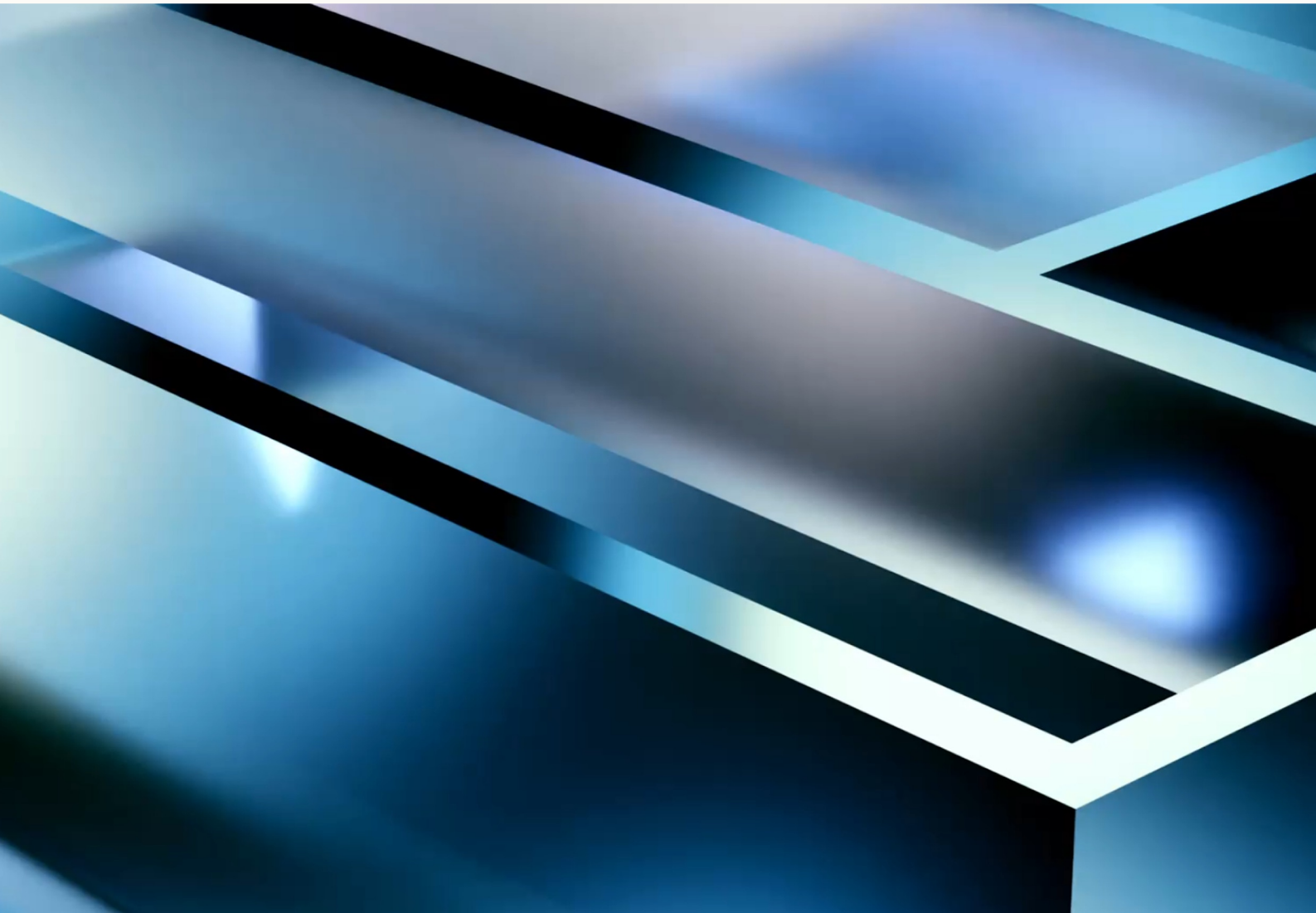
GovTech Deutschland

Cloud-Reallabor

Leitfaden zur Erstellung einer Cloud-Nutzungsstrategie

Erstveröffentlichung.
Stand Dezember 2025



GovTech Deutschland

Cloud-Reallabor

Leitfaden zur Erstellung einer Cloud-Nutzungsstrategie

Version 1.0 (Stand: 12/2025)

Disclaimer:
Dieser Leitfaden vereint die Expertise der Autoren und Projektbeteiligten mit aktuellen Veröffentlichungen zum Thema „Erstellung einer Cloud-Nutzungsstrategie“ (Strategie & Methodik) und entwickelt eine Schritt-für-Schritt-Anleitung zur Erstellung einer Cloud-(Nutzungs-)Strategie gemäß den Aufgaben des Mindeststandards zur Nutzung externer Cloud-Dienste des Bundesamtes für Sicherheit in der Informationstechnik. Dabei wird die fachspezifische Verwaltungsexpertise direkt mit einbezogen.

Hinweis: Die konkrete Erstellung von Cloud-Nutzungsstrategien erfordert eine eingehende Analyse der spezifischen Rahmenbedingungen. Es muss geklärt werden, ob und wo eine Nutzung der Cloud sinnvoll ist und verfolgt werden sollte.

Wie gelingt eine sichere Nutzung der Cloud und was ist strategisch notwendig?

Executive Summary

Viele digitale Dienste und Anwendungen, die heute in unserem Alltag unverzichtbar sind, basieren auf einer flexiblen und skalierbaren Cloud-Infrastruktur. Die Cloud ist gekommen, um zu bleiben. Jede Institutionsleitung sollte sich deshalb eher früher als später mit der Cloud und deren Auswirkungen auf die eigene Organisation beschäftigen.

Warum sollte man die Cloud nutzen? Was ist der Vorteil für die Institution? Wie rechnet sich der Business Case?

Vorteile in der Nutzung der Cloud können u.a. darin liegen, dass neue Lösungen schneller genutzt, Mitarbeitende und Kunden besser unterstützt und entlastet oder Lastspitzen wirtschaftlicher abgedeckt werden können. Als Reaktion auf den Fachkräftemangel kann es erforderlich sein, die eigene Fertigungstiefe zu reduzieren, mehr einzukaufen und weniger selbst herzustellen. Sofern diese Lösungen zwingend benötigt werden, kommt man um die Nutzung der Cloud-Angebote kaum herum.

Auf der anderen Seite gibt es auch Nachteile. Die Abläufe in der Institution verändern sich grundlegend, neue Abhängigkeiten entstehen, das erforderliche Expertenwissen fehlt und muss erst aufgebaut werden. Es entstehen neue Risiken aus der Zusammenarbeit mit externen Dienstleistern.

Vor der Nutzung der Cloud sind viele Aufgaben zu erledigen. Dabei spielen insbesondere die Anforderungen an die Informationssicherheit oder den Datenschutz eine zentrale Rolle. Um Institutionen den Zugang zur Cloud zu erleichtern, ist dieser Leitfaden erarbeitet worden. Er soll die Bearbeitung der einzelnen Aufgaben, die u.a. der Mindeststandard des BSI zur Nutzung externer Cloud-Dienste voraussetzt, erleichtern. Daher beziehen sich die Vorschläge, Checklisten und Kriterienkatalogen auf diese BSI-Vorgaben. Nicht zu vergessen ist die Diskussion rund um das Thema „Digitale Souveränität“, die ebenfalls immer stärker in den Mittelpunkt rückt.

Der Leitfaden erhebt keinen Anspruch auf Vollständigkeit. Vielmehr soll er den Einstieg in eine Cloud-Nutzung erleichtern und Themen und Aufgaben aufzeigen, die bei der Nutzung der Cloud im Vorfeld berücksichtigt werden müssen oder sollten. Es werden Beispiele angeführt, ohne gleich die eine passende Lösung vorzugeben, denn je nach Organisation und deren Rahmenbedingungen ergeben sich unterschiedliche Bewertungen und Ergebnisse.

Cloud-Nutzung ist kein reines IT-Thema? Wofür soll die Cloud genutzt werden und wie werden die Geschäftsziele damit unterstützt?

Vorwort

Wir haben in vielen Gesprächen erlebt, dass es leicht zu einem Missverständnis kommen kann, wenn es um das Thema „Cloud-Strategie“ geht. Auf unsere Nachfrage, ob es auch eine Cloud-Nutzungsstrategie gibt, erhalten wir häufiger die Antwort: „Ja wir haben eine Cloud-Strategie.“ Darin wird dann erklärt, was die Cloud ist und wie das eigene Rechenzentrum sich in hybriden Szenarien mit dieser verbinden kann. Doch es bleiben oft wichtige Fragen unbeantwortet: Warum soll die Cloud genutzt werden? Was sind die Geschäftsziele, die durch die Nutzung der Cloud erreicht werden sollen? Welchen Nutzen und welchen Mehrwert kann die Cloud bieten, aber auch welche Risiken können sich durch die Nutzung der Cloud ergeben?

Christian Janssen fragte mich Anfang des Jahres: „Was hältst du von der Idee, dass wir über das Cloud-Reallabor auf dem Campus von GovTech Deutschland gemeinsam eine Anleitung erstellen, wie man eine Cloud-Nutzungsstrategie erstellt?“. Ich war schnell überzeugt, dass dies für Viele einen echten Mehrwert bringen kann.

Harald: Christian, warum habt ihr als Capgemini ein Interesse daran, so einen Leitfaden zu erstellen? Geht das nicht zu Lasten eures Beratungsgeschäfts? Häufig werden externe Berater beauftragt, eine solche Cloud-Nutzungsstrategie zu erstellen.

Christian: Wenn wir kurzfristig und ausschließlich auf das Strategieberatungsgeschäft schauen, magst Du Recht haben. Wenn sich allerdings eine wesentlich höhere Zahl von Institutionen einfacher und schneller mit ihrer Cloud-Nutzungsstrategie beschäftigen können, dann erarbeiten sie die Grundlagen für eine erfolgreiche Cloud-Transformation der deutschen Verwaltung und damit schaffen wir als Berater einen Public Value. Das war unsere Motivation für die Erstellung dieses Leitfadens.

Harald: Was mir an dem Ansatz gefällt ist, dass die Institutionen wieder mehr selbst machen und sich mit den Dingen beschäftigen. Eine Cloud-Nutzungsstrategie ist zwar ein „Must-have“, doch sollte das nicht so verstanden werden, dass man diese Strategie von Dritten erstellen lässt und dann in den Schrank legt und nicht damit arbeitet.

Christian: In diesen dynamischen Zeiten ist eine kontinuierliche Beschäftigung mit der Strategie für die Institution eine der dringlichsten Leitungsaufgaben. Da Digitalisierung und Staatsmodernisierung eng mit der IT- und Cloud-Transformation verbunden sind, muss die Cloud-Nutzungsstrategie wesentlicher Baustein dieser Hausstrategie sein. Sie ist damit ein „Must-have“ und eben keine „Nice-to-have-Schrankware“.

Harald: Von der Idee bis zur Umsetzung hat es einige Zeit gedauert. In der Zwischenzeit hat das BSI ein Management-Blitzlicht zum Thema Cloud-Nutzungsstrategie veröffentlicht und auf den Cloud-Webseiten des BSI auch eine Anleitung und Folien für die Durchführung eines Workshops veröffentlicht. Haben wir jetzt umsonst gearbeitet?

Christian: Nein, das haben wir nicht. Unser Leitfaden ist eine Ergänzung, die auf den Dokumenten des BSI aufbaut. Wir beschäftigten uns mit unseren Umsetzungsvorschlägen, Checklisten und Kriterienkatalogen konkreter mit den notwendigen Themen und das immer mit Bezugnahme auf die Grundlagen des BSI.

Harald: Ja, da hat uns unser Netzwerk im Cloud-Reallabor gut geholfen, viele Hintergrundgespräche zu führen, um mögliche Dopplungen frühzeitig zu vermeiden und auf den Handreichungen des BSI aufzubauen. Nach der Veröffentlichung des BSI Management-Blitzlicht zum Thema Cloud-Nutzungsstrategie haben wir das noch einmal überprüft und etwas nachgeschärft und am Ende hat es richtig gut gepasst.

Christian: Ja, das hat gut funktioniert. Und nicht nur das BSI hat neue Dokumente veröffentlicht, auch die EU hat im September noch ihr Cloud Sovereignty Framework[1] veröffentlicht. Das Thema „Digitale Souveränität“ spielt natürlich auch eine gewichtige Rolle bei der Cloud-Nutzung.

Harald: Das kann ich nur unterstreichen. Wir hatten im Cloud-Reallabor in einem unserer Proof-of-Concepts die Wechselfähigkeit zwischen verschiedenen Cloud-Anbietern erprobt. Von Beginn an muss mitgedacht werden, wie kontrolliert in eine Cloud hineingegangen wird und wie diese auch wieder verlassen werden kann und wohin es dann gehen kann. Das Thema „Digitale Souveränität“ hat natürlich auch an der Stelle eine hohe Bedeutung in der Cloud-Nutzungsstrategie. Ein Deutsches, Europäisches Cloud-Angebot muss aus meiner Sicht Bestandteil einer jeden Multi-Cloud-Strategie sein.

Christian: Ja, das kann ich nur unterstreichen. Jede Institution sollte sich eine Multi-Cloud-Strategie erarbeiten und abwägen, welche Schwerpunkte sie dort setzen möchte.

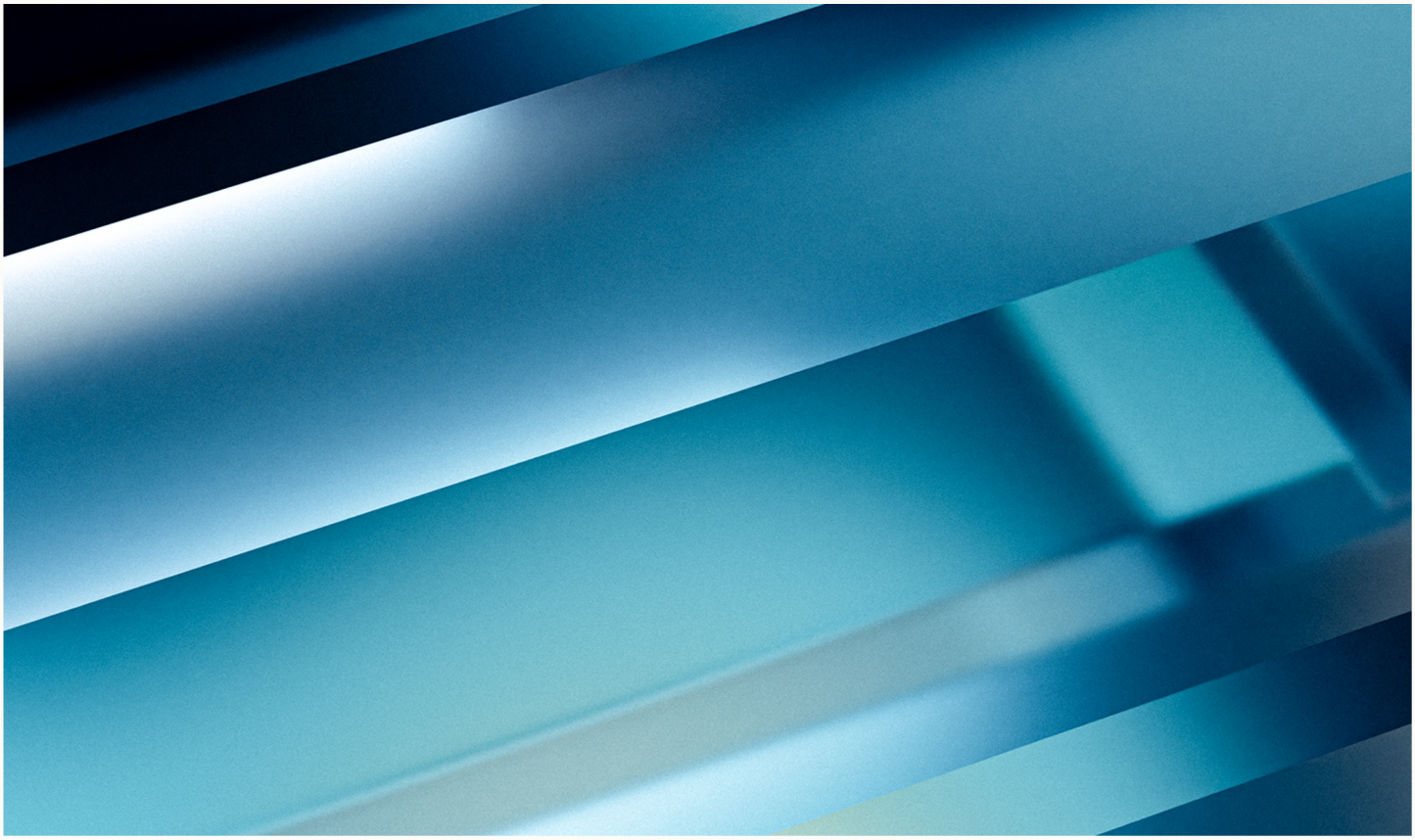
Harald: Nun sind wir fertig und der Leitfaden ist veröffentlicht. Ich bin einmal gespannt, ob und was es für Rückmeldungen gibt. An dieser Stelle noch einmal ausdrücklichen Dank für eure Idee und Bereitschaft hier mitzumachen, und auch ein herzliches Dankeschön an alle, die im Hintergrund mitgewirkt haben. Es war eine tolle Zusammenarbeit und hat Spaß gemacht.

Christian: Lieber Harald, ich danke Dir für die große Unterstützung und die vielen guten Gespräche rund um das Thema. Ich danke aber auch den Capgemini-Kollegen, insbesondere Martin Lambinet, die aktiv an der Erstellung dieses Leitfadens mitgewirkt haben.

Harald Joos
Projektleiter Cloud-Reallabor & Cloud-Beauftragter der DRV Bund

Dr. Christian Janssen
Direktor Cloud Center of Excellence Public Sector Capgemini Deutschland GmbH

1 - Hinweis: Die Fußnoten wurden aus Gründen der Lesbarkeit gesammelt am Ende des Dokuments platziert.



Inhaltsverzeichnis

Executive Summary 3
Vorwort 4
Ausgangssituation & Ziel des Leitfadens 7
Exkurs 8
Cloud-Nutzungsstrategie 9
Definition der Ziele der Cloud-Nutzung 11
Definition der Chancen der Cloud-Nutzung 12
Erstellung einer Richtlinie zur Risikoanalyse der Cloud-Nutzung 14
Dokumentation der rechtlichen & organisatorischen Anforderungen der Cloud-Nutzung 15
Dokumentation der technischen Anforderungen der Cloud-Nutzung 16
Festlegung, welche Dienste in welchem Bereitstellungsmodell von Cloud-Anbietern bezogen werden 17
Schlussfolgerungen & Ausblick 23
Autoren 24

Ausgangssituation & Ziel des Leitfadens

Ausgangssituation

In den letzten zehn Jahren haben Cloud-Technologien die globale Welt der IT grundlegend verändert. Viele digitale Dienste und Anwendungen, die heute in unserem Alltag unverzichtbar sind, basieren auf einer flexiblen und skalierbaren Cloud-Infrastruktur. In der industriellen Digitalisierung stellt die Cloud eine unverzichtbare Basis für innovative Prozesse und neue Geschäftsmodelle dar. Im Gegensatz dazu zeigt sich die deutsche Verwaltung bisher zurückhaltend gegenüber der Einführung von Cloud-Lösungen. Seit dem Jahr 2024 hat sich trotzdem einiges in Bewegung gesetzt: Für viele Institutionen wurden grundsätzliche Voraussetzungen geschaffen, um Cloud-Lösungen beschaffen zu können. Zudem wurden weiterführende Veröffentlichungen publiziert, wie z.B. der „Mindeststandard des BSI zur Nutzung externer Cloud-Dienste“ (eine erste Veröffentlichung erfolgte bereits 2017) sowie für die Umsetzung einer Cloud-Nutzungsstrategie hilfreiche Dokumente des BSI, wie das „Management Blitzlicht - Cloud sicher nutzen - das geht nur mit Strategie“ oder die „Anleitung und Folien zur Erstellung einer Cloud-Nutzungsstrategie“[2]. Zudem konnten praktische Erfahrungen der Mitglieder in die Projekte des Cloud-Reallabors auf dem Campus von GovTech Deutschland eingebracht werden.

Wie allerdings die Ergebnisse der Cloud-Studie des Wegweiser-Verlages aus dem Jahr 2024[3] zeigen, haben sich nur wenige Institutionen auf den Weg gemacht und die wesentlichen Themen der Cloud-Nutzung, Cloud-Nutzungsstrategie, Sicherheitsrichtlinie und Datenklassifikation umgesetzt. Diese Vorarbeiten sind jedoch ebenso essenzielle Voraussetzung, wie der Einbezug der Leitungsebene, um Cloud-Lösungen produktiv nutzen zu können.

Ziel dieses Leitfadens

Um Institutionen den Zugang zur Cloud zu erleichtern, ist in einem Projekt des Cloud-Reallabors auf dem Campus von GovTech Deutschland dieser Leitfaden erarbeitet worden. Der Leitfaden soll die Bearbeitung der einzelnen Aufgaben, welche u.a. der Mindeststandard des BSI zur Nutzung externer Cloud-Dienste fordert, durch Beispiele, Erläuterungen oder Checklisten erleichtern. So sollen Institutionen bei der Erstellung ihrer Cloud-Nutzungsstrategie unterstützt und befähigt werden, diese mit geringerem Aufwand und Dauer aber ausreichender inhaltlicher Qualität und einer notwendigen Beteiligung der Leitungsebene erstellen können. Sind diese Aufgaben bearbeitet, ist die Grundlage einer sich anschließenden Cloud-Nutzung gelegt. Weitere Schritte in die Cloud, wie z.B. der Aufbau einer Landingzone, können auf Basis der erarbeiteten Arbeitsergebnisse umgesetzt werden.

Der vorliegende Leitfaden ist als ein erstes „Minimal Viable Product“ (MVP) zu verstehen. Er soll durch Erfahrungen und Feedback der Anwendenden weiter geschärft und damit verbessert werden[4].

Der Leitfaden ist wie folgt aufgebaut:

- Kurzer Exkurs zur Erläuterung des Cloud-Begriffs
- Darstellung des Inhalts einer Cloud-Nutzungsstrategie
- Schritte zur Erarbeitung einer Cloud-Nutzungsstrategie

Die Kapitel beginnen jeweils mit den Anforderungen des Mindeststandards des BSI[5] sowie des für die Cloud-Nutzung relevanten BSI IT-Grundschutz Bausteins OPS 2.2[6]. Es werden Vorschläge für die operative Bearbeitung gemacht und eine Empfehlung gegeben, wer an der Bearbeitung der jeweiligen Aufgabe zu beteiligen ist bzw. mit einbezogen werden sollte. Die Umsetzungsvorschläge werden entweder in den Kapiteln des Leitfadens beschrieben oder durch die beigefügte Exceltabelle ergänzt.

Auch die Excelliste erhebt keinen Anspruch auf Vollständigkeit und ist ebenfalls ein erstes MVP. Sie enthält drei Arbeitsblätter. Jedes Arbeitsblatt besteht aus Checklisten oder Kriterienkatalogen, welche die Inhalte des jeweiligen Kapitelthemas inhaltlich vertiefen.

Exkurs

Alle reden von der Cloud, aber was ist eigentlich Cloud Computing?[7]

So wie eine Wolke keine scharfen Grenzen hat, gibt es auch keine exakte Definition von Cloud Computing. Denn Cloud Computing ist ein Paradigma. Damit ist eine grundsätzliche Denkweise gemeint, und das deutet schon darauf hin, dass es sich nicht nur um eine Evolution in der IT handelt, sondern um etwas Neues. Nach der Norm ISO/IEC 22123-1:2023 ist Cloud Computing ein „Paradigma, um einen netzwerkbasierten Zugang auf ein skalierbares und elastisches Reservoir gemeinsam nutzbarer physikalischer oder virtueller Ressourcen nach dem Selbstbedienungsprinzip und bedarfsgerechter Administration zu ermöglichen“. Ressourcen sind hier insbesondere Rechenleistung (compute), Speicher (storage) und Netze (network). Dieses Reservoir ist elastisch und skalierbar, d.h. es kann sehr schnell an den Bedarf angepasst werden, z.B. wenn temporär ein zusätzlicher Server oder weitere Ressourcen benötigt werden.

Das Cloud-Paradigma basiert auf einigen bekannten Prinzipien, die konsequent umgesetzt und geschickt miteinander kombiniert werden.

- **Entkopplung von der Hardware**, d.h. es gibt eine Virtualisierungsschicht über der Hardware: Wird z.B. Speicherplatz benötigt, bekommt der Kunde keine Festplatte, sondern nur Speicherplatz und es wird nicht mitgeteilt, wo genau die Daten gespeichert sind. Die Virtualisierungsschicht kümmert sich um den gemeinsam genutzten Speicherplatz.
- **Alles ist ein Service** und alle Kommunikation läuft über standardisierte Schnittstellen: Im obigen Beispiel würde ein Cloud-Dienst mit dem Speicherdienst über dessen Schnittstelle kommunizieren. Auch die Administration der gesamten Cloud-Services erfolgt über fest definierte Schnittstellen.
- **Alles ist Code**: Da nur über definierte Schnittstellen kommuniziert wird und alles Schnittstellen hat, kann über Code, also Skripte etc., alles definiert, implementiert und konfiguriert werden.
- **Alles ist maximal automatisiert**: Das Innenleben einer Cloud ist so automatisiert, dass im Regelfall keine manuellen Eingriffe im laufenden Betrieb notwendig sind. Neue Kunden buchen Cloud-Dienste und bauen z.B. ein komplexes virtuelles Rechenzentrum in der Cloud, ohne dass ein Administrator des Cloud-Anbieters irgendetwas tun muss.

Beim Cloud Computing von der „Industrialisierung der IT“ zu sprechen, beschreibt die neue technologische Entwicklung recht anschaulich. Die Möglichkeiten des Cloud Computings sind sehr vielfältig, sodass sich Cloud-Dienste zum Teil grundlegend voneinander unterscheiden. „Die Cloud“ gibt es nicht. Daher braucht es ein differenziertes Vokabular, um die Cloud besser (be-)greifen zu können.

Stellt ein Cloud-Anbieter seine Dienste für alle zugänglich im Internet zur Verfügung, spricht man von einer „Public Cloud“. Baut sich dagegen eine Institution eine Cloud ausschließlich für die eigene Nutzung, heißt sie „Private Cloud“. Das sind zwei Beispiele von vielen Varianten.

Auch der wesentliche Kern eines Cloud-Dienstes kann variieren. Bei „Infrastructure as a Service“ (IaaS) stellt der Cloud-Dienst Ressourcen wie Rechenleistung, Speicher und Netze zur Verfügung. „Software as a Service“ (SaaS) sind Cloud-Dienste, die ähnliche Funktionen wie eine herkömmliche Software anbieten, beispielsweise zur Bürokommunikation. Dazwischen liegt „Platform as a Service“ (PaaS), wo grundlegende Dienste angeboten werden, auf die z.B. Anwendungen nach „Software as a Service“ aufbauen. Die Service-Modelle unterscheiden sich wesentlich in Umfang und Dienstleistung.

Cloud-Nutzungsstrategie

Aufgaben nach BSI

Im Baustein „NCD.2.1.01 Strategie für die Cloud-Nutzung“ des Mindeststandards des BSI zur Nutzung externer Cloud-Dienste finden sich folgende Vorgaben zur Erarbeitung einer Cloud-Nutzungsstrategie[8]:

a) Die Einrichtung MUSS gemäß Anforderung „OPS.2.2.A1 Erstellung einer Strategie für die Cloud-Nutzung“ des BSI IT-Grundschutzbausteins OPS.2.2 erstellen.
b) Die Einrichtung MUSS in dieser Strategie für die Cloud-Nutzung festlegen, wie sie mit Risiken bei der Nutzung externer Cloud-Dienste umgeht. Hierzu MUSS eine Richtlinie zur Risikoanalyse erstellt werden.
c) Die Einrichtung MUSS prüfen, ob ein externer Cloud-Dienst grundsätzlich mit den in ihrer Strategie für die Cloud-Nutzung definierten Zielen, Chancen und Risiken vereinbar ist. Die Einrichtung DARF einen externen Cloud-Dienst NUR nutzen, wenn dieser die in der Strategie für die Cloud-Nutzung definierten Ziele, Chancen und Risiken angemessen unterstützt.
d) Die Einrichtung MUSS vor der Nutzung eines externen Cloud-Dienstes eine Risikoanalyse gemäß der in NCD.2.1.01 Buchstabe b) festgelegten Richtlinie durchführen.

Die Anforderung „OPS.2.2.A1 Erstellung einer Strategie für die Cloud-Nutzung“ des BSI IT-Grundschutzbausteins OPS.2.2 gibt folgende Vorgaben:

Eine Strategie für die Cloud-Nutzung MUSS erstellt werden. Darin MÜSSEN Ziele, Chancen und Risiken definiert werden, die die Institution mit der Cloud-Nutzung verbindet. Zudem MÜSSEN die rechtlichen und organisatorischen Rahmenbedingungen sowie die technischen Anforderungen untersucht werden, die sich aus der Nutzung von Cloud-Diensten ergeben. Die Ergebnisse dieser Untersuchung MÜSSEN in einer Machbarkeitsstudie dokumentiert werden. Es MUSS festgelegt werden, welche Dienste in welchem Bereitstellungsmodell zukünftig von Cloud-Anbietern bezogen werden sollen. Zudem MUSS sichergestellt werden, dass bereits in der Planungsphase zur Cloud-Nutzung alle grundlegenden technischen und organisatorischen Sicherheitsaspekte ausreichend berücksichtigt werden. Für den geplanten Cloud-Dienst SOLLTE eine grobe individuelle Sicherheitsanalyse durchgeführt werden. Diese SOLLTE wiederholt werden, wenn sich technische und organisatorische Rahmenbedingungen wesentlich verändern. Für größere Cloud-Projekte SOLLTE zudem eine Roadmap erarbeitet werden, die festlegt, wann und wie ein Cloud-Dienst eingeführt wird.

Weitere Vorgaben, welche in der Strategie enthalten sein müssen:

Die Einrichtung MUSS prüfen, ob ein externer Cloud-Dienst grundsätzlich mit den in ihrer Strategie für die Cloud-Nutzung definierten Zielen, Chancen und Risiken vereinbar ist. Die Einrichtung DARF einen externen Cloud-Dienst NUR nutzen, wenn dieser die in der Strategie für die Cloud-Nutzung definierten Ziele, Chancen und Risiken angemessen unterstützt.

Zudem MUSS sichergestellt werden, dass bereits in der Planungsphase zur Cloud-Nutzung alle grundlegenden technischen und organisatorischen Sicherheitsaspekte ausreichend berücksichtigt werden.

Abgeleitet aus den o.a. Forderungen MUSS die Cloud-Nutzungsstrategie die folgenden sechs Themen enthalten:

1. Definition der Ziele der Cloud-Nutzung
2. Definition der Chancen der Cloud-Nutzung
3. Erstellung einer Richtlinie zur Risikoanalyse der Cloud-Nutzung
4. Dokumentation der rechtlichen und organisatorischen Rahmenbedingungen der Cloud-Nutzung (in einer Machbarkeitsstudie)
5. Dokumentation der technischen Anforderungen der Cloud-Nutzung (in einer Machbarkeitsstudie)
6. Festlegung, welche Dienste in welchem Bereitstellungsmodell von Cloud-Anbietern bezogen werden

Im Folgenden werden zu den ersten fünf der o.a. Themen Vorschläge und Anregungen zur Erstellung einer Cloud-Nutzungsstrategie gegeben. Für die Bearbeitung des sechsten Themas - welche Dienste in welchem Bereitstellungsmodell von Cloud-Anbietern bezogen werden – erscheint aus Sicht der Autoren des Leitfadens eine Bearbeitung erst sinnvoll, nachdem die Organisation für sich selbst Klarheit darüber gewonnen hat, welche Service- und Bereitstellungsmodelle präferiert werden. Insofern werden in dem entsprechenden Abschnitt dieses Leitfadens dafür notwendige Vorüberlegungen beschrieben, die ebenfalls Bestandteil einer Cloud-Nutzungsstrategie sein sollten.

Ob ein externer Cloud-Dienst grundsätzlich mit den in der Strategie für die Cloud-Nutzung definierten Zielen, Chancen und Risiken vereinbar ist, wird im Kapitel zur Auswahl des Cloud-Servicemodells beschrieben.

Die Anforderung, dass bereits in der Planungsphase zur Cloud-Nutzung alle grundlegenden technischen und organisatorischen Sicherheitsaspekte berücksichtigt werden, wird inhaltlich durch die Abschnitte Richtlinie zur Risikoanalyse und Dokumentation der organisatorischen und technischen Anforderungen erfüllt.

BSI: IT-Grundschutz

Der IT-Grundschutz ist eine vom Bundesamt für Sicherheit in der Informationstechnik entwickelte und frei verfügbare Vorgehensweise, um ein ganzheitliches Informationssicherheits-Managementsystem in Institutionen umzusetzen.

Der IT-Grundschutz ist Methode, Anleitung, Empfehlung und Hilfe zur Selbsthilfe für Institutionen, Unternehmen und Behörden, die sich mit der Absicherung ihrer Daten, Systeme und Informationen befassen wollen.

Definition der Ziele der Cloud-Nutzung

Aufgabenstellung

Anforderung „OPS.2.2.A1 Erstellung einer Strategie für die Cloud-Nutzung“ des BSI IT-Grundschutzbausteins OPS.2.2:
„Eine Strategie für die Cloud-Nutzung MUSS erstellt werden. Darin MÜSSEN Ziele (...) definiert werden, die die Institution mit der Cloud-Nutzung verbindet.“

Umsetzungsvorschläge

Folgt man der These, dass Cloud Computing ein neues Paradigma ist, welches Institutionen, deren Mitarbeitenden und auch deren IT grundlegend verändert, dann ist es auch eine Leitungsaufgabe, sich inhaltlich mit diesem Thema auseinanderzusetzen. Angesichts eines hohen Digitalisierungsdrucks und der Möglichkeiten moderner Cloud-Technologien können diese der Institution helfen, die ständig steigenden Herausforderungen zu bewältigen.

Ausgangspunkt der Erarbeitung einer Cloud-Nutzungsstrategie sollte eine realistische Bestandsaufnahme innerhalb der Institution sein. Als Hilfsmittel hierfür dient das Arbeitsblatt Cloud-Readiness-Fragebogen im beigefügten Excel-Dokument. Die dort aufgeführten Kategorien und Reifegrade verdeutlichen Tiefe sowie Umfang der Veränderungen. Sie ermöglichen der Hausleitung einen ersten fundierten Überblick über den Status Quo ihrer Organisation und aktuellen IT-Landschaft bezogen auf deren Stand in der Cloud-Transformation zu bekommen, indem sie sich selbst nach den angebotenen Reifegraden bewertet[10].

Der zweite Schritt der Cloud-Nutzungsstrategie besteht in der Definition der Ziele der Cloud-Nutzung. Mögliche Ziele einer solchen Cloud-Strategie, welche die Institution kurz-, mittel- und langfristig erreichen will, könnten dabei sein:

- Weiterentwicklung und Erweiterung der bestehenden (IT-)Strategie um Cloud-Transformation und -Nutzung
- Systematische Auseinandersetzung mit dem langfristigen Einfluss der Cloud-Transformation und -Nutzung auf die eigene Institution und der damit einhergehenden Veränderungen
- Vorbereitung der eigenen Organisation und Prozesse auf den Einsatz neuer Technologien
- Übersicht über Kosten und Nutzen, d.h. über den notwendigen einmaligen und regelmäßigen Investitionsbedarf in Personal, Organisation und Infrastruktur sowie dem diesen gegenüberstehenden Mehrwert der Cloud-Nutzung für die Institution
- Erarbeitung einer Cloud-Transformationsstrategie für die Institution sowie einer Angebotsübersicht über Cloud-Dienste und über die Verfügbarkeit von Angeboten in den jeweiligen Cloud-Betriebsmodellen
- Erarbeitung von Kriterien zur Auswahl strategischer Cloud-Services, Anbietern sowie Servicemodelle (z.B. SaaS vor PaaS vor IaaS, IaaS only, ...)
- Schaffung klarer Regeln für den Cloud-Einsatz, auch zum bewussten Umgang mit einem möglichen Vendor Lock-in

Beteiligte

Institutionsleitung, Abteilungsleitung, IT-Leitung

Definition der Chancen der Cloud-Nutzung

Aufgabenstellung

Anforderung „OPS.2.2.A1 Erstellung einer Strategie für die Cloud-Nutzung“ des BSI IT-Grundschutzbausteins OPS.2.2:
„Darin MÜSSEN (...) Chancen (...) definiert werden, die die Institution mit der Cloud-Nutzung verbindet.“

Umsetzungsvorschläge

Mögliche Chancen und Vorteile einer Cloud-Nutzung sind nachfolgend exemplarisch aufgeführt. Diese sind dahingehend zu bewerten, inwieweit sie für die Institution relevant sind und in welcher Form sie in der Cloud-Strategie wirken sollen:

Höhere Effizienz und Skalierbarkeit:
Workloads können von einer automatischen Skalierbarkeit in der Private oder Public Cloud profitieren. Dadurch können Kosten für ungenutzte Infrastruktur vermieden und z.B. temporäre Workloads ohne initiale Kapitalinvestitionen ausgeführt werden.

Beschleunigung der Digitalisierung durch Nutzung innovativer Cloudservices:
Die Spezialisierung und das Wissen des Cloud-Anbieters durch Nutzung von Best Practices und organisatorische Erkenntnisse könnten dazu beitragen, das Design der Anwendungen und deren Workloads zu modernisieren und sie effektiver zu verwalten. Proof-of-Concepts, Proof-of-Values und Erprobungen neuer Technologien können auf einer temporären Infrastruktur durchgeführt werden. Diese kann schnell bereitgestellt und verworfen werden, wenn sie nicht mehr benötigt wird.

Verkürzte Einführungszeit neuer Verfahren:
Die Nutzung der Cloud kann die Markteinführungszeit von Verfahren verkürzen, da bereits vorhandene Lösungen genutzt werden können, ohne dass eine lokale Infrastruktur bereitgestellt und verwaltet werden muss.

Kostentransparenz durch Pay-per-Use-Modell:
Den Cloud-Kunden wird die Infrastruktur- und Dienste-Nutzung in Rechnung gestellt, die in Anspruch genommen wird. Cloud-Anbieter verfügen in der Regel über Metriken und Dashboards, um genaue Abrechnungs- und Nutzungsstatistiken bereitzustellen. Diese unterstützen die Kostentransparenz. Investive Ausgaben in Infrastruktur - welche sich zudem noch an einer Maximalauslastung über die Nutzungsdauer der Infrastruktur orientieren – ändern sich hin zu konsumptiv schwankenden Ausgaben. Mit welchen Kosten die Cloud-Nutzung verbunden ist und ob es durch die Cloud-Nutzung zu Kostensenkungen oder -erhöhungen kommt, sollte aus der Wirtschaftlichkeitsberechnung deutlich werden.

Verbesserte Erfüllung von Compliance- und Informationssicherheits-anforderungen:
Cloud-Anbieter sind bestrebt, Sicherheit durch Design zu bieten, den neuesten Stand der Technik und Best Practices in der Praxis widerzuspiegeln. Darüber hinaus verfügen sie in der Regel über viele nationale und internationale (Sicherheits-) Zertifizierungen bzw. Nachweise (z. B. BSI-IT-Grundschutz, C5-Testat).

Evergreening Software:
Cloud Services und insbesondere SaaS-Angebote haben in der Regel den Vorteil, dass sie immer auf dem neuesten Stand sind und kontinuierlich durch inkrementelle Updates Funktionserweiterungen erfahren, ohne dass für die Institution Betriebsaufwände entstehen. Damit verbundene Nachteile können entstehen, wenn z.B. neue funktionale Erweiterungen im Standard nicht genutzt werden sollen oder dürfen und sich diese nicht deaktivieren lassen.

Reduzierung der Fertigungstiefe zur Entlastung des Personals von (Routine-) Aufgaben:
Beim Bezug von SaaS-Services aus der Cloud ist kein dediziertes Team für Betrieb und Wartung der Anwendung inkl. Infrastruktur erforderlich. Wartung und Software-Updates sind in der Regel im Cloud-Angebot enthalten. Bei PaaS und IaaS wird nur die Infrastruktur und Laufzeitumgebung direkt vom Cloud-Anbieter verwaltet, die Entwicklung und der Betrieb der Anwendung muss jedoch weiterhin selbst (von der Institution) erbracht werden. In der Cloud spricht man bei den Service-Modellen von „shared responsibility“ - im Unterschied zu einem bisherigen 100%igen Eigenbetrieb, liegt ein Teil der Verantwortung zukünftig beim Cloud-Anbieter.

Dadurch reduziert sich der Aufwand der eigenen, internen IT-Mannschaft. Dies kann unterstützen, die altersbedingte Fluktuation und den prognostizierten Fachkräftemangel in der IT zu kompensieren.

Idealerweise lassen sich die identifizierten Chancen in der Cloud-Nutzungsstrategie so SMART[11] quantifizieren, dass sie im weiteren Zeitablauf zur Erfolgsmessung in der Umsetzung der Cloud-Strategie genutzt werden können. So geben diese auch einen Input zur ersten Kosten-Nutzen-Abschätzung für die initiale Beurteilung der Wirtschaftlichkeit der Cloud-Nutzung. In eine erste Kostenschätzung sind neben den reinen Betriebskosten der Nutzung eines Cloud-Dienstes auch die Kosten für die Einführung, die Schulung der Mitarbeitenden und des Administrationspersonals sowie gegebenenfalls für neue Hardware und den Ausbau der Netzkapazitäten zu berücksichtigen. In die Kosten-Nutzen-Abschätzung sollte auch der strategische Wert der Ressourcen Know-how, Mitarbeitende, IT-Systeme und Anwendung einfließen. So könnten sich auf der Nutzenseite beispielsweise Kostenersparnisse bei der Erneuerung von Hard- und Software ergeben, Leistungen können ggf. flexibler und schneller erbracht und die Cybersicherheit potenziell erhöht werden. Eine erste Kosten-Nutzen-Abschätzung kann aus der Bearbeitung der Spalten J-L der als Excel-Datei beigefügten Checkliste erfolgen.

Beteiligte

Fach-, IT-Verantwortliche, Institutions-, Unternehmensleitung, Informationssicherheits- und Datenschutzbeauftragter

Erstellung einer Richtlinie zur Risikoanalyse der Cloud-Nutzung

Aufgabenstellung

Anforderung „OPS.2.2.A1 Erstellung einer Strategie für die Cloud-Nutzung“ des BSI IT-Grundschutzbausteins OPS.2.2:
„Darin MÜSSEN (...) Risiken definiert werden, die die Institution mit der Cloud-Nutzung verbindet.“

Anforderung „OPS.2.2.A2 Erstellung einer Strategie für die Cloud-Nutzung“ des BSI IT-Grundschutzbausteins OPS.2.2:
„Auf Basis der Cloud-Nutzungs-Strategie MUSS eine Sicherheitsrichtlinie für die Cloud-Nutzung erstellt werden. Sie MUSS konkrete Sicherheitsvorgaben beinhalten, mit denen sich Cloud-Dienste innerhalb der Institution umsetzen lassen. Außerdem MÜSSEN darin spezielle Sicherheitsanforderungen an den Cloud-Diensteanbieter sowie das festgelegte Schutzniveau für Cloud-Dienste hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit dokumentiert werden. Wenn Cloud-Dienste internationaler Anbieter genutzt werden, MÜSSEN die speziellen länderspezifischen Anforderungen und gesetzlichen Bestimmungen berücksichtigt werden.“

Umsetzungsvorschläge

Standen bisher die Chancen und Potentiale der Cloud-Nutzung im Vordergrund, so ist es in gleichem Maße erforderlich, sich mit den spezifischen Risiken, insbesondere bei der Nutzung der Cloud-Angebote, auseinander zu setzen. Durch die Inanspruchnahme von Cloud-Services, statt diese wie bisher selbst zu betreiben, entstehen neue Herausforderungen und neue spezifische Risiken für die Institution. Mögliche Risiken lassen sich grundsätzlich in rechtliche, technische, politische, organisatorische sowie Business-Continuity-Risiken kategorisieren. So birgt bspw. eine nicht definierte Exit-Strategie für die Beendigung der Cloud-Nutzung eine Vielzahl von Risiken für die Institution. Die beigefügte Excelliste gibt im Arbeitsblatt Risikoliste[12] einen Überblick über das Exit-Risiko sowie weitere mögliche Risiken im Zusammenhang mit der Nutzung von Cloud Angeboten.

Durch die Erarbeitung einer Richtlinie zur Risikoanalyse der Cloud-Nutzung muss sich die Institution mit diesen Risiken beschäftigen und kann auf diese Weise ein standardisiertes und einheitliches Vorgehen zur Bewertung von Cloud-Services innerhalb der Institution geben. Idealerweise erweitert die Institution ihre bestehenden Risikoanalysen und Sicherheitsrichtlinien um die relevanten Themen der Cloud-Nutzung.

Aufgabe der Institution ist es nun, zu entscheiden, welche Risiken (s. Excel Arbeitsblatt Risikoliste) auf sie zutreffen und welche der beschriebenen Risikomitigationen für sie relevant sind. Relevante Risiken und Mitigationen sind als Inhalte der Richtlinie zur Risikoanalyse zu dokumentieren.

Beteiligte

Fach-, IT-Verantwortliche, Informationssicherheits-, Datenschutzbeauftragte, Management-Sponsor

Dokumentation der rechtlichen & organisatorischen Anforderungen der Cloud-Nutzung

Aufgabenstellung

Anforderung „OPS.2.2.A1 Erstellung einer Strategie für die Cloud-Nutzung“ des BSI IT-Grundschutzbausteins OPS.2.2:
„Zudem MÜSSEN die rechtlichen und organisatorischen Rahmenbedingungen (...) untersucht werden, die sich aus der Nutzung von Cloud-Diensten ergeben. Die Ergebnisse dieser Untersuchung MÜSSEN in einer Machbarkeitsstudie dokumentiert werden.“

Umsetzungsvorschläge

Bei den rechtlichen und organisatorischen Rahmenbedingungen zur Cloud-Nutzung gibt es zwar Schnittmengen, allerdings unterscheiden sich die Rahmenbedingungen von Institution zu Institution und sind daher zumindest in Teilen anders. Ausgehend von den bestehenden Rahmenbedingungen der IT-Nutzung sowie der aktuellen Sicherheitsrichtlinie gilt es für die Institution die externen und internen Faktoren zu definieren, die sich aus dem Umstand ergeben, dass die Datenhaltung und der Betrieb der Anwendungen nicht mehr innerhalb der eigenen Institution oder dem bisherigen IT-Dienstleister erfolgen. Den Einstieg und eine erste Strukturierung des Themas unterstützt die inhaltliche Beantwortung der Fragen 4-14 im beigefügten Excel-Arbeitsblatt Cloud-Readiness-Fragebogen. Zudem sollten die relevanten rechtlichen und organisatorischen Risiken aus dem beigefügten Excel-Arbeitsblatt Risikenliste weiter vertieft werden. Darüber hinaus kann die Beantwortung der folgenden Fragen unterstützen:

Rechtlicher Rahmen
- Welche Gesetze, Regelwerke, Standards, Kriterienkataloge sind einzubeziehen?
- Welche Anforderungen in Bezug auf Informationssicherheit, Daten- und Geheimschutz sind zu erfüllen?

Organisatorischer Rahmen
- Welche Änderungen ergeben sich in den Beschaffungsprozessen durch eine Cloud-Nutzung?
- Verändern sich Rollen und Zuständigkeiten durch das mit der Cloud-Nutzung verbundene Shared-Responsibility-Modell zwischen der Institution und dem Cloud-Anbieter?
- Ändern sich Rollen und Verantwortlichkeiten zwischen IT und Fachbereichen durch die Cloud-Nutzung?
- Müssen Personalgewinnungs- & Qualifizierungsmaßnahmen initiiert werden?

Finanzieller Rahmen
- Welche Haushaltsmittel sind für den Aufbau und den anschließenden Betrieb der Cloud erforderlich?
- Sind cloudbasierte Abrechnungsmodelle im Einklang mit dem bestehenden Haushaltsrecht?
- Erfordern Cloud-basierte Abrechnungsmodelle weitere Anpassungen in Finanzierung und Prozessen?

Beteiligte

Fach-, IT-Verantwortliche, Informationssicherheits-, Datenschutzbeauftragte, Management-Sponsor

Hinweis

Die Mindeststandards des BSI beschreiben die rechtlichen und organisatorischen Anforderungen in einer sogenannten Machbarkeitsstudie, ohne diese näher zu spezifizieren. Aus diesem Grunde empfiehlt dieser Leitfaden die Beschreibung dieser Anforderungen als eigenes Kapitel in der Cloud-Nutzungsstrategie zu dokumentieren.

Dokumentation der technischen Anforderungen der Cloud-Nutzung

Aufgabenstellung

Anforderung „OPS.2.2.A1 Erstellung einer Strategie für die Cloud-Nutzung“ des BSI IT-Grundschutzbausteins OPS.2.2:
„ … Zudem MÜSSEN (…) sowie die technischen Anforderungen untersucht werden, die sich aus der Nutzung von Cloud-Diensten ergeben. Die Ergebnisse dieser Untersuchung MÜSSEN in einer Machbarkeitsstudie dokumentiert werden.“

Umsetzungsvorschläge

Nachfolgend sind auf der Grundlage der zuvor geleisteten Vorarbeiten die technologischen Anforderungen zu definieren, die sich u.a. daraus ergeben, dass die Datenhaltung und der Betrieb der Anwendungen nicht mehr innerhalb der eigenen Institution oder dem bisherigen IT-Dienstleister erfolgen. Zum Einstieg und ersten Strukturierung des Themas wird die inhaltliche Beantwortung der Fragen 15-21 im beigefügten Excel-Arbeitsblatt Cloud-Readiness-Fragebogen empfohlen. Zudem sollten die relevanten technischen und Business-Continuity-Risiken aus dem beigefügten Excel-Arbeitsblatt Risikenliste weiter vertieft werden:

- Welche Maßnahmen und Sicherheitsanforderungen sind mit den jeweiligen Kategorien der Datenklassifizierung verbunden und welche Cloud-Umgebung lässt sich unter Berücksichtigung der jeweiligen Maßnahmen für welche Daten nutzen?
- Wie erfolgt ein sicherer Austausch von Daten zwischen unterschiedlichen Cloud-Plattformen und der On-Premise-Infrastruktur?
- Wie wird die Cloud-Lösung technisch und organisatorisch in bestehende IT-Infrastrukturen integriert?
- Welche Cloud-Dienste zur Virtualisierung und stellt der Cloud-Anbieter für den Cloud-Nutzer bereit (z.B. Docker und Kubernetes), um eine flexible Bereitstellung und Verwaltung von Anwendungen zu ermöglichen?
- Welche Netzwerkverbindungen mit welcher Bandbreite und Latenz sind vorhanden bzw. notwendig, um die Cloud-Dienste über eine sichere, stabile und schnelle Netzwerkverbindung (sowohl Internet als auch Direktverbindung) anbinden zu können?

Beteiligte

IT-Verantwortliche, Informationssicherheits- und Datenschutzbeauftragte

Festlegung, welche Dienste in welchem Bereitstellungsmodell von Cloud-Anbietern bezogen werden

Aufgabenstellung

Anforderung „OPS.2.2.A1 Erstellung einer Strategie für die Cloud-Nutzung“ des BSI IT-Grundschutzbausteins OPS.2.2:
“Es MUSS festgelegt werden, welche Dienste in welchem Bereitstellungsmodell zukünftig von Cloud-Diensteanbietenden bezogen werden sollen.“

Umsetzungsvorschläge

In den nachfolgenden Abschnitten wird das weitere Vorgehen in der Auswahl des Cloud-Bereitstellungsmodells, ergänzt um die Auswahl des Service-Modells, des Cloud-Services selbst sowie die Auswahl des Cloud-Anbieters beschrieben.

Auswahl des Cloud-Bereitstellungsmodells
Das Cloud-Bereitstellungsmodell bestimmt, wo die Cloud-Dienste ‚produziert‘ werden. Ob in der Private Cloud, welche von der Institution selbst oder von einem öffentlichen IT-Dienstleister betrieben wird, oder einer Public Cloud, deren Services von einem privatwirtschaftlichen Unternehmen der Institution angeboten werden. Bereits heute gibt es große Vielfalt an Cloud-Angeboten, aus denen die Institution auswählen kann. In der jetzigen Phase der Cloud-Strategie sollte sich die Institution grundlegend Gedanken über die Eignung dieser beiden Modelle für ihre Anwendungen machen. Dafür sollten auf der Grundlage der zuvor definierten Rahmenbedingungen und Anforderungen die Regeln definiert werden, in welchem grundsätzlichen Bereitstellungsmodell welche Anwendungen zu betreiben sind.

Dabei könnten beispielsweise die folgenden Abwägungen anwendungsbezogen erfolgen:

1. Schutzbedarf und Datenklassifizierung

- **Private Cloud:** Sehr hoher und ggf. hoher Schutzbedarf (z. B. Geheimschutz, VS-NfD, personenbezogene oder besonders schützenswerte Daten): Hier kommt oft eine Private Cloud in Betracht.
- **Public Cloud:** Die Verarbeitung sensibler Daten in einer Public Cloud ist nur unter strengen Auflagen und mit spezifischen Sicherheitskonzepten und Genehmigungen möglich. Öffentlich verfügbare Daten oder Daten mit einem geringeren Schutzbedarf können hingegen grundsätzlich auch in Public Clouds verarbeitet werden.

2. Compliance & Rechtliche Vorgaben

- **Private Cloud:** Kann oft spezifische regulatorische Anforderungen (z. B. DSGVO, BSI IT-Grundschutz) leichter erfüllen. Zu berücksichtigen ist, dass die intern erbrachten Leistungen häufiger nicht zusätzlich zertifiziert und auditiert werden bzw. sind. Durch physische Isolation und dedizierte Ressourcen kann grundsätzlich das geforderte Sicherheitsniveau erreicht werden.
- **Public Cloud:** Moderne Public Clouds bieten hohe Sicherheitsstandards, aber das Risiko von Multi-Tenant-Umgebungen und geteilten Ressourcen bleibt bestehen. Es muss der Nachweis erbracht werden, dass alle Compliance-Anforderungen erfüllt werden. Hier sind Zertifizierungen, Technisch-Organisatorische Maßnahmen und der Standort der Datenzentren zu berücksichtigen.

3. Kosten & Skalierbarkeit

- **Private Cloud:** Höhere Anfangsinvestitionen und oft höhere laufende Betriebskosten, da zusätzliche Ressourcen für eine schnelle Skalierung oder um auf mögliche Lastspitzen reagieren zu können, vorgehalten werden müssen.
- **Public Cloud:** Bietet hohe Skalierbarkeit und ein Pay-as-you-go-Modell, durch das keine hohen Infrastrukturinvestitionen nötig sind. Beispielsweise geeignet für dynamische Workloads, kurzfristig oder temporäre Ressourcennutzung und schnelle Innovationen.

4. Flexibilität & Kontrolle

- **Private Cloud:** Für Anwendungen, die maximale Kontrolle über Infrastruktur sowie individuelle Anpassungen erfordern, aber auch geringere Skalierung aufweisen.
- **Public Cloud:** Für Anwendungen, die flexibel und schnell skalierbar, eher standardisiert sind, aber weniger individueller Steuerungsoptionen bedürfen.

5. Innovation & Vendor Lock-In

- **Private Cloud:** Viele internationale Software-Anbieter bieten ihre Anwendungen vermehrt nur noch aus der Public Cloud an. Sofern parallel On-Premise-Lösungen angeboten werden, haben diese teilweise einen geringeren Funktionsumfang, als die Cloud-Angebote. Infolgedessen findet Innovation vermehrt und schneller in der Public Cloud statt. Es stellt sich daher auch die Frage, ob die gewünschte Anwendung noch und wie lange als lokal installierbare Software verfügbar ist.
- **Public Cloud:** Insbesondere bei innovativen SaaS-Anwendungen aus der Public Cloud gerät die Institution leicht in eine Anhängigkeit vom Cloud-Anbieter. Hier ist es wichtig, das Verhältnis des Nutzens der Cloud-Anwendung zum Vendor Lock-in bei dessen Cloud-Anbieter zu bewerten. Diese Abwägung wird u.a. im Abschnitt Cloud-Service-Modell vertieft. Bei den Abhängigkeiten sind vermehrt auch veränderte geopolitische Rahmenbedingungen zu berücksichtigen, wie sie im Rahmen der Diskussion um die „Digitale Souveränität“ deutlich werden.

Die nachfolgende Abbildung zeigt beispielhaft, wie die Ergebnisse der Cloud-Nutzungsstrategie in einem Entscheidungsbaum operationalisiert und visualisiert werden könnten. Ein solcher Entscheidungsbaum kann die Wahl des Bereitstellungsmodells für die Institution in konkreten Fällen unterstützen bzw. klären. Jede Institution muss diesen Entscheidungsbaum entsprechend ihrer Anforderungen selbst entwickeln und definieren

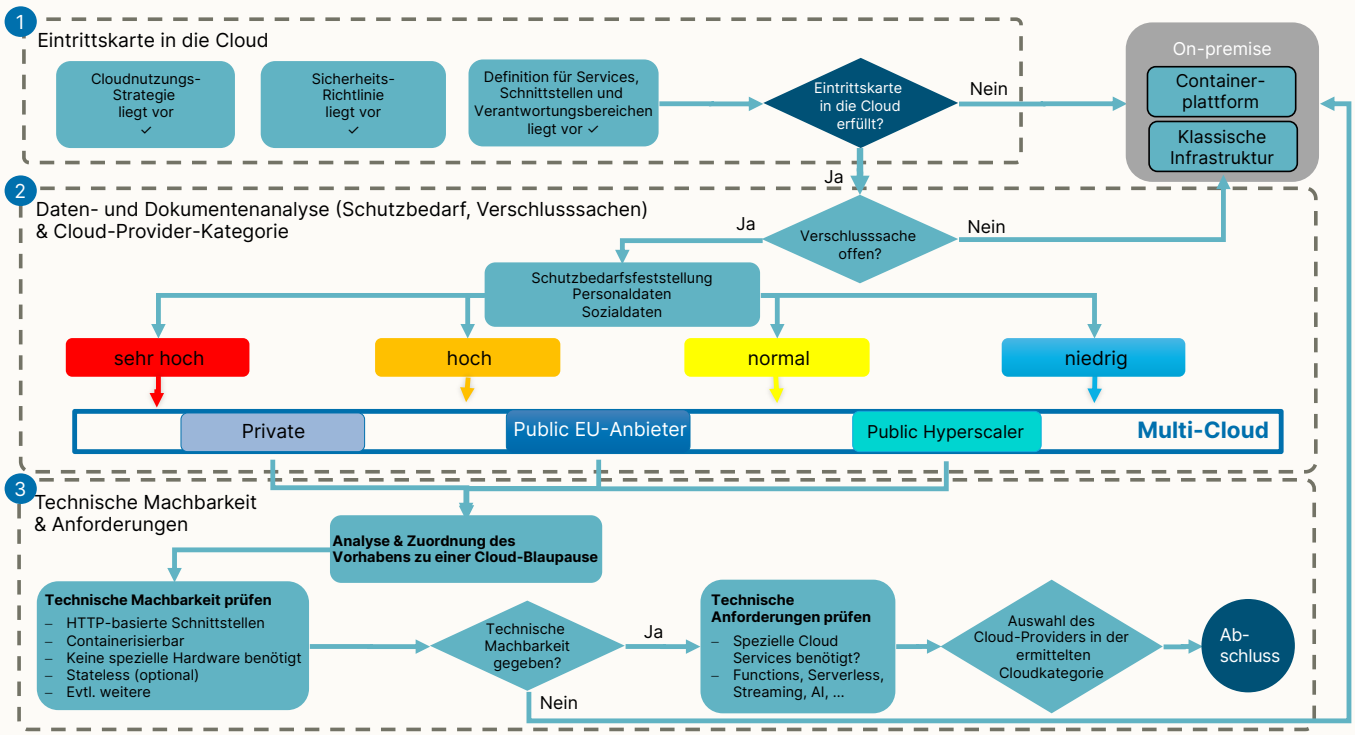


Abbildung 1: Beispiel eines Entscheidungsbaumes

Beteiligte

IT-Verantwortliche, Informationssicherheitsbeauftragte, Management-Sponsor

Auswahl des Cloud-Servicemodells

Nach der Festlegung der Entscheidungsregel für das passende Cloud-Bereitstellungsmodells und vor der Auswahl des oder der Cloud-Anbieter sollte sich die Institution Gedanken über ihre präferierten Cloud-Servicemodelle machen. Diese Modelle unterscheiden sich in ihrer Wertschöpfungstiefe und beeinflussen damit die organisatorischen und technischen Schnittstellen zum Cloud-Anbieter, die Eigenwertschöpfung der Institution und den unmittelbaren Mehrwert bzw. Nutzen des Cloud-Services.

Die Bewertung richtet sich nach den jeweiligen Rahmenbedingungen. Maßgeblich zu berücksichtigen sind u.a. Anforderungen an den Datenschutz, den Geheimschutz und die Informationssicherheit. Hierdurch ergeben sich häufig Einschränkungen bei den Nutzungsmöglichkeiten. Eine kurze Bewertung der Cloud-Servicemodelle könnte exemplarisch wie folgt aussehen:

Infrastructure as a Service (IaaS)
Die Institution kann virtualisierte Server, Speicher- und Netzwerkdienste buchen, deren Administration liegt bei der Institution.

Bewertung:
- **Vorteile:** Schnelle Umsetzung von Vorhaben, Kostenersparnis gegenüber eigener Hardware-Investitionen.
- **Nachteile:** Die Institution bleibt für die Sicherheit und Konfiguration der darauf laufenden Anwendungen selbst verantwortlich (z.B. Verschlüsselung, Netzwerksicherheit); Abhängigkeiten vom Cloud-Anbieter

Priorisierung:
Eher gering, da viele Anwendungen aktuell on-premise laufen und sich durch eine Verlagerung des IT-Betriebs erst einmal keine direkten Vorteile ergeben. Zudem gibt es wenige zwingende Ereignisse, um in eine Cloud-Migration zu investieren (Ausnahme: Erfolgreiche Cyberangriffe mit längerem Ausfall)

Platform as a Service (PaaS)
Die Institution plant Plattformdienste (z.B. Datenbanken, Container-Orchestrierung, DevOps-Tools, Identity Management, KI-Plattformen) zu nutzen. Diese Dienste werden vom Cloud-Anbieter betreut und sind z.B. Grundlage für die Entwicklung cloud-nativer Software oder von KI-Lösungen.

Bewertung:
- **Vorteile:** Skalierbarkeit, Integrationsmöglichkeiten, zentrale/kurzfristige Bereitstellung von Basisdiensten (z.B. Anonymisierung, Datenintegration).
- **Nachteile**: Abhängigkeiten, mögliche Vendor Lock-ins

Priorisierung:
Höher – PaaS-Services sind elementarer Bestandteil einer Digitalisierungs- und Anwendungserneuerungsstrategie, da viele Anwendungsfälle auf PaaS-Dienste angewiesen sind.

Software as a Service (SaaS)
Die Institution möchte fachagnostische oder fachliche Services out-of-the-Box einkaufen und nutzen (z. B. Fach- und Querschnittsanwendungen, Lernplattformen, KI-Modelle, Messenger, Datenplattformen).

Bewertung:
- **Vorteile:** Direkte Wertschöpfung/ Mehrwert für die Nutzergruppen, geringere Komplexität der IT-Infrastruktur, da u.a. Mandantenfähigkeit, Informationssicherheit, Skalierbarkeit durch den SaaS-Anbieter zu lösen sind.
- **Nachteile:** Hoher Vendor Lock-in, fehlende Individualität der Lösung

Priorisierung:
Hoch – SaaS-Dienste dienen zur Reduzierung der Komplexität und unterstützen eine schnelle Digitalisierung und Nutzung innovativer Lösungen.

Beteiligte

Fachbereiche, IT-Verantwortliche, Informationssicherheitsbeauftragte, Management-Sponsor

Cloud-Service-Auswahl

Nachdem die Institution eine Vorstellung über die Cloud-Bereitstellung und präferierten Service-Modelle entwickelt hat, sind auf der Grundlage dieser Ergebnisse, grundsätzliche Fragen zur Cloud-Service-Auswahl zu beantworten, die vor der Auswahlentscheidung zu klären sind. Die Fragen unterstützen dabei, Nutzen und Risiken des avisierten Cloud-Dienstes abzuwägen. Dieses gilt insbesondere vor der Verlagerung von kritischen Anwendungen in die Cloud. Beispielhaft sind nachfolgend einige Fragestellungen aufgeführt:

- Wie hoch ist der messbare Nutzen eines innovativen/einmaligen Cloud-Dienstes im Verhältnis zu dessen Vendor Lock-in?
- Gibt es Alternativen mit geringerem Lock-in, insbesondere Open-Source-Lösungen?
- Welche Risiken können in der operativen (Resilienz), Daten-, juristischen und digitalen Souveränität entstehen?
- Gibt es eine institutions-einheitliche Meinung zur Nutzung von Cloud-Lösungen. Welche Auffassungen werden vom Datenschutz und der Informationssicherheit vertreten?
- Welche strategischen Abhängigkeiten können zum Service-Anbieter entstehen?
- Über welchen Zeitraum kann sich die Institution stabile Nutzungsentgelt, Funktionsumfang und Serviceverfügbarkeit (z.B. Roadmap des Anbieters zur Verfügbarkeit des Services in den nächsten x Jahren) sichern?
- Ist ein (einfacher) Wechsel des Cloud-Services möglich?
- Verfügt der Cloud-Service über standardisierte Schnittstellen und Datenmodelle, um einfach(er) wechseln zu können?
- Wie hoch ist der Customizing-, Parametrisierungs- und Einführungsaufwand und damit die Höhe der „sunk costs“ (Kosten, die nicht wieder rückgängig gemacht werden können) bei einem späteren Wechsel zu einem anderen Anbieter oder Service?

Die Antworten und Abwägungen zu diesen Fragen unterstützen die Institution bei der Entscheidungsfindung, wie z.B. bei der Auswahl eines Cloud-Services.

Beteiligte

Fachbereiche, IT-Verantwortliche, Management-Sponsor

Cloud-Anbieter-Auswahl

Mittlerweile hat sich innerhalb der öffentlichen und der privaten Cloud-Anbieter ein breites Spektrum an unterschiedlichen Cloud-Angeboten entwickelt. Manche Cloud-Anbieter bieten sogar unterschiedliche Cloud-Modelle an, welche sich über die angebotene Daten-, operative und juristische Souveränität aber auch dem dafür bereitgestellten Umfang an Services und dessen Preisen unterscheiden. Verfolgt die Institution eine Multi-Cloud-Strategie, so könnte unter den Gesichtspunkten Souveränität und Wechselfähigkeit ein Dreiklang aus Private Cloud, mit der Public Cloud eines europäischen Anbieters sowie mit einer Public Cloud eines Hyperscalers eine Option für die Institution sein[13]. Die nachfolgende Abbildung soll exemplarisch aufzeigen, wie sich die Vielzahl der Cloud-Angebote aus Private und Public Cloud in unterschiedliche Gruppierungen einordnen lässt. So könnten z.B. mit Hilfe der identifizierten Segmente, Cloud-Anbieter zugeordnet und damit eine erste Übersicht erstellt werden:

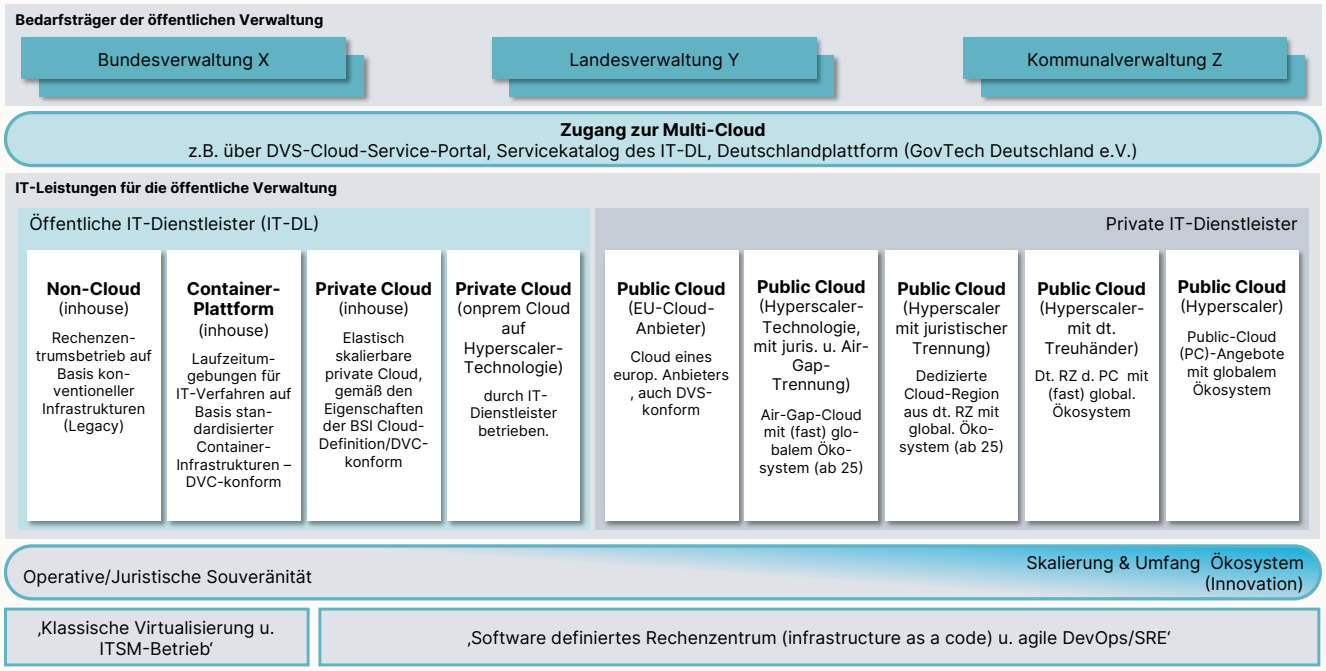


Abbildung 2: Exemplarische Übersicht über unterschiedliche Ausprägungen der Cloud-Angebote aus und für die dt. Verwaltung (Stand Sep. 25)

Sollte es der Institution möglich sein, über bestehende Cloud-Broker-Rahmenverträge Cloud-Services zu beziehen, so empfiehlt sich aus den bereits angestellten Vorüberlegungen einen Kriterienkatalog (eine erste Möglichkeit für einen Kriterienkatalog ist im beigefügten Excel-Arbeitsblatt Kriterien zur Anbieterauswahl enthalten) zu entwickeln, der die Grundlage einer fundierten Anbieterauswahl darstellt. Gibt es keine nutzbaren Rahmenverträge, so können Vorüberlegungen und Kriterienkatalog in ein zu beginnendes Beschaffungsvorhaben eingebracht werden. Weiter helfen auch die standardisierten und für die Verwaltung verbindlichen EVB-IT-Cloud-Vertragsmuster bei der Entscheidungsfindung und Beschaffung.

Beteiligte

IT-Verantwortliche, Informationssicherheitsbeauftragte, Einkauf/Beschaffung, Haushalt, Management-Sponsor

Schlussfolgerungen & Ausblick

Bedeutung einer Cloud-Nutzungsstrategie

Die Cloud-Nutzung ist kein Selbstzweck und die Cloud-Transformation ist unausweichlich. Jede Institution muss sich Gedanken machen, ob und wofür die Cloud genutzt werden soll. Die Cloud-Nutzungsstrategie geht über viele Bereiche der Institution hinweg und es bedarf eines gemeinsamen Verständnisses.

- Geopolitische Rahmenbedingungen und Risiken, die übernommen und gegenüber bestehenden Risiken abgewogen werden müssen, können z.T. nur vom obersten Management entschieden werden.
- Fragen zur „Digitalen Souveränität“ überlagern viele Facetten bei der Cloud-Nutzung. Neben den Public-Cloud-Angeboten der großen US-Firmen insbesondere der drei US-Hyperscaler Amazon, Microsoft und Google gibt es vermehrt „souveräne Angebote“. Die „Souveränität oder der Grad der Souveränität lässt sich bisher nicht eindeutig ermitteln. So bewerben die deutschen und europäischen Anbieter ihre Cloud-Lösungen als souverän, da diese grundsätzlich nicht dem Einfluss der USA oder anderer außereuropäischer Anbieter unterliegen. Die US-Hyperscaler versuchen mit spezialisierten Angeboten für Europa, die ebenfalls als „souverän“ bezeichnet werden, eine Antwort darauf zu finden. Fragen, die in diesem Kontext bei der Erstellung der Cloud-Nutzungsstrategie aufkommen sind häufig: Können die Daten bei einem Anbieter mit US-Technologie ausreichend vor fremdem Zugriff, z.B. durch die US-Regierung, geschützt werden? Ist es technisch möglich, dass eine Cloud aus den USA per Knopfdruck abgeschaltet wird (der sogenannte „Killswitch“)? „Digitale Souveränität“, DSGVO, EU-Angemessenheitsbeschluss, CLOUD-Act, FISA 702, Executive Order, Konzernstrukturen sind dabei einige der Begriffe, denen man in diesem Kontext häufig begegnet. Es würde den Rahmen sprengen, an dieser Stelle ausführlich darauf einzugehen. Festzuhalten bleibt: Die Nutzung der Public-Cloud Angebote der US-Hyperscaler ist mit Risiken verbunden, die es im Rahmen der Cloud-Nutzungsstrategie zu bewerten gilt.
- Fachabteilungen definieren den Nutzen für die Institution. Welche Chancen und Vorteile ergeben sich für sie?
- Datenschutzbeauftragte, Informationssicherheits-beauftragte (ISB/CISOs) und der IT-Betrieb klären rechtliche und technische Chancen, Risiken und Rahmenbedingungen und unterstützen bei der Mitigation der Risiken.

Ohne eine Cloud-Nutzungsstrategie, die für die gesamte Institution gilt, kann die Vielfalt der Fragen nicht geklärt werden. So bleiben Fragen offen, Diskussionen über das für und wider einer Cloud-Nutzung blockieren ein schnelles Vorankommen, denn es gibt immer Argumente, die für oder gegen eine Cloud-Nutzung sprechen. Es muss eine Entscheidung getroffen werden. Diese Entscheidung findet sich in der Cloud-Nutzungsstrategie wieder. Zeitraubende, immer wiederkehrende Diskussionen können vermieden werden, wenn alle Beteiligten in die Erstellung der Strategie mit einbezogen werden und Vor- und Nachteile aber auch die Gründe, die zu einer Entscheidung geführt haben klar dokumentiert werden. Transparenz schafft Vertrauen, erhöht die Akzeptanz aller Beteiligten und unterstützt ein schnelles Vorankommen Im Sinne der gesamten Institution.

Es ist daher von hoher Bedeutung, dass die Institutionen den Prozess der Erstellung einer Cloud-Nutzungsstrategie selbst gestalten und in der Institution fest verankern. Dieser Leitfaden soll ein erstes Herangehen an eine Cloud-Nutzungsstrategie erleichtern, sofern dies noch nicht erfolgt ist.

Autoren

Harald Joos
Projektleiter Cloud-Reallabor & Cloud-Beauftragter der Deutschen Rentenversicherung Bund

Harald Joos ist seit April 2023 „Cloud Beauftragter der Deutschen Rentenversicherung Bund“. In dieser Funktion kümmert er sich um die Nutzbarmachung von Public-Cloud-Angeboten für die öffentliche Verwaltung und leitet u.a. das Projekt „Cloud-Reallabor – sichere Verarbeitung in der Cloud“ am GovTech Campus. Von Februar 2021 bis Januar 2023 war er IT-Beauftragter der Bundesfinanzverwaltung und Leiter der Abteilung VI „Informationstechnik“ im Bundesministerium der Finanzen und zuvor Chief Information Officer (CIO) der Deutschen Rentenversicherung Bund. Nach seinem Studium zum Diplom Verwaltungswirt arbeitete Harald Joos u.a. als Softwareentwickler, Organisationsberater, IT-Servicemanager, systemischer Coach und Leiter des Rechenzentrums der Deutschen Rentenversicherung Bund.

Dr. Christian Janssen
Direktor Cloud Center of Excellence Public Sector
Capgemini Deutschland GmbH

Dr. Christian Janssen ist seit 2024 als Direktor im Cloud Center of Excellence - Public Sector bei Capgemini tätig. In dieser Funktion unterstützt er Kunden der öffentlichen Verwaltung in den Fragen der Cloud-Transformation und digitalen Souveränität von der Strategie bis zur Umsetzung. Seit vielen Jahren ist Dr. Christian Janssen in der IT-Services-Branche in verschiedenen Beratungs- und Management-Positionen tätig. Er war nach dem Studium in technisch orientierter Betriebswirtschaftslehre und Promotion in leitenden Positionen vorrangig für Kunden der öffentl. Verwaltung u.a. bei CompuNet, debis, T-Systems und init tätig, bevor er 2020 bei Capgemini die Leitung des Public Sector-Geschäftes bei den Capgemini Cloud Infrastructure Services übernahm.

Weitere Publikationen
aus dem Cloud-Reallabor unter
www.reallabor.cloud/insights/

Fußnoten & Quellenangaben

1 – www.commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en?filename=Cloud-Sovereignty-Framework.pdf%20

2 - www.bsi.bund.de/dok/Management-Blitzlicht oder www.bsi.bund.de/dok/Cloud-Nutzungsstrategie

3 - www.zukunftskongress.de/de/cloud_studie

4 - Out-of-scope der ersten Version dieses Leitfadens sind Anforderungen aus den Geheimschutz.

5 - www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Nutzung_externer_Cloud-Dienste_Version_2_1.pdf;
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Umsetzungshinweise_Mindeststandards_Externe_Cloud-Dienste_Version_2_1.pdf;
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Nutzung_externer_Cloud-Dienste_Version_2_1.pdf;
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Umsetzungshinweise_Mindeststandards_Externe_Cloud-Dienste_Version_2_1.pdf;
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Nutzung_externer_Cloud-Dienste_Version_2_1.pdf;
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Umsetzungshinweise_Mindeststandards_Externe_Cloud-Dienste_Version_2_1.pdf

6 - www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/04_OPS_Betrieb/OPS_2_2_Cloud-Nutzung_Edition_2023.html

7 - www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2024_02.pdf (S. 12ff.)

8 - www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Nutzung_externer_Cloud-Dienste_Version_2_1.pdf (S. 7)

9 - www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/04_OPS_Betrieb/OPS_2_2_Cloud-Nutzung_Edition_2023.html;
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/04_OPS_Betrieb/OPS_2_2_Cloud-Nutzung_Edition_2023.html (S.6)

10 - Sollte die Institution sich nicht in allen Kategorien im höchsten Reifegrad 3 bewerten, geben die im Vergleich zur getroffenen Einschätzung höheren Reifegrade eine Orientierung für messbare Ziele einer Cloud-Nutzungsstrategie.

11 - SMART sind Ziele, welche die fünf Kriterien spezifisch (specific), messbar (measurable), erreichbar (achievable), relevant (relevant) und terminiert (time-bound) erfüllen.

12 - Die aufgeführten Risiken entstammen dabei den folgenden Quellen:
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/04_OPS_Betrieb/OPS_2_2_Cloud-Nutzung_Edition_2023.html (S. 2ff.);
www.bk.admin.ch/dam/bk/de/dokumente/dti/themen/cloud/rechtsrahmen_anhang_c.pdf.download.pdf/AnhangRisikenundMassnahmenzumBerichtRechtlicherRahmenfuerdieNutzungvonPublic-Cloud-Diensten%inderBundesverwaltung.pdf

13 – www.omnisecure.berlin/wp-content/uploads/os25_Joos_Harald-2.pdf

GovTech Deutschland e.V.
Anschrift: Max-Urich-Straße 3
D-13355 Berlin

www.reallabor.cloud

Register: Vereinsregister beim Amtsgericht Charlottenburg
Registernummer: VR 39017 B
Umsatzsteuer-Identifikationsnummer: DE2764061593

Verantwortlich für den Inhalt: Harald Joos & Dr. Christian Janssen