ARBEITSBLATT ZUM BEITRAG

Erste Hilfe bei gehackter Website

Warnzeichen und Checkliste

Woran Sie einen Hack ohne Technikwissen erkennen und was Sie in den ersten 30 Minuten, am selben Tag und in den nächsten Tagen tun. Zum Ausdrucken, Abhaken und Weitergeben an Hoster oder Webentwickler.

KURZ GESAGT

Eine gehackte Website fällt nicht immer auf. Prüfen Sie den **Sicherheitsbericht der Search Console**, Ihre Seite in den Suchergebnissen und die **Benutzerliste im Backend**. Bei einem Verdacht: nichts löschen, Beweise sichern, Zugänge schließen, Hoster informieren und kein Backup blind einspielen.

WARNZEICHEN

Kreuzen Sie an, was Sie bemerkt haben. Ein Kreuz bei „Sofort“ heißt: gleich mit Seite 3 weitermachen.

- ☐ **Google oder der Browser warnen vor Ihrer Seite** — ● SOFORT
  Schadsoftware oder eingeschleuste Inhalte, die Google erkannt hat. Besucher sind gefährdet.
- ☐ **Besucher landen auf fremden Seiten oder sehen Pop-ups** — ● SOFORT
  Eingeschleuster Code leitet um oder blendet Werbung ein. Zeigt sich oft nur mobil oder nur für Besucher aus der Suche.
- ☐ **Unbekannte Administratoren oder Beiträge im Backend** — ● SOFORT
  Ein Angreifer hat Zugang erlangt. Zugänge und Passwörter gelten als kompromittiert.
- ☐ **Fremdsprachige oder unpassende Titel in der Google-Suche zu Ihrer Domain** — ◐ ZEITNAH
  Spam-Seiten, die jemand auf Ihrem Server abgelegt hat. Meist unbemerkt, schadet aber Ruf und Sichtbarkeit.
- ☐ **Ihr Hoster meldet Auffälligkeiten oder sperrt den Mailversand** — ◐ ZEITNAH
  Ihr Server verschickt Spam oder wird für Angriffe genutzt. Beim Hoster nachfragen, welche Dateien betroffen sind.
- ☐ **Die Seite wird spürbar langsamer oder fällt aus** — ○ PRÜFEN
  Kann Schadcode sein, ist aber oft eine andere Ursache. Erst prüfen, nicht gleich vom Hack ausgehen.

SEITE 2

Die Zehn-Minuten-Prüfung

Fünf Blicke ohne Technikkenntnisse. Am besten von einem Rechner aus, der selbst nicht verdächtig ist.

1 **Search Console öffnen.** Unter „Sicherheit und manuelle Maßnahmen“ steht der Bericht zu Sicherheitsproblemen. Google nennt ihn die maßgebliche Quelle.

☐ unauffällig ☐ auffällig

2 **Die eigene Domain suchen.** Bei Google *site:ihre-domain.de* eingeben und die Titel lesen. Fremdsprachige, medizinische oder Glücksspiel-Titel gehören nicht dazu.

☐ unauffällig ☐ auffällig

3 **Die Seite mobil aus der Suche aufrufen.** Auf dem Smartphone auf das Suchergebnis tippen, statt die Adresse einzutippen. Manche Umleitungen zeigen sich nur so.

☐ unauffällig ☐ auffällig

4 **Benutzerliste prüfen.** Im WordPress-Backend unter „Benutzer“ stehen alle Administratoren. Jeder, den Sie nicht kennen, ist ein Warnzeichen.

☐ unauffällig ☐ auffällig

5 **Beim Hoster nachfragen.** Gab es auffällige Dateien, Spam-Versand oder Zugriffe? Welche PHP-Version läuft?

☐ unauffällig ☐ auffällig

WAS SIE DABEI NICHT TUN

Löschen Sie nichts, was Ihnen verdächtig vorkommt. Manche Dateien sehen wie Schadcode aus und gehören zum System. Außerdem brauchen Sie den Zustand später als Spur, um zu verstehen, wie der Angreifer hineingekommen ist.

BEOBACHTUNGS-PROTOKOLL

Für Hoster, Webentwickler und eine spätere Ursachensuche. Dazu Screenshots sichern.

DATUM UND UHRZEIT DER ENTDECKUNG

ENTDECKT DURCH (SIE, KUNDE, HOSTER, GOOGLE)

WAS GENAU HABE ICH GESEHEN? SEITE, MELDUNG, GERÄT, BROWSER

SCREENSHOTS GESPEICHERT UNTER (ORDNER, DATEINAME)

SEITE 3

Die Checkliste

Von oben nach unten abarbeiten. Die Reihenfolge ist wichtig, weil der Angreifer sonst nach der Bereinigung wieder hereinkommt. Sie müssen nicht alles selbst können: Bei vielen Punkten reicht es, die richtigen Leute zu informieren.

1

DIE ERSTEN 30 MINUTEN

Ruhe bewahren, Spuren sichern

- [ ] **Ruhe bewahren und nichts löschen.** Auch verdächtige Dateien bleiben, wo sie sind. Sie sind später Spuren.
- [ ] **Beweise sichern.** Screenshots von der Seite, von Fehlermeldungen und auffälligen Google-Ergebnissen. Datum und Uhrzeit notieren.
- [ ] **Besucher schützen.** Warnt Google oder der Browser schon: Wartungsmodus oder Seite vorübergehend vom Netz nehmen. Der Hoster kann das auch für Sie tun.
- [ ] **Hoster und Webentwickler informieren.** Kurz schildern, was Sie gesehen haben, und die Screenshots mitschicken.

2

NOCH HEUTE

Zugänge schließen und aufräumen lassen

- [ ] **Alle Passwörter ändern.** Von einem sauberen Gerät aus, lang, neu und jedes nur einmal (Tabelle auf Seite 4).
- [ ] **Benutzer prüfen.** Unbekannte Administratoren notieren und vom Fachmann entfernen lassen.
- [ ] **Ein sauberes Backup einspielen lassen.** Das Datum muss vor dem Vorfall liegen. Ein Backup allein genügt nicht, solange das Einfallstor offen ist.
- [ ] **Updates durchführen lassen.** WordPress, Theme und Plugins aktualisieren, nicht mehr genutzte Plugins entfernen.

3

NÄCHSTE TAGE

Google, Kunden und Pflichten

- [ ] **Search Console prüfen.** Zeigt der Bericht noch ein Problem? Nach der Bereinigung lässt sich dort eine erneute Überprüfung anstoßen.
- [ ] **Kunden und Partner informieren, falls betroffen.** Etwa wenn Spam von Ihrer Seite kam oder Formulardaten betroffen sein könnten. Ehrlich sagen, was passiert ist und was Sie getan haben.
- [ ] **Meldepflicht klären lassen.** Waren möglicherweise personenbezogene Daten betroffen, kann eine Meldung an die Datenschutzaufsicht nötig sein, und die Fristen sind kurz. Mit Datenschutzbeauftragtem oder Rechtsbeistand sprechen.

4

DANACH

Damit es nicht wieder passiert

- [ ] **Ursache benennen lassen.** Wie ist der Angreifer hineingekommen? Das Einfallstor schließen lassen.
- [ ] **Absicherung festlegen.** Backups an einem getrennten Ort, feste Update-Termine, Zwei-Faktor-Anmeldung und eine klare Zuständigkeit für die Website.

SEITE 4

Zum Eintragen

PASSWÖRTER ERNEUERN

ZUGANG	GEÄNDERT AM	OK
WordPress (Backend)		☐
Hoster (Kundenmenü)		☐
FTP / SFTP		☐
Datenbank		☐
E-Mail-Konto für Passwort-Rücksetzung		☐

WER HILFT?

ROLLE	NAME	TELEFON
Hoster		
Webentwickler		
Datenschutzbeauftragter		
Rechtsbeistand		

WANN FACHLEUTE DAZUKOMMEN

Sobald Kundendaten betroffen sein könnten oder der Schadcode nach einer Bereinigung zurückkehrt. Der Hoster allein reicht nur, wenn ausschließlich sein Server betroffen ist.

NOTIZEN UND NÄCHSTE SCHRITTE

UND JETZT?

Unsicher, ob Ihre Seite sauber ist?

Vereinbaren Sie ein Gespräch zu Ihrer Website. Wir gehen Ihre Antworten mit Ihnen durch und klären, was die Warnzeichen bedeuten und wer handeln sollte. Das Strategiegespräch ist kostenlos und unverbindlich, auch per Videocall.

KONTAKT

All In Mediadesign
Münchener Str. 79
84453 Mühldorf am Inn

08631 18 32 000
Mo bis Fr, 8 bis 17 Uhr
info@all-in-mediadesign.com
all-in-mediadesign.com/kontakt/

Das Arbeitsblatt gehört zum Beitrag „Ist Ihre Website gehackt? Das erkennen Sie auch ohne Technikwissen“ auf all-in-mediadesign.com/marketing-know-how/. Hilfe bei gehackter Website: all-in-mediadesign.com/website-gehackt-hilfe/. Es ist eine Orientierungshilfe und ersetzt keine Rechts- oder IT-Forensik-Beratung.