webdev.trust

Quartalsbericht 10.02.2026 – 10.05.2026

Düsseldorf, den 11.05.2026

Erstellt von: webdevtrust GmbH · info@webdevtrust.com

Zusammenfassung

Im Berichtszeitraum vom 10. Februar bis 10. Mai 2026 war die Website stabil erreichbar und wurde aktiv durch Sicherheitsmonitoring geschützt. Die organische Sichtbarkeit in der Google Search Console zeigt eine gleichmäßige Entwicklung bei moderatem Klickvolumen. Der Sicherheits-Firewall hat im Quartal über 3.500 Angriffe abgewehrt.

1. Verfügbarkeit (Uptime-Monitoring)

Die Website wurde im gesamten Berichtszeitraum kontinuierlich überwacht. Die Gesamtverfügbarkeit über 90 Tage lag bei **98,11 %** bei einer Gesamtausfallzeit von **1 Std. 57 Min. 34 Sek.**

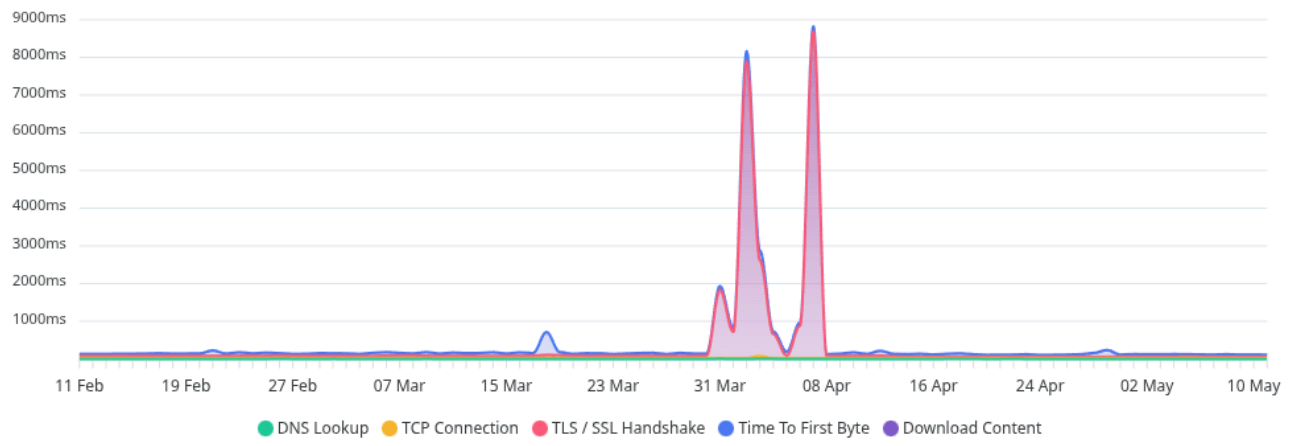
Monat	Verfügbarkeit	Ausfallzeit
März 2026	**99,98 %**	3 Min. 30 Sek.
April 2026	**97,25 %**	1 Std. 52 Min. 48 Sek.
Mai 2026	**99,97 %**	1 Min. 16 Sek.

Ausfälle im Detail

Beginn (UTC)	Ende (UTC)	Dauer	Bewertung
07.04.2026 06:48	07.04.2026 08:41	1 Std. 52 Min. 48 Sek.	Kritisch
06.05.2026 23:15	06.05.2026 23:18	3 Min.	Gering
11.05.2026 00:50	11.05.2026 00:51	1 Min.	Gering
11.05.2026 12:08	–	–	In Prüfung

Der Ausfall am **07. April 2026** mit knapp 2 Stunden Dauer ist der einzige nennenswerte Vorfall im Quartal. Ursache und Behebung sind zu dokumentieren.

2. Performance (Scanfully)



Scanfully misst kontinuierlich die Ladezeiten der Website und schlüsselt sie in einzelne Phasen auf: DNS-Lookup, TCP-Verbindung, TLS/SSL-Handshake, Time to First Byte (TTFB) und Download.

Bewertung

Im Großteil des Berichtszeitraums waren alle Metriken unauffällig und lagen im niedrigen dreistelligen Millisekunden-Bereich. Zwei Ausreißer stechen hervor:

Zeitraum	Spitzenwert	Hauptursache
ca. 15.–16. März 2026	~800 ms	TLS/SSL-Handshake-Verzögerung
ca. 31. März – 08. April 2026	~8.000–9.000 ms	Time to First Byte (TTFB) + TLS/SSL

Der zweite, deutlich ausgeprägtere Einbruch korreliert direkt mit dem **Serverausfall vom 07. April 2026** (vgl. Abschnitt 1). Der stark erhöhte TTFB deutet auf eine serverseitige Überlastung oder einen nicht reagierenden PHP/Datenbankprozess als Ursache hin – nicht auf ein Netzwerk- oder CDN-Problem.

Abseits dieser Ereignisse zeigt die Website eine **stabile Baseline-Performance** ohne nennenswerte Degradation über den Quartalsverlauf.

---

3. Entwicklung Google Search Console

Im Berichtszeitraum wurden folgende Werte in der Google Search Console erfasst:

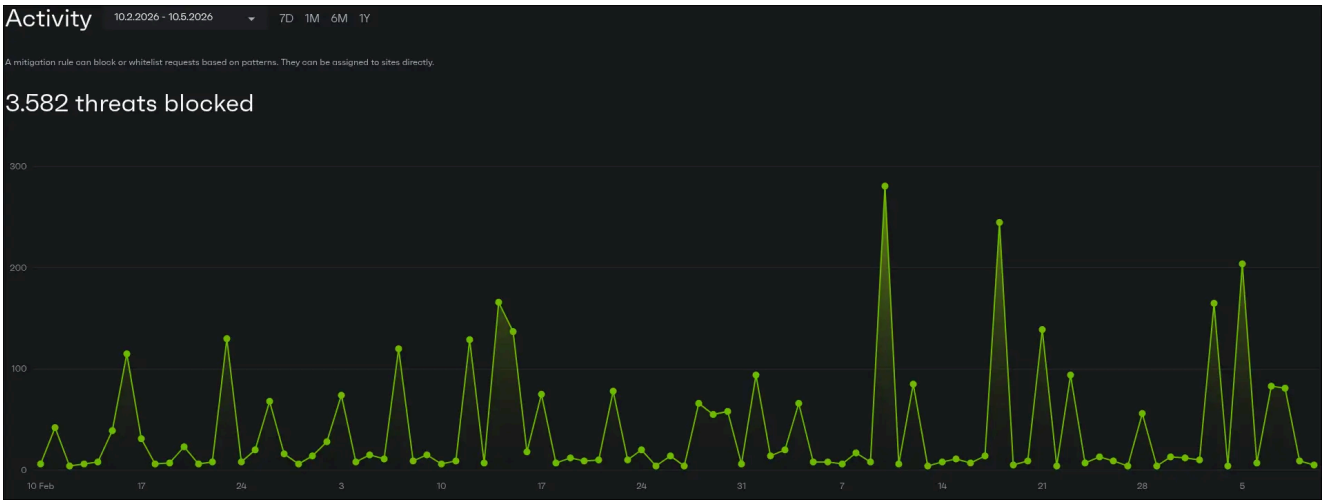
Kennzahl	Wert
Klicks insgesamt	**504**
Impressionen insgesamt	**9.580**
Durchschnittliche CTR	**5,3 %**
Durchschnittliche Position	**7**

Interpretation

Die Klickrate (CTR) von 5,3 % bei einer durchschnittlichen Position 7 ist ein solider Ausgangswert. Der Verlauf zeigt ein gleichmäßiges Klick- und Impressionsvolumen ohne größere Einbrüche. Ein lokaler Peak in der dritten Märzwoche ist erkennbar und könnte auf eine temporäre Verbesserung der Rankings oder eine saisonale Nachfrage zurückzuführen sein.

---

4. Sicherheit (Patchstack Firewall)



Die Patchstack Web Application Firewall hat im Berichtszeitraum aktiv Angriffe abgewehrt:

- **3.582 abgewehrte Bedrohungen** im Gesamtzeitraum
- Deutlicher Anstieg der Angriffsversuche ab Anfang April 2026
- Spitzenwerte: ca. 280 Blockierungen an einzelnen Tagen (07.–08. April, 14.–15. April)
- Die Firewall hat durchgehend zuverlässig reagiert

Gemeldete und behobene Schwachstellen im Quartal

Im Berichtszeitraum wurden durch Patchstack drei Schwachstellen in installierten Plugins erkannt. Alle drei wurden im Rahmen des laufenden Wartungsvertrags **umgehend geschlossen**.

Plugin	Schwachstelle	Gemeldet	Status
Meta Box ≤ 5.11.11	Arbitrary File Deletion (Contributor+)	09.03.2026	Behoben ✓
Elementor ≤ 3.35.7	Sensitive Information Exposure via Template (Contributor+)	30.03.2026	Behoben ✓
Elementor ≤ 4.0.4	Stored XSS via REST API (Contributor+)	01.05.2026	Behoben ✓

Meta Box · Version 7.2 · gemeldet am 09.03.2026 · Status: **Behoben** ✓

> ***Authenticated (Contributor+) Arbitrary File Deletion Vulnerability*** *Betrifft Versionen ≤ 5.11.11*

Angemeldete Nutzer mit Contributor-Rolle oder höher konnten beliebige Dateien auf dem Server löschen — ein kritisches Risiko, das bei Ausnutzung zu vollständigem Datenverlust oder einer kompromittierten WordPress-Installation führen kann. Patchstack hat den Angriff aktiv blockiert; das Plugin wurde umgehend aktualisiert.

Elementor · Version 4.3 · gemeldet am 30.03.2026 · Status: **Behoben** ✓

> ***Incorrect Authorization to Authenticated (Contributor+) Sensitive Information Exposure via Elementor Template Vulnerability*** *Betrifft Versionen ≤ 3.35.7*

Durch fehlerhafte Berechtigungsprüfung konnten angemeldete Nutzer auf nicht-öffentliche Elementor-Templates und darin enthaltene sensible Daten zugreifen. Das Plugin wurde im Rahmen des Wartungsvertrags zeitnah aktualisiert.

Elementor · gemeldet am 01.05.2026 · Status: **Behoben** ✓

> ***Low Priority Authenticated (Contributor+) Stored Cross-Site Scripting via REST API Vulnerability*** *Betrifft Versionen ≤ 4.0.4*

Über die REST API konnten angemeldete Nutzer schadhaften JavaScript-Code dauerhaft einschleusen (Stored XSS). Patchstack hat die Schwachstelle für domain.com am 01. Mai 2026 zunächst virtuell entschärft; das Plugin-Update erfolgte unmittelbar danach.

Warum kontinuierliches Schwachstellen-Monitoring entscheidend ist

Die drei Fälle dieses Quartals zeigen exemplarisch, warum reaktives Handeln — also das Aktualisieren von Plugins nur dann, wenn ein Problem bekannt wird — nicht ausreicht:

Zwischen Meldung und Ausnutzung vergehen oft nur Stunden. Sobald eine Schwachstelle öffentlich bekannt gemacht wird, beginnen automatisierte Angriffs-Bots innerhalb kürzester Zeit

mit dem Scannen und Ausnutzen betroffener Installationen. Ohne aktives Monitoring bleibt eine WordPress-Website in diesem Zeitfenster schutzlos — auch wenn sie nicht prominent oder groß ist.

Patchstack schließt die Lücke sofort, auch ohne Update. Der virtuelle Patch (Firewall-Regel) greift unmittelbar nach Bekanntwerden der Schwachstelle und schützt die Website, bevor der Plugin-Entwickler überhaupt ein Update veröffentlicht hat. Dieses Schutzfenster kann Tage bis Wochen betragen.

Wartungsverträge ohne Schwachstellen-Monitoring sind unvollständig. Ein Plugin, das einmal pro Monat pauschal aktualisiert wird, kann drei Wochen lang angreifbar sein. Kontinuierliches Monitoring erkennt neue CVEs tagesgenau und ermöglicht gezieltes, priorisiertes Handeln.

Für domain.com bedeutet das konkret: Alle drei Schwachstellen wurden erkannt, virtuell abgesichert und durch Plugin-Updates dauerhaft geschlossen — ohne dass ein einziger Angriff erfolgreich war. Das ist kein Zufall, sondern das Ergebnis eines strukturierten Schutzprozesses.

---

5. Empfehlung

Verfügbarkeit & Performance

Der Ausfall am 07. April 2026 (1 Std. 52 Min.) korreliert mit einem massiven TTFB-Anstieg auf über 8 Sekunden (Scanfully). Beides deutet auf eine serverseitige Überlastung hin. Falls noch nicht geschehen, empfehlen wir:

- Serverseitige Logs des betreffenden Zeitraums prüfen
- Ggf. PHP-Memory-Limit oder Serverressourcen anpassen
- Automatische Benachrichtigungen bei Ausfällen über 5 Minuten aktivieren

Google Search Console

Die organische Sichtbarkeit ist stabil, hat aber Potenzial zur Verbesserung:

- **Ziel:** Durchschnittliche Position von 7 auf unter 5 verbessern
- Für Keywords auf Position 8–15 gezielte On-Page-Optimierungen (Title, Meta-Description, Inhalt) durchführen
- Interne Verlinkung stärken, um thematische Relevanz für Kernbegriffe zu erhöhen
- Regelmäßige Veröffentlichung von neuem Content (1–2 Beiträge pro Monat) empfohlen

Sicherheit

Alle gemeldeten Schwachstellen wurden im Rahmen des Wartungsvertrags umgehend geschlossen — kein Handlungsbedarf für den Kunden. Für die laufende Absicherung empfehlen wir:

- Patchstack-Monitoring und virtuelle Patches aktiv halten (kein manueller Eingriff notwendig)
- Login-Schutz (2FA, Login-Versuche begrenzen) prüfen und ggf. nachrüsten
- Nutzer-Rollen regelmäßig prüfen: Contributor-Rechte nur vergeben, wenn wirklich benötigt (alle drei Schwachstellen setzten mindestens Contributor-Zugang voraus)

---

6. Nächste Schritte

- [ ] Ursache des April-Ausfalls klären und dokumentieren
- [x] Meta Box aktualisiert (Arbitrary File Deletion – behoben)
- [x] Elementor aktualisiert (Sensitive Information Exposure + Stored XSS – behoben)
- [ ] Nutzer-Rollen auf Contributor-Vergabe prüfen
- [ ] SEO-Audit für Top-10-Keywords durchführen
- [ ] Nächsten Bericht: August 2026
