La Cybersécurité dans les collectivités

Introduction

D'années en années, les cyberattaques se sont répandues dans nos sociétés en suivant le développement du numérique. La motivation première des attaquants reste à ce jour l'appât du gain (revente de numéro de cartes de crédit, de données personnelles…) mais peut aussi satisfaire à des intérêts politiques ou stratégiques entre nations (Kuru, 2017). Les cibles ont donc été dans un premier temps celles qui pouvaient s'avérer être les plus lucratives ou avoir un impact fort sur le fonctionnement d'une nation. Les cibles de premier choix ont déployé au fil des années des mesures de protection si bien que les gains escomptés pour les attaquants sont devenus trop faibles par rapport à l'investissement humain ou technique nécessaire. Les attaquants ont donc logiquement porté leur dévolu sur des acteurs plus vulnérables comme, par exemple, les collectivités territoriales (ANSSI, Avril 2019). Pourtant ces dernières élaborent des plans de transition vers le numérique dans les relations avec les citoyens ; la sécurité ne doit donc plus être perçue comme une contrainte mais bien comme un gage de confiance dans l'usage du numérique. Cette notion est essentielle pour le développement des villes connectées dîtes intelligentes.

Cet article présente donc dans un premier temps un état des lieux des incidents subis par les collectivités en France sur la base d'articles relayés dans la presse mais aussi des tendances observées à travers le monde. Dans un second temps nous verrons comment les états européens ont fait évoluer le cadre règlementaire. Enfin sera abordée la problématique de l'acculturation à la Cybersécurité ou comment cette dernière permet de transformer le maillon faible humain en un acteur au quotidien de la sécurité du numérique.

Etat des lieux

Dès 2015, une étude menée sur les incidents de Cybersécurité affectant les collectivités était menée par Rémy Février (Février, 2015). Elle indiquait clairement que ces dernières pouvaient être la cible de Cyberattaques sur les trois couches (physique, logique et sémantique) avec un impact dépassant largement le cadre de l'informatique et par extension les informaticiens.

Mais c'est l'incident qui affecta la ville d'Atlanta aux USA (Axelrod, 2018b) le 24 mars 2018 qui permet de réaliser la faiblesse et la sous-estimation du risque Cyber dans les « Smart Cities ». La ville s'est alors trouvée prise en otage, une rançon de 51 000 $ étant réclamée pour retrouver l'accès aux données. Le système d'information s'est donc trouvé inopérant pendant plus de dix jours. La ville dépensant alors 2.6 millions de $ en prestations informatiques et en communication de crise. (Axelrod, 2018a). Pourtant des audits de sécurité réalisés en 2010 et 2014 mettaient déjà l'accent sur une négligence importante des aspects de Cybersécurité (budget insuffisant, pas d'application des correctifs de sécurité…). L'attaque de mars 2018 aura coûté environ 17 millions de $ et aurait pu être évitée si les mesures d'hygiène numérique avaient été mises en œuvre mais aussi si le budget alloué à la protection de l'information avait été correctement dimensionné (Deere, 2018).

Si une métropole de la dimension d'Atlanta a été victime d'une attaque par rançongiciel qu'en est-il de petites communes, peuvent-elles être aussi des cibles ? La réponse est bien évidemment affirmative. Rappelons-nous de la motivation première des attaquants, faire de l'argent. Lancer une attaque sur plusieurs cibles simultanément augmente les chances de

succès et donc de ROI[1] pour l'attaquant. C'est l'amer constat que la mairie de Lacroix Valmer (~4000 habitants) dans le Var a été contrainte d'observer. En effet, le 31 juillet 2018 ses installations se trouvaient prises en otage par un rançongiciel pour la troisième fois (Max, 2018). La reconstruction du SI[2] s'est étalée sur 2 mois. Le directeur des services techniques dans une interview pour ARTE indiquait être surpris par la volonté de destruction qui anima les attaquants (Jalabert, 2019) et le manque de préparation de la ville face à ce type d'incident. L'élément récurrent, permettant le succès des attaques, commun aux grandes métropoles comme aux petites villes, semble être l'absence de gestion de l'obsolescence et des vulnérabilités. L'exemple de Chambéry dont les feux de circulation sont gérés par le système Windows XP (qui n'est plus maintenu depuis le 8 avril 2014) en est une belle illustration (Rosin, 2019). Les systèmes industriels ne sont pas mieux maintenus que leurs homologues bureautique ; bien au contraire. Les DSI[3] ont, pendant de nombreuses années, négligé les systèmes industriels lorsque ces derniers sont passés sur des liaisons IP[4]. Ce sont les automaticiens qui ont vu en ce changement de technique de liaison une opportunité de simplification. Cependant, les contraintes et la culture sécurité n'est pas la même entre le monde de l'OT[5] et de l'IT[6]. C'est ainsi que deux ingénieurs ont conduit des audits de sécurité sur différentes villes en Europe. Ces travaux ont été présentés au cours des conférences « Le Hack 2019 » qui s'est tenue en juillet dernier à Paris. Le constat est sans appel, le scénario catastrophe n'est plus qu'une question de temps si rien ne change (Gilbert, 2019). Si certaines villes arrivent à « résister » aux attaques à l'instar de Sarrebourg (Ugolini, 2019), certaines villes américaines commencent à payer les ravisseurs arguant que les couts de la rançon restent moindres par rapport aux dépenses à engager pour reconstruire un SI (Mazze, 2019). Si sur le principe le raisonnement peut sembler juste, il est sur le long terme totalement contreproductif car d'une part il entretien le système criminel et l'encourage à poursuivre et d'autre part, il n'y a aucune garantie de retrouver un accès aux données. La Cybersécurité doit être pensée et intégrée en amont des projets. Est-ce que la réponse ne se trouve pas dans un cadre règlementaire plus strict ?

Un cadre règlementaire

Des incidents comme celui causé par le ver Stuxnet en 2010 (Chen, 2014) ont conduit les états à repenser le côté stratégique du numérique. En France, des activités jugées vitales pour le fonctionnement de la nation ont ainsi été déterminée en 2013 dans le cadre de la loi de programmation militaire (Anon., 2013). Ceci a conduit en 2015 à la création des Opérateurs d'Importance Vitale (OIV). Ces derniers se trouvant soumis à une obligation de mise en conformité par rapport à un référentiel défini par l'ANSSI[7]. Les collectivités territoriales peuvent être concernées par ces mesures dès lors qu'elles traitent des domaines sensibles tels la distribution d'eau potable ou la production d'énergie. Ces mesures ont été complétées en 2016 par la directive NIS[8] qui dans sa déclinaison française (ANSSI, 2018) a conduit à la création d'Opérateur de Services Essentiels (OSE) en 2018. Les OSE sont définis comme des acteurs dont le service, tributaire d'un ou de plusieurs systèmes d'information, est essentiel au maintien de l'activité économique et sociétale. Là encore les collectivités sont concernées

[1] *Return On Investment*
[2] Système d'Information
[3] Direction des Systèmes d'Information
[4] Internet Protocol
[5] *Information Technology*
[6] *Information Technology*
[7] Agence Nationale de Sécurité des Systèmes d'Information
[8] Network and Information Security

comme par exemple les services en charge de la gestion du trafic routier ou bien la restauration scolaire. Lorsqu'elles sont désignées, un calendrier de mise en conformité est alors mis en œuvre par l'ANSSI et les non-conformités sanctionnées par une amende.
Sur le même calendrier que la directive NIS, le RGPD[9] est entré en vigueur le 25 mai 2018. Il impose la mise en œuvre des concepts de Privacy & Security by design dans les opérations manipulant des données personnelles de résidant de l'Union Européenne (Vétois, 2018). L'arrivée de ce règlement a conduit à des changements au niveau des acteurs du numérique ou de toute entité manipulant de la donnée personnelle, au premier rang desquelles se trouvent les collectivités territoriales. Pour ces dernières, le manquement aux obligations fixées par le RGPD peut se traduire par une amende dont le montant est compris entre 10 & 20 millions d'euros. La CNIL[10] étant désormais chargée de veiller à la bonne application du règlement.
Le cadrage règlementaire est nécessaire pour faire progresser nos SI mais ce dernier ne doit pas atteindre un point d'irrecevabilité qui le rend inapplicable (Le Dez, 2019). La Cybersécurité ne doit plus être perçue comme un frein et le RSSI comme « monsieur Non » mais doit absolument intégrer une approche humaine et impliquer tous les acteurs.

La sensibilisation

L'ENISA[11] dans son rapport annuel (ENISA, 2019) sur l'état de la menace, dresse un tableau plaçant l'utilisateur final comme la cible principale des 5 premiers types de cyberattaques. Il est donc essentiel de transformer le maillon faible de la chaine de Cybersécurité (l'Humain) en un acteur quotidien. Pour cela plusieurs actions peuvent être menées pour procéder à l'acculturation nécessaire des utilisateurs. Il est possible de créer des supports de communication, des vidéos, des sites Internet mais la mesure la plus efficace reste les formations en présentiel assurées par une personne utilisant un vocable compréhensible des non spécialistes mais aussi en capacité de répondre aux interrogations basiques comme celles plus pointues (Bras, 2019). Le ROI peut se mesurer rapidement avec par exemple des retours plus fréquents des utilisateurs en cas de réception de courriels malveillants, permettant aux équipes techniques de contrer une campagne d'hameçonnage en désactivant les liens au niveau des plateformes de filtrage. L'utilisateur change alors de posture et devient un acteur à part entière de la Cybersécurité replaçant ainsi l'humain au cœur de la Cyberdéfense.

Conclusion

De nos jours les Cyberattaques concernent tous les pans de notre société. Elles peuvent impacter l'individu comme les très grosses entreprises. Les collectivités ne font pas exception et doivent se préparer à y faire face. La Cybersécurité doit donc devenir le levier permettant de garantir la confiance dans les usages du numérique. Cette condition est indispensable pour faire en sorte que les citoyens puissent confier leurs données et profiter des avancées que peuvent apporter les villes intelligentes.

[9] Règlement Général de la Protection des Données
[10] Commission Nationale Informatique et Liberté
[11] European Union Agency For Network and Information Security

Biographie

Cyril Bras occupe depuis mars 2018 le poste de Responsable de la Sécurité des Systèmes d'Information pour la métropole grenobloise, il est également depuis plusieurs années, enseignant vacataire en Cybersécurité à l'Université Grenoble Alpes.

Bibliographie

Anon., 2013. *LOI n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.* s.l.:s.n.

ANSSI, 2018. *Directive Network and Information System Security (NIS).* [En ligne]
Available at: https://www.ssi.gouv.fr/entreprise/reglementation/directive-nis/
[Accès le 15 Juillet 2019].

ANSSI, Avril 2019. *Rapport annuel 2018,* s.l.: s.n.

Axelrod, J., 2018a. Atlanta pays $2.6 million for cybersecurity issues stemming from $51,000 ransomware attack.. *American City & County Exclusive Insight,* 3O Avril.

Axelrod, J., 2018b. Ransomware attack causes outages across Atlanta city servers. *American City & County Exclusive Insight,* 26 Mars.p. 1.

Bras, C., 2019. *Interview vidéo Cyril Bras, RSSI Grenoble-Alpes Métropole* [Interview] (08 Juillet 2019).

Chen, M. T., 2014. CYBERTERRORISM AFTER STUXNET. *Strategic Studies InstituteandU.S. Army War College Press.*

Deere, S., 2018. *CONFIDENTIAL REPORT: Atlanta's cyber attack could cost taxpayers $17 million.* [En ligne]
Available at: https://www.ajc.com/news/confidential-report-atlanta-cyber-attack-could-hit-million/GAljmndAF3EQdVWlMcXS0K/
[Accès le 14 Juillet 2019].

ENISA, 2019. *ENISA Threat Landscape Report 2018,* Athènes: ENISA.

Février, R., 2015. Toujours plus cyber-menacées : les collectivités territoriales. *Sécurité globale ,* Mars, Issue 3 & 4, pp. 9-93.

Gilbert, K., 2019. *Villes intelligentes : leur sécurité a tout du prochain scénario catastrophe.* [En ligne]
Available at: https://www.01net.com/actualites/villes-intelligentes-leur-securite-a-tout-du-prochain-scenario-catastrophe-1727467.html
[Accès le 15 Juillet 2019].

Jalabert, T., 2019. *Cyberattaques, les villes dans le viseur* [Interview] (31 Mai 2019).

Kuru, H., 2017. Evolution of War and Cyber Attacks in the Concept of Conventional Warfare. *Journal of Learning and Teaching in Digital Age (JOLTIDA),* Décembre, Volume III, pp. 12-20.

Le Dez, A., 2019. *Tactique Cyber. Le combat numérique.* Paris: Economica.

Max, A., 2018. *Var: La mairie de la Croix-Valmer refuse de payer une rançon après le piratage de son système informatique.* [En ligne]
Available at: https://www.20minutes.fr/high-tech/2315667-20180731-var-mairie-croix-valmer-refuse-payer-rancon-apres-piratage-systeme-informatique
[Accès le 15 Juillet 2019].

Mazze, i. P., 2019. *Hit by Ransomware Attack, Florida City Agrees to Pay Hackers $600,000.* [En ligne]
Available at: https://www.nytimes.com/2019/06/19/us/florida-riviera-beach-hacking-ransom.html
[Accès le 15 Juillet 2019].

Rosin, F., 2019. *Bouchons à Chambéry : les feux de circulation fonctionnaient sous Windows XP.* [En ligne]
Available at: https://www.ledauphine.com/savoie/2019/06/26/chambery-feux-de-circulation-fonctionnaient-windows-xp-bouchons-centre-ville
[Accès le 15 Juillet 2019].
Ugolini, S., 2019. *Comment la Ville de Sarrebourg a tenu bon face à un hacker.* [En ligne]
Available at: https://www.capital.fr/economie-politique/comment-la-ville-de-sarrebourg-a-tenu-bon-face-a-un-hacker-1341897
[Accès le 15 Juillet 2019].
Vétois, J., 2018. *RGPD et loi sur les données personnelles : nouvelles contraintes, nouvelles avancées ?.* [En ligne]
Available at: https://journals.openedition.org/terminal/2182
[Accès le 15 Juillet 2019].