CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Conseils de sécurité pour les dispositifs périphériques

Mai 2024

ITSAP.70.015

Les périphériques sont des dispositifs qui peuvent être branchés à un ordinateur hôte ou à un dispositif mobile, et ils servent à accroître les capacités et à améliorer l'expérience des utilisatrices et utilisateurs. Malgré les avantages qu'ils procurent, les périphériques peuvent également représenter pour des auteures et auteurs de menace un moyen de compromission des réseaux,

Périphériques et types d'utilisation

Les périphériques peuvent être des dispositifs internes ou externes. Les périphériques internes sont intégrés à un ordinateur ou à un appareil mobile par le fabricant, comme les cartes vidéo et son, les cartes d'interface de réseau et les disques durs. Les périphériques externes se branchent par câble dans un port du dispositif hôte, ou peuvent être sans fil à l'aide du Wi-Fi ou Bluetooth. On compte parmi les périphériques externes les claviers, caméras, imprimantes et disques durs externes.

Pour évaluer les risques posés par les périphériques, votre organisation doit identifier dans une des trois catégories suivantes les dispositifs utilisés actuellement ou dont la mise en œuvre est prévue :

- un **périphérique d'entrée** envoie de l'information et des instructions à l'ordinateur ou à l'appareil mobile auquel il est branché.
- an **périphérique de sortie** reçoit de l'information et des instructions de l'ordinateur ou appareil mobile auquel il est branché.
- un **périphérique de stockage** stocke et enregistre de l'information provenant d'un ordinateur ou appareil mobile.

Connaître le type de périphérique utilisé et le flux d'informations peut vous aider à choisir et à prioriser les contrôles de sécurité. Ces contrôles de sécurité peuvent renforcer la protection de vos systèmes et biens sensibles.

Risques liés à l'utilisation de périphériques

Les auteures et auteurs de menace peuvent tenter d'exploiter les périphériques, en vue d'avoir accès à vos réseaux, systèmes et informations de nature sensible. Les trois exemples suivants illustrent comment les périphériques peuvent être exploités pour réaliser des activités malveillantes.

Compromission de câbles intelligents

Des microcontrôleurs sont intégrés aux câbles intelligents, comme les câbles Lightning et Thunderbolt. Les auteures et auteurs de menace peuvent programmer ces microcontrôleurs pour les faire attaquer l'appareil auquel vous branchez le câble. Il existe même des câbles commerciaux qui contiennent un point d'accès sans fil pouvant être ciblé par des auteures et auteurs de menace.

Vulnérabilités des micrologiciels

Les auteures et auteurs de menace peuvent utiliser le micrologiciel d'un appareil (le logiciel qui contrôle le matériel de l'appareil) pour exécuter des « rootkits », un type de logiciel qui se camoufle et cache des maliciels dans votre appareil. Ce type de logiciel permet aux auteures et auteurs de menace de contrôler à distance les appareils et d'accéder à des éléments comme vos communications réseau ou votre caméra Web.

Attaques contre l'accès direct à la mémoire

Les attaques contre l'accès direct à la mémoire (DMA pour *Direct memory Access*) permettent aux dispositifs matériels de communiquer directement avec la mémoire système (RAM) du dispositif. Lorsqu'une auteure ou auteur de menace a compromis les micrologiciels d'un appareil ou qu'il a physiquement accès à un système, il peut alors mener une attaque contre l'accès direct à la mémoire (DMA) pour lire et réécrire la mémoire du système. En réécrivant la mémoire, l'auteure ou auteur de menace peut prendre contrôle du système et effectuer des activités malveillantes.

SÉRIE SENSIBILISATION

No de cat. D97-1/70-015-2024F-PDF
ISBN 978-0-660-70986-4

Canada

Utilisation sécuritaire des périphériques

Passez en revue ce qui suit pour aider à évaluer l'utilisation des périphériques.

Évaluer les fournisseurs de périphériques

Votre chaîne d'approvisionnement peut avoir un impact sur votre sécurité. Lorsque vous achetez des périphériques, assurez-vous d'avoir affaire à un fournisseur reconnu qui vend des périphériques ayant des mesures de sécurité intégrées. Faites preuve de prudence avant d'utiliser des périphériques qui vous sont donnés par de tierces parties inconnues, par exemple, un fournisseur lors d'une conférence. Ces périphériques gratuits peuvent contenir des maliciels conçus pour compromettre les dispositifs dans lesquels ils sont branchés.

Évaluer les besoins pour chaque périphérique

Vous pouvez réduire les risques associés aux dispositifs périphériques en limitant le nombre de périphériques que vous utilisez. Évaluez les risques liés à la sécurité que pose chaque périphérique utilisé. Dans la mesure du possible, n'utilisez que des périphériques qui sont nécessaires ou qui améliorent l'expérience de l'utilisatrice ou utilisateur.

Vérifier et authentifier les périphériques

Avant de brancher des périphériques à vos réseaux et dispositifs électroniques, vérifiez que le périphérique que vous choisissez est répertorié et connu et approuvé. Déterminez si le périphérique est désuet en vérifiant s'il est toujours pris en charge par le fournisseur, ou s'il a atteint sa fin de vie. Vous devriez remplacer les produits désuets pour limiter les vulnérabilités.

Vous pouvez utiliser des codes de jumelage et des clés d'accès pour authentifier et autoriser les connexions sans fil. Méfiez-vous si vous recevez une demande de jumelage ou de connexion que vous n'avez pas lancée. Un appareil qui se branche même une seule fois à votre système demeure dans votre liste d'appareils jumelés. Jusqu'à ce qu'il soit supprimé manuellement. Supprimez toujours les dispositifs perdus ou volés de votre liste de dispositifs jumelés.

Sécuriser les dispositifs physiques et les câbles

Gardez le contrôle et la garde de vos dispositifs, y compris les câbles et les chargeurs, pour vous assurer qu'ils ne sont pas modifiés ou remplacés par d'autres dispositifs. Étiquetez tous les périphériques avec un sceau de sécurité inviolable. L'étiquetage vous assure que les périphériques peuvent être facilement identifiés et cela empêche les auteures et auteurs de menace de les remplacer par d'autres dispositifs.

Changer les mots de passe par défaut

Généralement, les dispositifs électroniques viennent avec un mot de passe par défaut fourni par le fabricant. Assurez-vous de modifier tous les mots de passe attribués par défaut, y compris les mots de passe des administratrices et administrateurs.

Chaque périphérique doit avoir une phrase ou un mot de passe unique et complexe. Il est important de noter que les phrases de passe doivent compter au moins quatre mots et avoir une longueur d'au moins quinze caractères.

Corriger et mettre à jour les dispositifs

Vous êtes probablement déjà au courant de l'importance de tenir à jour le système d'exploitation et les applications de votre ordinateur et de vos appareils mobiles, mais ne négligez pas les périphériques. N'oubliez pas de régulièrement mettre à jour et déboguer vos micrologiciels et d'y appliquer les correctifs de sécurité pour faire en sorte que vos appareils soient sécurisés autant que possible.

Autres facteurs à prendre en considération en utilisant des périphériques

Avant d'utiliser un périphérique, faites-en l'évaluation en tenant compte de vos exigences opérationnelles et de sécurité afin de déterminer les risques et mettre en œuvre les mesures de protection adéquates. De plus, votre organisation devrait définir des politiques claires sur l'utilisation des dispositifs périphériques.

Adoptez les mesures suivantes pour accroître la sécurité de votre organisation :

- méfiez-vous avant de connecter des périphériques dont la fiabilité est incertaine lorsque vous visitez une organisation de tierce partie (p. ex. câbles HDMI, clé USB). Lisez attentivement les avertissements ou les demandes d'autorisations provenant de ces périphériques;
- fermez vos sessions et éteignez vos appareils lorsque vous ne vous en servez pas;
- désactivez les fonctionnalités de connexion automatique pour vous assurer que vos dispositifs ne se jumellent pas automatiquement avec des appareils inconnus ou ne se connectent pas à des réseaux non sécurisés;
- branchez les dispositifs périphériques à un réseau pour invités plutôt qu'à votre réseau interne principal;
- avant de jeter un périphérique, expurgez-le soigneusement afin de supprimer toute information sensible qu'il pourrait contenir;
- offrez une formation à vos employées et employés au sujet de l'utilisation acceptable des périphériques.

Pour en savoir plus

- Utiliser la technologie Bluetooth (ITSAP.00.011)
- Sécurité de l'Internet des objets (ITSAP.00.012)
- Conseils de cybersécurité pour le télétravail (ITSAP.10.116)
- Sécurité de la chaîne d'approvisionnement pour les petites et moyennes organisations (ITSAP.00.70)
- Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032)
- Produits obsolètes (ITSAP.00.095)