Bericht zur externen Angriffsfläche

consilum.de

Berichtsdatum	Prüfung	Prüfziele
14.11.2026	**Nr. 1**	**2**

Kurzüberblick
2 Hinweise.

Ergebnisübersicht

Prüfziel	Ergebnis
consilum.de	1 Hinweis
www.consilum.de	1 Hinweis

Umfang und Methode

Geprüfte Ziele: consilum.de, www.consilum.de.

Messbeginn: 14.11.2026, 21:00 MEZ.

Methode: öffentliche HTTPS-/TLS-Abfragen, HTTP-Header, Mail-DNS, Softwaremerkmale und Links zu Pflichtseiten. Mail-DNS wird an der Hauptdomain ausgewertet. Der Prüfstatus je Host steht unten.

Hostermittlung: bekannte Auftragsziele und öffentliche Zertifikatslogs. Die Abdeckung ist auf diese Quellen begrenzt.

Für Anwendungslogik, Anmeldung, Berechtigungen, Patchstand und die Wirksamkeit der Mailauthentifizierung an echten Nachrichten sind gesonderte Prüfungen erforderlich.

Erfassung eingeschränkt
Die Hostermittlung über öffentliche Zertifikatslogs war unvollständig. Weitere öffentliche Systeme können bestehen. Die Hostliste sollte bestätigt und die Ermittlung wiederholt werden.

1 Hinweis

Dokumentierte Prüfung

Erhobene Prüfbereiche: TLS/Zertifikate, Mail-DNS, HTTP-Header, Softwaremerkmale, Pflichtseiten-Links.
HTTP-Ziel: https://consilum.de/
Aufgelöste IPs: 76.76.21.21

Hinweis

Kein bekanntes Content-Management-System erkannt

Keines der unterstützten CMS-Muster für WordPress, TYPO3, Drupal, Joomla, Shopify, Wix oder Squarespace wurde erkannt. Sichtbar sind „Next.js“ (X-Powered-By) und „Vercel“ (Server).

Relevanz

Version und Aktualität der eingesetzten Komponenten erfordern einen gesonderten Abgleich.

Maßnahme

Halten Sie Ihre Website-Software und Erweiterungen trotzdem aktuell; fragen Sie Ihre Agentur nach dem Update-Rhythmus.

Nachweis N1

Weitere Prüfergebnisse

Prüfung	Feststellung und nächste Schritte
DKIM-Schlüssel gefunden	Für die Selektoren s1, s2 wurden DKIM-Schlüssel im DNS gefunden. Ob ausgehende Nachrichten damit gültig signiert werden, wurde nicht geprüft. Maßnahme An echten Nachrichten prüfen, ob DKIM besteht und die Signaturdomain zur sichtbaren Absenderdomain passt. Schlüssel und Einstellungen beim Wechsel des Versanddienstes aktualisieren. Nachweis N2

Weitere Prüfergebnisse

Prüfung	Feststellung und nächste Schritte
DMARC aktiv (p=quarantine)	Die Domain veröffentlicht p=quarantine als Behandlungsvorgabe für Nachrichten, die DMARC nicht bestehen. Dafür müssen sowohl SPF als auch DKIM ohne passend ausgerichtetes positives Ergebnis bleiben. Relevanz Der Empfänger entscheidet unter Einbeziehung weiterer Prüfungen über die Nachricht. Auch legitime Weiterleitungen und Mailinglisten können DMARC-Fehler verursachen. Maßnahme DMARC-Berichte und echte Mailflüsse regelmäßig prüfen. Legitime Versanddienste und DKIM-Alignment absichern, besonders bei Weiterleitungen und Mailinglisten. Die veröffentlichte Policy belegt keine vollständige Durchsetzung oder sichere Zustellung. Nachweis N2
SPF-Eintrag vorhanden	Ein SPF-Eintrag wurde gefunden. Ob alle legitimen Versanddienste enthalten sind und die Regel vollständig gültig ist, wurde nicht geprüft. Maßnahme Bei Änderungen am Mail- oder Newsletter-Anbieter den Eintrag prüfen und echte Versandtests durchführen. SPF allein garantiert weder Schutz vor Absenderfälschung noch Zustellung. Nachweis N2
6 von 6 Schutz-Headern gesetzt	Vorhanden: strict-transport-security, content-security-policy, x-frame-options, x-content-type-options, referrer-policy, permissions-policy. Maßnahme Die Anzahl bezieht sich auf vorhandene Header. Für die Bewertung ihrer Schutzwirkung sind die jeweiligen Einstellungen maßgeblich. Nachweis N3
Datenschutzerklärung verlinkt	Auf der Startseite wurde ein Link zur Datenschutzerklärung gefunden. Erreichbarkeit und Inhalt des Ziels sind gesondert zu prüfen. Maßnahme Linkziel und Inhalt anhand der tatsächlichen Datenverarbeitung prüfen und bei neuen Diensten aktualisieren. Nachweis N4

Weitere Prüfergebnisse

Prüfung	Feststellung und nächste Schritte
Impressum verlinkt	Auf der Startseite wurde ein Link zum Impressum gefunden. Erreichbarkeit und Inhalt des Ziels sind gesondert zu prüfen. Maßnahme Linkziel und Pflichtangaben prüfen und bei Änderungen der Geschäftsdaten aktualisieren. Nachweis N4
Gültiges Zertifikat, Verschlüsselung aktiv	Ihre Website ist verschlüsselt erreichbar; das Zertifikat ist bis zum 25.12.2026 gültig. Maßnahme Nichts zu tun. Achten Sie darauf, dass die Verlängerung automatisch läuft. Nachweis N5
TLS 1.3 beobachtet, alte TLS-Versionen abgelehnt	Die Verbindung verwendete TLS 1.3. Ein Verbindungsversuch mit TLS 1.0/1.1 wurde vom Server abgelehnt. Maßnahme Nichts zu tun. Nachweis N6

Technische Nachweise · consilum.de

N1 · Softwaremerkmale

X-Powered-By: Next.js
Server: Vercel

N2 · Mail-DNS

MX: consilum-de.mail.protection.outlook.com
SPF: v=spf1 include:spf.protection.outlook.com -all
DMARC: v=DMARC1; p=quarantine; rua=mailto:hello@consilum.de; pct=100
DKIM-Selektoren gefunden: s1, s2 (geprüft: default, google, selector1, selector2, k1, k2, k3, dkim, mail, s1, s2, smtp, mta, key1, mandrill, everlytickey1, mxvault, protonmail, zendesk1, sendgrid)

N3 · HTTP-Header

Geprüfte Adresse: https://consilum.de/ (Status 200)
content-security-policy: default-src 'self'; script-src 'self' 'nonce-qGldNQd5qxAvmiuBwgllZu3j81oYugx2lUnkaVUK/HM=' 'strict-dynamic' https://va.vercel-scripts.com https://connect.facebook.net https://www.googletagmanager.com ...
permissions-policy: camera=(), microphone=(), geolocation=()
referrer-policy: strict-origin-when-cross-origin
server: Vercel
strict-transport-security: max-age=31536000; includeSubDomains
x-content-type-options: nosniff
x-frame-options: DENY
x-powered-by: Next.js

N4 · Pflichtseiten-Links

Impressum: gefunden (verlinkt: https://consilum.de/impressum)
Datenschutzerklärung: gefunden (verlinkt: https://consilum.de/datenschutz)
Geprüfte Pfade: nur Verlinkung auf der Startseite

N5 · TLS/Zertifikate

Ausgestellt für: consilum.de
Aussteller: Let's Encrypt / YR1
Gültig ab: 26.09.2026
Gültig bis: 25.12.2026
Protokoll: TLSv1.3

N6 · TLS/Zertifikate

Server lehnte TLS 1.0/1.1 ab (ERR_SSL_TLSV1_ALERT_PROTOCOL_VERSION: 807FA7F001000000:error:0A00042E:SSL routines:ssl3_read_bytes:tlsv1 alert protocol version:ssl/record/rec_layer_s3.c:918:SSL alert number 70
)

www.consilum.de

1 Hinweis

Dokumentierte Prüfung

Erhobene Prüfbereiche: TLS/Zertifikate, HTTP-Header, Softwaremerkmale, Pflichtseiten-Links.
HTTP-Ziel: https://www.consilum.de/
Aufgelöste IPs: 66.33.60.130, 76.76.21.61

Hinweis

Kein bekanntes Content-Management-System erkannt

Keines der unterstützten CMS-Muster für WordPress, TYPO3, Drupal, Joomla, Shopify, Wix oder Squarespace wurde erkannt. Sichtbar sind „Next.js“ (X-Powered-By) und „Vercel“ (Server).

Relevanz

Version und Aktualität der eingesetzten Komponenten erfordern einen gesonderten Abgleich.

Maßnahme

Halten Sie Ihre Website-Software und Erweiterungen trotzdem aktuell; fragen Sie Ihre Agentur nach dem Update-Rhythmus.

Nachweis N1

Weitere Prüfergebnisse

Prüfung	Feststellung und nächste Schritte
6 von 6 Schutz-Headern gesetzt	Vorhanden: strict-transport-security, content-security-policy, x-frame-options, x-content-type-options, referrer-policy, permissions-policy. Maßnahme Die Anzahl bezieht sich auf vorhandene Header. Für die Bewertung ihrer Schutzwirkung sind die jeweiligen Einstellungen maßgeblich. Nachweis N2
Datenschutzerklärung verlinkt	Auf der Startseite wurde ein Link zur Datenschutzerklärung gefunden. Erreichbarkeit und Inhalt des Ziels sind gesondert zu prüfen. Maßnahme Linkziel und Inhalt anhand der tatsächlichen Datenverarbeitung prüfen und bei neuen Diensten aktualisieren. Nachweis N3
Impressum verlinkt	Auf der Startseite wurde ein Link zum Impressum gefunden. Erreichbarkeit und Inhalt des Ziels sind gesondert zu prüfen. Maßnahme Linkziel und Pflichtangaben prüfen und bei Änderungen der Geschäftsdaten aktualisieren. Nachweis N3
Gültiges Zertifikat, Verschlüsselung aktiv	Ihre Website ist verschlüsselt erreichbar; das Zertifikat ist bis zum 24.12.2026 gültig. Maßnahme Nichts zu tun. Achten Sie darauf, dass die Verlängerung automatisch läuft. Nachweis N4

Weitere Prüfergebnisse

Prüfung	Feststellung und nächste Schritte
TLS 1.3 beobachtet, alte TLS-Versionen abgelehnt	Die Verbindung verwendete TLS 1.3. Ein Verbindungsversuch mit TLS 1.0/1.1 wurde vom Server abgelehnt. Maßnahme Nichts zu tun. Nachweis N5

Technische Nachweise · www.consilum.de

N1 · Softwaremerkmale

X-Powered-By: Next.js
Server: Vercel

N2 · HTTP-Header

Geprüfte Adresse: https://www.consilum.de/ (Status 200)
content-security-policy: default-src 'self'; script-src 'self' 'nonce-axEWvrzVUDJmPIvy3qia98aGZcB9VYL9meu9/5mRhh4=' 'strict-dynamic' https://va.vercel-scripts.com https://connect.facebook.net https://www.googletagmanager.com ...
permissions-policy: camera=(), microphone=(), geolocation=()
referrer-policy: strict-origin-when-cross-origin
server: Vercel
strict-transport-security: max-age=31536000; includeSubDomains
x-content-type-options: nosniff
x-frame-options: DENY
x-powered-by: Next.js

N3 · Pflichtseiten-Links

Impressum: gefunden (verlinkt: https://www.consilum.de/impressum)
Datenschutzerklärung: gefunden (verlinkt: https://www.consilum.de/datenschutz)
Geprüfte Pfade: nur Verlinkung auf der Startseite

N4 · TLS/Zertifikate

Ausgestellt für: www.consilum.de
Aussteller: Let's Encrypt / YR2
Gültig ab: 25.09.2026
Gültig bis: 24.12.2026
Protokoll: TLSv1.3

N5 · TLS/Zertifikate

Server lehnte TLS 1.0/1.1 ab (ERR_SSL_TLSV1_ALERT_PROTOCOL_VERSION:
807FA7F001000000:error:0A00042E:SSL routines:ssl3_read_bytes:tlsv1 alert protocol
version:ssl/record/rec_layer_s3.c:918:SSL alert number 70
)

Die technischen Befunde wurden automatisch erhoben. Der Bericht wird nach fachlicher Prüfung freigegeben.