Checkvanta

web.de

Sicherheits- und Konfigurationsbericht

Erstellt am: 25.7.2026, 04:09:12 UTC

88

Gesamtscore

Website-Konfiguration

Subscore 90

DNS

95

- **Nameserver** Erforderlich
  4 Nameserver sind konfiguriert, 4 davon über IPv6 erreichbar.
- **IPv4-Adresse** Erforderlich
  Die Domain löst auf 2 IPv4-Adresse(n) auf, z. B. 82.165.229.138.
- **IPv6-Adresse** Empfohlen · Niedrig
  Die Domain hat keinen AAAA-Record (IPv6).
  Empfehlung: Ergänzen Sie einen AAAA-Record, damit reine IPv6-Clients die Seite erreichen.
- **MX-Records** Optional
  Für die Domain sind 2 Mail Server (MX) konfiguriert.
- **CAA-Record** Empfohlen
  6 CAA-Record(s) schränken ein, welche Zertifizierungsstellen Zertifikate ausstellen dürfen.
- **DNSSEC** Empfohlen
  DNSSEC ist aktiviert und die Validierungskette ist intakt.

DNS Server

100

- **DNS-Antwort** Erforderlich
  Die Nameserver der Domain liefern DNS-Antworten.
- **Nameserver-Redundanz** Erforderlich
  Die Domain hat 4 Nameserver.
- **Nameserver antworten** Erforderlich
  Alle 4 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 10 unterschiedliche Netze.
- **SOA Refresh** Empfohlen
  Der SOA-Refresh-Wert (28800) liegt im empfohlenen Bereich.
- **SOA Retry** Empfohlen
  Der SOA-Retry-Wert (7200) 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 (600) liegt im empfohlenen Bereich.

- **SOA-Serial-Format** Optional · Niedrig
  Die SOA-Seriennummer (2005104439) folgt nicht der üblichen Konvention (JJJJMMTTnn).
  Empfehlung: Falls Sie die Zone selbst pflegen: Verwenden Sie das Format JJJJMMTTnn und erhöhen Sie die Seriennummer bei jeder Änderung.
- **NS-Abgleich mit Parent** Empfohlen
  Die NS-Records der Zone stimmen mit der Delegation beim Parent überein.
- **Glue-Records** Empfohlen
  Es werden keine Glue-Records benötigt (keine Nameserver innerhalb der eigenen Zone).
- **Primary beim Parent gelistet** Empfohlen
  Der primäre Nameserver (ns-webde.ui-dns.de) ist in der Parent-Delegation enthalten.

HTTP / Security-Header 80

- **Erreichbarkeit** Erforderlich
  Die Seite ist über HTTPS erreichbar.
- **IPv6-Erreichbarkeit** Empfohlen · Niedrig
  Die Domain hat keinen AAAA-Record, daher ist der Webserver über IPv6 nicht erreichbar.
  Empfehlung: Veröffentlichen Sie einen AAAA-Record und stellen Sie sicher, dass der Webserver IPv6-Verbindungen auf Port 443 annimmt.
- **HTTPS-Redirect** Empfohlen
  Einfaches HTTP wird auf HTTPS umgeleitet.
- **HSTS** Empfohlen
  Ihr Webserver sendet eine HSTS-Richtlinie.
- **Content-Security-Policy** Empfohlen
  Ein Content-Security-Policy-Header ist gesetzt.
- **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
  Ein Referrer-Policy-Header ist gesetzt.
- **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.
- **HTTP/2** Empfohlen · Niedrig
  Der Webserver unterstützt nur HTTP/1.x.
  Empfehlung: Aktivieren Sie HTTP/2 in Ihrem Webserver bzw. Reverse Proxy (bei modernen Versionen von nginx, Apache, Caddy oder Traefik meist nur ein Konfigurationsschalter).
- **HTTP/3** Optional · Info
  Der Webserver kündigt kein HTTP/3 (QUIC) an.
  Empfehlung: Optional: Aktivieren Sie HTTP/3 in Ihrem Webserver/Reverse Proxy und stellen Sie sicher, dass UDP-Port 443 in der Firewall geöffnet ist.
- **Cookie-Sicherheit** Empfohlen · Niedrig
  5 von 5 Cookie(s) fehlen wichtige Sicherheits-Flags.
  Empfehlung: Setzen Sie sensible Cookies mit `Secure`, `HttpOnly` und einem passenden `SameSite`-Wert (`Lax` oder `Strict`). `SameSite=None` ist nur mit `Secure` und nur für bewusst seitenübergreifende Cookies sinnvoll.
- **Mixed Content** Erforderlich
  Die Seite bindet keine Ressourcen über unverschlüsseltes HTTP ein.
- **Subresource Integrity** Empfohlen · Info
  Die Seite bindet keine externen Skripte/Stylesheets ein, für die SRI sinnvoll wäre.

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 (3072 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 85

Mail 83

- **Mail Server (MX)** Erforderlich
  Die Domain hat 2 Mail Server (MX).
- **SPF** Empfohlen · Mittel
  Es ist ein SPF-Record veröffentlicht, seine Policy ist aber freizügig.
  Empfehlung: Veröffentlichen Sie einen SPF-Record, der Ihre legitimen Absender auflistet und mit `-all` (Hard Fail) endet. Halten Sie die Zahl der DNS-Lookups unter dem Limit von zehn.
- **DKIM** Empfohlen
  DKIM ist eingerichtet: Der `_domainkey`-Namespace der Domain enthält Selektoren – die einzelnen Selektor-Namen lassen sich aus dem DNS nicht auflisten.
- **DMARC** Empfohlen
  Es ist ein DMARC-Record mit durchsetzender Policy (p=quarantine) veröffentlicht.
- **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.
- **MTA-STS** Empfohlen
  MTA-STS ist eingerichtet, aber im Modus „testing“ – Verstöße werden nur gemeldet, nicht erzwungen.
- **TLS-RPT** Optional
  Die Domain veröffentlicht einen gültigen TLS-RPT-Record.
- **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
  Es sind DANE-(TLSA-)Records veröffentlicht, die zu den Zertifikaten der Mail Server passen.
- **Reverse DNS (PTR)** Empfohlen
  Alle geprüften Mailserver-IPs haben einen PTR-Record.
- **Open Relay** Erforderlich
  Kein Mailserver nimmt Mail an fremde Empfänger zur Weiterleitung an (kein Open Relay).

Blacklist 88

- **Spamhaus ZEN** Erforderlich
  Nicht auf Spamhaus ZEN gelistet (zen.spamhaus.org).
- **Spamhaus DBL** Erforderlich
  Nicht auf Spamhaus DBL gelistet (dbl.spamhaus.org).
- **Barracuda** Erforderlich
  Nicht auf Barracuda gelistet (b.barracudacentral.org).
- **SpamCop** Erforderlich
  Nicht auf SpamCop gelistet (bl.spamcop.net).
- **PSBL** Erforderlich
  Nicht auf PSBL gelistet (psbl.surriel.com).
- **0SPAM** Erforderlich
  Nicht auf 0SPAM gelistet (bl.0spam.org).
- **BLOCKLIST.DE** Erforderlich
  Nicht auf BLOCKLIST.DE gelistet (bl.blocklist.de).
- **SURBL multi** Empfohlen
  Nicht auf SURBL multi gelistet (multi.surbl.org).
- **SEM FRESH** Empfohlen
  Nicht auf SEM FRESH gelistet (fresh.spameatingmonkey.net).
- **SEM Blacklist** Empfohlen
  Nicht auf SEM Blacklist gelistet (bl.spameatingmonkey.net).
- **SEM Backscatter** Empfohlen
  Nicht auf SEM Backscatter gelistet (backscatter.spameatingmonkey.net).
- **SPFBL** Empfohlen
  Nicht auf SPFBL gelistet (dnsbl.spfbl.net).
- **GBUdb Truncate** Empfohlen
  Nicht auf GBUdb Truncate gelistet (truncate.gbudb.net).
- **SpamRATS RATS-Spam** Empfohlen
  Nicht auf SpamRATS RATS-Spam gelistet (spam.spamrats.com).
- **SpamRATS RATS-Dyna** Empfohlen
  Nicht auf SpamRATS RATS-Dyna gelistet (dyna.spamrats.com).
- **SpamRATS RATS-NoPtr** Empfohlen
  Nicht auf SpamRATS RATS-NoPtr gelistet (noptr.spamrats.com).
- **JustSpam** Empfohlen
  Nicht auf JustSpam gelistet (dnsbl.justspam.org).
- **Fabel Spamsources** Empfohlen · Mittel
  Auf Fabel Spamsources gelistet (spamsources.fabel.dk): mx-ha03.web.de (212.227.15.154).
  Empfehlung: Prüfen Sie beim Betreiber der Liste (spamsources.fabel.dk) den Grund der Listung und stellen Sie einen Delisting-Antrag, nachdem Sie die Ursache (z. B. kompromittiertes Konto, offenes Relay, Spam-Versand) behoben haben.
- **s5h.net** Empfohlen
  Nicht auf s5h.net gelistet (all.s5h.net).

- **DroneBL** Empfohlen
  Nicht auf DroneBL gelistet (dnsbl.dronebl.org).
- **InterServer RBL** Empfohlen
  Nicht auf InterServer RBL gelistet (rbl.interserver.net).
- **Mailspike** Empfohlen
  Nicht auf Mailspike gelistet (z.mailspike.net).
- **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).