Attaque informatique de la mairie : quelles leçons en tirer ? (2/2)

La commune de Sequedin était vigilante en matière de sécurité informatique mais elle n'a pas pu prévenir l'attaque, il y a près de deux ans. Aujourd'hui, les collectivités, comme la Métropole européenne de Lille (MEL) commencent à prendre la mesure des risques et des enjeux. Avec des moyens encore insuffisants.

PAR FRANCK BAZIN
loos@lavoixdunord.fr

Les attaques informatiques sont de plus en plus sophistiquées et demandent des outils de défense et des comportements adaptés pour s'en prémunir. PHOTO ARCHIVES PIB

SEQUEDIN. Le jeudi 11 juillet 2019, la mairie de Sequedin découvrait un système informatique piraté dans la nuit, complètement inutilisable (*notre précédente édition*). Pendant plusieurs semaines, avec la seule aide de son prestataire, la mairie a essayé de trouver des solutions pour pouvoir retravailler le plus rapidement possible, le plus normalement possible.

MUTUALISER LES COMPÉTENCES

Ce n'est qu'en septembre que le contact est établi, fortuitement, avec un nouveau service de la Métropole européenne de Lille (MEL), le RGPD mutualisé (Règlement général sur la protection des données). La réglementation européenne fait obligation à toutes les structures, qui traitent, stockent, etc., des données personnelles, de respecter des procédures afin de préserver les libertés individuelles.

Cette tâche est lourde et elle passe, notamment, par la nomination d'un délégué à la protection des données (ou *DPO, « data protection officer »* en anglais). L'intercommunalité a jugé qu'il pourrait être plus efficace et plus économique de mutualiser ces compétences : le service, composé de 4 DPO et d'un responsable de la sécurité des systèmes d'information (RSSI), est devenu opérationnel en juin 2019.

Sa mission devait être d'accompagner les communes dans leur mise en conformité par rapport à la réglementation. La grave crise sequedinoise a été un redoutable baptême du feu. Elle a peut-être permis à d'autres communes de comprendre à quel point les systèmes informatiques sont vulnérables. Sequedin n'étant pas la moins préparée des administrations locales.

Pierre Barrial, le RSSI, admet avoir découvert des systèmes totalement vulnérables : « *Les mairies font souvent confiance à leur prestataire et achètent ce qu'on leur présente comme étant le meilleur.* » Mais sans être en capacité de l'évaluer.

CINQUANTE-HUIT COMMUNES ADHÉRENTES

Avec sa collègue DPO Claire Cabaret, Pierre Barrial a aidé Sequedin à surmonter la crise. C'est, de loin, l'événement le plus grave auquel ils ont été confrontés depuis la naissance du service.

> ***“ Les mairies font souvent confiance à leur prestataire et achètent ce qu'on leur présente comme étant le meilleur. ”***

Aujourd'hui, le service peut difficilement répondre aux attentes et aux besoins des 58 communes adhérentes aux dispositifs, même en fonctionnant en surrégime.

Le travail impose, dans certaines structures, de revenir sur des années de mauvaises pratiques et d'habitudes dangereuses. ■

Les communes qui n'ont pas encore rejoint le dispositif de RGPD mutualisé peuvent pendre contact avec la MEL : www.lillemetropole.fr.

La société villeneuvoise AxBx lance une solution de protection contre les rançongiciel

La protection informatique est une guerre de mouvement. Et pas à armes égales, comme le constate depuis 15 ans, l'âge de sa solution de sécurité informatique VirusKeeper, l'entrepreneur villeneuvois Grégory Snauwaert : « *Contrairement à nous, les pirates ont un temps infini. Ils attaquent quand ils veulent et n'ont pas à respecter des règlements. Moi, je n'ai pas le droit de répliquer. Nous jouons exclusivement en défense.* »

Se prémunir de la menace passe par une organisation stricte : « *Dans beaucoup de structures, la direction veut un accès à tout le système, avec un compte administrateur. Ce sont souvent ces comptes qui sont des portes d'entrée. Il y a beaucoup trop de comptes “admin” dans les réseaux !* »

Il faut aussi des logiciels adaptés : un système d'exploitation (Windows) et des applications toujours mis à jour. Il faut un antivirus. Un vrai, payant. Les solutions gratuites sont peu satisfaisantes : Windows Defender ne réagit que trop rarement face à une attaque et, comme confirmé par une enquête en 2020, Avast vit grâce à la vente des données personnelles de ses utilisateurs.

DÉTECTER LES SIGNAUX ANNONÇANT L'ATTAQUE

Reste qu'il fallait développer une solution spécifique pour contrer les rançongiciel, ces programmes qui cryptent toutes les données d'un serveur et réclament une rançon à la victime pour libérer le système.

Grégory Snauwaert s'est appuyé sur l'analyse comportementale, une technique que sa société AxBx maîtrise parfaitement puisqu'elle est au cœur de VirusKeeper : « *Notre logiciel, RanShield, détecte les signaux faibles : le pirate prépare l'attaque pendant plusieurs jours, c'est ce travail qu'il faut identifier.* »

Le rançongiciel va ouvrir tous les fichiers pour les crypter. Si un programme se met à envoyer massivement des appels sur l'interface de programmation d'application (API) de chiffrement de Windows, c'est qu'une attaque commence. RanShield va alors bloquer le programme, isoler l'ordinateur et alerter le gestionnaire de réseau. ■

La solution est disponible depuis ce mercredi sur le site d'AxBx. Il en coûte à partir de 900 € pour 10 postes (mise à jour autour de 225 €).

Grégory Snauwaert s'est appuyé sur l'analyse comportementale, une technique que sa société AxBx maîtrise puisqu'elle est au cœur de son antivirus, VirusKeeper.