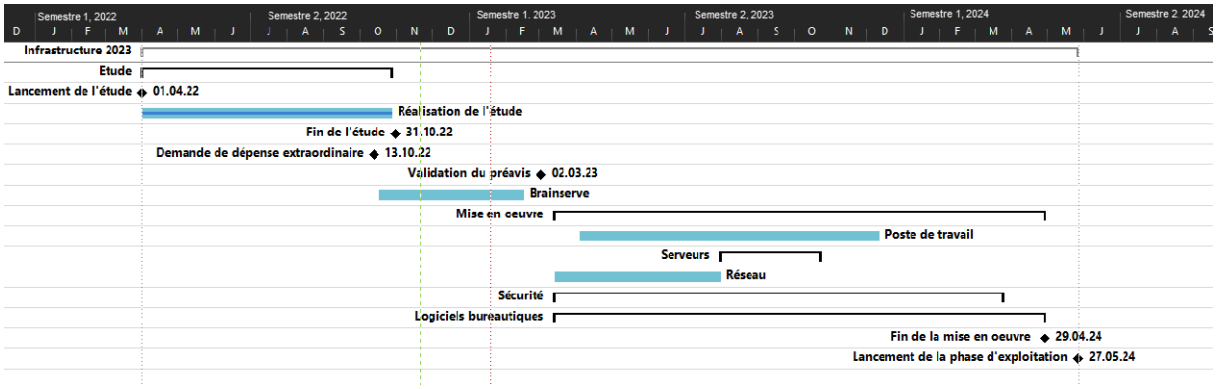

Figure 1 : Planning d'intention

6. Description des coûts

6.1 Coûts d'investissements

Le projet implique des coûts d'acquisition de matériel et de prestations d'ingénierie pour la mise en place de ces équipements.

L'ensemble des prestations/thématiques ci-dessous ont été soumises aux marchés publics, selon les seuils en vigueur.

Prestations	**Matériel et licences perpétuelles (TTC)**	**Ingénierie (TTC)**	**TOTAL (TTC)**
Crédit d'étude	-	CHF 90'000.-	CHF 90'000.-
Place de travail - Ecrans - Portables - Stations d'accueil (Docking station)	CHF 305'000.-	-	CHF 305'000.-
Infrastructures serveurs (VSI)	CHF 235'000.-	-	CHF 235'000.-
Réseau	CHF 140'000.-	CHF 12'300.-	CHF 152'300.-
Pare-feu (Firewall)	CHF 42'300.-	CHF 26'000.-	CHF 68'300.-
Bastion (PAM)	-	-	-
Application de contrôle web (WAF)	-	-	-
NAC	-	CHF 20'000.-	CHF 20'000.-
Sauvegardes et archives	CHF 78'000.-	CHF 3'300.-	CHF 81'300.-
Onduleurs - Remplacement UPS – Lausanne 33 - Remplacement UPS – Lausanne 35	CHF 20'000.-	-	CHF 20'000.-
Anti-spam	-	CHF 3'800.-	CHF 3'800.-
Système de chiffrement de la messagerie	CHF 7'500.-	CHF 3'600.-	CHF 11'100.-
Archiveur	CHF 30'000.-	CHF 2'500.-	CHF 32'500.-
TOTAL intermédiaire (TTC)	CHF 857'800.-	CHF 161'500.-	CHF 1'019'300.-
Divers et imprévus, environ 10% (TTC)			CHF 101'900.-
TOTAL (TTC)			**CHF 1'121'200.-**

À cela s'ajoutent, pour information, des montants pour la mise en place des fibres noires (à usage exclusif de la Ville de Renens) par TVT et VTX ainsi que pour la configuration des deux salles chez Brainserve. Ces montants ont été intégrés et financés dans le cadre du budget 2022.

6.2 Coûts d'exploitation

Hormis les coûts d'investissements décrits au chapitre 6.1 (matériels et ingénierie), le projet implique également des coûts d'exploitation pour les souscriptions aux solutions, qui sont devenues la majorité des modes de fonctionnement, les softwares assurances et les contrats de support.

2023 sera une année de transition, ce qui impliquera des doublons transitoires sur certaines licences (ex : Anti-spam, Firewall, etc.). Les engagements sur ces souscriptions sont de trois ans minimums.

Désignation	**N° de compte**	**2023**	**2024 et suivants**
Location Brainserver – Salles & courant électrique[1]	1100.3182.00	CHF 27'500.-	CHF 27'500.-
Location des fibres[1]	1100.3182.00	CHF 26'000.-	CHF 26'000.-
Remplacement des postes	1100.3111.02	*CHF - 20'000.-*	*CHF - 20'000.-*
Extension de garantie serveurs (actuel)	1100.3162.03	-	*CHF - 10'000.-*
Licences PcoIP– teradici (actuel)	1100.3162.03	-	*CHF - 7'000.-*
Liquidware – (actuel)	1100.3162.03	-	*CHF - 8'200.-*
Réseau – ExtremeNetworks	1100.3162.03	CHF 15'000.-	CHF 15'000.-
Pare-feu – Fortinet	1100.3162.03	CHF 23'000.-	CHF 23'000.-
Pare-feu – Sophos (actuel)	1100.3162.03	-	*CHF - 6'000.-*
Bastion (PAM) – Wallix	1100.3162.03	CHF 6'500.-	CHF 6'500.-
Abonnement WAF – F5	1100.3162.03	CHF 37'000.-	CHF 37'000.-
NAC – Extreme Network	1100.3162.03	CHF 8'300.-	CHF 8'300.-
Sauvegardes et archives – Silent Bricks	1100.3162.03	CHF 12'500.-	CHF 12'500.-
Microsoft 365 – ajout de 150 licences E3 + 50 Exchange Plan 2[2]	1100.3162.03	CHF 64'000.-	CHF 64'000.-
Zoom (actuel)	1100.3162.03	-	*CHF - 1'500.-*
Kaspersky (actuel)	1100.3162.03	-	*CHF - 10'000.-*
Antivirus – M365 E5 Security	1100.3162.03	CHF 54'000.-	CHF 54'000.-
Anti-spam – Fortimail	1100.3162.03	CHF 14'000.-	CHF 14'000.-
Anti-spam – Barracuda (actuel)	1100.3162.03	-	*CHF - 2'900.-*
Chiffrement des courriels – SEPPMail	1100.3162.03	CHF 8'500.-	CHF 8'500.-
Archiveur de courriels – Cryoserver	1100.3162.03	CHF 17'000.-	CHF 17'000.-

[1]Ces montants ont fait l'objet d'un rapport à la commission des finances, puisque déjà engagés et pris dans le budget 2023.

[2]Ce montant représente un besoin en extension de licences pour la fourniture d'une adresse électronique à l'ensemble du personnel (chapitre 4.5).

Désignation	N° de compte	2023	2024 et suivants
• Abonnements • Maintenance et software • Support			
Total (TTC)	**-**	**CHF 293'300.-**	**CHF 247'700.-**

7. Incidences financières

7.1 Dépenses déjà engagées

A ce jour, les dépenses pour l'étude et l'analyse de la place de travail (Workplace) et la VSI ont été engagées pour un montant de CHF 89'611.80 TTC. Elles sont intégrées dans le présent préavis.

Ce montant a été financé dans le cadre du préavis N° 1-2021 – Autorisations générales 2021-2026, chapitre N° 5 « *Le Conseil communal accorde à la Municipalité une autorisation générale pour la comptabilisation de certains frais d'études qui ne pouvaient être prévus au budget de fonctionnement, ceci à concurrence de CHF 100'000.- au maximum par cas* ».

Cette dépense a été enregistrée dans le compte d'attente d'investissement au bilan N° 9140.7031 - Renouvellement infrastructure.

7.2 Investissements

Comme décrit au chapitre 6.1, l'investissement nécessaire pour la refonte de l'infrastructure informatique se monte à **CHF 1'121'200.- TTC.**

Cet investissement sera imputé au nouveau compte d'investissement du patrimoine administratif N° 1100.3068.5060 – Changement infrastructure informatique.

7.3 Plan des investissements

Cette dépense figure au plan des investissements 2022-2026, adopté par la Municipalité le 5 septembre 2022, comme suit : compte N° 1100.8131.5060 – Changement infrastructure informatique.

7.4 Coût du capital

Le coût du capital (amortissements + intérêts) représente un coût de fonctionnement annuel moyen de CHF 241'058.- pendant cinq ans.

Ce coût se décompose de la manière suivante : amortissement CHF 224'240.- (CHF 1'121'200.- divisés par cinq ans) et intérêts CHF 16'818.- (CHF 1'121'200.- divisés par deux et multipliés par un taux moyen de 3%).

7.5 Comptes de fonctionnement

Outre le coût du capital, et comme décrit au chapitre 6.2, le projet implique des coûts générant une augmentation des charges de fonctionnement annuelles ayant une incidence sur le résultat estimée comme suit :

Désignation	No de compte	2023	2024 et suivants
Maintenance et licences contractuelles	1100.3162.03	259'800.-	214'200.-
Remplacement des postes	1100.3111.02	- 20'000.-	- 20'000.-
Honoraires, locations	1100.3185.02	53'500.-	53'500.-
Total		**293'300.-**	**247'700.-**

8. Conclusion de la Municipalité

La Municipalité voit dans cet investissement le moyen d'assurer les changements indispensables pour garantir la sécurité, la pérennité et l'efficience de l'informatique de la Ville de Renens pour les utilisatrices et les utilisateurs. Il s'agit d'un projet ambitieux, mais aussi conforme aux réalités et défis actuels, ouvrant ainsi de belles perspectives. Ces différents projets sont finalement nécessaires de par la vétusté et la fin de vie de certains équipements cruciaux.

Avec un ensemble de 15 projets différents qui touchent à la fois la sécurité, les serveurs, ainsi que la place de travail des collaboratrices et des collaborateurs, le but commun est d'améliorer le quotidien des usagères et usagers tout en assurant et protégeant l'accès aux données de la Ville de Renens.

Ces nouvelles technologies permettront d'améliorer et de mieux contrôler l'ensemble des systèmes informatiques de la Ville. Les solutions retenues ont déjà fait leurs preuves dans le domaine public et privé.

Les choix réalisés ont été faits dans un souci de précision mais aussi de cohérence globale en ne perdant pas de vue la compatibilité entre les différents systèmes, ceci pour conférer à l'ensemble de ce préavis une plus-value à deux niveaux.

Fondée sur l'exposé ci-dessus, la Municipalité prie le Conseil communal de bien vouloir voter les conclusions suivantes :

CONCLUSIONS

LE CONSEIL COMMUNAL DE RENENS,

Vu le préavis N° 33-2023 de la Municipalité du 23 janvier 2023,

Ouï le rapport de la Commission désignée pour étudier cette affaire,

Considérant que cet objet a été porté à l'ordre du jour,

ALLOUE à cet effet, à la Municipalité, un crédit de **CHF 1'121'200.- TTC** pour la refonte de l'infrastructure informatique, de ses composants matériels, des logiciels et de la place de travail des collaboratrices et des collaborateurs.

Cette dépense sera financée par voie d'emprunt, conformément à l'autorisation d'emprunter donnée par le Conseil communal.

Elle figurera dans le compte d'investissement du patrimoine administratif, sous le compte N° 1100.3068.5060 – Changement de l'infrastructure informatique.

Cette dépense sera amortie en cinq ans, selon l'art. 17 b du règlement du 14 décembre 1979 (mis à jour au 1er juillet 2006) sur la comptabilité des communes.

ACCEPTE les charges de fonctionnement supplémentaires au budget 2023 telles que décrites au chapitre 7.5 des incidences financières pour un montant total de CHF 293'300.- TTC réparties dans la section N° 1100 – Informatique, comptes Nos 1100.3111.02, 1100.3162.03 et 1100.3185.02.

PREND ACTE que soient portées aux budgets 2024 et suivants, les charges supplémentaires inhérentes au présent préavis telles que décrites au chapitre 7.5 des incidences financières.

———

Approuvé par la Municipalité dans sa séance du 23 janvier 2023.

AU NOM DE LA MUNICIPALITÉ

Le Syndic: Le Secrétaire municipal:

Jean-François Clément Michel Veyre

Membre de la Municipalité concerné: - M. Jean-François Clément, Syndic

Annexes : - N° 1 – Glossaire

- N° 2 – Détails techniques

Ville de Renens
Une différence créative

Annexe 1 - Glossaire

Les termes utilisés dans le préavis sont définis dans ce glossaire.

Termes	**Définitions**
Adresse MAC	Une adresse MAC est également appelée adresse matérielle. C'est un identifiant unique et propre à la carte réseau d'un PC.
Bastion (PAM)	Utilisé pour protéger les accès aux systèmes d'informations en fournissant une traçabilité des accès aux ressources internes.
Brainserve	Nom du centre de données situé à Crissier. Il regroupe un ensemble de salles qui est à disposition de différents clients.
Centre de données	Un lieu (et un service) où sont regroupés les équipements constituants d'un système d'information (ordinateurs centraux, serveurs, baies de stockage, équipements réseaux et de télécommunications, etc.).
Solution de détection et d'intervention sur les endpoints EDR	Une solution de détection et d'intervention sur les endpoints (EDR) est une solution de cybersécurité qui détecte et atténue les cybermenaces en surveillant en continu les endpoints et en analysant leurs données.
Fabric Connect	Fabric Connect élimine les multiples couches de protocoles et crée ainsi un réseau virtualisé agile et flexible. Avec Fabric Connect, seule la périphérie est configurée. Le service se propage automatiquement à travers tous les équipements concernés, notamment les cœurs de réseaux.
Hyperconvergence	L'hyperconvergence est un type d'architecture matérielle informatique qui agrège de façon étroitement liée les composants de traitement, de stockage, de réseau et de virtualisation de plusieurs serveurs physiques.
Internet des objets (IoT)	L'Internet of Things (IoT) décrit le réseau de terminaux physiques, les « objets », qui intègrent des capteurs, des softwares et d'autres technologies en vue de se connecter à d'autres terminaux et systèmes sur Internet et d'échanger des données avec eux.
Système de prévention d'intrusion (IPS)	Un système de prévention d'intrusion (ou IPS, *intrusion prevention system*) est un outil des spécialistes en sécurité des systèmes d'information, similaire aux systèmes de détection d'intrusion (ou IDS, *intrusion detection system*), permettant de prendre des mesures afin de diminuer les impacts d'une attaque.
Logiciel malveillant (Malware)	Un logiciel malveillant est un programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur dont l'ordinateur est infecté.
Contrôleur d'accès au réseau (NAC)	Un contrôleur d'accès au réseau (*network access control* ou NAC) est une méthode informatique permettant de soumettre l'accès à un réseau d'entreprise à un protocole d'identification de l'utilisateur et au respect par la machine de cet utilisateur des restrictions d'usage définies pour ce réseau.

Termes	Définitions
Pare-feu (Firewall)	Un pare-feu (de l'anglais *firewall*) est un logiciel et/ou un matériel permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique. Il surveille et contrôle les applications et les flux de données.
Proxy	Un proxy est un composant logiciel informatique qui joue le rôle d'intermédiaire en se plaçant entre deux hôtes pour faciliter ou surveiller leurs échanges.
Système de gestion des informations et des événements de sécurité (SIEM)	Le SIEM (Security Information Event Management) surveille, collecte et analyse les données provenant des différents ordinateurs d'une société et plus précisément des pare-feux, serveurs proxy, anti-virus qui les composent.
Commutateur réseau (Switch)	Un commutateur réseau (en anglais switch), est un équipement qui relie plusieurs segments (câbles ou fibres) dans un réseau informatique et de télécommunication et qui permet de créer des circuits virtuels. Il s'agit le plus souvent d'un boîtier disposant de plusieurs ports RJ45.
Coût global de possession (TCO)	Le TCO (Total Cost of Ownership) désigne le coût global d'un bien ou d'un service tout au long de son cycle de vie.
Client léger	Un client léger (Thin Client) est un ordinateur qui permet la connexion à l'infrastructure serveurs. Ce dernier embarque un système d'exploitation léger.
Infrastructure de postes de travail virtuels (VDI)	La VDI est une solution de virtualisation qui utilise des machines virtuelles pour fournir et gérer des postes de travail virtuels.
Réseau local virtuel (VLAN)	Un VLAN, pour Virtual Local Area Network, décrit un type de réseau local. On le traduit en français par réseau local virtuel. C'est ce dont dispose la Ville au sein de ses bureaux.
Réseau privé virtuel (VPN)	En informatique, un réseau privé virtuel, est un système permettant de créer un lien direct entre des ordinateurs distants, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics.
Infrastructure virtuelle de serveurs (VSI)	L'infrastructure virtuelle de serveurs consiste à mettre en place une solution de convergence permettant de consolider le stockage et les serveurs des sites distants en un seul et même équipement physique.
Pare-feu applicatif web (WAF)	Un Web Application Firewall (WAF) est un type de pare-feu qui protège le serveur d'applications Web dans le backend contre diverses attaques. Le WAF garantit que la sécurité du serveur Web n'est pas compromise en examinant les paquets de requête HTTP / HTTPS et les modèles de trafic Web.
Zero Client	Un Zero client est un ordinateur qui, dans une architecture client-serveur, n'a presque pas de logique d'application. Il dépend donc surtout du serveur central pour le traitement.

Annexe 2 – Détails techniques

1. Résumé des choix

Ci-dessous, un résumé des thématiques avec les solutions respectives retenues :

Thématiques	**Descriptions**	**Choix technologiques**	
Place de travail	Place de travail qui contient : un PC, une station d'accueil, souris, clavier, écrans, téléphone.	Gamme de produits Lenovo	Chapitre 2.2 Page 3
Infrastructure virtuelle serveurs (VSI)	Serveur permettant le stockage de l'ensemble des informations numériques de la commune.	Nutanix	Chapitre 2.3 Page 4
Réseau	Ensemble d'équipements permettant la connexion entre les systèmes informatiques.	Extreme Networks	Chapitre 2.4 Page 5
Pare-feu (Firewall)	Système de protection du réseau permettant de contrôler/filtrer ce qui sort et rentre du réseau informatique.	Fortinet	Chapitre 2.5 Page 6
Bastion (PAM)	Système qui sécurise et contrôle l'accès à nos serveurs pour des fournisseurs.	Wallix	Chapitre 2.6 page 7
Application de contrôle web (WAF)	Outil permettant de centraliser les demandes de connexion aux différents applications web.	F5	Chapitre 2.7 Page 8
Contrôleur d'accès au réseau (NAC)	Système de contrôle des prises réseaux (WiFi compris) se trouvant dans les bâtiments communaux.	Extreme NAC	Chapitre 2.8 Page 8
Sauvegardes et archives	Amélioration et extension des sauvegardes de données.	Veeam & FastLTA	Chapitre 2.9 Page 9
Onduleurs	Système électrique permettant de maintenir en tension une infrastructure durant un laps de temps défini.	Eaton (via Statron)	Chapitre 2.10 Page 10
Microsoft 365		Microsoft 365 E3	Chapitre 2.11 Page 11
Antivirus	Système de protection installé sur chaque PC.	M365 Security	Chapitre 2.12 Page 12
Anti-spam	Système de filtrage des courriels avant réception et envoi.	Fortimail	Chapitre 2.13 Page 12
Chiffrement des courriels	Permet de crypter des courriels afin d'en protéger le contenu durant le transfert entre l'expéditeur et le destinataire.	SEPPMail	Chapitre 2.14 Page 13
Archiveur des courriels	Permet de journaliser l'ensemble des courriels sortants et entrantsj afin de pouvoir les rechercher.	Cryoserver	Chapitre 2.15 Page 13

2. Thématiques détaillées

2.1 Connectivité au centre de données Brainserve

Actuellement, la ville dispose de deux salles distinctes pour héberger l'infrastructure informatique communale. Ces deux salles ne sont pas du tout adaptées pour l'accueil d'une nouvelle infrastructure informatique notamment en matière de sécurité et d'incendie. De plus, les problèmes potentiels d'approvisionnement en électricité doivent faire l'objet d'une réflexion approfondie. Cette thématique est ainsi également abordée dans le présent préavis.

> En lien avec le dernier point, il est à noter qu'actuellement, en cas de coupure de courant, l'infrastructure informatique ne peut fonctionner que très peu de temps (max. 1h) en utilisant les onduleurs actuellement en service. Cela signifie que l'ensemble du personnel n'aurait plus d'informatique (serveurs et PC) après ce laps de temps avec une dégradation croissante pendant l'heure écoulée.

Partant de ce constat, en complément avec les notions de mobilité et de flexibilité évoquées au chapitre 2.2, il est question de déplacer l'infrastructure communale existante au sein du centre de calcul Brainserve à Crissier. Ce dernier fait partie des références suisses en matière d'hébergement des grands opérateurs téléphoniques, des banques et des assurances. Il est classé en « tier-4 » (ce qui signifie une disponibilité de 99,995% avec une redondance de l'ensemble des composants).

L'objectif premier consiste à transférer les risques inhérents à l'infrastructure actuelle, aux pannes électriques, à l'incendie, à la sécurité d'accès et à la disponibilité chez Brainserve. En complément, étant donné que ces deux salles actuelles ne contiendront plus que des éléments basiques mais néanmoins cruciaux, ils ne généreront pas autant de chaleur qu'actuellement. Par conséquent, les systèmes de climatisation en fonction pourront être éteints, puis déconstruits par le Service Bâtiments-Domaines-Logement (BaDoLog). Cette action renforcera notre action écologique.

Parallèlement à ce transfert et en préparation de la nouvelle infrastructure, il est essentiel de mettre en place une nouvelle connectivité entre la rue de Lausanne 33 et Brainserve ainsi que la rue de Lausanne 35 et Brainserve. Pour ce faire, les actions suivantes sont entreprises :

- établissement d'une fibre entre la Rue de Lausanne 33 et Brainserve avec l'opérateur TVT ;
- établissement d'une fibre entre la Rue de Lausanne 35 et Brainserve avec l'opérateur VTX.

Ces deux fibres fonctionneront en parallèle et permettront ainsi une répartition de la charge utilisateur. De plus, le fait de choisir spécifiquement deux opérateurs distincts permet d'avoir deux chemins de fibres, menant à Brainserve, qui sont différents.

Cette double fibre permet de minimiser les risques suivants :

- panne d'un opérateur ;
- fibre endommagée par des travaux.

Suite à la mise à disposition de ces fibres, l'opération de transfert de l'infrastructure pourra débuter pour se réaliser en trois étapes :

- déménagement des serveurs de tests pour réaliser des opérations de configuration et de tests de lignes (réseau) entre la Ville de Renens et Brainserve ;
- déplacement progressif de l'infrastructure serveur durant les journées de travail. L'objectif est de maintenir l'activité des utilisatrices et utilisateurs durant ce point de migration ;
- déplacement de l'infrastructure de machines virtuelles (VDI) durant le week-end. Cette opération ne pourra pas se faire durant la semaine de travail, car l'ensemble des machines virtuelles seront indisponibles.

Cette thématique a déjà été traitée dans le cadre d'une annonce de dépense imprévisible et exceptionnelle. À la demande de la Commission des finances, tous les éléments qui sont rattachés à cette thématique sont présents dans ce préavis.

Dans un second temps, étant donné que la connectique entre Brainserve et la Ville aura été établie, la nouvelle infrastructure (présentée au chapitre 2.3) pourra être installée plus rapidement.

2.2 Place de travail

2.2.1 Situation actuelle

La place de travail est actuellement basée sur une infrastructure de machines virtuelles (VDI). Depuis la mise en œuvre de cette solution en 2015, il existe plusieurs configurations au sein de l'administration communale qui sont :

- configuration 1 - Zero client (Ecran Samsung) avec un écran HP à côté selon le besoin ;
- configuration 2 - Thin client (HP) avec deux écrans HP ;
- configuration 3 - Postes fixes HP (notamment pour le personnel traitant des aspects graphiques) ;
- configuration 4 - PC portables HP.

Ces configurations sont optimisables dans la mesure où il faut maintenir plusieurs systèmes en parallèle pour la gestion, le suivi et le renouvellement de ces différents équipements. Partant de ce constat, une étude a été réalisée avec la société TicTac Services pour identifier les besoins des utilisatrices et des utilisateurs en comparant l'écosystème actuel avec les possibilités futures telles qu'un parc 100% en PC portables, en stations fixes ou en hybrides (mélange de fixes/portables). Lors de cette étude, des ateliers ont été menés entre TicTac Services et les différents services de la Ville afin de déterminer les problèmes actuels, les besoins et la solution idéale selon eux.

À la suite de ce travail, il est clairement apparu que la place de travail n'est pas/plus adaptée aux besoins du personnel, tant pour le travail journalier que pour le télétravail.

2.2.2 Situation souhaitée

Selon les résultats reçus, une évaluation a été effectuée en tenant compte des aspects suivants :

- simplifier l'usage pour les collaboratrices et collaborateurs ;
- faciliter la mobilité pour les collaboratrices et collaborateurs ;
- déployer la visio-conférence et du télétravail ;
- réaliser des économies d'énergie.

Les résultats de l'évaluation montrent clairement que l'approche 100% PC portables permet de répondre à l'ensemble des critères ci-dessus. De plus, ce nouveau parc homogène offrira une gestion plus simple et harmonieuse.

En complément aux PC portables, la question des écrans a également été traitée, à savoir de proposer aux employé·e·s le choix entre deux gammes d'écrans :

- écrans 24'' ;
- écrans 34'' incurvés.

Cette offre a été mise sur pied notamment par le fait que dans certains contextes métiers, il est préférable d'avoir un écran 34'' plutôt que 2 écrans 24''. Un test a d'ailleurs été réalisé avec un écran 34'' dans les différents services. Il a été constaté que pour les finances, par exemple, ce type d'écran était meilleur que les deux 24''. À contrario, il n'est pas adapté pour les travaux de graphisme ou de dessin assisté par ordinateur.

À la suite d'un appel d'offres public (publié sur SIMAP), quatre offres ont été reçues. Suite au dépouillement qui a eu lieu le lundi 31 octobre 2022, la société retenue serait Bechtle Direct SA en cas d'acceptation de ce préavis par le Conseil communal. En effet, l'offre proposée est la plus aboutie d'un point de vue technologique et elle répond le mieux à tous les critères de la grille d'évaluation (meilleure note attribuée). Elle est également la plus intéressante d'un point de vue économique.

La solution repose sur la marque Lenovo avec les éléments suivants :

- portable (170 pièces) – lenovo T14 ;
- écran 24'' (140 écrans) – ThinkVision T34d-10 ;
- écran 34'' (70 écrans) – ThinkVision T34w-20 incurvé ;
- station de travail (Docking Station) – USB-C Lenovo ThinkPad.

La garantie de ces équipements est de quatre ans.

2.2.3 Mise en œuvre

La mise en place et la configuration, malgré les différents automatismes, sera longue. Aussi, il a été décidé de réaliser plusieurs livraisons durant l'année et ainsi de faire une mise en service par étape. Ceci permettra notamment d'absorber la charge en interne pour la mise en place de ces nouvelles machines.

En ce qui concerne le matériel actuel et dans un souci de sobriété numérique, les différents composants seront traités comme suit :

- les écrans HP, qui sont actuellement en fonction, resteront actifs dans le parc. Les vieux écrans (trop petits ou plus adaptés en matière de connectiques) seront remplacés ;
- l'ensemble des zero, thin client et postes physiques seront récupérés au service informatique. Pour les modèles plus anciens, hors garantie, ils seront soit donnés à des écoles (laboratoires de test, etc.) soit vendus pour une 2e vie auprès d'entreprises spécialisées.

L'ensemble des PC portables actuellement en circulation seront récupérés et une partie servira de matériel de secours (pannes). Les autres seront vendus (2e vie). En ce qui concerne le renouvellement de ce parc, il est prévu qu'il ait une durée de vie de cinq ans (la garantie est de quatre ans mais il est possible de la prolonger pour assurer une durée de vie plus longue). Par la suite, il se renouvellera au fil de l'eau par le biais du budget de fonctionnement.

2.3 Infrastructure serveurs (VSI)

2.3.1 Situation actuelle

L'infrastructure actuelle a été mise en place entre fin 2015 et courant 2016. Aucune évolution majeure n'a été faite depuis lors. Elle repose sur plusieurs serveurs qui permettent de fournir différents services à l'ensemble de l'administration de la Ville de Renens. Cette infrastructure repose notamment sur les éléments suivants :

- quatre serveurs HP ProLiant DL380 G9 → concerne la partie serveur ;
- deux serveurs HP ProLiant DL380 G9 → concerne la partie VDI ;
- deux serveurs de stockage et backup (notamment pour la solution Veeam qui traite des backups).

Cette infrastructure obsolète et sous-dimensionnée induit des problèmes de stabilité, de performance et ne permet pas de mettre à disposition des machines Windows dans de bonnes conditions. En effet, les serveurs traitant de la VDI sont régulièrement saturés et provoquent de gros ralentissements qui impactent fortement le travail des collaboratrices et collaborateurs.

De plus, la garantie prendra fin entre juin et décembre 2023, (selon les serveurs, et il ne sera plus possible de la prolonger au-delà de ces dates.

2.3.2 Situation souhaitée

Suite également à l'étude menée par l'entreprise TicTac, il est apparu que selon l'utilisation de l'informatique au quotidien, des types de travaux réalisés, de la volumétrie de données ou encore du mode de fonctionnement, une solution globale (système unifié dans un seul et même équipement) serait une bonne approche. La complexité de la solution est réduite, notamment par le fait qu'il s'agit d'une infrastructure informatique qui combine, dans un seul et même boitier, du stockage, du réseau et de la puissance de calcul (CPU).

Les avantages d'une telle solution sont notamment :

- réduction de la complexité des systèmes ;
- meilleure capacité d'adaptation en matière de dimensionnement (augmentation des ressources notamment) ;
- diminution du coût global de possession (TCO) par rapport à une infrastructure conventionnelle.

Afin de satisfaire les besoins des usagères et usagers et de répondre aux critères émis par l'étude et l'équipe informatique, la solution Nutanix a été retenue. Cet éditeur propose une solution hyperconvergée basée sur une infrastructure logicielle autorisant des charges de travail applicatives dans tous les environnements (sur site, cloud privé, cloud public, hybride). Nutanix, fondée en 2009, est un pionnier de l'hyperconvergence proposant aujourd'hui des solutions relatives au nuage (cloud) d'entreprise visant à faciliter la gestion de divers services IT sur une unique plate-forme logicielle. Nutanix compte plus de 18'000 clients à travers le monde et fait donc partie des acteurs majeurs, viables et pérennes du monde de l'hyperconvergence.

En lien avec la nouvelle connectique (voir chapitre 2.1), voici comment seront équipées chacune de des salles de la Ville. Ces configurations ont été déterminées durant l'étude préalable.

- 3 x NX-3060-G8, avec chacun : (2U High) ;
- 2 CPU 10c/2.3 GHZ ;
- 512 GB RAM. (up to 1TB) ;
- 4 * SSD 7.68TB (up to 6 disk per node);
- 2 * 10/25 Gbit SFP+.

L'objectif est de fournir une infrastructure basée sur le principe « active-active » entre les deux salles de Brainserve. Ce principe signifie que les deux salles seront utilisées pour les besoins informatiques des utilisatrices et utilisateurs au quotidien. À contrario, d'une infrastructure active-passive ou l'infrastructure passive est « dormante » est n'est utilisée qu'en cas de panne de la principale.

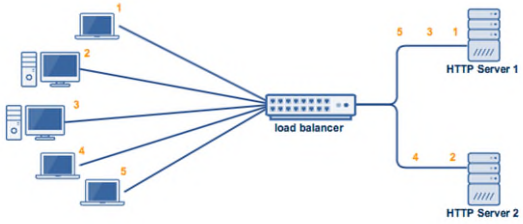

Figure 1 : Infrastructure active-active
source : Active-Active vs. Active-Passive High-Availability Clustering | JSCAPE

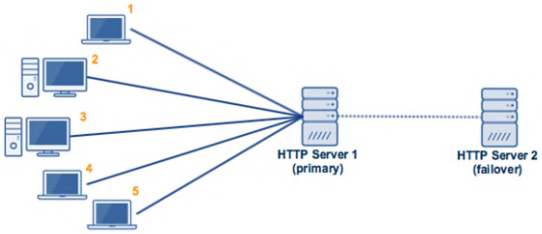

Figure 2 : Infrastructure active-passive
source : Active-Active vs. Active-Passive High-Availability Clustering | JSCAPE

Dans la future infrastructure active-active, si l'un ou l'autre des équipements d'une salle devait tomber en panne, l'autre salle sera parfaitement en mesure de prendre le relais.

2.3.3 Mise en œuvre

À la suite de l'appel d'offres sur invitation et au dépouillement du 31 octobre 2022, la société Darest Informatic SA a été retenue. En effet, il s'agit de l'offre la plus avantageuse économiquement et qui répond également à l'ensemble des critères de la grille d'évaluation. Pour rappel, le service informatique, par ses connaissances en interne, s'occupera de la mise en place et de la configuration de ces équipements. Ainsi, il n'y aura pas de prestations d'ingénierie pour cette partie.

2.4 Réseau

2.4.1 Situation actuelle

L'infrastructure réseau actuelle est en place depuis 2015. Elle est configurée sur une topologie réseau en étoile. Malheureusement, certains sites, au sein de cette étoile font partie d'une boucle (notamment certains sites périphériques). Cette composition ainsi que certains équipements posent des difficultés en matière de stabilité et de sécurité notamment. Actuellement, il serait trop onéreux de revoir l'ensemble de cette constellation pour n'en faire qu'un réseau en forme d'étoile (notamment par les

travaux que cela pourrait engendrer pour la fibre par exemple). Les équipements essentiels seront en fin de vie en décembre 2023.

2.4.2 Situation souhaitée

Étant donné les deux aspects évoqués ci-dessus que sont la topologie réseau et la fin de vie des équipements, il n'est pas possible de remplacer la boucle en une fois.

Le choix retenu est la solution Extreme Network. En effet, elle propose notamment un concept appelé « Fabric Connect » qui rationalise et simplifie le réseau en réduisant considérablement le nombre de protocoles ainsi que le nombre de points de contact. Le résultat est un réseau plus stable et résiliant. Ainsi, l'ensemble de nos switches seront, à terme, remplacés en fonction de leur nature d'utilisation :

- les switches de routage et distants seront renouvelés par des équipements ExtremeSwitching 5520. De plus, une redondance dans les deux salles (Lausanne 33 et 35) sera mise en place. Ce qui n'est actuellement pas le cas avec le réseau actuel ;
- pour la partie serveurs et datacenter, deux switches dédiés seront placés avec des équipements (VSP 7400). Ils seront installés dans les deux salles à disposition chez Brainserve (1 par salle).

En complément et afin d'avoir un réseau homogène, les switches qui se trouvent sur la boucle réseaux seront changés par des ExtremeSwitching 5320. Cela permettra de profiter de tout le potentiel de la technologie « fabric connect » d'Extreme Network. C'est également dans un souci de cohérence et d'homogénéité au sein du réseau que la solution NAC du même fabricant (Extreme Network) a été choisie (voir chapitre 2.8).

2.4.3 Mise en œuvre

La société SPIE collaborera afin d'assurer cette transition car l'opération est relativement complexe. Tout d'abord, l'ensemble du trafic sera rerouté sur les nouveaux switches (5520), puis toutes les connexions fibres seront basculées.

Ensuite, il sera procédé à l'installation des switches dédiés au datacenter et serveurs, ainsi qu'à la connexion des équipements de la VSI.

2.5 Pare-feu (Firewall)

2.5.1 Situation actuelle

Une protection firewall (pare-feu) est un maillon essentiel au sein d'un réseau informatique. Sa principale fonction est de vérifier et d'analyser le trafic entrant et sortant du réseau de l'administration communale.

Depuis 2016, la solution Sophos UTM est utilisée. Elle est redondante et permet de couvrir la base au niveau protection périmétrique en incluant des fonctions de filtrages web ainsi que la mise en place et l'usage des connexions à distance via un tunnel sécurisé (VPN). Ce produit est toujours supporté mais n'est plus vendu. Au vu de son âge et de sa technologie, il ne répond plus aux standards et n'offre pas les possibilités actuelles quant à l'analyse et aux configurations.

2.5.2 Situation souhaitée

Les menaces, au niveau sécurité informatique, sont de plus en plus grandes et surtout, il est difficile de s'en prémunir avec une seule solution, somme toute efficace mais insuffisante. C'est pourquoi il est proposé de mettre en place la solution Fortigate de la société Fortinet. Elle permet en effet d'avoir un firewall de type périmétrique mais aussi des protections internes comme des firewalls virtuels qui admettent une segmentation du réseau.

Les menaces modernes se traduisent souvent par une intrusion non visible et des attaques de type latérale qui permettent aux hackers de « sauter » d'un réseau à l'autre afin de compromettre le système d'information.

Nos différents réseaux (VLAN) sensibles seront protégés par des pare-feux virtuels qui permettront de contrôler le flux de données interne.

2.5.3 Mise en œuvre

Cette action sera exécutée en plusieurs étapes et en collaboration avec la société SPIE (notamment par la forte imbrication entre le réseau et les pare-feux) car il y aura beaucoup d'éléments à migrer tels que :

- toutes les règles existantes ;
- les configurations VPNs,
- la configuration IPS ;
- la configuration des boîtiers pour les sites distants.

Une fois la migration des configurations et équipements de pare-feu sur la nouvelle solution effectuée, la configuration des pare-feux virtuels pour les différents réseaux pourra commencer.

2.6 Bastion (PAM)

2.6.1 Situation actuelle

L'équipe informatique travaille avec de nombreux partenaires informatiques, que ce soit pour du développement d'applicatifs métiers, de la configuration réseau ou encore des mises à jour de composants.

Actuellement, les partenaires se connectent à l'infrastructure, depuis l'extérieur via un simple accès VPN et accèdent aux différents serveurs selon les droits octroyés, sans que nous sachions, ni même ne suivions les actions entreprises. Toute cette démarche se base sur la confiance et le professionnalisme de chacun. Ceci est d'autant plus dangereux lorsque les partenaires se connectent à des serveurs disposant de données sensibles et/ou confidentielles.

Cet état de fait ne peut plus continuer car il ne correspond plus aux standards minimaux de sécurité dans le monde informatique. C'est pourquoi, il est question de mettre en place un bastion (système qui sécurise et contrôle l'accès à nos serveurs pour des fournisseurs). En effet, un bastion permet de fournir un point d'accès unique à des zones spécifiques, et particulièrement sensibles, du système d'information. Il permet en outre d'enregistrer les sessions des accès distants afin de garder une trace en cas de problème.

2.6.2 Situation souhaitée

Après plusieurs démonstrations de produits (Cyberark, Wallix, Microsoft), le choix s'est porté sur le produit Wallix.

Wallix est un éditeur français de logiciels de sécurité informatique fondé en 2003. Il est spécialisé dans la sécurisation des systèmes d'information et la gestion des infrastructures informatiques critiques. La plate-forme Bastion (le Bastion) offre les fonctionnalités de PAM (Privileged Access Management) suivantes :

- contrôle d'accès ;
- coffre-fort à mots de passe (uniquement pour la connexion aux bastions) ;
- gestion de l'accès privilégié ;
- gestion des mots de passe et des clés SSH.

En complément au produit de base, le produit « Wallix Access Manager » sera implémenté. Il propose une solution de connectivité sécurisée basée sur HTML5, accessible depuis le navigateur de n'importe quel utilisateur ou utilisatrice. Il élimine le besoin d'ouvrir une connexion à distance depuis le point d'accès de l'utilisateur, rendant l'accès à WALLIX Bastion depuis l'extérieur simple et riche en fonctionnalités. Les sessions à distance bénéficient du même niveau de contrôle, d'approbation, de suivi et de surveillance que les sessions internes. Ceci permet aux superviseurs informatiques de contrôler, d'auditer et d'effectuer des vérifications pour leurs utilisateurs distants comme s'ils étaient au bureau.

2.6.3 Mise en œuvre

La mise en œuvre est assez simple et elle serait accompagnée par la société SCRT basée à Morges. Le système est installé sur une machine virtuelle fournie par l'éditeur. Les mises à jour du système d'exploitation (Linux) et du logiciel sont fournies par Wallix. Une liste des accès fournisseurs sera établie afin de configurer le système en renseignant les serveurs et autres applicatifs qui devront être visibles par les fournisseurs selon leurs privilèges.

2.7 Application de contrôle web (WAF)

2.7.1 Situation actuelle

Un Web Application Firewall (WAF) est un type de pare-feu qui vérifie les données des serveurs web transitant par Internet (p. ex. le serveur eSéances). Si cette demande est conforme à l'ensemble de règles du pare-feu, ce dernier peut alors transmettre la demande à l'application. D'une manière générale, un WAF peut être défini comme une politique de sécurité mise en place entre une application web et l'utilisateur final en complément de pare-feux conventionnels.

2.7.2 Situation souhaitée

Après la comparaison de trois solutions différentes (Fortinet, Barracuda et F5), la solution retenue est F5. Il s'agit d'un système éprouvé qui est utilisé dans de nombreuses sociétés suisses et qui offre plusieurs fonctionnalités additionnelles allant au-delà d'un simple WAF.

En plus d'être implémentée comme WAF avancé, cette solution permettra :

- de gérer les certificats SSL de manière centralisée ;
- de gérer les connexions VPN qui auront une importance notoire en lien avec la nouvelle infrastructure et place de travail ;
- de permettre de gérer et répartir la charge du trafic réseau externe et interne ;
- de mettre à disposition un portail de connexion centralisé pour les différentes applications web de la Ville de Renens.

2.7.3 Mise en œuvre

Cette solution remplacera la solution basique actuellement en place (proxy open-source). L'ensemble des certificats SSL seront déplacés et gérés à travers cette solution. Les connexions VPN, qui sont actuellement gérées par notre pare-feu, seront remplacées par cet applicatif. Un portail sera créé et les applications web seront disponibles au travers de ce système avec une authentification forte.

2.8 NAC

2.8.1 Situation actuelle

Un contrôleur d'accès au réseau (network access control ou NAC) permet d'appliquer une politique de sécurisation aux utilisatrices et utilisateurs qui se connectent au système informatique. Il permet d'identifier et par conséquent d'appliquer des mesures/règles, sur des composants se connectant au sein du réseau.

Après un audit de sécurité réalisé par la société Seculabs en septembre 2020, il a été constaté, parmi les points d'amélioration, la mise en place d'un NAC. Actuellement, aucune solution n'est installée au sein du réseau de la Ville de Renens afin de contrôler les accès physiques sur le réseau. En d'autres termes, cela signifie qu'une personne venant de l'extérieur de la Ville pourrait brancher son PC sur une de nos prises et avoir accès à notre réseau par exemple.

2.8.2 Situation souhaitée

Plusieurs sociétés comme Cisco Systems, Microsoft ou Nortel Networks ont développé des structures permettant d'implémenter des mécanismes de protection d'accès au réseau d'entreprise et de vérifier le respect, par les postes clients, des règles de sécurité imposées par l'entreprise : état de la protection antivirus, mises à jour de sécurité, présence d'un certificat, etc.

La solution NAC d'ExtremeNetwork a été choisie pour garantir une uniformité, une cohérence et une intégration idéale avec l'infrastructure réseau telle que décrite au chapitre 2.4. Cette solution permet de fournir un accès réseau hautement sécurisé aux utilisatrices et utilisateurs et aux appareils. Elle aide à avoir une visibilité sur ce qui se passe sur le réseau, à savoir notamment qui est connecté, quelles applications sont installées et en cours d'exécution. Elle partage également des données contextuelles vitales, telles que les identités des utilisatrices et utilisateurs et des appareils, les menaces et les vulnérabilités, afin d'identifier, contenir et corriger les menaces plus rapidement.

2.8.3 Mise en œuvre

La configuration de protection se fait principalement sur les points d'accès réseaux (switches). Une politique de sécurité est appliquée sur chaque port (USB, etc.) pour définir quel équipement a le droit d'accéder aux ressources de l'entreprise.

Dans un premier temps, l'authentification des appareils se fera avec le certificat généré par notre autorité de certification (chaque poste de travail en possède un). Pour les équipements qui ne peuvent pas gérer de certificats (imprimantes, IOT, etc.) l'authentification se fera par l'adresse MAC (identification unique de chaque carte de communication).

2.9 Sauvegardes et archives

2.9.1 Situation actuelle

Les sauvegardes (backups) de l'infrastructure informatique communale sont gérées par le logiciel Veeam. Elles sont actuellement stockées sur une série (baye) de disques à la rue de Lausanne 35. Celle-ci est répliquée dans une autre salle à la rue Lausanne 21. De plus, certaines sauvegardes des serveurs critiques sont aussi envoyées sur un stockage cloud chez Infomaniak en Suisse.

La fréquence des sauvegardes est journalière pour tous les serveurs (de 18h30à 00h00). La sauvegarde est incrémentielle. Plus performante et plus rapide qu'une sauvegarde totale, la sauvegarde incrémentielle permet de se focaliser sur les nouveaux fichiers ainsi que sur les fichiers ayant subi des modifications tout en minimisant l'impact sur le stockage de l'information. Ainsi, une sauvegarde incrémentielle peut être définie comme une suite logique d'une sauvegarde complète et d'une sauvegarde incrémentale. Par ailleurs, pour reconstituer une sauvegarde complète, toutes les sauvegardes précédentes doivent être regroupées.

Il est à noter que la capacité actuelle de sauvegardes ne permet pas de sauvegarder l'ensemble de nos systèmes sur une durée souhaitable. Elle ne permet pas une sauvegarde optimale en ce qui concerne sa rétention, sa fréquence ainsi que leur emplacement au sein de l'infrastructure réseau.

2.9.2 Situation souhaitée

L'objectif est d'accroitre et d'améliorer notre système de sauvegarde notamment sur les deux aspects suivants :

- mettre en place un vrai système de secours, en tirant parti de l'architecture de Brainserve. Nos systèmes seront placés dans deux salles différentes au sein de ce datacenter afin de garantir la sécurité et la redondance des données. De plus, toutes les sauvegardes seront exportées chez Infomaniak afin de garantir la troisième copie à l'extérieur de notre salle informatique ;
- accroitre notre système de sauvegarde qui est actuellement correct, en respectant encore plus scrupuleusement le principe 3-2-1-1 qui est :
    - disposer de trois copies (3) des données au moins ;
    - stocker ces copies sur deux supports (2) différents ;
    - conserver une copie (1) de la sauvegarde hors site ;
    - conserver une copie (1) de la sauvegarde hors-connexion.

  À ceci, viendrait se rajouter une notion d'archive inaliénable qui signifie que le support de stockage sera non effaçable. Ces supports permettent l'écriture de données mais ne permettent pas l'effacement. Il est donc possible d'écrire une fois et de lire autant de fois que souhaité sans jamais pouvoir physiquement effacer la donnée écrite.

2.9.3 Mise en œuvre

Le choix s'est porté sur une solution qui est pleinement compatible avec la solution actuellement utilisée pour les sauvegardes (Veeam). Cette dernière sera ainsi conservée pour des questions de connaissances et de coûts. La stratégie s'est portée sur un changement du type de support de stockage de ces sauvegardes.

La solution FAST LTA, fournie par la société Eurebis qui est un acteur spécialisé dans le monde du stockage de la sauvegarde, a été retenue car elle répond à l'ensemble des critères précités. Elle est éprouvée et bénéficie de références solides. Le principe de ce système est composé de briques de natures différentes (sauvegardes standards, inaliénables, etc.).

Voici la plateforme de base qui permet d'accueillir ces briques :

Figure 3 : Silent bricks – source : https://www.fast-lta.de/

Les briques sont présentées ainsi et peuvent être retirées/ajoutées au sein du système selon le contexte d'utilisation.

2.10 Onduleurs

Les onduleurs sont des équipements informatiques permettant de maintenir les serveurs, durant un certain laps de temps, actifs et ainsi d'effectuer un arrêt correct lors d'une panne/coupure de courant. La Ville dispose de différents types et tailles d'onduleurs selon leurs emplacements et leurs contextes d'utilisation.

Les onduleurs actuellement présents dans les deux salles du centre du calcul sont relativement imposants. Ils sont posés à même le sol (risqué en cas d'inondation) et ne tiennent qu'une heure. Ces salles, à terme, vont disposer de moins d'équipements mais qui devront tenir plus longtemps en cas de panne. Il est proposé de profiter de cette impulsion pour changer les onduleurs à la rue de Lausanne 33 et 35 avec les objectifs suivants :

- disposer de nouveaux onduleurs qui puissent être mis dans les armoires informatiques et par conséquent réduire le risque lié aux inondations ;
- étant donné la réduction du nombre d'équipements et par conséquent de leur consommation électrique, l'objectif est de pouvoir tenir 4h avec ces nouveaux composants.

Les équipements sont issus de la même entreprise qui s'occupe déjà des onduleurs communaux en l'occurrence la société Statron SA. La mise en œuvre de ces nouveaux onduleurs sera la suivante :

- mise en place des nouveaux onduleurs dans la salle de la rue de Lausanne 33 ;
- mise en place des nouveaux onduleurs dans la salle de la rue de Lausanne 35.

Dans un souci de sobriété numérique, les onduleurs actuellement en place à la rue de Lausanne 33 seront réutilisés et remis en marche pour l'étage de l'IT, car ils sont encore sous garantie. En revanche, ceux de la rue de Lausanne 35, ayant presque 10 ans et n'étant plus sous garantie, seront décommissionnés et détruits.

La maintenance des nouveaux onduleurs sera incluse dans celle qui est déjà en vigueur et traitée par voie budgétaire via le service Bâtiments-Domaines-Logement (BaDoLog).

2.11 Microsoft 365

2.11.1 Situation actuelle

La suite Microsoft Office 2019 fait partie des équipements logiciels incontournables de l'administration communale notamment pour les logiciels suivants : Word, Excel, PowerPoint et Outlook. Cette version dispose, plusieurs fois par année, de mises à jour de sécurité fournies dans le cadre des « mises à jour Windows mensuelles ».

La politique de Microsoft, depuis maintenant plusieurs années, consiste à une orientation de plus en plus marquée pour l'usage de son nuage (Cloud) notamment pour les produits Microsoft 365. À travers cette orientation, de nombreuses fonctionnalités et évolutions sont réservées à ceux bénéficiant de ces types de licences/abonnements. De plus, il apparait évident qu'une intégration parfaite entre les différents outils Microsoft passe obligatoirement par une centralisation de leur gestion et par conséquent par l'usage des solutions Microsoft 365.

2.11.2 Situation souhaitée

Un passage intégral à Microsoft 365 permettrait de tirer parti des nouvelles possibilités technologiques et des nouveaux logiciels. Voici ci-dessous quelques avantages :

- utilisation exclusive de Microsoft Teams pour l'ensemble des aspects de visio-conférences et de chats. Ceci permettrait de s'affranchir du logiciel Zoom ainsi que de multiples autres solutions hors de contrôle ;
- mise en place de la suite Office 365 pour l'ensemble des utilisateurs et utilisatrices qui ont actuellement Office 2019. Ceci permettra de s'affranchir des mises à jour réalisées manuellement ;
- fourniture d'une adresse électronique @renens.ch à l'ensemble des collaboratrices et collaborateurs de la Ville de Renens ;
- Intégration de la solution Microsoft Endpoint Manager (MEM) pour la gestion des périphériques mobiles (propriété de la ville) et les postes de travail ;
- la gestion des courriels ne sera plus faite à travers notre serveur interne. En effet, le serveur Microsoft Exchange est régulièrement la cible d'attaques dues aux nombreuses failles de sécurité. Par conséquent, l'usage de Microsoft Exchange Online (serveur de messagerie dans le cloud) permettrait d'être moins vulnérable à certaines failles. De plus, il est important de noter que Microsoft Exchange Online est un rouage essentiel au bon fonctionnement de l'écosystème Microsoft 365 notamment Microsoft Teams ;
- cependant, le fait de bénéficier de cette fonctionnalité, obligera la mise en place de mesures complémentaires quant à la confidentialité des données et de sécurité, notamment le cryptage de certains courriels (voir le point 2.14).

2.11.3 Mise en œuvre

Ce passage à Microsoft 365 s'accompagnera de plusieurs mesures indispensables en matière de gouvernance et de sécurité des données :

- préalablement, une analyse de risques est en cours d'élaboration pour mesurer les différents impacts et comment traiter ceux-ci ;
- les applications SharePoint, ainsi que Onedrive seront bloquées ;
- la mise en place de Microsoft Teams s'accompagnera de formations en interne ainsi que de certaines restrictions à l'usage afin de protéger la diffusion de certains types de documents ;
- le serveur de messagerie (Microsoft Exchange) sera remplacé par Exchange Online ;
- la suite Office 365 sera déployée sur l'ensemble des postes du personnel ;
- chaque collaboratrice et collaborateur de la Ville disposera d'une adresse électronique @renens.ch, ce qui impliquera une augmentation de l'abonnement 365.

2.12 Antivirus

2.12.1 Situation actuelle

L'antivirus utilisé au sein de l'informatique de Renens est Kaspersky Antivirus. Il s'agit d'un antivirus qui est réputé mais qui est complexe dans son administration et qui provoque certaines problématiques dans l'infrastructure actuelle (lenteur, analyse, gestion des mises à jour inadéquate). De plus, il s'agit d'un antivirus d'ancienne génération (basée sur des signatures). Cet antivirus, avec les licences actuelles, n'est pas prévu pour être déployé sur des périphériques autres que les PC comme notamment les mobiles de la Commune, les tablettes ou différents composants IoT.

2.12.2 Solution souhaitée

L'objectif est par conséquent de disposer d'une solution antivirus de dernière génération qui permette une centralisation de son administration, ainsi que de sa gestion/configuration. De plus, il doit pouvoir être utilisable dans d'autres contextes que les PC (fixes ou portables). Il doit offrir l'ensemble des fonctionnalités avancées notamment :

- gestion des bacs à sable (environnement de test ne mettant pas en péril la solution en production) pour analyser certains éléments ;
- gestion des périphériques ;
- nouvelle génération d'anti-malware ;
- possibilité dans le futur de s'interfacer avec les systèmes de gestion des événements et des informations de sécurité (SIEM) ;
- système de détection et réponse des terminaux (EDR).

2.12.3 Mise en œuvre

Après comparaison entre « 365 Security » de Microsoft et Crowdstrike de Falcon, la solution retenue est Microsoft 365 Security car elle offre une palette de fonctionnalités permettant une excellente couverture pour l'antivirus et l'EDR ainsi que dans la gestion des entités et dans l'analyse des activités. De plus, son intégration est parfaite avec l'écosystème Microsoft 365 souhaité et décrit au chapitre 2.11.

2.13 Anti-spam

2.13.1 Situation actuelle

Un système anti-spam permet de filtrer en amont et par conséquent avant réception dans le client de messagerie de l'utilisateur final, les courriels qui sont jugés comme étant indésirables (pub, hameçonnage). Il représente un maillon important de la chaine sécuritaire.

La Ville de Renens dispose actuellement d'une solution qui est fournie par un prestataire tiers et qui met à disposition son système anti-spam (Barracuda Anti-spam). L'administration de cette plateforme ainsi que ces règles d'exclusions ne sont pas en mains de l'équipe IT qui, par conséquent, pas la pleine latitude pour utiliser cet outil.

2.13.2 Situation souhaitée

En complément de la solution de pare-feu proposée, il est indispensable de pouvoir bénéficier d'un produit complétement intégré avec Fortigate (Société Fortinet) et ainsi proposer un système anti-spam allant au-delà d'une simple détection en offrant les fonctionnalités suivantes :

- détection avancée de malware ;
- suivi des messages ;
- prévention de perte de données ;
- bacs à sable pour exécuter pour analyser et ouvrir les courriels reçus ;
- intégration possible avec l'écosystème Microsoft 365 au besoin.

2.13.3 Mise en œuvre

La solution Fortimail a été retenue car elle présente l'ensemble des fonctionnalités ci-dessus. Elle offre une intégration avec la solution Fortigate (pare-feu). Avec celle-ci, il est possible soit de travailler avec

un écosystème local soit d'interagir directement avec Microsoft 365, ce qui permet de disposer d'une très bonne flexibilité quant à son implémentation dans différents environnements.

2.14 Chiffrement des courriels

Le chiffrement des courriels est un mécanisme de sécurisation entre l'expéditeur et le destinataire. Il permet d'en traiter le contenu qui est confidentiel et/ou qui contient des données jugées sensibles.

La solution retenue est la solution suisse se nommant : SEPPMAIL. Cette solution est une référence en la matière, notamment dans l'échange de courriels dans le domaine médical (ex : communication entre les hôpitaux). Elle permet à la fois de traiter des échanges sécurisés avec des partenaires disposant de la même solution ou d'une autre technologie. De plus, cette solution offre la possibilité de crypter ou non un courriel selon les besoins.

Cette mesure permet de renforcer la confidentialité des données dans un environnement de nuage (cloud).

2.15 Archivage des courriels

2.15.1 Situation actuelle

La Ville de Renens travaille actuellement avec une serveur Exchange local et son client de messagerie Microsoft Outlook. La gestion des archives n'est pas traitée dans la mesure où cette dernière est de la responsabilité de chaque collaborateur ou collaboratrice.

En effet, les archives sont actuellement gérées individuellement par l'entremise de fichiers *.pst qui sont des fichiers de données Outlook. Ces fichiers sont souvent problématiques notamment pour les raisons suivantes :

- ils sont sauvegardés à différents endroits sans forcément que l'utilisateur ou l'utilisatrice en soit conscient ;
- ils sont instables et s'ils venaient à être corrompus ou endommagés, il est très rare de pouvoir les récupérer ➔ Perte de données ;
- la taille de ces fichiers atteint parfois plusieurs Go de données. Par conséquent, ils consomment du stockage et ralentissement considérablement l'ouverture de la messagerie.

Ceci engendre finalement un risque certain de perte de courriels et de certaines informations qui sont parfois essentielles.

2.15.2 Situation souhaitée

L'objectif est de s'affranchir de ces fichiers PST par la mise en place d'un « archiveur » de courriels. Il permet d'enregistrer tous les courriels sortants et entrants des boites courriels sans qu'ils puissent être modifiés. Avec une telle solution, il sera possible de garantir le fait qu'un courriel soit inaliénable et par conséquent qu'il puisse être utilisé comme preuve dans certaines situations.

Chaque utilisateur ou utilisatrice pourra ainsi rechercher dans son archiveur les courriels reçus et envoyés sans devoir travailler avec des fichiers pst.

2.15.3 Mise en œuvre

En complément du chapitre 2.11, il est question d'utiliser une nouvelle solution d'archivage qui se veut être découplée de l'écosystème Microsoft. La solution retenue est Cryoserver.

Ce système est à la fois éprouvé à travers le monde et possède les avantages suivants :

- rendre ces archives inaliénables ;
- offrir un système de recherche performant et intégré à Outlook ;
- permettre l'interfaçage soit avec Exchange On Premise ou Microsoft 365 (Exchange Online).

Cet équipement se trouvera sur l'infrastructure communale à Brainserve, et par conséquent les archives courriels seront au sein de notre infrastructure.