Réponse de la Municipalité à deux interpellations

Interpellations de MM. Julien Pidoux et David Regamey, Conseillers communaux, quant à la cyberattaque au sein de l'administration communale

Secrétariat municipal

M. Alain Monod, Syndic

Réponse à l'interpellation adoptée par la Municipalité

Route de la Croix-Blanche 25
021 785 61 00
Case postale 187
greffe@epalinges.ch
1066 Epalinges
www.epalinges.ch

Table des matières

Objets des interpellations 2
Réponse de la Municipalité : 2
Résumé de la situation 2
Développement 2
Conclusion 4

Objets des interpellations

- M. Julian Pidoux – *Interpellation déposée le 7 septembre 2021 : La Commune d'Epalinges est-elle prête à faire face à une cyberattaque ?*

- M. David Regamey – Interpellation *déposée le 21 septembre 2021* : *Protéger l'administration communale, ainsi que les données personnelles des employés communaux et des administrés, contre les cyberattaques ?*

Réponse de la Municipalité :

Résumé de la situation

Au niveau contractuel, la sécurité du réseau informatique communal est déléguée et assurée par notre prestataire OFISA Informatique SA, à Renens. Cet établissement gère et entretient les différents systèmes (hardware et software), et maintient à jour les divers logiciels utilisés, soit de manière ponctuelle (serveurs, serveurs virtuels, ERP, Windows, Microsoft Office, etc.), dès que des correctifs peuvent être appliqués, soit de manière automatique pour les postes de travail, notamment.

Développement

Un audit de l'infrastructure et de l'utilisation des divers logiciels est en cours, principalement dans le but d'obtenir le label « Cybersafe », ainsi que pour définir clairement le ou les protocoles d'urgence, mais également pour déterminer l'ensemble des vulnérabilités, alors qu'une campagne de sensibilisation des utilisateurs vient d'être débutée avec la solution éprouvée TERRANOVA. Cette dernière doit permettre de sensibiliser chaque utilisateur avec les solutions informatiques actuelles, tout en intégrant des envois de mails factices (phishing ou hameçonnage) au cours de l'année que doit durer cette campagne (utile tant au niveau professionnel que privé), et qui, selon toute vraisemblance, sera reconduite dans le but d'assurer une formation continue du personnel.

Les récentes informations en lien avec des cyberattaques, survenues, notamment, dans deux collectivités publiques vaudoises et ayant largement été diffusées dans les médias et sur les réseaux sociaux, ont soudainement mis en avant la sécurité informatique devant alors être pointée du doigt ; cependant, de telles attaques ne datent pas seulement de 2021, mais interviennent depuis de nombreuses années. Raison pour laquelle il est impératif d'être toujours en alerte sur ce point, pas uniquement lorsque des cas surviennent et sont copieusement détaillés dans la presse.

De toute manière, en ce qui concerne la sécurité informatique, il faut bien être conscients que le risque zéro n'existe pas : aucune société, ni personne n'est intouchable (tant au niveau professionnel que personnel). En effet, les cybercriminels ont trouvé un filon qu'ils exploitent aujourd'hui sans réserve,

à savoir les attaques par rançongiciels (ransomwares), leur accordant des moyens financiers toujours plus conséquents.

De ce fait, ces tentatives d'intrusion ne cessent d'évoluer ; toutefois et en résumé, elles consistent principalement à s'introduire dans un système informatique en profitant d'une ou de plusieurs vulnérabilités comme, par exemple, un e-mail contenant une pièce jointe avec du contenu malicieux, un lien redirigeant sur un site frauduleux ou encore pour subtiliser un nom d'utilisateur et un mot de passe.

Ces étapes passées, les pirates cherchent alors, de manière plus ou moins automatisée, à chiffrer des fichiers ou des bases de données pour les rendre indisponibles et demander ensuite le paiement d'une rançon contre les clés de chiffrement. À noter également qu'ils profitent aussi parfois de dérober des données accessibles en masse pour mettre davantage de pression sur les victimes, les menaçant de les divulguer si elles ne paient pas une rançon, qui ne cesse ensuite d'être augmentée chaque jour.

De source cantonale, nous avons pu apprendre que toutes les récentes attaques, publiées ou non dans les médias, ont été lancées de la même manière : l'usurpation d'identité (vol d'un nom d'utilisateur et d'un mot de passe) pour se connecter ensuite à un accès à distance non sécurisé, ne comprenant qu'un seul facteur, soit ces seules informations.

L'authentification forte, ou à deux facteurs au minimum (informations précitées + un code à usage unique supplémentaire), aurait suffi à les éviter. Tous les accès à distance (VPN, RDP ou autres, ainsi que tous les autres accès aux ressources internes, comme la messagerie électronique, Sharepoint, etc.) doivent obligatoirement être sécurisés par une telle authentification.

Il faut également savoir que d'autres communes ont été ciblées, alors que certaines Villes vaudoises déjouent des attaques presque quotidiennement. Il est donc impératif de maintenir à jour tous les logiciels, applications, ainsi que l'infrastructure informatiques.

Toutes ces raisons ont toujours été une source de préoccupations nous ayant poussé à suivre avec attention ces problématiques, nous permettant d'affirmer que le réseau informatique communal est maintenu à jour de manière suivie (tant au niveau du matériel, récent, performant et fiable, que de tous les logiciels utilisés), alors que la sécurisation des accès à distance et la sensibilisation des utilisateurs sont des points que nous suivons et tentons de maintenir à un haut niveau.

En effet, l'authentification à double facteurs est de mise pour tout accès distant, alors que la politique de complexification et d'utilisation de mots de passe vient d'être accentuée, ne permettant plus d'utiliser des mots de passe « basiques » ou génériques (nombre de caractères minimal requis, choix de ceux-ci devant être mélangés à des chiffres ou caractères spéciaux) et devant être changés périodiquement (sans possibilité de réutiliser le même qu'auparavant et ne pouvant pas être modifié deux fois de suite en 24 heures).

À ce jour, et fort heureusement, la Commune d'Epalinges n'a pas fait l'objet d'une telle cyberattaque. Les moyens mis à disposition déjouent quelques tentatives, qui se sont intensifiées après le récent tapage médiatique sur ce sujet (il est bien connu que tant que personne n'en parle trop, ça n'attire pas spécialement l'attention, donc, par-là, les convoitises), mais les procédures mises en place et le suivi périodiques des mises à jour nous ont permis d'y échapper.

Cette réalité nous plonge surtout dans la constatation que la prochaine épidémie pourrait plutôt provenir d'un virus informatique ou d'une charge virale telle, qu'elle pourrait submerger les réseaux

informatiques ou bloquer internet. Ce qu'ont bien compris les compagnies d'assurances qui, jusqu'ici, proposaient certaines couvertures dites de « Cyberprotection » ; cependant, à la lumière des évènements se déroulant de plus en plus fréquemment et étant très vite et abondamment repris ou documentés dans la presse, en précipitent pourtant déjà certaines à retirer soudainement ces propositions d'assurances, trouvant alors les risques potentiels bien trop grands…

Pour le surplus, toutes les données informatiques sont sauvegardées quotidiennement (de manière incrémentielle) sur un site distant du lieu où sont situés les serveurs physiques (aucune donnée n'est stockée dans le Cloud ou de manière décentralisée, alors que les serveurs de sauvegardes sont hors ligne - ou hors réseau), puis entièrement de façons hebdomadaire et mensuelle, toujours sur une site distant différent. Les pertes potentielles de données en cas d'attaque(s) éventuelle(s) sont, de ce fait, réduites au maximum à une journée.

Les bases de données de nos logiciels ERP (logiciels de gestion - Office de la population et comptabilité) sont en passe d'être entièrement cryptées par nos fournisseurs (une partie l'étant déjà, les bases étant configurées de telle manière que chaque donnée mise bout à bout avec la suivante ne veut plus rien dire), dans le but évident de ne pas pouvoir être facilement lisibles ou compréhensibles ; ce dernier point accentuera encore l'amélioration de la sécurisation des données conservées dans nos ERP.

De plus, aucune donnée sensible nominative ou contenant des chiffres clairement établis sur nos contribuables ne sont conservées de façon à pouvoir les exploiter pour nuire ou semer le trouble ou des doutes en cas de vol(s). La délégation de compétences des taxations des contribuables au Canton accorde un degré de sécurité complémentaire à une entité ayant des moyens financiers et humains mieux proportionnés à la valeur des données y relatives.

Au niveau des synergies (autres Communes, Canton ou Confédération) et contrairement à d'autres Cantons (ce n'est de loin pas une priorité ou envie du Canton de Vaud), comme chaque collectivité vaudoise est libre de ses propres choix en matière d'informatique (et ce, malgré plusieurs tentatives pour tenter d'amener à centraliser des solutions applicatives ou matérielles, dans le but évident de mutualiser les coûts et infrastructures), à ce jour, il n'existe pratiquement aucune possibilité d'entrevoir des collaborations fructueuses, fiables et sûres.

Conclusion

Conformément à ce qui précède, les données personnelles des employés, des citoyens et des entreprises palinzardes peuvent être considérées comme étant activement protégées ou assez difficilement exploitables en l'état. Toutefois, comme déjà mentionné précédemment, le risque zéro n'existe et n'appartient qu'à celle ou celui s'enfermant derrière la croyance de posséder la plus sophistiquée et couteuse armure sécuritaire disponible sur le marché.

Par conséquent, nous estimons disposer et mettre en place tous les moyens nécessaires à sécuriser de la meilleure façon possible et éviter les potentielles fuites des données de nos collaborateurs, citoyens et des entreprises sises sur notre territoire communal ; jusqu'ici, à entière satisfaction, que nous désirons continuer d'améliorer et, ainsi, rechercher à faire en sorte que cette situation se poursuive dans les mois et années à venir.

Epalinges, le 3 novembre 2021

Au nom de la Municipalité

Le Syndic

Alain Monod

La Secrétaire municipale a.i.

Sylvie Guggenheim