ASSEMBLÉE NATIONALE

15ème legislature

Question N° : 34154	De **Mme Josiane Corneloup** (Les Républicains - Saône-et-Loire)	**Question écrite**

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

Rubrique >établissements de santé	**Tête d'analyse** >Cyberattaques- Protéger les établissements de santé	**Analyse** > Cyberattaques- Protéger les établissements de santé.

Question publiée au JO le : **24/11/2020**
Réponse publiée au JO le : **09/03/2021** page : **2016**
Date de changement d'attribution : **08/12/2020**

Texte de la question

Mme Josiane Corneloup appelle 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 mise en œuvre de dispositifs de sécurité en vue de protéger techniquement les données personnelles. D'origine malveillante ou non, les incidents de cybersécurité ont augmenté de 20 % dans les structures de santé en 2019. il s'agit d'une menace informatique qui concerne également le secteur social et médico-social. L'agence du numérique en santé (ANS) a publié le 11 juillet dernier 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. Selon ce rapport, 300 structures de santé sont concernées par 392 attaques dont 66 mises en danger relevées. Il semble que le nombre total de déclarations reste encore faible au regard du nombre de structures concernées par l'obligation de déclaration et il est probable qu'au moins la moitié des structures concernées a dû faire face à un incident ayant impacté son fonctionnement normal au cours de l'année selon l'ANS. En conséquence, elle lui demande de bien vouloir lui préciser quels sont les moyens mis en place par le gouvernent afin de pallier aux cyberattaques dont sont de plus en plus victimes les établissements de santé.

Texte de la réponse

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. Il en résulte une vulnérabilité d'autant plus préoccupante qu'elle peut ajouter aux difficultés rencontrées durant la pandémie en cours, ainsi qu'en atteste la grave cyberattaque dont a été victime l'hôpital de Dax au début du mois de février 2021. 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, elle 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.