LA CYBERSÉCURITÉ ET LES DISPOSITIFS MÉDICAUX CONNECTÉS

CANADIAN CENTRE FOR CYBER SECURITY

OCTOBRE 2021 | ITSAP.00.132

Les dispositifs médicaux connectés à Internet peuvent sauver la vie des personnes qui les utilisent, notamment grâce à l'administration de médicaments, à la régulation du rythme cardiaque et au suivi de la tension artérielle. Malgré ces bienfaits, la connexion à Internet peut exposer ces dispositifs à des cybermenaces, ce qui risque de nuire à leur performance et de faire du tort aux patients.

POURQUOI LES DISPOSITIFS MÉDICAUX SONT-ILS CIBLÉS?

Les auteurs de menace ciblent les dispositifs médicaux pour diverses raisons, par exemple pour accéder aux systèmes de soins de santé, recueillir les données qui y sont stockées ou analyser des technologies brevetées. Ces dispositifs contiennent des renseignements médicaux sensibles et se connectent souvent aux systèmes et réseaux d'organismes de soins de santé dans lesquels sont stockées des données financières et de recherche. Les auteurs de cybermenace peuvent se servir de ces renseignements pour commettre des cybercrimes ou encore les vendre à des fins inappropriées.

COMMENT LES AUTEURS DE MENACE CIBLENT-ILS LES DISPOSITIFS MÉDICAUX?

Les auteurs de menace peuvent compromettre les dispositifs médicaux connectés à Internet, y compris les dispositifs portables et ceux qui assurent le suivi de la santé. Voici quelques exemples de la manière dont les dispositifs médicaux peuvent être ciblés:

- Un auteur de menace pourrait compromettre les capacités de contrôle à distance, comme celles des pompes à insuline, pour prendre le contrôle du dispositif.
- Un auteur de menace pourrait utiliser les fonctionnalités de communication sans fil servant à transmettre des données à des fournisseurs de soins de santé, comme celles qu'on retrouve dans les stimulateurs cardiaques et les défibrillateurs implantables, pour accéder au dispositif et aux données qui y sont stockées.
- Un auteur de menace pourrait également manipuler des logiciels ou des micrologiciels obsolètes, notamment dans les tomodensitogrammes et les appareils d'imagerie par résonance magnétique, dans le but de les compromettre à des fins malveillantes.
- Les réseaux d'organismes de soins de santé peuvent également être compromis par l'entremise de dispositifs médicaux ou de techniques de cyberattaque conventionnelles.
- Il est possible de compromettre les dispositifs médicaux dont les contrôles d'accès sont faibles, dont les justificatifs d'identité sont codés en dur ou qui ne comportent aucun facteur d'authentification en passant par les dispositifs connectés.

QUELLES SONT LES RÉPERCUSSIONS?

Les cyberattaques ciblant les dispositifs médicaux peuvent entraîner des conséquences dévastatrices, voire mettre la vie des patients en danger. Il importe que les fabricants, les organismes de soins de santé, les fournisseurs de services infonuagiques (FSI) et les patients comprennent les risques associés à ces dispositifs et les mesures à prendre pour les sécuriser.

FABRICANTS DE DISPOSITIFS MÉDICAUX

Les fabricants devraient effectuer des évaluations des risques préalables à la mise en marché pour faire face aux risques en matière de cybersécurité. En l'absence d'une telle évaluation, les fabricants risquent de se voir refuser une licence pour la commercialisation du produit. Une fois le dispositif sur le marché, il revient aux fabricants de surveiller et d'atténuer les éventuels risques pour la sécurité, d'assurer la maintenance et de fournir régulièrement les mises à jour nécessaires pour corriger les vulnérabilités tout au long du cycle de vie du dispositif. Le défaut d'atténuer ces risques pourrait donner lieu à des problèmes juridiques et à des pertes financières.

FOURNISSEURS DE SERVICES INFONUAGIQUES (FSI)

Les FSI sont responsables de l'accessibilité, de l'intégrité et de la sécurité des données stockées sur leurs plateformes. Il convient de veiller à ce que la transmission de données depuis des dispositifs vers les plateformes ou les logiciels dans le nuage soit sécurisée et reste conforme aux lois sur la protection de la vie privée. Le défaut de le faire pourrait entraîner la perte ou la violation de données et des poursuites judiciaires.

ORGANISMES DE SOINS DE SANTÉ

Les organismes de soins de santé doivent faire preuve de diligence raisonnable au moment de se procurer des dispositifs médicaux. Des cyberattaques et des virus informatiques pourraient toucher l'ensemble d'un réseau de soins de santé, ce qui risque de compromettre les données cliniques, les renseignements médicaux et les initiatives de recherche exclusive. Il convient également de veiller à ce que les dispositifs achetés soient pris en charge à long terme, notamment au moyen de correctifs pour les logiciels et les vulnérabilités.

PATIENTS

La santé des patients risque d'être mise en péril par des cyberattaques ciblant les dispositifs médicaux, comme les dispositifs portables et les appareils de surveillance de la santé. La compromission des dispositifs de patients risque de nuire à la fonctionnalité de l'appareil, aux données transmises aux fournisseurs de soins de santé et aux notifications d'urgence.

ÉTUDES DE CAS

- **NOTPETYA 2017:** Cette attaque par rançongiciel a verrouillé les lecteurs de machines qui tournaient sur un système d'exploitation particulier. Bien que l'équipement médical n'ait pas été infecté, les ordinateurs permettant de consulter les données et les images provenant de ces machines n'étaient plus accessibles. NOTPETYA a causé des dommages de 10 milliards de dollars à l'échelle mondiale et retardé la prestation de services médicaux à des patients pendant des semaines.
- **WANNACRY 2017:** Cette attaque par rançongiciel a paralysé le National Health Service (NHS), l'organisme national de soins de santé du Royaume-Uni. Elle a nui à la capacité du NHS de voir des patients et d'effectuer des interventions médicales. Aux États-Unis, de l'équipement de radiologie a également été touché, ce qui a compromis la capacité de certains hôpitaux de fournir des soins à des patients.
- **UNIVERSAL HEALTH SERVICES (UHS) 2020**: Lors de cette attaque par rançongiciel, le réseau complet du fournisseur UHS aux États-Unis a été mis hors service et l'ensemble des données et des systèmes n'étaient plus accessibles. Plus de 400 organismes de soins de santé ont été touchés par le rançongiciel, ce qui a entraîné des pertes de revenus de 67 millions de dollars. UHS a mis trois semaines à se remettre de cette attaque.
- **BLUETOOTH À BASSE CONSOMMATION (BLE) 2020:** Santé Canada a publié un avis dans lequel il annonçait que des dispositifs médicaux dotés de puces BLE, comme des stimulateurs cardiaques, des glucomètres et des pompes à insuline, pouvaient être vulnérables à des cyberattaques. Les auteurs de menace qui réussissent de telles cyberattaques pourraient bloquer les dispositifs, les déverrouiller ou contourner les mesures de sécurité pour accéder à des fonctionnalités qui ne devraient être accessibles qu'aux utilisateurs autorisés.

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

COMMENT PUIS-JE PROTÉGER MON ORGANISATION?

Les fabricants, les organismes de soins de santé et les patients ont tous la responsabilité de sécuriser les dispositifs médicaux connectés. Comme un grand nombre de dispositifs sont maintenant basés sur l'infonuagique et en raison des liens étroits entre les dispositifs médicaux et les réseaux auxquels ils sont connectés, les fournisseurs de services infonuagiques (FSI) sont responsables de la sécurité de ces dispositifs. Le tableau ci-dessous présente les mesures que peuvent prendre les fabricants, les FSI et les organismes de soins de santé pour mieux protéger les dispositifs médicaux contre les cyberattaques. Ces mesures reposent sur les exigences, les règlements et les recommandations de Santé Canada. Pour en savoir plus, consultez la page Web sur les instruments médicaux de Santé Canada.

Recommandations pour les fabricants et les FSI	Recommandations pour les organismes de soins de santé
MaGérer les risques : Créez un processus de gestion des risques liés à la cybersécurité en parallèle avec vos processus habituels de gestion des risques pour les dispositifs. Lorsqu'un risque est atténué dans le cadre d'un des processus, il convient de tenir compte des effets de cette atténuation sur l'autre processus. Par exemple, le fait d'ajouter une connexion réseau sur un dispositif sans contrôle de sécurité n'aura probablement pas d'incidence sur la sécurité physique, mais cette connexion peut servir de vecteur d'attaque aux auteurs de cybermenace.	**Protéger le périmètre :** Prenez des mesures de sécurité, comme installer des pare-feux, des antivirus et des antimaliciels sur tous vos réseaux. Segmentez le réseau et envisagez de créer des réseaux invités et opérationnels.
Sécuriser la conception : Intégrez des contrôles de cybersécurité à la phase de conception du processus de développement. Envisagez l'ajout d'une option de commande manuelle permettant aux patients de prendre le contrôle du dispositif dans l'éventualité d'une menace pour leur sécurité. Les choix de conception devraient maximiser la cybersécurité sans nuire à la sûreté du dispositif. Élaborez un plan de gestion du cycle de vie pour les dispositifs afin de pouvoir accorder un soutien aux organismes, appliquer des mises à jour, corriger les vulnérabilités et mettre hors service les dispositifs obsolètes.	**Sécuriser les dispositifs :** Protégez vos systèmes et dispositifs au moyen de phrases de passe et de mots de passe forts. Utilisez une phrase de passe ou un mot de passe différent pour chaque dispositif et chaque compte. Sécurisez vos comptes et vos dispositifs avec une authentification multifacteur. Si l'authentification multifacteur est activée, il faudra utiliser deux facteurs d'authentification distincts ou plus pour déverrouiller un dispositif ou se connecter à un compte. Envisagez également de chiffrer vos dispositifs, surtout s'ils contiennent de l'information sensible ou s'ils y accèdent. Enfin, appliquez les correctifs et les mises à jour dès qu'elles sont disponibles afin de tenir à jour vos systèmes d'exploitation.
Vérifier et valider les dispositifs : Testez vos dispositifs pour vous assurer que leur comportement et leur performance sont conformes aux exigences de conception. Effectuez des tests de cybersécurité, comme les tests d'intrusion et l'analyse des vulnérabilités, afin de démontrer que le dispositif répond aux exigences de cybersécurité.	**Établir le cadre :** Créez des politiques et procédures de sécurité afin de protéger vos données et de gérer l'utilisation des renseignements médicaux. Envisagez d'appliquer le principe de droit d'accès minimal, c'est-à-dire accorder aux utilisateurs uniquement les autorisations d'accès dont ils ont besoin pour accomplir les tâches autorisées.
Surveiller les dispositifs déployés : Assurez le suivi et le signalement de toute vulnérabilité qui risque de nuire au dispositif médical. Fournissez régulièrement des correctifs et des mises à jour pour veiller à ce que vos dispositifs soient sécurisés et à ce qu'aucune vulnérabilité exploitable ne s'y trouve. Envisagez d'intégrer un mécanisme de mise à jour logicielle au dispositif lors de sa conception.	**Créer une culture de sécurité**Fournissez à votre personnel de la formation sur la cybersécurité et la protection des renseignements personnels et sensibilisez les utilisateurs aux cybermenaces qui risquent de toucher les dispositifs et les renseignements médicaux qu'ils contiennent. Mettez l'accent sur le fait que chaque membre de votre organisation est responsable de protéger l'information sensible. Pour obtenir des renseignements utiles à ce sujet, consultez le site Web Pensez cybersécurité.
Sécuriser les plateformes : Mettez en œuvre les contrôles de sécurité et de confidentialité nécessaires dans vos plateformes infonuagiques pour assurer la protection des données et des dispositifs des clients. Par exemple, veillez à mettre en place un processus de sauvegarde robuste et à appliquer l'authentification multifacteur à l'ensemble des systèmes et des applications pour assurer l'intégrité et la sécurité des données. Advenant la compromission de l'infrastructure infonuagique, les dispositifs ou leurs réseaux pourraient être infectés.	**Gérer les biens :** Sauvegardez votre information dans un emplacement de stockage sécurisé (p. ex. un disque dur externe ou un service de sauvegarde dans le nuage) qui n'est pas connecté à votre réseau. Mettez hors service tous les dispositifs qui ne sont pas pris en charge, dans la mesure du possible. Les dispositifs qui ne sont plus pris en charge ne reçoivent plus les correctifs et les mises à jour du fournisseur et sont donc vulnérables aux cybermenaces.

Contrôle Canadien des Dispositifs Médicaux

- Santé Canada examine les dispositifs médicaux pour en évaluer la sécurité, l'efficacité et la qualité avant d'en autoriser la vente au Canada.
- Le Bureau des matériels médicaux de la Direction des produits thérapeutiques (DPT) est l'organisme national qui contrôle et évalue la sûreté, l'efficacité et la qualité des matériels médicaux utilisés à des fins diagnostiques et thérapeutiques au Canada. Pour en savoir plus sur le rôle de ces organismes, consultez le feuillet d'information *Sûreté des matériels médicaux vendus au Canada*.
- Les fabricants de dispositifs canadiens sont assujettis au *Règlement sur les instruments médicaux* adopté en vertu de la *Loi sur les aliments et drogues*.
- Santé Canada a établi des lignes directrices sur *les exigences relatives à la cybersécurité des instruments médicaux avant leur mise en marché*.

POUR EN SAVOIR PLUS

Consultez le site Web du Centre pour la cybersécurité (**cyber.gc.ca**) pour en savoir plus sur la cybersécurité et pour consulter nos publications, notamment:

- La cybersécurité pour les organismes de santé : se protéger contre des cyberattaques courantes (ITSAP.00.131)
- Sécurité de l'Internet des objets pour les petites et moyennes organisations (ITSAP.00.012)
- Intelligence artificielle (ITSAP.00.040)
- Sécurité de la chaîne d'approvisionnement pour les petites et moyennes organisations (ITSAP.00.070)
- Application des mises à jour sur les dispositifs (ITSAP.10.096)
- Bulletin sur les cybermenaces : Incidence de la COVID-19 sur les cybermenaces pesant sur le secteur de la santé