HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

BACHELORARBEIT

Frau
Sandra Lindner

Cloudbackup Server unter Zero Trust – Bedingungen der Konfiguration

Mittweida, 2023

Fakultät Angewandte Computer- und Biowissenschaften

BACHELORARBEIT

Cloudbackup Server unter Zero Trust – Bedingungen der Konfiguration

Autor:
Frau

Sandra Lindner

Studiengang:
Allgemeine und Digitale Forensik

Seminargruppe:
FO19w2-B

Erstprüfer:
Prof. Dr. rer. nat. Dirk Labudde

Zweitprüfer:
B. Sc. Laura Pistorius

Einreichung:
Mittweida, 19.03.2023

Verteidigung/Bewertung:
Mittweida, 2023

Faculty Angewandte Computer- und Biowissen-
schaften

BACHELOR THESIS

Cloudbackup Server at Zero Trust - the conditions of the Configuration

author:
Ms.

Sandra Lindner

course of studies:
Allgemeine und Digitale Forensik

seminar group:
FO19w2-B

first examiner:
Prof. Dr. rer. nat. Dirk Labudde

second examiner:
B. Sc. Laura Pistorius

submission:
Mittweida, 19.03.2023

defence/ evaluation:
Mittweida, 2023

Bibliografische Beschreibung:

Lindner, Sandra:

Cloudbackup Server unter Zero Trust- Bedingungen der Konfiguration

Cloudbackup Server at Zero Trust - the conditions of the Configuration

106 Seiten
Hochschule Mittweida,
Fakultät Angewandte Computer- und Biowissenschaften,
Bachelorarbeit, 2023

Referat:

Das Ziel dieser Arbeit ist es, einen Anforderungskatalog für Anbieter eines Cloudbackup- Servers unter Zero Trust Bedingungen zu erstellen. Dabei werden nicht nur die technischen Voraussetzungen beschrieben, sondern auch ein kurzer Einblick in rechtlichen und organisatorischen Anforderungen gegeben, wobei das Hauptaugenmerk auf den Bestimmungen liegt, die in Deutschland und der EU gelten. Für die Erarbeitung werden dabei bereits existierende Anforderungskataloge und staatliche Veröffentlichungen verglichen und zusammengeführt. So wurde ein Anforderungskatalog erstellt, der alle Anforderungen enthält, die ein Cloudbackup- Server unter Zero Trust erfüllen muss. Der Katalog kann genutzt werden, um ein solches System umzusetzen.

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

A	Anforderung
API	Application Programming Interface
BGB	Bürgerliches Gesetzbuch
BKA	Bundeskriminalamt
BRD	Bundesrepublik Deutschland
BSI	Bundesamt für Sicherheit in der Informationstechnik
C5:2020	Cloud Computing Compliance Criteria Catalogue
CA	Certification Authority
CBC	Cipher Block Chaining
CC	Common Criteria
CDM	Continuous diagnostics and mitigation
CERT	Computer Emergency Response Team
CFB	Cipher Feedback
CPU	Central Processing Unit
CTR	Counter
DAN	Data Acquisition Network
DHKE	Deffie- Hellmann-Schlüsseltausch
DMZ	Demilitarisierte Zone
DNS	Domain Name System
DoS	Denial of Service
DDos	Distributed Denial of Service
DSGVO	Datenschutz-Grundverordnung
EAL	Evaluation Assurance Level
ECB	Electonic Codebook
ECDH	Diffie Hellmann mit elliptischen Kurven

EU	Europäische Union
FW	Firewall
IBN	Intent based Networking
ICAM	Identity, Credential and Access Management
IGP	Identity Governance Programm
IKE	Internet Key Exchange
IPSec	Internet Protocol Security
ISMS	Informationssicherheitsmanagementsystem
ISO/OSI	International Organization for Standardization/ Open Systems Interconnection
IT	Informationstechnologie
IV	Initialisierungsvektor
KRITIS	Kritische Infrastruktur
LAN	Local Area Network
MAC	Message Authentication Code
MCAP	microcore and perimeter
NAP	Network Access Protection
NAV	network analysis and visibility
NEA	Netzersatzanlagen
NIST	National Institute of Standards and Technology
oA	optionale Anforderung
OFB	Output Feedback
OOB	Out-of-Band-Authentisierung
PA	Policy Administrator
PDP	Policy Decisioin Point
PE	Policy Engine
PEP	Policy Enforcement Point
PKI	Public Key Infrastructure
RL	Risikolevel

RPO	Recovery Point Objective
RSA	Rivest- Shamir-Adleman
RTO	Recovery Time Objective
SDN	Software- defined- Networking
SDP	Software Defined Perimeter
SEM	Security Event Management
SG	Segmentation Gateway
SIEM	Security Information and Event Management
SIM	Security Infomation Management
SNMP	Simple Network Management Network
SOG-IS	Senior Officials Group Information Systems Security
SSH	Secure Shell
StGB	Strafgesetzbuch
TCP	Transmission Control Protocol
TKG	Telekommunikationsgesetz
TLS	Transport Layer Security
TMG	Telemediengesetz
TR	Technische Richtlinie
USB	Universal Serial Bus
USV	Unterbrechungsfreie Stromversorgung
WAN	Wide Area Network
XOR	Exklusives Oder
ZT	Zero Trust

1 Einleitung

Heute werden immer mehr wichtige Informationen in digitaler Form gespeichert und verarbeitet. Dabei spielt es keine Rolle, ob es sich um private Fotos, digitale Verträge, E-Mails oder um andere wichtige Daten handelt. Gleichzeitig sind diese Daten aber auch der ständigen Gefahr von Angriffen ausgesetzt.

So verzeichnet das Bundeskriminalamt (BKA) im Bereich der Cyberstraftaten 2021 einen weiteren Anstieg um 12 %. Dabei führt das BKA insbesondere sogenannte Ransomware als die Bedrohung mit dem höchsten Schadenspotential an und bezeichnet das Jahr 2021 auch als „das Jahr der Ransomware“. So ist der Schaden, der durch den Einsatz von Ransomware entstanden ist, von ca. 5,3 Mrd. Euro im Jahr 2019 auf ca. 24,3 Mrd. Euro gestiegen. Beim Einsatz von Ransomware werden mit Hilfe einer Schadsoftware die Daten eines Systems verschlüsselt und/oder die normale Nutzung der PCs unterbunden und eine Lösegeldforderung gestellt. Aber es entstehen durch den Einsatz von Ransomware nicht nur monetäre Schäden. Auch die Abläufe in betroffenen Firmen, Verwaltungen und Institutionen werden durch solche Angriffe empfindlich gestört. [1]

Um sich vor Datenverlust durch solche Angriffe zu schützen, fertigen Unternehmen Backups an. Diese werden jedoch häufig auch von der Schadsoftware erfasst und gleichzeitig mit verschlüsselt. Daran wird deutlich, dass diese Strategien oft nicht den gewünschten Schutz vor den Angriffen bieten. Es stellt sich also die Frage, welche Anforderungen eine Backupstrategie erfüllen muss, damit die Daten vor dem Verlust geschützt werden können.

1.1 Ziel der Arbeit

Das Ziel dieser Arbeit ist es, einen Anforderungskatalog für eine Backupstrategie aufzustellen, die auf der Grundlage eines Cloudbackup Systems funktioniert, das einen Zero Trust Ansatz nutzt. Dabei liegt das Hauptaugenmerk auf den zu erfüllenden technischen Anforderungen, die ein Anbieter eines solchen Backupsystems zu erfüllen hat. Es wird jedoch auch auf gesetzliche Regelungen zu diesem Thema kurz eingegangen.

Als Grundlage des erarbeiteten Anforderungskatalogs werden dabei unterschiedliche Anforderungskataloge von verschiedenen Organisationen und Institutionen genutzt.

1.2 Aufbau der Arbeit

Im Kapitel 2 dieser Arbeit werden die relevanten Grundlagen zu der Fragestellung erläutert. Unter anderem wird Grundlegendes zur IT-Sicherheit, zur Kryptologie, zu verteilten Systemen und zur Datensicherung beschrieben. In Kapitel 3 wird dann ein erster Anforderungskatalog aus der Theorie entworfen. Dieser wird danach in Kapitel 4 mit Hilfe von Richtlinien und Veröffentlichungen staatlicher Stellen überprüft und es wird ein vollständiger Anforderungskatalog für einen Cloudbackup Server unter Zero- Trust erstellt. In Kapitel 5 wird schließlich das Ergebnis dieser Arbeit zusammengefasst und ein Ausblick gegeben.

2 Grundlagen

Bevor in den nachfolgenden Kapiteln auf die Anforderungen, die an die Konfiguration von Cloudbackup Servern gestellt werden, eingegangen wird, sollen hier die wichtigsten Grundbegriffe näher erläutert werden.

2.1 IT- Sicherheit

Ganz gleich, ob es sich um private Fotos, Geschäftsdokumente oder Daten von Onlinebanking handelt, der Schutz unserer privaten und geschäftlichen Informationen spielt eine bedeutende Rolle in unseren modernen Zeiten. Doch was bedeutet eigentlich Informationssicherheit und welcher Zusammenhang besteht zwischen diesem Begriff und den Begriffen IT-Sicherheit und Cybersicherheit? Was muss eigentlich geschützt werden? Welchen Wert haben Informationen und wie hängt dies mit dem Unternehmenswert zusammen?

2.1.1 Sicherheit

Zu Beginn soll der Begriff der **Sicherheit** betrachtet werden. Was macht Sicherheit aus? Der Duden beschreibt Sicherheit als „Zustand des Sicherseins, [des] Geschütztseins vor Gefahr oder Schaden; [oder auch als] höchstmögliches Freisein von Gefährdungen“. [2]

Der Begriff der Sicherheit ist also ein sehr allgemeiner Begriff, der an sich nicht beschreibt, was geschützt werden soll und wovor. Aus diesem Grund muss er immer in einem entsprechenden Kontext betrachtet werden, um einen praktischen Nutzen zu haben.

2.1.1.1 Informationssicherheit und IT-Sicherheit

Die **Informationssicherheit** beschäftigt sich mit dem Schutz von Informationen unabhängig von ihrer Art und Herkunft. Es spielt dabei keine Rolle, ob diese in Papierform, nur gedanklich, als Wissen von natürlichen Personen, oder in Rechnersystemen gespeichert sind. Das heißt, dass nur autorisierte Personen auf die Informationen zugreifen und sie verändern können. Die Informationssicherheit wird in der Fachliteratur auch als security bezeichnet. [3, S. 8], [4, S. 6]

Die **IT-Sicherheit** ist das Teilgebiet der Informationssicherheit, das sich mit dem Schutz der Informationen, die auf elektronischen Systemen in Form von Daten gespeichert sind, beschäftigt.

Neben dem Schutz der Informationen beinhaltet die IT- Sicherheit auch den Schutz der Systeme, die für die Verarbeitung der Informationen genutzt werden. Dies wird auch als

Funktionssicherheit (engl. safety) bezeichnet. Dabei müssen die Ist- und Soll-Funktionalität übereinstimmen, das heißt „…, dass es unter allen (normalen) Betriebsbedingungen funktioniert.“ [4, S. 6] Durch IT-Sicherheit wird es einem Anwender also ermöglicht, elektronische Systeme trotz Risiken zur Informationsverarbeitung zu nutzen. [4, S. 6], [5, S. 16]

Doch was versteckt sich nun hinter dem so oft verwendeten Begriff der **Cyber-Sicherheit**? Dieser Begriff wird vor allem dann genutzt, wenn man hervorheben möchte, dass IT-Sicherheit auch in den heute hochgradig vernetzten und über das Internet erreichbaren IT-Systemen greifen muss. [5, S. 16]

2.1.1.2 Differenzierung von Datensicherheit und Datenschutz

Datensicherheit (engl. protection) bedeutet, dass unberechtigte Zugriffe auf Systemressourcen und Daten verhindert werden. Das heißt auch, dass Daten gesichert und vor Verlust geschützt werden müssen. Dies geschieht z. B. durch Backups, bei denen Sicherheitskopien erstellt werden. [4, S. 6]

Häufig werden im allgemeinen Sprachgebrauch Datensicherheit und Datenschutz synonym verwendet, was aber nicht korrekt ist. **Datenschutz** bezieht sich ausschließlich auf den Schutz personenbezogener Daten. Personenbezogene Daten sind „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person […] beziehen“. [6, Art. 4 Abs. 1] Datenschutz beschreibt das Recht der Person über die Weitergabe, die Verarbeitung und Löschung von Informationen, die sie selbst betreffen, zu bestimmen und ist gesetzlich geregelt. Der Datenschutz bezieht sich auf alle Informationen, die zu einer Person existieren, gleich in welcher Form und muss daher stets auch im Rahmen der IT- Sicherheit beachtet werden. [5, S. 36]

2.1.2 Schutzziele

Nachdem nun geklärt wurde, was sich hinter den unterschiedlichen Sicherheitsbegriffen verbirgt, sollen nun die Anforderungen, die ein System erfüllen muss, um als sicher zu gelten, näher beleuchtet werden. Diese Anforderungen werden auch als **Schutzziele** (engl. security objective) bezeichnet. Es werden dabei fünf Schutzziele genannt. Diese sind: Vertraulichkeit (engl. confidentiality), Integrität (engl. intergrity), Authentizität (engl. authenticity), Verfügbarkeit (engl. availability) und Verbindlichkeit (engl. non repudiation). Manchmal wird diese auch als Verantwortlichkeit (engl. accountability) bezeichnet. [4, S. 7-15], [5, S. 16]

Die **Vertraulichkeit** einer Information ist gewährleistet, wenn es unautorisierten Personen oder Systemen nicht möglich ist, auf diese zuzugreifen. Dies kann zum Beispiel durch die Beschränkung von Auffindbarkeit, Lesbarkeit und Zugriff gewährleistet werden. Maßnahmen um dies durchzuführen wären unter anderem Zugriffskontrollen, Verschlüsselungen und Steganographie. Es gilt dabei auch zu beachten, dass die verlorene Vertraulichkeit

einer Information nicht wiederherstellbar ist. Dadurch müssen alle Maßnahmen, die zum Schutz der Vertraulichkeit dienen, vor einem Verlust dieser getroffen werden. [5, S. 11]

Wenn von der **Integrität** von Systemen oder Daten die Rede ist, beschreibt dies, dass es nicht möglich sein darf, die Systeme oder Daten unbemerkt und/oder unautorisiert zu verändern. Die Integrität kann zum Beispiel durch das Festlegen von Lese- und Schreibberechtigungen für Dateien geschützt werden. Dass die Integrität verletzt wurde, kann zum Beispiel durch das Vergleichen erkannt werden. [5, S. 11], [4, S. 9]

Ein weiteres wichtiges Schutzziel ist die **Authentizität**. Informationen sind authentisch, also echt und glaubwürdig, wenn ihr Ursprung eindeutig verifizierbar ist. Durch Authentifizierung kann die Echtheit des Kommunikationspartners überprüft werden. Die Authentizität von Personen kann beispielsweise durch Passwörter, biometrische Merkmale (z.B. Iris- oder Fingerabdruckscan, Gesichtserkennung), Chipkarte oder Personalausweis erfolgen. Die Authentizität technischer Systeme wird in der Praxis durch kryptographische Verfahren überprüft. [5, S. 11], [4, S. 8f.]

Die **Verfügbarkeit** einer Information, eines Systems oder Dienstes ist genau dann gewährleistet, wenn ein berechtigter Nutzer oder ein berechtigtes System auf sie jederzeit im Rahmen seiner Rechte zugreifen kann. Die Verfügbarkeit eines Systems kann zum Beispiel durch Redundanzen und Maßnahmen der Netzwerksicherheit zum Verhindern von Angriffen auf die Verfügbarkeit durch DoS (Denial of Service)-Angriffe sichergestellt werden. [5, S. 11], [4, S. 12]

Die **Verbindlichkeit** oder auch **Verantwortlichkeit** ist dann gegeben, wenn Handlungen einem identifizierbaren Nutzer oder System eindeutig und unbestreitbar zugeordnet werden können. Dies kann zum Beispiel durch das Erstellen von Änderungs- und Zugriffsprotokollen gewährleistet werden. [5, S. 11f.], [4, S. 12ff.]

Wie schon aus den Beschreibungen der einzelnen Schutzziele hervorgeht, können diese auch voneinander abhängig sein bzw. können sie auch Voraussetzung zur Erfüllung anderer Schutzziele sein. Die Authentizität und Verbindlichkeit von Daten sind zum Beispiel nur dann möglich, wenn auch deren Integrität gewährleistet ist, da die Daten ansonsten unbemerkt manipuliert werden können. Vertraulichkeit erfordert manchmal Zugriffsregeln, auf Basis derer entschieden wird, welche Benutzer vertrauliche Informationen einsehen dürfen. Für die Zugriffsregeln ist wiederum die Authentizität des Benutzers notwendig, da ansonsten nicht gewährleistet werden kann, dass es sich nicht um eine andere Person handelt.

2.1.3 Der Wert von Informationen

Wie bereits in Kapitel 2.1.1.1 beschrieben wurde, versucht man mit Hilfe der IT-Sicherheit Informationen, die auf elektronischen Systemen gespeichert sind, zu schützen. Da diese für Unternehmen und Organisationen wichtig für ihren Erfolg sind, spricht man auch von einem Informationswert. Zu diesen **Informationswerten** gehören zum Beispiel

Kundendaten. Neben den Informationswerten gibt es auch noch weitere **Unternehmenswerte**. Zu diesen gehören nach BSI-Standard unter anderem IT-Systeme und Geschäftsprozesse. Um deren Funktionsweise zu gewährleisten, ist es notwendig, eine entsprechende IT-Infrastruktur seitens des Unternehmens bereitzustellen. Da das mit Kosten und personellen Ressourcen verbunden ist, stellt dies einen Wert für das Unternehmen dar, der geschützt werden muss. Der Unternehmenswert und der Informationswert werden auch unter dem Begriff **Wert** (engl. assets) zusammengefasst. [4, S. 17], [5, S. 10f.], [7, S. 10]

2.1.4 Bedrohungs- und Risikoanalyse, Risikomanagement und Sicherheitskategorien

Selbstverständlich hat jeder Eigentümer ein großes Interesse daran, dass die Werte, die er besitzt, erhalten bleiben. Um dies erreichen zu können ist es jedoch notwendig herauszufinden, wo es Probleme für die Sicherheit dieser Informationen gibt. Dies muss noch vor dem Eintritt eines Schadens geschehen. Das heißt, dass eine „vorsorgliche Analyse“ durchgeführt werden muss, um zielgerichtet Schaden abwenden zu können. [5, S. 12]

Es findet also eine vorsorgliche Analyse der Bedrohungen statt, die die Werte des Systems bedrohen. Unter **Bedrohungen** (engl. threat) versteht man dabei Szenarien oder Umstände, die ein absehbares Potenzial aufweisen, das zu einer Verletzung der Sicherheitsrichtlinien (engl. security policy) führt. Dabei richtet sich eine Bedrohung immer gegen einen Wert. Es kommt jedoch nur zu einem Schaden (engl. impact), wenn es eine Schwachstelle (engl. vulnerability) gibt, die von der Bedrohung ausgenutzt werden kann. Man bezeichnet diese Analyse auch als **Bedrohungsanalyse**. [5, S. 12f.]

Wenn es zum Aufeinandertreffen von Bedrohung und Schwachstelle kommt und das mit einer bestimmten Wahrscheinlichkeit ausgenutzt werden kann und so eine Beeinträchtigung des Werts erzeugt wird, wird auch von einem **Risiko** (engl. risk) gesprochen, dem der Wert ausgesetzt ist. Die Wahrscheinlichkeit für das Ausnutzen eines Risikos wird bei der **Risikoanalyse** abgeschätzt und der mögliche Schaden beziffert. So wird es möglich, auf Grundlage dieser Analyse Entscheidungen zu treffen und weitere Maßnahmen abzuleiten. Um Risiken vergleichbar zu machen, wird dabei meist auch der mögliche Schadenswert bestimmt. Dieser wird genutzt um bei der Risikobehandlung Prioritäten setzen zu können. Um das Risiko zu bestimmen, wird dabei meist das Produkt aus Eintrittswahrscheinlichkeit und Schaden gebildet. [5, S. 12ff.]

Diese Größe spielt eine große Rolle im **Risikomanagement**. Das Risikomanagement umfasst dabei alle Maßnahmen, die mit dem Umgang mit Risiken zu tun haben. Das heißt, dass sowohl die Identifikation, deren Bewertung bzw. Abschätzung sowie deren Behandlung und Kommunikation, als auch deren Überwachung und Überprüfung dazugehören. [5, S. 14]

> *„Die **Risikoidentifikation** verbindet [dabei] Bedrohungen mit Werten und betrachtet existierende Sicherheitsmaßnahmen und sucht nach Schwachstellen. Die Suche nach Schwachstellen bildet den Kern in dieser Analyse von Szenarien der Nutzung bzw. des Missbrauchs der IT.“ [5, S. 14]*

Für die **Risikobehandlung** (engl. risk treatment) gibt es die folgenden vier Möglichkeiten:

1. **Risikoakzeptanz** (engl. risk retention oder risk acceptance): Bei dieser Möglichkeit wird das vorhandene Risiko akzeptiert und es werden keine Maßnahmen dagegen eingeleitet. Bis zu welcher Höhe man das Risiko akzeptiert, kann dabei unterschiedlich sein. Man bezeichnet dies auch als Risikoappetit (engl. risk appetite). [5, S. 15]
2. **Risikominderung** (engl. risk reduction): Dies erreicht man, indem man Sicherheitsmaßnahmen implementiert und verbessert, um Schwachstellen zu beseitigen. Jedoch bleibt dabei ein Restrisiko (engl. residual risk). Falls dieses akzeptiert werden kann, wird nicht weiter an Verbesserungen gearbeitet. [5, S. 15]
3. **Risikoübertragung** (engl. risk transfer): Dies überträgt das Schadensrisiko auf eine dritte Partei, zum Beispiel ist dies bei Versicherungen so. [5, S. 15]
4. **Risikovermeidung** (engl. risk avoidance): Diese Möglichkeit sieht vor, dass, wenn die Risikominderung zu teuer oder nicht möglich ist, die Architektur so verändert wird, dass das Risiko nicht mehr oder nur vermindert auftritt. [5, S. 15]

Damit das Risiko für eine Organisation besser abgeschätzt werden kann, können sogenannte **Sicherheitskategorien** (engl. security category) genutzt werden. Diese verbinden einen möglichen Schaden mit den Sicherheitszielen Vertraulichkeit, Integrität und Verfügbarkeit und ermöglichen so eine vergleichbare Einschätzung. [5, S. 16]

Das NIST (National Institute of Standards and Technology) [8] beschreibt zur Messung von möglichen Schäden vier Risikolevel (engl. risk level) (RL): Niedrig (low), mittel (moderate), hoch (high) und nicht anwendbar (engl. not applicable). Aus diesen Kategorien und den genannten Sicherheitszielen wird dann der folgende Vektor gebildet:

$Sicherheitskategorie = [(Vertraulichkeit, RL), (Integrität, RL), (Verfügbarkeit, RL)]$ [8, S. 7]

Aus den Erkenntnissen der Analyse und den Maßnahmen zur Risikobehandlung können nun Sicherheitsmaßnahmen entwickelt oder bereits existierende genutzt werden. Dafür gibt es nach von Faber zwei Möglichkeiten. [5, S. 17]

Die erste Möglichkeit ist ein risikobasierter Ansatz. Ziel dieses Ansatzes ist es ein Sicherheitskonzept zu erarbeiten, das zur Verbesserung sowie Absicherung eines bestehenden Systems dient. Dafür wird eine Risiko- und Bedrohungsanalyse durchgeführt, die sich an

den Wegen der Informationsübertragung im System orientiert und dort Schwachstellen und Risiken ermittelt und in Abwägung mit den entstehenden Kosten behebt, reduziert, überträgt oder akzeptiert. Dieser Prozess ist in der Praxis meist sehr komplex. [5, S. 17]

Aus diesem Grund wird in der Praxis auch ein anderer Ansatz genutzt. Dabei erfolgt eine Analyse der Einsatzumgebung mit allen möglichen Bedrohungen. Danach wird definiert, welche der Sicherheitsziele angestrebt werden. Auf dieser Grundlage werden dann die Sicherheitsanforderungen bestimmt und konkrete Sicherheitsmaßnahmen abgeleitet. [5, S. 17f.]

2.2 Verschlüsselung

Nachdem nun die Grundlagen der IT-Sicherheit geklärt wurden, soll es nun um ein Thema gehen, dass einen wichtigen Beitrag zur Sicherheit von IT-Systemen leistet – die Verschlüsselungstechnik. Dabei soll ein Einblick in die wesentlichen Aspekte des Schlüsselmanagements geliefert werden. Weiterhin wird auf Signaturen und ihren Zusammenhang mit Hashfunktionen eingegangen. Darüber hinaus soll natürlich auch aufgezeigt werden, wie man mit Hilfe dieser Verfahren Kommunikationsverbindungen absichern kann.

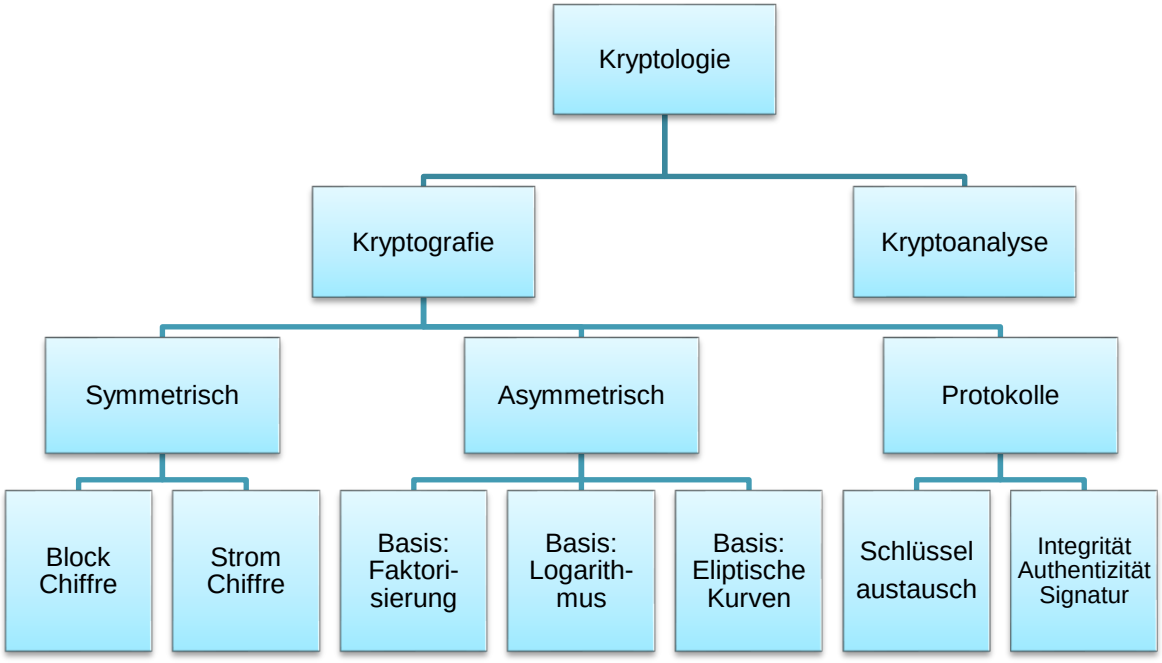

Abbildung 1 Taxonomie kryptografischer Verfahren nach [4], [5], [9], [10]

2.2.1 Überblick Kryptologie

Sobald man sich mit der Ver- und Entschlüsselung von Nachrichten oder Verbindungen auseinandersetzt, trifft man auf die drei Begriffe Kryptografie, Kryptoanalyse und Kryptologie. Diese sollen zu Beginn eingeordnet werden.

Der Duden definiert die **Kryptografie** als „Teilgebiet der Informatik, das sich mit der Entwicklung und Bewertung von Verfahren der Verschlüsselung geheimer Daten befasst“. [11] Die Kryptografie ist also die Wissenschaft, die sich mit Methoden zum Ver- und Entschlüsseln von Informationen und Kommunikationen beschäftigt, um diese vor unberechtigtem Zugriff zu schützen. Bei diesen zumeist mathematischen Methoden wird generell ein sogenannter Schlüssel verwendet, um die Nachricht zu verschlüsseln. Da bei der Kryptografie vor allem die Vertraulichkeit, Authentizität, Integrität und Verbindlichkeit geschützt wird, ist es mit ihr möglich, auch in elektronischer Form nachprüfbar Übereinkünfte zu schließen. [4, S. 279], [5, S. 217]

Die **Kryptoanalyse** hingegen beschäftigt sie damit, die verschlüsselten Informationen ohne Kenntnis des Schlüssels wieder lesbar zu machen. Sie beschäftigt sich also mit analytischen und praktischen Verfahren, die dazu genutzt werden können, Verschlüsselungsalgorithmen zu brechen. Aus diesem Grund besteht in der Praxis ein enger Zusammenhang zwischen Kryptografie und Kryptoanalyse, da nur mit Hilfe der Kryptoanalyse sichere Verschlüsselungsverfahren gefunden werden können. Die Verbindung der beiden Teilgebiete Kryptografie und Kryptoanalyse wird auch **Kryptologie** genannt. [4, S. 279], [5, S. 217]

Die kryptografischen **Protokolle** sind Verfahren, die der Steuerung des Ablaufes von Transaktionen für spezifische Anwendungen dienen. [9, S. 24]

Neben der Verschlüsselung von Nachrichten können Informationen auch geschützt werden, indem man verhindert, dass unberechtigte Personen Kenntnis über deren Existenz erlangen. Diese Wissenschaft wird als **Steganografie** bezeichnet und leitet sich von den griechischen Wörtern stegano, was so viel wie geheim bedeutet, und graphein, dem Wort für schreiben, ab. [5, S. 217], [4, S. 279]

2.2.2 Sicherheit von kryptografischen Verfahren

Das **Kerckoffs`sche Prinzip** ist bis heute eines der zentralen Gesetze der Kryptografie, obwohl es bereits 1883 von dem niederländischen Kryptografen Auguste Kerckoffs formuliert wurde. Es besagt, dass ein kryptografisches Verfahren seine Sicherheit nur auf Basis der Geheimhaltung des Schlüssels erhalten darf, nicht jedoch auf der Basis der Geheimhaltung des Verfahrens (kryptografischer Algorithmus). [10, S. 12]

Nach Ertel und Löhmann [9] gilt ein Algorithmus zur Verschlüsselung dann als sicher, wenn er eine der drei folgenden Bedingungen erfüllt: *„*

- *der zum Aufbrechen nötige Geldaufwand den Wert der verschlüsselten Daten übersteigt oder*
- *die zum Knacken erforderliche Zeit größer ist als die Zeit, die die Daten geheim bleiben müssen, oder*
- *das mit einem bestimmten Schlüssel chiffrierte Datenvolumen kleiner ist als die zum Knacken erforderliche Datenmenge.“ [9, S. 27]*

Als **uneingeschränkt sicher** sehen Ertel und Löhmann einen Algorithmus erst dann, wenn selbst bei uneingeschränkt zur Verfügung stehenden verschlüsselten Daten, nicht auf einen Klartext geschlossen werden kann. Eckert bezeichnet eine nach Ertel und Löhmann **sichere** Verbindung auch als **praktisch sicher** und eine **uneingeschränkt sichere** Verbindung als **absolut sicher**. [9, S. 27], [4, S. 296]

Weiterhin wird als wichtiges Kriterium für die Sicherheit kryptografischer Verfahren auf die Größe des Schlüsselraums verwiesen. Dabei gilt: Je größer der Schlüsselraum ist, desto höher ist der Aufwand, der betrieben werden muss, um einen Schlüssel für eine verschlüsselte Botschaft zu erraten. Das heißt, der Schlüsselraum muss für ein sicheres kryptografisches Verfahren so groß sein, dass es sich für einen Angreifer nicht lohnt oder er nicht in der Lage ist, diesen Aufwand zu betreiben um den Schlüssel zu erraten. [9, S. 27ff.]

Für die Länge eines Schlüssels, die notwendig ist, damit dieser Aufwand zu groß wird, werden weltweit von verschiedenen Institutionen und Organisationen Richtlinien oder Empfehlungen herausgeben; so auch vom Bundesamt für Sicherheit in der Informationstechnik (BSI). Dieses veröffentlicht eine Richtlinie, die unter anderem für verschiedene Verschlüsselungsverfahren Schlüssellängen vorschlägt. [12] Die Bundesnetzagentur verweist außerdem auf den SOG-IS (Senior Officials Group Information Systems Security) - Kryptokatalog. Dieser enthält neben empfohlenen Schlüssellängen auch Vereinbarungen, welche kryptografischen Verfahren für EU (Europäische Union)- Regierungsorganisationen als sicher gelten und damit EU-weit zum Austausch genutzt werden können. [13], [14] Neben diesen europäischen Organisationen gibt es auch noch eine Vielzahl weiterer Organisationen, die Empfehlungen herausgeben, darunter zum Beispiel auch das US-amerikanische

NIST(National Institute of Standards and Technology). Auf BlueKrypt findet sich eine Gegenüberstellung der Empfehlungen unterschiedlicher Organisationen. [15]

2.2.3 Symmetrische Verschlüsselung

Nach der Einordnung der wichtigsten Begriffe der Kryptografie sollen nun auf die Grundlagen der ersten großen Gruppe von kryptografischen Algorithmen eingegangen werden.

2.2.3.1 Konzept der symmetrischen Verschlüsselung

Als symmetrische Verschlüsselungsverfahren werden alle kryptografischen Algorithmen bezeichnet, die für die Ver- und Entschlüsselung denselben geheimen Schlüssel verwenden. Das heißt, dass sowohl dem Sender als auch dem Empfänger der Nachricht der Schlüssel bekannt sein muss, damit diese in der Lage sind zu kommunizieren (siehe auch Abbildung 2). Dies bedeutet aber auch, dass die Sicherheit der symmetrischen Verschlüsselungsverfahren nicht nur von der Länge des Schlüssels und der Stärke des Verfahrens abhängt, sondern auch davon, dass der Schlüssel sicher übertragen und bei beiden Teilnehmern sicher gespeichert wird. [5, S. 218f.], [4, S. 288f.]

2.2.3.2 Arten symmetrischer Verschlüsselung

Es gibt zwei Arten symmetrischer Verschlüsselungsverfahren, die Strom- und die Blockchiffren (siehe auch Abbildung 1). Die **Stromchiffren** nutzen zur Verschlüsselung einer Klartextbitfolge eine Folge von Schlüsselbits. Zu den Stromchiffren gehört auch das sogenannte **One-time-pad**. Dieses bereits 1917 erfundene Verfahren ist absolut sicher, da der Klartext mit einer genauso langen Folge von echten Zufallsbits verschlüsselt wird. Dadurch ist es nicht möglich, aus einem beliebig langen verschlüsselten Text den Klartext zu rekonstruieren. In der Praxis ergeben sich jedoch einige Herausforderungen bei der Umsetzung des Algorithmus. So ist es nicht möglich, echte Zufallszahlengeneratoren auf Computern zu programmieren und selbst wenn echte Zufallszahlen genutzt werden könnten, so müsste die Schlüsselfolge sowohl auf dem Ziel- als auch auf dem Quellrechner gespeichert werden. Auch der Austausch der Schlüssel stellt ein Problem dar. [9, S. 52-55] Aus diesem Grund werden die Schlüsselbits oder auch der Schlüsselstrom der Stromchiffren in der Praxis meist mit Hilfe eines Pseudozufallszahlengenerators erzeugt. Dieser wird mit einem Initialwert initialisiert und erzeugt dann deterministisch eine Schlüsselbitfolge, die jedoch die Eigenschaften einer echten Zufallsfolge erfüllt. Die Klartextbitfolge wird dann mit der Schlüsselbitfolge addiert und Modulo 2 gerechnet bzw. XOR (Exklusives Oder) verknüpft. Dies ist die eigentliche Verschlüsselungsfunktion. Damit eine Entschlüsselung beim Kommunikationspartner stattfinden kann, muss dann nur von beiden derselbe Pseudozufallszahlengenerator genutzt und der Initialwert übertragen werden. Stromchiffren werden häufig dann verwendet, wenn die Daten noch nicht vollständig vorliegen oder man nicht auf bestimmte Daten warten kann. So werden die Algorithmen zum Beispiel bei der Verschlüsselung von Übertragungen von Telekommunikationsdaten und Videodaten eingesetzt. [4, S. 302-307]

Bei den **Blockchiffren** wird der Klartext in Blöcke einer festen Länge geteilt. Die Länge eines solchen Blocks, auch Blockgröße genannt, sind üblicherweise binäre Potenzen. In der Praxis liegt die Blockgröße meist zwischen 64 Bit und 256 Bit. Da es passieren kann, dass der letzte Block des Klartextes nicht voll ist, wird dieser mit einem Füllmuster aufgefüllt. Dies wird auch als Padding bezeichnet. Nachdem der Klartext in die Blöcke aufgeteilt wurde, wird jeder Block einzeln mit einem Schlüssel verschlüsselt. Dies wird auch als **ECB-Modus** (Electronic Codebook Mode) bezeichnet. So erhält man einzelne verschlüsselte Blöcke. Beim ECB- Modus müssen diese auch zur Entschlüsselung einzeln betrachtet werden. [4, S. 302-307]

Eine weitere Möglichkeit, die Blöcke zu verschlüsseln, ist die verkettete Verschlüsselung, in der jeder neue Block mit dem bereits verschlüsselten Block per XOR verknüpft wird. Dies wird auch als **CBC-Modus** bezeichnet (Cipher Block Chaining Mode). Da bei dem ersten Block noch keine anderen Blöcke zum Verknüpfen vorliegen, wird beim CBC-Modus der erste Block mit einem IV (Initialisierungsvektor) verknüpft. Beim CBC- Modus müssen die Blöcke zur Entschlüsselung gemeinsam betrachtet werden. Solche Algorithmen werden hauptsächlich in Fällen eingesetzt, in denen die Daten schon vor Beginn der Verschlüsselung vollständig vorliegen; so zum Beispiel bei der Verschlüsselung von Festplatten. ECB- und CBC- Modus werden auch als **Betriebsmodi** von Blockchiffren bezeichnet. [4, S. 302-307] Neben den beiden bereits beschriebenen Betriebsmodi für Blockchiffren gibt es auch noch weitere. Diese sind der OFB-Modus (Output Feedback-Modus), der CFB-Modus (Cipher Feedback-Modus) und der CTR-Modus (Counter Modus). Diese ermöglichen es, Blockverschlüsselung auch als Stromverschlüsselung einzusetzen. Die Funktionsweise des OFB- und des CFB-Modus sind recht ähnlich und unterscheiden sich nur durch die Art, wie die Eingabeblöcke erzeugt werden. [4, S. 311ff.] Ein Modus, der bereits 1979 von Diffie und Hellmann entwickelt wurde, gewinnt heute immer mehr an Bedeutung – der **CTR-Modus**. Die Grundidee dieses Modus ist es, den Klartext in Blöcke mit einer bestimmten Länge n in Bit aufzuteilen. Danach wird jeder dieser Blöcke in zwei Phasen verschlüsselt. Zuerst wird eine Zufallszahl, auch Nonce, mit einem n-Bit langen Zählerwert, auch Ctr, XOR verknüpft. Dies ist dann die Eingabe für die Blockchiffre und wird mit einem geheimen Schlüssel verschlüsselt. Danach wird das Ergebnis mit dem Klartext XOR verknüpft. Der Ctr startet dabei mit einem beliebigen Wert und wird bei jedem Klartextblock verändert, zum Beispiel durch Hochzählen. [4, S. 313ff.]

2.2.4 Asymmetrische Verschlüsselung

Die zweite große Gruppe der Verschlüsselungsalgorithmen sind asymmetrische Verschlüsselungsverfahren.

2.2.4.1 Konzept der asymmetrischen Verschlüsselung

Im Gegensatz zu den symmetrischen Verschlüsselungsverfahren arbeitet die asymmetrische Verschlüsselung mit zwei Schlüsseln.

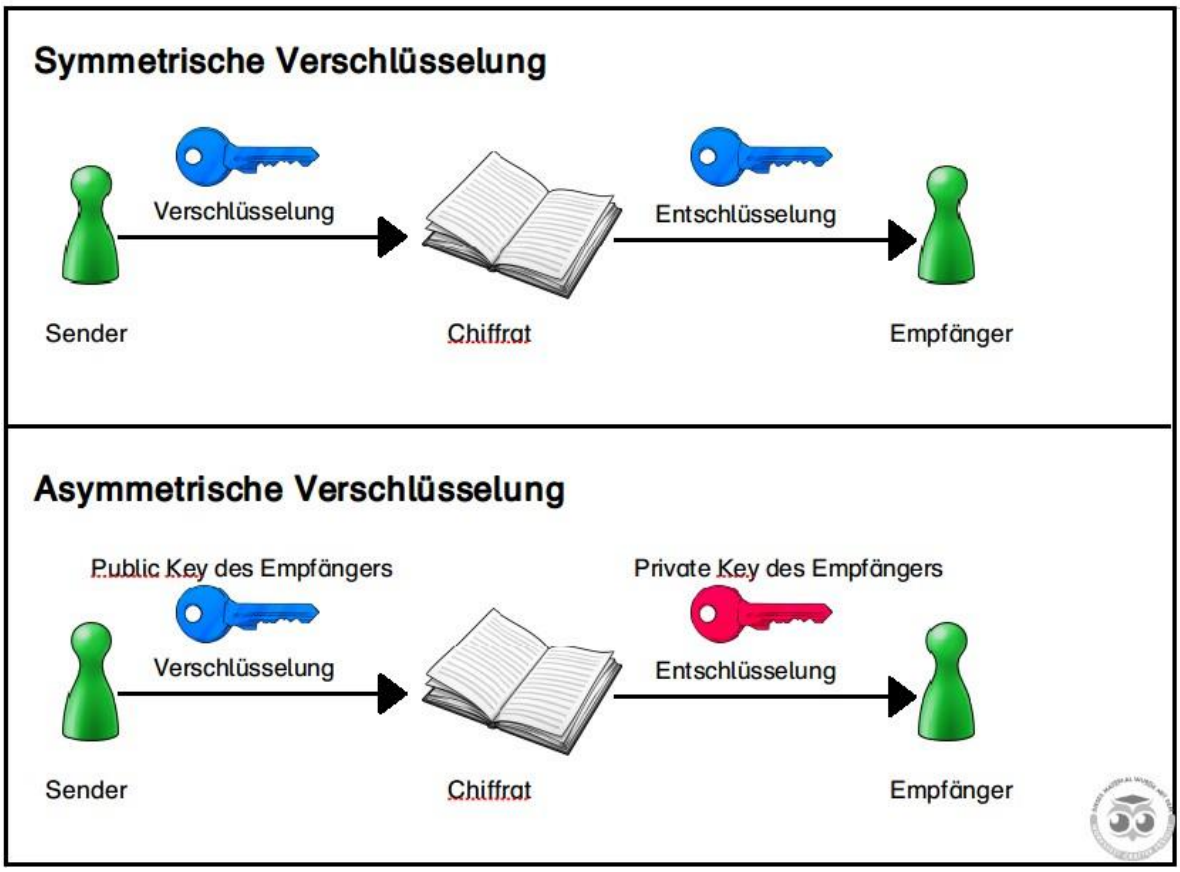

Abbildung 2 Symmetrische und Asymmetrische Verschlüsselung

Die asymmetrische Verschlüsselung wird auch als Public-Key-Kryptografie bezeichnet. Das Grundprinzip ist dabei, dass der Schlüssel, der zur Verschlüsselung einer Botschaft gebraucht wird, nicht geheim gehalten wird- im Gegenteil, er soll frei für alle zur Verfügung stehen. Aus diesem Grund wird er auch als Public Key bezeichnet. Der Public Key wird genau wie der Private Key vom späteren Empfänger erzeugt. Der Private Key darf im Gegensatz zum Public Key unter keinen Umständen veröffentlicht werden, da es sonst jedem möglich wäre, die verschlüsselten Klartexte zu dechiffrieren (siehe Abbildung 2). Die Algorithmen bauen dabei auf sogenannten Einwegfunktionen auf. Diese sind Funktionen f(x) = y, bei denen y leicht berechnet werden kann, die Umkehr aber so schwierig zu berechnen ist, dass es technisch unmöglich ist. [10, S. 178ff.]

2.2.4.2 Arten asymmetrischer Verschlüsselung

Die Arten der asymmetrischen Verschlüsselung sind durch die Arten der Einwegfunktionen, die als Basis genutzt werden, bestimmt. Die beiden am weitesten verbreiteten sind dabei die Faktorisierung und der Logarithmus. Sie beruhen auf dem Faktorisierungsproblem ganzer Zahlen (z. B. RSA [Rivest- Shamir- Adleman]) bzw. auf dem diskreten Logarithmusproblem (z. B. ElGamal). Nicht ganz so weit verbreitetet sind asymmetrische Verfahren, die auf der Grundlage von elliptischen Kurven basieren. Sie nutzen dabei Operationen mit Punktepaaren auf bestimmten elliptischen Kurven. Ein Beispiel wäre das ECDH (Diffie Hellmann mit elliptischen Kurven). [10, S. 173-180]

2.2.5 Protokolle

In diesem Abschnitt soll auf kryptografische Protokolle eingegangen werden, die nicht zu den asymmetrischen und symmetrischen Verfahren gehören. Es soll vielmehr der Austausch von Schlüsseln beschrieben und dargestellt werden und wie deren Authentizität gewährleistet werden kann. (siehe auch Abbildung 1)

2.2.5.1 Schlüsselaustausch

Wie bereits in Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**erwähnt w urde, hängt die Sicherheit von symmetrischen Verfahren zentral auch von der Sicherheit der Schlüsselübertragung ab. Aus diesem Grund gibt es verschiedene Protokolle, die sich mit der sicheren Übertragung von Schlüsseln über unsichere Kanäle beschäftigen und somit eine Lösung für das Schlüsseltauschproblem schaffen. Zu diesen Protokollen gehören zum Beispiel der Deffie-Hellman-Schlüsseltausch (DHKE). [10, S. 178ff.]

2.2.5.2 Authentizität, Integrität und Signatur

Inhalt	Erläuterung
Versionsnummer	beschreibt verwendetes Zertifikatformat
Seriennummer	eindeutiger Identifikator
Signatur	verwendete Algorithmen und Parameter
Zertifikataussteller	Name der ausstellenden Instanz
Gültigkeitsdauer	Angabe eines Zeitintervalls
Benutzername	eindeutiger Name des Benutzers
Schlüsselinformationen	Schlüssel des Benutzers und Algorithmen
eindeutiger Identifikator	in Version v2, v3
Erweiterungen	in Version v2, v3

Abbildung 3 Struktur eines X.509 bzw. X.509v3 Zertifikats [4, S. 398]

Neben dem Schlüsseltausch stellen sich noch weitere Probleme. Wie zum Beispiel stellt man die Authentizität/ Echtheit von öffentlichen Schlüsseln sicher? Sprich: Wie sorgt man dafür, dass ein öffentlicher Schlüssel wirklich zur entsprechenden Person gehört? Dies wird in der Praxis mit Hilfe von sogenannten **Zertifikaten** gewährleistet. Das sind digitale Bescheinigungen für genau dieses Problem. Zu beachten gilt dabei, dass Zertifikate nichts über den Inhalt des Objekts, das signiert wurde, oder über die Vertrauenswürdigkeit der Person aussagen. Struktur und Aufbau eines Zertifikates werden durch den X.509 Standard festgelegt. (siehe auch Abbildung 3)

> *„Das heißt, dass ein Zertifikat den Namen des Signierschlüsselinhabers, den zugeordneten öffentlichen Signierschlüssel, die verwendeten Algorithmen, den Gültigkeitszeitraum des Zertifikates und den Namen der Zertifizierungsstelle enthalten muss.“ [4, S. 398]*

Ausgestellt werden diese Zertifikate von **Zertifizierungsstellen** (engl. Trust Center oder Certification Authority) kurz CA. Diese nutzen ein bestimmtes Signaturverfahren. [4, S. 398ff.]

Diese Signaturverfahren basieren auf asymmetrischer Verschlüsselung. Grundlage dieser Verfahren ist es, dass der Absender das zu Signierende mit seinem privaten Schlüssel „unterschreibt“. Das heißt, solange der private Schlüssel geheim ist, kann auch nur er die Nachricht unterschreiben. Für das Unterschreiben wird die Nachricht zusammen mit dem privaten Schlüssel mit Hilfe eines Signaturalgorithmus verarbeitet und man erhält dadurch einen Hash-Wert. Dieser kann zusammen mit der Nachricht versendet werden. Der Empfänger kann dann mit Hilfe eines Verifikationsalgorithmus feststellen, ob die Nachricht tatsächlich vom entsprechenden Sender kommt. Dafür werden die Nachricht und die Signatur mit Hilfe des öffentlichen Schlüssels durch den Verifikationsalgorithmus verarbeitet und es wird eine binäre Entscheidung (kommt vom Sender/ kommt nicht vom Sender) getroffen. [10, S. 299ff.]

2.2.6 Hashverfahren

Im vorherigen Abschnitt wurde erklärt, wie mit Hilfe asymmetrischer Verschlüsselungsverfahrens eine Nachricht auf einen einzigen Hash-Wert reduziert werden kann. Doch was ist eigentlich ein Hash-Wert und gibt es auch noch andere Möglichkeiten einen solchen zu erzeugen?

Wie bereits beschrieben wurde, braucht es eine bestimmte Funktion, um aus einer Nachricht einen Hashwert zu erzeugen. Bei den asymmetrischen Verfahren zur Signatur wurde außerdem noch der private Schlüssel verwendet, um daraus eine Zahl zu erzeugen. Bei allgemeinen Hashfunktionen ist das nicht notwendig. Bei diesen werden Daten unterschiedlicher Länge mit Hilfe einer Einwegfunktion auf einen Wert mit einer festen Länge abgebildet. Eine Einwegfunktion, die auf diese Weise genutzt wird, bezeichnet man auch als Hashfunktion und den Wert, den sie erzeugt, als Hashwert. Da ein Hashwert eine feste Länge

hat (man spricht auch von einem Hashadressbereich) und dieser mit einer bestimmten Funktion erzeugt wird, kann es dazu kommen, dass unterschiedliche Daten auf demselben Hashwert abgebildet werden. Dies bezeichnet man auch als Kollision. Da ein Hashwert aber die Daten klar identifizieren soll, gilt es Verfahren zu finden, die möglichst keine Überschneidungen bei den Hashwerten aufweisen. Man spricht auch von einer Kollisionsresistenz. Dabei wird zwischen einer schwachen und starken Kollisionsresistenz unterschieden. Bei der schwachen Kollisionsresistenz ist es praktisch nicht möglich, aus einer gegebenen Nachricht und deren Hashwert eine zweite Nachricht mit demselben Hashwert zu bestimmen. Dies wird auch als zweite Urbildresistenz bezeichnet. Bei der starken Kollisionsresistenz ist immer die schwache Kollisionsresistenz gegeben. Zudem darf es nicht möglich sein, zwei frei wählbare Nachrichten zu haben, die denselben Hashwert haben. Solche Hashverfahren werden auch als kollisionsresistent bezeichnet. Durch die Kollisionsresistenz von Hashverfahren kommt es dazu, dass sehr ähnliche Texte meist einen stark unterschiedlichen Hashwert haben. [4, S. 365ff.]

Die Unterscheidung zwischen stark und schwach kollisionsresistenten Hashverfahren spielt dann eine Rolle, wenn es um Angriffe auf diese Verfahren geht. Schwache Hashfunktionen sind gegen solche Angriffe resistent, bei denen der Angreifer zu einer gegebenen Nachricht und deren Hashwert eine weitere Nachricht erzeugt will, die den gleichen Hashwert hat. Um eine solche zu finden, wird die ursprüngliche Nachricht in kleinen Schritten immer weiter verändert, bis eine Kollision gefunden wird. Dies wird auch als Substitutionsattacke bezeichnet. Starke Hashfunktionen sind hingegen auch gegen Angriffe resistent, bei denen ein Nachrichtenpaar frei gewählt werden kann. Der Angreifer generiert dabei immer weitere Nachrichtenpaare, die jeweils aus einer unauffälligen und einer schädlichen Nachricht bestehen, bis er bei zwei Nachrichten mit gleichem Hashwert erhält. Um schneller zu Ergebnissen zu kommen, können Nachrichtenpaare im Voraus erzeugt und gespeichert werden. Dies wird auch als Geburtstagsangriff bezeichnet. [10, S. 340ff.]

Hash-Verfahren werden neben dem Signieren von Nachrichten auch für weitere Zwecke in der Kryptografie genutzt. So sind sie zum Beispiel Grundlage für das Erzeugen von Prüfsummen (Message Authentication Code, kurz: MAC) oder auch für das Speichern von Passwörtern. Auch können mit Hilfe von Hashwerten bestimmte Dokumente oder Dateien schnell gefunden werden. Weiterhin kann mit Hilfe eines Hashwertes festgestellt werden, ob eine Datei verändert wurde. [4, S. 365ff.]

2.2.7 Sichere Netzwerkübertragungen

Wenn Daten sicher über ein ungesichertes Netzwerk transportiert werden sollen, kann dafür das **TLS** (Transport Layer Security) -Protokoll genutzt werden. Dies ist ein standardisiertes Protokoll, das die Authentifikation der Kommunikationspartner ermöglicht und die Integrität der übertragenen Daten sicherstellt. Für die Authentifikation werden dabei asymmetrische Verfahren genutzt. Um die Integrität der Daten zu gewährleisten, werden MACs genutzt. Es gibt dabei unterschiedliche Versionen dieses Protokolls. Die aktuellste ist die

Version 1.3. Diese Versionen nutzen unterschiedliche Verfahren zur Authentifikation und Integritätssicherung. Die genauen Verfahren werden beim Verbindungsaufbau zwischen den Kommunikationspartnern festgelegt und dann bis zum Ende der TLS-Sitzung beibehalten. [4, S. 778ff.]

Das TLS- Protokoll ist eine Erweiterung des Transmission Control Protocol (TCP) und ist ein Protokoll, das im ISO/OSI (International Organisation for Standardization/Open Systems Interconnection)-Modell der Sitzungs- und Präsentationsschicht zugeordnet ist. [4, S. 778]

2.3 Verteilte Systeme

In der Literatur gibt es keine eindeutige Definition für den Begriff der **verteilten Systeme**, vielmehr findet so gut wie jede Publikation ihre eigene Definition für diesen Begriff. Eine der bekanntesten Definitionen stammt von Tanenbaum und van Steen, die die folgende Definition geprägt haben:

> *„Ein verteiltes System ist eine Ansammlung unabhängiger Computer, die den Benutzern wie ein einzelnes kohärentes System erscheinen.“ [16, S. 11]*

Schill et al. beschreiben hingegen verteilte Systeme als eine Zusammenstellung mehrerer Einzelkomponenten, die sich auf unterschiedlichen Rechnern befinden und damit meist keinen gemeinsamen Speicher haben und so nur mittels Nachrichtenaustauschs kommunizieren können. Diese Kommunikation wird von dem System genutzt um in Zusammenarbeit eine gemeinsame Aufgabe bzw. Zielsetzung zu erreichen. [17, S. 4]

Es stellt sich also die Frage, was der Vorteil des Einsatzes verteilter Systeme ist und was sich hinter den unterschiedlichen Definitionen in der Praxis verbirgt. Oft werden dabei die Ressourcen innerhalb des verteilten Systems gemeinsam genutzt, wie zum Beispiel Peripheriegeräte, die ansonsten mehrfach angeschafft werden müssten oder Datenbanken. Auch findet in verteilten Systemen eine Parallelisierung der Aufgaben statt, die es ermöglicht, dass die Verarbeitungsleistung steigt. Dabei kann die gleiche Aufgabe von mehreren Servern erfüllt werden, wodurch Lastspitzen und Engpässe vermieden werden können. Auch kann durch die Aufteilung von Aufgaben eine höhere Fehlertoleranz, Ausfallsicherheit und Verfügbarkeit gewährleistet werden, da die Erledigung wichtiger Aufgaben mehrfach aufgebaut werden kann und somit beim Ausfall einer Systemkomponente, die eine Aufgabe erfüllt, eine andere einspringen kann. Auch ermöglicht der Einsatz von verteilten Systemen eine gute Skalierbarkeit des Systems. So ist es einfach möglich, die Kapazität des Systems durch Hinzufügen von Ressourcen zu erhöhen, ohne dass das System verändert werden muss. [17, S. 5f.]

Aber nicht nur die Ressourcen können bei verteilten Systemen einfach skaliert werden. Auch die geografische Verteilung und die Verwaltung können nach Luntovskyy und Gütter skaliert werden. Mit der geografischen Skalierbarkeit meinen sie, dass die Leistung des Systems nicht gravierend durch die geografische Lage der einzelnen Komponenten beeinflusst wird. Die Skalierung der Verwaltung beschreibt, dass auch mehrere unabhängige Organisationen Teil des verteilten Systems sein können, ohne dass der Verwaltungsaufwand zunimmt. [18, S. 356]

In den folgenden Abschnitten soll nun auf drei mögliche Architekturen von verteilten Systemen eingegangen werden. Es wird dabei auf die Client-Server-Architektur, die Cloud-Architektur und die Zero Trust-Architektur eingegangen und die Vor- und Nachteile der entsprechenden Architekturen aufgezeigt.

2.3.1 Client-Server-Architektur

Die Client-Server-Architektur ist eine der grundlegendsten Konzepte der verteilten Systeme. Dieses Modell beruht darauf, dass ein Anbieter eines Dienstes, auch Server genannt, diesen einem Kunden bzw. Nutzer (Client) zur Verfügung stellt. Dafür stellt der Client eine Anfrage über das Netzwerk an den Server. Dabei kann es sich zum Beispiel um den Aufruf einer Website oder einen Methodenaufruf handeln. Der Server verarbeitet dann diese Anfrage und sendet das Ergebnis bzw. die Datenpakete als Antwort zur Anfrage an den Client. [17, S. 14f.]

Dabei kann es aber auch sein, dass ein Server ein Client eines anderen Dienstes ist. Das heißt, dass er für die Erledigung seiner Aufgabe eine Anfrage an einen anderen Server schickt. So ist es also möglich, eine beliebig große Hierarchie aufzubauen. [17, S. 14f.]

Der große Nachteil des Einsatzes der Server-Client-Architektur ist die zentrale Position des Servers. Wenn dieser ausfällt, ist das komplette System nicht mehr in der Lage, seine Aufgabe zu erfüllen. Weiterhin wird für die Wartung und Skalierung eines solchen Systems entsprechendes Fachwissen sowie Zeit und Geld benötigt. Außerdem erfordert die Nutzung von Clustern einen Aufwand zur Synchronisation und Konfliktbehandlung, um Inkonsistenzen zwischen den Servern eines Clusters zu vermeiden. [17, S. 14f.]

2.3.2 Cloud-Architektur

Bei der Cloud-Architektur handelt es sich um eine Weiterentwicklung der klassischen Server-Client-Architektur. Es kommt auch dabei wieder zu einer Kommunikation zwischen einem Server und einem Client. Dieser Server existiert jedoch nicht physisch, sondern steht nur virtuell zur Verfügung. Das heißt, alle physischen Ressourcen des Cloudanbieters werden gebündelt und mit Virtualisierungstechniken zu virtuellen Ressourcen umgewandelt. Dadurch ist es dann möglich, flexibel Ressourcen einem Kunden zur Verfügung zu stellen oder diese zu entziehen. Der virtuelle Server des Kunden kann so flexibel z. B. mit

Speicherplatz und Rechenleistung ausgestattet werden. Für den Kunden spielt es dabei keine Rolle, woher die Ressourcen aus dem Netzwerk des Anbieters kommen, um den eigenen Server zu betreiben. Es ist irrelevant, ob die Ressourcen an einem oder mehreren Orten lokalisiert sind. Das heißt, ein Anbieter kann sowohl einen einzelnen Serverstandort haben als auch verteilte Rechenzentren. [17, S. 31-36]

Nach Luntovskyy und Gütter [18] bietet die Cloud-Architektur mehrere Vorteile. So benennen sie als ersten Vorteil die dynamische Verfügbarkeit und Anpassbarkeit der Ressourcen an den Bedarf. Weiterhin sehen sie einen Vorteil darin, dass eine Organisation sich nicht selbst die technische Infrastruktur schaffen muss, um z.B. rechenintensive Probleme zu lösen oder Speicherplatz für Backups zu haben. Als weiteren Vorteil sehen sie die Bündelung der physischen Ressourcen, die von unterschiedlichen Organisationen genutzt werden können, an einem Punkt. So entstehen für alle Organisationen geringere Kosten für Hardware und Verarbeitungszeit. [18, S. 378]

Nachteil dieser Netzwerkarchitektur ist, dass es für einen Nutzer nur schwer möglich, ist Fragen des Datenschutzes und der Sicherheit zu beantworten, da die genutzte IT-Infrastruktur mit ihrem Aufbau und Standort unbekannt ist. Dadurch kommt es zu einer Abhängigkeit vom Cloud-Anbieter, da der Nutzer sich darauf verlassen muss, dass der Anbieter für die Sicherheit der Daten sorgt. Außerdem ist es für den Nutzer bei der Nutzung bestimmter Anbieter nicht problemlos möglich, diesen zu wechseln, da es nicht einfach möglich ist, die genutzten Dienste zu einem anderen Anbieter zu überführen. [18, S. 378]

2.3.3 Zero Trust-Architektur

Der Begriff des **Zero Trust** (ZT) und die dazu gehörende Netzwerkarchitektur wurde 2009 von John Kindervag und dessen Mitarbeitern am Forrest Research Inc. entwickelt. [19]

Der Grundgedanke des Zero Trust Modells ist es, dass nichts und niemandem in einem Netzwerk vertraut werden kann. Aus diesem Grund muss jede Kommunikation kontrolliert werden. Dies stellt einen großen Unterschied zu herkömmlichen Netzwerkarchitekturen dar, die nur die Kommunikation mit externen Systemen als Gefahr einstufen. [20, S. 2]

Garbis und Chapman [21] definieren deshalb insgesamt 6 Prinzipien bzw. Merkmale für ZT, von denen sie drei als Kernprinzipien und drei als zusätzliche Prinzipen beschreiben. Die drei Kernprinzipien sind:

1. Sicherstellung des sicheren Zugriffs auf Ressourcen unabhängig von deren Position:
   Das heißt, dass ZT-Lösungen immer ganzheitliche Ansätze sind und dass jeglicher Zugriff auf Ressourcen, die nicht Teil des Zero Trust Netzwerkes sind oder von diesem geprüft wurden, unterbunden werden muss. Um dies zu erreichen, können z. B. Dateien verschlüsselt werden und verschlüsselte Tunnel für den Zugriff genutzt werden. [21, S. 13f.]

2. Eine Strategie mit minimalen Zugriffsberechtigungen und strengen Zugriffskontrollen:
   Damit meinen Garbis und Chapman, dass Systeme und Nutzer haben nur Zugriff auf die notwendigen Ressourcen haben. [21, S. 14]
3. Überprüfung und Protokollierung des gesamten Datenverkehrs:
   Als weiterer wichtiger Punkt ist die Aufzeichnung und Auswertung des Netzwerkdatenverkehrs zu sehen. Dies dient dazu, Auffälligkeiten schnell zu bemerken, um Gegenmaßnahmen einleiten zu können. [21, S. 14f.]

Die zusätzlichen Prinzipien sind nach Garbis und Chapman:

1. Sicherstellung, dass alle Komponenten APIs (Application Programming Interface) für Ereignis- und Datenaustausch unterstützen:
   Dies ermöglicht eine Verbindung aller Komponenten, um ein ganzheitliches IT- Sicherheitskonzept zu erstellen. [21, S. 15]
2. Automatisierung von Aktionen:
   Dies ist nötig, da aufgrund von Besonderheiten im Aufbau und der Regelverwaltung eine Automatisierung bestimmter Prozesse unerlässlich für einen reibungslosen Ablauf sind. So ist nur noch für bestimmte wichtige Entscheidungen das Eingreifen des Menschen nötig. [21, S. 15f.]
3. ZT bringt dem Unternehmen einen taktischen und strategischen Wert:
   Die Einführung einer ZT- Architektur erfordert zu Beginn einen technischen und finanziellen Aufwand und führt zu vielen Veränderungen im Aufbau der IT- Infrastruktur. Jedoch bringen diese Änderungen auch Vorteile mit sich, die im Weiteren noch näher beschrieben werden. [21, S. 16]

Im Folgenden soll nun ein kurzer Blick auf die praktische Umsetzung dieses Prinzips geworfen werden.

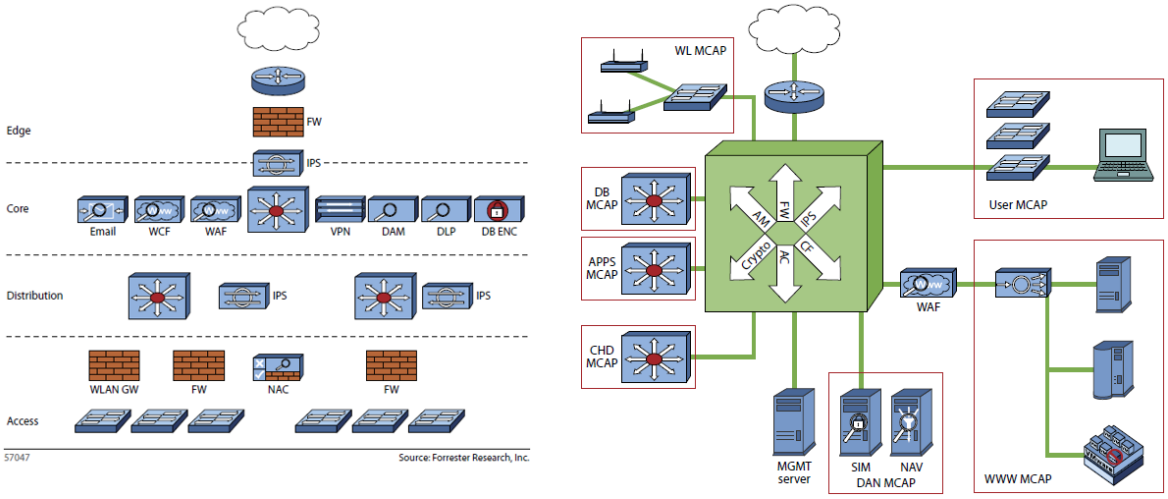

Abbildung 4 Gegenüberstellung traditionelles hierarchisches Netzwerk (links) und Zero Trust Netzwerk (rechts) [20, S. 5; 21]

Grundlegende Elemente der praktischen Umsetzung sind Segmentierung, zentrale Verwaltung, Parallelisierung und Protokollierung, sowie Auswertung des Datenverkehrs.

Bei traditionellen hierarchischen Netzwerken liegt das Hauptaugenmerk häufig auf den Perimetergrenzen. Ausgehend von dieser Grenze wird dann eine grobe Segmentierung vorgenommen. So werden zum Beispiel WANs (Wide Area Network), DMZ (Demilitarisierte Zone) und interne Netze entworfen. Aufgrund dessen, dass meist nur die Grenze gesichert wird, werden dort viele Sicherheitsfunktionen installiert, die einen hohen Kostenaufwand mit sich bringen. Allerdings leidet das Sicherheitskonzept unter einer solchen Einseitigkeit. Sollte es einem Angreifer gelingen, diese Hürden zu überwinden, trifft er meist nur noch auf geringen Widerstand. [20, S. 2-5]

Das hierarchische Modell ist aus drei wesentlichen Elementen aufgebaut: der Kante/Perimeter Grenze (engl. Edge), dem Kern/Rückgrat (engl. Core/Backbone und den Zugriffspunkten (engl. Access). Optional kann eine Verteilungsebene (engl. Distribution) integriert werden, die aufgrund der Leistungsfähigkeit heutiger Switches oft nicht mehr zwingend benötigt wird. [20, S. 3f.]

Die **Kante** trennt dabei internes und externes Netzwerk. Das heißt, dass dort die Instanzen zu finden sind, die für die Kontrolle der zwischen den Segmenten ein- und ausgehenden Datenpakete verantwortlich sind. Der **Kern** hingegen beinhaltet die Komponenten, die für die zentrale Weiterleitung der Datenpakete verantwortlich sind. Die Komponenten sind mit dem Internet verbunden und enthalten die elementaren Sicherheitsfunktionen. Wenn die **Verteilungsebene** vorhanden ist, wird dort eine Verbindung zwischen Kernelementen und Zugriffspunkten geschaffen. Die Verteilungsebene beinhaltete häufig Switches, die die Zugriffspunkte in logische Segmente gegliedert und mit dem Core Switch verbunden haben. Die Zugriffspunkte sind die Schnittstelle zu den Endgeräten, die an das Unternehmensnetzwerk angebunden werden. Dort befinden sich Sicherheitsfunktionen, wie Network Access Protection (NAP) oder Firewalls (FW) (siehe auch Abbildung 4). [20, S. 3f.]

Es stellt sich nun also die Frage, wie sich die hierarchische Struktur von einer ZT-Netzwerkarchitektur unterscheidet.

Die Sicherheit des Netzwerkes ist bei der ZT- Netzwerkarchitektur schon ein zentraler Bestandteil der Planung. So wird vorgeschlagen, zuerst die Endpunkte zu planen und danach die Verbindungen. Dadurch werden zuerst die Daten in logische Segmente unterteilt und danach wird überlegt, wie diese miteinander vernetzt werden können, ohne dass die Sicherheit der Daten und Systeme gefährdet wird. Auch gibt es bei der ZT-Netzwerkarchitektur keinen Core Switch. Vielmehr sollen mehrere kleine Switches eingesetzt werden, damit eine Optimierung des Datenverkehrs erreicht werden kann. Wird dies konsequent umgesetzt, kann das Netzwerk dynamisch erweitert werden und einfach mitwachsen. Am letzten dieser Punkte wird der Zugang zum Internet angebunden. [20, S. 2-5] Weiterhin wird für die Umsetzung dieser Architektur ein sogenanntes „segmentation gateway (SG)“ [20, S. 7] benötigt. Dieses zentrale Netzwerkelement hat alle Sicherheitskomponenten implementiert

und ermöglicht eine segmentübergreifende Sicherstellung der Sicherheit und Überwachung des Datenverkehrs. Rose et. al. [22] bezeichnen diese Gateways auch als PDP (Policy Decision Point)/PEP (Policy Enforcement Point)- Gateways. Der PEP ist dabei für das Aufbauen, Überwachen und Beenden von Verbindungen verantwortlich. Der PEP kommuniziert mit dem PA (Policy Administrator), um Anforderungen weiterzuleiten und/oder Richtlinienaktualisierungen vom PA zu empfangen. Der PA ist verantwortlich für das Einrichten und Schließen von Kommunikationskanälen. Der PA generiert außerdem alle Session IDs, Authentifizierungstokens und Berechtigungsnachweise, die für den Zugriff auf Ressourcen benötigt werden und konfiguriert den PEP. Der zweite Teil des PDP ist die PE (Policy Engine). Diese ist eng mit dem PA verbunden und trifft die endgültige Entscheidung, ob dem Client der Zugriff auf eine Ressource gewährt wird, und protokolliert diese. Für die Entscheidung nutzt die PE sowohl Unternehmensrichtlinien, als auch Eingaben von externen Quellen. Es ist möglich, die PE und den PA auch als einen einzigen Dienst zu implementieren. [22, S. 5-10]

Die Segmentierung des Netzwerkes wird mit einem sogenannten „microcore and perimeter“ kurz MCAP erreicht. Dieser ist mit dem zentralen SG verbunden und steuert den ein- und ausgehenden Datenverkehr. Durch die Verbindung zum SG erhält das MCAP die globalen Sicherheitsrichtlinien zum Schutz des Segments. Da jedem MCAP auf logische Weise Objekte auf Basis deren Funktionalität zugeordnet werden, können für diese die globalen Sicherheitsrichtlinien angewendet werden. Gleichzeitig existieren die einzelnen Segmente als isolierte Umgebungen. Jedes einzelne Segment kann über das SG erreicht werden. [20, S. 8]

Ein weiteres zentrales Merkmal der ZT- Netzwerkarchitektur ist die Nutzung eines zentralen Verwaltungssystems. Dieses ermöglicht eine Administration des Systems über eine graphische Oberfläche oder automatisiert diese Aufgabe über ein API. Auch die bereits erwähnte Protokollierung und Auswertung des Datenverkehrs ist ein zentraler Bestandteil. Die Auswertung dieser Protokolle erfolgt dabei nicht durch einen Menschen, sondern wird in der Regel automatisiert. Dafür kann der Administrator ein sogenanntes „security information management“ kurz SIM und eine NAV („network analysis and visibility“) Anwendung nutzen. [20, S. 8f.]

Ein SIM oder auch SIEM (Security Information and Event Management) sammelt, überwacht und analysiert Logdaten und verknüpft diese mit weiteren Ereignisdaten und Umgebungsinformationen. Es kann so Informationen über die Einhaltung von Regeln erhalten und mögliche Sicherheitsvorfälle erkennen. Ein SIM arbeitet dabei mit eher historischen Daten und ein SEM (Security Event Management) mit Realzeitinformationen. Das SIEM ist die Kombination aus beiden. [5, S. 191]

Eine NAV-Anwendung nutzt verschiedene Netzwerkanalysetools um den Datenverkehr zu analysieren und kann so Zwischenfälle, wie zum Beispiel Schadsoftware, erkennen und Reaktionen auf diese auslösen. [23, S. 2]

Die Auswertung und Protokollierung werden dabei in einem separaten Netzwerk vorgenommen. Man bezeichnet dieses Netzwerk auch als „Data Acquisition Network“ kurz DAN. Dieses Netzwerk dient dann zur Überwachung und Auswertung aller Protokolle, wie zum Beispiel Syslog oder Simple Network Management Protocol kurz SNMP. [20, S. 8f.]

Diese Netzwerkarchitektur bringt eine Reihe von Vorteilen mit sich. So ist ein Zero Trust Netzwerk aufgrund seiner Merkmale skalierbar und lässt sich gut erweitern. Auch bietet es einen guten Schutz vor Angriffen und ermöglicht durch seine Segmentierung, dass ein Angreifer, falls er Zugriff auf ein Segment erhält, nicht auf alle anderen Segmente einfach zugreifen kann. Jedoch ist der Aufbau einer solchen Architektur mit hohen Kosten verbunden und die Umsetzung des Konzepts ist sehr komplex.

2.4 Datensicherung

Pohlmann beschreibt eine **Datensicherung,** auch Backup genannt, als eine Kopie eines vorliegenden Datenbestandes eines IT-Systems, das auf einem oder mehreren externen Speichermedien als Sicherheitskopie gespeichert wird. Im Fall des Datenverlustes kann diese Sicherheitskopie auf das IT-System zurückkopiert werden. Dies wird auch als Recovery bezeichnet. Zu einem Datenverlust kann es zum Beispiel durch Naturkatastrophen, Unfälle oder auch Hardwaredefekte kommen. Aber auch durch Angriffe auf das IT-System oder durch Programmfehler kann es zu ungewolltem Datenverlust kommen. [24, S. 697ff.], [25, S. 244]

Bei Backups handelt es sich im Normalfall nicht um hochaktuelle Kopien des Originalsystems, vielmehr werden sie meist in periodischen Abständen von einem System erstellt. Der zeitliche Abstand kann dabei frei gewählt werden. So kann ein Backup beispielsweise wöchentlich, täglich oder stündlich erstellt werden. Dabei gilt zu beachten, je häufiger ein Backup erstellt wird, desto weniger Daten gehen im Schadensfall verloren. Im Normalfall wird für den Recovery- Prozess das aktuellste Backup genutzt. Es können jedoch auch ältere Backups genutzt werden, wenn zum Beispiel das aktuellste Backup beschädigt ist oder man eine ältere Version der Daten benötigt. [24, S. 697ff.]

Mit Hilfe von Backups können also verschiedenste Daten gesichert werden. Dabei hängt die Art der Daten, die gesichert werden, vom entsprechenden Einsatzgebiet ab. So können sowohl Backups von Verzeichnisstrukturen oder auch Konfigurations- und Anwendungsdateien gesichert werden. Natürlich können auch Images von ganzen Computersystemen angefertigt werden, die es ermöglichen, das ganze System wiederherstellbar zu machen. [24, S. 699]

2.4.1 Backup- Konzepte

Es gibt verschiedene Möglichkeiten Backups zu erstellen. In der Literatur wird zwischen drei verschiedenen Arten unterschieden. Diese sind die volle Sicherung (Full Backup), die differenzielle Sicherung (Differential Backup) und die inkrementelle Sicherung (Incremental Backup).

Wie die Bezeichnung der **vollen Sicherung** nahelegt, handelt es sich bei dem vollständigen Backup um das umfassendste Backup-Konzept. Bei diesem werden alle Daten gesichert, das heißt, das vollständige Laufwerk mit allen Ordnern, Dateien und Partitionen. Es spielt dabei auch keine Rolle, ob sich die Daten seit der letzten Sicherung verändert haben. Dadurch lassen sich die Daten durch einen Recovery-Prozess zwar schnell wiederherstellen, jedoch wird für die Sicherung sehr viel Zeit im Vergleich zu den anderen Sicherungskonzepten verbraucht. Weiterhin benötigen vollständige Backups einen großen Speicherplatz. Dies führt dazu, dass dieses Konzept in der Praxis meist nicht angewandt wird. [24, S. 699], [25, S. 246]

Ein weiteres Sicherungskonzept ist die **differenzielle Sicherung**. Bei diesem Sicherungskonzept werden nur die Daten kopiert, die seit dem letzten vollständigen Backup verändert oder neu erzeugt wurden. Dadurch wird für die Sicherung deutlich weniger Zeit und Speicherplatz benötigt. [24, S. 699f.], [25, S. 246]

Das letzte Sicherungskonzept ist die **inkrementelle Sicherung**. Bei dieser Art der Sicherung werden nur die Daten kopiert, die sich seit dem letzten Backup verändert haben, unabhängig davon, welcher Art dieses war. Um festzustellen, ob eine Datei verändert wurde, wird dabei das Änderungsdatum der Datei mit dem Datum des letzten Backups verglichen. Dadurch, dass nur die Daten kopiert werden, die verändert wurden, wird deutlich weniger Zeit zum Sichern benötigt als bei den anderen Sicherungskonzepten. Weiterhin wird auch weniger Speicherplatz benötigt. Jedoch steigt der Aufwand für den Recovery- Prozess. [24, S. 699], [25, S. 246]

2.4.2 Deduplizierung

Eine weitere Möglichkeit Speicherkosten zu sparen und die Netzwerkauslastung beim Erstellen von Backups zu reduzieren ist die Verwendung von Deduplizierung. Bei der **Deduplizierung** wird der Speicherplatzbedarf dadurch verringert, dass identische Daten erkannt und nur einmal gespeichert werden. Um dafür zu sorgen, dass bei dem Recoveryprozess die Daten an allen Stellen, sprich ohne Datenverlust, wiederhergestellt werden können, werden Referenzierungen genutzt. [26], [27, S. 87]

Die Deduplizierung kann dabei entweder an der Quelle oder dem Ziel der Daten durchgeführt werden. Dies hat vor allem Einfluss auf die Performance und die Funktionen des Backupsystems. [26], [27, S. 94]

Wenn die Deduplizierung an der Quelle stattfindet, spricht man auch von Source Deduplication. Dabei wird die benötigte Backup-Software an der Quelle installiert. Diese stellt dann fest, ob sich die Daten verändert haben und ob diese bereits gesichert wurden. So werden nur die neuen Daten gesichert. [26], [27, S. 96f.]

Wenn hingegen die Deduplizierung am Ziel stattfindet, spricht man auch von Target Deduplication. Dabei übernimmt das empfangende System die Deduplizierung. [26], [27, S. 98]

Bei dieser Art wird auch noch zwischen Inline- und Post-Process-Deduplication unterschieden. Die Inline- Deduplication dedupliziert die Daten, bevor diese vom Backupsystem gespeichert werden. Die Post-Process-Deduplication hingegen speichert die Daten zuerst und dedupliziert sie anschließend in einem asynchronen Prozess. [26], [27, S. 94 f.]

Die Auswahl des Ortes, an dem die Deduplizierung durchgeführt wird, bringt dabei unterschiedliche Vor- und Nachteile mit sich. So ist es beim Target Deduplication so, dass es relativ einfach zu einer bestehenden Backupstrategie zu ergänzen ist und diese auch ersetzen kann. Jedoch braucht der Server dann Zugang zu den Daten. Dies kann allerdings je nach Dateiformat oder Verschlüsslung der Daten schwierig sein. Der Vorteil der Source Deduplication ist, dass dort auf die Daten einfach zugegriffen werden kann und diese danach verschlüsselt werden können. Dadurch werden weniger Daten an den Server übertragen, was das Netzwerk entlastet. Jedoch muss dafür bestimmte Software angeschafft werden. [26], [27, S. 94-98]

Neben dem Ort der Deduplizierung spielt auch die Art eine Rolle. Es werden dabei vier Arten unterschieden. Diese Algorithmen sind:

- **Datei** (engl. Whole File Hashing oder Whole-File Chunking): Dabei wird der Inhalt der Datei gehasht und dies als Signatur der Datei genutzt. Wenn dann Dateien mit derselben Signatur festgestellt werden, können diese dedupliziert werden. [26], [28, S. S.28]
- **Fixe Blöcke** (engl. Fixed Block Hashing oder Static Chunking): Dafür werden die zu deduplizierenden Daten in Blöcke gleicher Größe zerlegt und anschließend jeder Block gehasht und damit signiert. Danach findet dann die Deduplizierung statt. Dieser Algorithmus hat jedoch große Probleme mit Dateien, die geändert wurden, da jede Änderung alle nachfolgenden Blöcke verschiebt und damit gleichbleibende Teile nicht mehr erkannt werden. [26], [28, S. 28]
- **Variable Blöcke** (engl. Variable Block Hashing): Dafür werden die zu deduplizierenden Daten in Blöcke variabler Größe zerlegt und anschließend jeder Block gehasht und damit signiert. Die Größe der Blöcke hängt dabei vom Dateninhalt ab. Die Blockgrenze wird dabei als Anker bezeichnet. Geändert werden können so nur einzelne Blöcke und es kommt zu keiner Verschiebung wie bei den fixen Blöcken. [26], [28, S. 28]

- **Applikationsspezifische Blöcke** (engl. Application-specific Chunking): Um dieses Verfahren nutzen zu können, wird anwendungsspezifisches Wissen benötigt, dass dann zur Blockeinteilung genutzt werden kann. So kann beispielsweise der Dateityp bestimmen, wie Blöcke eingeteilt werden mit denen schlussendlich genauso vorgegangen wird wie bei den anderen Verfahren. [28, S. 28]

Auch hier gibt es unterschiedliche Vor- und Nachteile, die jede Art der Deduplizierung mit sich bringt. So ermöglicht die Verwendung variabler Blöcke die größte Speicherplatzeinsparung, jedoch bringt diese Art der Deduplizierung auch den größten Aufwand zur Wiederherstellung mit sich. Dieser Aufwand zur Wiederherstellung muss auch bei Blöcken fixer Größe erbracht werden. Die Algorithmen, die Blöcke fester Länge bzw. Daten als Basis nutzen, verbrauchen zwar weniger CPU (Central Processing Unit) - Leistung, jedoch benötigen sie einen höheren Speicherplatz. Außerdem gilt allgemein für die Verwendung von Deduplizierung, dass, je gründlicher diese stattfindet, desto weniger Speicherplatz wird benötigt. Jedoch steigt der Aufwand für die Verwaltung der Metadaten. Auch führt die Einteilung von Dateien in kleine Blöcke zu deren Fragmentierung. Dies kann Auswirkungen auf die Performance des Systems haben. [26], [28, S. 28f.]

2.4.3 Backuplagerung

Neben der Erstellungsart eines Backups spielt auch der Lagerort eine wichtige Rolle für eine funktionierende Backupstrategie. Wenn die gewählten Speichermedien nicht zuverlässig sind, nützt auch das beste Backup nichts. Das heißt, dass man sich auch über die Lagerung eines Backups bei der Planung einer Backupstrategie Gedanken machen muss.

Man unterscheidet bei der Lagerung zwischen zwei großen Gruppen. Die erste Möglichkeit ist die **Online-Speicherung** oder auch Cloud-Speicherung. Bei dieser Art der Speicherung sind die Daten jederzeit verfügbar und es lässt sich schnell und kostengünstig einrichten. Jedoch ist diese Sicherung von außen angreifbar, da die Sicherung über ein Netzwerk stattfindet. [29], [24, S. 698]

Bei der zweiten Art handelt es sich um die **Offline-Speicherung**. Bei dieser Art erfolgt die Speicherung auf externen Speichermedien. Dazu gehören unter anderem externe Festplatten, Universal Serial Bus (USB)-Sticks oder auch Bänder und optische Medien. Bei der Offline- Speicherung werden diese Speichermedien nach dem Erstellen des Backups vom Netzwerk getrennt. Die Nachteile dieser Sicherung sind, dass die Anschaffung der Speichermedien und deren regelmäßiger Austausch bezahlt werden muss. Weiterhin stehen die Daten nicht sofort im Schadensfall zur Verfügung und die Sicherung ist aufwändiger. [29], [24, S. 698]

Neben der Unterscheidung zwischen Online- und Offline- Speicherung wird bei der Lagerung auch noch zwischen On- und Off-Site-Speicherung unterschieden. Die **On-Site- Speicherung** beschreibt dabei, dass das Backup in räumlicher Nähe zum gesicherten IT-System gelagert wird. Das heißt, es befindet sich zum Beispiel im selben Raum oder Gebäude.

Dadurch ist die Zeit bis zur Wiederherstellung im Schadensfall relativ kurz und kostengünstig. Jedoch kann es bei einer Katastrophe dazu kommen, dass die Backups mit vernichtet werden. [28, S. 31]

Bei der **Off-Site-Speicherung** werden die Backups an einem anderen Ort gespeichert. Das heißt zum Beispiel auf einem System oder Speichermedium in einem anderen Gebäude. Dies verhindert, dass in einem Katastrophenfall die Backups verloren gehen. Bei der Verwendung von Cloudsystemen muss dies auch beachtet werden. Der Nachteil ist jedoch, dass es eines höheren Aufwandes der Sicherung bedarf und die Daten nicht sofort zur Verfügung stehen. Außerdem ist die Off-Site- Speicherung mit höheren Kosten verbunden. [28, S. 31]

2.4.4 Wiederherstellzeit und Wiederanlaufpunkt

Wenn es zu einem Datenverlust kommt, möchte man, dass die Daten möglichst schnell und auf dem aktuellen Stand wiederhergestellt werden. Dabei rücken zwei Aspekte in den Vordergrund, die durch die Wahl der Backupart und Lagerung beeinflusst werden. [30, S. 103 f.]

Der erste ist die Wiederherstellzeit (engl. Recovery Time Objective) kurz RTO und der zweite ist der Wiederanlaufpunkt (engl. Recovery Point Objective) kurz RPO. Bei beiden handelt es sich um Zeitspannen. [30, S. 103 f.]

Die RTO ist dabei die Zeit, die benötigt wird, um die Daten und die Funktionalität des Systems wiederherzustellen. Das heißt, es gehört nicht nur die bloße Datenwiederherstellung, sondern auch die eventuelle Nachbearbeitung der Daten, das Ersetzen von beschädigten Hardwarekomponenten sowie die Konfiguration und Installation von Software, die benötigt wird, um das System wieder einsatzbereit zu machen, dazu. [30, S. 103 f.]

Der Wiederanlaufpunkt bzw. die Wiederanlaufzeit beschreibt hingegen den maximalen Zeitraum, in dem Daten verloren gehen können; sprich: den Abstand zwischen letzter Sicherung und Schadensfall. Das heißt, dass der Backupabstand eine bedeutende Rolle für den Wiederanlaufpunkt spielt und dass dadurch bestimmt wird, wie viele Daten verloren gehen. [30, S. 103 f.]

3 Anforderungen an ein Cloudbackupsystem unter Zero Trust

Um zu erreichen, dass ein Backupsystem unter Zero Trust sicher ist, muss dieses eine Reihe von Anforderungen erfüllen. Da das hier beschriebene Konzept eine Grundlage für die Entwicklung konkreter Umsetzungen sein soll, werden im Folgenden allgemeine Anforderungen an ein Cloudbackupsystem unter Zero Trust dargestellt. Diese wurden aus den oben beschriebenen theoretischen Grundlagen abgeleitet und zu einem Anforderungskatalog zusammengefasst.

Die folgende Tabelle zeigt die Anforderungen, die an ein solches System gestellt werden müssen. Im darauffolgenden Kapitel wird auch auf Richtlinien, die bei der Umsetzung eines solchen Systems beachtet werden sollten sowie rechtliche Regelungen, die bei der Planung berücksichtigt werden müssen, eingegangen. Daraus wird dann ein vollständiger Anforderungskatalog entwickelt.

Tabelle 1 Anforderungen an einen Cloudbackup Server unter ZT aus der Theorie

A01	**Datensicherung**: Wie jedes Backup-System hat auch dieses System den Anspruch, eine periodische Sicherung der Daten durchzuführen. Das heißt, es muss möglich sein, diesen Zeitabstand zu konfigurieren und die gesicherten Daten auf dem Cloudbackup Server zu speichern. [28, S. 36]
A02	**Sichern und Erkennen von Änderungen**: Um Speicherplatz zu sparen und das Netzwerk zu entlasten, soll nicht jedes Mal ein vollständiges Backup erstellt werden, vielmehr sollte auf eine inkrementelle Sicherung gesetzt werden. [28, S. 36]
A03	**Off-Site Speicherung der Backups:** Das heißt, dass das Backup an einem anderen Ort gespeichert wird. Dies ist dadurch gegeben, dass der Cloudbackup Server an einer anderen Stelle steht als die Komponenten des Ursprungssystems. [28, S. 36f.]

A04	**Minimierung der Sicherungszeit** Die größten Datenverluste entstehen dadurch, dass ein System vor Beendigung des Backupprozesses ausfällt. [31] Um A03 gewährleisten zu können, muss die Datenübertragung möglichst zügig erfolgen. Dies erfordert die Sicherstellung von technischen Voraussetzungen (z.B. eine ausreichend hohe Upload Bandbreite). [28, S. 38]
A05	**Vertrauliche Speicherung der Backups:** Das heißt, dass die Backups so gespeichert werden müssen, dass nur der Eigentümer diese abrufen kann. [28, S. 37]
A06	**Wiederherstellung:** Eine weitere wichtige Anforderung ist, dass die gesicherten Daten auch wiederhergestellt werden können. So muss es jederzeit möglich sein, einen beliebigen Backuppunkt wiederherzustellen, sodass die Daten dann wieder vollständig vorliegen. [28, S. 37]
A07	**Externe Überprüfung auf Schadsoftware:** Um sicherzustellen, dass die bereits erstellten Backups nicht durch ein neu erstelltes, infiziertes Backup mit beschädigt werden und so A05 nicht mehr erfüllt werden kann, soll jedes Backup, bevor es auf den Backup-Server gelangt, auf Schadsoftware überprüft werden.
A08	**Erkennung unvollständiger und/ oder manipulierter Sicherungen:** Damit A05 erfüllt werden kann, muss nicht nur Schadsoftware, sondern auch das Fehlen bzw. das Manipulieren von Backupdaten erkannt werden. [28, S. 37]
A09	**„Kompensation fehlerhafter oder fehlender Backups“** [28, S. 37]**:** Das System muss fehlende oder fehlerhafte Daten erkennen können und in der Lage sein, diese zu kompensieren. So kann es zum Beispiel beim Abbrechen der Verbindung zwischen dem zu sicherndem System und dem Backupserver zu Datenverlusten kommen. Dies muss vom System erkannt und behoben werden können. [28, S. 37]

A10	**Vertrauliche Kommunikation zwischen Client und Server** Jeglicher Datenverkehr muss so gesichert werden, dass es keinem Angreifer während der Backuperstellung oder des Recoveryprozesses möglich ist, auf die Daten zuzugreifen. [28, S. 37]
A11	**Überprüfung und Protokollierung des Datenverkehrs** Um schnell zu erkennen, dass A09 verletzt wurde oder andere Anforderungen verletzt wurden, muss eine Protokollierung und Auswertung des gesamten Datenaustauschs und der Erstellung der Backups erfolgen.
A12	**Minimale Zugriffsberechtigungen und strenge Zugriffskontrollen** Um zu erreichen, dass nur befugte Personen Zugriff auf die gesicherten Daten haben, muss eine strenge Beschränkung von zugriffsberechtigten Personen und deren Rechten erfolgen sowie deren Identität durch Zugriffskontrollen verifiziert werden.
A13	**Verschlüsselung der Daten:** Die Daten müssen mit geeigneten Verfahren verschlüsselt werden, damit es Unbefugten nicht möglich ist, auf diese zuzugreifen, sollten sie an die Daten gelangen. [28, S. 37]
A14	**Authentifizierungsmöglichkeit:** Um sicherzustellen, dass kein Unbefugter Daten auf dem Backupserver oder im Kundensystem verändern kann, muss eine Möglichkeit der Authentifizierung geschaffen werden. [28, S. 38]

Die nachfolgende Tabelle zeigt weitere Anforderung, die zur Sicherheit beitragen können, die jedoch für die Funktionsfähigkeit des Systems nicht zwingend erforderlich sind.

Tabelle 2 Optionale Anforderungen an ein Cloudbackupsystem unter ZT

oA01	**Automatisierung des Backup- und Recoveryprozesses** Um den Zugriff unbefugter Personen zu erschweren und möglichst wenig Zugriffsrechte zu ermöglichen (A10; A12), kann eine weitgehende Automatisierung des Backup- und Recoveryprozesses sinnvoll sein. Dies ermöglicht zudem eine Entlastung des Personals.
oA02	**Einhalten der 3-2-1-Daten-Backup-Regel:** Um das Risiko für einen Verlust des Backups zu reduzieren, kann das Backup vom Anbieter nach der 3-2-1 Datenbackup-Regel gesichert werden. Das heißt, es werden drei Kopien der Daten erstellt und diese werden auf zwei unterschiedlichen Speichermedien festgehalten, von denen sich eines an einem anderen geografischen Ort befindet. [32, S. 296]

4 Wichtige gesetzliche Grundlagen und Richtlinien zur Umsetzung von Cloudbackupsystemen unter Zero Trust

Nachdem im vorherigen Kapitel, die Anforderungen aufgelistet wurden, die man auf Grundlage des Wissens über Backups, Cloudsysteme, Kryptografie und die Zero Trust Architektur an ein entsprechendes System stellt, soll nun ein Einblick in die rechtlichen Grundlagen und Richtlinien, die sich mit der Umsetzung eines solchen Konzeptes auseinandersetzen, gegeben werden.

4.1 Rechtliche Grundlagen

Es stellen sich im Zusammenhang mit einem Cloudbackupsystem einige Fragen zu rechtlichen Aspekten, die bei der Umsetzung eines solchen Systems durch den Anbieter zu berücksichtigen sind. Insbesondere der Umgang mit personenbezogenen Daten stellt dabei eine große Herausforderung dar. Wichtigste gesetzliche Grundlage für den Umgang mit personenbezogenen Daten ist die DSGVO, die EU-weit gilt. Diese regelt den Umgang und den Schutz dieser Daten. [6, Art. 1]

Die DGSVO schreibt mehrere Grundsätze für die Verarbeitung personenbezogener Daten in Art. 5 vor. Dazu zählt auch, dass der für die Verarbeitung Verantwortliche für die Sicherheit dieser Daten Sorge zu tragen hat. Um dies zu erreichen, müssen „geeignete technische und organisatorische Maßnahmen“ getroffen werden. Dies umfasst nach Art. 32 Abs. 1 lit. c

> *„...die Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall [sicherzustellen und es zu ermöglichen die Daten dann] rasch wiederherzustellen.“ [6, Art. 32 Abs. 1 lit. c]*

Dies zu gewährleisten ist nur durch die Erstellung von Backups möglich. Das heißt, sollten keine Backups erstellt werden, ist der Verantwortliche schadensersatzpflichtig. Außerdem werden laut DSGVO empfindliche Bußgelder fällig. [6, Art. 83] Aus diesem Grund sollte jedes Unternehmen über ein umfassendes Backupkonzept verfügen.

Neben der bereits erwähnten Datensicherheit muss beim Entwurf des Backupkonzeptes auch die Löschung personenbezogener Daten mit eingeplant werden. Nach Art 17 DSGVO [6] hat jeder Betroffene unter bestimmten Voraussetzungen das Recht auf Löschung seiner personenbezogenen Daten. Dies gilt nicht nur für den aktuellen Datenbestand, sondern auch für kopierte und archivierte Daten. Dabei muss berücksichtigt werden, dass personenbezogene Daten auch gelöscht werden müssen, sobald der definierte Zweck der Erhebung nicht mehr gegeben ist [6, Art. 5]. Dafür stehen sechs bis zwölf Monate zur Verfügung. Es muss jedoch auch berücksichtigt werden, dass bestimmte Daten trotzdem über eine festgelegte Frist aufbewahrt werden müssen. Diese Aufbewahrungsfristen können sich je nach Art der Daten stark unterscheiden. So ist die Aufbewahrungsfrist für Daten, die einen Zusammenhang mit der Steuerpflicht haben, zehn Jahre lang. Im Steuerrecht mag diese Frist noch einheitlich sein, im Handelsrecht sieht dies schon anders aus. Hier reichen die Fristen von zwei bis hin zu zehn Jahren. Auch in anderen Rechtsbereichen gibt es Lösch- und Aufbewahrungsfristen. [33]

Es ist nach Art. 28 DSGVO [6] möglich, einen sogenannten Auftragsverarbeiter mit der Verarbeitung und Speicherung von Daten zu beauftragen. Dabei müssen aber einige Punkte beachtet werden.

> Ein *„… „Auftragsverarbeiter“ [ist] eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet…“. [6, Art. 4 Abs. 8]*

Grundlage der Auftragsverarbeitung ist ein Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter oder ein anderes Rechtsinstrument nach EU- oder Landesrecht. [6, Art. 28 Abs .3 Satz 1]. Dabei ist jedoch nicht einheitlich geregelt, welcher Art dieser Vertrag ist. In DSGVO Abs. 3 [6] ist geregelt, welche grundlegenden Inhalte im Vertrag bzw. mit dem Rechtsinstrument geregelt sein müssen. Dabei geht es vor allem um den Schutz personenbezogener Daten.

Als grundlegendes Gesetzeswerk für Verträge in der Bundesrepublik Deutschland (BRD) dient das Bürgerliche Gesetzbuch kurz BGB. Es gilt aber zu beachten, dass gerade Cloudanbieter ihren Sitz nicht immer in der BRD haben und deshalb auch Gesetze anderer Länder gelten können. Bei der Wahl eines Anbieters muss also ein Verantwortlicher darauf achten, dass der Auftragsverarbeiter sich an die Regelungen zum Datenschutz hält. Damit dies sichergestellt wird, sollte auf entsprechende Zertifikate und auf den Standort der Server geachtet werden. [18, S. 381f.]

Um einen passenden Anbieter auswählen zu können, ist der Kunde darauf angewiesen, dass der Anbieter entsprechende Angaben macht, auf deren Grundlage eine Entscheidung getroffen werden kann. Der C5:2020 (Cloud Computing Compliance Criteria Catalogue) Richtlinienkatalog des BSI [34, S. 32-35] verlangt dabei, dass ein Anbieter folgende Informationen an den Kunden für seine Entscheidung weitergibt:

- Gerichtsbarkeit und Lokation der Daten [34, S. 32-35]
- Verfügbarkeit des Dienstes, Störungsbeseitigung und Rechtsfolgen bei der Nichteinhaltung des Vertrags:
  Dieser Punkt umfasst auch die Klärung umstrittener Haftungsfragen zwischen Cloudanbieter und Kunde. [34, S. 32-35]
- Wiederanlaufparameter im Normalbetrieb [34, S. 32-35]
- Verfügbarkeit der Rechenzentren [34, S. 32-35]
- Umgang mit Ermittlungsanfragen staatlicher Stellen:
  Dazu gehören neben der Verifikation der Rechtsgrundlage auch die Information für den Kunden und Angaben darüber, ob der Anbieter in einem solchen Fall die Daten entschlüsseln und weitergeben kann sowie Widerspruchsmöglichkeiten des Kunden. Dabei gilt zu beachten, dass die Rechtsgrundlagen für die Befugnisse des Staates je nach Staat sehr unterschiedlich sein können. In Deutschland sind mögliche Rechtsgrundlagen in den Gesetzen der Bundes- und Landeskriminalämter, den Prozessordnungen der Gerichte und den Gesetzen der Nachrichtendienste geregelt. [34, S. 32-35]
- Zertifizierungen oder Bescheinigungen [34, S. 32-35]

Bei bestimmten Problemen können auch Regelungen des Telekommunikationsgesetzes (TKG) und des Telemediengesetzes (TMG) in Frage kommen. [18, S. 381f.]

Weiterhin gilt zu beachten, dass es für bestimmte Gruppen noch weitere Gesetze gibt, die zu bestimmten Anforderungen an den entsprechenden Cloudbackupdienst führen. So sind z.B. Unternehmen, Organisationen und Behörden der sogenannten KRITIS (Kritischen Infrastruktur) an das IT- Sicherheitsgesetz 2.0 gebunden und müssen somit die Richtlinien des BSI einhalten [35], [36]. Zur KRITIS gehören Wasser- und Energieversorgung, Ernährung, Finanz- und Versicherungswesen, Gesundheit, Informationstechnik und Telekommunikation, Abfallentsorgung, Medien und Kultur, Staat und Verwaltung sowie Transport und Verkehr [37].

Auch für Geheimnisträger stellen sich besondere Anforderungen, da es diesen in Deutschland verboten ist, ihre Daten an Dritte weiterzugeben. So können diese nur straffrei Clouddienste nutzen, wenn sie die Daten in ihrem System verschlüsseln und es für den Auftragsverarbeiter keine Möglichkeit gibt, diese zu entschlüsseln. Ansonsten würde sich der Kunde gemäß §203 StGB (Strafgesetzbuch) [38] -Verletzung von Privatgeheimnissen- strafbar machen.

„Darunter fallen unter anderem Ärzte, Psychologen, Anwälte, Notare, Verteidiger, Wirtschaftsprüfer, Buchprüfer, Steuerberater oder deren Bevollmächtigte, sowie Organe und Mitglieder deren Gesellschaften, als auch Beratungsstellen, Sozialarbeiter und Versicherungen. „ [39]

4.2 Richtlinien

Nachdem im Kapitel 3 ein Anforderungskatalog aus den theoretischen Grundlagen abgeleitet wurde und im Abschnitt 4.1 die rechtlichen Grundlagen näher beleuchtet wurden, soll nun ein Blick auf die Richtlinien und Veröffentlichungen staatlicher Stellen geworfen werden. Aus diesen wird ein Anforderungskatalog erstellt, der wesentliche Standards, die ein Cloudbackupsystem unter Zero Trust erfüllen sollte, beschreibt. Dabei wird, wie auch schon bei den rechtlichen Grundlagen, das Hauptaugenmerk auf Quellen aus der EU- insbesondere aus Deutschland- gerichtet. Da aber keine Publikation der EU oder Deutschlands sich konkret mit der Umsetzung eines Zero Trust Systems auseinandersetzt, wird auf eine Publikation des US- amerikanischen NIST zurückgegriffen [22].

4.2.1 Erarbeitung

Als Grundlage der Erarbeitung eines vollständigen Anforderungskatalogs dient hierbei der C5:2020 Kriterienkatalog [34], der um die Anforderungen an ein Zero Trust System erweitert bzw. dahingehend konkretisiert wird. Es wird sich dabei an den im C5:2020 Katalog beschriebenen 17 Bereichen orientiert.

4.2.1.1 Basis- und Zusatzkriterien des C5:2020 Kriterienkatalogs

Der erste Bereich ist dabei die **Organisation der Informationssicherheit**. Dazu gehört ein Informationssicherheitsmanagementsystem (ISMS), welches die Bestimmungen der ISO/IEC 27001 einhält. Diese muss für alle Organisationseinheiten, Standorte und Verfahren des Unternehmens gelten. Dabei muss der Aufbau, die Verwirklichung und die Aufrechterhaltung fortlaufend überprüft und verbessert werden. All dies muss auch dokumentiert werden. Dies kann auch zertifiziert werden. Eine Zertifizierung ist aber nicht zwingend erforderlich. [34, S. 37]

Des Weiteren muss von der Leitung des Cloudanbieters (einer oder mehreren natürlichen Personen) eine Leitlinie zur Informationssicherheit erarbeitet werden, über die alle Mitarbeiter des Anbieters und der Kunde informiert werden müssen. Diese orientiert sich an den Anforderungen des Kunden an die Informationssicherheit und den Aufgaben und Geschäftszielen des Anbieters. Sie beschreibt grundlegende Aspekte der Informationssicherheit wie Sicherheitsziele, angestrebtes Sicherheitsniveau sowie den organisatorischen Aufbau des ISMS. [34, S. 37f.]

Der Anbieter muss Schnittstellen und Abhängigkeiten von Drittanbietern, die Teile der Aufgaben übernehmen, dokumentieren und dem Kunden mitteilen. Besonderes Augenmerk muss dabei auf den Umgang mit Schwachstellen, Sicherheitsvorfällen und Störungen gelegt werden. Der Kunde wird so darüber informiert, dass er notwendige Tätigkeiten ausführen kann. Im Falle von Änderungen muss der Kunde rechtzeitig über diese informiert werden, so dass er mit Maßnahmen darauf reagieren kann, bevor die Änderungen umgesetzt werden. [34, S. 38]

Sollte es bei Aufgaben und Verantwortlichkeiten zum Konflikt kommen, müssen diese nach einer Risikobeurteilung getrennt werden. Sollte das aus organisatorischen oder technischen Gründen nicht möglich sein, muss eine Überwachung eingerichtet werden, um Änderungen- gleichgültig ob unbefugt, unabsichtlich oder missbräuchlich- zu erkennen und darauf reagieren zu können. [34, S. 39]

Als Grundlage der Risikobeurteilung dient eine Richtlinie für den Umgang mit Risiken. Diese Richtlinie muss, genauso wie andere Richtlinien, dokumentiert, kommuniziert und bereitgestellt werden (siehe auch Dokumentation, Kommunikation und Bereitstellung von Richtlinien und Anweisungen S. 37). Die Richtlinie muss sowohl die identifizierten Risiken als auch den Zusammenhang mit den Schutzzielen, die Eintrittswahrscheinlichkeiten und die Auswirkungen des Eintretens beinhalten. Des Weiteren müssen die Kriterien für die Akzeptanz von Risiken sowie die Priorisierung der Behandlung geregelt sein. Laut BSI-Kriterienkatalog [34] ist es zwingend notwendig, Maßnahmen zur Behandlung der Risiken und Akzeptanz der Restrisiken festzulegen sowie Regeln für deren Genehmigung festzuschreiben. Abschließend muss in der Richtlinie geregelt sein, wie die Dokumentation der Maßnahmen zur Risikobehandlung erfolgen soll, um konsistente, gültige und vergleichbare Ergebnisse zu erhalten. [34, S. 40f.]

Die Risikoprüfung erfolgt anlassbezogen, aber mindestens einmal im Jahr durch den Verantwortlichen. Um eine gute Bewertung und Erkennung der Risiken zu erreichen, ist es von großer Bedeutung, dass der Anbieter mit Behörden, Ministerien und Interessenverbänden in Kontakt steht, die ihn über neue Gefährdungen und Schwachstellen informieren, so dass diese Informationen in den Umgang mit Risiken und Schwachstellen eingebunden werden können. Sollte es sich beim Kunden um ein Unternehmen der KRITIS handeln, muss das Unternehmen sich auch beim Nationalen IT- Lagezentrum und dem CERT- Bund (Computer Emergency Response Team) informieren. [34, S. 39f.]

Der zweite Bereich beschäftigt sich mit den **Sicherheitsrichtlinien und Arbeitsanweisungen**. Dazu gehört unter anderem, dass diese einheitlich aufgebaut sind und an alle Mitarbeiter kommuniziert bzw. weitergegeben werden, die diese für ihre Arbeit benötigen. Die Richtlinien und Anweisungen müssen eine Versionsnummer besitzen um die Aktualität und Änderungen schnell erkennen zu können und von der Unternehmensleitung oder dazu beauftragtem Personal genehmigt werden. [34, S. 42]

Ebenso wie mindestens einmal jährlich eine Risikoprüfung stattfindet, müssen auch Anweisungen und Richtlinien, die sich mit der Sicherheit von Informationen auseinandersetzen, mindestens einmal jährlich auf ihre Aktualität und Angemessenheit von entsprechendem Personal geprüft werden. Bei der Prüfung müssen vor allem Änderungen im Verfahren der Bereitstellung des Dienstes sowie rechtliche und regulatorische Änderungen berücksichtigt werden. Bevor eine neue Version einer Richtlinie oder Anweisung gültig wird, muss diese genehmigt werden. [34, S. 43]

Sollte es zu Abweichungen von bestehenden Richtlinien oder Anweisungen kommen, müssen diese nach der Richtlinie zum Umgang mit Risiken geprüft werden und es ist zwingend erforderlich, sich eine Genehmigung dieser Ausnahme zu besorgen. Diese muss dokumentiert werden und ist zeitlich befristet. Außerdem muss sie mindestens einmal im Jahr überprüft werden. [34, S. 44]

Der dritte Bereich beschäftigt sich mit den Anforderungen an das **Personal.** Das Personal muss vor Beginn des Beschäftigungsverhältnisses auf Vertrauenswürdigkeit und nötige Qualifikation geprüft werden. Dazu gehört, soweit dies von der lokalen Gesetzgebung erlaubt ist, die Überprüfung der personenbezogenen Daten mittels des Personalausweises, die Überprüfung des Lebenslaufs und akademischer Titel bzw. der Abschlüsse, die Vorlage eines Führungszeugnisses bzw. eines nationalen Pendants und eine Risikobewertung hinsichtlich der Möglichkeit der Erpressbarkeit. [34, S. 45]

Weiterhin muss jeder Mitarbeiter in den Vertrags- und Beschäftigungsbedingungen auf die einzuhaltenden Richtlinien und Anweisungen zur Informationssicherheit hingewiesen und zu deren Einhaltung verpflichtet werden, bevor er Zugriff auf Daten und Systemkomponenten erhält. [34, S. 46]

Der Anbieter muss außerdem regelmäßige Schulungen und Sensibilisierungen für das Personal anbieten. Diese müssen fortlaufend anhand von Richtlinien- und Anweisungsänderungen sowie mit Blick auf neue Bedrohungslagen aktualisiert werden. Thematisiert werden sollten dabei der Umgang mit Systemkomponenten, Umgang mit Daten, aktuelle Bedrohungslagen und das Verhalten bei Sicherheitsvorfällen. Zusätzlich kann mit Hilfe von erzielten Lernerfolgen und Auswertungen der Erfolg der Schulungen und Sensibilisierungen gemessen werden. So können diese weiter verbessert werden. [34, S. 46f.]

Um die Einhaltung von Richtlinien und Anweisungen zu gewährleisten, muss ein Prozess zur Maßregelung definiert werden. Dabei gilt zu beachten, dass die Folgen eines Verstoßes mit der Art und Schwere des Verstoßes übereinstimmen. Die Angestellten müssen über mögliche Maßregelungen informiert und die Anwendung dokumentiert werden. [34, S. 47]

Die Mitarbeiter müssen außerdem über Verantwortlichkeiten, die über das Beschäftigungsverhältnis hinausgehen, informiert werden. Diese sind auch über eine Beendigung oder Änderung des Beschäftigungsverhältnisses hinaus gültig. [34, S. 48]

Als letzter Punkt gilt noch zu beachten, dass mit Angestellten sowie evtl. Dritten eine Vertraulichkeitsvereinbarung geschlossen werden muss, um Informationen und betriebliche Details zu schützen. Mit Dritten wird diese Vereinbarung zusammen mit dem Vertragsabschluss geschlossen; bei den eigenen Mitarbeitern, bevor diese Zugriff auf die Daten erhalten. Auch diese Vereinbarungen müssen mindestens einmal jährlich überprüft und gegebenenfalls aktualisiert werden. Über mögliche Änderungen muss das Unternehmen die entsprechenden Personen informieren und die neuen aktualisierten Vereinbarungen müssen mit diesen neu geschlossen werden. [34, S. 48f.]

Der vierte Bereich umfasst das sogenannte **Asset Management**. Dazu gehört unter anderem die Inventarisierung aller Werte. Diese kann automatisiert oder durch eine bzw. mehrere Personen durchgeführt werden. Es gilt dabei zu beachten, dass, solange diese Werte vorliegen, die Inventarisierung zu jedem Zeitpunkt vollständig, gültig, richtig und konsistent sein muss. Sollte es zu Änderungen kommen, müssen diese dokumentiert werden. Zusätzlich können Anwendungen zur Protokollierung und Überwachung der erfassten Informationen eingesetzt werden, um die Verletzung der Schutzziele schneller erkennen zu können und Gegenmaßnahmen einzuleiten. [34, S. 49f.]

Es muss weiterhin eine Richtlinie für den zulässigen Gebrauch und den sicheren Umgang mit Assets erstellt werden. Für diese gelten natürlich dieselben Anforderungen wie für die anderen Richtlinien. Außerdem sollte die Richtlinie Informationen über Genehmigungen für die Anschaffung, die Inbetriebnahme, die Instandhaltung, die Außerbetriebnahme, die Entsorgung, Inventarisierung, Klassifizierung und Kennzeichnung der Werte sowie Schutzmaßnahmen beschreiben. Weiterhin sollten Konfigurationen zur Fehlerbehandlung, Protokollierung, Verschlüsselung, Authentisierung und Autorisierung enthalten sein. Ebenso sollten Angaben zu Software- und Image-Versionen und Patches sowie zu weiteren Punkten, die die Sicherheit der Assets betreffen, gemacht werden. [34, S. 50f.]

Auf Basis dieser Richtlinie muss der Anbieter ein Verfahren zur In- und Außerbetriebnahme der Hardware entwickeln. Bei der Inbetriebnahme ist darauf zu achten, dass alle entstehenden Risiken identifiziert, analysiert und gemäß der Richtlinie behandelt wurden. Bei der Außerbetriebnahme muss darauf geachtet werden, dass alle Daten unwiederbringlich und vollständig gelöscht werden und die Datenträger vernichtet werden. Die beiden Prozesse benötigen eine Genehmigung. [34, S. 51f.]

Sollten an Mitarbeiter Assets zur Arbeit ausgehändigt werden, damit diese ihre Aufgaben erfüllen können, müssen die Assets nach Beendigung des Beschäftigungsverhältnisses wieder abgegeben werden. Dies bedarf zwingend eines Nachweises. Zusätzlich kann für die Verwaltung der Herausgabe und Rücknahme von Assets eine zentrale Stelle eingerichtet werden. [34, S. 53]

Es muss ein einheitliches Klassifizierungs- und Kennzeichnungssystem für Assets geschaffen werden. Dieses System orientiert sich am Schutzbedarf der Assets und wird von den Verantwortlichen erstellt. Dabei werden Schutzstufen für Vertraulichkeit, Integrität,

Verfügbarkeit und Authentizität festgelegt. Um für zusätzliche Sicherheit zu sorgen, können die Protokollierungs- und Überwachungssysteme die festgelegten Schutzbedarfe berücksichtigen und so bei Verstößen Priorisierungen treffen und das entsprechende Personal informieren. [34, S. 53f.]

Der fünfte Bereich beschäftigt sich mit der **physischen Sicherheit** der Rechenzentren. Aus der Informationssicherheitsrichtlinie und der Bewertung der physischen Risiken muss eine Sicherheitsanforderung für die Räumlichkeiten und die Gebäude verfasst werden. Bei dieser handelt es sich um ein Konzept oder eine Richtlinie. Damit gelten für diese dieselben Bedingungen wie für die anderen Richtlinien. Dabei müssen einige Risiken betrachtet und geeignete Lösungen gefunden werden. Dazu gehören Fehler bei der Planung, der Zutritt Unberechtigter, unzureichende Überwachung und Klimatisierung, Feuer und Rauch, Wasser, Stromausfälle und Verschmutzung. Sollte(n) das bzw. die Gebäude von Dritten betrieben werden, müssen die Kriterien für Subdienstleister erfüllt sein (siehe S. 37). Zusätzlich können Sicherheitsanforderungen für einen autarken Betrieb der Anlage bei außergewöhnlichen äußeren Ereignissen festgelegt werden. [34, S. 54f.]

Es müssen zwei Standorte geschaffen werden, die die Anforderungen der Sicherheitsrichtlinie für die Räumlichkeiten und Gebäude erfüllen und weit genug voneinander entfernt sind, um eine Redundanz zu erhalten, damit die Verfügbarkeit des Dienstes gewährleistet werden kann. Auch dies sollte mindestens einmal jährlich überprüft werden. Um einen noch bessere Georedundanz zu schaffen, können auch mehr als zwei Standorte geschaffen werden. [34, S. 56f.]

Eine weitere Anforderung an die physische Sicherheit ist der Perimeterschutz. Das heißt, dass die Gebäude und Räume solide und mit angemessenen Sicherheitsmaßnahmen versehen sind, um den Sicherheitsanforderungen gerecht zu werden. Die Sicherheitsmaßnahmen sind nur dann geeignet, wenn sie unberechtigten Zutritt rechtzeitig erkennen und verhindern. Das heißt, dass zum Beispiel alle Zugänge (Türen, Fenster, …) mindestens zehn Minuten einem Einbruchsversuch widerstehen (siehe auch DIN EN 1627). Zusätzlich kann auch Sicherheitspersonal angestellt werden, welches mindestens in Zweierteams das Gelände permanent überwacht. Zudem können Videoüberwachung und Einbruchsmeldeanlagen installiert werden. [34, S. 57]

Des Weiteren müssen die in der Sicherheitsanforderung für die Räumlichkeiten und die Gebäude festgelegten physischen Zutrittskontrollen umgesetzt werden. Dies wird durch ein Zutrittskontrollsystem gewährleistet. Dieses System umfasst ein Verfahren zur Vergabe und zum Entzug von Zutrittsberechtigungen (nach „Least- Privilege-“ und „Need-to-Know-Prinzip“), automatische Sperrung von Rechten, wenn diese 2 Monate nicht genutzt werden, automatischen Entzug von Rechten, wenn diese 6 Monate nicht genutzt werden, Zwei-Faktor- Authentisierung bei Bereichen mit Systemkomponenten. Besucher und Fremdpersonal werden getrennt erfasst, gekennzeichnet und bei der Arbeit beaufsichtigt. Außerdem müssen alle Zutritte protokolliert werden, damit jederzeit nachvollzogen werden kann, wann welche Person im Gebäude war. [34, S. 58]

Es müssen außerdem organisatorische und technische Maßnahmen getroffen werden, um den Schutz vor Feuer und Rauch zu gewährleisten. Dazu zählen die Schaffung von Brandabschnitten (Feuerwiderstandsdauer mind. 90 min.), Brandfrüherkennung mit automatischer Spannungsfreischaltung, Löschanlagen/ Sauerstoffreduzierung, Brandmeldeanlagen mit Verbindung zur Feuerwehr sowie regelmäßige Brandschutzbegehungen und Brandschutzübungen. Zusätzlich kann eine Überwachung der Umgebungsparameter stattfinden, damit starke Veränderungen erkannt und an das zuständige Personal weitergeleitet werden können. [34, S. 59]

Es muss auch für den Schutz der Versorgungseinrichtungen vor Ausfall gesorgt werden. Dazu gehören Redundanzen in der Kälte- und Stromversorgung, sowie der Einsatz von unterbrechungsfreier Stromversorgung (USV) und Netzersatzanlagen (NEA), die mindestens einmal jährlich überprüft werden. Es gehören aber auch die Instandhaltung dieser Einrichtungen und der Schutz der Stromversorgung und der Telekommunikation vor Beschädigung, Unterbrechung, Störung und Abhören dazu. Dies sollte mindestens alle 2 Jahre oder bei konkretem Verdacht geprüft werden. Zusätzlich können USV und NEA so konzipiert sein, dass der Betrieb des Dienstes mit ihnen mindestens 5 Tage lang weiterlaufen kann, ohne dass die Temperatur mehr als 3 K vom höchsten bis dahin gemessenen Normalwert abweicht. Es können auch zusätzlich genug Redundanzen geschaffen werden, so dass ein Ausfall eines einzelnen Tellkommunikationsnetzes nicht zu einem Ausfall des Dienstes führt. [34, S. 59f.]

Die letzte Anforderung im Bereich der physischen Sicherheit hängt mit dem Schutz vor Ausfall der Versorgungseinrichtungen zusammen. So müssen alle Betriebs- und Umgebungsparameter überwacht und geregelt werden, sodass, sollten diese einen Regelbereich verlassen, von entsprechendem Personal oder Systemkomponenten Gegenmaßnahmen eingeleitet werden können. [34, S. 61]

Der sechste Bereich des C5:2020 Katalogs beschäftigt sich damit, wie ein ordnungsgemäßer **Regelbetrieb** gewährleistet werden kann. Dazu gehört unter anderem das Kapazitätsmanagement, welches Planung, Überwachung, sowie Steuerung von Ressourcen umfasst. Bei der Planung gilt zu beachten, dass Prognosen bezüglich der zukünftig zu erwartenden Entwicklung der benötigten Kapazitäten berücksichtigt werden müssen, damit Systemüberlastung und Kapazitätsengpässe vermieden und so die vertraglichen Vereinbarungen eingehalten werden können. [34, S. 61f.]

Bei der Überwachung müssen technische und organisatorische Maßnahmen getroffen werden, die es ermöglichen, die Kapazitätsauslastung zu überwachen und die Provisionierung gemäß dem Vertrag anzupassen. Zusätzlich kann ein Portal für den Kunden geschaffen werden, welches die Informationen an den Kunden weiterleitet. [34, S. 62f.]

Bei der Steuerung der Ressourcen muss es dem Kunden möglich sein, entsprechend des Vertrags Systemressourcen zu steuern und zu überwachen. [34, S. 63]
Ein weiterer wichtiger Punkt für den Regelbetrieb ist der Schutz vor Schadprogrammen.

Hierbei werden sowohl an das Konzept als auch an die Umsetzung Anforderungen gestellt. Bei dem erarbeiteten Konzept handelt es sich um eine Richtlinie bzw. Anweisung (siehe S. 37). In diesem Konzept sollten die genutzten systemspezifischen Schutzmechanismen und die verwendeten Schutzprogramme auf Systemkomponenten und den Endgeräten der Mitarbeiter festgehalten werden. Zusätzlich können regelmäßige Reports zu Überprüfungen erstellt werden und vom Personal oder von Gremien überprüft und analysiert werden. Auch können bereits im Konzept Anweisungen enthalten sein, die die technischen Maßnahmen beschreiben. Um Kunden und Angestellte vor Schaden zu schützen werden regelmäßig Aktualisierungen durchgeführt. [34, S. 63f.]

Bei der Umsetzung gilt zu beachten, dass die im Konzept festgelegten Punkte beachtet und die verwendeten Schutzprogramme täglich aktualisiert werden. Zusätzlich kann die Konfiguration der Schutzmechanismen automatisch überwacht werden, damit Abweichungen von Vorgaben erkannt und an die zuständigen Mitarbeiter weitergeleitet werden können. [34, S. 64]

Ein weiterer wichtiger Teil der Gewährleistung eines ordnungsgemäßen Regelbetriebs ist die Datensicherung und -wiederherstellung. Auch hier gibt es verschiedene Unterpunkte, bei denen bestimmte Dinge beachtet werden müssen. So muss ein Konzept erarbeitet werden, in dem geregelt ist, in welchem Umfang und welcher Häufigkeit die Sicherung durchgeführt wird sowie die maximale RTO und RPO festgelegt wird. Außerdem muss die Sicherung verschlüsselt werden. Zugriff auf die Sicherungen dürfen nur autorisierte Personen haben. Zuletzt müssen die Tests der Wiederherstellungsverfahren festgehalten werden. Welche Anforderungen an die Tests gestellt werden, wird noch beschrieben (siehe S. 37). [34, S. 65]

Der Anbieter muss außerdem mit technischen und organisatorischen Maßnahmen die Datensicherung überwachen, damit Störungen schnell erkannt und behoben werden können und das Konzept eingehalten werden kann. Zusätzlich können dem Kunden die Protokolle der Sicherung oder eine Zusammenfassung dieser zur Verfügung gestellt werden, damit er überprüfen kann, dass die Vereinbarungen eingehalten werden. [34, S. 66]

Bei den Wiederherstellungstests gilt zu beachten, dass diese mindestens einmal jährlich durchgeführt werden und dass sie in geeigneter Art prüfen, ob vertragliche Vereinbarungen eingehalten werden. Sollte das nicht der Fall sein, muss dies an das zuständige Personal weitergegeben werden, damit die Abweichungen beurteilt und behoben werden können. Zusätzlich kann auch der Kunde über die Ergebnisse des Tests informiert werden und die Wiederherstellungstests können in das Notfallmanagement integriert werden. [34, S. 66f.]

Auch bei der Aufbewahrung der Backups gilt zu beachten, dass die Übertragung bzw. der Transport zum Remote-Standort der Sicherungen gesichert sein muss. Das heißt, sollte eine Übertragung über das Netz stattfinden, muss diese verschlüsselt werden. Für den Remote-Standort gelten dieselben Regeln wie für den Hauptstandort. [34, S. 67]

Der nächste Teilbereich ist die Protokollierung und Überwachung. Auch für diesen Bereich muss zuerst ein Konzept entwickelt werden. In diesem wird festgelegt, welche Ereignisse zu einer Verletzung der Schutzziele führen, wann Protokollierungen aktiviert, pausiert oder gestoppt werden, warum protokolliert wird und wie lange diese Protokolle aufbewahrt werden. Außerdem müssen Verantwortlichkeiten und Rollen für die Überwachung festgelegt und weitere Punkte geregelt sein. [34, S. 67f.]

Neben dieser Richtlinie muss bei der Protokollierung und Überwachung auch der Umgang mit Metadaten in einer Richtlinie geregelt werden. Dabei kann zusätzlich festgelegt werden, dass alle personenbezogenen Daten automatisch, soweit möglich automatisiert, aus den Protokollen gelöscht werden. [34, S. 68f.]

Es gilt weiterhin zu beachten, dass nur autorisierte Nutzer und Systeme Zugriff auf die Protokolle und Überwachung haben dürfen und dass eine Speicherung nur solange erfolgt, wie dies festgelegt wurde. Danach werden die Protokolle gelöscht. [34, S. 69f.]

Die Erkennung von Ereignissen, die die Schutzziele verletzen, muss nach den Richtlinien automatisiert werden, sodass auch Zusammenhänge zwischen Ereignissen erkannt und diese schnellstmöglich zur Beurteilung und dem Einleiten evtl. nötiger Maßnahmen an die zuständigen Personen oder Systeme weitergeleitet werden. [34, S. 70]

Es gilt aber auch bei der Aufbewahrung der Daten der Protokollierung einiges zu beachten. So müssen die Daten getrennt von der Quelle und unveränderlich gespeichert werden. Wie bereits beschrieben, müssen sie gelöscht werden, sobald der Zweck der Protokollierung nicht mehr gegeben ist. Außerdem muss eine Authentifizierung zwischen Protokollierungsserver und den Assets erfolgen. Zusätzlich kann der Anbieter auf Wunsch des Kunden auch die Protokollierung anpassen. [34, S. 70f.]

Die Zurechenbarkeit ist ein wichtiger Bestandteil von forensischen Analysen. Aus diesem Grund muss eine Protokollierung so stattfinden, dass ein Ereignis einem Nutzer zugeordnet werden kann und es müssen Schnittstellen existieren, um Sicherungen durchzuführen. Zusätzlich kann der Anbieter dem Kunden bei Vorfällen alle nötigen Protokolle zukommen lassen, sodass dieser selbst auch Analysen durchführen kann. [34, S. 71]

Bei der Konfiguration der Protokollierung und Überwachung ist zu beachten, dass, wie bereits öfter erwähnt, nur autorisierte Nutzer Zugriff auf diese haben dürfen. Da es bei Änderungen der Konfiguration zu Veränderungen am Informationssystem kommt, muss sich außerdem an die Richtlinie zur Änderung an Informationssystemen gehalten werden. Um für zusätzliche Sicherheit zu sorgen, kann bei Zugriff auf die Systemkomponenten eine Zwei-Faktor- Authentifizierung genutzt werden. [34, S. 71f.]

Um die Informationssicherheit zu gewährleisten, ist es nötig, dass die Protokollierungs- und Überwachungssysteme stets funktionsfähig sind. Aus diesem Grund muss eine automatische Überwachung dieser stattfinden, damit schnell auf Ausfälle reagiert werden kann.

Zusätzlich kann das System so aufgebaut werden, dass beim Ausfall einer Komponente nicht die Protokollierung und Überwachung ausfällt. [34, S. 72]

Auch für den Umgang mit Schwachstellen, Störungen und Fehlern muss eine Richtlinie verfasst werden. [34, S. 72f.]

Außerdem muss der Anbieter jährlich einen Penetrationstest von entsprechend qualifizierten Personen durchführen lassen um Schwachstellen besser erkennen zu können. Die Ergebnisse müssen bewertet und evtl. notwendige Verbesserungen vorgenommen werden. Zusätzlich kann man die halbjährlichen Tests auch ausschließlich von externen Dienstleistern durchführen lassen, um ein neutrales Ergebnis zu erhalten. [34, S. 73f.]

Damit die Angemessenheit, Eignung und Wirksamkeit des Umgangs mit den Schwachstellen beurteilt werden kann muss quartalsweise eine Analyse, Messung und Bewertung der Verfahren durchgeführt werden. [34, S. 74]

Der Anbieter muss den Kunden über Störungen im Regelbetrieb informieren, ihn, soweit dies angemessen ist, in die Behebung involvieren und über die Behebung informieren. [34, S. 74f.]

Es muss mindestens einmal im Monat eine automatisierte Prüfung auf bekannte Schwachstellen durchgeführt werden. Erkannte Schwachstellen müssen dabei in Schweregrade eingeteilt und behoben werden. Dabei kann sich am Common Vulnerability Scoring System (CVSS) orientiert werden. Sicherheitspatches der Kategorie „Kritisch“ sollten innerhalb von 3 Stunden, der Kategorie „Hoch“ innerhalb von 3 Tagen, der Kategorie „Mittel“ innerhalb eines Monats und Patches der Kategorie „Niedrig“ innerhalb von 3 Monaten eingespielt werden. [34, S. 75]

Um die Sicherheit des Systems zu gewährleisten, muss dieses nach den üblichen Standards gehärtet werden. Es müssen also die entsprechenden Bausteine des BSI IT- Grundschutz- Kompendiums angewendet werden. Das Vorgehen muss dokumentiert werden. Zusätzlich kann eine automatische Überprüfung der Vorgaben zur Härtung durchgeführt werden, damit Abweichungen erkannt und an das zuständige Personal weitergeleitet werden. [34, S. 75f.]

Um die Integrität und Vertraulichkeit der Kundendaten gewährleisten zu können, müssen die Daten der unterschiedlichen Kunden auf Basis einer Risikoanalyse strikt voneinander getrennt werden (siehe auch S. 37). Dies gilt insbesondere, wenn die Daten sich auf derselben physischen oder virtuellen Ressource befinden. Dies kann zusätzlich durch den Einsatz von LUN Binding und LUN Masking erfolgen. [34, S. 76f.]

Der siebente Bereich beschäftigt sich mit dem **Identitäts- und Berechtigungsmanagement**. Auch hierfür muss zunächst eine Richtlinie für Zugangs- und Zugriffsberechtigungen verfasst werden. Für diese Richtlinie gelten dieselben Anforderungen wie für die anderen Richtlinien auch (siehe S. 37). Basierend auf Sicherheitsanforderungen und Geschäftsidee

wird ein Rollen- und Rechtskonzept erstellt, aus dem Zugangs- und Zugriffsberechtigungen für Mitarbeiter und Systemkomponenten, die in automatisierte Autorisierungsprozesse eingebunden sind, abgeleitet werden. [34, S. 77ff.]

Für die Vergabe und Änderung der Zugriffs- und Zugangsberechtigungen sind geregelte Verfahren zu entwickeln. Diese müssen die Vorgaben des Rollen- und Rechtskonzepts sowie der Richtlinie zur Verwaltung von Zugangs- und Zugriffsberechtigungen erfüllen. Zusätzlich kann es dem Kunden über ein Portal ermöglicht werden, selbst Zugriffs- und Zugangsberechtigungen zu vergeben. [34, S. 79]

Weiterhin ist es zur Sicherheit wichtig, dass Zugangsberechtigungen, die über einen Zeitraum von zwei Monaten nicht verwendet wurden, gesperrt werden. Die Entsperrung kann nur mit der Genehmigung einer autorisierten Instanz vorgenommen werden. Sollte eine Zugangsberechtigung sechs Monate nicht genutzt werden, wird diese endgültig entzogen. Der Mitarbeiter oder die Systemkomponente kann dann nur über ein neues Vergabeverfahren wieder Zugangs- bzw. Zugriffsrechte erhalten. [34, S. 79f.]

Des Weiteren ist es wichtig, mindestens einmal jährlich zu prüfen, ob der Mitarbeiter bzw. die Systemkomponente erteilte Rechte noch benötigt. Geprüft wird dies durch autorisiertes Personal. Sollte erkannt werden, dass Rechte nicht mehr benötigt werden, sind diese spätestens bis sieben Tage nach der Prüfung zu entziehen. Zusätzlich können privilegierte Berechtigungen mindestens halbjährlich überprüft werden. [34, S. 80f.]

Bei der Vergabe oder Änderung von privilegierten Zugriffsberechtigungen gilt zu beachten, dass diese zeitlich befristet sind und nur für die Aufgabenwahrnehmung genutzt werden dürfen. Außerdem werden die Aktivitäten von Nutzern mit privilegierten Zugriffsberechtigungen protokolliert und automatisch auf Ereignisse, die einen Missbrauch darstellen, durchsucht. Sollte ein Verstoß festgestellt werden, wird dieser Sicherheitsvorfall an die Zuständigen weitergeleitet und gegebenenfalls Disziplinarmaßnahmen eingeleitet. (siehe auch S. 52). [34, S. 81f.]

Sollte, aus welchem Grund auch immer, vom Anbieter auf die Daten des Kunden zugegriffen werden, ist dieser bis spätestens 72 Stunden nach dem Zugriff zu informieren. Dabei muss dem Kunden mitgeteilt werden, ob die Verschlüsselung aufgehoben wurde, warum, wann, wie lange, wie und in welchem Umfang auf die Daten zugegriffen wurde, damit der Kunde eine Risikobeurteilung durchführen kann. Zusätzlich kann auch die Regelung getroffen werden, dass der Kunde jedem Zugriff vorher zustimmen muss. In diesem Fall werden dem Kunden vorab die Informationen zugesandt, die ansonsten im Nachhinein mitgeteilt werden. [34, S. 82]

Um die Vertraulichkeit der Informationen zu schützen, muss die Zuteilung von Authentifizierungsinformationen in einem geordneten Verfahren vergeben werden. Sollte es sich dabei um Passwörter handeln, muss die Vertraulichkeit dadurch sichergestellt werden, dass Nutzer bei der Erstanmeldung das Initialpasswort, welches nach 14 Tagen seine Gültigkeit

verliert, ändern müssen. Außerdem darf es technisch nicht möglich sein, Passwörter zu vergeben, die nicht den Passwortvorgaben entsprechen. Sollte es zu einer Änderung oder Zurücksetzung des Passworts kommen, muss der Kunde darüber informiert werden. Des Weiteren werden nur starke Passworthashfunktionen zur Speicherung genutzt. Sollte es dabei zu Abweichungen kommen, sind diese einer Risikoanalyse zu unterziehen und Maßnahmen einzuleiten. Zusätzlich kann von den Nutzern verlangt werden, eine Erklärung zu unterschreiben, in der der Nutzer sich verpflichtet, Authentifizierungsinformationen vertraulich zu behandeln. [34, S. 83]

Als Authentisierungsmechanismen wird für die Produktionsumgebung eine Zwei- oder Mehr- Faktor- Authentisierung genutzt. Wenn der Nutzer angemeldet ist, erfolgen weitere Authentifizierungen über Passwörter, digital signierte Zertifikate oder andere Verfahren mit gleichwertigem Sicherheitsniveau. Digital signierte Zertifikate werden dabei nach der Richtlinie zur Schlüsselverwaltung (siehe S.46) verwaltet. Für die Passwortvergabe wird eine Risikobewertung durchgeführt und aus dieser eine Richtlinie erstellt. (siehe S. 37) Die Einhaltung dieser Richtlinie ist durch die Konfiguration so umzusetzen, dass gegen diese technisch nicht verstoßen werden kann. Zusätzlich kann auch der Zugriff auf die Nicht- Produktionsumgebung durch Zwei- oder Mehr- Faktor- Authentisierung geregelt werden. Nach der Anmeldung erfolgen weitere Authentifizierungen im gleichen Maße wie nach der Anmeldung in der Produktionsumgebung. [34, S. 83f.]

Ein weiterer Teilbereich des Anforderungskatalogs des BSI ist der Bereich der **Kryptographie und des Schlüsselmanagements**. Auch hier muss eine Richtlinie erstellt werden. Diese beschäftigt sich mit den technischen und organisatorischen Maßnahmen, die für die Nutzung von Verschlüsselungsverfahren und der Schlüsselverwaltung getroffen werden müssen. Die Richtlinie beschreibt, wie starke Verschlüsselungsverfahren und sichere Netzprotokolle genutzt werden. Des Weiteren enthält sie Vorschriften für den Einsatz von Verschlüsselungen. Diese werden bestimmt durch die Informationsklassifikation (siehe S.39) und die verwendeten Kommunikationskanäle. Des Weiteren werden die Anforderungen an ein sicheres Schlüsselmanagement definiert und rechtliche und regulatorische Verpflichtungen betrachtet. Welche Verfahren als starke Verschlüsselungsverfahren und sichere Netzprotokolle gelten, kann sich mit der technischen Entwicklung ändern. Aus diesem Grund sind die aktuellen Fassungen der folgenden technischen Richtlinien (TR) des BSI zu berücksichtigen:

- TR-02102-1 Empfehlungen und Schlüssellängen [40]
- TR-02102-2 Verwendung von TLS [41]
- TR-02102-3 Verwendung von Internet Protocol Security (IPSec) und Internet Key Exchange (IKEv2) [42]
- TR-02102-4 Verwendung von Secure Shell (SSH) [43] [34, S. 84f.]

Bei der Übertragung von Daten über das öffentliche Netz muss der Anbieter technische Maßnahmen zur Verschlüsselung und Authentifizierung treffen. Zusätzlich kann er dies auch auf jegliche Übertragung von Daten ausweiten. [34, S. 85f.], [41]

Alle gespeicherten Daten müssen durch technische Maßnahmen und Verfahren verschlüsselt werden. Der private Schlüssel darf dabei nur dem Kunden bekannt sein. Ausnahmen bedürfen einer vertraglichen Regelung. Um Kunden, die z. B. Geheimnisträger sind, zu schützen, können jegliche Ausnahmen ausgeschlossen werden. [34, S. 86]

Des Weiteren müssen Verfahren und technische Maßnahmen zur Schlüsselverwaltung getroffen werden. Dazu gehört die Schlüsselgenerierung für kryptographische Systeme und Applikationen, die Einholung und Ausstellung von Public-Key- Zertifikaten, die Provisionierung und Aktivierung von Schlüsseln, die Nutzung eines separierten Key-Management-Systems mit der Beschreibung, wie autorisierte Nutzer Zugriff auf dieses haben, Richtlinien zur Änderung und Aktualisierung kryptographischer Schlüssel mit Bedingungen und Umsetzung, der Umgang, Entzug und die Löschung von Schlüsseln. [34, S. 87] „Falls preshared keys verwendet werden, sind die Besonderheiten in Bezug auf sichere Nutzung dieses Verfahrens gesondert aufgeführt“ [34, S. 87]

Ein weiterer wichtiger Sicherheitsaspekt bei der Planung, der Konfiguration und dem Betrieb eines Cloudsystems ist die **Kommunikationssicherheit**. Dabei müssen technische Schutzmaßnahen getroffen werden, die auf der Basis einer Risikoanalyse nach der Richtlinie für den Umgang mit Risiken (siehe S. 37) erarbeitet werden. Dazu gehört, dass durch diese Maßnahmen netzbasierte Angriffe erkannt werden und zeitnah darauf reagiert werden kann (z.B. DDoS [Distributed Denial of Service] Angriffe). Des Weiteren werden die durch die Maßnahmen erfassten Daten in einem übergreifenden SIEM- System analysiert, so dass auch korrelierende Ereignisse erkannt werden. Auch hierfür muss wieder eine Richtlinie erstellt werden. Zusätzlich kann der Anbieter technische Maßnahmen treffen, die verhindern, dass ein unbekanntes Gerät physischen oder virtuellen Zugriff auf das Netz erhält. [34, S. 87f.]

Zudem müssen vom Anbieter Sicherheitsanforderungen entworfen, veröffentlicht und bereitgestellt werden, die die Herstellung einer Verbindung zum Netz des Anbieters regeln. Der Anbieter muss festlegen, wann Sicherheitszonen separiert werden, wie Cloudkunden logisch oder physisch zu trennen sind, welche Kommunikationsbeziehungen, Netz- und Anwendungsprotokolle genutzt werden. Des Weiteren muss er Regelungen zur Trennung von Administrations- und Monitorings- Datenverkehr treffen. Ebenso muss geregelt werden, inwieweit interne standortübergreifende und externe Kommunikation zugelassen werden. [34, S. 88f.]

Eine Trennung zwischen vertrauenswürdigen und vertrauensunwürdigen Netzen auf Basis einer Risikobewertung ist zwingend erforderlich. Auf Grundlage dieser Trennung werden unterschiedliche Sicherheitszonen separiert und unterschiedliche Sicherheitsanforderungen für diese Bereiche angewandt. Maßnahmen müssen so konzipiert werden, dass sie die Vertrauenswürdigkeit des Netzes berücksichtigen und der Datenverkehr entsprechend überwacht wird. Mindestens einmal jährlich muss die Konzeption und Konfiguration der Überwachung überprüft werden. Die dabei erkannten Risiken müssen nach der Richtlinie zum Umgang mit Risiken (siehe S. 37) bewertet werden und Maßnahmen gegebenenfalls

angepasst werden. Des Weiteren müssen in definierten Abständen alle verwendeten Dienste, Protokolle und Ports überprüft werden. Sollte ein Protokoll verwendet werden, das als unsicher gilt, müssen auch die kompensierenden Maßnahmen festgelegt und begründet werden. [34, S. 89]

Für netzübergreifende Zugriffe müssen an den Netzperimetern Sicherheitsgateways eingerichtet werden. Welche netzübergreifenden Zugriffe stattfinden dürfen, muss auf Basis einer Sicherheitsbewertung entschieden werden. An den Netzperimetern können für zusätzliche Sicherheit redundante, hoch verfügbare Sicherheitsgateways eingerichtet werden. [34, S. 89f.]

Es müssen außerdem gesonderte Netze für die administrative Verwaltung der Infrastruktur und den Betrieb von Managementkonsolen geschaffen werden, die physisch und logisch vom Netz des Kunden getrennt sind. Diese können mit Hilfe von Multi- Faktor- Authentifizierung geschützt werden. Auch müssen erzeugte virtuelle Maschinen, die für die Migration erzeugt wurden, von den anderen Netzen getrennt werden. [34, S. 90]

Des Weiteren muss eine klare Dokumentation des Netzaufbaus existieren, damit im Störungsfall das Netz schnell wieder aufgebaut werden kann. In der Dokumentation wird erfasst, welche Subnetze existieren, wie das Netz zoniert und segmentiert ist und wo (geografische Lage) die Daten der Kunden gespeichert sind. [34, S. 91]

Es muss eine Richtlinie zur Datenübertragung verfasst werden, in der mit Bezug zur Klassifikation der übertragenen Daten technische und organisatorische Maßnahmen geregelt sind. Dazu gehören Maßnahmen, die den Schutz der Übertragung vor Abfangen, Manipulieren, Kopieren, Modifizieren, Umleiten oder Vernichten gewährleisten (Anforderungen an die Richtlinie: siehe S. 37) [34, S. 92]

Der nächste Bereich beschäftigt sich mit der **Portabilität und Interoperabilität** des Dienstes. Das heißt, es muss eine Möglichkeit geschaffen werden, den angebotenen Dienst auch über andere Clouddienste oder IT- Systeme anzusprechen. Außerdem müssen gespeicherte Daten nach dem Ende des Auftragsverhältnisses gelöscht werden können. Dafür müssen einige Anforderungen erfüllt werden. [34, S. 92]

So wird eine dokumentierte Eingangs- und Ausgangsschnittstelle, über die der Dienst angesprochen werden kann, benötigt. Aus der Dokumentation muss hervorgehen, wie diese Schnittstelle genutzt werden kann. Die Kommunikation mit dem Dienst muss über standardisierte Kommunikationsprotokolle laufen, damit die Vertraulichkeit und Integrität der Daten gewährleistet werden können. Sollte zur Kommunikation ein nicht vertrauenswürdiges Netz genutzt werden, muss die Kommunikation gemäß der verschlüsselten Übertragung (siehe S.46) von Daten verschlüsselt werden. Die Dokumentation wird aktuell gehalten. Wie umfangreich diese Dokumentation ist, orientiert sich am Informationsbedarf des Kunden. [34, S. 92f.]

Im Vertrag muss außerdem geregelt sein, was mit den Daten nach Beendigung des Auftragsverhältnisses passiert. Dazu gehört, in welchem Umfang, Format und in welcher Art die Daten übergeben werden, die Frist innerhalb derer die Daten beim Anbieter gelöscht werden, die Frist, die benötigt wird, um die Daten zur Verfügung zu stellen und welche Mitwirkungspflichten und Verantwortlichkeiten der Kunde erfüllen muss, um die Daten zu erhalten. Bei der Definition dieser Punkte müssen sowohl Kunden- und Anbieterwunsch als auch rechtliche und regulatorische Anforderungen berücksichtigt werden. Zusätzlich können mindestens einmal jährlich die vereinbarten vertraglichen Bedingungen auf Aktualität geprüft und bei Bedarf mit Zustimmung des Kunden angepasst werden. [34, S. 93f.]

Wenn das Auftragsverhältnis beendet wird, müssen die Vereinbarungen, die im Vertrag geregelt wurden, eingehalten werden. Dazu gehört auch die Löschung der Daten. Die Löschung umfasst dabei nicht nur den aktuellen Datenbestand, sondern auch Metadaten und Datensicherungen. Zu beachten ist dabei auch, dass das Löschverfahren so umgesetzt wird, dass die Daten selbst mit forensischen Mitteln nicht wiederhergestellt werden können. [34, S. 94f.]

Der elfte Bereich beschäftigt sich mit den Anforderungen, die an die **Beschaffung, Entwicklung und Änderung von Informationssystemen** gestellt werden müssen. Auch für diesen Bereich muss wieder eine Richtlinie geschaffen werden. Diese beschreibt die technischen und organisatorischen Maßnahmen, die für die Entwicklung des Dienstes nötig sind. Die Richtlinie muss aber auch Anweisungen für den gesamten Lebenszyklus des Dienstes beinhalten und sich dabei auf anerkannte Methoden und Standards stützen, so z.B. auf die ISO/IEC 27034. Es muss dabei vor allem die Sicherheit in der Software-Entwicklung, Software- Bereitstellung und im Betrieb berücksichtigt werden. Zusätzlich kann bei der Beschaffung darauf geachtet werden, dass Produkte mindestens ein Zertifikat der Prüftiefe EAL (Evaluation Assurance Level) 4 nach der „Common Creteria for Information Technology Security Evaluation“ kurz Common Creteria (CC) besitzen. Sollten beschaffte Produkte kein solches Zertifikat haben, kann eine Risikobewertung nach der Richtlinie zum Umgang mit Risiken durchgeführt werden. [34, S. 95f.]

Der Anbieter hat aber auch die Möglichkeit, Entwicklungsprozesse für den Dienst oder für einzelne Komponenten auszulagern. Dabei muss mit dem Entwickler vertraglich geregelt werden, dass die Entwicklung nach anerkannten Standards und Methoden durchgeführt wird und dass eine Abnahmeprüfung vorgenommen wird, um die Erfüllung der vereinbarten Anforderungen zu kontrollieren und die Qualität der erbrachten Leistung zu verifizieren. Außerdem muss festgelegt werden, welche Nachweise der Überprüfung von dem Entwickler erbracht werden müssen, um Schwachstellen ausschließen zu können. [34, S. 96]

Es muss auch noch eine weitere Richtlinie verfasst werden, die die nötigen technischen und organisatorischen Maßnahmen zur Verwaltung von Änderungen in der Konfiguration, Funktionalität und Sicherheit der Systemkomponenten beschreibt. Dabei muss besonderes Augenmerk auf die Kriterien der Risikobewertung, der Priorisierung und Kategorisierung von Änderungen, sowie deren Art und auf den Umfang der Testung gelegt werden.

Weiterhin muss geregelt werden, welche Genehmigungen für die Entwicklung und Implementierung von Änderungen erforderlich sind sowie, wie deren Freigabe in der Produktionsumgebung erfolgt. In der Richtlinie werden außerdem die Anforderungen an die Durchführung und Dokumentation von Tests festgeschrieben. Zudem werden Anforderungen bezüglich der Funktionstrennung bei der Entwicklung, bei Tests und der Freigabe von Änderungen festgelegt. Des Weiteren werden Anforderungen an die Kundeninformation nach Änderungen, Anforderungen an die Dokumentation von Änderungen sowie Anforderungen für Notfalländerungen definiert. [34, S. 96f.]

Der Anbieter muss außerdem ein Programm besitzen, das die Mitarbeiter über Standards und Methoden bei der Software- Entwicklung und Bereitstellung informiert und den sicheren Umgang mit entsprechenden Werkzeugen ermöglicht. Dieses Programm muss regelmäßig aktualisiert werden. [34, S. 97f.]

Wenn es zu Änderungen gemäß der Richtlinie zur Änderung von Informationssystemen kommt, muss der Anbieter eine Risikobewertung dieser durchführen, um Auswirkungen abschätzen zu können und so die Änderungen priorisieren und kategorisieren zu können. Zusätzlich kann der Kunde über Anlass, Zeitpunkt, Dauer, Art und Umfang der Änderungen informiert werden, bevor diese umgesetzt werden, damit er eine eigene Risikobeurteilung durchführen kann. Sollte eine Änderung der höchsten Risikokategorie umgesetzt werden, muss der Kunde informiert werden. [34, S. 98]

Wie bereits festgestellt wurde, müssen Änderungen Tests unterzogen werden. Bei diesen gilt zu beachten, dass sie in Art und Umfang der Risikobeurteilung entsprechen und dass sie durch qualifiziertes Personal oder automatisierte Testverfahren durchgeführt werden. Dabei können Kunden je nach Vertrag in die Testung eingebunden werden. Für die im Test erkannten Schwachstellen und Fehler muss ein Schweregrad festgelegt werden. Die Fehler und Schwachstellen werden nach definierten Kriterien bewertet und es werden zeitnah Maßnahmen zur Behebung oder Migration vorgenommen. [34, S. 98f.]

Bei der Protokollierung der Änderungen gilt zu beachten, dass die Systemkomponenten und Werkzeuge einem Rollen- und Rechtskonzept gemäß der Richtlinie für Zugriffs- und Zugangsberechtigungen entsprechen und durch Autorisierungsmechanismen Personen oder Systemkomponenten identifiziert werden. Das heißt, die Protokollierung muss so konfiguriert werden, dass die Änderungen auf eine Person oder Systemkomponente zurückgeführt werden können. [34, S. 99]

Es müssen weiterhin Möglichkeiten der Versionskontrolle geschaffen werden, die es ermöglichen Änderungen nachvollziehen zu können und bei Auftreten von Fehlern und Schwachstellen ältere Versionen wiederherzustellen. Zusätzlich kann das Verfahren so erstellt werden, dass eine ältere Version wiederhergestellt wird, dabei aber keine Kundendaten verloren gehen. [34, S. 100]

Die Freigabe der Änderungen am Dienst kann nur von autorisiertem Personal oder Systemkomponenten vorgenommen werden. Die Entscheidung wird dabei auf Basis der vorher definierten Kriterien getroffen und erfolgt vor der Bereitstellung in der Produktionsumgebung. Der Kunde wird in diesen Prozess, den vertraglichen Bedingungen entsprechend, eingebunden. [34, S. 100f.]

Die Test- oder Entwicklungsumgebung muss dabei zwingend physisch oder logisch von der Produktionsumgebung getrennt sein, damit kein Unbefugter Zugriff auf die Daten des Kunden erlangen kann, sich keine Schadsoftware ausbreiten kann und Änderungen an Systemkomponenten ausgeschlossen sind. Es dürfen auch keine Daten aus der Produktionsumgebung zum Testen verwendet werden, [34, S. 101]

Ein weiterer wichtiger Bereich ist die **Steuerung und Überwachung von Dienstleistern und Lieferanten**. Auch für diesen Bereich müssen wieder Anweisungen und Richtlinien verfasst werden. Diese beinhalten Vorgaben zur Risikobeurteilung durch Bezug von Leistungen durch Dritte, Klassifizierung Dritter auf Grundlage der Risikobeurteilung, Feststellung, ob es sich bei Dritten um Subdienstleister handelt, Anforderungen an Informationssicherheit bei der Verarbeitung, Speicherung oder Übertragung durch Dritte, Anforderungen an Schulungen und Sensibilisierungen des Personals für Informationssicherheit sowie rechtliche und regulatorische Anforderungen und Anforderungen für den Umgang mit Schwachstellen, Sicherheitsvorfällen und Störungen. Es müssen außerdem noch Vorgaben für vertragliche Vereinbarungen, Vorgaben für die Überwachung und Vorgaben für die Weitergabe von Daten an die Dienstleister, die von Dritten eingesetzt werden, enthalten sein. Zusätzlich kann der Anbieter vertraglich mit seinen Subdienstleistern vereinbaren, dass diese regelmäßige Bericht erstatten und von unabhängigen Stellen kontrolliert werden. Sollte die Berichterstattung nicht möglich sein, können auch Informations- und Prüfungsrechte vereinbart werden, um die Prüfung der Einhaltung von Vereinbarungen durch qualifiziertes Personal durchführen zulassen. [34, S. 101f.]

Bei der Risikobeurteilung der Drittdienstleister und Lieferanten nach der Richtlinie zur Steuerung und Überwachung von Dritten ist zu beachten, dass diese, bevor sie zur Bereitstellung beitragen, überprüft werden. Qualifiziertes Personal muss außerdem mindestens einmal jährlich prüfen, ob die Einschätzung weiterhin zutrifft. Die Beurteilung umfasst dabei den Schutzbedarf der Informationen, die durch den Dritten verarbeitet, gespeichert oder übertragen werden, Auswirkungen einer Schutzbedarfsverletzung, Abhängigkeit von den Lieferanten und Dienstleistern und Prüfung auf Alternativen. Der Prozess muss dokumentiert werden. [34, S. 103]

Der Anbieter muss außerdem ein Verzeichnis von Dienstleistern und Lieferanten führen. In diesem Verzeichnis werden jeweils Firmenname, Anschrift, Lokation der verarbeiteten und gespeicherten Daten, Ansprechpartner beim Dritten, Ansprechpartner beim Anbieter, die Beschreibung der Leistung, die Risikobeurteilung (Klassifizierung), der Beginn des Leistungsbezugs und der Nachweis für die Einhaltung vertraglicher Vereinbarungen festgehalten. Dieses Verzeichnis wird mindestens einmal jährlich auf Vollständigkeit, Richtigkeit und Gültigkeit geprüft. [34, S. 103f.]

Der Anbieter muss überwachen, dass sich Dienstleister und Lieferanten an die Vereinbarungen halten, damit die Informationssicherheit gewährleistet werden kann. Dafür müssen regelmäßig die von den Dritten erbrachten Nachweise überwacht werden. Dazu gehören Berichte über die Qualität der erbrachten Leistung, Zertifikate, Berichterstattungen unabhängiger Dritter und Aufzeichnungen zum Umgang mit Schwachstellen, Sicherheitsvorfällen und Störungen durch die Dritten. Durch die regelmäßige Überprüfung können die Dritten klassifiziert werden und die Risikobeurteilung besser durchgeführt werden. Wenn Verstöße erkannt werden, müssen diese nach der Richtlinie zum Umgang mit Risiken behandelt werden. Zusätzlich kann eine automatische Überwachung der Konfiguration, Leistung und Verfügbarkeit von Systemkomponenten sowie eine automatische Überwachung der Reaktionszeit bei Störungen und Sicherheitsvorfällen eingerichtet werden. Dabei können auch automatisiert Wiederherstellungszeiten überwacht werden. Die automatisierten Überwachungssysteme leiten Verstöße automatisch an den Anbieter weiter, damit der sie beurteilen und Maßnahmen einleiten kann. [34, S. 104f.]

Für Dritte, von denen der Anbieter eine sehr hohe Abhängigkeit hat, muss dieser eine Ausstiegsstrategie erarbeiten. Diese Strategie muss mit den Planungen zur betrieblichen Kontinuität abgestimmt werden. Sie umfasst die Analyse von potentiellen Kosten, Auswirkungen für das Unternehmen, ressourcentechnische und zeitliche Auswirkungen eines Wechsels, die Planung von Rollen, Verantwortlichkeiten und benötigten Ressourcen für den Übergang sowie Erfolgskriterien, Indikatoren für die Überwachung der Leistungserbringung und Ereignisse, die zum Ausstieg führen. [34, S. 105f.]

Der dreizehnte Bereich beschäftigt sich mit den Anforderungen zum **Umgang mit Sicherheitsvorfällen**. Auch hier muss wieder eine Richtlinie geschaffen werden. In dieser Richtlinie beschreibt der Anbieter die Vorgaben zur Klassifikation, Priorisierung und Eskalation von Sicherheitsvorfällen und legt technische und organisatorische Maßnahmen fest, die Reaktionen auf bekannte Sicherheitsvorfälle ermöglichen. Es werden außerdem Schnittstellen für Incident Management und zum Business Continuity Management geschaffen und ein CERT eingerichtet, das zur Lösung von Sicherheitsvorfällen beiträgt. Die Kunden müssen zeitnah über Sicherheitsvorfälle informiert werden. Zusätzlich können in Anweisungen Regelungen zur beweisfesten Sicherung von verdächtigen Daten gemacht werden. Auch können Analysepläne für Sicherheitsvorfälle erstellt werden, die Auswertemethodiken nutzen, die auch vor Gericht anerkannt werden. [34, S. 106f.]

Bei der Bearbeitung der Sicherheitsvorfälle muss darauf geachtet werden, dass das Personal die entsprechende Qualifikation besitzt. Sollte kein Mitarbeiter die entsprechende Qualifikation besitzen, muss ein externer Dienstleister die Klassifizierung, Priorisierung und Ursachenanalyse übernehmen. Zusätzlich kann auch mindestens einmal im Jahr eine Simulation eines Sicherheitsvorfalls oder eines Angriffs gemacht werden, um den Identifizierungs-, Analyse- und Abwehrprozess zu testen. [34, S. 107f.]

Nachdem eine Lösung für einen Sicherheitsvorfall gefunden wurde, muss diese dokumentiert und in Form eines Berichtes dem betroffenen Kunden zur Kenntnisnahme übermittelt werden. Zusätzlich kann man eine aktive oder passive (Lösung gilt nach Ablauf einer Frist als akzeptiert) Zustimmung eines Kunden für die Lösung verlangen. Zudem wird der Bericht nicht nur betroffenen Kunden, sondern allen Kunden zugestellt. Auch kann zusätzlich vertraglich geregelt werden, welche Daten dem Kunden im Fall eines Sicherheitsvorfalls zur eigenen Analyse mitgeteilt werden. [34, S. 108]

Der Anbieter muss alle Mitarbeiter und Geschäftspartner vertraglich dazu verpflichten, alle Sicherheitsvorfälle, die mit dem angebotenen Dienst im Zusammenhang stehen, an eine zentrale Stelle zu melden. Es muss dabei klar kommuniziert werden, dass Falschmeldungen keine negativen Folgen haben. [34, S. 109f.]

Es müssen Mechanismen zur Messung von Art und Umfang von Sicherheitsvorfällen existieren sowie Mechanismen zu deren Überwachung und Meldung. Die bei der Auswertung von Sicherheitsvorfällen gewonnenen Informationen werden dazu genutzt, neue Schutzmaßnamen zu entwerfen. [34, S. 109]

Der nächste Bereich beschäftigt sich mit der **Kontinuität des Geschäftsbetriebes und dem Notfallmanagement**. Die Verantwortung für das Kontinuitäts- und Notfallmanagement trägt die Unternehmensleitung. Diese muss dafür sorgen, dass sich Prozesse etablieren, Richtlinien eingehalten werden und genügend Ressourcen zur Verfügung stehen. Sie muss außerdem dafür sorgen, dass alle Mitarbeiter zum Kontinuitäts- und Notfallmanagement beitragen. [34, S. 110]

Es müssen weiterhin Richtlinien und Anweisungen zur Ermittlung der Auswirkungen von Störungen des Dienstes oder des Unternehmens erstellt werden. [34, S. 110f.]

Aus der Business Impact Analyse muss ein Rahmenwerk für die Planung der Betriebskontinuität und des Geschäftsplans erstellt werden. Die Inhalte des Rahmenwerks müssen eingeführt, dokumentiert und angewendet werden sowie anerkannte Standards einhalten. [34, S. 111f.]

Die erstellten Pläne müssen mindestens einmal jährlich oder nach größeren organisatorischen oder umgebungsbedingten Veränderungen überprüft, getestet und aktualisiert werden. Die Tests müssen dabei Kunden und Lieferanten sowie Dienstleister einbinden. Eine Dokumentation der Testergebnisse wird bei zukünftigen Maßnahmen berücksichtigt. Es

können zusätzlich zu den Tests auch Übungen zu in der Vergangenheit aufgetretenen Sicherheitsvorfällen eingebunden werden. [34, S. 112f.]

Der fünfzehnte Bereich beschäftigt sich mit der **Compliance**, sprich mit den einzuhaltenden gesetzlichen, regulatorischen, selbstauferlegten oder vertraglichen Anforderungen. Dazu gehört, dass der Anbieter die entsprechenden Anforderungen und Verfahren zu deren Einhaltung definiert sowie dokumentiert. [34, S. 113f.]

Es muss außerdem eine Richtlinie für die Planung und Durchführung von Audits geschaffen werden. In dieser wird geregelt, wie Lesezugriffe auf Systemkomponenten zur Prüfung und Durchführung der geplanten Aktivitäten nötig sind. Weiterhin muss geregelt sein, dass Aktivitäten, die zur Störung des Dienstes oder Nichteinhaltung von Vereinbarungen führen können, in planmäßigen Wartungszeiträumen und außerhalb der Lastspitzen stattfinden. Die Aktivitäten müssen dabei stets protokolliert und überwacht werden. Zusätzlich kann der Anbieter dem Kunden vertraglich zusichern, dass dieser Informations- und Prüfungsrechte erhält. [34, S. 114]

Der Anbieter muss außerdem mindestens einmal jährlich durch qualifiziertes Personal interne Audits am ISMS durchführen. Dabei wird dieses auf seine Compliance überprüft. Es muss auf die Einhaltung aller gesetzlichen, regulatorischen, selbstauferlegten (z.B. Richtlinien und Anweisungen) und vertraglichen Anforderungen geachtet werden. Sollten bei den Audits Schwachstellen und Abweichungen erkannt werden, müssen diese nach der Richtlinie zum Umgang mit Risiken geprüft und evtl. Gegenmaßnahmen eingeleitet werden. Zusätzlich können die Audits durch Verfahren zur automatischen Überwachung ergänzt werden. Diese prüfen die Konfiguration von Systemkomponenten, die Leistung und Verfügbarkeit dieser, die Reaktionszeit bei Störungen und Sicherheitsvorfällen und Wiederherstellungszeiten. Erkannte Schwachstellen und Abweichungen werden automatisch an die Zuständigen weitergeleitet. Zudem kann dem Kunden ermöglicht werden, bestimmte vertragliche Anforderungen in Echtzeit zu überwachen. [34, S. 115]

Die oberste Leitung muss in regelmäßigen Abständen über die Informationssicherheitsleistung des ISMS informiert werden, damit sie deren Eignung, Angemessenheit und Wirksamkeit mindestens einmal jährlich in einer Managementbeurteilung des ISMS bewerten kann. [34, S. 115f.]

Der sechzehnte Bereich beschäftigt sich mit dem **Umgang mit Ermittlungsanfragen staatlicher Stellen**. Diese müssen von qualifiziertem Personal juristisch beurteilt werden um sicherzustellen, dass die Anfrage auf anwendbarem und gültigem Recht basiert und festzustellen, welche Schritte einzuleiten sind. [34, S. 116]

Der Kunde muss über den Eingang der Ermittlungsanfrage informiert werden, solange dies nicht gegen die anwendbare Rechtsgrundlage verstößt oder ein eindeutiger Hinweis auf eine rechtswidrige Handlung im Zusammenhang mit der Nutzung des Dienstes existiert. [34, S. 117]

Des Weiteren darf nur auf die Daten des Kunden zugegriffen und diese offengelegt werden, wenn die juristische Beurteilung ergeben hat, dass eine anwendbare rechtsgültige Rechtsgrundlage existiert und dieser entsprochen werden muss. [34, S. 117f.]

Beim Zugriff und der Offenlegung der Daten muss darauf geachtet werden, dass diese wirklich nur die Daten betrifft, die Teil der Ermittlungsanfrage sind. Sollte aus irgendeinem Grund diese Eingrenzung nicht möglich sein, muss der Anbieter alle Daten pseudonymisieren und anonymisieren, die nur anderen Kunden zugeordnet werden können. [34, S. 118.]

Der letzte Bereich des C5:2020 Katalogs ist die **Produktsicherheit**. Dazu gehört, dass der Anbieter dem Kunden eine Leitlinie und Empfehlung für die sichere Nutzung des Dienstes erstellt und zugänglich macht. Die Leitlinie enthält Informationen zur sicheren Konfiguration, Installation und Nutzung des Dienstes, soweit diese im Verantwortungsbereich des Kunden ist. Der Umfang und die Art der Information ist dabei abhängig vom Bedarf des Kunden. In der Richtlinie enthalten sein müssen eine Anleitung zur Konfiguration, Informationen zu bekannten Schwachstellen und Aktualisierungsmechanismen, Fehlerbehandlungs- und Protokollierungsmechanismen, Rollen- und Rechtekonzepte (mit Risiken bestimmter Kombinationen) sowie Dienste und Funktionen der Administration. Auch diese Informationen werden regelmäßig aktualisiert. [34, S. 118f.]

Um die Produktsicherheit zu gewährleisten, muss weiterhin eine Identifikation von Schwachstellen des Clouddienstes, die durch den Softwareentwicklungsprozess entstehen können, stattfinden. Dafür können statische Code Analysen, dynamische Code Analysen, Code Reviews oder eingeholte Informationen über Schwachstellen genutzt werden. Identifizierte Schwachstellen müssen dann beurteilt und zeitnah behoben bzw. migriert werden. Zusätzlich können jährlich durch Dritte Code Reviews und Penetration-Tests durchgeführt werden, um Schwachstellen besser zu erkennen. [34, S. 119f.]

Der Anbieter muss ein tagesaktuelles Online-Register, das bekannte Schwachstellen der verwendeten Assets enthält, besitzen oder auf ein solches verweisen. Die Schwachstellen werden im Register nach dem CVSS dargestellt und sind leicht einsehbar. Des Weiteren muss es möglich sein, auf Grundlage des Registers eine Risikobewertung durchzuführen. Im Register müssen auch entsprechende Software-Aktualisierungen angegeben sein und es muss beschrieben werden, ob der Kunde oder der Anbieter diese durchführt. Zusätzlich können für den Kunden automatisierte Aktualisierungsmechanismen geschaffen werden. Der Kunde muss dann den Aktualisierungen nur noch zustimmen. [34, S. 120f.]

Der Dienst muss außerdem mit Fehlerbehandlungs- und Protokollierungsmechanismen ausgestattet werden, damit der Kunde die Möglichkeit hat, sicherheitsrelevante Informationen über den Dienst, seine bereitgestellten Daten oder Funktionen zu erhalten. Aus den Informationen muss hervorgehen, auf welche Daten, Dienste und Funktionen, die der Kunde zur Verfügung hat, durch wen und wann zugegriffen wurde, zu welchen Störungen es bei manuellen oder automatischen Aktionen gekommen ist und welche sicherheitsrelevanten Parameter (Konfigurationen, Fehlerbehandlungs- und

Protokollierungsmechanismen, Authentifizierungsmechanismen, Autorisierungen, Kryptographie, Kommunikationssicherheit) geändert wurden. Diese Informationen müssen unveränderlich gespeichert werden, vor unberechtigtem Zugriff geschützt werden und es muss dem Kunden möglich sein, diese zu löschen. Sollte der Kunde für die Protokollierungen zuständig sein, muss der Anbieter geeignete Protokollierungsfunktionen bereitstellen. Zusätzlich kann man dem Kunden ermöglichen, über eine Schnittstelle Informationen abzurufen, die dieser dann mit Hilfe eines eigenen SIEM überwachen kann. [34, S. 121f.]

Der Anbieter muss dem Kunden sichere Authentisierungsmechanismen anbieten, die der Kunde an den Zugangspunkten einrichten muss. Diese Mechanismen erzwingen eine starke Authentisierung der Nutzer, privilegierter Nutzer, IT-Komponenten und Anwendungen, die mit dem Dienst interagieren. Zusätzlich kann der Dienst eine Out-of-Band-Authentisierung (OOB) anbieten. Bei dieser werden die Faktoren über unterschiedliche Kanäle übertragen. [34, S. 122f.]

Es muss außerdem ein geeignetes Session Management eingerichtet werden. Dieses muss dem aktuellen Stand der Technik entsprechen und die Verbindung vor bekannten Angriffen schützen. Das Session Management muss weiterhin Mechanismen zur Erkennung von Inaktivität implementiert haben, die die Session bei Inaktivität automatisch invalidieren. Für das Erkennen von Inaktivität können Zeitmessungen erfolgen. Das Zeitintervall, nach welchem Inaktivität festgestellt wird, kann dabei vom Anbieter oder Kunden konfiguriert werden. [34, S. 123]

Um die Vertraulichkeit von Authentisierungsinformationen zu gewährleisten, müssen bei der Passwortsicherheit dieselben Maßnahmen wie bei den Authentifizierungsmechanismen des Identitäts- und Berechtigungsmanagements eingehalten werden. (Siehe S. 45) [34, S. 123f.]

Der Anbieter muss dem Kunden außerdem ein Rollen- und Rechtskonzept für die Verwaltung von Zugriffs- und Zugangsberechtigungen zur Verfügung stellen. In diesem Konzept beschreibt er Rechteprofile, die dafür geeignet sind, das „Least-Privilege-Prinzip“, „Need-to-Know-Prinzip“ und die Funktionstrennung zwischen operativen und kontrollierenden Funktionen umzusetzen. [34, S. 124f.]

Der Anbieter muss Zugriffskontrollen einrichten, die überprüfen, ob Nutzer oder IT-Komponenten die Berechtigungen für das Durchführen der geplanten Aktion besitzen. Die Funktionsfähigkeit dieser Autorisierungsmechanismen muss vor dem Bereitstellen neuer Funktionen oder vor der Umsetzung von Änderungen an den Autorisierungsmechanismen bestehender Funktionen geprüft werden. Sollten dabei Schwachstellen auffallen, sind diese zu beurteilen, in Schweregrade einzuordnen und zeitnah zu beheben. Sollten sie nicht behoben werden, müssen sie in das Online-Register eingetragen werden. Zusätzlich können diese Zugriffskontrollen attributbasiert durchgeführt werden. Dadurch wird ermöglicht, dass granulare und kontextbezogene Überprüfungen anhand mehrerer Attribute des Nutzers oder der IT-Komponente durchgeführt werden können. [34, S. 125]

Sollte der Dienst eine Möglichkeit zum Software-defined Networking (SDN) bieten, muss die Vertraulichkeit der Daten des Kunden durch geeignete SDN-Verfahren gewährleistet werden. Die Funktionsfähigkeit der SDN-Funktionen muss, bevor dem Kunden neue SDN-Funktionen bereitgestellt werden, überprüft werden. Auch hier erkannte Mängel müssen beurteilt und behoben werden. [34, S. 125f.]

Zuletzt muss der Anbieter eine Möglichkeit zur Bestimmung des geografischen Ortes (Land), an dem die Daten verarbeitet und gespeichert werden, für den Kunden schaffen. Dies muss beim Aufbau der Cloudarchitektur berücksichtigt werden. [34, S. 127]

4.2.1.2 Anforderungen an den Backup- Dienst

Nachdem nun die Anforderungen, die durch den C5:2020-Kriterienkatalog an den Anbieter gestellt werden, näher beschrieben wurden, stellt sich die Frage, wie dieser angepasst bzw. erweitert werden muss, um die speziellen Anforderungen für ein Cloudbackupsystem unter Zero Trust abzubilden.

Da es für Cloudbackupsysteme keinen eigenen Anforderungskatalog gibt, muss man sich an der Theorie und an Ausschnitten aus anderen Anforderungskatalogen orientieren. So kann für den Backupdienst anhand des C5- Katalogs [34] folgendes abgeleitet werden: Der Anbieter muss mit dem Kunden eine Richtlinie für die Datensicherung und -wiederherstellung erarbeiten. Weiterhin müssen technische und organisatorische Maßnahmen zur Überwachung der Datensicherung und -wiederherstellung getroffen werden. Der Anbieter muss mindestens einmal im Jahr einen Wiederherstellungstest durchführen und die Daten müssen verschlüsselt an den Backupserver gesendet werden. Zusätzlich können die Überwachungsprotokolle oder eine Zusammenfassung dieser an den Kunden übermittelt werden. Auch die Testergebnisse des Wiederherstellungstests können als zusätzliche Leistung dem Kunden zur Verfügung gestellt werden.

Aus der Theorie ergeben sich weitere Anforderungen, denen ein Backupdienst gerecht werden muss. So ist es nötig, dass die Zeitabstände, in denen das Backup erstellt wird, konfiguriert werden können. Es muss außerdem möglich sein, dass der Backupdienst Änderungen im Datenbestand des Kunden erkennt und nur diese sichert, um Speicherplatz zu sparen. Des Weiteren muss die Sicherungszeit möglichst minimiert werden. Die Backups müssen so gespeichert werden, dass nur der Eigentümer darauf Zugriff hat. Es muss außerdem möglich sein, jederzeit mehrere Backuppunkte wiederherstellen zu können. Des Weiteren muss eine Möglichkeit geschaffen werden, Schadsoftware zu erkennen, damit diese die Backups nicht beschädigen kann. Der Dienst muss eine Erkennung unvollständiger oder manipulierter Sicherungen möglich machen und fehlerhafte oder fehlende Backups kompensieren können. Die Backupdaten müssen außerdem verschlüsselt auf dem Backupserver gespeichert werden. Zusätzlich kann dieser Backup- und Recoveryprozess automatisiert werden und die Einhaltung der 3-2-1-Daten-Backup-Regel gewährleistet werden. Dies ist, sollte die Zusatzregel zur geografischen Redundanz (physische Sicherheit) des C5:2020- Kriterienkatalogs eingehalten werden, automatisch gegeben (vgl. S. 31 und S.

40). Um die Sicherheit des Backupdienstes zu gewährleisten, muss sich außerdem an die Anforderungen zur Produktsicherheit des C5:2020- Kriterienkatalogs gehalten werden.

4.2.1.3 NIST Anforderungen an ein Netzwerk unter ZT

Die Anforderungen des Kriterienkatalogs des BSI müssen im Hinblick auf die Einhaltung der Zero Trust Bedingungen jedoch noch angepasst und ergänzt werden.

Wie bereits in der Theorie beschrieben, ist die Grundannahme der ZT- Architektur, dass keinem Netzwerk vertraut werden kann und deshalb eine kontinuierliche Bewertung und Analyse der Risiken durchgeführt werden muss. Rose et. al. beschreiben in der Special Publication 800-207 des NIST die Anforderungen, die ein ZT- Netzwerk erfüllen muss. Dabei ist es möglich, schrittweise die ZT- Prinzipien umzusetzen und so Hybridformen eines ZT- basierten und eines perimeterbasierten Ansatzes zu schaffen. Dies ist möglich, da das ZT- Prinzip eine Sammlung von Leitprinzipien für Workflows, Systemdesign und Operationen ist, die auch unabhängig voneinander für mehr Sicherheit sorgen können. [22, S. 1]

Für die Umsetzung definieren Rose et.al. [22] sieben Grundsätze des ZT sowie zehn Anforderungen an den Netzwerkaufbau, die für die Umsetzung eines optimalen ZT-Netzwerkes notwendig sind. Die Grundsätze des ZT sind danach:

1. Alle Datenquellen und Datenverarbeitungsdienste werden als Ressource gesehen. [22, S. 6f.]

2. Die gesamte Kommunikation muss unabhängig vom Standort des Netzwerkes gesichert werden. Das heißt, dass auch Zugriffsanfragen von Systemkomponenten oder Nutzern, die zum eigenen Netzwerk gehören, überprüft und überwacht werden müssen. [22, S. 6f.]

3. Der Zugriff auf einzelne Unternehmensressourcen wird pro Session gewährt. Das bedeutet, dass sich jeder Teilnehmer für jeden Zugriff auf eine Ressource authentifizieren muss. Die Berechtigung für eine Ressource gewährt nicht automatisch Zugriff auf eine andere Ressource. [22, S. 6f.]

4. Der Zugang zu Ressourcen wird durch eine dynamische Verfahrensweise bestimmt. Dazu gehören das Überwachen der Identität von Clients, Diensten und angefragten Assets sowie weiterer Verhaltens- und Umgebungsattribute. Dies beinhaltet die Umsetzung des Need- to- Know- Prinzips und des Least- Privilege- Prinzips als Teil einer dynamischen Zugangs- und Zugriffsverwaltung auf Basis verschiedener Attribute und Artefakte, die zur Authentifizierung genutzt werden können. [22, S. 6f.]

5. Das Unternehmen überwacht und protokolliert den gesamten Datenverkehr. Dies umfasst, dass die Sicherheitspositionen bei Ressourcenabruf ständig neu bewertet werden müssen. Aus diesem Grund sollte ein Continuous diagnostics and mitigation (CDM) System durchgesetzt werden, um den Zustand aller Geräte und Anwendungen zu überwachen, die

Zugriff auf Ressourcen haben, und nötige Patches oder Fixes durchzuführen. Sollte ein System zu große Schwachstellen aufweisen, muss das CDM außerdem Verbindungen zu Unternehmensressourcen verhindern. Dafür ist ein robustes Monitoring- und Berichterstattungssystem notwendig. [22, S. 6f.]

6. Alle Authentifizierungen und Autorisierungen sind dynamisch und werden streng durchgesetzt, bevor ein Zugriff gewährt wird. Dafür ist ein kontinuierlicher Zyklus von Zugangsbeschaffung, Zugangskontrolle und Bedrohungseinschätzung nötig, der ständig neu bewertet und angepasst werden muss. Das Unternehmen muss außerdem ein Identity, Credential and Access Management (ICAM) und ein Asset Management System besitzen. Es muss zudem Multi- Faktor- Authentifizierung für Zugriffe oder ein System des kontinuierlichen Monitorings mit einem Konzept der Re- Authentifizierung und Re- Autorisierung auf Basis der Benutzeraktionen und der in einer Richtlinie definierten Voraussetzungen nutzen. Dabei muss ein ausgewogenes Verhältnis zwischen Sicherheit, Verfügbarkeit, Nutzbarkeit und Wirtschaftlichkeit angestrebt werden. [22, S. 6f.]

7. Das Unternehmen sammelt über den aktuellen Zustand der Anlagen, der Netzwerkinfrastruktur und der Kommunikation so viele Informationen wie möglich und nutzt diese zur Verbesserung der Sicherheit. [22, S. 6f.]

Zu den zehn Anforderungen an den Netzwerkaufbau gehören nach Rose et. al. [22]:

1. Grundlegende Netzwerkanbindung:
Dazu gehört ein LAN (Local Area Network), das über die grundlegenden Netzwerkinfrastrukturen verfügt. [22, S. 21f.]

2. Das Unternehmen muss in der Lage sein, den Sicherheitsstatus der Assets, die ihm gehören oder von ihm gemanagt werden, sowie der entsprechenden Geräte beurteilen und kontrollieren zu können. [22, S. 21f.]

3. Das Unternehmen ist in der Lage, den gesamten Netzwerkdatenverkehr zu überwachen und so Zugriffsanfragen zu erkennen und diese an die PE weiterzuleiten. Auf Basis dieser Überwachung können Richtlinien dynamisch angepasst und aktualisiert werden und das PE angepasst werden. [22, S. 21f.]

4. Das Erreichen einer Unternehmensressource ist ohne PEP nicht möglich. Dies erfordert technische Maßnahmen, die verhindern, dass durch einfache Anfragen Zugriff auf die Ressourcen genommen werden kann. Das heißt, das PEP richtet die Kommunikationswege ein und die Ressourcen dürfen ohne Zugriff auf das PEP nicht auffindbar sein. Dabei gilt zu beachten, dass dies bei bestimmten Komponenten (z. B. DNS [Domain Name System] - Servern) nicht möglich ist. [22, S. 21f.]

5. Datenebene und Kontrollebene sind logisch getrennt.
Das heißt, PE, PA und PEP befinden sich in einem logisch separierten Netzwerk, auf das Assets nicht unmittelbar zugreifen können. Die Datenebene wird dabei für den

Anwendungs- und Dienstdatenverkehr und die Kontrollebene von PE, PA und PEP zur Kommunikation und Verwaltung genutzt. Das PEP muss in der Lage sein, Nachrichten sowohl von der Datenebene als auch von der Kontrollebene zu erhalten und zu senden. [22, S. 21f.]

6. Die Assets müssen die PEP- Komponente erreichen können.
Um dies umzusetzen, gibt es unterschiedliche Möglichkeiten. So kann ein Netzwerkportal, ein Netzwerkgerät oder ein Software Agent genutzt werden. Das ist notwendig, damit die Komponenten Zugriff auf Dienste und Ressourcen erhalten können. [22, S. 21f.]

7. Das PEP ist die einzige Komponente, die auf die PA als Teil eines Ablaufs zugreifen kann.
Dies ist notwendig, damit ein Kommunikationsweg zwischen einem Client und einem Server aufgebaut werden kann. Das heißt auch, dass jeder Datenverkehr ein oder mehrere PEPs durchlaufen muss. [22, S. 21f.]

8. Remote- Assets sollten auf Ressourcen zugreifen können, ohne die Unternehmensnetzinfrastruktur durchlaufen zu müssen. [22, S. 21f.]

9. Die Entscheidungsprozesse des ZT- Netzwerks müssen skalierbar sein, um Änderungen in den Prozesslasten berücksichtigen zu können.
Da die PEs, PAs und PEPs Schlüsselkomponenten sind, muss bei der Planung und beim Aufbau dieser Komponenten die erwartete Auslastung berücksichtigt werden und rasch skalierbar sein, da es sonst zu Verzögerungen oder Ausfällen im Netz kommen kann. [22, S. 21f.]

10. Es kann anhand von Richtlinien und anderen Faktoren festgelegt werden, dass bestimmte Assets auf bestimmte Ressourcen nicht zugreifen können. So kann beispielsweise aus Sicherheitsgründen der Zugriff von Mobilgeräten unterbunden werden. [22, S. 21f.]

Für die Umsetzung von ZT gibt es unterschiedliche Ansätze, die sich dahingehend unterscheiden, welche Komponenten verwendet werden und wie die Regeln bestimmt werden. Diese Ansätze müssen alle Grundsätze des ZT erfüllen. Eine vollständige ZT- Lösung setzt jedoch alle drei dieser Ansätze um. Diese drei Ansätze sind eine verbesserte Identitätsverwaltung, Mikrosegmentierung und die netzbasierte Segmentierung. [22, S. 11]

Bei der verbesserten Identitätsverwaltung ist die Identitätsbestimmung der Nutzer und Systemkomponenten der wichtigste Teil der Richtliniengestaltung. Das heißt, der wichtigste Faktor ist der Besitz der entsprechenden Zugriffsrechte auf Ressourcen. Alle anderen Faktoren dienen nur dazu, diese anzupassen. Das heißt auch, die einzelnen Ressourcen und PEP- Komponenten müssen eine Möglichkeit haben, Objekte zu authentifizieren oder die Anfrage an einen Richtlinienmoduldienst weiterzuleiten bevor Zugriff auf die Ressourcen gewährt wird. [22, S. 11f.]

Bei der Mikrosegmentierung verteilt das Unternehmen einzelne Ressourcen oder Ressourcengruppen in einzelne Netzsegmente, die durch Sicherheitsgateways geschützt werden. Das Gateway kann dabei aus einer oder mehreren PEP- Komponenten bestehen. Für eine volle Funktionsfähigkeit muss ein Identity- Governance- Programm (IGP) vorhanden sein. Die wichtigste Voraussetzung für diesen Ansatz ist, dass die PEP- Komponenten verwaltet werden und in der Lage sein sollten, nach Bedarf zu reagieren und sich neu zu konfigurieren, um auf Bedrohungen oder Änderungen im Arbeitsablauf zu reagieren. [22, S. 12] Bei der netzbasierten Segmentierung wird die Netzwerkinfrastruktur genutzt, um das ZT-Prinzip zu implementieren. Dafür kann ein Overlay- Netzwerk genutzt werden. Solche Ansätze werden auch als Software Defined Perimeter (SDP)- Ansätze bezeichnet und umfassen häufig Konzepte, von SDN und Intent- based Networking (IBN). Bei diesem Ansatz dient der PA als Netzwerkcontroller, der das Netzwerk basierend auf den Entscheidungen des PEs einrichtet und konfiguriert. Die Clients stellen dabei weiterhin Zugriffsanfragen über die PEPs, die von der PA- Komponente verwaltet werden. [22, S. 12f.]

Zur Umsetzung der Prinzipien und Ansätze für eine ZT- Architektur müssen eine Reihe von Komponenten gegeben sein. Die Kernkomponente ist das PDP/ PEP- Gateway sprich: das SG, das aus PEP und PDP besteht. Der PDP wird dabei in PE und PA unterteilt. [22, S. 5-11]
Neben diesen Komponenten müssen- wie bereits an einigen Stellen beschrieben- noch weitere Komponenten eingebunden werden. Dazu gehört das CDM- System, das Informationen über den aktuellen Zustand des Systems sammelt, Aktualisierungen an den Konfigurationen und Softwarekomponenten vornimmt und die Informationen an den PE weiterleitet. Das CDM- System ist außerdem für die Identifikation und Durchsetzung von Richtlinien auf Nicht- Unternehmensgeräten verantwortlich. [22, S. 10]

Das Industry- Compliance- System stellt sicher, dass das Unternehmen sich an alle regulatorischen Vorschriften hält. [22, S. 10]

Eine weitere Komponente sind die Threat Intelligence Feeds. Diese sammeln Informationen aus internen und externen Quellen, die der PE dabei helfen, Zugriffsentscheidungen zu treffen. Dazu gehören zum Beispiel bekannt gewordene Schwachstellen sowie neuentdeckte Angriffe. [22, S. 10]

Das Unternehmen muss eine Komponente schaffen, die Systemaktivitäten und den Netzwerkdatenverkehr und andere Ereignisse überwacht und protokolliert und Feedback zum Sicherheitsstatus der Informationssysteme des Unternehmens liefert. [22, S. 10]

Des Weiteren muss eine Datenzugriffsrichtlinie erstellt werden, in der Attribute, Regeln und Richtlinien für den Zugriff auf Unternehmensressourcen geregelt sind. Diese Datenzugriffsrichtlinie kann codiert oder dynamisch von der PE generiert werden. [22, S. 10f.] Weiterhin wird eine Public Key Infrastructure (PKI) benötigt. Diese generiert und protokolliert die Zertifikate, die für Ressourcen sowie Nutzer, Dienste und Anwendungen ausgestellt wurden. [22, S. 11]

Es wird ein ID- Verwaltungssystem benötigt. Dieses erstellt, speichert und verwaltet Benutzerkonten und Identitätsdatensätze. Das System enthält die erforderlichen Nutzerinformationen und weitere Merkmale wie zugeordnete Rollen, Zugriffsattribute und zugewiesene Assets. Die Komponente wird häufig mit anderen Systemen verknüpft (z. B. PKI), die Artefakte erzeugen, die Benutzerkonten zugeordnet werden können. Zuletzt muss ein SIEM-System eingebunden werden. [22, S. 11]

4.2.1.4 Zusammenführung

Es zeigt sich also, dass einige der Anforderungen, die an ein ZT- System gestellt werden müssen, bereits im C5:2020 Kriterienkatalog des BSI als Basis- bzw. als Zusatzkriterium berücksichtigt wurden. Diese Anforderungen müssen für ein Cloudbackupsystem unter Zero Trust in einigen Bereichen jedoch angepasst, ergänzt und erweitert werden. Die wichtigsten Aspekte sollen an dieser Stelle kurz dargestellt werden:

So müssen im Bereich der **Organisation der Informationssicherheit** nicht nur Aufgaben und Verantwortlichkeiten, die zueinander in Konflikt stehen, getrennt werden. Unter ZT ist die Trennung von Aufgaben und Verantwortlichkeiten im Sinne einer Mikrosegmentierung zwingend erforderlich. Dies umfasst die Trennung von Ressourcen oder Ressourcengruppen in verschiedene Netzsegmente, die durch Sicherheitsgateways geschützt werden. Des Weiteren muss die netzwerkbasierte Segmentierung ergänzt werden. Dafür können Overlay-Netzwerke genutzt werden. Die PA dient dabei als Netzwerkcontroller, der auf Basis der Entscheidung des PEs das Netzwerk einrichtet und konfiguriert. Es muss berücksichtigt werden, dass die Clients nur Anfragen über PEPs stellen können.

Auch im Bereich des **Asset Management** müssen Änderungen vorgenommen werden. So wird die Inventarisierung der Assets sowie die Nutzung dieser Informationen bei der Protokollierung und Überwachung zur Basisanforderung. Es wird außerdem eine ständige Kontrolle und Überwachung aller Assets notwendig.

Im Bereich des **Regelbetriebs** müssen in allen Teilbereichen, ausgenommen ist die Datensicherung und -wiederherstellung, Änderungen vorgenommen werden. Beim Kapazitätsmanagement müssen auch bei der Planung der PDP/PEP- Gateways Prognosen in die Planung eingebunden werden, um Störungen im Arbeitsablauf zu vermeiden. Die regelmäßige Aktualisierung sowie die automatische Überwachung der Konfigurationen werden im Teilbereich des Schutzes vor Schadprogrammen zur Basisanforderung und durch ein CDM-System gesteuert und überwacht. Bei der Protokollierung und Überwachung wird die Zwei- oder Mehr- Faktor- Authentifizierung für den Zugriff auf Systemkomponenten zur Basisanforderung. Des Weiteren wird unter ZT eine dynamische Anpassung der Richtlinien auf Grundlage der PE- Entscheidungen und des CDM- Systems zur Zustandsüberwachung aller Geräte und Anwendungen nötig. Der Umgang mit Schwachstellen, Störungen und Fehlern wird um Threat Intelligence Feeds ergänzt. Diese sammeln Informationen aus internen und externen Quellen für Verbesserung des PEs.

Das **Identitäts- und Berechtigungsmanagement** ist unter ZT so anzupassen, dass alle Ressourcen und PEP- Komponenten eine Möglichkeit haben, Objekte zu authentifizieren oder ein Richtlinienmodul zu erreichen, das dies übernimmt. Auch müssen alle Authentifizierungen und Autorisierungen dynamisch sein und streng durch gesetzt werden. Des Weiteren wird die Multi- Faktor- Authentifizierung für Zugriffe zur Basisanforderung oder als Alternative zu dieser ein System des kontinuierlichen Monitorings mit einem Konzept der Re-Authentifizierung und Re-Autorisierung auf Basis der Benutzeraktionen und Richtlinien ergänzt.

Der Bereich **Kryptographie und Schlüsselmanagement** wird dahingehend verändert, dass die technischen Maßnahmen zur starken Verschlüsselung und Authentifizierung bei der Übertragung von Daten zur Basisanforderung werden.

Bei der **Kommunikationssicherheit** müssen die größten Veränderungen vorgenommen werden, da sich der Netzwerkaufbau unter ZT stark von dem im C5:2020-Kriterienkatalog beschriebenen System unterscheidet. So dürfen Unternehmensressourcen nur über PEPs erreichbar und auffindbar sein. Es muss eine logische Trennung in Datenebene und Kontrollebene vorgenommen werden. Die Assets müssen die PEPs erreichen können. Die PA darf nur von PEPs erreicht werden können. Des Weiteren muss ergänzt werden, dass Remote- Assets auf Ressourcen zugreifen können, ohne die gesamte Unternehmensstruktur durchlaufen zu müssen. Auch steuern ein oder mehrere PDP/ PEP- Gateways den Zugriff auf Systemressourcen. Zusätzlich kann festgelegt werden, dass bestimmte Assets keinen Zugriff auf bestimmte Ressourcen erhalten.

Bei der **Portabilität und Interoperabilität** wird konkretisiert, dass Kommunikation immer verschlüsselt werden muss.

Für den **Backup-Dienst** gelten die Anforderungen aus Kapitel 4.2.1.2 . Bei der **Produktsicherheit** muss das Sessionmanagement so angepasst werden, dass der Zugriff auf Unternehmensressourcen pro Session gewährt sowie Inaktivität erkannt und die Session bei erkannter Inaktivität invalidiert wird.

Die folgenden Bereiche müssen nicht angepasst werden, da das ZT- Prinzip keinen Einfluss auf diese hat: **Sicherheitsrichtlinien und Arbeitsanweisungen**, **Personal**, **Physische Sicherheit**, **Beschaffung**, **Entwicklung und Änderung von Informationssystemen**, **Steuerung und Überwachung von Dienstleistern und Lieferanten**, **Umgang mit Sicherheitsvorfällen**, **Kontinuität des Geschäftsbetriebes und Notfallmanagement**, **Compliance**, **Umgang mit Ermittlungsanfragen staatlicher Stellen**.

4.2.2 Anforderungskatalog

Es zeigt sich also, dass die Anforderungen an ein Cloudbackupsystem unter Zero Trust wesentlich komplexer sind als anfangs vermutet. Die nachfolgende Tabelle zeigt nun eine Zusammenfassung dieser Anforderungen.

Tabelle 3 Vollständiger Anforderungskatalog für den Anbieter eines Cloudbackupsystems unter ZT

Basisanforderungen	Zusatzanforderungen
1. Organisation der Informationssicherheit	
• ISMS	• Zertifizierung des ISMS nach ISO/IEC 27001 oder ISO 27001
• Leitlinie zur Informationssicherheit	
• Dokumentation und Kundeninformation zu Schnittstellen und Abhängigkeiten zu Dritten	
• Trennung von Aufgaben und Verantwortlichkeiten (Mikrosegmentierung) o Trennung von Ressourcen oder Ressourcengruppen in verschiedene Netzsegmente, die durch Sicherheitsgateways geschützt werden	
• netzwerkbasierte Segmentierung o Overlay- Netzwerk o PA dient als Netzwerkcontroller, der auf Basis der Entscheidung des PEs Netzwerk einrichtet und konfiguriert o Clients stellen Anfragen über PEP	
• Richtlinie für den Umgang mit Risiken	
• Risikoprüfung (anlassbezogen/ mindestens einmal jährlich)	

• Kontakt zu relevanten Behörden, Ministerien und Interessenverbänden	• Kontakt zum Nationalen IT- Lagezentrum und dem CERT- Bund
2. Sicherheitsrichtlinien und Arbeitsanweisungen	
• einheitliche Struktur und Kommunikation sowie Bereitstellung von Richtlinien und Anweisungen	
• Prüfung der Richtlinien und Anweisungen (mind. einmal jährlich) • Genehmigung der überarbeiteten Richtlinien	
• Abweichungen von bestehenden Richtlinien und Anweisungen müssen nach der Richtlinie für den Umgang mit Risiken geprüft und genehmigt werden	
3. Personal	
• Überprüfung der Qualifikation und der Vertrauenswürdigkeit	
• Verpflichtung zur Einhaltung der Richtlinien und Anweisungen durch Vertrags- und Beschäftigungsbedingungen	
• regelmäßige, fortlaufend verbesserte Schulungen und Sensibilisierungen	• Verbesserung der Schulungen durch Messung der Lernerfolge und Auswertungen
• bekannte Maßregelungsprozesse für Verstöße gegen Richtlinien und Anweisungen	
• Verantwortlichkeiten, die bei Beendigung oder Änderung der Beschäftigung erhalten bleiben	
• Vertraulichkeitsvereinbarungen mit Mitarbeitern und evtl. Dritten	

4. Asset Management	
• Inventarisierung der Assets sowie die Nutzung dieser Informationen bei der Protokollierung und Überwachung	
• ständige Kontrolle und Überwachung aller Assets	
• Richtlinie für den Umgang und den Gebrauch von Assets	
• Einhaltung der Richtlinie für In- und Außerbetriebnahme von Hardware	
• Rückgabe von Assets nach Beendigung des Beschäftigungsverhältnisses	• Schaffung einer zentralen Stelle für Ausgabe und Rücknahme von Assets
• einheitliches System für Klassifizierung und Kennzeichnung von Assets	• Protokollierung und Überwachung beachten den Schutzbedarf und treffen so eine Priorisierung
5. Physische Sicherheit	
• Sicherheitsrichtlinie für Räume und Gebäude	• Sicherheitsrichtlinie wird um Anforderungen an den autarken Betrieb ergänzt
• zwei Standorte, die die Richtlinie erfüllen (geografische Redundanz)	• mehr als zwei Standorte, die die Sicherheitsrichtlinie erfüllen
• mind. jährliche Kontrolle der Einhaltung der Richtlinie an allen Standorten	• Sicherheitspersonal, Videoüberwachung, Einbruchsmeldeanlagen
• gegebener Perimeterschutz aller Standorte	
• physische Zutrittskontrollen	
• bauliche, technische und organisatorische Rauch- und Brandschutzmaßnahmen	• Überwachung der Umgebungsparameter mit automatischer Alarmierung bei Verlassen des Regelbereichs
• Maßnahmen zum Schutz vor Ausfall der Versorgungseinrichtungen	• USV und NEA werden so konzipiert, dass der Weiterbetrieb mindestens fünf Tage gewährleistet werden kann

6. Regelbetrieb	
Kapazitätsmanagement	
• Einbindung von Prognosen in die Planung, um Engpässe und Ausfälle zu verhindern	
• Maßnahmen zur Überwachung und Provisionierung	
• Möglichkeit für den Kunden, die Systemressourcen zu steuern und zu überwachen	• Einrichtung eines Portals, über das der Kunde die Kapazität überwachen kann
• Einbindung von Prognosen in die Planung der PDP/PEP- Gateways um Störungen im Arbeitsablauf zu vermeiden	
Schutz vor Schadprogrammen	
• Richtlinie zum Schutz vor Schadprogrammen	• regelmäßige Reports von durchgeführten Überprüfungen werden von autorisierten Personen überprüft und analysiert • Konzept enthält Anweisungen, die technische Maßnahmen beschreiben
• regelmäßige Aktualisierung sowie die automatische Überwachung der Konfigurationen, gesteuert durch CDM-System	
Datensicherung und -wiederherstellung	
• Erarbeitung einer Richtlinie zur Datensicherung und -wiederherstellung	
• technische und organisatorische Maßnahmen zur Überwachung der Datensicherung	• Weiterleitung der Protokolle oder einer Zusammenfassung an den Kunden

• mind. einmal jährlich Wiederherstellungstests	• Weiterleitung der Ergebnisse an den Kunden • Einbindung der Wiederherstellungstests in das Notfallmanagement
• verschlüsselte Übertragung des Backups an den Remote-Standort	
Protokollierung und Überwachung	
• Richtlinie zur Protokollierung und Überwachung • Richtlinie zum Umgang mit Metadaten • nur autorisierte Nutzer und Systeme haben Zugriff auf Protokolle und Überwachung	• automatische Löschung personenbezogener Daten aus Protokollierungen
• Protokolle werden nach Zweckerfüllung gelöscht.	
• automatische Überwachung des gesamten Datenverkehrs um Schadereignisse zu erkennen	
• Daten der Protokollierung und der Überwachung müssen getrennt voneinander und in unveränderlicher Form gespeichert werden	• kundenspezifische Protokollierung
• Authentifizierung zwischen Protokollierungsserver und Assets	
• Protokollierung muss ermöglichen, ein konkretes Ereignis einem Nutzer zuzuordnen	• Protokolldaten werden auch Kunden zur Verfügung gestellt
• Schnittstellen für forensische Sicherung	
• Änderungen der Konfiguration immer nach Richtlinie zur Änderung an Informationssystemen	

• automatische Überwachung der Funktionsfähigkeit der Protokollierungs- und Überwachungssysteme	• Sicherstellung der Protokollierung und Überwachung, auch wenn eine Komponente ausfällt
• dynamische Anpassung der Richtlinien auf Grundlage der PE- Entscheidungen	
• CDM- System zur Zustandsüberwachung aller Geräte und Anwendungen	
• Zwei- oder Mehr- Faktor- Authentifizierung für Zugriff auf Systemkomponenten	
Umgang mit Schwachstellen, Störungen und Fehlern	
• mindestens jährlicher Penetrationstest	• mindestens halbjährlicher Penetrationstest durch externen Dienstleister
• Penetrationstest umfasst alle relevanten Systemkomponenten	
• quartalsweise Analyse, Messung und Bewertung des Umgangs mit Schwachstellen	
• Information des Kunden über Störungen des Regelbetriebs; evtl. Einbindung in die Behebung • Information des Kunden über Lösung	
• mindestens einmal im Monat automatisierte Prüfung bekannter Schwachstellen; Einteilen der Schwachstellen nach Schweregraden	• Einteilung nach CVSS, daraus abgeleitet, Zeit zur Behebung: ○ kritisch: 3 Stunden ○ hoch: 3 Tage ○ mittel: 1 Monat ○ niedrig: 3 Monate
• Systemhärtung nach üblichen Standards (z.B. BSI IT- Grundschutz- Kompendium)	• automatische Überprüfung der Vorgaben zu Härtung
• Daten unterschiedlicher Kunden strikt voneinander trennen	• Zonierung des Storage durch LUN Binding und LUN Masking

• Threat Intelligence Feeds zum Sammeln von Informationen aus internen und externen Quellen für Verbesserung des PEs	
7. Identitäts- und Berechtigungsmanagement	
• alle Ressourcen und PEP- Komponenten müssen Möglichkeit haben, Objekte zu authentifizieren oder ein Richtlinienmodul zu erreichen, das dies übernimmt	
• Richtlinie für Zugangs- und Zugriffsberechtigungen (Umsetzung von Least-Privilege-/ Need-to-Know- Prinzip)	
• dynamische Verfahren zur Vergabe und Änderung von Zugangs- und Zugriffsberechtigungen	• Kunde kann selbst Zugriffs- und Zugangsberechtigungen vergeben
• Sperrung von Zugangsberechtigungen, die 2 Monate nicht genutzt wurden (Entsperrung nur durch autorisierte Instanzen)	
• Entzug von Zugangsberechtigungen, die 6 Monate nicht genutzt wurden (nach Entzug neues Vergabeverfahren nötig)	
• mindestens einmal jährlich Prüfung, ob vergebene Rechte noch benötigt werden, falls nicht: Entzug der Rechte innerhalb von 7 Tagen	• halbjährliche Prüfung privilegierter Zugangsberechtigungen
• privilegierte Zugangsberechtigungen zeitlich befristet und Aktivitäten werden protokolliert und automatisch auf Missbrauch durchsucht; bei Verstoß: Disziplinarmaßnahmen	

• Zugriff auf Daten des Kunden: innerhalb von 72 Stunden Kunde informieren	• Kunde wird vor dem Zugriff informiert und muss zustimmen
• geordnete Verfahren für Zuteilung von Authentifizierungsinformationen	• Nutzer bestätigen Erklärung für Geheimhaltung von Authentisierungsinformationen
• Änderung des Initialpassworts (max. 14 Tage gültig) bei Erstanmeldung	
• technische Maßnahmen für Einhaltung der Passwortvorgaben	
• bei Änderungen und Zurücksetzung von Passwörtern: Kunden immer informieren	
• Verwendung starker Passworthashfunktionen (z. B. Argon2i) zur Speicherung von Passwörtern	
• Zwei- und Mehr- Faktor-Authentisierung oder Ersetzen dieser durch ein System des kontinuierlichen Monitorings mit einem Konzept der Re-Authentifizierung und Re-Autorisierung auf Basis der Benutzeraktionen und Richtlinien	
• Authentisierung innerhalb der Produktionsumgebung mit Hilfe von Passwörtern; digitaler, signierter Zertifikate und anderer Verfahren	
• Zertifikatsverwaltung nach Richtlinie zur Schlüsselverwaltung	
8. Kryptographie und Schlüsselmanagement	
• Richtlinie für Nutzung von Verschlüsselungsverfahren und Schlüsselverwaltung	

• technische Maßnahmen zur starken Verschlüsselung und Authentifizierung bei Übertragung von Daten (TLS)	
• Verschlüsselung aller gespeicherten Daten (Ausnahmen zur Entschlüsselung vertraglich geregelt)	• keine Ausnahmen möglich
• Verfahren und technische Maßnahmen zur sicheren Schlüsselverwaltung	
• PKI für die Verwaltung und Generierung von Zertifikaten	
9. Kommunikationssicherheit	
• Richtlinie für technische Schutzmaßnahmen zum Schutz vor netzbasierten Angriffen basierend auf Risikoanalyse	• technische Maßnahmen, verhindern, dass unbekannte Geräte dem Netz beitreten können
• übergreifendes SIEM- System	
• spezifische Sicherheitsanforderungen für Verbindungen	

• keine Verbindung wird als vertrauenswürdig angesehen
  ○ Unternehmensressourcen nur über PEP erreichbar (Ressourcen sind ohne PEP- Zugriff nicht auffindbar)
  ○ logische Trennung in Datenebene und Kontrollebene
  ○ Assets müssen PEP erreichen können
  ○ PA kann nur von PEP erreicht werden
  ○ Remote- Assets müssen auf Ressourcen zugreifen können, ohne die gesamte Unternehmensstruktur durchlaufen zu müssen
• mindestens einmal jährlich Konzeption und Konfiguration der Überwachung prüfen
• Bewertung von Risiken nach Richtlinie zum Umgang mit Risiken
• in definierten Abständen Dienste, Protokolle und Ports prüfen (kompensierende Maßnahmen für unsichere Protokolle)	

• ein oder mehrere PDP/ PEP- Gateways steuern den Zugriff auf Systemressourcen • Zugangsberechtigungen für netzübergreifenden Zugriff auf Basis der Anforderungen des Kunden	• bestimmte Assets keinen Zugriff auf bestimmte Ressourcen erhalten

• gesondertes Netz zur administrativen Verwaltung und Betrieb der Managementkonsole und durch Multi- Faktor-Authentifizierung • physische und logische Trennung von Netzen und virtuellen Maschinen, die zur Migration genutzt werden	
• nachvollziehbare Dokumentation des Netzes mit Subnetzen, Zonierungen, Segmentierungen und Lage der Kundendaten	
• Richtlinie zur Datenübertragung	
10. Portabilität und Interoperabilität	
• regelmäßig aktualisierte Dokumentation der Eingangs- und Ausgangsschnittstellen, die über standardisierte Kommunikationsprotokolle angesprochen werden • Verschlüsselung der Kommunikation • Art und Umfang der Dokumentation orientiert sich am Kundenbedarf	
• vertragliche Vereinbarung zur Bereitstellung (Art, Umfang, Format) von Daten, Fristen zur Löschung und Bereitstellung sowie Mitwirkungspflichten des Kunden • Berücksichtigung von Kunden-/ Anbieterwunsch, rechtliche und regulatorische Anforderungen	• rechtliche und regulatorische Anforderungen im Umfeld des Anbieters berücksichtigen • mindestens einmal jährliche Überprüfung der Anforderungen; ggf. Anpassung des Vertrags
• Löschung des aktuellen Datenbestands, Metadaten und Datensicherung nach Vertragsende • gelöschte Daten können nicht wiederhergestellt werden	

11. Beschaffung, Entwicklung und Änderung von Informationssystemen	
• Richtlinie zur Entwicklung bzw. Beschaffung von Informationssystemen • entspricht anerkannten Standards und Methoden (z.B. ISO/ IEC 27034)	• beschaffte Produkte mindestens Zertifikat der Prüftiefe EAL 4 (CC) • falls entsprechendes Zertifikat nicht vorhanden➔ Risikobewertung
• vertragliche Regelungen bei der Auslagerung von Entwicklungsprozessen • Abnahmeprüfung zur Qualitätssicherung	
• Richtlinie zur Änderung von Informationssystemen	
• „…Programm zur Sicherheitsausbildung und Sensibilisierung bezüglich kontinuierlicher Softwarebereitstellung und zugehöriger Systeme, Komponenten oder Werkzeuge“ [34, S. 97]	
• Risikobewertung, Kategorisierung und Priorisierung von Auswirkungen der Änderungen • Vorabinformation bei Änderungen der höchsten Risikokategorie	• Vorabinformation des Kunden über bevorstehende Änderungen
• Durchführung geeigneter Test für Änderungen durch qualifiziertes Personal oder automatische Testverfahren	
• Protokollierung der Änderungen unterliegt Autorisierungsmechanismen und Rollen- und Rechtskonzepten (ausführende Personen/ Systemkomponenten sind identifiziert und protokolliert)	
• Verfahren zur Versionskontrolle (Möglichkeit zum Zurücksetzen vom Systemkomponenten auf früheren Zustand	• Verfahren zur Versionskontrolle haben geeignete Schutzmaßnahmen für Integrität und Verfügbarkeit der Daten der Kunden

• Änderungen werden durch autorisiertes Personal/ Systemkomponenten freigegeben, bevor diese in der Produktionsumgebung bereitgestellt werden	
• Test- /Entwicklungsumgebung physisch oder logisch getrennt • Daten aus Produktionsumgebung werden nicht für Tests genutzt	
12. Steuerung und Überwachung von Dienstleistern und Lieferanten	
• Richtlinie zur Steuerung und Überwachung von Dienstleistern und Lieferanten	• vertragliche Vereinbarung mit Subdienstleistern zur regelmäßigen Berichterstattung und unabhängigen Kontrolle • falls Berichterstattung nicht möglich, müssen Informations- und Prüfungsrechte vereinbart werden (Prüfung durch qualifiziertes Personal)
• Risikobeurteilung der Dritten • mindestens 1x jährlich Einschätzung der bisher getroffenen Risikobeurteilung und Dokumentation	
• Verzeichnis der Dienstleister und Lieferanten	
• überwachen der Dienstleister und Lieferanten bezüglich der Einhaltung vertraglicher Vereinbarungen	• automatische Überwachung von Reaktionszeiten, Konfigurationen, Verfügbarkeit und Leistungen sowie Wiederherstellungszeiten und automatisierte Weiterleitung bei Verstößen
• Ausstiegsstrategie für den Bezug von Leistungen von Dritten, von denen eine sehr hohe Abhängigkeit besteht	

13. Umgang mit Sicherheitsvorfällen	
• Richtlinie zum Umgang mit Sicherheitsvorfällen • Schaffung eines CERT	• Anweisungen zur beweisfesten Sicherung von verdächtigen Daten • vor Gericht verwertbare Analysepläne für Sicherheitsvorfälle
• Klassifizierung, Priorisierung und Ursachenanalyse bei Sicherheitsvorfällen durch qualifiziertes Personal oder externe Sicherheitsdienstleister	• mindestens 1x jährlich Tests und Übungen zur Identifikation, Analyse und Abwehr von Sicherheitsvorfällen und Angriffen
• Lösungen werden dokumentiert und den betroffenen Kunden mitgeteilt	• Kunde kann Lösung aktiv oder passiv zustimmen • Information wird allen Kunden zugesandt • vertragliche Vereinbarung, welche Daten dem Kunden zur eigenen Analyse mitgeteilt werden
• Schaffung einer zentralen Stelle, an die Sicherheitsvorfälle gemeldet werden	
• Entwickeln neuer Schutzmaßnahmen auf der Grundlage der Auswertung und Dokumentation von Sicherheitsvorfällen	
14. Kontinuität des Geschäftsbetriebs und Notfallmanagement	

• Unternehmensleitung trägt Verantwortung für:
  ○ Etablierung der Prozesse und Richtlinien
  ○ ausreichende Ressourcen
  ○ Mitwirken aller Mitarbeiter	

• Richtlinie und Anweisungen zur Ermittlung von Auswirkungen von Störungen des Dienstes/ Unternehmens	

• Rahmenwerk für die Planung der Betriebskontinuität und des Geschäftsplans nach anerkannten Standards	
• erstellte Pläne werden mindestens 1x jährlich oder nach größeren organisatorischen/ umgebungsbedingten Veränderungen geprüft, getestet und aktualisiert • Einbindung von Kunden und Lieferanten	• Einbinden von Übungen anhand vergangener Sicherheitsvorfälle
15. Compliance	
• Einhaltung gesetzlicher, regulatorischer, selbstauferlegter oder vertraglicher Anforderungen • definieren und dokumentieren entsprechender Verfahren und Anforderungen	
• Richtlinie für Planung und Durchführung von Audits	• Anbieter gewährt Kunden vertraglich Informations- und Prüfungsrechte
• mindestens 1x jährlich Audits am ISMS durch qualifiziertes Personal	• Ergänzung durch Verfahren der automatischen Überwachung • automatische Weiterleitung an Zuständige • Kunde kann in Echtzeit Einhaltung bestimmter vertraglicher Anforderungen überwachen
• oberste Leitung wird über ISMS regelmäßig informiert und erstellt mindestens 1x jährlich eine Managementbewertung des ISMS	

16. Umgang mit Ermittlungsanfragen staatlicher Stellen	
• juristische Beurteilung von Ermittlungsanfragen durch qualifiziertes Personal	
• Kunde wird über Eingang der Ermittlungsanfrage informiert (soweit dies rechtlich möglich ist)	
• Zugriff und Offenlegung von Daten nur auf Grundlage und im Umfang einer anwendbaren rechtsgültigen Rechtsgrundlage	
• falls keine klare Abtrennung der Daten möglich ist: Pseudonymisierung und Anonymisierung aller Daten, die nicht Teil der Ermittlungsanfrage sind	
17. Backup- Dienst und Produktsicherheit	
Backup- Dienst	
• Erarbeitung einer Richtlinie zur Datensicherung und -wiederherstellung mit dem Kunden	• Automatisierung des Backup- und Recoveryprozesses • Einhalten der 3-2-1-Daten- Backup-Regel
• technische und organisatorische Maßnahmen zur Überwachung der Datensicherung	• Weiterleitung der Protokolle oder einer Zusammenfassung an den Kunden
• mind. einmal jährlich Wiederherstellungstests	• Weiterleitung der Ergebnisse an den Kunden
• verschlüsselte Übertragung des Backups an den Remote-Standort	
• Zeitabstände zur Backuperstellung können konfiguriert werden	

• Erkennung von Änderungen im Datenbestand des Kunden; nur diese werden gesichert (inkrementelle Sicherung)	
• Minimierung der Sicherungszeit	
• verschlüsselte Speicherung der Backups	
• Möglichkeit der Wiederherstellung unterschiedlicher Backuppunkte	
• Möglichkeit der Erkennung von Schadsoftware	
• Erkennung unvollständiger oder manipulierter Sicherungen	
• Erkennung fehlerhafter und fehlender Backups und Kompensation dieser	
Produktsicherheit	
• Leitlinie und Empfehlungen zur sicheren Nutzung des Dienstes (Angaben zur Konfiguration, Installation und Nutzung des Cloudbackupdienstes	
• Überprüfung des Dienstes auf durch Softwareentwicklungsprozesse entstandene Schwachstellen	• jährliche Code Reviews oder Security Penetrationstests durch qualifizierte Dritte
• tagesaktuelles Onlineregister bekannter Schwachstellen mit Angaben zu Softwareaktualisierungen	• automatisierte Aktualisierungsmechanismen (Kunde muss diesen nur noch zustimmen)

• Fehlerbehandlungs- und Protokollierungsmechanismen • gewonnene Informationen werden unveränderlich und geschützt vor unberechtigtem Zugriff gespeichert; Kunde hat Möglichkeit zur Löschung • wenn Protokollierung durch Kunden erfolgt, muss Anbieter Protokollierungsfunktionen bereitstellen	• dokumentierte Schnittstellen zum Abrufen von Informationen, die Kunden im eigenen SIEM auswerten können
• starke Authentifizierungsmechanismen an allen Zugangspunkten	• Möglichkeit einer OOB
• Sessionmanagement gewährt Zugriff auf Unternehmensressourcen pro Session, erkennt Inaktivität und invalidiert Session	
• Sicherstellen der Vertraulichkeit von Authentisierungsinformationen	
• Rollen- und Rechtskonzept setzt Least- Privilege- Prinzip und Need-to-Know- Prinzip sowie Funktionstrennung zwischen operativen und kontrollierenden Funktionen um	
• Autorisierungsmechanismen zur Überprüfung, ob Nutzer, IT-Komponenten oder Anwendungen Rechte für Aktion besitzt • Prüfung dieser, bevor neue Funktionen bereitgestellt oder Änderung an bestehender Funktion vorgenommen wird	• attributbasierte Zugriffskontrollen
• sollte SDN genutzt werden, muss Vertraulichkeit der Daten durch geeignete SDN- Verfahren sichergestellt werden	
• Kunde erhält Auswahlmöglichkeit des geografischen Ortes für die Speicherung und Verarbeitung seiner Daten	

5 Fazit und Ausblick

Der Schutz digitaler Informationen vor Verlust und Veränderung ist in der heutigen Zeit eine wesentliche Grundlage für die Funktionsfähigkeit von Wirtschaft und Gesellschaft. Dabei ist es wichtig, dass alle wesentlichen Daten so gesichert und aufbewahrt werden, dass sie auch nach Sicherheitsvorfällen- gleich welcher Art- wiederhergestellt werden können. Es ist also unabdingbar, regelmäßig Backups zu erstellen. Diese müssen so gelagert werden, dass sie zum einen sicher; zum anderen aber auch in angemessener Zeit verfügbar sind. Gleichzeitig muss gewährleistet werden, dass keine unberechtigten Personen oder Systeme Zugriff auf die Daten erhalten.

Zudem wird es immer schwieriger für Firmen und Institutionen, die ständig wachsenden Datenmengen zu verarbeiten, zu sichern und aufzubewahren. Daher werden zunehmend Clouddienste genutzt, die aber von außen angreifbar sind, weil die Sicherung über ein Netzwerk stattfindet.

Um die Sicherheit dieses Netzwerkes zu verbessern kann das ZT- Prinzip genutzt werden. Dieses basiert darauf, dass keinem Nutzer oder System vertraut werden kann und setzt aus diesem Grund auf eine verbesserte Identitätsverwaltung, Segmentierung und eine umfassende Überwachung und Protokollierung des gesamten Datenverkehrs.

Bei der Umsetzung eines Cloudbackupsystems unter Zero Trust müssen also sowohl die Anforderungen, die an die Sicherheit von Backups im Allgemeinen wie auch die Anforderungen an das Cloud Computing und die speziellen Anforderungen an das ZT- Prinzip beachtet werden.

Es wurde gezeigt, dass ein Anbieter eines Cloudbackup Servers unter ZT neben technischen und rechtlichen Anforderungen auch eine Reihe von organisatorischen Anforderungen bei der Planung, Konfiguration und dem Betrieb eines solchen Systems erfüllen muss.

Das BSI gibt im C5:2020 Kriterienkatalog 17 Bereiche an, die bei der Planung und technischen Umsetzung von Clouddiensten vom Anbieter berücksichtigt werden müssen. Dieser Katalog setzt sich jedoch ausschließlich mit den allgemeinen Anforderungen an das Cloud Computing auseinander. Aus diesem Grund wurden aus der Theorie und den Beschreibungen des C5:2020- Katalogs zur Datensicherung und -wiederherstellung die Anforderungen an den eigentlichen Cloudbackupdienst, der dem Kunden bereitgestellt wird, ergänzt. Da der C5:2020 Kriterienkatalog eine Hybridform aus einem ZT- basierten und einem perimeterbasierten Ansatz darstellt, mussten noch einige Punkte entsprechend der Special Publication 800-207 des NIST angepasst werden, um so eine vollständige Umsetzung des ZT-Prinzips zu erreichen. Dabei sind einige der Zusatzanforderungen aus dem C5:2020 Kriterienkatalog, die die Informationssicherheit betreffen, nun Basisanforderungen. Des

Weiteren wurden die Anforderungen an die Kommunikationssicherheit so angepasst, dass die logische Trennung von Datenebene und Kontrollebene umgesetzt wird und alle Assets nur noch über PDP/PEP- Gateways zu erreichen sind.

Die 17 Bereiche, die bei einem Cloudbackupsystem unter ZT beachtet werden müssen, sind:

- Organisation der Informationssicherheit
- Sicherheitsrichtlinien und Arbeitsanweisungen
- Personal
- Asset Management
- Physische Sicherheit
- Regelbetrieb
    - Kapazitätsmanagement
    - Schutz vor Schadprogrammen
    - Datensicherung- und -wiederherstellung
    - Protokollierung und Überwachung
    - Umgang mit Schwachstellen, Störungen und Fehlern
- Identitäts- und Berechtigungsmanagement
- Kryptografie und Schlüsselmanagement
- Kommunikationssicherheit
- Portabilität und Interoperabilität
- Beschaffung, Entwicklung und Änderung von Informationssystemen
- Steuerung und Überwachung von Dienstleistern und Lieferanten
- Umgang mit Sicherheitsvorfällen
- Kontinuität des Geschäftsbetriebs und Notfallmanagement
- Compliance
- Umgang mit Ermittlungsanfragen staatlicher Stellen
- Backup-Dienst und Produktsicherheit
    - Backup- Dienst
    - Produktsicherheit

Ein wichtiger Teil der Compliance ist die Einhaltung gesetzlicher, regulatorischer selbstauferlegter oder vertraglicher Anforderungen. Die rechtlichen Regelungen, die eingehalten werden müssen, sind zahlreich. Hier ist das Recht des Staates, in dem der Anbieter seinen Sitz hat, zu beachten. Zudem gibt es für Kunden verschiedener Branchen spezielle rechtliche Anforderungen beispielsweise in Bezug auf Informationssicherheit und Datenschutz sowie Fristen zur Aufbewahrung und Löschung bestimmter Daten. In der DSGVO, die EU-

weit gilt, ist der Umgang mit personenbezogenen Daten geregelt. Aber auch das entsprechende Vertragsrecht muss beachtet werden, da bei der Auftragsverarbeitung von Daten immer ein entsprechender Vertrag notwendig ist. Aufgrund dieser komplexen Gesetzeslage sollte bei der Planung immer ein Experte für die Klärung der rechtlichen Aspekte einbezogen werden.

Wie bei jedem ZT-Netzwerk gilt auch für das Cloudbackupsystem unter ZT, dass es aufgrund des Aufbaus das Netzwerk gut skalierbar und erweiterbar ist. Allerdings erfordern der Aufbau und die Wartung eines solchen Netzes aufgrund der komplexen Struktur ein hohes Maß an Fachwissen und ist mit hohen Kosten verbunden. Es kann jedoch auch eine Hybridform aus einem ZT- basierten und einem perimeterbasierten Ansatz geschaffen werden. Dies ist möglich, da es sich bei dem ZT- Prinzip um eine Sammlung von Leitprinzipien handelt und sich durch die Umsetzung einzelner dieser Punkte auch schon die Sicherheit des Netzwerks verbessert.

In Zukunft ist zu prüfen ob es möglich ist, den in dieser Arbeit erstellten Katalog mit seinen komplexen technischen, organisatorischen und rechtlichen Anforderungen in vollem Umfang umzusetzen und gleichzeitig ein vertretbares Verhältnis von Aufwand und Nutzen zu erreichen. Dabei muss insbesondere überprüft werden, ob die vollständige Erfüllung der Anforderungen auch zu einer tatsächlichen Verbesserung der Sicherheit führt, die den zusätzlichen Verwaltungsaufwand und die hohen Kosten rechtfertigt.

Literatur

[1] Bundeskriminalamt;, „Cybercrime. Bundeslagebild 2021,“ 9. 5. 2022. [Online]. Available: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2021.html. [Zugriff am 22. 1. 2023].

[2] Cornelsen Verlag GmbH, „Sicherheit,“ [Online]. Available: https://www.duden.de/rechtschreibung/Sicherheit. [Zugriff am 22. 1. 2023].

[3] Bundesamt für Sicherheit in der Informationstechnik, „BSI- Standard 200-1.Managementsystemefür Informationssicherheit (ISMS),“ 15. 11. 2017. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_1.html?nn=128578. [Zugriff am 22. 1. 2023].

[4] C. Eckert, IT-Sicherheit.Konzept-Verfahren-Protokolle, 10. Auflage Hrsg., Berlin/ Boston: Walter de Gruyter GmbH, 2018.

[5] E. von Faber, IT und IT- Sicherheit in Begriffen und Zusammenhängen. Thematisch sortiertes Lexikon mit alphabetischem Register zum Nachschlagen, 1. Auflage Hrsg., Wiesbaden: SpringerVieweg, 2021.

[6] „Verordnung (EU) 2016-679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG,“ 27. 4. 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex:32016R0679. [Zugriff am 22. 1. 2023].

[7] Bundesamt für Sicherheit in der Informationstechnik, „BSI- Standard 200-2.IT-Grundschutzmethodik,“ 15. 11. 2017. [Online]. Available:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.html?nn=128640. [Zugriff am 22. 1. 2023].

[8] National Institute of Standards and Technology, „FIPS PUB 199. Standards for Security Categorization of Federal Information and Information Systems," Februar 2004. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf. [Zugriff am 22. 1. 2023].

[9] W. Ertel und E. Löhmann, Angewandte Kryptographie, 6. aktualisierte Auflage Hrsg., München: Carl Hanser Verlag, 2020.

[10] C. Paar und J. Pelzl, Kryptografie verständlich. Ein Lehrbuch für Studierende und Anwender, 1. Auflage Hrsg., Berlin: Springer Vieweg, 2016.

[11] Cornelsen Verlag GmbH, „Duden.Kryptografie," [Online]. Available: https://www.duden.de/rechtschreibung/Kryptografie. [Zugriff am 23. 01. 2023].

[12] Bundesamt für Sicherheit in der Informationstechnik, „Kryptografische Verfahren: Empfehlungen und Schlüssellängen," 28. 01. 2022. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.html. [Zugriff am 23. 01. 2023].

[13] Bundesnetzagentur, „Empfehlung zur technischen Umsetzung von Signaturdiensten," 19. 12. 2017. [Online]. Available: https://www.bundesnetzagentur.de/EVD/SharedDocuments/Downloads/QES/Algorithmen/Empfehlungen2018.html. [Zugriff am 23. 01. 2023].

[14] Senior Officials Group Information Systems Security, „SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms," Januar 2020. [Online]. Available: https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.2.pdf. [Zugriff am 23. 01. 2023].

[15] D. Giry, „BlueKrypt. Cryptographic Key Length Recommendation," 24. 05. 2020. [Online]. Available: https://www.keylength.com/en/compare/. [Zugriff am 23. 01. 2023].

[16] J. Dunkel, A. Eberhart, S. Fischer, C. Kleiner und A. Koschel, Systemarchitekturen für Verteilte Anwendungen.Client-Server, Multi-Tier, SOA, Event-Driven Architecture, P2P, Grid, Web 2.0, München: Carl Hanser Verlag, 2008.

[17] A. Schill und T. Springer, Verteilte Systeme, 2. Auflage Hrsg., Heidelberg: Springer Verlag, 2012.

[18] A. Luntovskyy und D. Gütter, Moderne Rechnernetze. Protokolle, Standards und Apps in kombinierten drahtgebundenen, mobilen und drahtlosen Netzwerken, Wiesbaden: Springer Fachmedien Wiesbaden GmbH, 2020.

[19] J. Kindervag, „No More Chewy Centers: The Zero Trust Model Of Information Security. Vision: The Security Architecture And Operations Playbook," 23. 03. 2016. [Online]. Available: https://crystaltechnologies.com/wp-content/uploads/2017/12/forrester-zero-trust-model-information-security.pdf. [Zugriff am 24. 01. 2023].

[20] J. Kindervag, „Build Security Into Your Network`s DNA: The Zero Trust Network Architecture," 05. 11. 2010. [Online]. Available: https://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf. [Zugriff am 24. 01. 2023].

[21] J. Garbis und J. W. Chapman, Zero Trust Security. An Enterprise Guide, 1. Auflage Hrsg., New York: Apress Berkeley, CA, 2021.

[22] S. Rose, O. Borchert, S. Mitchell und S. Connelly, „NIST Special Publication 800-207. Zero Trust Architecture," [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf. [Zugriff am 27. 01. 2023].

[23] J. Zelonis, „Now Tech: Network Analysis And Visibility, Q2 2020. Forrester`s Overview Of 24 Network Analysis And Visibility Providers," 23. 06. 2020. [Online]. Available: https://www.nextgigsystems.com/new/wp-content/uploads/Now-Tech-Network-Analysis-And-Visibility-Q2-2020.pdf. [Zugriff am 26. 01. 2023].

[24] N. Pohlmann, Cyber-Sicherheit. Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheits-systemen in der Digitalisierung, 2. Auflage Hrsg., Wiesbaden: Springer Fachmedien Wiesbaden GmbH, 2022.

[25] R. Bär, G. Bischofberger, E. Dehler, N. Hammer, B. Schiemann und T. Wolf, Informatik und Informationstechnik für Gymnasien und höhere Bildungsgänge im beruflichen Schulwesen, 3. Auflage Hrsg., Haan- Gruiten: Verlag Europa- Lehrmittel, Nourney,Vollmer GmbH & Co. KG, 2017.

[26] TechTarget, Inc., „Datendeduplizierung. Definition," Juni 2020. [Online]. Available: https://www.computerweekly.com/de/definition/Daten-Deduplizierung. [Zugriff am 27. 02. 2023].

[27] S. Nelson, Pro Data Backup and Recovery. Securing your information in the terabyte age, 1. Auflage Hrsg., Apress Berkeley, CA, 2011.

[28] G. Lucny, „Konzeption und Implementierung einer Cloud-unterstützten Peer-to-Peer-Backuplösung. P2P-Backuplösung mit Cloud-Unterstützung," 11. 05. 2022. [Online]. Available: https://repositum.tuwien.at/handle/20.500.12708/20302. [Zugriff am 27. 02 2023].

[29] IONOS SE, „Daten sichern: Methoden und Medien im Überblick," 13. 09. 2022. [Online]. Available: https://www.ionos.de/digitalguide/server/sicherheit/daten-sichern/. [Zugriff am 01. 03. 2023].

[30] I. Hanschke, Informationssicherheit und Datenschutz - einfach & effektiv. Integriertes Managementinstrumentarium systematisch aufbauen und verankern, München: Carl Hanser Verlag, 2020.

[31] Bindig Media GmbH, „Rückblick 2022: Die häufigsten 10 Ursachen für Datenverlust," 28. 12. 2022. [Online]. Available: https://www.datareverse-datenrettung.de/ueber-uns/impressum/. [Zugriff am 27. 02. 2023].

[32] E. Tiemeyer (Hrsg.), Handbuch IT-System- und Plattformmanagement. Handlungsfelder, Technologien, Managementinstrumente, Good Practices, München: Carl Hanser Verlag, 2021.

[33] novinet GmbH & Co. KG, „Aufbewahrungsfristen und Löschfristen gemäß DSGVO," [Online]. Available: https://novidata.de/themen/aufbewahrungsfristen-und-loeschfristen-dsgvo/. [Zugriff am 23. 2. 2023].

[34] Bundesamt für Sicherheit in der Informationstechnik, „Cloud Computing Compliance Criteria Catalogue-C5:2020. Kriterienkatalog Cloud Computing," 19. 01. 2020. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/2020/C5_2020.html. [Zugriff am 23. 01. 2023].

[35] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), „Gesetze und Verordnungen des Bundes und Richtlinien der EU," [Online]. Available: https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Strategien-und-rechtlicher-Rahmen/Rechtlicher-Rahmen/rechtlicher-rahmen_node.html. [Zugriff am 26. 01. 2023].

[36] Bundesamt für Sicherheit in der Informationstechnik, „Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0). Neues IT-Sicherheitsgesetz für eine moderne Cyber-Sicherheit," [Online]. Available: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html. [Zugriff am 26. 01. 2023].

[37] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), „Sektoren und Branchen KRITIS," BBK, [Online]. Available: https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Sektoren-Branchen/sektoren-branchen_node.html. [Zugriff am 26. 01. 2023].

[38] Strafgesetzbuch (StGB) i. d. F. der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), zuletzt geändert durch Art. 4 des Gesetzes vom 4. Dezember 2022 (BGBl. I S. 2146).

[39] Proact Deutschland GmbH, „Rechtliche Hürden beim Backup in die Cloud," 18. 11. 2014. [Online]. Available: https://blog.proact.de/blog/2014/11/18/rechtliche-huerden-beim-backup-in-die-cloud/. [Zugriff am 2023 01. 2023].

[40] Bundesamt für Sicherheit in der Informationstechnik, „BSI TR-02102-1 "Kryptographische Verfahren: Empfehlungen und Schlüssellängen"," 24. 01. 2023. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.html. [Zugriff am 27. 02. 2023].

[41] Bundesamt für Sicherheit in der Informationstechnik, „Technische Richtlinie TR-02102-2 Kryptografische Verfahren: Empfehlung und Schlüssellängen. Teil 2 - Verwendung von Transport Layer (TLS)," 11. 02. 2022. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.html. [Zugriff am 23. 01. 2023].

[42] Bundesamt für Sicherheit in der Informationstechnik, „Technische Richtlinie TR-02102-3 Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Teil 3 – Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2)," 24. 01. 2023. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-3.html. [Zugriff am 27. 02. 2023].

[43] Bundesamt für Sicherheit in der Informationstechnik, „Technische Richtlinie TR-02102-4 Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Teil 4 – Verwendung von Secure Shell (SSH)," 24. 01. 2023. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-4.html. [Zugriff am 27. 02. 2023].

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Mülsen, den 19.03.2023

Sandra Lindner