D-TRUST
Ein Unternehmen der Bundesdruckerei

WHITEPAPER

Verschlüsseln und signieren.

Der Weg zu einer sicheren und vertrauenswürdigen E-Mail-Kommunikation

Inhalt

Management Summary

DATEN UND FAKTEN

100

Milliarden Euro

Schaden entstanden der deutschen Wirtschaft 2019 durch Cyberangriffe.

Quelle: Bitkom, Wirtschaftsschutz in der digitalen Welt, 2019, **www.bitkom.org**

56 %

der Anwender verwenden branchenübergreifend keine E-Mail-Verschlüsselung.

Quelle: REDDOXX-Studie, **E-Mail 2020**

Ransomware, Datendiebstahl oder ausspionierte Inhalte: Die E-Mail ist das größte Einfallstor für Cyberangriffe. Anhänge und Links in den E-Mails sind dabei die wichtigsten Türöffner für das Einschleusen von Schadprogrammen. Der Schaden für Industrie und Behörden ist groß, mit stark steigender Tendenz.

Neben wirtschaftlichen und finanziellen Nachteilen entstehen durch die Cyberangriffe auch juristische Probleme, teilweise große Imageschäden sowie Vertrauensverlust bei den Kunden.

Außerdem ist die Sicherheit der elektronischen Kommunikation zu einem zentralen Compliance-Faktor geworden. Sowohl die Datenschutz-Grundverordnung (DSGVO) als auch das IT-Sicherheitsgesetz (IT-SiG) fordern geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten und zu einer verbesserten IT-Sicherheit.

Die Absicherung der E-Mail-Kommunikation ist deshalb für Industrie und Behörden schon längst keine Kür mehr, sondern Pflicht. Aktuellen Umfragen zufolge verschlüsselt jedoch nur jeder achte Anwender regelmäßig seine E-Mails, in öffentlichen Verwaltungen sogar nur jeder zwölfte Mitarbeiter.

Dabei existieren etablierte technische Verfahren und Programme sowie klar definierte Standards. Das Verschlüsseln der E-Mails stellt die Vertraulichkeit der elektronischen Kommunikation sicher. Hierbei ist wichtig, dass die E-Mails mittels TLS-Technologie nicht nur auf dem Transportweg zwischen zwei Servern geschützt sind, sondern dass die Inhalte komplett verschlüsselt werden. Diese Inhaltsverschlüsselung basiert auf einem sogenannten asymmetrischen Verschlüsselungsverfahren mit zwei sich ergänzenden Schlüsseln.

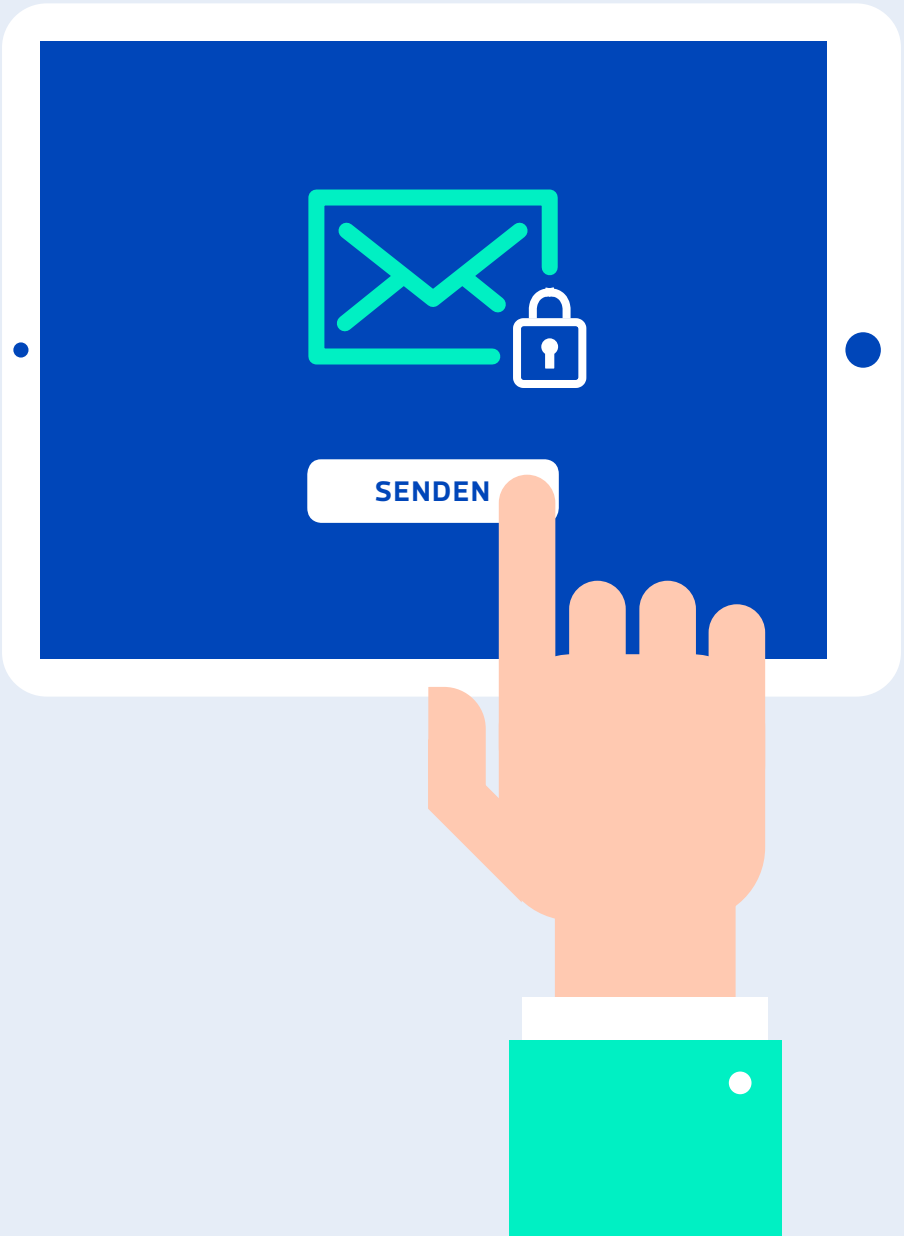
Die E-Mail-Signatur schützt die Inhalte vor Manipulationen und weist eindeutig auf die Identität des Absenders hin. Das Signieren der E-Mails reicht für viele Anwendungsfälle aus. Verschlüsselungsverfahren kommen dann zum Einsatz, wenn eine vertrauliche E-Mail-Kommunikation sichergestellt werden muss.

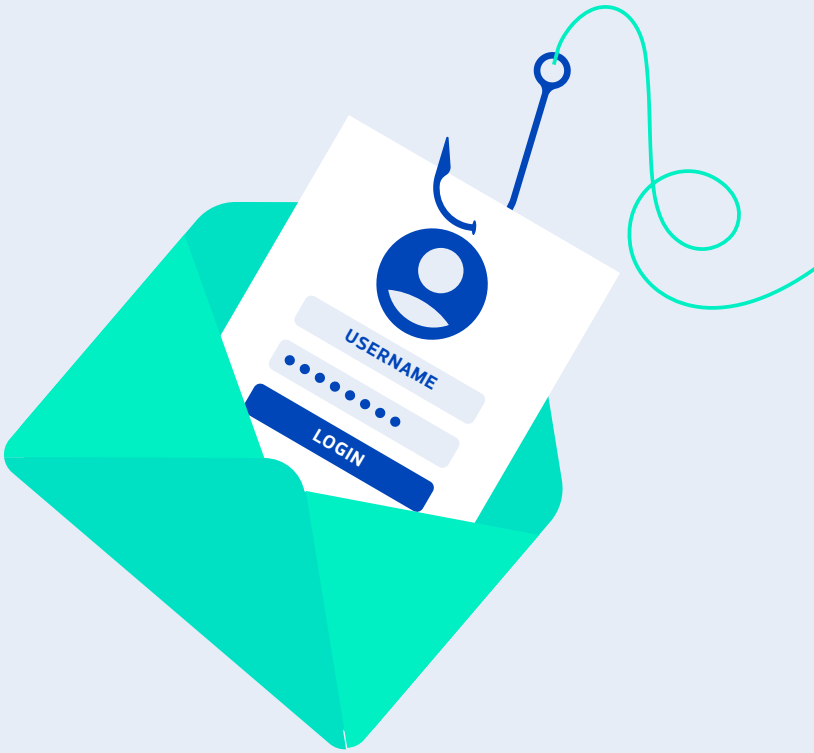
Am weitesten verbreitet sind serverseitige Verschlüsselungslösungen, die an zentraler Stelle des Unternehmensnetzwerks eingerichtet sind. Auf diesen E-Mail-Gateways laufen alle wichtigen Funktionen automatisiert ab – wie das Verschlüsseln, Entschlüsseln und elektronische Signieren. Das erleichtert die Handhabung sowie den Implementierungs- und Administrationsaufwand.

Kombiniert werden können Gateway-Lösungen mit clientbasierten Verschlüsselungsverfahren. Dabei werden die E-Mails vom Client des Absenders bis zum Client des Empfängers durchgehend verschlüsselt (End-to-End). Dafür muss jedoch auf jedem Rechner ein E-Mail-Programm installiert sein. Der Bedienungsaufwand ist dabei deutlich höher.

Um die Identität der E-Mail-Anwender eindeutig zu verifizieren, sind digitale Zertifikate notwendig. Das digitale Zertifikat enthält außer der kryptografischen Komponente für die Verschlüsselung auch die Identitätsinformationen des Anwenders. Zusätzlich zu Zertifikaten, die auf eine Person ausgestellt sind, gibt es auch sogenannte Team-IDs, die Angaben zu einer Organisation oder Abteilung enthalten. Diese dienen dem Absichern von Gruppenpostfächern.

Digitale Zertifikate müssen ausgestellt, verteilt, geprüft und verwaltet werden. Das für diese Aufgabe zuständige Sicherheitssystem wird als Public-Key-Infrastruktur (PKI) bezeichnet. Mit vielfältigen Dienstleistungen erleichtern externe Vertrauensdienstean-bieter den Aufbau und Erhalt einer PKI. Cloud-Lösungen, wie eine „Managed PKI", können dabei für ein effizientes Zertifikatsmanagement eingesetzt werden.





Warum E-Mails verschlüsseln und signieren so wichtig ist: zwei Fallbeispiele

E-Mail für Datenspionage eingesetzt

Der Datendiebstahl bei einem mittelständischen Energieerzeuger begann mit einer harmlos erscheinenden E-Mail: Dort richtete der als Mitarbeiter getarnte Cyberkriminelle eine Rückfrage gleich an mehrere „Kollegen". Diese gaben ihm die benötigten Informationen ahnungslos weiter.

Und nicht nur das: An ausgewählte Mitarbeiter wurde eine zweite E-Mail mit einer angehängten Excel-Datei geschickt. Es genügte der Klick nur eines Empfängers auf die Datei und schon nahm der Datendiebstahl seinen Lauf.

E-Mail mit Schadprogramm bringt Stadtverwaltung zum Stillstand

Der Anhang einer E-Mail genügte, um die Verwaltung einer mittelgroßen deutschen Stadt komplett lahmzulegen. Die Datei enthielt ein Schadprogramm, sogenannte Ransomware, die Tausende von Verwaltungsdaten verschlüsselte und somit unbrauchbar machte.

Zusätzlich konnte die Schadsoftware die E-Mail-Kommunikation auslesen, um die dort enthaltenen Informationen für weitere Angriffe zu nutzen.

Für die Entschlüsselung der Dateien musste ein stattliches Lösegeld gezahlt werden. Eine elektronische Kommunikation war nicht mehr möglich, Bauprojekte kamen wegen verschlüsselter Baupläne zum Stillstand und Sozialleistungen ließen sich nicht mehr auszahlen.

1 Einleitung

DATEN UND FAKTEN

8,5 %

der Verwaltungsmitarbeiter in Behörden verschlüsseln regelmäßig ihre E-Mails.

Quelle: REDDOXX-Studie, **E-Mail 2020**

Beide Fallbeispiele zeigen, wie wichtig eine sichere und vertrauenswürdige elektronische Kommunikation für die IT-Sicherheit und den Datenschutz ist.

Und damit ist nicht nur der Einsatz von Virenscanner, Spamschutz und Firewalls gemeint. Mit diesen Maßnahmen wird nur ein Teil der potenziellen Gefahren abgewehrt, viele jedoch nicht. Um das Vortäuschen eines falschen Absenders, das Mitlesen von E-Mails und einen Vertraulichkeitsverlust schützenswerter Informationen zu verhindern, sind zusätzliche Maßnahmen zur Verschlüsselung von E-Mails erforderlich.

Ein technisch ausgereiftes Verfahren zum Schutz der elektronischen Kommunikation ist die **E-Mail-Verschlüsselung.** Bei der Verschlüsselung wird eine lesbare Information (Klartext) in ihr unleserliches Pendant (Geheimtext) umgewandelt. Nur mit Hilfe eines passenden Schlüssels kann der Geheimtext wieder lesbar gemacht werden.

Eine weitere wichtige Schutzmaßnahme ist die E-Mail-Signatur. Sie weist eindeutig auf die Identität des Absenders (Authentizität) hin und schützt die E-Mail samt Anhang vor unerwünschten Manipulationen (Integrität).

Beide Verfahren können miteinander kombiniert werden, sind aber auch unabhängig voneinander einsetzbar.

Der großen Bedeutung der beiden Techniken steht eine geringe Verbreitung in der Praxis gegenüber. In einer aktuellen Umfrage des Security-Anbieters REDDOXX gaben **56 Prozent der Befragten branchenübergreifend an, nie eine E-Mail-Verschlüsselung** zu verwenden. **Nur jeder achte Anwender verschlüsselt seine E-Mails.**

In Behörden ist das Sicherheitsbewusstsein sogar noch geringer. **Lediglich 8,5 Prozent der Verwaltungsmitarbeiter verschlüsseln regelmäßig ihre E-Mails, 58 Prozent dagegen nie.**

Wer nach Gründen für diese Ergebnisse sucht, stößt auf fünf zentrale Mythen (siehe links). Diese fünf Mythen ziehen sich wie ein roter Faden durch das vorliegende White Paper, das sich sowohl an Unternehmen als auch an öffentliche Verwaltungen richtet.

Es beschäftigt sich zunächst mit der aktuellen Bedrohungslage durch Cyberangriffe, wichtigen rechtlichen Vorgaben für eine Verschlüsselungspflicht und den Schutzzielen der E-Mail-Verschlüsselung.

Der zweite große inhaltliche Block skizziert die technischen Verfahren und Standards wie die asymmetrische Verschlüsselung, den Unterschied zwischen client- sowie serverbasierter Verschlüsselung, die Bedeutung von Zertifikaten und einer Public-Key-Infrastruktur (PKI) und warum das digitale Signieren von E-Mails notwendig ist.

Der dritte Teil des White Papers gibt konkrete Handlungsempfehlungen, wie sich E-Mail-Verschlüsselung und E-Mail-Signatur Schritt für Schritt in der Praxis umsetzen lassen.

KURZ UND BÜNDIG

5

zentrale Mythen der E-Mail-Verschlüsselung

„Meine Daten sind für andere nicht interessant."

„E-Mail-Verschlüsselung ist für mich nicht verpflichtend."

„Natürlich verschlüsseln wir – mit TLS/SSL."

„Sicherheitsbehörden können ja sowieso mitlesen."

„Verschlüsseln und Signieren ist zu kompliziert."

2 Bedrohungslage, rechtliche Vorgaben und Schutzlage

2.1 Bedrohungen durch Cyberangriffe wachsen

Mythos 1: „Daten sind für andere nicht interessant."

Unternehmen und Verwaltungen sehen sich steigenden Bedrohungen durch Cyberangriffe ausgesetzt. **46 Prozent** der mittelständischen Unternehmen in Deutschland sind in der Vergangenheit schon einmal Opfer von Lösegelderpressung, digitaler Wirtschaftsspionage oder Datendiebstahl geworden.

Den Gesamtschaden für die deutsche Wirtschaft bezifferte der IT-Fachverband Bitkom **in einer aktuellen Studie auf über 100 Milliarden Euro pro Jahr**, Tendenz stark steigend.[1]

Immer mehr öffentliche Verwaltungen geraten zudem ins Visier der Cyberkriminellen. Laut einer Studie des Security-Software-Anbieters Kaspersky sind Ransomware-Angriffe auf kommunale Einrichtungen 2019 weltweit um 60 Prozent gestiegen. Dabei forderten die Kriminellen von 174 kommunalen Stellen Lösegeld in Höhe von insgesamt 14 Millionen Euro. Hauptzielmarkt war mit fast 9 Prozent der Fälle Deutschland.[2]

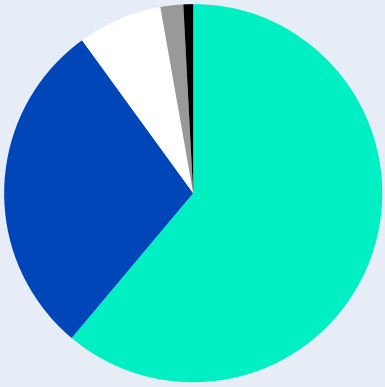
DATEN UND FAKTEN

46 %

der mittelständischen Unternehmen in Deutschland waren schon Opfer von Cyberangriffen.

Quelle: **DsiN-Praxisreport 2020 Mittelstand @ IT-Sicherheit**

Ransomware-Angriffe gegen städtische Einrichtungen 2019 (174 Kommunen)



Betroffene Systeme

- **61 %** Schulen
- **29 %** Rathäuser
- **7 %** Medizinische Einrichtungen
- **2 %** Versorgungsdienste
- **1 %** Sonstige

$ 15.663.200 – Summe öffentlich kommunizierter Lösegeldforderungen

$ 5.000–5.300.000 – Höhe der Lösegeldforderungen

$ 1.032.460 – Durchschnittliche Lösegeldforderungen

1 Bitkom: Wirtschaftsschutz in der digitalen Welt, 2019 **www.bitkom.org**

2 Kaspersky Security Bulletin: Cities under ransomware siege, 2019 **www.securelist.com**

2.2 E-Mail-Kommunikation als Achillesferse der Cybersicherheit

Mythos 1: „Meine Daten sind für andere nicht interessant."

DATEN UND FAKTEN

850

Milliarden E-Mails

werden pro Jahr in Deutschland versendet.

Quelle: REDDOXX-Studie, **E-Mail 2020**

Eines der wichtigsten Einfallstore für Cyberangriffe sind E-Mails, die im beruflichen Umfeld das Kommunikationsmittel Nummer eins sind. Pro Jahr werden in Deutschland rund 850 Milliarden E-Mails versendet, das entspricht über 2 Milliarden E-Mails pro Tag. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt in seinem Bericht zur Gefährdungslage 2020 fest, dass Schadprogramme in der Regel über Anhänge oder Links in den E-Mails in die IT-Systeme der Unternehmen gelangen.[3]

Mit Methoden des Social Engineerings gelingt es den Angreifern, viele Mitarbeiter zu Klicks auf schädliche E-Mails zu verleiten. Dabei werden vertraute Absendernamen oder interessante Neuigkeiten zu einem aktuellen Thema genutzt. Sehr verbreitet sind auch berufliche Zwänge, beispielsweise wenn die E-Mail vermeintlich von einem Vorgesetzten stammt oder ein Teil der beruflichen Tätigkeit ist – wie zum Beispiel das Öffnen eines Bewerbungsschreibens.

Sicherheitsaspekte sollten deshalb im Umgang mit E-Mails eine zentrale Rolle spielen. Das gilt sowohl für die Privatwirtschaft als auch für Behörden. Dort hat die sichere und vertrauliche Kommunikation innerhalb der Verwaltung und mit den Bürgern eine große Bedeutung. Sensible personenbezogene Inhalte zu Personalausweisen, Anträge für Sozialleistungen oder Meldebescheinigungen müssen sicher kommuniziert und verarbeitet sowie optimal vor Diebstahl geschützt werden. Gleichzeitig ist zu verhindern, dass über E-Mails Schadprogramme in die IT-Systeme von Bund, Ländern und Kommunen gelangen.

GUT ZU WISSEN

E-Mail-Kommunikation in Behörden: fünf Gründe für einen besseren Schutz

1. Sensible, personenbezogene Daten dürfen nicht in die Hände von Cyberkriminellen fallen.
2. Wichtige Digitalisierungsprojekte wie das Onlinezugangsgesetz setzen eine vertrauenswürdige elektronische Kommunikation voraus.
3. Eine abgesicherte Kommunikation stärkt das Vertrauensverhältnis zwischen Behörden und Bürgern.
4. Die Widerstandsfähigkeit der IT-Systeme wird erheblich erhöht.
5. Das Risiko einer Infektion mit Schadprogrammen lässt sich deutlich verringern.

3 Bundesamt für Sicherheit in der Informationstechnik (BSI): **Die Lage der IT-Sicherheit in Deutschland 2020**

2.3 Compliance fordert E-Mail-Verschlüsselung

Mythos 2: „E-Mail-Verschlüsselung ist für mich nicht verpflichtend."

Aktuelle gesetzliche Vorgaben machen es dringend erforderlich, sich mit der Sicherheit der eigenen elektronischen Kommunikation auseinanderzusetzen.

Ziel der **Datenschutz-Grundverordnung (DSGVO)** ist der Schutz personenbezogener Daten europäischer Bürger. Dafür sind entsprechende technische und organisatorische Maßnahmen zu treffen, die dem „Stand der Technik" entsprechen.

Ausdrücklich wird die Verschlüsselung personenbezogener Daten als eine der Schutzmaßnahmen genannt.[4] Bedeutet: **Wer seine E-Mails verschlüsselt, hat bereits einen wichtigen Teil der DSGVO erfüllt.**

Dabei bietet die E-Mail-Verschlüsselung im Rahmen der DSGVO einen weiteren Vorteil: Sind personenbezogene Daten verschlüsselt, entfällt die Pflicht, Datenschutzverletzungen innerhalb von 72 Stunden den betroffenen Personen zu melden.

Technisch-organisatorische Maßnahmen nach dem Stand der Technik fordert auch das **IT-Sicherheitsgesetz (IT-SiG).** Ziel des Gesetzes ist die Verbesserung der IT-Sicherheit von Betreibern sogenannter Kritischer Infrastrukturen (KRITIS). Dies sind Organisationen mit wichtiger Bedeutung für das Funktionieren des staatlichen Gemeinwesens wie zum Beispiel Wasserwerke, Energielieferanten, Telekommunikationsdienstleister, Gesundheitseinrichtungen, Transport- und Verkehrsunternehmen.

Der Geltungsbereich des IT-Sicherheitsgesetzes wird kontinuierlich ausgeweitet. So wurden die Betreiber Kritischer Infrastrukturen um den Sektor Abfallwirtschaft erweitert. Zusätzlich fallen unter den Anwendungsbereich des Gesetzes jetzt auch „Unternehmen im besonderen öffentlichen Interesse". Darunter fallen Unternehmen, die nach Ansicht des Gesetzgebers von „erheblicher volkswirtschaftlicher Bedeutung für die Bundesrepublik Deutschland sind oder die für solche Unternehmen als Zulieferer wegen ihrer Alleinstellungsmerkmale von wesentlicher Bedeutung sind" (§ 2 Abs. 14 Nr. 2).[5]

Wer E-Mails nicht verschlüsselt, riskiert, dass personenbezogene Daten in falsche Hände geraten und die IT-Sicherheit erheblich eingeschränkt wird. Dies kann gemäß der vorgestellten gesetzlichen Vorgaben hohe Bußgelder und Strafzahlungen zur Folge haben. DSGVO und IT-SiG sehen bei Gesetzesverstößen Sanktionen in Höhe von bis zu 20 Millionen Euro oder 4 Prozent des weltweiten Jahresumsatzes vor.

4 Art. 32 DSGVO: **Sicherheit der Verarbeitung**

5 Gute Zusammenfassung der wichtigsten Neuerungen des IT-Sicherheitsgesetzes: **Bundesamts für Sicherheit in der Informationstechnik (BSI)**

2.4 Schutzziele der E-Mail-Verschlüsselung und E-Mail-Signatur

Die Ziele der E-Mail-Verschlüsselung orientieren sich an den zentralen Prinzipien der Informationssicherheit: Authentizität, Integrität, Vertraulichkeit und Verbindlichkeit.

Die **Authentizität** einer E-Mail ist dann gegeben, wenn die Nachricht tatsächlich vom angegebenen Absender stammt. Der Absender ist somit eindeutig identifizierbar, seine Urheberschaft nachprüfbar.

Die **Integrität** einer E-Mail meint die Gewissheit, dass ihr Inhalt nachweislich vollständig und unverändert ist.

Schutzmaßnahmen zur **Vertraulichkeit** einer E-Mail stellen sicher, dass nur dazu berechtigte Personen in der Lage sind, die Nachricht zu lesen, mit der E-Mail verschickte Daten einzusehen oder Informationen über den Inhalt der E-Mail zu erlangen.

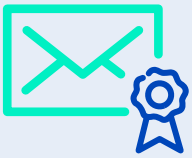
Die Verbindlichkeit einer E-Mail verhindert, dass der Urheber der Daten oder der Absender einer Nachricht seine Urheberschaft bestreiten kann. Gegenüber Dritten sollte diese eindeutig nachweisbar sein.

GUT ZU WISSEN

Welche Ziele hat der Schutz von E-Mail-Verschlüsselung und E-Mail-Signatur?

Vertraulichkeit

Der Inhalt von E-Mails kann nur von berechtigten Personen gelesen werden.



Authentizität und Verbindlichkeit

Die Nachricht stammt tatsächlich vom angegebenen Absender.

Integrität

Der Inhalt von E-Mails ist vollständig und unverändert.

3 Technische Verfahren und Standards

Die Bedrohungslage ist eindeutig und die rechtlichen Aspekte sprechen klar für eine Verschlüsselung der E-Mail-Kommunikation. Bevor es an die praktische Umsetzung geht, ist es ratsam, sich über einige Grundlagen der Verschlüsselungstechnik zu informieren. Die wichtigsten Fragen ergeben sich aus den genannten Schutzzielen.

Mit welchen technischen Verfahren und Standards lässt sich am besten sicherstellen, dass die Nachricht nicht von Unbefugten gelesen werden kann, dass der Absender wirklich die Person ist, als die er sich ausgibt, und dass die Nachricht auf dem Weg zum Empfänger nicht verändert wurde?

3.1 Schutz der Vertraulichkeit

Transportverschlüsselung (TLS/SSL) – sicher bei der Übertragung

Mythos 3: „Natürlich verschlüsseln wir – mit TLS/SSL."

Bei der Transportverschlüsselung werden die E-Mails durch einen verschlüsselten Kanal verschickt. Das bedeutet: Nur auf dem Transportweg zwischen zwei Servern besteht der Schutz durch Verschlüsselung. Beim Absender und Empfänger sowie auf dazwischenliegenden Knoten liegen die E-Mails in unverschlüsselter Form vor.

Bei der Transportverschlüsselung kommt die TLS-Technologie zum Einsatz. Transport Layer Security (TLS), früher bekannt als Secure Sockets Layer (SSL), ist ein Standardprotokoll zur Verschlüsselung von Datenübertragungen im Internet.

Die Transportverschlüsselung bietet einen Basisschutz und gilt als Mindestanforderung, um die gesetzlichen Vorgaben an die IT-Sicherheit und den Datenschutz zu erfüllen.[6]

Sie wird in vielen Fällen mit einer Inhaltsverschlüsselung kombiniert. Bei dieser werden die Inhalte der E-Mails komplett verschlüsselt. Damit sind die E-Mails nicht nur auf dem Transportweg, sondern auch beim Absender und beim Empfänger geschützt.

6 Einschätzung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder: **Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail**

Asymmetrische Inhaltsverschlüsselung

Mythos 4: „Sicherheitsbehörden können ja sowieso mitlesen."

Im geschäftlichen Umfeld haben sich asymmetrische Verfahren als Standard für die E-Mail-Verschlüsselung etabliert. Dabei gibt es immer zwei sich ergänzende Schlüssel:

- den öffentlichen Schlüssel des Empfängers (Public Key) für das Verschlüsseln der Nachricht sowie
- den privaten Schlüssel des Empfängers (Private Key) für das Entschlüsseln der Nachricht.

Beide Schlüssel stehen in einer bestimmten mathematischen Abhängigkeit zueinander. Mit Hilfe kryptografischer Verfahren ist der private Schlüssel durch die Kenntnis des öffentlichen Schlüssels nicht errechenbar. Dadurch bleibt der Inhalt vertraulich und kann nicht gelesen werden. **Das Schutzziel der Vertraulichkeit ist erreicht!**

Der Absender verschlüsselt die E-Mails mit dem öffentlichen Schlüssel des Empfängers. Dieser ist, wie der Name sagt, öffentlich zugänglich, beispielsweise auf im Internet zugänglichen Schlüsselservern. Die Entschlüsselung erfolgt dann mit dem privaten Schlüssel des Empfängers, den nur dieser kennt.

Gut vorstellen lässt sich die asymmetrische Verschlüsselung mit öffentlichem (Public Key) und privatem Schlüssel (Private Key), wenn man an einen gesicherten Briefkasten denkt. Jeder kann dort für den Besitzer des Briefkastens etwas hinterlegen, ohne dass andere Zugriff darauf haben. Zum Öffnen des Briefkastens ist allerdings der private Schlüssel des Adressaten notwendig. Der öffentliche Schlüssel entspricht dann dem Briefkastenschlitz, in den jeder Post einwerfen kann. Weil aber nur der Empfänger über den geheimen, privaten Schlüssel verfügt, kann nur er den Briefkasten öffnen und die Post entnehmen beziehungsweise die Nachricht lesen.

Sie wird in vielen Fällen mit einer Inhaltsverschlüsselung kombiniert. Bei dieser werden die Inhalte der E-Mails komplett verschlüsselt. Damit sind die E-Mails nicht nur auf dem Transportweg, sondern auch beim Absender und beim Empfänger geschützt.

Client- und serverbasierte Verschlüsselungslösungen

Die technische Umsetzung der asymmetrischen Verschlüsselung erfolgt entweder über clientbasierte oder serverbasierte Verschlüsselungslösungen.

Bei ersterer ist die **E-Mail vom Client des Absenders bis zum Client des Empfängers durchgehend verschlüsselt.** Dafür ist jeder Rechner mit einem sicheren E-Mail-Client ausgestattet, der kryptografische Funktionen beherrschen muss.

Serverseitige Verschlüsselungslösungen sind an zentraler Stelle des Unternehmensnetzwerks implementiert. Sie können wahlweise auf einen vorhandenen E-Mail-Server aufgesetzt werden oder als eigenständiger Server laufen. Auf diesen **E-Mail-Gateways** finden sämtliche kryptografische Funktionen statt – wie das Verschlüsseln, Entschlüsseln und elektronische Unterschreiben (inklusive Signaturprüfung).

Die Gateways nehmen Mitarbeitern beziehungsweise individuell definierten Nutzergruppen alle relevanten kryptografischen Vorgänge automatisiert ab. Ausgehende E-Mails werden dabei im E-Mail-Client oder auf dem Mailbox-Server erstellt und versendet. Dieser leitet die E-Mail an das Verschlüsselungs-Gateway, wo die Nachricht verschlüsselt und signiert wird. Nach Prüfung der E-Mail samt Anhang durch einen Virenscanner erfolgt das Zustellen der elektronischen Nachricht an den Empfänger.

Umgekehrt nimmt die Anti-Virus-Software eingehende verschlüsselte und signierte E-Mails entgegen und prüft diese auf Schadsoftware. Danach werden die E-Mails an das Verschlüsselungs-Gateway weitergeleitet, das die elektronischen Nachrichten entschlüsselt, die Signatur überprüft und am Ende einem E-Mail-Client oder Mailbox-Server zustellt.

GUT ZU WISSEN

Orientierungshilfe zur E-Mail-Verschlüsselung

Von der Konferenz der unabhängigen Datenschutzbehörden gibt es eine aktuelle Orientierungshilfe über „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“.[7] Das im Internet frei erhältliche Dokument informiert Unternehmen und Behörden über die sich aus der DSGVO ergebenden Vorgaben im Hinblick auf die E-Mail-Kommunikation. Dabei werden die Verpflichtungen bei den unterschiedlichen Risiken besprochen sowie die Anforderungen an die eingesetzten Verschlüsselungs- und Signaturverfahren detailliert beschrieben.

7 Einschätzung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder: **Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail**

3.2 Schutz der Authentizität und Integrität

Zertifikate und PKI

Die asymmetrische Verschlüsselung von E-Mails erfüllt das Schutzziel der Vertraulichkeit. Sie erhöht aber nur dann die Sicherheit und den Datenschutz, wenn sie mit den Zielen der Authentizität und Integrität verknüpft ist.

Damit wird auch bei asymmetrischen Verschlüsselungsverfahren das Problem des „Man in the Middle" gelöst. Der Begriff weist darauf hin, dass es im Internet oft leicht ist, sich für jemand anderen auszugeben. Für die falsche Identität ließen sich problemlos Schlüsselpaare generieren und Public Keys in Umlauf bringen. Auf diese Weise wäre es für den Fälscher möglich, vertrauliche Botschaften zu lesen.

Wie kann der Absender, der den öffentlichen Schlüssel des Empfängers zum Verschlüsseln nutzt, sicher sein, dass dieser auch wirklich dem Empfänger gehört?

Die Antwort auf diese Frage und die Lösung für die beschriebene „Man in the Middle"-Problematik ist das **Modell der Public-Key-Infrastruktur (PKI).** Bei diesem werden asymmetrische Schlüsselpaare den jeweiligen Identitäten zugeordnet. Dies erfolgt in Form von digitalen Zertifikaten. Der öffentliche Schlüssel (Public Key) ist in der Regel in ein digitales Zertifikat integriert. Dort sind ferner die Identitätsinformationen zum Inhaber (zum Beispiel Name und E-Mail-Adresse) gespeichert und die Kombination aus öffentlichem Schlüssel und Identität ist durch einen Dritten beglaubigt.

AUF DEN PUNKT GEBRACHT

Public-Key-Infrastrukturen (PKI) sind Sicherheitssysteme zum Ausstellen, Verteilen und Prüfen digitaler Zertifikate. Sie erlauben eine sichere Kommunikation innerhalb unsicherer Netzwerke.

Bei der E-Mail-Verschlüsselung haben sich **zwei Standardformate etabliert: S/MIME (Secure/Multipurpose Internet Mail Extensions) und OpenPGP (Pretty Good Privacy).** Beide sind nicht miteinander kompatibel. Anwender müssen sich daher für das eine oder das andere Standardformat entscheiden, um verschlüsselte Nachrichten untereinander austauschen zu können.

Der **S/MIME-Standard kommt überwiegend in Unternehmen und im Behördensektor zum Einsatz,** während OpenPGP im privaten Bereich und im akademischen Umfeld eine große Verbreitung hat. Die beiden Standards unterscheiden sich in der Art und Weise, wie die Authentizität der öffentlichen Schlüssel verlässlich bestätigt wird.

OpenPGP sieht vor, dass sich die Teilnehmer untereinander ihre öffentlichen Schlüssel zertifizieren. Dadurch entsteht ein „Web of Trust" (WOT), ein Netzwerk des Vertrauens, das ohne Hierarchien auskommt. Bei dieser Variante müssen die Benutzer selbst besondere Maßnahmen zur Erreichung einer hohen Vertrauenswürdigkeit treffen. Zudem muss bei der Generierung der Schlüssel darauf geachtet werden, dass es zu keiner Kompromittierung durch Angreifer kommen kann.

Bei **S/SMIME** dagegen findet die Zertifizierung der öffentlichen Schlüssel durch eine hierarchische Kette von Zertifizierungsinstanzen statt. Das letzte Glied einer solchen Kette wird als Wurzel-Zertifizierungsstelle bezeichnet. Dabei übernehmen **sogenannte Vertrauensdiensteanbieter (VDA) die Rolle der vertrauenswürdigen Instanz.**

VDA unterliegen strengen gesetzlichen Regelungen, müssen eine breite Palette an Sicherheitsanforderungen erfüllen und stehen unter der Aufsicht der Bundesnetzagentur. Sie geben die individuellen Schlüsselpaare heraus, verknüpfen sie mit der Identität einer Person und halten diese Daten dauerhaft zur Verfügung.

In gängigen Betriebssystemen und E-Mail-Programmen sind die Wurzelzertifikate (Root Certificates) des Vertrauensdiensteanbieters hinterlegt. Damit werden die S/MIME-Zertifikate des VDA ordnungsgemäß angezeigt, sodass Vertrauenswürdigkeit entstehen kann.

AUF DEN PUNKT GEBRACHT

Vertrauensdiensteanbieter sind die Vertrauensanker innerhalb der digitalen Welt. Im komplexen Zusammenspiel von Zertifikaten und elektronischen Schlüsseln sind sie die Instanz, die für Zuverlässigkeit und Sicherheit sorgt.

E-Mail-Signatur

Personenzertifikate sind die Voraussetzung dafür, eine E-Mail zu signieren. Was bedeutet das konkret? Zunächst müssen zwei Missverständnisse ausgeräumt werden. Erstens ist die E-Mail-Signatur keine Unterschrift, mit der eine Willenserklärung zum Ausdruck gebracht wird und die dann zum Beispiel auch archivierbar wäre. E-Mail-Signaturen dürfen zweitens nicht mit der Signatur verwechselt werden, die sich in E-Mail-Programmen am Ende eines E-Mail-Textes festlegen lässt – meistens die Kontaktinformationen des Absenders.

Die E-Mail-Signatur schützt die Inhalte vor Manipulationen und ermöglicht es, die Identität des Absenders eindeutig zu verifizieren. **Dadurch werden die Schutzziele der Authentizität und Integrität erfüllt.**

Technisch funktioniert die E-Mail-Signatur mit asymmetrischer Verschlüsselung wie folgt:

- Um eine Signatur zu erzeugen, wird zunächst aus den in der Nachricht enthaltenen Informationen eine Prüfsumme fester Länge, der sogenannte Hash-Wert, gebildet. Bei unverändertem Inhalt des Dokuments führt die Hash-Berechnung immer zum selben Ergebnis.
- Der Unterzeichner verschlüsselt dann mit seinem privaten Schlüssel den Hash-Wert und verbindet diesen mit dem Zertifikat des Unterschreibenden sowie dem Ursprungsdokument. Alle bilden gemeinsam das elektronisch unterschriebene Dokument.
- Beim Empfänger angekommen, wird über den im Zertifikat mitgelieferten öffentlichen Schlüssel der verschlüsselte Hash-Wert entschlüsselt. Unabhängig davon wird aus dem elektronischen Ursprungsdokument der Hash-Wert der vorliegenden Datei berechnet. Stimmen die beiden Hash-Werte überein, ist das vorliegende Dokument unverfälscht.
- Die Authentizität des Urhebers wird mit demselben Mechanismus verifiziert, indem die elektronische Signatur des Zertifikats geprüft wird.

GUT ZU WISSEN

Hash-Werte

Hash-Werte sind kryptografische Zusammenfassungen von beliebigen Inhalten. Sie stellen eine eindeutige Zeichenfolge aus Zahlen und Buchstaben dar, die aus dem Inhalt einer Datei berechnet werden. Eine Rekonstruktion des ursprünglichen Inhalts aus dem Hash-Wert ist nicht möglich. Man kann jedoch anhand des Hash-Werts vergleichen, ob zwei Dateien identisch sind. Damit ist ein Hash-Wert vergleichbar mit einem Fingerabdruck – nur eben für eine Datei, nicht für einen Finger.

4 Handlungsempfehlungen

E-Mail-Verschlüsselung und E-Mail-Signatur können auf eine solide technische und rechtliche Grundlage bauen. Die Verfahren sind ausgereift, die Standards sind klar definiert und unabhängige Instanzen in Form der Vertrauensdiensteanbieter (VDA) sorgen für Sicherheit und Vertrauenswürdigkeit.

Darüber hinaus gibt es eine Vielzahl von Software-Programmen und Beratungsleistungen, die bei der E-Mail-Verschlüsselung unterstützen.

Die folgende Schritt-für-Schritt-Anleitung soll wichtige Praxiskenntnisse rund um die E-Mail-Verschlüsselung vermitteln und Hemmnisse abbauen.

Schritt 1 Bedarfsanalyse und Konzeptentwicklung

In einem ersten Schritt gilt es, in der Organisation Bewusstsein zu schaffen, Ziele zu definieren und ein Konzept für die Umsetzung zu erstellen.

In einem Basis-Workshop erhalten Mitarbeiter eine Einführung in die Thematik, bekommen Basiswissen zu unterschiedlichen Verschlüsselungsverfahren vermittelt und verschaffen sich einen Überblick über die wichtigsten technischen Lösungen.

Während der Bedarfsanalyse werden die Prozesse identifiziert, die für eine E-Mail-Verschlüsselung entscheidend sind. Dazu gehört auch die Bestimmung der entscheidenden 5 bis 10 Prozent der Daten, die zu den Kronjuwelen eines Unternehmens gehören. Für diese sind Verschlüsselungsverfahren auf höchstem Sicherheitsniveau zu wählen.

Ob die E-Mail-Verschlüsselung in Kombination mit der E-Mail-Signatur oder unabhängig von dieser eingesetzt werden soll, ist eine weitere wichtige Frage. Bei der E-Mail-Signatur geht es darum, den Absender und die Integrität der Nachricht zu verifizieren. Die Identität des Absenders lässt sich eindeutig bestimmen, und die Mail ist vor Manipulation geschützt. Sie bleibt aber lesbar. Für viele Anwendungsfälle mag die E-Mail-Signatur genügen. Geht es jedoch darum, eine vertrauliche E-Mail-Kommunikation sicherzustellen, ist das Verschlüsseln Pflicht.

Auf der Basis konkreter Anwendungsfälle erfolgt die Formulierung der Zielsetzung, die Definition geeigneter Verschlüsselungsverfahren und damit zusammenhängend die Auswahl von Software und benötigten Dienstleistungen.

All diese Erkenntnisse finden dann Einzug in ein ganzheitliches Konzept, das konkrete Handlungsvorgaben für die Einführung, Migration und Schulung enthält. Bei der Umsetzung des ersten Schritts kann es hilfreich sein, ein externes Consulting in Anspruch zu nehmen.

Schritt 2 Die richtige Lösung finden

E-Mail-Gateways korrigieren die weit verbreitete Sichtweise, dass **Verschlüsseln und Signieren zu kompliziert und umständlich sei (Mythos 5).**

Die gesamten Prozesse laufen über einen Server automatisiert ab, ohne dass der einzelne Anwender eingreifen muss. Das senkt die Hemmschwelle für die E-Mail-Verschlüsselung erheblich.

Während beim clientbasierten Verfahren die Verschlüsselungs-Software auf jedem Rechner installiert werden muss, geschieht dies bei der serverbasierten Lösung einmalig und zentral. Weitere Anwender und die entsprechenden Verschlüsselungselemente lassen sich dann schnell und sehr einfach hinzufügen. Dadurch wird der Implementierungs- und Administrationsaufwand erheblich verringert.

Einheitliche Sicherheitsrichtlinien für E-Mails lassen sich mit E-Mail-Gateways einfacher umsetzen. Die entsprechenden Regeln werden zentral definiert und verwaltet. Solche Regeln können beispielsweise aus Schlüsselwörtern im Betreff oder im Inhalt der E-Mail bestehen, oder sie beziehen sich auf bestimmte E-Mail-Empfänger.

Zudem ermöglichen Gateway-Lösungen, dass E-Mail-Verschlüsselung auch mit mobilen Endgeräten genutzt werden kann. Dabei liegen die E-Mails entschlüsselt in der Mailbox des Smartphone- und Tablet-Anwenders.

Und schließlich ist es bei der serverbasierten Verschlüsselung möglich, den Virenscan vor dem E-Mail-Server durchzuführen. Viren und Inhalte lassen sich somit zentral und gemäß den Unternehmensrichtlinien prüfen.

Außerdem können gesendete und empfangene E-Mails zentral archiviert werden und sind für den Benutzer per Volltextsuche erschließbar, da sie im Klartext in den Mailboxen vorgehalten werden.

Gateway-Lösungen sind aufgrund der genannten Vorteile heute Standard bei der E-Mail-Verschlüsselung.

Daneben gibt es Anwendungen, die für bestimmte Daten einen hohen Schutzbedarf fordern. Dazu gehören zum Beispiel Gesundheitsdaten, Rechtsdokumente und Verträge oder Patentinformationen und Konstruktionspläne. Clientbasierte Verschlüsselungslösungen sind hierfür eine sinnvolle Ergänzung. Sie schützen den gesamten Weg der E-Mail von einem Endgerät zum anderen Endgerät (E2E). Dafür müssen jedoch alle Anwenderrechner mit einer zusätzlichen Software und den entsprechenden anwenderspezifischen Zertifikaten und Schlüsseln ausgerüstet werden.

Beide Ansätze sind miteinander kombinierbar: serverbasierte Verschlüsselung für den Standardbenutzer und clientbasierte Sicherung für die Nutzer mit höherem Schutzbedarf.

Schritt 3 Zertifikate und Signaturen besorgen

Die Schutzziele der Authentizität und Integrität setzen die Einführung einer Public-Key-Infrastruktur (PKI) voraus. Dabei müssen Zertifikate mit den dazugehörigen Schlüsselpaaren erstellt, verteilt und verwaltet werden. Eine komplexe Aufgabe, die Zeit und Ressourcen in Anspruch nimmt.

Es empfiehlt sich deshalb, auf einen externen Dienstleister, den Vertrauensdiensteanbieter, zurückzugreifen. Dort erhalten Anwender die notwendigen Mittel für das Verschlüsseln und Signieren von E-Mails durch vertrauenswürdige Zertifikate.

Dazu gehören **Personenzertifikate**, die sich sowohl **mit E-Mail-Gateways** als auch mit clientbasierten Verschlüsselungslösungen einsetzen lassen. Dafür wird das Zertifikat entweder auf dem Rechner des Anwenders oder zentral auf dem E-Mail-Gateway-Server des Unternehmens installiert. Alle E-Mails, die diesen Server passieren, lassen sich bei Bedarf zusätzlich mit einer fortgeschrittenen elektronischen Signatur versehen.

Personenzertifikate beziehen sich auf eine natürliche Person. Daneben bieten einige Vertrauensdiensteanbieter wie D-Trust – ein Unternehmen der Bundesdruckerei-Gruppe – auch eine **Team-ID** an. Diese dient dem Absichern der E-Mail-Kommunikation von Gruppenpostfächern wie vertrieb@mustermann.de. Das entsprechende Zertifikat beinhaltet neben der E-Mail-Adresse ausschließlich Angaben zu einer Organisation und einer Abteilung.

Für eine **E-Mail-Kommunikation auf dem Niveau der Geheimhaltungsstufe VS-NfD (Verschlusssache – Nur für Dienstgebrauch)** sind ebenso vom Vertrauensdiensteanbieter D-TRUST Personenzertifikate aus einer besonders geschützten V-PKI (Verwaltungs-PKI) erhältlich. Diese sind nach der technischen Richtlinie TR-03145 des Bundesamts für Sicherheit in der Informationstechnik (BSI) zertifiziert.[8]

Die bei Vertrauensdiensteanbietern erhältlichen Zertifikate unterstützen den X.509-Standard. Dadurch ist die Interoperabilität mit anderen Systemen und Infrastrukturen gegeben.

IN EIGENER SACHE

Certificate Service Manager (CSM) – Managed-PKI-Plattform

Der Certificate Service Manager ist ein Managed-PKI-Service für Organisationen, die jährlich mehrfach Zertifikate beantragen. Die webbasierte Lösung unterstützt dabei, Zertifikate zu verwalten, zu beantragen und die Benutzer zu administrieren. Damit reduzieren Anwender Aufwand, Kosten und Zeit, die mit dem Einsatz einer großen Anzahl an Zertifikaten verbunden sind. Über eine API-Schnittstelle gelingt die nahtlose Integration in bestehende Unternehmensanwendungen und -workflows.[9]

8 Auf der Website der Bundesdruckerei findet sich ein **Überblick über die unterschiedlichen Typen von Personenzertifikaten**

9 Auf der Website der Bundesdruckerei gibtes **mehr Informationen zum Certificate-Service-Manager**

Für die clientbasierte Ende-zu-Ende-Verschlüsselung können Personenzertifikate softwarebasiert als sogenannter Softtoken (zum Beispiel per E-Mail) ausgeliefert werden. Diese mit einem Passwort geschützte und verschlüsselte elektronische Datei enthält die Zertifikate und das Schlüsselmaterial. Softtoken lassen sich in fast allen gängigen Browsern und S/MIME-konformen E-Mail-Clients verwenden.

Eine große Anzahl von Personenzertifikaten muss effizient verwaltet und ausgestellt werden. Bei dieser Herausforderung unterstützen webbasierte Managed-PKI-Lösungen (siehe Kasten Seite 19). E-Mail-Gateways beantragen die benötigten Zertifikate automatisiert über diese Managed PKI.

Ein weiterer Trend sind vollintegrierte, ganzheitliche Lösungen für das Zertifikate-Management und die Nutzung von digitalen Zertifikaten auf mobilen Endgeräten. Dafür kooperieren Softwareanbieter und Vertrauensanbieter (siehe Kasten unten).

Schritt 4 Vertrauensanker nutzen

Vertrauensdiensteanbieter nehmen in der digitalen Welt die Funktion eines Vertrauensankers ein, indem sie die Identität einander unbekannter Personen zuverlässig beglaubigen und die entsprechenden Daten sicher verwalten. Gleichzeitig stellen sie die Mittel und Infrastruktur bereit, um zuverlässig und sicher E-Mails zu verschlüsseln und Dokumente zu signieren.

Vertrauensdiensteanbieter mit dem höchsten Sicherheitsniveau besitzen den Status eines qualifizierten Vertrauensdiensteanbieters (qVDA). Die Arbeit als qVDA setzt eine umfangreiche und detaillierte Konformitätsprüfung durch nationale Aufsichtsbehörden wie den TÜViT und die Bundesnetzagentur voraus. Dabei wird von unabhängigen Experten festgestellt, ob der qualifizierte Vertrauensdiensteanbieter die rechtlichen Vorgaben im Hinblick auf IT-Sicherheit und Datenschutz erfüllt. Diese Prüfung wird in regelmäßigen Abständen wiederholt.

IN EIGENER SACHE

Über D-Trust

Die D-Trust GmbH mit Sitz in Berlin ist ein Unternehmen der Bundesdruckerei-Gruppe. Technologisch ausgereifte Lösungen machen es zu einem Vorreiter für sichere digitale Identitäten. Als unabhängiger und qualifizierter Vertrauensdiensteanbieter ist D-Trust bereits seit 2016 im Rahmen der europäischen Verordnung über elektronische Identifizierung und Vertrauensdienste (eIDAS) bei der Bundesnetzagentur gelistet. Das Unternehmen stellt rechtssichere und zertifizierte Vertrauensdienste wie digitale Zertifikate und elektronische Signaturen zur Verfügung.

5 Schlusswort

Was wäre, wenn Energieerzeuger und öffentliche Verwaltung ihre E-Mails verschlüsselt und signiert hätten?

Bei den betrügerischen E-Mails wäre die falsche Identität des Absenders sofort aufgefallen. Bereits das fehlende Zertifikat hätte Skepsis über die Vertrauenswürdigkeit der E-Mail hervorgerufen.

Ist ein digitales Zertifikat mit Signatur vorhanden, kann der Empfänger durch Abfrage beim zuständigen Vertrauensdiensteanbieter einfach feststellen, ob die Identität des Absenders echt ist. Der Versuch des Datendiebstahls und die Infizierung der IT-Systeme mit einem Schadprogramm wären daher erfolglos geblieben.

Werden konsequent nur verschlüsselte E-Mails verschickt und empfangen, ist ein Ausspionieren von sensiblen E-Mail-Inhalten nicht möglich. Denn die Angreifer haben keine Kenntnis von den notwendigen Schlüsseln, ohne die sich die Nachrichten nicht entschlüsseln lassen.

Aufwand für und Investitionen in E-Mail-Verschlüsselungen lohnen sich. Sie sind der einzige Weg, um eine sichere und vertrauenswürdige Kommunikation im digitalen Zeitalter sicherzustellen

D-Trust GmbH
Kommandantenstraße 18
10969 Berlin
Deutschland

Tel.: +49 30 25 98-0
vertrieb@d-trust.net
www.d-trust.net

Stand: September 2021