Protéger le matériel de recherche médicale contre les cybermenaces

Février 2022 | ITSAP.00.134

Le matériel de recherche médicale est vital aux opérations de votre organisation. Il sert à recueillir les données dans le cadre de vos projets et ainsi qu'à répondre à des besoins essentiels dans le domaine médical. Le milieu de la recherche médicale est riche en données, tout comme l'infrastructure numérique sur laquelle ces données sont stockées, ce qui en fait des cibles de choix pour les auteurs de cybermenace. Plus les laboratoires de recherche médicale sont connectés, plus leurs données risquent d'être visées par des accès non autorisés. En effet, les auteurs de menace peuvent accéder à des dispositifs connectés non sécurisés (p. ex., les congélateurs de laboratoire) et s'en servir pour infiltrer vos réseaux et vos systèmes et consulter vos données. En prenant connaissance des risques qui pèsent sur vous et des mesures que vous pouvez prendre pour les atténuer, vous serez plus à même de protéger votre matériel et vos données sensibles.

Exemples de menaces

Les exemples suivants illustrent les types d'incidents de cybersécurité qui peuvent toucher le matériel de recherche médicale connecté.

Analyse des dispositifs d'examen de biologie médicale délocalisée : Les auteurs de menace peuvent exfiltrer des données en accédant à votre réseau par un dispositif d'examen de biologie médicale délocalisée (p. ex., un appareil de dépistage rapide). Pour y arriver, ils ont habituellement recours à l'hameçonnage pour tromper les utilisateurs et les inciter à cliquer sur un lien ou à télécharger un fichier qui contient un maliciel.

Pénétration du stockage de données : Les auteurs de menace trouvent des vulnérabilités dans un point d'entrée afin d'accéder à vos réserves de données. Les réserves de données contiennent de l'information d'une grande valeur (résultats de recherches, propriété intellectuelle, renseignements médicaux personnels, etc.).

Exploitation de l'automatisation laboratoire : Plus les installations de recherche sont connectées à des systèmes automatisés, plus elles risquent d'être la cible de cyberattaques. Les auteurs de cybermenaces ciblent les systèmes automatisés pour en exfiltrer les données ou pour avoir accès aux réseaux.

Menace interne : On entend par une menace interne toute personne qui connaît l'infrastructure ou l'information de votre organisation, ou qui y a accès, et qui utilise, consciemment ou non, ses connaissances ou son accès pour nuire à l'organisation. Les données produites par votre matériel de recherche pourraient être vulnérables aux menaces internes. Pour savoir comment protéger votre organisation contre les menaces internes, consultez le document *ITSAP.10.003 Comment protéger votre organisation contre les menaces internes*.

COMMENT LES AUTEURS DE MENACE CIBLENT-ILS LE MATÉRIEL DE RECHERCHE MÉDICALE?

Le matériel de recherche médicale sert à recueillir et à analyser de l'information sensible, que ce soit des renseignements médicaux, des résultats de recherche ou de la propriété intellectuelle. Les auteurs de menace souhaitent passer par le matériel connecté, comme les spectromètres de masse et les calibreurs de particules, pour accéder aux données à des fins malveillantes.

Les attaques ne se limitent pas aux exemples de menaces fournis dans le présent document. Les points d'attaques sont nombreux et peuvent comprendre les éléments suivants:

- Exploitation du matériel ou des systèmes plus vieux qui ne sont plus corrigés et mis à jour.
- Compromission du matériel et des systèmes connectés avec un maliciel (p. ex., un rançongiciel).
- Détection de vulnérabilités sur le matériel et les réseaux non protégés, comme l'absence de chiffrement ou de coupe-feu, et exploitation de ces vulnérabilités aux fins d'accès aux données.

QUELLES SONT LES RÉPERCUSSIONS DE CES ATTAQUES SUR LES CHERCHEURS ET LES DONNÉES?

Les cyberattaques peuvent viser la plupart des pièces de matériel de recherche médicale, du système de chromatographie en phase liquide à très haute performance allant jusqu'au dispositif de stockage périphérique (comme une clé USB). Si vous êtes victime d'une cyberattaque, les résultats de recherche, la propriété intellectuelle et les renseignements médicaux pourraient être compromis.

Depuis le début de la pandémie, les auteurs de menace s'en prennent de plus en plus aux installations de recherche médicale au moyen de rançongiciels et de tactiques d'exfiltration de données. Le coût de remplacement et de récupération des données et du matériel compromis pourrait être dévastateur pour votre organisation.

Sensibilisez les membres de votre organisation aux mesures de sécurité nécessaires à la protection du matériel de recherche médicale. Encadrez les employés avec des lignes directrices et des politiques en matière de cybersécurité et offrez-leur de la formation à l'interne.

RÉSEAU CANARIE

Les hôpitaux de recherche, les universités, les collèges, les centres scientifiques et les autres centres universitaires et de recherche du Canada peuvent se connecter au réseau CANARIE par l'entremise de leurs partenaires provinciaux ou territoriaux du Réseau national de la recherche et de l'éducation (RNRE). Le RNRE connecte les organisations de partout au Canada entre elles ainsi qu'à d'autres réseaux mondiaux de la recherche et de l'éducation.

- Le réseau CANARIE offre gratuitement des outils de surveillance et de maintenance de réseau.
- En effet, les membres admissibles du RNRE peuvent participer au programme Initiatives en cybersécurité (PIC), financé par le gouvernement du Canada. Les participants au PIC bénéficient d'une protection coupe-feu, d'un système de détection d'intrusion et d'un fil de menaces consolidé.

Pour vous renseigner sur le PIC de CANARIE, consultez le programme Initiatives en cybersécurité (PIC).

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

COMMENT PUIS-JE PROTÉGER MON ORGANISATION?

Pour protéger vos données, vous devez absolument sécuriser votre matériel de recherche médicale. Tout dispositif muni d'un logiciel et connecté à votre réseau est vulnérable aux cybermenaces. En appliquant les conseils de cybersécurité ci-dessous, vous améliorerez votre environnement et renforcerez la protection de votre matériel de recherche, de vos dispositifs et de vos données.

Renforcez la sécurité : Sécurisez votre cyberenvironnement pour protéger vos laboratoires, vos réseaux, vos dispositifs connectés et votre information.

- Utilisez un réseau privé virtuel (RPV) pour connecter vos dispositifs.
- Protégez les comptes et les dispositifs connectés de l'équipement de laboratoire au moyen de l'authentification multifacteur et optez pour des mots de passe ou des phrases de passe robustes.
- Accordez les droits d'accès et les privilèges système aux utilisateurs en fonction de leurs tâches.
- Désactivez les comptes des utilisateurs qui changent de fonctions ou qui quittent l'organisation.
- Remplacez le matériel désuet qui n'a pas d'adresse unique ou de journaux des événements ou qui n'est pas configurable.
- Chiffrez le stockage des dispositifs et les communications entre dispositifs.
- Recourez à une solution de surveillance des journaux qui surveille les journaux de nombreux dispositifs et systèmes et lance une alerte lorsque des anomalies sont détectées.
- Demandez aux responsables des TI de segmenter les réseaux en les divisant en plus petites zones de sorte à mieux contrôler les flux de trafic.
    - La segmentation permet aussi d'isoler et d'arrêter la propagation de maliciel dans différentes sections du réseau, ainsi que de contrôler et de restreindre l'accès aux renseignements.
- Intégrez les normes de cybersécurité et de sécurité des données aux ententes de service conclues avec vos fournisseurs.
- Assurez-vous que chaque fournisseur de la chaine d'approvisionnement a en place de contrôles de cybersécurité robustes.
- Examinez les politiques de vos fournisseurs en matière de gestion des données et de sécurité, et déterminez l'endroit où vos données seront stockées et la façon dont elles seront traitées.

Protégez vos renseignements : Vos données de grande valeur doivent être à l'abri des auteurs de menace.

- Chiffrez vos données qui se trouvent dans vos réseaux, vos systèmes ou dans le nuage.
- Faites régulièrement des copies de sauvegarde de vos données dans des lieux de stockage hors site qui ne sont pas accessibles à partir de vos réseaux ou de vos connexions Internet.
- Instaurez un système de classification des données pour que les systèmes de secours puissent établir facilement la distinction entre les données de grande valeur et les autres données.

Gérez vos biens : Dites-vous que le matériel médical et les données sont des biens de l'organisation et protégez-les en conséquence.

- Élaborez une stratégie de gestion du cycle de vie qui comprend la planification et la budgétisation pour l'acquisition de nouveau matériel de recherche et de logiciel connexe.
    - Viendra un moment où un certain dispositif de recherche ne sera plus pris en charge. En planifiant le remplacement du dispositif, vous contribuez à éviter les failles de sécurité informatique après son élimination.
- Vérifiez les dispositifs Web et connectés à Internet. Assurez-vous d'appliquer régulièrement les correctifs et les mises à jour pour corriger les vulnérabilités.

DE QUELS ÉLÉMENTS DOIS-JE TENIR COMPTE AU MOMENT DE FAIRE L'ACQUISITION DE NOUVEAU MATÉRIEL?

Les lignes directrices du National Institute of Standards and Technology (NIST) des États-Unis recommandent aux gestionnaires de laboratoire de tenir compte des fonctions ou des capacités suivantes lorsqu'ils font l'acquisition de dispositifs connectés au réseau:

- **Identification** : Le dispositif doit avoir sa propre adresse dans les réseaux.
- **Configuration** : Un gestionnaire de laboratoire doit pouvoir accéder facilement aux configurations de sécurité (logiciel, micrologiciel et réglage) et les modifier.
- **Protection des données** : Le chiffrement doit être intégré au dispositif pour le protéger contre les accès et les modifications non autorisés.
- **Interfaces réseau limitées** : L'authentification doit être obligatoire pour accéder au dispositif, ce qui limite l'accès aux réseaux locaux et étendus.
- **Mises à jour du logiciel et du micrologiciel** : Il doit y avoir une façon sécuritaire et configurable de mettre à jour le logiciel et le micrologiciel du dispositif, que ce soit automatiquement ou manuellement.
- **Journalisation des événements** : Le dispositif doit journaliser les événements de cybersécurité pour informer les gestionnaires de laboratoire des vulnérabilités et permettre une analyse criminalistique en cas de piratage.

POUR EN SAVOIR PLUS

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).

- Facteurs à considérer sur le plan de la recherche et du développement (ITSAP.00.130)
- Sécurité de l'Internet des objets pour les petites et moyennes organisations (ITSAP.00.012)
- Sauvegarder et récupérer vos données (ITSAP.40.002)
- Application des mises à jour sur les dispositifs (ITSAP.10.096)
- Protection de l'information de grande valeur : Conseils pour les petites et moyennes entreprises (ITSAP.40.001)
- Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030)
- Utiliser le chiffrement pour assurer la sécurité des données sensibles (ITSAP.40.016)

Travail à distance

Le travail à distance a gagné en popularité pendant la pandémie, ce qui a eu pour effet d'augmenter l'exposition aux menaces et, par le fait même, de faciliter le travail des auteurs de menace. Les cybermenaces qui pèsent sur les installations de recherche se sont intensifiées, car les auteurs de menace peuvent exploiter les dispositifs personnels et les connexions non protégées pour accéder aux systèmes, aux données et au matériel du réseau de ces installations. Pour renforcer la sécurité de votre organisation alors que vos employés sont en télétravail, appliquez les conseils énumérés précédemment, mais assurez-vous surtout de brancher les dispositifs par l'entremise d'un RPV, d'appliquer les correctifs et les mises à jour aux logiciels, aux micrologiciels et aux systèmes d'exploitation et d'opter pour des mots de passe et des phrases de passe robustes. Pour obtenir d'autres conseils de sécurité sur le télétravail, consultez Conseils de sécurité pour les organisations dont les employés travaillent à distance (ITSAP.10.016) et Conseils de cybersécurité pour le télétravail (ITSAP.10.116).

Communications Security Establishment
Centre de la sécurité des télécommunications
Canada