Website Security Check – Marketing-Text

Das Problem: Die meisten Websites sind angreifbarer als gedacht

Angreifer setzen keine exotischen Methoden ein. Sie scannen täglich automatisiert Millionen von Websites auf bekannte Schwachstellen – veraltete Plugins, unsichere Formular-Handler, fehlende DNS-Einträge. **43 % aller Cyberangriffe treffen kleine und mittelständische Unternehmen.** Und 72 % der Betreiber wissen nichts von ihrer Lücke – bis es zu spät ist.

Wer die eigene Website nicht kennt, kann sie nicht schützen.

Die Lösung: Ein vollständiger Sicherheitsbericht – verständlich, umsetzbar, fair bepreist

Der **Website Security Check von IT Logic & Dr. DSGVO** durchleuchtet eine Website von der Domain bis zum Backend. Kein roher Datenberg, sondern ein strukturierter Bericht mit klaren Diagnosen, Risikobewertungen und konkreten Schritt-für-Schritt-Anleitungen – auch ohne IT-Hintergrund verständlich.

Hoher Nutzen, günstiger Preis.

Leistungsmerkmale

Umfassende Außenprüfung aus einer Hand

Der Bericht deckt alle wesentlichen Sicherheitsbereiche in einem einzigen Durchlauf ab – das, wofür man sonst 7 separate Tools bräuchte:

- **CVE-Schwachstellenanalyse** – bekannte Sicherheitslücken in eingesetzter Software werden erkannt, nach Schweregrad bewertet (CVSS) und mit Behebungsanleitung versehen
- **DNS & E-Mail-Sicherheit** – SPF, DKIM, DMARC, DNSSEC: Schutz vor Phishing und E-Mail-Spoofing
- **SSL/TLS & DANE** – Zertifikatsprüfung, TLS-Versionen, Cipher-Suiten, HSTS und DANE-Validierung (Alleinstellungsmerkmal)
- **HTTP-Sicherheitsheader** – CSP, X-Frame-Options, Referrer-Policy u. v. m. mit sofort einsetzbaren Konfigurationszeilen
- **JavaScript & XSS-Analyse** – DOM-Inspektion auf Cross-Site-Scripting-Schwachstellen mit exakten Fundstellen

- **Cookie- & Storage-Scan** – alle Cookies, LocalStorage und SessionStorage auf sensible oder sicherheitskritische Daten
- **CMS-spezifische Prüfungen** – WordPress, TYPO3, Drupal, Magento: Login-Routen, Plugin-CVEs, Benutzerenumeration, exponierte Dateien
- **Kontaktformular-Prüfung** – Form-Handler und Eingabefelder auf SQL-Injection, CSRF und weitere Angriffsvektoren
- **IP- & URL-Reputation** – Abgleich gegen globale Blacklist- und Abuse-Datenbanken
- **Infrastruktur-Analyse** – Webserver, Betriebssystem, CDN, offene Ports, Banner-Grabbing

Barrierefreiheit (optional, aber günstig integriert)

Vollständige WCAG-2.2-Prüfung für alle Seiten, Farbkontrast-Analyse mit konkreten Farbvorschlägen und Farbenblindheits-Simulation (Deuteranopie, Protanopie, Tritanopie). Deutlich günstiger als ein separates Accessibility-Audit – und seit dem European Accessibility Act (Juni 2025) für viele Unternehmen gesetzlich relevant.

SEO & Speed (optional zubuchbar)

Core Web Vitals, Seitenstruktur, Keywords, Bildoptimierung, strukturierte Daten – ein vollständiges Bild der Website-Qualität.

Befundverwaltung & Management Summary

Befunde lassen sich direkt im Bericht mit Status versehen (erledigt, zurückgestellt, nicht relevant). Daraus kann ein kompakter Abschlussbericht erstellt werden – geeignet als Nachweis für Auftraggeber oder Datenschutzbeauftragte, exportierbar als PDF.

Vorteile

Alles in einem Bericht, nicht in sieben Tools SSL Labs, securityheaders.com, MXToolbox, WPScan, AbuseIPDB, WAVE – all das steckt im Security Check. Kein mühsames Zusammenführen von Teilergebnissen aus unterschiedlichen Quellen.

Verständlich, nicht technisch einschüchternd Jeder Befund enthält eine Erklärung in einfacher Sprache, eine Risikobewertung und konkrete Abhilfeschritte – mit Konfigurationsbeispielen, weiterführenden Links (OWASP, MDN) und realen Angriffsszenarien, die zeigen, was auf dem Spiel steht.

Schnell und unkompliziert Keine Installation, keine Abstimmung, kein wochenlanger Prozess. URL eingeben, buchen – Bericht in der Regel innerhalb von 30 Minuten oder wenigen Stunden per E-Mail. Scan mit geringer Last, kein Ausfall.

Fair bepreist, einmalig Ab 64 € zzgl. MwSt. Professionelle Tiefenanalyse ohne großes Budget.

Made in Germany, kein AWS, kein Azure Alle beteiligten Dienstleister haben ihren Stammsitz in Deutschland und sind unabhängig von außereuropäischen Einheiten. Daten bleiben in Europa.

Keine KI – bewusst Der Scanner setzt auf speziell entwickelte, regelbasierte Prüfroutinen statt auf KI. Das Ergebnis: präzisere, schnellere und reproduzierbare Resultate ohne die typischen Unschärfen KI-basierter Analysen. Eine eigene lokale KI wird nur für die Erstellung verständlicher Befundtexte eingesetzt.

Welches Problem löst das Produkt?

Website-Betreiber – ob Selbstständige, KMU oder Agenturen – haben keine Zeit, IT-Sicherheitsexperten zu werden. Gleichzeitig sind Schwachstellen auf öffentlich erreichbaren Websites kein abstraktes Risiko, sondern tägliche Realität: Automatisierte Scanner finden neue Lücken innerhalb von Minuten nach Veröffentlichung einer CVE.

Der Security Check löst drei konkrete Probleme:

1. **Unsichtbarkeit** – Betreiber wissen nicht, welche Schwachstellen ihre Website hat. Der Bericht macht sie sichtbar, priorisiert und erklärbar.
2. **Überforderung** – Rohe Scan-Ergebnisse aus Einzeltools überfordern ohne Kontext und Anleitung. Der Bericht übersetzt technische Befunde in klaren Handlungsbedarf.
3. **Aufwand** – Sieben verschiedene Tools zu kombinieren, ihre Ergebnisse zu gewichten und daraus einen Maßnahmenplan zu erstellen, ist für die meisten Betreiber nicht realistisch. Der Security Check liefert das in einem einzigen strukturierten Durchlauf.

Wer wissen will, ob eine Website sicher ist – und was zu tun ist, wenn sie es nicht ist – bekommt hier eine klare, ehrliche Antwort. Ohne Fachjargon-Barriere. Ohne Abo-Falle.

Powered by Dr. DSGVO & IT Logic – Geprüfte Qualität von Datenschutz- und IT-Sicherheitsexperten seit 2017.