Notfall-Leitfaden: JTL-Shop Kompromittierung

Klassifizierung: Kundeninformation | **Version:** 1.0 | **Stand:** Juli 2026 **Zielgruppe:** Shop-Betreiber, E-Commerce-Manager, Datenschutzbeauftragte **Framework:** Basierend auf SANS PICERL Incident Response Methodik [1]

> **Im Notfall sofort kontaktieren: EcomSec Notfall-Support:** support@ecomsec.de | +49 (0) XX XXX XXXX Reaktionszeit: innerhalb von 2 Stunden (Werktage), 4 Stunden (Wochenende/Feiertage) Bitte bereithalten: Hosting-Provider, Shop-URL, ungefährer Zeitpunkt der Entdeckung.

Sofort-Checkliste (erste 60 Minuten)

Wenn Sie einen Verdacht auf Kompromittierung haben, führen Sie diese fünf Schritte in genau dieser Reihenfolge aus, bevor Sie irgendetwas anderes tun:

① **Shop auf Serverebene sperren** — Bitten Sie Ihren Hosting-Provider, den Shop sofort zu sperren, oder setzen Sie eine `.htaccess`-Sperre. Der JTL-Wartungsmodus allein reicht nicht aus.

② **Nichts löschen** — Löschen Sie keine Dateien, auch wenn diese verdächtig aussehen. Jede gelöschte Datei vernichtet Beweise, die für die Analyse und für rechtliche Schritte benötigt werden.

③ **Passwörter noch nicht ändern** — Ändern Sie Passwörter erst nach Rücksprache mit uns. Die Reihenfolge ist entscheidend: Erst forensisches Backup, dann Passwort-Rotation.

④ **EcomSec kontaktieren** — Rufen Sie uns an oder schreiben Sie eine E-Mail mit dem Betreff „NOTFALL: Shop-Kompromittierung”. Wir koordinieren alle weiteren Schritte.

⑤ **Hosting-Provider informieren** — Informieren Sie Ihren Hosting-Provider über den Verdacht, damit dieser auf seiner Seite die Logs sichert und ggf. weitere Maßnahmen einleiten kann.

Die sechs Phasen der Incident Response

Ein Sicherheitsvorfall in Ihrem JTL-Shop erfordert schnelles und strukturiertes Handeln. Der folgende Leitfaden erklärt, was in jeder Phase passiert, was wir tun und was Sie als Betreiber beitragen müssen.

---

1. Vorbereitung (Preparation)

Ein erfolgreiches Krisenmanagement beginnt vor dem eigentlichen Vorfall. Als Shop-Betreiber sollten Sie sicherstellen, dass Sie im Ernstfall wissen, wen Sie kontaktieren müssen. Legen Sie eine interne Notfall-Kontaktliste an, die Ihre technischen Dienstleister, Ihren Hosting-Provider und Ihren Datenschutzbeauftragten umfasst. Prüfen Sie zudem regelmäßig, ob Sie funktionierende und getrennte Backups Ihres Shops und Ihrer Datenbank besitzen. Wir empfehlen den Einsatz des EcomSec Backup Professional Plugins, um im Ernstfall auf nachweislich saubere Datenstände zurückgreifen zu können.

---

2. Identifikation (Identification)

In dieser Phase stellen wir fest, ob ein tatsächlicher Angriff stattgefunden hat und welche Daten betroffen sein könnten. Ein Vorfall wird meist durch Auffälligkeiten im Shop, Warnungen Ihres Hosting-Providers oder durch automatisierte Scans des EcomSec Security Scanners entdeckt. Unsere Experten analysieren die Server-Logs und Scanner-Ergebnisse, um den Angriffsweg nachzuvollziehen. Für Sie als Betreiber ist es wichtig zu wissen, dass bei einer Kompromittierung potenziell folgende Daten ausgelesen worden sein können: Datenbank-Zugangsdaten, FTP-Passwörter, API-Keys von Zahlungsdienstleistern sowie unter Umständen Kundendaten aus der Datenbank [3].

---

3. Eindämmung (Containment)

Um zu verhindern, dass der Angreifer weiteren Schaden anrichtet oder zusätzliche Daten abfließen, muss der Shop sofort isoliert werden. Das Mittel der Wahl ist die **Sperrung auf Serverebene** — nicht der JTL-Wartungsmodus. Der Wartungsmodus verhindert zwar den Kundenzugang, führt jedoch weiterhin PHP aus, sodass eine platzierte Webshell für den Angreifer weiterhin erreichbar bleibt. Wir koordinieren die Serversperre mit Ihrem Hosting-Provider und blockieren alle verdächtigen Zugriffe. Bevor Bereinigungsmaßnahmen starten, erstellen wir ein forensisches Backup des kompromittierten Zustands. Diese Beweissicherung ist entscheidend, falls rechtliche Schritte eingeleitet werden sollen oder eine detaillierte Analyse für Ihren Datenschutzbeauftragten notwendig wird.

---

4. Beseitigung (Eradication)

Der Angreifer und alle von ihm platzierten Hintertüren müssen restlos aus dem System entfernt werden. Ein einfaches Löschen gefundener Schaddateien reicht hierfür nicht aus [3]. Als Betreiber müssen Sie nach unserer Anweisung alle Passwörter und API-Keys vollständig rotieren. Dies betrifft nicht nur die offensichtlichen Zugänge wie Shop-Admin und FTP, sondern auch die API-Keys Ihrer Zahlungsdienstleister (PayPal, Mollie, Klarna etc.), da ein Angreifer mit diesen Zugängen Zahlungen umleiten kann. Parallel übernehmen wir die technische

Bereinigung: Der Shop wird aus einer sauberen, vertrauenswürdigen Quelle komplett neu aufgebaut. Eigene Dateien wie Produktbilder werden vor der Wiederherstellung auf versteckten Schadcode geprüft. Abschließend wird die ursprüngliche Sicherheitslücke durch das Einspielen des aktuellen JTL-Sicherheitspatches geschlossen [2].

---

5. Wiederherstellung (Recovery)

Nach der erfolgreichen Bereinigung wird Ihr Shop sicher wieder in den produktiven Betrieb überführt. Wir führen einen vollständigen Abgleich mit Ihrer JTL-Wawi durch, um sicherzustellen, dass keine manipulierten Daten — wie veränderte Preise oder falsche Lieferadressen — im Shop verbleiben. Bevor wir den Shop für Ihre Kunden freigeben, erfolgt ein finaler Security-Check mit dem EcomSec Security Scanner. Nach der Freischaltung überwachen wir die Server-Zugriffe für mindestens 48 Stunden engmaschig, um sofort reagieren zu können, falls der Angreifer über andere Wege zurückkehren sollte.

---

6. Nachbereitung (Lessons Learned)

Nachdem der Shop wieder sicher läuft, analysieren wir den Vorfall gemeinsam und erstellen einen detaillierten Bericht. Eine wichtige Aufgabe für Sie als Betreiber ist die datenschutzrechtliche Bewertung. Sie müssen gemeinsam mit Ihrem Datenschutzbeauftragten prüfen, ob eine Meldepflicht an die zuständige Aufsichtsbehörde nach **Art. 33 DSGVO** besteht. Diese Meldung muss **innerhalb von 72 Stunden** nach Bekanntwerden des Vorfalls erfolgen. Zusätzlich ist zu prüfen, ob eine Informationspflicht gegenüber Ihren Kunden nach Art. 34 DSGVO besteht [4]. Abschließend beraten wir Sie gerne zu präventiven Maßnahmen, wie dem EcomSec Monitoring-Cluster für automatisiertes Patch-Management und kontinuierliche Schwachstellen-Überwachung, um das Risiko zukünftiger Vorfälle dauerhaft zu minimieren.

Referenzen

[1] SANS Institute — Incident Handler’s Handbook [2] JTL-Software — Offizielles Security Advisory CVE-2026-54390 (JTL Partner-Newsletter, 17.06.2026) [3] BSI — IT-Grundschutz: Behandlung von Sicherheitsvorfällen (ORP.5) [4] Bundesbeauftragter für den Datenschutz — Art. 33 DSGVO: Meldung von Datenschutzverletzungen

---