HISOLUTIONS

IT-Grundschutz Konformität mit Azure

Version 20. Januar 2017

MICROSOFT DEUTSCHLAND GMBH

Inhaltsverzeichnis

1 Einleitung

1.1 Zusammenfassung

Microsoft Azure ist die öffentliche Cloud Computing-Plattform von Microsoft, die Cloud-Dienste auf verschiedenen Ebenen anbietet – von "Infrastructure as a Service" (IaaS) über "Platform as a Service" (PaaS) bis hin zur "Software as a Service" (SaaS). Azure eignet sich besonders für den Einsatz in Hybridumgebungen, die eigene Infrastruktur mit Cloud-Infrastrukturen verbinden.

Microsoft strebt an, möglichst alle vorhandenen globalen Azure-Dienste in der Azure Cloud Deutschland bereitstellen. Die Dienste der Azure Cloud Deutschland werden physisch in Deutschland betrieben und bieten zusätzlichen Schutz vor nach deutschem Recht unzulässigen Zugriffen durch ausländische Behörden. Dies ist auch Voraussetzung für die Einhaltung deutschen und europäischen Datenschutzrechts, welches den Transfer personenbezogener Daten in andere Länder stark einschränkt.

In Deutschland stellt das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Vorgehensweise nach IT-Grundschutz zur Verfügung. Diese besteht aus einem ISO 27001-kompatiblen ISMS (BSI Standards 100-1, 100-2), einem Verfahren zur Risikoanalyse auf der Basis von IT-Grundschutz (BSI Standard 100-3) und den IT-Grundschutz-Katalogen, welche standardisierte Gefährdungen und Maßnahmen für gängige Geschäftsumgebungen bereitstellen.

Dieses Dokument soll Kunden der Microsoft Cloud Deutschland dabei unterstützen, die Nutzung von Cloud-Diensten im Rahmen einer bestehenden oder geplanten ISO-27001-Zertifizierung auf Basis von IT-Grundschutz in ihrem Informationsverbund abzubilden.

Es wird aufgezeigt, wie die Cloud-Dienste als Teil des Verbunds modelliert werden können und wie die IT-Grundschutz-Vorgehensweise auf Anwendungen innerhalb der Cloud anzuwenden ist. Ein Überblick zur Implementierung des zentralen IT-Grundschutz-Bausteins B 1.17 Cloud-Nutzung erfolgt auf Basis der einzelnen Maßnahmen.

1.2 Modell der gemeinsamen Verantwortung

Bei der Implementierung von IT-Anwendungen in einer Cloud-Umgebung wird die Verantwortung für die Implementierung und Pflege von Sicherheitsmaßnahmen zwischen Kunde und Dienstleister aufgeteilt. Abbildung 1 zeigt einen Überblick, wie eine solche Aufteilung aussehen kann. Vom Standpunkt der IT-Grundschutz-Vorgehensweise liegt die endgültige Verantwortung immer beim Kunden (dem Dateneigentümer).

Eine Übertragung der Verantwortung kann nur erfolgen, wenn der Anbieter die Anwendungen des Kunden mit einem angepassten Risikomanagement in seinem eigenen Geltungsbereich für die Zertifizierung einbezieht (klassisches Outsourcing-Szenario).

Aktuelle Versionen des IT-Grundschutz ermöglichen ein gemeinsames Verantwortungsmodell, das die Verantwortlichkeiten zwischen Kunden und Dienstleister entlang der Virtualisierungsgrenzen trennt, so dass für jeden Aspekt nur eine Partei zuständig ist.

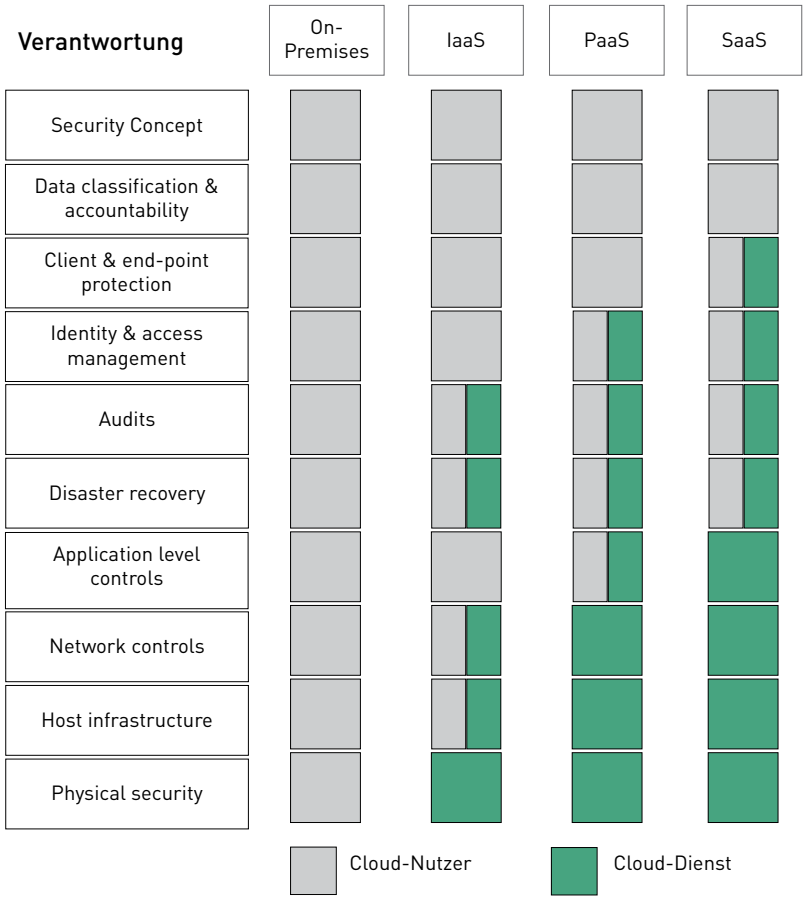

Abbildung 1: Gemeinsame Verantwortung für Sicherheit im Cloud Computing[1]

1.3 Grundlegende Umsetzung des IT-Grundschutz

Dieses Dokument basiert auf der 15. Ergänzungslieferung der IT-Grundschutz-Kataloge (Stand 2016). Seit der 14. Ergänzungslieferung wird die Nutzung von Cloud-Diensten in einem eigenen Baustein abgedeckt: B 1.17 Cloud-Nutzung. Zusammen mit dem Baustein B 5.23 Cloud Management bildet es die Basis für eine geordnete Separierung der Verantwortlichkeiten zwischen Cloud-Kunden und Cloud-Dienstleistern (siehe Abbildung 1).

[1] Vgl. Simorjay, Frank: Shared Responsibilities for Cloud Computing. Ed. Microsoft, März 2016. (https://aka.ms/sharedresponsibility)

Die 14. und 15. Ergänzungslieferung der IT-Grundschutz-Kataloge des BSI und die Entwicklung des Bausteins B 1.17 Cloud-Nutzung haben die Möglichkeit geschaffen, klassisches IT-Outsourcing von der Nutzung von Cloud-Diensten zu trennen. Jede Anforderung der zugrundeliegenden Dienste wird vom Cloud-Kunden als Teil des Bausteins B 1.17 Cloud-Nutzung implementiert.

2 Zertifizierungs-anforderungen

2.1 Vorgehensweise zur IT-Grundschutz-Konformität

Um bei der Nutzung der Cloud-Dienste der Microsoft Cloud Deutschland IT-Grundschutz-konform zu bleiben, müssen diese in das IT-Sicherheitskonzept nach BSI-Standard 100-2 aufgenommen werden. Bei Bedarf muss der Informationsverbund um die Cloud-Dienste erweitert werden.

Die Vorgehensweise hierfür ist wie folgt:

1. Alle einzusetzenden Cloud-Dienste und alle direkt betroffenen oder zusätzlich benötigten Zielobjekte (z. B. Webserver, Netzkomponenten etc.) müssen ermittelt werden. Bei der Strukturanalyse sollten alle Zielobjekte desselben Typs in Zielgruppen zusammengefasst werden, um die Komplexität zu reduzieren.
2. Die Schutzbedarfsfeststellung für jeden Cloud-Dienst wird durch einen Verantwortlichen aus dem Fachbereich ermittelt.
3. Den entsprechenden Zielobjekten sind die entsprechenden IT-Grundschutz-Bausteine und deren jeweilige Maßnahmen zugeordnet. Im Fall einer IaaS-Nutzung sind weitere zusätzliche Bausteine (abhängig von den Cloud-Diensten) anzuwenden, da der Kunde eine höhere Kontrolle über das Zielobjekt ausübt und eine dementsprechend höhere Sicherheitsverantwortung wahrnimmt.
4. In den Basis-Sicherheitschecks (BSCs) werden die bereits vorhandenen Sicherheitsmaßnahmen mit den Vorgaben der Bausteine abgeglichen.
5. Der nächste Schritt betrifft Zielobjekte, für die erhöhte Sicherheitsanforderungen gelten oder für die kein IT-Grundschutz-Baustein exisitert. Für jedes dieser Zielobjekte wird eine ergänzende Sicherheitsanalyse durchgeführt, um festzustellen, ob die vorhanden Risiken durch die bestehenden Maßnahmen abgedeckt sind oder eine zusätzliche Risikoanalyse erforderlich ist.
6. Für die entsprechenden Zielobjekte wird eine Risikoanalyse durchgeführt, in der die Gefährdungen und die daraus resultierenden Risiken identifiziert und ergänzende Maßnahmen festgelegt werden.

2.2 Integration von Microsoft Cloud-Diensten in einen Informationsverbund

Ein hilfreicher Ansatz für die Integration von Cloud-Diensten in den Informationsverbund ist es, diese so zu strukturieren wie eine äquivalente eigene Infrastruktur, welche die Cloud-Dienste ersetzen. Je nach anwendbarem Betriebsmodell fallen verschiedene Schichten (des Grundschutz-Modells) in die Verantwortung des Cloud-Dienstleisters.

Abbildung 2 zeigt ein praktisches Beispiel. Die vom Cloud-Kunden betriebenen Server und Dienste werden hier als „virtuelle Kundeninfrastruktur“ bezeichnet.

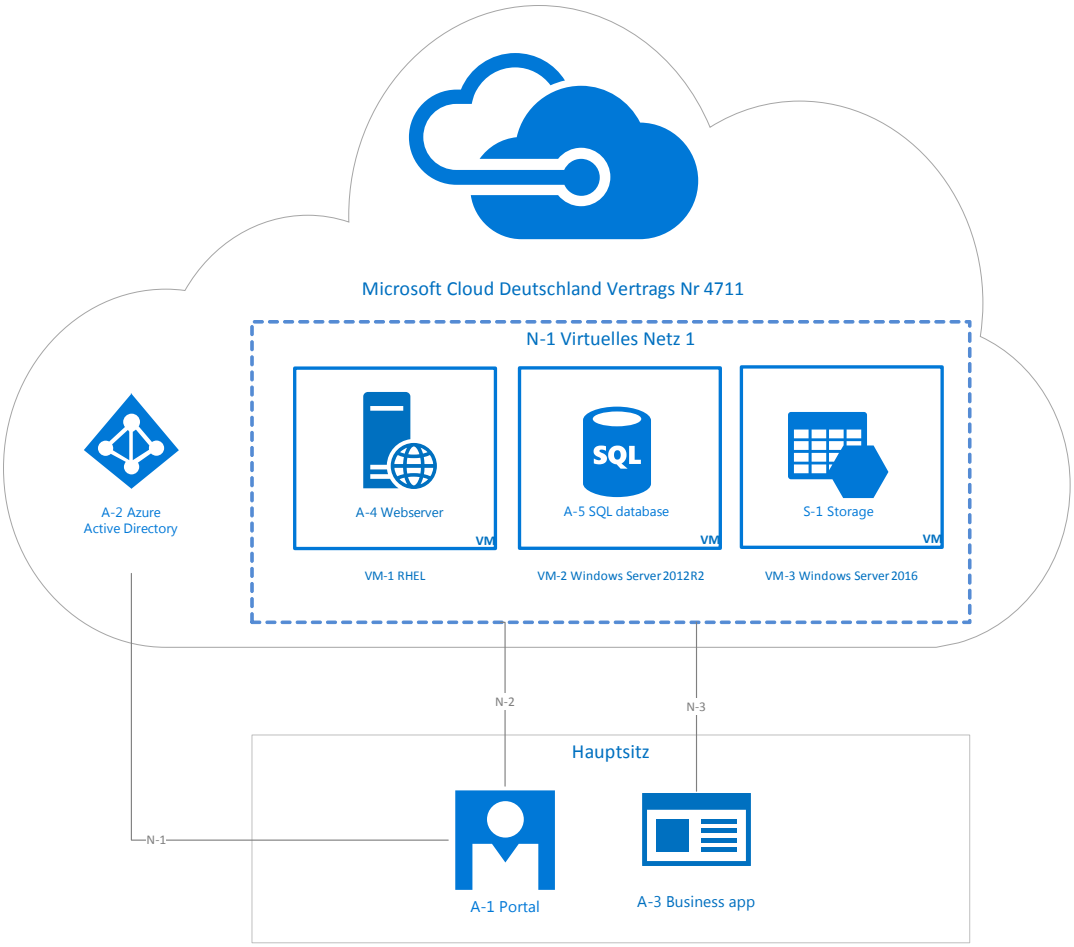

Abbildung 2: Netzplan eines beispielhaften Informationsverbunds nach IT-Grundschutz mit Azure SaaS- und IaaS-Diensten

2.2.1 Einbeziehung der Cloud in die Strukturanalyse

Die IT-Grundschutz-Kataloge verwenden Schichten zur Modellierung von Maßnahmen: Schicht 1 deckt die übergreifenden Aspekte ab, die Schichten 2 bis 4 die „physische Plattform" (Schicht 2 - Infrastruktur, Schicht 3 - IT-Systeme und Schicht 4 - Netze) und Schicht 5 die Anwendungen.

Der Cloud-Nutzer muss lediglich die Anwendungsschicht (Schicht 5) betrachten, wenn die Verwendung von Cloud-Diensten (z. B. das Azure Active Directory-Abonnement) angedacht wird. Die darunter liegenden Schichten 2 (Infrastruktur), 3 (IT-Systeme) und 4 (Netze) werden alle durch Microsoft administriert und kontrolliert und stehen nicht unter der Kontrolle des Cloud-Nutzers.

Die folgenden Objekte müssen in der Strukturanalyse durch den Cloud-Nutzer für jeden Cloud-Dienst berücksichtigt werden:

Schicht	Cloud Infrastruktur	Virtuelle Kunden-infrastruktur IaaS	Virtuelle Kunden-infrastruktur SaaS	Virtuelle Kunden-infrastruktur PaaS
Schicht 1: Übergreifende Aspekte	Baustein B 1.17 Cloud- Nutzung	Standard-modellierung nach IT-Grundschutz	Standard-modellierung nach IT-Grundschutz	Standard-modellierung nach IT-Grundschutz
Schicht 2: Infrastruktur[2]	Nicht relevant für den Cloud-Nutzer	Nicht relevant	Nicht relevant	Nicht relevant
Schicht 3: IT Systeme	Nicht relevant für den Cloud-Nutzer	Standard-modellierung nach IT-Grundschutz	Nicht relevant	Nicht relevant
Schicht 4: Netze	Nicht relevant für den Cloud-Nutzer	Nicht relevant für den Cloud-Nutzer	Nicht relevant	Nicht relevant
Schicht 5: Anwendungen	Nicht relevant für den Cloud-Nutzer	Standard-modellierung nach IT-Grundschutz	Standard-modellierung nach IT-Grundschutz	Standard-modellierung nach IT-Grundschutz

Tabelle 1: Relevante IT-Grundschutz-Schichten für eine Strukturanalyse durch den Cloud-Nutzer

2.2.2 Schutzbedarfsfeststellung für die Cloud-Dienste

Die IT-Grundschutz-Vorgehensweise zur Schutzbedarfsfeststellung basiert auf einem Vererbungsmodell. In diesem Modell wird zunächst der Schutzbedarf für die Anwendungen ermittelt, der sich hinsichtlich der Vertraulichkeit, Integrität und Verfügbarkeit der von ihnen verarbeiteten Daten und der von ihnen unterstützten Geschäftsprozesse ergibt. Der Schutzbedarf wird dann auf die IT-Systeme vererbt, auf denen die Anwendungen laufen und von dort aus auf die Netze, mit denen die IT-Systeme verbunden sind und zu den Orten, an denen sich die IT-Systeme befinden (z. B. Rechenzentren).

Für die virtuelle Kundeninfrastruktur wird die Schutzbedarfsfeststellung nach der IT-Grundschutz-Vorgehensweise vorgenommen. Der Schutzbedarf für jeden Cloud-Dienst wird vergleichbar zu einer Standard-Infrastruktur ermittelt, wobei jeder Dienst auch den Schutzbedarf der darauf laufenden Anwendungen oder IT-Systeme erbt.

[2] Hinweis: Die Schicht „Infrastruktur" bezieht sich auf physische Sicherheitsaspekte in Bezug auf bestimmte Standorte (z. B. Rechenzentren, Bürogebäude), Räume (z. B. Büros, Serverräume) oder Verkabelungen (z. B. elektrotechnische oder IT-Verkabelung).

2.3 Modellierung von Microsoft Cloud Basisdiensten

Die virtuelle Kundeninfrastruktur muss so modelliert werden, wie eine vergleichbare physische oder virtuelle Infrastruktur modelliert werden würde. Dazu gehören virtuelle Server, virtuelle Netze und die Anwendungen. Dabei ist zu beachten, dass der Modellierungsprozess den individuellen Geltungsbereich, die Bedingungen und die Maßnahmen der Cloud-Dienste und Infrastruktur berücksichtigen muss. Daher konzentriert sich dieses Dokument auf die Modellierung der Cloud-Infrastruktur als solche durch den Einsatz des Bausteins B 1.17 Cloud-Nutzung aus den IT-Grundschutz Katalogen.

Der BSI-Standard gibt vor, dass dieses Modul jeweils „auf einen konkreten Cloud Service" verwendet wird, ohne eine Definition für „Cloud Service" bereitzustellen. Dies kann interpretiert werden als „einmal pro Cloud-Dienstleister", einmal pro Dienst-Modell oder sogar sehr feingranular, einmal pro Anwendung. Eine angemessene Lösung oder Interpretation muss erzielt werden.

Wir empfehlen, die individuellen Azure-Dienste im Informationsverbund zu gruppieren, so dass das Modul höchstens einmal pro Dienst-Modell und Dienstleister angewendet wird.

Zur Gruppierung der Azure-Dienste sollten die Gruppierungsanforderungen der IT-Grundschutz-Vorgehensweise (siehe BSI Standard 100-2) beachten werden.[3] Wird beispielsweise das gleiche Servicemodell für interne Anwendungen mit stark unterschiedlichen Schutzbedarfsfeststellungen verwendet, sollte ein feingranularerer Ansatz gewählt werden.

Microsoft Cloud Deutschland Basisdienste	Service Model
Active Directory	SaaS/PaaS[4]
Azure KeyVault	SaaS/PaaS
Azure Portal	SaaS
Cloud Services	PaaS
Service Fabric	PaaS
SQL DB	SaaS/PaaS
Storage	PaaS
Virtual Machine Scale Sets (VMSS)	IaaS
Virtual Machines	IaaS
Virtual Networks	IaaS

Tabelle 2: Modellierung der Microsoft Cloud Deutschland Basisdiensten

[3] Zielobjekte können derselben Gruppe zugeordnet warden, wenn alle Objekte vom gleichen Typ sind, sie in gleicher Weise konfiguriert und in ein Netz integriert werden, dieselben grundlegenden administrativen und ifrasturkturellen Anforderungen erfüllen, ähnliche Anwendungen betreiben und die gleichen Schutzbedarfsfeststellungen enthalten.

[4] Üblicher Weise wird bei der Betrachtung der Servicemodelle SaaS / PaaS die tatsächliche Nutzung berücksichtigt. Obwohl diese Dienste sehr individuell angepasst werden und als Basis für weitere Dienstleistungen genutzt werden können, werden sie häufig im SaaS-Sinne verwendet.

3 Umsetzung des Bausteins B 1.17 Cloud-Nutzung

Im Folgenden wird beschrieben, wie alle prüfrelevanten Maßnahmen aus dem Baustein B 1.17 Cloud-Nutzung[5] für die Microsoft Cloud Deutschland umgesetzt werden können. Jede Maßnahme enthält Fragen zur Überprüfung in Form einer Checkliste; Hinweise auf mögliche Antworten werden – sofern anwendbar – am Ende jeder Maßnahme bereitgestellt.

Während einige der Maßnahmen nur individuell umgesetzt werden können, sind viele der Anforderungen der Maßnahmen bereits durch Standardvorkehrungen der Microsoft Cloud Deutschland abgedeckt bzw. können generisch adressiert werden.

Die folgende Tabelle gibt einen Überblick über die Maßnahmen, bei denen Microsoft mit Informationen unterstützen kann, sowohl hinsichtlich der Umsetzungsdetails als auch bei spezifischen, maßnahmenbezogenen Fragen.

Maßnahme	Unterstützende Informationen von Microsoft verfügbar?	Beschreibung
M 2.40 (A) Rechtzeitige Beteiligung des Personal-/ Betriebsrates	Nein	Diese Maßnahme ist organisationsspezifisch. Microsoft bietet eine detaillierte Beschreibung der einzelnen Cloud-Dienste an, um die Erörterung dieser Maßnahme zu unterstützen.
M 2.42 (A) Festlegung der möglichen Kommunikationspartner	Ja	Microsoft bietet ergänzende Informationen zu relevanten Vertragsbeziehungen (z. B. "ADV-Vereinbarung") sowie Einzelheiten der Daten-Treuhänderrolle der T-Systems Deutschland GmbH.
M 2.534 (A) Erstellung einer Cloud-Nutzungs-Strategie	Ja	Microsoft hat zur Unterstützung der Nutzer bei der Formulierung einer Cloud-Nutzungsstrategie den Leitfaden "Enterprise Cloud-Strategie" bereitgestellt.
M 2.535 (A) Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung	Ja	In diesem Abschnitt werden die Sicherheitsanforderungen und Verfahren von Microsoft Cloud Deutschland dargelegt.

[5] Die Grundschutz-Kataloge umfassen Maßnahmen zu erläuternden Zwecken, die keine Auditrelevanz haben (mit „W" bezeichnet) - diese sind nicht in der Liste enthalten.

Maßnahme	Unterstützende Informationen von Microsoft verfügbar?	Beschreibung
M 2.536 (A) Service-Definition für Cloud-Dienste durch den Anwender	Ja	Diese Maßnahme ist organisationsspezifisch, da sie dazu dient, interne Anforderungen und das erforderliche Schutzniveau in einem Format zu dokumentieren, das einen einfachen Vergleich von Cloud-Dienstleistern ermöglicht.
M 2.537 (A) Planung der sicheren Migration zu einem Cloud Service	Ja	Microsoft hat zur Unterstützung der Nutzer bei der Migration auf die Cloud-Infrastruktur den Leitfaden "Enterprise Cloud-Strategie" bereitgestellt.
M 2.538 (A) Planung der sicheren Einbindung von Cloud Services	Nein	Dieser Maßnahme ist organisationsspezifisch, da sie die interne Planung für die sichere Einbindung bestehender Dienste beinhaltet.
M 2.539 (A) Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung	Ja	Obwohl es keine generische Vorlage für die spezifischen Anforderungen jedes Unternehmens gibt, werden seitens Microsoft Cloud Deutschland hier die meisten technischen Bedrohungen mittels entsprechender Gegenmaßhnahmen adressiert.
M 4.459 (Z) Einsatz von Verschlüsselung bei Cloud-Nutzung	Ja	Microsoft Cloud Deutschland hat eine Vielzahl von Informationen zur Verschlüsselung bereitgestellt, wo sie standardmäßig angewendet wird und welche Verschlüsselungsoptionen dem Endnutzer zur Verfügung stehen.
M 4.461 (Z) Portabilität von Cloud Services	Ja	Für jeden Dienst, der im Kapitel 2.3 Modellierung von Microsoft Cloud Basisdiensten aufgeführt ist, werden auch die Fragestellungen zur Portabilität thematisiert.
M 2.540 (A) Sorgfältige Auswahl eines Cloud-Diensteanbieters	Ja	Informationen zum Vergleich von Cloud-Dienstleistern finden Sie im Microsoft Online Subscription-Programm.
M 2.541 (A) Vertragsgestaltung mit dem Cloud-Diensteanbieter	Ja	Detaillierte Informationen zu den Standardsicherheitsanforderungen von Microsoft Cloud Deutschland finden Sie in dieser Maßnahme.
M 2.542 (A) Sichere Migration zu einem Cloud Service	Ja	Diese Maßnahme ist organisationsspezifisch und deckt die interne Planung für die sichere Integration bestehender Dienste ab. Microsoft stellt unterstützende Werkzeuge bereit, um vorhandene Ressourcen nach Azure zu migrieren.

Maßnahme	Unterstützende Informationen von Microsoft verfügbar?	Beschreibung
M 2.543 (A) Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb	Ja	Bereitstellung von Informationen zur Aufrechterhaltung eines hohen Niveaus der Informationssicherheit und über Methoden, mit denen der Nutzer die geforderten Ansprüche testen kann.
M 2.544 (C) Auditierung bei Cloud-Nutzung	Ja	Informationen und Anleitungen zu aktuellen und vergangenen Audits und Sicherheitszertifikaten werden bereitgestellt, einschließlich öffentlich verfügbarer Berichte und Ergebnisse, sodass der Kunde keine eigene Prüfung durchführen muss.
M 4.460 (Z) Einsatz von Federation Services	Ja	Verbunddienste mit eigenen Sicherheitsanforderungen werden über den Microsoft Cloud Deutschland Dienst Azure Active Directory bereitgestellt.
M 2.307 (A) Geordnete Beendigung eines Outsourcing- oder Cloud-Nutzungs-Verhältnisses	Ja	Informationen und Anleitungen zur Beendigung eines Microsoft Cloud Deutschland-Abonnements werden bereitgestellt, einschließlich der Richtlinien zur Kündigung und Datenvernichtung.
M 6.155 (A) Erstellung eines Notfallkonzeptes für einen Cloud Service	Ja	Das Notfallkonzept muss für jeden Cloud-Dienst individuell entwickelt werden. Dennoch werden allgemeine Richtlinien genannt.
M 6.156 (Z) Durchführung eigener Datensicherungen	Nein	Dies muss von Ihrer Organisation initiiert werden; entweder durch sie selbst oder durch einen anderen, unabhängigen Dienst.

3.1 M 2.40 (A) Rechtzeitige Beteiligung des Personal-/Betriebsrates

Diese Maßnahme fordert die Zustimmung der Arbeitnehmervertreter / des Betriebsrats zu allen Maßnahmen, welche eine Überwachung des Verhaltens oder der Leistung der Arbeitnehmer ermöglichen.

Dieser Maßnahme ist organisationsspezifisch. Microsoft bietet eine detaillierte Beschreibung aller Cloud-Dienste an, um die Abstimmung dieser Maßnahme zu unterstützen.

3.2 M 2.42 (A) Festlegung der möglichen Kommunikationspartner

Diese Maßnahme zielt darauf ab, vollständige Transparenz über alle (externen) Dritten zu gewährleisten, die Zugriff auf die Kundendaten haben. Sie ist in erster Linie aus Datenschutzgründen, insbesondere aufgrund der Bestimmungen des Bundesdatenschutzgesetzes (BDSG) und anderer anwendbarer Datenschutzregelungen (EU, Bundesländer), erforderlich.

Der Umfang dieser Maßnahme hängt weitgehend von der Art der Daten ab, die in der Cloud gespeichert werden oder auf die von der Cloud aus zugegriffen werden kann. Der Kunde muss den Schutzbedarf der Daten bereits festgestellt haben, d.h. er hat:

1. Eine Vertraulichkeitsklassifikation der besagten Daten.
2. Eine Liste der Personen, welche die Informationen erhalten dürfen.

Die Microsoft Cloud Deutschland nutzt eine besondere Konstruktion für alle in der Microsoft Cloud Deutschland gespeicherten Daten – die des „Datentreuhänders".

- Alle Zugriffe auf Kundendaten (mit Ausnahme der vom Kunden selbst oder durch seine Endkunden initiierten Zugriffe) werden durch den deutschen Datentreuhänder kontrolliert und überwacht. Der Datentreuhänder ist die T-Systems International GmbH (TSI), ein in Deutschland ansässiger, weltweit führender Dienstleister für IT- und Kommunikationstechnologien und eine 100% Tochtergesellschaft der Deutsche Telekom AG.
- Bei Anfragen nach Daten durch ausländische Behörden oder Gerichtsbeschlüsse werden Kundendaten durch das Datentreuhänder-Modell geschützt. Der Datentreuhänder (TSI) ist nach deutschem Recht tätig und gewährt Dritten den Zugriff auf Kundendaten nur nach ausdrücklicher Zustimmung des Kunden oder wenn geltendes deutsches Recht dies erfordert.
- Jeglicher Zugriff auf Kundendaten durch Microsoft-Mitarbeiter oder Dritte wird durch den Datentreuhänder geprüft und überwacht und wird nur im Einklang mit deutschem Recht oder nach Erlaubnis durch den Kunden gewährt.
- Erlaubter externer Zugriff wird auf das zur Lösung des vorliegenden Problems notwendige Minimum beschränkt.

Die Liste von autorisierten Dritten mit Zugang zu den Daten kann aus den AGBs „Ergänzende Bestimmungen für Onlinedienste für Deutsche Onlinedienste, Zusatzvereinbarung ID M370" entnommen werden. Diese sind Bestandteil der vertraglichen Vereinbarung zwischen Microsoft und dem Datentreuhänder.

Es gibt nur zwei relevante Situationen, in denen ein Zugriff durch Microsoft-Personal auftreten kann:

1. Wenn der Datentreuhänder Microsoft Zugang gewährt, um kurzfristig operationelle Problemfälle zu lösen oder bei einer Kundendienstanfrage an den Datentreuhänder. In diesem Fall wird der Zugriff durch den Datentreuhänder überwacht und auf das notwendige Minimum begrenzt, das erforderlich ist, um das vorhandene Problem zu lösen.
2. Wenn der Kunde Daten direkt an den Microsoft-Kundensupport sendet (z. B. per E-Mail bei einer Support-Anfrage oder bei Freigabe des Bildschirms).

Die vollständige Liste aller für diesen Datenzugriff in Frage kommenden juristischen Personen ist in der "Microsoft Services Supplier List" dokumentiert.[6]

Das oben genannte gilt natürlich nur für gespeicherte Informationen ohne vom Kunden selbst zugelassene externe Zugriffe. Bei der Implementierung von Diensten, die andere Zugriffsformen zulassen, muss diese Liste um die vom Kunden selbst zugelassenen Dritten erweitert werden.

[6] https://www.microsoft.com/en-us/download/details.aspx?id=50426

Review-Frage	Antwort	Referenz
Ist festgelegt, welche Kommunikationspartner welche Informationen erhalten dürfen?	Die Auftragsdatenverarbeitungs-Vereinbarung mit dem Datentreuhänder beschränkt Zugriffe auf die Daten auf den Datentreuhänder und Personal wie oben beschrieben. Jeder weitere Zugriff durch Dritte muss durch ihre Organisation selbst erlaubt und entsprechend dokumentiert werden.	Ergänzende Bestimmungen für Onlinedienste für Deutsche Onlinedienste, Zusatzvereinbarung ID M370.

3.3 M 2.534 (A) Erstellung einer Cloud-Nutzungs-Strategie

Diese Maßnahme dient der frühzeitigen Planung vor, wie die Cloud-Dienste verwendet werden sollen als auch die Identifizierung von Herausforderungen für das Sicherheitsmodell im Voraus.

Sie umfasst die Strategie, die Schnittstellen, die Vernetzung, die Administrationsmodelle und die Datenverwaltung.

Microsoft hat einen Leitfaden zur allgemeinen Unterstützung bei der Erstellung einer Cloud-Nutzungsstrategie erstellt, der wichtige Fragen beantwortet und Empfehlungen auf der Basis von Erfahrungen in den Bereichen Cloud-Strategie, Cloud-Services-Modelle und Sicherheitserwägungen bereitstellt.[7]

Beachten Sie, dass der Umfang der Planung zwangsläufig von den spezifischen Anforderungen der Dienste abhängt, die in die Cloud portiert oder dort implementiert werden.

Für den Abgleich Ihrer Anforderungen mit den Microsoft Cloud Deutschland-Angeboten finden sie im Anhang A und in diesem Abschnitt Referenzinformationen.

3.4 M 2.535 (A) Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung

Diese Maßnahme dient der eindeutigen Definition und einheitlichen Umsetzung der Sicherheitsstandards für die Cloud. Sie umfasst zwei Bereiche: Sicherheitsanforderungen an die eigene Organisation und Sicherheitsanforderungen an den Cloud-Dienstleister. Um alle essentiellen Bereiche abzudecken, müssen organisatorische, technische und rechtliche Erwägungen berücksichtigt werden.

Sicherheitsanforderungen an die eigene Organisation

Dies sind Anforderungen, die von ihnen umgesetzt werden sollten, um Daten und Prozesse in der Cloud zu schützen, z. B. Verschlüsselung hochsensibler Daten vor der Übertragung oder die Erstellung von lokalen Sicherungen oder Offline-Caches für hochverfügbare Informationen. Diese Maßnahmen sollten im Sicherheitskonzept dokumentiert werden (siehe 3.8 M 2.539 (A) Erstellen eines Sicherheitskonzepts für Cloud-Nutzung).

[7] https://info.microsoft.com/enterprise-cloud-strategy-ebook.html

Sicherheitsanforderungen an den Cloud-Dienstleister

Hierbei sollten die Anforderungen dokumentiert werden, welche bei der Auswahl eines Cloud-Dienstleisters überprüft werden sollen. Zu berücksichtigende Punkte beinhalten die geografische Lage, Verfügbarkeitszusagen und SLAs, die Verwendung von Dritt-Personal und ob andere organisatorische Sicherheitsanforderungen oder Zertifizierungen erforderlich sind.

Datenzugriff und Datenschutzprobleme

Microsoft setzt für die Microsoft Cloud Deutschland die folgenden hier relevanten Maßnahmen um:

- Der Speicherort der Daten ist Deutschland.
- Der Zugriff auf Kundendaten (mit Ausnahme der vom Kunden oder dessen Endkunden initiierten Zugänge) wird durch den deutschen Datentreuhänder kontrolliert.
  Diese Einschränkung adressiert speziell die Gewährung des Zugangs ausschließlich nach deutschem bzw. EU-Recht durch deutsche Gerichte und beinhaltet auch den Zugriff durch Microsoft selbst.
- Der Kunde schließt einen Vertrag zur Auftragsdatenverarbeitung mit dem deutschen Datentreuhänder ab, der die Nutzung der Kundendaten auf die für die Bereitstellung der Cloud-Dienste notwendigen Zwecke limitiert.

Verfügbarkeit

Die angebotenen Verfügbarkeitsanforderungen und Service-Level sind abhängig von der verwendeten Dienstleistung. Im Allgemeinen garantiert Microsoft aber eine Verfügbarkeit von 99,5 oder 99,9% pro Monat mit unterschiedlichen Arten von Gutschriften, falls dies nicht erreichen werden sollte.

Sofern höhere Absicherung notwendig ist, sollte dies durch die Verwendung eigener technischer Maßnahmen zur Bereitstellung von Fallback- oder Ersatzdiensten sichergestellt werden.

Spezifische Absicherungen und Konformität

Microsoft Azure verfügt diverse sicherheitsbezogener Zertifizierungen für ausgewählte Dienste, z. B.:

- ISO/IEC 27018 (Anwendungsregel für den Schutz von Personenbezogenen Daten (PII) in Public Clouds, die als PII Processor auftreten)
- ISO/IEC 27001 (Informationssicherheits-Managementsysteme)
- PCI-DSS (Payment Card Industry Data Security Standard)
- SOC 1 - SOC 2 - SOC 3 (SSAE16 / ISAE 3402)

Microsoft beabsichtigt, diese Zertifizierungen für Microsoft Azure Deutschland nach der Umsetzung der allgemeinen Verfügbarkeit zu erlangen, die ISO/IEC 27001 und ISO/IEC 27018 Zertifizierungen liegen bereits vor. Spezifische Maßnahmen oder Anforderungen können den verpflichtenden Maßnahmen in diesen Standards zugeordnet werden. Weitere Informationen finden sich in Kapitel 4 (Microsofts Verpflichtungen als Cloud-Dienstanbieter).

Weitere relevante Absicherungen sind verfügbar in:

- "Ergänzende Bestimmungen für Onlinedienste für Deutsche Onlinedienste, Zusatzvereinbarung ID M370" (Vereinbarung zur Auftragsdatenverarbeitung)

- Vereinbarungen zum Servicelevel für Microsoft-Onlinedienste: OnlineSvcsConsolidatedSLA(WW)(Deutsch) (January2017)[8]
- Vereinbarungen zum Servicelevel (SLAs) für Azure-Dienste: https://azure.microsoft.com/de-de/support/legal/sla/
- Die Liste der Zertifizierungen für Microsoft Azure finden Sie unter: https://www.microsoft.com/de-de/TrustCenter/Compliance?service=Azure#Icons

Prüffrage	Antwort
Beinhaltet die Sicherheitsrichtlinie konkrete und ausreichend detaillierte Sicherheitsvorgaben für die Umsetzung innerhalb der Institution?	Die Sicherheitsrichtline muss individuell für jede Organisation festgelegt werden (siehe oben, "Sicherheitsanforderungen an die eigene Organisation").
Sind spezifische Sicherheitsanforderungen an den Cloud-Diensteanbieter dokumentiert?	Dies sind Ihre eigenen Anforderungen, aber siehe oben "Sicherheitsanforderungen an den Cloud-Dienstanbieter" für spezifische Absicherungen seitens der Microsoft Cloud Deutschland.
Ist der festgelegte Schutzbedarf für den Einsatz von Cloud Services hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit dokumentiert?	Dies sind Ihre eigenen Anforderungen, aber siehe oben "Sicherheitsanforderungen an den Cloud-Dienstanbieter" für spezifische Absicherungen seitens der Microsoft Cloud Deutschland.
Sind länderspezifische Anforderungen beziehungsweise gesetzliche Bestimmungen bei Nutzung von Cloud Services internationaler Cloud-Diensteanbieter bekannt?	Dies bezieht sich explizit auf konkurrierende Rechtsrahmen für internationale Dienstleister; diese Fragestellung ist aufgrund der Realisierung durch den deutschen Datentreuhänder irrelevant (siehe Abschnitt 3.2 „M 2.42 (A) Festlegung der möglichen Kommunikationspartner“ für eine ausführliche Erläuterung).

3.5 M 2.536 (A) Service-Definition für Cloud-Dienste durch den Anwender

Diese Maßnahme fordert von ihrer Organisation, die gewünschten Cloud-Dienste in Bezug auf ihre geschäftliche Auswirkung zu definieren – und schlägt vor, dafür die Form sogenannter Service Templates nach ITIL zu wählen.

Diese Maßnahme ist organisationsspezifisch, da sie dazu dient, interne Anforderungen und erforderliche Absicherungen in einem Format zu dokumentieren, das eine Vergleichbarkeit von Cloud-Dienstleistern ermöglicht.

Des Weiteren enthält diese Maßnahme zusätzliche praktische Anforderungen, für die folgende Informationen verfügbar sind:

[8] http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=37

Konformitäts-anforderungen	Implementierung bei Microsoft Cloud Deutschland	Referenz
Auswahl sicherer Authentisierungsmethoden, Zwei-Faktor-Authentisierung für Administration	Zur Steuerung von Cloud-Diensten über das Azure Portal steht eine rollenbasierte Zugriffskontrolle zur Verfügung. Für ein sicheres, weitreichendes Identitäts- und Berechtigungs-managementsystem bietet Microsoft je nach anstehenden Anforderungen unterschiedliche Optionen von Active Directory Diensten (Azure Active Directory, Azure Active Directory B2C) an. Ein Abonnement der Microsoft Cloud Dienste Multi-Factor-Authentisierung ermöglicht die Verwendung von Multifaktor-Authentisierung.	https://azure.microsoft.com/de-de/features/azure-portal/ https://azure.microsoft.com/de-de/services/multi-factor-authentication/ https://azure.microsoft.com/de-de/services/active-directory/ https://azure.microsoft.com/de-de/services/active-directory-b2c/
Verschlüsselungsanforderungen	Die Microsoft Cloud Deutschland bietet Verschlüsselung in Verbindung mit einer Vielzahl von Cloud-Diensten. Der Cloud Dienst Virtual Network ermöglicht die Realisierung einer sicheren, isolierten Umgebung mit einem dedizierten DNS-Server. Eine sichere Verbindung kann mit einem IPSec VPN oder dem ExpressRoute Cloud Dienst aufgebaut werden.	Ergänzende Bestimmungen für Onlinedienste für Deutsche Onlinedienste, Zusatzvereinbarung ID M370 https://www.microsoft.com/de-de/TrustCenter/Security/Encryption https://azure.microsoft.com/de-de/documentation/articles/storage-service-encryption/ https://blogs.msdn.microsoft.com/azure-security/2015/05/11/azure-disk-encryption-management-for-windows-and-linux-virtual-machines/ https://azure.microsoft.com/de-de/services/virtual-network/ https://azure.microsoft.com/de-de/services/expressroute/
Interoperabilität der Client-Software	Entwickler-Werkzeuge und SDKs stehen für eine Vielzahl von Programmiersprachen und Plattformen zur Verfügung, welche die Integration und Entwicklung sowie die Administration von Microsoft-Cloud-Deutschland-Dienstabonnements vereinfachen.	https://azure.microsoft.com/de-de/tools/

3.6 M 2.537 (A) Planung der sicheren Migration zu einem Cloud Service

Der Übergang (von Teilen) des IT-Betriebs zur Cloud-Nutzung erfordert eine sorgfältige Konzeption und Planung, welche als Teil des übergeordneten Sicherheitskonzeptes gesehen werden muss.

Die organisatorischen Vereinbarungen, Verantwortlichkeiten und Prozesse rund um die Migration sowie adäquate Test- und Übergabeverfahren sind im Rahmen dieser Maßnahme zu ermitteln. Dies geht einher mit einer Überprüfung der Umsetzung aller bereits bestehenden Vereinbarungen. Sowohl die verbleibende eigene IT-Infrastruktur als auch die aktuellen Arbeitsprozesse müssen überprüft werden, um festzustellen, ob sie für die Nutzung von Cloud-Diensten angepasst werden müssen.

Microsoft bietet ein umfassendes Handbuch an[9], das sie bei der Migrationsplanung unterstützt. Der Leitfaden kombiniert Antworten auf wichtige Fragen und Empfehlungen auf der Basis von Erfahrungen für die Migration in eine Cloud. Ein zusätzliches Handbuch, das die Migration von SQL Server-Datenbanken abdeckt, ist ebenfalls verfügbar.[10]

3.7 M 2.538 (A) Planung der sicheren Einbindung von Cloud Services

Diese Maßnahme soll sicherzustellen, dass notwendige Änderungen für die Einführung von Cloud-Diensten frühzeitig erkannt und entsprechend geplant werden können.

- Schnittstellensysteme (Load-Balancer, Proxies, Router, sichere Gateways etc.):
  - Bestehende Systeme müssen geeignete Interoperabilität, Effizienz, Performanz und Durchsatzleistung leisten und eine akzeptable Redundanz für die Nutzung des Cloud-Dienstes bieten. Alternativ können auch neue Systeme beschafft werden.
  - Wenn eine API für die Anbindung verwendet wird, können weitere Sicherheitsmaßnahmen (B 5.24 Web-Services) erforderlich werden.
- Anpassung der Netzanbindung:
  Die für die Nutzung des Cloud-Dienstes genutzte Netzanbindung muss genügend Bandbreite bereitstellen, um die Anforderungen des Dienstes zu erfüllen. Abhängig vom Schutzbedarf der Systeme können redundante Anbindungen oder andere zusätzliche Maßnahmen angebracht bzw. erforderlich sein.
- Anpassung des Administrationsmodells:
  Für die Administration und Nutzung des Cloud-Dienstes muss ein rollenbasiertes Berechtigungsmodell angewendet oder neu erstellt werden.
- Anpassung des Datenmanagementmodells:
  Für die in der Cloud gespeicherten Daten muss eine angemessene Datensicherungs- und Datenaufbewahrungsstrategie entwickelt werden.

Dieser Maßnahme ist organisationsspezifisch, da sie die interne Planung für die sichere Integration bestehender Dienste abdeckt.

[9] https://info.microsoft.com/enterprise-cloud-strategy-ebook.html

[10] https://blogs.msdn.microsoft.com/microsoft_press/2016/05/11/free-ebook-microsoft-azure-essentials-migrating-sql-server-databases-to-azure/

3.8 M 2.539 (A) Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung

Diese Maßnahme beinhaltet die Erstellung eines Sicherheitskonzepts für jeden modellierten Cloud-Dienst, einschließlich aller erforderlichen Sicherheitsmaßnahmen für dessen Verwendung. Diese Maßnahmen werden aus den Anforderungen der Sicherheitsrichtlinie für den Cloud-Dienst abgeleitet. Darüber hinaus legt das Sicherheitskonzept die jeweilige Konfiguration (Cloud-Nutzer, Cloud-Dienstanbieter, Internet-Dienstanbieter, etc.) und das Bedrohungsmodell fest, gegen das die konkreten Maßnahmen entwickelt werden.

Obwohl es keine allgemeine Vorlage für ein solches Sicherheitskonzept gibt, adressiert die Microsoft Cloud Deutschland die meisten konkreten technischen Bedrohungen und Reduktionsmaßnahmen, die in der Maßnahme erwähnt werden:

Bedrohung	Verfügbare Reduktionsmaßnahmen	Referenz
Fehlende Portabilität von Daten und Systemen Verwendung von proprietären Datenformaten	Viele Dienste auf Azure haben eine vergleichbare Konfiguration wie eine eigene Infrastruktur; die meisten von ihnen verwenden dabei Standardformate, z. B.: - Azure Virtuelle Maschinen können zu Hyper-V zurück übertragen werden - Azure SQL-Dienste können zu einem eigenen Microsoft SQL-Server zurück migriert werden	https://blogs.technet.microsoft.com/cbernier/2014/01/27/move-vms-between-hyper-v-and-windows-azure/ https://azure.microsoft.com/de-de/documentation/articles/sql-database-copy/
Fehlende Kenntnis über den Speicherort von Informationen	Die Microsoft Cloud Deutschland speichert Daten ausschließlich in deutschen Rechenzentren	Siehe 3.2 M 2.42 (A) Festlegung der möglichen Kommunikationspartner
Unbefugter Zugriff auf Informationen, zum Beispiel durch Administratoren des Cloud-Diensteanbieters oder Dritte	Datentreuhänder-Modell	Siehe 3.4 M 2.535 (A) Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung
Regelungen zur Überwachung der Service-Erbringung und zum Berichtswesen	SLA-Überwachung durch das Modul "Service Health" in der Portalanwendung	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/

Bedrohung	Verfügbare Reduktionsmaßnahmen	Referenz
Unbefugter Zugriff durch Dritte (Verschlüsselung der Informationen)	Data-at-Rest-Verschlüsselung ist optional verfügbar	Siehe 3.9 M 4.459 (Z) Einsatz von Verschlüsselung bei Cloud-Nutzung
Unbefugter Zugriff durch Dritte (Verschlüsselung der Informationen)	Data-in-transit-Verschlüsselung	Siehe 3.9 M 4.459 (Z) Einsatz von Verschlüsselung bei Cloud-Nutzung
Isolierung/Mandantentrennung	Die Umgebung jedes Cloud-Nutzers wird von den anderen isoliert. Die entsprechenden Technologien und Prozesse (z. B. Hypervisor-Isolation, Root-OS, Gast-VMs und Netzisolation) hängen vom jeweiligen Cloud-Dienst ab.	https://azure.microsoft.com/de-de/blog/new-windows-azure-security-overview-white-paper-now-available/ https://azure.microsoft.com/de-de/blog/microsoft-azure-network-security-whitepaper-version-3-is-now-available/

Prüffrage	Antwort
Hat der Netzanbieter ein Sicherheitskonzept nach den geltenden Richtlinien und Standards erstellt?	Das Sicherheitskonzept der Microsoft Cloud Deutschland erfüllt eine Vielzahl von Sicherheitsstandards. Weitere Informationen hierzu sind im Abschnitt 3.4 M 2.535 (A) Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung.
Wurde das Vorhandensein und die Implementierung des Sicherheitskonzeptes vom Cloud-Dienstleister oder von einem unabhängigen Dritten überprüft?	Microsoft Azure und die Microsoft Cloud Deutschland werden bedingt durch die Anforderungen mehrerer Konformitätsstandards und Zertifizierungen kontinuierlich auditiert. Informationen und Anleitungen zu laufenden und abgeschlossenen Audits und Sicherheitszertifikaten werden einschließlich der öffentlich verfügbaren Berichte und Ergebnisse bereitgestellt.

3.9 M 4.459 (Z) Einsatz von Verschlüsselung bei Cloud-Nutzung

Diese Zusatz-Maßnahme soll bei erhöhten Schutzbedarf gewährleisten, dass eine geeignete Verschlüsselung genutzt wird, um Daten sowohl bei der Übermittlung als auch bei der Speicherung zu schützen. Abhängig von der Verschlüsselungsmethode kann die Verantwortung entweder beim Kunden oder beim Cloud-Dienstleister liegen. Wenn der Cloud-Dienstleister für die Verschlüsselung verantwortlich ist, sollte der bereitgestellte Verschlüsselungsdienst mit den in der Servicedefinition festgelegten Standards abgeglichen werden.

Die Microsoft Cloud Deutschland verwendet bereits standardmäßig Verschlüsselung in vielen verschiede-

nen Bereichen. Der Cloud-Nutzer hat die Möglichkeit, die Verschlüsselung der einzelnen Cloud-Dienste zu aktivieren bzw. individuelle Verschlüsselungseinstellungen zu nutzen.[11]

Prüffrage	Antwort	Referenz
Existieren bei Verschlüsselung durch den Cloud-Diensteanbieter vertragliche Regelungen, die diesem Vorgaben zur Auswahl sicherer Verschlüsselungsmechanismen und zum Einsatz geeigneter Schlüssellängen machen?	Microsoft bietet Verschlüsselung in Verbindung mit einer Reihe von Cloud-Diensten an. Beispielsweise beinhaltet Azure Storage die Azure Storage Service Encryption (SSE) -Funktionalität, welche Daten verschlüsselt, wenn diese auf dem Cloud-Speichersystem abgelegt werden. Mit Key Vault ist es außerdem möglich, die virtuellen Festplatten von cloudbasierten Windows- und Linux-VMs zu verschlüsseln.	https://www.microsoft.com/de-de/TrustCenter/Security/Encryption https://azure.microsoft.com/de-de/services/key-vault/ https://azure.microsoft.com/de-de/documentation/articles/storage-security-guide/ https://azure.microsoft.com/de-de/documentation/articles/storage-service-encryption/ https://blogs.msdn.microsoft.com/azuresecurity/2015/05/11/azure-disk-encryption-management-for-windows-and-linux-virtual-machines/ https://azure.microsoft.com/de-de/services/key-vault/ https://azure.microsoft.com/de-de/documentation/articles/expressroute-introduction/ https://azure.microsoft.com/de-de/services/virtual-machines/security/
Wird beim Einsatz eigener Verschlüsselungs-mechanismen die Umsetzung eines geeigneten Schlüsselmanagements sichergestellt?	Diese Anforderung liegt in der Verantwortung des Cloud-Nutzers. Microsoft Azure bietet ein sicheres Key-Management sowie die sichere Speicherung von Schlüsseln für mit dem Cloud-Dienst Key Vault an, der die Schlüssel für andere Cloud-Dienste verwalten kann.	https://azure.microsoft.com/de-de/services/key-vault/
Werden Besonderheiten der Cloud-Nutzung hinsichtlich des gewählten Service-Modells bei der Umsetzung von Verschlüsselung berücksichtigt?	Diese Anforderung liegt in der Verantwortung des Cloud-Nutzers. Die verwendete Verschlüsselung sollte gegen mutmaßliche Angriffsszenarien helfen - z. B. hilft eine Data-at-rest-Verschlüsselung für eine Datenbank nicht gegen Online-Angriffe mittels SQL-Injektion.	

[11] Detaillierte Informationen unter https://www.microsoft.com/de-de/TrustCenter/Security/Encryption

3.10 M 4.461 (Z) Portabilität von Cloud Services

Diese zusätzliche Maßnahme zielt darauf ab, ein hohes Maß an Flexibilität beim Wechseln des Cloud-Dienstleisters zu gewährleisten oder um einen Cloud-Dienst in die eigene IT-Infrastruktur zurück zu potieren. In diesem Fall sind einige Anforderungen, insbesondere an Dateiformate und Portabilitätstests, zu berücksichtigen.

Microsoft hat seine Absichtserklärung zur Interoperabilität und Portabilität veröffentlicht.[12] Die Cloud Dienste API Management und die Cloud-Dienste nutzen Standardformate und bieten eine Vielzahl von unterschiedlichen Verbindungsmethoden.

Weitere Aspekte zur Portabilität sind in der folgenden Tabelle aufgeführt:

Cloud-Dienst	Portabilität	Referenz
Azure Active Directory	Die Verwendung von Azure Active Directory ermöglicht die Nutzung von Single-Sign-On über tausende von Cloud-SaaS-Anwendungen. Mit Azure AD Connect können lokale Profile in Azure Active Directory integriert und über die Cloud synchronisiert werden.	https://azure.microsoft.com/de-de/services/active-directory/ https://azure.microsoft.com/de-de/documentation/articles/active-directory-whatis/ https://azure.microsoft.com/de-de/documentation/articles/active-directory-aadconnect/
Azure KeyVault	Key Vault ist ein Cloud-Dienst zur sicheren Verwaltung von Geheimnissen auf der Microsoft Cloud Deutschland. Portabilität ist nicht vorgesehen.	https://azure.microsoft.com/de-de/services/key-vault/
Azure Portal	Azure Portal ist eine von Microsoft bereitgestellte Webanwendung. Portabilitität wird nicht berücksichtigt.	https://azure.microsoft.com/de-de/features/azure-portal/
Cloud Services	Cloud Services ist eine Plattform zur Entwicklung und Bereitstellung eigener Cloud-Dienste und Anwendungen. Portabilitität wird nicht berücksichtigt.	https://azure.microsoft.com/de-de/services/cloud-services/
Service Fabric	Service Fabric ist eine Plattform zur Entwicklung und Bereitstellung von Mikroservice-basierten Anwendungen und die Verwaltung ihres Lebenszyklus. Portabilitität wird nicht berücksichtigt.	https://azure.microsoft.com/de-de/services/service-fabric/

[12] Microsoft Azure Responses to Cloud Security Alliance Consensus Assessments Initiative Questionnaire v3.0.1 (Version 1, Veröffentlicht März 2016): Interoperability and Portability: Controls IPY-01 through IPY-05, https://gallery.technet.microsoft.com/Azure-Responses-to-CSA-46034a11

Cloud-Dienst	Portabilität	Referenz
SQL DB	Die Azure SQL-Datenbanken können kopiert und einfach in anderen Umgebungen bereitgestellt werden.	https://azure.microsoft.com/de-de/services/sql-database/ https://azure.microsoft.com/de-de/documentation/articles/sql-database-copy/
Storage	Azure Storage ermöglicht Kunden, Daten zu im- und exportieren.	https://azure.microsoft.com/de-de/services/storage/ https://azure.microsoft.com/de-de/documentation/articles/storage-import-export-service/#wann-sollte-der-importexport-dienst-von-azure-verwendet-werden
Virtual Machine Scale Sets (VMSS)	VMSS ist ein Cloud-Dienst zur Skalierung von virtuellen Maschinen in der Microsoft Cloud Deutschland. Portabilität ist nicht vorgesehen.	https://azure.microsoft.com/de-de/services/virtual-machine-scale-sets/
Virtual Machines	Microsoft bietet das „Virtual Machine Readiness Assessment“ Werkzeug an, das physische oder virtuelle Umgebungen überprüft und einen umfangreichen Bericht mit den erforderlichen Schritten für eine Migration zur Microsoft Cloud Deutschland erstellt. Darüber hinaus bietet Microsoft das „Virtual Machine Optimization Assessment Tool“ an, um die Performance von VMs zu optimieren (z. B. nach der Migration in die Cloud)	https://azure.microsoft.com/de-de/services/virtual-machines/ https://azure.microsoft.com/de-de/downloads/vm-readiness-assessment/ https://azure.microsoft.com/de-de/downloads/vm-optimization-assessment/
Virtual Networks	Azure Virtual Network bietet eine isolierte, sichere Umgebung für virtuelle Maschinen und Anwendungen an. Portabilitität wird nicht berücksichtigt.	https://azure.microsoft.com/de-de/services/virtual-network/

Prüffrage	Antwort	Referenz
Wurden alle wichtigen Anforderungen für den Wechsel des Cloud-Diensteanbieters oder die Rückholung in die eigene IT definiert?	Diese Anforderung liegt in der Verantwortung des Cloud-Nutzers.	

Prüffrage	Antwort	Referenz
Ist die Durchführung von Portabilitätstests vorgesehen?	Diese Anforderung liegt in der Verantwortung des Cloud-Nutzers. Microsoft bietet das „Virtual Machine Readiness Assessment" Werkzeug an, das physische oder virtuelle Umgebungen überprüft und einen umfangreichen Bericht mit den erforderlichen Schritten für eine Migration zur Microsoft Cloud Deutschland erstellt.	https://azure.microsoft.com/de-de/downloads/vm-readiness-assessment/
Sind Vorgaben zur Realisierung der Portabilität in die Vertragsgestaltung mit dem Cloud-Diensteanbieter eingeflossen?	Portabilität ist nicht vertraglich geregelt, Microsoft hat aber viele Vorkehrungen getroffen. Beispielsweise können Daten des Storage Service importiert und exportiert werden, SQL-Datenbanken können kopiert und in lokale Umgebungen importiert werden. Darüber hinaus können APIs verwendet werden, die durch Azure Powershell oder den Cloud Dienst API Management verwaltet werden können.	https://azure.microsoft.com/de-de/documentation/articles/storage-import-export-service/#wann-sollte-der-importexport-dienst-von-azure-verwendet-werden https://azure.microsoft.com/de-de/documentation/articles/sql-database-copy/ https://azure.microsoft.com/de-de/documentation/articles/powershell-install-configure/ https://azure.microsoft.com/de-de/services/api-management/

3.11 M 2.540 (A) Sorgfältige Auswahl eines Cloud-Diensteanbieters

Ziel dieser Maßnahme ist es, die Auswahl eines geeigneten Cloud-Diensteanbieters sicherzustellen. Für einen detaillierten und vollständigen Vergleich sollte ein detailliertes Anforderungsdokument erstellt werden. Dieses Dokument muss genau abgrenzen, was von dem Cloud-Dienst erwartet und gefordert wird, einschließlich einer Beschreibung des Sicherheitskonzepts und der Sicherheitsrichtlinien. Eine zuvor durchgeführte Analyse der Anforderungen kann bei der Erstellung des Dokuments hilfreich sein.

Ausgehend von den definierten Anforderungen kann ein Servicekatalog oder eine Spezifikation der Anforderungen erstellt werden. Dieser Katalog kann dann verwendet werden, um die konkurrierenden Cloud-Diensteanbieter zu vergleichen und sie mit einer Punktematrix zu bewerten. Abschließend sollte eine Kosten-Nutzen-Analyse durchgeführt werden, um die verbleibenden Angebote zu vergleichen und eine realistische Einschätzung der potenziellen Kosteneinsparungen vom Umzug in ein Cloud-Dienstmodell zu ermöglichen.

Die grundlegenden Aspekte, die in der nachstehenden Tabelle aufgelistet sind, müssen untersucht und adäquate Antworten bereitgestellt werden, bevor die Angebote ausgewertet werden. Wenn die Ergebnis-

se nicht zufriedenstellend sind, kann ein Cloud-Diensteanbieter aus der weiteren Betrachtung entfernt werden.[13]

Prüffrage	Antwort	Referenz
Wurde auf der Basis der Service-Definition für den Cloud-Dienst ein detailliertes Anforderungsprofil für einen Cloud-Diensteanbieter erstellt?	Diese Anforderung liegt in der Verantwortung des Cloud-Nutzers.	
Existiert eine Leistungsbeschreibung oder ein Lastenheft zum Abgleich und zur Bewertung vorliegender Angebote unterschiedlicher Cloud-Diensteanbieter?	Diese Anforderung liegt in der Verantwortung des Cloud-Nutzers.	
Fanden ergänzende Informationsquellen (zum Beispiel Marktanalysen, vertragliche Regelungen oder Standortwahl) Eingang in die Bewertung eines Cloud-Diensteanbieters?	Diese Anforderung liegt in der Verantwortung des Cloud-Nutzers.	
Wurden die verfügbaren Service-Beschreibungen (SLAs oder AGBs) des Cloud-Diensteanbieters sorgfältig geprüft und hinterfragt?	Diese Anforderung liegt in der Verantwortung des Cloud-Nutzers. Relevante Vereinbarungen sind der Microsoft Online-Abonnementvertrag als auch die SLAs der einzelnen Cloud-Dienste.	https://azure.microsoft.com/de-de/support/legal/subscription-agreement/

3.12 M 2.541 (A) Vertragsgestaltung mit dem Cloud-Diensteanbieter

Diese Maßnahme stellt sicher, dass vertragliche Vereinbarungen hinsichtlich der Art, des Umfangs und des Detaillierungsgrades für die Schutzbedarf der Daten und der Anwendungen angemessen sind.

Die zuvor definierten Anforderungen müssen berücksichtigt werden, mindestens die folgenden Punkte erfordern außerdem eine Antwort in Bezug auf die Microsoft Cloud Deutschland.

Vertragsdokumente	Microsoft Cloud Deutschland	Referenz
Ort der Leistungserbringung durch den Cloud-Diensteanbieter	Die Cloud-Dienste werden auf Rechenzentren in Deutschland betrieben. Die gesamte Verarbeitung von Kundendaten durch den Datentreuhänder erfolgt innerhalb Deutschlands.	https://www.microsoft.com/de-de/cloud/deutschland/default.aspx (M370)EnrAmend(WW)(GER)(Aug2016)

[13] Weitere Aspekte und Unterstützung bei der Auswahl eines Cloud-Dienstleisters gibt es von Microsoft unter https://azure.microsoft.com/de-de/overview/choosing-a-cloud-service-provider/

Vertragsdokumente	Microsoft Cloud Deutschland	Referenz
An der Erbringung des Services beteiligte Subunternehmer oder andere Dritte	Microsoft setzt Subunternehmer nur für bestimmte, begrenzte Supportaufgaben ein. Ein deutscher Datentreuhänder ist damit beauftragt, jeden Zugriff auf Kundendaten zu kontrollieren.	https://www.microsoft.com/en-us/download/confirmation.aspx?id=50426
Regelungen hinsichtlich der Infrastruktur des Cloud-Diensteanbieters	Die für die Microsoft Cloud Deutschland verwendeten Rechenzentren befinden sich (aus Redundanz) in Frankfurt am Main und in Magdeburg. Sie sind über ein privates Netz miteinander verbunden, über das Daten kontinuierlich ausgetauscht werden. Die Implementierung einer Multiclient-Infrastruktur folgt den Konformitätsstandards, die von Microsoft Azure in Europa erfüllt werden.	https://www.microsoft.com/de-de/cloud/deutschland/default.aspx https://www.microsoft.com/de-de/TrustCenter/Compliance/default.aspx
Regelungen hinsichtlich des Personals beim Cloud-Diensteanbieter	Das für die Microsoft Cloud Deutschland eingesetzte (interne und externe) Personal hat alle erforderlichen Qualifikationen und wird gemäß interner Richtlinien überprüft.	Internes Dokument: HR Policy Microsoft Azure Standard Operating Procedure: Personnel Screening (SOP ID: 21)
Regelungen zu Prozessen, Arbeitsabläufen und Zuständigkeiten	Die Microsoft Cloud Deutschland unterliegt einem umfassenden Regelwerk, in dem auch Informations¬sicherheits-richtlinien (z. B. Asset Management, Malwareschutz) enthalten sind.	Verschiedene Microsoft Azure Standard Operating Procedures
Regelungen zur Beendigung des Vertragsverhältnisses	Jeder Cloud-Dienst wird auf Abonnement-Basis angeboten, wobei eine Kündigung jederzeit möglich ist. (Zusätzliche Optionen für Laufzeitverpflichtungen zu ermäßigten Preisen sind immer optional.)	https://azure.microsoft.com/de-de/support/legal/subscription-agreement/
Sicherstellung der Datenlöschung beim Cloud-Diensteanbieter	Kundendaten werden innerhalb von 180 Tagen nach Kündigung gelöscht. Physische Speichermedien werden am Ende ihrer Lebensdauer sicher vor Ort zerstört. Der Kunde kann darüber hinaus die sichere Löschung seiner Daten durch Verschlüsselung der in der Cloud gespeicherten Daten mit der durch die Microsoft Cloud Deutschland angebotenen Verschlüsselung sicherstellen.	(M370)EnrAmend(WW)(GER)(Aug2016) https://www.microsoft.com/de-de/TrustCenter/Security/Encryption Internes Dokument: On-Site Data Bearing Device Destruction Procedure

Vertragsdokumente	Microsoft Cloud Deutschland	Referenz
Regelungen zu Zutritts- und Zugriffsberechtigungen	Zugang zu Kundendaten ist in erster Linie dem Kunden vorbehalten. Nur für Support- und Wartungszwecke, mit kontinuierlicher Überwachung durch den Datentreuhänder, ist das Microsoft-Supportpersonal berechtigt, auf gespeicherte Kundendaten zuzugreifen. Das für die Microsoft Cloud Deutschland eingesetzte (interne und externe) Personal hat alle erforderlichen Qualifikationen und wird gemäß interner Richtlinien überprüft.	(M370)EnrAmend(WW)(GER)(Aug2016) Microsoft Sovereign Cloud - Compliance in the cloud for German business organizations Internes Dokument: HR Policy; Microsoft Azure Standard Operating Procedure: Personnel Screening (SOP ID: 21)
Regelungen zur Notfallvorsorge	Microsoft hat angemessene Vorsorge für den Betrieb der Cloud-Dienste gemäß dem in den SLA definierten Niveau getroffen. Entsprechende Maßnahmen umfassen auch die geografische Trennung der Rechenzentren und die kontinuierliche Replikation der Daten zwischen ihnen. Der Kunde kann weitere Verfügbarkeitsanforderungen durch die Nutzung zusätzlicher Cloud-Dienste wie Backup oder Site Recovery erfüllen.	Internes Dokument: Business Continuity und Disaster Recovery (SOP ID: 20) https://www.microsoft.com/de-de/cloud/deutschland/default.aspx https://azure.microsoft.com/de-de/services/backup/ https://azure.microsoft.com/de-de/services/site-recovery/
Regelungen zu rechtlichen Rahmenbedingungen	Microsoft erfüllt alle Gesetze und Vorschriften bezüglich der Bereitstellung der Cloud-Dienste. Der Datentreuhänder erfüllt ebenfalls alle Gesetze, die seine Rolle bei der Bereitstellung der Cloud-Dienste betreffen. Weitere Vorschriften und Richtlinien sind in der internen Richtlinie „Legal and Regulatory Compliance“ enthalten.	MicrosoftOnlineServicesTerms(German)(January2017)(cr).docx Microsoft Azure Standard Operating Procedure: Legal and Regulatory Compliance (SOP ID: 11)
Festlegungen zum Änderungsmanagement und zu Testverfahren	Änderungsmanagement und Testverfahren werden in einer internen Richtlinie definiert.	Microsoft Azure Standard Operating Procedure: Hardware Change and Release Management (SOP ID: 24) Microsoft Azure Standard Operating Procedure: Secure Development Lifecycle (SDL) (SOP ID: 15)

Vertragsdokumente	Microsoft Cloud Deutschland	Referenz
Regelungen zur Durchführung von Kontrollen	Die Microsoft Cloud Deutschland bietet Kunden die Möglichkeit, die SLA-Konformität mit dem Modul „Service Health“ im Azure Portal zu überwachen. Cloud-Nutzer haben die Möglichkeit, Penetrationstests gegen ihre Cloud-Dienste durchzuführen, wenn dem zuvor zugestimmt wurde. Die Überwachung der Microsoft Cloud Deutschland unterliegt einer Reihe von internen Vorgaben. Erfolgreiche und erfolglose Zugriffsversuche auf Kundendaten und Änderungen an den Daten werden protokolliert und die Protokolle für ein Jahr vorgehalten. Systemprotokolle werden nach 90 Tagen gelöscht. Microsoft Azure und Microsoft Cloud Deutschland werden bedingt durch die Anforderungen mehrerer Konformitätsstandards und Zertifizierungen kontinuierlich auditiert. Informationen und Anleitungen zu laufenden und abgeschlossenen Audits und Sicherheitszertifikaten werden einschließlich der öffentlich verfügbaren Berichte und Ergebnisse bereitgestellt.	https://security-forms.azure.com/penetration-testing/terms Microsoft Azure Standard Operating Procedure: Logging and Monitoring (SOP ID: 12) Microsoft Azure Standard Operating Procedure: Penetration Testing (SOP ID: 23) https://www.microsoft.com/de-de/TrustCenter/Compliance/default.aspx https://trustportal.office.com/
Berücksichtigung besonderer Anforderungen	In der Microsoft Cloud Deutschland hat der Cloud-Nutzer die Möglichkeit, Backups über einen Cloud-Dienst wie Azure Backup zu erstellen. Daten können auch importiert und exportiert werden (zusätzlich zu den vorhandenen Portabilitätsvorkehrungen der einzelnen Cloud-Dienste).	https://azure.microsoft.com/de-de/services/backup/ https://azure.microsoft.com/de-de/documentation/articles/storage-import-export-service/ Siehe 3.10 M 4.461 (Z) Portabilität von Cloud Services

Prüffrage	Antwort	Referenz
Sind die vertraglichen Regelungen in Art, Umfang und Detaillierungsgrad dem Schutzbedarf der Daten und Anwendungen angepasst, die im Zusammenhang mit der Cloud-Nutzung stehen?	Es existiert ein Prozess für Microsoft Cloud Deutschland, der es ermöglicht, alle Kundendaten, die in der Cloud gespeichert werden können, nach Sensibilität zu klassifizieren und entsprechende Schutzmaßnahmen zu treffen. Das Verfahren stellt außerdem sicher, dass das Microsoft-Servicepersonal keinen Zugriff auf Kundendaten ohne vorherige Genehmigung durch den Kunden oder Authorisierung und Überwachung durch den Datentreuhänder erhält.	Internes Dokument: Asset Management (SOP ID: 03); Asset Classification and Protection Matrix (Azure) (M370)EnrAmend(WW)(GER)(Aug2016)
Wurde geregelt, an welchem Standort der Cloud-Diensteanbieter seine Leistungen erbringt?	Die Cloud-Dienste werden aus Rechenzentren in Deutschland betrieben. Die Verarbeitung von Kundendaten durch den Datentreuhänder erfolgt innerhalb Deutschlands.	https://www.microsoft.com/de-de/cloud/deutschland/default.aspx (M370)EnrAmend(WW)(GER)(Aug2016)
Wurden klare Verantwortlichkeiten, Eskalationsstufen und Kommunikationswege zwischen der beauftragenden Institution und dem Cloud-Diensteanbieter definiert?	Nutzer von Microsoft Cloud Deutschland haben Zugriff auf die Kontoverwaltung und die Rechnungserstellung sowie den Support und Leitlinien, die im Azure Portal bereitgestellt werden. Technische Unterstützung kann über das Azure Portal bei Kauf eines entsprechenden Supportpakets angefordert werden.	https://azure.microsoft.com/de-de/support/options/ https://azure.microsoft.com/de-de/support/faq/ https://azure.microsoft.com/de-de/support/plans/
Existieren Vereinbarungen über die sichere Löschung von Daten durch den Cloud-Diensteanbieter?	Kundendaten werden innerhalb von 180 Tagen nach Kündigung gelöscht. Der Kunde kann die sichere Löschung seiner Daten durch Verschlüsselung der in der Cloud gespeicherten Daten mit der von Microsoft Cloud Deutschland angebotenen Verschlüsselung sicherstellen.	(M370)EnrAmend(WW)(GER)(Aug2016) https://www.microsoft.com/de-de/TrustCenter/Security/Encryption https://azure.microsoft.com/de-de/documentation/articles/storage-service-encryption/ https://blogs.msdn.microsoft.com/azuresecurity/2015/05/11/azure-disk-encryption-management-for-windows-and-linux-virtual-machines/

Prüffrage	Antwort	Referenz
Wurden Kündigungsregelungen schriftlich fixiert?	Jeder Cloud-Dienst wird auf Abonnement-Basis angeboten, wobei eine Kündigung jederzeit möglich ist. (Zusätzliche Optionen für Laufzeitverpflichtungen zu ermäßigten Preisen sind optional verfügbar.)	https://azure.microsoft.com/de-de/support/legal/subscription-agreement/

3.13 M 2.542 (A) Sichere Migration zu einem Cloud Service

Diese Maßnahme betrachtet die eigentliche Migration zum Cloud-Dienst unter Berücksichtigung des zuvor erwähnten Migrations-Sicherheitskonzeptes. Die Migration muss kontinuierlich überwacht werden, um erforderliche Änderungen oder Ursachen, die eine Migration verhindern oder behindern, zu erkennen und reagieren zu können. Falls erforderlich, sollte die Migration abgebrochen und eine Untersuchung der Ursachen durchgeführt werden. Um das Risiko signifikanter Probleme zu reduzieren, sollten zuerst Tests oder ein Pilotprojekt zur Migration durchgeführt werden.

Diese Maßnahme ist organisationsspezifisch, da sie die interne Planung für eine sichere Integration von bestehenden Diensten abdeckt. Microsoft bietet Werkzeuge zur Unterstützung einer Migration von aktuellen Ressourcen nach Azure an.[14]

3.14 M 2.543 (A) Aufrechterhalten der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb

Ziel dieser Maßnahme ist es, nach einer Migration zu einem Cloud-Dienst eine vergleichbare oder erhöhte Informationssicherheit zu erhalten. Dementsprechend sollten Richtlinien und Dokumentationen auf dem neuesten Stand gehalten werden und die Konformität mit Standards sollte sowohl auf Seiten des Cloud-Nutzers als auch des Cloud-Dienstleisters regelmäßig überprüft werden.

Prüffrage	Antwort	Referenz
Werden Dokumentationen und Richtlinien (zum Beispiel Betriebshandbücher und Nutzungsanweisungen) regelmäßig aktualisiert?	Diese Anforderung liegt in der Verantwortung des Cloud-Nutzers.	

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

Prüffrage	Antwort	Referenz
Wird die Service-Erbringung regelmäßig kontrolliert?	Diese Anforderung liegt in der Verantwortung des Cloud-Benutzers. Microsoft Cloud Deutschland beinhaltet ein integriertes SLA Monitoring System („Service Health"), über das die Einhaltung der Dienste überprüft werden kann. Diese Anforderung liegt in der Verantwortung des Cloud-Nutzers.	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/
Wurden Sicherheitsnachweise durch den Cloud-Diensteanbieter erbracht?	Diese Anforderung liegt in der Verantwortung des Cloud-Benutzers. Microsoft Cloud Deutschland bietet in dieser Hinsicht eine Vielzahl von Publikationen und Prüfungen sowie geltende Zertifizierungen an. Dies kann von Nutzer der Microsoft Cloud Deutschland auf der öffentlichen Website sowie in Form eines Audits überprüft werden, welches im Service Trust Portal eingesehen werden kann.	https://www.microsoft.com/de-de/TrustCenter/STP/default.aspx https://www.microsoft.com/de-de/TrustCenter/Compliance/default.aspx https://trustportal.office.com/
Werden regelmäßige Abstimmungsrunden zwischen Cloud-Diensteanbieter und nutzender Institution durchgeführt?	Microsoft Cloud Deutschland bietet eine Vielzahl von Supportoptionen. Cloud-Nutzer werden im Falle einer erheblichen Betriebsstörung kontaktiert.	
Werden Übungen und Tests zur Reaktion auf Systemausfälle geplant und durchgeführt?	Diese Anforderung liegt in der Verantwortung des Cloud-Nutzers. Microsoft Cloud Deutschland hat interne Regelungen für die Erbringung der Service-Kontinuität gemäß dem in den SLA definierten Niveau festgelegt.	Internes Dokument: Business Continuity and Disaster Recovery (SOP ID: 20)

3.15 M 2.544 (C) Auditierung bei Cloud-Nutzung

Durch diese Maßnahme soll sichergestellt werden, dass der Cloud-Nutzer seine Anforderungen an die Durchführung von Audits erfüllt und dass vertragliche Regelungen beidseitig eingehalten werden. Dies kann unabhängig vom Cloud-Dienstmodell z. B. durch Vor-Ort-Audits oder spezielle Fragebögen erreicht werden.

Microsoft Azure und Microsoft Cloud Deutschland werden aufgrund der Anforderungen verschiedener Konformitätsstandards und Zertifizierungen kontinuierlich auditiert. Die Liste der Konformitätsstandards

für Microsoft Azure beinhaltet ISO/IEC 27018, ISO/IEC 27001, PCI-DSS und SOC 1/2/3 (für weitere Einzelheiten siehe Kapitel 4)), für Microsoft Azure Deutschland liegen bereits ISO/IEC 27001 und ISO/IEC 27018 Zertifizierungen vor. Diese Audits werden von akkreditierten Auditoren durchgeführt. Zusätzlich werden interne Audits von Microsoft durchgeführt. Informationen über diese Audits sind online über das Microsoft Trust Center verfügbar. Darüber hinaus können Behörden- und Firmenkunden Zugriff auf das Service Trust Portal (STP) erhalten, welches direkten Zugriff auf viele der Prüfberichte und Bescheinigungen ermöglicht.

Microsoft strebt an, Auditanforderungen aus dem IT-Grundschutz durch unabhängige Dritte (d. h. durch Zertifizierungsaudits) prüfen zu lassen.

Penetrationstests können nach Vorankündigung und unter Beachtung der Bandbreitenlimits durchgeführt direkt durch den Kunden (oder durch von ihm beauftragte Dritte) durchgeführt werden.

Prüffrage	Antwort	Referenz
Hat sich die Institution das Recht zur Durchführung von Audits vertraglich zusichern lassen? Wird die Umsetzung der mit dem Cloud-Diensteanbieter vereinbarten Sicherheitsmaßnahmen regelmäßig in Form von Audits oder durch die Beantwortung von Fragebögen überprüft? Werden bei der Planung und der Durchführung von Audits die Besonderheiten der Service-Modelle IaaS, PaaS und SaaS berücksichtigt?	Microsoft Azure und Microsoft Cloud Deutschland werden bedingt durch die Anforderungen mehrerer Konformitätsstandards und Zertifizierungen kontinuierlich auditiert. Informationen und Anleitungen zu laufenden und abgeschlossenen Audits und Sicherheitszertifikaten werden einschließlich der öffentlich verfügbaren Berichte und Ergebnisse bereitgestellt. Dadurch ist der Kunde nicht mehr verpflichtet, ein eigenes Audit durchführen zu müssen. Firmenkunden können Zugriff auf das Service Trust Portal (STP) erhalten, welches direkten Zugriff auf die meisten Prüfberichte gestattet.	https://www.microsoft.com/de-de/TrustCenter/Compliance/default.aspx https://trustportal.office.com/ https://www.microsoft.com/de-de/TrustCenter/STP/default.aspx https://security-forms.azure.com/penetration-testing/terms

3.16 M 4.460 (Z) Einsatz von Federation Services

Diese zusätzliche Maßnahme für hohen Schutzbedarf berücksichtigt die Sicherheitsanforderungen an Cloud-Verbunddienste. Mit Verbunddiensten können Benutzerinformationen oder andere persönliche Informationen von Mitarbeitern sicher außerhalb des Unternehmens übertragen werden. Das Schlüssel-

merkmal ist die Trennung von Authentisierung (durch den Identity Provider) und Autorisierung (durch den Service Provider).

Die primäre Sicherheitsmaßnahme ist, nur die notwendigen Mindestinformationen in einem SAML[15] -Ticket an den Cloud-Dienstleister zu senden. Darüber hinaus müssen Benutzerrechte und Rollen regelmäßig überprüft werden, um sicherzustellen, dass nur autorisierte Benutzer Zugriff haben.

Microsoft Cloud Deutschland bietet Verbunddienste über Azure Active Directory an.

Prüffrage	Antwort	Referenz
Ist sichergestellt, dass nur die erforderlichen Informationen in dem sogenannten SAML-Ticket an den Cloud-Diensteanbieter übertragen werden?	Diese Anforderung liegt in der Verantwortung des Cloud-Nutzers. Microsoft bietet Verbunddienste mit Azure Active Directory an, dass sowohl das SAML 2.0-Protokoll als auch WS-Federation und OpenID Connect unterstützt. Welche Informationen in den SAML-Tickets enthalten sind, kann gemäß den eigenen Anforderungen oder den Anforderungen jeder einzelnen Anwendung konfiguriert werden.	https://azure.microsoft.com/de-de/services/active-directory/ https://azure.microsoft.com/de-de/documentation/articles/active-directory-single-sign-on-protocol-reference/ https://azure.microsoft.com/de-de/documentation/articles/active-directory-saas-custom-apps/ https://azure.microsoft.com/de-de/documentation/articles/active-directory-saml-claims-customization/ https://azure.microsoft.com/de-de/documentation/articles/active-directory-token-and-claims/
Werden die Benutzererberechtigungen regelmäßig geprüft und wird sichergestellt, dass lediglich berechtigten Benutzern ein SAML-Ticket ausgestellt wird?	Diese Anforderung liegt in der Verantwortung des Cloud-Nutzers.	

3.17 M 2.307 (A) Geordnete Beendigung eines Outsourcing- oder Cloud-Nutzungs-Verhältnisses

Diese Maßnahme soll sicherstellen, dass ein Umstieg auf einen anderen Cloud-Dienstleister oder zurück auf ein klassisches Infrastrukturmodell genau so gründlich wie eine initiale Integration geplant wird. Das

[15] SAML (Security Assertion Markup Language) ist ein standardisiertes Protokoll für den Austausch von Authentisierungs- und Autorisierungsinformationen

Planungs- und Migrationskonzept sollte das Sicherheitskonzept genauso berücksichtigen wie beim ursprünglichen Umzug in die Cloud.

Zum Schutz der Kundendaten hat Microsoft Cloud Deutschland die T-Systems International GmbH als Datentreuhänder beauftragt. Die Kundendaten werden spätestens 180 Tage nach der vereinbarten Nutzungsdauer oder der Kündigung des Nutzungsvertrages gelöscht.[16]

Prüffrage	Antwort	Referenz
Regelt der Vertrag mit dem Outsourcing-Dienstleister oder dem Cloud-Diensteanbieter auch alle Aspekte der Beendigung des Dienstleistungsverhältnisses?	Jeder Cloud-Dienst wird als Abonnement angeboten, wobei eine Kündigung jederzeit möglich ist. (Zusätzliche Optionen für Laufzeitverpflichtungen zu ermäßigten Preisen sind optional verfügbar.)	https://azure.microsoft.com/de-de/support/legal/subscription-agreement/
Ist sichergestellt, dass eine Beendigung des Dienstleistungsverhältnisses mit dem Outsourcing-Dienstleister oder Cloud-Diensteanbieter die Geschäftstätigkeit des Auftraggebers nicht beeinträchtigt?	Diese Anforderung liegt in der Verantwortung des Cloud-Nutzers.	

3.18 M 6.155 (A) Erstellung eines Notfallkonzeptes für einen Cloud Service

Diese Maßnahme sieht vor, die Cloud-Nutzung durch die Erstellung eines Notfallkonzepts zu sichern. Dazu gehören alle technischen und organisatorischen Aspekte des Business Continuity Managements.

Das Notfallkonzept muss für jeden Cloud-Dienst individuell erstellt werden. Die Notfallwiederherstellung muss während des Entwicklungsprozesses der Anwendungen für Microsoft Cloud Deutschland berücksichtigt werden. [17] Um bei diesem Prozess zu unterstützen, bietet Microsoft Cloud Deutschland eine Datenwiederherstellung innerhalb der Cloud über den Site Recovery Cloud Service an.[18] Sofern weitreichenderer Schutz erforderlich ist, kann das Hybrid Cloud Platform-Produkt Microsoft Azure Stack verwendet werden, um eine Datenwiederherstellung zu unterstützen.[19]

[16] (M370)EnrAmend(WW)(GER)(Aug2016)

[17] https://azure.microsoft.com/de-de/documentation/articles/resiliency-disaster-recovery-high-availability-azure-applications/

[18] https://azure.microsoft.com/de-de/services/site-recovery/

[19] https://azure.microsoft.com/de-de/overview/azure-stack/

3.19 M 6.156 (Z) Durchführung eigener Datensicherungen

Diese zusätzliche Maßnahme für hohe Schutzbedarfsfeststellungen zielt darauf ab, die Verfügbarkeit der Daten zu gewährleisten, wenn der Zugriff auf Cloud-Dienste verloren geht oder die Cloud-Dienste selbst nicht verfügbar sind.

Dies muss durch ihre eigene Organisation initiiert werden; entweder durch sie selbst oder durch einen anderen, unabhängigen Dienst. Wurde ein externer Anbieter dafür ausgewählt, muss der Kunde sicherstellen, dass alle Anforderungen für die Datensicherung und Datensicherheit erfüllt sind.

4 MICROSOFT's Verantwortlichkeiten als Cloud-Dienstanbieter

Microsoft ist für die Sicherheit der Cloud unterhalb der Virtualisierungsschicht verantwortlich, wobei der Zugang zu Kundendaten vom Datentreuhänder T-Systems überwacht wird. Um den Cloud-Kunden in der Lage zu versetzen, die Sicherheit der Cloud ohne die Durchführung eines vollständigen Audits der technischen Infrastruktur (aber mit ähnlicher Gewissheit) zu bewerten, hat Microsoft diverse sicherheitsbezogene Zertifizierungen für Azure durchführen lassen.

Die wichtigsten davon sind:

- ISO/IEC 27018 (Anwendungsregel für den Schutz von Personenbezogenen Daten (PII) in Public Clouds, die als PII Processor auftreten)
- ISO/IEC 27001 (Informationssicherheits-Managementsysteme)
- PCI-DSS (Payment Card Industry Data Security Standard)
- SOC 1 - SOC 2 - SOC 3 (SSAE16 / ISAE 3402)

Microsoft strebt an, diese Zertifizierungen für Microsoft Cloud Azure nach der allgemeinen Verfügbarkeit der Dienste ebenfalls zu erlangen , die ISO/IEC 27001 und ISO/IEC 27018 Zertifizierungen liegen bereits vor. Spezifische Maßnahmen oder Anforderungen können den verpflichtenden Maßnahmen in diesen Standards zugeordnet werden.

Darüber hinaus wird derzeit die Machbarkeit einer „ISO 27001 Zertifizierung auf Basis von IT-Grundschutz" für Microsoft Cloud Deutschland analysiert.[20] Eine solche Zertifizierung kann die Zertifizierung von Cloud-Kunden erheblich erleichtern, ist aber für eine grundschutzkonforme Umsetzung nicht zwingend notwendig.

Die Sicherheit des Cloud-Dienstleisters kann auch mit dem Anforderungskatalog Cloud Computing (C5) des BSI überprüft werden. Hier werden die Anforderungen festgelegt, die ein Cloud-Dienstleister erfüllen muss, bzw. die von einem Dienstleister zu erfüllenden Mindeststandards.[21] Zusätzlich zum C5-Anforderungskatalog werden Anforderungen und Empfehlungen aus den Standards ISO/IEC 27001:2013, CSA Cloud Controls Matrix 3.01, AICPA - Trust Services Principles Criteria 2014, ANSSI Référentiel Secure Cloud 2.0 (Entwurf), IDW ERS FAIT 5 04.11.2014, BSI IT-Grundschutz 14. EL 2014 und BSI SaaS Sicherheitsprofile 2014 ebenfalls referenziert. Eine Machbarkeitsstudie zur Zertifizierung nach diesen Standards wird derzeit durchgeführt.

Zur Unterstützung von Sicherheitsaudits soll in einem zukünftigen zweiten Teil dieses Leitfadens dargestellt werden, wie die existierenden Sicherheitsmaßnahmen und Zertifizierungen von Microsoft Cloud Deutschland auf den IT-Grundschutz abgebildet werden können.

[20] https://www.microsoft.com/de-de/cloud/deutschland/default.aspx

[21] https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Anforderungskatalog/Anforderungskatalog_node.html

Quellen zu weiterführenden Informationen

Anhang

Thema	Weblink
Rechtliche Hinweise	https://azure.microsoft.com/de-de/support/legal/ http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=37 https://azure.microsoft.com/de-de/support/legal/subscription-agreement/
Azure-Dienste, Werkzeuge und weitere Informationen	https://info.microsoft.com/enterprise-cloud-strategy-ebook.html https://azure.microsoft.com/de-de/overview/choosing-a-cloud-service-provider/ https://azure.microsoft.com/de-de/services/ https://azure.microsoft.com/de-de/features/azure-portal/ https://azure.microsoft.com/de-de/services/active-directory/ https://azure.microsoft.com/de-de/services/active-directory-b2c/ https://azure.microsoft.com/de-de/services/virtual-network/ https://azure.microsoft.com/de-de/services/expressroute/ https://azure.microsoft.com/de-de/services/virtual-machine-scale-sets/ https://azure.microsoft.com/de-de/services/virtual-machines/ https://azure.microsoft.com/de-de/services/api-management/ https://azure.microsoft.com/de-de/services/backup/ https://azure.microsoft.com/de-de/services/site-recovery/ https://azure.microsoft.com/de-de/services/cloud-services/ https://azure.microsoft.com/de-de/services/service-fabric/ https://azure.microsoft.com/de-de/services/sql-database/ https://azure.microsoft.com/de-de/services/storage/ https://azure.microsoft.com/de-de/services/key-vault/ https://azure.microsoft.com/de-de/tools/ https://blogs.technet.microsoft.com/cbernier/2014/01/27/move-vms-between-hyper-v-and-windows-azure/

Thema	Weblink
	https://azure.microsoft.com/de-de/documentation/articles/sql-database-copy/
	https://azure.microsoft.com/de-de/documentation/articles/insights-how-to-customize-monitoring/
	https://azure.microsoft.com/de-de/status/
	https://azure.microsoft.com/de-de/documentation/articles/active-directory-whatis/
	https://azure.microsoft.com/de-de/documentation/articles/active-directory-aadconnect/
	https://azure.microsoft.com/de-de/documentation/articles/storage-import-export-service/#wann-sollte-der-importexport-dienst-von-azure-verwendet-werden
	https://azure.microsoft.com/de-de/documentation/articles/storage-import-export-service/
	https://azure.microsoft.com/de-de/downloads/vm-readiness-assessment/
	https://azure.microsoft.com/de-de/downloads/vm-optimization-assessment/
	https://azure.microsoft.com/de-de/documentation/articles/powershell-install-configure/
	https://azure.microsoft.com/de-de/support/options/
	https://azure.microsoft.com/de-de/support/faq/
	https://azure.microsoft.com/de-de/support/plans/
	https://azure.microsoft.com/de-de/overview/azure-stack/
Sicherheitsaspekte Microsoft Cloud Deutschland	https://www.microsoft.com/de-de/cloud/deutschland/default.aspx
Sicherheitsaspekte Azure	https://www.microsoft.com/de-de/TrustCenter/Compliance/default.aspx
	https://www.microsoft.com/de-de/TrustCenter/Security/AzureSecurity
	https://trustportal.office.com/
	https://security-forms.azure.com/penetration-testing/terms
	https://www.microsoft.com/de-de/TrustCenter/STP/default.aspx
	https://azure.microsoft.com/de-de/services/multi-factor-authentication/
	https://www.microsoft.com/de-de/TrustCenter/Security/Encryption
	https://azure.microsoft.com/de-de/documentation/articles/storage-security-guide/
	https://azure.microsoft.com/de-de/documentation/articles/storage-service-encryption/

Thema	Weblink
	https://blogs.msdn.microsoft.com/azuresecurity/2015/05/11/azure-disk-encryption-management-for-windows-and-linux-virtual-machines/
	https://azure.microsoft.com/de-de/blog/new-windows-azure-security-overview-white-paper-now-available/
	https://azure.microsoft.com/de-de/blog/microsoft-azure-network-security-whitepaper-version-3-is-now-available/
	https://azure.microsoft.com/de-de/services/virtual-machines/security/
	https://gallery.technet.microsoft.com/Azure-Responses-to-CSA-46034a11
	https://azure.microsoft.com/de-de/documentation/articles/active-directory-single-sign-on-protocol-reference/
	https://azure.microsoft.com/de-de/documentation/articles/active-directory-saas-custom-apps/
	https://azure.microsoft.com/de-de/documentation/articles/active-directory-saml-claims-customization/
	https://azure.microsoft.com/de-de/documentation/articles/active-directory-token-and-claims/
	https://azure.microsoft.com/de-de/documentation/articles/resiliency-disaster-recovery-high-availability-azure-applications/
Liste der Microsoft Dienstleister	https://www.microsoft.com/en-us/download/details.aspx?id=50426
BSI	https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html;jsessionid=F6BE71C1337EB6140D7D0952EA479087.2_cid368
	https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html;jsessionid=F6BE71C1337EB6140D7D0952EA479087.2_cid368
	https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Anforderungskatalog/Anforderungskatalog_node.html

Manuel Atug, Enno Ewers
Phone +49 30 533289-0
matug@hisolutions.com
ewers@hisolutions.com

HiSolutions AG
Bouchéstraße 12
12435 Berlin

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

HiSolutions AG
Niederlassung
Frankfurt am Main
Mainzer Landstraße 50
60325 Frankfurt am Main

Phone +49 30 533 289-0
Fax + 49 30 533 289-900

HiSolutions AG
Niederlassung
Köln
Theodor-Heuss-Ring 23
50688 Köln

Phone +49 221 77 109-550
Fax + 49 30 533 289-900

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

Phone +49 22 852 268 175
Fax + 49 30 533 289-900