

Rapport de la commission ad hoc chargée d'étudier le préavis municipal N° 1/2023 – Réponse au postulat de MM. François Costa et Yvan Krähenbühl « Un label pour donner confiance à la population »

Au Conseil Communal de La Tour-de-Peilz,

Monsieur le Président,

Mesdames et Messieurs les membres du Conseil,

La commission chargée d'examiner l'objet cité en titre s'est réunie le jeudi 9 février 2023 à 20h00, en Salle 2 de la Maison de Commune. Elle était composée de:

Lyonel Kaufmann (PSDG), président, présent

Michel Chappuis (PLR), présent

Yvan Krähenbühl (PLR), présent

Diego Pasquali (LV), présent

Maëlle Le Boudec (LV), présente

Margareta Brüssow (LCIVL), présente

Héraclès Dellas (UDC), présent

La municipalité était représentée par :

Monsieur Jean-Pierre Schwab, Municipal

Monsieur Michael Zenger, Chef de service des Finances & Informatique et office de la population

Après les salutations d'usage du président de la commission, la parole est donnée à M. Schwab.

Présentation du projet

Après avoir succinctement rappelé le contexte du dépôt du postulat avec les différentes cyberattaques ayant touché notamment les communes de Rolle et Montreux ainsi que de Sécurité Riviera, Jean-Pierre Schwab cède la parole à Michael Zenger.

Michael Zenger souligne la matière relativement sommaire du préavis qui propose de passer par le label CyberSafe (<http://www.cyber-safe.ch>) auquel il apporte quelques compléments et précisions.

Concernant la cybersécurité de l'administration communale ainsi que des entités externes bénéficiant des prestations de notre service informatique tel la Fondation des structures d'accueil de La Tour-de-Peilz (FSAT), le Musée suisse du jeu, le Centre de loisirs pour seniors L'Escale et l'Agence d'assurances sociales (AAS), les mesures entreprises se sont accélérées avec l'introduction du télétravail (2020) et avaient conduit en 2021 à l'engagement d'un informaticien système. Ce dernier a entamé en 2022 une formation de "Cyber Security Specialist" qui sera sanctionnée par un brevet fédéral en octobre 2023 en cas de réussite.

Porté au budget 2023, le troisième poste de technicien informatique vient lui d'être mis au concours ce jour même de la séance de commission. Concernant les questions de cybersécurité, son rôle consistera à

assurer le lien avec les utilisateurs des services informatiques communaux (introduction, formation et helpdesk) ainsi que le support technique de 1er niveau des systèmes.

Avec cet engagement supplémentaire, l'unité informatique de la commune, internalisée à partir de 2018, reposera ainsi sur trois personnes. S'il a fallu au moment de l'internalisation et en premier lieu s'occuper du renouvellement des infrastructures informatiques remontant en partie à 1998, l'engagement de cette 3^e personne permettra véritablement la mise en place à terme d'une cyberadministration.

On assiste donc à une montée en puissance progressive des services informatiques communaux qui relativement aux questions de cybersécurité, domaine actuellement en ébullition. Les trois postes peuvent être mis en relation avec les 400 collaborateur·trices informatiques (internes) de l'État de Vaud et les 80 collaborateur·trices informatiques (internes) à la commune de Lausanne. Yverdon, Pully et Morges sont les principales entités communales disposant ensuite de services informatiques actives au sein de l'Association vaudoise des responsables informatiques des Communes (AVRIC) en échangeant sur de nombreux projets.

Concernant le label choisi, celui-ci propose un scan de la sécurité de nos infrastructures et de notre réseau et nullement une démarche de certification iso que certains labels plus poussés proposent mais qui représentent un investissement démesuré pour une commune de la taille de La Tour-de-Peilz.

Historique des démarches entreprises depuis 2021 jusqu'à aujourd'hui

- novembre-décembre 2021 : sensibilisation auprès des collaborateurs (160 machines utilisées au niveau communal), par un intervenant externe ;
- janvier 2022 : sensibilisation avancée auprès de répondant·es informatiques (via SecuLabs société dépendant de l'EPFL) avec notamment une démonstration live d'un hacking
- février 2022 : opération d'hameçonnage après la formation
- depuis : pas de nouvelle sensibilisation auprès des utilisateur·trices

Les étapes suivantes pourront intervenir avec/après l'engagement du troisième collaborateur·trice.

Concernant la certification retenue, celle-ci nous permettra de nous situer plus précisément en matière de sécurité et ceci de manière régulière.

Réponses aux questions des commissaires

Actuellement une personne se forme. Que se passe-t-il si la personne part dans deux ans après sa formation au terme de la convention de formation ?

La formation sera largement rentabilisée. Les coûts de la formation (chf 15'300.- desquels seront déduites les subventions de la Confédération de 50% et de Fonpro de 25%, soit un solde d'environ chf 3'825.- à charge de la Commune) peuvent être comparé avec les honoraires d'un spécialiste senior en matière de cybersécurité s'élevant entre chf 300.- à 500.- l'heure.

La sensibilisation des utilisateur·trices est prévue à quels intervalles ?

Ce sera le rôle de la troisième personne qui va être engagé d'organiser notamment des ateliers auprès des utilisateurs et d'avoir un contact régulier avec eux. Cette personne aura la charge d'assurer une sensibilisation régulière.

Elle s'occupera également de la mise en œuvre des recommandations faite suite au scan effectué par CyberSafe.

La commune se donne les moyens pour se protéger efficacement déjà maintenant et elle prévoit d'agir pour le futur au niveau de la formation du personnel. A quoi sert alors de plus cette certification. Est-ce juste se rassurer qu'on fait bien avec un effet psychologique. La commune ne peut-elle pas simplement avoir confiance en elle ?

Il faudra voir le résultat de l'audit. En premier lieu, cela nous donne un deuxième avis relativement à la sécurité informatique de notre réseau communal.

Après le scan, la démarche CyberSafe proposera la mise en place de mesures complémentaires. La démarche pourrait être renouvelée ensuite tous les deux ans (nouveaux tests et suivi des mesures prises).

Le niveau d'expertise des gens du label challengera le spécialiste interne qui s'occupe par ailleurs d'autres prestations informatiques ou projet informatique pour la commune.

Le label est également et évidemment un moyen de rassurer la population.

Qu'en est-il du dispositif des sauvegardes internes/externes de la commune ?

La commune dispose d'un premier système de sauvegarde en local et d'un deuxième dans le cloud sur Lausanne.

Dans le cadre du raccordement via la fibre optique, il est prévu à terme un nouveau système de backup à Béranges 111. Nous disposerons ainsi de trois systèmes de backup.

Cependant, pour pouvoir remonter très rapidement en production suite à une éventuelle cyberattaque, il est aussi nécessaire de doubler les serveurs informatiques (CHF 100'000.- à 150'000.- pour une telle infrastructure). La construction d'un deuxième data center à terme est planifiée sous le collège Courbet.

Si le label ne devait pas se mettre en place, est-ce que cela vous inquiéterait ?

Oui. On repartirait avec SecuLabs.

Avez-vous un exemple de commune ayant recouru à ce label et du coût qui paraît peu élevé relativement à notre commune ?

Pas d'exemple concret en tête du côté de la commune.

Après vérification, le site internet du label cyber-safe.ch ne liste pas de Communes de référence. A notre connaissance, les Communes de Payerne et Ollon ont opté pour ce label.

Aller plus loin que ce processus de labélisation, qu'est-ce cela signifierait ?

Le label ne va pas beaucoup plus loin. Ce serait alors d'autres démarches avec d'autres prestataires. Mais c'est trop tôt.

Discussion entre les commissaires :

Il est rappelé que le postulat fait suite aux impacts à la commune de Rolle, Montreux et à Sécurité Riviera de cyberattaques.

Tous les commissaires sauf un-e exprime un avis favorable à très favorable relativement à la mise en place de la démarche cybersécurité communale et du label CyberSafe. Les éléments suivants sont mis en avant :

- le label oblige la commune de se mettre à jour et en question tous les deux ans ;
- l'internalisation du service informatique avec des gens à proximité est un plus pour traiter et intervenir sur les éventuels problèmes rencontrés ;

- le label permet de rassurer les citoyens sur les process ;
- le regard externe et l'ouverture sont bienvenues en la matière ainsi que le recours d'un organisme tiers ;
- les explications par M. Zenger données étaient pertinentes et indiquaient le niveau de maîtrise communal relativement au sujet ;
- la démarche permet de pousser les services informatiques communaux dans leurs derniers retranchements ;
- les tests techniques et l'approche psychologiques vont de pair et ont leur nécessité ;
- les tests techniques et le côté psychologique sont deux éléments complémentaire et nécessaire ;
- c'est aussi une plus-value qu'offre la commune pour les organismes externes (Fondation des structures d'accueil de La Tour-de-Peilz, le Musée suisse du jeu, le Centre de loisirs pour seniors L'Escale et l'Agence d'assurances sociales) qui bénéficieront aussi de la démarche et du label.

Un-e commissaire émet un avis négatif relativement à la démarche de labélisation. La personne émet la crainte que cela ne soit qu'un effet psychologique. Elle doute donc de la nécessité de la démarche même si le préavis répond au postulat déposé.

Avant de passer au vote, la parole est donnée à Yvan Krähenbühl, un des deux postulants. Celui-ci s'estime satisfait par la réponse de la municipalité à son postulat. La démarche répond aux recommandations tant du canton que de la Confédération. Pour 10'000.-, c'est aussi une bonne assurance devant les conséquences financières potentielles d'une cyberattaque et compte tenu du prix exorbitant aujourd'hui d'une telle assurance pour une collectivité publique telle que la nôtre. Le label est aussi un bon investissement ou une bonne mesure de précaution à l'égard de particuliers ou d'entités recourant à la justice.

Décision

Lors du vote, le préavis est approuvé à l'unanimité.

Conclusions

En conclusion, nous vous demandons, Monsieur le Président, Mesdames et Messieurs les Conseillères et Conseillers, de bien vouloir voter les conclusions suivantes :

Le Conseil communal de La Tour-de-Peilz,

- vu le préavis municipal N° 1/2023,
- ouï le rapport de la Commission chargée d'examiner ce dossier,
- considérant que cet objet a été porté à l'ordre du jour,

décide :

de considérer que ce préavis répond au postulat de MM. François Costa et Yvan Krähenbühl (PLR) « Un label pour donner confiance à la population ».

Pour la commission, le Président-rapporteur

Lyonel Kaufmann

La Tour-de-Peilz, le 20 février 2023

PRÉAVIS MUNICIPAL N° 1/2023

le 8 février 2023

Réponse au postulat de MM. François Costa et Yvan Krähenbühl (PLR) « Un label pour donner confiance à la population »

10.03.02-2301-Preavis-01-Postulat-label-cybersecurite.docx

Au Conseil communal de
1814 La Tour-de-Peilz

Monsieur le Président,
Mesdames et Messieurs,

1. Objet du préavis

Lors de la séance du Conseil communal du 9 février 2022, MM. François Costa et Yvan Krähenbühl (PLR) ont déposé le postulat « Un label pour donner confiance à la population », qui a été renvoyé directement à la Municipalité.

Suite à des cyberattaques subies par différentes communes vaudoises, les postulants proposent à la Municipalité d'entreprendre les démarches nécessaires pour l'obtention du label de cybersécurité www.cyber-safe.ch, afin de certifier la sécurité des systèmes d'information communaux et de montrer à la population que la cybersécurité est prise très au sérieux.

A propos du label cyber-safe.ch

Ce label a été développé par l'Association suisse pour le label de cybersécurité (ASLaC), fondée en 2018, avec pour objectif de favoriser une gestion responsable de la cybersécurité dans les petites et moyennes organisations en Suisse.

Le label est censé permettre aux PME et communes d'atteindre un niveau de sécurité informatique défini comme acceptable par un ensemble de partenaires publics et privés, en implémentant des mesures préventives à plus forte valeur ajoutée pour sécuriser leurs activités.

Reposant sur une méthode d'évaluation alliant outil en ligne, questionnaires, tests d'hameçonnage et interventions humaines, le label offre un outil d'aide à la décision et de connaissance fine des cyber-risques en matière d'infrastructure, d'organisation et de compétences humaines.

L'Union des communes vaudoises (UCV) a participé, en 2020, à un groupe de travail afin d'aider l'ASLaC à affiner les critères du label, dans le but d'y intégrer les besoins des communes.

Le processus de labellisation s'effectue en trois étapes :

1. Diagnostic et feuille de route

Il s'agit de faire un état des lieux grâce à des diagnostics techniques, des collaborateurs, de la gouvernance puis de définir des actions prioritaires et des mesures correctives.

2. Audit de cybersécurité

Un audit exécuté dans les locaux de la Commune vise à vérifier que les failles et les vulnérabilités mises en évidence lors du diagnostic ont été adressées et corrigées puis de contrôler l'implémentation effective des exigences cyber-safe.ch dans l'organisation.

3. Labellisation

Dans le cas d'un taux de réussite de plus de 80% de l'audit de cybersécurité, le label est octroyé, avec une validité de 2 ans.

La stratégie de transformation numérique de la Municipalité

Pour mémoire, dans le cadre de la nouvelle stratégie informatique élaborée en 2017 et face aux nombreux projets dans les années à venir, la Municipalité s'est donné les moyens afin de disposer à terme d'une équipe interne de spécialistes informatiques dédiés, pour assurer non seulement la gestion et le développement de son système d'information mais également sa protection, la sécurité représentant désormais un travail quotidien et dont la complexité augmente en permanence.

Elle a ainsi mis sur pied l'Unité informatique au sein du Service des finances en 2018, en mettant au budget un poste d'administrateur des systèmes informatiques et en engageant l'ingénieur qui maintenait les systèmes informatiques communaux depuis plus de 15 ans pour le compte d'une société de services.

En mars 2020, la Municipalité a été la première Commune vaudoise à visiter le nouveau centre de surveillance informatique (Security Operation Center) du canton de Vaud à Renens et à prendre part à une sensibilisation contre les cyber-risques.

Lors de l'élaboration du budget 2021, la Municipalité a défini sa stratégie de transformation numérique pour les prochaines années, basée sur les trois axes suivants :

- Accélération de la numérisation des processus
- Augmentation de la sécurité des systèmes informatiques
- Formation continue des utilisateurs

Afin de pouvoir mettre en œuvre cette stratégie tout en poursuivant l'effort d'internalisation des compétences informatiques pour optimiser l'indépendance, la réactivité et la maîtrise des coûts, l'Unité informatique a été renforcée en 2021 par l'engagement d'un informaticien systèmes avec CFC et brevet fédéral de spécialiste systèmes et réseaux TIC, portant pour l'instant l'effectif à 2 EPT.

Cet informaticien systèmes a entamé en 2022 une formation de "*Cyber Security Specialist*" qui sera sanctionnée par un brevet fédéral en octobre 2023 en cas de réussite. Il accompagnera ce processus de certification tout en mettant également en application ses nouvelles connaissances en cours d'acquisition.

Finalement, dans le cadre du budget 2023, un poste de technicien informatique a été créé, permettant de décharger l'administrateur et l'informaticien systèmes, soumis à une charge de travail conséquente, en lui confiant les tâches en lien avec les utilisateurs (introduction, formation et helpdesk) ainsi que le support technique de 1^{er} niveau des systèmes.

L'Unité informatique a déjà mis en place un certain nombre de mesures humaines et techniques afin d'élever et de maintenir au mieux le niveau de protection de ses systèmes, dans la mesure des connaissances et des ressources à disposition, ces efforts étant poursuivis en permanence.

A ce jour, ce secteur gère les systèmes informatiques de la Commune, comprenant les réseaux informatiques (réseaux administratifs internes et externes à la Maison de commune, réseau wifi public), la téléphonie IP, l'infrastructure (serveurs, postes de travail, imprimantes, périphériques, etc) et les logiciels métiers.

Postulat de François Costa et Yvan Kraehenbuehl

Un label pour donner confiance à la population

Nul besoin de vous rappeler que les communes vaudoises sont devenues des cibles faciles et intéressantes pour les hackers. Les systèmes d'information communaux doivent se mettre à jour pour faire face à cette menace. Bien que le risque zéro n'existe pas, il peut être réduit fortement si des mesures adéquates sur le plan humain et technique sont prises. Etant donné que la sécurisation du parc informatique est une question communale, nous pensons que la municipalité devrait faire les démarches nécessaires dans le but d'obtenir le label de cybersécurité proposé par le site www.cyber-safe.ch. L'obtention d'un label permet de montrer à la population que la municipalité prend la question de la cybersécurité très au sérieux. Ce label comporte selon nous 3 avantages.

1. Le label certifie la sécurité des systèmes d'information communaux
2. Une bonne sécurisation des systèmes communaux limite les dégâts en cas d'attaques.
3. Le label permet de montrer à la population que la municipalité de La Tour-de-Peilz prend au sérieux la question des attaques informatiques.

Le processus est en deux étapes :

1. Diagnostic et feuille de route
 - a. Identification des failles techniques
 - b. Test de vigilance (pishing)
 - c. Aide au pilotage
 - d. Plan de réduction de vulnérabilité
2. Audit de cybersécurité
 - a. Examen final de conformité
 - b. Audit sur site par un auditeur indépendant
 - c. Certification d'absence de vulnérabilités critiques et implémentation des exigences du label

Ce label est soutenu par la Confédération ainsi que l'union des communes Vaudoises (UCV) qui recommande l'obtention de ce label :

“Partenaire de [cyber-safe.ch](http://www.cyber-safe.ch), l'UCV a participé, en 2020, à un groupe de travail afin d'aider l'ASLaC (Association suisse pour le label de cybersécurité), à l'origine de ce label, à affiner les critères du label de cybersécurité qu'elle propose, dans le but d'y intégrer les besoins des communes. C'est donc tout naturellement que l'UCV a fait appel, en 2021, à l'ASLaC afin de s'assurer que ses données,

réseaux et accès sont protégés et sécurisés de façon appropriée. Cette association identifie les vulnérabilités des PME et collectivités publiques et les aide à se protéger des cyber-attaques en leur fournissant des conseils pour la mise en place de solutions adéquates. L'UCV est heureuse d'avoir ainsi pu optimiser sa sécurité informatique et remplir les exigences du label. Notre association encourage fortement les communes à suivre son exemple”*

Nous souhaitons que ce postulat soit directement transmis à la municipalité.

François Costa

Yvan Kraehenbuehl

Sources :

- www.cyber-safe.ch
- www.ucv.ch/thematiques/securite/cybersecurite/detail-cybersecurite/lucv-premiere-association-a-obtenir-le-label-de-cybersecurite-cyber-safech