ASSEMBLÉE NATIONALE

15ème legislature

Question N° : 36592	De **M. Bastien Lachaud** (La France insoumise - Seine-Saint-Denis)	**Question écrite**

Ministère interrogé > Solidarités et santé	**Ministère attributaire** > Premier ministre

Rubrique >établissements de santé	**Tête d'analyse** >Sécurité informatique du système de santé	**Analyse** > Sécurité informatique du système de santé.

Question publiée au JO le : **23/02/2021**
Réponse publiée au JO le : **24/08/2021** page : **6446**
Date de changement d'attribution : **09/03/2021**

Texte de la question

M. Bastien Lachaud alerte M. le ministre des solidarités et de la santé sur la sécurité informatique des hôpitaux français. L'hôpital de Dax a été victime d'une cyberattaque. Le système informatique est inutilisable : données médicales, coordonnées des patients mais aussi logiciels permettant de réaliser des soins en radiothérapie ou cancérologie. Le centre de vaccination contre la covid-19 est suspendu jusqu'à nouvel ordre, dépendant entièrement du système informatique. L'arrivée de nouveaux patients est limitée au maximum, les patients sont injoignables pour reporter les rendez-vous. Les malfaiteurs ont installé un logiciel qui bloque le système informatique et réclament une rançon pour les débloquer. Moins d'une semaine plus tard, l'hôpital de Villefranche-sur-Saône a également été victime d'une cyberattaque. Les interventions chirurgicales ont dû être déprogrammées et les patients qui ont besoin de se rendre aux urgences sont redirigés ailleurs. Une telle situation est catastrophique, et particulièrement criminelle en pleine pandémie. Mais ces attaques ne sont pas les premières : en décembre 2020, à Narbonne, à Albertville-Moutiers, à l'AP-HP en 2020. En 2019, le CHU de Rouen avait été touché par une cyberattaque d'ampleur. Les rançongiciels sont des logiciels installés à l'insu de l'utilisateur, qui peuvent bloquer le système informatique. Les données sont inaccessibles et peuvent faire l'objet d'un chantage pour leur restitution ou leur non-divulgation. Les attaquants réclament alors une rançon en promettant un retour à la normale si elle est payée. En mai 2017, le rançongiciel WannaCry était parvenu à infecter plus de 300 000 ordinateurs, dans 150 pays. Victime parmi d'autres de cette attaque, le service national de santé britannique (NHS) avait été durement touché et le fonctionnement de certains services gravement affecté. Plus récemment, fin 2020, 400 hôpitaux aux États-Unis ont été attaqués informatiquement. Le nombre d'attaques au rançongiciel est en nette hausse en 2020, selon un rapport de l'ANSSI publié le 1er février 2021 : alors que 54 incidents liés à des rançongiciels ont été signalés à l'ANSSI en 2019, l'agence a enregistré une hausse de 255 % en 2020 avec 192 incidents rapportés. Dans une réponse à une question orale au Sénat, le secrétaire d'État chargé de la transition numérique et des communications électroniques a indiqué qu'il y avait eu 27 attaques majeures sur des hôpitaux en 2020, et une par semaine depuis 2021. Le rapport de l'ANSSI affirme que « les hôpitaux et autres entités du secteur de la santé représentent globalement l'une des cibles privilégiées des attaquants » et que la tendance s'est « accrue en 2020, notamment dans le contexte de pandémie liée à la covid-19 ». Celui-ci pousserait « plus facilement les hôpitaux à payer la rançon au vu du besoin critique de continuité d'activité ». Le rapport conclut que « les revenus générés par les attaques par rançongiciel et l'émergence d'assurances et de sociétés de négociation validant leur modèle économique suggère que le phénomène rançongiciel continuera à croître dans les années à venir » et souligne que de telles attaques peuvent mettre « en danger la vie des patients » pour ce qui est des attaques ciblant le système de santé. Par ailleurs, des plateformes privées de prise de rendez-vous médicaux avec lesquelles collaborent les services publics, comme

Doctolib (en partenariat avec la sécurité sociale, avec l'AP-HP depuis 2017, pour la gestion des rendez-vous de vaccination contre la covid-19) présentent des failles de sécurité informatique. Celles-ci sont à même de mettre en danger la sécurité des données de santé des patients, le secret médical, voire de perturber l'organisation de la campagne de vaccination si elles étaient exploitées. La plateforme s'est fait pirater des données relatives à des rendez-vous médicaux à l'été 2020 par exemple. M. le député a présenté en juillet 2018 un rapport parlementaire à la commission de la défense nationale et des forces armées. Le rapport analyse de tels risques et comporte des propositions pour améliorer la résilience du pays face aux cyberattaques, notamment celle de ses hôpitaux. Aussi, il souhaite savoir ce que le ministre a fait depuis les premières alertes en 2020 et compte faire pour améliorer la résilience du système de santé face aux cyberattaques, qui risquent de se démultiplier dans les prochaines années.

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.