Bundesverband IT-Sicherheit e.V.

TeleTrusT
Pioneers in IT security.

E-Mail-Verschlüsselung

Rechtssichere und vertrauliche E-Mail-Kommunikation

2020

Danksagung

Diese Publikation wurde in der TeleTrusT-AG "Cloud Security"/AK "Mail Security" erarbeitet. TeleTrusT bedankt sich bei den nachstehenden Personen für ihre Mitwirkung im TeleTrusT-Arbeitskreis "Mail Security" sowie für die aktive Mitgestaltung dieser Handreichung.

Autoren
Oliver Dehning, Hornetsecurity
Leiter der TeleTrusT-AG "Cloud Security"

Peter Hansemann, ICN
Leiter des TeleTrusT-AK "Mail Security"

Redaktion

Abou Nasser, Morad - Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Adolf, Alexander - Condition ALPHA
Bartels, Karsten U. - HK2 Rechtsanwälte
Bernard, Yvonne - Hornetsecurity
Cink, Stephan - Net at Work
Heutger, Christian - PSW Group
Köhler, Tim - Zertificon
Mühlbauer, Holger - Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Mühlbauer, Roland - SEPPmail Deutschland
Wichmann, Markus - Siemens
Wiegel, Burkhard - Zertificon

Impressum

Herausgeber:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Chausseestraße 17
10115 Berlin
Tel.: +49 30 4005 4306
Fax: +49 30 4005 4311
E-Mail: info@teletrust.de
https://www.teletrust.de

Inhalt

1 Einleitung

Sie versenden gerne Postkarten? - Postkarten? Haben Sie schon seit Jahren nicht mehr geschrieben, sagen Sie. Und wenn, dann nur im Urlaub …

Die Realität sieht anders aus

Die Kommunikation über E-Mail mit Kunden und Geschäftspartnern ist mittlerweile zur Lebensader des Tagesgeschäftes vieler Unternehmen und Organisationen geworden. Die meisten Nutzer wissen allerdings nicht, dass die Versendung einer E-Mail dem Transport einer Postkarte durch Unbekannte entspricht.

Ungeachtet dessen werden täglich viele geschäftliche Informationen - darunter auch unternehmenskritische Vorgänge und sensible Daten - über das "Postkartensystem" versendet. Diese übermittelten Informationen sind nicht nur für Fremde lesbar, sondern können auch auf dem Transportweg manipuliert oder gar gelöscht werden.

Hinzu kommt ein weiterer Aspekt, der gerade beim Austausch von rechtsrelevanten Dokumenten wie z.B. Rechnungen oder Lastschriftmandaten wichtig ist: Wie kann ich sicher sein, mit wem ich kommuniziere?

Die nachfolgenden Ausführungen sollen Ihnen helfen, fünf wichtige Fragen hinsichtlich Ihrer E-Mail-Kommunikation zu beantworten:

1. Benötigen Sie eine verbindliche Bestätigung über die Zustellung?
2. Möchten Sie Rechtsgeschäfte per E-Mail abwickeln?
3. Müssen Sie die Authentizität des Absenders sicherstellen?
4. Muss der Inhalt vor einer Manipulation gesichert werden?
5. Welcher Schaden kann entstehen, wenn die Informationen und Daten in die Hände Dritter gelangen?

2 Motivation für Verschlüsselung

2.1 Postkarten mit Geheimschrift

Die Verschlüsselung von E-Mails stellt einen wesentlichen Schritt zu einer vertrauenswürdigen E-Mail-Kommunikation dar. Somit wird aus der gewöhnlichen Postkarte eine "Postkarte mit Geheimschrift", die nur der berechtigte Empfänger lesen kann.

Zwei Triebkräfte bringen Entscheider dazu, sich mit dem Thema Verschlüsselung zu beschäftigen. Zum einen gibt es das ureigene Interesse eines Unternehmens oder einer Organisation, bestimmte Daten wirklich geheim zu halten. Kunden- und Finanzdaten, Konzepte und neue Entwicklungen sollen zum Schutz vor Industriespionage und Manipulation verschlüsselt werden. Zum anderen gilt es, die Compliance zu erfüllen. Der Gesetzgeber macht nicht zuletzt seit Geltung der Datenschutz-Grundverordnung (DSGVO) Vorgaben zum Umgang mit personenbezogenen Daten und nimmt die Verantwortlichen in die Haftung (Art. 83 DSGVO). Aber auch Geschäftsführer und Vorstände müssen mit einer persönlichen Haftung rechnen (z. B. gem. § 42 Abs. 1 GmbHG, § 91 Abs. 2 AktG).

Hinzu kommt eine Vielzahl nationaler und internationaler, teils branchenspezifischer Vorgaben, die unter anderem die Kreditwürdigkeit mit dem Stand der eingesetzten IT-Sicherheit verknüpfen.

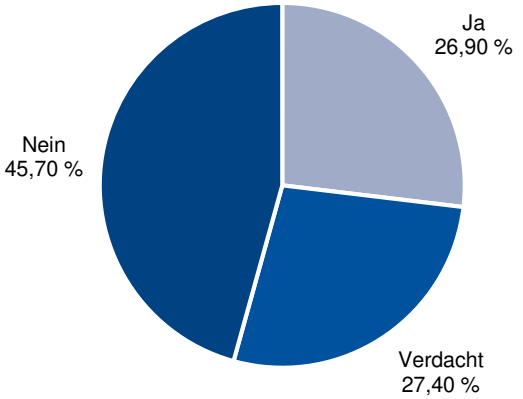
2.2 Bedrohungslage

Die Studie "Industriespionage 2014 - Cybergeddon der Wirtschaft durch NSA & Co.?" von Corporate Trust wurde in Zusammenarbeit mit AON Risk Solutions, der Securiton GmbH und der Zurich Gruppe Deutschland erstellt. Erstmalig wurden sowohl in Deutschland als auch in Österreich das Risiko und die aktuellen Vorfälle erfasst. Für die Erstellung der Studie wurde nach dem Zufallsprinzip ein repräsentativer Querschnitt von Firmen aller Branchen ausgewählt und dann 6.767 Unternehmen in Deutschland sowie 1.396 Unternehmen in Österreich befragt.

Jedes zweite Unternehmen hatte in den vergangenen beiden Jahren einen Spionageangriff oder Verdachtsfall zu beklagen. Konkret waren 26,90 % in Deutschland und 27,10 % in Österreich von einem Vorfall betroffen. Weitere 27,40 % (Deutschland) bzw. 19,50 % (Österreich) hatten zumindest einen

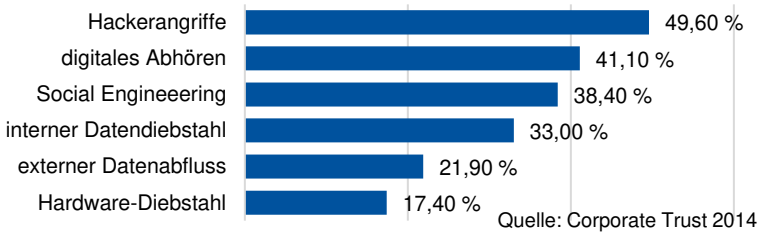
Verdachtsfall. In Deutschland stellt dies einen Anstieg um 5,50 % im Vergleich zu den Ergebnissen aus der Studie 2012 dar. Für Österreich wurden die Zahlen erstmalig erhoben.

Gab es in Ihrem Unternehmen konkrete Spionagefälle?



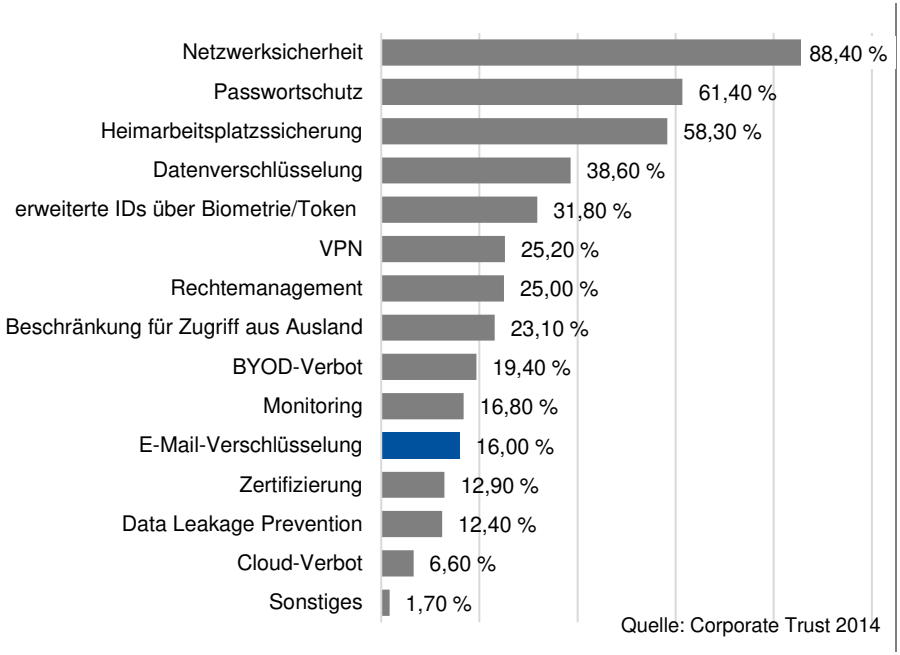
Quelle: Corporate Trust 2014

Am häufigsten wurden von den Unternehmen Hackerangriffe auf EDV-Systeme und Geräte (Deutschland: 49,60 %; Österreich: 41,80 %) festgestellt. Die zweithäufigste Angriffsform war ebenfalls technischer Natur: **Das Abhören bzw. Abfangen von elektronischer Kommunikation wurde in Deutschland in 41,10 % und in Österreich in 40,00 % der Fälle festgestellt.** In Deutschland war Social Engineering mit 38,4 % die dritthäufigste Angriffsform, in Österreich die bewusste Informations- oder Datenweitergabe bzw. der Datendiebstahl durch eigene Mitarbeiter (38,20 %).



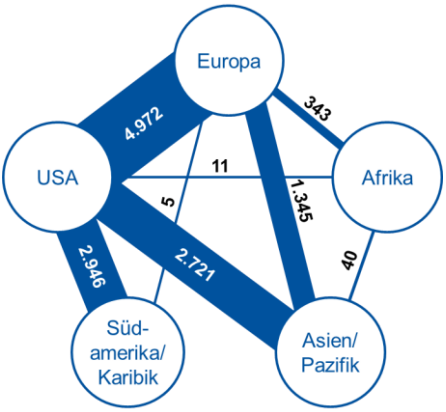
Quelle: Corporate Trust 2014

Jedoch setzen lediglich 16% der befragten Unternehmen E-Mail-Verschlüsselung als Instrument der IT-Sicherheit ein:



Aufgrund der gewaltigen internationalen Datenströme muss man davon ausgehen, dass sehr große Datenmengen zwischen Kommunikationspartnern unverschlüsselt ausgetauscht werden. Ein wesentlicher Teil davon wird über E-Mail übertragen.

Weltweite Datenströme 2011 in GB/s

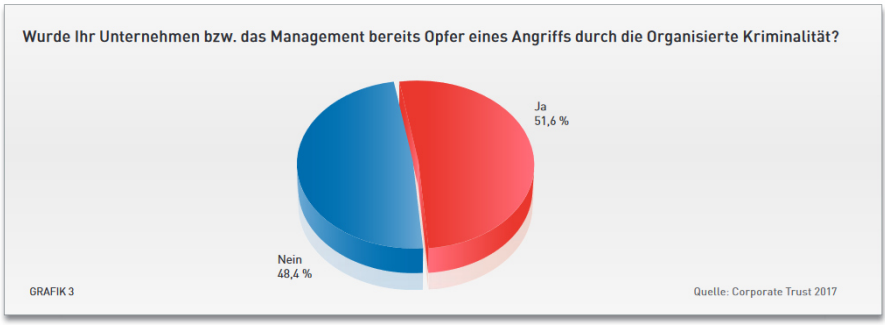


Grafik nach: BLZ/ Rita Böttcher Quelle: Telegeography Research

Im Rahmen des "FUTURE REPORT"[1] wurden von Corporate Trust im Jahr 2017 erneut 3.342 Unternehmen in Deutschland, sowie 1.396 Unternehmen in Österreich nach aufgetretenen Sicherheitsvorfällen und dabei erlittenen Schäden befragt. Darüber hinaus war Ziel der Befragung, die Einschätzung zukünftiger Risiken und präventiver Maßnahmen aus Sicht der Unternehmen zu erhalten.

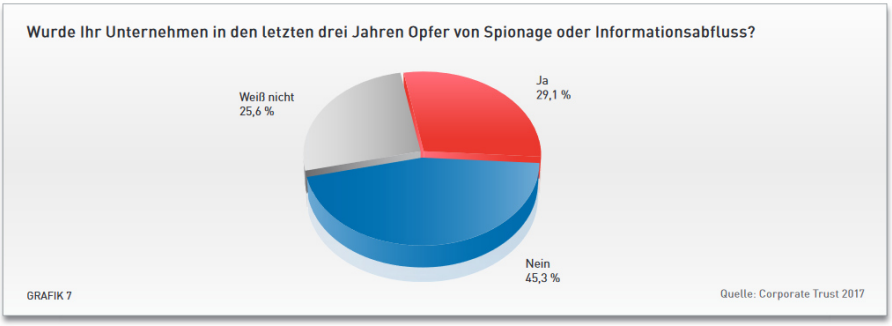
Analog zur Studie aus dem Jahr 2014 gaben auch 2017 mehr als die Hälfte der Unternehmen an, Opfer eines Angriffes geworden zu sein. In der aktuellen Studie wurde der Fokus der Angriffe auf "Organisierte Kriminalität" ausgeweitet:

[1] Corporate Trust 2017 FUTURE REPORT - https://www.corporate-trust.de/wp-content/uploads/2017/11/Future_report_2017_DT_webv2.pdf

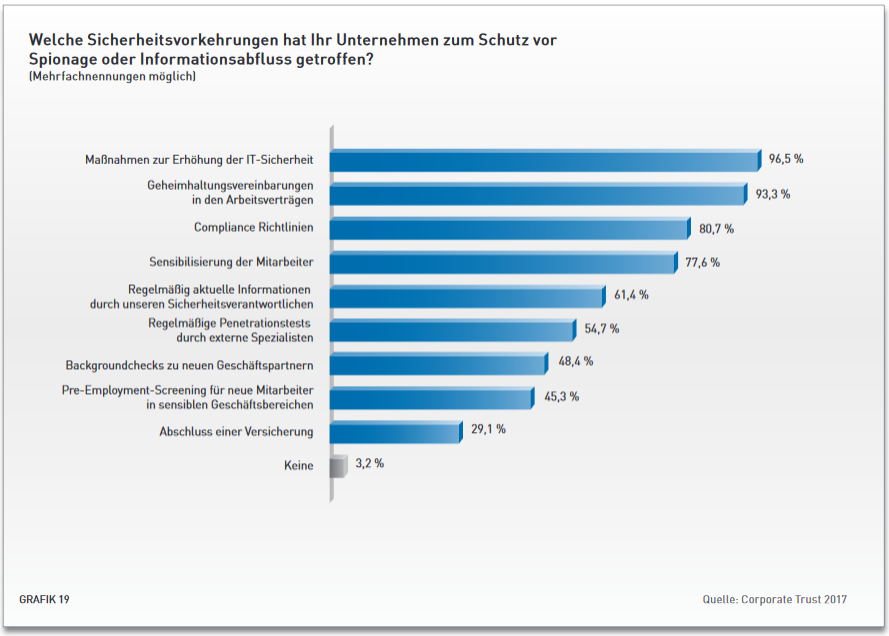


Die genannten Schwerpunkte der erlittenen Angriffe liegen aber trotzdem weiterhin überwiegend im Bereich der Informationstechnik. Eine sehr große Rolle spielen Szenarien, die durch Social Engineering vorbereitet werden, aber auf Basis technischer Systeme wie E-Mail durchgeführt werden.

Fast 30% der Unternehmen gehen davon aus, dass im Rahmen eines Angriffs Informationen abgeflossen sind:



Nahezu alle Unternehmen (96,5%) nennen bei der Frage nach Sicherheitsvorkehrungen zum Schutz vor Spionage und Informationsabfluss das Thema "Maßnahmen zur Erhöhung der IT-Sicherheit":



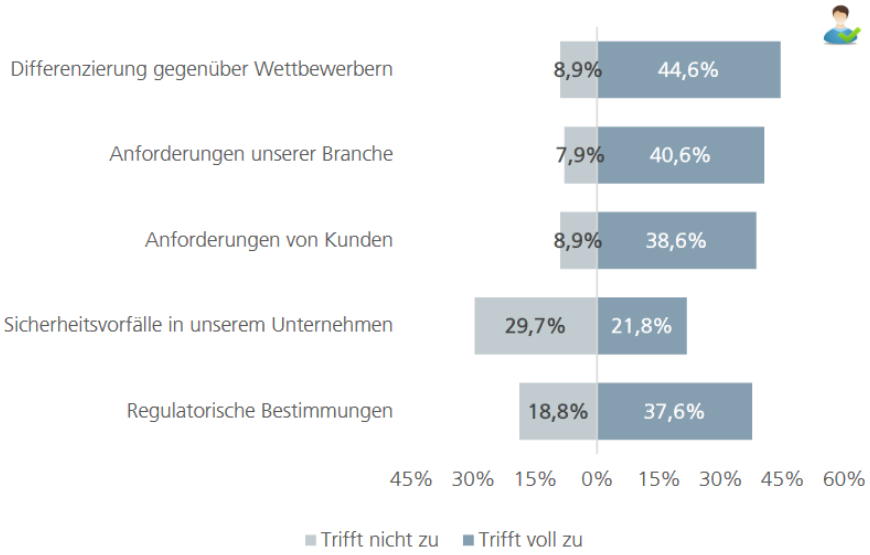
2.3 Wettbewerb als Motivation

Im Rahmen der Studie "Einsatz von elektronischer Verschlüsselung - Hemmnisse für die Wirtschaft"[2] hat das BMWi 2018 u.a. die Motivation von Unternehmen (KMU) für den Einsatz von Verschlüsselung untersucht. Für diese Studie wurden 212 Unternehmen befragt, von denen 140 weniger als 500 Mitarbeiter beschäftigen.

"Die Motivation von kleinen und mittleren Unternehmen für den Einsatz von Ver-schlüsselung ist derzeit vor allem durch das Wettbewerbsumfeld geprägt. 45 Pro-zent der KMU geben an, sich durch Kommunikationsverschlüsselung vor allem von anderen Wettbewerbern differenzieren zu wollen. Branchen- und Kundenanforderungen sind mit ca. 40 Prozent ebenfalls wichtige Faktoren für den Einsatz von Verschlüsselung. Tatsächlich eingetretene Sicherheitsvorfälle werden von 22 Prozent der KMU als Grund für den heutigen Einsatz von Verschlüsselungslösungen angegeben, ein deutlich geringerer Wert als bei den übrigen Motivationsgründen."

[2] BMWi 2018 Einsatz von elektronischer Verschlüsselung - Hemmnisse für die Wirtschaft https://www.BMWi.de/Redaktion/DE/Publikationen/Studien/einsatz-von-elektronischer-verschluesselung-hemmnisse-fuer-die-wirtschaft.pdf?__blob=publicationFile

Abb. 5 Anwender von Kommunikationsverschlüsselung in KMU: Gründe für den Einsatz



Quelle: BMWI 2018

2.4 Compliance als Motivation

Eine ausdrückliche Pflicht zur E-Mail-Verschlüsselung ist gesetzlich nicht geregelt. Allerdings ist es aufgrund aktueller gesetzlicher Anforderungen aus Sicht der Compliance erforderlich, sich mit dem Erfordernis einer entsprechenden Verschlüsselung im Einzelfall auseinanderzusetzen.

Die DSGVO normiert umfassende Anforderungen an den technischen und organisatorischen Schutz personenbezogener Daten in Art. 32 DSGVO, wonach Verantwortliche ein dem Risiko angemessenes Schutzniveau zu gewährleisten haben.

Ähnliche Vorgaben gelten für Betreiber Kritischer Infrastrukturen durch die Anpassungen aufgrund des IT-Sicherheitsgesetzes (ITSiG) sowie durch die Durchführungsverordnung zur NIS-Richtlinie EU 2018/151 für bestimmte Anbieter digitaler Dienste, zu denen Online-Marktplätze und -Suchmaschinen sowie Cloud-Computing-Dienste gehören können.

Auch die Umsetzung der Richtlinie (EU) 2016/943 zum Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, das geplante Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG), könnte im Einzelfall eine Verschlüsselung von E-Mails erfordern.

2.5 Anwendersicht

Eine Erklärung für die geringe Nutzung vorhandener Technologien und Werkzeuge aus dem Bereich der E-Mail- und Datenverschlüsselung lässt sich aus den weitverbreiteten Anwendersichten auf das Thema IT-Sicherheit ableiten. Insbesondere in kleinen und mittleren Unternehmen (KMU) begegnen sowohl Entscheider als auch Nutzer den Gefahren und Risiken der Nutzung von vernetzten IT-Systemen oft mit zu wenig Sensibilität und Aufmerksamkeit. Der Schutzbedarf der eigenen IT-Systeme und der verarbeiteten und gespeicherten Daten wird erfahrungsgemäß falsch eingeschätzt.

Berater oder Verantwortliche für IT-Sicherheit werden in Gesprächen mit Anwendern und Entscheidern häufig mit solchen "Kernthesen" konfrontiert:

- "Meine Daten interessieren niemanden."
- "Die NSA kann trotzdem mitlesen."
- "Verschlüsselung ist kompliziert und unpraktisch."

In Unternehmen und Organisationen, die IT-Systeme nutzen, muss durch Aufklärung die Sensibilität für die vorhandenen Gefahren erhöht werden. Entscheider und Anwender müssen in die Lage versetzt werden, den Schutzbedarf der Anwendungen und Daten des eigenen Unternehmens oder der eigenen Organisation richtig einschätzen zu können.

In diesem Kontext muss vermittelt werden, dass es nicht das Ziel der IT-Sicherheitsstrategie sein kann, sich gegen die Möglichkeiten eines staatlichen Dienstes zu rüsten. Vielmehr muss die Schwelle für den Missbrauch von Daten und Systemen von innen wie von außen durch technische und organisatorische Maßnahmen möglichst hoch gesetzt werden. Der Einsatz vorhandener, bezahlbarer und praktikabler Lösungen für Datenverschlüsselung, insbesondere E-Mail-Verschlüsselung, unterstützen Unternehmen und Organisationen dabei, die Angriffsschwelle zu erhöhen.

2.6 Rechtliche Aspekte

Ob und inwieweit der Einsatz von Verschlüsselungsverfahren beim E-Mailing für den Versender oder Empfänger verpflichtend ist, ist gesetzlich nicht klar geregelt. Deshalb bleibt der Einsatz von Verschlüsselung i.d.R. Ergebnis einer individuellen Risikobeurteilung. Daraus kann jedoch nicht der Schluss gezogen werden, dass keine Pflichten beim Austausch von Informationen über das Kommunikationsmittel E-Mail bestehen. Im Rahmen der Vertragsgestaltungsfreiheit können Vertragsparteien jedoch Klarheit schaffen.

2.6.1 Vertragliche Pflichten

Vertragsklauseln zur E-Mail-Verschlüsselung sollten insbesondere im Blick haben, welche Mitarbeiter oder Unternehmensbereiche verpflichtet werden sollen. Andere Bezugspunkte können Kategorien von Inhalten resp. Informationen, einzelne Projekte, Geschäftsbereiche oder auch bestimmte Kommunikationspartner betreffen. Dazu ist es sachdienlich, die Eckpunkte zur technischen Umsetzung klarzustellen bzw. Alternativen vorzusehen. Je nach Fall kann es opportun sein, ein Sanktionsregime für Pflichtverstöße aufzusetzen.

Wird eine E-Mail-Verschlüsselung vertraglich vereinbart, ist es grundsätzlich geboten, weitere Maßnahmen der IT-Sicherheit zu regeln. Ansonsten droht die Verschlüsselung ins Leere zu laufen. Bisher vereinbaren Vertragsparteien eher selten Regelungen, die unmittelbar Pflichten zur Verschlüsselung der E-Mail-Kommunikation begründen. Dies sollte und wird sich ändern.

Die Nutzung unverschlüsselter E-Mails kann auch ein Pflichtverstoß gegen eine Geheimhaltungsvereinbarung (NDA) darstellen. Wer sich dazu verpflichtet, Informationen vertraulich zu behandeln und alle zumutbaren Maßnahmen zu treffen, um die Vertraulichkeit einer Information zu schützen, wird E-Mails nicht ohne weiteres unverschlüsselt versenden dürfen.

2.6.2 Gesetzliche Pflichten

Ein umfassendes Gesetz zur IT-Sicherheit gibt es bislang nicht. Eine allgemeine Verschlüsselungspflicht gibt es ebenfalls nicht. Vielmehr können sich aus unterschiedlichen Normen Maßstäbe an die E-Mail-Verschlüsselung ableiten lassen, die teilweise nur auf bestimmte Personengruppen (z.B. Ärzte und Rechtsanwälte, § 203 StGB), Branchen oder Bereiche bzw. auf bestimmte Inhalte Anwendung finden (z.B. nur personenbezogene Daten, § 9

BDSG). Daneben gibt es zwar anerkannte Regelungen, wie z.B. BSI-Grundschutz, technische Richtlinien oder Branchenstandards. Diese entfalten jedoch nur bedingt eine Bindungswirkung, da es ihnen an der Allgemeinverbindlichkeit eines Gesetzes fehlt. Dennoch können derartige Standards von einem Gericht herangezogen werden, um den Sorgfaltsmaßstab im Einzelfall zu bestimmen. Es ist daher, insbesondere in Ermangelung einer gesetzlichen Regelung, empfehlenswert, sich mit diesen Standards auseinanderzusetzen.

Bei der Verarbeitung personenbezogener Daten bildet § 9 BDSG einen Anknüpfungspunkt für die Bestimmung von IT-Sicherheitsstandards. Die für die Datenverarbeitung verantwortliche Stelle hat alle technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Regelungen des BDSG einzuhalten (z.B. Weitergabekontrolle). Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Ob daher Maßnahmen zur E-Mail-Verschlüsselung getroffen werden müssen, richtet sich nach dem Ergebnis einer Risiko- bzw. Schutzbedarfsanalyse. Eine solche Risiko- und Schutzbedarfsanalyse stellt einen umfassenden Abwägungsprozess dar, dessen Bezugspunkte unten beschrieben werden. Im Ergebnis sollte eine nachvollziehbare und dokumentierte Abwägung hinsichtlich der bestehenden Prozesse entstehen, um Sorgfaltspflichten bestimmen zu können. Das Dokument kann auch in einem IT-Sicherheitskonzept verwertet oder einem Dritten gegenüber verwendet werden.

Als Parameter für eine Schutzbedarfsanalyse können herangezogen werden:

- Art der Daten/Informationen
- Zweck der Datenverarbeitung
- Schadensrisiko
- Objektive Risikolage (allgemein und branchenspezifisch)
- Subjektive Risikolage
    - Bereichsspezifische Vorgaben (z.B. Sozial- und Berufsrecht)
    - zurückliegende Vorfälle
    - vertragliche Pflichten
- Unternehmensgröße/wirtschaftliche Leistungsfähigkeit
- Überlegenes Wissen

Das Ergebnis der Schutzbedarfsanalyse sowie die technische und organisatorische Umsetzung sollten regelmäßig überprüft werden.

Wenn und soweit eine Verschlüsselung für nicht erforderlich gehalten wird oder vom Kommunikationspartner nicht ohne Weiteres umgesetzt werden kann, bietet es sich in schadensgeneigten Situationen an, den Kommunikationspartner ausdrücklich auf vorhandene Verschlüsselungsverfahren oder alternative Übertragungswege hinzuweisen und deren Umsetzung anzubieten. Macht dieser davon keinen Gebrauch, dürften sich Ansprüche des Kommunikationspartners verbieten, wenn er auf eine unsichere Datenübermittlung bestanden bzw. diese bewusst praktiziert hat.

An der unklaren Gesetzeslage wird nach derzeitigem Diskussionsstand das IT-Sicherheitsgesetz[3], die geplante NIS-Richtlinie[4] oder die geplante EU-Datenschutzgrundverordnung[5] nichts wesentlich ändern. Ob im Rahmen einer künftigen Rechtsverordnung (§ 10 BSIG-E) des IT-Sicherheitsgesetz-Entwurfs Verschlüsselungspflichten statuiert werden, bleibt abzuwarten.

2.6.3 Haftung

Verstöße gegen eine Verschlüsselungspflicht können Unterlassungs- und Schadenersatzansprüche gegen das versendende Unternehmen begründen. Dies ist auch für den Fall möglich, indem die Pflicht zur E-Mail-Verschlüsselung vertraglich nicht ausdrücklich bestimmt wird, es aber eine entsprechende nebenvertragliche Pflicht gibt.

Daneben sind Regressansprüche des ersatzpflichtigen Unternehmens gegen die Unternehmensleitung denkbar. Denn die E-Mail-Verschlüsselung gehört als Maßnahme der IT-Sicherheit zum Risikomanagement, für deren Durchführung Geschäftsführer und Vorstände persönlich haften (§ 43 GmbHG, §§ 91, 93, 116 AktG).

2.7 Fazit

Die Ergebnisse der Studien von Corporate Trust legen nahe, dass auf die Mehrheit der Unternehmen (> 50%) bereits IT-basierte Angriffe durchgeführt wurden, die zu Schäden und zum Abfluss von Informationen geführt haben.

---

[3] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)
[4] Vorschlag für eine Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union, 2013/0027, COM(2013) 48 final
[5] Vorschlag für Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung, COM(2012) 011 final

Insbesondere die Untersuchung von Corporate Trust aus dem Jahr 2014 zeigt, dass mehr als die Hälfte (54,30 %) der befragten Unternehmen in Deutschland einen Spionagevorfall oder einen Verdacht auf einen erfolgten Angriff hatten. Nahezu jedes zweite betroffene Unternehmen (41,10 %) nennt das "Abhören/Abfangen von elektronischer Kommunikation, z.B. E-Mails, Fax, etc." als bewiesene oder vermutete Handlung des Angreifers. Nur 16 % der Unternehmen nutzen E-Mail-Verschlüsselung als Instrument der IT-Sicherheit.

Von den Unternehmen wird klar erkannt, dass diese Themen große Gefahren in der Zukunft darstellen und dass entsprechende Schutzmaßnahmen notwendig sind.

Die Verschlüsselung der Unternehmenskommunikation, insbesondere per E-Mail, erhöht die Schwelle für potentielle Angreifer und setzt offensichtlich an einem bekannten Schwachpunkt an.

Die notwendigen Technologien und Werkzeuge sind vorhanden, werden aber in der Praxis zu wenig oder nicht konsequent eingesetzt.

Die Studie des BMWi bestätigt einerseits die Motivation der Unternehmen Verschlüsselung einzusetzen, zeigt aber auch unterschiedliche Hemmnisse für die praktische Umsetzung auf.

Die gesetzlichen Rahmenbedingungen bieten große Interpretationsspielräume hinsichtlich der Verpflichtung, Schutztechnologien wie Verschlüsselung der Kommunikation oder von Daten einzusetzen.

3 Vorhandene Technologien

3.1 Verschlüsselungs- und Signaturverfahren

Die moderne Kryptologie entstand Mitte des letzten Jahrhunderts und basiert durchweg auf Mathematik. Sie löste das alte Sicherheitsprinzip "Security through Obscurity" (Sicherheit durch Unklarheit) ab, bei der die Sicherheit durch die Geheimhaltung der Funktionsweisen gewährleistet war - ein risikoreicher und durchweg proprietärer Ansatz mit hohen Abhängigkeiten.

Marktübliche Verschlüsselungsprodukte setzen auf bekannte Algorithmen. Um den Klartext in einen Geheimtext umzuwandeln, wird als Parameter ein Schlüssel benötigt und dieser ist das Geheimnis. Algorithmen wie AES (Advanced Encryption Standard) gelten als sehr sicher. Der Aufwand einer "Brute Force Attack", bei der alle möglichen Kombinationen durchgerechnet und ausprobiert werden, steigt mit der Schlüssellänge exponentiell.

3.2 Symmetrie der Schlüssel

Grundsätzlich wird zwischen symmetrischer und asymmetrischer Verschlüsselung unterschieden. Bei der symmetrischen Verschlüsselung, zum Beispiel nach dem AES-Standard, wird derselbe Schlüssel zum Ver- und Entschlüsseln der Daten genutzt. Die Sicherheit ist an die Geheimhaltung des Schlüssels gebunden. In der direkten Nutzung zur Kommunikation gibt es das Problem, dass mindestens zwei Parteien diesen Schlüssel zuerst initial miteinander teilen und ihn anschließend sicher verwahren müssen.

Bei einer symmetrischen Verschlüsselung wird Klartext mittels einer Krypto-Funktion (Algorithmus) und dem geheimen Schlüssel in einen Geheimtext gewandelt. Der Empfänger kann mittels desselben geheimen Schlüssels die Nachricht wieder entschlüsseln. Dieses Verfahren ist schnell, aber man hat das Problem, dass man das Geheimnis, den geheimen Schlüssel, allen Kommunikationspartnern auf einem anderen sicheren Kanal mitteilen muss. Zum Beispiel müssen bei passwortbasierten PDF- oder ZIP-Container-Verschlüsselungen die Passwörter an den Kommunikationspartner weitergegeben werden - und das möglichst auf einem anderen Kommunikationskanal.

Schematische Darstellung der symmetrischen Verschlüsselung

Bei der asymmetrischen Verschlüsselung werden zwei Schlüssel als Parameter genutzt: Ein öffentlicher Schlüssel (public key) wird für die Verschlüsselung genutzt. Ein privater, geheimer Schlüssel (private key) ermöglicht die Entschlüsselung der Daten. Beide Schlüssel stehen in einer bestimmten mathematischen Abhängigkeit. Der private Schlüssel lässt sich aber durch die Kenntnis des öffentlichen Schlüssels nicht errechnen. RSA, benannt nach Ron Rivest, Adi Shamir und Leonard Adleman, ist ein weit verbreiteter Standard in der asymmetrischen Verschlüsselung.

Eine sichere Mitteilung eines geheimen symmetrischen Schlüssels ist somit nicht mehr nötig. Meist wird der öffentliche Schlüssel in einem Zertifikat integriert, in dem unter anderem Identitäts-Informationen zum Inhaber (z.B. Name und E-Mail-Adresse) gespeichert sind und die Kombination aus öffentlichem Schlüssel und Identität durch einen Dritten beglaubigt wird.

Schematische Darstellung der asymmetrischen Verschlüsselung

3.3 Private und öffentliche Schlüssel mit Identitäten

Das initiale Problem der Schlüsselverteilung und Geheimhaltung ist mit der Aufteilung in öffentliche und private Schlüssel gelöst.

Asymmetrische Schlüsselpaare werden Identitäten zugeordnet. Hierin begründet sich das Modell der Public-Key-Infrastruktur (PKI), die Basis der Public-Key-Kryptografie, welche letztlich die sichere Kommunikation innerhalb unsicherer Netzwerke erlaubt. Die öffentlichen Schlüssel werden als

Zertifikate auf bestimmte Identitäten ausgestellt und breit gestreut. Mit der Echtheits- und Gültigkeitsprüfung von Zertifikaten können Identitäten zu diesem Zeitpunkt zweifelsfrei festgestellt werden.

PKIen werden im Bereich der E-Mail-Verschlüsselung genutzt, indem Nachrichten mit den Zertifikaten der jeweiligen Empfänger verschlüsselt werden. Nur der Inhaber des privaten Schlüssels zum jeweiligen Zertifikat kann die Nachrichten entschlüsseln.

3.4 S/MIME und OpenPGP - Zertifikat oder Schlüssel?

Zur PKI-basierten E-Mail-Verschlüsselung haben sich zwei Standards etabliert: S/MIME (Secure/Multipurpose Internet Mail Extensions) und OpenPGP (Pretty Good Privacy). Beide nutzen im Grunde die gleichen kryptografischen Verfahren. Sie unterscheiden sich jedoch in der Zertifizierung der öffentlichen Schlüssel und damit in den Vertrauensmodellen.

Beide Standards sind nicht zueinander kompatibel - das bedeutet, Anwender des einen Verfahrens können keine signierten oder verschlüsselten Nachrichten mit Anwendern des anderen Verfahrens austauschen.

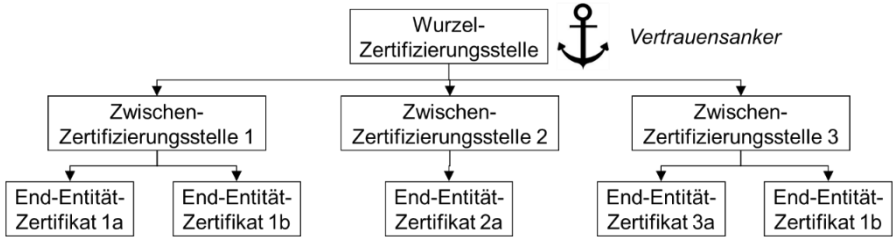
3.4.1 S/MIME und X.509

S/MIME bezeichnet einen Standard, bei dem sogenannte X.509[6]-Zertifikate genutzt werden. Die Zertifizierung der öffentlichen Schlüssel wird als Dienstleistung durch öffentliche Trustcenter als Certification Authority (CAs) angeboten. Je nach Prüfungsverfahren und der damit verbundenen Vertrauensstufe sind die Zertifikate kostenpflichtig.

Das Vertrauensmodell ist hierarchisch. Die Identitäten werden über eine Zertifikatskette vom Nutzerzertifikat über eventuelle zweckgebundene Zwischen-CAs bis hin zum Wurzel-CA-Zertifikat der ausgebenden Stelle verifiziert.

[6] D.h., die Informationen im Zertifikat sind einheitlich nach X.509-Standard aufgelistet.

Hierarchisches Vertrauensmodell



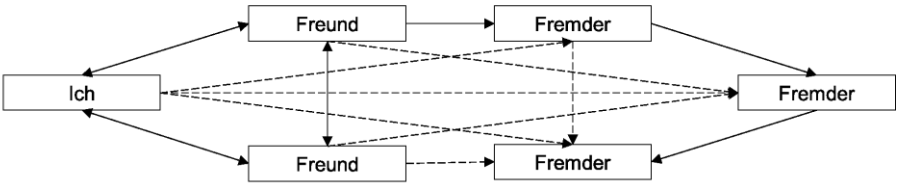
Schematische Darstellung des hierarchischen PKI-Vertrauensmodells

S/MIME ist als Kommunikationsstandard in den gängigen E-Mail-Programmen bereits implementiert und die CA- und Sub-CA-Zertifikate der bekannten Trustcenter sind zur Prüfung der Nutzerzertifikate ebenfalls vorinstalliert.

3.4.2 OpenPGP

OpenPGP sieht vor, dass sich die Teilnehmer untereinander ihre öffentlichen Schlüssel signieren und damit zertifizieren. Dadurch entsteht ein "Web of Trust (WOT)", ein Netzwerk des Vertrauens, das ohne Hierarchien auskommt. Schlüsselpaare werden selbst erstellt und öffentliche PGP-Schlüssel von Teilnehmern beispielsweise auf Key Signing Partys gegenseitig zertifiziert. PGP-Nutzer können die öffentlichen Schlüssel anderer Nutzer mit ihren eigenen privaten Schlüsseln signieren, um deren Echtheit zu dokumentieren. Im Unterschied zu Zertifikaten, die nur von einer CA unterzeichnet werden, kann ein PGP-Key beliebig viele digitale Unterschriften enthalten.

Web of Trust



Schematische Darstellung des WOT-Vertrauensmodells

OpenPGP ist in den gängigen E-Mail-Programmen nicht vorinstalliert, sodass der Nutzung immer eine Client-Installation wie beispielsweise Enigmail für Thunderbird vorausgehen muss.

3.4.3 Nutzung und Sicherheit

Die Nutzung von OpenPGP und S/MIME in Webmailern ist noch nicht befriedigend gelöst.

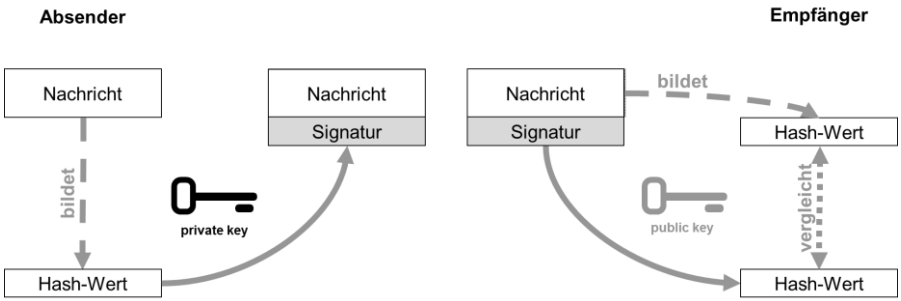
Unter Sicherheitsaspekten bieten beide Verfahren Vor- und Nachteile. Für den geschäftlichen Austausch von Nachrichten hat sich S/MIME durchgesetzt, da hier eine zentrale Instanz organisatorische Aufgaben übernimmt und je nach Prüfungsverfahren die Vertrauenswürdigkeit der Zertifikate hoch eingestuft werden kann. Andererseits müssen Wurzelzertifizierungsstellen besonders geschützt werden, da sie einen zentralen Punkt für Angreifer darstellen.

Im PGP-Verfahren ist durch das Web of Trust kein solcher zentraler Angriffspunkt vorhanden. Jedoch muss der Benutzer zur Erreichung einer hohen Vertrauenswürdigkeit (über die Verschlüsselungsmöglichkeit hinaus) selbst besondere Maßnahmen ergreifen. Auch bei der Generierung des Schlüssels sind Besonderheiten zu berücksichtigen, damit keine Kompromittierung durch Angreifer durchgeführt werden kann.

3.5 Signieren von E-Mails

Durch die Nutzung des PKI-Modells lassen sich auch digitale Signaturen erstellen, welche im Bereich der E-Mail-Sicherheit Anwendung finden. Diese dienen als eine Art Fingerabdruck, um die Echtheit einer E-Mail-Adresse bzw. der versendenden Identität entsprechend zu bestätigen.

Beim Signieren von E-Mails bildet der Sender über seine Nachricht eine Prüfsumme (Hash) und verschlüsselt diese mit seinem privaten Schlüssel. Das Ergebnis verschickt er als Signatur zusammen mit der Nachricht. Die Echtheit einer Nachricht kann der Empfänger verifizieren, indem er die Prüfsumme in der Signatur mit dem öffentlichen Schlüssel des Absenders dechiffriert, den Hash erneut berechnet und die Ergebnisse vergleicht. Wenn sie übereinstimmen, ist die Signatur gültig und der Inhalt der Nachricht nach dem Signieren nicht mehr geändert worden.



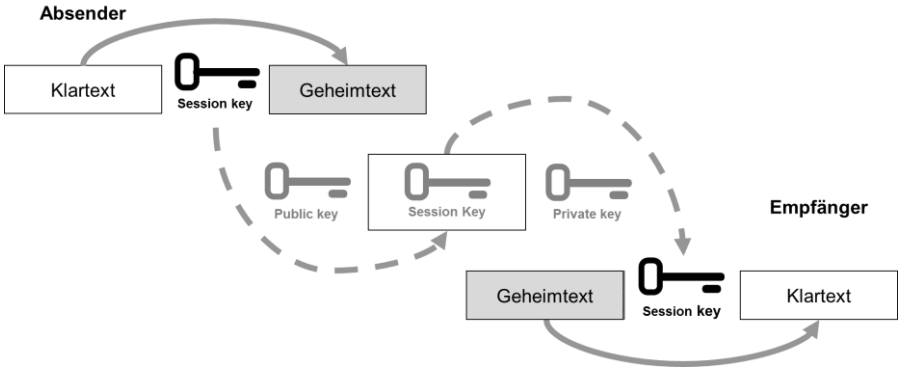
Schematische Darstellung der Erstellung von Signaturen

Damit Ver- und Entschlüsselung und Signieren bzw. Signaturprüfen funktionieren, müssen Sender und Empfänger nicht unbedingt dasselbe E-Mail-Programm nutzen, doch die Formate der Schlüssel, die Hashwertberechnung und die Verschlüsselungsverfahren müssen übereinstimmen.

3.6 Hybride Verschlüsselung

Vor dem komplexen Hintergrund der PKI erscheint die eigentliche Verschlüsselung beinahe trivial. In der Praxis wird aus Performancegründen nicht der gesamte E-Mailinhalt asymmetrisch verschlüsselt. Stattdessen wird die schnellere symmetrische Verschlüsselung genutzt, dann der symmetrische Schlüssel mit dem asymmetrischen Verfahren "versteckt" und mit der verschlüsselten E-Mail übertragen.

Beispiel: Der Absender möchte dem Empfänger eine S/MIME-verschlüsselte Nachricht zukommen lassen. Die Verschlüsselungs-Software generiert zunächst einen symmetrischen Session-Key. Mit diesem werden die im Klartext vorliegenden Daten verschlüsselt. Der Session-Key wird dann mit dem Zertifikat vom Empfänger verschlüsselt und mit an die Nachricht angehängt. Die verschlüsselte Nachricht enthält nun die Information, mit welchem Zertifikat die Nachricht verschlüsselt wurde, damit die Software des Empfängers den zum Zertifikat gehörigen privaten Schlüssel zur Entschlüsselung nutzen kann. Der Empfänger erhält die Nachricht. Mit seinem privaten Schlüssel kann er zunächst den symmetrischen Session-Key entschlüsseln, den das Programm des Absenders für diese Nachricht erstellt hat. Mit diesem Session-Key kann die Software des Empfängers schließlich die Originalnachricht entschlüsseln.



Schematische Darstellung der hybriden Verschlüsselung

3.7 Transportverschlüsselung

Wesentlicher Aspekt der Ende-zu-Ende-Verschlüsselung von E-Mails: Kein System kann auf dem Übertragungsweg auf die Inhalte der E-Mail zugreifen. Dies bedeutet allerdings gleichzeitig den kompletten Verzicht auf Content-Filter, Antivirus, Antispam, Data Loss Prevention und Archivierung.

Eine Alternative für Organisationen mit abweichenden Vorhaben ist daher die Transportverschlüsselung. Hierbei werden die Einzelnachrichten innerhalb eines verschlüsselten Transportkanals (auch Tunnel genannt) versendet, sodass ein Angreifer den Transport nicht abhören und somit die übertragenen Daten nicht mitlesen kann.
Am Anfangs- und Endpunkt der Verbindung aber liegen die Daten unverschlüsselt vor. Betreiber der Anfangs- und Endpunkte der Verbindung können die Daten daher im Klartext lesen. Wenn die Übertragung über eine Reihe von hintereinandergeschalteten Verbindungen erfolgt, gilt dies für jede einzelne Verbindung.

Die Transportverschlüsselung ist dann sinnvoll, wenn Anfangs- und Endpunkt der Verbindung in kontrollierten, geschützten Systemen liegen, die Übertragung zwischen diesen geschützten Systemen aber durch ein ungeschütztes Netz erfolgt, z.B. durch das öffentliche Internet. Streng genommen sind praktisch alle am Internet betriebenen Systeme kontrolliert und zumindest auf einer niedrigeren Ebene geschützt. Von und an diese Systeme übermittelte Daten gehen den Betreiber der genutzten Übertragungswege grundsätzlich nichts an. Deshalb wäre es sinnvoll, Transportverschlüsselung generell auf allen Ebenen zu nutzen. Das ist jedoch nicht der Fall.

So sind in der Praxis viele im Internet genutzte Leitungen unverschlüsselt. Das gilt insbesondere für Anbindungen von Haushalten, Firmen etc. an das Internet, z.B. per DSL oder Kabelanschluss. Auch in größeren Unternehmen mit mehreren Standorten oft als VPN (Virtual Private Network) genutzte MPLS-Anbindungen sind grundsätzlich nicht verschlüsselt. Ein Angreifer muss sich nur Zugang zur auch physisch oft nur wenig gesicherten Leitung verschaffen (z.B. an der Hausanschlussdose), um alle dort übertragenen Daten abzuhören.

Im E-Mail-Verkehr ist deshalb mindestens der Einsatz von TLS (Transport Layer Security) oder ein verschlüsseltes VPN mittels IPsec bei der Übermittlung generell anzuraten. Bei beiden Verfahren erfolgt über eine bestehende Verbindung zunächst ein Austausch öffentlicher Schlüssel. Mit Hilfe dieser öffentlichen Schlüssel wird dann per asymmetrischer Verschlüsselung ein symmetrischer Schlüssel ausgehandelt (Session-Key), mit dem dann die eigentlich zu übertragenden Daten verschlüsselt werden.

TLS und IPsec kapseln die zu übertragenden Datenpakete des eigentlich genutzten Protokolls und übernehmen dabei die Daten vom eigentlichen Service zur Verschlüsselung, bzw. übergeben nach der Entschlüsselung die entschlüsselten Daten an den Service auf Empfängerseite. Für den unterliegenden Service ist TLS und IPsec vollkommen transparent. TLS eignet sich gut zur Verschlüsselung vieler standardisierter Internet-Protokolle: aus SMTP wird SMTPS, aus IMAP wird IMAPs etc.

Alternativ kann eine TLS-Verschlüsselung nach erfolgtem Verbindungsaufbau eines Service eingerichtet werden (STARTTLS). Genutzt wird das z.B. beim E-Mail-Protokoll SMTP.

Der Vorteil: die Ansprache des Service erfolgt über den gleichen Port wie für den unverschlüsselten Dienst. Das ist aber gleichzeitig auch ein Nachteil, weil die Übertragung über diese Ports dann sowohl unverschlüsselt als auch verschlüsselt stattfinden kann und die tatsächliche Durchführung der Verschlüsselung schwerer zu überprüfen ist. Dennoch scheint sich STARTTLS zumindest im E-Mail-Verkehr gegenüber SMTPS durchzusetzen.

Der Namenswechsel von SSL zu TLS erfolgte nach SSL 3.0; TLS 1.0 entspricht SSL 3.1. Versionen bis SSL 3.0 werden heute als nicht mehr sicher angesehen, zum Einsatz kommen sollte in der Praxis mindestens TLS 1.0.

Das BSI empfiehlt den Einsatz von TLS 1.2[7]. Es reicht nicht aus, die richtige Version von TLS einzusetzen, auch das über TLS genutzte Verschlüsselungsverfahren muss sicher sein. Als extrem unsicher gilt DES, RC4 gilt als geknackt, Triple DES als bedingt sicher, AES-128 als sicher und AES-256 als derzeit sehr sicheres Verfahren, das bevorzugt genutzt werden sollte[8].

Ein weiteres Problem bei TLS, das im Übrigen prinzipiell bei allen Verschlüsselungen besteht, bei denen ein symmetrischer Session-Key ausgehandelt wird: ein Angreifer könnte die gesamte Kommunikation inklusive der Aushandlung des Session-Keys mitschneiden und für eine spätere Auswertung speichern. Wenn zu einem späteren Zeitpunkt dann die privaten Schlüssel der beim Verbindungsaufbau genutzten asymmetrischen Schlüssel in die Hände des Angreifers gelangen, kann er die symmetrischen Session-Keys rückwirkend entschlüsseln. Damit hat er Zugriff auf den Klartext der gesamten gespeicherten Kommunikation.

Tatsächlich wird berichtet, dass die NSA genau dies tut[9]. Der im April 2014 entdeckte Heartbleed-Bug in der viel genutzten Open-SSL Implementierung von TLS machte zudem das Auslesen genutzter privater Schlüssel möglich[10].

Um diesem Problem zu begegnen, wurde "Perfect Forward Secrecy" (PFS) entwickelt. Dabei werden aus den asymmetrischen Langzeitschlüsseln zunächst zufällige Kurzzeitschlüssel generiert, über die dann erst Session-Keys ausgehandelt werden. Die genutzten Kurzzeitschlüssel werden dann wieder verworfen und sind später auch bei Kenntnis der Langzeitschlüssel nicht wieder berechenbar. Eine etwa aufgezeichnete Kommunikation kann deshalb auch bei Kenntnis des privaten Schlüssels nicht entschlüsselt werden.

---

[7] BSI, Technische Richtlinie TR-02102-2: "Kryptographische Verfahren: Empfehlungen und Schlüssellängen Teil 2 - Verwendung von Transport Layer Security (TLS)", Version 2014-01, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2_pdf

[8] Institut für Internet-Sicherheit, Buch: Sicher im Internet, http://www.internet-sicherheit.de/institut/buch-sicher-im-internet/workshops-und-themen/verschluesselung-und-identitaeten/ssltls-verschluesselung/

[9] Siehe u.a. Zeit Online: "Verschlüsselte Mails machen die NSA neugierig", 21.6.2013, http://www.zeit.de/digital/datenschutz/2013-06/nsa-speichert-verschluesselte-mails

[10] Siehe z.B. heise Security: "So funktioniert der Heartbleed-Exploit", 10.4.2014, http://www.heise.de/security/artikel/So-funktioniert-der-Heartbleed-Exploit-2168010.html

Das BSI hält den Einsatz von PFS bei der Verwendung von TLS zum Schutz personenbezogener oder anderer sensibler Daten für grundsätzlich notwendig[5].

Mit der Verabschiedung von TLS 1.3 wurde 2018 nicht nur der Handshake zum Verbindungs- und Wiederaufbau komplett neu designt, um sicherer und latenzärmer zu arbeiten, sondern noch eine Vielzahl großer Veränderungen gegenüber der Vorgängerversion eingeführt.

Zudem wurde der Grundstein für die Verwendung neuer, kryptographisch auch bei künftiger Verwendung von Quantenrechnern als sicher angesehene, Cipher Suites gesetzt. Bei flächendeckender Einführung wird eine Vielzahl bisher noch verbreiteter Cipher Suites nicht mehr verwendet.

Mit eTLS wurde durch die ETSI eine Variante von TLS1.3 etabliert, die jedoch im Gegensatz zu reinen TLS 1.3 Implementierung für den internen Netzwerkverkehr auf die Perfect Forward Secrecy gänzlich verzichtet und somit eine unnötige Schwächung darstellt.

Zusätzlich sollte für die Ende-zu-Ende-Verschlüsselung oder Organisation-zu-Organisation-Verschlüsselung S/MIME bzw. PGP verwendet werden. Eine Kombination aus den Technologien ermöglicht dann einen umfassenden Schutz und authentische Kommunikation.

3.8 Zusammenspiel Clients - Endpoint Security

Die Absicherung der Kommunikation zwischen zwei Nutzern z.B. über eine durchgängige Verschlüsselung der ausgetauschten E-Mails setzt voraus, dass keine systembedingten Schwachstellen in der Kette des Informationsflusses auftreten. Häufig bieten die eingesetzten Nutzerendgeräte leichte Ansatzpunkte für potenzielle Angreifer, da oft grundlegende Regeln des IT-Betriebs - insbesondere für Windows-Systeme - von den Anwendern nicht beachtet werden. Nicht regelmäßig durchgeführte Updates von Betriebssystem und Anwendungen (Patchmanagement) sind neben dem Einsatz von unsicheren Anwendungen häufig auftretende Probleme. Darüber hinaus kann ein Nutzerendgerät durch fehlende oder veraltete Endgeräteschutzsoftware ("Virenschutz"), sowie durch sorglosen Umgang mit externen Datenträgern oder durch Öffnen kompromittierter Websites oder E-Mails leicht angegriffen werden.

Beispielsweise beruht das "EFAIL" genannte Szenario der vermeintlichen Entschlüsselung verschlüsselter E-Maildaten letztendlich auf der Tatsache, dass im Vorfeld der Entschlüsselung bereits ein Angriff auf die beteiligten Systeme stattgefunden hat, um Daten mitschneiden zu können. Die Ursachen, dass dieser Angriff möglich ist, liegen ausschließlich in der eingesetzten E-Mail-Software sowie der Sicherheitskonfiguration der Clientsysteme.

Abhängig von dem Schutzbedarf der Informationen, die auf einem Nutzerendgerät verarbeitet, gespeichert oder von diesem Endgerät mit anderen Nutzern geteilt werden, müssen die Schutzsysteme für das System dimensioniert werden. Hierbei müssen neben den o.g. Aspekten auch die Verschlüsselung des Endgerätes sowie der Einsatz einer umfassenden Überwachungslösung in Betracht gezogen werden.

4 Lösungen für die Praxis

In der Praxis existieren zwei Ansätze, die bei der Kommunikation zwischen Organisationen durchweg und für den User nicht ersichtlich gemischt werden können: Verschlüsselung ausgehend vom Mailprogramm/Client des Anwenders oder die Verwendung von Verschlüsselungsgateways.

Bei der Verschlüsselung über das Mailprogramm bzw. dem Client des Users, müssen die Zertifikate auf dem Client entweder auf einem Token (z.B. einer Smartcard) im TPM des Rechners oder als Soft-Key vorhanden sein. Dies hat den Vorteil, dass eine Verschlüsselung Ende-zu-Ende realisiert werden kann und die Mail auch auf dem Mailserver und im internen Netz der jeweiligen Organisation immer verschlüsselt vorliegt. Auch ist dem User immer klar, ob eine Mail verschlüsselt ist oder nicht.

Für ein reibungsloses Funktionieren ist es notwendig, dass organisatorische und technische Prozesse existieren, um sicherzustellen, dass die User über eigenes Schlüsselmaterial verfügen und dieses benutzen können. Die gängigen Mailprogramme wie z.B. Outlook unterstützen nativ bereits die Mailverschlüsselung über S/MIME. Für PGP ist i.d.R. ein Zusatzprogramm notwendig.

Bei der Nutzung eines Verschlüsselungsgateways wird zentral auf dem Gateway konfiguriert welche E-Mails verschlüsselt versendet werden. Hier wird Komplexität vom User weggenommen und durch entsprechende Prozesse in der IT-Administration abgedeckt. Durch die Nutzung eines Gateways kann so auch sichergestellt werden, dass bestimmte Kommunikation immer verschlüsselt wird. Gleichzeitig können z.B. Mailinhalte automatisch vor der Verschlüsselung bzw. nach der Entschlüsselung auf Viren, Malware oder kritische Inhalte geprüft werden. Es ist von der jeweiligen Implementierung abhängig, ob der User erkennen kann, ob eine E-Mail verschlüsselt oder unverschlüsselt ist.

Jede Organisation muss für sich selbst entscheiden, welche der beiden beschriebenen Ansätze im organisatorischen, rechtlichen und technischen Kontext am besten geeignet ist. In der Regel ist auch ein gemischter Ansatz möglich, bei dem bestimmte Mitarbeiter bereits am Client verschlüsseln müssen, während der Großteil der Belegschaft die Verschlüsselungsfunktion des Gateways nutzen können.

Bei der Nutzung der E-Mail-Verschlüsselung zwischen Unternehmen/Organisationen ist insbesondere der automatische Austausch von Zertifikaten

wichtig. Hierfür ist einmal eine Vertrauensstellung sowie nach Möglichkeit ein automatischer Abruf der Verschlüsselungszertifikate der Anwender notwendig. Die European Bridge CA bietet hier unter dem Dach von TeleTrusT mit dem Austausch von Root-Zertifikaten der teilnehmenden Unternehmen (die einem Mindest-Standard entsprechen) und der Bereitstellung eines Verzeichnisdienstes einen Ansatz, über den die Zertifikate der Teilnehmer automatisch abgerufen werden können.

4.1 Basisabsicherung

In heutigen Messaging-Systemen - damit sind sowohl E-Mail-Programme für Nutzer-endgeräte, als auch E-Mail-Serversysteme auf verschiedenen Betriebssystemplattformen gemeint - sind standardmäßig Verschlüsselungstechnologien implementiert, die häufig von Anwendern oder auch Administratoren nicht genutzt werden.

So können die meisten Clients E-Mails mit Servern auf Basis einer verschlüsselten Verbindung austauschen. Damit ist zumindest ein Teil des Übertragungsweges einer E-Mail abgesichert. Diese Mechanismen funktionieren in der Regel auch mit den heute gängigen Freemail-Systemen, die häufig im privaten Bereich genutzt werden.

Für die Verschlüsselung der Kommunikation zwischen den Serversystemen, bieten die meisten gängigen Produkte am Markt die Möglichkeit das Sicherheitsprotokoll TLS zu nutzen.

4.1.1 Transportverschlüsselung Client - Server (Beispiel MS Outlook)

Am Beispiel des E-Mail-Programmes MS Outlook, das u.a. für die Betriebssystem-plattformen MS Windows und MacOS verfügbar ist, lässt sich aufzeigen, dass durch entsprechende Konfigurationseinstellungen der Datenaustausch durch Verschlüsselung abgesichert werden kann. Weitergehende Informationen finden Sie im Abschnitt A1 des technischen Kompendiums im Anhang.

4.1.2 Transportverschlüsselung Server - Server (TLS/SMTPS)

Die Absicherung einer SMTP-Datenverbindung zwischen zwei E-Mail-Servern kann mit einfachen Mitteln über TLS erfolgen. Üblicherweise können die meisten der in der Praxis eingesetzten E-Mail-Systeme für die Nutzung verschlüsselte SMTP-Verbindungen über TLS konfiguriert werden. Abhängig von der Konfiguration der kommunizierenden E-Mail-Server **kann** der Datenaustausch verschlüsselt (Opportunistic TLS) oder **muss** verschlüsselt (Forced TLS) erfolgen.

In dem Fall, dass ein E-Mail-Server zwingend die Verschlüsselung des Transportkanals verlangt, kommt ein E-Mail-Austausch nicht zustande, wenn das System auf der Gegenseite nicht verschlüsseln kann. Für die Verschlüsselung muss auf beiden Servern ein gültiges SSL-Zertifikat installiert sein. Weitergehende Informationen finden Sie im Abschnitt 3.7 und A1 (technisches Kompendium im Anhang).

4.1.3 Mail-Verschlüsselung Client - Client (SMTP)

Für die E-Mail-Verschlüsselung via S/MIME ist nur ein persönliches Zertifikat notwendig und der Zugang zum öffentlichen Schlüssel des Empfängers.

Im Abschnitt A2 des technischen Kompendiums wird ausführlich am Beispiel der TeleTrusT European Bridge CA erklärt, wie diese Möglichkeiten in vorhandenen Systemen nutzbar gemacht werden können.

4.2 Verschlüsselung mit Plugins in E-Mail-Clients

Alternativ zu den bereits erwähnten gateway-basierten Lösungen ist es auch möglich, die Verschlüsselung bzw. Signierung im eigentlichen E-Mail-Client durchführen zu lassen. Dies hat gegenüber den Gateways Vor- und Nachteile, die individuell, bezogen auf den Anwendungsfall, abgewogen werden müssen.

Zu den Vorteilen zählen unter anderem der geringe Eingriff in die IT-Infrastruktur (Wegfall der Implementation eines Gateways in die Netzwerkarchitektur) sowie die Tatsache, dass Nachrichten, vom Benutzer gesteuert, bis

zum Endpunkt E-Mail-Client verschlüsselt bleiben, ohne aufgebrochen zu werden. So kann ein Höchstmaß an Informationssicherheit erreicht werden. Verschlüsselte Nachrichten verlassen den Rechner des Endanwenders in jedem Falle verschlüsselt.

Das gilt auch dann, wenn mit dem E-Mail-Server, gleich aus welchen Gründen, nicht verschlüsselt kommuniziert werden sollte. Der Endanwender besitzt zudem die Hoheit über das eingesetzte Schlüsselmaterial.

Aus dieser Hoheit ergibt sich jedoch gleichzeitig auch die Verantwortung über das eingesetzte Schlüsselmaterial. Nur wenige Verschlüsselungslösungen für E-Mail-Clients verfügen über die zusätzliche Möglichkeit zentraler Administration und Schlüsselverwaltung. Jedenfalls sind bei einem nicht nur punktuellen Einsatz zusätzliche Vorkehrungen zur Sicherung des eingesetzten Schlüsselmaterials gegen Verlust oder Missbrauch zu treffen. Dies kann durch einfache organisatorische Maßnahmen erreicht werden.

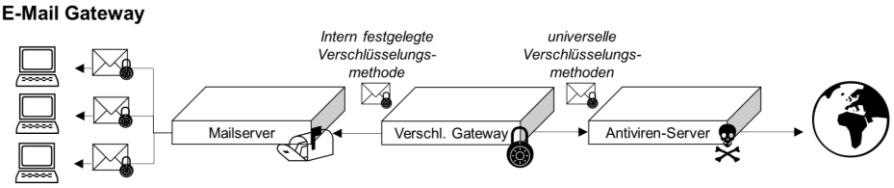
Die Verschlüsselung innerhalb von E-Mail-Programmen mittels Plugins stellt oftmals einen einfachen, ersten Schritt in die Verschlüsselungswelt dar, insbesonders dann, wenn nur einzelne Personen mit verschlüsselten E-Mails arbeiten sollen. Bei der Auswahl eines geeigneten Plugins sollten eine einfache und problemlose Installation sowie größtmögliche Usability im Vordergrund stehen. Gerade Neuanwender profitieren von einer Benutzerführung, die dabei hilft, Fehler zu vermeiden.

4.3 Secure E-Mail Gateways - serverbasierte Lösungen

Im Bereich der E-Mail-Verschlüsselung sind sogenannte Secure E-Mail Gateways weit verbreitet. Sie sichern serverbasiert und damit zentral und transparent für die Nutzer den gesamten durchlaufenden E-Mail-Verkehr gemäß eingestellter Regelwerke (Policies) ab. Compliance Enforcement, hohe User-Akzeptanz sowie der Verzicht auf Client-Installationen machen den Einsatz effizient und wirtschaftlich.

Secure E-Mail Gateways greifen zur PKI-basierten Verschlüsselung auf die Dienste der Zertifikats-Server zu. Für Kommunikationspartner ohne PKI wurden alternative Zustellmethoden entwickelt, bei denen z.B. ein Passwort den privaten Schlüssel ersetzt. Ein Secure E-Mail Gateway kann somit neben

S/MIME- und OpenPGP-verschlüsselten E-Mails auch passwortverschlüsselte PDF-, HTML- oder ZIP-Container ausliefern. Auch die Ad-hoc-Erstellung sicherer Web-Mailer-Accounts ist eine beliebte Alternative. De-Mail-Anbindungen, VPN- und TLS-Unterstützung sind ebenfalls auf einigen Gateways verfügbar. Zusätzlich bieten einige E-Mail Gateways bei Bedarf die Möglichkeit, zusätzliche Anti-Virus-Scans oder Spamfilter zu verwenden.



Schematische Darstellung eines E-Mail Gateways

4.3.1 "Organisational" und "Personal" Ende-zu-Ende-Verschlüsselung

Es gibt inzwischen Secure E-Mail Gateways, die interne und externe E-Mail-Verschlüsselung intelligent verknüpfen, sodass E-Mails nicht nur über das Internet, sondern auch innerhalb der firmeninternen Netze in verschlüsseltem Zustand übertragen werden. Dazu wird eine rein interne PKI aufgesetzt, die eine S/MIME-Verschlüsselung zwischen den internen Clients sowie die Verschlüsselung für den externen E-Mail-Verkehr mit dem Secure E-Mail Gateway direkt auf dem Client umsetzt. Jede E-Mail, egal an wen, ob intern oder extern, kann so ad-hoc per S/MIME verschlüsselt werden. Die relevanten E-Mail-Clients auf dem Desktop-PC oder Mobile Device unterstützen S/MIME von Hause aus. Optional stehen ggf. Plugins und Apps zur Verfügung.

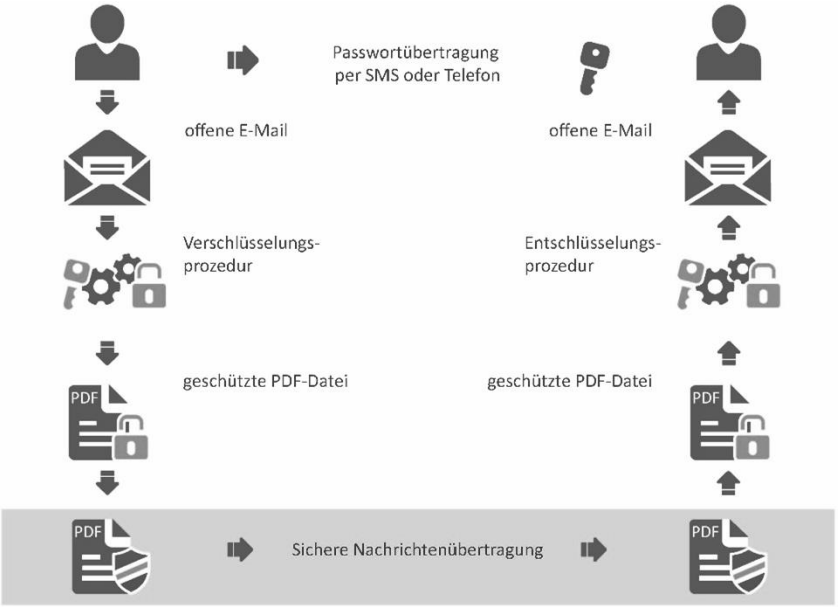
Ausgehende S/MIME E-Mails werden auf dem Secure E-Mail Gateway zunächst entschlüsselt und dann entsprechend den für einen Empfänger verfügbaren Möglichkeiten sowie ggf. auf Basis definierter Unternehmensrichtlinien neu verschlüsselt. Je nach Verfügbarkeit von Zertifikaten der externen Kommunikationspartner werden dann S/MIME, OpenPGP, passwortbasierte Verfahren (Push/Pull/HTML/PDF), De-Mail, TLS oder ähnliches genutzt. Umgekehrt erreichen alle eingehenden in jedweder Art verschlüsselten E-Mails den internen User als S/MIME-verschlüsselte E-Mail. Der beschriebene Ansatz wird mit "Organisational End-to-End" bezeichnet.

Im Moment der Umverschlüsselung können im Gegensatz zu durchgängiger Ende-zu-Ende-Verschlüsselung die E-Mails zentral durch Content-Filter, Data-Loss-Prevention-Systeme, Archivierungslösungen etc. bearbeitet werden. Ebenso ist von großem Vorteil, dass bei diesem Ansatz vom Secure E-Mail Gateway die Vielzahl der verschiedenen E-Mail-Verschlüsselungsformate der externen Kommunikationspartner unterstützt und nach innen einheitlich S/MIME für die Verschlüsselung verwendet werden. Entsprechend muss auf Clients keine spezielle Software für z.B. Passwortverschlüsselung oder OpenPGP installiert, verwaltet und technisch unterstützt werden. Das komplexe Zertifikatsmanagement auf Clients entfällt ebenfalls, da nur die interne CA auf den Clients unterstützt werden muss.

Secure E-Mail Gateways können je nach Sicherheitsanforderungen und Unternehmensrichtlinien sowohl den o.g. flexiblen Umverschlüsselungsmodus und durchgängige Ende-zu-Ende-Verschlüsselung als auch "Personal End-to-End"-Verschlüsselung problemlos parallel unterstützen. Trotz der Usability-Nachteile auf dem Client kann echte Ende-zu-Ende-Verschlüsselung für Anwendungsfälle mit Hochsicherheitsanforderungen durchaus gewünscht sein.

4.3.2 Passwortbasierte PDF-Verschlüsselung für E-Mails

Moderne Gateway-Systeme für Verschlüsselung und Signatur bieten für Fälle, in denen für Empfänger keine Zertifikate zu ermitteln sind, passwortbasierte Verschlüsselungsfunktionalitäten. Eine Variante ist u. a. die E-Mail-**PDF-Verschlüsselung**. Hierbei wird das Gateway vom Anwender direkt über seinen Outlook-Client oder durch zentrale Policies "angewiesen", die ausgehende E-Mail inklusive aller Dateianhänge komplett als PDF-Container zu verschlüsseln. Der Empfänger erhält eine standardisierte E-Mail mit einer verschlüsselten PDF-Datei im Anhang, die nur mit einem vom Absender übermittelten Passwort geöffnet und entschlüsselt werden kann. Moderne Gateways bieten dem Empfänger verschiedene Möglichkeiten, um das entsprechende Passwort zu erhalten. Die Liste reicht hier von SMS-Funktionen bis hin zu einem Selbstregistrierungsprozess.



Grafik: ICN, Dortmund

4.3.3 HTML-Push-Verfahren

Eine weitere Möglichkeit der sicheren Ad-Hoc Kommunikation stellt die Verwendung von verschlüsselten HTML-Mails dar. Hierbei wird die komplette zu versendende E-Mail am Gateway symmetrisch verschlüsselt und in einen HTML-Anhang verpackt. Anschließend wird eine unverschlüsselte, aber signierte, Träger- E-Mail an den Empfänger der eigentlichen Nachricht versendet, in deren Anhang sich der verschlüsselte HTML Container befindet. Das heißt, die komplette E-Mail wird an den Empfänger ausgeliefert und geht somit in dessen Verantwortungsbereich über. Dieses patentierte Verfahren bietet sehr viele Vorteile. So müssen ausgehende E-Mails nicht beim Absender zwischengespeichert werden. Beim Empfänger sind keine weiteren Komponenten erforderlich, das heißt dieses Verfahren ist vollkommen plattformunabhängig. Der Empfänger kann sofort auf die erhaltene E-Mail verschlüsselt antworten. Darüber hinaus kann man als Sender eine Lesebestätigung anfordern, um einen Nachweis für den Zugang der E-Mail zu erhalten. Die Ausstellung dieser Lesebestätigung kann vom Empfänger nicht abgestellt werden. Der Absender erhält auf jeden Fall eine Rückmeldung, ob und wann seine E-Mail den Empfänger erreicht hat. Die automatische Lesebestätigung kann damit immer als Anscheinsbeweis eingesetzt werden.

4.3.4 HTML Pull-Verfahren

Bei diesem Verfahren wird mit dem Container lediglich eine Referenz auf die E-Mail, welche noch auf dem Gateway vorgehalten wird, versendet. Der Anwender öffnet den HTML Container und baut damit einen gesicherten Rückkanal zum E-Mail Gateway des Absenders auf. Hier kann er sich dann mit einem Passwort anmelden und die E-Mail entschlüsseln.

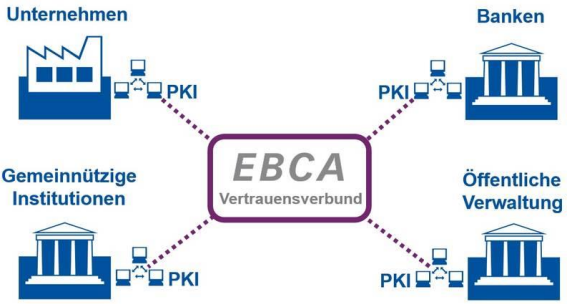
Vorteil beider HTML-Verfahren ist, dass der Empfänger sich nur ein Passwort merken muss. Auch eine Passwortwiederherstellung oder -rücksetzung stellt sich durch die Verwendung einer zentralen Komponente entsprechend einfach dar.

4.4 Sicherheit beim Zertifikats- und Schlüsselmanagement

4.4.1 TeleTrusT European Bridge CA - ein PKI-Vertrauensverbund

Mit der European Bridge CA (EBCA) hat TeleTrusT eine Initiative ins Leben gerufen, die für Nutzer den sicheren und komfortablen Austausch verschlüsselter Daten ermöglicht.

Sie ist ein Zusammenschluss einzelner, gleichberechtigter Public-Key-Infrastrukturen (PKIen) zu einem PKI-Verbund und ermöglicht eine sichere und authentische Kommunikation zwischen den beteiligten Unternehmen, Institutionen und öffentlichen Verwaltungen.



Schematische Darstellung des Vertrauensverbundes "TeleTrusT European Bridge CA"

Durch die Teilnahme an der EBCA können ausgegebene Zertifikate über lokale "Identitätsinseln" hinaus verwendet werden (siehe Abbildung). Somit werden unterschiedliche Geschäftsprozesse (Secure E-Mail, Secure Logon, Secure eID etc.) über die Grenzen der einzelnen Organisationen hinweg nutzbar gemacht.

Je größer das Netzwerk einer Bridge CA ist, desto größer ist der Nutzen für alle teilnehmenden Organisationen. Die TeleTrusT EBCA stellt kostenlos eine Liste der Wurzelzertifikate und untergeordneten Zertifizierungsstellen der Teilnehmer, sowie einen Verzeichnisdienst bereit. Damit können auch Außenstehende mit den EBCA Teilnehmern sicher kommunizieren. Durch die Bereitstellung dieser Tools werden zwei zentrale Probleme der sicheren Kommunikation über Organisations- und PKI-Grenzen hinweg gelöst.

1. Lösung der Verteilungsproblematik durch die Bereitstellung eines zentralen Verzeichnisdienstes.

2. Lösung der Validierungsproblematik durch die Bereitstellung von Sperrlisteninformationen und Zertifikatslisten.

4.4.2 Volksverschlüsselung

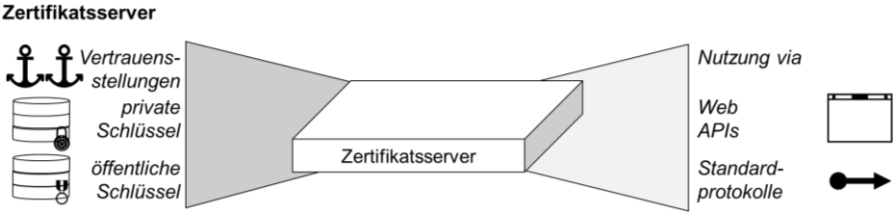
Die "Volksverschlüsselung", eine Initiative vom Fraunhofer SIT, stellt seit Sommer 2016 Privatpersonen kostenlose E-Mail-Zertifikate mit vorheriger Identitätsprüfung zur Verfügung. So sind diese Zertifikate auch für Organisationen durch Verifikation der Identität vertrauenswürdig. In der Regel erfolgt bei der Vergabe von kostenlosen Zertifikaten keine Identitätsprüfung, daher bietet die Volksverschlüsselung einen Mehrwert gegenüber anderen kostenlosen Zertifikaten. Nutzer der Volksverschlüsselungs-Zertifikate können dabei ebenfalls direkt mit den EBCA-Teilnehmerunternehmen verschlüsselte E-Mails austauschen, da die Volksverschlüsselung ebenfalls integriert ist. Die öffentlichen Schlüssel werden automatisch über den Verzeichnisdienst bereitgestellt. Mit der kostenlosen Verfügbarkeit von E-Mail-Zertifikaten für Bürger wird eine gute Möglichkeit geschaffen, verschlüsselte und vertrauenswürdige E-Mail-Kommunikation in der Gesellschaft zu etablieren.

4.4.3 Zertifikatsserver als technischer Lösungsansatz

Dass die vertrauliche Kommunikation zwischen Absender und Empfänger so einfach wie beschrieben funktioniert, ist der Idealfall. Vorab sind bei jeder einzelnen Verschlüsselung folgende Fragen zu klären: Woher bekommt der Absender das Zertifikat des Empfängers? Ist das Zertifikat echt? Ist es gültig? Ist es vertrauenswürdig? Dass der Absender das Zertifikat des Empfängers bekommt, ist unabdingbar.

Die Verifizierung des aufgefundenen Zertifikats schützt gegen die "Man-in-the-Middle"-Attacke. Bei einem solchen Angriff gibt jemand mit einem falschen Zertifikat vor, der Empfänger zu sein. Er fängt die Nachricht ab und leitet sie anschließend mit dem echten Zertifikat verschlüsselt an den Empfänger weiter. Das könnte über Wochen und Monate so laufen und der Empfänger und der Absender würden nie davon erfahren. Auch ein zurückgerufenes (revoked) Zertifikat könnte ohne Validierung von Angreifern weiter benutzt werden.

Die Komplexität der PKI mit der Fülle an Informationen zur Echtheits- und Gültigkeitsprüfung wird nur teilweise von den Client-Systemen erfasst und korrekt wiedergegeben. Das macht ein manuelles Schlüssel- und Zertifikatsmanagement praktisch unmöglich. Dafür sind als Zertifikatsserver benannte Lösungen entwickelt worden, die das Management der Zertifikate und öffentlichen Schlüssel einschließlich der Verifizierung und Validierung automatisiert übernehmen.



Schematische Darstellung eines Zertifikatsservers

Zertifikatsserver sind über verschiedene Schnittstellen mit den Trustcentern und den CAs größerer Firmen, Organisationen oder Verzeichnisdiensten wie der EBCA verbunden. Sie rufen Gültigkeitsinformationen über Rückruflisten (CRLs - Certificate Revocation Lists) ab und führen Echtzeitabfragen via Online Certificate Service Protocols (OCSP) durch. So werden Daten eingeholt,

Prüfsummen verglichen und der lokale Zertifikatsbestand permanent damit aktualisiert.

Zertifikatsserver sind heute integrale Komponenten von E-Mail-Verschlüsselungs-Gateways oder werden in Unternehmen auch stand-alone eingesetzt um E-Mail-Clients mit Zertifikaten, Rückruflisten und ggf. auch mit CA-Zertifikaten zu versorgen. Sie bieten eine Webanwendung, über die Kommunikationspartner auch manuell Zertifikate suchen und austauschen können.

Öffentliche Zertifikatswebportale mit Funktionen zum Suchen und Veröffentlichen von Zertifikaten sind z.B. GlobalTrustPoint oder CertBox[11], die online von jedermann in normalem Umfang kostenfrei genutzt werden können. Die European Bridge CA[12], ein Zusammenschluss von gleichberechtigten Unternehmens-PKIen, bietet ein Zertifikatsportal an, welches eigens festgelegten Mindestsicherheitsrichtlinien entspricht. Hierüber können ebenfalls zahlreiche öffentliche Zertifikate abgerufen werden.

Die Zertifikatsserver stehen neben der E-Mail-Verschlüsselung auch anderen PKI-basierten Anwendungen zur Verfügung. Als Identität eines Zertifikats kann statt einer Person auch ein System (beispielsweise mit Host-Namen oder IP-Adresse) eingetragen werden.

4.4.4 DANE

Beim Betrieb von unabhängigen Zertifikatsstellen (Certificate Authorities, kurz CAs), wie sie heute von Web-Browsern und E-Mail Systemen verwendet werden, kam es in der Vergangenheit mehrfach vor, dass diese nachlässig bei der Prüfung des Antragstellers waren und Missbrauch ermöglichten oder vollständig unter die Kontrolle von Kriminellen gerieten, was zu falsch ausgestellten Zertifikaten führte. Um die Vertrauenswürdigkeit des Systems der Zertifikatsstellen aufrecht zu erhalten sind daher fortwährende, aufwendige Maßnahmen erforderlich. Zum einen müssen die Zertifikatsstellen selbst regelmäßig hinsichtlich ihrer operationellen Praxis bewertet werden, zum anderen müssen die Verzeichnisse der gültigen Vertrauensanker in Web-Browsern und E-Mail-Systemen von deren Herstellern kontinuierlich entsprechend der Bewertungsergebnisse angepasst werden. Auch gestaltet sich eine objektive Bewertung der Vertrauenswürdigkeit einer Zertifikatsstelle schwierig, da zu einer Auditierung die Kooperation der untersuchten Zertifikatsstelle erforderlich ist. Selbst wenn dieser Prozess immer fehlerfrei

[11] globaltrustpoint.com oder certbox.org
[12] dir.ebca.de

wäre, bleibt für Zertifikate einer missbrauchten Zertifikatsstelle stets ein Zeitfenster bis zum nächsten Software-Update der Web-Browser und E-Mail-Systeme, um Schaden anzurichten und Angriffe zu ermöglichen. Vor diesem Hintergrund wird inzwischen auch grundsätzliche Kritik am System der Zertifikatsstellen geäußert[13][14][15]. Wirtschaftlich ist eine Zertifikatsstelle daran interessiert möglichst viele Zertifikate auszustellen, da sie je Zertifikat ein Entgelt vom Antragssteller erhält. Hinsichtlich Vertrauenswürdigkeit und Reputation sollte eine Zertifikatsstelle jedoch daran interessiert sein, zweifelhafte Zertifikatsanträge abzulehnen und somit nur wenige Zertifikate auszustellen. Im Spannungsfeld dieses intrinsischen Interessenskonflikts muss jede Zertifikatsstelle eingehende Anträge bewerten.

DANE steht für DNS-based Authentication of Named Entities und hilft alle diese Probleme zu vermeiden. Es ermöglicht Zertifikate von zentralen Stellen zu beziehen, ohne dass hierfür eine gesonderte Infrastruktur von gesonderten Zertifikatsstellen erforderlich wäre. Stattdessen beruht DANE darauf, dass jede Organisation ihre eigenen Zertifikate als Teil der über sie im Domain Name System[16] (DNS) verfügbaren Informationen selbst bereitstellt. Hierbei tritt jede Organisation als ihre eigene Zertifikatsstelle und nur für sich selbst auf, ohne, dass Dritte daran beteiligt sind. Als Vertrauensanker dient dabei das DNS, welches das zentrale Verzeichnis zur Namensauflösung im Internet ist. Ohne eine zuverlässige Namensauflösung durch das DNS könnte z.B. keine Webseite abgerufen werden. Da den Betreibern des DNS durch die Bereitstellung der Zertifikate keinerlei Mehreinnahmen entstehen, besteht auch kein Interessenskonflikt wie im Fall der unabhängigen Zertifikatsstellen. Da die Dienste des DNS zudem bereits in allen Industrie- und Schwellenländern durch DNSSEC[17] abgesichert verfügbar sind[18], steht mit DANE ein robustes, verteiltes System zur Verteilung und Überprüfung von Zertifikaten zur Verfügung, welches die Authentizität der Zertifikate sicherstellen kann und das frei von Interessenskonflikten der beteiligten Organisationen ist.

Weitergehende Informationen über DANE finden Sie im Anhang Abschnitt A4.

---

[13] https://stripe.ian.sh
[14] https://www.theregister.co.uk/2011/04/11/state_of_ssl_analysis/
[15] https://www.intezer.com/digital-certificates-when-the-chain-of-trust-is-broken/
[16] https://de.wikipedia.org/wiki/Domain_Name_System
[17] https://www.internetsociety.org/deploy360/dnssec/
[18] https://www.internetsociety.org/deploy360/dnssec/maps/

4.5 Geschlossene E-Mailsysteme

4.5.1 De-Mail

Das von der Bundesregierung geförderte und per entsprechendem Gesetz begleitete De-Mail-System wird mit "So einfach wie E-Mail und so sicher wie Papierpost" beworben. Es ist daraus ableitbar, dass es um den nächsten Schritt zur Digitalisierung der immer noch existierenden Papierpost geht. Hierzu werden im Standard zu De-Mail beispielsweise auch entsprechende digitale Alternativen zum herkömmlichen Einschreibeverfahren umgesetzt. De-Mail ist funktionsfähig, wird aber in der Unternehmenspraxis wenig angewendet. Häufiger kommt es im Umfeld von Behörden zum Einsatz.

Die dafür abgebildeten Sicherheitsmaßnahmen umfassen unter anderem auch die Transportverschlüsselung mit gegenseitiger Authentisierung der jeweiligen Kommunikationspartner, sodass beispielsweise auch ein Abfangen und Löschen von De-Mails auf dem Transportweg nicht möglich ist.

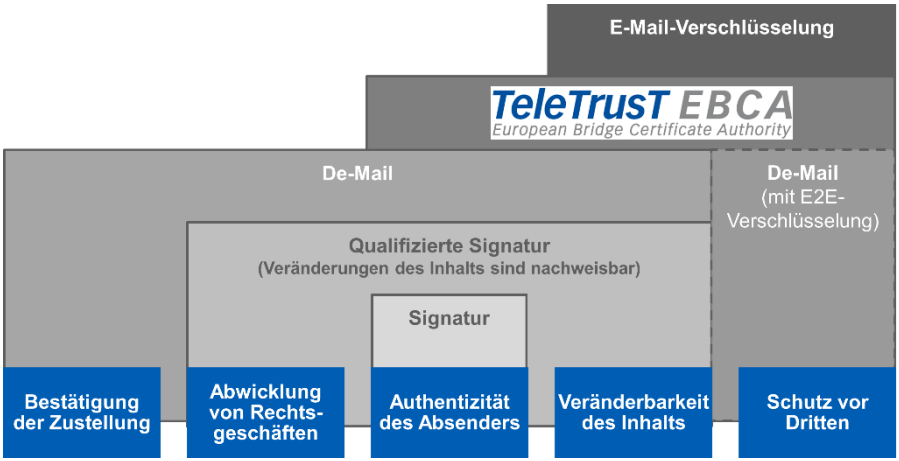
Architekturbedingt haben die vom Bund akkreditierten De-Mail-Provider Zugriff auf den Klartext von De-Mails, wenn sie nicht zusätzlich vom Absender Ende-zu-Ende verschlüsselt wurden. In die Kritik kam die De-Mail, weil diese Ende-Zu-Ende-Verschlüsselung nicht als verpflichtende Eigenschaft definiert wurde, sondern nur optional durch den Anwender genutzt werden kann.

De-Mail lässt aber auch die Übertragung von verschlüsselten Inhalten zu, sodass jeder die wirklichen Vorteile von De-Mail - stark authentifizierte Teilnehmer und "Einschreiben-ähnliche" Verbindlichkeit von elektronischen Nachrichten - auch zusammen mit starker Verschlüsselung nutzen kann. De-Mail beruht auf den gängigen E-Mail-Standards, daher können auch S/MIME oder auch OpenPGP zusammen mit De-Mail genutzt werden.

Jeder De-Mail-Nutzer kann seine S/MIME-Zertifikate im öffentlichen Verzeichnisdienst speichern, sodass auch die Beschaffung der Zertifikate zur Verschlüsselung einfach abgebildet ist. Die De-Mail-Provider wollen mit einer eingebundenen PGP-Verschlüsselung nun auch die Nutzung von OpenPGP in den web-basierten Nutzerschnittstellen einfacher machen. Für Unternehmen bieten einige Hersteller von Secure E-Mail Gateways entsprechende Lösungen an.

4.6 Zusammenhang zwischen De-Mail, Signatur und Verschlüsselung

Die nachfolgende Grafik veranschaulicht das funktionale Zusammenspiel von De-Mail als gesetzlich geregeltes, rechtssicheres E-Mail-System, der einfachen und qualifizierten Signatur, sowie der Verschlüsselung von E-Mails. Nur das Versenden einer verschlüsselten Nachricht über das De-Mail-System erfüllt die angegebenen fünf Kriterien. Setzt man nur eine Lösung zur Verschlüsselung von E-Mails ein, so kann man damit den Inhalt einer versendeten E-Mail vor Veränderung und dem unbefugten Zugriff von Dritten schützen.



Grafik: ICN /TeleTrusT

5 Fazit

Die Zukunft der sicheren und vertrauenswürdigen E-Mail-Kommunikation liegt in der verschlüsselten Übertragung zwischen den beteiligten Unternehmen, unabhängig davon, ob direkt vom Mailclient des einzelnen Users oder durch ein Verschlüsselungsgateway versendet wird. Möglichkeiten wie die "PDF-Verschlüsselung" oder "HTML-Verfahren" bieten pragmatische Ansätze für eine heutige Nutzung, ziehen aber immer einen Medienbruch nach sich, was trotz höherer Sicherheit die Nutzerfreundlichkeit in Mitleidenschaft zieht.

Private Anwender stehen vor der Herausforderung, dass die Nutzung von Verschlüsselungszertifikaten im privaten Umfeld nicht sehr verbreitet ist, auch wenn durch z.B. die EBCA technische Möglichkeiten zum Schlüsselaustausch bereitstehen und die gängigen Mailprogramme die E-Mailverschlüsselung unterstützen. Ein interessantes Projekt, welches Bürgern kostenlose Zertifikate mit einer Identitätsprüfung zur Verfügung stellt, ist die Volksverschlüsselung.

Generell ist die Durchdringung mit E-Mailverschlüsselung nach wie vor nicht in dem gewünschten Ausmaß gegeben und daher noch immer mit teilweise erheblichem Mehraufwand verbunden.

Technisches Kompendium

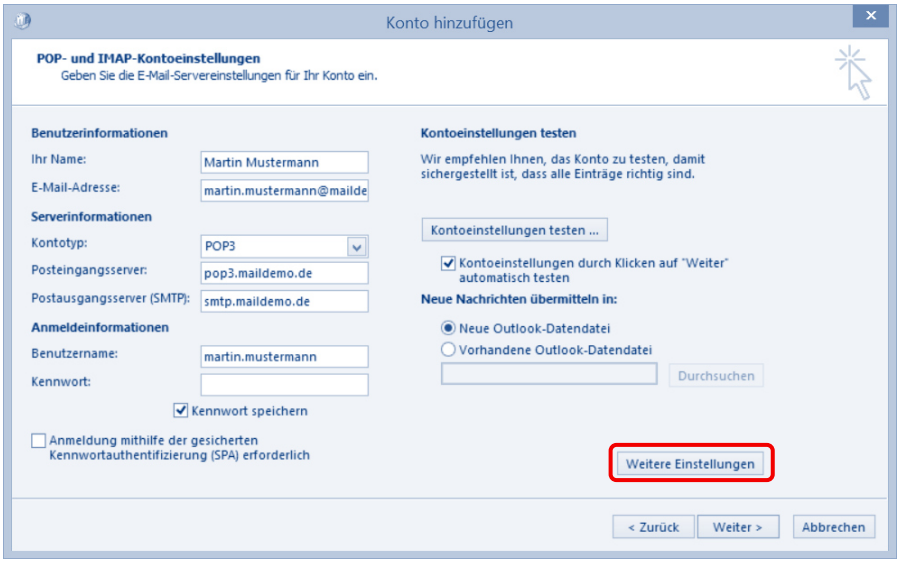
Auf den folgenden Seiten finden sich detaillierte technische Anleitungen und Beschreibungen zuvor angesprochener Themen. So wird dem Leser die Umsetzung von der Theorie in die Praxis ermöglicht.

A1 Verschlüsselung Client - Server (MS Outlook)

A1.1 Internet Mail Server

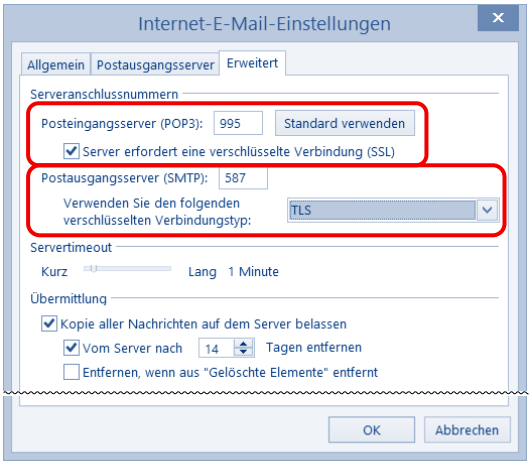
Bei der Einrichtung des Kontos sollten die Konto- und Serverparameter manuell eingestellt werden:

In diesem Beispiel wird ein Zugang zum Postfach auf dem Internet-Mail-Server über POP3 konfiguriert. Der E-Mail-Versand vom Outlook-Client zum E-Mail-Server erfolgt über das Protokoll SMTP.



Über den Button "Weitere Einstellungen" gelangt man zur Konfiguration der Parameter für die Verbindung zum E-Mail-Server.

Auf Basis der Konfigurationsvorgaben des E-Mail-Serverproviders werden auf der Registerkarte "Erweitert" die Protokollparameter für die Nutzung der verschlüsselten Transportwege vom E-Mail-Server zum Client (Mail-Empfang) und vom Client zum E-Mail-Server (Mail-Versand) festgelegt:



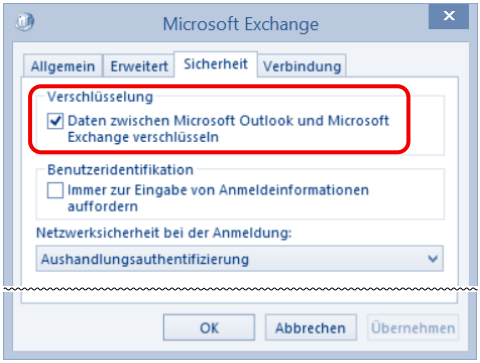
In diesem Beispiel wird der E-Mail-Empfang verschlüsselt mit SSL über POP3 und den Netzwerkport 995 abgewickelt. Der E-Mail-Versand erfolgt verschlüsselt mit TLS über SMTP und nutzt den Netzwerkport 587. Abhängig vom Provider oder genutzten Protokoll können ggf. auch andere Netzwerkports verwendet werden.

A1.2 MS Exchange

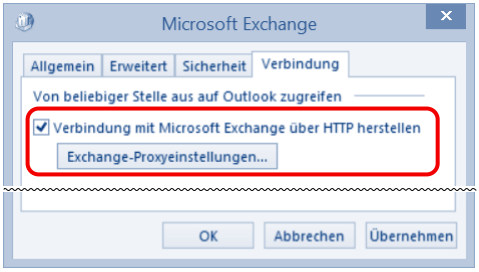
Auch bei der Konfiguration eines E-Mail-Kontos auf einem E-Mail-Server unter Microsoft Exchange werden die Serverparameter manuell eingestellt:

Über den Button "Weitere Einstellungen" gelangt man zur Konfiguration der Parameter für die Verbindung zum E-Mail-Server.

Auf der Registerkarte "Sicherheit" besteht die Möglichkeit die Verschlüsselung der Verbindung zwischen dem Outlook-Mail-Client und dem Exchangeserver im lokalen Netzwerk zu aktivieren:

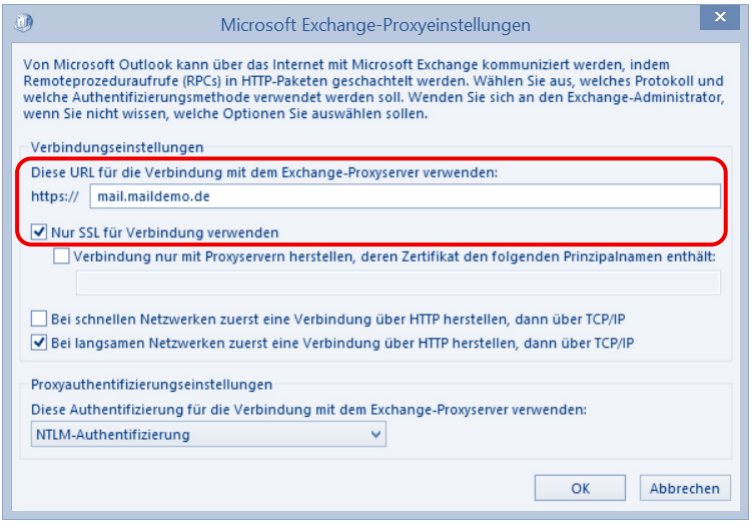


Als Ergänzung zum direkten Zugriff über das lokale Netzwerk kann der Zugriff des Outlook-Clients auf den E-Mail-Server mit Hilfe eines Proxyservers über das Protokoll https eingestellt werden:



Über den Button "Exchange-Proxyeinstellungen" gelangt man zur Konfiguration der Parameter für die Verbindung zum E-Mail-Server.

Für diesen Zugriffskanal kann vorgeschrieben werden, dass die Datenübertragung verschlüsselt erfolgen muss. In diesem Fall wird die Zugriffsadresse des Proxyservers eingestellt. Auf dem Proxyserver muss ein entsprechendes SSL-Zertifikat installiert werden, das für die Verschlüsselung der Kommunikation verwendet wird.



A1.3 Verschlüsselung Server - Server (TLS/SMTPS)

Die Absicherung einer SMTP-Datenverbindung zwischen zwei E-Mail-Servern kann mit einfachen Mitteln über das Verschlüsselungsprotokoll TLS erfolgen. Dieses Verfahren zur Absicherung der Kommunikation beim E-Mail-Transport via SMTP über SSL/TLS wird auch als SMTPS bezeichnet und ermöglicht dadurch Authentifizierung der Kommunikationspartner auf Transportebene sowie Integrität und Vertraulichkeit der übertragenen Nachrichten. Üblicherweise können die meisten der in der Praxis eingesetzten E-Mail-Systeme für die Nutzung verschlüsselte SMTP-Verbindungen über TLS konfiguriert werden.

Das Aushandeln der Verschlüsselung erfolgt direkt beim Verbindungsaufbau, noch bevor irgendwelche E-Mail-Daten ausgetauscht werden. Abhängig von der Konfiguration der kommunizierenden E-Mail-Server **kann** der Datenaustausch verschlüsselt (Opportunistic TLS) oder **muss** verschlüsselt (Forced TLS) erfolgen. In dem Fall, dass ein E-Mail-Server zwingend die Verschlüsselung des Transportkanals verlangt, kommt ein E-Mail-Austausch nicht zustande, wenn das System auf der Gegenseite nicht verschlüsseln kann. Für die Verschlüsselung muss auf beiden Servern ein gültiges SSL-Zertifikat installiert sein.

A2 Verschlüsselung und Vertrauen Client - Client

A2.1 Anleitung zur Installation der EBCA-Zertifikatsliste (CTL)

Die folgenden Abbildungen zeigen, wie Zertifikatslisten bzw. Zertifikate in den eigenen Speicher geladen (installiert) werden können.

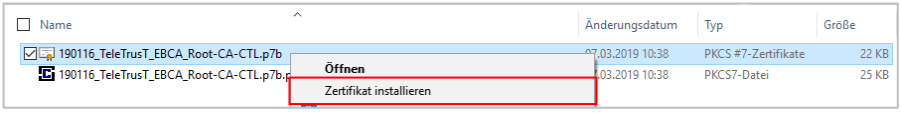
A2.1.1 Bevor Sie beginnen

- Prüfen Sie die signierten Dateien: https://www.seccomerce.de/de/produkte/webcontrust/secsigner/secsigner_verify.html
- Laden Sie die unsignierte Datei herunter (wenn nicht zuvor extrahiert): httpss://www.ebca.de/de/nutzung-der-ebca/vertrauen-herstellen/

A2.1.2 Anleitung zur Installation von Zertifikatslisten für MS Speicher

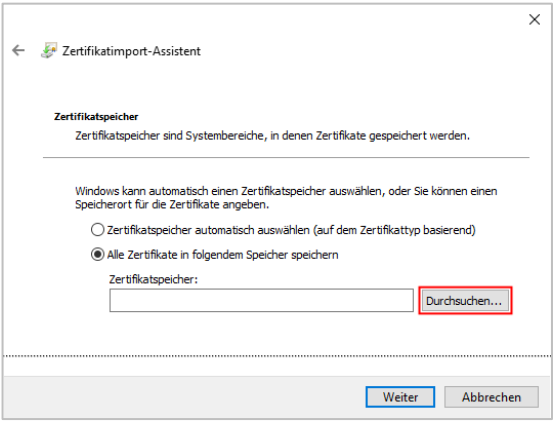
Wenn Sie die Zertifikatslisten in Thunderbird installieren möchten, nutzen Sie bitte folgende Anleitung: httpss://www.ebca.de/nutzung-der-ebca/vertrauen-herstellen/anleitung-ctl-installation-thunderbird/

1. Klicken Sie auf die zu installierende Liste mit der rechten Maustaste.

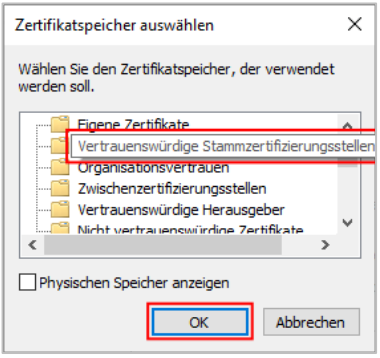


2. Starten Sie den Assistenten.

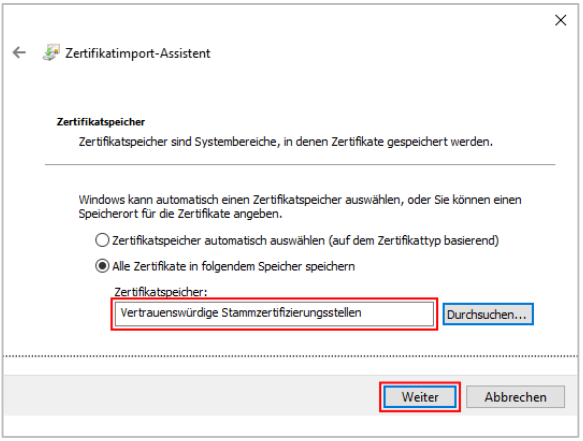
3a. Legen Sie den Zertifikatsspeicher fest.



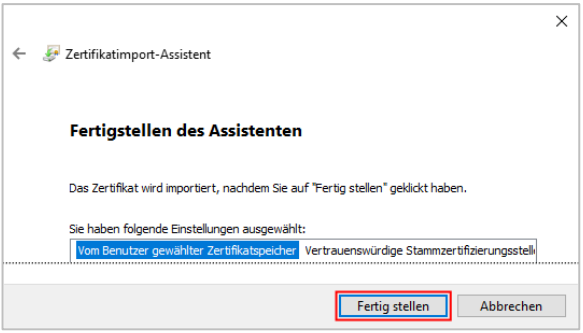
3b. Wählen Sie dazu den Speicher "Vertrauenswürdige Stammzertifizierungsstellen".



3c. Schließen Sie die Auswahl des Speichers ab.



4. Stellen Sie die Installation fertig.



A2.2 Anleitung zur EBCA-Verzeichnisdienstabfrage über Web

Die folgenden Abbildungen zeigen, wie ein Zertifikat über die Webseite des EBCA-Verzeichnisdienstes abgerufen werden kann.

Nach erfolgreichem Abruf des gesuchten Zertifikats kann dieses gespeichert und für den verschlüsselten E-Mail-Austausch mittels S/MIME-Standard genutzt werden.

A2.2.1 Bevor Sie beginnen

- Rufen Sie die Webseite mit dem Verzeichnisdienst auf: https://dir.ebca.de/search/basic/
- Bringen Sie die E-Mail-Adresse Ihres Empfängers in Erfahrung

A2.2.2 Anleitung zur Abfrage eines Zertifikates über Web

1. Rufen Sie die Webseite mit dem Verzeichnisdienst auf: https://dir.ebca.de/search/basic/

2. Füllen Sie die Sicherheitsabfrage aus und tragen Sie die E-Mail-Adresse ein zu der Sie das Zertifikat abrufen wollen und führen Sie die Suche durch.

3. Bei erfolgreicher Suche wird das Zertifikat angezeigt, und Sie können es direkt oder als digitale Visitenkarte herunterladen. Je nach genutztem E-Mail-Programm ist nun eine verschlüsselte Kommunikation mit dem Empfänger möglich.

Wie eine verschlüsselte Kommunikation in Ihrem E-Mail-Programm umgesetzt wird, erfahren Sie bei den Herstellern. Folgende Anleitungen stellen ausgewählte Hersteller bereit:

Microsoft Office Outlook 2013: https://goo.gl/CuuKff

Microsoft Office Outlook Mac 2011: https://goo.gl/QaOvgk

Apple Mail (Mavericks): https://goo.gl/MevZeG

Thunderbird: https://goo.gl/NhRvb

A2.3 Anleitung zur Verzeichnisdienstabfrage über LDAP

Die folgenden Abbildungen zeigen, wie ein Zertifikat über LDAP-Anbindung in einem E-Mail-Programm abgerufen werden kann.

A2.3.1 Bevor Sie beginnen

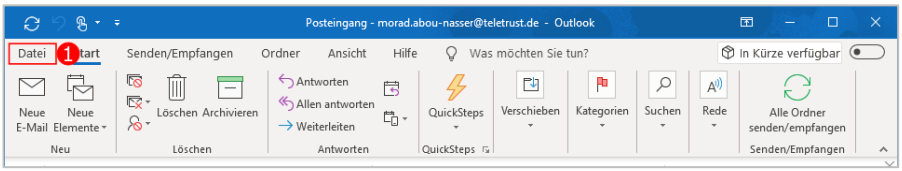
Der EBCA-Verzeichnisdienst kann als LDAP-Verzeichnis in Ihr E-Mail-Programm eingebunden werden. Dazu sind folgende Daten relevant:

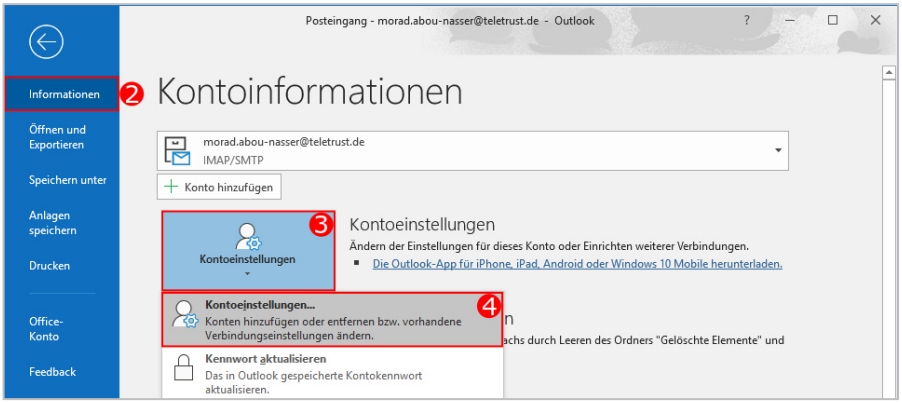
Verzeichnisdienstserver	dir.ebca.de
Port	389
Suchbasis	o=ebca

A2.3.2 Schritt-für-Schritt-Anleitung zur Konfiguration in Outlook 2010

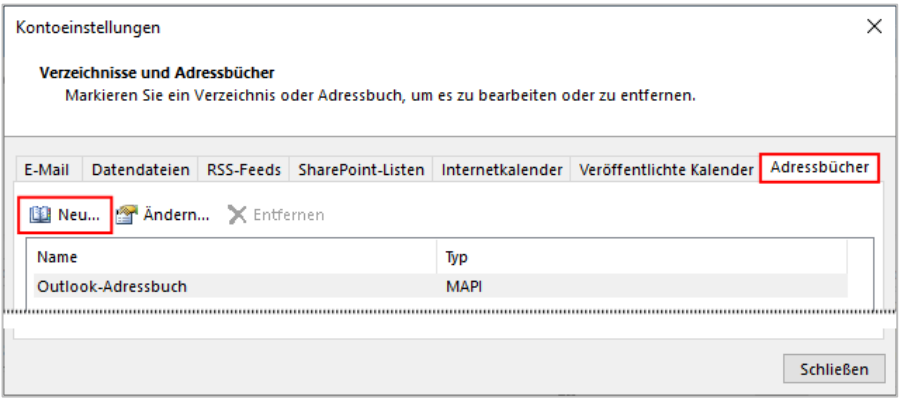
Diese Anleitung entspricht dem Vorgehen in Outlook 2010 und kann in anderen Versionen ähnlich sein.

1. Öffnen Sie Outlook und wechseln Sie zu "Kontoeinstellungen".
   In die Kontoeinstellungen gelangen Sie über die Registerkarte "Datei" (1) - "Informationen" (2) - "Kontoeinstellungen" (3) - "Kontoeinstellungen…" (4).

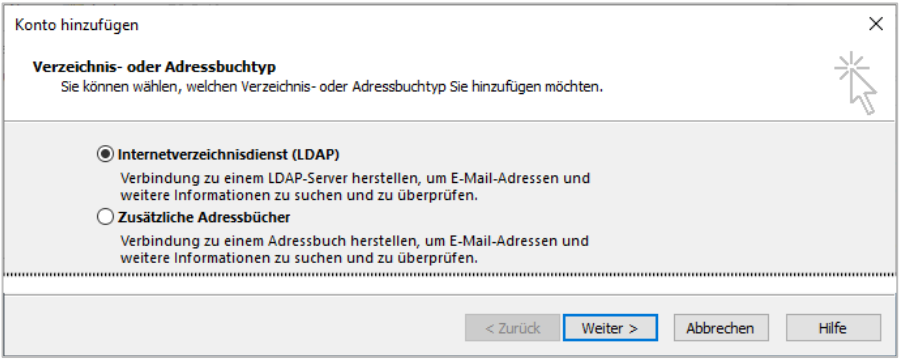




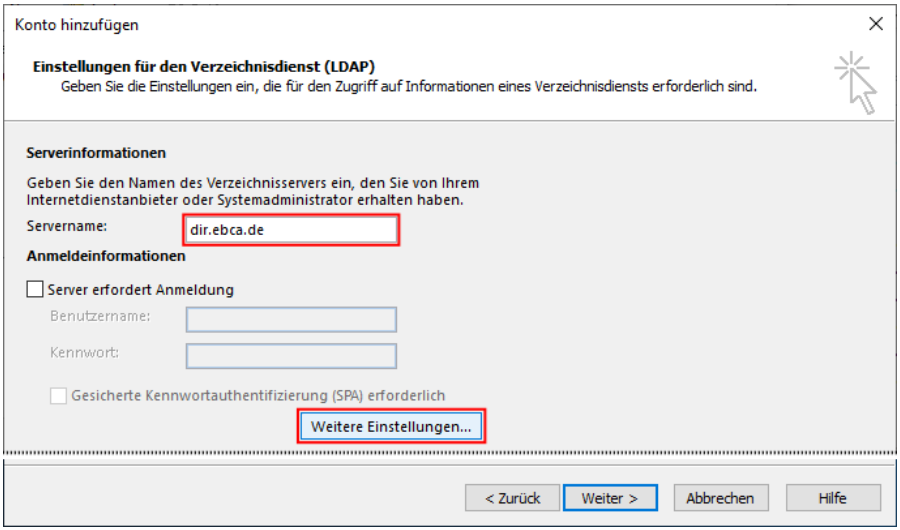
2. Wechseln Sie im neuen Fenster auf den Reiter "Adressbücher" und klicken Sie auf den Knopf "Neu".



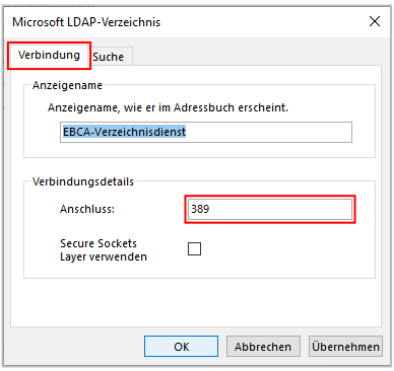
3. Wählen Sie im neuen Fenster "Internetverzeichnisdienst (LDAP)" aus und klicken Sie auf "Weiter".

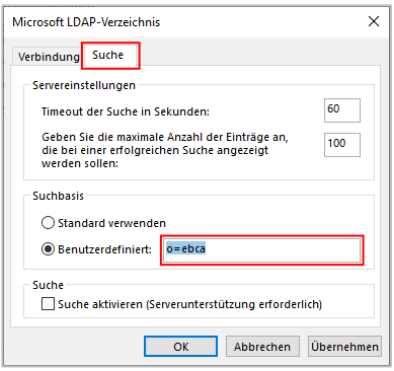


4. Tragen Sie unter "Servername" **dir.ebca.de** ein und klicken Sie auf "Weitere Einstellungen".



5. Tragen Sie unter "Verbindung" den Anschluss 389 und unter "Suche" die Suchbasis o=ebca ein.



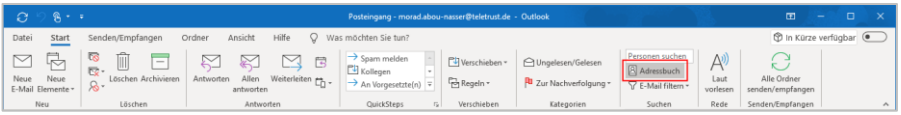


6. Bestätigen Sie Ihre Eingaben mit "OK" und beenden Sie die Konfiguration mit "Weiter" & "Fertig stellen".

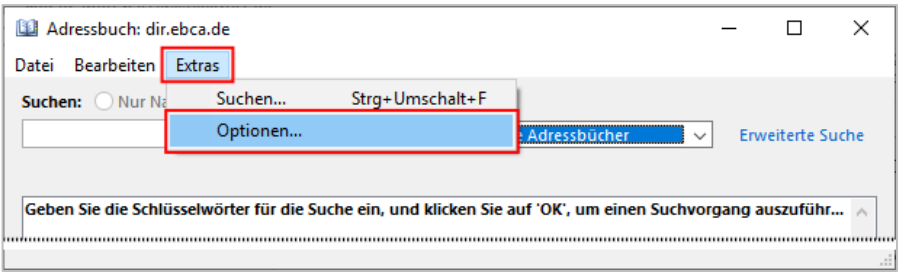
7. Starten Sie Outlook neu.

Für die automatische Abfrage beim verschlüsselten Senden von Nachrichten definieren Sie eine Abfragereihenfolge wie folgt:

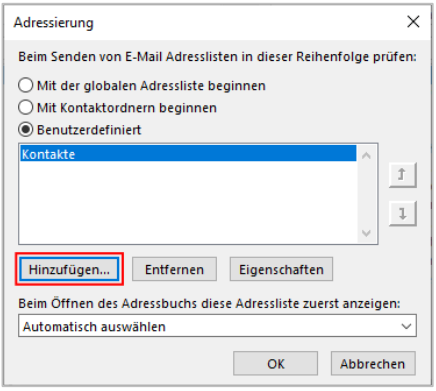
1. Ausgehend vom Reiter "Start" gehen Sie auf den Knopf "Adressbuch"

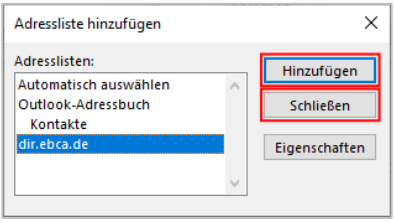


2. Gehen Sie im neuen Fenster auf "Extras" - "Optionen".

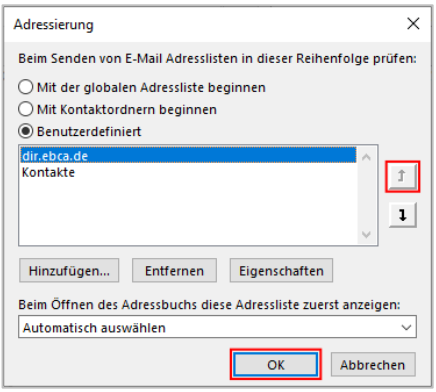


3. Fügen Sie Ihre neue Adressliste hinzu. Wählen Sie die neue Adressliste und drücken Sie auf "Hinzufügen" - "Schließen".





4. Schieben Sie den neuen Eintrag über den Pfeil auf die erste Stelle. Nun wird der EBCA-Verzeichnisdienst automatisch auf Zertifikate abgefragt, wenn eine verschlüsselte Nachricht gesendet werden soll.



Wie man ein LDAP-Verzeichnis in anderen E-Mail-Programmen einträgt, erfahren Sie bei den Herstellern. Folgende Anleitungen stellen ausgewählte Hersteller bereit:

Microsoft Office Outlook 2013: analog zu Office Outlook 2010

Apple Mail (Mavericks): https://goo.gl/RwE3A3

Thunderbird (englisch): https://goo.gl/cPLuQ

Microsoft Office Outlook 2010: https://goo.gl/qgNe1m

A3 Abgrenzung Vertrauensbereiche

A3.1 On Premise

Bei einer On-Premise-Verschlüsselungslösung werden sogenannte Gateway-Systeme (ggf. virtuell) in der Kundeninfrastruktur bereitgestellt, jedoch vom Security-Anbieter in Absprache mit dem Kunden konfektioniert und konfiguriert. Oftmals ist der Kunde selbst für den Betrieb, Wartung etc. verantwortlich und muss entsprechend ausgebildetes Personal vorhalten, Serviceupdates spielt jedoch üblicherweise der Dienstleister ein und benötigt hierzu administrativen Zugriff. Dafür besitzt er jedoch selbst physikalische Kontrolle derart, dass er Zugriff auf die in seinen Rechenzentren stehenden Appliances besitzt. Generell profitieren On-Premise-Kunden von der Unabhängigkeit vom Internetzugriff, im Bereich E-Mail ist dieser Vorteil jedoch fraglich.

A3.2 Cloud Services

Cloud Services lagern den Betrieb der E-Mail-Verschlüsselung ebenfalls komplett auf Dienstleister aus: Analog zu On-Premise-Lösungen wird eine Gateway-Verschlüsselung geboten und das komplette Zertifikats- und Key-Handling ohne Arbeitsaufwand für die die eigentliche Infrastruktur betreibenden Administratoren autark übernommen. Der Kunde kann auf den Service weltweit zugreifen, lediglich ein Internetzugriff muss hierzu sichergestellt werden, was jedoch im Bereich E-Mail ohnehin vorausgesetzt wird.

Hierbei ist jedoch die Software as a Service (SaaS) ausschlaggebend: Es wird der Service als solches zur Verfügung gestellt, der E-Mail-Strom selbst wird zunächst in die vom Dienstleister betriebene Cloud gelenkt (bsw. über entsprechende MX Records) und anschließend über verschlüsselte Verbindungen an den Kunden weitergereicht (eingehender Verkehr) oder je nach Kundeneinstellungen dem Kommunikationspartner des Kunden zugeführt (ausgehender Verkehr).

Üblicherweise sind viele Einstellungsmöglichkeiten vorhanden und beraten die Anbieter den Kunden umfassend bei der initialen Einrichtung des Verschlüsselungsservices.

Bei der Entscheidung für einen Cloud Service stehen oftmals Sicherheitsaspekte im Sinne der Verfügbarkeit im Vordergrund: Cloud-Anbieter sind in der

Lage, den Verkehr transparent über mehrere, bestenfalls über ganz Deutschland verteilte Rechenzentren zu routen und somit eine Hochverfügbarkeit zu gewährleisten, die mit lokal installierten Lösungen nur schwer zu erreichen sind. Aufgrund der hohen Redundanz können System- und Serviceupdates sicher und ohne Leistungseinbußen im laufenden Betrieb vorgenommen werden.

Auch die Kosten einer Cloud-Lösung sind üblicherweise geringer als bei On Premise-Betrieb, da die Betriebskosten vollständig mit outgesourced werden können. Aufgrund der Weitergabe von Daten ist eine gründliche Anbieterauswahl im Hinblick auf geltende Datenschutzbestimmungen empfehlenswert, üblicherweise haben die Dienstleister bereits hierauf abgestimmte Vertragswerke.

Ebenfalls lohnt sich ein genauer Blick auf Ort und Art der Leistungserbringung durch den Security-Dienstleister: betreibt der Anbieter seine Cloud selbst, stehen die Server in Deutschland oder nutzt der Anbieter selbst externe Cloud-Anbieter wie AWS, Microsoft Azure etc.?

A4 DANE

DANE steht für DNS-based Authentication of Named Entities. Im Abschnitt 4.4.4 wurden bereits die Schwachstellen des Systems der Zertifikatsstellen, und die Vorteile von DANE aufgeführt. Im Folgenden finden Sie weitere, technische Details zu DANE.

A4.1 Funktionsweise

DANE ermöglicht eine automatische Verteilung von TLS-Zertifikaten sowie die Überprüfung dieser Zertifikate auf Authentizität, d.h. es ermöglicht das Erkennen von Spoofing und Man-in-the-middle Angriffen. Die dazu notwendigen Informationen werden per DNS (Domain Name System) bereitgestellt und abgefragt. Das verwendete Protokoll ist identisch mit dem für Namensauflösung und -zuordnung von Hostnamen und IP-Adressen eingesetzten. Es wird beim DNS Server lediglich nach anderen Datensatztypen als bei der Namensauflösung gefragt.

Da im DANE System jede Organisation Zertifikate für ihre eigenen Systeme und Dienste selbst bereitstellt und verwaltet, anstatt hierfür eine externe Zertifikatsstelle zu beauftragen, muss ein Server-Betreiber zunächst ein TLS Zertifikat erzeugen. Dieses ist mit seinem eigenen, geheimen Schlüssel signiert und wird daher als selbst-signiert bezeichnet. Es lässt sich ganz ohne Zuhilfenahme weiterer Schlüssel oder Zertifikate überprüfen und verwenden, daher könnte es als Vertrauensanker des Server-Betreibers dienen. Dieses Erzeugen eines selbstsignierten Vertrauensankers wird auch von jeder Zertifizierungsstelle durchgeführt, um entsprechende Vertrauensanker für sich zu erhalten. Mit dem Erzeugen eines solchen TLS Zertifikats wird der Server-Betreiber daher sozusagen zu seiner eigenen Zertifizierungsstelle.

Um das neue Zertifikat den Client-Systemen bekannt zu machen, hinterlegt der Server-Betreiber in der DNS-Zone, zu der ein Server gehört, schließlich den Hash-Wert des Zertifikats in einem TLSA-Record. Anschließend installiert er es in geeigneter Weise auf seinem Server-System, um z.B. die Seiten seines Web-Servers über HTTPSS auszuliefern. Während eines Verbindungsaufbaus kann ein Client per DNSSEC den TLSA-Record aus der DNS Domain des Servers abfragen und damit Echtheit und Gültigkeit des vom Server im Zuge des Verbindungsaufbaus ausgehändigten Zertifikats prüfen. Weil dieser TLSA-Record in der für den Server zuständigen DNS-Zone hinterlegt sein muss, ist der Betreiber selbst für die Richtigkeit des Zertifikats

verantwortlich. Es ist nicht mehr notwendig, einer externen Zertifikatsstelle zu vertrauen, die das Zertifikat signiert.

Auch das DNSSEC Verfahren, welches zur Authentifizierung der DNS-Verkehre für DANE eingesetzt wird, kommt nicht ohne Vertrauensanker-Zertifikate aus. Diese liegen aufgrund der Rolle des DNS als kritische Infrastruktur des Internets jedoch bei den gemeinnützigen Organisationen ICANN (Internet Corporation for Assigned Names and Numbers) und IANA (Internet Assigned Numbers Authority), bzw. von diesen gewählten und beauftragten Trusted Community Representatives und nicht mehr bei privatwirtschaftlichen Unternehmen die Interessenskonflikten und der Gewinnerzielung unterworfen sind.

A4.2 Verwendung beim E-Mail-Versand

Um eine E-Mail mit DANE über SMTP zu versenden, sind folgende Schritte erforderlich:

1. Die E-Mail-Anwendung des Benutzers gibt, nachdem der Benutzer den Befehl zum Absenden erteilt hat, die zu versendende E-Mail an den lokalen E-Mail-Server ab.

2. Der lokale E-Mail-Server erfragt beim DNS den für den Empfänger zuständigen E-Mail-Server.

3. Der lokale E-Mail-Server erfragt beim DNS den TLSA-Record (Hash-Wert des Server-Zertifikats) des für den Empfänger zuständigen E-Mail-Servers und fordert hierbei die Verwendung von DNSSEC an. Ist ein entsprechender TLSA-Record im DNS vorhanden, liefert das DNS diesen an den lokalen E-Mail-Server zurück und da DNSSEC angefordert wurde, signiert es die Antwort mit dem für den jeweiligen DNS-Server zugeordneten Vertrauensanker-Zertifikat. Durch Überprüfung der Signatur der DNS-Antwort kann der lokale E-Mail-Server feststellen, ob die Antwort vom richtigen DNS-Server stammt und, ob sie während der Übertragung von Dritten verändert wurde. Nur wenn beide Überprüfungen erfolgreich verlaufen, akzeptiert der lokale E-Mail-Server die DNS-Antwort.

4. Wenn die Anfrage nach einem TLSA-Record erfolgreich war, baut der lokale E-Mail-Server eine mit TLS verschlüsselte Verbindung zum empfangenden E-Mail-Server auf. Hierbei berechnet er den Hash-Wert des vom für den Empfänger zuständigen E-Mail-Server im Rahmen

des TLS Verbindungsaufbaus übertragenen TLS-Zertifikats und vergleicht diesen mit dem zuvor aus dem DNS erhaltenen Hash-Wert. Stimmen beide überein, kann das erhaltene TLS-Zertifikat als gültig betrachtet werden.

5. Stimmen die Hash-Werte nicht überein oder scheitert der Aufbau einer TLS-Verbindung aus anderen Gründen (z.B. fehlende Port-Freigabe), kann der lokale Server den Vorgang entweder abbrechen, oder auf eine unverschlüsselte Verbindung wechseln und den E-Mail-Versand hierüber fortsetzen. Dieses Verhalten muss im lokalen E-Mail-Server konfiguriert werden. Abgesehen von begründeten Ausnahmefällen, ist ein Abbruch aus Sicherheitsgründen stets vorzuziehen.

6. Kommt eine verschlüsselte Verbindung zustande, wird hierüber die E-Mail-Mitteilung unter Verwendung von SMTP übertragen. Falls nicht, wird die Übertragung abgebrochen.

DANE selbst ist bereits seit August 2012 standardisiert (RFC 6698) und fast alle DNS-Zonen bieten heute volle Unterstützung für DNSSEC[19]. DANE für SMTP ist seit Oktober 2015 standardisiert (RFC 7672) und wird nach Kenntnis der Autoren (Stand Februar 2019) mindestens von folgenden E-Mail-Server Lösungen unterstützt:

- Postfix (seit 2014)[20],
- Halon (ab Version 3.4-rocky-r2)[21],
- Exim (ab Version 4.91)[22].

Zusätzlich muss natürlich eine entsprechender TLSA-Record für das Zertifikat des E-Mail-Servers im DNS hinterlegt werden.

Die Absicherung des Transportweges einer E-Mail mittels DANE stellt zwar sicher, dass die E-Mail zwischen zwei Servern in einer verschlüsselten Verbindung übertragen wird, oft sind jedoch Weiterleitungen über mehrere E-Mail-Server erforderlich, um die Mitteilung zuzustellen. Um vom ersten sendenden bis zum letzten empfangenden E-Mail-Server dieser Kette stets verschlüsselt zu übertragen, müssen alle Transportabschnitte entlang des Weges TLS unterstützen. Die Verwendung von DANE über alle Teilabschnitte

[19] https://www.internetsociety.org/deploy360/dnssec/maps/
[20] http://www.postfix.org/TLS_README.html#client_tls_dane
[21] https://wiki.halon.io/DANE
[22] http://www.exim.org/exim-html-current/doc/html/spec_html/ch-encrypted_smtp_connections_using_tlsssl.html#SECDANE

des Transportweges kann zwar technisch nicht erzwungen werden, ist aber für eine Vertrauenswürdige E-Mail-Beförderung unerlässlich.

Nicht verwechselt werden darf DANE für SMTP mit einer Ende-zu-Ende-Verschlüsselung für E-Mail. Die E-Mail an sich wird trotz DANE und TLS weiterhin im Klartext übertragen und liegt auch auf allen entlang des Transportweges involvierten Servern im Klartext vor. Es wird lediglich sichergestellt, dass der Transportweg zuverlässig und verlässlich verschlüsselt wird und unbefugte Dritte die Datenverkehre nicht abfangen können (Man-in-the-middle).

A4.3 Ende-zu-Ende-Verschlüsselung mit DANE

Für die Absicherung der Transportverschlüsselung per TLS ist DANE schon bei kleinen und großen E-Mail-Providern im Einsatz. Aber neben der Absicherung der Transportverschlüsselung kann DANE auch zur Absicherung der Ende-zu-Ende Verschlüsselung bei E-Mail eingesetzt werden.

Die meistverwendeten Protokolle zur Ende-zu-Ende Verschlüsselung von E-Mail sind S/MIME und Pretty Good Privacy (PGP). Beide Protokolle können mit DANE sicherer betrieben werden, zudem kann mit DANE eine (begrenzte) Interoperabilität zwischen beiden Protokollen hergestellt werden.

A4.3.1 S/MIME

Die Benutzung von DANE zur Absicherung von S/MIME-E-Mail wird in RFC 8162 beschrieben. Die Probleme mit S/MIME-Zertifikaten sind ähnlich wie die Probleme bei der Benutzung von TLS mit Zertifikaten in Servern: dem System der Zertifikatsstellen (CAs) wird nicht von allen Kommunikationsteilnehmern vertraut. Ähnlich wie bei TLS ermöglicht DANE die Vertrauensprüfung ohne Zertifikatsstellen.

Der Besitzer eines X.509 E-Mail Zertifikats publiziert einen sog. SMIMEA-Record im DNS. Der SMIMEA-Record funktioniert analog zum TLSA-Record für TLS (die Datenfelder sind identisch). Er wird vom Empfänger eines fremden Zertifikats benutzt, um die Echtheit des Zertifikats zu ermitteln. Hierzu fragt der Empfänger des E-Mailzertifikats den zugehörigen SMIMEA-Record im DNS des Zertifikatbesitzers ab und prüft das Zertifikat anhand der Informationen im SMIMEA-Record. Der SMIMEA-Record mit den Zertifikatsdaten wird hierbei unter der E-Mailadresse des Zertifikat-Besitzers gespeichert. Im

DNS kann auch ein Root-Zertifikat für eine Gruppe von Benutzern gespeichert werden, welches im Weiteren die Zertifikate der Benutzer authentisiert (z.B. ein Firmenzertifikat).

A4.3.2 OPEN PGP KEY

Die Benutzung von DANE zur Absicherung von PGP-E-Mail wird in RFC 7929 beschrieben. Die Herausforderungen bei Ende-zu-Ende Verschlüsselung mittels PGP sind zwar andere als bei S/MIME, die Lösung per DANE ist jedoch sehr ähnlich. Bei PGP muss der Sender einer E-Mail (beim Verschlüsseln) oder der Empfänger einer E-Mail (zum Prüfen der Signatur) den öffentlichen Schlüssel des Kommunikationspartners besitzen. In einem dezentral organisierten System wie PGP kann dies problematisch sein.

PGP-Schlüssel werden heute über sogenannte Key-Server verteilt. Diese Key-Server können jedoch keine Aussage über die Richtigkeit und Vertrauenswürdigkeit der Schlüssel treffen. Benutzer müssen die Schlüssel manuell oder per Web-of-Trust mittels Unterschriften auf dem Schlüssel verifizieren. Mit DANE kann ein PGP-Benutzer seinen öffentlichen PGP-Schlüssel in einer (DNSSEC-gesicherten) DNS-Zone speichern. Der Besitzer des Schlüssels behält, anders als bei den PGP-Key-Servern, die Kontrolle über den Schlüssel und kann den Schlüssel ersetzen oder entfernen.

Die Absicherung der Abfrage des PGP-Keys per DNSSEC gesichertem DNS ersetzt nicht die Prüfung des Schlüssels per Web-of-Trust, eine E-Mail per ungeprüften PGP-Key zu versenden ist jedoch immer noch besser, als eine E-Mail komplett unverschlüsselt und ungesichert zu senden.

A5 Efail

A5.1 Der Scoop

Im Mai 2018 sorgte eine Welle medialer Berichterstattung für Aufmerksamkeit, in der behauptet wurde, die OpenPGP- und S/MIME-Verfahren zur Ende-zu-Ende Verschlüsselung von E-mails seien nicht mehr sicher. Ein Forscherteam der FH Münster, der Ruhr-Universität Bochum und der KU Leuven hatten zunächst im Dezember 2017 zwei Common Vulnerabilities and Exposures (CVE) registriert, je eine für das OpenPGP Verfahren[23] und das S/MIME Verfahren[24]. Solche neu registrierten CVE sind zunächst nicht öffentlich, sondern werden nur den Anbietern betroffener Produkte mitgeteilt. Diese treten dann in der Regel mit den Anmeldern der CVE in Kontakt, um mehr über die Verwundbarkeit zu erfahren und diese beseitigen zu können. Hat der Anbieter sein Produkt entsprechend verbessert, teilt er dies der CVE Registrierungsstelle mit, woraufhin diese die CVE veröffentlicht, zusammen mit der Information auf welche Produktversion die Anwender ihre Systeme aktualisieren sollten um geschützt zu sein.

Aus der Berichterstattung und den Diskussionen der beteiligten Sicherheitsforscher auf sozialen Plattformen scheint es jedoch so, als ob in diesem Fall die Reaktionen der betroffenen Anbieter nicht geeignet gewesen waren, um beim Forscherteam den Eindruck entstehen zu lassen, dass die Schwachstellen schnell behoben werden würden. Die Forscher trafen daher im Mai 2018 die Entscheidung, die Meldung öffentlich zu machen, wohl in der Hoffnung, damit Druck auf die Anbieter ausüben zu können. Hierzu veranlassten sie bei der CVE Registrierungsstelle die Veröffentlichung der beiden CVE, sie lancierten eine eigene, offensiv gestaltete Web-Präsenz[25] und wandten sich an die Medien. Die darauf einsetzende Berichterstattung entwickelte sich schnell mit einer Art Tsunami-Effekt zu immer größerer Dramatik. Wurde zunächst noch zurückhaltend berichtet, ließ die nächste Publikation, die die Meldung aufnahm einige Details weg und steigerte die Dramatik noch etwas mehr. Im Endergebnis führt dies dazu, dass in nationalen Tageszeitungen[26] und Fernsehnachrichten[27] vom Ende der E-Mail-Sicherheit

[23] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17688
[24] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17689
[25] https://www.efail.de
[26] https://www.zeit.de/digital/datenschutz/2018-05/pgp-s-mime-e-mail-verschluesselung-sicherheitsluecke-technik
[27] https://www.tagesschau.de/inland/e-mail-verschluesselung-101.html

berichtet wurde. Zum einen wollten die beteiligten Sicherheitsforscher natürlich eine hinreichende Aufmerksamkeit für ihre langwierige Arbeit erzeugen. Zum anderen wurden aber auch die Medien Opfer eigener, widersprüchlicher Ziele; manche Sachverhalte wurden überspitzt dargestellt, um einerseits deutlich genug vor Problemen zu warnen, andererseits erschwert ein kompliziertes Themenfeld wie die Kryptographie die Recherche und schließlich benötigt jede Publikation Aufmerksamkeit.

Auch die Fachwelt ließ sich durch die spektakuläre Berichterstattung vereinzelt zu unüberlegten Reaktionen hinreißen. So stellte der Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in einem Interview die OpenPGP- und S/MIME-Verfahren zur Ende-zu-Ende Verschlüsselung als unsicher dar[28] und die Electronic Frontier Foundation (EFF) empfahl gar die E-Mail-Verschlüsselung ganz abzuschalten und entsprechende Produkte zu deinstallieren[29,30].

In der folgenden zum Großteil öffentlich geführten Debatte brachten sich weitere Sicherheitsexperten ein und es wurde schnell klar, dass die beiden CVE Meldungen irreführende Überschriften trugen, dass die Darstellungen auf der Webpräsenz der Entdecker Fehlinterpretationen offenbar billigend in Kauf nahmen und dass die mediale Berichterstattung vollends aus dem Ruder gelaufen war[31]. In Folge dessen sahen sich sowohl die Entdecker, als auch unüberlegt reagierende Experten wie die EFF und der BSI-Präsident heftiger Kritik aus Expertenkreisen ausgesetzt und gestanden Fehleinschätzungen und Darstellungsfehler ein. Aber auch die Szene der Sicherheitsexperten übte dahingehend Selbstkritik, dass keine Peer- oder Kontrollmechanismen existieren, um ein derart einfaches lancieren einer Panikkampagne zu verhindern[32].

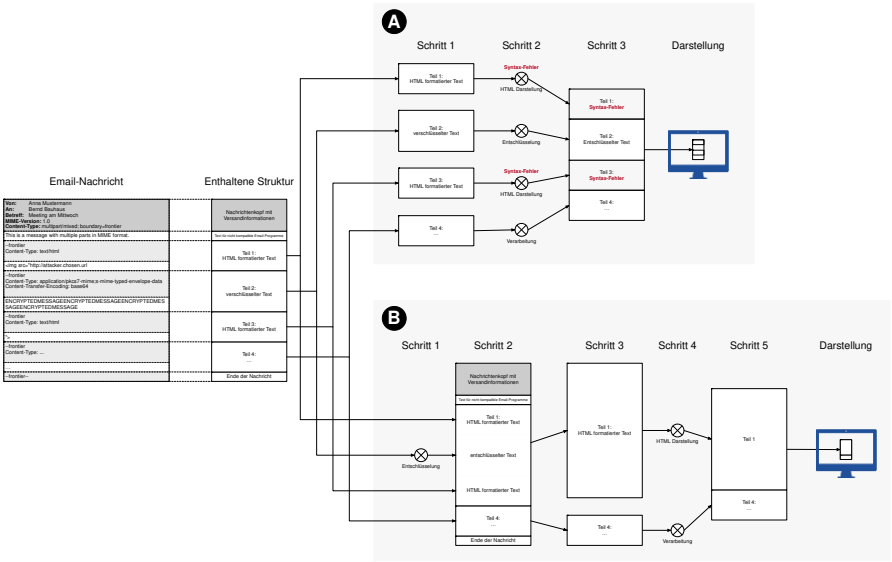
A5.2 Was tatsächlich entdeckt wurde

Im Gegensatz zur Darstellung in der Mehrheit der medialen Berichterstattung waren jedoch keine Schwachstellen in den OpenPGP- und S/MIME-Verfah-

---

[28] https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/efail-schwachstellen_15052018.html
[29] https://twitter.com/EFF/status/995906839958061056
[30] https://www.eff.org/deeplinks/2018/05/attention-pgp-users-new-vulnerabilities-require-you-take-action-now
[31] https://www.djv-bawue.de/2018/05/18/efail-investigative-journalisten-und-der-trend-zur-panikmache/
[32] https://medium.com/@cipherpunk/efail-a-postmortem-4bef2cea4c08

ren entdeckt worden, sondern in deren Einbindung in Software-Programmen, mit denen Anwender E-Mail-Nachrichten lesen und versenden, wie z.B. Microsoft Outlook.



Schematische Darstellung der Verarbeitung einer E-Mail die versucht die Efail-Verwundbarkeit auszunutzen

Die in der Abbildung auf der linke Seite gezeigte E-Mail-Nachricht verwendet das Multipurpose Internet Mail Extensions (MIME) Format, um den Inhalt der Nachricht in mehrere Teile unterteilen zu können und darin neben reinem Text auch Inhalte in anderen Formaten (z.B. HTML) und Anhänge übertragen zu können. Da einer der Teile verschlüsselten Text enthält, wird dies als Secure MIME (S/MIME) bezeichnet. Die in dieser böswilligen S/MIME Nachricht enthaltene Struktur ist ebenfalls auf der linken Seite dargestellt.

Im weiteren Verlauf sind zwei Varianten (in der Abbildung mit A bzw. B gekennzeichnet) für die Verarbeitung dieser Nachricht in einer E-Mail-Anwendung gezeigt. Der Unterschied zwischen beiden Varianten besteht darin, daß im Fall A zunächst die MIME-Struktur zerlegt und dann jeder Teil getrennt verarbeitet wird. Im Fall B werden dagegen zuerst verschlüsselte Bestandteile gesucht und entschlüsselt und erst anschließend die MIME-Struktur aufgelöst. Konzeptionell könnte man dies dahingehend zusammenfassen, dass in beiden Fällen die gleichen Verfahren angewandt werden (Entschlüsseln und MIME-Struktur auflösen), jedoch in jeweils umgekehrter Reihenfolge.

Die Verarbeitung im Fall A entspricht der konzeptionellen Schichtung der verschiedenen, bei dieser E-Mail-Nachricht verwendeten Verfahren. Auf unterster Ebene werden zunächst die einzelnen, enthaltenen MIME-Container identifiziert und separiert. Dies ist eine naheliegende Vorgehensweise, da die MIME-Container lediglich generische Transportbehälter darstellen. Die darin enthaltenen Inhalte sind daher von diesen Containern unabhängig und können jeder für sich alleine verarbeitet werden. Somit stellen die Containerinhalte die nächsthöhere Schicht dar. Die Verarbeitung im Fall A folgt also dieser logischen Schichtung und behandelt die Container als lose gekoppelte Objekte, deren einzige Verbindung darin besteht, dass sie gemeinsam auf dem Bildschirm dargestellt werden. Dies bedeutet praktisch, dass der Benutzer den entschlüsselten Text in jedem Fall angezeigt bekommt, dass die Darstellung der für sich jeweils strukturell unvollständigen HTML Container zu Fehlermeldungen führt und dass der entschlüsselte Text in keinem Fall in den Besitz des Angreifers gelangen kann.

Die Verarbeitung im Fall B weicht jedoch von dieser logischen Schichtung ab. Zunächst wird nach verschlüsselten Containern gesucht. Diese werden entschlüsselt und der entschlüsselte Text wird an Stelle des verschlüsselten Textes eingesetzt. Hierbei werden ebenfalls die Markierungen für Containergrenzen entfernt, da keine weitere Verarbeitung des betroffenen Containers mehr erforderlich ist. Dies führt dazu, dass (wie in der Abbildung gezeigt) ein ursprünglich verschlüsselter Container mit dem vorausgehenden und dem nachfolgenden Container zu einem einzigen verschmolzen wird ("aus drei mach eins"). Genau hier setzte der Efail-Angriff an, indem eine MIME-strukturierte E-Mail-Nachricht so gestaltet wurde, dass im Zuge einer Verarbeitung wie im Fall B ein verschlüsselter Text zunächst entschlüsselt und dann in einer für den Benutzer unsichtbaren Form in einem HTML-Dokument eingebettet wird. Weiter ist dieses HTML-Dokument so gestaltet, dass der entschlüsselte Text an einen vom Angreifer kontrollierten Webserver geschickt wird. Somit gelangt der Angreifer in den Besitz des unverschlüsselten Texts. Um sicher zu gehen, dass der zur Entschlüsselung erforderliche, geheime Schlüssel vorliegt, verwendet der Angreifer Text aus einer verschlüsselten Nachricht, die er vorher abgefangen hat. Diesen verpackt er dann in einer böswilligen E-Mail-Nachricht wie in der Abbildung gezeigt und sendet diese an den Absender des verschlüsselten Texts. Als Absender verfügt er mit Sicherheit über seinen eigenen, geheimen Schlüssel und kann den Text entschlüsseln.

Bei Efail handelt es sich also tatsächlich nicht um Schwachstellen in den OpenPGP- und S/MIME-Verfahren selbst, sondern vielmehr um Schwachstellen in einigen, weit verbreiteten E-Mail-Applikationen.

A5.3 Empfohlene Gegenmaßnahmen

Da alle großen Hersteller inzwischen Aktualisierungen herausgegeben haben, welche die Efail-Verwundbarkeit beheben, sollten Sie sicherstellen, dass ausschließlich die jeweils aktuellste Version der jeweiligen E-Mail-Applikation im Einsatz ist.

Da Efail die HTML-Darstellung in der E-Mail-Applikation sowie deren Fähigkeit Bestandteile von HTML-Nachrichten (z.B. Bilder und Graphiken) von externen Webservern nachzuladen ausnutzte, können Sie zudem noch konservative Einstellungen an Ihrer E-Mail-Applikation vornehmen, um das Verarbeiten von HTML, bzw. das Nachladen von Inhalten von externen Webservern zu unterbinden. Wie dies erfolgt unterscheidet sich von Applikation zu Applikation. Für einige, weit verbreitete E-Mail-Applikationen stehen Anleitungen im Web zur Verfügung[33,34]. Im Zweifelsfalle konsultieren Sie die Dokumentation Ihrer E-Mail-Applikation und wenden Sie sich an deren Anbieter. Da HTML-Inhalte in E-Mail-Nachrichten neben Efail oft auch zur Unterwanderung der Privatsphäre (z.B. zu werblichen Zwecken) eingesetzt werden, ist das Unterbinden der Verarbeitung von HTML, bzw. des Nachladens von Inhalten von externen Webservern in E-Mail-Applikationen, auch unabhängig von Efail, grundsätzlich empfehlenswert.

[33] https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/efail_schwachstellen.html
[34] https://www.condition-alpha.com/blog/?p=1538

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Experten, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Expertenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Vertrauenszeichens "IT Security made in Germany". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Kontakt:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Dr. Holger Mühlbauer
Geschäftsführer
Chausseestraße 17
10115 Berlin
Telefon: +49 30 4005 4306
E-Mail: holger.muehlbauer@teletrust.de
https://www.teletrust.de

TeleTrusT
Pioneers in IT security.


TeleTrusT
Pioneers in IT security.