**Looks Einkaufs & Verwaltungs GmbH**
looksgoods.de · Wangen im Allgäu

# Website-Sicherheit für Allgäuer Betriebe

Leitfaden mit Checkliste · Alexandra Looks · Stand November 2026

Ein Leitfaden für Handwerksbetriebe, Gastronomie, Hofläden und Händler im Allgäu, die eine eigene Website haben, aber keine eigene IT-Abteilung. Er beruht auf einem echten Angriff auf unsere eigenen Websites im Juli 2026 und auf dem, was wir danach umgebaut haben.

> **Die Kurzfassung in fünf Sätzen**
>
> - Die meisten Website-Hacks bei kleinen Betrieben kommen über Erweiterungen und Vorlagen, nicht über „Hacker, die es auf Sie abgesehen haben".
> - Website, E-Mail und Buchhaltung gehören auf getrennte Systeme.
> - Eine Sicherung zählt nur, wenn die Website sie nicht erreichen kann.
> - Sicherheits-Plugins ersetzen keine Kontrolle, ob sich Dateien verändert haben.
> - Im Ernstfall gilt: zuerst abschotten, dann untersuchen, dann neu aufbauen.

## Warum das Thema gerade kleine Betriebe trifft

Angreifer suchen nicht gezielt nach der Zimmerei in Isny oder dem Café in Wangen. Sie lassen Programme laufen, die Millionen Websites nach bekannten Lücken absuchen, und nehmen, was offen ist. Ein kleiner Betrieb ist dabei nicht uninteressant, sondern bequem: Die Website läuft oft jahrelang ohne Pflege, der Webdesigner von damals ist nicht mehr greifbar, und niemand schaut regelmäßig hinein.

Bei uns war es genauso unspektakulär. Eine Hintertür kam im April 2026 über Erweiterungen aus einer inoffiziellen Quelle auf unsere WordPress-Seiten und wurde beim Umzug auf den eigenen Server mitgenommen. Im Juli wurde sie aktiv: Besucher sahen die normale Seite, Google bekam Spam-Seiten in fremder Sprache. Die Zugriffe des Google-Crawlers stiegen innerhalb einer Woche von 44 auf über 15.000 am Tag. Die ganze Geschichte steht im Beitrag Website gehackt – was tun?.

## Teil 1: Zehn Punkte, die Sie heute prüfen können

1. **Wer hat Zugang?** Liste aller Konten mit Administratorrechten auf der Website, beim Hosting-Anbieter und bei der Domain. Ehemalige Mitarbeiter, Praktikanten und frühere Agenturen raus. Bei uns tauchten nach dem Angriff vier gefälschte Administrator-Konten auf.
2. **Woher kommen Erweiterungen und Vorlagen?** Nur aus dem offiziellen Verzeichnis oder direkt vom Hersteller. Eine „kostenlose Premium-Version" von einer Download-Seite ist der häufigste Weg für Schadcode.

3. **Wie viele Erweiterungen laufen?** Jede ist eine mögliche Tür. Auf unserer Marktseite sind nach dem Aufräumen von 20 Erweiterungen zwei übrig geblieben. Die Seite kann trotzdem alles, was sie können muss.
4. **Werden Updates eingespielt?** Website-System, Erweiterungen und die Server-Software (meist PHP) brauchen zeitnahe Updates. Fragen Sie Ihren Dienstleister schriftlich, wer das macht und wie oft.
5. **Liegen E-Mail und Website auf demselben System?** Wenn ja: trennen. Bei uns lagen die Postfächer bei einem eigenen Anbieter. Der Angreifer kam deshalb weder an Mails noch an Rechnungen oder Passwörter.
6. **Wo liegen die Sicherungen?** Eine Sicherung auf demselben Server oder im selben Hosting-Paket kann ein Angreifer löschen oder verseuchen. Mindestens eine Kopie muss außer Reichweite liegen. Unsere alten Sicherungen lagen in Reichweite. Dass der Angreifer sie nicht gelöscht hat, war Glück.
7. **Ist der zweite Faktor eingeschaltet?** Für Website-Login, Hosting, Domain-Verwaltung, E-Mail und Google-Konto. Ein Passwort-Tresor macht es leicht, für jedes Konto ein eigenes, langes Passwort zu haben.
8. **Sieht Google dasselbe wie Ihre Kunden?** In der Google Search Console unter „Seiten" und „Sicherheitsprobleme" nachsehen. Plötzlich viele neue Seiten in fremder Sprache sind ein Alarmsignal. Ohne Search-Console-Zugang sehen Sie diesen Angriff nicht, denn im Browser sieht die Seite normal aus.
9. **Ist Ihre Mail-Domain gegen Fälschung geschützt?** Die Einträge SPF, DKIM und DMARC sorgen dafür, dass niemand Mails in Ihrem Namen verschicken kann, die beim Empfänger als echt durchgehen. Fragen Sie Ihren Mail-Anbieter, ob alle drei gesetzt sind.
10. **Tauchen Ihre Adressen in Datenlecks auf?** Kostenlos prüfen beim Identity Leak Checker des Hasso-Plattner-Instituts (sec.hpi.de/ilc), beim Leak Checker der Universität Bonn (leakchecker.uni-bonn.de) oder bei Have I Been Pwned (haveibeenpwned.com).

## Teil 2: Wenn es passiert ist – die ersten 24 Stunden

1. **Abschotten.** Website offline nehmen oder den Hosting-Anbieter bitten, sie zu sperren. Nicht zuerst „aufräumen". Bei uns war die Website noch am Abend des ersten Verdachts gestoppt.
2. **Sichern, aber nicht wiederherstellen.** Eine Kopie des befallenen Stands für die Spurensuche anlegen und deutlich beschriften: „niemals wiederherstellen".
3. **Prüfen, was noch betroffen ist.** Andere Websites im selben Hosting-Paket, E-Mail-Konten, Google-Konto, Zahlungsdienste.
4. **Den letzten sauberen Stand finden.** Nicht die letzte Sicherung, sondern die letzte nachweislich saubere. Bei uns lag die Hintertür schon Monate vor dem Ausbruch im System.
5. **Neu aufbauen statt flicken.** System frisch aus der offiziellen Quelle, nur die nötigsten Erweiterungen, Inhalte aus dem sauberen Stand übernehmen.
6. **Alle Zugänge tauschen.** Passwörter, Benutzernamen, Schlüssel für angebundene Dienste, aktive Sitzungen beenden. Fremde Einträge in der Google Search Console entfernen.

7. **Melden, wo nötig.** Wurden personenbezogene Daten abgegriffen (zum Beispiel aus Kontaktformularen oder einem Shop), ist die Meldung an die Datenschutzaufsicht innerhalb von 72 Stunden Pflicht (Art. 33 DSGVO): in Baden-Württemberg beim Landesbeauftragten für den Datenschutz, in Bayern beim Landesamt für Datenschutzaufsicht. Strafanzeige nimmt die Zentrale Ansprechstelle Cybercrime (ZAC) des jeweiligen Landeskriminalamts entgegen.

## Teil 3: Wie man sich dauerhaft aufstellt

Wir haben unsere Websites nach dem Angriff grundsätzlich anders gebaut. Nicht jeder Betrieb muss das genauso machen, aber die Prinzipien passen auf fast jede Website:

- **Öffentlich nur fertiges HTML.** Unsere Seiten werden intern erstellt und als fertige Dateien ausgeliefert, ohne Datenbank und ohne Programmcode im Netz. Wo kein Programm läuft, kann keins angegriffen werden. Für eine Visitenkarten-Website mit Öffnungszeiten, Leistungen und Kontakt reicht das fast immer.
- **Jede Nacht eine Kontrolle.** Ein Prüfprogramm vergleicht die Dateien mit dem bekannten Stand und meldet jede Abweichung per Mail.
- **Verwaltung nicht offen im Internet.** Anmeldeseiten und Verwaltungsoberflächen nur über VPN oder mit zweitem Faktor.
- **Getrennte Häuser.** Website, E-Mail, Cloud-Ablage, Passwort-Tresor und Buchhaltung je für sich. Wer in eines einbricht, steht nicht in den anderen.

## Fragen für das nächste Gespräch mit Ihrem Webdesigner

- Wer spielt Updates ein, wie oft, und wo kann ich das nachlesen?
- Wo liegen die Sicherungen, und wie schnell ist die Seite im Notfall wieder online?
- Welche Erweiterungen laufen, und welche davon brauchen wir wirklich?
- Wer bekommt eine Nachricht, wenn sich Dateien verändern?
- Habe ich selbst Zugang zu Hosting, Domain und Google Search Console, auch wenn wir nicht mehr zusammenarbeiten?

Diesen Leitfaden gibt es auch als PDF zum Ausdrucken. Wenn Sie Fragen zu Ihrer Website haben oder die Punkte gemeinsam durchgehen wollen: looks@looksgoods.de.

---

Looks Einkaufs & Verwaltungs GmbH · Kellerbühlstraße 15 · 88239 Wangen im Allgäu · looks@looksgoods.de · https://looksgoods.de/
Amtsgericht Ulm HRB 747569 · Geschäftsführerin Alexandra Looks · Online-Fassung: https://looksgoods.de/website-sicherheit-leitfaden/