

# Code P.O.R.T.E.

## Porte Ouverte à Risque Technologie Élevé

Depuis leur démocratisation, les technologies de l'information ont complètement remanié notre manière de vivre. Le passage au tout-numérique a permis d'accélérer le traitement et l'échange de données, ouvrant ainsi la voie à une nouvelle ère de services dits virtuels. L'adoption mondiale de l'informatique a alors ancré cette dernière comme pilier des sociétés modernes.

Ce n'est qu'au fil des deux dernières décennies que l'on a pu être témoins de la puissance dévastatrice des attaques informatiques. La perte de contrôle des systèmes critiques mène inexorablement à des catastrophes pouvant mettre à genoux le monde entier. En 2017, le seul ransomware<sup>1</sup> WannaCry a infecté près de 300'000 appareils à travers 150 pays<sup>i</sup>, causant sur son chemin des dénis de service paralysant notamment hôpitaux, réseaux ferroviaires, services PTT et compagnies aériennes sur tous les continents<sup>ii</sup>.

Les usagers de technologie, privés comme professionnels, délaissent bien trop souvent la sécurité pour cause de procédures lourdes à implémenter, par peur de casser ce qui marche, par ignorance des risques encourus, ou tout simplement pour causes d'argent. Le public oublie que le coût de la guérison dépasse largement celui de la prévention : le groupe logistique Maersk estime<sup>iii</sup> à USD 300'000'000 les dommages qu'il a essuyés à cause de Petya<sup>2</sup> en 2017.

Ces attaques, ayant vu le jour grâce à un logiciel développé par la NSA<sup>iv</sup> qui exploite une vulnérabilité dans Windows, nous rappellent deux importantes leçons : 1) la sécurité par l'obscurité est un concept fondamentalement imparfait et extrêmement dangereux et 2) les menaces sont réelles, à bout portant, et frappent sans préavis.

La ville de Vevey a validé CHF 1'155'000 des dépenses pour la Direction des Systèmes d'Information (DSI) entre les bouquets de licences Microsoft (P03/2019), le renouvellement de son infrastructure informatique (P35/2019), et la création du nouveau site Web vevey.ch (P17/2018). La mention de sécurité a souvent dû être arrachée par les commissaires qui traitaient des sujets en mention, mais rarement a-t-on reçu des preuves concrètes de sa prise en considération voire de son implémentation. Face aux réalités que nous devons affronter, il est nécessaire de vivre avec son temps et adapter sa stratégie. La politique de l'autruche n'est pas viable sur le long terme.

1 Logiciel malveillant forçant à payer des rançons en bloquant l'accès à un système

2 Ransomware similaire à WannaCry

Séance du 18 juin 2020

Mes questions pour la Municipalité sont :

1. La Municipalité a-t-elle déjà mené un audit de sécurité sur son infrastructure IT et le nouveau site Web de la ville ?
  - a) Si oui, quel en fut le résultat ? Un rapport est-il disponible ?
  - b) Si non, quand cela est-il prévu ? Quels seront les points traités ?
  
2. La Municipalité a-t-elle déjà évalué l'option des logiciels libres pour son infrastructure IT (uniquement serveurs, réseau, etc.) ?
  - a) Si non, pour quelles raisons ? Quels étaient les critères comparatifs ?
  - b) Si oui, quel fut le bilan ? Quelles décisions furent prises en conséquence ?

Je demande à recevoir une réponse écrite.

Vevey, le 11.06.2020

Au nom du groupe UDC

Moïn Danai

Références:

- Europol, «Internet Organised Crime Threat Assessment (IOCTA) 2017», 2017
- A.P. Møller – Mærsk A/S, «Annual Report 2017», 2017
- The Guardian, <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded>, [accédé le 24.02.2020]
- Der Spiegel, <https://www.spiegel.de/international/the-germany-file-of-edward-snowden-documents-available-for-download-a-975917.html>, [accédé le 24.02.2020]
- Wired, <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>, [accédé le 24.02.2020]
- Telegraph, <https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/>, [accédé le 13.05.2020]
- Reuters, <https://www.reuters.com/article/us-cyber-attack-russia/exclusive-wannacry-hits-russian-postal-service-exposes-wider-security-shortcomings-idUSKBN18K26O>, [accédé le 13.05.2020]



## Interpellation

Conseil communal de Vevey

Séance du 18 juin 2020

- Reuters, <https://www.reuters.com/article/us-cyber-attack-germany-rail/german-rail-operator-affected-by-global-cyber-attack-idUSKBN1890DM>, [accédé le 13.05.2020]

- 
- i Selon rapport Europol, page 19
  - ii Selon articles Telegraph et Reuteurs
  - iii Selon rapport annuel Maersk, page 54
  - iv Selon article Wired