ASSEMBLÉE NATIONALE

16ème legislature

Question N° : 3372	De **M. Frédéric Valletoux** (Horizons et apparentés - Seine-et-Marne)	**Question écrite**
Ministère interrogé > Transition numérique et télécommunications	**Ministère attributaire** > Première ministre	
Rubrique >numérique	**Tête d'analyse** >Protection des collectivités territoriales face aux cyberattaques	**Analyse** > Protection des collectivités territoriales face aux cyberattaques.
Question publiée au JO le : **22/11/2022** Réponse publiée au JO le : **21/02/2023** page : **1707** Date de changement d'attribution : **20/12/2022** Date de signalement : **14/02/2023**		

Texte de la question

M. Frédéric Valletoux appelle l'attention de 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 sécurité numérique des collectivités territoriales. Les questions de cybersécurité constituent une préoccupation grandissante à mesure que le numérique pénètre de plus en plus dans les vies. En effet, compte tenu du déploiement important du télétravail depuis la crise sanitaire, et de la numérisation croissante des services aux usagers, la réorganisation de la protection cyber des collectivités est nécessaire. Selon le rapport d'activité 2021 du site *Cybermalveillance.gouv.fr*, basé sur une étude réalisée à la fin de la même année, sur « la cybersécurité dans les collectivités de moins de 3 500 habitants », 2/3 des publics (maires, adjoints, agents, DGS) n'ont pas été sensibilisés à la sécurité numérique et 57 % des responsables informatiques interrogés ne sont pas formés à la sécurité numérique. Cela affecte directement la continuité du service public qui est propre aux administrations françaises et qui recouvre un large champ de mission, de la cantine scolaire aux réseaux de transport en passant par l'action sociale. Les petites ou moyennes communes ne sont donc pas suffisamment préparées à ce type d'attaque et les conséquences peuvent être irréversibles. Les territoires à plus grande échelle ne sont pas non plus épargnés : à titre d'exemple, le département de Seine-et-Marne est victime depuis le 6 novembre 2022 d'une attaque informatique inédite et une rançon au montant exorbitant est exigée par les *hackers*. La fuite, le vol ou la perte de données personnelles des habitants du territoire est à prendre en considération, et ce ne serait pas le premier cas de figure : 5 mois après la cyberattaque du Grand Annecy, en mai 2021, des tests covid-19 ou coordonnées personnelles de plus de 1 000 agents de la communauté d'agglomération ont été diffusés sur le *web* alternatif. Alors que le Gouvernement avait mobilisé, en février 2021, 136 millions d'euros dans le cadre du volet cybersécurité du plan France Relance qui visait chaque commune quelle que soit sa taille, ces mesures semblent insuffisantes. Il paraît ainsi important de réfléchir davantage sur la sensibilisation et sur la formation à la cybersécurité, et sur les moyens à disposition des collectivités pour lutter contre ces actes de malveillance. En conséquence, il souhaiterait connaître les pistes envisagées par le Gouvernement pour renforcer la sécurité numérique des collectivités et anticiper la survenance de cyberattaques.

Texte de la réponse

ASSEMBLÉE NATIONALE

Dans son Panorama de la cybermenace 2022 publié au mois de février 2023, l'Agence nationale de sécurité des systèmes d'information (ANSSI) fait apparaître que, malgré une année marquée par le conflit russo-ukrainien et ses effets dans le cyberespace, les tendances identifiées en 2021 se sont confirmées en 2022. Le niveau général de la cybermenace se maintient avec 831 intrusions avérées contre 1082 en 2021. Celle légère diminution ne saurait être interprétée comme une baisse du niveau de la menace. En effet, la diminution de l'activité de cyber-rançonnage des opérateurs régulés publics et privés observée par l'ANSSI traduit avant tout une bascule d'effort des attaquants. Les activités criminelles visent désormais prioritairement des entités moins bien protégées. Parallèlement les malfaiteurs améliorent constamment leurs capacités d'attaque, utilisées à des fins crapuleuses, d'espionnage et de déstabilisation. Cette amélioration s'illustre en particulier dans le ciblage des accès aux réseaux des victimes les plus discrets et pérennes, via des équipements périphériques. Ce ciblage périphérique se décline également dans le type d'entités attaquées et confirme l'intérêt des attaquants pour les prestataires, les fournisseurs, les sous-traitants, les organismes de tutelle et l'écosystème plus large de leurs cibles finales. La convergence des outils et des techniques des différents types d'attaquants se poursuit également en 2022 et continue de poser des difficultés de caractérisation de la menace. L'utilisation de rançongiciels d'origine crapuleuse par des services gouvernementaux illustre une porosité déjà identifiée en 2021. Dans ce contexte corrosif, il convient de maintenir ou intensifier l'ensemble des efforts de rehaussement du niveau de cybersécurité des entités publiques, parmi lesquelles les collectivités et les établissements hospitaliers. S'agissant des établissements hospitaliers, un important travail est en cours, à la demande de la Première ministre, sous l'égide du ministre de la santé et avec le concours de l'ANSSI. S'agissant des collectivités territoriales, beaucoup a été fait récemment grâce aux crédits 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 ; il est méthodologique, avec une démarche conçue par l'ANSSI ; il a une dimension humaine, 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.