ASSEMBLÉE NATIONALE

16ème legislature

Question N° : 3371	De **Mme Patricia Lemoine** (Renaissance - Seine-et-Marne)	**Question écrite**

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

Rubrique >numérique	**Tête d'analyse** >Cyberattaques contre les collectivités territoriales et structures publiques	**Analyse** > Cyberattaques contre les collectivités territoriales et structures publiques.

Question publiée au JO le : **22/11/2022**
Réponse publiée au JO le : **21/02/2023** page : **1706**
Date de changement d'attribution : **20/12/2022**

Texte de la question

Mme Patricia Lemoine 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 les récentes cyberattaques perpétrées à l'encontre de collectivités territoriales telles que le département de Seine-et-Marne. Alors que le département de Seine-Maritime a fait l'objet d'une cyberattaque le 10 octobre 2022 ayant pour conséquence l'arrêt de nombreux services publics, c'est le département de Seine-et-Marne qui cette fois a été visé le 6 novembre 2022 par une attaque de grande ampleur. Ce sont ainsi 5 000 agents territoriaux qui ont été impactés par cette attaque. Si des solutions ont été trouvées pour assurer la continuité des missions de service public (MDS, PAT, MDPH, PMI), l'activité normale du département ne reprendra que sous un délai de six semaines. Depuis plusieurs années, ces attaques se multiplient contre les structures publiques françaises, encore trop souvent peu équipées pour y faire face. Ce phénomène est d'autant plus inquiétant qu'il a en outre visé dernièrement l'hôpital de Corbeil-Essonnes, les pirates informatiques réclamant le paiement d'une rançon de plusieurs millions d'euros. Ces cyberattaques, qui impactent sérieusement le fonctionnement des services publics mais également mettent en danger des informations sensibles et les informations personnelles des administrés, risquent de se multiplier dans un contexte de guerre en Europe, certaines puissances étrangères ayant massivement recourt à ces méthodes. Elle lui demande donc quelles mesures sont actuellement envisagées pour renforcer la sécurité informatique des collectivités et structures publiques face à ces attaques qui se multiplieront à l'avenir, afin de protéger les données des Français et d'assurer le bon fonctionnement des services publics.

Texte de la réponse

La numérisation des services offerts au public accroît la vulnérabilité des collectivités territoriales face au risque de cyberattaques. Parmi les entités publiques, elles font partie des cibles les plus exposées. Le Gouvernement considère cette situation comme particulièrement préoccupante. L'Agence nationale de sécurité des systèmes d'information (ANSSI) y accorde donc une attention particulière. Dans la mesure où les collectivités ne sont ni des administrations sous l'autorité des ministères, ni des établissements publics, les efforts de l'ANSSI portent particulièrement sur l'assistance à l'amélioration de la gouvernance de la cybersécurité au sein de chaque collectivité et leur accompagnement, technique, méthodologique et même financier au travers du plan de relance.

Le travail d'amélioration de la gouvernance s'insère dans une méthodologie qui requiert au moins trois exigences. La première est la sensibilisation des élus et décideurs pour leur permettre de prendre pleinement conscience de l'acuité du risque de cyberattaques et du niveau idoine des moyens à consentir à sa prévention, voire à son traitement. La deuxième est la diffusion et la pédagogie des outils, guides et référentiels adéquats, puis leur utilisation effective. De cette mise en œuvre résulte l'augmentation du niveau de cybersécurité. La troisième exigence est la mise en œuvre d'un accompagnement local pour orienter, conseiller et soutenir. À des fins de sensibilisation des acteurs concernés, l'ANSSI a développé de nombreux partenariats avec l'association des maires de France, l'association des départements de France, Régions de France, l'association DECLIC regroupant les opérateurs de service numérique… A titre d'exemple, un partenariat fructueux existe entre l'ANSSI et l'association des départements de France dans le but de favoriser la prise de conscience des élus et des cadres territoriaux. Au mois de janvier 2023, des rencontres ont été organisées pour tirer profit des premiers enseignements des attaques récentes menées contre certains conseils départementaux et pour partager largement les conseils de l'Agence sur la sécurisation numérique. Parallèlement, l'ANSSI met à la disposition de tous des outils dont l'usage est indispensable. Parmi ces outils, on peut mentionner le service Active Directory Security-ADS permettant la sécurisation des annuaires ou le service SILENE pour la cartographie de la surface d'exposition sur Internet. Ces outils, accessibles aux collectivités territoriales sur simple inscription, sont gratuits et disponibles autant que de besoin pour assurer le suivi de la cybersécurité dans le temps et en fonction des actions menées. L'ANSSI élargit la gamme de ces outils en mettant à disposition depuis la fin de l'année 2022 l'outil MonServiceSecurise.beta.gouv.fr qui fournit les conseils techniques adaptés pour la sécurisation des services publics accessibles en ligne et simplifie la démarche d'homologation. Un outil de diagnostic, actuellement en évaluation, MonAideCyber.beta.gouv.fr, élaboré en collaboration avec la gendarmerie nationale et cybermalveillance.gouv.fr, viendra compléter ce dispositif durant l'année 2023. L'ANSSI accompagne aussi les collectivités territoriales, tout comme les entreprises, localement. Depuis octobre 2022, le dispositif territorial de l'agence est complètement déployé, avec au moins un délégué par région et un délégué pour les outre-mer. De très nombreuses actions de sensibilisation peuvent être menées, souvent en étroite collaboration avec le commandement de la gendarmerie nationale dans le cyberespace (ComCyberGend) et le GIP ACYMA-cybermalveillance.gouv.fr. Parmi les efforts les plus significatifs consentis par le Gouvernement, il convient de rappeler le volet « cybersécurité » du plan d'investissement France Relance. Piloté par l'ANSSI, ce plan vise à augmenter durablement le niveau de cybersécurité de l'État et des services publics. Ce plan, doté de 176 millions d'euros sur la période 2021-2022, a permis de déployer plusieurs dispositifs au profit de la cybersécurité des services publics et d'augmenter concrètement leur niveau de sécurité. Les collectivités territoriales ont été les premières bénéficiaires de ce plan, à hauteur de 94 M€. Ces crédits ont financé des parcours de cybersécurité qui comprennent à la fois une évaluation de leur niveau de cybersécurité de la collectivité, l'établissement d'une feuille de route efficace et pragmatique et le déploiement des solutions indispensables à une élévation rapide et concrète de leur niveau de cybersécurité. L'accompagnement dont bénéficient les collectivités revêt trois aspects : il est financier, sous la forme d'une subvention de 90 000 euros ; méthodologique, avec une démarche conçue par l'ANSSI ; humain, grâce à un suivi personnalisé par des prestataires spécialisés. Plus de 700 collectivités ont ainsi pu être accompagnées en deux ans, pour disposer d'une évaluation de la sécurité de leurs systèmes d'information et d'un soutien pour les protéger concrètement et de manière adaptée. Ils ont aussi financé des appels à projet de déploiement de produits de sécurité. Ce mécanisme permet de financer l'installation à grande échelle de solutions efficaces de sécurité dans les collectivités territoriales, en recourant à des opérateurs de services numériques. Ces appels à projets contribuent ainsi au déploiement et à la sécurisation, par ces opérateurs, de solutions informatiques mutualisées au profit des plus petites communes ne disposant pas de compétences informatiques, ni de budgets permettant de financer un tel effort. Ils permettent notamment de subventionner les licences globales de certaines applications ou produits de sécurité essentiels (antivirus, pare feu, protection de messagerie). Au travers de 27 projets, un potentiel de 11 000 communes est ainsi couvert pour un montant de 5,2 M€. Le plan d'investissement a aussi permis de soutenir la création de centres régionaux de réponse aux incidents de cybersécurité. Ces centres aident les structures de taille intermédiaire (entreprises, collectivités, associations…) à faire face en cas d'attaque. Sur les treize régions métropolitaines, douze sont engagées dans la démarche et ont ainsi bénéficié d'une subvention d'1 million d'euros chacune permettant le fonctionnement du centre pendant 3 ans et d'un programme d'incubation, au sein de l'ANSSI

et du CERT-FR, pour leur assurer une mise en route rapide. Deux centres sont aujourd'hui en service. Les autres seront opérationnels en 2023. Un effort particulier a été consenti au bénéfice des collectivités d'outre-mer à travers la création de centres de ressources en cybersécurité visant à faire émerger, par zone géographique, les compétences nécessaires à l'émergence d'une cybersécurité locale. Cette émergence passe par un travail de sensibilisation, de mises en relation et d'animation d'un écosystème constitué d'offreurs, de demandeurs et de l'ensemble des acteurs et parties prenantes du domaine.