Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Bundesamt für Cybersicherheit BACS
Analyse und Prävention

2. Mai 2025

Technologiebetrachtung: Cloud Computing und Cybersicherheit

1 Einführung und Ausgangslage

«Cloud» respektive «Cloud Computing» wird oft als Paradigmenwechsel dargestellt, etwas Neues, das neuen Regeln folgt. Eine Diskussion der Cybersicherheit beim Einsatz von Cloud-Lösungen ist deshalb oft schwierig. Dies zeigt sich bei vielen Vorhaben, beispielsweise, wenn es um einen Entscheid für den Einsatz von Cloud-Diensten oder auch um die Verbesserung der Sicherheit von bereits im Einsatz stehenden Cloud-Lösungen geht.

Dieses Dokument soll IT-Verantwortlichen und IT-Entscheidungsträgern bei Firmen, Behörden oder Bildungsinstitutionen die notwendigen Grundlagen vermitteln, um diese Situation zu verbessern. Dazu erläutert die Technologiebetrachtung im ersten Kapitel konkret, was unter dem Begriff «Cloud» verstanden wird, weshalb verschiedene Cloud-Lösungen sehr unterschiedlich sein können und welche Herausforderungen die Verwendung von Cloud-Lösungen in Bezug auf die Cybersicherheit mit sich bringen. Im Kapitel wird ebenfalls aufgezeigt, dass Cloud Computing nicht ein neues Paradigma, sondern eine Möglichkeit ist, ein IT-Outsourcing umzusetzen.

Hier knüpft das zweite Kapitel an und zeigt ein konkretes Vorgehen für Entscheidungsträger, wie (Cloud-)Lieferanten beurteilt und ausgewählt werden können.

Es ist nicht Ziel dieses Dokumentes, konkrete auf Cloud-Diensten aufbauende Lösungsarchitekturen für die Cybersicherheit vorzustellen. Diese Arbeit folgt im Rahmen der Systemplanung und Entwicklung, nach dem Entscheid, einen Cloud-Dienst einzusetzen oder eine Cloud-Lösung zu beschaffen.

1.1 Geschichte

Die Geschichte des Cloud Computing ist faszinierend und reicht weiter zurück, als Viele denken. Bereits in den 1950er Jahren entwickelte IBM erste Ideen zur Verteilung von Daten und Aufgaben auf mehrere Rechnereinheiten. In den 1960er Jahren schlug John McCarthy, ein Pionier der Informatik, vor, dass Rechenleistung und Anwendungen als öffentliche Versorgungseinrichtungen bereitgestellt werden könnten. Diese frühen Konzepte legten den Grundstein für das, was wir heute als Cloud Computing kennen.

In den 1970er Jahren brachte Intel die ersten Mikroprozessoren auf den Markt, was die Entwicklung von Personal Computern ermöglichte. Die 1980er Jahre sahen die Einführung von Personal Computern und die Entwicklung des Client-Server-Modells, das es Unternehmen ermöglichte, ihren Bedarfsträgern IT-Leistungen über interne Netzwerke zur Verfügung zu stellen. Mit der Verbreitung des Internets in den 1990er Jahren begannen Unternehmen, wie Amazon und Google, die Grundlagen für moderne Cloud-Dienste zu legen. Der Begriff «Cloud Computing» wurde in den 2000er Jahren popularisiert, als Amazon Web Services (AWS) 2006 begann, skalierbare IT-Ressourcen über das Internet anzubieten. In den 2010er

Jahren wurden Cloud-Dienste immer ausgereifter und vielfältiger, Unternehmen wie Microsoft, Google und IBM traten in den Markt ein.

Mit zunehmender Beliebtheit des Cloud Computing kamen auch vermehrt Sicherheitsbedenken auf. Unternehmen sorgten sich um die Sicherheit ihrer Daten, die in Cloud-Diensten gespeichert waren, da sie nicht mehr die volle Kontrolle über die Infrastruktur hatten. Es gab auch vermehrt Bedenken hinsichtlich der Compliance mit regulatorischen Anforderungen beim Datenschutz.

In den 2010er Jahren kamen eine Vielzahl von Cloud-Sicherheitslösungen auf den Markt. Diese boten Funktionen wie Datenverschlüsselung, Zugriffskontrolle und Überwachung. Diese Sicherheitslösungen sollten das Vertrauen in das Cloud Computing stärken.

1.2 Cloud Computing

Die Bedeutung der Begriffe «Cloud», respektive «Cloud Computing» hat sich in den letzten Jahren zunehmend ausgeweitet und ist heute verschwommen, wobei die Verwendung des Begriffs zu Werbezwecken einiges zu dieser Entwicklung beigetragen hat. Um über Cybersicherheit in der Cloud sprechen zu können, muss zunächst beschrieben werden, was unter einer «Cloud» zu verstehen ist. Erst anschliessend lässt sich eine sinnvolle und zweckmässige Diskussion über deren Cybersicherheit führen. Zudem muss die Sicherheitsdiskussion abhängig von den gewählten Cloud-Diensten geführt werden. Um dies zu ermöglichen, beschreiben die folgenden Abschnitte die Charakteristiken von Cloud-Diensten, die Art der damit angebotenen Dienstleistungen sowie die Service- und Bereitstellungsmodelle. Diese Begriffe sind nicht neu oder unbekannt. Die bekannten Definitionen sind aber teilweise unpräzise und lassen zu viel Interpretationsspielraum.

Bei jeder Art von Cloud-Dienstleistungen ist gegeben, dass die Kundin respektive der Kunde die physische Kontrolle über seine Daten und Dienstleistungen zumindest teilweise an einen Dritten abgibt. Die Cloud-Anbieter stehen damit in jedem Fall in einer Lieferantenbeziehung zu den Kundinnen und Kunden.

Um Missverständnisse zu vermeiden, werden in dieser Technologiebetrachtung Begriffe wie «In der Cloud» oder «Gang in die Cloud» nicht verwendet. Stattdessen werden folgende Begriffe benutzt:

- **Cloud-Anbieter**: Eine Firma, welche Cloud-Dienste oder -Angebote anbietet (und betreibt).
- **Cloud-Dienste, -Lösungen oder -Angebote**: Lösungen, welche die Cloud-Charakteristiken (siehe 1.2.1) erfüllen.
- **Cloud Computing**: Der Überbegriff für alle Cloud-Dienste und -Angebote.

1.2.1 Grundcharakteristiken

Cloud Computing ist ein Modell, das den Zugriff auf IT-Ressourcen und -Dienste über ein Netzwerk ermöglicht. Anstatt eigene Hardware und Software zu kaufen und zu warten, können Organisationen und Einzelpersonen diese Ressourcen von einem Cloud-Anbieter mieten und nach Bedarf nutzen.

Die folgenden fünf Grundcharakteristiken stammen von der «Definition of Cloud Computing» [1] vom National Institute of Standards and Technology (NIST). Diese gelten als allgemein anerkannt und akzeptiert.

- **On-Demand-Zugriff**: Nutzer können jederzeit (bevorzugt über ein Self-Service Portal oder eine Programmierschnittstelle) auf die benötigten Cloud-Dienste zugreifen, ohne dass eine manuelle Intervention des Cloud-Anbieters erforderlich ist.[1]
- **Ressourcen-Pooling**: Die Netzwerk-, Speicher- oder Prozessor-Ressourcen des Anbieters werden gebündelt und mehreren Nutzern dynamisch zugewiesen. Dies ermöglicht eine effiziente Nutzung dieser Ressourcen.
- **Schnelle Skalierbarkeit**: Die Ressourcen können schnell, automatisiert und nach Bedarf skaliert werden, um auf veränderte Anforderungen zu reagieren.
- **Messbarkeit**: Die Nutzung der Ressourcen wird kontinuierlich überwacht und gemessen; dies ermöglicht eine transparente Abrechnung und Optimierung.
- **Zugang übers Internet**: Der Management-Zugang zum Cloud-Account ist über das Internet erreichbar.[2] Dabei wird die Management-Umgebung (das Netzwerk, über welches Dienste betrieben und administriert werden) von der Systemumgebung (die Umgebung, in der die (Server-) Systeme laufen und die Daten gespeichert werden) unterschieden. Die Systemumgebung muss nicht übers Internet erreichbar sein.

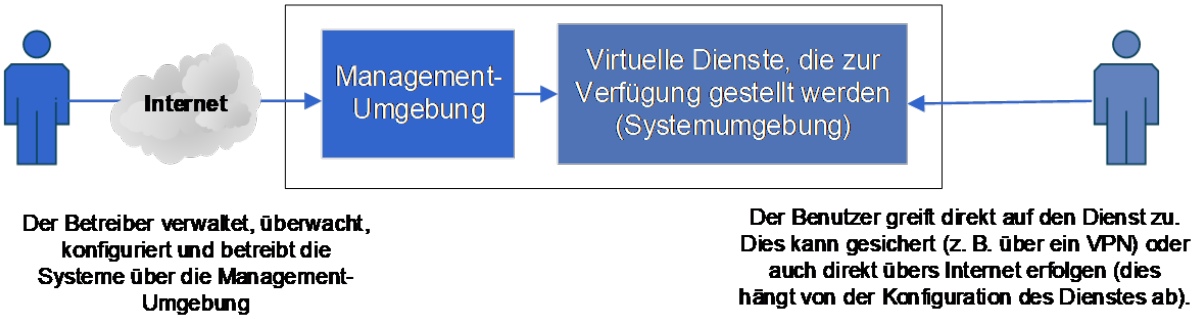

Abbildung 1: Use-Case-Diagramm: Management und Systemumgebung bei Cloud-Diensten

Eine öffentliche Cloud-Dienstleistung wird nur dann als solche verstanden, wenn der Anbieter (mindestens) diese fünf Charakteristiken erfüllt.[3]

1.2.2 Dienstleistungen

Cloud-Dienste unterscheiden sich in Bezug auf die angebotenen Dienstleistungen, welche natürlich auch kombiniert werden können:

1. Datenspeicherung: Die Leistung besteht primär im Aufbewahren von Daten.
2. Rechenleistung: Es wird primär Rechenkapazität zur Verfügung gestellt.
3. Netzwerk: Es geht hauptsächlich darum, Daten im Internet effizient zur Verfügung zu stellen (rascher Zugriff auf Daten unabhängig vom geographischen Standort).

[1] Die Charakteristik «On-Demand-Zugriff» ist bei grösseren Firmen und auch in der Bundesverwaltung bei Erstbeschaffungen nicht immer nutzbar. Obwohl der Cloud-Anbieter eigentlich ein Self-Service-Portal für den Bezug der Cloud-Dienste hat, erlauben die Beschaffungsprozesse nicht immer, dieses auch zu nutzen.

[2] Die Definition nach NIST spricht hier nur von «Broad Network Access» und erwähnt den Management-Zugang nicht. Bei Cloud-Diensten ist es aber gerade der Management-Zugang, der über das Internet zugänglich ist. Ob die virtuellen Ressourcen, welche vom Cloud-Anbieter zur Verfügung gestellt werden, auch über das Internet verfügbar sind, entscheidet der Kunde, respektive die Kundin. Mehr dazu in Kapitel 1.2.4.

[3] Eine weitere Charakteristik, die oft mit Cloud-Diensten assoziiert wird, ist die Verwendung moderner Methoden bei Entwicklung und Betrieb sowie die Automatisierung von Arbeitsschritten. Dieses Merkmal ist aber nicht nur bei Cloud-Diensten relevant, sondern unterscheidet eher zwischen einer modernen und einer klassischen Arbeitsweise.

1.2.3 Servicemodelle

Im Cloud Computing gibt es mehrere Servicemodelle, die dem Kunden oder der Kundin mehr oder weniger Spielraum bei der Verwendung der Dienstleistungen überlassen. Daraus ergeben sich auch unterschiedliche Erwartungen an die Verantwortung des Cloud-Anbieters, respektive den Kunden oder der Kundin. Die drei Hauptservicemodelle sind:

- **Infrastructure-as-a-Service (IaaS)**: Der Cloud-Anbieter bietet grundlegende IT-Ressourcen wie Rechenleistung, Speicher und Netzwerke an. Die Kunden können virtualisierte Netzwerke, Server und Speicher selbst konfigurieren. Bei IaaS werden Infrastrukturen von Dritten im Auftragsverhältnis betrieben. Für den Betrieb der Server, Datenbanken, Anwendungen und anderen Diensten sind die Kunden zuständig.
- **Platform-as-a-Service (PaaS)**: Der Cloud-Anbieter stellt eine Plattform zur Verfügung, auf der Anwendungen entwickelt, bereitgestellt und betrieben werden können. Bei PaaS werden Plattformen von Dritten im Auftragsverhältnis betrieben, für den Betrieb der Anwendungen sind die Kunden zuständig.
- **Software-as-a-Service (SaaS)**: Der Cloud-Anbieter ermöglicht den Zugriff auf Software-Anwendungen über das Internet, ohne dass diese lokal installiert werden müssen. Bei SaaS werden also Software-Lösungen von Dritten im Auftragsverhältnis betrieben.

Es gibt auch Kombinationen der verschiedenen Modelle: M365 z. B. stellt einerseits die bekannten Office-Applikationen bereit (als SaaS-Lösung), bietet aber auch die Plattform zur Verwaltung, Authentifizierung oder Bereitstellung und Entwicklung eigener Applikationen an (PowerTools).

Obwohl SaaS im Kontext von Cloud-Computing gesehen wird, ist dies für die Organisation, welche eine SaaS-Lösung einkauft, betreffend den Überlegungen zur Cybersicherheit und Resilienz weniger relevant. Die Kunden müssen sich nicht mit (Cloud-)Technologien an sich, sondern nur mit Fragen zum Management von IT-Lieferanten und mit dem IT-Outsourcing befassen.[4]

1.2.4 Bereitstellungsmodelle

Weiter werden Cloud-Dienste in nachfolgend drei Bereitstellungsmodelle aufgeteilt.

- **Öffentliche Cloud (Public Cloud)**: Der Zugriff auf die Management-Umgebung zur Verwaltung der Cloud-Dienste wird über das öffentliche Internet bereitgestellt. Die Infrastruktur wird dabei von mehreren Kunden (Mandanten) gemeinsam genutzt. Dabei kann ein Kunde jeweils seine eigenen Daten nutzen, bearbeiten und entscheiden, wem diese zugänglich gemacht werden sollen. Die Systemumgebung ist nur dann öffentlich zugänglich, wenn der Kunde oder die Kundin das so vorsieht.
- **Private Cloud (Private Cloud)**: Cloud-Dienste werden für einen geschlossenen Kreis von Organisationen bereitgestellt und bieten eine höhere Kontrolle. Dies wird meist dadurch sichergestellt, dass die Dienste für die Organisation auf dedizierter Hardware laufen. Dies kann «On premises (On Prem)», das heisst in eigenen Räumlichkeiten, oder beim Cloud-Anbieter erfolgen. Die Management-Umgebung ist dabei grundsätzlich nicht aus dem Internet erreichbar.[5] Wenn sich die Hardware beim Cloud-Anbieter

[4] Dazu gehören selbstverständlich auch die Fragen, wie man seine Daten sichert und seine Prozesse auch bei einem Ausfall des Lieferanten weiterbetreibt.

[5] Während der Begriff Public Cloud relativ klar definiert ist und meist richtig verstanden wird, ist dies beim Begriff der Private Cloud nicht der Fall. Viele Anbieter verstehen darunter einfach eine Umgebung, welche auf ihren eigenen Servern betrieben wird, anstatt die Dienste eines grossen Anbieters wie Amazon, Google oder Microsoft zu verwenden. Dieses Verständnis ist nicht zweckdienlich. Aus Sicht des Bundesamtes für Cybersicherheit (BACS) kann nur dann von einer Private Cloud gesprochen werden, wenn der Management-Zugang eingeschränkt ist.

befindet, wird der Zugang zur Management-Umgebung über einen gesicherten Kanal[6] gewährleistet.

- **Hybride Cloud (Hybrid Cloud)**: Eine hybride Cloud ist eine Kombination aus öffentlicher und privater Cloud, um die Vorteile beider Modelle zu nutzen. Diese Kombination bezieht sich auf die gesamte Infrastruktur einer Organisation, so kann ein Server in einer privaten und ein anderer in einer öffentlichen Umgebung laufen.

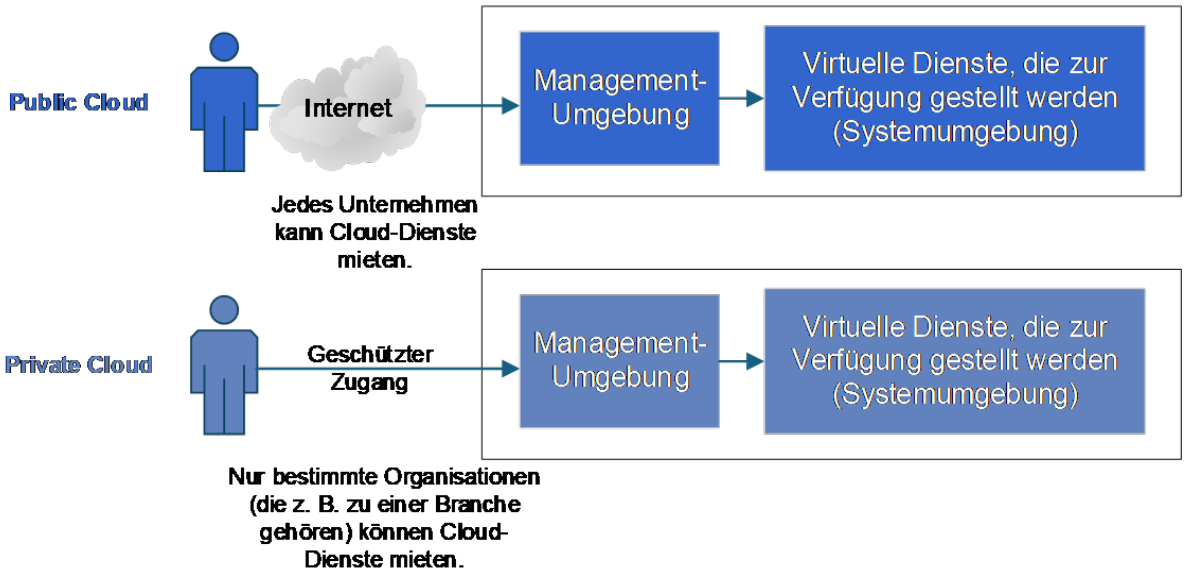

Abbildung 2: Unterscheidung zwischen öffentlicher und privater Cloud aus technischer Perspektive und Sicht des Bundesamtes für Cybersicherheit.

Eine klare Beurteilung, ob eine öffentliche oder private Umgebung verwendet wird, ist nicht immer möglich, da auch Mischformen denkbar sind. Deshalb spielen Bereitstellungs-Modelle für die Beurteilung, ob eine Cloud-Lösung die richtige ist, auch nur eine untergeordnete Rolle. Für die Cybersicherheit ist es eine Frage der Reduktion der Angriffsfläche, diese ist bei einer privaten Umgebung bereits stärker reduziert.

1.2.5 Nicht jede Cloud ist gleich

Aus den Beschreibungen in den letzten Abschnitten wird ersichtlich: Nicht jede Cloud ist gleich. Die folgende Tabelle zeigt dies an konkreten Beispielen auf. Die Entscheidung, diese Dienstleistungen von einem Cloud Provider zu beziehen, muss im Kontext der geplanten Anwendungen geschehen. Es geht also nicht darum, eine binäre Entscheidung für oder gegen eine Cloud-Dienstleistung zu treffen, sondern darum, ob der spezifische Cloud-Dienst in der Zielarchitektur für das Projekt oder die Organisation die richtige Wahl ist.[7]

Servicemodelle	Dienstleistungen	Bereitstellungsmodell	Beispiel
Infrastructure-as-a-Service (IaaS)	Datenspeicherung	Public Cloud	Konfigurierbare Online-Speicherlösungen wie Amazon S3, Google Bucket oder Azure Blob
	Datenspeicherung	Private Cloud	Konfigurier- und skalierbare On-Prem Speicher-Lösungen wie NetAPP SAN
	Rechenleistung	Public Cloud	Virtuelle Server wie Amazon EC2, Azure VM oder Google Compute Engine

[6] Standleitung, Direct Peering, SD-WAN, VPN, sowie explizit erzwungene Zugangsbeschränkung (oft Conditional Access genannt) und weitere ähnliche Technologien sind denkbar.

[7] Diese Sichtweise ermöglicht die Klärung des Begriffs Cloud als Paradigmenwechsel für IT-Dienstleistungen.

	Netzwerk	Public Cloud	Netzwerklösungen wie AWS NAT Gateway, Azure WAF, Google Cloud Firewall
Platform-as-a-Service (PaaS)	Rechenleistung	Public Cloud	Kubernetes-Dienste wie Amazon EKS, Azure AKS, Google GKS oder auch serverless-Dienste wie AWS Lambda oder Azure Functions
	Netzwerk	Public Cloud	Minimalkonfigurierbare Netzwerkdienste wie Google Cloud Armor als DDoS-Schutz.
	Alle	Public Cloud	Anwendungsentwicklungs- und Betriebs-Plattformen wie Microsoft PowerTools oder Google AppSheet.
Software-as-a-Service (SaaS)	Rechenleistung	Public Cloud	Grid Computing, oder auch AWS Quantum Computing Service.
	Datenspeicherung	Public Cloud	Online-Speicherplatz wie Dropbox, Google Drive oder Microsoft OneDrive
	Alle	Public Cloud	Anwendungen wie Microsoft M365, SAP S/4HANA, ChatGPT, Deepl oder Miro.

Tabelle 1: Beispiele verschiedener Cloud-Dienste.

1.3 Cybersicherheit bei Verwendung von Cloud-Diensten

Neben der Tatsache, dass jede Verwendung von Cloud-Diensten eine Frage des Lieferantenmanagements ist, ergeben sich aus den Charakteristiken, Service- und Bereitstellungsmodellen weitere grundsätzliche Herausforderungen:

- Bei Cloud-Lösungen sind die Daten nicht unter alleiniger Kontrolle der Organisation. Bei Problemen mit der Netzwerkanbindung oder beim Dienstleister kann der Zugriff auf die Informationen und Dienstleistungen temporär oder im schlimmsten Fall permanent verloren gehen.
- Für den kryptografischen Schutz von gespeicherten und übertragenen Daten zwischen Kunden und dem Cloud-Anbieter gibt es heute Lösungen. Die grosse Herausforderung ist aber der kryptografische Schutz von Daten, die bearbeitet werden (d. h. sich im Prozessor befinden). Das ist ein aktives Forschungsthema (z. B. «voll homomorphe Verschlüsselung». Hier werden Lösungen gesucht, die es erlauben, verschlüsselte Daten zu bearbeiten, ohne diese zuerst zu entschlüsseln). Weil noch keine entsprechende Lösung vorhanden ist, wird versucht, etwas ähnliches mit spezieller Hardware zu erreichen (Confidential Computing).
- Ein grosses Thema ist auch das Key Management, da der Cloud-Dienst die Entschlüsselungen vornimmt und somit auch die Schlüssel selbst verwaltet. Lösungen, bei denen die Ver- und Entschlüsselung auf dem Client geschehen[8], sind selten. Diese Tatsache gekoppelt mit dem Ressourcen-Pooling führt dazu, dass ein Angreifer, der Zugriff auf die Schlüsselinfrastruktur erlangt[9], auf die Daten vieler Kunden zugreifen kann.
- In traditionellen Netzwerkarchitekturen wird die Management-Zone abgeschottet, sodass der Zugriff nur über gesicherte Zugänge, Netzwerke oder Terminals möglich ist. Bei Verwendung von Public-Cloud-Diensten, ist dieser Zugang im Normalfall für alle möglich, sollten die Zugangsdaten (z. B. ein API-Schlüssel) abhandenkommen, Zugänge falsch konfiguriert werden, oder Schwachstellen in den Cloud-Diensten gefunden werden. Dies bringt unmittelbar die ganze Infrastruktur in Gefahr und ist eine

[8] Diese werden auch als «Hold-Your-Own-Key» bezeichnet.

[9] Als Beispiel dazu: Der Angriff von Storm0588 auf die Microsoft-Umgebung: https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/

zusätzliche Herausforderung, da unautorisiert Zugreifende auch die Protokollierung und das Backup löschen oder modifizieren könnten, wenn sich diese im gleichen Cloud Account befinden sollten.

- Fehlkonfigurationen können zum Beispiel eine unabsichtliche Veröffentlichung eines Cloud-Speichers verursachen. Sie bedingen eine Überwachung und Reaktionsfähigkeit, welche bei anderen, nicht im Internet exponierten Lösungen, weniger essenziell sind. Grundsätzlich ist diese Überwachung (oft auch «Observability» genannt) bei Cloud-Diensten komplexer und anspruchsvoller.
- Nicht direkt sicherheitsrelevant, aber trotzdem wichtig, sind die Kosten. Sicherheitslösungen in der Cloud haben zusätzliche Kosten zur Folge, welche oft linear mit der Anzahl Benutzer wachsen. Dies kann bei grösseren Organisationen dazu führen, dass die Cloud-Dienste teurer werden, als eine eigene Infrastruktur aufzubauen. Ein weiterer Aspekt, gerade bei kleineren Unternehmen: Beim Bezug von Cloud-Diensten wird bei kleinem Budget eher auf zusätzliche, aber notwendige Sicherheitslösungen verzichtet.

2 Cybersicherheits-Überlegungen beim Einsatz von Cloud-Diensten

Dadurch, dass es sich beim Einsatz von Cloud-Computing meist um ein IT-Outsourcing handelt, müssen die Lieferanten entsprechend beurteilt und ausgewählt werden. Die richtige Auswahl der Lieferanten, Zulieferer und Provider ist eine wichtige Voraussetzung, um einen sicheren Betrieb zu gewährleisten. Diese Entscheidung stellt die erste Phase bei der Umsetzung dar. Die zweite Phase umfasst die Systemplanung, Entwicklung und Inbetriebnahme der Cloud-Lösung. Die dritte Phase beinhaltet den Einbezug der Cloud-Dienste im kontinuierlichen Lieferanten-Management der Organisation.[10]

Für die Entscheidungsfindung (erste Phase) sehen wir drei wichtige Schritte, welche wir in den nächsten Abschnitten detaillierter betrachten:

1. Prüfen, ob die rechtlichen Anforderungen an den Cloud-Anbieter erfüllbar sind (siehe Kapitel 2.1).
2. Prüfen, ob technische und organisatorische Anforderungen für einen sicheren und resilienten Betrieb erfüllbar sind (siehe Kapitel 2.2).
3. Anhand der Erfüllbarkeit dieser Anforderungen und wichtiger Kriterien wie der zeitlichen Verfügbarkeit, der Auswirkungen bei Datenverlust oder der IT-Fähigkeiten der eigenen Organisationen beurteilen, ob der Einsatz von Cloud-Diensten die richtige Wahl ist (siehe Leitfragen in Kapitel 2.3).

2.1 Rechtliche Anforderungen

Die rechtlichen Anforderungen hängen von der Rechtsnatur und dem Sitz des Cloud-Anbieters und der Art der bearbeiteten Daten ab. Folgende Anforderungen sollten geprüft werden, weitere branchenspezifischen Anforderungen oder Richtlinien müssen je nach Organisation zusätzlich mitberücksichtigt werden:

1. Sofern die Organisation Daten an einen Cloud-Anbieter übermittelt und von diesem bearbeiten und/oder speichern lässt, braucht es einen **Vertrag** zwischen den Parteien, welcher die gegenseitigen Rechte und Pflichten regelt.[11] Es ist seitens der Organisation zu prüfen, ob gesetzliche oder vertragliche Geheimhaltungsinteressen, wie das Berufs- oder Amtsgeheimnis, dem Vertragsabschluss entgegenstehen. Diesfalls ist sicherzustellen, dass der

[10] Siehe dazu auch: Cybersicherheit in der Lieferkette Bundesamt Cybersicherheit BACS (2024) [2].

[11] Siehe dazu auch: Best Practices für Lieferantenverträge in [2].

Cloud-Anbieter diese Pflichten wahrnehmen kann (vorgängige «Due Diligence»). Zu den Pflichten des Anbieters gehört, dass der Zugang für die Mitarbeiter zu den Systemen strikt geregelt und kontrolliert sein muss. Zudem dürfen bei einer Bearbeitung von Daten, die dem Amts- oder Berufsgeheimnis unterstehen, nur explizit autorisierte Hilfspersonen Zugriff auf solche Daten erhalten. [12]

2. Falls Personendaten von natürlichen Personen an den Cloud-Anbieter übermittelt und von diesem bearbeitet und/oder gespeichert werden, ist ein so genannter **Auftragsdatenbearbeitungsvertrag** (**«Data Processing Agreement»)** zwischen den Parteien abzuschliessen. Im Sinn der jeweiligen Datenschutzgesetzgebung hat die Organisation die Pflichten des Verantwortlichen und der Cloud-Anbieter diejenigen des Auftragsbearbeiters zu erfüllen. Eine Bearbeitung der Daten durch den Cloud-Anbieter als Auftragsbearbeiter ist nur zulässig, falls er die Daten so bearbeitet, wie der Verantwortliche (also die Organisation) es selbst tun dürfte und keine gesetzlichen oder vertraglichen Geheimhaltungspflichten die Übertragung der Datenbearbeitung verbieten. Die Organisationen müssen sich insbesondere vergewissern, dass der Cloud-Anbieter in der Lage ist, die Datensicherheit zu gewährleisten.
3. Wenn eine Bearbeitung der Personendaten ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen natürlichen Person mit sich bringen kann, so muss die Organisation prüfen, ob vorgängig eine **Datenschutz-Folgenabschätzung (DFSA)**, entsprechend den Anforderungen der jeweils anwendbaren Datenschutzgesetzgebung, erstellt werden muss.
4. Personendaten dürfen nur an einen Cloud-Anbieter im **Ausland** übermittelt werden, wenn bestätigt wurde, dass das betreffende Land[13] einen angemessenen Datenschutz gewährleistet. Ist dies nicht so, kann die Übermittlung trotzdem erfolgen, sofern ein geeigneter Schutz durch einen völkerrechtlichen Vertrag, spezielle Vertragsklauseln, spezifische Garantien eines Bundesorgans, vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) genehmigte Standardklauseln oder durch verbindliche organisationsinterne Datenschutzregeln sichergestellt ist.

2.2 Technische und organisatorische Anforderungen

Die Kunden von Cloud-Diensten müssen einerseits Massnahmen vorsehen für den Fall, dass der Cloud-Dienst nicht mehr zur Verfügung stehen sollte (Punkt A) und andererseits den Anbietern Vertrauen können, dass technische und organisatorische Massnahmen wie vereinbart umgesetzt werden. Der dazu notwendige Vertrauensaufbau benötigt Transparenz von Seiten der Anbieter (Punkte B – E). Alle Anforderungen sind so beschrieben, dass die Kundin oder der Kunde dies selbst überprüfen kann, ohne den Versprechen des Cloud-Anbieters blind zu vertrauen:

A. **Notfallplanung und Offline-Backup:** Die Daten in der Cloud-Lösung sollen als Teil der Notfallplanung exportierbar sein und gespeichert werden können. Der Export sollte als Backup auch offline abgelegt werden (als Schutz vor Ransomware). Es sollte auch eine Exit-Strategie definiert werden, um sicherzustellen, dass ein Wechsel des Anbieters jederzeit ohne Datenverlust möglich ist.[14]
B. **Transparenz der Sicherheitsfunktionen:** Die Umsetzung grundsätzlicher Sicherheitsanforderungen zur Gewährleistung der Datensicherheit durch den Cloud-Anbieter muss für die Organisation transparent dokumentiert sein. Zu diesen grundsätzlichen Anforderungen gehören:

[12] Art. 320 und Art. 321 Strafgesetzbuch (StGB)

[13] Siehe dazu auch die Länderliste https://www.fedlex.admin.ch/eli/cc/2022/568/de#annex_1/lvl_u1

[14] Man könnte z. B. einen Wechsel zu einem anderen Anbieter im Notfall bereits planen, diesen aber erst im Bedarfsfall vollziehen.

1. Die Datenübermittlung zwischen der Organisation und dem Cloud-Anbieter muss immer verschlüsselt erfolgen (mittels aktuellen Verschlüsselungsprotokollen wie der aktuellen Version von TLS oder über ein VPN oder ein verschlüsseltes SD WAN).
2. Der Cloud-Anbieter verfügt über Funktionen für die Zugangssteuerung gemäss dem «Need-to-Know-Prinzip» und jede Zugriffsanfrage erfolgt authentisiert. Die Authentisierung muss standardmässig mehrere Faktoren (MFA) verwenden und das Vergeben von Zugängen an Mitarbeiter, Partner, Lieferanten oder Kunden der Organisation muss einfach und übersichtlich[15] sein.
3. Der Management-Zugriff auf die Cloud-Dienste sowie der Zugriff auf Cloud-Anwendungen ist überwacht und vor Denial-of-Service-Angriffen (dem Überlasten der Anwendung mittels vieler Anfragen) oder Brute-Force-Login-Versuchen (dem Versuch, in schneller Abfolge viele Login-Kombinationen auszuprobieren) geschützt.
4. Das Schlüssel-Management ist dokumentiert und entspricht dem Stand der Technik.
5. Da Fehlkonfigurationen schnell zu einer Exponierung von Daten im Internet führen, muss ein Dienst vorhanden sein, welcher Fehlkonfigurationen erkennt, alarmiert und wenn möglich automatisiert beseitigt.

C. **Zugriffstransparenz**: Es gibt eine Funktion, die es Administratoren der Organisation erlaubt, alle Zugriffe auf die Daten und deren Bearbeitung zu überwachen und nachzuvollziehen. Dies beinhaltet auch Zugriffe von Lieferanten und Partner des Cloud-Anbieters. Die Zugriffe und die Bearbeitungen müssen protokolliert werden können und sollten auch Teil der Offline-Backups sein, damit eine Kompromittierung des Cloud-Anbieters die Nachvollziehbarkeit nicht beeinträchtigt.

D. **Produktsicherheit**: Der Cloud-Anbieter zeigt transparent auf, welche Methoden für die sichere Entwicklung ihrer Cloud-Dienste verwendet wurden.

E. **Meldung von Vorfällen und Schwachstellen**: Der Cloud-Anbieter hat einen Prozess, welcher sicherstellt, dass Vorfälle sowie für die Organisation relevante Schwachstellen schnell an die Organisation gemeldet werden. Er publiziert Patches und Änderungen an seinen Diensten öffentlich und hat eine Meldestelle für sicherheitsrelevante Vorfälle und Schwachstellen.[16]

2.3 Leitfragen zur Beurteilung des Einsatzes von Cloud-Diensten

Die Beantwortung nachfolgender Fragen soll als Entscheidungsgrundlage betreffend den Einsatz von Cloud-Diensten dienen und mögliche Risiken aufzeigen, welche entsprechend behandelt werden müssen. Die detaillierten Lösungsarchitekturen, welche nach diesem Entscheid umzusetzen wären, sind nicht Teil der vorliegenden Betrachtung.

Frage 1 - *Anforderungen*: Sind die rechtlichen, organisatorischen oder technischen Anforderungen erfüllbar (Kapitel 2.1 und Kapitel 2.2)?

Wenn die rechtlichen Anforderungen nicht erfüllbar sind, ist auf den Einsatz der Cloud-Lösung zu verzichten.

Bei fehlender Erfüllbarkeit der technischen und organisatorischen Anforderungen, z. B. weil Daten nicht exportierbar sind (und deshalb kein eigener Notfallplan vorbereitet werden kann), oder weil der Cloud-Anbieter die minimal notwendigen Sicherheitsfunktionen nicht anbietet, respektive bei der Dokumentation der Sicherheit nicht transparent ist, ist Vorsicht geboten. Die damit einhergehenden Risiken sind sorgfältig zu betrachten. In diesem Fall fehlen die

[15] Wenn das Management der Berechtigungen kompliziert ist, führt dies schnell zu Fehlern. Daher muss eine übersichtliche und einfache Lösung oder Schnittstelle zur Verfügung stehen.

[16] Diese kann im Rahmen einer über das Web verfügbaren security.txt-Datei gemäss RFC 9116 erfolgen.

Grundlagen, um dem Anbieter zu vertrauen. Insbesondere bei der Bearbeitung von Personendaten sind so die Anforderungen an die Datensicherheit nicht mehr umsetzbar.

Wenn keine der geprüften Cloud-Lösungen die Voraussetzungen erfüllen kann, ist eine Lösung im Eigenbetrieb (on-premise oder unter eigener Kontrolle gehostet) zu bevorzugen.

Frage 2 - *Zeitliche Verfügbarkeit*: Ist die Cloud-Lösung für die Aufrechterhaltung der Geschäftsprozesse zeitkritisch?

Diese Frage ist wichtig, denn ein wichtiges Merkmal der Cloud-Dienste ist, dass der Zugriff von der Verfügbarkeit des Internets abhängt. Wenn z. B. ein Patienteninformationssystem über das Internet angeboten wird, welches ohne Unterbruch verfügbar sein sollte, müssen Alternativen im Hinblick auf den Ausfall der Cloud-Infrastruktur vorhanden sein. Auch muss eine permanente Verfügbarkeit der Internet-Verbindung sichergestellt sein.

Frage 3 - *Datenverlust*: Wie schwerwiegend sind die Folgen eines Datenverlusts für die Betroffenen?

Wenn für die Organisation selbst oder für die Personen, deren Daten im System bearbeitet werden, ein Verlust der Daten schwerwiegend ist (z. B. bei Gerichtsakten), muss ein Offline-Backup der Daten in der Organisation selbst einrichtbar sein.

Bei schwerwiegenden Auswirkungen bei einem unautorisierten Zugang oder einer Veröffentlichung dieser Daten (Verletzung der Vertraulichkeit) ist der Einsatz von Cloud-Lösungen nicht empfohlen, da Unsicherheiten verbleiben, wer genau auf die Daten zugreifen kann. Wenn dennoch die Nutzung von Cloud-Diensten geplant ist, sollten die Daten kryptographisch stark geschützt werden und bei der Systemplanung und -entwicklung auf diese Bedrohung hingewiesen werden.

Frage 4 - *Fähigkeiten der (IT-)Organisation*: Ist unsere Organisation fähig, die notwendigen eigenen Massnahmen zum Schutz umzusetzen?

Wenn die Fähigkeiten der Organisation beschränkt sind, ist ein Outsourcing bei einem Cloud-Anbieter risikoreich. Der Einsatz von Cloud-Lösungen, gerade bei Infrastructure-as-a-Service Servicemodellen, erfordert eine höhere Maturität der eigenen IT, da die Überwachung und der Betrieb dieser Lösungen im Vergleich zum Eigenbetrieb eine zusätzliche Komplexität mit sich bringen. Bei SaaS-Lösungen ist hingegen die Fähigkeit der Notfallplanung bei einem Ausfall des Anbieters entscheidend. Diese Notfallplanung könnte auch über einen weiteren IT-Outsourcing-Partner beschafft werden, was jedoch die Kosten und auch den Aufwand des Lieferanten-Managements erhöht und mit den Vorteilen gut abgewogen werden sollte.

3 Referenzen

[1] Mell, P.; Grance, T. *The NIST Definition of Cloud Computing - NIST SP 800-145* National Institute of Standards and Technology (2011), Zugriff am 2. Mai 2025, https://csrc.nist.gov/publications/detail/sp/800-145/final

[2] *Cybersicherheit in der Lieferkette* Bundesamt Cybersicherheit BACS (2024), Zugriff am 2. Mai 2025, https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/lieferkette.html