ASSEMBLÉE NATIONALE

16ème legislature

Question N° : 7480	De **M. Karl Olive** (Renaissance - Yvelines)	**Question écrite**

Ministère interrogé > Transition numérique et télécommunications	**Ministère attributaire** > Première ministre

Rubrique >collectivités territoriales	**Tête d'analyse** >Appui aux collectivités contre les cyberattaques	**Analyse** > Appui aux collectivités contre les cyberattaques.

Question publiée au JO le : **25/04/2023**
Réponse publiée au JO le : **27/06/2023** page : **5785**
Date de changement d'attribution : **23/05/2023**

Texte de la question

M. Karl Olive interroge M. le ministre délégué auprès du ministre de l'économie, des finances et de la souveraineté industrielle et numérique, chargé de la transition numérique et des télécommunications, sur la progression des violations de données personnelles qui ciblent les collectivités. Les collectivités territoriales sont fréquemment la cible de cyberattaques : 20 % des attaques réalisées en 2021, année marquée selon l'ANSSI par la professionnalisation des acteurs malveillants et la multiplication des incidents. Soit plus de 250 intrusions avérées dans les systèmes d'information des collectivités, avec une hausse de 37 % par rapport à 2020. Cela pose un double problème : d'une part les collectivités ne disposent pas des fonds nécessaires ni pour payer les rançons, ni pour investir dans de nouveaux logiciels de sécurité plus efficaces et d'autre part, dans certains cas, les données personnelles des usagers peuvent être mises en ligne par les pirates voire utilisées à des fins détournées. Mme la Première ministre soulignait dans sa réponse à la question écrite n° 22781 que les conséquences de ces attaques sont dangereuses pour le bon fonctionnement des services publics, notamment en matière de transports publics, pour la gestation des prestations sociales ou la bonne tenue de l'état civil. Pour pallier l'accroissement continu de ces risques de criminalité (augmentation de 80 % lors du premier trimestre 2022 par rapport à l'année précédente), des mesures de sécurisation ont déjà été mises en place, que les collectivités sont sommées de respecter. De plus, l'Agence nationale de la sécurité des systèmes d'information (ANSSI), en collaboration avec l'Association des maires de France (AMF), a publié un guide de mise en œuvre d'une démarche de cybersécurité. En outre, dans le cadre du plan France Relance lancé en septembre 2020, dont le volet sécurité a été doté d'un fonds de 136 millions d'euros, un parcours de cybersécurité est proposé aux collectivités volontaires afin de renforcer leur sécurité. La démarche introduite par France Relance est fondée sur l'accompagnement des collectivités dans le but d'élever substantiellement le niveau de sécurité numérique en apportant des compétences *via* des prestataires de cybersécurité, en encadrant les parcours sur le plan technique, en subventionnant les collectivités à hauteur de 90 000 euros. Toutefois, aujourd'hui encore, les nombreuses cyberattaques dirigées contre des collectivités sont la preuve que des écueils subsistent. En effet, le 1er mars 2023, la mairie de Lille a été victime d'une cyberattaque dans laquelle des données personnelles ont été volées dans les serveurs et dont les conséquences sont à nouveau critiques pour la commune : la billetterie pour de nombreux services de la ville est restée inactive de nombreux jours, les terminaux de paiement électronique étaient inutilisables. Aussi, M. le député souhaite connaître les mesures envisagées par le ministère pour pallier l'augmentation exponentielle des cyberattaques contre les collectivités. Si le bilan de 2021 du plan France Relance est positif, qu'en est-il pour 2022 ? Comment le ministère compte-t-il accentuer ses démarches afin d'inciter les collectivités à prendre la mesure de ces dangers ? Enfin, il lui

demande ce que peut faire l'État face pour effacer les données piratées déjà présentes sur le *dark web*.

Texte de la réponse

Les collectivités territoriales font l'objet d'une attention particulièrement soutenue de la part de l'Agence nationale de sécurité des systèmes d'information (ANSSI), en raison de leur exposition particulière au risque de cyberattaques. Cette exposition tient notamment à des processus de numérisation volontaristes et une importante offre de services numériques à la population administrée. Afin de concilier au mieux les impératifs de cette numérisation avec ceux de la cybersécurité, un important travail de sensibilisation a été engagé en direction des élus et cadres territoriaux, conjointement par l'Association des départements de France et l'ANSSI. Ainsi, des actions ont été conduites au début de l'année 2023 pour tirer les premiers enseignements des attaques récemment menées contre certains conseils départementaux et pour prodiguer des conseils destinés à améliorer la cybersécurité. De surcroît, divers outils de cybersécurité sont mis à disposition par l'ANSSI. C'est le cas du service de protection des « annuaires » Active Directory Security (ADS), qui contiennent de nombreuses informations utiles aux attaquants, ou de la démarche de cartographie de la surface d'exposition sur Internet d'un système, au travers du service SILENE. Afin de compléter cette offre, l'ANSSI met à disposition depuis la fin de l'année 2022 l'outil MonServiceSécurisé qui permet de sécuriser et d'homologuer gratuitement et rapidement les services publics en ligne. Un outil de diagnostic dénommé MonAideCyber est actuellement en phase d'évaluation. Il viendra compléter le dispostif dans le courant de l'année 2023. Au-delà, l'ANSSI accompagne très directement les collectivités. Depuis le mois d'octobre 2022, le dispositif territorial de l'agence est complet, avec au moins un délégué de l'Agence par région et un délégué pour les outre-mer. De nombreuses actions de sensibilisation décentralisées, sont menées, souvent en étroite collaboration avec le commandement de la gendarmerie nationale dans le cyberespace et le groupement d'intérêt public ACYMA (cybermalveillance.gouv.fr). Elles sont rendues possibles par les liens étroits tissés avec les associations d'élus (AMF, ADF, ARF…). Le plan de relance a également permis de financer un effort historique en faveur de la sécurité des systèmes d'information des collectivités territoriale, à hauteur de 100 millions d'euros sur les 176 millions d'euros dont bénéficiait la totalité du volet consacré à la cybersécurité. Ce très important effort budgétaire consenti par le Gouvernement a permis de financer trois types d'actions. Premièrement, un dispositif de « parcours cyber » visant à accompagner une amélioration des compétences en matière de cybersécurité. Ces parcours s'appuient sur des prestataires de cybersécurité, déclinant une méthodologie fixée par l'ANSSI. Ces dispositifs permettent de disposer d'une évaluation de la sécurité des systèmes d'information et d'un soutien pour les protéger concrètement et de manière adaptée aux enjeux et au niveau de menace. Deuxièmement, des appels à projet ont permis de sélectionner des « solutions » de sécurité, permettant notamment aux plus petites collectivités de s'équiper, alors qu'elles ne disposent pas nécessairement des budgets ou compétences pour réaliser les études préalables ou financer ces acquisitions. Troisièmement, le plan a permis de soutenir la création de centres régionaux de réponse à incident cyber (CSIRT régionaux), destinés à fournir leur aide aux structures de taille intermédiaire (entreprises, collectivités, associations…) en cas d'attaque. Environ 750 collectivités territoriales ont bénéficié d'un accompagnement au titre du plan de relance. Les premiers enseignements tirés de ces parcours de cybersécurité confirment le fort intérêt manifesté pour ce dispositif mais aussi la forte implication de la gouvernance des collectivités concernées dans le succès de ces démarches. Cette implication constitue un facteur décisif de succès pour l'initiation d'une démarche durable de maitrise du risque numérique. Au-delà du plan de relance, les efforts se poursuivent. Le 16 novembre 2022, le ministre délégué chargé de la transition numérique et des télécommunications a annoncé plusieurs mesures en faveur de la cybersécurité des collectivités territoriales. Dans ce cadre, en 2023, l'ANSSI mène plusieurs actions parmi lesquelles un élargissement des parcours de cybersécurité à de nouveaux bénéficiaires, la prolongation des parcours préalablement entamés par des bénéficiaires apparaissant comme particulièrement sensibles et le soutien au développement et au déploiement d'outils destinés aux collectivités territoriales, pour permettre notamment une sécurisation simplifiée et mutualisée de certains services. Ce soutien porte sur la transmission d'expertise par l'ANSSI à d'autres administrations, mais peut aussi se matérialiser par des délégations de gestion.