

# Wolf-Agents Security Report

## E-Mail-Security-Check

Ausgabe: de / none / 2026-10-05.2 · Technische Ergebnisse, Erläuterungen und Fachquellen ohne zusätzliche rechtliche Einordnung. · Hinweise geprüft: 2026-10-05

### Prüfgegenstand

wolf-agents.com

Prüfzeitpunkt: 06.10.2026, 22:31 Uhr (MESZ)

Dokument erzeugt am: 06.10.2026, 22:55 Uhr (MESZ)

Die Erläuterungen in diesem Bericht wurden mit KI erstellt. Vorhandene Messwerte wurden automatisiert erhoben; Bewertungen folgen festen Regeln. Zur Entstehung: <https://wolf-agents.com/ki-hinweis/>

Katalogstand der Messung: 1.9

Reportdarstellung: 2026-10-05.legal-2

Scan-Kennung: 4e500d11-959a-4e48-9f42-ccffcd4e56c3

Reportmodell: 1.10

Vertraulichkeit: für den Empfänger und von ihm benannte Dritte

Aussteller: Wolf-Agents.com - kontakt@wolf-agents.com

### Gesamtbild

**A**

118 von 142 Punkten - Gute Konfiguration im Außencheck

21 Prüfpunkte: 11 bestanden, 0 nicht bestanden, 2 nicht auswertbar, 7 Hinweise, 1 nicht anwendbar.

2 von 21 Prüfpunkten sind mit den gespeicherten Daten nicht abschließend auswertbar. Der volle Modellnenner bleibt bestehen; Messausfälle verbessern die Gesamtquote nicht. Im Lauf gespeicherte Messabdeckung nach möglichen Punkten: 124 von 142. Die Gruppennenner der Punktebilanz summieren sich auf 126; darin sind 2 mögliche Produktpunkte nicht anwendbarer Prüfpunkte enthalten. Diese erklären die Differenz zur gespeicherten Messabdeckung, die sie nicht mitzählt. Die heutige Befundbilanz kann wegen korrigierter Interpretation davon abweichen.

### Schneller Einstieg

Hinweise, nicht anwendbare und bestandene Checks stehen im vollständigen Katalog unten. Die Kennungen bezeichnen die Abschnitte auch im Ausdruck.

#### Bestätigte negative Befunde

Im dokumentierten Prüfumfang sind keine bestätigten negativen Befunde enthalten.

#### Offen / nicht auswertbar

[smtp-tls](#) · nicht auswertbar · [SMTP TLS-Zertifikat](#)

[smtp-zertifikat](#) · nicht auswertbar · [SMTP-Zertifikatsstatus](#)

### Grenzen der Aussage

- Die Prüfung ist unauthentifiziert und erfolgt ausschließlich von außen.
- Momentaufnahme der extern sichtbaren DNS-Konfiguration. Keine Konformitäts- oder Betroffenheitsfeststellung und keine Prüfung durch eine Prüfstelle.
- Dies ist kein Penetrationstest. Es wurde keine Schwachstelle aktiv ausgenutzt.
- Kein Quellcode-, Infrastruktur- oder Prozessaudit.
- Momentaufnahme zum genannten Zeitpunkt. Spätere Änderungen sind nicht erfasst.
- Falschmeldungen sind möglich. Vorgeschaltete CDN-, WAF- oder Ratenbegrenzungs-Systeme können das Ergebnis verfälschen.

- Prüfpunkte ohne auswertbaren Messbeleg, etwa bei nicht erreichbaren oder nicht antwortenden Systemen, erscheinen als „nicht auswertbar“ und nicht als „bestanden“.
- Diese Einordnung ist allgemein gehalten und ersetzt keine Rechtsberatung.
- Der aktuelle DNSSEC-Messweg prüft die Antworten auf MX und TXT am eingegebenen DNS-Namen. AD ist der Validierungsbeleg des über Loopback oder HTTPS angebotenen, als validierend vorausgesetzten Resolvers; der Scanner validiert die Signaturen nicht selbst. Eine authentifizierte negative Antwort belegt das Fehlen der angefragten Daten, keinen Mailsdienst. Die Zonengrenze wird nicht gesondert ermittelt. Die Abfragezeit bezeichnet den Abruf; Antworten können aus dem Resolvercache stammen. Andere MX-Zonen, TLSA, SPF-include/redirect-Ziele und DKIM-Selektoren sind damit nicht automatisch bestätigt. DNSSEC verschlüsselt keine Nachricht und belegt weder Zustellung noch den Resolverbetrieb des Mailanbieters.
- Statische SPF-Policyanalyse am eingegebenen DNS-Namen einschließlich begrenzter include-/redirect-Verfolgung. Keine konkrete Nachricht oder Senderautorisierung für MAIL FROM, HELO/EHLO oder leeren SMTP-Rückpfad geprüft; die Eingabe belegt keine tatsächliche Absenderrolle. RFC 7208 §2.3 empfiehlt die getrennte HELO-Prüfung (SHOULD); §2.4 verwendet bei leerem Rückpfad die MAIL-FROM-Identität postmaster@<HELO>. Ein fehlender SPF-Record löst keinen Ersatz durch einen beliebigen empfangenden MX aus. Für eine zusätzliche Auswertung werden eine verlässliche Sender-IP, die HELO/EHLO-Identität und MAIL FROM einschließlich der Angabe benötigt, ob der Rückpfad leer ist. Der Scanner enthält derzeit keinen vollständigen SPF-Auswerter entsprechend check\_host(). Mit diesen Eingaben wäre eine Szenarioprüfung auch ohne Mail möglich; sie würde das vorgegebene Szenario und keine beobachtete Verbindung bestätigen. Das eigene EHLO des Scanners am Empfangsserver belegt keine ausgehende HELO-Identität.
- DNSSEC ist eine allgemeine Härtungsempfehlung (RFC 9364/BCP 237) und Voraussetzung für SMTP-DANE. Im Transportprofil BSI TR-03108 2.0, 4.1.4/4.1.5, sind validierende Resolver sowie signierte Empfangs- und MHS-Zonen verpflichtend. BSI TR-03182 1.0, 4.1.1, empfiehlt die Signierung der SPF-publizierenden Senderzone (SHOULD); 4.1.2 verlangt Resolvvalidierung beim SPF-prüfenden MHS (MUST). Der eingegebene Name ist kein Nachweis dieser Mailrollen. Der Außencheck bestätigt weder die vollständigen Profile noch eine allgemeine gesetzliche DNSSEC-Pflicht.

Automatisierte Momentaufnahme im dokumentierten Prüfumfang. Kein Audit, keine Zertifizierung und keine Rechtsberatung. Gesetzliche Rechte bleiben unberührt. Messstand: 06.10.2026.

Belegnotation e1: Originalbackslashes werden verdoppelt; \u{HEX} steht für genau einen Unicode-Codepoint. Rohbelege stellen so jedes Leer-, Steuer-, kombinierende oder nicht unterstützte Zeichen ausdrücklich dar. Keine Normalisierung. Layoutumbrüche sind keine Originalzeichen. CSV-Rohfelder erhalten zusätzlich den vollständigen Belegtext; Cookie-Werte und Lokalteile von E-Mail-Adressen sind dort wie überall als \*\*\* ausgeblendet.

---

## Bewertungsschema

Die folgende Skala gilt nur für nicht bestandene Prüfpunkte, nicht für Hinweise, nicht auswertbare oder nicht anwendbare Checks. Die Begriffe für Schadenspotenzial und Reaktionspriorität orientieren sich am BSI-Praxis-Leitfaden, Version 1.2, Abschnitt 4.1.3. Die Zuordnung der Scannerbefunde sowie Punkte und Note folgen unserer dokumentierten Bewertungsmethodik. Daraus entstehen keine gesetzlichen Fristen. hoch = sofort, mittel = kurzfristig, niedrig = mittelfristig, zur Information = langfristig. Befundinterpretation 1.9. Punkte bewerten gemessene Konfigurationsmerkmale; fehlende Maximalpunkte bedeuten nicht automatisch einen Fehler. Bewertungsmethodik 1.8: DNSSEC behält 8 von 142 möglichen Punkten. Für A+ müssen die abgefragten MX- und TXT-Antworten beide DNSSEC-validiert sein. Fehlende Bestätigung begrenzt auf A; bei unklarer Messung fehlt der Nachweis für A+, es ist kein gemessener Sicherheitsmangel. Meldet der vertrauenswürdig angebundene Resolver ausdrücklich DNSSEC-bogus, gilt höchstens B. SMTP-, DANE- und Zertifikatspunkte verwenden die begrenzt ausgewählten gleichrangigen MX-Ziele; ein bestätigter schwächerer Pfad wird nicht durch einen guten Pfad verdeckt, ungemessene Pfade bleiben unbekannt. Andere Zusatzpunkte gleichen diese Bedingungen nicht aus. Das getrennte Non-Sending-Profil mit 30 Punkten bleibt unverändert und erhebt DNSSEC nicht. Die Punktzahl ist eine Produktgewichtung und keine Sicherheitswahrscheinlichkeit. Modell 1.9 bewertet bis zu 142 Sicherheitspunkte. BIMl, Zertifikatsverweis, ARC-, Gateway- und SPF-DKIM-Anbieterhinweise sind ungewichtet; ihr Fehlen mindert die Sicherheitsnote nicht. Nicht erhobene Prüfpunkte bleiben im Modellnenner; die Messabdeckung wird gesondert ausgewiesen. Die Note folgt festen Punktschwellen und fachlichen Kappen, nicht einer aus verbleibenden Messungen hochgerechneten Prozentzahl. Es wird bewusst KEIN CVSS-Wert vergeben - für Konfigurationsbefunde gibt es keine autoritative CVSS-Bewertung, und eine selbst gerechnete Zahl in der Notation eines Standards wäre eine Genauigkeit, die es nicht gibt.

BSI – Ein Praxis-Leitfaden für IS-Penetrationstests · v1.2 (2016-11), Kap. 4.1.3, S. 25-26 · geprüft 2026-10-05 ·

[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest\\_Webcheck/Leitfaden\\_Penetrationstests.pdf?\\_\\_blob=publicationFile&v=3](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Leitfaden_Penetrationstests.pdf?__blob=publicationFile&v=3)

### Zustände je Prüfpunkt:

[+] bestanden - im angegebenen Prüfumfang bestätigt; keine Abweichung belegt. [!] nicht bestanden - Befund vorhanden. [?] nicht auswertbar - für diesen Prüfpunkt liegt kein auswertbarer Messbeleg vor; das ist weder ein positiver noch ein negativer Befund. Der Einzelbefund nennt eine dokumentierte Messgrenze oder fehlende gespeicherte Angaben. [i] Hinweis - beobachtetes Konfigurationssignal ohne nachgewiesenen Sicherheitsmangel. [-] nicht anwendbar - für den beobachteten Antwortkontext nicht anwendbar; kein bestandener Sicherheitscheck.

---

# Ausgehende E-Mail-Sicherheit

79 von 87 Punkten

Diese Prüfpunkte betreffen Nachrichten, die im Namen der Domain versendet werden: ob empfangende Systeme erkennen können, dass eine Nachricht echt ist, und wie sie mit Fälschungen umgehen sollen. Die Punktbilanz enthält 2/2 gespeicherte Produktpunkte aus nicht anwendbaren Prüfpunkten. Diese Werte bleiben in der Bewertung erhalten; sie belegen keine erfolgreiche Messung der nicht anwendbaren Prüfung.

## [+] spf · Sender Policy Framework

Zustand: bestanden | Kennung: spf | Regelgewichtung (kein aktueller negativer Befund): Info | Schadenspotenzial: zur Information | Gewicht: 20 Punkte

Geprüft wird: Statische SPF-Policyanalyse am eingegebenen DNS-Namen: Syntax, begrenzte include-/redirect-Verfolgung und wirksamer Abschluss (-all, ~all, ?all). Keine konkrete Sender-IP, MAIL-FROM-, HELO- oder Null-Absender-Autorisierung geprüft.

### **Befund: SPF-Policy mit Hard Fail veröffentlicht**

Die veröffentlichte SPF-Policy endet mit -all (Hard Fail). 2/10 DNS-Lookup-Terme im statisch untersuchten Pfad.

Bewertet werden veröffentlichte Versandquellen und die abschließende SPF-Policy. Das DMARC-Alignment wurde nicht an einer Nachricht geprüft; Empfänger entscheiden über die Zustellung.

DNS-Prüfname: wolf-agents.com. Statische SPF-Policyanalyse am eingegebenen DNS-Namen einschließlich begrenzter include-/redirect-Verfolgung. Keine konkrete Nachricht oder Senderautorisierung für MAIL FROM, HELO/EHLO oder leeren SMTP-Rückpfad geprüft; die Eingabe belegt keine tatsächliche Absenderrolle. Produktpunkte im gespeicherten Lauf: 20/20.

Nachweis: \u{20}v=spf1\u{20}include:spf.tutanota.de\u{20}include:\_spf.tem.scaleway.com\u{20}-all

Referenzen: BSI APP.5.3.A9 | RFC 7208

Referenzen: BSI APP.5.3.A9 · E-Mail-Clients und -Server: Erweiterte Sicherheitsmaßnahmen, Standard (S), Baustein S. 5 · IT-Grundschutz, Edition 2023 (2023-02) · geprüft am 05.10.2026 ·

[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompodium/IT\\_Grundschutz\\_Kompodium\\_Edition2023.pdf?\\_\\_blob=publicationFile&v=4](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompodium/IT_Grundschutz_Kompodium_Edition2023.pdf?__blob=publicationFile&v=4)

Referenzen: IETF · RFC 7208: SPF: Versandberechtigung · geprüft am 05.10.2026 ·

<https://www.rfc-editor.org/rfc/rfc7208>

## [+] dkim · DomainKeys Identified Mail

Zustand: bestanden | Kennung: dkim | Regelgewichtung (kein aktueller negativer Befund): Info | Schadenspotenzial: zur Information | Gewicht: 20 Punkte

Geprüft wird: Ob unter den geprüften Selektoren ein DKIM-Schlüssel im DNS auffindbar ist und welche Schlüssellänge beziehungsweise welches Verfahren er verwendet.

### **Befund: Öffentliche DKIM-Schlüssel gefunden**

Gefundene öffentliche DNS-Schlüssel: s1: RSA 2048 Bit; s2: RSA 2048 Bit.

Dieser DNS-Check prüft keine Nachrichtensignatur. Aktive Signierung, Integrität einer Nachricht und DMARC-Alignment bleiben ungeprüft; unbekannte weitere Selektoren sind nicht ausgeschlossen. Die Punkte bewerten ausschließlich die gefundenen Schlüssel. Produktpunkte im gespeicherten Lauf: 20/20.

Nachweis:\u{20}s1:\u{20}v=DKIM1;\u{20}k=rsa;\u{20}h=sha256;\u{20}p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4d/jridMLV9rZ/IBiDYA17BWKWIHnvLzCVGoFcOENqxLym8ro869rgp82mcxobr2kPyd+sfAS/REOoZ+pkf1wnyywQrf4r9i1O9Bnop4/WsRXTIfgKtaIOtwyhgsv9JH5KpxeQxHwl9CEHhquFjp808gbqRZt6PDp2YetB23EyJ5kp/jpn5/aCvVpC27+jnQH6NoYN8wNsC6cTSA1EhL1etUwjrZUwRtf8S2PIDJom1/CUtc9a/d3sZk15LDtUUbODrQMrj5mzMzHPYp43MwLFRlvSa/O+xlx8esNxwnDa7PH6PZLB8lhtkY49/4ofKV5BQKMGmGmyn+rgYDHD8iwIDAQAB\u{A}\u{A}s2:\u{20}v=DKIM1;\u{20}k=rsa;\u{20}h=sha256;\u{20}p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4d/jridMLV9rZ/IBiDYA17BWKWIHnvLzCVGoFcOENqxLym8ro869rgp82mcxobr2kPyd+sfAS/REOoZ+pkf1wnyywQrf4r9i1O9Bnop4/WsRXTIfgKtaIOtwyhgsv9JH5KpxeQxHwl9CEHhquFjp808gbqRZt6PDp2YetB23EyJ5kp/jpn5/aCvVpC27+jnQH6NoYN8wNsC6cTSA1EhL1etUwjrZUwRtf8S2PIDJom1/CUtc9a/d3sZk15LDtUUbODrQMrj5mzMzHPYp43MwLFRlvSa/O+xlx8esNxwnDa7PH6PZLB8lhtkY49/4ofKV5BQKMGmGmyn+rgYDHD8iwIDAQAB

Referenzen: BSI APP.5.3.A9 | RFC 6376 | RFC 8301 | RFC 8463

Referenzen: BSI APP.5.3.A9 · E-Mail-Clients und -Server: Erweiterte Sicherheitsmaßnahmen, Standard (S), Baustein S. 5 · IT-Grundschutz, Edition 2023 (2023-02) · geprüft am 05.10.2026 ·

[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompodium/IT\\_Grundschutz\\_Kompodium\\_Edition2023.pdf?\\_\\_blob=publicationFile&v=4](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompodium/IT_Grundschutz_Kompodium_Edition2023.pdf?__blob=publicationFile&v=4)

Referenzen: IETF · RFC 6376: DKIM: Signatures · geprüft am 05.10.2026 · <https://www.rfc-editor.org/rfc/rfc6376>

Referenzen: IETF · RFC 8301: DKIM-Schlüssel · geprüft am 05.10.2026 · <https://www.rfc-editor.org/rfc/rfc8301>

Referenzen: IETF · RFC 8463: DKIM mit Ed25519 · geprüft am 05.10.2026 · <https://www.rfc-editor.org/rfc/rfc8463>

## [+] dmarc · Domain-based Message Authentication

Zustand: bestanden | Kennung: dmarc | Regelgewichtung (kein aktueller negativer Befund): Info | Schadenspotenzial: zur Information | Gewicht: 35 Punkte

Geprüft wird: Welche DMARC-Policy im geprüften DNS-Pfad veröffentlicht und für den untersuchten Namen anwendbar ist (p/sp/np, Vererbung und Testmodus t=y). Nachrichtenthautentisierung und Empfängerbehandlung werden nicht geprüft.

### **Befund: DMARC-Policy reject**

Die ausgewählte Policy bittet um Ablehnung DMARC-fehlschlagender Nachrichten.

Policyquelle: \_dmarc.wolf-agents.com; eigener Record. Veröffentlicht: p=reject, sp=nicht angegeben, np=nicht angegeben.

Fehlendes sp ist kein Mangel: Im einschlägigen geerbten Namensraum wird p=reject verwendet, soweit np nicht anwendbar ist.

Ohne np gilt für nicht existierende Subdomains sp, ersatzweise p.

Eigene gültige Subdomain-Records haben Vorrang; deren Bestand wurde nicht vollständig erhoben.

Alignment-Einstellungen: SPF s, DKIM s; beide Modi r und s sind standardkonform.

Aggregate-Reportziele veröffentlicht: \*\*\*@wolf-agents.com. Das belegt weder Reporterzeugung noch Zustellung oder Auswertung.

Fehlerberichtziele (ruf) veröffentlicht: \*\*\*@wolf-agents.com. Der Scan prüft weder Erzeugung noch Inhalt solcher Berichte.

Produktgewichtung für die DNS-Konfiguration: quarantine ist standardkonform; zusätzliche Punkte für reject sind eine strengere Produktgewichtung. Ein Punkteabstand allein begründet keine Fehlerbehebung.

Geprüft wurde die DNS-Policy. Nachrichtensignaturen, SPF-/DKIM-Erfolge, Alignment, Annahme, Ablehnung und tatsächliche Empfängerbehandlung wurden nicht geprüft. Empfänger entscheiden nach ihren eigenen Regeln. Produktpunkte im gespeicherten Lauf: 35/35.

Nachweis: \u{20}v=DMARC1;\u{20}p=reject;\u{20}spf=s;\u{20}adkim=s;\u{20}rua=mailto:\*\*\*@wolf-agents.com;\u{20}ruf=mailto:\*\*\*@wolf-agents.com;\u{20}fo=1

Referenzen: BSI APP.5.3.A9 | RFC 9989 | RFC 9990

Referenzen: BSI APP.5.3.A9 · E-Mail-Clients und -Server: Erweiterte Sicherheitsmaßnahmen, Standard (S), Baustein S. 5 · IT-Grundschutz, Edition 2023 (2023-02) · geprüft am 05.10.2026 ·

[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/IT\\_Grundschutz\\_Kompendium\\_Edition2023.pdf?\\_\\_blob=publicationFile&v=4](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4)

Referenzen: IETF · RFC 9989: DMARC: Richtlinien und Alignment · geprüft am 05.10.2026 ·

<https://www.rfc-editor.org/rfc/rfc9989>

Referenzen: IETF · RFC 9990: DMARC-Sammelberichte · geprüft am 05.10.2026 · <https://www.rfc-editor.org/rfc/rfc9990>

## [i] bimi • Brand Indicators for Message Identification

Zustand: Hinweis | Kennung: bimi | Regelgewichtung (kein aktueller negativer Befund): Info | Schadenspotenzial: zur Information | Gewicht: 0 Punkte

Geprüft wird: Ob ein BIMI-Record im DNS steht und auf eine Logodatei verweist, die unterstützende E-Mail-Programme neben der Nachricht anzeigen können.

### **Befund: BIMI-Logo-URL veröffentlicht**

Der Check liest die Logo-URL aus dem DNS-Record. Die Logo-Datei, Empfängeranzeige und Markenberechtigung werden nicht abgerufen oder validiert. Ein leeres l= kann BIMI bewusst deaktivieren. Eine Logoanzeige hängt außerdem von DMARC und den Regeln des Empfängers ab. Produktpunkte im gespeicherten Lauf: 0/0.

Nachweis: \u{20}v=BIMI1;\u{20}l=https://wolf-agents.com/bimi-logo.svg

## [i] vmc • Verified Mark Certificate

Zustand: Hinweis | Kennung: vmc | Regelgewichtung (kein aktueller negativer Befund): Info | Schadenspotenzial: zur Information | Gewicht: 0 Punkte

Geprüft wird: Ob der BIMI-Record eine HTTPS-Zertifikats-URL nennt. Zertifikatstyp (VMC/CMC), Inhalt und Gültigkeit werden nicht abgerufen oder validiert.

### **Befund: Kein Zertifikatsverweis für BIMI gefunden**

Im BIMI-Record wurde keine verwendbare HTTPS-Adresse für ein Markenzertifikat gefunden. Das ist ein optionales Merkmal zur Markenanzeige und kein Nachweis einer E-Mail-Sicherheitslücke. Produktpunkte im gespeicherten Lauf: 0/0.

Empfehlung [vmc]: Prüfen Sie nur bei gewünschter BIMI-Anzeige die aktuellen Zertifikatsanforderungen Ihrer Ziel-Empfänger. Dieser Scanner validiert keine Markenzertifikate.

## [i] arc • Authenticated Received Chain

Zustand: Hinweis | Kennung: arc | Regelgewichtung (kein aktueller negativer Befund): Info | Schadenspotenzial: zur Information | Gewicht: 0 Punkte

Geprüft wird: Begrenzte Hinweise aus DKIM-ähnlichen Tags am Selektornamen arc.\_domainkey oder einer gespeicherten MX-Anbieterzuordnung. Keine Nachricht, ARC-Kopfzeile, kryptografische Kettenvalidierung oder Vertrauensbewertung wird geprüft.

### **Befund: ARC per Domaincheck nicht verifizierbar**

Am untersuchten Namen arc.\_domainkey wurde kein verwendeter Namens-/Taghinweis auf ARC erkannt. Andere Selektoren und Nachrichtenwege wurden nicht untersucht; fehlendes ARC ist damit nicht nachgewiesen. ARC kann frühere Authentifizierungsergebnisse über Zwischenstationen weiterreichen. Dieser Domaincheck hat keine Nachricht, Kopfzeile, Signatur oder ARC-Kette geprüft. ARC ist in diesem Lauf ein ungewichteter Hinweis (0/0); sein Fehlen ist kein Mangel und mindert die Sicherheitsnote nicht. Standards-Stand 09.09.2026: RFC 8617 ist Experimental. Der aktive WG-Entwurf draft-ietf-dmarc-arc-to-historic-00 schlägt Historic vor; diese Einstufung ist noch nicht beschlossen. Auch DKIM2 ist ein Entwurf, ohne zugesagten Migrationstermin. Daraus folgt keine automatische Empfehlung, ARC abzuschalten. Produktpunkte im gespeicherten Lauf: 0/0.

Empfehlung [arc]: Ein separater Selektor namens arc ist nicht vorgeschrieben. ARC verwendet DNS-Schlüsselabfragen ähnlich DKIM; daraus folgt keine zwingende Wiederverwendung eines gewöhnlichen DKIM-Schlüssels. Bei Mailinglisten oder Weiterleitungen können Sie eine kontrolliert empfangene Nachricht gesondert untersuchen lassen: ARC-Seal, ARC-Message-Signature und ARC-Authentication-Results sind zunächst nur Kopfzeilen. Eine ARC-Validierung prüft unter anderem vollständige, konsistente ARC-Sets und kryptografische Signaturen; das Vertrauen in die Zwischenstationen ist anschließend eigenständig zu bewerten. Ein übernommenes cv=pass ist eine Angabe der Nachricht, kein vom Domaincheck berechnetes Prüfergebnis. Selbst eine validierte Kette garantiert weder ungefährliche Inhalte noch erfolgreiche Zustellung.

Referenzen: RFC 8617

Referenzen: IETF • RFC 8617: ARC: weitergegebene Authentisierungsergebnisse (experimentell) • geprüft am 05.10.2026 • <https://www.rfc-editor.org/rfc/rfc8617>

## [i] dkim-ed25519 · DKIM Moderne Kryptographie

Zustand: Hinweis | Kennung: dkim-ed25519 | Regelgewichtung (kein aktueller negativer Befund): Info |

Schadenspotenzial: zur Information | Gewicht: 5 Punkte

Geprüft wird: Ob die gefundenen DKIM-Schlüssel modernen Verfahren entsprechen — Ed25519 oder RSA mit ausreichender Schlüssellänge.

### **Befund: Zusätzliche DKIM-Kryptographie nicht nachgewiesen**

Bewertet werden ausschließlich die gefundenen öffentlichen Schlüssel. Ein RSA-/Ed25519-Paar ermöglicht parallele Signaturen; tatsächliches Dual-Signing und Empfängerkompatibilität sind ohne Nachrichten nicht nachgewiesen. RSA-2048 entspricht der Empfehlung von RFC 8301. Mehr Bonuspunkte sind eine Produktgewichtung, keine Pflicht zur Umstellung. Produktpunkte im gespeicherten Lauf: 0/5.

Referenzen: RFC 8463

Referenzen: IETF · RFC 8463: DKIM mit Ed25519 · geprüft am 05.10.2026 · <https://www.rfc-editor.org/rfc/rfc8463>

## [i] dkim-redundanz · DKIM-Selector-Redundanz

Zustand: Hinweis | Kennung: dkim-redundanz | Regelgewichtung (kein aktueller negativer Befund): Info |

Schadenspotenzial: zur Information | Gewicht: 3 Punkte

Geprüft wird: Ob mehrere unterschiedliche DKIM-Schlüssel unter den geprüften Selektoren veröffentlicht sind. Aktive Nutzung und der Ablauf einer Rotation sind nicht nachgewiesen.

### **Befund: 1 unterschiedlicher DKIM-Schlüssel gefunden**

Mehrere veröffentlichte Schlüssel können einen kontrollierten Wechsel vorbereiten. Identische Schlüssel unter verschiedenen Selektoren zählen nicht mehrfach. DNS belegt weder aktive Nutzung noch unabhängige Versanddienste oder unterbrechungsfreie Rotation. Auch mit einem aktuellen Selektor ist sichere Rotation durch rechtzeitiges Veröffentlichen eines neuen Schlüssels möglich. Produktpunkte im gespeicherten Lauf: 0/3.

Empfehlung [dkim-redundanz]: Veröffentlichen Sie den neuen öffentlichen Schlüssel vor dem Signaturwechsel. Behalten Sie den alten Schlüssel für noch unterwegs befindliche Nachrichten und berücksichtigen Sie DNS-TTL sowie Laufzeiten. Prüfen Sie anschließend Signaturen tatsächlicher Nachrichten.

## [+] spf-qualitaet · SPF-Qualität

Zustand: bestanden | Kennung: spf-qualitaet | Regelgewichtung (kein aktueller negativer Befund): Info |

Schadenspotenzial: zur Information | Gewicht: 2 Punkte

Geprüft wird: Ob der SPF-Record ohne überholte Mechanismen auskommt und innerhalb der zulässigen Zahl von DNS-Abfragen bleibt.

### **Befund: SPF-Struktur ohne veralteten PTR-Mechanismus**

Die untersuchten SPF-Records binden Versandquellen über include ein. Das kann die Pflege externer Dienste erleichtern; eigene Server dürfen genauso direkt per IP, a oder mx autorisiert werden.

Produktpunkte im gespeicherten Lauf: 2/2.

Referenzen: RFC 7208

Referenzen: IETF · RFC 7208: SPF: Versandberechtigung · geprüft am 05.10.2026 · <https://www.rfc-editor.org/rfc/rfc7208>

## [i] spf-dkim-abdeckung · SPF-DKIM-Anbieterhinweise

Zustand: Hinweis | Kennung: spf-dkim-abdeckung | Regelgewichtung (kein aktueller negativer Befund): Info |

Schadenspotenzial: zur Information | Gewicht: 0 Punkte

Geprüft wird: Ob bekannte SPF-Zielnamen und DKIM-Selektornamen zusammenpassen. Auch über redirect aufgelöste includes werden berücksichtigt; tatsächlicher Nachrichtenversand wird nicht geprüft.

### **Befund: Bekannte SPF-Anbieter und DKIM-Selektornamen gefunden**

SPF-Zielnamen und bekannte DKIM-Selektornamen werden heuristisch zugeordnet. Eigene Server, unbekannte Anbieter und individuelle oder dynamische Selektoren sind zulässig. Auch passende Namen beweisen weder die Zuordnung des Schlüssels zum Versanddienst noch tatsächliche DKIM-Signaturen oder DMARC-Alignment. Für diesen optionalen Hinweis gibt es keine Sicherheits- oder Bonuspunkte. Produktpunkte im gespeicherten Lauf: 0/0.

Referenzen: RFC 6376 | RFC 8301 | RFC 8463

Referenzen: IETF · RFC 6376: DKIM: Signaturen · geprüft am 05.10.2026 · <https://www.rfc-editor.org/rfc/rfc6376>

Referenzen: IETF · RFC 8301: DKIM-Schlüssel · geprüft am 05.10.2026 · <https://www.rfc-editor.org/rfc/rfc8301>

Referenzen: IETF · RFC 8463: DKIM mit Ed25519 · geprüft am 05.10.2026 · <https://www.rfc-editor.org/rfc/rfc8463>

## **[ - ] dmarc-report-auth · DMARC Report-Autorisierung**

Zustand: nicht anwendbar | Kennung: dmarc-report-auth | Regelgewichtung (kein aktueller negativer Befund): Info |

Schadenspotenzial: zur Information | Gewicht: 2 Punkte

Geprüft wird: Ob externe Empfänger von DMARC-Berichten den Empfang autorisiert haben — nachweisbar über einen Freigabe-Record in deren Domain.

### **Befund: Reports gehen an eigene Domain**

Als Reportziel ist **\*\*\*@wolf-agents.com** innerhalb der Policy-Domain eingetragen. Der DNS-Verweis belegt keine tatsächliche Reporterzeugung oder Zustellung. Produktpunkte im gespeicherten Lauf: 2/2.

Referenzen: RFC 9989 | RFC 9990

Referenzen: IETF · RFC 9989: DMARC: Richtlinien und Alignment · geprüft am 05.10.2026 ·

<https://www.rfc-editor.org/rfc/rfc9989>

Referenzen: IETF · RFC 9990: DMARC-Sammelberichte · geprüft am 05.10.2026 · <https://www.rfc-editor.org/rfc/rfc9990>

---

## **Eingehende E-Mail-Sicherheit**

15 von 15 Punkten

Diese Prüfpunkte betrachten konfigurierte Empfangsziele und veröffentlichte Transport- und Reportingpolicies für eingehende E-Mails.

### **[ + ] mx · Mail Exchange Records**

Zustand: bestanden | Kennung: mx | Regelgewichtung (kein aktueller negativer Befund): Info | Schadenspotenzial: zur Information | Gewicht: 0 Punkte

Geprüft wird: MX-Namen und Prioritäten einschließlich Null MX sowie gespeicherte Anbieter-Namensmuster. Die ergänzende PTR-Prüfung umfasst höchstens die erste IPv4-Adresse des ersten MX und kann ausgelassen oder unvollständig sein. Schutzbetrieb, SMTP-Erreichbarkeit, A/AAAA-Fallback und Zustellung sind dadurch nicht geprüft.

#### **Befund: MX-Einträge im DNS gefunden**

1 MX-Eintrag/Einträge beobachtet: 10 mail.tutanota.de. Der erste MX-Name passt zum gespeicherten Namensmuster mail.tutanota.de von Tutanota / Tuta (Germany) (Cloud\_Privacy). Das ist eine Namenszuordnung, kein Nachweis gebuchter Schutzfunktionen, aktivierter Mandantenrichtlinien oder erfolgreicher Filterung.

Ein explizites MX-Ziel wurde beobachtet.

PTR/FCrDNS wurde in diesem MX-Befund nicht abschließend erhoben. Eine Providerzuordnung ersetzt diese Messung nicht.

MX-DNS-Einträge belegen weder aktive Schutzfunktionen noch SMTP-Erreichbarkeit oder erfolgreiche Zustellung. Eine separat gespeicherte SMTP-Messung gilt nur für ihren Host, Zeitpunkt und Verbindungsabschnitt. Produktpunkte im gespeicherten Lauf: 0/0.

Nachweis: \u{20}10\u{20}mail.tutanota.de

## [+] mta-sts · MTA Strict Transport Security

Zustand: bestanden | Kennung: mta-sts | Regelgewichtung (kein aktueller negativer Befund): Info | Schadenspotenzial: zur Information | Gewicht: 10 Punkte

Geprüft wird: DNS-Versionsmarker und id-Tag, begrenzter HTTPS-Abruf, Policyparser, veröffentlichter Modus und max\_age sowie MX-Namensabgleich bei vorhandenen Eingaben. Keine vollständige RFC-Abnahme, SMTP-Zertifikatsprüfung oder Beobachtung der Anwendung durch fremde Sender.

### **Befund: MTA-STs enforce veröffentlicht; MX-Namen abgedeckt**

Ein DNS-Versionsmarker mit id-Tag und ein vom Policyparser akzeptierter Inhalt sind dokumentiert. Das bestätigt die geprüften Merkmale, keine vollständige RFC- oder Betriebsabnahme.

DNS: \_mta-sts.wolf-agents.com; 1 Record(s) mit Versionsmarker, erkanntes id=20260524. Kandidatenzahl und id-Marker sind keine vollständige DNS-Syntaxprüfung.

HTTPS-Antwort: HTTP 200, lesbarer Policyinhalt vom Parser akzeptiert.

Gespeicherter Modus: enforce. Ein Sender, der diese Policy anwendet, muss die vorgegebenen MX-/TLS-/Zertifikatsbedingungen erfüllen und darf bei deren Fehlschlag nicht unter dieser Policy zustellen.

Gespeicherte Policy-MX-Muster: mail.tutanota.de.

MX-Eingaben dieses Abgleichs: 10 mail.tutanota.de.

Alle im Abgleich gespeicherten MX-Namen passen zu den Policy-Mustern.

max\_age: 86400 Sekunden (1 Tag(e)). Die Laufzeit beschreibt den vorgesehenen Sendercache, keinen gemessenen Schutzzeitraum.

Der Policyabruf über HTTPS ist keine STARTTLS- oder SMTP-Zertifikatsprüfung der MX. Tatsächliche Senderanwendung, Nachrichtenversand, Zustellung und Berichtsempfang wurden hier nicht geprüft; separate SMTP-Befunde gelten nur für ihren eigenen Host, Messzeitpunkt und Prüfumfang. Produktpunkte im gespeicherten Lauf: 10/10.

Nachweis:\u{20}DNS-Record:\u{A}v=STSV1;\u{20}id=20260524\u{A}\u{A}Policy-Datei:\u{A}version:\u{20}STSV1\u{D}\u{A}mode:\u{20}enforce\u{D}\u{A}mx:\u{20}mail.tutanota.de\u{D}\u{A}max\_age:\u{20}86400

Empfehlung [mta-sts]: Prüfen Sie die dokumentierten Policymerkmale und den gewünschten Nachrichtenweg kontrolliert. Reportingbetrieb muss am vorgesehenen TLS-RPT-Ziel gesondert eingerichtet und geprüft werden.

Referenzen: BSI APP.5.3.A9 | RFC 8461

Referenzen: BSI APP.5.3.A9 · E-Mail-Clients und -Server: Erweiterte Sicherheitsmaßnahmen, Standard (S), Baustein S. 5 · IT-Grundschutz, Edition 2023 (2023-02) · geprüft am 05.10.2026 ·

[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompodium/IT\\_Grundschutz\\_Kompodium\\_Edition2023.pdf?\\_\\_blob=publicationFile&v=4](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompodium/IT_Grundschutz_Kompodium_Edition2023.pdf?__blob=publicationFile&v=4)

Referenzen: IETF · RFC 8461: MTA-STs: veröffentlichte Transportpolicy · geprüft am 05.10.2026 ·

<https://www.rfc-editor.org/rfc/rfc8461>

## [+] tls-rpt · TLS Reporting

Zustand: bestanden | Kennung: tls-rpt | Regelgewichtung (kein aktueller negativer Befund): Info | Schadenspotenzial: zur Information | Gewicht: 5 Punkte

Geprüft wird: TXT-Versionsmarker, Anzahl passender TLS-RPT-Records, rua-Felder und begrenzte Merkmale der mailto:- und https:-Ziele. Keine vollständige RFC-Validierung; Reporterzeugung, Übertragung, Empfang, Auswertung und Alarmierung werden nicht geprüft.

### **Befund: TLS-RPT-Policy mit Reportingziel im DNS gefunden**

Ein Record mit v=TLSRPTv1 und 1 rua-Feld(ern) wurde gefunden. Als verwendbar erkannte Reportingziele: mailto:\*\*\*@wolf-agents.com. Die Prüfung umfasst TXT-Versionsmarker, Anzahl passender Records, rua-Felder und begrenzte URI-Merkmale (mailto-Adresse beziehungsweise HTTPS-Host ohne Zugangsdaten). Sie ist keine vollständige RFC-Validierung. Erzeugung durch sendende Systeme, Erreichbarkeit des Ziels, Übertragung, tatsächlicher Empfang, Auswertung und Alarmierung wurden nicht getestet. Produktpunkte im gespeicherten Lauf: 5/5.

Nachweis: \u{20}v=TLSRPTv1;\u{20}rua=mailto:\*\*\*@wolf-agents.com

Empfehlung [tls-rpt]: Prüfen Sie am vorgesehenen Reportingziel mit dessen Betreiber den tatsächlichen Empfang und die Auswertung von TLS-Berichten sowie die gewünschte Alarmierung. Auch sendende Systeme müssen Berichte erzeugen und übertragen; eine DNS-Veröffentlichung allein belegt diesen Betrieb nicht.

Referenzen: BSI APP.5.3.A13 | RFC 8460

Referenzen: BSI APP.5.3.A13 · E-Mail-Clients und -Server: TLS-Reporting, erhöht (H), Baustein S. 6 · IT-Grundschutz, Edition 2023 (2023-02) · geprüft am 05.10.2026 ·

[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompodium/IT\\_Grundschutz\\_Kompodium\\_Edition2023.pdf?\\_\\_blob=publicationFile&v=4](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompodium/IT_Grundschutz_Kompodium_Edition2023.pdf?__blob=publicationFile&v=4)

Referenzen: IETF · RFC 8460: TLS-RPT: Berichte zur SMTP-Transportsicherheit · geprüft am 05.10.2026 ·

<https://www.rfc-editor.org/rfc/rfc8460>

## [i] seg-provider · Secure Email Gateway

Zustand: Hinweis | Kennung: seg-provider | Regelgewichtung (kein aktueller negativer Befund): Info |

Schadenspotenzial: zur Information | Gewicht: 0 Punkte

Geprüft wird: Ob MX-Namen zu bekannten Gateway-Anbietermustern passen. Ein aktiver Filter oder seine Wirksamkeit wird nicht geprüft.

### **Befund: Kein bekanntes Anbieter-Muster in den MX-Namen**

Die beobachteten MX-Namen passen zu keinem Gateway-Anbietermuster dieser Erkennung. Zur Einordnung: Die Erkennung arbeitet mit bekannten MX-Mustern — nicht gelistete oder individuell gehostete Gateways erfasst sie nicht. Ein fehlender Anbieterhinweis ist kein Sicherheitsmangel und beeinflusst die Note nicht. Produktpunkte im gespeicherten Lauf: 0/0.

## DNS-Sicherheit & weitere Härtung

24 von 24 auswertbaren Punkten (16 weitere Punkte sind nicht auswertbar)

Diese Gruppe enthält begrenzte DNS-, TLSA-, SMTP- und weitere Härtungsbefunde. DNSSEC ist in der Bewertungsmethodik 1.8 dieses Laufs zusätzlich eine Bedingung für die Spitzennote. Punkte und Beobachtungen bestätigen keine vollständige Absicherung oder Zustellung.

### [+] dnssec · DNS Security Extensions

Zustand: bestanden | Kennung: dnssec | Regelgewichtung (kein aktueller negativer Befund): Info | Schadenspotenzial: zur Information | Gewicht: 8 Punkte

Geprüft wird: DNSSEC-Validierungsbelege der MX- und TXT-Antworten am eingegebenen Namen über den vertrauten Resolverkanal. Positive, negative, nicht authentifizierte und unklare Antworten werden getrennt; keine vollständige Zonen- oder Mailpfadprüfung.

**Befund: MX- und TXT-Antworten DNSSEC-validiert**

MX wolf-agents.com: RRset vorhanden; DNSSEC-validiert (AD). RCODE: 0. Messzeit:

2026-10-06T20:31:45.616Z. Resolverkanal: loopback-udp. RRset-Namen: wolf-agents.com.

TXT wolf-agents.com: RRset vorhanden; DNSSEC-validiert (AD). RCODE: 0. Messzeit:

2026-10-06T20:31:45.618Z. Resolverkanal: loopback-udp. RRset-Namen: wolf-agents.com.

Der aktuelle DNSSEC-Messweg prüft die Antworten auf MX und TXT am eingegebenen DNS-Namen. AD ist der Validierungsbeleg des über Loopback oder HTTPS angebotenen, als validierend vorausgesetzten Resolvers; der Scanner validiert die Signaturen nicht selbst. Eine authentifizierte negative Antwort belegt das Fehlen der angefragten Daten, keinen Maildienst. Die Zonengrenze wird nicht gesondert ermittelt. Die Abfragezeit bezeichnet den Abruf; Antworten können aus dem Resolvercache stammen. Andere MX-Zonen, TLSA, SPF-include/redirect-Ziele und DKIM-Selektoren sind damit nicht automatisch bestätigt. DNSSEC verschlüsselt keine Nachricht und belegt weder Zustellung noch den Resolverbetrieb des Mailanbieters. Produktpunkte im gespeicherten Lauf: 8/8.

Nachweis:\u{20}wolf-agents.com\u{20}IN\u{20}MX\u{20}10\u{20}mail.tutanota.de.\u{A}wolf-agents.com\u{20}IN\u{20}TXT\u{20}"v=spf1\u{20}include:spf.tutanota.de\u{20}include:\_spf.tem.scaleway.com\u{20}-all"\u{A}wolf-agent s.com\u{20}IN\u{20}TXT\u{20}"google-site-verification=qn\_HX0HbTp5w4HUg4H-xan\_QuSKtPrL6M9YSZqyYJag"\u{A}w olf-agents.com\u{20}IN\u{20}TXT\u{20}"t-verify=1f523ee67b0a2d1bd3411818a20c05ee"

Referenzen: BSI TR-03108 2.0, 4.1.4/4.1.5 (Transportprofil) | BSI TR-03182 1.0, 4.1.1/4.1.2 (getrennte SPF-Rollen) | RFC 4033 | RFC 4035 | RFC 9364

Referenzen: BSI TR-03108 · Sicherer E-Mail-Transport · v2.0 (2023-06-01), 4.1.4–4.1.5 · geprüft am 05.10.2026 · [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03108/TR03108.pdf?\\_\\_blob=publicationFile&v=3](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03108/TR03108.pdf?__blob=publicationFile&v=3)

Referenzen: BSI TR-03182 · E-Mail-Authentisierung · v1.0 (2024-01-24), 4.1.1–4.1.2 · geprüft am 05.10.2026 · [https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03182/BSI-TR-03182.pdf?\\_\\_blob=publicationFile&v=6](https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03182/BSI-TR-03182.pdf?__blob=publicationFile&v=6)

Referenzen: IETF · RFC 4033: DNSSEC: Grundlagen · geprüft am 05.10.2026 · <https://www.rfc-editor.org/rfc/rfc4033>

Referenzen: IETF · RFC 4035: DNSSEC: Protokoll · geprüft am 05.10.2026 · <https://www.rfc-editor.org/rfc/rfc4035>

Referenzen: IETF · RFC 9364: DNSSEC: Betriebsempfehlungen · geprüft am 05.10.2026 · <https://www.rfc-editor.org/rfc/rfc9364>

## [+] dane · DNS-based Authentication of Named Entities

Zustand: bestanden | Kennung: dane | Regelgewichtung (kein aktueller negativer Befund): Info | Schadenspotenzial: zur Information | Gewicht: 10 Punkte

Geprüft wird: Ob unterschiedliche MX-Hosts der niedrigsten numerischen Präferenz innerhalb der dokumentierten Messgrenze DNSSEC-validierte TLSA-Einträge mit unterstützten SMTP-Parametern veröffentlichen. Zertifikatsabgleich und MX anderer Präferenzstufen sind nicht geprüft.

### **Befund: DNSSEC-validierter SMTP-TLSA-Record gefunden**

Für mail.tutanota.de wurde ein DNSSEC-validierter TLSA-Record mit unterstützten SMTP-Parametern gefunden. Die Zertifikatsdaten wurden nicht mit dem tatsächlich präsentierten SMTP-Zertifikat verglichen. Geprüft wurde nur dieser MX-Host; weitere MX-Ziele und der reale Nachrichtenfluss sind damit nicht bestätigt. Gemessen wurde der einzige ausgewählte MX der niedrigsten numerischen Präferenz (mail.tutanota.de). Produktpunkte im gespeicherten Lauf: 10/10.

Nachweis:\u{20}\_25\_tcp.mail.tutanota.de\u{20}TLSA\u{20}3\u{20}0\u{20}1\u{20}d141f8f3a4aac2e4d2677aafcc723d8e5cc7b146e968c3aea348ed93996bbe6f

Referenzen: BSI APP.5.3.A9 | RFC 6698 | RFC 7672

Referenzen: BSI APP.5.3.A9 · E-Mail-Clients und -Server: Erweiterte Sicherheitsmaßnahmen, Standard (S), Baustein S. 5 · IT-Grundschutz, Edition 2023 (2023-02) · geprüft am 05.10.2026 ·

[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompodium/IT\\_Grundschutz\\_Kompodium\\_Edition2023.pdf?\\_\\_blob=publicationFile&v=4](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompodium/IT_Grundschutz_Kompodium_Edition2023.pdf?__blob=publicationFile&v=4)

Referenzen: IETF · RFC 6698: DANE/TLSA · geprüft am 05.10.2026 · <https://www.rfc-editor.org/rfc/rfc6698>

Referenzen: IETF · RFC 7672: DANE für SMTP · geprüft am 05.10.2026 · <https://www.rfc-editor.org/rfc/rfc7672>

## [+] caa · Certificate Authority Authorization

Zustand: bestanden | Kennung: caa | Regelgewichtung (kein aktueller negativer Befund): Info | Schadenspotenzial: zur Information | Gewicht: 2 Punkte

Geprüft wird: Ob CAA-Einträge im DNS festlegen, welche Zertifizierungsstellen für die Domain überhaupt Zertifikate ausstellen dürfen.

### **Befund: CAA vollständig konfiguriert**

Erlaubte CAs: pki.goog, letsencrypt.org, globalsign.com, sectigo.com, digicert.com, comodoca.com. Als optionales Meldungsziel ist eingetragen: mailto:\*\*\*@wolf-agents.com. Tatsächliche Meldungen und die gesamte Zertifikatsausstellung wurden nicht geprüft.

Empfehlung: Ein issuewild-Tag ist nur für abweichende Wildcard-Regeln nötig; ohne ihn gilt issue auch für Wildcards. Produktpunkte im gespeicherten Lauf: 2/2.

Nachweis:\u{20}0\u{20}issue\u{20}"pki.goog"\u{A}0\u{20}issue\u{20}"letsencrypt.org"\u{A}0\u{20}issue\u{20}"globalsign.com"\u{A}0\u{20}issue\u{20}"sectigo.com"\u{A}0\u{20}iodef\u{20}"mailto:\*\*\*@wolf-agents.com"\u{A}0\u{20}issue\u{20}"digicert.com"\u{A}0\u{20}issue\u{20}"comodoca.com"

Referenzen: RFC 8659

Referenzen: IETF · RFC 8659: CAA: Zertifikatsaussteller im DNS · geprüft am 05.10.2026 ·

<https://www.rfc-editor.org/rfc/rfc8659>

## [?] smtp-tls · SMTP TLS-Zertifikat

Zustand: nicht auswertbar | Kennung: smtp-tls | Regelgewichtung (kein aktueller negativer Befund): Info |

Schadenspotenzial: zur Information | Gewicht: 13 Punkte

Geprüft wird: Ob unterschiedliche MX-Hosts der niedrigsten numerischen Präferenz innerhalb der dokumentierten Messgrenze eine verschlüsselte SMTP-Verbindung anbieten, welche TLS-Version jeweils beobachtet wurde und ob das jeweilige Zertifikat zum Hostnamen passt. Gemessene gleichrangige MX-Ziele: mail.tutanota.de. Nicht gemessene gleichrangige Ziele: keine. Backup-Präferenzstufen: keine. SMTP-Messzeit: mail.tutanota.de: 2026-10-06T20:31:59.422Z.

### **Befund: SMTP-Messung nicht vollständig abgeschlossen**

Untersuchter MX/Host: mail.tutanota.de. STARTTLS-Angebot: nicht abschließend erhoben. TLS-Handshake: nicht abschließend bestätigt.

TLS-Version: nicht dokumentiert. Zertifikatsvertrauensketten: nicht dokumentiert; Hostnamenzuordnung: nicht dokumentiert.

SMTP-Messzeit: 2026-10-06T20:31:59.422Z. Messgrenze/Fehler: Socket-Zeitüberschreitung.

Prüfstandorte: primär: Teilmessung, Versuch ab 2026-10-06T20:31:46.398Z bis 2026-10-06T20:31:56.444Z, Messfehler: Socket-Zeitüberschreitung; Fallback: Teilmessung, Versuch ab 2026-10-06T20:31:49.400Z bis 2026-10-06T20:31:59.421Z, Messfehler: Socket-Zeitüberschreitung. Ein Fallback-Erfolg vervollständigt den Befund des anderen Standorts nicht.

Der Befund gilt für diesen beobachteten Verbindungsabschnitt vom Prüfstandort aus. Weitere MX, Fallback-Standorte und Transportstrecken sind kein Vollnachweis. Keine Ende-zu-Ende-Verschlüsselung oder tatsächliche Zustellung wurde geprüft. Ein Verbindungs-, EHLO- oder Handshakefehler allein beweist keine fehlende Verschlüsselungsfähigkeit. Gemessen wurde der einzige ausgewählte MX der niedrigsten numerischen Präferenz (mail.tutanota.de). Das Gewicht von 13 Punkten bezeichnet das Katalogmaximum dieses nicht auswertbaren Prüfpunkts, keine erreichten Punkte und keinen bestätigten Abzug. Die gespeicherten 0/0 Produktpunkte kennzeichnen den Messausfall, nicht das Kataloggewicht. Produktpunkte im gespeicherten Lauf: 0/0.

Empfehlung [smtp-tls]: Klären Sie die protokollierte Messgrenze anhand der Serverlogs und des Prüfstandorts, bevor Sie eine TLS-Fehlkonfiguration annehmen.

Referenzen: BSI APP.5.3.A2

Referenzen: BSI APP.5.3.A2 · E-Mail-Clients und -Server: Sicherer Betrieb, Basis (B), Baustein S. 3-4 · IT-Grundschutz, Edition 2023 (2023-02) · geprüft am 05.10.2026 ·

[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompodium/IT\\_Grundschutz\\_Kompodium\\_Edition2023.pdf?\\_\\_blob=publicationFile&v=4](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompodium/IT_Grundschutz_Kompodium_Edition2023.pdf?__blob=publicationFile&v=4)

## [?] smtp-zertifikat · SMTP-Zertifikatsstatus

Zustand: nicht auswertbar | Kennung: smtp-zertifikat | Regelgewichtung (kein aktueller negativer Befund): Info |

Schadenspotenzial: zur Information | Gewicht: 3 Punkte

Geprüft wird: Wie lange die beobachteten TLS-Zertifikate der begrenzt ausgewählten gleichrangigen MX-Hosts noch gültig sind und ob ihre Restlaufzeit für eine geordnete Erneuerung reicht.

### **Befund: Zertifikatsprüfung nicht durchführbar**

Für diesen Scan lagen keine Zertifikatsdaten des Mailservers vor (SMTP-Test nicht verfügbar). Das ist kein Befund über Ihr Zertifikat. Gemessen wurde der einzige ausgewählte MX der niedrigsten numerischen Präferenz (mail.tutanota.de). Das Gewicht von 3 Punkten bezeichnet das Katalogmaximum dieses nicht auswertbaren Prüfpunkts, keine erreichten Punkte und keinen bestätigten Abzug. Die gespeicherten 0/0 Produktpunkte kennzeichnen den Messausfall, nicht das Kataloggewicht. Produktpunkte im gespeicherten Lauf: 0/0.

## [+] ptr-fcrdns · Reverse DNS / FCrDNS

Zustand: bestanden | Kennung: ptr-fcrdns | Regelgewichtung (kein aktueller negativer Befund): Info |

Schadenspotenzial: zur Information | Gewicht: 4 Punkte

Geprüft wird: Ob zur ersten ermittelten IPv4-Adresse des primären MX ein PTR-Name vorliegt und dessen A-Einträge wieder die ursprüngliche IP-Adresse enthalten (Forward-confirmed reverse DNS).

### **Befund: FCrDNS vollständig korrekt**

Die geprüfte IPv4-Adresse bestätigt den Reverse-DNS-Eintrag: 185.205.69.214 → mail.w14.tutanota.de → 185.205.69.214. Der PTR-Name muss für FCrDNS nicht dem MX-Namen entsprechen. Geprüft wird der primäre MX-Host (Empfangsrichtung); abweichende ausgehende Server, weitere Adressen und IPv6 sind nicht abgedeckt. Produktpunkte im gespeicherten Lauf: 4/4.

Referenzen: RFC 1035

Referenzen: IETF · RFC 1035: DNS-Ressourceneinträge · geprüft am 05.10.2026 · <https://www.rfc-editor.org/rfc/rfc1035>