SPF SANTÉ PUBLIQUE
SÉCURITÉ DE LA CHAÎNE ALIMENTAIRE
ET ENVIRONNEMENT

Direction générale Soins de santé

CONSEIL FÉDÉRAL DES
ÉTABLISSEMENTS HOSPITALIERS

Bruxelles, le 16 décembre 2021

Réf. : CFEH/D/544-1 (*)

Avis à l'intention du ministre concernant la cybersécurité — partie 2

Au nom du Président,
Margot Cloet

Annick Poncé
(Signature)

Digitally signed by Annick Poncé
(Signature)
Date: 2022.01.11 10:42:54 +01'00'

Annick Poncé
Directeur général ad interim

(*) Le présent avis a été approuvé par la plénière le 16/12/2021 et ratifié par le Bureau à cette même date.

Par la présente, le CFEH souhaite partager son avis en réponse à la demande d'avis du ministre Vandenbroucke du 19/05/2021.

Dans un premier avis (CFEH/D/536-2) du 29 juin 2021, des réponses ont déjà été données à certaines questions urgentes. En outre, un premier positionnement a été décrit par rapport à la problématique liée à la cybersécurité.

1. *Contexte de la problématique*

Dans sa demande d'avis du 19 mai 2021, le ministre a souligné l'intention du cabinet d'apporter son soutien aux hôpitaux, sur le plan organisationnel et administratif, dans le cadre de la mise en œuvre de la politique en matière de cybersécurité, en mettant l'accent sur la responsabilisation et la poursuite des objectifs à long terme. Il a également été fait référence aux préparatifs nécessaires à la publication d'une nouvelle directive européenne concernant ce domaine. À cet égard, l'accent sera placé sur la gestion des risques et sur la conformité à une liste de mesures de sécurité minimales.

Entre-temps, un groupe de travail composé d'experts a été mis sur pied au sein du CFEH afin de se pencher sur cette problématique.

De plus, dans la demande d'avis, il a été demandé d'accorder une attention particulière à la sensibilisation du secteur et l'objectif d'accroître la maturité en ce qui concerne la politique de cybersécurité.

2. *Remarques préalables*

Lors de la réunion conjointe des groupes de travail BMUC et Cybersécurité du 17 novembre 2021, le cabinet a expliqué les budgets prévus, entre autres, pour le volet « cybersécurité ». Le CFEH a été informé à cette occasion qu'une enveloppe de 20 millions d'euros serait mise à la disposition des hôpitaux pour 2022. Il s'agirait à cet égard d'un apport unique de moyens financiers. Le CFEH est reconnaissant de cet apport nécessaire de moyens financiers comme fonds de soutien pour faire face à une menace d'envergure sur notre système de santé. Néanmoins, il déplore le caractère unique dudit budget. Il est clair que la menace posée par les cyberattaques est de plus en plus chronique par nature, avec des conséquences souvent considérables qui ne peuvent être résolues en investissant dans des personnes et des ressources de manière ponctuelle. D'ailleurs, le CFEH renvoie également à une enquête récemment menée dans les hôpitaux flamands et portant sur le coût par lit qu'engendrent les efforts nécessaires en termes de cybersécurité. Une augmentation du coût moyen par lit y a été observée, passant de 368 euros par lit en 2019 à 484 euros par lit en 2020.

Partant de 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 du niveau de maturité au niveau de menace actuel et futur nécessitera par conséquent un financement structurel. Un financement insuffisant renforcera systématiquement le risque systémique de cybersécurité, alors que plusieurs hôpitaux se situent déjà dans la zone à risque.

Le CFEH note qu'au cours de l'année écoulée, trois cyberattaques majeures ont été perpétrées contre des hôpitaux, entraînant des conséquences lourdes sur la prestation de services et d'éventuelles implications sur la qualité des soins. Il ne s'agit donc plus d'événements fortuits, mais d'une preuve que le secteur des soins de santé en général (et les hôpitaux en particulier) est une cible de choix pour ce type d'attaque. Les informations provenant d'un contexte international soulignent également cette tendance.

Le CFEH note que les mesures prises jusqu'à présent par les hôpitaux pour résoudre ce problème sont très variables. Certains hôpitaux ont déjà fait des efforts considérables pour évaluer et adapter leurs systèmes. D'autres hôpitaux sont actuellement encore en phase de démarrage. Lorsque, dans le nouvel avis sur l'approche proposée en matière de cybersécurité dans les hôpitaux, nous décrirons plus en détail les mesures à prendre, le ministre devra tenir compte du fait que certaines mesures ont déjà été prises dans un certain nombre d'hôpitaux, tandis que pour d'autres, elles constitueront la base de leur nouvelle approche. Le CFEH tient à souligner qu'en matière de protection contre les cyberattaques, il va de soi qu'il est préférable d'adopter une approche proactive, permettant de détecter et d'éviter les attaques potentielles en temps utile. Toutes les autres mesures sont secondaires mais n'en demeurent pas moins importantes. Nous aborderons donc ces divers éléments en tant que tels.

Enfin, le CFEH tient à souligner au préalable qu'il est préférable d'allouer le financement à l'échelle individuelle de l'hôpital. Comme déjà susmentionné, la maturité des hôpitaux en ce qui concerne la cybersécurité connaît des degrés divers. Cela signifie que chaque hôpital est confronté à ses propres priorités qui nécessitent sa propre interprétation. Cela ne signifie pas qu'il ne faut pas prêter attention aux solutions collectives. Dans la mesure du possible, nous devons chercher des moyens de coopérer les uns avec les autres afin de dépenser les ressources aussi efficacement que possible (voir également ci-dessous).

3. *Actions de cybersécurité au sein des hôpitaux*

Le CFEH souhaite se référer à son avis CFEH/D/536-2(*) où les mesures à prendre et les implications financières ont déjà été discutées en détail.

Nous souhaitons attirer une nouvelle fois l'attention sur les différentes étapes, en tenant toutefois compte du fait que certains hôpitaux ont déjà pris un certain nombre de ces mesures. C'est pourquoi le FRZV n'est pas favorable à rendre obligatoires un certain nombre de ces mesures. Les rendre obligatoires (par exemple, un audit à l'échelle du secteur) n'est pas une manière efficace de dépenser des ressources rares ou, en d'autres termes, cela implique des ressources que les hôpitaux pourraient bien mieux utiliser dans des mesures offrant un degré de protection plus élevé.

- Création de sensibilisation
  Le CFEH tient à souligner que la sensibilisation requise à cette problématique est primordiale au sein des organisations. Chaque membre du personnel hospitalier endosse une responsabilité à cet égard, comme en atteste à maintes reprises l'évaluation des incidents. Bien que dans de nombreux hôpitaux, l'accent est placé, à juste titre, sur la mise en œuvre technique de solutions, l'application d'une politique d'implication du personnel est l'une des pierres angulaires d'une politique réussie. Dans son premier avis, le CFEH préconise les formations e-learning pour familiariser le personnel avec les directives et les mesures de sécurité.
  Voir recommandation : prévoir un financement structurel adéquat

- Mesurer la maturité de l'organisation et identifier les risques
  Une autre étape importante consiste à déterminer la maturité et à identifier les principaux risques et les priorités pour y remédier. Dans ce cadre, il importe que l'hôpital puisse se positionner par rapport à une norme minimale (voir également ci-dessous).
  Voir recommandation : élaborer un cadre de référence en matière de cybersécurité.

- Élaboration d'un plan (d'urgence) complet axé sur la cybersécurité

  L'analyse de risque et la mesure de maturité ci-dessus peuvent servir de base à l'élaboration d'un plan (d'urgence) en cas d'incident (Incident Response Plan) comme partie intégrante du plan d'urgence global de l'hôpital si tel n'est pas encore le cas. Les récentes cyberattaques ont attesté la très grande nécessité de s'appuyer sur des protocoles et des directives.

  Voir recommandation : Incident Response Plan : élaborer des templates et organiser l'échange d'expériences

- Rassembler les compétences et les mettre à disposition

  Le CFEH constate qu'il n'est pas évident de développer et de maintenir l'expertise spécifique en matière de cybersécurité dans le domaine des soins hospitaliers. Les hôpitaux ne sont pas suffisamment en mesure d'attirer des profils spécialisés. En outre, les collaborateurs ICT dans les hôpitaux combinent plusieurs tâches. Lorsqu'il est fait appel à un expert externe, la connaissance de la spécificité d'un hôpital pose souvent problème. Pour ces raisons, la mise en commun (*pooling*) d'expertise, tant interne qu'externe, peut être une piste intéressante qui mérite d'être approfondie.

  Voir recommandation : créer une Emergency Response Team (« S-CERT »)

- Échange d'expériences entre hôpitaux

  Face à des conditions qui ne facilitent pas le développement d'une expertise suffisante (voir ci-dessus), l'échange d'expériences et de connaissances peut être une façon d'éviter les erreurs, de raccourcir les courbes d'apprentissage... afin de permettre une utilisation plus efficace des moyens limités. Plusieurs hôpitaux organisent déjà ce type d'échange entre eux. La question est de savoir comment rassembler et partager le mieux possible les connaissances présentes dans et en dehors de nos hôpitaux.

  Voir recommandation : créer une plateforme favorisant l'échange d'expériences entre hôpitaux

- SIEM/SOC

  Comme susmentionné également dans le précédent avis, l'installation d'un SIEM (*Security Information and Event Management*) ou d'un SOC (*Security Operations Center*) est considérée comme essentielle. Un monitoring permanent des éventuelles menaces 7 jours sur 7, 24 h sur 24 permet d'anticiper les cyberattaques. Le CFEH constate que le secteur considère cela comme une priorité dans le cadre d'une politique de cybersécurité efficace et adéquate.

  Voir recommandation : élaborer un SOC/SIEM pour les hôpitaux belges

- Interventions techniques

  Enfin, n'oublions pas que ce sont surtout les interventions techniques/technologiques effectuées au sein de l'hôpital individuel qui réduisent le risque de cyberattaque : autoriser des logiciels et installer du matériel informatique qui interviennent au niveau des processus et de l'architecture déjà en place. De nombreux hôpitaux savent ce qu'ils doivent faire pour se préserver de certains risques, mais ne disposent tout simplement pas des moyens nécessaires.

  Voir recommandation : prévoir un financement structurel et suffisant

4. *Problématique spécifique*

Comme indiqué dans le précédent avis, le CFEH souhaite soulever encore quelques problèmes supplémentaires.

- Assurabilité du risque en cas de cyberattaque
  Le CFEH constate que l'assurabilité du risque en cas de cyberattaque est rejetée par le secteur de l'assurance. Il ne s'agit plus seulement d'augmenter les primes, mais simplement de ne pas vouloir inclure ce type de risque dans le portefeuille d'assurances. Ceci entraîne, bien entendu, d'importantes répercussions pour le secteur. Cette évolution est inacceptable aux yeux du CFEH.

- Financement de fonctions liées à la cybersécurité au sein de l'hôpital
  Le précédent avis a déjà fait référence à l'obligation des hôpitaux d'engager un conseiller en matière de sécurité de l'information et un DPO depuis quelques années déjà, sans qu'aucun financement ne soit prévu à cette fin. Dans le cadre de la problématique liée à la cybersécurité, on ne peut sous-estimer le rôle de ces fonctions au sein d'un hôpital. Elles jouent en effet un rôle crucial tout au long du trajet de cybersécurité. Dès lors, le CFEH demande à nouveau au ministre de prévoir un financement adapté à ces fonctions au sein des hôpitaux.

- Réglementation
  Aux Pays-Bas, l'interdiction de verser une rançon en cas de piratage est à l'étude. On éliminerait ainsi une grande partie de la motivation dans le chef des auteurs de ces attaques. On peut se pencher sur la question de savoir si une législation similaire serait utile en Belgique. Un contre-argument que l'on pourrait formuler ici est que, dans ce cas, les pirates informatiques se concentreront sans doute sur les organisations les plus vulnérables pour cause de problématique spécifique, comme les hôpitaux.
  Voir aussi aux États-Unis : Ransomware and Financial Stability Act

5. *Recommandations concrètes à l'attention des autorités*

- **Prévoir un financement structurel et suffisant**
  Pour plus de détails : voir mécanisme de financement

- **Soutenir le travail de sensibilisation en matière de cybersécurité en milieu hospitalier**
  Ceci peut se faire en rendant ces actions éligibles au financement. Voir aussi : mécanisme de financement.

- **Élaborer un cadre de référence en matière de cybersécurité**
  Nous disposons à ce jour d'une série de normes minimales (https://www.ehealth.fgov.be/ehealthplatform/fr/normes-minimales) qui peuvent faire office de point de départ pour l'élaboration d'un cadre approprié en tant qu'outil technique pour :
  - évaluer la maturité individuelle et les risques de l'hôpital ;
  - effectuer un benchmarking entre hôpitaux ;
  - permettre un échange d'expériences structuré.

  Le CFEH propose de constituer un groupe de travail dont la mission serait de composer et d'entretenir ce cadre. En d'autres termes, ce groupe de travail serait permanent.

- **Créer une plateforme favorisant l'échange d'expériences entre hôpitaux**
  Cette plateforme doit permettre un échange d'informations le plus optimal possible entre tous les hôpitaux. Cette recommandation est déjà mise en pratique.

- **Incident Response Plan : élaborer des templates et organiser l'échange d'expériences**
  Au moyen de modèles (*templates*) et par voie d'échanges, les hôpitaux peuvent élaborer ou ajuster leurs plans. Cette recommandation est déjà mise en pratique par le biais d'un groupe de travail qui se penche sur la question.

- **Élaborer un SOC/SIEM pour les hôpitaux belges**
  L'idéal serait d'organiser ce système au niveau du secteur pour ainsi mettre en commun un maximum de moyens et de compétences (même les compétences en externe sont rares). Toutefois, une coordination poussée entre les hôpitaux est nécessaire avant qu'un SOC de ce type puisse être collectivement mis en place. Par exemple, le niveau de maturité de base des hôpitaux participants devra être harmonisé, sous peine de rendre l'organisation d'un SOC collectif trop complexe. Par ailleurs, il faudra prévoir aussi certaines politiques : p. ex. définir ce qu'est un incident, déterminer la façon de réagir face aux incidents, etc.

- **Créer une Emergency Response Team (« S-CERT »)**
  Les équipes d'intervention qui sont généralement mobilisées en cas d'incident par l'organisme assureur ou les autorités p. ex. ne sont pas toujours familiarisées avec les spécificités du secteur hospitalier. C'est pourquoi le CFEH propose de travailler avec une « Emergency Response Team » spécifique au secteur et susceptible d'être appelée dans ces circonstances. Il s'agit ici d'employés du secteur hospitalier, familiarisés avec les implications d'une attaque et aussi avec les aspects organisationnels d'un hôpital pour apporter un soutien à l'établissement touché. De cette manière, il est également possible d'assurer dans chaque organisation l'approfondissement de connaissances spécifiques. Le partage de connaissances et d'informations entre établissements revêt aussi une importance. La S-CERT (Computer Emergency Response Team pour les Soins) peut travailler en étroite collaboration avec le CERT.be existant, ainsi qu'avec des équipes S-CERT sectorielles de l'étranger. Cette organisation peut aussi servir de base à la mise en commun de compétences plus larges.

- **Éliminer le risque d'inassurabilité**
  Les autorités peuvent prendre des mesures visant à encourager le secteur des assurances à trouver une solution en la matière. Les autorités pourraient aussi envisager de prendre en charge elles-mêmes l'assurance des hôpitaux. Surtout lorsque le secteur entreprend des démarches pour gérer du mieux possible les risques, il est scandaleux de constater que les hôpitaux devraient supporter eux-mêmes l'ensemble des conséquences financières si des incidents surviennent quand même.

- **Envisager des initiatives réglementaires**
  Des initiatives législatives sont en préparation dans différents pays pour dissuader les cybercriminels en supprimant l'incitant financier. Des initiatives de ce genre pourraient également être prises en Belgique. Le CFEH est néanmoins conscient du fait que cela ne relève pas des attributions du ministre de la Santé publique.

- **Coordination**
  Outre le financement des hôpitaux, le CFEH recommande d'investir dans la coordination des initiatives à prendre et décrites ci-dessus. La création d'un cadre, l'identification de l'offre du marché pour les services SOC, ce ne sont là que quelques exemples pour lesquels réunir des groupes de travail ne suffira pas. C'est pourquoi le CFEH préconise le lancement d'un marché pour l'accompagnement de fond et de projets pour les initiatives à prendre.

6. Mécanisme de financement

Une estimation a été réalisée dans le précédent avis concernant les coûts liés aux différentes mesures à prendre dans le développement de la cybersécurité au sein des hôpitaux.

Comme indiqué dans l'introduction, le CFEH tient à souligner à nouveau sa gratitude pour l'apport financier prévu par les autorités, à hauteur de 20 millions d'euros. Néanmoins, le caractère unique dudit investissement est en contradiction avec la continuité qu'il faut garantir, ainsi que la nature cyclique de l'évaluation p. ex. et de la mise à jour du degré de protection. Le CFEH préconise donc un financement structurel, récurrent pour soutenir et développer la cybersécurité dans les hôpitaux.

- Répartition HG-HP a priori

  Le CFEH propose, à l'instar de ce qui se fait pour le financement BMUC, de déterminer cette répartition en fonction de la proportion relative des deux secteurs dans le BMF. Cela correspond à une répartition de 85,5 % (HG) -14,5 % (HP). Cette distribution préalable des moyens disponibles permet d'identifier et de garantir un budget spécifique pour les deux secteurs. En ce qui concerne les autres mécanismes d'allocation, le CFEH ne fait actuellement pas de distinction entre HG et HP.

- Répartition entre les hôpitaux

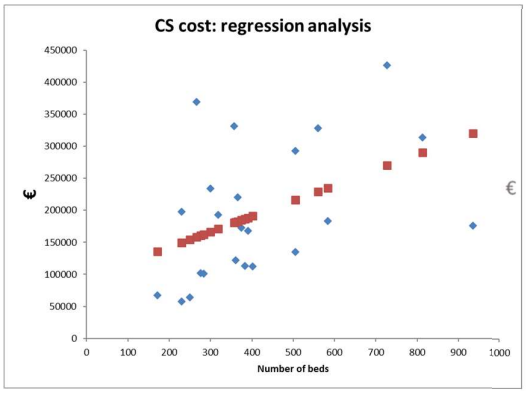
  Étant donné que nous ne disposons pas d'un cadre adapté pour la cybersécurité, il n'est pas possible, à brève échéance, de baser le financement sur un système analogue aux BMUC, à savoir le financement basé sur la réalisation de certaines étapes. Tout comme pour le financement DPI, le CFEH propose de prévoir, dans le cadre de l'affectation du financement à chaque hôpital, une composante fixe (montant fixe par hôpital) et variable (en fonction du nombre de lits) que l'hôpital peut utiliser pour une série d'interventions prédéfinies selon le niveau de maturité. Ceci permettra de couvrir les prochains besoins de l'hôpital et de garantir une mise en œuvre (plus) efficace des moyens. Pour ce faire, les autorités (idéalement en collaboration avec les hôpitaux) doivent établir une liste des actions/interventions qui entrent en ligne de compte. Certaines ont déjà été évoquées :

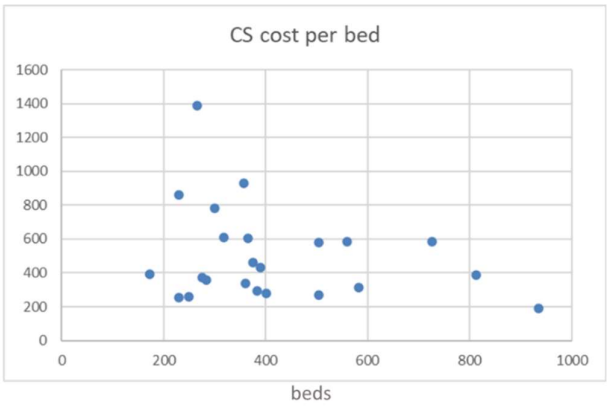
  - Sensibilisation
  - Inventarisation des risques
  - Incident Response Planning
  - SIEM/SOC
  - Interventions techniques/technologiques

  Concernant ces dernières, il n'est pas facile, dans certains cas, de distinguer les interventions qui sont supposées faire partie du développement de l'infrastructure hospitalière, de celles qui sont typiquement nécessaires à la cybersécurité (le back-up en est un bel exemple). Il est par conséquent indispensable de bien argumenter cette nécessité.

- <u>Composante fixe et variable</u>

  L'enquête de Zorgnet-Icuro de 2020 sur les coûts de la cybersécurité donne les graphiques suivants :





  Ces graphiques confirment avant tout la grande différence de maturité (à supposer que l'on puisse quelque peu la déduire des dépenses).

  Il est clair aussi que les hôpitaux de plus petite taille dépensent proportionnellement plus. Le CFEH en conclut que la composante fixe du financement devrait être importante, d'autant plus qu'un pourcentage trop faible risquerait de trop réduire le montant pour les hôpitaux plus petits pour être encore pertinent. Le CFEH propose dès lors de répartir 50 % du budget par secteur au prorata du nombre d'hôpitaux, et 50 % en fonction du nombre de lits et de places.

- <u>Financement à long terme</u>

  Le CFEH propose de fonder le financement à plus long terme sur le cadre à élaborer par analogie avec les BMUC. Ce faisant, la maturité pourra être prise en compte et nous pourrons nous atteler de manière structurelle à la réalisation d'un niveau de maturité minimum pour tous les hôpitaux.