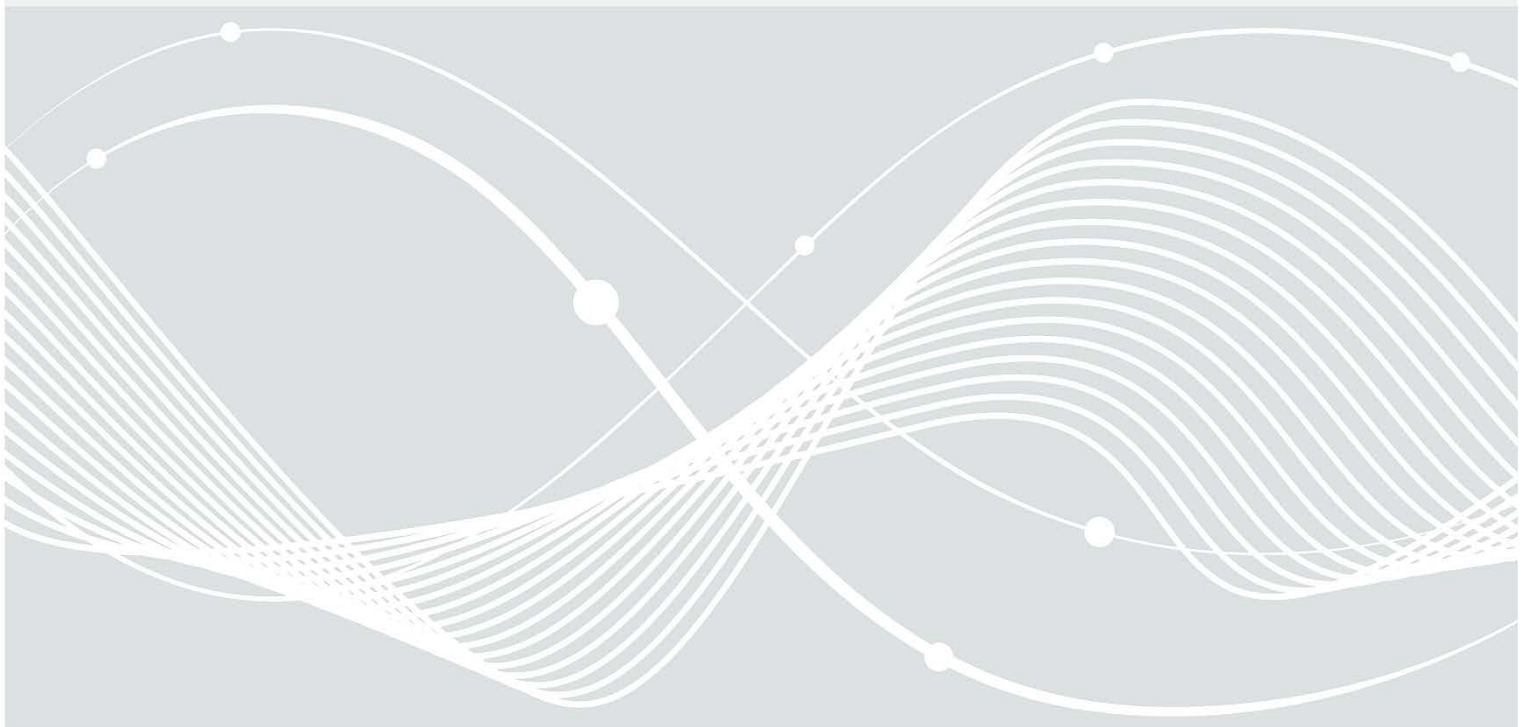




Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Prävention und Erste Hilfe bei Webseiten Kompromittierung oder Defacement



Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel: +49 22899 9582-0
E-Mail: certbund@bsi.bund.de
Internet: <https://www.bsi.bund.de>
© Bundesamt für Sicherheit in der Informationstechnik 2021

Inhalt

1	Welche Arten von Kompromittierung gibt es?	4
1.1	Defacement.....	4
1.2	Schadsoftware.....	4
1.3	Weitere Formen	4
2	Wie erlangen Angreifer Zugriff auf (m)eine Internetpräsenz?.....	5
3	Welche Schritte gilt es nach einem Angriff zu befolgen?.....	6
4	Wie kann ich Angriffen vorbeugen?.....	7
5	Beispielfälle.....	8
6	Mustertext bei Kompromittierung der Webseite.....	9

1 Welche Arten von Kompromittierung gibt es?

1.1 Defacement

Das Wort „Defacement“ stammt vom Englischen „to deface“, was entstellen oder verunstalten bedeutet. Bei einem Defacement wird eine Webseite durch einen Angreifer unter Ausnutzung von Schwachstellen oder ausgespähten bzw. erratenen Zugangsdaten mutwillig verändert. Es werden bestehende Webseiten manipuliert oder neue Unterseiten mit eigenen Inhalten integriert. Die Motivation des Angreifers besteht darin, die Reputation des Webseiten-Betreibers zu schädigen und / oder Ansehen in der Defacement-Szene zu erlangen. In einer verschärften Variante wird die Webseite in ihrem Aussehen komplett verändert und zur Verbreitung von tendenziösen Informationen genutzt. Diese Angriffe sind häufig politisch oder religiös motiviert. Die Webseite Zone-H¹ bietet beispielsweise ein Archiv an (aktuellen) Webseiten-Defacements an.

1.2 Schadsoftware

In der kriminelleren Variante wiederum nutzen Angreifer ein Defacement zur Verbreitung von Schadprogrammen. Wichtigster Zweck ist es, Schadprogramme mithilfe von Drive-by-Exploits² zu verbreiten, d. h. Schadcode auf der Webseite zu platzieren. Ziel ist es beispielsweise, an persönliche Daten der Webseiten-Besucher zu gelangen oder Spam zu verbreiten. So ist ein Ausspähen von persönlichen Daten wie Anschriften oder Kreditkartendaten möglich. Weitere über diesen Weg verbreitete Schadprogramme können andere Schadprogramme nachladen und so letztlich die Dateien auf dem PC des Webseiten-Besuchers verschlüsseln und für die Entschlüsselung ein Lösegeld fordern (Ransomware).

Die Verbreitung von Schadprogrammen erfolgt entweder aus wirtschaftlicher Motivation heraus oder um gezielt sensible Informationen auszuspähen. Im Rahmen von gezielten Angriffen sind derartige Manipulationen von Webseiten unter "Watering Hole" bekannt. In diesem Fall wählt der Angreifer gezielt Webseiten aus, die das Opfer häufig nutzt, um gezielt dieses spezifische Opfer zu infizieren.

1.3 Weitere Formen

Eine weitere Schwachstelle kann ein verwendetes Werbenetzwerk darstellen. Gelegentlich werden über eingebundene Werbung Schadprogramme eingeschleust und Nutzende durch reines Aufrufen der Webseite infiziert.

Genannt seien an dieser Stelle auch speziell eingerichtete Vertipper-Domains, die den Nutzer bei Fehleingaben auf ihre Webseite umleiten (engl. Typo Squatting). Vertippt man sich beispielsweise beim Aufruf von "google.com" und gibt "goggle.com" in seinem Browser ein, landet man gegebenenfalls nicht auf der Webseite der Suchmaschine, sondern auf einer Webseite, die nicht zum Unternehmen der Suchmaschine gehört und möglicherweise mit dem Ziel eingerichtet wurde, Daten abzugreifen oder den Nutzer mit Schadprogrammen zu infizieren.

¹ <https://www.zone-h.org/>

² <https://www.bsi.bund.de/SharedDocs/Glossareintraege/DE/D/Drive-by-Download.html>

2 Wie erlangen Angreifer Zugriff auf (m)eine Internetpräsenz?

Die Verwaltung von Webseiten-Inhalten (Content) wird häufig mithilfe eines CMS (Content Management Systems) durchgeführt. Hier gibt es verschiedene Systeme, die von vielen Betreibern genutzt werden und damit eine interessante Plattform für Angreifer darstellen. Diese finden in regelmäßigen Abständen Sicherheitslücken in den Systemen oder Plugins. Wird also ein veraltetes CMS verwendet, kann es einem Angreifer gelingen, die Webseite nach Belieben zu verändern.

Eine weitere Möglichkeit ist das Erlangen von Zugangsdaten. Denkbar ist hier die Verwendung von Standardpasswörtern, leicht zu erratenden Benutzernamen/Passwort-Kombinationen oder das Abgreifen mittels Schadprogrammen. Erlangt ein Angreifer die Zugangsdaten zur Web-Oberfläche oder zum Webserver, kann er die Webseite beliebig verändern, aber auch beliebigen Code zur Ausführung bringen.

3 Welche Schritte gilt es nach einem Angriff zu befolgen?

1. Bewahren Sie Ruhe und gehen Sie mit Bedacht vor!
2. Schalten Sie die betroffene Webseite offline und ersetzen Sie sie durch eine statische Informationsseite. Einen Beispieltext finden Sie unter Abschnitt 6. Bestenfalls nehmen Sie den befallenen Server komplett vom Netz, um herausfinden zu können, wie der Angreifer Zugriff erlangen konnte.
3. Sichern Sie die Logdateien der Webseite (Webserver-Zugriffe und ggf. Datenbank-Logs).
4. Alle Web-Administratoren müssen Ihren PC auf Schadprogramme untersuchen. Nur so kann überprüft und ausgeschlossen werden, dass Ihr Computer der Ausgangspunkt für den Angriff auf Ihre Webseite gewesen ist. Nutzen Sie Ihren PC erst dann wieder für das Anmelden am Webserver oder der Web-Oberfläche, wenn sichergestellt ist, dass er nicht kompromittiert ist. Ansonsten wäre ein Angreifer nach Änderung der Passwörter in der Lage, diese erneut abzugreifen. Hilfe zu diesem Thema finden Sie auf der Webseite "Digitaler Verbraucherschutz"³ oder nutzen Sie die Antivirenprogramme gängiger Hersteller, um Ihren PC auf Schadprogramme zu untersuchen.
5. Untersuchen Sie Ihren Webserver auf Schadprogramme. Ein erster Schritt stellt das Untersuchen des Webserver auf unbekannte und neue Dateien dar. Ein Abgleich mit einem vorhandenen Backup hilft hier, veränderte Dateien zu erkennen. Weiterhin ist es bei Nutzung eines CMS meist möglich, ein Plugin zum Aufspüren von verdächtigen Dateien zu installieren.
 - Keine Schadprogramme gefunden: Weiter mit Schritt 6.
 - Schadprogramme gefunden: Überprüfen Sie alle Verzeichnisse auf Schadprogramme. Es kann durchaus sein, dass mehrere Webseiten infiziert sind. Wurden die Dateien bzw. Datenbankinhalte gefunden, müssen die infizierten Dateien/Inhalte entfernt werden.
6. Ändern Sie sämtliche Passwörter. Hierunter fällt der Zugang zum Webserver, aber auch der Zugang zum CMS sowie weitere verwendete Software.
7. Setzen Sie die Webseite neu auf.
 - Backup vorhanden: Löschen Sie Ihren kompletten Webspace und spielen Sie Ihr aktuellstes Backup vor Auftreten der Manipulation ein. Vor Online-Schaltung sollte das System auf dem aktuellen Stand sein.
 - Kein Backup vorhanden: Sichern Sie die Daten des Servers auf einem lokalen System. In der Regel lassen sich viele Daten wiederherstellen.
8. Nach Wiederherstellung: Beachten Sie die unten genannten Maßnahmen, um einem erneuten Befall vorzubeugen. Stellen Sie Strafanzeige⁴.
9. Auf dem Server sind Kundendaten hinterlegt: Sollten auf dem Server Kunden- oder Nutzerdaten (also zum Beispiel Anschrift, E-Mail-Adressen oder Passwörter) hinterlegt sein, sollte geprüft werden, ob ein Datenabfluss möglich gewesen ist. Nach Art. 34 DSGVO ist bei unrechtmäßiger Kenntniserlangung von Daten der Betroffene zu informieren. Ggf. muss auch eine Meldung an die zuständige Stelle erfolgen.

³ https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/verbraucherinnen-und-verbraucher_node.html

⁴ https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/IT-Sicherheitsvorfall/Unternehmen/Kontakt-zur-Polizei/Zentrale-Ansprechstellen-Cybercrime/zentrale-ansprechstellen-cybercrime_node.html

4 Wie kann ich Angriffen vorbeugen?

- Aktualisieren Sie regelmäßig sowohl Betriebssystem, CMS sowie jegliche installierte Software, Plugins bzw. Erweiterungen. Verwenden Sie, wenn möglich, automatische Sicherheitsupdates. Hinweise zur sicheren CMS-Installation sowie Informationen über neue Versionen bieten die jeweiligen CMS-Produkte.
- Ändern Sie die Standard-Logins und verwenden Sie nur sichere Passwörter. Des Weiteren sollte eine Mehrfaktor-Authentisierung berücksichtigt werden, um einen wirksamen Schutz gegen gestohlene Passwörter zu bieten.
- Deinstallieren Sie nicht benötigte Software, Plugins bzw. Erweiterungen. Vermeiden Sie die Preisgabe von Informationen, z. B. durch Deaktivierung detaillierter Fehlermeldungen bei der Auslieferung der Webseite.
- Achten Sie auf eventuell bestehende Schwachstellen in Ihren Systemen. Nutzen Sie dafür beispielsweise den Warn- und Informationsdienst von CERT-Bund.
- Erstellen Sie regelmäßig Backups, um im Falle eines Angriffes schnell wieder verfügbar zu sein. Beispielsweise sollten die Inhalte der Webseite sowie der Datenbank gesichert werden. Zusätzlich müssen die Backups regelmäßig auf ihre Nutzbarkeit hin überprüft werden.
- Setzen Sie ggf. auf dem Webserver ein Virenschutz-Programm ein. Damit können beispielsweise schadhafte Inhalte schon beim Hochladen aufgespürt werden.
- Setzen Sie eine Firewall ein, um den Zugriff auf den Webserver zu kontrollieren und ggf. zu unterbinden. Beispielsweise sollte der Webserver nur unter den Ports 443 (verschlüsselt) und ggf. Port 80 (unverschlüsselt) erreichbar sein. Schränken Sie den administrativen Zugriff auf die Webseite ein (z. B. Filterung auf Quell-IP-Adressen, Fail2ban).
- Verschlüsseln Sie vertrauliche und sensible Daten. Für den verschlüsselten Transport von Daten muss SSL/TLS eingesetzt werden. Für die verschlüsselte Speicherung von Daten muss eine sichere Hashfunktion benutzt werden.
- Legen Sie Zugriffsrechte auf die Verzeichnisse des Webserver fest. Des Weiteren statten Sie den Webserver mit eigenen Benutzerrechten aus und führen Sie bestimmte Server-Dienste nur in einer gekapselten Umgebung aus.
- Überwachen Sie den Netzwerkverkehr auf sicherheitsrelevante Aktivitäten, um ungewöhnliches Datenaufkommen zu erkennen. Protokollieren Sie beispielsweise die Anfragen an den Webserver und die Zugriffe auf das CMS.
- Prüfen Sie ggf., ob Ihre Webseite manipuliert wurde (z. B. durch die Beauftragung eines Dienstleisters, um mit Scans die Sicherheit zu erhöhen).

Weitere Informationen zum Vorbeugen von Angriffen finden Sie in den folgenden Veröffentlichungen des BSI:

- [„Absicherung von Telemediendiensten nach Stand der Technik“](#)
- [„Sicheres Bereitstellen von Web-Angeboten \(ISi-Web-Server\)“](#)

5 Beispielfälle

- Hackerangriffe auf mehrere ukrainische Regierungsw Webseiten (14.01.2022):
<https://www.bleepingcomputer.com/news/security/multiple-ukrainian-government-websites-hacked-and-defaced/>
- Iranischer Hackerangriff auf israelische Zeitung «Jerusalem Post» (03.01.2022):
<https://www.nzz.ch/technologie/israel-iranischer-hackerangriff-auf-jerusalem-post-ld.1662892>
- Defacement-Angriff auf die Spieleseite der Twitch-Webseite (Live-Streaming-Videoportal) (08.10.2021):
<https://www.bleepingcomputer.com/news/security/twitch-game-page-backgrounds-defaced-with-jeff-bezos-face/>
- Cyber-Angriff auf US-Regierungsseite (05.01.2020):
<https://www.bild.de/politik/ausland/politik-ausland/cyber-angriff-auf-us-regierungsseite-iranische-hacker-posten-blutenden-trump-67100284.bild.html>

6 Mustertext bei Kompromittierung der Webseite

Sehr geehrte/r Nutzer/in,

wir bedauern, Ihnen mitteilen zu müssen, dass unsere Webseite nach aktuellem Kenntnisstand vom ... bis zum ... kompromittiert war und schädliche Inhalte an Nutzer ausgeliefert hat.

Der Grund hierfür liegt in einem Angriff auf unsere Webseite, bei dem schädliche Inhalte unrechtmäßig integriert wurden. Sollten Sie unsere Webseite in diesem Zeitraum besucht haben, besteht die Möglichkeit, dass auch Ihr PC infiziert wurde.

Unsere Empfehlung lautet daher Ihr Gerät mit einer Antivirensoftware zu untersuchen und hierbei erkannte Schadprogramme umgehend zu entfernen.

Hilfe zu diesem Thema finden Sie unter anderem auf folgenden Webseiten:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Wegweiser_Checklisten_Flyer/Brosch_DINlang_Schadprogramme.pdf

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Virenschutz-Firewall/Virenschutzprogramme/virenschutzprogramme_node.html

Allgemeine Tipps zum sicheren Surfen im Internet finden Sie unter:

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/verbraucherinnen-und-verbraucher_node.html

Wir möchten uns auf diesem Wege vielmals für den Zwischenfall und die eventuell entstandenen Unannehmlichkeiten entschuldigen. Sollte Ihr PC befallen worden sein, lautet unsere Empfehlung Strafanzeige zu stellen.

Mit freundlichen Grüßen

...