GOLDMEDIA

if(is) internet-sicherheit.

KOMPASS IT-VERSCHLÜSSELUNG

ORIENTIERUNGS- UND ENTSCHEIDUNGSHILFEN FÜR KLEINE UND MITTLERE UNTERNEHMEN

Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi)

Kompass IT-Verschlüsselung

Orientierungs- und Entscheidungshilfen für KMU zum Einsatz von Verschlüsselungslösungen

Datum: 20.02.2018

Autoren

Goldmedia GmbH
Strategy Consulting
Prof. Dr. Klaus Goldhammer
Dr. André Wiegand
Sebastian Lehr

if(is) - Institut für Internet-Sicherheit,
Westfälische Hochschule, Gelsenkirchen
Prof. Norbert Pohlmann
Chris Wojzechowski
Johnny Hoang
Ole Jötten

Titelbild: © kras99_Fotolia.com

Inhalt

Tabellen

Abbildungen

Daten mit Verschlüsselung sicher übertragen und ablegen

Daten sind das Kapital der Zukunft. Mit dem Voranschreiten der Digitalisierung sowie dem Ausbau von Technologien wie der Industrie 4.0 und dem Internet der Dinge wird das Datenaufkommen auch zukünftig weiter steigen. Bereits heute produzieren, versenden und speichern Unternehmen im täglichen Betrieb große Datenmengen. Teile dieser Daten sind aus wirtschaftlichen Gründen schützenswert oder aus rechtlichen Gründen schutzpflichtig. Damit diese Daten vor unberechtigten Einblicken geschützt sind, sollten sie verschlüsselt werden. Das gilt sowohl für die Aufbewahrung von Daten als auch für deren Versand über sämtliche Kommunikationskanäle hinweg.

Viele kleine und mittlere Unternehmen stehen jedoch weiterhin vor der Herausforderung, wie sie für ihre schutzbedürftigen Daten eine praxistaugliche und bezahlbare Verschlüsselung implementieren können. Vermeintlich hoher Bedienaufwand und die vermeintlich hohen Kosten für verfügbare Verschlüsselungslösungen schrecken die Unternehmen ab und bilden die größten Hemmnisse.

Dieses Dokument soll Unternehmen als Orientierung dienen, an welchen Stellen eine Verschlüsselung sinnvoll ist und welche Möglichkeiten der Umsetzung zur Verfügung stehen. Darüber hinaus werden anhand von Leitfragen in den jeweiligen Abschnitten Hilfen zu Entscheidungsfindung gegeben, welche Lösungen im eigenen Unternehmen umzusetzen sind. Die Leitfragen sollen in den Themenabschnitten als Orientierung dienen und einen leichteren und strukturierten Einstieg in das Thema Verschlüsselung bieten.

Den Schutzbedarf der wertvollen Daten ermitteln

Daten haben, je nachdem welchen Inhalt und Informationen sie beherbergen, einen unterschiedlichen Schutzbedarf. Diese Unternehmensdaten müssen identifiziert und differenziert werden. Daher ist es essenziell, eine Schutzbedarfsfeststellung der Daten vorzunehmen. Unternehmenswertvolle Daten wie z.B. Kundendaten oder personenbezogene Daten können erst so identifiziert werden. Anschließend müssen Maßnahmen ermittelt werden, wie diese Unternehmensdaten zu schützen sind. Dies kann mithilfe von Unternehmensrichtlinien zur Informationssicherheit gelingen. So können die Daten in Schutzklassen differenziert werden und mit Zugriffsrechten für unterschiedliche Mitarbeitergruppen versehen werden.

Zur Ermittlung der für Sie relevanten Kapitel beantworten Sie bitte zunächst folgende Fragen für sich:

- *Handelt es sich um unternehmenskritische Daten, ohne die der Betrieb oder die Produktion des Unternehmens eingeschränkt wäre?*

➔ Weiterführende Informationen finden Sie in Kapitel 2: „Daten sicher ablegen – dank Verschlüsselung“, Seite 32

- *Handelt es sich bei den Daten um Betriebsgeheimnisse oder unterliegen diese datenschutzrechtlichen Vorschriften?*

➔ Weiterführende Informationen finden Sie in Kapitel 2.2: „Dateiverschlüsselung – sicher vor Einblicken Dritter“, Seite 37

- *Sollen Daten außerhalb des Unternehmensumfeldes verfügbar sein?*

➔ Weiterführende Informationen finden Sie in Kapitel 1.6: „Virtual Private Network – der private Tunnel ins Unternehmen“, Seite 27

1 Daten übertragen – so geht es sicher und verschlüsselt!

Die Übertragung potenziell schützenswerter Daten eines Unternehmens erfolgt in der Regel über folgende zentrale Plattformen:

- E-Mail-Server
- IP- und ISDN-basierte Sprachtelefonie
- Messaging-Dienste
- Kollaborationsplattformen für die Projektarbeit mit Dritten
- eigene Webseiten, die personenbezogene Daten erfassen, oder anmeldepflichtige Dienste, die z.B. kostenpflichtige Datendienste oder E-Commerce-Anwendungen bereitstellen
- LAN und VPN zur Verbindung mit firmeneigenen Datenservern und dem Intranet

Damit diese Informationen während des Transports geschützt sind, braucht es verschlüsselte Kommunikationswege. Dieses Kapitel zeigt, welche Möglichkeiten zur Verschlüsselung bei den einzelnen Diensten zum Einsatz kommen können.

1.1 E-Mail – zusätzliche Infrastruktur, aber sicher!

Die E-Mail ist schnell, kostenlos, einfach zu bedienen, erfüllt im Schriftverkehr die Textform und dient häufig als Voraussetzung und sicherer, verifizierter Ausgangspunkt für das Anlegen und Zurücksetzen von Benutzerkonten. Durch diese Eigenschaften stellt die E-Mail weiterhin das zentralste Kommunikationsmedium in der Geschäftswelt dar.

Vier von fünf Unternehmen nutzen das Medium für ihre Geschäftskommunikation[1]. Die etablierten Protokolle decken jedoch nicht die IT-Sicherheitsaspekte der Verfügbarkeit, Integrität und Vertraulichkeit ab. Eine versendete E-Mail erfüllt somit keine IT-Sicherheitseigenschaften zum Schutz vor Einblicken durch Dritte. Das Abfangen und Manipulieren der Nachricht ist möglich, die Verifizierung des Absenders schwierig. Mit dem stark wachsenden Aufkommen täuschend echter Phishing-E-Mails an Endkunden und im B2B-Umfeld erodiert das Vertrauen in diesen Kommunikationsweg zunehmend. 81 Prozent der Unternehmen sind lt. BVDW in Deutschland bereits jetzt der Meinung, dass die Sicherheit der E-Mail-Kommunikation stark verbesserungswürdig ist.

Unterschiede GNUPG/PGP und S/MIME

GNUPG/PGP und S/MIME sind untereinander nicht kompatibel. Der Unterschied zwischen beiden Verfahren liegt, neben einem unterschiedlichen Nachrichten-Austauschformat, vor allem in den Schlüsselformaten und den dazugehörenden Vertrauensinstanzen und Hierarchien:

S/MIME setzt auf personenbezogene Zertifikate, die durch Zertifizierungsdienste-Anbieter, sog. Trust-Center, ausgegeben werden. Die Trust-Center bilden die oberste Ebene einer Public-Key-Infrastructure, in dem die Zertifikate streng hierarchisch verifiziert werden. Jedem Zertifikat wird durch eine höhere Instanz die Zugehörigkeit zur Public-Key-Infrastructure (PKI) attestiert. Es gibt drei unterschiedliche Klassen von Zertifikaten. Bei Klasse-1-Zertifikaten wird die Echtheit der E-Mail-Adresse verifiziert

[1] Nutzung und Trends in der E-Mail-Kommunikation deutscher Unternehmen, Januar 2015 (BVDW)

und in die Signatur aufgenommen. Klasse-2-Zertifikate beinhalten neben der E-Mail-Adresse auch den Namen, die Firma oder Organisation des Antragstellers, welche mit dem Personalausweis und dem Handelsregister abgeglichen werden müssen. Bei Klasse-3-Zertifikaten muss der Antragsteller sich persönlich bei einer Zertifizierungsstelle verifizieren lassen. Die Klassen unterscheiden sich nur in der Stärke der Authentizität.

Bei **GNUPG/PGP** wird das Schlüsselpaar (öffentlicher und privater Schlüssel) durch den Nutzer oder das Unternehmen selbst erzeugt, und die öffentlichen Schlüssel werden auf Schlüsselservern hochgeladen, die dann diese Schlüssel in einem international synchronisierten Ring von Key-Servern bereithalten. Der Vertrauensanker wird in diesem Fall nicht durch ein Trust-Center, sondern durch das Web of Trust hergestellt. Das bedeutet, Teilnehmer verifizieren sich gegenseitig die Richtigkeit der Schlüssel. Mit jeder Unterschrift, die ein Schlüssel von anderen Mitarbeitern oder externen Kontaktpartnern erhält, gewinnt der Schlüssel an Glaubwürdigkeit.

Unternehmen mit mehreren Mitarbeitern wird bei intensiverer Nutzung von PGP die Inbetriebnahme, Pflege und Etablierung einer eigenen PKI empfohlen, wo die Schlüsselerzeugung und -verwaltung in der Regel zentral erfolgt. Es ist eine ganze Reihe von Produkten erhältlich, mit denen ein Unternehmen oder eine Unternehmensgruppe eine eigene PKI realisieren kann. Dies bringt einen hohen Grad an Vertrauenswürdigkeit mit sich, da Zertifikate von der eigenen Organisation und deren Mitarbeiter/innen ausgestellt, geprüft und gepflegt werden.

Verschlüsselung mit GNUPG/PGP und S/MIME

Obwohl Signatur- und Verschlüsselungslösungen für E-Mails vorhanden sind, werden diese bislang nicht flächendeckend eingesetzt. Der Grund: Um eine E-Mail verschlüsselt zu versenden, ist die Einbindung zusätzlicher Software nötig. In den letzten Jahren haben sich dabei GNUPG/PGP (Pretty Good Privacy) und S/MIME (Secure / Multipurpose Internet Mail Extensions) als Standard durchgesetzt. PGP und v.a. die kostenfreie GNUPG-Variante wird in der Praxis häufiger von kleinen Unternehmen (i.d.R. für dedizierte Kommunikationskontakte) eingesetzt, während größere Unternehmen verstärkt auf S/MIME setzen.

Bei beiden Verfahren wird die Nachricht durch den Sender der E-Mail, mithilfe des öffentlichen Schlüssels des Nachrichten-Empfängers, verschlüsselt. Dieser kann die empfangene Nachricht, mithilfe seines privaten Schlüssels, wieder entschlüsseln. Sollte der private Schlüssel oder das Passwort verloren gehen, können die E-Mails nicht mehr entschlüsselt werden und sind folglich nicht mehr in einem lesbaren Zustand. Hierbei kommt es beim Ausscheiden eines Mitarbeiters immer wieder zu Problemen, da in diesem Fall kein Zugriff auf die verschlüsselten E-Mails mehr besteht. Daher sollte für solche Fälle eine entsprechende Regelung in den Richtlinien definiert werden.

Abb. 1: Ende-zu-Ende verschlüsselter E-Mailversand

Quelle: if[is]/Goldmedia 2018

Einrichtung und Betrieb von GNUPG/PGP und S/MIME auf stationären und mobilen Endgeräten

Die erste Hürde beim Einsatz verschlüsselter E-Mail-Kommunikation ist die Auswahl einer Vertrauensinfrastruktur und der damit verbundene Erwerb von Lizenzen sowie das durch Ablauf der Gültigkeit bedingte Lizenzmanagement. Zusätzlich stellen v.a. die über Open-Source verfügbaren Plug-Ins, welche bestehende Mailprogramme um komplexe Funktionen für die E-Mail-Verschlüsselung erweitern, gerade bei einer nur sporadischen Anwendung der Verschlüsselung die Nutzer vor Bedienungshürden. Für Unternehmen gibt es hierfür kostenpflichtige Software-Plug-Ins, welche sich der unfreundlichen Benutzerführung bei der Implementierung der Plug-Ins, dem Upload von Schlüsseln oder dem Management von Zertifikaten angenommen haben.

Das Lesen und Verschicken verschlüsselter E-Mails sollte dabei nicht nur stationären PCs oder Laptops vorbehalten sein, sondern auch auf mobilen Endgeräten wie Smartphones und Tablets ermöglicht werden. Erst ab diesem Zeitpunkt ist eine durchgängig verschlüsselte Kommunikation mithilfe der E-Mail möglich. Die fehlende Integrationsmöglichkeit für GNUPG/PGP in die nativen Mailclients der Hersteller erschweren die Umsetzung für diesen Standard enorm. Für mobile Endgeräte ist es wesentlich komfortabler E-Mails, mithilfe von S/MIME zu verschlüsseln. Diverse proprietäre Applikationen ermöglichen zwar das Empfangen und Versenden von PGP-verschlüsselten E-Mails auf mobilen Geräten, die Benutzerfreundlichkeit leidet jedoch stark darunter und stellt das mobile Device Management vor neue Herausforderungen. Der Verlust des Gerätes hängt zwangsweise mit dem möglichen Verlust der Schlüssel und der möglichen Kompromittierung der Nachrichten zusammen.

Tab. 1: Möglichkeiten zur mobilen E-Mail-Verschlüsselung nach Verschlüsselungsstandard

Mobile E-Mail Verschlüsselung	iOS	Android
… mit GNUPG/PGP	✗	✓*
… mit S/MIME	✓	✓*

**=über Drittanbieter-Plugins/Apps möglich*
Quelle: if[is]/Goldmedia 2018

Erwägungen für die Nutzung von E-Mail-Gateways

Unternehmen, die mehrere Verschlüsselungsstandards bedienen müssen, eine lokale Installation von Plug-Ins inkl. Schlüsseln und Lizenzen auf jedem Rechner vermeiden wollen und auch keine verschlüsselte Speicherung der E-Mails bis auf die Ebene des einzelnen Mitarbeiterpostfachs wünschen, sollten für die Verschlüsselung E-Mail-Gateways einrichten.

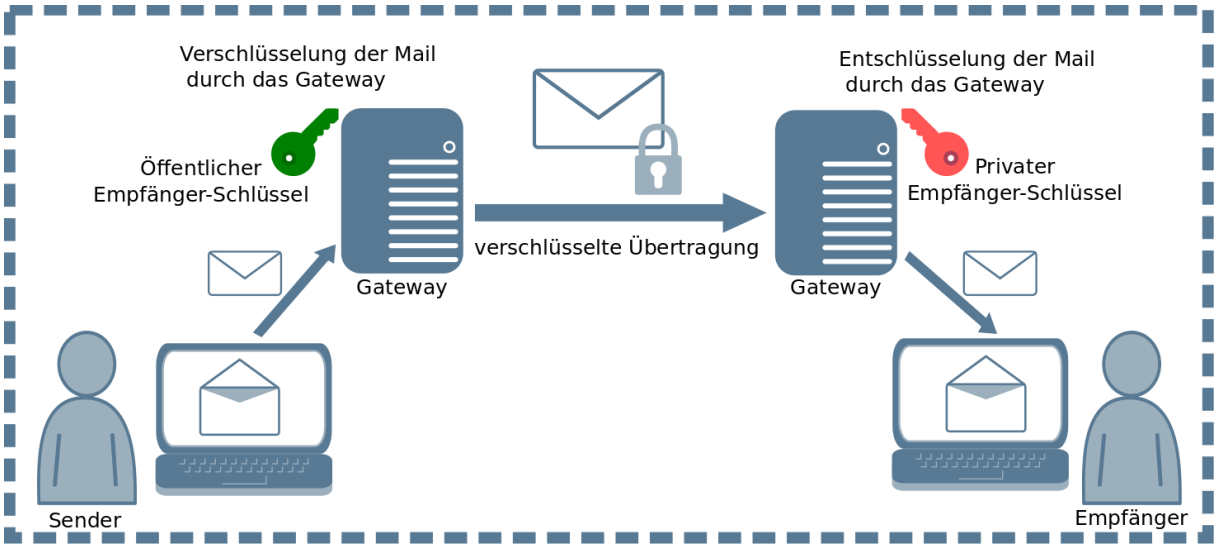
Gateway-Lösungen werden insbesondere dann relevant, wenn die Unternehmen in der B2B-Kommunikation oder ggf. auch bei der B2C-Kommunikation standardmäßig verschlüsseln und hier bereits entsprechende Netzwerkeffekte bei den Kommunikationspartnern erzielen können.

E-Mail-Gateways verschlüsseln alle E-Mails gemäß einer zu definierenden Policy. Diese legt fest, unter welchen Umständen E-Mails wie verschlüsselt werden (GNUPG/PGP oder S/MIME). Die E-Mails verlassen und erreichen dann das Unternehmensnetzwerk mit Inhalteverschlüsselung, können jedoch im E-Mail-Postfach des einzelnen Mitarbeiters im Klartext gespeichert werden. Die Speicherung der E-Mails als Klartext in den Postfächern der Mitarbeiter wird sowohl aus Revisions- als auch aus Praktikabilitätsgründen vielfach bevorzugt. E-Mails sind bei einer Ende-zu-Ende-Verschlüsselung im Postfach nicht mehr durchsuchbar. Bei Verlust des Passworts sind die E-Mails auch nicht mehr lesbar. Außerdem können wichtige Überprüfungen, wie Virenscans oder „Data Loss Prevention“ (Schutz gegen den Abfluss von Daten), nicht durchgeführt werden, da diese nur unverschlüsselte E-Mails prüfen können.

E-Mail-Gateways eignen sich insbesondere, wenn die verschlüsselte E-Mail-Kommunikation über mehrere heterogene Clients stattfindet. Die zentrale Ver- und Entschlüsselung bringt selten Kompatibilitätsprobleme mit sich. Der Einsatz von Verschlüsselungsgateways kann auf diesem Wege mangelndem Bewusstsein/Compliance auf Anwenderebene entgegenwirken.

E-Mail-Gateways ermöglichen keine Ende-zu-Ende verschlüsselte Kommunikation, sichern jedoch, unabhängig von dem mobilen Betriebssystem des Endgerätes, die Nachrichten zusätzlich ohne Zutun des Nutzers ab.

Abb. 2: Verschlüsselter E-Mailversand zwischen zwei Gateways



Quelle: if[is]/Goldmedia 2018

De-Mail – eine elektronische Alternative zum Brief

Das Projekt De-Mail ist ein webbasiertes Kommunikationsmittel für einen rechtlich verbindlichen und sicheren Austausch von elektronischen Daten für Behörden, Unternehmen und Privatanwender. Der Benutzer kann sich zwischen mehreren Anbietern (GMX, Telekom uvm.) entscheiden. Die Akkreditierung der Anbieter erfolgt durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) gemäß § 21 des De-Mail-Gesetzes. Alle drei Jahre muss die Akkreditierung wiederholt werden. Für die Verbindlichkeit wird neben einer Nutzerregistrierung ein Identitätsverfahren durchgeführt. Dieses dient der Verifizierung der Identität. Auf diese Weise wird die Authentizität der Kommunikationspartner sichergestellt.

Benutzer können das Sicherheitsniveau ihres Logins auf der Webplattform des Anbieters zusätzlich mit einer Mehr-Faktor-Authentisierung erhöhen. Die Nachricht ist auf dem Transportweg vom Absender bis zum Anbieter und vom Anbieter bis zum Empfänger mithilfe von SSL/TLS und HTTPS verschlüsselt. Beim Anbieter liegen die Nachrichten für eine kurze Zeit unverschlüsselt vor. Diese Vorsichtsmaßnahme dient der Prüfung auf Schadsoftware. Zusätzlich kann eine elektronisch signierte Versand-, Eingangs- und Absenderbestätigung angefordert sowie die Versandart „Persönlich“ ausgewählt werden. Dies ist jedoch nur dann im vollen Umfang möglich, wenn Absender und Empfänger ein höheres Authentisierungsniveau eingerichtet haben. Eine optionale Ende-zu-Ende-Verschlüsselung auf Basis von PGP kann durch zusätzliche Software für den Browser realisiert werden. Die privaten Schlüssel liegen ausschließlich bei den Kommunikationspartnern.

De-Mail ist nicht als Ersatz für die reguläre E-Mail gedacht, sondern als elektronische Alternative zum regulären Briefverkehr. Der Einsatz von De-Mail sollte in Betracht gezogen werden, wenn die Verbindlichkeit der elektronischen Nachrichten vorrangig ist. Es sollte auch beachtet werden, dass das Versenden von Nachrichten gebührenpflichtig ist, die Anbieter i.d.R. aber ein kostenfreies Kontingent bereitstellen.

Tab. 2: Übersicht über mögliche E-Mail-Verschlüsselungslösungen

Lösung	Beschreibung
S/MIME	Der Secure/ Multipurpose Internet Mail Extensions Standard ist eine von zwei Möglichkeiten, E-Mails zu signieren und zu verschlüsseln. Den Sicherheitsanker bildet ein personen- bzw. organisationsbezogenes, ausgestelltes Zertifikat, in dem die Schlüsselpaare des Nutzers enthalten sind. Abhängig davon, wer das Zertifikat ausgestellt hat, welche Identitätsprüfungen stattgefunden haben und wie lange das Zertifikat gültig ist, steigt das Sicherheitsniveau und das damit verbundene Vertrauen.
GNUPG/PGP	Bei Pretty Good Privacy wird für jeden Anwender ein öffentlicher und ein geheim zu haltender Schlüssel erzeugt. Das Hoch- und Herunterladen der öffentlichen Schlüssel auf Schlüsselserver ist für den Austausch und die Kommunikation, zumindest einmalig, nötig. Das Web of Trust stellt einen Vertrauensanker dar, indem andere Teilnehmer die Echtheit eines Schlüssels bestätigen können.
Gateway-Lösungen	Eine Hard- oder Software-Gateway-Lösung ist die einfachste Möglichkeit, E-Mail-Verschlüsselung zu etablieren. E-Mails werden nach definierten Regeln automatisch verschlüsselt. Dies geschieht erst ab dem Zeitpunkt, an dem sie das Gateway passieren. Sollte zu diesem Zeitpunkt kein gültiger Schlüssel des Empfängers vorliegen oder angefordert werden können, kann die E-Mail bzw. der Inhalt alternativ als passwortgeschützte PDF oder ZIP-Container verschlüsselt werden. Eine Ende-zu-Ende-Verschlüsselung findet nicht statt. Für ein Gateway fallen teilweise Anschaffungskosten/Implementierungskosten, in jedem Fall aber Lizenzgebühren i.d.R. abhängig von der Zahl der Nutzer im Unternehmen an. Die Regeln bzgl. der Verschlüsselung werden auf dem Gateway definiert. Auch die Schlüsselinformationen der Anwender werden hier hinterlegt. Der Benutzer muss sein E-Mail-Kommunikationsverhalten i.d.R. nicht weiter anpassen.
De-Mail	Steht die Verbindlichkeit einer E-Mail im Vordergrund, kann auf die kostenpflichtige Nutzung eines Anbieters von De-Mail zurückgegriffen werden. Absender und Empfänger müssen für die Nutzerregistrierung beim Anbieter eine Identifikationsprüfung mit amtlichen Dokumenten (Ausweis) durchlaufen. Versand und Empfang einer De-Mail-Nachricht ist rechtlich verbindlich. Der Versand einer Nachricht über De-Mail ist auf dem Transportweg zum Anbieter verschlüsselt. Optional kann auch eine Ende-zu-Ende-Verschlüsselung ergänzt werden.
Manuelle Datei-Verschlüsselung	Wenn keine Infrastruktur für den verschlüsselten E-Mail-Versand aufgebaut ist, können unterschiedliche, formatspezifische Maßnahmen ergriffen werden, um die an die E-Mail angehängten Dateien vor der Einsicht von Dritten zu schützen. Die Übermittlung des Passworts, auf einem anderen Weg als mit der Versendung einer E-Mail, ist bei der manuellen Dateiverschlüsselung eine Herausforderung.

Quelle: if[is]/Goldmedia 2018

Tab. 3: E-Mail-Verschlüsselungstechnologien: Vor-/Nachteile und Skalierungsmöglichkeiten

Lösung	Vorteile	Nachteile	Skalierbarkeit
Gateway	▪ hoher Nutzerkomfort ▪ Policy-konforme Verschlüsselung ▪ kein geändertes Bedienerverhalten ▪ Unterstützung verschiedener Standards ▪ zentrale Schlüsselverwaltung ▪ Malware-Prüfung vor Zustellung der Mails ▪ revisionssicher ▪ Data-Loss-Prevention	▪ hohe Anschaffungskosten ▪ begrenzte Kapazitäten ▪ keine Ende-zu-Ende-Verschlüsselung ▪ hoher Konfigurationsaufwand ▪ hoher Aufwand bei der Erstellung einer Policy	▪ sehr gute Skalierbarkeit ▪ Einsatz geeignet für mittlere und große Unternehmen
GNUPG/PGP	▪ Open Source ▪ kostenfrei ▪ Ende-zu-Ende-Verschlüsselung	▪ komplexes Verfahren ▪ veränderte User-Experience ▪ Web of Trust als Sicherheitsanker ▪ verschlüsselt gespeicherte E-Mails sind nicht mehr durchsuchbar ▪ Verlust des privaten Schlüssels oder Passworts führt zum Verlust der verschlüsselten E-Mails	▪ gute Skalierbarkeit ▪ Einsatz möglich in allen Unternehmen jeder Größe
S/MIME	▪ Ende-zu-Ende-Verschlüsselung ▪ einfache Verwendung ▪ kein Schlüsselmanagement durch den Nutzer	▪ Identitätsüberprüfung zur Steigerung des Vertrauens ▪ Achtsamkeit nötig ▪ veränderte User Experience ▪ Verlust des privaten Schlüssels oder Passworts führt zum Verlust der verschlüsselten E-Mails	▪ gute Skalierbarkeit ▪ Einsatz möglich in allen Unternehmensgrößen
De-Mail	▪ hoher Nutzerkomfort ▪ Transportverschlüsselung ▪ optionale Ende-zu-Ende Verschlüsselung ▪ Verbindlichkeit der E-Mail ist gesetzlich gewährleistet ▪ Nutzerregistrierung erfordert eine Identitätsprüfung ▪ mehrere Anbieter vorhanden	▪ kostenpflichtig ▪ Postfach muss regelmäßig eingesehen werden ▪ lange Anmeldezeiten zur Prüfung der Identität des Antragstellers ▪ Empfänger muss ebenfalls bei De-Mail registriert sein ▪ geringe Verbreitung ▪ inkompatibel mit anderen E-Mail-Diensten	▪ Einsatz für jede Unternehmensgröße geeignet
Manuelle Dateiverschlüsselung	▪ Datei bleibt nach dem Herunterladen geschützt, E-Mail dient nur als Transport ▪ Keine Infrastrukturerweiterung notwendig	▪ Inhalt der Mail bleibt unverschlüsselt ▪ Sicherheit ist abhängig vom Format und der Software ▪ Passwortstärke legt Sicherheitsniveau fest ▪ händische Ver- und Entschlüsselung der Dokumente ▪ benötigt verschlüsselten Kommunikationskanal für den Schlüsselaustausch	▪ Skalierung schlecht bei vielen Dokumenten

Quelle: if[is]/Goldmedia 2018

Zur besseren Ermittlung des individuellen Schutzbedarfes Ihres Unternehmens beantworten Sie bitte zunächst folgende Leitfragen für sich:

- *Soll Verschlüsselung obligatorisch oder nur bei Bedarf eingesetzt werden?*

➔ Ein Gateway verschlüsselt stets mit S/MIME oder GNUPG/PGP.

- *Sollen alle Angestellten verschlüsselt kommunizieren können?*

➔ PGP und S/MIME benötigen eine Nutzer-Einführung. Ein Gateway hingegen funktioniert im Hintergrund automatisch.

- *Soll die externe E-Mail-Kommunikation verschlüsselt werden?*

➔ Externe Kommunikationspartner benötigen ebenfalls GNUPG/PGP oder S/MIME für eine vollständig vertrauenswürdige Kommunikation.

- *Soll unternehmensintern verschlüsselt kommuniziert werden?*

➔ GNUPG/PGP und S/MIME eignen sich auch für einen unternehmensinternen Einsatz.

- *Müssen Angestellte verschlüsselte Nachrichten auch auf mobilen Endgeräten lesen können?*

➔ Die Schlüssel- und Zertifikatsverteilung auf mobilen Geräten ist mit zusätzlichem Aufwand verbunden.

- *Ist eigenes Personal für Instandhaltung und Support der Verschlüsselungslösung vorhanden?*

➔ Die Anzahl der Geräte und der zentralen Konfigurationsmöglichkeiten sollte im Vorhinein analysiert werden.

Die folgende Tabelle gewährt einen Überblick, wie sich die verfügbaren Lösungen in den verschiedenen Anwendungsszenarien unterscheiden.

Tab. 4: Vergleich möglicher E-Mail-Verschlüsselungslösungen

Verschlüsselung…	Datei-verschlüsselung*	GNUPG/PGP	Gateway	S/MIME
… obligatorisch	✗	✗	✓	✗
… für alle Angestellten	✓	✓	✓	✓
…für externe Kommunikation	✗	✓*	✓	✓*
… auch unternehmensintern	✓	✓	✗	✓
… auch für mobile Geräte verfügbar	(✓)	✗	✓	✓
Personal vorhanden und interner Support möglich	(✓)	✗	✓	✓
Summe (Anzahl der Haken)	*4*	*3*	*5*	*5*

Quelle: if[is]/Goldmedia 2018

** = Kommunikationspartner benötigt Software, Infrastruktur und/oder Zertifikate, () = Formats-Kompatibilität vorausgesetzt*

Die folgende Tabelle stellt dar, welche E-Mail-Verschlüsselungslösungen für welchen Schutzbedarf und welche Unternehmensgröße geeignet sind. Die Lösungen sind nach Wirkungsklassen[2] für unterschiedliche IT-Systeme eingestuft.

[2] IT-Sicherheitsstrategie für Deutschland, 09.03.2015 (Teletrust.de)

In der **Wirkungsklasse 1** befinden sich Verschlüsselungslösungen für IT-Systeme eines Unternehmens oder einer Organisation, die zwar eine positive Relevanz haben, denen jedoch keine existenzielle Bedeutung zukommt.

In der **Wirkungsklasse 2** werden die Verschlüsselungslösungen geführt, die die absolut relevanten IT-Systeme einer Organisation schützen sollen. Ein Ausfall oder ein erfolgreicher Einbruch in diese Systeme können neben extrem hohen Kosten, auch die Existenz dieses Unternehmens bedrohen.

Die **Wirkungsklasse 3** gilt für Verschlüsselungslösungen, die den Schutz „kritischer Infrastrukturen" gem. IT-Sicherheitsgesetz gewährleisten sollen. Kritische Infrastrukturen dienen der Gewährleistung kritischer Dienstleistungen wie der Energie-, Wasser- oder auch Krankenversorgung. Kritische Infrastrukturen werden von Behörden, kommunalen Unternehmen und Unternehmen der Privatwirtschaft betrieben.

Tab. 5: E-Mail-Verschlüsselung: Matrixcluster zu Schutzbedarf und Unternehmensgröße

Schutzbedarf Wirkungsklasse	Kleinst-Unternehmen bis 10 Mitarbeiter	Unternehmen bis 50 Mitarbeiter	Größere Mittelständler
Niedriger Schutzbedarf Wirkungsklasse 1	Verschlüsselung angehängter Dateien, S/MIME der geprüften Stufe 1 oder GNUPG/PGP	Gateway-Lösung ohne Ende-zu-Ende-Verschlüsselung	Gateway-Lösung ohne Ende-zu-Ende-Verschlüsselung
Ab mittlerem Schutzbedarf (Wirkungsklasse 2) ist eine Ende-zu-Ende-Verschlüsselung empfehlenswert.			
Mittlerer Schutzbedarf Wirkungsklasse 2	S/MIME Zertifikate der geprüften Stufe 2, ggf. GNUPG/PGP mit eigener PKI	S/MIME Zertifikate der geprüften Stufe 2, ggf. GNUPG/PGP mit eigener PKI	S/MIME Zertifikate der geprüften Stufe 3 oder 4, ggf. GNUPG/PGP mit eigener PKI
Hoher Schutzbedarf Wirkungsklasse 3	GNUPG/PGP mit eigener PKI	GNUPG/PGP mit eigener PKI	S/MIME Zertifikate der geprüften Stufe 4 oder GNUPG/PGP mit eigener PKI

Quelle: if[is]/Goldmedia 2018

Fazit

Das Sicherheitsniveau der E-Mail ist nicht ausreichend. Anwender und Unternehmen sind gleichermaßen gefordert und müssen Software, welche es ermöglicht, E-Mails verschlüsselt und signiert abzusenden und zu empfangen, nachträglich installieren. Dies ist jedoch nicht durch eine Ein-Klick-Installation möglich. Bei der Auswahl einer Verschlüsselungslösung sollten Unternehmen neben Einführungskosten auch Schulungskosten berücksichtigen sowie Wartungs- und Support-Verträge prüfen. Proprietäre Software genießt gegenüber Open-Source-Produkten Vorteile. Diese werden jedoch obsolet, wenn die Entwicklung eingestellt wird. Abhängig von der Unternehmensgröße, dem Schutzbedarf der Unternehmenswerte, der IT-Affinität der Mitarbeiter und deren Sensibilität für IT-Sicherheit müssen die geeigneten Systeme ausgewählt werden.

GNUPG/PGP und S/MIME bieten Vor- und Nachteile, weshalb es gilt, diese sorgfältig abzuwägen. Abhängig von der Abstraktionsfähigkeit und IT-Affinität der Mitarbeiter und Mitarbeiterinnen, eignen sich die Verfahren unterschiedlich gut. Gateway-Lösungen sind als alternative Lösung zwar mit zusätzlichen Lizenzkosten verbunden, ermöglichen jedoch eine automatisierte Ver- und Entschlüsselung von E-Mails. Gateways beeinflussen die Handhabung von Mailprogrammen nicht und sind somit besonders benutzerfreundlich, da sie keine hohen Compliance-Anforderungen an die Mitarbeiter stellen.

Die Kombination eines Gateways in Verbindung mit einer internen, PKI-basierten E-Mail-Verschlüsselung bietet eine ausreichend sichere Lösung für die meisten Unternehmensszenarios.

Weiterführende Links zum Thema E-Mail

- **BSI – Sicherer Betrieb von E-Mail-Servern (ISi-Mail-Server)**
  https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-Mail-Server/mail_server_node.html

- **BSI – Sichere Nutzung von E-Mails (ISi-Mail-Client)**
  https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-Mail-Client/mail_client_node.html

- **TeleTrust – E-Mail-Verschlüsselung**
  https://www.teletrust.de/vim/e-mail-verschluesselung

- **Informationsbroschüre von DATEV und Deutschland sicher im Netz e.V.**
  https://www.teletrust.de/vim/verschluesselung-datev

- **Initiative Mittelstand verschlüsselt**
  https://www.e-mail-verschluesselung.de/

- **E-Mail Verschlüsselung mit GPG**
  https://github.com/behrmann/tutorials_de/blob/master/GNUPG/PGP-Mail-Krypto.md

- **Teletrust Anbieterverzeichnis**
  https://www.teletrust.de/anbieterverzeichnis/

- **E-Mail Verschlüsselung mit S/MIME**
  http://t3n.de/news/mails-verschlusseln-eigentlich-482381

1.2 Telefonie – VoIP löst ISDN nach und nach ab

Nach wie vor gehört das Telefonieren zu den Standards der Bürokommunikation. Rund 39 Minuten beträgt die durchschnittliche tägliche Nutzungsdauer von Telefondiensten laut dem Media Activity Guide 2016. Die klassischen ISDN-Telefone wurden mittlerweile weitestgehend durch IP-basierte Sprachkommunikation (Voice-over-IP; VoIP) abgelöst. Mittlerweile ist laut Bundesnetzagentur mehr als die Hälfte der Telefonanschlüsse in Deutschland auf VoIP umgestellt. Ein Angreifer, der in der Lage ist, die Leitung zwischen zwei Gesprächspartnern abzuhören, besitzt nach Zusammensetzen der übertragenen IP-Pakete das Gespräch. Durch die IP-Telefonie kommen, im Vergleich zu leitungsvermittelnden Telefondiensten, Schwachstellen hinzu, die sich auf der Übertagungsebene der VoIP-Protokolle befinden.

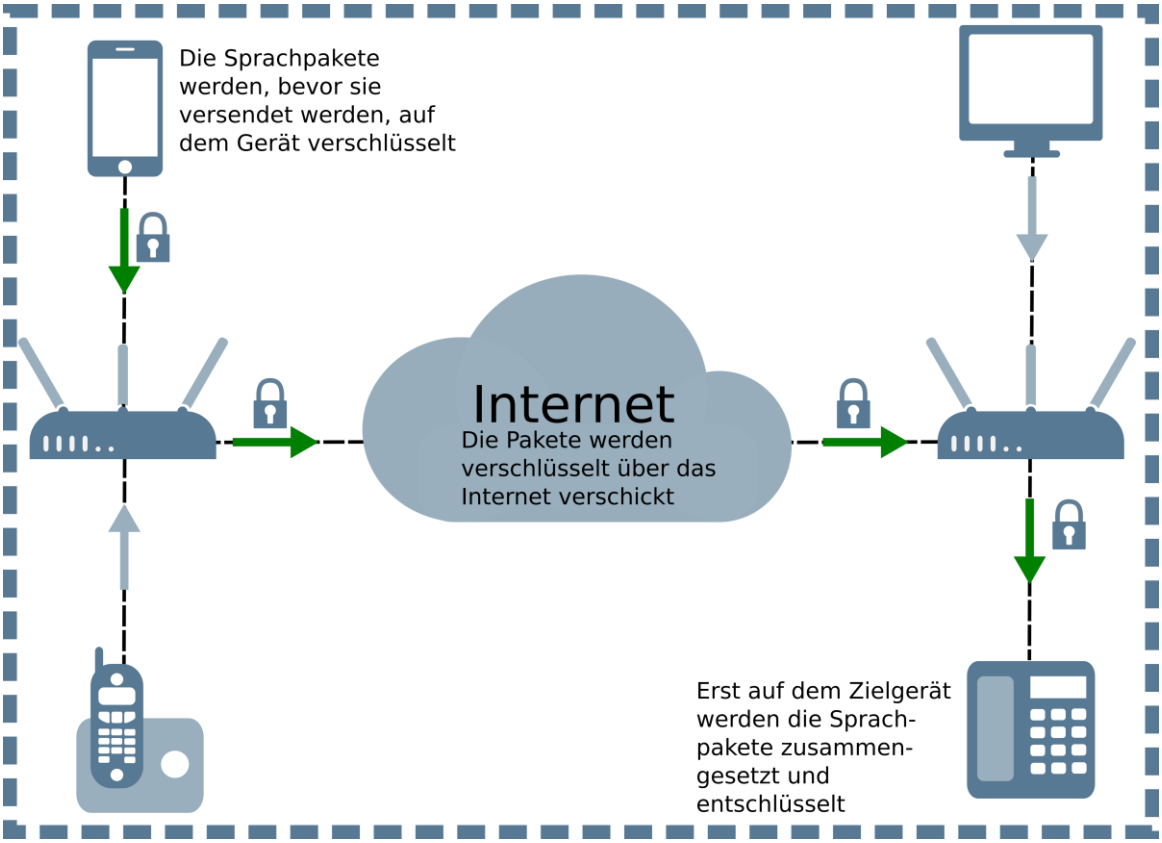
Verschlüsselung der Sprachpakete

Viele VoIP-Lösungen bieten standardmäßig ein Protokoll an, welches die Sprachdaten vor der Übertragung verschlüsselt. Das Secure Real-Time Transport Protocol (SRTP) nutzt dafür eine AES-Verschlüsselung (Advanced Encryption Standard) und liefert zusätzlich Möglichkeiten zur Authentifizierung des Absenders und zur Überprüfung der Integrität der Nachricht.

Sicherer Schlüsselaustausch

Neben der Verschlüsselung der Sprachdateien sollten auch die Signalisierungsdaten verschlüsselt übertragen werden. Hierfür bietet sich z.B. der Einsatz von TLS an. Um einen direkten Schlüsselaustausch zwischen zwei VoIP-Endgeräten zu ermöglichen und dadurch eine vollständige Ende-zu-Ende-Verschlüsselung zu erzielen, kann auf das ZRTP-Protokoll (Kombination aus Diffie-Hellman-Schlüsselaustausch und SRTP) zurückgriffen werden.

Abb. 3: Verschlüsseltes VoIP-Telefonat zwischen zwei Endpunkten



Quelle: if[is]/Goldmedia 2018

Durch die Verwendung geheimer, beim Aufbau der Verbindung ausgehandelter, temporärer Schlüssel sind die Nutzdaten auch vor Missbrauch durch den Betreiber der VoIP-Vermittlungsplattform gesichert. Die Verwendung eines VPN-Gateways bietet die Möglichkeit, sowohl die Sprachdaten als auch die Signalisierungsdaten verschlüsselt zu übertragen, wenn diese das lokale Netzwerk verlassen. Die Gateway-Lösung hilft bei der Vernetzung von Telefonanlagen, die sich an verteilten Standorten befinden.

Sichere Protokolle bei den Endgeräten sind erforderlich

Die Endgeräte (VoIP-Telefone) müssen die Verwendung sicherer Protokolle unterstützen, damit eine flächendeckende, verschlüsselte Kommunikation erfolgen kann. Bei Telefonaten mit nicht IP-basierten Endgeräten hören die Möglichkeiten der Verschlüsselung häufig an der Schnittstelle zum leitungsvermittelnden Netz auf, da nur wenige Telefone eingebaute Schutzmechanismen besitzen. Kommen internetbasierte Kommunikationsdienste zum Einsatz, nutzen diese unter Umständen zwar verschlüsselte Kanäle, die Umsetzung ist aber selten überprüfbar.

Die professionellen VoIP-Produkte am Markt besitzen die Möglichkeit der Verwendung verschlüsselter Protokolle und erlauben es, sowohl die Sprachdaten als auch die Signalisierungsdaten verschlüsselt zu übertragen. Bei der Auswahl und Administration der VoIP-Komponenten sollte auf die Unterstützung von abgesicherten Protokollen auf allen Endgeräten geachtet werden. Die verfügbaren Schutzmechanismen müssen durch die Administratoren konsequent aktiviert werden.

Mit Voranschreiten des Ausbaus der VoIP-Infrastrukturen und konsequenter Ausstattung der Endgeräte mit Verschlüsselungsmöglichkeiten durch die Telefondienstanbieter werden Verschlüsselungsprobleme bei Telefonaten in herkömmliche Telefonnetze zunehmend an Bedeutung verlieren und das Telefonieren allgemein abhörsicherer.

Tab. 6: Lösungen zur Verschlüsselung von internetbasierter Sprachtelefonie

Lösung	Beschreibung
Verschlüsselte VoIP-Transportprotokolle	Die verschlüsselten Medienübertragungsprotokolle liefern eine Möglichkeit zum Echtzeitaustausch von Kommunikationsdaten und verschlüsseln diese vor der Übertragung mithilfe des AES-Verfahrens. Das SRTP-Protokoll ist in allen professionellen VoIP-Diensten integriert.
Verschlüsselte VoIP-Signalisierungsprotokolle	Eine Verschlüsselung der Signalisierungsdaten schützt die Vertraulichkeit und Integrität. Eine sichere Verschlüsselung kann durch den Einsatz von TLS erreicht werden. Eine entsprechende Option steht in den meisten VoIP-Produkten zur Verfügung.
VPN-Gateway	Ein VPN-Gateway verschlüsselt Sprach- und Signalisierungsdaten zwischen entfernten LANs eines Unternehmens. Auch bei Anbindung der eigenen Telefonanlage an das Netz eines Telefonanbieters sollte ein VPN die Verbindung zwischen der internen VoIP-Schnittstelle und der Schnittstelle des Dienstanbieters absichern. Sobald eine Verbindung zu einem Anschluss in einem nicht IP-basierten Telefonnetz aufgebaut wird, endet die verschlüsselte Leitung am Übergang zum klassischen Telefonnetz.
Internetbasierte Kommunikationsdienste	Viele internetbasierte Kommunikationsdienste wie etwas Skype bieten von Haus aus verschlüsselte Kommunikation an. Problematisch ist, dass diese Dienste häufig nicht einsehbare Protokolle verwenden, die eine Überprüfung der Sicherheitsmaßnahmen sowie der Infrastruktur nicht zulassen.

Quelle: if[is]/Goldmedia 2018

Fazit

Der konsequente Einsatz von Protokollen wie SRTP in Verbindung mit einer verschlüsselten Übertragung der Signalisierungsdaten (z.B. mit Hilfe von TLS) bietet einen guten Schutz von Integrität und Vertraulichkeit im Bereich der IP-Telefonie. In besonders kritischen Bereichen bietet sich die Verwendung des ZRTP-Protokolls an, welches eine Ende-zu-Ende-Verschlüsselung der Daten ermöglicht. Betreibt ein Unternehmen mehrere Telefonanlagen in unterschiedlichen Liegenschaften, bietet sich der Einsatz von VPN-Gateways an, um einen verschlüsselten Transport der VoIP-Daten zwischen den einzelnen LANs zu ermöglichen. Bei konsequentem Einsatz von Verschlüsselungslösungen im Bereich VoIP lässt sich eine höhere Abhörsicherheit der Daten erzielen als in klassischen Telefonnetzen, in denen die Nutzerdaten meist ungesichert übertragen werden.

Weiterführende Links zum Thema Telefonie

- **BSI-Leitlinie zur Internet-Sicherheit IP-Telefonie**
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_voip_leitlinie_pdf.pdf?__blob=publicationFile
- **Teletrust Anbieterverzeichnis**
  https://www.teletrust.de/anbieterverzeichnis/
- **BSI-Grundschutzkatalog Umfang der Verschlüsselung von VoIP**
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02374.html

1.3 Messaging – immer überall kommunizieren, aber sicher!

Analog zu der Entwicklung in der Privatkommunikation werden auch Messaging-Dienste immer häufiger im Unternehmensumfeld eingesetzt. Wesentliche Treiber hierbei sind die Verfügbarkeit der Dienste auf nahezu allen Endgeräten und die Integration einer Vielzahl unternehmensrelevanter Funktionalitäten wie Gruppenchats, Video-Conferencing und Video-Präsentationen und der direkte Austausch von Mediendateien. Dies macht die Dienste für den Unternehmenseinsatz attraktiv, und Fragen nach der Sicherheit rücken oftmals in den Hintergrund.

Unterschiedliche Lösungen für Messaging-Dienste

Die Mehrzahl der Chat- und Messaging-Plattformen bieten Business- oder Corporate-Versionen ihres Dienstes an. Ausgewählte Messenger sind auf den Einsatz im Unternehmen bzw. im Rahmen von Projekten zugeschnitten und stellen erweiterte Archivierungs- und Datenschutzfunktionen bereit. Neben einer oftmals kostenfreien Basisversion bieten diese Plattformen für ein- bis zweistellige Monatsgebühren pro Nutzer umfängliche Messaging- und Präsentationsdienste für größere Teilnehmergruppen zur Verfügung. Bei Plattformen wie Slack oder Ryver, deren Fokus klar auf geschlossene Benutzergruppen liegt (Team Communication), ist die Grenze hin zu Groupeware- oder Kollaborationsplattformen fließend.

Art und Ort der Speicherung, die Einbindungsmöglichkeiten in das unternehmenseigene Client- und Mobile-Device-Management sowie die technische Absicherung der Daten (v.a. die Art der Verschlüsselung) unterscheiden sich dabei. Mehrere Messaging-Plattformen bieten mittlerweile an, die Messaging-Plattform direkt auf Unternehmensservern zu hosten (On-Premise-Lösung). Einzelne Chat- oder Messaging-Plattformen können auch als White-Label-Lösung eingekauft und an das Unternehmensdesign angepasst werden. Für die Unternehmen ist es jedoch schwer zu kontrollieren, welcher Dienst tatsächlich ein ausreichendes Maß an Sicherheit bietet.

Verschlüsselung der Nachrichten

Damit übermittelte Daten nicht mitgelesen werden können, empfiehlt sich ein Messenger, der eine Ende-zu-Ende-Verschlüsselung einsetzt. Diese Art der Verschlüsselung verhindert, dass Dritte, etwa der Dienstanbieter selbst, Einblicke in die Nachrichten erhalten. Neben der Ende-zu-Ende-Verschlüsselung der Nachrichten auf Anwendungsebene bieten einige Anbieter eine zusätzliche Transportverschlüsselung an, um die Verbindungsdaten auf dem Weg zum Server abzusichern. Es gilt nur denjenigen Diensten zu vertrauen, die transparent Auskünfte über die eingesetzten Verschlüsselungsverfahren geben und nur als sicher geltende Verschlüsselungslösungen einsetzen.

Unternehmenseigene Messaging-Plattform

Um den Aspekten *Sicherheit* und *Ort der Speicherung* besser Rechnung zu tragen, setzen größere Unternehmen häufig auf vorkonfigurierte Out-of-the-Box-Lösungen. Neben spezialisierten Anbietern sind auch alle größeren Telekommunikationsanbieter im Bereich des Enterprise-Messagings aktiv.

Eigene Messaging-Dienste werden vielfach auf Basis von am Markt verfügbarer Software-Development-Kits (SDKs) und offener Protokollstandards (v.a. IRC und XMPP) entwickelt. Hierbei kann der Messenger stark auf die Bedürfnisse des Unternehmens abgestimmt werden. Mit Aufbau einer eigenen Infrastruktur kann die Übertragung sowie das Speichern der Nachrichten konform der eigenen Policy gestaltet werden. Nachteilig ist jedoch der hohe Kostenaufwand für die Entwicklung und das benötigte Know-how, welches für den Aufbau und den Betrieb der Infrastruktur benötigt wird.

Tab. 7: Technische Lösungen im Bereich Instant Messaging

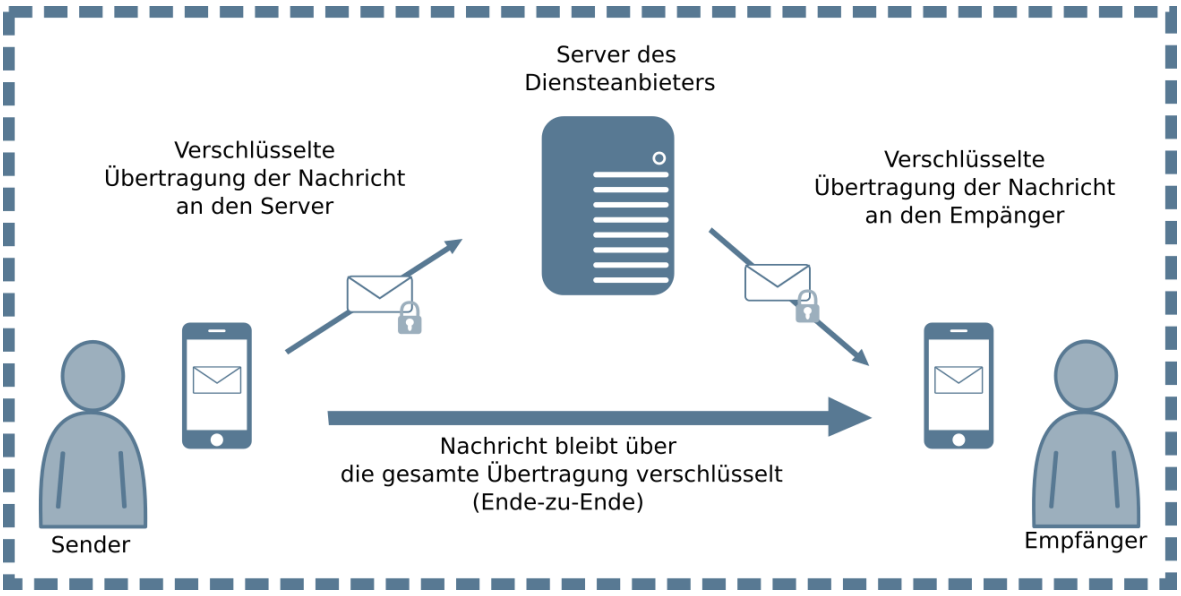
Lösung	Beschreibung
Messaging-Plattform eines Dienstanbieters	Die Clients für die Nutzung von Basis- oder Businessprodukten großer Messaging-Plattformen sind für fast alle Endgeräte/Betriebssysteme erhältlich. Die meist proprietär angebotenen Dienste werden vom Anbieter bereitgestellt und sind häufig nicht mit denen anderer Anbieter kompatibel. In puncto Sicherheit und Verschlüsselung müssen Anwender in die vom Dienstanbieter implementierten Mechanismen vertrauen.
Eigene Messaging-Plattform	Bei der Wahl einer passenden Messanging-Plattform kann es für ein Unternehmen sinnvoll sein, eine eigene Messanging-Plattform aufzubauen und über die eigene Infrastruktur zu verteilen. Für diese Eigenentwicklungen kann auf offene Protokolle, verschiedene Software-Development-Kits und fertige Module für Client- und Serveranwendungen zurückgegriffen werden.

Quelle: if[is]/Goldmedia 2018

Unternehmen sollten ihre Anforderungen an ein sicheres Messaging daher klar definieren. Dadurch wird es möglich, aus der großen Anzahl an Diensten und Protokollen einen passenden Dienst auszuwählen. Potenzielle Dienste können strukturiert sondiert werden, um den für die eigenen Anforderungen passenden zu finden.

Fehlendes Know-how bei der Planung und Umsetzung einer eigenen Messaging-Infrastruktur kann durch den Einsatz externer Experten kompensiert werden. Die Mitarbeiter können durch Schulungen und Fortbildungsmaßnahmen in die Funktionsweise des unternehmensinternen Messaging-Dienstes ausreichend eingeführt und im Rahmen der Policy datenschutzrechtlich sensibilisiert werden, um eine optimale Nutzung zu ermöglichen. Steht den Mitarbeitern ein gut funktionierender Dienst zur Verfügung, der ausschließlich verschlüsselte Kommunikation zulässt, gibt es für die Mitarbeiter wenig Gründe, für die berufliche Nutzung innerhalb des Unternehmens auf andere Messaging-Plattformen auszuweichen.

Abb. 4: Verschlüsselte Übertragung von Sofortnachrichten



Quelle: if[is]/Goldmedia 2018

Problem fehlender Netzwerkeffekte

Der Grund, warum in vielen Unternehmen trotzdem Skype auf Desktops oder WhatsApp auf Firmenhandys genutzt werden darf, sind die fehlenden Netzwerkeffekte beim Einsatz firmenindividueller Lösungen bei der Einbindung externer Kommunikationspartner. Hier bedarf es einer ernsthaften Nutzen-/Risikoabwägung.

Außerhalb firmeninterner Nutzerkreise müssen Dritte für die B2B- oder B2C-Kommunikation explizit zur Nutzung des Firmendienstes eingeladen werden. Zwar funktionieren die meisten Systeme auch rein browserbasiert, für eine komfortable Nutzung ist jedoch die Installation der jeweiligen App empfehlenswert. Die Nutzung zusätzlicher Messaging-Dienste über bereits installierte Clients anderer Messaging-Dienste ist trotz zunehmender Öffnung der Schnittstellen (APIs) untereinander weiterhin eine technische Herausforderung, die nicht auf Anwenderebene gelöst werden kann.

Zudem verleitet die gelernte Nutzung kostenfreier Messenger-Dienste im Privatbereich (v.a. WhatsApp) die Mitarbeiter dazu, ihre geschäftliche Kommunikation über ihre privat genutzten Chat-Dienste fortzuführen. Dies ist insbesondere dann problematisch, wenn eine „Bring-your-own-Device-Policy“ z.B. die Nutzung von Geschäfts-E-Mail-Konten auf privaten Endgeräten ermöglicht, ohne dass ein entsprechendes Mobile-Device-Management zwischen beruflicher und privater Nutzung trennt.

Eine Nutzung von WhatsApp und Co. auf privaten Endgeräten für berufliche Zwecke kann aber auch mit getrennten Firmen- und Privat-Modi nicht verhindert werden. Daher müssen die Mitarbeiter über Leitfäden und Schulungen deutlich darauf hingewiesen werden, auf die berufliche Verwendung der Dienste im Unternehmen zu verzichten.

Tab. 8: Verschlüsselung von Messaging-Diensten: Vor-/Nachteile

Lösung	Vorteile	Nachteile
Messaging-Plattform eines Dienstanbieters	▪ zu betreiben ohne großen Aufwand ▪ kostengünstig (wenige Euro pro Account)	▪ Verschlüsselung möglicherweise nicht überprüfbar ▪ externe Speicherung der Daten ▪ Drittanbieter hat Zugriff auf Metadaten
Eigene Messaging Plattform	▪ Messenger anpassbar an Unternehmensanforderungen ▪ Speicherung der Daten& Metadaten im eigenen Unternehmen ▪ Verschlüsselung konform mit der eigenen Policy	▪ bindet Ressourcen im eigenen IT-Betrieb ▪ hohe Entwicklungskosten ▪ benötigt spezielles Know-how

Quelle: if[is]/Goldmedia 2018

Fazit

Die Sicherheit beim Instant-Messaging hängt stark vom eingesetzten Dienst ab. Wenn Mitarbeiter Messaging-Dienste für die unternehmensinterne Kommunikation nutzen, sollte ein Dienst verwendet werden, der sowohl eine Ende-zu-Ende-Verschlüsselung zwischen den Clients, als auch eine Transportverschlüsselung für die Verbindungsdaten nutzt. Größere Unternehmen, die sicherstellen wollen, dass die Nachrichten das eigene Netzwerk nicht verlassen, sollten den Betrieb einer eigenen Messaging-Plattform in Betracht ziehen. Dies setzt hinreichendes Know-how und ausreichende Ressourcen für den Betrieb der Dienste voraus, bietet gleichzeitig ein hohes Maß an Sicherheit und Datenhoheit.

Weiterführende Links zum Thema Messaging

- **BSI für Bürger Instant Messenger: Tipps (evtl.)**
  https://www.bsi-fuer-buer-ger.de/BSIFB/DE/DigitaleGesellschaft/KommunikationUeberInternet/Messenger/Tipps/tipps_node.html

- **Teletrust Anbieterverzeichnis**
  https://www.teletrust.de/anbieterverzeichnis/

- **Marktplatz IT-Sicherheit-Anbieter für IT-Sicherheit**
  https://www.it-sicherheit.de/anbieter/anbieter_suchen

- **Übersicht über XMPP Server-Software**
  https://de.wikipedia.org/wiki/Liste_von_XMPP-Server-Software

1.4 Kollaborationsplattformen – zusammenarbeiten, von überall

Kollaborationsplattformen bieten ihren Nutzern die Möglichkeit einer engen Zusammenarbeit trotz räumlicher Trennung an. Die Plattformen machen es durch netzbasierten Datenaustausch möglich, Bildschirminhalte zu teilen, Präsentationen zu halten, gemeinsam Dokumente zu lesen, zu bearbeiten und sich dabei auszutauschen. In vielen Unternehmen gehören Kollaborationsplattformen wie WebEx, Citrix, GoToMeeting, Projectplace oder Adobe Connect zu den Standard-Arbeitsanwendungen und sorgen für eine flexible Zusammenarbeit und sinkende Reisekosten. Ausgewählte Anwendungen, wie z.B. Qiata oder Cryptshare, spezialisieren sich auf einzelne Bereiche wie z.B. den Versand oder Empfang von Dateien und kompletten Dateistrukturen.

Auch bei den Kollaborationsplattformen gibt es herstellerabhängige Abweichungen bezüglich der eingesetzten Verschlüsselungslösungen und des Unterschieds zwischen einer Ende-zu-Ende-Verschlüsselung und der reinen Verschlüsselung der Transportwege. Zu den Kollaborationswerkzeugen, die sowohl eine Transport- als auch eine Ende-zu-Ende-Datenverschlüsselung bieten, zählen beispielsweise Cisco WebEx und Citrix GoToMeeting.

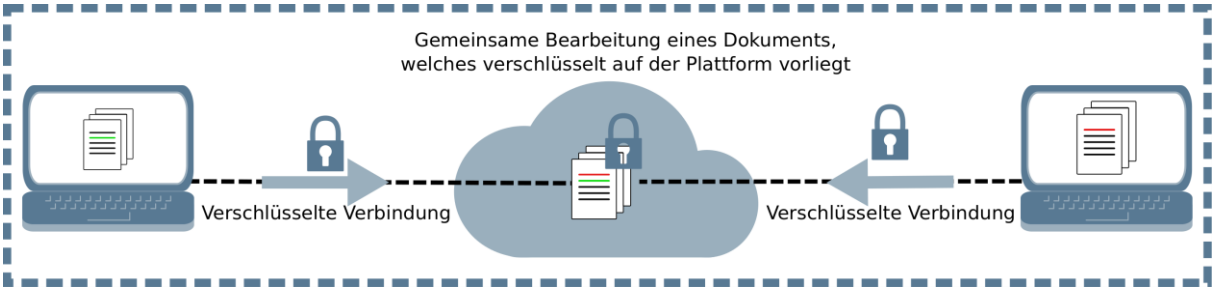
Tab. 9: Technische Lösungen im Bereich Kollaborationsplattformen

Lösung	Beschreibung
Cloudbasierte Kollaborationsplattform	Professionelle Kollaborationsplattformen greifen in der Regel auf Protokolle zurück, die eine Ende-zu-Ende-Verschlüsselung der Daten bedeuten.
On-Premise-Betrieb der Kollaborationsplattform	Viele Anbieter von Kollaborationsplattformen bieten an, die Plattform auf einem Server im eigenen Unternehmen zu betreiben. Diese Konfiguration erhöht das Sicherheitsniveau für das Unternehmen, da die Daten das eigene Unternehmen nicht verlassen.

Quelle: if[is]/Goldmedia 2018

Für die Nutzung einer Kollaborationsplattform benötigen die Nutzer in der Regel eine Client Software, mindestens jedoch einen Browser. Der Austausch der Daten zwischen den Nutzern geschieht i.d.R. über die Plattform des Dienstanbieters. In welchem Maße die Verbindungen dabei verschlüsselt sind, hängt von der ausgewählten Plattform ab. Alternativ zur Nutzung einer Plattform beim Dienstanbieter vor Ort gibt es bei einigen Anbietern die Möglichkeit, eine Plattform auf einem Server im eigenen Unternehmen bereitzustellen, was einen deutlich höheren administrativen Aufwand bedeutet, aber auch die höchste Vertraulichkeit und Datenhoheit bietet.

Abb. 5: Verschlüsselte Kollaborationsplattform



Quelle: if[is]/Goldmedia 2018

Fazit

Bei Kollaborationsplattformen hängt die Sicherheit stark vom eingesetzten Produkt ab. Professionelle Plattformen nutzen in der Regel von Haus aus Protokolle, die eine Ende-zu-Ende-Verschlüsselung unterstützen. Hier muss den Angaben der Dienstanbieter vertraut werden, ansonsten bleibt nur der Betrieb einer eigenen Infrastruktur. Diese bietet die vollständige Kontrolle über eingesetzte Verschlüsselungen und verhindert, dass Daten das eigene Unternehmen verlassen.

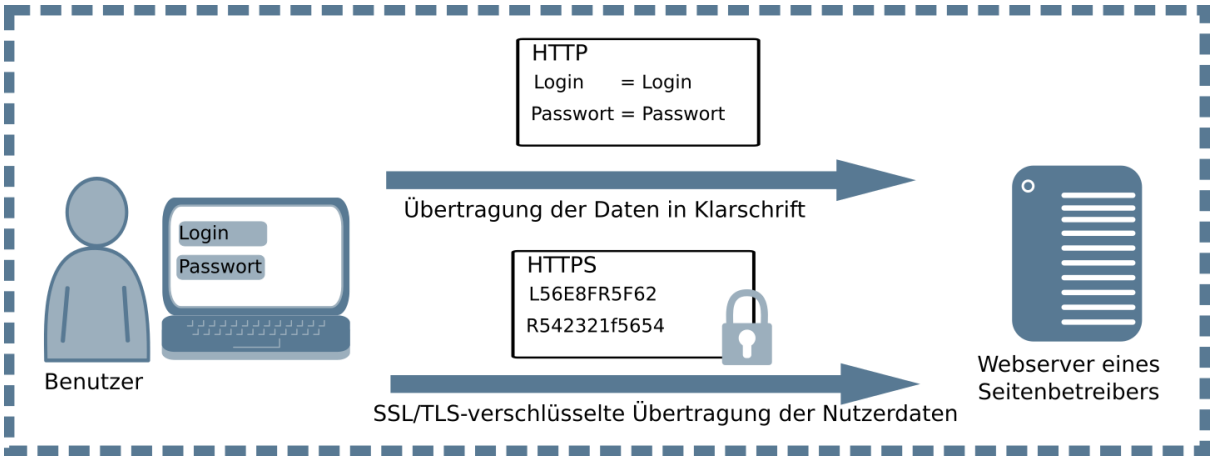
Weiterführende Links zu Kollaborationsplattformen

- **Teletrust Anbieterverzeichnis**
  https://www.teletrust.de/anbieterverzeichnis/
- **Etherpad – Open Source Online Editor**
  http://etherpad.org/

1.5 SSL/TLS Webseitenverschlüsselung mithilfe von HTTPS

Wenn es um die verschlüsselte Datenübertragung geht, kommt heutzutage oft das Transport Layer Security Protocol (TLS) zum Einsatz. TLS ist eine Weiterentwicklung des mittlerweile veralteten Secure Sockets Layer Protocol (SSL). Das TLS-Protokoll arbeitet auf der Transportschicht des OSI-Modells und ist sehr effizient beim Transport von Datenpaketen. Mithilfe von SSL/TLS-Sicherheitszertifikaten kann die eindeutige Identität des Dienstes oder Servers bestimmt werden. Darüber hinaus wird verhindert, dass Nachrichten manipuliert werden. Um eine TLS-Verschlüsselung verwenden zu können, braucht es auf der übergeordneten Applikationsschicht ein entsprechendes Protokoll. Das wohl bekannteste Beispiel ist die Anwendung des HTTPS-Protokolls, welches auf TLS basiert und, im Gegensatz zu HTTP, einen verschlüsselten Datenaustausch im World Wide Web ermöglicht. Bereits mehr als die Hälfte aller Webseiten im Internet werden mittlerweile über HTTPS[3] abgerufen.

Abb. 6: Transportverschlüsselung bei der Datenübertragung von Webseiten



Quelle: if[is]/Goldmedia 2018

Die folgenden Fragen sollen dabei helfen, den Schutzbedarf für die Unternehmenswebseite zu überprüfen:

- Enthält Ihr Webangebot Eingabefelder (Kontaktformular, Login-Felder) für persönliche Daten?
- Betreiben Sie einen Onlineshop?

  Wenn Sie bereits Verschlüsselung auf Ihrer Homepage einsetzen, gibt es jemand, der regelmäßig die Gültigkeit überprüft?

Damit die eigene Webseite über HTTPS erreichbar ist, bedarf es eines von einer vertrauenswürdigen Certificate Authority (CA) ausgestellten SSL/TLS-Sicherheitszertifikats. Die Sicherheitszertifikate besitzen eine beschränkte Gültigkeitsdauer von zwei Jahren. Wird eine Webseite mit ungültigen Zertifikaten aufgerufen, zeigen aktuelle Browser entsprechende Warnmeldungen und Hinweise an. Einzelne Browser wie z.B. der Firefox gehen noch einen Schritt weiter und warnen im Allgemeinen vor nicht verschlüsselten Verbindungen, auf denen nach Passwörtern gefragt wird. Eine solche Warnung schreckt potenzielle Seitenbesucher ab. Um Warnmeldungen und andere Hinweise für die eigene Website zu

[3] HTTPS-Verschlüsselung im Web erreicht erstmals 50 Prozent, 16.10.2016 (Heise)

vermeiden, sollte der Webmaster Sicherheitszertifikate verwenden und regelmäßig aktualisieren. Aufmerksamkeit sollte das Zertifikat auch erhalten, wenn es von externen Dienstleistern gepflegt wird. So ist es u.a. wichtig, dass jede verfügbare Website verschlüsselt ist und auch nur verschlüsselt erreichbar ist.

Fazit

Das TLS-Protokoll kann variabel eingesetzt werden, um Daten auf dem Transportweg zu schützen. Immer mehr Webseiten sind über HTTPS-Verbindungen erreichbar und ermöglichen den Besuchern so einen verschlüsselten Datenaustausch mit den Servern. Gleichzeitig warn mehrere Browseranbieter bereits explizit vor dem Besuch unverschlüsselter Webseiten, was potenzielle Besucher abschrecken könnte. Unternehmen signalisieren mit dem Einsatz von SSL/TLS-Sicherheitszertifikaten auf ihren Internetseiten Authentizität und Vertrauenswürdigkeit beim Besucher.

Weiterführende Links zu SSL/TLS-Webseitenverschlüsselung mithilfe von HTTPS

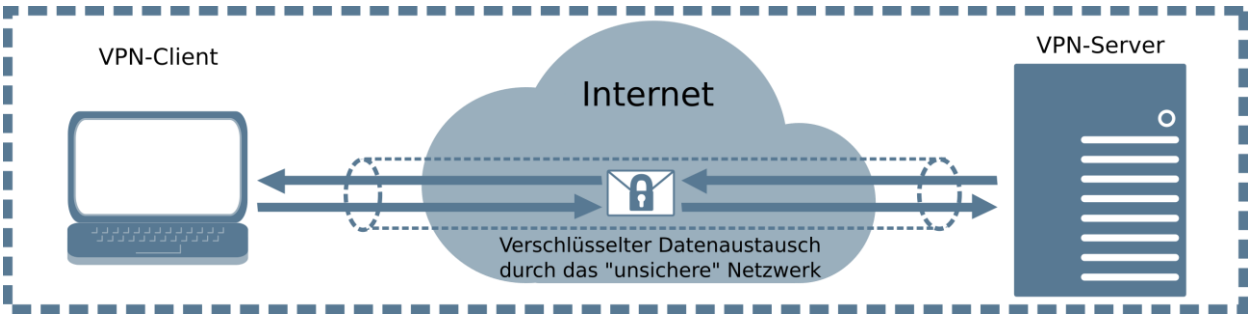
- **Empfehlung im Unternehmen TLS/SSL Best Practice**
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_012.pdf?__blob=publicationFile&v=4
- **Empfehlung: Internet-Dienstleister: Bereitstellung von Webangeboten**
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_041.pdf?__blob=publicationFile&v=3
- **Digitaler Mittelstand SSL-Verschlüsselung: Wie Ihre Seite sicherer wird**
  https://digitaler-mittelstand.de/technologie/ratgeber/ssl-verschluesselung-wie-ihre-seite-sicherer-wird-28475
- **Let's Encrypt**
  https://letsencrypt.org/getting-started/
- **Teletrust Anbieterverzeichnis**
  https://www.teletrust.de/anbieterverzeichnis/

1.6 Virtual Private Network – der private Tunnel ins Unternehmen

Jedes dritte Unternehmen bietet seinen Mitarbeitern die Möglichkeit, im Homeoffice zu arbeiten. Damit auch am Heimarbeitsplatz alle benötigten Dienste wie der E-Mail-Client oder die Netzlaufwerke verfügbar sind, wird der Arbeitscomputer über das Internet mit dem Firmennetzwerk verbunden.

Diese Verbindung wird in der Regel durch ein virtuelles privates Netzwerk (VPN) realisiert, welches die Infrastruktur des Internets nutzt, um eine direkte Verbindung zwischen dem Arbeitscomputer und dem Netzwerk des Unternehmens aufzubauen. Weitere Einsatzszenarien von VPN sind die Verbindung der (WAN-)Netze unterschiedlicher Unternehmensniederlassungen zu einem unternehmensweiten VPN oder die Verbindung zwischen verschiedenen Unternehmen.

Abb. 7: Funktionsweise eines verschlüsselten VPN-Tunnels



Quelle: if[is]/Goldmedia 2018

Ein VPN-Tunnel bietet zusätzliche Möglichkeiten zur Absicherung der Verbindung an. Der Einsatz von Passwörtern, Schlüsseln oder Zertifikaten erlaubt eine gegenseitige Authentifizierung der VPN-Endpunkte. Um die Sicherheit weiter zu steigern, kann auf eine Zweifaktor-Authentifizierung bestanden werden. Gebräuchlich ist der Einsatz eines Sicherheitstokens oder einer Smartcard in Verbindung mit einer Passphrase. Die meisten VPN-Protokolle wie z.B. IPSec bieten darüber hinaus die Möglichkeit, den Datenverkehr zwischen beiden Endpunkten zu verschlüsseln, und schützen dadurch sowohl die Integrität als auch die Vertraulichkeit der Daten.

Softwarebasierte VPN-Lösungen

Die Erstellung einer VPN-Verbindung geschieht auf der Softwareebene. Grundsätzlich ist auf beiden über das VPN zu verbindenden Endgeräten eine VPN-Software installiert, die für die richtige Adressierung sorgt. Installiert werden kann eine VPN-Serversoftware auf Standard-Hardware und auf virtuellen Umgebungen.

Hardwarebasierte VPN-Lösungen

Viele Hersteller bieten Hardwareprodukte an, die für den Betrieb als VPN-Gateway optimiert sind. Sie werden mit gehärteten Betriebssystem betrieben, unterstützen verschiedene VPN-Protokolle und können als Einwahlknoten für das unternehmensinterne Netzwerk dienen. An diesem können sich die VPN-Clients einwählen.

Tab. 10: Überblick über mögliche VPN-Szenarien

Lösung	Beschreibung
Site-to-Site-VPN	Sicherung der Verbindung zwischen zwei physisch getrennten Netzwerken, etwa bei der Anbindung einer Zweigstelle an das Netzwerk des Unternehmens
End-to-End-VPN	Verbindung zweier Server oder eines Clients und eines Servers
End-to-Site-VPN	Verbindung eines Endgeräts mit einem Gateway, um Zugang auf das dahinterliegende Netzwerk zu erlangen. Typischer Anwendungsfall ist die Verbindung eines externen Rechners (z.B. Homeoffice) mit dem Firmennetzwerk.

Quelle: if[is]/Goldmedia 2018

Die Anforderungen beim Aufbau einer Verbindung zum unternehmensinternen Netzwerk müssen hoch sein. Die Administration der VPN-Zugänge ist mit Aufwänden verbunden und fordert darüber hinaus das benötigte Know-how im Unternehmen. Die regelmäßige Überprüfung von Updates gehört zur Routine, sobald es Externen erlaubt wird, eine Verbindung zum Unternehmensnetzwerk aufbauen zu dürfen. Für die Verbindung einzelner weniger PCs mit dem Unternehmen ist die Anschaffung eines VPN-Gateways gründlich zu bewerten.

Tab. 11: Abgrenzung von Software-VPN zu Gateway-Lösungen

Lösung	Beschreibung
Software-VPN	Grundsätzlich ist für den Aufbau einer VPN-Verbindung eine Software notwendig, die auf beiden Endpunkten des Tunnels installiert werden muss. Die benötigte Software ist für alle gängigen Betriebssysteme verfügbar. Anbieter wie OpenVPN bieten ihre Software als Open Source Produkte an und bieten damit vor allem kleinen Unternehmen eine einfache Möglichkeit, einen VPN-Zugang bereitzustellen. Bei der Auswahl der Clients sollte berücksichtigt werden, dass einige Lösungen Administratorenrechte auf den Geräten voraussetzen, um eine Verbindung aufbauen zu können. Auch hier gibt es alternative Lösungen, z.B. den Securepoint OpenVPN Client.
Gateway-VPN	Häufigste Form der Gateway-Lösungen sind Hardware-VPN-Gateways. Es handelt sich um Geräte, die für die Ausführung einer VPN-Software spezialisiert sind. Die Geräte laufen mit gehärteten Betriebssystemen, und die Hardware der Gateways ist für die Ausführung der optionalen Verschlüsselungen optimiert. Es werden auch Produkte vertrieben, in denen die VPN-Software als Zusatzfunktion einer anderen IT-Sicherheitskomponente bereitgestellt wird, etwa als Teil einer Firewall-Komponente.

Quelle: if[is]/Goldmedia 2018

Bei der Auswahl eines Gateways sollte auf den möglichen Datendurchsatz geachtet werden. Je nach Anzahl der zu erwartenden Verbindungen sollte ein auf das Unternehmen abgestimmtes Gateway angeschafft werden.

Tab. 12: Vergleich vorgestellter VPN-Konfigurationen

Lösung	Vorteile	Nachteile	Skalierbarkeit
Software-VPN	▪ Geringe bzw. keine Anschaffungskosten (Open-Source)	▪ Administrationsaufwand kann höher sein ▪ VPN teilt sich die Hardware mit anderen Prozessen	▪ gute Skalierbarkeit ▪ Einsatz geeignet für kleinere Unternehmen
Gateway-VPN	▪ Höhere Stabilität ▪ Höhere Leistung / Durchsatz ▪ Hardware auf den Einsatz als VPN abgestimmt	▪ Höhere Anschaffungskosten	▪ gute Skalierbarkeit ▪ erst ab einer gewissen Anzahl von VPN-Verbindungen wirtschaftlich

Quelle: if[is]/Goldmedia 2018

Für große und mittelständische Unternehmen, die einen hohen Anteil an Heimarbeitsplätzen und/ oder Außendienstmitarbeitern haben, ist ein Hardware-VPN-Gateway eine mögliche Lösung. Für kleine und mittelständische Unternehmen, die nur wenige VPN-Anbindungen benötigen, kann eine Softwarelösung in Betracht gezogen werden. Bei vorhandenen Virtualisierungsmöglichkeiten kann die VPN-Software auch auf einer virtuellen Maschine installiert werden. Bei der Anbindung von Zweigstellen an das Unternehmensnetz ist ein leistungsstarkes VPN-Gateway nötig.

Fazit

Bei der Auswahl einer geeigneten VPN-Lösung spielt die Anzahl der benötigten Verbindungen eine wesentliche Rolle, um eine angemessene, leistungsstarke Komponente auszuwählen. Auch die Überlegung, ob eine Hardware- oder Software-Lösung zum Einsatz kommen soll, ist neben den Anschaffungskosten vorrangig von der benötigten Leistung abhängig. Zu erwähnen bleibt noch, dass sowohl bei der Verwendung eines Software-VPN, als auch beim Einsatz eines VPN-Gateways hohe Kosten für die Einrichtung und Administration der VPN-Komponente anfallen können.

Weiterführende Links zum Thema Virtual Private Network

- **ISI Leitfaden BSI**
  https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-VPN/vpn_node.html
- **BSI Grundschutzbaustein VPN**
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b04/b04004.html
- **Teletrust Anbieterverzeichnis**
  https://www.teletrust.de/anbieterverzeichnis/
- **Aufbau von Virtual Private Networks (VPN) und Integration in Sicherheitsgateways**
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/vpn_pdf.pdf?__blob=publicationFile

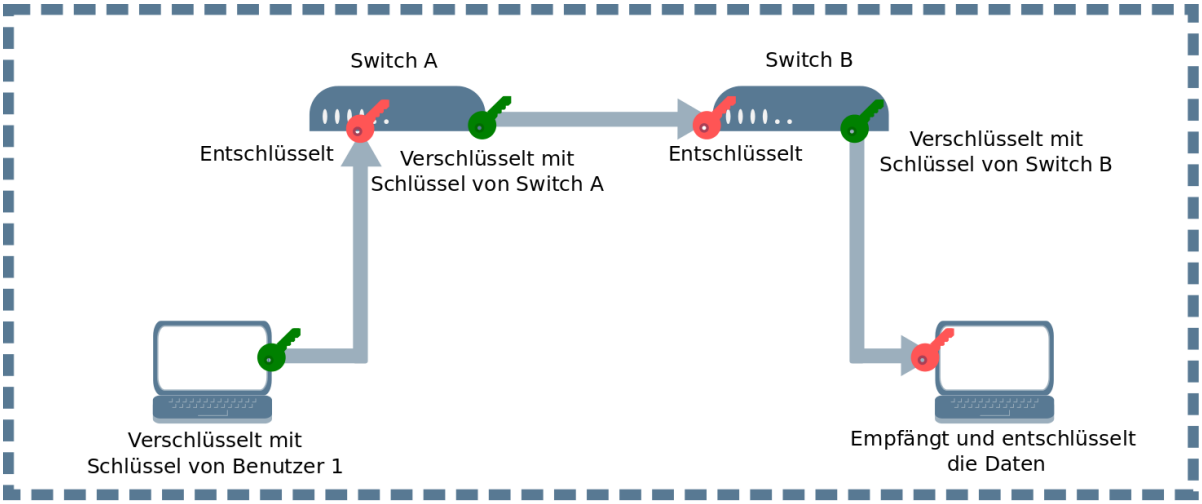
1.7 LAN Transportverschlüsselung mit Netzwerkzugangskontrollen

Die Netzwerkanschlüsse eines Unternehmens bieten Zugang zu allen, sich im Netzwerk befindenden Systemen und Daten. Zugang zum Unternehmensnetzwerk kann über physische Netzwerkzugänge oder optional auch über Funknetzwerke erlangt werden. Wenn sie ungeschützt sind, können nicht nur die eigenen Mitarbeiter auf die wichtigen Informationen des Unternehmens zugreifen, sondern auch jeder Besucher oder externe Dienstleister, der sich mit einer freien Netzwerkdose verbindet.

In Zeiten von Netzlaufwerken und zentralisierten Datenspeichern, in denen viele der zu speichernden Daten über das Netzwerk gesendet werden, können so große Teile des Datenbestands der Firma eingesehen werden. Weitere Gefahr geht vom Einschleusen von Schadsoftware aus.

Offene WLAN-Netzwerke bieten, im Vergleich zu nicht geschützten Netzwerken, noch größere Angriffsmöglichkeiten. Jeder, der sich in Reichweite eines WLAN-Netzwerks befindet, kann sich mit diesem verbinden.

Abb. 8: Funktionsweise der MACsec-Verschlüsselung



Quelle: if[is]/Goldmedia 2018

Der Einsatz von einfachen MAC-Filtern

Das Verwenden sogenannter MAC-Filter, die nur Geräten mit eingetragener MAC-Adresse den Zugang zum Netzwerk gewähren, verhindert die Teilnahme unbefugter Geräte am Netzwerkverkehr. Die MAC-Filter erfüllen ihren Zweck, solange sich niemand vorsätzlich unbefugten Zugang zum Netzwerk verschaffen will. Für Kriminelle ist es vergleichsweise einfach, die eigene Geräteadresse zu verschleiern und dem Netzwerk eine andere, autorisierte MAC-Adresse vorzugaukeln.

Netzzugangskontrollen durch MACsec

Einen zuverlässigen, sich ebenfalls auf der Netzwerkzugriffsschicht befindlichen Schutz bietet ein unter dem Namen MACsec bekanntes Verfahren. Das im IEEE 802.1AE beschriebene Verfahren ermöglicht eine Verschlüsselung des Netzwerkverkehrs und schließt nicht berechtigte Geräte von der Kommunikation des Netzes aus. Die Geräte sind aufgrund fehlender Schlüssel nicht in der Lage, Daten richtig zu ver- und entschlüsseln. Die Verwendung von MACsec ist nur möglich, wenn alle Komponenten im Netzwerk MACsec unterstützen. Bei bestehender Infrastruktur, in der die Unterstützung nicht gegeben ist, ist eine Umstellung auf MACsec mit erheblichem Aufwand verbunden.

Netzzugangskontrollen für Funknetzwerke

Für die Zugangskontrolle in WLAN-Netzen sollte der Verschlüsselungsstandard WPA2 eingesetzt werden. Nicht mehr verwendet werden sollte hingegen der alte WPA- sowie der WEP-Standard, da diese mittlerweile als unsicher gelten. Die Kommunikation wird bei WPA2 mit dem symmetrischen Verschlüsselungsverfahren AES verschlüsselt. So kann kein Dritter die Daten auslesen.

Tab. 13: Übersicht der Netzzugangslösungen: Vor-/Nachteile

Lösung	Vorteile	Nachteile
MACsec	▪ Zertifikatgestützte Authentisierung aller Netzteilnehmer ▪ Sicherer Schlüsselaustausch ▪ Verschlüsselte Kommunikation	▪ Benötigt entsprechende Hardware (Router, Switche) ▪ Hohe Kosten für die Anschaffung
MAC-Filter	▪ Keine zusätzlichen Kosten ▪ Einfache Netzzugangskontrollen	▪ Unverschlüsselte Kommunikation ▪ MAC-Adresse kann gefälscht werden
WPA2	▪ Nur Zugang für autorisierte Netzteilnehmer ▪ Authentifizierung von Teilnehmern ▪ Mit AES verschlüsselte Kommunikation	▪ Beim kurzen Passwort anfällig für Wörterbuchangriffe

Quelle: if[is]/Goldmedia 2018

Fazit

Die Verschlüsselung von kabellosen Netzwerken in einer Firma ist zwingend notwendig, damit sich fremde Geräte keinen Zugang zum Unternehmensnetzwerk verschaffen können. Eine ausreichend sichere Verschlüsselung bietet der WPA2-Standard. Auch das übrige Netzwerk sollte gegen unbefugte Kommunikationsteilnehmer abgesichert werden. Die Verwendung von MAC-Filtern kann helfen, ungewollte Geräte von der Kommunikation auszuschließen. Einem Angreifer, der gezielt in das Netzwerk eindringen will, stehen aber Möglichkeiten offen, die Filterung zu umgehen. Einen besseren Schutz bietet das MACsec-Protokoll. Dieses setzt allerdings voraus, dass alle Geräte im Netzwerk das Protokoll unterstützen, was bei einer bestehenden Infrastruktur zu hohen Kosten führen kann.

Weiterführende Links zu LAN Transportverschlüsselung mit Netzwerkzugangskontrollen

- **ISI Leitfaden BSI**
  https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-VPN/vpn_node.html
- **BSI Überblickspapier Netzzugangskontrolle BSI**
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_Netzzugangskontrolle.pdf?__blob=publicationFile
- **Teletrust Anbieterverzeichnis**
  https://www.teletrust.de/anbieterverzeichnis/
- **BSI Sicherer Anschluss von Laptops an lokale Netze**
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05122.html
- **WLAN und LAN sichern mit IEEE 802.1X und Radius**
  https://www.heise.de/ct/artikel/WLAN-und-LAN-sichern-mit-IEEE-802-1X-und-Radius-979513.html

2 Daten sicher ablegen – dank Verschlüsselung

Der Verlust und Diebstahl von Geräten ist das am häufigsten vorkommende Delikt im Bereich der Cyberkriminalität[4]. Bei Industriespionage zählt in 17 Prozent der Fälle der Diebstahl von IT- oder Telekommunikationsgeräten zu den wesentlichen Ursachen (lt. Corporate Trust).

Der Diebstahl von Geräten ist so verbreitet, da gerade der Diebstahl mobiler Geräte leicht ist und es dem Angreifer auf diese Weise sehr einfach gemacht wird, in den Besitz sensibler Daten zu gelangen. Ob die Verschlüsselung einzelner Dateien, die Aufbewahrung von Dateien in verschlüsselten Containern oder die Verschlüsselung des gesamten Systems - das Verschlüsseln von Daten hilft, die Integrität und die Vertraulichkeit der Daten sicherzustellen.

Tab. 14: Zentrale Teilbereiche der Verschlüsselung gespeicherter Daten

Lösung	Beschreibung
Verschlüsselung aus Anwendungsprogrammen	Möglichkeiten, die erstellten Dateien verschlüsselt zu speichern, bieten alle gängigen Anwendungsprogramme (Office, Acrobat etc.). Entsprechend der Version kommen aktuellste Algorithmen zum Einsatz. Dabei wird nur die gespeicherte Datei selbst vor Einblicken Dritter geschützt, mögliche vom System erzeugte temporäre Dateien bleiben unverschlüsselt. Aktuelle Versionen der Anwendungen erreichen mit einem hinreichend langen Passwort ein gutes Sicherheitslevel. Eine weitere Möglichkeit, Dateien aus einem Anwendungsprogramm heraus zu verschlüsseln, bieten Kompressionsprogramme, die eine Verschlüsselung mehrerer Dateien und deren Metadaten zulassen.
Verschlüsselungsfunktion des Betriebssystems	Microsoft-Betriebssysteme bieten mit EFS (Encrypting File System) integriert ein Filesystem an mit der Möglichkeit, einzelne Dateien oder Verzeichnisse zu verschlüsseln. Bei der EFS-Verschlüsselung einer Datei erzeugt das System einen zufälligen Schlüssel. Der File Encryption Key (FEK) wird dann mit einem öffentlichen Benutzerschlüssel verschlüsselt und zusammen mit der Datei abgelegt. Entschlüsselt wird mit dem privaten Schlüssel berechtigter Personen.
Dedizierte Verschlüsselungsprogramme	Es gibt eine Vielzahl an Werkzeugen, die bei der Verschlüsselung von Dateien eingesetzt werden kann. Häufig bieten Anwendungen, die für die vollständige Verschlüsselung von Datenträgern eingesetzt werden können, auch die Funktion an, einzelne Dateien oder Verzeichnisse zu verschlüsseln. Viele der Verschlüsselungslösungen bieten auch die Funktion der Container-Verschlüsselung an, bei der eine Datei als „Container“ verwendet wird, um Daten verschlüsselt abzulegen. Diese Datei muss, um Zugriff auf den Inhalt zu erlangen, ähnlich einem virtuellen Laufwerk eingelesen und mittels Passphrase geöffnet werden.

Quelle: if[is]/Goldmedia 2018

[4] Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter, 2016 (Bitkom e.V.)

2.1 Geräte- und Datenträgerverschlüsselung – der Datenschutz

Eine Komplettverschlüsselung von Computersystemen und Massenspeichern kann die darauf befindlichen Daten effektiv vor dem Zugriff Dritter schützen. Allein ein Benutzerpasswort stellt weder eine Verschlüsselung, noch einen ausreichenden Schutz der Daten dar. Spätestens wenn jemand direkten Zugriff auf die Festplatte eines Geräts hat, ist der Schutz obsolet. Jeder, der Zugriff hat, kann die auf dem Gerät enthaltenden Daten lesen, manipulieren und ggf. kopieren.

Mobile Device Management

Der Einsatz eines zentralen Mobile Device Managements (MDM) in Verbindung mit umfangreichen Sicherheitsrichtlinien kann die Einrichtung bzw. die Konfiguration von mobilen Endgeräten bei einer größeren Mitarbeiterzahl erleichtern und die Datensicherheit steigern. Die Gerätefunktionen der mobilen Endgeräte können zentral gesteuert werden. Die systemeigene Geräteverschlüsselung für den Speicher des mobilen Endgerätes kann vorausgesetzt und bei der Konfiguration bereits aktiviert werden, bevor ein Mitarbeiter ein unverschlüsseltes Endgerät benutzen kann. Zusätzlich kann beim Verlust oder Diebstahl des Endgerätes die Fernlöschung des Gerätespeichers veranlasst werden.

Geräteverschlüsselung

Geräteverschlüsselung bedeutet, dass alle Datenträger, die Bestandteil eines Computersystems sind, Informationen nur in verschlüsselter Form speichern. Zur Entschlüsselung wird ein geheimer Schlüssel in Form einer Passphrase oder einer anderen Art der Authentifizierung (z.B. Smart-Card oder Token) benötigt. Vor jedem Start des Betriebssystems muss der geheime Schlüssel eingegeben werden, um den Zugriff zu den gespeicherten Daten zu erhalten.

Datenträgerverschlüsselung

Bei Massenspeichern wie USB-Sticks oder externen Festplatten ist die potenzielle Gefahr durch direktes Auslesen der Daten besonders hoch. Eine Komplettverschlüsselung des Massenspeichers hilft, die darauf befindlichen Daten vor dem Einblick Dritter zu schützen.

Tab. 15: Verschlüsselungsmöglichkeiten für Geräte und Datenträger

Lösung	Beschreibung
Softwarebasierte Verschlüsselung	Eine weitverbreitete, rein softwarebasierte Möglichkeit zur Verschlüsselung von Laufwerken, Ordnern und Dateien ist die Open-Source-Software VeraCrypt, die den Advanced Encryption Standard (AES) zur Verschlüsselung einsetzt. Die aktuellen Pro- und Enterprise-Versionen von Windows und alle aktuellen MacOS-Versionen halten ebenfalls die Möglichkeit bereit, eine kostenlose Verschlüsselung aller Datenträger zu realisieren. Bitlocker (für Windows mit RSA-Verschlüsselung) kann zusätzlich auf spezielle, in den jeweiligen PCs verbaute Hardware-Chips zurückgreifen (siehe Kapitel 2.1). Für den unternehmensweiten Einsatz von Verschlüsselungslösungen bietet sich eine zentral verwaltete Verschlüsselungslösung an. So können bspw. verlorengegangene Passwörter von einem Administrator zurückgesetzt werden. Solche Verwaltungstools werden sowohl für die Betriebssystem-Lösungen angeboten, aber auch als eigenständige Lösungen verkauft.
Hardwarebasierte Verschlüsselung	Voraussetzung sind spezielle, mit Hardware-Krypto-Controllern (sog. Trusted Platform Modules/TPM) ausgestattete Festplatten oder USB-Sticks. TPMs beinhalten eigene Prozessoren mit Keyword-Generatoren. Sie sind entsprechend teurer als Standard-Datenträger, ermöglichen aber eine schnellere Ver- und Entschlüsselung, da die Rechenoperationen durch die auf ihnen befindlichen Prozessoren möglichst hardware-nah ausgeführt werden. Die Platten speichern ausschließlich verschlüsselte Daten, und die Verschlüsselung der Festplatten lässt sich nicht ausschalten. Das bedeutet, man muss immer erst einen Code eingeben, bevor man das Laufwerk nutzen kann. Die selbst verschlüsselnden Geräte bieten die Möglichkeit, das Geheimnis zu erneuern. In dem Falle sind alle mit dem alten Geheimnis verschlüsselten Daten unbrauchbar. Das funktioniert bei einigen der Geräte sogar automatisch, wenn diese an „fremde“ Hardware angeschlossen wird. Ein Gerät mit TPM, speziell angepasstem Betriebssystem und entsprechender Software bildet zusammen eine Trusted Computing Plattform (TC-Plattform). Eine solche „vertrauenswürdige Plattform“ kann nicht mehr entgegen den Interessen des Herstellers genutzt werden, sofern dieser Beschränkungen festgelegt hat. Ein klassisches Beispiel ist die Bitlocker-Verschlüsselung in Windows-Betriebssystemen.

Quelle: if[is]/Goldmedia 2018

Zur Verschlüsselung der Datenträger werden asymmetrische Verschlüsselungsalgorithmen verwendet. Die Sicherheit der Verschlüsselung kann durch die Kombination mehrerer Schlüssel gesteigert werden. So können etwa eine Passphrase und ein Token kombiniert werden, welche beide vor jedem Start des Betriebssystems eingegeben werden müssen, um die Entschlüsselung der Daten zu ermöglichen.

Kopieren, manipulieren und das Löschen von Dateien ist möglich, sobald das Passwort richtig ist. Die Daten, die sich auf den Datenträgern des Geräts befinden, sind nur geschützt, solange die Passphrase nicht korrekt eingegeben wurde. Im laufenden Betrieb sind die Daten zugänglich und von jedermann einsehbar, kopierbar oder veränderbar. Jeder, der die Passphrase besitzt, hat auch die Möglichkeit, die Daten zu entschlüsseln.

Hierarchisierung des Geheimschutzes ist aufwendig

Die Anfertigung diverser verschlüsselter Partitionen kann, je nach Geheimhaltungsstufe der Informationen, sinnvoll sein. Dies geht jedoch mit einem hohen Verwaltungs- und Organisationsaufwand einher. Während eine komplett verschlüsselte Festplatte nach der Eingabe des Passworts wie gewohnt zur Verfügung steht, braucht es beim Einsatz mehrerer verschlüsselter Partitionen auch mehrere sichere Passwörter, um einen verstärkten Schutz zu erreichen.

Die kostenlosen, frei verfügbaren Verschlüsselungsprogramme sind oft nur in englischer Sprache verfügbar und lassen sich selten zentral verwalten. Handbücher sind entweder nicht vorhanden oder für Laien kaum verständlich. Die zwingende Auswahl von Sicherheitsfeatures, deren Bedeutung oft nur Spezialisten geläufig ist, wirft weitere Fragen bei der Bedienung auf. Die Möglichkeiten zur Deaktivierung der Verschlüsselung sowie Notfallroutinen, z.B. beim Vergessen eines Passwortes, sind, wenn sie implementiert sind, oft versteckt. Bei größeren Unternehmen, die über eine zentrale IT-Administration verfügen, sind diese Hürden zum großen Teil beseitigt. Kleine Unternehmen hingegen müssen auf externe Dienstleister zurückgreifen, wenn sie nicht über nötiges Know-how verfügen.

Tab. 16: Vor- und Nachteile software- und hardwarebasierter Verschlüsselungstechnologien

Lösung	Vorteile	Nachteile
Software-basierte Verschlüsselung	▪ In vielen Betriebssystemen integriert ▪ Open Source-Anwendungen vorhanden ▪ Zentralisierte Verwaltung möglich	▪ Obwohl i.d.R. Teil der Standardausstattung, ist das Feature im Auslieferungszustand deaktiviert. ▪ Performanceeinbußen in der Nutzung ▪ Benötigt (z.B. rudimentäres) Verschlüsselungs- und Recovery-Konzept
Hardware-basierte Verschlüsselung	▪ Schnelle Ver- und Entschlüsselung	▪ Höherer Preis für einzelne Datenträger ▪ Benötigt (z.B. rudimentäres) Verschlüsselungs- und Recovery-Konzept

Quelle: if[is]/Goldmedia 2018

Die folgenden Fragen sollen Ihnen eine Orientierung geben, wann eine Datenträgerverschlüsselung in Betracht gezogen werden sollte, und Ihnen die Möglichkeit zu einer Selbsteinschätzung geben:

- *Gibt es in Ihrem Unternehmen mobile Endgeräte?*

➔ Falls ja, sollten alle Zugänge und Daten von allen Zugangspunkten abgesichert und verschlüsselt sein.

- *Stellt der Verlust eines mobilen Endgerätes ein Risiko für Ihr Unternehmen dar?*

➔ Falls ja, sollte der potenzielle Schaden so gering wie möglich gehalten werden. Alle Geräte sollten mit starken Methoden zur Authentifizierung ausgestattet und verwendet werden.

- *Gibt es ein zentrales Mobile-Device-Management?*

➔ Falls ja, sollte beachtet werden, dass die Verwaltung von mobilen Geräten einen hohen Administrationsaufwand mit sich bringt, der mit Verwaltungssoftware reduziert werden kann.

Fazit

Die Frage, ob alle Datenträger innerhalb einer Organisation verschlüsselt werden sollten, ist abhängig von den individuellen Schutzbedürfnissen der Geräte. Grundsätzlich sollten alle mobilen Geräte und mobilen Datenträger verschlüsselt werden, da ein sehr hohes Risiko besteht, dass mobile Datenträger verloren gehen, gestohlen oder unbemerkt kopiert werden.

Stationäre Systeme, die gegen Diebstahl durch weitere physische Barrieren geschützt sind, sollten zumindest dann verschlüsselt werden, wenn auf ihnen Informationen gespeichert sind, die einen Unternehmenswert darstellen. Dies können sowohl Daten aus der Forschung und Entwicklung als auch Kundendaten sein.

Weiterführende Links zu Geräte- und Datenträgerverschlüsselung

- **Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme**
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04029.html?nn=6610630
- **Einsatz von Datenträgerverschlüsselung**
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04433.html
- **Selbstverschlüsselnde Festplatten**
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04435.html
- **Teletrust Anbieterverzeichnis**
  https://www.teletrust.de/anbieterverzeichnis/
- **Einsatz von BitLocker Drive Encryption**
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04337.html

2.2 Dateiverschlüsselung – sicher vor Einblicken Dritter

Eine Alternative zur Datenträgerverschlüsselung stellt die gezielte Verschlüsselung einzelner Dateien, Ordner und Verzeichnisse dar. So können besonders sensible Dateien selektiv und ressourcenschonend geschützt werden. Die Verschlüsselung schützt die Vertraulichkeit der Daten auch im laufenden Betrieb eines Computersystems. Der Zugriff auf die Daten ist erst nach erfolgreicher Eingabe eines Passworts möglich. So kann auch bei paralleler Nutzung eines Systems die Berechtigung zur Einsicht der Daten geregelt werden. Auch für den sicheren Transport von Daten via E-Mail oder Massenspeicher ist die Verschlüsselung einzelner Daten eine einfache, aber effektive Lösung.

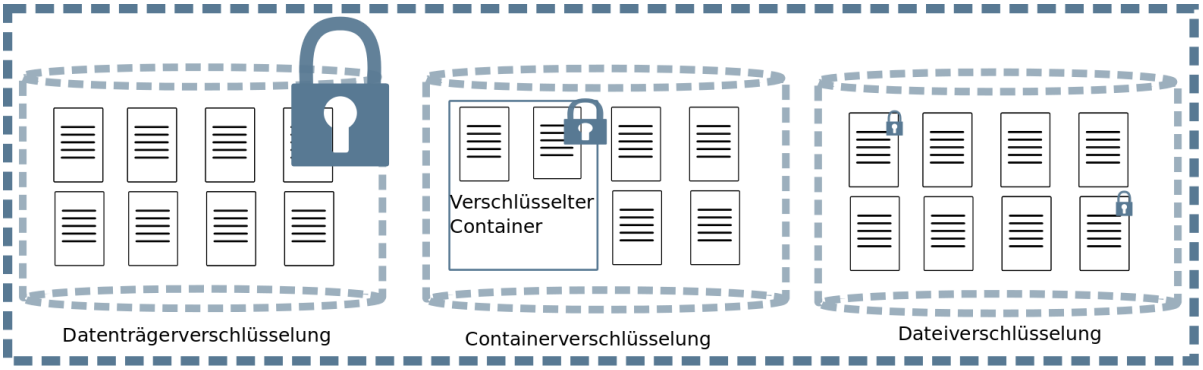
Erhöhter Aufwand beim Schlüsselmanagement

Möglicher Schwachpunkt bei der Verschlüsselung auf Anwendungsebene ist ein langfristiges Schlüsselmanagement für die Schlüssel der einzelnen Dateien. Der Nutzer sollte für jede Datei ein Passwort angeben. Nutzt er für jedes Dokument ein separates Passwort, ist es schwer, den Überblick zu behalten. Bei Verlust eines Passworts ist die verschlüsselte Datei nicht mehr zu entschlüsseln. Verschärft wird dieses Problem durch die Tatsache, dass die Mitarbeiter vieler Unternehmen alleine für das Management ihrer Schlüssel sorgen müssen und die Passwortverwaltung dadurch nur unzureichend geregelt ist.

Abhilfe schafft ein sicherer Passwortmanager. Zu einem weiteren Problem könnte der Schlüsselaustausch bei der Nutzung der Daten durch mehrere Nutzer werden, wenn kein verschlüsselter Kommunikationskanal vorhanden ist. Sobald Mitarbeiter selbstständig anfangen, Dateien auf ihren Geräten zu verschlüsseln, kann es passieren, dass Unternehmensdaten für andere Mitarbeiter oder Administratoren nicht mehr zugänglich sind und dem Unternehmen bei Ausscheiden des Mitarbeiters verloren gehen. Es ist deshalb davon abzuraten, solche Lösungen im Unternehmen zu kommunizieren, wenn kein Konzept zur zentralen Schlüsselverwaltung vorliegt.

Ebenfalls problematisch sind fehlende Compliance-Vorgaben und die dadurch entstehende Selbstverwaltung der Nutzer. Diese müssen dann selbst entscheiden, wann Dateien verschlüsselt werden sollen und wann nicht. Dies führt im Zweifel dazu, dass schutzbedürftige Daten unverschlüsselt bleiben. Selbst mit bestehendem Verschlüsselungskonzept braucht es eine ausreichende Sensibilisierung der Mitarbeiter, die z.B. über Awareness-Maßnahmen erzielt werden kann, damit die Schutzbedarfe der Dateien berücksichtigt werden.

Abb. 9: Überblick über Level der Dateiverschlüsselung



Quelle: if[is]/Goldmedia 2018

Dedizierte Verschlüsselungsprogramme

Eine Alternative zur Dateiverschlüsselung bietet die Erstellung verschlüsselter Container, in denen Dateien und Ordner abgelegt werden können. Die Sicherheit der Container hängt von der Sicherheit der gewählten Passwörter ab. Zusätzlich ist es möglich, eine Zweifaktor-Authentifikation zur Entschlüsselung der Container einzurichten. Zu einem sicheren Passwort kann noch eine Schlüsseldatei oder ein Sicherheits-Token verlangt werden. Die Sicherheit erhöht sich dadurch, weil das Wissen um das Passwort zur Entschlüsselung alleine nicht ausreicht. Auch hier besteht das Problem, dass bei Nutzung durch mehrere Nutzer ein sicherer Weg für den Austausch der Schlüsseldateien und des Passworts erforderlich ist.

Ferner ist es auch möglich, versteckte Container anzulegen. Diese werden im Dateisystem nicht angezeigt und erst nach Eingabe eines weiteren Passworts sichtbar. Da die Container beim Speichern immer im Ganzen neu synchronisiert werden müssen, können bei großen Containern Komplikationen bei der Synchronisation auftreten. Regelmäßige Updates, um Sicherheitslücken bei der Umsetzung der Verschlüsselungsalgorithmen zu schließen, sind notwendig, da eine Aushebung der Verschlüsselung diese wirkungslos machen würde.

Tab. 17: Vor- und Nachteile der Technologien zur Dateiverschlüsselung

Lösung	Vorteile	Nachteile
Verschlüsselung aus Anwendungsprogrammen	▪ ohne zusätzliche Software nutzbar ▪ bietet ohne viel Aufwand ein ausreichendes Level an Vertraulichkeit	▪ langfristiges Schlüsselmanagement schwierig ▪ Probleme bei der Schlüsselübermittlung bei mehreren Nutzern
Verschlüsselungsfunktion des Betriebssystems	▪ ohne nachträgliche Installation anwendbar ▪ bei Nutzung durch mehrere Benutzer können öffentliche Schlüssel aus dem Active Directory genutzt werden	▪ nur bei bestimmten Systemen einsetzbar
Dedizierte Verschlüsselungsprogramme	▪ mehrere Möglichkeiten, Daten zu verschlüsseln ▪ ermöglicht Container-Verschlüsselung	▪ langfristiges Schlüsselmanagement schwierig ▪ Probleme bei der Schlüsselübermittlung bei mehreren Nutzern

Quelle: if[is]/Goldmedia 2018

Fazit

Die Verschlüsselung einzelner Dateien erhöht deren Vertraulichkeit und hilft, sie vor Einblicken Dritter zu schützen. Dabei greift der Schutz auch im laufenden Betrieb eines IT-Systems, wenn das Passwort für die Verschlüsselung des Datenträgers bereits eingegeben wurde. Deshalb ist es sinnvoll, besonders schutzbedürftige Dateien z.B. in verschlüsselten Containern abzulegen. Auch beim nicht verschlüsselten Versand von E-Mails kann die Verschlüsselung der angehängten Dateien für ein nötiges Maß an Sicherheit sorgen. Problematisch beim Verschlüsseln einzelner Dateien ist immer die Verwaltung der Schlüssel.

Weiterführende Links zu Dateiverschlüsselung

- **Veracrypt**
  https://veracrypt.codeplex.com/
- **Teletrust Anbieterverzeichnis**
  https://www.teletrust.de/anbieterverzeichnis/
- **Einsatz von Datenträgerverschlüsselung**
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04433.html

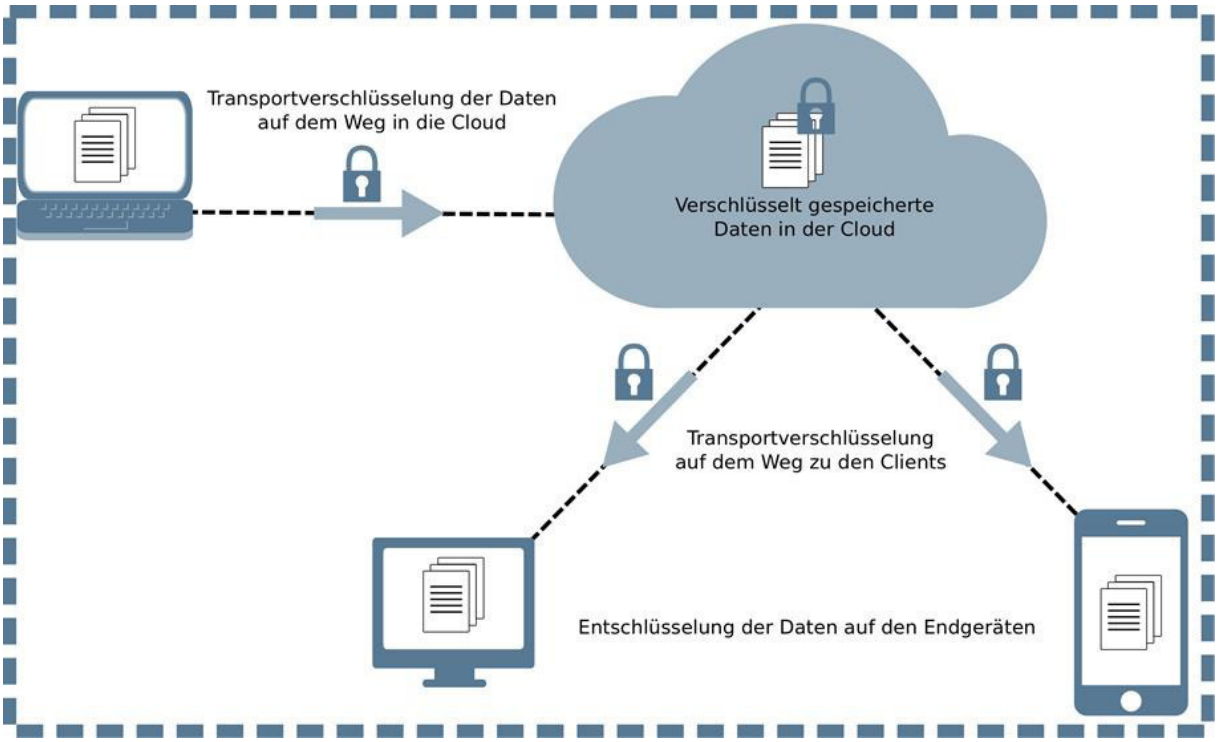
2.3 Cloud-Speicher-Dienste und Verschlüsselung

Die einfache Synchronisation, der standortunabhängige Zugang und die ständige Verfügbarkeit gespeicherter Daten machen die Nutzung von Cloud-Speicher-Diensten zu beliebten Werkzeugen. So ist es kaum verwunderlich, dass die Mehrheit der von uns befragten Unternehmen Cloudlösungen nutzt. Nutzern ist es möglich, ihre Daten an einer zentralen Stelle zu speichern und von verschiedenen Plattformen auf sie zuzugreifen. Zudem bietet das Online-Backup eine einfache Form zur Datensicherung. Cloud-Speicher-Dienste können für verteilt arbeitende Arbeitsgruppen eine Möglichkeit für unternehmensweite Kollaborationen bieten und die Effizienz von Arbeitsabläufen und Prozessen signifikant steigern.

Häufig besteht die Möglichkeit, durch Client-Software oder durch ein Web-Portal von vielen unterschiedlichen Geräteklassen auf die Daten zuzugreifen. Namenhafte Cloud-Speicher-Dienste sind u.a. Dropbox, OneDrive von Microsoft und Google Drive. Alternativ lässt sich auch mithilfe von z.B. *OwnCloud* oder *Nextcloud* eine eigene Cloud-Infrastruktur betreiben. Die Software ist Open Source und lässt sich an die eigenen Bedürfnisse anpassen.

Das Nutzen von Cloud-Speicher-Diensten ist mit Risiken verbunden, da die Daten in die Obhut des Anbieters gegeben werden. Dienstausfälle der Anbieter können die Arbeitsprozesse stark einschränken. Sollen vertrauliche Daten mit hohem Schutzbedarf in die Cloud ausgelagert werden, können ohne zusätzliche Sicherheitsmechanismen datenschutzrelevante Risiken entstehen. Es droht der Verlust der Vertraulichkeit und Integrität der Daten. Die durchgeführte Erhebung zeigt, dass trotz dieser Risiken viele Unternehmen auf fertige Cloud-Lösungen setzen und auch in puncto Verschlüsselung auf die Angebote des Herstellers zurückgreifen.

Abb. 10: Verschlüsselungsmöglichkeiten einer Cloud-Anwendung



Quelle: if[is]/Goldmedia 2018

Transportwege und Speicherort der Daten

Es besteht ein Risiko für die Vertraulichkeit der Daten, wenn der Transport und die Speicherung der Daten unverschlüsselt stattfinden. Sollen schützenswerte Daten online gespeichert werden, sollte über den Einsatz von Verschlüsselungsverfahren nachgedacht werden. Dabei gibt es drei Bereiche, die je nach Schutzbedarf abgedeckt werden sollten:

- die Transportwege (Data-in-Motion),
- der Speicherort der Daten (Data-at-Rest) und
- der Speicherort beim jeweiligen Benutzer (Data-at-Rest).

Die Verschlüsselung der Daten auf dem Transportweg wird oft bei den Anbietern standardmäßig und ohne zusätzliche Kosten angeboten. Daher sollte bei der Auswahl des Anbieters auf eine angemessene Transport-Sicherheit Wert gelegt werden.

Die Verschlüsselung der Daten auf Dateiebene am Speicherort erhöht zwar die Sicherheit der Daten, allerdings sollte berücksichtigt werden, dass der Anbieter die Verantwortung für das Schlüsselmanagement hat. So wäre der Anbieter potenziell in der Lage, die verschlüsselten Daten wieder zu entschlüsseln. Bei der Auswahl des Anbieters sollte das Verschlüsselungsverfahren und das Schlüsselmanagement transparent und nachvollziehbar sein.

Verschlüsselung auf Dateiebene

Die größte Sicherheit kann erreicht werden, wenn die Daten vor dem Übertragen beim Client schon verschlüsselt werden. Dies kann durch Zusatzsoftware wie *Boxcryptor* oder *Cryptomator* ermöglicht werden (siehe Kapitel 2.2). Die Daten werden lokal mit einem Krypto-Verfahren verschlüsselt und erst dann in die Cloud geladen, so werden nur verschlüsselte Daten übermittelt. Der Nutzer muss ein geeignetes Schlüsselmanagement verwenden, um z.B. Daten mit Dritten zu teilen. Ferner muss der Nutzer seinen eigenen kryptografischen Schlüssel sicher aufbewahren.

Es kann weder der Anbieter noch ein Dritter die gespeicherten Daten einsehen. Lediglich Personen, die über die entsprechende Passphrase oder den passenden Schlüssel verfügen, haben die Möglichkeit zur Entschlüsselung. Häufig kann das Verschlüsselungsverfahren optional ausgewählt werden. Falls eine eigene Cloud-Infrastruktur betrieben wird, kann die clientseitige Verschlüsselung ein zusätzliches Sicherheitsfeature darstellen.

Unternehmen müssen ihre Anforderungen an einen Cloud-Speicher-Dienst klar definieren. Bei der Auswahl des Cloud-Anbieters sollte auf Siegel und erfüllte Anforderungskataloge geachtet werden. Ebenso sollte an eine Verschlüsselung auf Dateiebene gedacht werden. Kosten für Zusatzsoftware sollten bei der Kalkulation berücksichtigt werden. Das Teilen der Daten wird dadurch komplexer. Nutzer müssen mehr Aufwand für ein geeignetes Schlüsselmanagement mit sicherem Schlüsselaustausch aufbringen. Das Teilen von verschlüsselten Daten wird zusätzlich komplexer, falls die Zusatzsoftware keine Funktionen zum Teilen von Daten unterstützt. Die Möglichkeit zur Zusammenarbeit könnte eingeschränkt werden.

Die kostenpflichtige Zusatzsoftware *Boxcryptor* ermöglicht eine effiziente Kollaboration. *Cryptomator* ist eine kostenfreie Lösung, bietet jedoch kein Schlüsselmanagement an. Freie Lizenzen gibt es häufig nur für den privaten Gebrauch und sind oft in ihrer Funktionalität stark eingeschränkt. Zudem kann eine aufwendige Konfiguration der Software den Einsatz erschweren.

Tab. 18: Vor- und Nachteile zur Methodik von Cloud-Speicher-Diensten

Lösung	Vorteile	Nachteile
Anbieter von Cloud-Speicher-Diensten (z.B. Dropbox oder OneDrive)	▪ vorhandene Transportverschlüsselung ▪ keine zusätzliche Pflege und Verwaltung der Infrastruktur ▪ Speicherplatz skalierbar ▪ Support durch Anbieter	▪ kostenpflichtig für den gewerblichen Gebrauch ▪ Verschlüsselung auf Dateiebene (Data-at-Rest) nur mit Einschränkungen (falls vorhanden) ▪ kaum konfigurierbar
Eigene Cloud-Speicher-Infrastruktur (z.B. Owncloud oder Nextcloud)	▪ flexibel konfigurierbar ▪ Unternehmen behalten Kontrolle über ihre Daten ▪ Open-Source-Lösungen vorhanden ▪ bietet höchstes Sicherheitspotenzial	▪ hoher Pflege- und Verwaltungsaufwand ▪ zusätzliche Kosten für den Betrieb ▪ Speicherplatz nur mit Aufwand skalierbar

Quelle: if[is]/Goldmedia 2018

Die folgenden Fragen sollen zur Orientierung beim Einsatz von Cloud-Speicher-Diensten dienen:

- Sollen sensible Unternehmensdaten in die Cloud ausgelagert werden?
- Bietet der Anbieter eine effiziente Transportverschlüsselung der Daten an?
- Ist der Speicherort der Daten bekannt?
- Gibt es eine Verschlüsselung auf Dateiebene?
- Sollen verschlüsselte Dateien mit mehreren Anwendern synchronisiert werden?
- Benötigt Ihr Unternehmen eine flexible Skalierbarkeit der Speichergröße?
- Besitzt Ihr Unternehmen die Ressourcen und Fachwissen, um eine eigene Speicher-Infrastruktur aufzubauen?
- Welche Dateien- und Datenschutzmaßnahmen hat das Unternehmen erfüllt?

Fazit

Cloud-Speicher-Dienste sind nicht mehr aus den Unternehmensabläufen wegzudenken. Synchronisation, der standortunabhängige Zugang und die ständige Verfügbarkeit der Daten sind für Arbeitsabläufe und Kollaborationsarbeiten von großem Vorteil. Je nach Sicherheitsanforderungen gibt es viele Möglichkeiten, Cloud-Speicher-Dienste in eine Unternehmensumgebung zu integrieren.

Das höchste Maß an Sicherheit kann durch eine eigene Infrastruktur erreicht werden. Ständige Pflege und entsprechendes Know-how sind für eine Gewährleistung der Sicherheit unabdingbar.

Weiterführende Links zu Cloud-Speicher-Diensten und Verschlüsselung

- **BSI - Sicherheitsempfehlungen für Cloud-Computing-Anbieter**
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf?__blob=publicationFile&v=6

- **Überblickspapier Online-Speicher**
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_Online-Speicher_pdf.pdf?__blob=publicationFile

- **BSI Sichere Nutzung von Cloud-Diensten**
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Sichere_Nutzung_Cloud_Dienste.pdf?__blob=publicationFile&v=8

- **Deutschland sicher im Netz: Cloud Computing Infos**
  https://www.sicher-im-netz.de/cloud-computing-infos

- **Teletrust Anbieterverzeichnis**
  https://www.teletrust.de/anbieterverzeichnis/

Glossar

Administratorenrechte	Als Administratorenrechte werden erweiterte Befugnisse eines Benutzers beschrieben, welche es ermöglicht, besondere Dateien zu verändern, zu löschen und zu verschieben.
Adobe Connect	Siehe Kollaborationsplattform.
AES (Advanced Encryption Standard)	Es handelt sich um ein elektronisches und symmetrisches Verschlüsselungsverfahren.
API (Application Programming Interface)	APIs bezeichnen Programmierschnittstellen auf Anwendungsentwicklungsebene, die anderen Softwaresystemen oder Programmen zur Anbindung bereitgestellt werden.
Authentizität	Die Authentizität ist eines der Schutzziele der Informationssicherheit. Sie beschreibt die Echtheit von Daten.
B2B (Business-To-Business)	Geschäftsbeziehungen zwischen 2 Unternehmen werden als B2B bezeichnet.
B2C (Business-To-Customer)	In Abgrenzung zu B2B beschreibt B2C die Geschäftsbeziehungen zwischen Unternehmen und Kunden.
BitLocker	BitLocker ist eine Festplattenverschlüsselungssoftware von Microsoft für Windows.
Boxcryptor	Boxcryptor ist eine kostenpflichtige Softwarelösung zur Dateiverschlüsselung.
Bring-your-own-Device-Policy	Richtlinien für den Umgang mit privaten Endgeräten für den geschäftlichen Einsatz.
CA (Certificate Authority)	Zertifizierungsstellen für digitale Zertifikate, um öffentliche Schlüssel Personen oder Organisationen zuzuordnen.
Citrix	Siehe Kollaborationsplattform.
Container	Container sind verschlüsselte virtuelle Behälter für die Lagerung von Dateien.
Cryptomator	Im Gegensatz zu Boxcryptor ist Cryptomator eine kostenlose Softwarelösung zur Dateiverschlüsselung.
Diffie-Hellman	Das Diffie-Hellmann-Protokoll ist ein Verfahren, welches genutzt wird, um einen geheimen Schlüssel für z.B. ein Kryptosystem über eine öffentliche Leitung sicher auszutauschen.
Dropbox	Dropbox ist ein kommerzieller Cloud-Speicher-Anbieter.
EFS (Encryption File System)	Das Encrypting File System ist ein Verfahren zur Dateiverschlüsselung auf NTFS-Datenträgern. Dieses Verfahren kann in Betriebssystemen von Microsoft wie Windows eingesetzt werden.
E-Mail Gateway	Ein E-Mail-Gateway ist ein zentraler Knotenpunkt, in dem ausgehende E-Mails automatisiert verschlüsselt werden können.

Ende-zu-Ende-Verschlüsselung	Die übertragenen Daten werden auf der Senderseite verschlüsselt und erst auf der Empfängerseite wieder entschlüsselt, sodass die Datenübertragung über alle Übertragungsstationen hinweg verschlüsselt ist und von keinem Dritten eingesehen werden kann.
FEK (File Encryption Key)	Um eine verschlüsselte Datei oder ein verschlüsseltes Laufwerk zu entschlüsseln, wird ein File Encryption Key benötigt.
FileVault 2	FileVault 2 ist eine Datei- und Speicherverschlüsselungsfunktion unter dem Betriebssystem Mac.
GoToMeeting	Siehe Kollaborationsplattform.
Google Drive	Google Drive ist der Cloud-Speicher-Dienst von Google
HTTP (Hypertext Transfer Protocol)	Das HTTP-Protokoll ist ein Übertagungsprotokoll, welches auf der Anwendungsschicht arbeitet. Es wird dazu benutzt, um Webseiten in einem Webbrowser zu laden.
HTTPS (Hypertext Transfer Protocol Secure)	HTTPS basiert auf HTTP, wobei jedoch die übertragenen Daten der Webseiten verschlüsselt und dadurch abhörsicher übertragen werden, bevor sie im Webbrowser angezeigt werden.
IEEE 802.1AE	Siehe MACsec.
Integrität	Die Integrität ist eines der Schutzziele der Informationssicherheit. Sie beschreibt die Unversehrtheit der Daten vor unautorisierten Modifikationen Dritter.
IPSec	Es handelt sich bei IPSec um eine Erweiterung für das Internet-Protokoll (IP) von der Internet Engineering Task Force (IETF). Mit IPSec lassen sich IP-Pakete verschlüsseln und gesichert über Netze transportieren. Zudem wurde das Protokoll um Authentisierungsmechanismen erweitert. So können Absender oder Schlüssel authentisiert werden.
IRC (Internet Relay Chat)	IRC ist ein Messaging-Dienst. Es ist ein textbasiertes Chat-System.
ISDN (Integrated Services Digital Network)	ISDN ist ein internationaler Standard für ein digitales Telekommunikationsnetzwerk, welches heute hauptsächlich zur Telefonie genutzt wird.
Kollaborationsplattformen	Kollaborationsplattformen sind zumeist Online-Plattformen, die gruppen- und unternehmensübergreifende Zusammenarbeit an Projekten und die Synchronisation und Austausch von Daten ermöglicht.
LAN (Local Area Network)	LAN beschreibt ein lokales Heim- oder Unternehmensnetzwerk.
MAC-Adresse (Media-Access-Control-Adresse)	Eine MAC-Adresse ist eine eindeutige Hardware-Adresse des Netzwerkadapters. Sie dient zur eindeutigen Identifikation in Rechnernetzen. Je nach Betriebssystem ist sie auch unter Physikalischer Adresse oder Ethernet-ID bekannt.
MACsec	MACsec umfasst ein Authentisierungsverfahren für MAC-Adressen aller im lokalen Netz verbundenen Geräte.

Messaging-Dienst	Messaging-Dienste sind Softwarelösungen zum Austausch von Kurznachrichten, zumeist in Textform oder aber auch in anderen Datenformaten wie Audio- und Videoform.
Mobile-Device-Management	Ein Mobile-Device-Management dient zur zentralen Konfiguration und Verwaltung von mobilen Endgeräten im Unternehmensumfeld.
Nextcloud	Nextcloud ist ein Open Source (siehe Open Source) und eine frei verfügbare Softwarelösung für einen Online-Speicher-Dienst, welcher komplett selber konfigurierbar ist. Es basiert auf Owncloud.
OneDrive	OneDrive ist ein Cloud-Speicher-Dienst von Microsoft.
Open Source	Als Open Source gilt Software, dessen Quelltext öffentlich zugänglich ist und von Dritten genutzt und verändert werden kann.
OpenVPN	Ist eine freie Software, um Zugang zu einem virtuellen privaten Netzwerk aufzubauen.
OSI-Modell	Das OSI-Modell ist ein Referenzmodell für Netzwerkprotokolle, welches in mehreren Schichten aufgebaut ist und Schnittstellen für die anderen Schichten und Protokolle beinhaltet.
Owncloud	Owncloud ist ein Open Source (siehe Open Source) und eine frei verfügbare Softwarelösung für einen Online-Speicher-Dienst, welcher komplett selber konfigurierbar ist. Owncloud dient insbesondere zum Aufbau einer eigenen Infrastruktur für einen Online-Speicher-Dienst.
GNUPG/PGP (Pretty Good Privacy)	Bei GNUPG/PGP handelt es sich um eine Software, die verwendet werden kann, um Daten zu verschlüsseln und elektronisch zu signieren. Oft wird GNUPG/PGP benutzt, um E-Mails zu verschlüsseln. Es wird ein asymmetrisches Public-Key-Verfahren verwendet, um die Nachrichten zu verschlüsseln bzw. wieder zu entschlüsseln.
Policy	Policys sind Richtlinien, welche eine Handlungs- oder Ausführungsvorschrift in einem Unternehmensumfeld beschreiben.
Projectplace	Siehe Kollaborationsplattform.
PKI (Public-Key-Infrastructure)	Eine Infrastruktur für öffentliche Schlüssel ist eine Hierarchie von digitalen Zertifikaten. Sie dienen dazu, digitale Zertifikate sicher auszutauschen.
Quvert	Siehe Messaging-Dienst.
Ryver	Siehe Messaging-Dienst.
S/MIME (Secure / Multipurpose Internet Mail Extensions)	S/MIME ist ein Standard zum Verschlüsseln und Signieren von Dateien.
Schadsoftware	Schadsoftware oder Malware ist schädlicher Quellcode, welcher das Ziel hat, auf dem infizierten informationstechnischen System Schaden anzurichten. Bekannte Beispiele dafür sind Viren, Würmer oder auch Trojaner.

Schlüsseldatei	Eine Schlüsseldatei ist eine Datei, welche als Faktor zur Authentisierung dient. So kann z.B. für das Öffnen einer Datei neben einem Passwort noch zusätzlich eine Schlüsseldatei benötigt werden.
Secure Real-Time Transport Protocol (SRTP)	SRTP ist eine verschlüsselte Variante des RTP-Protokolls zur Kommunikation im Internet, welches zunehmend Verwendung bei IP-Telefonie findet.
Sicherheitstoken	Sicherheitstoken fungieren ähnlich wie eine Schlüsseldatei zur Authentisierung. Allerdings ist ein Sicherheitstoken eine Hardwarekomponente meist in Form eines USB-Sticks
Skype	Skype ist eine Software von Microsoft zur Internet-Telefonie.
Slack	Siehe Messaging-Dienst.
Smartcard	Eine Smartcard oder Chipkarte ist eine Kunststoffkarte mit einem integrierten Chip. Zum Auslesen wird ein Kartenlesegerät benötigt
Software-Development-Kits (SDKs)	SDKs sind Sammlungen von Werkzeugen und Bibliotheken zum Programmieren und dienen Softwareentwicklern zum Erstellen von Anwendungen.
SSL (Secure Sockets Layer)	SSL ist ein Verschlüsselungsprotokoll für den Datentransfer auf der Transportschicht des TCP/IP-Protokollstapels und Vorgänger von TLS.
SSL/TLS-Sicherheitszertifikaten	SSL/TLS-Sicherheitszertifikate dienen zur Authentisierung von Webseiten.
TLS (Transport Layer Security)	TLS ist ein Verschlüsselungsprotokoll für den Datentransfer auf der Transportschicht des TCP/IP-Protokollstapels und Nachfolger von SSL.
TPM (Trusted Platform Module)	TPMs sind spezielle Hardwarekomponenten mit kryptografischen Funktionen.
Trust Center	Siehe CA.
Veracrypt	Veracrypt ist ein Programm, mit dem ganze Speicherlaufwerke verschlüsselt oder verschlüsselte Container erstellt werden können.
Vertraulichkeit	Die Authentizität ist eines der Schutzziele der Informationssicherheit. Sie beschreibt den Schutz der Daten vor dem Zugriff unautorisierter Dritter.
Virtuellen Maschine (VM)	Eine virtuelle Maschine ist eine reale Nachbildung eines Rechnersystems mit real existierenden Hardwarekomponenten, in dem ein Rechnersystem emuliert werden kann.
Virtuelles Laufwerk	Ein virtuelles Laufwerk ist eine Emulation eines Datenträgers oder Wechselmediums, wie z.B. eines CD- oder DVD-Laufwerks.
Voice-over-IP	Das Verfahren beschreibt die paketvermittelnde Telefonie über das Internet.

VPN (Virtual Private Network)	VPNs sind in sich geschlossene Kommunikationsnetzwerke, welche genutzt werden, um verschlüsselten Fernzugriff auf Unternehmensdaten herzustellen.
WebEx	Siehe Kollaborationsplattform.
WhatsApp	Siehe Messaging-Dienst.
White-Label-Lösung	Eine White-Label-Lösung beinhaltet einen eingekauften Dienst oder ein Produkt, das auf die Unternehmensanforderungen angepasst werden kann.
WPA (Wi-Fi Protected Access)	WPA ist eine veraltete Verschlüsselungsmethode für drahtlose Netzwerke.
WPA2 (Wi-Fi Protected Access 2)	WPA2 ist der Nachfolger von WPA und eine Verschlüsselungsmethode für drahtlose Netzwerke.
XMPP (Extensible Messaging and Presence Protocol)	Das XMPP ist ein offenes Kommunikationsprotokoll. Es wird häufig für Messaging-Dienste benutzt (siehe Messaging-Dienst). Durch Erweiterungen kann die Funktionalität beliebig und individuell erweitert werden.
ZRTP (Z und Real-Time Transport Protocol)	ZRTP ist ein Schlüsselaustauschprotokoll und wird verwendet, um Schlüssel für eine Verschlüsselung zwischen zwei Endpunkten eines VoIP- (siehe VoIP) basierten Telefonats auszutauschen.
Zweifaktor-Authentifizierung	Die Zweifaktor-Authentifizierung beschreibt ein Authentifizierungsverfahren, das zwei unterschiedliche Faktoren zur erfolgreichen Authentifizierung benötigt. Z. B. werden ein Passwort und eine Schlüsseldatei benötigt, um Zugang zu bekommen.