HISOLUTIONS

IT-Grundschutz Compliance für Office 365

1. Februar 2022
MICROSOFT DEUTSCHLAND GMBH

Inhaltsverzeichnis

1 Einleitung

Office 365 ist Microsofts Büroanwendungssuite, die mit Funktionalitäten zur Kommunikation und Zusammenarbeit in der Cloud erweitert wurde. Office 365 bietet plattformübergreifende Office-Anwendungen und -Dienste, einschließlich Geschäfts-E-Mails, Team-Chat, Videokonferenzen, gemeinsame Kalender und Cloud-Speicher. Die Region in Office 365 wird in Abhängigkeit vom ersten aktivierten Abonnement des Kunden zugeordnet und kann jederzeit über das Adminportal in Office 365 überprüft werden.

In Deutschland stellt das Bundesamt für Sicherheit in der Informationstechnik (BSI) die IT-Grundschutz-Methodik zur Verfügung (und entwickelt diese stetig weiter). Die Methodik besteht aus einem ISO 27001-kompatiblen Informationssicherheitsmanagementsystem (ISMS), das in den BSI-Standards 200-1 und 200-2 beschrieben ist. Dies wird ergänzt mit einer speziellen Risikoanalysemethode (BSI-Standard 200-3), einem Business Continuity Management (BSI-Standard 100-4; derzeit in der Überarbeitung) und dem IT-Grundschutz-Kompendium, einer Standardauflistung von Gefährdungen und Anforderungen für typische Geschäftsumgebungen.

Ziel dieses Leitfadens ist es, Office 365-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*[1] als Teil des Informationsverbunds[2] gegeben. Kapitel 4 informiert über die Umsetzung des Standards „Mindeststandard des BSI zur Nutzung externer Cloud-Dienste“[3], der sich an die Bundesbehörden richtet. Kapitel 5 behandelt die Verantwortlichkeiten von Microsoft als Cloud-Diensteanbieter.

[1] 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

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

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

2 Zertifizierungsanforderungen

Der vorliegende Leitfaden für Office 365 basiert auf der überarbeiteten Version des BSI IT-Grundschutz Kompendiums aus dem Jahr 2021[4]. In dieser Version des IT-Grundschutzes ist der Baustein *OPS.2.2 Cloud-Nutzung*[5] enthalten. Im IT-Grundschutz wird zwischen der Nutzung von Cloud-Diensten wie Office 365 und klassischem IT-Outsourcing unterschieden.

2.1 Modell der gemeinsamen Verantwortung

Im Gegensatz zur lokalen IT-Infrastruktur wird in einer Cloud- Umgebung die Verantwortung für die Implementierung und Wartung von Sicherheitsanforderungen für IT-Anwendungen zwischen Kunde und Cloud-Diensteanbieter geteilt. Eine vollständige Übertragung der Verantwortlichkeiten kann nur dann erfolgen, wenn der Cloud-Diensteanbieter die Anwendungen der Kunden in seinen eigenen Zertifizierungsumfang (d.h. in ein klassisches Outsourcing-Szenario) einschließlich eines abgestimmten Risikomanagements einbezieht. Es ist zu beachten, dass nach der IT-Grundschutz-Methodik die endgültige Verantwortung immer beim Kunden (dem Dateneigentümer) liegt.

Durch die neuen Versionen des IT-Grundschutzes wird ein gemeinsames Verantwortungsmodell ermöglicht. Dieses unterteilt die Verantwortung zwischen dem Kunden und dem Cloud-Diensteanbieter entlang der Applikationsgrenzen, so dass jeweils nur eine Partei für einen bestimmten Aspekt verantwortlich ist.

Tabelle 1 zeigt einen Überblick auf Makroebene, wie eine solche Partitionierung für Software-as-a-Service (SaaS) aussehen kann. Das Shared-Responsbility-Modell ist in mehrere Aspekte unterteilt (siehe Beschreibungen unten). Die Aspekte liegen in der Verantwortung des Kunden, des Cloud-Diensteanbieters oder von beiden. Die Tabelle beschreibt auch den verfügbaren Support für den Kunden, der von Microsoft in seiner Rolle als Cloud-Diensteanbieter bereitgestellt wird.

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

[5] 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 Verantwortung für die Sicherheit im Cloud-Computing (SaaS-Modell)[6]

Aspekt/Verantwortung Cloud Kunde Cloud-Diensteanbieter		Beschreibung
Sicherheitskonzept		Sicherheitskonzepte sind ein wesentlicher Bestandteil der IT-Grundschutz-Methodik. Ein Sicherheitskonzept ist eine dokumentierte Risikoanalyse und -behandlung mit einem definierten Geltungsbereich. Es beinhaltet die daraus resultierenden Maßnahmen zur Erhöhung der Sicherheit des Systems oder der Umgebung. Dieser Leitfaden kann bei der Erstellung eines Sicherheitskonzeptes für Office 365 helfen.
Datenklassifizierung & Verantwortlichkeit		Der Wert der Daten kann nur vom Kunden bestimmt werden, der daher seine Daten identifizieren, klassifizieren und kennzeichnen sollte. Office 365 unterstützt Kunden beim Schutz ihrer Daten durch Lösungen wie Microsoft Information Protection[7].
Kunden- und Endpunkte-Schutz		Kunden sollten klar definieren, welche Geräte und Clients auf die Cloud zugreifen dürfen.
Identitäts- und Berechtigungsmanagement		Office 365 bietet verschiedene Optionen für das Identitäts- und Berechtigungsmanagement an – von der vollständig Cloud-basierten Option[8] bis hin zur Föderation mit dem lokalen Active Directory[9]. Zusammen mit Azure Active Directory kann der Kunde Kennwortrichtlinien und Multi-Faktor-Authentifizierung (MFA)[10] nach seinen spezifischen Richtlinien konfigurieren. Es ist zu beachten, dass auch bei der nur Cloud-basierten Identitätsoption die Verantwortung für das Identitäts- und Berechtigungsmanagement teilweise noch beim Kunden liegt. Der Zugriff auf Kundendaten durch Mitarbeiter von Microsoft kann über Customer Lockbox[11] gesteuert werden.
Audits		Office 365 wird aufgrund der Anforderungen verschiedener Compliance-Standards und Zertifizierungen kontinuierlich von unabhängigen

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

[7] https://docs.microsoft.com/de-de/microsoft-365/compliance/information-protection

[8] https://docs.microsoft.com/de-de/office365/enterprise/about-office-365-identity

[9] https://docs.microsoft.com/de-de/office365/enterprise/plan-for-directory-synchronization

[10] https://docs.microsoft.com/de-de/office365/admin/security-and-compliance/multi-factor-authentication-plan

[11] https://docs.microsoft.com/de-de/microsoft-365/compliance/customer-lockbox-requests

Aspekt/Verantwortung Cloud Kunde Cloud-Diensteanbieter		Beschreibung
		Dritten auditiert. Die Liste der Konformitätsnormen für Office 365 umfasst BSI C5, ISO 27001, ISO 27017 und ISO 27018.[12]
Portabilität		Kundendaten, die in Office 365 gespeichert sind, können mit Hilfe von Tools von Microsoft oder Drittanbietern exportiert und heruntergeladen werden.
Notfallwiederherstellung		Die Office 365-Dienste sind der gebotenen Sorgfalt konzipiert worden. Die Dienste halten mehrere Live-Kopien von Kundendaten in verschiedenen Rechenzentren bereit, um die vertragliche Verfügbarkeit sicherzustellen[13]. Kunden sollten einen Notfallwiederherstellungsplan entwickeln, der auch die Datensicherung umfasst.
Maßnahmen auf Anwendungsebene		Für Office 365-Kunden werden die allgemeinen Kontrollen auf Anwendungsebene (z. B. Anti-Malware- und Patch-Management) von Microsoft bereitgestellt.
Netzwerksteuerungen		Für Office 365-Kunden wird das Netzwerk von Microsoft verwaltet, konfiguriert und gesichert.
Host-Infrastruktur		Die Host-Infrastruktur wird von Microsoft bereitgestellt und verwaltet. Das Management der Host-Infrastruktur umfasst beispielsweise die Beschaffung von Servern und deren sichere Konfiguration.
Physische Sicherheit		Die physische Sicherheit garantiert, dass nur autorisierte Mitarbeiter physischen Zugriff auf Server, Netzwerkgeräte usw. erhalten. Dazu gehört auch das Business Continuity Management, um sicherzustellen, dass der Cloud-Dienst im Falle von schweren Vorfällen oder Katastrophen, wie beispielsweise einem Ausfall an einem anderen physischen Standort, verfügbar bleibt.

[12] https://docs.microsoft.com/de-de/microsoft-365/compliance/offering-home

[13] https://docs.microsoft.com/de-de/compliance/assurance/assurance-resiliency-and-continuity

2.2 Modellierung von Office 365 Deutschland

Um die IT-Grundschutzkonformität bei Nutzung der Office 365-Dienste zu erhalten, muss das IT-Sicherheitskonzept um den Cloud-Dienst Office 365 nach BSI-Standard 200-2[14] erweitert werden.

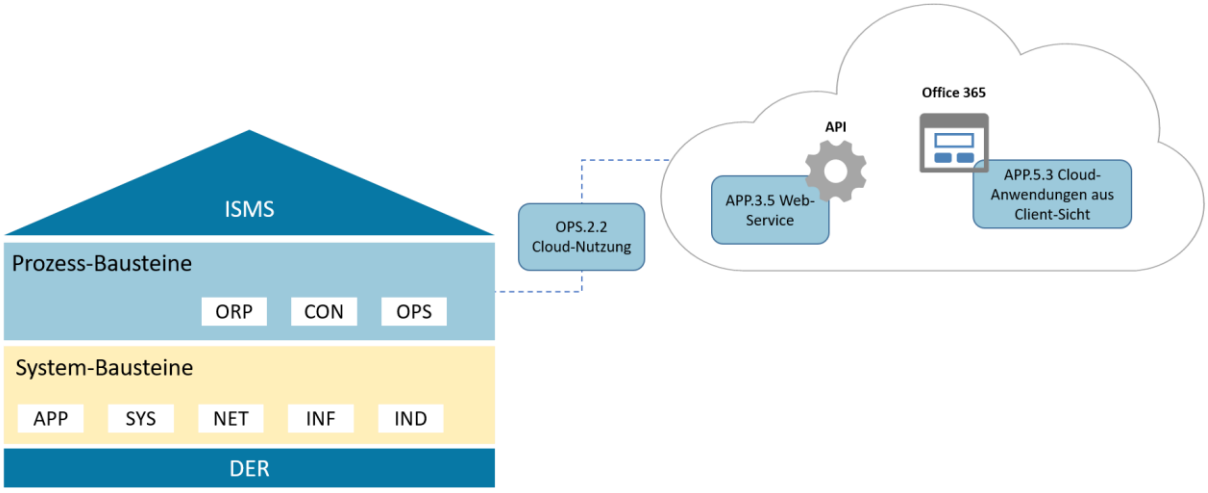

Abbildung 1 Schichtenmodell des IT-Grundschutz-Kompendiums mit Cloud-Nutzung als SaaS

Das IT-Grundschutz-Kompendium verfolgt einen schichtbasierten Ansatz zur Modellierung des Informationsverbunds. Dieses Modell besteht aus vier Schichten: dem Informationssicherheitsmanagementsystem Baustein (ISMS), Prozessbausteinen (ORP, CON, OPS), Systembausteinen (APP, SYS, NET, INF, IND) und Detektions- und Reaktionsbausteinen (DER). Wie in Kapitel 2.1 erläutert, teilt der Ansatz der gemeinsamen Verantwortung die Verantwortlichkeiten für die einzelnen IT-Grundschutz-Bausteine und die darin enthaltenen Anforderungen zwischen dem Kunden und Microsoft auf. Da Office 365 durch das Bereitstellungsmodell Software as a Service (SaaS), werden in diesem Leitfaden nur die gemeinsamen Verantwortlichkeiten für SaaS behandelt. Nach dem IT-Grundschutz-Ansatz ist Microsoft als Cloud-Diensteanbieter für den gesamten Cloud-Computing Stack verantwortlich, vom Rechenzentrum über Server und Netzwerke bis hin zur SaaS-Anwendung. Auf Kundenseite definiert der Baustein *OPS.2.2 Cloud-Nutzung*[15] die Verantwortlichkeiten des Kunden über das gesamte Auslagerungsvorhaben.

Der Baustein *OPS.2.2 Cloud-Nutzung* betrifft Anwendungen, die als Cloud-Dienst bereitgestellt werden, sowie deren Verwaltung. Das IT-Grundschutz-Kompendium[16] 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-Dienstanbietern bei der Umsetzung des Bausteins betrachtet werden.

[14] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard202/ITGStandard202_node.html

[15] 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

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

Weitere Anforderungen an die Absicherung von Office 365 aus Kundensicht werden in den neuen Bausteinen *APP.5.3 Cloudanwendungen aus Client-Sicht* und *APP.3.5 Web-Services* enthalten sein, die noch nicht veröffentlicht sind. Solange die Bausteine noch nicht veröffentlicht sind, muss eine Risikoanalyse nach der IT-Grundschutz Risikoanalysemethode[17] durchgeführt werden. Abbildung 1 zeigt, dass der Baustein *OPS.2.2 Cloud-Nutzung*[17] als Schnittstelle zwischen der lokalen Umgebung des Kunden und der Cloudumgebung des Kunden fungiert.

Abbildung 2 zeigt eine Möglichkeit, wie Office 365 in einen Informationsverbund nach IT-Grundschutz eingegliedert 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-Verbindung) als Teil des Systems mit den entsprechenden Bausteinen zur Kombination von Netzwerkkomponenten und Internetanbieter zu modellieren.

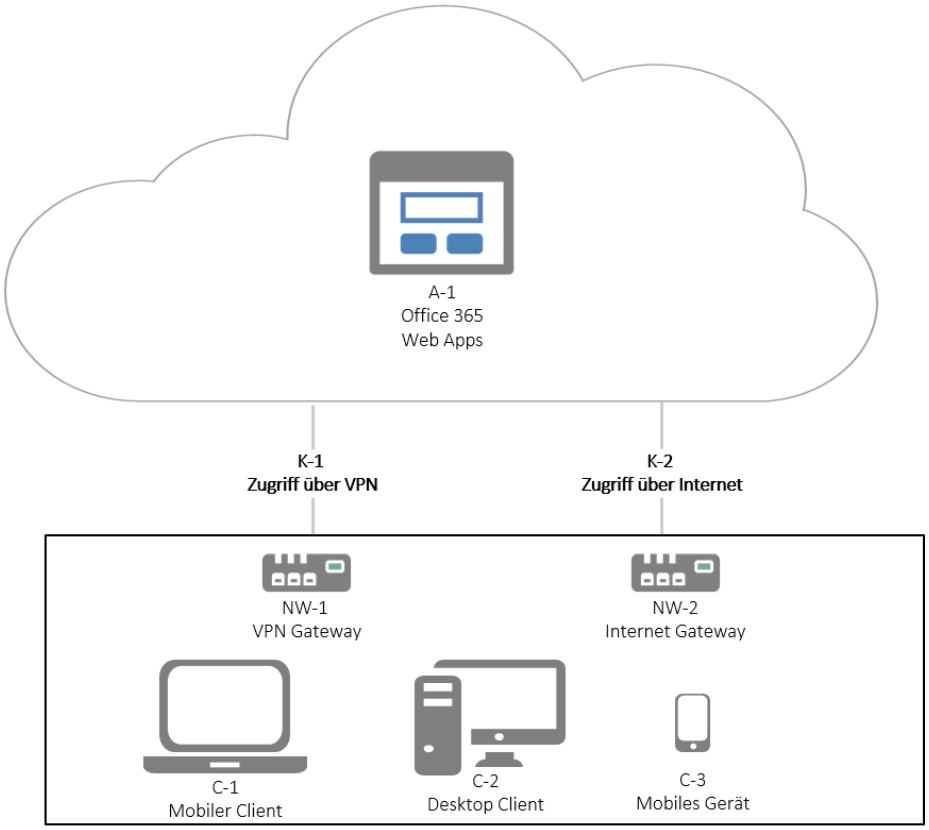

Abbildung 2 Modellierung von Office 365 in einem IT-Grundschutz-Netzplan (Beispiel)

Die im folgenden Kapitel beschriebenen Anforderungen enthalten zusätzliche Informationen, auf die sich der Baustein *OPS.2.2 Cloud-Nutzung*[18] und die entsprechenden Implementierungshinweise oder hilfreiche Online-Ressourcen von Microsoft beziehen.

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

[18] 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 Implementierung des Bausteins OPS.2.2 Cloud-Nutzung

In diesem Kapitel wird beschrieben, wie alle Anforderungen aus dem Baustein *OPS.2.2 Cloud Nutzung*[19] für Office 365 umgesetzt werden können. Im überarbeiteten IT-Grundschutz wurden die Anforderungen von den Umsetzungshinweisen getrennt. Die Umsetzungshinweise für die *OPS.2.2 Cloud Nutzung*[20] enthalten konkrete Sicherheitsmaßnahmen, mit denen die Anforderungen umgesetzt werden können.

Während einige Anforderungen nur individuell durch 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 2: Überblick über die Anforderungen, für die Microsoft unterstützende Informationen bereitstellen kann.

Anforderung	Unterstützende Informationen von Microsoft?	Beschreibung
OPS.2.2.A1 Erstellung einer Cloud-Nutzungs-Strategie	Ja	Microsoft hat den Leitfaden „Enterprise Cloud Strategy“[21] veröffentlicht, um Anwender bei der Formulierung einer Cloud-Nutzungsstrategie zu unterstützen.
OPS.2.2.A2 Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung	Ja	Die Sicherheitsanforderungen und -verfahren für die Nutzung von Office 365 innerhalb einer Institution müssen definiert werden. Die Institution wird mit Einzelheiten versorgt, die bei der Definition von Sicherheitsanforderungen in Bezug auf die Vertraulichkeit, Integrität und Verfügbarkeit der von Office 365 verarbeiteten Informationen helfen.

[19] 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

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

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

Anforderung	Unterstützende Informationen von Microsoft?	Beschreibung
OPS.2.2.A3 Service-Definition für Cloud-Dienste durch den Anwender	Ja	Diese Anforderung berücksichtigt zusätzliche praktische Anforderungen an Office 365 in Bezug auf sichere Authentifizierung, Verschlüsselung und Interoperabilität von Office 365. Microsoft stellt Informationen über Funktionen zur Verfügung, die der Kunde zur Datensicherung nutzen kann.
OPS.2.2.A4 Festlegung von Verantwortungsbereichen und Schnittstellen	Ja	Diese Anforderung betrifft die Aufteilung der Verantwortungen zwischen dem Cloud-Diensteanbieter und dem Cloud-Kunden. Die Verantwortlichkeiten der einzelnen Parteien sind in der Dokumentation von Microsoft beschrieben.[22] Microsoft bietet verschiedene Schnittstellen zur Anbindung anderer Systeme oder Dienste und zur Administration von Office 365 an.
OPS.2.2.A5 Planung der sicheren Migration zu einem Cloud-Dienst	Ja	Microsoft stellt detaillierte Informationen zu Sicherheitsaspekten zur Verfügung, die bei der Migration auf Office 365-Onlinedienste zu berücksichtigen sind.[23]
OPS.2.2.A6 Planung der sicheren Einbindung von Cloud-Diensten	Ja	Diese Anforderung trägt zur sicheren Integration von Office 365 in die Kundenumgebung bei.[24]
OPS.2.2.A7 Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung	Ja	Obwohl es keine generische Vorlage für die Anforderungen jeder einzelnen Institution gibt, befasst sich Office 365 mit den meisten technischen Bedrohungen und Sicherheitsmaßnahmen, die in der Anforderung erwähnt werden, um die Institution bei der Erstellung eines Sicherheitskonzepts für Office 365 zu unterstützen.
OPS.2.2.A8 Sorgfältige Auswahl eines Cloud-Dienstanbieters	Ja	Microsoft bietet Unterstützung für die Evaluierung von Office 365 an.

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

[23] https://docs.microsoft.com/de-de/exchange/mailbox-migration/office-365-migration-best-practices

[24] https://docs.microsoft.com/de-de/microsoft-365/enterprise/microsoft-365-integration

Anforderung	Unterstützende Informationen von Microsoft?	Beschreibung
OPS.2.2.A9 Vertragsgestaltung mit dem Cloud-Diensteanbieter	Ja	Detaillierte Informationen zu den vertraglichen Vereinbarungen zwischen dem Kunden und Microsoft werden in dieser Anforderung betrachtet.
OPS.2.2.A10 Sichere Migration zu einem Cloud-Dienst	Ja	Diese Anforderung umfasst die Durchführung der zuvor geplanten Migration. Microsoft bietet Tools zur Unterstützung bei der Migration aktueller Ressourcen nach Office 365 an.
OPS.2.2.A11 Erstellung eines Notfallkonzeptes für einen Cloud-Dienst	Ja	Das Notfallkonzept muss individuell für Office 365 entwickelt werden. Dabei sind die entsprechenden Service Level zu berücksichtigen. Es werden allgemeine Richtlinien und Informationen bereitgestellt.
OPS.2.2.A12 Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb	Ja	Es werden Informationen über die Aufrechterhaltung eines hohen Niveaus der Informationssicherheit sowie über Verfahren zur Verfügung gestellt, mit denen der Benutzer die festgelegten Ansprüche, insbesondere die Einhaltung der Office 365 SLA, überprüfen kann.
OPS.2.2.A13 Nachweis einer ausreichenden Informationssicherheit bei der Cloud-Nutzung	Ja	Microsoft stellt Informationen über Zertifizierungen, die entsprechenden Auditberichte und andere sicherheitsrelevante Informationen, wie z. B. Penetrationstestberichte, zur Verfügung.
OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses	Ja	Informationen und Anleitungen zum Exportieren von in Office 365 gespeicherten Daten nach Beendigung eines Office 365-Abonnements werden bereitgestellt. Hierzu gehören auch Informationen zur Kündigung und Richtlinien zur Löschung von Kundendaten.
OPS.2.2.A15 Portabilität von Cloud-Diensten	Ja	Portabilitätsaspekte für Office 365 werden anhand von Beispielen betrachtet.

Anforderung	Unterstützende Informationen von Microsoft?	Beschreibung
OPS.2.2.A16 Durchführung eigener Datensicherungen	Ja	Datensicherungen müssen von der Institution initiiert werden; entweder direkt oder über einen Drittanbieter. Office 365 bietet integrierte Funktionen zur Datensicherung und -wiederherstellung.
OPS.2.2.A17 Einsatz von Verschlüsselung bei Cloud-Nutzung	Ja	Microsoft hat Informationen darüber veröffentlicht, wie Office 365 die Verschlüsselung von Daten während der Übertragung und im Ruhezustand ermöglicht, um gegebenenfalls erhöhte Schutzanforderungen zu erfüllen.
OPS.2.2.A18 Einsatz von Verbunddiensten	Ja	Verbunddienste werden über den Microsoft Azure-Dienst Azure Active Directory bereitgestellt, der für die Verwaltung von Benutzern und Gruppen in Office 365 verwendet werden kann.
OPS.2.2.A19 Sicherheitsüberprüfung von Mitarbeitern	Ja	Im Rahmen hoher Sicherheitsanforderungen sind Hintergrundüberprüfungen der Mitarbeiter des Cloud-Diensteanbieters und seiner Subunternehmer 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 Office 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 Office 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, die sich auf die Institution auswirken, betrachtet. Dazu gehört auch die Berücksichtigung rechtlicher Aspekte sowie technischer und sicherheitsrelevanter Anforderungen. Infolgedessen sollten das Bereitstellungsmodell für Cloud-Dienste und erste Cloud-Sicherheitsanforderungen identifiziert werden.

Microsoft hat einen allgemeinen Leitfaden für die Erstellung einer Cloud-Nutzungsstrategie veröffentlicht. Dieser Leitfaden beantwortet wichtige Fragen und liefert erfahrungsbasierte Empfehlungen zu Themen, wie Cloud-Strategie, Cloud-Dienst-Modellen und Sicherheitsaspekte.[25] Der Leitfaden deckt auch verschiedene Migrationsszenarien für Office 365 ab.

Der Kunde muss entscheiden, welche Anwendungen oder Dienste auf Office 365 migriert werden sollen. Dies kann die teilweise Integration von Diensten (z. B. über Office 365 Online, aber einen lokal betriebenen Outlook/Exchange-Dienst) oder die Integration von lokal betriebenen operativen Diensten (z. B. Integration von lokalem Active Directory) bedeuten.

Je nach gewähltem Microsoft 365 oder Office 365-Plan[26] gibt es verschiedene Lösungen mit unterschiedlichem Integrations- und Verbindungsgrad zwischen Cloud-Diensten, lokalen Diensten und Client-Anwendungen. Die am besten geeignete Strategie variiert von Kunde zu Kunde. Die folgende Tabelle beschreibt zwei mögliche Varianten mit unterschiedlicher Komplexität für verschiedene Integrationsszenarien. Die optimale Lösung liegt in der Regel für jeden Kunden zwischen den beiden in der Tabelle aufgeführten Varianten.

Tabelle 3: Unterschiedliche Komplexität der Office 365-Integration

Geringe Komplexität der Integration	Hohe Komplexität der Integration
Ausschließlich Cloud-Dienste, weniger Administrations- und Kontrollfunktionen	Cloud-Dienste im Zusammenhang mit lokalen Diensten (z. B. Exchange, SharePoint und Active Directory)
Zwei-Faktor-Authentifizierung nur über Microsoft-Funktionen möglich	Alternative Zwei-Faktor-Authentifizierung möglich (z. B. über Smartcards)
Keine Verbindung und Synchronisation zwischen Cloud-Diensten und lokalen Diensten, höhere administrative Anforderungen (z. B. Benutzerverwaltung)	Hohe Integration und Synchronisation zwischen Cloud-Diensten und lokalen Diensten bedeutet geringeren Verwaltungsaufwand, fein abgestuftes Benutzerzugriffsmanagement, sowie automatisierte Anwendungs- und Lizenzbereitstellung verfügbar.
Hohe Abhängigkeits- und Verfügbarkeitsanforderungen an die Internetverbindung	Synchronisierte Online- und Offline-Verarbeitung von Geschäftsinformationen
Webbasierte Office 365-Anwendungen	Webbasierte und lokale Installation von Office 365-Anwendungen

Weiterführende Informationen zum Abgleich der Anforderungen mit den Office 365-Angeboten befinden sich in Anhang B.

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

[26] https://docs.microsoft.com/de-de/office365/servicedescriptions/office-365-platform-service-description/office-365-plan-options

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

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

Microsoft stellt Office 365-spezifische Informationen zur Verfügung, um Institutionen bei der Erstellung ihrer Sicherheitsrichtlinien in Bezug auf Datenschutz, Compliance, Transparenz und anderen individualisierten Kundenanforderungen zu unterstützen[27]. Der Inhalt einer Richtlinie für die Nutzung der Cloud hängt von den genehmigten Bereitstellungsmodellen und Cloud-Diensten ab. Die folgende Tabelle listet Informationen über Sicherheits- oder Compliance-Anforderungen auf, die vom gewählten Cloud-Diensteanbieter erfüllt werden können.

Tabelle 4: Nützliche Informationen zu den Compliance-Anforderungen für eine Sicherheitsrichtlinie zur Cloud-Nutzung

Compliance-Anforderung	Implementierung in Office 365	Referenzen
Identitäts- und Berechtigungsmanagement	Office 365 verwendet Azure Active Directory zur Verwaltung von Identitäten und Authentifizierung. Office 365 unterstützt Identitäten, die sowohl lokal als auch in der Cloud verwendet werden (hybride Identitäten), als auch Identitäten, die ausschließlich in der Cloud verwendet werden. Hybride Identitäten werden lokal verwaltet und mit Azure Active Directory synchronisiert (mit oder ohne Übertragung des Passworthashes). Azure Active Directory bietet verschiedene Möglichkeiten, hybride Identitäten für Office 365 zu verwenden: • Die Passwort-Hash-Synchronisation (PHS) synchronisiert lokale Konten, einschließlich eines Hashwerts des Passwort-Hash nach Azure Active Directory.	https://docs.microsoft.com/de-de/microsoft-365/enterprise/about-microsoft-365-identity 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

[27] https://docs.microsoft.com/de-de/microsoft-365/security/
https://docs.microsoft.com/de-de/compliance/assurance/assurance-risk-assessment-guide

Compliance-Anforderung	Implementierung in Office 365	Referenzen
	• Die Pass-through-Authentifizierung (PTA) ermöglicht es einem Benutzer, sich mit seinen lokalen Anmeldeinformationen bei Azure anzumelden, und Azure validiert dann das Passwort mit Hilfe des lokalen Active Directory. • Beim Active Directory Federation Service ist ein Vertrauensverhältnis zwischen Azure Active Directory und einem lokalen Active Directory hergestellt. Die Benutzer werden anhand des lokalen Active Directory authentifiziert. Office 365 unterstützt rollenbasierte Zugriffskontrolle (RBAC) und bietet mehrere integrierte Rollen. Neben internen Konten einer Institution oder Firma ermöglicht Office 365 das Hinzufügen und Verwalten von Gastkonten und externen Partnern (Business-to-Business, B2B). Office 365 unterstützt mehrere Multi-Faktor-Authentifizierungs-(MFA)-Methoden, z. B. über mobile App, Smartcard oder bestimmte MFA-Lösungen von Drittanbietern. Der Dienst Privileged Identity Management (PIM) ermöglicht die Verwaltung und Überwachung des administrativen Zugriffs auf Office 365. So kann beispielsweise der Zugriff mit privilegierten Berechtigungen zeitlich begrenzt werden. Die Funktion für den bedingten Zugriff (sog. Conditional Access) von Azure Active Directory kann auch für Office 365 verwendet werden. Mit dieser Funktion können Office 365-Kunden automatisierte Zugriffskontrollentscheidungen für den Zugriff auf Daten und Anwendungen in Office 365 hinzufügen, die zustandsabhängig sind. Weitere Informationen und Links zu Verschlüsselungs- und Kryptofunktionen befinden sich in der Tabelle 10 im Kapitel 3.17	https://docs.microsoft.com/de-de/azure/active-directory/external-identities/o365-external-user https://docs.microsoft.com/de-de/microsoft-365/admin/add-users/about-admin-roles https://docs.microsoft.com/de-de/azure/active-directory/authentication/concept-mfa-licensing https://docs.microsoft.com/de-de/azure/active-directory/privileged-identity-management/pim-configure https://docs.microsoft.com/de-de/azure/active-directory/conditional-access/overview https://docs.microsoft.com/de-de/microsoft-365/admin/basic-mobility-security/set-up https://docs.microsoft.com/de-de/mem/intune/fundamentals/what-is-intune https://docs.microsoft.com/de-de/microsoft-365/compliance/encryption

Compliance-Anforderung	Implementierung in Office 365	Referenzen
	OPS.2.2.A17 Einsatz von Verschlüsselung bei Cloud-Nutzung. Mit Mobile Device Management (MDM) oder Intune können mobile Geräte, die auf Office 365 zugreifen dürfen, gesichert und konfiguriert werden.	
Asset Management	Ressourcen, Benutzer und Gruppen können über das Admin-Center von Office 365 verwaltet werden. Office 365 ermöglicht es, Daten entsprechend der Vertraulichkeit zu kennzeichnen und die Schutzeinstellungen basierend auf den Labels automatisch durchzusetzen. Microsoft Information Protection (MIP) kann bei der Klassifizierung von Daten helfen und kann verwendet werden, um Labels zu vergeben und optional zusätzliche technische Sicherheitsmaßnahmen zu treffen. Die Labels können automatisch auf der Grundlage von Regeln / Bedingungen oder manuell zugeordnet werden.	https://docs.microsoft.com/en-us/microsoft-365/admin/admin-overview/about-the-admin-center https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection
Schutz der Daten	Die Mandantentrennung innerhalb von Office 365 wird mit unterschiedlichen technischen Mitteln realisiert. Dazu gehören die logische Trennung durch rollenbasierte Zugriffskontrolle, Verschlüsselung und Trennung auf der Speicherebene für SharePoint. Gespeicherte und übertragene Daten können mit kryptographischen Methoden und Protokollen, die dem Stand der Technik entsprechen, wie AES, IPSec oder TLS/SSL verschlüsselt werden. Beispielsweise E-Mails und Anhänge, die in der Office 365-Mailbox gespeichert sind, oder die Kommunikation von Geräten mit Office 365. Microsoft testet und überwacht kontinuierlich die Sicherheit von Office 365 und	https://docs.microsoft.com/de-de/compliance/assurance/assurance-microsoft-365-isolation-controls https://docs.microsoft.com/de-de/microsoft-365/compliance/encryption https://docs.microsoft.com/de-de/compliance/assurance/assurance-monitoring-and-testing https://servicetrust.microsoft.com/ViewPage/TrustDocuments https://docs.microsoft.com/de-de/microsoft-365/enterprise/view-service-health

Compliance-Anforderung	Implementierung in Office 365	Referenzen
	ergreift entsprechende Maßnahmen. Entsprechende Berichte, z. B. für Penetrationstests oder Audits, sind über das Trust Center zugänglich. Der Dienstzustand von Office 365 kann auf der Office 365 Service Health Seite im Office 365 Admin-Center eingesehen werden. Office 365 verfügt über eine detaillierte Protokollierungsfunktionalität. Die Protokolle sind in einem einheitlichen und durchsuchbaren Format zugänglich, das es ermöglicht, die Benutzer- und Administratoraktivitäten in Office 365 anzuzeigen. Daten können automatisch auf der Grundlage von zugewiesenen Datenkennzeichnungen geschützt werden, z. B. durch automatische Verschlüsselung oder mit Data Loss Prevention (DLP)-Schutzmaßnahmen.	https://status.office365.com/ (in Englisch) https://docs.microsoft.com/de-de/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance https://docs.microsoft.com/de-de/microsoft-365/compliance/sensitivity-labels https://docs.microsoft.com/de-de/microsoft-365/compliance/encryption-sensitivity-labels https://docs.microsoft.com/de-de/microsoft-365/security/office-365-security/security-roadmap
Compliance und Audit	Microsoft hat in die Prozesse investiert, um die Anforderungen der Standardvertragsklauseln der Europäischen Union zu erfüllen. Office 365 stellt sicher, dass Kunden in der Lage sind, die Anforderungen an die Benachrichtigung über Verstöße gegen die DSGVO zu erfüllen, indem es die Angabe eines Datenschutzkontaktes ermöglicht, der innerhalb von 72 Stunden über Verstöße informiert wird. Die Mitteilung enthält eine Beschreibung der Art der Verletzung, der ungefähren Auswirkungen auf die Benutzer und der Maßnahmen zur Schadensminimierung einschließlich Zeitvorgaben für die Behebung. Darüber hinaus gibt Microsoft eine Anleitung, wie die Anforderungen der Datenschutzgrundverordnung (DSGVO) in Office 365 durch den Kunden umgesetzt werden können. Dazu gehört eine	https://docs.microsoft.com/de-de/compliance/regulatory/offering-EU-Model-Clauses https://docs.microsoft.com/de-de/compliance/regulatory/gdpr-dpia-office365 https://docs.microsoft.com/de-de/compliance/regulatory/gdpr-dsr-Office365 https://docs.microsoft.com/de-de/compliance/regulatory/gdpr-breach-Office365 https://docs.microsoft.com/de-de/compliance/regulatory/gdpr-arc-Office365 https://docs.microsoft.com/de-de/compliance/regulatory/offering-ISO-27018

Compliance-Anforderung	Implementierung in Office 365	Referenzen
	Checkliste zur Vorbereitung auf die Rechenschaftspflicht, eine Vorlage für eine Datenschutz-Folgenabschätzung und die angemessene Beantwortung von Anfragen der betroffenen Personen. Microsoft erfüllt mit seinen Cloud-Diensten verschiedene nationale und internationale Compliance-Anforderungen und lässt diese von Dritten zertifizieren oder bescheinigen. Die entsprechenden Zertifikate oder Bescheinigungen werden im Trust Center veröffentlicht. Office 365 bietet mehrere Protokollier- und Berichtsfunktionen, darunter ein einheitliches Protokoll mit Suchfunktionen, um Benutzer- oder Administratoraktivitäten nachzuvollziehen. Microsoft stellt detaillierte Dokumentationen zur Verfügung, wie mit Office 365 Sicherheit und die Einhaltung gesetzlicher oder regulatorischer Standards erreicht werden können. Office 365 ermöglicht die Definition von Datenerhaltungsrichtlinien zur effektiven Verwaltung von Daten in Übereinstimmung mit Richtlinien, Vorschriften und gesetzlichen Anforderungen. Die Datenerhaltungsrichtlinien können sicherstellen, dass Inhalte nicht vor Ablauf einer Aufbewahrungsfrist dauerhaft gelöscht werden können. Darüber hinaus können die Richtlinien dazu verwendet werden, Inhalte nach Ablauf der Aufbewahrungsfrist dauerhaft zu löschen. Microsoft gibt einen Überblick über seine Datenspeicherorte für Office 365. Compliance Manager ist ein workflowbasiertes Risikobewertungswerkzeug zur Verfolgung, Zuweisung und Überprüfung von Compliance-Aktivitäten im Zusammenhang mit Office 365. Es bietet ein zentralisiertes Dashboard für Standards,	https://docs.microsoft.com/de-de/compliance/regulatory/offering-home https://docs.microsoft.com/de-de/compliance/assurance/assurance-auditing-and-reporting-overview https://docs.microsoft.com/de-de/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance https://docs.microsoft.com/de-de/microsoft-365/ https://docs.microsoft.com/de-de/microsoft-365/compliance/retention https://docs.microsoft.com/de-de/microsoft-365/enterprise/o365-data-locations https://docs.microsoft.com/de-de/microsoft-365/compliance/compliance-manager https://docs.microsoft.com/de-de/microsoft-365/compliance/ediscovery https://docs.microsoft.com/de-de/microsoft-365/compliance/overview-ediscovery-20

Compliance-Anforderung	Implementierung in Office 365	Referenzen
	Vorschriften und Implementierung, einschließlich der Ergebnisse für Dienstbewertungen. Electronic Discovery (eDiscovery) ist der Prozess zur Identifizierung und Bereitstellung elektronischer Informationen, die als Beweismittel in rechtlichen Verfahren verwendet werden können. Der eDiscovery-Dienst ermöglicht die Suche, Identifizierung, Aufbewahrung und den Export von Inhalten aus Office 365. Die Verwendung der erweiterten eDiscovery-Lösung ermöglicht beispielsweise eine weitergehende Analyse der von eDiscovery gefundenen Inhalte.	
Sicherung und Archivierung	Office 365 bewahrt permanente Dateien aller Daten, in einem nicht wiederbeschreibbaren, nicht löschbaren Format auf. Dies erfolgt unter Verwendung von Aufbewahrungs- und Archivierungsrichtlinien einschließlich einer Aufbewahrungssperre. Datenresilienz und Wiederherstellbarkeit sind in Office 365 integriert, um die Zuverlässigkeit zu maximieren und negative Auswirkungen auf die Kunden zu minimieren. Dies wird durch eine Kombination aus physischer Infrastruktur und Softwarelösungen erreicht, z. B. durch das Speichern von Kopien von Kundendaten in verschiedenen Fehlerzonen oder in so vielen Fehlerdomänen wie möglich. Exchange Online Backup und Archivierung kann vom Kunden mit Exchange Online Archivierung realisiert werden, um Postfachdaten in verschiedenen Rechenzentren zu speichern. Darüber hinaus können Lösungen von Drittanbietern eingesetzt werden, um Datensicherungen und Datenarchive für verschiedene Office 365-Dienste zu realisieren.	https://docs.microsoft.com/de-de/compliance/assurance/assurance-data-immutability https://docs.microsoft.com/de-de/compliance/assurance/assurance-data-resiliency-overview https://docs.microsoft.com/de-de/sharepoint/safeguarding-your-data https://docs.microsoft.com/de-de/exchange/back-up-email

Compliance-Anforderung	Implementierung in Office 365	Referenzen
Bedrohungsschutz	Microsoft bietet Schutz gegen Distributed Denial of Service (DDoS)-Angriffe mithilfe von den drei Kernprinzipien Absorption, Erkennung und Eindämmung. Aufgrund der Größe und Menge der Cloud-Dienste von Microsoft ist es möglich, DDoS-Angriffe bis zur Erkennung und Eindämmung zu absorbieren und so den Kunden einen starken Netzwerkschutz zu bieten. Darüber hinaus können DDoS-Sicherheitslösungen von Drittanbietern eingesetzt werden, um Office 365 vor DDoS-Angriffen zu schützen. Office 365 verfügt über einen starken Malware-Schutz. Dazu gehören automatische Scans der Umgebung, mindestens wöchentliche Scans des Dateisystems, Echtzeit-Scans von Dateien beim Herunterladen, Öffnen oder Ausführen, automatische tägliche Signatur-Updates sowie das ändern, bereinigen und abmildern erkannter Malware.	https://docs.microsoft.com/de-de/compliance/assurance/assurance-microsoft-dos-defense-strategy https://docs.microsoft.com/de-de/compliance/assurance/assurance-malware-and-ransomware-protection
Änderungsmanagement	Microsoft bietet eine Anleitung, wie Kunden mit den schnellen Entwicklungen in Office 365 auf dem Laufenden bleiben und die neuesten Update-Informationen erhalten können. Hierfür stellt Microsoft eine Roadmap für laufende und geplante Updates zur Verfügung.	https://docs.microsoft.com/de-de/microsoft-365/admin/manage/stay-on-top-of-updates https://www.microsoft.com/de-de/microsoft-365/roadmap

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

Für jeden geplanten und bestellten Cloud-Dienst sollte eine Service-Definition gemäß der Cloud-Nutzungsstrategie (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-Nutzung*) festgelegt werden. Die Definition sollte auf den Mehrwert oder die angestrebten Ergebnisse der geplanten oder genutzten Dienstleistung für den Kunden hinweisen. Die Verwendung von standardisierten Dienstvorlagen im ITIL-Stil kann von Vorteil sein, wenn es in der Institution kein anderes vordefiniertes Format gibt. Im Rahmen der Dienst-Definition sollten die wichtigsten technischen Parameter definiert werden.

Microsoft stellt detaillierte Beschreibungen der mit Office 365 verfügbaren Dienste und Funktionen zur Verfügung.[28] Jeder Dienst hat seine eigene Dienstbeschreibung, die relevante Informationen für diesen Dienst enthält, z. B. eine Dienstübersicht, Voraussetzungen, Systemanforderungen, Features, die in den verschiedenen Abonnements enthalten sind, und die entsprechenden Preise.

Im Rahmen der Dienst-Definition für Cloud-Dienste sollte sich das Institut auch mit den folgenden Aspekten eingehender befassen: Auswahl der sicheren Authentifizierungsmethoden, Definition von Operational Level Agreements (OLAs), Service Level Agreements (SLAs) und weiterer Sicherheitsaspekte, wie die, die in der folgenden Tabelle beschrieben werden.

Tabelle 5: Compliance-Anforderungen an die Dienstdefinitionen

Compliance-Anforderung	Implementierung in Office 365	Referenzen
Auswahl von sicheren Authentifizierungsmethoden	Office 365 bietet grundlegende Azure Active Directory-Funktionen, einschließlich Azure Multi-Faktor-Authentifizierung (MFA). Für die Steuerung von Cloud-Diensten über das Microsoft Office 365 Portal steht eine rollenbasierte Zugriffskontrolle zur Verfügung. Abhängig vom Office 365-Plan können weitere Multi-Faktor-Authentifizierungsfunktionen verwendet werden. Azure Active Directory ermöglicht es Kunden, rollenbasierte Zugriffsrechte innerhalb der Cloud oder als Hybridlösung mit ihrem lokalen Active Directory bereitzustellen. Die Funktion „Conditional Access“ ermöglicht es, den Zugriff auf Dienste basierend auf kundendefinierbaren Bedingungen wie Quell-IP, Gerätebenutzer oder der Authentifizierungsmethode einzuschränken. Intune kann verwendet werden, um mobile Geräte zu sichern und zu konfigurieren, die auf Office 365 zugreifen dürfen.	https://docs.microsoft.com/de-de/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication https://docs.microsoft.com/de-de/azure/active-directory/authentication/concept-mfa-licensing https://docs.microsoft.com/de-de/microsoft-365/admin/add-users/about-admin-roles https://docs.microsoft.com/de-de/azure/active-directory/conditional-access/overview https://docs.microsoft.com/de-de/intune/fundamentals/what-is-intune

[28] https://docs.microsoft.com/de-de/office365/servicedescriptions/office-365-service-descriptions-technet-library

Compliance-Anforderung	Implementierung in Office 365	Referenzen
Weitere Überlegungen zu Sicherheitsaspekten	Office 365 bietet Verschlüsselungsformen für gespeicherte Daten und Daten, die übertragen werden, an (siehe auch unter *Vertraulichkeit* in der Tabelle im Kapitel 3.17 *OPS.2.2.A17 Einsatz von Verschlüsselung bei Cloud-Nutzung*). Die Customer-Lockbox ermöglicht es dem Kunden, den Zugriff auf Kundendaten von Mitarbeitern des Microsoft-Support im Rahmen von Supportfällen zu genehmigen oder zu verweigern. Die Isolierung zwischen den Tenants (Multi-Tenancy) wird auf Rechen-, Speicher-, Datenbank- und Netzwerkebene realisiert, um sicherzustellen, dass auch bei gleichem Hardwarebetrieb kein Zugriff auf die Daten anderer Kunden möglich ist. Datenresilienz und Wiederherstellbarkeit sind in Office 365 integriert, um die Zuverlässigkeit zu maximieren und negative Auswirkungen auf die Kunden zu minimieren. Dies wird durch eine Kombination aus physischer Infrastruktur und Softwarelösungen erreicht, z. B. durch das Speichern von Kopien von Kundendaten in verschiedenen Fehlerzonen oder so vielen Fehlerdomänen wie möglich. Für Exchange Online kann die Sicherung und Archivierung durch den Kunden mit Exchange Online-Archivierung realisiert werden, um Postfachdaten in verschiedenen Rechenzentren zu speichern. Darüber hinaus können Lösungen von Drittanbietern eingesetzt werden, um Backups und Archive für verschiedene Office 365-Dienste zu realisieren.	https://docs.microsoft.com/de-de/microsoft-365/compliance/encryption https://docs.microsoft.com/de-de/microsoft-365/compliance/data-encryption-in-odb-and-spo https://docs.microsoft.com/de-de/office365/servicedescriptions/skype-for-business-online-service-description/skype-for-business-online-features https://docs.microsoft.com/de-de/microsoft-365/compliance/email-encryption https://docs.microsoft.com/de-de/microsoft-365/compliance/office-365-service-encryption https://docs.microsoft.com/de-de/microsoft-365/compliance/customer-lockbox-requests https://docs.microsoft.com/de-de/compliance/assurance/assurance-microsoft-365-isolation-controls https://docs.microsoft.com/de-de/compliance/assurance/assurance-data-resiliency-overview https://docs.microsoft.com/de-de/compliance/assurance/assurance-microsoft-365-isolation-controls https://docs.microsoft.com/de-de/sharepoint/safeguarding-your-data https://docs.microsoft.com/de-de/exchange/back-up-email

Compliance-Anforderung	Implementierung in Office 365	Referenzen
Interoperabilität der Client-Software	Office 365 bietet eine Vielzahl von Funktionalitäten über Office 365 APIs. Alle Office 365 Management-APIs sind konsistent in Design und Implementierung mit der aktuellen Suite von Office 365 REST-APIs und verwenden gängige Industriestandard-Ansätze, einschließlich O-Auth v2, OData v4 und JSON.	https://docs.microsoft.com/de-de/office/office-365-management-api/office-365-management-apis-overview

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-Diensteanbieter 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 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.[29] Weitere Informationen zum Modell der gemeinsamen Verantwortung befinden sich in Kapitel 2.1 *Modell der gemeinsamen Verantwortung* am Anfang dieses Dokuments.

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 Dienst-Definition des Benutzers dokumentiert werden, die in Kapitel 3.3 *OPS.2.2.A3 Service-Definition für Cloud-Dienste durch den Anwender* behandelt wird. Anschließend kann die sichere Migration und Integration des Cloud-Dienst geplant werden.

[29] 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)

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 Aufgabenverteilungen zu berücksichtigen. Dazu gehören Verantwortlichkeiten, Test- und Transferverfahren, die für einen widerstandsfähigen und sicheren Geschäftsbetrieb von besonderer Bedeutung sind. Im weiteren Verlauf sollte die institutionseigene IT im Migrationsprozess betrachtet werden, um zu überprüfen, ob z. B. die Performance als ausreichend angesehen werden kann.

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

Um ein kontinuierliches und hohes Sicherheitsniveau zu gewährleisten, muss die Migration zu Office 365 von einer lokalen Umgebung, die möglicherweise andere Cloud-Dienste einschließt, entsprechend geplant werden.

Microsoft bietet ein Leitfaden[30] an, der Kunden bei der Migrationsplanung unterstützt. Der Leitfaden kombiniert Antworten auf wichtige Fragen mit erfahrungsbasierten Empfehlungen für eine Migration in die Cloud. Bei der Planung der Migration sollte der Kunde Sicherheitsaspekte in den verschiedenen Phasen berücksichtigen.

Die Migration zu Office 365 umfasst Datentypen wie Dateien (z. B. Dateiserver)[31] und Postfächer (z. B. Microsoft Exchange)[32]. Microsoft bietet Unterstützung für die Migration mehrerer E-Mail-Konten zu Office 365[33] und für die Migration zu SharePoint Online[34]. Zusätzlich bietet Microsoft den Dienst Fast-Track für gültige Abonnements an, die den Migrationsprozess unterstützen[35].

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 Integration von Office 365 für einen sicheren und kontinuierlichen IT-Betrieb unerlässlich. Diese Anforderung berücksichtigt Aspekte, die über die Planung der Migration hinausgehen.

---

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

[31] https://docs.microsoft.com/de-de/sharepointmigration/migrate-to-sharepoint-online
https://docs.microsoft.com/de-de/sharepointmigration/sharepoint-online-and-onedrive-migration-speed

[32] https://docs.microsoft.com/de-de/microsoft-365/compliance/use-network-upload-to-import-pst-files

[33] https://docs.microsoft.com/de-de/Exchange/mailbox-migration/mailbox-migration

[34] https://docs.microsoft.com/de-de/sharepointmigration/migrate-to-sharepoint-online

[35] https://docs.microsoft.com/de-de/fasttrack/introduction

Es gibt verschiedene Methoden, um die Integration von cloudbasierten Office 365-Funktionen vorzubereiten. Hierzu muss die Institution ein Sicherheitskonzept erstellen und dokumentieren, wie die Sicherheitsanforderungen berücksichtigt werden, die sich auf die folgenden Aspekte auswirken:

- Erforderliche Anpassungen der bestehenden IT-Landschaft
- Eignung bestehender Schnittstellen (z. B. Proxy) für die Nutzung von Office 365
- Definition des Administrationsmodells für die cloudbasierten Office 365-Funktionen, z. B. Nutzung von Azure Active Directory (Azure AD) vs. Active Directory Federation Services (ADFS)
- Informationsmanagement (Datensicherung und Datenaufbewahrungsstrategie) für in der Cloud und On-Premise gespeicherte Informationen

Zu den Integrationsmöglichkeiten von[36] Office 365 gehören:

- Hybride Nutzung (Cloud-Dienste und On-Premise Dienste) mit Synchronisation, einschließlich der Möglichkeit der Migration auf cloudbasierte Dienste und der Deaktivierung von lokalen Komponenten in einem nachgelagerten Schritt.
- Nutzung der Datenportabilität von Microsoft[37] für Exchange, SharePoint und benutzerdefinierte Domänen innerhalb der Microsoft Cloud.
- Einsatz von Drittanbieter-Tools für die Office 365- und SharePoint-Integration

Um die Verbindung zwischen Cloud-Diensten und On-Premise Diensten zu sichern, 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.[38]

Mit Microsoft Information Protection (MIP)[39] können lokale als auch in der Cloud gespeicherte Daten klassifiziert werden. Aufgrund der Klassifizierung können dann Sicherheitsmaßnahmen umgesetzt werden, wie beispielsweise, dass ein Dokument nur von einem eingegrenzten Personenkreis gelesen werden darf. Im Rahmen dieser Anforderung sollte entschieden werden, inwieweit die Funktionalitäten ins lokale Netzwerk eingebunden werden.[40]

Zusätzlich wird eine Lernplattform angeboten, auf der viele spezifische unterstützende Inhalte für Schulungszwecke zu finden sind.[41]

Mit dem Evergreen-Ansatz ist Microsoft bestrebt, alle Office 365-Dienste und die gesamte Plattform sicher, konform und mit kontinuierlichen Updates immer auf dem neuesten Stand zu halten. Dieser Ansatz bringt neue Verantwortlichkeiten für die Kunden im Bereich Änderungsmanagement mit sich, da sie Änderungen in der Nutzung oder, falls erforderlich, in ihren Geschäftsprozessen berücksichtigen müssen.

---

[36] https://docs.microsoft.com/de-de/microsoft-365/enterprise/about-microsoft-365-identity
https://docs.microsoft.com/de-de/microsoft-365/enterprise/microsoft-365-integration

[37] https://docs.microsoft.com/de-de/openspecs/data_portability/ms-dataportlp/a2bc1311-e0e7-4808-970a-4dc0a100f708
https://docs.microsoft.com/de-de/office365/servicedescriptions/exchange-online-service-description/interoperability-connectivity-and-compatibility

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

[39] https://docs.microsoft.com/de-de/microsoft-365/compliance/information-protection

[40] https://docs.microsoft.com/de-de/microsoft-365/compliance/dlp-learn-about-dlp

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

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

Basierend auf den identifizierbaren Anforderungen (siehe Kapitel 3.2 *OPS.2.2.A2 Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung*) sollte ein Sicherheitskonzept für die Nutzung von Office 365 als Cloud-Dienst entwickelt werden. Gefährdungen ergeben sich aus Vertragsmängeln, Abhängigkeiten oder Verantwortlichkeiten. Sie führen zu Kontrollverlust und ineffizienter Leistung. Es sind mehrere Parteien beteiligt, insbesondere im Hinblick auf die Cloud-Dienste. Zumindest die folgenden Parteien sollten berücksichtigt werden: Cloud- Kunde, Microsoft als Cloud-Diensteanbieter und der Netzbetreiber.

Obwohl es keine generische Vorlage für die Anforderungen einer Institution gibt, geht Microsoft Office 365, wie folgt dargestellt, auf viele der in den offiziellen Implementierungsempfehlungen im IT-Grundschutz genannten Bedrohungen und Abhilfemaßnahmen ein.

Tabelle 6: Gefährdungen, die im Sicherheitskonzept für die Cloud-Nutzung zu berücksichtigen sind

Cloud-spezifische Gefährdung	Informationen Office 365	Referenzen
Geordnete oder zwangsweise Beendigung des Vertrages	Die Vertragsbeendigung wird im Rahmen einer speziellen Anforderung detailliert behandelt.	Kapitel 3.14 *OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses*
Fehlende Portabilität, z. B. aufgrund proprietärer Datenformate (möglicherweise entsteht ein Lock-in Effekt)	Portabilität wird im Rahmen einer speziellen Anforderung behandelt.	Kapitel 3.15 *OPS.2.2.A15 Portabilität von Cloud-Diensten*
Fehlende Kenntnisse über den physischen Datenspeicherort	Office 365 bietet einen Überblick über die Rechenzentren innerhalb einer Region und ermöglicht die Auswahl der Regionen innerhalb eines Abonnements. Die Daten werden dann in den Rechenzentren gespeichert, die sich in dieser Region befinden. Alle Rechenzentren von Microsoft sind physisch gegen unbefugten Zugriff und verschiedene andere Bedrohungen geschützt.	https://docs.microsoft.com/de-de/microsoft-365/enterprise/o365-data-locations 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	Mit Mobile Device Management (MDM) oder Intune können mobile Geräte, die auf Office 365 zugreifen dürfen, abgesichert und konfiguriert werden. Zusammen mit dem bedingten Zugriff („Conditional Access“) kann MDM ver-	https://docs.microsoft.com/de-de/microsoft-365/admin/basic-mobility-security/set-up https://docs.microsoft.com/de-de/mem/intune/fundamentals/what-is-intune

Cloud-spezifische Gefährdung	Informationen Office 365	Referenzen
Software (PC, Laptop, Smartphone, Browser, Apps usw.) abgerufen werden	wendet werden, um den Zugriff auf bestimmte Daten oder Dienste innerhalb von Office 365 zu beschränken. Die Zugriffsbeschränkungen basieren auf mehreren festzulegenden Bedingungen: wie dem Gerätestandort, der verwendeten Authentifizierungsmethode, dem Zustand des Geräts oder der Konfiguration des verwendeten Geräts gemäß den Anforderungen des Kunden.	https://docs.microsoft.com/de-de/azure/active-directory/conditional-access/overview
Unbefugter Zugriff (z. B. durch Cloud-Diensteanbieter-Administratoren oder andere Cloud-Kunden)	Standardmäßig haben Microsoft-Mitarbeiter keinen Zugriff auf Kundendaten. Durch die Verwendung von „Lockbox" kann der Kunde Microsoft den Zugriff auf seine Daten genehmigen oder verweigern. Der Zugriff auf Kundendaten durch Microsoft-Mitarbeiter ist durch starke Sicherheitsvorkehrungen wie Multi-Faktor-Authentifizierung (MFA) und detaillierte Protokollierung und Überwachung geschützt. Auch bei gleichem Hardwarebetrieb wird die Isolation zwischen den Tenants auf Rechen-, Speicher-, Datenbank- und Netzwerkebene realisiert, um sicherzustellen, dass kein Zugriff auf die Daten anderer Kunden möglich ist. Um einen unbefugten Zugriff auf Kundendaten zu verhindern, werden sie im gespeicherten Zustand und wenn sie übertragen werden, einschließlich der Übertragung zwischen Office 365-Rechenzentren, mit Hilfe anerkannter Protokolle und kryptografischen Methoden wie AES verschlüsselt.	https://docs.microsoft.com/de-de/azure/security/fundamentals/protection-customer-data https://www.microsoft.com/de-de/trust-center/privacy/data-access https://go.microsoft.com/fwlink/p/?LinkID=2162834 (Whitepaper: How does Microsoft handle your data in the cloud?; in Englisch) https://docs.microsoft.com/de-de/microsoft-365/compliance/customer-lockbox-requests https://docs.microsoft.com/de-de/compliance/assurance/assurance-microsoft-365-isolation-controls https://docs.microsoft.com/de-de/microsoft-365/compliance/office-365-service-encryption

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

Im Anschluss an den Planungs- und Konzeptionsprozess sollte ein detailliertes Anforderungsprofil von Microsoft als Cloud-Diensteanbieter entwickelt werden. Diese Anforderungen sollten gemäß den Dienst-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 Dienstanforderungen. Ist der Mehrwert der Cloud-Lösung gering oder gar negativ, sollte die gesamte Migration in Frage gestellt oder die Dienst-Definition überprüft und gegebenenfalls angepasst werden. Bei der Kostenberechnung müssen zusätzliche Investitions- und Betriebskosten getrennt werden, so dass die Kosten für die eigene Infrastruktur und Dienstleistungen während und nach der Migration für einen bestimmten Zeitraum betrachtet werden können.

Vor der Bewertung der Angebote müssen die grundlegenden Aspekte untersucht und entsprechende Antworten eingeholt werden.[42] Wenn die Ergebnisse nicht zufriedenstellend sind, kann ein Cloud-Diensteanbieter von der weiteren Betrachtung ausgeschlossen werden. Microsoft unterstützt Due-Diligence-Prüfungen mit einer Checkliste, die auf dem internationalen Standard ISO/IEC 19086-1 basiert, dem ersten Teil von vier Normen, die einen Rahmen für Service Level Agreements im Cloud Computing definieren.[43]

Die folgende Tabelle listet Informationen auf, die vor der Migration in die Cloud gesammelt und bewertet werden sollten.

Microsoft stellt Informationen für eine gründliche Bewertung von Office 365 zur Verfügung.[44]

Tabelle 7: Zu berücksichtigende Aspekte vor der Migration zu Office 365

Zu berücksichtigende Überlegungen	Bedingungen für Office 365	Referenzen
Öffentlich zugängliche Informationen über den Anbieter (Reputation, Bewertungen und Rankings, Kerngeschäft, Performance, Cloud-Erlebnis)	Cloud-Computing gehört zu den Kerngeschäften von Microsoft und Microsoft gehört zu den am besten bewerteten Cloud-Dienstanbietern laut verschiedenen Erhebungen. Office 365 wird ständig aktualisiert und weiterentwickelt. Microsoft veröffentlicht auf seiner Webseite Roadmaps und weitere Informationen über geplante Updates für Office 365. In der Microsoft Technet Community können sich Kunden mit anderen Kunden austauschen, um weitere Informationen über Office 365 zu erhalten.	https://www.microsoft.com/en-us/investor/default.aspx (in Englisch) https://www.microsoft.com/de-de/microsoft-365/roadmap https://techcommunity.microsoft.com/t5/Office-365/bd-p/Office365General (in Englisch) https://www.microsoft.com/de-de/microsoft-365/customer-stories

[42] Kunden erhalten von Microsoft weitere Informationen und Unterstützung bei der Auswahl eines Cloud-Diensteanbieters unter https://azure.microsoft.com/de-de/overview/choosing-a-cloud-service-provider/

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

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

Zu berücksichtigende Überlegungen	Bedingungen für Office 365	Referenzen
	Microsoft stellt Kundenberichte über die Verwendung von Office 365 zur Verfügung. Microsoft bietet die Funktion Service Health im Office 365-Administrationszentrum, die den aktuellen Status von Diensten wie Office 365 anzeigt. Das Dashboard kann angepasst werden und bietet dem Benutzer die Möglichkeit, relevante Ereignisse zu verfolgen oder Ereignisalarme zu konfigurieren.	https://docs.microsoft.com/de-de/office365/enterprise/view-service-health https://login.microsoftonline.com/ https://status.office365.com/ (in Englisch) https://docs.microsoft.com/de-de/office365/servicedescriptions/office-365-platform-service-description/service-health-and-continuity
Due-Diligence	Microsoft stellt eine Checkliste für die Bearbeitung der Due-Diligence-Schritte zur Verfügung. Microsoft bietet eine breite Palette von Compliance-Angeboten, die als Grundlage für die Due-Diligence-Schritte herangezogen werden können.	https://www.microsoft.com/de-de/trust-center/compliance/due-diligence-checklist https://docs.microsoft.com/de-de/compliance/regulatory/offering-home
Zugriff durch Cloud-Diensteanbieter oder Dritte	Microsoft-Mitarbeiter haben standardmäßig keinen Zugriff auf Kunden-Tenants und Kundendaten. Wenn Zugriff erforderlich ist, ist eine Mehrfaktor-Authentifizierung zwingend erforderlich und es werden das Least-Privilege-Prinzip sowie eine permanente Protokollierung und Überwachung angewendet. Der Zugang kann vom Kunden über die Funktionen der Customer-Lockbox verweigert oder genehmigt werden. Die in Office 365 implementierte Mandantentrennung stellt sicher, dass verschiedene Tenants nicht auf die Daten anderer zugreifen können, auch wenn sie auf derselben Hardware verarbeitet oder gespeichert werden. Die Daten werden in Office 365 im gespeicherten Zustand als auch während der Übertragung verschlüsselt, so dass Unbefugte keinen Zugriff auf die enthaltenen Informationen haben.	https://www.microsoft.com/de-de/trust-center/privacy/data-access https://go.microsoft.com/fwlink/p/?LinkID=2162834&clcid=0x407 (Whitepaper: How does Microsoft handle your data in the cloud?; in Englisch) https://docs.microsoft.com/de-de/microsoft-365/compliance/customer-lockbox-requests https://docs.microsoft.com/de-de/compliance/assurance/assurance-microsoft-365-isolation-controls https://docs.microsoft.com/de-de/microsoft-365/compliance/encryption

Zu berücksichtigende Überlegungen	Bedingungen für Office 365	Referenzen
Installation von zusätzlicher Software	Auf Office 365 kann mit dem Browser oder mit zur lokalen Installation geeigneter Office-Anwendungen zugegriffen werden. Der Zugriff auf die letzteren variiert je nach Abonnementtyp.	https://www.microsoft.com/de-de/microsoft-365/microsoft-365-and-office-resources
Standorte des Cloud-Diensteanbieters	Die Kundendaten werden in der oder den vom Kunden ausgewählten geografischen Regionen gespeichert. Aus Gründen der Datenverarbeitung können Kundendaten jedoch auch außerhalb der gewählten Regionen verarbeitet werden. Zu Sicherungszwecken werden Kundendaten in andere Rechenzentren innerhalb derselben Region repliziert.	https://docs.microsoft.com/de-de/microsoft-365/enterprise/o365-data-locations
Subunternehmer des Cloud-Diensteanbieters	Microsoft veröffentlicht und aktualisiert regelmäßig eine Liste von Subunternehmern, die mit den Daten von Kunden arbeiten. 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, den Standardvertragsklauseln der EU zustimmen.	https://www.microsoft.com/en-us/download/details.aspx?id=50426 (Microsoft Dienste Lieferantenliste, in Englisch) https://go.microsoft.com/fwlink/?LinkId=2096306&clcid=0x407 (Microsoft Online Services Subprocessors List, in Englisch) https://www.microsoft.com/de-de/trust-center/privacy/data-access https://go.microsoft.com/fwlink/p/?LinkID=2162834&clcid=0x407 (Whitepaper: How does Microsoft handle your data in the cloud?; in Englisch) https://www.microsoft.com/en-us/procurement/supplier-contracting.aspx (in Englisch)
Berücksichtigung von Vertragsgrundlagen und Regelungen	Die Service Level Agreements und die Bestimmungen für Onlinedienste von Microsoft sind die Standardbedingungen für die Nutzung von Office 365-Diensten.	https://www.microsoft.com/licensing/terms/productoffering (in Englisch)

Zu berücksichtigende Überlegungen	Bedingungen für Office 365	Referenzen
	Sie werden auf der Webseite veröffentlicht und sind ohne Microsoft-Abonnement oder Office 365-Konto zugänglich.	https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services (in Englisch)
Bewertung von Dienstleistungen einschließlich Garantien	Leistungsbeschreibungen, Dokumentationen und Preisinformationen werden auf der Webseite der einzelnen Dienste veröffentlicht.	https://docs.microsoft.com/de-de/office365/servicedescriptions/office-365-service-descriptions-technet-library https://www.microsoft.com/de-de/microsoft-365/business/compare-more-office-365-for-business-plans

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

Nach der Auswahl eines oder mehrerer geeigneter Cloud-Diensteanbieter sollten die relevanten Aspekte in vertraglichen Service Level Agreements definiert werden. Die vertraglichen Vereinbarungen zwischen dem Kunden und dem Cloud-Diensteanbieter sollten in Art, Umfang und Detaillierungsgrad mit den Schutzbedarfsanforderungen der in Office 365 verarbeiteten Daten konform sein. Die zuvor definierten Anforderungen sind zu berücksichtigen und mindestens die folgenden Punkte sind in Bezug auf Office 365 zu beantworten.

Tabelle 8: Inhalt, der bei der Vertragsgestaltung berücksichtigt werden sollte

Vertragsunterlagen	Bedingungen für Büro 365	Referenzen
Physischer Standort der Dienste und Cloud-Diensteanbieter	Die Cloud-Dienste werden in Rechenzentren in der vom Kunden gewählten Region betrieben. Die Kundendaten werden in der vom Kunden ausgewählten Region gespeichert. Aus Gründen der Datenverarbeitung können Kundendaten jedoch außerhalb der gewählten Region verarbeitet werden. Bis Ende 2022 wird die Datenspeicherung und -verarbeitung für u.a. Office 365 ausschließlich in Europa stattfinden.	https://docs.microsoft.com/de-de/microsoft-365/enterprise/o365-data-locations https://azure.microsoft.com/de-de/global-infrastructure/geographies/ https://docs.microsoft.com/de-de/compliance/assurance/assurance-datacenter-security https://techcommunity.microsoft.com/t5/security-compliance-and-identity/eu-data-boundary-for-the-microsoft-

Vertragsunterlagen	Bedingungen für Büro 365	Referenzen
	Alle Rechenzentren sind physisch gegen unbefugten Zugriff und andere typische Bedrohungen geschützt. Microsoft hat verschiedene Sicherheitsvorkehrungen getroffen und bietet diese an, um die Verfügbarkeit der Dienste zu gewährleisten.	cloud-frequently-asked/bap/2329098 (in Englisch)
Überwachung der Leistungserbringung	Microsoft bietet die Funktion Service Health im Office 365-Administrationszentrum, die den aktuellen Status von Diensten wie Office 365 anzeigt. Kunden können die Service-Statusseite auf bekannte Probleme überprüfen, die verhindern, dass sich Kunden bei ihrem Tenant anmelden können.	https://docs.microsoft.com/de-de/microsoft-365/enterprise/view-service-health https://admin.microsoft.com/ https://status.office365.com/ (in Englisch) https://docs.microsoft.com/de-de/office365/servicedescriptions/office-365-platform-service-description/service-health-and-continuity
Subunternehmer und Dritte, die an der Erbringung von Dienstleistungen beteiligt sind.	Microsoft setzt Subunternehmer für spezifische, begrenzte Supportaufgaben ein. Eine Liste mit allen Subunternehmern und eine separate Liste mit Subunternehmern mit möglichem Zugriff auf Kundendaten ist öffentlich zugängig.	https://www.microsoft.com/en-us/download/details.aspx?id=50426 (Microsoft Dienste Lieferantenliste, in Englisch) https://go.microsoft.com/fwlink/?LinkId=2096306&clcid=0x407 (Microsoft Online Services Subprocessors List, in Englisch) https://www.microsoft.com/en-us/procurement/supplier-contracting.aspx (in Englisch)
Regeln für das Personal des Cloud-Dienstanbieters	Das bei Microsoft beschäftigte Personal (intern und extern) verfügt über alle erforderlichen Kompetenzen und wird gemäß den internen Richtlinien überprüft.	https://www.microsoft.com/de-de/corporate-responsibility/empowering-employees (in Englisch) https://docs.microsoft.com/de-de/compliance/assurance/assurance-human-resources

Vertragsunterlagen	Bedingungen für Büro 365	Referenzen
Regeln für Kommunikationskanäle und Ansprechpartner	Die zentrale Anlaufstelle für den Kunden ist der Account Manager. Das Supportmenü im administrativen Portal von Office 365 stellt den Hauptkommunikationskanal dar. Über die Support-Webseite kann Microsoft ebenfalls kontaktiert werden.	https://support.office.com/de-de/home/contact
Regeln für Prozesse, Arbeitsabläufe und Verantwortlichkeiten	Office 365 wird als Online-Cloud-Dienst bereitgestellt und unterliegt einem umfassenden Regelwerk, einschließlich Informationssicherheitsrichtlinien (z. B. für Asset Management, Malware-Schutz). Die Aufteilung der Verantwortlichkeiten, Prozesse und Verfahren ist in der Regel in den jeweiligen Vereinbarungen festgelegt. Darüber hinaus werden dem Kunden von Office 365 vielfältige Möglichkeiten zur Unterstützung, Dienstüberwachung und zum weiteren Informationsaustausch angeboten. Microsoft veröffentlicht auf seiner Webseite Informationen über Updates, geplante Features und Entwicklungen. Das Änderungsmanagement und die Testrichtlinien sind in einem internen Richtliniendokument definiert.	https://www.microsoft.com/de-de/licensing/product-licensing/products.aspx https://status.office365.com/ (in Englisch) Kapitel 2.1 *Modell der gemeinsamen Verantwortung* https://www.microsoft.com/de-de/microsoft-365/roadmap
Bestimmungen zur Beendigung der vertraglichen Vereinbarung	Office 365 wird im Rahmen eines Jahresabonnements angeboten. Eine vorzeitige Kündigung kann möglich sein.	https://www.microsoft.com/de-de/licensing/product-licensing/products.aspx https://www.microsoft.com/de-de/microsoft-365/business/compare-more-office-365-for-business-plans Kapitel 3.14 *OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses*
Sichere Löschung der Daten durch den Cloud-	Wenn ein bezahltes Abonnement gekündigt wird oder endet, wird das	https://docs.microsoft.com/de-de/office365/Enterprise/office-

Vertragsunterlagen	Bedingungen für Büro 365	Referenzen
Diensteanbieter sicherstellen	Kundenkonto von Office 365 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.	365-data-retention-deletion-and-destruction-overview https://www.microsoft.com/en-us/trust-center/privacy/data-management https://aka.ms/DPA https://docs.microsoft.com/de-de/compliance/assurance/assurance-data-bearing-device-destruction
Notfallvorsorge	Office 365 hat Regeln für die Fortsetzung der Dienste auf dem im SLA festgelegten Niveau definiert. Zu den entsprechenden Sicherheitsvorkehrungen gehören die geografische Trennung der Rechenzentren und die kontinuierliche Replikation der Daten zwischen diesen.	https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services (in Englisch) https://docs.microsoft.com/de-de/compliance/assurance/assurance-data-resiliency-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.	https://www.microsoft.com/en-us/corporate-responsibility/lerr (in Englisch)
Externe Prüfungen und Audits	Office 365 wird aufgrund der Anforderungen mehrerer Normen und Zertifizierungen kontinuierlich auditiert. Microsoft stellt Informationen über seine Konformität, Audits und Zertifizierungen zur Verfügung - einschließlich öffentlich zugänglicher Berichte und Ergebnisse. Cloud-Kunden haben die Möglichkeit, Penetrationstests an ihren Cloud-Diensten durchzuführen. Hierüber muss Microsoft nicht gesondert informiert werden. Die Durchführung von Penetrationstests ist an die Einhaltung der von Microsoft aufgestellten Einsatzbestimmungen gebunden. Die	https://docs.microsoft.com/de-de/compliance/regulatory/offering-home https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement (in Englisch)

Vertragsunterlagen	Bedingungen für Büro 365	Referenzen
	Haupteinschränkung besteht darin, dass keine Denial of Service (DoS)-Tests erlaubt sind und auch dürfen keine andere Office 365-Kunden durch Penetrationstests gestört werden.	
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, in Übereinstimmung mit der DSGVO übermittelt werden. Infolge des Urteils des Europäischen Gerichtshofs (EuGH) vom Juli 2020, das das EU-US Privacy Shield Abkommen für ungültig erklärt hat, wurde der *Datenschutznachtrag zu den Produkten und Services von Microsoft* um den *Anhang C – Nachtrag zu zusätzlichen Schutzmaßnahmen* ergänzt. In diesem Anhang werden zusätzliche Sicherheitsmaßnahmen bezüglich der Verarbeitung personenbezogener Daten beschrieben. 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	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 (in Englisch)

Vertragsunterlagen	Bedingungen für Büro 365	Referenzen
	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 zu erkennen und darauf zu reagieren, falls die Probleme die Migration verhindern oder behindern. Gegebenenfalls sollte die Migration abgebrochen und eine Untersuchung der Probleme durchgeführt werden. Um das Risiko von signifikanten Schwierigkeiten zu verringern, sollte zunächst eine Test- oder Pilotmigration durchgeführt werden.

Microsoft FastTrack bietet eine Vielzahl von Tools, die bei der Migration aktueller Ressourcen nach Office 365 helfen.[45]

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

Als präventive Sicherheitsmaßnahme für Office 365 sollte ein Notfallkonzept entwickelt werden. Insbesondere das Fehlen eines Notfallwiederherstellungsplans kann zu langen Ausfallzeiten führen, einschließlich Produktivitätseinschränkungen und Einschränkungen bei Cloud-Diensten. Der Notfallwiederherstellungsplan sollte organisatorische und technische Aspekte enthalten. Auf der einen Seite sollten die Verantwortlichkeiten definiert und auf der anderen Seite ausfallsichere Infrastrukturen mit Redundanzen definiert werden.

Diese Anforderung deckt keine der Besonderheiten der Notfallwiederherstellung für den Cloud-Dienst selbst ab - das ist die Aufgabe von Microsoft und wird vertraglich durch die Service Level Agreements abgedeckt.[46] Stattdessen deckt diese Anforderung den individuellen Wiederherstellungsplan für eine Institution im Falle des Verlustes des Cloud-Dienste selbst oder des kurzfristigen Ausfalls ab. Es geht auch um Situationen, in denen die geltenden Service Levels die Anforderungen nicht erfüllen.

Sollten die Onlinedienste nicht verfügbar sein, kann der Notfallwiederherstellungsplan die Durchführung von Datensicherungen (siehe Kapitel 3.16 *OPS.2.2.A16 Durchführung eigener Datensicherungen)* und die Verwendung der Desktop-Version von Office 365 beinhalten. In diesem Fall muss ein Microsoft 365 oder Office 365-Plan mit Desktop-Software gewählt werden. Alternativ könnte auch die Verwendung von Office 365 als Hybridlösung in Betracht gezogen werden, um die Auswirkungen der Nichtverfügbarkeit von Onlinediensten zu verringern.

[45] https://www.microsoft.com/de-de/fasttrack/

[46] https://www.microsoft.com/de-de/licensing/product-licensing/products.aspx (in Englisch)

Bei der Verwendung von hybriden oder reinen Online-Lösungen von Office 365 sollte man auch die erhöhte Abhängigkeit von der Verfügbarkeit der Internetverbindung im Vergleich zu lokalen Lösungen berücksichtigen. Daher sollte der Notfallwiederherstellungsplan auch eine Vereinbarung mit dem Internetdienstanbieter oder eine Bestimmung für eine redundante Verbindung enthalten.

Darüber hinaus sollten Business Continuity Pläne für die relevanten Geschäftsprozesse, die von Office 365 abhängen, spezifisch und detailliert auf den Verlust der Verfügbarkeit geprüft werden. Diese ist unabhängig von der Ursache des Verfügbarkeitsverlustes zu planen (z. B. Ausfall des Internetzugangs im lokalen Netz, Ausfall beim Internet-Anbieter).

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

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

Tabelle 9: Schutzmaßnahmen zur Wahrung der Informationssicherheit

Erforderliche Sicherheitsvorkehrungen	Details zu Office 365	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 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/
Regelmäßige Überprüfung von erbrachten Dienstleistungen	Office 365 beinhaltet ein integriertes SLA-Überwachungssystem („Service Health"), das die Überprüfung der Einhaltung der Dienste ermöglicht. Dazu gehört auch das Empfangen von Meldungen der Dienste auf einem mobilen Gerät. Laut den jeweils geltenden Vertragsbedingungen, die mit den Dienstleistern geschlossen werden, behält sich Microsoft das Recht vor, Prüfungen bei Vertragspartnern durchzuführen.	http://status.office365.com/ (in Englisch) https://docs.microsoft.com/de-de/microsoft-365/enterprise/view-service-health https://www.microsoft.com/de-de/licensing/product-licensing/products.aspx https://www.microsoft.com/en-us/procurement/contracting-terms-conditions.aspx (in Englisch)

Erforderliche Sicherheitsvorkehrungen	Details zu Office 365	Referenzen
Bereitstellung von Sicherheitsnachweisen durch den Cloud-Diensteanbieter	Office 365 bietet in diesem Fall eine Vielzahl von Veröffentlichungen und Überprüfungen sowie entsprechende Zertifizierungen an. Dies kann von einem Benutzer von Office 365 auf der öffentlichen Webseite sowie in den Auditergebnissen, die im Service Trust Portal (STP) eingesehen werden können, überprüft werden.	https://servicetrust.microsoft.com/ https://www.microsoft.com/de-de/trust-center/compliance/compliance-overview https://servicetrust.microsoft.com/Documents/ComplianceReports
Regelmäßige Abstimmungsgespräche zwischen dem Cloud-Diensteanbieter und dem Kunden	Office 365 bietet eine Vielzahl von Möglichkeiten zur Unterstützung und Erfassung von Statusinformationen. Im Falle einer erheblichen Störung des Dienstes werden die Kunden kontaktiert.	http://status.office365.com/ (in Englisch) https://support.office.com/de-de/home/
Planung von Übungen und Tests zur Reaktionssimulation von Systemausfällen	Office 365 hat Regeln für die Fortführung von Diensten auf dem im SLA festgelegten Niveau definiert.	https://docs.microsoft.com/de-de/office365/servicedescriptions/office-365-platform-service-description/service-health-and-continuity https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services (in Englisch)
Sicherstellung der ordnungsgemäßen Verwaltung von Cloud-Diensten	Eine fehlerhafte Cloud-Administration kann aufgrund der sehr hohen Komplexität zu erheblichen Sicherheitsproblemen (Ausfall des Dienstes, Datenverlust etc.) führen. Schon kleine Fehler oder Ausfälle können einen großen Einfluss (nicht nur auf die Sicherheit) auf eine Cloud-Infrastruktur haben. Microsoft bietet Sicherheitsrichtlinien und eine Secure-Score-Funktionalität, um über Konfigurationen zu informieren, die als unsicher gelten könnten.	https://docs.microsoft.com/de-de/microsoft-365/security/office-365-security/reference-policies-practices-and-guidelines https://docs.microsoft.com/de-de/microsoft-365/security/mtp/microsoft-secure-score
Sicherstellung der Interoperabilität von Cloud-Diensten	Bei der Nutzung mehrerer Cloud-Dienste sollten für jeden Dienst Interoperabilitätstests durchgeführt werden, um eine ordnungsgemäße	https://www.microsoft.com/en-us/legal/interoperability/default.aspx (in Englisch) https://docs.microsoft.com/de-de/office365/servicedescriptions/exchange-online-service-

Erforderliche Sicherheitsvorkehrungen	Details zu Office 365	Referenzen
	Zusammenarbeit zwischen den verschiedenen Cloud-Diensten zu gewährleisten.	description/interoperability-connectivity-and-compatibility Kapitel 3.15 *OPS.2.2.A15 Portabilität von Cloud-Diensten*
Ordnungsgemäße Durchführung von Datensicherungen	Eine ordnungsgemäße Durchführung der Datensicherung muss gewährleistet sein, damit keine kritischen Geschäftsprozesse durch einen Ausfall gefährdet werden. Datensicherungen können entweder durch eine hybride Umgebung oder durch einen Datensicherungs-Dienst eines externen Anbieters oder eines Datensicherungs-Systems des Kunden durchgeführt werden. Wird sich für einen externen Anbieter entschieden, muss der Kunde sicherstellen, dass alle Anforderungen an Datensicherungen 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	Die IT-Organisation sollte die technischen Maßnahmen, z. B. mit Hilfe von Proxy-Servern oder Cloud Access Security Brokern (CASB), kontrollieren, um die unberechtigte Nutzung von Diensten zu verhindern. Mit dem Cloud-Dienst Microsoft Information Protection (MIP) lassen sich sowohl lokale Daten als auch in der Cloud gespeicherte Daten klassifizieren. Auf der Grundlage der Klassifizierung können dann Sicherheitsmaßnahmen implementiert werden, z. B. dass ein Dokument nur von einer begrenzten Gruppe von Personen gelesen werden darf.	https://docs.microsoft.com/de-de/azure/active-directory/users-groups-roles/roles-delegate-by-task https://docs.microsoft.com/de-de/defender-cloud-apps/what-is-defender-for-cloud-apps https://docs.microsoft.com/de-de/microsoft-365/compliance/information-protection
Durchführung von Audits, Sicherheitschecks, Penetrationstests oder Schwachstellenanalysen	Cloud-Anwender haben die Möglichkeit, Penetrationstests oder Schwachstellenscans gegen ihre Cloud-Dienste durchzuführen, ohne Microsoft zu benachrichtigen, ob die entsprechenden Einsatzregeln eingehalten werden. Die Haupteinschränkung besteht darin, dass keine Denial of Service (DoS)-Tests erlaubt sind	https://docs.microsoft.com/de-de/azure/security/fundamentals/pen-testing https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement (in Englisch)

Erforderliche Sicherheitsvorkehrungen	Details zu Office 365	Referenzen
	und dass keine anderen Kunden durch die durchgeführten Tests gestört werden dürfen.	

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 die Auditanforderungen erfüllt und auch die Vereinbarungen auf beiden Seiten eingehalten werden. Dies kann beispielsweise durch Vor-Ort-Audits oder spezifische Fragebögen unabhängig von der Art des Cloud-Dienstes erreicht werden.

Microsoft Cloud und Office 365 werden aufgrund der Anforderungen mehrerer internationaler und nationaler Compliance-Standards und Zertifizierungen kontinuierlich auditiert. Die Liste der Konformitätsnormen für Office 365 umfasst BSI C5, ISO 27001, ISO 27017 und ISO 27018 (siehe Kapitel 4 für weitere Details). Diese Audits oder Überprüfungen werden von akkreditierten Prüfstellen durchgeführt, wobei zusätzliche interne Audits von Microsoft durchgeführt werden. Informationen zu diesen Audits sind online im Microsoft Trust Center verfügbar. Darüber hinaus können sich Vertragskunden von Unternehmen und Behörden im Service Trust Portal (STP)[47] anmelden, das direkten Zugriff auf viele der Compliance-Berichte und -Zertifikate bietet.

Die Verantwortung für das Lesen und Bewerten der Berichte liegt beim Cloud-Kunden. Die Bewertung sollte nur von qualifiziertem Personal des Kunden durchgeführt werden.

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-Dienstevertrags definiert werden. In einer kritischen Situation verhindert das Fehlen vertraglicher Regelungen die Beendigung des Dienstleistungsverhältnisses. 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 Migration zu Office 365. Das Planungs- und Migrationskonzept sollte das Sicherheitskonzept genauso berücksichtigen wie bei der ursprünglichen Umstellung auf die Cloud.

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

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“[48] unterstützend zur Verfügung.

Office 365 bietet verschiedene Möglichkeiten, Kundendaten zu exportieren. Dokumente können problemlos in bestehende Microsoft-Formate wie Excel oder Word exportiert werden und Exchange-Postfächer können im.pst-Dateiformat exportiert werden. Im Allgemeinen können Office 365-Anwendungsdaten problemlos in das lokale Gegenstück importiert werden.

Mit der Hybridlösung von Office 365 können Daten mit dem lokalen IT-System synchronisiert werden.[49] Andernfalls, wenn ein Massenexport durchgeführt werden muss, stehen Lösungen von Drittanbietern zur Verfügung.

Standardmäßig können Office 365-Daten bei Vertragsbeendigung für 90 Tage exportiert werden. Kundendaten werden innerhalb von 180 Tagen nach Ablauf der vereinbarten Nutzungsdauer oder der Kündigung des Nutzungsvertrages gelöscht.[50]

Bei der Kündigung des Office 365-Vertrags als Onlinedienst sollte die Institution unter anderem Folgendes sicherstellen:

- 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.

3.15 OPS.2.2.A15 Portabilität von Cloud-Diensten

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

Office 365 unterstützt verschiedene Methoden der Datenmigration:

1. Verwendung von Office 365-APIs, die den Zugriff auf Kundendaten ermöglichen.[51]

[48] 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)

[49] https://docs.microsoft.com/de-de/office/office-365-management-api/

[50] https://docs.microsoft.com/de-de/office365/Enterprise/office-365-data-retention-deletion-and-destruction-overview

https://www.microsoft.com/de-de/trust-center/privacy/data-management

https://aka.ms/DPA

[51] https://docs.microsoft.com/de-de/previous-versions/office/office-365-api

2. Nutzung von Portabilitätsoptionen, die von den einzelnen Cloud-Diensten bereitgestellt werden. Beispielsweise das Herunterladen von Dokumenten aus SharePoint Online oder das Exportieren von Exchange-Online-Daten mit dem Import- und Export-Assistenten.[52, 53]
3. Synchronisation von Daten mit lokalen Komponenten bei Verwendung der hybriden Cloud-Lösung.[54]
4. Verwendung von Drittanbieterwerkzeugen für Office 365 zum Importieren/Exportieren von Daten.

Die Daten werden in gängigen Formaten exportiert, z. B. Microsoft Office (Word, Excel, PowerPoint etc.) oder .pst-Dateien (Exchange). Die Spezifikationen der relevanten Office Open XML- oder .pst-Dateiformate sind frei verfügbar.[55] Der Azure-Dateispeicher kann zum Speichern der Dateien verwendet werden. Da Azure File Storage das SMB-Protokoll unterstützt, können die Dateien dann über SMB auf eine Windows-Freigabe übertragen werden.[56]

Der Wechsel zu einem anderen Cloud-Diensteanbieter oder zurück zur lokalen Umgebungen sollte angemessen geplant und getestet werden. Die folgenden Fragen sollten berücksichtigt werden:

- Bietet die Zielumgebung die gleichen Funktionen wie Office 365 (Funktionalität, Sicherheit, Leistung, Skalierbarkeit etc.)?
- Ist die neue Plattform in der Lage, die exportierten Daten von Office 365 zu verarbeiten?
- Gibt es Tools von Microsoft oder Drittanbietern zur Konvertierung der Daten oder Dateiformate in die Zielformate?

3.16 OPS.2.2.A16 Durchführung eigener Datensicherungen

Diese Anforderung zielt darauf ab, die Datenverfügbarkeit sicherzustellen, wenn der Zugriff auf Office 365-Daten verloren geht, Cloud-Dienste selbst nicht verfügbar sind oder Daten durch Benutzeraktionen (z. B. versehentliches Löschen von Daten) verloren gehen.

Office 365 bietet mehrere integrierte Funktionen und Optionen zur Datenrettung, z. B. „Papierkorb", Online-Datensicherungs- oder Archivierungsfunktionen sowie Anwendungen von Drittanbietern.

Kunden sollten entscheiden, ob die Datenrettungsfunktionen und -optionen in Office 365 ihren Bedürfnissen entsprechen, z. B. gesetzlichen, vertraglichen und allgemeinen Schutzanforderungen, oder ob ein zusätzlicher Export in lokale oder andere Cloud-Datensicherungs-Speicher implementiert werden

[52] https://support.office.com/de-de/article/exportieren-von-sharepoint-nach-excel-bfb2ea48-6118-4fa9-abb6-cced9424e5d9

[53] https://support.office.com/de-de/article/herunterladen-von-dateien-und-ordnern-aus-onedrive-oder-sharepoint-5c7397b7-19c7-4893-84fe-d02e8fa5df05

[54] https://docs.microsoft.com/de-de/microsoft-365/solutions/cloud-architecture-models

[55] DOCX-Dateien: https://docs.microsoft.com/en-us/openspecs/office_standards/ms-docx/b839fe1f-e1ca-4fa6-8c26-5954d0ab-bccd (in Englisch)
XLSX- Dateien: https://docs.microsoft.com/en-us/openspecs/office_standards/ms-xlsx/2c5dee00-eff2-4b22-92b6-0738acd4475e (in Englisch)
PST- Dateien: https://docs.microsoft.com/en-us/openspecs/office_file_formats/ms-pst/141923d5-15ab-4ef1-a524-6dce75aae546 (in Englisch)

[56] https://docs.microsoft.com/de-de/azure/storage/files/storage-how-to-use-files-windows

soll. Dies sollte in der Datensicherungsrichtlinie der Institution berücksichtigt werden, die im IT-Grundschutz-Baustein *CON.3 Datensicherungskonzept*[57] als Teil des IT-Grundschutz-Kompendiums beschrieben ist. Insbesondere der Inhalt der Anforderung *CON.3.A1 Erhebung der Einflussfaktoren der Datensicherung, CON.3.A3 Ermittlung von rechtlichen Einflussfaktoren auf die Datensicherung, CON.3.A6 Entwicklung eines Datensicherungskonzepts und CON.3.A8 Funktionstests und Überprüfung der Wiederherstellbarkeit* sollten bei der Entscheidungsfindung berücksichtigt werden.

In Office 365 sind mehrere Funktionen und Schnittstellen für den Datenexport implementiert. Es gibt eine Reihe von kommerziellen Lösungen, die auch Datensicherungen in der Cloud selbst oder auf lokalem Speicher anbieten.

Bei der Entscheidung und Durchführung von Datensicherungen sollten Kunden die folgenden Aspekte berücksichtigen:

- Welche Daten oder Dateien müssen exportiert und einzeln gesichert werden?
- Welche Exportfunktionen stehen zur Verfügung?
- Entsprechen die Exportfunktionen den gesetzlichen, vertraglichen, allgemeinen Schutz- und sonstigen Anforderungen?
- Entspricht das Backup-Speichermedium (lokal oder cloudbasiert) den gesetzlichen, vertraglichen, allgemeinen Schutz- und sonstigen Anforderungen?
- Können die gesicherten Daten und Dateien wiederhergestellt werden?

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

Für die Verschlüsselung und anderen kryptographischen Schutz 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. Office 365 bietet verschiedene Verschlüsselungsoptionen mit Verschlüsselung in einer Reihe von Bereichen. Je nach gewähltem Dienst haben Kunden die Möglichkeit, die Verschlüsselung mit Standard- oder individuellen Verschlüsselungstechnologien zu aktivieren.[58] Die verschiedenen Verschlüsselungsoptionen sind dienstabhängig und müssen vom Kunden von Fall zu Fall anhand der von Microsoft für Office 365 bereitgestellten Dokumentation und Richtlinien bewertet werden.[59]

Die folgende Tabelle veranschaulicht die von Office 365 bereitgestellte Funktionalität zur Verschlüsselung von gespeicherten und übertragenen Daten als auch zur sicheren Verwaltung von Geheimnissen.

[57] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/03_CON_Konzepte_und_Vorgehensweisen/CON_3_Datensicherungskonzept_Edition_2021.pdf

[58] https://www.microsoft.com/de-de/security/operations

[59] https://docs.microsoft.com/de-de/microsoft-365/compliance/encryption

Tabelle 10: Angebote zur Verschlüsselung und Kryptographie in Office 365

Kategorie	Details	Referenzen
Verschlüsselung von Daten im gespeicherten Zustand	Office 365-Server verschlüsselt gespeicherte Kundendaten und anderen Inhalten mittels Festplattenverschlüsselung (BitLocker mit AES 256). BitLocker wird auch z. B. für die Verschlüsselung der Postfachdaten in Exchange Online verwendet. Microsoft stellt Informationen über die BitLocker-Konfiguration zur Verfügung. Die Verschlüsselung auf Dienstebene verschlüsselt alle Postfachdaten auf Postfachebene. Alle Kundendateien in Microsoft SharePoint Online und OneDrive for Business sind durch eindeutige Schlüssel pro Datei geschützt. Dateien werden verschlüsselt im angeschlossenen Azure Storage gespeichert. Microsoft Teams verwendet SharePoint Online zur Speicherung von Daten, diese Date sind mit AES 256-Bit-Schlüsseln verschlüsselt. Mit Skype for Business bietet Microsoft auch die Verschlüsselung mit AES 256-Bit-Schlüsseln für Kundendaten auf dem Webkonferenz-Server an.	https://docs.microsoft.com/de-de/compliance/assurance/assurance-encryption https://docs.microsoft.com/de-de/compliance/assurance/assurance-encryption-for-microsoft-365-services
Verschlüsselung von Daten während der Übertragung	Office 365 verschlüsselt Verbindungen mit Industriestandards wie AES und TLS/SSL. Für die E-Mail-Verschlüsselung bietet Office 365 verschiedene Optionen: Office Message Encryption (OME), Secure/Multipurpose Internet Mail Extensions (S/MIME) und Information Rights Management (IRM). Office Message Encryption und Information Rights Management basieren auf Azure Rights Management (RMS). Die Verschlüsselung wird in Office 365 standardmäßig verwendet.	https://docs.microsoft.com/de-de/compliance/assurance/assurance-encryption-in-transit https://docs.microsoft.com/de-de/microsoft-365/compliance/exchange-online-uses-tls-to-secure-email-connections https://docs.microsoft.com/de-de/microsoft-365/compliance/email-encryption

Kategorie	Details	Referenzen
	In Skype for Business werden Daten über HTTPS während Konferenzen ausgetauscht. Azure Rights Management (Azure RMS) ist Teil von Azure Information Protection (AIP). Es beinhaltet Verschlüsselungs-, Identitäts- und Autorisierungsrichtlinien. Die entsprechende Verschlüsselung ist für den Benutzer transparent.	https://docs.microsoft.com/de-de/compliance/assurance/assurance-encryption-for-microsoft-365-services https://docs.microsoft.com/de-de/microsoft-365/compliance/ome https://docs.microsoft.com/de-de/azure/information-protection/how-does-it-work
Schlüsselverwaltung und eigene Verschlüsselungsmechanismen	Als SaaS-Anwendung ist es nicht möglich, einen eigenen Verschlüsselungsmechanismus zu implementieren. Microsoft stellt für seine Online-Anwendungen ein geeignetes Key Management über eine eigene Trust Center Infrastruktur zur Verfügung. In diesem Zusammenhang bietet Microsoft Azure mit dem Key Vault Cloud-Dienst eine sichere Schlüsselverwaltung und Speicherung für andere Cloud-Dienste. Im Rahmen von Azure Rights Management kann der Kunde die Schlüssel verwalten (das "bring your own key", BYOK-Szenario). Darüber hinaus unterstützt Office 365 Kundenschlüssel, die auf Dienst-Verschlüsselung basieren und Double Key Encryption für volle Kundenkontrolle (jedoch mit dem Verlust an Funktionalität).	https://azure.microsoft.com/de-de/services/key-vault/ https://docs.microsoft.com/de-de/azure/information-protection/operations-customer-managed-tenant-key https://docs.microsoft.com/de-de/office365/enterprise/activate-rms-in-office-365 https://docs.microsoft.com/de-de/microsoft-365/compliance/controlling-your-data-using-customer-key https://docs.microsoft.com/de-de/microsoft-365/compliance/double-key-encryption

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 der Institution 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[60] SAML-Ticket an den Cloud-Diensteanbieter gesendet werden. Darüber hinaus müssen die Benutzerrechte und -rollen regelmäßig überprüft werden, um sicherzustellen, dass nur autorisierte Benutzer Zugriff haben.

Mit Azure Active Directory können sowohl lokale als auch Konten/Identitäten, die ausschließlich in der Cloud sind, verwaltet werden.[61]. Es gibt drei allgemeine Möglichkeiten, hybride Konten zu realisieren. Diese bringen unterschiedlichen Vor- und Nachteilen mit: [62]

- Password Hash Synchronization (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.[63]
- Pass-Through Authentication (PTA): PTA ermöglicht es Benutzern, sich On-Premise und in Cloudbasierten Anwendungen 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.[64]
- Active Directory Federation Services (ADFS): 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 On-Premise erfolgen und ermöglicht es Administratoren, strengere Zugriffskontrollen durchzuführen. PHS kann optional als Backup für den Fall eines ADFS-Ausfalls implementiert werden.[65]

Azure Active Directory, unterstützt das SAML 2.0 Protokoll sowie WS-Federation und OpenID Connect.[66] Die in den SAML-Tickets enthaltenen Informationen können entsprechend den organisatorischen Anforderungen oder den Anforderungen der jeweiligen Anwendung konfiguriert werden.[67]

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 Zugriffsrechtevergabe sein. Der IT-Grundschutz-Baustein *ORP.4 Identitäts- und Berechtigungsmanagement* [68] beinhaltet die Richtlinien für die Umsetzung der notwendigen Verfahren.

---

[60] SAML (Security Assertion Markup Language) ist ein Standard-Authentifizierungs- und Autorisierungsprotokoll.

[61] https://docs.microsoft.com/de-de/microsoft-365/compliance/use-your-free-azure-ad-subscription-in-office-365

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

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

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

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

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

[67] https://docs.microsoft.com/de-de/azure/active-directory/manage-apps/view-applications-portal
https://docs.microsoft.com/de-de/azure/active-directory/develop/active-directory-saml-claims-customization

[68] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs/02_ORP_Organisation_und_Personal/ORP_4_Identitaets_und_Berechtigungsmanagement_Editon_2020.pdf

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.

3.19 OPS.2.2.A19 Sicherheitsüberprüfung von Mitarbeitern

Der Kunde sollte sicherstellen, dass der Dienstleister im Rahmen der gesetzlichen Vorgaben Sicherheitsüberprüfungen von Mitarbeitern durchführt.

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

Darüber hinaus befolgt Microsoft eine strenge Dienstleisterpolitik. Für eine erfolgreiche Zusammenarbeit mit Dienstleistern und Lieferanten definiert das Dienstleisterprogramm von Microsoft die Art und Weise, wie wichtige geschäftskritische und strategische Dienstleister und Lieferanten mit Microsoft Geschäfte tätigen, einschließlich der Anforderungen und Erwartungen von Microsoft und der Kunden.[69] 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 den Dienstleister vor der Erbringung der Dienstleistung für Microsoft die eigenen Mitarbeitern einer Hintergrundüberprüfung zu unterziehen, soweit dies nach geltendem Recht zulässig ist.[70] 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.[71] Microsoft bietet auch das SCoC-Schulungsprogramm an, um die Mitarbeiter der Dienstleister und Lieferanten zu schulen.[72]

[69] https://www.microsoft.com/en-us/procurement/msp-overview.aspx?activetab=pivot1:primaryr3 (in Englisch)

[70] https://www.microsoft.com/en-us/procurement/supplier-conduct.aspx?activetab=pivot:primaryr4 (in Englisch)

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

[72] https://www.microsoft.com/en-us/procurement/supplier-conduct.aspx?activetab=pivot:primaryr5 (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 Office 365, 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*[73] für Office 365 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*[74] hinsichtlich der umzusetzenden Anforderungen auf IT-Grundschutz-Anforderungen. Die folgende Tabelle gibt einen Überblick auf die Verweise zu IT-Grundschutz Anforderungen.

Tabelle 11: 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-Nutzung*

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

[74] 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 Notfallkonzeptes 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-Nutzung*
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 Office 365 den Anforderungen dieser entspricht. Im Rahmen einer Risikoanalyse ist die Nutzung von Office 365 zu überprüfen.

Microsoft stellt Informationen zur Erstellung einer Cloud-Nutzungs-Strategie beispielsweise in Form des Leitfadens „Enterprise Cloud Strategy“[75] 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[76] und Sicherheitsmaßnahmen, die durch den Cloud-Kunden[77] durchgeführt werden können, bereit.

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-Nutzung* (siehe Kapitel 3.2) ist von der Institution, die Office 365 einsetzen möchte, eine Sicherheitsrichtlinie durch die verantwortlichen Personen zu erstellen. Der *Mindeststandard des BSI zur Nutzung externer Cloud-Dienste*[78] gibt vor, dass die Umsetzung und Einhaltung der Basiskriterien nach dem BSI Kriterienkatalog Cloud Computing (C5)[79] als spezielle Sicherheitsanforderungen an den Cloud-Diensteanbieter in der Sicherheitsrichtlinie festgelegt werden muss.

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

[76] https://docs.microsoft.com/de-de/microsoft-365/security/

[77] https://docs.microsoft.com/de-de/compliance/

[78] https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_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

Externe Prüfer haben für Office 365 die Einhaltung der Basiskriterien nach dem BSI Kriterienkatalog Cloud Computing (C5)[80] festgestellt. Der SOC 2-Bericht zur Prüfung kann im Service Trust Portal (STP)[81] eingesehen werden.

4.3 NCD.2.1.03 Sicherheitskonzept für den externen Cloud-Dienst

Neben der Cloud-Nutzungsstrategie (siehe Kapitel 4.1 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 ein 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[82] und Sicherheitsmaßnahmen, die durch den Cloud-Kunden[83] durchgeführt werden können, bereit.

So kann der Cloud-Kunde mittels Sensitivity Labels[84] eine Datenklassifizierung in Office 365 durchführen. Dies kann mittels Azure Information Protection[85] ergänzt werden, so dass aufgrund der Datenklassifizierung Richtlinien, die beispielsweise den Versand von vertraulichen Daten per E-Mail verhindern, umgesetzt werden.

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

4.4 NCD.2.1.04 Notfall- und Kontinuitätsmanagement

Wie in der IT-Grundschutz Anforderung *OPS.2.2.A11 Erstellung eines Notfallkonzeptes für einen Cloud-Dienst* (siehe Kapitel 3.11) fordert auch der *Mindeststandard des BSI zur Nutzung externer Cloud-Dienste*[86] eine Bewertung durch die Institution, wie sich ein Ausfall von Office 365 auf die Institution auswirken würde. Zusätzlich sollte zusammen mit dem zuständigen Notfallbeauftragten überprüft werden, ob sich die Nutzung von Office 365 auf die bisherige Notfallbehandlung auswirkt und somit die bisherigen präventiven / reaktiven Maßnahmen angepasst werden können.

[80] 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

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

[82] https://docs.microsoft.com/de-de/microsoft-365/security/

[83] https://docs.microsoft.com/de-de/compliance/

[84] https://docs.microsoft.com/de-de/microsoft-365/compliance/data-classification-overview

[85] https://docs.microsoft.com/de-de/microsoft-365/compliance/sensitivity-labels

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

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. So kann ein Szenario in der Notfallplanung den Einsatz von Office 365 im Home-Office vorsehen.

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

4.5 NCD.2.2.01 Umsetzung der Sicherheitsanforderungen

Vor dem Vertragsabschluss muss bewertet werden, ob Office 365 die in der Sicherheitsrichtlinie (siehe Kapitel 3.2 *OPS.2.2.A2 Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung* und 4.2 *NCD.2.1.02 Sicherheitsrichtlinie externe Cloud-Dienste*) vorgegebenen Anforderungen erfüllen kann und im Rahmen des Einsatzes von Office 365 ist regelmäßig zu überprüfen, ob die umsetzbaren Sicherheitsmaßnahmen und die vorhandenen Sicherheitsnachweise weiterhin der Sicherheitsrichtlinie entsprechen.

Microsoft stellt weitreichende Informationen zu eigenen Sicherheitsmaßnahmen[87] und Sicherheitsmaßnahmen, die durch den Cloud-Kunden[88] durchgeführt werden können, bereit.

Microsoft lässt Audits durch Kunden zu in der Microsoft Online Services DPA[89] 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 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)[90] 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.

---

[87] https://docs.microsoft.com/de-de/microsoft-365/security/

[88] https://docs.microsoft.com/de-de/compliance/

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

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

Microsoft stellt eine Liste von Subunternehmern zur Verfügung und bietet Zugang zu standardisierten Dienstvereinbarungen, Richtlinien und Verhaltensregeln.[91] Externe Prüfer haben für Office 365 die Einhaltung der Basiskriterien nach dem BSI Kriterienkatalog Cloud Computing (C5)[92] festgestellt. Der SOC 2-Bericht zur Prüfung kann im Service Trust Portal (STP)[93] 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.[94]

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

4.8 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 Office 365 gespeichert sind.[95] Darüber hinaus veröffentlicht Microsoft zweimal jährlich eine Statistik zu Anfragen von Strafverfolgungsbehörden aus der ganzen Welt.[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*.

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*

---

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

[92] 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

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

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

[95] https://docs.microsoft.com/de-de/microsoft-365/enterprise/o365-data-locations
https://docs.microsoft.com/de-de/microsoft-365/enterprise/eu-data-storage-locations

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

zur Nutzung externer Cloud-Dienste[97] auch die Vereinbarung von Vertragsvertragsstrafen bei Nichterfüllung vorsieht.

Microsoft hat eine interne Richtlinie[98] zur Benachrichtigung der betroffenen Parteien während eines Vorfalls zur Informationssicherheit. Informationen über die Informationspflichten der Personen im Rahmen der EU-DSGVO werden ebenfalls veröffentlicht[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*.

4.10 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.[101] Alle Speichergeräte, auf denen Kundendaten gespeichert

---

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

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

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

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

[101] https://docs.microsoft.com/de-de/microsoft-365/commerce/subscriptions/cancel-your-subscription

https://www.microsoft.com/de-de/trust-center/privacy/data-management

https://aka.ms/DPA

sein könnten, werden mit Hilfe eines Verfahrens gelöscht, das den Vorgaben nach NIST SP-800-88 entspricht.[102]

4.12 NCD.2.3.01 ISMS einbinden

Office 365 als Cloud-Dienst sollte in das ISMS der Institution integriert werden. Dabei sollte beachtet werden, dass die im BSI Kriterienkatalog Cloud Computing (C5)[103] 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.

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*[104] und der Risikoanalyse des Kunden umfasst. Weiterhin verpflichtet diese Anforderung den Cloud-Kunden, diese Nachweise regelmäßig hinsichtlich der Erfüllung von Sicherheitsanforderungen zu überprüfen.

Office 365 verfügt über mehrere globale und regionale Zertifizierungen[105]. Darüber hinaus werden Auditberichte und andere Compliance-Informationen, wie z. B. Penetrationstests, regelmäßig auf der Webseite von Microsoft veröffentlicht[106,107]. Die Verantwortung für die Definition der erforderlichen Zertifizierungen und die Überprüfung, ob Office 365 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 An-

---

[102] https://docs.microsoft.com/de-de/compliance/assurance/assurance-data-bearing-device-destruction

[103] 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

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

[105] https://docs.microsoft.com/de-de/microsoft-365/compliance/offering-home

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

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

forderungen 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.

Microsoft stellt Informationen zur Verfügung, wie die Bandbreite vor der Migration zu Office 365 bewertet und die Leistung von Ressourcen im Allgemeinen optimiert werden können.[108] Der aktuelle Dienststatus kann online zu den Office 365-Diensten abgerufen werden.[109]

Weitere Informationen und Links zur Migration und Integration nach Office 365 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* enthalten.

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 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)[110] 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.[111]

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.

---

[108] https://docs.microsoft.com/de-de/microsoft-365/enterprise/network-planning-and-performance

[109] https://docs.microsoft.com/de-de/microsoft-365/enterprise/view-service-health

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

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

Weitere Informationen zum Abruf der Daten aus Office 365 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*.

4.19 NCD.2.5.01 Mitnutzung externer Cloud-Dienste

Sofern ein Cloud-Dienst einer anderen Institution mitgenutzt wird, 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 4.1)
- *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[112].

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

Microsoft veröffentlicht die allgemein gültigen Vertragsbedingungen im Licensing-Portal[113]. Zusatzvereinbarungen sollten durch den Vertragspartner bereitgestellt werden, mit dem die Cloud gemeinsam genutzt wird.

Office 365 verschlüsselt Verbindungen mit Industriestandards, wie AES und TLS/SSL.[114] Office 365 verschlüsselt neben den Kommunikationsdaten auch die ruhenden Daten mittels verschiedener Methoden.[115] 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.[116] Zusammen mit dem bedingten Zugriff kann dies genutzt werden, um den Zugriff auf bestimmte Daten oder Dienste in Office 365 zu beschränken.[117]

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*.

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

[114] https://docs.microsoft.com/de-de/microsoft-365/compliance/office-365-encryption-for-data-in-transit

https://docs.microsoft.com/de-de/microsoft-365/compliance/exchange-online-uses-tls-to-secure-email-connections

[115] https://docs.microsoft.com/de-de/microsoft-365/compliance/encryption

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

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

5 Die Verantwortung von Microsoft als Cloud-Diensteanbieter

Microsoft teilt sich mit dem Kunden die Verantwortung für die Sicherheit von Office 365 (siehe Kapitel 2.1 *Modell der gemeinsamen Verantwortung*). Da der Cloud-Kunde in der Lage sein sollte, die Sicherheit der Cloud ohne den Aufwand einer vollständigen Auditierung der technischen Infrastruktur, aber mit ebenso ausreichender Bestimmtheit zu bewerten, hat Microsoft eine Reihe von sicherheitsrelevanten Zertifizierungen für Office 365 vorbereitet.

Die wichtigsten davon sind:

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

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 oder 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 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 Anforderungen und Umsetzungshinweise 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 (in Englisch) https://aka.ms/DPA
Sorgfaltsüberprüfung	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/de-de/investor/default.aspx https://www.microsoft.com/de-de/corporate-responsibility/lerr (in Englisch)
Compliance-Informationen	https://servicetrust.microsoft.com/ https://www.microsoft.com/de-de/TrustCenter/Compliance https://docs.microsoft.com/de-de/compliance/regulatory/gdpr-action-plan https://docs.microsoft.com/de-de/compliance/regulatory/offering-home https://www.microsoft.com/de-de/corporate-responsibility/lerr (in Englisch)
Office 365 Dienstleistungen, Werkzeuge und weitere Informationen	https://info.microsoft.com/enterprise-cloud-strategy-ebook.html (in Englisch) https://azure.microsoft.com/de-de/overview/choosing-a-cloud-service-provider/ http://status.office365.com/ (in Englisch) https://docs.microsoft.com/de-de/office365/enterprise/view-service-health https://www.microsoft.com/de-de/fasttrack/

Sicherheitsaspekte Office 365	https://servicetrust.microsoft.com/ https://docs.microsoft.com/de-de/microsoft-365/security/defender/overview-security-center https://docs.microsoft.com/de-de/azure/active-directory/ https://docs.microsoft.com/de-de/microsoft-365/solutions/cloud-architecture-models https://docs.microsoft.com/de-de/office/office-365-management-api/ https://docs.microsoft.com/de-de/azure/information-protection/activate-office365 https://docs.microsoft.com/de-de/microsoft-365/compliance/encryption https://docs.microsoft.com/de-de/compliance/assurance/assurance-human-resources https://go.microsoft.com/fwlink/p/?LinkID=2162834&clcid=0x407 (Whitepaper: How does Microsoft handle your data in the cloud?)
Microsoft Liste der Dienstleister	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)
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/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Anforderungskatalog-Cloud_Computing-C5.pdf https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Nutzung_externer_Cloud-Dienste.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