ASSEMBLÉE NATIONALE

15ème législature

Multiplication des cyberattaques et vulnérabilité informatique

Question écrite n° 36630

Texte de la question

M. Bernard Perrut 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 la multiplication des cyberattaques qui a récemment mis en évidence la vulnérabilité informatique des établissements publics. Après Dax, l'hôpital Nord-Ouest de Villefranche-sur-Saône a été la victime d'une attaque par le cryptovirus rançongiciel RYUK ce lundi 15 février 2021. S'apparentant à une « prise d'otage numérique », ces rançongiciels rendent un grand nombre de fichiers inaccessibles, en immobilisant serveurs et ordinateurs des entreprises ou institutions qui en sont victimes. Les pirates réclament, ensuite, une rançon pour les déverrouiller. Ainsi, les données des sites de Villefranche, Tarare et Trévoux de l'hôpital Nord-Ouest étant cryptées et donc inaccessibles, une grande partie de l'activité de l'hôpital a été paralysée et une rançon a été demandée contre leur restitution. Les conséquences pour l'hôpital sont graves : consultations déprogrammées, services fermés, prise en charge des patients ralentie. Afin de limiter la propagation du virus, les accès au système d'information et à internet ont été coupés et les postes de travail déconnectés. L'ensemble de la téléphonie a été rendue inaccessible. Toutes les équipes hospitalières ont immédiatement mis en place des procédures dites « dégradées » pour assurer les échanges d'informations nécessaires à la prise en charge des patients. Dans ce cas, ces attaques informatiques mettent des vies en danger ! Selon un rapport publié le 1er février 2021 par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), les hôpitaux et autres entités du secteur « santé » représentent une des cibles privilégiées des attaquants par rançongiciel. Cette tendance s'est accrue depuis 2020 avec la pandémie qui pousserait « plus facilement les hôpitaux à payer la rançon au vu du besoin critique de continuité d'activité ». L'ANSSI a été appelée à 192 reprises en 2020, contre 54 fois en 2019, pour des faits liés aux rançongiciels. À la section cybercriminalité du parquet de Paris, le nombre de procédures pour attaque au rançongiciel est passé de 148 à 436 entre 2019 et 2020. Une quarantaine d'autres ont déjà été ouvertes pour le seul mois de janvier 2021. Institutions, établissements publics, entreprises, aucun organisme n'est à l'abri de ce phénomène exponentiel. Mais les interpellations pour des faits liés aux rançongiciels demeurent très rares et un seul suspect dans une affaire a été jugé, en octobre 2020 en France, traduisant l'impunité dont bénéficient ces *hackers*. L'ampleur de ces cyberattaques remet aujourd'hui en cause l'efficacité de la lutte contre la cybermenace. Il lui demande donc s'il compte mettre en place urgemment une véritable politique publique de prévention, d'accompagnement, de protection et de réponse contre la cybercriminalité, la mise à disposition d'outils pour s'en prémunir et riposter en cas d'attaque ; par ailleurs le système de poursuites judiciaires doit être adapté à cette nouvelle forme de délinquance qui porte directement atteinte à l'intégrité numérique d'acteurs essentiels de la société.

Texte de la réponse

Le 9 mars 2022, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a publié un Panorama de la menace informatique 2021 qui analyse les grandes tendances ayant marqué l'année 2021 et souligne les risques d'évolution à court terme. Dans un contexte de généralisation des usages numériques, le nombre de

cyberattaques est en forte hausse. En effet, le nombre d'intrusions avérées dans des systèmes d'information signalées à l'ANSSI a augmenté de 37 % entre 2020 et 2021. La menace représentée par les rançongiciels semble s'être stabilisée, néanmoins à un niveau très élevé (203 attaques traitées en 2021 contre 192 en 2020). Les entités touchées en premier lieu par les rançongiciels sont les TPE, PME et ETI qui représentent 34 % des victimes en 2021 (+ 53 % par rapport à 2020), suivies par les collectivités (19 %) et les entreprises stratégiques (10 %). Ces attaques aux fins de rançonnage, souvent très médiatisées, ne doivent pas occulter le caractère très préoccupant des campagnes d'espionnage et de sabotage. Les opérations d'espionnage informatique restent en effet la principale finalité des attaques opérées par les services de renseignements étrangers et leurs sous-traitants. Elles visent tout autant les institutions que des acteurs privés. Cette hausse des cyberattaques s'explique de deux façons. D'une part, les vulnérabilités sont de plus en plus exploitées et les nouveaux usages numériques, moins maitrisés, comme le Cloud sont également exploités par les cyberattaquants ; d'autre part, les capacités d'action des acteurs malveillants, dont les principales intentions demeurent le gain financier, l'espionnage, la déstabilisation et le sabotage, ne cessent de se renforcer. Face à ce renforcement de la cybermenace, le Gouvernement a mis en place de nombreux dispositifs, notamment en déclinaison des mesures du plan France Relance et de la stratégie nationale d'accélération pour la cybersécurité. La plan France Relance poursuit trois grands axes d'effort dans le domaine de la cybersécurité. D'abord, grâce au dispositif des parcours de cybersécurité, 900 collectivités territoriales, établissements publics et établissements de santé seront accompagnés pendant deux ans dans une démarche de renforcement rapide et concrète de leur niveau de cybersécurité. Ensuite, des services automatisés de cybersécurité sont développés pour mieux détecter les cyberattaques, les filtrer au plus tôt et alerter les organisations de leurs vulnérabilités, susceptibles d'être exploitées par des cyberattaquants. Enfin, des centres de réponses à incidents sont créés, en coopération avec les conseils régionaux. Les premiers seront opérationnels dès l'automne 2022 dans toutes les régions volontaires. De même, des secteurs sensibles, comme celui de la santé, le secteur social ou encore ceux du transport aérien et maritime, disposeront de telles structures. La stratégie nationale d'accélération pour la cybersécurité, désormais intégrée dans le plan France 2030, poursuit un double objectif d'accompagnement du développement d'un potentiel économique important et de maitrise des technologies visant à garantir la souveraineté nationale. Ce plan mobilise 1 milliard d'euros, dont 720 millions de financements publics. Son volet économique repose sur cinq axes : le développement de solutions souveraines de cybersécurité ; le renforcement des liens entre les acteurs de la filière ; la sensibilisation de l'ensemble des acteurs à la cybersécurité (individus, entreprises, collectivités, agents et organismes de l'État), la formation de la jeunesse et des professionnels à la cybersécurité afin de pallier la pénurie de personnel dans ce secteur ; un soutien en fonds propres. Elle s'articule avec des programmes structurants, notamment les actions du Comité stratégique de filière « Industries de sécurité » et appuie des initiatives comme le Campus cyber ou le Grand défi cyber.

Données clés

Auteur : M. Bernard Perrut
Circonscription : Rhône (9e circonscription) - Les Républicains
Type de question : Question écrite
Numéro de la question : 36630
Rubrique : Internet
Ministère interrogé : Transition numérique et communications électroniques
Ministère attributaire : Première ministre

Date(s) clée(s)

Question publiée au JO le : 23 février 2021, page 1659
Réponse publiée au JO le : 7 juin 2022, page 3317