

CYBERATTQUES

Gare à l'imprudence humaine



Il faut s'intéresser à la cybercriminalité, avant d'être pris de vitesse, mettent en garde le CEO d'AZ Informatique Jean-Pierre Rérat, le criminologue Olivier Beaudet-Labrecque et la syndique de Rolle Monique Choulat-Pugnale (de g. à dr.) photo Stéphane Gerber

BENJAMIN FLEURY

► **Victime d'une cyberattaque, la commune de Rolle a vu le ciel lui tomber sur la tête l'an passé. Dans le Jura, une telle situation est possible, selon un expert de passage jeudi à Delémont. À le croire, la cybercriminalité devient un business, tant l'impunité est grande, et il faut s'y préparer.**

La petite salle de Cinemont est bien remplie ce jeudi. Les 80 personnes présentes, dont de nombreux représentants communaux, ne sont pourtant pas là pour assister au nouveau *Top Gun* et à ses spectaculaires offensives aériennes. Il est cette fois question d'attaques moins visibles, plus sournoises et potentiellement graves.

L'entreprise bruntrutaine AZ Informatique avait convié le public à une conférence sur le thème actuel de la cybercriminalité, avec une invitée des plus concernées: la syndique de Rolle. Coïncidence du calendrier, la commune vaudoise avait vu il y a quasiment une année les données de 5000 habitants être volées, puis publiées sur le darknet (un espace numérique souterrain, qui présente souvent une dimension criminelle).

Le traumatisme de Rolle

Un épisode traumatisant pour ses autorités et notamment sa syndique, Monique Choulat Pugnale. «Nos citoyens étaient inquiets quand l'affaire a été publiée dans les médias. De quoi avaient-ils peur? De la publication de leurs données fiscales. C'est humain», souligne celle qui connaît bien le Jura, pour avoir grandi à Grandgourt.

La commune avait fait le choix au début de ne pas communiquer sur cette attaque afin de ne pas se rendre plus vulnérable encore. Mais les révélations des médias ont ensuite provoqué un véritable tsunami, relève la syndique, qui se rappelle avoir passé des nuits très courtes pour rassurer les citoyens, mais aussi résoudre le problème. «On a dû analyser toutes les données publiées sur le darknet. Je ne vous dis pas le travail!» relève-t-elle. En tout 65 boîtes mail ont été piratées et 32 GB de données subtilisées. Tout cela à cause de la mauvaise manipulation d'une employée, reconnaît à demi-mot Monique Choulat Pugnale.

Attaque à Vendlincourt

Ce cauchemar est provoqué dans la plupart des cas par une erreur humaine. Celle-ci arrive par exemple en ouvrant une simple pièce jointe qu'il ne faudrait pas. Les différentes administrations veulent à tout prix éviter que cela n'arrive. Le cas de Rolle a servi d'électrochoc. À Porrentruy, dont la taille est relativement similaire à celle de Rolle, les autorités ont déjà imposé une double identification dans certaines manipulations informatiques, organisé des formations et mis sur pied des tests à l'aveugle suite à l'affaire. «Le risque existe. Il est en augmentation. La véritable question est de savoir quand on sera attaqué», confie en aparté le maire Gabriel Voirol.

Des attaques informatiques, en fait, c'est déjà une réalité dans le canton du Jura. La commune de Vendlincourt en a subi une il y a quelques mois. Dans ce cas-là, c'est l'ouverture d'un simple SMS par une employée communale qui a permis à un virus de se frayer un chemin, confirme le maire Éric Gerber. Mais heureusement, les criminels n'ont pu mettre la main sur aucune donnée sensible. «Elles sont protégées par un serveur spécial, relève-t-il. La seule chose qu'ils ont pu consulter, c'est la comptabilité générale de la commune, mais elle est publique», sourit-il. Aucune demande de rançon n'a été faite. Plus de peur que de mal donc.

Administrations pas toujours bien préparées

Mais il n'en demeure pas moins que cette histoire semble montrer à quel point les cyberattaques peuvent concerner tout le monde. «Elles sont en hausse, dans le Jura comme partout», confirme Olivier Beaudet-Labrecque, criminologue. Selon lui, les raisons sont simples. C'est un vrai business. «Les cybercriminels se rendent compte qu'ils peuvent vraiment gagner beaucoup d'argent, qu'il y a un manque de préparation au niveau des cibles et qu'il y a une forme d'impunité. Contrairement à ce qu'on pense, ce ne sont plus des gens en capuchon qui font cela, mais des personnes en costard qui développent de vrais business models», souligne cet expert de l'Institut de lutte contre la criminalité économique à Neuchâtel.

En Suisse, le taux d'élucidation des différentes infractions numériques est en effet très faible. Les cybercriminels dorment tranquilles. Dans le canton du Jura l'année passée, aucun des 12 cas d'arnaque au président, de phishing, de cheval de Troie bancaire ou de ransomware n'a ainsi été élucidé.

Pour Olivier Beaudet-Labrecque, les administrations doivent à tout prix prendre le risque au sérieux. «Si on se fait voler, souvent on ne retrouve pas l'auteur. Prendre des mesures préventives est très important», met-il en garde.