CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

OCTOBRE 2024| ITSAP.40.017

Sécurité liée aux navigateurs Web : un aperçu

Presque tous les appareils informatiques que vous utilisez de nos jours ont un navigateur Web installé. C'est pourquoi il est très important de s'assurer qu'ils sont sécurisés. Pour ce faire, il faut non seulement configurer les paramètres de sécurité, mais aussi comprendre comment certains protocoles Web fonctionnent. Ce faisant, vous aidez à protéger vos données et vos systèmes informatiques contre les auteures et auteurs de menace. La présente publication souligne certains des principaux moyens de communication Web et la façon dont ils protègent vos renseignements personnels.

Protocoles de communications

Les protocoles sont des ensembles de règles qui permettent à plusieurs appareils de transmettre des données et de communiquer entre eux. Ces règles définissent le type de données qui peut être envoyé, la structure de l'information et la façon dont chaque appareil reçoit les données.

Il existe beaucoup de protocoles de communications de nos jours. En voici quelques-uns des plus courants :

- Protocole de sécurité de la couche transport (TLS pour *Transport Layer Security*)
- Protocole de transfert hypertexte (HTTP pour *Hypertext Transfer Protocol*)
- Protocole de transfert hypertexte sécurisé (HTTPS pour *Hypertext Transfer Protocol Secure*)

Certificat TLS

Le protocole TLS protège les données envoyées par l'entremise de l'Internet. Il garantit que les auteures et auteurs de menace ne peuvent pas voir l'information que vous transmettez, comme vos mots de passe ou numéros de carte de crédit. De plus, il authentifie les serveurs Web au moyen d'un certificat émis par une entité de confiance, appelée autorité de certification. Le certificat lie une clé cryptographique à l'adresse de domaine du serveur Web. Grâce à cette clé cryptographique, le protocole TLS utilise le chiffrement pour garantir que le transfert des données entre le serveur Web et le navigateur est sécurisé.

HTTP

Le protocole HTTP est utilisé pour transférer des données par l'intermédiaire d'un réseau. Il n'offre pas de sécurité. Par conséquent, vos données se retrouvent en texte clair et peuvent être surveillées à tout moment dans le chemin de transmission réseau entre le serveur Web et votre navigateur.

HTTPS

Le protocole HTTPS utilise le protocole TLS pour chiffrer les données envoyées à partir d'un réseau ou reçu sur ce-lui-ci. Un symbole de cadenas au début de l'adresse Web sur certains navigateurs indique l'utilisation du protocole HTTPS.

Ce protocole chiffre le contenu afin de protéger les renseignements personnels et les authentifier, de sorte à empêcher leur modification. Même si le protocole HTTPS est plus sécurisé que le protocole HTTP, il n'est pas à l'abri des attaques de type adversaire au milieu (AitM pour *Adversary in the Middle*).

Le déclassement TLS est une technique AitM qu'utilisent les auteures et auteurs malveillants pour convertir une connexion sécurisée HTTPS en connexion non sécurisée HTTP. Les navigateurs Web avertissent parfois les internautes lorsque le protocole HTTPS est rejeté ou qu'il est déclassé à HTTP et lui donne l'option de mettre fin à sa connexion.

La présence du protocole HTTPS ne garantit pas en soi qu'un site Web est légitime. Les auteures et auteurs de menace sophistiqués peuvent mystifier un site Web en créant un site en apparence sécurisé afin de vous inciter à inscrire vos renseignements personnels. On conseille aux internautes de vérifier attentivement que l'adresse Web correspond au bon domaine.

HSTS

Le protocole HTTPS Strict Transport Security (HSTS) est un outil de stratégies de sécurité Web, qui force le navigateur à charger la version sécurisée d'un site Web et ignore les tentatives de redirection à un site Web non sécurisé. Le protocole HSTS est une configuration du côté du serveur. Il aide à prévenir le déclassement TLS.

Stratégie de sécurité du contenu

La Stratégie de sécurité du contenu est une norme de sécurité des navigateurs Web largement reconnue, qui détecte et atténue certains types d'attaques, comme le script intersites et l'injection de code. Ces attaques peuvent entraîner un vol de données, la défiguration de sites Web ou la distribution de maliciels.

Pour mettre en œuvre la Stratégie, les développeuses et développeurs Web doivent produire une liste des origines approuvée pour tout le contenu qu'un navigateur est autorisé à charger pour un site Web précis. En d'autres mots, le contenu que le navigateur peut charger et d'où il peut l'être. Le contenu peut inclure les suivants :

- JavaScript;
- Feuilles de style en cascade (CSS pour *Cascading Style Sheets*);
- Fichiers HTML;
- Police;
- Fichiers audio, vidéo et image.

Pixels espions

Les pixels espions sont de minuscules images de taille 1x1 pixel, qui sont incrustés dans le langage HTML des pages Web, des publicités et des courriels. Ces images sont hébergées sur un serveur et recueillent de l'information à propos de l'utilisatrice ou de l'utilisateur pendant qu'il navigue sur la page Web. Les entreprises les utilisent généralement pour améliorer leurs efforts publicitaires en recueillant de l'information à propos des intérêts et des habitudes d'une personne dans le but de créer des publicités ciblées. Les pixels espions peuvent notamment :

- recueillir de l'information sur l'emplacement, comme des adresses IP;
- déterminer si vous avez fait certaines actions sur une page Web, comme vous inscrire à une liste de distribution;
- suivre les pages vues, les clics et les redirections;
- établir le type d'appareil utilisé et le système d'exploitation.

Un des principaux problèmes liés aux pixels espions est la protection des renseignements personnels. Ils recueillent souvent des données qu'ils envoient à leur serveur d'origine sans que l'internaute le sache ou donne son consentement. Les pixels espions sont également vulnérables aux fuites de données si l'information qu'ils recueillent n'est pas correctement dépouillée des renseignements personnels et identifiables avant d'être transmise au serveur. Les pages Web devraient divulguer qu'elles utilisent des pixels espions et donner l'option à l'internaute de les refuser. Veuillez consulter la section sur les extensions et les plugiciels pour obtenir des conseils quant à l'atténuation.

Centre de la sécurité des télécommunications Canada
Communications Security Establishment Canada

No. de cat D97-1/40-017-2024F-PDF

ISBN 978-0-660-73889-5

Canada

Témoins Internet

À l'instar des pixels espions, les témoins recueillent et stockent de l'information à propos des utilisatrices et utilisateurs et leurs habitudes en ligne. Cette information est stockée dans le fichier du navigateur Web.

L'utilisation des témoins peut aider à améliorer l'expérience utilisateur, comme poursuivre la connexion au site d'un détaillant pour mettre à jour les articles dans le panier. Ils peuvent également être utilisés pour améliorer les efforts publicitaires, puisqu'ils surveillent qui visite une page Web et comment se passe l'interaction avec du contenu en ligne précis. Certains témoins sont nécessaires pour assurer le bon fonctionnement d'un site Web, étant donné qu'ils permettent d'authentifier et de gérer la session d'une utilisatrice ou d'un utilisateur. D'autres témoins peuvent être désactivés par l'utilisatrice ou utilisateur, comme les témoins publicitaires.

Toutefois, les témoins peuvent être vulnérables à l'empoisonnement ou au piratage. Les auteures et auteurs de menace peuvent se servir des témoins pour se faire passer pour des utilisatrices ou utilisateurs et voler des renseignements sensibles. La pratique exemplaire recommandée est d'autoriser seulement les témoins de fonctionnement.

Pratiques exemples concernant les pixels espions et témoins Internet

- N'autorisez que les témoins nécessaires et de fonctionnement.
- Effectuez régulièrement des balayages de maliciel.

Plugiciels et extensions de navigateurs Web

De nombreux plugiciels et extensions de navigateurs prétendent mieux protéger les renseignements personnels et la cybersécurité. Ils peuvent notamment bloquer les publicités, gérer les mots de passe et générer des coupons lors du magasinage en ligne. Ils peuvent permettre à l'internaute de personnaliser son expérience de navigation de toutes sortes de manières. Il y a constamment de nouveaux plugiciels et de nouvelles extensions. Il faut payer pour certains, tandis que d'autres sont gratuits. Certains sont créés par des entreprises légitimes, d'autres non.

Les extensions et plugiciels se voient accorder certaines autorisations dans le navigateur, qui peuvent être exploitées par les auteures et auteurs de menace. Ils peuvent demander l'autorisation de recueillir toute l'information que le navigateur voit, y compris les mots de passe et les saisies au clavier. Certaines extensions peuvent avoir secrètement un maliciel dans leur code qui pourrait affecter votre appareil dès le téléchargement. Le moins d'extensions vous avez, mieux c'est.

Pratiques exemplaires concernant les plugiciels et extensions

- Ne téléchargez des plugiciels ou extensions qu'à partir de sites officiels de confiance.
- Passez en revue les autorisations avant de les accepter.
- Lisez les avis des autres internautes avant d'installer un plugiciel ou une extension.

Paramètres de sécurité de votre navigateur Web

Bien souvent, le navigateur installé sur un appareil fonctionne en utilisant seulement les paramètres de sécurité par défaut. Afin d'accroître la sécurité de votre navigateur, prenez les mesures suivantes :

- Bloquer les témoins de tierce partie pour éviter le suivi;
- Bloquer les fenêtres publicitaires;
- Activer les mises à jour automatiques;
- Éviter d'enregistrer des mots de passe dans le navigateur en soi;
- Autoriser Java seulement lorsqu'il est nécessaire;
- Vérifier vos paramètres de navigateur avant de naviguer à l'extérieur de
- l'Intranet géré par votre organisation (p. ex. le mode Internet Explorer est-il activé dans Microsoft Edge?).

Si vous configurez un site Web, il est recommandé de prendre les mesures suivantes :

- Publier les services au moyen du protocole HTTPS;
- Rediriger les utilisatrices et utilisateurs de la version HTTP de vos services à l'option HTTPS;
- Utiliser le logiciel TLS le plus récent et y apporter les correctifs
- régulièrement;
  Activer le protocole HSTS pour sécuriser les connexions à vos services.

Mesures de sécurité pour votre ordinateur

Sécuriser votre ordinateur va de pair avec sécuriser votre navigateur. Il suffit de prendre des mesures simples comme les suivantes pour sécuriser votre ordinateur :

- Utiliser des mots de passe forts et uniques pour vous connecter à des services;
- Installer et exécuter un logiciel antivirus et antimaliciel;
- Activer les mises à jour automatiques si possible;
- Adopter le principe de droit d'accès minimal à vos comptes utilisateur;
- Éviter les comportements risqués en ligne;
- Sauvegarder vos données régulièrement;
- Filtrer les URL au niveau du pare-feu.

Recommandations de sécurité liées aux navigateurs Web pour votre organisation

- Déterminez les sites de confiance et d'accès restreint.
- Confirmez la fiabilité des bloqueurs de publicité ou des plugiciels tiers.
- Vérifiez les autorisations pour déterminer le niveau de privilèges.
- Utilisez un navigateur Web standard partout dans votre organisation.
- Autorisez seules les témoins de fonctionnement.
- Éduquez votre personnel au sujet des fenêtres publicitaires, des témoins et des vulnérabilités des navigateurs Web.
- Mettez à jour le logiciel antimaliciel régulièrement et installez un pare-feu.
- Passez régulièrement en revue les appareils périphériques pour détecter les produits obsolètes.

Centre de la sécurité des télécommunications Canada
Communications Security Establishment Canada

Canada