ASSEMBLÉE NATIONALE

16ème legislature

Question N° : 9626	De **Mme Pascale Martin** (La France insoumise - Nouvelle Union Populaire écologique et sociale - Dordogne)	**Question écrite**

Ministère interrogé > Santé et prévention	**Ministère attributaire** > Santé et prévention

Rubrique >établissements de santé	**Tête d'analyse** >Cyberattaques visant des hôpitaux : il y a urgence	**Analyse** > Cyberattaques visant des hôpitaux : il y a urgence.

Question publiée au JO le : **04/07/2023**
Réponse publiée au JO le : **21/11/2023** page : **10547**
Date de changement d'attribution : **21/07/2023**

Texte de la question

Mme Pascale Martin interroge M. le ministre de la santé et de la prévention sur les cyberattaques récurrentes dans les hôpitaux, qui mettent en danger la santé et la vie privée des citoyennes et des citoyens. L'Agence du numérique en santé avait décompté 730 cyberattaques sur l'année 2021. En réponse, M. le ministre des solidarités et de la santé avait martelé en août 2022 : « La santé des Français ne sera pas prise en otage ». Cependant, dès le mois de septembre 2022, le groupe de *hackers* russe « LockBit 3.0 » a mené une cyberattaque contre le centre hospitalier sud-francilien de Corbeil-Essonnes (CHSF). Face au refus de l'hôpital de payer la rançon, les criminels ont commencé à divulguer du contenu sensible comme des comptes rendus d'examens gynécologiques, de coloscopies, d'accouchements... Le 3 décembre 2022, c'est l'hôpital André-Mignot de Versailles qui a été frappé à son tour, le contraignant à limiter l'accueil aux seules urgences. Par ailleurs, outre la rançon réclamée, un hôpital victime d'une cyberattaque se voit obligé de refonder l'entièreté de son système informatique. Ce fut notamment le cas pour le centre hospitalier de Dax qui, en 2021, a dû débourser près de 2,3 millions d'euros. Le Gouvernement a bien essayé de remédier à ce problème. La stratégie de cybersécurité pour les établissements de santé et médico-sociaux s'est renforcée avec une enveloppe de 350 millions d'euros. 25 millions d'euros ont été alloués à des audits de cybersécurisation des établissements de santé. Dans le cadre du plan France relance, l'Autorité nationale en matière de sécurité et de défense des systèmes d'information (ANSSI) a reçu une enveloppe d'un montant de 136 millions d'euros pour renforcer la cybersécurité de l'État et des territoires pour la période 2021-2022. Mais ces mesures sont de toute évidence insuffisantes : les cyberattaques dans les hôpitaux se poursuivent et les établissements de santé y sont toujours aussi vulnérables. Le mercredi 21 juin 2023, le centre hospitalier universitaire de Rennes a lui aussi été victime d'une cyberattaque, sans incidence sur la prise en charge des patientes et patients, mais qui a entraîné une fuite de données dont l'ampleur n'est pas encore connue. Elle lui demande donc quelles nouvelles mesures le Gouvernement compte prendre afin d'améliorer la protection des établissements de santé face à ces cyberattaques à répétition.

Texte de la réponse

La sécurisation des systèmes d'information hospitaliers (SIH) constitue l'un des fondements stratégiques de la politique numérique mise en œuvre de longue date par le ministère de la santé et de la prévention au service des établissements et des patients, et les moyens, en particulier financiers, mis à disposition des établissements de santé ont évolué au fil du temps en parallèle du développement des cybermenaces. Les premiers accompagnements

hospitaliers ont débuté dès 2012 pour une mise en place des prérequis relatifs à la sécurité numérique. Ils ont été portés par les différents programmes de financement des systèmes d'information hospitaliers : Plan Hôpital Numérique 2012-2017 et programme HOPE'N 2018-2022, ainsi que dans le cadre du volet numérique du Ségur de la santé. Dès 2021, le ministère a renforcé la panoplie des outils contribuant à la fois à l'organisation du déploiement rapide des mesures de sécurité, et en évaluer les effets. L'Agence nationale de sécurité des systèmes informatiques (ANSSI) et l'Agence du numérique en santé (ANS) réalisent des audits de sécurité pour les établissements de santé. L'ANS propose par ailleurs des kits destinés aux établissements pour organiser leurs exercices de crise. Le référentiel MATURIN'H, outil d'amélioration continue de la qualité des systèmes d'information, permet à chaque établissement d'évaluer son niveau de maturité au regard des mesures prioritaires du domaine de la cybersécurité, et d'objectiver les actions entreprises. L'Observatoire permanent de la sécurité des systèmes d'information des établissements de santé (OPSSIES), annoncé par le Président de la République lors de la présentation de la stratégie nationale pour la cybersécurité en 2021, constitue un outil d'aide à la décision pour les acteurs nationaux et régionaux dans la lutte contre la cybercriminalité dirigée contre le secteur sanitaire. Sur le volet financier, les établissements déclarés OSE (Opérateurs de services essentiels) ayant réalisé les audits couvrant les annuaires centraux et de cybersurveillance sont éligibles à un accompagnement financier dans le cadre des aides à la contractualisation (AC) portées par les agences régionales de santé. À ces mesures s'ajoutent des accompagnements financiers dans le cadre, du Ségur relevant du fonds pour la modernisation et l'investissement en santé (FMIS), et du plan France Relance, dont une partie est affectée à la mise en place de « parcours de cybersécurité ». Pour accompagner les équipes hospitalières, le guide d'aide à la préparation de la gestion du risque numérique (plan blanc numérique) a été diffusé le 15 juin 2023 aux agences régionales de santé pour diffusion auprès des établissements de santé. Ce guide vise à fournir un cadre méthodologique et pratique pour prévenir le risque numérique, et des recommandations à suivre pour gérer au mieux une cyberattaque, et ses conséquences, dans l'environnement hospitalier. Lancé en 2023 par le ministère de la santé et de la prévention, le programme CaRE (Cybersurveillance accélération et résilience des établissements), vise à renforcer la résilience numérique des établissements de santé, en mettant à leur disposition des référentiels et des outils pour faire face aux incidents, rattraper leur retard et pérenniser leur niveau de cybersécurisation. Dans la continuité des actions et dispositifs précédemment décrits, il élargit le périmètre des établissements ciblés. Il se structure autour des thématiques de gouvernance et résilience, de ressources et de leur mutualisation, de sensibilisation, de sécurité opérationnelle et s'accompagne de financements. Le ministère de la santé et de la prévention accompagne au quotidien l'ensemble des établissements de santé. Au-delà des mesures déjà engagées, il continuera d'adapter les réponses et les outils aux évolutions d'une cybermenace multiforme et évolutive.