CYBERATTAQUES

Le virus numérique circule (aussi) activement dans les collectivités

Elles font de plus en plus la une de l'actualité. Marseille, Angers, La Rochelle… le nombre de cyberattaques contre les collectivités locales a bondi de 50 % en 2020. Peuvent-elles contrarier la transition numérique de nos sociétés, porteuse d'espérances pour faciliter l'érection d'un monde plus soucieux des ressources naturelles ? La réponse publique tente de s'organiser.

Stéphane Menu

Un mauvais clic et un monde s'effondre… Domnin Rauscher, DGS de la métropole Aix-Marseille-Provence, avait évoqué le sujet dans nos colonnes lorsque la collectivité fut victime, en mars 2020, au début du premier confinement, de l'appétit vorace d'un logiciel malveillant. « Nos serveurs ont été cryptés à hauteur de 90 % contre une demande de rançon. La police judiciaire a pris le relais sur ce dossier et la métropole a porté plainte. Il faut donc reconstruire un système complet. » Un chantier d'un mois et demi pour sortir la tête de l'eau…

En tout, 159 collectivités locales ont officiellement signalé une cyberattaque sur le portail Cybermalveillance.gouv.fr

La métropole marseillaise ne représente pas un cas isolé, tant s'en faut. En janvier 2021, Angers, La Rochelle et Annecy ont subi des tentatives d'extorsion de fonds suite à l'introduction d'un logiciel malveillant dans le système informatique des mairies. Toutes les tailles de collectivité sont touchées. Vincennes et Alfortville, en banlieue parisienne, ont été ciblées en 2020, mais aussi la petite commune d'Aulnoye-Aymeries (9 000 habitants) dans le Nord. En tout, 159 collectivités locales ont officiellement signalé une cyberattaque auprès du groupement d'intérêt public Acyma et son portail Cybermalveillance.gouv.fr. Une hausse de 50 % par rapport aux 109 cyberattaques recensées en 2019.

Le coût financier du blocage

Le logiciel rançonneur, autrement dénommé « ransomware », s'introduit dans le système informatique de sa cible, brouille le maximum de données disponibles et exige une rançon pour les rendre de nouveau accessibles. « Une grande majorité de victimes ne paie pas. Mais beaucoup sont confrontées au dilemme d'ignorer la menace financière et de voir ainsi disparaître des informations ou des souvenirs capitaux, des photos de ses enfants, des livres, des données personnelles, etc. Dans ce cas, elles cèdent au chantage », explique Loïc Guézo, secrétaire général du Clusif (Club de la sécurité informatif français, réunissant entreprises privées et secteur public depuis une trentaine d'années, lire en encadré).

Bloqué, le système informatique stoppe net le quotidien de la collec-

tivité. « Plus d'actes civils, plus de documents d'urbanisme, plus rien pour établir la moindre relation avec les usagers », confirme Loïc Guézo.

Les autorités conseillent de ne pas payer la rançon, mais l'arrêt du fonctionnement informatique peut occasionner de lourdes factures

Si les autorités conseillent aux victimes de ne pas payer la rançon, cet arrêt du fonctionnement informatique et les frais à consentir pour lui redonner vie peuvent occasionner de lourdes factures, comme ce fut le cas en 2019 pour la ville du Maryland : 18 millions de dollars pour la remise en route puis la sécurisation du système informatique.

Plus de télétravail équivaut à plus de risques

Pour Pascal Le Digol, directeur en France de WatchGuard, un éditeur de logiciels de sécurité qui travaille avec plusieurs grandes communes françaises, interrogé par Les Échos, la recrudescence des attaques s'explique par leur industrialisation. « En ce moment, il y en a pour tout le monde, mais les municipalités peuvent moins facilement cacher une attaque que les PME. » Le recours au télétravail, lié à la crise sanitaire, est de ce fait propice aux agissements des criminels, les mises à jour de sécurité ne se faisant plus aussi automatiquement que lorsque, sur place, les responsables informaticiens apportent les éclairages nécessaires. Les agents sont donc de plus en plus livrés à eux-mêmes.

Dans la nuit du 27 au 28 décembre 2020, la totalité des données de l'agglomération d'Annecy ont été rendues inopérantes

Une menace pour la transition numérique ?

Dans son « Panorama de la Cybersécurité 2020 », publié le 26 janvier 2021, le Clusif recense les collectivités victimes d'un rançongiciel. Panorama illustré d'exemples très précis donnant froid dans le dos. Dans la nuit du 27 au 28 décembre ›››

© PAVIOT TRISTAN

Loïc Guézo, secrétaire général du Clusif

« Mieux former les agents au risque »

Comment les collectivités font-elles face au risque de cybercriminalité ?

Le Clusif est une association qui réunit 1000 membres environ, depuis une trentaine d'années. On y trouve à la fois des offreurs de services informatiques et des utilisateurs, qu'ils soient privés ou publics. Nous avons créé un groupe de travail sur les collectivités territoriales. Dans les grandes entreprises du CAC 40, l'enjeu est si important qu'un directeur de la cybersécurité est embauché, disposant de moyens importants, matériels et humains, pour éviter à l'entreprise des mésaventures. Dans les collectivités, les dispositifs sont moins importants, même si la fonction RSSI (Ndlr, le responsable de la sécurité des systèmes d'information – en anglais, Chief information security officer ou Ciso) est de plus en plus transverse. D'ailleurs, les collectivités qui s'en sortent le mieux sont celles qui ont des niveaux d'expertise élevés de la protection de leur réseau. Aujourd'hui, la capacité de réponse est proportionnelle à la taille de la collectivité.

Comment se déroule une attaque cybercriminelle ?

C'est un rançongiciel qui cherche à intégrer le système informatique. Prenons le cas d'une grosse collectivité, avec des milliers d'agents. Il suffit que le DGS ou le gardien d'un équipement clique sur un mauvais lien pour que le logiciel malveillant fasse des dégâts. Il n'y a pas de protection à 100 %. Les portes blindées sont de plus en plus sophistiquées, les alarmes de plus en plus perfectionnées, pour autant, il existe toujours des cambriolages ! Le fishing d'anarque s'améliore de plus en plus, ils sont de plus en plus individualisés. Il y a peu, les fautes d'orthographe ou encore les logos mal déchargés pouvaient susciter un doute. Aujourd'hui, le malfrat sait sur quel sujet vous travaillez, ses mails sont plus élaborés et comme nous lisons tous des dizaines de mails par jour, le risque du clic fatal est plus élevé. Il faut donc que les collectivités investissent sur la formation et notamment que les agents se demandent chaque fois qu'ils ouvrent un mail s'il est normal qu'il l'ait reçu et s'ils doivent impérativement le traiter. Les spams font un premier travail d'élagage mais certains mails passent cette protection parce que les malfrats ont su innover.

A-t-on une idée de l'ampleur du phénomène ?

Avec la crise du Covid-19 et donc l'isolement numérique des agents, les attaques se sont multipliées. Elles ont été multipliées par 4 de 2019 à 2020, aux dires de l'Agence nationale des systèmes d'information.

La riposte s'organise-t-elle ?

Depuis six ans, Emotet a infecté des centaines de milliers d'ordinateurs dans le monde. Les pirates vendaient ensuite l'accès à ces machines compromises, ouvrant la voie à des cyberattaques par rançongiciel. Il a été démantelé en début d'année grâce à une opération internationale d'envergure. C'est sans doute un tournant dans la lutte contre la cybercriminalité mais les malfrats resteront toujours inventifs et sauront se renouveler, notamment dans des pays où l'espionnage informatique est une arme diplomatique très ancrée.

›››

2020, la totalité des données de l'agglomération d'Annecy a été rendue inopérante. Pendant plusieurs jours, les agents n'ont plus eu accès à internet et à leurs mails pros. Scénario similaire à l'agglo de La Rochelle. Attaqués, les réseaux informatiques de la collectivité ont été fermés. Début janvier, la presse locale révélait que le groupe Netwalker avait revendiqué sur son blog la cyberattaque. Preuves à l'appui puisque les pirates auraient transmis sur des réseaux privés et semi-privés des données appartenant à différents services de la ville. Marseille et sa métropole, ainsi que Martigues, dans les Bouches-du-Rhône, ont ramé pour rendre de nouveau opérants près de 300 ordinateurs.

Des informaticiens mieux formés à ce risque ont été intégrés et prennent part au plus près aux réunions de direction

Face à l'accentuation de ce risque, de nombreuses collectivités ont réagi. Des informaticiens mieux formés à ce risque ont été intégrés et prennent part au plus près aux réunions de direction (les fameux Codir et autres Comex) afin de rappeler en permanence aux cadres la portée des risques encourus. Dans le même temps, police et gendarmerie nationales s'adaptent de mieux en mieux au péril, même s'ils ne peuvent répondre au flux des plaintes, en majorité déposées par des particuliers peu au fait des subtilités numériques et tombant trop facilement dans les panneaux tendus par des criminels aguerris. À l'heure où la transition numérique est considérée comme l'un des vecteurs essentiels pour basculer dans un monde moins énergivore et plus soucieux de la préservation des ressources, la lutte contre la cybercriminalité s'impose comme une urgence. ◆

AU FOND DU TROU

Les élus dans le piège de l'exécution provisoire

« En décidant de réprimer sévèrement le délit de détournement de fonds publics commis par un élu, les législateurs – qui sont eux-mêmes des élus – ont de fait donné aux magistrats cette capacité de peser sur le processus électoral que certains leur reprochent aujourd'hui : la peine d'inéligibilité est obligatoire et son exécution provisoire possible, suivant le degré d'atteinte à la probité », déclare dans Sud-Ouest Guillaume Beaussonie, professeur de droit pénal à l'université de Toulouse (Haute-Garonne).

Pourtant, la loi votée en 2017 n'a pas connu beaucoup d'applications depuis, notamment quant à la possibilité d'une exécution provisoire dès la première instance, sans attendre l'épuisement de tous les recours. Certes, quelques « grands » élus avaient été sanctionnés de cette façon comme Gaston Flosse en Polynésie, et Patrick Balkany à Levallois-Perret (Hauts-de-Seine), mais ils restaient rares. Désormais, cette mesure est utilisée partout en France, aussi bien dans le Grand Est (Moyeuvre-Grande en Moselle, où le maire a été condamné à cinq ans d'inéligibilité en janvier 2021 pour des violences conjugales sur son ex-épouse) que dans le Grand Ouest (Bassussarry dans les Pyrénées-Atlantiques, Gaillac dans le Tarn, et Montauban dans le Tarn-et-Garonne, ces six derniers mois) pour détournement de fonds ou prise illégale d'intérêts.

Lors du prononcé du délibéré condamnant la maire de Montauban, Brigitte Barrège, le président du tribunal correctionnel de Toulouse a expliqué sa position en soulignant qu'« en tant qu'élue de la population française au suffrage universel, elle se devait de respecter trois obligations : probité, transparence et exemplarité ».

Son collègue d'Albi (Tarn), avait été encore plus précis le 17 septembre 2020 à l'encontre de l'ancien maire de Gaillac, Patrice Gausserand, condamné à dix mois de prison avec sursis et cinq ans d'inéligibilité pour prise illégale d'intérêt et corruption passive. « Ce type d'infraction participe de manière importante à la défiance de plus en plus grande que l'opinion publique exprime à l'encontre des élus publics, son absence de remise en cause personnelle, ne serait-ce que sur la gestion des conflits d'intérêts en cause, impose une peine d'inéligibilité avec exécution provisoire pour permettre l'élection d'un maire intègre dans cette ville du Tarn ».

Les faits reprochés à la maire de Montauban méritent une mention particulière : le détournement de fonds publics pour laquelle elle est condamnée en première instance (le procureur a parlé d'un dévoiement dans l'utilisation de fonds publics) tient au fait que son chargé de communication avait été payé pour écrire des articles élogieux à son égard dans une publication locale. Licencié de son poste dans le cadre d'une procédure disciplinaire, il s'était confié à la justice à ce sujet…

Le résultat est toujours le même : dès notification du préfet, faite à la demande du procureur, l'élu perd l'ensemble de ses mandats.