LEITFADEN DER KOMMISSION INTERNET UND DIGITALES

IT-Sicherheit-kompakt

E-Mail Verschlüsselung für Unternehmen

Der Mittelstand.
BVMW e.V.
Bundesverband

www.bvmw.de

In diesem Leitfaden wird die Bedeutung von E-Mail-Verschlüsselungsverfahren aufgezeigt, sowie Lösungen vorgestellt, welche über die Standardverfahren S/MIME und PGP hinaus gehen. Der Leitfaden ist als Ergänzung zum Blogbeitrag „Digitale Signatur und Verschlüsselung von E-Mails“ des Mittelstand Digitalzentrum Berlin zu sehen.

Problemstellung unverschlüsselte E-Mails

Welche Bedeutung haben E-Mails derzeit und in Zukunft?
Laut einer Erhebung von Statista wird sich die Anzahl der täglich versendeten und empfangenen E-Mails weltweit im Jahr 2023 auf 347 Milliarden belaufen. Bis 2026 werden es ca. 400 Milliarden E-Mails täglich sein. Je mehr E-Mails kursieren, umso mehr Schadmails mit Trojanern, Phishing-Mails, Spam und E-Mails mit sonstigen unliebsamen und immer echter wirkenden Fake-Inhalten landen in den Postfächern.
Von daher versteht es sich, dass dem Thema E-Mail-Sicherheit besonders hohe Bedeutung zukommt.

Warum ist eine unverschlüsselte E-Mail problematisch?
Im Internet gehen Sie, genauso wie beim Versand einer Postkarte, immer das Risiko ein, dass andere Personen E-Mails unbefugt mitlesen. Sie geben damit Hackern die Möglichkeit, personenbezogene Daten auszuspähen und für kriminelle Zwecke auszunutzen, z. B. Unternehmensspionage, Identitätsklau u. v. m. Zum Schutz der eigenen Daten und der Daten des Empfängers sowie Dritter ist es daher besonders wichtig, den E-Mail-Verkehr zu verschlüsseln.

Ist eine E-Mail-Verschlüsselung nach DSGVO Pflicht?
Die DSGVO und das Bundesdatenschutzgesetz (BDSG) empfehlen eine E-Mail-Verschlüsselung, eine Pflicht besteht jedoch nicht. Allerdings sollte man bedenken, dass personenbezogene Daten immer vor dem Zugriff Unbefugter geschützt werden müssen, damit für den Betroffenen kein Schaden entsteht. Gerade bei dem Versand von personenbezogenen Daten ist das Risiko für mögliche Zugriffe hoch. Dies gilt vor allem beim Versand von Daten der besonderen Arten (z. B. Gesundheitsdaten, biometrische Daten, Religionszugehörigkeit usw.).
Unverschlüsselte personenbezogene Daten (aber auch alle anderen Daten) aus E-Mails lassen sich zu Spionagezwecken, für Identitätsdiebstahl oder für sonstige Betrugs- und Erpressungszwecke leicht abfangen. Hierzu gibt es sogar Spionagetools im Internet (z. B. dem Dark Net). Von daher versteht es sich fast von selbst, hier für guten Schutz der E-Mails und der darin enthaltenen Daten zu sorgen.
Eine Verschlüsselung personenbezogener Daten hat für den Verantwortlichen und/oder den Auftragsverarbeiter allerdings auch noch weitere Vorteile. So muss etwa der Verlust eines mobilen Datenträgers, auf dem die Daten nach aktuellem Stand der Technik verschlüsselt wurden, in der Regel den Datenschutzbehörden nicht gemeldet werden. Darüber hinaus haben die Aufsichtsbehörden bei der Entscheidung, ob und in welcher Höhe eine Sanktion anfällt, gemäß Art. 83 Abs. 2 lit. c) DSGVO eine erfolgte Verschlüsselung positiv zu berücksichtigen.

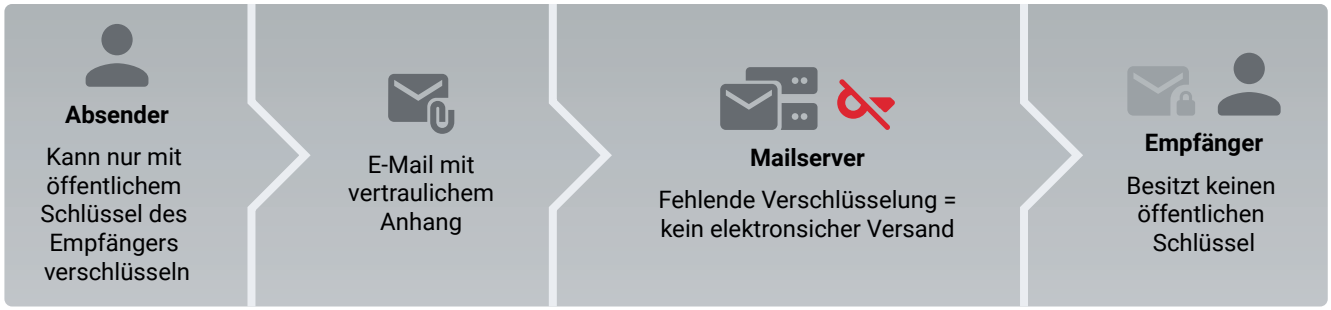
E-Mail-Verschlüsselung mit Standards

Was sind standardmäßige Verschlüsselungsverfahren?
Transportverschlüsselung: Sie schicken eine sichere E-Mail durch einen „verschlüsselten Tunnel“. Die E-Mail liegt bei Absender und Empfänger entschlüsselt vor, auf dem Weg ist sie aber unlesbar, sofern die Transportverschlüsselung richtig angewendet wird.
Bei einer Transportverschlüsselung ist die E-Mail nur auf dem Transportweg verschlüsselt. Sie befindet sich vor und nach dem Transport unverschlüsselt auf dem Server. Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) weist deshalb darauf hin, dass die Transport Layer Security (TLS) Verschlüsselung ein „notwendiger Baustein“ für die elektronische Kommunikation ist. Sie ist aber kein Ersatz für eine Ende-zu-Ende-Verschlüsselung, sprich eine Inhaltsverschlüsselung.

Inhaltsverschlüsselung: Die Meta-Informationen der E-Mail, sprich Absender, Empfänger und Betreff, sind weiterhin lesbar, der restliche Inhalt ist verschlüsselt.
Bei der Inhaltsverschlüsselung ist das Standardprotokoll OpenPGP für die PGP Verschlüsselung sowie das Protokoll S/MIME gebräuchlich. Weit verbreitet sind auch die RMS (Microsoft Rights Management Services). Sie eignen sich für die Azure Cloud und für den On-Premise-Einsatz, aber auch andere Anbieter haben sogenannte Information Rights Services (IRM) Lösungen zur Sicherung der Inhalte im Angebot.

Um einen bestmöglichen Sicherheitsstandard zu gewährleisten, kombinieren Sie am besten beide Verschlüsselungsarten.

Was ist an standardmäßigen Verfahren problematisch?
Leider sind die herkömmlichen Verschlüsselungsmethoden S/MIME und PGP für Unternehmen und öffentliche Institutionen in



der Praxis nur schwer umsetzbar: Die verwendeten Verschlüsselungsmechanismen sind inhomogen, die damit verbundenen Prozesse schwer zu vermitteln und im Ergebnis oft frustrierend für Sie und Ihre Kommunikationspartner.
Zusätzlich erschwert wird der Prozess für die Mitarbeiter, wenn unterschiedliche Technologien für unterschiedliche Empfänger genutzt werden.

Nachteile von PGP- und S/MIME-Verschlüsselung speziell aus Sicht von Unternehmen und Organisationen:

- Hoher Schulungsbedarf, um unterschiedliche Ansätze, Schlüsseltypen und -formate etc. den Mitarbeitern und den Administratoren näherzubringen
- Inkompatibilitäten mit Prozesssoftware, die in den E-Mail-Workflow eingebunden ist, und verschlüsselte Mails nicht verarbeiten kann
- Probleme bei auslaufenden Schlüsseln/Zertifikaten der Kommunikationspartner, die häufig manuell ausgetauscht werden müssen
- Probleme nach eigenem Schlüsselwechsel, wenn Kommunikationspartner noch die alten Schlüssel nutzen
- Probleme mit der E-Mail-Archivierungssoftware, die entweder verschlüsselte E-Mails nicht verarbeiten kann oder eine eigene Schlüssel-Verwaltung benötigt, in der alle über die Zeit verwendeten Schlüssel jedes Nutzers gespeichert werden müssen
- Keine Kontrolle, wie oft die zur Verfügung stehende Verschlüsselung tatsächlich genutzt wird (werden die Schutzziele erreicht?)
- Alternative Ansätze der Inhaltsverschlüsselung bringen Notwendigkeiten zum Einsatz von Passwörtern sowie Medienbrüche (Passworteingabe, Öffnen verschlüsselter Anhänge, Log-in-Vorgänge in Portalen) mit sich
- Häufig Ablehnung durch Kommunikationspartner (andere Organisationen), die den Einrichtungsaufwand scheuen

Welche weiteren Verfahren gibt es?

Adaptive Verschlüsselung
Unter adaptiver Verschlüsselung ist die Verknüpfung von Transport- und Inhaltsverschlüsselung und deren automatisierte Anwendung zu verstehen. Die E-Mail-Übertragung mit Transportverschlüsselung erfüllt bei Einhaltung der Sicherheitskriterien die gesetzlichen Anforderungen.
Wenn Unternehmen oder öffentliche Einrichtungen Daten per E-Mail an externe Empfänger versenden, sind Anforderungen an die Sicherheit der Übertragung einzuhalten, z. B. der gesetzliche Datenschutz oder Anforderungen an erhöhte Vertraulichkeit – etwa für Berufsgeheimnisträger.

Was ist an der adaptiven Verschlüsselung besonders?
Die Anwendung der adaptiven Verschlüsselung bedeutet in der Praxis:

- Bei jedem E-Mail-Versand wird eine **automatisierte Prüfung** durchgeführt, ob bei der Übertragung an den Empfänger-Server die Anforderungen einer obligatorischen/qualifizierten TLS-Verschlüsselung erfüllt werden.
- Abhängig von den vorliegenden Risiken (vorab pauschal konfiguriert oder im Einzelfall entschieden) werden E-Mails genau dann mittels **Transportverschlüsselung übertragen, wenn diese sicher genug ist**.
- Ansonsten erfolgt ein „Fallback" auf einen Sicherheitsautomatismus z. B.
  - » Versand der E-Mail nur nach Absenderfreigabe oder
  - » automatische Anwendung einer Passwortverschlüsselung.

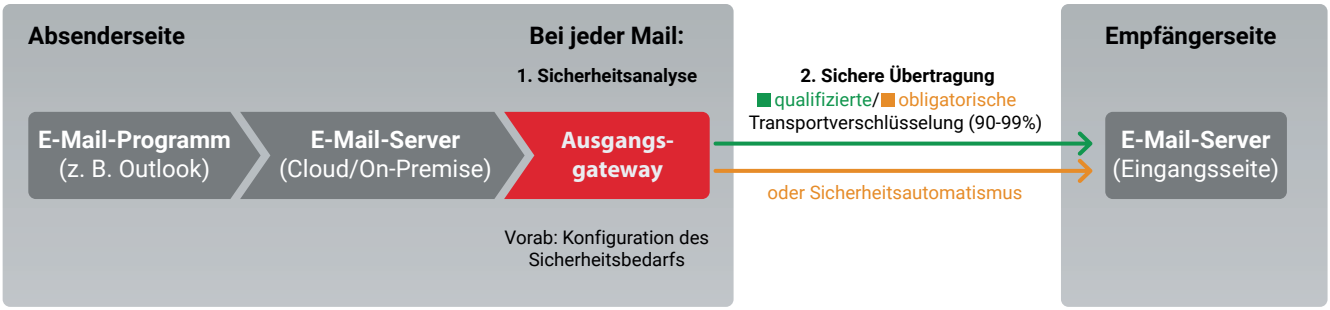
Welche Vorteile ergeben sich für Unternehmen?
Der Einsatz von adaptiver Verschlüsselung in Unternehmen oder öffentlichen Einrichtungen mindert den Aufwand der sicheren E-Mail-Übertragung erheblich, weil

- ca. 95 % der Empfänger Ihre E-Mails als „normale E-Mails" erhalten, unter Einhaltung aller Sicherheitsvorgaben – auch für Nachrichten mit „hohen Datenschutzrisiken",
- in diesen Fällen keinerlei Mehraufwand für die Nutzer entsteht,
- Empfänger mit unzureichend sicher konfiguriertem Server einen Anreiz haben, eine sichere Konfiguration herbeizuführen.

Weitere Vorteile für Unternehmen/öffentliche Einrichtungen sind:

- Die Einhaltung der Sicherheitsbedingungen kann automatisiert protokolliert werden (Nachweispflicht).
- Die Verantwortung für die Einhaltung der Sicherheitsvorgaben liegt nicht länger ausschließlich beim Absender (Ausschluss/Minderung des menschlichen Fehlerpotentials).
- Neben der Sicherheit der Übertragung kann auch die Tatsache der Übertragung an sich nachgewiesen werden (protokollierte Übergabe an den Empfänger-Server).

Was ist an der Dateiverschlüsselung besonders?
Die Dateiverschlüsselung ist eine alternative Methode zur Transportverschlüsselung. Diese verschlüsselt nicht, wie oben beschrieben, den Transport, sondern die Daten selbst. Damit sind die Daten beim Transport geschützt und eine Transportverschlüsselung ist nicht mehr notwendig. Der Vorteil liegt hierbei bei der Ende-zu-Ende Verschlüsselung und einer somit personengenauen Verschlüsselung. Ein weiterer Vorteil ist die zusätzliche Möglich-



keit, die Daten lokal, zentral oder in der Cloud sicher zu speichern. Der Nachteil liegt hierbei beim Schlüsselmanagement, konkret in der Erzeugung und dem Austausch von Schlüsseln. Hier sollte man auf eine besonders einfache Applikation zurückgreifen, die bereits in vorhandene Systeme integriert werden kann.

Wie bekomme ich diese Verfahren im Unternehmen umgesetzt?
Die Entscheidung, welche Art und welchen Umfang eine Verschlüsselung der E-Mail-Kommunikation haben muss, unterliegt den gesetzlichen und technischen Anforderungen der jeweiligen Unternehmung. Hier macht es Sinn, den Schutzbedarf und die Anforderungen genau zu definieren und eine individuelle Entscheidung zu treffen. Eine Integration in bereits vorhandene Systeme ist dabei im Hinblick auf die vorhandenen Ressourcen zu empfehlen. Fakt ist, dass die Gefahren durch Schadsoftware zunehmen werden, wodurch eine rasche Handlung notwendig ist.

Archivierung von E-Mails

Alle Unternehmen – Kleingewerbetreibende ausgenommen – müssen ihre komplette Geschäftskorrespondenz für sechs bis zehn Jahre ab Ende des Kalenderjahres aufbewahren. Daher ist es sinnvoll, die Geschäftskorrespondenz eines Unternehmens per E-Mail für zehn Jahre zu archivieren und danach ebenso zuverlässig zu löschen.
Je nach Inhalt der E-Mail können vertragliche oder gesetzliche Vorschriften die Art und Dauer der Aufbewahrung bestimmen.
Eine gesetzliche Pflicht, E-Mails zu archivieren, kann sich aus verschiedenen Vorschriften ergeben. Diese gelten nicht alternativ, sondern kumulativ. Je nach Fall, können daher mehrere Vorschriften einschlägig sein.

Die Fälle unterschieden sich nach
- der Rechtsform der Unternehmung,
- dem Tätigkeitsbereich,
- dem Inhalt der E-Mail sowie
- den anzuwendenden Vorschriften (diese ergeben sich aus den vorgenannten Fallunterscheidungen).

Im Rahmen der Archivierung müssen die E-Mails einschließlich der angehängten Dateien
- vollständig,
- manipulationssicher,
- jederzeit verfügbar und
- maschinell lesbar

über die Dauer der Aufbewahrungsfrist in **digitaler Form** abgelegt werden.

Neben den E-Mails an sich muss auch die Hard- und Software bereitgehalten werden, um die E-Mails und deren Anhänge wiederherstellen und lesbar machen zu können, etwa dann, wenn die E-Mails in komprimierter Form archiviert werden. Dabei sollte beachtet werden, dass nicht jeder Mitarbeiter Zugriff auf die Daten hat, um den betrieblichen Datenschutz zu gewährleisten und die Daten vor Manipulationen zu schützen.

Muss ein E-Mail-Archiv verschlüsselt sein?
Der Gesetzgeber verlangt keine Verschlüsselung. Einige Fälle von unbeabsichtigten Datenverlusten zeigen aber, dass es im Eigeninteresse der Unternehmen liegen sollte, Daten verschlüsselt zu speichern und zu übertragen. So sind nicht nur die eigenen Daten geschützt, auch der Verlust und die damit einhergehenden Entschädigungsklagen Dritter lassen sich vorbeugen. Eine rechtskonforme technische Lösung ermöglicht, die Daten in ihrer Gesamtheit sicher zu verwahren und im Bedarfsfall an den Berechtigten entschlüsselt zu übergeben.
Ein Problem bei der verschlüsselten Archivierung von E-Mails kann allerdings die dann nicht mehr funktionierende Suchfunktion sein. Hier gilt es also zu prüfen und abzuwägen, was für das Unternehmen die sinnvollste Möglichkeit darstellt.

Autoren:
Rüdiger Gropp
Pro-Icon IT-Consulting und Unternehmensberatung
https://pro-icon.de

Georg Nestmann
comcrypto
https://www.comcrypto.de

Henrike Ewald
procilon Group
https://www.procilon.de

Der BVMW

- vertritt im Rahmen seiner Mittelstandsallianz rund 900.000 Unternehmerstimmen
- wird von 340 BVMW-Repräsentanten bundesweit vertreten
- organisiert mehr als 2.000 Veranstaltungen im Jahr
- ist mit Auslandsbüros in über 60 zentralen Wachstumsmärkten vertreten
- hat in über 30 Ländern strategische Partnerschaften mit Verbänden

Herausgeber

Der Mittelstand. BVMW e.V.
Potsdamer Straße 7, 10785 Berlin
Tel.: 030 533206-0, Fax: 030 533206-50
E-Mail: politik@bvmw.de,
Website: www.bvmw.de

@BVMWeV

Stand: Juli 2023 | Titelbild: stockyme – stock.adobe.com | EU-Transparenzregisternr. 082217218282-59