LES OUTILS DE SÉCURITÉ PRÉVENTIVE

NOVEMBRE 2020 **ITSAP.00.058**

Les outils de sécurité préventive offrent d'importantes couches de protection pour vos réseaux et vos appareils. Ils peuvent aider votre organisation à réduire les risques d'intrusion malveillante (p. ex. les maliciels, les espiogiciels et les utilisateurs non autorisés). Chacun de ces outils cible des aspects précis afin de prévenir la compromission des réseaux et des appareils de votre organisation.

EXEMPLES D'OUTILS DE SÉCURITÉ PRÉVENTIVE

Pare-feux

Un pare-feu est une barrière de sécurité érigée entre deux réseaux pour contrôler le volume et le type de trafic qui passe entre les deux. Les pare-feux préviennent la transmission non autorisée de données d'une zone du réseau à une autre grâce aux fonctionnalités suivantes :

- surveillance du trafic entrant et sortant, puis filtrage du contenu pour bloquer le trafic de sources malveillantes connues;
- vérification des données téléchargées pour veiller à ce qu'elles proviennent d'une connexion légitime;
- déchiffrement et analyse des données téléchargées pour vérifier qu'il ne s'agit pas de contenu malveillant avant de les transmettre à votre réseau.

Logiciels antivirus

Les logiciels antivirus défendent les appareils contre les maliciels grâce aux fonctionnalités suivantes :

- analyse des fichiers pour y détecter les virus avant le téléchargement sur votre appareil;
- blocage du téléchargement de logiciels malveillants connus;
- analyse des fichiers de votre système en fonction d'une liste de virus connus et suppression de tout virus détecté.

Réseaux privés virtuels (RPV)

Un RPV constitue un réseau de communications privé (qu'on appelle un tunnel) qui passe à travers un réseau non fiable. Il sert à établir une connexion sécurisée au moyen de l'authentification et à protéger le trafic de données.

Le RPV permet de transmettre et de recevoir des données par l'entremise d'un tunnel chiffré qui les protège contre les auteurs de menace. Vous pouvez l'utiliser au sein de votre organisation ou entre diverses organisations pour communiquer sur un réseau élargi.

Pour en savoir plus sur les RPV, consultez l'ITSAP.80.101 (*Les réseaux privés virtuels)* sur le site Web du CCC.

Liste d'applications autorisées

Les listes d'applications autorisées permettent de contrôler les applications autorisées à s'exécuter sur un appareil.

- Elles autorisent les applications et les composantes connexes pouvant s'exécuter sur les systèmes de l'organisation.
- Elles empêchent les utilisateurs d'installer des logiciels non autorisés.

Virtualisation

La virtualisation consiste à créer un environnement isolé dans lequel des applications particulières peuvent s'exécuter sur votre appareil. Elle permet de renforcer la sécurité grâce aux fonctionnalités suivantes :

- séparation des applications professionnelles des applications utilisées à des fins personnelles;
- isolation d'applications et de processus particuliers pour des groupes et secteurs d'activité donnés;
- téléchargement de contenu malveillant aux fins d'analyse dans un environnement isolé de manière à prévenir l'accès à d'autres applications.

SÉRIE SENSIBILISATION

Bloqueurs de publicité

Un bloqueur de publicité est un module d'extension d'un navigateur qui empêche les messages publicitaires (p. ex. les publicités intégrées aux pages Web et les fenêtres surgissantes) de s'afficher lorsque vous naviguez sur le Web.

Logiciels antihameçonnage

Les logiciels antihameçonnage signalent et bloquent les courriels d'hameçonnage dans le but de prévenir les attaques et leur propagation (p. ex. par l'entremise d'autres destinataires). Ils peuvent vous aider à prévenir le vol d'identité, la fraude par carte de crédit et les pertes financières.

Vous devriez également appliquer les stratégies DMARC (Domain-based Message Authentication, Reporting, and Conformance) afin d'empêcher les hameçonneurs d'usurper le domaine de votre organisation pour envoyer de faux courriels. Ces stratégies authentifient et filtrent également les domaines, ce qui permet de détecter les domaines d'hameçonnage dissimulés parmi les domaines légitimes.

Pour en savoir plus sur la prévention de l'hameçonnage, consultez l'ITSAP.00.100 *(Reconnaître les courriels malveillants)* et l'ITSAP.00.101 *(Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage)* sur le site Web du CCC.

Services de sécurité infonuagique

Dans le cadre des services infonuagiques, vous pouvez vous procurer des services de sécurité afin de protéger vos réseaux, vos données et vos comptes dans le nuage. Voici quelques exemples de fonctionnalités de sécurité :

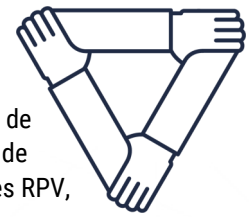
- chiffrement et gestion des clés pour protéger vos données;
- filtrage du trafic en fonction de règles que vous créez (p. ex. bloquer les adresses HTTP et les modes d'attaques courants);
- détection d'activités réseau et de comportements liés aux comptes qui sont associés à des menaces (p. ex. l'accès non autorisé) dans votre environnement infonuagique;
- protection antirançongiciel et antimaliciel visant à empêcher les auteurs de menace de voler ou d'endommager les données.

Courtier de sécurité d'accès au nuage (CASB pour *Cloud Access Security Broker*)

Un logiciel CASB vous aide à surveiller l'utilisation de vos services infonuagiques en offrant les fonctionnalités de sécurité suivantes :

- validation du trafic réseau entre les appareils de votre organisation et le fournisseur de services infonuagiques pour veiller à ce qu'il soit conforme avec les stratégies de sécurité de votre organisation;
- détection des menaces et surveillance des données sensibles en transit.

GESTION UNIFIÉE DES MENACES (UTM POUR *UNIFIED THREAT MANAGEMENT*)



Les solutions UTM (p. ex. des appliances matérielles, des logiciels ou des services infonuagiques) comportent de multiples fonctions permettant de contrer divers types de menaces. Elles comptent souvent des outils de sécurité préventive comme des pare-feux, des RPV, des logiciels antihameçonnage, des listes d'applications autorisées et le filtrage du contenu Web. Les solutions UTM analysent le contenu entrant dans le système pour s'assurer qu'il est inoffensif avant de le transmettre à l'utilisateur. Elles suppriment le contenu malveillant détecté avant que l'appareil y accède, puis envoie un avis à l'utilisateur pour l'informer de cette suppression.

POINTS À RETENIR

Vos politiques organisationnelles en matière de sécurité peuvent vous aider à choisir les outils de sécurité préventive qui conviennent à votre organisation. Bien que ces outils de sécurité contribuent à réduire les risques en matière de cybersécurité, les auteurs de menace peuvent avoir recours à d'autres techniques pour accéder à vos systèmes. Par conséquent, nous vous recommandons de mettre en œuvre les pratiques de sécurité additionnelles ci-dessous :

- Appliquez régulièrement les correctifs et les mises à jour de vos logiciels de sécurité.
  - Si vos logiciels sont obsolètes, vos appareils sont plus susceptibles de se faire infecter par du contenu malveillant.
  - Pour en savoir plus, consultez l'ITSAP.10.096 *(Application des mises à jour sur les dispositifs)*.
- Appliquez le principe du droit d'accès minimal.
  - Accordez aux utilisateurs uniquement les privilèges dont ils ont besoin pour faire leur travail, ce qui limitera les dommages en cas d'utilisation non autorisée ou inappropriée (accidentelle ou non) des données et des systèmes.
- Offrez aux employés de la formation sur mesure.
  - Favorisez la sensibilisation aux menaces courantes pour la cybersécurité.
  - Veillez à ce que les employés connaissent leurs responsabilités en ce qui concerne l'utilisation des outils de sécurité préventive.
  - Pour en savoir plus, consultez l'ITSAP.10.093 *(Offrir aux employés une formation sur mesure en cybersécurité)*.

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**.