HISOLUTIONS

IT-Grundschutz Compliance für Azure

1. Februar 2022
MICROSOFT DEUTSCHLAND GMBH

Inhaltsverzeichnis

1 Einleitung

Mit Microsoft Azure wird von Microsoft eine öffentliche Cloud-Computing-Plattform angeboten, die es ihren Kunden ermöglicht virtuelle Maschinen und Plattform-as-a-Service (PaaS)-Dienste für sich zu erstellen, einzusetzen und zu verwalten. Die Azure-Plattform basiert auf einem mehrschichtigen Sicherheitskonzept, das die physische Sicherheit seiner Rechenzentren, Hardware- und Firmware-Komponenten mit integrierten Sicherheitskontrollen sowie den sicheren Betrieb der Plattform umfasst.

Die Azure-Infrastruktur wird in Rechenzentrum betrieben, die weltweit verteilt sind. Die einzelnen Rechenzentren werden Regionen zugeordnet. Die beiden ehemaligen deutschen Regionen (Deutschland Nordost und Deutschland Mitte) wurden inzwischen geschlossen. Die neuen Regionen (Deutschland West Mitte und Deutschland Nord[1]) sind Teil der globalen Azure-Infrastruktur und sind seit 2019 geöffnet. Je nach Kundenwunsch können die Daten in einer oder mehreren Regionen gespeichert werden, z. B. aus Gründen der Verfügbarkeit.

In Deutschland stellt das Bundesamt für Sicherheit in der Informationstechnik (BSI) die IT-Grundschutz-Methodik zur Verfügung (und entwickelt sie stetig weiter). Diese besteht aus einem ISO 27001-kompatiblen ISMS (BSI-Standards 200-1 und 200-2), einer speziellen Risikoanalysemethode (BSI-Standard 200-3), einem Business Continuity Management (BSI-Standard 100-4; derzeit in der Überarbeitung) und dem IT-Grundschutz-Kompendium, in dem standardisierte Gefährdungen und Anforderungen an die Informationssicherheit für typische Geschäftsumgebungen aufgeführt sind.

Ziel dieses Leitfadens ist es Microsoft Azure-Kunden bei der Anwendung der IT-Grundschutz-Methodik im Rahmen ihrer bestehenden oder geplanten ISO 27001-Zertifizierung auf Basis von IT-Grundschutz zu unterstützen.

Kapitel 2 gibt einen Überblick über Cloud-Computing im Rahmen des IT-Grundschutz. In Kapitel 3 wird auf Ebene der einzelnen Anforderungen ein Überblick über die Implementierung des IT-Grundschutz-Bausteins *OPS.2.2 Cloud-Nutzung*[2] als Teil des Informationsverbunds[3] gegeben. Kapitel 4 informiert über die Umsetzung des Standards „Mindeststandard des BSI zur Nutzung externer Cloud-Dienste“[4],

---

[1] https://news.microsoft.com/europe/2018/08/31/microsoft-to-deliver-cloud-services-from-new-datacentres-in-germany-in-2019-to-meet-evolving-customer-needs/ (in Englisch)

[2] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/04_OPS_Betrieb/OPS_2_2_Cloud-Nutzung_Edition_2021.pdf

[3] Im Anhang A Glossar der BSI IT-Grundschutz-Begriffe befinden sich normative Begriffe mit besonderer Bedeutung.

[4] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Nutzung_externer_Cloud-Dienste.html

der sich an die Bundesbehörden richtet. Kapitel 5 behandelt die Verantwortlichkeiten von Microsoft als Cloud-Diensteanbieter.

2 Zertifizierungsanforderungen

Der vorliegende Leitfaden für Microsoft Azure basiert auf der überarbeitenden Version des IT-Grundschutz-Kompendiums aus dem Jahr 2021[5]. In dieser Version des IT-Grundschutzes ist der Baustein *OPS.2.2 Cloud-Nutzung*[6] enthalten. Im IT-Grundschutz wird zwischen der Nutzung von Cloud-Diensten wie Microsoft Azure und klassischem IT-Outsourcing unterschieden.

2.1 Modell der gemeinsamen Verantwortung

In einer Cloud-Umgebung wird, im Gegensatz zu einer lokalen IT-Infrastruktur, die Verantwortung für die Implementierung und Aufrechterhaltung von Sicherheitsanforderungen für IT-Anwendungen zwischen dem Kunden und dem Cloud-Diensteanbieter geteilt. Nach der Vorgehensweise des BSI IT-Grundschutzes kann diese Verantwortung an den Cloud-Diensteanbieter dann abgegeben werden, wenn dieser die Anwendungen des Kunden in seinen eigenen Zertifizierungsbereich einschließlich des angepassten Risikomanagements übernimmt. Dies gleicht einem klassischen Outsourcing-Szenario. Dabei ist zu beachten, dass entsprechend der Vorgehensweise des BSI IT-Grundschutzes die endgültige Verantwortung beim Kunden (als Dateneigentümer) liegt. Durch die neueren Versionen des IT-Grundschutzes wird ein gemeinsames Verantwortungsmodell ermöglicht. Dieses unterteilt die Verantwortung zwischen dem Kunden und dem Cloud-Diensteanbieter entlang der Virtualisierungsgrenzen, so dass jeweils nur eine Partei für einen bestimmten Aspekt verantwortlich ist.

Die Tabelle 1 zeigt eine mögliche Aufteilung nach dem Infrastruktur as a Service (IaaS) Modell. Das Cloud-Modell kann in verschiedene Aspekte unterteilt werden, für die entweder der Kunde, der Cloud-Diensteanbieter oder beide die Verantwortung tragen. Die Tabelle beschreibt zudem die verfügbare Unterstützung von Microsoft für den Kunden, die Microsoft in der Rolle als Cloud-Diensteanbieter anbietet.

[5] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2021.html

[6] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/04_OPS_Betrieb/OPS_2_2_Cloud-Nutzung_Edition_2021.pdf

Tabelle 1 Gemeinsame Verantwortlichkeiten für die Sicherheit in Cloud-Computing (IaaS Modell)[7]

Aspekt/Verantwortung Cloud Kunde Cloud Diensteanbieter		Beschreibung
Sicherheits-konzept		Sicherheitskonzepte sind ein wesentlicher Bestandteil der IT-Grundschutz-Methodik. Ein Sicherheitskonzept ist eine dokumentierte Risikoanalyse mit einem definierten Umfang. Sie beinhaltet die aus der Risikoanalyse resultierenden Maßnahmen zur Erhöhung der Sicherheit des Systems oder der Umgebung. Dieser Leitfaden kann bei der Erstellung eines Sicherheitskonzeptes für Azure unterstützen.
Datenklassifikation und Verantwortlichkeit		Der Schutzbedarf der Daten kann ausschließlich durch den Kunden selbst bestimmt werden. Dieser sollte daher seine Daten und andere Werte in der Cloud identifizieren, klassifizieren und kennzeichnen.
Client- und Endpoint-Schutz		Kunden sollten die Geräte und Clients, die auf die Cloud Dienste zugreifen dürfen, klar definieren.
Identitäts- und Berechtigungs-management		Microsoft Azure bietet verschiedene Möglichkeiten zur Identitäts- und Berechtigungsmanagement. Diese reichen von der vollständig Cloud-basierten[8] Identitäts- und Berechtigungsmanagement bis hin zu einem hybriden Ansatz[9], bei dem Benutzerdaten lokal verwaltet werden. Mit Azure Active Directory kann der Kunde Kennwortrichtlinien und Multi-Faktor-Authentifizierung[10] nach seinen spezifischen Richtlinien konfigurieren. Es ist zu beachten, dass Microsoft für die Bereitstellung eines funktionalen und sicheren Identitäts- und Berechtigungsmanagement verantwortlich ist. Beim Cloud-Kunden liegt jedoch auch bei der Cloud-basierten Identität die Verantwortung für das Identitäts- und Berechtigungsmanagement. Der Zugriff auf Kundendaten durch Microsoft-Mitarbeiter kann mit dem Dienst Customer Lockbox[11] gesteuert werden.
Audits		Audits, die von unabhängigen Dritten durchgeführt werden, helfen, Vertragsverletzungen aufzudecken. Microsoft Azure wird kontinuierlich von unabhängigen Dritten auditiert, da die Anforderungen verschiedener Compliance-Standards und Zertifizierungen zu erfüllen sind. Die Liste der Konformitätsnormen für Microsoft Azure umfasst unter anderem BSI C5, ISO 27001, ISO 27017 und ISO 27018.
Portabilität		Viele Cloud-Dienste von Azure verfügen über Portabilitätsfunktionalitäten; die meisten von ihnen verwenden Standardformate. Zum Beispiel:

[7] https://aka.ms/sharedresponsibility

[8] https://docs.microsoft.com/de-de/azure/active-directory/governance/entitlement-management-overview

[9] https://docs.microsoft.com/de-de/azure/active-directory/fundamentals/resilience-in-hybrid

[10] https://docs.microsoft.com/de-de/azure/active-directory/fundamentals/concept-fundamentals-mfa-get-started

[11] https://docs.microsoft.com/de-de/azure/security/fundamentals/customer-lockbox-overview

Aspekt/Verantwortung Cloud Kunde Cloud Diensteanbieter		Beschreibung
		- Azure Virtual Machines sind portabel zu Hyper-V. - Azure SQL-Dienste können auf einen Microsoft SQL-Server migriert werden. Außerdem können Speicherdaten importiert und exportiert werden und SQL-Datenbanken können kopiert und in andere Umgebungen importiert werden.
Notfallkonzept		Microsoft hat seine Azure-Dienste mit der notwendigen Sorgfalt entworfen. Azure speichert mehrere Live-Kopien von Kundendaten in verschiedenen Rechenzentren der gewählten Regionen, um die vertraglich garantierte Verfügbarkeit zu erreichen. Kunden sollten einen Notfallplan entwickeln, das auch ein Datensicherungskonzept umfasst.
Maßnahmen der Anwendungsebenen		Bei Microsoft Azure liegt die Kontrolle über die Anwendungsebene hauptsächlich beim Kunden, da der Kunde seine eigenen Anwendungen bereitstellt. Werden Cloud-Dienste von Microsoft bereitgestellt und betrieben, die in diesen Anwendungen zum Einsatz kommen, dann liegt die Verantwortung für die sichere Bereitstellung und den sicheren Betrieb dieser Dienste bei Microsoft. So ist Microsoft für ein sicheres Datenbankmanagement zuständig während der Kunde die verwendete Datenbank absichern muss.
Netzwerkkontrollen		Für Kunden von Microsoft Azure wird das Netzwerkmanagement zwischen Microsoft und dem Kunden geteilt. So wird beispielsweise das der Cloud zugrundeliegende Netzwerk von Microsoft betrieben und verwaltet. Andererseits liegt das vom Kunden zwischen verschiedenen virtuellen Maschinen eingerichtete virtuelle Netzwerk in der Verantwortung des Kunden.
Host-Infrastruktur		Die Verantwortung für die Host-Infrastruktur hängt vom jeweiligen Azure-Dienst ab. Der Kunde ist für jede virtuelle Maschine verantwortlich, die er einsetzt. Bei der Verwendung anderer Azure-Dienste wie Active Directory ist Microsoft jedoch für die Host-Infrastruktur verantwortlich.
Physische Sicherheit		Physische Sicherheitsmaßnahmen stellen sicher, dass nur autorisierte Mitarbeiter physischen Zugriff auf Server, Netzwerkgeräte usw. erhalten. Hierzu gehört auch das Business Continuity Management, um sicherzustellen, dass der Cloud-Dienst im Falle von schweren Vorfällen oder Katastrophen verfügbar bleibt, z. B. durch Ausfall an einem anderen physischen Standort.

2.2 Modellierung von Office 365 Deutschland

Um bei Nutzung der Cloud Dienste von Microsoft Azure IT-Grundschutz konform zu bleiben, muss das IT-Sicherheitskonzept um die Cloud Dienste nach BSI Standard 200-2[12] ergänzt werden.

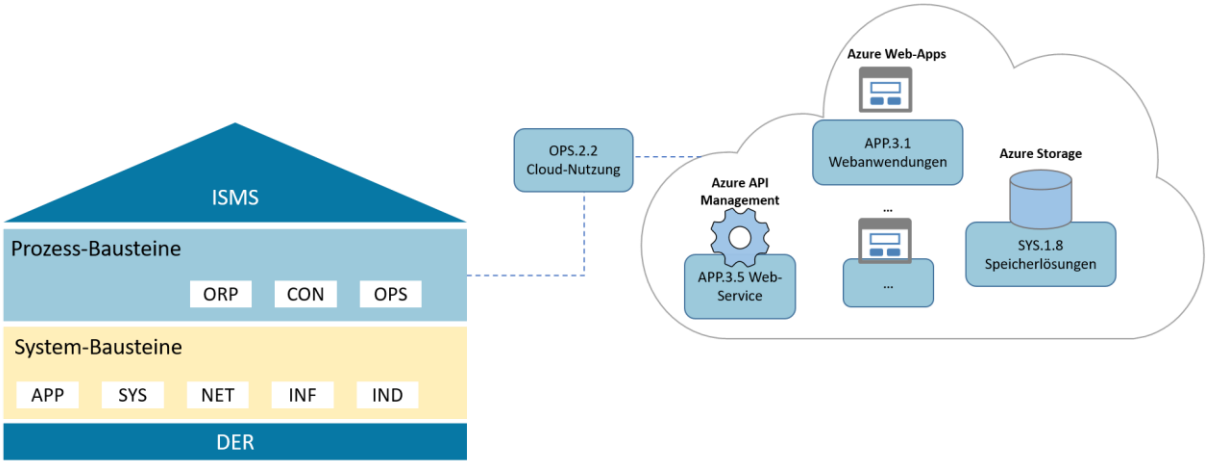

Abbildung 1 Schichtenmodell des BSI IT-Grundschutz-Kompendiums mit Cloud-Nutzung als IaaS

Das IT-Grundschutz-Kompendium verfolgt einen schichtbasierten Ansatz zur Modellierung des Informationsverbunds. Das Modell besteht aus vier Schichten: dem Informationssicherheitsmanagementsystem (ISMS), Prozessbausteinen (ORP, CON, OPS), Systembausteinen (APP, SYS, NET, INF, IND) und den Bausteinen zu Detektion und Reaktion (DER). Wie in Kapitel 2.1 erläutert, trennt der Ansatz der gemeinsamen Verantwortung die Verantwortlichkeiten für die einzelnen IT-Grundschutz-Bausteine und die darin enthaltenen Anforderungen zwischen dem Kunden und Microsoft. Azure wird durch das Infrastructure-as-a-Service (IaaS) und Platform-as-a-Service (PaaS) Bereitstellungsmodell abgedeckt. Dieser Leitfaden behandelt die gemeinsamen Verantwortlichkeiten nur in Bezug auf IaaS. Nach dem IT-Grundschutz-Ansatz ist Microsoft als Cloud-Diensteanbieter für den Management-Server für die Cloud und den Virtualisierungsserver verantwortlich.[12] Der Baustein *OPS.2.2 Cloud-Nutzung*[13] ist durch den Kunden über den gesamten Cloud-Stack anzuwenden.

Der Baustein *OPS.2.2 Cloud-Nutzung*[17] betrifft Anwendungen, die als Cloud-Dienst bereitgestellt werden, sowie deren Verwaltung. Das IT-Grundschutzkompendium[14] verlangt, dass der Baustein *OPS.2.2 Cloud-Nutzung* immer auf eine „konkrete Cloud-Dienstleistung" angewendet wird. Bei der Nutzung mehrerer Cloud-Diensteanbieter ist der Baustein für jeden Cloud-Diensteanbieter einmal anzuwenden. Dabei müssen auch die Schnittstellen zwischen den unterschiedlichen Cloud-Diensteanbietern bei der Umsetzung des Bausteins betrachtet werden.

Weitere Anforderungen an die Absicherung von Microsoft Azure aus Kundensicht ergeben sich beispielsweise an die Bausteine des Netzwerks (NET), der Systeme (SYS) und ggf. der industriellen (IND)

[12] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.html

[13] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/04_OPS_Betrieb/OPS_2_2_Cloud-Nutzung_Edition_2021.pdf

[14] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2021.html

Schichten. Andererseits werden Anforderungen auch in neue Bausteine aufgenommen werden, wie z. B. *APP.5.3 Cloud-Anwendungen aus Client-Sicht* und *APP.3.5 Webservices*, die noch nicht veröffentlicht sind. Solange die Bausteine noch nicht veröffentlicht sind, muss eine Risikoanalyse nach 200-3[15] (IT-Grundschutz-Methode) durchgeführt werden. Abbildung 1 zeigt auf, dass der Baustein *OPS.2.2 Cloud-Nutzung* eine Schnittstelle zur Kundenumgebung außerhalb der Cloud darstellt.

Abbildung 2 zeigt, wie eine virtuelle Maschine, die in der Microsoft Azure-Umgebung betrieben wird, in den Informationsverbund aufgenommen werden kann. Die Cloud-Dienste werden als Anwendungen modelliert, die direkt in der Cloud laufen (d.h. ohne zugrundeliegendes physisches System oder verbundene Serverräume). Es ist auch notwendig, die Kommunikationsverbindungen (d.h. die Internet- und/oder VPN-Verbindungen) als Teil des Systems mit den entsprechenden Bausteinen zu modellieren.

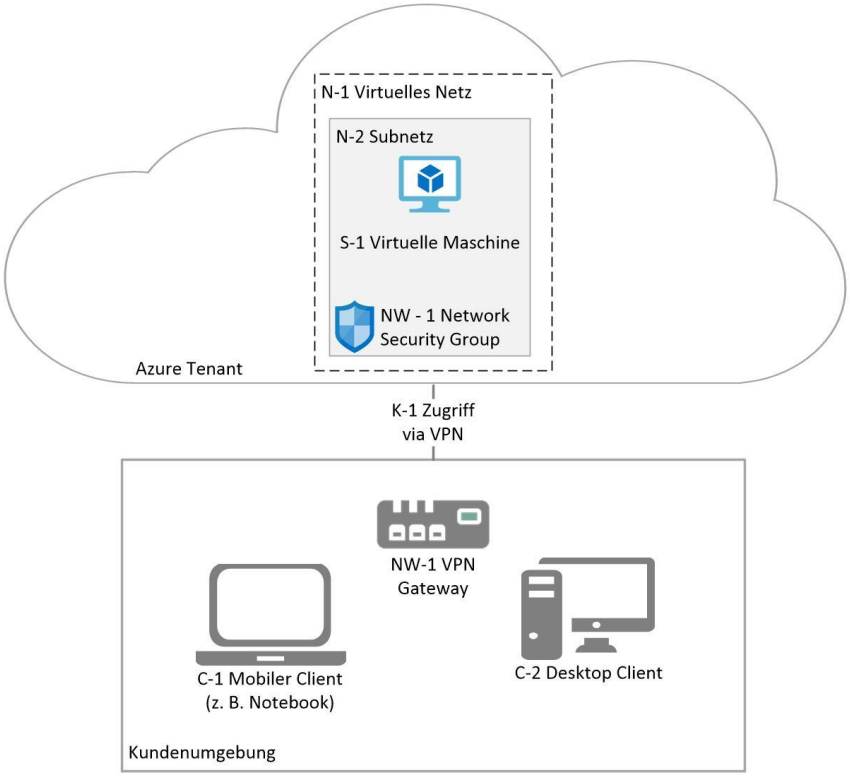

Abbildung 2 Referenzarchitektur einer virtuellen Maschine, die auf Azure gehostet wird.[16]

Im IaaS-Modell ist Microsoft für die gesamte physische Infrastruktur verantwortlich, wie bereits in Kapitel 2.1 beschrieben. Aus diesem Grund sind Anforderungen erforderlich, die diese Verantwortung definieren.

Zum besseren Verständnis wird die Modellierung anhand eines Beispiels erläutert. Dieses Beispiel basiert auf den Referenzarchitekturen einer virtuellen Microsoft Azure-Maschine unter Windows. Diese Architektur (siehe Abbildung 2 *Referenzarchitektur einer virtuellen Maschine, die auf Azure gehostet wird.*) kann als angepasstes Netzwerkdiagramm für die Zielobjekte der verwendeten Azure-Dienste verwendet werden. Anschließend werden die passenden Bausteine des IT-Grundschutz-Kompendiums auf die Zielobjekte abgebildet. Die Modellierung ist nur ein Auszug und es werden nur die Bausteine

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

[16] Abbildung basiert auf https://docs.microsoft.com/de-de/azure/architecture/reference-architectures/n-tier/windows-vm

der spezifischen Komponenten der jeweiligen IaaS-Umgebung definiert. Die umfassenden und organisatorischen Bausteine werden nicht berücksichtigt.

Die virtuelle Umgebung des Kunden innerhalb der Cloud wird ähnlich modelliert wie bei einer herkömmlichen physischen oder virtuellen Infrastruktur, einschließlich virtueller Server, Netzwerke und Anwendungen. Für IaaS stellt Microsoft lediglich eine virtuelle "Hülle" über ein virtuelles Netzwerk zur Verfügung und ist für die Absicherung des Netzwerks verantwortlich, während die Cloud-Benutzer für die IT-Systeme des Cloud-Angebots verantwortlich sind.[12]

Für die in der Referenzarchitektur definierten Komponenten sollten zumindest die in Tabelle 2 aufgeführten Bausteine des IT-Grundschutz-Kompendiums berücksichtigt werden.

Tabelle 2 Bausteine der Referenzarchitektur

Service	Beschreibung	Bausteine
Virtuelle Maschine	Virtuelle Maschine (VM) unter Windows 2012 als benutzerdefiniertes, verwaltetes Image.	SYS.1.2.2 Windows Server (Win2012)
Azure Active Directory	Authentifizierungssystem	APP.2.1 Allgemeiner Verzeichnisdienst
Virtuelles Netzwerk	Jede VM wird in einem virtuellen Netzwerk bereitgestellt, das in mehrere Subnetze unterteilt werden kann.	NET.1.1 Netzarchitektur und Design NET.1.2 Netzmanagement
VPN-Gateway	Das VPN-Gateway verbindet die Umgebung des Kunden über ein virtuelles privates Netzwerk mit der Azure-Umgebung.	NET.3.1 Router und Switches NET.3.2 Firewall NET.3.3 VPN

Beim Modellierungsprozess sind der individuellen Umfang, die Bedingungen und Anforderungen der Cloud-Dienste und der Infrastruktur zu berücksichtigen. Aus diesem Grund berücksichtigt dieser Leitfaden nur den allgemein notwendigen Baustein *OPS.2.2 Cloud-Nutzung*[13] als Grundlage der individuellen Anforderungen. Die im folgenden Kapitel 3 beschriebenen Anforderungen enthalten zusätzliche Informationen, die sich den Baustein *OPS.2.2 Cloud-Nutzung*[13] und die entsprechenden Umsetzungshinweise beziehen. Weiterhin werden hilfreiche Online-Ressourcen von Microsoft benannt.

3 Implementierung des Bausteins OPS.2.2 Cloud-Nutzung

In diesem Kapitel wird beschrieben, wie alle Anforderungen aus dem Baustein *OPS.2.2 Cloud-Nutzung*[17] für Microsoft Azure umgesetzt werden können. Im überarbeiteten IT-Grundschutz wurden die Anforderungen von den Umsetzungshinweisen getrennt. Die Umsetzungshinweise für den Baustein *OPS.2.2 Cloud-Nutzung*[18] enthalten konkrete Sicherheitsmaßnahmen, mit denen die Anforderungen umgesetzt werden können.

Während einige Anforderungen nur individuell durch den Kunden erfüllt werden können, kann Microsoft für viele der Anforderungen Informationen bereitstellen. Die folgende Tabelle gibt einen Überblick über die Anforderungen, für die Microsoft unterstützende Informationen zur Verfügung stellt.

Tabelle 3 Informationen von Microsoft zu den Anforderungen von *OPS.2.2 Cloud-Nutzung*

Anforderungen	Unterstützende Informationen von Microsoft?	Beschreibung
OPS.2.2.A1 Erstellung einer Cloud-Nutzungs-Strategie	Ja	Microsoft hat den Leitfaden „Enterprise Cloud Strategy“[19] veröffentlicht, um Anwender bei der Formulierung einer Cloud-Nutzungsstrategie zu unterstützen.
OPS.2.2.A2 Erstellung einer Sicherheitsrichtlinie für die Cloud	Ja	In dieser Anforderung werden Sicherheitsanforderungen und -verfahren an die Cloud-Nutzung definiert. Microsoft unterstützt durch die Bereitstellung von Dokumentationen zu den Sicherheitsmaßnahmen in Microsoft Azure.
OPS.2.2.A3 Service-Definition für Cloud-Dienste durch den Anwender	Ja	Diese Anforderung ist organisationsspezifisch, da sie dazu dient, interne Anforderungen und das er-

[17] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/04_OPS_Betrieb/OPS_2_2_Cloud-Nutzung_Edition_2021.pdf

[18] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/Umsetzungshinweise_Kompendium_CD_2019.html

[19] https://info.microsoft.com/enterprise-cloud-strategy-ebook.html (in Englisch)

		forderliche Schutzniveau einheitlich zu dokumentieren, um so einen einfachen Vergleich von Cloud-Dienstanbietern zu ermöglichen.
OPS.2.2.A4 Festlegung von Verantwortungsbereichen und Schnittstellen	Ja	Aufgrund dieser Anforderung sind alle Verantwortlichkeiten und Schnittpunkte zu dokumentieren. Die Verantwortlichkeiten vom Microsoft und der Cloud-Kunden sind im Dokument „Shared responsiblities“[20] festgehalten. Microsoft bietet verschiedene Methoden zur Anbindung und Verwaltung von Microsoft Azure an.
OPS.2.2.A5 Planung der sicheren Migration zu einem Cloud-Dienst	Ja	Microsoft hat den Leitfaden „Grundlagen zur Cloudmigration“[21] veröffentlicht, um Anwender bei der Migration in die Cloud zu unterstützen.
OPS.2.2.A6 Planung der sicheren Einbindung von Cloud-Diensten	Ja	Diese Anforderung trägt zur sicheren Integration von Azure in die Kundenumgebung bei. Microsoft bietet verschiedene Methoden und Dienste zur Integration von Azure in lokale Umgebungen als auch zur Anwendungsintegration an.[22]
OPS.2.2.A7 Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung	Ja	Obwohl es keine generische Vorlage für die Anforderungen eines jeden Unternehmens gibt, stellt Microsoft zu den meisten der bekannten Bedrohungen Sicherheitslösung bereit.
OPS.2.2.A8 Sorgfältige Auswahl eines Cloud-Diensteanbieters	Ja	Microsoft bietet Anleitungen und Informationen zur Evaluierung von Azure und Microsoft als Cloud Diensteanbieter an.
OPS.2.2.A9 Vertragsgestaltung mit dem Cloud-Diensteanbieter	Ja	Detaillierte Informationen zu den Standardsicherheitsanforderungen von Microsoft Azure werden in dieser Anforderung beschrieben.
OPS.2.2.A10 Sichere Migration zu einem Cloud-Dienst	Ja	Diese Anforderung ist organisationsspezifisch und umfasst die interne Planung zur sicheren Integration bestehender Dienste. Microsoft bietet Tools zur Unterstützung bei der Migration aktueller Ressourcen nach Azure an.
OPS.2.2.A11 Erstellung eines Notfallkonzepts für einen Cloud-Dienst	Ja	Das Notfallkonzept für Azure muss individuell entwickelt werden. Es werden allgemeine Richtlinien, Dienste und Informationen bereitgestellt.

[20] https://aka.ms/sharedresponsibility

[21] https://azure.microsoft.com/de-de/resources/cloud-migration-essentials-e-book/

[22] https://azure.microsoft.com/de-de/product-categories/integration/

OPS.2.2.A12 Aufrechterhaltung der Informationssicherheit	Ja	Es werden Informationen über die Aufrechterhaltung der Informationssicherheit sowie Informationen zu Verfahren zur Verfügung gestellt, mit denen der Benutzer die Informationen von Microsoft überprüfen kann.
OPS.2.2.A13 Nachweis einer ausreichenden Informationssicherheit bei der Cloud-Nutzung	Ja	Der Nachweis der Informationssicherheit wird von Microsoft regelmäßig in Form von Zertifizierungen, Auditberichten, Penetrationstestergebnissen und anderen relevanten Berichten veröffentlicht.
OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzung	Ja	Informationen und Anleitungen zur Kündigung eines Microsoft Azure-Abonnements werden bereitgestellt, einschließlich der Informationen zu Kündigung und Datenlöschung.
OPS.2.2.A15 Portabilität von Cloud-Diensten	Ja	Es werden beispielhaft für Azure Basisdienste die entsprechenden Portabilitätsaspekte angesprochen.
OPS.2.2.A16 Durchführung eigener Datensicherungen	Ja	Die Backups müssen organisationsspezifisch geplant und initiiert werden. Microsoft stellt einen Backup Dienst zur Verfügung.
OPS.2.2.A17 Einsatz von Verschlüsselung bei Cloud-Nutzung	Ja	Microsoft stellt zu Azure Informationen über die Verschlüsselung zur Verfügung – so wird der Kunde darüber informiert, wo standardmäßig verschlüsselt wird und wo die Verschlüsselung vom Kunden vorgenommen wird.
OPS.2.2.A18 Einsatz von Verbunddiensten	Ja	Verbunddienste werden über den Microsoft Azure-Dienst Azure Active Directory bereitgestellt. Es werden Informationen zu den Sicherheitsmaßnahmen bereitgestellt.
OPS.2.2.A19 Sicherheitsüberprüfung von Mitarbeitern	Ja	Im Rahmen der hohen Sicherheitsanforderungen sind Hintergrundüberprüfungen der internen und externen Mitarbeitern erforderlich.

Microsoft hat insgesamt drei IT-Grundschutz Leitfäden veröffentlicht, die bei der Einhaltung der vom Standard definierten Anforderungen beim Einsatz von Cloud-Diensten unterstützen sollen. Die Leitfäden sind verfügbar für Microsoft 365, Dynamics 365 und Azure. Bei der Implementierung nutzt Microsoft Synergien zwischen den Online-Diensten, was dem Cloud-typischen Ansatz entspricht, da so die Ressourcenauslastung optimiert werden kann. Diese Synergien und gemeinsamen Methoden spiegeln sich auch in den großen Gemeinsamkeiten innerhalb der drei Leitfäden wieder. Auf diese Weise können Kunden, die IT-Grundschutz für mehr als einen dieser Dienste nutzen, von den Gemeinsamkeiten und Synergien dieser Dienste stark profitieren, indem sie bestimmte Vorgehensweisen im Allgemeinen behandeln und nur Besonderheiten der einzelnen Dienste jeweils ergänzen müssen. So kann beispielsweise Azure Active Directory für das Identitäts- und Berechtigungsmanagement von Azure, Dynamics 365 und Microsoft 365 verwendet werden.

3.1 OPS.2.2.A1 Erstellung einer Cloud-Nutzungs-Strategie

In einer Cloud-Nutzungs-Strategie werden die Ziele, Chancen und Risiken der Cloud Nutzung betrachtet. Hierzu gehört auch die Berücksichtigung rechtlicher Aspekte sowie technischer und sicherheitsrelevanter Anforderungen. Infolgedessen sollten erlaubte Bereitstellungsmodelle für Cloud-Dienste und erste Cloud-Sicherheitsanforderungen identifiziert werden.

Der Ansatz zur Festlegung einer Strategie für die Cloud-Nutzung hängt vom jeweiligen Umfang der Nutzung ab. Microsoft hat ein E-Book veröffentlicht, um die Entwicklung einer Cloud-Strategie zu unterstützen. Das E-Book behandelt Themen wie die Cloud-Bereitstellungsmodelle und Servicemodelle, Cloud-Risikomanagement und Sicherheitsaspekte.[23]

Microsoft bietet auch das *Strategie- und Implementierungshandbuch für Azure* an, um eine solide Grundlage für die Entwicklung und den Betrieb von Cloud-Anwendungen, das Service Management und die Governance zu schaffen oder um diese Themen zu stärken.[24]

Weitere Informationen zu Compliance, Datenschutz und Sicherheit sind im Microsoft Trust Center zu finden.[25]

Der Kunde muss entscheiden, welche Anwendungen oder Dienste nach Azure migriert werden sollen. Dies kann die teilweise Integration von Diensten oder die Integration von operativen Diensten On-Premise (z. B. Integration von Active Directory) beinhalten. Es gibt verschiedene Lösungen mit unterschiedlichem Integrations- und Verbindungsgrad zwischen nativen Cloud-Diensten, und der ausschließlich lokalen Nutzung von Client-Anwendungen.

3.2 OPS.2.2.A2 Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung

Die Sicherheitsrichtlinie für die Cloud-Nutzung wird auf Basis der Cloud Nutzungs-Strategie definiert (siehe Kapitel 3.1 *OPS.2.2.A1 Erstellung einer Cloud-Nutzungs-Strategie*). Die Sicherheitsrichtlinie deckt alle Sicherheitsanforderungen ab, die in einer Institution für den Cloud-Betrieb festgelegt werden müssen. Dazu gehören alle Sicherheitsanforderungen an den Anbieter auf der Grundlage der ermittelten Schutzanforderungen. Alle technischen Schnittstellen zwischen Kunde und Cloud-Diensteanbieter sind Teil der Sicherheitspolitik sowie der organisatorischen, technischen und rechtlichen Rahmenbedingungen. Bei der Nutzung von Cloud-Diensten internationaler Cloud-Diensteanbieter sind auch länderspezifische Anforderungen und Gesetze zu berücksichtigen.

Jeder Kunde muss seine eigene, geeignete Cloud-Sicherheitsrichtlinie unter Berücksichtigung seiner Sicherheitsbedürfnisse und gesetzlicher oder Compliance-Anforderungen entwickeln und einen Cloud-Diensteanbieter wählen, der die Anforderungen erfüllen kann. Microsoft stellt Azure-spezifische Informationen zur Verfügung, um Unternehmen bei der Erstellung ihrer Sicherheitsrichtlinien in Bezug auf Datenschutz, Compliance, Transparenz und andere individuelle Kundenvorgaben zu unterstützen. Die folgende Tabelle listet typische Themen auf, die innerhalb einer Cloud-Sicherheitsrichtlinie berücksichtigt werden sollten, einschließlich der Hinweise, wie die Anforderungen von Azure erfüllt werden

[23] https://info.microsoft.com/enterprise-cloud-strategy-ebook.html (in Englisch)

[24] https://azure.microsoft.com/de-de/resources/azure-strategy-and-implementation-guide-fourth-edition/

[25] https://www.microsoft.com/de-de/trust-center/

oder erfüllt werden können.

Tabelle 4 Referenzinformationen für die Cloud-Sicherheitsrichtlinie

Sicherheitsaspekte	Implementierungen in Microsoft Azure	Referenzen
Identitäts- und Berechtigungsmanagement	Azure Active Directory wird zur Verwaltung von Identitäten und den Authentifizierungsmerkmalen verwendet. Azure unterstützt die Schaffung von dedizierten Identitäten, die nur in der Cloud verwendet werden - als auch hybriden Identitäten, die dann auch lokal verwendet werden können. Hybride Identitäten werden On-Premise verwaltet und mit Azure Active Directory synchronisiert (mit oder ohne Passwort-Hash). Azure Active Directory bietet verschiedene Möglichkeiten, hybride Identitäten in Azure anzuwenden: • Mit der Kennworthashsynchronisation werden die lokale Konten, einschließlich der Kennwort-Hashwerten nach Azure Active Directory synchronisiert. • Die Passthrough-Authentifizierung ermöglicht es einem Benutzer, sich mit seinen lokalen Anmeldeinformationen bei Azure anzumelden, und Azure validiert dann das Passwort anhand des lokalen Active Directory. Es werden keine Kennwort-Hashwerte nach Azure Active Directory übertragen. • Beim Active Directory Federation Service wird ein Vertrauensverhältnis zwischen Azure Active Directory und dem lokalen Active Directory hergestellt. In diesem Fall werden die Benutzer anhand des lokalen Active Directory authentifiziert. In Azure erfolgt die Zugriffssteuerung rollenbasiert (RBAC). Hierzu bietet Azure verschiedenen integrierten Rollen an oder die Möglichkeit eigene, benutzerdefinierte Rollen zu definieren. Neben den internen Konten einer Institution oder eines Unternehmens ermöglicht Azure auch das Hinzufügen und Verwalten von Gastkonten und Konten von externen Partnern (Business-to-Business, B2B).	https://docs.microsoft.com/de-de/azure/active-directory/fundamentals/active-directory-whatis https://docs.microsoft.com/de-de/azure/active-directory/hybrid/ https://docs.microsoft.com/de-de/azure/active-directory/hybrid/whatis-phs https://docs.microsoft.com/de-de/azure/active-directory/hybrid/how-to-connect-pta https://docs.microsoft.com/de-de/azure/active-directory/hybrid/whatis-fed https://docs.microsoft.com/de-de/azure/role-based-access-control/role-assignments-portal https://docs.microsoft.com/de-de/azure/role-based-access-control/built-in-roles https://docs.microsoft.com/de-de/azure/active-directory/b2b/index https://docs.microsoft.com/de-de/intune/fundamentals/what-is-intune https://docs.microsoft.com/de-de/azure/active-directory/authentication/howto-mfa-get-started https://docs.microsoft.com/de-de/azure/role-based-access-control/pim-azure-resource https://docs.microsoft.com/de-de/azure/role-based-access-control/conditional-access-azure-management

Sicherheitsaspekte	Implementierungen in Microsoft Azure	Referenzen
	Intune kann genutzt werden, um mobiler Geräte zu verwalten und damit den Zugriff von mobilen Geräten einzuschränken oder abzusichern. Es stehen verschiedene Multifaktor-Authentifizierungsmethoden (MFA) zur Verfügung, mit denen der Zugriff auf Azure gesichert werden kann, z. B. über mobile Apps oder Smartcards. Außerdem können MFA-Lösungen von Drittanbietern verwendet werden. Das Privileged Identity Management (PIM) ermöglicht die Verwaltung und Überwachung des administrativen Zugriffs auf Azure. So kann beispielsweise mit PIM der Zugriff auf Berechtigungen zeitlich begrenzt werden. Mit der Conditional Access-Funktion können Azure-Kunden automatisierte Zugriffskontrollentscheidungen für den Zugriff auf Daten und Anwendungen in Azure hinzufügen, die auf kundenspezifischen Bedingungen basieren. Mit der Funktion Just-in-time (JIT) kann der Zugriff auf virtuelle Maschinen eingeschränkt werden.	https://docs.microsoft.com/de-de/azure/security-center/security-center-just-in-time
Asset Management	In Azure können virtuelle Maschinen, einfache Webanwendungen bis hin zu komplexen Infrastrukturen erstellt, verwaltet und überwacht werden. Hierbei können benutzerdefinierte Dashboards für eine organisierte Ansicht von Ressourcen unterstützen. Darüber hinaus bietet der Azure Ressourcenmanager eine Verwaltungsebene, die es ermöglicht, Ressourcen in einem Abonnement zu erstellen, zu aktualisieren und zu löschen. Azure bietet verschiedene Dienste an, die die Beschriftung / das Tagging von Assets ermöglichen.	https://docs.microsoft.com/de-de/azure/azure-portal/azure-portal-overview https://docs.microsoft.com/de-de/azure/azure-resource-manager/resource-group-overview https://docs.microsoft.com/de-de/azure/architecture/cloud-adoption/decision-guides/resource-tagging/ https://docs.microsoft.com/de-de/azure/azure-resource-manager/resource-group-using-tags
Datenschutz	Microsoft hat seine Prozesse derart angepasst, um die Anforderungen der EU-Standardklauseln zu erfüllen.	https://www.microsoft.com/de-de/trustcenter/Compliance/EU-Model-Clauses

Sicherheitsaspekte	Implementierungen in Microsoft Azure	Referenzen
	Azure stellt sicher, dass Kunden in der Lage sind, die Anforderungen an die Benachrichtigung über Datenschutzverstöße zu erfüllen, indem über mögliche Datenschutzverstöße innerhalb von 72 Stunden informiert wird. Die Mitteilung enthält eine Beschreibung der Art der Verletzung, der ungefähren Auswirkungen auf die Benutzer und eine Beschreibung der Maßnahmen einschließlich Zeitangaben. Darüber hinaus gibt Microsoft eine Anleitung, wie die Anforderungen des Datenschutzes in Azure vom Kunden umgesetzt werden können. Dazu gehören eine Checkliste, eine Folgenabschätzung zum Datenschutz und die Beantwortung von Anfragen der betroffenen Personen. Die Mandantentrennung in Azure wird mit verschiedenen technischen Mitteln realisiert. Dazu gehören die logische Isolierung durch rollenbasierte Zugriffskontrolle, Verschlüsselung und die Trennung auf Speicherebene. Azure schützt Kundendaten im gespeicherten Zustand und während der Übertragung mit modernsten kryptografischen Methoden und Protokollen wie AES, IPSec oder TLS/SSL. Azure ermöglicht die Definition, Zuweisung und Verwaltung von Sicherheitsrichtlinien (Security Policies). Sie können verwendet werden, um Ressourcen zu regulieren, so dass ihre Nutzung mit den Unternehmensstandards oder -anforderungen übereinstimmen. Microsoft testet und überwacht kontinuierlich die Sicherheit von Azure und ergreift entsprechende Maßnahmen. Entsprechende Berichte, z. B. für Penetrationstests oder Audits, sind über das Trust Center zugänglich. Der Zustand des Dienstes kann auf der Seite Azure Service Health eingesehen werden. Azure ermöglicht die Definition von (Sicherheits-) Blueprints, die es ermöglichen, die gleichen Konfigurationen oder	https://docs.microsoft.com/de-de/compliance/regulatory/gdpr-arc https://docs.microsoft.com/de-de/compliance/regulatory/gdpr-breach-notification https://docs.microsoft.com/de-de/microsoft-365/compliance/gdpr-dsr-azure https://docs.microsoft.com/de-de/azure/azure-monitor/platform/personal-data-mgmt https://docs.microsoft.com/de-de/azure/azure-monitor/app/data-retention-privacy https://www.microsoft.com/de-de/trustcenter/compliance/iso-iec-27018 https://docs.microsoft.com/de-de/azure/security/fundamentals/isolation-choices https://docs.microsoft.com/de-de/azure/security/azure-protection-of-customer-data https://docs.microsoft.com/de-de/azure/governance/policy/overview https://servicetrust.microsoft.com/ViewPage/TrustDocuments https://docs.microsoft.com/de-de/azure/service-health/service-health-overview https://status.azure.com/de-de/status https://docs.microsoft.com/de-de/azure/governance/blueprints/overview https://docs.microsoft.com/de-de/azure/security/fundamentals/log-audit

Sicherheitsaspekte	Implementierungen in Microsoft Azure	Referenzen
	Richtlinien konsistent und wiederholt anzuwenden. Azure bietet eine Vielzahl von konfigurierbaren Sicherheitsüberprüfungs- und Protokollierungsoptionen, um Lücken in den Sicherheitsrichtlinien und -mechanismen zu identifizieren. Dazu gehören Aktivitätsprotokolle, Ereignisprotokolle von virtuellen Maschinen oder der Datenverkehr über Netzwerksicherheitsgruppen.	
Compliance und Audit	Microsoft erfüllt mit seinen Cloud-Diensten verschiedene nationale und internationale Compliance-Anforderungen und lässt diese von unabhängigen Dritten auditieren und zertifizieren. Die entsprechenden Zertifikate oder Testate werden im Trust Center veröffentlicht. Microsoft hat in die Prozesse implementiert, um die Anforderungen der Standardvertragsklauseln hinsichtlich der Übermittlung personenbezogener Daten an Auftragsverarbeiter zu erfüllen. Azure stellt sicher, dass Kunden in der Lage sind, die Anforderungen der GDPR für die Benachrichtigung bei Datenschutzverletzungen zu erfüllen, indem sie die Angabe einer Kontaktperson für den Datenschutz ermöglichen, die innerhalb von 72 Stunden über Datenschutzverletzungen informiert wird. Die Benachrichtigung enthält eine Beschreibung der Art des Verstoßes, der ungefähren Auswirkungen auf die Nutzer und der Schritte zur Behebung des Verstoßes einschließlich eines Zeitrahmens. Darüber hinaus bietet Microsoft eine Anleitung, wie die Anforderungen der General Data Protection Regulation (GDPR) in Azure vom Kunden umgesetzt werden können. Dazu gehören eine Checkliste zur Rechenschaftspflicht, eine Vorlage für eine Datenschutz-Folgenabschätzung und eine Anleitung zur angemessenen Beantwortung von Anfragen der betroffenen Personen.	https://docs.microsoft.com/de-de/compliance/regulatory/offering-home https://www.microsoft.com/de-de/trustcenter/Compliance/EU-Model-Clauses https://docs.microsoft.com/de-de/compliance/regulatory/gdpr-arc-azure-dynamics-windows https://docs.microsoft.com/de-de/compliance/regulatory/gdpr-breach-notification https://docs.microsoft.com/de-de/microsoft-365/compliance/gdpr-dsr-azure https://docs.microsoft.com/de-de/azure/azure-monitor/platform/personal-data-mgmt http://azuredatacentermap.azurewebsites.net/ (in Englisch) https://docs.microsoft.com/de-de/azure/azure-monitor/app/data-retention-privacy https://www.microsoft.com/de-de/trustcenter/compliance/iso-iec-27018 https://docs.microsoft.com/de-de/azure/active-directory/reports-monitoring/overview-monitoring

Sicherheitsaspekte	Implementierungen in Microsoft Azure	Referenzen
	Azure bietet mehrere Audit- und Berichtsfunktionen, mit denen beispielsweise die Benutzer- oder Administratoraktivitäten verfolgt werden können. Microsoft bietet eine Übersicht über alle Datenspeicherplätze für Azure. Microsoft Defender für Cloud ist ein in Azure integriertes Tool, das einen Überblick über die aktuelle Sicherheitslage gibt, als auch Maßnahmen zum Schutz vor Bedrohungen mitbringt. So bietet es beispielsweise Härtungsempfehlungen auf der Grundlage des Azure Security Benchmark an und für Azure-Daten- und PaaS-Dienste hilft die Anomalieerkennung bei der Identifizierung von Angriffen.	https://docs.microsoft.com/de-de/azure/active-directory/reports-monitoring/overview-reports https://docs.microsoft.com/de-de/security/benchmark/azure/overview
Kryptografie	Azure bietet mehrere Methoden zur Realisierung einer sicheren Verschlüsselung von Daten, die in einer speziellen Anforderung behandelt werden.	Kapitel 3.17 *OPS.2.2.A17 Einsatz von Verschlüsselung bei Cloud-Nutzung*
Datensicherung und Archivierung	Der Azure-Backup-Service ermöglicht es, lokale Daten und bestimmte Daten in Azure wie virtuelle Maschinen zu sichern. Skalierbarkeit und Wiederherstellbarkeit sind in Azure integriert, um die Zuverlässigkeit zu maximieren und negative Auswirkungen auf Kunden zu minimieren. Darüber hinaus stellt Microsoft Kunden Informationen zur Verfügung, wie sie eine robuste Umgebung und Anwendungen in Azure implementieren können. Mit Azure Site Recovery können lokale virtuelle Maschinen, Azure Stack sowie physische Server als auch virtuelle Azure-Computer zwischen Azure Regionen repliziert werden, um ein Failover der Maschinen zu ermöglichen. Die Archivierung von Cloud-Anwendungen und Daten innerhalb dedizierter Speicher in Azure kann beispielsweise mit Azure Blob Storage realisiert werden.	https://docs.microsoft.com/de-de/azure/backup/backup-overview https://azure.microsoft.com/de-de/features/resiliency/ https://azure.microsoft.com/de-de/resources/resilience-in-azure-whitepaper/ (in Englisch) https://docs.microsoft.com/de-de/azure/site-recovery/site-recovery-overview https://docs.microsoft.com/de-de/azure/storage/blobs/storage-blob-storage-tiers https://azure.microsoft.com/de-de/solutions/architecture/backup-archive-cloud-application/

Sicherheitsaspekte	Implementierungen in Microsoft Azure	Referenzen
	Für die Sicherung oder Archivierung von Daten aus Azure-Diensten stehen verschiedene Lösungen von Drittanbietern zur Verfügung.	
Sichere Konfiguration	Microsoft bietet Best Practices und Blueprints für die Konfiguration von Azure an. Die im Abschnitt Datenschutz genannten konfigurierbaren Blueprints und Sicherheitsrichtlinien (Security Policies) können auch zur Gewährleistung einer sicheren Konfiguration verwendet werden.	https://docs.microsoft.com/de-de/azure/security/fundamentals/best-practices-and-patterns https://docs.microsoft.com/de-de/azure/governance/blueprints/overview https://docs.microsoft.com/de-de/azure/governance/policy/overview
Protokollierung und Überwachung	Azure stellt innerhalb seiner Dienste verschiedene Arten von Protokolldaten zur Verfügung, die beispielsweise zur Verfolgung von Aktivitäten oder zur Identifizierung von Bedrohungen verwendet werden können. Die Überwachung mit unterschiedlichen Schwerpunkten (Ressourcennutzung, Compliance, riskante Konten, Sicherheitsprobleme) ist mit verschiedenen Diensten von Azure möglich. Mit dem Log Analytics Agent sammelt das Security Center Daten von Azure Virtual Machines (VMs), IaaS-Containern usw., um mögliche Sicherheitsschwachstellen frühzeitig zu erkennen. Azure Threat Protection (ATP) überwacht das Benutzerverhalten, um mögliche Angriffe auf das Active Directory zu identifizieren. Darüber hinaus hilft Azure Active Directory Identity Protection beim Schutz und der Überwachung der Kundenidentitäten. Azure Sentinel ist eine Cloud-native Security Information Event Management (SIEM) und Security Orchestration Automated Response (SOAR) Lösung.	https://docs.microsoft.com/de-de/azure/security/azure-log-audit https://docs.microsoft.com/de-de/azure/azure-monitor/overview https://docs.microsoft.com/de-de/azure/azure-monitor/app/app-insights-overview https://docs.microsoft.com/de-de/azure/security-center/security-center-enable-data-collection https://docs.microsoft.com/de-de/azure-advanced-threat-protection/what-is-atp https://docs.microsoft.com/de-de/azure/active-directory/identity-protection/overview https://docs.microsoft.com/de-de/azure/sentinel/overview

Sicherheitsaspekte	Implementierungen in Microsoft Azure	Referenzen
Bedrohungsschutz	Azure verfügt über einen grundlegenden DDoS-Schutz, der für gängige Angriffe auf Netzwerkebene ausreichend sein kann. Ein Abonnement für den Standard-DDoS-Schutz bietet Schutz vor komplexeren Angriffen. Azure bietet einen kostenlosen Echtzeit-Malwareschutz, um verschiedene Arten von Schadsoftware wie Viren oder Spyware zu identifizieren und zu entfernen. Azure bietet Dienste und Ansichten, die es ermöglichen, Anomalien wie ungewöhnliches Verhalten von Konten oder verdächtiges Verhalten zu erkennen.	https://docs.microsoft.com/de-de/azure/virtual-network/ddos-protection-overview https://docs.microsoft.com/de-de/azure/security/fundamentals/antimalware https://docs.microsoft.com/de-de/azure-advanced-threat-protection/what-is-atp
Änderungsmanagement	Azure wird ständig erweitert und weiterentwickelt, um zusätzliche Funktionalität oder Sicherheit zu bieten. Microsoft stellt eine Roadmap mit begonnenen und geplanten Änderungen für Azure zur Verfügung, die von Kunden genutzt werden kann, um sich auf bevorstehende Änderungen vorzubereiten. Azure Automation ist ein Service zur Automatisierung von Änderungen und besteht aus Prozessautomatisierung, Update-Management und Konfigurationsfunktionen.	https://azure.microsoft.com/de-de/updates/ (Meldungen in Englisch) https://docs.microsoft.com/de-de/azure/automation/automation-intro

3.3 OPS.2.2.A3 Service-Definition für Cloud-Dienste durch den Anwender

Für jeden geplanten und bestellten Cloud-Dienst sollte eine Beschreibung gemäß der definierten Cloud-Nutzungs-Strategie (siehe Kapitel 3.1 *OPS.2.2.A1 Erstellung einer Cloud-Nutzungs-Strategie*) und der Sicherheitsrichtlinie (siehe Kapitel 3.2 *OPS.2.2.A2 Erstellung einer Sicherheitsrichtlinie für* die Cloud) erstellt werden. Die Beschreibung sollte auf den Mehrwert oder die angestrebten Ergebnisse der geplanten oder genutzten Dienstleistung für den Kunden hinweisen. Die Verwendung von standardisierten Servicevorlagen im ITIL-Stil kann von Vorteil sein, wenn es in dem Unternehmen kein anderes vordefiniertes Format gibt. Im Rahmen der Servicedefinition sollten die wichtigsten technischen Parameter definiert werden.

Microsoft stellt auf verschiedenen Websites Informationen über die Cloud-Dienste zur Verfügung[26]. Eine Suchanfrage auf der globalen Infrastruktur-Website von Microsoft Azure[27] kann verwendet werden, um herauszufinden, ob ein Cloud-Dienst in der gewählten Region verfügbar ist. Die Verfügbarkeitsverpflichtungen in Form von Service Level Agreements (SLAs) werden pro Cloud-Dienst definiert.[28]

Neben den Beschreibungen und garantierten Verfügbarkeiten der Cloud-Dienste sollten auch Authentifizierungsmethoden pro Cloud-Dienst dokumentiert werden. Das zentrale Identitätsmanagement wird in Azure über Azure Active Directory abgewickelt.[29] Für die Steuerung des Zugriffs auf Cloud-Dienste und Ressourcen stehen Multifaktor-Authentifizierung[30] und rollenbasierte Zugriffskontrolle zur[31] Verfügung. Der Multifaktor-Authentifizierungsdienst kann entweder von Microsoft[30] oder von einem externen Authentifizierungsanbieter[32] verwendet werden. Für das Management weiterer Sicherheitsaspekte bietet Microsoft in Azure weitere Optionen an, um den Zugriff auf und von Cloud-Diensten weiter zu sichern. Microsoft Azure bietet unter anderem Verschlüsselung in Verbindung mit einer Vielzahl von Cloud-Diensten an. Die Daten in den Speichern und in der Übertragung werden automatisch verschlüsselt; diese Verschlüsselung kann nicht deaktiviert werden.[33] Der Kunde kann entweder die Geheimnisse wie Passwörter, API-Schlüssel oder Zertifizierungen ausschließlich softwarebasiert oder unter Verwendung eigener Hardware-Sicherheitsmodule, gemeinsamer Hardware-Sicherheitsmodule von Microsoft oder dedizierter Hardware-Sicherheitsmodule von Microsoft im Azure Key Vault speichern.[34]

Darüber hinaus bietet die Kunden Lockbox von Microsoft eine Schnittstelle, über die Kunden Datenzugriffsanfragen überprüfen und dann genehmigen oder ablehnen können, z. B. wenn ein Microsoft-Mitarbeiter während einer Supportanfrage auf Kundendaten zugreifen muss.[35]

3.4 OPS.2.2.A4 Festlegung von Verantwortungsbereichen und Schnittstellen

Die Verantwortung für den sicheren Cloud-Betrieb und die Nutzung wird zwischen dem Cloud-Dienstanbieter und dem Kunden geteilt. Dabei können die genauen Verantwortlichkeiten von Cloud-Dienst zu Cloud-Dienst variieren, insbesondere, wenn verschiedene Bereitstellungsmodelle wie Infrastructure as a Service (IaaS), Platform as a Service (PaaS) und Software as a Service (SaaS) einbezogen werden. Es

[26] https://azure.microsoft.com/de-de/services/

https://docs.microsoft.com/de-de/azure/#pivot=products

[27] https://azure.microsoft.com/de-de/global-infrastructure/services/

[28] https://azure.microsoft.com/de-de/support/legal/sla/

[29] https://docs.microsoft.com/de-de/azure/active-directory/

[30] https://docs.microsoft.com/de-de/azure/active-directory/authentication/concept-mfa-howitworks

[31] https://docs.microsoft.com/de-de/azure/role-based-access-control/

[32] https://docs.microsoft.com/de-de/windows-server/identity/ad-fs/operations/configure-additional-authentication-methods-for-ad-fs

[33] https://docs.microsoft.com/de-de/azure/security/fundamentals/encryption-overview

[34] https://docs.microsoft.com/de-de/azure/key-vault/key-vault-hsm-protected-keys

https://docs.microsoft.com/de-de/azure/dedicated-hsm/

[35] https://docs.microsoft.com/de-de/azure/security/fundamentals/customer-lockbox-overview

ist wichtig, dass die Verantwortlichkeiten klar voneinander abgegrenzt werden können, da dies sonst zu einem unterschiedlichen Verständnis von Verantwortlichkeiten und damit zu Sicherheitslücken führen kann.

Microsoft stellt verschiedene Informationen über ihren Ansatz und ihre Sichtweise auf dieses Modell der gemeinsamen Verantwortung zur Verfügung.[36] Weitere Informationen zum Modell der gemeinsamen Verantwortung werden in diesem Leitfaden in Kapitel 2.1 *Modell der gemeinsamen Verantwortung* beschrieben.

Nach der Identifizierung der Verantwortlichkeiten ist es wichtig, die Schnittstellen zwischen dem Kunden und dem Cloud-Diensteanbieter klar zu definieren, damit beide Seiten ihre Aufgaben angemessen erfüllen können.

Die definierten Verantwortlichkeiten und Schnittstellen sollten im Rahmen der Cloud-Dienste-Definition des Kunden dokumentiert werden. Dies wird in Kapitel 3.3 *OPS.2.2.A3 Service-Definition für Cloud-Dienste durch den Anwender* behandelt. Anschließend kann die sichere Migration und Integration des Cloud-Dienst geplant werden.

3.5 OPS.2.2.A5 Planung der sicheren Migration zu einem Cloud-Dienst

Die Entwicklung eines Migrationskonzeptes bildet eine wichtige Grundlage für eine sichere und nachhaltige Migration in die Cloud. Dabei sind vor allem organisatorische Regelungen und Aufgabenzuordnungen zu berücksichtigen. Dazu gehören auch Verantwortlichkeiten, Test- und Transferverfahren, die für einen widerstandsfähigen und sicheren Geschäftsbetrieb von besonderer Bedeutung sind. Im weiteren Verlauf sollte die unternehmenseigene IT im Migrationsprozess ausreichend mitbetrachtet werden.

Für eine sichere Migration in die Cloud müssen verschiedene, kundenspezifische Bedingungen berücksichtigt werden. Dies gilt insbesondere, wenn bei der Migration andere, bereits genutzte Cloud-Dienste mitberücksichtigt werden sollen. Dabei sind die Portabilitätsmerkmale des Cloud-Dienstes von Bedeutung. Diese Merkmale werden im Kapitel 3.15 *OPS.2.2.A15 Portabilität von Cloud-Diensten* behandelt.

Um ein kontinuierliches und hohes Sicherheitsniveau zu gewährleisten, muss die Migration von einer lokalen Umgebung, die möglicherweise anderer Cloud-Dienste bereits enthält, zu Azure entsprechend geplant werden.

Microsoft bietet einen Leitfaden[37] zur Unterstützung bei der Migrationsplanung an. Der Leitfaden kombiniert Antworten auf wichtige Fragen und erfahrungsbasierte Empfehlungen für eine Migration in die

[36] https://aka.ms/sharedresponsibility
https://azure.microsoft.com/mediahandler/files/resourcefiles/d8e7430c-8f62-4bbb-9ca2-f2bc877b48bd/Azure%20Onboarding%20Guide%20for%20IT%20Organizations.pdf (in Englisch)
https://www.microsoft.com/security/blog/2018/06/19/driving-data-security-is-a-shared-responsibility-heres-how-you-can-protect-yourself/ (in Englisch)

[37] https://azure.microsoft.com/de-de/resources/cloud-migration-essentials-e-book/

Cloud. Ein weiterer Leitfaden behandelt die Migration von SQL Server-Datenbanken ist ebenfalls verfügbar.[38] Microsoft bietet auch weitere Informationen und Empfehlungen zur Migration im Azure Migrationszentrum an[39]. Das Azure Migrationszentrum bietet unteranderem Links für Schulungen zur Cloud-Migration und Hilfe bei der Suche nach Migrationsexperten, Partnern und Tools an.[40]

Um eine geordnete und sichere Migration unter Aufrechterhaltung eines normalen Betriebs für die bestehende Umgebung zu realisieren, müssen die erhöhten Ressourcenanforderungen (Finanzen, Wissen und Personal) für Planung, Migration, Test und die frühen Betriebsphasen berücksichtigt werden.

Die Migrationsplanung muss berücksichtigen, wie Daten und Dienste sicher in die Cloud übertragen werden können. Für Azure wird dies in diesem Leitfaden in Kapitel 3.15 *OPS.2.2.A15 Portabilität von Cloud-Diensten* beschrieben.

Neben der Migration zu einem Cloud-Dienst muss auch dessen Integration während und nach der Migration in die bestehende IT-Infrastruktur berücksichtigt werden. Dies wird im Kapitel 3.6 *OPS.2.2.A6 Planung der sicheren Einbindung von Cloud-Diensten* beschrieben.

3.6 OPS.2.2.A6 Planung der sicheren Einbindung von Cloud-Diensten

Neben der Planung einer sicheren Migration (siehe Kapitel 3.5*OPS.2.2.A5 Planung* der sicheren Migration zu einem Cloud-Dienst) ist die sichere Integration von Azure für einen sicheren, kontinuierlichen IT-Betrieb unerlässlich. Diese Anforderung berücksichtigt Aspekte, die über die Planung der Migration hinausgehen.

Es gibt verschiedene Methoden, um die Integration von Cloudbasierten Features vorzubereiten. Das Unternehmen muss ein Sicherheitskonzept erstellen und dokumentieren, dass die Sicherheitsanforderungen berücksichtigt sind, die sich auf die folgenden Aspekte auswirken:

- Erforderliche Anpassungen der bestehenden IT-Landschaft
- Eignung bestehender Schnittstellen (z. B. Proxy) für die Verwendung mit Azure
- Definition des Administrationsmodells für die Cloud, z. B. Nutzung von Azure Active Directory (Azure AD) vs. Active Directory Federation Services (ADFS)
- Informationsmanagement (Datensicherung und Datenhaltungsstrategie) für in der Cloud und On-Premise gespeicherte Informationen

Für die Anwendungsintegration ist es häufig erforderlich, mehrere unabhängige Systeme zu verbinden. Dieser Vorgang kann sich sehr komplex gestalten. Das Whitepaper "Azure Integration Services"[41] beschreibt die Komponenten von Azure-Integrationsdiensten (API Management, Logic Apps, Service Bus und Event Grid) und wie diese ineinander greifen, um eine vollständige Lösung für die Integration von lokalen Anwendungen und Cloudanwendungen zu ermöglichen.

---

[38] https://azure.microsoft.com/de-de/resources/migrating-sql-server-to-azure-sql-managed-instance-step-by-step/

[39] https://azure.microsoft.com/de-de/migration/

[40] https://azure.microsoft.com/de-de/migration/migration-modernization-program/

[41] https://azure.microsoft.com/mediahandler/files/resourcefiles/azure-integration-services/Azure-Integration-Services-Whitepaper-v1-0.pdf (in Englisch)

Um die Verbindung zwischen Cloud-Diensten und lokalen Systemen und Diensten abzusichern, kann ein Cloud Access Security Broker (CASB) wie Microsofts Cloud App Security verwendet werden. Ein CASB kann beispielsweise als Reverse-Proxy fungieren, eine verbesserte Datentransparenz bieten, den Zugriff auf Cloud-Dienste steuern oder zur Erkennung von Bedrohungen im Zusammenhang mit genutzten Cloud-Diensten verwendet werden.[42]

Zusätzlich wird eine Lernplattform angeboten, auf der viele unterstützende Inhalte für Schulungen zu finden sind.[43]

Mit dem Evergreen-Ansatz ist Microsoft bestrebt, alle Azure-Dienste und die gesamte Plattform sicher, konform und mit stetigen Updates immer auf dem neuesten Stand zu halten. Dieser Ansatz bringt neue Verantwortlichkeiten für die Kunden im Bereich Change Management mit sich, da sie Änderungen in der Nutzung oder, falls erforderlich, in ihren Geschäftsprozessen berücksichtigen müssen.[44]

3.7 OPS.2.2.A7 Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung

Auf der Grundlage der identifizierbaren Anforderungen (siehe Kapitel 3.2 *OPS.2.2.A2 Erstellung einer Sicherheitsrichtlinie für die Cloud*) sollte ein Sicherheitskonzept für die Nutzung von Cloud-Diensten entwickelt werden. Die Gefährdungen ergeben sich aus Vertragsmängeln, Abhängigkeiten oder unklaren Verantwortlichkeiten. Sie führen zu Kontrollverlust und ineffizienter Leistung. Es sind mehrere Parteien beteiligt, insbesondere im Zusammenhang mit Cloud-Diensten. Zumindest die folgenden Parteien sollten berücksichtigt werden: Cloud-Kunde, Cloud-Diensteanbieter und der Netzbetreiber.

Obwohl es keine generische Vorlage für die Anforderungen Ihrer Organisation gibt, geht Microsoft Azure wie folgt auf viele der in den offiziellen Implementierungsempfehlungen von IT-Grundschutz genannten Bedrohungen und Abhilfemaßnahmen ein:

Tabelle 5 Referenzinformationen für ein Cloud-Dienst-Sicherheitskonzept

Cloud-spezifische Bedrohungen	Informationen über Microsoft Azure	Referenzen
(Nicht) fristgerechte Beendigung des Vertrages	Die Vertragsbeendigung wird im Rahmen einer speziellen Anforderung detailliert behandelt.	Kapitel 3.14 *OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzung*
Fehlende Portabilität, z. B. aufgrund proprietärer Datenformate	Die Portabilität wird im Rahmen einer speziellen Anforderung detailliert behandelt.	Kapitel 3.15 *OPS.2.2.A15 Portabilität von Cloud-Diensten*
Fehlende Kenntnisse über den physischen Datenspeicherort	Azure bietet einen Überblick über Rechenzentren innerhalb einer Region und ermöglicht die Auswahl der Geolokalität innerhalb des Abonnements. Die Daten	https://azure.microsoft.com/de-de/global-infrastructure/

[42] https://docs.microsoft.com/de-de/cloud-app-security/what-is-cloud-app-security

[43] https://docs.microsoft.com/de-de/learn/azure/

[44] https://www.microsoft.com/de-de/cloud/laufende-updates.aspx

Cloud-spezifische Bedrohungen	Informationen über Microsoft Azure	Referenzen
	werden dann in den Rechenzentren gespeichert, die sich in dieser Geolokation befinden. Alle Azure-Rechenzentren sind physisch gegen unbefugten Zugriff und verschiedene andere Bedrohungen geschützt.	http://azuredatacentermap.azurewebsites.net/ (in Englisch) https://docs.microsoft.com/de-de/azure/security/fundamentals/infrastructure
Hohe Mobilität der Informationen: In der Cloud gespeicherte Informationen können von verschiedenen Standorten aus mit verschiedenen Arten von Geräten oder Software (PC, Laptop, Smartphone, Browser, Apps usw.) abgerufen werden.	Mobile Device Management (MDM) oder Intune können verwendet werden, um mobile Geräte abzusichern und zu konfigurieren, ob und unter welchen Umständen diese auf Azure zugreifen dürfen. Zusammen mit dem bedingten Zugriff kann dies verwendet werden, um den Zugriff auf bestimmte Daten oder Dienste innerhalb von Azure zu beschränken. Die Beschränkungen können auf verschiedenen Bedingungen basieren, wie dem Standort des Geräts, der verwendeten Authentifizierungsmethode, dem Zustand des Geräts oder der Konfiguration des verwendeten Geräts gemäß den Anforderungen des Kunden.	https://docs.microsoft.com/de-de/intune/fundamentals/what-is-intune https://docs.microsoft.com/de-de/windows/client-management/mdm/azure-active-directory-integration-with-mdm https://docs.microsoft.com/de-de/azure/active-directory/conditional-access/overview
Unbefugter Zugriff (z. B. durch Administratoren des Cloud-Dienstanbieters oder andere Cloud-Kunden)	Standardmäßig haben Microsoft-Mitarbeiter keinen Zugriff auf Kundendaten. Wenn Zugriff erforderlich ist, ist eine Multifaktor-Authentifizierung erforderlich und es werden die geringsten Privilegien sowie eine permanente Protokollierung und Überwachung angewendet. Zusätzlich kann die Kunden Lockbox verwendet werden, um den Zugriff von Microsoft in Supportfällen anzuzeigen und zu genehmigen oder zu verweigern. Die Mandantentrennung zwischen den Kunden wird auf Zugriffs-, Compute-, Speicher-, Datenbank- und Netzwerkebene realisiert, um sicherzustellen, dass auch bei gleichem Hardwarebetrieb kein Zugriff auf die Daten anderer Kunden möglich ist. Um einen unbefugten Zugriff auf Kundendaten zu verhindern, werden die Daten im gespeicherten Zustand und während der Übertragung, einschließlich der Übertragung zwischen Rechenzentren, mit Hilfe modernster Protokolle und	https://docs.microsoft.com/de-de/azure/security/fundamentals/protection-customer-data https://www.microsoft.com/de-de/trust-center/privacy/data-access https://docs.microsoft.com/de-de/azure/security/fundamentals/customer-lockbox-overview https://docs.microsoft.com/de-de/azure/security/fundamentals/isolation-choices https://docs.microsoft.com/de-de/azure/security/fundamentals/encryption-overview

Cloud-spezifische Bedrohungen	Informationen über Microsoft Azure	Referenzen
	Kryptographie wie AES und TLS verschlüsselt.	

3.8 OPS.2.2.A8 Sorgfältige Auswahl eines Cloud-Diensteanbieters

Im Anschluss an den Planungs- und Konzeptionsprozess sollte ein detailliertes Anforderungsprofil für Cloud–Diensteanbieter entwickelt werden. Dieses Anforderungsprofil sollten gemäß den Service-Definitionen definiert werden (siehe Kapitel 3.3 *OPS.2.2.A3 Service-Definition für Cloud-Dienste durch den Anwender*) und auch Vertragsspezifikationen beinhalten.

Ausgehend von den definierten Anforderungen kann ein Leistungskatalog oder eine Anforderungsspezifikation erstellt werden. Anhand dieses Katalogs können dann die konkurrierenden Cloud-Diensteanbieter verglichen und anhand einer Punktmatrix bewertet werden.

Vor der Migration in die Cloud sollte eine Kosten-Nutzen-Analyse den Entscheidungsprozess bei der Auswahl eines Cloud-Diensteanbieters unterstützen. Der Fokus der Analyse liegt auf den realistischen Kosten, insbesondere unter Berücksichtigung der wachsenden Serviceanforderungen. Ist der Mehrwert der Cloud-Lösung gering oder gar negativ, sollte die gesamte Migration in Frage gestellt oder die Service-Definition überprüft und gegebenenfalls angepasst werden. Bei der Kostenberechnung müssen zusätzliche Investitions- und Betriebskosten getrennt betrachtet werden, so dass die Kosten für die eigene Infrastruktur und Dienstleistungen während und nach der Migration betrachtet werden können.

Vor der Bewertung der Angebote müssen die grundlegenden Aspekte untersucht und entsprechende Antworten eingeholt werden. Wenn die Ergebnisse nicht zufriedenstellend sind, kann ein Cloud-Diensteanbieter von der weiteren Betrachtung ausgeschlossen werden[45]. Microsoft unterstützt Due Diligence-Bewertungen mit einer Checkliste[46], die auf dem internationalen Standard ISO/IEC 19086-1, dem Cloud Computing Service Level, basiert.

In Tabelle 6 werden die Informationen aufgelistet, die vor der Migration in die Cloud gesammelt und bewertet werden sollten, einschließlich entsprechender Informationen für Microsoft Azure.

Tabelle 6 Referenzinformationen für die sorgfältige Auswahl eines Cloud-Diensts

Zu berücksichtigende Überlegungen	Bedingungen für Microsoft Azure	Referenzen
Öffentlich zugängliche Informationen über den Anbieter (Reputation, Bewertungen und Rankings, Kerngeschäft,	Cloud-Computing gehört zu den Kerngeschäften von Microsoft und Microsoft gehört zu den am besten bewerteten Cloud-Diensteanbieter laut verschiedener Erhebungen.	https://www.microsoft.com/en-us/investor/default.aspx (in Englisch)

[45] Weitere Aspekte und Unterstützung bei der Auswahl eines Cloud-Diensteanbieters sind abrufbar unter https://azure.microsoft.com/de-de/overview/choosing-a-cloud-service-provider/ (in Englisch)

[46] https://www.microsoft.com/de-de/trust-center/compliance/due-diligence-checklist

Zu berücksichtigende Überlegungen	Bedingungen für Microsoft Azure	Referenzen
Performance, Cloud-Erlebnis)	Microsoft bietet einen allgemeinen Überblick über wichtige Themen zu Azure, die als Grundlage für die Due-Diligence dienen können. Microsoft bietet die Funktion Service Health. Das Dashboard kann angepasst werden und bietet den Benutzern die Möglichkeit, relevante Ereignisse zu verfolgen oder Ereignisalarme zu konfigurieren. Azure wird ständig aktualisiert und weiterentwickelt. Microsoft veröffentlicht Roadmaps und weitere Informationen über geplante Updates auf Webseiten. In der Microsoft technet Community können sich Kunden mit anderen Kunden austauschen, um weitere Informationen über Azure zu erhalten. Microsoft liefert Kundenberichte über den Einsatz von Azure.	https://azure.microsoft.com/de-de/overview/what-is-azure/ https://docs.microsoft.com/de-de/azure/service-health/service-health-overview https://status.azure.com/de-de/status https://azure.microsoft.com/de-de/updates/ (Meldungen in Englisch) https://techcommunity.microsoft.com/t5/Azure/ct-p/Azure (in Englisch) https://azure.microsoft.com/de-de/case-studies/ https://customers.microsoft.com/de-de/home
Due-Diligence	Microsoft stellt eine Checkliste für Due-Diligence-Überprüfungen zur Verfügung. Microsoft bietet eine breite Palette von Compliance-Angeboten, die als Grundlage für Due-Diligence-Überprüfungen herangezogen werden können.	https://www.microsoft.com/de-de/trust-center/compliance/due-diligence-checklist https://www.microsoft.com/de-de/trustcenter/compliance/complianceofferings
Zugriff durch Cloud–Diensteanbieter oder Dritte	Microsoft Mitarbeiter haben standardmäßig keinen Zugriff. Wenn Zugriff erforderlich ist, ist eine Mehrfaktor-Authentifizierung zwingend erforderlich und es werden die geringsten Privilegien sowie eine permanente Protokollierung und Überwachung angewendet. Der Zugang kann vom Kunden über die Funktionen der Kunden Lockbox verweigert oder genehmigt werden. Die in Azure implementierte Mandantentrennung stellt sicher, dass verschiedene Kunden nicht auf die Daten anderer zugreifen können, auch wenn diese auf derselben Hardware berechnet oder gespeichert werden.	https://docs.microsoft.com/de-de/azure/security/fundamentals/protection-customer-data https://www.microsoft.com/de-de/trust-center/privacy/data-access https://docs.microsoft.com/de-de/azure/security/fundamentals/customer-lockbox-overview https://docs.microsoft.com/de-de/azure/security/fundamentals/isolation-choices https://docs.microsoft.com/de-de/azure/security/fundamentals/encryption-overview

Zu berücksichtigende Überlegungen	Bedingungen für Microsoft Azure	Referenzen
	Die Daten werden während der Übertragung verschlüsselt und können im gespeicherten Zustand mit Hilfe modernster kryptografischer Verfahren und Protokolle verschlüsselt werden, so dass Unbefugte keinen Zugriff auf die enthaltenen Informationen haben.	
Installation von zusätzlicher Software	Azure kann über einen Browser oder über eine API aufgerufen werden. Wenn ein Dienst zusätzliche Software installiert werden muss, wird dies in der Regel zusammen mit relevanten Installationsinformationen angegeben.	https://docs.microsoft.com/de-de/rest/api/azure/
Standorte des Cloud-Anbieters	Die Kundendaten werden in der oder den vom Kunden ausgewählten Regionen gespeichert. Aus Gründen der Datenverarbeitung können Kundendaten jedoch außerhalb der gewählten Region verarbeitet werden. Zu Sicherungszwecken werden Kundendaten in andere Rechenzentren innerhalb derselben Region repliziert. Ab Ende 2022 wird die Datenspeicherung und -verarbeitung u.a. für Azure ausschließlich in Europa stattfinden.	https://azure.microsoft.com/de-de/global-infrastructure/ http://azuredatacentermap.azurewebsites.net/ (in Englisch) https://techcommunity.microsoft.com/t5/security-compliance-and-identity/eu-data-boundary-for-the-microsoft-cloud-frequently-asked/ba-p/2329098 (in Englisch)
Subunternehmer des Cloud-Diensteanbieters	Microsoft veröffentlicht und aktualisiert regelmäßig eine Liste der Subunternehmer und zusätzlich eine Liste der Subunternehmer, die auf die Daten der Kunden zugreifen können. Subunternehmer, die für Microsoft arbeiten, sind verpflichtet, am Microsoft Supplier Security and Privacy Assurance Program teilzunehmen. Dieses Programm stellt sicher, dass die in Microsoft implementierten Regeln und Prozesse auch von Subunternehmern eingehalten werden. Es trägt dazu bei, die Praktiken im Umgang mit Daten zu standardisieren und zu stärken. So müssen beispielsweise diejenigen Subunternehmer, die Zugang zu Kundendaten haben oder haben könnten, ebenfalls entsprechend der EU-Standardklauseln arbeiten.	https://www.microsoft.com/de-de/trust-center/privacy/data-access https://go.microsoft.com/fwlink/?LinkId=2096306&clcid=0x407 (Microsoft Online Services Subprocessors List) https://www.microsoft.com/en-us/download/confirmation.aspx?id=50426 (Microsoft Commercial Support Subcontractors) https://www.microsoft.com/en-us/procurement/supplier-contracting.aspx

Zu berücksichtigende Überlegungen	Bedingungen für Microsoft Azure	Referenzen
Berücksichtigung von Vertragsgrundlagen und Regelungen	Die Service Level Agreements und die Bestimmungen für Onlinedienste von Microsoft sind die Standardbedingungen für die Nutzung der Microsoft Azure-Dienste. Die Standard-SLAs, Preise und Bestimmungen für Onlinedienste sind auf der Webseite veröffentlicht und ohne Microsoft-Abonnement oder Azure-Konto zugänglich. Darüber hinaus veröffentlicht Microsoft eine FAQ-Liste mit aktuellen Fragen zu Preisen und SLAs.	https://azure.microsoft.com/de-de/support/legal/ https://www.microsoft.com/licensing/docs https://www.microsoftvolumelicensing.com/(in Englisch) https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services (in Englisch) https://azure.microsoft.com/de-de/support/legal/sla https://azure.microsoft.com/de-de/pricing/faq/
Bewertung von Dienstleistungen einschließlich Garantien	Leistungsbeschreibungen, Dokumentationen und Preisinformationen werden auf der Webseite der einzelnen Dienste veröffentlicht. Darüber hinaus haben interessierte Kunden die Möglichkeit, den Kostenrechner von Microsoft für Kostenvergleiche zu nutzen.	https://azure.microsoft.com/de-de/services/ https://azure.microsoft.com/de-de/pricing/calculator/

3.9 OPS.2.2.A9 Vertragsgestaltung mit dem Cloud-Diensteanbieter

Nach der Auswahl eines geeigneten Cloud-Diensteanbieters sollten die relevanten Aspekte vertraglichen definiert werden. Die vertraglichen Vereinbarungen zwischen dem Kunden und dem Cloud-Diensteanbieter sollten in Art, Umfang und Detaillierungsgrad dem Schutzbedarf der verarbeiteten Informationen die in Azure gespeichert oder verarbeitet werden entsprechen. Auch hier sind die zuvor definierten Anforderungen zu berücksichtigen. Nachfolgend sind mögliche Aspekte aufgeführt.

Tabelle 7 Cloud-Vertragsdokumentation

Zu berücksichtigende Aspekte	Informationen von Microsoft Azure	Referenzen
Physischer Standort der Cloud-Dienste und des Cloud-Diensteanbieters	Die Cloud-Dienste werden von Rechenzentren in der Region betrieben, die vom Kunden gewählt wurde. Die Kundendaten werden an dem vom Kunden ausgewählten geografischen Standort gespeichert. Aus Gründen der Datenverarbeitung können Kundendaten	https://azure.microsoft.com/de-de/global-infrastructure/ https://azure.microsoft.com/de-de/global-infrastructure/geographies

Zu berücksichtigende Aspekte	Informationen von Microsoft Azure	Referenzen
	jedoch außerhalb der gewählten Region verarbeitet werden. Ab Ende 2022 wird die Datenspeicherung und -verarbeitung u.a. für Azure ausschließlich in Europa stattfinden. Alle Rechenzentren sind physisch gegen unbefugten Zugriff und andere typische Bedrohungen in Rechenzentren geschützt. Microsoft hat verschiedene Sicherheitsmaßnahmen implementiert, um die Verfügbarkeit von Diensten zu gewährleisten.	https://docs.microsoft.com/de-de/azure/security/fundamentals/infrastructure https://docs.microsoft.com/de-de/azure/security/fundamentals/infrastructure-availability https://techcommunity.microsoft.com/t5/security-compliance-and-identity/eu-data-boundary-for-the-microsoft-cloud-frequently-asked/ba-p/2329098 (in Englisch)
Subunternehmer und Dritte, die an der Erbringung von Cloud-Dienstleistungen beteiligt sind.	Microsoft setzt Subunternehmer für spezifische und begrenzte Supportaufgaben ein. Eine Liste mit allen Subunternehmern und eine separate Liste mit Subunternehmern mit Zugriff auf Kundendaten wird online veröffentlicht. Subunternehmer, die für Microsoft arbeiten, sind verpflichtet, am Microsoft Supplier Security and Privacy Assurance Program teilzunehmen. Dieses Programm stellt sicher, dass die in Microsoft implementierten Regeln und Prozesse auch von Subunternehmern eingehalten werden. Es trägt dazu bei, die Praktiken im Umgang mit Daten zu standardisieren und zu stärken. So müssen beispielsweise diejenigen Subunternehmer, die Zugang zu Kundendaten haben oder haben könnten, ebenfalls entsprechend der EU-Standardklauseln agieren.	https://go.microsoft.com/fwlink/?LinkId=2096306&clcid=0x407 (Microsoft Online Services Subprocessors List; in Englisch) https://www.microsoft.com/en-us/download/confirmation.aspx?id=50426 (Microsoft Commercial Support Subcontractors; in Englisch) https://www.microsoft.com/en-us/procurement/supplier-contracting.aspx (in Englisch)
Regeln für das Personal des Cloud-Dienstanbieters	Die internen und externen Mitarbeiter von Microsoft verfügen über die erforderlichen Kompetenzen und werden gemäß den internen Richtlinien in die Tätigkeiten eingearbeitet.	https://www.microsoft.com/en-us/corporate-responsibility/empowering-employees (in Englisch) https://docs.microsoft.com/de-de/office365/Enterprise/office-365-personnel-controls (Verweis auf Office 365, gilt jedoch auch für Azure)

Zu berücksichtigende Aspekte	Informationen von Microsoft Azure	Referenzen
		Kapitel 3.19 *OPS.2.2.A19 Sicherheitsüberprüfung von Mitarbeitern*
Kommunikationswege, Ansprechpartner und Support	Der Account Manager ist der primäre Ansprechpartner für den Kunden. Microsoft bietet mehrere Möglichkeiten für die Kommunikation und Unterstützung in Bezug auf Azure an. Dazu gehören unterstützende Dokumentationen für alle Cloud-Dienste, ein Knowledge Center, ein Azure-Portal, FAQ-Listen oder die Azure-Community mit Unterstützung von Microsoft-Technikern. Darüber hinaus bietet Microsoft verschiedene Supportstufen, die für die Abonnements ausgewählt werden können.	https://azure.microsoft.com/de-de/resources/knowledge-center/ https://azure.microsoft.com/de-de/support/faq/ https://docs.microsoft.com/de-de/azure/azure-portal/ https://azure.microsoft.com/de-de/support/community/ https://azure.microsoft.com/de-de/support/options/
Netzwerksicherheit (von Azure)	Es sind Sicherheitsmechanismen für das Produktionsnetzwerk (Kunden- und Administration) sowie das gesamte Netzwerk innerhalb von Azure, z. B. zwischen Rechenzentren, implementiert. Die Netzwerksicherheit wird auch durch kryptografische Mittel erreicht.	https://docs.microsoft.com/de-de/azure/security/fundamentals/production-network https://docs.microsoft.com/de-de/azure/security/fundamentals/infrastructure-network https://azure.microsoft.com/de-de/blog/azure-network-security/ (in Englisch) https://azure.microsoft.com/de-de/blog/how-microsoft-builds-its-fast-and-reliable-global-network/ (in Englisch) Kapitel 3.17 *OPS.2.2.A17 Einsatz von Verschlüsselung bei Cloud-Nutzung*
Regeln für Prozesse, Arbeitsabläufe, Änderungen und Verantwortlichkeiten	Azure wird als Online-Cloud-Dienst bereitgestellt. Ein umfassendes Regelwerk, einschließlich Informationssicherheitsrichtlinien (z. B. Asset Management, Malware-Schutz) liegt Azure zugrunde. Die Aufteilung der Verantwortlichkeiten, Prozesse und Verfahren ist in der Regel in den jeweiligen Vereinbarungen festgelegt.	https://www.microsoft.com/licensing/terms/productoffering (in Englisch) https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services Kapitel 2.1 *Modell der gemeinsamen Verantwortung*

Zu berücksichtigende Aspekte	Informationen von Microsoft Azure	Referenzen
	Darüber hinaus werden den Azure Kunden vielfältige Möglichkeiten hinsichtlich des Supports, der Serviceüberwachung und zum weiteren Informationsaustausch angeboten. Microsoft gibt einen Überblick über sicherheitsrelevante Informationen zu Azure, wie z. B. physische Infrastruktur, Netzwerk, Überwachung oder Malware-Schutz. Microsoft veröffentlicht auf seinen Webseiten Informationen über Updates, Features und geplante Entwicklungen. Änderungsmanagement und Testrichtlinien werden in einem internen Richtliniendokument definiert.	https://docs.microsoft.com/de-de/azure/security/ https://docs.microsoft.com/de-de/azure/security/fundamentals/infrastructure-monitoring https://azure.microsoft.com/de-de/updates/ (Meldungen in Englisch)
Bestimmungen zur Beendigung der vertraglichen Vereinbarung	Azure wird auf Abonnementbasis angeboten, eine vorzeitige Kündigung ist möglich. Weitere Informationen zum Vertragsende wird in der entsprechenden Anforderung beschrieben.	https://www.microsoft.com/licensing/terms/productoffering (in Englisch) https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services https://docs.microsoft.com/de-de/azure/cost-management-billing/manage/cancel-azure-subscription Kapitel 3.14 *OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzung*
Sichere Löschung der Daten durch den Cloud-Diensteanbieter sicherstellen	Wenn ein nicht vorab gebührenpflichtiges Abonnement gekündigt wird oder endet, wird das Azure-Kundenkonto in ein Konto mit eingeschränkter Funktion umgewandelt. Dann haben die Kunden 90 Tage Zeit, ihre Daten zu exportieren. Nach diesen 90 Tagen wird das Konto gesperrt und die Kundendaten gelöscht. Das Konto selbst wird spätestens 180 Tage nach seiner Kündigung oder Beendigung des Abonnements gelöscht. Physische Speichermedien werden am Ende ihrer Nutzungsdauer vor Ort sicher vernichtet.	https://docs.microsoft.com/de-de/azure/cost-management-billing/manage/cancel-azure-subscription https://www.microsoft.com/de-de/trust-center/privacy/data-management https://aka.ms/DPA https://docs.microsoft.com/de-de/azure/security/fundamentals/physical-security#data-bearing-devices

Zu berücksichtigende Aspekte	Informationen von Microsoft Azure	Referenzen
	Microsoft verwendet Best Practice-Verfahren und ein Löschverfahren, das NIST 800-88-konform ist. Alle Azure-Dienste nutzen genehmigte Dienstleistungen zur Lagerung und Entsorgung von Medien.	
Notfallvorsorge	Azure hat Sicherheitsmaßnahmen festgelegt, um die Verfügbarkeit der Cloud-Dienste laut dem in den SLAs festgelegten Niveau sicherzustellen. Zu den entsprechenden Sicherheitsvorkehrungen gehört die geografische Trennung der Rechenzentren und die kontinuierliche Replikation zwischen ihnen. Azure bietet Dienste zur Bereitstellung von Replikations-, Failover- und Wiederherstellungsprozessen wie Azure Backup und Site Recovery an.	https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services https://docs.microsoft.com/de-de/azure/architecture/reliability/disaster-recovery https://docs.microsoft.com/de-de/azure/backup/backup-overview https://docs.microsoft.com/de-de/azure/site-recovery/site-recovery-overview
Gesetzliche Anforderungen	Microsoft hält sich an die Gesetze und Regeln bezüglich der Bereitstellung des Cloud-Dienstes. Microsoft veröffentlicht statistische Daten über Anfragen von Strafverfolgungsbehörden auf der ganzen Welt zwei Mal im Jahr. Microsoft stellt Informationen über den Umgang mit personenbezogenen Daten und die Einhaltung der europäischen Datenschutz-Grundverordnung (EU-DSGVO) zur Verfügung. Die gesamten rechtlichen Informationen können über die Webseite der Rechtsberatung abgerufen werden.	https://www.microsoft.com/en-us/corporate-responsibility/lerr (in Englisch) https://www.microsoft.com/de-de/trust-center/privacy https://docs.microsoft.com/de-de/compliance/regulatory/gdpr-arc-azure-dynamics-windows https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3 (Berichte und Zertifikate in Englisch) https://docs.microsoft.com/de-de/compliance/regulatory/offering-EU-Model-Clauses https://azure.microsoft.com/de-de/support/legal/
Regeln für Kontrollen und Audits	Azure wird aufgrund der Anforderungen mehrerer Normen und Zertifizierungen kontinuierlich auditiert. Microsoft stellt Informationen über die Konformität, Audits und Zertifizierungen zur Verfügung.	https://docs.microsoft.com/de-de/compliance/regulatory/offering-home https://docs.microsoft.com/de-de/azure/service-health/

Zu berücksichtigende Aspekte	Informationen von Microsoft Azure	Referenzen
	Dies schließt auch öffentlich zugängliche Berichte und Ergebnisse ein. Microsoft Azure bietet Kunden die Möglichkeit, die Einhaltung von SLAs mit dem Modul "Service Health" zu überwachen. Cloud-Kunden haben die Möglichkeit, Penetrationstests oder Schwachstellenscans gegen ihre Cloud-Dienste durchzuführen, ohne Microsoft zu benachrichtigen, wenn die entsprechenden Einsatzregeln eingehalten werden. Die Haupteinschränkung besteht darin, dass keine Denial-of-Service Tests erlaubt sind und dass keine anderen Kunden durch die durchgeführten Tests gestört werden dürfen. Für die Steuerung eigener Dienste bietet Azure eine breite Palette von Protokollierungs- und Überwachungsfunktionen.	https://docs.microsoft.com/de-de/azure/security/fundamentals/pen-testing https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement (in Englisch) https://docs.microsoft.com/de-de/azure/security/fundamentals/log-audit
Überwachung der Leistungserbringung	Die Servicebereitstellung kann mit dem Modul „Service Health“ im Azure-Portal, auf der Azure-Status-Website oder durch Anpassung der von Azure bereitgestellten Überwachungsfunktionen überwacht werden.	https://azure.microsoft.com/de-de/documentation/articles/insights-how-to-customize-monitoring/ https://azure.microsoft.com/de-de/features/azure-portal/ https://azure.microsoft.com/de-de/status/
Datenschutz	Die vertraglichen Regelungen zum Datenschutz können sich von Organisation zu Organisation unterscheiden und sollten daher gemeinsam mit dem Datenschutzbeauftragten oder der Rechtsabteilung geprüft werden. Microsoft bietet seinen Kunden die EU-Standardvertragsklauseln (SCC) (auch bekannt als EU-Musterklauseln) an, die spezifische Schutzmaßnahmen für die Übermittlung personenbezogener Daten für die in den Anwendungsbereich fallenden Dienste vorsehen, um vertraglich sicherzustellen, dass alle personenbezogenen Daten, die den EWR verlassen,	https://aka.ms/DPA https://docs.microsoft.com/de-de/compliance/regulatory/offering-eu-model-clauses https://www.microsoft.com/de-de/trust-center/privacy/gdpr-overview https://docs.microsoft.com/de-de/compliance/regulatory/gdpr https://eu-coc.cloud/en/home.html

Zu berücksichtigende Aspekte	Informationen von Microsoft Azure	Referenzen
	in Übereinstimmung mit der DSGVO übermittelt werden. Infolge des Urteils des Europäischen Gerichtshofs (EuGH) vom Juli 2020, mit dem das EU-US-Datenschutzschild-Abkommen für ungültig erklärt wurde, wurde das Datenschutz-Addendum zu Microsoft-Produkten und -Diensten durch das Appendix C Additional Safeguard Addendum ergänzt. In diesem Anhang werden zusätzliche Sicherheitsmaßnahmen im Hinblick auf die Verarbeitung personenbezogener Daten festgelegt. Microsoft informiert darüber, wie die GDPR-Anforderungen gehandhabt werden und gibt auch Informationen darüber, wie Cloud-Kunden die GDPR-Anforderungen handhaben können. Darüber hinaus hat Microsoft den EU Cloud Code of Conduct (EU Cloud CoC) unterzeichnet und bescheinigt damit, dass seine Cloud-Dienste den strengen europäischen Datenschutzanforderungen entsprechen.	

3.10 OPS.2.2.A10 Sichere Migration zu einem Cloud-Dienst

Diese Anforderung konzentriert sich auf die eigentliche Migration zu einem Cloud-Dienst gemäß den Überlegungen im zuvor diskutierten Migrationssicherheitskonzept (siehe Kapitel 3.5 *OPS.2.2.A5 Planung der sicheren Migration zu einem Cloud-Dienst*). Die Migration muss kontinuierlich überwacht werden, um erforderliche Änderungen oder Probleme frühzeitig zu erkennen und darauf zu reagieren können. Gegebenenfalls sollte die Migration abgebrochen und eine Untersuchung der Probleme durchgeführt werden. Um das Risiko von signifikanten Problemen zu verringern, sollte zunächst eine Test- oder Pilotmigration durchgeführt werden.

Microsoft FastTrack kann bei der Migration zu Microsoft Azure helfen. FastTrack ist ein Dienst, der in den Azure-Abonnements enthalten ist. Durch Microsoft FastTrack erhalten Unternehmen Zugang zu Experten von Microsoft, die auf die Migration nach Microsoft Azure spezialisiert sind. Ebenso listet Microsoft viele seiner externen Partner als Cloud-Experten auf der Webseite auf.[47]

[47] https://azure.microsoft.com/de-de/partners/

Microsoft bietet Tools zur Unterstützung bei der Migration aktueller Ressourcen nach Azure.[48]

Microsoft Azure bietet verschiedene Dienstleistungen für die Entwicklung und den Test von Anwendungen an[49], die von der gemeinsamen Nutzung und Zusammenarbeit von Quelltext bis hin zu automatisierten Builds und Testumgebungen reichen.

3.11 OPS.2.2.A11 Erstellung eines Notfallkonzepts für einen Cloud-Dienst

Als präventiver Schutz sollte ein Notfallkonzept für Azure-Dienste entwickelt werden. Insbesondere das Fehlen von Wiederherstellungsplänen kann zu langen Ausfallzeiten führen, einschließlich Produktivitätseinschränkungen und Einschränkungen bei der Nutzung von Cloud-Diensten. Der Wiederherstellungsplan sollte organisatorische und technische Aspekte enthalten. Auf der einen Seite sollten die Verantwortlichkeiten definiert werden und auf der anderen Seite ausfallsichere Infrastrukturen mit Redundanzen festgelegt werden.

Diese Anforderung deckt keine der Besonderheiten der Notfallwiederherstellung für den Cloud-Dienste selbst ab - dies ist die Aufgabe von Microsoft und wird über die jeweiligen Service Levels Agreements vertraglich abgedeckt[50]. Stattdessen deckt diese Anforderung den individuellen Notfallplan für Ihr Unternehmen bei Verlust des Cloud-Dienstes selbst oder bei Verlust des Zugangs zu ihm ab. Es geht auch um Situationen, in denen die geltenden Service Levels Ihre Anforderungen nicht erfüllen.

Sollten die Online-Dienste nicht verfügbar sein, kann der Notfallplan auch die Durchführung von Datensicherungen gemäß Kapitel 3.16 *OPS.2.2.A16 Durchführung eigener Datensicherungen* beinhalten.

Darüber hinaus sollten die Notfallkonzepte für die relevanten Geschäftsprozesse, die von Azure abhängen, den Verlust der Verfügbarkeit spezifisch und detailliert berücksichtigen. Dies ist unabhängig von der Ursache des Verfügbarkeitsverlustes zu planen (z. B. Ausfall des Internetzugangs im lokalen Netz, Ausfall beim Internet Service Provider).

Tabelle 8 Azure Unterstützung für die Notfallplanung

Aspekte	Unterstützung durch Microsoft	Referenzen
Organisatorische Aspekte der Notfallplanung bei der Nutzung der Cloud	Microsoft bietet Anleitungen für die Implementierung Wiederherstellungsplänen innerhalb von Microsoft Azure.	https://docs.microsoft.com/de-de/azure/architecture/reliability/disaster-recovery
Technische Aspekte der Notfallplanung bei der Nutzung der Cloud	Azure Backup und Site Recovery oder ähnliche Dienste eines externen Backup-Anbieters können zur Implementierung eines Datensicherungskonzepts und zur Wiederherstellung verlorener Daten verwendet werden.	https://azure.microsoft.com/de-de/services/site-recovery/ https://azure.microsoft.com/de-de/services/backup/ https://azure.microsoft.com/de-de/overview/azure-stack/

[48] https://azure.microsoft.com/de-de/downloads/

[49] https://azure.microsoft.com/de-de/product-categories/devops/

[50] https://www.microsoft.com/de-de/licensing/product-licensing/products.aspx (Service Level Agreements (SLA))

Aspekte	Unterstützung durch Microsoft	Referenzen
	Einen weiteren Schutz in einer hybriden Cloud-Umgebung bietet Azure Stack. Azure Stack ermöglicht die konsistente Ausführung von Hybridanwendungen auf lokaler Ebene ohne Einschränkungen der Cloud. Für Systeme mit sehr hohen Schutzanforderungen kann eine hybride Umgebung mit Azure Stack in Betracht gezogen werden.	

3.12 OPS.2.2.A12 Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb

Ziel dieser Anforderung ist es, nach der Migration zu einem Cloud-Dienst ein vergleichbares oder erhöhtes Maß an Informationssicherheit aufrechtzuerhalten. Dementsprechend sollten Richtlinien und Dokumentationen auf dem neuesten Stand gehalten werden und die Einhaltung der Sicherheitsstandards sowohl vom Kunden als auch vom Cloud-Diensteanbieter regelmäßig überprüft werden.

Tabelle 9 Aufrechterhaltung der Informationssicherheit

Erforderliche Sicherheitsvorkehrungen	Beschreibung	Referenzen
Aktualisierung der Dokumentation und Richtlinien (z. B. Betriebsanleitungen und Verfahren)in regelmäßigen Abständen	Die regelmäßige Überprüfung und Aktualisierung der Richtlinien ist Teil eines effektiven Informationssicherheitsmanagementsystems (ISMS). Dieser Prozess sollte innerhalb des Dokumentenmanagementprozesses implementiert werden. Microsoft weist die Erfüllung dieser Anforderung durch Zertifizierungen nach. Die Zertifizierungen können über das Service Trust Portal (STP) eingesehen werden.	https://servicetrust.microsoft.com/ (in Englisch)
Regelmäßige Überprüfung von erbrachten Dienstleistungen	Microsoft Azure stellt ein integriertes SLA-Überwachungssystem („Service Health“) zur Verfügung, mit dem der Kunde die Einhaltung der Cloud-Dienste überprüft werden kann. Laut den jeweils geltenden Vertragsbedingungen, die mit den	https://docs.microsoft.com/de-de/azure/azure-monitor/platform/data-platform https://azure.microsoft.com/de-de/features/azure-portal/ https://status.azure.com/de-de/status

Erforderliche Sicherheitsvorkehrungen	Beschreibung	Referenzen
	Dienstleistern geschlossen werden, behält sich Microsoft das Recht vor, Prüfungen bei Vertragspartnern durchzuführen.	https://www.microsoft.com/de-de/licensing/product-licensing/products.aspx (Online Service Terms (OST)) https://www.microsoft.com/en-us/procurement/contracting-terms-conditions.aspx (in Englisch)
Bereitstellung von Sicherheitsnachweisen durch den Cloud-Diensteanbieter	Microsoft Azure bietet in diesem Zusammenhang eine Vielzahl von Publikationen und Berichte sowie entsprechende Zertifizierungen an. Die Berichte zu den Zertifizierungen und Testaten können über das Service Trust Portal (STP) eingesehen werden.	https://servicetrust.microsoft.com (in Englisch) https://servicetrust.microsoft.com/Documents/ComplianceReports
Regelmäßige Abstimmungsgespräche zwischen dem Cloud-Diensteanbieter und dem Kunden	Microsoft Azure bietet eine Vielzahl von Supportoptionen an. Cloud-Kunden werden im Falle einer erheblichen Störung des Dienstes kontaktiert.	https://azure.microsoft.com/de-de/support/options/
Planung von Übungen und Tests zur Reaktionssimulation bei Systemausfällen	Microsoft Azure hat Sicherheitsmaßnahmen implementiert, die Fortsetzung der Dienste auf dem im SLA festgelegten Niveau sicherstellen. Zusätzlich bietet Microsoft einen Leitfaden für die Erstellung einer zuverlässigen Anwendung in Azure.	https://www.microsoft.com/licensing/terms/productoffering (in Englisch) https://docs.microsoft.com/de-de/azure/architecture/framework/resiliency/overview
Sicherstellung der ordnungsgemäßen Verwaltung von Cloud-Diensten	Eine fehlerhafte Cloud-Administration kann aufgrund der sehr hohen Komplexität zu erheblichen Sicherheitsproblemen (z. B. Serviceausfall, Datenverlust) führen. Schon kleine Fehler oder Ausfälle können einen großen Einfluss (nicht nur auf die Sicherheit) auf eine Cloud-Infrastruktur haben. Microsoft bietet Blueprints als Instrument an, um einen wiederholbaren Satz von Cloud-Ressourcen mit einem Regelsatz zu definieren. Ein solcher Regelsatz kann Konfigurationen, aber auch Sicherheitseinschränkungen beinhalten.	https://docs.microsoft.com/de-de/azure/governance/blueprints/overview

Erforderliche Sicherheitsvorkehrungen	Beschreibung	Referenzen
Sicherstellung der Interoperabilität von Cloud-Diensten	Bei der Nutzung mehrerer Cloud-Diensten sollten für jeden Service Interoperabilitätstests durchgeführt werden, um eine ordnungsgemäße Zusammenarbeit zwischen den verschiedenen Cloud-Diensten zu gewährleisten.	https://www.microsoft.com/en-us/legal/interoperability (in Englisch)
Ordnungsgemäße Durchführung von Datensicherungen	Eine ordnungsgemäße Durchführung der Datensicherung muss gewährleistet sein, damit keine kritischen Geschäftsprozesse durch einen Ausfall gefährdet werden können. Backups können entweder mit einem Backup-Service von Azure, einem Backup-Service eines externen Anbieters oder einem Backup-System des Kunden durchgeführt werden. Wird sich ein externer Anbieter entschieden, muss der Kunde sicherstellen, dass alle Anforderungen an Backup und Datensicherheit erfüllt sind.	https://docs.microsoft.com/de-de/azure/backup/backup-overview Kapitel 3.16 *OPS.2.2.A16 Durchführung eigener Datensicherungen*
Kontrolle der technischen Maßnahmen zur Verhinderung der Nutzung nicht autorisierter Dienste	Diese Anforderung liegt in der Verantwortung des Cloud-Kunden. Die IT-Organisation sollte die technischen Maßnahmen, z. B. mit Hilfe von Proxys oder Cloud Access Security Brokern (CASB), kontrollieren, um die unberechtigte Nutzung von Diensten zu verhindern.	https://docs.microsoft.com/de-de/azure/backup/backup-overview https://docs.microsoft.com/de-de/defender-cloud-apps/what-is-defender-for-cloud-apps
Durchführung von Audits, Sicherheitschecks, Penetrationstests oder Schwachstellenanalysen	Cloud-Kunden haben die Möglichkeit, Penetrationstests oder Schwachstellenscans gegen ihren Cloud-Dienst durchzuführen. Dies muss bei Microsoft nicht angemeldet werden. Die Tests müssen entsprechend der Regeln erfolgen. Die Haupteinschränkung besteht darin, dass keine Denial-of-Service Tests erlaubt sind und dass keine anderen Kunden durch die durchgeführten Tests gestört werden dürfen.	https://docs.microsoft.com/de-de/azure/security/fundamentals/pen-testing https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement (in Englisch)

3.13 OPS.2.2.A13 Nachweis einer ausreichenden Informationssicherheit bei der Cloud-Nutzung

Im Rahmen eines effizienten Informationssicherheitsmanagements sollte die regelmäßige Überprüfung der festgelegten Sicherheitsvorkehrungen durchgeführt werden. Dadurch wird sichergestellt, dass der Kunde seine Auditanforderungen erfüllt und die Vereinbarungen auf beiden Seiten eingehalten werden. Dies kann beispielsweise durch Vor-Ort-Audits oder spezifische Fragebögen unabhängig vom Cloud-Service-Modell erreicht werden.

Microsoft Azure wird aufgrund der Anforderungen mehrerer internationaler und nationaler Compliance-Standards und Zertifizierungen kontinuierlich auditiert und stellt entsprechende Konformitätsberichte und mehrere Bewertungsberichte zur Verfügung.[51] Dazu gehören die Berichte für ISO 27017, ISO 27018 und SOC (siehe Kapitel 4 für weitere Details). Diese Audits oder Überprüfungen werden von akkreditierten Auditgesellschaften durchgeführt, wobei zusätzliche interne Audits unter der Kontrolle von Microsoft durchgeführt werden. Informationen zu diesen Audits sind online im Microsoft Trust Center verfügbar. Darüber hinaus können Vertragskunden über das das Service Trust Portal (STP)[52] direkten Zugriff auf viele der Compliance-Berichte und -Zertifikate erhalten.

Die Verantwortung für das Lesen und Bewerten der Berichte liegt beim Cloud-Kunden. Der Kunde sollte sicherstellen, dass die Auswertung der Berichte von qualifiziertem Personal durchgeführt wird.

3.14 OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses

Vor Abschluss eines Vertrages mit einem Cloud-Diensteanbieter sollten die relevanten Aspekte für die Beendigung des Cloud-Dienste-Vertrags definiert werden. In einer kritischen Situation kann das Fehlen vertraglicher Regelungen die Beendigung des Dienstleistungsverhältnisses verhindern. Nach Beendigung des Dienstleistungsvertrages sollte der Geschäftsbetrieb nicht negativ beeinflusst werden. Mit dieser Anforderung soll deutlich gemacht werden, dass ein Wechsel entweder zu einem anderen Cloud-Diensteanbieter oder zurück zu einem lokalen Infrastrukturmodell ebenso sorgfältig geplant werden muss wie die Erstintegration. Das Planungs- und Migrationskonzept sollte das Sicherheitskonzept ähnlich wie bei der ursprünglichen Umstellung auf die Cloud berücksichtigen.

Die Vorbereitung einer Exit-Strategie hilft die Risiken zu minimieren, die mit einem kurzfristigen Wechsel eines oder mehrerer Cloud-Dienste verbunden sind. Microsoft stellt seinen Kunden den Leitfaden „Exit Planning for Microsoft Cloud Services"[53] zur Verfügung.

Azure bietet mehrere Möglichkeiten, Daten aus Azure zu exportieren, die im Kapitel 3.15 *OPS.2.2.A15 Portabilität von Cloud-Diensten* behandelt werden. Bei der Kündigung des Azure-Vertrags als Online-Dienst sollte unter anderem Folgendes sichergestellt werden:

---

[51] https://servicetrust.microsoft.com/Documents/ComplianceReports

[52] https://servicetrust.microsoft.com/

[53] https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3?command=Download&downloadType=Document&downloadId=4aa0c653-312f-4098-b78a-0d499e07825e&tab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913&docTab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913_FAQ_and_White_Papers (in Englisch)

- Alle relevanten Arbeitsdaten wurden vollständig in die neue Umgebung übertragen.
- Alle relevanten Daten, die aufbewahrt oder archiviert werden sollen, wurden in einen geeigneten Speicher übertragen.
- Die neue Umgebung bietet alle notwendigen Eigenschaften und Funktionen.

Kündigungsfristen sind in den Datenschutzvereinbarungen (DPA) geregelt. [54]In Microsoft Azure werden Kundendaten spätestens 90 oder 180 Tage nach Ablauf der vereinbarten Nutzungsdauer oder der Kündigung des Nutzungsvertrages gelöscht[55].

3.15 OPS.2.2.A15 Portabilität von Cloud-Diensten

Ziel dieser Anforderung ist es, ein hohes Maß an Flexibilität beim Wechsel des Cloud-Diensteanbieters, beim Einbringen von Daten in die Cloud oder bei der Rückführung eines Cloud-Dienst in die lokale Infrastruktur zu gewährleisten. In diesem Fall sind eine Reihe von Anforderungen zu berücksichtigen, insbesondere in Bezug auf Dateiformate und Portabilitätstests.

Microsoft hat sich für Interoperabilität und Portabilität eingesetzt. Azure unterstützt eine breite Auswahl an Betriebssystemen, Programmiersprachen, Frameworks, Tools, Datenbanken und Geräten, so dass der Kunde die am besten geeigneten Lösungen auswählen kann[56]. Zusätzlich unterstützen Drittanbieter-Tools den Import und Export von Daten in verschiedene Azure-Dienste.

Weitere Überlegungen zur Portabilität sind in der folgenden Tabelle für ausgewählte Cloud-Dienste aufgeführt.

Tabelle 10 Portabilität von Cloud-Diensten in Azure

Cloud-Dienste	Informationen zur Portabilität	Referenzen
Azure Active Directory	Die Verwendung von Azure Active Directory ermöglicht die Verwendung von Single-Sign-On über tausende von Cloud-Diensten und -Anwendungen hinweg. Mit Azure AD Connect können lokale Profile in Azure Active Directory integriert und über die Cloud synchronisiert werden.	https://docs.microsoft.com/de-de/azure/active-directory/fundamentals/active-directory-whatis https://docs.microsoft.com/de-de/azure/active-directory/hybrid/whatis-hybrid-identity
Azure Key Vault	Key Vault ist ein Cloud-Dienst für die Verwaltung sicherer Geheimnisse in Azure. Die Portabilität ist	https://docs.microsoft.com/de-de/azure/key-vault/general/overview

[54] https://azure.microsoft.com/de-de/support/legal/subscription-agreement/

[55] https://docs.microsoft.com/de-de/azure/cost-management-billing/manage/cancel-azure-subscription (in Englisch)

https://aka.ms/DPA

[56] https://docs.microsoft.com/de-de/azure/#pivot=products
https://docs.microsoft.com/de-de/azure/#pivot=sdkstools
https://docs.microsoft.com/de-de/azure/containers/

Cloud-Dienste	Informationen zur Portabilität	Referenzen
	für Azure Key Vault nicht vorgesehen.	
Azure-Portal	Das Azure Portal ist eine Webanwendung von Microsoft. Die Portabilität ist für Azure-Portal nicht vorgesehen.	https://docs.microsoft.com/de-de/azure/azure-portal/azure-portal-overview
Blob Speicher	Der Azure Blob Speicher ermöglicht es dem Kunden, Daten mit Hilfe der Import-/Exportfunktionalität zu importieren und zu exportieren. Die Azure Storage Import-Export REST API bietet eine API zur Verwaltung der automatischen Übertragung von Daten zu oder von Blob-Speichern.	https://docs.microsoft.com/de-de/azure/storage/blobs/storage-blobs-overview https://docs.microsoft.com/de-de/azure/import-export/storage-import-export-service https://docs.microsoft.com/en-us/rest/api/storageimportexport/ (in Englisch)
Cloud Services	Cloud Services ist eine Plattform für die Entwicklung und Bereitstellung eigener Cloud-Dienste und Anwendungen. Die Portabilität ist für Cloud Services nicht vorgesehen.	https://docs.microsoft.com/de-de/azure/cloud-services/cloud-services-choose-me
Cosmos Datenbanken	Cosmos Databases bietet eine Auswahl an APIs, über die in der Datenbank gespeicherten Daten gearbeitet werden kann. Es ermöglicht die Migration von Anwendungen unter Beibehaltung wesentlicher Teile Ihrer Anwendungslogik. Es wurde entwickelt, um Anwendungen portabel und damit herstellerunabhängig zu halten.	https://docs.microsoft.com/de-de/azure/cosmos-db/introduction
Kubernetes	Mit Kubernetes können containerisierte Workloads nahtlos von lokalen Entwicklungsmaschinen in verschiedene Umgebungen verschoben werden.	https://docs.microsoft.com/de-de/azure/aks/intro-kubernetes
Service Fabric	Service Fabric ist eine Plattform für die Entwicklung und Bereitstellung von Microservice-basierten Anwendungen und die Verwal-	https://docs.microsoft.com/de-de/azure/service-fabric/service-fabric-overview

Cloud-Dienste	Informationen zur Portabilität	Referenzen
	tung ihrer Lebenszyklen. Die Portabilität ist für Service Fabric nicht vorgesehen.	
SQL-Datenbanken	Die Azure SQL-Datenbanken können in eine BACPAC-Datei kopiert und einfach in anderen Umgebungen eingesetzt werden.	https://docs.microsoft.com/de-de/azure/sql-database/sql-database-technical-overview https://docs.microsoft.com/de-de/azure/sql-database/sql-database-export
Virtuelle Maschinen	Virtuelle Maschinen können in Azure importiert werden, indem man die generalisierte oder spezialisierte virtuelle Festplatte (VHD) importiert. Die Migration von VMware Virtual Machines nach Azure ist sowohl Agenten-los als auch Agenten-basiert möglich. Virtuelle Maschinen können einfach exportiert werden, indem die virtuelle Festplatte (VHD) heruntergeladen und die VHD auf eine andere virtuelle Maschine geladen wird.	https://docs.microsoft.com/de-de/azure/virtual-machines/windows/prepare-for-upload-vhd-image https://docs.microsoft.com/de-de/azure/virtual-machines/windows/on-prem-to-azure https://docs.microsoft.com/de-de/azure/virtual-machines/windows/upload-generalized-managed https://docs.microsoft.com/de-de/azure/migrate/server-migrate-overview https://docs.microsoft.com/de-de/azure/migrate/tutorial-migrate-vmware https://docs.microsoft.com/de-de/azure/migrate/tutorial-migrate-vmware-agent https://docs.microsoft.com/de-de/azure/virtual-machines/windows/download-vhd
Virtuelle Netzwerke	Azure Virtual Network bietet eine isolierte, sichere Umgebung für virtuelle Maschinen und Anwendungen. Eine Netzwerkkonfigurationsdatei kann in Azure importiert und von dort exportiert werden, um virtuelle Netzwerke zu konfigurieren.	https://docs.microsoft.com/de-de/azure/virtual-network/virtual-networks-overview

3.16 OPS.2.2.A16 Durchführung eigener Datensicherungen

Diese Anforderung zielt darauf ab, die Datenverfügbarkeit sicherzustellen, wenn der Zugriff auf Azure-Daten verloren geht, Cloud-Dienste selbst nicht verfügbar sind oder wenn Daten durch Benutzeraktionen (z. B. versehentliches Löschen von Daten) verloren gehen.

Microsoft bietet den Cloud-Dienst Azure Backup an. Mit diesem Dienst können beispielsweise virtuelle Maschinen, die sich entweder vor Ort oder in Azure befinden, gesichert werden. Es sind auch Lösungen von Drittanbietern für Backups verfügbar. Einige Anbieter bieten zum Beispiel eine Lösung an, die ein lokales Backup oder ein Backup bei einem anderen Cloud-Anbieter beinhaltet.[57]

3.17 OPS.2.2.A17 Einsatz von Verschlüsselung bei Cloud-Nutzung

Für die Verschlüsselung und anderen kryptografischen Verfahren ist es notwendig, geeignete Sicherheitsvorkehrungen wie Algorithmen, Protokolle oder Schlüssellänge zu identifizieren und zu definieren, da unzureichend geschützte Daten von unbefugten Dritten eingesehen werden können.

Microsoft Azure bietet verschiedene Verschlüsselungsoptionen und verwendet dabei die Verschlüsselung in einer Reihe von Bereichen. [58] Kunden haben die Möglichkeit, die Verschlüsselung abhängig vom gewählten Dienst mit Standard- oder individuellen Verschlüsselungstechnologien zu aktivieren. Die verschiedenen Verschlüsselungsmöglichkeiten sind vom jeweiligen Dienst abhängig und müssen daher vom Kunden im Einzelfall unter Verwendung der von Microsoft für jeden Dienst bereitgestellten Dokumentationen und Richtlinien bewertet werden.

Die folgende Tabelle zeigt exemplarisch die von Azure bereitgestellten Funktionalitäten zur Verschlüsselung von Daten im gespeicherten Zustand, während der Übertragung und wie entsprechende Geheimnisse sicher verwaltet werden können.

Tabelle 11 Verschlüsselung und Schlüsselverwaltung

Kategorien	Informationen zur Verschlüsselung und Schlüsselverwaltung	Referenzen
Verschlüsselung von Daten im gespeicherten Zustand	Im Allgemeinen ist für Azure-Dienste eine client-seitige Verschlüsselung (Kunde) und/oder eine serverseitige Verschlüsselung (innerhalb der Cloud) für gespeicherte Daten möglich. Bei der client-seitigen Verschlüsselung behält der Cloud-Kunde die Kontrolle über die Verschlüsselung und die zugehörigen Schlüssel, kann aber die Funktionalität des Cloud-Dienstes verlieren.	https://docs.microsoft.com/de-de/azure/security/fundamentals/encryption-atrest https://docs.microsoft.com/de-de/sql/relational-databases/security/encryption/transparent-data-encryption

[57] https://docs.microsoft.com/de-de/azure/backup/backup-overview

[58] https://docs.microsoft.com/de-de/azure/security/fundamentals/encryption-overview

https://docs.microsoft.com/de-de/azure/security/fundamentals/protection-customer-data

Kategorien	Informationen zur Verschlüsselung und Schlüsselverwaltung	Referenzen
	Azure bietet Festplattenverschlüsselung für virtuelle Maschinen über BitLocker für Windows oder über dmcrypt für Linux an. Die entsprechenden Schlüssel können im Azure Key Vault gespeichert werden. Der Azure Storage Dienst bietet Verschlüsselung für Azure Blob Storage und Azure File Shares unter Verwendung von Azure Storage Service Encryption mit einer AES256 Verschlüsselung. Die entsprechende Verschlüsselung ist für den Benutzer transparent. Für die verschiedenen Arten von Datenbanken in Azure stehen verschiedene Verschlüsselungsmethoden zur Verfügung. Transparente Datenverschlüsselung wird für die serverseitige Verschlüsselung verwendet. Für Azure SQL ist auch eine client-seitige Verschlüsselung über die Funktion „Always Encrypted“ möglich. Zusätzlich bietet Azure eine Verschlüsselung auf Zellen- oder Spaltenebene für bestimmte Datenbanken, die die Verwendung unterschiedlicher symmetrischer oder asymmetrischer Schlüssel pro Zelle oder Spalte ermöglichen. Azure Data Lake Store bietet dem Kunden eine transparente Verschlüsselung. Es gibt verschiedene Verschlüsselungslösungen von Drittanbietern für Azure, die eine kundenseitige Verschlüsselung unter Beibehaltung bestimmter Cloud-Dienst-Funktionen wie Suchfunktionen realisieren.	https://docs.microsoft.com/de-de/azure/security/fundamentals/azure-disk-encryption-vms-vmss https://docs.microsoft.com/de-de/azure/storage/common/storage-service-encryption https://docs.microsoft.com/de-de/azure/storage/blobs/security-recommendations https://docs.microsoft.com/de-de/sql/relational-databases/security/encryption/transparent-data-encryption https://docs.microsoft.com/de-de/azure/data-lake-store/data-lake-store-encryption
Verschlüsselung der Daten während der Übertragung	Microsoft verwendet das Transport Layer Security (TLS)-Protokoll mit Perfect Forward Secrecy (PFS), um Daten zu schützen, wenn Daten zwischen den Cloud-Diensten und Kunden übermittelt werden.	https://docs.microsoft.com/de-de/azure/security/fundamentals/encryption-overview#encryption-of-data-in-transit

Kategorien	Informationen zur Verschlüsselung und Schlüsselverwaltung	Referenzen
	Der Zugriff auf Azure Speicher über Azure Portal und über REST API kann über HTTPS geschützt werden. Die Verwendung von HTTPS kann konfiguriert werden. Daten während der Übertragung zu, von und zwischen virtuellen Maschinen in Azure können verschlüsselt werden. Der Zugriff auf virtuelle Windows-Maschinen kann mit RDP über TLS gesichert werden. Der Zugriff auf Linux basiert auf SSH, das standardmäßig verschlüsselt ist. Azure virtuelle Netzwerke können über VPN über einen sicheren Tunnel angesprochen werden. Dabei bietet Azure verschiedene Möglichkeiten für VPNs: • Point-to-Site VPN ermöglicht es einzelnen Clients, über das Secure Socket Tunnel Protocol (SSTP) auf ein virtuelles Azure-Netzwerk zuzugreifen. Dabei können Kunden ihre eigenen PKI-Zertifikate verwenden. • Site-to-Site und Multi-Site können für standortübergreifende und hybride virtuelle Netzwerkkonfigurationen verwendet werden. Die Verbindung wird über IPsec/IKE (IKEv1 oder IKEv2) realisiert. • VNet-to-VNet kann verwendet werden, um verschiedene virtuelle Netzwerke über IPsec/IKE (IKEv1 oder IKEv2) zu verbinden. Daten, die an den Data Lake Store übertragen werden, werden mit HTTPS verschlüsselt.	https://docs.microsoft.com/de-de/azure/security/fundamentals/encryption-overview#in-transit-encryption-in-vms https://docs.microsoft.com/de-de/azure/vpn-gateway/vpn-gateway-about-vpngateways https://docs.microsoft.com/de-de/azure/data-lake-store/data-lake-store-encryption
Verschlüsselung von Daten während diese verarbeitet werden	Azure ist in der Lage, Daten während der Verarbeitung zu verschlüsseln. Mit Azure Confidential Computing bietet Microsoft Funktionen zur Datensicherheit durch Trusted Execution Environments (TEEs) oder Verschlüsselungsmechanismen zum	https://azure.microsoft.com/de-de/solutions/confidential-compute/ https://www.microsoft.com/en-us/research/uploads/prod/2018/08/Confiden-

Kategorien	Informationen zur Verschlüsselung und Schlüsselverwaltung	Referenzen
	Schutz von Daten während der Nutzung. TEEs sind Hard- oder Software-Implementierungen, die die zu verarbeitenden Daten vor dem Zugriff von außerhalb des TEE schützen.	tal_Computing_Mark-Russinovich_Manuel-Costa.pdf (in Englisch)
Schlüsselmanagement	Azure bietet die Möglichkeit Zertifikate und andere geheime Informationen sicher zu speichern und bietet verschiedene Methoden, um z. B. eine sichere Schlüsselverwaltung zu realisieren: • Azure Key Vault speichert Geheimnisse in einem virtuellen Schlüsselspeicher oder einem mit anderen Kunden geteilten Hardware-Sicherheitsmodul. • Ein dediziertes HSM stellt sicher, dass das Hardware-Sicherheitsmodul für die Schlüsselverwaltung nur von einem Kunden verwendet wird. Bring-Your-Own-Key ermöglicht die Schlüsselerzeugung im HSM des Kunden. Der Schlüssel wird dann innerhalb von Azure auf ein HSM übertragen.	https://docs.microsoft.com/de-de/azure/key-vault/about-keys-secrets-and-certificates https://docs.microsoft.com/de-de/azure/key-vault/key-vault-overview https://docs.microsoft.com/de-de/azure/dedicated-hsm/overview https://docs.microsoft.com/de-de/azure/key-vault/keys/hsm-protected-keys https://docs.microsoft.com/de-de/azure/information-protection/configure-adrms-restrictions

3.18 OPS.2.2.A18 Einsatz von Verbunddiensten

Im Rahmen von Cloud-Computing-Projekten sollte die Nutzung von Verbunddiensten überprüft werden. Über Verbunddienste können Benutzerinformationen oder andere persönliche Informationen von Mitarbeitern sicher außerhalb des Unternehmens übertragen werden. Das Hauptmerkmal ist die Trennung von Authentifizierung (Identity Provider) und Autorisierung (Service Provider).

Der primäre Schutz besteht darin, sicherzustellen, dass nur die minimal notwendigen Informationen im SAML-Ticket an den Cloud-Diensteanbieter gesendet werden.[59] Darüber hinaus müssen die Benutzerrechte und -rollen regelmäßig überprüft werden, um sicherzustellen, dass nur autorisierte Benutzer Zugriff haben.

[59] SAML (Security Assertion Markup Language) ist ein Standard-Auszeichnungssprache zum Austausch von Authentifizierungs- und Autorisierungsinformationen.

Mit Azure Active Directory können sowohl lokale als auch Konten/Identitäten, die ausschließlich in der Cloud sind, verwaltet werden. Es gibt drei allgemeine Möglichkeiten, hybride Konten zu realisieren. Diese bringen unterschiedlichen Vor- und Nachteilen mit:[60]

- Passwort-Hash-Synchronisation (PHS): Für PHS synchronisiert Azure Active Directory Connect einen Hash des Benutzerpasswort-Hashes von einem lokalen Active Directory des Kunden mit dem Azure Active Directory, so dass Azure Active Directory Benutzerpasswörter direkt validieren kann.[61]
- Pass-Through-Authentifizierung (PTA): PTA ermöglicht es Benutzern, sich lokal und in Azure mit dem gleichen Passwort anzumelden. Wenn sich ein Benutzer bei der Verwendung von Azure Active Directory anmeldet, validiert PTA das Passwort direkt gegen das lokale Active Directory und ermöglicht so die Durchsetzung der lokalen Active Directory-Sicherheits- und Passwortregeln.[62]
- Active Directory Federation Services (ADFS):[63] Mit ADFS wird ein Vertrauensverhältnis zwischen der lokalen Umgebung und Azure Active Directory eingerichtet, das für die Authentifizierung und Autorisierung verwendet werden kann. ADFS stellt sicher, dass alle Benutzerauthentifizierungen lokal erfolgen und ermöglicht es Administratoren, strengere Zugriffskontrollen durchzuführen. PHS kann optional als Backup für den Fall eines ADFS-Ausfalls implementiert werden.

Azure Active Directory, unterstützt das SAML 2.0 Protokoll[64] sowie WS-Federation und OpenID Connect.[65] Die in den SAML-Tickets enthaltenen Informationen können je nach organisatorischen Anforderungen oder den Anforderungen der jeweiligen Anwendung konfiguriert werden.[66]

Die Benutzerrechte sollten regelmäßig überprüft werden und es sollte sichergestellt sein, dass ein SAML-Ticket nur an berechtigte Benutzer vergeben werden kann. Die Überprüfung der Vergabe von Berechtigungen sollte Teil eines klar definierten Prozesses der Identitäts- und Berechtigungsmanagement sein. Das IT-Grundschutz-Modul *ORP.4 Identitäts- und Berechtigungsmanagement*[67] zeigt die Anforderungen an die Umsetzung der notwendigen Verfahren auf.

Darüber hinaus sollte die Überprüfung des korrekten Ticketausgabeprozesses von SAML an autorisierte Benutzer Teil von Audits und technischen Tests im Rahmen des etablierten ISMS sein. Die Erfüllung dieser Anforderung liegt in der Verantwortung des Kunden.

---

[60] https://docs.microsoft.com/de-de/azure/active-directory/hybrid/whatis-hybrid-identity

[61] https://docs.microsoft.com/de-de/azure/active-directory/hybrid/whatis-phs

[62] https://docs.microsoft.com/de-de/azure/active-directory/hybrid/how-to-connect-pta

[63] https://docs.microsoft.com/de-de/azure/active-directory/hybrid/whatis-fed

[64] https://docs.microsoft.com/de-de/azure/active-directory/develop/single-sign-on-saml-protocol

[65] https://docs.microsoft.com/de-de/azure/active-directory/develop/id-tokens

[66] https://docs.microsoft.com/de-de/azure/active-directory/manage-apps/configure-single-sign-on-non-gallery-applications

https://docs.microsoft.com/de-de/azure/active-directory/develop/active-directory-saml-claims-customization

[67] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2022/02_ORP_Organisation_und_Personal/ORP_4_Identitaets_und_Berechtigungsmanagement_Editon_2022.pdf

3.19 OPS.2.2.A19 Sicherheitsüberprüfung von Mitarbeitern

Der Kunde sollte sicherstellen, dass der Dienstleister im Rahmen der gesetzlichen Vorgaben Mitarbeiter-Hintergrundprüfungen durchführt.

Microsoft führt Sicherheitschecks und Hintergrundüberprüfungen aller internen und externen Mitarbeiter durch, die Zugriff auf Daten von Cloud-Kunden haben können.

Darüber hinaus verfolgt Microsoft eine strenge Dienstleisterpolitik. Für eine erfolgreiche Zusammenarbeit mit Lieferanten und Dienstleistern definiert das Dienstleisterprogramm von Microsoft die Art und Weise, wie wichtige geschäftskritische und strategische Lieferanten und Dienstleister mit Microsoft Geschäfte tätigen, einschließlich der Anforderungen und Erwartungen von Microsoft und der Kunden.[68] Außerdem werden Lieferanten und Dienstleister nur dann zum Dienstleisterprogramm von Microsoft zugelassen, wenn diese die Microsoft-Compliance-Anforderungen erfüllen.

Darüber hinaus verpflichtet der Microsoft Supplier Code of Conduct (SCoC) den Lieferanten und Dienstleister vor der Erbringung der Dienstleistung für Microsoft die eigenen Mitarbeitern einer Hintergrundüberprüfung zu unterziehen, soweit dies nach geltendem Recht zulässig ist.[69] Für das interne Personal von Microsoft ist die Hintergrundüberprüfung abhängig von der Rolle und den erforderlichen Zugriffsrechten definiert und ist im *Microsoft Personnel Screening Standard* vorgeschrieben.[70] Microsoft bietet auch das SCoC-Schulungsprogramm an, um die Mitarbeiter der Lieferanten und Dienstleister zu schulen.[71]

[68] https://www.microsoft.com/en-us/procurement/msp-overview.aspx?activetab=pivot1:primaryr4 (in Englisch)

[69] https://www.microsoft.com/en-us/procurement/supplier-conduct.aspx?activetab=pivot:primaryr7 (in Englisch)

[70] https://docs.microsoft.com/de-de/compliance/assurance/assurance-human-resources

[71] https://www.microsoft.com/en-us/procurement/supplier-conduct.aspx?activetab=pivot:primaryr7 (in Englisch)

4 Umsetzung des Mindeststandards zur Nutzung externer Cloud-Dienste

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat einen Mindeststandard veröffentlicht, der für Bundesbehörden gilt und Anforderungen an die Beschaffung, (Mit-)Nutzung und Beendigung von Cloud-Diensten stellt. Externe Cloud-Dienste sind in diesem Zusammenhang Cloud-Dienste, die nicht vom Bund bereitgestellt werden.

Kann der Bedarf an einem IT-Dienst nicht durch eigene IT-Ressourcen des Bundes gedeckt werden, sondern z. B. durch Azure, kann die Bundesbehörde entscheiden, den externen Cloud-Dienst anstelle von internen IT-Ressourcen zu nutzen. Dies ist definiert als die Nutzung externer Cloud-Dienste. Im Gegensatz dazu beschreibt die Mitnutzung von externen Cloud-Diensten die Nutzung externer Cloud-Dienste durch Nutzer einer Bundesbehörde ohne Vertragsverhältnis zwischen der Bundesbehörde und dem Cloud-Diensteanbieter.

In diesem Kapitel wird beschrieben, wie alle Anforderungen des *Mindeststandards des BSI zur Nutzung externer Cloud-Dienste*[72] für Azure umgesetzt werden können. Während einige Anforderungen nur individuell durch Kunden erfüllt werden können, kann Microsoft für alle Anforderungen Informationen bereitstellen.

Häufig verweist der *Mindeststandard des BSI zur Nutzung externer Cloud-Dienste*[73] hinsichtlich der umzusetzenden Anforderungen auf IT-Grundschutz-Anforderungen. Die folgende Tabelle gibt einen Überblick auf die Verweise zu IT-Grundschutz Anforderungen.

Tabelle 12: Überblick Schnittstellen zu IT-Grundschutz Anforderungen

Anforderung	Verweise
NCD.2.1.01 Cloud-Nutzungs-Strategie	Kapitel 3.1 *OPS.2.2.A1 Erstellung einer Cloud-Nutzungs-Strategie*
NCD.2.1.02 Sicherheitsrichtlinie externe Cloud-Dienste	Kapitel 3.2 *OPS.2.2.A2 Erstellung einer Sicherheitsrichtlinie für die Cloud*

[72] https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html

[73] https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html

Anforderung	Verweise
NCD.2.1.03 Sicherheitskonzept für den externen Cloud-Dienst	Kapitel 3.7 *OPS.2.2.A7 Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung*
NCD.2.1.04 Notfall- und Kontinuitätsmanagement	Kapitel 3.11 *OPS.2.2.A11 Erstellung eines Notfallkonzepts für einen Cloud-Dienst* Kapitel 3.15 *OPS.2.2.A15 Portabilität von Cloud-Diensten* Kapitel 3.16 *OPS.2.2.A16 Durchführung eigener Datensicherungen*
NCD.2.2.01 Umsetzung der Sicherheitsanforderungen	Kapitel 3.2 *OPS.2.2.A2 Erstellung einer Sicherheitsrichtlinie für die Cloud*
NCD.2.2.02 Umgang mit Unterauftragnehmern und anderen externen Dritten vertraglich zusichern	Kapitel 3.8 *OPS.2.2.A8 Sorgfältige Auswahl eines Cloud-Diensteanbieters* Kapitel 3.9 *OPS.2.2.A9 Vertragsgestaltung mit dem Cloud-Diensteanbieter*
NCD.2.2.03 Gerichtsbarkeit vertraglich zusichern	Kapitel 3.9 *OPS.2.2.A9 Vertragsgestaltung mit dem Cloud-Diensteanbieter*
NCD.2.2.04 Lokation vertraglich zusichern	Kapitel 3.9 *OPS.2.2.A9 Vertragsgestaltung mit dem Cloud-Diensteanbieter*
NCD.2.2.05 Offenbarungspflichten und Ermittlungsbefugnisse vertraglich zusichern	Kapitel 3.9 *OPS.2.2.A9 Vertragsgestaltung mit dem Cloud-Diensteanbieter*
NCD.2.2.06 Beendigung des Vertragsverhältnisses regeln	Kapitel 3.9 *OPS.2.2.A9 Vertragsgestaltung mit dem Cloud-Diensteanbieter* Kapitel 3.14 *OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses*
NCD.2.2.07 Datenrückgabe und Datenlöschung beim Cloud-Diensteanbieter vertraglich zusichern	Kapitel 3.9 *OPS.2.2.A9 Vertragsgestaltung mit dem Cloud-Diensteanbieter* Kapitel 3.14 *OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses* Kapitel 3.15 *OPS.2.2.A15 Portabilität von Cloud-Diensten*

Anforderung	Verweise
NCD.2.3.01 ISMS einbinden	Kapitel 3.7 *OPS.2.2.A7 Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung* Kapitel 3.12 *OPS.2.2.A12 Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb*
NCD.2.3.02 Sicherheitsnachweise prüfen	Kapitel 3.13 *OPS.2.2.A13 Nachweis einer ausreichenden Informationssicherheit bei der Cloud-Nutzung*
NCD.2.3.03 Leistungsfähigkeit prüfen	Kapitel 3.5 *OPS.2.2.A5 Planung der sicheren Migration zu einem Cloud-Dienst* Kapitel 3.6 *OPS.2.2.A6 Planung der sicheren Einbindung von Cloud-Diensten*
NCD.2.3.04 Informationspflichten nachhalten	Kapitel 3.4 *OPS.2.2.A4 Festlegung von Verantwortungsbereichen und Schnittstellen* Kapitel 3.12 *OPS.2.2.A12 Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb*
NCD.2.3.05 Zwei-Faktor-Authentifizierungen aktivieren	Kein Verweis
NCD.2.4.01 Datenrückgabe durchführen	Kapitel 3.14 *OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses* Kapitel 3.15 *OPS.2.2.A15 Portabilität von Cloud-Diensten*
NCD.2.4.02 Datenlöschung bestätigen	Kapitel 3.9 *OPS.2.2.A9 Vertragsgestaltung mit dem Cloud-Diensteanbieter* Kapitel 3.14 *OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses*
NCD.2.5.01 Mitnutzung externer Cloud-Dienste	Kapitel 3.1 *OPS.2.2.A1 Erstellung einer Cloud-Nutzungs-Strategie* Kapitel 3.2 *OPS.2.2.A2 Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung* Kapitel 3.7 *OPS.2.2.A7 Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung*

Anforderung	Verweise
	Kapitel 3.9 *OPS.2.2.A9 Vertragsgestaltung mit dem Cloud-Diensteanbieter* Kapitel 3.17 *OPS.2.2.A17 Einsatz von Verschlüsselung bei Cloud-Nutzung*

4.1 NCD.2.1.01 Cloud-Nutzungs-Strategie

Es ist durch die Institution eine Cloud-Nutzungs-Strategie entsprechend der BSI IT-Grundschutz Anforderung *OPS.2.2.A1 Erstellung einer Cloud-Nutzungs-Strategie* (siehe Kapitel 3.1) zu erstellen. Im Rahmen der Cloud-Nutzungs-Strategie ist durch die Institution zu entscheiden, wie sie mit den Risiken, die durch die Auslagerung in die Cloud einhergehen, umgeht. Nach Erstellung der Cloud-Nutzungs-Strategie ist zu überprüfen, ob die Nutzung von Azure den Anforderungen dieser entspricht. Im Rahmen einer Risikoanalyse ist die Nutzung von Azure zu überprüfen.

Microsoft stellt Informationen zur Erstellung einer Cloud-Nutzungs-Strategie beispielsweise in Form des Leitfadens „Enterprise Cloud Strategy“[74] zur Verfügung. Weitere Informationen zur Erstellung einer Cloud Nutzungs-Strategie sind im Kapitel 3.1 *OPS.2.2.A1 Erstellung einer Cloud-Nutzungs-Strategie* enthalten.

Für die Risikoanalyse stellt Microsoft weitreichende Informationen zu eigenen Sicherheitsmaßnahmen[75] und Sicherheitsmaßnahmen pro verwendeten Cloud-Dienst, die durch den Cloud-Kunden durchgeführt werden können, bereit. So kann beispielsweise die „Always Encrypted“-Funktionalität[76] für manche Datenbankarten aktiviert werden, damit einzelne Datenbankspalten verschlüsselt werden.

4.2 NCD.2.1.02 Sicherheitsrichtlinie externe Cloud-Dienste

Entsprechend der BSI IT-Grundschutz Anforderung *OPS.2.2.A2 Erstellung einer Sicherheitsrichtlinie für die Cloud* (siehe Kapitel 3.2) ist von der Institution, die Azure einsetzen möchte, eine Sicherheitsrichtlinie durch die verantwortlichen Personen zu erstellen. Der *Mindeststandard des BSI zur Nutzung externer Cloud-Dienste*[77] gibt vor, dass die Umsetzung und Einhaltung der Basiskriterien nach dem BSI

[74] https://info.microsoft.com/enterprise-cloud-strategy-ebook.html (in Englisch)

[75] https://docs.microsoft.com/de-de/azure/security/fundamentals/overview

[76] https://docs.microsoft.com/de-de/sql/relational-databases/security/encryption/always-encrypted-database-engine

[77] https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html

Kriterienkatalog Cloud Computing (C5)[78] als spezielle Sicherheitsanforderungen an den Cloud-Dienste-anbieter in der Sicherheitsrichtlinie festgelegt werden muss.

Externe Prüfer haben für Azure die Einhaltung der Basiskriterien nach dem BSI Kriterienkatalog Cloud Computing (C5)[79] festgestellt. Der SOC 2-Bericht zur Prüfung kann im Service Trust Portal (STP)[80] eingesehen werden.

4.3 NCD.2.1.03 Sicherheitskonzept für den externen Cloud-Dienst

Neben der Cloud-Nutzungsstrategie (siehe Kapitel 4

NCD.2.1.01 Cloud-Nutzungs-Strategie) und eine Cloud-Sicherheitsrichtlinie (siehe Kapitel 4.2 *NCD.2.1.02 Sicherheitsrichtlinie externe Cloud-Dienste*) ist nach der IT-Grundschutzanforderung des BSI *OPS.2.2.A7 Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung* (siehe Kapitel 3.7) auch eine Sicherheitskonzept zu erstellen.

Im Rahmen des IT-Sicherheitskonzepts ist insbesondere der Schutzbedarf der in der Cloud verarbeiteten dienstlichen Daten in einer Risikoanalyse zu betrachten. Für die Risikoanalyse stellt Microsoft weitreichende Informationen zu eigenen Sicherheitsmaßnahmen[81] und Sicherheitsmaßnahmen pro verwendeten Cloud-Dienst, die durch den Cloud-Kunden durchgeführt werden können, bereit. So kann beispielsweise die „Always Encrypted"-Funktionalität[82] für manche Datenbankarten aktiviert werden, um einzelne Datenbankspalten zu verschlüsseln.

Über das Tagging[83] können die Cloud-Kunde die Datenklassifizierung an die einzelnen Cloud-Dienste anbringen und anhand dieser Datenklassifizierung mittels Azure Policy[84] oder Azure Purview[85] Sicherheitsvorgaben, wie beispielsweis, dass eine Datenbank niemals unverschlüsselt deployt werden darf, durchsetzen. Zudem bringen verschiedene Datenbank-Services eigene Datenklassifizierungsmechanismen[86] mit.

Weitere Informationen zur Erstellung eines Cloud-Sicherheitskonzepts ist in Kapitel 3.7 *OPS.2.2.A7 Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung* beschrieben.

---

[78] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_AktuelleVersion/C5_AktuelleVersion_node.html

[79] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_AktuelleVersion/C5_AktuelleVersion_node.html

[80] https://servicetrust.microsoft.com/Documents/ComplianceReports

[81] https://docs.microsoft.com/de-de/azure/security/fundamentals/overview

[82] https://docs.microsoft.com/de-de/sql/relational-databases/security/encryption/always-encrypted-database-engine

[83] https://docs.microsoft.com/de-de/azure/azure-resource-manager/management/tag-resources

[84] https://docs.microsoft.com/de-de/azure/azure-resource-manager/management/tag-policies
https://docs.microsoft.com/de-de/azure/governance/policy/overview

[85] https://docs.microsoft.com/de-de/azure/purview/overview

[86] https://docs.microsoft.com/de-de/azure/azure-sql/database/data-discovery-and-classification-overview

4.4 NCD.2.1.04 Notfall- und Kontinuitätsmanagement

Wie in der IT-Grundschutz Anforderung *OPS.2.2.A11 Erstellung eines Notfallkonzepts für einen Cloud-Dienst* (siehe Kapitel 3.11) fordert auch der *Mindeststandard des BSI zur Nutzung externer Cloud-Dienste*[87] eine Bewertung durch die Institution, wie sich ein Ausfall von Azure oder einzelner Azure-Dienste auf die Institution auswirken würde. Zusätzlich sollte zusammen mit dem zuständigen Notfallbeauftragten überprüft werden, ob sich die Nutzung von Cloud-Diensten in Azure auf die bisherige Notfallbehandlung auswirkt und somit die bisherigen präventiven / reaktiven Maßnahmen angepasst werden können.

Microsoft stellt mit der eigenen Architektur und Infrastruktur der Rechenzentren und der darin betriebenen Cloud-Dienst sicher, dass ein definiertes Maß an Ausfallsicherheit vorhanden ist. Zusätzlich können beispielsweise Datenspeicher redundant ausgelegt werden[88], so dass auf Azure betriebene Anwendungen auf andere Regionen geschwenkt werden können.

Die Erstellung eines Notfallkonzepts wird in den Kapiteln 3.11 *OPS.2.2.A11 Erstellung eines Notfallkonzepts für einen Cloud-Dienst*, 3.15 *OPS.2.2.A15 Portabilität von Cloud-Diensten* und 3.16 *OPS.2.2.A16 Durchführung eigener Datensicherungen* weitergehend beschrieben.

4.5 NCD.2.2.01 Umsetzung der Sicherheitsanforderungen

Vor dem Vertragsabschluss muss bewertet werden, ob Azure die in der Sicherheitsrichtlinie (siehe Kapitel 3.2 *OPS.2.2.A2 Erstellung einer Sicherheitsrichtlinie für die Cloud* und 4.2 *NCD.2.1.02 Sicherheitsrichtlinie externe Cloud-Dienste*) vorgegebenen Anforderungen erfüllen kann und im Rahmen des Einsatzes von Azure ist regelmäßig zu überprüfen, ob die umsetzbaren Sicherheitsmaßnahmen und die vorhandenen Sicherheitsnachweise weiterhin der Sicherheitsrichtlinie entsprechen.

Microsoft stellt weitreichende Informationen zu eigenen Sicherheitsmaßnahmen[89] und Sicherheitsmaßnahmen pro verwendeten Cloud-Dienst, die durch den Cloud-Kunden durchgeführt werden können, bereit. So kann beispielsweise die „Always Encrypted"-Funktionalität[90] für manche Datenbankarten aktiviert werden, um einzelne Datenbankspalten zu verschlüsseln.

Microsoft lässt Audits durch Kunden zu in der Microsoft Online Services DPA[91] festgelegten Bedingungen zu. Wenn die Audit-Anforderungen des Kunden gemäß den Standardvertragsklauseln oder den Datenschutzanforderungen durch Audit-Berichte, Dokumentationen oder sonstige Compliance-Informationen, die Microsoft den Kunden allgemein zugänglich macht, nicht angemessen erfüllt werden können, bietet Microsoft die Möglichkeit, zusätzliche Audit-Anforderungen des Kunden zu erfüllen. Bevor

[87] https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html

[88] https://docs.microsoft.com/de-de/azure/storage/common/storage-redundancy

[89] https://docs.microsoft.com/de-de/azure/security/fundamentals/overview

[90] https://docs.microsoft.com/de-de/sql/relational-databases/security/encryption/always-encrypted-database-engine

[91] https://aka.ms/DPA

ein Audit beginnt, legt Microsoft mit dem Kunden den Umfang, den Zeitpunkt, die Dauer, die Kontroll- und Nachweisanforderungen sowie die Auditgebühren fest.

Microsoft führt ständig eigene Audits nach mehreren nationalen und internationalen Normen durch und hat entsprechende Zertifizierungen, Nachweise oder Auditberichte im Service Trust Portal (STP)[92] veröffentlicht. Dort kann auch der aktuelle SOC 2-Bericht zur Prüfung des Kriterienkatalogs Cloud Computing (C5) abgerufen werden.

4.6 NCD.2.2.02 Umgang mit Unterauftragnehmern und anderen externen Dritten vertraglich zusichern

Die Institution sollte sicherstellen, dass sie die Informationen zu Subunternehmer von Microsoft und ihre Geschäftsbeziehungen erhält. Updates sollten über ein Internetportal oder eine Push-Benachrichtigung angekündigt werden.

Microsoft stellt eine Liste von Subunternehmern zur Verfügung und bietet Zugang zu standardisierten Dienstvereinbarungen, Richtlinien und Verhaltensregeln.[93] Externe Prüfer haben für Azure die Einhaltung der Basiskriterien nach dem BSI Kriterienkatalog Cloud Computing (C5)[94] festgestellt. Der SOC 2-Bericht zur Prüfung kann im Service Trust Portal (STP)[95] eingesehen werden.

Weitergehende Informationen sind in den Kapiteln 3.8 *OPS.2.2.A8 Sorgfältige Auswahl eines Cloud-Diensteanbieters* und 3.9 *OPS.2.2.A9 Vertragsgestaltung mit dem Cloud-Diensteanbieter* enthalten.

4.7 NCD.2.2.03 Gerichtsbarkeit vertraglich zusichern

Nach Möglichkeit sollte der Gerichtsstand Deutschland sein. Es sollte sichergestellt sein, dass kein Zeitverlust und keine Handlungseinbußen entstehen, wenn ein Rechtsschutz erforderlich ist.

In den Datenschutzbestimmungen wird das Land des Kunden als Gerichtsstand definiert.[96]

Informationen und Links zum Vertragsentwurf und zu den Dokumenten befinden sich im Kapitel 3.9 *OPS.2.2.A9 Vertragsgestaltung mit dem Cloud-Diensteanbieter*.

[92] https://servicetrust.microsoft.com/Documents/ComplianceReports

[93] https://www.microsoft.com/de-de/licensing/product-licensing/products.aspx

[94] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_AktuelleVersion/C5_AktuelleVersion_node.html

[95] https://servicetrust.microsoft.com/Documents/ComplianceReports

[96] https://aka.ms/DPA

4.8 NCD.2.2.04 Lokation vertraglich zusichern

Der Ort, an dem die Daten verarbeitet werden, sollte vertraglich vereinbart werden. Die Berechtigung zur Datenverarbeitung in den gesicherten Regionen ist abhängig von der Datenkategorisierung gemäß des Mindeststandards, der Risikoanalyse und den Zugangsmöglichkeiten eines ausländischen Staats.

Microsoft veröffentlicht die Regionen, in denen Daten von Azure gespeichert sind.[97] Aus Gründen der Datenverarbeitung können Kundendaten jedoch außerhalb der gewählten Region verarbeitet werden. Die geografische Speicherregion für Daten kann vom Kunden frei gewählt werden.[98] Ab Ende 2022 wird die Datenspeicherung und -verarbeitung u.a. für Azure ausschließlich in Europa stattfinden.[99]

Darüber hinaus veröffentlicht Microsoft zweimal jährlich eine Statistik zu Anfragen von Strafverfolgungsbehörden aus der ganzen Welt.[100]

Informationen und Links zum Vertragsentwurf und zu den Dokumenten befinden sich im Kapitel 3.9 *OPS.2.2.A9 Vertragsgestaltung mit dem Cloud-Diensteanbieter*.

4.9 NCD.2.2.05 Offenbarungspflichten und Ermittlungsbefugnisse vertraglich zusichern

Als Cloud-Diensteanbieter sollte Microsoft Sicherheitsvorfälle (und alle anderen Vorfälle) an die Kunden melden. Diese Anforderung sollte vertraglich geregelt werden. Wobei der *Mindeststandard des BSI zur Nutzung externer Cloud-Dienste*[101] auch die Vereinbarung von Vertragsvertragsstrafen bei Nichterfüllung vorsieht.

Microsoft hat eine interne Richtlinie[102] zur Benachrichtigung der betroffenen Parteien während eines Informationssicherheitsvorfalls. Informationen über die Informationspflichten der Personen im Rahmen der EU-DSGVO werden ebenfalls veröffentlicht[103]. Darüber hinaus veröffentlicht Microsoft zweimal jährlich eine Statistik zu Anfragen von Strafverfolgungsbehörden aus der ganzen Welt.[104]

Informationen und Links zum Vertragsentwurf und zu den Dokumenten befinden sich im Kapitel 3.9 *OPS.2.2.A9 Vertragsgestaltung mit dem Cloud-Diensteanbieter*.

---

[97] https://azure.microsoft.com/de-de/global-infrastructure/services/

[98] https://azure.microsoft.com/de-de/global-infrastructure/regions/

[99] https://techcommunity.microsoft.com/t5/security-compliance-and-identity/eu-data-boundary-for-the-microsoft-cloud-frequently-asked/ba-p/2329098 (in Englisch)

[100] https://www.microsoft.com/en-us/corporate-responsibility/lerr (in Englisch)

[101] https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html

[102] https://docs.microsoft.com/de-de/compliance/regulatory/gdpr-breach-notification

[103] https://servicetrust.microsoft.com/ViewPage/GDPRBreach

[104] https://www.microsoft.com/en-us/corporate-responsibility/lerr (in Englisch)

4.10 NCD.2.2.06 Beendigung des Vertragsverhältnisses regeln

Die Kündigung des Vertrages sollte mit einer dem Einsatzszenario angemessenen Kündigungsfrist möglich sein. Dabei sollten kurzfristige einseitige Kündigungs- oder Zurückbehaltungsrechte an den vereinbarten Leistungen zu Lasten der Institution vertraglich ausgeschlossen werden.

Die Standard-SLAs von Microsoft bieten dem Kunden jederzeit ein Kündigungsrecht. Weitere Informationen und Links zur Beendigung des Vertrages befinden sich in den Kapiteln 3.9 *OPS.2.2.A9 Vertragsgestaltung mit dem Cloud-Diensteanbieter* und 3.14 *OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses*.

4.11 NCD.2.2.07 Datenrückgabe und Datenlöschung beim Cloud-Diensteanbieter vertraglich zusichern

Im Rahmen der Vertragsgestaltung (siehe auch Kapitel 3.9 *OPS.2.2.A9 Vertragsgestaltung mit dem Cloud-Diensteanbieter* und 3.14 *OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses*) sollte die Portierbarkeit der Daten (siehe auch Kapitel 3.15 *OPS.2.2.A15 Portabilität von Cloud-Diensten*) als auch die nachfolgende Löschung der Daten verhandelt und vertraglich festgehalten werden.

Microsoft gewährt mindestens 90 Tage Datenzugriff nach Beendigung des Abonnements. Spätestens nach 180 Tagen werden die Daten gelöscht. Alle Speichergeräte, auf denen Kundendaten gespeichert sein könnten, werden mit Hilfe eines Verfahrens gelöscht, das den Vorgaben nach NIST SP-800-88 entspricht.[105]

4.12 NCD.2.3.01 ISMS einbinden

Azure als auch die auf Azure betriebenen Cloud-Dienste sollte in das ISMS der Institution integriert werden. Dabei sollte beachtet werden, dass die im BSI Kriterienkatalog Cloud Computing (C5)[106] enthaltenen Anforderungen, die sich an den Cloud-Kunden wenden, im ISMS umgesetzt sind.

Dies ist eine kundenspezifische Anforderung. Informationen zum Sicherheitskonzept befinden sich im Kapitel 3.7 *OPS.2.2.A7 Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung* und in Kapitel 3.12 *OPS.2.2.A12 Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb* werden Maßnahmen zum Compliance-Erhalt beschrieben.

[105] https://www.microsoft.com/de-de/trust-center/privacy/data-management
https://docs.microsoft.com/de-de/azure/cost-management-billing/manage/cancel-azure-subscription
https://docs.microsoft.com/de-de/compliance/assurance/assurance-data-bearing-device-destruction

[106] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_AktuelleVersion/C5_AktuelleVersion_node.html

4.13 NCD.2.3.02 Sicherheitsnachweise prüfen

Diese Anforderung ist kundenspezifisch, da sie erforderliche Zertifizierungen und Auditberichte auf der Grundlage der Datenkategorien gemäß des *Mindeststandards des BSI zur Nutzung externer Cloud-Dienste*[107] und der Risikoanalyse des Kunden umfasst. Weiterhin verpflichtet diese Anforderung den Cloud-Kunden, diese Nachweise regelmäßig hinsichtlich der Erfüllung von Sicherheitsanforderungen zu überprüfen.

Azure verfügt über mehrere globale und regionale Zertifizierungen[108]. Darüber hinaus werden Auditberichte und andere Compliance-Informationen, wie z. B. Penetrationstests, regelmäßig auf der Webseite von Microsoft veröffentlicht[109][110]. Die Verantwortung für die Definition der erforderlichen Zertifizierungen und die Überprüfung, ob Azure diese besitzt, liegt beim Kunden.

Informationen finden sich auch im Kapitel 3.13 *OPS.2.2.A13 Nachweis einer ausreichenden Informationssicherheit bei der Cloud-Nutzung*.

4.14 NCD.2.3.03 Leistungsfähigkeit prüfen

Vor der Migration in die Cloud sollte sich der Cloud-Anwender vergewissern, dass die lokale Infrastruktur in Bezug auf die Leistung ausreichend ist. Insbesondere sollte die Internetverbindung den Anforderungen an Verfügbarkeit und Bandbreite entsprechen. Diese Überprüfung sollte jährlich wiederholt werden und dabei sollte auch die Leistungsfähigkeit des Cloud-Diensteanbieters und des Cloud-Dienstes sowie der Netzverbindung zum Cloud-Diensteanbieter beurteilt werden.

Der aktuelle Dienststatus kann online zu den Azure-Diensten abgerufen werden.[111]

Weitere Informationen und Links zur Migration und Integration nach Azure befinden sich in den Kapiteln 3.5 *OPS.2.2.A5 Planung der sicheren Migration zu einem Cloud-Dienst* und 3.6 *OPS.2.2.A6 Planung der sicheren Einbindung von Cloud-Diensten*.

4.15 NCD.2.3.04 Informationspflichten nachhalten

Es ist die Aufgabe der Institution darauf zu achten, dass Microsoft als Cloud-Diensteanbieter seinen vertraglichen Informationspflichten nachkommt. Vertragliche Informationspflichten liegen beispielsweise vor, wenn ein Subunternehmer ausgetauscht wird oder ein relevanter Cyberangriff vorliegt.

Microsoft veröffentlicht zu verschiedenen Szenarien und Vorkommnissen Informationen, um seinen Informationspflichten nachzukommen. Weitere Informationen sind in den Kapiteln 3.4 *OPS.2.2.A4*

---

[107] https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html

[108] https://docs.microsoft.com/de-de/compliance/regulatory/offering-home

[109] https://servicetrust.microsoft.com/Documents/ComplianceReports

[110] https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3 (in Englisch)

[111] https://status.azure.com/de-de/status

Festlegung von Verantwortungsbereichen und Schnittstellen und 3.12 *OPS.2.2.A12 Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb* enthalten.

4.16 NCD.2.3.05 Zwei-Faktor-Authentifizierungen aktivieren

Diese Anforderung verlangt die Nutzung von Multi-Faktor-Authentifizierung (MFA), sofern sie verfügbar ist. Dabei ist Multi-Faktor-Authentifizierung (MFA) mindestens für administrative Konten einzusetzen.

Im Azure Active Directory werden verschiedene Optionen angeboten, um Multi-Faktor-Authentifizierung (MFA)[112] zu konfigurieren. Multi-Faktor-Authentifizierung kann dabei für alle Benutzer, für einzelne Benutzer oder mit Hilfe des bedingten Zugriffs zu bestimmten Szenarien oder Ereignissen aktiviert werden. Dabei werden verschiedene Multi-Faktor-Authentifizierungs-(MFA)-Methoden, z. B. über mobile App, Smartcard oder bestimmte MFA-Lösungen von Drittanbietern unterstützt.[113]

4.17 NCD.2.4.01 Datenrückgabe durchführen

Alle Kundendaten müssen nach Beendigung der Cloud-Nutzung vom Cloud-Diensteanbieter in der vereinbarten Form zurückgegeben werden.

Weitere Informationen zum Abruf der Daten aus Azure befinden sich in den Kapiteln 3.14 *OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses* und 3.15 *OPS.2.2.A15 Portabilität von Cloud-Diensten*.

4.18 NCD.2.4.02 Datenlöschung bestätigen

Wird die Datenlöschung vom Kunden gewünscht, muss der Cloud-Dienstleister die Löschung aller Daten gemäß NCD.2.2.07 Datenrückgabe und Datenlöschung beim Cloud-Diensteanbieter vertraglich zusichern (siehe Kapitel 4.11) bestätigen. Dies schließt auch Datensicherungen beim Cloud-Diensteanbieter als auch Daten und Datensicherungen bei möglichen Subunternehmern und anderen externen Dritten ein.

Der Kunde muss sich mit Microsoft bzgl. eines schriftlichen Nachweises der Datenlöschung in Verbindung setzen.

Informationen und Links zur Beendigung der Cloud-Nutzung befinden sich in den Kapiteln 3.9 *OPS.2.2.A9 Vertragsgestaltung mit dem Cloud-Diensteanbieter* und 3.14 *OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses*.

[112] https://docs.microsoft.com/de-de/azure/active-directory/authentication/concept-mfa-licensing

[113] https://docs.microsoft.com/de-de/azure/active-directory/authentication/concept-mfa-howitworks

4.19 NCD.2.5.01 Mitnutzung externer Cloud-Dienste

Sofern ein Cloud-Dienst einer anderen Institution mitgenutzt wird, dann sind diverse Anforderungen einzuhalten. So müssen die nachfolgend aufgeführten Anforderungen ganz oder teilweise auch von der Institution, die einen Cloud-Dienst mit nutzt, durchgeführt werden.

-
- *NCD.2.1.01* Cloud-Nutzungs-Strategie (siehe Kapitel 4)
- *NCD.2.2.01 Umsetzung der Sicherheitsanforderungen* (siehe Kapitel 4.5)
- *NCD.2.2.04 Lokation vertraglich zusichern* (siehe Kapitel 4.8)

Weiterhin sollten die vertraglichen Unterlagen gesichtet und mit den eigenen Sicherheitsanforderungen abgeglichen werden. Ebenfalls sollten die eingesetzten Verschlüsselungsarten den eigenen Sicherheitsanforderungen entsprechen.

Auch sollte überprüft werden, ob Softwareinstallationen zur gemeinsamen Nutzung auf Arbeitsplatzrechnern oder mobilen Geräten benötigt werden. Es sollte überprüft werden, ob die zu diesem Zweck zu erteilenden Zugriffs- und Ausführungsrechte mit der Informationssicherheitspolitik und dem Sicherheitskonzept der mitnutzenden Institution übereinstimmen und ob separate Lizenzen erforderlich sein können. Darüber hinaus kann sich die mitnutzende Behörde am *Mindeststandard für das Management mobiler Geräte* orientieren[114].

Microsoft veröffentlicht die allgemein gültigen Vertragsbedingungen im Licensing-Portal[115]. Zusatzvereinbarungen sollten durch den Vertragspartner bereitgestellt werden, mit dem die Cloud gemeinsam genutzt wird.

Azure verschlüsselt Kommunikationsdaten mit Industriestandards, wie AES und TLS/SSL und auch ruhende Daten werden mittels verschiedener Methoden verschlüsselt.[116] Weitere Informationen und Links befinden sich im Kapitel 3.17 *OPS.2.2.A17 Einsatz von Verschlüsselung bei Cloud-Nutzung.*

Mit Intune stellt Microsoft ein Mobile Device Management (MDM) zur Absicherung von mobilen Geräten zur Verfügung.[117] Zusammen mit dem bedingten Zugriff kann dies genutzt werden, um den Zugriff auf bestimmte Daten oder Dienste in Azure zu beschränken.[118]

Weitere Informationen und Links zu Aspekten des Managements mobiler Geräte und des bedingten Zugangs befinden sich im Kapitel 3.7 *OPS.2.2.A7 Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung.*

[114] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Mobile-Device-Management.pdf

[115] https://aka.ms/licensingdocs

[116] https://docs.microsoft.com/de-de/azure/security/fundamentals/encryption-overview

[117] https://support.office.com/de-de/article/einrichten-der-verwaltung-mobiler-ger%C3%A4te-mdm-in-office-365-dd892318-bc44-4eb1-af00-9db5430be3cd

[118] https://docs.microsoft.com/de-de/azure/active-directory/conditional-access/overview

5 Die Verantwortung von Microsoft als Cloud-Diensteanbieter

Microsoft ist für die Sicherheit der Cloud unterhalb der Virtualisierungsschicht mit Zugriff auf Kundendaten verantwortlich. Der Cloud-Kunde sollte in der Lage sein, die Sicherheit der Cloud zu bewerten, ohne den Aufwand einer vollständigen Prüfung der technischen Infrastruktur betreiben zu müssen. Zu diesem Zweck weist Microsoft eine Reihe von sicherheitsrelevanten Zertifizierungen und Testaten für Azure vor, welche sie regelmäßig aktualisieren und veröffentlichen.

Die wichtigsten Zertifizierungen und Testate sind:

- ISO 27001 (Informationssicherheitsmanagementsystem)
- ISO 27017 (Verhaltenskodex für Informationssicherheitskontrollen basierend auf ISO 27002 für Cloud Services)
- ISO 27018 (Verhaltenskodex für den Schutz personenbezogener Daten (PII) in Public Clouds als PII-Verarbeiter)
- Kriterienkatalog - Cloud Computing (C5)
- SOC 1 - SOC 2 - SOC 3 (SSAE16 / ISAE 3402)
- PCI-DSS (Payment Card Industry Data Security Standard) für die Zahlungskartenindustrie

Darüber hinaus wird derzeit die Machbarkeit einer „ISO 27001 Zertifizierung auf Basis von IT-Grundschutz“ für Azure analysiert. Eine solche Zertifizierung wird die Zertifizierung des Cloud-Kunden erheblich erleichtern, ist aber nicht erforderlich.

Anhang A
Glossar der IT-Grundschutz-Begriffe

Begriff	Beschreibung
Anforderung	Als Sicherheitsanforderung werden Anforderungen für den organisatorischen, personellen, infrastrukturellen und technischen Bereich bezeichnet, deren Erfüllung zur Erhöhung der Informationssicherheit notwendig ist bzw. dazu beiträgt. Eine Sicherheitsanforderung beschreibt also, was getan werden muss, um ein bestimmtes Niveau bezüglich der Informationssicherheit zu erreichen. Wie die Anforderungen im konkreten Fall erfüllt werden können, ist in entsprechenden Sicherheitsmaßnahmen beschrieben.
Baustein	Das IT-Grundschutz-Kompendium enthält für unterschiedliche Vorgehensweisen, Komponenten und IT-Systeme Erläuterungen zur Gefährdungslage, Sicherheitsanforderungen und weiterführende Informationen, die jeweils in einem Baustein zusammengefasst sind. Das IT-Grundschutz-Kompendium ist aufgrund der Baustein-Struktur modular aufgebaut und legt einen Fokus auf die Darstellung der wesentlichen Sicherheitsanforderungen in den Bausteinen. Die grundlegende Struktur des IT-Grundschutz-Kompendiums sieht eine Unterteilung in prozess- und systemorientierte Bausteine vor, zudem sind sie nach Themen in ein Schichtenmodell einsortiert.
Informationsverbund	Unter einem Informationsverbund ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Objekten zu verstehen, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein Informationsverbund kann dabei als Ausprägung die gesamte Institution oder auch einzelne Bereiche, die durch organisatorische Strukturen (z. B. Abteilungen) oder gemeinsame Geschäftsprozesse bzw. Anwendungen (z. B. Personalinformationssystem) gegliedert sind, umfassen.
IT-Grundschutz-Kompendium	Die Bausteine des IT-Grundschutzes sind im IT-Grundschutz-Kompendium zusammengefasst. Es stellt den Nachfolger der bis zur 15. Ergänzungslieferung verfügbaren IT-Grundschutz-Kataloge dar.
Mindeststandard des BSI zur Nutzung externer Cloud-Dienste	Dieser Standard enthält Mindestsicherheitsanforderungen für die Nutzung externer Cloud-Dienste in der öffentlichen Verwaltung.

Modellierung	Bei den Vorgehensweisen nach IT-Grundschutz wird bei der Modellierung der betrachtete Informationsverbund einer Institution oder einer Behörde mit Hilfe der Bausteine aus dem IT-Grundschutz-Kompendium nachgebildet. Hierzu enthält Kapitel 2.2 des IT-Grundschutz-Kompendiums für jeden Baustein einen Hinweis, auf welche Zielobjekte er anzuwenden ist und welche Voraussetzungen dabei gegebenenfalls zu beachten sind.
OPS.2.2 Cloud-Nutzung	Der Baustein OPS.2.2 Cloud-Nutzung bietet Empfehlungen für die sichere Nutzung von Cloud-Diensten. Er beschreibt Cloud-Dienst-spezifische Bedrohungen und Anforderungen, um das mit den Auswirkungen unerwünschter Ereignisse verbundene Risiko zu minimieren.
Sicherheitskonzeption	Die Erstellung einer Sicherheitskonzeption ist eine der zentralen Aufgaben des Informationssicherheitsmanagements. Aufbauend auf den Ergebnissen von Strukturanalyse und Schutzbedarfsfeststellung werden hier die erforderlichen Sicherheitsmaßnahmen identifiziert und im Sicherheitskonzept dokumentiert.

Anhang B
Weiterführende Informationen

Thema	Informationszeiger
Rechtliche Informationen	https://www.microsoft.com/de-de/licensing/product-licensing/products.aspx https://www.microsoft.com/licensing/terms/welcome/welcomepage (in Englisch) https://www.microsoft.com/licensing/docs (in Englisch) https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services https://aka.ms/DPA
Due Diligence	https://azure.microsoft.com/de-de/overview/choosing-a-cloud-service-provider/ https://www.microsoft.com/de-de/trust-center/compliance/due-diligence-checklist https://www.microsoft.com/en-us/investor/default.aspx (in Englisch) https://www.microsoft.com/en-us/corporate-responsibility/lerr (in Englisch)
Compliance	https://servicetrust.microsoft.com/ https://www.microsoft.com/de-de/trust-center/ https://docs.microsoft.com/de-de/compliance/regulatory/gdpr https://docs.microsoft.com/de-de/compliance/regulatory/gdpr-breach-azure-dynamics-windows https://docs.microsoft.com/de-de/compliance/regulatory/gdpr-dpia-azure
Datenstandort	https://azuredatacentermap.azurewebsites.net (in Englisch)
Lieferanten- und Subunternehmer-Management	https://www.microsoft.com/en-us/procurement/msp-overview.aspx (in Englisch) https://go.microsoft.com/fwlink/?LinkId=2096306&clcid=0x407 (Microsoft Online Services Subprocessors List; in Englisch) https://www.microsoft.com/en-us/download/confirmation.aspx?id=50426 (Microsoft Commercial Support Subcontractors; in Englisch)

Migration und Portabilität	https://www.microsoft.com/en-us/legal/interoperability https://azure.microsoft.com/de-de/migration/ https://azure.microsoft.com/de-de/resources/cloud-migration-simplified/ https://azure.microsoft.com/mediahandler/files/resourcefiles/d8e7430c-8f62-4bbb-9ca2-f2bc877b48bd/Azure%20Onboarding%20Guide%20for%20IT%20Organizations.pdf (in Englisch) https://azure.microsoft.com/mediahandler/files/resourcefiles/efc32c2a-5c32-407c-a67d-6116cb810546/Azure_Strategic_Implementation_Guide_for_IT_Organizations_New_to_Azure.pdf (in Englisch) https://docs.microsoft.com/de-de/azure/import-export/storage-import-export-service
Verfügbarkeit, Backup und Ausfallsicherheit	https://docs.microsoft.com/de-de/azure/ddos-protection/ddos-protection-overview https://azure.microsoft.com/de-de/resources/resilience-in-azure-whitepaper https://azure.microsoft.com/de-de/features/resiliency https://azure.microsoft.com/de-de/services/backup https://docs.microsoft.com/de-de/azure/backup/backup-overview https://docs.microsoft.com/de-de/azure/architecture/framework/resiliency/backup-and-recovery
Protokollierung und Überwachung	https://docs.microsoft.com/de-de/azure/azure-monitor/overview https://docs.microsoft.com/de-de/azure/security/fundamentals/log-audit https://azure.microsoft.com/de-de/status/ https://docs.microsoft.com/de-de/azure/sentinel/overview https://docs.microsoft.com/de-de/azure/service-health
Verschlüsselung	https://docs.microsoft.com/de-de/azure/security/fundamentals/encryption-overview https://docs.microsoft.com/de-de/azure/storage/common/storage-service-encryption https://docs.microsoft.com/de-de/azure/security/fundamentals/azure-disk-encryption-vms-vmss https://docs.microsoft.com/de-de/azure/security/fundamentals/encryption-overview https://docs.microsoft.com/de-de/azure/dedicated-hsm/overview
Weitere Sicherheitsaspekte von Azure	https://info.microsoft.com/enterprise-cloud-strategy-ebook.html (in Englisch)

	https://docs.microsoft.com/de-de/azure/active-directory/conditional-access/overview https://docs.microsoft.com/de-de/azure/security/fundamentals/customer-lockbox-overview https://azure.microsoft.com/de-de/solutions/confidential-compute https://docs.microsoft.com/de-de/defender-cloud-apps/what-is-defender-for-cloud-apps https://docs.microsoft.com/de-de/mem/intune/fundamentals/what-is-intune https://docs.microsoft.com/de-de/azure/security/fundamentals/isolation-choices https://docs.microsoft.com/de-de/azure/security/fundamentals/protection-customer-data https://docs.microsoft.com/de-de/azure/security/fundamentals/anti-malware https://docs.microsoft.com/de-de/azure/governance/blueprints/overview https://docs.microsoft.com/de-de/azure/governance/policy/overview https://azure.microsoft.com/de-de/blog/azure-network-security https://docs.microsoft.com/de-de/azure/security/fundamentals/pentesting
Änderungsmanagement	https://azure.microsoft.com/de-de/updates
BSI	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_1.html https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.html https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.html https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2021.html https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/04_OPS_Betrieb/OPS_2_2_Cloud-Nutzung_Edition_2021.pdf https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Criteria_Catalogue/C5_NewRelease/C5_NewRelease_node.html

Inés Atug, Manuel Atug, Marie-Luise Wegg, Andre Windsch

HiSolutions AG
Schloßstraße 1
12163 Berlin

info@hisolutions.com
www.hisolutions.com
Tel +49 30 533 289-0
Fax +49 30 533 289-900

HiSolutions AG
Niederlassung
Frankfurt am Main
Mainzer Landstraße 50
60326 Frankfurt am Main

Tel:+49 30 533 289-0
Fax: +49 30 533 289-900

HiSolutions AG
Niederlassung
Bonn
Heinrich-Brüning-Straße 9
53113 Bonn

Tel: +49 30 533 289-0
Fax: +49 30 533 289-900

HiSolutions AG
Niederlassung
Nürnberg
Zeltnerstraße. 3
3. OG
90443 Nürnberg

Tel: +49 911 8819 72 63
Fax: +49 30 533 289-900

HiSolutions AG
Niederlassung
Düsseldorf
Kaiserswerther Straße 135
40474 Düsseldorf

Tel: +49 30 533 289-0
Fax: +49 30 533 289-900