

PASSIVES AUDIT DER WEBSITE-QUALITÄT

Website-Prüfung *example.com*



GESAMTSCORE

75 / 100

B

Erfordert Aufmerksamkeit · 40 Befunde, davon 8 mit hoher Schwere

8

hoch

6

mittel

15

niedrig

11

info

Scan durchgeführt 24.09.2026 12:00 UTC
Bericht erstellt 24.09.2026 12:00 UTC
Bewertungsversion 3.0.0

Der Bericht liest nur öffentlich verfügbare Daten und greift in keiner Weise in die Website ein. Er ist weder ein Penetrationstest noch eine rechtliche Beurteilung. Details in Kapitel 16 Wie wir messen.

01

ZUSAMMENFASSUNG

Zusammenfassung für Website-Betreiber

GESAMTBEWERTUNG

75 / 100

Note B · erfordert
Aufmerksamkeit
Messabdeckung 100 %

Die Website example.com erreicht im Gesamtscore 75 von 100 Punkten, Note B, doch die Note allein sagt nicht alles: 8 Befunde mit hohem Schweregrad können dem Unternehmen Probleme bereiten, deshalb lohnt es sich, sie zu beheben.

Am stärksten: E-Mail-Authentifizierung und Exponierte Inhalte (100). Am schwächsten: Sicherheits-Header (49) und SEO (59).

GRÖSSTE RISIKEN

1 Die Besuchermessung läuft schon vor der Einwilligung HOCH

Tracking-Tools starten auf der Website schon vor der Einwilligung der Besucher, obwohl sie nach den Cookie-Regeln erst danach laufen sollten.

Beruh auf dem Befund „Tracking-Cookies vor der Einwilligung gespeichert“ (Schweregrad: hoch): Im Browser wurden ohne jede Interaktion Tracking-Cookies gesetzt: _ga (.example.com, Laufzeit: 2 J.) · damit verbunden: 1 weiterer Befund.

2 Langsames Laden kann Anfragen von Mobilgeräten kosten HOCH

Die Startseite lud in der Google-PageSpeed-Messung langsam. Langsames Laden kann mobile Besucher abschrecken, bevor sie die Seite überhaupt sehen. Google wertet Geschwindigkeit als eines von vielen Signalen; Vorrang hat der Inhalt.

Beruh auf dem Befund „Langsames Laden des Hauptinhalts (LCP)“ (Schweregrad: hoch): LCP 4,1 s (Lighthouse-Labor, mobil, Median aus 3 Durchläufen); Schwelle für „gut“ ≤ 2,5 s.

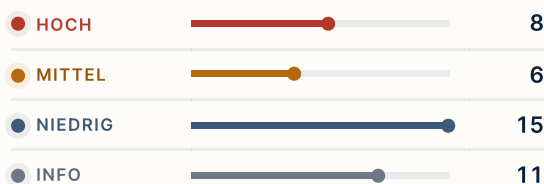
3 WordPress hat wahrscheinlich die Sicherheitsupdates nicht installiert HOCH

In neueren Versionen behobene Fehler sind öffentlich beschrieben und Bots suchen automatisch danach; die Versionsnummer ist eine Schätzung aus öffentlichen Spuren, den tatsächlichen Stand prüft der Administrator. Wir empfehlen, WordPress auf die neueste Version zu aktualisieren und automatische Updates einzuschalten; nach einer langen Pause prüfen lassen, ob die Website missbraucht wurde.

Beruh auf dem Befund „WordPress hat wahrscheinlich die Sicherheitsupdates nicht installiert“ (Schweregrad: hoch): Die Startseite nennt WordPress 6.2 (Quelle: meta generator). Für diesen Zweig ist die Korrektur 6.2.13 erschienen, die den Fehler CVE-2026-87902 behebt; die US-Behörde CISA führt ihn als tatsächlich ausgenutzt · damit verbunden: 1 weiterer Befund.

Die Risiken sind nach Schweregrad und Auswirkung der Befunde ausgewählt; es handelt sich um mögliche Folgen des festgestellten Zustands, nicht um einen bestätigten Vorfall.

RISIKOPROFIL



VERTEILUNG DER SCORES



Anzahl der Bereiche je Band: ≥ 75 in Ordnung · 40–74 Vorsicht · < 40 Risiko · nicht gemessen.

02

BEREICHE

Score nach Bereichen

13 von 15 Bereichen haben einen Score; 10 davon gehen gewichtet in den Gesamtscore ein.
Cyberhygiene und Drittanbieter sind Übersichten ohne Score.

BEREICH	STATUS		SCORE	GEWICHTUNG
Sicherheits-Header	gemessen		49	13
E-Mail-Authentifizierung	gemessen		100	12
TLS / Zertifikat	gemessen		89	15
DNS & Infrastruktur	teilweise gemessen		89	6
Cookies / DSGVO	gemessen		60	6
Leistung (Core Web Vitals)	gemessen		74	14
SEO	gemessen		59	11
begrenzt: grundlegende Titel und Beschreibungen fehlen				
Barrierefreiheit	gemessen		60	5
CMS / Technologie	gemessen		59	8
begrenzt: Software wahrscheinlich ohne Updates				
Exponierte Inhalte	teilweise gemessen		100	10
KI-Suchmaschinen	gemessen		100	info
Unternehmen & Onlineshop	teilweise gemessen		100	info
Suchmaschinen (außer Google)	gemessen		97	info

Bereiche mit der Gewichtung „info“ sind vorerst informativ: Sie zeigen den Zustand der Website, fließen aber nicht in den Gesamtscore ein.

Der Hinweis „begrenzt“ bedeutet, dass der Bereich einen schwerwiegenden Befund hat, wegen dem seine Punktzahl nicht grün sein kann, egal wie die übrigen Punkte aussehen.

Der Gesamtscore ist der gewichtete Durchschnitt der *gemessenen* Bereiche. In diesem Scan wurden alle gewichteten Bereiche geprüft (Abdeckung 100 %).

Ohne optionale externe Quelle geprüft: DNS & Infrastruktur (Quelle RIPEstat nicht verfügbar), Exponierte Inhalte (Quelle crt.sh nicht verfügbar). Deren Daten fehlen in diesem Scan; der Ausfall eines fremden Dienstes verändert den Score der Website nicht.

WORAUF SIE ACHTEN SOLLTEN

Sicherheits-Header ● HOCH 49
Sicherheits-Header sind Anweisungen, mit denen die Website dem Browser mitteilt, wie er sie schützen soll. Fehlen sie, kann ein Angreifer die Seite leichter missbrauchen, zum Beispiel sie in eine betrügerische Website einbetten oder ihr fremden Code unterschieben.

Cookies / DSGVO ● HOCH 60
Analyse- und Werbetoools dürfen erst nach der Einwilligung der Besucher laufen. WebMeter prüft, ob sie früher starten.

Leistung (Core Web Vitals) ● HOCH 74
Die Ladegeschwindigkeit zählt vor allem auf dem Smartphone. Langsames Laden kann Besucher abschrecken, bevor sie Ihr Angebot sehen. Google sieht Geschwindigkeit als eines von vielen Signalen, Vorrang hat der Inhalt.

SEO 59
SEO bestimmt, wie leicht Menschen Sie über eine Suchmaschine finden. Hapert es daran, finden Kunden, die nach Ihren Leistungen suchen, eher die Konkurrenz.

Barrierefreiheit ● HOCH 60
Barrierefreiheit bedeutet, dass auch Menschen mit eingeschränktem Sehvermögen, ältere Menschen oder Nutzer von Smartphones die Website bedienen können. Für Onlineshops und einige weitere Dienstleistungen schreibt das Barrierefreiheitsgesetz sie seit dem 28. Juni 2025 vor (Kleinstunternehmen sind ausgenommen).

CMS / Technologie ● HOCH 59
Das CMS, die Erweiterungen und Bibliotheken, auf denen die Website läuft. Veraltete Versionen haben oft bekannte Schwachstellen, nach denen Bots im Internet gezielt suchen.

03

VERBINDUNGSSICHERHEIT

Zertifikat und HTTPS

Aussteller	● Test Trust
Zertifikatstyp	● Validierungstyp nicht angegeben · Schlüssel ECDSA P-256
Gültig bis	● 23.11.2026
Tage bis zum Ablauf	● 60
Zertifikatserneuerung	● wahrscheinlich automatisch (Laufzeit 70 Tage)
Vertrauenswürdig	● ja
Widerrufsstatus	● nicht widerrufen (OCSP: good)
Unterstützte TLS-Versionen	● TLS 1.0, TLS 1.2 und TLS 1.3 — auch veraltete Versionen sind aktiviert
Schwache Cipher Suites	● keine gefunden
Forward Secrecy	● ja
OCSP Stapling	● nein, der Browser prüft den Zertifikatsstatus selbst
HTTP/2	● ja
HTTP/3	● ja, der Server bietet es an
Weiterleitung auf HTTPS	● in Ordnung — alle Varianten führen zu https://example.com/
HSTS Preload	● HSTS gilt langfristig; im Header fehlt die Direktive includeSubDomains, die für Preload nötig ist (optional)
Unverschlüsselte Ressourcen auf der Seite	● 0 Skripte/Stylesheets/Frames, 1 Bilder/Medien über http://

Gemessen wird nur, was der Server beim Verbindungsaufbau einem gewöhnlichen Client zeigt, sowie öffentliche Quellen (OCSP der Zertifizierungsstellen, HSTS-Preload-Liste). TLS-Versionen und schwache Cipher Suites werden mit je einem gewöhnlichen Verbindungsaufbau pro Version und Gruppe von Cipher Suites geprüft; es handelt sich nicht um eine vollständige Analyse aller Cipher Suites, wie sie SSL Labs durchführt. Was sich so nicht ermitteln lässt, ist als „nicht ermittelt“ angegeben.

04

EXPONIERTE INHALTE

Öffentliche Spuren der Domain

Subdomains in öffentlichen Zertifikatseinträgen (CT) ○ Quelle nicht erreichbar, Subdomains nicht geprüft

Die Subdomain-Namen stammen aus öffentlichen Einträgen ausgestellter Zertifikate (Certificate Transparency). Die Sensibilität beurteilen wir nur nach dem Namen; bei der Einordnung nach Dienstyp prüfen wir zusätzlich im DNS, dass der Name noch existiert. Das ist keine Bestätigung, dass ein Dienst oder Port aus dem Internet erreichbar wäre. Der öffentliche Bericht zeigt nur Anzahlen und teilweise maskierte Beispiele, keine vollständigen Namen.

Grundlagen der Cyberhygiene

Die EU-Richtlinie NIS2 (in Tschechien umgesetzt durch das neue Cybersicherheitsgesetz, in Kraft seit dem 1. 11. 2025) betrifft auch viele mittlere und große Unternehmen in ausgewählten Branchen. Ihre Pflichten reichen weit über die Website hinaus; hier sind acht Grundlagen, die von außen sichtbar sind und jeder Website guttun.

3 von 8 Grundlagen in Ordnung · teilweise: 3 · fehlt: 2

GRUNDLAGE	STATUS
Verschlüsselte Verbindung (HTTPS, TLS 1.2+) Die Verbindung ist verschlüsselt, aber der Server akzeptiert auch die veralteten Versionen TLS 1.0.	● TEILWEISE
Erzwungenes HTTPS (HSTS) Browser haben die Anweisung, die Website nur über HTTPS zu öffnen.	● IN ORDNUNG
Schutz vor gefälschten E-Mails (SPF, DKIM) Der SPF-Eintrag ist in Ordnung und eine DKIM-Signatur wurde gefunden.	● IN ORDNUNG
DMARC-Richtlinie Empfänger sollen gefälschte E-Mails in Ihrem Namen in den Spam verschieben (p=quarantine).	● IN ORDNUNG
Aktuelle Website-Software Die Website verwendet wahrscheinlich einen veralteten Kern des Redaktionssystems, Serversoftware nach Supportende und veraltete oder nicht mehr unterstützte JavaScript-Bibliotheken; Details stehen in den Befunden.	● FEHLT
Sicherheits-Header 3 von 4 Schutzmaßnahmen im Browser fehlen: Regeln für das Laden von Inhalten (CSP), das Verbot, die Website in fremde Seiten einzubetten und Regeln für die Weitergabe der Adresse (Referrer-Policy). Sie werden vom Website- oder Hosting-Administrator gesetzt.	● FEHLT
Kontakt für Schwachstellenmeldungen (security.txt) Die Datei security.txt ist ein öffentlicher Briefkasten für die Meldung von Sicherheitslücken. Sie ist gute Praxis, keine Pflicht; etwa 2 % der Websites haben sie.	● TEILWEISE
Signierte Domain (DNSSEC) Die Domain ist nicht signiert (DNSSEC). Das ist eine Empfehlung, kein Fehler; etwa zwei Drittel der .cz-Domains nutzen es. Der DNS-Administrator schaltet es ein, oft mit einem Klick.	● TEILWEISE
Dies ist keine Prüfung der Einhaltung des Gesetzes. Wir zeigen nur, was von außen auf der Website und im DNS sichtbar ist.	

06

DRITTANBIETER

Wem die Website Besucherdaten schickt

Wir zeigen die Dienste, die die Startseite sofort beim Öffnen lädt, ohne Scrollen und noch vor der Einwilligung des Besuchers. Unterseiten, den Warenkorb und über den eigenen Server der Website angebundene Dienste sehen wir hier nicht. WebMeter klickt nie auf das Einwilligungsbanner und sieht daher nicht, was die Website erst nach der Einwilligung lädt.

2	0	2	0	2
Drittanbieterdienste insgesamt	davon außerhalb des EWR in einem Land mit angemessenem Schutzniveau	davon mit Betreiber mit Sitz in den USA	davon mit Betreiber in einem anderen Drittland	davon Reichweitenmessung und Werbung

DIENT	ZWECK	SITZ DES BETREIBERS	INTEGRITÄTSPRÜFUNG (SRI)
Google Analytics www.google-analytics.com	Analyse	● USA · außerhalb der EU/des EWR	—
Google Tag Manager www.googletagmanager.com	Analyse	● USA · außerhalb der EU/des EWR	—

Der Sitz ist das Land des Unternehmens, das den Dienst betreibt (bei internationalen Konzernen der Sitz der Muttergesellschaft), laut unserer Dienstübersicht (Version 2026-09-29); nicht der Standort der Server. Dienste außerhalb der Übersicht führen wir als unbekannt und zählen sie nicht zu außerhalb der EU/des EWR.

Länder mit einem Angemessenheitsbeschluss der Europäischen Kommission (z. B. Vereinigtes Königreich, Schweiz, Kanada) führen wir gesondert auf; für Übermittlungen dorthin gelten dieselben Regeln wie innerhalb der EU (Länderliste geprüft zum 15.10.2026). Eine Einwilligung in Messung und Werbung ist unabhängig vom Land nötig.

Das Laden eines Dienstes bedeutet noch nicht, dass er personenbezogene Daten gesendet hat; ob Mess- und Werbedienste Besucher vor der Einwilligung verfolgen, behandeln die Befunde des Bereichs Cookies / DSGVO. Dies ist keine rechtliche Bewertung der Datenübermittlung.

In der Spalte SRI markieren wir nur Bibliotheken mit fester Version von öffentlichen CDNs, die ohne Integritätsprüfung geladen werden. Bei anderen Diensten ist eine Integritätsprüfung nicht möglich oder wir können sie nicht beurteilen.

Wie die Website in gängigen Tools abschneiden würde

Schätzung, kein offizielles Ergebnis. Es handelt sich um eine Schätzung nach der öffentlichen Methodik der genannten Tools, berechnet aus den Daten, die dieser passive Scan gesammelt hat. Das offizielle Ergebnis kann abweichen: Die Tools testen mehr und ändern ihre Methodik laufend. Wo der Scan eine Angabe nicht ermittelt hat, steht „nicht ermittelt“.

TOOL	ERGEBNIS	HINWEIS
SSL Labs (Qualys SSL Server Test) HTTPS-Konfiguration: Zertifikat, TLS-Protokollversionen, Cipher Suites und Schlüsselaustausch.	B	Protokolle: bestes TLS 1.3, schlechtestes TLS 1.0 → 95 Punkte. · Schlüsselaustausch: RSA-Äquivalent 3072 Bit → 90 Punkte. · Cipher-Suites: stärkste ermittelte 256 Bit, schwächste 128 Bit → 90 Punkte (ohne vollständige Aufzählung der Cipher-Suites). · Numerischer Score 91,5 → A. · Unterstützt: TLS 1.0 → höchstens B. · Schätzung nach der öffentlichen Methodik von SSL Labs auf Basis einer begrenzten Zahl von Verbindungen, kein offizielles Ergebnis von SSL Labs.
Mozilla HTTP Observatory Sicherheits-Header und Einstellungen der Website im Browser (CSP, HSTS, Cookies, Weiterleitungen, SRI).	F (20 Punkte)	—
securityheaders.com Vorhandensein der empfohlenen HTTP-Sicherheits-Header.	D	—
internet.nl — Website-Test Moderne Internetstandards der Website: IPv6, DNSSEC, HTTPS, Sicherheitsoptionen, RPKI.	0 von 5 Kategorien erfüllt, 1 nicht ermittelt	IPv6: nicht erfüllt · DNSSEC: nicht erfüllt · HTTPS: mit Einschränkung · Sicherheitsoptionen: nicht erfüllt · RPKI: nicht ermittelt
internet.nl — E-Mail-Test Moderne E-Mail-Standards der Domain: IPv6, DNSSEC, DMARC/DKIM/SPF, DANE und STARTTLS, RPKI.	1 von 5 Kategorien erfüllt, 1 nicht ermittelt	IPv6: nicht erfüllt · DNSSEC: nicht erfüllt · DMARC, DKIM und SPF: erfüllt · DANE und STARTTLS: nicht erfüllt · RPKI: nicht ermittelt
Regeln von Gmail, Yahoo und Microsoft für Massensender Anforderungen an Absender von rund 5.000 E-Mails täglich: Google und Yahoo seit 2/2024, Outlook.com (Hotmail, Live) seit 5/2025.	3 von 5 Anforderungen erfüllt, 2 nicht ermittelt	SPF: erfüllt · DKIM: erfüllt · DMARC (mindestens p=none): erfüllt · Domain-Alignment (Domain im From = Domain von SPF oder DKIM): nicht ermittelt · Abmeldung mit einem Klick (Google und Yahoo, Massensender): nicht ermittelt
Google PageSpeed Insights Ladezeit der Startseite in einer Labormessung (Lighthouse).	Leistung 61 von 100	Labormessung mit Lighthouse (Mobilgerät, Median aus 3 Durchläufen). · Weitere Lighthouse-Kategorien: Barrierefreiheit 84 (automatische Prüfung, kein Audit), Best Practices 78, SEO 92. · Das Ergebnis von PageSpeed Insights schwankt zwischen einzelnen Durchläufen leicht. · Den Wert des Bereichs Leistung in der Bereichstabelle (74 von 100) berechnet WebMeter wie bei den übrigen Bereichen aus den Messbefunden. PageSpeed Insights nennt einen eigenen Lighthouse-Laborwert (61 von 100); deshalb weichen die beiden Zahlen voneinander ab.
DNSViz Detaillierte Analyse der DNSSEC-Signaturkette der Domain.	die Domain ist nicht signiert	—
MXToolbox Mailserver der Domain (MX) und deren grundlegende Prüfungen.	1 MX-Eintrag	—
HTML-Validator (W3C) Validität des HTML-Codes der Startseite.	keine Schätzung	Die HTML-Validität prüft dieser Scan nicht; das Ergebnis zeigt nur der offizielle Validator.

08

GESCHWINDIGKEIT

Website-Geschwindigkeit

Hauptinhalt (LCP)	● 4,1 s
Blockierung des Hauptthreads (TBT)	● 320 ms
Layout-Verschiebung (CLS)	● 0,06
Serverantwort	● 640 ms
Echte Besucher (Core Web Vitals)	○ Google hat nicht genug Daten für eine Bewertung

09

BARRIEREFREIHEIT

Barrierefreiheit

Der automatische Test hat 2 Probleme auf der Startseite gefunden. Er deckt nur einen Teil der Anforderungen der WCAG 2.2 ab; Tastaturbedienung, Formulare, Bestellprozess und Zahlung muss ein Mensch prüfen.

Hoher Schweregrad: Kunden mit Screenreader können die Aufgabe nicht abschließen. Mittel: es geht, aber mit Mühe.

Gemessen mit axe-core Version 4.13.0 in der Ansicht 1366 × 900.

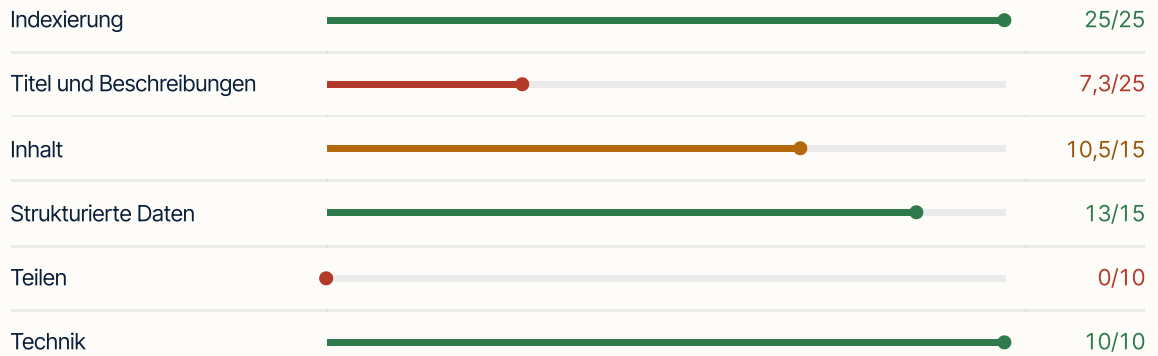
10

SEO

SEO im Detail

Wie eine Suchmaschine die Startseite sieht: Vorschau in den Ergebnissen, Meta-Angaben, Überschriftenstruktur, Text und eine Stichprobe von Unterseiten.

SEO: 59/100. Indexierung 25/25 · Titel und Beschreibungen 7,3/25 · Inhalt 10,5/15 · Strukturierte Daten 13/15 · Teilen 0/10 · Technik 10/10.



Punktzahl begrenzt: Auf den meisten Seiten fehlen eigener Titel und eigene Beschreibung.

Grünes SEO bedeutet, dass jede bewertete Seite einen eigenen Titel und eine eigene Beschreibung hat und die Website für Suchmaschinen erreichbar ist.

example.com

example.com

Příklad s.r.o. – náradí pro profesionály

E-shop s náradím a příslušenstvím pro řemeslníky.

Die Vorschau ist eine Orientierung — Suchmaschinen können Seitentitel und Beschreibung kürzen oder ersetzen.

META - ANGABEN

Seitentitel (title)	● Příklad s.r.o. – náradí pro profesionály (40 Zeichen)
Beschreibung (Meta-Description)	● E-shop s náradím a příslušenstvím pro řemeslníky. (49 Zeichen)
Canonical	● https://example.com/
Meta-Robots	● nicht angegeben (alles indexieren)
Sprache der Seite (lang)	● cs
Darstellung auf dem Smartphone (Viewport)	● ja
Zeichenkodierung	● utf-8
Open Graph (Teilen in sozialen Netzwerken)	● 0 von 5 Eigenschaften · Bild fehlt

Karte für X (Twitter) ● nicht angegeben

Website-Symbol (Favicon) ● nein

Strukturierte Daten (JSON-LD) ● Organization

ÜBERSCHRIFTENSTRUKTUR

H1	H2	H3	H4	H5	H6
1	0	0	0	0	0

H1 Nářadí pro profesionály

TEXT UND SCHLÜSSELWÖRTER

Textmenge ● 23 Wörter

Häufigste Wörter ● kořík (2×), partner (2×), stará (2×)

Hauptwörter in Seitentitel und H1 ● im Seitentitel: keine · in H1: keine

Dichte des häufigsten Wortes ● „kořík“ 8,7 % des Textes

Satzlänge ● durchschnittlich 4,0 Wörter pro Satz · lange Sätze 0 %

Wortschatzvielfalt ● 96 % unterschiedliche Wörter

Vertrauenslinks (E-E-A-T) ● Kontakt · fehlt: über das Unternehmen, Datenschutz

Der Text wird ohne JavaScript bewertet, so wie ihn Suchmaschinen lesen. Die Schätzung KI-generierter Texte ist eine Orientierung (typische Floskeln, Gedankenstriche, gleichförmige Satzlänge) — einen zuverlässigen Detektor gibt es nicht, und Google bewertet die Nützlichkeit eines Textes, nicht seine Herkunft.

STICHPROBE VON UNTERSEITEN

SEITE	SEITENTITEL	ZEICHEN IM SEITENTITEL	ZEICHEN IN DER BESCHREIBUNG	H1
/kontakt Titel fehlt, Beschreibung fehlt	fehlt	fehlt	fehlt	1
/obchodni-podminky nicht bewertet (Rechtsseite, Anmeldung oder Warenkorb)	fehlt	fehlt	fehlt	1
/kosik nicht bewertet (Rechtsseite, Anmeldung oder Warenkorb)	fehlt	fehlt	fehlt	1
/produkt/vrtacka Titel fehlt, Beschreibung fehlt	fehlt	fehlt	fehlt	1

Bewertet werden höchstens 5 Unterseiten, auf die die Startseite verlinkt.

11

KI-SUCHMASCHINEN

Wie KI Sie sieht

Immer mehr Menschen suchen über KI-Assistenten wie ChatGPT oder Perplexity. Ist die Website für deren Crawler gesperrt oder ohne JavaScript leer, weiß die KI möglicherweise nichts von Ihnen und empfiehlt eher die Konkurrenz.

KI-Such-Bots	● haben Zugriff
Bots auf Nutzeranfrage	● haben Zugriff
Crawler für KI-Training	● haben Zugriff
KI-Antworten von Seznam	● die Regeln der Website verbieten sie nicht
Inhalt ohne JavaScript	● KI-Crawler sehen 58 % des Seitentextes
Firmenangaben für KI (strukturierte Daten)	● Organization · fehlt: Links zu Profilen
Ausschnitte in Suchmaschinen (KI-Antworten)	● die Regeln der Website verbieten sie nicht
Copilot (Bing)	● die Regeln der Website verbieten die Nutzung nicht
Datei llms.txt	● nein

OAI-SearchBot OpenAI · Suche	erlaubt
Claude-SearchBot Anthropic · Suche	erlaubt
PerplexityBot Perplexity · Suche	erlaubt
MistralAI-Index Mistral AI · Suche	erlaubt
Amzn-SearchBot Amazon · Suche	erlaubt
meta-webindexer Meta · Suche	erlaubt
ChatGPT-User OpenAI · Nutzeranfrage	erlaubt
Claude-User Anthropic · Nutzeranfrage	erlaubt
Perplexity-User Perplexity · Nutzeranfrage	erlaubt
MistralAI-User Mistral AI · Nutzeranfrage	erlaubt
Google-Agent Google · Nutzeranfrage	erlaubt
Amzn-User Amazon · Nutzeranfrage	erlaubt
meta-externalfetcher Meta · Nutzeranfrage	erlaubt
Seznam-Extended Seznam.cz · KI-Antworten von Seznam	erlaubt
AI Seznam.cz · KI-Antworten von Seznam	erlaubt

MachineLearning Seznam.cz · KI-Antworten von Seznam	erlaubt
GPTBot OpenAI · Modelltraining	erlaubt
ClaudeBot Anthropic · Modelltraining	erlaubt
MistralAI-Training Mistral AI · Modelltraining	erlaubt
Google-Extended Google · Training und Grounding für Gemini	erlaubt
Applebot-Extended Apple · Modelltraining	erlaubt
Amazonbot Amazon · Modelltraining	erlaubt
meta-externalagent Meta · Training und Indexierung	erlaubt
CCBot Common Crawl · Modelltraining	erlaubt
Bytespider ByteDance · Modelltraining	erlaubt
Googlebot Google · klassische Suche	erlaubt
bingbot Microsoft · klassische Suche	erlaubt
Applebot Apple · klassische Suche	erlaubt

Ausgewertet werden die Regeln der robots.txt für die Startseite (RFC 9309); einzelne Crawler-Betreiber können sich unterschiedlich verhalten. Das Sperren von Trainings-Crawlern ist eine legitime Entscheidung des Website-Betreibers und hat auf die Anzeige in KI-Antworten in der Regel keinen direkten Einfluss.

So finden Sie heraus, ob KI Sie erwähnt: Die Google Search Console hat einen Bericht zu generativer KI und in den Einstellungen die Option, ob die Website in KI-Funktionen erscheinen darf. Die Bing Webmaster Tools zeigen Zitate in Copilot. In Google Analytics 4 achten Sie auf den Kanal AI Assistant.

12

UNTERNEHMEN & ONLINESHOP

Unternehmen & Onlineshop

Das Gesetz verlangt, dass die Website eines Unternehmens angibt, wer sie betreibt — Name, Sitz und Firmennummer (IČO) —, und ein Onlineshop zusätzlich AGB, Reklamationsbedingungen und eine Widerrufsbelehrung. Fehlende Angaben mindern das Vertrauen der Kunden, und es drohen Sanktionen, zum Beispiel durch die Tschechische Handelsinspektion (ČOI).

Unternehmensangaben in strukturierten Daten	● ergänzbar: taxID, legalName, address
Onlineshop	● ja
An wen der Onlineshop verkauft	● Verbraucher
AGB	● ja
Reklamationsbedingungen	● in den AGB
Widerrufsbelehrung	● in den AGB
Datenschutzerklärung	● nicht gefunden
Informationen zur Barrierefreiheit	● nicht gefunden
Produktdaten für Google	● Preis und Währung vorhanden, es fehlt availability
Manuell zu prüfen	● die Schaltfläche „zahlungspflichtig bestellen“, Bestellbestätigung per E-Mail, Endpreis im Warenkorb

Die Unternehmensangaben stammen aus dem öffentlichen Register ARES. Bewertet werden nur öffentlich zugängliche Seiten der Website; eine als fehlend markierte Angabe hat die Prüfung dort nicht gefunden. Es handelt sich um kein Rechtsgutachten. Hinweis zum Scan: die Startseite hat im HTML wenig Text (wird vermutlich per JavaScript gerendert) — fehlende Angaben melden wir nicht.

13

SUCHMASCHINEN (AUSSER GOOGLE)

Sichtbarkeit in Suchmaschinen

Menschen in Tschechien suchen nicht nur über Google und Seznam (diese bewertet der Bereich SEO), sondern auch über Bing, DuckDuckGo oder Apple. Wenn die Website deren Bots aussperrt, eine fehlerhafte Sitemap hat oder auf nicht mehr funktionierende Websites verlinkt, ist sie in diesen Suchmaschinen schwerer zu finden.

Suchmaschinen-Crawler	● haben Zugriff
Ausschluss aus dem Index (noindex)	● keine gezielten
Sitemap (Website-Karte)	● in Ordnung, Adressen: 3

Stichprobe von Adressen aus der Sitemap ● 2 geprüfte Adressen in Ordnung

In robots.txt gesperrte Adressen aus der Sitemap ● keine

IndexNow ○ nicht ermittelt

Ausgehende Links ● 3 nicht funktionierend von 3 geprüften

SUCHMASCHINE	CRAWLER	ZUGRIFF LAUT ROBOTS.TXT
Google	Googlebot	erlaubt
Seznam.cz	SeznamBot	erlaubt
Microsoft Bing	bingbot	erlaubt
DuckDuckGo	DuckDuckBot	erlaubt
Apple (Siri, Spotlight)	Applebot	erlaubt
Yandex	YandexBot	erlaubt
Brave Search	Brave	erlaubt

WebMeter misst Stärke und Popularität der Domain nicht automatisch (die Quellen erfordern einen Schlüssel oder eine Registrierung).

Ausgewertet werden die Regeln in robots.txt für die Startseite (RFC 9309), die Sitemap und öffentliche Signale der Website. Der Teil ergänzt SEO um Suchmaschinen außer Google (Bing, DuckDuckGo, Apple, Brave, Yandex); eine Sperre für Google und Seznam wird im SEO gewertet.

14

ERGEBNISSE

Befunde nach Schweregrad

● HOCH · 8 BEFUNDE

Bilder ohne Alternativtext

● HOCH

`accessibility.axe.image-alt`**WAS DAS FÜR SIE
BEDEUTET****Bilder haben keine Textbeschreibung.****NACHWEIS**

Der automatische Barrierefreiheitstest (axe-core) hat auf der Startseite 1 Element mit diesem Problem gefunden.

AUSWIRKUNG

Blinde Nutzer erfahren nicht, was das Bild vermittelt (Produkt, Schema, Kontakt).

EMPFEHLUNG

Einen beschreibenden alt-Text ergänzen; rein dekorative Bilder mit alt="" kennzeichnen. WCAG 1.1.1.

Formularfelder ohne Beschriftung

● HOCH

`accessibility.axe.label`**WAS DAS FÜR SIE
BEDEUTET****Formularfelder haben keine Beschriftung.****NACHWEIS**

Der automatische Barrierefreiheitstest (axe-core) hat auf der Startseite 1 Element mit diesem Problem gefunden.

AUSWIRKUNG

Ohne Beschriftung wissen Screenreader-Nutzer nicht, was sie in das Feld eintragen sollen — das Formular wird zur Barriere.

EMPFEHLUNG

Das Feld mit <label for> verknüpfen oder aria-label ergänzen. WCAG 1.3.1 / 4.1.2.

WordPress hat wahrscheinlich die Sicherheitsupdates nicht installiert

● HOCH

`cms.outdated_core`**WAS DAS FÜR SIE
BEDEUTET****WordPress hat wahrscheinlich die Sicherheitsupdates nicht installiert.****NACHWEIS**

Die Startseite nennt WordPress 6.2 (Quelle: meta generator). Für diesen Zweig ist die Korrektur 6.2.13 erschienen, die den Fehler CVE-2026-87902 behebt; die US-Behörde CISA führt ihn als tatsächlich ausgenutzt.

AUSWIRKUNG

In neueren Versionen behobene Fehler sind öffentlich beschrieben und Bots suchen automatisch danach. Die Versionsnummer ist eine Schätzung aus öffentlichen Spuren; den tatsächlichen Stand prüft der Website-Administrator.

EMPFEHLUNG

WordPress vom Administrator auf die neueste Version aktualisieren und automatische Updates einschalten lassen. Wurde lange nicht aktualisiert, prüfen lassen, ob die Website missbraucht wurde.

Tracking-Cookies vor der Einwilligung gespeichert

 HOCH`cookies.pre_consent_tracking_cookie`

WAS DAS FÜR SIE BEDEUTET

Die Besuchermessung läuft schon vor der Einwilligung.

NACHWEIS

Im Browser wurden ohne jede Interaktion Tracking-Cookies gesetzt: `_ga` (.example.com, Laufzeit: 2 J.)

AUSWIRKUNG

Analyse- und Werbe-Cookies dürfen erst nach der Einwilligung des Besuchers gesetzt werden (§ 89 Abs. 3 des tschechischen Gesetzes über elektronische Kommunikation). Hier wurden sie früher gesetzt. Es handelt sich um eine technische Messung der Startseite, nicht um ein Rechtsgutachten.

EMPFEHLUNG

Nicht technisch notwendige Cookies bis zu einer nachweisbaren Opt-in-Einwilligung blockieren.

Tracking-Dienste wurden ohne Einwilligungsverwaltung ausgeführt

 HOCH`cookies.third_party_trackers_no_cmp`

WAS DAS FÜR SIE BEDEUTET

Die Website trackt Besucher ohne Möglichkeit zur Einwilligung.

NACHWEIS

Geladene Dienste ohne erkannte CMP: Google Analytics (www.google-analytics.com); 1 Google-Ping ohne Consent-Mode-Parameter (`gcs/gcd`)

AUSWIRKUNG

Analyse- und WerbETOOLS dürfen erst nach der Einwilligung des Besuchers laufen (§ 89 Abs. 3 des tschechischen Gesetzes über elektronische Kommunikation). Hier haben sie bereits vorher Daten gesendet. Es handelt sich um eine technische Messung der Startseite, nicht um ein Rechtsgutachten. Die Website fragt dabei gar nicht nach einer Einwilligung (wir haben weder ein Banner noch ein CMP gefunden).

EMPFEHLUNG

Eine CMP im Blockiermodus einsetzen und Tracker erst nach der Einwilligung ausführen.

Langsames Laden des Hauptinhalts (LCP)

 HOCH`performance.lcp_poor`

WAS DAS FÜR SIE BEDEUTET

Langsames Laden kann Anfragen von Mobilgeräten kosten.

NACHWEIS

LCP 4,1 s (Lighthouse-Labor, mobil, Median aus 3 Durchläufen); Schwelle für „gut“ $\leq 2,5$ s

AUSWIRKUNG

Langsames Laden kann mobile Besucher abschrecken. Google wertet Geschwindigkeit als eines von vielen Signalen; Vorrang hat der Inhalt.

EMPFEHLUNG

Das Hauptbild oder den Hauptblock beschleunigen (Größe, Format, vorrangiges Laden), die Serverantwortzeit verkürzen und blockierendes JS/CSS reduzieren.

Content-Security-Policy fehlt

 HOCH`sec_headers.missing_csp`

WAS DAS FÜR SIE
BEDEUTET

Die Website legt nicht fest, von wo der Browser Skripte ausführen darf.

NACHWEIS

Der Header Content-Security-Policy ist nicht vorhanden.

AUSWIRKUNG

Ohne CSP hat der Browser keine Abwehr gegen eingeschleuste Skripte (XSS) und Dateninjektionen.

EMPFEHLUNG

Content-Security-Policy mit explizitem `script-src` (Nonce/Hash) einführen.

Die Seite kann in fremde Websites eingebettet werden

 HOCH`sec_headers.missing_frame_protection`

WAS DAS FÜR SIE
BEDEUTET

Die Seite kann in fremde Websites eingebettet werden.

NACHWEIS

Sowohl X-Frame-Options als auch CSP `frame-ancestors` fehlen.

AUSWIRKUNG

Eine fremde Seite kann Ihre Website in einem unsichtbaren Rahmen anzeigen, und Besucher klicken womöglich auf etwas anderes, als sie denken.

EMPFEHLUNG

In der CSP `frame-ancestors` `'self'` setzen (oder die eigenen Domains aufzählen), alternativ X-Frame-Options: SAMEORIGIN.

 MITTEL · 6 BEFUNDE

Wahrscheinlich nicht mehr unterstützte Version der Serversoftware

 MITTEL`cms.eol_runtime`

WAS DAS FÜR SIE
BEDEUTET

Der Server läuft wahrscheinlich mit Software ohne Sicherheitsupdates.

NACHWEIS

nginx 1.18.0 (der Support für den Zweig 1.18 endete am 2021-04-20; Header Server); PHP 7.4.3 (der Support für den Zweig 7.4 endete am 2022-11-28; Header X-Powered-By).

AUSWIRKUNG

Ein Zweig erhält nach dem Ende des Supports von den Autoren keine Sicherheitsupdates mehr. Es handelt sich um einen wahrscheinlichen Zustand: Die Version im Header muss nicht der Realität entsprechen, weil Hoster und Distributionen Korrekturen zurückportieren, und eine passive Prüfung kann das nicht verifizieren.

EMPFEHLUNG

Beim Hoster die tatsächliche Version prüfen und auf einen unterstützten Zweig wechseln; zugleich die genauen Versionen in den Headern Server und X-Powered-By nicht mehr veröffentlichen.

Cookies ohne Sicherheitsattribute

 MITTEL`sec_headers.cookie_attributes`

WAS DAS FÜR SIE
BEDEUTET

Die Cookies der Website haben nicht alle Schutzattribute.

NACHWEIS

Die Startseite setzt 1 Cookie ohne empfohlene Attribute: PHPSESSID (fehlt: Secure, HttpOnly, SameSite).

AUSWIRKUNG

Ein Cookie ohne Secure kann unverschlüsselt übertragen werden, ein Sitzungscookie ohne HttpOnly kann von einem Skript auf der Seite gelesen werden, und ohne SameSite wird das Cookie auch bei Anfragen von fremden Websites mitgesendet.

EMPFEHLUNG

Für Cookies die Attribute Secure und SameSite (Lax oder Strict) setzen, für Sitzungs- und Anmelde-Cookies zusätzlich HttpOnly.

Beim Teilen erscheinen weder Bild noch treffender Titel

 MITTEL`seo.missing_open_graph`

WAS DAS FÜR SIE
BEDEUTET

Beim Teilen erscheinen weder Bild noch treffender Titel.

NACHWEIS

Die Seite hat keine Open-Graph-Tags (og:title, og:image, og:type, og:url).

AUSWIRKUNG

Ein Link auf Facebook, LinkedIn oder in Nachrichten wirkt leer.

EMPFEHLUNG

og:title, og:image (mindestens 1200 × 630 px), og:type und og:url ergänzen.

2 von 2 Unterseiten haben keinen Titel

 MITTEL`seo.subpages_missing_title`

WAS DAS FÜR SIE
BEDEUTET

Unterseiten haben keinen Titel.

NACHWEIS

Betrifft: <https://example.com/kontakt>, <https://example.com/produkt/vrtacka>.

AUSWIRKUNG

Ohne Titel wählt die Suchmaschine den Linktext selbst, oft unpassend. Die Seite ist in den Ergebnissen schwerer erkennbar und wird seltener angeklickt.

EMPFEHLUNG

Jeder Unterseite einen eigenen Titel passend zu ihrem Inhalt geben.

2 von 2 Unterseiten haben keine Beschreibung für Suchmaschinen

 MITTEL`seo.subpages_missing_description`

WAS DAS FÜR SIE
BEDEUTET

Unterseiten haben keine Beschreibung für Suchmaschinen.

NACHWEIS

Betrifft: <https://example.com/kontakt>, <https://example.com/produkt/vrtacka>.

AUSWIRKUNG

Google zeigt dann unter dem Link einen zufälligen Textauszug.

EMPFEHLUNG

Für jede Hauptseite einen eigenen Satz schreiben, was der Kunde dort findet.

Server unterstützt veraltete Versionen TLS 1.0/1.1

 MITTEL

tls.legacy_protocols

WAS DAS FÜR SIE
BEDEUTET**Die Website akzeptiert veraltete verschlüsselte Verbindungen.**

NACHWEIS

Der Server hat auch mit TLS 1.0 eine Verbindung aufgebaut.

AUSWIRKUNG

TLS 1.0 und 1.1 sind seit 2021 veraltet (RFC 8996) und bieten schwächeren Schutz; aktuelle Browser benötigen sie nicht, aktiviert vergrößern sie nur den Spielraum für schwächere Verbindungen.

EMPFEHLUNG

TLS 1.0 und TLS 1.1 deaktivieren, TLS 1.2 und TLS 1.3 beibehalten.

NIEDRIG · 15 BEFUNDE

Empfehlungen zu Befunden mit niedriger Schwere und informativen Befunden stehen im Aktionsplan, die vollständige Beschreibung jedes Befunds in der HTML-Version des Berichts.

Die Website verrät die genaue Softwareversion	cms.version_disclosure	 NIEDRIG
Veraltete JavaScript-Bibliotheken auf der Website	cms.outdated_js_library	 NIEDRIG
DNSSEC ist nicht aktiv	dns.no_dnssec	 NIEDRIG
Website ist nicht über IPv6 erreichbar	dns.no_ipv6_web	 NIEDRIG
Mailserver ist nicht über IPv6 erreichbar	dns.no_ipv6_mail	 NIEDRIG
Nameserver befinden sich in einem einzigen Netz	dns.nameservers_same_network	 NIEDRIG
Unterdurchschnittliche Blockierzeit des Hauptthreads (TBT)	performance.tbt_average	 NIEDRIG
Der Server antwortet langsamer als empfohlen	performance.server_average	 NIEDRIG
Die Startseite verlinkt auf nicht funktionierende Websites	search.broken_outbound_links	 NIEDRIG
Header verraten die Softwareversion	sec_headers.version_leak	 NIEDRIG
HTML der Seite wird ohne Komprimierung gesendet	sec_headers.no_compression	 NIEDRIG
Die Beschreibung für Suchmaschinen sagt nichts aus	seo.weak_description	 NIEDRIG
Einem Teil der Bilder fehlt alt	seo.alt_coverage_partial	 NIEDRIG
Defekte interne Links auf der Startseite	seo.broken_links	 NIEDRIG
Bilder oder Videos haben eine http://-Adresse	tls.mixed_content_passive	 NIEDRIG

INFO · 11 BEFUNDE

Die Produktdaten nennen keine Verfügbarkeit	business.product_data_tips	 INFO
Strukturierte Daten zum Unternehmen lassen sich um Registerangaben ergänzen	business.org_identity_tips	 INFO
DANE für den Mailserver ist nicht eingerichtet	email.dane_mx_missing	 INFO

BIMI fehlt — Firmenlogo im Posteingang	email.bimi_missing	● INFO
Unterdurchschnittlicher Leistungsscore im Labortest	performance.lighthouse_average	● INFO
Die Website hat keine eigene Regel für die Weitergabe der Seitenadresse	sec_headers.missing_referrer_policy	● INFO
Permissions-Policy fehlt	sec_headers.missing_permissions_policy	● INFO
Datei security.txt fehlt	sec_headers.missing_security_txt	● INFO
Link auf das Website-Symbol (Favicon) fehlt	seo.missing_favicon	● INFO
Zertifikat hat keine eingebetteten Certificate-Transparency-Einträge	tls.no_embedded_sct	● INFO
Server liefert kein OCSP-Stapling	tls.no_ocsp_stapling	● INFO

01

02

03

04

05

06

07

08

09

10

11

12

13

14

15

16

17

18

15

AKTIONSPLAN

Aktionsplan (nach Priorität)

PRIORITÄT	BEREICH	EMPFOHLENER SCHRITT
 HOCH	Barrierefreiheit	Einen beschreibenden alt-Text ergänzen; rein dekorative Bilder mit alt="" kennzeichnen. WCAG 1.1.1.
 HOCH	Barrierefreiheit	Das Feld mit <label for> verknüpfen oder aria-label ergänzen. WCAG 1.3.1 / 4.1.2.
 HOCH	CMS / Technologie	WordPress vom Administrator auf die neueste Version aktualisieren und automatische Updates einschalten lassen. Wurde lange nicht aktualisiert, prüfen lassen, ob die Website missbraucht wurde.
 HOCH	Cookies / DSGVO	Nicht technisch notwendige Cookies bis zu einer nachweisbaren Opt-in-Einwilligung blockieren.
 HOCH	Cookies / DSGVO	Eine CMP im Blockiermodus einsetzen und Tracker erst nach der Einwilligung ausführen.
 HOCH	Leistung (Core Web Vitals)	Das Hauptbild oder den Hauptblock beschleunigen (Größe, Format, vorrangiges Laden), die Serverantwortzeit verkürzen und blockierendes JS/CSS reduzieren.
 HOCH	Sicherheits-Header	Content-Security-Policy mit explizitem script-src (Nonce/Hash) einführen.
 HOCH	Sicherheits-Header	In der CSP frame-ancestors 'self' setzen (oder die eigenen Domains aufzählen), alternativ X-Frame-Options: SAMEORIGIN.
 MITTEL	CMS / Technologie	Beim Hoster die tatsächliche Version prüfen und auf einen unterstützten Zweig wechseln; zugleich die genauen Versionen in den Headern Server und X-Powered-By nicht mehr veröffentlichen.
 MITTEL	Sicherheits-Header	Für Cookies die Attribute Secure und SameSite (Lax oder Strict) setzen, für Sitzungs- und Anmelde-Cookies zusätzlich HttpOnly.
 MITTEL	SEO	og:title, og:image (mindestens 1200 × 630 px), og:type und og:url ergänzen.
 MITTEL	SEO	Jeder Unterseite einen eigenen Titel passend zu ihrem Inhalt geben.
 MITTEL	SEO	Für jede Hauptseite einen eigenen Satz schreiben, was der Kunde dort findet.
 MITTEL	TLS / Zertifikat	TLS 1.0 und TLS 1.1 deaktivieren, TLS 1.2 und TLS 1.3 beibehalten.
 NIEDRIG	CMS / Technologie	Software aktuell halten; die Version lässt sich verbergen, das ersetzt aber kein Update.
 NIEDRIG	CMS / Technologie	Die genannten Bibliotheken aktualisieren (bei WordPress durch Aktualisierung von Core, Theme und Plugins) und die Funktion der Website prüfen; Bibliotheken mit eingestellter Entwicklung (AngularJS, Moment.js) schrittweise durch gepflegte Alternativen ersetzen.
 NIEDRIG	DNS & Infrastruktur	DNSSEC beim DNS-Anbieter aktivieren und den DS-Eintrag vom Registrar eintragen lassen. Die meisten Registries (einschließlich .cz, .eu und .com) unterstützen DNSSEC.
 NIEDRIG	DNS & Infrastruktur	Beim Hosting-Anbieter eine IPv6-Adresse anfordern und einen AAAA-Eintrag veröffentlichen (für die Domain ohne www und für www).

PRIORITÄT	BEREICH	EMPFOHLENER SCHRITT
● NIEDRIG	DNS & Infrastruktur	Beim E-Mail-Anbieter die IPv6-Unterstützung prüfen und AAAA-Einträge für die MX-Hosts veröffentlichen.
● NIEDRIG	DNS & Infrastruktur	Mindestens einen Nameserver in ein anderes Netz verlegen (anderes /24 bei IPv4, anderes /48 bei IPv6), z. B. sekundäres DNS bei einem anderen Anbieter.
● NIEDRIG	Leistung (Core Web Vitals)	Die Ausführung von JavaScript im Hauptthread optimieren.
● NIEDRIG	Leistung (Core Web Vitals)	Seiten-Caching einschalten oder schnelleres Hosting erwägen.
● NIEDRIG	Suchmaschinen (außer Google)	Die Links korrigieren oder entfernen.
● NIEDRIG	Sicherheits-Header	Vor allem die Software aktuell halten; das Ausblenden der Version in den Headern Server und X-Powered-By ist erst der zweite Schritt.
● NIEDRIG	Sicherheits-Header	Auf dem Server oder CDN die Komprimierung mit gzip oder Brotli für HTML, CSS, JS und SVG aktivieren.
● NIEDRIG	SEO	Ein bis zwei Sätze darüber schreiben, was die Firma anbietet, für wen und wo.
● NIEDRIG	SEO	alt bei den übrigen Bildern ergänzen.
● NIEDRIG	SEO	Links auf nicht existierende Seiten korrigieren oder entfernen; aufgegebene Adressen dauerhaft (HTTP 301) auf neue Inhalte weiterleiten.
● NIEDRIG	TLS / Zertifikat	Die Adressen auf https:// ändern (oder relative Adressen verwenden).

16

WIE WIR MESSEN

Methodik und Grenzen

Methodik: Ausgewertet werden ausschließlich öffentlich zugängliche, passive Signale — DNS über DoH, öffentliche HTTP-Header und HTML (wie ein gewöhnlicher Browser), TLS-Handshake, öffentliche APIs (PageSpeed Insights, CT-Logs, RDAP) sowie `robots.txt` / `sitemap.xml`. Das entspricht derselben Kategorie wie `securityheaders.com`, Mozilla Observatory oder Google PageSpeed.

Bewertungsversion 3.0.0: Gewichte der Bereiche, Punkte je Schweregrad und Notenbereiche bleiben gleich; neu haben einige Bereiche eine Obergrenze der Punktzahl, und SEO wird aus Säulen berechnet. Punktzahlen aus Versionen 2.x lassen sich damit nicht direkt vergleichen.

Verwendet die Website wahrscheinlich Software ohne Sicherheitsupdates, kann der Bereich nicht grün sein. Obergrenzen der Bereiche: E-Mail ohne angewendete DMARC-Richtlinie erhält höchstens 74 Punkte, und die informativen Bereiche KI und Suchmaschinen mit einem Befund hoher Schwere ebenfalls höchstens 74; bei einem begrenzten Bereich steht das in der Punktetabelle.

SEO ist die Summe aus sechs Säulen (Indexierung 25, Titel und Beschreibungen 25, Inhalt 15, strukturierte Daten 15, Teilen 10, Technik 10 Punkte), nach dem Anteil der bewerteten Inhaltsseiten; SEO-Befunde erklären, ziehen aber keine Punkte ab. Schwellen begrenzen die Punktzahl: wenn Suchmaschinen die Startseite nicht anzeigen dürfen (höchstens 20) oder wenn den meisten Seiten eigene Titel und Beschreibungen fehlen (höchstens 59; nur eines davon höchstens 74).

Der Browser misst aus der EU mit tschechischen Einstellungen (Sprache cs-CZ, Zeitzone Europe/Prague) und klickt nie auf das Cookie-Banner.

Gemessen mit axe-core Version 4.13.0 in der Ansicht 1366 × 900.

Subdomains stammen aus öffentlichen Zertifikatslogs (`crt.sh`, ersatzweise Cert Spotter). Bei der Schnittstelle `crt.sh` wendet WebMeter deren `robots.txt` bewusst nicht an, weil dieselbe Liste jeder abrufen kann; es sendet eine Abfrage pro Scan und speichert das Ergebnis für eine Weile.

Grenzen: Das Tool probiert weder Anmeldungen noch Passwörter aus, testet keine Schwachstellen, sendet keine Payloads und umgeht keine Schutzmaßnahmen. Das Vorhandensein einer Anmeldeseite wird lediglich erkannt. Die Ergebnisse sind *Indikatoren und Schätzungen* aus öffentlichen Spuren — kein offizielles Gutachten und keine vertragliche Garantie. Die Version des TLS-Protokolls wird aus dieser Laufzeitumgebung nicht als Tatsache angegeben, sofern sie nicht zuverlässig überprüfbar ist.

Automatische Empfehlungen (zum Beispiel, ob sich eine Reparatur oder eine neue Website lohnt) sind eine grobe Schätzung; den konkreten Umfang und Preis legt erst eine Beratung fest.

17

FÜR TECHNIKER

Anhang: technische Details

Maschinelle Kennungen der Befunde und Status der einzelnen Messungen — für Techniker, die die Behebung umsetzen.

MESSSTATUS DER BEREICHE

BEREICH	ID	STATUS	HINWEIS
Sicherheits-Header	security_headers	gemessen	—
E-Mail-Authentifizierung	email_auth	gemessen	—
TLS / Zertifikat	tls_cert	gemessen	—
DNS & Infrastruktur	dns_infra	teilweise gemessen	RPKI (RIPEstat) nicht erreichbar — Status der Route zur Website nicht geprüft.
Cookies / DSGVO	cookies_gdpr	gemessen	—
Leistung (Core Web Vitals)	performance	gemessen	—
SEO	seo	gemessen	—
Barrierefreiheit	accessibility	gemessen	—
CMS / Technologie	cms_tech	gemessen	—
Exponierte Inhalte	exposure	teilweise gemessen	CT-Logs (crt.sh) nicht erreichbar — Subdomains ausgelassen.
KI-Suchmaschinen	ai_visibility	gemessen	—
Unternehmen & Onlineshop	business	teilweise gemessen	Die Startseite hat im HTML wenig Text (wird vermutlich per JavaScript gerendert) — fehlende Angaben melden wir nicht
Suchmaschinen (außer Google)	search_visibility	gemessen	—

Das kann *Ihr Website-Administrator* beheben.

Schicken Sie ihm den Bericht — bei jedem Befund steht, was zu tun ist. Wenn Sie statt Reparaturen lieber eine komplett neue Website möchten, baue ich sie.

Beratung zu einer neuen Website vereinbaren →

BETREIBER DES TOOLS UND VERANTWORTLICHER FÜR DIE DATEN

Angaben in den Datenschutzhinweisen von WebMeter:
webmeter.eu/de/datenschutz#spravce · Kontakt
kontakt@webmeter.eu

Dieser Bericht entstand auf Anfrage durch eine passive Prüfung öffentlich zugänglicher Informationen über die Website. Prüfergebnis und Bericht werden höchstens 365 Tage gespeichert, das PDF 30 Tage; danach werden sie gelöscht. Einzelheiten zur Datenverarbeitung und zu Ihren Rechten finden Sie unter webmeter.eu/de/datenschutz.

SPEICHERUNG UND LÖSCHUNG

Die Löschung gespeicherter Scan-Ergebnisse und den Ausschluss der Domain von weiteren Analysen können Sie per E-Mail an kontakt@webmeter.eu beantragen. Der Website-Administrator kann die Analyse auch in der `robots.txt` untersagen:

User-agent: WebMeterBot
Disallow: /

Zeitstempel des Scans: 24.09.2026 12:00 UTC · Scoring-Version 3.0.0. Der Bericht ist eine informative Übersicht auf Grundlage öffentlich zugänglicher Signale.