WebAuditPlus ist ein Dienst von Belitum BV

Cybersicherheit-Auditbericht für Ihre Website

Firmenname: Conson

Website: https://www.conson.com/de

WebAuditPlus-ID: WAPL-1830-7458-5491-3391

WebAuditPlus-Version: 1.0.1

Erstellt am: 2026-07-22

Inhaltsverzeichnis

Einleitung

Dieser Bericht bietet eine unabhängige Analyse Ihrer Website mit Fokus auf sichtbare Risiken, Verbesserungspotenziale und die allgemeine Qualität.

Er ist so gestaltet, dass er sowohl für technische als auch für nicht-technische Leser verständlich ist.

Was Ihnen dieser Bericht verständlich macht

- Ob Ihre Website sichtbare Cybersecurity- oder Datenschutzrisiken aufweist

- Ob dies Ihre Sichtbarkeit, das Vertrauen oder Ihre Geschäftsergebnisse beeinträchtigen kann

- Was in Bezug auf Leistung, SEO und technische Qualität verbessert werden kann

- Wie Ihre Website von Nutzern und KI-Systemen wahrgenommen werden kann

- Welche Maßnahmen und Empfehlungen helfen können, diese Risiken zu verringern oder zu mindern

Wie dieser Bericht zu verwenden ist

Sie müssen nicht alles im Detail lesen.

Wir empfehlen, mit dem Abschnitt Zusammenfassung zu beginnen, der die wichtigsten Feststellungen und Prioritäten hervorhebt.

Jeder Abschnitt des Berichts enthält:

- eine klare Beschreibung des Problems

- praktische Empfehlungen und vorgeschlagene Maßnahmen

Sie können sich je nach Bedarf auf die relevantesten Bereiche konzentrieren.

Wichtiger Hinweis

Für diesen Bericht ist kein technischer Zugriff auf Ihre Website erforderlich.

Er basiert auf öffentlich zugänglichen Informationen und sichtbaren Indikatoren.

Benötigen Sie Hilfe, um diesen Bericht zu verstehen oder danach zu handeln?

Wir können Sie bei diesem Bericht und seinen Empfehlungen unterstützen, indem Sie uns über info@webauditplus.com kontaktieren.

Zusammenfassung

Dieser Abschnitt bietet eine Zusammenfassung der wichtigsten Risiken und Prioritäten. Er hilft Ihnen, die aktuelle Cybersicherheitslage der Website zu verstehen und zu erkennen, wo Behebungsmaßnahmen zuerst beginnen sollten.

Metrisch	Wert
Gesamtrisikoniveau	Hoch
Gesamtpunktzahl (0-100)	65
Grad	D
Gesamtabzug	180.46
Verteilung der Befunde	Kritisch 0 | Hoch 1 | Mittel 19 | Niedrig 11 | Info 16

Der Score (0-100) spiegelt das Gesamtrisiko und die Qualität der Website wider. Der Abzug ist die gesamte Score-Reduktion durch Feststellungen. Die Note ist die Score-Klasse (A ist am besten).

Top 10 Prioritäten

Hinweis: Die Top-10-Prioritäten basieren ausschließlich auf verifizierten Befunden (validierten Nachweisen), nicht auf Annahmen.

Schwere	Module	Beschreibung
Hoch	Tracking-Indikatoren	Es wurden tracking-technologien erkannt, aber auf der homepage wurde kein einwilligungs-/cmp-signal gefunden (heuristik) stellen sie sicher, dass einwilligungsmanagement und offenlegungen bei bedarf implementiert werden
Mittel	HTTP-Sicherheitsheader	Content-Security-Policy fehlt (eine CSP hilft, XSS- und dateninjektionsrisiken zu reduzieren)
Mittel	Bildressourcen	4 einzelne bilder überschreiten 500 kb, was die ladezeiten der seite verlangsamen kann
Mittel	Sitemaps und robots.txt	Es wurde keine erreichbare sitemap gefunden (robots txt-sitemap-zeilen oder /sitemap xml)
Mittel	KI-Wahrnehmungsanalyse	Verwirrung um die Produktverfügbarkeit
Mittel	KI-Wahrnehmungsanalyse	Barriere der technischen Komplexität
Mittel	KI-Wahrnehmungsanalyse	Installationsabhängigkeit unklar
Mittel	KI-Wahrnehmungsanalyse	Mögliche Verwirrung bezüglich der Produktkompatibilität.
Mittel	KI-Wahrnehmungsanalyse	Unsicherheit bezüglich der Installationsanforderungen.
Mittel	KI-Wahrnehmungsanalyse	Unklare Produktmerkmale.

Größter Score-Einfluss (Module)

Modul	Kategorie	Abzug	Feststellungen
KI-Wahrnehmungsanalyse	KI	94.5	14
HTTP-Sicherheitsheader	Sicherheit	25.02	6
Tracking-Indikatoren	Datenschutz	17.32	2
Bildressourcen	Leistung	11.88	4
Sitemaps und robots.txt	SEO	9.5	2
Link-Gesundheit	SEO	9.0	2
Grundlagen der Barrierefreiheit	Barrierefreiheit	5.74	1
Formulare	Datenschutz	2.75	2
Erweiterte SEO-Analyse	SEO	2.5	2
JavaScript-Indikatoren	Leistung	2.25	3

Einhaltung der DSGVO und des Datenschutzes	Compliance	0.0	0
ISO 27001-Indikatoren	Compliance	0.0	1

KI-Wahrnehmungsanalyse

In diesem Abschnitt wird analysiert, wie die Website von modernen KI-Systemen und großen Sprachmodellen auf Basis öffentlich zugänglicher Informationen wahrgenommen werden könnte.

KI-Systeme dienen zunehmend als erste Informationsquelle. Sind Ihre Inhalte vage oder widersprüchlich, können KI-Antworten Ihr Unternehmen falsch darstellen oder wichtige Angebote außer Acht lassen.

Ergebnisse pro Modell (was die KI von Ihrer Website versteht)

Modell	Was sie denken, was du tust	Für wen	Erwähnte Dienstleistungen	Klarheit (0-100)
openai/gpt-4o-mini	Conson bietet Produkte für die Haus- und Gebäude automation an.	Für Hausbesitzer und Baufachleute, die Automatisierungslösungen suchen.	Produkte zur Steuerung und Überwachung von Beleuchtung, Bildschirmen, Thermostaten und mehr über verschiedene Geräte	85
google/gemini-3-flash-preview	Conson produziert und liefert Hardware- und Softwaremodule für die Haus- und Gebäudeautomation und ist spezialisiert auf dezentrale Steuerungssysteme für Beleuchtung, Heizung und Rollläden.	Elektroinstallateure, Ingenieurbüros und Immobilieneigentümer, die nach zuverlässigen, rückwärtskompatiblen Smart-Building-Lösungen suchen.	Bereitstellung von Automatisierungshardware (Relais, Dimmer, Gateways), kostenloser Konfigurationssoftware (Contool), Fernverwaltungssystemen (Consonbox) und technischer Dokumentation für Altsysteme	88
x-AI/grok-4.3	Hersteller von Hardware und Software für die modulare Haus- und Gebäudeautomation, insbesondere für Beleuchtung, Jalousien, Thermostate und zugehörige Steuerungen.	Hausbesitzer, Gebäudeeigentümer, Elektriker/Installateure und Ingenieurbüros	Dezentrale Automatisierungsmodule (XP-Serie), Netzteile, Gateways, Dimmer, Konfigurationssoftware (Contool), Fernverwaltung über Consonbox	82
anthropic/claude-sonnet-4	Produziert und vertreibt Produkte für die Haus- und Gebäudeautomation, darunter intelligente Module, Dimmer, Relaismodule, Netzteile und Managementsysteme zur Steuerung von Beleuchtung, Jalousien, Thermostaten und anderen Gebäudesystemen.	Hausbesitzer, Gebäudebesitzer, Elektroinstallateure, Ingenieurbüros und Händler, die nach kostengünstigen Lösungen für die Haus- und Gebäudeautomation suchen	Haus- und Gebäudeautomatisierungsprodukte mit kostenloser Konfigurationssoftware (Contool), internetbasiertem Managementsystem (Consonbox mit CONLINX-Software), technischer Dokumentation und Händlernetzwerk-Support	85

Modellübergreifende Konsistenz

häufigste Kernaktivität	Produziert und vertreibt Produkte für die Haus- und Gebäudeautomation, darunter intelligente Module, Dimmer, Relaismodule, Netzteile und Managementsysteme zur Steuerung von Beleuchtung, Jalousien, Thermostaten und anderen Gebäudesystemen.
Häufigstes Publikum	Hausbesitzer, Gebäudebesitzer, Elektroinstallateure, Ingenieurbüros und Händler, die nach kostengünstigen Lösungen für die Haus- und Gebäudeautomation suchen

Gängigste Angebote	Haus- und Gebäudeautomatisierungsprodukte mit kostenloser Konfigurationssoftware (Contool), internetbasiertem Managementsystem (Consonbox mit CONLINX-Software), technischer Dokumentation und Händlernetzwerk-Support
Konsistenzniveau	niedrig

Risiken und Behebung von Fehlinterpretationen von KI-Systemen (aus Modellausgaben)

Modell	Risiko	Lösungsvorschlag
anthropic/claude-sonnet-4	Verwirrung um die Produktverfügbarkeit	Erstellen Sie eine übersichtliche Produktlebenszyklusseite und präsentieren Sie auf den Hauptseiten ausschließlich die aktuellen Produkte der XP-Serie.
anthropic/claude-sonnet-4	Barriere der technischen Komplexität	Ergänzen Sie die technischen Spezifikationen um einfache, nutzenorientierte Beschreibungen.
anthropic/claude-sonnet-4	Installationsabhängigkeit unklar	Klären Sie, welche Produkte für die Selbstmontage geeignet sind und welche eine professionelle Installation erfordern.
openai/gpt-4o-mini	Mögliche Verwirrung bezüglich der Produktkompatibilität.	Geben Sie konkretere Beispiele für kompatible Produkte an.
openai/gpt-4o-mini	Unsicherheit bezüglich der Installationsanforderungen.	Klären Sie, ob die Produkte selbst installiert werden können oder ob ein Fachmann erforderlich ist.
openai/gpt-4o-mini	Unklare Produktmerkmale.	Die Sprache vereinfachen und benutzerfreundliche Erklärungen bereitstellen.
openai/gpt-4o-mini	Mangelnde Informationen über Unterstützungsangebote.	Fügen Sie einen separaten Supportbereich mit Kontaktinformationen hinzu.
google/gemini-3-flash-preview	Endnutzer könnten versuchen, direkt zu kaufen.	Geben Sie klar an, ob es sich um einen B2B-Hersteller handelt oder ob sie direkt an Endverbraucher verkaufen.
google/gemini-3-flash-preview	Verwirrung bezüglich der Produktverfügbarkeit.	Verwenden Sie einen übersichtlicheren visuellen Abschnitt „Legacy vs. Current", um aktive Produkte von Artikeln zu trennen, die nur noch Support erhalten.
google/gemini-3-flash-preview	Sprachmischung in lokalisierten Versionen.	Überprüfen Sie die lokalisierten Seiten, um eine einheitliche Übersetzung aller UI-Elemente und des Fließtextes sicherzustellen.

Erkenntnisse

✓ Verifizierter Befund

Schwere	Beschreibung	Empfehlung
Mittel ✓	Verwirrung um die Produktverfügbarkeit	Erstellen Sie eine übersichtliche Produktlebenszyklusseite und präsentieren Sie auf den Hauptseiten ausschließlich die aktuellen Produkte der XP-Serie.
Mittel ✓	Barriere der technischen Komplexität	Ergänzen Sie die technischen Spezifikationen um einfache, nutzenorientierte Beschreibungen.
Mittel ✓	Installationsabhängigkeit unklar	Klären Sie, welche Produkte für die Selbstmontage geeignet sind und welche eine professionelle Installation erfordern.
Mittel ✓	Mögliche Verwirrung bezüglich der Produktkompatibilität.	Geben Sie konkretere Beispiele für kompatible Produkte an.

Mittel ✓	Unsicherheit bezüglich der Installationsanforderungen.	Klären Sie, ob die Produkte selbst installiert werden können oder ob ein Fachmann erforderlich ist.
Mittel ✓	Unklare Produktmerkmale.	Die Sprache vereinfachen und benutzerfreundliche Erklärungen bereitstellen.
Mittel ✓	Mangelnde Informationen über Unterstützungsangebote.	Fügen Sie einen separaten Supportbereich mit Kontaktinformationen hinzu.
Mittel ✓	Missverständnis bezüglich des Begriffs „Consonbox".	Erklären Sie detailliert, was Consonbox ist und welche Vorteile es bietet.
Mittel ✓	Übersehene Produktaktualisierungen.	Produktaktualisierungen sollten prominent auf der Startseite hervorgehoben werden.
Mittel ✓	Endnutzer könnten versuchen, direkt zu kaufen.	Geben Sie klar an, ob es sich um einen B2B-Hersteller handelt oder ob sie direkt an Endverbraucher verkaufen.
Mittel ✓	Verwirrung bezüglich der Produktverfügbarkeit.	Verwenden Sie einen übersichtlicheren visuellen Abschnitt „Legacy vs. Current", um aktive Produkte von Artikeln zu trennen, die nur noch Support erhalten.
Mittel ✓	Sprachmischung in lokalisierten Versionen.	Überprüfen Sie die lokalisierten Seiten, um eine einheitliche Übersetzung aller UI-Elemente und des Fließtextes sicherzustellen.
Mittel ✓	Wahrnehmung als Komplettanbieter für Installationsdienstleistungen und nicht als Produktlieferant	Fügen Sie einen ausdrücklichen Hinweis hinzu, dass Conson lediglich Produkte liefert und keine Installationen durchführt.
Mittel ✓	Verwirrung zwischen älteren und aktuellen Produktlinien	Erstellen Sie eine separate Supportseite für ältere Systeme mit klaren Migrationshinweisen.

Crawl & Website-Überblick

Diese Tabelle zeigt, wie die gescannten Seiten während des Crawls geantwortet haben. Seiten mit 200-Codes wurden erfolgreich geladen, 300-Codes leiten zu einer anderen URL weiter, 400-Codes weisen auf Client-Fehler wie defekte oder nicht zugängliche Seiten hin, und 500-Codes weisen auf Server-Fehler hin, die technisch untersucht werden sollten.

Metrik	Wert
Gecrawlte Seiten	8
2xx (Erfolgreich)	8
3xx (Weiterleitung)	0
4xx (Clientfehler)	0
5xx (Serverfehler)	0
Defekte Seiten	0
Durchschnittliche Antwortzeit (ms)	1821

Technologie & CMS

Dieser Abschnitt liefert Best-Effort-Hinweise auf Plattformen auf Basis öffentlicher Signale und kann Fehlalarme enthalten.

Erkannte / mögliche Plattform: WordPress (Vertrauensniveau: mittel)

Signale beobachtet:

Der Beweis wird aus dem Markup öffentlicher Seiten (Meta-Tags, Skripte/Links und entdeckte Pfade) abgeleitet.

- Pfad: /wp-content/

- Pfad: /wp-includes/

- Pfad: /wp-json/

- Pfad: https://www.conson.com/wp-json/

- Datei: https://www.conson.com/wp-content/plugins/cookie-law-info/public/css/cookie-law-info-public.css?ver=1.8.9

- Datei: https://www.conson.com/wp-content/plugins/sitepress-multilingual-CMS/res/js/jquery.cookie.js?ver=4.3.16

- Datei: https://www.conson.com/wp-includes/css/dist/block-library/style.min.css

- Datei: https://www.conson.com/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp

KI-generierte kontextuelle Erkenntnisse

Die folgenden Erkenntnisse werden mithilfe von KI ausschließlich auf Basis verifizierter technischer Feststellungen aus diesem Modul erzeugt. Sie bieten eine kontextbezogene Interpretation und ersetzen weder eine formelle Sicherheitsbewertung noch eine Rechtsberatung.

Modell: anthropic/claude-sonnet-4

Bereich	Interpretation	Auswirkung
Plattform-Erkennung	WordPress mit mittlerem Vertrauensniveau identifiziert	Plattformspezifische Sicherheitsüberlegungen können zutreffen

Modell: x-ai/grok-4.3

Bereich	Interpretation	Auswirkung
CMS-Plattform	Primäre Plattform als WordPress mit mittlerem Vertrauen anerkannt.	Keine validierten Ausstellungen identifiziert.

Modell: google/gemini-3-flash-preview

Bereich	Interpretation	Auswirkung
Plattform- Identifizierung	WordPress wurde mit mittlerer Sicherheit als primäres Content-Management-System identifiziert.	Das Ökosystem ermöglicht eine umfassende Plugin-Integration, erfordert jedoch eine konsequente Wartung.
Sicherheitslücken	Während des Scans wurden keine validierten Schwachstellen oder aktive Sicherheitslücken festgestellt.	Die aktuelle CMS-Konfiguration weist keine unmittelbar bekannten Sicherheitsrisiken auf.

Erkenntnisse

✓ Verifizierter Befund

Schwere	Beschreibung	Empfehlung

Info	Über fingerprinting-signale erkannt (vertrauen: mittel)	Halten sie die plattform und plugins aktuell, minimieren sie öffentlich sichtbare versionsinformationen und prüfen sie härtungsleitfäden für diesen stack

Server- und Hosting-Indikatoren

In diesem Abschnitt werden beobachtbare Server-/Hosting-Signale aus HTTP-Antwortheadern zusammengefasst, z. B. CDN/WAF-Hinweise, Caching-Strategie, Komprimierung und HTTP/3-Ankündigung. Es basiert auf Heuristik und spiegelt möglicherweise nicht die gesamte Infrastruktur wider.

Metrisch	Wert
Endgültige URL	https://www.conson.com/de/
Server-Header	Apache
CDN/WAF-Kandidaten	Keine erkannt
Cache-Kontrolle	no-cache, no-store, must-revalidate
Inhaltskodierung	gzip
HTTP/3 angekündigt (Alt-Svc)	NEIN

Empfohlene Maßnahmen

Aktivieren Sie die Komprimierung (gzip/brotli) für Text-Assets, definieren Sie eine Caching-Strategie (Cache-Control) und ziehen Sie gegebenenfalls ein CDN/WAF in Betracht. Halten Sie die Infrastruktur in der Dokumentation transparent und stimmen Sie technische Kontrollen mit Sicherheitsanforderungen ab.

Erkenntnisse

✓ Verifizierter Befund

Schwere	Beschreibung	Empfehlung
Info	In den antwortheadern wurde kein klares CDN/WAF-signal erkannt (heuristik)	Prüfen Sie diese Feststellung und setzen Sie die passende Abhilfemaßnahme auf Grundlage des beschriebenen Problems um.

HTTP-Sicherheitsheader

HTTP-Antwortheader können die Sicherheit und den Datenschutz verbessern, indem sie gängige browserbasierte Angriffsvektoren (z. B. XSS, Clickjacking) reduzieren. In diesem Abschnitt wird die Homepage-Antwort auf häufig verwendete Sicherheitsheader überprüft.

Metrik	Wert / Status
Strict-Transport-Security	max-age=31536000; includeSubdomains;
Content-Security-Policy	Fehlt
X-Frame-Options	DENY
X-Content-Type-Options	nosniff
Referrer-Policy	no-referrer
Permissions-Policy	Fehlt
Cross-Origin-Opener-Policy	Fehlt
Cross-Origin-Embedder-Policy	Fehlt
Cross-Origin-Resource-Policy	Fehlt

Endgültige URL	https://www.conson.com/de/
Server	Apache
X-Powered-By	N / A
Cache-Kontrolle	no-cache, no-store, must-revalidate

Empfohlene Maßnahmen

Fügen Sie gegebenenfalls fehlende Sicherheitsheader hinzu. Beginnen Sie mit HTTPS + HSTS, implementieren Sie dann eine Content-Security-Policy und überprüfen Sie den Clickjacking- und MIME-sniffing-Schutz. Testen Sie Änderungen immer im Staging, da strenge Richtlinien die Funktionalität beeinträchtigen können.

Erkenntnisse

✓ Verifizierter Befund

Schwere	Beschreibung	Empfehlung
Mittel ✓	Content-Security-Policy fehlt (eine CSP hilft, XSS- und dateninjektionsrisiken zu reduzieren)	Erstellen sie eine Content-Security-Policy, um das risiko von XSS und dateninjektion zu reduzieren beginnen sie im report-only-modus, prüfen sie die verstöße und erzwingen sie die richtlinie nach erfolgreicher prüfung
Niedrig ✓	Permissions-Policy fehlt (browserfunktionen werden möglicherweise nicht auf das minimal erforderliche maß beschränkt)	Konfigurieren sie einen Permissions-Policy-header, damit sensible browserfunktionen wie kamera, mikrofon, geolokalisierung und zahlungen auf das beschränkt werden, was die website wirklich benötigt
Niedrig ✓	Cross-Origin-Opener-Policy fehlt (cross-origin-fensterinteraktionen werden möglicherweise weniger strikt eingeschränkt, wodurch bestimmte isolationsrisiken steigen)	Erwägen sie Cross-Origin-Opener-Policy, wo dies passend ist, um die cross-origin-isolation zu verbessern und risiken durch nicht vertrauenswürdige browsing-kontexte zu reduzieren
Niedrig ✓	Cross-Origin-Embedder-Policy fehlt (externe ressourcen werden möglicherweise weniger strikt isoliert, wodurch bestimmte cross-origin-datenleckri siken steigen)	Erwägen sie Cross-Origin-Embedder-Polic y, wenn die website eine starke cross-origin-isolation benötigt testen sie sorgfältig, da drittanbieterressourcen blockiert werden können

Niedrig ✓	Cross-Origin-Resource-Policy fehlt (externe websites können bestimmte ressourcen möglicherweise freier laden als vorgesehen)	Erwägen sie Cross-Origin-Resource-Policy für sensible ressourcen, um zu steuern, welche origins diese laden dürfen
Info	Der server header ist vorhanden	Minimieren oder entfernen sie nach möglichkeit detaillierte server-header-informationen, um technology fingerprinting zu begrenzen

TLS & Transportsicherheit

HTTPS (TLS) verschlüsselt den Datenverkehr zwischen Besuchern und der Website. In diesem Abschnitt werden die grundlegende HTTPS-Erreichbarkeit, die HTTP->HTTPS-Umleitung und die Zertifikateigenschaften (Ablauf, Aussteller, Protokoll) überprüft.

Metrisch	Wert
Endgültige URL	https://www.conson.com/de/
HTTPS-Status	200
HTTP -> HTTPS-Umleitung	Ja
TLS-Protokoll	TLSv1.3
Chiffre	TLS_AES_256_GCM_SHA384 (TLSv1.3)
Zertifikat gültig ab	2026-07-05T22:58:10Z
Zertifikat gültig bis	2026-10-03T22:58:09Z
Emittent	countryName=US, organizationName=Let's Encrypt, commonName=YR1

Empfehlung

Stellen Sie sicher, dass die Site immer über HTTPS mit einem gültigen Zertifikat bereitgestellt wird. Leiten Sie HTTP zu HTTPS um, lassen Sie die Zertifikate erneuert und bevorzugen Sie nur TLS 1.2/1.3. Erwägen Sie bei Hochsicherheitsstandorten die Absicherung von Verschlüsselungssammlungen und die Aktivierung von HSTS nach dem Testen.

Cookies und Sitzungssicherheit

Dieses Modul bewertet während des Crawls beobachtete Cookies und hebt Sicherheitsattribute (Secure, HttpOnly, SameSite), Lebensdauer, Drittanbieter-Nutzung und mögliche Tracking-Indikatoren hervor.

Metrisch	Wert
Beobachtete Cookies (einzigartig)	0
Cookies von Erstanbietern	0
Cookies von Drittanbietern (nach Domain)	0
Sitzungscookies	0
Dauerhafte Cookies	0
Langlebig (>= 365 Tage)	0
Mit Secure	0
Mit HttpOnly	0
Mit SameSite	0
Sicher fehlt	0
HttpOnly fehlt	0
SameSite fehlt	0
SameSite=Keine ohne Secure	0
Tracking-Cookie-Indikatoren	0
Max. beobachtete Lebensdauer (Tage)	0
Cookie-Sicherheitsbewertung (0-100)	100

Wie sind diese Ergebnisse zu interpretieren?

- Sichere Cookies werden bei der Übertragung geschützt, wenn HTTPS erzwungen wird.

- HttpOnly reduziert die Gefährdung durch clientseitigen Skriptzugriff während XSS.

- SameSite kann das CSRF-Risiko reduzieren;Verwenden Sie standardmäßig Lax und None+Secure nur bei Bedarf.

- Tracking-Cookies und Drittanbieter-Domains erfordern in der Regel eine sorgfältige Einwilligung und Dokumentation.

KI-generierte kontextuelle Erkenntnisse

Die folgenden Erkenntnisse werden mithilfe von KI ausschließlich auf Basis verifizierter technischer Feststellungen aus diesem Modul erzeugt. Sie bieten eine kontextbezogene Interpretation und ersetzen weder eine formelle Sicherheitsbewertung noch eine Rechtsberatung.

Modell: anthropic/claude-sonnet-4

Beobachtung	Interpretation	Geschäftsrisiko
Während des Sicherheitsaudits wurden keine Cookies erkannt	Die Website funktioniert ohne das Setzen von Cookies, wurde auf einen minimalen Datensammlungs ansatz hingewiesen	Niedrig - Keine Cookie-bezogenen Sicherheitslücken vorhanden

Modell: x-ai/grok-4.3

Beobachtung	Interpretation	Geschäftsrisiko
Es wurden keine Cookies erkannt.	Die Website verwendet keine Cookies, wodurch cookiebasierte Sicherheitsrisiken ausgeschlossen werden.	Kein damit verbundenes Geschäftsrisiko.

Modell: google/gemini-3-flash-preview

Beobachtung	Interpretation	Geschäftsrisiko
Beim Website-Crawling wurden keine Cookies erkannt.	Die Website arbeitet ohne Speicherung des lokalen Status oder von Tracking-IDs über Cookies in der aktuellen Sitzung.	Keine identifiziert. Das Fehlen von Cookies eliminiert Risiken im Zusammenhang mit Cookie-basiert em Session-Hijacking oder der Nichteinhaltung von Tracking-Vorgaben.

Erkenntnisse

✓ Verifizierter Befund

Schwere	Beschreibung	Empfehlung
Info	In den gecrawlten HTTP-antworten wurden keine set-cookie-header gefunden das kann bei statischen websites oder bei websites normal sein, die cookies erst nach einwilligung, anmeldung oder javascript-ausführung setzen	Wenn die website analysen, login-sitzungen oder consent-banner verwendet, prüfen sie das cookie-verhalten in einer echten browser-sitzung (vor und nach der einwilligung) und stellen sie sicher, dass die cookie-attribute korrekt konfiguriert sind

Sitemaps und robots.txt

robots.txt gibt Suchmaschinen und anderen Crawlern eine Crawling-Anleitung. Eine Sitemap hilft Suchmaschinen dabei, wichtige Seiten zu entdecken. In diesem Abschnitt wird überprüft, ob robots.txt und eine oder mehrere Sitemap-URLs erreichbar sind.

Metrisch	Wert
Basis-URL	https://www.conson.com
robots.txt-URL	https://www.conson.com/robots.txt
robots.txt-Status	200 (OK)
Sitemaps überprüft	1

robots.txt-Übersicht

- User-Agents: *
- Sitemaps: Keine
- Disallow-Regeln: 0

Sitemap-Abrufergebnisse

URL	Status
https://www.conson.com/sitemap.xml	500 (Interner Serverfehler)

Empfehlung

Stellen Sie eine robots.txt-Datei mit klaren Crawling-Anleitungen bereit und veröffentlichen Sie eine sitemap.xml, die wichtige kanonische Seiten auflistet. Stellen Sie sicher, dass Sitemap-URLs erreichbar und aktualisiert sind, wenn sich die Site-Struktur ändert.

Erkenntnisse

✓ Verifizierter Befund

Schwere	Beschreibung	Empfehlung
Mittel ✓	Es wurde keine erreichbare sitemap gefunden (robots txt-sitemap-zeilen oder /sitemap xml)	Fügen sie sitemap-referenzen zu robots txt hinzu und stellen sie sicher, dass /sitemap xml (oder ihre sitemap-url) 200 zurückgibt und auf dem neuesten stand gehalten wird
Niedrig ✓	Einige sitemap-urls waren nicht erreichbar korrigieren oder entfernen sie defekte sitemap-referenzen	Prüfen Sie diese Feststellung und setzen Sie die passende Abhilfemaßnahme auf Grundlage des beschriebenen Problems um.

Link-Gesundheit

Dieser Abschnitt analysiert die Qualität der Links, die auf 8 gecrawlten Seiten der Website gefunden wurden, basierend auf dem für diesen Bericht konfigurierten Crawl-Limit. Er hilft dabei, fehlerhafte Links, Weiterleitungen und Seiten ohne gültige HTTP-Antwort zu identifizieren.

Interne Links

Metrik	Wert
Gesamtzahl interner Links	72
OK / erreichbar	64
Weiterleitungen	6
Fehler / nicht erreichbar	1

Interne Links mit Problemen

URL	Status	Empfehlung
https://www.conson.com/wp-json/oembed/1.0/embed	400 (Fehlerhafte Anfrage)	Aktualisieren Sie die interne URL oder fügen Sie eine korrekte Weiterleitung zu einer funktionierenden Seite hinzu.

Externe Links

Metrik	Wert
Gesamtzahl externer Links	5
OK / erreichbar	3
Fehler / nicht erreichbar	2

Externe Links mit Problemen

URL	Status	Empfehlung
https://fonts.googleapis.com/css	400 (Fehlerhafte Anfrage)	Prüfen Sie die Drittanbieter-URL und ersetzen, entfernen oder aktualisieren Sie die Referenz.
https://fonts.googleapis.com	404 (Nicht gefunden)	Prüfen Sie die Drittanbieter-URL und ersetzen, entfernen oder aktualisieren Sie die Referenz.

Erkenntnisse

✓ Verifizierter Befund

Schwere	Beschreibung	Empfehlung
Mittel ✓	Ein oder mehrere interne links haben einen fehler zurückgegeben oder konnten nicht erreicht werden	Beheben sie defekte interne links, indem sie die ziel-url korrigieren, die zielseite wiederherstellen oder eine geeignete weiterleitung einrichten

Niedrig ✓	Ein oder mehrere externe links haben einen fehler zurückgegeben oder konnten nicht erreicht werden	Prüfen sie betroffene drittanbieter-links und ersetzen, entfernen oder aktualisieren sie nicht mehr funktionierende referenzen

Performance-Indikatoren

Dieser Abschnitt enthält einfache Performance-Indikatoren auf Basis einer einzelnen Anfrage an die Startseite.

Metrisch	Wert
Endgültige URL	https://www.conson.com/de/
HTTP-Status	200 (OK)
Reaktionszeit (ms)	1712
HTML-Größe (Byte)	77933
Cache-Kontrolle	no-cache, no-store, must-revalidate

Erkenntnisse

✓ Verifizierter Befund

Schwere	Beschreibung	Empfehlung
Info	Cache-control schlägt vor, dass das caching deaktiviert ist (nein-store/nein-cache)	Stellen sie sicher, dass dies beabsichtigt ist wenn nicht, aktivieren sie das caching für nicht sensible inhalte und statische ressourcen

Grundlagen der Barrierefreiheit

Schnelle WCAG-Prüfungen auf Basis der gecrawlten Seiten. Eine WCAG-Prüfung ist eine Barrierefreiheitsprüfung einer Website oder Webseite anhand der Web Content Accessibility Guidelines.

Meta-Description fehlt auf 0/8 Seiten.

Titel fehlt auf 0/8 Seiten.

HTML-Sprache fehlt auf 0/8 Seiten.

Bei 152/168 gecrawlten Bildern fehlt Alternativtext.

URL	Titel	Meta	Sprache	ALT fehlt
https://www.conson.com/de	✓	✓	✓	19/21
https://www.conson.com	✓	✓	✓	19/21
https://www.conson.com/pt-pt	✓	✓	✓	19/21
https://www.conson.com/nl	✓	✓	✓	19/21
https://www.conson.com/it	✓	✓	✓	19/21
https://www.conson.com/fr	✓	✓	✓	19/21
https://www.conson.com/es	✓	✓	✓	19/21
https://www.conson.com/da	✓	✓	✓	19/21

Erkenntnisse

✓ Verifizierter Befund

Schwere	Beschreibung	Empfehlung
Mittel ✓	Alt-text fehlt bei 152/168 gecrawlten bildern	Fügen sie aussagekräftigen alt-text für informative bilder hinzu; für dekorative bilder leeres alt verwenden kurz und beschreibend halten

Grundlegende SEO-Analyse

Suchmaschinen nutzen Seitentitel, Meta-Beschreibungen, kanonische URLs und Überschriften, um Inhalte zu verstehen. Dieser Abschnitt prüft grundlegende SEO-Signale auf der Homepage und sorgt für schnelle Verbesserungen.

Metrisch	Wert
Endgültige URL	https://www.conson.com/de/
Titel	Conson - Produkte für die Haus- und Gebäudeautomation
Meta-Beschreibung	Steigern Sie Ihren Komfort mit unseren Produkten für die Haus- und Gebäudeautomation. Steuern und überwachen Sie Ihr Zuhause von überall mit Ihrem PC, Telefon oder Tablet.
Kanonisch	https://www.conson.com/de/
Roboter-Meta	index, follow, noarchive
H1-Anzahl	5
H2-Anzahl	6

H1-Übersicht

- Steigern Sie Ihren Komfort mit unseren Produkten für die Haus- und Gebäudeautomation
- Steuerung und Überwachung Ihres Hauses von überall mit Ihrem PC, Telefon oder Tablet
- Steuern Sie einfach Ihre Beleuchtung, Storen oder Thermostate und vieles mehr
- Nur ein Drucktaste in diesem Gebäude? Wie wird der Rest serviert? Siehe weiter ...

H2-Übersicht

- WERTE
- Produkte
- Downloads
- HÄNDLER
- UBER
- Kontakt

Empfehlung

Erstellen Sie eindeutige Titel pro Seite, schreiben Sie eine überzeugende Meta-Beschreibung, legen Sie kanonische URLs für Schlüsselseiten fest und strukturieren Sie Inhalte mit einem klaren H1. Fügen Sie OpenGraph/Twitter-Tags hinzu, um die Linkvorschau in sozialen Medien zu verbessern.

Erkenntnisse

✓ Verifizierter Befund

Schwere	Beschreibung	Empfehlung
Info	Mehrere h1-überschriften erkannt bevorzugen sie aus gründen der klarheit und struktur ein einzelnes haupt-h1	Prüfen Sie diese Feststellung und setzen Sie die passende Abhilfemaßnahme auf Grundlage des beschriebenen Problems um.
Info	Opengraph og:title fehlt	Prüfen Sie diese Feststellung und setzen Sie die passende Abhilfemaßnahme auf Grundlage des beschriebenen Problems um.

Info	Open-Graph-Bild fehlt auf der Startseite	Fügen sie ein og:image-meta-tag mit einer passenden bild-url hinzu (absolute url empfohlen) das verbessert link-vorschauen beim teilen in sozialen netzwerken

Erweiterte SEO-Analyse

Dieser Abschnitt bietet einen konsolidierten Überblick über die wichtigsten SEO-Signale auf der gesamten Website, die auf den analysierten Seiten identifiziert wurden, wobei der Schwerpunkt auf strukturellen, technischen und inhaltsbezogenen Faktoren liegt, die die Suchsichtbarkeit und die organische Leistung beeinflussen können.

Kategorie	Metrik	Wert / Seiten
Abdeckung	Gecrawlte Seiten	8
Abdeckung	Analysierte Seiten	8
Metadaten	Lange Seitentitel	2
Metadaten	Fehlende Meta-Beschreibungen	0
Metadaten	Lange Meta-Beschreibungen	5
Überschriften	Seiten ohne H1	0
Überschriften	Seiten ohne H2	0
Indexierung und kanonische URL	Seiten mit gültiger kanonischer URL	8
Indexierung und kanonische URL	Seiten ohne kanonische URL	0
Indexierung und kanonische URL	Seiten mit ungültiger kanonischer URL	0
Indexierung und kanonische URL	Seiten mit abweichender kanonischer URL	0
Indexierung und kanonische URL	Seiten mit noindex-Kennzeichnung	0
Duplikate	Gruppen mit doppelten Titeln	0
Duplikate	Gruppen mit doppelten Meta-Beschreibungen	0

Erkenntnisse

✓ Verifizierter Befund

Schwere	Beschreibung	Empfehlung
Niedrig ✓	Zu lange <title>-tags wurden erkannt	Kürzen sie titel auf ~50-60 zeichen, um abschneidung zu vermeiden wichtigstes keyword nach vorne
Info	Zu lange meta descriptions wurden erkannt	Kürzen sie meta descriptions auf ~120-160 zeichen (fokus auf den ersten satz), damit snippets nicht abgeschnitten werden

Bildressourcen

Wir haben 280 Bilder überprüft, die während des Crawls auf 8 von 8 gecrawlten Seiten gefunden wurden. 37 Bild-URLs wurden technisch geprüft.

4 große Bilddateien wurden bei der Prüfung von 280 Bildvorkommen erkannt.

Bilder ≥ 500 KB

Quelle	Bild-URL	Alt	BxH	Laden	Größe	Typ
https://www.conson.com/de/	https://www.conson.com/wp-content/uploads/2020/07/BackgroundB.png		1183 x1136	Nicht gesetzt	1.8 MB	png
https://www.conson.com/de/	https://www.conson.com/wp-content/uploads/2020/08/BackgroundVillaGsm-2.png		1183 x1136	Nicht gesetzt	1.9 MB	png
https://www.conson.com/de/	https://www.conson.com/wp-content/uploads/2020/08/KitchenTabletGrijs.png		1183 x1136	Nicht gesetzt	1.1 MB	png
https://www.conson.com/de/	https://www.conson.com/wp-content/uploads/2020/08/BuildingWitXp.png		1183 x1135	Nicht gesetzt	1.2 MB	png

Erkenntnisse

✓ Verifizierter Befund

Schwere	Beschreibung	Empfehlung
Mittel ✓	4 einzelne bilder überschreiten 500 kb, was die ladezeiten der seite verlangsamen kann	Komprimieren/skalieren sie bilder, verwenden sie moderne formate (webp/avif) und aktivieren sie gegebenenfalls caching/CDN
Niedrig ✓	Bei 152 bildvorkommen fehlt alt-text	Fügen sie aussagekräftigen alternativtext für inhaltsbilder hinzu verwenden sie für dekorative bilder das leere alt (alt="")
Niedrig ✓	Bei 32 bildvorkommen fehlen explizite width/height-attribute	Fügen sie breiten- und höhenattribute (oder css-seitenverhältnisse) für bilder hinzu, um layoutverschiebungen zu reduzieren
Info	Bei 168 bildvorkommen fehlt ein loading-attribut	Verwenden sie „loading="lazy" für „below-the-fold"-bilder und halten sie kritische bilder bereit

JavaScript-Indikatoren

Dieser Abschnitt analysiert die auf der Website erkannten JavaScript-Ressourcen. Er bietet Einblick in Skripte, Drittanbieter-Abhängigkeiten und clientseitige Technologien, die Sicherheit, Datenschutz, Leistung und Wartbarkeit beeinflussen können.

Metrisch	Wert
Gescannten Seiten	8
Seiten mit Skripten	8
Seiten mit Inline-Skripten	8
Limit	100
Eindeutige Skript-URLs erkannt	21
Skript-URL-Vorkommen	168
Metric Total Script Tag Occurrences	256
Durchschnittliche Anzahl von Skriptvorkommen pro Seite	32.0
Maximale Anzahl von Skriptvorkommen auf einer Seite	32
Seiten mit Inline-Skripten	8
Metric Inline Script Occurrences	88
Durchschnittliche Anzahl von Inline-Skriptvorkommen pro Seite	11.0
Maximale Anzahl von Inline-Skriptvorkommen auf einer Seite	11

Skripte (alle)

URL	Async/Defer	Seiten
https://www.google-analytics.com/analytics.js	async	8
https://www.conson.com/wp-includes/js/jquery/jquery.js	-	8
https://www.conson.com/wp-includes/js/jquery/jquery-migrate.min.js	-	8
https://www.conson.com/wp-content/plugins/sitepress-multilingual-CMS/res/js/jquery.cookie.js	-	8
https://www.conson.com/wp-content/plugins/sitepress-multilingual-CMS/res/js/cookies/language-cookie.js	-	8
https://www.conson.com/wp-content/plugins/cookie-law-info/public/js/cookie-law-info-public.js	-	8
https://www.conson.com/wp-content/plugins/sitepress-multilingual-CMS/templates/language-switchers/legacy-dr...	-	8
https://www.conson.com/wp-content/plugins/sitepress-multilingual-CMS/dist/js/browser-redirect/app.js	-	8
https://www.conson.com/wp-content/themes/onepress/assets/js/plugins.js	-	8
https://www.conson.com/wp-content/themes/onepress/assets/js/bootstrap.min.js	-	8
https://www.conson.com/wp-content/themes/onepress/assets/js/owl.carousel.min.js	-	8
https://www.conson.com/wp-content/themes/onepress/assets/js/theme.js	-	8
https://www.conson.com/wp-content/plugins/onepress-plus/assets/js/slider.js	-	8
https://www.conson.com/wp-content/plugins/onepress-plus/assets/js/onepress-plus.js	-	8
https://www.conson.com/wp-includes/js/wp-embed.min.js	-	8
https://www.conson.com/wp-content/plugins/wpforms/assets/js/wpforms.js	-	8

https://www.conson.com/wp-content/plugins/wpforms-captcha/assets/js/wpforms-captcha.min.js	-	8
https://www.conson.com/wp-content/plugins/wpforms/assets/js/choices.min.js	-	8
https://www.conson.com/wp-content/plugins/wpforms/assets/js/jquery.validate.min.js	-	8
https://www.conson.com/wp-content/plugins/wpforms/assets/js/mailcheck.min.js	-	8
https://www.google.com/recaptcha/API.js	-	8

Details zu Skript-URLs (HEAD-Anfragen)

URL	Größe (KB)	Typ
https://www.google-analytics.com/analytics.js	20	text/javascript
https://www.conson.com/wp-includes/js/jquery/jquery.js	32	application/javascript
https://www.conson.com/wp-includes/js/jquery/jquery-migrate.min.js	3	application/javascript
https://www.conson.com/wp-content/plugins/sitepress-multilingual-CMS/res/js/jquery.cookie.js	1	application/javascript
https://www.conson.com/wp-content/plugins/sitepress-multilingual-CMS/res/js/cookies/language-cookie.js	0	application/javascript
https://www.conson.com/wp-content/plugins/cookie-law-info/public/js/cookie-law-info-public.js	7	application/javascript
https://www.conson.com/wp-content/plugins/sitepress-multilingual-CMS/templates/language-switchers/legacy-dr...	0	application/javascript
https://www.conson.com/wp-content/plugins/sitepress-multilingual-CMS/dist/js/browser-redirect/app.js	27	application/javascript
https://www.conson.com/wp-content/themes/onepress/assets/js/plugins.js	26	application/javascript
https://www.conson.com/wp-content/themes/onepress/assets/js/bootstrap.min.js	11	application/javascript
https://www.conson.com/wp-content/themes/onepress/assets/js/owl.carousel.min.js	11	application/javascript
https://www.conson.com/wp-content/themes/onepress/assets/js/theme.js	6	application/javascript
https://www.conson.com/wp-content/plugins/onepress-plus/assets/js/slider.js	0	application/javascript
https://www.conson.com/wp-content/plugins/onepress-plus/assets/js/onepress-plus.js	4	application/javascript
https://www.conson.com/wp-includes/js/wp-embed.min.js	0	application/javascript
https://www.conson.com/wp-content/plugins/wpforms/assets/js/wpforms.js	15	application/javascript
https://www.conson.com/wp-content/plugins/wpforms-captcha/assets/js/wpforms-captcha.min.js	0	application/javascript
https://www.conson.com/wp-content/plugins/wpforms/assets/js/choices.min.js	18	application/javascript
https://www.conson.com/wp-content/plugins/wpforms/assets/js/jquery.validate.min.js	7	application/javascript
https://www.conson.com/wp-content/plugins/wpforms/assets/js/mailcheck.min.js	1	application/javascript
https://www.google.com/recaptcha/API.js	1	text/javascript; charset=utf-8

Erkenntnisse

✓ Verifizierter Befund

Schwere	Beschreibung	Empfehlung
Info	Viele Skript-Tags erkannt	Reduzieren sie die anzahl der scripts, indem sie ungenutzte bibliotheken entfernen, dateien bündeln und nur das nötige laden
Info	Viele Inline-Skripte erkannt	Verschieben sie wiederholte inline-skripte in wiederverwendbare dateien und nutzen sie caching; inline nur für kritisches bootstrapping
Niedrig ✓	Einige Skripte haben kein async/defer	Fügen sie async/defer zu nicht-kritischen skripten hinzu, um das rendering nicht zu blockieren blockierende skripte nur verwenden, wenn für above-the-fold erforderlich

Formulare

Dieser Abschnitt prüft auf der Website erkannte Formulare und hebt beobachtbare formularbezogene Indikatoren hervor.

Form	Methode	Eingaben	Details
https://www.conson.com/da https://www.conson.com/de https://www.conson.com/es https://www.conson.com/fr https://www.conson.com/it https://www.conson.com/nl https://www.conson.com/pt-pt https://www.conson.com	POST	18	- wpforms[fields][4] (text, required) - wpforms[fields][5] (text, required) - wpforms[fields][9] (email, required) - wpforms[fields][7] (text, not required) - wpforms[fields][8] (text, not required) - wpforms[fields][26][] (checkbox, required) - wpforms[fields][29][] (checkbox, not required) - wpforms[fields][31][a] (text, required) - wpforms[fields][31][cal] (hidden, not required) - wpforms[fields][31][n2] (hidden, not required) - wpforms[fields][31][n1] (hidden, not required) - wpforms[hp] (text, not required) - g-recaptcha-hidden (text, required) - wpforms[id] (hidden, not required) - wpforms[author] (hidden, not required) - wpforms[post_id] (hidden, not required) - wpforms[fields][2] (textarea, required) - wpforms[fields][3] (select, required) • ... (+3 weitere Elemente)

Erkenntnisse

✓ Verifizierter Befund

Schwere	Beschreibung	Empfehlung
Info	Formulare, die offenbar personenbezogene daten wie eine e-mail-adresse erfassen, wurden ohne klare einwilligungs- oder datenschutz-hinweis-check box erkannt	Fügen sie einen klaren datenschutzhinweis in der nähe des absende-buttons hinzu und, falls passend, eine einwilligungs-checkbox mit link zur datenschutzerklärung
Niedrig ✓	Post-formulare wurden ohne CSRF-ähnliches token anhand versteckter eingabefelder erkannt	Implementieren sie serverseitigen CSRF-schutz und fügen sie bei post-formularübermittlungen ein sitzungsbezogenes tokenfeld hinzu

Tracking-Indikatoren

Dieser Abschnitt identifiziert Tracking-Technologien und Indikatoren, die auf der Website erkannt wurden, wie Analysewerkzeuge, Werbeplattformen, Tag-Management-Systeme und Einwilligungsmechanismen. Er hilft zu verstehen, wie Besucheraktivitäten gemessen oder mit Dritten geteilt werden können.

Metrik	Wert
Endgültige URL	https://www.conson.com/de/
Tracker-Technologien erkannt	1
CMP-/Zustimmungssignale erkannt	0
Cookie-Banner-Hinweis	✗
Drittanbieter-Domains (Skripte/Iframes)	5

Erkannte Tracker-Familien

Name	Beispiel-URLs
Google Analytics	https://www.google-analytics.com/analytics.js

Drittanbieter-Domains

Vollständige Liste (alle während des Audits beobachteten Drittanbieter-Domains).

Domain
gmpg.org
www.google-analytics.com
fonts.googleapis.com
s.w.org
www.google.com

Erkenntnisse

✓ Verifizierter Befund

Schwere	Beschreibung	Empfehlung
Hoch ✓	Es wurden tracking-technologien erkannt, aber auf der homepage wurde kein einwilligungs-/cmp-signal gefunden (heuristik)	Wenn sie nicht unbedingt erforderliche tracker (analysen/marketing) verwenden, stellen sie sicher, dass die einwilligung eingeholt wird, bevor sie sie laden, und dokumentieren sie anbieter/zwecke in ihrer cookie-/datenschutzrichtlinie
Info	Mehrere drittanbieter-ressourcen wurden erkannt drittanbieter-skripte bedeuten nicht automatisch tracking, sollten aber hinsichtlich datenschutz und einwilligung geprüft werden	Prüfen Sie diese Feststellung und setzen Sie die passende Abhilfemaßnahme auf Grundlage des beschriebenen Problems um.

Einhaltung der DSGVO und des Datenschutzes

In diesem Abschnitt wird bewertet, ob die Website die wesentlichen Transparenz- und Einwilligungsanforderungen der DSGVO erfüllt.

Metrisch	Wert
DSGVO-Compliance-Score (0-100)	100
Rechtliches Risikoniveau (Heuristik)	Niedrig

Wichtige Richtlinien und Zustimmungssignale

Artikel	Status
Datenschutzrichtlinie	✓
Cookie-Richtlinie	✓
Allgemeine Geschäftsbedingungen	✓
Cookie-Zustimmungsbanner	✓

Erkannte Richtlinien-Seiten oder Links

Artikel	Erkannte Seite oder erkannter Link
Datenschutzrichtlinie	https://www.conson.com/wp-content/uploads/2020/08/Privacy-declaration_EN.pdf
Cookie-Richtlinie	https://www.conson.com/wp-content/uploads/2020/08/CookiePolicy_EN.pdf
Allgemeine Geschäftsbedingungen	https://www.conson.com/wp-content/uploads/2020/08/Terms_and_conditions_www.conson.com_EN.pdf

Details zum Cookie-Einwilligungsbanner

Artikel	Wert
Erkennungsmethode des Cookie-Banners	Technischer/CMP-Indikator im HTML
Cookie-Banner-Indikator	cookie-law-info

Expositionsprüfungen

Dieses Modul identifiziert potenzielle Cybersicherheitsrisiken. Dieser Abschnitt überprüft öffentlich sichtbare Expositionsindikatoren wie offengelegte Pfade, Kontaktdaten, Tokens und Entwicklerreferenzen.

Offengelegte Pfadbefunde

Pfad	URL	HTTP	Content-Type / Hinweis
/wp-json/wp/v2/users	https://www.conson.com/de/wp-json/wp/v2/users	200 (OK)	application/json; charset=UTF-8

Indikatoren für offengelegte Kommunikationsdaten

In den gecrawlten Seiten wurden keine offengelegten E-Mail-Adressen oder Telefonnummern erkannt.

Mögliche Secrets oder Zugangsdaten

In den gecrawlten Seiten wurden keine offengelegten Secrets, Tokens oder zugangsdatenähnlichen Muster erkannt.

Indikatoren für internes Netzwerk und Zugangsdaten in URLs

Es wurden keine internen IP-Adressen oder Zugangsdaten-in-URL-Muster erkannt.

Indikatoren für Entwickler- und Debug-Exposition

Es wurden keine Entwickler-/Debug-Expositionssignale erkannt (z. B. Source Maps, Stack Traces, Debug-Flags, Admin- oder Entwicklungsverweise).

Cloud-Speicher- und Dienstreferenzen

In den gecrawlten Seiten wurden keine Cloud-Speicher- oder Dienstreferenzen erkannt.

OWASP-Grundlagen

Dieser Abschnitt ordnet beobachtete Website-Signale den Risikobereichen der OWASP Top 10 zu. Die Prüfungen sind automatisiert und heuristisch und ersetzen keinen vollständigen Penetrationstest.

Metrisch	Wert
Basis-Sicherheitsbewertung (0-100)	100
Gefundene Indikatoren (Themen mit Signalen)	9

Überblick über die OWASP Top-10-Themen

Thema	Beschreibung	Status
A01 - Fehlerhafte Zugriffskontrolle	Einschränkungen und Autorisierungsfehler, die es Benutzern ermöglichen, über die vorgesehenen Berechtigungen hinaus auf Daten oder Funktionen zuzugreifen.	Öffentliche Hinweise gefunden: Zugängliche Admin-/Login-Pfade: https://www.conson.com/de/login, https://www.conson.com/de/wp-login.php; Öffentlich zugängliche sensible oder eingeschränkte Dateien: https://www.conson.com/de/readme.html, https://www.conson.com/de/CHANGELOG.txt
A02 - Kryptografische Fehler	Schwachstellen in der Verschlüsselung oder Transportsicherheit, die zur Offenlegung sensibler Daten führen können.	Öffentliche Hinweise gefunden: HTTPS für die geprüfte Website festgestellt
A03 - Injektion	nicht vertrauenswürdige Eingaben, die Interpreter (SQL/NoSQL/OS/LDAP) erreichen, in manchen Kontexten auch XSS.	Öffentliche Hinweise gefunden: HTML-Formulare auf öffentlichen Seiten: 1; Inline-Script-Tags erkannt: 11
A04 - Unsicheres Design	Fehlende oder ineffektive Sicherheitskontrollen aufgrund des Designs (erfordert eine Überprüfung der Architektur).	Öffentliche Hinweise gefunden: POST-Formulare ohne sichtbares CSRF-ähnliches Token: 1
A05 - Fehlkonfiguration der Sicherheit	Unsichere Standardeinstellungen, fehlende Header, offengelegte Dateien oder falsch konfigurierte Dienste.	Öffentliche Hinweise gefunden: Fehlende Security-Header: Content-Security-Policy, Permissions-Policy; Technologieinformationen über Header vorhanden: Server; Offengelegte Konfigurations-/sensible Dateien: https://www.conson.com/de/readme.html, https://www.conson.com/de/CHANGELOG.txt
A06 - Anfällige und veraltete Komponenten	Verwendung von Bibliotheken, Frameworks oder Plattformen mit bekannten Schwachstellen oder offengelegten Versionsinformationen.	Öffentliche Hinweise gefunden: Versions-/Paketmetadaten offengelegt: https://www.conson.com/de/readme.html, https://www.conson.com/de/CHANGELOG.txt; Scripts ohne Integritätsattribut: 2; Generator-Metadaten erkannt auf: https://www.conson.com/de
A07 - Identifikations- und Authentifizierungsfehler	Schwachstellen bei Anmeldung, Sitzungsverwaltung oder Verarbeitung von Anmeldedaten.	Öffentliche Hinweise gefunden: Login-/Authentifizierungspfade offengelegt: https://www.conson.com/de/login, https://www.conson.com/de/wp-login.php; POST-Formulare ohne sichtbares CSRF-ähnliches Token: 1

A08 - Software- und Datenintegritätsfehler	Fehlende Integritätsprüfungen (z. B. SRI) oder unsichere Update- und CI-Pipelines.	Öffentliche Hinweise gefunden: Versions-/Paketmetadaten offengelegt: https://www.conson.com/de/readme.html, https://www.conson.com/de/CHANGELOG.txt; Drittanbieter-Domains referenziert: www.google-analytics.com, www.google.com
A09 - Sicherheitsprotokollierungs- und Überwachungsfehler	Unzureichende Protokollierung oder Überwachung zur Erkennung und Reaktion auf Angriffe.	Öffentliche Hinweise gefunden: Technologieinformationen über Header vorhanden: Server
A10 - Serverseitige Anforderungsfälschung (SSRF)	Der Server ruft von Angreifern kontrollierte URLs ab, häufig über URL-Eingaben; in der Regel sind tiefergehende Tests erforderlich.	Kein öffentlicher Hinweis gefunden

Hinweis

Diese Erkenntnisse basieren auf automatisierten Prüfungen und Heuristiken. Für eine höhere Sicherheit führen Sie eine manuelle Überprüfung und/oder einen Penetrationstest durch, insbesondere bei Authentifizierungs-, Autorisierungs- und Anwendungslogik-Schwachstellen.

Erkenntnisse

✓ Verifizierter Befund

Schwere	Beschreibung	Empfehlung
Info	OWASP-indikatoren basieren nur auf öffentlichen signalen; dies ist kein penetrationstest	Prüfen Sie diese Feststellung und setzen Sie die passende Abhilfemaßnahme auf Grundlage des beschriebenen Problems um.

ISO 27001-Indikatoren

Diese Analyse spiegelt Cybersicherheitskontrollen wider, die an ISO 27001 ausgerichtet sind. Dieser Abschnitt behandelt ISO-27001-Indikatoren auf Basis öffentlich beobachtbarer Informationen. Für jedes Thema wird angegeben, ob ein öffentlicher Hinweis gefunden wurde, kein öffentlicher Hinweis gefunden wurde oder das Thema nicht auf Hinweise untersucht wurde.

Metrisch	Wert
Rahmen	ISO-27001-Indikatoren
Indikatoren	7
Themen mit öffentlichen Indikatoren	6

Übersicht der Indikatoren nach Thema

Kontrollthema	Objektiv	Status
A.9 Zugriffskontrolle	Zugangsbezogene Einstiegspunkte zeigen Anzeichen kontrollierter Authentifizierung und Request-Schutz	Öffentliche Hinweise gefunden. Beweis: Erreichbare Admin-/Login-Pfade erkannt: https://www.conson.com/de/login, https://www.conson.com/de/wp-login.php; Öffentlich erreichbare sensible Pfade erkannt: https://www.conson.com/de/readme.html, https://www.conson.com/de/CHANGELOG.txt; POST-Formulare ohne sichtbares CSRF-ähnliches Token: 1
A.10 Kryptographie	Transportverschlüsselung und Cookie-Schutz sind sicher konfiguriert	Öffentliche Hinweise gefunden. Beweis: HTTPS für die geprüfte Website festgestellt
A.12 Betriebssicherheit	Die operative Konfiguration reduziert Informationslecks und unsichere Standardeinstellungen	Öffentliche Hinweise gefunden. Beweis: Offengelegte sensible Dateien/Pfade: https://www.conson.com/de/readme.html, https://www.conson.com/de/CHANGELOG.txt
A.13 Kommunikationssicherheit	Externe Kommunikation und Datenaustausch mit Dritten sind kontrolliert und transparent	Öffentliche Hinweise gefunden. Beweis: HTTPS für Website-Kommunikation verwendet; Fehlende Sicherheitsheader: Content-Security-Policy, Permissions-Policy; Kommunikationsdomains von Drittanbietern beobachtet: www.google-analytics.com, www.google.com
A.14 Systemerwerb, Entwicklung und Wartung	Technologieentscheidungen und Entwicklungssignale unterstützen eine sichere Wartung	Öffentliche Hinweise gefunden. Beweis: Versions-/Paketmetadaten offengelegt: https://www.conson.com/de/readme.html, https://www.conson.com/de/CHANGELOG.txt; Externe JavaScript-Dateien erkannt: 21; Generator-Metadaten erkannt auf: https://www.conson.com/de
A.16 Management von Informationssicherheitsvo...	Öffentliche Sicherheits- und Incident-Kontaktkanäle sind sichtbar und nutzbar	Kein öffentlicher Hinweis gefunden

A.18 Compliance	Öffentliche Transparenz- sowie Datenschutz-/Compliance-Signale unterstützen gesetzliche und regulatorische Pflichten	Öffentliche Hinweise gefunden. Beweis: Datenschutzerklärungsseite erkannt: https://www.conson.com/wp-content/uploads/2020/08/Privacy-declaration_EN.pdf; Cookie-Richtlinienseite erkannt: https://www.conson.com/wp-content/uploads/2020/08/CookiePolicy_EN.pdf; Seite mit allgemeinen Geschäftsbedingungen erkannt: https://www.conson.com/wp-content/uploads/2020/08/Terms_and_conditions_www.conson.com_EN.pdf; Tracking-Skripte auf Seiten erkannt: 1

Notizen

- Die ISO/IEC 27001-Zertifizierung kann nicht allein durch automatisiertes Scannen von Websites bestätigt werden.

- Diese Indikatoren ordnen technische Signale hochrangigen ISO 27001/Anhang A-Themen zu, um die Diskussion und Priorisierung zu unterstützen.

Disclaimer

Dies sind lediglich indikative Signale. Eine ISO/IEC-27001-Zertifizierung erfordert eine vollständige ISMS-Umfangsbewertung, die Prüfung von Nachweisen und Audits. Verwenden Sie diesen Abschnitt als Bereitschafts- und Best-Practice-Perspektive, nicht als Compliance-Erklärung.

Erkenntnisse

✓ Verifizierter Befund

Schwere	Beschreibung	Empfehlung
Info	Iso-27001-indikatoren basieren auf öffentlich beobachtbaren website-informationen und stellen keine zertifizierungsbewertung dar	Prüfen Sie diese Feststellung und setzen Sie die passende Abhilfemaßnahme auf Grundlage des beschriebenen Problems um.

Risiko- und Aktionsplan

Dieser Abschnitt identifiziert Cybersicherheitsrisiken und überführt die wichtigsten Feststellungen in einen priorisierten Maßnahmenplan.

Top 10 Prioritäten

Schwere	Module	Beschreibung
Hoch	Tracking-Indikatoren	Es wurden Tracking-Technologien erkannt, aber auf der Homepage wurde kein Einwilligungs-/CMP-Signal gefunden (Heuristik). Stellen Sie sicher, dass Einwilligungsmanagement und Offenlegungen bei Bedarf implementiert werden.
Mittel	HTTP-Sicherheitsheader	Content-Security-Policy fehlt. (Eine CSP hilft, XSS- und Dateninjektionsrisiken zu reduzieren.)
Mittel	Bildressourcen	4 einzelne Bilder überschreiten 500 KB, was die Ladezeiten der Seite verlangsamen kann.
Mittel	Sitemaps und robots.txt	Es wurde keine erreichbare Sitemap gefunden (robots.txt-Sitemap-Zeilen oder /sitemap.xml).
Mittel	KI-Wahrnehmungsanalyse	Verwirrung um die Produktverfügbarkeit
Mittel	KI-Wahrnehmungsanalyse	Barriere der technischen Komplexität
Mittel	KI-Wahrnehmungsanalyse	Installationsabhängigkeit unklar
Mittel	KI-Wahrnehmungsanalyse	Mögliche Verwirrung bezüglich der Produktkompatibilität
Mittel	KI-Wahrnehmungsanalyse	Unsicherheit bezüglich der Installationsanforderungen
Mittel	KI-Wahrnehmungsanalyse	Unklarheiten bei den Produktmerkmalen

Übersicht des vorgeschlagenen Zeitplans

Vorgeschlagener Zeitplan	Schwere	Elementbeschreibung	Modul
0-30 Tage	Hoch	Es wurden Tracking-Technologien erkannt, aber auf der Homepage wurde kein Einwilligungs-/CMP-Signal gefunden (Heuristik). Stellen Sie sicher, dass Einwilligungsmanagement und Offenlegungen bei Bedarf implementiert werden.	Tracking-Indikatoren
0-30 Tage	Mittel	Content-Security-Policy fehlt. (Eine CSP hilft, XSS- und Dateninjektionsrisiken zu reduzieren.)	HTTP-Sicherheitsheader
0-30 Tage	Mittel	Es wurde keine erreichbare Sitemap gefunden (robots.txt-Sitemap-Zeilen oder /sitemap.xml).	Sitemaps und robots.txt
30-60 Tage	Mittel	Verwirrung um die Produktverfügbarkeit	KI-Wahrnehmungsanalyse
30-60 Tage	Mittel	Barriere der technischen Komplexität	KI-Wahrnehmungsanalyse
30-60 Tage	Mittel	Installationsabhängigkeit unklar	KI-Wahrnehmungsanalyse
30-60 Tage	Mittel	Mögliche Verwirrung bezüglich der Produktkompatibilität	KI-Wahrnehmungsanalyse
30-60 Tage	Mittel	Unsicherheit bezüglich der Installationsanforderungen	KI-Wahrnehmungsanalyse
30-60 Tage	Mittel	Unklarheiten bei den Produktmerkmalen	KI-Wahrnehmungsanalyse
30-60 Tage	Mittel	Mangelnde Informationen über Unterstützungsdienste	KI-Wahrnehmungsanalyse
30-60 Tage	Mittel	Missverständnis des Begriffs „Consonbox"	KI-Wahrnehmungsanalyse

30-60 Tage	Mittel	Übersehene Produktaktualisierungen	KI-Wahrnehmungsanalyse
30-60 Tage	Mittel	Endnutzer könnten versuchen, direkt zu kaufen	KI-Wahrnehmungsanalyse
30-60 Tage	Mittel	Verwirrung über die Produktverfügbarkeit	KI-Wahrnehmungsanalyse
30-60 Tage	Mittel	Sprachmischung in lokalisierten Versionen	KI-Wahrnehmungsanalyse
30-60 Tage	Mittel	Wahrnehmung als Komplettanbieter für Installationsdienstleistungen und nicht als Produktlieferant	KI-Wahrnehmungsanalyse
30-60 Tage	Mittel	Verwirrung zwischen älteren und aktuellen Produktlinien	KI-Wahrnehmungsanalyse
30-60 Tage	Mittel	4 einzelne Bilder überschreiten 500 KB, was die Ladezeiten der Seite verlangsamen kann.	Bildressourcen
30-60 Tage	Mittel	Ein oder mehrere interne Links haben einen Fehler zurückgegeben oder konnten nicht erreicht werden.	Link-Gesundheit
30-60 Tage	Mittel	Alt-Text fehlt bei 152/168 gecrawlten Bildern.	Grundlagen der Barrierefreiheit
30-60 Tage	Niedrig	Permissions-Policy fehlt. (Browserfunktionen werden möglicherweise nicht auf das minimal erforderliche Maß beschränkt.)	HTTP-Sicherheitsheader
30-60 Tage	Niedrig	Cross-Origin-Opener-Policy fehlt. (Cross-Origin-Fensterinteraktionen werden möglicherweise weniger strikt eingeschränkt, wodurch bestimmte Isolationsrisiken steigen.)	HTTP-Sicherheitsheader
30-60 Tage	Niedrig	Cross-Origin-Embedder-Policy fehlt. (Externe Ressourcen werden möglicherweise weniger strikt isoliert, wodurch bestimmte Cross-Origin-Datenleckrisiken steigen.)	HTTP-Sicherheitsheader
30-60 Tage	Niedrig	Cross-Origin-Resource-Policy fehlt. (Externe Websites können bestimmte Ressourcen möglicherweise freier laden als vorgesehen.)	HTTP-Sicherheitsheader
30-60 Tage	Niedrig	POST-Formulare wurden ohne CSRF-ähnliches Token anhand versteckter Eingabefelder erkannt.	Formulare
30-60 Tage	Niedrig	Zu lange <title>-Tags wurden erkannt.	Erweiterte SEO-Analyse
60+ Tage	Niedrig	Bei 152 Bildvorkommen fehlt ALT-Text.	Bildressourcen
60+ Tage	Niedrig	Bei 32 Bildvorkommen fehlen explizite width/height-Attribute.	Bildressourcen
60+ Tage	Niedrig	Einige Sitemap-URLs waren nicht erreichbar. Korrigieren oder entfernen Sie defekte Sitemap-Referenzen.	Sitemaps und robots.txt
60+ Tage	Niedrig	Ein oder mehrere externe Links haben einen Fehler zurückgegeben oder konnten nicht erreicht werden.	Link-Gesundheit
60+ Tage	Niedrig	Einige Skripte haben kein async/defer	JavaScript-Indikatoren
60+ Tage	Info	Der Server Header ist vorhanden. Erwägen Sie, Server- oder Versionsinformationen möglichst zu minimieren.	HTTP-Sicherheitsheader
60+ Tage	Info	Mehrere Drittanbieter-Ressourcen wurden erkannt. Drittanbieter-Skripte bedeuten nicht automatisch Tracking, sollten aber hinsichtlich Datenschutz und Einwilligung geprüft werden.	Tracking-Indikatoren
60+ Tage	Info	Bei 168 Bildvorkommen fehlt ein loading-Attribut.	Bildressourcen
60+ Tage	Info	Formulare, die offenbar personenbezogene Daten wie eine E-Mail-Adresse erfassen, wurden ohne klare Einwilligungs- oder Datenschutz-Hinweis-Checkbox erkannt.	Formulare

60+ Tage	Info	Zu lange Meta Descriptions wurden erkannt.	Erweiterte SEO-Analyse
60+ Tage	Info	Viele Skript-Tags erkannt	JavaScript-Indikatoren
60+ Tage	Info	Viele Inline-Skripte erkannt	JavaScript-Indikatoren
60+ Tage	Info	In den gecrawlten HTTP-Antworten wurden keine Set-Cookie-Header gefunden. Das kann bei statischen Websites oder bei Websites normal sein, die Cookies erst nach Einwilligung, Anmeldung oder JavaScript-Ausführung setzen.	Cookies und Sitzungssicherheit
60+ Tage	Info	OWASP-Indikatoren basieren nur auf öffentlichen Signalen; dies ist kein Penetrationstest.	OWASP-Grundlagen
60+ Tage	Info	Cache-Control schlägt vor, dass das Caching deaktiviert ist (no-store/no-cache).	Performance-Indikatoren
60+ Tage	Info	Mehrere H1-Überschriften erkannt. Bevorzugen Sie aus Gründen der Klarheit und Struktur ein einzelnes Haupt-H1.	Grundlegende SEO-Analyse
60+ Tage	Info	OpenGraph og:title fehlt. Fügen Sie es hinzu, um die Linkvorschau auf sozialen Plattformen zu verbessern.	Grundlegende SEO-Analyse
60+ Tage	Info	Open-Graph-Bild fehlt auf der Startseite	Grundlegende SEO-Analyse
60+ Tage	Info	In den Antwortheadern wurde kein klares CDN/WAF-Signal erkannt (Heuristik). Erwägen Sie gegebenenfalls ein CDN/WAF für Leistung und Sicherheit.	Server- und Hosting-Indikatoren
60+ Tage	Info	Über Fingerprinting-Signale erkannt (Vertrauen: medium).	Technologie & CMS

Nächste Maßnahmen / Servicepaket

Service	Empfehlung
KI-Sichtbarkeitspaket	Verbessern Sie die Auffindbarkeit für KI: strukturierte Daten, Entity-Signale, thematische Autorität und Zitierfähigkeit.
Sicherheitsheader-Paket	Implementieren Sie CSP, HSTS, X-Content-Type-Options und Referrer-Policy und härten Sie die Header-Konfiguration ab.

Disclaimer

Dieser Bericht wurde auf Grundlage öffentlich zugänglicher Informationen erstellt. Er stellt keine Rechtsberatung dar, dient als Bewertung der Cybersicherheit und ersetzt keinen vollständigen Penetrationstest.

Überprüfen Sie kritische Feststellungen und ziehen Sie qualifizierte Fachleute für Sicherheits-, Rechts- und Compliance-Entscheidungen hinzu.

Keine Gewährleistung

Dieser Bericht wird „wie besehen" ohne ausdrückliche oder stillschweigende Gewährleistung bereitgestellt, einschließlich (ohne Einschränkung) Gewährleistungen hinsichtlich Vollständigkeit, Richtigkeit, Eignung für einen bestimmten Zweck oder Nichtverletzung. Das Ausbleiben von Feststellungen bedeutet nicht, dass keine Schwachstellen, Risiken oder Compliance-Lücken bestehen.

Haftungsbeschränkung

Soweit nach geltendem Recht maximal zulässig, haftet Belitum BV nicht für indirekte, zufällige, Folge-, besondere, punitive, rufschädigende oder betriebsunterbrechungsbedingte Schäden (einschließlich Verlust von Gewinn, Umsatz, Goodwill oder Daten), die aus diesem Bericht entstehen oder damit zusammenhängen, selbst wenn Belitum BV auf die Möglichkeit solcher Schäden hingewiesen wurde. In jedem Fall ist die Gesamthaftung von Belitum BV auf den für die Erstellung dieses Berichts gezahlten Betrag begrenzt.

Keine Zertifizierung, keine Bescheinigung

Verweise auf DSGVO, ISO/IEC 27001, OWASP, NIST oder andere Standards und Frameworks sind rein indikative Zuordnungen auf der Grundlage automatisierter Signale. Sie stellen weder eine Zertifizierung noch eine behördliche Genehmigung, ein formelles Audit oder eine rechtliche Konformitätsbewertung dar. Formale Compliance erfordert eine angemessen abgegrenzte Prüfung durch qualifizierte Fachleute.

Verantwortung des Kunden & Validierung

Der Empfänger bleibt allein verantwortlich für die Bewertung und Validierung der Feststellungen, die Umsetzung von Maßnahmen und die Einhaltung geltender Gesetze und Vorschriften. Kritische Feststellungen sollten vor Maßnahmen unabhängig validiert werden. Ziehen Sie für Sicherheits-, Rechts- und Compliance-Entscheidungen qualifizierte Fachleute hinzu.

Sicherheit ist fortlaufend

Sicherheit und Compliance sind fortlaufende Prozesse. Dieser Bericht garantiert weder Immunität gegen Cyberangriffe noch gegen zukünftige Schwachstellen oder dauerhafte Compliance. Ergebnisse können sich durch Updates, Konfigurationsänderungen, Drittanbieterdienste oder neu offengelegte Schwachstellen ändern.

Vertraulichkeit & Nutzung

Dieser Bericht ist für den angegebenen Empfänger bestimmt. Er darf ohne vorherige schriftliche Zustimmung von Belitum BV nicht kopiert, verbreitet, veröffentlicht oder von Dritten verwendet werden.

Anwendbares Recht & zuständiges Gericht

Für diesen Bericht gilt belgisches Recht. Streitigkeiten unterliegen der ausschließlichen Zuständigkeit der zuständigen Gerichte am Sitz von Belitum BV.