

E-Mailing

Unsere Verantwortung für die Gesellschaft

Michael Georg Schmidt



Eine Veranstaltung im Rahmen des

CEC - Cyber Ethics Camp

Moderation und Impuls

Prof. Dr. Matthias Schmidt (BHT)

Michael Georg Schmidt (THL)

Kontakt:

E info@its-explained.com

M +49 155 60 988 500

Signal: ITS_Nerd.01

Threema: WYH86UFA

14. Oktober 2025

Zusammenfassung

Um der besseren Lesbarkeit Willen verwende ich in diesem Text nur die generische Geschlechtsform. Dennoch ist mir die Gleichberechtigung aller Geschlechter ausgesprochen wichtig.

E-Mails benutzen wir alle. Täglich. In diesen E-Mails sind in der Regel *personenbezogene Daten* enthalten. Je persönlicher, desto relevanter für Dritte. E-Mails sind nämlich im Normalfall wie Postkarten. „Alle“ können sie mitlesen. Einige Anbieter halten es für einen *Service*, dass sie unsere E-Mails mitlesen, semantisch auswerten und zu persönlichen Profilen verarbeiten. Persönlichen Profilen auch Dritter. Diese E-Mailanbieter sind oft so organisiert, dass eine wirksame Verschlüsselung von E-Mails nicht möglich ist. Damit auch nicht der Schutz der Privatsphäre. Wenn wir für uns allein entscheiden, dass wir auf Privatsphäre verzichten wollen, ist das eine Sache. Wenn wir jedoch personenbezogene Daten Dritter exponieren, tun wir das in der Regel ohne deren Einverständnis. Hier kommt E-Mailverschlüsselung ins Spiel, um die Privatsphäre Dritter zu schützen. Die eigene natürlich auch.

Inhaltsverzeichnis

1	E-Mails - wie elektronische Postkarten	4
1.1	E-Mails schützen - mit Verschlüsselung	4
1.2	Symmetrische Verschlüsselung kurz erklärt	5
2	Anbieter	5
2.1	Einige Anbieter mit vertrauenswürdigem Ruf	5
2.2	Persönliche Präferenz des Autors	6
2.3	Begründung für meinen Einsatz von ProtonMail	6
2.4	Zum Abschluss	7
	Quellennachweis	8

1 E-Mails - wie elektronische Postkarten

E-Mails sind von Dritten leicht mitlesbar. Damit haben wir keine Kontrolle darüber, wer welche Informationen erhält. Das können Betriebs-Internas sein, aber auch personenbezogene Daten Dritter. Diese Dritten können sich nicht dagegen wehren, dass Informationen über sie unkontrolliert verbreitet werden. Das ist nicht nur *ethisch* fragwürdig, sondern auch *rechtswidrig*.

1.1 E-Mails schützen - mit Verschlüsselung

Gegen die ungewollte Verbreitung von Daten per E-Mail hilft es, E-Mails zu verschlüsseln. Am besten mit einer *Ende-zu-Ende-Verschlüsselung* - *End-to-End-Encryption* - *E2EE* [19]. E2EE bedeutet, dass Ihre Daten auf dem Gerät, auf dem Sie die E-Mail verfassen, verschlüsselt wird. Wenn Sie einen *E-Mail-Client* - wie *Thunderbird* [3] - nutzen, sogar lokal. Bei Webmails auf dem Mailserver. Das birgt die Gefahr, dass auf dem Weg von Ihrem Gerät zum Mailserver ein Angreifer mitliest. Anschließend wird die E-Mail verschlüsselt übertragen. Verschlüsselt zwischengespeichert. Erst der Empfänger kann sie wieder entschlüsseln - mit dem richtigen Passwort.

Zwei Möglichkeiten zur Verschlüsselung

Hier benenne ich *zwei Möglichkeiten* zur Verschlüsselung.

1. PGP - Pretty Good Privcy [20]
eine *asymmetrische Verschlüsselung* [18]
2. ProtonMail [11]
eine *symmetrische Verschlüsselung* [17]

PGP ist ein Klassiker der Verschlüsselung. Es setzt jedoch voraus, dass beide Seiten PGP nutzen und damit umgehen können. Beides ist eher selten der Fall. Wenn man PGP falsch anwendet, kann es schnell „gefährlich“ werden. Außerdem besteht bei PGP die Möglichkeit, dass sich Dritte als man selbst ausgeben. Dagegen kann man nichts machen. Daher gehe ich an dieser Stelle nicht weiter auf die Nutzung von PGP ein.

Symmetrische Verschlüsselung hingegen macht es möglich, E2EE leicht zu nutzen, und es ist keine Installation eines Programms notwendig, auf keiner Seite.

1.2 Symmetrische Verschlüsselung kurz erklärt

Bei der *symmetrischen Verschlüsselung* kommt *ein Schlüssel* sowohl für die *Verschlüsselung* als auch für die *Entschlüsselung* zum Einsatz. In diesem Fall legen Sie ein *Passwort* fest, das Sie dem Empfänger mitteilen. Dieser kann die E-Mail mit dem Passwort öffnen. So ist sichergestellt, dass keine unbefugte Person Zugriff auf die Inhalte und Anhänge der E-Mail nehmen kann.

2 Anbieter

Bei der Wahl eines E-Mailproviders - Anbieters - sollte man folgende Dinge beachten

- Anbieter sollte seinen Firmensitz in der *EU* oder der *Schweiz* haben. Damit genießt man ein hohes Maß an Datenschutz. Am 01. September 2023 trat das reformierte DSG der Schweiz in Kraft. Kritiker sind der Meinung, dass es den Datenschutz schwächt. Die Intention ist jedoch das Gegenteil.
- Anbieter sollte *auf keinen Fall* seinen Firmensitz in den *USA* haben. „Nicht Amerikaner“ genießen in den USA ***keinen*** Datenschutz. Die Möglichkeit des geheimen Zugriffs auf Daten durch amerikanische Behörden ist gegeben. Unter den aktuellen politischen Bedingungen ist die Wahrscheinlichkeit noch höher.
- Anbieter sollte *E2EE* anbieten, am besten *symmetrisch*.

2.1 Einige Anbieter mit vertrauenswürdigen Ruf

Die folgenden Anbieter für E-Maildienste genießen ein gutes Renommè.

- GMX [5] - Form von PGP-Verschlüsselung
- mailbox.org [8] - PGP-Verschlüsselung
- Tresorit [1] - Symmetrische Verschlüsselung
- Tuta [14] - Symmetrische Verschlüsselung
- Posteo [10] - PGP-Verschlüsselung
- ProtonMail [11] - Symmetrische Verschlüsselung
- Web.de [15] - Form von PGP-Verschlüsselung

Die Anbieter GMX und Web.de haben den gleichen Mutterkonzern und treten auch sehr ähnlich auf. Diese Aufzählung ist *nicht* vollständig. Es gibt vermutlich noch mehr vertrauenswürdige E-Mailanbieter.

2.2 Persönliche Präferenz des Autors

Ich nutze am liebsten *ProtonMail* [11].

2.3 Begründung für meinen Einsatz von ProtonMail

ProtonMail [11] ist ein Anbieter aus der Schweiz, der damit ein hohes Maß an *Datenschutz* garantiert. Dieser ist durch das schweizer *Bundesgesetz über den Datenschutz* [13] garantiert.

ProtonMail [11] bietet aus meiner Sicht folgende weitere Vorteile

- Ende-zu-Ende-Verschlüsselung (symmetrisch) [19, 17]
- leicht zu bedienen
- einsetzbar auf Desktop und Mobilgeräten (Apps)
- auch per Web(mail) nutzbar
- Entfernt auf Wunsch *Metadaten* [16] von angehängten Bildern
- erkennt, wenn angezeigter Absender und Absende-Domain nicht übereinstimmen - Schutz vor Phishing
- selbst zerstörende E-Mails
- geplant versendete E-Mails (Zeitpunkt des Versands kann vorher festgelegt werden)
- entfernt automatisch bekannte E-Mail-Tracker - Anbieter von E-Mailtrackern [7, 9, 6, 4, 2, 12] ¹
- bietet bei Einrichtung eines (kostenlosen) E-Mailkontos folgende weitere Sicherheits-Features an
 - verschlüsselte Kalender (3)
 - VPN [21] mit Servern in 5 Ländern
 - 5 GB Cloudspeicher

¹Diese Aufzählung soll zeigen, wie verbreitet E-Mail-Tracking ist.

- gemeinsame Dokumentbearbeitung
- Passwortmanager
- 10 E-Mailadressen zur Verschleierung der eigenen E-Mailadresse

Diese Features sind *kostenlos*. In der Bezahlversion gibt es noch die Möglichkeit eigene *Maildomains* zu verwenden und alle angebotenen Möglichkeiten können erheblich ausgedehnt werden. Mit einer entsprechenden Desktop-App kann der Cloudspeicher in den lokalen „Datei-Explorer“ eingebunden werden. Es ist zusätzlich möglich, Ordner und Dateien in eine *automatische* Echtzeitsicherung einzubinden. Da diese *inkrementell* [22] ist, werden nur die Änderungen in die Cloud geladen und man spart Speicherplatz.

2.4 Zum Abschluss

Wichtig ist, dass Sie einen E-Mailanbieter *innerhalb Europas* oder aus der *Schweiz* wählen. *E2EE* sollte auf jeden Fall möglich sein. Welchen Anbieter und welche Form der Verschlüsselung Sie vorziehen, ist Geschmackssache, möglicherweise auch eine Entscheidung der Kosten. *ProtonMail* [11] ist dabei preislich moderat.

Vielleicht kennen Sie auch andere Anbieter, die unbedingt empfehlenswert sind. In diesem Fall würde ich mich über einen Hinweis freuen.

Quellennachweis

- [1] TresorIT Knowledge Base. “So senden Sie verschlüsselte E-Mails”. In: (Aug. 2025). 06. URL: <https://support.tresorit.com/hc/de/articles/4978900013842-So-senden-Sie-verschl%C3%BCsselte-E-Mails>.
- [2] Jeroen Corthout. “7 beste E-Mail-Tracker für Gmail & Outlook”. In: (Aug. 2025). 06. URL: <https://blog.salesflare.com/de/beste-email-tracker>.
- [3] Mozilla Foundation. “Befreien Sie Ihren Posteingang”. In: (Aug. 2025). 06. URL: <https://www.thunderbird.net/de/>.
- [4] Mail Tracker for Gmail. “Know when your E-Mails are opened”. In: (Aug. 2025). 06. URL: <https://mailtrack.email/>.
- [5] GMX. “GMX E-Mail”. In: (Aug. 2025). 06. URL: https://www.gmx.net/mail/#.pc_page.homepage.index.nav.mail.
- [6] Hubspot. “Kostenlose E-Mail-Tracking Software”. In: (Aug. 2025). 06. URL: <https://www.hubspot.de/products/sales/email-tracking>.
- [7] inxmail. “Wie funktioniert E-Mail-Tracking?” In: (Aug. 2025). 06. URL: <https://www.inxmail.de/de/wissen/knowledge-base/verteileraufbau-und-pflege/wie-funktioniert-e-mail-tracking/>.
- [8] mailbox.org. “Damit Privates privat bleibt”. In: (Aug. 2025). 06. URL: <https://mailbox.org/de/>.
- [9] Mailsuite. “Email Tracker for Gmail”. In: (Aug. 2025). 06. URL: <https://mailsuite.com/en/>.
- [10] Posteo. “Grün, sicher, werbefrei”. In: (Aug. 2025). 06. URL: <https://posteo.de/de>.
- [11] Proton. “Ein besseres Internet beginnt mit Privatsphäre und Freiheit”. In: (Aug. 2025). 06. URL: <https://proton.me/de>.
- [12] ReadNotify.com. “track your email”. In: (Aug. 2025). 06. URL: <https://www.readnotify.com/>.
- [13] Schweiz. “Bundesgesetz über den Datenschutz”. In: (Sep. 2020). 25. URL: <https://www.fedlex.admin.ch/eli/cc/2022/491/de>.
- [14] Tuta. “Turn ON Privacy”. In: (Aug. 2025). 06. URL: <https://tuta.com/de>.
- [15] Web.de. “E-Mail, Cloud und smarte Funktionen”. In: (Aug. 2025). 06. URL: https://web.de/email/#.pc_page.homepage.index.nav.mail.

- [16] Wikiepedia. “Metadaten”. In: (Aug. 2025). 06. URL: <https://de.wikipedia.org/wiki/Metadaten>.
- [17] Wikiepedia. “Symmetrisches Kryptosystem”. In: (Aug. 2025). 06. URL: https://de.wikipedia.org/wiki/Symmetrisches_Kryptosystem.
- [18] Wikipedia. “Asymmetrisches Kryptosystem”. In: (Aug. 2025). 06. URL: https://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem.
- [19] Wikipedia. “Ende-zu-Ende-Verschlüsselung”. In: (Aug. 2025). 06. URL: <https://de.wikipedia.org/wiki/Ende-zu-Ende-Verschl%C3%BCsselung>.
- [20] Wikipedia. “Pretty-Good-Privacy”. In: (Aug. 2025). 06. URL: https://de.wikipedia.org/wiki/Pretty_Good_Privacy.
- [21] Wikipedia. “Virtual Private Network”. In: (Aug. 2025). 06. URL: https://de.wikipedia.org/wiki/Virtual_Private_Network.
- [22] Wiktionary. “inkrementell”. In: (Aug. 2025). 06. URL: <https://de.wiktionary.org/wiki/inkrementell>.