Bundesverband IT-Sicherheit e.V.

TeleTrusT
Pioneers in IT security.

Leitfaden Cloud Security

Sichere Nutzung von Cloud-Anwendungen

2021

Danksagung

Diese Publikation wurde in der TeleTrusT-Arbeitsgruppe "Cloud Security" erarbeitet. TeleTrusT bedankt sich bei den nachstehenden Personen für ihre Mitwirkung sowie für die aktive Mitgestaltung dieses Positionspapieres.

Projektleitung
Oliver Dehning, Leiter der TeleTrusT-AG "Cloud Security"

Autorenliste (Auszug)

Bartels, RA Karsten U. LL.M. - HK2 Rechtsanwälte
Bernard, Dr. Yvonne - Hornetsecurity
Cink, Stefan - Net at Work
Demand, Marion - BSI
Gora, Stefan - secorvo
Hansemann, Peter - ICN
Jäger, Dr. Hubert - Digital Trust Innovations
Kahrs, Malte - MTRIX
Kipker, Dr. Dennis-Kenji - Universität Bremen
Kurz, Alexander - eperi
Lawicki, Tomasz - m3 management consulting
Pfeiffer, Anna Katharina - esatus
Rieken, Dr. Ralf - Uniscon
Rost, Peter - secunet
Simon, Yvonne - eperi
Weiss, Andreas - eco

Redaktion

Abou Nasser, Morad - Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Mühlbauer, Dr. Holger - Bundesverband IT-Sicherheit e.V. (TeleTrusT)

In dieser Publikation werden zahlreiche Anglizismen verwendet, da sie sich in der zugrundeliegenden Fachdiskussion branchentypisch verfestigt haben.

Dieses Dokument dient als Anhaltspunkt und bietet einen Überblick. Er erhebt weder Anspruch auf Vollständigkeit noch auf die exakte Auslegung der bestehenden Rechtsvorschriften. Er darf nicht das Studium der relevanten Richtlinien, Gesetze und Verordnungen ersetzen. Des Weiteren sind die Besonderheiten der jeweiligen Produkte sowie deren unterschiedliche Einsatzmöglichkeiten zu berücksichtigen. Insofern sind bei den im Dokument angesprochenen Beurteilungen und Vorgehensweisen eine Vielzahl weiterer Konstellationen denkbar.

Impressum

Herausgeber:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Chausseestraße 17
10115 Berlin
Tel.: +49 30 400 54 310
Fax: +49 30 400 54 311
E-Mail: info@teletrust.de
https://www.teletrust.de

© 2021 TeleTrusT

Inhalt

Zusammenfassung **5**

1 Einleitung **6**
1.1 Motivation 6
1.2 Definitionen 7
1.3 Scope 8

2 Risiken bei der Nutzung von Cloud Services **9**
2.1 Allgemeine IT-Risiken 9
2.1.1 Risiken aufgrund von Cyber-Angriffen (Cyber-Risiken) 9
2.1.2 Risiken aus menschlicher Handlung (menschliche Risiken) 9
2.1.3 Risiken aufgrund technischer Fehler (technische Risiken) 10
2.1.4 Risiken aus Verletzung rechtlicher Vorgaben (rechtliche Risiken) 10
2.1.5 Risiken durch Naturgewalten (Naturgewalt-Risiken) 10
2.2 Cloud-spezifische Risiken 10
2.3 Rechtliche Anforderungen / Datenschutzanforderungen 11
2.4 Sicherheitsvorteile von Cloud Services 15

3 Technische Maßnahmen zur Sicherung der Nutzung von Cloud Services **16**
3.1 Nutzung von in Cloud Services enthaltenen Sicherheitsmechanismen 16
3.2 Identity und Access Management 16
3.2.1 Multi-Faktor-Authentisierung (MFA) 17
3.2.2 Identity-Provider 18
3.2.3 Single-Sign-On 19
3.2.4 Integrierte Verschlüsselung 21
3.3 Cloud Security Layer 22
3.3.1 Cloud Access Security Broker (CASB) 22
3.3.2 Cloud Encryption Gateway 22
3.3.2.1 E-Mail-Verschlüsselung 23
3.3.2.2 E-Mail-Authentication 24
3.3.2.3 Abwehr von Spam und Malware 25
3.3.3 Cloud VPN 26
3.3.3.1 Definition "Cloud VPN" 26
3.3.3.2 Einsatzzweck und Vorteile von VPNs 27
3.3.3.3 Nachteile von VPNs 27
3.3.3.4 VPN Varianten 28
3.3.3.5 Fazit VPN 29
3.3.4 Cloud Firewall 29
3.3.4.1 Definition "Cloud Firewall" 29
3.3.4.2 Gemeinsamkeiten Cloud Firewall und herkömmliche Firewalls 29
3.3.4.3 Nachteile von Cloud Firewalls 30
3.3.4.4 Vorteile von Cloud Firewalls 30
3.3.4.5 Anforderungen und Aufgaben zu Cloud Firewalls 30
3.3.5 Confidential Computing 30
3.3.5.1 Vor welchen Bedrohungen schützt Confidential Computing? 30
3.3.5.2 Welche Implementierungen von Confidential Computing gibt es? 31
3.3.5.3 Grenzen von Confidential Computing 31
3.4 Backup Strategien Cloud / Notfallplanung 32
3.4.1 Konzepte für Backup und Wiederherstellung 32
3.4.2 Anforderungen an Backup und Wiederherstellung 32
3.4.3 Verteilte IT-Infrastruktur 32
3.4.4 Anbindung an die Cloud 32
3.4.5 Geolokalisierung Datenspeicher 32
3.4.6 Backupverfahren 32
3.4.7 Notfallplanung 33

4 Organisatorische und rechtliche Maßnahmen zur Sicherung **34**
4.1 Aufgabenverteilung zwischen Anbieter und Nutzer 34
4.2 Vertragsgestaltung 36

4.2.1 Einleitung ... 37
4.2.2 Datenschutzrechtliche Verantwortlichkeit ... 37
4.2.3 DPA nach Art. 28 DSGVO ... 37
4.2.4 Empfohlene zusätzliche Regelungen ... 38
4.2.5 Datentransfer in Drittstaaten ... 40
4.2.6 Fazit Vertragsgestaltung ... 41

5 Testate und Zertifikate ... 42
5.1 Wie kann ich als Anwender Zertifikate und Testate nutzen? ... 42
5.2 Was erhalte ich? ... 42
5.3 Unterschied Zertifikate/Testate ... 42
5.4 Landschaft ... 43
5.5 Zertifikate bei Cloud ... 43
5.6 Testate bei Cloud ... 43

6 Glossar ... 45

Zusammenfassung

Cloud Computing ist inzwischen ein breit akzeptiertes IT-Betriebsmodell und wird von den allermeisten Unternehmen genutzt. Auch viele IT-Anbieter haben in ihrer Strategie auf "Cloud First" gewechselt, zum Teil sogar auf "Cloud Only". Die Bedrohungslage hat sich ebenfalls verändert: Cloud-Plattformen sind zunehmend im Blickfeld von Cybercrime. Die sichere Nutzung von Cloud Services ist deshalb ein zentraler Baustein der IT-Sicherheit von Unternehmen insgesamt.

Der vorliegende Leitfaden richtet sich vorwiegend an kleine und mittlere Unternehmen. Er beginnt mit einer systematischen Betrachtung der Risiken bei der Nutzung von Cloud-Diensten, gegliedert nach allgemeinen IT-Risiken, Cloud-spezifischen Risiken und rechtlichen Anforderungen. Betrachtet werden auch die Sicherheitsvorteile von Cloud Services.

Der Leitfaden zeigt dann technische, organisatorische und rechtliche Maßnahmen zur Reduktion und Beherrschung ermittelter Risiken auf. Neben Mechanismen und Konfigurationsmöglichkeiten, die integraler Bestandteil der Cloud-Dienste sind, wird fokussiert auf externe Sicherungsmechanismen eingegangen: Identity-Provider, Cloud Access Security Broker (CASB), Cloud Encryption Gateways, E-Mail Security Gateways, Cloud VPNs, Cloud Firewalls, Confidential Computing, Backup und Notfallplanung.

Im Bereich organisatorischer Maßnahmen wird auf die Aufgabenverteilung zwischen Anbieter und Nutzer sowie auf die Vertragsgestaltung eingegangen. Der Leitfaden schließt mit einer Betrachtung von Testaten und Zertifikaten im Cloud-Umfeld.

1 Einleitung

1.1 Motivation

Die erste Ausgabe dieses Leitfadens wurde 2012 von der TeleTrusT-AG "Cloud Security" veröffentlicht. Damals stand Cloud Computing noch in den Anfängen, war im Markt wenig verbreitet und wurde von vielen Akteuren skeptisch gesehen.

Die Situation hat sich seitdem grundlegend verändert: Cloud Computing ist inzwischen ein breit akzeptiertes IT-Betriebsmodell. Die allermeisten Unternehmen nutzen heute Cloud Services in irgendeiner Form. Viele IT-Anbieter haben in ihrer Strategie auf "Cloud First" gewechselt, zum Teil sogar auf "Cloud Only". Die weltweiten Ausgaben für Public Cloud Services werden laut Gartner im Jahr 2021 304,9 Mrd. US-Dollar betragen, ein Wachstum von 18,4% gegenüber 2020. Das Tempo des Wachstums wird dabei durch die Corona-Pandemie noch beschleunigt. Bis zum Jahr 2024 soll der Anteil der Ausgaben für Cloud Computing auf 14,2% der Unternehmensausgaben für IT wachsen, gegenüber 9,1% im Jahr 2000[1].

Für Unternehmen stellt sich daher kaum noch die Frage, ob Cloud Computing genutzt werden kann, sondern wie - insbesondere mit Blick auf die IT-Sicherheit. Auch die Bedrohungslage hat sich nämlich verändert: Cloud-Plattformen sind zunehmend im Blickfeld von Cybercrime.

Hinzu kommt, dass sich seit 2012 auch die gesetzlichen Rahmenbedingungen erheblich verändert haben. 2015 brachte das IT-Sicherheitsgesetz (ITSiG) und kurz darauf erschien die KRITIS-VO, die die Vorgaben an die IT-Sicherheit der kritischen Infrastrukturen konkretisierte. 2018 wurde die EU-Datenschutz-Grundverordnung wirksam. Die Entscheidung des EuGH zum Privacy-Shield-Abkommen wirft zudem die Frage auf, ob Cloud Services US-amerikanischer Anbieter aus Datenschutzsicht überhaupt genutzt werden können.

Die sichere Nutzung von Cloud Services ist deshalb ein zentraler Baustein der IT-Sicherheit von Unternehmen insgesamt. Insbesondere kleine und mittlere Unternehmen müssen dabei unterstützt werden. Sie haben oft nicht die nötigen Kapazitäten zum Aufbau eigener Expertise.

Die vorliegende neue und deutlich überarbeitete Fassung des TeleTrusT-Leitfadens "Cloud Security" richtet sich daher vorwiegend an kleine und mittlere Unternehmen. Er soll einen Überblick und Hilfestellung zum sicheren Betrieb von Cloud Services geben.

[1] Gartner, Inc.: Gartner Forecasts Worldwide Public Cloud End User Spending to Grow 18% in 2021; Nov. 2020; https://www.gartner.com/en/newsroom/press-releases/2020-11-17-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-18-percent-in-2021

1.2 Definitionen

Cloud Computing

Cloud Computing ist ein Ansatz, der den bequemen On-Demand-Netzwerk-Zugriff auf einen gemeinsamen Pool konfigurierbarer Rechner-Ressourcen (z. B. Netzwerke, Server, Speichersysteme, Anwendungen und Dienstleistungen) ermöglicht, die mit nur geringem Management-Aufwand oder Eingriff eines Service-Anbieters schnell bereitgestellt und freigegeben werden können.

Nach der Definition des NIST[2] zeichnet sich Cloud Computing durch die folgenden fünf Kriterien aus:

1. Automatisierte Bereitstellung mit bedarfsorientierter Zugriffsmöglichkeit
2. Breitbandiger Netzwerkzugriff
3. Pooling von Ressourcen
4. Vollständige Elastizität und Skalierbarkeit
5. Nutzungsabhängige Zahlung ("Pay per use"-Prinzip)

Es werden die folgenden Bereitstellungs- (Deployment-) und Service-Modelle unterschieden:

- Deployment-Modelle:
  1. Public Cloud
  2. Private Cloud
  3. Community Cloud
  4. Hybrid Cloud

(im Leitfaden Fokus auf Angebote mit Public-Cloud-Eigenschaften - Public Cloud, Hybrid Cloud, Virtual Private Cloud etc.)

- Service Modelle:
  1. Infrastructure-as-a-Service (IaaS)
  2. Platform-as-a-Service (PaaS)
  3. Software-as-a-Service (SaaS)

Informationssicherheit

ISO 27000 definiert Informationssicherheit als Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen[3]. Weitere Schutzziele der Informationssicherheit sind Authentizität, Zurechenbarkeit, Nicht-Abstreitbarkeit und Verlässlichkeit. Systeme sollen vor Gefahren bzw. Bedrohungen geschützt, Schäden vermieden und Risiken minimiert werden.

Vertraulichkeit, Integrität und Verfügbarkeit werden in der Norm wie folgt definiert:

- Vertraulichkeit: Informationen dürfen unberechtigten Personen, Einheiten oder Prozessen nicht verfügbar gemacht oder enthüllt werden. Das System muss so aufgebaut sein, dass ein Zugriff nur für befugte (autorisierte) Personen oder Dienste möglich ist.

- Integrität: Absicherung von Richtigkeit und Vollständigkeit von Werten. Informationen, Systeme und Netze dürfen nicht unbemerkt verändert werden können. Das System muss so beschaffen sein, dass eine Veränderung offensichtlich wird. Die Sicherstellung der Integrität beinhaltet die Komponenten Übereinstimmung, Genauigkeit, Korrektheit und Vollständigkeit.

- Verfügbarkeit: Informationen, Systeme und Netze müssen verfügbar, d.h. einer berechtigten Einheit auf Verlangen zugänglich sein und genutzt werden können. Das System muss bei einem Zugriff in einem definierten Zeitraum antworten bzw. bestimmte Aktionen ausführen. Zum Schutzziel der Verfügbarkeit werden die Komponenten Fehlertoleranz, Zuverlässigkeit, Robustheit und Wiederherstellbarkeit gezählt.

---

[2] NIST- National Institute of Standards and Technology, 2011, The NIST Definition of Cloud Computing, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[3] ISO/IEC 27000:2018

1.3 Scope

Der vorliegende Leitfaden zur sicheren Nutzung von Cloud-Anwendungen richtet sich vorwiegend an kleine und mittlere Unternehmen. Er beginnt mit einer systematischen Betrachtung der Risiken bei der Nutzung von Cloud-Diensten. Die Einschätzung dieser Risiken ist im konkreten Fall durch die Anwender in Bezug auf Datensicherheit, Verfügbarkeitsanforderungen, regulatorischer Rahmenbedingen und gesetzlicher Anforderungen vorzunehmen.

Ein wichtiges Element ist die Datenschutz-Folgeabschätzung im Sinne der DSGVO. Bei der zusätzlichen Nutzung von Cloud-Diensten sind entsprechende Dokumentationspflichten zu erfüllen, die besonders auch die technischen und organisatorischen Maßnahmen des Anbieters und auch den Rechtsraum der Speicherung und Verarbeitung der Daten eindeutig regelt. Eine wesentliche Grundlage stellen die hier gemachten Empfehlungen zur sicheren Nutzung von Cloud-Diensten.

Im Weiteren zeigt der Leitfaden technische, organisatorische und rechtliche Maßnahmen zur Reduktion und Beherrschung ermittelter Risiken auf. Zur Einschätzung der Wirksamkeit solcher Maßnahmen bieten Cloud-Anbieter oftmals eine Reihe von Zertifikaten, Testaten und Gütesiegeln an, die eine qualitative Bewertung zur Umsetzung notwendiger technischer und organisatorischer Maßnahmen durch geschulte unabhängige Prüfer darstellt.

2 Risiken bei der Nutzung von Cloud Services

2.1 Allgemeine IT-Risiken

IT-Risiken und deren systematische Behandlung haben insbesondere aufgrund der starken Abhängigkeit von Geschäftsprozessen von der Informationstechnologie eine hohe Bedeutung. Angetrieben wird dies durch fortschreitende Digitalisierung, wachsende Funktionsvielfalt, Vernetzung der Infrastruktur, komplexere Prozesse bei kürzeren Reaktionszeiten und schärfere Compliance-Vorgaben. Es gibt heutzutage kaum Geschäftsprozesse, die nicht von der Verfügbarkeit der Informationstechnologie abhängen. Ausfälle wichtiger IT-Komponenten haben enorme Auswirkung auf die Geschäftsprozesse und können zu beträchtlichen wirtschaftlichen Schäden führen.

Ein Risiko wird im Allgemeinen definiert als die Eintrittswahrscheinlichkeit eines künftigen Ereignisses mit einer daraus folgenden Auswirkung auf ein bestimmtes Objekt. IT-Risiken beziehen sich auf mögliche Ereignisse mit negativer Auswirkung auf die IT-Infrastruktur, IT-Anwendungen und IT-Services. Aufgrund der möglichen Schäden ist es wichtig diese Risiken frühzeitig zu identifizieren, zu reduzieren oder zu beseitigen und sie nicht zu Vorfällen werden zu lassen.

Es gibt eine Fülle von Risiken, die im Umfeld der Informationstechnologie identifiziert werden können. Beispielsweise nennt der BSI Standard 200-3 bis zu 47 sogenannte elementare Gefährdungen mit Auswirkung auf die IT. [4] [5] Diese könnten in den folgenden Gruppen zusammengefasst werden:

2.1.1 Risiken aufgrund von Cyber-Angriffen (Cyber-Risiken)

Spricht man über IT-Risiken, werden sehr schnell Risiken aufgrund von Cyber-Angriffen genannt. Dazu gehört jegliche Art von Angriffen auf die IT-Infrastruktur (gezielt oder zufällig). Das sind beispielsweise (Auswahl):

- **DDoS-Angriffe**
  Bei einem Distributed Denial of Service (DDoS) Angriff wird ein angegriffenes System oder ein angegriffener Service mit Datenanfragen überflutetet, bis er überlastet ist und nicht mehr funktioniert. Ein auf diese Weise angegriffener Dienst (z.B. eine Webseite) ist dadurch nicht mehr erreichbar. Somit ist die Auswirkung eines solchen Angriffs in diesem Fall die fehlende Verfügbarkeit des Dienstes (Schaden), aber das zu betrachtende Risiko wäre die erfolgreiche menschliche Handlung.

- **Advanced Persistent Threats**
  Advanced Persistent Threats (APT) sind langfristig angelegte, komplexe Angriffe, die darauf abzielen, Systeme zu infiltrieren und/oder so viele wertvolle Daten wie möglich zu erspähen, ohne entdeckt zu werden.

- **Malware**
  Bei Malware handelt es sich um Programme, die dem Angriffsziel bewusst Schaden zufügen sollen. Dazu gehören beispielsweise Viren, Trojaner, Rootkits oder Spyware. Oftmals werden die Programme verwendet, um weitere Angriffe vorzubereiten.

- **Ransomware**
  Ransomware steht für eine Spezies von Schadprogrammen, die den Zugriff auf Daten und Systeme einschränken oder unterbinden (z.B. durch Verschlüsselung). Für die Freigabe wird dann ein Lösegeld verlangt. Neuere Versionen der Angriffe leiten auch gezielt wertvolle oder kompromittierende Daten aus und drohen mit deren Veröffentlichung.

2.1.2 Risiken aus menschlicher Handlung (menschliche Risiken)

Nicht nur durch externe Angriffe, sondern ebenfalls durch interne Handlungen entstehen Risiken für die Informationstechnologie. Diese Handlungen können sowohl gewollt als auch ungewollt geschehen.

---

[4] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_3.html

[5] Gefährdungen sind nach Definition des BSI das Zusammenwirken von Bedrohungen (z. B. Naturkatastrophen, Pandemien, Einbruch, Hacker, Innentäter) und Schwachstellen (z. B. Softwarefehler, organisatorische Mängel, technische Defekte). Konkretisierte und mit der Eintrittswahrscheinlichkeit versehenen Gefährdungen sind Risiken.

Die gewollten Handlungen erfolgen oftmals aus niederen Beweggründen. Es sind beispielsweise gekündigte Mitarbeiter, die als Rache den gesamten Kundenbestand des nun ehemaligen Arbeitgebers löschen.
Darüber hinaus können Risiken aus ungewollter Handlung interner Mitarbeiter zu großen Schäden der verwendeten Informationstechnologie führen. Solche ungewollten Handlungen sind beispielsweise die Verwendung einfacher Passwörter, ihre Weitergabe oder versehentliche Fehler bei der Konfiguration von sicherheitsrelevanten IT-Komponenten. Ebenfalls das sogenannte "Social Engineering" gehört zu dieser Kategorie. Dabei wird die menschliche Gutgläubigkeit durch externe Angreifer gezielt ausgenutzt, um an sicherheitsrelevante Informationen zu kommen.

2.1.3 Risiken aufgrund technischer Fehler (technische Risiken)

Zu den größten technischen Risiken gehören insbesondere Ausfälle aufgrund technischer Fehler. Gründe sind beispielsweise Materialermüdung und Abnutzung von IT-Komponenten, ein Stromausfall (z.B. hervorgerufen durch Baggerarbeiten) oder auch Systemfehler (insbesondere Softwarefehler) sowie wartungsbedingte Ausfälle.

2.1.4 Risiken aus Verletzung rechtlicher Vorgaben (rechtliche Risiken)

Strikt genommen, sind Risiken aus Verletzung von rechtlichen Vorgaben keine unmittelbaren IT-Risiken. Allerdings spätestens mit der Publikation der europäischen Datenschutz-Grundverordnung (DSGVO) sind Maßnahmen zur Sicherung von IT-Systemen verpflichtend. Nicht-Einhaltung kann mit sehr hohen Strafen geahndet werden und muss somit in die Risiko-Betrachtung aufgenommen werden.

2.1.5 Risiken durch Naturgewalten (Naturgewalt-Risiken)

Durch die erkennbare Klimaveränderung rücken die Risiken aufgrund höherer Gewalt mehr in den Vordergrund. So stellen Überflutungen, Starkregen, Erdbeben und Stürme Risiken mit Auswirkung auf die Informationstechnologie dar.

Unabhängig davon, ob die verwendete Informationstechnologie in Haus (on-premise) oder ausgelagert (Cloud) ist, müssen die IT-Risiken betrachtet, ihre Eintrittswahrscheinlichkeit ermittelt und geeignete Maßnahmen aufgesetzt werden.

2.2 Cloud-spezifische Risiken

Die Speicherung und Verarbeitung von Daten in einem Cloud-Dienst bedeuten eine Abgabe von direkter Kontrolle gegenüber dem Betrieb eigener IT-Systeme, auch wenn die tatsächliche Kontrolle eigener IT-Systeme oft geringer ist als gemeinhin angenommen. Vor allem bisherige Perimeter-Konzepte decken den heutigen Sicherheitsbedarf nicht mehr ab.

Cloud-spezifische Risiken betreffen folgerichtig vor allem die mögliche Verletzung von Compliance-Anforderungen im Kontext der Organisation, den Anforderungen der konkreten Anwendung sowie Anforderungen von Dritten, zum Beispiel aus Verträgen. Insbesondere die Erfüllung der Konformität mit der DSGVO ist hier relevant. Während der Cloud-Anbieter eine Mitwirkungspflicht hat, verbleibt die Verantwortung bei der Organisation, die die entsprechenden Analysen von insbesondere Sinn, Zweck und Ort der Speicherung sowie Verarbeitung und Schutzmaßnahmen auch hier durchführen muss.

Für Verfügbarkeit von Daten und Services ist es wichtig, basierend auf der Risikoanalyse Redundanz und Fallback-Strategien für Konnektivität zu planen. Bei besonderen Anforderungen an Konnektivität zu eigenen Prozessen und Anwendungen sowie Latenz bei Kritikalität sollte eine dedizierte Leitung mit garantierter Bandbreite geplant werden. Anforderungen an die Verfügbarkeit der Internetverbindung beim Provider sollten in einem Service-Level-Agreement vereinbart werden. Alternativ können auch redundante Verbindungen als Fallback vorgehalten werden (z.B. eine Mobilfunkanbindung via LTE o.ä. als Fallback für eine Festnetz-Anbindung).

Um unautorisierten Zugriff auf Daten und Dienste sowie unautorisierte Änderung oder Löschung von Daten zu verhindern ist es entscheidend, dass der Cloud-Dienst ein transparentes Rollen- und Rechtemodell unter Kundenverwaltung bietet, zum Beispiel auch um Subunternehmern und Lieferanten Zugriff auf für sie relevante Daten zu gewähren. Gleichzeitig stellt die Verwaltung des Rollen- und Rechtemodells ein hohes operatives Risiko dar, da Fehlbedienung unautorisierten Zugriff auf Daten ermöglichen kann, aber nur schwer zu identifizieren ist.

Bereits bei der Planung der Nutzung von Cloud-Diensten muss der Zugriff auf Daten am Vertragsende oder bei einer eventuellen Insolvenz des Providers berücksichtigt und zum Beispiel im SLA vereinbart werden. Wichtige Faktoren sind Datenumfang und Übertragungsmöglichkeiten sowie entsprechende Exportmöglichkeiten.

Es muss transparent sein, auf welchem Servicemodell der Dienst betrieben wird und welche Subunternehmer involviert sind, zum Beispiel im Fall von zukünftigen Erweiterungen. Benachrichtigungen bei relevanten Veränderungen des Betriebsmodells müssen vertraglich geregelt sein. Auch diese Aspekte sollten im SLA abgedeckt sein.

Insbesondere systemkritische Dienste müssen gegen Angriffe und Ausfälle gehärtet werden zum Beispiel durch Nutzung von Failover oder Verteilung auf mehrere Verfügbarkeitszonen. Die Umsetzung grundlegender IT-Sicherheitsmaßnahmen, zum Beispiel Schutz vor Schadsoftware, ist abhängig von dem verwendeten Servicemodell.

2.3 Rechtliche Anforderungen / Datenschutzanforderungen

Unternehmerische Compliance umfasst nicht nur allgemeine betriebswirtschaftliche, sondern im Sinne der Informationssicherheit immer stärker auch technisch-organisatorische Aspekte, die durch rechtliche Maßstäbe und Anforderungen entscheidend geprägt werden. In diesem Sinne verstanden befasst sich die IT-Compliance mit der Einhaltung derjenigen Vorgaben, die sich speziell mit der IT-Sicherheit und dem Datenschutz befassen - zwei Themenbereiche, die auch für vertrauenswürdige und zukunftsfähige Cloud-Anwendungen nicht zu vernachlässigen sind und sowohl im geschäftlichen wie auch im privaten Umfeld eine immer größere Rolle spielen.

Die in diesem Zusammenhang zu nennenden rechtlichen Erkenntnisquellen sind vielfältig, und reichen von der internationalen, über die europäische bis hin zur nationalen Regulierungsebene, erstrecken sich auf unterschiedliche gesetzgeberische Instrumentarien und erstrecken sich vom öffentlichen Recht, über das Zivilrecht, bis hin zum Strafrecht. Eine Cloud-spezifische Gesetzgebung, die sich ausschließlich mit der Sicherheit entsprechender Anwendungen befasst, existiert hingegen nicht - lediglich die NIS-Richtlinie der EU verweist in ihrem Anhang auf Cloud Computing. Dies ist nicht zuletzt auch der Tatsache geschuldet, dass Cloud Computing in den unterschiedlichsten Formen und Anwendungsszenarien vorkommen kann, was eine einheitliche Regulierung erschwert, sodass der Blick auf die IT-Sicherheitsanforderungen von Cloud immer einzelfallbezogen ist.

Gerade in den letzten Jahren hat das Tempo, mit dem immer neue gesetzgeberische Maßstäbe zur Informationssicherheit geschaffen werden, deutlich zugenommen. Das folgende Kapitel soll, ohne einen Anspruch auf Vollständigkeit zu erheben, eine Momentaufnahme des gegenwärtigen Standes der rechtlichen Anforderungen an die Informationssicherheit mit Bezug auf Cloud Computing liefern und die wesentlichen rechtlichen Grundlagen systematisieren und in der gebotenen Kürze wiedergeben.

Soweit es die IT-sicherheitsspezifische Gesetzgebung mit Relevanz für die Cloud anbelangt, können zurzeit folgende Rechtsquellen als wesentliche Impulsgeber der unternehmerischen Informationssicherheit herangezogen werden:

- die EU Netz- und Informationssicherheitsrichtlinie aus 2016 (EU NIS-RL, mit einem Vorschlag der EU-Kommission für eine NIS-RL 2 vom 16. Dezember 2020)
- die EU Datenschutz-Grundverordnung aus 2016 (wirksam geworden in 2018, DSGVO, umfasst die Verarbeitung von personenbezogenen Daten und deren Datensicherheit, mit technischen und organisatorischen Maßnahmen zur Datensicherheit in Art. 5 Abs. 1 lit. f., Art. 24 als genereller Verantwortlichkeitsnorm und Art. 32), die EU Cybersecurity-Verordnung aus 2019 (EU CSA)
- das deutsche IT-Sicherheitsgesetz aus 2015 (ITSiG) inkl. der den Anwendungsbereich konkretisierenden BSI-Kritisverordnung (BSI-KritisV aus 2016 und 2017)
- das IT-Sicherheitsgesetz 2.0 (ITSiG 2.0, Inkrafttreten am 28.05.2021)
- das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) aus 2019
- das Zweite Datenschutzanpassungs- und Umsetzungsgesetz EU aus 2019 (2. DSAnpUG-EU), das den bereichsspezifischen Bundesdatenschutz an die Vorgaben der DSGVO anpasst und in diesem Zusammenhang auch für die Informationssicherheit relevante Gesetzesänderungen enthält, z. B. im Hinblick auf das BSIG
- und die Digitale-Inhalte-Richtlinie der EU (DID-RL) aus 2019 und die entsprechenden, zurzeit für Deutschland im Gesetzgebungsverfahren befindlichen nationalen Umsetzungsgesetze, die zum 1. Januar 2022 in Kraft treten und die verbraucherbezogene IT-Sicherheit für Cloud Computing aufgreifen

Neben spezifischen Rechtsvorschriften, die ausschließlich auf Fragen der Informationssicherheit abzielen, existieren im Rahmen der IT-Compliance auch allgemeine gesetzliche Rahmenvorschriften, die sich im eigentlichen Sinne nicht explizit mit diesem Thema befassen, aber im Rahmen der juristischen Auslegung auch Pflichten zur Informationssicherheit enthalten können. Zu nennen sind hier beispielsweise die Pflichten aus § 43 GmbHG, der vorschreibt, dass

die Geschäftsführer in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden haben - die heutzutage auch Fragen der Informationssicherheit betrifft, und zwar nicht nur für Cloud, sondern in einem allumfassenden Sinne verstanden. Geschäftsführer, welche ihre entsprechenden Obliegenheiten verletzen, haften der Gesellschaft für den eingetretenen Schaden solidarisch. Das AktG schreibt in seinen §§ 91, 93 AktG im gleichen Maßstab für die Organisation, Sorgfaltspflicht und Verantwortlichkeit der Vorstandsmitglieder vor, dass von diesen geeignete Maßnahmen zu treffen sind, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen frühzeitig erkannt werden. Überdies haben auch die Vorstandsmitglieder einer Aktiengesellschaft bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden, wozu mittlerweile unstreitig auch angemessene Maßnahmen zur Informationssicherheit zählen.

Das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) aus 2019 ist mit Blick auf die Cloud Security vor allem unter dem Gesichtspunkt einer effektiven Absicherung der zu schützenden geschäftlichen Geheimnisse relevant. Ausgehend von der Definition in § 2 Nr. 1 GeschGehG ist das Geschäftsgeheimnis im Rechtssinne eine Information, die weder allgemein bekannt oder ohne Weiteres zugänglich ist und daher von wirtschaftlichem Wert ist und die Gegenstand von angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und bei der ein berechtigtes Interesse an der Geheimhaltung besteht. Soweit folglich im Geschäftsbetrieb Cloud Services genutzt werden, muss sichergestellt werden, dass die verwendeten Cloud-Lösungen hinreichend sicher sind. Denn eine Information, die nicht durch angemessene TOM (technische und organisatorische Maßnahmen) geschützt wird, genießt laut der Definition des GeschGehG nicht den Schutz eines im rechtlichen Sinne verstandenen Geschäftsgeheimnisses. Die Folge wäre eine Haftung der Geschäftsleitung für unterlassenen Schutz. Bei der Umsetzung der TOM kann eine Orientierung am entsprechenden Maßnahmenkatalog des Art. 32 DSGVO sinnvoll sein. Denkbar sind deshalb für die sichere Cloud-Nutzung im Sinne des GeschGehG vor allem die folgenden Maßnahmen: Rechtemanagement, Verschlüsselung, Separationsmechanismen, Updates und Backups.

Die IT-sicherheitsspezifischen Regelungen, die durch das deutsche ITSiG getroffen wurden, adressieren im Kern die Betreiber von Kritischen Infrastrukturen. Diese sind generell in § 2 Abs. 10 BSIG legaldefiniert und werden durch die zahlenmäßigen Festlegungen der BSI-KritisV ("Schwellenwerte") konkretisiert. Ausschlaggebend sind dabei die Kriterien der Qualität und der Quantität. Dies bedeutet, dass eine Einrichtung grundsätzlich dann als kritische Infrastruktur im Sinne des Gesetzes eingestuft wird, soweit eine sektorale Zugehörigkeit zu Energie, Informationstechnik, Telekommunikation, Transport, Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen besteht. Hinzukommen muss im Sinne einer "Fehlerfolgenerheblichkeit" als quantitatives Kriterium, dass die Infrastruktur eine hohe Bedeutung für das Funktionieren des Gemeinwesens hat, weil durch ihren Ausfall oder infolge ihrer Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Der Maßstab ebenjener Fehlerfolgenerheblichkeit wird vorrangig durch die zahlenmäßigen Festlegungen in der BSI-KritisV gespeist.

Das deutsche ITSiG ist ein sog. "Artikelgesetz" und enthält einen Regelungsauftrag an den Gesetzgeber, verschiedene Einzelgesetze zu novellieren. Hierzu gehören u.a. das Atomgesetz, das BSI-Gesetz, das Energiewirtschaftsgesetz, das Telekommunikationsgesetz und das Telemediengesetz. In all diesen Vorschiften finden sich spezielle Anforderungen an die Informationssicherheit, die durch die jeweiligen Betreiber vorzusehen sind. Dabei gehen die Gesetze selbst, was die konkreten inhaltlichen Pflichten anbelangt, im Regelfall nicht weiter auf die technisch-organisatorischen Details ein, sondern es werden zumeist nur allgemeine, an die Informationssicherheit anzulegende Ziele definiert, oder es wird auf "angemessene" Maßnahmen verwiesen, die dem "Stand der Technik" entsprechen. Hierbei handelt es sich um einen sog. "unbestimmten Rechtsbegriff" bzw. eine "Generalklausel", die in den vergangenen Jahren durch die Anwendungspraxis konkretisiert wurde. Juristisch einzuordnen ist der "Stand der Technik" in die Begriffstrias aus "allgemein anerkannter Regel der Technik" und "Stand von Wissenschaft und Forschung", wobei der "Stand der Technik" den technisch-organisatorischen Mittelwert zwischen diesen beiden Extrema abbildet. Es kommt in der Umsetzung folglich darauf an, was zum jeweils gegenwärtigen Zeitpunkt technisch notwendig, geeignet, angemessen und an Fehlfunktionen und Risiken vermeidbar ist[6]. Neben den technisch-organisatorischen IT-Sicherheitspflichten gem. "Stand der Technik" tritt für Kritische Infrastrukturen noch eine Meldepflicht an das BSI hinzu.

Die Entwicklungen um ein spezifisch europäisches und deutsches Recht der Informationssicherheit werden durch die EU NIS-RL, den EU CSA sowie durch den Entwurf für ein ITSiG 2.0 ergänzt. Die NIS-RL enthält Verpflichtungen an sog. "wesentliche Dienste", die für Deutschland den Kritischen Infrastrukturen entsprechen. Als EU-Richtlinie entfaltet sie grundsätzlich keine unmittelbare Wirkung in den Mitgliedstaaten, sondern muss durch ein nationales Umsetzungsgesetz in das deutsche Recht eingebracht werden. Dies ist bereits im Jahr 2017 geschehen und hat dazu geführt, dass zusätzlich zu den Pflichten, wie sie für Kritische Infrastrukturen gelten, auch die Betreiber von sog. "digitalen Diensten" in den Pflichtenkreis zur Informationssicherheit einbezogen werden. Laut Anhang II der

[6] TeleTrusT-Handreichung "Stand der Technik": https://www.teletrust.de/publikationen/broschueren/stand-der-technik/

NIS-RL fallen hierunter Online-Marktplätze, Cloud Computing Services und Online-Suchmaschinen. Gemäß der Definition in § 2 Abs. 11 Nr. 3 BSIG sind Cloud-Computing-Dienste solche, die den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglichen. Besondere Technisch-organisatorische Anforderungen an die Anbieter von digitalen Diensten finden sich im nationalen Recht in § 8c BSIG. Die dort genannten Anforderungen gelten jedoch nicht für Kleinstunternehmen und kleine Unternehmen im Sinne der Empfehlung 2003/361/EG. Ausgenommen von den KRITIS-Regelungen sind folglich solche Cloud-Diensteanbieter, deren Unternehmen weniger als 50 Personen beschäftigen und deren Jahresumsatz/Jahresbilanz 10 Mio. EUR nicht übersteigt. Die Regelungen gelten außerdem nicht für Unternehmen, die öffentliche Kommunikationsnetze oder öffentlich zugängliche Kommunikationsdienste bereitstellen sowie für Vertrauensdiensteanbieter. Gerade für das Cloud Computing stellt sich oft die Frage des Auslandsbezugs der Anbieter und damit die Frage nach der territorialen Anwendbarkeit von nationalen und europäischen Rechtsvorschriften. Auf die komplexe juristische Sachlage kann an dieser Stelle nicht im Detail eingegangen werden, vielmehr wird auf entsprechende Fachliteratur[7] verwiesen. Inhaltlich treffen die erfassten Anbieter von digitalen Diensten IT-Sicherheits- und Meldepflichten - insoweit besteht eine gewisse Vergleichbarkeit mit den Kritischen Infrastrukturen. Die entsprechenden Maßnahmen sind unter Berücksichtigung des Stands der Technik zu treffen und müssen ein Sicherheitsniveau gewährleisten, das dem bestehenden Risiko angemessen ist. Dabei ist den folgenden Aspekten Rechnung zu tragen: der Sicherheit der Systeme und Anlagen; der Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen; dem Betriebskontinuitätsmanagement, der Überwachung, Überprüfung und Erprobung sowie der Einhaltung von internationalen Normen. Eine entsprechende Durchführungsverordnung der EU-Kommission regelt in diesem Zusammenhang weitere Details.[8] Wie aus dieser Entwicklung bereits ersichtlich wird, tritt der Gesetzgeber mehr und mehr für IT-sicherheitsbezogene Regelungen ein, die über den Kreis der Kritischen Infrastrukturen hinausgehen - besonders deutlich wird diese Entwicklung durch den CSA sowie durch den Entwurf des ITSiG 2.0. Der CSA entwickelt ein umfassendes, sektoren- und branchenübergreifendes, zurzeit noch freiwilliges Zertifizierungssystem der IT-Sicherheit. Cloud Services werden in diesem Zusammenhang ebenfalls adressiert, die ENISA hat schon 2019 den Call einer entsprechenden Ad-hoc Working Group ausgeschrieben. Das ITSiG 2.0 bringt Regelungsvorschläge ein, die auch auf IoT, Cloud und den Consumer-Bereich abzielen, ohne hier aber im Sinne einer bestimmten Technologie konkret zu werden. Es ist davon auszugehen, dass diese rechtlichen Entwicklungen die allgemeine sowie die Cloud-spezifische Informationssicherheit in den kommenden Jahren erheblich prägen werden.

Soweit es die Verwendung von Cloud Computing im Consumer-Bereich (B2C) anbelangt, sind die rechtlichen Vorgaben aus der Digitale-Inhalte-Richtlinie (DID-RL) der Europäischen Union zu beachten, die zum gegenwärtigen Zeitpunkt in das nationale Recht umgesetzt wird. Die Rechtspflichten treffen hier in erster Linie nicht den Verbraucher, sondern das Unternehmen, das für den Verbraucher Cloud Services bereitstellt. In der weiteren Lieferkette und damit im B2B-Segment können die Regelungen aber auch mittelbar Rechtskraft entfalten, soweit es zu internen Regressansprüchen kommt. Das europäische Recht definiert in Art. 2 Nr. 2 DID-RL digitale Dienstleistungen als solche, die dem Verbraucher die Erstellung, Verarbeitung oder Speicherung von Daten in digitaler Form oder den Zugang zu solchen Daten ermöglichen, oder die gemeinsame Nutzung der vom Verbraucher oder von anderen Nutzern der entsprechenden Dienstleistung in digitaler Form hochgeladenen oder erstellten Daten oder sonstige Interaktionen mit diesen Daten ermöglichen. Umfasst davon sind Software-as-a-Service (SaaS) und anderen Formen des Datei-Hostings, die in einer Cloud-Computing-Umgebung angeboten werden. Zur Beurteilung der Mangelfreiheit solcher Dienste bestimmt die DID-RL objektive Anforderungen an die Vertragsmäßigkeit der gegenüber dem Verbraucher zu erbringenden Leistungen. Hierzu gehören u.a. auch die IT-Sicherheit und die Aufrechterhaltung der IT-Sicherheit in einer Weise, die üblich und zu erwarten ist.

In privatrechtlicher Hinsicht treffen den Betreiber einer Einrichtung, genauso wie den Geschäftsführer oder Vorstand eines jeden Unternehmens, verschiedene Verkehrssicherungspflichten, für die er im Außenverhältnis rechtlich verantwortlich ist. Dies kann insbesondere bei Schadensersatzansprüchen relevant sein, die infolge eines durch mangelnde Informationssicherheit verursachten materiellen oder immateriellen Schadens durch Dritte geltend gemacht werden. Mehr und mehr beziehen sich ebenjene Verkehrssicherungspflichten auch auf Fragen der Informationssicherheit, wovon denknotwendigerweise auch die in Unternehmen mittlerweile allgegenwärtige Cloud-Nutzung umfasst ist. Soweit es um die zivilrechtliche Haftung für IT-Sicherheitsvorfälle geht, ist zwischen vertraglichen Anforderungen und deliktsrechtlichen Anforderungen zu unterscheiden. IT- bzw. Informationssicherheit kann sich auf vertraglicher Ebene nicht nur als Hauptleistungspflichten durch Vereinbarungen zwischen den Vertragsparteien ergeben (beispielsweise in der Form eines Cloud-Vertrags, der als Dauerschuldverhältnis ausgestaltet ist), sondern auch mittelbar, ohne dass dies explizit vereinbart wurde, in der Form von Neben- oder Schutzpflichten in den vertraglichen Pflichtenkreis einfließen. Im deliktischen Bereich, d. h. ohne, dass eine vertragliche Vereinbarung besteht und somit

---

[7] Siehe dazu Beucher/Ehlen, in: Kipker, Cybersecurity, S. 397 f.

[8] Durchführungsverordnung (EU) 2018/151 der Kommission vom 30.01.2018 über Vorschriften für die Anwendung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates hinsichtlich der weiteren Festlegung der von Anbietern digitaler Dienste beim Risikomanagement in Bezug auf die Sicherheit von Netz- und Informationssystemen zu berücksichtigenden Elemente und Parameter für die Feststellung erheblicher Auswirkungen eines Sicherheitsvorfalls, Abl. 2018 L 26, 48.

grundsätzlich gegenüber jedermann, ergeben sich die Sorgfaltsmaßstäbe zur Informationssicherheit aus den eingangs bereits genannten Verkehrssicherungspflichten. Generell gilt hier, dass, wer eine Gefahrenquelle schafft, z.B. durch Entwicklung und Betrieb eines IT-Produkts oder IT-Services, für dieses gegenüber Dritten auch rechtlich verantwortlich ist.

Für das Bestehen einer vertraglichen Haftung ist es nicht nur erforderlich, dass ein Schuldverhältnis (Vertrag) zwischen den Parteien besteht und eine Pflichtverletzung vorliegt, sondern diese Pflichtverletzung der Vertragspartei auch individuell vorgeworfen werden kann. Man spricht insoweit auch von einem "Verschulden". Dieses liegt entweder bei Vorsatz (bewusstem Wissen und Wollen der schädigenden Handlung) oder Fahrlässigkeit als Regelfall vor. Fahrlässig handelt, wer die im Verkehr erforderliche Sorgfalt außer Acht lässt. Was im Verkehr jeweils erforderlich ist, ist einzelfallabhängig. Für die Informationssicherheit wird man sagen können, dass die Fahrlässigkeit von der Risikoklasse der Datenverarbeitung, ihrem Umfang, den verarbeiteten (personenbezogenen) Daten und der Einstufung ggf. als Kritische Infrastruktur abhängig ist. Regelmäßiger Anknüpfungspunkt bei einer deliktischen Haftung ist das Unterlassen der Erfüllung von Verkehrssicherungen zur Informationssicherheit. Da die Geltendmachung von Ansprüchen aus der vertraglichen Haftung und aus der deliktischen Haftung grundsätzlich. parallel nebeneinander möglich ist, ist der Maßstab der "im Verkehr erforderlichen Sorgfalt" strukturell grundsätzlich mit den deliktischen Verkehrssicherungspflichten vergleichbar.

Der Maßstab der Verkehrssicherungspflichten bestimmt sich einerseits nach den berechtigten Sicherheitserwartungen des Verkehrs, andererseits nach dem zumutbaren Aufwand für die Kontrolle möglicher Risiken. Auch hier gilt: Eine generelle juristische Bestimmung ist nicht möglich, sondern richtet sich stets nach den Erfordernissen des jeweiligen Einzelfalls.

Folgende Aspekte können zur Bestimmung für Hersteller und Anbieter von IT-Produkten und IT-Leistungen allgemein herangezogen werden:

- Kein Schutz individueller Sicherheitserwartungen oder besonderer Schadensanfälligkeiten
- Keine Sicherung von Produkten gegen Missbräuche, die jedermann bekannt sind
- Jedoch: Produzent und Diensteanbieter haftet für Schäden infolge nicht-bestimmungsgemäßen Gebrauchs, der sich noch im Rahmen der allgemeinen Zweckbestimmung bewegt und vom Hersteller vorhergesehen werden kann
- Basissicherheit ist immer zu gewährleisten

Je höherrangiger die bedrohten Rechtsgüter sind, umso höher sind die anzulegenden Sicherheitsmaßstäbe, beispielsweise für Kritische Infrastrukturen oder digitale Dienste, die wie zuvor dargestellt auch Cloud Computing umfassen können. Außerdem ist bei der Bestimmung und Konzeptionierung die technische Normung zu berücksichtigen, soweit entsprechende Standards oder Anwendungsregeln existieren. Diese spielen im Falle der juristischen Bewertung eines geltend gemachten Anspruches auf Schadensersatz ebenfalls eine Rolle, z. B. durch einen technischen Gutachter. Die Sicherheitserwartung kann sich überdies ändern, soweit neue Risiken bekannt werden. Insoweit umfasst das Management der Informationssicherheit im volatilen technischen Raum zugleich immer auch eine entsprechende Produkt- und Dienstbeobachtungspflicht. Das muss erst recht für Dauerschuldverhältnisse gelten, die zumeist die vertragliche Grundlage zur Nutzung von Cloud-Angeboten sind. Deutlich wird dies auch am unbestimmten Rechtsbegriff "Stand der Technik", der zu seiner Einhaltung die fortlaufende Beobachtung und Evaluierung der technisch-organisatorischen Maßnahmen zur Informationssicherheit im Sinne eines ISMS erfordert.

Die Datenschutz-Grundverordnung ist im Hinblick auf die Thematik Cloud Security relevant, wenn personenbezogene Daten im Sinne des Artikel 4 Ziff. 1 DSGVO verarbeitet werden. Ausgehend von der Definition in Artikel 4 Absatz 1 DSGVO sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Der Begriff der Verarbeitung umfasst gemäß der DSGVO jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Soweit folglich im Geschäftsbetrieb Cloud Service im Rahmen der Verarbeitung von personenbezogenen Daten genutzt werden, muss sichergestellt werden, dass die verwendeten Cloud-Lösungen hinreichend abgesichert sind. Ein personenbezogenes Datum, das nicht durch entsprechende (angemessene) TOM geschützt wird, stellt laut Definition der DSGVO einen Verstoß dar. Die Folge wäre eine Haftung der verantwortlichen Partei für nicht hinreichend geschützte personenbezogene Daten. Hierbei können Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden, je nachdem, welcher der Beträge höher ist. Für die Umsetzung der TOM bietet die

DSGVO im Artikel 32 einen entsprechenden Maßnahmenkatalog an. Zudem stellt der § 64 BDSG eine sinnvolle Ergänzung des Art. 32 DSGVO dar. Denkbar sind deshalb für die sichere Cloud-Nutzung im Sinne der DSGVO vor allem die folgenden Maßnahmen: Rechtemanagement, Verschlüsselung, Separationsmechanismen, Updates und Backups. Zudem ein weiterer wichtiger Aspekt der DSGVO ist das Thema der Auftragsverarbeitung. Wie bereits vor der DSGVO bleibt es grundsätzlich dabei, dass die Auftragsverarbeitung (neben der Einhaltung der Rechtmäßigkeit der Verarbeitung gem. Art. 6 DSGVO) die datenschutzrechtliche Grundlage für die Nutzung von Cloud Services ist. Auch die Kernkomponenten einer Auftragsverarbeitung bleiben: Weisungsgebundenheit gegenüber dem Auftraggeber, eine Vereinbarung mit Inhalten nach Maßgabe der datenschutzrechtlichen Regelungen über die Auftragsverarbeitung und Dokumentation der Vereinbarung.

2.4 Sicherheitsvorteile von Cloud Services

Abhängig von Zertifizierung oder Testierung des Anbieters und Management und Umsetzung der Maßnahmen samt einer Datenschutzbetrachtung ergeben sich eine Reihe von Sicherheitsvorteilen durch die Nutzung von Cloud-Diensten. Abhängig vom Provider erfolgt eine plattform-unabhängige Überwachung der Sicherheit des Cloud-Dienstes. Während eine Absicherung der Leistungen über SLA grundsätzlich möglich und manchmal sinnvoll ist, sollte diese im Rahmen einer Bewertung von Kosten/Nutzen sowie Risiko mit Augenmaß an den tatsächlichen Bedarf angepasst werden.

Verglichen mit Inhouse IT, bieten Cloud-Dienste im Allgemeinen durch Security-on-Demand-Provisionierung eine höhere Sicherheit vor Ausfall und einen besseren und flexibleren Schutz vor Bedrohungen. Abhängig vom verwendeten Dienst kann das Schutzniveau an veränderte Anforderungen und Risiken angepasst werden, zum Beispiel durch einen Software-defined Perimeter. Auch ist ein weiterer Schutz von Backends vor Zugriff ohne Authentisierung realisierbar.

Auf der Kundenseite ist eine Trennung der eigenen Mandanten relativ einfach möglich, entweder durch Nutzung verschiedener Dienste oder das oben bereits erwähnte Rollen- und Rechtemodell. Für Entwickler erlauben Cloud-Dienste eine Entwicklung von Systemen und Strukturen unabhängig von Legacy-Systemen. Das von Cloud-Diensten unterstützte agile Deployment erlaubt kürzere Turnaround Zeiten als in traditionellen Verfahren, insbesondere bei erkannten Lücken.

3 Technische Maßnahmen zur Sicherung der Nutzung von Cloud Services

3.1 Nutzung von in Cloud Services enthaltenen Sicherheitsmechanismen

Cloud-Anbieter stellen in aller Regel eine Reihe von Mechanismen und Konfigurationsmöglichkeiten zur Absicherung der erbrachten Cloud-Dienste zur Verfügung, oft als integralen Bestandteil der Dienste und ohne Aufpreis. Manche dieser Sicherheitsmechanismen sind als Default konfiguriert, andere müssen gesondert aktiviert werden. Übliche Sicherheitsmechanismen sind:

- Zugangskontrolle: Mindestens Benutzername und Passwort, zunehmend verbreitet auch Multi-Faktor-Authentisierung (z.B. per Authenticator, Mobile-TAN; siehe auch Abschnitt 3.2.1), Einschränkung des Zugangs auf bestimmte IP-Adressbereiche,
- Zugriffskontrolle, Rechtemanagement (wer darf was), oft über Rollenprofile, vier-Augen-Prinzip für bestimmte Zugriffe,
- Backup Mechanismen, Archivierung von Daten (siehe auch Abschnitt 3.4),
- Redundanzen: Konfiguration redundanter Systeme, ggf. mit Failover, bis hin zur Hochverfügbarkeit von Diensten,
- Verschlüsselung von Daten, ggf. mit kundeneigenen Schlüsseln ("Bring your own key")
- Audit-Trails: Aufzeichnung von Zugriffen und Änderungen für spätere Analyse und Nachweis (was wurde wann von wem getan).

Die hier dargestellten Sicherheitsmechanismen der Cloud-Anbieter stellen nur Beispiele dar. Aufgrund des dynamischen Cloud-Umfelds kann diese Aufzählung nicht abschließend sein, sie soll lediglich einen Eindruck über die Angebote der Cloud-Anbieter ermöglichen.

Unternehmen sollten sich auf Basis der individuellen Anforderungen sowie der beim Cloud-Anbieter verfügbaren Leistungspakete einen umfassenden Überblick verschaffen.

3.2 Identity und Access Management

Die zu Beginn des Jahres 2021 überwiegend eingesetzte Authentisierungsmethode für Nutzer gegenüber ihren Geräten, Netzwerkdomänen und Anwendungen ist die Eingabe von Benutzername und Passwort. Seit vielen Jahren häufen sich die Meldungen über im Darknet angebotene, gestohlene Nutzername/Passwort-Listen vieler großer und kleiner Online-Plattformen, Unternehmen und sogar Behörden, mit denen Kriminelle unbefugt und ohne weitere technische Sicherheitsmaßnahmen auch weithin unbemerkt in Firmennetze eindringen und Betreibern und Benutzern Schaden zufügen. Selbst von Diensteanbietern kryptographisch gesichert gespeicherte Passwörter können mit Hilfe sogenannter Rainbow-Tables in Klartext umgesetzt und genutzt werden.

Ohne weitere Sicherheitsmaßnahmen ist der Einsatz von Benutzername und Passwort damit nicht mehr Stand der Technik. Traditionelle Vorgaben zur Wahl komplexer Passwörter und häufiger Passwortwechsel haben Anwender einerseits oft überfordert und zu Vermeidungsstrategien und dezentralen Hilfs-Tools geführt, die zu neuen Angriffszielen wurden (Klebezettel am Monitor, Passwortmanager). Andererseits sind sie inzwischen überholt: Passwortlänge ist hoher Komplexität inzwischen mindestens ebenbürtig[9]. Überkommene Fachanwendungen erlauben jedoch selten mehr als 12 Zeichen lange Passwörter, so dass Komplexität und damit Kompliziertheit erzwungen wird. Wenn software-migrationstechnisch keine zügige Abkehr vom Passwort als alleiniger Authentisierungsmethode möglich ist, sollen Single-Sign-On (SSO) und regelmäßige Passwort-Qualitätsaudits genutzt werden.

Besteht dringender Verdacht auf passwort-basierte Angriffe, oder hohes Risiko dafür (etwa in halb-öffentlichen, hoch frequentierten Bereichen), sollen Zwei- oder Mehr-Faktor-Authentisierung eingesetzt werden (2FA, MFA, siehe

[9] Passwort-Empfehlungen des BSI für Bürger, abgerufen am 14.12.2020: https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html

Abschnitt 3.2.1). Zusätzlich zum Wissen des Nutzers (Benutzername, Passwort) werden hierbei weitere relevante Faktoren abgefragt, wie der Besitz personengebundener physischer Objekte (Mitarbeiterausweis, Gerätenummer, USB-Stick), die Nutzung zusätzlicher Kommunikationskanäle (QR-Code über Smartphone-Scanner und Mobilfunkverbindung), biometrischer Merkmale (Sprache, Augenhintergrund, Gangprofil) und Kontextfaktoren (zulässige Geographie, Uhrzeit). Für bestimmte Nutzergruppen und Anwendungsfälle sind auch passwortlose 2FA/MFA Kombinationen denkbar und sinnvoll, um die Sicherheit, Usability und Geschwindigkeit der Authentisierungsprozesse nicht durch schwache oder oft vergessene Passwörter bei nicht IT-affinen und häufig wechselnden Nutzern zu gefährden.

Die genannten Authentisierungsmethoden sind in den folgenden Abschnitten der Handreichung beschrieben.

3.2.1 Multi-Faktor-Authentisierung (MFA)

"Als Multi-Faktor-Authentifizierung (MFA) bezeichnet man den Nachweis der Identität eines Nutzers mit mehr als einem Faktor (z.B. Passwort + One-Time-Password (OTP) oder Passwort + Fingerabdruck + Sicherheitstoken)."[10]

"Neben dem klassischen Passwort sind diverse Methoden und Lösungen der Authentifizierung (MFA-Systeme) verfügbar. Die Methoden lassen sich in drei wesentliche Kategorien einteilen:

- Wissensbasierte Faktoren (z.B. Passwort, PIN, Passphrase, etc.)
- Besitzbasierte Faktoren (z.B. Sicherheitstoken, Smartcard, etc.)
- Biometrische Faktoren (z.B. Fingerabdruck, Iris, etc.)

MFA-Systeme kombinieren in der Regel jeweils zwei Methoden aus unterschiedlichen Kategorien zu einer Authentifizierungskette, wobei einige MFA-Systeme auch die Verkettung von beliebig vielen Methoden zulassen. Die Kombination von Methoden aus nur einer Kategorie ist nicht ratsam. Es ist zu beachten, dass nicht zwangsläufig alle Methoden aus diesen drei Kategorien, auch in ihrer Kombination gleichwertig sind. Jedoch stellt jegliche Kombination eine Verbesserung gegenüber dem Einsatz von Passwörtern allein dar. Welche Authentifizierungsmethoden kombiniert werden sollten, hängt vom Schutzbedarf der Anwendung bzw. Nutzeridentität sowie den technischen Voraussetzungen ab."[11] Für den Schutz von Cloud Services bieten sich treiber- und plattformunabhängige Methoden und Protokolle am ehesten an. Diese sind unter anderem:

OTP

Das One-Time-Password (OTP) oder auch Einmalkennwort wird für die einmalige Verwendung zur Authentifizierung genutzt und kann kein zweites Mal verwendet werden. Somit erfordert jede Anmeldung ein neues Einmalkennwort. Diese bewährte Methode basiert auf symmetrischen Schlüsselpaaren und ist schnell und einfach in eine Cloud-Anwendung zu implementieren. Weiterhin ist diese Methode für den User verständlich und einfach in der Handhabung. Die jeweils generierten Einmalpasswörter können sowohl serverseitig als auch auf der Userseite generiert werden. Serverseitig generierte OTP werden zumeist per E-Mail, per SMS oder Voice Call an den User übermittelt. Ein Benutzer kann OTP aber auch per Smartphone App (z.B. Google Authenticator, Microsoft Authenticator) oder auf einem Hardwaretoken generieren lassen und jeweils eingeben. OTP Verfahren gelten als sicher, jedoch aufgrund der symmetrischen Schlüsselpaare und der jeweiligen 1:1 Beziehung als etwas "in die Jahre gekommenes" Verfahren.

FIDO

Die FIDO-Protokolle sind von der FIDO (Fast Identity Online) Allianz entwickelte, offene und lizenzfreie Authentifizierungsprotokolle für die sichere Authentifizierung im World Wide Web. Eine Vielzahl an Sicherheitstoken und Authentisierungslösungen und Anwendungen nutzen bzw. unterstützen bereits FIDO Protokolle. Diese bieten durch die Verwendung von asymmetrischen Schlüsselpaaren besonders hohe Sicherheit. Ein einzelner Token/ Authenticator kann 1-n Anwendung absichern. Die FIDO-Protokolle sind W3C Standard und erfreuen sich daher hoher Prominenz und steigender Verbreitung.

[10] TeleTrusT-Handreichung "Stand der Technik", 2020, Kapitel Multifaktor-Authentifizierung, Seite 22
[11] TeleTrusT-Handreichung "Stand der Technik", 2020, Kapitel Multifaktor-Authentifizierung, Seite 23

Smartphones (Out of Band)

"Das Smartphone kann zum Generieren von OTP per App und dem Empfangen von SMS sowie als Out of Band Authenticator verwendet werden. Hierbei wird dem Benutzer eine Aufforderung zur Bestätigung oder Ablehnung eines Logins an eine App versendet. Dieses Verfahren ist für den User recht komfortabel und erfreut sich hoher Akzeptanz."[12]

3.2.2 Identity-Provider

Verfahren zur starken Authentisierung können im einfachsten Fall direkt in den Cloud Service integriert werden[13], was aus Sicherheitsgründen vorteilhaft sein kann. Auf der anderen Seite ist der Aufwand zur Integration unterschiedlicher Authentisierungsmechanismen oftmals proportional zur Anzahl der unterstützten Verfahren und der Cloud Service muss immer dann angepasst werden, wenn Änderungen an der eingesetzten Authentisierungstechnologie notwendig werden.

Abbildung 1: Direkte Integration der starken Authentisierung

Um den Prozess der starken Authentisierung von den fachlichen Abläufen in Cloud Services zu entkoppeln, empfiehlt sich der Einsatz eines spezialisierten Authentisierungsdienstes ("Identity Provider"), der über standardisierte Protokolle für das föderierte Identitätsmanagement angesprochen werden kann. Hierdurch können leicht unterschiedliche Mechanismen zur starken Authentisierung unterstützt und notwendige Fortentwicklungen in der Authentisierungstechnologie ohne Auswirkungen auf den Cloud Service vorgenommen werden.

In diesem Fall erfolgt nach dem Zugriff des Benutzers auf den Cloud Service (1) eine Umleitung des Benutzers zum Identity Provider (2), der die starke Authentifizierung des Benutzers im Auftrag des Cloud Service mit einem sicherheitstechnisch geeigneten Verfahren durchführt (3) und das Ergebnis der Authentifizierung in einer gesicherten Weise zum Cloud Service zurückschickt (4), bevor der Benutzer im Erfolgsfall Zugriff erhält (5).

[12] TeleTrusT-Handreichung "Stand der Technik", 2020, Kapitel Multifaktor-Authentifizierung, Seite 23

[13] D. Hühnlein, C. Ziske, T. Hühnlein, T. Wich, D. Nemmert, S. Rohr, M. Hertlein, C. Kölbel: *Starke Authentisierung – jetzt!*, Tagungsband DACH Security, 2017, https://www.2fa.jetzt/pub/DACH2017.pdf

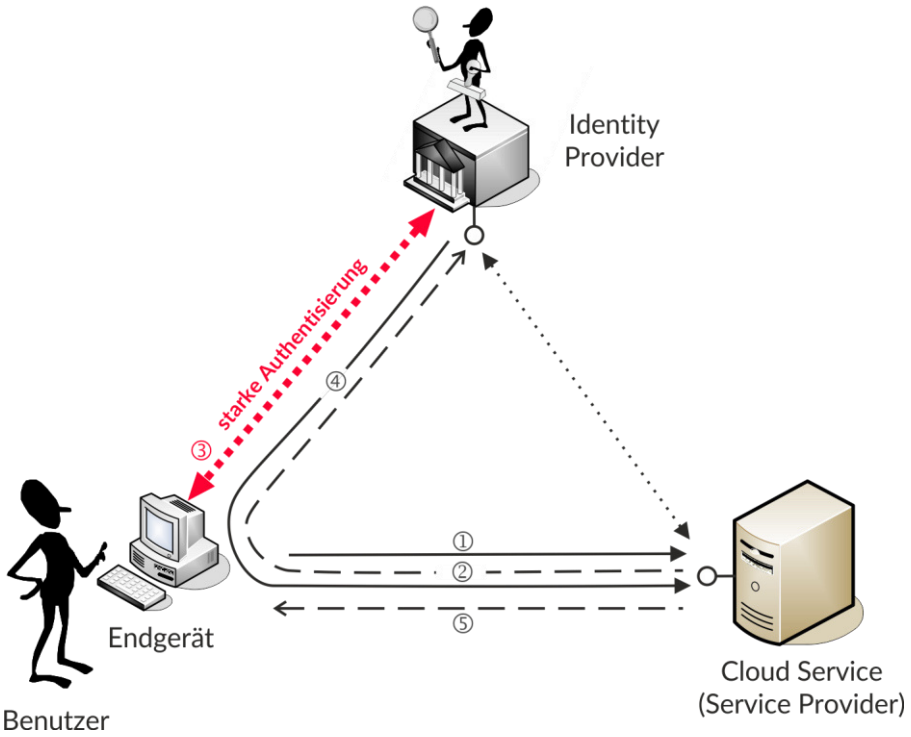

Abbildung 2: Integration über Identity Provider

Damit die ausgelagerte Authentifizierung nicht missbraucht werden kann, müssen geeignete Sicherheitsmaßnahmen implementiert werden, die regelmäßig im Rahmen von geeigneten Zertifizierungsverfahren (z.B. gemäß ISO/IEC 27001 oder ISO 27001 auf Basis von IT-Grundschutz) geprüft und zertifiziert werden. Soweit im Rahmen der starken Authentifizierung auch personenbezogene Daten verarbeitet werden, sind die Anforderungen des Bundesdatenschutzgesetzes zu berücksichtigen, deren Erfüllung beispielsweise im Rahmen einer Zertifizierung gemäß des "Trusted Cloud Datenschutz-Profils" (TCDP) für Cloud-Dienste bzw. zukünftig mittels "GDPR Cloud Certificate" (GDPR CC) nachgewiesen werden kann.

3.2.3 Single-Sign-On

Durch den Einsatz von Identity Providern, die nach einer einmal durchgeführten Authentifizierung eine längerlebige Session etablieren, die die Anmeldung an weiteren Cloud-Diensten ermöglicht, kann ein so genanntes "Single Sign-On" realisiert werden.

Das heute vermutlich am weitesten verbreitete Protokoll für das föderierte Identitätsmanagement und die Auslagerung der starken Authentisierung an einen spezialisierten Authentisierungsdienst ist das im Jahr 2005 vom Security Services Technical Committee der internationalen Standardisierungsorganisation OASIS standardisierte SAML (Security Assertion Markup Language) Protokoll[14], bei dem XML-basierte Nachrichten ausgetauscht werden.

Hierbei wird in Schritt (2) im Zuge der Umleitung an den Identity Provider ein so genannter `<AuthnRequest>` an diesen geschickt und in Schritt (4) das Ergebnis der Authentifizierung in einer `<Response>`-Nachricht an den Cloud Service (Service Provider) zurückgeschickt.

[14] S. Cantor, J. Kemp, R. Philpott & E. Maler: *Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0.*, 2005, https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

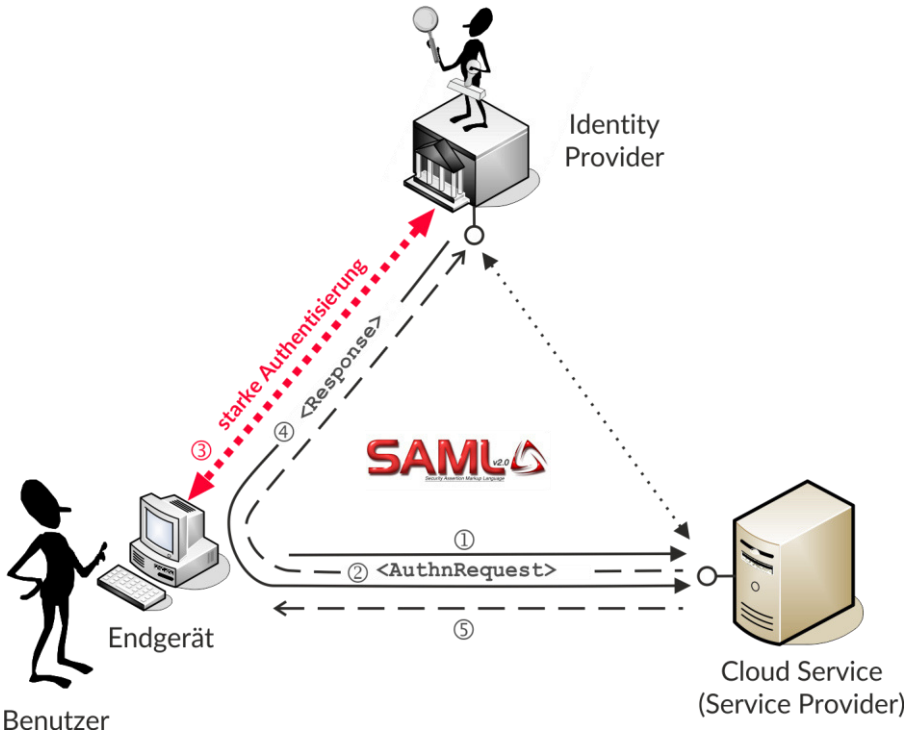

Abbildung 3: SAML-basierte Integration

Ein weiteres Protokoll für die Auslagerung der starken Authentisierung ist das auf dem OAuth 2.0 Authorization Framework basierende OpenID Connect Protokoll[15]:

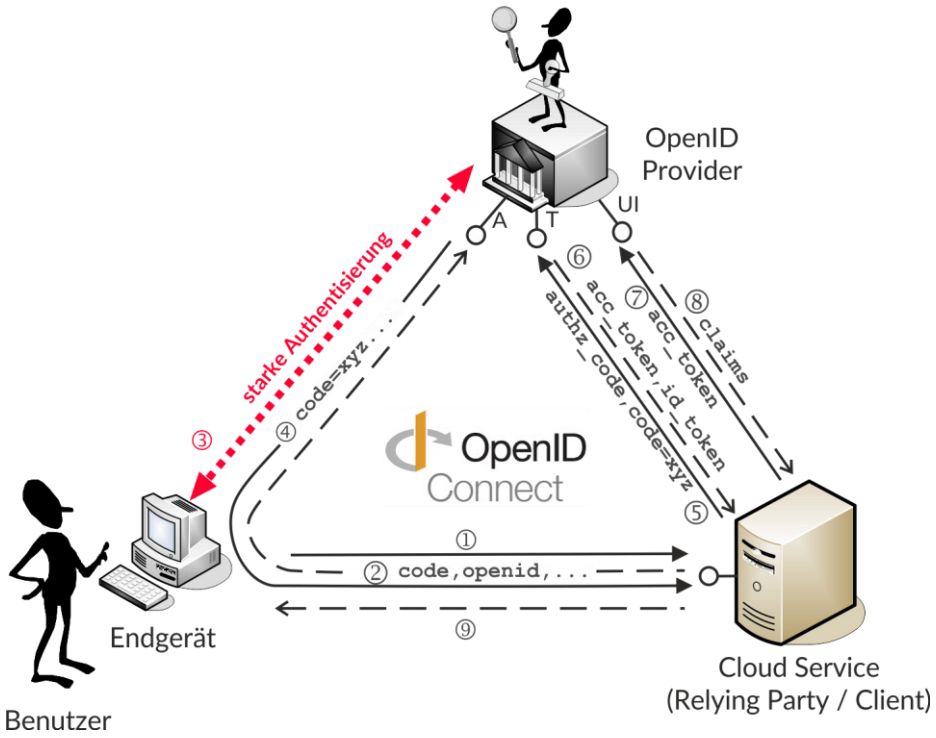

Abbildung 4: OpenID Connect-basierte Integration

Anders als bei SAML bietet der Identity Provider, der bei OpenID Connect auch "OpenID Provider" genannt wird, zusätzlich zum Authentisierungsendpunkt weitere Endpunkte (Authorization Endpoint (A), Token Endpoint (T) und UserInfo Endpoint (UI)) an, von den zumindest die ersten beiden im Zuge eines Authentisierungsvorganges vom

[15] N. Sakimura, J. Bradley, M. Jones, B. de Medeiros, C. Mortimore: *OpenID Connect Core 1.0*, November 8, 2014, http://openid.net/specs/openid-connect-core-1_0.html

Cloud Service angefragt werden müssen, um das Ergebnis der Authentifizierung und möglicherweise weitere Identitätsinformationen (Claims) zu erhalten.

3.2.4 Integrierte Verschlüsselung

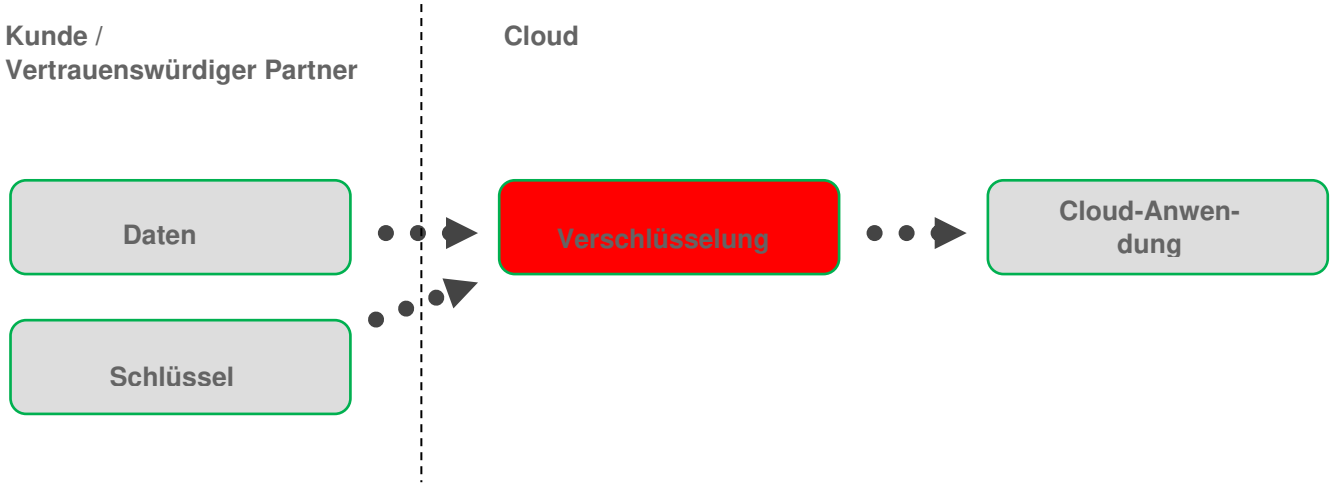

Abbildung 5: Integrierte Verschlüsselung

In der Bewertung des Sicherheitsniveaus von in Cloud Services integrierten Verschlüsselungslösungen ist es maßgeblich, zwischen der "Kontrolle über den Schlüssel" und der "Kontrolle über den Verschlüsselungsprozess" zu unterscheiden. Im Folgenden werden die gängigsten nativen Verschlüsselungslösungen der Cloud-Anbieter dargestellt und deren Funktionsweise beleuchtet:

Service Managed Keys

Bei dienstseitig verwalteten Schlüsseln stellt der Cloud Provider nicht nur die Verschlüsselungsmechanismen zu Verfügung, sondern er erstellt und verwaltet auch die benötigten Schlüssel. Da alle Teile des Verschlüsselungsvorgangs vom Dienstanbieter kontrolliert werden, verursacht diese Variante die wenigsten Einschränkungen bei der Funktionalität. Ein Sicherheitsgewinn ergibt sich hier gegenüber Angriffen von Dritten, aber nicht gegenüber dem Dienstanbieter selbst, der durch den direkten Zugriff auf die Schlüssel auch jederzeit auf die Daten zugreifen kann.

BYOK (Bring your own Key)

BYOK ermöglicht es dem Kunden, die kryptografischen Schlüssel selbst zu erzeugen und zu verwalten. Nur der Kunde hat Zugriff auf die Schlüsselverwaltung. Bei diesem Verfahren werden die zu verschlüsselnden Daten in lesbarer Form in die Cloud übertragen, um dort verschlüsselt und abgelegt zu werden. Somit liegt zwar die Kontrolle über den Schlüssel beim Kunden, der Verschlüsselungsprozess geschieht jedoch außerhalb seines Einflusses.

HYOK (Hold your Own Key)

Wie bei BYOK werden die kryptografischen Schlüssel bei HYOK durch den Kunden erzeugt und verwaltet. Im Unterschied zu BYOK werden die Schlüssel allerdings nur isoliert von der Cloud verwendet. Dies bedeutet, dass die Daten bereits verschlüsselt in die Cloud übertragen werden. Durch dieses Verfahren werden jedoch Einschränkungen bei der Funktionalität der Cloud-Anwendungen verursacht. So sind z. B. Auswertungen der verschlüsselten Daten serviceseitig nicht möglich und Such- und Sortierfunktionalitäten eingeschränkt (Undurchsichtigkeit der Daten - Data Opacity).

Durch die alleinige Kontrolle sowohl des Schlüssels als auch des Verschlüsselungsprozesses durch den Kunden, ist das Sicherheitsniveau von HYOK im Vergleich zu BYOK höher zu bewerten. Da die Undurchsichtigkeit der Daten jedoch Nachteile bei der Verarbeitung mit sich bringt, empfiehlt sich HYOK oftmals nur für sehr sensible Daten.

Double Key Encryption

Hierbei handelt es sich um ein Verschlüsselungsmodell von Microsoft, das stark HYOK ähnelt. Da der Begriff Double Key Encryption häufig in Zusammenhang mit Cloud-Sicherheit genannt wird, soll er hier kurz erläutert werden. Es werden zwei Schlüssel eingesetzt - einer unter der Kontrolle des Kunden, einer unter Kontrolle des Cloud Providers. Die Einschränkungen (Data Opacity) entsprechen denen bei HYOK.

Im Vergleich zu HYOK ist das Sicherheitsniveau - durch den durch den Cloud Provider kontrollierten Schlüssel - jedoch niedriger zu bewerten.

HSM (Hardware Security Module)

Ein Hardware Security Module (HSM) ist eine Hardware-Komponente, die die kryptografischen Verfahren absichert und ist damit kein Verschlüsselungsmodell wie die anderen hier aufgeführten Verfahren. Ein HSM kann jedoch unterstützend für diese Verschlüsselungsmodelle eingesetzt werden, indem es Schlüssel erzeugen und verwalten oder, im Falle von HYOK, den kompletten Verschlüsselungsvorgang übernehmen kann. Beim Zusammenwirken des HSM mit Cloud-Anwendungen wird das HSM meist vom Cloud-Anbieter gestellt oder verwaltet. Der Kunde kann aber dessen Funktionalitäten verwenden.

Entsprechend der Zugriffsmöglichkeiten durch den Cloud-Anbieter, ist das Sicherheitsniveau des HSM individuell zu beurteilen.

3.3 Cloud Security Layer

3.3.1 Cloud Access Security Broker (CASB)

CASBs sind -ein unverzichtbarer Bestandteil jeder IT-Sicherheitsstrategie, da sie automatisiert und in Echtzeit Informationen liefern und aktiv die Cloud-Nutzung auf das aus Sicherheitssicht gewünschte Maß limitieren. Mit ihnen lassen sich idealerweise auch die Themen Governance und Compliance (z.B. mit der DSGVO) managen und dokumentieren.

CASBs erfassen, überwachen und kontrollieren den Zugriff aller Mitarbeiter der eigenen Organisation auf sämtliche von ihnen genutzten Cloud-Dienste, unabhängig davon, mit welchen Geräten der Zugriff erfolgt und ob diese im eigenen Netz angemeldet sind, über VPN an das Firmennetz angebunden sind, oder aus dem Internet heraus direkt auf den Cloud-Dienst zugreifen. Damit liefern CASBs eine Übersicht über alle tatsächlich von einer Organisation genutzten Cloud-Dienste. Anhand dieser Übersicht können IT-Sicherheitsverantwortliche und -zuständige eine Risikoanalyse durchführen sowie erforderlichenfalls die Cloud-Nutzungsregeln neu definieren und deren Einhaltung überprüfen. Über Nutzungsregeln (Policies) kontrollieren CASBs alle Cloud-Zugriffe auf gültige Nutzerberechtigungen und den jeweils erlaubten Kontext, wie etwa das benutzte Gerät, dessen Status (gemanagt, ungemanagt, gepatcht oder nicht, oder gar gerootet), des geographischen Standorts, der Uhrzeit und weiteren Kontextfaktoren. Cloud-Zugriffe können je nach Kontext auch auf bestimmte Applikationen begrenzt werden.

Je nach Produkt und Hersteller schließen CASB-Produkte auch Funktionalitäten wie Data Loss Prevention und automatische Datenklassifizierung, Auswertungen zu Art und Umfang des anfallendes Cloud Traffics zu/von Cloud-Diensten sowie die Analyse des Nutzer- und Geräteverhaltens mit ein, die bessere Erkenntnisse und höhere Sicherheit bieten. Einige CASBs können auch maliziöse Aktivitäten Dritter auf in der Cloud vorgehaltene Applikationen und Datenbestände der eigenen Organisation entdecken und melden.

CASB-Lösungen werden zunehmend von Cloud-Nutzungs-Sicherheitstools unterstützt (CSPM - Cloud Security Posture Management), die einen Überblick über die derzeit bestehende Cloud-Sicherheitskonfiguration der Organisation über alle einbezogenen Cloud-Dienste-Anbieter liefern und auf eventuellen Anpassungsbedarf hinweisen.

Langfristig werden CASBs in ein umfassendes Sicherheitskonzept einfließen, das heute noch getrennte Funktionen wie sichere Web-Gateways, sowie neuere Architekturen wie Zero Trust Network Access, die kontextbasierte Authentisierung aller menschlichen und maschinellen Nutzer mit Applikationen und M2M-Services über die gesamte Organisation sicherstellt und mit software-definierten WAN-Funktionalitäten ausgestattet sein kann. Dieses Konzept wird auch als Secure Access Service Edge bezeichnet (SASE), da es sowohl zentrale Orchestrierungs-, als auch dezentrale, am Rand (Edge) der Cloud platzierte Komponenten umfasst.

3.3.2 Cloud Encryption Gateway

Zur Erstellung dieses Abschnitts erfolgte eine Orientierung an Kapitel 3.2.12 der Handreichung zum Stand der Technik in der IT-Sicherheit (Datenablage in der Cloud)[16]. Für weitergehende Informationen verweisen wir entsprechend hierauf.

[16] TeleTrusT-Handreichung "Stand der Technik": https://www.teletrust.de/publikationen/broschueren/stand-der-technik/

Eine grundlege Maßnahme zur Sicherung von Daten in hybriden Multi-Cloud-Umgebungen ist die Verschlüsselung sensibler Daten durch ein sogenanntes Cloud Encryption Gateway bevor diese die sichere/interne Umgebung verlassen. Dies wird gemeinhin als "Kontrolle der Verschlüsselung" bezeichnet. Zur Verschlüsselung notwendige Schlüssel sollten allein dem Data Controller (dem Unternehmen) bekannt sein. Die Kontrolle der Schlüssel verhindert, dass unbefugte Dritte (intern oder extern) Zugriff auf die Daten erhalten. Ohne den kryptografischen Schlüssel können unberechtigte Personen mit den erbeuteten, verschlüsselten Daten nichts anfangen.

Bei der Auswahl eines geeigneten Verschlüsselungsgateways sollte der Erhalt wichtiger Funktionalitäten wie Suchen, Filtern, Reporting etc. ein zentrales Kriterium darstellen. Die wichtigen Funktionalitäten sollten durch den Einsatz der Gateways nicht eingeschränkt werden, um die Effizienz gewohnter Arbeitsabläufe zu erhalten. Um die Zukunftsfähigkeit der gewählten Lösung sicher zu stellen, sollte diese PQC Ready sein, um die Datensicherheit auch bei zukünftigem Einsatz von Quantencomputern zu gewähren.

E-Mail Security Gateway

E-Mail ist seit Jahren Angriffsvektor Nr. 1. Die Gründe hierfür sind vielfältig:

- E-Mail-Adressen lassen sich beispielsweise durch Adressbuchattacken oder Website crawling leicht auffinden
- Der Angreifer muss sich nicht authentifizieren und bleibt anonym
- Der E-Mail-Versand verursacht nahezu keine Kosten
- E-Mails sind üblicherweise nicht zusätzlich durch Zugriffskontrollen des Unternehmensnetzwerks geschützt - sie sind weltweit abrufbar

E-Mail ist der Standardkommunikationsweg für Unternehmenskommunikation, auch mit sensiblen Inhalten. Mitarbeiter können direkt kontaktiert und somit attackiert werden.

Der Trend, E-Mail-Postfächer in die Cloud zu verschieben, ist nach wie vor ungebrochen. Die Verwendung von Cloud-Produkten wie Exchange Online oder Googles G-Suite entbindet trotz integrierter Sicherheitslösungen nicht grundsätzlich von der Verwendung einer 3rd Party-Lösung für E-Mail Security.

Für zusätzlichen Schutz, unabhängig vom Sicherheitsniveau des jeweiligen Cloud-Postfachanbieters, empfiehlt sich der Einsatz eines externen Anbieters, der sich auf die Absicherung des E-Mail-Wegs spezialisiert hat.

Damit ein solcher Dienst genutzt werden kann, werden in der Regel ein- und ausgehende E-Mails über Server des E-Mail-Security-Anbieters geleitet. Zusätzlich sollten Standardeinstellungen im Hinblick auf verwendete Filter etc. geprüft werden, ob sie den eigenen Anforderungen genügen.

Darüber hinaus werden üblicherweise Benutzerdaten synchronisiert. Im Normalfall reichen die E-Mail-Adressen, Vor- und Nachnamen der Benutzer vollkommen aus. Wenn neben dem eigentlichen Schutz vor Spam und Malware noch weitere Dienste wie z.B. ein Disclaimer zum Einsatz kommen, ergibt es Sinn, auch Adressdaten zu synchronisieren, damit sie automatisch in die E-Mail eingefügt werden können.

3.3.2.1 E-Mail-Verschlüsselung

Ein nach wie vor häufig vernachlässigter Bestandteil der E-Mail-Security-Strategie von Unternehmen ist die E-Mail-Verschlüsselung. E-Mail-Verschlüsselung kann auf zwei unterschiedliche Art und Weisen umgesetzt werden. Die sogenannte Ende-zu-Ende-Verschlüsselung (E2E) beschreibt die Umsetzung der Verschlüsselung auf dem Client des Benutzers. Für die Ver- und Entschlüsselung müssen dabei dem E-Mail-Client alle benötigten Zertifikate zur Verfügung stehen. Beim Einsatz von mobilen Geräten stellt dies mitunter eine nur schwer lösbare Aufgabe dar. Der Vorteil bei E2E ist die etwas höhere Informationssicherheit, da die E-Mail in verschlüsselter Form im Postfach des Benutzers liegt. Dies ist zugleich auch der größte Nachteil, da der Aufwand beispielsweise bei der Stellvertretereinrichtung enorm ansteigt. Der Stellvertreter muss ebenfalls im Besitz des richtigen Schlüsselmaterials sein. Der mobile Zugriff auf das Postfach, Archivierung und automatische Weiterleitungen sind entweder herausfordernd oder gar unmöglich.

Zentrale Verschlüsselungs-Gateways automatisieren die Verwaltung des Schlüsselmaterials und übernehmen darüber hinaus vollständig transparent die Verschlüsselung, Entschlüsselung, Signatur und die Prüfung der Signatur. In der Praxis bedeutet das, dass der Endanwender überhaupt nicht mehr in den Prozess eingreifen muss - und auch der zuständige Administrator nachhaltig entlastet wird.

Nachteilig ist, dass die E-Mail unverschlüsselt im Postfach des Benutzers liegt. In diesem Fall gilt es, das Postfach mit möglichst engen Zugriffsberechtigungen und durchgängiger Transportverschlüsselung bestmöglich zu schützen. In den allermeisten E-Mail-Server-Infrastrukturen stellt dies heute jedoch keine Hürde mehr dar.

Ein weiterer, äußerst wichtiger Punkt ist die Betriebssicherheit. Bei E2E kann der Inhalt einer E-Mail erst am E-Mail-Client auf Spam- und Virengehalt geprüft werden. In der Regel stehen dort dann nicht mehr dieselben Filter und Werkzeuge zur Verfügung, wie am Gateway. Benutzer, die E2E nutzen, müssen demzufolge nicht nur hinsichtlich der Verschlüsselung gut geschult werden, sondern auch besonders wachsam im Umgang mit Anhängen und URLs in E-Mails sein.

Die Verfügbarkeit von zentralen Verschlüsselungs-Gateways als Cloud Service ist mittlerweile keine Seltenheit mehr. Der Cloud-Anbieter übernimmt in aller Regel nicht nur die Verschlüsselungs- und Signaturoperationen, sondern verwaltet auch die benötigten Zertifikate.

Für einen detaillierteren Blick in das Thema "E-Mail-Verschlüsselung" verweisen wir aus Gründen der Übersichtlichkeit auf den TeleTrusT-Leitfaden "E-Mail-Verschlüsselung"[17].

3.3.2.2 E-Mail-Authentication

Ein wichtiger Baustein der eigenen E-Mail-Sicherheitsstandards ist die sogenannte E-Mail-Authentication. Diese ermöglich es einem empfangenden E-Mail-Server zweifelsfrei festzustellen, ob der einliefernde Server die Nachricht im Namen der absendenden Domain ausliefern darf, oder nicht.

Verfahren zur Sender- und Empfängerreputation sind bereits seit Jahren bekannt und entsprechende Standards in den RFC definiert. Sie bieten ein erhebliches Plus an Sicherheit mit vergleichsweise geringem Aufwand und sind auch ohne teure Werkzeuge umzusetzen. Die Durchdringung in Unternehmen ist jedoch vergleichsweise gering. Durch die immer intelligenter werdenden Bedrohungen u.a. durch Ransomware, ist der Bedarf an Aufklärung hoch.

Möglich wird die Absenderprüfung durch die Verwendung von speziellen Methoden zur Absenderidentifizierung. Die einzelnen Methoden sind unter den Abkürzungen SPF (Sender Policy Framework), DKIM (Domain Keys Identified Mail) sowie DMARC (Domain-based Messaging, Authentication, Reporting and Conformance) und ARC (Authenticated Receive Chain) bekannt und bauen aufeinander auf.

Bei der Einführung der genannten Technologien gilt es zwei Aspekte zu berücksichtigen: Zum einen müssen die entsprechenden SPF, DKIM, DMARC Informationen für die eigenen Domains veröffentlicht und damit den externen Kommunikationspartnern zur Verfügung gestellt werden. Mit diesem Schritt werden zwei wichtige Ziele verfolgt. Zunächst wird dem Kommunikationspartner die Möglichkeit gegeben, zweifelsfrei festzustellen, dass die E-Mail tatsächlich vom korrekten Absender kommt. Nicht zu unterschätzen ist jedoch auch die massive Senkung des Reputationsrisikos für die eigenen Domains und damit des gesamten Unternehmens oder der Behörde. Immer häufiger verwenden Angreifer Plattformen, die über die genannten Methoden schon verfügen. Legitime E-Mails von Absendern ohne diese Merkmale sind somit automatisch im Hintertreffen.

Der zweite Aspekt kommt beim Empfang von E-Mails zum Tragen. Hier muss eine Software zum Einsatz kommen, die die gerade genannten Informationen abfragen und korrekt umsetzen kann. Bei der Auswahl des richtigen Cloud-Anbieters für E-Mail-Sicherheit sollte dieses Kriterium unbedingt berücksichtigt werden.

Sender Policy Framework (SPF)

Im Sender Policy Framework (SPF) gibt der Inhaber einer Domain im Domain Name System (DNS) an, welche Server autorisiert sind, E-Mails im Namen der eigenen Domain zu versenden. Dazu erstellt er in der entsprechenden DNS-Zone einen sogenannten SPF-Record. Technisch gesehen handelt es sich hierbei um einen TXT Record, dessen Syntax in der RFC7208 exakt spezifiziert ist.

Domain Keys Identified Mail (DKIM)

Bei Domain Keys Identified Mail (DKIM) wird ebenfalls ein TXT-Record in Form einer RFC normierten Syntax in der DNS-Zone der zu schützenden Domain erstellt. Zusätzlich kommt bei DKIM mit dem Public-Key-Verfahren eine kryptografische Komponente zum Tragen.

[17] TeleTrusT-Leitfaden "E-Mail-Verschlüsselung": https://www.teletrust.de/publikationen/broschueren/e-mail-verschluesselung/

Die DKIM-Signatur stellt zwei Dinge sicher: Zum einen weiß der empfangende Server, dass die E-Mail samt Inhalt auf dem Transportweg nicht verändert worden ist. Zum anderen weiß er, dass der Inhaber der im Header angegebenen Absender-Domain den Server autorisiert hat.
Im Unterschied zu kryptografischen Signaturen mittels S/MIME oder PGP sieht der Empfänger einer E-Mail die DKIM-Signatur nicht. Es ist ein rein serverbasiertes Verfahren. Erst wenn man sich den Header einer E-Mail anzeigen lässt, wird die DKIM-Signatur sichtbar.

Domain-based Message Authentication, Reporting and Conformance (DMARC)

Weder SPF noch DKIM geben dem empfangenden Server einer E-Mail klare Anweisungen, was mit E-Mails passieren soll, die die SPF und DKIM-Prüfung nicht erfolgreich bestanden haben. Diese Lücke schließt DMARC.

Ein empfangender E-Mail-Server weiß aufgrund des vorhandenen DMARC-Records für die Absender-Domain, dass sowohl eine SPF- als auch eine DKIM-Prüfung erforderlich ist. Wenn beide Prüfungen fehlschlagen, bekommt er über das sogenannte Policy-Flag mitgeteilt, wie in diesem Fall mit der E-Mail umgegangen werden soll. Im Idealfall wird die E-Mail abgewiesen.

Eine weitere Besonderheit von DMARC ist die Berichtsfunktion. Sie sorgt dafür, dass der Inhaber einer Domain regelmäßig darüber informiert wird, welche Server in seinem Namen E-Mails versendet haben und ob die Prüfung beim Empfänger erfolgreich war oder nicht. So bekommt er nicht nur einen guten Überblick über "seine" E-Mails im Internet, sondern auch wertvolle Informationen, ob seine SPF und DKIM Einträge vollständig und syntaktisch korrekt sind.

Authenticated Received Chain (ARC)

ARC ist die jüngste Technologie in dieser Reihe und befindet sich seit Juli 2019 im Status "Experimental". Der Verbreitungsgrad ist gerade bei den Cloud-basierten Diensten von Google, Microsoft etc. relativ hoch, da es als Authentifizierungssystem ein bekanntes Problem bei der Verwendung von SPF, DKIM und DMARC im Rahmen von Mailinglisten oder anderen Weiterleitungsdiensten löst. Genauer gesagt, ermöglicht ARC, die ursprünglichen Authentifizierungsergebnisse einer E-Mail zu signieren und damit zu konservieren. So kann ein empfangender Dienst eine E-Mail validieren, wenn die SPF- und DKIM-Einträge der E-Mail durch die Verarbeitung eines Zwischenservers ungültig werden.

3.3.2.3 Abwehr von Spam und Malware

Pattern basierte Verfahren

Über eine spezifische Byte-Abfolge - die Virensignatur - ist jedes Virus eindeutig identifizierbar. Man könnte sie auch als Fingerabdruck bezeichnen. Für das Erstellen eines solchen Fingerabdrucks ist es notwendig, mehrere Exemplare eines Virus zu untersuchen, da es im Laufe der Ausbreitung zu Veränderungen im Code geben kann. Für Anti-Viren-Programme sind Datenbanken, die die aktuellen Signaturen enthalten, die wichtigste Voraussetzung, um einen Schutz garantieren zu können. Die Sammlung aller bekannten Signaturen in einer Datei nennt man Patternfile. Sie werden je nach Hersteller unterschiedlich oft erneuert. Aktuelle Veröffentlichungen des BSI zeigen auf, dass es täglich mehrere Hunderttausend neue Informationen für Patternfiles gibt, so dass dieses Verfahren immer einen großen zeitlichen Nachteil hat, da zunächst das Virus erkannt werden muss, anschließend muss die Signatur dem Patternfile hinzugefügt werden und es muss an die einzelnen Installationen verteilt werden.

KI-basierte Verfahren

KI-basierte Verfahren versuchen Malware mit Hilfe verhaltensbasierter Erkennung zu finden. Der Entscheidungsfindung zugrunde liegen immer Algorithmen. Die Trefferquote hängt bei diesem Verfahren von der verwendeten Datenbasis und der Qualität sowie Passung der verwendeten Algorithmen ab.

Advanced Threat Protection (ATP)

ATP bezeichnet eine spezielle Kategorie von Security-Lösungen zur Abwehr von hochentwickelter Malware oder Hacking-basierter Angriffe. Da ATP immer ganzheitlich betrachtet werden muss, sind E-Mail Security Gateways nur ein Baustein des Konzepts. Als Perimeter-Schutz für E-Mails ist es jedoch ein sehr elementarer Baustein.

Zwei wichtige Elemente bei ATP sind der Realtime-Ansatz und der Kontext, grundsätzlich gilt aber, je mehr Daten für die Analyse zur Verfügung stehen, umso höher ist das Schutzniveau. Für die E-Mail-Sicherheit bedeutet das konkret, dass Anhänge und URLs in E-Mails besser und schneller bewertet werden können, wenn die Herkunft gut

geprüft und mit anderen, vergleichbaren Anhängen und URLs abgeglichen werden kann. Vor allem die Meta-Daten wie IP-Adresse des einliefernden Gateways und Teile des Headers spielen hier eine große Rolle bei der Bewertung einer E-Mail. Der reine Text in E-Mails kann in aller Regel vernachlässigt werden, da von ihm keine echte Bedrohung im Sinne einer ATP-Attacke ausgeht. Anhänge und URLs hingegen sind die geeigneten Werkzeuge für einen Angreifer, um Schadcode zu verstecken.

CEO Fraud Attacken

Bei einem CEO Fraud handelt es sich um eine Masche im Bereich der Cyberkriminalität, die mittlerweile immer häufiger zum Einsatz kommt. Es handelt sich um eine Form des Social Engineerings. Zu den besonders gefährdeten Personengruppen in einem Unternehmen zählen Mitarbeiter aus der Buchhaltung sowie jene, die im Auftrag der Geschäftsführung handeln dürfen. Gemeint sind Personengruppen, die z.B. durch eine Prokura dazu berechtigt sind, entsprechende Geldanweisungen vorzunehmen.

Diesen Umstand nutzen Angreifer für sich aus. Dabei erfolgt die Kontaktaufnahme gezielt per E-Mail oder direkt über ein Telefonat. Die Angreifer haben diese Sonderrechte sowie die damit zusammenhängenden Hierarchien der Mitarbeiter vorab genau recherchiert.

Neben einer Sensibilisierung der Mitarbeiter sind auch für das Thema CEO-Fraud technische Lösungen Stand der Technik und ihre Verwendung zu empfehlen. Insbesondere sollte auf die Einbindung von Verzeichnisdiensten geachtet werden, um unzulässige Kombinationen aus Realname und E-Mail-Adresse automatisiert zu ermitteln.

3.3.3 Cloud VPN

3.3.3.1 Definition "Cloud VPN"

Der Begriff VPN setzt sich aus drei Komponenten zusammen:

- Virtual (virtuell)
- Private (privat)
- Network (Netzwerk)

Ein VPN ist also zunächst ein Computernetzwerk über das damit verbundene Systeme miteinander kommunizieren. Es verhält sich wie ein Netzwerk und wird auch wie ein normales Netzwerk genutzt, d.h. angeschlossene Systeme senden ihre Daten an das Netzwerk und es ist die Aufgabe des Netzwerks dafür zu sorgen, dass die Daten an der Zieladresse ankommen.

Anders als herkömmliche Computernetze existiert ein VPN aber nur virtuell, nicht physisch. Das Netz wird also nicht mit Hilfe physischer Netzwerkkomponenten aufgebaut (Netzwerkkarten, Kabel, Switches, Router etc.), sondern durch Software auf bestehende Netze abgebildet. Die VPN Software schaltet dazu Verbindungen zwischen den beteiligten Systemen, die die Hardware des unterliegenden Netzes transparent passieren, d.h. die Komponenten des unterliegenden physischen Netzes sind für die am VPN angeschlossenen Systeme praktisch nicht existent. Die so geschalteten Verbindungen werden auch "Tunnel" genannt - man "untertunnelt" das physische Netz.

Durch die Tunnel wird das Netz privat, d.h. nicht für außenstehende Dritte nutzbar. Zum Schutz der im VPN fließenden Daten werden Verbindungen zudem in der Regel verschlüsselt. Der Inhalt der übermittelten Daten ist dadurch in den genutzten Netzkomponenten außerhalb der Endknoten der Verbindungen nicht einsehbar und kann auch nicht verändert werden, ohne dass das VPN dies bemerkt. Das ermöglicht den Aufbau eines geschützten privaten Netzes über öffentliche Netze wie das Internet hinweg.

Ein VPN kann damit auch ein bestehendes privates Netz über die physischen Grenzen des privaten Netzes hinaus erweitern und auch zwei oder mehrere private physische Netze sicher miteinander verbinden.

Bei einem Cloud VPN wird als Zugangspunkt ein Cloud Service genutzt, im Unterschied zu einem on-premise betriebenen Zugangspunkt bei einem herkömmlichen VPN. Cloud VPNs werden als Service von vielen Providern angeboten.

3.3.3.2 Einsatzzweck und Vorteile von VPNs

Allgemein werden VPNs für folgende Zwecke eingesetzt:

- Schutz der Datenübertragung bei Internet-Verbindungen über öffentliche Zugangspunkte (z.B. beim Internet-Zugang über Public WiFi)
- Schutz der Privatsphäre: Der Internet-Zugangsprovider kann nicht nachverfolgen, wohin Daten gesendet werden - er "sieht" nur die VPN-Verbindung, nicht die darüber übertragenen Daten
- Sicherer Zugang auf das Firmennetz und Ressourcen im Firmennetz (z.B. aus dem Home-Office) - die in VPNs meist eingerichtete Authentisierung gegenüber dem VPN dient als zusätzlicher Zugangsschutz für ansonsten von außen nicht zugängliche Systeme
- Sichere Verbindung zweier (oder mehrerer) Netze - z.B. Verbindung von Firmennetzen an verschiedenen Standorten
- Nahtloses Roaming ("Seamless Roaming") trotz wechselnden Netzzugangs z.B. bei mobilen Systemen (z.B. Übergang von WiFi zu LTE). Die IP-Adresse des mobilen Systems bleibt dabei gegenüber genutzten Ressourcen dieselbe, trotz Wechsel des Netzzugangs
- Nutzen eines anderen Zugangs in das Internet, mit den damit verbundenen Konsequenzen (andere IP-Adresse, dadurch andere Geo-Lokation, andere Regeln des Netzes, etc.). Dies wird u.a. genutzt, um Restriktionen eines Netzes zu umgehen. Das erlaubt den Zugriff auf Ressourcen, auf die sonst nicht zugegriffen werden kann - beispielsweise regional begrenzte Angebote. Manche Internet Zugangsprovider sperren z.B. den Port 25 (SMTP) - auch das kann per VPN umgangen werden

Gegenüber herkömmlich on-premise betriebenen VPNs haben Cloud VPNs folgende Vorteile:

- Zugangspunkte zu Cloud VPNs sind in der Regel breitbandig angebunden und aus dem Internet besser erreichbar als on-premise betriebene VPN Zugangspunkte
- Cloud VPN sind gegenüber on-premise VPN insbesondere dann sinnvoll, wenn sowohl Clients als auch Services außerhalb der Firmenräume betrieben werden, wie das z.B. beim mobilen Zugriff auf Cloud Services der Fall ist

3.3.3.3 Nachteile von VPNs

VPNs haben gegenüber herkömmlichen Netzen generell folgende Nachteile:

- VPN-Verbindungen setzen auf bestehenden Verbindungen auf und erzeugen dadurch zusätzliche Konfigurations- und Wartungsaufwand
- Auf den beteiligten Systemen wird CPU-Leistung zur Verschlüsselung und Entschlüsselung benötigt. Bei den meisten Clients ist das in der Regel kein Problem. Es kann aber auf Systemen mit geringer CPU-Leistung zu Schwierigkeiten führen
- Die Ver- und Entschlüsselung der Daten führt außerdem zur Reduzierung der Bandbreite, abhängig vom genutzten Protokoll (siehe Grafik)
- VPNs haben wegen des zusätzlichen Aufwands naturgemäß eine höhere Latenz (Dauer der Übertragung von Paketen) als die unterliegenden Netze

Bei Cloud VPNs ist außerdem zu beachten, dass der Cloud VPN Provider die übermittelten Datenpakete einsehen kann, weil er den Endpunkt der verschlüsselten Verbindung betreibt. Mit diesem Provider müssen dementsprechend vertragliche Vereinbarungen zum Schutz der Daten getroffen werden, ähnlich wie mit einem Internet-Zugangsprovider.

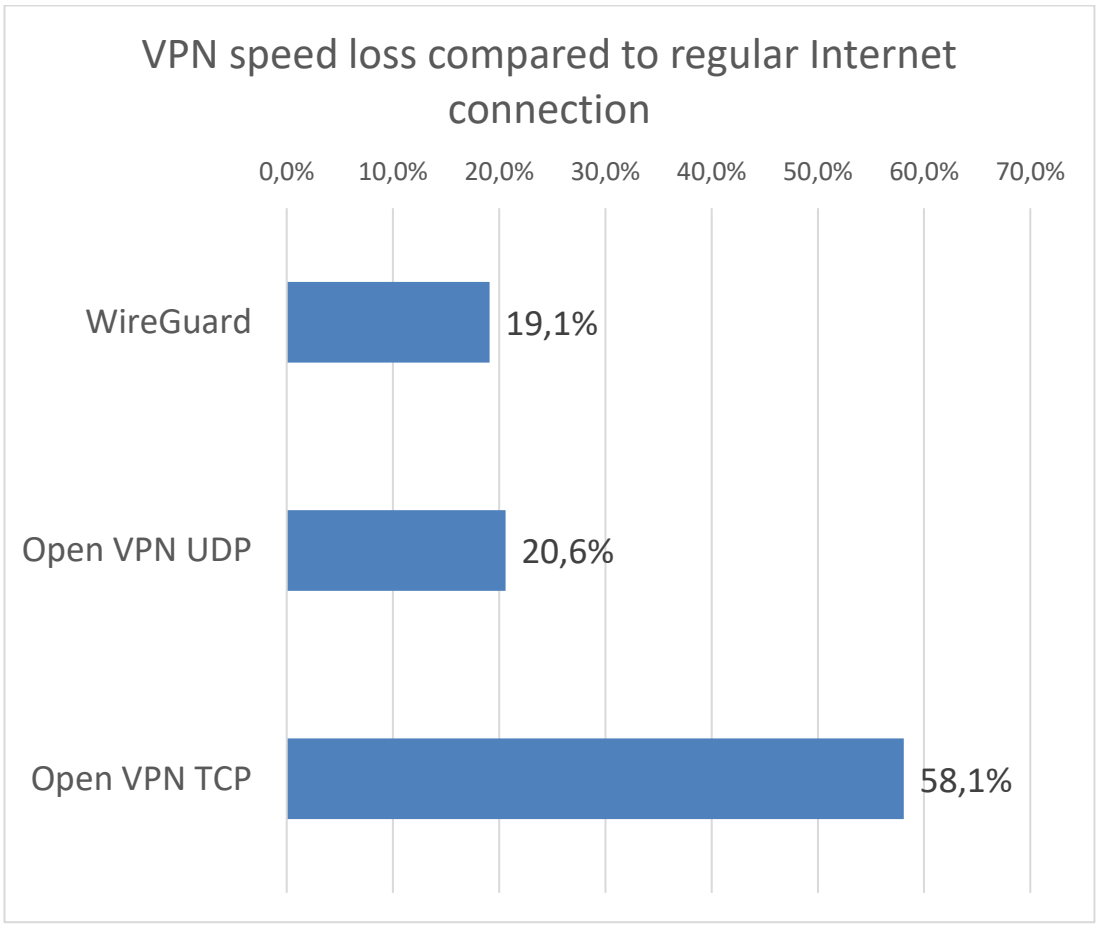

Abbildung 6: Geschwindigkeitsverlust durch VPN

3.3.3.4 VPN Varianten

Die meistgenutzten VPN Varianten sind die folgenden:

IPSec

IPSec verschlüsselt IP-Pakete direkt. Dabei unterstützt IPSec viele verschiedene Kryptoverfahren. IPSec wird von vielen Betriebssystemen (u.a. Windows, MacOS, Linux, iOS, Android) direkt, d.h. ohne zusätzliche Software unterstützt.

IPSec gilt als sicher und schnell, ist jedoch wegen seiner hohen Flexibilität mit einigem Konfigurationsaufwand verbunden. IPSec bereitet einige Probleme beim Roaming, weil beim Wechsel der unterliegenden Internet-Verbindung z.B. bei mobilen Systemen die IPSec-Verbindung neu aufgebaut werden muss. Es gibt allerdings VPN-Lösungen im Markt, die nahtloses Roaming ("Seamless Roaming") auch über IPSec unterstützen.

OpenVPN

Bei OpenVPN wird ein SSL/TLS Tunnel über TCP oder UDP aufgebaut. OpenVPN nutzt ein eigenes Security Protocol und eine Auswahl von Kryptoverfahren basierend auf der OpenSSL Library. OpenVPN ist ein Open Source Projekt.

OpenVPN über TCP eignet sich besonders bei instabilen Internet-Zugängen, hat allerdings wegen des doppelten Protokoll-Aufwands (TCP über TCP) Performance-Nachteile. Generell gilt OpenVPN als sicher, OpenVPN über UDP auch als schnell. OpenVPN Clients sind für alle gängigen Betriebssysteme verfügbar.

WireGuard

WireGuard ist ein relativ junges Protokoll, das von Jason A. Donenfeld entwickelt und unter der GNU GPLv2 als freie Software zur Verfügung gestellt wurde. Seit März 2020 ist WireGuard im Linux Kernel Release enthalten.

WireGuard sendet verschlüsselte Pakete via UDP und nutzt dabei nur ausgewählte, nicht änderbare (feste) Krypto-Verfahren, was die Konfiguration erleichtert. WireGuard gilt dennoch als sicher.

WireGuard zeichnet sich auch durch seine sehr schlanke Implementierung aus: Der WireGuard Code umfasst nur etwa 1% der Codezeilen von OpenVPN oder IPSec. Das hat große Vorteile hinsichtlich der Prüfung auf Korrektheit des Codes und wirkt sich auch auf die Geschwindigkeit aus. WireGuard ist deutlich schneller beim Verbindungsaufbau als IPSec oder OpenVPN und gilt auch als effizienter und schneller bei der Datenübertragung. Nahtloses Roaming ("Seamless Roaming") funktioniert problemlos ohne weitere Konfiguration.

WireGuard Clients sind für die wichtigen Betriebssysteme (u.a. Windows, MacOS, Linux, iOS, Android) verfügbar.

3.3.3.5 Fazit VPN

VPNs haben zwei wesentliche Nutzenaspekte aus Sicherheitssicht:

- Durch das VPN übermittelte Daten werden während des Transports verschlüsselt.
- "Verstreut" liegende Ressourcen werden in einem Netzwerk gebündelt und können entsprechend über dieses Netzwerk verwaltet und geschützt werden.

VPNs sind, bei richtiger Konfiguration, sicher, robust, schnell und für die allermeisten Plattformen verfügbar. Je mehr Cloud Computing und Mobile Computing in einer Organisation eingesetzt werden, desto sinnvoller ist der Einsatz eines VPN zum Schutz der IT-Ressourcen der Organisation.

3.3.4 Cloud Firewall

3.3.4.1 Definition "Cloud Firewall"

Unter dem Begriff Cloud Firewall können prinzipiell unterschiedliche Sicherheitslösungen verstanden werden:

- Eine in der Cloud betriebene "virtuelle" Firewall. Diese ist vom Prinzip her mit einer vor Ort "on-premise" selbst betriebenen Firewall vergleichbar, sie steht nur nicht im eigenen Rechenzentrum: "Firewall-as-a-service"
- Eine virtuelle Firewall, die dediziert Schutz für die gebuchten Cloud Services wie PaaS, IaaS bietet, also die Regeln umsetzt, die der Kunde für seinen gebuchten Dienst festlegt. Hier handelt es sich um eine neue Technologie, bei der wirksame Schutzmaßnahmen ergriffen werden, egal auf welchem Server/Infrastruktur und sogar in welchem Land die zur Verfügung gestellten Dienste gerade laufen. Die Umsetzung wird je nach eingesetzter Technologie unterschiedlich an die physikalischen Firewalls und Switches durchgereicht, die dementsprechend generischer eingestellt sind. Eine derartige Firewall bietet demnach Schutz der Ressourcen, auch bei sich laufend ändernden Zuständen
- Eine so genannte "Next Generation Firewall", welche durch die Anbindung an eine Hersteller-Cloud zusätzliche Sicherungsfunktionen erbringt ("Intelligence Cloud"). Hierdurch kann dynamisch auf Erkenntnisse des Herstellers wie Ergänzungen in Blacklists beim Zugriff auf Webseiten reagiert werden. Die Ereignisse vieler Kunden werden in einer Cloud gesammelt und übergreifend ausgewertet. Diese über reine Netzwerk-Filterung hinausgehenden Funktionen können auch mit weiteren Technologien wie Web Application Firewalls und Application Level Gateway sowie Intrusion Detection Verfahren auf Netz- oder Anwendungsebene kombiniert werden

Im Kontext dieses Beitrags wird der Fokus auf die ersten beiden Lösungen gelegt. Zum ersten sollen Einsatzzwecke und Gemeinsamkeiten mit herkömmlichen "on-premise" Firewalls aufgezeigt und im Anschluss kurz die Vor- und Nachteile von Cloud Firewalls dargelegt werden.

3.3.4.2 Gemeinsamkeiten Cloud Firewall und herkömmliche Firewalls

Generell dienen Cloud Firewalls wie auch herkömmliche Firewalls der Zugangskontrolle zu Servern/Diensten und (Web-)Anwendungen. Die Kommunikation wird basierend auf Vorgaben und Filter-Regeln gesteuert. Angriffsmöglichkeiten auf Dienste und Anwendungen, die nur unter bestimmten Voraussetzungen erreichbar sein sollen, werden erschwert. Neben der reinen Netzwerk-Topologie und Filterung nach Netzen und IP-Adressen sowie Ports können weitere Kriterien berücksichtigt werden - beispielsweise auf welche Art Clients auf Dienste zugreifen. Der regionale Standort und die verwendete Übertragungstechnologie sowie unterschiedliche Authentifizierungsverfahren können als Kriterium herangezogen werden.

3.3.4.3 Nachteile von Cloud Firewalls

Nachteile von Cloud Firewalls sind zum einen Cloud immanent: Ist der Anbieter nicht in der Lage, die Dienste zu erbringen, kommt die Kommunikation zum Erliegen. Man verdichtet somit das Risiko, dass weder von Mitarbeitern noch von Kunden die bereitgestellten Cloud-Dienste erreichbar sind. Das ist aber ein generelles Thema bei Cloud-Sicherungsinfrastrukturen und wird im Abschnitt 2.2 der Handreichung betrachtet.

3.3.4.4 Vorteile von Cloud Firewalls

Für den Einsatz von Cloud Firewalls sprechen eine Reihe von Vorteilen: Zum einen generell wie bei weiteren Cloud Services, man muss sich nur um das kümmern, was man eigentlich möchte. Im Falle der virtuellen Firewall um die Kommunikations-Regeln und wenn die Firewall einen Cloud-Dienst schützt, weitestgehend nur noch um die Anwendung selbst. Aufwände und Aufgaben für den Betrieb der Cloud Firewall können an den Anbieter abgetreten werden (Was schon hier nahelegt, dass der genaue Umfang der Aufgaben im Detail abgestimmt werden sollte). Der Nutzer/Nutznießer der Cloud Firewall kann sich aber auf die wesentliche Aufgabe, die gewünschte Kommunikationsfilterung/gebuchte Anwendung, fokussieren. Zum anderen besteht die Möglichkeit, weitere Features und Sicherungsfunktionen zu nutzen, die ggf. hohe personelle Anforderungen erfordern würden, und somit durch die Skalierungseffekte beim Anbieter kostengünstiger erbracht werden kann. Hierdurch kann ein Mehrwert entstehen, dessen Bedarf aber sorgsam abgeschätzt werden sollte. Insbesondere können auch Technologien wie beispielsweise die Nutzung eines SIEM (Security Information and Event Management) ggf. einfach hinzugefügt und vom Anbieter mit erbracht werden. Im Kontext der Anbieter-Auswahl sollte von daher das Gesamt-Sicherungspaket und nicht nur die bereitgestellte Funktionalität der Cloud Firewall allein betrachtet werden.

3.3.4.5 Anforderungen und Aufgaben zu Cloud Firewalls

Es wird empfohlen, ergänzend zu Abschnitt 4.1 die folgenden Anforderungen und Aufgaben im Detail festzulegen und mit dem Anbieter abzustimmen, wer wofür zuständig ist:

- Pflege von Regelwerken
- Vergabe von Berechtigungen der Cloud Firewall
- Aktualisierung der Komponenten der Cloud Firewall
- Auswertung von Logfiles, Alerting, Berichtswesen

Dies stellt nur die Mindestanforderungen dar. Details sollten vertraglich abgestimmt und dokumentiert werden. Ebenso welche Funktionen genau genutzt werden sollen und wie im Detail die Abstimmung zwischen Kunden und Anbieter erfolgt. Somit wird explizit festgehalten, was Bestandteil des Betriebs der Cloud Firewall ist und welche Aufgaben kundenseitig selbst übernommen werden.

3.3.5 Confidential Computing

3.3.5.1 Vor welchen Bedrohungen schützt Confidential Computing?

Daten sind bei der Übertragung von den Endgeräten der Nutzer zur Cloud bzw. im Internet der Dinge von den "Dingen" zur Cloud sowie bei der dauerhaften Speicherung durch kryptografische Verschlüsselung gut vor Zugriff durch unbefugte Dritte geschützt. Maßnahmen für die so genannte "vertrauliche Verarbeitung" ("Confidential Computing") schützen dagegen Daten auch vor unbefugten Zugriffen interner Angreifer und privilegierter Benutzer während des Rechnens in den Prozessorkernen (CPU), im Arbeitsspeicher (RAM), und auf den Systembussen. Bei Systemen ohne Confidential Computing kann oft zwischen Wartungstätigkeiten der Administratoren mit einem betriebsnotwendigen, privilegierten Zugriff und unbefugtem Zugriff auf die durch die Nutzer der Cloud in dieser verarbeiteten Daten trotz der Überwachung der Administratoren durch Systeme des "Privileged Access Management" nicht unterschieden werden.

Durch Confidential Computing kann durch zusätzliche technische Barrieren vor einem Missbrauch des - vor der Verfügbarkeit dieser Technologie - bislang noch notgedrungen akzeptierten Betreiberprivilegs durch Externe oder Innentäter geschützt werden. Darüber hinaus kann Confidential Computing gegen Angriffe via Exploits oder Hintertüren schützen, die im Betriebssystem oder den verschiedenen Komponenten der Middleware enthalten sein können. Außerdem kann Confidential Computing gegen mögliche Side-Channel-Angriffe auf Daten während deren Verarbeitung schützen.

3.3.5.2 Welche Implementierungen von Confidential Computing gibt es?

Die Kernfunktionalität von Confidential Computing ist die Bereitstellung einer gesicherten und vertrauenswürdigen Verarbeitungsumgebung (Trusted Execution Environment, TEE). Der Perimeter der TEE kann die CPU des Prozessorchips der Cloud Server mit einer zugehörigen Speicher-"Enklave" (Chip-basierte Prozessor-TEE) oder eine mit Penetrationssensorik ausgerüstete Kapsel auf Gehäuse- oder Rack-Ebene um einen oder mehrere Cloud Server sein (Penetrationssensorik-basierte Multi-Server-TEE). In diesen Systemen wird entsprechend dem Standard für die höchste Schutzklasse bei Hardware Security Modulen, FIPS 140-2, beim Ansprechen der Penetrationssensorik eine vorsorgliche Löschung der unverschlüsselten Daten der Cloud-Nutzer vorgenommen (Data Clean-up). Beiden Implementierungsarten ist gemein, dass die zu verarbeitenden Daten erst innerhalb der TEE entschlüsselt und vor dem Verlassen der TEE wieder verschlüsselt werden und dass der sichere Betriebszustand, der so genannte "versiegelte Zustand" der TEE erst nach einem Audit und nachfolgender Initialisierung der "Enklave" bzw. des TEE, erreicht wird[18].

Die Chip-basierten Prozessor-TEE schützen insbesondere gegen Angriffe durch Schwachstellen in den Betriebssystemen und den Komponenten der Systemsoftware. Die Penetrationssensorik-basierten Multi-Server-TEE schützen besser vor Side-Channel-Angriffen. Den besten Schutz bieten die Kombinationen von Penetrationssensorik-basierten Muli-Server-TEE und Chip-basierten Prozessor-TEE. Darüber hinaus gibt es noch weitere, jedoch nur einen schwächeren Schutz vermittelnde Software-TEE.

Da die Chip-basierten Prozessor-TEE sehr Hardware-nahe Funktionen sind, bedarf es für die praktische Anwendung der Technologie die Unterstützung durch Softwarekomponenten zur Einrichtung und Verwaltung der gekapselten Software und Verarbeitungsumgebungen. Neben den Internetriesen und Hyperscalern aus den Vereinigten Staaten etablieren sich für diese Hilfsfunktionen für Confidential Computing auch eine Reihe von Start-ups mit dieser Aufgabe und kooperieren u.a. auch mit europäischen Cloud-Anbietern.

3.3.5.3 Grenzen von Confidential Computing

Aus der Perspektive der Sicherheit bleiben trotz des durch Confidential Computing vermittelten besonders hohen Schutzniveaus offene Fragen bezüglich der Vertrauenswürdigkeit der das Confidential Computing implementierenden Hard- und Systemsoftware. Aufgrund der hohen Systemkomplexität muss praktisch - trotz der Prüfung der Lösungen durch externe Auditoren - auf die Vertrauenswürdigkeit der Hersteller gebaut werden.

Vorausgesetzt, Confidential Computing ist sorgfältig und vertrauenswürdig implementiert, ist für eine vertrauenswürdige Ende-zu-Ende-Lösung, beispielsweise einen Software-as-a-Service-Dienst, zusätzlich eine vertrauenswürdige Umsetzung der in einer TEE betriebenen Userland-Software des SaaS notwendig. Ab dem Moment der Versiegelung, ggf. der Signierung der Userland-Software und Initialisierung in der TEE kann zwar die Userland-Software nicht mehr verändert werden, d.h. deren Integrität ist gesichert, doch können bei der Produktion der Userland-Software sowie bei Updates Schwächen oder beabsichtigte Hintertüren übersehen werden und so in das System gelangen.

Aus der Perspektive der Performance stehen mittel- und langfristig Plattformen mit Confidential Computing den existierenden Computing-Plattformen bezüglich der RAM-Größen um nichts nach. Gegenwärtig weisen jedoch die existierenden Implementierungen der Chip-basierten Prozessor-TEE noch Grenzen im Bereich mehrerer 100 MB RAM je so genannter "Speicher-Enklave" auf, wobei jedoch viele Enklaven parallel betrieben werden können. Im Bereich der Penetrationssensorik-basierten Multi-Server-TEE existieren diese vorläufigen Speicherbegrenzungen nicht.

Allerdings erfordern Chip-basierte Prozessor-TEE systemimmanent und damit langfristig einen höheren Energieeinsatz für die vertrauliche Verarbeitung, da jeder Datenverarbeitungsbefehl, der in die CPU gesendet wird erst entschlüsselt und dann ausgeführt wird und jedes Datenverarbeitungsergebnis zuerst verschlüsselt wird, bevor es wieder über die Busse zum RAM weitergeleitet wird. Mit Penetrationssensorik-basierten Multi-Server TEE können die Side-Channel-Angriffe, für die Chip-basierte TEE noch empfindlich sind, abgesichert werden, führen aber nicht zu einem erhöhten Energiebedarf.

Aus der Perspektive der Entwicklung und des Betriebs (DevOps) ist zu beachten, dass Cloud-Infrastrukturen mit Confidential Computing mit entsprechender Hardware, entweder nur Chips, nur DCUAs oder beidem ausgestattet sein müssen. Weiter muss der Cloud-Systemsoftware-Stack das Management der Verarbeitungsumgebungen und des Prozesses der Initialisierung und Versiegelung beinhalten.

[18] Jäger, Rieken, et.al. (2020). Manipulationssichere Cloud-Infrastrukturen. ISBN 978-3-658-31848-2. Springer Nature

Als Anschlusstechnologie zu Confidential Computing ist die vertrauenswürdige Produktion der Userland Software, die damit ausgeführt werden soll anzusehen. Unsichere oder den Datenschutz nicht respektierende Userland Software wird durch Confidential Computing nicht notwendigerweise reingewaschen und sicher.

3.4 Backup Strategien Cloud / Notfallplanung

3.4.1 Konzepte für Backup und Wiederherstellung

Daten und Systeme sind für die meisten Unternehmen heute ein wichtiger Teil des Geschäftsbetriebs und müssen zur Sicherstellung der Verfügbarkeit entsprechend gesichert werden. Um eine Strategie für die Sicherung von Daten zu entwickeln, müssen als erstes die relevanten Daten und Systeme hierfür gemäß den Wiederherstellungsanforderungen identifiziert werden. Hierbei sind zwei Konzepte besonders wichtig. Die Recovery Point Objective (RPO) beschreibt den maximal tolerierbaren Zeitraum aus dem Daten verloren gehen dürfen. Hieraus ergibt sich die Anforderung, wie oft Backups durchgeführt werden müssen. Die Recovery Time Obective (RTO) ist die maximal tolerierbare Zeitspanne, die ein System nach einem Absturz ausfallen darf. Hieraus ergibt sich die Anforderung, wie lange die Wiederherstellung der Daten und Systeme dauern darf.

3.4.2 Anforderungen an Backup und Wiederherstellung

Diese und sonstige Anforderungen an die Verfügbarkeit von Daten und Systemen müssen auf Basis regelmäßiger Risikoanalysen ermittelt und als Teil der IT-Strategie festgeschrieben werden. Da die Systeme als Plattform der Datenspeicherung und -verarbeitung ein wesentliches Element des Geschäftsbetriebs darstellen, müssen System-Backup und -Wiederherstellung Teil der Betrachtung von RPO und RTO sein. Das Ergebnis dieser Analyse unterstützt die Entscheidung, welche Daten und Systeme über Backups gesichert werden sollen.

3.4.3 Verteilte IT-Infrastruktur

Zunehmend nutzen Unternehmen verschiedene Arten von Infrastruktur, die entweder als klassische Rechner oder Cloud-Infrastruktur lokal platziert sind oder virtualisiert bei Cloud-Anbietern laufen, oder bei denen Dienste spezieller Anbieter genutzt werden. Die Cloud dient hierbei zusätzlich als Ziel des Backups, stellt Daten und Dienste des Unternehmens bereit, die gesichert werden sollen, oder beides.

3.4.4 Anbindung an die Cloud

In allen Szenarien ist die zu verwendende technische Anbindung zur Übertragung des Backups und der spätere Zugriff bei Test oder Rücksicherung wesentlich.

3.4.5 Geolokalisierung Datenspeicher

Zunächst ist die Frage zu klären, wo das Backup gespeichert wird und wo es aus Compliance-Gründen gespeichert werden darf. Hierbei spielt insbesondere die Datenschutzverordnung eine wesentliche Rolle aber auch vertragliche Verpflichtungen.

3.4.6 Backupverfahren

Ein weiterer wesentlicher Aspekt ist das anzuwendende Backupverfahren, das entweder inkrementell, vollständig oder als Mix aus beidem durchgeführt werden kann. Wichtig ist hierbei die benötigte Zeit für sowohl Backup als auch Wiederherstellung. Replikation ist hier eine erwägenswerte Ergänzung von Backupstrategien, indem in Echtzeit Kopien von Daten erstellt werden, die dann jederzeit verfügbar sind.

Außerdem muss wie bei lokalen Backups auf Speichermedien als Teil der Risikoanalyse bei Sicherung in die Cloud die Frage der Redundanz zum Schutz vor Verlust geklärt werden, zum Beispiel durch Nutzung verschiedener Verfügbarkeitszonen. Als Teil einer Backup-Strategie ist die Cloud als ein weiteres Medium zu betrachten und dementsprechend zu behandeln.

Alle hier erwähnten Faktoren beeinflussen die für die Durchführung eines Backups oder einer Rücksicherung benötigte Zeit. Hier kann die oben erwähnte Replikation für wesentliche Daten mit Erfolg angewandt werden. Für Backups von Cloud-Anwendungen sind hier häufig die Konditionen in Service Level Agreements entscheidend.

3.4.7 Notfallplanung

Die Cloud-Infrastruktur muss auch im Rahmen der Notfallplanung berücksichtigt werden. Zu betrachten ist hier insbesondere die Auswirkung einer Nichtverfügbarkeit der Dienste und Daten, sei es durch eine Unterbrechung der Verbindung oder durch den tatsächlichen Verlust von Diensten und insbesondere Daten sowie deren Veränderung.

Während die Zuverlässigkeit der Erreichbarkeit insbesondere über Infrastrukturmaßnahmen wie redundante Netzzugänge erhöht werden kann, erfordert die Verfügbarkeit von Diensten und Daten Maßnahmen in der Cloud-Plattform.

Die Redundanz von Diensten und Daten kann in Cloud-Diensten durch Replikation erzielt werden. Bei hohen Anforderungen kann die Absicherung auch in Rechenzentren in verschiedenen geographischen Zonen erfolgen. Anforderungen aus der DSGVO sind hierbei natürlich weiter zu beachten.

Zum Schutz der Integrität von Daten und Diensten können Methoden zur kontinuierlichen Überwachung eingesetzt werden, die zum Beispiel Zugriffe überwachen oder regelmäßig die Daten auf Veränderungen überprüfen.

Die Cloud-Infrastruktur spielt des Weiteren eine wichtige Rolle als Teil der Notfallplanung, zum Beispiel als Ziel der Datensicherung wie oben beschrieben, zur Replikation von Applikationen und schließlich als Maßnahme, um in einem Notfall ein vollständiges Arbeiten in der Cloud zu ermöglichen.

4 Organisatorische und rechtliche Maßnahmen zur Sicherung

4.1 Aufgabenverteilung zwischen Anbieter und Nutzer

Betreibt man seine IT-Infrastruktur samt Anwendungen eigenständig (on-premises), liegt die Verantwortung und somit alle damit verbundenen Aufgaben ganz eindeutig bei der eigenen IT-Abteilung. Dazu gehören beispielsweise operativer Betrieb und Sicherung des Rechenzentrums, Überwachung des Netzwerkes, Schwachstellen- und Patchmanagement für Betriebssysteme und eingesetzte Anwendungen, Backup und Wiederherstellung, etc.

Mit dem Schritt zur Auslagerung der IT können, je nach Sourcing-Modell, Teile der Verantwortung und der Aufgaben auf den Dienstleister übertragen werden. Im Cloud-Umfeld wird in dem Zusammenhang von einer "geteilten Verantwortung" (Engl.: "shared responsibility") gesprochen. Dieser Begriff ist jedoch missverständlich, da er suggeriert, dass Dienstleister (Anbieter) und Kunde (Nutzer) gemeinsam und womöglich gleichzeitig verantwortlich sind. Dem ist jedoch nicht so. Sowohl Anbieter als auch Nutzer tragen niemals gemeinsam Verantwortung für eine und dieselbe Sache. Die Verantwortung hängt immer von den Komponenten/Assets ab, die der jeweilige Beteiligte bereitstellt und in seinem unmittelbaren Zugriff hat. Daher ist der Begriff der "verteilten Verantwortung" (Eng: "divided responsibility") konkreter und auch inhaltlich passender.

Es ist klar, dass die Informationssicherheit ganzheitlich betrachtet werden muss, denn jeder ungeklärte Bereich kann eine Schwachstelle enthalten, die durch Angreifer ausgenutzt werden kann. Der Nutzer muss daher klar verstehen, welche Themen vom Anbieter bereitgestellt werden und welche weiterhin seiner Verantwortung bleiben. Grundsätzlich gilt, je mehr Leistung von einem Anbieter übernommen wird, desto mehr Pflichten und Aufgaben werden vom Nutzer auf den Anbieter übertragen.

Besonders brisant ist die Aufgabenteilung in den Sourcing Modellen "IaaS" und "PaaS". Denn gerade bei diesen beiden Sourcing-Modellen sind die Verantwortlichkeiten zwischen Anbieter und Nutzer am stärksten verzahnt und müssen eindeutig geklärt werden.

Im Modell "Infrastructure as a Service" (IaaS) verwendet der Nutzer nur die Rechenressourcen (virtuelle Server, Speicher, Hardware, etc.) des Anbieters. Darauf baut er seine eigenen Betriebssysteme, Middleware, entwickelt oder nutzt eigene Anwendungen. Das "Platform as a service" - Modell (PaaS) geht einen Schritt weiter. Hier stellt der Anbieter die grundlegende Infrastruktur, die Entwicklungsumgebung und Laufzeitumgebung bereit. Der Nutzer verwendet diese Grundlagen für die Entwicklung und den Betrieb eigener Anwendungssoftware und ihrer Daten verwendet. Und schließlich wird im "Software as a service" - Modell (SaaS) das gesamte Leistungsspektrum (Infrastruktur und Anwendungen) vom Anbieter bereitgestellt. Der Nutzer greift auf die Anwendungen und Daten über das Internet zu.

Trotz dieser Aufteilung in die Sourcing-Modelle gibt es zwischen einzelnen Anbietern Unterschiede bezüglich der angebotenen Leistungen. Daher müssen die Zuständigkeiten bei der Wahl des Sourcing-Modells individuell identifiziert und schriftlich festgelegt werden, um geeignete Sicherheitsmaßnahmen für möglichen Schwachstellen aufzusetzen.

Eine Tendenz bezüglich der Zuordnung der Verantwortlichkeiten kann der nachfolgenden Grafik entnommen werden:

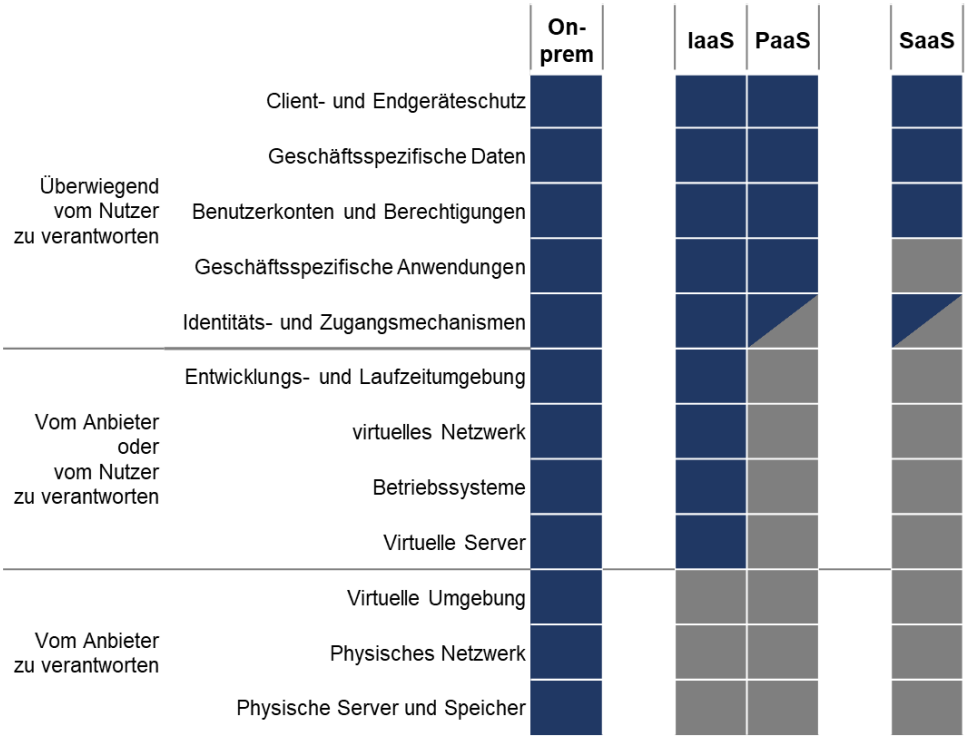

Abbildung 1: Zuordnung der Verantwortlichkeiten[19]

Vom Anbieter zu verantworten

Zu den wesentlichen Aufgaben des Anbieters in allen Sourcing-Modellen gehört die Sicherstellung einer hochverfügbaren Host-Infrastruktur. Dazu gehört beispielsweise:

- Bereitstellung der physischen Server und Speicher
- Netzwerkverwaltung
- Lastenausgleich
- Schwachstellen und -Patchmanagement der Grundinfrastruktur
- Festlegung von Sicherheitsanforderungen für Räumlichkeiten und Gebäude
- Umsetzung eines Redundanzmodells
- Perimeterschutz
- Zutrittskontrolle
- Schutz vor Feuer und Rauch
- Schutz vor Ausfall der Versorgungseinrichtungen
- Überwachung der Betriebs- und Umgebungsparameter

Darauf wird die Virtualisierung aufgebaut, in der die vorhandenen physischen Ressourcen (Hardware, Speicher, CPU, etc.) virtuell aufgeteilt werden. Durch die Virtualisierung kann jeder virtuelle Computer individuell verwaltet und angesteuert werden. Beispielsweise können unterschiedliche Betriebssysteme installiert oder diese unterschiedlich konfiguriert und genutzt werden, während die gleichen physischen Ressourcen verwendet werden.

Vom Anbieter oder vom Nutzer zu verantworten

Im IaaS greift der Nutzer auf die Rechenkapazitäten aus der Cloud zu, baut darauf seine eigene Umgebung (Netzwerk, VM, Storage, etc.) auf und entwickelt ggfs. seine eigene Anwendungssoftware. Hierfür ist er für die Sicherheit und Verwaltung zuständig.

[19] In Anlehnung an Cloud Security Alliance, https://cloudsecurityalliance.org/

Werden, wie im PaaS, die virtuellen Server, das virtuelle Netzwerk und Middleware vom Anbieter bereitgestellt, übernimmt dieser auch die Verantwortung für die Sicherheitskonfiguration und Verwaltung der jeweiligen Komponente.

Im SaaS hingegen werden die Anwendungen vom Anbieter bereitgestellt, weshalb er für die Sicherheitskonfiguration und Verwaltung der Anwendung verantwortlich ist. Der Nutzer ist jedoch für die Einhaltung der Sicherheitsrichtlinien innerhalb der Anwendersoftware sowie der Daten verantwortlich. In manchen Fällen ist seitens des Nutzers gezielte Konfiguration von Sicherheitsfunktionen der Anwendungen sowie Integration mit kundenseitigen Lösungen (z.B. Single-Sign-On) erforderlich.

Überwiegend vom Nutzer zu verantworten

Im IaaS liegt die Verantwortung für die Bereitstellung der Identitäts- und Zugriffsmechanismen beim Nutzer. Für die Identifikation können unterschiedliche Methoden verwendet werden, die an die eigenen Rahmenbedingungen angepasst werden müssen. Dazu gehören beispielsweise:

- die Anbindung an die Unternehmens-"Active Directory"
- die Einrichtung eines (externen) Identitätsanbieters
- die Konfiguration von Verwaltungsdiensten
- die Einrichtung und Konfiguration von Benutzeridentitäten und
- die Implementierung von rollenbasierten Zugriffskontrollen für die genutzten Dienste
- Überwachung und Protokollierung der Zugriffe

Je nach Anbieter und gewähltem Service können im PaaS die Authentisierungsmechanismen vom Anbieter oder vom Nutzer geliefert werden. Im SaaS hingegen werden sie vom Anbieter bereitgestellt.

Die Verwaltung der Benutzerkonten und Berechtigungen bleibt jedoch in allen Sourcing-Modellen in der Verantwortung des Nutzers.

Ebenfalls bleibt der Nutzer für die Unternehmensdaten verantwortlich. Denn nur er kennt die eigenen Geschäftsprozesse und kann die Daten gemäß nachvollziehbaren Kriterien klassifizieren. Im SaaS Modell muss gegebenenfalls für geeignete Konfiguration der Anwendungssoftware sorgen. Er muss sicherstellen, dass sensible Daten besonders beschützt werden, während allgemeine Daten eine weniger strikt gehandhabt werden können.

Zudem ist der Nutzer für die sichere Konfiguration und Betrieb der Endgeräte verantwortlich, die auf die Cloud-Dienste zugreifen. Dazu gehören beispielsweise das Patchmanagement oder geeigneter Zugriffsschutz der Geräte.

Unabhängig vom Sourcing-Modell muss der Nutzer über eigene qualifizierte Personalressourcen verfügen, um die Sicherheitskonfiguration der verwendeten Komponenten gesamtheitlich zu verstehen, zu überprüfen oder ggfs. anzupassen.

Über alle Ebenen müssen die individuellen Verantwortlichkeiten in Richtlinien festgehalten und die erforderlichen Maßnahmen umgesetzt werden.

4.2 Vertragsgestaltung

Über alle Ebenen müssen die individuellen Verantwortlichkeiten in Richtlinien festgehalten und die erforderlichen Maßnahmen umgesetzt werden.

Dazu wird dargestellt, wie Cloud-Anbieter und Kunde im Hinblick auf die datenschutzrechtliche Verantwortlichkeit einzuordnen sind (4.2.2). Anschließend werden die gesetzlich vorgeschriebenen Mindestinhalte einer Vereinbarung über die Auftragsverarbeitung (auch "AV-Vereinbarung" oder "DPA" stehend für data processing agreement) dargestellt (4.2.3), um dann darüber hinausgehende Regelungen aufzuzeigen, die dazu geeignet sind, die Datenverarbeitung weiter abzusichern (4.2.4). Schließlich wirft der Beitrag einen Blick auf die Folgen des sog. Schrems-II-Urteils des EuGH für die Gestaltung von Cloud-Verträgen bzgl. des Datentransfers in Drittstaaten (4.2.5).

Es sind bei der Vertragsgestaltung noch diverse weitere Rechtsbereiche im Auge zu behalten, wie der Geheimnisschutz nach dem Geschäftsgeheimnisschutzgesetz, die bereichsspezifischen Normen für Betreiber Kritischer Infrastrukturen, das AGB-Recht des Bürgerlichen Gesetzbuches und weiteres mehr.

4.2.1 Einleitung

Bei der Nutzung von Cloud-Lösungen von Drittanbietern werden die zu verarbeitenden Daten notwendigerweise aus der eigenen Herrschaftssphäre entlassen. Es ist daher von entscheidender Bedeutung, rechtssichere Vereinbarungen mit dem Cloud-Anbieter zu treffen, welche zum einen die IT-Sicherheitsmaßnahmen des Cloud-Anbieters hinsichtlich sämtlicher Verarbeitungsvorgänge, an denen er beteiligt ist, regeln und zum anderen wirksame Werkzeuge bereithalten, um gegen mögliches Fehlverhalten des Cloud-Anbieters schnell und effizient vorgehen zu können.

Diese Aufgabe übernehmen der Leistungsvertrag zwischen dem Nutzer und dem Cloud-Anbieter als auch das gesetzlich notwendige DPA nach Art. 28 DSGVO oder eine Vereinbarung über die gemeinsame Verantwortlichkeit ("JC-Vereinbarung", stehend für Vereinbarung zur Joint Controllership) nach Art. 26 DSGVO. Im Hinblick auf die rechtliche Wirksamkeit macht es keinen Unterschied, wo die Regelungen getroffen werden; vielmehr kommt es auf den Inhalt der einzelnen Regelungen an. Gleichwohl bietet es sich in der Regel an, die im Folgenden dargestellten Regelungsbereiche im Rahmen des DPA (oder der JC-Vereinbarung) zu berücksichtigen. Der Gesetzgeber sieht für Processor to Controller-Konstellationen (Auftragsverarbeitung) ohnehin bestimmte Mindestinhalte für das DPA vor, die eine sinnvolle Grundlage für eine ausdifferenzierte vertragliche Regelung bieten, Art. 28 Abs. 3 DSGVO. Art. 26 DSGVO enthält keine ausdrücklichen Vorgaben zur Datensicherheit. Diese Anforderungen sind aber nach Abs. 1 S. 1 und 2 grundsätzlich im Rahmen der Festlegung der "Mittel" der Verarbeitung und der Aufteilung der Verpflichtungen aus der DSGVO mitzubestimmen.

4.2.2 Datenschutzrechtliche Verantwortlichkeit

Wesentlicher Ausgangspunkt für die Vertragsgestaltung ist die Auseinandersetzung mit der Frage, wer datenschutzrechtlich Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO ist. Verantwortlich ist derjenige, der allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Der Cloud-Anbieter bietet eine Leistung (Cloud Hosting) an, deren wesentlicher Inhalt die Verarbeitung von Daten ist. Diese führt er in der Regel auf Weisung des Kunden aus. Der Kunde bestimmt, ob und wann welcher Verarbeitungsvorgang ausgelöst wird. Datenschutzrechtlich Verantwortlicher ist damit in der Regel der Kunde. Der Cloud-Anbieter verarbeitet die Daten für diesen lediglich im Auftrag. Für diesen Fall der kollaborativen Datenverarbeitung schreibt die DSGVO in Art. 28 bestimmte vertragliche Mindestinhalte vor, um die Sicherheit der Datenverarbeitung zu gewährleisten.

Je nach Art der konkreten kollaborativen Datenverarbeitung ist auch denkbar, dass der Cloud-Anbieter und der Kunde gemeinsam verantwortlich sind. Das ist dann anzunehmen, wenn der Cloud-Anbieter mit der Datenverarbeitung eigene Zwecke verfolgt (z. B. Auswertung der personenbezogenen Daten des Kunden zu eigenen Zwecken) und selbst Möglichkeiten hat, über die Zwecke und Mittel zu bestimmen. Auch in diesem Fall schreibt der Gesetzgeber eine datenschutzrechtliche Vereinbarung vor (Art. 26 DSGVO).

Im Folgenden wird sowohl auf die Mindestanforderungen für die Auftragsverarbeitung als auch die zu empfehlenden zusätzlichen Regelungen eingegangen, um die rechtlichen Gestaltungsmöglichkeiten für Cloud-Hosting-Verträge darzustellen. Diese Ausführungen sind auf Konstellationen der gemeinsamen Verantwortlichkeit in weiten Teilen übertragbar. In den meisten Fällen wird die Leistungsbeziehung zwischen den Akteuren so ausgestaltet sein, dass eine Auftragsverarbeitung vorliegt, so dass diese im Folgenden als Prämisse unterstellt wird.

4.2.3 DPA nach Art. 28 DSGVO

Die vom Gesetzgeber vorgesehenen Mindestanforderungen für ein DPA sind recht streng, in ihrem Regelungsumfang aber überschaubar.

Zu folgenden Bereichen sind gem. Art. 28 Abs. 3 DSGVO zwingend Regelungen zwischen dem Cloud-Anbieter und dem Kunden zu treffen:

- Gegenstand, Dauer, Art und Zweck der Verarbeitung
- Pflichten und Rechte des Verantwortlichen
- Verarbeitung darf nur auf Weisung des Verantwortlichen erfolgen
- Auftragsverarbeiter stellt sicher, dass seine Mitarbeiter zur Vertraulichkeit verpflichtet sind
- Auftragsverarbeiter verpflichtet sich, angemessene technische und organisatorische Schutzmaßnahmen zu treffen
- Einschaltung von Unterauftragnehmern nur mit Zustimmung des Verantwortlichen

- Pflicht des Auftragnehmers zur Unterstützung des Verantwortlichen bei Betroffenenrechten und bei der Umsetzung der gesetzlich vorgeschriebenen Sicherheit der personenbezogenen Daten sowie
- Umgang mit Daten nach Abschluss der Verarbeitungsleistung

Für die Gewährleistung der IT-Sicherheit der Daten sind die Regelungen zu den technischen und organisatorischen Maßnahmen ("TOM") von zentraler Bedeutung. Art. 32 DSGVO schreibt vor, dass geeignete technische und organisatorische Maßnahmen zu treffen sind, um ein dem durch die Verarbeitungstätigkeit begründeten Risiko für die Rechte und Freiheiten natürlicher Personen angemessenes Schutzniveau zu gewährleisten. Dafür kommen insbesondere folgende Maßnahmen in Betracht:

- Pseudonymisierung und Verschlüsselung
- Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen sowie
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Die technischen und organisatorischen Maßnahmen sind nach der Höhe des Schutzbedarfs auszuwählen. Der Schutzbedarf wiederum ergibt sich insbesondere aus der Eintrittswahrscheinlichkeit und Schwere des Risikos für Rechte und Freiheiten der Betroffenen (i. e. natürliche Personen). Diese Prüfung hat für jeden Verarbeitungsvorgang zu erfolgen. Je höher der Schutzbedarf eingestuft wird, desto näher müssen die Maßnahmen am Stand der Technik orientiert sein.

Die vom Gesetz geforderte Berücksichtigung des Stands der Technik erfordert eine besonders exakte Beachtung und planmäßige Umsetzung. Zu unterscheiden ist auf einer objektiv-technischen Ebene die Identifizierung von Maßnahmen dieses Technologieniveaus. Dazu leistet die Handreichung zum "Stand der Technik" des TeleTrusT eine hervorragende Grundlage[20]. Gesondert davon ist die Frage zu betrachten, ob im subjektiven, konkreten Fall eine solche Maßnahme gesetzlich geboten ist.[21]

Diese Aufzählung von Maßnahmen und IT-Sicherheitszielen in Art. 32 Abs. 1 DSGVO ist aus Sicht der IT-Sicherheit unvollständig, unsystematisch und einigermaßen beliebig. Die Maßnahmen in Art. 32 Abs. 1 DSGVO kennzeichnet der Gesetzgeber durch das Wort "gegebenenfalls" als nicht zwingend. Es handelt sich lediglich um Beispiele. Welche Maßnahme im konkreten Fall zu treffen ist, um die Anforderungen von Art. 32 DSGVO zu wahren, ist daher von einer Einzelfallprüfung abhängig. Es genügt also nicht, lediglich die vom Gesetzgeber genannten Maßnahmen zu implementieren. Es bedarf vielmehr einer dem Einzelfall entsprechenden Maßnahme, die derart umfangreich dokumentiert wird, dass der Entscheidungsprozess der Einzelfallentscheidung nachvollziehbar ist. Im Zweifel sind sowohl für die Entscheidung bzgl. der zu wählenden Maßnahme als auch für die Dokumentation spezialisierte Rechtsanwälte zurate zu ziehen.

Für die Darstellung der TOM trifft das Gesetz keine genauen Vorgaben. Eine ausführliche Darstellung hat den Vorteil, dass der Verantwortliche sich bereits im Rahmen der Vertragsgestaltung von der Einhaltung angemessener Sicherheitsstandards überzeugen kann. Die Praxis zeigt, dass in sog. kunden- oder leistungsbezogenen TOM (im Gegensatz zu unternehmensinternen TOM-Dokumentationen) eine vertiefte Darstellung vergeblich erwartet wird. Auch die TOM-Dokumentationen vieler Cloud-Anbieter sind deutlich zu wenig detailliert und kaum konkret prüfbar. Deshalb ist es ratsam, die TOM-Listen der Cloud-Anbieter sorgfältig auf die umfänglichen Anforderungen des Art. 32 DSGVO hin zu prüfen und ggf. nachzufassen.

4.2.4 Empfohlene zusätzliche Regelungen

Die Berücksichtigung der vom Gesetzgeber vorgesehenen Mindestinhalte allein sind bei weitem noch kein Garant für eine effektive vertragliche Absicherung der in der Cloud befindlichen Daten. Im Rahmen der Vertragsfreiheit bietet es sich daher an, deutlich umfassendere und konkretere Regelungen für den Umgang mit den Daten und den zu treffenden Maßnahmen zu vereinbaren. Im Rahmen dieses Leitfadens können des Umfangs wegen nur einige Beispiele zusammengestellt werden. Eine weitergehende Befassung sollte unter Einbeziehung der Bereiche IT, IT-Sicherheit, Datenschutzbeauftragte/r und IT-Rechtsanwältin/-anwalt erfolgen.

---

[20] TeleTrusT-Handreichung "Stand der Technik": https://www.teletrust.de/publikationen/broschueren/stand-der-technik/
[21] Bartels/ Backer, Die Berücksichtigung des Stands der Technik in der DSGVO, DuD, 4-2018, 214.

Audit-Klausel

Eine ausdifferenzierte Audit-Klausel ist ein entscheidendes Werkzeug, um effektiv bereits im Vorfeld sicherstellen zu können, dass Sicherheitsmaßnahmen eingehalten werden. Eine entsprechende Klausel kann überdies auch auf den Auftragsverarbeiter incentivierend wirken, proaktiv und nachhaltig die Einhaltung der Sicherheitsmaßnahmen sicherzustellen, wenn bestimmte Rechtsfolgen vertraglich an die Nichteinhaltung gebunden worden sind. Des Weiteren sind sinnvoll: 1. eine klare Kostenregelung. Audits verursachen Aufwände auf beiden Vertragspartnerseiten. 2. eine Vereinbarung konkreter Rechtsfolgen. Es bedarf einer Antwort zur Frage, wie mit (negativen) Feststellungen aus erfolgten Audits umzugehen ist.

Unterauftragnehmer des Cloud-Anbieters

Die DSGVO verlangt bereits eine Regelung zur Einschaltung von Subunternehmern durch den Auftragnehmer mittels Zustimmung des Auftraggebers. Überdies kann im Einzelfall eine Berechtigung des Auftraggebers sinnvoll sein, auch bei Subunternehmern angemessene Überprüfungen und Inspektionen durchführen zu dürfen. Ein solches Kontrollrecht erhöht die Wahrscheinlichkeit, dass auch der Subunternehmer die vereinbarten Regelungen tatsächlich einhält.

Rechtsfolgenregime

Von herausragender Wichtigkeit für die praktische Wirksamkeit des DPA ist ein austariertes Rechtsfolgenregime. Ist die Nichteinhaltung an spürbare Rechtsfolgen gebunden, steigt die Wahrscheinlichkeit, dass sich die Vertragsparteien an die Vereinbarungen halten. Wirksam sind u. a. Malus-Regelungen, Regelungen zum Schadenersatz, Schadenersatzpauschalierung, Vertragsstrafen und die Einordnung als wichtiger Kündigungsgrund.

Technische und organisatorische IT-Sicherheitsmaßnahmen

Wie oben dargestellt (vgl. III. DPA nach Art. 28 DSGVO) empfiehlt es sich, die technischen und organisatorischen Maßnahmen umfangreich zu dokumentieren. Zusätzlich können hier Maßgaben zur Detaillierung, Methode, Form der Dokumentation, Revisionszyklen, Abstimmungsprozessen, externen Maßstäben, Zertifizierungen u. a. m. geregelt werden, um für die gesamte Laufzeit des Vertrages gesetzeskonforme TOM umsetzen zu können - und gleichzeitig sicherzustellen, dass die jeweilige Anpassung der TOM hinsichtlich der Verfahren, der Technik und Kosten planbar bleibt (siehe auch Ziff. 5 unten).

IT Security Services/ Change Management

Das DPA ist in der Regel in seiner Laufzeit an den Leistungsvertrag gekoppelt. Bei Dauerschuldverhältnissen zur IT-Sicherheit stellt sich die Frage, wie mit Änderungen der äußeren Gegebenheiten umzugehen ist. Der Stand der Technik verändert sich und entwickelt sich bspw. während der Laufzeit weiter, so dass die getroffenen Maßnahmen im Zweifel nicht mehr der ursprünglich getätigten Abwägung standhalten. Auch der Austausch von Hardware kann dazu führen, dass die vertraglichen Vereinbarungen nicht mehr zu den tatsächlichen Umständen passen. Damit derartige Umstände nicht zu (vermeidbaren) Friktionen zwischen den Parteien führen, empfehlen sich explizite Klauseln für ein IT Security Change Management. Diese Klauseln sollten klare Fristen vorsehen, innerhalb derer die jeweils andere Vertragspartei über anstehende Änderungen (z. B. Hardwareaustausch, Softwareupdate etc.) informiert werden muss. Im Zuge dieser Mitteilung kann auch dargestellt werden, warum sich durch die Veränderung das Schutzniveau nicht vermindert. Im Gegenzug kann vereinbart werden, dass die Einwilligung in die Veränderung nur verweigert werden darf, wenn begründete Zweifel dargelegt werden, dass durch die Veränderung das Schutzniveau sinkt. Überdies können sich Regelungen über bestimmte Leistungen und Pflichten mit IT-Sicherheitsbezügen anbieten, die vergleichbar sind mit üblichen Service Level Agreements (SLA) für die Hauptleistung.

Kommunikation

Insbesondere wenn es im Rahmen der Vertragsdurchführung zu Leistungsstörungsereignissen kommt, können dezidierte Regelungen zur Kommunikation und ein explizites Eskalationsregime unnötige Rechtsstreitigkeiten verhindern und die langfristige Stabilität des Vertragsverhältnisses gewährleisten. Dabei sollte antizipiert werden, dass in solchen Fällen verschiedenste Akteure auf Seiten der Parteien eingebunden werden müssen (zu denken ist u. a. an die Bereiche IT, IT-Sicherheit(-sbeauftragte/r), Datenschutzbeauftragte/r, Rechtsabteilung/ Rechtsanwalt/-anwältin, Compliance und u. U. Fachabteilung). Klare Regelungen darüber, wer wen wann worüber zu informieren hat, sind daher dringend anzuraten.

Benachrichtigungspflichten

Im Falle von IT-Sicherheitsvorfällen und Schwachstellen auf Seiten des Auftragnehmers muss sich der Auftraggeber darauf verlassen können, dass der Auftragnehmer ihn rechtzeitig auf den Vorfall hinweist. Nur so ist gewährleistet, dass der Auftraggeber seinen Meldepflichten nachkommen kann. Es empfiehlt sich daher, ausdrückliche Regelungen über den Umfang, das Verfahren und den zeitlichen Ablauf der Benachrichtigung zu treffen und zu vereinbaren, welche Mitwirkungspflichten der Auftragnehmer schuldet. Das sollte auch für Verdachtsfälle gelten, die gesetzlich nicht adressiert sind.

4.2.5 Datentransfer in Drittstaaten

Die Datenübermittlung in ein Land außerhalb der EU ("Drittland") ist nur unter bestimmten Voraussetzungen zulässig. Eine Vielzahl von Cloud-Anbietern hat nicht nur seinen Sitz in den USA, sondern betreibt dort auch die eigenen Server-Farmen. Es kommt bei Inanspruchnahme dieser Angebote damit zwingend zu einem Datentransfer in einen Drittstaat.

Die DSGVO sieht in den Art. 44 ff. verschiedene Möglichkeiten vor, den Datentransfer rechtskonform zu gestalten. Die Variante mit der höchsten praktischen Relevanz sind die sog. Standarddatenschutzklauseln ("SCC", bislang: EU-Standardvertragsklauseln).

SCC

Dabei handelt es sich um von der Europäischen Union genehmigte Klauseln zur vertraglichen Absicherung des Datentransfers in Drittländer. Die SCC (Standard Contractual Clauses) eignen sich insbesondere für die Übermittlung personenbezogener Daten an Empfänger, die die Daten zum Zwecke der Auftragsdatenverarbeitung erhalten.

Schrems II

Durch die sog. Schrems-II-Entscheidung (EuGH, Urteil vom 16. Juli 2020, Rs. C-311/18) hat der Europäische Gerichtshof festgestellt, dass das EU-U.S. Privacy Shield und der darin enthaltene Angemessenheitsbeschluss der EU-Kommission, der bis dahin eine Rechtsgrundlage für den Datentransfer in die USA bot, ungültig sind. Nach Ansicht des EuGH bietet das US-Recht kein Schutzniveau, das dem der EU im Wesentlichen gleichwertig ist. Dabei nimmt der EuGH insbesondere Bezug auf die weitreichenden Befugnisse für US-amerikanische Geheimdienste. Ein Datentransfer in die USA unter Nutzung der SCC soll aber weiterhin möglich sein, wobei es dann zusätzlicher Sicherheitsmaßnahmen bedürfe, um ein der EU vergleichbares Schutzniveau zu gewährleisten.

Am 4. Juni 2021 hat die EU-Kommission neue Standarddatenschutzklauseln veröffentlicht, die die Vorgängermodelle, die aufgrund der Datenschutzrichtlinie verabschiedet worden waren, ablösen. Die neuen SCC sollen die Erfordernisse, die der EuGH im Schrems-II-Urteil herausgearbeitet hat, besser umsetzen. Eine Überprüfung der Rechtslage im Drittland und das Treffen zusätzlicher Maßnahmen wird dadurch aber im Einzelfall dennoch nicht vermeidbar sein.

Es ist daher auch künftig zu prüfen, ob in dem Drittland ein angemessenes Datenschutzniveau besteht und ob ggf. Maßnahmen zu treffen sind, um ein angemessenes Datenschutzniveau zu sichern. Wie die zusätzlichen Sicherheitsmaßnahmen aussehen, ist vom Einzelfall abhängig. Für die USA heißt das konkret, dass insbesondere verhindert werden muss, dass US-Behörden auf die in den USA gespeicherten Daten zugreifen können.

Dem könnte man sich etwa durch eine Verpflichtung zu besonderen Verschlüsselungsstandards annähern. Ebenfalls denkbar ist eine Vereinbarung, wonach der Auftragsverarbeiter sich verpflichtet, sich gegen jedes Herausgabeverlangen einer US-Behörde von Daten eines EU-Kunden zu widersetzen und Rechtsmittel einzulegen, um das Vorgehen - unabhängig von den Kosten - anzufechten. Zu berücksichtigen ist aber, dass solche Vereinbarungen immer nur zwischen den Vertragsparteien Wirkung entfalten und insbesondere gesetzliche Zugriffsrechte von staatlichen Behörden nicht einschränken können. Ein Datentransfer in Drittstaaten mit besonders extensiven Zugriffsrechten auf personenbezogene Daten wird damit faktisch in der Regel nicht vollständig DSGVO-konform abzubilden sein.

Überdies empfiehlt sich die Nutzung der vom Europäischen Datenschutzausschuss (EDSA) entwickelten Checkliste[22] zur Absicherung von Datentransfers in Drittstaaten. Diese beschreibt ein Vorgehen in sechs Schritten, mit dem Unternehmen ihre Datentransfers einer ersten Prüfung unterziehen können.

[22] https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

Jedenfalls bedingt die Nutzung von Cloud-Angeboten mit Drittstaatenbezug die dauerhafte und regelmäßige Überprüfung der Voraussetzungen und Maßnahmen, die bei bzw. vor Nutzungsbeginn zur Feststellung der Rechtskonformität beigetragen haben.

4.2.6 Fazit Vertragsgestaltung

Die Nutzung von Cloud-Anbietern sollte insbesondere aus datenschutzrechtlicher Perspektive vertraglich umfassend geregelt werden. Es empfiehlt sich, es nicht bei der Erfüllung der gesetzlichen Mindestanforderungen zu belassen, sondern im Rahmen der Privatautonomie weitere explizite Regelungen zu treffen. So lassen sich spätere Rechtsstreitigkeiten vermeiden und das Sicherheitsniveau deutlich erhöhen.

Bei einem Datentransfer in einen Drittstaat sind überdies zusätzliche Anforderungen zu berücksichtigen. Auch die neuen SCC werden aller Voraussicht nach keinen risikofreien Datentransfer ermöglichen. Eine sorgfältige Einzelfallprüfung bleibt erforderlich. Letztlich ist es weiterhin ratsam - wo möglich - Cloud-Anbieter, die eine Datenverarbeitung ausschließlich innerhalb der EU gewährleisten, vorzuziehen.

5 Testate und Zertifikate

5.1 Wie kann ich als Anwender Zertifikate und Testate nutzen?

Zertifikate und Testate werden dafür genutzt, das Vertrauen in das geprüfte System zu erhöhen. Eine neutrale Stelle prüft das System hierfür nach vorher festgelegten Kriterien, die dem Anwender bestätigen, ob das System die Kriterien erfüllt oder nicht. Der Hersteller kann damit ein Zertifikat oder Testat als Nachweis gegenüber Kunden einsetzen, ohne den Kunden gegenüber zu viel geistiges Eigentum offenlegen zu müssen. Er selbst kann zusätzlich fordern, dass die Lieferanten ihre Produkte zertifizieren lassen, um die Anhebung der Vertrauenswürdigkeit auch auf seine Lieferanten auszudehnen.

5.2 Was erhalte ich?

Der Kunde erhält durch ein Zertifikat oder Testat einen Nachweis über sicherheits- bzw. datenschutzrelevanten Eigenschaften des Systems. Dies beinhaltet insbesondere welche Sicherheitsvorkehrungen die Daten vor potentiellem Missbrauch schützen, wo die Daten verarbeitet werden oder wie beispielsweise bei Sicherheitsvorfällen oder (Natur-) Katastrophen vorgegangen wird. Der Kunde benötigt diese Auskünfte als Grundlage für sein eigenes Risikomanagement, sofern dieses durch die Cloud-Nutzung betroffen ist.

Bei der Auswahl der Zertifikate oder Testate, die ein beauftragter Cloud-Dienst-Anbieter für seinen Dienst ausweisen können sollte, ist dem Kunden des Cloud-Anbieters empfohlen darauf achten, ob diese für sein Geschäftsmodell tatsächlich relevant sind. Möchte der Kunde beispielsweise personenbezogene Daten mit Hilfe des Cloud-Dienstes verarbeiten und eine hinreichende Bestätigung der datenschutzrechtlich korrekten Nutzung des Cloud-Dienstes erhalten, sollte der Kunde einen Cloud-Dienst auswählen, der nach den Kriterien eines durch den Europäischen Datenschutzausschuss oder eine Datenschutzaufsichtsbehörde seines Mitgliedstaates genehmigten Kataloges geprüft wurde und das entsprechende Zertifikat erhielt.

Liegt jedoch die Bestätigung der IT-Sicherheit für nicht-personenbezogene aber geschäftskritische Daten, oder eine zusätzlich zum Datenschutz relevante Bestätigung der IT-Sicherheit im Interesse des Kunden, so kann dies durch ein IT-Sicherheitszertifikat nach ISO/IEC-Standards oder beispielsweise ein Testat nach dem Verfahren und den Kriterien des C5-Kataloges des Bundesamtes für Sicherheit in der Informationstechnik (BSI) erfolgen.

5.3 Unterschied Zertifikate/Testate

Bei einer Zertifizierung prüft ein Auditor einer anerkannten, unabhängigen Prüfstelle den Prüfgegenstand nach vorher festgelegten Kriterien (Standards). Anschließend bestätigt die akkreditierte, neutrale Zertifizierungsstelle durch ein Zertifikat, dass im Prüfbericht alle für das Zertifikat notwendigen Bedingungen enthalten sind. Durch ein Testat testiert im Vergleich dazu ein Wirtschaftsprüfer, dass der Cloud-Dienst die Kriterien eines anerkannten Prüfkatalogs erfüllt und er das geprüft hat.

Wirtschaftsprüfer treffen für die Testate nur Aussagen über gegenwärtige oder vergangene Gegebenheiten, dementsprechend gilt ein Testat für die Vergangenheit. Dahingegen werden Zertifikate für die Zeit nach der Prüfung ausgestellt.

Die Prüftiefe, d.h. der Umfang und der Prüfungen sowohl für Testate als auch Zertifikate kann sich erheblich unterscheiden und bestimmt vielfach deren Aussagekraft. Daher sei Kunden von Cloud-Diensten empfohlen, falls möglich, zusätzlich zu den Aussagen des Testats bzw. Zertifikats auch detailliertere Aussagen der Prüfberichte zu berücksichtigen.

Die Verantwortung zur korrekten Arbeitsweise der Prüfer/Auditoren liegt grundsätzlich bei den Prüfern bzw. der Prüfstelle selbst. Sie sichern sich gegenüber dem Cloud-Anbieter dadurch ab, dass sie ihre Aussagen unter dem Vorbehalt treffen, dass der Cloud-Anbieter seine Aussagen gegenüber den Prüfern korrekt getroffen hat.

In jedem Fall muss bei der Auswahl des Cloud-Dienstes darauf geachtet werden, dass das Testat oder Zertifikat durch zugelassene Wirtschaftsprüfer bzw. von durch die Deutsche Akkreditierungsstelle DAkkS akkreditierte Stellen ausgestellt wird. Gesellschafter der DAkks sind zu 1/3 die Bundesrepublik Deutschland, zu 1/3 die Bundesländer und zu 1/3 der Bundesverband der Industrie.

Bei Testaten sollte der betrachtete Prüfzeitraum nicht zu lange zurückliegen und bei Zertifikaten die Gültigkeitsdauer noch nicht abgelaufen sein.

5.4 Landschaft

Es gibt eine große Anzahl von Verfahren, mit denen Cloud-Anbieter ihre Umsetzung von Anforderungen an Cloud-Dienste nachweisen können. Dies ist vor allem der Popularität dieser Dienste geschuldet, und damit einhergehenden vermehrten Nachfragen nach Garantien für die Qualität der verschiedenen Aspekte der Dienste, so zum Beispiel Leistung und Informationssicherheit.

Zu den als stabil erachteten Verfahren gehören die weit verbreiteten Zertifizierungen nach ISO Standards, hier insbesondere ISO 27001 zu Anforderungen an Informationssicherheits-Managementsysteme und ISO 27002 als Leitfaden für das Informationssicherheits-Management, aber insbesondere auch ISO 27017 als Anwendungsleitfaden für Informationssicherheitsmaßnahmen basierend auf ISO/IEC 27002 für Cloud-Dienste und ISO 27018 in Bezug auf Leitfaden zum Schutz personenbezogener Daten (PII) in öffentlichen Cloud-Diensten als Auftragsdatenverarbeitung. Wie die Titel der Verfahren bereits andeuten, haben sie in der Regel Fokus auf allgemeine IT-Systeme und sind nur begrenzt auf Cloud-spezifische Anforderungen ausgerichtet. Abhängig von einer Bewertung des zu nutzenden Dienstes und der erwarteten Anwendung ist auch die Auswahl von Cloud Providern zu erwägen, die nach ISO 27001 auf der Basis vom BSI IT-Grundschutz zertifiziert sind.

Das vom Bundesministerium für Wirtschaft und Energie geförderte AUDITOR-Projekt entwickelt eine Datenschutzzertifizierung nach Maßgabe der Datenschutz-Grundverordnung, um Kunden mit besonderen Anforderungen die Auswahl von Cloud-Anbietern zu ermöglichen, die hinreichende Garantien zur Einhaltung des Datenschutzes vorweisen können.

Als Testierung ist insbesondere der Kriterienkatalog Cloud Computing C5 des BSI zu nennen, der auf die Sicherheit des Cloud-Dienstes (und nicht allein auf das ISMS des Anbieters) abzielt.

5.5 Zertifikate bei Cloud

Zertifikate werden von einer Zertifizierungsstelle basierend auf dem Bericht eines Auditors ausgestellt. Der Antragsteller stellt einen Antrag auf Zertifizierung bei der Zertifizierungsstelle, ein Auditor bekommt den Prüfauftrag, prüft die jeweiligen Kriterien beim Antragsteller, und erstellt einen Prüfbericht, den eine neutrale (akkreditierte) Zertifizierungsstelle zertifiziert.

Für die Prüfung gibt es für die einzelnen Standards kein festgelegtes Schema, sondern eine Liste von zu erfüllenden Kriterien. Hier ist es aus Sicht des Anwenders der Scope des Zertifikats wichtig, der beschreibt welche Teile des jeweiligen Standards abgedeckt werden, unter welchen Umständen das Zertifikat gilt und welche Standorte des Cloud-Anbieters umfasst sind.

Der Prüfbericht wird für die Zertifizierungsstelle und den Cloud-Anbieter geschrieben, ist aber in der Regel nicht für Kunden zugänglich. Das Zertifikat bestätigt das Ergebnis und sollte wo relevant mit Schutzklassenangabe erfolgen.

Das erstellte Zertifikat gilt für die Zukunft, bis sich das Unternehmen und die Umsetzung des geprüften Systems sich ändert. Das Zertifikat bestätigt damit die Erwartung, dass der Cloud-Anbieter in Zukunft die Aspekte des zertifizierten Standards umsetzt. Zertifizierungen müssen daher in regelmäßigen Abständen erneuert werden, meistens alle 2-3 Jahre.

5.6 Testate bei Cloud

Testate werden vorrangig im Bereich der Wirtschaftsprüfung bspw. nach Prüfungen des ISAE 3000-Standards ausgestellt. Die Prüfungen nach diesen Standards liefern ein umfassendes Bild über die internen Kontrollsysteme der geprüften IT-Systeme und Anwendungen. Die Ergebnisse sind mit den Ergebnissen aus Prüfungen mit ähnlichen Voraussetzungen vergleichbar.

Wegen der hohen Aussagekraft der Testate hat das BSI einen an das Verfahren der Wirtschaftsprüfung angelehnten Kriterienkatalog für Cloud-Dienste (C5) entwickelt, um eine Methodik anzubieten, mit der auch für komplexe Cloud-

Dienste ein umfassender und vergleichbarer Vertrauensnachweis erbracht werden kann. Hierfür wird wie folgt vorgegangen:

Ein Antragsteller (Firma/Anbieter) beantragt eine Prüfung, welche von einem Wirtschaftsprüfer durchgeführt wird. Dieser prüft in einer Typ 1 oder Typ 2 Prüfung, ob die internen Kontrollsysteme der für den geprüften Cloud Service nötigen IT-Systeme und -Prozesse die Sicherheitsziele des C5-Kriterien Katalogs erfüllen. Bei einer Typ 1 Prüfung wird eine Angemessenheitsprüfung durchgeführt. Hierbei wird testiert, dass die Kriterien zu einem Zeitpunkt angemessen umgesetzt waren. Bei der Typ 2 Prüfung wird darüber hinaus eine Wirksamkeitsprüfung durchgeführt, wodurch am Ende testiert wird, dass die Maßnahmen über einen definierten Zeitraum in der Vergangenheit wirksam waren. Da beide Prüfungen Testate über die Vergangenheit ausstellen, wird empfohlen, regelmäßig die Prüfungen zu erneuern, so dass immer ein aktuelles Testat vorliegt.

Bei der Prüfung werden die Kriterien geprüft, die als Sicherheitsziele formuliert sind. Es obliegt hierbei dem Prüfer, zu beurteilen, ob das Kriterium eingehalten ist oder nicht und wie das Sicherheitsziel erreicht ist. Da der Prüfer seine Prüfungshandlungen im Prüfbericht dokumentiert, ist für den Leser dieses Prüfungsurteil weitestgehend nachvollziehbar.

Das Ergebnis der Prüfung ist ein Prüfbericht, der das Informationsbedürfnis des Anwenders über den Sicherheitsstand des Cloud Service befriedigen soll. Der Anwender kann sich über den Prüfbericht über die Eigenschaften des geprüften Gegenstandes informieren und damit entscheiden, ob der Cloud Service für seinen Anwendungszweck geeignet ist. Zusätzliches Vertrauen entsteht dadurch, dass die Aussagen der gesetzlichen Vertreter des Antragstellers zur den Sicherheitseigenschaften Teil des Vertrags werden und somit jeder Verstoß als Vertragsbruch gesehen werden kann. Zusätzlich haftet auch der Prüfer für die Aussagen aus dem Prüfbericht.

6 Glossar

AG	Arbeitsgruppe
BDSG	Bundesdatenschutzgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
CASB	Cloud Access Security Broker
DPA	Data Processing Agreement
FIDO	"Fast IDentity Online" - FIDO Authentication Standard der FIDO Alliance
IaaS	Infrastructure as a Service
ISO	International Organization for Standardization
ITSiG	IT-Sicherheitsgesetz
ITSmiE	IT Security made in EU
ITSmiG	IT Security made in Germany
KMU	Kleine und mittlere Unternehmen
KRITIS	Kritische Infrastrukturen
MFA	Multifaktor-Authentisierung
NIST	National Institute of Standards and Technology
on-premise	in den eigenen Räumlichkeiten, lokal
OTP	One Time Password
PaaS	Platform as a Service
PGP	Pretty Good Privacy
PQC	Post-quantum cryptography
SaaS	Software as a Service
SASE	Secure Access Service Edge
SAML	Security Assertion Markup Language
SCC	Standarddatenschutzklauseln ("Standard Contractual Clauses")
SLA	Service Level Agreement
S/MIME	Secure / Multipurpose Internet Mail Extensions
SSL	Secure Sockets Layer
SSO	Single Sign On
TLS	Transport Layer Security
VPN	Virtual Private Network

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Experten, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Expertenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Vertrauenszeichens "IT Security made in Germany". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Kontakt:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Dr. Holger Mühlbauer
Geschäftsführer
Chausseestraße 17
10115 Berlin
Telefon: +49 30 4005 4306
E-Mail: holger.muehlbauer@teletrust.de
https://www.teletrust.de

TeleTrusT
Pioneers in IT security.