GOUVERNEMENT
Liberté
Égalité
Fraternité

Paris, le 21 décembre 2022

COMMUNIQUÉ DE PRESSE

DE NOUVEAUX ENGAGEMENTS POUR RENFORCER LA CYBERSÉCURITÉ DES ÉTABLISSEMENTS DE SANTÉ

Gérald DARMANIN, ministre de l'Intérieur et des Outre-mer, François BRAUN, ministre de la Santé et de la Prévention et Jean-Noël BARROT, ministre délégué chargé de la Transition numérique et des Télécommunications ont organisé ce jour une réunion de travail sur la cybersécurité des hôpitaux, avec l'ensemble des services mobilisés et les principales fédérations hospitalières.

Ces derniers mois, deux attaques cyber d'envergure ont visé des hôpitaux français : le CHU de Corbeil-Essonnes (91) le 21 août et le CH de Versailles (78) le 3 décembre. Ces attaques ont eu des impacts opérationnels importants sur des services hospitaliers déjà en tension. Dans les deux cas, le plan blanc pour les urgences sanitaires graves a été déclenché, et certains patients dans les états les plus critiques ont dû être transférés vers d'autres hôpitaux.

Les ministres ont tenu à saluer la réactivité et l'engagement exceptionnel des professionnels de ces établissements, qui ont permis d'assurer la continuité des soins pour tous les patients dans les meilleures conditions possibles.

Ce type d'attaque démontre à quel point nous devons amplifier collectivement nos efforts, d'autant plus que tous les indicateurs des menaces cyber sont en hausse :

- En 2021, environ 260 000 procédures judiciaires liées au cyber ont été enregistrées par les forces de sécurité intérieure (+ 20% par rapport à 2020) ;
- Un millier d'attaques au rançongiciel ont été constatées en 2021 sur le territoire ;
- La plateforme Thésée pour la plainte en ligne pour les escroqueries sur Internet lancée en mars atteint déjà 75 000 signalements.

Afin de répondre à ces enjeux, la loi d'orientation et de programmation du ministère de l'Intérieur et des Outre-mer renforce considérablement les moyens en la matière, avec par exemple le recrutement de 1 500 cyber patrouilleurs.

Dans le cadre de la stratégie d'accélération pour la cybersécurité de France 2030, le Gouvernement mobilise également un programme d'investissement d'un milliard d'euros. Cette stratégie vise à soutenir le développement d'un écosystème privé de fournisseurs de solutions souveraines et innovantes, qui permettent notamment de répondre aux besoins de cybersécurité des établissements de santé.

Depuis près de deux ans, un ambitieux plan de renforcement cyber a été mené : audits des établissements conduits par l'ANSSI, vaste campagne de sensibilisation « Tous cyber vigilants », déblocage de nouveaux financements pour améliorer la sécurisation des logiciels et autres outils techniques, etc. A la suite de la cyberattaque ayant visé le CHU de Corbeil-Essonnes cet été, une enveloppe supplémentaire de 20 millions d'euros avait été débloquée pour financer des actions de renforcement du niveau de cybersécurité des établissements de santé.

Afin de renforcer encore davantage la préparation des établissements et leur permettre de faire face en cas d'attaques, les ministres annoncent aujourd'hui le lancement d'un vaste programme de préparation aux incidents cyber. L'objectif est que 100 % des établissements de santé les plus prioritaires aient réalisé de nouveaux exercices d'ici mai 2023. Par ailleurs, un plan blanc numérique sera élaboré au premier trimestre 2023 pour doter les établissements des réflexes et pratiques à adopter si un incident cyber survient (activation d'une cellule de crise, évaluation des impacts, notamment). Enfin, ce nouveau plan entend mutualiser les ressources compétentes au niveau de chaque région en lien avec les Agences régionales de santé (ARS).

Les ministres ont réaffirmé que la nouvelle feuille de route 2023-2027 du numérique en santé accordera une place centrale à la cybersécurité des établissements. A cet effet, une *task force* associant l'ensemble des autorités compétentes est créée aujourd'hui pour bâtir d'ici mars 2023 un nouveau projet de plan cyber pluriannuel massif.

A cette occasion, les ministres ont enfin rappelé la posture constante de l'Etat de non-paiement des rançons lors d'attaque sur les organismes publics. Les ministres ont aussi rappelé l'importance de porter plainte systématiquement afin que des enquêtes puissent être menées et aboutir. Récemment, un hacker russe au Canada qui avait participé à plus de 115 attaques contre des victimes françaises a été interpellé au Canada.

Contacts presse

Cabinet de M. Gérald DARMANIN
service-presse@interieur.gouv.fr – 01 40 07 22 22

Cabinet de M. François BRAUN
sec.presse.cabsante@sante.gouv.fr – 01 40 56 60 60

Cabinet de M. Jean-Noël BARROT
presse@numerique.gouv.fr – 01 53 18 43 42