



Mint Secure

M365 Härtung Demo

Demo GmbH

Ansprechpartner

Demo GmbH

Mint Secure



Inhaltsverzeichnis

1	Executive Summary	4
2	Rahmenbedingungen der M365 Härtung / Konfiguration	5
2.1	Ziele der Härtung	5
2.2	Vorgehensweise & Ablauf	5
2.3	Scope	5
3	Dokumentation zu Härtungsmaßnahmen	6
3.1	AAD: Legacy-Authentifizierung	6
3.2	AAD: Risikobasierte Politiken	7
3.3	AAD: Starke Authentifizierung und ein sicheres Registrierungsverfahren	10
3.4	AAD: Zentralisierte Protokollerfassung	19
3.5	AAD: Registrierung und Zustimmung zum Antrag	21
3.6	AAD: Passwörter	23
3.7	AAD: Hochprivilegierter Benutzerzugang	24
3.8	AAD: Zugang für Gastbenutzer	33
3.9	DEFENDER: Voreingestellte Sicherheitsprofile	37
3.10	DEFENDER: Schutz vor Nachahmung	43
3.11	DEFENDER: Sichere Anhänge	47
3.12	DEFENDER: Prävention von Datenverlusten	48
3.13	DEFENDER: Warnungen	54
3.14	DEFENDER: Audit-Protokollierung	57
3.15	EXO: Automatische Weiterleitung an externe Domains	60
3.16	EXO: Malware-Scanning	61
3.17	EXO: Phishing-Schutz	65
3.18	EXO: IP-Zulassungslisten	69
3.19	EXO: Mailbox-Überprüfung	71
3.20	EXO: Eingehende Anti-Spam-Schutzmaßnahmen	73
3.21	EXO: Link Schutz	77
3.22	EXO: Warnungen	81



3.23	EXO: Audit-Protokollierung	84
3.24	EXO: Rahmen der Absenderpolitik	87
3.25	EXO: DomainKeys Identifizierte Mail	89
3.26	EXO: Bereichsbasierte Nachrichtenauthentifizierung, -meldung und -konformität (DMARC)	90
3.27	EXO: Simple Mail Transfer Protocol-Authentifizierung	93
3.28	EXO: Gemeinsame Nutzung von Kalender und Kontakten	94
3.29	EXO: Externe Sender Warnungen	96
3.30	EXO: Lösungen zur Verhinderung von Datenverlusten	98
3.31	EXO: Dateianhang Dateityp	102
3.32	POWERPLATFORM: Erstellung von Power Platform-Umgebungen	106
3.33	POWERPLATFORM: Power Platform-Richtlinien zur Verhinderung von Datenverlusten	109
3.34	POWERPLATFORM: Power Platform Mieterisolierung	112
3.35	POWERPLATFORM: Power Apps Inhaltssicherheitsrichtlinie	113
3.36	POWERPLATFORM: Erstellung von Power Pages	114
3.37	SHAREPOINT: Externe Freigabe	115
3.38	SHAREPOINT: Standardeinstellungen für die gemeinsame Nutzung von Dateien und Ordnern	118
3.39	SHAREPOINT: Sicherheit von Links und Verifizierungscode-Benutzern	119
3.40	TEAMS: Richtlinien für Sitzungen	122
3.41	TEAMS: Externer Benutzerzugang	130
3.42	TEAMS: Teams E-Mail-Integration	133
3.43	TEAMS: App-Verwaltung	134
3.44	TEAMS: Prävention von Datenverlusten	138
3.45	TEAMS: Malware-Scanning	139
3.46	TEAMS: Link-Schutz	142
4	Kontakt & Nächste Schritte	145



1 Executive Summary

Azure Active Directory	9 passes	4 warnings	13 failures	4 manual checks
Microsoft 365 Defender	4 passes	6 warnings	5 failures	4 manual checks
Exchange Online	8 passes	2 warnings	4 failures	26 manual checks
Microsoft Power Platform	4 passes	1 warning	1 failure	2 manual checks
SharePoint Online	4 passes			4 manual checks
Microsoft Teams	13 passes	1 warning	1 failure	6 manual checks



2 Rahmenbedingungen der M365 Härtung / Konfiguration

In diesem Kapitel wird beschrieben, wie genau die Härtung der M365 Umgebung erfolgt ist und welche Standards dazu herangezogen wurden.

2.1 Ziele der Härtung

2.2 Vorgehensweise & Ablauf

Die Härtung eines Microsoft 365 Tenants beginnt mit einer umfassenden Bestandsaufnahme der aktuellen Sicherheitskonfiguration und Identifizierung potenzieller Schwachstellen. Anschließend werden bewährte Sicherheitsrichtlinien und -Maßnahmen definiert, basierend auf den Empfehlungen von Microsoft und gängigen Best Practices. Daraufhin erfolgt die schrittweise Implementierung dieser Maßnahmen, einschließlich der Anpassung von Identitäts- und Zugriffsrichtlinien, Überwachungseinstellungen und Compliance-Vorgaben. Nach der Umsetzung werden regelmäßige Überprüfungen und Tests durchgeführt, um die Wirksamkeit der Maßnahmen zu gewährleisten und mögliche Sicherheitslücken frühzeitig zu erkennen. Abschließend erfolgt eine kontinuierliche Optimierung und Anpassung der Sicherheitsstrategie, um auf neue Bedrohungen und veränderte Geschäftsanforderungen zu reagieren. Die Methode stützt sich auf gängige Best Practice im Auditumfeld (siehe dazu mehr in 4 „Information zur Durchführung von Audits“).

2.3 Scope

Es handelt sich um folgenden Tenant:

Tenant Display Name	DEMO TENANT
Tenant Domain Name	DEMO DOMAIN
Tenant ID	123456789

Weitere Systeme (insbesondere jene aus dem On-Premise Bereich) waren nicht im Betrachtungsfeld / Scope enthalten, sodass sich die Maßnahmen rein auf den M365Tenant beschränken.



3 Dokumentation zu Härtingsmaßnahmen

Das folgende Kapitel stellt die Härtingsmaßnahmen nach Anforderungen der CISA und Microsoft dar.

3.1 AAD: Legacy-Authentifizierung

Dieser Abschnitt enthält Richtlinien zur Verringerung der Sicherheitsrisiken im Zusammenhang mit älteren Authentifizierungsprotokollen, die keine Multifaktor-Authentifizierung (MFA) unterstützen.

Ressourcen

- Legacy-Authentifizierung mit Conditional Access blockieren](<https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-conditional-access-policy-block-legacy>)
- Fünf Schritte zur Sicherung Ihrer Identitätsinfrastruktur](<https://learn.microsoft.com/en-us/azure/security/fundamentals/steps-secure-identity>)

MS.AAD.1.1v1

Status: **Fail** (0 conditional access policy(s) found that meet(s) all requirements.)

Criticality: Shall

Die Legacy-Authentifizierung MUSS blockiert werden.

- Begründung:_ Das Sicherheitsrisiko bei der Zulassung von Legacy-Authentifizierungsprotokollen besteht darin, dass sie keine MFA unterstützen. Durch die Blockierung von Legacy-Protokollen werden die Auswirkungen des Diebstahls von Benutzeranmeldeinformationen verringert.
- Letzte Änderung:_ Juni 2023
- NIST SP 800-53 Rev. 5 FedRAMP High Baseline Mapping:_ CM-7
- MITRE ATT&CK TTP Mapping:
 - [T1110: Brute Force](#)
 - [T1110.001: Passwort-Erraten](#)
 - [T1110.002: Passwort-Knacken](#)
 - [T1110.003: Passwort-Sprühen](#)
 - [T1078: Gültige Konten](#)
 - [T1078.004: Cloud-Konten](#)

MS.AAD.1.1v1 Anweisungen

1. [Feststellen, ob die vorhandenen Anwendungen einer Behörde die Legacy-Authentifizierung verwenden](#), bevor die Legacy-Authentifizierung für die gesamte Anwendungsbasis gesperrt wird.
2. Erstellen Sie eine Richtlinie für bedingten Zugriff, um die Legacy-Authentifizierung zu blockieren.

Benutzer > Einschließen > **Alle Benutzer**

Zielressourcen > Einschließen > **Alle Ressourcen (früher "Alle Cloud-Anwendungen")**

Bedingungen > Clientanwendungen > Konfigurieren > **Ja** > Veraltete Authentifizierungsclients > Nur **Exchange ActiveSync-Clients** und **Andere Clients** auswählen

Zugriffskontrolle > Gewähren > **Zugriff sperren**



4 Kontakt & Nächste Schritte

Als mögliche nächste Schritte empfehlen wir:

- Jährliche Security Reviews
- Penetrationstests von Netzwerk- oder Office Umgebungen
- Weitere Durchführung von Härtingsmaßnahmen

Gerne unterstützen wir Sie bei diesen Schritten. Bei Anfragen, Vorfällen und allgemeinen Fragen können Sie sich gerne an uns wenden:

Mint Secure GmbH

Pappelallee 78/79
10437 Berlin

Tel.: 0162 867 5772

Geschäftsführer: Tim Philipp Schäfers

anfrage@mint-secure.de