ASSEMBLÉE NATIONALE

16ème legislature

Question N° : 5339	De **Mme Émilie Chandler** (Renaissance - Val-d'Oise)	**Question écrite**

Ministère interrogé > Économie, finances, souveraineté industrielle et numérique	**Ministère attributaire** > Première ministre

Rubrique >numérique	**Tête d'analyse** >Augmentation des risques liés à l'espionnage cyber	**Analyse** > Augmentation des risques liés à l'espionnage cyber.

Question publiée au JO le : **07/02/2023**
Réponse publiée au JO le : **28/03/2023** page : **2860**
Date de changement d'attribution : **07/03/2023**

Texte de la question

Mme Émilie Chandler attire l'attention de M. le ministre de l'économie, des finances et de la souveraineté industrielle et numérique sur l'augmentation des risques liée à l'espionnage cyber. Le 24 janvier 2023, l'ANSSI a publié son panorama de la Cybermenace pour l'année 2022. Dans celui-ci, l'Agence souligne que malgré un nombre d'intrusions avérées en légère diminution puisque l'on en dénombre 831 en 2022 contre 1 082 en 2021, la qualité des attaques s'est pour sa part améliorée avec une convergence de l'outillage des attaquants qu'il s'agisse d'acteurs étatiques ou de groupes criminels. De plus, l'Agence Nationale de la Sécurité des Systèmes d'Information, souligne une évolution des victimes notamment d'attaques par rançongiciel avec 40 % de TPE/PME/ETI en 2022 contre 51 % en 2021, mais surtout les établissements publics de santé et les établissements d'enseignement supérieur, qui sont plus fréquemment la cible des attaques. Ces attaques entraînent de nombreuses pertes notamment financières, la seule attaque du Centre Hospitalier de DAX ayant un coût de 2,3 millions d'euros. Ainsi, elle souhaiterait connaître les actions qu'entendant prendre le Gouvernement afin d'améliorer la protection des acteurs économiques et locaux français face à l'augmentation du risque et comment il entend préparer au mieux le pays face au regain probable d'attaques contre la France dans la perspective des Jeux Olympiques et Paralympiques 2024 .

Texte de la réponse

Comme le relève justement l'auteure de la question, la menace constituée par les attaques informatiques conserve toute son acuité. Parmi les cibles les plus exposées, les opérateurs économiques de petite et moyenne tailles disposant de peu de capacités de cybersécurité, les collectivités territoriales, les établissements publics et notamment les établissements de soins font l'objet de nombreuses attaques. Face au caractère endémique de la cyberdélinquance crapuleuse, le Gouvernement souhaite une élévation globale du niveau de cybersécurité du plus grand nombre des structures économiques et de service au public. A cette fin, il promeut, via l'action de l'Agence nationale de sécurité des systèmes d'information, la création de centres régionaux de réponse aux cyber-incidents au profit des entités implantées sur le territoire régional. Ces Computer Security Incident Response Teams (CSIRT), dont la création est financée dans le cadre du plan d'investissement France relance, ont pour mission de traiter les demandes d'assistance des acteurs de taille intermédiaire que sont les petites et moyennes entreprises, les entreprises de taille intermédiaire, les collectivités territoriales et les associations, par exemple. Elles assurent l'intermédiation entre ces victimes et leurs interlocuteurs de proximité, qu'il s'agisse de prestataires de réponse à

incident ou de services de l'État. L'action des CSIRT régionaux s'articule avec celle de la plateforme cybermalveillance.gouv.fr et les services du CERT-FR national. Elle constitue un service gratuit. Au-delà de leur contribution à la remédiation, les CSIRT assurent également des missions de prévention, de sensibilisation et d'accompagnement des acteurs territoriaux, dans une démarche d'élévation de leur niveau de cybersécurité. A ce jour, 12 CSIRT régionaux existent. Trois sont à l'état opérationnel. Les autres le seront durant cette année 2023. S'agissant spécifiquement de la cybersécurité des jeux Olympiques et Paralympiques de 2024, la Première ministre a souhaité que l'Agence nationale de sécurité des systèmes d'information supervise l'ensemble du dispositif national. L'agence, en liaison avec l'ensemble des acteurs de la cybersécurité impliqués, a engagé une action préparatoire résolue dans cinq directions : une analyse précise de l'ensemble des cybermenaces pesant sur l'évènement ; une action générale de mise en sécurité des systèmes d'information les plus indispensables ; la protection des données sensibles ; une vaste action de sensibilisation aux enjeux de cybersécurité de l'ensemble des acteurs impliqués ; la planification et l'entraînement à la réponse opérationnelle à une cyberattaque. La mise en sécurité des systèmes d'information les plus indispensables, axe prioritaire entre tous, sera effectuée durant cette année 2023. La liste de ces systèmes a été arrêtée par l'Agence nationale de sécurité des systèmes d'information, en concertation avec le délégué interministériel aux jeux Olympiques et Paralympiques, le ministère de l'intérieur et des outre-Mer et le groupement d'intérêt public PARIS 2024. Le processus de sécurisation prendra la forme d'audits et d'actions d'accompagnement technique, réalisés soit par l'Agence nationale de sécurité des systèmes d'information elle-même, soit par des prestataires qualifiés. La planification et l'entraînement à la réponse opérationnelle à une cyberattaque est un autre axe d'effort prioritaire. L'Agence nationale de sécurité des systèmes d'information s'attachera à préciser dans le courant de cette année, en lien avec le coordinateur national pour la sécurité des jeux Olympiques et Paralympiques 2024, les services du ministère de l'intérieur, ceux du ministère des armées, ainsi que les autres parties prenantes – notamment le comité d'organisation des jeux Olympiques et Paralympiques –, le dispositif opérationnel de veille, d'alerte et de réponse aux incidents de cybersécurité qui pourraient affecter les jeux Olympiques et Paralympiques 2024, en amont ou lors de leur déroulement. Ce dispositif sera testé lors de plusieurs entraînements. Enfin, face au risque de cyberattaques ciblant de multiples sites sur le territoire national, des procédures permettant de recourir en urgence à des renforts issus d'autres administrations de l'État ou du secteur privé sont en cours de définition.