

Rapport de la Municipalité

sur le

Postulat du 23 avril 2021 de M. Marc MAILLARD intitulé

« *Données communales et piratage informatique* »

Table des matières

1	Préambule.....	2
2	Une approche globale.....	2
3	Actions entreprises.....	2
3.1	Solutions matérielles	3
3.1.1	Accès aux locaux techniques	3
3.1.2	Redondance.....	3
3.1.3	Documentation.....	3
3.2	Solutions logicielles et techniques	3
3.2.1	Accès distant.....	3
3.2.2	Double authentification.....	3
3.2.3	Infrastructure.....	3
3.2.4	Outils informatiques	3
3.3	Solutions humaines	3
3.3.1	Engagement d'un responsable informatique	3
3.3.2	Formation des collaborateurs.....	4
3.3.3	Développement d'une culture du dialogue.....	4
4	Audit de sécurité	4
5	Poursuite des efforts	4
5.1	Risques résiduels	4
6	Conclusion.....	5

1 Préambule

Le postulat demande à la Municipalité si celle-ci a procédé à une analyse de risque pour notre Commune en ce qui concerne sa possible vulnérabilité informatique, en particulier face aux risques d'une attaque informatique ciblant ses données et celles personnelles et fiscales de ses administrés ou le cas échéant, de faire cet exercice et de présenter ensuite au Conseil son constat sur l'état de préparation de notre Commune en termes de protection de ses données informatiques. En corollaire, la demande consiste également à savoir comment sont évalués la qualité de nos infrastructures et le savoir-faire des responsables de l'informatique communale et de leurs utilisateurs face à de telles attaques.

2 Une approche globale

La Municipalité traite le sujet du numérique avec sérieux et est consciente des enjeux qui y sont liés. En effet, si le postulat concerne principalement la question sécuritaire et des attaques venant de l'extérieur, il est important de pouvoir rappeler que le développement d'une approche globale du sujet est nécessaire. La numérisation peut apporter des solutions intéressantes dans le traitement de l'information et dans ce sens, elle peut présenter des opportunités. Elle doit également permettre à l'administration de communiquer en son sein de manière efficace, tout comme avec ses partenaires externes. Le stockage, le partage et la disponibilité d'information, indépendamment du lieu et du temps, doivent participer à fluidifier les flux de travail. Or, si ces solutions s'imposent avec le temps et deviennent indispensables, elles engendrent alors aussi de nouveaux risques.

Certaines méthodes de travail sont imposées par les autorités cantonales ou fédérales, notamment dans des domaines tels que la comptabilité et le contrôle des habitants. Dans ce contexte, de nombreuses démarches ont d'ores et déjà été entreprises depuis le début de la législature pour limiter le risque de survenance d'un événement entraînant une coupure de service, la perte ou le vol de données et limiter l'impact d'un tel événement. Cette double démarche doit être un souci permanent, le contexte interne et externe de l'administration étant en constante évolution. C'est ainsi qu'à l'avenir, d'autres mesures continueront à être prises pour améliorer encore la protection des données informatiques communales.

Actuellement, les efforts pour limiter les risques et protéger les données sont concentrés principalement – mais pas exclusivement - dans les trois domaines suivants:

- matériel (accès, redondance, etc.)
- logiciel/technique (accès, mise à jour, chiffrement, solution sécuritaire, etc.)
- humain (formation, sensibilisation, développement d'une culture ouverte, etc.)

Pour accompagner ce processus, la Municipalité a décidé d'internaliser certaines tâches liées à l'informatique en procédant à l'engagement d'un collaborateur (voir chapitre 3.3.1). Toutefois, dans certains domaines particuliers et spécifiques, il est fait appel à des spécialistes.

On ne peut toutefois nier que les investissements consentis par le passé n'ont parfois pas été à la hauteur des défis. Cette situation tend à se corriger, mais l'inertie d'une telle démarche peut être de plusieurs années.

3 Actions entreprises

Bien que la sécurité des données communales a toujours été une préoccupation, un renforcement des mesures a été opéré. L'actualité a donné raison à la Municipalité et la réconforte dans son action.

Voici une liste non exhaustive – mais permettant de se rendre compte des efforts - des actions entreprises au sein de l'administration communale récemment pour protéger ses données.

3.1 Solutions matérielles

3.1.1 Accès aux locaux techniques

Les accès physiques aux locaux techniques ont été revus. Leur accès est limité strictement au personnel nécessaire.

3.1.2 Redondance

L'infrastructure est répartie dans plusieurs locaux, situés dans plusieurs bâtiments différents. Cela permet d'avoir une certaine redondance quant à l'exploitation et au stockage des données.

3.1.3 Documentation

L'ensemble de l'infrastructure communale a été documenté. Cela doit permettre d'identifier plus rapidement chaque élément. De plus, la connaissance n'est ainsi plus l'apanage d'une seule personne, mais permet si nécessaire d'inclure d'autres collaborateurs.

3.2 Solutions logicielles et techniques

3.2.1 Accès distant

Seuls les services informatiques absolument nécessaires sont exposés et accessibles depuis l'extérieur (internet). Pour ces derniers, les protocoles utilisés et leur mise en application sont chaque fois analysés. En cas de doute, le service est coupé. Bien que cette mesure soit exceptionnelle, elle a déjà été activée.

3.2.2 Double authentification

Chaque fois que cela est possible, une double authentification est mise en place. Cette mesure ne peut néanmoins pas être systématiquement mise en application, tous les fournisseurs ne la proposant pas.

3.2.3 Infrastructure

Un suivi des mises à jour de l'infrastructure a été mis en place pour limiter les possibles vulnérabilités des systèmes informatiques. De plus, tous les services, les applications et les serveurs obsolètes ou non utilisés sont supprimés.

3.2.4 Outils informatiques

Divers outils sont mis à disposition des collaborateurs afin d'améliorer la sécurité des données et limiter les risques.

- Un antispam contrôle les fichiers reçus par email et limite le nombre d'emails indésirables reçu par le personnel de l'administration communale.
- Un antivirus sur les serveurs et les postes de l'administration bloque l'exécution de programmes malveillants et contrôle les documents téléchargés.
- Un gestionnaire de mots de passe a été déployé pour améliorer la sauvegarde, la complexité et le partage des mots de passe utilisés pour les différents accès aux applications, plateformes en ligne, etc.
- Des certificats personnels pour les emails ont été installés pour permettre d'authentifier l'expéditeur des messages et de chiffrer certains emails.

3.3 Solutions humaines

3.3.1 Engagement d'un responsable informatique

Un chef de projet "systèmes d'information" (ETP 80%) a été engagé au 1^{er} janvier 2022 pour reprendre la gestion complète de l'infrastructure informatique et du budget informatique ainsi que pour mener à

bien les projets liés au SI. C'est également la personne de référence pour les prestataires externes liés à l'informatique. Ce collaborateur a également rejoint l'Association Vaudoise des Responsables informatiques Communaux (AVRIC) courant 2022 pour se tenir au fait des problématiques informatiques des autres communes vaudoises, ainsi que des questions de cybersécurité.

3.3.2 Formation des collaborateurs

Plusieurs formations/sensibilisations ont été dispensées au personnel de l'administration communale pour améliorer ses connaissances au niveau des risques liés à l'utilisation des outils informatiques, pour limiter les risques d'intrusion et afin d'apprendre à reconnaître les menaces informatiques. Les collaborateurs ont été informés sur les bonnes pratiques à adopter pour sécuriser leur poste de travail et limiter les risques lors de l'utilisation d'application ou de plateformes externes à l'administration communale. La dernière formation en cybersécurité a été suivie à la fin de l'année 2023 par 62 collaborateurs de l'administration communale. Cette démarche a concerné tout le personnel ayant accès à du matériel informatique communal : chefs de service, employés de voirie, secrétaires, personnel technique, agents d'exploitation, etc. Ceci dans tous les services de l'administration.

3.3.3 Développement d'une culture du dialogue

La Municipalité promeut une culture d'entreprise qui tolère un certain droit à l'erreur et qui permet aux collaborateurs de tirer des apprentissages de ces échecs. Cet environnement les encourage à demander, en cas de doute ou de problème, et à partager leurs expériences, pour limiter le risque de reproduction des erreurs.

4 Audit de sécurité

Afin d'évaluer l'efficacité de certaines mesures et la situation générale de l'infrastructure informatique de l'administration, il a été fait appel à une société externe spécialisée dans la sécurité informatique. Mandat lui a été donné pour effectuer un audit de sécurité de notre infrastructure.

L'audit s'est déroulé en deux parties :

- Un test d'intrusion externe
- Une tentative de compromission de l'infrastructure depuis le réseau interne

Le test d'intrusion depuis l'extérieur a permis de confirmer que les mesures de limitation des accès distants mises en place permettent de bloquer les tentatives d'intrusion, et que la sécurité de notre infrastructure est adéquate.

La situation interne est satisfaisante. À la suite de cet audit, plusieurs modifications ont été entreprises pour augmenter le niveau de sécurité et limiter les risques de compromission de l'infrastructure. Un contrôle supplémentaire, effectué après ces modifications, a montré que les correctifs adaptés ont été appliqués correctement.

5 Poursuite des efforts

La Municipalité est consciente que d'autres efforts doivent encore être consentis, notamment au niveau des réseaux informatiques, qui sont actuellement parfois disparates et qui devraient être mutualisés et uniformisés au niveau communal. La formation continue des collaborateurs au niveau de la sécurité des données et la vigilance par rapport aux risques liés à l'utilisation d'internet et aux tentatives d'intrusion et/ou de vol de données doivent également continuer à retenir toute l'attention des services communaux dans la période actuelle compliquée.

5.1 Risques résiduels

Si la Municipalité prend la question au sérieux, son influence est souvent réduite dans le cadre, par exemple, d'associations intercommunales. En effet, ces dernières sont parfois appelées à gérer des

données sensibles (au sens de la loi fédérale sur la protection des données (LPD) et de la loi cantonale vaudoise sur la protection des données personnelles (LPrD)) telles que des données fiscales et de santé. Or, leur état de préparation n'est pas toujours connu et dans ce sens, le risque n'est pas toujours maîtrisé.

De même, si les correctifs nécessaires sont appliqués régulièrement, la Municipalité est tributaire de la qualité du travail de ses fournisseurs. Si un éditeur de logiciel occulte certains dangers et n'y apporte pas de solution sans en avertir ses clients, la situation est également problématique. C'est pourquoi le sérieux des fournisseurs est régulièrement vérifié. Si nécessaire, des audits de sécurité sont demandés.

6 Conclusion

Au vu de ce qui précède, la Municipalité demande au Conseil communal de bien vouloir prendre la décision suivante:

LE CONSEIL COMMUNAL DU MONT-SUR-LAUSANNE

- Vu le rapport de la Municipalité du 21 février 2023 ;
- Ouï le rapport de la Commission ad hoc désignée pour examiner cette affaire ;
- Considérant que cet objet a été porté à l'ordre du jour ;

décide

de prendre acte du rapport de la Municipalité et de classer le postulat « *Données communales et piratage informatique* »


La syndique
Laurence Muller Achteri

Au nom de la Municipalité




Le secrétaire
Sébastien Varrin