Cyberattaques contre les collectivités territoriales : le pire est-il à venir ?

Rémy Février Maître de Conférences HDR en Sciences de Gestion - Equipe Sécurité-Défense-Renseignement

Publié le 15 décembre 2022 – Mis à jour le 19 décembre 2022

Depuis le début de la crise du Covid-19 et notamment durant la période de confinement, on assiste à une augmentation sans précédent des cyberattaques touchant les collectivités territoriales françaises (régions, départements, communes, communautés de communes, etc.). Toutefois, ces dernières sont souvent occultées par celles qui affectent les établissements de santé du fait de leurs conséquences potentiellement dramatiques, à l'image de l'attaque qui a touché, début décembre, le centre hospitalier de Versailles, au Chesnay-Rocquencourt (Yvelines).

Cyberattaques contre les collectivités territoriales : le pire est-il à venir ?

Nos travaux sur la vulnérabilités des collectivités territoriales françaises face aux cyberattaques ont notamment été sanctionnés par la première (et seule à ce jour) thèse en sciences de gestion soutenue dès 2012 et donné lieu à plusieurs articles scientifiques ultérieurs. Ces travaux furent l'occasion d'appeler à la mise en place d'une politique publique nationale d'accompagnement des collectivités territoriales relativement à la nécessaire sécurisation de leurs systèmes d'information (SI), malheureusement sans grand succès.

Si nous aurions préféré avoir tort quant aux évolutions envisagées, force est de constater que le sujet est finalement apparu sur l'agenda médiatique depuis la crise du Covid pour ne plus la quitter depuis lors. Eu égard à la structuration territoriale française (45 205 collectivités locales en 2022), ces dernières revêtent une importance prépondérante, autant pour leur proximité directe avec les citoyens qu'en termes de services rendus. C'est vraisemblablement ce constat qui a amené de plus en plus de groupes de hackers à les choisir pour cibles.

Les cyberattaques menées demeurent pour le moment essentiellement liées à l'envoi de ransomwares (logiciels malveillants se diffusant à l'intérieur d'un système d'information et chiffrant l'ensemble des données accessibles) et visent un objectif exclusivement pécuniaire au travers de la demande d'une rançon dont le paiement préalable conditionne l'envoi (ou pas) d'un code de déchiffrement. Ce type d'offensive s'avère effectivement d'une efficacité redoutable en cas de sauvegarde non redondante.

Triple défi numérique

Appelant de nos vœux une véritable prise de conscience des enjeux liés à une mauvaise sécurité des SI, il nous semble impératif d'alerter sur d'autres types d'atteintes aux données des collectivités, d'autant plus dangereux selon nous qu'ils s'avèrent potentiellement cumulatifs.

À trop se focaliser sur les rançongiciels touchant leurs serveurs, on en vient à oublier que les collectivités territoriales se situant intrinsèquement à l'intersection de trois univers (politique, économique et sociétal), celles-ci relèvent quotidiennement trois défis numériques majeurs : l'administration électronique, l'e-démocratie et la dématérialisation des appels d'offres.

[*Près de 80 000 lecteurs font confiance à la newsletter de The Conversation pour mieux comprendre les grands enjeux du monde*. Abonnez-vous aujourd'hui]

Dépassant largement la mise à disposition des administrés de nouveaux moyens de communication, l'administration électronique, régulièrement plébiscitée par les Français depuis plusieurs années, est devenue un outil stratégique de service public. Et cet état de fait devint encore plus évident durant la période de confinement relative au Covid-19 : il est aisé d'imaginer l'impact politique et social qu'auraient engendré des cyberattaques privant des citoyens d'un moyen d'interaction devenu d'autant plus essentiel qu'ils se trouvaient dans l'incapacité de se déplacer pour effectuer la moindre démarche administrative. Il convient par conséquent de sécuriser les SI afférents afin d'assurer une continuité de service public en cas de crise majeure.

Le même problème se pose en ce qui concerne l'e-démocratie. Nous avons récemment mis en évidence l'existence d'une typologie des interactions entre la collectivité et ses administrés selon le support numérique utilisé : interaction forte (échanges directs entre les citoyens et les exécutifs territoriaux), modérée (enquête en ligne ou dialogue sur les réseaux sociaux) ou faible (remontée d'informations ponctuelles à l'initiative des administrés).

Le degré de gravité d'une cyberattaque touchant les SI d'e-démocratie sera donc directement corrélé au vecteur numérique : pertes ou vols potentiels d'informations à caractère personnel dans les deux premières hypothèses et perte de confiance dans tous les cas. Ici encore se pose la question de l'impact de telles attaques contre des outils précisément mis en place pour tenter de favoriser une meilleure participation à la vie publique de citoyens de plus en plus méfiants vis-à-vis des institutions démocratiques.

À cela s'ajoute enfin la possibilité que les SI dédiés aux appels d'offres des collectivités puissent également être ciblés. Que se soit en termes de fonctionnement ou d'investissement une collectivité, à l'image de la grande majorité des organisations, se trouve dans l'obligation de faire appel à des prestataires extérieurs.

La dématérialisation de ces procédures fut précisément menée pour permettre une meilleure fluidité dans la gestion des appels d'offres, ainsi que dans le souci de permettre de simplifier les procédures afin de permettre à des petites et moyennes entreprises (PME) de répondre à ceux-ci avec une chance raisonnable de succès. Une offensive numérique visant les échanges entre les soumissionnaires et la collectivité s'avérerait également lourde de conséquences, non seulement en matière économique mais également en termes de crédibilité intrinsèque.

Acteurs de la défense

Face à l'ensemble des défis précités, on peut espérer que le volet dédié au financement numérique des collectivités territoriales du plan gouvernemental « France Relance » permettra d'améliorer sensiblement la sécurisation des SI territoriaux. Pour autant, l'opportunité budgétaire ne fait pas tout, *a fortiori* lorsque les projets potentiellement finançables entrent immanquablement en compétition les uns avec les autres et que les capacités d'accompagnement financier d'origine étatique demeurent par nature limitées.

Or, il convient de conserver à l'esprit qu'en matière de sécurisation des SI, comme nous le mettions déjà en évidence dans le premier ouvrage dédié à cette problématique et paru dès 2014, l'une des conditions essentielles du succès, voire la principale d'entre elles, relève d'une volonté politique forte au sens ou l'impulsion doit venir directement des exécutifs territoriaux.

Notre expérience d'universitaire spécialiste du sujet et d'ancien élu d'une ville de plus de 100 000 habitants nous incite donc à préconiser la définition d'une véritable politique publique d'accompagnement des collectivités territoriales en matière de sécurisation de leurs SI. Et ce d'autant plus qu'à la lumière des enseignements tactiques issus du conflit ukrainien, on redécouvre la nécessité de renforcer la défense opérationnelle du territoire français dont les collectivités territoriales demeurent des parties prenantes essentielles.

Rémy Février, Maître de Conférences HDR en Sciences de Gestion - Equipe Sécurité-Défense-Renseignement, *Conservatoire national des arts et métiers (CNAM)*

Cet article est republié à partir de The Conversation sous licence Creative Commons. Lire l'article original.

| Numérique | Société

voir le site de l'équipe Sécurité & Défense

https://esd.cnam.fr/cyberattaques-contre-les-collectivites-territoriales-le-pire-est-il-a-venir--1380848.kjsp?RH=1588237