EST-CE QUE VOTRE APPAREIL INTELLIGENT VOUS ÉCOUTE?

OCTOBRE 2020 **ITSAP.70.013**

Les appareils intelligents sont de plus en plus présents dans notre environnement tant au travail qu'à la maison. Ils peuvent se connecter à d'autres appareils, ce qui crée un réseau que l'on surnomme « Internet des objets » (IdO). Certains appareils peuvent contrôler tous les autres appareils intelligents d'un IdO à l'aide de services de commandes vocales. Ces appareils s'appellent des assistants personnels virtuels ou des assistants numériques. Ces assistants numériques se connectent à d'autres appareils et à Internet pour exécuter diverses tâches (p. ex. consulter la météo, changer les réglages du thermostat, faire jouer de la musique). Votre organisation doit tenir compte des risques envers la cybersécurité causés par l'utilisation d'assistants numériques avant de les déployer dans ses réseaux.

« *OK*, MAIS COMMENT ÇA FONCTIONNE UN ASSISTANT NUMÉRIQUE? »

Les assistants numériques ont plusieurs formes, il peut notamment s'agir d'un haut-parleur, d'une montre intelligente, d'applications de téléphones intelligents, etc. Les assistants numériques répondent aux commandes humaines à l'aide d'un programme de reconnaissance vocale. Ces appareils sont toujours à l'écoute d'un terme qui dénote une commande (p. ex. « *Ok* » suivi du nom de l'appareil). Une fois la commande énoncée, l'appareil enregistre votre message et recherche la réponse appropriée. Au fil du temps et de l'utilisation que vous en faites, votre assistant numérique crée des profils afin d'identifier les différentes personnes qui lui donnent des commandes. Les assistants numériques enregistrent des données de reconnaissance vocale (p. ex. échantillons vocaux et langage naturel) et ils stockent des données sur les ressources et sur les appareils intelligents qu'ils utilisent pour répondre à vos demandes (p. ex. les sites Web consultés, la machine à laver utilisée, la température habituellement programmée dans le thermostat, etc.).

QUELS SONT LES RISQUES?

Les assistants numériques représentent des cibles de grande valeur pour les auteurs de cybermenaces qui cherchent à voler de l'information de nature sensible. Les auteurs de cybersécurité peuvent tirer parti des vulnérabilités des assistants numériques des manières suivantes :

- Accéder aux renseignements personnels et à l'historique des conversations.
- Espionner les conversations de nature sensible.
- Surveiller et stocker les enregistrements de reconnaissance vocale.
- Accéder à d'autres appareils de l'IdO de votre réseau.
- Trafiquer les contrôles d'autres dispositifs intelligents branchés à votre réseau (p. ex. température, sécurité).

QUELLES SONT CERTAINES MÉTHODES D'ATTAQUE?

Votre assistant virtuel pourrait être ciblé par des auteurs de cybermenaces à l'aide de la méthode d'attaque et maliciel du « dauphin ».

« ATTAQUE DU DAUPHIN »

L'attaque du « dauphin » consiste à émettre des fréquences ultrasoniques qui déclenchent la fonction d'enregistrement des assistants numériques. Les sons à cette fréquence sont imperceptibles par l'humain et peuvent être intégrés dans des vidéos, des sites Web et d'autres sources afin de cibler les assistants numériques qui se trouvent dans un certain rayon. Les auteurs de cybermenaces utilisent les « attaques du dauphin » pour transférer des fichiers, faire des achats et voler des données sensibles.

MALICIELS

Les maliciels (c.-à-d. des logiciels malveillants) peuvent infecter les assistants numériques à partir de pièces jointes téléchargées et d'hyperliens (p. ex. en se faisant passer pour une application offrant des fonctions supplémentaires) et permettent aux auteurs de menaces d'accéder à vos informations sensibles. Les maliciels sont très difficiles à détecter et à diagnostiquer dans les assistants numériques. Les auteurs de menaces peuvent faire appel à des maliciels pour enregistrer votre voix et utiliser cet enregistrement pour effectuer d'autres activités malveillantes comme déchiffrer l'authentification par reconnaissance vocale dans vos appareils.

Même si les assistants numériques peuvent créer des profils pour reconnaître les commandes vocales individuelles, ils répondent à toute commande vocale qu'ils peuvent interpréter et enregistrent toutes ces commandes.

SÉRIE SENSIBILISATION

© Gouvernement du Canada
Le présent document est la propriété exclusive du gouvernement du Canada. Toute modification, diffusion à un public autre que celui visé, production, reproduction ou publication, en tout ou en partie, est strictement interdite sans l'autorisation expresse du CST.

ÉLÉMENTS À CONSIDÉRER AVANT DE CHOISIR UN APPAREIL

Il est important de comprendre l'énoncé de confidentialité du contrat de licence utilisateur-final de votre fournisseur. Posez-vous les questions suivantes avant de sélectionner un assistant numérique :

- L'appareil a-t-il une option « appuyer pour activer »?
- L'appareil a-t-il une option pour désactiver la fonction d'écoute afin de protéger les discussions et événements privés?
- Y a-t-il une option d'indicatif sonore ou de clignotant lumineux pour indiquer à l'utilisateur que l'appareil est en train d'enregistrer?
- Quelles sont les données qui sont envoyées au service de traitement vocal?
- Qu'est-ce qui est retourné pour demander un service ou une application?
- Qui a accès aux données de voix brutes ou au texte analysé?
- Comment les données conservées sont-elles utilisées et pendant combien de temps?
- Les données générées par l'appareil sont-elles chiffrées?
- Existe-t-il des options de désinscription de certaines fonctionnalités, si nécessaire (p. ex. où les données sont envoyées, quelles données sont renvoyées et conservées, qui peut accéder aux données)?

Consultez les critiques des utilisateurs et les évaluations de sécurité concernant les fournisseurs pour voir si leurs bases de données ont des vulnérabilités connues ou si leurs installations de stockage ont déjà été compromises.

RESSOURCES SUPPLÉMENTAIRES

Pour en savoir plus sur la cybersécurité, consultez le site Web du Centre pour la cybersécurité (**cyber.gc.ca**) où vous trouverez la liste de toutes nos publications et d'autres ressources, notamment :

- *Protéger l'organisme contre les maliciels (ITSAP.00.057)*.
- *Sécurité de l'Internet des objets pour les petites et moyennes organisations (ITSAP.00.012)*
- *Les réseaux privés virtuels (ITSAP.80.101)*

COMMENT PUIS-JE SÉCURISER MON ASSISTANT NUMÉRIQUE?

Lorsque vous configurez votre assistant numérique, déterminez quelles sont les informations (p. ex. informations de niveau plus sensible) auxquelles vos appareils intelligents peuvent accéder par l'entremise de votre réseau. Selon les exigences de sécurité de votre organisation, il vaudrait peut-être mieux isoler l'assistant numérique sur un réseau distinct, tel qu'un réseau invité, pour protéger votre réseau principal en cas de compromis. Pensez à mettre en œuvre certaines des pratiques exemplaires suivantes pour sécuriser votre appareil :

- Attribuez un mot de passe unique à votre assistant numérique, différent de tous vos autres mots de passe.
- Configurez un NIP pour votre assistant numérique afin de prévenir l'utilisation non autorisée de l'assistant vocal.
- Si vous devez discuter de sujets personnels ou sensibles à proximité de votre assistant numérique, éteignez-le.
- Désactivez les fonctions d'accès des assistants numériques leur permettant d'effectuer des opérations de sécurité sensibles (p. ex. déverrouillage des portes ou des commandes de caméra).
- Désactivez les fonctions d'accès à distance sur les appareils si vous n'en avez pas besoin (p. ex. caméra intelligente).
- Appliquez dès qu'ils sont disponibles les correctifs de sécurité et les mises à jour à vos logiciels et micrologiciels.
- Utilisez un réseau privé virtuel dans le réseau auquel votre assistant numérique est connecté.

Faites preuve de prudence par rapport aux types d'informations que vous partagez avec les assistants numériques et dont vous discutez à proximité des assistants numériques.

QUE DOIS-JE FAIRE SI MON ASSISTANT NUMÉRIQUE EST PIRATÉ?

Suivez les étapes suivantes si vous suspectez que des activités malveillantes se déroulent dans votre assistant numérique et vos appareils intelligents :

1. Déconnectez immédiatement l'appareil IdO de votre réseau.
2. Communiquez avec votre fournisseur de services pour localiser le point d'intrusion et déterminer quelles données ont été compromises.
3. Réinitialisez votre appareil aux paramètres d'usine et mettez-le immédiatement à jour avec la dernière version disponible.
4. Faites un balayage avec un logiciel antivirus de votre réseau et de vos appareils branchés à l'IdO.
5. Signalez les activités suspectes au Centre pour la cybersécurité : cyber.gc.ca

Vous avez des questions ou vous avez besoin d'aide? Vous voulez en savoir plus sur les questions de cybersécurité? Consultez le site Web du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) à **cyber.gc.ca**.