HISOLUTIONS

IT-Grundschutz Compliance von Dynamics 365

20. Februar 2023

MICROSOFT DEUTSCHLAND GMBH

Inhaltsverzeichnis

1 Einleitung

Microsoft Dynamics 365 ist eine Suite mit intelligenten Geschäftsanwendungen. Dynamics 365 vereint die Funktionen Customer Relationship Management (CRM) und Enterprise Resource Planning (ERP), indem es fachspezifische Anwendungen bereitstellt, die bei der Ausführung bestimmter Geschäftsfunktionen helfen. Mit Dynamics 365 bietet Microsoft Cloud-Dienste für das Management von Kundenbeziehungen, die Überwachung von Vertrieb und Marketing und Analyse und Reporting von Geschäftsdaten an.[1]

Kunden können eine oder mehrere Regionen auswählen, aus denen Dynamics 365 bereitgestellt wird. In Deutschland werden die beiden bestehenden Regionen (Germany Northeast und Germany Central) durch die Regionen Germany West Central und Germany North ergänzt[2]. Je nach Kundenwunsch können die Daten in einer oder mehreren Regionen gespeichert werden, beispielsweise aus Gründen der Verfügbarkeit.

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), welches in den BSI-Standards 200-1 und 200-2 beschrieben ist. Dies wird ergänzt mit einer speziellen Methode zur Risikoanalyse (BSI-Standard 200-3), einem Standard für Business Continuity (BSI-Standard 100-4; derzeit in der Überarbeitung) und dem IT-Grundschutz-Kompendium, einer Standardauflistung von Bedrohungen und Anforderungen für typische Geschäftsumgebungen.

Ziel dieses Leitfadens ist es, Dynamics 365 Kunden bei der Anwendung der IT-Grundschutz-Methodik im Rahmen ihrer bestehenden oder geplanten Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz zu unterstützen.

Hierzu gibt Kapitel 2 einen Überblick über Cloud-Computing im Rahmen von IT-Grundschutz. Ein

[1] https://www.microsoft.com/en-us/dynamics365/what-is-crm (in Englisch)

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

Überblick darüber, wie der IT-Grundschutz-Baustein *OPS.2.2 Cloud-Nutzung*[3] als Teil des Informationsverbunds[4] implementiert wird, wird je Anforderung in Kapitel 3 wiedergegeben. In Kapitel 4 sind Hinweise für die Umsetzung der BSI-Mindeststandards "Mindeststandard für die Nutzung externer Cloud-Dienste"[5] enthalten, die sich an Bundesbehörden richten und für diese verbindlich gelten. Kapitel 5 behandelt die Rolle und die damit verbundenen Verantwortlichkeiten von Microsoft als Cloud-Diensteanbieter.

[3] 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

[4] Siehe

für normative Begriffe, die eine besondere Bedeutung haben.

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

2 Compliance-Anforderungen

Der vorliegende Leitfaden für Microsoft Dynamics 365 basiert auf der überarbeiteten Version des IT-Grundschutz-Kompendiums aus dem Jahr 2021[6]. In dieser Version des IT-Grundschutzes ist der Baustein *OPS.2.2 Cloud-Nutzung*[7] enthalten. Im IT-Grundschutz wird zwischen der Nutzung von Cloud-Diensten wie Dynamics 365 und klassischem IT-Outsourcing unterschieden.

2.1 Modell der gemeinsamen Verantwortung (Shared Responsibility)

Im Gegensatz zur lokalen IT-Infrastruktur wird in einer Cloud-Umgebung die Verantwortung für die Implementierung und Aufrechterhaltung 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 Zertifizierungsverbund einschließlich eines abgestimmten Risikomanagements einbezieht (klassisches Outsourcing-Szenario). 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 Kunde und Cloud-Diensteanbieter entlang der Applikationsgrenzen, so dass jeweils nur eine Partei für einen bestimmten Aspekt verantwortlich ist.

Tabelle 1 zeigt einen Überblick, wie eine solche Aufteilung 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 umreißt pro Aspekt den verfügbaren Support für den Kunden, der von Microsoft in seiner Rolle als Cloud-Diensteanbieter zur Verfügung steht.

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

[7] 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 beim Einsatz von Cloud-Computing (SaaS-Modell)[8]

Aspekt/Verantwortung Cloud Kunde Cloud-Diensteanbieter		Beschreibung
Sicherheitskonzept		Sicherheitskonzepte sind ein wesentlicher Bestandteil der IT-Grundschutz-Methodik. Ein Sicherheitskonzept ist eine dokumentierte Risikoanalyse und -behandlug 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 Dynamics 365 helfen.
Datenklassifizierung & Verantwortlichkeit		Der Wert der Daten kann nur vom Kunden bestimmt werden, der daher seine Daten identifizieren, klassifizieren und kennzeichnen sollte. In Dynamics 365 können die Felder klassifiziert werden, die personenbezogene oder sensible Daten enthalten.[9]
Kunden- und Endgeräteschutz		Kunden sollten klar definieren, welche Geräte und Clients auf die Cloud zugreifen dürfen.
Identitäts- und Berechtigungsmanagement		Dynamics 365 bietet verschiedene Möglichkeiten zur Identitäts- und Berechtigungsmanagement. Diese reichen von der vollständig Cloud-basierten[10] Identitäts- und Berechtigungsmanagement bis hin zu einem hybriden Ansatz[11], bei dem Benutzerdaten lokal verwaltet werden. Mit Azure Active Directory kann der Kunde Kennwortrichtlinien und Multi-Faktor-Authentifizierung[12] nach seinen spezifischen Richtlinien konfigurieren. Es ist zu beachten, dass Microsoft für die Bereitstellung eines funktionalen und sicheren Identitäts- und Berechtigungsmanagement verantwortlich ist. Beim Cloud-Kunden liegt jedoch auch bei der Cloud-basierten Identität die Verantwortung für das Identitäts- und Berechtigungsmanagement. Der Zugriff auf Kundendaten durch Microsoft-Mitarbeiter kann mit dem Dienst Customer Lockbox[13] gesteuert werden.

[8] vgl. Simorjay, Frank und Tierling, Eric: Shared Responsibilities - For Cloud Computing. Ed. Microsoft, Oktober 2019. (https://azure.microsoft.com/de-de/resources/shared-responsibility-for-cloud-computing/; in Englisch)

[9] https://docs.microsoft.com/de-de/dynamics365/business-central/dev-itpro/developer/devenv-classifying-data-sensitivity and https://docs.microsoft.com/de-de/dynamics365/business-central/dev-itpro/developer/devenv-classifying-data (in Englisch)

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

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

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

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

Aspekt/Verantwortung Cloud Kunde Cloud-Diensteanbieter		Beschreibung
Audits		Dynamics 365 wird aufgrund der Anforderungen verschiedener Compliance-Standards und Zertifizierungen kontinuierlich von unabhängigen Dritten auditiert. Die Liste der Konformitätsnormen für Dynamics 365 umfasst beispielsweise BSI C5, ISO 27001, ISO 27017 und ISO 27018.[14]
Portabilität		Die mit Dynamics 365 gespeicherten Kundendaten können mit Hilfe von Microsoft-Tools oder Tools von Drittanbietern exportiert und heruntergeladen werden.
Notfallwiederherstellung		Dynamics 365 hat seine Dienste mit der notwendigen Sorgfalt konzipiert. Mehrere Live-Kopien von Kundendaten werden von den Diensten in mehreren Rechenzentren in der gewählten Region bereitgehalten, um die vertragliche Verfügbarkeit sicherzustellen[15]. Kunden sollten einen Notfallplan entwickeln, der auch die Datensicherung umfasst.
Maßnahmen der Anwendungsebene		Für Dynamics 365-Kunden werden die allgemeinen Maßnahmen auf Anwendungsebene (z. B. Antimalware- und Patch-Management) von Microsoft implementiert.
Netzwerksteuerungen		Das Netzwerk wird von Microsoft für Dynamics 365-Kunden 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 stellt sicher, 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.

2.2 Modellierung von Dynamics 365

Um konform zum IT-Grundschutz zu bleiben und gleichzeitig die Dienste von Dynamics 365 nutzen zu

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

[15] https://docs.microsoft.com/de-de/power-platform/admin/new-datacenter-regions

können, muss das IT-Sicherheitskonzept um den Cloud-Dienst Dynamics 365 gemäß BSI-Standard 200-2[16]ergänzt werden.

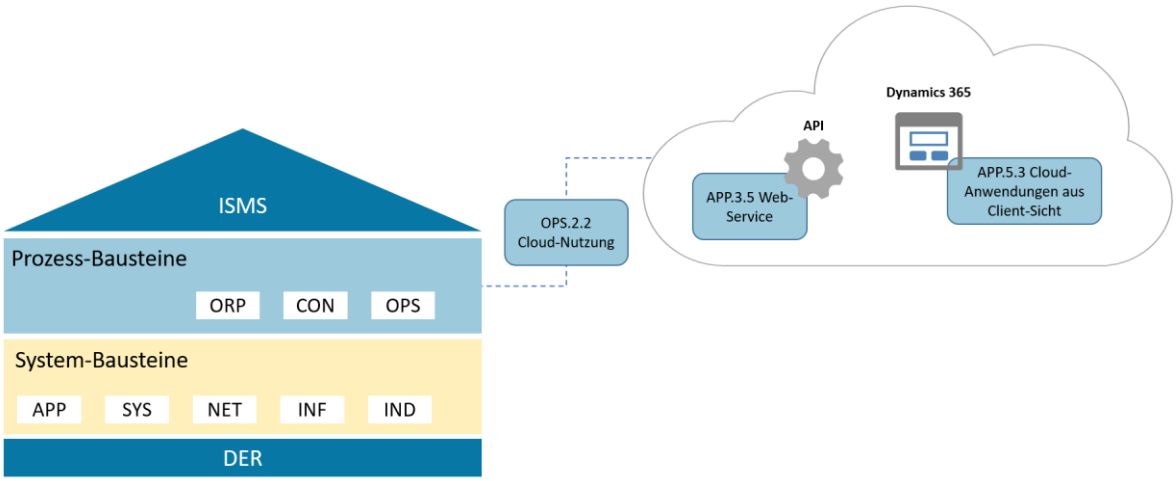

Abbildung 1 Schichtenmodell des IT-Grundschutz-Kompendiums mit Cloud-Nutzung als SaaS

Das IT-Grundschutz-Kompendium verfolgt einen schichtbasierten Ansatz zur Modellierung des Informationsverbunds. Dieses Modell besteht aus vier Schichten: dem Baustein Informationssicherheitsmanagementsystem (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 Dynamics 365 durch das Bereitstellungsmodell Software as a Service (SaaS) abgedeckt ist, werden in diesem Leitfaden nur die gemeinsamen Verantwortlichkeiten für SaaS behandelt. Nach dem IT-Grundschutz-Ansatz ist Microsoft als Cloud-Diensteanbieter für alle Schichten vom Cloud-Computing verantwortlich, vom Rechenzentrum über Server und Netzwerke bis hin zur SaaS-Anwendung. Auf Kundenseite definiert der Baustein *OPS.2.2 Cloud-Nutzung*[17] die Verantwortlichkeiten des Kunden über das gesamten Auslagerungsvorhaben.

Der Baustein *OPS.2.2 Cloud-Nutzung*[17] betrifft Anwendungen, die als Cloud-Dienst bereitgestellt werden, sowie deren Verwaltung. Das IT-Grundschutzkompendium[18] verlangt, dass der Baustein *OPS.2.2 Cloud-Nutzung* immer auf eine „konkrete Cloud-Dienstleistung" angewendet wird. Bei der Nutzung mehrerer Cloud-Diensteanbieter ist der Baustein für jeden Cloud-Diensteanbieter einmal anzuwenden. Dabei müssen auch die Schnittstellen zwischen den unterschiedlichen Cloud-Diensteanbietern bei der Umsetzung des Bausteins betrachtet werden.

Weitere Anforderungen zur Absicherung von Dynamics 365 aus Kundensicht werden voraussichtlich in den bisher noch nicht veröffentlichten Bausteinen *APP.5.3 Cloud-Anwendung aus Client-Sicht* und *APP.3.5 Web-Services* betrachtet werden. In der Zwischenzeit muss eine Risikoanalyse nach der Methode aus dem IT-Grundschutz[19] durchgeführt werden. Abbildung 1 zeigt, dass der Baustein

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

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

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

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

OPS.2.2 Cloud-Nutzung als Schnittstelle zwischen der lokalen Umgebung des Kunden und der Cloudumgebung fungiert.

Abbildung 2 zeigt die allgemeine Struktur von Dynamics 365 und wie es in einen Informationsverbund nach IT-Grundschutz eingebunden werden kann. Die Cloud-Dienste werden als Anwendungen modelliert, die direkt in der Cloud laufen, also ohne zugrundeliegende IT-Systeme oder verbundene Serverräume. Kommunikationsverbindungen (d.h. Internet- und/oder VPN-Verbindung) werden mit den entsprechenden Bausteinen für die Kombination aus Netzwerkkomponenten und Internet-Anbieter modelliert.

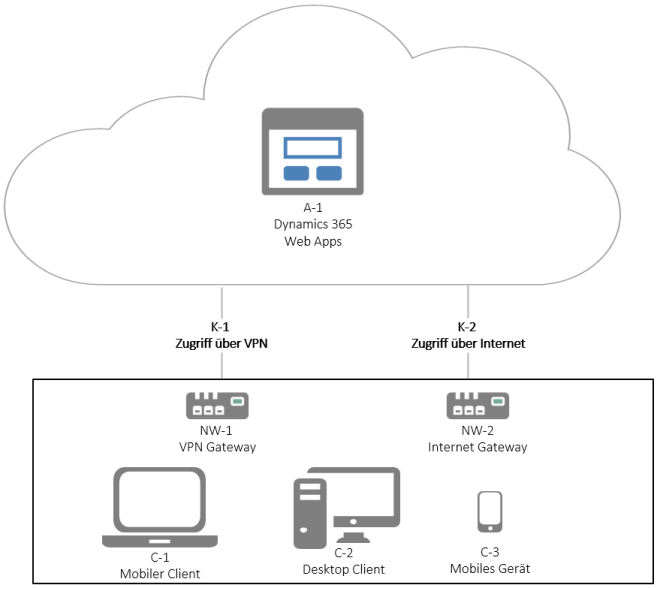

Abbildung 2 Modellierung von Dynamics 365 in einem IT-Grundschutz-Netzplan (Beispiel)

Die im nachfolgenden Kapitel beschriebenen Anforderungen enthalten zusätzliche Informationen, die sich auf den Baustein *OPS.2.2 Cloud-Nutzung*[20] und die entsprechenden Umsetzungshinweise oder hilfreiche Online-Ressourcen von Microsoft beziehen.

[20] 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 Umsetzung des Bausteins OPS.2.2 Cloud-Nutzung

In diesem Kapitel wird beschrieben, wie alle Anforderungen aus dem Baustein *OPS.2.2 Cloud-Nutzung*[21] für Dynamics 365 umgesetzt werden können. Im modernisierten IT-Grundschutz wurden die Anforderungen von Umsetzungshinweisen getrennt. Die Umsetzungshinweise für *OPS.2.2 Cloud-Nutzung*[22] enthalten konkrete Schutzmaßnahmen, mit denen die Anforderungen umgesetzt werden können und werden in einem eigenen Dokument des BSI beschrieben.

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

Tabelle 2 Von Microsoft bereitgestellte Informationen für die Anforderungen von *OPS.2.2 Cloud-Nutzung*

Anforderung	Unterstützende Informationen von Microsoft?	Beschreibung
OPS.2.2.A1 Erstellung einer Cloud-Nutzungs-Strategie	Ja	Microsoft hat den Leitfaden „Enterprise Cloud Strategy"[23] 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 -prozesse für den Einsatz von Dynamics 365 innerhalb einer Institution müssen definiert werden. Microsoft stellt Informationen zur Verfügung, die bei der Definition von Sicherheitsanforderungen bezüglich der Vertraulichkeit, Integrität und Verfügbarkeit der von Dynamics 365 verarbeiteten Informationen helfen.

[21] 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

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

[23] 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 Dynamics 365 bezüglich sicherer Authentifizierung, Verschlüsselung und Interoperabilität von Dynamics 365. Informationen über Funktionen, die der Kunde zur Datensicherung nutzen kann, werden von Microsoft zur Verfügung gestellt.
OPS.2.2.A4 Festlegung von Verantwortungsbereichen und Schnittstellen	Ja	Diese Anforderung betrifft die Aufteilung der Verantwortungen zwischen Cloud-Diensteanbieter und Cloud-Kunde. Microsoft bietet verschiedene Schnittstellen für Dynamics 365 an.[24]
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 Dynamics 365 Onlinedienste zu berücksichtigen sind.
OPS.2.2.A6 Planung der sicheren Einbindung von Cloud-Diensten	Ja	Diese Anforderung trägt zur sicheren Integration von Dynamics 365 in die Kundenumgebung bei. Microsoft bietet verschiedene Methoden zur Integration von Dynamics 365 in lokale Umgebungen an.
OPS.2.2.A7 Erstellung eines Sicherheitskonzepts für die Cloud-Nutzung	Ja	Obwohl es keine generische Vorlage für die Anforderungen jeder einzelnen Institution gibt, adressiert Dynamics 365 die meisten der technischen Bedrohungen und Sicherheitsmaßnahmen, die in der Anforderung erwähnt werden, um die Institution bei der Erstellung eines Sicherheitskonzepts für Dynamics 365 zu unterstützen.
OPS.2.2.A8 Sorgfältige Auswahl eines Cloud-Diensteanbieters	Ja	Microsoft bietet eine Anleitung für die Evaluierung von Dynamics 365.
OPS.2.2.A9 Vertragsgestaltung mit dem Cloud-Diensteanbieter	Ja	Die 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 Dynamics 365 an.

[24] cf. Simorjay, Frank and Tierling, Eric: Shared Responsibilities - For Cloud Computing. Ed. Microsoft, October 2019. (https://azure.microsoft.com/de-de/resources/shared-responsibility-for-cloud-computing/)

Anforderung	Unterstützende Informationen von Microsoft?	Beschreibung
OPS.2.2.A11 Erstellung eines Notfallkonzepts für einen Cloud-Dienst	Ja	Das Notfallkonzept wird individuell für Dynamics 365 entwickelt. Es werden allgemeine Richtlinien und Informationen zur Verfügung gestellt.
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 Verfahren zur Verfügung gestellt, mit denen der Benutzer die festgelegten Ansprüche, insbesondere die Einhaltung des Dynamics 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. Berichte von Penetrationstests zur Verfügung.
OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses	Ja	Informationen und Anleitungen, wie Daten, die in Dynamics 365 gespeichert sind, nach Beendigung eines Microsoft Dynamics 365-Abonnements exportiert werden können, werden bereitgestellt - einschließlich Kündigungs- und Datenlöschungsrichtlinien.
OPS.2.2.A15 Portabilität von Cloud-Diensten	Ja	Portabilitätsaspekte werden für Dynamics 365 werden anhand von Beispielen behandelt.
OPS.2.2.A16 Durchführung eigener Datensicherungen	Ja	Datensicherungen müssen von der Institution initiiert werden; entweder direkt oder über einen Drittanbieter. Dynamics 365 bietet integrierte Funktionen zur Datensicherung und –wiederherstellung an.
OPS.2.2.A17 Einsatz von Verschlüsselung bei Cloud-Nutzung	Ja	Microsoft hat Informationen darüber veröffentlicht, wie Dynamics 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	Föderierte Dienste werden über Azure Active Directory bereitgestellt, das für die Verwaltung von Benutzern und Gruppen in Dynamics 365 verwendet werden kann.
OPS.2.2.A19 Sicherheitsüberprüfung von Mitarbeitern	Ja	Im Rahmen hoher Sicherheitsanforderungen sind Hintergrundüberprüfungen der Mitarbeiter des Cloud-Dienstanbieters 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 Microsoft Azure, Dynamics 365 und Microsoft 365. 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. Außerdem können sie von den Gemeinsamkeiten und Synergien dieser Dienste stark profitieren, indem sie bestimmte Methoden im Allgemeinen behandeln und nur Besonderheiten der einzelnen Dienste jeweils ergänzen müssen. So kann beispielsweise Azure Active Directory für das Identitäts- und Berechtigungsmanagement von Azure, Dynamics 365 und Microsoft 365 verwendet werden.

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

In einer Cloud-Nutzungs-Strategie werden die Ziele, Chancen und Risiken der Cloud-Nutzungs betrachtet, die sich auf eine Institution auswirken können. Dazu gehört auch die Berücksichtigung rechtlicher Aspekte sowie technischer und sicherheitsrelevanter Anforderungen. Infolgedessen sollten erlaubte Bereitstellungsmodelle für Cloud-Dienste und erste Cloud-Sicherheitsanforderungen identifiziert werden.

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

Der Kunde muss entscheiden, welche Anwendungen oder Dienste nach Dynamics 365 migriert werden sollen. Dies kann eine teilweise Integration von Diensten (z. B. mit Dynamics 365 online, aber auch mit dem Exchange-Dienst on-Premise[26]) oder eine Integration der operativen Diensten vor Ort in die Cloud (z. B. Integration von Active Directory on-Premise) bedeuten.

Je nach gewähltem Dynamics 365 Plan[27]gibt es mehrere Lösungen, mit unterschiedlichen Integrationsmöglichkeiten und Schnittstellen zwischen Cloud-Diensten, lokal installierten Diensten und Client-Anwendungen. Die am besten geeignete Strategie variiert meist von Kunde zu Kunde. Die folgende Tabelle beschreibt zwei mögliche Varianten mit unterschiedlicher Komplexität im Hinblick auf verschiedene Integrationsszenarien. Die optimale Lösung liegt in der Regel für jeden Kunden zwischen den beiden in der Tabelle aufgeführten Varianten.

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

[26] https://docs.microsoft.com/en-us/power-platform/admin/connect-exchange-server-on-premises (in Englisch)

[27] https://dynamics.microsoft.com/de-de/pricing/
https://docs.microsoft.com/en-us/dynamics365/business-central/dev-itpro/developer/devenv-classifying-data-sensitivity (in Englisch)

Tabelle 3: Unterschiedliche Komplexitäten der Integration von Dynamics 365

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 und Active Directory)
Zwei-Faktor-Authentifizierung ausschließlich über die von Microsoft zur Verfügung gestellten Funktionen	Alternative Zwei-Faktor-Authentifizierung mit Azure Active Directory möglich, z. B. über Smartcards
Keine Verbindung und Synchronisation zwischen Cloud-Diensten und lokalen Anwendungen, bedeutet höhere adminstrative Anforderungen (z. B. bei der Benutzerverwaltung)	Hohe Integration und Synchronisation zwischen Cloud-Diensten und lokalen Diensten, bedeutet geringeren Verwaltungsaufwand, ein fein abgestuftes Benutzerzugriffsmanagement, sowie automatisierte Anwendungs- und Lizenzbereitstellung.
Hohe Abhängigkeit und Verfügbarkeitsanforderungen an die Internetverbindung	Synchronisierte Online- und Offline-Verarbeitung von Geschäftsinformationen
Webbasierte Dynamics 365-Anwendungen	Web-basierte und lokale Installation von Dynamics 365-Anwendungen

Weitere Informationen zum Abgleich der Anforderungen mit den Angeboten von Dynamics 365 befinden sich in Anhang B.

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

Die Sicherheitsrichtlinie für die Nutzung der Cloud wird auf Grundlage der Strategie definiert (siehe Kapitel 3.1 *OPS.2.2.A1 Erstellung einer Cloud-Nutzungs-Strategie*OPS.2.2.A1). 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 spezifische Informationen in Form eines Whitepapers zur Sicherheit von Dynamics 365 zur Verfügung, um Institutionen bei der Erstellung ihrer Sicherheitsrichtlinien in Bezug auf Datenschutz, Compliance, Transparenz und andere individualisierte Maßnahmen zu unterstützen[28]. Der Inhalt

[28] https://docs.microsoft.com/en-us/dynamics365/customer-engagement/admin/security-concepts
Whitepaper "Skalierbare Sicherheitsmodellierung mit Microsoft Dynamics CRM". (in Englisch)

einer Richtlinie für die Cloudnutzung 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 Dynamics 365	Referenzen
Identitäts- und Berechtigungsmanagement	Dynamics 365 wird auf der Azure-Plattform von Microsoft bereitgestellt und verwendet Azure Active Directory zur Verwaltung von Identitäten und Authentifizierung. Dynamics 365 unterstützt cloud-basierte Benutzer sowie hybride Identitäten. Hybride Identitäten werden on-Premise verwaltet- und mit Azure Active Directory synchronisiert (mit oder ohne Übertragung des Passwort-Hashes). Azure Active Directory bietet verschiedene Möglichkeiten, hybride Identitäten für Dynamics 365 zu verwenden: • Die Passwort-Hash-Synchronisation (PHS) synchronisiert lokale Konten, einschließlich eines Hashwerts des Passwort-Hash nach Azure Active Directory. • Die Pass-through-Authentifizierung (PTA) ermöglicht es einem Benutzer, sich mit seinen lokalen Anmeldeinformationen bei Azure anzumelden, und Azure validiert dann das Passwort anhand 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. Dynamics 365 unterstützt rollenbasierte Zugriffskontrolle und bietet mehrere integrierte Rollen. Neben internen Konten einer Institution oder einer Institution ermöglicht Dynamics 365 das Hinzufügen und Verwalten von Gastkonten und externen Partnern (Business-to-Business, B2B).	https://docs.microsoft.com/de-de/azure/active-directory/fundamentals/active-directory-whatis https://docs.microsoft.com/de-de/azure/active-directory/hybrid/ https://docs.microsoft.com/de-de/azure/active-directory/hybrid/whatis-phs https://docs.microsoft.com/de-de/azure/active-directory/hybrid/how-to-connect-pta https://docs.microsoft.com/de-de/azure/active-directory/hybrid/whatis-fed https://docs.microsoft.com/en-us/dynamics365/customer-engagement/admin/security-roles-privileges (in Englisch) https://docs.microsoft.com/en-us/dynamics365/customer-engagement/admin/invite-users-azure-active-directory-b2b-collaboration (in Englisch) https://docs.microsoft.com/de-de/dynamics365/business-central/dev-itpro/security/multifactor-authentication (in Englisch) https://docs.microsoft.com/de-de/azure/active-directory/authentication/concept-mfa-howitworks https://docs.microsoft.com/de-de/azure/active-directory/privileged-identity-management/pim-configure

Compliance-Anforderung	Implementierung in Dynamics 365	Referenzen
	Dynamics 365 unterstützt mehrere Multi-Faktor-Authentifizierung-Methoden (MFA), z. B. über mobile App, Smart Card oder bestimmte MFA-Lösungen von Drittanbietern. Privileged Identity Management (PIM) ermöglicht Verwaltung und Überwachung des administrativen Zugriffs auf Dynamics 365. So kann beispielsweise mit PIM der Zugriff auf Berechtigungen zeitlich begrenzt werden. Administratoren können ein Timeout, für jede ihrer Dynamics 365 Customer Engagement Instanzen, für Inaktivität festlegen, der ein automatisches Abmelden bewirkt. Die Anwendung meldet den Benutzer ab, wenn die Sitzung aufgrund Inaktivität abläuft. Die Funktion für den bedingten Zugriff (sog. Conditional Access) von Azure Active Directory kann auch für Dynamics 365 verwendet werden. Mit dieser Funktion kann der Kunde von Dynamics 365 automatisierte Zugriffskontrollentscheidungen für Zugriff auf Daten und Anwendungen in Dynamics 365 hinzufügen, die zustandsabhängig sind. Weitere Informationen und Links zu Verschlüsselungs- und Kryptofunktionen befinden sich in der **Fehler! Verweisquelle konnte nicht gefunden werden.** im Kapitel 3.17 *OPS.2.2.A17 Einsatz von Verschlüsselung bei Cloud-Nutzung.* Mit Mobile Device Management (MDM) oder Intune können mobile Geräte, die auf Dynamics 365 zugreifen dürfen, gesichert und konfiguriert werden.	https://docs.microsoft.com/de-de/power-platform/admin/user-session-management (in Englisch) https://docs.microsoft.com/de-de/azure/active-directory/conditional-access/overview https://docs.microsoft.com/de-de/dynamics365/mobile-app/v8/set-up-manage/secure-manage https://docs.microsoft.com/de-de/intune/fundamentals/what-is-intune
Asset Management	Über Dynamics 365 Business Central Benutzer und Gruppen verwaltet werden. Kunden von Dynamics 365 können ihre Daten klassifizieren. Für Dynamics 365 Finance und Dynamics 365 Supply Chain Management ist	https://docs.microsoft.com/de-de/dynamics365/business-central/ui-define-granular-permissions https://docs.microsoft.com/de-de/dynamics365/business-central/admin-classifying-data-sensitivity

Compliance-Anforderung	Implementierung in Dynamics 365	Referenzen
	Asset Management als Teil eines Preview-Release verfügbar.	https://docs.microsoft.com/de-de/dynamics365/supply-chain/asset-management/
Schutz der Daten	Die Mandantentrennung innerhalb von Dynamics 365 wird mit verschiedenen technischen Mitteln realisiert. Dazu gehört auch die logische Trennung durch rollenbasierte Zugriffskontrolle. In Dynamics 365 kann der Zugriff über die so genannte Field-Level-Sicherheit auf einzelnen Felder beschränkt werden. Gespeicherte Daten und Daten, die übertragen werden, werden mit kryptographischen Methoden und Protokollen wie AES, IPSec oder TLS/SSL verschlüsselt. Für gespeicherte Daten wird eine Verschlüsselung auf Zellenebene verwendet. Microsoft testet und überwacht kontinuierlich die Sicherheit von Dynamics 365 und ergreift erforderliche Maßnahmen. Entsprechende Berichte, z. B. für Penetrationstests oder Audits, sind über das Trust Center zugänglich. Der Dienstzustand von Dynamics 365 kann auf der Dynamics 365 Service Health Seite im Microsoft 365 Admin Center eingesehen werden. Dynamics 365 verfügt über umfangreiche Protokollierungs- und Überwachungsfunktionen. Die Protokolldaten sind in einem einheitlichen und durchsuchbaren Format zugänglich, das es ermöglicht, Benutzer- und Administratoraktivitäten in Dynamics 365 anzuzeigen.	https://docs.microsoft.com/de-de/dynamics365/admin/multiple-online-instances-tenants https://docs.microsoft.com/de-de/power-platform/admin/field-level-security https://docs.microsoft.com/de-de/dynamics365/admin/data-encryption https://docs.microsoft.com/de-de/microsoft-365/compliance/office-365-encryption-in-microsoft-dynamics-365 https://docs.microsoft.com/de-de/microsoft-365/compliance/offering-home https://docs.microsoft.com/de-de/power-platform/admin/notifications-explained#service-health-dashboard (in Englisch) https://docs.microsoft.com/de-de/power-platform/admin/enable-use-comprehensive-auditing (in Englisch) https://docs.microsoft.com/de-de/dynamics365/customerengagement/on-premises/deploy/microsoft-dynamics-365-monitoring-service
Compliance und Audit	Microsoft hat die Prozesse so angepasst, dass Anforderungen aufgrund der Standardvertragsklauseln der Europäischen Union erfüllt werden. Dynamics 365 stellt sicher, dass Kunden in der Lage sind, die Anforderungen an	https://docs.microsoft.com/de-de/microsoft-365/compliance/offering-eu-model-clauses (in Englisch) https://docs.microsoft.com/de-de/microsoft-365/compliance/gdpr-dpia-dynamics

Compliance-Anforderung	Implementierung in Dynamics 365	Referenzen
	die Benachrichtigung über Verstöße gemäß Datenschutzgrundverordnung (DSGVO) zu erfüllen. Realisiert wird dies durch die Angabe eines Datenschutzbeauftragten, 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 Maßnahmen zur Schadensminimierung einschließlich Zeitvorgaben für die Behebung. Darüber hinaus stellt Microsoft Dokumentationen bereit, wie die Anforderungen der DSGVO in Dynamics 365 vom Kunden umgesetzt werden können. Dazu gehören eine Checkliste zur Vorbereitung auf die Rechenschaftspflicht, eine Datenschutz-Folgenabschätzung und Empfehlungen, wie Anfragen von betroffenen Personen angemessen beantwortet werden können. 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. Dynamics 365 bietet mehrere Audit- und Berichtsfunktionen an, darunter eine einheitliche Protokollierung mit Suchfunktionen. Dieses kann auch zum Nachvollziehen von Benutzer- oder Administratoraktivitäten verwendet werden. Microsoft bietet detaillierte Dokumentationen an, wie mit Dynamics 365 die Einhaltung gesetzlicher oder behördlicher Standards gewährleistet werden kann. Mit Dynamics 365 Fraud Protection können personenbezogene Daten identifiziert, gelöscht oder exportiert werden. Darüber hinaus ermöglichen Anwendungen wie die Datenarchivierungs- und Aufbewahrungsfunktion dem Benutzer die Archivierung von Daten in einer	https://docs.microsoft.com/de-de/microsoft-365/compliance/gdpr-dsr-dynamics365 https://docs.microsoft.com/de-de/microsoft-365/compliance/gdpr-breach-dynamics365 https://docs.microsoft.com/de-de/microsoft-365/compliance/gdpr-arc-dynamics365 https://docs.microsoft.com/de-de/microsoft-365/compliance/offering-iso-27018 (in Englisch)https://docs.microsoft.com/de-de/microsoft-365/compliance/offering-home https://docs.microsoft.com/de-de/powerapps/developer/common-data-service/auditing-overview https://docs.microsoft.com/de-de/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance https://docs.microsoft.com/de-de/power-platform/admin/audit-data-user-activity (in Englisch) https://docs.microsoft.com/de-de/microsoft-365/compliance/offering-home https://docs.microsoft.com/de-de/dynamics365/fraud-protection/security-compliance https://appsource.microsoft.com/de-de/product/dynamics-365/microsoft_labs.dataarchival https://www.microsoft.com/de-de/trust-center/privacy/data-location https://docs.microsoft.com/de-de/microsoft-365/compliance/meet-data-protection-

Compliance-Anforderung	Implementierung in Dynamics 365	Referenzen
	Cosmos-Datenbank. Die App ermöglicht die Definition von Datenhaltungsrichtlinien zur effektiven Verwaltung von Daten in Übereinstimmung mit Richtlinien, Vorschriften und gesetzlichen Anforderungen. Die Datenhaltungsrichtlinien unterstützten dabei, dass Inhalte nicht vor Ablauf der Aufbewahrungsfrist dauerhaft gelöscht werden können. Microsoft gibt einen Überblick über seine Datenspeicherorte für Dynamics 365. Der Compliance Manager ist ein workflowbasiertes Risikobewertungs-Tool zur Verfolgung, Zuweisung und Überprüfung von Compliance-Aktivitäten im Zusammenhang mit Dynamics 365. Es bietet ein zentralisiertes Dashboard für Standards, Vorschriften und Implementierungen, einschließlich der Ergebnisse für Dienstbewertungen.	and-regulatory-reqs-using-microsoft-cloud
Sicherung und Archivierung	Bei Verwendung der Datenarchivierungs- und Aufbewahrungsfunktion bewahrt diese App permanente Dateien aller Daten auf, welche in einem schreibgeschützten, nicht löschbaren Format gespeichert wurden. Die Aufbewahrung erfolgt unter Berücksichtigung von eingestellten Aufbewahrungsrichtlinien einschließlich einer Aufbewahrungssperre. Datenresilienz und Wiederherstellbarkeit sind über die integrierten Funktionen der Azure-Plattform, auf der Dynamics 365 läuft, vorhanden, um die Zuverlässigkeit zu maximieren und negative Auswirkungen auf die Kunden zu minimieren. Dies wird durch eine Kombination der physischen Infrastruktur mit Softwarelösungen erreicht. Backups sind für Azure SQL-Datenbanken möglich, wenn Dynamics 365-Daten in ihnen gespeichert sind.	https://appsource.microsoft.com/de-de/product/dynamics-365/microsoft_labs.dataarchival https://azure.microsoft.com/de-de/features/resiliency/ https://azure.microsoft.com/de-de/resources/resilience-in-azure-whitepaper/ (in Englisch) https://docs.microsoft.com/de-de/azure/sql-database/sql-database-automated-backups https://docs.microsoft.com/de-de/dynamics365-release-plan/2019wave2/dynamics365-commerce/planned-features

Compliance-Anforderung	Implementierung in Dynamics 365	Referenzen
	Für folgende Releases von Dynamics 365 sind zusätzliche Sicherungsmöglichkeiten geplant (z. B. Download von Datensicherungen in Dynamics 365). Andernfalls sind Lösungen von Drittanbietern verfügbar. Im Microsoft Dynamics 365 Rechenzentrum wird auf einem weiteren Server eine doppelte und synchronisierte (alternative) Kopie der gespeicherten Daten verwaltet. Im Falle eines Vorfalls im Rechenzentrum, der den Zugriff auf die Daten verhindert, ist es möglich den Standort zu wechseln, wodurch die Schwere der Betriebsunterbrechung minimiert wird. Sobald das Problem behoben ist, kann der Dienstzugriff auf den primären Standort wiederhergestellt werden.	
Bedrohungsschutz	Azure und somit auch Dynamics 365 verfügen über einen automatischen und kostenlosen DDoS-Schutz (Distributed Denial of Service), der für gängige Angriffe auf Netzwerkebene ausreichend ist. Ein Abonnement für den Standard-DDoS-Schutz bietet Schutz vor komplexeren Angriffen und unterstützt DDoS-Experten bei der Administration und bei dem Umgang mit DDoS-Angriffen. Azure bietet einen kostenlosen Echtzeit-Malwareschutz, welchen Dynamics 365 Kunden in ihrem Azure-Abonnement verwenden können , um verschiedene Arten von Schadsoftware wie Viren oder Spyware zu identifizieren und zu entfernen.	https://docs.microsoft.com/de-de/azure/virtual-network/ddos-protection-overview https://docs.microsoft.com/de-de/azure/security/fundamentals/antimalware
Veränderungsmanagement	Microsoft stellt Informationen über Änderungen in Dynamics 365 zur Verfügung, damit Kunden über die schnelle Entwicklung in Dynamics 365 auf dem Laufenden bleiben und wie sie die neuesten Update-Informationen erhalten. Dabei stellt Microsoft eine Roadmap für	https://dynamics.microsoft.com/de-de/roadmap/overview/ https://docs.microsoft.com/de-de/dynamics365-release-plan/2019wave2/change-history https://docs.microsoft.com/de-de/dynamics365/fin-ops-

Compliance-Anforderung	Implementierung in Dynamics 365	Referenzen
	laufende und geplante Updates zur Verfügung. Unter anderem bietet der Service Finance and Operations eine interne Änderungsverfolgung in Microsoft Dynamics 365.	core/dev-itpro/data-entities/entity-change-track (in Englisch)

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 Dienstdefinition sollten die wichtigsten technischen Parameter definiert werden.

Microsoft stellt detaillierte Beschreibungen der für Dynamics 365verfügbaren Dienste und Funktionen zur Verfügung.[29] Jeder Dienst hat eine 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 Dienstdefinition für Cloud-Dienste sollte sich eine Institution auch mit folgenden Aspekten im Detail befassen: Auswahl der sicheren Authentifizierungsmethoden, Definition von Operational Level Agreements (OLAs) und Service Level Agreements (SLAs) sowie weitere Sicherheitsaspekte, wie die, die in der folgenden Tabelle beschrieben werden.

Tabelle 5: Compliance-Anforderungen an die Dienstdefinitionen

Compliance-Anforderung	Implementierung in Dynamik 365	Referenzen
Auswahl von sicheren Authentifizierungsmethoden	Dynamics 365 bietet grundlegende Azure Active Directory-Funktionen, einschließlich Azure Multi-Faktor-Authentifizierung (MFA). Für die Steuerung von Cloud-Diensten über das Microsoft	https://docs.microsoft.com/de-de/azure/active-directory/authentication/concept-mfa-licensing https://docs.microsoft.com/de-de/dynamics365/fin-ops-core/dev-itpro/sysadmin/role-based-security (in Englisch)

[29] https://docs.microsoft.com/de-de/office365/servicedescriptions/microsoft-dynamics-365-online-service-description

Compliance-Anforderung	Implementierung in Dynamik 365	Referenzen
	Azure Portal steht eine rollenbasierte Zugriffskontrolle zur Verfügung. 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 durch Kunden definierbaren Bedingungen wie Quell-IP, Gerätebenutzer oder der Authentifizierungsmethode einzuschränken. Intune kann verwendet werden, um mobile Geräte abzusichern und zu konfigurieren, die auf Dynamics 365 zugreifen dürfen.	https://docs.microsoft.com/de-de/dynamics365/admin/security-roles-privileges https://docs.microsoft.com/de-de/office365/enterprise/hybrid-cloud-overview https://docs.microsoft.com/de-de/azure/active-directory/conditional-access/overview https://docs.microsoft.com/de-de/dynamics365/mobile-app/v8/set-up-manage/secure-manage
Weitere Überlegungen zu Sicherheitsaspekten	Dynamics 365 bietet Verschlüsselungsformen für gespeicherte Daten und Daten, die übertragen werden an (siehe auch *Vertraulichkeit* in der Tabelle im Kapitel 3.17 *OPS.2.2.A17 Einsatz von Verschlüsselung* bei Cloud-Nutzung). Die Isolierung zwischen den Tentants (Multi-Tenancy) wird auf Rechen-, Speicher-, Datenbank- und Netzwerkebene realisiert, um sicherzustellen, dass auch auf gleicher Hardware kein Zugriff auf die Daten anderer Kunden möglich ist. Datenresilienz und Wiederherstellbarkeit können über die integrierten Funktionen der Dynamics 365 zugrundeliegenden Azure-Plattform genutzt werden. Dadurch lassen sich die Zuverlässigkeit maximieren und negative Auswirkungen auf die Kunden minimieren. Dies wird durch	https://docs.microsoft.com/de-de/dynamics365/admin/data-encryption https://docs.microsoft.com/de-de/microsoft-365/compliance/office-365-encryption-in-microsoft-dynamics-365 https://docs.microsoft.com/de-de/azure/security/fundamentals/isolation-choices https://azure.microsoft.com/de-de/features/resiliency/ https://azure.microsoft.com/de-de/resources/resilience-in-azure-whitepaper/ (in Englisch) https://docs.microsoft.com/de-de/power-platform/admin/restrict-access-online-trusted-ip-rules https://docs.microsoft.com/de-de/dynamics365-release-plan/2019wave2/dynamics365-commerce/planned-features

Compliance-Anforderung	Implementierung in Dynamik 365	Referenzen
	eine Kombination aus physischer Infrastruktur und Softwarelösungen erreicht. Zusätzlich kann der Zugriff durch IP-Adressregeln in Dynamics 365 eingeschränkt werden. Für zukünftige Dynamics 365 Releases sind Sicherungsmöglichkeiten geplant (z. B. Download von Datensicherungen in Dynamics 365).	
Interoperabilität der Client-Software	Dynamics 365 bietet eine Vielzahl von Funktionalitäten über Dynamics 365 APIs. Alle Dynamics 365 Management-APIs sind konsistent in Design und Implementierung mit der aktuellen Suite der Dynamics 365 REST-APIs und verwenden gängige Industriestandardansätze, einschließlich OAuth v2, OData v4 und JSON.	https://docs.microsoft.com/de-de/rest/dynamics365/ (in Englisch)

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-Dienstleanbieter 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 infolgedessen zu Sicherheitslücken führen kann.

Microsoft stellt verschiedene Informationen über ihren Ansatz und ihre Sichtweise zu diesem Modell der gemeinsamen Verantwortung zur Verfügung.[30] Weitere Informationen zum Modell der gemeinsamen Verantwortung befinden sich in Kapitel 2.1 *Modell der gemeinsamen Verantwortung* am Anfang dieses Dokuments.

[30] vgl. Simorjay, Frank und Tierling, Eric: Shared Responsibilities - For Cloud Computing. Ed. Microsoft, Oktober 2019. (https://azure.microsoft.com/de-de/resources/shared-responsibility-for-cloud-computing/in Englisch) https://azure.microsoft.com/mediahandler/files/resourcefiles/d8e7430c-8f62-4bbb-9ca2-f2bc877b48bd/Azure%20Onboarding%20Guide%20for%20IT%20Organizations.pdf (in Englisch)

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-Dienstes geplant werden.

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

Die Entwicklung eines Migrationskonzeptes bildet eine wichtige Grundlage für eine sichere und nachhaltige Migration in die Cloud. Dabei sind vor allem organisatorische Regelungen und Aufgabenverteilungen zu berücksichtigen. Dazu gehören Verantwortlichkeiten, Test- und Transferverfahren, die für einen widerstandsfähigen und sicheren Geschäftsbetrieb von besonderer Bedeutung sind. Im weiteren Verlauf muss die institutionseigene IT im Migrationsprozess bewertet werden, um zu prüfen, ob z. B. die Performance als ausreichend angesehen werden kann.

Für eine sichere Migration in die Cloud müssen verschiedene, kundenspezifische Bedingungen berücksichtigt werden. Dies gilt insbesondere, wenn bei der Migration andere, bereits genutzte Cloud-Dienste 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 von einer lokalen Umgebung, möglicherweise einschließlich anderer Cloud-Dienste, zu Dynamics 365 entsprechend geplant werden.

Microsoft bietet einen Leitfaden[31] zur Unterstützung des Kunden bei der Migrationsplanung an. 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 über die verschiedenen Phasen hinweg berücksichtigen.

Microsoft bietet Unterstützung bei der Migration von Online-Tenant zu Online-Tenant oder von lokalen Lösungen zu Dynamics 365 Onlinediensten an.[32] Zusätzlich bietet Microsoft den Dienst FastTrack für gültige Abonnements an, die den Migrationsprozess unterstützen[33].

Hinweis: Diese Anforderung ist kundenspezifisch, da sie die interne Planung für die sichere Migration bestehender Dienste umfasst.

https://www.microsoft.com/security/blog/2018/06/19/driving-data-security-is-a-shared-responsibility-heres-how-you-can-protect-yourself/ (in Englisch)

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

[32] https://dynamics.microsoft.com/de-de/cloud-migration/

[33] https://docs.microsoft.com/de-de/dynamics365/get-started/fasttrack/customer-engagement/microsoft-fasttrack-dynamics-365

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

Neben der Planung einer sicheren Migration (siehe Kapitel 3.5 *OPS.2.2.A5 Planung der sicheren Migration zu einem Cloud-Dienst*) ist die sichere Integration von Dynamics 365 in den IT-Landschaft für einen sicheren, kontinuierlichen IT-Betrieb unerlässlich. Diese Anforderung berücksichtigt entsprechend die Aspekte über die Planung der Migration hinaus.

Es gibt verschiedene Methoden, um die Integration von cloud-basierten Dynamics 365 Funktionen vorzubereiten. Die Institution muss ein Sicherheitskonzept erstellen und dokumentieren, dass 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 Dynamics 365
- Definition des Administrationsmodells für die cloud-basierten Dynamics 365 Funktionen, z. B. Nutzung von Azure Active Directory (Azure AD) vs. Active Directory Federation Services (ADFS)
- Informationsmanagement (Datensicherung und Datenhaltungsstrategie) für in der Cloud und On-Premise gespeicherte Informationen

Zu den Integrationsmöglichkeiten von Dynamics 365 gehören:

- Hybride Nutzung (Gemeinsame Nutzung von Cloud-Diensten und lokale Diensten) mit Synchronisation, einschließlich der Möglichkeit der Migration auf cloud-basierte Dienste und der Deaktivierung von lokalen Komponenten in einem nachgelagerten Schritt.[34]
- Verwendung von Drittanbieterwerkzeugen für Dynamics 365

Um die Verbindung zwischen Cloud-Diensten und lokalen Diensten abzusichern, kann ein Cloud Access Security Broker (CASB) wie Microsofts Cloud App Security[35] verwendet werden. Zum Zeitpunkt der Erstellung dieses Leitfadens, waren die CASB-Funktionen nur für Dynamics 365 CRM verfügbar. 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.

Zusätzlich wird eine Lernplattform angeboten, auf der viele spezifische und unterstützende Inhalte für Schulungszwecke zu finden sind.[36]

Mit dem Evergreen-Ansatz ist Microsoft bestrebt, alle Azure-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 Change Management mit sich, da sie Änderungen in der Nutzung oder, falls erforderlich, in ihren Geschäftsprozessen berücksichtigen müssen.[37]

Hinweis: Diese Anforderung ist kundenspezifisch, da sie die interne Planung für die sichere Integration bestehender Dienste umfasst.

[34] https://docs.microsoft.com/de-de/powerapps/developer/common-data-service/data-export-service

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

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

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

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

Basierend auf den identifizierten Anforderungen (siehe Kapitel 3.2 *OPS.2.2.A2 Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung*) sollte ein Sicherheitskonzept für die Nutzung von Dynamics 365 als Cloud-Dienst entwickelt werden. Gefährdungen ergeben sich unter anderem 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-Dienst-Kunde, Microsoft als Cloud-Dienstanbieter und Netzbetreiber.

Obwohl es keine allgemeine Vorlage für die Anforderungen einer Institution gibt, geht Microsoft Dynamics 365 wie in der folgenden Tabelle dargestellt, auf viele der in den offiziellen Umsetzungshinweisen des IT-Grundschutz genannten Bedrohungen und Sicherheitsmaßnahmen ein:

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

Cloud-spezifische Bedrohungen	Bedingungen für Dynamics 365	Referenzen
Freiwillige oder erzwungene Beendigung des Vertrages	Die Vertragsbeendigung wird im Rahmen einer gesonderten Anforderung detailliert behandelt.	Kapitel 3.14 *OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses*
Fehlende Portabilität, z. B. aufgrund proprietärer Datenformate (möglicherweise mit der Folge von Lock-in-Effekten)	Portabilität wird im Detail in einer gesonderten Anforderung behandelt.	Kapitel 3.15 *OPS.2.2.A15 Portabilität von Cloud-Diensten*
Fehlende Kenntnisse über den physischen Datenspeicherort	Dynamics 365 bietet einen Überblick von Rechenzentren innerhalb der Regionen und ermöglicht die Standortauswahl innerhalb eines Abonnements. Die Daten werden dann in den Rechenzentren an diesem Standort gespeichert. Alle Rechenzentren von Microsoft sind physisch gegen unbefugten Zugriff und verschiedene andere Bedrohungen geschützt.	https://aka.ms/dynamics_365_international_availability_deck (in Englisch) https://www.microsoft.com/de-de/trust-center/privacy/data-location 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	Mit Mobile Device Management (MDM) oder Intune können mobile Geräte, die auf Dynamics 365 zugreifen dürfen, gesichert und konfiguriert werden.	https://docs.microsoft.com/de-de/dynamics365/mobile-app/v8/set-up-manage/secure-manage

Cloud-spezifische Bedrohungen	Bedingungen für Dynamics 365	Referenzen
Arten von Geräten oder Software (PC, Laptop, Smartphone, Browser, Apps usw.) abgerufen werden	Zusammen mit dem bedingten Zugriff (Conditional Access) kann MDM verwendet werden, um den Zugriff auf bestimmte Daten oder Dienste innerhalb von Dynamics 365 zu beschränken. Diese 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)	Die Funktion für den bedingten Zugriff (Conditional Access) ermöglicht es, den Zugriff auf Dienste basierend auf kundendefinierbaren Bedingungen wie Quell-IP, Gerätebenutzer oder der Authentifizierungsmethode einzuschränken. Zusätzlich kann der Zugriff mit vertrauenswürdigen IP-Adressregeln in Dynamics 365 eingeschränkt werden. Auch bei Betrieb auf gleicher Hardware 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 diese im gespeicherten Zustand und während des Transports, einschließlich der Übertragung zwischen Dynamics 365-Rechenzentren, mit Hilfe anerkannter Protokolle und kryptographischer Methoden wie AES verschlüsselt. Die Verschlüsselung muss gegebenenfalls aktiviert werden.	https://docs.microsoft.com/de-de/azure/active-directory/conditional-access/overview https://docs.microsoft.com/de-de/power-platform/admin/restrict-access-online-trusted-ip-rules https://docs.microsoft.com/de-de/dynamics365/admin/multiple-online-instances-tenants https://docs.microsoft.com/de-de/dynamics365/admin/data-encryption https://docs.microsoft.com/de-de/microsoft-365/compliance/office-365-encryption-in-microsoft-dynamics-365

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 z. B. anhand einer Punktematrix 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 Anforderungen an den Cloud-Dienst. 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 fest definierten Zeitraum betrachtet werden können.

Vor der Bewertung der Angebote müssen die grundlegenden Aspekte untersucht und entsprechende Antworten eingeholt werden.[38] 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.[39]

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 Dynamics 365 zur Verfügung.[40]

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

Zu berücksichtigende Überlegungen	Bedingungen für Dynamics 365	Referenzen
Öffentlich zugängliche Informationen über den Anbieter (Reputation, Bewertungen und Rankings, Kerngeschäft, Performance, Cloud-Erfahrung)	Cloud-Computing gehört zu den Kerngeschäften von Microsoft und Microsoft gehört zu den am besten bewertetesten Cloud-Diensteanbietern laut verschiedenen Erhebungen. Dynamics 365 wird ständig aktualisiert und weiterentwickelt. Microsoft veröffentlicht auf seiner Webseite Roadmaps und weitere Informationen über geplante Updates für Dynamics 365. In der Microsoft technet Community können sich Kunden mit anderen Kunden austauschen, um weitere Informationen über Dynamics 365 zu erhalten.	https://www.microsoft.com/en-us/investor/default.aspx (in Englisch) https://dynamics.microsoft.com/de-de/business-applications/product-updates/ https://docs.microsoft.com/de-de/dynamics365-release-plan/2019wave2/ https://techcommunity.microsoft.com/ (in Englisch) https://dynamics.microsoft.com/de-de/customer-stories/

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

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

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

Zu berücksichtigende Überlegungen	Bedingungen für Dynamics 365	Referenzen
	Microsoft stellt Kundenberichte über den Einsatz von Dynamics 365 zur Verfügung. Microsoft bietet die Funktion Service Health im Microsoft 365 Admin Center, die den aktuellen Status von Diensten wie Dynamics 365 anzeigt. Kunden können die Dienste-Statusseite auf bekannte Probleme hin überprüfen, ohne sich mit anmelden zu müssen.	https://docs.microsoft.com/en-us/dynamics365/customer-engagement/admin/check-online-service-health (in Englisch)
Due-Diligence	Microsoft stellt eine Checkliste für die Bearbeitung der Due-Diligence-Schritte zur Verfügung. Microsoft bietet eine breite Palette an 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/microsoft-365/compliance/offering-home
Zugriff durch Cloud-Diensteanbieter oder Dritte	Microsoft-Mitarbeiter haben standardmäßig keinen Zugriff auf Kundendaten und Kunden-Tenants. Wenn ein Zugriff erforderlich ist, wird MFA verpflichtend eingesetzt und es wird nach dem Least-Privilege-Prinzip sowie mit permanenter Protokollierung und Überwachung gearbeitet. Die in Dynamics 365 implementierte Kundenisolierung stellt sicher, dass Kunden nicht auf die Daten anderer Kunden zugreifen können, auch wenn sie auf derselben Hardware verarbeitet oder gespeichert werden. Daten werden in Dynamics 365 auf dem Speichermedium und während der Übertragung verschlüsselt, sodass Unbefugte keinen Zugriff auf die enthaltenen Informationen erhalten.	https://www.microsoft.com/de-de/trust-center/privacy/data-access https://docs.microsoft.com/de-de/dynamics365/admin/multiple-online-instances-tenants https://docs.microsoft.com/de-de/dynamics365/admin/data-encryption https://docs.microsoft.com/de-de/microsoft-365/compliance/office-365-encryption-in-microsoft-dynamics-365
Installation von zusätzlicher Software	Auf Dynamics 365 kann mit dem Browser oder mit zur lokalen Installation geeigneter Anwendungen zugegriffen werden. Der Zugriff auf Letztere variiert je nach Abonnementtyp.	https://docs.microsoft.com/de-de/dynamics365/customer-engagement/on-premises/deploy/system-requirements-required-technologies

Zu berücksichtigende Überlegungen	Bedingungen für Dynamics 365	Referenzen
Standorte des Cloud-Diensteanbieters	Die Kundendaten werden in der oder den vom Kunden ausgewählten Regionen gespeichert. Aus Gründen der Datenverarbeitung können Kundendaten jedoch auch außerhalb der gewählten Region verarbeitet werden. Zu Sicherungszwecken werden Kundendaten in andere Rechenzentren innerhalb derselben Region repliziert.	https://docs.microsoft.com/de-de/dynamics365/get-started/availability https://www.microsoft.com/de-de/trust-center/privacy/data-location https://www.microsoft.com/de-de/TrustCenter/Privacy/dynamics365-finance-operations
Subunternehmer des Cloud-Diensteanbieters	Microsoft veröffentlicht und aktualisiert regelmäßig eine Liste von Subunternehmern, die mit den Daten von Kunden arbeiten dürfen. Subunternehmer, die für Microsoft arbeiten, sind verpflichtet, am Microsoft Supplier Security and Privacy Assurance Program teilzunehmen. Dieses Programm stellt sicher, dass die von Microsoft implementierten Regeln und Prozesse auch von Subunternehmern eingehalten werden. Es trägt dazu bei, den Umgang mit Daten zu standardisieren und abzusichern. 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-Services-Lieferantenliste, in Englisch) http://download.microsoft.com/download/0/4/3/043398DF-05CD-45F4-9A55-EEC1EECEF386/Online_Serv_Subcontractor_List.pdf (Liste der Subunternehmer, in Englisch) https://www.microsoft.com/de-de/trust-center/privacy/data-access https://www.microsoft.com/en-us/procurement/supplier-contracting.aspx (in Englisch)
Berücksichtigung von Vertragsgrundlagen und Vorschriften	Die Service Level Agreements und die Bestimmungen für Onlinedienste von Microsoft sind die Standardbedingungen für die Nutzung von Dynamics 365-Diensten. Sie werden auf der Webseite veröffentlicht und sind ohne Microsoft oder Dynamics 365 Konto zugänglich.	https://www.microsoft.com/de-de/licensing/product-licensing/products.aspx (Service Level Agreements (SLA))
Bewertung von Dienstleistungen einschließlich Garantien	Leistungsbeschreibungen, Dokumentationen und Preisinformationen werden auf den Webseiten der einzelnen Dienste veröffentlicht.	https://dynamics.microsoft.com/de-de/pricing/

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

Nach der Auswahl von einem 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 Dynamics 365 verarbeiteten Daten konform sein. Die zuvor definierten Anforderungen sind zu berücksichtigen und mindestens die folgenden Punkte sind in Bezug auf Dynamics 365 zu beantworten.

Tabelle 8: Inhalt, der bei der Vertragsausarbeitung zu berücksichtigen ist

Vertragsunterlagen	Bedingungen für Dynamics 365	Referenzen
Physischer Standort der Dienste und des Cloud-Diensteanbieter	Die Cloud-Dienste werden in Rechenzentren in den vom Kunden ausgewählten Region betrieben. Die gespeicherten Daten werden in der gewählten Region gespeichert. Aus Gründen der Datenverarbeitung können Kundendaten jedoch außerhalb der gewählten Geolokalisierung verarbeitet werden.	https://docs.microsoft.com/de-de/dynamics365/get-started/availability https://www.microsoft.com/de-de/trust-center/privacy/data-location https://www.microsoft.com/de-de/TrustCenter/Privacy/dynamics365-finance-operations https://azure.microsoft.com/de-de/global-infrastructure/regions/
Überwachung der Leistungserbringung	Microsoft stellt die Funktion Service Health im Microsoft 365 Admin Center zur Verfügung, die den aktuellen Status von Dynamics 365 Diensten anzeigen. Kunden können die Statusseite des Dienstes auf bekannte Probleme überprüfen, ohne sich bei ihrem Tenant anmelden zu müssen.	https://docs.microsoft.com/en-us/dynamics365/customer-engagement/admin/check-online-service-health (in Englisch)
Subunternehmer und Dritte, die an der Erbringung von Dienstleistungen beteiligt sind	Microsoft setzt Subunternehmer für spezifische, begrenzte Unterstützungsaufgaben 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 Services Lieferantenliste, in Englisch) http://download.microsoft.com/download/0/4/3/043398DF-05CD-45F4-9A55-EEC1EECEF386/Online_Serv_Subcontractor_List.pdf (Liste der Subunternehmer, in Englisch)

Vertragsunterlagen	Bedingungen für Dynamics 365	Referenzen
		https://www.microsoft.com/en-us/procurement/supplier-contracting.aspx (in Englisch)
Regeln für das Personal des Cloud-Dienstean-bieters	Das bei Microsoft beschäftigte Personal (intern und extern) verfügt über alle erforderlichen Kompetenzen und wird gemäß den internen Richtlinien überprüft.	https://www.microsoft.com/en-us/corporate-responsibility/empowering-employees (in Englisch)
Regeln für Kommunikationskanäle und Ansprechpartner	Die zentrale Anlaufstelle für Kunden ist der Account Manager. Der Supportmenüpunkt im administrativen Portal von Dynamics 365 stellt den Hauptkommunikationskanal dar. Über die Support-Webseite kann Microsoft ebenfalls kontaktiert werden.	https://dynamics.microsoft.com/de-de/contact-us/
Regeln für Prozesse, Arbeitsabläufe und Verantwortlichkeiten	Dynamics 365 wird als Online-Cloud-Dienst bereitgestellt und unterliegt einem umfassenden Regelwerk, einschließlich Informationssicherheitsrichtlinien (z. B. Asset Management, Schutz vor Malware). Die Aufteilung der Verantwortlichkeiten, Prozesse und Verfahren ist in der Regel in den jeweiligen Vereinbarungen festgelegt. Darüber hinaus werden dem Kunden für Dynamics 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 festgelegt.	https://www.microsoft.com/de-de/licensing/product-licensing/products.aspx https://docs.microsoft.com/de-de/microsoft-365/compliance/offering-home Kapitel 2.1 *Modell der gemeinsamen Verantwortung* https://dynamics.microsoft.com/de-de/business-applications/product-updates/ https://docs.microsoft.com/de-de/dynamics365-release-plan/2019wave2/

Vertragsunterlagen	Bedingungen für Dynamics 365	Referenzen
Bestimmungen zur Beendigung der vertraglichen Vereinbarung	Dynamics 365 wird im Rahmen eines Jahresabonnements angeboten. Eine vorzeitige Kündigung kann möglich sein.	https://www.microsoft.com/de-de/licensing/product-licensing/products.aspx (Online Service Terms (OST)) Kapitel 3.14 *OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses*
Sichere Löschung der Daten durch den Cloud-Diensteanbieter	Wenn ein bezahltes Abonnement gekündigt wird oder endet, wird das Kundenkonto von Dynamics 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 werden gelöscht. Das Konto selbst wird spätestens 180 Tage nach seiner Kündigung oder Beendigung des Abonnements gelöscht. Physische Speichermedien werden am Ende ihrer Nutzungsdauer vor Ort sicher vernichtet.	https://www.microsoft.com/de-de/TrustCenter/Privacy/You-are-in-control-of-your-data https://www.microsoft.com/en-us/trust-center/privacy/data-management https://aka.ms/DPA
Notfallvorsorge	Dynamics 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/de-de/licensing/product-licensing/products.aspx (Servie Level Agreements (SLA)) https://www.microsoft.com/de-de/trust-center/privacy/data-location
Gesetzliche Anforderungen	Microsoft hält sich an die Gesetze und Regeln bezüglich der Bereitstellung des Cloud-Dienstes. Microsoft veröffentlicht zweimal jährlich Daten über Anfragen von Strafverfolgungsbehörden auf der ganzen Welt und darüber, wie sie behandelt wurden.	https://www.microsoft.com/en-us/corporate-responsibility/lerr (in Englisch)
Externe Prüfungen und Audits	Dynamics 365 wird aufgrund der Anforderungen mehrerer Normen und Zertifizierungen kontinuierlich auditiert. Microsoft stellt Informationen über seine Konformität, Audits und	https://docs.microsoft.com/de-de/microsoft-365/compliance/offering-home

Vertragsunterlagen	Bedingungen für Dynamics 365	Referenzen
	Zertifizierungen zur Verfügung – einschließlich öffentlich zugänglicher Berichte und Ergebnisse.	https://docs.microsoft.com/de-de/azure/security/fundamentals/pen-testing
	Cloud-Kunden haben die Möglichkeit, Penetrationstests an ihren Cloud-Diensten durchzuführen. Hierüber muss Microsoft nicht informiert werden. Die Durchführung von Penetrationstests ist an die Einhaltung der von Microsoft aufgestellten Einsatzbestimmungen gebunden. Die Haupteinschränkung besteht darin, dass keine Denial of Service (DoS)-Tests erlaubt sind. Auch andere Dynamics 365-Kunden dürfen durch den Penetrationstest nicht gestört werden.	https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement (in Englisch)

Hinweis: Die vertraglichen Regelungen zum Datenschutz können von Institution zu Institution unterschiedlich sein und sollten daher gemeinsam mit dem Datenschutzbeauftragten oder der Rechtsabteilung bewertet werden. Solange keine zertifizierbaren Nachweise der DSGVO-Konformität vorliegen, können die bestehenden Vertragsklauseln gemeinsam mit Microsoft verschärft werden.[41]

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, die die Migration verhindern oder behindern können, zu erkennen und darauf zu reagieren. Gegebenenfalls sollte die Migration abgebrochen und eine Untersuchung der Probleme durchgeführt werden. Um das Risiko von wesentlichen Schwierigkeiten zu verringern, sollte zunächst eine Test- oder Pilotmigration durchgeführt werden.

Hinweis: Diese Anforderung ist kundenspezifisch, da sie die interne Planung für die sichere Migration bestehender Dienste abdeckt. Microsoft FastTrack bietet eine Vielzahl von Tools, die bei der Migration aktueller Ressourcen zu Dynamics 365 helfen.[42]

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

Als präventive Sicherheitsmaßnahme für Dynamics 365 sollte ein Notfallkonzept entwickelt werden. Insbesondere das Fehlen eines Notfallwiederherstellungsplans kann zu langen Ausfallzeiten führen,

[41] https://www.microsoft.com/de-de/trust-center/privacy/gdpr-overview

[42] https://www.microsoft.com/de-de/fasttrack/
https://docs.microsoft.com/de-de/dynamics365/get-started/fasttrack/customer-engagement/microsoft-fasttrack-dynamics-365

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[43] abgedeckt. Stattdessen deckt diese Anforderung den individuellen Wiederherstellungsplan für eine Institution im Falle des Verlustes des Cloud-Dienstes selbst oder des kurzfristigen Ausfalls ab. Es geht auch um Situationen, in denen die geltenden Service Levels die Anforderungen nicht erfüllen.

Sollte der Onlinedienst 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 Dynamics 365 beinhalten. In diesem Fall muss ein Dynamics 365 Plan mit dem Einsatz von Desktop-Software gewählt werden. Alternativ könnte auch die Verwendung von Dynamics 365 als Hybridlösung[44] in Betracht gezogen werden, um die Auswirkungen der Nichtverfügbarkeit von Onlinediensten zu reduzieren.

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

Darüber hinaus sollten Notfallpläne für die relevanten Geschäftsprozesse, die auf Dynamics 365 basieren, spezifisch und detailliert auf den Verlust der Verfügbarkeit hin untersucht werden. Dies ist unabhängig von der Ursache des Verfügbarkeitsverlustes zu planen (z. B. Ausfall des Internetzugangs im lokalen Netz, Ausfall beim Internetanbieter).

Hinweis: Diese Anforderung ist kundenspezifisch, da sie die interne Planung für ein Notfallmanagement abdeckt.

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

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

Tabelle 9: Sicherheitsvorkehrungen zur Wahrung der Informationssicherheit

Erforderliche Sicherheitsvorkehrungen	Details zu Dynamics 365	Referenzen
Aktualisierung der Dokumentation und Richt-	Die regelmäßige Überprüfung und Aktualisierung der Richtlinien ist Teil eines effektiven ISMS. Dieser Prozess	https://servicetrust.microsoft.com/ (in Englisch)

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

[44] https://docs.microsoft.com/de-de/office365/enterprise/hybrid-cloud-overview

Erforderliche Sicherheitsvorkehrungen	Details zu Dynamics 365	Referenzen
linien (z. B. Betriebsanleitungen und Verfahren) in regelmäßigen Abständen	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.	
Regelmäßige Überprüfung von erbrachten Dienstleistungen	Dynamics 365 beinhaltet ein integriertes SLA-Überwachungssystem ("Service Health"), das es Kunden ermöglicht, die Einhaltung der Dienste über das Microsoft 365 Admin Center zu überprüfen. Dazu gehört auch das Empfangen von Meldungen des Dienstes 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.	https://docs.microsoft.com/en-us/dynamics365/customer-engagement/admin/check-online-service-health (in Englisch) https://www.microsoft.com/de-de/licensing/product-licensing/products.aspx (Online Service Terms (OST)) https://www.microsoft.com/en-us/procurement/contracting-terms-conditions.aspx (in Englisch)
Bereitstellung von Sicherheitsnachweisen durch den Cloud-Diensteanbieter	Dynamics 365 bietet in diesem Fall eine Vielzahl von Publikationen und Verifizierungen sowie entsprechende Zertifizierungen. Dies kann von einem Benutzer von Dynamics 365 auf der öffentlichen Webseite sowie in den Auditergebnissen, die im Service Trust Portal (STP) eingesehen werden können, überprüft werden.	https://servicetrust.microsoft.com/ (in Englisch) https://docs.microsoft.com/de-de/microsoft-365/compliance/offering-home?tem=Dynamics%20365 https://servicetrust.microsoft.com/Documents/Compliance-Reports
Regelmäßige Abstimmungsgespräche zwischen dem Cloud-Diensteanbieter und dem Kunden	Dynamics 365 bietet eine Vielzahl von Möglichkeiten zur Unterstützung und Erfassung von Statusinformationen (z. B. mit Service Health über das Microsoft 365 Admin-Center). Im Falle einer erheblichen Störung des Dienstes werden die Kunden kontaktiert.	https://docs.microsoft.com/en-us/dynamics365/customer-engagement/admin/check-online-service-health (in Englisch) https://dynamics.microsoft.com/de-de/support/
Planung von Übungen und Tests zur Reaktionssimulation bei Systemausfällen	Dynamics 365 hat Regeln für die Fortsetzung der Dienste auf dem im SLA festgelegten Niveau definiert.	https://www.microsoft.com/de-de/licensing/product-licensing/products.aspx (Online Service Terms (OST))

Erforderliche Sicherheitsvorkehrungen	Details zu Dynamics 365	Referenzen
Sicherstellung der ordnungsgemäßen Verwaltung von Cloud-Diensten	Diese Anforderung liegt in der Verantwortung des Cloud-Nutzers. 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. Die Verwaltung von Dynamics 365 ist im Admin Center von Dynamics 365 zentralisiert. Für Administratoren ist eine Dokumentation verfügbar.	https://docs.microsoft.com/de-de/dynamics365/marketing/dynamics-365-admin-center https://docs.microsoft.com/de-de/dynamics365/fin-ops-core/dev-itpro/sysadmin/security-architecture (in Englisch) https://docs.microsoft.com/de-de/dynamics365/
Sicherstellung der Interoperabilität von Cloud-Diensten	Bei der Nutzung mehrerer Cloud-Dienste sollten für jeden Dienst Interoperabilitätstests durchgeführt werden, um eine ordnungsgemäße Zusammenarbeit zwischen den verschiedenen Cloud-Diensten zu gewährleisten. Dynamics 365 bietet z. B. Interoperabilität für Outlook an.	https://www.microsoft.com/en-us/legal/interoperability/default.aspx (in Englisch) https://docs.microsoft.com/de-de/dynamics365/outlook-addin/admin-guide/dynamics-365-for-outlook https://docs.microsoft.com/de-de/dynamics365/get-started/fast-track/customer-engagement/microsoft-fasttrack-dynamics-365 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. Diese Anforderung liegt in der Verantwortung des Kunden. Datensicherungen können entweder durch eine hybride Umgebung oder durch einen Datensicherungsdienst eines externen Anbieters oder eines Datensicherungssystems des Kunden durchgeführt werden. Wird sich für einen externen Anbieter entschieden, muss der Kunde sicherstellen, dass alle Anforderungen an Datensicherung und Datensicherheit erfüllt sind.	https://docs.microsoft.com/de-de/dynamics365/admin/backup-restore-instances Kapitel 3.16 *OPS.2.2.A16 Durchführung eigener Datensicherungen*

Erforderliche Sicherheitsvorkehrungen	Details zu Dynamics 365	Referenzen
	Dynamics 365 sichert alle Instanzen kontinuierlich und die Backups werden für 28 Tage aufbewahrt. Der Cloud-Nutzer kann auf Wunsch und in eigener Verantwortung Datensicherungen durchführen.	
Kontrolle der technischen Maßnahmen zur Verhinderung der Nutzung nicht autorisierter Dienste	Diese Anforderung liegt in der Verantwortung des Kunden. Die IT-Organisation sollte die technischen Maßnahmen, z. B. mit Hilfe von Proxies oder Cloud Access Security Brokern (CASB), kontrollieren, um die unberechtigte Nutzung von Diensten zu verhindern.	https://docs.microsoft.com/de-de/azure/active-directory/users-groups-roles/roles-delegate-by-task https://docs.microsoft.com/de-de/cloud-app-security/
Durchführung von Audits, Sicherheitschecks, Penetrationstests oder Schwachstellenanalysen	Cloud-Nutzer haben die Möglichkeit, Penetrationstests oder Schwachstellenscans gegen ihre Cloud-Dienste durchzuführen, ohne Microsoft zu benachrichtigen, wenn die entsprechenden Einsatzbestimmungen eingehalten werden. Die Haupteinschränkungen bestehen darin, dass keine Denial of Service (DoS)-Tests erlaubt sind und dass keine anderen Kunden durch die durchgeführten Tests gestört werden dürfen. Microsoft führt Penetrationstests und Schwachstellenscans gegen Dynamics 365 und Audits durch. Die Berichte werden den Cloud-Nutzer im Service Trust Portal (STP) zur Verfügung gestellt.	https://docs.microsoft.com/de-de/azure/security/fundamentals/pen-testing https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement (in Englisch) https://servicetrust.microsoft.com (in Englisch)

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

Im Rahmen eines effizienten Informationssicherheitsmanagements sollte die regelmäßige Überprüfung der festgelegten Sicherheitsvorkehrungen durchgeführt werden. Dadurch wird sichergestellt, dass der Kunde 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 Dynamics 365 wird aufgrund der Anforderungen mehrerer internationaler und nationaler Compliance-Standards und Zertifizierungen kontinuierlich auditiert. Die Liste der Konformitätsnormen für Dynamics 365 umfasst ISO 27001 ISO 27017 und ISO 27018[45] (siehe Kapitel 5 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)[46] 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.

Hinweis: Diese Anforderung ist kundenspezifisch, da sie die regelmäßige Überprüfung der Sicherheitsvorkehrungen zur Erfüllung der Auditanforderungen durch den Kunden umfasst.

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-Nutzungs-Verhätnisses definiert werden. In einer kritischen Situation verhindert das Fehlen vertraglicher Regelungen die Auflösung des Dienstleistungsverhältnisses. Nach Auflösung 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 Dynamics 365. Das Planungs- und Migrationskonzept sollte das Sicherheitskonzept genauso berücksichtigen wie bei der ursprünglichen Umstellung auf die Cloud.

In Dynamics 365 sind mehrere Funktionen und Schnittstellen für den Datenexport implementiert. Es gibt eine Reihe kommerzieller Lösungen, die auch Datensicherungen in die Cloud selbst oder auf lokalem Speicher anbieten (siehe Kapitel 3.16 *OPS.2.2.A16 Durchführung eigener Datensicherungen*).

Standardmäßig können Dynamics 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[47].

Bei der Kündigung des Dynamics 365 Vertrags als Online-Dienst sollte der Kunde unter anderem Folgendes sicherstellen:

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

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

[46] https://servicetrust.microsoft.com/ (in Englisch)

[47] https://www.microsoft.com/de-de/TrustCenter/Privacy/You-are-in-control-of-your-data
https://www.microsoft.com/en-us/trust-center/privacy/data-management
https://aka.ms/DPA

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-Diensteanbieters oder bei der Rückführung eines Cloud-Diensts in die eigene Infrastruktur zu gewährleisten. In diesem Fall sind eine Reihe von Anforderungen zu berücksichtigen, insbesondere in Bezug auf Dateiformate und Portabilitätstests.

Dynamics 365 unterstützt verschiedene Methoden der Datenmigration:

1. Verwendung von Dynamics 365 APIs, die den Zugriff auf Kundendaten ermöglichen.[48]
2. Mit dem Add-On-Dienst Data Export (z. B. für Customer Engagement) können Daten aus Dynamics 365 Deutschland in eine Microsoft Azure SQL-Datenbank repliziert werden.[49]
3. Synchronisation von Daten mit lokalen Komponenten bei Verwendung der hybriden Cloud-Lösung.[50]
4. Verwendung von Drittanbieterwerkzeugen für Dynamics 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.[51]

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 Dynamics 365 (Funktionalität, Sicherheit, Leistung, Skalierbarkeit etc.)?
- Ist die neue Plattform in der Lage, die exportierten Daten von Dynamics 365 zu verarbeiten?
- Gibt es Werkzeuge 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 Dynamics 365 Daten verloren geht, Cloud-Dienste selbst nicht verfügbar sind oder Daten durch Benutzeraktionen (z. B. versehentliches Löschen von Daten) verloren gehen.

Der Kunde sollte entscheiden, ob die Datenrettungsfunktionen und -optionen in Dynamics 365 seinen Anforderungen entsprechen, z. B. gesetzliche, vertragliche oder allgemeine Schutzanforderungen, oder ob ein zusätzlicher Export in lokale oder andere Cloud-Datensicherungsspeicher implementiert werden soll. Dies sollte in der Datensicherungsrichtlinie der Institution berücksichtigt werden, die im

[48] https://docs.microsoft.com/de-de/dynamics365/fin-ops-core/dev-itpro/data-entities/data-management-api (in Englisch)

[49] https://appsource.microsoft.com/en-us/product/dynamics-365/mscrm.44f192ec-e387-436c-886c-879923d8a448?tab=Overview (in Englisch)

[50] https://www.microsoft.com/en-us/download/details.aspx?id=18039 (Microsoft Dynamics CRM Online-Migration auf Microsoft Dynamics CRM vor Ort, in Englisch)

[51] DOCX-Dateien: https://msdn.microsoft.com/en-us/library/dd773189(v=office.12).aspx (in Englisch)
XLSX-Dateien: https://msdn.microsoft.com/en-us/library/dd922181(v=office.12).aspx (in Englisch)
PST-Dateien: https://msdn.microsoft.com/en-us/library/ff385210(v=office.12).aspx (in Englisch)

IT-Grundschutz Baustein *CON.3 Datensicherungsrichtlinie*[52] 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 Entscheidung berücksichtigt werden.

Dynamics 365 bietet verschiedene Möglichkeiten zum Exportieren und Sichern von Daten. Beispielsweise wird der Customer Engagement Service standardmäßig gesichert[53]. Außerdem läuft er auf einer Azure SQL-Datenbank, die ebenfalls standardmäßig gesichert wird.[54] Zusätzlich ist ein Export nach Excel[55] möglich. Dynamics 365 Daten können bei einer lokalen Installation von Microsoft Dynamics CRM verwendet werden. Die Daten können auch mit einer lokalen Anwendung synchronisiert werden[56]. Falls ein Massenexport durchgeführt werden muss, stehen Lösungen von Drittanbietern zur Verfügung.

Bei der Entscheidung und Durchführung von Datensicherungen sollte der Kunde 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, Schutz- und sonstigen Anforderungen?
- Entspricht das Datensicherungs-Speichermedium (lokal oder Cloudbasiert) den gesetzlichen, vertraglichen, 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. Microsoft Azure bietet Verschlüsselung für seine Infrastructure as a Service, Platform as a Service und Software as a Service Optionen mit Verschlüsselung in einer Reihe von Bereichen. Dynamics 365 ist bereits durch das sichere in Microsoft Azure laufende Backend geschützt. Der Cloud-Nutzer hat die Möglichkeit, die Verschlüsselung mit Standard- oder individuellen Verschlüsselungstechnologien zu aktivieren, je nach gewähltem Dienst.[57] Die verschiedenen Verschlüsselungsoptionen sind Dienst-abhängig und müssen vom Kunden von Fall zu Fall anhand der von Microsoft für Dynamics 365 bereitgestellten Dokumentation und Richtlinien bewertet werden.

[52] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_3_Datensicherungskonzept.html

[53] https://docs.microsoft.com/de-de/dynamics365/admin/backup-restore-instances

[54] https://docs.microsoft.com/de-de/azure/sql-database/sql-database-automated-backups

[55] https://docs.microsoft.com/de-de/dynamics365/customerengagement/on-premises/basics/export-data-excel

[56] https://www.microsoft.com/en-us/download/details.aspx?id=18039 (Microsoft Dynamics CRM Online-Migration auf Microsoft Dynamics CRM vor Ort, in Englisch)

[57] https://docs.microsoft.com/de-de/microsoft-365/compliance/office-365-encryption-in-the-microsoft-cloud-overview

Die folgende Tabelle veranschaulicht die Funktionalitäten von Dynamics 365 zur Verschlüsselung von übertragenen und gespeicherten Daten als auch die sicheren Verwaltung von Geheimnissen.

Tabelle 10: Angebote zur Verschlüsselung und Kryptographie in Dynamics 365

Kategorie	Details	Referenzen
Verschlüsselung von gespeicherten Daten	Die Datenbanken von Dynamics 365 Customer Engagement werden mit der FIPS 140-2-konformen Transparent Data Encryption (TDE) von Microsoft SQL Server (und der Azure SQL Datenbank) verschlüsselt. Zusätzlich bietet Microsoft eine Verschlüsselung auf Feldebene in der SQL Datenbank für Dynamics 365 an.	https://docs.microsoft.com/en-us/dynamics365/customer-engagement/admin/data-encryption (in Englisch) https://docs.microsoft.com/de-de/previous-versions/dynamicscrm-2016/developers-guide/dn481562(v=crm.8)
Verschlüsselung von Daten während der Übertragung	Dynamics 365 verschlüsselt Verbindungen mit Industriestandards wie AES und TLS/SSL.	https://docs.microsoft.com/de-de/microsoft-365/compliance/office-365-encryption-in-microsoft-dynamics-365
Schlüsselverwaltung und eigene Verschlüsselungsmechanismen	Als SaaS-Anwendung ist es nicht möglich, einen eigenen Verschlüsselungsmechanismus zu implementieren. Microsoft stellt für seine Online-Anwendungen eine geeignete Schlüsselverwaltung 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. Darüber hinaus unterstützt Dynamics 365 Kundenschlüssel, die auf Dienst-Verschlüsselung basieren.	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/power-platform/admin/manage-encryption-key

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 SAML-Ticket an den Cloud-Diensteanbieter gesendet werden.[58] 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.[59]. Es gibt drei allgemeine Möglichkeiten hybride Konten zu realisieren. Diese bringen unterschiedlichen Vor- und Nachteilen mit:[60]

- Password Hash-Synchronisation (PHS):Für PHS synchronisiert Azure Active Directory Connect einen Hash des Benutzerpasswort-Hashes von einem lokalen Active Directory des Kunden mit dem Azure Active Directory, so dass Azure Active Directory Benutzerpasswörter direkt validieren kann.[61]

- Pass-Through-Authentifizierung (PTA):PTA ermöglicht es Benutzern, sich 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.[62]

- 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.[63]

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

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

---

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

[59] https://docs.microsoft.com/de-de/office365/enterprise/subscriptions-licenses-accounts-and-tenants-for-microsoft-cloud-offerings

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

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

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

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

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

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

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

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

[67] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_4_Identit%C3%A4ts-_und_Berechtigungsmanagement.html

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 Sicherheitüberprüfungen der Mitarbeiter durchführt.

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

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

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

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

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

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

[71] https://www.microsoft.com/en-us/procurement/supplier-conduct.aspx?activetab=pivot:primaryr5 (in Englisch)

4 Umsetzung der Mindeststandards des BSI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat zwei Mindeststandards veröffentlicht, die nur für Bundesbehörden gelten und Anforderungen an die Beschaffung, Nutzung und Beendigung von Cloud-Diensten stellen. Das BSI unterscheidet zwei Szenarien: die Nutzung[72] und Mitnutzung externer Cloud-Dienste durch eine Bundesbehörde.[73] Externe Cloud-Dienste sind in diesem Zusammenhang Cloud-Dienste, die nicht von einer Bundesbehörde bereitgestellt werden.

Kann der Bedarf an einem IT-Dienst nicht durch eigene IT-Ressourcen des Bundes gedeckt werden, sondern z. B. durch Dynamics 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 externer Cloud-Dienste die Nutzung externer Cloud-Dienste durch Nutzer einer Bundesbehörde ohne Vertragsverhältnis zwischen der Bundesbehörde und dem Cloud-Diensteanbieter.

Die Anforderungen an die Nutzung externer Cloud-Dienste werden in Kapitel 4.1 und die Anforderungen an die Mitnutzung externer Cloud-Dienste in Kapitel 4.2 behandelt.

4.1 Mindeststandard - Nutzung externer Cloud-Dienste

Die folgende Tabelle gibt einen Überblick über die Anforderungen bei der Nutzung externer Cloud-Dienste.

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

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Mitnutzung_externer_Cloud-Dienste.html

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

Tabelle 11: Übersicht über die Anforderungen an den Mindeststandard zur Nutzung externer Cloud-Dienste

Anforderung	Beschreibung
CD.01 Systembeschreibung und weitergehende Informationen fordern	Diese Anforderung stellt sicher, dass der Cloud-Diensteanbieter für den Cloud-Dienst auf die BSI C5-Anforderungen ausgerichtet ist und dem Cloud-Nutzer entsprechende Informationen zur Verfügung stehen. Dynamics 365 wird mindestens einmal jährlich hinsichtlich der Einhaltung der BSI C5-Anforderungen überprüft. Microsoft veröffentlicht den Auditbericht im Trust-Center.[74]
CD.02 Zertifizierungen oder Bescheinigungen unabhängiger Dritter festlegen	Diese Anforderung ist kundenspezifisch, da sie erforderliche Zertifizierungen und Auditberichte auf der Grundlage der Datenkategorien gemäß des Mindeststandards und der Risikoanalyse des Kunden umfasst. Microsoft verfügt über mehrere globale und regionale Zertifizierungen für Dynamics 365[75]. Darüber hinaus werden Auditberichte und andere Compliance-Informationen, wie z. B. Penetrationstests, regelmäßig auf der Webseite von Microsoft veröffentlicht[76]. Die Verantwortung für die Definition der erforderlichen Zertifizierungen und die Überprüfung, ob Dynamics 365 diese besitzt, liegt beim Kunden.
CD.03 Systembeschreibung und weitergehende Informationen auswerten	Die von Microsoft bereitgestellten Informationen sollten ausgewertet und mit der Dienstbeschreibung abgeglichen werden. Die Bewertung muss vom Kunden selbst durchgeführt werden. Dynamics 365 wird mindestens einmal jährlich hinsichtlich der Einhaltung der BSI C5-Anforderungen überprüft. Microsoft veröffentlicht den Auditbericht im Trust-Center[77], der als Referenz für die Bewertung verwendet werden kann. Informationen und Links zu Dienst-Definitionen befinden sich im Kapitel *3.3 OPS.2.2.A3 Service-Definition für Cloud-Dienste durch den Anwender*.
CD.04 Sicherheitsnachweise vertraglich zusichern	Die notwendigen Sicherheitszertifizierungen und -bescheinigungen, die in der Anforderung CD.02 *Zertifizierungen oder Bescheinigungen unabhängiger Dritter festlegen* definiert wurden, sollten vertraglich garantiert werden. Als absolutes Minimum muss der Cloud-Diensteanbieter die BSI C5-Bescheinigung regelmäßig vorlegen.

[74] https://www.microsoft.com/en-us/trustcenter/Compliance/C5 (in Englisch)

[75] https://www.microsoft.com/en-us/TrustCenter/Compliance/complianceofferings (in Englisch)

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

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

[77] https://www.microsoft.com/en-us/trustcenter/Compliance/C5 (in Englisch)

Anforderung	Beschreibung
	Microsoft besitzt die BSI C5-Bescheinigung für Dynamics 365 und veröffentlicht den Auditbericht.[74] Informationen und Links zur Informationssicherheit befinden sich im Kapitel 3.13 *OPS.2.2.A13 Nachweis einer ausreichenden Informationssicherheit* bei der Cloud-Nutzung.
CD.05 Zusätzliche Anforderungen vertraglich zusichern	Identifizierte Bedrohungen oder Risiken, die nicht durch die grundlegenden Anforderungen der BSI C5-Bescheinigung abgedeckt sind, sollten berücksichtigt werden. Für diese zusätzlichen Anforderungen sollten auf vertraglicher Basis geeignete Nachweise erbracht werden. Microsoft besitzt die BSI C5-Bescheinigung für Dynamics 365 und veröffentlicht den Auditbericht.[74] Zusätzliche Anforderungen müssen direkt mit Microsoft verhandelt werden. Informationen und Links zu Verträgen befinden sich im Kapitel 3.9 *OPS.2.2.A9 Vertragsgestaltung mit dem Cloud*. Informationen und Links zur Informationssicherheit befinden sich im Kapitel 3.13 *OPS.2.2.A13 Nachweis einer ausreichenden Informationssicherheit bei der Cloud-Nutzung*.
CD.06 Recht auf Prüfungen und Kontrollen vertraglich zusichern	Diese Anforderung betrifft die Durchführung von Audits der Dynamics 365-Umgebung durch den Kunden. Microsoft lässt Audits durch Kunden unter bestimmten, in der Microsoft Online Services DPA[78] 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 in seinem Trustcenter veröffentlicht.[79]
CD.07 Umgang mit Unterauftragnehmern und anderen externen Dritten vertraglich zusichern	Subunternehmer und ihre Geschäftsbeziehungen sind dem Kunden bekanntzugeben. Updates sollten per E-Mail oder durch eine Push-Benachrichtigung von einem Portal angekündigt werden.

[78] https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=67 (Microsoft Online Services DPA)

[79] https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings (in Englisch)

Anforderung	Beschreibung
	Microsoft stellt eine Liste von Subunternehmern zur Verfügung und bietet Zugang zu standardisierten Dienstvereinbarungen, Richtlinien und Verhaltensregeln.[80]
CD.08 Gerichtsbarkeit vertraglich zusichern	Nach Möglichkeit sollte der Gerichtsstand Deutschland sein. Es sollte sichergestellt sein, dass kein Zeitverlust entsteht, wenn ein Rechtsschutz erforderlich ist. In den Datenschutzbestimmungen wird das Land des Kunden als Gerichtsstand definiert.[81]
CD.09 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 zu einem anderen Staat. Microsoft veröffentlicht die Regionen, in denen Daten gespeichert sind, in Dynamics 365[82]. Aus Gründen der Datenverarbeitung können Kundendaten jedoch außerhalb der gewählten Region verarbeitet werden. Die geografische Speicherregion für Daten kann vom Kunden frei gewählt werden.[83] Informationen und Links zum Vertragsentwurf und zu den Dokumenten befinden sich im Kapitel 3.9 *OPS.2.2.A9 Vertragsgestaltung mit dem Cloud-Diensteanbieter*.
CD.10 Offenbarungspflichten und Ermittlungsbefugnisse vertraglich zusichern	Als Cloud-Diensteanbieter sollte Microsoft sicherstellen, dass die verarbeiteten Daten nicht im Rahmen der Offenlegungspflichten an die Ermittlungsbehörden eines ausländischen Staates weitergegeben werden. Einzelheiten zur Offenlegung von Kundendaten durch Microsoft sind in den Bestimmungen für Onlinedienste[89] geregelt. Darüber hinaus veröffentlicht Microsoft zweimal im Jahr eine Statistik zu Anfragen von Strafverfolgungsbehörden aus der ganzen Welt.[84] Informationen und Links zum Vertragsentwurf und zu den Dokumenten befinden sich im Kapitel 3.9 *OPS.2.2.A9 Vertragsgestaltung mit dem Cloud-Diensteanbieter*.

[80] https://www.microsoft.com/de-de/trustcenter/professional-services/suppliers

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

https://www.microsoft.com/de-de/servicesagreement/

[82] https://www.microsoft.com/de-de/trust-center/privacy/data-location

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

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

Anforderung	Beschreibung
CD.11 Weitere rechtliche Vereinbarungen vertraglich zusichern	Als Cloud-Diensteanbieter sollte Microsoft Sicherheitsvorfälle (und alle anderen Vorfälle) an die Behörden melden. Diese Anforderung sollte vertraglich geregelt werden. Microsoft hat eine Richtlinie[85] zur Benachrichtigung der betroffenen Parteien während eines Vorfalls zur Informationssicherheit. Informationen über die Informationspflichten der Personen im Rahmen der DSGVO werden ebenfalls veröffentlicht[86].
CD.12 Beendigung des Vertragsverhältnisses regeln	Die Kündigung des Vertrages sollte mit einer dem Einsatzszenario angemessenen Kündigungsfrist möglich sein. Die Standard-SLAs[92] von Microsoft bieten dem Kunden jederzeit ein Kündigungsrecht. Die Datenspeicherung nach der Kündigung kann zwischen den Diensten unterschiedlich sein. Informationen und Links zur Beendigung des Vertrages befinden sich im Kapitel 3.14 *OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses*.
CD.13 Datenrückgabe und Datenlöschung beim Cloud-Diensteanbieter vertraglich zusichern	Die Rückgabe der Daten muss geregelt werden und die Sicherheitsvorkehrungen müssen den festgelegten Schutzanforderungen entsprechen. Microsft gewährt 90 Tage Datenzugriff nach Beendigung des Abonnements. Spätestens nach 180 Tagen werden die Daten gelöscht.[87] Informationen und Links zum Vertragsentwurf und zur Kündigung befinden sich in den Kapiteln 3.9 *OPS.2.2.A9 Vertragsgestaltung mit dem Cloud* und 3.14 *OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses*.
CD.14 ISMS einbinden	Dynamics 365 als Cloud-Dienst sollte in das ISMS der Institution integriert werden. Dies ist eine kundenspezifische Anforderung. Informationen zum Sicherheitskonzept befinden sich im Kapitel 3.7 *OPS.2.2.A7 Erstellung eines Sicherheitskonzepts für die Cloud-Nutzung*.

[85] https://docs.microsoft.com/de-de/microsoft-365/compliance/gdpr-breach-dynamics365

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

[87] https://www.microsoft.com/de-de/TrustCenter/Privacy/You-are-in-control-of-your-data
https://www.microsoft.com/en-us/trust-center/privacy/data-management
https://aka.ms/DPA

Anforderung	Beschreibung
CD.15 Sicherheitsnachweise prüfen	Diese Anforderung verpflichtet den Nutzer, regelmäßig Nachweise zur Erfüllung der Sicherheitsanforderungen und andere Berichte von Microsoft anzufordern und zu überprüfen. Die aktuellen Zertifizierungen und Nachweise von Microsoft stehen registrierten Nutzern als [88]Prüfzeugnisse, Zertifikatsberichte etc. zur Verfügung. Die Zeiträume sind in den Berichten angegeben. Informationen befinden sich auch im Kapitel 3.13 *OPS.2.2.A13 Nachweis einer ausreichenden Informationssicherheit bei der Cloud-Nutzung*.
CD.16 Leistungsfähigkeit prüfen	Vor der Migration in die Cloud sollte sich der Cloud-Kunde vergewissern, dass die lokale Infrastruktur in Bezug auf die Leistung ausreichend ist. Insbesondere sollte die Internetverbindung den Anforderungen an Verfügbarkeit und Bandbreite entsprechen. Microsoft stellt Informationen zur Verfügung, wie die Bandbreite vor der Migration auf Dynamics 365 Onlinedienste bewertet werden kann (z. B. für Customer Engagement[89] oder Finance and Operations)[90]. Weitere Informationen und Links zur Migration und Integration von Dynamics 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*
CD.17 Informationspflichten nachhalten	Der Kunde sollte Informationen aufbewahren, die zur Beurteilung der Vertragserfüllung durch Microsoft verwendet werden können. Darüber hinaus sollten diese Informationen in das bestehende ISMS integriert werden. Die zu speichernden Informationen umfassen unter anderem die Anforderungen *CD.07 Umgang mit Unterauftragnehmern und anderen externen Dritten* vertraglich zusichern und *CD.11 Weitere rechtliche Vereinbarungen vertraglich zusichern*. Microsoft bietet die Möglichkeit, die Protokollierung unter Dynamics 365[91] zu aktivieren, und der Service Health Status[92] kann verwendet werden, um den aktuellen Status des Onlinedienstes anzuzeigen.
CD.18 Datenrückgabe durchführen	Die nutzende Behörde sollte das BSI bis zum 31. Januar eines jeden Jahres über die eigene Nutzung externer Cloud-Dienste informieren. Diese Informationen umfassen auch die Kündigung und den Wechsel von externen Cloud-Diensten.

[88] https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings (in Englisch)

[89] https://docs.microsoft.com/en-us/dynamics365/customer-engagement/admin/online-requirements (in Englisch)

[90] https://docs.microsoft.com/en-us/dynamics365/unified-operations/fin-and-ops/get-started/system-requirements (in Englisch)

[91] https://docs.microsoft.com/de-de/dynamics365/customerengagement/on-premises/deploy/microsoft-dynamics-365-monitoring-service

[92] https://docs.microsoft.com/en-us/dynamics365/customer-engagement/admin/check-online-service-health (in Englisch)

Anforderung	Beschreibung
	Diese Anforderung ist kundenspezifisch.
CD.19 Datenrückgabe ausführen	Alle Kundendaten müssen nach Beendigung der Cloud-Benutzung vom Cloud-Diensteanbieter in der vereinbarten Form zurückgegeben werden. Weitere Informationen zum Abruf der Daten aus Dynamics 365 befinden sich in der Anforderung *CD.13 Datenrückgabe und Datenlöschung beim Cloud-Diensteanbieter vertraglich zusichern* und Kapitel 3.15 *OPS.2.2.A15 Portabilität von Cloud-Diensten.*
CD:20 Datenlöschung bestätigen	Wird die Datenlöschung vom Kunden gewünscht, muss der Cloud-Diensteanbieter die Löschung aller Daten, auch der vorhandenen Datensicherungen, bestätigen. Dazu gehören auch Daten und Datensicherungen bei möglichen Subunternehmern und anderen externen Dritten. Der Kunde muss sich mit Microsoft über einen schriftlichen Nachweis der Datenlöschung in Verbindung setzen. Informationen und Links zur Beendigung der Cloud-Nutzung befinden sich im Kapitel 3.14 *OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses.*

4.2 Mindeststandard - Mitnutzung externer Cloud-Dienste

Die folgende Tabelle gibt einen Überblick über die Anforderungen bei der Mitnutzung externer Cloud-Dienste.

Tabelle 12: Übersicht über die Anforderungen an den Mindeststandard für die Mitnutzung externer Cloud-Dienste

Anforderung	Beschreibung
MCD.2.1.01 Anwendbares Recht, Gerichtsstand	Der Gerichtsstand sollte in Deutschland sein. Die Akzeptanz von Vereinbarungen ohne deutsche Rechtsgrundlage sollte im Hinblick auf Datenkategorien gemäß dem Mindeststandard und Risikoanalysen überprüft werden. Dies ist eine kundenspezifische Anforderung. Weitere Informationen und Links befinden sich in den Kapiteln 3.1 *OPS.2.2.A1 Erstellung einer Cloud-Nutzungs-Strategie* und 3.9 *OPS.2.2.A9 Vertragsgestaltung mit dem Cloud.*
MCD.2.1.02 Offenbarungspflichten und Ermittlungsbefugnisse	Diese Anforderung ist kundenspezifisch und richtet sich an Ermittlungsbehörden, die vom Cloud-Diensteanbieter zur Offenlegung verpflichtet sind. Die Abwicklung eines solchen Informationsaustauschs sollte vom

Anforderung	Beschreibung
	Kunden individuell auf der Grundlage der Klassifizierung der Daten bewertet und mit dem Cloud-Diensteanbieter geregelt werden. Diese Anforderung ist vergleichbar mit der Anforderung CD.10 *Offenbarungspflichten und Ermittlungsbefugnisse vertraglich zusichern*. Weitere Informationen und Links befinden sich im Kapitel 3.9 *OPS.2.2.A9 Vertragsgestaltung mit dem Cloud-Diensteanbieter*.
MCD.2.1.03 Datenlokationen	Der Nutzer sollte den Ort der Datenverarbeitung bestimmen. Darüber hinaus sollte die Eignung des Standortes (z. B. im Hinblick auf gesetzliche Regelungen) aus Sicht der mitnutzenden Behörde bewertet werden. Die Daten sollten daher entsprechend klassifiziert werden. Microsoft bietet Onlinedienste in mehreren Regionen an, diese sollten vertraglich zugesichert werden (siehe *CD.09 Lokation vertraglich zusichern*). Weitere Informationen und Links befinden sich im Kapitel 3.9 *OPS.2.2.A9 Vertragsgestaltung mit dem Cloud-Diensteanbieter*.
MCD.2.1.04 Nutzung und Weitergabe von Daten an Dritte	Es ist zu klären, welche Rechte dem Cloud-Diensteanbieter oder Dritten bei oder mit der Verarbeitung der Daten eingeräumt werden. Es ist zu prüfen, ob die Vereinbarungen und Bedingungen des Cloud-Diensteanbieters mit den IT-Sicherheitsrichtlinien der mitnutzenden Behörde übereinstimmen. Rechte, auf deren Grundlage Daten an Dritte für kommerzielle Zwecke verkauft oder von Microsoft selbst außerhalb der konkreten, beabsichtigten Leistungserbringung genutzt werden können, sind grundsätzlich nicht zu akzeptieren. Dies ist eine unternehmensspezifische Anforderung und vergleichbar mit der Anforderung *CD.07 Umgang mit Unterauftragnehmern und anderen externen Dritten vertraglich zusichern* Weitere Informationen und Links befinden sich im Kapitel3.9 *OPS.2.2.A9 Vertragsgestaltung mit dem Cloud-Diensteanbieter*.
MCD.2.1.05 Verfügbarkeit der Daten	Die mitnutzende Behörde als Cloud-Kunde hat dafür zu sorgen, dass das Schutzniveau für die Verfügbarkeit durch die vertraglichen Verpflichtungen des Cloud-Diensteanbieters eingehalten wird. Die Service Level Agreements und die Bestimmungen für Onlinedienste von Microsoft sind die Standardvoraussetzungen für die Nutzung von Dynamics 365-Diensten und beinhalten auch Verfügbarkeitsanforderungen.[93] Weitere Informationen und Links befinden sich in den Kapiteln 3.2 *OPS.2.2.A2 Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung*, 3.6 *OPS.2.2.A6 Planung der sicheren Einbindung von Cloud-Diensten* und 3.8 OPS.2.2.A8 Sorgfältige Auswahl eines Cloud.

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

Anforderung	Beschreibung
MCD.2.1.06 Verschlüsselung der Datenübertragung	Die Datenübertragung sollte über einen sicheren, fest definierten Kanal erfolgen. Darüber hinaus sollte geprüft werden, ob die Schlüsselstärke den IT-Sicherheitsanforderungen der mitnutzenden Behörde entspricht. Steht für die Datenübertragung eine separate BSI IT-Sicherheitsanforderung zur Verfügung, sollte diese berücksichtigt werden. Dynamics 365 verschlüsselt Verbindungen mit Industriestandards wie AES und TLS/SSL.[94] Weitere Informationen und Links befinden sich im Kapitel 3.17 *OPS.2.2.A17 Einsatz von Verschlüsselung bei Cloud-Nutzung*
MCD.2.1.07 Verschlüsselung der Daten	Gegenstand dieser Anforderung ist die Definition der verschlüsselten Speicherung von Daten. Die Entscheidung zur Verschlüsselung von Daten sollte auf den Ergebnissen der Datenkategorisierung gemäß des Mindeststandards und Risikoanalyse basieren. Die Datenbanken von Dynamics 365 Customer Engagement werden mit der FIPS 140-2-konformen Transparent Data Encryption (TDE) von Microsoft SQL Server (und der Azure SQL Datenbank) verschlüsselt.[95] Zusätzlich bietet Microsoft die Verschlüsselung auf Feldebene in der SQL Datenbank für Dynamics 365 an.[96] Weitere Informationen und Links befinden sich im Kapitel 3.17 *OPS.2.2.A17 Einsatz von Verschlüsselung bei Cloud-Nutzung*
MCD.2.1.08 Erforderliche Softwareinstallationen	Diese kundenspezifische Anforderung verlangt Regelungen für Softwareinstallationen zur gemeinsamen Nutzung auf Arbeitsplatzrechnern oder mobilen Geräten, soweit diese bei der Nutzung von Dynamics 365 erforderlich sind. Es sollte überprüft werden, ob die zu diesem Zweck zu erteilenden Zugriffs- und Ausführungsrechte mit der Informationssicherheitspolitik und dem Sicherheitskonzept der mitnutzenden Behörde übereinstimmen und ob separate Lizenzen erforderlich sein können. Darüber hinaus können sich die Behörden an dem Mindeststandard für das Management mobiler Geräte orientieren.[97] Mit Mobile Device Management (MDM) oder Intune können mobile Geräte gesichert und konfiguriert werden, die auf Dynamics 365 zugreifen dürfen.[98] Zusammen mit dem bedingten Zugriff kann dies genutzt werden, um den Zugriff auf bestimmte Daten oder Dienste innerhalb von Dynamics 365 einzuschränken.[99]

[94] https://docs.microsoft.com/de-de/microsoft-365/compliance/office-365-encryption-in-microsoft-dynamics-365

[95] https://docs.microsoft.com/en-us/dynamics365/customer-engagement/admin/data-encryption (in Englisch)

[96] https://docs.microsoft.com/de-de/previous-versions/dynamicscrm-2016/developers-guide/dn481562(v=crm.8)

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

[98] https://docs.microsoft.com/de-de/dynamics365/mobile-app/v8/set-up-manage/secure-manage
https://docs.microsoft.com/de-de/intune/fundamentals/what-is-intune

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

Anforderung	Beschreibung
	Weitere Informationen und Links zu Aspekten des Managements mobiler Geräte und des bedingten Zugangs befinden sich in der **Fehler! Verweisquelle konnte nicht gefunden werden.** im Kapitel 3.7 *OPS.2.2.A7 Erstellung eines Sicherheitskonzepts für die Cloud-Nutzung*.
MCD.2.1.09 Berechtigungsvergabe	Es sollte ein Prozess für die Vergabe von Zugriffsrechten definiert werden. Insbesondere sollte die Vergabe von privilegierten Berechtigungen im Rahmen des Genehmigungsverfahrens der mitnutzenden Behörde bewertet werden. Dynamics 365 verwendet Azure Active Directory zur Verwaltung von Identitäten und zur Authentifizierung. Dynamics 365 unterstützt Identität, die sowohl lokal als auch in der Cloud genutzt werden, als auch Identitäten, die ausschließlich in der Cloud genutzt werden. Weitere Informationen zum Identitäts- und Berechtigungsmanagement befinden sich in der **Fehler! Verweisquelle konnte nicht gefunden werden.** im Kapitel 3.2 *OPS.2.2.A2 Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung*.
MCD.2.1.10 Kündigungsfristen	Kündigungsfristen sollten mit Microsoft vereinbart werden. Es ist zu prüfen, ob die vereinbarten Kündigungsfristen mit dem Szenario der Mitnutzung vereinbar sind. Kurzfristige einseitige Kündigungs- oder Zurückbehaltungsrechte sind stets kritisch zu hinterfragen. Dies ist eine kundenspezifische Anforderung und vergleichbar mit der Anforderung CD.12 *Beendigung des Vertragsverhältnisses regeln*. Dynamics 365 wird im Rahmen eines Jahresabonnements angeboten[100]. Weitere Informationen und Links zum Vertrag zwischen dem Nutzer und Microsoft als Cloud-Diensteanbieter befinden sich in der **Fehler! Verweisquelle konnte nicht gefunden werden.** in Kapitel 3.9 *OPS.2.2.A9 Vertragsgestaltung mit dem Cloud*. Informationen zur Vertragskündigung befinden sich im Kapitel 3.14 *OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses*.
MCD.2.1.11 Datenrückgabe und Datenlöschung	Diese kundenspezifische Anforderung erfordert eine vertragliche Festlegung der Übertragbarkeit von Kundendaten und deren Löschung. Darüber hinaus ist zu prüfen, ob die Rechte und Garantien für die Rückgabe und Löschung von Daten mit den Ergebnissen der Datenkategorisierung gemäß des Mindeststandards und Risikoanalyse sowie den gesetzlichen Anforderungen vereinbar sind.

[100] https://www.microsoft.com/de-de/TrustCenter/Privacy/You-are-in-control-of-your-data

Anforderung	Beschreibung
	Dies ist eine kundenspezifische Anforderung und vergleichbar mit der Anforderung CD.13 Datenrückgabe und Datenlöschung beim Cloud-Diensteanbieter vertraglich zusichern. Microsoft gewährt 90 Tage Datenzugriff nach Beendigung des Abonnements. Spätestens nach 180 Tagen werden die Daten gelöscht.[101] Weitere Informationen befinden sich im Kapitel 3.9 *OPS.2.2.A9 Vertragsgestaltung mit dem Cloud* und 3.14 *OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses*.
MCD.2.1.12 Informationsaustausch	Diese kundenspezifische Anforderung betrifft die jährliche Verpflichtung der mitnutzenden Behörde, das BSI über gemeinsame externe Cloud-Dienste zu informieren. Dazu gehört auch die Kündigung und Portierung von Cloud-Diensten. Diese Anforderung ist vergleichbar mit der Anforderung CD.18 Datenrückgabe durchführenCD.18 .
MCD.2.2.01 Mindestanforderung an Kennwörter	Bei der Verwendung von Passwörtern sollten die von der Behörde, die den Auftrag hält, festgelegten Anforderungen an Passwörter von der mitnutzenden Behörde bewertet und gegebenenfalls angepasst werden. Unter Berücksichtigung der Ergebnisse der Datenkategorisierung gemäß des Mindeststandards und Risikoanalyse sollten für den Zugriff auf externe Cloud-Dienste ausreichend sichere Passwörter verwendet werden. Vor allem müssen sie resistent gegen Brute-Force-Angriffe sein. Azure Active Directory, das für das Identitäts- und Berechtigungsmanagement für Dynamics 365 verwendet wird, bietet Multi-Faktor-Authentifizierung (MFA)[102] inklusive bedingtem Zugriff[103] und schützt zusammen mit diesen Sicherheitsvorkehrungen vor Brute-Force- und Passwortspraying-Angriffen. Weitere Informationen zum Identitäts- und Berechtigungsmanagement befinden sich in der **Fehler! Verweisquelle konnte nicht gefunden werden.** im Kapitel 3.2 *OPS.2.2.A2 Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung*.
MCD.2.2.02 Umgang mit Benutzernamen und Kennwörtern	Diese Anforderung besagt, dass die gemeinsame Nutzung von Anmeldeinformationen zu vermeiden und die erforderlichen Sicherheitsvorkehrungen zu treffen sind.

[101] https://www.microsoft.com/en-us/trust-center/privacy/data-management
https://aka.ms/DPA
[102] https://docs.microsoft.com/de-de/azure/active-directory/authentication/concept-mfa-licensing
[103] https://docs.microsoft.com/de-de/azure/active-directory/conditional-access/overview

Anforderung	Beschreibung
	Dynamics 365 verwendet Azure Active Directory zur Verwaltung von Identitäts- und Berechtigungsmanagement[104]. Multifaktor-Authentifizierung (MFA)[102] verwendet werden, um die gemeinsame Nutzung von Konten zu erschweren. Weitere Informationen zum Identitäts- und Berechtigungsmanagement befinden sich in der **Fehler! Verweisquelle konnte nicht gefunden werden.** im Kapitel 3.2 *OPS.2.2.A2 Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung*.
MCD.2.2.03 Mitteilungen bei Änderungen	Um diese kundenspezifische Anforderung zu erfüllen, ist es notwendig, Änderungen oder beabsichtigte Änderungen an den externen Cloud-Diensten dem zuständigen IT-Sicherheitsbeauftragten mitzuteilen. Microsoft stellt Updates für Dynamics 365 zur Verfügung, die nach Datum sortiert sind. Dazu gehören Informationen über neue und geänderte Funktionen, Sicherheitsupdates und Änderungen im Unterauftragsnehmerverhältnis.[105]

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

[105] https://dynamics.microsoft.com/de-de/business-applications/product-updates/

5 Die Verantwortung von Microsoft als Cloud-Diensteanbieter

Microsoft teilt sich mit dem Kunden die Verantwortung für die Sicherheit von Dynamics 365 (siehe Kapitel 2.1Modell 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 Sicherheit zu bewerten, hat Microsoft eine Reihe von sicherheitsrelevanten Zertifizierungen für Dynamics 365[106]vorbereitet.

Die wichtigsten davon sind:

- ISO 27001 (Informationssicherheitsmanagementsystem)
- ISO 27017 (Verhaltenskodex für Informationssicherheitskontrollen basierend auf ISO/IEC 27002 für Cloud-Dienste)
- ISO 27018 (Verhaltenskodex für den Schutz personenbezogener Daten (PBD) in Public Clouds als PBD-Verarbeiter)
- Anforderungskatalog - 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.

[106] https://docs.microsoft.com/de-de/microsoft-365/compliance/offering-home (in Englisch)

Anhang A
Glossar der IT-Grundschutz Begriffe

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

Begriff	Beschreibung
Mindeststandard des BSI nach § 8 Abs. 1 Satz 1 BSIG zur Nutzung externer Cloud-Dienste in der Bundesverwaltung	Dieser Standard enthält Mindestsicherheitsanforderungen für die Nutzung externer Cloud-Dienste in der öffentlichen Verwaltung.
Mindeststandard des BSI nach § 8 Abs. 1 Satz 1 BSIG zur Mitnutzung externer Cloud-Dienste in der Bundesverwaltung	Dieser Standard legt Mindestsicherheitsanforderungen für die gemeinsame Nutzung externer Cloud-Dienste in der öffentlichen Verwaltung fest.
Modellierung	Bei den Vorgehensweisen nach IT-Grundschutz wird bei der Modellierung der betrachtete Informationsverbund einer Institution oder einer Behörde mit Hilfe der Bausteine aus dem IT-Grundschutz-Kompendium nachgebildet. Hierzu enthält Kapitel 2.2 des IT-Grundschutz-Kompendiums für jeden Baustein einen Hinweis, auf welche Zielobjekte er anzuwenden ist und welche Voraussetzungen dabei gegebenenfalls zu beachten sind.
OPS.2.2 Cloud-Nutzung	Der Baustein OPS.2.2 Cloud-Nutzung enthält Anforderungen und Umsetzungshinweise zur 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

Topic	Information Pointer
Rechtliche Informationen	https://www.microsoft.com/de-de/licensing/product-licensing/products.aspx (Online Service Terms (OST), Service Level Agreements (SLA)) https://aka.ms/DPA
Compliance-Informationen	https://servicetrust.microsoft.com/ (in Englisch) https://www.microsoft.com/de-de/trust-center/compliance/compliance-overview?market=de https://www.microsoft.com/en-us/corporate-responsibility/lerr (in Englisch) https://docs.microsoft.com/de-de/microsoft-365/compliance/gdpr-breach-dynamics365
Dynamics 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/ https://docs.microsoft.com/de-de/power-platform/admin/notifications-explained#service-health-dashboard https://dynamics.microsoft.com/de-de/roadmap/overview/ https://www.microsoft.com/en-us/download/details.aspx?id=18039 (Microsoft Dynamics CRM Online-Migration auf Microsoft Dynamics CRM on Premise, in Englisch) https://docs.microsoft.com/de-de/dynamics365/get-started/availability https://www.microsoft.com/de-de/fasttrack/
Sicherheitsaspekte Dynamics 365	https://www.microsoft.com/en-us/TrustCenter/STP/default.aspx (White paper "Scalable Security Modeling with Microsoft Dynamics CRM", in Englisch) https://docs.microsoft.com/en-us/dynamics365/customer-engagement/admin/security-concepts (in Englisch)

Topic	Information Pointer
	https://docs.microsoft.com/de-de/azure/active-directory/ https://docs.microsoft.com/de-de/office365/enterprise/hybrid-cloud-overview https://docs.microsoft.com/de-de/azure/active-directory/hybrid/ https://docs.microsoft.com/de-de/microsoft-365/compliance/office-365-encryption-in-microsoft-dynamics-365 https://docs.microsoft.com/en-us/dynamics365/unified-operations/dev-itpro/data-entities/data-management-api (in Englisch) https://docs.microsoft.com/en-us/rest/dynamics365/ (in Englisch) https://docs.microsoft.com/de-de/cloud-app-security/ https://docs.microsoft.com/en-us/dynamics365/customer-engagement/admin/field-level-security (in Englisch)
Microsoft Liste der Dienstleister	https://www.microsoft.com/en-us/download/details.aspx?id=50426 (Microsoft Liste der Dienstleister, in Englisch) http://download.microsoft.com/download/0/4/3/043398DF-05CD-45F4-9A55-EEC1EECEF386/Online_Serv_Subcontractor_List.pdf (Microsoft Liste der Subunternehmern, in Englisch)
BSI	https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Standards/Standard201/ITGStandard201_node.html https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Standards/Standard202/ITGStandard202_node.html https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Standards/Standard203/ITGStandard203_node.html https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Kompendium/itgrundschutzKompendium_node.html https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Anforderungskatalog/Anforderungskatalog_node.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/Mindeststandards/Mindeststandard_Nutzung_externer_Cloud-Dienste.html

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

HiSolutions AG
Schloßstraße 1
12163 Berlin

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

HiSolutions AG
Niederlassung
Brüsseler Str. 1-3
Tower One - Spaces
60327 Frankfurt am Main

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

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

Fon: +49 22 852 268 175
Fax: +49 30 533 289 900

HiSolutions AG
Niederlassung
Nürnberg
Bahnhofstraße 2
3. OG
90402 Nürnberg

Fon: +49 30 533 289 0
Fax: +49 30 533 289 900

HiSolutions AG
Niederlassung
Düsseldorf
Kaiserswerther Straße 135
40474 Düsseldorf

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