RAPPORT DE LA COMMISSION TECHNIQUE

Préavis municipal n° 32bis/2023

Demande de crédit pour la sécurité informatique

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

La commission technique (ci-après CT) constituée de :

- son président : Christian Bovey
- ses membres : Karim Ben Nsir et Rudolf Kraftsik

a élaboré par échange de courriel une liste de question. Elle s'est réunie le mardi 25 avril en présence de Madame la Municipale Jennifer Dagon, de Monsieur le Municipal Denis Favre et de Nicolas Ray (Secrétaire municipal et responsable informatique). Nous les remercions pour leurs explications et les réponses aux dites questions. La commission s'est encore réunie le jeudi 4 mai 2023 avant le retrait de la première version du préavis.

La commission s'est à nouveau réunie le mardi 22 août 2023 (Karim Ben Nsir excusé) en présence de Monsieur le Municipal Denis Favre et de Monsieur Pardo (Directeur technique chez Silicom Group). Nous les remercions pour les explications et les réponses aux questions.

La commission s'est encore réunie le 28 août 2023 afin de statuer et finaliser son rapport.

1. Documentation à disposition

La CT s'est basée sur les documents suivant pour établir son rapport :

- Les deux versions du préavis auquel s'ajoutent les documents demandés et obtenus suivants :
- le schéma du réseau informatique de la commune
- les offres du prestataire (Silicom Group, à Romanel), en consultation lors des séances
- un tableau récapitulatif des investissements/contrats par sujet

2. Préambule

Comme nous le montre régulièrement l'actualité, les problèmes liés à la sécurité informatique sont de plus en plus fréquents et peuvent bloquer complètement une entreprise ou une administration communale.

Notre commune a déjà fait l'objet d'une attaque et les frais de remise en état, sans tenir compte du temps perdu, représentaient une somme dépassant largement celle demandée dans ce préavis.

Dans son rapport en 2021[1], la commission de gestion s'était penchée sur ces aspects et faisait entre-autres les recommandations suivantes :

- Pour les employés communaux et les Municipaux, avoir la possibilité de se connecter à distance de façon simple, fiable et de manière sécurisée ; la méthode actuelle ne donnant pas satisfaction
- Les sauvegardes sur bande et les machines (serveurs) ne devraient pas être localisées dans le même bâtiment
- Veiller à ce que le responsable informatique de la Commune suive régulièrement des formations en lien avec la sécurité du système informatique.

Comme nous allons le voir, ce préavis permet de répondre à une partie de ces recommandations.

[1] Rapport commission de gestion 2021, page 8-12

3. Solution de connexion à distance

La solution utilisée actuellement utilise des clés « Ubiquiti » et ne donne pas satisfaction, le fonctionnement est aléatoire, particulièrement sur les portables tout en ne proposant pas de double-authentification.

Le prestataire informatique propose de mettre en place une architecture exploitant VMware Horizon pour la connexion au réseau. Les utilisateurs pourront à partir de cette connexion accéder à un « terminal-serveur[2] ».

- Cette solution va donc au-delà de l'accès à distance en offrant à la fois plus de sécurité et de souplesse.
    - Les utilisateurs itinérants ne sont pas directement connectés au réseau communal, mais à une session virtuelle sécurisée hébergée par un serveur de la commune.
        - Les fichiers restent sur les serveurs de la commune et ne peuvent pas être copiés à l'extérieur, à l'inverse il n'est pas possible d'introduire des éléments dangereux sur le réseau communal.
        - Les seules données qui transitent (via un tunnel sécurisé) sont uniquement l'affichage et le son depuis la session virtuelle vers l'utilisateur et les commandes (clavier, souris, …) dans l'autre sens.
        - Cette solution permet en outre d'utiliser n'importe quel type d'équipement pour se connecter et travailler (par exemple un iPad ou une tablette Android), et ce avec toutes les applications métier.
    - Enfin, cela simplifie le travail itinérant en permettant de passer d'une machine physique à une autre en conservant l'intégralité de la session ouverte, comme si on avait uniquement changé d'écran.
- La connexion passera par une double authentification (identifiant et mot de passe, puis validation par une application sur smartphone). Une vérification par SMS pourrait également être mise en place, mais n'est ni privilégiée ni recommandée.
    - La CT s'est demandé si la double authentification resterait requise même si l'utilisateur se connecte depuis le réseau communal. Cela sera effectivement le cas de manière à offrir un mode de fonctionnement uniforme quelle que soit la situation.

Cette solution requiert plusieurs licences dont certaines ne peuvent être commandées que par lot de 10 au minimum.

Liste des licences et attributions si la solution est mise en place à plus large échelle :

Licences/Utilisateur	Qté. min.	Municipalité	Employés	Total
MS Defender for server – Antivirus	1	2 licences (VMware + terminal serveur)		
Vmware Horizon ***(Une par accès concurrent)***	5	5	5	10
Microsoft – Business Premium ***(Voir le point sur Office 365)***	10	5	35	40

Tableau d'attribution des licences

Dix utilisateurs peuvent utiliser la solution en même temps :

- Nos cinq municipaux qui devraient utiliser la solution quotidiennement.
- Cinq parmi les employés communaux, avec une prévision de 1 à 2 accès par semaine pour chacun d'eux.

[2] Un terminal-serveur met à disposition de l'utilisateur une session sur laquelle il peut se connecter et retrouver ses documents et ses applications.

Un des objectifs de la solution est de permettre d'accéder aux applications communales. Les programmes prévus sont les suivants :

- les produits de la suite MS Office (Word, Excel, Outlook, …)
- les composants de l'ERP communal (Abacus, Innosolve et GED)
- les outils spécifiques de chaque service (Mobatime, gestion des séances, SIT, MaCantine, …)

Les collaborateurs se connectent avec leur propre matériel à la maison ou avec leur portable professionnel au travail. Il n'est pour l'instant pas prévu de les laisser prendre leurs PC professionnels à la maison.

La CT s'interroge pour les séances se déroulant à l'extérieur. Nos Municipaux ou collaborateurs n'auront pas toujours accès à un réseau et dès lors cette solution ne permettra pas d'accéder aux données communales. Afin de contourner ce problème, les utilisateurs concernés pourront préalablement transférer les fichiers nécessaires sur leurs portables professionnels sécurisés (Il ne doit pas y avoir de données communales sur des machines privées).

La CT trouve cette solution pertinente, elle isole plus efficacement le réseau communal et devrait offrir une connexion fiable aux utilisateurs.

Pour la phase de test, un terminal-serveur virtuel sera installé sur un des serveurs déjà présents à la commune, il ne sera donc pas nécessaire d'acheter du matériel. Ce serveur sera en outre capable de gérer la charge de dix utilisateurs concurrents si la solution est retenue. Au niveau des licences, des versions d'évaluation seront utilisées.

4. Passage des utilisateurs sur Office 365 et mise à jour des anti-virus et anti-spams

Ce sujet ne faisait pas entièrement partie de la première version du préavis. A l'origine, seuls les utilisateurs se connectant à distance étaient concernés.

Différentes versions de la suite Office sont actuellement installées sur les ordinateurs de la commune, dont certaines ne sont plus maintenues. La Municipalité profite de cette opération pour mettre à niveau tout le parc et de l'aligner à la dernière version.

La CT s'est interrogée sur le type de licence, plusieurs variantes étant possibles et la plus chère (Business Premium) ayant été retenue. Plusieurs raisons expliquent ce choix :

- Seule cette version peut être installée sur un terminal-serveur.
- Elle inclut une licence pour Defender Business Premium qui offre une meilleure sécurité et permet de se passer d'un antivirus supplémentaire
- Elle permet une gestion centralisée de ces applications

La majeur partie des licences seront nominatives. Quelques-unes seront dédiées à des comptes génériques pour les collaborateurs à temps partiel. 39 licences sont dédiées à sécuriser les adresses mails non nominatives (Ex : secretariat.cc@romanel-sur-lausanne.ch)

Il aurait été possible de faire quelques économies sur ces licences (en prenant 20 licences business standard), mais au prix d'une solution hétérogène, nettement plus compliquée à maintenir et moins sécurisée.

Le stockage des données dans le cloud est interdit, mais l'utilisation de logiciels tels que « Teams » restera possible. Les utilisateurs seront sensibilisés afin de ne pas transférer de fichier par ce biais.

La CT est donc d'avis que la solution retenue est la bonne.

5. Externalisation des copies de sécurité

La CT s'est premièrement demandé si une solution intercommunale avait été envisagée. Cela n'est pas le cas. D'une part il n'est pas forcément évident de trouver une commune de taille similaire. D'autre part, par expérience, les communes tiennent à leurs indépendances à ce niveau.

La prestation comprend la sauvegarde des systèmes complets (OS + programmes + données), la restauration en cas de problèmes et le monitoring des sauvegardes.
Les postes utilisateurs ne sont pas concernés, cependant les employés sont sensibilisés au fait que les données ne doivent pas être stockées en local mais sur les serveurs uniquement.

Les sauvegardes sont effectuées de manières quotidiennes, hebdomadaires et mensuelles. Elles permettent au besoin de facilement et rapidement revenir en arrière en garantissant une perte de données minimum dans ce genre de situation.

Les données étant sauvegardées plusieurs fois, sur des supports et sites différents par le prestataire, la CT relève qu'il devrait être possible de diminuer le nombre de sauvegarde en interne. On nous a confirmé que c'est effectivement un objectif. Cela permettra de supprimer une tâche récurrente (le changement des bandes sur le serveur de sauvegarde), mais également de se passer du renouvellement du matériel de sauvegarde.

Les données transiteront par notre prestataire, mais seront hébergée chez Infomaniak.

Bien que cela ne soit pas son rôle, la CT s'est étonnée du prix demandé pour le stockage des données. Une part de l'explication provient des technologies utilisées (VEEAM), mais aussi du processus utilisé lors du transit qui permet de garantir que les données ne peuvent pas être supprimées même par les administrateurs. Une solution alternative qui n'est arrivée qu'après la rédaction du préavis est envisagée et pourrait diminuer les coûts. Elle laisse le soin à la COFIN d'amender le préavis si elle le juge nécessaire.

Sur le plan technique, la CT trouve cette solution appropriée.

6. Renouvellement et mise à jour de licences serveurs

Lors du préavis n°18/18, les licences nécessaires au fonctionnement des serveurs ainsi que les extensions de garanties ont été signés pour cinq ans. Entre les deux versions du préavis, ces licences ont expirés.

Cette dépense a été oubliée dans le budget 2023. La CT estime nécessaire de renouveler ces licences et extensions au plus vite afin de garantir le fonctionnement de notre infrastructure. Il n'est pas utile à ce stade d'essayer de changer de version ou prestataire. Ces démarches devront néanmoins être effectuées lorsque le matériel devra être renouvelé.

7. Réalisation d'un audit de sécurité

L'audit de sécurité choisi est celui recommandé par l'UCV (Union des Communes Vaudoises). Il a déjà été mise en œuvre avec satisfaction dans plusieurs communes.

Plusieurs versions et processus peuvent être sélectionnés. Le modèle retenu est le plus complet :

- Il commence par un diagnostic initial. Selon l'expérience de Monsieur Ray qui a déjà eu l'occasion d'en faire un, de nombreux points nécessiteront une adaptation avant de pouvoir passer à l'audit. Une grande part de ces corrections concernera la documentation des processus. La CT sera tenue au courant des résultats de ce premier diagnostic. Un préavis complémentaire sera peut-être nécessaire à ce stade.
- Une fois que tous les points à régler l'auront été, l'audit pourra avoir lieu et la commune recevra sa certification.

- La certification est valable durant deux années. Durant cette période, la société « Cyber-Safe » procédera encore à des tests de sécurité.

Cet audit semble essentiel à la CT. Il permettra non-seulement de corriger les faiblesses dans le système d'informations communal, mais amènera également à une documentation qui facilitera le travail par la suite.

8. SwissID

Bien que cela ne soit pas le sujet direct de ce préavis, un membre de la CT se demande si le système d'identification SwissID sera mis en place au niveau de la commune. Nous avons obtenu la réponse suivante :

Il s'agit d'une piste très intéressante et qui deviendra probablement indispensable dans un proche futur (actuellement, elle est surtout utilisée par des cantons ou par les villes, plus que par les petites communes). Actuellement, aucune démarche n'a encore été entreprise par manque de temps.

9. Remarques

La CT souhaite que parallèlement à l'audit de sécurité une réflexion globale soit menée sur les besoins futurs afin d'anticiper le renouvellement de matériel et de préparer le passage à Windows 11 (ou son éventuel successeur).

La CT souhaite qu'une formation/sensibilisation à l'utilisation de Microsoft 365 et de ces services cloud soit mise en place.

La CT rappelle que les données sensibles ne doivent pas être transférées sur des ordinateurs privés et recommande l'usage de portables gérés par notre prestataire.

Dans le contexte actuel, la mise en place des solutions proposées dans ce préavis devient vitale pour le bon fonctionnement de l'administration communale et de ces services. Il est en outre de sa responsabilité de protéger ses données sensibles ainsi que celles de nos citoyens. De manière générale, la CT pense que la mise en place de ce préavis devrait permettre de tendre vers ces objectifs.

10. Conclusions

Compte tenu des éléments ci-dessus, la CT adopte à l'unanimité de ses membres le préavis n°32bis/2023 et vous invite, Mesdames et Messieurs les Membres du Conseil Communal de bien vouloir prendre les décisions suivantes :

LE CONSEIL COMMUNAL DE ROMANEL-SUR-LAUSANNE

- vu le préavis municipal No 32bis/2023 adopté en séance de Municipalité du 31 juillet 2023 ;
- ouï le rapport de la Commission des finances ;
- ouï le rapport de la Commission technique ;
- considérant que cet objet a été porté à l'ordre du jour ;

décide :

- d'accepter le préavis tel que présenté ;
- d'accorder un crédit de CHF 36'000.00 TTC pour la réalisation d'un audit de sécurité informatique et la mise en place de mesures urgentes ;
- d'autoriser le financement de cette dépense par la trésorerie courante ou, au besoin, sur les lignes de crédit disponibles, dans les limites du plafond de l'endettement ;
- d'autoriser l'amortissement de cette dépense sur une durée maximale de trois ans.

Romanel-sur-Lausanne, le 28 août 2023

Le Président-rapporteur :

Christian Bovey

Les autres membres :

Karim Ben Nsir

Rudolf Kraftsik