CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

La cybersécurité pour les organismes de santé : se protéger contre des cyberattaques courantes

NON CLASSIFIÉ

SEPTEMBRE 2020 | ITSAP.00.131

Les organismes de santé sont appelés à traiter de l'information très sensible comme des renseignements médicaux personnels, de l'information financière et des données liées à la recherche, ce qui en font des cibles très attrayantes pour les auteurs de cybermenace. Les renseignements médicaux personnels sont d'ailleurs plus rentables sur le marché noir que tous les autres types de renseignements personnels. Ils sont utilisés pour créer de fausses réclamations d'assurance, acheter de l'équipement médical ou remplir des ordonnances dans le but de prendre ou de vendre les médicaments ainsi obtenus. La cybersécurité constitue peut-être une nouvelle priorité pour vous, mais nul besoin d'être un expert en informatique pour vous protéger contre les auteurs de cybermenace. Pour en savoir plus sur la cybersécurité, consultez le site Web du Centre canadien pour la cybersécurité au **cyber.gc.ca**

Pour vous aider à vous familiariser avec la cybersécurité, nous présentons ici des techniques courantes qu'utilisent les auteurs de cybermenace pour voler des renseignements médicaux personnels et de la propriété intellectuelle, ou encore pour perturber les activités des organismes de santé.

RANÇONGICIELS

Il s'agit d'un type de maliciel qui vous empêche d'accéder à vos systèmes, à vos appareils et à vos fichiers tant que vous n'avez pas payé la rançon à l'auteur de menace. Même si vous la payez, vous n'obtiendrez pas nécessairement l'accès à vos systèmes et rien n'empêche l'auteur de menace de vendre ou de diffuser les données en ligne. Une attaque par rançongiciel risque de ralentir ou d'interrompre vos processus essentiels, et vous pourriez perdre l'accès aux données sur votre recherche ou aux renseignements sur vos patients.

HAMEÇONNAGE

Les auteurs de menace tentent de duper (hameçonner) leurs cibles pour les amener à dévoiler de l'information sensible ou à télécharger un logiciel malveillant. Méfiez-vous des courriels, des textos ou des appels téléphoniques de personnes qui vous demandent de fournir des renseignements personnels, d'ouvrir une pièce jointe ou de cliquer sur un lien. Les auteurs de menace conçoivent ces messages et ces appels pour qu'ils semblent provenir de sources légitimes.

DÉNI DE SERVICE (DoS pour *Denial of Service*)

Lors d'une attaque par déni de service, l'auteur de menace inonde une cible (p. ex. un serveur) de trafic dans le but de faire planter des systèmes ou d'interrompre l'accès à des sites Web et à des services internes. Les auteurs de menace ont recours à ce type d'attaque pour perturber les services et les activités de recherche ou pour vous distraire. Pendant que vous tentez de rétablir les services, ils peuvent essayer de voler des données. Vous pourriez même être vulnérable si une telle attaque est lancée contre l'un de vos fournisseurs de services.

PULVÉRISATION DE MOTS DE PASSE

Les auteurs de menace utilisent des zombies (des ordinateurs robots connectés à Internet qui effectuent des tâches répétitives) et des listes de mots de passe courants pour lancer des attaques par force brute (c'est-à-dire soumettre autant de mots de passe que possible jusqu'à ce que le bon mot de passe soit « deviné ») en ciblant un grand nombre de comptes plutôt qu'un seul. Vous vous exposez à des risques plus élevés si vous utilisez le même mot de passe pour plusieurs comptes.

Pour commencer à protéger les réseaux, les systèmes et l'information de votre organisme, vous pouvez commencer par prendre trois mesures : accroître la sensibilisation à la cybersécurité, compliquer la tâche des auteurs de menace et sécuriser l'environnement de travail. Il existe cependant toute une gamme de mesures permettant de contrer les cybermenaces. Pour en savoir plus sur la cybersécurité et les pratiques exemplaires, consultez le site Web du Centre canadien pour la cybersécurité (cyber.gc.ca).

1 ACCROÎTRE LA SENSIBILISATION À LA CYBERSÉCURITÉ

Adoptez une approche proactive à la sécurité et améliorez votre sensibilisation à la cybersécurité en suivant de la formation et en participant à des activités éducatives.

Apprenez à reconnaître les tentatives d'hameçonnage. Sachez reconnaître les caractéristiques d'une tentative d'hameçonnage, notamment les adresses courriel et numéros de téléphone inconnus, les erreurs d'orthographe et de grammaire, les demandes de renseignements personnels, les menaces ou les offres trop belles pour être vraies.

Faites preuve de prudence lorsque vous ouvrez des pièces jointes ou cliquez sur des liens. Pensez-y à deux fois avant d'ouvrir une pièce jointe ou de cliquer sur un lien. Bien qu'ils puissent sembler provenir de source légitime ou être inoffensifs, les liens et les pièces jointes pourraient contenir du code malveillant. Prenez l'habitude de vérifier si l'URL intégrée correspond au lien qui s'affiche dans le courriel, de taper manuellement l'URL dans un navigateur ou un moteur de recherche au lieu de cliquer sur le lien, ou encore de communiquer avec l'expéditeur pour vérifier si la demande d'information est légitime.

Consultez d'autres ressources. Le site Web du Centre canadien pour la cybersécurité (cyber.gc.ca) présente des publications, des blogues et des infographies sur divers sujets liés à la cybersécurité, ainsi que des alertes et des bulletins de sécurité.

Pendant la pandémie de COVID-19, le Centre pour la cybersécurité a constaté un accroissement des risques de cybersécurité pour les organismes de santé du Canada.

2 COMPLIQUER LA TÂCHE DES AUTEURS DE MENACE

Même si vous prenez des précautions pour vous protéger, un auteur de menace pourrait quand même réussir à accéder à vos comptes et à votre information. Vous pouvez toutefois prendre certaines mesures pour qu'il soit plus difficile de pirater vos appareils et vos comptes.

Utilisez une phrase de passe ou un mot de passe unique pour chaque compte. Dans la mesure du possible, utilisez une phrase de passe au lieu d'un mot de passe. Comme une phrase de passe est composée de plusieurs mots, elle est plus facile à retenir que la série de caractères aléatoires qu'il faut choisir pour créer un mot de passe complexe. Les phrases de passe devraient compter au moins 4 mots et 15 caractères.

Sur les ordinateurs et appareils partagés, évitez de sélectionner l'option « Mémoriser mes informations » ou « Enregistrer le mot de passe » lorsque vous vous connectez à vos comptes. Fermez toujours la session lorsque vous avez terminé. Si vous avez besoin d'aide pour vous souvenir de vos mots de passe, envisagez d'utiliser un gestionnaire de mots de passe (basé sur le navigateur ou comme application autonome). Assurez-vous de choisir une phrase de passe forte pour protéger l'accès à votre gestionnaire de mots de passe. Si un auteur de menace arrivait à deviner le mot de passe de votre gestionnaire, il aurait accès à tous les mots de passe qui y sont stockés.

Activez l'authentification multifacteur. Ne vous contentez pas d'une phrase de passe. Ajoutez une couche de sécurité en activant l'authentification multifacteur, qui consiste à utiliser au moins deux facteurs différents pour confirmer votre identité. Par exemple, vous pouvez utiliser un mot de passe et une empreinte digitale pour déverrouiller un appareil. L'option vous permettant d'activer l'authentification multifacteur se trouve généralement dans les paramètres des appareils ou des comptes. Cette mesure protégera vos comptes et vos renseignements si votre mot de passe est compromis à la suite d'une attaque par hameçonnage, par force brute ou par pulvérisation de mots de passe.

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

3 SÉCURISER L'ENVIRONNEMENT DE TRAVAIL

Que vous travailliez dans un bureau ou à distance, vous pouvez réduire les risques d'attaques et les répercussions de telles attaques en adoptant quelques habitudes simples.

Utilisez un réseau sans fil (Wi-Fi) sécurisé. Lorsque vous travaillez à distance, évitez d'utiliser les réseaux sans fil publics. Si vous devez en utiliser un, évitez d'envoyer de l'information sensible ou de vous connecter à des comptes sensibles. Un réseau privé virtuel (RPV) constitue un autre moyen de protéger l'information lorsque vous utilisez un réseau public. Il s'agit d'un tunnel chiffré sécurisé par l'intermédiaire duquel l'information est transmise.

Protégez votre réseau sans fil à la maison en modifiant le mot de passe par défaut que vous a donné votre fournisseur. Vous pourriez également créer un réseau d'invité pour réduire le nombre de personnes qui utilisent votre réseau principal.

Faites appel à des systèmes d'adressage par domaine (DNS pour *Domain Name System*) protégés, comme le Bouclier canadien, qui permettent de bloquer activement les sites Web malveillants connus lorsque vous tentez de vous y connecter.

Utilisez des logiciels et des applications de sources fiables. Au travail, utilisez uniquement les applications et les logiciels autorisés. Si vous avez besoin d'un nouveau logiciel ou d'une nouvelle application, communiquez avec les services TI. Si vous téléchargez vous-même des logiciels et des applications, assurez-vous qu'ils proviennent de fournisseurs dignes de confiance.

N'ignorez pas les rappels de mise à jour des logiciels et des applications. Les mises à jour servent à corriger les bogues et les vulnérabilités de sécurité et à vous protéger contre les cybermenaces. Faites les mises à jour sur vos appareils et dans vos applications dès que possible.

Utilisez des outils de sécurité pour soutenir vos efforts. Installez un logiciel antivirus sur vos ordinateurs, vos portables et vos appareils mobiles. Les antivirus vous protègent contre les maliciels en analysant les fichiers et votre système.

Protégez vos réseaux et vos systèmes au moyen d'un pare-feu, un outil de sécurité qui filtre le trafic malveillant connu pour l'empêcher d'accéder à votre réseau.

Assurez-vous de faire régulièrement les mises à jour de tout outil que vous utilisez.

Faites des copies de sauvegarde de vos informations. Dans l'éventualité d'un incident, comme une catastrophe naturelle ou une attaque par rançongiciel, il importe d'avoir des copies de sauvegarde afin de pouvoir continuer d'accéder à l'information et aux systèmes essentiels, de mener les activités de recherche et de soigner les patients.

Lorsque vous faites des copies de sauvegarde, assurez-vous d'utiliser les supports de stockage approuvés par votre organisme (p. ex. espace de stockage basé sur le nuage ou supports de stockage comme des clés USB ou des disques durs externes). Prenez en considération le type d'information que vous sauvegardez; il convient de chiffrer l'information sensible ou de la protéger par un mot de passe.

Gérez les comptes en fonction des considérations liées à la sécurité. Il est très rare qu'une personne ait besoin d'accéder à toute l'information. Veillez à ce que les privilèges administratifs soient accordés uniquement aux personnes qui en ont besoin.

Bien qu'il puisse être pratique d'utiliser un compte partagé pour lequel plusieurs personnes connaissent le mot de passe, cette façon de faire comporte des risques de violation de données ou d'atteinte à la vie privée. Assurez-vous d'avoir vos propres comptes et mots de passe.

POUR EN SAVOIR PLUS

Les conseils présentés ici constituent un bon point de départ. Pour obtenir des précisions sur certains points clés, consultez les publications connexes ci-dessous, qui se trouvent sur le site Web du Centre pour la cybersécurité (cyber.gc.ca).

Cybermenaces :

- Cybermenaces pesant sur les organismes de santé canadiens (AL20-008)
- Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage (ITSAP.00.101)
- Rançongiciels : comment les prévenir et s'en remettre (ITSAP.00.099)
- Protéger son organisation contre les attaques par déni de service (ITSAP.80.100)
- Êtes-vous victim de piratage ? (ITSAP.00.15)

Pratiques exemplaires et conseils :

- Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032)
- Conseils de sécurité sur les gestionnaires de mots de passe (ITSAP.30.025)
- Repensez vos habitudes en regard de vos mots de passe de manière à protéger vos comptes des pirates informatiques (ITSAP.30.036)
- Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030)
- Application des mises à jour sur les dispositifs (ITSAP.10.096)
- Conseils de cybersécurité pour le télétravail (ITSAP.10.116)
- Les réseaux privés virtuels (ITSAP.80.101)

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada