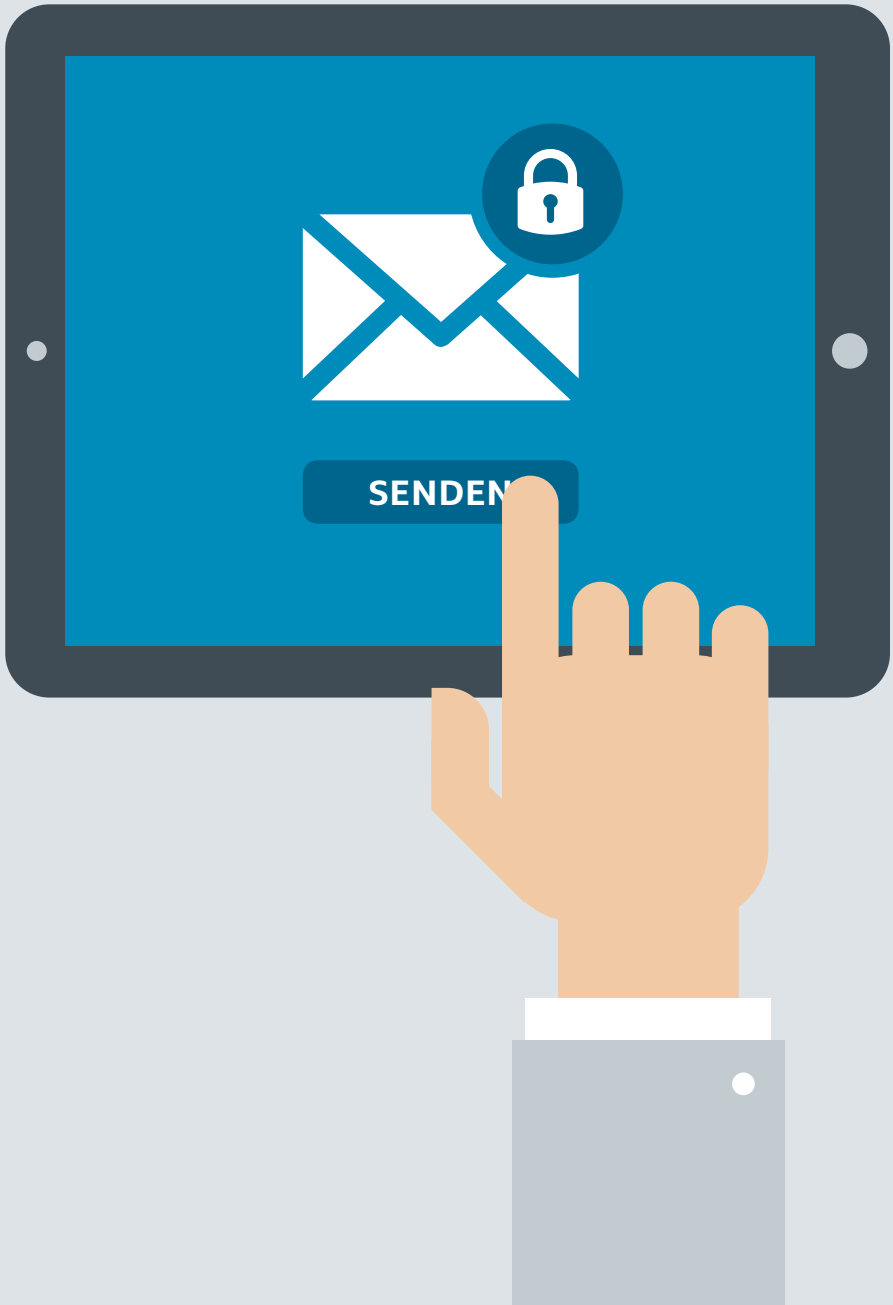
BUNDESDRUCKEREI

Verschlüsseln und signieren

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

Sichere Organisation


SENDEN

Management Summary

DATEN UND FAKTEN

96 %

DER IM RAHMEN DES DSIN-SICHERHEITSMONITORS 2015 – MITTELSTAND BEFRAGTEN UNTERNEHMEN NUTZEN E-MAIL FÜR GESCHÄFTLICHE ZWECKE.

56 %

DIESER UNTERNEHMEN HABEN KEINE VORKEHRUNGEN ZUM E-MAIL-SCHUTZ GETROFFEN,

QUELLE: Deutschland sicher im Netz (DsiN): Sicherheitsmonitor 2015 – Mittelstand

Die E-Mail ist das bevorzugte Mittel für die Übermittlung geschäftlicher Informationen. Dabei werden zunehmend auch vertrauliche und geschäftskritische Informationen versandt, zum Beispiel Rechnungen, Patente, Verträge oder Vereinbarungen. Wenn solche Daten in die falschen Hände geraten, kann das ernsthafte Konsequenzen haben – wirtschaftliche und finanzielle Nachteile, juristische Probleme und nicht zuletzt negative Auswirkungen auf Image und Glaubwürdigkeit.

Was viele nicht bedenken: Der Schutz der E-Mail-Kommunikation ist in einigen Fällen gesetzlich gefordert, wie zum Beispiel bei der elektronischen Übertragung personenbezogener Daten. Die Bedeutung rechtlicher Aspekte beim Schutz der E-Mail-Kommunikation wird zudem durch das Mitte 2015 in Kraft getretene IT-Sicherheitsgesetz weiter zunehmen.

Angesichts der Risiken und gesetzlichen Vorgaben beim elektronischen Versand sensibler Informationen ist es sehr bedenklich, dass zahlreiche Unternehmen ihre E-Mail-Kommunikation nicht oder nur unzureichend schützen. Bei kleinen und mittelständischen Unternehmen liegt der entsprechende Anteil bei über 50 Prozent. Vielen ist diese Sicherheitslücke nicht bewusst, da Internetschutz oftmals mit E-Mail-Sicherheit verwechselt wird. Firewalls, Virenscanner oder Spamschutz decken jedoch die wichtigsten Schutzbereiche der E-Mail-Kommunikation nicht ab. Um das unberechtigte Mitlesen von E-Mails, das Vortäuschen eines falschen Absenders und Manipulationen der E-Mail-Inhalte zu verhindern, sind dezidierte Maßnahmen zur Verschlüsselung von E-Mails erforderlich.

Im behördlichen und geschäftlichen Umfeld hat sich das Standardformat S/MIME für die E-Mail-Verschlüsselung fest etabliert. Es basiert auf einem asymmetrischen Verschlüsselungsverfahren mit zwei Schlüsseln. Die technische Umsetzung erfolgt über clientbasierte oder serverbasierte Verschlüsselungslösungen. Letztere verschlüsseln und entschlüsseln alle E-Mails zentral auf einem sogenannten Secure E-Mail Gateway, während bei der clientbasierten Verschlüsselung die Rechner des Absenders und Empfängers selbst die Verschlüsselungsaufgaben übernehmen. In der technischen Praxis werden beide Lösungen oft kombiniert: Gateway für Standard-E-Mails, Client für sicherheitskritische E-Mails und Anhänge.

Der Einsatz digitaler Zertifikate stellt sicher, dass die Nachricht tatsächlich vom angegebenen Absender stammt. Bei der zertifikatsbasierten Verschlüsselung wird das Schlüsselpaar mit einem digitalen Zertifikat gekoppelt, das die Identitätsinformationen des Besitzers beinhaltet (zum Beispiel Name und E-Mail-Adresse). Digitale Zertifikate sind auch die Voraussetzung dafür, E-Mails elektronisch zu unterschreiben und dadurch das signierte Dokument vor nachträglicher Veränderung zu schützen.

Das Sicherheitssystem zum Ausstellen, Verteilen und Prüfen digitaler Zertifikate wird als Public-Key-Infrastruktur (PKI) bezeichnet. Mit vielfältigen Dienstleistungen erleichtern externe Zertifizierungsdiensteanbieter, auch als Trustcenter bezeichnet, den Aufbau und Erhalt einer Public-Key-Infrastruktur. Cloud-Lösungen, wie eine „Managed PKI“, können dabei für ein effizientes Zertifikatsmanagement eingesetzt werden.

1 Bedrohungslage und Ziele

Fallstudie

Der Geschäftsführer eines traditionsreichen Unternehmens der Zuliefererbranche für die Automobilindustrie war fassungslos: Am Messestand des asiatischen Mitbewerbers entdeckte er ein Bauteil, das eins zu eins der kurz zuvor patentierten eigenen Komponente entsprach. Die Erklärung lag auf der Hand: Sein Unternehmen wurde ausspioniert.

Sofort beauftragte er einen Dienstleister für IT-Sicherheit mit der Spurensuche. Der stellte fest, dass der digitale Spionageakt über eine sorgfältig präparierte E-Mail erfolgte. Getarnt als Mitarbeiter des Unternehmens, richtete der Absender eine harmlos erscheinende Rückfrage gleich an mehrere „Kollegen“. Die gaben ihm die benötigten Informationen beflissen weiter. Und nicht nur das: Bei der Überprüfung der E-Mail-Protokolle wurde in einer zusätzlich angehängten Excel-Datei ein Trojaner entdeckt. Es genügte der Klick nur eines Empfängers auf die Datei und schon nahm der Datenklau seinen Lauf.

Für den Unternehmer endete die ganze Sache einigermaßen glimpflich. Per einstweilige Verfügung erreichte er die Entfernung der Produktfälschung von der Messe. Mithilfe der deutschen Zollbehörden konnten die patentverletzenden Bauteile an den deutschen Grenzen beschlagnahmt werden. Der asiatische Konkurrent gab die Produktion schließlich auf.

Ein irreparabler wirtschaftlicher Schaden konnte zwar verhindert werden, doch entstanden erhebliche Ausgaben für Anwalt, Privatdetektiv und IT-Dienstleister.

1.1
„Made in Germany“ gerne kopiert

DATEN UND FAKTEN

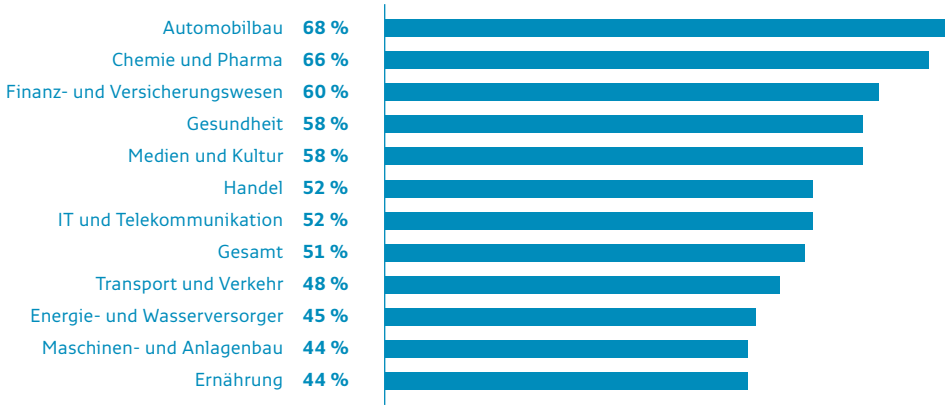
51%

ALLER UNTERNEHMEN IN DEUTSCHLAND SIND IN DEN VERGANGENEN JAHREN OPFER VON DIGITALER WIRTSCHAFTS-SPIONAGE, SABOTAGE ODER DATENDIEBSTAHL GEWORDEN.

Der geschilderte Fall von Cyberspionage ist beileibe kein Einzelfall, sondern Alltag in deutschen Unternehmen, wie eine aktuelle Studie[1] des Digitalverbandes Bitkom herausfand. Geschätzter Schaden für die deutsche Wirtschaft: 51 Milliarden Euro, das sind 1,75 Prozent des jährlichen Bruttoinlandsprodukts.

Cyberkriminalität ist nicht nur für große Unternehmen, sondern auch für den Mittelstand ein Risiko, wie die Beratungsgesellschaft PricewaterhouseCoopers in einer Ende 2015 veröffentlichten Umfrage unter 400 mittelständischen Unternehmen feststellte.[2] Demnach wurde 2015 jeder zehnte Mittelständler mindestens einmal Opfer einer Attacke aus dem Internet. Im Durchschnitt entstand bei jedem Angriff ein wirtschaftlicher Schaden von 80.000 Euro. In einzelnen Fällen summierte er sich sogar auf mehr als 500.000 Euro.

Betroffene Unternehmen nach Branchen



1 – Bitkom: Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter 2015 www.bitkom.org/Bitkom/Publikationen/Spionage-Sabotage-und-Datendiebstahl-Wirtschaftsschutz-im-digitalen-Zeitalter.html

2 – PricewaterhouseCoopers (PwC): Angriff aus dem Cyber Space: So gefährdet sind mittelständische Unternehmen www.pwc-wissen.de/pwc/de/shop/publikationen/

QUELLE DER GRAFIK
Bitkom 2015: Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter
Basis: alle befragten Unternehmen (n = 1.074)

QUELLE DES KASTENS
www.bundesdruckerei.de/id-kompass/glossar

KURZ UND BÜNDIG

Trojaner

Als Trojanisches Pferd, im EDV-Jargon auch kurz Trojaner genannt, bezeichnet man ein Computerprogramm, das hinter seiner eigentlichen Funktion weitere Anwendungen versteckt, die nicht dokumentiert sind. Trojanische Pferde zählen zu den schädlichen Programmen, der sogenannten Malware. Trojaner werben mit den nützlichen Funktionen ihres Wirtsprogramms. Häufig verbergen sie sich im Anhang von E-Mails. Einmal ausgeführt, verändern oder löschen sie Programme, bspw. Systemeinstellungen, spionieren Passwörter aus und versenden diese.

Peter Bartels, Vorstandsmitglied von PwC:

„Viele Mittelständler haben den Ernst der Lage noch nicht erkannt und verfügen weder über ausreichende technische Sicherheitsmaßnahmen noch über einen angemessenen Versicherungsschutz."

Neben den entstandenen materiellen Schäden gibt es auch noch eine Reihe von immateriellen Risiken, die von Unternehmen häufig unterschätzt werden.

DATEN UND FAKTEN

52%

DER DEUTSCHEN UNTERNEHMEN ERWARTEN EINEN ANSTIEG DER BEDROHUNG DURCH INDUSTRIESPIONAGE.

Risiken von Cyberspionage

MATERIELLE RISIKEN

- → Ausfall und Schädigung der IT
- → Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen
- → Kosten für Rechtsstreitigkeiten und IT-Dienstleister
- → Datenschutzrechtliche Maßnahmen

IMMATERIELLE RISIKEN

- → Patentrechtsverletzungen
- → Imageschäden bei Kunden oder Lieferanten
- → Negative Medienberichterstattung
- → Höhere Mitarbeiterfluktuation

Und auch für die Zukunft sind die deutschen Unternehmen eher skeptisch, wie eine Umfrage von Corporate Trust[3] herausgefunden hat. Demnach erwarten über 52 Prozent der deutschen Unternehmen in den nächsten Jahren einen Anstieg der Bedrohung durch Industriespionage. Diese Einschätzung wird auch von IT-Analysten und IT-Beratern geteilt. Dabei werden neue Gefahrenbereiche stärker in den Mittelpunkt rücken.

3 – Corporate Trust: Industriespionage 2014 – Cybergeddon der Wirtschaft durch NSA & Co. www.corporate-trust.de/index.php/de/presse-n-medien/studien

PwC: Angriff aus dem Cyber Space: So gefährdet sind mittelständische Unternehmen:

„Basierend auf internationalen Vergleichswerten dürften Übergriffe auf Kundendaten und Vertragskonditionen sowie geistiges Firmeneigentum in den kommenden Jahren deutlich zunehmen."

1.2
Einfallstor E-Mail

DATEN UND FAKTEN

41%

MIT 41% WIRD DAS ABHÖREN UND ABFANGEN VON ELEKTRONISCHER KOMMUNIKATION ALS ZWEITHÄUFIGSTE SPIONAGEAKTION IN DEUTSCHEN UNTERNEHMEN GENANNT.

Eine der größten Schwachstellen in der IT-Infrastruktur und Einfallstor für viele Spionageaktionen sind E-Mails. Die in der Corporate-Trust-Studie befragten deutschen Unternehmen bezeichnen das Abhören und Abfangen von elektronischer Kommunikation als zweithäufigste Angriffsform (41,1 Prozent), nur kurz hinter den Hackerangriffen auf EDV-Systeme und -Geräte (49,6 Prozent). Trotz dieses großen Gefahrenpotenzials sind die Vorkehrungen zum Schutz von E-Mails mangelhaft, besonders bei klein- und mittelständischen Unternehmen.

Initiative Deutschland sicher im Netz e.V.:

„Es besteht ein enormer Handlungsbedarf bei der Absicherung von Daten und Informationen durch Verschlüsselung."

Die Initiative Deutschland sicher im Netz e.V. (DsiN) spricht in ihrem aktuellen Sicherheitsmonitor 2015[4] von einem „besorgniserregend niedrigen Niveau". In der Rangliste der implementierten Schutzmaßnahmen liegt die E-Mail-Sicherheit an letzter Stelle. Und die Tendenz, Sicherheitsvorkehrungen bei E-Mails zu treffen, war im Zeitraum von 2011 bis 2014 rückläufig.

Die fehlende E-Mail-Sicherheit steht im scharfen Kontrast zum ungebremsten Wachstum der E-Mail-Nutzung. 96 Prozent der im Rahmen des DsiN-Sicherheitsmonitors 2015 befragten Unternehmen nutzen E-Mail für geschäftliche Zwecke, zunehmend auch für die Übermittlung sensibler Informationen, wie Geschäftsbriefe, Verträge und Verfahrensdokumentationen.

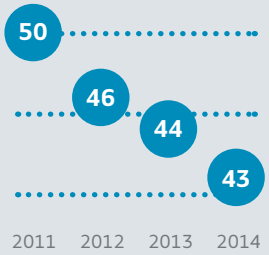
Diese Diskrepanz basiert auf einer gewissen Passivität in vielen Unternehmen, als Reaktion auf die öffentlich diskutierten Sicherheitsvorfälle sowie auf die Enthüllungen über Geheimdienstaktivitäten. Ein hoher Sicherheitsgrad, so die fatalistische Einstellung, ist sowieso nicht erreichbar. Der Hauptgrund für die Sorglosigkeit im Umgang mit E-Mails liegt jedoch in einem großen Missverständnis. Viele Unternehmen denken, dass die Sicherung des Internetzugangs gleichbedeutend sei mit dem Schutz von E-Mails. Doch konzentrieren sich Lösungen für den Internetschutz schwerpunktmäßig auf Gefährdungen von außen. Die wichtigsten Schutzelemente sind Virenscanner, Spamschutz und Firewalls. Damit wird aber nur ein Teil der potenziellen Gefahren berücksichtigt, wie Schadprogramme, Überlastung durch eingehende E-Mails oder der Missbrauch aktiver Inhalte in E-Mails.

Eine Vielzahl von Gefährdungen wird durch den Internetschutz nicht abgedeckt. 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.

Internetschutz bietet keine E-Mail-Sicherheit. E-Mail-Verschlüsselung ist daher für jedes Unternehmen zumindest bei geschäftskritischen Informationen Pflicht.

4 – Deutschland sicher im Netz (DsiN): Sicherheitsmonitor 2015 – Mittelstand www.sicher-im-netz.de/downloads/dsin-sicherheits-monitor-mittelstand-2015

Vier-Jahres-Vergleich:
Datensicherung während der E-Mail-Übertragung in Prozent



1.3
Schutzziele und rechtliche Aspekte

Die Ziele der E-Mail-Verschlüsselung beziehen sich auf die Schutzbereiche 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.

Mit der **Integrität einer E-Mail** ist die Gewissheit gemeint, 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.

Die Schutzziele der E-Mail-Verschlüsselung

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.

Authentizität und Integrität sind für den Geschäftsverkehr von großer Bedeutung. Denn Willenserklärungen per E-Mail besitzen die gleiche Rechtswirksamkeit wie mündliche oder schriftliche Erklärungen, solange der Gesetzgeber keinen Formzwang vorschreibt.

Die gesamte in E-Mails gehaltene Geschäftskorrespondenz eines Unternehmens gilt als Handelsbrief im Sinne des Handelsgesetzbuchs (§ 238 Abs. 2). Bei der Übermittlung von geschäftlichen Willenserklärungen, Informationen und Dokumenten sollte man deshalb dafür sorgen, dass Inhalte und Absenderinformationen nicht durch Dritte verändert werden können.

Auch aus dem Bundesdatenschutzgesetz ergeben sich Vorgaben für die Festsetzung von IT-Sicherheitsstandards. Betroffen ist die Verarbeitung personenbezogener Daten, zum Beispiel von Finanzbuchhaltungsdaten. Dabei ist durch technische und organisatorische Maßnahmen, insbesondere durch „die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren", sicherzustellen, „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 BDSG).

§ 43 GmbHG, §§ 91, 93, 116 AktG:

Verstöße gegen eine Verschlüsselungspflicht können Unterlassungs- und Schadenersatzansprüche zur Folge haben. In diesem Fall ist es möglich, dass die Firmenleitung des verurteilten Unternehmens persönlich haften muss.

Das Mitte 2015 in Kraft getretene IT-Sicherheitsgesetz sieht weitere regulatorische Vorgaben zur Informationssicherheit vor. Das Gesetz gilt zwar zunächst für die Betreiber sogenannter Kritischer Infrastrukturen – zum Beispiel Wasser, Energie, Telekommunikation, Gesundheit, Transport und Verkehr. Es wird aber aufgrund der zunehmenden Digitalisierung seinen Geltungsbereich kontinuierlich ausdehnen. Mittelfristig ist daher zu erwarten, dass Unternehmen gezwungen sein werden, den Anforderungen des IT-Sicherheitsgesetzes auch dann zu entsprechen, wenn sie nicht direkt zu den Kritischen Infrastrukturen gehören.

GUT ZU WISSEN

Das IT-Sicherheitsgesetz

Das IT-Sicherheitsgesetz[5] ist 2015 in Kraft getreten. Zweck dieses Gesetzes ist die „signifikante Verbesserung der Sicherheit informationstechnischer Systeme (IT-Sicherheit) in Deutschland" und der „Schutz Kritischer Infrastrukturen, welche gerade für das Funktionieren des Gemeinwesens zentral sind".

Das Gesetz regelt unter anderem, dass Betreiber sogenannter Kritischer Infrastrukturen ein Mindestniveau an IT-Sicherheit einhalten und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) IT-Sicherheitsvorfälle melden müssen.

Tun sie dies nicht, droht ihnen ein Bußgeld. § 8 a verpflichtet sie dazu, „organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen".[6]

5 – IT-Sicherheitsgesetz: docs.dpaq.de/10168-bgbl115s1324_109747.pdf

6 – Mehr Informationen zum Sicherheitsgesetz im Whitepaper der Bundesdruckerei „Einführung eines Informationssicherheits-Management-Systems (ISMS) bei Energieversorgern": www.bundesdruckerei.de/digitalisierung/whitepaper/whitepaper-isms

2 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 orientieren sich an den ausgegebenen 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?

2.1
Schutz der Vertraulichkeit

2.1.1 Asymmetrische und symmetrische Verschlüsselung

Grundsätzlich unterscheidet man zwischen symmetrischer und asymmetrischer Verschlüsselung.

Beim symmetrischen Verschlüsselungsverfahren verwenden Absender und Empfänger den gleichen Schlüssel. Die Sicherheit dieses Verfahrens ist an die Geheimhaltung des Schlüssels gebunden. Das birgt Gefahren, denn jeder, der in Besitz des Schlüssels kommt, kann die Nachricht entschlüsseln. Besonders der Austausch des geheimen Schlüsselmaterials stellt einen großen Risikofaktor dar.

Ein weiterer Nachteil im Unternehmensbereich ist die sehr große Menge an benötigtem Schlüsselmaterial. Denn für jeden Kommunikationsweg zwischen zwei Personen ist ein eigener Schlüssel notwendig. In einem typischen Mittelstandsunternehmen geht die Anzahl der benötigten Schlüssel allein für die Verschlüsselung der internen Kommunikation leicht über die Millionengrenze (siehe Grafik).

Zu verteilende Schlüssel bei den beiden Verfahren

Verschlüsselung	12 Mitarbeiter	2.000 Mitarbeiter
Symmetrisch	66	1,9 Millionen
Asymmetrisch	12	2.000

Das Schlüsselverteilungsproblem wird durch das asymmetrische Verfahren gelöst. Dabei gibt es immer zwei sich ergänzende Schlüssel:

→ **Den öffentlichen Schlüssel (Public Key)** für das Verschlüsseln der Nachricht.

→ **Den privaten Schlüssel (Private Key)** für das Entschlüsseln der Nachricht.

Beide Schlüssel stehen in einer bestimmten mathematischen Abhängigkeit zueinander. Mithilfe des sogenannten RSA-Verfahrens ist der private Schlüssel nicht aufgrund der Kenntnis des öffentlichen Schlüssels errechenbar (siehe Kasten „Gut zu Wissen“ Seite 12).

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.

GUT ZU WISSEN

Der RSA-Standard

RSA ist ein weit verbreiteter Standard in der asymmetrischen Verschlüsselung, benannt nach den Entwicklern Ron L. Rivest, Adi Shamir und Leonard Adleman. Vereinfacht ausgedrückt werden beim RSA-Verfahren zwei Primzahlen miteinander multipliziert.

Das Ergebnis (Produkt) entspricht dem öffentlichen Schlüssel (Public Key), die beiden Primzahlen (Faktoren) sind der private Schlüssel (Private Key). Mathematisch ist es speziell bei großen Zahlen nicht möglich, die beiden Primzahlen (Faktoren) aus der Kenntnis des Endergebnisses (Produkt) zu berechnen.

Die Sicherheitsniveaus werden in Form von Schlüssellängen beschrieben, beispielsweise RSA-1024 oder RSA-2048. Mathematisch bedeutet das die Faktorisierung (Faktor x Faktor = Produkt) von Primzahlen mit 309 Dezimalstellen (RSA-1024) beziehungsweise 617 Dezimalstellen (RSA-2048).[7]

7 – Siehe people.csail.mit.edu/rivest/Rsapaper.pdf

2.1.2 Client- und serverbasierte Verschlüsselungslösungen

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

Bei ersteren übernehmen die Endgeräte, ausgestattet mit entsprechender Software, selbst das Verschlüsseln, das Entschlüsseln sowie auch das Signieren und Verifizieren. Dieser Ansatz bietet die durchgängige Verschlüsselung einer E-Mail über ihren gesamten Übertragungsweg und wird daher auch als Ende-zu-Ende-Verschlüsselung (End to End) bezeichnet.

Das Resultat ist eine hohe Sicherheit gegen Manipulationen, aber auch ein höherer Aufwand für die Schlüsselverwaltung und die Administration der Clients, speziell im Vergleich zu serverbasierten Lösungen.

Dabei übernehmen E-Mail-Gateways die Verschlüsselungs- und Entschlüsselungsaufgaben, der Anwender bekommt von diesen Aktivitäten nichts mit. Der Vorteil liegt vor allem in der einfachen Handhabung. Dafür ist jedoch keine Ende-zu-Ende-Sicherheit gegeben, da der Transportweg zwischen Client und E-Mail-Gateway ungeschützt ist oder die Nachricht teilweise ungesichert gespeichert wird.

In der Charta zur Stärkung der vertrauenswürdigen Kommunikation, die von Bundesinnenminister Thomas de Maizière sowie Wirtschafts- und Forschungsvertretern unterzeichnet wurde, wird ausdrücklich die clientbasierte Verschlüsselungstechnologie favorisiert.[8]

8 – Charta zur Stärkung der vertrauenswürdigen Kommunikation: www.bundesregierung.de/Content/Infomaterial/BMI/charta-vertrauenswuerdige-kommunikation_7051680.html

GUT ZU WISSEN

Die Charta zur Stärkung der vertrauenswürdigen Kommunikation

Die Charta zur Stärkung der vertrauenswürdigen Kommunikation wurde auf dem IT-Gipfel im November 2015 vorgestellt. Sie enthält die klare Zielvorgabe, für mehr Sicherheit und Schutz im Netz zu sorgen. Konkret legen die Unterzeichner von Bundesregierung, Wirtschaft und Forschern Folgendes fest:

„Wir stellen sichere Infrastrukturen zur Verfügung, um die eigene Identität im Netz besser zu schützen und sicher zu kommunizieren (...) Wir unterstützen mehr und bessere Verschlüsselung. Wir wollen Verschlüsselungs-Standort Nr. 1 auf der Welt werden."

Dabei geben die Unterzeichner unter anderem ein Bekenntnis zur Bedeutung des Themas, zur Nutzerfreundlichkeit, zur Technologieneutralität und Standardkonformität, zu Innovation sowie zu „Security Made in Germany/Europe" ab.

2.2
Schutz der Authentizität und Integrität

2.2.1. 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, und jemand fälschlicherweise behaupten könnte, er sei der berechtigte Empfänger. Für die falsche Identität ließen sich problemlos Schlüsselpaare generieren und Public Keys in Umlauf bringen. Der Fälscher könnte dann vertrauliche Botschaften lesen, weil die Absender seinen Schlüssel genutzt haben, statt den des eigentlichen Empfängers. Wie kann der Absender, der den öffentlichen Schlüssel des Empfängers zum Verschlüsseln nutzt, sicher sein, dass er auch wirklich dem Empfänger gehört?

KURZ UND BÜNDIG

Das Man-in-the-Middle-Problem

Auf Deutsch: Mann in der Mitte; ein unbefugter Dritter schaltet sich unbemerkt in die Kommunikation zwischen zwei Partnern ein, die einander vertrauen. Der Man in the Middle täuscht beiden Seiten vor, der jeweils andere Kommunikationspartner zu sein. Sein Ziel ist es, den Kommunikationskanal und damit auch den Datenverkehr zu kontrollieren, um an sensible Informationen zu gelangen.

QUELLE
www.bundesdruckerei.de/id-kompass/glossar

Die Antwort auf oben gestellte Frage und die Lösung für die beschriebene Man-in-the-Middle-Problematik ist das Modell der Public-Key-Infrastruktur (PKI). Bei dieser 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.

Public-Key-Infrastrukturen 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 zueinander kompatibel. Anwender müssen sich daher für das eine oder 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.

Bei S/MIME findet dies durch eine hierarchische Kette von Zertifizierungsinstanzen statt. Das letzte Glied einer solchen Kette wird als Wurzelzertifizierungsstelle bezeichnet. Dagegen sieht OpenPGP 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 ergreifen. Zudem muss bei der Generierung der Schlüssel darauf geachtet werden, dass es zu keiner Kompromittierung durch Angreifer kommen kann.

KURZ UND BÜNDIG

Digitale Zertifikate

Digitale Zertifikate sind elektronische Bescheinigungen, die von einer Zertifizierungsinstanz ausgestellt und signiert wurden und die dem Zertifikatsinhaber bestimmte Informationen zuordnen. Das gebräuchlichste Zertifikatformat ist X.509.

QUELLE
www.bundesdruckerei.de/id-kompass/glossar

Die Rolle der vertrauenswürdigen Instanz bei S/MIME-Verschlüsselungsverfahren übernehmen in Deutschland sogenannte Trustcenter, die verschiedene Zertifizierungsdienstleistungen anbieten. Deshalb werden sie auch als Zertifizierungsdiensteanbieter bezeichnet. Trustcenter unterliegen strengen gesetzlichen Regelungen und müssen eine breite Palette an Sicherheitsanforderungen erfüllen. Sie geben die individuellen Schlüsselpaare heraus, verknüpfen sie mit der Identität einer Person und halten diese Daten dauerhaft zur Verfügung. Ausgeliefert werden die so entstandenen Personenzertifikate entweder als elektronische Datei oder auf einem Speichermedium, meistens einer Signaturkarte.

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

2.2.2 Digitale Signatur[9]

9 – Siehe zum Thema auch das Whitepaper der Bundesdruckerei „Elektronisch unterschreiben – rechtssicher und komfortabel“ www.bundesdruckerei.de/digitalisierung/whitepaper/whitepaper-elektronisch-unterschreiben

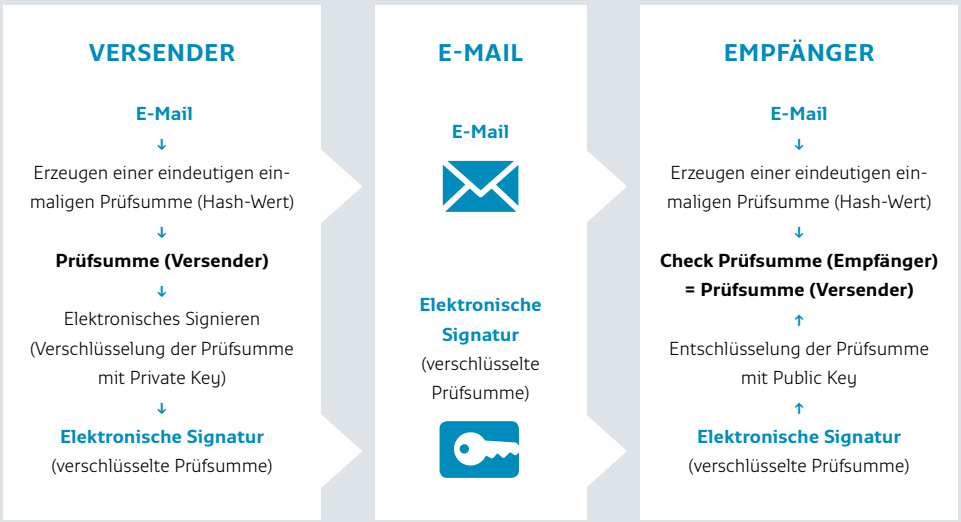
Personenzertifikate sind Voraussetzung dafür, elektronische Signaturen zu erzeugen und damit eine Nachricht zu unterschreiben. Mithilfe elektronischer Signaturen lässt sich die Identität des Absenders verifizieren und das unterschriebene Dokument vor nachträglicher Veränderung schützen. Dadurch werden die Schutzziele der Authentizität und der Integrität erfüllt.

Dies lässt sich gut anhand des skizzierten Datendiebstahls am Anfang des Whitepapers verdeutlichen. Bei einer signierten E-Mail wäre die falsche Identität des Versenders sofort aufgefallen. Der Versuch des Datenklaus über den Trojaner wäre erfolglos geblieben. Zudem wären die per verschlüsselter E-Mail übersandten Informationen für den Angreifenden nicht lesbar und damit unbrauchbar gewesen.

Technisch funktioniert das Verfahren der elektronischen Signatur mit asymmetrischer Verschlüsselung wie folgt:

1. Um eine Signatur zu erzeugen, wird zunächst aus den zu signierenden Daten eine Prüfsumme fester Länge, der sogenannte Hash-Wert, gebildet. Bei unverändertem Inhalt des Dokuments führt die Hash-Berechnung immer zum selben Ergebnis.
2. Der Unterzeichner verschlüsselt dann mit seinem privaten Schlüssel den Hash-Wert und verbindet diesen zusammen mit dem Zertifikat des Unterschreibenden sowie dem Ursprungsdokument. Alle bilden gemeinsam das elektronisch unterschriebene Dokument.
3. 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.
4. Die Authentizität des Urhebers wird mithilfe desselben Mechanismus verifiziert, indem die elektronische Signatur des Zertifikats geprüft wird.

Funktionsweise der elektronischen Signatur



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 Inhaltes aus dem Hash-Wert ist nicht möglich. Man kann jedoch anhand des Hash-Wertes vergleichen, ob zwei Dateien identisch sind. Damit ist ein Hash-Wert vergleichbar mit einem Fingerabdruck – nur eben für eine Datei.

Digitale Signaturen sind Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden und die der Unterzeichner zum Unterschreiben verwendet. Nur digitale Signaturen stellen sicher, dass Inhalte nicht durch Dritte verändert werden können.

Der Zusammenhang zwischen den Schutzzielen der E-Mail-Verschlüsselung sowie den technischen Verfahren und Standards wird in der folgenden Grafik zusammengefasst:

Schutzziele, Verfahren und Standards

SCHUTZZIEL	VERFAHREN	STANDARD
Vertraulichkeit	**Symmetrische Verschlüsselung**	**RSA**
	Asymmetrische Verschlüsselung → Clientbasierte Verschlüsselung → Serverbasierte Verschlüsselung	**RSA**
Authentizität und Verbindlichkeit	**Digitale Zertifikate mittels PKI**	**S/MIME** (Unternehmen und Behörden) **OpenPGP** (Privatbereich)
Integrität	**Digitale Signaturen**	

3 Handlungsempfehlungen

Die E-Mail-Verschlüsselung kann auf eine solide technische und rechtliche Grundlage bauen. Die Verfahren sind ausgereift, die Standards sind klar definiert und unabhängige Instanzen in Form der Trustcenter sorgen für Sicherheit und Vertrauenswürdigkeit.

Darüber hinaus gibt es eine Vielzahl von Softwareprogrammen 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

Im ersten Schritt gilt es, in der Organisation ein Bewusstsein für da E-Mail-Verschlüsselung zu schaffen, Ziele zu definieren und ein Konzept für die Umsetzung zu erstellen.

In einem Basisworkshop 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 essentiell sind. Dazu gehört auch die Bestimmung der entscheidenden fünf bis zehn Prozent der Daten, die zu den Kronjuwelen eines Unternehmens gehören. Für sie sind Verschlüsselungsverfahren auf höchstem Sicherheitsniveau zu wählen.

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

All diese Erkenntnisse finden Eingang 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

Asymmetrische Verschlüsselungsverfahren sind aufgrund der Vorteile bei der Schlüsselverteilung (besserer Schutz gegen Missbrauch) und Schlüsselverwaltung (deutlich geringeres Schlüsselaufkommen) im geschäftlichen Umfeld eindeutig die erste Wahl.

Sollen die E-Mails clientbasiert oder am Gateway verschlüsselt werden? So lautet die nächste Frage, die sich dem Anwender stellt. Eine serverbasierte Lösung, die alle E-Mails zentral auf einem sogenannten Secure E-Mail Gateway ver- und entschlüsselt, ist einfach zu handhaben und zu administrieren. Die gesamten Verschlüsselungsvorgänge laufen über einen Server automatisiert ab, ohne dass der einzelne Anwender eingreifen muss.

Zu den Nachteilen serverbasierter Lösungen gehört neben der anspruchsvolleren Konfiguration in Konstellationen, bei denen individuelle Regelungen für verschiedene Anwender definiert werden, vor allem der ungeschützte Transportweg der E-Mail zwischen Client und Gateway. Administratoren und andere Mitarbeiter haben Zugriff auf die Mails.

Weiterhin sind serverbasierte Lösungen für den Einsatz digitaler Signaturen nur bedingt geeignet, da der Anwender hierbei nicht direkt und auch nur im Einzelfall seine elektronische Unterschrift autorisiert.

Deshalb empfiehlt sich für Inhalte, die ein sehr hohes Sicherheitsniveau benötigen und bei denen Signaturen eingesetzt werden, die clientbasierte Verschlüsselung. Dieser Ansatz ermöglicht die durchgängige Verschlüsselung einer E-Mail über ihren gesamten Übertragungsweg und wird daher auch als Ende-zu-Ende-Verschlüsselung bezeichnet.

In der Praxis lassen sich beide Lösungen miteinander kombinieren: Gateway für Standard-Mails und -Dokumente, Client für besonders sicherheitskritische E-Mails und Anhänge.

Die Auswahl der Software richtet sich nach dem eingesetzten Standardformat der Verschlüsselung, S/MIME oder OpenPGP. Beide Standards sind nicht miteinander kompatibel. Für den geschäftlichen Austausch von verschlüsselten Nachrichten hat sich S/MIME durchgesetzt.

Der Markt bietet eine Vielzahl an Programmen, die eine S/MIME-Verschlüsselung unterstützen. Das gilt bereits für Native Clients wie Outlook und Notes. Doch bieten diese Standardlösungen oft nicht die Funktionalitäten, die für einen Betrieb mit hohen Sicherheitsanforderungen notwendig sind. Zusätzlich existieren beim Einsatz von Zertifikaten und Signaturen häufig erhebliche Einschränkungen.

Wichtige Bestandteile des Funktionsumfangs sollten sein:

1. Verschlüsselung der gesamten E-Mail einschließlich Anhang (einige Programme verschlüsseln nur die Inhalte der E-Mail, nicht aber angehängte Dateien und Dokumente).
2. Einheitliche Administration aller Verschlüsselungs- und Signaturfunktionalitäten.
3. Ein sehr hohes Sicherheitsniveau bedingt die Zulassung für VS-NfD (Verschlusssache – Nur für den Dienstgebrauch).
4. Flexibler Smartcard-Support, wenn die zur Verschlüsselung und zum Signieren von E-Mails genutzten Schlüssel sich auf einer Smartcard befinden.
5. ISIS-MTT-Konformität: ISIS-MTT ist ein deutscher Standard für die Verschlüsselung und das Signieren von E-Mails, der vor allem im Behördenumfeld eine wichtige Rolle spielt.
6. OCSP-Unterstützung: Mit diesem Protokoll (OCSP – Online Certificate Status Protocol) kann in Echtzeit überprüft werden, ob der Schlüssel (beziehungsweise das digitale Zertifikat) eines anderen Anwenders gesperrt ist.

IN EIGENER SACHE

Die Verschlüsselungslösung s/mail[10]

s/mail ist eine Software zur Ende-zu-Ende-Verschlüsselung und zum Signieren von E-Mails im professionellen Umfeld. Sie ist als Erweiterung (Plug-in) für gängige E-Mail-Clients in der Windows-Welt konzipiert.

Laut Prüfung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) erfüllt die Software sehr hohe Sicherheitsstandards. Sie hat als erste Verschlüsselungslösung die Zulassung für VS-NfD erhalten. s/mail nutzt das Standardformat S/MIME und unterstützt den Zertifikatsstandard X.509 und den Behördenstandard ISIS-MTT. Damit lässt sie sich unkompliziert in eine Public-Key-Infrastruktur (PKI) integrieren.

Bei aller Funktionsvielfalt ist s/mail einfach zu handhaben. So verfügt die Software unter anderem über eine leicht zu bedienende Benutzeroberfläche. Zentrale Konfigurationen lassen sich bequem über Gruppenrichtlinien verteilen und gewährleisten eine einheitliche Administration. Die Verschlüsselungslösung s/mail ist eine Entwicklung der Bundesdruckerei-Beteiligung cryptovision.

10 – Verschlüsselungslösung s/mail: www.cryptovision.com/products/smail/

Schritt 3

Zertifikate und Signaturen besorgen

Die Schutzziele der Authentizität und der 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 Zertifizierungsdiensteanbieter, ein sogenanntes Trustcenter, zurückzugreifen. Dort erhalten Anwender die notwendigen Mittel für das Verschlüsseln und Signieren von E-Mails.

Wer einen Teil seines elektronischen E-Mail-Verkehrs serverbasiert absichern will, kann Gateway oder Personenzertifikate einsetzen. Dafür können Zertifikate auf dem E-Mail-Gateway des Unternehmens gegebenenfalls auch automatisiert zur Verfügung gestellt werden. Alle E-Mails, die diesen Server passieren, werden automatisch mit einer digitalen Signatur versehen und mit einem hochsicheren Verfahren verschlüsselt.

Durch die Unterstützung des X.509-Standards ist die Interoperabilität mit anderen Systemen und Infrastrukturen sichergestellt. Gateway-Zertifikate sind nicht personengebunden, sondern auf den Namen einer Organisation ausgestellt.

Für die clientbasierte Ende-zu-Ende-Verschlüsselung bieten sich Personenzertifikate an. Sie sind entweder als Softtoken oder gespeichert auf einer Signaturkarte erhältlich. Softtoken enthalten die Zertifikate und das Schlüsselmaterial und werden als Datei (zum Beispiel per E-Mail) ausgeliefert oder sind bequem über Selfservice-Portale durch die Unternehmen zu beziehen. Softtoken lassen sich in fast allen gängigen Browsern und S/MIME-konformen E-Mail-Clients verwenden.

Eine Signaturkarte erhöht das Sicherheitsniveau und erweitert die Anwendungsmöglichkeiten.

Sie enthält ein Zertifikat zur Authentifizierung, zum Verschlüsseln und für den Einsatz zur E-Mail-Signatur. Auch zusätzliche Zertifikate, wie z. B. qualifizierte Zertifikate, können auf den gleichen Karten aufgebracht werden.

Trustcenter – wie z.B. D-TRUST der Bundesdruckerei – bieten die Basis für sichere Public-Key-Infrastrukturen (PKI). Neue Angebote und Dienste – wie die Möglichkeit Zertifikate Online zu beziehen und zu verwalten (siehe Kasten „Managed PKI“) – erleichtern den Einsatz von Verschlüsselungstechnik.

IN EIGENER SACHE

Managed PKI

Die Lösung Managed PKI der Bundesdruckerei bietet ein effizientes Zertifikatsmanagement aus der Cloud und richtet sich besonders an kleine und mittelgroße Organisationen. Diese können mit dem als „Public Key Infrastructure as a Service“ konzipierten Dienst jetzt auch von den Vorteilen moderner, hochsicherer Verschlüsselungs-, Signatur- und Authentifizierungslösungen profitieren.

Über Standardschnittstellen lassen sich bestehende Infrastrukturen und Systeme an die Public-Key-Infrastrukturen der Bundesdruckerei anbinden. Die Lösung ermöglicht es, Zertifikate für elektronische Identitäten einfach und sicher im akkreditierten Trustcenter D-TRUST der Bundesdruckerei zu erstellen und manuell oder automatisiert zu beziehen.

Über einen integrierten Prüfdienst können Anwendungen und Geschäftspartner jederzeit die Echtheit und Gültigkeit der Zertifikate überprüfen.

Schritt 4

Vertrauensanker nutzen

Trustcenter fungieren in der digitalen Welt als Vertrauensanker, indem sie die Identität einander unbekannter Personen zuverlässig beglaubigen und die entsprechenden Daten sicher verwalten. Gleichzeitig stellen sie die Mittel und die Infrastruktur bereit, um zuverlässig und sicher E-Mails zu verschlüsseln und Dokumente zu signieren.

Trustcenter müssen sich bei der Bundesnetzagentur akkreditieren lassen. Damit wird sichergestellt, dass sie die hohen Anforderungen an Sicherheit und Betrieb des deutschen Signaturgesetzes erfüllen.

Als Full-Service-Anbieter helfen sie in allen Fragen rund um die E-Mail-Verschlüsselung, ob mit Beratung oder mit technischen Lösungen. Die aktuelle Liste der Zertifizierungsdiensteanbieter findet sich auf der Website der Bundesnetzagentur.[11]

11 – Siehe: www.bundesnetzagentur.de/DE/Service-Funktionen/QualifizierteelektronischeSignatur/WelcheAufgabenhatdieBundesnetzagentur/AufsichtundAkkreditierungvonAnbietern/01_Auflistung_aktuelle_ZDA.html

Schlusswort

Was wäre wenn?

Was wäre, wenn der Automobilzulieferer vom Anfang des Whitepapers ein E-Mail-Verschlüsselungsverfahren eingesetzt hätte?

Eine asymmetrische Verschlüsselung mit Public-Key-Infrastruktur (PKI) bietet in diesem Fall doppelten Schutz. So wäre die falsche Identität bei einer verschlüsselten und signierten E-Mail sofort aufgefallen. Wird ein digitales Zertifikat erwartet, ruft sein Fehlen sofort Skepsis in Bezug auf die vermeintliche Identität des Absenders hervor. Bei fehlerhaften Signaturen wird der Empfänger bereits durch das E-Mail-Programm auf Unstimmigkeiten hingewiesen. Ist ein digitales Zertifikat mit Signatur vorhanden, kann der Empfänger durch Abfrage beim zuständigen Trustcenter einfach feststellen, ob die Identität des Absenders echt ist.

Wurden Informationen versehentlich an den Angreifer geschickt, sind aber vorab mit dem Schlüssel des richtigen Adressaten verschlüsselt worden, wären sie zumindest durch den Angreifer nicht lesbar. Denn auch hier ist der private Schlüssel des adressierten Mitarbeiters notwendig, um die Nachricht zu entschlüsseln.

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

BUNDES DRUCKEREI

Kontakt

Bundesdruckerei GmbH
Kommandantenstraße 18
10969 Berlin
Tel.: +49 (0) 30 – 25 98 – 18 30
Fax: +49 (0) 30 – 25 98 – 22 05
sales@bdr.de
www.bundesdruckerei.de