13 jan 2026 -17:58

Les hôpitaux belges renforcent la cybersécurité grâce à une collaboration sectorielle

Trois hôpitaux belges sur quatre doivent urgemment prendre des mesures supplémentaires pour atteindre le niveau requis de maturité en cybersécurité. Le rapport *Statut de la cybersécurité dans les hôpitaux belges*, élaboré par l'ASBL SHIELD en collaboration avec le SPF Santé Publique le démontre. L'analyse est basée sur des mesures récentes de maturité dans plus de cinquante hôpitaux à travers le pays. En outre, le rapport met en évidence une prise de conscience aiguë des risques liés à la cybersécurité au sein du secteur hospitalier, qui se traduit par une accélération tangible des avancées, rendue possible par une coopération structurelle.

Menace cybernétique et maturité des hôpitaux

Dans un contexte géopolitique où les cyberattaques sont de plus en plus utilisées pour provoquer des perturbations sociales, le secteur de la santé est également une cible potentielle. Pour les hôpitaux, non seulement la protection des données sensibles est centrale, mais surtout la continuité et la sécurité des soins.

Le rapport montre que les différences de maturité cybernétique entre les hôpitaux restent importantes. Un hôpital sur quatre atteint déjà ou s'approche du niveau requis, tandis que les hôpitaux plus petits, et les hôpitaux psychiatriques en particulier, accusent du retard en raison de ressources limitées et d'un manque de profils spécialisés. Il existe aussi des différences régionales : les hôpitaux flamands obtiennent en moyenne de meilleurs résultats que les hôpitaux wallons et bruxellois.

NIS2 comme norme pour la cybersécurité

La directive européenne NIS2 exige que les organisations des secteurs essentiels, y compris les hôpitaux, renforcent de manière démontrable leur cybersécurité. La directive combine des mesures techniques, telles que la détection et la sécurité réseau, avec une opération interne formellement organisée autour des processus, des responsabilités et de la gestion des incidents. Les deux éléments sont nécessaires pour répondre aux exigences du NIS2.

Collaboration et outils partagés pour améliorer la cybersécurité

La tendance générale dans le secteur hospitalier est positive. Grâce à une coopération intensive et à des outils partagés, de plus en plus d'hôpitaux progressent, notamment dans le domaine de la gouvernance et de l'intégration formelle de la cybersécurité.

L’asbl SHIELD joue un rôle central en tant que plateforme de coopération neutre qui réunit hôpitaux, prestataires de services ICT et gouvernement. En collaboration avec le SPF Santé Publique, l’asbl SHIELD soutient une approche sectorielle dans laquelle la maturité est mesurée de manière systématique et où les connaissances et solutions sont partagées.

Un outil important à cet égard est la Bibliothèque SHIELD : un ensemble sectoriel de processus, procédures et documents de politique élaborés à l'échelle du secteur, élaborés par et pour les hôpitaux belges. La bibliothèque est alignée sur le NIS2 et sur des normes reconnues telles que ISO/IEC 27001 et CyberFundamentals. Cela évite la duplication des efforts, garantit une plus grande cohérence et accélère la mise en œuvre des mesures de cybersécurité.

SHIELD et le SPF Santé Publique ne se limitent pas à produire un rapport. Les mesures de maturité constituent la base des actions ciblées. Dans le cadre d’une plateforme neutre, les hôpitaux collaborent avec le gouvernement et les prestataires de services ICT sur des solutions axées sur la demande, adaptées à leur contexte et à leurs besoins spécifiques.

Feuilles de route pour renforcer la cyberrésilience

La progression de la maturité sera continuellement surveillée et mise à jour. De plus, une feuille de route individuelle est élaborée pour chaque hôpital pour les 36 prochains mois, avec des priorités claires, des solutions planifiées et une estimation du déploiement nécessaire des effectifs et des budgets. Ces feuilles de route individuelles sont rassemblées dans une feuille de route sectorielle, qui offre un aperçu des efforts conjoints nécessaires pour accélérer la cyberrésilience des soins de santé belges et où un soutien supplémentaire est approprié.

Le ministre de la Santé met à disposition chaque année 15 M€ pour la cybersécurité, qui sont mis à disposition des hôpitaux généraux et psychiatriques. Avec les one-shots de 2022 (20 M€) et 2024 (40 M€), 105 M€ ont déjà été investis depuis 2022.

Nous avons co-investi dans l’asbl Shield, une initiative des hôpitaux, afin de développer des services de cybersécurité pour les hôpitaux pour qu’ils puissent joindre leurs forces et partager leurs connaissances. Nous sommes convaincus de soutenir les efforts de santé publique pour rendre les hôpitaux conformes au NIS2. Plus de 90 % des hôpitaux généraux travaillent déjà sur ce sujet et ont fait des progrès significatifs ces dernières années, mais il reste encore beaucoup de travail à faire. Par exemple, des exercices mensuels sont organisés avec les hôpitaux pour savoir comment gérer les cyberincidents afin de développer et d'améliorer les meilleures pratiques.

Le rapport est disponible sur www.shield-vzw.be

SPF Santé publique, Sécurité de la Chaîne alimentaire et Environnement
Avenue Galilée, 5 bte 2
1210 Bruxelles
Belgique
+32 2 524 97 97
http://www.health.belgium.be

Justine Cerise
Porte-parole (FR)
+32 (0)499 27 40 30
+32 (0)2 524 99 13
justine.cerise@health.fgov.be

Vinciane Charlier
Porte-parole (FR)
+32 (0)2 524 99 21
+32 (0)475 93 92 71
vinciane.charlier@health.fgov.be

Annelies Wynant
Porte-parole (NL)
+32 2 524 97 38
+32 485 73 44 05
annelies.wynant@health.fgov.be