

Sicherheitsanforderung

M365 Power Apps

Deutsche Telekom Gruppe

Version	1.2
Datum	01.12.2023
Status	Freigegeben

Impressum

Herausgeber
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Deutschland

Dateiname	Dokumentennummer 8.02	Dokumententyp Sicherheitsanforderung
Version 1.2	Stand 01.12.2023	Status Freigegeben
Fachlicher Ansprechpartner Telekom Security psa.telekom.de	Gültigkeitsdauer 01.12.2023 - 30.11.2028	Freigegeben von Stefan Pütz, Leiter SEC-T-TST

Zusammenfassung

Power Apps ist eine Suite von Apps, Diensten und Konnektoren sowie eine Datenplattform, die eine Umgebung für die schnelle Entwicklungsumgebung bereitstellt, in der benutzerdefinierte Apps für Geschäftsanforderungen erstellt werden können. Durch die Nutzung von Power Apps können schnell benutzerdefinierte Geschäftsanwendungen erstellt werden, die eine Verbindung zu verschiedenen Online und OnPrem-Datenquellen herstellen, wie beispielsweise SharePoint Online, M365 Dataverse, MS Dynamics, SQL Server, etc.

Copyright © 2023 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.	Data Connectors	5
3.	Logging & Detection	7
4.	Power Apps	8

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. Data Connectors

Req 1	Non-blockable Data Connectors müssen durch einen Approval Prozess abgenommen werden
-------	---

Vor der Verwendung der non-blockable Data Connectors müssen diese im Rahmen eines PSA Verfahrens beschrieben und freigegeben werden.

Gültigkeit: Plattformbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.02-1/1.2

Req 2	Externe Systeme, die per Data Connector angebunden werden, dürfen nur mit einer Authentication verwendet werden
-------	---

Werden externe Systeme, die außerhalb der eigenen Organisation liegen, mittels Data Connectors an eine Power App angebunden, so muss eine Authentication am externen System durchgeführt 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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.02-2/1.2

Req 3	Nur freigegebene interne Systeme dürfen per Data Connector angebunden werden
-------	--

Interne Systeme der Organisation müssen vor einer Anbindung durch einen Data Connector im Rahmen eines PSA Verfahrens freigegeben sein.

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.02-3/1.2

Req 4	Nur freigegebene Authentifizierungsmodi dürfen verwendet werden
-------	---

Für jeden Data Connector dürfen ausschließlich non-shared Credentials oder AAD Connections verwendet werden.

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.02-4/1.2

3. Logging & Detection

Req 5 Audit Logs & Anomalie Erkennung müssen aktiviert werden

Im Rahmen des Betriebs der Power Apps müssen Audit Logs und die Anomalie Erkennung aktiviert und an das SIEM der Organisation angebunden 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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.02-5/1.2

4. Power Apps

Req 6	Power Apps dürfen in der externen Community nicht geteilt werden
-------	--

Erstellte Power Apps dürfen außerhalb der Organisation nicht mit anderen Personen oder Institutionen geteilt werden.

Gültigkeit: Plattformbetrieb, Applikationsbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.02-6/1.2