

Sicherheitsanforderung

M365 Power BI

Deutsche Telekom Gruppe

Version	4.0
Datum	01.07.2024
Status	Freigegeben

Impressum

Herausgeber
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Deutschland

Dateiname	Dokumentennummer 8.01	Dokumententyp Sicherheitsanforderung
Version 4.0	Stand 01.07.2024	Status Freigegeben
Fachlicher Ansprechpartner Telekom Security psa.telekom.de	Gültigkeitsdauer 01.07.2024 - 30.06.2029	Freigegeben von Stefan Pütz, Leiter SEC-T-TST

Zusammenfassung

Power BI ist eine Sammlung von Softwarediensten, Apps und Data Connectors, die zusammenwirken, um nicht verbundene Datenquellen in kohärente, visuell überzeugende und interaktive Einblicke umzuwandeln. Die Daten können als Excel-Kalkulationstabelle oder als eine hybride Sammlung von cloudbasierten und lokalen Data Warehouse-Instanzen vorliegen. Mit Power BI ist es möglich, Verbindungen zwischen Ihren Datenquellen herstellen, wichtige Punkte zu entdecken und zu visualisieren sowie die Ergebnisse mit relevanten Personen zu teilen.

Copyright © 2024 by Deutsche Telekom AG.

Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

Inhaltsverzeichnis

1.	Einleitung	4
2.	Dataflow	5
3.	Data Gateway	6
4.	Data Connectivity	8
5.	Reports	9
6.	M365 Allgemeine Anforderungen	10
6.1.	Tenant & IAM	10
6.2.	Backend	14
6.3.	Applications	14
6.4.	Data Security	15

1. Einleitung

Dieses Dokument wurde auf Basis der Vorgaben aus der Konzernrichtlinie Sicherheit (Group Security Policy). Die vorliegende Sicherheitsanforderung dient u.a. als Grundlage zur Freigabe im PSA-Prozess. Sie dient darüber hinaus als Umsetzungsempfehlung für Vorgaben der Konzernrichtlinie Sicherheit (Group Security Policy) in Einheiten, die nicht am PSA-Verfahren teilnehmen. Diese Anforderungen müssen bereits während der Planungs- und Entscheidungsprozesse berücksichtigt werden und gelten für alle M365 Umgebungen der jeweiligen Einheit.

Bei der Umsetzung der Sicherheitsanforderung ist das jeweils vorrangige nationale, internationale und supranationale Recht zu beachten. Sollte die Einhaltung der beschriebenen Anforderungen in individuellen Fällen nicht oder nur eingeschränkt umsetzbar sein, ist gemeinsam mit einem Sicherheits- und/oder Datenschutzexperten (entsprechend der betroffenen Anforderung) eine Risikobewertung vorzunehmen und mögliche alternative Schutzmaßnahmen abzustimmen.

2. Dataflow

Req 1	Bei Verwendung von Power BI Dataflows darf die Arbeitsbereichsrolle "Viewer"/"Anzeige" nicht verwendet werden.
-------	--

Es muss sichergestellt werden, dass auf einen Arbeitsbereich, der Power BI Dataflows enthält, nur Berichts-Entwickler direkten Zugriff haben. Die Arbeitsbereichsrolle "Viewer" / "Anzeige" ist nicht zu verwenden. Es müssen, für Power BI Dataflows und Berichte getrennte Arbeitsbereiche genutzt werden.

Motivation: Alle Nutzerinnen und Nutzer, die in einem Arbeitsbereich die Rolle "Viewer" / "Anzeige" besitzen, sind in der Lage, über den Power BI Desktop Client (Cloud und Report Server Version) auf alle Power BI Dataflows im Arbeitsbereich zuzugreifen. Sie können auf Basis der Dataflow-Daten eigene Berichte erstellen und verteilen, ohne dass der Dataflow-Besitzer dies erfährt. Dies soll mit dieser Anforderung verhindert werden.

ID: 8.01-1/4.0

Req 2	Die Power BI Dataflow Funktion "AutoML" (Automatisiertes Machine Learning) darf nicht verwendet werden.
-------	---

Bei der Erstellung und Verwendung eines Power BI Dataflows ist die Funktion "AutoML" (Automatisiertes Machine Learning) nicht gestattet. Es muss ebenfalls in der Systembeschreibung dokumentiert werden, dass diese Funktionalität nicht verwendet werden wird.

Motivation: Bis eine abschließende Regelung im Konzern DTAG für den Umgang mit AI/KI und ML Service getroffen worden ist, soll durch diese Anforderung die Verarbeitung / Manipulation von DTAG Information durch 3rd Party Services verhindert werden.

ID: 8.01-2/4.0

3. Data Gateway

Req 3	Initiierung der Verbindung darf nur von Intern nach Extern erfolgen
-------	---

Aufgrund der nur sehr schwer bis gar nicht zu kontrollieren Datenströme von Extern nach Intern, dürfen Verbindungen nur von Intern nach Extern aufgebaut werden. In diesem Kontext ist Intern mit On Premise bzw. IaaS in einer von der eigenen Organisation kontrollierten Landing Zone bzw. Private/Public Cloud definiert. Mit Extern hingegen sind die übrigen Bereiche einer Public Cloud bzw. allgemeine Ressourcen im Internet gemeint.

Gültigkeit: Applikationsbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 8.01-3/4.0

Req 4	Das 4-Augen Prinzip bei Registrierung eines Data Gateways im Tenant muss gewahrt werden
-------	---

Das Recht der Registrierung eines Data Gateways im gewünschten Tenant muss auf wenige Mitarbeiter begrenzt sein. Zur Wahrung des 4-Augen Prinzips dürfen die Mitarbeiter, die ein Data Gateway implementiert haben bzw. betreiben, nicht das Recht der Registrierung des Data Gateways im Tenant bekommen.

Gültigkeit: Plattformbetrieb, Applikationsbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 8.01-4/4.0

Req 5	Berechtigungsstufe der Benutzer des Data Gateways muss auf "Can use" gesetzt werden
-------	---

Ein Data Gateway darf verwendet aber nicht mit anderen Benutzern oder Applikationen geteilt werden. Aus diesem Grund muss die Berechtigungsstufe für Accounts, die auf das Data Gateway berechtigt werden, auf "Can use" gestellt werden.

Gültigkeit: Plattformbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unbemerkt durchführbare Angriffe

ID: 8.01-5/4.0

Die folgenden Lifecycle- und Management-Prozesse für ein Data Gateway müssen eingehalten werden:

- Dokumentation der Registrierung eines Data Gateways im Tenant
- Zweckbindung des Data Gateways; Dokumentation der Zweckbindung erfolgt durch den Business Case
- Das Data Gateway muss zentral durch den Plattformbetrieb gemanaged werden

Gültigkeit: Plattformbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten

ID: 8.01-6/4.0

4. Data Connectivity

Req 7	Ein Disclaimer muss bei Verwendung des Import Mode eingeblendet werden
-------	--

Bei Verwendung des Import Mode muss ein Disclaimer eingeblendet werden, der den Anwendern darauf hinweist, dass mit der Verwendung des Import Mode Daten aus der Datenquelle in die Cloud hochgeladen und dort gespeichert werden.

Gültigkeit: Plattformbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Abstreiten von durchgeführten Aktionen

ID: 8.01-7/4.0

Req 8	Bei Verwendung der Direct Query/des Live Connects muss ein Approval Process implementiert werden
-------	--

Es muss ein Approval Prozess implementiert, freigegeben und verwendet werden, der auf Antrag Zugriff auf die Daten der jeweiligen Datenquelle gestattet oder verweigert. Dies muss in einer Nutzungsvereinbarung zwischen Plattform- und Applikationsbetrieb dokumentiert werden.

Gültigkeit: Plattformbetrieb

ID: 8.01-8/4.0

Req 9	Es muss verhindert werden, dass bei Verwendung von Data Flow potentielle Daten einer Quelle in veränderter Form dargestellt und/ oder die Unternehmensgrenzen verlassen werden.
-------	---

Bei Verwendung von Data Flow muss die Verwendung und Ausgestaltung dezidiert beschrieben freigegeben werden, da es möglich ist unter Verwendung von Data Flow pot. Daten einer Quelle in Veränderter Form dazustellen. Der Data Owner wird darüber nicht automatisch informiert. In diesem Kontext ist dezidierte Überprüfung durchzuführen, ob diese Art der Verwendung durch den Data Owner zugestimmt wurde.

Gültigkeit: Applikationsbetrieb

Motivation: Verhinderung von ungewolltem Abgang von vertraulichen Informationen/Daten über Unternehmensgrenzen hinaus, sowie eine falsche Verwendung von Informationen/Daten die nicht der eingestuften Daten Klassifikation entspricht

ID: 8.01-9/4.0

5. Reports

Req 10	Reports müssen mit einem Default Sensitivity Label versehen werden
--------	--

Werden mit Power BI Reports erstellt, so müssen diese mit einem Sensitivity Labeln von Microsoft Information Protection (MIP) versehen werden, der standardmäßig nur Mitarbeitern der eigenen Organisation Zugriff auf den jeweiligen Report ermöglicht.

Gültigkeit: Applikationsbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unbemerkt durchführbare Angriffe

ID: 8.01-10/4.0

Req 11	Eine Nutzungsvereinbarung zwischen Data Owner und Konsument eines Reports muss abgeschlossen werden
--------	---

Die Konsumenten eines jeden Reports müssen auf den korrekten Umgang mit den im Report enthaltenen Daten hingewiesen werden. Dies kann durch den Data Owner auf verschiedene Arten realisiert werden:

- Nutzungsvereinbarung zwischen Data Owner und Konsument
- Disclaimer im Power BI Arbeitsbereich
- In der Präambel des Reports

Gültigkeit: Applikationsbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten

ID: 8.01-11/4.0

Req 12	Benutzer dürfen nicht mit "Build-Permission" Rechten auf das Dataset einer Applikation zugreifen
--------	--

Um zu verhindern, dass Benutzer, die keinen Zugriff auf den Workspace einer Applikation bzw. lediglich eine Viewer Role besitzen, auf das Dataset einer Applikation zugreifen und damit Reports erstellen können, muss die Option "Allow all users to connect to the app's underlying datasets using the Build permission" auf der Power BI App Ebene deaktiviert bzw. auf "Access to specific individuals or groups" gesetzt werden.

Gültigkeit: Applikationsbetrieb

Motivation: Minimierung der Angriffsfläche

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten

ID: 8.01-12/4.0

6. M365 Allgemeine Anforderungen

6.1. Tenant & IAM

Req 13	Modern Authentication muss aktiviert werden
--------	---

Um zu verhindern, dass für den Login in mindestens die folgenden Services eine schwache Authentifizierung verwendet wird, muss Modern Authentication im M365 Tenant aktiviert werden:

- Exchange Online
- Skype for Business
- Sharepoint Applications

Gültigkeit: Plattformbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Unbemerkt durchführbare Angriffe

ID: 8.00-1/1.2

Req 14	Conditional Access (CA) muss verwendet werden um die Verwendung von legacy Authentication zu unterbinden
--------	--

Um eine Verwendung von schwachen Authentifizierungen, sogenannten legacy Authentication zu unterbinden, muss eine Anmeldung, die eine legacy Authentication verwendet, durch eine geeignete Conditional Access Policy blockiert werden.

Gültigkeit: Plattformbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Unbemerkt durchführbare Angriffe

ID: 8.00-2/1.2

Req 15	Multi Factor Authentication (MFA) muss unter Verwendung von Conditional Access (CA) für jeden Account aktiviert werden
--------	--

Um die Übernahme eines Accounts z.B. durch einen Password Leak zu verhindern, muss jeder Account, der sich über das Internet am Azure Active Directory (AAD) anmeldet, Multi Factor Authentication (MFA) verwenden.

Gültigkeit: Plattformbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 8.00-3/1.2

Req 16	Password Protection für Active Directory muss aktiviert sein
--------	--

Um das Verwenden schwacher oder leaked Passwörter zu unterbinden muss die Password Protection für Active Directory aktiviert werden.

Gültigkeit: Plattformbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit

ID: 8.00-4/1.2

Req 17	Ein Password-Reset eines privilegierten oder Break-Glass Accounts muss alarmiert werden
--------	---

Um überprüfen zu können, ob der Wechsel des Passwortes eines privilegierten oder eines Break-Glass Accounts rechtmäßig war muss jeder Wechsel des Passwortes dieser Accounts alarmiert werden.

Gültigkeit: Plattformbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 8.00-5/1.2

Req 18	Der Zugriff auf das Azure Portal muss nach dem Need-to-Know bzw. Least-Privilege Prinzip reguliert werden
--------	---

Zugriffe auf das Azure Portal dürfen nur von einigen Mitarbeitern unter Wahrung der Prinzipien Need-to-Know und Least-Privilege durchgeführt werden.

Gültigkeit: Plattformbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 8.00-6/1.2

Req 19	Für den privilegierten Zugriff dürfen nur Privileged Access Workstations (PAW) verwendet werden
--------	---

Um eine Kompromittierung privilegierter Accounts zu verhindern, dürfen privilegierte Zugriffe auf den M365 Tenant nur mit Hilfe von Privileged Access Workstations (PAW) durchgeführt werden. Die PAW muss mindestens den folgenden Anforderungen genügen

- Verwendung einer modernen Endpoint Detection und Response Lösung wie beispielsweise Microsoft Defender for Endpoint oder vergleichbar
- Die PAW darf keinen direkten Kontakt mit dem Internet haben, der Zugriff auf die M365 Umgebung muss über eine gesonderte Infrastruktur für privilegierte Zugriffe durchgeführt werden
- Die PAW muss besonders gehärtet und verschlüsselt sein
- Anmeldung an der PAW muss mit einer MFA erfolgen
- Der Benutzer darf keine lokalen Administrationsberechtigungen auf der PAW besitzen

Gültigkeit: Plattformbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 8.00-7/1.2

Req 20	Zur Dokumentation der verwendeten privilegierten Rollen und Berechtigungen muss ein Administrationskonzept erstellt werden
--------	--

Zur Dokumentation und Nachvollziehbarkeit der verwendeten privilegierten Rollen und Berechtigungen innerhalb der M365 Umgebung muss ein Administrationskonzept erstellt werden.

Gültigkeit: Plattformbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 8.00-8/1.2

Req 21	Um die Identitäten zu schützen, muss Microsoft Defender for Identity verwendet werden
--------	---

Zur Absicherung der Identitäten und Erkennen von Missbrauch muss Microsoft Defender for Identity verwendet werden.

Gültigkeit: Plattformbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

Req 22	Mittels Defender for Cloud Apps müssen Zugangskontrollen und geografische Blockierungsregeln für privilegierte Konten genutzt werden
--------	--

Microsoft Defender for Cloud Apps enthält risikobasierte Regeln, die ungewöhnliches Verhalten oder unlogische Aktionen erkennen. Beispielsweise wird sichtbar, wenn eine Anmeldung von einem Land aus erfolgt und gleich darauf eine zweite von einer IP-Adresse eines anderen Landes aus, und das innerhalb eines so kurzen Zeitraums, dass es logisch gar nicht möglich ist.

Gültigkeit: Plattformbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

Req 23	Cloud Service Provider (CSP) Verwaltungsrechte dürfen nicht verwendet werden
--------	--

Dritten (außerhalb des Plattformbetriebs) dürfen keine CSP-delegierten Administrationsrechte eingeräumt werden. Stattdessen muss für solche Usecases ein vollständiger Benutzer-Account für den Dritten eingerichtet werden, da so Admin-Privilegien granular zugewiesen werden können.

Gültigkeit: Plattformbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

Req 24	Applikationen, die M365 Services verwenden, müssen im Tenant explizit registriert werden
--------	--

Applikationen, die M365 Services verwenden, müssen im Tenant explizit registriert werden. Eine Dokumentation, bspw. in Form einer Schnittstellenvereinbarung, muss angefertigt und unterschrieben werden.

Gültigkeit: Plattformbetrieb, Applikationsbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

6.2. Backend

Req 25	Jeder Server, der Backend-Dienste für die M365 Umgebung anbietet muss mit einer modernen Endpoint Detection und Response Lösung geschützt werden
--------	--

Jeder Server, der Backend-Dienste für die M365 Umgebung anbietet muss mit einer modernen Endpoint Detection und Response Lösung, wie beispielsweise Microsoft Defender for Endpoint oder vergleichbar, geschützt werden

Gültigkeit: Plattformbetrieb, Applikationsbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 8.00-13/1.2

Req 26	Eine geeignete zentrale Mobile Device Management (MDM) Lösung muss verwendet werden, um Zugriffe auf die M365 Services durchführen zu können
--------	--

Eine geeignete zentrale Mobile Device Management (MDM) Lösung muss verwendet werden, um Zugriff auf die M365 Services durchführen zu können. Dabei ist ein aktueller OS Level ebenso wie eine Trennung zwischen privaten und geschäftlichen Daten sowie Applikationen zu beachten.

Gültigkeit: Plattformbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 8.00-14/1.2

6.3. Applications

Req 27	Alle Applikationen die sich zu M365 Services verbinden, müssen Web Account Manager (WAM) verwenden
--------	--

Alle Applikationen die sich zu M365 Services verbinden, müssen Web Account Manager (WAM) verwenden.

Gültigkeit: Plattformbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

Req 28	Nur freigegebene Third-Party Apps, Addons, Bots, Connectors etc. dürfen durch den Benutzer installiert und verwendet werden
--------	---

Um beispielsweise eine unbemerkte Data Exfiltration aus dem Tenant zu verhindern, dürfen nur zentral freigegebene Third-Party Apps, Addons, Bot, Connectors, etc. durch den Benutzer installiert und verwendet werden.

Gültigkeit: Plattformbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

Req 29	Der Admin-Consent Workflow muss aktiviert sein
--------	--

Um zu verhindern, dass ein normaler Benutzer Zugriffsberechtigungen von einer bzw. für eine Applikation vergeben kann, muss der Admin-Consent Workflow entsprechend konfiguriert und aktiviert sein.

Gültigkeit: Plattformbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

6.4. Data Security

Req 30	Links für External Sharing mit Anonymous Access müssen mit einem zeitlichen Ablauf versehen werden
--------	--

Um eine Data Exfiltration durch einen Angreifer zu erschweren, müssen External Sharing Links, die einen anonymen Zugang ermöglichen, zeitlich limitiert sein.

Gültigkeit: Plattformbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten

Req 31	Data Loss Prevention Policies (DLP) müssen konfiguriert und implementiert werden
--------	--

Zur Verhinderung eines Data Leakage beispielsweise im Rahmen eines Angriffs durch Hacker oder durch eine Unauf-

merksamkeit müssen Data Loss Prevention Policies (DLP) auf Mandantenebene im Kontext der jeweiligen Applikation sowie auf Plattformebene implementiert werden, wo dies technisch möglich ist.

Gültigkeit: Plattformbetrieb, Applikationsbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten

ID: 8.00-19/1.2

Req 32	Microsoft Information Protection (MIP) muss konfiguriert und implementiert werden
--------	---

Zum Schutz der im M365 zu verarbeitenden und zu speichernden Daten muss Microsoft Information Protection auf Mandantenebene im Kontext der jeweiligen Applikation sowie auf Plattformebene implementiert werden, wo dies nach aktuellem Stand technisch möglich ist.

Gültigkeit: Plattformbetrieb, Applikationsbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten

ID: 8.00-20/1.2

Req 33	Custer Lockbox muss verwendet werden
--------	--------------------------------------

Zum Schutz der im M365 zu verarbeitenden und zu speichernden Daten der Organisation gegenüber dem Provider und der Nachvollziehbarkeit der Zugriffe auf die Daten der Organisation durch Mitarbeiter des Providers muss das Feature Customer Lockbox verwendet werden.

Gültigkeit: Plattformbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 8.00-21/1.2