Checkvanta

watson.ch

Sicherheits- und Konfigurationsbericht

Erstellt am: 25.7.2026, 04:13:53 UTC

87
Gesamtscore

Website-Konfiguration

Subscore **84**

DNS

83

- **Nameserver** Erforderlich
  4 Nameserver sind konfiguriert, 4 davon über IPv6 erreichbar.
- **IPv4-Adresse** Erforderlich
  Die Domain löst auf 4 IPv4-Adresse(n) auf, z. B. 51.89.11.70.
- **IPv6-Adresse** Empfohlen
  Die Domain löst auf 4 IPv6-Adresse(n) auf, z. B. 2a01:4f8:2b02:24b::2.
- **MX-Records** Optional
  Für die Domain sind 5 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

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.
- **SOA Refresh** Empfohlen
  Der SOA-Refresh-Wert (3600) liegt im empfohlenen Bereich.
- **SOA Retry** Empfohlen
  Der SOA-Retry-Wert (900) 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 (300) liegt im empfohlenen Bereich.

- **SOA-Serial-Format** Optional · Niedrig
  Die SOA-Seriennummer (1782891088) 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
  Die Glue-Records beim Parent stimmen mit den tatsächlichen Nameserver-Adressen überein.
- **Primary beim Parent gelistet** Empfohlen
  Der primäre Nameserver (dns1.watson.ch) ist in der Parent-Delegation enthalten.

HTTP / Security-Header 61

- **Erreichbarkeit** Erforderlich
  Die Seite ist über HTTPS erreichbar.
- **IPv6-Erreichbarkeit** Empfohlen
  Der Webserver ist über IPv6 erreichbar (2a01:4f8:2b02:eaf::2).
- **HTTPS-Redirect** Empfohlen
  Einfaches HTTP wird auf HTTPS umgeleitet.
- **HSTS** Empfohlen · Mittel
  Ihr Webserver sendet keine HSTS-Richtlinie.
  Empfehlung: HSTS setzt voraus, dass Ihre Website vollständig über HTTPS funktioniert – inklusive eines gültigen Zertifikats einer öffentlich vertrauenswürdigen Zertifizierungsstelle. Gehen Sie schrittweise vor:

  1. Stellen Sie sicher, dass Ihre Website jetzt und dauerhaft vollständig über HTTPS funktioniert (z. B. mit einem verlässlichen Zertifikats-Rollover-Prozess).
  2. Erhöhen Sie die HSTS-Gültigkeitsdauer stufenweise. Prüfen Sie nach jeder Stufe auf Erreichbarkeitsprobleme und warten Sie die volle `max-age`-Dauer ab, bevor Sie zur nächsten Stufe wechseln.
  3. Wiederholen Sie Schritt 1–2 für jede Subdomain, die Sie absichern möchten. Nutzen Sie `includeSubDomains` nur, wenn wirklich alle (verschachtelten) Subdomains HTTPS zuverlässig unterstützen.
  4. Nutzen Sie `preload` nur mit grosser Vorsicht — es ist schwer rückgängig zu machen und kann die Erreichbarkeit der gesamten Domain samt Subdomains beeinträchtigen.
- **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 · Niedrig
  Es ist kein X-Frame-Options-Header gesetzt.
  Empfehlung: Senden Sie X-Frame-Options: DENY oder SAMEORIGIN, oder eine gleichwertige frame-ancestors-CSP-Direktive.
- **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 · Niedrig
  Es ist keine security.txt veröffentlicht.
  Empfehlung: Veröffentlichen Sie eine signierte `/.well-known/security.txt` mit mindestens einem `Contact:`- und einem `Expires:`-Feld.
- **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 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_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 (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.
- **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.

Mail-Konfiguration

Subscore **95**

Mail 90

- **Mail Server (MX)** Erforderlich
  Die Domain hat 5 Mail Server (MX).
- **SPF** Empfohlen
  Es ist ein SPF-Record mit Soft-Fail-Policy (~all) veröffentlicht.

- **DKIM** Empfohlen
  DKIM ist eingerichtet, der Schlüssel ist mit 1024 bit aber nur knapp ausreichend.
- **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
  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
  Kein Mailserver nimmt Mail an fremde Empfänger zur Weiterleitung an (kein Open Relay).

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.