

Dein Verschlüsselungs-Check

Drei Bereiche, neun Kriterien, maximal 100 Punkte. Geh die Kriterien durch, kreuz an, was bei Deiner Domain erfüllt ist, und zähl die Punkte zusammen.

Wo Du nachsiehst: Vieles siehst Du direkt im do.de-Kundenmenü. Für Einstellungen auf Deinem Web- oder Mailserver hilft der kostenlose Testdienst internet.nl (Website-Test und E-Mail-Test): Domain eingeben, kurz warten, Ergebnis ablesen.

Domain: _____

Datum: _____

1 Deine Website

max. 40 Punkte

☐ HTTPS mit gültigem Zertifikat +10

Die Verbindung zu Deiner Website ist verschlüsselt.

Prüfung: Ruf Deine Website auf. Beginnt die Adresse mit https:// und zeigt der Browser keine Warnung, dann ist Dein Zertifikat gültig. Zertifikate von do.de siehst Du zusätzlich in der SSL-Übersicht im Kundenmenü.

☐ HTTPS wird per HSTS erzwungen +10

Browser rufen Deine Website nur noch verschlüsselt auf.

Prüfung: HSTS ist eine Einstellung auf Deinem Webserver, im Browser siehst Du sie nicht. Am einfachsten prüfst Du sie mit dem Website-Test auf internet.nl. Alternativ fragst Du Deinen Hoster.

☐ Aktuelle TLS-Protokolle +10

TLS 1.2 und 1.3 sind aktiv, die unsicheren Versionen 1.0 und 1.1 abgeschaltet.

Prüfung: Welche Versionen aktiv sind, legt Dein Hoster fest. Im Zweifelsfall zeigt Dir der Website-Test auf internet.nl, ob noch veraltete Versionen im Einsatz sind.

☐ Zertifikate erneuern sich automatisch +10

Zertifikate erneuern sich von selbst, auch für Subdomains. Seit März 2026 gelten sie höchstens 200 Tage.

Prüfung: Hast Du Dein Zertifikat bei do.de gekauft, verlängert es sich automatisch. Du siehst Deine Zertifikate in der SSL-Übersicht im Kundenmenü. Bei Zertifikaten von Dritten gilt: Prüfe in Deinem Hosting-Menü oder per Anfrage bei Deinem Hoster, ob sich Deine Zertifikate automatisch verlängern. Musst Du selbst an die Verlängerung denken, gibt es hier keine Punkte.

Zwischensumme _____ / 40

2 Deine E-Mails

max. 35 Punkte

☐ Dein Mailserver unterstützt Verschlüsselung per STARTTLS +10

Mailserver bieten einander eine verschlüsselte Verbindung an.

Prüfung: STARTTLS wird weithin unterstützt und direkt von Deinem Mailanbieter eingerichtet. Gewissheit, ob Dein Mailserver verschlüsselte Verbindungen annimmt, bringt Dir der E-Mail-Test auf internet.nl.

☐ MTA-STS und TLS-Reporting +15

Mails an Deine Domain dürfen nur verschlüsselt zugestellt werden.

Prüfung: Öffne die DNS-Verwaltung in Deinem do.de-Kundenmenü (Domains → Einstellungen → Weiterleitung / DNS) und prüfe, ob dort ein TXT-Eintrag mit dem Namen `_mta-sts` angelegt ist.

☐ DANE für Deinen Mailserver (erfordert DNSSEC) +10

Ein Fingerabdruck im DNS sorgt dafür, dass Mails nur verschlüsselt beim echten Server ankommen.

Prüfung: Der E-Mail-Test auf internet.nl zeigt Dir, ob DANE aktiv ist. Betreibst Du einen eigenen Mailserver, siehst Du den zugehörigen TLSA-Eintrag auch in den DNS-Einträgen Deiner Domain im do.de-Kundenmenü. Beachte: Ohne DNSSEC ist dieses Kriterium nicht erfüllbar.

Zwischensumme _____ / 35

3 Das Fundament im DNS

max. 25 Punkte

Die beiden hierfür angesetzten Kriterien verschlüsseln zwar selbst nichts, sie sichern aber die Vertrauenskette ab, auf der Deine Verschlüsselung aufbaut.

☐ DNSSEC aktiv +15

Digitale Unterschrift für Deine DNS-Einträge und Voraussetzung für DANE.

Prüfung: Im do.de-Kundenmenü zeigt das DNSSEC-Symbol in den Domain-Einstellungen, ob DNSSEC aktiv ist. Liegt Deine Domain bei einem anderen Anbieter, prüfst Du es mit dem Website-Test auf internet.nl.

☐ CAA-Eintrag hinterlegt +10

Legt fest, welche Zertifizierungsstellen SSL-Zertifikate für Deine Domain ausstellen dürfen.

Prüfung: Öffne in Deinem do.de-Kundenmenü die DNS-Verwaltung Deiner Domain (Domains → Einstellungen → Weiterleitung / DNS). Gibt es dort einen Eintrag vom Typ CAA, bekommst Du die Punkte.

Zwischensumme _____ / 25

Mein Verschlüsselungs-Score _____ / 100

Auswertung: Wo steht Deine Domain?

0–30 Punkte Mangelhaft Die Basisverschlüsselung fehlt oder ist unvollständig. Starte mit HTTPS und automatischer Zertifikatsverlängerung.	35–60 Punkte Grundschutz Deine Website ist weitgehend sauber verschlüsselt. Der Weg Deiner E-Mails und das DNS sind noch offen.	65–85 Punkte Gut aufgestellt Ein solider Stand. Meist fehlen hier nur noch DNSSEC, DANE oder MTA-STS.	90–100 Punkte Vorbildlich Verschlüsselung plus abgesicherte Vertrauenskette – damit bist Du auf dem aktuellen Stand der Technik.
--	--	--	---

Bis zu 35 Punkte in 15 Minuten

Siehst Du noch Luft nach oben bei Deinem Score? Dann starte mit diesen drei Schritten, denn sie bringen die meisten Punkte bei geringstem Aufwand.

- 1 DNSSEC aktivieren** DO.DE-KUNDENMENÜ +15 Punkte
Nutzst Du do.de-Nameserver, aktivierst Du DNSSEC mit einem Klick auf das DNSSEC-Symbol in den Domain-Einstellungen. Bei eigenen Nameservern legst Du DNSSEC manuell an. Anleitung: do.de/wiki/dnssec-einrichten
- 2 CAA-Eintrag setzen** DO.DE-KUNDENMENÜ +10 Punkte
Trag in Deiner DNS-Verwaltung ein, welche Zertifizierungsstelle Zertifikate ausstellen darf, zum Beispiel `0 issue "letsencrypt.org"`. Wichtig: Frag vorher Deinen Hoster, welche Stelle er nutzt, sonst sperrst Du Dein eigenes Zertifikat aus. Anleitung: do.de/wiki/dns
- 3 HSTS einschalten** BEI DEINEM HOSTER +10 Punkte
Bei vielen Hostern ist das ein Schalter im Menü, bei WordPress hilft ein Sicherheits-Plugin. Wichtig: Alle Seiten müssen zuverlässig per HTTPS erreichbar sein.



Alle Erklärungen und Anleitungen

Was hinter jedem Kriterium steckt und wie Du es Schritt für Schritt umsetzt, liest Du im ausführlichen Artikel. Einfach QR-Code scannen.

do.de/blog/verschluesselungs-check