Checkvanta

heise.de

Sicherheits- und Konfigurationsbericht

Erstellt am: 25.7.2026, 04:11:31 UTC

87
Gesamtscore

Website-Konfiguration

Subscore **87**

DNS

88

- **Nameserver** Erforderlich
  5 Nameserver sind konfiguriert, 5 davon über IPv6 erreichbar.
- **IPv4-Adresse** Erforderlich
  Die Domain löst auf 1 IPv4-Adresse(n) auf, z. B. 193.99.144.80.
- **IPv6-Adresse** Empfohlen
  Die Domain löst auf 1 IPv6-Adresse(n) auf, z. B. 2a02:2e0:3fe:1001:302::.
- **MX-Records** Optional
  Für die Domain sind 4 Mail Server (MX) konfiguriert.
- **CAA-Record** Empfohlen
  6 CAA-Record(s) schränken ein, welche Zertifizierungsstellen Zertifikate ausstellen dürfen.
- **DNSSEC** Empfohlen · Mittel
  DNSSEC ist für diese Domain nicht aktiviert.
  Empfehlung: Aktivieren Sie DNSSEC bei Ihrem DNS-Betreiber und veröffentlichen Sie den DS-Record beim Registrar; reparieren Sie eine gebrochene Kette.

DNS Server

100

- **DNS-Antwort** Erforderlich
  Die Nameserver der Domain liefern DNS-Antworten.
- **Nameserver-Redundanz** Erforderlich
  Die Domain hat 5 Nameserver.
- **Nameserver antworten** Erforderlich
  Alle 5 Nameserver antworten auf Anfragen.
- **Autoritative Antworten** Erforderlich
  Alle Nameserver antworten autoritativ für die Zone.
- **SOA-Serial synchron** Empfohlen
  Alle Nameserver melden dieselbe SOA-Seriennummer.
- **Offene Rekursion** Erforderlich
  Kein Nameserver beantwortet rekursive Anfragen für fremde Domains.
- **Öffentliche NS-Adressen** Erforderlich
  Alle Nameserver-Adressen sind öffentlich erreichbar.
- **Netz-Streuung** Empfohlen
  Die Nameserver verteilen sich auf 9 unterschiedliche Netze.
- **SOA Refresh** Empfohlen
  Der SOA-Refresh-Wert (14400) liegt im empfohlenen Bereich.
- **SOA Retry** Empfohlen
  Der SOA-Retry-Wert (3600) liegt im empfohlenen Bereich.
- **SOA Expire** Empfohlen
  Der SOA-Expire-Wert (604800) liegt im empfohlenen Bereich.
- **SOA Minimum TTL** Empfohlen
  Der SOA-Minimum-TTL-Wert (86400) liegt im empfohlenen Bereich.

- **SOA-Serial-Format** Optional
  Die SOA-Seriennummer (2026072405) folgt der üblichen Konvention (JJJJMMTTnn).
- **NS-Abgleich mit Parent** Empfohlen
  Die NS-Records der Zone stimmen mit der Delegation beim Parent überein.
- **Glue-Records** Empfohlen
  Die Glue-Records beim Parent stimmen mit den tatsächlichen Nameserver-Adressen überein.
- **Primary beim Parent gelistet** Empfohlen
  Der primäre Nameserver (ns.heise.de) ist in der Parent-Delegation enthalten.

HTTP / Security-Header 78

- **Erreichbarkeit** Erforderlich
  Die Seite ist über HTTPS erreichbar.
- **IPv6-Erreichbarkeit** Empfohlen
  Der Webserver ist über IPv6 erreichbar (2a02:2e0:3fe:1001:302::).
- **HTTPS-Redirect** Empfohlen
  Einfaches HTTP wird auf HTTPS umgeleitet.
- **HSTS** Empfohlen
  Ihr Webserver sendet eine HSTS-Richtlinie.
- **Content-Security-Policy** Empfohlen · Mittel
  Es ist kein Content-Security-Policy-Header gesetzt.
  Empfehlung: Definieren Sie eine Content-Security-Policy, die nur die tatsächlich benötigten Quellen erlaubt.
- **X-Frame-Options** Empfohlen
  Ein X-Frame-Options-Header ist gesetzt.
- **X-Content-Type-Options** Empfohlen
  Der X-Content-Type-Options-Header ist auf nosniff gesetzt.
- **Referrer-Policy** Empfohlen · Niedrig
  Es ist kein Referrer-Policy-Header gesetzt.
  Empfehlung: Senden Sie eine Referrer-Policy wie strict-origin-when-cross-origin oder no-referrer.
- **HTTP-Kompression** Optional · Niedrig
  HTTP-Kompression (gzip) ist aktiv – ein Performance-Pluspunkt.
  Empfehlung: Aktivieren Sie HTTP-Kompression (gzip oder Brotli) für Text-Antworten, um Ladezeiten und Bandbreite zu verbessern.
- **security.txt** Empfohlen
  Es ist eine security.txt mit Kontaktadresse veröffentlicht.

TLS 90

- **HTTPS erreichbar** Erforderlich
  Ein HTTPS-Dienst ist erreichbar und hat einen TLS-Handshake abgeschlossen.
- **TLS-Versionen** Erforderlich
  Es werden nur moderne TLS-Versionen (1.2 und/oder 1.3) angeboten.
- **Cipher Suite** Erforderlich
  Die ausgehandelte Cipher Suite (TLS_AES_256_GCM_SHA384) bietet Forward Secrecy.
- **Zertifikat** Erforderlich
  Das Zertifikat ist vertrauenswürdig und für diesen Host gültig.
- **Zertifikatsschlüssel** Erforderlich
  Das Zertifikat verwendet einen starken RSA-Schlüssel (2048 Bit).
- **Zertifikatssignatur** Erforderlich
  Das Zertifikat verwendet einen sicheren Signaturalgorithmus (SHA256-RSA).
- **OCSP-Stapling** Empfohlen · Niedrig
  Der Server liefert keine OCSP-Antwort per Stapling mit.
  Empfehlung: Aktivieren Sie OCSP-Stapling auf dem Webserver.

- **DANE (HTTPS)** Optional · Niedrig
  Für HTTPS sind keine DANE-(TLSA-)Records veröffentlicht.
  Empfehlung: Veröffentlichen Sie bei aktivem DNSSEC TLSA-Records unter `_443._tcp.<host>`, die zu Ihrem Zertifikat passen, und rotieren Sie sie gemeinsam mit dem Zertifikat.

Mail-Konfiguration

Subscore **87**

Mail

78

- **Mail Server (MX)** Erforderlich
  Die Domain hat 4 Mail Server (MX).
- **SPF** Empfohlen
  Es ist ein SPF-Record mit Soft-Fail-Policy (~all) veröffentlicht.
- **DKIM** Empfohlen
  Für 3 Selektor(en) wurden DKIM-Schlüssel gefunden.
- **DMARC** Empfohlen · Mittel
  Es ist ein DMARC-Record veröffentlicht, aber nur im Monitoring-Modus (p=none).
  Empfehlung: Veröffentlichen Sie einen DMARC-Record und heben Sie die Policy, sobald legitime Mail sicher besteht, von `p=none` auf `p=quarantine` und dann `p=reject`. Setzen Sie eine `rua`-Adresse für Aggregate-Reports.
- **BIMI** Optional · Info
  Die Domain veröffentlicht keinen BIMI-Record.
  Empfehlung: Optional: Veröffentlichen Sie ein SVG-Logo (SVG Tiny PS) unter einer HTTPS-URL und einen TXT-Record `default._bimi.<domain>` mit `v=BIMI1; l=<Logo-URL>`. Voraussetzung ist eine DMARC-Policy `p=quarantine` oder `p=reject`; für einige Anbieter zusätzlich ein kostenpflichtiges VMC-Zertifikat.
- **findings.mail.bl.sorbsbadconf.title**
  findings.mail.bl.sorbsbadconf.verdict.clean
- **findings.mail.bl.sorbsnomail.title**
  findings.mail.bl.sorbsnomail.verdict.clean
- **MX über IPv6** Empfohlen · Niedrig
  Kein Mail Server hat eine IPv6-Adresse.
  Empfehlung: Veröffentlichen Sie AAAA-Records für Ihre MX-Hosts und stellen Sie sicher, dass sie SMTP über IPv6 annehmen.
- **STARTTLS** Erforderlich
  Alle Mail Server bieten STARTTLS mit gültigem Zertifikat.
- **Mail-TLS-Version** Erforderlich
  Alle Mail Server handeln eine moderne TLS-Version aus (1.2 oder 1.3).
- **DANE (SMTP)** Empfohlen · Niedrig
  Für die Mail Server sind keine DANE-(TLSA-)Records veröffentlicht.
  Empfehlung: Veröffentlichen Sie bei aktivem DNSSEC TLSA-Records unter `_25._tcp.<mx>`, die zum Zertifikat jedes Mail Servers passen, und rotieren Sie sie gemeinsam mit dem Zertifikat.

Blacklist

100

- **Spamhaus ZEN** Erforderlich
  Nicht auf Spamhaus ZEN gelistet (zen.spamhaus.org).
- **Spamhaus DBL** Erforderlich
  Nicht auf Spamhaus DBL gelistet (dbl.spamhaus.org).
- **SURBL multi** Empfohlen
  Nicht auf SURBL multi gelistet (multi.surbl.org).
- **UCEPROTECT Level 1** Empfohlen
  Nicht auf UCEPROTECT Level 1 gelistet (dnsbl-1.uceprotect.net).
- **UCEPROTECT Level 2** Optional
  Nicht auf UCEPROTECT Level 2 gelistet (dnsbl-2.uceprotect.net).

- **UCEPROTECT Level 3** Optional
  Nicht auf UCEPROTECT Level 3 gelistet (dnsbl-3.uceprotect.net).
- **Barracuda** Erforderlich
  Nicht auf Barracuda gelistet (b.barracudacentral.org).
- **PSBL** Erforderlich
  Nicht auf PSBL gelistet (psbl.surriel.com).
- **SEM FRESH** Empfohlen
  Nicht auf SEM FRESH gelistet (fresh.spameatingmonkey.net).
- **SEM Blacklist** Empfohlen
  Nicht auf SEM Blacklist gelistet (bl.spameatingmonkey.net).
- **0SPAM** Erforderlich
  Nicht auf 0SPAM gelistet (bl.0spam.org).
- **BLOCKLIST.DE** Erforderlich
  Nicht auf BLOCKLIST.DE gelistet (bl.blocklist.de).