

VERTRAULICH

M365 KUNDENBERICHT

Security & Compliance Assessment

M365 Tenant Check – Ergebnisbericht

KUNDE

Mustermann Logistik GmbH

DATUM

15. Mai 2026

CONSULTANT

Marc Schramm / Previder

TENANT

mustermann-logistik.de

231

GEPRÜFTE TESTS

89

FEHLGESCHLAGEN

24

ZU PRÜFEN

118

BESTANDEN

Executive Summary

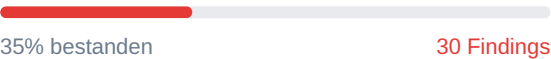
Der M365 Tenant der Mustermann Logistik GmbH wurde am 15. Mai 2026 mit 231 automatisierten Tests in 7 Sicherheitsmodulen überprüft. 89 Tests haben kritische oder relevante Abweichungen von Microsoft-Best-Practices und Zero-Trust-Empfehlungen identifiziert.



RISIKOEINSTUFUNG: HOCH

3 kritische High-Severity-Findings erfordern unmittelbares Handeln (MFA, Legacy Auth, Audit Log)

Entra ID / Azure AD



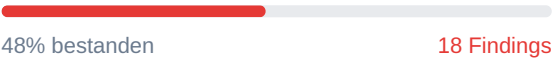
Microsoft Defender



Exchange Online



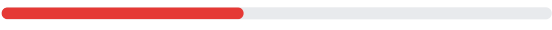
Intune / Endpoint



Microsoft Teams



SharePoint & OneDrive



67% bestanden

5 Findings

44% bestanden

7 Findings

Purview / Compliance

35% bestanden

9 Findings

⚡ 3 SOFORT-MASSNAHMEN (INNERHALB 48 STUNDEN)

- 1 Legacy-Authentifizierung blockieren:** POP3, IMAP und SMTP Auth ermöglichen MFA-Umgehung. Conditional-Access-Policy sofort aktivieren.
- 2 MFA für alle Admin-Konten erzwingen:** 3 Global-Admin-Konten sind ohne Multi-Faktor-Authentifizierung – höchstes Angriffspotenzial.
- 3 Unified Audit Log aktivieren:** Ohne aktives Audit-Log sind Angriffe und Datenzugriffe im Nachhinein nicht nachvollziehbar – auch für DSGVO-Compliance kritisch.

✓ Was bereits gut funktioniert (118 bestandene Tests)

- ✓ **SPF-Records** für alle Domains korrekt konfiguriert (E-Mail-Spoofing-Schutz aktiv)
- ✓ **Breakglass-Konten** sind eingerichtet und von Conditional-Access-Richtlinien ausgenommen
- ✓ **MFA-Registrierung** bei Standardnutzern: 94% abgedeckt – gute Ausgangsbasis für vollständige Erzwingung
- ✓ **Anti-Spam-Policies** für Exchange Online aktiv und korrekt konfiguriert
- ✓ **iOS App Protection Policies** für mobile Geräte aktiv

Entra ID / Azure AD

✗ 30 Failed

⚠ 4 Prüfen

✓ 18 Bestanden

MT.1001 · Custom · Entra ID

● High

✗ Fehlgeschlagen

Legacy-Authentifizierung ist nicht für alle Protokolle blockiert

Aktueller Status: Für 4 Legacy-Protokolle ist die Authentifizierung ohne Multi-Faktor-Authentifizierung möglich. Dies ermöglicht Angreifern, die MFA-Pflicht vollständig zu umgehen.

Protokoll	Status	Risiko
POP3	Aktiviert	Kritisch – MFA-Bypass möglich
IMAP	Aktiviert	Kritisch – MFA-Bypass möglich
SMTP Auth	Aktiviert	Hoch – App-Passwörter angreifbar
Basic Auth EWS	Aktiviert	Kritisch – Credential Stuffing
Modern Auth OIDC	Aktiviert	Korrekt konfiguriert

Warum ist das ein kritisches Risiko?

Legacy-Authentifizierungsprotokolle unterstützen keine moderne Multi-Faktor-Authentifizierung. Angreifer, die Zugangsdaten über Phishing oder Dark-Web-Leaks erlangt haben, können sich damit direkt einloggen – vollständig an MFA-Richtlinien vorbei. Laut Microsoft sind über 99 % der kompromittierten Konten auf fehlenden MFA-Schutz oder aktive Legacy-Authentifizierung zurückzuführen.

Empfehlung

- Conditional Access Policy erstellen: Legacy-Authentifizierung blockieren (Bedingung: Client-App = Other clients)
- Betroffene Nutzer und Apps auf Modern Auth migrieren (Exchange Online unterstützt OAUTH 2.0)
- Sicherheitsstandards (Security Defaults) als Ausgangspunkt nutzen, falls noch keine CA-Richtlinien existieren

EIDSCA.AP01 · EIDSCA · Entra ID

• High

✗ Fehlgeschlagen

Privilegierte Konten ohne registrierte MFA

3 von 5 Global-Administrator-Konten haben keine Multi-Faktor-Authentifizierung registriert. Diese Konten haben uneingeschränkten Zugriff auf alle Microsoft-365-Dienste und -Daten.

Konto	Admin-Rolle	MFA-Status	Letzte Anmeldung
admin@mustermann-log.de	Global Admin	Nicht registriert	12.05.2026
it-leitung@mustermann-log.de	Global Admin	Nicht registriert	08.05.2026
backup-admin@mustermann-log.de	Global Admin	Nicht registriert	14.03.2026
svc-admin@mustermann-log.de	Global Admin	Registriert	15.05.2026
breakglass@mustermann-log.de	Global Admin	Registriert (Ausnahme)	—

Warum ist das ein kritisches Risiko?

Global-Administrator-Konten sind das höchste Angriffsziel in jeder Microsoft-365-Umgebung. Ein kompromittiertes Admin-Konto ermöglicht vollständigen Datenzugriff, Löschen aller Postfächer, Deaktivierung von Sicherheitsrichtlinien und Ransomware-Verteilung an alle Geräte.

MT.1022 · Custom · Entra ID

• High

✗ Fehlgeschlagen

Privileged Identity Management (PIM) nicht konfiguriert

PIM ist für keine privilegierte Rolle aktiviert. Alle 5 Global-Admins haben permanente Admin-Rechte ohne zeitliche Begrenzung oder Aktivierungs-Workflow. Normales Arbeiten sollte ohne Admin-Rechte erfolgen (Least-Privilege-Prinzip).

Empfehlung

Entra ID PIM aktivieren: Admin-Rechte werden nur bei Bedarf (Just-in-Time) für max. 1–4 Stunden aktiviert, mit Benachrichtigung an Sicherheits-Team. Reduktion der permanenten Angriffsfläche um ca. 80 %.

EIDSCA.AP08 · EIDSCA · Entra ID

• Medium

⚠ Zu prüfen

Conditional Access – Risikobewertung deckt nicht alle Nutzer ab

Eine risikobasierte Conditional-Access-Richtlinie ist vorhanden, deckt jedoch nur **78 % der Nutzer** ab. 22 % der Benutzerkonten (ca. 55 Konten) sind von der Risiko-Richtlinie ausgenommen – absichtlich oder versehentlich?

Bitte prüfen, ob die ausgenommenen Konten legitime Ausnahmen darstellen (z. B. Service-Konten) oder versehentlich von der Richtlinie ausgeschlossen wurden. Service-Konten sollten mit separaten CA-Richtlinien gesichert oder durch Managed Identities ersetzt werden.

✓ 18 weitere Tests in diesem Modul bestanden – u. a. Breakglass-Konten, SSPR-Konfiguration, Gastzugriff-Einschränkungen, Named Locations

Microsoft Defender

✗ 12 Failed

⚠ 3 Prüfen

✓ 22 Bestanden

ORCA.133 · ORCA · Defender

● Medium

✗ Fehlgeschlagen

Defender for Office 365 – Safe Links für interne E-Mails deaktiviert

Safe-Links-Schutz ist für **interne E-Mails (Nutzer-zu-Nutzer)** nicht aktiviert. Phishing-Links in intern weitergeleiteten E-Mails werden nicht in Echtzeit geprüft. Externe E-Mails sind korrekt geschützt.

Risiko

Ein Angreifer, der ein Postfach kompromittiert hat, kann über interne Weiterleitungen Phishing-Links an alle Empfänger senden – ohne Safe-Links-Schutz werden diese Links nicht geblockt.

MT.DEF005 · Custom · Defender

● High

✗ Fehlgeschlagen

Defender for Endpoint – Geräte-Onboarding unvollständig

Nur 14 von 47 Geräten (30 %) sind in Defender for Endpoint onboardet und werden aktiv auf Bedrohungen überwacht.

Gerätekategorie	Geräte gesamt	Ongeboardet	Status
Windows Laptops	38	12 / 38	32% – kritische Lücke
Windows Server	5	5 / 5	100% – vollständig
macOS	4	0 / 4	0% – nicht konfiguriert

70 % der Endgeräte haben keinen Endpoint-Detection-&-Response-Schutz. Angriffe auf diese Geräte werden nicht erkannt. Empfehlung: Onboarding über Intune-Deployment-Policy für alle Windows-Geräte automatisieren.

✓ 22 weitere Tests bestanden – u. a. Anti-Spam Policies, Anti-Phishing Policy, Safe Attachments aktiviert, DKIM für .onmicrosoft.com

CISA.EX01 · CISA EX0 · Exchange

● High

X Fehlgeschlagen

DKIM-Signierung für Primärdomain nicht konfiguriert

DKIM (DomainKeys Identified Mail) ist für die Domain **mustermann-logistik.de** nicht aktiviert. Ausgehende E-Mails enthalten keine kryptographische Signatur.

Domain	DKIM-Status	SPF	DMARC
mustermann-logistik.de	Nicht konfiguriert	✓ Vorhanden	p=none (kein Schutz)
mustermann-log.onmicrosoft.com	Aktiv (Standard)	✓ Vorhanden	✓ p=quarantine

Risiko

Ohne DKIM können Angreifer E-Mails fälschen, die scheinbar von *@mustermann-logistik.de* stammen – Business Email Compromise (BEC) und Phishing-Angriffe auf Lieferanten und Kunden werden wesentlich erleichtert. DMARC mit p=none hat keinen Durchsetzungseffekt.

CISA.EX04 · CISA EX0 · Exchange

● Medium

X Fehlgeschlagen

DMARC Policy ohne Durchsetzung konfiguriert (p=none)

Der DMARC-Eintrag für **mustermann-logistik.de** ist mit p=none konfiguriert. Das bedeutet: Unauthentifizierte E-Mails werden *nicht abgelehnt oder in Quarantäne verschoben*, sondern lediglich protokolliert. Empfänger-Server ignorieren die Richtlinie vollständig.

Empfehlung

Nach DKIM-Aktivierung und Testphase (2–4 Wochen) DMARC-Policy auf p=quarantine und dann p=reject anpassen. Dies verhindert Domain-Spoofing vollständig.

✓ 25 weitere Tests bestanden – u. a. SPF-Records, TLS 1.2 erzwungen, Audit-Log für Exchange aktiv, Postfach-Weiterleitungsblockade

Intune / Endpoint Management

X 18 Failed

⚠ 8 Prüfen

✓ 24 Bestanden

MT.IT003 · Custom · Intune

● High

X Fehlgeschlagen

Keine aktiven Device Compliance Policies für Windows-Geräte

3 Compliance-Policies sind in Intune vorhanden, aber **0 Policies sind aktiven Gerätegruppierungen zugewiesen**. Alle Windows-Geräte gelten damit automatisch als „konform“ – unabhängig von ihrem tatsächlichen Sicherheitszustand.

Risiko

Conditional-Access-Richtlinien, die „Konformes Gerät“ als Bedingung verwenden, sind wirkungslos, wenn Compliance nicht tatsächlich geprüft wird. Kompromittierte oder veraltete Geräte erhalten vollen M365-Zugriff. Empfehlung: Policies den Intune-Gerätegruppen zuweisen und zunächst im Report-Only-Modus testen.

MT.IT012 · Custom · Intune

● High

✗ Fehlgeschlagen

BitLocker-Festplattenverschlüsselung nicht durch Richtlinie erzwungen

Die Compliance-Policy enthält **keine Anforderung für BitLocker-Verschlüsselung**. Eine Stichprobenprüfung zeigt: 28 von 38 Windows-Geräten (74 %) haben BitLocker nicht aktiviert.

Risiko

Ein gestohlener Laptop ohne BitLocker ermöglicht direkten Zugriff auf alle gespeicherten Daten – Firmendokumente, gespeicherte Passwörter, Zertifikate. DSGVO-Meldepflicht bei Datenverlust (Art. 33 DSGVO) wäre in diesem Fall wahrscheinlich ausgelöst.

MT.IT020 · Custom · Intune

● Medium

⚠ Zu prüfen

Personal Device Enrollment (BYOD) nicht eingeschränkt

Die Enrollment-Einschränkungen erlauben das Einschreiben **persönlicher Privatgeräte** in das Unternehmensmanagementsystem ohne Genehmigungsprozess.

Bitte prüfen: Ist das Einschreiben persönlicher Geräte für Ihr Unternehmen gewünscht (BYOD-Konzept)? Falls ja, sollten separate App-Protection-Policies ohne vollständige Geräteverwaltung verwendet werden. Falls nein, Enrollment-Einschränkungen auf Corporate-owned-Geräte begrenzen.

✓ 24 weitere Tests bestanden – u. a. iOS App Protection Policy, Windows Hello for Business aktiviert, Intune-Connector konfiguriert, Autopilot-Profile

Microsoft Teams

✗ 5 Failed

⚠ 3 Prüfen

✓ 16 Bestanden

MT.TE002 · Custom · Teams

● Medium

✗ Fehlgeschlagen

Meeting-Warteraum für externe Teilnehmer deaktiviert

Die globale Meeting-Policy erlaubt externen Gästen und anonymen Nutzern, **Meetings ohne Warteraum (Lobby Bypass) direkt beizutreten**. Meetings können ohne Wissen des Veranstalters abgehört werden, wenn der Link weitergegeben wurde.

Empfehlung: Lobby-Einstellung auf „Jeder aus meiner Organisation“ ändern. Externe Teilnehmer warten im Warteraum bis sie vom Veranstalter zugelassen werden. Dies verhindert unberechtigte Meeting-Teilnahme auch bei geleakten Meeting-Links.

✓ 16 weitere Tests bestanden – u. a. Drittanbieter-Apps blockiert, Gastzugriff nur mit Genehmigung, Teams-Verschlüsselung aktiv

SharePoint & OneDrive

✗ 7 Failed

⚠ 2 Prüfen

✓ 7 Bestanden

CISA.SP01 · CISA SP0 · SharePoint

• High

✗ Fehlgeschlagen

Anonyme Freigabelinks für Dateien und Ordner erlaubt

Der Standard-Freigabelinktyp in SharePoint Online und OneDrive ist auf „**Jeder mit dem Link (anonym)**“ gesetzt. Mitarbeiter können Dateien ohne Anmeldepflicht für jeden im Internet freigeben – auch versehentlich.

Einstellung	Aktueller Wert	Empfohlener Wert
Externer Freigabelinktyp	Jeder (anonym)	Bestimmte Personen
Standard-Link-Ablaufzeit	Kein Ablauf	30 Tage
Externe Freigabe SharePoint	Neue und bestehende Gäste	Neue und bestehende Gäste (akzeptabel)

Risiko

Sensible Firmendaten (z. B. Verträge, Kundenlisten, Lieferdaten) können durch versehentliche anonyme Links öffentlich zugänglich werden, ohne dass dies erkannt wird. DSGVO-Relevanz: Art. 32 verpflichtet zur angemessenen Zugangskontrolle für personenbezogene Daten.

✓ 7 weitere Tests bestanden – u. a. OneDrive-Synchronisation auf Domain-Geräte eingeschränkt, Zugriffsprotokollierung aktiv

Purview / Compliance

✗ 9 Failed

⚠ 2 Prüfen

✓ 6 Bestanden

MT.PC008 · Custom · Purview

• High

✗ Fehlgeschlagen

Unified Audit Log ist nicht aktiviert

Das **Unified Audit Log ist deaktiviert**. Benutzeraktivitäten, Admin-Änderungen, Anmeldeereignisse und Datenzugriffe werden nicht protokolliert und sind im Nachhinein nicht rekonstruierbar.

Warum ist das kritisch?

Ohne aktives Audit Log ist es bei einem Sicherheitsvorfall unmöglich festzustellen: Was wurde zugegriffen? Wann wurde die Konfiguration geändert? Welcher Admin hat was getan? Dies ist auch eine **DSGVO-Anforderung** (Nachweis der Verarbeitungstätigkeiten, Art. 5 Abs. 2 DSGVO – Rechenschaftspflicht). Abhilfe: Im Microsoft Purview Compliance-Portal unter Audit → Überwachung aktivieren (1 Klick). Protokollierung beginnt sofort.

DSGVO: Keine DLP-Policy für sensible personenbezogene Daten

Im Tenant sind **keine Data Loss Prevention (DLP)-Richtlinien** für DSGVO-relevante Datentypen konfiguriert (IBAN, Personalausweisnummern, medizinische Daten, etc.). Es ist unklar, ob und in welchem Umfang personenbezogene Daten in Exchange, SharePoint oder Teams ungeschützt übertragen werden.

Bitte prüfen: Verarbeitet Mustermann Logistik GmbH personenbezogene Daten von Kunden, Mitarbeitern oder Lieferanten in M365? Falls ja, empfehlen wir den Start mit den Microsoft-eigenen DSGVO-DLP-Vorlagen als Ausgangspunkt. Eine Sensitivitätslabel-Strategie wird ebenfalls empfohlen.

✓ 6 weitere Tests bestanden – u. a. Sensitivitätslabels aktiviert, Retention-Policies konfiguriert, Kommunikationsverschlüsselung

Empfohlene nächste Schritte**SOFORT – WOCHE 1**

- ✗ Legacy-Auth blockieren (CA-Policy)
- ✗ MFA für alle Admins erzwingen
- ✗ Unified Audit Log aktivieren
- ✗ DKIM für mustermann-logistik.de aktivieren

KURZFRISTIG – MONAT 1

- ⚠ Device Compliance Policies zuweisen
- ⚠ BitLocker-Verschlüsselung erzwingen
- ⚠ SharePoint-Freigabelinks einschränken
- ⚠ DMARC auf p=quarantine anheben

MITTELFRISTIG – QUARTAL 2

- PIM für privilegierte Rollen einrichten
- Defender for Endpoint vollständig ausrollen
- DLP-Policies für DSGVO-Daten konfigurieren
- Sensitivitätslabels-Rollout planen

CONTINUOUS MONITORING

- ✓ Monatliche automatisierte Tenant Scans
- ✓ Trendanalyse: Fortschritt sichtbar machen
- ✓ Frühwarnung bei neuen Konfigurationsabweichungen
- ✓ Previder Managed Security Service