Checkvanta

facebook.com

Sicherheits- und Konfigurationsbericht

Erstellt am: 25.7.2026, 17:34:33 UTC

86
Gesamtscore

Website-Konfiguration

Subscore **86**

DNS

88

- **Nameserver** Erforderlich
  4 Nameserver sind konfiguriert, 4 davon über IPv6 erreichbar.
- **IPv4-Adresse** Erforderlich
  Die Domain löst auf 1 IPv4-Adresse(n) auf, z. B. 157.240.17.35.
- **IPv6-Adresse** Empfohlen
  Die Domain löst auf 1 IPv6-Adresse(n) auf, z. B. 2a03:2880:f15b:83:face:b00c:0:25de.
- **MX-Records** Optional
  Für die Domain sind 1 Mail Server (MX) konfiguriert.
- **CAA-Record** Empfohlen
  1 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 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 8 unterschiedliche Netze.
- **Nameserver über IPv6** Empfohlen
  4 Nameserver sind über IPv6 erreichbar.
- **SOA Refresh** Empfohlen
  Der SOA-Refresh-Wert (14400) liegt im empfohlenen Bereich.
- **SOA Retry** Empfohlen
  Der SOA-Retry-Wert (1800) 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 (300) liegt im empfohlenen Bereich.
- **SOA-Serial-Format** Optional
  Die SOA-Seriennummer (4207849484) ist ein gültiger, aufsteigender Integer (wie bei vielen Managed-DNS-Anbietern üblich).
- **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 (a.ns.facebook.com) ist in der Parent-Delegation enthalten.

HTTP / Security-Header 90

- **Erreichbarkeit** Erforderlich
  Die Seite ist über HTTPS erreichbar.
- **IPv6-Erreichbarkeit** Empfohlen
  Der Webserver ist über IPv6 erreichbar (2a03:2880:f15b:83:face:b00c:0:25de).
- **Gleiche Website über IPv6** Empfohlen · Niedrig
  Über IPv6 wird ein deutlich anderer Inhalt ausgeliefert als über IPv4 (nur 33% Textähnlichkeit).
  Empfehlung: Stellen Sie sicher, dass der IPv6-Server dieselben Inhalte ausliefert wie der IPv4-Server (Ähnlichkeit aktuell 33%). Meist liegt es an einem separaten, nicht synchronisierten IPv6-Backend.
- **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 · 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
  HTTP-Kompression (br) ist aktiv – ein Performance-Pluspunkt.
- **security.txt** Empfohlen
  Es ist eine security.txt mit Kontaktadresse veröffentlicht.
- **HTTP/2** Empfohlen
  Der Webserver unterstützt HTTP/2.
- **HTTP/3** Optional
  Der Webserver kündigt HTTP/3 (QUIC) per Alt-Svc-Header an.
- **Cookie-Sicherheit** Empfohlen · Info
  Die Startseite setzt keine Cookies, die geprüft werden könnten.
- **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.

RPKI 100

- **RPKI (Webserver)** Empfohlen
  Die Route-Origin-Autorisierung des Webservers ist per RPKI gültig.
- **RPKI (Nameserver)** Empfohlen
  Die Route-Origin-Autorisierung der Nameserver ist per RPKI gültig.

TLS 65

- **HTTPS erreichbar** Erforderlich
  Ein HTTPS-Dienst ist erreichbar und hat einen TLS-Handshake abgeschlossen.
- **TLS-Versionen** Erforderlich · Hoch
  Der Server bietet noch eine veraltete TLS-Version (1.0 oder 1.1) an.
  Empfehlung: Deaktivieren Sie TLS 1.0 und 1.1 in Ihrer Webserver- oder CDN-Konfiguration und bieten Sie nur TLS 1.2 und 1.3 an.
- **Cipher Suite** Erforderlich
  Die ausgehandelte Cipher Suite (TLS_AES_128_GCM_SHA256) bietet Forward Secrecy.
- **Zertifikat** Erforderlich
  Das Zertifikat ist vertrauenswürdig und für diesen Host gültig.
- **Zertifikatsschlüssel** Erforderlich
  Das Zertifikat verwendet einen starken ECDSA-Schlüssel (256 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 · Info
  Für HTTPS sind keine DANE-(TLSA-)Records veröffentlicht – für Web ein optionaler Bonus, kein Mangel.
- **Cipher-Reihenfolge** Empfohlen
  Mit TLS 1.3 wählt der Server aus einem kleinen Satz durchweg sicherer Verfahren – die Reihenfolge ist unkritisch.
- **Key Exchange** Erforderlich
  Der Schlüsselaustausch nutzt ECDHE mit Hash SHA256 – Forward Secrecy ist gegeben.
- **TLS-Kompression** Erforderlich
  TLS 1.3 kennt keine Record-Kompression – die Schwachstelle entfällt.
- **Renegotiation** Erforderlich
  TLS 1.3 hat Renegotiation vollständig entfernt – kein Angriffsvektor.
- **Extended Master Secret** Empfohlen
  Der Schlüsselplan von TLS 1.3 ersetzt Extended Master Secret – die Schwäche entfällt.
- **TLS 1.3 0-RTT (Early Data)** Optional · Niedrig
  Der Server akzeptiert TLS-1.3-0-RTT (max. 0 Bytes Early Data). Achten Sie auf Replay-Schutz.
  Empfehlung: Aktivieren Sie 0-RTT nur, wenn Ihr Server wirksamen Replay-Schutz bietet und ausschließlich sichere, idempotente Anfragen als Early Data zulässt. Im Zweifel deaktivieren.

Mail-Konfiguration

Subscore 86

Mail 71

- **Mail Server (MX)** Erforderlich
  Die Domain hat 1 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 · Mittel
  Der DKIM-Selektor ist vorhanden, aber der Schlüssel wurde widerrufen (leerer `p=`-Wert).
  Empfehlung: Veröffentlichen Sie einen DKIM-Schlüssel mit mindestens 2048 bit (RSA) unter `<selector>._domainkey.<domain>` und aktivieren Sie die DKIM-Signierung auf Ihrem Mail Server. Widerrufene (leere) Schlüssel sollten entfernt werden, sobald keine alten Mails mehr damit verifiziert werden müssen.
- **DMARC** Empfohlen
  Es ist ein DMARC-Record mit durchsetzender Policy (p=reject) 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
  Alle Mail Server haben eine IPv6-Adresse.
- **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.
- **Cipher Suite (Mail)** Empfohlen
  Alle Mailserver nutzen Cipher Suites mit Forward Secrecy.
- **Mailserver-Zertifikat** Erforderlich
  Alle Mailserver präsentieren ein gültiges, zum Hostnamen passendes Zertifikat.
- **Mailserver-Schlüssel** Erforderlich
  Die Zertifikatsschlüssel aller Mailserver sind ausreichend stark.
- **Mailserver-Signatur** Erforderlich
  Die Zertifikate aller Mailserver verwenden eine sichere Signatur.
- **TLS-Kompression (Mail)** Erforderlich
  Kein Mailserver hat TLS-Kompression aktiviert.
- **Renegotiation (Mail)** Erforderlich
  Alle Mailserver unterstützen sichere Renegotiation bzw. nutzen TLS 1.3.
- **Extended Master Secret (Mail)** Empfohlen
  Alle Mailserver unterstützen Extended Master Secret bzw. nutzen TLS 1.3.
- **Reverse DNS (PTR)** Empfohlen
  Alle geprüften Mailserver-IPs haben einen PTR-Record.
- **Open Relay** Erforderlich · Info
  Der Open-Relay-Test konnte nicht durchgeführt werden (keine SMTP-Verbindung).

Blacklist 100

- **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
  Nicht auf Fabel Spamsources gelistet (spamsources.fabel.dk).
- **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).

RPKI (Mail) **95**

- **RPKI (Mailserver)** Empfohlen · Niedrig
  Für die IP-Adressen der Mailserver existiert keine RPKI-Autorisierung (ROA).
  Empfehlung: Veröffentlichen Sie für die IP-Präfixe der Mailserver bei Ihrem Netzbetreiber bzw. RIR ein ROA (Route Origin Authorisation), das die korrekte announcierende ASN und maximale Präfixlänge autorisiert. Bei „ungültig“ prüfen Sie ASN und maximale Präfixlänge im bestehenden ROA.