Website Security Check – Produktübersicht

Kurzbeschreibung

Der Website Security Check von IT Logic & Dr. DSGVO ist eine vollständige, automatisierte Sicherheitsanalyse für öffentlich erreichbare Websites. Er prüft alle wesentlichen Sicherheitsbereiche – von der Domain-Infrastruktur über CMS-Schwachstellen bis hin zu JavaScript-Code und Formularen – und liefert die Ergebnisse als strukturierten Bericht mit verständlichen Diagnosen, Risikobewertungen und konkreten Handlungsempfehlungen. Entwickelt von deutschen Datenschutz- und IT-Sicherheitsexperten, einmalig buchbar, ohne Abonnement.

Top 3 Vorteile

Ein Bericht statt sieben Tools. CVE-Scan, DNS, SSL, HTTP-Header, Cookies, Formulare, CMS-Schwachstellen – vollständig, priorisiert, in einem Durchlauf.

Befunde, die jeder versteht. Technische Ergebnisse werden in klare Sprache übersetzt – mit konkreten Handlungsempfehlungen, die ohne IT-Hintergrund umsetzbar sind.

Sofort buchbar. Ergebnis in 30 Minuten.

Wer braucht den Security Check?

- **Website-Betreiber** jeder Größe, die wissen wollen, ob ihre Seite angreifbar ist
- **KMU und Selbstständige**, die keine eigene IT-Abteilung haben
- **Agenturen und Webentwickler**, die Sicherheits-Audits für Kundenprojekte anbieten oder nachweisen wollen
- **Unternehmen mit WordPress, TYPO3, Drupal, Magento oder dem Government Site Builder**, deren Plugin-Landschaft selten systematisch geprüft wird
- **Behörden und öffentliche Einrichtungen**, die den Government Site Builder (GSB) einsetzen
- **Datenschutzbeauftragte und Compliance-Verantwortliche**, die einen dokumentierten Nachweis über den Sicherheitsstatus einer Website benötigen
- **Unternehmen mit Barrierefreiheitspflicht** ab Juni 2025 (European Accessibility Act)
- Alle, die bisher auf kostenlose Einzeltools gesetzt haben und ein konsolidiertes, priorisiertes Gesamtbild benötigen

---

Vorteile – auf einen Blick

- Vollständige Sicherheitsanalyse in einem einzigen Bericht – ersetzt 7+ Einzeltools
- Ergebnisse in verständlicher Sprache, auch ohne IT-Hintergrund nutzbar
- Jeder Befund mit Risikobewertung, Erklärung und Schritt-für-Schritt-Anleitung
- CVE-Schwachstellenanalyse gefiltert nach tatsächlich eingesetzten Technologien
- CMS-spezifische Prüfungen für WordPress, TYPO3, Drupal, Magento und den Government Site Builder (GSB)
- Barrierefreiheitsprüfung (WCAG 2.2) optional integriert – günstiger als Einzelaudit
- Befundverwaltung im Bericht: Status, Kommentare, Fortschrittsanzeige
- Management Summary als PDF-Export für Auftraggeber und DSB
- Preis ab 64 € zzgl. MwSt.
- Ergebnis in der Regel innerhalb von 30 Minuten bis wenigen Stunden
- Kein IT-Vorwissen, keine Installation, keine Abstimmung erforderlich
- Made in Germany – keine Datenverarbeitung über AWS oder Azure
- Regelbasierte Prüflogik statt KI – präzise, reproduzierbar, zuverlässig
- Minimalinvasiver Scan – kein Ausfall, keine Beeinträchtigung des Betriebs

---

Was wird geliefert?

Nach der Buchung erhält der Kunde einen sicheren Link zu einem strukturierten Online-Bericht, der folgende Inhalte umfasst:

Sicherheitsanalyse (Kern)

- Gesamtrisiko-Score mit Einzelbewertungen je Prüfbereich
- CVE-Schwachstellen: Auflistung bekannter Lücken in erkannten Technologien, jeweils mit CVSS-Schweregrad, Betroffenheitsanalyse und Behebungsanleitung
- DNS- und E-Mail-Sicherheit: SPF, DKIM, DMARC, DNSSEC mit Diagnose und Konfigurationsvorschlägen
- SSL/TLS-Bericht: Zertifikat, Protokollversionen, Cipher-Suiten, HSTS, DANE
- HTTP-Sicherheitsheader: vollständige Prüfung mit sofort einsetzbaren Code-Snippets
- JavaScript- und XSS-Analyse: DOM-Inspektion mit Fundstellen und Erläuterungen
- Cookie- und Storage-Scan: alle Browser-Speicher auf sensible Daten geprüft
- CMS- und Plugin-Erkennung mit CVE-Abgleich
- Kontaktformular-Prüfung auf Injection und CSRF
- IP- und URL-Reputation gegen globale Blacklists
- Infrastruktur-Analyse: Webserver, offene Ports, Banner, CDN

Befundverwaltung

- Statusvergabe je Befund (erledigt / zurückgestellt / nicht relevant / ignoriert)
- Freitext-Kommentarfeld pro Befund (z. B. Ticket-Nummer, Verantwortlicher)
- Fortschrittsanzeige über alle Befunde

Management Summary (Abschlussbericht)

- Kompakte Übersicht erledigter und offener Maßnahmen
- Restrisiko-Bewertung nach Kritikalität
- Exportierbar als PDF, geeignet als Nachweis für Auftraggeber oder Datenschutzbeauftragte

Kurzbericht für Entscheider Komprimierte Top-Level-Ansicht auf den vollständigen technischen Bericht. Alle Befunde in nichttechnischer, verständlicher Sprache – für Geschäftsführer, Auftraggeber und Führungskräfte ohne IT-Hintergrund, die einen schnellen, klaren Überblick über den Sicherheitsstatus benötigen.

Übersichtsbericht Ebenfalls eine nichttechnische Zusammenfassung des Vollberichts, mit etwas mehr Tiefe als der Kurzbericht. Geeignet für interne Abstimmungen, Präsentationen oder als Grundlage für die Kommunikation mit externen Dienstleistern und Datenschutzbeauftragten.

Optional zubuchbar

- Barrierefreiheitsprüfung: WCAG-2.2-Check für alle Seiten, Farbkontrast-Analyse, Farbenblindheits-Simulation, priorisierte Abhilfemaßnahmen
- SEO-Check: Keywords, Seitenstruktur, strukturierte Daten, Content-Qualität
- Speed-Check: Core Web Vitals, HTTP-Timings, Bildoptimierung

---

Die 5 wichtigsten FAQ

Für wen ist der Security Check geeignet? Für alle Betreiber einer öffentlich erreichbaren Website – unabhängig von Unternehmensgröße oder technischem Vorwissen. Der Bericht ist so aufgebaut, dass er für technisch versierte Nutzer ebenso verwertbar ist wie für Geschäftsführer oder Datenschutzbeauftragte ohne IT-Hintergrund.

Wird die Website durch den Scan beeinträchtigt? Nein. Der Scan erfolgt mit bewusst geringer Last und ist auf störungsfreien Parallelbetrieb ausgelegt. Es werden keine Änderungen an der Website vorgenommen. Der optionale Portscan kann bei der Buchung abgewählt werden, ohne nennenswerte Einbußen beim restlichen Bericht.

Wann ist der Bericht verfügbar? In der Regel innerhalb von 30 Minuten nach Zahlungsbestätigung, bei starker Auslastung nach wenigen Stunden. Der Bericht wird per E-Mail als sicherer Link zugestellt und ist jederzeit abrufbar und ausdruckbar.

Was unterscheidet diesen Check von kostenlosen Tools wie SSL Labs oder securityheaders.com? Kostenlose Einzeltools prüfen jeweils nur einen Teilbereich – SSL Labs ausschließlich TLS-Konfiguration, securityheaders.com nur HTTP-Header. Für ein vollständiges Sicherheitsbild wären mindestens 7 verschiedene Tools nötig, deren Ergebnisse manuell konsolidiert und gewichtet werden müssten. Der Security Check liefert all das in einem einzigen Durchlauf – mit einheitlicher Priorisierung, gemeinsamer Gesamtbewertung und konkreten Handlungsempfehlungen für jeden Befund.

Setzt der Scanner künstliche Intelligenz ein? Nein – bewusst nicht. Der Scanner arbeitet mit speziell entwickelten, regelbasierten Prüfroutinen. Eigene Tests haben gezeigt, dass dieser Ansatz bei technischen Sicherheitsanalysen präzisere, schnellere und reproduzierbarere Ergebnisse liefert als KI-basierte Verfahren, die in diesem Bereich zu Unschärfen und Falsch-Positiven neigen.