Zeitschrift: Schweizer Monat : die Autorenzeitschrift für Politik, Wirtschaft und Kultur

Band: 102 (2022)

Heft: 1093

Artikel: Viel ungeschützter Verkehr

Autor: Etter, Kaspar

DOI: https://doi.org/10.5169/seals-1035429

Viel ungeschützter Verkehr

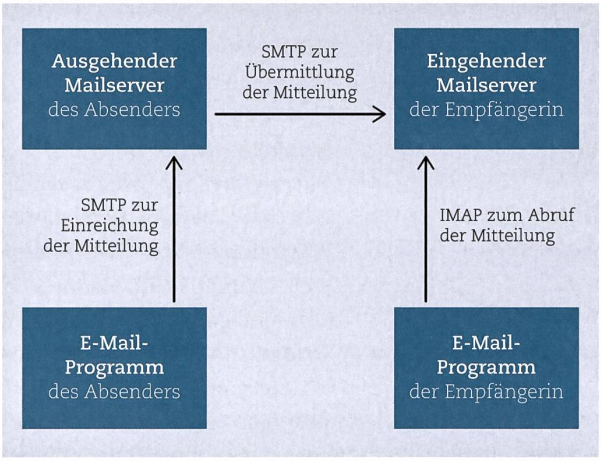
E-Mails können heute sicher übermittelt werden, wenn Absender und Empfängerin das auch beide wollen. Insbesondere in der Geschäftswelt fehlt es aber an den nötigen Sicherheitsvorkehrungen.

von Kaspar Etter

Die E-Mail ist in unserem Alltag allgegenwärtig – wir verwenden sie sowohl am Arbeitsplatz wie auch in unserem Privatleben. Wir erhalten per E-Mail Zahlungsaufforderungen und setzen die Passwörter unserer Online-Konten zurück. Ist das wirklich sicher? Oder sollten wir uns ernsthafte Sorgen machen, wie leichtfertig wir sensitive Daten via E-Mail teilen?

Um die Probleme von E-Mail nachvollziehen zu können, müssen wir zuerst verstehen, wie E-Mail überhaupt funktioniert. E-Mails werden mit dem *Simple Mail Transfer Protocol (SMTP, 1982)* verschickt und in der Regel mit dem *Internet Message Access Protocol (IMAP, 1988)* abgefragt. Das kann man sich so vorstellen:

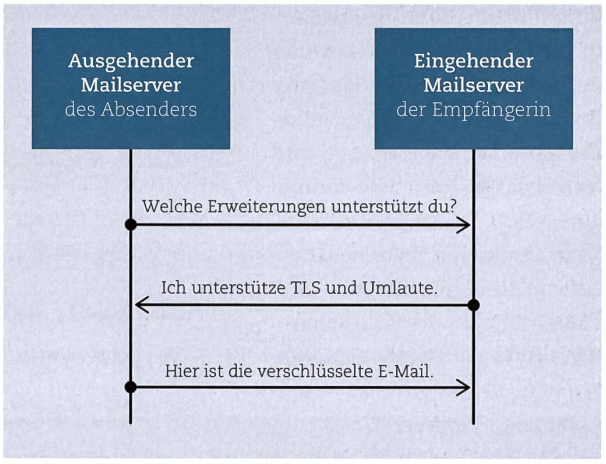
Abbildung 1



Unsichere Übermittlung

E-Mails wurden ursprünglich ungesichert über das öffentliche Internet versendet – die Betreiber der beteiligten Computernetzwerke hatten Zugriff auf den Inhalt jeder Nachricht und konnten diese beliebig verändern. 1999 wurde SMTP erweitert, so dass eine unsichere Verbindung nachträglich mit *Transport Layer Security (TLS, 1995 als SSL eingeführt)* verschlüsselt werden kann, wenn beide Server diese Erweiterung unterstützen. Die Kommunikation sieht dann wie folgt aus:

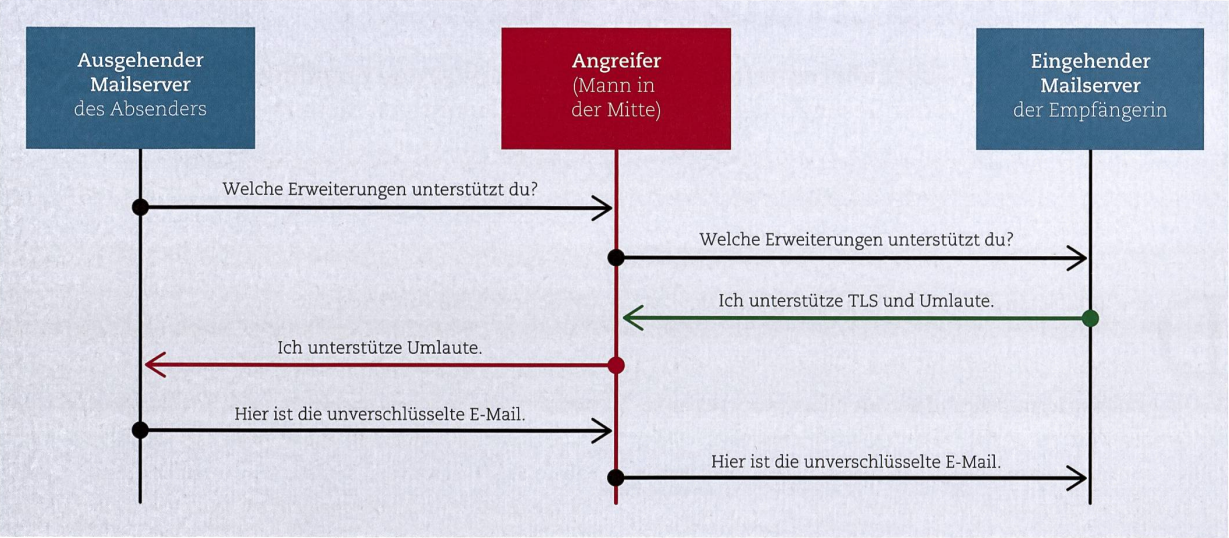
Abbildung 2



Bei der Beurteilung der Sicherheit von E-Mails interessieren uns zwei Eigenschaften. Erstens die *Vertraulichkeit:* Wie wird sichergestellt, dass Mitteilungen nicht von unbeteiligten Personen eingesehen werden können? Zweitens die *Echtheit:* Wie kann garantiert werden, dass eine Mitteilung vom angegebenen Absender stammt und nicht verändert wurde? Damit E-Mails als «sicher» bezeichnet werden können, sind diese beiden Aspekte bei Einreichung, Übermittlung und Abruf wichtig. Da die Übermittlung der Mitteilung zwischen den beiden Mailservern das schwächste Glied ist, fokussiere ich mich in diesem Artikel auf diese Verbindung.

Auch nach Einführung der TLS-Erweiterung wurden die meisten E-Mails für lange Zeit noch unverschlüsselt übermittelt, weil viele Administratoren von Mailservern nicht die notwendigen Anpassungen vornahmen. Ein Umdenken fand erst vor wenigen Jahren statt, was sich an einer von Google veröffentlichten Statistik von seinem Maildienst Gmail deutlich erkennen lässt: Während im Jahr 2013 lediglich etwa 30 Prozent seiner E-Mails an andere Anbieter verschlüsselt übermittelt wurden, sind es heute etwa 90 Prozent. Der starke Anstieg liegt vermutlich an den Enthüllungen von Edward Snowden über die Überwachungstätigkeiten der amerikanischen Geheimdienste.

Abbildung 3



Heisst das also, dass Ihre E-Mails dank der Verschlüsselung der Verbindung nun «sicher» sind? Ganz so einfach ist es leider nicht: Da E-Mail immer rückwärtskompatibel erweitert wurde, sind alle Erweiterungen freiwillig. Unterstützt der Mailserver der Empfängerin TLS nicht, übermittelt der Server des Absenders die E-Mail einfach über eine unsichere Verbindung. Ein Angreifer kann die Kommunikation zwischen den beiden Servern abfangen und TLS einfach aus der Liste der unterstützten Erweiterungen löschen. Der Angriff ist in der Abbildung 3 dargestellt.

Sie merken: Obwohl dank TLS E-Mails verschlüsselt übermittelt werden können, ist es für einen genügend mächtigen Angreifer ein leichtes Spiel, Zugriff auf Ihre Mailgeheimnisse zu erhalten. Immerhin: Im Gegensatz zur Überwachung einer unverschlüsselten Verbindung hinterlässt ein solcher Angriff allerdings Spuren in der Logdatei des Absenders.

Es gäbe durchaus neuere Erweiterungen, welche die Übermittlung von E-Mails auch in der Gegenwart eines aktiven Angreifers vertraulich machen: *DNS-Based Authentication of Named Entities (DANE, 2015)* und *Mail Transfer Agent Strict Transport Security (MTA-STS, 2018)*. Mit der Ausnahme von professionellen Mailanbietern haben diese Standards jedoch noch kaum Verbreitung gefunden – Ihr Arbeitgeber verwendet diese Erweiterungen mit grosser Wahrscheinlichkeit nicht.

«In der Zwischenzeit haben wir Standards zur Verhinderung von missbräuchlichen Absenderadressen, doch leider hapert es auch hier an der Umsetzung.»

Kaspar Etter

Mangelhafte Überprüfung

Ein weiteres Sicherheitsdefizit besteht bei der Überprüfung der Absenderadresse. Dieses lässt sich ebenfalls auf historische Umstände zurückführen: In der Urform von E-Mail konnte man als Absender wie bei der Briefpost eine beliebige Adresse angeben, ohne dass die Empfängerin diese verifizieren konnte. In der Zwischenzeit haben wir Standards zur Verhinderung von missbräuchlichen Absenderadressen, doch leider hapert es auch hier an der Umsetzung: Zu viele Firmen und Organisationen nehmen nicht die notwendigen Einträge im *Domain Name System (DNS, 1983)* vor, um ihre Domain vor Missbrauch zu schützen. Zudem weisen viele Mailserver unechte E-Mails noch nicht strikt genug zurück. Leider zeigen die meisten E-Mail-Programme auch nicht an, ob die Echtheit der Absenderadresse überprüft werden konnte.

Ist es denn so schwierig, einen Absender auf seine Echtheit zu überprüfen? Eigentlich nicht – damit der Mailserver der Empfängerin erkennen kann, ob eine E-Mail tatsächlich vom angegebenen Absender stammt, benötigt der Domainname (der Teil nach dem @-Symbol in der Mailadresse) des Absenders lediglich Einträge im Domain Name System für die folgenden drei Erweiterungen: *Sender Policy Framework (SPF, 2006)*, *DomainKeys Identified Mail (DKIM, 2007)* und *Domain-Based Message Authentication, Reporting, and Conformance (DMARC, 2015)*. Die Verwendung von SPF und DMARC bringt keinerlei Nachteile. DKIM hingegen verwendet kryptografische Signaturen, wodurch man als Benutzerin den Inhalt einer Nachricht nicht mehr abstreiten kann. Dies wurde den amerikanischen Demokraten um Hillary Clinton zum Verhängnis, da WikiLeaks so die Echtheit der veröffentlichten E-Mails beweisen konnte.

Mögliche Alternativen

Auch wenn Sie sich nun in Ihrer privaten Kommunikation für den Mailanbieter entscheiden, der sämtliche Erweiterungen umsetzt, bleiben Ihre E-Mails für die Betreiber der Mailserver jedoch noch immer einsehbar und veränderbar. Wer seinem Mailanbieter nicht vertrauen will, kann seine Mitteilungen bereits in seinem E-Mail-Programm für die Empfängerin signieren und verschlüsseln – man spricht dann von «Ende-zu-Ende-Verschlüsselung». Die weitverbreitetsten Standards dafür sind *Pretty Good Privacy (PGP, 1996)* und *Secure/Multipurpose Internet Mail Extensions (S/MIME, 1998)*. Diese beiden Standards gewährleisten unabhängig von den involvierten Anbietern einen sicheren Mailverkehr, doch setzen sie ein gewisses Mass an technologischem Fachwissen voraus und funktionieren ebenfalls nur, wenn beide Parteien sie verwenden. Da sich zu wenige Nutzer um ihre Privatsphäre im Mailverkehr kümmern, wird die Verbreitung dieser Standards wohl kaum zunehmen. Umso wichtiger ist es, dass Anbieter zumindest die Verbindungen zwischen ihren Mailservern sichern.

Alles in allem ist es um die Sicherheit von E-Mail leider recht schlecht bestellt: Als Absender kann man sich nicht darauf verlassen, dass die Mitteilung während der Übermittlung verschlüsselt ist, und für die Empfängerin ist nicht immer garantiert, dass eine Mitteilung vom angegebenen Absender kommt. Auch bezüglich Privatsphäre schneidet E-Mail sowohl für den Absender als auch für die Empfängerin schlecht ab. Deshalb empfehle ich Ihnen für Mitteilungen, bei denen Sicherheit oder Privatsphäre wichtig sind, auf proprietäre Mitteilungsdienste wie Signal oder Threema auszuweichen. Da E-Mail einer der wenigen dezentralen Dienste ist, die wir noch haben, täten wir gut daran, diesem mehr Sorge zu tragen. Üben Sie daher ruhig Druck auf den IT-Administrator Ihrer Firma oder den Mailanbieter Ihres Vertrauens aus, damit auch diese in Zukunft den sicheren Mailverkehr zum Standard machen. ‹

Der Autor hat der E-Mail-Technologie einen ausführlichen Beitrag auf seinem Blog gewidmet: ef1p.com/email. Dort können Sie auch mit interaktiven Tools überprüfen, ob die erwähnten Standards auf Ihrer Domain richtig konfiguriert wurden.

Kaspar Etter
studierte Informatik an der ETH Zürich und arbeitet als freischaffender Autor.

Illustration von Stephan Schmitz.