LEO DESSANI, PROF. DR. RONALD PETRLIC

DANE ALS LÖSUNG FÜR SICHERE E-MAIL-ÜBERTRAGUNG

In der Anfangszeit der E-Mail-Kommunikation ging es primär um die Möglichkeit überhaupt elektronisch kommunizieren zu können. Das SMTP-Protokoll, nach dessen Vorgaben die E-Mail-Kommunikation abläuft, sah in der ursprünglichen Version keine verschlüsselte Übermittlung von E-Mails vor. Die Absicherung der Kommunikation war damals nicht so relevant wie heute. Mit der stetig zunehmenden Nutzung der E-Mail-Kommunikation in Wirtschaft und Wissenschaft, aber auch im Privaten, wurde der Sicherheit eine immer größere Bedeutung beigemessen. Seit einigen Jahren haben sich zahlreiche technische Standards zur Absicherung der E-Mail-Kommunikation durchgesetzt (1). Gleichzeitig haben immer mehr Mail-Server-Betreiber die verschlüsselte Übermittlung von E-Mails zwischen ihren Mail-Servern ermöglicht. Die Statistiken des Mail-Dienstes Gmail von Google bestätigen das: Zwischen Juli und Oktober 2022 wurden 87 Prozent aller ausgehenden und 91 Prozent aller eingehenden E-Mails transportverschlüsselt übertragen (2). Die Zahlen zeigen aber auch, dass längst nicht alle E-Mails verschlüsselt übermittelt werden. Das liegt daran, dass Mail-Server meist die sogenannte opportunistische Transportverschlüsselung unterstützen. Konkret bedeutet das, dass eine E-Mail nur dann transportverschlüsselt übermittelt wird, wenn beide Kommunikationspartner, also der sendende und der empfangende Mail-Server, TLS unterstützen. Wenn auf einem von beiden Mail-Servern kein TLS konfiguriert ist, wird die E-Mail unverschlüsselt übertragen. TLS ist das Verschlüsselungsprotokoll, das die Transportverschlüsselung ermöglicht.

Orientierungshilfe der Datenschutzaufsichtsbehörden

Mit der Intention, einheitliche Vorgaben in Bezug auf die E-Mail-Sicherheit zu machen, haben sich die Aufsichtsbehörden nach zähem Ringen (und gegen die Stimme Bayerns) im März 2020 auf eine Orientierungshilfe zur E-Mail-Sicherheit geeinigt;[1] sie wurde im März 2021 aktualisiert,[2] dabei wurden jedoch keine wesentlichen Änderungen vorgenommen. Die Orientierungshilfe ist nicht die erste Veröffentlichung staatlicher Stellen zur E-Mail-Sicherheit. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat bereits 2009 erste Empfehlungen zum "sicheren Betrieb von E-Mail-Servern" gegeben (3). Vor Kurzem hat das BSI das erste IT-Sicherheitskennzeichen an einen E-Mail-Provider auf Basis der Technische Richtlinie TR-03108-1[3] vergeben (4). Allerdings zeigt die Orientierungshilfe der DSK auf, welche konkreten Maßnahmen die Aufsichtsbehörden fordern. Diese Maßnahmen werden im Folgenden erläutert. Für Erklärungen zu den erwähnten Begriffen und Verfahren verweisen die Autoren auf ihre Website:

▶ https://mail-sicherheit.jetzt/blog/sicherheit-des-mail-oekosystems/

Zunächst unterscheidet die Orientierungshilfe zwischen dem Empfang und dem Versand von E-Mails. Im Detail unterscheidet sie weiter zwischen normalem und hohem

[1] vgl. https://mail-sicherheit.jetzt/wp-content/uploads/2021/07/orientierungshilfe_dks_email_2020.pdf, Letzter Zugriff: 03.10.2022.

[2] vgl. https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschluesselung.pdf, Letzter Zugriff: 03.10.2022.

[3] vgl. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03108/TR03108-1.pdf?__blob=publicationFile, Letzter Zugriff: 07.10.2022.

LINKS UND LITERATUR ZUR SICHEREN E-MAIL

1. Chen/Paxson/Jiang (2020): Composition kills: A case study of email sender authentication. In: 29th USENIX Security Symposium (USENIX Security 20), S. 2183-2199.

2. Google-Transparenzbericht zur E-Mail-Verschlüsselung bei der Übertragung: https://transparencyreport.google.com/safer-email/overview.

3. Bundesamt für Sicherheit in der Informationstechnik: Sicherer Betrieb von E-Mail-Servern. BSI-Studie zur Internet-Sicherheit (2009): https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_mail_server_studie_pdf.pdf?__blob=publicationFile&v=1,

4. IT-Sicherheitskennzeichen des Bundesamts für Sicherheit in der Informationstechnik: https://www.bsi.bund.de/SharedDocs/IT-Sicherheitskennzeichen/DE/2022/sik-01001_mail_de_freemail.html

5. Moriarty/Farrell (2021): RFC 8996, Deprecating TLS 1.0 and TLS 1.1. Internet Engineering Task Force (IETF). https://datatracker.ietf.org/doc/rfc8996/

6. Petrlic/Dessani (2021): E-Mail-Sicherheit auf dem Prüfstand: Forderungen der Aufsichtsbehörden vs. Absicherung in der Realität. In: Datenschutz und Datensicherheit, Ausgabe 8, S. 534-540.

7. Dessani/Petrlic (2021): Fehlender Vertrauensanker: Datenschutzprobleme bei Mailhosting-Anbietern. In: c't – magazin für computertechnik, Ausgabe 13, S. 132-137.

8. Google Workspace: Advancing email security for Gmail and beyond with BIMI. https://cloud.google.com/blog/products/identity-security/bringing-bimi-to-gmail-in-google-workspace, 2021.

Risiko. Der Risikobegriff wird in der Orientierungshilfe selbst nicht näher definiert, jedoch hat die Datenschutzkonferenz dazu bereits ein Kurzpapier[4] veröffentlicht.

Für den **Empfang von E-Mails mit normalem Risiko** müssen die Mail-Server laut der Orientierungshilfe mindestens eine opportunistische Verschlüsselung unterstützen; technisch wird das mit dem Verfahren START-TLS realisiert. Unverschlüsselte Verbindungsversuche können abgelehnt werden, eine Verpflichtung hierzu besteht aber nicht. Die verschlüsselten Verbindungen müssen mit sicheren Algorithmen nach dem Stand der Technik aufgebaut werden, die das BSI in der Technischen Richtlinie TR 02102-2[5] freigegeben hat. Konkret bedeutet das die Verwendung von TLS 1.2 und 1.3 mit sicheren Cipher Suites, nicht mehr aber TLS 1.0 und 1.1 (5). Zusätzlich muss für eingehende E-Mails – sofern vorhanden – die DKIM-Signatur überprüft werden, um sicherzustellen, dass die E-Mail von einem berechtigten Absender verschickt wurde.

Beim **Empfang von E-Mails mit hohem Risiko** fordert die Orientierungshilfe die Implementierung einer sogenannten "qualifizierten Transportverschlüsselung". Dabei müssen die eingesetzten TLS-Versionen – nach heutigem Stand – TLS 1.2 oder 1.3 sein und den Anforderungen der TR 02102-2 genügen sowie Perfect Forward Secrecy (PFS)[6] unterstützen. Außerdem müssen die Verantwortlichen die DNS-Einträge ihrer Domains mittels DNSSEC signieren und dafür sorgen, dass die Authentizität des Mail-Servers über einen zweiten Kanal überprüft werden kann. Was sich kompliziert anhört, ist im Endeffekt nichts anderes als die Konfiguration von DANE. Alternativ ist die Konfiguration von MTA-STS möglich, allerdings weist dieses Verfahren im Vergleich zu DANE einige Schwächen auf (6). Die Orientierungshilfe gibt zusätzlich vor, dass Verantwortliche den Empfang Ende-zu-Ende-verschlüsselter E-Mails ermöglichen müssen. Im besten Fall wird das durch Bereitstellen eines öffentlichen PGP- oder S/MIME-Schlüssels ermöglicht. Außerdem müssen Verantwortliche vorhandene PGP- oder S/MIME-Signaturen überprüfen.

Für den **Versand von E-Mails mit normalem Risiko** fordern die Aufsichtsbehörden in ihrer Orientierungshilfe zwingend eine verschlüsselte Übertragung der E-Mail ("obligatorische Transportverschlüsselung"). Demzufolge dürfen E-Mails nur dann versendet werden, wenn der Empfangsserver entsprechend der TR 02102-2 sichere TLS-Versionen unterstützt, also wieder TLS 1.2 oder 1.3 mit sicheren Cipher Suites.

Einen Schritt weiter gehen die Aufsichtsbehörden beim **Versand von E-Mails mit hohem Risiko**: Hier fordern sie "regelmäßig" eine qualifizierte Transportverschlüsselung. Eine E-Mail sollte also nur dann übertragen werden, wenn der empfangende Mail-Server TLS 1.2 oder 1.3 mit sicheren Cipher Suites, PFS und DANE bzw. MTA-STS unterstützt. Außerdem wird "regelmäßig" eine Ende-zu-Ende-Verschlüsselung gefordert. Wenn Verantwortliche also bei ausgehenden E-Mails sowohl eine qualifizierte Transportverschlüsselung als auch eine Ende-zu-Ende-Verschlüsselung einsetzen, sind sie auf der sicheren Seite.

[4] vgl. Kurzpapier Nr. 18: Risiko für die Rechte und Freiheiten natürlicher Personen, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf.

[5] vgl. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?__blob=publicationFile&v=4.

[6] Perfect Forward Secrecy (PFS) verhindert, dass eine aufgezeichnete verschlüsselte Kommunikation im Nachhinein entschlüsselt werden kann, und zwar auch dann, wenn der geheime Schlüssel ("Langzeitschlüssel") später versehentlich bekannt wird. Siehe auch: Claudia Eckert (2018): IT-Sicherheit. De Gruyter Oldenbourg, Berlin, 10. Auflage, S. 418.

Die von den Aufsichtsbehörden geforderten Maßnahmen sind zur besseren Übersicht in der folgenden Tabelle dargestellt:

	SMTP mit TLS (TLS 1.2 oder 1.3)	DKIM	Ende-zu-Ende-Verschlüsselung	Signaturprüfung	Obligatorische Transportverschlüsselung	Qualifizierte Transportverschlüsselung
Empfang, normales Risiko	ja, STARTTLS	Bei eingehenden Mails prüfen				
Empfang, hohes Risiko	ja		ja, im besten Fall öffentlichen Schlüssel bereitstellen	ja		ja
Versand, normales Risiko	ja				ja	
Versand, hohes Risiko	ja		ja			ja

Eine unmittelbare (rechtliche) Pflicht zur Umsetzung der geforderten Maßnahmen lässt sich aus der Orientierungshilfe nicht ableiten. Allerdings sind Verantwortliche u. a. nach Art. 32 DSGVO für die Sicherheit bei der Verarbeitung personenbezogener Daten nach dem „Stand der Technik" zuständig. Auch wenn die geforderten Maßnahmen in der Orientierungshilfe als Empfehlungen zu verstehen sind und es an mehreren Stellen Optimierungspotential gibt, stellen sie ein gutes Schutzniveau dar. Außerdem spiegeln sie die Sichtweise fast aller Aufsichtsbehörden wider und können insofern als guter Wegweiser verstanden werden.

Stand der Umsetzung der Orientierungshilfe

Nachdem bis Mitte 2021 keine Ergebnisse zum Stand der Umsetzung der Orientierungshilfe bekannt waren, entschieden sich die Autoren dieses Beitrags zu einer großflächigen Prüfung: Einerseits sollten namhafte Webhosting-Provider und große Anwaltskanzleien getestet werden, gleichzeitig sollte geprüft werden, ob die Aufsichtsbehörden ihre eigenen Vorgaben einhalten. Im Jahr 2022 untersuchte einer der Autoren dieses Beitrags, Prof. Dr. Ronald Petrlic, gemeinsam mit einer Studierendengruppe der TH Nürnberg zusätzlich die Umsetzung der Maßnahmen bei medizinischen Einrichtungen in Deutschland.[7]

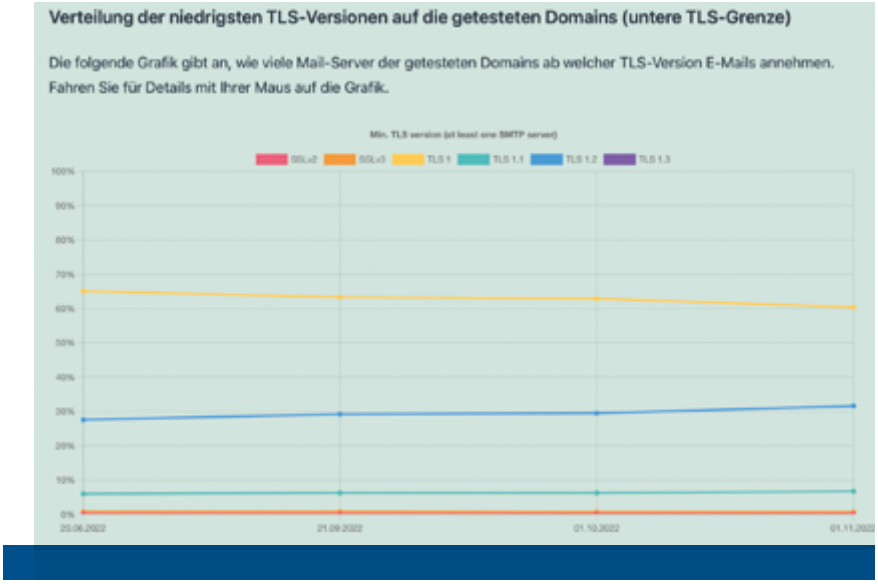
Webhosting-Provider, die die Websites der Verantwortlichen in (eigenen) Rechenzentren bereitstellen, betreiben meist auch deren Mail-Dienst. Eine Untersuchung der Mail-Server namhafter Webhosting-Provider, die teilweise mehrere Millionen Domains hosten, lieferte daher einen guten Überblick über den Stand der E-Mail-Sicherheit bei Verantwortlichen (7).

Insgesamt testeten die Autoren 18 Webhosting-Provider. Alle Webhosting-Provider ermöglichten die opportunistische Transportverschlüsselung mittels STARTTLS und PFS. Bei allen Providern stand TLS 1.2 zur Verfügung, bei manchen sogar TLS 1.3. Leider unterstützten fast alle Provider auch die veralteten TLS-Versionen 1.0 und 1.1 oder gar den unsicheren TLS-Vorgänger SSL. DANE und eine obligatorische Transportverschlüsselung unterstützten nur jeweils zwei Provider. Somit setzte kaum ein Verantwortlicher, der einen (Auftragsver-

[7] Lange/Chang/Fiedler/Petrlic: An Email a Day Could Give Your Health Data Away. In: Data Privacy Management Workshop (DPM), 2022.

arbeitungs-)Vertrag mit einem der getesteten Webhosting-Provider hatte, alle Forderungen der Orientierungshilfe um.

Auch Kanzleien waren Teil des Tests der Autoren (6). Insgesamt wurden sechs Kanzleien getestet. Deren Mail-Server unterstützten die opportunistische Transportverschlüsselung mittels STARTTLS und PFS sowie TLS 1.2, manche auch TLS 1.3. Leider konnten die Autoren bei den Mail-Servern einiger Kanzleien auch TLS 1.0 oder 1.1 oder gar SSL 3 feststellen. DANE wurde von keiner Kanzlei unterstützt, SPF von allen.



Aktuelle Testergebnisse stehen auf der Autoren-Website unter

▶ www.mail-sicherheit.jetzt/tests

zur Verfügung. Sie werden monatlich aktualisiert.

Vorschläge für die Praxis

Die in der Orientierungshilfe genannten Maßnahmen zur E-Mail-Sicherheit sind zum Teil praxisnah umsetzbar und dienen als guter Wegweiser. Allerdings vermissen die Autoren an einigen Stellen den Blick für die Praxis. Außerdem fehlen wichtige Verfahren zur Sicherung der E-Mail-Kommunikation oder werden nicht ausreichend beschrieben.

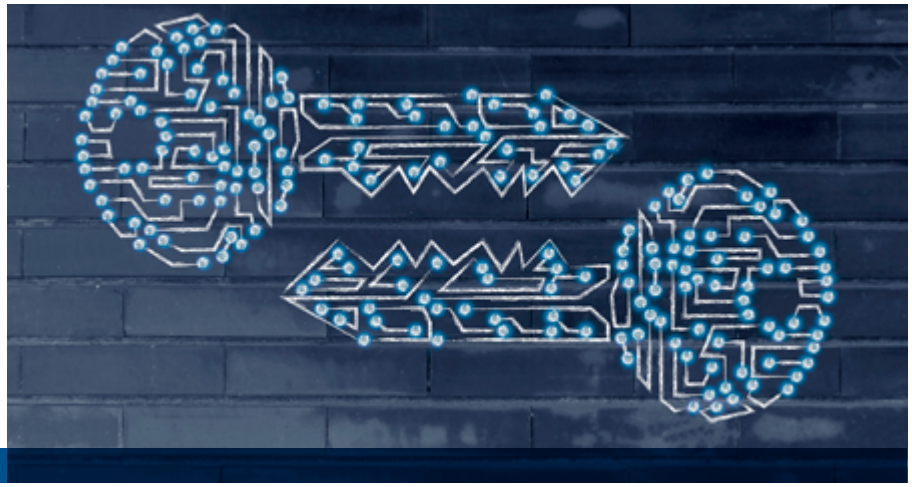
Auch bei den Aufsichtsbehörden des Bundes und der Länder waren die Ergebnisse durchwachsen (6): Alle unterstützten opportunistische Transportverschlüsselung mittels STARTTLS und PFS. Bei allen Behörden war mindestens TLS 1.2 konfiguriert, teilweise auch 1.3. DANE unterstützten allerdings nur wenige. SPF war nicht bei allen Behörden konfiguriert, obwohl das seit Langem zum Stand der Technik gehört (1). Zwar existieren bei den Behörden teilweise Abhängigkeiten von der IT-Infrastruktur der Länder, dennoch zeigte sich in den Tests der Autoren, dass die Aufsichtsbehörden ihre eigenen Forderungen an die E-Mail-Sicherheit nicht vollständig umsetzen.

Der Stand der E-Mail-Sicherheit bei medizinischen Einrichtungen in Deutschland war wie folgt: Die Unterstützung von STARTTLS war mit 99,5 Prozent aller getesteten Mail-Server erwartungsgemäß hoch. Des Weiteren unterstützten 99,5 Prozent die aktuellen TLS-Versionen 1.2 und 1.3. Die Verfügbarkeit von DANE war mit ~0,9 Prozent aller getesteten Mail-Server allerdings sehr gering. Nur 25 von 2836 analysierten Mail-Servern – die von 81 verschiedenen medizinischen Einrichtungen genutzt werden – waren vollständig mit DANE geschützt und erfüllten damit die Anforderungen der Aufsichtsbehörden für E-Mail-Kommunikation mit hohem Risiko. Alle anderen medizinischen Einrichtungen dürften entsprechend den Vorgaben der Aufsichtsbehörden beispielsweise keine Gesundheitsdaten nach Art. 9 Abs. 1 DSGVO per E-Mail übermitteln, es sei denn, sie setzen weitere technische Schutzmaßnahmen ein wie eine Ende-zu-Ende-Verschlüsselung mittels PGP oder S/MIME ein. In der Praxis dürfte das unter anderem aufgrund der schlechten Benutzerfreundlichkeit und der hohen Komplexität nicht realistisch umsetzbar sein.

Die Forderung nach Ende-zu-Ende-Verschlüsselung ist nicht wirklichkeitsnah. Zwar wäre der großflächige Einsatz von Ende-zu-Ende-Verschlüsselung wünschenswert – in der Praxis nutzt aber kaum eine Privatperson Verfahren wie PGP oder S/MIME[8], sodass allein schon der Bezug des öffentlichen Schlüssels vom Kommunikationspartner scheitern dürfte. Anstelle der Ende-zu-Ende-Verschlüsselung sprechen sich die Autoren für den großflächigen Einsatz von DANE aus: Damit kommt man einer obligatorischen Transportverschlüsselung sehr nahe und kann gleichzeitig sicherstellen, dass eine E-Mail tatsächlich an den richtigen Mail-Server übermittelt wird. DANE ist ein Verfahren, das vom Administrator des Mail-Servers aktiviert und konfiguriert werden muss, also meist vom Webhosting- oder Mail-Provider. Der Endnutzer hat keine Möglichkeit das Verfahren selbst zu aktivieren – was den Vorteil hat, dass er sich nicht in die Details der Konfiguration einarbeiten muss.

Darüber hinaus gehören zu einem Mail-Setup, das dem Stand der Technik entspricht, mindestens das Signieren von ausgehenden E-Mails mit DKIM und das Einrichten von SPF so-

[8] Christian Stransky, Oliver Wiese, Volker Roth, Yasemin Acar und Sascha Fahl (2022): 27 Years and 81 Million Opportunities Later: Investigating the Use of Email Encryption for an Entire University. In 43rd IEEE Symposium on Security & Privacy. IEEE Computer Society.



wie DMARC, um Spam-Mails mit einem Absender der eigenen Domain erkennen zu können. Diese Maßnahmen werden in der Orientierungshilfe leider nicht beschrieben; sie sind aber für eine zeitgemäße Absenderauthentifizierung relevant.

Für noch mehr Sicherheit lohnt sich ein Blick auf ein vielversprechendes, aktuell aber noch junges Verfahren: BIMI ermöglicht es, eine Bildmarke – beispielsweise das Logo eines Unternehmens – als Icon beim Empfang von E-Mails anzuzeigen und wird unter anderem bereits von Gmail unterstützt (8). Dabei wird gewährleistet, dass nur der Markeninhaber ein gültiges Icon anzeigen kann. Wird also eine Spam-Mail von einer gefälschten Adresse versendet, ist für den Empfänger unmittelbar erkennbar, dass die E-Mail nicht authentisch ist. BIMI setzt SPF, DKIM, DMARC und die Eintragung einer Bildmarke in einem Markenregister voraus, weswegen die Implementierungskosten aktuell nicht gering sind.

Über die Autoren

Leo Dessani
ist Mitarbeiter am Lehrstuhl für Rechtsinformatik der Universität des Saarlandes. Er war im Sommersemester 2022 Lehrbeauftragter für IT-Sicherheit an der Hochschule Reutlingen und ist seit dem Wintersemester 2022/2023 Lehrbeauftragter für IT-Sicherheit und Datenschutz an der Deutschen Universität für Verwaltungswissenschaften Speyer. Sein Forschungsinteresse liegt in den Bereichen technischer Datenschutz, Privacy-Preserving Machine Learning und Sicherheit von Rechnernetzen.

Prof. Dr. Ronald Petrlic
ist seit 2020 Professor für Informationssicherheit an der TH Nürnberg. Davor war er Leiter des Technik-Referats beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg. Er ist Autor zahlreicher wissenschaftlicher Artikel, Gesetzes-Kommentare und des ersten Lehrbuchs zu „Privacy by Design".

Um die E-Mail-Kommunikation sicher zu machen ist eine regelmäßige Überprüfung der eingesetzten Techniken nötig. Die Autoren betreiben unter ▶ www.mail-sicherheit.jetzt ein Portal für das Voranbringen der E-Mail-Sicherheit in der Praxis, auf dem sich Tipps dazu finden.