Les outils de sécurité préventive

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Mai 2024 | ITSAP.00.058

Les outils de sécurité préventive offrent d'importantes couches de protection pour vos réseaux et vos appareils. Ils peuvent également aider votre organisation à réduire les risques d'intrusion malveillante, dont les maliciels, les espiogiciels et les utilisatrices et utilisateurs non autorisés.

Exemples d'outils de sécurité préventive

Chacun des outils de sécurité suivants cible des aspects précis afin de prévenir la compromission des réseaux et des appareils de votre organisation.

Les pare-feux sont des barrières de sécurité placées entre deux réseaux qui contrôlent le volume et les types de trafic autorisés à passer d'un réseau à l'autre. Ils préviennent la transmission non autorisée de données d'une zone du réseau à une autre grâce aux fonctionnalités suivantes :

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

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

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

Les réseaux privés virtuels (RPV) sont des réseaux de communications privés (que l'on appelle des tunnels) qui passent à travers un réseau non fiable. Un RPV 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 auteures et 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 la publication intitulée Les réseaux privés virtuels (ITSAP.80.101).

Les bloqueurs de publicité constituent un type de module d'extension d'un navigateur qui empêche les messages publicitaires, notamment les publicités intégrées aux pages Web et les fenêtres surgissantes, de s'afficher lorsque vous naviguez sur le Web.

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 :

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

Les listes d'applications autorisées et interdites permettent de contrôler les applications autorisées à s'exécuter sur un appareil. Elles peuvent :

- autoriser les applications et les composantes connexes à s'exécuter sur les systèmes d'une organisation;
- empêcher les utilisatrices et utilisateurs d'installer des logiciels non autorisés.

Les logiciels antihameçonnage signalent et bloquent les courriels d'hameçonnage dans le but de prévenir les attaques et leur propagation 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 hameçonneuses et 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 les publications intitulées Reconnaître les courriels malveillants (ITSAP.00.100) et Ne mordez pas à l'hameçon : reconnaître et prévenir les attaques par hameçonnage (ITSAP.00.101).

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Cat No. D97-1/100-058-2024F-PDF

ISBN 978-0-660-70841-6

Canada

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. Ces services peuvent comprendre des fonctions de sécurité telles que les suivantes :

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

Un agent de sécurité d'accès au nuage est une solution logicielle qui applique les stratégies de sécurité de votre organisation grâce aux fonctionnalités suivantes :

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

Outils de sécurité basés sur l'intelligence artificielle

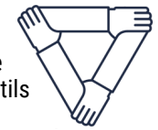
L'intelligence artificielle (IA) assure une application plus efficace et précise des outils de sécurité. Les algorithmes d'apprentissage automatique permettent à l'IA de s'adapter aux nouvelles menaces et d'y réagir en temps réel. De nombreux outils de sécurité traditionnels reposent sur des systèmes de détection basés sur les règles ou les signatures qui fonctionnent seulement pour la détection de menaces connues. Dans les outils de sécurité basés sur l'intelligence artificielle, les algorithmes utilisent des données d'entraînement pour apprendre à répondre à différentes situations.

L'intelligence artificielle peut améliorer la sécurité des façons suivantes :

- suivre le rythme des menaces émergentes et inconnues;
- simplifier le processus d'intervention par l'automatisation des tâches courantes;
- journaliser et analyser de larges volumes de données;
- limiter le nombre de faux positifs dans les résultats de menaces et améliorer les taux de détection.

Il convient cependant de souligner que l'intelligence artificielle n'est pas exempte de défauts. Elle est sujette à ses propres biais en fonction de ses données d'entraînement, et les détections de menaces basées sur l'IA devraient toujours être accompagnées d'une expertise humaine. Les données sur lesquelles repose l'entraînement de l'IA peuvent s'avérer inexactes ou illogiques. Elles peuvent aussi faire l'objet de falsification et de mésinformation. Pour en savoir plus sur l'IA, consultez les publications intitulées Intelligence artificielle (ITSAP.00.040) et L'intelligence artificielle générative (ITSAP.00.041).

Gestion unifiée des menaces



La gestion unifiée des menaces (UTM pour *Unified Threat Management*) est une solution qui intègre de multiples fonctions permettant de contrer divers types de menaces. Elle compte souvent des outils de sécurité préventive comme des pare-feux, des RPV, des logiciels antihameçonnage, des listes d'applications autorisées et le filtrage de 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'utilisatrice ou à l'utilisateur. Elles suppriment le contenu malveillant détecté avant que l'appareil y accède, puis envoie un avis à l'utilisatrice ou à l'utilisateur pour l'informer de cette suppression.

Pratiques de sécurité additionnelles

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 auteures et auteurs de menace peuvent avoir recours à d'autres techniques pour accéder à vos systèmes. Par conséquent, il est recommandé de mettre en œuvre les pratiques de sécurité additionnelles ci-dessous.

- Appliquez régulièrement les correctifs et les mises à jour à 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 la publication intitulée Application des mises à jour sur les dispositifs (ITSAP.10.096).
- Appliquez le principe du droit d'accès minimal.
  - Vous devriez accorder aux utilisatrices et utilisateurs uniquement les privilèges dont ils ont besoin pour effectuer leur travail.
  - Ce principe permet de limiter les dommages pouvant résulter d'une utilisation non autorisée, abusive ou accidentelle des données et des systèmes.
  - Pour plus d'information, consultez la publication intitulée Gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA) (ITSAP.30.018).
- Offrez au personnel de la formation sur mesure.
  - Favorisez la sensibilisation aux menaces courantes en matière de cybersécurité.
  - Veillez à ce que les employées et employés connaissent leurs responsabilités en ce qui concerne l'utilisation des outils de sécurité préventive.
  - Pour plus de détails, consultez la publication intitulée Offrir aux employés une formation sur mesure en cybersécurité (ITSAP.10.093).

Pour en savoir plus

- Apprenez à protéger votre information et vos données lorsque vous utilisez des applications (ITSAP.40.200)
- Journalisation et surveillance de la sécurité de réseau (ITSAP.80.085)
- Les 10 mesures de sécurité des TI : No 10, Mettre en place une liste d'applications autorisées (ITSM.10.095)
- Cybersecurity and Infrastructure Security Agency: Free cybersecurity services and tools (en anglais seulement)