

Sicherheitsanforderung

M365 Dataverse

Deutsche Telekom Gruppe

Version	2.2
Datum	01.12.2023
Status	Freigegeben

Impressum

Herausgeber
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Deutschland

Dateiname	Dokumentennummer 8.06	Dokumententyp Sicherheitsanforderung
Version 2.2	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

M365 Dataverse ermöglicht die Integration von Daten aus verschiedenen Quellen in einen einzigen Speicher, der dann in unterschiedlichen Services wie M365 Power Apps, M365 Power Automate, M365 Power BI oder M365 Dynamics verwendet werden kann.

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.	Access Policies	5
3.	Data Security	6
4.	Logging & Detection	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. Access Policies

Req 1 Für den Zugriff auf das Dataverse muss eine Conditional Access (CA) Policy implementiert werden

Es dürfen nur berechnigte Personen bzw. Applikationen auf das Dataverse zugreifen. Aus diesem Grund muss eine CA Policy erstellt und aktiviert werden, die nur berechtigten Rollen und/oder Accounts Zugriff auf das Dataverse erlaubt.

Gültigkeit: Plattformbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechnigte Einsichnahme oder Abgriff von Daten
- Unberechnigte Modifikation von Daten
- Unberechnigte Nutzung von Diensten oder Ressourcen

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.06-1/2.2

3. Data Security

Req 2 Record-level security in Dataverse muss verwendet werden

Um den Zugriff auf die Daten kontrollieren und einschränken zu können, muss für jede einzelne Database eine adäquate Record-Level Security implementiert werden.

Gültigkeit: Applikationsbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.06-2/2.2

Req 3 Field-level security in Dataverse muss verwendet werden

Um den Zugriff auf die Daten kontrollieren und einschränken zu können, muss für jede einzelne Database eine adäquate Field-Level Security implementiert werden.

Gültigkeit: Applikationsbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.06-3/2.2

Req 4 Die Erreichbarkeit der Forms einer Tabelle muss eingeschränkt sein

Es muss sichergestellt sein, dass die Forms einer Tabelle im Dataverse nicht von jedem innerhalb der Organisation erreicht werden kann. Aus diesem Grund muss die entsprechende Option auf "Specify Security Roles" gesetzt und die entsprechenden Security Roles implementiert werden.

Gültigkeit: Applikationsbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.06-4/2.2

Req 5 Bestimmte Dateien in Form von Anhängen müssen blockiert werden

Um die Wahrscheinlichkeit beispielsweise einer Ransomware-Attacke oder einer Daten Exfiltration zu minimieren müssen die folgenden Dateien als Anhänge blockiert werden:

de,adp,app,asa,ashx,asmx,asp,bas,bat,cdx,cer,chg,class,cmd,com,config,cpl,crt,csd,dll,exe,fxp,hlp,hta,htr,htw,ida,idc,idq,inf,ins,isp,its,jar,js,jse,ksh,lnk, mad,maf,mag,mam,maq,mar,mas,mat,mau,mav,maw,mda,mdb,mde,mdt,mdw,mdz,msc,msh,msh1,msh1xml,msh2,m

sh2xml,mshxml,msi,msp,mst,
ops,pcd,pif,prf,prg,printer,pst,reg,rem,scf,scr,sct,sh,shb,shs,shtm,shtml,soap,stm,tmp,url,vb,vbe,vbs,vsmacros,vss,vst,
vsw,ws,wsc,wsf,wsh

Gültigkeit: Applikationsbetrieb

Motivation: Minimierung der Angriffsfläche

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.06-5/2.2

Req 6	Um die Wahrscheinlichkeit von Angriffen mit Hilfe von Emails zu minimieren, muss die Option "Use secure frames" aktiviert werden
-------	--

Um die Wahrscheinlichkeit von Angriffen mit Hilfe von Emails zu minimieren, muss die Option "Use secure frames" aktiviert werden.

Gültigkeit: Plattformbetrieb, Applikationsbetrieb

Motivation: Verringerung der Arbeitsfläche

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.06-6/2.2

4. Logging & Detection

Req 7 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, 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
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.06-7/2.2