Website-Kidnapping

Das können Sie tun, wenn ihre Website gehackt wurde

Wer als Unternehmer:in feststellt, dass die eigene Website gehackt wurde, steht oftmals unter Schock. Häufig kann man sich gar nicht erklären, wie es zu dem Angriff gekommen ist. Doch Hacker können Websites so manipulieren, dass eine unbemerkte Weiterleitung auf Fake-Shops oder andere illegale Inhalte stattfindet. Besonders betroffen sind kleine und mittlere Unternehmen (KMU), da sie oft nicht über ausreichende IT-Sicherheitsmaßnahmen verfügen.

Was versteht man unter Website-Kidnapping?

Immer mehr österreichische Unternehmen werden Opfer von Website-Kidnapping – einer Form der Website-Kompromittierung, bei der Kriminelle unbemerkt Kontrolle über eine Website übernehmen.

Diese Angriffe, auch als Cloaking (engl. Verhüllen) oder Website Defacement (engl. Verunstalten) bekannt, bleiben oft lange unentdeckt, da die Manipulation auf den ersten Blick nicht sichtbar ist.

Beispiel - Kims Online-Shop

Kim betreibt seit vielen Jahren einen Online-Shop für Gartenzubehör. Eines Tages erzählt ihr eine Kundin, dass beim Klick auf Kims Website plötzlich ein Shop für dubiose Medikamente erscheint. Der Grund: Hacker haben im Hintergrund von Kims seriösem Online-Shop Weiterleitungen auf Fake-Shops mit illegalen Produkten platziert.

Kims seriöses Unternehmen

Betrügerischer Fake-Shop

Website-Kidnapping

Holen Sie sich Ihre Website zurück!

Glücklicherweise gibt es gezielte Maßnahmen, mit denen sich betroffene Website-Betreiber:innen gegen solche Angriffe wehren und ihre Website wiederherstellen können. Ein strukturiertes Vorgehen hilft dabei, den Schaden zu begrenzen, Sicherheitslücken zu schließen und zukünftige Angriffe zu verhindern:

1 Website offline nehmen

Als ersten Schritt sollten Sie Ihre Website vorübergehend über Ihr Hosting-Panel (z.B. WordPress-Dashboard) deaktivieren.
Zusätzlich kann eine Wartungsseite eingerichtet werden, die Besucher:innen darüber informiert, dass die Website derzeit überarbeitet wird. So stellen Sie sicher, dass keine weiteren Weiterleitungen auf Fake-Shops oder illegale Inhalte über Ihre Website erfolgen.

2 Informieren Sie Ihren Webmaster

Falls Sie nicht selbst die technische Betreuung der Website übernehmen, informieren Sie umgehend den Webmaster oder IT-Support.

3 Zeitpunkt des Hackings ermitteln

Um den Angriff besser zu verstehen, sollten Sie den Zeitpunkt des Hackings herausfinden. Dies ist hilfreich, um gezielte Maßnahmen zur Schadensbegrenzung zu ergreifen. Um den Zeitpunkt des Hacking-Angriffs zu bestimmen, gibt es verschiedene Methoden:

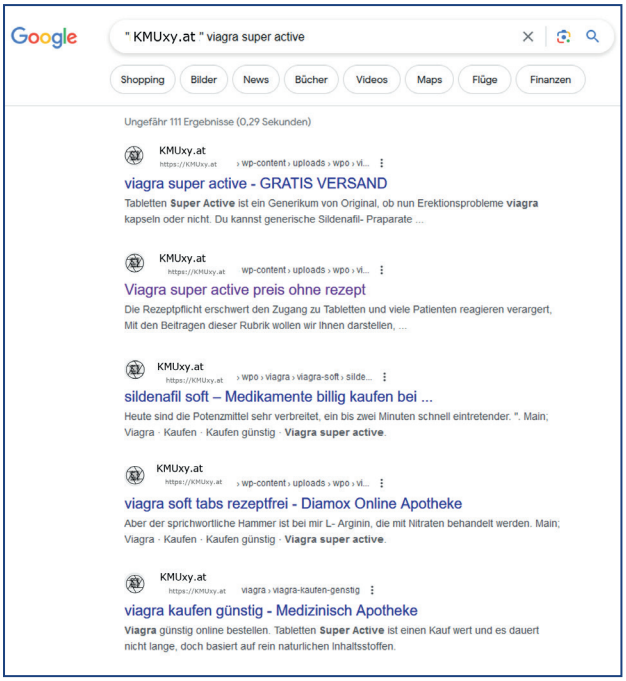
3.1 Suchmaschinen nutzen

Suchmaschinen wie Google können Hinweise auf den Zeitpunkt des Angriffs geben. Wenn eine Website gehackt wurde, kann sie mit einem neuen Datum in den Google-Suchergebnissen erscheinen. Dieses Datum zeigt, wann Google die veränderte Seite erkannt hat. So können Sie den Zeitraum des Angriffs eingrenzen.

Website-Kidnapping

➔ So geht's in Google:

- **Unterseiten anzeigen:** Geben Sie in Google „site:ihredomain.com" ein. So sehen Sie alle Unterseiten, die mit Ihrer Website verknüpft sind.
- **Datum prüfen:** In einigen Fällen zeigt Google das Datum an, an dem die Seite zum ersten Mal in der Suchmaschine gelistet wurde. Dies hilft, den Zeitraum einzugrenzen, in dem die betrügerische Website online ging.
- **Zeitraum filtern:** Nutzen Sie den „Suchfilter" rechts unter der Suchleiste. Wählen Sie anschließend unter „Beliebige Zeit" den gewünschten Zeitraum aus. So können Sie die Zeitspanne eingrenzen und sehen, welche Unterseiten in diesen Zeitraum erstellt wurden.



Unseriöse Suchmaschinenergebnisse weisen auf das Hacking hin.

3.2 Überprüfung des Modifikationsdatums

Eine weitere Methode, den Zeitpunkt eines Hacking-Angriffs zu bestimmen, ist die Überprüfung der Modifikationsdaten von Dateien auf dem Server. Das Modifikationsdatum zeigt an, wann eine Datei zuletzt verändert wurde.

➔ So geht's:

- **Prüfen Sie wichtige Dateien:** Sehen Sie sich die Dateien auf Ihrem Server an und prüfen Sie, wann sie zuletzt geändert wurden.
- **Achten Sie auf ungewöhnliche Änderungen:** Wenn das Datum der letzten Änderung anders ist, als erwartet oder Sie sich an keine Änderungen erinnern können, könnte dies ein Hinweis auf einen Hackerangriff sein.
- **Unbekannte Dateien identifizieren:** Achten Sie darauf, ob neue oder unbekannte Dateien hinzugefügt wurden. Dies könnte ein Hinweis auf einen Hackerangriff sein.

3.3 Logfiles überprüfen

Logfiles sind Dateien, die alle Aktivitäten auf Ihrem Server aufzeichnen. Sie zeigen, wer und wann auf Ihre Website zugegriffen hat. Diese Protokolle helfen dabei, herauszufinden, wie Besucher:innen mit Ihrer Seite interagieren und wann Fehler oder ungewöhnliche Aktivitäten auftreten.

Achten Sie beim Überprüfen der Logfiles auf verdächtige Aktivitäten, wie:

- **Ungewöhnliche Anmeldeversuche:** Viele fehlgeschlagene Login-Versuche können ein Zeichen für einen Hackerangriff sein.
- **Fremde IP-Adressen:** IP-Adressen, die nicht zu Ihren normalen Besuchern gehören, könnten von Kriminellen stammen.

Hilfreich könnte auch ein ZIP-File aller PHP-Dateien Ihrer Website sein. Diese enthalten den Code Ihrer Website und können für die Analyse und Wiederherstellung Ihrer Seite nützlich sein. Diese Dateien können Sie an Expert:innen übergeben, um den Vorfall verstehen und das nächste Mal verhindern zu können.

4 Backup erstellen

Erstellen Sie ein Backup Ihrer Website, bevor Sie mit der Bereinigung beginnen, damit Sie jederzeit auf die gesicherten Dateien zurückgreifen können, falls während der Bereinigung etwas schiefgeht.

Checkliste

- Backup erstellen
- Webmaster informieren
- Zeitpunkt des Hackings feststellen
- ZIP-Datei aller PHP-Dateien herunterladen

5 Sicherheitslücke schließen und Website bereinigen

Nachdem Sie den Zeitpunkt des Hacks ermittelt und ein Backup Ihrer Website erstellt haben, sollten Sie nun mit der Beseitigung des Schadens und der Absicherung Ihrer Website beginnen.
Eine Möglichkeit besteht darin, eine Version vor dem Hackerangriff einzuspielen und danach alle Sicherheitsupdates durchzuführen. Es besteht jedoch die Gefahr, dass zu diesem Zeitpunkt bereits eine Hintertür (geheimer Zugang für Hacker) auf Ihrem Server installiert wurde. Daher ist es in vielen Fällen sicherer, die Website komplett neu aufzusetzen.

Website-Kidnapping

5.1 CMS und Plugins aktualisieren

Installieren Sie alle verfügbaren Sicherheitsupdates und aktualisieren Sie Ihr Content Management System (CMS) sowie die verwendeten Plugins.
Bei WordPress können Sie beispielsweise das Plugin „Wordfence" einsetzen, um Manipulationen zu erkennen und Ihre Dateien regelmäßig auf Veränderungen zu überprüfen. Zusätzlich informiert Sie Wordfence per E-Mail, wenn ein Update erforderlich ist.

Die kostenlose Version sollte in den meisten Fällen ausreichend sein.

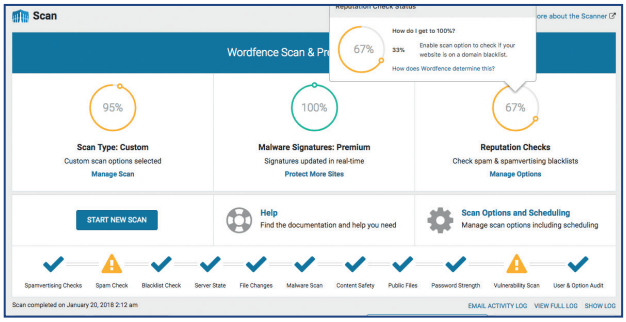
Zu viele Plugins können die Sicherheit Ihrer Website gefährden. Verwenden Sie nur die notwendigen Plugins und halten Sie diese auf dem neuesten Stand.

5.2 Schadsoftware bzw. Schadcode entfernen

Nach einem Hackerangriff sollten Sie alle Dateien Ihrer Website auf bösartigen oder unbekannten Code (einzelne Anweisungen, die in die Dateien Ihrer Website geschrieben werden) überprüfen.

Um den Schadcode zu identifizieren und zu entfernen, haben Sie verschiedene Möglichkeiten:

- **Automatische Entfernung mit einem Sicherheits-Plugin:** Ein zuverlässiges Plugin wie z.B. Wordfence kann Ihre Website automatisch auf Schadsoftware scannen. Nach Abschluss des Scans zeigt das Plugin die gefundenen Bedrohungen an und bietet Ihnen die Möglichkeit, den Schadcode automatisch zu entfernen.
- **Verwendung eines Online-Scanners:** Websites wie SiteCheck bieten kostenlose Online-Scanner an, die Ihre Seite auf Schadsoftware untersuchen. Diese eignen sich um schnell einen groben Überblick, über potenzielle Bedrohungen zu erhalten. Allerdings müssen diese im Anschluss manuell entfernt werden.
- **Manuelle Prüfung:** Wenn Sie sich mit den technischen Aspekten von Content-Management-Systemen wie z.B. WordPress gut auskennen, können Sie manuell nach schadhafter Software suchen. Diese Methode erfordert ein tiefgehendes Verständnis von PHP, HTML, JavaScript und Datenbanken, da Sie den Code und die Struktur Ihrer Website selbst durchsuchen und potenziell schadhafte Elemente erkennen müssen.



Beispiel Wordfence Scan Resultat

Website-Kidnapping

6 Passwörter ändern:

Nach einem Hacking-Angriff ist es unbedingt erforderlich, alle Passwörter zu ändern, die mit der Verwaltung Ihrer Website verbunden sind. Dies betrifft insbesondere die Passwörter für das Hosting, die Datenbank und das Content Management System (CMS). Aktivieren Sie zusätzlich die Zwei-Faktor-Authentifizierung (2FA), um eine zusätzliche Sicherheitsebene hinzuzufügen. Damit wird beim Log-in neben dem Passwort ein weiterer Code benötigt, der in der Regel auf einem anderen Gerät (z. B. Ihrem Smartphone) generiert wird.

Checkliste

- CMS und Plugins
- Schwachstellen überprüfen
- Schadsoftware entfernen
- Passwort ändern
- Zwei-Faktor-Authentifizierung einrichten

7 Betrügerische Inhalte aus Suchmaschinen entfernen

Nach der Wiederherstellung Ihrer Website ist es entscheidend, sicherzustellen, dass schadhafte Inhalte, die mit Ihrer Website in Verbindung stehen, nicht weiterhin in den Suchergebnissen erscheinen. Einerseits ist dies wichtig, damit Nutzer:innen nicht Ihre Website mit Fake-Shops und illegalen Inhalte in Verbindung bringen. Andererseits besteht die Gefahr, dass Suchmaschinen sonst Ihre Website aus ihrer Indexierung entfernen.

➔ So geht's:

- **Google Search Console nutzen:** Melden Sie sich in der Google Search Console an – ein kostenloses Tool von Google, das Ihnen hilft, Ihre Website zu verwalten. Hier können Sie URLs, die schadhafte oder manipulierte Inhalte enthalten, aus dem Google-Index entfernen. Diese Funktion hilft also, die ungewünschten Seite schnell aus den Suchergebnissen zu löschen.
- **Erneute Überprüfung beantragen:** Falls Google Ihre Website als unsicher markiert hat, können Sie nach der Bereinigung eine erneute manuelle Überprüfung anfordern, um die Warnung zu entfernen.

Website-Kidnapping

8 Meldung an die zuständigen Behörden

Ein weiterer wichtiger Schritt ist, die zuständigen Sicherheitsbehörden zu informieren, insbesondere wenn personenbezogene Daten von dem Angriff betroffen sind. In der EU sind Sie gemäß der Datenschutz-Grundverordnung (DSGVO) verpflichtet, Datenpannen innerhalb von 72 Stunden der zuständigen Aufsichtsbehörde zu melden. Dies ist ein wichtiger Schritt, um den Schaden zu begrenzen und rechtliche Konsequenzen zu vermeiden. Weiters sollten Sie auch die Strafverfolgungsbehörden informieren, wenn Ihre Website für betrügerische Zwecke genutzt wurde.

Checkliste auf einen Blick

- [ ] Website offline nehmen
- [ ] Webmaster informieren
- [ ] Zeitpunkt des Hackings feststellen
- [ ] ZIP-Datei aller PHP-Dateien erstellen
- [ ] CMS und Plugins aktualisieren
- [ ] Schwachstellen überprüfen
- [ ] Schadsoftware entfernen
- [ ] Passwort ändern
- [ ] Zwei-Faktor-Authentifizierung einrichten
- [ ] Inhalte aus Suchmaschinen entfernen
- [ ] Meldung an zuständige Behörden