Défigurement de site Web

Février 2024

ITSAP.00.060

La défiguration de site Web est une forme de cyberattaque. Vous pouvez penser à la défiguration comme du vandalisme ou un graffiti virtuel. Une ou un pirate défigure un site Web en changeant son apparence ou son contenu. Les auteures et 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, l'auteure ou auteur de menace défigure un site Web en y injectant du code malveillant. Le présent document peut vous aider à savoir comment protéger votre site Web 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. Les pirates peuvent avoir recours à un logiciel de balayage automatisé pour trouver les vulnérabilités du site Web. Ils peuvent ensuite accéder au site à partir d'une faille du programme, comme par injection SQL (Structured Query Language) injection ou par script intersites. Les pirates peuvent aussi se faire passer pour des utilisatrices et utilisateurs autorisés, accéder à distance aux fichiers des sites Web et exécuter leurs propres commandes. Veuillez consulter la publication Les réseaux privés virtuels (ITSAP.80.101) pour en apprendre davantage.

Pourquoi des sites Web sont-ils défigurés?

Les pirates peuvent défigurer un site Web pour des motivations personnelles et politiques. Il y a plusieurs raisons qui les motivent à compromettre ou à défigurer des sites Web. En voici des exemples :

- les motivations sociales et politiques, par exemple, protester contre un mouvement en particulier, c'est le cas des « hacktivistes »;
- la possibilité de réaliser des profits ou d'exploiter des victimes en redirigeant le trafic vers des sites Web commerciaux ou infectés;
- le piratage de la bande passante ou une ressource informatique, comme de propager des attaques automatiques;
- le vol de renseignements personnels, par exemple, voler les renseignements personnels d'un client;
- l'ego, c'est-à-dire le plaisir personnel ou le défi, comme 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. 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, comme les clients, les fournisseurs et les tierces parties;
- 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.

AWARENESS SERIES

Cat. No. D97-1/00-060-2024F-PDF
ISBN 978-0-660-70413-5

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.

Planification

- Quelles procédures de sécurité le fournisseur a-t-il en place?
- À quelle fréquence les sauvegardes informatiques du fournisseur 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, par exemple, des pare-feu et le protocole TLS?

Réponse

- À quelle fréquence le fournisseur surveille-t-il le réseau pour déceler les activités non autorisées?
  - Si un maliciel est détecté assez tôt, on peut en réduire les méfaits en faisant tourner un antivirus et en procédant 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 administratrices et administrateurs affectés à l'intervention en cas d'incidents
- Que faut-il faire pour contrôler l'accès des administratrices et administrateurs?
  - Limitez le nombre d'accès administrateur.
  - Utilisez l'authentification à facteurs multiples (AFM) pour tous les comptes lorsque c'est possible.
  - Effectuez un filtrage de sécurité pour les administratrices et administrateurs avant qu'on leur donne accès.

Reprise

- Dans combien de temps prévoit-on que le site Web soit récupéré s'il était attaqué?
  - Préparez une page de maintenance.
  - 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 de vérification sont-ils conservés à des fins d'examen et d'analyse? Par exemple, assez longtemps pour permettre de surveiller la potentielle répétition de menaces?
- Le fournisseur sait-il comment gérer des menaces émergentes? Par exemple, sait-il s'il y a des vulnérabilités qui peuvent être exploitées avant qu'un correctif soit publié
- Quelles sont les procédures pour éviter les attaques d'ingénierie sociale, comme lorsqu'une auteure ou un auteur de 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 mises 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 votre site Web autohébergé?

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 auteures et 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. Par exemple, supprimer les utilisatrices et utilisateurs qui quittent l'organisme ou qui n'ont plus besoin d'accès en particulier;
- déterminez une personne-ressource et une remplaçante ou remplaçant pour intervenir en cas d'incident;
- formez les employées et employés sur les procédures d'intervention en cas d'incident;
- 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; pour ce faire, il faut :

- encoder les données de sortie (p. ex., fichiers HTML et URL) de manière appropriée pour prévenir les exploits intersite;
- utiliser des options de codage particulières (comme la bibliothèque d'une tierce ou d'un tiers) pour protéger les sites Web contre les exploits d'injection de SQL;
- configurer vos témoins avec l'attribut « HTTPS-only » pour protéger votre site Web contre les pirates qui tenteraient d'accéder aux justificatifs d'identité d'une utilisatrice ou d'un utilisateur;
- veiller à ce que le code du côté serveur ne puisse pas être téléchargé;
- utiliser un système de prévention d'intrusion **(SPI)** pour surveiller les activités malveillantes.

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.

Open Web Application Security Project (OWASP) est un organisme sans but lucratif qui 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

- Trafiquage du service de noms de domaine (DNS) (ITSAP.40.021)
- Journalisation et surveillance de la sécurité de réseau (ITSAP.80.085)
- Facteurs à considérer en matière de cybersécurité pour votre site Web (ITSM.60.005)
- Sauvegarder et récupérer vos données (ITSAP.40.002)
- Gestion et contrôle des privilèges administratifs (ITSAP.10.094)
- Étapes à suivre pour déployer efficacement l'authentification multifacteur (ITSAP.00.105)
- Les 10 mesures de sécurité des TI : n° 6, misé sur une formation sur mesure en matière de cybersécurité (ITSM.10.093)
- Les 10 mesures de sécurité des TI :N^{o} 2 – Appliquer des correctifs aux applications et aux systèmes d'exploitation (ITSM.10.096)