« Cyberfeux » sur les collectivités territoriales, une nouvelle menace ?

Stéphane MEYNET

Président-fondateur
CERTitude Numérique

Le nombre de collectivités territoriales victimes d'actes de cybercriminalité ne cesse de croître, comme le montre l'actualité depuis plusieurs mois, à tel point que les recenser précisément devient complexe.

Est-ce un phénomène nouveau, un phénomène existant mais renforcé par le développement forcé du télétravail dans le cadre de la crise sanitaire actuelle ou un « simple » effet des médias relayant d'avantage le phénomène aujourd'hui ?

Un postulat : les collectivités territoriales, quelle que soit leur taille, constituent en France des cibles potentielles au même titre que les grands groupes, PME/PMI, TPE, etc. Plus d'un millier de collectivités françaises étaient déjà ciblées en 2019 par des cyberattaques[1], avec des impacts plus en moins étendus sur leur fonctionnement. Un rappel : parmi les menaces dont sont victimes les collectivités figurent en tête aujourd'hui les rançongiciels et les fuites de données, les deux pouvant d'ailleurs être combinés.

Le phénomène des rançongiciels, s'il constitue aujourd'hui probablement la première menace à traiter face à l'explosion de ce type de cyberattaques, n'est pour autant pas un phénomène nouveau. Il sévit depuis 2015 dans tous les secteurs, touchant institutions publiques, entreprises privées de toutes tailles, ainsi que les citoyens. Le secteur de la santé a ainsi été particulièrement touché dans certains pays lors des vagues Wannacry et NotPetya de 2017.

Les collectivités constituent depuis longtemps une cible pour les cybercriminels. Rappelons qu'elles sont ainsi par exemple, depuis des années, victimes de défiguration de sites web. La liste s'allonge chaque semaine. Souvent trivial, ce type d'attaque vise à déstabiliser les élus locaux ou, comme cela fut le cas en 2015, à la suite des attentats Charlie Hebdo, à déstabiliser la France.

Les conséquences de tous ces « simples » actes de cybercriminalité, au-delà des coûts financiers importants pour la remise en service des systèmes numériques et la récupération des données (avec éventuellement le paiement de la rançon), impactent non seulement les citoyens qui se trouvent brusquement privés de certains services, mais également la sérénité et la démocratie locales. Imaginez une commune dont l'état civil est paralysé car toutes les données sont « prise en otage » par un rançongiciel. Imaginez une collectivité qui n'est plus en mesure de gérer les payes de son personnel, les cantines scolaires, certaines de ses missions sociales car les outils numériques sont indisponibles. Que dire de ces mêmes phénomènes en pleine période électorale et de l'impact sur le fonctionnement serein de la démocratie ?

L'objectif n'est, ni de pointer du doigt les collectivités victimes et leurs élus, ni de noircir le paysage de nos territoires mais nous devons comprendre et accepter que la cybercriminalité est désormais une réalité quotidienne. Nous devons la traiter, la gestion de ce risque s'ajoutant à la longue liste de ceux que doivent déjà traiter les élus et agents territoriaux.

Quelles actions à mener ?

La sécurité numérique est avant tout « l'école de l'humilité ». Même les plus grandes entreprises françaises spécialisées en cybersécurité ont été victimes de cyberattaques à des degrés de sévérité différents. Thales, Sopra-Steria et récemment Stormshield en sont des exemples.

Ne pas négliger la menace en pensant que cela n'arrive qu'aux autres, mieux la connaître pour appliquer les bons gestes barrières comme nous le faisons dans la lutte contre la COVID puis engager une approche pragmatique, portée par les élus, s'inscrivant dans un plan stratégique en soutien au développement du numérique et de la sécurité globale des territoires, tels sont les premiers conseils que nous pouvons proposer aux élus et directions des collectivités.

Force est de constater que le degré de maturité est très hétérogène sur l'ensemble du territoire national. Certaines collectivités, régions, départements, métropoles, communautés de communes, communautés d'agglomération se sont déjà emparées du sujet. D'autres ne l'ont toujours pas pris en compte. Et ce n'est pas là une question de dimension.

En complément d'une action durable portée par les collectivités elles-mêmes, l'État a bien évidement un rôle à jouer dans ce domaine.

Nous pouvons souligner l'action de la gendarmerie, de la police, des préfets et sous-préfets qui œuvrent sur le terrain pour sensibiliser les acteurs au risque cyber, expliquer les bonnes pratiques et apporter une aide aux victimes. Cette sensibilisation débute d'ailleurs dès le plus jeune âge par des actions menées par policiers et gendarmes auprès des élèves dans les écoles[2].

Soulignons également le groupement d'intérêt public (GIP) Cybermalveillance.gouv.fr, un dispositif directement issu de la Stratégie nationale de sécurité numérique présentée par le Premier ministre en 2015[3]. Ce dispositif apporte à tous citoyens, pme-pmi, collectivités, associations une réponse concrète au travers de fiches conseil, de guides de sensibilisation et de parcours victimes. Cybermalveillance.gouv.fr qui vient de fêter ses trois ans est unanimement reconnu pour son travail, d'autant plus exceptionnel au regard de ses moyens.
Ne doutons pas de la volonté de l'État de renforcer les moyens de ce dispositif.

Ses instances, déployées sur les territoires, pourraient certainement contribuer efficacement à développer la confiance et la sécurité numériques de nos collectivités. La Revue stratégique de cyberdéfense[4] publiée en 2018 par le Secrétariat Général de la Défense et de la Sécurité Nationale (SGDNS) évoque d'ailleurs cette nécessité de mutualisation des ressources au niveau territorial. Cette revue soulignait également la nécessité de développer une offre des produits et de services adaptée aux collectivités. Le Label ExpertCyber[5] initié par Cybermalveillance.gouv.fr à destination des prestataires de service de proximité s'inscrit pleinement dans cette logique. Dans le prolongement de cette action, et dans la continuité des produits qualifiés par l'ANSSI, le lancement dès 2021 d'un label pour les produits de sécurité adaptés aux besoins des collectivités serait pertinent.
Le Plan de relance engagé par le gouvernement est sans doute une opportunité à saisir pour agir en renforçant l'existant et en développant de nouvelles solutions pour les collectivités territoriales. Le directeur général de l'ANSSI a d'ailleurs évoqué cette possibilité pour développer l'action de Cybermalveillance.gouv.fr au profit des territoires lors d'une audition au Sénat en novembre dernier[6].

En amont de ces actions, l'État a depuis plus de 10 ans, élaboré une réglementation sur la sécurité numérique dont une partie concerne les collectivités.

L'ANSSI a publié à cet effet un guide utile sur l'essentiel de la réglementation pour les collectivités territoriales[7]. Le lecteur pourra constater que la France et l'Europe ont bâti un corpus réglementaire important, pouvant d'ailleurs parfois être déstabilisant pour les collectivités de petites tailles disposant de peu de moyens. Parmi ces réglementations, le règlement européen pour la protection des données (RGPD) a souvent occupé le devant de la scène, focalisant les moyens et les énergies, en reléguant au second plan les autres problématiques de sécurité numérique comme les rançongiciels, qui représentent aujourd'hui une menace majeure.

Mais comme le soulignent des élus, fonctionnaires territoriaux et représentants de l'État sur les territoires, lors des étapes du Tour de France de la Cybersécurité (TDFCyber) depuis 2018, la réglementation pour être pleinement utile doit avant toute chose être connue et comprise par ceux qui

doivent la mettre en œuvre. De plus, est c'est un point essentiel, la réglementation doit être accompagnée de politiques publiques efficaces et adaptées aux contraintes des territoires. Enfin, une évaluation des réglementations et politiques publiques est indispensable pour mesurer leur efficacité et s'assurer qu'elles s'inscrivent bien à une démarche d'amélioration continue et durable.
A titre d'exemple, la commande publique, dont une réforme a été mainte fois évoquée, une TVA réduite ou un dispositif d'accès au fonds de compensation de la TVA (FCTVA) pour les fournitures et prestations de sécurité numérique, pourraient constituer un formidable levier pour développer la confiance et la sécurité numériques des collectivités.
Sur ces sujets, l'État peut agir.

Enfin d'autres actions développées par des acteurs de confiance apportent aux collectivités des réponses parfois peu connues. Citons les travaux du Groupe La Poste, acteur historique et opérateur de service public, qui en plus des solutions et des services d'identité numérique propose des services[8] pour aider les collectivités dans leur transformation numérique. Citons également la Banque des Territoires qui a publié un guide pratique[9] pour une collectivité et un territoire numérique de confiance. Une initiative à saluer s'inscrivant dans cette logique constructive de soutien aux collectivités, plus que jamais nécessaire face au risque numérique.

En conclusion, le menace cyber touchant les collectivités territoriales n'est pas un phénomène nouveau mais les statistiques augmentent incontestablement. Nous devons apprendre à vivre avec cette nouvelle forme de menace. De la défiguration de sites web aux rançongiciels, en passant par les fuites de données, l'ensemble du panel des menaces cyber touche nos collectivités. Le sabotage d'infrastructures industrielles des collectivités (eau, énergie, traitement des déchets, transport), peu développé aujourd'hui en France, constitue un risque qu'il est indispensable de prendre en compte, à l'image de ce qui se passe dans d'autres pays, aux Etats-Unis et Israël par exemple.

Mais face à cette montée des menaces, retenons que des collectivités ont engagé une vraie démarche de sécurité numérique, ce qu'il faut saluer. Retenons aussi que l'État, au travers de plusieurs dispositifs, apporte son soutien à l'ensemble des acteurs.

De grands travaux restent toutefois à engager au niveau local et national. La perspective des prochaines élections sur les territoires et le plan de relance engagé par le gouvernement à la suite de la crise de la COVID19, constituent sans aucun doute des opportunités à saisir.

1 Chiffre mis en avant par la banque des territoires https://www.banquedesterritoires.fr/pour-une-cybersecurite-territoriale-efficace-la-banque-des-territoires-sengage
2 cf. le rapport du ministère de l'Intérieur sur l'état de la menace liée au numérique en 2019 https://www.interieur.gouv.fr/content/download/117535/942891/file/Rapport-Cybermenaces2019-HD-web-modifi%C3%A9.pdf
3 Objectif n° 2 - confiance numérique, vie privée, données personnelles, cybermalvaillance, de la stratégie nationale pour la sécurité du numérique : https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf
4 http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/
5 https://expertcyber.afnor.org/
6 http://videos.senat.fr/video.1797742_5fa25ae07cf94.plf-2021---audition-conjointe-de-m-stephane-bouillon-sgdsn-et-de-m-guillaume-poupard-directeur-?timecode=5873000
7 https://www.ssi.gouv.fr/uploads/2020/01/anssi-guide-securite_numerique_collectivites_territoriales-reglementation.pdf
8 cf. étude présentée lors du TDFCyber 2019 https://cybercercle.com/rcyberara-tdfcyber2019-archive/
9 https://www.banquedesterritoires.fr/guide-pratique-pour-une-collectivite-et-un-territoire-numerique-de-confiance