# Sicherheits- und Datenschutzanalyse der E-Mail-Server von Krankenhäusern und Kliniken

## Eine praktische Analyse auf Datenschutzkonformität gemäß den Vorgaben der Datenschutzaufsichtsbehörden

Tim Wambach[1]

**Abstract:** Mit einer Orientierungshilfe formulierten 2021 die unabhängigen Datenschutzbehörden des Bundes und der Länder Mindestanforderungen für den technischen Schutz der Übermittlung personenbezogener Daten durch die E-Mail-Infrastruktur. Dabei wird, je nach Risiko, eine wirksame Verschlüsselung der Daten auf dem Übertragungsweg gefordert. Die hier vorgestellte Studie zeigt, dass nur 7 von 822 überprüften Mailserver die Anforderungen für normales Risiko der Orientierungshilfe erfüllen. Die Arbeit soll verdeutlichen, an welchen Stellen die derzeitige Praxis hinter den Erwartungen der Aufsichtsbehörden bleibt.

**Keywords:** Datenschutz, E-Mail, Sicherheit, TLS, Transportverschlüsselung, DSGVO

## 1 Einleitung

Im Mai 2021 hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) eine Orientierungshilfe zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail veröffentlicht[2]. Diese soll Schutzanforderungen konkretisieren, die bei Versand und Entgegennahme von E-Mail-Nachrichten durch Verantwortliche[3]zu berücksichtigen sind.

Grundsätzlich kann bei der Übertragung von E-Mails ein Schutz auf dem Transportweg durch Verschlüsselung erreicht werden. Dabei wird zwischen E-Mail-Client und E-Mail-Server des Senders, zwischen E-Mail-Server des Senders und E-Mail-Server Empfängers und E-Mail-Client des Empfängers und E-Mail-Server des Empfängers eine Transportverschlüsselung auf Basis von TLS eingesetzt. Die Orientierungshilfe der Aufsichtsbehörden fokussiert auf den Schutz zwischen den E-Mail-Servern des Senders

[1] Hochschule für Polizei und öffentliche Verwaltung Nordrhein-Westfalen, Abteilung Köln, Erna-Scheffler-Str. 4, 51103 Köln, tim.wambach@hspv.nrw.de

[2] „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“, abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschluesselung.pdf, zuletzt abgerufen am 06.03.2022.

[3] Entsprechend der Definition aus Art. 4 Nr. 7 DSGVO. Die Anforderung richten sich in gleicher Weise an Auftragsverarbeiter, die im Folgenden aus Gründen der Übersichtlichkeit nicht weiter genannt werden.

doi:10.18420/inf2022_50

und Empfängers (auch MTAs genannt). Sie spezifiziert Maßnahmen, die Verantwortliche auf Sender- und Empfängerseite berücksichtigen müssen, mit dem Ziel ein möglichst hohes Schutzniveau zu erreichen.

Es stellt sich die Frage, ob die Anforderungen der Aufsichtsbehörden, ein Jahr nach Veröffentlichung der Orientierungshilfe, in der Praxis eingehalten werden. Dies soll insbesondere bei einer Gruppe von Verantwortlichen überprüft werden, an die besonders hohe Erwartungen bezüglich des Schutzes personenbezogener Daten gestellt werden. So wurden 938 E-Mail-Server von Verantwortlichen aus dem Gesundheitswesen auf eine Umsetzung der Schutzmaßnahmen aus der Orientierungshilfe überprüft. Genauer handelt sich um E-Mail-Server von Krankenhäusern und Kliniken. Neben einer technischen Übersicht und einer Zusammenfassung der Forderungen der Aufsichtsbehörden werden die Ergebnisse dieser quantitativen Studie vorgestellt.

## 2 Technischer Ablauf beim E-Mail-Versand

Die Orientierungshilfe zielt auf die Schutzmaßnahmen auf dem Übertragungsweg zwischen dem E-Mail-Server des Senders und dem E-Mail-Server des Empfängers ab. Nicht berücksichtigt werden mögliche weitere Datenschutzanforderungen an Verantwortliche bzgl. Fragen der Aufbewahrung, Speicherbegrenzung oder Zweckbindung. In diesem Abschnitt sollen die technischen Hintergründe bei Versand und Empfang von E-Mails näher beschrieben werden.

Der Versand von E-Mail-Nachrichten erfolgt über SMTP[4]. Bei Versand einer E-Mail wird unter Verwendung einer E-Mail-Anwendung (Mail User Agent), wie beispielsweise Outlook, im ersten Schritt ein so genannter Mail Submission Agent (MSA) beauftragt die Nachricht zu übermitteln. Der MSA übergibt diese im zweiten Schritt an einen Mail Transmission Agent (MTA).

Im dritten Schritt wird der Nameserver der Empfängerseite bezüglich des zuständigen Mailservers befragt (MX-Eintrag) um im vierten Schritt über das SMTP-Protokoll die Nachricht an diesen zu übermitteln. Der MTA der Gegenseite übergibt die E-Mail dem Mail Delivery Agent (MDA) im fünften Schritt. Dieser bewahrt die E-Mail auf, bis der Empfangende im sechsten Schritt unter Verwendung der eigenen E-Mail-Anwendung (MUA) die E-Mail abruft.

Der Ablauf wird in Abb. 1 zusammengefasst, wobei die Pfeilrichtung die Richtung der Kontaktaufnahme zeigt. Es handelt sich um eine vereinfachte Darstellung – nicht berücksichtigt werden Schutzmaßnahmen zur SPAM-Prävention wie z. B. Blacklist-Anbieter oder der Einsatz von SPF (vgl. Abschnitt 3.4), für die weitere Abfragen und Kontaktaufnahmen erforderlich sind. Je nach Infrastruktur und eingesetzter Software

[4] Protokollbeschreibung des SMTP: Simple Mail Transfer Protocol abrufbar unter https://datatracker.ietf.org/doc/html/rfc5321 und zuletzt abgerufen am 06.03.2022.

werden die Rollen MSA/MTA bzw. MTA/MDA auch in einer Applikation zusammengefasst. Breite Anwendung finden hierbei die Serveranwendungen wie Postfix, Exim, qmail und Exchange.

Im Fokus der Orientierungshilfe der Aufsichtsbehörden steht eine Absicherung der Kommunikation zwischen den Verantwortlichen – also Schritt drei (DNS-Abfrage[5]) und vier (Übermittlung). Während die Schritte 1 und 2 sowie 5 und 6 üblicherweise in der eigenen Hand der jeweiligen Verantwortlichen oder dessen Auftragsverarbeiters liegen, stellt sich die Frage, wie die Übermittlung zwischen Sender und Empfänger gesichert werden kann. Das Ziel, in Bezug auf Vertraulichkeit, Integrität und Authentizität ein möglichst hohes Schutzniveau auf dem Transportweg zu erreichen, steht dabei jedoch in Konflikt mit dem Ziel, möglichst jede E-Mail-Nachricht entgegennehmen zu können (Verfügbarkeit).

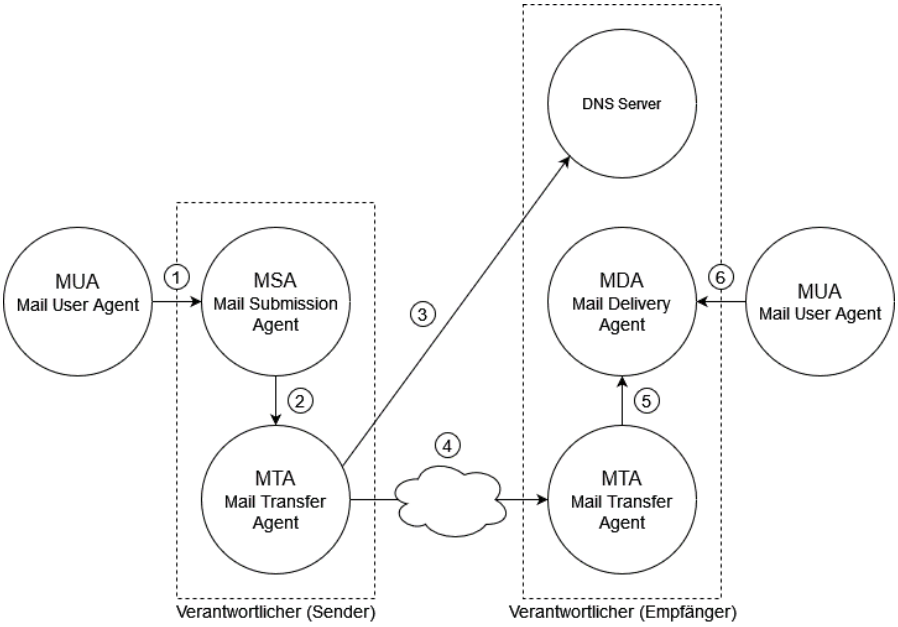


Abb. 1: Beteiligte Parteien bei Übertragung einer E-Mail

[5] DNS-Antwort kann möglicherweise auch aus einem Cache stammen. Dabei ist zu berücksichtigen, dass der Verantwortliche dies beeinflussen kann.

## 3 Bestehende Schutzmöglichkeiten

In diesem Abschnitt sollen die technischen Schutzmöglichkeiten kurz erläutert und bezüglich ihrer Schutzwirkung eingeordnet werden. Die Schutzmaßnahmen werden in Tab. 1 zusammengefasst.

| Technologie | Schutzziel |
|---|---|
| (SSL/) TLS | Schutz der Vertraulichkeit und Authentizität des Zielservers bei Übermittlung. |
| MTA-STS[6] | Sicherstellung der Verschlüsselung, Schutz vor Downgrade-Attacken sowie begrenzter Schutz der Authentizität des Zielservers. |
| DANE[7] | Sicherstellung der Verschlüsselung und Authentizität des Zielservers, erfordert DNSSEC. |
| TLSA[8] | Bereitstellung von Zertifikatsinformationen durch einen DNS-Eintrag. |
| SPF[9] | Schutz vor gefälschten E-Mail-Absendern durch DNS-Einträge. |
| DKIM[10] | Schutz vor gefälschten E-Mail-Absendern durch digitale Signaturen des sendenden MTA. |
| DMARC[11] | Basiert auf SPF und DKIM und regelt den Umgang mit E-Mails bei Fehlern. |
| S/MIME, PGP, GPG | Ende-zu-Ende-Verschlüsselung sowie Authentizität des Absenders und Integrität der E-Mail-Nachricht durch Signaturen. |

Tab. 1: Technologien und Schutzziele

[6] „SMTP MTA Strict Transport Security" (MTA-STS) vgl. RFC 8461.
[7] „SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS)" vgl. RFC 7672.
[8] „The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA" vgl. RFC 6698
[9] „Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1" vgl. RFC 4408.
[10] „DomainKeys Identified Mail (DKIM) Signatures" vgl. RFC 6376.
[11] „Domain-based Message Authentication, Reporting, and Conformance (DMARC)" vgl. RFC 7489.

### 3.1 Transportverschlüsselung durch TLS

Bei einer Transportverschlüsselung mittels TLS werden die Daten verschlüsselt, integritätsgeschützt und das Protokoll ermöglicht zusätzlich eine Authentifizierung und einen Schutz vor Replay-Angriffen.

Ursprünglich wurde SMTP als unverschlüsseltes Klartextprotokoll entwickelt. Sukzessive wurden Sicherheitsmaßnahmen hinzugefügt, um das Schutzniveau zu erhöhen und gleichzeitig abwärtskompatibel bleiben zu können. Sofern vom Server unterstützt, kann über den **STARTTLS** Befehl der E-Mail-Server angewiesen werden, eine SSL- bzw. TLS-geschützte Kommunikation auf Basis der bestehenden Verbindung zu ermöglichen. Auf diese Weise hatte der Verbindende die Wahl, auf welche Weise die Kommunikation fortgesetzt werden soll. Eine solche Wahlmöglichkeit führt zu einer **opportunistischen Transportverschlüsselung**: die Sicherheit orientiert sich an den Möglichkeiten des Senders und erlaubt zudem eine unverschlüsselte Übertragung, sofern STARTTLS nicht befohlen wird. Neben STARTTLS besteht auch die Möglichkeit direkt nach der Verbindungsaufnahme eine verschlüsselte Verbindung zu initiieren (Implicit TLS).

Der Sender kann auch den Einsatz einer Verschlüsselung erzwingen oder andernfalls die Kommunikation abbrechen und den Mailsender über die fehlgeschlagene Übermittlung informieren. Dieser Modus wird als **obligatorische Transportverschlüsselung** (auch enforce TLS oder mandatory TLS) bezeichnet[12]. Anbieter wie beispielsweise Posteo ermöglichen die Aktivierung von mandatory TLS und führen nur dann die Übertragung durch, wenn eine verschlüsselte Verbindung zustande gekommen ist.

Innerhalb einer TLS-gesicherten Verbindung soll der Einsatz von Zertifikaten vor Man-in-the-Middle Angriffen schützen. Ein solches Zertifikat enthält den Hostname des Servers und einen damit verbundenen öffentlichen Schlüssel. Der öffentliche Schlüssel wird im Zuge der Kommunikation verwendet und für die Entschlüsselung ist der Kenntnis des korrespondierenden privaten Schlüssels erforderlich. Auf diese Weise kann die Gegenseite prüfen, ob Kenntnis über den privaten Schlüssel besteht. Grundsätzlich können beide Kommunikationspartner solche Zertifikate zur gegenseitigen Authentisierung einsetzen, üblicherweise weist sich jedoch nur der Server (Empfänger) über ein Zertifikat aus. Der Client übermittelt die Daten erst dann, wenn an der Authentizität des Servers keinen Zweifel besteht.

Die Zertifikate werden üblicherweise von einer dritten Partei beglaubigt. Sofern eine solche Beglaubigung von einem Dritten fehlt, handelt es sich möglicherweise um ein **selbstsigniertes** (self signed) **Zertifikat**. Auch kann es vorkommen, dass das Zertifikat für eine andere Domain als die verwendete ausgestellt wurde. So wäre ein Zertifikat für www.example.com nicht gültig für mail.example.com. Zertifikate werden nur für einen Zeitraum erteilt und können deshalb abgelaufen oder zurückgerufen worden sein.

[12]Der Begriff „Mandatory TLS“ wird in RFC 7672 näher definiert, vgl. https://datatracker.ietf.org/doc/html/rfc7672 zuletzt abgerufen am 06.03.2022.

Je nach eingesetzter Version von SSL bzw. TLS besteht eine breite Auswahl an verschiedenen Kombinationen von Algorithmen, auch Cipher Suites genannt. Um einen möglichst hohen Schutz sicherzustellen, wird von der Nutzung alter SSL- bzw. TLS-Versionen abgeraten. Stand 2022 raten das BSI und die IANA zum ausschließlichen Einsatz von TLS in der Version 1.2 und 1.3 vgl. Tab. 2.

| | |
|---|---|
| SSL 1.0 | nicht final veröffentlicht |
| SSL2.0 | nicht länger empfohlen seit 2011 |
| SSL 3.0 | nicht länger empfohlen seit 2015 |
| SSL 3.1 / TLS 1.0 | nicht länger empfohlen seit 2020, Empfehlung zu Deaktivierung wurde aufgrund der Covid19-Pandemie auf März 2021 verschoben |
| TLS 1.1 | |
| TLS 1.2 | derzeitiger Standard |
| TLS 1.3 | |

Tab. 2: SSL/TLS-Versionen und Empfehlungsstatus IANA

Die Version legt den grundsätzlichen Konfigurationsrahmen fest. Auch ist es möglich innerhalb der Versionen eine spezifische Auswahl der unterstützten Algorithmen zu treffen. Client und Server handeln auf Basis dieser Auswahl einen gemeinsam unterstützen Algorithmus aus. Schlägt dieser Aushandlungsprozess fehl, kann die Verbindung nicht aufgebaut werden.

Im Zuge des Aushandlungsprozesses könnte ein Angreifer versuchen die Aushandlung einer möglichst schwachen Verschlüsselung zu forcieren, um die Angriffsposition zu verbessern. Aus diesem Grund sollten ausschließlich starke Verschlüsselungen zum Einsatz kommen. In der technischen Richtlinie 02102-2[13] gibt das BSI eine Empfehlung zu den nutzbaren Cipher Suites ab.

[13] „Technische Richtlinie TR-02102-2 Kryptografische Verfahren: Empfehlungen und Schlüssellängen“ in der Version 2022-01, zuletzt abgerufen am 06.03.2022 unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf;jsessionid=663AE421E20CD6ADFE6BC5E124067D31.internet482?__blob=publicationFile&v=4

### 3.2 MTA-STS

Bei erstem Verbindungsaufbau ist unklar, ob vom Server eine verschlüsselte Verbindung unterstützt wird. MTA-STS (Mail Transfer Agent-Strict Transport Security), näher spezifiziert in RFC 8461[14], adressiert das Problem des Downgrade-Angriffs.

Dabei gibt sich ein Angreifer in beide Richtungen als die jeweilig andere Kommunikationspartei aus. Ein Angreifer, der in der Lage ist, die Kommunikation zwischen zwei Mailservern mitzuhören und zu modifizieren, kann das STARTTLS-Angebot vom empfangenden Mailserver entfernen. In diesem Fall würde der sendende E-Mail-Server nicht in den TLS-geschützten Modus wechseln.

Um dieses Problem zu beheben, wird im Domain Name System (DNS) neben dem MX-Eintrag zum E-Mail-Server auch ein Verweis auf eine Ressource eines Webserver platziert. Vom Webserver können weitere Daten (Policy) abgerufen werden, wie die Information, dass der E-Mail-Server über eine Verschlüsselung verfügt und angefragt werden kann. Somit kann der Client sich auf diesem Umweg versichern, ob das STARTTLS-Angebot vom Server erwartet werden kann. Ein Angreifer müsste in der Lage sein die HTTPS-geschützte Policy zu modifizieren.

MTA-STS adressiert allein das Problem des Downgrade-Angriffs, nicht die Manipulation durch Dritte auf dem Kommunikationsweg. Aus diesem Grund wird in der RFC 8461 explizit gefordert, dass das Zertifikat des Mailservers von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt wurde und nicht abgelaufen ist.

### 3.3 DANE

Um ein von der PKI losgelöstes Konzept zur zuverlässigen Verteilung von Zertifikaten zu erreichen kann ein DNS-basiertes Verteilungssystem für Zertifikate genutzt werden: DNS-based Authentication of Named Entities (kurz: DANE). Es ermöglicht die Überprüfung des Zertifikats des Zielservers ohne gemeinsames Wurzelzertifikat. Das dafür notwendige Schlüsselmaterial wird hierfür im Domain Name System (DNS) platziert: diese Einträge werden TLSA-Einträge genannt und ermöglichen die Zertifikatsüberprüfung. Um die Vertrauenswürdigkeit der Antworten sicherzustellen, müssen Antworten über DNSSEC (Domain Name System Security Extensions) gesichert sein. Wurde DNSSEC etabliert, ist ein Domaininhaber in der Lage Zertifikate für die eigene Domäne selbst auszustellen.

Die Nutzung von DANE setzt somit eine Unterstützung von DNSSEC voraus, um vor einer Manipulation der Zertifikatsinformationen durch Dritte zu schützen. Dies sowohl

[14] „SMTP MTA Strict Transport Security (MTA-STS)“, abrufbar unter https://datatracker.ietf.org/doc/html/rfc8461 und zuletzt abgerufen am 06.03.2022.

beim Empfänger, der Schlüsselmaterial im DNS ablegt, als auch beim Sender, der diese Informationen beziehen und zu validieren in der Lage sein muss.

### 3.4 DKIM, SPF und DMARC

Auch ohne Sicherung durch DNSSEC kann ein Eintrag im DNS die Sicherheit erhöhen. Ein **SPF**-Eintrag im DNS (vom Typ TXT seit 2014) soll vor gefälschten E-Mail-Absendern schützen. Über diesen Eintrag kann vom empfangenden Server geprüft werden, ob die IP-Adresse oder der Hostname des Servers, der eine E-Mail übertragen möchte, auch zur Übermittlung von E-Mails berechtigt ist. Auf diese Weise findet eine eingeschränkte Authentifizierung des sendenden E-Mail-Servers statt.

Auch ist es möglich, Schlüsselmaterial im DNS zu platzieren, um die Authentizität einer eingehenden E-Mail-Nachricht zu überprüfen. Dabei unterschreibt der sendende MTA die E-Mail mit einer digitalen Signatur und übermittelt diese als **DKIM**-Signatur in den Header-Daten der E-Mail. Der Zielserver kann auf Basis des im DNS abgelegten Schlüsselmaterials den Ursprung (im Sinne des sendenden Servers) gegenprüfen. DKIM soll somit das Fälschen von E-Mail-Absendern erschweren, da nur der sendende Mailserver zur Ausstellung einer gültigen Signatur in der Lage ist.

**DMARC** (Domain-based Message authentication, Reporting and Conformance) baut auf den Techniken SPF und DKIM auf und regelt darüber hinaus, wie der empfangende Mailserver im Falle eines Fehlers reagieren soll. Gemeinsam sollen diese Technologien die Authentizität des Absenders sicherstellen und indirekt vor SPAM-E-Mails schützen.

### 3.5 Ende-zu-Ende-Verschlüsselung

Eine Verschlüsselung, die beim Sender startet und bis zum Empfänger ununterbrochen bestehen bleibt, wird als Ende-zu-Ende-Verschlüsselung bezeichnet. Auf diese Weise soll insbesondere die Vertraulichkeit des Inhalts sichergestellt sein. Sofern Schlüsselmaterial vorhanden ist, kann über digitale Signaturen auch die Integrität und Authentizität gesichert werden. S/MIME und PGP bzw. GPG ermöglichen einen solchen Schutz.

## 4 Orientierungshilfe der DSK

Mit der Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“ mit Stand vom 16.06.2021 haben die Aufsichtsbehörden ihre Anforderungen an E-Mail-Systeme gestellt, die personenbezogene Daten übermitteln. Je nach Risiko werden technische Anforderungen an beide Seiten, den Sender und den Empfänger, gestellt. Auch wenn die Verantwortung für die Übertragung beim Sender liegt, werden Voraussetzungen für den sicheren Empfang gefordert. An dieser Stelle sollen nur die für diese Analyse wesentlichen Informationen zusammengefasst werden.

### 4.1 Obligatorische- und qualifizierte Transportverschlüsselung

Die Orientierungshilfe unterscheidet zwischen der obligatorischen und der qualifizierten Transportverschlüsselung. Bei einer obligatorischen Transportverschlüsselung soll die unverschlüsselte Übertragung ausgeschlossen werden. Sofern der Sender oder Empfänger keine Verschlüsselung unterstützen, muss die Verbindung abgebrochen werden.

Bei einer qualifizierten Transportverschlüsselung wird auf die Anforderungen der Technischen Richtlinie BSI TR-02102-2 verwiesen. Dabei soll die IP-Adresse des Zielservers über DNSSEC validiert werden. Sofern die Gegenseite zertifikatsbasiert authentisiert wird, wird die Vertrauenswürdigkeit über ein gemeinsames Wurzelzertifikat oder via DANE publizierten Vertrauensanker überprüft.

### 4.2 Risiko

Die Orientierungshilfe unterscheidet zwischen zwei Arten von Risiken: normales und hohes Risiko für die Rechte und Freiheiten natürlicher Personen. Zur Einstufung von Risiken wird auf das Kurzpapier Nr. 18 der unabhängigen Datenschutzbehörden des Bundes und der Länder „Risiko für die Rechte und Freiheiten natürlicher Personen“ verwiesen[15].

Bei normalem Risiko wird gefordert[16], dass der empfangende Server mindestens

- den Aufbau von TLS-Verbindungen ermöglichen muss und
- hierbei ausschließlich die in der BSI TR 02102-2 aufgeführten Algorithmen verwenden darf.

Innerhalb dieses Rahmens sollte der Verantwortliche für Verschlüsselung und Authentifizierung ein möglichst breites Spektrum an Algorithmen anbieten. Bei normalem Risiko wird für den Sender eine obligatorische Transportverschlüsselung gefordert und empfohlen, sich an der TR 03108-1[17] zu orientieren. Um Authentizität und Integrität zu schützen, sollten DKIM-Signaturen zum Einsatz kommen und Fehler entsprechend den Festlegungen des Absenders (DMARC) behandeln.

---

[15] Kurzpapier zur Risikoeinstufung, abrufbar unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf zuletzt abgerufen am 06.03.2022.

[16] Abschnitt „4.1.1 Verpflichtungen bei normalen Risiken“ https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschluesselung.pdf zuletzt abgerufen am 06.03.2022.

[17] Secure E-Mail-Transport, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03108/TR03108-1.pdf;jsessionid=A5F52626B2BD0E2B8207AC38E7F5BDE1.internet482?__blob=publicationFile&v=2 in der Version vom 17.02.2022.

Bei einem gezielten Empfang von E-Mails, deren Verlust der Vertraulichkeit ein hohes Risiko bedeuten, muss

- sowohl eine qualifizierte Transportverschlüsselung,
- als auch der Empfang von Ende-zu-Ende-verschlüsselten Nachrichten ermöglicht werden.

Sofern bei Verlust der Integrität ein hohes Risiko zu erwarten ist, muss ferner auch der Einsatz von digitalen Signaturen ermöglicht werden. Beim Versand wird offengelassen, wie qualifizierte Transportverschlüsselung und Ende-zu-Ende-Verschlüsselung zu kombinieren sind, um ein geeignetes Schutzniveau sicherzustellen.

Verantwortliche, die gemäß § 203 StGB zur Geheimhaltung von Kommunikationsinhalten verpflichtet sind, müssen die Anforderungen von normalem und hohem Risiko erfüllen und können darüber hinaus noch weitere Sicherheitsmaßnahmen ergreifen.

# 5 Analyse des aktuellen Stands

## 5.1 Design der Analyse

Ziel der quantitativen Analyse ist ein Vergleich der Vorgabe der Aufsichtsbehörden mit den derzeitigen Konfigurationen in der Serverlandschaft. Derartige Analysen von Mail-Servern im Internet wurden in der Vergangenheit schon häufiger durchgeführt[18].

Grundsätzlich lässt sich von außen nicht abschätzen, welche Informationen über einen E-Mail-Server ausgetauscht werden. Anhand der Zielgruppe der Analyse, Mailserver von Krankenhäusern und Kliniken, ist zu erwarten, dass personenbezogene Daten ein relevanter Teil davon sind. Auch wenn zu vermuten ist, dass eine umfassende Risikoabschätzung bzgl. der möglichen Gefahren beim E-Mail-Versand nicht immer durchgeführt wird, kann und soll nicht pauschal von einem hohen Risiko ausgegangen werden. Aus diesem Grund soll sich die Analyse nur an den Anforderungen der Aufsichtsbehörden für **normalem Risiko** orientieren, welches jedoch das Mindestmaß darstellt.

Ferner fokussiert sich die Analyse an den technischen Möglichkeiten, die von außen überprüfbar sind. Dies umfasst die Unterstützung der Transportverschlüsselung durch TLS (STARTTLS sowie Implicit TLS), die Bereitstellung eines gültigen Zertifikates, die

[18] Wilfried Mayer, Aaron Zauner, Martin Schmiedecker, Markus Huber: No Need for Black Chambers: Testing TLS in the E-mail Ecosystem at Large. ARES 2016: 10-20, abrufbar unter https://publications.sba-research.org/publications/scanTLS.pdf

Unterstützung von MTA-STS und DANE sowie die unterstützen Verschlüsselungsalgorithmen (Cipher Suites).

## 5.2 Werkzeuge

Die Analyse setzt darauf, möglichst erprobte Werkzeuge einzusetzen. Diese mussten in Teilen jedoch angepasst und erweitert werden, um eine quantitative Analyse zu ermöglichen. Zum Einsatz gekommen sind:

- die Prüfwebseite https://www.checktls.com/ ermöglicht eine Überprüfung der Mailserver in Bezug auf Verschlüsselung, Zertifikate sowie (sofern zusätzlich aktiviert) MTA-STS und DANE.
- Über das Python Modul sslyze wurden die Mailserver bzgl. der verfügbaren Protokolle und unterstützten Verschlüsselungen analysiert.
- Das zu OpenSSL zugehörige s_client-Werkzeug wurde genutzt, um zu prüfen, welche TLS-Protokolle verfügbar sind.
- Über das Python Modul dnspython wurden DNS-Einträge und die Unterstützung von DNSSEC ermittelt.

## 5.3 Ethische Aspekte und Einschränkungen

An dieser Stelle sollen auch die ethischen Aspekte einer solchen Analyse berücksichtigt werden. Protokollbedingt erfordert die Ermittlung der unterstützen Algorithmen eine Vielzahl an Verbindungsversuchen. Dabei bietet der Client bei jedem Verbindungsaufbau nur einen Algorithmus an und prüft, ob der Server diesen akzeptiert. Dabei fallen ca. 0,5 Megabyte Datenvolumen pro Server an. Aus diesem Grund wurde das Modul sslyze so modifiziert, die punktuelle Last möglichst gering zu halten, indem die Analyse auf eine längere Zeitspanne ausgedehnt wird. Trotz dieser Maßnahmen wurde beobachtet, dass einige Mailserver nach mehreren fehlgeschlagenen Verbindungsversuchen weitere Tests unterbinden. Aus diesem Grund muss davon ausgegangen werden, dass die Liste der unterstützen Cipher Suites nicht vollständig ist und ist als Untergrenze anzusehen.

Um weitgehende Vollständigkeit bzgl. der unterstützen Protokolle sicherzustellen, wurde die Ergebnisse mit openssl s_client erneut geprüft und ergänzt – dabei ist jeweils nur ein Verbindungsaufbau pro Protokoll erforderlich.

Sofern nicht explizit anders erwähnt, wurde nicht geprüft, ob die E-Mail-Adresse tatsächlich verwendet bzw. auf dem Webauftritt publiziert wurden. Auf ein solches Crawling von E-Mail-Adressen vom Internetauftritt wurde aufgrund der damit verbundenen Serverbelastung verzichtet.

### 5.4 Testmenge und -umfang

Ausganspunkt der Analyse war eine Testmenge von 3415 Adressen von Krankenhäusern und Kliniken aus verschiedenen öffentlich zugänglichen Quellen (kliniken.de, weisse-liste.de, Verzeichnisse von Krankenkassen).

Diese wurde dahingehend geprüft, ob die Webseiten noch erreichbar sind sowie Mehrfacheinträge entfernt. Für die verbleibenden 1810 Webauftritte wurde über das Domain Name System (DNS) der zugehörige Mailserver abgefragt – sofern ein Eintrag verfügbar war. Anschließend wurden Einträge zusammengefasst, die auf den gleichen Mailserver verweisen. Dies ist insbesondere bei größeren Klinikgruppen der Fall. Abschließend wurde getestet, ob ein Verbindungsaufbau zum Mailserver möglich ist, um veraltete Einträge auszuschließen. Entfernt wurden ebenfalls jene Kliniken, die Microsoft als Cloud-Dienstleister nutzen (121 Einrichtungen) – dies wird in Abschnitt „Microsoft als Dienstleister“ thematisiert.

Somit verblieben 936 E-Mail-Server, die von 1687 Einrichtungen genutzt werden bzw. deren Webauftritt über 1687 verschiedenen URLs erreichbar sind. Die Analysen fanden im Zeitraum vom 20.02.2022 bis 06.03.2022 statt.

## 6 Ergebnisse

Die Analyse ergab, dass 33 der 936 E-Mail-Server keine verschlüsselte Kommunikation ermöglichten. Der STARTTLS-Befehl wurde nicht angeboten und ein direkter verschlüsselter Verbindungsaufbau ist fehlgeschlagen. Eine daran anschließende stichprobenartige Betrachtung der Internetauftritte der Verantwortlichen zeigte jedoch, dass die E-Mail-Server in Verwendung zu sein scheinen.

In den verbleibenden 903 Mailservern, die eine Verschlüsselung unterstützen, wurden

- die Zertifikate,
- unterstützten SSL/TLS-Protokolle,
- unterstützten Verschlüsselungsalgorithmen,
- MTA-STS und
- DANE-Unterstützung

überprüft. Im Zuge der tiefergehenden Analysen ergaben sich in 81 der 936 Fälle Mailserver, die auf ein oder mehrere Analysewerkzeuge nicht reagiert haben. Dies kann durch vorgeschaltete Sicherheitsmaßnahmen (Firewalls, Gateways) begründet sein.

### 6.1 Überprüfung der Zertifikate

Neben den 33 E-Mail-Servern, die keine Verschlüsselung unterstützen, ergab sich, dass in 378 Fällen (40 %) die verwendeten Zertifikate nicht zur Authentifizierung genutzt werden können. Die Gründe hierfür sind, dass die Zertifikate selbstsigniert oder nicht für den Hostnamen des Mailservers ausgestellt waren.

Somit wird in diesen Fällen zwar eine Verschlüsselung ermöglicht, jedoch kann der Sender die Gegenseite vor der Übermittlung nicht authentifizieren. In den verbleibenden 525 Fällen (56 %) war mindestens von einem Mailserver ein gültiges Zertifikat verfügbar.

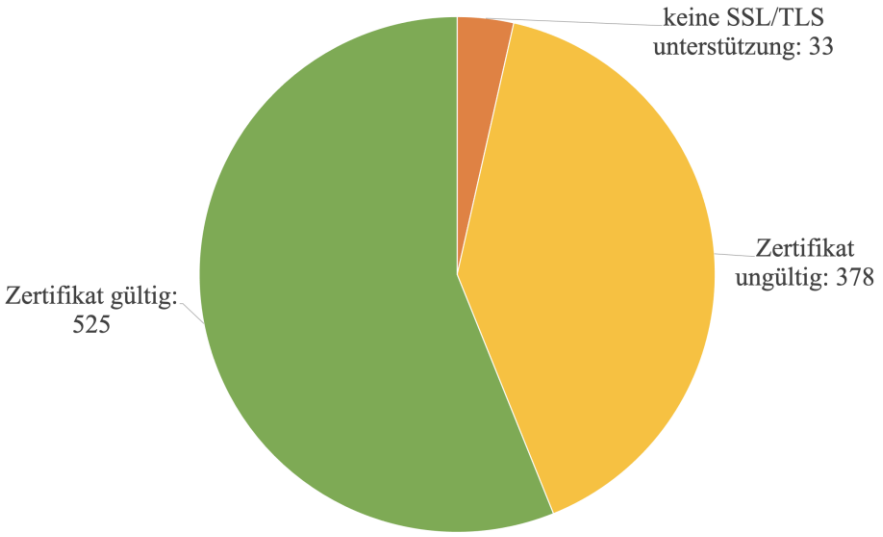


Abb. 2: Beteiligte Parteien bei Übertragung einer E-Mail

### 6.2 Unterstützte SSL/TLS-Protokolle

Wie bereits erwähnt waren hier 822 Testergebnisse aussagekräftig. In einem Fall wurde noch SSL in der Version 2 unterstützt. Bei 21 Fällen war noch eine Unterstützung von SSL in der Version 3.0 vorhanden. TLS in der Version 1.0 und 1.1 waren, entgegen der Empfehlung vom BSI, noch in 71 % bzw. 83 % unterstützt. Nahezu alle Mailserver haben eine Unterstützung von TLS in der Version 1.2 angeboten. Nur 27 % der Mailserver haben bereits eine Unterstützung von TLS in der Version 1.3.

In zwei Fällen war keine Unterstützung von TLS v1.2 und TLS v1.3 verfügbar – diese Ergebnisse wurden nochmal manuell validiert bestätigt – TLS v1.2 wurde im Jahr 2008 veröffentlicht. Somit konnten diese Server nur mittels TLS v1.1 und darunter erreicht werden.

| Unterstützte Protokolle | Anzahl | Anteil | Alleinige Unterstützung |
|---|---|---|---|
| SSL v2.0 | 1 | 0,12 % | 2: 0,24 % |
| SSL v3.0 | 24 | 2,92 % | |
| TLS v1.0 | 590 | 71,78 % | |
| TLS v1.1 | 689 | 83,82 % | |
| TLS v1.2 | 820 | 99,76 % | 126: 15,33 % |
| TLS v1.3 | 227 | 27,62 % | |
| Gesamt | 822 | | |

Tab. 3: Liste der unterstützten Protokolle

In Tab. 1 werden die Ergebnisse zusammengefasst. Zu sehen sind die Anzahl der Mailserver, welche die Protokolle unterstützt haben und deren Anteil an der Gesamtmenge. In der letzten Spalte werden die Ergebnisse dahingehend zusammengefasst, wie viele Mailserver ausschließlich nicht-empfohlene (2) oder empfohlene (126) Versionen akzeptieren. Aus der Differenz zu 822 ergibt sich, dass 696 Server (ca. 84 %) nicht-empfohlene Versionen akzeptieren.

### 6.3 Unterstützte Algorithmen

Die Analyse der unterstützten Algorithmen bei den 822 Mailservern ergab, dass nicht empfohlene Algorithmen noch eine breite Anwendung finden. Die zwei am häufigsten eingesetzten Cipher Suiten TLS_RSA_WITH_AES_256_CBC SHA bzw. TLS_RSA_WITH_AES_128_CBC_SHA, die von 93 % der Sever unterstützt werden, gelten als schwache Verfahren. Dies ist u.a. mit einer seit 2013 bekannten Schwachstelle im CBC-Modus begründet[19].

Ein Vergleich der unterstützten Algorithmen mit den Empfehlungen des BSI[20] zeigte, dass in 7 der 822 Fällen die Mailserver ausschließlich vom BSI empfohlene Algorithmen

[19] vgl. Rizzo & Duong in Practical Padding Oracle Attacks. WOOT 2010.
[20] Technische Richtlinie TR-02102-2 Kryptografische Verfahren: Empfehlungen und Schlüssellängen in der Version 2022-01, zuletzt abgerufen am 06.03.2022 unter

unterstützt werden. In den verbleibenden 815 Fällen wurden Algorithmen unterstützt, die nicht empfohlen sind.

Bei einem Vergleich mit den Empfehlungen der IANA zeigten sich nur in 10 der 822 Fälle Mailserver, die ausschließlich von der IANA empfohlene Algorithmen einsetzen. In den verbliebenen 812 Fällen wird mindestens ein Algorithmus verwendet, der von der IANA nicht empfohlen wird.

Werden die Empfehlungen von IANA und BSI zusammengefasst entsprechen 14 der 822 E-Mail-Server den Vorgaben – die verbleibenden 808 Server verwenden mindestens einen nicht empfohlenen Algorithmus.

Besonders bemerkenswert ist eine Unterstützung von EXPORT Cipher Suiten in zwei Fällen. Dabei handelt es für den Zweck des Exports absichtlich geschwächte Verschlüsselungen und gelten als Relikt bzw. sind nicht länger Bestandteil von TLS seit Version 1.2. Im Jahr 2015 wurden Schwachstellen aufgrund dieser Algorithmen unter dem Akronym FREAK bekannt[21].

Kritisch ist ebenso, dass 9 % der Server die Stromchiffre RC4 unterstützen, die seit 2015 nicht länger eingesetzt werden sollte[22]. Auch die Unterstützung von 3DES bei 22 % der Server muss als Risiko betrachtet werden. Eine vollständige Übersicht der unterstützen Algorithmen ist in Tab. 4im Anhang zu finden.

## 6.4 MTA-STS

Die Unterstützung von MTA-STS wurde über die Überprüfung eines entsprechenden DNS-Eintrags geprüft. Unabhängig von dem Ergebnis wurde ebenso versucht die Policy über HTTPS abzurufen. Es zeigte sich, dass nur vier der 822 Mailserver eine entsprechende Policy anbieten, wobei einer davon einen fehlerhaften Inhalt aufwies.

## 6.5 DANE

Insgesamt 24 der 822 Mailserver wiesen eine Unterstützung von DANE auf (2 %). Dabei konnte der DNS-Eintrag über DNSSEC validiert und der öffentliche Schlüssel zur Überprüfung des Zertifikates abgerufen werden. Inwieweit DANE tatsächlich von den E-Mail-Servern beim Versand genutzt bzw. validiert wird, kann nicht ermittelt werden.

---

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf

[21] Der FREAK-Angriff, abrufbar unter https://blog.cryptographyengineering.com/2015/03/03/attack-of-week-freak-or-factoring-nsa/ und zuletzt abgerufen am 06.03.2022.

[22] „Prohibiting RC4 Cipher Suites", RFC 7465, abrufbar unter https://datatracker.ietf.org/doc/html/rfc7465.

### 6.6 Microsoft als Dienstleister

Bei 121 Einrichtungen wurden die Ergebnisse vor Start der Analyse zusammengefasst und sind nicht Teil der 938 zuvor analysierten Mailserver. In diesen 121 Fällen wird als Dienstleister auf einen Service von Microsoft zurückgegriffen bzw. auf eine Microsoft-Domain verwiesen. Die Hostnamen der Mailserver entsprechen alle dem Aufbau „<domain>.mail.protection.outlook.com“. Da es sich um eine höhere Quantität handelt wurden diese aus der Gesamtbetrachtung herausgelöst.

Die Liste der gesichteten Cipher Suiten kann in Tab. 5 im Anhang eingesehen werden. Der Mailserver war ausschließlich über TLS in der Version 1.2 ansprechbar – eine Unterstützung von TLS 1.3 oder älteren Protokollen wurde nicht festgestellt.

### 6.7 Zusammenfassung der Ergebnisse

Entsprechend der Orientierungshilfe der Aufsichtsbehörden muss für normales Risiko eine TLS-geschützte Verbindung genutzt werden, wobei ausschließlich die vom BSI empfohlenen Algorithmen zum Einsatz kommen sollen. Die Analyse zeigt, dass dies nur in 7 der 822 Mailserver tatsächlich vorliegt. Ferner muss die Frage diskutiert werden, inwieweit von einem Schutz durch TLS ausgegangen werden kann, wenn das Zertifikat des E-Mail-Servers bei 40 % nicht geprüft werden kann.

In der technischen Richtlinie des BSI wird darauf hingewiesen, dass eine fehlende Empfehlung nicht grundsätzlich Unsicherheit bedeutet. Die Unterstützung von veralteten TLS-Protokollen bei 84 % der analysierten Mailserver ist allerdings als kritisch zu werten, da sich hier auch langfristig die Frage nach technischer Unterstützung und Sicherheitsupdates stellen würde.

Durch einen Vergleich mit den Empfehlungen der IANA zeigt sich, dass auch hier nur wenige Server (10) die Empfehlungen erfüllen. Sofern die Empfehlungen von BSI und IANA zusammengefasst werden, würden auch nur 14 Server diese einhalten.

Die geringe Abdeckung von DANE (2 %) und die Tatsache, dass in 40 % kein gültiges Zertifikat vom Mailserver ausgewiesen wird, deutet darauf hin, dass eine Umsetzung einer qualifizierten Transportverschlüsselung nur von einem kleinen Teil der Verantwortlichen angestrebt wird.

## 7 Diskussion

Die Analysen zeigen, dass die Forderungen der DSK in Bezug auf die eingesetzten Algorithmen bei den betrachteten E-Mail-Servern bisher nur wenig Berücksichtigung finden. Selbst für ein normales Risiko wird das angestrebte Schutzniveau nicht erreicht.

Die Unterstützung von nicht länger empfohlenen bzw. unterstützen Protokollen (SSL 2.0 bis TLS 1.1) bei mehr als 4 von 5 Servern ist als kritisch zu werten. Zwar kann der Wunsch nach einer möglichst breiten Kompatibilität mit älteren E-Mail-Servern aus Sicht der Betreiber nachvollzogen werden, allerdings ist TLS 1.2 bereits seit 14 Jahren veröffentlicht und es zeigten sich nur zwei Server, die dieses Protokoll nicht unterstützen. Als Betreiber wäre es in diesem Fall unkritisch die Unterstützung älterer Protokolle zu deaktivieren, was aus Sicherheitsgründen unmittelbar geschehen sollte.

Da 40 % der betrachteten Anbieter kein gültiges Zertifikat vorweisen, muss vermutet werden, dass dieses beim Versand auch nicht berücksichtigt wird. Es stellt sich jedoch die Frage, weshalb die E-Mail-Sicherheit hier so deutlich unterhalb der Möglichkeiten bleibt.

Die Ergebnisse vermitteln den Eindruck, dass im Zielkonflikt zwischen Vertraulichkeit und Authentizität auf der einen Seite und Verfügbarkeit auf der anderen Seite, die Verfügbarkeit derzeit einen höheren Stellenwert einnimmt. So ist zu vermuten, dass aus Angst vor Kompatibilitätsverlust mit älteren E-Mail-Servern eine möglichst breite Auswahl an Protokollen und Algorithmen angeboten wird.

Ähnliche Probleme konnten noch vor wenigen Jahren beim Wechsel von HTTP nach HTTPS beobachtet werden. Die Ankündigung einiger Browserhersteller, dass Webseiten ohne Verschlüsselung nur noch eingeschränkt verfügbar sein werden (Warnhinweise, insbesondere bei Passworteingabe), führte der äußeren Beobachtung nach zu einem schnellen Umdenken. Beim E-Mail-Verkehr könnten solche Änderungen von den führenden MTA-Softwareanbietern stärker forciert werden.

# 8 Anhang

| Beschreibung | Sichtungen | Anteil | BSI | IANA |
|---|---|---|---|---|
| TLS_RSA_WITH_AES_256_CBC_SHA | 709 | 93,78% | nein | nein |
| TLS_RSA_WITH_AES_128_CBC_SHA | 707 | 93,52% | nein | nein |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | 698 | 92,33% | nein | nein |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | 697 | 92,20% | ja | nein |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | 696 | 92,06% | ja | ja |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 | 696 | 92,06% | ja | nein |
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | 693 | 91,67% | ja | ja |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | 691 | 91,40% | nein | nein |
| TLS_RSA_WITH_AES_256_CBC_SHA256 | 678 | 89,68% | nein | nein |
| TLS_RSA_WITH_AES_128_CBC_SHA256 | 670 | 88,62% | nein | nein |

| | | | | |
|---|---|---|---|---|
| TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 | 640 | 84,66% | ja | ja |
| TLS_RSA_WITH_AES_256_GCM_SHA384 | 632 | 83,60% | nein | nein |
| TLS_RSA_WITH_AES_128_GCM_SHA256 | 624 | 82,54% | nein | nein |
| TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 | 623 | 82,41% | ja | nein |
| TLS_DHE_RSA_WITH_AES_256_CBC_SHA | 621 | 82,14% | nein | nein |
| TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 | 615 | 81,35% | ja | nein |
| TLS_DHE_RSA_WITH_AES_128_CBC_SHA | 614 | 81,22% | nein | nein |
| TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 | 600 | 79,37% | ja | ja |
| TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA | 487 | 64,42% | nein | nein |
| TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA | 487 | 64,42% | nein | nein |
| TLS_RSA_WITH_CAMELLIA_128_CBC_SHA | 486 | 64,29% | nein | nein |
| TLS_RSA_WITH_CAMELLIA_256_CBC_SHA | 481 | 63,62% | nein | nein |
| TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 | 205 | 27,12% | nein | ja |
| TLS_CHACHA20_POLY1305_SHA256 | 203 | 26,85% | nein | ja |
| TLS_AES_256_GCM_SHA384 | 203 | 26,85% | nein | ja |
| TLS_AES_128_GCM_SHA256 | 203 | 26,85% | nein | ja |
| TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 | 173 | 22,88% | nein | ja |
| TLS_RSA_WITH_3DES_EDE_CBC_SHA | 171 | 22,62% | nein | nein |
| TLS_RSA_WITH_SEED_CBC_SHA | 170 | 22,49% | nein | nein |
| TLS_ECDH_anon_WITH_AES_256_CBC_SHA | 170 | 22,49% | nein | nein |
| TLS_ECDH_anon_WITH_AES_128_CBC_SHA | 170 | 22,49% | nein | nein |
| TLS_RSA_WITH_AES_256_CCM | 165 | 21,83% | nein | nein |
| TLS_RSA_WITH_AES_128_CCM | 165 | 21,83% | nein | nein |
| TLS_DHE_RSA_WITH_SEED_CBC_SHA | 160 | 21,16% | nein | nein |
| TLS_RSA_WITH_AES_256_CCM_8 | 152 | 20,11% | nein | nein |
| TLS_RSA_WITH_AES_128_CCM_8 | 152 | 20,11% | nein | nein |
| TLS_DHE_RSA_WITH_AES_256_CCM | 145 | 19,18% | ja | ja |
| TLS_DHE_RSA_WITH_AES_128_CCM | 145 | 19,18% | ja | ja |
| TLS_DHE_RSA_WITH_AES_256_CCM_8 | 136 | 17,99% | nein | nein |

| | | | | |
|---|---|---|---|---|
| TLS_DHE_RSA_WITH_AES_128_CCM_8 | 136 | 17,99% | nein | nein |
| TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384 | 135 | 17,86% | nein | nein |
| TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 | 135 | 17,86% | nein | nein |
| TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384 | 132 | 17,46% | nein | nein |
| TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256 | 132 | 17,46% | nein | nein |
| TLS_RSA_WITH_ARIA_256_GCM_SHA384 | 126 | 16,67% | nein | nein |
| TLS_RSA_WITH_ARIA_128_GCM_SHA256 | 126 | 16,67% | nein | nein |
| TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256 | 126 | 16,67% | nein | nein |
| TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 | 126 | 16,67% | nein | nein |
| TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256 | 119 | 15,74% | nein | nein |
| TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256 | 119 | 15,74% | nein | nein |
| TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA | 113 | 14,95% | nein | nein |
| TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384 | 110 | 14,55% | nein | nein |
| TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256 | 110 | 14,55% | nein | nein |
| TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA | 100 | 13,23% | nein | nein |
| TLS_RSA_WITH_IDEA_CBC_SHA | 73 | 9,66% | nein | nein |
| TLS_RSA_WITH_RC4_128_SHA | 68 | 8,99% | nein | nein |
| TLS_RSA_WITH_RC4_128_MD5 | 58 | 7,67% | nein | nein |
| TLS_DH_anon_WITH_AES_256_CBC_SHA | 57 | 7,54% | nein | nein |
| TLS_DH_anon_WITH_AES_128_CBC_SHA | 57 | 7,54% | nein | nein |
| TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA | 55 | 7,28% | nein | nein |
| TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA | 55 | 7,28% | nein | nein |
| TLS_DH_anon_WITH_AES_256_GCM_SHA384 | 55 | 7,28% | nein | nein |
| TLS_DH_anon_WITH_AES_256_CBC_SHA256 | 55 | 7,28% | nein | nein |
| TLS_DH_anon_WITH_AES_128_GCM_SHA256 | 55 | 7,28% | nein | nein |
| TLS_DH_anon_WITH_AES_128_CBC_SHA256 | 55 | 7,28% | nein | nein |
| TLS_DH_anon_WITH_SEED_CBC_SHA | 52 | 6,88% | nein | nein |
| TLS_ECDHE_RSA_WITH_RC4_128_SHA | 46 | 6,08% | nein | nein |
| TLS_AES_128_CCM_SHA256 | 30 | 3,97% | nein | ja |

| | | | | |
|---|---|---|---|---|
| TLS_DH_anon_WITH_3DES_EDE_CBC_SHA | 24 | 3,17% | nein | nein |
| TLS_ECDH_anon_WITH_RC4_128_SHA | 21 | 2,78% | nein | nein |
| TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA | 21 | 2,78% | nein | nein |
| TLS_DH_anon_WITH_RC4_128_MD5 | 21 | 2,78% | nein | nein |
| TLS_AES_128_CCM_8_SHA256 | 20 | 2,65% | nein | nein |
| TLS_RSA_WITH_DES_CBC_SHA | 5 | 0,66% | nein | nein |
| TLS_DHE_RSA_WITH_DES_CBC_SHA | 5 | 0,66% | nein | nein |
| TLS_DH_anon_WITH_DES_CBC_SHA | 4 | 0,53% | nein | nein |
| TLS_RSA_EXPORT_WITH_RC4_40_MD5 | 3 | 0,40% | nein | nein |
| TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 | 3 | 0,40% | nein | nein |
| TLS_RSA_EXPORT_WITH_DES40_CBC_SHA | 3 | 0,40% | nein | nein |
| TLS_DH_anon_EXPORT_WITH_RC4_40_MD5 | 3 | 0,40% | nein | nein |
| TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA | 3 | 0,40% | nein | nein |
| TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA | 3 | 0,40% | nein | nein |
| TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 | 2 | 0,26% | ja | ja |
| TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 | 2 | 0,26% | ja | ja |
| SSL_CK_RC4_128_WITH_MD5 | 1 | 0,13% | nein | nein |
| SSL_CK_DES_192_EDE3_CBC_WITH_MD5 | 1 | 0,13% | nein | nein |

Tab. 4: Liste aller gesichteten Cipher Suiten

| Beschreibung | BSI | IANA |
|---|---|---|
| TLS_RSA_WITH_AES_256_GCM_SHA384 | nein | nein |
| TLS_RSA_WITH_AES_256_CBC_SHA256 | nein | nein |
| TLS_RSA_WITH_AES_256_CBC_SHA | nein | nein |
| TLS_RSA_WITH_AES_128_GCM_SHA256 | nein | nein |
| TLS_RSA_WITH_AES_128_CBC_SHA256 | nein | nein |
| TLS_RSA_WITH_AES_128_CBC_SHA | nein | nein |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ja | ja |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ja | nein |

| | | |
|---|---|---|
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ja | nein |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | nein | nein |
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ja | ja |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 | ja | nein |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | nein | nein |

Tab. 5: Liste der Cipher Suiten von Outlook.com