ASSEMBLÉE NATIONALE

15ème législature

Cyberattaques contre les établissements de santé

Question écrite n° 36629

Texte de la question

M. Lionel Causse attire l'attention de 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 dans le contexte de crise sanitaire. Ces derniers mois, de nombreuses institutions publiques ont été victimes de cyberattaques, en particulier dans le domaine de la santé. Les cyberattaques ont augmenté de 20 % dans les structures de santé en 2019. Ainsi, le ciblage du système de santé représente aujourd'hui une menace majeure. De telles cyberattaques pourraient avoir des effets critiques sur la capacité à faire face à la pandémie dans un premier temps, mais aussi dans le suivi des patients et le fonctionnement courant des établissements de santé. L'Agence du numérique en santé (ANS) a publié le 11 juillet 2020 son rapport pour 2019 qui porte sur l'évolution des incidents de sécurité informatique affectant les établissements de santé. L'un des constats est que des logiciels malveillants prennent en otage les données des établissements de santé. Ces cyberattaques paralysent les services de santé, les obligeant à ne plus utiliser leurs matériels informatiques durant plusieurs semaines, et ayant pour conséquence la perte de toutes les données de leurs patients. En conséquence, il lui demande de bien vouloir lui préciser quels sont les moyens mis en place par le Gouvernent afin de pallier les cyberattaques dont sont de plus en plus victimes les établissements de santé.

Texte de la réponse

L'attaque de grande ampleur subie par le centre hospitalier de Dax le 8 février 2021, dont le système informatique médical, comptable et de communication a été neutralisé, a une nouvelle fois illustré l'acuité de la cybermenace sur les établissements publics. Depuis 2018, le secteur de la santé est régulièrement la cible d'attaques informatiques de sophistication et d'intensité variables. Les effets de ces attaques sont particulièrement préoccupants au regard du niveau de cybersécurité des établissements de soins. La sécurité des systèmes d'information est rarement une priorité pour ces établissements. Il en résulte une vulnérabilité d'autant plus préoccupante qu'elle peut ajouter aux difficultés rencontrées durant la pandémie en cours. Dans tous les cas, une cyberattaque à l'encontre d'un hôpital peut interrompre des systèmes d'information indispensables à la fourniture des soins, ou provoquer des pertes de données médicales sensibles. Dans les cas les plus graves, la cyberattaque peut, de façon directe ou indirecte, mettre en danger la vie des patients. Face à ces risques, la cybersécurité des établissements de santé est considérée comme une priorité nationale. Le ministère des solidarités et de la santé (MSS) a ainsi lancé un plan de renforcement des établissements face au risque numérique. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) accompagne le ministère afin d'accélérer la sécurisation d'un certain nombre d'établissements hospitaliers particulièrement importants. En lien avec le ministère, l'ANSSI accompagne ainsi ces hôpitaux afin, dans un premier temps, d'évaluer leur degré d'exposition aux attaques et, dans un second temps, de relever leur niveau de sécurité par l'application de recommandations adaptées. Il s'agit en outre, au travers d'actions de sensibilisation et de recommandations sectorielles spécifiques, d'obtenir à moyen terme une prise de relais par des prestataires compétents, à même d'accompagner l'ensemble des établissements hospitaliers, très nombreux et aux besoins

de cybersécurité très variés. À cet égard, parmi les points particuliers nécessitant une attention soutenue, le sujet de la protection des nombreuses données sensibles produites ou utilisées par le secteur de la santé mérite une mention particulière. Ces données sont particulièrement prisées par des attaquants d'un haut niveau de compétence technique, qu'ils soient des cybercriminels ou soutenus par des États. Il est à ce titre indispensable de veiller à la mise en sécurité au niveau idoine des bases de données de santé, en particulier les plus sensibles, c'est-à-dire celles qui sont susceptibles de contenir des données personnelles.

Données clés

Auteur : M. Lionel Causse
Circonscription : Landes (2e circonscription) - La République en Marche
Type de question : Question écrite
Numéro de la question : 36629
Rubrique : Internet
Ministère interrogé : Transition numérique et communications électroniques
Ministère attributaire : Premier ministre

Date(s) clée(s)

Question publiée au JO le : 23 février 2021, page 1659
Réponse publiée au JO le : 24 août 2021, page 6447