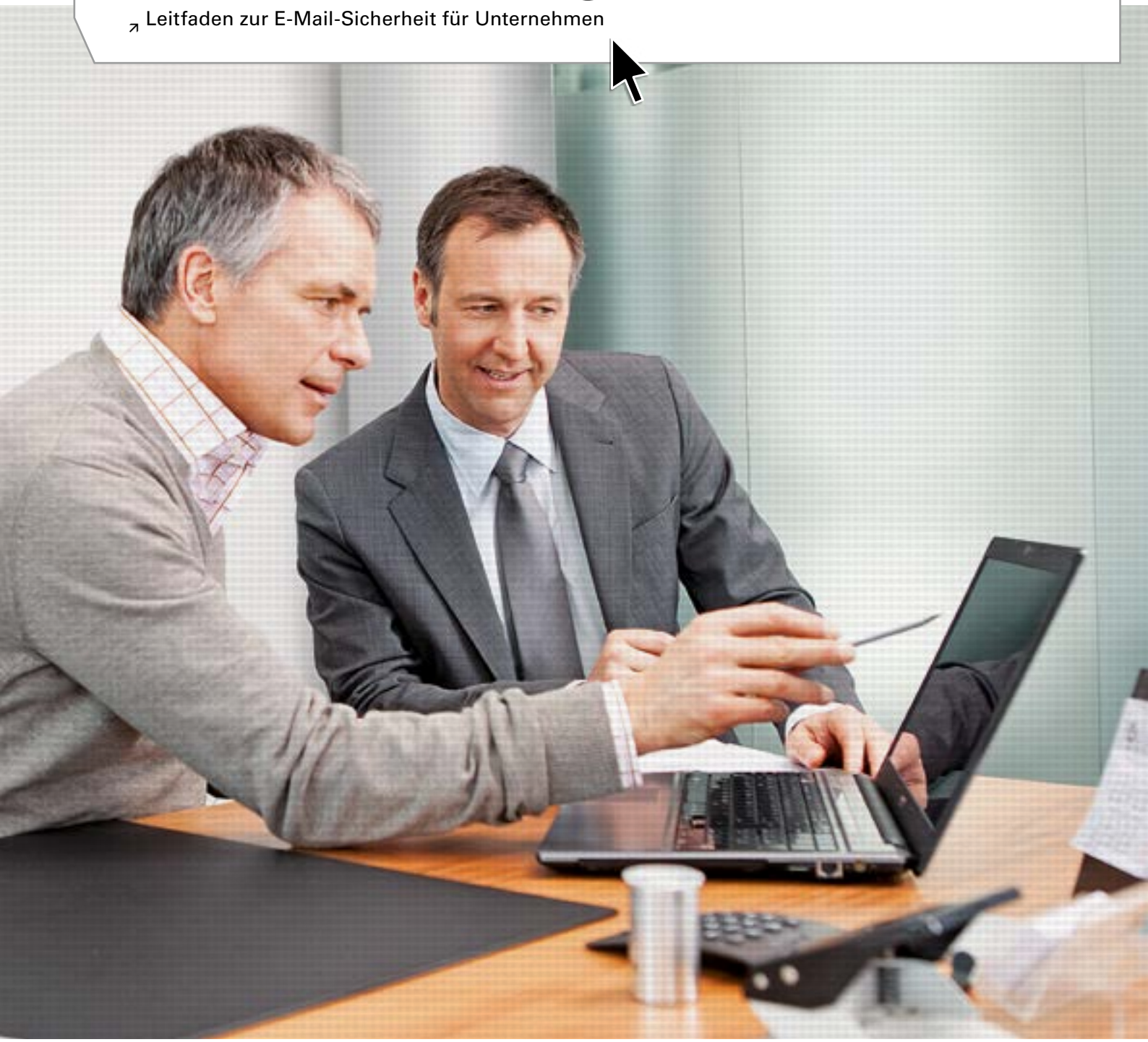
DATEV

Verschlüsselung von E-Mails

Leitfaden zur E-Mail-Sicherheit für Unternehmen



Eine Informationsbroschüre von DATEV und Deutschland sicher im Netz e. V.

Gefördert durch:

Deutschland sicher im Netz

Bundesministerium für Wirtschaft und Technologie

aufgrund eines Beschlusses des Deutschen Bundestages

TASK FORCE IT-SICHERHEIT IN DER WIRTSCHAFT
Mehrwert und Schutz für Rechner.

Vorwort

Mangelnde IT-Sicherheit kann zu gravierenden Imageschäden und ernsten wirtschaftlichen Einbußen führen. Daher engagiert sich der Verein Deutschland sicher im Netz e. V. (DsiN) bereits seit 2011 als Mitglied der Task Force „IT-Sicherheit in der Wirtschaft“ des Bundesministeriums für Wirtschaft und Technologie für eine breite Aufklärung zu diesem wichtigen Thema.

Die Task Force sensibilisiert mit verschiedenen Projekten vor allem kleine und mittelständische Unternehmen (KMU) für IT-Sicherheit und unterstützt diese, die Sicherheit der Informations- und Kommunikationstechnik (IKT) zu verbessern. 2013 schult DsiN gemeinsam mit Partnern in bundesweiten Workshops Anwälte, Steuerberater, Interne Revisoren, Unternehmensberater sowie Wirtschaftsprüfer zu Brückenbauern für IT-Sicherheit. Sie sollen ihre mittelständischen Klienten und Mandanten für das Thema sensibilisieren.

Ein wichtiger Aspekt dabei ist E-Mail-Sicherheit. Lediglich 44 Prozent der KMU kümmern sich um den Schutz ihrer Mails. Zu diesem Ergebnis kommt die DsiN-Studie „IT-Sicherheitslage im Mittelstand 2013“[1]. Der vorliegende Leitfaden soll einen kleinen Beitrag zu mehr E-Mail-Sicherheit leisten. Er gibt einen Überblick über die wichtigsten Aspekte der E-Mail-Sicherheit und insbesondere über die Verschlüsselung von E-Mails.

Task Force „IT-Sicherheit in der Wirtschaft“

Die Task Force „IT-Sicherheit in der Wirtschaft“ ist eine Initiative des Bundesministeriums für Wirtschaft und Technologie, die gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung vor allem kleine und mittelständische Unternehmen für IT-Sicherheit sensibilisieren und dabei unterstützen will, die Sicherheit der IKT-Systeme zu verbessern.

Weitere Informationen zur Task Force und ihren Angeboten sind unter www.it-sicherheit-in-der-wirtschaft.de abrufbar.

Dr. Christian P. Illek,
Vorstandsvorsitzender Deutschland sicher im Netz e. V.

[1] Die Studie kann auf der DsiN-Webseite abgerufen werden:
https://www.sicher-im-netz.de/unternehmen/sicherheitslage_mittelstand_2013.aspx

Verschlüsselung von E-Mails

Leitfaden zur E-Mail-Sicherheit für Unternehmen

Leitfaden: Das sollten Sie als Unternehmer beachten

Management Summary

Leitfaden

Im Geschäftsleben hat die E-Mail der Briefpost längst den Rang abgelaufen. Nahezu alle Unternehmen nutzen E-Mail für geschäftliche Zwecke – oft für die Übermittlung sensibler Informationen und Daten. Allerdings bietet im Gegensatz zur Briefpost der E-Mail-Verkehr gegenüber unerwünschten Mitlesern zunächst einmal keine Sicherheit, wobei Internet-Kriminalität, Wirtschaftsspionage und Lauschangriffe immer stärker zunehmen. Trotzdem hat ein großer Teil der deutschen Unternehmen noch keine Vorkehrungen getroffen, um die Vertraulichkeit ihrer E-Mail-Kommunikation zu schützen.

Eine Ursache für diese Situation dürfte die fehlende Trennschärfe der Begriffe Internet-Schutz und E-Mail-Sicherheit für die Anwender sein.[2]

Nahezu alle Unternehmen betreiben bereits Lösungen für den Internet-Schutz, welche vorgeben, auch die E-Mail-Sicherheit zu gewährleisten. In der Tat schützen diese Lösungen aber nur vor Bedrohungen des IT-Systems durch Schadsoftware – um die Vertraulichkeit der E-Mails auch auf dem Weg zum Empfänger wirksam zu sichern, sind zusätzliche Maßnahmen erforderlich. Dies sind insbesondere Maßnahmen zur Verschlüsselung von E-Mails.

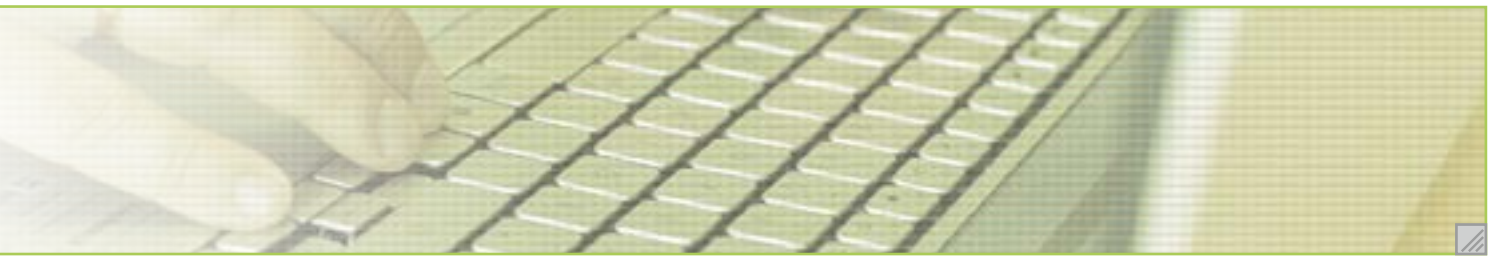
[2] In der Sicherheitsbranche wird E-Mail Security häufig mit Schutz vor Malware in E-Mails und auf E-Mail-Servern verstanden. Internet-Schutz beinhaltet i. d. R. Anti-Spam, Web Security, Anti-Malware etc. Die E-Mail-Sicherheit bietet mit Verschlüsselungstechnologien eine vertrauliche E-Mail-Kommunikation.

1 Einleitung

Drei Jahrzehnte nachdem der Siegeszug der E-Mail in Deutschland seinen Anfang nahm wächst die Zahl der E-Mail-Nutzer noch immer. Auch die Übermittlung geschäftlicher Informationen – oft vertraulichen Inhalts – per E-Mail ist heute längst Alltag. Der Nutzen elektronischer Geschäftsdokumente liegt auf der Hand: Sie sind schnell übermittelt und leicht weiterzuverarbeiten, Medienbrüche werden vermieden.

Gleichzeitig aber wird derzeit nur in wenigen Unternehmen dafür Sorge getragen, die übermittelten Informationen angemessen zu schützen. Offenbar ist bei vielen Anwendern das Bewusstsein darüber, welchen Gefahren die E-Mail-Kommunikation ausgesetzt sein kann und wie wichtig ihre Absicherung heute ist, noch immer nicht ausreichend vorhanden. Der Grund dafür liegt nicht zuletzt in der fehlenden Klarheit und Trennschärfe der Begriffe „E-Mail-Sicherheit/-Schutz“ und „Internet-Schutz“.

Der vorliegende Leitfaden grenzt diese Begriffe klar voneinander ab und stellt dar, warum Lösungen für den Internet-Schutz noch keine ausreichende E-Mail-Sicherheit – im Sinne einer vertraulichen E-Mail – garantieren und wie dieses Problem gelöst werden kann. Wir stellen aktuelle Lösungsansätze für die E-Mail-Verschlüsselung vor und diskutieren ihre Stärken und Schwächen.



2 Sorgenkind E-Mail-Kommunikation

2.1 Aktuelle Entwicklungen bei der E-Mail-Kommunikation

Auch wenn einige Experten aufgrund der zunehmenden Nutzung sozialer Netzwerke schon das baldige Ende der E-Mail voraussagen: Die Zahlen der Marktforscher belegen das Gegenteil. In den vergangenen Jahren hat der Anteil an Internet-Nutzern, die mindestens monatlich auf E-Mails zurückgreifen, noch einmal deutlich zugenommen. Zu diesem Ergebnis kommt zum Beispiel die europaweite Studie „Mediascope 2012" des IAB Europe, die in Deutschland in Zusammenarbeit mit dem Bundesverband Digitale Wirtschaft BVDW e. V. durchgeführt wurde.[3] In 2012 kommunizierten demnach 97 Prozent aller deutschen Internet-Nutzer via E-Mail. 75 Prozent nutzten sogar mindestens einmal täglich diesen Kommunikationskanal.

Der Hauptanteil des E-Mail-Verkehrs wird durch die geschäftliche E-Mail-Nutzung verursacht. Mehr als 100 Milliarden geschäftliche E-Mails pro Tag (und nur 82 Milliarden private) werden derzeit weltweit gesendet und empfangen; bis 2017 soll diese Zahl um ca. 7 Prozent pro Jahr auf über 132 Milliarden ansteigen.[4] Der Briefpost hat die E-Mail im Geschäftsleben längst den Rang abgelaufen. 2013 nutzten 97 Prozent von 1.529 im Rahmen des „DsiN-Sicherheitschecks" befragten Unternehmen E-Mail für geschäftliche Zwecke (2012: 93 Prozent; 2011: 89 Prozent).[5] In einer anderen Umfrage unter Internet-Nutzern gaben rund 70 Prozent der Befragten an, regelmäßig E-Mails für ihre kommerzielle Korrespondenz zu nutzen, während per Briefpost über die Hälfte der Befragten (rund 52 Prozent) nur noch weniger als einmal pro Jahr geschäftlich kommunizieren.[6]

[3] Bundesverband Digitale Wirtschaft (BVDW) e. V.: „E-Mail-Monitor. Aktuelle Studienergebnisse zu E-Mail-Marketing, Geschäfts- und Servicekommunikation", April 2013

[4] The Radicati Group, Email Statistics Report, 2013–2017

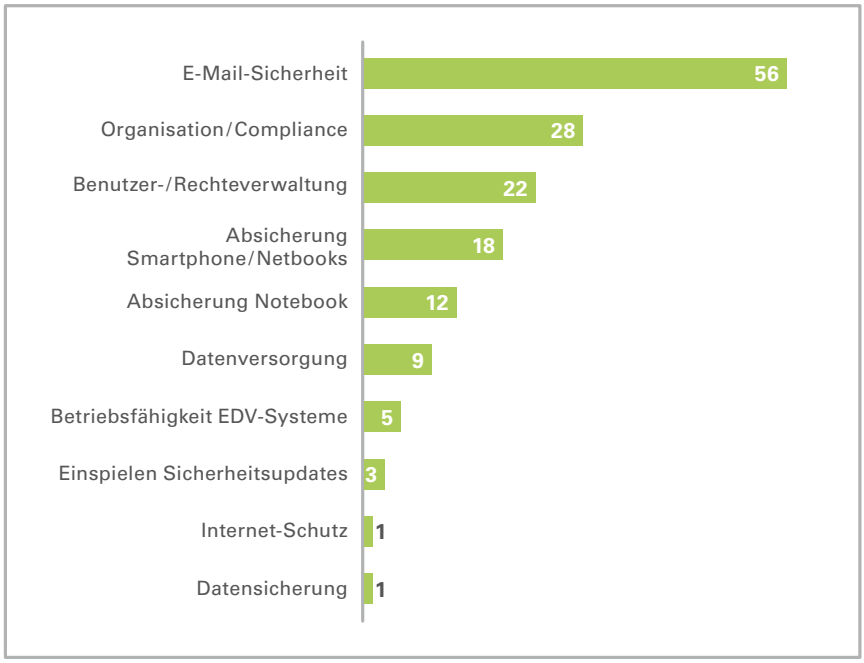
[5] Initiative Deutschland sicher im Netz e. V. (DsiN): „IT-Sicherheitslage im Mittelstand 2011" und „IT-Sicherheitslage im Mittelstand 2012" (Update der Studie von 2011) „Sicherheitslage im Mittelstand 2013"; konzipiert und durchgeführt von den DsiN-Mitgliedern BITKOM, DATEV, SAP & Sophos.

[6] United Internet Dialog GmbH: „Geschäftliche Kommunikation per Briefpost hat massiv an Bedeutung verloren (...)" (Pressemeldung vom 5.3.2012).

2.2 Die Sicherheit der E-Mail-Kommunikation wird vernachlässigt

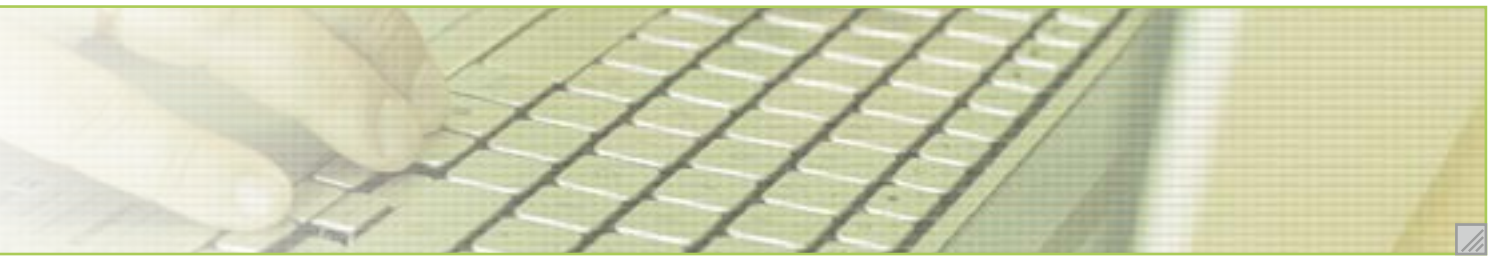
Angesichts dieser Zahlen ist es mehr als beunruhigend, dass zahlreiche Unternehmen ihre E-Mail-Kommunikation nicht oder nur unzureichend schützen. Laut der DsiN-Sicherheitsstudie 2013 hat sich das Bewusstsein für IT-Sicherheit bei den mittelständischen Unternehmen in Deutschland insgesamt positiv entwickelt und nahezu alle Betriebe sorgen inzwischen für einen hinreichenden Internet-Schutz, bei der Absicherung der E-Mail-Kommunikation besteht aber weiter Nachholbedarf. So gaben 56 Prozent der Befragten an, keine Vorkehrungen zur E-Mail-Sicherheit getroffen zu haben (siehe Abbildung 1).

Abbildung 1:
Keine Schutzmaßnahmen vorhanden (Quelle: DsiN-Studie zur Sicherheitslage im Mittelstand 2013, Angaben in %)



Dieser Wert hat sich gegenüber dem Vorjahr sogar nochmal um zwei Prozentpunkte verschlechtert. Die E-Mail-Sicherheit kann offenbar mit dem Wachstum der E-Mail-Nutzung in kleineren und mittleren Unternehmen nicht Schritt halten – 65 Prozent der Befragten sind kleine Unternehmen mit bis zu 50 Mitarbeitern.

Besonders gravierend ist dieser Befund im Hinblick auf die Tatsache, dass in Deutschland zunehmend auch vertrauliche und geschäftskritische Informationen, z. B. Geschäftsbriefe, Rechnungen, Patente, Verträge und Vereinbarungen, Protokolle oder Steuermeldungen, per E-Mail versandt werden (siehe Abbildung 2). Diese geschäftskritischen Informationen werden ungeschützt über ein Medium versendet, das im Standard keinerlei Funktionen zum Schutz der Vertraulichkeit vorsieht: Ohne spezifische Schutzmaßnahmen wie zum Beispiel Verschlüsselung ist eine E-Mail für Dritte so leicht lesbar wie eine Postkarte.



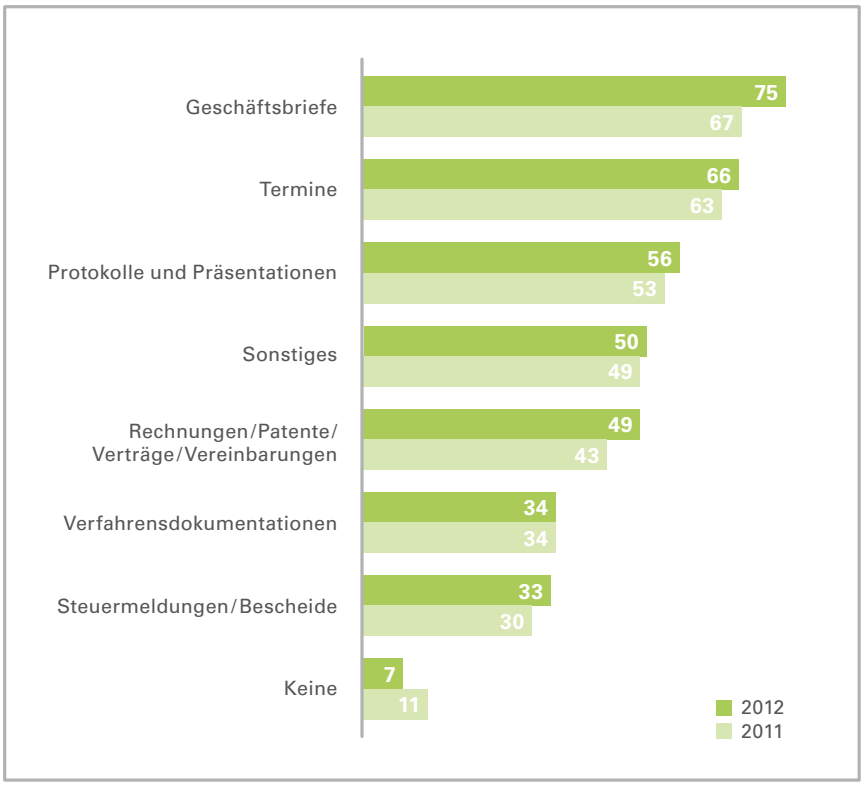


Abbildung 2:
Welche vertraulichen/geschäftskritischen Informationen senden Sie per E-Mail? (Quelle: DsiN 2012, Angaben in %)

Die Gründe für diese Sicherheitslücke sind sicher vielgestaltig. Neben einem mangelnden Gefährdungsbewusstsein dürften dabei oft auch fehlende Kenntnisse zur sicheren E-Mail-Kommunikation eine Rolle spielen – die Autoren der DsiN-Studie äußern in diesem Zusammenhang die Vermutung, dass „einige mittelständische Unternehmen Internet-Schutz mit E-Mail-Sicherheit verwechseln" (S. 10). Diese Vermutung wird gestützt durch den Fakt, dass von den über 1.500 befragten Unternehmen nur 1 Prozent über keinen Internet-Schutz verfügt – eine deutliche Diskrepanz zu den 56 Prozent ohne E-Mail-Sicherheit. Möglicherweise verfügen viele dieser meist kleineren Unternehmen nicht über das nötige Problembewusstsein und Know-how, um eine für ihre Bedürfnisse angemessene E-Mail-Sicherheit zu realisieren. Der vorliegende Leitfaden soll zeigen, dass auch kleinere Unternehmen mit wenigen Ressourcen ihre E-Mail-Kommunikation wirksam schützen können, und es soll dabei helfen, die Sicherheitslücke zu schließen.

3 Internet-Schutz bietet keine E-Mail-Sicherheit!

Bei der E-Mail-Kommunikation mit Geschäftspartnern werden regelmäßig vertrauliche und sensible Informationen und Dokumente ausgetauscht. Wenn solche Daten in die falschen Hände geraten, kann das ernste Konsequenzen haben – wirtschaftliche und finanzielle Nachteile, juristische Probleme und nicht zuletzt auch negative Auswirkungen auf Image und Glaubwürdigkeit. Die Absicherung der E-Mail-Kommunikation ist daher von hoher Wichtigkeit.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt in seinen IT-Grundschutz-Katalogen eine umfassende Übersicht über die Gefährdungen, denen die (geschäftliche) E-Mail-Kommunikation ausgesetzt sein kann.[7] In unserem Zusammenhang sind daraus insbesondere die folgenden dort unter „Vorsätzliche Handlungen" aufgelisteten Gefahren interessant:

- Unberechtigte IT-Nutzung (nach Überwinden der Authentisierung z. B. per Brute-Force-Angriff oder Aufzeichnung der Anmeldeinformationen)
- Schadprogramme
- Maskerade/Vortäuschen eines falschen Absenders
- Analyse des Nachrichtenflusses
- Mitlesen von E-Mails
- Vertraulichkeitsverlust schützenswerter Informationen
- Überlastung durch eingehende E-Mails
- Verhinderung von Diensten (Denial of Service)
- Web-Bugs (in die E-Mail eingebettete Bilder, die von einem Server nachgeladen werden und so u. a. einen Rückschluss auf das Öffnen der E-Mail erlauben)
- Missbrauch aktiver Inhalte in E-Mails.

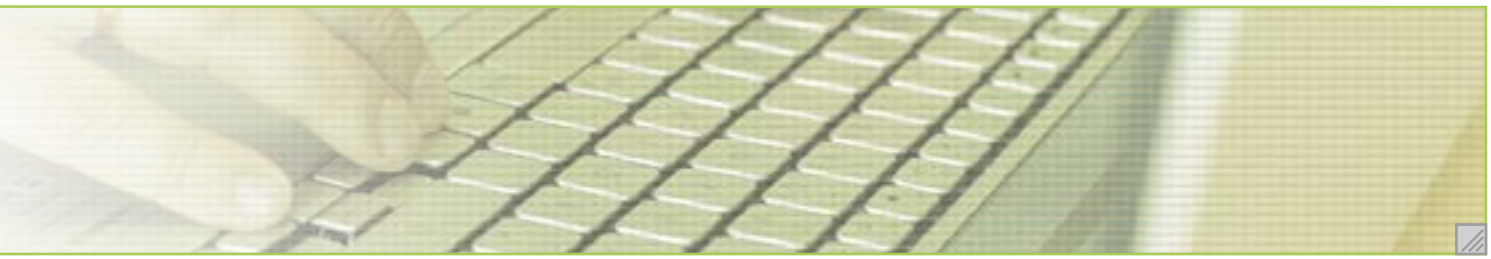
Da die E-Mail-Kommunikation einen wesentlichen Bestandteil der Internet-Nutzung darstellt, müssten die Lösungen für den Internet-Schutz demnach auch die Vertraulichkeit der E-Mails zuverlässig absichern können. Leider ist das nicht immer der Fall. Denn von den gerade genannten Gefährdungen für die E-Mail-Kommunikation wird im Rahmen des Internet-Schutzes nur ein kleiner Teil abgedeckt. Die folgenden Abschnitte sollen hier etwas Klarheit schaffen.

3.1 Internet-Schutz

Lösungen für den Internet-Schutz schützen das Unternehmensnetzwerk vornehmlich vor den vielfältigen Gefährdungen von **außen**, die eine Nutzung des Internets mit sich bringt. Im Web lauern bekanntlich zahlreiche Gefahren, zum Beispiel durch Viren, Würmer und andere Schadsoftware, Spam-Mails (ca. 70 Prozent des Mailverkehrs machen derzeit unerwünschte Werbemails aus[8]) und Phishing bis hin zu Datenspionage, Hacker- und DoS-Angriffen (Denial of Service: das Überlasten von Rechnern oder Netzen durch massenhafte Anfragen). Während Internet-Angriffe früher meist leicht erkannt werden konnten, weil sie vor allem darauf ausgerichtet waren, Schaden anzurichten, bleiben heute die

[7] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kataloge, B 5.3 Groupware. Die folgende Aufzählung lässt die missbräuchliche Nutzung durch eigene Mitarbeiter unberücksichtigt und beschränkt sich auf die Gefährdungen, die durch die Nutzung des Internets als Übertragungsmedium entstehen.

[8] Kaspersky Security Bulletin 2012: Spam im Jahr 2012



Angriffsversuche oft unbemerkt. Internet-Kriminelle wollen meist entweder die Rechner ihrer Opfer ausspähen, um wertvolle Daten (zum Beispiel Passwörter, Bank- oder Kreditkarteninformationen) zu erbeuten, oder die Computer ganz in ihre Gewalt bringen, um sie per Fernsteuerungssoftware zum Bestandteil eines „Botnetzes" zu machen und etwa für den Versand von Spam-Mails, für Brute-Force-Attacken oder DoS-Angriffe zu nutzen. Deshalb versuchen sie, entweder unbemerkt ins Netzwerk einzudringen und/oder Software einzuschleusen, die dann im Verborgenen aktiv wird und zum Beispiel Benutzereingaben aufzeichnet, Informationen an den Server des Angreifers schickt (Spyware), Hintertüren ins System öffnet, die Befehle des zentralen Botnetz-Servers ausführt oder auch weitere Software aus dem Netz nachlädt.

Um Netzwerke und Rechner zu kompromittieren, nutzen die Angreifer bevorzugt Sicherheitslücken des Betriebssystems oder installierter Programme, insbesondere des Browsers und seiner Plugins (Flash, PDF, Java). Ein weiterer Angriffsweg wird als Social Engineering bezeichnet: Man versucht, den Anwender dazu zu bewegen, Informationen herauszugeben (Phishing-Mails) oder Programme zu installieren – entweder durch Software, die sich als nützliches Programm tarnt, aber im Hintergrund andere Funktionen ausführt (Trojaner) oder indem bei einem Klick auf einer Webseite oder beim Öffnen eines Mailanhangs unbemerkt ein Programm ausgeführt wird. Sind Webserver nicht ausreichend gesichert, können eigentlich harmlose Internet-Angebote mit Schadprogrammen infiziert werden, welche gegebenenfalls Sicherheitslücken im Browser ausnutzen und auch ohne Zutun des Nutzers aktiv werden können (sogenannte Drive-by-Downloads).

Daraus wird auch deutlich, dass die E-Mail-Kommunikation im Rahmen des Internet-Schutzes nur einen von mehreren möglichen Wegen eines Angriffes von außen darstellt und auch so behandelt wird. Die wichtigsten Elemente des Internet-Schutzes sind Virenscanner, Spamschutz und Firewall – heute zunehmend realisiert durch sogenannte Next Generation Firewalls oder UTM-Geräte („Unified Threat Management"), die je nach Anforderungsprofil neben klassischen Firewall-Funktionen auch u. a. Funktionen zur Entdeckung und Verhinderung von Angriffen (Intrusion Detection/Prevention), Applikationskontrolle, Antivirus- und Antispam-Funktionen bieten. Verschlüsselungsfunktionen bieten diese Geräte in der Regel nicht, ebenso wenig wie die dedizierten E-Mail Security Appliances oder Services. Bei diesen Geräten kommen meist die gleichen Anti-Malware-Engines zum Einsatz wie in anderen Internet-Schutz-Systemen, ergänzt um einen sogenannten Message-Transfer-Agent, der grundlegende Mailserver-Funktionen bereitstellt.

Fazit: Weil Lösungen für den Internet-Schutz sich vornehmlich auf Gefährdungen von außen konzentrieren, liegt der Schutz der E-Mail-Kommunikation – des Austausches von Informationen und Daten – außerhalb ihres Fokusses, auch wenn die Anbieter oft undifferenziert von „E-Mail-Sicherheit" sprechen. Internet-Schutzlösungen adressieren daher von den oben aufgeführten Gefahren für die E-Mail-Kommunikation oft lediglich einen Teil: unberechtigte IT-Nutzung, Schadprogramme, Überlastung durch eingehende E-Mails, Missbrauch aktiver Inhalte in E-Mails und Denial-of-Service-Attacken.

3.2 E-Mail-Sicherheit

Seit den Anfängen der schriftlichen Nachrichtenübermittlung wird Wert auf Diskretion gelegt. Schon die Babylonier des zweiten Jahrtausends vor Christus, die einander mit Keilschrift beschriebene Tontafeln zusandten, versahen wichtige Nachrichten mit einer Art Umschlag, einer extra Schicht aus Ton, um sie vor fremden Augen zu schützen. Die alten Ägypter nutzten dafür versiegelte Papyrusrollen. Den heute bekannten Briefumschlag gibt es seit 1820.

Die E-Mail dagegen, das heute wichtigste Medium der schriftlichen Kommunikation, kennt keinen solchen schützenden Umschlag.[9] Das E-Mail-Protokoll SMTP (Simple Mail Transfer Protocol, deutsch etwa „Einfaches Nachrichtenübermittlungsprotokoll"), das heute bei nahezu jedem E-Mail-Versand zum Einsatz kommt, wurde 1982 mit dem erklärten Ziel veröffentlicht, Nachrichten „verlässlich und effizient" zu übermitteln[10] – von Sicherheit war damals noch keine Rede. Das junge Internet wurde zu dieser Zeit noch vorwiegend von Universitäten und Forschungseinrichtungen genutzt und die Betreiber von Internet-Servern konnten sich gegenseitig vertrauen. Authentifizierung oder Verschlüsselung sind bei SMTP nicht vorgesehen und die Echtheit der Daten, die vom Client des Absenders geliefert werden, wird vom Mailserver nicht geprüft. Seit den 90er Jahren wurde zwar eine Reihe von SMTP-Erweiterungen (SMTP-AUTH, START-TLS) eingeführt, deren Anwendung aber nicht zwingend ist und sie somit keine Garantie für eine sichere Übermittlung bieten.

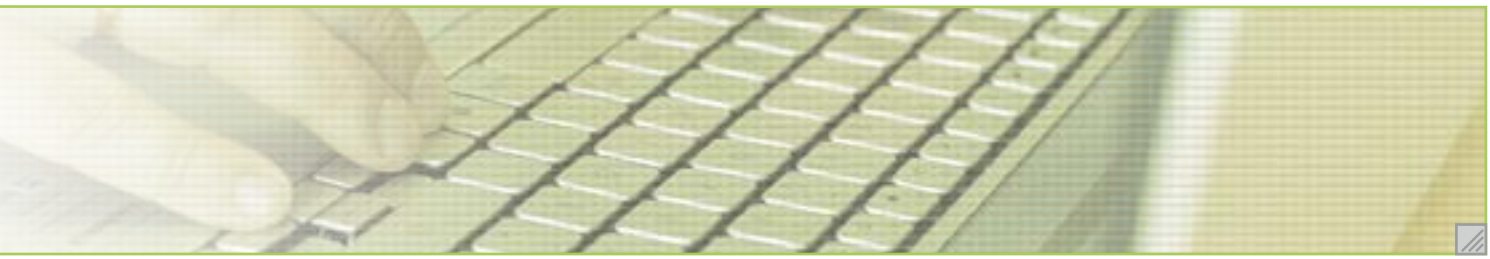
Deshalb ist tatsächlich das Kommunikationsmedium E-Mail in den meisten Fällen noch immer mit einer Postkarte vergleichbar – jeder, der darauf in irgendeiner Weise Zugriff erhält, kann mitlesen, und Absenderinformationen können leicht gefälscht werden. Schlimmer noch: Anders als Postkarten lassen sich elektronische Dokumente auch leichter verändern, ohne dass das im Nachhinein feststellbar wäre. Um eine sichere und den Datenschutzvorschriften entsprechende E-Mail-Kommunikation zu gewährleisten, müssen Unternehmen daher auch die folgenden vom BSI aufgeführten Gefährdungen berücksichtigen:

- Mitlesen von E-Mails
- Vertraulichkeitsverlust schützenswerter Informationen
- Analyse des Nachrichtenflusses
- Web-Bugs
- Maskerade/Vortäuschen eines falschen Absenders

Diese Gefährdungen betreffen also im Wesentlichen die Schutzbereiche **Authentizität**, **Integrität** sowie **Vertraulichkeit** bzw. **Datenschutz**.

[9] Der „Envelope", der bei SMTP der eigentlichen Mail vorangestellt wird, enthält nur Adressinformationen und erfüllt keine Schutzfunktion.

[10] The objective of Simple Mail Transfer Protocol (SMTP) is to transfer mail reliably and efficiently." Simple Mail Transfer Protocol, Internet Standard Document RFC 821, p. 1 (http://tools.ietf.org/html/rfc821)



3.2.1 Authentizität und Integrität

Die Authentizität einer E-Mail meint die Gewissheit, dass die Nachricht tatsächlich vom angegebenen Absender stammt, ihre Integrität die Gewissheit, dass ihr Inhalt vollständig und unverändert ist. Beides ist im geschäftlichen Verkehr von großer Bedeutung, da auch Erklärungen in E-Mails verbindlich sind. Solange der Gesetzgeber keinen Formzwang vorschreibt, sind Willenserklärungen per E-Mail genauso rechtswirksam wie mündliche oder andere schriftliche Erklärungen. Auch wenn für Rechtsgeschäfte Textform (§ 126b BGB) vorgeschrieben ist, können sie per E-Mail abgeschlossen werden. E-Mails gelten entsprechend auch als Handelsbriefe im Sinne des HGB.

Aus diesen Gründen ist es wichtig, bei der Übermittlung wichtiger Willenserklärungen, Informationen und Dokumente dafür Sorge zu tragen, dass Inhalte und Absenderinformationen nicht durch Dritte verändert werden können. Dies kann durch eine elektronische Signatur gewährleistet werden. Nur die qualifizierte elektronische Signatur ersetzt beim elektronischen Informationsaustausch die eigenhändige Unterschrift auf Papierdokumenten. Das deutsche Signaturgesetz beschreibt dafür drei verschiedene Arten der Signatur: die einfache elektronische Signatur (an die keine besonderen Anforderungen gestellt werden), die fortgeschrittene elektronische Signatur und die qualifizierte elektronische Signatur. Für die meisten Anwendungsfälle und auch beim E-Mail-Versand ist die fortgeschrittene elektronische Signatur ausreichend. Bei Rechtsgeschäften, für die vom Gesetzgeber Schriftform vorgeschrieben ist, ist eine qualifizierte elektronische Signatur erforderlich, um die Schriftform durch die elektronische Form zu ersetzen (§ 126a BGB). Bei fortgeschrittener und qualifizierter elektronischer Signatur stellen kryptografische Verfahren die Authentizität und Integrität des signierten Dokuments oder der Nachricht sicher und die Identität des Absenders muss auf geeignete Weise bestätigt werden, in der Regel durch eine unabhängige Instanz, also einen Zertifizierungsdienstleister.

Eine Liste der aktuell aktiven Zertifizierungsdienstanbieter wird von der Bundesnetzagentur angeboten.[11] Die Zertifizierungsdienstanbieter halten die notwendige Software und Hardware für qualifizierte elektronische Signaturen bereit. Diese können in allen Fällen Authentizität und Integrität gewährleisten. Auf Basis des neuen Personalausweises erlaubt es ein neues Angebot, kurzfristig eine Signaturfunktion einzurichten und dadurch mögliche Hemmschwellen gegen den Einsatz qualifizierter elektronischer Signaturen zu senken.

[11] http://www.bundesnetzagentur.de/cln_1911/DE/Service-Funktionen/QualifizierteelektronischeSignatur/WelcheAufgabenhatdieBundesnetzagentur/AufsichtundAkkreditierungvonAnbietern/ZertifizierungsDiensteAnbietr_node.html

3.2.2 Vertraulichkeit und Datenschutz

Die Vertraulichkeit der geschäftlichen Kommunikation zu sichern liegt im Interesse jedes Unternehmens. Dies gilt umso mehr, als sich heute die internetbasierte Wirtschaftsspionage längst zu einem einträglichen Wirtschaftszweig entwickelt hat. Einer Umfrage der Wirtschaftsprüfungs- und Beratungsgesellschaft KPMG zufolge war in den Jahren 2011 und 2012 in Deutschland jedes vierte Unternehmen schon einmal Opfer von Cyber-Kriminalität. Die Angriffe werden zunehmend gezielter, komplexer und professioneller, und ein Schaden von mehr als einer Million Euro pro e-Crime-Vorfall ist laut KPMG nicht ungewöhnlich. Die Hälfte der befragten Unternehmen sieht in der Übertragung geschäftskritischer Daten an Dritte eine bedeutsame Gefahrenquelle.[12] Der aktuelle Symantec-Sicherheitsbericht belegt ebenfalls den Trend zu gezielten Attacken, und zwar zunehmend gegen mittelständische Unternehmen.[13]

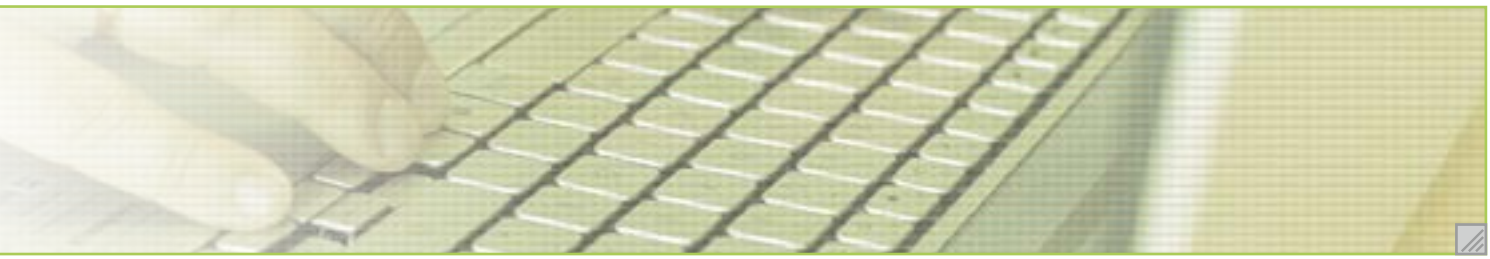
E-Mails machen es Spionen und Betrügern besonders leicht mitzulesen. Geschäftliche E-Mails müssen deshalb besser geschützt werden, als es bei den meisten Unternehmen derzeit noch der Fall ist. E-Mail-Verschlüsselung sollte daher für jedes mittelständische Unternehmen zumindest bei geschäftskritischen Informationen und Daten obligatorisch werden.

Die Vertraulichkeit von E-Mails durch Verschlüsselung kann aber auch gesetzlich gefordert sein. Immer dann, wenn personenbezogene Daten betroffen sind, zum Beispiel Lohn- oder FiBu-Daten oder Verträge, gelten die gleichen strengen Datenschutzvorschriften wie für Akten oder den Datenzugriff im Unternehmensnetzwerk. Dabei ist durch technische und organisatorische Maßnahmen, insbesondere durch „die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren", zu gewährleisten, „dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können" (Anlage zu § 9 Bundesdatenschutzgesetz).

In besonderer Weise ist die Anwendung von Verschlüsselungsverfahren für Unternehmen bzw. Personen ratsam, die der beruflichen Verschwiegenheitspflicht unterliegen. Denn hier wird teilweise vertreten, dass Privat-, Betriebs- oder Geschäftsgeheimnisse im Sinne von § 203 StGB verletzt werden; betroffen sind zum Beispiel Anwälte, Notare, Wirtschafts- und Buchprüfer, Steuerberater, Ärzte, Apotheker, Psychologen oder Versicherer. Auch ist nicht sichergestellt, ob eine Einverständniserklärung des Mandanten hier rechtliche Konsequenzen völlig ausschließt. Die Frage stellt sich unter anderem deshalb, weil beim Dokumentenversand oft auch Rechte Dritter betroffen sind, etwa von Angestellten oder Kunden des Mandanten.

[12] „e-Crime: Computerkriminalität in der deutschen Wirtschaft mit Kennzahlen für Österreich und Schweiz" (KPMG 2013)

[13] „Internet Security Threat Report 2013" (Symantec)



4 Lösungen für die E-Mail-Verschlüsselung

Die angesprochenen Gefahren für Authentizität, Integrität und Vertraulichkeit der E-Mail-Kommunikation sind kritisch – aber sie können abgewehrt werden. Von den vom BSI aufgeführten Gefährdungen sind an dieser Stelle insbesondere das „Mitlesen von E-Mails", der „Vertraulichkeitsverlust schützenswerter Informationen" und die „Analyse des Nachrichtenflusses" – also Gefährdungen der Vertraulichkeit und des Datenschutzes – relevant. Auf die Sicherstellung der Authentizität und Integrität durch elektronische Signaturen ist bereits oben in Kap. 3.2.1 hingewiesen worden. Das Gefährdungspotenzial von Web-Bugs wiederum ist vergleichsweise gering und moderne E-Mail-Clients können so konfiguriert werden, dass sie das automatische Nachladen der Bilder vom Server verhindern.

Eine Alternative zu den Verschlüsselungsverfahren ist die Möglichkeit, vertrauliche Daten in verschlüsselten Anhängen, wie beispielsweise in passwortgeschützten PDF-Dateien oder in ZIP-Archiven, zu versenden. Dies ist einfach umzusetzen, allerdings ist dieses Verfahren deutlich weniger sicher. Dabei ist ein ausreichend sicheres Kennwort (8 bis 12 Zeichen, alphanumerisch mit Sonderzeichen und Groß- und Kleinschreibung) Mindestvoraussetzung.

Die wichtigste Maßnahme für die E-Mail-Sicherheit ist die Anwendung eines passenden Verschlüsselungsverfahrens. Welches Verfahren für ein Unternehmen das geeignetste ist, hängt von verschiedenen Kriterien ab, darunter Schutzziele und Anforderungen, Unternehmensgröße, verfügbares IT-Know-how und natürlich das Budget. Der folgende kurze Vergleich verschiedener Lösungsansätze für die E-Mail-Verschlüsselung soll eine erste Orientierung ermöglichen.

Die meistgenutzten Standards bei der E-Mail-Verschlüsselung sind S/MIME und OpenPGP. Beide basieren auf einem asymmetrischen Verschlüsselungsverfahren, bei dem jeder Kommunikationspartner ein zusammengehörendes Schlüsselpaar erhält: Einen öffentlichen, den andere Kommunikationspartner dazu nutzen können, um an ihn gerichtete Nachrichten zu verschlüsseln, und einen privaten, den nur er kennt und der der Entschlüsselung dieser Nachrichten dient. Grundvoraussetzung für eine verschlüsselte Kommunikation ist also, dass alle Teilnehmer auf die öffentlichen Schlüssel ihrer Kommunikationspartner zugreifen können. Um die Authentizität eines öffentlichen Schlüssels verlässlich zu bestätigen, wird dieser durch geeignete Instanzen zertifiziert – bei S/MIME durch eine hierarchische Kette von Zertifizierungsstellen (PKI, Public Key Infrastructur), bei OpenPGP durch andere Kommunikationsteilnehmer in einem „Netz des Vertrauens" (Web of Trust).

Wer bereits über qualifizierte elektronische Signaturen nach dem Signaturgesetz verfügt, besitzt damit alle Voraussetzungen, dass ihm Nachrichten verschlüsselt gesendet werden können.

4.1 Clientbasierte Verschlüsselungslösungen (End-to-end-Verschlüsselung)

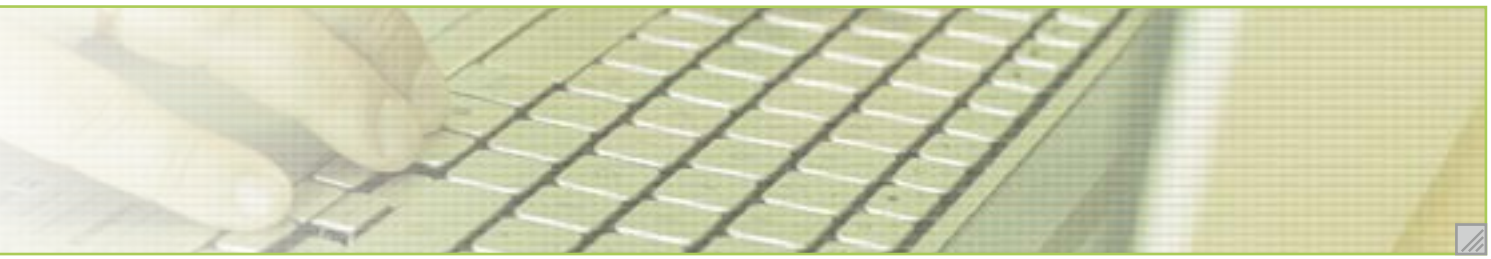
Bei der clientbasierten Verschlüsselung übernehmen die Endgeräte von Sender und Empfänger selbst das Verschlüsseln, Entschlüsseln, Signieren und die Verifikation von Nachrichten. Dieser Ansatz ermöglicht die durchgängige Verschlüsselung einer E-Mail über ihren gesamten Übertragungsweg und wird daher auch als Ende-zu-Ende-Ansatz (end-to-end) bezeichnet. Die E-Mail-Clients von Sender und Empfänger müssen dazu mit einer Verschlüsselungsfunktion ausgestattet sein. Während einige Clients, zum Beispiel Microsoft Outlook, diese bereits mitbringen, können andere Programme mit Hilfe von Erweiterungen nachgerüstet werden.

Clientbasierte Verschlüsselungslösungen erfordern häufig – insbesondere bei einer größeren Anzahl von Clients – einen hohen Administrationsaufwand und einige Fachkenntnisse bei den Anwendern. Weitere Nachteile: Verschlüsselte E-Mails können nicht zentral auf Viren geprüft werden, sodass die Umsetzung unternehmensweiter Sicherheitsrichtlinien erschwert wird. Außerdem kann sich die Schlüsselverwaltung für Mitarbeiter und Kommunikationspartner kompliziert gestalten und führt bei der externen E-Mail-Kommunikation evtl. zu weiteren Problemen (fehlende Infrastruktur auf der Empfängerseite, fehlende Interoperabilität der jeweils eingesetzten Verschlüsselung).

4.2 Serverbasierte Lösungen / E-Mail-Gateways

Eine serverbasierte Lösung, die alle E-Mails zentral auf einem sogenannten Secure E-Mail Gateway ver- und entschlüsselt, hat diese Probleme nicht. Eine solche Lösung, oft als „virtuelle Poststelle" bezeichnet, ist den Ende-zu-Ende-Lösungen in Bezug auf zentrale Administrierbarkeit und Entlastung der Anwender überlegen. Serverbasierte Lösungen erlauben die Umsetzung von unternehmensweiten Sicherheitsrichtlinien. In der Regel kommen hier PKI-basierte Verschlüsselungsverfahren zum Einsatz, möglich ist aber alternativ – wenn die Kommunikationspartner nicht per PKI kommunizieren – auch eine passwortgestützte Alternativverschlüsselung. Dabei werden Nachrichten oder wichtige Dokumente in ein Format konvertiert, das einen Passwortschutz bietet, z. B. PDF oder ZIP oder auf einem im Internet erreichbaren Server sicher abgelegt. Es müssen also nicht mehr Schlüssel oder Zertifikate, sondern nur noch Passwörter ausgetauscht bzw. kommuniziert werden – das aber auf einem anderen Kommunikationskanal wie z. B. per Telefon.

Zu den Nachteilen serverbasierter Verschlüsselungslösungen gehören neben den Anschaffungskosten eine anspruchsvollere Konfiguration und zum anderen der ungeschützte Transportweg der E-Mail zwischen Client und Gateway. Der muss eventuell zusätzlich abgesichert werden, wenn sich das Gateway zum Beispiel bei einem Dienstleister und nicht im eigenen Unternehmensnetzwerk befindet.



4.3 E-Mail Security as a Service

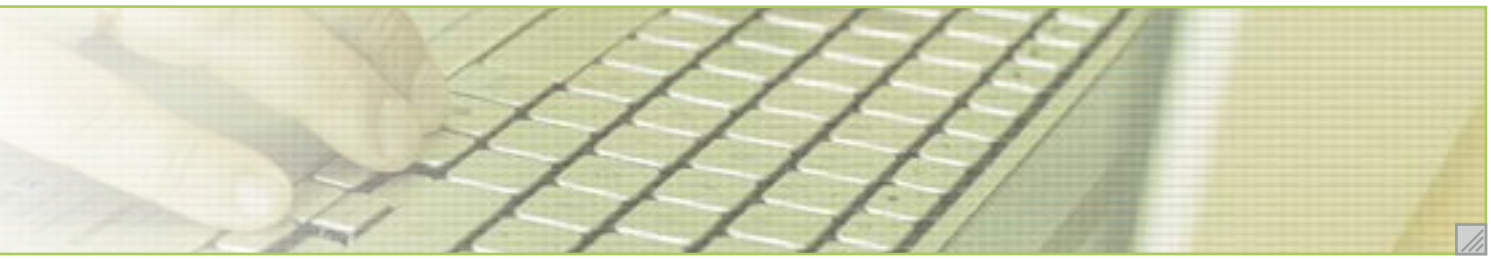
Um die unter Punkt 4.2 beschriebenen Alternativen auch für kleinere Unternehmen und Selbstständige interessant zu machen, bieten zunehmend externe Anbieter die IT-Aufgaben wie zum Beispiel die E-Mail-Verschlüsselung als „Managed Services" an. Das Modell wird auch als „Software as a Service" (SaaS) oder „cloud-basierte" Lösung bezeichnet und meint im Wesentlichen, dass die Ver- und Entschlüsselung im Rechenzentrum des jeweiligen Anbieters abläuft. Betrieb, Konfiguration und Wartung der benötigten IT-Systeme liegen beim Anbieter. Die Vorteile: Der Kunde muss die nötige Hardware und Software weder anschaffen noch einrichten und administrieren. Der Sicherheitsservice ist sofort nutzbar, Investitionskosten und Kapitalbindung sind geringer und es wird kein speziell ausgebildetes IT-Personal benötigt. Die zu erwartenden Kosten sind eindeutig kalkulierbar und wenn sich der Performance-Bedarf ändert, kann die Lösung leicht skaliert werden. Ist der Service einmal eingerichtet, werden E-Mails zentral und auf Wunsch automatisiert ver- und entschlüsselt, ohne dass sich der vertraute E-Mail-Workflow der Anwender ändert oder die Flexibilität der Geschäftsprozesse beeinträchtigt wird.

Unternehmen, die sich für einen solchen Service interessieren, müssen allerdings bei der Auswahl des richtigen Anbieters einige wichtige Punkte beachten. Der wichtigste: Sie vertrauen einem fremden Unternehmen ihre sensiblen Daten an – der gewählte Partner sollte also absolut vertrauenswürdig sein, sein zertifiziertes (z. B. nach ISO 27001) Rechenzentrum in Deutschland betreiben und natürlich auch über die notwendige Erfahrung und Leistungsfähigkeit verfügen. Die Lösung sollte dabei auch eine abgesicherte Verbindung vom eigenen Unternehmensnetzwerk zum Gateway des externen Dienstleisters bieten.

4.4 Sonderlösungen: E-Postbrief und De-Mail

Wer keine eigene Verschlüsselungsinfrastruktur betreiben möchte, kann heute auf die Dienste verschiedener Service-Provider zurückgreifen. Neben den in Kap. 4.3 dargestellten SaaS-Diensten wird im Zusammenhang mit sicherer Kommunikation oft auch auf den E-Postbrief und die De-Mail verwiesen. Allerdings ist die Sicherung der Vertraulichkeit, wie sie die E-Mail-Verschlüsselung anstrebt, nicht der Zweck dieser Angebote. Vielmehr wird neben der (unverschlüsselten) E-Mail und dem Papierbrief ein weiterer Kommunikationskanal geöffnet. Beide Dienste treten an, eine rechtssichere, datenschutzkonforme und nachweisbare digitale Kommunikation zum Beispiel mit Vertragspartnern und Behörden zu gewährleisten. Sie sollen sozusagen nicht den Briefumschlag, sondern das Einschreiben ersetzen. Die Verschlüsselung der elektronischen Kommunikation ist quasi ein Nebenprodukt.

Beide Dienste sind wahlweise über eine Web-Oberfläche oder auch per Mail-Client nutzbar. Für die verschlüsselte Kommunikation ist bei beiden Diensten ein Konto erforderlich, was einerseits die Authentizität von Absender und Empfänger sicherstellt, andererseits aber den Kreis der Kommunikationspartner auf Kontoinhaber beschränkt. Bei De-Mail sieht es noch ähnlich aus, jedoch ist der Dienst nicht auf einen einzelnen Anbieter beschränkt. Das staatlich geförderte, auf ein Projekt des Bundesinnenministeriums zurückgehende Vorhaben wird durch das De-Mail-Gesetz vom 28.4.2011 geregelt und sieht vor, dass die entsprechenden De-Mail-Dienstleistungen von entsprechend akkreditierten privaten Unternehmen angeboten werden. Die konkrete Ausgestaltung der De-Dienste und Funktionen wird sich also (im Rahmen der gesetzlichen Vorgaben) von Anbieter zu Anbieter unterscheiden.



4.5 Zusammenfassung

Für die Realisierung einer zuverlässigen E-Mail-Verschlüsselung stehen heute zahlreiche Lösungen zur Verfügung, aus denen Unternehmen in Abhängigkeit von den eigenen Anforderungen und Ressourcen die geeignetste auswählen können. Dabei ist immer auch zu prüfen, ob alle gewünschten Kommunikationspartner die verschlüsselten Nachrichten lesen können.

Clientbasierte Verschlüsselungsverfahren sind aufwendig umzusetzen und setzen entsprechende Fachkenntnisse beim Anwender voraus, erlauben aber sehr individuelle Lösungen. Die zentrale (serverbasierte) Verschlüsselungslösung per Secure E-Mail Gateway benötigt keine Software-Installation und keine besonderen Kenntnisse aufseiten der Endnutzer, eignet sich aber vor allem für größere Unternehmen mit eigener IT-Abteilung. Für kleinere Unternehmen ohne eigenes IT-Know-how bzw. wenig Personalressourcen ist eine Managed-Service-Lösung besonders interessant. Hierbei muss keine Hard- und Software angeschafft und eingerichtet werden und eine zentrale Ver- und Entschlüsselung auf dem Server des Anbieters sichert die Vertraulichkeit der Kommunikation und die Einhaltung datenschutzrechtlicher Pflichten. Nur serverbasierte und SaaS-Lösungen gestatten alternativ die Nutzung passwortgestützter Verschlüsselung, um alle potenziellen Kommunikationspartner einzubeziehen.

Herausgeber:
Deutschland sicher im Netz e. V.
Albrechtstraße 10 a
10117 Berlin
info@sicher-im-netz.de
www.sicher-im-netz.de

2015-04-01