LERNEN EINFACH GEMACHT

Sonderausgabe
Boxcryptor

Datensicherheit und Cloud-Verschlüsselung

für dummies®

Datenschutz
im Cloud-Speicher

Verschlüsselte Dateien
gemeinsam nutzen

Datensicherheit und
Zugriffsmanagement

Lisa Figas
Moritz Ober

Datensicherheit und Cloud-Verschlüsselung für Dummies

Lisa Figas und Moritz Ober

Datensicherheit und Cloud-Verschlüsselung

für dummies®

Sonderausgabe Boxcryptor

WILEY-VCH
WILEY-VCH GmbH

Datensicherheit und Cloud-Verschlüsselung für Dummies

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Coverfoto: © Secomba GmbH
Korrektur: Dr. Petra-Kristin Bonitz, Hemmingen
Satz: Straive, Chennai, India
Druck und Bindung

Auf einen Blick

Inhaltsverzeichnis

Einleitung

Mit diesem Buch bieten wir Ihnen einen Service, den Sie auf Google nicht finden. Schließlich suchen Sie mit einer Suchmaschine nur nach Antworten, deren Fragen Sie bereits kennen. Wir geben Ihnen Antworten auf Fragen, an die Sie bisher noch gar nicht gedacht haben. So können Sie das ganze Thema der Cloud-Verschlüsselung überblicken und gehen bestens vorbereitet in den Prozess, diesen zusätzlichen Schutz in die IT-Infrastruktur Ihres Unternehmens einzugliedern.

Wir kennen uns richtig gut aus mit Verschlüsselung. Schließlich gibt es Boxcryptor seit mehr als zehn Jahren. In dieser Zeit haben wir mit unserer Software beachtliche Datenmengen durch Ende-zu-Ende-Verschlüsselung geschützt und damit viel für den Schutz sensibler Daten getan.

Beim Schreiben hatten wir die Unternehmen im Kopf, mit denen wir jeden Tag in Kontakt treten und die wir teilweise schon seit Jahren begleiten. Wir kennen die Fragen, die in unseren Beratungsgesprächen auftauchen und überblicken den gesamten Prozess vom ersten Gespräch bis hin zur verschlüsselten Datei. Dieses Wissen stellen wir Ihnen hier zur Verfügung.

Verstehen Sie dieses Buch aber auch als Ausdruck unserer Sorge. Wir sehen Jahr für Jahr die Statistiken, aus denen hervorgeht, dass immer noch viel zu wenige Unternehmen ihre Daten verschlüsseln. Dabei sind die Sicherheitsrisiken bekannt und die Beispiele für Datenlecks zahlreich. Im Vergleich zu dem Schaden, den unerlaubter Zugriff auf sensible Inhalte verursachen kann, ist die Einführung einer Verschlüsselungssoftware im Unternehmen ein Klacks. Na gut, vielleicht kein Klacks, aber dringend notwendig. Und das ist der Grund, warum wir *Datensicherheit und Cloud-Verschlüsselung für Dummies* geschrieben haben. Packen Sie es gemeinsam mit uns an!

Zielgruppe des Buches

Wir sprechen mit diesem Buch Menschen an, die sich in Ihrem Unternehmen mit den Themen Datenschutz und Datensicherheit befassen. Dafür bauen wir auf vorhandenem Wissen auf und vertiefen es. Wir möchten, dass Sie so kompetent im Bereich Verschlüsselung werden, dass Sie *echte* Ende-zu-Ende-Verschlüsselung erkennen, dass Sie alle kritischen Fragen beantworten können und dass Sie

zielsicher den passenden Anbieter für Verschlüsselungssoftware für Ihr Unternehmen auswählen können.

Sie sind hier genau richtig, wenn …

- ✔ … Sie in den Bereichen Datenschutz, Datensicherheit, IT-Sicherheit, Cloud-Sicherheit oder in einem verwandten Bereich arbeiten oder sich engagieren. Sie verfügen bereits über ein gewisses technisches Verständnis und kennen relevante Grundbegriffe. Fachwörter erklären wir natürlich, damit alle auf einem gemeinsamen Nenner sind.
- ✔ … Ihnen der Wert bewusst ist, den sensible Daten haben und Sie die Anforderungen durch die DSGVO und die verschiedenen Normen, die für die jeweilige Branche vorgeschrieben sind, kennen (zur Erinnerung haben wir diese Regeln in Kapitel 2 aber auch noch einmal zusammengefasst).
- ✔ … Sie bereit sind, sich für den Schutz personenbezogener Daten und Geschäftsgeheimnisse einzusetzen.
- ✔ Sie Neugier mitbringen, *wie genau* sensible Daten geschützt werden und wie Sie Verschlüsselung dafür einsetzen können. Sie möchten sich vielleicht auch nur ganz allgemein im Bereich Verschlüsselung fortbilden oder haben sogar Respekt vor dem Themenkomplex, weil er auf den ersten Blick unüberschaubar erscheint.

Erkennen Sie sich in diesen Punkten wieder? Prima, dann haben Sie uns gesucht und gefunden. Lassen Sie uns mit einer kurzen Vorstellung beginnen, damit auch Sie wissen, mit wem Sie es hier zu tun haben.

Über Secomba GmbH | Boxcryptor

Seit 2011 bieten wir Ende-zu-Ende-Verschlüsselung für Dateien an. Wir haben uns auf den Schutz von Daten spezialisiert, die in Cloud-Speichern abgelegt werden. Unsere Software steht für Einzelnutzer und Teams zur Verfügung. Bei unseren größten Kunden verschlüsseln zig Tausende Accounts ihre Daten. Unsere Software steht für die größten Betriebssysteme Windows, Android, MacOS und iOS zur Verfügung. Mehr als 30 Cloud-Speicher unterstützen wir nativ und zahllose weitere können über das WebDAV-Protokoll mit Boxcryptor verbunden werden.

Unser Team in Augsburg umfasst mehr als 30 Mitarbeiterinnen und Mitarbeiter Der größte Teil von ihnen arbeitet in der Entwicklungsabteilung und sorgt dafür,

dass Boxcryptor stets für jedes aktuelle Betriebssystem zur Verfügung steht und alle Features reibungslos funktionieren.

Gegründet wurde das Unternehmen von der Wirtschaftsjuristin Andrea Pfundmeier und dem IT-Spezialisten Robert Freudenreich. Das Gründungsteam leitet das Unternehmen noch immer gemeinsam und freut sich auf die kommenden Jahre.

Über dieses Buch

Wenn Sie dieses Buch gelesen haben, wissen Sie alles, was Sie beachten müssen, um sensible Unternehmensdaten in der Cloud zu schützen. Wenn Sie schon Vorwissen haben, dann stürzen Sie sich am besten gleich auf die Kapitel, die Sie am meisten interessieren. Jedes Kapitel steht für sich, sodass das Buch auch als Nachschlagewerk dient.

Kapitel 1: Hier geht es um Datenspeicher im Allgemeinen und Cloud-Speicher im Besonderen. In diesem Kapitel beschreiben wir die Entwicklung der Speichereinheiten und bewerten die Vor- und Nachteile von Cloud-Speichern.

Kapitel 2 befasst sich mit Datenschutzgesetzen und -regelungen. Welche Vorgaben gibt es im Bereich Datenschutz? Wir blicken auf unterschiedliche Länder, Regionen und Branchen. Lernen Sie außerdem den entscheidenden Unterschied zwischen Vertraulichkeit und Integrität von Daten kennen.

Kapitel 3 erläutert alles zu Datensicherheit und Datenschutz. Hier geht es um den Schutz vor Verlust von Daten und den Schutz vor unbefugtem Zugriff auf Daten. Eine gute Sicherheitsstrategie umfasst beide Aspekte.

Kapitel 4 definiert, was Verschlüsselung eigentlich bedeutet. In diesem Kapitel klären wir Grundbegriffe und beschreiben die verschiedenen Arten von Verschlüsselung sowie die jeweiligen Vor- und Nachteile.

Kapitel 5: Hier lernen Sie die Anwendungsbereiche von Verschlüsselung kennen. Wenn Sie planen, Verschlüsselung zu verwenden, müssen Sie genau analysieren, wo verschlüsselt werden soll. Wir definieren die Unterschiede von soft- und hardwaregestützter Verschlüsselung sowie von Open- und Closed-Source-Software. Dieses Kapitel unterstützt Sie dabei, die richtigen Fragen zu stellen.

Kapitel 6 liefert Argumente. Sich im Unternehmen für Fortschritt einzusetzen, kann eine zähe Mission sein. Wir wappnen Sie für jedes Meeting mit den

passenden Stichworten und helfen Ihnen dabei, die Perspektive der Stakeholder einzunehmen.

Kapitel 7 bietet mehrere Fallbeispiele. Jede Organisationsstruktur ist individuell. Parallelen gibt es trotzdem. Nutzen Sie unsere Fallbeispiele, um den Einsatz von Verschlüsselung in Ihrem eigenen Unternehmen zu implementieren.

Kapitel 8 listet Anbieter von Verschlüsselungssoftware auf. Solche Anbieter haben unterschiedliche Ansatzpunkte für den Schutz Ihrer Daten. Wir stellen beispielhaft beliebte Lösungsansätze vor und führen die Voraussetzungen und Einschränkungen auf.

Kapitel 9 zeigt Ihnen die zehn Schritte zur passenden Verschlüsselungslösung und machen Sie auf die wichtigsten Fragen aufmerksam, die Sie klären sollten, bevor Sie sich für einen Anbieter entscheiden.

Kapitel 10 verschafft Ihnen einen Überblick über gängige Missverständnisse und Fehlannahmen über Verschlüsselung. Sie finden hier die wichtigsten Hintergrundinformationen, um souverän auf Fragen und Vorurteile zu reagieren.

Der **Anhang** stellt Ihnen hilfreiche Links und Wissenswertes rund um das Thema Datenschutz und Verschlüsselung zur Verfügung. Stöbern Sie durch die empfohlenen Webseiten, wagen Sie mit uns einen Blick in die Zukunft und probieren Sie unsere Social-Media-Tipps aus.

Wie geht es nun weiter? Nachdem Sie sich einen Überblick über die Kapitel verschafft haben, können Sie direkt an dem Punkt einsteigen, an dem der Schuh drückt. Wenn Sie mehr Zeit haben, dann empfehlen wir, das Buch von vorn nach hinten zu lesen. Die Kapitel sind zwar in sich abgeschlossen, bauen aber doch aufeinander auf.

Symbole, die in diesem Buch verwendet werden

In diesem Buch verwenden wir zur Orientierung drei Symbole, die besondere Kategorien von Informationen hervorheben:

Neben diesem Icon finden Sie Tipps, mit denen wir Sie bei der Umsetzung unterstützen.

Hier haben wir nützliches Zusatzwissen und Hintergrundinformationen zu einem Thema zusammengestellt.

Sie ahnen es: Dieses Icon zeigt an, dass hier besondere Vorsicht geboten ist.

Wie es weitergeht

»Datensicherheit und Cloud-Verschlüsselung für Dummies« begleitet Sie durch den Prozess, für Dateien, die in einer Cloud gespeichert sind, Datensicherheit und Datenschutz zu gewährleisten. Aus Erfahrung wissen wir, dass es viele kleine Schritte und einige Meetings benötigt, dieses Thema in einem Unternehmen umzusetzen. Wenn Sie sich am Anfang dieses Prozesses befinden, dann empfehlen wir den Einstieg mit Teil I und II, denn die Grundlagen helfen Ihnen später beim technischen Verständnis. Wenn Sie bereits fortgeschritten sind, dann können Sie gleich mit Teil III starten, um praktische Hilfe für die Einführung von Verschlüsselungssoftware in Ihrem Unternehmen zu bekommen. Einen Überblick über den Prozess und die notwendigen Schritte verschaffen Sie sich am schnellsten in Teil IV.

Teil I

Datenschutz und Datensicherheit

IN DIESEM TEIL ...

In diesem Teil lernen Sie alles über die Entwicklung der Speichereinheiten vom fotografischen bis zum magnetischen Speicher. Sie erfahren, was die Cloud ist, und lernen wichtige Fachbegriffe kennen. Sie bekommen außerdem einen guten Überblick über die Vor- und Nachteile von Cloud-Speichern für Unternehmen.

IN DIESEM KAPITEL

- Unterschiedliche Arten von Datenspeichern
- Wichtige Begriffe zum Thema Cloud-Computing
- Vorteile und Risiken von Cloud-Speichern

Kapitel 1
Daten ... und wo sie zu finden sind

Haben Sie heute schon ein Textdokument an Ihrem Computer erstellt? Oder einen Termin im Smartphone angelegt? Möglicherweise haben Sie auch eine Messenger-Nachricht verschickt? Oder einfach nur einen kleinen Einkaufszettel aus Papier am Küchentisch hinterlassen? Bei all diesen Tätigkeiten (und natürlich unzähligen weiteren) entstehen Daten, die aufgezeichnet, gespeichert, verändert, geladen oder gelöscht werden. Daten und ihre Verarbeitung sind also allgegenwärtig und die Inhalte entweder analog oder elektronisch »abrufbar«. Vorgehalten werden die Informationen in Datenspeichern. Die verschiedenen Arten von Datenspeichern kennenzulernen, ist ein guter Einstieg in die Frage, wie die enthaltenen Informationen geschützt werden können. Also, los geht's.

Datenspeicher im Wandel der Zeit

Daten zu speichern, ist heute wichtiger denn je. Vor allem zur Archivierung, Weitergabe und Vervielfältigung von Informationen werden Datenspeicher benötigt. Damit sind häufig sogenannte Speichermedien gemeint. Diese müssen meist von Computern oder anderen elektronischen Geräten ausgelesen werden. Aber das war nicht immer so.

Neben dem gesprochenen Wort sind zum Beispiel auch Höhlenmalereien und frühe Schriftsysteme Möglichkeiten, Informationen zu verpacken (»codieren«) und weiterzugeben. Diese Formen werden auch als »nicht-technische« Datenspeicher bezeichnet, denn sie sind ohne Hilfsmittel von Menschen direkt angefertigt und auch lesbar.

Der Beginn der technischen Datenspeicher wird grob auf das späte 19. Jahrhundert datiert. Seitdem ging es rasant weiter: Was etliche tausend Jahre zur initialen Entwicklung gebraucht hat, wurde in weniger als 150 Jahren zu einem feingliedrigen System aus Speichern, Formaten und Verwaltungsstrategien ausgebaut.

Der größte Unterschied zu allen bisher existierenden Möglichkeiten der Datenspeicherung: Ohne eine Maschine läuft heute nichts mehr. Oder haben Sie schon einmal versucht, eine CD per Hand abzuspielen?

Zu Beginn werfen wir einen Blick auf die verschiedenen technischen Datenspeicher (siehe Abbildung 1.1).

- **Fotografische Speicher**: Hier werden Daten chemisch als Lichtbilder gespeichert. Dazu gehören neben gewöhnlichen Fotos auf Fotopapier auch Filme und andere lichtsensitive Materialien. Der bereits 1859 erfundene Mikrofilm, ein fotografisches Speichermedium, ist bis heute die vermutlich am längsten haltbare, technische Speicherform. Damit können sowohl analoge als auch digitale Daten für circa 500 Jahre aufbewahrt werden – sachgemäße Lagerung vorausgesetzt.

- **Mechanische Speicher**: Etwas später als der Mikrofilm wurde die Lochkarte erfunden. Sie kommt ab dem späten 19. Jahrhundert zum Einsatz. Gemeinsam mit Schallplatten gehört sie zu den mechanischen Speichern. Auch gepresste CDs, Blu-Ray-Discs et cetera sind mechanisch hergestellte Datenträger.

- **Optische Speicher**: Wesentliches Merkmal der optischen Speicher ist, dass sie mit Lasern (und damit kontaktlos) ausgelesen werden. Dazu gehören vor allem Speicher, die wie eine CD aussehen. Einige optische Speichermedien können auch mithilfe von Lasern beschrieben, also »gebrannt« werden.

- **Magnetische Speicher**: Weit verbreitet, zum Beispiel in Festplatten, Sicherungsbändern und Magnetstreifen – so wie früher in Disketten, Audio- und Videokassetten – sind Datenspeicher aus magnetisierbarem Material. Sie werden von einem Schreibkopf beschrieben.

  Während magnetische Speicher an sich günstig verfügbar sind, sorgen Magnetfelder, bewegliche Elemente und Abnutzung jedoch für eine relativ große Anfälligkeit gegenüber Beschädigungen. Die acht Terabyte große Festplatte mit den wichtigen Bauplänen fallen zu lassen, wäre jedenfalls keine gute Idee …

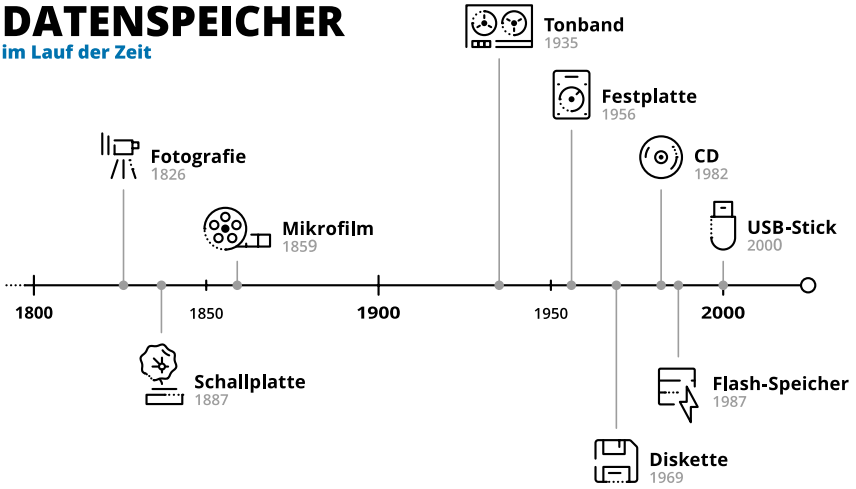

Abbildung 1.1: Datenspeicher im Lauf der Zeit

- ✔ **Elektronische Speicher**: Heutzutage werden hauptsächlich moderne Flash-Speicher verwendet. Sie finden sich überall: Smartphones, USB-Sticks, SD-Karten und viele weitere Geräte haben keine klobige Magnetscheibe mehr im Inneren. Stattdessen werden die Eigenschaften elektronischer Halbleiter genutzt, um Informationen zu schreiben, zu speichern und abzurufen. Dadurch benötigen sie nicht nur weniger Platz, sondern sind auch physikalischen Beschädigungen gegenüber wesentlich robuster.

Alle genannten Datenspeicher haben eines gemeinsam: Sie sind in der Regel an nur einem Ort gleichzeitig verfügbar. Bei Beschädigung oder Diebstahl droht der Verlust der gespeicherten Daten. Der verschüttete Kaffee auf dem Notizblock? Eine heruntergefallene Festplatte? Ein defekter Flash-Speicher? Tschüss, Daten!

Nicht zuletzt deshalb erleben Cloud-Speicher seit gut zehn Jahren einen gewaltigen Aufschwung. Sie machen Speicherkapazität über das Internet immer und überall verfügbar.

Erleben wir also gerade eine Revolution der Datenspeicherung? Hier lohnt sich ein genauerer Blick.

Cloud-Speicher

Der Begriff »Cloud« klingt romantisch. Haben Sie sich schon einmal vorgestellt, dass Daten, dass gar das ganze Internet, als Wolke über uns schwebt? Die dauerhafte und unsichtbare Verbindung zwischen den Dateien und unseren Computern, Tablets und Mobiltelefonen unterstützt diese Vorstellung. Tatsächlich handelt es sich aber um handfeste Rechenzentren mit jeder Menge Speicherkapazität.

Das amerikanische National Institute of Standards and Technology (NIST) definiert die Cloud als Netzwerk aus Computing-Ressourcen, wie Speicher, Server, Anwendungen und Dienste, die dem Nutzer über das Internet jederzeit und überall nach Bedarf zur Verfügung stehen.

Wesentlich für die Cloud sind folgende Merkmale:

- ✔ Nutzer können selbst die Bereitstellung von Ressourcen veranlassen.
- ✔ Das Netzwerk aus Ressourcen steht jederzeit und überall auf Abruf über alle möglichen Endgeräte zur Verfügung.

- ✔ Die Speicher-Kapazitäten des Cloud-Speicher-Anbieters sind aus verschiedenen geografischen Orten zu einem virtuellen Ressourcen-Pool zusammengeschlossen.
- ✔ Je nach Bedarf können schnell und einfach zusätzliche Ressourcen bereitgestellt sowie nicht benötigte Ressourcen wieder freigegeben werden. Flexible Abo-Modelle sind die Regel.
- ✔ In der Cloud werden Ressourcen nach tatsächlichem Verbrauch abgerechnet. Nutzer können kurzfristig ein Up- oder Downgrade durchführen.

Der Begriff der »Cloud« etablierte sich als vage Beschreibung wolkenartig vernetzter Ressourcen in Rechenzentren. Ein Cloud-Speicher ist also Speicher-Kapazität in einem speziell geschützten Gebäude, die Sie mieten können. Sie können Ihre Cloud-Server in der Regel weder besuchen noch anfassen, deshalb müssen Sie es uns einfach glauben: Auch Cloud-Daten liegen auf einer stinknormalen Festplatte.

»Nennen Sie es nicht Cloud.« (Security-Experte Graham Cluley): Die Cloud ist ein Netzwerk von Rechenzentren, also eigentlich nichts anderes als ein fremder Computer.

Daten sind dank dem Cloud-Netzwerk permanent und überall verfügbar. Sie müssen sich also keine Sorgen machen, dass Sie eine Datei nicht »dabeihaben«. Gleichzeitig sind sie aber auch für fremde Personen prinzipiell zugänglich. Sie sollten also dafür Sorge tragen, dass die Daten auch inhaltlich geschützt sind.

IaaS, PaaS & SaaS – klingt komplizierter, als es tatsächlich ist

Im Cloud-Computing gibt es verschiedene Kategorien (siehe Abbildung 1.2): Infrastructure as a Service (IaaS), Platform as a Service (PaaS) und Software as a Service (SaaS).

- ✔ Bei **IaaS** handelt es sich um Basisservices, die virtuelle Infrastruktur, wie etwa Datenspeicher oder Rechenleistung. Anstatt teure Hardware zu kaufen, können Unternehmen die für ihre anfallenden Aufgaben erforderliche Serverkapazitäten einfach mieten.
- ✔ **PaaS** ist in der Entwicklung von Funktionsweisen der Cloud der nächste logische Schritt nach IaaS. Unternehmen können vordefinierte Plattformen zur Softwareentwicklung in der Cloud mieten. Dies wird häufig für die Entwicklung von Apps genutzt.

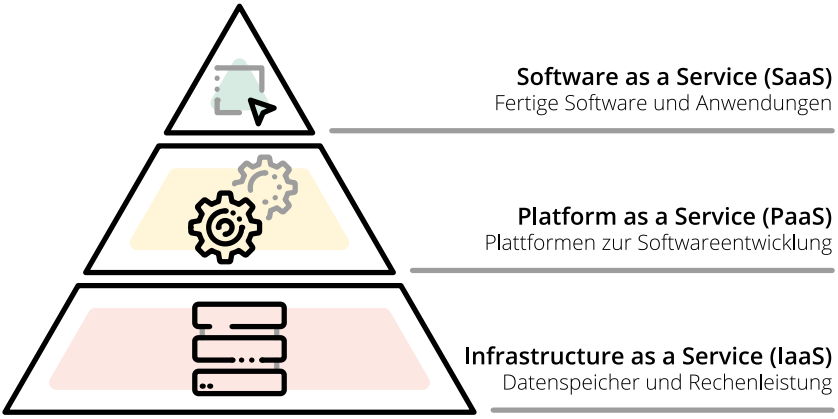

Abbildung 1.2: Cloud-Modell

- ✔ **SaaS** ist das, was die meisten Menschen mit der Cloud assoziieren. Es umfasst cloudbasierte Anwendungssoftware, auf die der Endnutzer über das Internet von diversen Geräten aus zugreifen kann. Die Online-Dienste werden sozusagen »all-inclusive« gemietet: Der Anbieter übernimmt jegliche Wartung von Infrastruktur und Software. Man muss also selbst kein Expertenwissen haben, wenn man SaaS-Cloud-Angebote nutzen will. Alles ist bereits fertig eingerichtet und man bedient die Einstellungen über eine praktische Nutzeroberfläche.

Cloud-Speicherdienste wie OneDrive, Dropbox oder Google Drive gehören zu den SaaS-Diensten. Sie stellen Speicherkapazitäten über das Internet bereit, die sich für die Endnutzer wie eine Festplatte verwenden lassen. Dafür müssen auch keine komplizierten Upload-Programme genutzt werden, denn die Anbieter liefern die Nutzeroberfläche gleich mit. Außerdem kümmern sie sich darum, dass die benutzten Datenträger immer funktionieren und Ihre Daten nicht verloren gehen. Auch die Datensicherung und die Wiederherstellung gelöschter Dateien gehören zum Service der meisten Anbieter.

Ein Nachteil ist, dass Nutzerinnen und Nutzer in der Regel nicht bestimmen können, an welchem Standort ihre Daten gespeichert werden. Tatsächlich ist es oft gar nicht so leicht, herauszufinden, in welchen Ländern die Rechenzentren stehen, in denen die eigenen Daten liegen.

Da die Rechtslage in Bezug auf den Datenschutz und die Zugriffsmöglichkeiten von Behörden in jedem Land unterschiedlich ist, ergeben sich daraus immer wieder Probleme. Dazu kommt, dass die Erreichbarkeit der Rechenzentren zwar in der Regel sehr gut ist, praktisch aber niemand zu 100 Prozent garantieren kann, dass der Zugriff wirklich jederzeit möglich ist.

Vorteile und Risiken von Cloud-Speichern

Bei der Entscheidung für oder gegen eine Cloud-Speicherlösung müssen Sie Vorteile und Risiken gründlich gegeneinander abwiegen. Planen Sie dafür Ressourcen ein.

Keine Sorge, die wichtigsten Punkte haben wir für Sie schon einmal zusammengefasst – die Entscheidung ist weniger schwierig, als Sie es sich vielleicht vorstellen.

Zunächst die positiven Aspekte. Die Vorteile von Cloud-Speichern sind:

- ✔ Der Zugriff auf die Daten ist – bei bestehender Internetverbindung – von jedem Ort zu jeder Zeit möglich.
- ✔ Die Zusammenarbeit im Team ist durch den gemeinsamen Zugriff auf Dateien einfach möglich.
- ✔ Cloud-Speicher bieten eine große Speicherkapazität bei geringen Kosten.
- ✔ Das ganze System ist auf Skalierbarkeit optimiert, wodurch kurzfristige Erweiterungen möglich sind.
- ✔ Bereitstellung und Pflege der Infrastruktur werden vom Cloud-Anbieter übernommen.
- ✔ Kontrollen und Auditing werden durch den gemeinsamen Zugriff auf den Speicher vereinfacht.
- ✔ Datensicherheit und Katastrophenschutz werden vom Cloud-Anbieter übernommen.

Sehen Sie sich nun die negativen Aspekte an. Doch keine Sorge: Wir wollen Ihnen die Nutzung der Cloud keineswegs ausreden. Betrachten Sie den folgenden Abschnitt lieber als eine To-do-Liste für die Risikominimierung.

Die Risiken von Cloud-Speichern sind:

- ✔ Indem Sie die Dateien in fremde Hände geben, geben Sie ein Stück der Kontrolle ab.
- ✔ In Bezug auf Sicherheit, Leistung und Kosten sind Sie vom Anbieter abhängig.
- ✔ Sie sind auf die Verfügbarkeit einer stabilen Internetverbindung mit einer ausreichenden Bandbreite angewiesen.

Um die Risiken zu minimieren, empfehlen wir Ihnen, Ihre Anforderungen an einen Cloud-Anbieter so genau wie möglich zu definieren.

Die Optionen sind vielfältig und Sie müssen mehrere Faktoren bedenken: Verfügbarkeit, Funktionen und Sicherheit. Neben den großen amerikanischen Anbietern wie Microsoft, Google und Dropbox gibt es inzwischen auch vertrauenswürdige europäische Anbieter, die in punkto Datenschutz oft besser bewertet werden.

Cloud-Speicher – ein Ausblick

Für die Zukunft lässt sich mit großer Sicherheit sagen: Die Cloud wird weiterwachsen. Immer mehr digitale Dienste sind Cloud-basiert, manche mehr, manche weniger offensichtlich. Dazu gehören neben Datenspeichern auch Online-Kollaborationstools, Streaming-Dienste und Netzwerke.

Mit der Beliebtheit der Cloud-Speicher steigt auch ihre Attraktivität für Angreifer. Deshalb müssen die hochgeladenen Daten besonders gut geschützt werden.

Die Cloud ist aber nicht automatisch unsicher. Bei Speicherdiensten bestimmt der Standort der Anbieter maßgeblich das Schutzniveau und den (erlaubten) Umgang mit den gespeicherten Inhalten.

Vor der Auswahl einer Cloud sollten Sie sich über den Firmensitz und die Standorte der Rechenzentren informieren.

Am besten abgesichert sind Sie, wenn sich beides an einem Standort mit hohen Datenschutz-Standards befindet. Anbieter innerhalb der Europäischen Union haben dabei oft die Nase vorn.

Und natürlich können Sie auch selbst noch eine ganze Menge für den Schutz Ihrer Daten tun. Wie das ohne viel technisches Vorwissen möglich ist, lesen Sie in Kapitel 3. Zunächst aber erfahren Sie mehr über das Thema Datenschutz.

IN DIESEM KAPITEL

- Datenschutzgesetze und -regelungen
- Die Lage in verschiedenen Ländern, Regionen und Branchen
- Der Unterschied zwischen Vertraulichkeit und Integrität von Daten

Kapitel 2
Daten … und warum sie zu schützen sind

Wer sich mit Datenschutz beschäftigt, kommt schnell mit den ganz großen Themen in Berührung: Grundrechte, Privatsphäre, Freiheit, Demokratie. Um Sie nicht gleich zu erschlagen, fangen wir aber zum Einstieg etwas kleiner an und fragen zunächst: Was ist denn eigentlich Datenschutz?

Datenschutz ist im Duden definiert als »Schutz der Bürger[innen] vor unbefugter Speicherung und Weitergabe von Daten, die ihre Person betreffen«.

Es geht also darum, dass Informationen zu einer bestimmten Person im Spannungsfeld zwischen der Wahrung der Privatsphäre und der Deutung durch das Umfeld stehen. Denken Sie beispielsweise an die Adresse einer Person, die zwar privat ist, aber für die Zustellung von Briefen notwendigerweise verarbeitet werden muss.

Dieses Spannungsfeld wird durch Gesetze und Verordnungen reguliert. Und die lernen Sie im nächsten Abschnitt genauer kennen.

In diesem Kapitel erfahren Sie, auf welche Aspekte Sie dabei achten sollten. Bedenken Sie allerdings, dass wir Ihnen keine Rechtsberatung geben können, da wir einerseits keine Anwälte sind und andererseits beim Thema Datenschutz oft Details den Ausschlag geben. Für Ihren speziellen Anwendungsbereich sollten Sie sich individuell beraten lassen – zum Beispiel von einer Datenschutzbeauftragten oder einem Fachanwalt.

Besonders schützenswert: personenbezogene Daten

Das Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) am 25. Mai 2018 hat für viel Wirbel gesorgt. Gefühlt musste sich plötzlich jeder mit dem Thema Datenschutz auseinandersetzen. Viele waren verunsichert und empfanden das Thema als sehr belastend.

Ein Begriff stach in der ganzen Verunsicherung rund um die DSGVO besonders hervor: *personenbezogene Daten*.

Bereits im Bundesdatenschutzgesetz (BDSG) war die Verarbeitung von personenbezogenen Daten geregelt. Durch die neuen Maßnahmen, die die DSGVO vorschreibt, haben jedoch Informationen, mit denen sich eine Person eindeutig identifizieren lässt, noch weiter an Bedeutung gewonnen und müssen besonders geschützt werden.

Was genau sind nun personenbezogene Daten? Daten sind dann personenbezogen, wenn sie die Identifikation einer Person ermöglichen. Darunter fallen beispielsweise …

- ✔ Namen,
- ✔ Merkmale, die eindeutig zuzuordnen sind, wie eine E-Mail-Adresse, eine Postadresse oder eine Kennnummer im System, die für eine Person steht, und
- ✔ Merkmale, die für sich oder in Kombination die Identifikation ermöglichen.

Denken Sie an alle Informationen, welche die physische, physiologische, genetische, psychische, wirtschaftliche, kulturelle oder soziale Identität betreffen.

Der Umgang mit personenbezogenen Daten wird in Artikel 4 der DSGVO geregelt.

Wichtig: Es ist stets diejenige Person oder Stelle für den Schutz der Daten zuständig, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Anders gesagt:

Der Datenschutz muss von den Personen gewährleistet werden, die mit den gespeicherten Informationen arbeiten.

Der oder die Datenschutzbeauftragte (DSB) unterstützt Sie bei der Einhaltung der Datenschutzmaßnahmen und erstellt Risikoanalysen. Haftbar ist der DSB bei einem Datenschutzverstoß allerdings nicht.

Je größer eine Organisation ist, desto mehr Beteiligte müssen in die Datenschutz-Strategie eingebunden werden. Nur so können alle Prozesse und Speicherorte berücksichtigt werden. Datenschutz ist Teamsport!

Exkurs: Datenschutz im Privatleben

Auch abseits von Gesetzen, im privaten Bereich, muss der Datenschutz beachtet werden. Was viele nicht wissen: Etliche Dinge, die Sie mit Ihren Smartphones jeden Tag tun, erfordern eigentlich eine Einwilligung der Betroffenen, weil die AGB der Anbieter das so vorsehen. Damit wird die Verantwortung für die Datenverarbeitung auf die Anwender übertragen – was den meisten allerdings nicht bewusst ist.

Im Alltag ist das schwer umsetzbar, und solange sich niemand beschwert, sehen viele auch keinen Grund, etwas zu ändern. Deshalb wird der Datenschutz im privaten Miteinander leider oft als weniger wichtig angesehen. Einige Beispiele:

- ✔ **Telefonnummern** (oder Chat-Kontakte) sollten nur dann weitergegeben werden, wenn die betroffene Person zuvor eingewilligt hat.
- ✔ **Private Fotos** sollten keinesfalls ohne ausdrückliche Zustimmung der abgebildeten Personen in den sozialen Netzwerken geteilt werden.
- ✔ **Adressbücher** in Apps und Webseiten hochzuladen, die automatisiert nach Accounts von Kontakten suchen, ist besonders kritisch. Dazu gehören beispielsweise WhatsApp, LinkedIn oder Twitter. Diese Funktion darf – laut den AGB der Anbieter – ausschließlich mit Einwilligung aller Betroffener genutzt werden. Diese Voraussetzung kann in der Praxis kaum jemand erfüllen.

Beim Thema Datenschutz kann man als Einzelperson mit gutem Beispiel vorangehen, wirkungsvoll umsetzen lässt er sich aber nur gemeinschaftlich.

Unternehmen müssen Geschäftsgeheimnisse schützen

Für viele Unternehmen gibt es abseits der personenbezogenen Daten auch andere Informationen, die hohen Schutz benötigen. Denken Sie beispielsweise an die Rezepte eines Lebensmittelkonzerns, die Marktanalysen eines Investmentfonds oder die Erfindungen eines Industriekonzerns.

All diese Informationen müssen ebenfalls sorgfältig geschützt werden, da die Veröffentlichung oder der Verlust katastrophale Auswirkungen auf die Geschäftsfähigkeit hätten. Hier bewegen Sie sich thematisch allerdings nicht mehr im Rechtsrahmen der DSGVO, sondern im Bereich des *Geschäftsgeheimnisgesetzes* (GeschGehG).

Datenschutzgesetze

Datenschutzgesetze setzen einheitliche Standards, aus denen sich Handlungsanweisungen ableiten lassen – und zwar für beide Seiten: Verantwortliche und Betroffene.

Verantwortliche für den Datenschutz (zum Beispiel Datenschutzbeauftragte, Wirtschaftsjuristen und -juristinnen, Compliance-Beauftragte) erhalten durch Datenschutzgesetze Vorgaben und Rahmenbedingungen für die Erfüllung ihrer Aufgaben.

Betroffene bekommen durch Datenschutzgesetze die Sicherheit, dass ihre persönlichen Informationen sorgfältig verarbeitet werden. Außerdem ist es möglich, bei einem Verstoß vor Gericht sein Recht einzufordern.

Datenschutzgesetze sind die Grundlage für Sanktionsmaßnahmen wie Beschwerden, Klagen und Bußgelder.

Im nächsten Abschnitt finden Sie eine Auswahl internationaler Datenschutzgesetze. Natürlich können wir Ihnen hier keinen vollständigen Überblick über alle Regelungen auf der ganzen Welt bieten. Sie sehen aber, dass es bereits viele Regelungen gibt, die möglicherweise für Ihr Unternehmen relevant sind. Das ist vor allem dann der Fall, wenn Ihr Unternehmen international tätig ist. Oft geht es um die Verarbeitung personenbezogener Daten. Da so ein Vorgang auch geschieht, wenn zum Beispiel eine Webseite aufgerufen oder ein Online-Dienst genutzt wird, müssen sich auch Unternehmen aus den USA an die DSGVO halten, da sich

die betroffenen Nutzer in der EU befinden. Wenn ein europäisches Unternehmen die gesetzlich definierte Schwellengrenze von 50.000 kalifornischen Nutzern erreicht hat, muss es sich an die Vorgaben des CCPA halten. Einen Überblick über die relevanten Datenschutzgesetze finden Sie auf den nächsten Seiten.

Datenschutz-Grundverordnung der Europäischen Union

Die DSGVO ist eine Verordnung der Europäischen Union, die nach einer zweijährigen Übergangsphase am 25. Mai 2018 in Kraft getreten ist. Dazu musste die DSGVO in allen Mitgliedsstaaten in nationales Recht umgesetzt werden. In Deutschland ist so das *Bundesdatenschutzgesetz* (BDSG-neu) entstanden.

Die Ziele der Vorordnung sind:

- ✔ Den Datenschutz und das Recht auf Privatsphäre aller europäischen Bürgerinnen und Bürger zu stärken.
- ✔ Die Datenschutzgesetze in der EU zu vereinheitlichen.

Der Fokus liegt darauf, *wie genau* Unternehmen und Organisationen Daten von natürlichen Personen schützen müssen. Neben dem Schutz der Daten erhalten die Betroffenen aber auch neue Rechte:

- ✔ das **Auskunftsrecht,** das es jeder betroffenen Person gestattet, die über sie gespeicherten Informationen einzusehen;
- ✔ das **Recht auf Vergessenwerden**, das besagt, dass Betroffene von einem Anbieter oder einer Organisation verlangen können, die über sie gespeicherten personenbezogenen Daten zu löschen.

Data Protection Act 2018 des Vereinigten Königreichs

Der Data Protection Act ist die nationale Gesetzgebung für den Datenschutz im Vereinigten Königreich. Durch den Austritt Großbritanniens aus der Europäischen Union fallen Staatsangehörige Englands, Schottlands, Wales und Nordirlands nicht mehr in den Wirkbereich der EU-DSGVO. Dennoch hat das Parlament eine Regulierung geschaffen, die sich sehr eng an der europäischen Verordnung orientiert.

Hin und wieder wird der Data Protection Act auch als UK-DSGVO bezeichnet. Mit Ausnahme von Strafverfolgung und Nachrichtendiensten müssen sich Organisationen im Vereinigten Königreich bei der Verarbeitung personenbezogener

Daten weitgehend an dieselben Prinzipien halten wie Organisationen in den Mitgliedsstaaten der EU. Dadurch wird das Vereinigte Königreich von der EU-Kommission auch als sicheres Drittland mit einem angemessenen Datenschutzniveau angesehen.

California Consumer Privacy Act

Der California Consumer Privacy Act (CCPA) ist das erste große Datenschutzgesetz in den USA. Mit seinem Inkrafttreten haben kalifornische Bürgerinnen und Bürger fünf neue Rechte erhalten, die ihnen mehr Macht über die Verwendung ihrer persönlichen Informationen geben:

- ✔ Das Recht, eine Auskunft anzufordern.
- ✔ Das Recht, eine Kopie der Daten, die einen selbst betreffen, zu erhalten.
- ✔ Das Recht auf Löschung der Informationen.
- ✔ Das Recht, dem Verkauf personenbezogener Daten zu widersprechen.
- ✔ Das Recht, nicht diskriminiert zu werden.

Dem letzten Punkt kommt aufgrund zunehmender Automatisierung durch Algorithmen immer mehr Bedeutung zu.

An den CCPA müssen sich vor allem große Unternehmen halten, die Daten von mehr als 50.000 Kaliforniern verarbeiten.

Singapore Personal Data Protection Act

Der Singapore Personal Data Protection Act (PDPA) befasst sich hauptsächlich mit dem Schutz personenbezogener Daten. Darüber hinaus ermöglicht er der Einwohnerschaft Singapurs die Registrierung in einer sogenannten »Do Not Call«-Datenbank. Mit einem Eintrag meldet man sich von unerwünschten Telemarketing-Anrufen ab.

Lei Geral de Proteção de Dados in Brasilien

Personenbezogene Daten stehen auch beim LGPD im Mittelpunkt. So wird eine Zustimmung zur Datenerhebung verlangt (mit ähnlichen Ausnahmen wie bei der DSGVO). Die betroffenen Personen haben außerdem die Möglichkeit,

- ihre Dateien einzusehen,
- eine Korrektur zu verlangen,
- ihre Daten zu anderen Diensten umzuziehen.

Außerdem verlangt das LGPD, dass so wenig Daten wie möglich gesammelt werden.

Branchenspezifische Regelungen

Neben allgemeinen nationalen Datenschutzgesetzen gibt es auch Regelungen, die sich auf bestimmte Branchen beziehen.

Gesundheitswesen

Gesundheitsinformationen gehören laut DSGVO zu den besonders sensiblen personenbezogenen Daten. Deshalb muss dem Datenschutz im Gesundheitswesen besondere Beachtung geschenkt werden.

- Es dürfen ausschließlich Daten erhoben werden, die für die Behandlung notwendig sind.
- Jede Weitergabe an Dritte (beispielsweise Dienstleister für die Abrechnung oder Angehörige) ist nur nach ausdrücklicher Einwilligung zulässig.

Die Möglichkeiten für Daten-Missbrauch sind im Gesundheitsbereich extrem hoch, da Patienten über ihre Krankheitsgeschichte erpressbar sind. Auch Pharma-Unternehmen und Versicherungen haben großes Interesse an den Daten, was eine Regulierung notwendig macht.

Die Schweigepflicht von Ärztinnen und Ärzten ist ein wichtiger Aspekt des Datenschutzes.

Übrigens: In Kapitel 7 finden Sie ein Fallbeispiel für den Einsatz von Verschlüsselungssoftware in einer Arztpraxis.

Banken und Finanzsektor

Die Finanzbranche arbeitet mit personenbezogenen Daten, die ein hohes Missbrauchspotenzial bieten. Entsprechend stark ist diese Branche reguliert.

In der Europäischen Union machte zuletzt die neue *Zahlungsdiensterichtlinie* (Payment Service Directive 2 – besser bekannt unter dem Kürzel PSD2) Schlagzeilen. Seit dem 13. Januar 2018 bietet PSD2 mehr Sicherheit durch stärkere Kundenauthentifizierung (beispielsweise beim Online-Banking). Außerdem regelt die Richtlinie die Weitergabe von Kontodaten an Drittanbieter, die im Auftrag der Kontoinhaber Zahlungsströme analysieren.

In den USA gelten FINRA (betrifft den Wertpapierhandel an US-Börsen) und SOX (bestimmt die Verschlüsselung von Berichten von Unternehmen am US-Kapitalmarkt).

Telekommunikation

In absehbarer Zeit wird dieser Bereich EU-weit von der ePrivacy-Verordnung (ePVO) reguliert. Wann diese verabschiedet wird, ist aktuell noch unklar. Experten rechnen frühestens 2023 mit einem Inkrafttreten, doch dann wird es in Deutschland noch eine Übergangsfrist von 24 Monaten geben.

Doch auch schon vor dem Inkrafttreten der ePrivacy-Verordnung hat der Gesetzgeber in Deutschland eine einheitliche Regelung geschaffen, welche die Vorgaben im Bereich Datenschutz aus den Telemedien, der Telekommunikation, der DSGVO und der ePrivacy-Verordnung zusammenfasst: Das *Telekommunikations-Telemedien-Datenschutz-Gesetz* (TTDSG) gilt in Deutschland seit dem 1. Januar 2022.

Datenschutz versus Überwachung

Unter dem Stichwort *Crypto Wars* wird eine Reihe von politischen Bestrebungen zusammengefasst, die es seit vielen Jahren auf nationaler und internationaler Ebene gibt. Allen gemein ist, dass für Strafverfolgungsbehörden gesonderte Zugänge eingerichtet werden sollen, die es ermöglichen würden, verschlüsselte Nachrichten zu untersuchen.

Solche Sonderzugänge, auch Hintertüren genannt, hebeln die Privatsphäre der Nutzerinnen und Nutzer der jeweiligen Kommunikationsplattform aus und stehen dem Gedanken des Datenschutzes diametral gegenüber.

Auch wenn sich die bisherigen Bemühungen darauf konzentrieren, Kommunikationsdienste zu überwachen, sind auch ruhende Dateien in Gefahr. Die USA haben mit dem *CLOUD Act* bereits einen Rechtsrahmen geschaffen, der das

Durchsuchen von Cloud-Speichern erlaubt. In der Europäischen Union wird derzeit mit der *e-Evidence-Verordnung* eine ähnliche Regelung vorbereitet. Experten gehen davon aus, dass die Verordnung frühestens Ende 2022 durch das EU-Parlament und den Rat verabschiedet wird. Wann sie in Kraft tritt, ist derzeit noch nicht absehbar.

Datenschutz im Kontext von Wirtschaftsinteressen

Die Zeit, in der wir gerade leben, wird häufig als »Informationszeitalter« bezeichnet. Der Begriff spricht für sich, sind Informationen doch eines der wichtigsten Güter, die weltweit gewonnen, verarbeitet und gespeichert werden. Darunter fallen zum Beispiel Forschungsergebnisse, Geschäftsgeheimnisse oder gesammelte Informationen, die allein dadurch wertvoll werden, dass es so viele von ihnen gibt, Stichwort: Big Data.

Der Wert dieser Informationen bemisst sich daran, wer darauf zugreifen kann und in der Lage ist, sie auszuwerten. Einige Beispiele:

- ✔ Unternehmen sichern ihre Daten gegen Industriespionage ab, um der Konkurrenz keinerlei Wissensvorsprung zu gewähren.
- ✔ Eine Kundendatenbank mit Kreditkarteninformationen ist für Hacker hochinteressant, weil die Zahlungsinformationen auf dem Schwarzmarkt viel Geld einbringen können.
- ✔ Geheimdienste interessieren sich besonders für die internationale Chat-Kommunikation von Terroristen.

Der Datenschutz befindet sich im Spannungsfeld der Interessen verschiedener Akteure. Dass diese Interessen grundsätzlich legitim sein können (Beispiel Terrorabwehr), darf jedoch nicht die generelle Aushebelung des Rechts auf Privatsphäre zur Folge haben.

Vertraulichkeit

Ein Schutzziel von Informationssicherheit ist die Vertraulichkeit. Diese wird dadurch hergestellt, dass zu jedem Zeitpunkt nachvollziehbar festgelegt ist, welche Personen Zugriff auf schützenswerte Dateien haben. In der Regel wird dies durch automatisierte Systeme im Hintergrund gewährleistet.

Die Herausforderung besteht darin, die Authentifizierung der berechtigten Personen fälschungssicher zu ermöglichen. Stellen Sie sich dieses System als die virtuelle Version des Pförtners vor, der den Eingang des Betriebsgeländes kontrolliert und notiert, wer zu welchem Zeitpunkt kommt und geht.

Integrität

Neben der Vertraulichkeit fällt auch die Integrität der Daten in den Bereich Datenschutz. Der Schutz gegen Manipulation ist ebenso wichtig, wie der Schutz vor unerlaubtem Zugriff. Nur wenn Daten vor Manipulation geschützt sind, bleibt ihr Wert erhalten.

Das Erkennen von Datenmanipulation sollte ein wichtiger Bestandteil Ihrer Datenschutzstrategie sein.

Verfügbarkeit

Daten sind nur dann gut geschützt, wenn sie im geplanten Umfang zuverlässig erreichbar sind, also für berechtigte Personen zum gewünschten Zeitpunkt. Dies ist durch Compliance-Richtlinien geregelt und wird automatisiert gesteuert.

Auch der Schutz gegen Systemausfälle im Rechenzentrum gehört in den Bereich der Verfügbarkeit. Cloud-Anbieter geben hier in der Regel hohe Garantien und schützen die Daten durch Backups und Gebäudeschutz-Systeme.

Eine weitere Bedrohung für die Verfügbarkeit sind Cyberkriminelle, die Dateien löschen oder verschlüsseln und somit den Zugriff durch die rechtmäßigen Eigentümerinnen und Eigentümer verhindern. Das ist eine beliebte Masche von Erpressern, die sich mit sogenannter *Ransomware* Zugriff auf ein System verschaffen. Die Dateien stehen dem angegriffenen Unternehmen oder der Behörde dann erst wieder zur Verfügung, wenn ein Lösegeld gezahlt oder die Schadsoftware entfernt wurde.

Geschäftsgeheimnis versus öffentliches Interesse

Whistleblowing beschreibt den Prozess, dass Insider über Missstände berichten, um die Öffentlichkeit in Kenntnis zu setzen. Beispiele für solche Missstände sind

Straftaten wie Korruption, Insiderhandel, Menschenrechtsverletzungen oder Datenmissbrauch.

Obwohl sie in der Öffentlichkeit oft als Helden gefeiert werden, laufen die Hinweisgeber Gefahr, ihren Job und ihr soziales Netz zu verlieren, weil sie durch die gegenwärtige Rechtsprechung nicht gut geschützt sind.

Prominente Whistleblower sind der ehemalige US-Geheimdienstmitarbeiter Edward Snowden und die ehemalige US-Soldatin Chelsea Manning. Beide haben hohe persönliche Opfer gebracht.

Die Europäische Union hat mit der *Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden*, verbindliche Rahmenbedingungen geschaffen. Deutschland wird dafür kritisiert, dass es die Richtlinie bisher nicht in nationales Recht umgesetzt hat.

Wie Sie sehen, ist die Gesetzeslage rund um den Datenschutz ständig im Fluss. Hier am Ball zu bleiben, ist eine große Herausforderung. Die technischen Grundprinzipien für den Schutz der gespeicherten Informationen ändern sich jedoch nicht so schnell. Lesen Sie im nächsten Kapitel die Details dazu.

IN DIESEM KAPITEL

- Datenschutz und Datensicherheit
- Den Verlust von Daten verhindern
- Daten vor unbefugtem Zugriff schützen

Kapitel 3
Daten … und wie sie zu schützen sind

Datensicherheit und Datenschutz werden im allgemeinen Sprachgebrauch oft synonym verwendet. Die beiden Bereiche gehen zwar tatsächlich Hand in Hand, allerdings gibt es klare Unterschiede. Der Unterschied wird durch die jeweils zugrundeliegende Fragestellung deutlich:

- ✔ **Datensicherheit**: Welche Maßnahmen müssen ergriffen werden, um alle Daten des Unternehmens vor Verlust, Zerstörung, Diebstahl oder sonstigen Gefahren zu schützen?
- ✔ **Datenschutz**: Dürfen *personenbezogene* Daten erhoben werden und wie können diese Daten nach aktueller Rechtslage verarbeitet, gespeichert oder genutzt werden?

Sowohl der Bereich Datensicherheit als auch der Datenschutz befassen sich mit Maßnahmen, die getroffen werden müssen, um den Schutz von Daten zu gewährleisten.

Die beiden Bereiche können sich aber auch in die Quere kommen. Ein Beispiel: Als Maßnahme für die *Datensicherheit* wird in Ihrem Unternehmen ein Backup erstellt. Als Speicherort wird ein Cloud-Speicher gewählt. Die Speicherung der Daten in einer Cloud schwächt jedoch den *Datenschutz*, da die Daten an den Cloud-Speicher-Anbieter übermittelt werden und nun auf einmal deutlich mehr Personen Zugriff auf die Daten haben. Wie Sie dieses Dilemma lösen, erfahren Sie in Kapitel 5.

Bewährte Maßnahmen und Technologien

Eines vorweg: Wenn Sie die Vorzüge des Cyber-Zeitalters nutzen möchten, ist eine hundertprozentige Abwehr aller Gefahren nicht möglich.

So hat die Nutzung eines Cloud-Speichers für Unternehmen zahlreiche Vorteile, wie Sie in Kapitel 1 nachlesen können. Doch gleichzeitig müssen sich Security-Manager bei Einführung einer Cloud neuen Risiken stellen, die durch eine Abhängigkeit vom Cloud-Speicher-Anbieter in puncto Sicherheit, Leistung und Kosten hervorgerufen werden.

Insbesondere bei neuen Techniken, beispielsweise dem Internet of Things (Internet der Dinge), das eine Vernetzung von physischen und virtuellen Geräten ermöglicht, lassen sich die zum Teil noch unbekannten Risiken nicht vollständig erfassen. Deshalb ist es wichtig, dass Sie die verschiedenen Risiken bewerten und Maßnahmen ergreifen, um Gefahren zu minimieren.

Speziell für den Datenschutz werden in der Europäischen Datenschutz-Grundverordnung »geeignete technische und organisatorische Maßnahmen« (sogenannte TOMs) nach Artikel 32 genannt. Je sensibler die Informationen, umso wichtiger sind geeignete TOMs.

Technische Maßnahmen

Beispiele für technische Maßnahmen sind:

- ✔ Alarmanlagen, Videoüberwachung oder Sicherheitspersonal als physischer Schutz vor Zutritt von unbefugten Personen
- ✔ Sicherheitskopien und Backups, um Daten im Notfall wiederherstellen zu können
- ✔ Firewalls, um Angreifern das Eindringen in das Netzwerk zu erschweren
- ✔ Benutzerkonten mit Passwort, damit nur autorisierte Personen Zugang zu Unternehmens-Hardware oder Software haben.

Organisatorische Maßnahmen

Beispiele für organisatorische Maßnahmen sind:

- ✔ Sensibilisierung und Schulung von Angestellten
- ✔ Benennung eines Ansprechpartners für Notfälle oder Datenschutzfragen
- ✔ Dokumentation und Regulierung des Zugriffs auf Informationen.

Zwei TOMs hebt die DSGVO als vorgesehene Methoden zum Schutz personenbezogener Daten vor Missbrauch hervor. In der Verordnung werden diese in Artikel 32 direkt an erster Stelle in Absatz 1 genannt: *Pseudonymisierung* und *Verschlüsselung*. In den nächsten beiden Absätzen erklären wir Ihnen diese beiden Themen genauer. Und weil es so gut passt, auch gleich die *Anonymisierung*.

Personenbezug mit Pseudonymisierung und Anonymisierung verschleiern

Die beiden Methoden der Pseudonymisierung und Anonymisierung können Daten schützen, ohne sie zu verschlüsseln. Sie eignen sich aber nur für bestimmte Anwendungsfälle.

Pseudonymisierung begegnet uns im Alltag zum Beispiel bei einem Buch, das vom Autor unter einem Fantasienamen veröffentlicht wurde. Das ist eine gute Möglichkeit, die wahre Identität zu verheimlichen.

In der Datenschutz-Praxis wird bei Pseudonymisierung das identifizierende Merkmal (beispielsweise der Name oder die E-Mail-Adresse) durch einen Platzhalter, das Pseudonym, ersetzt. Das kann ein Zahlencode oder eine Buchstabenkombination sein. So kann mit den Datensätzen gearbeitet werden, ohne dass bekannt ist, um welche Personen es sich handelt. Ein gutes Beispiel dafür ist die Forschung in den Bereichen Medizin oder Sozialwissenschaft.

Je nachdem wie detailliert ein Datensatz ist und in welchem Kontext die Daten stehen, kann ein Rückschluss auf die Person möglich sein. Dies lässt sich dadurch erschweren, dass man die verschiedenen Informationen getrennt voneinander speichert. Absolute Sicherheit

gibt es hier aber nicht. Durch geschicktes Kombinieren oder durch Verwendung des Pseudonymisierungsschlüssels ist eine Zuordnung der Daten zu einer Person jederzeit möglich.

Im Gegensatz zur Pseudonymisierung stellt die *Anonymisierung* von Daten die dauerhafte und unumkehrbare Beseitigung des Personenbezugs dar.

Ein gutes Beispiel dafür sind die Wahlzettel bei einer geheimen Abstimmung. Man kann zwar nachvollziehen, *wer* eine Stimme abgegeben hat, aber nicht *welche*, weil die Stimmabgabe und die Stimmauswertung nicht miteinander verknüpft sind.

Erfolgreich anonymisierte Daten sind keine personenbezogenen Daten mehr, da der *Bezug* zu einer bestimmten Person nicht mehr gegeben ist. Die Verarbeitung dieser Daten fällt also nicht mehr in den Anwendungsbereich der DSGVO.

Inhalte durch Verschlüsselung schützen

Erinnern Sie sich an Ihre Schulzeit, als Sie während der nicht enden wollenden Geschichtsstunde versucht haben, eine Nachricht an den besten Freund vier Reihen weiter vorn zu übermitteln? Ein kleiner Zettel musste dazu unauffällig durch viele Hände wandern. Aber wie konnten Sie sicherstellen, dass die Überbringer in den Reihen dazwischen die Nachricht nicht lesen? Eine gute Methode ist das Austauschen von Buchstaben. Nur Sie und Ihr bester Freund kannten den Schlüssel und wussten, was man tun muss, um die »verschlüsselte« Nachricht zurückzuübersetzen.

Auch wenn die Zettel heute aus der Mode gekommen sind und Schülerinnen und Schüler lieber mithilfe von Chat-Apps kommunizieren – das Prinzip ist das Gleiche: Nur Sender und Empfänger können den Klartext der Nachricht lesen.

Unter *Verschlüsselung* versteht man die Umwandlung eines Klartextes in einen Geheimtext. Dafür wird ein Schlüssel verwendet. Die Ausgangsinformationen können nur unter Verwendung des passenden Gegenstücks (meist der gleiche Schlüssel) wieder lesbar gemacht werden.

Warum verschlüsselt man also? Auf diese Frage gibt es gleich mehrere Antworten: Verschlüsselung …

- ✔ … schützt personenbezogene Daten auf dem Transportweg.
- ✔ … sichert Daten am Speicherort ab.
- ✔ … schließt Personen ohne Berechtigung vom Zugriff aus.
- ✔ … minimiert das Missbrauchsrisiko.

Ob Verschlüsselung Daten zuverlässig schützt, hängt entscheidend von der Stärke des verwendeten Algorithmus und der Zufälligkeit des Schlüssels ab. Damit Sie das gut einschätzen können, stellen wir Ihnen in Kapitel 4 die verschiedenen Algorithmen vor.

Im Sinne der DSGVO ist eine Verschlüsselung dann als TOM geeignet, wenn sie dem »Stand der Technik« (DSGVO, Artikel 32) entspricht. Dazu muss ein moderner und sicherer Algorithmus verwendet werden. Ist dies der Fall, dann bietet sich Verschlüsselung als eine geeignete technische Maßnahme an,

- ✔ um Datenschutzvorschriften gerecht zu werden,
- ✔ um Datenpannen mit personenbezogenen Daten vorzubeugen,
- ✔ um die Datensicherheit im Unternehmen zu stärken und
- ✔ um alle Daten zu schützen.

In den folgenden Kapiteln zeigen wir, wie Verschlüsselung funktioniert, was sie bezwecken soll und wie sie heutzutage eingesetzt wird.

Teil II
Verschlüsselung

IN DIESEM TEIL ...

In diesem Teil definieren wir Verschlüsselung und stellen die verschiedenen Anwendungsbereiche vor. Sie lernen Grundbegriffe kennen und verstehen, warum Verschlüsselung nicht gleich Verschlüsselung ist. Außerdem betrachten wir die Vor- und Nachteile der verschiedenen Verschlüsselungsverfahren. Wir definieren die Unterschiede von soft- und hardwaregestützter Verschlüsselung sowie von Open- und Closed-Source-Software.

IN DIESEM KAPITEL

- Definition von Verschlüsselung
- Verschlüsselungsverfahren und ihre Vor- und Nachteile
- Der Umgang mit privaten und öffentlichen Schlüsseln

Kapitel 4
Verschlüsselung … und wie sie funktioniert

Bevor wir nun tiefer in das Thema Verschlüsselung einsteigen, werden wir kurz klären, was Verschlüsselung eigentlich ist.

Verschlüsselung ist ein Verfahren, bei dem mithilfe eines Schlüssels lesbarer Klartext in unverständlichen Geheimtext umgewandelt wird.

Doch halt, eine verschlüsselte Botschaft muss auch wieder lesbar gemacht werden können:

Entschlüsselung beschreibt die Umwandlung von Geheimtext in lesbaren Klartext. Sie kann nur mit dem passenden Schlüssel durchgeführt werden.

Vorläufer: die ersten Verschlüsselungsverfahren

Verschlüsselungsverfahren werden dazu benutzt, Informationen vertraulich zu übermitteln. Sie kommen bereits seit vielen hundert Jahren zum Einsatz, allerdings mit ganz anderen Methoden, als sie heute genutzt werden.

Wir betrachten zum Einstieg in das Thema Verschlüsselung ein Verfahren, das gar keine Verschlüsselung im eigentlichen Sinn ist, die Funktionsweise aber verdeutlicht: die sogenannte *Cäsar-Chiffre*. Hier wird jeder Buchstabe durch einen anderen ersetzt. Aus einem A wird beispielsweise immer ein D und aus einem M immer ein P. Es handelt sich hierbei um eine Verschiebung um 3 Buchstaben.

In Abbildung 4.1 können Sie es einmal ausprobieren.

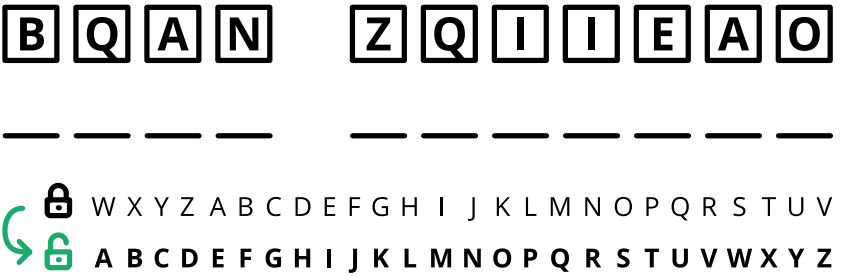

Abbildung 4.1: Cäsar-Chiffre

Die *Rotations-Chiffre* ist die Weiterentwicklung der Cäsar-Chiffre und erlaubt eine freie Wahl der Anzahl der Verschiebungen. Bei beiden Verfahren ist die Gefahr sehr hoch, dass Unbefugte die Anzahl der Verschiebungen herausfinden. Der Klartext wäre somit schnell einsehbar. Gelingt dies, spricht man von einer *geknackten Verschlüsselung*.

Wer die häufigsten Buchstaben der verwendeten Sprache kennt (in Deutsch wäre das beispielsweise das E), kann diese Art Verschlüsselung innerhalb von Minuten knacken. Dazu benötigt man nur Zettel und Stift. Deshalb eignet sich dieses Verfahren höchstens für die Schatzsuche beim Kindergeburtstag.

Sichere Verschlüsselungsverfahren

Ein sicherer Verschlüsselungsalgorithmus ist komplex und lässt sich nicht mehr durch die Anzahl von Buchstabenverschiebungen darstellen.

Heutige Verschlüsselungs*verfahren* werden bewusst *nicht* geheim gehalten, sodass eine große Anzahl an Fachleuten sie überprüfen kann. Dadurch geht man sicher, dass sie keine Schwachstellen enthalten. Erst dann werden sie zum Standard erklärt. Die Verschlüsselungs*schlüssel* sind jedoch höchst vertraulich!

Zwei Dinge sind also wichtig, damit eine Verschlüsselung sicher ist:

1. ein Algorithmus (öffentlich bekannt),
2. ein Schlüssel (geheim).

Wie genau diese beiden Komponenten zusammenspielen, erfahren Sie gleich. Zunächst leiten wir dieses komplexe mathematische Thema mit einem Bild ein, das die Wirkung von Verschlüsselung zeigt. In Abbildung 4.2 sehen Sie, wie ein mit modernen Algorithmen verschlüsselter Text aussehen könnte.

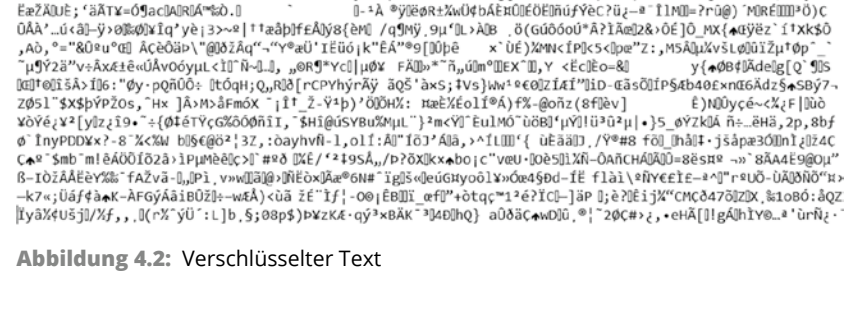

Abbildung 4.2: Verschlüsselter Text

Verschlüsselungsverfahren unterscheiden sich dadurch, ob sie *symmetrisch*, *asymmetrisch* oder *hybrid* verschlüsseln. In diesem Kapitel lernen Sie diese Verfahren und ihre jeweiligen Vor- und Nachteile kennen.

Symmetrische Verschlüsselung

»Symmetrische Verschlüsselung« beschreibt ein Verfahren, bei dem es *einen* Schlüssel gibt, der gleichermaßen ver- und entschlüsselt. Und das ist auch schon der wichtigste Punkt bei diesem Verfahren, denn der Schlüssel, mit dem die Nachricht verschlüsselt wurde, muss zusätzlich zur Nachricht ebenfalls übermittelt werden. In der Praxis wird dieses Verfahren kaum verwendet. Es ist aber ein wichtiger Bestandteil der hybriden Verschlüsselung, die Sie im nächsten Abschnitt kennenlernen und deshalb wichtig für das Verständnis.

Im Jahr 1997 hatte das US-amerikanische *National Institute of Standards and Technology* (NIST) die Suche nach einem neuen Verfahren für symmetrische Verschlüsselung ausgeschrieben. Man brauchte einen *Advanced Encryption*

Standard (AES). Ins Finale kamen die Algorithmen *MARS, RC6, Twofish, Serpent* und *Rijndael*. Letzterer setzte sich am Ende als neuer Standard durch.

Der von Joan Daemen und Vincent Rijmen entwickelte Algorithmus kann mit unterschiedlicher Bit-Länge verwendet werden und heißt deshalb entweder *AES-128*, *AES-192* oder *AES-256*. Je höher die Anzahl an Bits, desto mehr Runden durchläuft er. Mit jedem zusätzlichen Schlüssel-Bit steigt die Komplexität. Das bedeutet: Der Schlüsselraum wird größer und ein Angriff, bei dem die verschiedenen Schlüsseloptionen durchprobiert werden, dauert länger. Bereits bei AES-128 würde dies mehr Zeit in Anspruch nehmen, als das Universum alt ist.

Symmetrische Verschlüsselung zusammengefasst:

- ✔ **Vorteil**: Symmetrische Verschlüsselung zeichnet sich durch eine besonders schnelle Verarbeitung aus und benötigt vergleichsweise wenig Rechenleistung.
- ✔ **Nachteil**: Die Schlüsselübergabe ist ein Problem, denn sie sollte verständlicherweise nicht gemeinsam mit der Nachricht übermittelt stattfinden. Ein Angreifer, der die Nachricht abfängt, könnte sonst die Inhalte sofort lesen.

Das Problem der Schlüsselübergabe wird deshalb durch die Kombination mit anderen Verschlüsselungsverfahren gelöst. Wie das funktioniert, erfahren Sie gleich.

Asymmetrische Verschlüsselung

Im Gegensatz zu symmetrischer Verschlüsselung brauchen die kommunizierenden Parteien bei asymmetrischer Verschlüsselung keinen gemeinsamen geheimen Schlüssel. Jeder erzeugt sein eigenes Schlüsselpaar, das aus einem öffentlichen und einem geheimen Teil besteht.

Den »öffentlichen Schlüssel« muss man sich wie ein Vorhängeschloss vorstellen. Wichtigste Eigenschaft: Es kann von jeder beliebigen Person verschlossen werden. Aber nur mit dem passenden »privaten Schlüssel« aus dem selbst erzeugten Schlüsselpaar kann man es auch wieder öffnen. Möchte Person A eine Nachricht verschlüsseln, nimmt sie sich eines der »Vorhängeschlösser« von Person B und sichert die Botschaft damit ab.

Der wichtigste asymmetrische Verschlüsselungsalgorithmus und aktueller Standard ist das Kryptosystem RSA, das nach seinen Erfindern Ronald L. Rivest, Adi Shamir und Leonard Adleman benannt ist.

Asymmetrische Verschlüsselung zusammengefasst:

- ✔ **Vorteil**: Es sind zwei Schlüssel für die Entschlüsselung nötig und der eigene geheime Schlüssel muss nicht an den Empfänger kommuniziert werden.
- ✔ **Nachteil**: Die hohe Sicherheit geht auf Kosten der Geschwindigkeit, denn für dieses Verfahren wird viel Rechenleistung benötigt. Asymmetrische Verschlüsselung ist daher nur für kleine Datenmengen geeignet.

Hybride Verschlüsselung

Diese Methode ist eine Kombination aus symmetrischer und asymmetrischer Verschlüsselung. Hier kommen *zwei verschiedene* Schlüssel zum Einsatz.

Bei hybrider Verschlüsselung wird die Datei mit einem symmetrischen Schlüssel (beispielsweise AES) verschlüsselt und dieser Schlüssel wiederum mit einem asymmetrischen Schlüssel (beispielsweise RSA) verschlüsselt. Danach wird der asymmetrisch verschlüsselte, symmetrische Schlüssel zum Beispiel an die Datei angehängt. Dazu muss jede kommunizierende Partei ein eigenes Schlüsselpaar erzeugen, das jeweils aus einem *öffentlichen* und einem *geheimen* Schlüssel besteht.

Dieser Ablauf erlaubt auch die Verschlüsselung großer Datenmengen (ab mehreren hundert Bytes), da das asymmetrische Verschlüsselungsverfahren nur für den (vergleichsweise kleinen) Schlüssel genutzt wird und nicht für die gesamte Datei.

Einsatzgebiete sind beispielsweise das Netzwerkprotokoll TLS oder das Protokoll zur E-Mail-Verschlüsselung PGP. Das funktioniert dann so, dass beispielsweise Journalisten, die vertrauliche Informationen entgegennehmen, ihren öffentlichen PGP-Schlüssel zur Verfügung stellen. So kann man ihnen verschlüsselte E-Mails schicken.

Eine neue Entwicklung im Bereich der hybriden Verschlüsselung ist die Verwendung von *Elliptic Curve Cryptography* (ECC). Dieser asymmetrische Verschlüsselungsalgorithmus ist moderner als RSA, schneller und für manche Anwendungsfälle besser geeignet. Er basiert auf mathematischen Operationen auf elliptischen Kurven. ECC wird bereits als Nachfolger für RSA empfohlen.

Hybride Verschlüsselung zusammengefasst:

- ✔ **Vorteil**: Der hybride Ansatz löst das Schlüsselverteilungsproblem unter der Voraussetzung, dass die kommunizierenden Parteien ihre öffentlichen Schlüssel bereits ausgetauscht haben. Ein weiterer Vorteil ist, dass eine

verschlüsselte Datei weiteren Empfängern und Empfängerinnen zugänglich gemacht werden kann, ohne dass die komplette Datei neu verschlüsselt werden muss.

✔ **Nachteil**: Hybride Verschlüsselung ist sehr komplex und deshalb fehleranfällig.

Um die Sicherheit der verschiedenen Verschlüsselungsverfahren einschätzen zu können, finden Sie in Tabelle 4.1 eine Übersicht. Diese zeigt, wie lange es dauern würde, mit einem sogenannten *Brute-Force-Angriff* die jeweilige Verschlüsselung zu knacken. Bei dieser Art von Angriff werden alle potenziellen Lösungen (Schlüssel) probiert – bis der richtige gefunden ist. Bei der Berechnung der Zeit gehen wir hier von der Rechenleistung des derzeit schnellsten Superrechners aus, dem »Fugaku« in Japan.

Verschlüsselungsalgorithmus	Dauer
Rotations-Chiffre	Wenige Millisekunden
56 Bit (DES)	3 Minuten
128 Bit (AES)	24 Billiarden Jahre
256 Bit (AES)	8 Nonillion Jahre

Tabelle 4.1: Vergleich der Sicherheit von Verschlüsselungsalgorithmen

Zum Vergleich: Das Universum ist etwa 13,8 Milliarden Jahre alt.

Key Management

Möglicherweise haben wir Sie mit den Schlüsselpaaren rund um den privaten und den öffentlichen Schlüssel nun etwas verwirrt. Das Thema ist tatsächlich komplex und man kann es sich schwer vorstellen. Doch keine Sorge: In der Praxis spielen die verschiedenen Schlüssel für Sie keine große Rolle, denn die Verwaltung der Schlüssel (das sogenannte Key Management) übernimmt die jeweilige Verschlüsselungssoftware. Die Anwender der Verschlüsselungssoftware bekommen von dem Schlüsselaustausch nichts mit.

Im nächsten Abschnitt widmen wir uns wieder alltagspraktischen Fragen und klären, *wo genau* Verschlüsselung eingesetzt wird.

IN DIESEM KAPITEL

- Anwendungsbereiche von Verschlüsselung
- Verschiedene Arten von Verschlüsselungssoftware
- Wichtige Fragen identifizieren

Kapitel 5
Verschlüsselung … und wie sie eingesetzt wird

Verschlüsselung wurde lange Zeit vor allem von Geheimdiensten, militärischen Einheiten oder von Personen mit kriminellen Absichten genutzt. Im Ersten und Zweiten Weltkrieg kam es zu einem Wettkampf zwischen den Kryptografen. Sie entwickelten neue Verschlüsselungsmethoden und bemühten sich, den Kryptoanalytikern zuvorzukommen, deren Ziel es war, die neuen Methoden so schnell wie möglich zu knacken. Das Können dieser Experten verschaffte ihren Regierungen bedeutende Vorteile in der Kommunikation und beeinflusste das Kriegsgeschehen enorm.

Die deutsche Wehrmacht setzte im Zweiten Weltkrieg die Rotor-Schlüsselmaschine ENIGMA ein. Die maschinelle Verschlüsselung war damals neu und galt als sicher. Durch die Erfindung der »Turing-Bombe« war es den Alliierten jedoch möglich, fast alle deutschen Funksprüche zu entziffern.

Heutzutage ist Verschlüsselung allgegenwärtig und aus unserem Leben nicht mehr wegzudenken. Zu verdanken ist dies unter anderem dem Physiker Phil Zimmermann, der 1991 eine Standardmethode zur Verschlüsselung von E-Mails entwickelte: Pretty Good Privacy, kurz PGP.

Im Vergleich zu früheren Verschlüsselungsmethoden kann PGP, unabhängig vom jeweils genutzten E-Mail-System, für die Transport- und auch für die Speicherverschlüsselung eingesetzt werden. Da sowohl symmetrische als auch asymmetrische Verschlüsselungsverfahren zum Einsatz kommen, handelt es sich bei PGP um eine hybride Verschlüsselung.

Doch nicht nur Ihre E-Mails sind verschlüsselt. Auch andere Plattformen, die Sie täglich verwenden, nutzen verschlüsselte Kommunikation:

- ✔ Videokonferenzen,
- ✔ Messenger-Dienste,
- ✔ Speichermedien,
- ✔ Rechenzentren.

Im Alltag ergeben sich unterschiedliche Anforderungen an Verschlüsselungslösungen, und zwar im Privatleben ebenso wie in Unternehmen. Je nach Anwendungsfall ist eine andere Strategie nötig. Auf den nächsten Seiten erhalten Sie die Informationen, die Sie brauchen, um die passende Strategie festzulegen.

Warum der Status einer Datei für ihre Verschlüsselung entscheidend ist

Für die Wahl der Verschlüsselung ist es relevant, was mit den Dateien in dem Moment geschieht, wo sie verschlüsselt werden: nichts, eine Übertragung oder eine Bearbeitung.

Dateien, die »nur so herumliegen« – beispielsweise auf einer Festplatte oder als Backup in einem Cloud-Speicher – bezeichnet man als *Data at Rest*. Diese Daten können durch Zugangskontrolle und Verschlüsselung gesichert werden. Im besten Fall verwendet man beides.

Transportverschlüsselung wird für *Data in Transit* verwendet und funktioniert wie ein gepanzerter Geldtransporter: Die Daten sind während der Übertragung geschützt. Vor dem Versand (auf dem Endgerät) und nach dem Versand (auf dem Server im Rechenzentrum) sind sie allerdings im Klartext gespeichert.

Das *https-Protokoll*, mit dem Daten zwischen Geräten und Webseiten übertragen werden, ist ein gutes Beispiel für Transportverschlüsselung. Sie erkennen es daran, dass eine URL mit der Zeichenfolge »*https://*« beginnt.

Besonders anspruchsvoll wird es, wenn Daten *während* der Nutzung, beispielsweise ein Dokument in einem Textbearbeitungsprogramm, durchgängig verschlüsselt bleiben sollten, also während sie verändert werden.

Die softwarebasierte Verschlüsselung von *Data in Use* ist sehr kompliziert, weil die üblichen Bearbeitungsfunktionen für verschlüsselte Dateien genauso funktionieren sollen, wie die Nutzer es bei unverschlüsselten Dateien gewohnt sind. Gleichzeitig soll der Inhalt der Datei aber geheim bleiben. Puh!

Mit dem Problem der Verschlüsselung während der Bearbeitung befasst sich das Forschungsfeld der *homomorphen Verschlüsselung*. Bei dieser speziellen Art der Verschlüsselung werden Berechnungen auf den Geheimtext durchgeführt, die den mathematischen Operationen auf den entsprechenden Klartext entsprechen. Dabei ist der Klartext aber nicht bekannt und wird auch nicht entschlüsselt. Dieses Verfahren findet derzeit aufgrund der Komplexität und fehlenden Marktreife noch keinen Einsatz, könnte aber in Zukunft im Bereich Cloud-Computing eine Rolle spielen.

In der Praxis wählt man meist einen anderen, einfacheren Weg: die hardwareseitige Abschottung des Bereiches, in dem die Daten bearbeitet werden. Verschlüsselung von *Data in Use* ist also nicht zwingend notwendig, wenn die Bearbeitung auf einem Endgerät stattfindet – also außerhalb der Cloud.

Daten sollten zumindest im Ruhezustand und während einer Übertragung *immer* verschlüsselt sein. Von der Bearbeitung unverschlüsselter Daten raten wir vor allem in reinen Online-Anwendungen (zum Beispiel Google Docs) ab.

Verschlüsselung in der Cloud

Da immer mehr Daten über das Internet ausgetauscht werden, wächst das Interesse an Verschlüsselung – vor allem an Verschlüsselung für Dateien, die das eigene Netzwerk verlassen.

Standardfunktionen, wie zum Beispiel die Verschlüsselung der Übertragung von Informationen zwischen dem eigenen Endgerät und einer Webseite (oder einem Cloud-Speicher) werden mittlerweile von allen Anbietern mit Transportverschlüsselung versehen. Diese sichert allerdings nur die Übertragung selbst ab, nicht die gespeicherten Daten vor und nach dem Transport.

Viele Online-Dienste führen zusätzlich die Verschlüsselung der ruhenden Daten durch. Dies wird in einem zweiten, von der Transportverschlüsselung unabhängigen Rechenprozess durchgeführt.

Diese Art der Verschlüsselung schützt allerdings nur vor bestimmten Angriffen:

- ✔ Cyberkriminelle, die sich Zugriff auf das Rechenzentrum und die dort gespeicherten Daten verschaffen, können ohne die dazugehörigen Schlüssel nichts mit den Dateien anfangen.
- ✔ Falls der Datenverkehr zwischen dem Endgerät und dem Rechenzentrum abgehört wird, sind die erhaltenen Informationen ohne die dazugehörigen Schlüssel wertlos.

Die Verschlüsselung der ruhenden Daten schützt allerdings nicht vor Zugriff durch den Cloud-Speicher-Anbieter selbst.

Szenarien, mit denen Sie sich auseinandersetzen müssen, sind:

- ✔ Hochgeladene Dateien werden vom Cloud-Anbieter zu Forschungszwecken oder zum Trainieren von künstlicher Intelligenz gescannt und ausgewertet.
- ✔ Bei Anfragen durch Behörden sind die Cloud-Speicher-Anbieter gezwungen, die Informationen herauszugeben. Besonders in den USA ist dies durch den CLOUD Act vergleichsweise einfach.
- ✔ Angestellte der Cloud-Speicher-Anbieter verschaffen sich Zugang zu den gespeicherten Dateien und dem Schlüssel.
- ✔ Cyberkriminelle übernehmen den Server des Cloud-Anbieters. Während dort die empfangenen Dateien von Transport- auf »at-rest«-Verschlüsselung umgeschlüsselt werden, kann die Information einen Moment lang unverschlüsselt gelesen werden.

Das Versprechen, dass Ihre Daten während der Übertragung und auf fremden Servern verschlüsselt sind, reicht nicht aus. Wer auch immer die Schlüssel hat, kann frei darauf zugreifen.

Die Verschlüsselung von Daten während der Übertragung und bei der Speicherung ist also kein echtes Sicherheitsversprechen. Informationen können an den beiden Enden des Transportweges und von den Cloud-Anbietern selbst entschlüsselt und damit inhaltlich ausgewertet werden.

Nicht nur Ihre Dokumente selbst können wertvolle Informationen nach außen geben. Sogenannte **Metadaten**, dazu gehören zum Beispiel Dateigröße und Datum, aber auch der Dateiname, verraten bereits viel. Ordner- und Dateinamen ebenfalls zu verschlüsseln, empfiehlt sich deshalb, wenn Sie eine Analyse Ihrer Datenstrukturen von außen verhindern möchten.

Wenn Sie dieses Buch lesen, weil Ihnen der Schutz Ihrer Daten wichtig ist, sollten Sie auf Ende-zu-Ende-Verschlüsselung setzen.

Ende-zu-Ende-Verschlüsselung

Ende-zu-Ende-Verschlüsselung (auch E2EE, vom Englischen »end-to-end encryption«, siehe Abbildung 5.1) ist eine der wichtigsten und sichersten Verschlüsselungsformen, wenn es um die Übertragung von Informationen geht.

Echte Ende-zu-Ende-Verschlüsselung liegt dann vor, wenn ausschließlich Sender und Empfänger, also die beiden Endpunkte einer Nachricht, deren Inhalt einsehen können.

Dafür wird die Information vor dem Versand verschlüsselt und erst nach dem Empfang wieder entschlüsselt. Der Überbringer der Nachricht hat zu keinem Zeitpunkt Einsicht in den Klartext – ganz egal, ob es sich dabei um eine Chat-App, einen E-Mail-Server oder einen Cloud-Speicher handelt.

Bei dieser Art der Verschlüsselung wird die Nachricht (oder Datei) auf dem Gerät des Senders in der Regel mit hybrider Verschlüsselung (siehe Kapitel 4) unlesbar gemacht. Die hybride Verschlüsselung wird aus Effizienzgründen verwendet und bedeutet, dass die Nachricht mit einem symmetrischen Schlüssel (zum Beispiel AES) verschlüsselt wird. Der verwendete AES-Schlüssel wird mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und sowohl die verschlüsselte Nachricht als auch der verschlüsselte AES-Schlüssel werden an den Empfänger geschickt. Dieser kann nun zunächst den AES-Schlüssel mit seinem privaten Schlüssel, dann die Nachricht mit dem mitgesendeten AES-Schlüssel entschlüsseln.

Ende-zu-Ende-Verschlüsselung

mit öffentlichen und privaten Schlüsseln

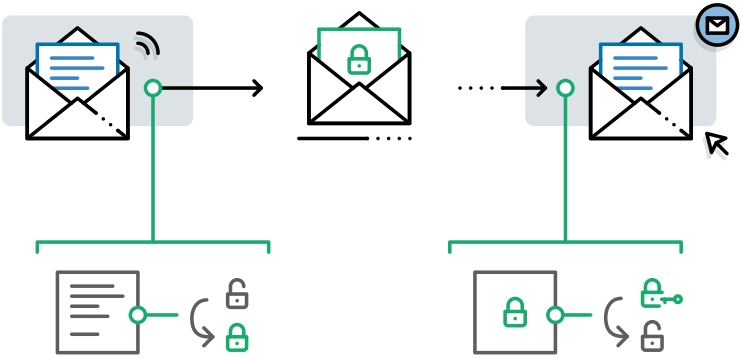

Abbildung 5.1: Ende-zu-Ende-Verschlüsselung

Zero Knowledge

Der Begriff *Zero Knowledge* wird Ihnen häufig begegnen, wenn Sie sich mit Verschlüsselungslösungen befassen. Deshalb erklären wir ihn hier ausführlich. Doch Achtung, wir müssen hier ein bisschen ausholen, denn der Begriff wird unterschiedlich verwendet.

Der Zero-Knowledge-Beweis beziehungsweise Nicht-Wissen-Beweis im akademischen Sinn beschreibt ein Verfahren, wonach eine Person versucht, einer anderen Person zu beweisen, dass sie ein bestimmtes Geheimnis kennt. Dabei wird das Geheimnis selbst aber nicht preisgegeben. Ein Beispiel: Es soll bewiesen werden, dass das Geheimnis, mit welcher Technik man eine Truhe öffnet, bekannt ist. Eine Person geht in einen Nebenraum, um dort die verschlossene Truhe zu öffnen. Gelingt es, kann die Person einen Gegenstand herausholen, zurückkommen und ihn den Beobachtern präsentieren. Dann ist der Beweis erbracht, dass sie in der Lage ist, die Truhe zu öffnen. Für die Beobachter ist nur das Ergebnis (der Gegenstand) relevant. Die Art und Weise, *wie* die Truhe geöffnet wurde, bleibt geheim.

Geheimwissen wird bewiesen, indem ein Ergebnis mehrfach und fehlerfrei vorgelegt wird. Damit kann die Person, die den Beweis fordert, sichergehen, dass die Person, die den Beweis liefert, das Geheimnis wirklich kennt.

Der Lösungsweg, also das Geheimnis, wird dabei im Verborgenen ausgeführt – zum Beispiel in einem anderen Raum. Je häufiger das geforderte Ergebnis fehlerfrei vorgelegt werden kann, desto *wahrscheinlicher* ist es, dass der Person, die den Beweis liefert, der Lösungsweg tatsächlich bekannt ist und es sich nicht um Zufallstreffer handelt.

Am Ende eines Zero-Knowledge-Beweises kann die Person, die den Beweis fordert, davon ausgehen, dass die Person, die den Beweis liefert, ein Geheimnis wirklich kennt, ohne selbst darin eingeweiht zu sein.

In Bezug auf Datenverschlüsselung hat Whistleblower Edward Snowden den Begriff jedoch weiter geprägt: Er verwendet *Zero Knowledge* auch als Beschreibung für ein Versprechen der sicheren Verschlüsselung von Informationen. Konkret bedeutet das, dass die Instanz, die die Verschlüsselung bereitstellt, keine Möglichkeit hat, die Verschlüsselung rückgängig zu machen und die Daten zu lesen.

In keinem Fall dürfen unbefugte Dritte, also zum Beispiel neugierige Nachbarn, Industriespione oder Behörden, Zugriff auf Klartext-Informationen bekommen. Um dies zu erreichen, wird Ende-zu-Ende-Verschlüsselung eingesetzt.

Ende-zu-Ende-Verschlüsselung ist die Strategie, mit der Zero Knowledge erzielt wird.

Unabhängige Verschlüsselung sorgt dafür, dass die Aufbewahrung und Verarbeitung von Daten und die Ausführung der Verschlüsselung bei unterschiedlichen Anbietern liegt.

Damit das Zero-Knowledge-Versprechen vollständig erfüllt wird, darf der Anbieter der Verschlüsselungslösung selbst auch keine Kenntnis über die Schlüssel haben. Nur so können Sie sicherstellen, dass Unbefugte nicht ohne Ihre Hilfe in Besitz der verschlüsselten Daten sowie der zugehörigen Schlüssel kommen können.

Möglich wird dies, indem Schlüssel, mit denen Nachrichten oder Dokumente gesichert werden, selbst verschlüsselt werden, und zwar mit einem selbstgewählten Passwort. Dazu erfahren Sie im nächsten Abschnitt mehr. Beim Thema Passwort sollten Sie sich auf jeden Fall merken:

Das Passwort ist die Zugriffshürde. Ein starkes Passwort ist Voraussetzung für sichere Verschlüsselung.

Zero-Knowledge-Verschlüsselung für Cloud-Speicher bietet zahlreiche Vorteile und ein absolutes Plus an Schutz für Ihre Daten.

Übrigens, wenn Sie nun auch noch eine Verschlüsselungssoftware wählen, die neben dem hohen Schutz weiterhin alle vertrauten Funktionen der Cloud ermöglicht, dann haben Sie die bestmögliche Lösung für Ihr Unternehmen gefunden. Eine Entscheidungshilfe bieten wir Ihnen in Kapitel 8.

Die Kombination von Cloud-Speicher und Zero-Knowledge-Verschlüsselung im Überblick:

- ✔ Durch die absolute Kontrolle über Ihre Daten können Sie Compliance-Vorschriften auch in der Cloud problemlos einhalten.
- ✔ Die unabhängige Verschlüsselung gibt Ihnen Spielraum bei der Auswahl des Cloud-Anbieters und schränkt Sie nicht auf bestimmte Funktionen oder Regionen ein.
- ✔ Sie teilen sich die Aufgaben: Für den physischen Schutz der Daten sorgt der Cloud-Anbieter, für die Privatsphäre sorgen Sie selbst – mithilfe der Verschlüsselungslösung.
- ✔ Sie können Backups sicher auslagern und müssen dafür keine eigenen Kapazitäten bereithalten.
- ✔ Sie müssen Ihrem Cloud-Anbieter keinen »Vertrauensvorschuss« entgegenbringen (»Zero Trust«).

Weiterführende Informationen zu Zero Knowledge finden Sie unter `https://boxcryptor.info/zk`. Mehr zu Ende-zu-Ende-Verschlüsselung gibt es hier: `https://boxcryptor.info/e2ee`.

Das Passwort: der Schlüssel zu Ihren Daten

Ein starkes Passwort ist die wichtigste Voraussetzung für erfolgreichen Schutz – unabhängig davon, mit welcher Art von Verschlüsselung Ihre Daten geschützt werden sollen.

Ein starkes Passwort hat mindestens 12 Zeichen und beinhaltet Zahlen, Buchstaben und Sonderzeichen. Das Passwort darf kein echtes Wort, also nicht im Duden zu finden sein.

Hier ein Vergleich, damit Sie sich das besser vorstellen können: Der Verschlüsselungsalgorithmus ist der Tresor, das Passwort ist die geheime Zahlenkombination für das Schloss.

Moderne, kryptografische Operationen sind einem Safe natürlich überlegen: Ein Passwort lässt sich eben nicht mit einem Schweißbrenner aushebeln. Ohne das richtige Passwort bräuchte ein digitaler Panzerknacker ein paar Milliarden Jahre Zeit.

Leider liegt es in der Natur des Menschen, Dinge zu vergessen. Das führt dazu, dass ein starkes Passwort zwar der Schlüssel für eine erfolgreiche Verschlüsselung ist, aber hin und wieder auch der Grund für große Verzweiflung, denn wenn das Passwort verloren geht, sind die Daten verschlüsselt und werden es für immer bleiben. Ein kleiner Trost: In so einem Fall können Sie zumindest sicher sein, dass auch niemand sonst auf Ihre Informationen zugreifen kann.

Für die Erstellung und Verwaltung sicherer Passwörter gibt es jedoch eine Lösung: Passwortmanager. Diese Software und die verschiedenen Anbieter ausführlich vorzustellen, würde allerdings den Rahmen dieses Buches sprengen.

Der wahre Schlüssel zu Ihren Daten ist bei allen Verschlüsselungslösungen Ihr persönliches Passwort. Wie Sie gute Passwörter anlegen und verwalten, erklären wir Ihnen hier:
`https://boxcryptor.info/123`.

Soft- oder Hardware-basierte Verschlüsselung

Um *Hardware-basierte Verschlüsselung* handelt es sich, wenn die Verschlüsselungsoption in eine Hardwarekomponente eingebaut wird. Darunter fallen beispielsweise Festplatten, externe Festplatten, Speichersticks und Netzwerkspeicher (NAS).

Wer die verschlüsselten Daten lesen will, muss sich authentifizieren. Dafür gibt es verschiedene Methoden:

- ✔ das Passwort wird über eine Web-Oberfläche abgefragt,
- ✔ der Schlüssel ist auf einem USB-Stick gespeichert,

✔ der Schlüssel ist auf einem internen Speicherchip gespeichert.

Eines haben alle Methoden gemeinsam: Die Authentifizierung erfolgt immer auf Hardware-Ebene.

Software-basierte Verschlüsselung dagegen nutzt Programme, um Daten auf einem Laufwerk zu verschlüsseln. Wenn ein Laufwerk das erste Mal verschlüsselt wird, generiert die Verschlüsselungssoftware einen eindeutigen, geheimen Schlüssel, der im Speicher des jeweiligen Geräts hinterlegt wird. Der Schlüssel wird mit einem Passwort verschlüsselt, das vom Nutzer festgelegt wird.

Ob für Ihr Unternehmen Hard- oder Software-basierte Verschlüsselung die beste Lösung ist, hängt von den jeweiligen Faktoren ab. In Tabelle 5.1 finden Sie eine Übersicht.

Hardware-basiert	**Software-basiert**
Systemleistung	
Die Verschlüsselung erfolgt in einem separaten Prozessor und hat daher keine Auswirkungen auf die Gesamtleistung des Systems.	Das gesamte System kann verlangsamt werden, da der Prozessor des Geräts auch die Ver- und Entschlüsselung ausführen muss.
Kosten	
Anschaffung: vergleichsweise teuer.	Implementierung: vergleichsweise günstig.
Wartung	
Erfordert in der Regel keinerlei Treiber-, Update- oder Softwareinstallation, sondern ist an das jeweilige Speichermedium gebunden.	Installation von Treibern, Updates oder Software ist immer wieder nötig.
Skalierbarkeit	
Bei Wachstum ist der Kauf zusätzlicher Verschlüsselungshardware nötig.	Software-basierte Verschlüsselung ist beliebig skalierbar.
Schutzniveau	
Die Verschlüsselung ist immer aktiv und kann daher weder von Endnutzern noch von Malware deaktiviert werden.	Die Verschlüsselung ist nur so sicher wie das Gerät, auf dem sie eingesetzt wird. Zusätzlicher Geräteschutz und Maßnahmen bei Verlust und Diebstahl sind nötig.
Kontinuitätsmanagement	
Hardware-verschlüsselte Daten lassen sich im Fall eines Datenverlusts nur schwer wiederherstellen.	Software-Verschlüsselungssysteme verfügen in der Regel über eingebaute Wiederherstellungsmechanismen.

Tabelle 5.1: Vergleich von Software- und Hardware-basierter Verschlüsselung

Konnten Sie sich schon auf eine Verschlüsselungsmethode festlegen, oder hadern Sie noch? Nun, es gibt eine weitere Entscheidung, die Sie treffen müssen, wenn Sie die passende Verschlüsselungslösung für Ihr Unternehmen finden wollen: Soll es eine Open-Source-Lösung oder eine Closed-Source-Lösung sein?

Open Source oder Closed Source

Die Idee, den Quellcode einer Software zu veröffentlichen und damit für andere zur Bewertung, Nutzung und Verbesserung freizugeben, stammt aus den Jahren kurz vor der Jahrtausendwende. Mittlerweile hat sich eine weltweite *Open-Source*-Community gebildet, die auf dem Austausch von Wissen (in Form von Code) basiert.

Die Debatte um die Veröffentlichung oder Geheimhaltung bestimmter Software wird teilweise leidenschaftlich geführt. Alle Argumente hier aufzuführen, würde zu weit führen. Wir haben für Sie aber in Tabelle 5.2 die wichtigsten Punkte zusammengefasst, die Sie wissen müssen, um die Auswahl der passenden Verschlüsselungslösung für Ihr Unternehmen weiter einzugrenzen:

Open Source-Software	**Closed Source-Software**
Quellcode	
Der Quellcode ist öffentlich und kann von allen eingesehen werden.	Der Quellcode ist nur für autorisierte Personen (zum Beispiel Mitarbeitende) einsehbar.
Beteiligung	
Nutzer können den Quellcode kopieren, verändern oder löschen beziehungsweise einen Antrag darauf stellen.	Nur autorisierte Personen können den Code bearbeiten.
Nutzungsrecht	
Je nach Lizenz können Nutzer die Open-Source-Software in ihren eigenen Programmen verwenden.	Nutzer müssen beim Hersteller eine Lizenz kaufen, wenn sie die Software verwenden wollen.
Kosten	
Häufig kostenlos oder gegen eine Spende verfügbar.	In der Regel mit Kosten verbunden.
Vertrauen	
Wird der Code offengelegt, können alle ihn analysieren und Verbesserungsvorschläge machen, wenn Fehler oder Schwachstellen entdeckt werden.	Die Weiterentwicklung des Codes liegt in der Verantwortung des Herstellers. So auch die Sicherstellung, dass Fehler und Schwachstellen behoben werden.

Open Source-Software	Closed Source-Software
Nutzerfreundlichkeit	
Open-Source-Software ist möglicherweise nicht so benutzerfreundlich wie Closed-Source-Software, da Benutzerfreundlichkeit ein sehr aufwendiger Prozess ist.	Der Hersteller hat Interesse daran, dass eine stabile und benutzerfreundliche Softwarelösung entwickelt wird, damit die Nutzer zufrieden sind.
Support	
Bei Problemen kann es schwierig sein, technische Unterstützung zu erhalten, insbesondere bei weniger verbreiteten Programmen, die keine große Community haben.	Für Unterstützung bei Problemen sorgt in der Regel der Kundendienst des Software-Herstellers.
Planungssicherheit	
Bei reinen Open-Source-Lösungen kann es passieren, dass sie plötzlich nicht mehr weiterentwickelt werden. Das kann mittel- und langfristig zu Problemen führen.	Unternehmen, die Closed-Source-Lösungen anbieten, kalkulieren langfristig und richten ihre Produktstrategie darauf aus, Kunden langfristig ein Angebot machen zu können.

Tabelle 5.2: Vergleich von Open Source- und Closed Source-Lösungen

Wirklich relevant ist das Thema Open-Source-Software nur für Programme, die Sie privat verwenden. Im Unternehmens- und Enterprise-Bereich werden kaum quelloffene Programme genutzt, weil die Zukunftsfähigkeit nicht gewährleistet ist und weil meist kein zuverlässiger Support angeboten wird.

Sie haben nun einen Überblick über die verschiedenen Einsatzgebiete und Prinzipien der Verschlüsselung. Wir hoffen, Sie fühlen sich nun gut gewappnet für die nächste Nuss, die Sie knacken müssen: Verschlüsselungssoftware tatsächlich im Unternehmen zu etablieren. Als Erstes müssen Sie die Entscheiderinnen und Entscheider überzeugen.

Teil III
Und jetzt ab in die Praxis

IN DIESEM TEIL ...

In diesem Teil befassen wir uns mit Argumenten. Wir wappnen Sie für jedes Meeting mit den passenden Stichworten und helfen Ihnen dabei, die Perspektive der Stakeholder einzunehmen.

Außerdem finden Sie hier Fallbeispiele, die Ihnen dabei helfen, den Einsatz von Verschlüsselung in Ihrem eigenen Unternehmen zu skizzieren. Am Ende lernen Sie unterschiedliche Cloud-Sicherheitslösungen für Unternehmen kennen.

IN DIESEM KAPITEL

- Überzeugend für Verschlüsselung argumentieren
- Unterschiedliche Perspektiven
- Vorteile von Verschlüsselung, die über den Datenschutz hinausgehen

Kapitel 6
Argumentationshilfe für den unternehmensinternen Einsatz von Verschlüsselung

Prima: Sie haben nun gelernt, wie Verschlüsselung funktioniert. Das war der einfache Teil: Jetzt müssen Sie im Unternehmen Überzeugungsarbeit leisten, damit Verschlüsselung eingeführt wird. Als Argumentationshilfe können Sie die folgenden Tipps anwenden. Anschließend erhalten Sie zu jedem Tipp ausführliche Formulierungshilfen.

- ✔ Beziehen Sie die Belegschaft ein.
- ✔ Werben Sie für Digitalisierung.
- ✔ Betonen Sie die Notwendigkeit betrieblicher Kontinuität.
- ✔ Zeigen Sie Einsparpotenzial auf.
- ✔ Präsentieren Sie Beispielunternehmen.
- ✔ Rufen Sie die drohenden Geldstrafen bei einem Verstoß gegen die DSGVO in Erinnerung.
- ✔ Zeigen Sie bekannte Fälle von Datenschutzverletzungen.

Beziehen Sie die Belegschaft ein

Jeder Rechner und somit jeder Anwender und jede Computernutzerin im Unternehmen stellt ein potenzielles Sicherheitsrisiko dar. Verpflichtende Datenschutzschulungen vermindern bestimmte Gefahren möglicherweise, der »Faktor Mensch« bleibt jedoch bestehen. Das Ziel muss sein, den Anteil dieses Faktors zu verringern und so viele sicherheitsrelevante Abläufe wie möglich zu automatisieren. Das entlastet den Einzelnen, denn »vorsichtig sein« ist eine lästige und vage Zusatzaufgabe.

Stellen Sie klar dar, wie sich die neue Software in den Arbeitsalltag einfügen wird. Erklären Sie genau, welche Arbeitsabläufe beeinflusst werden, damit die betroffenen Mitarbeiterinnen und Mitarbeiter den Aufwand einschätzen können. Dieses Thema sollten Sie natürlich auch bei der Auswahl der Verschlüsselungssoftware berücksichtigen. Im besten Fall fügt sich das neue Programm nahtlos in bestehende Prozesse ein und arbeitet im Hintergrund.

Erklären Sie, dass Verschlüsselungssoftware jeden Einzelnen entlastet, weil sie das Risiko für Datenschutzvorfälle senkt.

Werben Sie für Digitalisierung

Die Digitalisierung ist notwendig und wird früher oder später auch den letzten Vorgang im Unternehmen erreicht haben. Da auch Ihre Firma nicht darum herumkommen wird, Prozesse zu digitalisieren, ist es sinnvoll, rechtzeitig damit anzufangen und nicht darauf zu warten, bis man durch äußere Umstände dazu gezwungen wird.

Ein Beispiel: Unternehmen, die bereits vor der Coronapandemie eine Cloud-Infrastruktur für ihre Datenablage aufgebaut hatten, waren klar im Vorteil, als im März 2020 Arbeitsplätze von heute auf morgen ins Homeoffice verlegt wurden. Mit einer sicher verschlüsselten Cloud ist die dezentrale Arbeit kein Problem, denn die bestehenden Systeme können standortunabhängig genutzt werden. Viele Firmen hatten zuvor der Sicherheit der Cloud nicht getraut und deshalb kein sicheres Setup aufgebaut. Nun mussten sie überstürzt in die Cloud (beispielsweise zu Microsoft Teams) wechseln, ohne Sicherheitsvorkehrungen (wie Verschlüsselung) getroffen zu haben. So ist in vielen Betrieben ein Risiko entstanden, das mit besserer Vorbereitung hätte vermieden werden können. Machen Sie sich also dafür stark, dass das Thema Sicherheit von Anfang an bei der Digitalisierungsstrategie mitgedacht wird.

Erklären Sie, dass überhastetes Einführen neuer Software zu Fehlern führt. Nutzen Sie ruhige Phasen für solche Projekte.

Betonen Sie die Notwendigkeit betrieblicher Kontinuität

Neben globalen Pandemien gibt es noch zahlreiche weitere Vorfälle, die die Geschäftstätigkeit einschränken können. Indem Sie die Daten an einen professionellen Anbieter (Cloud-Dienstleister) auslagern und verschlüsseln, machen Sie das Unternehmen widerstandsfähig im Falle eines Brandes, bei Stromausfällen oder Naturkatastrophen. Die räumliche Trennung von Betrieb und Datenspeicher erhöht die Verfügbarkeit von Daten.

Ihre Kollegen argumentieren, dass auch ein Rechenzentrum abbrennen könnte? Das stimmt. Allerdings haben die Cloud-Anbieter selbst wiederum umfangreiche Backup-Strategien, mit denen Daten in verschiedene Regionen der Welt gespiegelt werden. Das ist praktisch, wenn es um die **physikalische Sicherheit** der Dateien geht. Dass die **Vertraulichkeit** der Daten durch eigene Verschlüsselung gewährleistet sein muss, wird dadurch umso deutlicher.

Um mit den Cloud-Dateien zu arbeiten, muss übrigens nicht ununterbrochen eine Internetverbindung vorhanden sein. Viele Anbieter haben spezielle Funktionen für die Offline-Arbeit. Dabei werden Dateien lokal gespeichert und bei nächster Gelegenheit in die Cloud synchronisiert. Im Alltag ist das vor allem für Kolleginnen und Kollegen praktisch, die im Zug oder im Flugzeug arbeiten.

Betriebliche Kontinuität sichert das Unternehmen und damit die Arbeitsplätze. Sie liegt also im Interesse aller.

Zeigen Sie Einsparpotenzial auf

Ein wichtiger Punkt, den Sie hervorheben sollten, ist die **Kosteneinsparung**. Schließlich ist die Nutzung moderner Cloud-Infrastruktur wesentlich günstiger als der Unterhalt eines eigenen Rechenzentrums. Bedenken Sie, welche Ausgaben anfallen würden, wenn Ihr Unternehmen ein eigenes Rechenzentrum (mit ähnlicher Verfügbarkeit und Sicherheit wie bei einem spezialisierten Anbieter) betreiben wollte.

Ein eigenes Rechenzentrum erfordert:

- ✔ einen Raum für die Server mit entsprechender Lüftung, Stromanschlüssen und einer Löschanlage,
- ✔ ein Notstromaggregat,
- ✔ einen oder mehrere Administratoren.

Bedenken Sie: Neben dem branchenüblichen Lohn müssen hier Nacht-, Feiertags- und Bereitschaftszuschüsse kalkuliert werden.

Im Gegensatz dazu buchen Sie den Cloud-Speicher beim Profi nur in dem Umfang, indem er benötigt wird. So richten sich die Kosten für den Speicherplatz nach der benötigten Speichermenge und der Anzahl an Lizenzen. In Kombination mit einer Verschlüsselungssoftware, die ebenfalls nach Lizenzen berechnet wird, liegen Sie dann weit unter den Kosten für ein eigenes Rechenzentrum.

Hätten Sie es gewusst? Die Kosten für ein eigenes Rechenzentrum zählen zu den Kapitalaufwendungen. Wenn die IT-Infrastruktur bei einem Cloud-Anbieter als Service genutzt wird, zählen die Ausgaben zu den Betriebskosten.

Eine Umstrukturierung der Kosten kann vorteilhaft sein. Holen Sie sich bei diesem Thema Unterstützung aus der Buchhaltung.

Die **Flexibilität** der Cloud besteht nicht nur auf dem Papier: Stellen Sie sich einen Cloud-Dienst wie eine Versorgungsleistung vor. Sie bezahlen (je nach Vertrag) nur die tatsächlich genutzten Ressourcen. Ein eigenes Rechenzentrum zu unterhalten, kann man mit einem festen Abonnement vergleichen – mit einer sehr langen Kündigungsfrist. Sollten sich die Anforderungen an Speicherkapazität und Rechenleistung ändern, können die Kosten für den Cloud-Dienst dagegen kurzfristig angepasst werden. So eine Umstellung kann zum Beispiel durch eine betriebliche Umstrukturierung, neue (effizientere) Software oder Änderungen im Compliance-Bereich notwendig werden.

Auch die positiven Auswirkungen auf die Energiebilanz sollten Sie nicht unterschätzen. Wenn Sie etwa die Cloud-Dienste von AWS nutzen, ist die Datenverarbeitung 3,6-mal energieeffizienter als ein durchschnittliches Rechenzentrum, wie eine Befragung unter US-Unternehmen ergeben hat. Große Anbieter stecken viel Geld und Aufwand in die Umweltbilanzen ihrer Rechenzentren. Öko-Strom und energieeffiziente Geräte sind ein fester Bestandteil der Strategie. Die meisten Anbieter bescheinigen Ihnen die guten Werte mit Siegeln oder Zertifikaten. Diese können Sie wiederum in ihrer **Unternehmensbilanz** nutzen. Denken Sie darüber nach, diese guten Nachrichten für PR zu nutzen und besprechen Sie das mit der Marketing-Abteilung.

Ein toller Nebeneffekt: Gegebenenfalls auftretende IT-Probleme an der Server-Infrastruktur muss Ihr Unternehmen nicht mehr selbst lösen. Darum kümmern sich die Experten des Cloud-Anbieters.

Heben Sie die drei Kernbereiche **Flexibilität**, **Kosteneinsparung** und **Unternehmensbilanz** hervor, die durch eine cloud-fokussierte Unternehmenskultur gefördert werden.

Präsentieren Sie Beispielunternehmen

Zeigen Sie auf, dass andere Unternehmen der gleichen Größe oder Branche ebenfalls Verschlüsselungssoftware verwenden. Das ist ein schlagkräftiges Argument. Vertrauenswürdige Anbieter stellen auf ihrer Webseite Fallstudien zur Verfügung, die Interessierten bei der Entscheidungsfindung helfen. Hier wird dargestellt, wie die Implementierung der Verschlüsselungssoftware ablief und wie sich das neue Programm im Arbeitsalltag bewährt. Sollten Sie keine passenden Beispiele finden, lohnt es sich, den Anbieter direkt anzusprechen. Oft bekommen Sie hilfreiche Informationen im direkten Kontakt.

Einige Beispielunternehmen stellen wir Ihnen in Kapitel 7 vor.

Erfolgsgeschichten (im besten Fall aus der gleichen Branche) sind ein starkes Argument. Eventuell lohnt es sich, die Unternehmen direkt zu kontaktieren, um weitere Details zu erfahren.

Rufen Sie die drohenden Geldstrafen bei einem Verstoß gegen die DSGVO in Erinnerung

Die Datenschutz-Grundverordnung sieht drastische Strafen vor, wenn personenbezogene Daten nicht ausreichend geschützt sind und dadurch ein Risiko besteht, dass sie in die falschen Hände geraten: Bis zu vier Prozent des Jahresumsatzes oder 20 Millionen Euro – je nachdem, was höher ist.

Abgesehen davon, dass Unternehmen sich ohnehin gegen jede Art von Spionage, Datenverlust oder Sicherheitslücken absichern sollten, sind die Geldstrafen natürlich ein starkes Argument. Das Risiko für eine derart hohe Zahlung können Sie minimieren, indem Sie alle personenbezogenen Daten mit Ende-zu-Ende-Verschlüsselung

nach Stand der Technik schützen, denn selbst wenn diese Daten dann in falsche Hände geraten, sind sie – dank Verschlüsselung – komplett unbrauchbar.

In der Regel entfällt in so einem Fall sogar die Meldepflicht an die Aufsichtsbehörde. Entscheidend ist, ob der Schlüssel, der für die Verschlüsselung verwendet wurde, ebenfalls abhandengekommen ist oder nicht. Der Verschlüsselungsanbieter wird Sie deshalb zum Key Management beraten, um auch an dieser Stelle jedes Risiko auszuschließen.

Da etliche Medien regelmäßig über die neuesten DSGVO-Strafen berichten, sparen Sie Ihrem Unternehmen mit vorbeugenden Maßnahmen nicht nur eine große Menge Geld, sondern auch ein PR-Desaster.

Zeigen Sie bekannte Fälle von Datenschutzverletzungen auf

Sie müssen ja nicht gleich Horror-Szenarien für Ihre Argumentation einsetzen. Dennoch möchten wir Ihnen ein paar Beispiele an die Hand geben, mit denen Sie arbeiten können, um die Dringlichkeit von Verschlüsselung zu unterstreichen.

Je effektiver Sie Datenschutzvorfälle vermeiden, desto geringer ist die Wahrscheinlichkeit, dass das Unternehmen in ein **PR-Desaster** gerät. Je nach Geschäftsmodell und Zielgruppe kann es sehr ungemütlich werden, wenn hämische Artikel erscheinen oder in sozialen Netzwerken von den Produkten abgeraten wird. Die Kunden werden immer sensibler, wenn es um ihre persönlichen Informationen geht.

- ✔ Der Chat-Dienst WhatsApp sorgte Anfang 2021 für einen extremen Zuwachs bei der Konkurrenz (allen voran beim Dienst Signal), weil die neuen Datenschutzrichtlinien den Nutzern nicht gefallen haben.
- ✔ Apple musste seine geplanten Maßnahmen zum automatischen Scan von Bildern auf Eis legen, weil die Pläne weltweit Protestaktionen auslösten.

Sie sehen: Nutzerinnen und Nutzer sind wachsam und haben dank der Vernetzung in den sozialen Medien schnell großen Einfluss.

Ebenfalls besorgniserregend sind **Betriebsausfälle** durch Cyberangriffe:

- ✔ Im Juni 2017 wurde die Reederei Maersk mit einer Schadsoftware angegriffen. Das global agierende Unternehmen musste einige Systeme abschalten und konnte den Betrieb nur langsam wieder hochfahren. Zeitungsberichten zufolge ist durch die Saboteure ein Schaden in Höhe von 300 Millionen Dollar entstanden.

- ✔ Vom gleichen Angriff waren auch die Zentralbank und ein Flughafen in der Ukraine betroffen. Das Atomkraftwerk Tschernobyl musste vorübergehend einige Prozesse manuell durchführen, weil auch dort Systeme abgeschaltet werden mussten.

- ✔ Im September 2020 kam es nach einer Hackerattacke zu einem tragischen Todesfall. Die Düsseldorfer Uni-Klinik wurde angegriffen, um Geld zu erpressen. Durch die Beeinträchtigung der Computersysteme konnte die Behandlung einer Patientin erst nach Verzögerung stattfinden und die Frau verstarb wenig später. Das ist der erste Todesfall, der unmittelbar mit einem Hackerangriff in Verbindung gebracht werden konnte. Gegen die Kriminellen wird wegen fahrlässiger Tötung ermittelt. Ein ähnlicher Fall wurde 2021 aus einem US-Krankenhaus gemeldet.

Skizzieren Sie realistische Bedrohungsszenarien, damit Ihr Team die Gefahr einschätzen kann. Beispiele helfen dabei.

IN DIESEM KAPITEL

Kapitel 7
Verschlüsselt zusammenarbeiten – Beispiele aus Unternehmen

In diesem Kapitel finden Sie Beispiele, wie Verschlüsselung im Arbeitsalltag vieler Unternehmen bereits genutzt wird. Selbstverständlich stellt diese Auswahl nur einen kleinen Teil der vielfältigen Anwendungsmöglichkeiten dar. Alle haben sie eines gemeinsam: Es geht darum, Geheimnisse oder vertrauliche Informationen zu schützen.

Fallbeispiel 1: die Presseagentur

Die Presseagentur arbeitet international. Mitarbeiterinnen und Mitarbeiter liefern News und Reportagen. Manche Recherchen dauern mehrere Jahre und umfassen eine Vielzahl an Personen. Dabei müssen immer wieder die gleichen Herausforderungen gemeistert werden:

- ✔ eingeschränkte Pressefreiheit,
- ✔ Quellenschutz,
- ✔ Übermittlung brisanter Dokumente.

Um Informationen und Meldungen schnell zu übermitteln, braucht es nicht viel: Ein Cloud-Speicher reicht aus, um auch in Presseagenturen mit mehreren tausend Mitarbeitenden nahezu beliebig viele Daten in Sekundenschnelle um die Welt zu schicken und gemeinsam zu bearbeiten.

Insbesondere bei sensiblen Themen, etwa einer Investigativ-Recherche, müssen die Agenturen für die Vertraulichkeit der Daten und den Schutz ihrer Quellen sorgen. Unverschlüsselte Informationen können schwerwiegende Konsequenzen nach sich ziehen.

Dank sicherer Ende-zu-Ende-Verschlüsselung, wie sie inzwischen auf fast jedem Endgerät möglich ist, wird die Arbeit von Journalistinnen und Journalisten weltweit erleichtert, denn sie ermöglicht die Nutzung von Cloud-Diensten. Dabei sind zwei Faktoren besonders entscheidend:

- ✔ ortsunabhängige Zusammenarbeit und
- ✔ sichere Speicherung der Daten.

Fallbeispiel 2: der Sportverein

Ein regionales Anwendungsbeispiel für starke Datenverschlüsselung könnte Ihnen begegnen, wenn Sie Mitglied in einem Sportverein sind. Je nachdem, wie dieser Verein die Daten seiner Mitglieder verwaltet, kann auch hier Verschlüsselung zum Einsatz kommen.

Zwingend notwendig macht diesen Extra-Schutz seit Mai 2018 die DSGVO. Dass die neue EU-Verordnung auch Vereine betrifft, hatte damals für einige Aufregung gesorgt, da diese für die Umsetzung der neuen Regeln oft weder Budget noch Personal hatten.

Doch natürlich gilt auch für Vereine: Wenn Dateien extern gespeichert werden – zum Beispiel bei Cloud-Angeboten wie Microsoft OneDrive oder Dropbox, müssen personenbezogene Daten besonders geschützt werden.

Davon sind die meisten Vereine betroffen, denn gerade für kleine Organisationen ohne hauptamtliche Mitarbeitende ergibt die Nutzung der Cloud Sinn, weil sie großen Nutzen (wie ortsunabhängiges Arbeiten) mit geringen Kosten verbindet.

Verschlüsselung kann hier eine einfach einzurichtende und sehr effektive Maßnahme sein. Es reicht, einen Cloud-Speicher auszuwählen und die Verschlüsselungssoftware auf den Rechnern derjenigen zu installieren, die auf die Daten zugreifen müssen. Danach können die bereits vorhandenen Dateien verschlüsselt in die Cloud gelegt werden. Müssen sensible Daten mit Außenstehenden geteilt werden, ist dies dank einer hybriden Verschlüsselung mit öffentlichen und privaten Schlüsseln weiterhin möglich.

Das Beste daran: Nicht nur aus rechtlicher Sicht ist der Verein so auf der sicheren Seite. Auch die Mitglieder wissen, dass ihre Daten gut aufgehoben sind und die Verantwortlichen großen Wert auf den Schutz Ihrer persönlichen Informationen setzen.

Fallbeispiel 3: die Arztpraxis

Im Gesundheitswesen wird eine Vielzahl personenbezogener Daten verarbeitet. Die sensibelsten sind mit Abstand die Akten und Befunde der Patienten und Patientinnen. Der zweite, große Bereich sind die Personalakten und alle Informationen über die zahlreichen Beschäftigten. Diese Daten müssen um jeden Preis geschützt werden, und vor allem in den letzten Jahren ist das Gesundheitswesen zu einem beliebten Ziel von Cyberkriminellen geworden. Die erbeuteten Informationen sind auf dem Schwarzmarkt begehrt.

Jede Arztpraxis muss daher die medizinischen Informationen ihrer Patientinnen und Patienten sicher ablegen. Dazu verpflichtet nicht nur der strenge Datenschutz und das Arztgeheimnis: Die anvertrauten Gesundheitsinformationen zählen für die meisten Menschen auch zu den persönlichsten und sensibelsten Informationen, die Sie außerhalb ihrer eigenen vier Wände preisgeben.

Die begründete Angst um die Daten führt in vielen Praxen dazu, dass die Daten lieber »gehortet« werden. Eigene Server in den eigenen Räumlichkeiten, hohe Hardwarekosten und Sicherungskopien, die nach Feierabend mit nach Hause getragen werden – das ist die Realität für viele niedergelassene Ärzte. Das Risiko für Daten-Diebstahl durch Angestellte oder Dritte, die Zugang zu den Praxisräumen bekommen, ist hoch.

Diese Probleme können durch die Migration der Daten in die Cloud gelöst werden. Und die Cloud hat weitere Vorteile:

- ✔ Sie ist wesentlich kostengünstiger.
- ✔ Sie erleichtert die interne Datenverwaltung.
- ✔ Sie unterstützt einen effizienten Arbeitsablauf.

Es ist verständlich, dass eine gewisse Hemmung besteht, die Daten in die Hände Dritter zu geben. Doch tatsächlich handelt es sich nur um einen gefühlten Kontrollverlust, keinen realen.

Eine Praxis kann mit geringem Aufwand sichere und komfortable Datenspeicherung nutzen, indem sie zusätzlich zum praktischen Cloud-Speicher auch sichere Ende-zu-Ende-Verschlüsselung einsetzt. Auf diese Weise behalten Ärztinnen und Ärzte die volle Kontrolle über die Daten der Patienten und Mitarbeiterinnen, weil die Informationen verschlüsselt sind, bevor sie in die Cloud übermittelt werden. Diese Lösung berücksichtigt auch das kleinteilige Zugriffsmanagement, denn die Daten sollen von verschiedenen Geräten in verschiedenen Räumen für verschiedene Personen erreichbar sein.

IN DIESEM KAPITEL

- Erstellung eines Threat Models
- Sichere Nutzung der Cloud
- Beispiellösungen für Verschlüsselungssoftware

Kapitel 8
Software und Lösungen für das sichere Arbeiten in der Cloud

Damit sich Ihr Unternehmen gezielt gegen Cyber-Bedrohungen zur Wehr setzen kann, müssen Sie sich klar machen, worin genau die Bedrohungen bestehen. Dazu betrachtet man die IT-Struktur sehr detailliert und notiert die Schwachstellen. Das Dokument, was dadurch entsteht, nennt man Threat Model.

Definieren Sie Ihr Threat Model

Das Threat Model, auf Deutsch die Bedrohungsmodellierung, identifiziert und analysiert potenzielle Sicherheitslücken und Schwachstellen in der IT-Struktur eines Unternehmens.

Bei der Analyse der Geschäftsprozesse und der IT-Infrastruktur wird auf sensible Ressourcen wie Passwörter, Dokumente und Zugriffsrechte geachtet. Auch die verwendeten Software- und Speicherlösungen müssen betrachtet werden. Ein Threat Model kann ein Schaubild oder ein Textdokument sein. Das bleibt Ihnen überlassen. Die identifizierten Schwachstellen und (gegebenenfalls fehlenden) Schutzmaßnahmen werden aufgelistet und nach Schwere der Bedrohung priorisiert.

Erstellen Sie ein Threat Model für Ihr Unternehmen, sodass Sie gezielt Maßnahmen zum Schutz Ihrer Daten und Infrastruktur ergreifen können. Achten Sie besonders auf die Stellen, an denen Verschlüsselung das Risiko verringern kann.

Sie sind nun überzeugt davon, dass eine Verschlüsselungslösung Teil Ihrer Unternehmens-IT werden muss? Hervorragend! Im nächsten Abschnitt erhalten Sie einen Überblick über den Markt der Verschlüsselungsanbieter.

Ansätze für die sichere Cloud-Nutzung im Unternehmen

Wir stellen Ihnen drei verschiedene technische Ansätze vor, mit denen Sie die Cloud sicher nutzen können.

In Kapitel 5 haben Sie gelernt, dass die großen Clouds wie OneDrive, SharePoint oder Dropbox die Daten verschlüsseln, die in der Cloud abgelegt werden: *Data at Rest*. In diesem Kapitel lernen Sie Ansätze kennen, die mit Ende-zu-Ende-Verschlüsselung oder anderer, zusätzlicher Verschlüsselung einen höheren Schutz gewährleisten.

Die Ansätze der verschiedenen Verschlüsselungslösungen lassen sich grob in zwei Varianten aufteilen:

- ✔ Die Verschlüsselung ist *on top*, also ein eigenes Produkt, das Sie zusätzlich zum Cloud-Speicher installieren.
- ✔ Die Verschlüsselung ist ein integrierter Bestandteil eines Cloud-Speichers.

Beide verfolgen jedoch dasselbe Ziel, nämlich Daten in der Unternehmens-Cloud zu schützen.

In der folgenden Liste gehen wir auf die jeweiligen Vor- und Nachteile der einzelnen Ansätze der Verschlüsselung ein.

Zero-Knowledge-Cloud

Bei einer Zero-Knowledge-Cloud handelt es sich um einen Cloud-Speicher, der Zero-Knowledge-Verschlüsselung bereits integriert hat. Bei dieser Variante werden alle Daten, die in der ausgewählten Cloud gespeichert sind, automatisch durch starke Verschlüsselung geschützt. Im Gegensatz zu den gängigen Cloud-Anbietern haben Zero-Knowledge-Anbieter keine Möglichkeit, auf Ihre Daten zuzugreifen.

Der Vorteil dieser Variante ist, dass die Bedienung vergleichsweise einfach ist. Schließlich haben Sie nur einen Anbieter, mit dessen Einstellungen und Benutzeroberfläche Sie zurechtkommen müssen (anstatt zwei, wenn Sie die

Cloud und einen Verschlüsselungsanbieter kombinieren). Dafür sind Sie aber auf diesen einen Speicher-Anbieter festgelegt, denn die Verschlüsselung ist an den Speicher gebunden. Sie können also eine Zero-Knowledge-Cloud nicht mit einer weiteren Cloud kombinieren. Andere Cloud-Anbieter (Multi-Cloud-Strategien sind relativ üblich bei Unternehmen) oder Netzgebundene Speicher (NAS) können nicht in die Verschlüsselung integriert werden und benötigen zusätzlich eine eigene Strategie zum Schutz der Daten.

Ein weiterer Nachteil der Zero-Knowledge-Cloud ist, dass die Synchronisation der Daten möglicherweise nicht so reibungslos und schnell funktioniert, wie man das von den Innovatoren im Cloud-Umfeld, Dropbox und Co. gewohnt ist.

Zero-Knowledge-Cloud-Verschlüsselung eines unabhängigen Anbieters

Ein anderer Ansatz ist es, die Cloud-Verschlüsselung zusätzlich zum Cloud-Speicher einzurichten. Dazu nutzen Sie eine spezielle Software, die unabhängig vom Cloud-Anbieter ist. Solch eine Software verschlüsselt im Idealfall alle gängigen Clouds der großen Anbieter.

Unsere Verschlüsselungslösung Boxcryptor, beispielsweise, verschlüsselt sämtliche Clouds, inklusive SharePoint, aber auch NAS-Systeme, lokale Daten und USB-Sticks und bietet zusätzlich Verschlüsselung für Microsoft Teams.

Dieser Ansatz bietet größtmögliche Flexibilität beim Schutz der Unternehmensdaten. Wenn Sie beispielsweise schrittweise Daten in die Cloud migrieren, können zuerst die Netzlaufwerke des Unternehmens gesichert und verschlüsselt werden. Im Zuge des Umzugs in die Cloud kann einfach der Cloud-Speicher als Speicherort hinzugefügt werden.

Im Idealfall bietet der Anbieter umfangreiche Funktionen zur effektiven Nutzung der verschlüsselten Cloud, sodass Sie weiterhin von den Vorteilen der Cloud profitieren können.

Achten Sie beim Test darauf, dass diese Funktionen verfügbar sind:

- ✔ Funktionen für die einfache Nutzerverwaltung (Active-Directory-Unterstützung, SCIM, SSO),
- ✔ Audit-Funktionen,
- ✔ die Möglichkeit, Daten sicher mit Externen zu teilen,
- ✔ individuell anpassbare Compliance-Richtlinien.

Gateway-Lösungen

Bei einer Gateway-Lösung wird an einer zentralen Stelle im Unternehmensnetzwerk eine Art Tor, das sogenannte Gateway, implementiert, das alle Daten von bestimmten Anwendungen automatisch verschlüsselt, die durch das Tor hindurch geleitet werden. Gateway-Lösungen kommen beispielsweise bei der Verschlüsselung von E-Mails zum Einsatz, doch es gibt auch Anbieter für Cloud-Verschlüsselung.

Der offensichtliche Vorteil ist, dass die Verschlüsselung automatisch passiert, die Mitarbeiterinnen und Mitarbeiter nichts davon merken und dadurch die Anwendung sehr einfach ist. Ebenfalls praktisch: Alle Daten sind verschlüsselt. Dadurch ist ausgeschlossen, dass jemand (beabsichtigt oder unbeabsichtigt) unverschlüsselte Dateien erstellt.

Die Nachteile von Gateway-Lösungen sind die hohen Einführungskosten, laufende Anforderungen an die Infrastruktur und die Tatsache, dass das Gateway technisch immer hochverfügbar sein muss. Diese Lösung hat also einen sehr hohen Personal- und Pflegeaufwand. Außerdem sind Daten in Transit zwischen dem Mitarbeiter und dem Gateway nicht verschlüsselt. Anders gesagt: Innerhalb der Firma besteht kein Schutz durch Ende-zu-Ende-Verschlüsselung, da diese erst in dem Moment vorgenommen wird, in dem die Datei das Netzwerk verlässt, durch das Gateway geschickt und dann an den Cloud-Provider übertragen wird. Um interne Compliance-Richtlinien durchzusetzen, damit etwa die Marketing-Abteilung keinen Zugriff auf die HR-Dateien hat, ist eine Gateway-Lösung nicht geeignet.

Treffen Sie Ihre Wahl

Glückwunsch! Sie haben nun alle Informationen, die Sie brauchen, um einen passenden Ansatz für die Cloud-Verschlüsselung in Ihrem Unternehmen auszuwählen. Hilfestellung dazu erhalten Sie im nächsten Kapitel.

Teil IV

Top-Ten-Teil

IN DIESEM TEIL ...

In diesem Teil geht es um Fragen rund um das Thema Cloud-Verschlüsselung. Unsere Checkliste hilft Ihnen dabei, die richtigen Fragen zu stellen. Und die Liste der Missverständnisse in Kapitel 10 hilft Ihnen dabei, die richtigen Antworten auf die Fragen Ihrer Kolleginnen und Kollegen zu geben.

IN DIESEM KAPITEL

- Wichtige Fragen, die Sie klären sollten
- Tipps zur Auswahl einer Verschlüsselungslösung
- Weiterführende Informationen

Kapitel 9
In zehn Schritten zur passenden Verschlüsselungslösung

Welche Fragen müssen Sie sich stellen, wenn Sie sich für Ihr Unternehmen auf die Suche nach einer geeigneten Verschlüsselungslösung zum Schutz Ihrer sensiblen Dateien machen?

Checkliste: zehn wichtige Fragen

Nutzen Sie unsere Checkliste, um sich über Ihre Anforderungen bewusst zu werden und verschiedene Lösungen zu vergleichen.

Welcher Verschlüsselungsalgorithmus mit welcher Bit-Länge wird verwendet?

Prüfen Sie, ob ein öffentliches, standardisiertes Verschlüsselungsverfahren verwendet wird. Über die verschiedenen Algorithmen erfahren Sie in Kapitel 4 mehr. Genauso wichtig wie die Art des Algorithmus und die verschiedenen, miteinander kombinierten Verschlüsselungsverfahren sind die Schlüssellängen. In Deutschland gibt beispielsweise das Bundesministerium für Sicherheit in der Informationstechnologie die Empfehlung, *spätestens ab dem Jahr 2023 eine Schlüssellänge von 3000 Bit zu nutzen*.

Werden die Dateien direkt auf den Endgeräten der Mitarbeitenden verschlüsselt, bevor sie das Gerät verlassen?

Es ist sehr wichtig, dass die Dateien zu keinem Zeitpunkt unverschlüsselt im Internet unterwegs sind. Deshalb sollte die Verschlüsselungslösung alle Daten direkt auf dem Gerät verschlüsseln. Nur dann handelt es sich um eine echte Ende-zu-Ende-Verschlüsselung, also um eine sehr sichere Variante. Die Details dazu können Sie in Kapitel 5 nachlesen.

Können alle wichtigen Dateiformate (zum Beispiel docx, jpg, pdf, avi, mp4 et cetera) verschlüsselt werden?

Es gibt Verschlüsselungslösungen, die nur bestimmte Dateiformate unterstützen. Es ist deshalb sehr wichtig, dass Sie darauf achten, dass wirklich alle Dateien verschlüsselt werden können. Dazu lohnt es sich, mit den verschiedenen Abteilungen zu sprechen und zu fragen, welche Datenformate verwendet werden. So vermeiden Sie böse Überraschungen.

Funktioniert die Verschlüsselungslösung für alle Speicherorte, die Sie benötigen (Cloud-Speicher, USB-Speichermedium, Festplatte, Netzwerklaufwerk)?

Die meisten Unternehmen haben mehr als einen Speicherort. Das liegt teilweise an der historischen Entwicklung, weil beispielsweise nicht alle Dateien vom Netzwerklaufwerk in die Cloud umgezogen wurden. Teilweise liegt das an der sogenannten Schatten-IT. Damit sind Programme und Speichermedien gemeint, die von den Angestellten verwendet werden, aber nicht in die offizielle IT-Struktur eingebettet sind. Es wäre schade, wenn Sie diesen Aspekt übersehen und dadurch neue Angriffslücken und Datenlecks entstehen.

Können bei Wechsel des Speicherortes oder des Speicheranbieters die verschlüsselten Daten einfach und sicher umgezogen werden?

Es empfiehlt sich, eine gewisse Flexibilität zu wahren. Wenn die Verschlüsselung unabhängig vom Datenspeicher ist, haben Sie die Möglichkeit, die Daten umzuziehen oder auf mehrere Cloud-Speicher zu verteilen. Wenn Sie sich hingegen durch die Verschlüsselung auf einen bestimmten Cloud-Speicher festlegen, dann verlieren Sie Handlungsoptionen. Die Unterschiede stellen wir in Kapitel 8 ausführlich vor.

Funktioniert die Verschlüsselungssoftware auf allen gängigen Plattformen wie Windows, Android, macOS und iOS?

Unserer Erfahrung nach nutzen die meisten Unternehmen verschiedene Geräte und unterschiedliche Betriebssysteme – oder planen das in Zukunft. Denn: Mitarbeitenden das Gerät zu geben, mit dem sie sich wohlfühlen, ist ein wichtiges Element in Zeiten von Fachkräftemangel. Wer sich privat mit einem Mac durch das Internet bewegt, möchte beruflich nicht gern mit Windows arbeiten. Dazu kommt, dass Smartphones zunehmend wichtiger werden, weil Arbeit mobiler und dezentraler wird und vieles nebenbei oder unterwegs bearbeitet wird. Deshalb ist es wichtig, dass die Verschlüsselungslösung diese Anforderungen moderner Arbeitswelten berücksichtigt.

Können Sie auch dann auf Ihre Dateien zugreifen, wenn es zu Server-Ausfällen kommt oder es den Verschlüsselungsanbieter nicht mehr gibt?

Beim Thema Verschlüsselung ist die entscheidende Frage: Wer hält die Schlüssel in der Hand? Dazu haben wir uns in Kapitel 4 ausführlich ausgelassen. Wer den Schlüssel hat, kann verschlüsselte Dateien wieder lesbar machen. Normalerweise werden die Schlüssel innerhalb der Software verwaltet, doch die Frage ist berechtigt: Was passiert, wenn der Anbieter bankrottgeht oder die Server von einem Kometen getroffen werden?

Ein guter Verschlüsselungsanbieter wird Ihnen die Option bieten, selbst die Schlüssel zu verwalten beziehungsweise als Sicherungskopie zu exportieren. Lassen Sie sich also dazu beraten, ob und wie das Key Management bei der von Ihnen bevorzugten Verschlüsselungssoftware aussieht.

Können Sie im Notfall auf Unternehmensdateien zugreifen, auch wenn sie das Passwort des Mitarbeiters nicht kennen oder der Schlüssel verloren geht?

Kein Unternehmen sollte von seinen Mitarbeitenden abhängig sein, wenn es um den Zugang zu den eigenen Dateien geht. Moderne Verschlüsselungssoftware beinhaltet deshalb einen Master Key, der die Entschlüsselung verschlüsselter Dateien auch dann möglich macht, wenn ein Mitarbeiter sein Passwort verloren hat oder aus dem Unternehmen ausscheidet. Prüfen Sie, ob dieses Feature enthalten ist.

Gibt es zusätzliche Sicherheitsfunktionen?

Auch, wenn der Verschlüsselungsalgorithmus gut ist, bietet die Verschlüsselung allein keinen 100-prozentigen Schutz. Sie müssen sich fragen, ob und wie beispielsweise die Geräte gesichert sind und welche Schutzmechanismen es für die Accounts gibt. Etablierte Strategien sind:

- ✔ Multifaktor-Account-Authentifizierung via Passwort und weiteren Schutzmechanismen wie PIN oder biometrische Merkmale,
- ✔ Vorgaben für die Stärke des Passwortes (zum Beispiel in Bezug auf die Länge und die verwendeten Zeichen),
- ✔ automatische Klassifizierung sensibler Daten durch die Verschlüsselungssoftware,
- ✔ Funktion für sicheres Löschen von Dateien,
- ✔ integrierte Funktion für automatische Sicherungskopien.

Gibt es eine umfangreiche Admin-Oberfläche?

Was bei kleineren Teams von fleißigen Administratoren händisch erledigt werden kann, muss in großen Unternehmen automatisiert werden: Single Sign-on, User-Account-Provisioning (SCIM) und Nutzung von Active Directory. Weitere Funktionen, die für Sie relevant sein könnten, sind das Auditing der Nutzeraktivitäten und die Durchsetzung individueller Nutzungsrichtlinien. Prüfen Sie, ob die Verschlüsselungssoftware in der Lage ist, diese Anforderungen zu erfüllen.

Mit dieser Checkliste haben Sie einen Überblick über die wichtigsten Themen, die Sie durchgehen müssen. Viele Antworten bekommen Sie direkt von den Anbietern für Verschlüsselungssoftware. Lassen Sie sich also ruhig ausführlich beraten und nutzen Sie unsere Checkliste als Gesprächs- und Recherche-Leitfaden. Eine ausführliche Version dieser Liste finden Sie unter: `https://boxcryptor.info/checkliste`.

Die drei wichtigsten Meilensteine

Wir hoffen, dass Sie jetzt Mut gefasst haben, um die Verschlüsselung von Daten in Ihrem Unternehmen als Sicherheitsmaßnahme einzuführen. Unser Ziel war es, den großen Aufgabenberg in kleine Pakete zu unterteilen.

Ihre wichtigsten Meilensteine sind:

- ✔ Begründen Sie, warum Verschlüsselung notwendig ist.
- ✔ Prüfen Sie, welche Art von Verschlüsselung benötigt wird.
- ✔ Überlegen Sie, wie Sie das Thema im Unternehmen voranbringen.

Der Datenspeicher ist eine der größten Schwachstellen in jedem Unternehmen. Orte, an denen Unternehmensdaten gespeichert werden, sollten immer verschlüsselt werden. Dies trifft besonders zu, wenn die Datenspeicher mit dem Internet verbunden sind oder die Daten von externen Anbietern gehostet werden, wie beispielsweise in Microsoft Teams oder in Clouds wie OneDrive oder Dropbox.

IN DIESEM KAPITEL

Missverständnisse auflösen

Gespräche vorbereiten

Kapitel 10
Sechs häufige Missverständnisse über Verschlüsselung

Über Verschlüsselung kursieren zahlreiche Missverständnisse, die Ihnen bei Gesprächen begegnen könnten. Wir haben die häufigsten Fehlannahmen zusammengestellt und liefern Ihnen die Aufklärung gleich mit dazu.

Missverständnis 1: Verschlüsselung ist sehr schwierig

»Verschlüsselung ist ein komplexes Thema, bei dem man unbedingt Experten für die Umsetzung benötigt.« Diese Annahme stimmt zum Teil, denn Verschlüsselung ist tatsächlich komplex – mathematisch gesehen. Die gute Nachricht: Sie brauchen die Algorithmen nicht zu verstehen, um Informationen zu verschlüsseln. Verwenden Sie die Software, die von den Verschlüsselungsexperten angeboten wird. Sie ist so gestaltet, dass Sie sich nicht direkt mit der Mathematik befassen müssen, und bietet eine Benutzeroberfläche, die eine einfache Bedienung erlaubt.

Verschlüsselungssoftware ist so gestaltet, dass auch Personen ohne Fachwissen sie bedienen können.

Missverständnis 2: Verschlüsselung erfordert zeitraubende Schulungen

Die Vorstellung, dass alle Mitarbeitenden oder ganze Abteilungen stundenlang in Schulungen sitzen, ist für viele Unternehmen eine abschreckende Vorstellung. Das ist aber auch gar nicht nötig.

Verschlüsselungssoftware kann verschiedene Strategien verfolgen (Verschlüsselung aller Dateien, automatische Auswahl schützenswerter Dokumente und so weiter – das können Sie in Kapitel 5 nachlesen). Eines haben jedoch alle guten Programme gemein: Die Verschlüsselung erfolgt auf eine Art und Weise, die die Arbeitsabläufe möglichst wenig beeinträchtigt. Das hat den positiven Nebeneffekt, dass der zusätzliche Schutz nichts ist, an das die Mitarbeitenden zusätzlich denken müssen. Ist die Verschlüsselung einmal installiert und wurde die Funktionsweise der Software verstanden, bekommt das Team davon kaum mehr etwas mit.

Verschlüsselungssoftware ist so gestaltet, dass sie sich gut in bestehende Arbeitsprozesse einfügt.

Missverständnis 3: Verschlüsselung ist teuer

Es hilft Ihnen wenig, wenn wir einfach behaupten, dass das nicht stimmt, denn »teuer« und »billig« sind relative Begriffe. Beim Thema Verschlüsselung ergibt es deshalb Sinn, die Kosten im Verhältnis zu einem Cyberangriff oder einem Datenleck zu sehen.

Betrachten Sie also die Lizenzgebühr für die Verschlüsselungslösung und überlegen Sie, welche Kosten entstehen könnten. Wie hoch wäre der Schaden, wenn es durch ein Datenleck zum Vertrauensverlust bei Partnern und Kunden kommt? Welche Kosten entstehen durch den Anfall bestimmter IT-Systeme und Anlagen? Mit welchen Strafzahlungen und Lösegeldern muss kalkuliert werden? Die Überlegungen sind dabei mit der Kalkulation einer Vollkasko-Versicherung für ein Auto vergleichbar. Nur dass Sie diesmal nicht den Blechschaden als Maßstab nehmen, sondern den wirtschaftlichen Verlust, den Ihr Unternehmen schlimmstenfalls erleiden würde.

Verschlüsselungssoftware ist günstiger als der Schaden, der entsteht, wenn Sie keine Verschlüsselungssoftware einsetzen.

Missverständnis 4: Verschlüsselung macht Computer langsam

Die Vorstellung, dass beim Rechner ständig der Lüfter auf Hochtouren läuft und die Performance leidet, ist unangenehm. Tatsächlich stellt Verschlüsselung für moderne Geräte aber keine Herausforderung mehr dar. Selbst Mobilgeräte sind so leistungsstark, dass die Einbußen durch Verschlüsselung kaum spürbar sind. Dieses Problem ist bei den Standard-Geräten, die man im Büroalltag benötigt, also zu vernachlässigen.

Anders sieht es bei Geräten aus, die zum Internet of Things (IoT) gehören. Eine smarte Glühbirne hat möglicherweise nicht die Ressourcen, um verschlüsselt zu funktionieren. Geräte, auf denen Sie Dateien speichern und bearbeiten, aber mit Sicherheit schon.

Einen Flaschenhals gibt es an anderer Stelle: Die Antwortzeiten der Server der Cloud-Anbieter. Die Verschlüsselung arbeitet in der Regel schneller, als der Cloud-Speicher die Daten annehmen kann. So wird der Prozess der sicheren Datenablage nicht durch die Verschlüsselung gedrosselt, sondern durch die Speicherung.

Verschlüsselung kann von modernen Geräten ohne Einbußen bei der Rechenleistung durchgeführt werden.

Missverständnis 5: Meine Daten sind schon verschlüsselt

Verschlüsselung ist überall. Wie in Kapitel 5 beschrieben wurde, verwenden viele Services Verschlüsselung zum Schutz der Daten während der Übertragung. Entscheidend ist aber, ob es sich um Ende-zu-Ende-Verschlüsselung oder sogar Zero-Knowledge-Verschlüsselung handelt. Zur Erinnerung: Das ist Verschlüsselung, bei der nur autorisierte Sender und Empfänger den Schlüssel haben.

Dieses hohe Sicherheitsniveau erhalten Sie in der Regel nicht automatisch. Sie müssen es durch zusätzliche Software oder einen passwortgeschützten Nutzer-Account erzeugen, denn aus dem Passwort wird der Schlüssel für die Verschlüsselung generiert.

Wenn Sie beispielsweise an die Transportverschlüsselung (TLS) im Browser denken, dann ist der Datenverkehr zwar durch Verschlüsselung geschützt, aber

eben nicht durch Ende-zu-Ende-Verschlüsselung. Genauso ist es, wenn Sie einen Cloud-Speicher ohne zusätzlichen Schutz verwenden.

Verschlüsselungssoftware unterstützt sie dabei und organisiert die Prozesse im Hintergrund, die nötig sind, um den Schlüsselaustausch und die Ver- und Entschlüsselung durchzuführen.

Zero-Knowledge-Verschlüsselung muss meist aktiv und selbstständig implementiert werden, um ein hohes Schutzniveau zu erreichen.

Ausnahmen sind Cloud-Anbieter, die bereits eine Ende-zu-Ende-Verschlüsselung eingebaut haben. Doch davon gibt es nur wenige und die Kombination mit anderen Speichermedien oder Clouds ist nicht möglich, wie wir im Abschnitt zur Zero-Knowledge-Cloud bereits erläutert haben (siehe Kapitel 8).

Missverständnis 6: Verschlüsselung wird früher oder später ohnehin gebrochen

Dieses Vorurteil hat einen historischen Hintergrund. Bevor Verschlüsselung auf mathematischen und wissenschaftlichen Prinzipen aufbaute, war es möglich, sie zu knacken.

Heute gibt es kaum noch Angriffe auf Verschlüsselung. Der Grund ist: Es lohnt sich einfach nicht, da die Erfolgsaussichten zu gering sind. Und das ist auch schon der wichtigste Beweis dafür, dass es sich bei der Annahme, Verschlüsselung sei ohnehin knackbar, um ein Missverständnis handelt.

Selbst wenn ein Algorithmus in unbestimmter Zukunft vielleicht mal gebrochen werden könnte, lohnt sich der Einsatz von Verschlüsselung trotzdem. Und zwar aus zwei Gründen:

1. Die Zahl der Angreifer wird reduziert. Wenn nur noch diejenigen übrigbleiben, die möglicherweise über ausreichend Fähigkeiten verfügen, Verschlüsselung zu knacken, so sind die Inhalte doch vor allen anderen (mutwilligen oder versehentlichen) Zugriffen geschützt.

2. Verschlüsselung ist bewährter Standard im Bereich Datenschutz und in vielen Fällen durch Gesetze und Regelungen vorgeschrieben. So kann es allein aus Haftungsgründen notwendig sein, Verschlüsselung zu implementieren.

Verschlüsselung ist immer besser als keine Verschlüsselung.

Teil V
Anhang

Hilfreiche Links und Wissenswertes

Wer ist für Datenschutz zuständig?

Europäische Unternehmen benötigen spätestens seit der Einführung der DSGVO 2018 einen **Datenschutzbeauftragten** – zumindest dann, wenn mindestens 20 Mitarbeiterinnen und Mitarbeiter regelmäßig personenbezogene Daten verarbeiten. Dieser Datenschutzbeauftragte kann jemand aus dem eigenen Team sein oder ein externer Experte. Letztendlich haftbar bei Datenschutzverstößen ist jedoch der **CEO**, wodurch es auch im Interesse der obersten Management-Ebene liegt, den Datenschutz zu wahren (bedenken Sie das, wenn Sie intern nach Verbündeten suchen).

Eine wichtige Schlüsselfigur sind außerdem die **IT-Systemadministratorinnen und -administratoren**, die am Ende für den reibungslosen Ablauf sorgen müssen. Besonderes Interesse an der Umsetzung von Datenschutz im Sinne von Zugriffsbeschränkungen hat der oder die Compliance-Beauftragte.

Weitere Positionen, die mit dem Thema Verschlüsselung in Berührung kommen, sind der Chief Information and Security Officer (CISO), der IT-Systems Engineer, der Referent für Datenschutz, der Datenschutzberater, der Berater für IT-Compliance und der Wirtschaftsjurist.

Was ändert sich durch Quantencomputer?

Quantencomputer basieren auf einem physikalischen Verfahren, das eine extrem hohe Rechenleistung ermöglicht. Experten gehen davon aus, dass bis zum Jahr 2031 der Einsatz so weit optimiert ist, dass die heute gängigen asymmetrischen Verschlüsselungsalgorithmen mit einem Quantencomputer geknackt werden können.

Das klingt im ersten Moment schockierend. Allerdings entwickelt sich parallel auch die Forschung im Bereich der Quantenkryptografie weiter, sodass wir damit

rechnen können, auch bald ebenso starke, neue Verschlüsselungssysteme zu erhalten.

Weitere Informationen zum Thema Quantenverschlüsselung können Sie hier nachlesen: `https://boxcryptor.info/quanten`.

Wie kann ich mich beim Thema Verschlüsselung auf dem Laufenden halten?

Ob es nun eine bahnbrechende Erfindung wie der Quantencomputer oder einfach nur ein neues Datenschutzgesetz ist – Sie sollten das Thema Verschlüsselung im Blick haben, damit Sie Neuigkeiten mitbekommen und für Ihr Unternehmen einordnen können. Damit Ihnen das leicht fällt, haben wir einige Quellen für Sie zusammengestellt.

Dr. Datenschutz – ein Blog für Fachleute

Wer sich beruflich mit den Themen Datenschutz, IT-Sicherheit und IT-Forensik befasst, für den ist die Webseite *Dr. Datenschutz* genau das richtige. Das Team aus Juristinnen und Juristen veröffentlicht jeden Tag einen umfangreichen und gut recherchierten Artikel zu den genannten Themenbereichen. Dabei gehen sie oft auf aktuelle Themen ein, wie DSGVO-Bußgelder oder wegweisende Gerichtsurteile im Bereich Datenschutz. Wir empfehlen den Newsletter, der jeden Artikel zuverlässig und bequem ins eigene E-Mail-Postfach liefert.

`www.dr-datenschutz.de`

Boxcryptor-Blog – Schwerpunkt Cloud-Verschlüsselung

In unserem Unternehmensblog behandeln wir regelmäßig wichtige Themen aus dem Bereich der Cloud-Security und Cloud-Verschlüsselung. Wir richten uns

mit unseren Artikeln an Privatnutzer sowie Unternehmen, die einen oder mehrere Cloud-Dienste nutzen und diese absichern wollen.

Einsteigerthemen und Fachartikel wechseln sich ab. Mit einem Newsletter-Abo verpassen Sie keines davon. Und ganz nebenbei sind Sie über die neuesten Produkt-Entwicklungen bei Boxcryptor bestens informiert.

`www.boxcryptor.com/blog`

National Institute of Standards and Technology (NIST)

Bei der US-amerikanischen Behörde für Standardisierung finden Sie allgemeine Informationen und Publikationen zum Thema Verschlüsselung.

Besonders interessant sind die Veröffentlichungen rund um das Projekt Post-Quantum Cryptography Standardization. Es wurde ins Leben gerufen, um einen oder mehrere Quanten-resistente kryptografische Algorithmen, unter anderem für asymmetrische Verschlüsselungsverfahren, zu bewerten und zu standardisieren.

`www.nist.gov/cryptography`

Bundesamt für Sicherheit in der Informationstechnik

Konkrete Empfehlungen zum Thema Verschlüsselung erhalten Sie beim deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI). Unternehmen aus dem Bereich der kritischen Infrastruktur müssen sich an das BSI-Gesetz halten und IT-Sicherheit nach »Stand der Technik« umsetzen. Alle anderen Unternehmen und Organisationen finden auf den Webseiten des BSI ebenfalls hilfreiche Veröffentlichungen.

`www.bsi.bund.de`

Soziale Netzwerke – Suchfunktion nutzen

Der Kurznachrichtendienst Twitter ist dafür bekannt, dass Neuigkeiten sich hier besonders schnell verbreiten. Unserer Erfahrung nach kann man hier fachlich interessante Accounts entdecken und Themen verfolgen. Nutzen Sie dafür die Hashtag-Funktion. Mit einer Raute markierte Wörter werden automatisch in einen Link umgewandelt und führen zu einer Liste weiterer, passender Tweets. Erfahrungsgemäß eignen sich folgende Hashtags besonders gut:

- ✔ #Datenschutz
- ✔ #Datensicherheit
- ✔ #Verschlüsselung
- ✔ #TeamDatenschutz

Bitte bewerten Sie die Kanäle, denen Sie folgen, genau und prüfen Sie die Quelle der Informationen. Im Bereich Datenschutz sind uns bisher noch keine Verschwörungserzählungen begegnet, grundsätzlich besteht dafür aber in sozialen Netzwerken immer eine gewisse Gefahr.

`www.twitter.com`

Stichwortverzeichnis

Datensicherheit in die Cloud auslagern – Datenschutz souverän managen

Daten in der Cloud zu speichern, ist kosteneffizient und sorgt für hohe Verfügbarkeit. Doch Cloud-Speicher haben einen großen Nachteil: den Kontrollverlust über die Inhalte der Dateien und damit die mangelnde Datensicherheit. Der Datenschutz kann nicht konsequent gewährleistet werden, Betriebsgeheimnisse und personenbezogene Daten werden einem externen Anbieter anvertraut. In diesem Buch erfahren Sie, wie Verschlüsselung dieses Dilemma löst. Außerdem erhalten Sie handfeste Tipps für die Einführung einer Verschlüsselungslösung in Ihrem Unternehmen.

Sie erfahren

- Wie Sie sensible Daten DSGVO-konform in der Cloud speichern
- Welche Rolle Verschlüsselung beim Datenschutz spielt
- Wie Sie Verschlüsselung in Ihrem Unternehmen einführen

Lisa Figas ist Expertin für Privatsphäre im Netz und spricht auf Konferenzen über internationale Datenschutzgesetze in gesellschaftlichem Kontext. **Moritz Ober** ist Datenschutz-Experte bei der Secomba GmbH Boxcryptor und schreibt über Sicherheitsanwendungen für Unternehmen in verschiedensten Branchen.

Mach dich schlau:
www.fuer-dummies.de

WILEY

für dummies®

boxcryptor

Coverfoto: © Secomba GmbH

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley's ebook EULA.