>MUNICIPALITE

REPONSE ECRITE

À l'interpellation de Mme la Conseillère communale Frédérique Beauvois intitulée « La sécurité numérique à Renens » et à l'interpellation de M. le Conseiller communal Jonas Kocher intitulée « Plan d'action en cas d'attaque !? »

Renens, le 7 février 2022

Madame la Présidente,
Mesdames les Conseillères communales, Messieurs les Conseillers communaux,

En date des 9 septembre et 11 novembre 2021, Mme la Conseillère communale Frédérique Beauvois et M. le Conseiller communal Jonas Kocher ont respectivement interpellé la Municipalité sur des questions en lien avec la gestion de l'informatique dans le contexte du télétravail ainsi qu'en relation avec les récentes attaques informatiques communales.

Différentes questions sont adressées à la Municipalité pour lesquelles elle propose les éléments de réponse suivants :

- ***Qu'est-ce que la commune a pu faire pour renforcer la sécurité du télétravail ?***

  Au-delà des mises à jour régulières de l'infrastructure serveurs, du parc informatique ainsi que de la sécurité via les antivirus et le firewall, la complexité et la fréquence de changement des mots de passe ont été renforcées. De plus, pour toutes connexions hors du réseau de la Commune (par exemple depuis le domicile), un système de double authentification (MFA) a été mis en place et rendu obligatoire.

- ***Qu'en est-il de la protection des données des citoyens et des données personnelles des collaborateurs ?***

  Les données des Renanaises et des Renanais traitées par la Ville de Renens sont actuellement hébergées au sein de nos deux « centres de données » installés sur notre Commune. Il en va de même pour les données des collaboratrices et des collaborateurs.

  L'accès à ces données est réservé uniquement aux personnes autorisées à travers des droits et profils utilisateurs administrés au sein de l'infrastructure de la Ville de Renens. Il est dès lors très limité (toutes les données ne sont pas accessibles partout). De plus, lorsqu'il est nécessaire d'y avoir accès à travers internet, un mécanisme d'authentification forte est mis en place.

./.

- ***Existe-t-il un plan d'urgence en cas de cyberattaque ?***

  En cas d'urgence, le plan fourni par la DGNSI (Direction générale du numérique et des systèmes d'information) du Canton de Vaud ainsi que les bonnes pratiques recommandées par l'UCV (Union des Communes Vaudoises), notamment le guide NEDIK et le label suisse de cybersécurité Cybersafe seront appliqués.

  Le projet de changement d'infrastructure en 2022 permettra la mise en place d'un plan complet de continuité de l'activité. Ces éléments seront précisés dans le préavis qui sera soumis prochainement au Conseil communal.

- ***Est-ce que les collaborateurs sont formés aux réactions d'urgence adéquates, comme par exemple, ne pas connecter les ports USB et se débrancher du réseau, ne pas éteindre les ordinateurs mais de les débrancher.***

  Une formation de sensibilisation a été donnée il y a un peu plus de deux ans. Etant donné le contexte très changeant quant à la nature des attaques et les moyens à disposition pour les réaliser, il est important de refaire une campagne de sensibilisation sur les bonnes pratiques à adopter pour l'usage de nos outils informatiques et des points de vigilance à avoir. Par conséquent, une nouvelle série de formations à la cybersécurité sera prévue cette année.

- ***Quel est le plan d'action de la Municipalité pour pouvoir remettre en marche le navire après l'attaque et s'il n'existe pas, compte-t-il en mettre un en place ?***

  Comme évoqué plus haut, la procédure de la DGNSI serait utilisée conjointement avec des prestataires tiers et des membres du SOC (Security Operation Center) du Canton de Vaud. Un système de sauvegarde déporté (hors du réseau de la ville) est actuellement en fonction de manière quotidienne dans le but d'avoir à disposition les données critiques pour une éventuelle restauration de nos données la plus rapide possible.

- ***Comment est articulée la collaboration entre le SOC (Security Operation Center) basé à Renens, la Confédération et la Ville de Renens ?***

  Actuellement, le SOC communique des informations en lien avec des attaques et/ou des failles de sécurité qui apparaissent à l'échelle nationale, voire même internationale comme récemment Log4shell. De plus, la Ville de Renens possède dans son infrastructure, des équipements informatiques propriétés du Canton. Par conséquent, lorsque des failles peuvent potentiellement toucher leurs équipements, le SOC nous informe des possibles vulnérabilités et des actions à entreprendre liées spécifiquement à ses composants.

  À contrario, si nous devions subir une attaque ou encore découvrir une faille identifiée au sein du réseau de la Ville, nous informerions directement le SOC : d'une part pour qu'ils prennent des mesures dans d'autres environnements informatiques et d'autre part pour des prestations de soutien.

  En complément, depuis le 12 janvier dernier, le Conseil fédéral a ouvert une procédure de consultation sur l'avant-projet de modification de la loi sur la sécurité de l'information relatif à l'introduction d'une obligation de signaler les cyberattaques contre les infrastructures critiques. Cela signifie que lors d'une attaque sur une infrastructure critique (qui comprend aussi les autorités cantonales et communales), les exploitants seront dans l'obligation de déclarer l'incident auprès du Centre national pour la cybersécurité (NCSC). En contrepartie, le NCSC fournira un soutien de premier secours aux exploitants dans la gestion des cyber incidents.

./.

- ***Les attaques ont souvent lieu aux heures creuses (weekend ou en soirée) où il est plus difficile de réagir, dès lors, est-ce qu'une coordination de piquet avec les communes avoisinantes existe ? Sinon est-elle envisagée à court terme ?***

  Pour l'heure, il n'existe aucun service de piquet pour le service informatique de la commune. L'hétérogénéité des infrastructures informatiques (architecture, composants, marques, configuration, etc.) des différentes villes ne permet pas une mutualisation d'un service de piquet apportant une plus-value de fonctionnement. En effet, au vu de ce qui précède, il faudrait de toute façon faire appel au service informatique voire même aux prestataires externes de ladite commune pour intervenir.

  Néanmoins, le personnel du service informatique est conscient qu'il peut être sollicité en dehors des heures de travail pour intervenir dans le cas d'une situation critique.

La Municipalité considère ainsi par la présente avoir répondu respectivement à l'interpellation de Mme la Conseillère communale Frédérique Beauvois concernant la sécurité informatique, ainsi qu'à l'interpellation de M. le Conseiller communal Jonas Kocher concernant un plan d'actions en cas d'attaque informatique.

AU NOM DE LA MUNICIPALITE

Le Syndic: Le Secrétaire municipal:

Jean-François Clément Michel Veyre