COVID-19 ET CYBERSÉCURITÉ

Le confinement n'a pas arrêté les cybercriminels

VUE D'ENSEMBLE

La pandémie de COVID-19 a entraîné une augmentation bien accueillie des soins virtuels à la grandeur du Canada, mais avec un effet secondaire regrettable : le secteur des soins de santé est maintenant encore plus vulnérable aux menaces de cybersécurité. Récemment, les services de renseignements sur la cybersécurité du Royaume-Uni, des États-Unis et du Canada ont désigné les services de renseignements de la Russie comme étant responsables du ciblage d'organisations menant des recherches sur des vaccins. Toutes les agences nationales de cybersécurité continuent de lancer des signaux d'alarme en indiquant que les renseignements liés à la pandémie constituent une cible prioritaire. SoinsSanté*CAN* a examiné les incidences pour ses membres en vue de leur fournir une feuille de route qui peut atténuer ce risque émergent et de déterminer les prochaines étapes cruciales.

LA PANDÉMIE A ACCRU LES RISQUES DE CYBERSÉCURITÉ

La pandémie de COVID-19 a changé le monde tel que nous le connaissons. Elle a entraîné une expansion massive des soins primaires virtuels dans tout le Canada[1] et plus de la moitié des visites des patients chez les prestataires de soins de santé se sont déroulées sous forme virtuelle[2]. L'Association médicale canadienne a récemment publié les résultats d'un sondage qui révèle que parmi les 1 800 Canadiens interviewés, 91 % ont déclaré être satisfaits des services de soins virtuels et 42 % préféreraient continuer à y recourir[3] une fois la crise pandémique passée.

SoinsSanté*CAN* a effectué un sondage auprès de ses membres en avril 2020 pour connaître leurs besoins immédiats concernant les soins virtuels pendant la pandémie de COVID-19. Leurs réponses ont souligné l'importance d'accroître les structures de soutien. Ils ont cerné plusieurs lacunes et ont notamment suggéré :

- l'intégration avec les dossiers médicaux informatisés;
- un meilleur partage entre les plateformes et les bases de données régionales;
- une augmentation des investissements dans les infrastructures;
- l'expansion des ressources aux communautés rurales et isolées.

Alors que les services de soins virtuels continuent d'augmenter au sein de notre système de santé, les organisations de soins de santé doivent améliorer leurs capacités de cybersécurité. Il est également crucial que le secteur des soins de santé réalise que la cybersécurité n'est pas seulement une question de TI. Une intrusion dans les installations de soins de santé peut avoir des incidences sur l'intégrité, la confidentialité et la disponibilité de renseignements vitaux (p. ex., les dossiers des patients, les rendez-vous, les horaires de garde des médecins, la réservation des salles d'opération, etc.), ce qui fait de la sécurisation des infrastructures essentielles une question d'affaires urgente.

Les prestataires de soins de santé ont accès à d'énormes quantités de données sensibles qui sont attrayantes pour les acteurs malicieux. Parmi les cyberattaques les plus courantes, mentionnons :

- **Piratage :** Un terme qui décrit généralement la tentative d'une tierce partie de compromettre des appareils numériques et qui peut englober l'utilisation de l'une ou l'autre des tactiques décrites ci-dessous.
- **Hameçonnage et harponnage :** Une tentative visant à obtenir des données personnelles, des renseignements bancaires et d'autres renseignements sensibles par imitation ou usurpation d'une marque spécifique, généralement bien connue. Les pirates informatiques peuvent alors utiliser les renseignements pour commettre des actes frauduleux. Le harponnage est très ciblé sur une personne en particulier et souvent, le courriel corrompu semble provenir d'une source fiable et contient des renseignements personnalisés.
- **Rançongiciel :** Un type de maliciel (logiciel malveillant, virus, vers, etc.) qui empêche un utilisateur d'accéder à un système ou à des données jusqu'au paiement d'une somme d'argent.

[1] Lignes directrices sur la télémédecine et les soins virtuels (et autres ressources cliniques sur la COVID-19). Consulté à : http://www.royalcollege.ca/rcsite/documents/about/covid-19-resources-telemedicine-virtual-care-f

[2] Réaction rapide à la crise de la COVID-19. Consulté à : https://infoway-inforoute.ca/fr/solutions/reaction-rapide-a-la-crise-de-la-covid-19

[3] Les soins virtuels sont de vrais soins : un sondage national indique que les Canadiens sont pleinement satisfaits des soins de santé virtuels. Consulté à : https://www.cma.ca/fr/actualites/les-soins-virtuels-sont-de-vrais-soins-un-sondage-national-indique-que-les-canadiens

- **Déni de service (DS) ou attaque par déni de service distribué (ADSD) :** Toute activité qui rend un service indisponible pour les utilisateurs légitimes (par ex., la prise de rendez-vous) ou qui retarde les opérations et les fonctions du système. Alors qu'une attaque de DS utilise un seul dispositif pour monter l'attaque, l'ADSD utilise plusieurs dispositifs pour attaquer une cible, par exemple, en faisant planter un site Web en le submergeant par un trafic excessif de multiples dispositifs.
- **Pulvérisation des mots de passe :** Une attaque qui tente d'obtenir l'accès non autorisé à un grand nombre de comptes en essayant quelques mots de passe couramment utilisés.
- **Exploitation de failles importantes :** Exploitation des erreurs de configuration et de l'utilisation de logiciels non corrigés. Ce type de cyberattaque est particulièrement préoccupant en période de pandémie de COVID-19, car les entreprises se sont empressées de fournir à leur personnel de nouveaux moyens de travailler à distance[4].

SOINSSANTÉ*CAN* SE FAIT LE CHAMPION DE LA RÉSILIENCE EN MATIÈRE DE CYBERSÉCURITÉ

SoinsSanté*CAN* reconnaît l'importance de promouvoir la résilience des infrastructures essentielles et la cybersécurité. La pandémie a entraîné une augmentation soudaine du nombre de personnes qui travaillent à distance, sans avoir le filet de sécurité des TI de leur organisation (p. ex, infrastructures, pare-feu, politiques, etc.), ce qui rend encore plus probables les risques de violation de la cybersécurité. Le secteur des soins de santé est confronté aux défis additionnels liés à l'utilisation de technologies anciennes, au manque de financement et de ressources et au manque de directives et de soutien des pouvoirs publics et du secteur. Nous collaborons avec plusieurs organisations pour nous tenir au courant de la situation actuelle et atténuer les risques pour nos membres.

En 2019, avec notre membre Eastern Health in Newfoundland and Labrador et notre partenaire, la **Fondation Canada-Israël pour la recherche et le développement industriel (FCIRDI)**, nous avons organisé l'Échange Canada-Israël sur la cybersécurité en santé à St. John's. L'Échange a été créé comme outil pour atténuer les lacunes en cybersécurité en renforçant la collaboration entre des experts techniques israéliens, des partenaires de l'innovation canadiens (p. ex., Telus, Becton, Dickson and Company, communément appelée BD, ou GE Santé), des leaders du système de santé et des gouvernements provinciaux et territoriaux. Le programme de l'événement était axé sur deux objectifs :

- sensibiliser aux divers domaines de la cybersécurité et à la manière dont ils s'intègrent dans les soins de santé; et
- établir des liens entre les besoins locaux et l'expertise des entreprises canadiennes et israéliennes pour encourager les partenariats qui répondent à ces besoins.

L'Échange a mis en lumière nombre de nos vulnérabilités en matière de cybersécurité et certains experts ont souligné que si l'investissement optimal en cybersécurité se situe entre 9 et 14 % de tout le budget de TI, l'investissement réel se situe en moyenne à près de 6 %. Les experts ont également souligné que sur la scène mondiale, la croissance du nombre et des coûts des cyberattaques est importante et ne cesse d'augmenter. Parmi les secteurs d'activité visés, les soins de santé se classent constamment aux premier, deuxième ou troisième rangs sur le plan du volume d'attaques. Le coût global des attaques augmente dans

[4]Cybermenaces pesant sur les organismes de santé canadiens. Consulté à : https://cyber.gc.ca/fr/avis/cybermenaces-pesant-sur-les-organismes-de-sante-canadiens

les deux chiffres chaque année. Mais le budget de sécurité des établissements a eu tendance à rester le même[5].

Nous représentons le secteur de la santé au **Forum national intersectoriel sur les infrastructures essentielles (FNIIE**). Dans le cadre de ce forum, nous travaillons au maintien d'une approche canadienne exhaustive et collaborative aux infrastructures essentielles en fournissant un mécanisme directeur pour la discussion et l'échange d'information au sein des gouvernements fédéral, provinciaux et territoriaux et des secteurs des infrastructures essentielles et entre eux.

Nous collaborons également étroitement avec le **Centre canadien pour la cybersécurité (CCC)** pour rester au courant des menaces actuelles en matière de cybersécurité et nous participons à un appel hebdomadaire sur la COVID-19 avec des organisations pancanadiennes de la santé. Le CCC prévient que les tentatives de pénétration du réseau (hameçonnage, piratage, pulvérisation des mots de passe, etc.) sont en hausse. Il prévient également que des criminels pourraient profiter de la pression accrue exercée sur les organisations canadiennes de la santé en réponse à la pandémie pour obtenir des paiements de rançons ou dissimuler d'autres compromis. Pour témoigner de la rapidité avec laquelle les cybercriminels tirent parti d'une situation qui évolue rapidement, le CCC souligne que lorsque le gouvernement fédéral canadien a annoncé l'introduction d'une application de traçage de contacts, le CCC a presque immédiatement identifié un rançongiciel « CryCrypter » se faisant passer pour la prétendue application.

En mai 2020, le CCCS a indiqué qu'il avait reçu de l'information de la Cybersecurity and Infrastructure Security Agency (CISA) des États-Unis et du National Cyber Security Centre (NCSC) du Royaume-Uni concernant les efforts continus des groupes de menace persistante avancée (APT) pour cibler les organisations impliquées dans la réponse à COVID-19. Le CCC a évalué que des acteurs de menaces sophistiquées peuvent tenter de voler la propriété intellectuelle d'organismes engagés dans la recherche et le développement liés à COVID-19, ou des données sensibles liées à la réponse du Canada à COVID-19. La menace ciblait notamment la recherche et le développement de vaccins et de médicaments par des sociétés pharmaceutiques et la collecte d'informations personnelles en vrac auprès d'organismes de soins de santé. Dans un développement stupéfiant, le groupe APT29 a récemment été relié aux agences de renseignement russes. Ce groupe a déjà été reconnu responsable du piratage de partis politiques aux États-Unis et en Norvège. Ses membres utilisent diverses tactiques telles que l'hameçonnage et l'exploitation des failles des logiciels, mais ils savent s'adapter très rapidement, ce qui rend la vigilance en matière de cybersécurité d'autant plus importante[6].

NOS OBJECTIFS

SoinsSanté*CAN* plaide en faveur d'une meilleure sensibilisation et d'une attention accrue aux lacunes en matière de cybersécurité dans les soins de santé, tant auprès de ses membres que dans le cadre de ses solides relations de travail avec Sécurité publique Canada, Santé Canada et l'Agence de la santé publique du Canada. Nous nous efforçons également de fournir de l'information et de partager les meilleures pratiques de renforcement de la cybersécurité dans le secteur de la santé. Pour améliorer la protection des renseignements sensibles et privés et fournir les services essentiels exempts de cyberattaques, nous devons de toute urgence :

1. **Porter une plus grande attention à la cybersécurité dans le secteur des soins de santé.** La sensibilité des renseignements des soins de santé et l'escalade des cyberattaques en font un secteur d'une importance cruciale qui est largement ignoré. Le paysage de la menace et son impact sur le fonctionnement des services de santé doivent être communiqués clairement et de toute urgence.

[5] Données provenant d'un expert lors de l'Échange Canada-Israël sur la cybersécurité en santé.
[6] Déclaration du CST sur les menaces visant le développement d'un vaccin contre la COVID-19 - Jeudi 16 juillet 2020. Consulté à : https://cse-cst.gc.ca/fr/media/2020-07-16

2. **Accroître les ressources pour renforcer les capacités.** Les organisations de soins de santé ont besoin d'un plus grand investissement du gouvernement fédéral pour les aider à évaluer les risques, à créer un centre de gestion de la sécurité centralisé, à fournir de la formation aux employés, à améliorer la résilience en matière de cybersécurité et à utiliser de meilleures pratiques de cyberdéfense.
3. **Élaborer des normes nationales pour la cybersécurité dans les organisations de soins de santé.** Nous avons continué de plaider vigoureusement pour l'élaboration de normes nationales de cybersécurité dans les organisations de soins de santé. Ces efforts sont devenus encore plus essentiels avec l'augmentation des soins virtuels et du nombre de personnes qui travaillent à distance.

FEUILLE DE ROUTE POUR NOS MEMBRES

SoinsSanté*CAN* continue de suivre étroitement cette menace pour notre secteur qui évolue rapidement et a formulé des questions clés que devraient se poser les organisations de soins de santé comme point de départ des discussions sur la cybersécurité avec leurs équipes de cadres supérieurs :

1. Y a-t-il un dialogue actif et efficace au sein de votre organisation entre le conseil d'administration, la direction et l'équipe de cybersécurité pour déterminer où se crée la valeur dans l'organisation, où sont les actifs essentiels et quelle est leur vulnérabilité face aux principales menaces?
2. Avec l'expansion des soins virtuels, considérez-vous la cybersécurité sous un angle qui englobe toute l'entreprise?
3. Dans votre organisation, la protection des renseignements essentiels est-elle considérée comme une question de TI plutôt que comme une bonne pratique d'affaires?
4. Êtes-vous à la recherche de nouvelles façons d'investir dans la cybersécurité pour atténuer les risques?
5. Vous demandez-vous comment vous pourriez porter à l'attention des gouvernements provinciaux et territoriaux le fait qu'il faut accroître le financement pour la cybersécurité?
6. Comment SoinsSanté*CAN* peut aider votre organisation à répondre à ces besoins de cybersécurité d'un point de vue politique ou de défense des intérêts?

POUR UN SUPPLÉMENT D'INFORMATION

SoinsSanté*CAN* informera ses membres de tout développement dans ce dossier. Si vous avez des questions ou des commentaires, ou si vous souhaitez discuter de préoccupations particulières en matière de cybersécurité, n'hésitez pas à communiquer avec nous.

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

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