**COMMUNICATION DE LA MUNICIPALITE AU CONSEIL COMMUNAL**

**C 19/2021**

Vevey, le 27 septembre 2021

# Ce document doit au préalable être traité en séance du Conseil communal du jeudi 07 octobre 2021

**Réponse à l'interpellation de Mme Fabienne Despot UDC « Cyber - emmentaler ! »**

Madame la Présidente, Mesdames, Messieurs,

Concernant les questions de Mme Fabienne Despot, les réponses de la Municipalité sont les suivantes :

1. Notre commune se rend-elle compte qu'elle est dans le viseur de hackers ?

   **Réponse** :
   *Oui, comme la totalité des autres communes, états, entités parapubliques ou sociétés privées. En effet, il n'y a pas que les villes qui sont des cibles, tout ce qui est connecté à Internet est scanné en permanence par les hackers à la recherche de vulnérabilités. Les hackers peuvent soit cibler spécifiquement une entreprise ou une commune, soit aller à la pêche aux vulnérabilités non corrigées.*
   *Le service des systèmes d'information est conscient de ces menaces et a initié l'année passée une vérification de tous les aspects liés à la cybersécurité avec une société externe. Un budget a été voté et les opérations sont en cours depuis ce printemps, avec également en parallèle des cours de sensibilisation/formation en ligne aux cybermenaces pour les collaborateur·rices, qui sont un des maillons essentiels de la sécurité informatique.*

2. La DSI dispose-t-elle d'un système de détection d'intrusion ? Si oui,utilise-t-elle les alertes à son avantage ? Si non, pourquoi n'est-ce pas le cas ?

   **Réponse** :
   *Oui le service des systèmes d'information utilise un Firewall récent et à jour qui détecte et bloque les intrusions (IPS). Cela est complété par des antivirus sur tous les ordinateurs (PC et serveurs).*

3. Peut-on dire que la commune de Rolle avait une sécurité de moindre qualité que Vevey et que d'autres cités vaudoises, ce qui expliquerait qu'elle ait été touchée avant d'autres ? En tel cas, pourquoi considérez-vous que Vevey serait mieux protégée ? Comment situez-vous notre ville en termes de sécurité informatique vis-à-vis des autres communes du Canton et de Suisse ?

**Réponse** :
*Le service des systèmes d'information ne peut se prononcer sur le cas de Rolle faute de connaître ni son infrastructure informatique, ni les mesures adoptées, ni le niveau de sensibilisation de ses utilisateur·rices aux cybermenaces.*
*Ne connaissant pas en détail la sécurité qui était en place à Rolle, nous nous concentrons sur notre commune. Dans notre cas et suite à un audit réalisé par une société externe en juin (donc avant que l'événement de Rolle ne soit connu), aucune vulnérabilité critique n'a été remontée. Des améliorations ont été demandées et sont en cours de réalisation depuis le mois de juillet. Concernant la comparaison avec les autres communes du Canton et de Suisse, comme il n'y a pas d'informations publiques sur les diverses infrastructures mises en place, nous ne pouvons pas nous prononcer.*

4. La DSI est-elle à jour avec tous les correctifs de sécurité pour tous les logiciels qu'elle exploite, et tout particulièrement en ce qui concerne le même point d'entrée que celui exploité à Rolle ? Si non, pourquoi ne l'avoir pas fait et quand compte-t-elle le faire ?

   **Réponse** :
   *Oui les mises à jour sont régulièrement faites grâce à nos équipes internes ainsi qu'aux diverses sociétés externes qui nous ont vendu ces matériels ou logiciels et qui nous informent parfois avant les publications officielles. Le point d'entrée apparemment utilisé à Rolle et mentionné dans l'interpellation a été traité.*

5. Si la Ville devait subir le même sort que Rolle, quelles pourraient être les données sensibles atteignables par les pirates et donc potentiellement mises en circulation ?

   **Réponse** :
   *Dans le cas ou des hackers parviendraient, malgré les outils et mesures en place, à accéder aux données sur les différents serveurs de la Ville, on ne pourrait pas exclure qu'ils accèdent également aux données du contrôle des habitant·es où figurent des données sensibles des habitant·es. Par contre notre Commune surveille activement l'utilisation des lignes Internet et le fait d'exfiltrer un grand volume de données dans un temps limité génère des alarmes, que ce soit du trafic normal (voulu par la Commune) ou non.*

6. La DSI peut-elle financièrement quantifier un préjudice possible dont elle pourrait faire la cible ? Si oui, investit-elle suffisamment d'énergie pour le contrer ?

   **Réponse** :
   *Il est très dur de mettre une valeur sur les données détenues par la Ville, d'autant plus qu'il est également très compliqué de savoir ce qui pourrait avoir été collecté avant que les alarmes ne se déclenchent. Dans le cas de Rolle, le résultat de la fuite des données est plus un important dégât d'image qu'un dégât financier pour la commune.*
   *Entre les mises à jour des postes et des serveurs à effectuer, la gestion des règles du pare-feu, les systèmes de filtrage des emails et de blocage des sites internet, la sensibilisation des utilisateurs, une importante énergie est dépensée par le service des systèmes d'information pour assurer la sécurité. Il serait difficile d'aller au-delà sans avoir à renforcer l'équipe.*

7. La Ville est-elle en contact préventif avec les autorités compétentes comme fedpol, Interpol et le Centre national pour la cybersécurité ? La DSI se concerte-t-elle avec les départements IT d'autres communes et avec la DSI cantonale ?

**Réponse** :
*Au niveau cantonal, le Security Operation Center (SOC) n'est pas à disposition des communes et encore moins de manière préventive. Il ne peut être engagé qu'à la demande de la permanence Cybercriminalité de la police cantonale après que celle-ci ait été contactée par une commune suite à une attaque informatique.*
*Les autorités fédérales sont surchargées de même et ne répondent qu'en cas d'incident avéré. Il s'agit là plus d'un service d'enregistrement des incidents et attaques, permettant de réaliser un baromètre des tendances et d'établir des recommandations concernant les menaces en cours les plus fréquentes. Par contre la DSI est bien évidemment en contact avec certains services du Canton, comme celui gérant le réseau cantonal ainsi que diverses entreprises spécialisées.*

Ainsi adopté en séance de Municipalité, le 27 septembre 2021

Au nom de la Municipalité

| le Syndic | le Secrétaire |
| --- | --- |
| Yvan Luccarini | Grégoire Halter |

Annexe : Interpellation Mme Fabienne Despot UDC « Cyber - emmentaler ! »

# Cyber-emmentaler

Le 20 août dernier, la presse[1] nous révélait que la commune de Rolle avait été victime d'une cyberattaque un plus tôt dans l'année, et ce dans l'ignorance totale d'une grande partie de son administration. Signée au nom du groupe «*Vice Society*», cette cyberattaque a divulgué de nombreux documents internes ainsi que des données personnelles relatives aux habitants de la ville.

Notre groupe UDC, par la voix de notre conseiller communal Moïn Danai, nous disait dans son interpellation du 18 juin 2020 que « les menaces sont réelles, à bout portant, et frappent sans préavis ». Il demandait également un état des lieux sur la sécurité de l'infrastructure IT de la Ville. Dans la réponse de la Municipalité[2], on apprenait que « la priorité de ces dernières années […] a été […] d'effectuer la remise à niveau des équipements et logiciels ». La Municipalité d'alors semblait oublier que la sécurité est un processus continu, pas du tout intermittent.

Il avait été également fait mention de « formations des collaborateurs de la Ville quant à la sécurité informatique et les cybermenaces à l'aide d'un prestataire spécialisé ». Cela faisait fortement penser, qu'on le veuille ou non, à une politique de l'autruche.

Il est bon de se rappeler la sévère abstention de notre Conseil lors du vote concernant le postulat sur le renouvellement de l'infrastructure IT de la Ville[3], une abstention massive due en partie à la cécité de la DSI face aux problématiques sécuritaires. Il ne paraît pas totalement insensé de supputer un certain amateurisme qui gangrène notre administration en matière d'informatique. Une gangrène qui pourrait suffisamment la crisper pour la conduire à un nouveau scandale à l'image de celui de Rolle[4].

Avec inquiétude, nous posons les questions suivantes à la Municipalité :

1. Notre commune se rend-elle compte qu'elle est dans le viseur de hackers ?
2. La DSI dispose-t-elle d'un système de détection d'intrusion ? Si oui, utilise-t-elle les alertes à son avantage ? Si non, pourquoi n'est-ce pas le cas ?
3. Peut-on dire que la commune de Rolle avait une sécurité de moindre qualité que Vevey et que d'autres cités vaudoises, ce qui expliquerait qu'elle ait été touchée avant d'autres ? En tel cas, pourquoi considérez-vous que Vevey serait mieux protégée ? Comment situez-vous

[1] https://www.watson.ch/fr/suisse/vaud/323755680-vaud-rolle-a-ete-piratee-par-des-hackers-donnees-volees-sur-le-darknet [accédé le 07.09.2021]
[2] C13/2020
[3] P35/2019
[4] https://www.rts.ch/info/regions/vaud/12456135-les-pirates-informatiques-de-rolle-pourraient-sattaquer-a-dautres-communes-suisses.html [accédé le 07.09.2021]

notre ville en termes de sécurité informatique vis-à-vis des autres communes du Canton et de Suisse ?

4. La DSI est-elle à jour avec tous les correctifs de sécurité pour tous les logiciels qu'elle exploite, et tout particulièrement en ce qui concerne le même point d'entrée[5] que celui exploité à Rolle ? Si non, pourquoi ne l'avoir pas fait et quand compte-t-elle le faire ?
5. Si la Ville devait subir le même sort que Rolle, quelles pourraient être les données sensibles atteignables par les pirates et donc potentiellement mises en circulation ?
6. La DSI peut-elle financièrement quantifier un préjudice[6] possible dont elle pourrait faire la cible ? Si oui, investit-elle suffisamment d'énergie pour le contrer ?
7. La Ville est-elle en contact préventif avec les autorités compétentes comme fedpol, Interpol et le Centre national pour la cybersécurité ? La DSI se concerte-t-elle avec les départements IT d'autres communes et avec la DSI cantonale ?

D'avance je remercie la Municipalité pour ses réponses claires et précises.

Vevey, le 08.09.2021

Pour l'UDC Vevey

Fabienne Despot

[5]https://blog.talosintelligence.com/2021/08/vice-society-ransomware-printnightmare.html [accédé le 07.09.2021]
[6]https://hub.packtpub.com/understanding-the-cost-of-a-cybersecurity-attack-the-losses-organizations-face/ [accédé le 07.09.2021]