

Sicherheitsanforderung

M365 Sharepoint Online

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 8.04	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

SharePoint ist ein Website-basiertes System zur Zusammenarbeit, das Workflow-Anwendungen, Listen-Datenbanken und andere Webparts und Sicherheitsfunktionen nutzt, um die Zusammenarbeit von Geschäftsteams zu ermöglichen. SharePoint gestattet dem Unternehmen, das die Plattform einsetzt, außerdem die Kontrolle des Zugriffs auf Informationen und die geschäftseinheitsübergreifende Automatisierung von Workflow-Prozessen.

Die Microsoft Cloud-Version von SharePoint, SharePoint Online, verfügt über zahlreiche zusätzliche Funktionen zur Integration mit anderen Cloud-Anwendungen und ergänzt viele mit einer Office 365- oder Microsoft 365-Lizenz angebotenen Microsoft-Pakete.

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.	Content Sharing	7
4.	Sharepoint Sites	9

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	Die Security Controls für den restriktiven Zugriff müssen auf Site-Collection Level implementiert werden
-------	--

Da die Implementierung der Security Controls auf dem Site-Collection Level restriktiver als die Implementierung auf Tenant-Level ist müssen die Security Controls auf Site-Collection Level implementiert 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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.04-1/1.2

Req 2	Für den Zugriff auf SPO von nicht-gemanagten Devices muss eine Conditional Access (CA) Policy implementiert werden
-------	--

Erfolgt der Zugriff auf SPO von nicht-gemanagten Devices, so müssen die Zugriffe restriktiver gestaltet werden. Aus diesem Grund muss für den Zugriff auf SPO von nicht-gemanagten Devices eine Conditional Access (CA) Policy abgestimmt und implementiert 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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.04-2/1.2

Req 3	Session Timeouts müssen implementiert werden
-------	--

Für den Zugriff auf SPO müssen die folgenden Session Timeouts konfiguriert werden:

- Zugriff von Managed Devices: 5 Tage
- Zugriff von nicht-gemanagten Devices: 1 Tag

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
- Abstreiten von durchgeführten Aktionen

- Unbemerkt durchführbare Angriffe

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.04-3/1.2

3. Content Sharing

Req 4	Wenn beim Content Sharing die Option "Teilen mit Jedem" ausgewählt wird, dann muss der Anwender dies explizit bestätigen
-------	--

Sobald ein Anwender beim Content Sharing Option "Teilen mit Jedem" auswählt, dann muss er vom System explizit darauf hingewiesen werden, dass er Content mit Jedem in der Organisation teilen möchte und was das für Auswirkungen haben könnte. Anschließend muss der Anwender seine Wahl explizit bestätigen.

Gültigkeit: Plattformbetrieb

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: 8.04-4/1.2

Req 5	Beim ersten Zugriff auf einen extern geteilten Inhalt muss ein Disclaimer eingeblendet werden
-------	---

Greift ein Anwender zum ersten Mal auf einen externen geteilten Inhalt zu, dann muss ein Disclaimer eingeblendet werden.

Gültigkeit: Plattformbetrieb

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: 8.04-5/1.2

Req 6	Inhalt darf nur mit existierenden Guest-Accounts Extern geteilt werden
-------	--

Es darf nur mit existierenden Guest-Accounts Inhalt Extern geteilt werden. Aus diesem Grund muss der Level auf "Existing Guests" gestellt werden.

Gültigkeit: Plattformbetrieb

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: 8.04-6/1.2

Req 7	Gäste müssen sich mit dem Account anmelden, an den die Einladung für das externe Teilen von Inhalt versendet wurde
-------	--

Wird eine Einladung an einen Gast Account verschickt, mit dem Inhalt extern geteilt werden soll, so muss für den Login der Account verwendet werden, an den die Einladung verschickt wurde.

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: 8.04-7/1.2

Req 8 Guest-Accounts dürfen nur Inhalte teilen, die sie selbst besitzen

Anwender mit einem Guest-Account dürfen nur Inhalte teilen, für die sie als Eigentümer eingetragen sind.

Gültigkeit: Plattformbetrieb

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: 8.04-8/1.2

4. Sharepoint Sites

Req 9	SPO Custom Scripts dürfen nicht verwendet werden
-------	--

SPO Custom Scripts dürfen nicht verwendet werden. Folgende Alternativen/Workarounds können verwendet werden, um dieselbe Usability zu erreichen:

- Nutzung von SFPx oder Power Apps
- Teams müssen eine Modern Team Site erhalten, so dass Formulare zu Power Apps umgewandelt 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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.04-9/1.2