ASSEMBLÉE NATIONALE

15ème legislature

Question N° : 37235	De **M. Éric Diard** (Les Républicains - Bouches-du-Rhône)	**Question écrite**

Ministère interrogé > Transition numérique et communications électroniques	**Ministère attributaire** > Première ministre

Rubrique >Internet	**Tête d'analyse** >Cyberattaques contre les PME, administrations et hôpitaux français	**Analyse** > Cyberattaques contre les PME, administrations et hôpitaux français.

Question publiée au JO le : **16/03/2021**
Réponse publiée au JO le : **21/06/2022** page : **3361**
Date de changement d'attribution : **17/05/2022**

Texte de la question

M. Éric Diard alerte M. le secrétaire d'État auprès des ministres de l'économie, des finances et de la relance, et de la cohésion des territoires et des relations avec les collectivités territoriales, chargé de la transition numérique et des communications électroniques, sur les cyberattaques qui se multiplient à l'encontre des administrations et entreprises françaises. Déjà depuis plusieurs mois, les pirates informatiques lancent des attaques dans un but lucratif à l'encontre d'entreprises françaises à l'aide de « rançongiciels », qui menacent les victimes de la destruction de leurs données numériques si elles ne paient pas une rançon avant un certain temps. La plupart des entreprises visées étant des PME, nombreuses sont celles pour qui ces attaques constituent un coup dur pour leurs finances et peuvent avoir des conséquences allant jusqu'au dépôt de bilan. La situation s'est aggravée jusqu'à devenir particulièrement alarmante quand les pirates informatiques ont fait des hôpitaux leurs cibles privilégiées, car ces derniers sont sous tension depuis maintenant un an en raison de la crise sanitaire que l'on traverse, ne leur laissant pas d'autre choix que de payer les sommes exigées. Il lui demande ainsi quelles mesures le Gouvernement entend prendre pour protéger la France face à cette menace numérique qui devient chaque jour de plus en plus dangereuse pour le système de santé et la sécurité des Français les plus vulnérables.

Texte de la réponse

De façon générale, la cybermenace croît structurellement sans qu'il soit possible d'imaginer une amélioration de la conjoncture à terme prévisible. Au contraire, la poursuite de la numérisation des usages professionnels, administratifs ou de vie courante laisse augurer du caractère pérenne de cette menace. S'agissant de la menace cybercriminelle et à l'exclusion des activités d'espionnage ou de déstabilisation, elle vise prioritairement des opérateurs à la fois vulnérables et dont l'exposition médiatique serait importante en cas d'interruption d'activité. Tant les collectivités territoriales que les établissements hospitaliers présentent ces caractéristiques et sont donc particulièrement attaqués, quand bien même ils sont dans l'incapacité de satisfaire aux demandes de rançons qui leur sont présentées. Les axes d'amélioration envisageables sont donc le renforcement de la cybersécurité de chacune des cibles potentielles et du dispositif collectif. Ces renforcements demanderont des moyens importants. L'ANSSI et ses partenaires ont reçu mission de proposer des pistes pour accélérer l'action de l'État en faveur de la cybersécurité et de la cyberdéfense. Un « nouvel élan cyber » a donc été proposé pour renforcer trois piliers de la cybersécurité nationale : la réponse de l'État face aux cyberagressions, la cybersécurité de l'État et des services

publics, ainsi que l'accompagnement de l'État pour renforcer la cybersécurité de la Nation. La sécurité numérique de l'État et des services publics est d'ores et déjà en cours de renforcement grâce au volet cybersécurité du plan France Relance. Initialement doté de 136 millions d'euros, ce volet a été augmenté de 40 millions supplémentaires début 2022. Il a pour objectif d'élever significativement le niveau de cybersécurité des acteurs publics et s'adresse en priorité aux collectivités territoriales, qui comptent parmi les principales victimes des attaques par rançongiciel, et aux entités impliquées dans la vie quotidienne du citoyen, particulièrement vulnérables aux effets d'une cyberattaque. Deux dispositifs ont été développés à cette fin : des parcours de cybersécurité qui permettent d'aider des acteurs publics à définir l'état de sécurité de leurs systèmes d'information et les travaux les plus urgents à réaliser, grâce à des prestataires de cybersécurité ; la création de centres régionaux de réponse aux incidents de cybersécurité, qui pourront accompagner l'ensemble des acteurs socio-économioques régionaux en fournissant une assistance adaptée à chaque victime de cyberattaques.