N°2125
Entrée le 17.04.2025
Chambre des Députés

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de la Santé
et de la Sécurité sociale

Réponse de Madame la Ministre de la Santé et de la Sécurité sociale à la question parlementaire n° 2125 du 21 mars 2025 de l'honorable Député Monsieur Gusty Graas.

En réponse à la question parlementaire de l'honorable Député, il convient de rappeler que la communication d'informations sensibles en matière de cybersécurité peut elle-même représenter un risque, en exposant des éléments exploitables à des fins malveillantes. Dans cette optique de prudence, il est à souligner que des mesures sont déjà en place et que des efforts significatifs sont déployés pour améliorer constamment la cybersécurité dans les systèmes hospitaliers.

1. Quel a été le nombre total de cyberattaques visant les hôpitaux au cours de l'année écoulée ? Parmi celles-ci, combien ont été classées comme graves ? Quelles ont été les principales typologies d'attaques observées ? Quels enseignements ont pu en être tirés ?

Les établissements hospitaliers sont quotidiennement exposés à un flot relativement constant de tentatives d'intrusion et d'alertes issues de courriels suspects et d'autres signaux d'alerte. Selon les informations à disposition du ministère de la Santé et de la Sécurité sociale, aucun incident grave n'a cependant dû être notifié aux autorités compétentes.

L'analyse de ces incidents réguliers a permis de confirmer l'efficacité des dispositifs de surveillance et de détection en place. Cependant, elle a aussi mis en lumière quelques axes d'amélioration, notamment en ce qui concerne la gestion de ces incidents et le soutien aux équipes en charge de la gestion des situations d'attaque. Cette expérience souligne également l'importance capitale de la sensibilisation régulière du personnel aux enjeux de la cybersécurité. Des procédures d'amélioration continue des moyens de protection informatique sont en place afin de minimiser autant que possible les risques encourus.

2. Quelles performances ont été relevées lors des exercices de simulation ? Quelles conclusions ont été dégagées et ont-elles déjà été mises en application ?

Les exercices menés par l'ILR ont été notés autour de 4 sur 5 pour l'ensemble des hôpitaux et ont permis de confirmer une réactivité globale adaptée tout en mettant en lumière des marges de progression. Ces tests confirment la pertinence des approches adoptées.

Les enseignements tirés de ces observations et simulations ont conduit à des ajustements progressifs des procédures internes. Des campagnes de sensibilisation régulières ont également été instaurées pour renforcer les bonnes pratiques en matière de cybersécurité. Grâce à ces mesures et au soutien de partenaires tels que LuxITH et l'Agence eSanté, le secteur hospitalier continue d'améliorer ses dispositifs de sécurité afin de garantir une résilience face aux menaces évolutives.

En résumé, bien que de nombreuses tentatives d'attaque soient observées quotidiennement, les dispositifs de sécurité et de surveillance en place permettent de limiter les impacts opérationnels et de maintenir une vigilance constante. Les retours d'expérience et les initiatives de sensibilisation contribuent à renforcer encore davantage la résilience du secteur sans révéler d'éléments stratégiques susceptibles d'être exploités.

Face à une digitalisation croissante du secteur hospitalier et à l'émergence rapide de nouvelles technologies, il demeure indispensable de poursuivre les efforts d'investissement et d'adaptation. Le maintien d'un haut niveau de cybersécurité passe par une mise à jour continue des moyens humains, techniques et organisationnels afin de répondre efficacement aux menaces actuelles et futures et de garantir l'intégrité et la confidentialité des données de santé des citoyens, tout en assurant la disponibilité des systèmes nécessaires au bon fonctionnement des établissements.

3. Quelles recommandations l'OSIS a-t-il formulées en matière de nouvelles lignes directrices ?

Depuis son établissement en novembre 2022 par le ministère de la Santé, l'Organe de Sécurité Informatique en Santé (OSIS) définit des recommandations appliquées au secteur hospitalier, ainsi qu'à des entités associées de support (telles que LuxITH), afin d'harmoniser notamment les sujets suivants :

1. Les processus de cybersécurité organisationnels et opérationnels ;
2. Les mesures de cybersécurité techniques et
3. La gestion de certains projets „structurants" pour les entités concernées et tels que le SOC sectoriel, le déploiement des SIEMs ou l'usage de Microsoft M365.

Depuis son établissement, OSIS est intervenu en particulier dans les sujets suivants :

1. Politique de sécurité de l'information ;
2. Sensibilisation des praticiens et du personnel hospitalier, quant aux conditions d'utilisation des adresses email professionnelles ;
3. Politique de gestion des mots de passe appliquée aux praticiens et personnel hospitalier ;
4. Supervision de la mise en place d'un service de réaction en cas de cyber incidents ;
5. Gestion de la relation avec les sous-traitants ;
6. Projets SOC sectoriel, SIEMs et M365.

Dans ce contexte, l'Union Européenne a publié le 01 avril 2025[1] ProtectEU, une nouvelle stratégie européenne de sécurité intérieure. Un des axes de développement vise à renforcer la résilience face aux menaces hybrides et notamment à aider les États membres à sécuriser toutes les infrastructures critiques physiques et numériques. Ces travaux seront suivis de près par le M3S et par la Direction de la santé afin de renforcer le niveau de préparation et de sécurité du secteur hospitalier.

[1] https://ec.europa.eu/commission/presscorner/detail/en/ip_25_920

4. Comment s'organise la collaboration entre l'OSIS et les différentes parties prenantes ? Des améliorations ont-elles été proposées concernant les procédures mises en œuvre par les acteurs concernés ? »

OSIS a été mis en place au sein du M3S afin d'accompagner les acteurs dans les orientations à prendre et pour proposer des initiatives de gestion cohérente de l'environnement de sécurisation des données.

Le comité de gestion OSIS est composé de représentants du M3S et du GIE INCERT.

Un Comité de Pilotage de Cybersécurité (CPC) a été établi en parallèle au comité de gestion OSIS. Ce comité est composé de représentants du M3S, du GIE INCERT, de la FHL, de LuxITH, de la CNS et de l'Agence eSanté, et a pour missions :

1. d'accompagner les structures concernées dans l'application des recommandations émises par OSIS, et ceci dans une optique :
    a. d'harmonisation des bonnes pratiques ;
    b. de mutualisation des ressources et
    c. de s'assurer que toutes les parties prenantes disposent du même niveau d'information.

2. de proposer par ailleurs auprès d'OSIS des recommandations de cybersécurité.

Les interactions entre des représentants d'OSIS et du CPC sont régulières, et des améliorations ont ainsi été proposées et mises en œuvre par les établissements hospitaliers en lien avec les sujets évoqués à la précédente question. Selon les sujets traités, l'élaboration des propositions d'approches se fait par le biais de groupes de travail auxquels participent les responsables de la sécurité des systèmes d'information (RSSI) et les délégués à la protection des données (DPO) des établissements hospitaliers.

Luxembourg, le 17 avril 2025

La Ministre de la Santé
et de la Sécurité sociale

(s.) Martine Deprez