HealthCareCAN
Leading. Innovation. Together.

SoinsSantéCAN
Leadership. Innovation. Collaboration.

Bâtir une norme nationale pour la cyberrésilience dans les soins de santé

VUE D'ENSEMBLE

La santé virtuelle, la télémédecine, les dispositifs médicaux et les dossiers de santé électroniques ne sont que certains exemples qui illustrent concrètement comment la transformation numérique dans le secteur des soins de santé remodèle notre système de santé pour le mieux. Toutefois, alors que les soins de santé sont de plus en plus numérisés, automatisés et connectés, l'exposition aux cybermenaces suscite une préoccupation croissante.

Les cybercriminels continuent de profiter des vulnérabilités accrues en raison du travail à distance et de la pression que subissent des secteurs essentiels pour cibler des établissements de soins de santé et demander le paiement de rançons. Le Centre canadien pour la cybersécurité a rapporté 235 incidents liés à des rançongiciels ayant touché des victimes canadiennes du début de janvier au 16 novembre 2021. Selon le Centre, plus de la moitié des victimes œuvraient dans des secteurs essentiels, comme les soins de santé, mais comme seulement les plus grandes attaques sont signalées, les autorités fédérales n'ont pas suffisamment de données sur l'étendue réelle de la menace[1].

[1] Global News, Canadian health, energy sectors increasingly targeted by ransomware attacks. https://globalnews.ca/news/8427930/canadian-health-energy-sectors-increasingly-targeted-by-ransomware-attacks/

Alors qu'elles dépendent de plus en plus des systèmes numériques, les organisations de soins de santé doivent maintenir un haut niveau de confiance envers leur capacité de réagir aux cybermenaces. Grâce à une consultation continue de ses membres et au maintien de solides relations de travail avec Sécurité publique Canada, Santé Canada et l'Agence de la santé publique du Canada, SoinsSanté*CAN* a concentré son travail de sensibilisation dans le domaine de la cybersécurité sur les points suivants :

- sensibiliser davantage à la cybersécurité dans le secteur des soins de santé :
- accroître les ressources pour renforcer les capacités;
- élaborer des normes nationales pour la cybersécurité dans les organisations de soins de santé[2].

SoinsSanté*CAN* continue de plaider en faveur d'une attention et d'un investissement accrus dans la cybersécurité dans le domaine des soins de santé, mais l'absence de normes claires est reconnue comme un obstacle à la cyberrésilience dans les établissements du Canada. Pour remédier à cette situation, SoinsSanté*CAN* collabore avec le Conseil stratégique des DPI avec le soutien du Programme de coopération en matière de sécurité de Sécurité publique Canada dans le double objectif suivant :

- élaborer un nouvel ensemble de normes en appui à la cyberrésilience dans le système de soins de santé du Canada; et
- faciliter les occasions de partage de l'information en ciblant le personnel des soins de santé qui offre des soins directs.

L'établissement d'un cadre de travail clair et le renforcement des capacités en matière de cybersécurité auront pour effet de mieux protéger les organisations de soins de santé du Canada contre le cybercrime et leur permettront de réagir plus efficacement aux menaces changeantes et de défendre les infrastructures essentielles.

COMPRENDRE LE PAYSAGE DE LA CYBERMENACE

En tant que porte-parole national des organisations de soins de santé et des hôpitaux du Canada, SoinsSanté*CAN* continue de réunir avec succès des partenaires et des parties prenantes clés pour discuter de l'évolution du paysage de la cybermenace pour les organisations de soins de santé du Canada. Nous orientons nos efforts sur les points suivants :

- mieux faire comprendre le paysage actuel et évolutif de la cybermenace dans le système de soins de santé du Canada;
- accroître les occasions d'améliorer la cyberrésilience et d'atténuer le risque pour les organisations de soins de santé;
- analyser les initiatives de prévention et d'atténuation en cours au Canada.

L'utilisation des technologies de l'information et des communications augmente rapidement dans le secteur de santé. Pourtant, le degré de préparation en matière de sécurité varie considérablement dans le secteur, même si l'on reconnaît l'importance cruciale d'une sensibilisation de base et d'une évaluation. Entre-temps, bien des organisations déclarent subir régulièrement des cyberattaques de divers types.

Le contexte actuel permet de croire que les organisations de soins de santé sont très vulnérables aux cyberattaques et les données indiquent que le secteur de la santé est une cible de plus en plus prisée pour plusieurs facteurs déterminants :

- renseignements personnels;
- ressources financières;

[2] SoinsSanté*CAN*, COVID-19 et cybersécurité : Le confinement n'a pas arrêté les cybercriminels. https://www.healthcarecan.ca/wp-content/themes/camyno/assets/document/PolicyDocs/2020/HCC/FR/PolicyBrief-COVIDCybersecurity_FR.pdf

- grande visibilité et grand impact;
- pression reliée à la pandémie[3].

Une vaste consultation auprès de ses membres et d'autres intervenants clés a permis à SoinsSanté*CAN* d'identifier un certain nombre d'opportunités pour améliorer la cyberrésilience. L'une des principales recommandations qui en découlent porte sur un engagement à favoriser une culture de la cybersécurité dans le système de santé du Canada par des normes cohérentes et l'adoption d'une approche systématique à la sensibilisation du secteur de la santé aux cyberrisques et à leur atténuation.

BESOINS SPÉCIFIQUES DU SECTEUR DES SOINS DE SANTÉ DANS L'ÉLABORATION D'UNE NORME NATIONALE

La promotion de la résilience des infrastructures essentielles suppose l'élaboration de normes de cybersécurité nationales spécifiques au secteur pour que les organisations de soins de santé puissent remédier à leurs vulnérabilités et se préparer à de futurs incidents.

Les 9 et 10 mars 2022, SoinsSanté*CAN* et le Conseil stratégique des DPI ont tenu conjointement une série d'ateliers dans les deux langues officielles dans l'objectif de recueillir les commentaires des leaders de la technologie des soins de santé de tout le pays sur leurs préoccupations, leurs problèmes et leurs besoins en matière de cybersécurité. Ces commentaires guideront l'élaboration d'une Norme nationale pour la cyberrésilience dans les soins de santé au Canada.

Quelque 120 leaders des technologies de la santé de tout le Canada ont participé à ces ateliers, y compris des responsables au sein d'organisations membres de SoinsSanté*CAN.* On leur a demandé de répondre aux cinq questions suivantes :

- Quel est votre principal sujet d'inquiétude si vous devenez la cible d'une cyberattaque?
- Quel est le plus grand risque pour le système de santé aujourd'hui?
- Quel(s) domaine(s) d'intérêt aimeriez-vous voir inclus dans une norme nationale du Canada?
- Quels sont les facteurs de réussite concernant l'élaboration et la mise en œuvre d'une norme nationale pour la cybersécurité du système de santé canadien?
- Votre organisation utilise-t-elle actuellement ou cherche-t-elle à adopter une norme reconnue en matière d'information et de cybersécurité?

Les participants aux ateliers ont identifié les soins aux patients, la sécurité, la protection de l'information sur la santé et la capacité d'assurer la continuité des soins comme certains des domaines d'inquiétude les plus importants. Ils ont également estimé qu'une approche pancanadienne spécifique aux soins de santé serait nécessaire pour traiter des facteurs de risque les plus courants pour les organisations de soins de santé, notamment les rançongiciels, les infrastructures de TI existantes, le manque de financement, l'engagement des dirigeants et les normes.

Comme bien des organisations auront besoin de ressources additionnelles pour mettre en œuvre un tel programme, les participants ont estimé qu'une approche par paliers assurerait l'accessibilité à toutes les organisations du système de soins de santé du Canada. Les participants ont insisté sur l'importance d'une formation approfondie pour le personnel de première ligne et le personnel clinique et de mesures de soutien à l'application des connaissances.

Le rapport final de ces groupes de discussion est disponible ici.

[3] SoinsSanté*CAN*. Cybersafe Healthcare: Options for Strengthening Cybersecurity in Canada's Health Sector. https://www.healthcarecan.ca/wp-content/themes/camyno/assets/document/Cyber%20Security/Options%20Brief%20Summit%20Report.pdf

CRÉER UNE CULTURE DE LA CYBERHYGIÈNE

Une vaste consultation menée auprès des membres de SoinsSanté*CAN*, de partenaires clés et de parties prenantes révèle une variation importante du niveau de cyberrésilience et de préparation parmi les organisations de soins de santé du Canada. L'élaboration d'un nouvel ensemble de normes pour soutenir la cyberrésilience du système de santé du Canada assurera une préparation cohérente des organisations de soins de santé de tout le pays. L'élaboration de matériel d'application des connaissances soulignera pour sa part l'importance de la cyberhygiène pour tous les employés et leur donnera les connaissances nécessaires pour éviter les menaces les plus courantes et les plus graves en leur permettant de réagir en cas d'attaque des systèmes.

Lors de l'élaboration des ressources éducatives et du matériel d'application des connaissances, il sera important d'envisager divers formats de formation et d'activités pour maintenir l'engagement et la sensibilisation des personnes, y compris :

- les cours et la formation
- les exercices pratiques et les simulations
- les vidéos, les affiches et les organigrammes
- les tables rondes, les ateliers et les webinaires
- les publications scientifiques

L'amélioration de la cyberhygiène est essentielle pour que les organisations de soins de santé puissent se protéger contre les atteintes à la sécurité et les cyberattaques. L'élaboration de programmes de formation et de ressources complets sur les meilleures pratiques, politiques et procédures en matière de cybersécurité aidera les organisations de soins de santé du Canada à maintenir un haut niveau de confiance dans leur capacité de réagir aux cybermenaces.

PROCHAINES ÉTAPES

Le Conseil stratégique des DPI et SoinsSanté*CAN* sont en train de former un comité technique d'experts de la cybersécurité provenant d'organisations privées, publiques et gouvernementales et d'institutions membres de SoinsSanté*CAN*. Ce comité sera chargé de créer la norme nationale sur la cyberrésilience dans les soins de santé. SoinsSanté*CAN* et le Conseil stratégique des DPI créeront également du matériel d'application des connaissances et lanceront une campagne de sensibilisation des fournisseurs lors d'événements clés. Les membres de SoinsSanté*CAN* seront consultés pendant l'élaboration de ce matériel et auront l'occasion de fournir leurs commentaires sur la norme et le matériel d'application des connaissances.

POUR UN SUPPLÉMENT D'INFORMATION

Si vous avez des questions, des commentaires, ou si vous souhaitez discuter de ces questions ou vous impliquer davantage, veuillez communiquer avec :

Siri Chunduri
Analyste des politiques et de la recherche
schunduri@healthcarecan.ca

Jonathan Mitchell
Vice-président, Recherche et politiques
jmitchell@healthcarecan.ca

Merci à Claire Samuelson-Kiraly, consultante, SoinsSantéCAN.