Checkvanta

swiss.com

Sicherheits- und Konfigurationsbericht

Erstellt am: 25.7.2026, 13:59:36 UTC

81

Gesamtscore

Website-Konfiguration

Subscore **88**

DNS

73

- **Nameserver** Erforderlich · Niedrig
  2 Nameserver sind konfiguriert, aber keiner ist über IPv6 erreichbar.
  Empfehlung: Konfigurieren Sie mindestens zwei Nameserver und stellen Sie sicher, dass diese auch über IPv6 erreichbar sind.
- **IPv4-Adresse** Erforderlich
  Die Domain löst auf 1 IPv4-Adresse(n) auf, z. B. 146.216.3.74.
- **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 · Niedrig
  Es ist kein CAA-Record konfiguriert.
  Empfehlung: Ergänzen Sie einen CAA-Record mit Ihrer Zertifizierungsstelle.
- **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

88

- **DNS-Antwort** Erforderlich
  Die Nameserver der Domain liefern DNS-Antworten.
- **Nameserver-Redundanz** Erforderlich
  Die Domain hat 2 Nameserver.
- **Nameserver antworten** Erforderlich
  Alle 2 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 2 unterschiedliche Netze.
- **Nameserver über IPv6** Empfohlen · Mittel
  Kein Nameserver der Domain hat eine IPv6-Adresse (AAAA).
  Empfehlung: Sorgen Sie dafür, dass mindestens zwei Nameserver einen AAAA-Record haben und DNS-Anfragen über IPv6 auf Port 53 beantworten.
- **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 (1209600) liegt im empfohlenen Bereich.
- **SOA Minimum TTL** Empfohlen
  Der SOA-Minimum-TTL-Wert (900) liegt im empfohlenen Bereich.
- **SOA-Serial-Format** Optional
  Die SOA-Seriennummer (2026072401) 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 (ns1.swiss.com) ist in der Parent-Delegation enthalten.

HTTP / Security-Header 90

- **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.
- **Gleiche Website über IPv6** Empfohlen · Info
  Die Domain hat keinen AAAA-Record – ein IPv6/IPv4-Vergleich entfällt.
- **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
  HTTP-Kompression (gzip) 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 · 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
  1 von 1 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.

RPKI 95

- **RPKI (Webserver)** Empfohlen · Niedrig
  Für die IP-Adressen des Webservers existiert keine RPKI-Autorisierung (ROA).
  Empfehlung: Veröffentlichen Sie für die IP-Präfixe des Webservers 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.
- **RPKI (Nameserver)** Empfohlen
  Die Route-Origin-Autorisierung der Nameserver ist per RPKI gültig.

TLS 95

- **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_ECDHE_RSA_WITH_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 RSA-Schlüssel (4096 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
  Der Server erzwingt seine eigene Cipher-Reihenfolge.
- **Key Exchange** Erforderlich
  Der Schlüsselaustausch nutzt ECDHE mit Hash SHA256 – Forward Secrecy ist gegeben.
- **TLS-Kompression** Erforderlich
  TLS-Kompression ist deaktiviert.
- **Renegotiation** Erforderlich
  Der Server unterstützt sichere Renegotiation und lässt keine Client-initiierte Renegotiation zu.
- **Extended Master Secret** Empfohlen
  Der Server unterstützt Extended Master Secret (RFC 7627).
- **TLS 1.3 0-RTT (Early Data)** Optional · Info
  Der Server nutzt kein TLS 1.3; 0-RTT ist damit nicht anwendbar.

Mail-Konfiguration

Subscore **65**

Mail 23

- **Mail Server (MX)** Erforderlich
  Die Domain hat 2 Mail Server (MX).

- **SPF** Empfohlen · Mittel
  Es ist kein SPF-Record veröffentlicht.
  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=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 · Niedrig
  Die Domain veröffentlicht keine MTA-STS-Policy.
  Empfehlung: Veröffentlichen Sie den TXT-Record `_mta-sts.<domain>` sowie eine gültige Policy-Datei unter `https://mta-sts.<domain>/.well-known/mta-sts.txt` mit `version`, `mode`, `max_age` und Ihren `mx`-Einträgen. Beginnen Sie mit `mode: testing` und wechseln Sie nach Prüfung der Reports auf `mode: enforce`.
- **TLS-RPT** Optional · Niedrig
  Die Domain veröffentlicht keinen TLS-RPT-Record.
  Empfehlung: Veröffentlichen Sie einen TXT-Record `_smtp._tls.<domain>` mit `v=TLSRPTv1; rua=mailto:tls-reports@<domain>` (oder einer HTTPS-Reporting-URL).
- **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.
- **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 · Niedrig
  1 von 2 Mailserver-IPs fehlt ein PTR-Record.
  Empfehlung: Legen Sie beim Betreiber der IP-Adresse (Hoster/Provider) einen PTR-Record an, der auf den Hostnamen Ihres Mailservers zeigt – idealerweise mit passendem Forward-Record (A/AAAA) zurück auf dieselbe IP.

- **Open Relay** Erforderlich · Kritisch
  2 Mailserver akzeptiert(en) die Weiterleitung an eine fremde Zieladresse (Open Relay).
  Empfehlung: Konfigurieren Sie Ihren Mailserver so, dass er Weiterleitung nur für authentifizierte Nutzer bzw. eigene Domains zulässt (`smtpd_relay_restrictions` bei Postfix o. Ä.) und fremde Empfänger ohne Authentifizierung ablehnt.

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) 100

- **RPKI (Mailserver)** Empfohlen
  Die Route-Origin-Autorisierung der Mailserver ist per RPKI gültig.