



COMMUNE D'AIGLE

LA MUNICIPALITÉ

Au Conseil communal d'Aigle

PRÉAVIS MUNICIPAL N° 2023-16 du lundi 11 décembre 2023

relatif à

**A LA REPONSE AU POSTULAT DE
M. NICOLAS BIFFIGER (PLR), DEPOSE LE 12 OCTOBRE 2021 ET
INTITULE « CYBERSECURITE »**

Monsieur le Président,
Mesdames, Messieurs les Conseillers,

1. PREAMBULE

La Municipalité partage les préoccupations du postulant. Soucieuse de protéger les données du vol ou de leur perte et comprenant l'importance de la sécurité de ces données pour la ville d'Aigle et ses habitants, la Municipalité a mis en place différentes mesures afin de renforcer la sécurité, déjà en fonction depuis de nombreuses années.

2. HISTORIQUE

Le 30 mai 2021, l'administration communale de Rolle a été victime d'une cyberattaque. L'intrusion a été détectée dans le système informatique et des données ont été cryptées par les cybercriminels. Mais celles-ci ont pu être rapidement restaurées. Une plainte pénale a été déposée.

Le 10 octobre 2021, la commune de Montreux a, à son tour, subi une attaque du même type.

3. CONTEXTE ACTUEL

La montée du danger de cyberattaques a bien entendu provoqué un fort émoi dans le public et les administrations cantonales et communales vaudoises notamment.

En plus des réactions individuelles des communes, leurs deux faîtières se sont saisies du dossier. De son côté, le Canton a mis en place une page web contenant diverses informations utiles : https://www.vd.ch/static/vd_secure/#/a-propos

Par ailleurs, l'Etat de Vaud et les faîtières ont entrepris des négociations, lesquelles ont abouti à la signature d'une convention en juillet 2023. Cette convention entrera en vigueur le 1^{er} janvier 2024 (voir point 8 de la présente réponse).

4. INFORMATION ET FORMATION DES COLLABORATEURS

Les erreurs humaines constituent une des premières causes des cyberattaques (par exemple, ouverture imprudente d'un courriel ou d'un fichier suspect et usage d'un mot de passe trop facile à pirater). Un effort particulier a donc été accompli en la matière. Dans ce cadre, les mesures suivantes ont été prises :

- Etablissement d'une politique de sécurité du système d'information (PSSI), signée par la Municipalité et communiquée à tous les collaborateurs. C'est la pierre angulaire de la sécurité informatique, ce document exprimant clairement la volonté de la Municipalité de protéger ces données et de l'orientation que cette sécurité doit respecter ;

- Mise à jour de la charte informatique, notamment pour inclure les nouvelles menaces et les bonnes pratiques actuelles. La nouvelle charte informatique a été signée par l'ensemble du personnel ayant accès à l'informatique de l'administration communale d'Aigle ;
- Etablissement d'une convention de télétravail depuis la Covid, afin que les règles du travail à distance soient clairement énoncées et préparation du matériel pour ce télétravail, aucun poste privé ne devant être utilisé. Mise en place générale du VPN avec authentification à facteur multiple et nominatif pour tous les accès distants sur le réseau communal ;
- Informations régulières par courriels aux collaborateurs des menaces à la mode, des bonnes pratiques, des informations sur l'évolution du monde cyber, etc. Le bon niveau de formation des utilisateurs de l'informatique diminue largement le risque.

5. MESURES TECHNIQUES

Un autre volet important en matière de cybersécurité est purement technique. Il s'agit par exemple de mettre en place des antivirus et pare-feux solides et d'assurer la sauvegarde des données enregistrées dans l'hypothèse où un serveur serait piraté ou détruit. Dans ce cadre, la Municipalité a pris les mesures suivantes :

- Mise en place d'un outil de management du parc informatique afin de centraliser les alertes de chaque poste et serveurs. De plus, cet outil comprend une solution antivirus efficace déployée sur l'ensemble des postes et serveurs. Ces alertes sont contrôlées par le service informatique afin de prendre les mesures qui s'imposent.
- Renforcement des sauvegardes, au niveau des données et des serveurs d'applications. Les sauvegardes étaient depuis plus de 10 ans faites sur trois supports, un de ces supports comprend désormais un datacenter en Suisse, hors territoire aiglon.
- Renforcement de la messagerie avec la mise en place d'une authentification multi facteur pour chaque compte.
- Mise à jour du parc informatique permanent avec le remplacement des systèmes d'exploitation obsolètes (plus maintenus par leur éditeur).
- Redondance des serveurs internes, dans deux bâtiments différents.
- Mise à jour régulière des informations sur les données que traite la commune, de leur emplacement et des droits d'accès à ces données.

6. CONTRÔLE ET AUDIT EXTERNES

En matière informatique, il est difficile, voire impossible, d'effectuer des contrôles totalement neutres et de détecter les éventuelles faiblesses du système avec les seuls moyens internes. S'ajoute à cela que ces contrôles peuvent nécessiter des moyens importants et très pointus au niveau technique.

Dès lors, un contrôle quotidien des sauvegardes est fait en interne. De plus les enregistrements des sauvegardes sont aussi contrôlés par un partenaire externe, puisque le service informatique se compose d'un 0.9 EPT et que les alertes sur les sauvegardes

doivent être traitées dans les plus brefs délais. Le service informatique ne peut assurer seul cette tâche, surtout pendant les vacances.

Par ailleurs, une demande de labélisation « CyberSafe » est en cours avec un auditeur indépendant, qui a déjà procédé à plusieurs reprises à l'analyse complète du parc informatique, à sa documentation et qui a réalisé un test de phishing (campagne de mail frauduleux) et de pénétration du système.

En substance, cette labélisation comprend trois points principaux :

- test des systèmes informatiques, des collaborateurs et de notre gouvernance afin d'identifier les failles et vulnérabilités pour dresser un état des lieux de notre cybersécurité ;
- mise en place d'une feuille de route pour la conduite opérationnelle (gestion des priorités selon les risques, les impacts financiers et le secteur d'activité). Sur la base de l'état des lieux, une liste d'actions prioritaires pour améliorer notre cybersécurité a été établie ;
- audit des communes candidates et vérification que les mesures correctives suggérées ont été appliquées. Il s'agit donc de contrôler la conformité de la cybersécurité des candidats aux exigences du Label avant de le délivrer.

7. GESTION DE CRISES

La survenance d'une crise implique forcément un niveau de stress important. Il est par ailleurs difficile d'agir de manière totalement efficace dans l'urgence.

Dès lors, un plan de reprise d'activités a été établi afin qu'une crise soit gérée de façon optimale en suivant des instructions réfléchies, et non pas dans l'urgence de la crise.

De plus, une analyse de risques comprenant tout ce qui peut toucher aux données, de la catastrophe naturelle au vol par un collaborateur, a été effectuée. De ce document découle les actions que la Municipalité a ordonnées afin d'établir une protection efficace.

8. NOUVELLES MESURES DEPUIS LE 1 JANVIER 2024

Le 1^{er} janvier 2024, la convention de cybersécurité Canton-Communes entrera en vigueur pour tout le canton de Vaud. Cette convention permet la mise en place d'un groupe d'experts externes aux communes, qui servira, en cas de cyberattaque, à piloter efficacement la cellule de crise, à apporter des connaissances pointues pour aider les communes et à rétablir leur infrastructure rapidement, ainsi que d'apporter de l'aide quant à la gestion du vol de données.

Cette convention se base sur les propositions d'un groupe de travail Canton-Communes et prône la volonté de s'appuyer sur les forces en présence. L'équipe d'intervention sera ainsi composée d'experts en cybersécurité du Centre opérationnel de sécurité (SOC) de la Direction générale du numérique et des systèmes d'information (DGNSI), à laquelle pourront se joindre, selon les situations de crise, des experts de la cybercriminalité de la Police cantonale vaudoise (PolCant) ainsi que des spécialistes de la gestion de crise de l'Etat-major cantonal de conduite (EMCC). Elle s'appuiera également sur une coopération avec des prestataires privés locaux en vue de renforcer la réponse technique d'urgence en cas de cyberattaque sur une entité communale.

Cette convention a été signée par le Canton et les deux associations faîtières de communes le 4 juillet 2023.

9. CONCLUSIONS

En conclusion, nous avons l'honneur, Monsieur le Président, Mesdames et Messieurs les Conseillers, de vous demander de bien vouloir prendre les décisions suivantes :

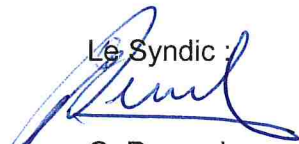
LE CONSEIL COMMUNAL D'AIGLE

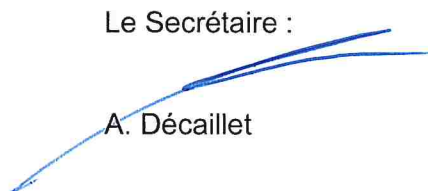
- Vu le préavis n° 2023-16 du 11 décembre 2023
- Ouï le rapport de la Commission chargée de l'étude de cet objet
- Considérant que ledit objet a été porté à l'ordre du jour

DÉCIDE

1. De prendre acte de la réponse au postulat de M. Nicolas Biffiger : « Cybersécurité »
2. De prendre acte du train de mesures pris par la Municipalité dans le domaine de la cybersécurité.

AU NOM DE LA MUNICIPALITÉ

Le Syndic :

G. Devaud

Le Secrétaire :

A. Décaillet

Municipal délégué : Grégory Devaud

Annexes :

- Politique de sécurité du système d'information (PSSI)
- Charte informatique de la commune
- Convention de télétravail
- Plan de reprise d'activité