Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren
Conférence des directrices et directeurs cantonaux de la santé
Conferenza delle direttrici e dei direttori cantonali della sanità

Fiche d'information

Étude du Partenariat mondial pour la santé numérique
Cybersécurité

Situation initiale

Fondé en 2018, le Partenariat mondial pour la santé numérique (*Global Digital Health Partnership, GDHP*) est une coopération entre les autorités de différents pays, ainsi qu'avec l'Organisation mondiale de la santé (OMS). Ce partenariat, auquel participe la Suisse, vise à favoriser les échanges sur les meilleures stratégies et pratiques en matière de services de santé numériques afin de générer des connaissances permettant d'améliorer leur mise en œuvre au sein des pays participants. Dans le cadre de cette coopération, des livres blancs ont été rédigés sur divers sujets clés, comme l'« interopérabilité », la « cybersécurité », les « preuves et l'évaluation » et l'« accès des citoyens aux données relatives à leur santé ».

En février 2019, le groupe de travail Cybersécurité du GDHP a lancé le livre blanc intitulé « *Sécuriser la santé numérique : premières réflexions pour orienter les efforts mondiaux en matière de cybersécurité dans le domaine de la santé* » lors du sommet de New Delhi. Depuis la publication de ce rapport, les membres du GDHP ayant pris part aux travaux sur la cybersécurité ont poursuivi leur collaboration pour élaborer un cadre de compétences fondamentales (FCF).

Cette fiche d'information résume les principales conclusions du Rapport 2020 sur la cybersécurité[1]. Les commentaires, les faits et les arguments sont ceux du GDHP.

Objectif de la recherche

Alors que dans la santé, la révolution numérique se poursuit à un rythme soutenu, il convient de s'assurer que les avantages et le potentiel de cette transformation s'accompagnent de la mise en place de systèmes de cybersécurité robustes dans les pays participants. Au vu des stades et degrés de maturité différents dans lesquels se trouvent les participants, et considérant la volonté exprimée de se concentrer sur l'interopérabilité, l'établissement d'un cadre unifié de cyber-compétences est possible et nécessaire. Il convient non seulement de couvrir les éléments traditionnels de la cybersécurité, mais aussi de prêter une attention particulière aux risques posés par les dispositifs médicaux hérités en réseau et à l'émergence de l'Internet des objets médicaux (IdO).

La présente recherche a pour objectif premier d'identifier et de comprendre les champs d'opportunités et de défis communs. Elle fournit également un Cadre de compétences (FCF) qui

[1] Santé numérique mondiale, *2020 Le Partenariat mondial pour la santé numérique lance des livres blancs*, https://www.gdhp.org/gdhp-whitepapers consulté le 21 août 2020.

GCA
Août 2020

Schwarzenburgstrasse 157
CH-3003 Berne

www.e-health-suisse.ch

ehealthsuisse
Kompetenz- und Koordinationsstelle von Bund und Kantonen
Centre de compétences et de coordination de la Confédération et des cantons
Centro di competenza e di coordinamento di Confederazione e Cantoni

représente un outil supplémentaire pouvant être utilisé par les pays participants pour structurer, façonner et évaluer leurs propres programmes, capacités et structures de cybersécurité d'une manière cohérente et prévisible.

Le champ d'application de ce document de recherche couvre sept domaines d'enquête clés. Le questionnaire comporte 59 questions dans ces catégories. Près de la moitié des participants au GDHP ont apporté leur contribution à ce document de recherche qui est donc représentatif de ses membres, contribuant à la fiabilité et à la validité des résultats.

Principales conclusions

Les résultats ont fourni un aperçu à la fois des compétences fondamentales actuelles et des domaines d'amélioration pour les participants au cours des 18 prochains mois.

Maturité actuelle : les catégories où la capacité est la plus faible sont la « Cyber-résilience, continuité des opérations et reprise après sinistre » et la « Résilience et sécurité de la chaîne d'approvisionnement ». Le GDHP reconnaît la nécessité de soutenir les pays affichant les résultats les plus modestes en encourageant les échanges internationaux. La catégorie dans laquelle les résultats sont les meilleurs est « Comprendre la menace stratégique », où de nombreux participants utilisent les capacités et l'expérience nationales dont ils disposent pour accélérer la maturité du secteur de la santé. Le GDHP fournit une plate-forme de partage d'informations sur les menaces, qui a déjà permis de réaliser des progrès importants et doit permettre de soutenir les échanges internationaux.

Maturité prévue dans 18 mois : la « cyber-résilience, la continuité des opérations et la reprise après sinistre » ne sont pas au centre des préoccupations des pays participants. Pourtant, ces éléments sont essentiels à la disponibilité des services dans le domaine de la santé. Par ailleurs, tous les participants prévoient des améliorations significatives dans le domaine de la « Résilience et sécurité de la chaîne d'approvisionnement ».

1. Alignement des résultats cliniques

Les processus de gestion de la sécurité aident à identifier les actifs et les systèmes cliniques critiques. Leur utilisation permet de fixer les priorités pour renforcer la résistance des actifs et des réseaux sur la base des risques identifiés, d'appliquer des contrôles de sécurité et d'atténuer les risques. Les menaces de sécurité dans les milieux de la santé constituent les principaux défis identifiés, ce qui s'explique par la difficulté de diffuser suffisamment rapidement les informations liées à ces menaces sous une forme exploitable permettant une action sur les plans aussi bien technique que stratégique. D'autres défis consistent à sensibiliser et à former les hauts responsables pour les aider à comprendre que le risque de cybersécurité représente un véritable danger commercial stratégique qui, s'il n'est pas traité, peut avoir des conséquences catastrophiques et empêcher la prestation de soins aux patients et les résultats y afférents.

2. Cyber-réponses : préparation et récupération

Tous les pays participants disposent de niveaux d'alerte définis et de niveaux et procédures d'escalade des incidents. Un certain nombre de procédures et de processus de réponse aux incidents suivent, ou s'appuient sur, la réponse à des incidents informatiques traditionnels plutôt que d'être spécifiques à la cybersécurité. Les tests tendent également à être réalisés après des incidents majeurs plutôt que d'être menés régulièrement.

3. Compréhension de la menace stratégique

Tous les pays participants disposent d'équipes spécialisées dans le renseignement sur les menaces pour le secteur de la santé, ce qui permet d'élaborer et transmettre des renseignements plus ciblés et plus spécifiques à des destinataires précis. Bien qu'une majorité des participants disposent de renseignements solides sur les menaces, certains n'ont pas de vision stratégique et précise. L'ensemble des participants bénéficient du soutien des agences et des autorités chargées de l'application des lois ainsi que de groupes consultatifs intersectoriels, mais la nature et l'intensité de la coopération varient d'un participant à l'autre.

4. Cyber-résilience, continuité des opérations et reprise après sinistre

Une réglementation accrue (par exemple, directives européennes) n'améliore pas directement les compétences et, dans certains cas, a pour conséquence involontaire de favoriser une culture de conformité « à la carte » plutôt qu'un changement culturel nécessaire pour faire face à un risque commercial stratégique. Certains pays participants abordent la cyber-résilience, la continuité des opérations et la reprise après sinistre, ainsi que les capacités et contraintes en matière de sécurité par conception au moyen de questions spécifiques.

5. Proportionnalité et efficacité budgétaires et d'investissement

Les pays participants tendent à disposer d'un budget dédié à la cybersécurité pour le domaine de la santé. Celui-ci n'est cependant pas toujours distinct des budgets informatiques, ce qui conduit à des profils d'investissement trop orientés vers la technologie, qui excluent des personnes et éléments clés du processus. Dans d'autres cas, le budget et les investissements en matière de cybersécurité sont gérés par un secteur autre que celui de la santé et sont soumis au contrôle d'un ministère tiers. Bien que cela favorise dans une certaine mesure la mise en commun des ressources financières, cela réduit aussi la flexibilité et le contrôle des autorités sanitaires.

6. Gouvernance, culture et leadership

Il existe un certain chevauchement des responsabilités entre le secteur de la santé et d'autres ministères ou autorités chargées de l'application des lois, ce qui entraîne une certaine confusion ou un manque de clarté en termes de prise de décision et d'appropriation des risques. Il existe des opportunités communes de développer le modèle opérationnel de cybersécurité dans le domaine de la santé à l'échelle du système et au niveau national et de veiller à ce qu'il complète et s'intègre à des structures et des capacités nationales plus larges de cybersécurité. Une nouvelle tendance à nommer des chefs de la sécurité est apparue, mais celle-ci doit s'accompagner d'une formation au niveau du conseil d'administration et de politiques de sensibilisation à l'échelle du système.

7. Résilience et sécurité de la chaîne d'approvisionnement

Des règlementations comme le règlement général de l'UE sur la protection des données ont pour effet de renforcer les contraintes en matière de cybersécurité dans la chaîne d'approvisionnement. Toutefois, un manque de standardisation dans la formulation et la rédaction des clauses et obligations contractuelles a pour effet d'introduire des incohérences et, dans certains cas, d'exonérer le fournisseur de ses responsabilités et obligations.

Les clauses et obligations contractuelles ainsi que la mise en œuvre des protections sont principalement motivées par des préoccupations et des obligations en matière de confidentialité des données plutôt que par la cybersécurité

Maturité prévue dans 18 mois

La cybersécurité reste un sujet sensible. Les États membres ne partagent pas facilement les informations à leur disposition en matière de planification, d'attentes et de faits pour les 18 mois à venir. Cependant, tous s'attendent à améliorer leurs compétences en matière de résultats cliniques, d'évaluation des risques et, en particulier, de gouvernance. Les principales améliorations se concentrent sur la mise en place de nouveaux rôles et d'une nouvelle chaîne de commandement pour la cybersécurité.

Les finances, la cyber-résilience et la reprise après sinistre sont les points faibles des développements futurs. Les raisons de ce dernier point ne sont pas claires. Une hypothèse de travail est cependant que la continuité des opérations et la reprise après sinistre continueront à être « détenues » et pilotées par les processus informatiques traditionnels.

Enfin, les contrats et les produits hérités constituent toujours un défi, mais les participants s'efforcent de veiller à ce que les nouveaux contrats et les renouvellements transmettent les contraintes correctes à la chaîne d'approvisionnement, avec des sanctions appropriées.