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

Dossier suivi par: JOME Laurent
Tel: 247 85510
Email: laurent.jome@ms.etat.lu

Monsieur le Ministre
aux Relations avec le Parlement
Service central de Législation
5, rue Plaetis
L – 2338 Luxembourg

Luxembourg, le 9 janvier 2020

Concerne: Question parlementaire n° 1568 du 4 décembre 2019 de Monsieur le Député Gilles Baum et de Madame la Députée Carole Hartmann
Réf. : 829x5b4ae

Monsieur le Ministre,

J'ai l'honneur de vous faire parvenir en annexe la réponse du soussigné à la question parlementaire n° 1568 du 4 décembre 2019 de Monsieur le Député Gilles Baum et de Madame la Députée Carole Hartmann concernant la "Cybersécurité dans le secteur de la santé".

Veuillez agréer, Monsieur le Ministre, l'assurance de ma considération très distinguée.

Étienne SCHNEIDER
Ministre de la Santé

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

Réponse de Monsieur le Ministre de la Santé à la question parlementaire n° 1568 du 4 décembre 2019 de Monsieur le Député Gilles Baum et de Madame la Députée Carole Hartmann concernant la "Cybersécurité dans le secteur de la santé".

Je tiens au préalable à souligner que la sécurité des réseaux et systèmes d'information ainsi que celle des données relatives à la santé joue un rôle crucial pour l'intégration des technologies d'information et de communication dans le domaine de la santé, alors qu'elle constitue d'une part un levier essentiel pour susciter la confiance des patients et professionnels de la santé dans le numérique et qu'elle permet, d'autre part, d'éviter des incidents susceptibles de nuire à la dispensation de soins de santé et d'entraîner des pertes financières conséquentes.

1. Les hôpitaux et les cabinets médicaux luxembourgeois sont-ils protégés adéquatement contre des cyberattaques ? Dans affirmative, quelles mesures ont été prises ?

Il résulte des dispositions applicables en matière de sécurité de l'information et de cyber sécurité qu'il appartient à tous les responsables des hôpitaux et cabinets médicaux ainsi qu'à leurs sous-traitants de traiter les données à caractère personnel de manière à garantir une sécurité et une confidentialité appropriées, y compris à prévenir l'accès non autorisé à ces données et à l'équipement informatique utilisé pour leur traitement.

De ce fait, les établissements hospitaliers aigus ont développé une approche « Système de Management de la Sécurité de l'Information » (SMSI) comportant notamment des analyses de risques et des mesures pour les atténuer, des audits de sécurité du système d'information ainsi que des tests d'intrusion. Ils s'investissent également à compléter celle-ci, sous l'impulsion de l'Agence eSanté, par une approche de certification ISO27001 des systèmes d'information hospitaliers. Grâce à des audits externes aux établissements, ces dernières viennent appuyer les différents SMSI. Cette approche inclut pour les établissements hospitaliers des mises à jour régulières des systèmes d'informations à l'aide de « patchs de sécurité » qui, de plus en plus performants contre les menaces et vulnérabilités connues, permettent la mise à jour des réseaux, pares feux, antivirus et applications améliorant ainsi significativement le niveau de sécurité des systèmes.

Un CIRT (Cyber Incident Response Team) santé a été créé et animé par l'Agence eSanté et ses partenaires. Des tests et formations sont également organisés afin de vérifier les bonnes pratiques des politiques et procédures de sécurité face à d'éventuelles menaces.

Par ailleurs une charte informatique commune prévoit les mesures de sécurité suivantes à mettre en œuvre par les établissements de santé:

- la tenue d'un inventaire des moyens informatiques connectés au réseau qui sont sous leur responsabilité ;
- l'installation de logiciels qui proviennent de sources réputées et qui respectent les licences d'utilisation de l'éditeur ;
- la mise en place de protections contre les logiciels malveillants notamment par l'application régulière des correctifs de sécurité et l'installation d'antivirus ;
- la sensibilisation des utilisateurs à la sécurité de l'information par la mise en place d'informations et de formations adaptées pour la bonne utilisation des moyens informatiques mis à disposition ;
- la sauvegarde des données et de la protection physique des moyens informatiques ;
- l'utilisation du réseau et de ses services dans le respect de la législation applicable à l'établissement de santé et à la protection des données à caractère personnel.

Il importe finalement de souligner que pour établir une connexion à l'application dossier de soins partagé, le programme informatique utilisé par les hôpitaux et les cabinets médicaux luxembourgeois doit être conforme aux critères de connexion inclus dans les référentiels d'interopérabilité définis pour la plateforme nationale d'échange et de partage des données de santé de l'Agence eSanté et obtenir l'attestation de conformité y relative.

2. Est-ce que des mesures additionnelles sont envisagées dans le futur ? Dans l'affirmative, lesquelles?

En vue d'améliorer les bonnes pratiques en matière de sécurité informatique, il est prévu non seulement d'augmenter la surveillance des systèmes d'information avec des audits réguliers mais également de moderniser les outils qui intègrent d'office la sécurité, ainsi que de développer les échanges entre acteurs de la santé autour du CIRT et avec les instances nationales et autres acteurs hébergés au Luxembourg.

Un autre axe à développer constitue celui de la formation des responsables d'hôpitaux et collaborateurs en vue de les assister à prévenir et à identifier les cyber menaces et, pour certains, à les gérer.

3. Les hôpitaux nationaux font-ils des exercices d'urgence, simulant des attaques informatiques ? Dans l'affirmative, quelles conclusions ont été tirées ?

Les hôpitaux réalisent régulièrement des audits de sécurité (internes ou externes) en particulier avec des Pen Tests. Les menaces sur les données sont des risques qui évoluent perpétuellement avec des outils de plus en plus performants. Ces risques doivent donc être traités avec des approches similaires et donc des outils de plus en plus performants et appropriés comme tels par tous les utilisateurs jusqu'aux directions générales. Il importe qu'un travail collaboratif entre tous les acteurs hospitaliers et les fournisseurs et hébergeurs des systèmes soit maintenu et soutenu par les directions générales de toutes les structures.

Certains établissements hospitaliers participeront au cyber exercice organisé en 2020 par l'ENISA (European Network and Information Security Agency).

4. Est-ce que la sécurité des systèmes de gestion de cabinets médicaux au Luxembourg est garantie par des fournisseurs de services informatiques certifiés? Dans l'affirmative, qui est responsable pour la certification de ces fournisseurs au Luxembourg ?

Actuellement le ministère de la Santé n'a pas connaissance de logiciels de cabinets libéraux qui sont en certification Iso27001 avec un SMSI formalisé. Toutefois certains cabinets mettent en œuvre un certain nombre de bonnes pratiques en matière de sécurité.