

Sicherheitsanforderung

M365 Allgemeine Anforderungen

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 8.00	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

Microsoft 365 (M365) ist die Cloud Plattform von Microsoft, welche durch das Zusammenspiel verschiedener Services es ermöglicht, Kommunikations- und Digitalisierungslösungen im Digital Workplace zu erstellen. Neben den Online Versionen von beispielsweise Word oder Excel stehen neben verschiedenen Services für Collaboration (MS Teams, Sharepoint Online), und der eigenen Produktivität (Mail, Calendar, Notes) auch Tools für die digitale Abbildung von Prozessen und die Erstellung von Applikationen basierend auf M365 und Azure Services (Power Platform, MS Dynamics) zur Verfügung. Die M365 Cloud wird dabei als eigenständige Cloud definiert, die neben der Azure Cloud durch Microsoft angeboten wird.

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.	Tenant & IAM	5
3.	Backend	10
4.	Applications	11
5.	Data Security	13

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. Tenant & IAM

Req 1 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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.00-1/1.2

Req 2 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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.00-2/1.2

Req 3 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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.00-3/1.2

Req 4 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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.00-4/1.2

Req 5 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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.00-5/1.2

Req 6 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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.00-6/1.2

Req 7 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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.00-7/1.2

Req 8 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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.00-8/1.2

Req 9	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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.00-9/1.2

Req 10	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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.00-10/1.2

Req 11	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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.00-11/1.2

Req 12	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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.00-12/1.2

3. Backend

Req 13	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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.00-13/1.2

Req 14	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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.00-14/1.2

4. Applications

Req 15	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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.00-15/1.2

Req 16	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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.00-16/1.2

Req 17	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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.00-17/1.2

5. Data Security

Req 18	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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.00-18/1.2

Req 19	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 Unaufmerksamkeit 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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.00-19/1.2

Req 20	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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.00-20/1.2

Req 21	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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 8.00-21/1.2