Communiqué de presse 17 mai 2022

La situation des hôpitaux en matière de cybersécurité est critique : en l'absence d'un financement adéquat, notre système de soins de santé restera à la merci des hackers, avec les conséquences que l'on connaît

Une nouvelle cyberattaque frappant le secteur hospitalier et des institutions de soins rappelle à quel point celui-ci est vulnérable dans un contexte où le nombre et le degré de sophistication de ces menaces d'un genre nouveau ne fait que croître. Affaiblis plus que jamais financièrement et en termes de personnel par la crise sanitaire, dépourvus de subsides pour se prémunir face aux cyber-risques et privés du statut d'organismes essentiels à protéger, les hôpitaux représentent aujourd'hui une cible de choix pour les pirates qui écument l'internet. Faute de mesures et d'un financement structurel adéquat, c'est toute notre système de soins de santé qui risque de sombrer.

Ce samedi 14 mai vers 03h30, l'intercommunale de soins de santé Vivalia a été victime, à son tour, d'une cyberattaque. Celle-ci a entraîné le blocage de 200 serveurs et de 1.500 postes de travail au sein de ses hôpitaux, maison de repos et crèches. Si le personnel a pu réagir rapidement en mettant notamment en place une cellule de crise, l'attaque perturbe ou paralyse encore une partie substantielle de ses activités et ce, pour un temps indéfini. Certaines mesures ont dû être prises en conséquence : opérations non-urgentes supprimées, consultations et examens annulés, centres de prélèvements et antennes COVID-19 à l'arrêt et déclenchement du Plan d'Urgence Hospitalier (PUH).

Cette nouvelle attaque de hackers contre l'un des hôpitaux de notre pays n'a hélas rien d'étonnant lorsqu'on connaît la situation budgétaire catastrophique dans laquelle ceux-ci se retrouvent actuellement. Déjà affaiblis financièrement avant la crise sanitaire, celle-ci n'a fait que renforcer leur vulnérabilité, dans un contexte où ils ne bénéficient d'aucun subside, fédéral ou régional, pour se prémunir contre des cyber-risques pourtant de plus en plus nombreux et sophistiqués. Plus interpellant encore, nos hôpitaux ne sont même pas considérés à l'heure actuelle comme l'une des catégories de structures essentielles à protéger des pirates du web, ce statut leur étant refusé par les décideurs politiques belges.

Pour contextualiser, rappelons l'adoption en 2016 de la Directive européenne NIS (*Network and Information System Security*) visant à assurer un niveau de cybersécurité élevé et commun pour les réseaux et les systèmes d'information de l'Union européenne. Transposée en droit belge en 2019 seulement, elle impose une série d'obligations aux Opérateurs de Services Essentiels (OSE) - identifiés comme tel par chaque autorité sectorielle nationale - en vue de mettre en place un système de gestion de la sécurité de l'information basé sur les normes ISO 27001/27002. En tant qu'autorité sectorielle, le SPF Santé publique devait identifier les premiers OSE pour le 3 novembre 2019. Cependant, celui-ci n'a pas procédé à cette identification, privant ainsi le texte de ses effets dans le secteur des soins de santé. Une erreur qui n'a pas échappé aux yeux de la Commission Européenne, celle-ci l'ayant pointée dès le 30 octobre 2020, parmi d'autres manquements de la Belgique en matière de mise en conformité à la Directive NIS.

En tant que fédération sectorielle, santhea a tenté, sans succès, de rencontrer le SPF Santé publique à ce sujet, afin de plaider pour l'identification des hôpitaux comme OSE et l'octroi d'un subventionnement à la hauteur de ce statut en matière de cybersécurité. Malgré la crise sanitaire que nous avons traversée, laquelle a démontré une nouvelle fois à quel point les institutions de soins sont essentielles au bon fonctionnement de notre pays, le SPF Santé Publique se réfère à l'existence des Plans d'Urgence Hopitaliers (PUH), aux processus d'accréditation et aux normes ISO 27001/27002 pour justifier sa position. Ne nous leurrons cependant pas : dans les faits, le PUH n'est qu'un plan de réaction à une situation d'urgence, et non une mesure visant à anticiper les attaques et renforcer la sécurité ; les accréditations Canadienne/Américaine ne se penchent pas sur la sécurité informatique ; et très peu d'hôpitaux sont aujourd'hui accrédités aux normes ISO précitées.

En pratique, la loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique du 7 avril 2019 (loi NIS) précise que l'autorité sectorielle « assure le suivi permanent du processus d'identification et de désignation des opérateurs de services essentiels et de leurs services essentiels (...). L'autorité sectorielle évalue et, le cas échéant, met à jour l'identification des opérateurs de service essentiels et de leurs services essentiels au moins tous les deux ans ». Partant, nous réitérons une nouvelle fois notre position, malheureusement confortée par les nombreuses cyberattaques dont le secteur a fait les frais dernièrement, en affirmant qu'il nous semble essentiel et indispensable de définir un périmètre d'application de la Directive et de la loi belge NIS dans le secteur de la santé, ainsi qu'un budget annuel structurel suffisant pour permettre la mise en œuvre de cette réglementation et, plus largement, d'une politique de cybersécurité de qualité au sein des institutions de soins.

En termes de budget, le Ministre des Affaires sociales et de la Santé publique Santé Frank Vandenbroucke a informé le secteur, en novembre 2021, qu'une enveloppe de 20 millions d'euros serait mise à la disposition des hôpitaux en 2022 pour renforcer leur niveau de cybersécurité. Il s'agit cependant d'un budget unique loin de rencontrer les besoins actuels. Ainsi, selon une enquête récemment menée dans les hôpitaux flamands, le coût moyen qu'engendrent les efforts nécessaires en termes de cybersécurité serait passé de 368 euros par lit en 2019 à 484 euros par lit en 2020. En extrapolant ces chiffres, on arrive à un coût annuel de plus de 24 millions d'euros pour l'ensemble des hôpitaux généraux et psychiatriques belges. L'adaptation de leur niveau de maturité au niveau de cybermenace actuel et futur nécessiterait par conséquent un financement structurel. Faute de quoi, le risque encouru par les hôpitaux et leurs patients ne fera que se renforcer avec le temps.

À titre de comparaison, la France, bien que disposant d'un réseau d'hôpitaux bien plus étendu que le nôtre, a adopté un plan de lutte contre la cybercriminalité d'un milliard d'euros d'ici 2025. Santhea demande dès lors que nos dirigeants prennent également la mesure de l'urgence en la matière, avant que ne survienne le premier décès belge imputé officiellement à une cyberattaque, comme ce fût le cas pour une patiente de l'hôpital universitaire de Düsseldorf en septembre 2020.

Yves Smeets
Directeur général de santhea
Rue du Pinson, 36 à 1170 BRUXELLES
02/210.42.70 – yves.smeets@santhea.be – www.santhea.be