DÉFIGURATION DE SITE WEB

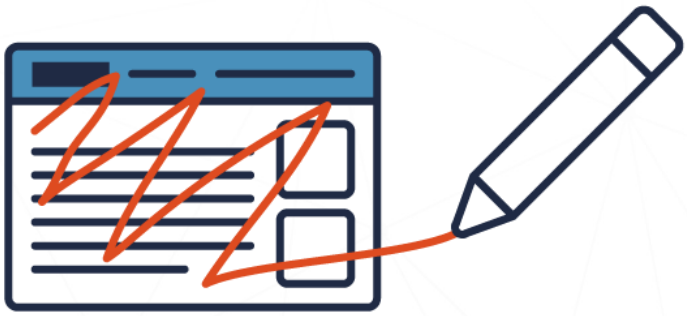
MAY 2020

ITSAP.00.060

Le présent document vise à vous faire découvrir la **défiguration de site Web**, une forme de cyberattaque. Vous pouvez penser à la défiguration comme du vandalisme ou un graffiti virtuel. Un pirate défigure un site Web en changeant son apparence ou son contenu. Les auteurs de menaces choisissent la défiguration pour différentes raisons : pour tenter d'embarrasser les propriétaires de sites Web ou pour faire la promotion de points de vue différents. Dans certains cas, un auteur de menace défigure un site Web en y injectant du code malveillant. Lisez les paragraphes qui suivent pour savoir comment vous protéger contre ce type d'attaques.

COMMENT LES SITES WEB SONT-ILS DÉFIGURÉS?

Les pirates ont recours à différentes méthodes pour défigurer des sites Web. Habituellement, ils injectent du code malicieux dans le script du site, ce qui leur permet d'en prendre le contrôle. En contrôlant le site, ils peuvent obtenir des accès privilégiés et accéder à son contenu. Lorsqu'ils défigurent un site, les pirates informatiques peuvent utiliser un réseau virtuel privé (RPV) pour garantir leur anonymat. En utilisant un logiciel de balayage automatisé pour trouver les vulnérabilités du site Web, les attaquants peuvent ensuite accéder au site à partir d'une faille du programme (c.-à-d., une vulnérabilité). Les pirates peuvent prétendre être des utilisateurs autorisés, accéder à distance aux fichiers des sites Web et exécuter leurs propres commandes.



POURQUOI DES SITES WEB SONT-ILS DÉFIGURÉS?

Il y a plusieurs raisons qui motivent des attaquants à compromettre ou à défigurer un site Web. Ce peut être, entre autres, pour des raisons personnelles ou politiques ou encore pour les suivantes :

- des motivations sociales ou politiques (p. ex., protester contre un mouvement en particulier, c'est le cas des « hacktivistes »);
- du trafic qui génère un profit (p. ex., rediriger le trafic commercial vers des sites Web infectés pour faire du profit ou pour exploiter des cibles);
- le piratage de la bande passante ou d'une ressource informatique (p. ex., propager des attaques automatiques);
- le vol de renseignements personnels (p. ex., voler les renseignements personnels d'un client);
- l'ego, c'est-à-dire le plaisir personnel ou le défi (p. ex., narguer les propriétaires de sites Web en exploitant leurs vulnérabilités).

QU'EST-CE QUE JE FAIS SI MON SITE WEB EST DÉFIGURÉ?

Ne paniquez pas! Les auteurs de menaces cherchent une réaction de votre part (p. ex., votre attention, de la peur). Si vous êtes victime d'une attaque, suivez les étapes ci-dessous pour restaurer votre site Web :

- Si votre site est hébergé par un fournisseur, communiquez avec lui pour signaler toute activité anormale;
- Remplacez immédiatement votre site Web par une page de maintenance;
- Inspectez tout le contenu et les dernières sauvegardes informatiques du site pour y déceler tout maliciel ou vulnérabilité cachée;
- Informez les parties concernées de l'incident (p. ex., clients, fournisseurs, tierce partie);
- Faites une déclaration publique pour préserver la réputation de votre organisme;
- Restaurez votre site Web à partir de vos sauvegardes informatiques pour garantir un rapide retour à la normale;
- Signalez tout incident à la police;
- Demandez à votre équipe de soutien technique de faire une analyser pour découvrir de quelle manière votre site Web a été défiguré et pour évaluer votre processus d'intervention (p. ex., pour vous améliorer de manière à éviter des complications futures).

COMMENT CHOISIR UN FOURNISSEUR POUR HÉBERGER MON SITE WEB?

Si vous pensez héberger votre site Web chez un fournisseur, posez les questions ci-dessous afin de cerner quelles mesures le fournisseur a en place pour intervenir en cas de défiguration et pour récupérer votre site.

PLAN

- Quelles procédures de sécurité le fournisseur a-t-il en place?
- À quelle fréquence les sauvegardes informatiques sont-elles effectuées et où sont-elles enregistrées?
  - Les sauvegardes informatiques devraient être enregistrées loin du serveur principal et en un lieu sûr pour garantir qu'une récupération saine du système est possible.
  - Un historique de sauvegarde informatique devrait être considéré pour déterminer si une sauvegarde précédente peut être utilisée pour restaurer votre site, selon l'état de la dernière sauvegarde.
- Quel type de technologie ou d'outil est utilisé pour empêcher les intrusions (p. ex., pare-feu et protocole SSL)?

INTERVENTION

- À quelle fréquence le fournisseur surveille le réseau pour déceler les activités non autorisées?
  - Si un maliciel est détecté assez tôt, on peut en réduire les méfaits (p. ex., on peut faire tourner un antivirus et procéder à un balayage de maliciel);
  - Les résultats de ces balayages devraient être accessibles.
- Est-ce que le fournisseur a un plan d'intervention et des procédures pour déterminer qui sont les administrateurs affectés à l'intervention en cas d'incidents?
- De quelle manière un administrateur obtient le contrôle?
  - Le nombre d'accès administrateur devrait être limité;
  - On devrait utiliser une authentification à multiples facteurs;
  - Les administrateurs devraient passer un contrôle de sécurité avant qu'on leur donne accès.

RÉCUPÉRATION

- Dans combien de temps prévoit-on que le site Web soit récupéré s'il était attaqué?
  - Une page de maintenance devrait être préparée et prête à publier;
  - Pensez à une mention spécifique relative au temps de récupération de votre site Web dans votre entente de services.
- Pendant combien de temps les rapports d'audit sont-ils conservés à des fins d'examen et d'analyse (p. ex., assez longtemps pour permettre de surveiller la potentielle répétition de menaces)?
- Est-ce que le fournisseur est au courant des menaces émergentes (p. ex., des vulnérabilités qui peuvent être exploitées avant qu'un correctif soit publié)?
- Quelles sont les procédures pour éviter les attaques d'ingénierie sociale (p. ex., l'auteur d'une menace appelle pour demander le changement d'une donnée)?
- De quelle manière le fournisseur protège-t-il les données? Par des routeurs et des interrupteurs de sécurité qui permettent de s'assurer que les attaques n'atteignent pas le site?
- Est-ce que les données sont chiffrées, et les clés de chiffrement en lieu sûr?
  - Les clés de chiffrement ne devraient pas être entreposées avec les données. Elles devraient être entreposées par le fournisseur ou par un tiers fournisseur.

COMMENT PROTÉGER LE SITE WEB QUE J'HÉBERGE MOI-MÊME?

Si vous hébergez votre site Web vous-même, vous devriez considérer les conseils de sécurité ci-dessous pour protéger votre site Web de la défiguration :

- Utilisez une phrase de passe ou un mot de passe robuste pour éviter de faciliter l'accès aux auteurs de menace en utilisant des justificatifs d'identité par défaut;
- Gérez les accès des comptes d'utilisateur et minimisez les privilèges aux comptes d'administrateur (p. ex., supprimer les utilisateurs qui quittent l'organisme ou qui n'ont plus besoin d'accès en particulier);
- Déterminez une personne-ressource (et un remplaçant) pour intervenir en cas d'incident;
- Formez les employés sur les procédures d'intervention en cas d'incident;
- Utilisez un pare-feu pour signaler et bloquer le trafic malicieux;
- Utilisez des outils de surveillance et de détection pour suivre les changements non autorisés à votre site Web;
- Faites les sauvegardes informatiques normales avant de faire des mises à jour;
- Mettez à jour les plugiciels afin de corriger les bogues et les problèmes de sécurité;
- Installez les mises à jour et les correctifs sur le serveur de votre site Web.

La sécurité devrait être prise en considération dès la conception et le développement de votre site Web. Collaborez avec les membres de votre équipe de développement pour vous assurer qu'ils sont formés en sécurité informatique et qu'ils adoptent des pratiques de codage sécuritaire, comme les suivantes :

- Encodez les données de sortie (p. ex., fichiers HTML et URL) de manière appropriée pour prévenir les exploits intersite;
- Utilisez des options de codage particulières (p. ex., la bibliothèque d'un tiers) pour protéger les sites Web contre les exploits d'injection de SQL;
- Configurez vos témoins avec l'attribut « HTTPS-only » pour protéger votre site Web contre les pirates qui tenteraient d'accéder aux justificatifs d'identité d'un utilisateur;
- Assurez-vous que le code du côté serveur ne puisse pas être téléchargé.

Vous choisirez peut-être de faire appel à un spécialiste de la sécurité qui vous aidera à évaluer le niveau de sécurité de vos systèmes ainsi qu'à déterminer d'autres façons de protéger votre site Web, par exemple en faisant des balayages pour trouver des vulnérabilités ou en effectuant des tests de pénétration.

Un organisme sans but lucratif appelé *Open Web Application Security Project* (OWASP) offre des ressources éducatives, des lignes directrices et des outils à source ouverte qui peuvent vous aider à améliorer la sécurité du logiciel que vous utilisez.
Pour en savoir plus, visitez leur site Web : **https://www.owasp.org/**

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**.