Fraunhofer
SIT

FRAUNHOFER-INSTITUT FÜR SICHERE INFORMATIONSTECHNOLOGIE

SIT TECHNICAL REPORTS

VERTRAULICHKEITSSCHUTZ DURCH VERSCHLÜSSELUNG

STRATEGIEN UND LÖSUNGEN FÜR UNTERNEHMEN

03/2015

FRAUNHOFER VERLAG

VERTRAULICHKEITSSCHUTZ DURCH VERSCHLÜSSELUNG

Strategien und Lösungen für Unternehmen

Reiner Kraft, Frank Weber, Ronald Marx, Mechthild Stöwer, Hubert Große-Onnebrink, Pedro Larbig, Alexander Oberle

Fraunhofer-Institut für Sichere Informationstechnologie
Darmstadt und Sankt Augustin

Investition in Ihre Zukunft

Investitionen für diese Entwicklung wurden von der Europäischen Union aus dem Europäischen Fonds für regionale Entwicklung und vom Land Hessen kofinanziert.

Dieser Report wurde aus dem Projekt Enterprise Encryption finanziert.

FRAUNHOFER VERLAG

IMPRESSUM

Kontaktadresse:
Fraunhofer-Institut für
Sichere Informationstechnologie SIT
Rheinstraße 75
64295 Darmstadt
Telefon 06151 869-213
Telefax 06151 869-224
E-Mail info@sit.fraunhofer.de
URL www.sit.fraunhofer.de

Hrsg. Michael Waidner
SIT Technical Reports
SIT-TR-2015-1: Vertraulichkeitsschutz durch Verschlüsselung
Reiner Kraft, Frank Weber, Ronald Marx, Mechthild Stöwer,
Hubert Große-Onnebrink, Pedro Larbig, Alexander Oberle
März 2015

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.
ISBN: 978-3-8396-0872-2
ISSN: 2192-8162

Druck und Weiterverarbeitung:
IRB Mediendienstleistungen
Fraunhofer-Informationszentrum Raum und Bau IRB, Stuttgart

Für den Druck des Buches wurde chlor- und säurefreies Papier verwendet.

Fraunhofer-Informationszentrum Raum und Bau IRB
Postfach 800469, 70504 Stuttgart
Nobelstraße 12, 70569 Stuttgart
Telefon 0711 970-2500
Telefax 0711 970-2508
E-Mail verlag@fraunhofer.de
URL http://verlag.fraunhofer.de

Vorwort des Ministers Tarek Al-Wazir

Ohne Informations- und Kommunikationstechnologie ist schon heute kein Wirtschaftsleben mehr vorstellbar. Und die digitale Vernetzung dringt immer weiter vor. „Industrie 4.0“ wird unsere Produktionsprozesse und den Austausch von Waren, Dienstleistungen und Informationen tiefgreifend verändern. Das eröffnet neue Chancen für Innovationen und wirtschaftliche Dynamik, macht uns jedoch auch immer mehr davon abhängig, dass unsere IT-Systeme reibungslos funktionieren. Gerade Unternehmen müssen ihre informationstechnische Infrastruktur und ihre sensiblen Daten richtig schützen.

Neben dem Breitbandausbau betrachten wir IT-Sicherheit als Grundvoraussetzung, um den digitalen Wandel so zu gestalten, dass er uns allen nutzt und zu unserem Wohlstand beiträgt. Mit dem Leitfaden „Vertraulichkeitsschutz durch Verschlüsselung“ möchten wir das Bewusstsein der Unternehmen für die Risiken ungewollten Informations- und Know-how-Verlustes schärfen und zeigen, was sie dagegen unternehmen können. Damit wollen wir die Innovationskraft und die Wettbewerbsfähigkeit unserer Unternehmen stärken.

Verfasst hat den Leitfaden das Fraunhofer-Institut für Sichere Informationstechnologie (Fraunhofer SIT) in Darmstadt – eine der Einrichtungen, die zur internationalen Spitzenstellung Hessens in der IT-Sicherheit beitragen. Gerade in Darmstadt konzentriert sich die Expertise in einzigartiger Weise durch die Zusammenarbeit der Technische Universität Darmstadt, des Fraunhofer SIT und der Hochschule Darmstadt. Mit den untereinander verbundenen Zentren CASED (Center for Advanced Security Research Darmstadt) und EC SPRIDE (European Center for Security and Privacy by Design) arbeiten dort die führenden Einrichtungen deutscher und europäischer Cybersicherheitsforschung. Ich freue mich, dass wir deren Erkenntnisse mit Publikationen wie dieser für unsere Unternehmen nutzbar machen können.

Tarek Al-Wazir,
Hessischer Minister für Wirtschaft, Energie, Verkehr und Landesentwicklung

Inhalt

1 Überblick

Praktisch alle Unternehmen sind heutzutage existenziell von Informations- und Kommunikationstechnik abhängig. Parallel dazu ist der Grad der Vernetzung zwischen den Akteuren im Wirtschaftsleben – Unternehmen, Kunden und staatlichen Einrichtungen – stetig gestiegen. Dies ermöglicht völlig neuartige Anwendungen mit hoher Wertschöpfung, birgt gleichzeitig aber auch ebenso neuartige Risiken für das störungsfreie Funktionieren der kritischen Prozesse eines Unternehmens und die Vertraulichkeit der in ihnen gespeicherten, bearbeiteten und übertragenen Daten.

In Hochlohnländern wie Deutschland sind Unternehmen in besonderem Maße gezwungen, das eigene Know-how und geistige Eigentum gut gegen Wettbewerber zu schützen. Unternehmensentscheider, deren Anliegen ist, Risiken zu kennen und Maßnahmen zu ihrer Beherrschung bewerten zu können, müssen sich daher mit den Herausforderungen eines effektiven Informationsschutzes befassen und Verfahren einordnen können, die hierzu einen wichtigen Beitrag leisten. Die Verschlüsselung von Informationen ist ein wirksames technisches Verfahren für diese Aufgabe. Es ist jedoch kein leichtes Unterfangen für ein Unternehmen, ein angemessenes Gesamtkonzept für die Nutzung von Verschlüsselung zu entwerfen, da diese Verfahren auf sehr unterschiedlichen Ebenen der Informationstechnik genutzt werden können und ihr Einsatz prozessübergreifend geplant werden muss.

Der vorliegende Leitfaden soll einen Beitrag dazu leisten, die Hürden für einen effizienten und effektiven Einsatz von Verschlüsselung im Unternehmen zu meistern. Er soll Unternehmen darüber aufklären, wie Verschlüsselung hilft, die Vertraulichkeit von Informationen beim Einsatz moderner Informations- und Kommunikationstechnik zu schützen. Er zeigt auf, in welchen Anwendungsbereichen und gegen welche Angriffe Verschlüsselung zweckmäßig ist und wie die verschiedenen Verschlüsselungsverfahren sinnvoll miteinander kombiniert werden können.

Der Leitfaden richtet sich an Geschäftsführer, Abteilungsleiter und andere Entscheidungsträger, die sich mit der Anwendung von Verschlüsselungstechnik vertraut machen möchten, um Schritte zum Entwurf einer für ihr Unternehmen sinnvollen Verschlüsselungsarchitektur zu planen. Im Blick sind insbesondere kleine und mittlere Unternehmen, da auch sie im Fokus von Wirtschaftsspionage stehen und sie zudem ein höheres Risiko haben, dass sich der Verlust der Vertraulichkeit sensibler Informationen existenzgefährdend auswirkt.

Der Inhalt in Stichpunkten

Warum Verschlüsselung? • Wie verbreitet ist die Anwendung?
→ **Kapitel 2**

Funktionsweise und grundlegende Verfahren für Verschlüsselung • Wozu dienen Zertifikate? • Wie sicher ist Verschlüsselung?
→ **Kapitel 3**

Wie können durch Verschlüsselung Daten sicher gespeichert und übertragen werden? • Wie werden Schlüssel sicher und effizient verwaltet?
→ **Kapitel 4**

Beispielszenarien für die Anwendung von Verschlüsselung
→ **Kapitel 5**

Zusammenfassung: elementare Regeln für die Anwendung von Verschlüsselung im Unternehmen
→ **Kapitel 6**

2
Schutz der Vertraulichkeit zur Sicherung der Wertschöpfung

2.1
Bedrohungen der Vertraulichkeit

Innerhalb weniger Jahrzehnte ist Informations- und Kommunikationstechnik zur zentralen Ressource sowohl für die Prozesse innerhalb eines Unternehmens als auch für den Austausch mit Kunden, Dienstleistern, Kooperationspartnern, Aufsichtsbehörden und anderen öffentlichen und privaten Institutionen geworden. Produktionsverfahren und die Bereitstellung von Waren und Dienstleistungen wurden so beschleunigt und intensiviert, Innovationszyklen verkürzt und Märkte globalisiert. Diese Entwicklung ist noch nicht abgeschlossen. Sie geht Hand in Hand mit einer immer durchgängigeren Vernetzung der verschiedenen Akteure im Wirtschaftsleben insbesondere über das Internet. Unternehmen, die wettbewerbsfähig bleiben wollen, können sich der immer stärkeren IT-Durchdringung und Vernetzung nicht entziehen, egal in welcher Branche sie tätig sind und unabhängig davon, ob es sich bei ihnen um lokal agierende kleinere Unternehmen oder weltweit operierende Großkonzerne handelt.

Dieser Trend bewirkt aber nicht nur eine effizientere und effektivere Wertschöpfung, sondern ist auch mit einer Vielzahl an neuartigen Gefährdungen verbunden. Diese speisen sich aus der Verletzbarkeit der im Einsatz befindlichen IT-Systeme und Übertragungsverfahren, unzureichenden technischen und organisatorischen Sicherheitsmaßnahmen und Fehlern der Benutzer der IT-Systeme. Insbesondere die Anbindung an das Internet sowie die immer stärkere Verwendung von Standardsoftware und -hardware in den eingesetzten IT-Verfahren bergen hohe Gefahren, da sich hierdurch die Zahl möglicher Angreifer ausweitet.

Erfolgreiche Angriffe auf Unternehmensnetze können empfindliche Folgen haben. Werden Daten verfälscht oder wird die Funktionsfähigkeit wichtiger Systeme beeinträchtigt, können daraus resultierende Produktions- oder Lieferverzögerungen zu spürbaren finanziellen Einbußen führen. Schwerwiegender und langfristiger nachwirkend können sich angesichts des Stellenwerts, den Informationen und Know-how für die Konkurrenzfähigkeit eines Unternehmens haben, jedoch Verluste der Vertraulichkeit wichtiger Unternehmensdaten auswirken. Forschungs- und Entwicklungsergebnisse, Strategiepapiere, Einzelheiten von Verträgen, Angebote und Preiskalkulationen, Kundendaten, die Korrespondenz mit Geschäftspartnern, Informationen über die Besonderheiten der Unternehmens-IT – dies sind nur einige Beispiele für solche Daten in einem Unternehmen, bei denen Verletzungen der Vertraulichkeit gravierende Folgen haben können:

- Geraten Information über Herstellungsprozesse und die Besonderheiten von Produkten (Rezepturen, Konstruktionspläne etc.) in unbefugte Hände, droht einem Unternehmen der Verlust seiner wichtigen Alleinstellungsmerkmale.

- Werden strategische Entwürfe, etwa solche zur zukünftigen Ausrichtung eines Unternehmens, Marketingstrategien oder Übernahmepläne vorzeitig bekannt, können diese Konzepte vorzeitig scheitern.

- Konkurrenten können sich einen Wettbewerbsvorteil verschaffen, wenn sie Zugriff auf Daten erlangen, die der Vorbereitung von Aufträgen dienen, beispielsweise Preisen, Kalkulationsformeln oder Details zu den angebotenen Leistungen.

- Kundendaten unterliegen einem besonderen gesetzlichen Schutz durch das Datenschutzrecht. Verletzungen der Vertraulichkeit können Strafzahlungen nach sich ziehen und den Ruf des betroffenen Unternehmens nachhaltig beschädigen.

- Das Bekanntwerden der vertraulichen Informationen von Geschäftspartnern oder Auftraggebern kann zu Konventionalstrafen führen und eine Geschäftsbeziehung ungewollt beenden.

- Geraten sicherheitsrelevante Informationen eines Netzes, beispielsweise Passwörter, die Konfiguration der Firewall, geheime kryptographische Schlüssel in die falschen Hände, kann dies beliebige Angriffe auf ein Unternehmensnetz zur Folge haben.

Kundendaten und andere sensible Unternehmensdaten sind ein häufiges Ziel von Cyberattacken. Die Liste der Unternehmen, die in den in den letzten Jahren von solchen Angriffen betroffen waren, ist lang. Nachfolgend nur zwei Beispiele:

- Im Jahr 2013 wurde das amerikanische Unternehmen Adobe Opfer eines solchen Angriffs. Hier gelangten Hacker an Zugangsdaten, Kreditkarteninformationen und andere kritische Daten von mindestens 38 Millionen Kunden. Darüber hinaus konnten die Hacker auf den Quellcode der wichtigsten Adobe-Produkte zugreifen und diesen kopieren, darunter so bekannte Produkte wie Acrobat oder Photoshop. Als weitere Konsequenz dieses Vorfalls, der wesentliche Vermögenswerte des Unternehmens betraf, rechnete Adobe mit nachgelagerten Kosten zum Beispiel durch Rechtsverfahren und Haftungsübernahmen.[1]

- Über zehn Jahre zuvor drangen Hacker in die Computersysteme des einstmals bedeutenden nordamerikanischen Telekommunikationsausrüsters Nortel ein. Es gelang den Angreifern, sich dauerhaft in den Systemen einzunisten und über viele Jahre hinweg technische Papiere, Forschungs- und Entwicklungsberichte, Geschäftspläne, E-Mails von Mitarbeitern und andere wichtige Dokumente herunterzuladen. Die erst im Jahr 2012 bekanntgewordene jahrelange erfolgreiche Spionage schwächte das Unternehmen und trug auch zu dessen Insolvenz im Jahr 2009 und der anschließenden Zerschlagung in den Folgejahren bei.[2]

Insbesondere Wirtschaftsspionage ist ein großes Problem für viele Unternehmen. Zum genauen Umfang des Schadens gibt es zwar keine amtlichen Statistiken. Die vorliegenden Schätzungen verweisen gleichwohl auf die Dringlichkeit des Problems. So berechnet die von dem Beratungsunternehmen Corporate Trust veröffentlichte Studie »Industriespionage 2014« auf Basis einer Befragung von Sicherheits- und Risikoverantwortlichen in deutschen Unternehmen einen jährlichen Gesamtschaden von rund 12 Milliarden Euro für die deutsche Wirtschaft.[3] Deutlich höher noch liegen die Schätzungen des Bundesinnenministeriums: Bei einer Tagung bezifferte der zuständige Minister den jährliche Gesamtschaden für Deutschland durch dieses Delikt auf rund

[1] Siehe Die Welt, 4.10.2013: »Cyberangriff – Hacker stehlen Kreditkartendaten von Adobe-Kunden«, www.welt.de/120627719, sowie Nicole Perlroth: »Adobe Hacking Attack Was Bigger Than Previously Thought«, The New York Times October 29, 2013, bits.blogs.nytimes.com/2013/10/29/adobe-online-attack-was-bigger-than-previously-thought.

[2] Siehe Lisa Hemmerich: »Nortel: Hacker kannten Passwörter von Top-Managern – Telekomausrüster jahrelang ausgespäht«, Netzwelt, 14.2.2012, www.netzwelt.de/news/90847-nortel-hacker-jahrelang-zugang-zentralen-dokumenten.html.

[3] Siehe www.corporate-trust.de/pdf/CT-Studie-2014_DE.pdf, S. 23.

50 Milliarden Euro.[1] Die »Studie Industriespionage 2014« zeigt auch, dass nicht nur große Konzerne von Wirtschaftsspionage betroffen sind, sondern in besonderem Maß auch der Mittelstand: Nahezu jedes dritte mittelständische deutsche Unternehmen wurde im Befragungszeitraum durch dieses Delikt geschädigt.[2] Als Täter kommen zwar auch Kunden, Lieferanten und eigene Mitarbeiter infrage, der größere Teil der Vorfälle beruhe jedoch – so die Studie – auf Angriffen von Hackern und wird somit durch IT-Schwachstellen begünstigt.[3] Die Angreifer können im Eigeninteresse tätige Privatpersonen sein, ebenso wie Akteure aus der in- und ausländischen Konkurrenz, der Geheimdienste oder der organisierten Kriminalität. Angesichts der hohen Professionalität der Angriffe ist es im Einzelnen allerdings oft schwierig, eine konkrete Täterschaft nachzuweisen.

2.2 Maßnahmen zum Schutz der Vertraulichkeit

Zum Schutz der Vertraulichkeit der Daten, die in seinem Netz gespeichert, bearbeitet und übertragen werden, sollte für ein Unternehmen – neben einer systematischen Verschlüsselung sensibler Daten – die Umsetzung elementarer Sicherheitsmaßnahmen selbstverständlich sein. Hierzu zählen:

- die Absicherung der externen Schnittstellen des Unternehmensnetzes durch ein effektives Firewall-System,
- ein aktuell gehaltener Malware-Schutz der Computersysteme im Netz und an dessen externen Schnittstellen,
- eine rasche Reaktion auf bekannt gewordene sicherheitsrelevante Schwachstellen in Computersystemen und die zeitnahe Installation der von den Herstellern bereitgestellten Patches und Updates,
- eine ausreichender physischer Schutz der IT-Systeme gegen unerlaubte Zugriffe sowie
- eine an dem »Need to know«-Prinzip ausgerichtete Vergabe der Zugriffsberechtigungen zu den IT-Systemen und den auf ihnen gespeicherten Information, die dafür sorgt, dass Mitarbeiter nur auf diejenigen Ressourcen zugreifen können, die sie für die Erfüllung ihrer Arbeitsaufgaben benötigen.

Die technischen Sicherheitsmaßnahmen müssen von organisatorischen Regelungen flankiert werden, die auf einen verantwortungsbewussten Umgang mit vertraulichen Informationen abzielen. Dazu gehören eine sorgfältige Auswahl der Mitarbeiter, die Zugriff auf vertrauliche Informationen haben, eine Sensibilisierung für die Bedeutung der Informationssicherheit und eine ausreichende Schulung für einen Umgang mit der IT-Infrastruktur, der dieser Bedeutung gerecht wird.[4]

[1] Siehe www.handelsblatt.com/politik/deutschland/wirtschaftsspionage-50-milliarden-schaden/8705934.html.
[2] Siehe www.corporate-trust.de/pdf/CT-Studie-2014_DE.pdf, S. 9.
[3] Siehe www.corporate-trust.de/pdf/CT-Studie-2014_DE.pdf, S. 30.
[4] Umfassende Maßnahmenempfehlungen zu den grundlegenden Sicherheitsmaßnahmen enthalten die anerkannten Standards zur Informationssicherheit, insbesondere ISO 27001/2 und die IT-Grundschutz-Kataloge des Bundesamts für Sicherheit in der Informationstechnik.

Alle genannten Maßnahmen sind, selbst wenn sie oft nur unzureichend umgesetzt werden, elementare Maßnahmen (»Basics«) für Informationssicherheit. Der wirksamste Baustein zum Schutz der Vertraulichkeit ist es darüber hinaus, alle Daten durchgängig zu verschlüsseln, deren ungewolltes Bekanntwerden einen hohen Schaden für das betroffene Unternehmen verursachen würde. Dieser Schutz wirkt selbst dann, wenn andere Maßnahmen versagen, beispielsweise Zugriffsberechtigungen missbraucht werden oder Speichermedien mit vertraulichen Daten abhandenkommen. Verschlüsselung empfiehlt sich insbesondere dann, wenn die Daten ansonsten weitgehend ungeschützt sind, also bei ihrer Übertragung über unsichere Netze oder ihrer Speicherung in offenen Umgebungen. Dies bedeutet andererseits nicht, dass durch Verschlüsselung andere Maßnahmen zum Schutz der wichtigen Unternehmensdaten überflüssig werden.

SSL/TLS (Secure Socket Layer/Transport Layer Security) ist eine Protokollfamilie zum Aufbau sicherer Verbindungen zwischen einem Client (z. B. einem Webbrowser) und einem Server (z. B. einem Online-Shop) über IP-Netze. SSL/TLS ermöglicht verschlüsselte Verbindungen, sichert die Integrität der übertragenen Daten und dient der Authentisierung der beteiligten Kommunikationspartner. Das Verfahren beruht auf asymmetrischer Verschlüsselung und Zertifikaten (siehe Kapitel 3).

Verschlüsselung ist bereits seit Jahrzehnten ein fester Bestandteil der Informations- und Kommunikationstechnik und in vielen Produkten vorhanden. Verschlüsselung findet sich in Kommunikationsprotokollen wie SSL/TLS[1] oder Mobilfunkstandards wie UMTS[2], sie sichert die Anbindung von Telearbeitern an ein Unternehmensnetz, sie ermöglicht eine vertrauliche E-Mail-Kommunikation und vieles mehr.

Werden personenbezogene Daten übertragen oder gespeichert, trägt Verschlüsselung insbesondere auch dazu bei, Anforderungen an den Datenschutz gemäß Bundesdatenschutzgesetz (BDSG) zu erfüllen. Aus diesem Grund wird in der Anlage zu § 9 Satz 1 des BDSG ausdrücklich herausgestellt, dass eine dem Stand der Technik gemäße Verschlüsselung eine geeignete Maßnahme ist, um den unbefugten Zugriff auf personenbezogene Daten und ihre unzulässige Preisgabe zu verhindern und damit die Datenschutzziele Zugangs-, Zugriffs- und Weitergabekontrolle zu unterstützen.[3]

Die vorhandenen Verschlüsselungsfunktionen werden jedoch oft nicht oder nur partiell genutzt. Wie die Ergebnisse einer umfangreichen Untersuchung zur Lage der Informationssicherheit aus dem Jahr 2012 zeigen, setzte damals immerhin etwas mehr als die Hälfte der 133 mittleren und großen deutschen Unternehmen, die sich an der Befragung beteiligten, Verschlüsselung ein, um E-Mails oder die Daten auf Festplatten mobiler Geräte vor unerwünschten Mitlesern zu schützen (siehe Abb. 01[4]). Ein großer Teil der Unternehmen, in denen diese technischen Sicherheitsmaßnahmen bis dahin nicht eingeführt waren, hatte zumindest entsprechende Planungen. Obwohl daher eine mittlerweile etwas breitere Anwendung der Verschlüsselung vermutet werden kann, dürfte gleichwohl noch in vielen Unternehmen und in vielen möglichen Anwendungsfeldern ein großer Nachholbedarf beim Einsatz dieser Sicherheitstechnik bestehen.

Verschlüsselung wird dann häufig angewendet, wenn dies von den Benutzern weitgehend unbemerkt geschieht, ihnen also keine besonderen Anstrengungen abverlangt. Beispielsweise verzichtet heutzutage kein seriöser Online-Anbieter mehr auf die Absi-

[1] Secure Socket Layer/Transport Layer Security

[2] Universal Mobile Telecommunications System

[3] Siehe www.gesetze-im-internet.de/bdsg_1990.

[4] Lagebericht zur Informations-Sicherheit (3), in: <kes> – Die Zeitschrift für Informations-Sicherheit, Nr. 6/2012, Seite 52ff

Schutz der Vertraulichkeit zur Sicherung der Wertschöpfung

cherung seiner E-Business-Anwendungen mit SSL/TLS. Hier werden die Daten transparent im Hintergrund verschlüsselt. E-Mails oder Dateien mit vertraulichem Inhalt werden, wie viele Untersuchungen belegen, auch im Unternehmensbereich in der Regel jedoch immer noch viel zu oft unverschlüsselt verschickt oder gespeichert. Die Gründe für diese lediglich partielle Anwendung kryptographischer Sicherheitstechnik sind vielfältig: Eine trotz aller bekannt gewordenen Sicherheitsvorfälle nach wie vor fehlende Sensibilität für die IT-Risiken spielt ebenso eine Rolle wie Bequemlichkeit, die Unkenntnis der vorhandenen Verschlüsselungslösungen ebenso wie die oft nur geringe Benutzerfreundlichkeit der kryptographischen Programme. Stark ins Gewicht fallen dürfte auch, dass die Zuständigen in vielen Unternehmen die Möglichkeiten zur Datenverschlüsselung in den eingesetzten Softwareprodukten oder ergänzender Tools noch nicht hinreichend kennen oder nicht wissen, wie sie diese Lösungen effizient miteinander kombinieren können.

Dieser Leitfaden soll Unternehmen darin unterstützen, mit möglichst einfachen Mitteln zu ihren Anforderungen passende Einsatzweisen von Verschlüsselung zu finden. Er soll dazu beitragen, die Hemmschwellen für einen durchgängigen Einsatz von Verschlüsselung zum Schutz vertraulicher Daten in einem Unternehmen abzusenken.

Abb. 01 Ergebnisse einer Befragung zur Anwendung von Verschlüsselung aus dem Jahr 2012
(in Klammern: Anteil der Unternehmen, die den künftigen Einsatz der Technik planten)

Anwendungsbereich für Verschlüsselung	Server/ Zentrale	Clients/ Endstellen	Mobile Endgeräte
Sensible Daten	58% (14%)	50% (11%)	48% (13%)
Festplatten/ eingebaute Speicher (komplett/partitionsweise)	28% (13%)	39% (11%)	55% (15%)
Mobile Speichermedien (USB-Sticks[1], DVD[2] etc.)	25% (13 %)	35% (19%)	35% (20%)
Archivdatenträger/ Backups	36% (9%)	19% (7%)	16% (5%)
LAN[3]/Intranet-Verbindungen	61% (2%)	52% (2%)	51% (2%)
WLAN[4]-Verbindungen	62% (1%)	63% (1%)	66% (4%)
WAN[5]/Internet-Verbindungen	75% (4%)	73% (2%)	72% (3%)
Mobile Verbindungen (UMTS etc.)	48% (3%)	45% (5%)	61% (7%)
Telefon/Fax (Festnetz/GSM[6])	12% (5%)	11% (6%)	15% (8%)
Voice-over-IP[7]	28% (10%)	27% (13%)	25% (10%)
E-Mail	47% (13%)	51% (14%)	51% (15%)

[1] Universal Serial Bus
[2] Digital Versatile Disc
[3] Local Area Network
[4] Wireless Local Area Network
[5] Wide Area Network
[6] Global System for Mobile Communications
[7] Internet Protocol

3 Grundlagen der Verschlüsselung

Bei der Verschlüsselung werden im Klartext vorliegende Ausgangsdaten – dies können Texte, aber beispielsweise auch digitalisierte Bilder oder Töne sein – mithilfe ausgeklügelter mathematischer Verfahren, sogenannten **kryptographischer Algorithmen** und mit **kryptographischen Schlüsseln** als Parameter, umgewandelt. Dies geschieht auf eine solche Weise, dass es nur dann möglich ist, anhand der verschlüsselten Daten die Ausgangsdaten zu erkennen, wenn man weiß, mit welchem Verfahren diese Daten entschlüsselt werden können und den zugehörigen Schlüssel kennt oder besitzt.

Verschlüsselung hat eine lange Tradition. Schon bei den Spartanern in der Zeit um das Jahr 500 vor Christi Geburt oder wenige Jahrhunderte später bei den Römern diente sie dazu, militärische Botschaften und andere Geheimnisse sicher zu überbringen. Die verwendeten mathematischen Verfahren waren noch wenig komplex, bestanden etwa wie bei der aus dem römischen Reich überlieferten »Cäsar-Verschlüsselung« lediglich aus einer Verschiebung von Schriftzeichen um einen festen Zahlenwert, dessen Kenntnis der Schlüssel zum Verständnis der verschlüsselten Botschaft war. Auch moderne kryptographische Algorithmen stützen sich auf vergleichbar einfache Operationen: Zeichenfolgen werden vertauscht, ersetzt und verschoben oder durch mathematische Methoden wie Multiplikation, Addition oder Restbildung unkenntlich gemacht. Die Kombination dieser Operationen und die Verfahren zur Erzeugung der verwendeten kryptographischen Schlüssel sind jedoch weitaus aufwendiger.

Die Vielzahl an Verschlüsselungsverfahren, die mittlerweile entwickelt wurden, wird in der Kryptographie, der Wissenschaft von der Verschlüsselung, üblicherweise in zwei Gruppen eingeteilt:

- Wird derselbe Schlüssel sowohl für die Verschlüsselung als auch die Entschlüsselung eingesetzt, handelt es sich um eine **symmetrischen Verschlüsselung**,

- erfolgen diese Operationen hingegen mit unterschiedlichen Schlüsseln wird dies als **asymmetrische Verschlüsselung** bezeichnet.

Verschlüsselung schützt wirksam die Vertraulichkeit von Informationen. Moderne kryptographische Verfahren können darüber hinaus weitere **Sicherheitsziele** unterstützen, nämlich dabei helfen,

- unbefugte Veränderungen an Daten zu erkennen (Schutz der Integrität),

- die Identität von Kommunikationspartnern nachzuweisen (Schutz der Authentizität) und

- das erfolgreiche nachträgliche Abstreiten einer Handlung – z. B. des Versands einer Nachricht – zu verhindern (Schutz der Nichtabstreitbarkeit und Verbindlichkeit).

Für die Gewährleistung dieser Ziele werden unterschiedliche kryptographische Instrumente eingesetzt. Die wichtigsten sind neben bereits genannten Verfahren zur symmetrischen und asymmetrischen Verschlüsselung, **Zertifikate** und **Public-Key-Infrastrukturen**, **elektronische Signaturen** und **kryptographische Hashfunktionen**. Auch wenn diese Verfahren auf teilweise recht komplizierten mathematischen Algorithmen beruhen, ist für ihre Anwendung kein mathematisches Wissen, sondern lediglich das Verständnis einiger weniger elementarer Sachverhalte erforderlich, die nachfolgend beschrieben werden.

3.1 Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung, der ältesten und bis vor wenigen Jahrzehnten einzig bekannten Art der Verschlüsselung, dient, wie eingangs dieses Kapitels geschrieben, derselbe Schlüssel sowohl für die Verschlüsselung als auch die Entschlüsselung der Daten. Weil dieser Schlüssel geheim bleiben muss, wird das Verfahren auch als **Private-Key-Verschlüsselung** bezeichnet.

Bei den Verfahren zur symmetrischen Verschlüsselung werden Blockchiffren und Stromchiffren voneinander unterschieden:

- Bei Blockchiffren werden die Ausgangsdaten in einzelne Blöcke zerlegt und dann blockweise verschlüsselt. Weithin verbreitete Algorithmen dieser Gruppe sind 3DES[1], AES[2], IDEA[3] und RC5[4]. Am häufigsten genutzt wird AES, ein Verfahren, das in Europa entwickelt wurde und im Jahr 2000 von der US-amerikanischen Standardisierungsbehörde NIST[5] als Nachfolger des bis dahin vorherrschenden, aber nicht mehr als hinreichend sicher geltenden DES-Algorithmus bestimmt wurde. Die bei AES verwendeten Schlüssel sind mindestens 128 Bit lang.

- Bei Stromchiffren werden die Ausgangsdaten hingegen zeichenweise verschlüsselt. Diese Technik wird insbesondere dann angewendet, wenn Daten in Echtzeit übertragen werden sollen, also beispielsweise im Mobilfunk oder bei der Kommunikation via Bluetooth.

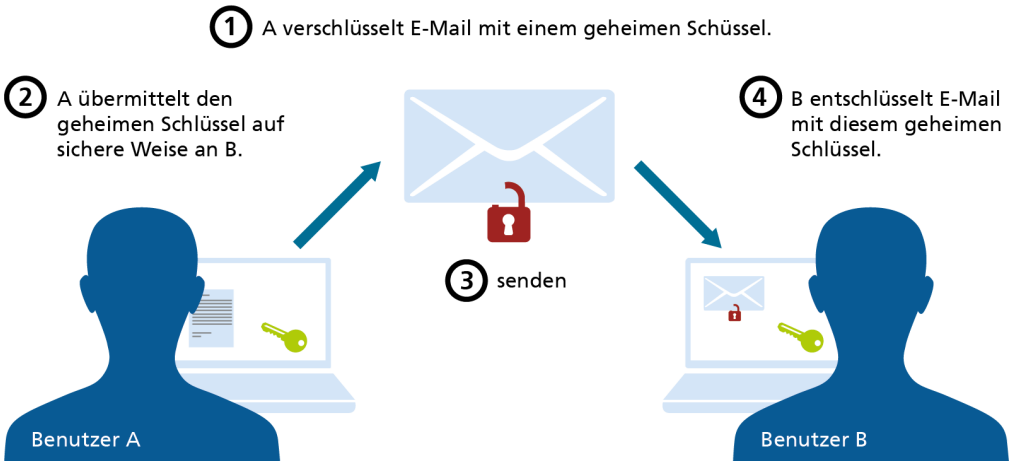


Abb. 02 Symmetrische Verschlüsselung (am Beispiel E-Mail)

Abb. 02 zeigt am Beispiel des Versands einer E-Mail ein grundlegendes Problem der symmetrischen Verschlüsselung. Sollen nämlich verschlüsselte Informationen zwischen unterschiedlichen Kommunikationspartnern – dies können Personen, aber auch technische Systeme sein – ausgetauscht werden, muss gewährleistet werden, dass der für die Entschlüsselung erforderliche Schlüssel geheim bleibt. Hierfür ist er über einen sicheren

[1] Triple Data Encryption Standard, eine Weiterentwicklung des DES-Algorithmus, der aufgrund seiner nur 56 Bit langen Schlüssel nicht mehr als sicher gilt. Bei 3DES sind die Schlüssel 168 Bit lang.
[2] Advanced Encryption Standard
[3] International Data Encryption Algorithm
[4] Rivest Cipher 5
[5] National Institute of Standards and Technology

Kanal und getrennt von den verschlüsselten Informationen zu übertragen. Je mehr Kommunikationspartner Zugriff auf die Informationen haben sollen, desto mehr Übertragungswege sind folglich für den Austausch der Schlüssel erforderlich. Bei einer großen Teilnehmerzahl ist symmetrische Verschlüsselung daher wenig praktikabel. Zudem ist bei einer großen Zahl an Mitwissern die Gefahr sehr groß, dass geheime Schlüssel Unbefugten zugänglich werden, da jeder Ort, an dem diese aufbewahrt werden, und jeder Kanal, über den sie übertragen werden, mögliche Angriffspunkte sind.

3.2 Asymmetrische Verschlüsselung

Die asymmetrische Verschlüsselung wurde erstmals Ende der siebziger Jahre des zwanzigsten Jahrhunderts vorgestellt und hat sich seitdem rasch zu dem vorherrschenden Verfahren für eine verschlüsselte Kommunikation entwickelt. Anders als bei der symmetrischen Verschlüsselung kommen hier unterschiedliche, aber zueinander gehörige Schlüssel für die Verschlüsselung und Entschlüsselung zum Einsatz. Diese Schlüsselpaare müssen so beschaffen sein, dass Daten, die mit einem der beiden Schlüssel verschlüsselt werden, nur mit dem jeweils anderen wieder entschlüsselt werden können.

Die asymmetrische Verschlüsselung wird auch als **Public-Key-Verschlüsselung** bezeichnet, weil der Schlüssel, mit dem die Daten verschlüsselt werden, nicht mit dem identisch ist, mit dem diese wieder entschlüsselt werden können. Damit muss der Verschlüsselungsschlüssel (»öffentlicher Schlüssel«, »Public Key«) auch nicht geheim gehalten werden, anders als der Entschlüsselungsschlüssel (»privater Schlüssel« »Private Key«). Daher darf es auch nicht möglich sein, den privaten Schlüssel aus dem öffentlichen Schlüssel zu berechnen.

Während der öffentliche Schlüssel keine besonderen Schutzvorkehrungen benötigt, ist ein zuverlässiger Schutz des privaten Schlüssels unabdingbar für die Sicherheit des Verfahrens. Die Sicherheit der asymmetrischen Verschlüsselung beruht darüber hinaus auf mathematischen Problemen, für die gegenwärtig noch keine rasch umzusetzenden Lösungsverfahren bekannt sind. Bei RSA[1], dem am häufigsten benutzten Algorithmus, ist dieses Problem beispielsweise das Fehlen einer Methode zur effizienten Berechnung der Primfaktoren sehr großer Zahlen. Eine weitere Gruppe von Verschlüsselungslösungen beruht auf dem Problem der Berechnung diskreter Logarithmen, für das ebenfalls noch keine effizienten Lösungen bekannt sind.

Mithilfe von asymmetrischer Verschlüsselung kann – wie in Abb. 03 am Beispiel einer E-Mail veranschaulicht – auch das Problem einer sicheren Verteilung symmetrischer Verschlüsselung umgangen werden:

- Wollen zwei Partner verschlüsselt miteinander kommunizieren, so benötigt jeder der beiden ein Schlüsselpaar, das aus einem öffentlichen und einem privaten Schlüssel besteht.

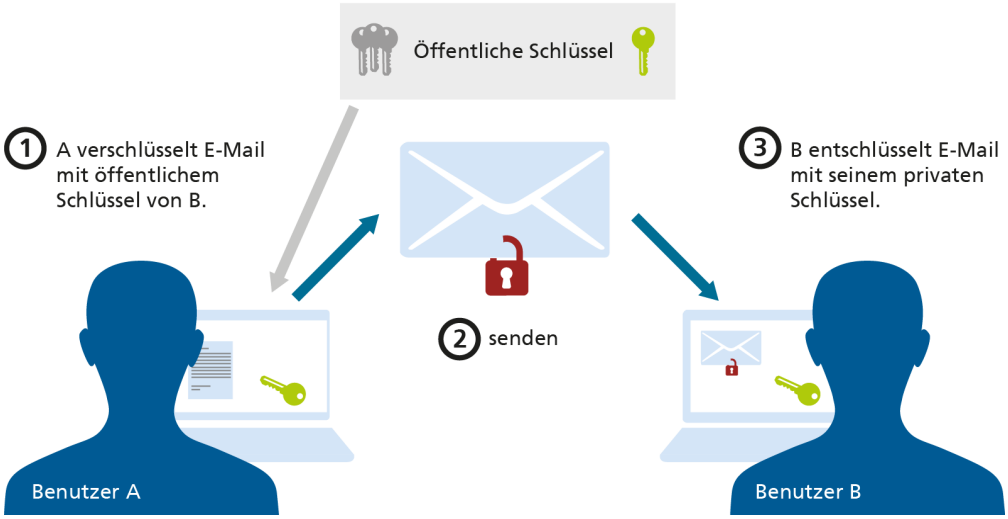
- Der öffentliche Schlüssel wird an den Kommunikationspartner verschickt, der damit Nachrichten an den Absender des Schlüssels verschlüsseln kann.

[1] Rivest, Shamir, Adleman – benannt nach den Nachnamen der Erfinder des Algorithmus

- Der zweite Schlüssel verbleibt als privater Schlüssel beim Eigentümer des Schlüsselpaars und dient der Entschlüsselung der an den Eigentümer gesandten verschlüsselten Nachrichten.

Anders als bei der symmetrischen Verschlüsselung ist folglich kein geheimer Kanal mehr zum Austausch von Entschlüsselungsschlüsseln mehr erforderlich. Dies erleichtert es auch entscheidend, in größeren und offeneren Kreisen von Kommunikationspartnern verschlüsselt miteinander zu kommunizieren.

Abb. 03 Asymmetrische Verschlüsselung (am Beispiel E-Mail)



Public-Key-Kryptographie ist heutzutage in vielfältigen Einsatzfeldern in Gebrauch, beispielsweise dient sie der Verschlüsselung von E-Mail oder der Absicherung der Internet-Kommunikation mittels SSL/TLS (zu beidem siehe Kapitel 4.2). Üblicherweise werden dabei symmetrische und asymmetrische Verfahren miteinander verknüpft. Bei dieser so bezeichneten **hybriden Verschlüsselung** werden die Ausgangsdaten zunächst mithilfe eines zufällig generierten geheimen Schlüssels symmetrisch verschlüsselt, zum Beispiel gemäß dem AES-Verfahren. Dieser sogenannte Sitzungsschlüssel (»Session Key«) wird anschließend asymmetrisch mit den Public Keys der Adressaten (etwa mithilfe des RSA-Verfahrens) verschlüsselt und den verschlüsselten Ausgangsdaten (z. B. einer E-Mail) beigefügt. Hybride Verschlüsselung ermöglicht somit den sicheren Austausch symmetrischer Schlüssel.

3.3 Kryptographische Hashfunktionen und elektronische Signaturen

Neben der Verschlüsselung unterstützen moderne kryptographische Verfahren weitere Sicherheitsziele, insbesondere auch den Nachweis der Urheberschaft und der Unverfälschtheit einer Information mittels elektronischer (digitaler) Signaturen. Diese spezielle Form einer elektronischen Unterschrift stützt sich auf sogenannte **kryptographische Hashfunktionen**.

Bei derartigen Funktionen handelt es sich um Verfahren, mit denen eine Zeichenkette beliebiger Länge auf eine Zeichenkette fester Länge, den »Hashwert«, abgebildet wird. Dieser ist so beschaffen, dass es praktisch nicht möglich ist,

- aus ihm den Ausgangstext zu rekonstruieren sowie
- eine zweite Zeichenfolge zu konstruieren, die einen identischen Hashwert ergibt.

Bekannte und derzeit noch als hinreichend sicher, also die genannten Anforderungen erfüllend, geltende Hash-Funktionen sind SHA-256[1] oder RIPEMD-160[2].

Der Hauptanwendungszweck kryptographischer Hashfunktionen ist der Nachweis der Integrität von Informationen. Bei jeder Anwendung auf gegebene Daten muss eine solche Funktion einen identischen Hashwert liefern. Ist dies nicht der Fall, ist damit nachgewiesen, dass es sich um andere oder aber geänderte Daten handelt.

Diese Eigenschaft wird bei elektronischen Signaturen ausgenutzt. Abb. 04 veranschaulicht den Ablauf exemplarisch am Beispiel der Signatur einer E-Mail und bei Verwendung des im vorherigen Abschnitt genannten asymmetrischen RSA-Verschlüsselungsverfahrens:

Mit kryptographischen Hashfunktionen kann z. B. auch die Vertraulichkeit von **Passwörtern oder PINs** besser geschützt werden. Auf einem System (z. B. einem Webserver) wird dazu das Passwort oder die PIN nur gehasht abgespeichert und nicht im Klartext. Bei der Eingabe eines Passworts oder einer PIN wird der abgespeicherte Hashwert mit dem Hashwert der eingegebenen Zeichenkette verglichen. Stimmen beide überein, wird der Zugriff gewährt, andernfalls wird dieser abgelehnt.

- Zunächst wird mittels einer kryptographischen Hashfunktion aus einer Nachricht ein Hashwert gebildet, mit dessen Hilfe überprüft werden kann, ob die Nachricht nachträglich verändert wurde.
- Dieser Hashwert wird mit dem privaten Schlüssel der signierenden Instanz (Person oder System) signiert und der Nachricht beigefügt.
- Mit dem öffentlichen Schlüssel der signierenden Instanz kann der Hashwert anschließend verifiziert und mit dem Resultat einer erneuten Anwendung der Hashfunktion auf die empfangene Nachricht verglichen werden. Stimmen beide Werte überein, ist die Unverfälschtheit der Nachricht nachgewiesen.

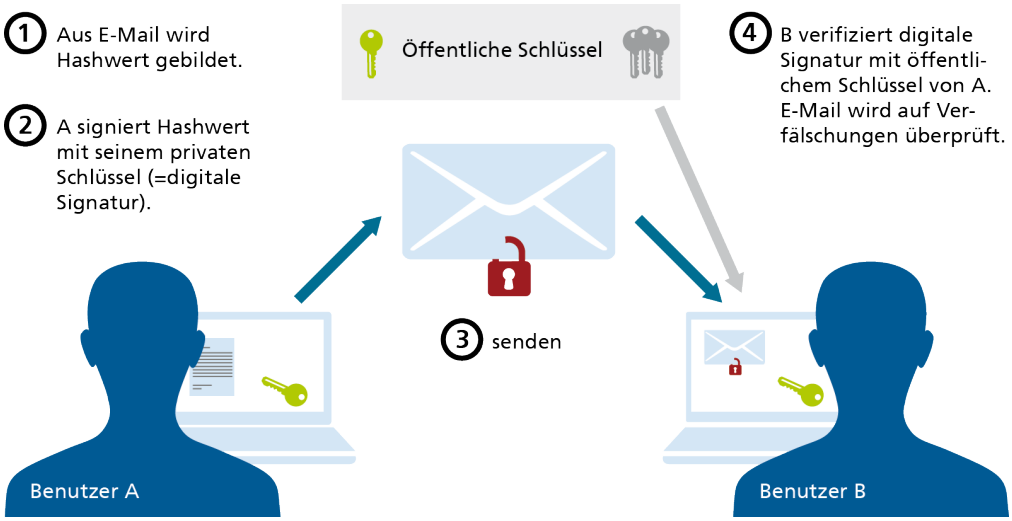


Abb. 04 Elektronische Signaturen (am Beispiel E-Mail)

[1] Secure Hash Algorithm
[2] RACE Integrity Primitives Evaluation Message Digest

Da dieser Vergleich ebenfalls nur dann positiv ausfallen kann, wenn der Hashwert tatsächlich mit dem privaten Schlüssel des Absenders der Nachricht verschlüsselt wurde – nur dann ist eine korrekte Entschlüsselung des Hashwerts mit dessen öffentlichem Schlüssel möglich –, ist somit auch die Authentizität des Absenders gesichert, vorausgesetzt der für die Entschlüsselung benutzte öffentliche Schlüssel gehört tatsächlich zu dem behaupteten Absender.

3.4 Zertifikate und Public-Key-Infrastrukturen

Bei der asymmetrischen Kryptographie ist die Verteilung des Verschlüsselungsschlüssels problemlos möglich, weil dieser – per Definition – als öffentlicher Schlüssel allgemein bekannt sein darf. Der Nachweis, dass er tatsächlich zu dem vorgegebenen Inhaber gehört, also vertrauenswürdig ist, erfordert hingegen einen zusätzlichen Aufwand. Dieser Aufwand ist allerdings notwendig, um auszuschließen, dass eine dritte Instanz sich in betrügerischer Absicht als Inhaber eines bestimmten öffentlichen Schlüssels ausgibt.

Das erforderliche Vertrauen in die Echtheit (»Authentizität«) des öffentlichen Schlüssels kann grundsätzlich auf zwei Weisen hergestellt werden:

- Die Teilnehmer einer verschlüsselten Kommunikation erklären einem öffentlichen Schlüssel unmittelbar ihr Vertrauen, nachdem sie sich von dessen Echtheit und der Authentizität des Inhabers überzeugt haben. Ein solches dezentrales Vertrauensmodell, bei dem durch die Entscheidungen der Beteiligten ein »Web of Trust« gebildet wird, ist beispielsweise eine Grundidee der weithin verbreiteten Verschlüsselungssoftware »PGP – Pretty Good Privacy«.

Für die Überprüfung der Echtheit und Authentizität eines öffentlichen Schlüssels dient oft der Vergleich von **elektronischen Fingerabdrücken (»Fingerprints«)**, anhand derer ein Schlüssel eindeutig identifiziert werden kann. Diese »Fingerprints« werden mittels kryptografischer Hashfunktionen gebildet. (→ Kapitel 3.3).

- Für große Benutzergruppen geeigneter ist das hierarchische Vertrauensmodell: Eine zentrale vertrauenswürdige Instanz bezeugt (»zertifiziert«) die Echtheit der Schlüssel und die Authentizität ihrer Inhaber. Ein Benutzer muss somit nicht mehr jeden einzelnen Schlüssel prüfen, um ihn als vertrauenswürdig einstufen zu können, sondern es genügt, der zentralen Instanz zu vertrauen, wodurch alle von dieser zertifizierten Schlüssel automatisch als vertrauenswürdig gelten.

Technisch wird eine derartige digitale Beglaubigung in Form von Zertifikaten umgesetzt – einem Schlüssel beigefügte Informationen über dessen Echtheit und Vertrauenswürdigkeit. Für das Format dieser Zertifikate hat sich X.509v3, ein Normenwerk der Internationalen Fernmeldeunion ITU[1], als Standard etabliert.

Systeme, mit denen Zertifikate und zugehörige Schlüssel erzeugt, verteilt und verwaltet werden können, werden als Public-Key-Infrastruktur (PKI) bezeichnet. Zentrale Aufgabe einer PKI ist die Herausgabe von Zertifikaten. Die zugehörigen Tätigkeiten werden auch

[1] International Telecommunication Unit

mit dem Begriff »Certification Authority« (CA) bezeichnet. Daneben gibt es weitere Aufgaben wie

- die Registrierung der Teilnehmer (»Registration Authority«),
- das Führen eines Verzeichnisdienstes für die ausgestellten Zertifikate,
- das Führen von Sperrlisten (»Certificate Revocation List«) für die nicht mehr gültigen Zertifikate,
- die Überprüfung vorhandener Zertifikate,
- eine sorgfältige Dokumentation der PKI-Prozesse und der eingesetzten Technik als Nachweis für die Vertrauenswürdigkeit der PKI (siehe Abb. 05).

Für ein größeres Unternehmen kann es sich lohnen, eine eigene PKI zu betreiben. Kleinere Einrichtungen können anstelle dessen ihre Zertifikate sowie die zugehörigen kryptographischen Schlüssel von darauf spezialisierten Anbietern für Zertifizierungsdienste beziehen. Bekannte Anbieter sind beispielsweise CAcert, D-Trust, GeoTrust, GlobalSign, Thawte, T-Systems und VeriSign.

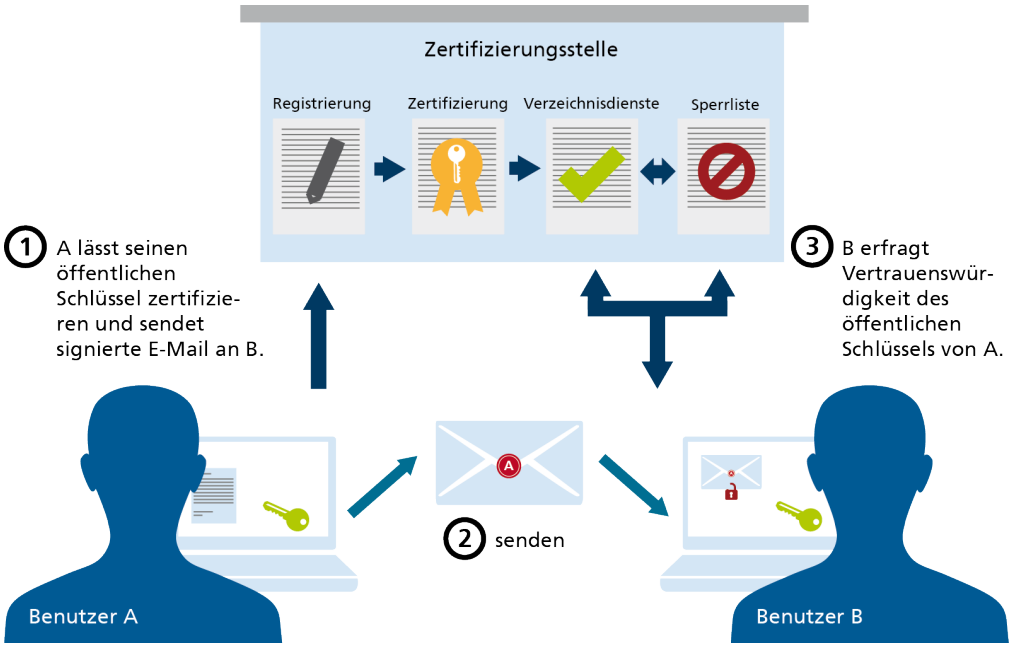


Abb. 05 Zertifikate und Aufgaben einer Public-Key-Infrastruktur

3.5 Sicherheit der Verschlüsselung

Wird sie richtig angewendet, setzt Verschlüsselung unerwünschten Mitlesern nahezu unüberwindliche Hürden, an vertrauliche Informationen zu gelangen. Allerdings bietet sie nur solange eine hohe Sicherheit, wie es gelingt, die zur Entschlüsselung erforderlichen Schlüssel vor potenziellen Angreifern geheim zu halten. Dazu ist es notwendig, dass

- die geheimen Schlüssel in einer sicheren Umgebung erzeugt, verteilt und aufbewahrt werden,
- der Zugriff auf die geheimen Schlüssel geschützt ist,
- die Verschlüsselungssoftware frei von Schwachstellen ist, die das Auslesen und Erraten der Schlüssel ermöglichen oder andere Hintertüren zur Entschlüsselung öffnen,
- die einer Verschlüsselung zugrunde liegenden Algorithmen in absehbarer Zeit nicht gebrochen werden (z. B. infolge des wissenschaftlichen und technischen Fortschritts).

Nachfolgend werden diese Anforderungen kurz erläutert.

Sichere Erzeugung, Verteilung und Speicherung geheimer Schlüssel

Ein kryptographischer Schlüssel kann letztlich als eine sehr große Zahl verstanden werden. Je größer der Zahlenraum ist, aus dem ein Schlüssel stammen kann, desto schwieriger ist er zu erraten. Je länger ein Schlüssel ist, als desto sicherer kann er folglich gelten. Zusätzlich muss – auch bei einem sehr großen Zahlenraum – dafür gesorgt werden, dass ein Schlüssel nicht aufgrund von Besonderheiten bei seiner Erzeugung vorhersagbar ist. Diese Voraussetzung ist erfüllt, wenn ein Schüssel rein zufällig aus dem verfügbaren Zahlenraum gewählt wird. Bei den automatisch generierten kryptographischen Schlüsseln sorgen sogenannte Zufallsgeneratoren dafür, dass diese Voraussetzung erfüllt wird. Hier liegt aber auch eine mögliche Schwachstelle: Ein schlechter Zufallsgenerator, also einer der leicht vorhersehbare Ergebnisse liefert oder der nur einen Teil des möglichen Zahlenraums nutzt, erzeugt unsichere, leicht zu erratende Schlüssel.

Für die Geheimhaltung kryptographischer Schlüssel ist es darüber hinaus erforderlich, dass sie bereits bei ihrer Erzeugung nicht von Dritten mitgelesen oder mitgeschnitten werden können. Dies setzt einen guten Schutz der zur Generierung verwendeten IT-Systeme voraus. Schlüssel können zentral, beispielsweise mithilfe einer darauf spezialisierten Hardware, oder dezentral, also unmittelbar an ihren Einsatzorten oder bei den zugeordneten Benutzern, erzeugt werden. Zentrale Systeme sind in der Regel besser abzusichern als dezentrale, allerdings ist dabei auf eine sichere, verschlüsselte, Übertragung der Schlüssel und eine korrekte Authentisierung der Instanzen – Benutzer oder technischen Systeme – zu achten, denen die Schlüssel zugeordnet sind.

Geheime Schlüssel können auf beliebigen Medien gespeichert werden. Dies sollte immer zugriffsgeschützt erfolgen. Eine deutliche höhere Sicherheit als übliche Speichermedien wie Festplatten oder USB-Sticks bieten Smartcards, die mit einem eigenen Chip ausgestattet sind, der die Daten ver- und entschlüsselt. Es ist folglich nicht mehr notwendig, die für diese Funktionen erforderlichen Schlüssel in den Hauptspeicher eines Computers zu kopieren, wo sie von kenntnisreichen Angreifern leicht ausgelesen werden können.

Zugriffsschutz für geheime Schlüssel

Um eine unerwünschte Verwendung geheimer Schlüssel zu verhindern, müssen diese mit einem wirksamen Zugriffsschutz versehen werden. Sind die Schlüssel auf konventioneller Hardware gespeichert, beispielsweise auf einer Festplatte oder einem USB-Stick, geschieht dies in der Regel mithilfe von Passwörtern, befinden sich die Schlüssel auf

Smartcards, dienen PINs[1] diesem Zweck. Als Berechtigungsnachweise können ferner auch die Schlüssel dienen, die zur Entschlüsselung verwendet werden. Gelangen Passwörter, PINs oder andere Berechtigungsnachweise in die falschen Hände oder sind sie zu leicht zu erraten, kann jede Verschlüsselung mühelos gebrochen werden. Daher ist es wichtig, darauf zu achten und die Benutzer dafür zu sensibilisieren, dass Kennwörter und PINs sorgfältig gewählt werden und geheim bleiben. Hierzu gehört auch, dass die Computer, auf denen die Schlüssel verwendet werden, wirksam gegen Schadsoftware geschützt sind. Der Gebrauch spezieller Hardware zur Eingabe von PINs und Kennwörtern erhöht den Zugriffsschutz bei der Eingabe dieser Berechtigungsnachweise an einem Computer, da dadurch das Auslesen dieser Informationen durch sogenannte Keylogger – Schadsoftware, die Tastatureingaben mitschneidet – verhindert wird.

Sicherheit der kryptographischen Software

Dass Verschlüsselungssoftware – wie jede andere Software auch – grundsätzlich nicht frei von unter Umständen gravierenden Schwachstellen ist, zeigte der im Jahr 2014 bekanntgewordene Heartbleed-Bug: Eine weit verbreitete und bis zur Entdeckung der Schwachstelle als sicher geltende ältere Version der Krypto-Bibliothek OpenSSL enthielt einen Programmierfehler, der es erlaubte, von betroffenen Systemen geheime Schlüssel, Passwörter und andere Daten auszulesen. Aufgrund der starken Verbreitung der Bibliothek war von dieser Sicherheitslücke ein großer Teil der weltweiten Internet-Infrastruktur betroffen, darunter auch viele populäre Websites, deren Benutzer gezwungen waren, ihre Zugangskennungen zu ändern.[2]

Ein zweiter Aspekt der Sicherheit kryptographischer Software ist deren Vertrauenswürdigkeit. Anwender müssen sicher sein, dass sie keine »Hintertüren« enthält, die eine unerwünschte Entschlüsselung ihrer Daten durch Dritte ermöglichen. Insbesondere US-amerikanische Krypto-Software steht seit den Enthüllungen von Edward Snowden im Sommer 2013 verstärkt unter dem Verdacht, dass darin solche Nebeneingänge für den nachrichtendienstlichen Zugriff eingebaut sind. Software aus Deutschland oder anderen europäischen Ländern, in denen es keine gesetzlichen Vorschriften zu Hintertüren in kryptographischer Software gibt, haben in dieser Hinsicht jedoch einen »Vertrauensvorschuss«. Gleiches gilt für Open-Source-Produkte, da bei ihnen der Quelltext der Software offengelegt werden muss und damit eine unabhängige Prüfung der Software möglich ist. Wie der Heartbleed-Bug zeigt, ist dieser Vertrauensvorschuss allerdings nicht mit einer hundertprozentigen Sicherheitsgarantie gleichzusetzen.

Anwender von Verschlüsselungssystemen sollten die einschlägigen Informationsquellen nutzen, um über die Sicherheit ihrer Software auf dem Laufenden zu bleiben und bekanntgewordene Schwachstellen zügig beheben zu können. Es gibt hierfür zahlreiche Informationsquellen, beispielsweise Meldungen der Softwarehersteller oder die diesbezüglichen Veröffentlichungen auf den Seiten des Bundesamts für Sicherheit in der Informationstechnik[3] und auf anderen Sicherheitsportalen (siehe dazu die bundesweiten und hessischen Anlaufstellen im Anhang unter Abschnitt 7.2). Gleichwohl ist es insbesondere für kleine und mittlere Unternehmen (KMU) schwierig, sich aus der Vielzahl an Informationsangeboten die für sie relevanten Meldungen herauszusuchen.

[1] Personal Identification Number

[2] Für mehr Informationen zu dieser Sicherheitslücke siehe z. B. www.heise.de/security/artikel/So-funktioniert-der-Heartbleed-Exploit-2168010.html.

[3] Siehe www.bsi.bund.de.

Sicherheit der kryptographischen Algorithmen und der verwendeten Schlüssel

Entgegen der üblichen Meinung, dass eine Verschlüsselung umso sicherer ist, je geheimer der kryptographische Algorithmus bleibt, wird in der modernen Kryptographie gerade die Offenlegung des Verfahrens und die dadurch mögliche intensive Prüfung durch unabhängige Experten gefordert, um mögliche Fehler und Hintertüren auszuschließen, die eine unberechtigte Entschlüsselung der Daten ermöglichen. Bei derart gründlich geprüften Algorithmen entscheiden folglich im Wesentlichen die Beschaffenheit und die Handhabung der verwendeten Schlüssel über die Sicherheit der Verschlüsselung.

Grundsätzlich ist eine Verschlüsselung umso sicherer, je länger die verwendeten Schlüssel sind. Theoretisch kann – auch bei noch so langen Schlüsseln – jede mit den üblichen Verfahren durchgeführte Verschlüsselung gebrochen werden, notfalls durch sogenannte Brute-Force-Angriffe, also das Ausprobieren aller möglichen Schlüssel. Hinreichend sicher sind daher Algorithmen und Schlüssel folglich nur dann, wenn solche Angriffe auch mit modernsten Hochleistungsrechnern nur mit einem unverhältnismäßig großen Zeitaufwand erfolgreich und damit praktisch unmöglich wären. Es hängt vom verwendeten Algorithmus ab, welche Längen unter dieser Prämisse als hinreichend sicher gelten. Generell benötigen asymmetrische Verfahren längere Schlüssel für eine sichere Verschlüsselung als symmetrische: Während bei asymmetrischen Verfahren wie RSA oder Elgamal Schlüssel 2048 Bit lang sein sollten, genügen derzeit beispielsweise noch 128 Bit für eine sichere Verschlüsselung mit dem symmetrischen Verfahren AES.

Weil Computer immer leistungsfähiger werden und das Wissen über mathematische Algorithmen stetig steigt, können heutzutage noch sichere Verschlüsselungsverfahren und Schlüssellängen im Laufe der Zeit unsicher werden. Beispielweise könnte der auf der Schwierigkeit, die Primfaktoren sehr großer Zahlen zu ermitteln, beruhende RSA-Algorithmus aus den folgenden beiden Gründen unsicher werden:

- Die Computersysteme haben sich technisch so weiterentwickelt, dass die Berechnung dieser Faktoren mit den vorhandenen mathematischen Methoden entscheidend beschleunigt wird.

- Es gelingt, neuartige und effizientere mathematische Methoden für die Zerlegung in Primfaktoren zu entwickeln, so dass auch mit weniger leistungsfähigen Computersystemen dieses Problem gelöst werden kann.

Es muss daher regelmäßig geprüft werden, ob die verwendeten Algorithmen und Schlüssellängen noch eine hinreichende Sicherheit bieten. Eine Übersicht über die Sicherheit von Verschlüsselungsalgorithmen und Schlüssellängen mit detaillierten technischen Erläuterungen enthält die regelmäßig aktualisierte Technische Richtlinie TR-02102-1: »Kryptographische Verfahren: Empfehlungen und Schlüssellängen« des Bundesamts für Sicherheit in der Informationstechnik.[1]

[1] Siehe unter www.bsi.bund.de/TR.

4 Anwendungslösungen für Verschlüsselung

Es gibt grundsätzlich drei Zustände, in denen sich Daten befinden können:

- Sie können gespeichert sein (»Data at Rest«),
- sie können übertragen werden (»Data in Transit«) und
- sie können in Bearbeitung sein (»Data in Use«).

Während es für die beiden erstgenannten Zustände effiziente Verfahren zur Verschlüsselung gibt, ist die kryptographische Absicherung von in Bearbeitung befindlichen Daten (die sogenannte »homomorphe Verschlüsselung«) mit heutiger Hardware und den bislang entwickelten Methoden noch nicht effizient anwendbar und deswegen auch nicht Gegenstand der weiteren Betrachtung.

Daten können auf unterschiedlich gearteten Medien und an unterschiedlich gut geschützten Orten gespeichert sein. Sie können sich auf eigener Hardware (auf der Festplatte eines Computers, einem USB-Stick oder einem anderen Datenträger) befinden oder aber bei einem externen Provider, beispielsweise einem Cloud Service oder einem E-Mail-Provider. Ebenso gibt es unterschiedliche Verfahren und Wege, mit und auf denen Daten übertragen werden, z. B. mittels E-Mail, Voice-over-IP (VoIP) oder einem anderen Internet-Protokoll. Dementsprechend gibt es verschiedene Ansatzpunkte und Varianten zur Verschlüsselung (siehe Abb. 06). Diese werden in diesem Kapitel gegliedert in je einen Abschnitt zur verschlüsselten Ablage (siehe Abschnitt 4.1) und zur verschlüsselten Übertragung von Informationen (siehe Abschnitt 4.2) vorgestellt. Dabei wird auf den jeweils sinnvollen Anwendungsbereich, mögliche Vor- und Nachteile der einzelnen Verfahren und weitere zu beachtende Aspekte eingegangen. Bei vielen dieser Verschlüsselungsverfahren obliegt es dem Benutzer, für eine sichere Verwaltung der verwendeten kryptographischen Schlüssel zu sorgen. Dem »Schlüsselmanagement« ist daher als Abschluss dieses Kapitels ein eigener Abschnitt gewidmet (siehe Kapitel 4.3).

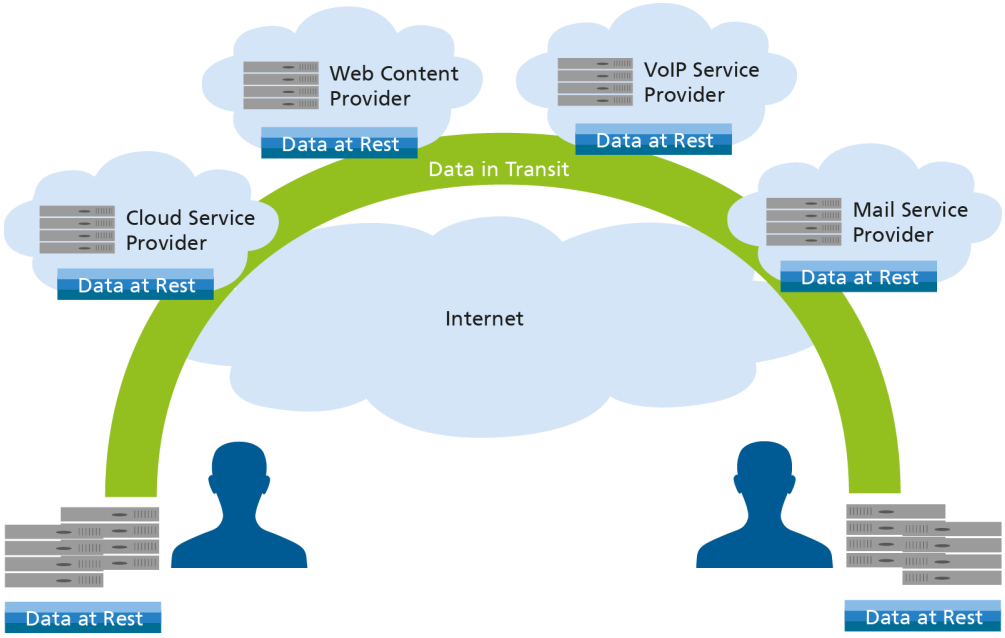


Abb. 06 Ansatzpunkte für Verschlüsselung

4.1 Ablage von Informationen (»Data at Rest«)

Es gibt verschiedene Speicherorte und Arten von Speichermedien, an und auf denen Daten abgelegt sein können:

- stationäre Arbeitsplatzrechner,
- mobile Speichermedien, z. B. USB-Sticks, externe Festplatten oder DVDs,
- mobile IT-Systeme, z. B. Notebooks, Tablets oder Smartphones,
- unter eigener Kontrolle befindliche interne Server,
- unter fremder Kontrolle befindliche Server z. B. solche bei einem Cloud-Provider.

Grundsätzlich ist bei allen Arten von Speichermedien und an allen Speicherorten die Vertraulichkeit von Daten gefährdet, wenn Unbefugte Zugang zu und Zugriff auf das Medium und die auf ihm gespeicherten Daten haben. Es empfiehlt sich daher immer, Daten zu verschlüsseln, wenn diese vertraulich gehalten werden sollen. Je nach Anwendungszweck und Art des Speichermediums können unterschiedliche Verschlüsselungsstrategien zur Anwendung kommen.

Besonders hoch ist das Risiko, dass vertrauliche Informationen in die falschen Hände gelangen, bei mobilen IT-Systemen und Speichermedien. Aber auch physisch einfacher zu schützende stationäre Computersysteme sind nicht davor gefeit, dass vertrauliche Informationen missbraucht werden, beispielsweise als Folge eines Einbruchs. Bei allen Geräten drohen Vertraulichkeitsverluste zudem nicht nur bei unerwünschten physischen Zugriffen, sondern auch durch Angriffe innerhalb eines unzureichend gesicherten Unternehmensnetzes oder aus dem Internet. Werden Daten auf externen Servern gespeichert, die unter fremder Kontrolle stehen (z. B. bei einem Cloud Service), ist die Vertraulichkeit dieser Daten in besonders hoher Weise gefährdet.

In allen Fällen kann Verschlüsselung dazu beitragen, die Vertraulichkeit der gespeicherten Informationen zu sichern. In diesem Kapitel werden verschiedene Möglichkeiten hierfür aufgezeigt, die sich in der Ebene, auf der die Verschlüsselung ansetzt, und dem Umfang, in dem Daten verschlüsselt werden, unterscheiden (siehe Abb. 07).

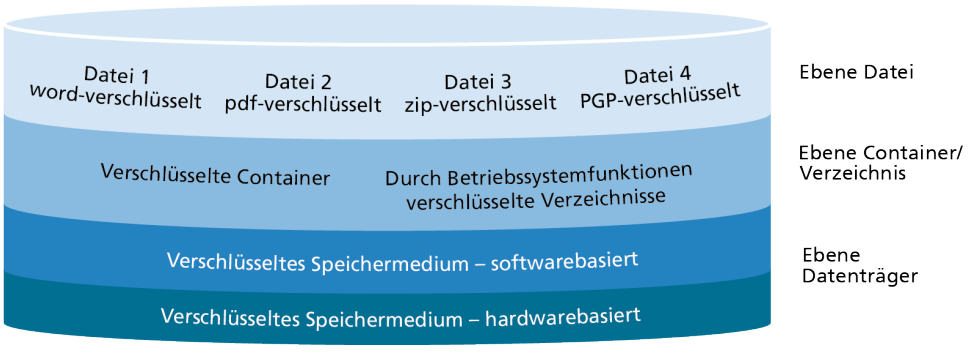


Abb. 07 Data at Rest: unterschiedliche Verfahren

Die Verfahren zur Verschlüsselung gespeicherter Daten werden nachfolgend in zwei Gruppen zusammengefasst dargestellt:

- Abschnitt 4.1.1 beschreibt die **Datenträgerverschlüsselung**, bei der vollständige Speichermedien oder festgelegte Teilbereiche (Partitionen, Volumes) von diesen verschlüsselt werden.

- Abschnitt 4.1.2 zeigt Möglichkeiten der **Datei- und Containerverschlüsselung** auf, bei der gezielt einzelne Dateien, Verzeichnisse oder logische Bereiche auf einem Speichermedium mithilfe entsprechender Funktionen des Betriebssystems, der Anwendungsprogramme oder spezialisierter kryptographischer Software verschlüsselt werden.

Zusätzlich wird in zwei weiteren Abschnitten die verschlüsselte Ablage von Daten in **Cloud-Speichern** (Abschnitt 4.1.3) und auf Besonderheiten beim **Backup** und bei der **Archivierung** verschlüsselter Daten (Abschnitte 4.1.4 und 4.1.5) eingegangen.

4.1.1 Datenträgerverschlüsselung

Bei der vollständige Datenträgerverschlüsselung (engl. »Full Disk Encryption«, FDE) werden alle Daten bei jedem Schreibvorgang auf den Datenträger oder einer seiner Partitionen verschlüsselt und ebenso automatisch wieder entschlüsselt, wenn sie vom Datenträger in den Hauptspeicher eingelesen werden. Aufgrund dieser Automatismen bleiben dem Benutzer somit die fehlerträchtigen Entscheidungen erspart, welche Dateien verschlüsselt werden sollen und welche nicht sowie welche Schlüssel er hierfür einsetzen soll. Lediglich beim ersten Zugriff auf einen Datenträger – im Falle eines verschlüsselten Betriebssystems beim Start dieses Systems – muss er durch Eingabe eines vorab festgelegten Kennworts oder einer anderen Art der Autorisierung (z. B. einer Smartcard, eines Fingerabdrucks oder eines USB-Tokens) die Entschlüsselung der Daten freigeben. Statt einer Vielzahl von Schlüsseln bei einer fallweisen Verschlüsselung von Dateien muss also nur ein einziger Schlüssel sicher verwaltet werden.

Die Begriffe **Schlüssel** und **Kenn-** oder **Passwort** werden häufig synonym benutzt. Sie bezeichnen jedoch unterschiedliche Sachverhalte: Der Schlüssel dient ausschließlich zum Verschlüsseln und wird meist direkt vom System vergeben und ist dort oder auf einem anderen Medium wie Smartcard, USB-Stick abgelegt. Um seine Vertraulichkeit zu schützen, wird ein Schlüssel mit einem Passwort geschützt.

Ein besonderer Vorteil der Datenträgerverschlüsselung liegt darin, dass dieser Schutz nicht nur die gespeicherten Dateien und deren Metadaten (Namen, Zeitstempel, Längenangaben, Ordnerstrukturen etc.) umfasst, sondern in der Regel auch die von den Anwendungsprogrammen angelegten temporären Dateien sowie – sofern die Systempartition verschlüsselt wurde – auch das Betriebssystem, dessen Auslagerungsdatei und weitere Systemdateien. Die Verschlüsselung der Systempartition hat damit auch den positiven Nebeneffekt, die Integrität des Betriebssystems gegen Manipulationen zu schützen.

Damit die gespeicherten Daten auch dann noch wieder entschlüsselt werden können, wenn etwa das als Zugriffsschutz gewählte Kennwort vergessen wurde oder der hierfür nötige Schlüssel beschädigt ist, bieten alle Lösungen Verfahren an, mit denen eine Entschlüsselung der Daten über Wiederherstellungskennwörter oder -schlüssel möglich bleibt. Diese werden bei Einrichtung des verschlüsselten Datenträgers erzeugt und müssen einerseits vor unberechtigten Zugriffen geschützt, andererseits aber auch für berechtigte Personen hinreichend zugänglich aufbewahrt werden.

Festplattenverschlüsselung bewahrt die Vertraulichkeit der auf einem Datenträger befindlichen Daten bei dessen Verlust oder Diebstahl. Diese Aufgabe wird zuverlässig erfüllt, solange ein Datenträger nicht im Einsatz ist. Dies gilt jedoch nicht mehr, sobald der Entschlüsselungsschlüssel nach Eingabe des Kennworts freigeschaltet ist und folglich keine weitere Authentisierung für die Entschlüsselung der Daten mehr erforderlich ist, also beispielsweise bei einem Laptop im Betriebszustand.

Sinnvoll ist die Datenträgerverschlüsselung in erster Linie für Laptops, USB-Sticks, externe Festplatten und andere mobile Geräte, die ein besonders hohes Diebstahls- und Verlustrisiko haben.

Grundsätzlich lassen sich hardware- und softwarebasierte Lösungen zur Datenträgerverschlüsselung unterscheiden:

- Als **hardwarebasierte Lösungen** werden von zahlreichen Hardware-Herstellern (Toshiba, Seagate, Plextor, Western Digital etc.) sogenannte selbstverschlüsselnde Festplatten und USB-Sticks angeboten (engl. »Self-encrypting Devices«, SED). Diese Medien, die deutlich teurer sind als solche ohne dieses Leistungsmerkmal, verschlüsseln und entschlüsseln die Daten vergleichsweise schnell mithilfe eines auf ihnen befindlichen speziellen Prozessors. Ihr Einsatz kommt also insbesondere dann infrage, wenn Rechenzeit ein kritischer Faktor ist.

  Einige SED-Festplatten bieten zusätzlich die Möglichkeit, sie (etwa mithilfe des TPM-Chips[1]) an eine bestimmte Hardware zu koppeln, sodass sie nur an festgelegten Computern lesbar sind. Es gibt auch Festplatten, die mit einer automatischen Löschfunktion ausgestattet sind und so konfiguriert werden können, dass der Entschlüsselungsschlüssel automatisch gelöscht wird, wenn mit »fremder« Hardware auf sie zugegriffen wird. Derartige Funktionen sind vor allem dann interessant, wenn die gespeicherten Daten besonders hohe Vertraulichkeitsanforderungen haben. Es ist vorab allerdings sehr sorgfältig abzuwägen, ob der zusätzliche Vertraulichkeitsschutz tatsächlich das erhöhte Risiko eines unwiederbringlichen Verlusts wichtiger Daten aufwiegt, der bei Defekten des verknüpften IT-Systems möglich wird.

- Bei **softwarebasierten Lösungen**, die wie Bitlocker für Windows oder FileVault 2 für Apple iOS fester Bestandteil aller neueren Versionen der gängigen Betriebssysteme sind, werden die kryptographischen Funktionen durch spezielle Programme oberhalb der Hardware-Schicht ausgeführt. Sowohl das gesamte System als auch einzelne Partitionen können verschlüsselt werden. Optionen zur Datenträgerverschlüsselung bieten auch Produkte kommerzieller Anbieter (z. B. von Symantec, Sophos, Checkpoint oder McAfee). Bis zu der Einstellung der Entwicklung der Software im Mai 2014 wurde für diesen Zweck sehr häufig auch das kostenfreie Open-Source-Tool TrueCrypt eingesetzt.

  Bei allen Verfahren werden die Daten mit einem symmetrischen Schlüssel verschlüsselt, der bei der Aktivierung der Verschlüsselung mit einem Zufallsverfahren erzeugt wird. Der Zugriff auf diesen Schlüssel, der beispielsweise im TPM-Chip, auf einem USB-Stick oder in einem Verzeichnisdienst (z. B. im Active Directory) abgelegt sein kann, wird durch ein festzulegendes Kennwort, einen Fingerprint, oder ein anderes Authentisierungsmittel geschützt.

  Softwarebasierte Verschlüsselungslösungen werden kostenpflichtig und zum Teil auch als Freeware angeboten. Kostenpflichtige Programme bieten unter anderem

[1] Trusted Platform Module – Bezeichnung für einen speziellen kryptographischen Sicherheitschip, der heutzutage für die meisten professionellen Computern angeboten wird.

den Vorteil, dass der Anbieter bei der Einrichtung und dem Betrieb der Software Unterstützung gewährt.

Darauf ist zu achten:

- Die Datenträgerverschlüsselung eignet sich vor allem dazu, die Vertraulichkeit von Informationen auf mobilen Geräten und Speichern zu schützen, da diese ein besonders hohes Diebstahl- oder Verlustrisiko haben.
- Sobald ein System im Betriebszustand ist, ist der Entschlüsselungsschlüssel freigeschaltet und bietet die Datenträgerverschlüsselung keinen Vertraulichkeitsschutz mehr. Besonders sensible Daten sollten daher zusätzlich durch weitere Maßnahmen geschützt werden (siehe Abschnitt 4.1.2).
- Wenn Rechenleistung besonders wichtig ist, empfehlen sich hardwarebasierte Lösungen zur Verschlüsselung.

4.1.2 Datei- und Containerverschlüsselung

Häufig ist es sinnvoll, nur ausgewählte Dateien, Ordner oder Verzeichnisse eines Datenträgers zu verschlüsseln. Hierfür dienen die in diesem Abschnitt beschriebenen Optionen zur Datei- und Containerverschlüsselung, mit denen einzelne besonders schützenswerte Elemente auch während des Betriebs eines Computersystems vor unerwünschter Einsichtnahme geschützt werden können. Ein Zugriff auf die jeweiligen Daten ist dabei erst nach Eingabe des passenden Kennworts möglich, so dass die Möglichkeit zur Einsichtnahme in gespeicherte Informationen gezielt auf einen gewünschten Benutzerkreis eingeschränkt werden kann, auch wenn noch weitere Benutzer auf ein Speichermedium zugreifen können. Verschlüsselte Dateien können darüber hinaus gesichert übertragen werden, zum Beispiel elektronisch als Anhang einer E-Mail oder manuell auf einem beliebigen Datenträger.

Es gibt grundsätzlich drei Wege, gezielt einzelne Dateien, Ordner oder Verzeichnisse zu verschlüsseln, nämlich

- die Nutzung der diesbezüglichen Funktionen in **Anwendungsprogrammen,**
- Verschlüsselung auf der Ebene des **Betriebssystems** oder aber
- den Einsatz dedizierter **Verschlüsselungsprogramme**.

Verschlüsselungsfunktionen von Anwendungsprogrammen

Alle gängigen Anwendungsprogramme (Office, Acrobat etc.) bieten die Möglichkeit zu einer symmetrischen Verschlüsselung, deren Benutzung insbesondere für den gelegentlichen Austausch von Dateien in kleineren Arbeitsgruppen sinnvoll sein kann. Verschlüsselt werden bei diesem Verfahren jedoch nur die eigentlichen Dateien, nicht jedoch Kopien oder temporäre Dateien, die das Anwendungsprogramm oder das Betriebssystem möglicherweise im Hintergrund erzeugen.

In älteren Versionen von Microsoft Office, Adobe Acrobat und anderer Software boten diese Funktionen wegen schwacher oder fehlerhaft implementierter Algorithmen nur

einen geringen Schutz. Dies gilt allerdings nicht mehr für die neueren Versionen, die eine derzeit als sicher geltende AES-Verschlüsselung mit 128 oder 256 Bit anwenden. Bei Wahl hinreichend sicherer, mindestens 18 Zeichen langer Passwörter ist dies ein unkomplizierter und in der Regel ausreichender Schutz für die Vertraulichkeit der Inhalte einer Datei. Die Verschlüsselungsfunktion von Kompressionsprogrammen wie WinZip oder 7-Zip erlaubt es darüber hinaus, Dateinamen, Verfasser, Speicherzeitpunkt und andere Metadaten der Dateien zu verbergen, die in einer Archivdatei aufbewahrt werden.

Mögliche **Schwachpunkte** der Verschlüsselung auf Anwendungsebene liegen in

- der langfristigen Sicherung des Zugriffs auf die verwendeten Schlüssel, also dem Schlüsselmanagement, sowie
- dem Schlüsselaustausch, wenn mehrere Benutzer Zugriff auf die verschlüsselten Dateien haben sollen.

Werden symmetrisch verschlüsselte Dateien ausgetauscht, muss das Kennwort, mit dem der Schlüssel geschützt wird, den gewünschten Kommunikationspartnern auf sichere Weise zugänglich gemacht werden. Je umfangreicher dieser Personenkreis, desto aufwendiger und unsicherer wird der Austausch dieser Informationen. Für den regelmäßigen und professionellen Einsatz ist diese Variante der Verschlüsselung daher nur begrenzt geeignet.

Verschlüsselungsfunktionen des Betriebssystems

Seit Windows XP enthalten die Microsoft-Betriebssysteme das Encrypting File System (EFS), mit dem eine Datei oder auch ein Verzeichnis unter Nutzung des öffentlichen Schlüssels eines oder mehrerer Benutzer verschlüsselt werden kann. Bei jedem Verschlüsselungsvorgang wird ein neuer symmetrischer Verschlüsselungsschlüssel (»File Encryption Key«) erzeugt, der mit den öffentlichen Schlüsseln der zur Entschlüsselung berechtigten Personen verschlüsselt wird. Die Entschlüsselung erfolgt mit den privaten Schlüsseln der Berechtigten in einem für die Benutzer transparenten Verfahren. Die öffentlichen Schlüssel sind im Active Directory verfügbar, es können aber auch bereits implementierte Public-Key-Infrastrukturen genutzt werden.

Zusätzlich wird bei jeder Verschlüsselung der öffentliche Schlüssel eines ausgewählten Benutzers verwendet, der als »Key Recovery Agent« (bzw. »Data Recovery Agent«) fungiert, damit auch bei Verlust oder Beschädigung eines privaten Schlüssels Dateien und Verzeichnisse wieder entschlüsselt werden können. Bei einer entsprechenden Konfiguration dieses Agenten können Dateiinhalte auch vor Systemadministratoren verborgen werden.

Mithilfe der frei verfügbaren Betriebssystemerweiterung EncFS[1] gibt es auch Möglichkeiten zur Verschlüsselung einzelner Dateien und Verzeichnisse unter Unix/Linux oder Apple iOS.

Die Verschlüsselung der Dateien und Verzeichnisse auf Betriebssystemebene ist für Benutzer sehr einfach zu handhaben, die Administration des Systems und insbesondere auch die Verwaltung der Schlüssel sind jedoch insbesondere bei der Nutzung von Gruppenlaufwerken außerordentlich komplex und fehlerträchtig. Ob eine Arbeitsgruppe, die Ressourcen im Netz benutzt, die Dateiverschlüsselung des EFS verwenden sollte,

[1] Encrypting File System

muss daher sehr sorgfältig unter Abwägung des Administrationsaufwands geprüft werden.

Dedizierte Verschlüsselungsprogramme

Es gibt eine Fülle von Tools zur Verschlüsselung von Dateien. Einige der in Abschnitt 4.1.1 vorgestellten Softwarelösungen zur Verschlüsselung von Datenträgern können auch genutzt werden, um einzelne Dateien oder Verzeichnisse symmetrisch oder asymmetrisch zu verschlüsseln. Besondere Bedeutung hat das Programm PGP als asymmetrisches Verschlüsselungsverfahren gewonnen. PGP ist eine Software, die im Anwendungskontext der E-Mail-Verschlüsselung entwickelt wurde, aber auch Optionen für die Dateiverschlüsselung bietet. Dies gilt sowohl für die freien Lösungen GnuPG (GNU Privacy Guard) und Gpg4win (GNU Privacy Guard for Windows) als auch die kommerziellen Versionen dieser im Laufe ihrer Geschichte von verschiedenen Herstellern angebotenen kryptographischen Software. Die kostenpflichtigen Versionen bieten darüber hinaus weitere Funktionen wie die Unterstützung unterschiedlicher Authentifizierungsverfahren, Instrumente zur Durchsetzung von Richtlinien sowie ein zentrales Schlüsselmanagement (einschließlich der Verfahren und zur Rekonstruktion der Schlüssel oder der verschlüsselten Daten bei Verlust oder Beschädigung eines geheimen Schlüssels).

Viele Verschlüsselungstools bieten ferner eine besondere Form der Verschlüsselung an: die sogenannte **Container-Verschlüsselung.** Bei dieser dient eine spezielle Datei als »Container« für die verschlüsselte Ablage vertraulicher Daten. Nach außen hin erscheint ein solcher Speicherbereich wie eine (virtuelle) Partition, die gezielt ausgeblendet und verborgen werden kann und erst durch Eingabe eines Passworts aktiviert wird. Einmal aktiviert kann der Container wie ein normales Dateisystem verwendet werden. Die Dateien können also in Verzeichnissen strukturiert abgelegt werden mit der Besonderheit, dass diese wie bei der Datenträgerverschlüsselung ohne weiteres Zutun des Benutzers verschlüsselt werden. Komplette Container können darüber hinaus als einzelne Datei auf einem Speichermedium gesichert werden. In diesem Sinn können verschlüsselte Archivdateien, die mithilfe von Komprimierungsprogrammen wie WinZip oder 7-Zip erzeugt wurden, ebenfalls als Container verstanden werden.

Darauf ist zu achten:

- Im Gegensatz zur Datenträgerverschlüsselung ist die Datei- und Verzeichnisverschlüsselung auch geeignet, die Vertraulichkeit von Daten auf Rechnern differenziert nach Benutzerkreisen zu schützen.

- Viele Anwendungsprogramme bieten eine Verschlüsselungsfunktion, um einzelne Dateien zu schützen und damit auch beispielsweise dem Zugriff des Administrators zu entziehen. Diese Option kann auch gewählt werden, um eine Datei per E-Mail verschlüsselt zu übertragen. Dies ist eine einfache Maßnahme, die den Vertraulichkeitsschutz für sensible Daten signifikant erhöht.

- Verfahren, bei denen sich ein Anwender selbst um die Verteilung und die Sicherheit der Schlüssel kümmern muss, sind fehleranfällig. Es besteht das Risiko, dass Schlüssel nicht mehr im Zugriff sind oder aber an Unberechtigte gelangen. Wenn sehr wichtige Informationen verschlüsselt werden, auf die langfristig zugegriffen werden muss, sind die Verfahren für die Verwaltung der Schlüssel sehr sorgfältig festzulegen (siehe Kapitel 4.3).

4.1.3 Verschlüsselung von Daten in der Cloud

Cloud-Dienste können in vielfältiger Weise dazu beitragen, die Effizienz von Arbeitsabläufen bei verteilt arbeitenden Arbeitsgruppen zu erhöhen und erleichtern ein standortunabhängiges Arbeiten, selbst wenn keine speziellen Kollaborationswerkzeuge im Einsatz sind (siehe dazu Abschnitt 4.2.4).

Eine besondere Form von Cloud-Diensten sind die sogenannten Cloud-Speicher-Dienste. Diese werden unter Namen wie CloudMe, CrashPlan, Dropbox, Google Drive oder Wuala angeboten. Solche Dienste lassen sich z. B. mit der frei verfügbaren Software ownCloud aber auch in Eigenregie (oder einen darauf spezialisierten Serverdienst) betreiben.

Die über den Cloud-Speicher-Dienst angebotenen Ressourcen dienen als zentrale Ablage für dezentral erhobene und genutzte Daten oder für das Backup von Dokumenten, ermöglichen die Synchronisation der Daten zwischen mobilen Geräten und Rechnern im Firmennetz oder erleichtern das File-Sharing in kooperativen Arbeitsumgebungen. Derartige Online-Speicher haben den großen Vorteil, dass auf sie von überall und zu jeder Zeit von unterschiedlichsten Geräten aus zugegriffen werden kann und die Speicherkapazität praktisch beliebig erweiterbar ist. Ohne ergänzende Sicherheitsmaßnahmen ist die Benutzung von Cloud-Speicherdiensten aber auch mit dem Risiko verbunden, dass die Vertraulichkeit der gespeicherten Daten verletzt werden kann. Um dieses Risiko zu minimieren, ist es daher notwendig, die Daten sowohl bei der Übertragung als auch ihrer Speicherung durch Verschlüsselung zu schützen:

- Für den sicheren Transport muss zwischen den Systemen des Benutzers und den Cloud-Speichern eine mittels SSL/TLS gesicherte Verbindung bestehen (siehe dazu auch Abschnitt 4.2). Diese Anforderung wird von den Anbietern der Cloud-Dienste in der Regel erfüllt.

- Viele Hersteller bieten eine verschlüsselte Datenablage an, bei dieser verbleiben die hierfür verwendeten Schlüssel häufig jedoch in der Obhut des jeweiligen Providers, der dadurch die Daten für sich oder interessierte Dritte einsehbar machen könnte. Die Vertraulichkeit der Daten hängt folglich von der Vertrauenswürdigkeit des Anbieters ab. Offen bleibt auch, wie sicher dieser seine Schlüsselverwaltung organisiert oder welche rechtlichen Verpflichtungen dieser gegenüber staatlichen Einrichtungen hat, den Verschlüsselungsschutz von Daten aufzuheben.

Fraunhofer SIT hat in der im Jahr 2012 veröffentlichten Studie »On the Security of Cloud Storage Services«[1] die Sicherheit vieler weithin eingesetzter Cloud-Speicherdienste untersucht. Keines der betrachteten sieben Produkte erfüllte alle Sicherheitsanforderungen. Besonders große Defizite gab es bei der Verschlüsselung: Nur zwei Produkte boten die Möglichkeit einer Verschlüsselung der Daten vor dem Transfer in den Cloud-Speicher, bei dem die Daten sowohl verschlüsselt übertragen werden als auch eine unerwünschte Einsichtnahme in die Daten beispielsweise durch Mitarbeiter des Cloud-Betreibers hinreichend wirksam ausgeschlossen wird.

Folgende Verfahren bieten sich an, um eine verschlüsselte Übertragung als auch Speicherung der Daten zu erreichen:

- alle in Kapitel 4.1.2 genannten Möglichkeiten zur Verschlüsselung auf Dateiebene,

[1] Siehe www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Cloud-Storage-Security_a4.pdf.

- Verschlüsselungsfunktionen in der von manchen Cloud-Service-Providern (z. B. von Wuala) bereitgestellten Client-Software oder

- spezielle Zusatzsoftware, die für häufig genutzte Online-Speicherdienste Verschlüsselung ermöglicht (z. B. BoxCryptor).

Die als Zusatzsoftware angebotenen Tools werden zum Teil kostenlos abgegeben, meist aber nur an Privatanwender oder nur mit Grundfunktionen. Funktionen, die für den geschäftlichen Einsatz von Bedeutung sein können, fehlen darin in der Regel. Es gibt z. B. keine Verschlüsselung der Dateinamen, nur eine eingeschränkte Anzahl unterstützter Cloud-Service-Provider, keinen Support, nur begrenzte Möglichkeiten zur Integration ins Unternehmensnetz oder aber nur eine geringe Speicherkapazität. Viele kostenpflichtige Tools unterstützen gleichzeitig mehrere Speicheranbieter und können beispielsweise für jeden Provider einen eigenen Ordner auf dem Client anlegen, der mit dem Cloud-Speicher des Cloud-Service-Providers synchronisiert wird. Manche Tools unterstützen auch die Zusammenarbeit mehrerer Benutzer.

Wenn und solange die für Entschlüsselung der Daten erforderlichen Schlüssel beim Benutzer verbleiben, sind die vorstehend genannten Verfahren zur Verschlüsselung eine sichere Möglichkeit, die Vertraulichkeit der Daten in der Cloud zu wahren. Der Benutzer muss sich aber seiner Verantwortung für die Verfügbarkeit und Vertraulichkeit der verwendeten kryptographischen Schlüssel und Kennwörter bewusst sein und entsprechend sorgfältig mit ihnen umgehen.

Eine vertrauliche Speicherung von Daten in der Cloud verspricht das Produkt IDGard der Münchner Firma Uniscon.[1] Es beruht auf dem Konzept der »Sealed Cloud«, das durch ein Bündel an technischen und ergänzenden organisatorischen Vorkehrungen – z. B. durch Prüfung der eingesetzten Hardware, eine ausgeklügelte Schlüsselverwaltung sowie eine unabhängige Auditierung des Cloud-Betreibers – dafür sorgt, dass die Kundendaten (einschließlich ihrer Metadaten) vollständig vor unerwünschten Zugriffen geschützt bleiben. Auch die Administratoren der Cloud-Infrastruktur haben gemäß des Konzepts der »Sealed Cloud« keine Möglichkeit zur Einsichtnahme in die Daten.

Einen sicheren, unternehmensweiten Einsatz von Cloud-Diensten verfolgt auch das Produkt »OmniCloud« von Fraunhofer SIT.[2] Zielsetzung von »OmniCloud« ist es, über eine Gateway-gestützte Lösung Anwendern einen einfachen Zugang zu Cloud-Speicherdiensten zu bieten und gleichzeitig die gespeicherten Daten durch Verschlüsselung zuverlässig gegen Spähangriffe zu schützen. Durch die Integration weiterer Funktionen – etwa die Kombination mehrerer Cloud-Speicher zu einem großen, die Speichereinsparung durch Vermeidung von Datendubletten in der Cloud oder die Unterstützung gemeinsamer Ordner zum Datenaustausch innerhalb eines Projekts – unterscheidet sich diese Lösung von den momentan angebotenen Produkten.

Darauf ist zu achten:

- Bei der Nutzung von Cloud-Speicherdiensten sollten sowohl der Transfer zum Provider als auch die Ablage der Dateien verschlüsselt erfolgen. Letzteres ist nur dann sicher gewährleistet, wenn die Daten vor ihrer Übertragung zur Cloud verschlüsselt werden.

[1] Siehe www.IDGard.de.
[2] Siehe www.omnicloud.sit.fraunhofer.de.

- Eine von einem Cloud-Storage-Dienst bereitgestellte verschlüsselte Ablage, bei der die verwendeten Schlüssel durch den Anbieter verwaltet werden, entlastet den Kunden zwar von der Aufgabe, sich um das Schlüsselmanagement kümmern zu müssen, bietet jedoch nur eine eingeschränkte Sicherheit. Weil die Schlüssel im Zugriff des Cloud-Anbieters sind, kann dieser jederzeit Einsicht in die gespeicherten Daten nehmen oder Dritten gewähren.

- Immer dann, wenn Anwendungsprogramme beim Provider genutzt werden, zum Beispiel solche zur Textverarbeitung, sind die Daten während der Bearbeitung unverschlüsselt. Wie in Kapitel 4 eingangs beschrieben ist eine kryptographische Absicherung von in Bearbeitung befindlichen Daten mit heutiger Hardware nämlich in der Regel noch nicht effizient anwendbar.

4.1.4 Datensicherung (Backup)

Vorrangiges Ziel einer Datensicherung (Backup) ist es, die Verfügbarkeit von Programmen und Daten z. B. nach einem Systemdefekt oder versehentlichem Löschen wieder herstellen zu können. In der Regel werden dazu die Daten und Programme in regelmäßigen Abständen auf externe Datenträger (Band, DVD, Platte etc.) gesichert und diese dann an einem sicheren Ort verwahrt. Sofern die Daten vor dem Backup nicht bereits schon verschlüsselt waren, kann die Vertraulichkeit der gesicherten Daten sowohl auf dem Transportweg (z. B. durch einen externen Dienstleister) des Datenträgers zum Aufbewahrungsort und am Aufbewahrungsort selbst gefährdet sein.

Um die Vertraulichkeit von Backups durch Verschlüsselung sicherzustellen, bieten sich zwei Lösungsvarianten an:

- Bei der ersten Variante werden vor Durchführung des Backups alle als vertraulich eingestuften Daten mit einem der gängigen Verschlüsselungsprogramme (siehe Abschnitt 4.1.2) verschlüsselt und erst danach auf dem Datenträger gesichert, der für das Backup verwendet wird.

  Die Sicherung bereits verschlüsselter Daten in Containern kann zeitaufwendiger sein, da die Daten immer vollständig gesichert werden, sobald eine einzige Datei sich im Container geändert hat. Eine inkrementelle Sicherung von nur geänderten Dateien ist bei der Containerverschlüsselung nicht möglich.

- Bei der zweiten Variante wird ein Backup vollständig verschlüsselt. Dies sollte insbesondere dann überlegt werden, wenn die verwendeten Datenträger an Orten aufbewahrt oder über Wege übertragen werden, bei denen der Zugriff nur bedingt kontrolliert werden kann. Es gibt eine Reihe an Backup-Programmen, die eine solche Option anbietet. Hierbei werden alle Daten bei der Sicherung mithilfe eines zufällig erzeugten symmetrischen Schlüssels verschlüsselt und mit einem Kennwort geschützt auf dem Backup-Datenträger abgelegt. Beim Wiedereinspielen werden die Daten dann wieder entschlüsselt. Dies ist allerdings nur nach Eingabe des Kennworts und bei Zugriff auf den aus Sicherheitsgründen nicht auf dem Backup-Datenträger abgelegten Verschlüsselungsschlüssel möglich.

Darauf ist zu achten:

- Sensible Daten sind auch bei der Datensicherung verschlüsselt abzulegen.

- Beim Backup eines verschlüsselten Datenträgers werden alle dort gespeicherten Daten entschlüsselt. Auf dem Backup-Medium sind folglich nur solche Daten verschlüsselt, die explizit mithilfe der Datei- oder Containerverschlüsselung verschlüsselt wurden (siehe Abschnitt 4.1.2), es sei denn, das oben beschriebene Verfahren zur vollständigen Verschlüsselung einer Datensicherung wurde angewendet.

- Kopien der Schlüssel und der vergebenen Kennwörter sollten an einem sicheren Ort außerhalb des Systems verwahrt werden, um die Verfügbarkeit der Backups in Notfällen wieder an die Daten gelangen zu können, beispielsweise bei Beschädigung eines Schlüssels, beim Vergessen eines Kennworts oder bei Abwesenheit des Administrators, der üblicherweise Zugriff auf diese Berechtigungsnachweise hat.

- Wenn es bei der Sicherung verschlüsselter Informationen zu Fehlern kommt, sind meist die Daten nicht mehr brauchbar. Die Datensicherung ist daher – auch wiederholt – sorgfältig zu testen.

4.1.5 Archivierung

Ein Backup zielt darauf ab, die bei einem Ausfall oder der Störung von IT-Systemen drohenden Datenverluste zu minimieren, um die Arbeitsfähigkeit der Geschäftsprozesse sicherzustellen. Hierfür genügt es in der Regel, wenn auf die gesicherten Datenbestände der letzten Wochen oder Monate zurückgreifen zu können. Archivierung zielt im Gegensatz dazu auf eine längerfristige Speicherung von Daten und dient darüber hinaus auch noch weiteren Zwecken. Beispielsweise müssen geschäftsprozessbezogene Dokumente und E-Mails revisionssicher aufbewahrt werden, steuerrelevante Unterlagen oder Geschäftsbriefe etwa bis zu zehn Jahren, Verträge oft sogar noch länger. Dies kann in digitaler Form durch elektronische Archivsysteme geschehen, die heutzutage meist Teil umfassender Dokumentenmanagementsysteme (DMS) sind. Die verwendeten Archivierungslösungen müssen die Informationsbestände langfristig gegen Manipulation schützen und sie reproduzieren können.

Damit auch nach vielen Jahren Dokumente noch entschlüsselt werden können, müssen nicht nur Hard- und Softwareplattformen in aktuelle Systemumgebungen migrieren, sondern es muss auch auf ein langfristig funktionierendes Schlüsselmanagement geachtet werden. Dies kann für große Archive mit hohem Aufwand verbunden sein. Aktuelle DMS-Produkte können Dokumente auch verschlüsselt ablegen und bieten hierfür eigene Schlüsselverwaltungssysteme an.

Für elektronisch verschlüsselte und signierte Dokumente ist zu beachten, dass Schlüssel im Zeitablauf an Sicherheitswirkung verlieren (»altern«), beispielsweise weil aufgrund leistungsfähigerer Hardware die verwendeten Schlüssellängen nicht mehr hinreichend sicher sind. Im Lauf der Zeit kann daher eine Umschlüsselung erforderlich sein.

Um sicherzustellen, dass Dokumente über einen langen Zeitraum lesbar bleiben, aber auch hinreichend sicher verschlüsselt sind, müssen organisatorische Maßnahmen zur Verwaltung der Schlüssel implementiert und dem Stand der Technik entsprechende kryptographische Verfahren genutzt werden. Dies gilt insbesondere dann, wenn die Integrität elektronischer Archive zur Erfüllung gesetzlicher Anforderungen mithilfe von

elektronischen Signaturen geschützt wird. Diese Problematik und Lösungen hierzu werden ausführlich in dem SIT-Whitepaper »Warum digitale Signaturen altern und wie man trotzdem ihren Wert erhält«[1] beschrieben.

Umfassende Empfehlungen und ein Vorgehensmodell für den Aufbau und den Betrieb eines Archivsystems, das die Integrität und Vertraulichkeit der Informationen gewährleistet, enthält der Baustein B 1.12: »Archivierung« der IT-Grundschutz-Kataloge.[2]

Darauf ist zu achten:

- Bei der Archivierung verschlüsselter Informationen ist besonders darauf zu achten, dass die verwendeten Schlüssel langfristig geschützt und reproduzierbar bleiben.
- Es ist zu berücksichtigen, dass Schlüssel und Verschlüsselungsverfahren im Zeitablauf an Sicherheitswirkung verlieren und eine Umschlüsselung der Daten erforderlich ist. Hierfür sind geeignete Verfahren zu festzulegen.

4.2 Übertragung von Informationen (»Data in Transit«)

Praktisch jeder Betrieb ist heute auf Datenübertragung angewiesen, also die Möglichkeit, auf elektronischem Wege Informationen von anderen Instanzen zu empfangen oder an diese zu versenden. Hierbei ist zunächst zweitrangig, ob Daten lediglich unternehmensintern oder mit externen Partnern (z. B. Kunden, Lieferanten oder Consultants) ausgetauscht werden. In beiden Fällen können Daten über offene Netze übertragen werden und ist folglich die Vertraulichkeit der enthaltenen Informationen gegen unbefugtes Mitlesen durch Dritte zu schützen. Dies lässt sich am besten durch eine angemessene Verschlüsselung realisieren. Es gibt zahlreiche Verfahren zur verschlüsselten Datenübermittlung. Dies gilt gleichermaßen für E-Mails wie auch für die Sprach- und Videotelefonie bis hin zu Protokollen, die z. B. in der unternehmensinternen Netzwerkkommunikation zum Einsatz kommen. In allen Fällen hängt die Wahl der optimalen Verschlüsselung sowohl vom genutzten Dienst als auch vom Übertragungsweg ab. Zu bedenken ist darüber hinaus, dass manche Dienste auch das Zwischenspeichern von Daten in der Infrastruktur von Dienstbetreibern erforderlich machen, beispielsweise zur Vermittlung von E-Mails über einen oder mehrere E-Mail-Provider.

Abb. 08 zeigt mögliche Verschlüsselungslösungen am Beispiel des Versands von E-Mail sowie beim Austausch von Dateien über zentrale Online-Speicher (etwa einem Cloud-Speicherdienst oder einem Versionsverwaltungsarchiv). Die verschiedenen Ebenen (Anwendungsschicht, Transportschicht etc.), auf denen Verschlüsselungsmechanismen eingesetzt werden können, sind angelehnt an das ISO/OSI-Referenzmodell[3], ein standardisiertes System zur Einordnung und Beschreibung technischer Kommunikation.[4]

Sowohl beim Versand von E-Mails über Mail Service Provider als auch beim Austausch von Dateien über zentrale Speicherdienste (z. B. über Content- oder Cloud-Service-Provider) empfiehlt sich die Nutzung eines verschlüsselten Transportprotokolls (meist

[1] Siehe www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/whitepaper-archisoft-2009-de.pdf.

[2] Siehe unter www.bsi.bund.de/IT-Grundschutz-Kataloge.

[3] International Organization for Standardization/Open Systems Interconnection

[4] Siehe auch die Darstellung in Maßnahme M 4.90: *Einsatz von kryptographischen Verfahren auf den verschiedenen Schichten des ISO/OSI-Referenzmodells* der IT-Grundschutz-Kataloge www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04090.html.

auf Basis von SSL/TLS). Diese Verschlüsselung schützt die Daten gegen unbefugtes Mitlesen beim Transport durch das Internet zwischen Anwender und Provider, jedoch nicht bei den Providern selbst oder zwischen den verschiedenen Providern. Außerdem ist zu beachten, dass sämtliche Daten (z. B. E-Mails oder auszutauschende Dateien) möglicherweise auf den Servern der Provider vorübergehend oder dauerhaft unverschlüsselt abgelegt werden, selbst wenn für den Versand eine Transportverschlüsselung genutzt wurde. Für den Austausch von Dateien über zentrale Speicherdienste empfiehlt sich deshalb die Verschlüsselung der Daten vor dem Hochladen mit einem geeigneten Verschlüsselungswerkzeug (siehe Abschnitt 4.1.2). Bei E-Mail empfiehlt sich eine Ende-zu-Ende-Verschlüsselung in der Anwendungsschicht. So ist sichergestellt, dass nur berechtigte Empfänger ihren Inhalt dechiffrieren können (näheres dazu in Abschnitt 4.2.1).

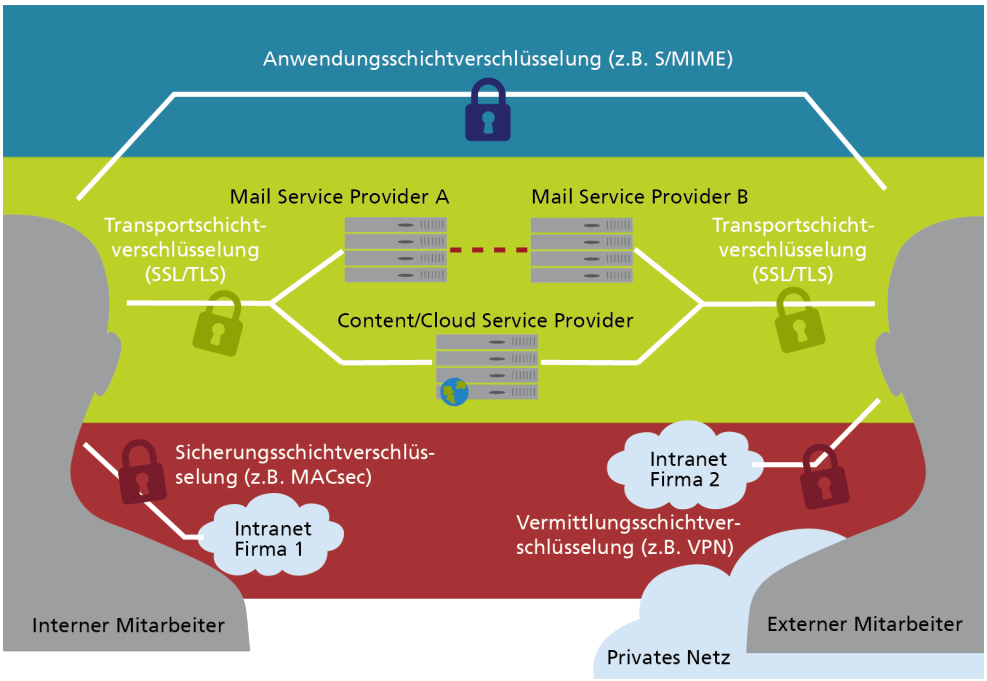


Abb. 08 Verschlüsselungslösungen bei der Übertragung von Informationen

Abb. 08 zeigt als weiteres Anwendungsbeispiel die Art der Anbindung von Computern an Firmennetze. Der PC des links unten dargestellten Mitarbeiters ist direkt mit dem internen Netz der Firma 1 verbunden. Dieses ist im Beispiel mit einer Verschlüsselung auf der Sicherungsschicht (z. B. MACsec[1]) geschützt, um Insider-Angriffen vorzubeugen. Der PC des rechts unten abgebildeten Mitarbeiters ist hingegen aus Firmensicht an ein Fremdnetz angeschlossen, im Beispiel an ein privates Netz, das Heimnetz des Telearbeiters. Mit einem VPN[2] wird ein verschlüsselter Tunnel in das Firmennetz aufgebaut, über den ein geschützter Datenaustausch zwischen dem Firmennetz und dem Computer des Mitarbeiters gewährleistet wird.

MACsec ist ein Protokoll, das u. a. die verschlüsselte Übermittlung von Daten z. B. in einem Firmennetz über Ethernet ermöglicht. Mit MACsec können nichtautorisierte LAN-Verbindungen identifiziert und die entsprechenden Komponenten von der Kommunikation innerhalb des jeweiligen Netzes ausgeschlossen werden.

[1] Media Access Control secure
[2] Virtual Private Network, Virtuelles Privates Netzwerk

4.2.1 E-Mail-Kommunikation

Ein großer Teil der heutigen internen und externen Unternehmenskommunikation basiert auf dem Austausch von E-Mails. Wie bereits beispielhaft in der Einleitung des Abschnitts 4.2 erwähnt, sollte für die Übermittlung von E-Mails grundsätzlich eine Transportverschlüsselung mittels SSL/TLS eingesetzt werden. Dies schützt die E-Mail vor unberechtigtem Mitlesen und Verfälschen auf dem Weg zwischen dem eigenen E-Mail-Programm und dem Server des eigenen E-Mail-Dienstanbieters. SSL/TLS wird von allen seriösen Anbietern von E-Mail-Diensten und allen aktuellen E-Mail-Programmen unterstützt, ist in letzteren allerdings nicht immer voreingestellt. Gegebenenfalls müssen daher also alle E-Mail-Programme innerhalb des Unternehmens entsprechend angepasst werden. Die exakte Konfiguration der Programme ist abhängig von verschiedenen Parametern, die beim E-Mail-Dienstbetreiber erfragt werden können. Grundsätzlich kann ein Anwender nicht ohne Weiteres nachvollziehen, ob im Rahmen des E-Mail-Versands bzw. -Empfangs eine Transportverschlüsselung eingesetzt wird. Hierzu sollte ggf. der Administrator des eigenen Unternehmens befragt werden.

Bei der **Ende-zu-Ende-Verschlüsselung** wird eine Nachricht (z. B. eine E-Mail) so verschlüsselt, dass nur ihr Empfänger sie wieder entschlüsseln kann. Die Nachricht ist also auf dem vollständigen Weg vom Sender zum Empfänger vor unerwünschten Mitlesern geschützt.
Unter **Hop-by-Hop-Verschlüsselung** versteht man die abschnittsweise Verschlüsselung einer Datenübertragung. Hierbei werden die Daten beim Eintritt in den jeweiligen Transportabschnitt verschlüsselt und liegen am Ende des betreffenden Abschnitts wiederum unverschlüsselt vor. Ein Beispiel hierfür ist eine Transportverschlüsselung (meist mit SSL/TLS) lediglich vom E-Mail-Client bis zum E-Mail-Server des eigenen Providers. Was auf den übrigen Kommunikationsabschnitten geschieht, entzieht sich der Kontrolle des Benutzers.

Transportverschlüsselung kann eine E-Mail jedoch nur auf der Übermittlungsstrecke zwischen einem Unternehmen und seinem E-Mail-Dienstanbieter schützen (sogenannte Hop-by-Hop-Verschlüsselung). Sie garantiert weder eine verschlüsselte Ablage auf den Servern des Dienstanbieters noch eine geschützte Weitervermittlung an den Adressaten. Beides kann jedoch mit einer sogenannten Ende-zu-Ende-Verschlüsselung erreicht werden. Hierdurch entsteht ein wirksamer Schutz gegen unbefugtes Mitlesen der E-Mail auf ihrem gesamten Weg vom Absender bis zum Empfänger (»Ende-zu-Ende«) über sämtliche Zwischeninstanzen hinweg.

Für größere Unternehmen stellt das S/MIME[1]-Verfahren eine gute Wahl für die Ende-zu-Ende-Verschlüsselung von E-Mails dar. Es bietet eine vollständige Integration in eine PKI (siehe Abschnitt 3.3), die ausgestellten Schlüssel können also von einer zentralen Instanz ausgegeben, verwaltet und zurückgezogen werden. So können interne und externe Kommunikationspartner über die Zertifizierungsinstanz die Schlüssel aller Betriebsangehörigen abrufen und validieren.

Alternativ dazu kann ein auf PGP[2] basierendes Verfahren eingesetzt werden. Die Qualität der verwendeten kryptographischen Verfahren ist mit der von S/MIME vergleichbar. Allerdings muss bei PGP das Vertrauen in den Absender einer E-Mail selbst von den Benutzern verwaltet werden, da es keine zentrale Zertifizierungsinstanz (z. B. in Form einer PKI) gibt.

[1] Secure/Multipurpose Internet Mail Extension
[2] Pretty Good Privacy

Eine echte Ende-zu-Ende-Verschlüsselung bis zum E-Mail-Client auf dem Computer des Anwenders kann jedoch auch Nachteile mit sich bringen. Beispielsweise können verschlüsselte E-Mails, mit deren Hilfe Schadprogramme in das Unternehmen eingeschleust werden sollen, nicht durch zentrale Filter-Instanzen erkannt und abgefangen werden. Der Grund hierfür ist, dass diese Filter keinen Zugriff auf die zur Entschlüsselung erforderlichen geheimen Schlüssel haben.

Abhilfe kann eine kommerzielle E-Mail-Gateway-Lösung mit integrierter Verschlüsselungsfunktion schaffen, wie sie von verschiedenen Herstellern angeboten wird (z. B. von Sophos, Symantec oder Zertificon). Derartige Lösungen bieten typischerweise Funktionen zum Untersuchen eingehender E-Mails auf schädliche Dateianhänge oder zum Zurückhalten von Spam-Mails. Gleichzeitig kann ggf. das unerlaubte Versenden unternehmensinterner Daten an externe Empfänger erkannt und verhindert werden (Data Leakage Prevention). Die Gateway-Lösung benötigt zur Erfüllung ihrer Aufgabe Zugriff auf den Klartext aller ein- und ausgehenden E-Mails. Aus diesem Grund sollte eine solche Lösung ausschließlich von einem vertrauenswürdigen Hersteller bezogen werden. Des Weiteren sollte beachtet werden, dass die Verschlüsselung im Gegensatz zu einer Ende-zu-Ende-Verschlüsselung nicht im E-Mail-Client des Mail-Absenders oder -Empfängers, sondern im E-Mail-Gateway des jeweiligen Unternehmens terminiert wird. Der Einsatz einer E-Mail-Gateway-Lösung (auch Krypto-Gateway genannt) in einem Unternehmen bedingt nicht, dass Kommunikationspartner, mit denen verschlüsselte E-Mail ausgetauscht werden sollen, ebenfalls über ein E-Mail-Gateway verfügen. Auch der Betrieb einer PKI ist von keiner Seite zwingend erforderlich.

Aus Anwendersicht liegt der Vorteil eines derartigen Gateways u. a. in der Transparenz der Verschlüsselungsmaßnahmen für den Nutzer, was zu einer im Vergleich zu herkömmlichen E-Mail-Verschlüsselungslösungen deutlich leichteren Bedienbarkeit führt. So kann der Anwender E-Mails erstellen und versenden oder empfangen, ohne sich Gedanken über ggf. notwendige Maßnahmen zur Ver- bzw. Entschlüsselung machen zu müssen. Hierzu untersucht das zentral im Firmennetz aufgestellte Gateway sowohl ein- als auch ausgehende E-Mails und wendet bei Bedarf geeignete Ver- bzw. Entschlüsselungsverfahren an. Die Regeln, anhand derer über eine Verschlüsselung ausgehender E-Mails entschieden wird, können durch den Administrator des Gateways festgelegt werden. Beispielsweise könnte eine solche Regel vorsehen, dass alle E-Mails an ein bestimmtes Unternehmen grundsätzlich etwa mittels PGP verschlüsselt werden müssen, egal welcher Mitarbeiter des eigenen Unternehmens die E-Mail abgesendet hat.

Unabhängig davon, ob eine Verschlüsselung per E-Mail-Client oder per Krypto-Gateway erfolgt, ist die Verschlüsselung von Sender- und Empfänger-Adressen aus technischen Gründen auf eine Hop-by-Hop-Verschlüsselung beschränkt, da die Server aller beteiligten E-Mail-Provider diese Informationen für das Weiterleiten der E-Mails benötigen.

S/MIME (Secure/Multipurpose Internet Mail Extension) ist eine standardisierte Methode zur Ende-zu-Ende-Verschlüsselung von E-Mail-Inhalten. Es basiert auf einem Public-Key-Verfahren und benötigt eine PKI (Public-Key-Infrastruktur) zum Betrieb.

PGP (Pretty Good Privacy) stellt Verschlüsselungsdienste für E-Mail-Inhalte sowie Dateien bereit. Über herkömmliche E-Mail-Dienste kann so eine Ende-zu-Ende-Verschlüsselung eingerichtet werden. PGP basiert auf einem Public-Key-Verfahren, bietet jedoch kein integriertes Schlüsselmanagement. Die Nutzer müssen also selbst für die Schlüsselverwaltung sorgen.

Sowohl die unternehmensweite Etablierung von Ende-zu-Ende-Verschlüsselung als auch die Anschaffung entsprechender E-Mail-Gateways erfordert gewisse Investitionen. Ob und in welchem Fällen sich diese rentieren, hängt auch von den Anforderungen der Kommunikationspartner eines Unternehmens ab, z. B. den bestehenden oder erwarte-

ten Geschäftspartnern. Die Einführung entsprechender Verschlüsselungslösungen kann beispielsweise der Schaffung von Schnittstellen für die vertrauensvolle Kommunikation zwischen Unternehmen dienen oder zu deren Interoperabilität beitragen.

Sollen lediglich in Einzelfällen Textdokumente oder sonstige Dateien verschlüsselt per E-Mail übermittelt werden, genügt es unter Umständen, die Datei selbst zu verschlüsseln und an eine ansonsten unverschlüsselte E-Mail anzuhängen. Hierfür kann auf die in Abschnitt 4.1.2 behandelten Verschlüsselungsfunktionen von Anwendungsprogrammen (z. B. Adobe PDF, MS Office, WinZip) zurückgegriffen werden. In diesem Fall sollte der Schlüssel (bzw. das Kennwort) zum Dechiffrieren der Datei separat an den Empfänger übergeben werden, am besten über ein anderes Medium (beispielsweise telefonisch). Keinesfalls sollte der Schlüssel im Klartext in derselben E-Mail enthalten sein, an die die verschlüsselte Datei angehängt ist.

Alternativ zum Versand per E-Mail können zum Austauschen von Dateien zwischen mehreren Partnern auch Cloud-Dienste verwendet werden, z. B. wenn diese die gemeinsame Nutzung von Dateien zulassen (Sharing-Funktion). Je nach Anbieter besteht auch hier die Option der Verschlüsselung (siehe Abschnitt 4.1.3).

Die wesentlichen für die E-Mail-Kommunikation verfügbaren Verschlüsselungsmechanismen werden in Abb. 09 gegenübergestellt.

Abb. 09 Mechanismen zur Verschlüsselung von E-Mails

	S/MIME	**PGP, GPG**	**E-Mail-Gateway**	**Verschlüsselte Dateianhänge**
Ende-zu-Ende-Verschlüsselung	✓	✓	(eingeschränkt)	✓
Bedienungsaufwand für Endnutzer	Mittel	Eher hoch	Gering	Mittel
Benutzerfreundliches Schlüsselmanagement	✓	×	✓	×
Finanzieller Aufwand bei Einführung	Eher hoch	Gering	Eher hoch	Gering

Darauf ist zu achten:

- Das Abrufen und das Versenden von E-Mails sollten immer über ein verschlüsseltes Transportprotokoll (SSL/TLS) erfolgen.
- Die am weitesten verbreiteten Verfahren für die Ende-zu-Ende-Verschlüsselung von E-Mails sind die Verfahren S/MIME und PGP. Welches Verfahren gewählt wird, ist von Faktoren wie der Unternehmensgröße, den Anforderungen an den Bedienungskomfort, der technischen Interoperabilität oder dem Schulungsaufwand für die Endbenutzer abhängig.
- Der Einsatz eines E-Mail-Gateways bietet einen hohen Vertraulichkeitsschutz, vermeidet dabei aber einige der Probleme, die sich bei einer echten Ende-zu-Ende-Verschlüsselung ergeben können.

4.2.2 Instant Messaging

Instant Messaging-Dienste sind heute als Medium für die schnelle und unkomplizierte Textkommunikation weit verbreitet. Entsprechende Clients für die unterschiedlichen Dienste (z. B. WhatsApp oder Threema) gibt es als App für Mobiltelefone und Tablets oder in Form von Programmen für klassische Computer. Einige Anbieter teilen sich den Markt, die Dienste und Clients der verschiedenen Provider sind meist proprietär gestaltet und untereinander nicht kompatibel. Einige Dienste bieten neben dem Versand von Kurzmitteilungen auch die Möglichkeit von Gruppenchats sowie die Übertragung von Bild-, Ton- und Videomitteilungen über die jeweilige Messenger-Software bis hin zur Internet-Telefonie und -Videokonferenz.

Die leichte Bedienung sowie die meist vorhandenen guten Importmöglichkeiten bestehender Kontaktdaten beispielsweise aus Adressbüchern machen Instant Messaging zu einer auch in der Geschäftswelt zunehmend beliebten Kommunikationsform. Die Frage nach der Wahrung der Vertraulichkeit ausgetauschter Informationen gerät hierbei leicht in Vergessenheit. Ähnlich wie bei der E-Mail-Kommunikation muss auch bei Instant Messaging neben dem Schutz der Informationen gegen unerlaubtes Mitlesen während der Übertragung das Vertrauen in den Dienstanbieter hinterfragt werden. Hinsichtlich des Schutzes der Kommunikation gegen unbefugtes Mitlesen ist der Nutzer meist auf die Maßnahmen angewiesen, die der jeweilige Dienstanbieter selbst zur Verfügung stellt. Hier gibt es große Unterschiede zwischen den einzelnen Anbietern: Während manche Anbieter keine als zuverlässig anerkannte Transportverschlüsselung einsetzen und teilweise auf eine Ende-zu-Ende-Verschlüsselung verzichten (z. B. WhatsApp), setzen andere (z. B. myEnigma) auf selbstentwickelte Verschlüsselungsmechanismen, die nicht hinreichend analysiert und entsprechend auch nicht hinsichtlich ihrer Sicherheit beurteilt werden können. Manche Clients (z. B. Xabber) verfügen über eine optional nutzbare Schnittstelle zur Einbindung von OTR[1] Messaging, einer frei verfügbaren Plug-In-Software, die u. a. die Ende-zu-Ende-Verschlüsselung von Instant Messaging ermöglicht. Hierzu werden eingegebene Kurzmitteilungen in einem Zwischenschritt mit dem Schlüssel des jeweiligen Kommunikationspartners verschlüsselt und erst danach durch den Instant Messaging-Client übermittelt. Auch einige sogenannte Multi-Protokoll-Messenger-Clients (z. B. die Clients Adium und Pidgin) unterstützen OTR. Hierbei handelt es sich um Instant Messaging-Programme, die Schnittstellen zu verschiedenen, untereinander ansonsten nicht kompatiblen Instant Messaging-Diensten in einer Client-Software vereinen.

OTR (= Off the Record) ist ein Protokoll zur Verschlüsselung von Instant Messaging-Nachrichten, das als Plugin (Erweiterung) für verschiedene Instant Messaging-Programme erhältlich ist.

Einige Messenger-Clients nutzen das bei korrekter Implementierung als sicher geltende SSL/TLS für die Verschlüsselung des Datenverkehrs zwischen der Client-Software des Anwenders und dem zentralen Server des entsprechenden Messaging-Dienstes. Hierdurch sind die Daten gegen unbefugtes Mitlesen während des Transports geschützt, und zwar sowohl auf dem Weg vom Absender der Nachricht zum Dienste-Server als auch auf dem Weg vom Server zum Nachrichtenempfänger. Diese Methode wird u. a. vom Threema-Client unterstützt, der zusätzlich ein hinreichend untersuchtes Verfahren für die Ende-zu-Ende-Verschlüsselung einsetzt. Hierzu gibt der Anbieter auf seiner Web-Seite detailliert Auskunft.[2]

[1] Off The Record

[2] Siehe www.threema.ch/de/faq/why_secure.

Als Sicherheitsstrategie für Unternehmen, die auf die Kommunikation mit Messenger-Diensten angewiesen sind, kann es sich empfehlen, die benötigten Dienste selbst zu betreiben, um grundlegend zu verhindern, dass sensible Daten das Unternehmen verlassen können. Neben kommerziellen Lösungen, die sich oft in Unified-Communication-Paketen finden lassen, gibt es einige offene Protokolle (z. B. IRC[1] und XMPP[2]) und eine große Auswahl zugehöriger Clients und Server-Implementationen dazu, die sich in bestehende Sicherheitsinfrastrukturen integrieren lassen und bei Bedarf auch externen Partnern sicheren Zugang zum firmeneigenen Instant Messaging-Dienst bieten können.

Darauf ist zu achten:

- Für Instant Messaging stehen einige konkurrierende Lösungen zur Auswahl. Manche bieten lediglich proprietäre (und somit kaum überprüfbare), andere hingegen gar keine Verschlüsselungsoptionen.
- Vertrauen sollte nur den Instant-Messaging-Lösungen geschenkt werden, die überprüfbare Verfahren für Transport- und Ende-zu-Ende-Verschlüsselung einsetzen. Diese sollten sorgfältig ausgewählt werden.
- Unternehmen, die häufig auf Instant Messaging angewiesen sind, können überlegen, solche Dienste in ihrer eigenen Infrastruktur bereitzustellen. Dies setzt allerdings voraus, dass im Unternehmen hinreichendes Know-how und ausreichende Ressourcen zum Betrieb der Dienste vorhanden sind.

4.2.3 Sprachkommunikation

Telefongespräche über klassische Telefonnetze werden zunehmend durch IP-basierte Sprachkommunikation (**Voice-over-IP**; VoIP) abgelöst. Ein Angreifer, der aufgrund räumlicher oder technischer Gegebenheiten in der Lage ist, die zu einem Telefonat gehörenden IP-Pakete abzufangen oder aufzuzeichnen, wird als Man-In-The-Middle bezeichnet. Dieser kann ohne größeren Aufwand in den Besitz eines vollständigen Mitschnitts der geführten Konversation gelangen (siehe Abb. 10). Aus diesem Grund sollten Sprachnutzdaten grundsätzlich verschlüsselt werden, bevor sie über IP-Netze ausgetauscht werden. Hierfür empfiehlt sich die ausschließliche Nutzung von SRTP[3], einem verschlüsselten Protokoll für den Austausch von Echtzeitnutzdaten wie Sprach- und Videodatenströmen, das in allen professionellen VoIP-Produkten integriert ist.

Generell empfiehlt es sich, nicht nur die Sprach-, sondern auch die Signalisierungsdaten ausschließlich verschlüsselt zu übermitteln. Hierfür eignet sich am besten SSL/TLS für den verschlüsselten Transport. Diese Form der Verschlüsselung ist eine Option in den meisten VoIP-Kommunikationsprodukten und kann einfach aktiviert werden.

Für den Einsatz in kritischen Umgebungen gibt es weitere Verfahren, die eine echte »Ende-zu-Ende«-Verschlüsselung der Nutzdatenschlüssel unmittelbar zwischen den Kommunikationsstellen ermöglichen (z. B. ein standardisiertes Verfahren namens

[1] Internet Relay Chat
[2] Extensible Messaging and Presence Protocol
[3] Secure Real-time Transport Protocol

ZRTP[1]), so dass die Schlüssel selbst vor unerlaubtem Zugriff durch den Betreiber der VoIP-Vermittlungsplattform geschützt sind.

Im Falle einer IP-basierten Schnittstelle zur Anbindung an das öffentliche Telekommunikationsnetz (z. B. SIP[2] Trunk) kann durch den Einsatz von SRTP und SSL/TLS ebenfalls ein hohes Maß an Sicherheit gewährleistet werden. Bei der Wahl eines Netzbetreibers sollte auf die Unterstützung dieser Funktionen geachtet werden. Gleiches gilt auch bei der Anschaffung einer eigenen Kommunikationsanlage sowie bei der Wahl eines **externen Sprachtelefoniedienstleisters**. Letzteres bietet sich an, falls ein Unternehmen (z. B. aus Kostengründen) keine eigene Vermittlungsplattform betreiben möchte und diesen Dienst daher an einen externen Dienstleister auslagert. In diesem Fall empfiehlt sich der Einsatz eines Virtual Private Networks (VPN), also eines sicheren Datentunnels zwischen den Netzen des Dienstnutzers und des Dienstanbieters. Letzterer sollte das VPN zur Verfügung stellen. Weitere Informationen zum Thema VPN können Abschnitt 4.2.5 entnommen werden. In jedem Fall empfiehlt sich zwischen Dienstanbieter und Kunden die Aushandlung vertraglicher Vereinbarungen, die sicherstellen, dass der Dienstanbieter etwaige aus der Nutzung des Kommunikationsdienstes resultierenden Informationen nicht missbrauchen kann.

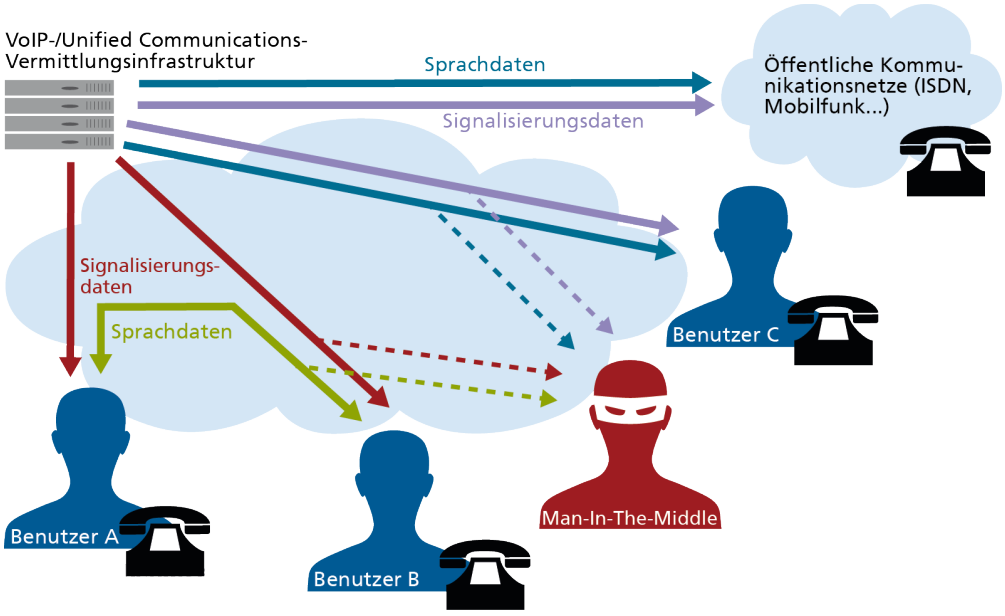


Abb. 10 Mögliche Angriffsszenarien auf die Vertraulichkeit von Voice-over-IP

In klassischen **leitungsvermittelten Kommunikationsnetzen** (beispielsweise ISDN[3]-basiert) werden üblicherweise weder Sprach- noch Signalisierungsdaten verschlüsselt. Für die Verschlüsselung von analogen und digitalen Sprach-, Daten- und Fax-Verbindungen sind jedoch Produkte in verschiedenen Größen- und Leistungsklassen auf dem Markt erhältlich. Da die entsprechenden Verschlüsselungskomponenten bei allen Gesprächsteilnehmern verfügbar sein müssen, sollten Firmen die Anschaffung eines solchen Produkts gegenüber einem neuen, moderneren IP-basierten Sprachtelefoniedienst abwägen, der meist schon die Möglichkeiten für Verschlüsselung kostenlos mitbringt (siehe oben).

[1] Z Real-time Transport Protocol
[2] Session Initiation Protocol
[3] Integrated Services Digital Network

Viele Unternehmen setzen zunehmend auch auf alternative, **internet-basierte Kommunikationsdienste**. Beispielsweise verspricht Skype, der wohl bekannteste Anbieter dieser Dienste, einen verschlüsselten Austausch sowohl der Vermittlungs- als auch der Sprach- und Videonutzdaten. Allerdings ist hier erhebliche Skepsis geboten: Zwar werden diese Daten tatsächlich verschlüsselt übermittelt, so dass sie gegen das einfache unbefugte Mithören oder Mitlesen geschützt sind. Da beispielsweise Skype jedoch grundsätzlich proprietäre Protokolle einsetzt und generell nur wenig über die Beschaffenheit der zugehörigen Dienste-Infrastruktur bekannt ist, kann nicht beurteilt werden, in welchem Maß die integrierten Sicherheitsmechanismen durch Angreifer ausgehebelt werden können. Des Weiteren wurde im Jahr 2013 bekannt, dass in die Skype-Software Schnittstellen zur Erleichterung der Kommunikationsüberwachung durch US-Behörden eingebracht wurden[1]. Aufgrund fehlender Transparenz können auch diese Schnittstellen hinsichtlich ihrer Auswirkungen auf den Schutz der Kommunikation sowie auf die Wahrung der Privatsphäre der Nutzer nicht beurteilt werden.

Herkömmliche **Mobiltelefonie** nach dem u. a. in Europa eingesetzten GSM[2]-Standard bietet von Hause aus eine im Normalfall grundsätzlich aktivierte Verschlüsselung der Nutzdaten. Auf diese Weise wird verhindert, dass die über den Mobilfunkkanal übertragenen Sprachdaten mit einfachsten Mitteln abgehört werden können. Allerdings sind die standardmäßig verwendeten Algorithmen zur Schlüsselgenerierung, die aus der Entstehungszeit der GSM-Technik stammen, als nicht mehr zeitgemäß anzusehen. Es muss heute davon ausgegangen werden, dass das Brechen der Verschlüsselung (und somit das unmittelbare Abhören) von GSM-Telefonaten mit verhältnismäßig geringem technischen Aufwand quasi in Echtzeit realisierbar ist. Der UMTS[3]-Mobilfunkstandard bietet mit einer gegenüber GSM optimierten Sicherheitsarchitektur, moderneren Verschlüsselungsalgorithmen sowie endgerät- und netzseitiger Authentifizierung und Integritätsprüfung einen grundsätzlich höheren Sicherheitsstandard als das GSM-Netz[4]. Aber auch in diesem Falle wird keine Ende-zu-Ende-Verschlüsselung zwischen den Endgeräten der Kommunikationspartner realisiert, sondern die Verschlüsselung wird im Netzwerk des Mobilfunk-Providers terminiert. Falls das Mobiltelefon im Rahmen der Sprachkommunikation häufig für den Austausch sensibler Informationen zwischen denselben Kommunikationspartnern genutzt wird, empfiehlt sich der Einsatz zusätzlicher, speziell für Mobiltelefone entwickelter Ende-zu-Ende-Verschlüsselungssysteme. Diese werden von verschiedenen Herstellern sowohl auf Hardware- als auch auf Software-Basis angeboten. Eine Hardwarelösung ist z. B TopSec Mobile von Rhode & Schwarz, eine verbreitete Softwarelösung ist PhoneCrypt von SecuStar.

Eine vergleichsweise günstige Möglichkeit für verschlüsselte Sprachkommunikation zwischen Mobiltelefonen bietet der Einsatz spezieller Sprachverschlüsselungs-Apps beispielsweise RedPhone oder Silent Phone. Beide Apps nutzen ZRTP zur Verschlüsselung der Sprachnutzdaten. Für die Anwendung ist es erforderlich, dass die entsprechende App auf den Mobiltelefonen beider Kommunikationspartner installiert ist. Die verschlüsselten Sprachsignale werden per Voice-over-IP übermittelt, auf beiden an der Kommunikation beteiligten Mobiltelefonen muss also eine Internet-Anbindung verfügbar und aktiviert sein (z. B. per WLAN, UMTS oder LTE).

[1] Siehe www.nytimes.com/2013/06/20/technology/silicon-valley-and-spy-agency-bound-by-strengthening-web.html?_r=0.

[2] Global System for Mobile communication

[3] Universal Mobile Telecommunication System

[4] Siehe Claudia Eckert: IT-Sicherheit. 8. Auflage, Oldenbourg, 2013. ISBN: 978-3-486-72138-6.

Darauf ist zu achten:

- Aufgezeichnete VoIP-Nutzdaten ergeben einen perfekten Gesprächsmitschnitt. Deshalb sollten sie immer verschlüsselt übermittelt werden. Hierfür gibt es mit ZRTP und SRTP leistungsfähige Verfahren.

- Auch VoIP-Signalisierungsdaten enthalten potenziell sensible Informationen. Auch sie sollten immer verschlüsselt werden. Die entsprechenden Verfahren sind seit Langem standardisiert.

- Auch der Datenaustausch mit externen VoIP-Dienstleistern sollte ausschließlich verschlüsselt erfolgen. Ggf. kann hierfür ein VPN zum Einsatz kommen.

- Vor der Nutzung internet-basierter Kommunikationsdienste sollte deren Vertrauenswürdigkeit überprüft werden, auch wenn die Kommunikation verschlüsselt erfolgt.

- Eine verschlüsselte Kommunikation über leitungsvermittelte Netze (drahtgebundene wie das ISDN, sowie drahtlose wie das GSM-Netz) ist möglich, aber nur mit Aufwand realisierbar.

- Für die verschlüsselte drahtgebundene Sprachkommunikation empfiehlt sich der Umstieg auf VoIP.

- Verschlüsselte drahtlose Sprachkommunikation lässt sich am günstigsten durch den Einsatz von Apps zur Sprachverschlüsselung realisieren. In beiden Fällen gilt: Sollen die Sprachdaten Ende-zu-Ende verschlüsselt werden, müssen beide Seiten das entsprechende Verschlüsselungsverfahren unterstützen.

4.2.4 Kollaborationsanwendungen

Kollaborationsanwendungen erlauben durch netzwerkbasierten Datentransfer in Echtzeit das Betrachten und bisweilen auch Bearbeiten von Bildschirminhalten und elektronischen Arbeitsdokumenten über Raum- und Firmengrenzen hinweg. Beispielsweise können elektronische Foliensätze aus der Ferne präsentiert, Textdokumente gemeinsam gelesen und kommentiert oder auch Softwarecode gemeinsam bearbeitet werden, ohne dass sich die beteiligten Personen hierzu in einem Raum befinden müssen. Bereits seit einigen Jahren zählen Kollaborationsanwendungen wie Cisco WebEx, Citrix GoToMeeting und Adobe Connect in vielen Betrieben zu den täglich genutzten Arbeitswerkzeugen. Durch die von vielen Anwendungen zusätzlich unterstützte Möglichkeit der Sprach- und teilweise auch der Videobildübermittlung wird authentisches Präsentieren und konstruktives Arbeiten aus der Ferne möglich. So können Zeit und Reisekosten eingespart werden, weshalb sich diese Anwendungen zunehmender Beliebtheit erfreuen.

Das Angebot an Kollaborationstools ist mittlerweile recht vielfältig. Bei den meisten Lösungen müssen die Teilnehmer einer Kollaborationssitzung eine anbieterspezifische Client-Software auf ihren Computern installieren. Die Bild- und Eingabedaten werden dann über eine Vermittlungsplattform zwischen den Clients ausgetauscht. Diese Plattform wird üblicherweise vom Anbieter des jeweiligen Kollaborationswerkzeugs betrieben, die Kollaborationsdaten werden also über das Internet zwischen den Rechnern der Sitzungsteilnehmer und der Vermittlungsplattform des Anbieters ausgetauscht. Die meisten Kollaborationstools sehen grundsätzlich ein Mindestmaß an Verschlüsselung zum Schutz der Vertraulichkeit vor; allerdings gibt es auch Werkzeuge, die vollständig darauf verzichten. Beispiele für Letzteres sind Citrix Netviewer, Cisco Unified Meeting-

Place und BigBlueButton. Es lohnt sich, die Verschlüsselungsfunktionalität vor der Wahl einer bestimmten Kollaborationslösung abzuklären.

Wie schon bei der Kommunikation per E-Mail und Instant Messaging muss auch bei der Verwendung von Kollaborationstools zwischen einer reinen Transportverschlüsselung und der weitergehenden Ende-zu-Ende-Verschlüsselung unterschieden werden. Im Falle der Transportverschlüsselung sind die auszutauschenden Daten zwar vor Zugriffen während der Übermittlung über Netzwerke geschützt, liegen jedoch beim Betreiber der jeweiligen Kollaborationsplattform unverschlüsselt vor. Unterstützt das verwendete Kollaborationswerkzeug hingegen eine Ende-zu-Ende-Verschlüsselung, sind die auszutauschenden Daten in gewissem Umfang selbst vor einem potenziellen Zugriff durch den Dienstbetreiber geschützt. Zu den Kollaborationswerkzeugen, die sowohl eine Transport- als auch eine Ende-zu-Ende-Datenverschlüsselung bieten, zählen beispielsweise Cisco WebEx und Citrix GoToMeeting. Grundsätzlich kann davon ausgegangen werden, dass das Schlüsselmanagement durch die Kollaborationstools selbst bzw. durch die zentrale Plattform des Dienstanbieters erfolgt und somit für die Nutzer transparent ist.

Eine Alternative zur Nutzung eines Kollaborationstools, dessen Vermittlungsplattform im Internet von einem Dienstanbieter betrieben wird, ist der Eigenbetrieb eines entsprechenden Servers, sofern die entsprechende Kollaborationslösung dies erlaubt. Diese Option bietet beispielsweise Adobe Connect. Auch Cisco (für sein Produkt WebEx) sowie die Anbieter TrueConf und RHUB bieten Serverlösungen zum Eigenbetrieb für ihre Produkte an.

Werden hingegen keine Echtzeitkommunikationsdienste für die gemeinsame Arbeit an digitalen Dokumenten benötigt, kann anstelle einer Kollaborationslösung auch ein entsprechender Cloud-Dienst eingesetzt werden, um z. B. das Verteilen und unabhängige Nutzen von Dokumenten durch mehrere Personen zu ermöglichen, ohne dass eine gleichzeitige Abstimmung nötig ist (siehe dazu Abschnitt 4.1.3).

Darauf ist zu achten:

- Es existiert eine Vielzahl verschiedener Kollaborationstools mit unterschiedlichen Funktionen. Nicht alle bieten eine Transportverschlüsselung. Noch weniger erlauben die (noch sicherere) Ende-zu-Ende-Verschlüsselung der sensiblen Daten. Es lohnt sich also, bei der Auswahl eines Kollaborationstools genau abzuwägen.

- Den besten Schutz bietet der Betrieb einer eigenen Kollaboration-Vermittlungsplattform innerhalb der eigenen Infrastruktur. Dies setzt allerdings voraus, dass im Unternehmen die Ressourcen und das Know-how hierfür vorhanden sind.

4.2.5 Virtuelle Private Netze (VPN)

Mitarbeiter, die im Rahmen ihrer Tätigkeit häufig z. B. zu Geschäftstreffen oder Tagungen reisen müssen oder die über einen Heimarbeitsplatz verfügen, benötigen zeitweise Zugriff auf Daten bzw. Funktionen, die nur innerhalb der Netzwerkinfrastruktur ihres Unternehmens und somit nicht öffentlich verfügbar sind. Der Einsatz virtueller privater Netze (VPN) ermöglicht einen vergleichsweise sicheren Zugriff auf interne Ressourcen aus dem öffentlichen Netz. Praktisch betrachtet wird hierzu nach einer persönlichen Authentifizierung ein transportverschlüsselter Tunnel zwischen dem Rechner des von extern zugreifenden Mitarbeiters und einem sogenannten VPN-Gateway aufgebaut,

das an einem speziell gestalteten Übergang zwischen dem Unternehmensnetz und dem Internet zwischengeschaltet wird. Da die Transportverschlüsselung unmittelbar an den vertrauenswürdigen Knoten terminiert (nämlich am VPN-Gateway des eigenen Unternehmens sowie auf dem Rechner des Mitarbeiters), ist der Datenaustausch über das Internet gegen Mitlesen durch unbefugte Dritte hinreichend geschützt.

Sowohl auf dem Rechner des Mitarbeiters als auch auf dem VPN-Gateway wird hierfür spezielle Software benötigt, die von verschiedenen Herstellern angeboten wird. Im Rahmen des Verbindungsaufbaus erfolgt eine Authentifizierung, bei der ein Nutzer meist seine individuelle Nutzerkennung und das zugehörige Passwort eingeben muss. Wurde der Mitarbeiter erfolgreich am VPN-Gateway authentifiziert, wird sein Rechner virtuell in das interne Unternehmensnetzwerk eingebunden. Beispielsweise wird dem Rechner eine IP-Adresse aus dem Adresspool des Unternehmensnetzwerks zugewiesen, so dass aus Netzwerksicht praktisch kein Unterschied zwischen dem per VPN eingebundenen und einem direkt an das interne Netzwerk angeschlossenen Rechner besteht. Die am häufigsten eingesetzten VPN-Verfahren (IPsec[1]) verfügen über integrierte Protokolle für das Schlüsselmanagement, das somit aus Anwendersicht transparent abläuft.

Da der Hauptnutzen dieser Systeme ist, die Verbindungen abzusichern, ist der verschlüsselte Datenaustausch eines ihrer Hauptmerkmale. Daher ist bei aktuellen VPN-Produkten meist ein ausreichendes Sicherheitsniveau gegeben und gängige Kryptographieverfahren werden korrekt angewandt. Einen zusätzlichen Schutz, beispielsweise gegen das Auslesen von VPN-Zugangspasswörtern durch Spähsoftware auf dem betreffenden Computer, bieten Systeme wie die NCP GovNet Box an. Hier wird die Verbindung in einer gesondert gesicherten USB-Box terminiert, die Manipulationen ihrer eigenen Hard- und Software erkennen kann. Die Zugangsdaten selbst sind auf Smartcards gespeichert, die PIN wird auf der Box selbst eingegeben statt auf dem möglicherweise kompromittierten Rechner des Benutzers. Durch diese Trennung des VPN-Betriebs vom Zielsystem erreicht NCP die Zulassung nach VS-NfD (Verschlusssache – Nur für Dienstgebrauch; eine definierte Geheimhaltungsstufe bundesdeutscher Behörden).

Neben der Anbindung einzelner Mitarbeiter an ein Firmennetzwerk werden VPNs auch dazu genutzt, ganze Unternehmensstandorte untereinander zu vernetzen oder an das Datennetzwerkes des Hauptfirmensitzes anzubinden. Hier liegt der Vorteil insbesondere in der kostengünstigeren geschützten Anbindung per VPN über das öffentliche Netz im Vergleich zur ansonsten benötigten, deutlich teureren Direktanbindung.

Darauf ist zu achten:

- VPNs ermöglichen eine grundsätzlich verschlüsselte Kommunikation sowohl zwischen einem Client-Rechner und einem VPN-Gateway in einem Firmennetzwerk als auch zwischen ganzen Netzwerken an verschiedenen Standorten.

- Für eine einfache VPN-Verbindung zwischen einem Client-PC und einem VPN-Gateway wird entsprechende Software auf beiden IT-Systemen benötigt.

- Im Falle erhöhten Schutzbedarfs sollten Hardwarelösungen zur Etablierung eines softwareunabhängigen VPNs eingesetzt werden, beispielsweise die NCP GovNet Box oder vergleichbare Produkte der Firma genua.

[1] Internet Protocol Security

4.2.6 Externe Zugriffe auf Unternehmensressourcen

Neben der Nutzung eines VPN gibt es zahlreiche weitere Möglichkeiten, um aus dem Internet auf Daten und Dienste innerhalb der Unternehmensinfrastruktur zuzugreifen. Diese dienen unterschiedlichen Anwendungszwecken:

- **Übertragung von Dateien**
  Zur einfachen Dateiübertragung zwischen einem zentralen Server und Clients an beliebigen Orten wird häufig FTP[1] eingesetzt, ein prinzipiell bewährtes Protokoll, das allerdings keine Verschlüsselungsfunktion bietet. Gleiches gilt auch für CIFS[2], eine Erweiterung des hauptsächlich in Windows-Netzen angewendeten SMB-Protokolls[3] zur Steuerung von Datei- oder Druckerfreigaben und anderen Domänendiensten. Obwohl das »I« in CIFS für »Internet« steht, sollte es mangels hinreichender Verschlüsselung nicht für den Informationsaustausch über das Internet genutzt werden. Alternativen, bei denen dieser Schutz enthalten ist, sind die FTP-Erweiterung FTPS, bei der der Transport von FTP-Paketen über SSL/TLS abgesichert ist, sowie SFTP[4], das technisch auf dem nachfolgend beschriebenen Protokoll SSH[5] beruht.

- **Kommandozeilenorientierte Steuerung von Betriebssystemen und Anwendungen**
  Das verschlüsselnde Protokoll SSH bietet eine sichere Möglichkeit, um Computer und andere Hardware sowie darauf befindliche Programme mittels Betriebssystemkommandos aus der Ferne zu konfigurieren, zu starten oder zu beenden. Das funktional ähnliche Protokoll Telnet sollte hingegen aufgrund fehlender Verschlüsselungsmöglichkeiten nicht über öffentliche Netze angewendet werden.

- **Fernwartung über die grafische Benutzungsoberfläche**
  In einigen Unternehmen werden für Wartungs- und Konfigurationszwecke Anwendungen eingesetzt, die es ermöglichen, die grafische Oberfläche eines Computers aus der Ferne zu benutzen. Hierfür werden Bildschirminhalte des entfernten Computers an einen steuernden lokalen Computer übertragen, der wiederum seine Mausbewegungen und Tastatureingaben an den entfernten Computer zurückliefert. Die zugrunde liegenden Protokolle sind entweder RDP[6] oder aber VNC[7]. In beiden Fällen enthalten die meisten Anwendungen nur unzureichende Verschlüsselungsmöglichkeiten. Einige auf RDP basierende Anwendungen (z. B. Windows Remotedesktop und iFreeRDP) unterstützen zwar SSL/TLS als Transportverschlüsselung; allerdings entspricht dies nicht generell der Voreinstellung, erfordert folglich eine explizite Konfiguration.

- **Netzwerküberwachung**
  Gerade in Netzwerkumgebungen, in denen zentrale Dienste auf mehreren Servern angeboten werden, werden häufig Monitoring-Anwendungen eingesetzt, um das einwandfreie Funktionieren der Komponenten und Dienst-Software zu überwachen (z. B. Nagios). Des Weiteren existieren Lösungen für die Erkennung und Verhinderung unberechtigten Eindringens in private Netzwerke (sogenannte IDS[8] bzw. IPS[9],

[1] File Transfer Protocol
[2] Common Internet File System
[3] Server Message Block
[4] SSH File Transfer Protocol
[5] Secure SHell
[6] Remote Desktop Protocol
[7] Virtual Network Computing
[8] Intrusion Detection System
[9] Intrusion Prevention System

z. B. Snort). Sollen derartige Anwendungen über das Internet steuerbar sein, ist dringend auf eine geeignete Transportverschlüsselung zu achten. Zugriffe mittels Browser auf die Webschnittstelle der Überwachungssoftware sollten beispielsweise immer über SSL/TLS abgesichert sein.

Darauf ist zu achten:

- Unterschiedliche Anwendungen (z. B. Dateiübermittlung oder Fernwartung) bedingen den Einsatz unterschiedlichster Verfahren und Protokolle für den externen Zugriff auf Unternehmensressourcen. Es sollten stets Verfahren bzw. Varianten gewählt werden, die eine verschlüsselte Kommunikation ermöglichen.

4.2.7 Interne Netzwerkkommunikation

Mitarbeiter des eigenen Betriebs, aber auch Besucher und externe Dienstleister (z. B. Wartungstechniker) haben meist uneingeschränkten Zugriff auf einen oder mehrere Netzwerkanschlüsse eines Unternehmens und somit unmittelbar auf das Netz selbst. Dies birgt potenzielle Gefahren, wie beispielsweise das gewollte oder ungewollte Einschleusen von Schadsoftware in das interne Netz. Auch lassen sich bestimmte Anschlüsse, etwa solche von Netzwerkdruckern, zum Abfangen sensibler Daten nutzen.

Sogenannte MAC[1]-Filter, die heute insbesondere in kleineren Netzwerken eingesetzt werden, bieten lediglich einen vergleichsweise beschränkten Schutz gegen den unbefugten Zugriff auf interne Netzwerkinfrastrukturen. Sie realisieren eine Netzwerkzugriffsauthentifizierung, die auf der jeweils geräteindividuellen MAC-Adresse (physische Netzwerkadresse einer Netzkomponente) basiert und so theoretisch nur zuvor registrierten Komponenten Zugriff auf das jeweilige Netzwerk gewährt. Jedoch ist es für IT-Kriminelle vergleichsweise leicht, die MAC-Adresse eines einzubringenden Gerätes zuvor anzupassen und so die Identität einer autorisierten Netzwerkkomponente vorzutäuschen. Aus dem gleichen Grund bieten auch sogenannte VLANs[2] (also die virtuelle Aufteilung physischer Netze in logische Segmente) nur eingeschränkten Schutz gegen unberechtigten Zugriff in internen Netzwerken.

Einen zuverlässigen Schutz gegen den Missbrauch einer internen Netzwerkinfrastruktur bietet eine aktuellen Ansprüchen genügende Verschlüsselung bereits auf der Netzwerkzugriffsebene (sogenannte MAC-Schicht). Hierzu hat sich ein Verfahren nach dem Standard IEEE 802.1AE bewährt, das unter der Bezeichnung MACsec bekannt ist. Durch den konsequenten Einsatz von MACsec innerhalb eines Unternehmensnetzes ist es möglich, unautorisiert angeschlossene Komponenten vollständig vom Netzwerkverkehr auszuschließen, da sie nicht in der Lage sind, Daten mit dem jeweils korrekten Schlüssel zu verschlüsseln bzw. empfangene verschlüsselte Daten zu dekodieren. Somit wird ein wirksamer Schutz gegen unbefugten Zugriff auf das Unternehmensnetzwerk geboten, also ein sich selbst verschlüsselndes LAN geschaffen. Hierzu muss jedoch die Netzwerkinfrastruktur vollständig auf den Einsatz von MACsec vorbereitet sein, was insbesondere auch für die internen Vermittlungsknoten (sogenannte Switches) gilt. Je nach individuellen Gegebenheiten und Schutzbedürfnis genügt es auch, lediglich diejenigen Segmente eines Netzes mittels MACsec abzusichern, in denen sensible Daten gelagert oder transportiert werden, in denen also eine höhere Kritikalität besteht.

[1] Media Access Control
[2] Virtual Local Area Network

Da die Verbreitung MACsec-unterstützender Komponenten zwar zunimmt, jedoch insbesondere ältere Switches meist noch nicht darauf ausgelegt sind, kann es notwendig sein, einzelne oder unter Umständen auch alle Switches innerhalb des Netzwerks zu ersetzen, was mit teilweise nicht unerheblichen Investitionen in die neue Infrastruktur verbunden sein kann. Der Einsatz von MACsec bietet sich u. a. deshalb hauptsächlich für größere Unternehmen an.

Ist das Unternehmensnetzwerk mit WLAN-Zugängen ausgestattet, sollten diese ausschließlich einen verschlüsselten Funkzugriff auf das Netzwerk ermöglichen. Hierbei sollte von einer Verschlüsselung nach dem WEP[1]-Standard abgesehen werden, da diese bereits seit einigen Jahren als unsicher anzusehen ist. Stattdessen sollte mindestens das Verfahren WPA[2], besser noch das neuere und sicherere WPA2 verwendet werden. In kleinen Firmennetzwerken, die nur über wenige WLAN-Zugangspunkte verfügen, lassen sich die Zugangsberechtigungen einschließlich der Schlüssel unmittelbar auf den Access Points konfigurieren (PSK[3]-Verfahren). In größeren Netzen mit mehreren WLAN-Zugangspunkten empfiehlt sich hingegen der Einbezug eines auf einem zentralen Server betriebenen Authentifizierungsdienstes auf Basis des Standards IEEE 802.1X/EAP[4] (Infrastrukturmodus).

Darauf ist zu achten:

- Auch interne Netzwerkschnittstellen sollten vor unbefugtem Zugriff und Missbrauch geschützt werden. Dies gilt insbesondere für Netzwerkabschnitte, die aufgrund der Kritikalität der darüber transportierten und zugreifbaren Daten sowie ihrer Exposition gegenüber potentiellen Angreifern besonders gefährdet erscheinen.

- MAC-Filter, VLAN und ähnliche Technologien bieten hier nur eingeschränkten Schutz. Zuverlässiger ist die konsequente Verschlüsselung bereits auf der Zugriffsebene (MACsec).

- Bei Funkschnittstellen (WLAN) auf die Anwendung moderner Verschlüsselungsverfahren (am besten WPA2) achten.

- Bei der Auswahl von Hard- und Softwarekomponenten, mit denen ein Netz aufgebaut wird (Router, Switche etc.), ist auch auf deren Herkunft zu achten. Hardware aus Ländern, in denen das Risiko geringer ist, dass Verschlüsselungsfunktionen eingebaute Hintertüren für Geheimdienste aufweisen, kann als vertrauenswürdiger angesehen werden.

4.3 Schlüsselmanagement

Alle zuvor genannten Verschlüsselungsanwendungen verwenden kryptographische Schlüssel. Teilweise geschieht dies transparent, also ohne dass die anwendenden Unternehmen und die Benutzer hierfür etwas tun müssen. Dies gilt etwa für die Trans-

[1] Wired Equivalent Privacy
[2] Wi-Fi Protected Access
[3] Pre-Shared Key
[4] Extensible Authentication Protocol

portverschlüsselung mittels SSL/TLS oder verschlüsselnde Dienste wie SSH. In vielen Fällen muss ein Anwender jedoch ausdrücklich dafür Sorge tragen, dass die kryptographischen Schlüssel sicher erzeugt, aufbewahrt, verwendet und – wenn sie nicht mehr benötigt werden – zurückgezogen oder deaktiviert werden. Diese Aufgabe verlangt eine besondere Sorgfalt, damit Schlüssel einerseits im Bedarfsfall für berechtigte Zugriffe rasch verfügbar, andererseits gegen unberechtigte Zugriffe hinreichend gut geschützt sind. Eine besondere Herausforderung entsteht insbesondere dann, wenn eine Institution vielfältige Verschlüsselungsverfahren einsetzt und dementsprechend viele Schlüssel verwalten muss.

Ansatzweise vergleichbar ist diese Herausforderung mit der Schlüsselverwaltung beim Gebäudemanagement. Ist die Schlüsselverwaltung für einen einzigen Nutzer einer Wohnung noch trivial (»Nutzer verschlüsselt Datei«), so wächst die Komplexität schon mit einer Vergrößerung der Anzahl der Bewohner der Wohnung (»mehrere Nutzer haben Zugriff auf eine verschlüsselte Datei«). Weitaus komplexer wird die Schlüsselverwaltung für die Schließanlage eines ganzen Bürogebäudes mit unterschiedlichen Schlüsseln für verschiedene Funktionsträger und unterschiedlichen Zugangsbereichen. Vor allem in Umgebungen, in denen verschiedenartige Verschlüsselungslösungen, z. B. eine PKI für den sicheren Mailverkehr, Dateiverschlüsselung für Dokumente, Festplattenverschlüsselung für Notebooks zum Einsatz kommen, kann die Verwaltung der Schlüssel sehr aufwendig und fehleranfällig sein.

Eine umfassende Darstellung des Schlüsselmanagements überschreitet den Rahmen dieses Leitfadens. Daher werden nachfolgend nur einige der grundlegenden Fragestellungen genannt, die in diesem Kontext zu klären sind:

- Wo werden die Schlüssel sicher abgelegt? Gibt es für die Schlüsselablage einen zentralen besonders geschützten Server oder wird der Schlüssel lokal auf dem persönlichen Rechner gespeichert? Wie ist der Schlüssel auf dem persönlichen Rechner geschützt vor Diebstahl oder Verlust z. B. bei einem Festplattenfehler?

- Wie werden die Schlüssel sicher verteilt? Wie werden Personen korrekt identifiziert, die einen Schlüssel erhalten sollen?

- Wozu sollen Schlüssel verwendet werden (Personenauthentifizierung, Verschlüsselung von Datenträger etc.)?

- Wie erfolgt der Wechsel von Schlüsseln (z. B. bei Ablauf ihrer Gültigkeitsdauer)?

- Gibt es eine organisierte Datensicherung der Schlüssel? Wo werden Sicherungskopien der Schlüssel gehalten?

- Mit welchen Verfahren können verschlüsselte Informationen im Bedarfsfall wieder entschlüsselt werden, wenn die für die Entschlüsselung eigentlich vorgesehenen Schlüssel verloren gehen oder beschädigt werden?

- Wie sind Schlüssel zu deaktivieren, deren weitere Verwendung nicht mehr gewünscht wird, z. B. weil ihr Gültigkeitsdatum abgelaufen ist oder sie aufgrund eines Sicherheitsvorfalls als nicht mehr sicher gelten?

- In welcher Weise werden die Sicherheitsrichtlinien des Unternehmens (z. B. bezüglich der Schlüssellängen) unterstützt und eingehalten?

- Wie werden Sicherheitsvorfälle behandelt und dokumentiert?

Wird in einem Unternehmen nur sporadisch in Einzelfällen Verschlüsselung eingesetzt, kann es reichen, durch einzelne organisatorische und technische Maßnahmen festzulegen, wie verschlüsselte Dokumente und deren Schlüssel zu behandeln sind. Bei einem stärkeren Gebrauch von Verschlüsselungsverfahren sollte über eine professionelle und softwaregestützte Schlüsselverwaltung sichergestellt werden, dass die Vertraulichkeit und Verfügbarkeit der verschlüsselten Daten und deren Schlüssel gewahrt bleiben.

Werden für die Verschlüsselung kommerzielle Produkte eingesetzt, ist eine derartige Schlüsselverwaltung oft schon Bestandteil der Software. Die Funktionen sind dabei auf das jeweilige Produkt und auf den jeweiligen Anbieter abgestimmt. In den meisten Fällen werden diese Lösungen lokal auf dem Client ohne zentrales Management betrieben.

Im Gegensatz zu diesen dezentral gesteuerten Lösungen können zentrale Lösungen alle Schlüssel über einen Server zusammen mit anderen Anwendungen im Unternehmen verwalten. Häufig bieten die Hersteller für ihre Verschlüsselungslösungen z. B. für Mail und Dokumente auch ein einheitliches Verwaltungstool an. Ein besonderes Merkmal dieser Lösungen kann sein, dass sie auch die Umsetzung unternehmensweiter Sicherheitsrichtlinien zum Gebrauch der kryptographischen Schlüssel unterstützen.

Darüber hinaus bietet der Markt besonders sichere Lösungen an, bei denen die Schlüsselverwaltung getrennt von allen anderen Anwendungen auf speziellen Servern installiert und betrieben werden. Eine besonders hohe Sicherheit bieten speziell Hardware-Sicherheitsmodule für die Erzeugung und Verwaltung kryptographischer Schlüssel.

Werden in einem Unternehmen mehrere Verschlüsselungslösungen möglicherweise unterschiedlicher Hersteller eingesetzt, kann die Schlüsselverwaltung noch aufwendiger und fehleranfälliger sein. Abhilfe können zentrale Verwaltungstools bieten, bei denen die unterschiedlichen Einzellösungen zur Schlüsselverwaltung an einem einzigen Punkt konzentriert sind. Damit der gemeinsame Einsatz von Produkten unterschiedlicher Hersteller möglich ist, sollten die zentrale Komponente wie auch alle einzubindenden Schlüsselverwaltungsprogramme ihre Informationen austauschen können. Hierfür wurde von mit dem »Key Management Interoperability Protocol« (KMIP) ein eigener Kommunikationsstandard entworfen, der seit seiner Erstveröffentlichung im Jahr 2010 von immer mehr Anbietern kryptographischer Lösungen unterstützt wird.

Darauf ist zu achten:

- Um das Management von Schlüsseln zu vereinfachen, sind unternehmensweite Vorgaben für die Nutzung von Verschlüsselung zu entwickeln. Für die Handhabung der Schlüssel sind sowohl organisatorische Regelungen (etwa Zugriff auf hinterlegte Schlüssel für Vertretungsfälle) als auch technische Maßnahmen (etwa die Nutzung von Verwaltungssoftware für dezentral abgelegte Schlüssel) zu ergreifen.

- Immer dann, wenn Benutzer für die sichere Handhabung von kryptographischen Schlüsseln verantwortlich sind, müssen sie durch eine Sensibilisierung für die möglichen Folgen eines fahrlässigen Umgangs mit diesen Instrumenten, eindeutigen Regelungen und bei Bedarf auch Schulungen in der sachgerechten Verwendung der Schlüssel unterstützt werden.

5 Anwendungsszenarien für Verschlüsselung

Die Verschlüsselungslösungen und -produkte, die in Kapitel 4 beschrieben wurden, lassen sich entsprechend der betrieblichen Anforderungen an die Vertraulichkeit der übertragenen und gespeicherten Daten sowie der eingesetzten IT-Lösungen kombinieren. Bei einer solchen Kombinationen von Verschlüsselungslösungen

- ist zum einen der Vertraulichkeitsbedarf der Informationen zu bewerten,
- sind zum anderen sind die Gefährdungen, denen die IT-Komponenten und Kommunikationsverbindungen, auf denen diese Informationen gespeichert und übertragen werden, zu identifizieren.

Ein besonderes Augenmerk sollte insbesondere auf den Schutz solcher Informationen gelegt werden, bei denen Vertraulichkeitsverluste einen hohen Schaden bewirken könnten, seien es finanzielle Verluste oder juristische Sanktionen, Imageschäden oder auch mögliche Folgeschäden bei Dritten. Dort wo personenbezogene Informationen verarbeitet werden oder sehr sensibles Know-how die Basis des Unternehmenserfolgs ist, ist der Schutzbedarf in der Regel sehr hoch. Derart kritische Daten können beispielsweise Kundendaten, Personaldaten, Planungen zu neuen Produkten und Angeboten, strategische Dokumente zur Unternehmensentwicklung oder die Kommunikation mit und Informationen von Geschäftspartnern sein. Auf jeden Fall kritisch sind Zugangsinformationen in das Unternehmensnetz (Informationen zu Benutzern, Konfigurationsdateien, Systemprotokolle etc.) und alle Daten, zu deren vertraulicher Behandlung ein Unternehmen gesetzlich verpflichtet ist. Je vertraulicher die Informationen sind, desto mehr empfiehlt sich, diese zu verschlüsseln.

Um das Risiko von Vertraulichkeitsverlusten gezielt zu verringern, ist es erforderlich, alle Speicherorte und Übertragungswege zu kennen und geeignet abzusichern, die einen Missbrauch vertraulicher Informationen zur Folge haben können. Je vertraulicher die Informationen und je unsicherer ein Übertragungsweg ist, desto dringlicher wird die Verschlüsselung der übertragenen und gespeicherten Daten. Ein besonderer Fokus liegt dabei auf

- Segmenten innerhalb des internen Netzes, in denen besonders vertrauliche Daten übertragen, gespeichert oder bearbeitet werden, beispielsweise Personaldaten, sensible Entwicklungsdaten oder Kundendaten,
- Kommunikationsanwendungen und -verbindungen, die über öffentliche Netze wie das Internet verlaufen, da die übertragenen Daten ohne den Einsatz von Verschlüsselung ansonsten ungeschützt sind,
- mobilen Geräten und Datenträgern, da diese physisch nur sehr schwer umfassend zu schützen sind.

Unternehmen, die in ihrer Leistungserbringung sehr stark exponiert sind, also viele Angriffspunkte bieten, sind folglich gefährdeter als Unternehmen, die ihre Informationstechnik kaum nach außen öffnen. So ist ein Online-Shop etwa leichter anzugreifen als ein Unternehmen, das außer einer Website mit Informationen über das Unternehmen keine internetbasierte Kommunikation mit Kunden oder Lieferanten hat. Auch die Attraktivität eines Unternehmens spielt hinsichtlich der Gefährdung eine Rolle. Dort wo ein Angriff finanziell sehr ertragreich sein kann, wird es eher Angriffe geben, als bei Unternehmen, bei denen der Diebstahl vertraulicher Informationen weniger lukrativ ist.

Basierend auf den Bewertungen des Schutzbedarfs, der Gefährdungslage und der Kritikalität der Speicherorte und Übertragungswege sind unter Berücksichtigung zusätzlicher Aspekte, insbesondere der wirtschaftlichen Angemessenheit, der Benutzerfreundlichkeit, der Kompatibilität mit der vorhandenen IT-Infrastruktur eines Unternehmens, hinreichend wirksame Verschlüsselungslösungen auszuwählen. Auch das IT-Know-how eines Unternehmens spielt bei der Wahl einer Lösung eine Rolle. Dort wo nur geringe Kenntnisse vorhanden sind, muss eine einfach zu handhabende Lösung gewählt werden. Insbesondere bei kleineren Unternehmen können IT-Dienstleister bei der Auswahl und Einführung der Verschlüsselungslösungen Unterstützung bieten.

Dieses Kapitel veranschaulicht diese Vorgehensweise und stellt exemplarische Verschlüsselungsarchitekturen für verschiedene Einsatzszenarien anhand fiktiver, bewusst auf einige wenige typische Grundelemente reduzierter Beispielunternehmen vor. Die Lösungen können naturgemäß nicht den Gesamtumfang der Anwendungsfälle und der benutzten Software sowie der branchenspezifischen Anforderungen abdecken.

Diese Szenarien sollen es erleichtern, eine geeignete Verschlüsselungsarchitektur für ein konkretes Unternehmen zu entwickeln. Sie dienen somit als Referenz. In einem realen Einsatzumfeld können, je nach individuellen Gegebenheiten, Abweichungen von diesen oder Kombinationen aus diesen Musterlösungen sinnvoll sein. Damit die Beschreibungen kompakt bleiben, konzentrieren sich die Szenarien darüber hinaus auf die technischen Lösungen und wird auf eine Beschreibung der zugehörigen organisatorischen Maßnahmen weitgehend verzichtet.

5.1 Lösungsbeispiel für ein Kleinunternehmen

A) Kennzeichen des Anwendungsfalls

Bei diesem Referenzunternehmen handelt es sich um ein kleines Unternehmen (beispielsweise einen Handels- oder Handwerksbetrieb), das inhabergeführt ist und rund zehn Mitarbeiter hat. Es gibt externe Kommunikationsbeziehungen über E-Mail etwa zu Lieferanten und Kunden. Hierzu werden Datenbestände wie Adress-, Angebots- und Umsatzdaten verwaltet. Die Kunden des Unternehmens sind in der Regel Privatkunden oder aber andere kleine Unternehmen mit einfacher IT-Infrastruktur und entsprechend geringer IT-Kompetenz.

Die Finanzbuchhaltung wird intern erledigt, der Jahresabschluss erfolgt durch einen Steuerberater, der auch die Lohn- und Gehaltsbuchhaltung übernimmt.

Die IT-Infrastruktur ist nicht komplex. Es gibt drei PCs, einen davon mit Serverfunktion zur Ablage der Dateien und für die zentrale Datensicherung. Um bei Kundenbesuchen Informationen zu liefern und Angebote zu kalkulieren, gibt es einen Laptop, der aus der Ferne auch mit dem Firmennetz verbunden werden kann.

Das Unternehmen nutzt eine auf die Geschäftsanforderungen zugeschnittene Anwendungslösung und ein Finanzbuchhaltungsprogramm, für individuelle Korrespondenz und für Kalkulationen gängige Office-Pakete.

Das Unternehmen wird von einem kleinen IT-Dienstleister betreut, der sowohl die Hardware als auch die Anwendungslösungen bereitstellt und konfiguriert. Kleine Anpassungen macht der Inhaber des Handwerksbetriebs selber, im Unternehmen sind

jedoch keine explizite IT-Expertise und nur ein geringes Know-how zur IT-Sicherheit vorhanden.

B) Schutzbedarf der Informationen

Informationsbestände	Bewertung
Personaldaten mit Gehaltsinformationen, Fehlzeiten etc.	Dies sind sehr sensible Informationen mit sehr hohen Vertraulichkeitsanforderungen.
Kundendaten (Adressdaten, Angebote, erbrachte Leistungen und Umsätze)	Dies sind sensible Informationen mit hohen Vertraulichkeitsanforderungen.
Leistungsverzeichnisse, Lagerinformationen	Diese Informationen haben geringe Vertraulichkeitsanforderungen, da sie z. T. öffentlich verfügbar sind. Dort, wo sie unternehmensspezifisch sind, würde bei unberechtigten Zugriffen kein Schaden entstehen.
Kalkulationen	Dies sind für das Unternehmen sensible Informationen. Die Vertraulichkeitsanforderungen sind hoch, da diese Informationen das Know-how der Firma repräsentieren und einen Konkurrenzvorteil bieten können.
Buchhalterische Daten	Dies sind sehr sensible Informationen. Die Vertraulichkeitsanforderungen sind sehr hoch.

C) Gefährdungen, Kritikalität von Speicherorten und Übertragungswegen

Ein solches Unternehmen stellt in der Regel kein spezifisch attraktives und exponiertes Angriffsziel dar. Die Gefahr, gezielt angegriffen zu werden, ist gering. Trotz allem kann das Unternehmen von breit gestreuten Attacken betroffen sein.

- Es kann zu Vertraulichkeitsverletzungen durch Zugriff auf Datenträger beim Verlust von mobilen Geräten kommen und Kundendaten und Kalkulationen könnten nicht berechtigten Personen (z. B. Konkurrenzunternehmen) zugänglich werden.

- Auf den Arbeitsplatzrechnern könnten nicht Berechtigte auf Informationen über Mitarbeiter, Kunden, Kalkulationen und Finanzen zugreifen. So könnten etwa unzufriedene Mitarbeiter Kundendaten abgreifen, um sie beim Ausscheiden mit in eine neue Firma zu nehmen.

- Der unberechtigte Zugriff auf personenbezogene Daten kann zu Datenschutzverletzungen mit strafrechtlichen Konsequenzen führen.

- Bei der Übertragung von Informationen, z. B. bei der E-Mail-Kommunikation mit Kunden über Angebote und der Bereitstellung von Informationen für den Steuerberater, kann es zu unberechtigten Zugriffen auf schutzbedürftige Daten kommen.

Obwohl die Gefahr gezielter Hackerangriffe von außen vergleichsweise gering ist, hat das Unternehmen daher Anforderungen an die Vertraulichkeit seiner Daten und damit einen Bedarf, diese zu schützen.

D) Lösung

Das Handwerksunternehmen sollte für kritische Daten Verschlüsselungslösungen wählen. Eventuell sollte das Unternehmen seinen IT-Dienstleister ansprechen und Unterstützung für die Planung und Umsetzung von Lösungen nutzen.

Gespeicherte Informationen

- Eine besonders kritische Anwendung ist die Nutzung eines Laptops für Arbeiten bei den Kunden. Um unberechtigte Zugriffe auf schutzwürdige Informationen zu erschweren, sollten die Datenbestände auf diesem Gerät grundsätzlich regelmäßig daraufhin überprüft werden, ob sie für den mobilen Einsatz benötigt werden. Es sollten nur wirklich erforderliche Firmendaten auf der Festplatte des Geräts abgelegt sein.

- Darüber hinaus sind die Informationen auf den mobilen Systemen durch eine Festplattenverschlüsselung zu schützen ebenso wie ein eventuell genutzter USB-Stick eine Hardwareverschlüsselung besitzen sollte. Die verwendeten Kennwörter und Wiederherstellungsschlüssel sind sicher zu hinterlegen, damit sie im Notfall verfügbar sind.
  ➢ Siehe hierzu Abschnitt 4.1.1.

- Auch die Informationsbestände auf den Arbeitsplatzrechnern sollten durch eine angemessene Verschlüsselung geschützt werden. Die bei dem Unternehmen genutzten Anwendungsprogramme bieten in der Regel keine Verschlüsselungsmöglichkeiten für Datenbestände. Daher ist es sinnvoll, die Anwendungen und die von ihnen genutzten Dateien in verschlüsselten Containern auf der Festplatte des Arbeitsplatzrechners abzulegen. Dies gilt insbesondere für sensible personenbezogene Daten, die dadurch dem Zugriff Unberechtigter entzogen sind.
  ➢ Siehe hierzu Abschnitt 4.1.2.

Übertragung von Informationen

- Werden personenbezogene oder buchhalterische Daten per E-Mail übertragen, sind diese zu verschlüsseln. Sind die Anhänge mit einem Office-Programm verschlüsselt, muss der Kommunikationspartner den Schlüssel kennen. Er könnte etwa in einem Telefonat mitgeteilt werden. Die E-Mail selber ist dann jedoch noch nicht verschlüsselt. Sie könnte mit PGP verschlüsselt werden oder aber der Text der Nachricht wird als Datei verschlüsselt angehängt. Welche Lösung hier sinnvoll umgesetzt wird, sollte etwa mit dem Steuerberater gemeinsam entschieden werden.
  ➢ Siehe hierzu Abschnitt 4.2.1.

- Ein verschlüsselter Datenaustausch mit Kunden ist in der Regel nicht erforderlich und in der Praxis auch schwierig umzusetzen, da das Know-how auf dieser Seite fehlt. Bei größeren Projekten oder in Beziehung zu größeren Unternehmen könnte eventuell ein verschlüsselter E-Mail-Verkehr gewünscht sein. Hierfür ist bei Bedarf – abhängig von den Anforderungen und technischen Voraussetzungen des Kommunikationspartners – ein passendes Verfahren abzustimmen.
  ➢ Siehe hierzu Abschnitt 4.2.1.

5.2 Lösungsbeispiel für einen Freiberufler

A) Kennzeichen des Anwendungsfalls

In diesem Beispiel handelt es sich um einen Angehörigen der freien Berufe, der ohne Angestellte arbeitet, z. B. eine beratende Ingenieurin, einen Gutachter, eine Journalistin oder einen Übersetzer.

Die Kunden des Freiberuflers sind Unternehmen, denen er seine Expertise in Form von in geeigneter Weise aufbereiteten Dokumenten zur Verfügung stellt. Der Freiberufler nutzt vielfältige Quellen für seine Recherchen. Ein Steuerberater erledigt seine finanziellen Belange.

Die IT-Infrastruktur ist nicht komplex. Es gibt einen Laptop, die Datensicherung wird durch eine externe Platte unterstützt. Es wird ein Office-Paket genutzt, für Kalkulationen kann es spezielle Programme geben, deren Resultate jedoch wieder in die mit einem Textverarbeitungsprogramm erstellten Dokumente integriert werden. Für die gemeinsame Bearbeitung von Dokumenten werden gelegentlich Kollaborationsplattformen genutzt, um die Notwendigkeit für beruflich bedingte Reisen zu reduzieren.

B) Schutzbedarf der Informationen

Freiberufler stellen eine sehr spezifische Expertise bereit, die für ihre Auftraggeber von hohem Wert sein kann. Zudem gehen sie auch mit streng vertraulichen Kundeninformationen um, die sie als Auftragnehmer geheim halten müssen. Sie »erben« die Vertraulichkeitsanforderungen ihres Auftraggebers. Bei manchen Freiberuflern gibt es aufgrund ihres Berufsstandes zudem weitere Anforderungen, so müssen Journalisten ihre Quellen schützen oder aber Rechtsanwälte Mandanteninformationen selbst vor staatlichen Stellen geheim halten.

Schutzverletzungen können dazu führen, dass vertragliche Vereinbarungen verletzt werden, was wiederum Strafzahlungen nach sich ziehen kann. Üblicherweise sichern sich Freiberufler durch den Abschluss einer Berufshaftpflichtversicherung gegen mögliche Vermögensschäden ab. Unter Umständen ist dieser Versicherungsschutz aber gefährdet, wenn der Freiberufler auf angemessene Schutzmaßnahmen verzichtet, mit denen ein Schaden hätte vermieden werden können. Der mit einem Schaden verbundene Reputationsverlust kann darüber hinaus existenzgefährdend für den Freiberufler sein.

Informationsbestände	Bewertung
Informationen über Kunden (Adressdaten, Angebote, erbrachte Leistungen und Umsätze)	Dies sind sehr sensible Informationen mit sehr hohen Vertraulichkeitsanforderungen.
Arbeitsergebnisse	Dies sind für den Freiberufler aber auch für ihre Auftraggeber sehr sensible Informationen. Die Vertraulichkeitsanforderungen sind sehr hoch.
Finanzbuchhaltungsdaten	Dies sind sensible Informationen. Die Vertraulichkeitsanforderungen sind hoch.

C) Gefährdungen, Kritikalität von Speicherorten und Übertragungswegen

Die sehr speziellen Informationen, mit denen Freiberufler umgehen, können ein attraktives Angriffsziel sein, um vertrauliche Angaben über ihre Auftraggeber oder ihre Informationsquellen zu erhalten. Sie müssen damit rechnen, gezielt angegriffen zu werden. Der Verlust der Vertraulichkeit kann eine Verletzung der vertraglichen Vereinbarungen mit entsprechenden Strafen darstellen, der Reputationsverlust könnte zudem für den Freiberufler existenzgefährdend sein.

- Es kann zu Vertraulichkeitsverletzungen durch Zugriff auf Datenträger der mobilen Geräte oder auch Arbeitsplatzrechner kommen.

- Auch das Abhören von Telefonverbindungen und das Mitlesen von E-Mails und Dokumenten bei der Kommunikation mit Externen stellen weitere Gefährdungen dar.

D) Lösung

Der Freiberufler sollte die Informationen, die er verwaltet und erzeugt, bewerten und angemessene Verschlüsselungslösungen implementieren. Folgende Maßnahmen sind sinnvoll:

Gespeicherte Informationen

- Die Festplatten des Laptops müssen als Basisschutz verschlüsselt sein. Zusätzlich sollten externe Festplatten genutzt werden, um Informationen hierhin auszulagern, wenn sie abgeschlossene oder aktuell nicht bearbeitete Projekte betreffen. Falls erforderlich, sollte ein hardwareverschlüsselter USB Stick genutzt werden.
  ➢ Siehe hierzu Abschnitt 4.1.1.

- Die Festplatte sollte untergliedert und eine Containerverschlüsselung genutzt werden, um Teile der Informationen auch während der Arbeit mit dem Rechner verschlüsselt zu halten. Um Informationen gezielt zu verschlüsseln, können auch die Möglichkeiten von Anwenderprogrammen oder des Betriebssystems genutzt werden. Wichtig ist, dass während der Arbeit mit Anwendungen und projektbezogenen Informationsbeständen nicht genutzte Daten verschlüsselt bleiben.
  ➢ Siehe hierzu Abschnitt 4.1.2.

- Die Nutzung von Cloud-Speicherdiensten sollte erwogen werden. Hierbei müssen sowohl der Transport als auch die Speicherung verschlüsselt werden.
  ➢ Siehe hierzu Abschnitt 4.1.3.

- Wichtig ist eine Datensicherung, die die Datenbestände verschlüsselt hält.
  ➢ Siehe hierzu Abschnitt 4.1.4.

Übertragung von Informationen

- Die Texte von E-Mails und die beigefügten Anhänge sind in jedem Fall zu verschlüsseln. Mit den Auftraggebern ist abzustimmen, welche Lösung hierzu genutzt wird. Gibt es vom Auftraggeber keine Vorgaben, bietet sich die Nutzung von PGP (z. B. über das frei verfügbare Programm gpg4win) an.
  ➢ Siehe hierzu Abschnitt 4.2.1.

- Bei der Übertragung von Dateien können auch die Verschlüsselungskomponenten von Anwenderprogrammen genutzt werden (z. B. ZIP, PDF). Die Schlüssel müssen über einen separaten Weg übertragen werden (z. B. in einem persönlichen Telefo-

nat). Die Nutzung dieser symmetrischen Verschlüsselung birgt die Gefahr, die Kontrolle über die Schlüssel zu verlieren, da die Adressaten der Dateien diese weitergeben können.
➢ Siehe hierzu Abschnitt 4.1.2.

- Werden regelmäßig besonders sensible Informationen über Mobiltelefone übertragen, sollte die Nutzung von Verfahren zur Ende-zu-Ende-Verschlüsselung erwogen werden. Hier sind Apps zur Sprachverschlüsselung verfügbar, die – bei beiden Kommunikationspartnern installiert – ein hohes Maß an Vertraulichkeit gewährleisten.
  ➢ Siehe hierzu Abschnitt 4.2.3.

- Ob internet-basierte Kommunikationsdienste genutzt werden sollten, muss im Anwendungsfall entschieden werden. Trotz Verschlüsselung der Vermittlungs-, Sprach- und Nutzerdaten gibt es Zweifel an der Sicherung der Vertraulichkeit.
  ➢ Siehe hierzu Abschnitt 4.2.3.

- Kollaborationsplattformen sind für Freiberufler sehr nützliche Anwendungen. Es sollte eine Plattform gewählt werden, die sowohl eine Transport- als auch eine Ende-zu-Ende-Datenverschlüsselung erlaubt.
  ➢ Siehe hierzu Abschnitt 4.2.4.

- Alternativ dazu können auch die von bestimmten Cloud-Diensten für ein gemeinsames Arbeiten bereitgestellten Funktionalitäten genutzt werden.
  ➢ Siehe hierzu Abschnitt 4.1.3.

5.3 Lösungsbeispiel für eine Beratungsfirma

A) Kennzeichen des Anwendungsfalls

Es handelt sich bei diesem Beispielunternehmen um eine mittelgroße Beratungsfirma, die großen Industriebetrieben, aber auch dem Mittelstand ihre Expertise anbietet. Zielgruppe sind insbesondere Automobilunternehmen und ihre Zulieferer. Aufgabenschwerpunkte sind unter anderem die Unterstützung bei der Optimierung von Produktionsprozessen, die Entwicklung von Marketingkonzepten und die Durchführung von Schulungen. Es gibt einen Standort, jedoch arbeiten die Berater bei den Kunden vor Ort. Die Unternehmung hat 120 Mitarbeiter und verfügt über eine eigene Verwaltung für das Abrechnungs- und Finanzwesen.

Die IT-Infrastruktur umfasst zentrale Server und Arbeitsplatzrechner, im Wesentlichen in den Verwaltungsbereichen. Die Berater sind mit mobilen Systemen (Laptops, Smartphones, Tablets) ausgestattet.

Es gibt ein kleines Team, das die IT-Infrastruktur betreut. Basiswissen zur IT-Sicherheit ist vorhanden.

B) Schutzbedarf der Informationen

Informationsbestände	Bewertung
Informationen über Kunden (Adressdaten, Angebote, Beauftragungen und Umsätze)	Dies sind vertrauliche Kundeninformationen, gleichzeitig geben sie wertvolle Informationen über die Positionierung am Markt des Beratungsunternehmens. Sie haben sehr hohe Vertraulichkeitsanforderungen.
Projektinformationen (Zwischenberichte, Studien, Kalkulationen)	Dies sind sehr sensible Informationen aus den Unternehmen der Kunden. Sie haben sehr hohe Vertraulichkeitsanforderungen.
Finanzbuchhaltungsinformationen, Jahresabschlüsse	Diese Informationen reflektieren die Ertragskraft des Unternehmens. Sie haben sehr hohe Vertraulichkeitsanforderungen.
Lohn- und Gehaltsdaten	Dies sind personenbezogene Informationen mit sehr hohen Vertraulichkeitsanforderungen.
Informationsmaterial über das Unternehmen	Diese Informationen werden breit genutzt und haben keine besonderen Vertraulichkeitsanforderungen.

C) Gefährdungen, Kritikalität von Speicherorten und Übertragungswegen

Das Unternehmen hat eine sehr spezifische Expertise, die für Angreifer interessant ist. Zudem verwaltet es höchst vertrauliche Informationen über seine Kunden, ihre Struktur und Produktionsprozesse. Es muss daher damit gerechnet werden, dass dieses Unternehmen Gegenstand gezielter Angriffe werden kann. Dies würde nicht nur die Verletzung von Verträgen, in den Vertraulichkeitsvereinbarungen enthalten sind, bedeuten, sondern der Reputationsverlust könnte die Existenz des Unternehmens gefährden.

Angriffe könnten sich auf die im Unternehmen gespeicherten Informationen richten, aber auch die mobilen Systeme, die breit im Einsatz sind, bergen sowohl bei der Speicherung und Übertragung von Daten als auch der Sprachkommunikation besondere Risiken. Die Berater, die bei Kunden vor Ort arbeiten müssen in besonderer Weise über Vertraulichkeitsrisiken informiert und zu einem sicherheitskonformen Verhalten motiviert werden.

D) Lösung

Für das Unternehmen ist eine sorgfältige Analyse und Klassifizierung der genutzten Informationen unabdingbar. Eine Richtlinie zur Handhabung der Informationen muss erstellt und überwacht werden. Jedem Mitarbeiter muss die Bedeutung eines angemessenen Umgangs mit Informationen in regelmäßig stattfindenden Schulungen kommuniziert werden.

Für die wichtigsten Informationen – dies sind die Informationen über Kunden und die Projekte mit ihnen – müssen Maßnahmen implementiert werden, die höchsten Vertraulichkeitsanforderungen genügen. Ein Verschlüsselungskonzept ist zu entwickeln. Dieses

muss die nachfolgend beschriebenen Maßnahmen für die Speicherung und Übertragung der Informationen adressieren.

Gespeicherte Informationen

- Auf den Laptops der Berater sollten nur die aktuell benötigten Informationen und Anwendungen verfügbar sein. Die Festplatten der Geräte sind zu verschlüsseln.
  ➢ Siehe hierzu Abschnitt 4.1.1.

- Die Festplatte des Laptops ist zu gliedern und eine Containerverschlüsselung zu nutzen, um Teile der Informationen auch während der Arbeit mit dem Rechner verschlüsselt zu halten. Um Informationen gezielt zu verschlüsseln, können auch die Möglichkeiten von Anwenderprogrammen oder des Betriebssystems genutzt werden. Wichtig ist, dass während der Arbeit mit Anwendungen und projektbezogenen Informationsbeständen nicht genutzte Daten verschlüsselt bleiben.
  ➢ Siehe hierzu Abschnitt 4.1.2.

- Wenn Cloud-Dienste Datenablage genutzt werden, kann auf Reisen ins Ausland auf die Speicherung von Projektinformationen auf dem Laptop verzichtet werden. Die Daten, die auf Cloud-Speichern abgelegt werden, müssen sowohl beim Transport als auch bei der Speicherung verschlüsselt sein. Die Nutzung von Cloud-Speichern ist für diesen Anwendungsfall zu empfehlen, da bei der Einreise in bestimmte Länder Laptops zumindest zeitweise beschlagnahmt und überprüft werden.
  ➢ Siehe hierzu Abschnitt 4.1.3.

- Nutzung von hardwareverschlüsselten USB-Sticks
  ➢ Siehe hierzu Abschnitt 4.1.1.

- Auch die PCs in der Firmenzentrale sind in das Verschlüsselungskonzept einzubeziehen. Hierfür bietet sich für die Festplatten eine Containerverschlüsselung an, so dass nur Befugte auf Projektinformationen zugreifen können. Diese sollten auch dem Zugriff durch Administratoren entzogen werden.
  ➢ Siehe hierzu Abschnitt 4.1.2.

- Wichtig ist eine regelmäßige Datensicherung, die die Datenbestände verschlüsselt hält.
  ➢ Siehe hierzu Abschnitt 4.1.4.

Übertragung von Informationen

- Die Texte von E-Mails und die beigefügten Anhänge sind in jedem Fall zu verschlüsseln. Für das Unternehmen ist die Nutzung von PGP eine Handlungsoption. Da die E-Mail-Verschlüsselung von so großer Bedeutung ist, sollte das Unternehmen die Nutzung einer externen oder aber sogar den Aufbau einer eigenen Public-Key-Infrastruktur (PKI) erwägen. Dies ermöglicht eine deutlich vereinfachte Nutzung durch die Anwender. Für diese Projekte ist eventuell externe Unterstützung erforderlich.
  ➢ Siehe hierzu Abschnitt 3 und 4.2.1.

- Für die Sprachkommunikation sollte VoIP gewählt und bei der Wahl eines externen Dienstleisters darauf geachtet werden, dass dieser Funktionen bereitstellt, um nicht nur die Kommunikation mit Externen, sondern auch die Signalisierungs- und Nutzdaten zu und vom Serviceprovider dem Zugriff Dritter zu entziehen.
  ➢ Siehe hierzu Abschnitt 4.2.3.

- Auch die Mobilfunkverbindungen müssen durch zusätzliche Sicherungsmaßnahmen verschlüsselt werden. Hierzu können Apps bei beiden Kommunikationspartnern installiert werden.
  ➢ Siehe hierzu Abschnitt 4.2.3.

- Die Nutzung von Kollaborationsanwendungen ist für das Beratungsunternehmen sehr wichtig. Hier müssen Werkzeuge eingesetzt werden, die eine wirksame Ende-zu-Ende-Verschlüsselung erlauben.
  ➢ Siehe hierzu Abschnitt 4.2.4.

- Alternativ dazu können auch die von bestimmten Cloud-Diensten für ein gemeinsames Arbeiten bereitgestellten Funktionalitäten genutzt werden.
  ➢ Siehe hierzu Abschnitt 4.1.3.

Übergreifende Maßnahmen

- Da Verschlüsselung für verschieden Anwendungsfälle genutzt wird, ist ein Schlüsselmanagementsystem zu entwerfen, das die Vertraulichkeit der Schlüssel und ihre langfristige Nutzung sichert. Eine eigene PKI (siehe oben) kann hierfür ein wichtiger Baustein sein.
  ➢ Siehe hierzu die Abschnitte 3.4 und 4.3.

5.4 Lösungsbeispiel für ein mittleres Unternehmen

A) Kennzeichen des Anwendungsfalls

Es handelt sich bei diesem Beispielunternehmen um ein Produktionsunternehmen, das in seinem Leistungsspektrum Marktführer ist. Es gibt neben der Zentrale einen weiteren Produktionsstandort in einem europäischen Land, Verkaufsniederlassungen mit jeweils wenigen Mitarbeitern jedoch in allen wichtigen Industrieländern. Die Unternehmung hat 500 Mitarbeiter, von denen 300 in der Zentrale arbeiten. Neben der Produktion gibt es Verwaltungseinheiten und eine Entwicklergruppe, die die vorhandenen Produkte optimiert und neue Lösungen erarbeitet. Der Inhaber des Unternehmens hält mehrere Patente. Die Entwicklungsarbeiten sichern dem Unternehmen seine Marktführerschaft.

Die IT-Infrastruktur umfasst zentrale Server und Arbeitsplatzrechner für den Verwaltungs- und Entwicklungsbereich. Zusätzlich sind Produktionssteuerungssysteme im Einsatz. Es gibt wenige Laptops, im Wesentlichen nur für die Ingenieure Diese werden für Fernwartungszwecke genutzt.

Es gibt ein kleines Team, das die IT-Infrastruktur betreut, Basiswissen zur IT-Sicherheit ist vorhanden.

B) Schutzbedarf der Informationen

Informationsbestände	Bewertung
Informationen über Kunden (Adressdaten, Angebote, Beauftragungen und Umsätze)	Dies sind vertrauliche Kundeninformationen, die etwa für Konkurrenten von großem Wert wären. Sie haben sehr hohe Vertraulichkeitsanforderungen.
Forschungs- und Entwicklungsergebnisse zu den Produkten des Unternehmens, Know-how über Produktionsverfahren	Dies sind die wertvollsten Informationen des Unternehmens. Sollten sie an die Konkurrenz gelangen, gefährdet dies die Marktposition und damit die Existenz des Unternehmens. Sie haben sehr hohe Vertraulichkeitsanforderungen.
Analysen zur Entwicklung und Besonderheiten der Märkte für die Produkte des Unternehmens	Auch dies sind sehr wichtige Informationen, die die Marktführerschaft langfristig absichern. Sie haben sehr hohe Vertraulichkeitsanforderungen.
Finanzbuchhaltungsinformationen, Jahresabschlüsse	Diese Informationen reflektieren die Ertragskraft des Unternehmens. Sie haben sehr hohe Vertraulichkeitsanforderungen.
Lohn- und Gehaltsdaten	Dies sind personenbezogene Informationen mit sehr hohen Vertraulichkeitsanforderungen.
Informationsmaterial über das Unternehmen	Diese Informationen werden breit genutzt und keine besonderen Vertraulichkeitsanforderungen.

C) Gefährdungen, Kritikalität von Speicherorten und Übertragungswegen

Die Ertragskraft des Unternehmens basiert auf dem produktspezifischen Know-how und einer guten Kenntnis der Zielmärkte. Auch Informationen über die Herstellungsverfahren sind von großer Wichtigkeit und sichern den Vorsprung im Markt. Sollten der Konkurrenz hierzu Details bekannt werden, ist die Existenz des Unternehmens gefährdet. Insbesondere diese Informationen müssen besonders gesichert werden.

Durch seine dezentrale Produktionsstruktur und seine Vertriebsorganisation mit Niederlassungen in vielen Ländern der Welt, bieten sich möglichen Angreifern mehrere Zielpunkte für Cyberattacken. Von besonderem Interesse sind die Entwicklungsabteilung und die dort tätigen Ingenieure.

Das Unternehmen muss damit rechnen, gezielt angegriffen zu werden. Dies betrifft die IT-Systeme des Unternehmens aber auch die Mitarbeiter, die durch »Social Engineering«-Attacken betroffen sein können. Ihr Verhalten könnte ausspioniert werden, ihre Aktivitäten im Internet könnten verfolgt und sie durch gezielte Ansprache dazu verleitet werden, – auch unbeabsichtigt – geheime Informationen an nicht Berechtigte weiterzugeben.

D) Lösung

Für das Unternehmen ist eine sorgfältige Analyse und Klassifizierung der genutzten Informationen unabdingbar. Eine Richtlinie zur Handhabung der Informationen muss erstellt und überwacht werden. Insbesondere dem Entwicklerteam muss die Bedeutung eines angemessenen Umgangs mit Informationen regelmäßigen Schulung und Sensibilisierungsveranstaltungen kommuniziert werden.

Auch wenn die Gefährdungen, denen die sensiblen Unternehmensdaten ausgesetzt sind, sich durch Verschlüsselung nicht vollständig vermeiden lassen, trägt diese Maßnahme doch dazu bei, das Risiko von Vertraulichkeitsverlusten wesentlich zu senken. Ein Verschlüsselungskonzept, das insbesondere die Gefährdungen des sensiblen Produktionswissens adressiert, muss daher entwickelt werden. Es sollte folgende Maßnahmen für die Speicherung und Übertragung der Informationen enthalten:

Gespeicherte Informationen

- Auf den Laptops der Ingenieure, die sie im Wesentlichen für Fernwartungen nutzen, sollten nur die aktuell benötigten Informationen und Anwendungen verfügbar sein. Die Festplatten der Geräte sind zu verschlüsseln.
  ➢ Siehe hierzu Abschnitt 4.1.1.

- Auch die Infrastruktur der Firmenzentrale, des weiteren Produktionsstandorts und die Vertriebsniederlassungen sind in dem Verschlüsselungskonzept zu berücksichtigen. Dabei sollten die IT-Systeme der Entwicklungsabteilung besonders abgesichert werden.

- Die Festplatten der genutzten Systeme sollten zusätzlich zu einem sorgfältig überwachten Berechtigungssystem, eine Containerverschlüsselung enthalten, so dass gewährleistet ist, dass nur Befugte auf bestimmte Bereiche zugreifen können. Diese besonders sensiblen Bereiche, sollten auch dem Zugriff durch Administratoren entzogen werden.
  ➢ Siehe hierzu Abschnitt 4.1.2.

- Wichtig ist eine regelmäßige Datensicherung, die insbesondere die Daten über Produktionsverfahren und Entwicklungsergebnisse verschlüsselt hält.
  ➢ Siehe hierzu Abschnitt 4.1.4.

Übertragung von Informationen

- Die Texte von E-Mails und die beigefügten Anhänge sind in jedem Fall zu verschlüsseln. Dies ist von besonderer Relevanz für die Austausch mit den Handelsniederlassungen in Ländern außerhalb der Europäischen Union. Für das Unternehmen ist die Nutzung von PGP oder einer anderen Software zur E-Mail-Verschlüsselung eine Handlungsoption. Da die E-Mail-Verschlüsselung von so großer Bedeutung ist, sollte das Unternehmen eine eigene Public-Key-Infrastruktur aufbauen und betreiben. Dies ermöglicht eine deutlich vereinfachte Nutzung durch die Anwender. Für dieses Projekt ist eventuell externe Unterstützung erforderlich.
  ➢ Siehe hierzu Abschnitt 4.2.1.

- Zum Austausch von Daten zwischen Zentrale und den weiteren Standorten des Unternehmens sollte VPN zur Verfügung stehen.
  ➢ Siehe hierzu Abschnitt 4.2.5.

- Für Wartungs- und Konfigurationszwecke über das Internet sollten sichere Dienste genutzt werden. Systeme auf der Basis von RDP oder VNC müssen zusätzlich durch eine Transportverschlüsselung gesichert werden.
  ➢ Siehe hierzu Abschnitt 4.2.6.

- Das Unternehmensnetz ist entsprechend der Kritikalität der jeweils gespeicherten, bearbeiteten und übertragenen Daten zu segmentierten. Aufgrund des hohen Geheimhaltungsbedarfs der Informationen in der Entwicklergruppe bilden deren Computer ein eigenes Netzsegment, das mithilfe von MACsec abgesichert wird.
  ➢ Siehe hierzu Abschnitt 4.2.7.

- Das Unternehmen sollte eine eigene VoIP-basierte Telefonanlage betreiben oder die Dienste eines vertrauenswürdigen externen Anbieters von VoIP-Diensten nutzen. In beiden Fällen müssen sowohl die Nutzdaten als auch die Signalisierungsdaten durch Verschlüsselung dem Zugriff Dritter entzogen werden.
  ➢ Siehe hierzu Abschnitt 4.2.3.

- Auch die Mobilfunkverbindungen müssen durch zusätzliche Sicherungsmaßnahmen verschlüsselt werden. Hierzu sind Apps verfügbar, die beide Kommunikationspartner installieren müssen.
  ➢ Siehe hierzu Abschnitt 4.2.3.

- Kollaborationsanwendungen sind für Konferenzen mit dem weiteren Standort und der Handelsniederlassung hilfreich. Hierfür müssen Werkzeuge eingesetzt werden, die eine wirksame Ende-zu-Ende-Verschlüsselung erlauben.
  ➢ Siehe hierzu Abschnitt 4.2.4.

Übergreifende Maßnahmen

- Das Unternehmen nutzt Verschlüsselung für eine Vielzahl von Anwendungsfällen. Damit die genutzten Schlüssel vertraulich bleiben und auch langfristig im Zugriff sind, muss ein angemessenes Schlüsselmanagement implementiert werden. Hierfür bietet sich eine zentrale Softwarelösung zur Schlüsselverwaltung an.
  ➢ Siehe hierzu Abschnitt 4.3.

5.5 Lösungsbeispiel für eine Firma mit Außendienstmitarbeitern

A) Kennzeichen des Anwendungsfalls

Es handelt sich bei dem Beispielunternehmen um ein großes Versicherungsunternehmen, das mit vielen Außendienstmitarbeitern zur Betreuung der Privatkunden arbeitet. In diesem Szenario wird ausschließlich die Handhabung der Informationsbestände betrachtet, die diesen zur Verfügung gestellt werden und die diese wiederum an die Zentrale übertragen.

Das Versicherungsunternehmen stellt den Außendienstlern alle relevanten Informationen für die Betreuung der Kunden zur Verfügung, bei Abschluss und Änderung von Verträgen geben die Mitarbeiter diese Informationen an ihre Zentrale weiter. Zur Diskussion über Produktdarstellungen oder aber Übersichten über Vertriebsergebnisse werden Kollaborationsplattformen eingesetzt.

Sie nutzen für ihre Arbeit Laptops, die auch für eigene und ihre Vertriebsaufgaben relevante Anwendungen verwendet werden. Dies sind in der Regel Office-Pakete, mit denen sie zusätzliche Kundeninformationen verwalten oder Kalkulationen erstellen.

Beim Versicherungsunternehmen sind eine hohe IT-Kompetenz und auch IT-Sicherheits-Know-how vorhanden. Dies trifft jedoch nicht auf die Vertriebsmitarbeiter zu. Sie erhalten ihren Laptop mit den erforderlichen Anwendungslösungen konfiguriert von der IT-Abteilung der Versicherung.

Bei den Privatkunden, die von den Außendienstmitarbeitern betreut werden, ist nur sehr geringe IT-Kompetenz vorauszusetzen. Es gibt jedoch auch sehr bewusste Kunden, die hinsichtlich der Fragen der IT-Sicherheit inzwischen sensibilisiert sind.

B) Schutzbedarf der Informationen

Informationsbestände	Bewertung
Informationen über Kunden (Adressdaten, Angebote, Verträge und Umsätze)	Dies sind vertrauliche Informationen, die essentiell wichtig für einen Vertriebsmitarbeiter sind, sie haben sehr hohe Vertraulichkeitsanforderungen. Dies gilt insbesondere durch den Personenbezug zu Kunden etwa bei Krankenversicherungen.
Informationen über strategische Planungen, kundespezifische Preiskalkulationen, Vertriebsanweisungen	Dies sind sehr sensible Informationen des Versicherungsunternehmens, die von hohem Wert für Konkurrenzunternehmen sind und deswegen sehr hohe Vertraulichkeitsanforderungen haben.
Informationsmaterial über das Versicherungsunternehmen und seine Produkte	Diese Informationen werden breit genutzt und sind z. T. sogar öffentlich verfügbar, es gibt keine besonderen Vertraulichkeitsanforderungen

C) Gefährdungen, Kritikalität von Speicherorten und Übertragungswegen

Außendienstmitarbeiter verfügen über sensible Informationen, die für potenzielle Angreifer von großem Wert sein können, dies sind sowohl kunden- als auch versicherungsbezogene Informationen. Gelangen etwa Informationen im Zusammenhang mit dem Abschluss einer Krankenversicherung über den Gesundheitszustand eines Kunden an Unbefugte, verstößt dies gegen Datenschutzvorschriften. Dies kann sowohl bei dem Außendienstmitarbeiter als auch bei der Versicherung geahndet werden. Gelangen personenbezogene Informationen an die Öffentlichkeit, ist das zudem mit großen Reputationsschäden verbunden. Entsprechend des Datenschutzgesetzes müssen in diesem Fall Betroffene informiert werden, was zu einem aufwendigen Kommunikationsprozess führt. Zudem ist nicht auszuschließen, dass es zu umfangreichen Kündigungen kommt.

Die Vertraulichkeit sichert zudem die Wettbewerbsposition des Versicherungsunternehmens. Erlöse aus neuen Produkten und Vertriebsstrategien sind gefährdet, wenn Informationen hierzu vorzeitig an die Konkurrenz gelangen.

Es ist nicht auszuschließen, dass gezielte Angriffe auf die Informationsbestände erfolgen.

D) Lösung

Insbesondere personenbezogene Daten und vertrauliche Informationen über Strategien zur Planung und Entwicklung von Produkte des Versicherungsunternehmens müssen besonders geschützt werden.

Hierzu ist ein Verschlüsselungskonzept zu entwerfen, das auf der Klassifizierung der Informationen in den Geschäftsprozessen basiert. Dieses Konzept sollte folgende Maßnahmen für die Speicherung und Übertragung der Informationen adressieren:

Gespeicherte Informationen

- Die Festplatten der von den Außendienstmitarbeitern genutzten Laptops sind zu verschlüsseln.
  ➢ Siehe hierzu Abschnitt 4.1.1.

- Zusätzlich sollte Containerverschlüsselung für die Ablage vertraulicher Daten genutzt werden.
  ➢ Siehe hierzu Abschnitt 4.1.2.

- Die Nutzung von Cloud-Diensten ist sinnvoll. Es ist darauf zu achten, dass die Daten verschlüsselt übertragen und beim Provider verschlüsselt gehalten werden.
  ➢ Siehe hierzu Abschnitt 4.1.3.

- Die Daten des Laptops sind regelmäßig in die unternehmensinterne Datensicherung einzubeziehen. Sie müssen verschlüsselt abgelegt werden.
  ➢ Siehe hierzu Abschnitt 4.1.4.

Übertragung von Informationen

- Die Texte von E-Mails und die beigefügten Anhänge sind in jedem Fall zu verschlüsseln. Das Versicherungsunternehmen sollte eine eigene PKI betreiben, die den Außendienstmitarbeitern eine komfortable Verschlüsselung ihrer E-Mails im internen Verkehr ermöglicht. Angebote an Kunden sollten nicht per E-Mail verschickt, sondern ein eigenes sicheres webbasiertes Kundenportal oder der klassische Postweg sollte genutzt werden. Sind die Außendienstmitarbeiter für Industriekunden aktiv, so ist ein Austausch von öffentlichen Schlüsseln sinnvoll, um eine vertrauliche Kommunikation zu ermöglichen. Dies gilt auch für Privatkunden, die über S/MIME-Zertifikate verfügen.

  Auf Wunsch besonders sensibilisierter Privatkunden, die nicht über S/MIME-Zertifikate verfügen, könnte für die Kommunikation per E-Mail PGP genutzt werden.
  ➢ Siehe hierzu Abschnitt 4.2.1.

- Falls Informationen mit Kunden über einen Messenger ausgetauscht werden, sollten Produkte genutzt werden, die eine Verschlüsselung anbieten. Hier sollte der Außendienstmitarbeiter seine Kunden für die Nutzung sicherer Lösungen motivieren.
  ➢ Siehe hierzu Abschnitt 4.2.2.

- Kollaborationsanwendungen sind für Außendienstmitarbeiter nützlich. Hier müssen Werkzeuge eingesetzt werden, die eine wirksame Ende-zu-Ende-Verschlüsselung erlauben.
  ➢ Siehe hierzu Abschnitt 4.2.4.

- Für die Sprachkommunikation sollte VoIP gewählt und bei der Wahl eines externen Dienstleisters darauf geachtet werden, dass dieser Funktionen bereitstellt, um nicht nur die Kommunikation mit Externen sondern auch die Signalisierungs- und Nutzdaten zu und vom Serviceprovider dem Zugriff Dritter zu entziehen.
  ➢ Siehe hierzu Abschnitt 4.2.1.

- Auch die Mobilfunkverbindungen zwischen Außendienstmitarbeitern und Mitarbeitern des Versicherungsunternehmens müssen durch zusätzliche Sicherungsmaßnahmen verschlüsselt werden. Dies kann durch die Installation entsprechender Apps bei den Smartphones beider Kommunikationspartner erreicht werden.
  ➢ Siehe hierzu Abschnitt 4.2.3.

- Zur Übertragung von Daten und zur Nutzung zentraler Anwendungen ist eine VPN-Verbindung erforderlich.
  ➢ Siehe hierzu Abschnitt 4.2.5.

Übergreifende Maßnahmen

- Da im Versicherungsunternehmen eine PKI implementiert ist, die Dienste für die Verschlüsselung der E-Mail-Kommunikation bereitstellt, ist die Verwaltung der Schlüssel zentral organisiert und sind alle wichtigen Aufgaben in diesem Kontext adressiert. Die Handhabung weiterer Schlüssel, etwa für die Verschlüsselung von Festplatten und Dateien auf den Laptops, muss durch ein erweitertes Konzept beschrieben werden.
  ➢ Siehe hierzu die Abschnitte 3.4 und 4.3.

5.6 Zusammenfassung aller Szenarien

Die exemplarischen Lösungen für die fiktiven Beispielunternehmen haben gezeigt, dass Verschlüsselungsmaßnahmen individuell konzipiert werden müssen. Die Anforderung an eine Lösung wird im wesentlich bestimmt durch:

- die **Kritikalität der Daten**, also die Frage, welche Auswirkung auf die Ertragskraft eines Unternehmens eine Verletzung der Vertraulichkeit hat; auch Haftungszusagen oder gesetzliche oder vertragliche Verpflichtungen spielen eine Rolle;

- mögliche **Angriffspunkte in der IT-Nutzung**; insbesondere, wenn Firmen sehr stark auf internetbasierte Prozesse und mobile Anwendungen angewiesen sind, müssen die übertragenen Daten und die verwendeten IT-Systeme durch geeignete Verschlüsselungsmaßnahmen geschützt werden;

- das **Know-how** der Anwender und IT-Administratoren zur IT im Allgemeinen und zur IT-Sicherheit im Besonderen; es dürfen nur solche Verschlüsselungslösungen eingesetzt werden, die auch von den betroffenen Unternehmen und Benutzern organisatorisch bewältigt und beherrscht werden können.

Für alle Unternehmen jedoch gilt, dass Vertraulichkeitsverletzungen erhebliche Konsequenzen haben können. Sie müssen sich daher aus der Vielzahl der Lösungsoptionen die für sie geeigneten zusammenstellen.

Abb. 11 gibt eine tabellarische Übersicht über die wesentlichen Empfehlungen der möglichen Lösungen für die beschriebenen exemplarischen Unternehmen.

Abb. 11 Zusammenfassung der Beispielszenarien

Maßnahme	**Kleinunternehmen**	**Freiberufler**	**Beratungsfirma**	**Mittleres Unternehmen**	**Unternehmen mit Außendienst**
Verschlüsselung des Speichermediums	X (für Laptop)	X (für Laptop)	X (für Laptops)	X (für Laptops)	X (für Laptops)
Containerverschlüsselung	X	X	X	X	X
Verschlüsselung mithilfe von Anwendungsprogrammen	X	X			
Verschlüsselung für Cloudspeicher		X	X		X
E-Mails – S/MIME			(X)	X	X
E-Mails – PGP	Ü	X	X		
Verschlüsseltes Instant Messaging				X	
VoIP – intern				X	
VoIP – extern			X		X
Verschlüsselungslösungen für Mobilfunk		X	X	X	X
Verschlüsselte Kollaborationsanwendungen		X	X	X	X
VPN				X	X
Weitere Verschlüsselungsmaßnahmen für externe Zugriffe				X	
Verschlüsselungslösungen für die interne Kommunikation				X	

Legende:

X	=	Empfehlung
(X)	=	bedingte Empfehlung
Ü	=	keine zwingende Anwendung, da Überlappung mit anderer Technik (Im Beispiel kann vertraulicher Inhalt auch übertragen werden, indem dieser als Anhang verschickt wird, der zuvor mithilfe der diesbezüglichen Funktionen eines Anwendungsprogramms verschlüsselt wurde.)
<leeres Feld>	=	keine Anwendung, nicht relevant

6 Zusammenfassung

Dieser Leitfaden liefert einen Überblick über mögliche Verfahren zur Verschlüsselung und deren Anwendungsbereiche. Die folgenden Punkte fassen die wichtigsten Empfehlungen zusammen:

1. Risikobewertung für sensible Informationen durchführen

Der Einsatz von Verschlüsselung sollte auf einer Bewertung des Schutzbedarfs der Informationen in einem Unternehmen und möglicher Angriffsszenarien beruhen. Darauf aufbauend sind die Kritikalität von Datenspeichern und der Datenübertragung zu bestimmen und angemessene Verschlüsselungslösungen zu wählen.

2. Datenübertragung absichern

Wenn vertrauliche Daten über Netze ausgetauscht werden, bei denen sie ohne eine solche Absicherung im Klartext mitgelesen werden können, ist auf eine ausreichende Verschlüsselung der Verbindung zu achten – bei der Übertragung im Internet beispielsweise auf den Einsatz von SSL/TLS und die Gültigkeit der hierfür verwendeten Zertifikate.

3. Vertrauliche Informationen verschlüsseln

Oft ist es darüber hinaus erforderlich, nicht nur die Übertragungswege, sondern auch die übertragenen Daten selber zu verschlüsseln, etwa um zu verhindern, dass der Administrator eines Servers, auf dem die Daten zwischengespeichert werden, diese einsieht. Das hierfür zu verwendende Verfahren hängt von dem gewählten Anwendungszweck und den Anforderungen der beteiligten Kommunikationspartner ab. Für den Versand vertraulicher Informationen via E-Mail bieten sich beispielsweise die folgenden Möglichkeiten an:

- Sofern mit einem Kommunikationspartner regelmäßig vertrauliche E-Mails ausgetauscht werden, bietet sich eine Ende-zu-Ende Verschlüsselung der Nachrichten und der Austausch entsprechender Schlüssel an. Ob das gewählte Verfahren auf PGP oder S/MIME beruht, ist zwischen den Kommunikationspartnern zu vereinbaren.

- In vielen Fällen ist aus Unternehmenssicht keine Ende-zu-Ende-Verschlüsselung erforderlich oder wünschenswert. Dann ist eine Gateway-Verschlüsselung, also die Verschlüsselung der E-Mail am Übergang zwischen Unternehmensnetz und Internet, eine Alternative für den sicheren Transport der Nachricht.

- Bei einem lediglich sporadischen Austausch vertraulicher Dateien innerhalb eines überschaubaren Kreises von Kommunikationspartnern bietet es sich an – sofern andere Verfahren als zu aufwendig erscheinen –, Dateien mithilfe der diesbezüglichen Funktionen der zugrundeliegenden Anwendungen (Office, Acrobat etc.) oder eines ZIP-Archivs zu verschlüsseln und anstelle der unverschlüsselten Originale zu versenden.

4. Sprachkommunikation absichern

Bei der modernen Voice-over-IP-Sprachkommunikation ist auf die Aktivierung von Sicherheitsfunktionen der verwendeten Client-Programme und Endgeräte zu ach-

ten. Hierzu zählt die Verschlüsselung der Sprachdaten ebenso wie die Verschlüsselung der Signalisierungsnachrichten. Dies gilt unabhängig davon, ob tatsächlich über das Internet, in geschlossenen, privaten IP-Netzen oder über externe Dienstanbieter telefoniert wird. Unter Umständen müssen nicht nur die Clients und Endgeräte, sondern auch das zugehörige Telekommunikations- oder Unified-Communications-System entsprechend konfiguriert werden.

5. Absicherung vertraulicher Daten im internen Netz nicht vernachlässigen

Vertrauliche Daten sollten auch im internen Netz vor unbefugten Zugriffen geschützt bleiben. Teilbereiche mit hochgradig vertraulichen Daten sollten ein eigenes Netzsegment bilden, in dem die Daten verschlüsselt übertragen werden.

6. Besonders vertrauliche Dateien und Verzeichnisse gesondert verschlüsseln

Personaldaten sollten beispielsweise nicht von den Administratoren eingesehen werden können. In solchen und anderen Fällen, in denen der Inhalt nur ein ausgesuchter Personenkreis einsehen darf, sollten Dateien so verschlüsselt werden, dass sie ausschließlich von dazu Berechtigten entschlüsselt werden können. Hierfür bietet sich die Public-Key-Verschlüsselung an.

7. Für effizientes Schlüsselmanagement sorgen

Es sollte versucht werden, Verschlüsselungsverfahren zu integrieren, sofern dies technisch möglich und aus Sicherheitssicht unbedenklich ist. Ein möglichst zentrales Schlüsselmanagement erleichtert es, Verschlüsselung im Unternehmen effizient und wirksam umzusetzen.

8. Notfälle berücksichtigen

Verschlüsselung bietet einen wirksamen Schutz der Vertraulichkeit, birgt andererseits aber auch die Gefahr, dass Informationen nicht mehr verfügbar sind, wenn beispielsweise die zur Entschlüsselung erforderlichen Schlüssel und Kennwörter verloren gehen oder beschädigt werden. Diese Gefahr kann durch zusätzliche Entschlüsselungsschlüssel oder sicher aufbewahrte Kopien verringert werden.

9. Verschlüsselungskonzepte aktuell halten

Weil die Voraussetzungen eines Verschlüsselungskonzepts sich ändern können, muss regelmäßig geprüft werden, ob die gewählte Verschlüsselungsarchitektur noch den Anforderungen genügt.

Korrekt angewendet ist Verschlüsselung eine hochgradig wirksame Maßnahme zum Schutz der Vertraulichkeit sensibler Unternehmensinformationen. Für eine umfassende Sicherheit muss ein Unternehmen darüber hinaus weitere Vorkehrungen treffen, wie beispielsweise der Schutz gegen Schadsoftware, die Absicherung und Härtung externer Netzschnittstellen, eine sichere Konfiguration der eingesetzten Hard- und Software, ein effektives Patchmanagement, eine sicherheitsgerechte Vergabe von Berechtigungen, Notfallvorsorge oder eine ausreichende Sensibilisierung und Schulung der Benutzer. Verschlüsselung stellt eine sinnvolle Ergänzung dar. Wichtig ist aber, dass selbst durch die korrekte Anwendung von Verschlüsselung diese Maßnahmen bei weitem nicht überflüssig werden.

7
Anhang

7.1
Abkürzungen

3DES	Triple Digital Encryption Standard
AES	Advanced Encryption Standard
BDSG	Bundesdatenschutzgesetz
CIFS	Common Internet File System
DMS	Dokumentenmanagementsystem
DES	Digital Encryption Standard
DVD	Digital Versatile Disc
EAP	Extensible Authentication Process
EFS	Encrypting File System
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GSM	Global System for Mobile Communications
HTTPS	HyperText Transfer Protocol Secure
IDEA	International Data Encryption Algorithm
IDS	Intrusion Detection System
IRC	Internet Relay Chat
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
IT	Informationstechnik
ITU	International Telecommunication Union
KMIP	Key Management Interoperability Protocol
KMU	Kleine und mittlere Unternehmen
LAN	Local Area Network
MAC	Media Access Control
MACsec	Media Access Control secure
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
OSI	Open Systems Interconnection
OTR	Off The Record
PGP	Pretty Good Privacy
PIN	Persönliche Identifikationsnummer
PKI	Public-Key-Infrastruktur
PSK	Pre-shared Key
RC5	Rivest Cipher 5
RDP	Remote Desktop Protocol
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
RSA	Rivest, Shamir, Adleman
SD	Secure Digital
SED	Self-encrypting Devices
SFTP	SSH File Transfer Protocol
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SMB	Server Message Block
S/MIME	Security/Multipurpose Internet Mail Extension

SRTP	Secure Real-Time Transport Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
TLS	Transport Layer Security
TPM	Trusted Platform Module
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VNC	Virtual Network Computing
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
XMPP	Extensible Messaging and Presence Protocol
ZRTP	Z Real-time Transport Protocol

7.2 Weiterführende Informationen

Es gibt viele Informationen zu Verschlüsselungsmethoden und zur Nutzung von Lösungen für die in diesem Leitfaden adressierten Anwendungsfelder. Im Folgenden sind einige Quellen sowie einige wichtige bundesweite und hessische Anlaufstellen zur Informationssicherheit aufgeführt.

Grundlegendes zur Funktionsweise und Sicherheit von Verschlüsselung

Informationen zu Verschlüsselungsverfahren bietet das Bundesamt für Sicherheit in der Informationstechnik – BSI für Bürger auf seinen Internet-Seiten:
www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/Datenverschluesselung/Grundlagen/Funktionsweise/

Auch der Leitfaden zur Erstellung von Kryptokonzepten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) erläutert Methoden und Verfahren:
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Kryptokonzept_pdf

Einen Workshop mit Informationen zu den grundlegenden Begriffen hat das Institut für Internet-Sicherheit der Westfälischen Hochschule zusammengestellt:
www.internet-sicherheit.de/institut/buch-sicher-im-internet/workshops-und-themen/verschluesselung-und-identitaeten/kryptographie/grundlagen-der-kryptographie/

In einer Technischen Richtlinie (TR-02102-1) bewertet das BSI die Sicherheit von kryptographischen Verfahren:
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102_pdf

Hilfestellung bei der Umsetzung von Verschlüsselungslösungen

Die IT-Grundschutz-Kataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bietet eine umfassende Zusammenstellung von Sicherheitsmaßnahmen:
www.bsi.bund.de/IT-Grundschutz-Kataloge.
Darunter befinden sich auch Empfehlungen zum Einsatz von Verschlüsselung, z. B.

- M 6.56: Datensicherung bei Einsatz von Verschlüsselungsverfahren
- M 2.264: Regelmäßige Aufbereitung von verschlüsselten Daten bei der Archivierung

Eine leicht verständliche Einführung in das Thema E-Mailverschlüsselung gibt die Informationsbroschüre von DATEV und Deutschland sicher im Netz e.V., Verschlüsselung von E-Mails, Leitfaden zur E-Mail-Sicherheit für Unternehmen:
www.sicher-im-netz.de/sites/default/files/download/leitfaden-e-mail-verschluesselung.pdf

An Verbraucher richtet sich das Informationsangebot des Bundesministeriums der Justiz und für Verbraucherschutz zum Thema E-Mail-Verschlüsselung. Auf diesen Seiten finden sich auch viele Verweise zu weiteren Informationsquellen:
www.bmjv.de/DE/Themen/InternetundDatensicherheit/SicherimNetz/SicherimNetz_node.html

Vorgehensweise zur Klassifizierung von Informationen

Mit der Einführung der Informationsklassifizierung befasst sich Frank von Stetten in einem Artikel der Zeitschrift <kes>:
www.kes.info/archiv/online/11-6-012.htm

Nutzung von Verschlüsselung für Cloud Lösungen

Das Fraunhofer SIT hat Cloud Storage Services bewertet und die Ergebnisse in einem technischen Report veröffentlicht:
On the Security of Cloud Storage Services. SIT Technical Reports, 2012
www.sit.fraunhofer.de/de/angebote/projekte/cloud-studie/

Das Fraunhofer SIT bietet mit OmniCloud eine Lösung zur sicheren Nutzung von Cloud-Speicherdiensten an:
www.omnicloud.sit.fraunhofer.de

Praxisorientierte Tipps und Hinweise zur E-Mail-Verschlüsselung

Anleitung zu PGP und GnuPG (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein):
www.datenschutzzentrum.de/selbstdatenschutz/internet/pgp/index.htm

Artikel aus der Zeitschrift c't zur Nutzung von S/MIME, auch auf mobilen Endgeräten:
www.heise.de/ct/artikel/Brief-mit-Siegel-1911842.html

Angebote an Freeware-Lösungen für Verschlüsselung

Downloadangebote des Heise Verlags:
www.heise.de/download/sicherheit/verschluesselung-50000505182/

Auch das BSI bietet Lösungen an:
www.bsi.bund.de/DE/Themen/ProdukteTools/produktetools_node.html

Informationen und Download für die Verschlüsselungslösung Gpg4win:
www.bsi.bund.de/DE/Themen/ProdukteTools/Gpg4win/gpg4win_node.html

Informationen zu angesprochenen Standards

Casner, S.; Frederick, R.; Jacobson, V.: RFC 3550 – RTP: A Transport Protocol for Real-Time Applications. IETF, July 2003.

Baugher, M.; McGrew, D.; Naslund, M.; Carrara, E.; Norrman, K.: RFC 3711 – The Secure Real-time Transport Protocol. IETF, March 2004.

Zimmermann, P.; Johnston, A. (Ed.); Callas, J.: RFC 6189 – ZRTP: Media Path Key Agreement for Unicast Secure RTP. IETF, April 2011.

H.323 security: Framework for security in H-series (H.323 and other H.245-based) multimedia systems. ITU-T, January 2014.

H.323: Packet-based multimedia communications systems. ITU-T, December 2009.

Federal Information Processing Standards Publication 197: Announcing the Advanced Encryption Standard (AES). National Institute of Standards and Technology (NIST), November 2001.

Grundlegendes zur Bedeutung von Vertraulichkeit und Entwicklungstrends

Der Trend- und Strategiebericht des Fraunhofer SIT »Privatsphärenschutz und Vertraulichkeit im Internet« beleuchtet die einzelnen Handlungsfelder und zeigt Forschungsfragen auf:
www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/TuS-Bericht_Privacy.pdf

Bundesweite Anlaufstellen zur Informationssicherheit

Bundesamt für Sicherheit in der Informationstechnik (BSI): www.bsi.de.

BITKOM Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien e.V.: www.bitkom.org/de/themen/50790.aspx.

eco Verband der deutschen Internetwirtschaft e.V.: sicherheit.eco.de.

Nationale Initiative für Internet-Sicherheit (NIFIS e.V.): www.nifis.de.

ASW – Arbeitsgemeinschaft für Sicherheit der Wirtschaft: www.asw-online.de.

Teletrust Deutschland e.V.: www.teletrust.de.

Deutschland sicher im Netz: www.sicher-im-netz.de.

Allianz für Cybersicherheit: www.allianz-fuer-cybersicherheit.de.

IT-Sicherheitsnavigator: www.it-sicherheit-in-der-wirtschaft.de/IT-Sicherheit/Navigation/Angebote/navigator.html.

Virtuelles Datenschutzbüro: www.datenschutz.de.

Hessische Anlaufstellen zur Informationssicherheit

Fraunhofer-Institut für Sichere Informationstechnologie (Fraunhofer SIT):
www.sit.fraunhofer.de.

Center for Advanced Security Research Darmstadt (CASED): www.cased.de.

Center for Industrial Research in Cloud Security (CIRECS): www.cirecs.de.

Competence Center for Applied Security Technology (CAST e.V.):
www.cast-forum.de/home.html.

Expertengruppe IT-Sicherheit des Arbeitskreises Forum Hessen-IT:
www.hessen-it.de/forum.

Der Hessische Datenschutzbeauftragte: www.datenschutz.hessen.de.

ISBN 978-3-8396-0872-2