CUSTODIT

CYBER
SECURITY
ASSESSMENT

SICHERHEITSREPORT

Mustermann Maschinenbau GmbH

Berichtszeitraum: Juli 2026
Erstellt am 14.7.2026

ZUSAMMENFASSUNG

Auf einen Blick

Der Sicherheitsscore liegt bei 74 von 100 Punkten (BEFRIEDIGEND).

In den letzten 7 Tagen wurden Legacy Sign-ins erkannt. Legacy Auth ist ein häufiges Einfallstor (Password Spraying) und umgeht moderne Controls.

Aktive CA Policies: - · MFA Policies: -. Ohne MFA-Enforcement steigt das Risiko von Kontoübernahmen deutlich.

Weitere 2 Thema(en) - Details ab Seite 3.

3 Bereich(e) ohne Auffaelligkeiten.

Gegenueber Juni 2026 hat sich der Score um 13 Punkte verbessert.

NAECHSTE SCHRITTE

- CA Policy aktivieren: Legacy Clients blocken (mit Break-Glass
- Ausnahme).
- Betroffene User/Apps identifizieren (Top User/IPs/Client apps) und
- priorisieren.
- CA-Policy erstellen/aktivieren: MFA als Grant Control (Break-Glass
- Ausnahme).
- Audit: Wer braucht wirklich Global Admin? Inaktive/überflüssige
- entfernen.

Mustermann Maschinenbau GmbH

SCORE	OK	WARNUNGEN	KRITISCH
74 BEFRIEDIGEND	3	3	1

Mandant: Mustermann Maschinenbau GmbH | Tarif: Plus | Nutzer: 42 | Stand: 14.7.2026, 10:51:36

WICHTIGSTE THEMEN

Priorisiert nach Dringlichkeit

- Legacy Auth Nutzung (letzte 7 Tage): In den letzten 7 Tagen wurden Legacy Sign-ins erkannt. Legacy Auth ist ein häufiges Einfallstor (Password Spraying) und umgeht moderne Controls.
- Conditional Access: MFA Policy vorhanden: Aktive CA Policies: - · MFA Policies: -. Ohne MFA-Enforcement steigt das Risiko von Kontoübernahmen deutlich.
- Anzahl Global Admins: Es wurden mehrere Global Admin(s) erkannt. Zu viele Vollzugriffs-Konten erhöhen Risiko und Governance-Aufwand.
- Gast-Accounts (extern) im Tenant: Es wurden Gast-Accounts erkannt. Gäste sind oft nötig, müssen aber aktiv governanced werden.

ALLE PRUEFUNGEN

Aktueller Status

THEMA	STATUS
Legacy Auth Nutzung (letzte 7 Tage) - In den letzten 7 Tagen wurden Legacy Sign-ins erkannt.	KRITISCH
Conditional Access: MFA Policy vorhanden - Aktive CA Policies: - · MFA Policies: -. Ohne	WARNUNG
Anzahl Global Admins - Es wurden mehrere Global Admin(s) erkannt. Zu viele Vollzugriffs-Konten	WARNUNG
Gast-Accounts (extern) im Tenant - Es wurden Gast-Accounts erkannt. Gäste sind oft nötig,	WARNUNG
Risky Sign-ins (letzte 7 Tage) - Keine Auffaelligkeiten	OK
Conditional Access aktiv (mind. 1 Policy) - Keine Auffaelligkeiten	OK
Security Defaults aktiv - Keine Auffaelligkeiten	OK

Was wurde diesen Monat erkannt und abgewehrt?

Custodit ueberwacht Microsoft 365, Firewall und Endgeraete rund um die Uhr. Die folgenden Zahlen fassen den Zeitraum Juli 2026 zusammen.

EREIGNISSE	DAVON KRITISCH	VORFAELLE OFFEN	VORFAELLE ERLEDIGT
1428	12	1	2
ausgewertet	hohe Prioritaet	in Bearbeitung	abgewehrt/geloest

Trend zum Vormonat
Der Sicherheitsscore hat sich gegenueber Juni 2026 verbessert: 61 -> 74 Punkte (+13).

ERKANNTE EREIGNISSE NACH ART

Haeufigste Quellen

Fehlgeschlagene Anmeldungen	643
Riskante Anmeldungen	21
Rollenänderungen	4
Firewall: blockierte Zugriffe	512

SICHERHEITSVORFAELLE

Erkannt und bearbeitet

VORFALL	SCHWEREGRAD	STATUS	EREIGNISSE
Brute-Force-Versuch auf mehrere Konten	Hoch	Erledigt	214
Riskante Anmeldung aus untypischem Land	Mittel	Offen	6

KRITISCH **Legacy Auth Nutzung (letzte 7 Tage)** Geprueft: 14.7.2026, 10:51:36

BEFUND

Was wurde festgestellt?

In den letzten 7 Tagen wurden Legacy Sign-ins erkannt. Legacy Auth ist ein häufiges Einfallstor (Password Spraying) und umgeht moderne Controls.

- CA Policy aktivieren: Legacy Clients blocken (mit Break-Glass Ausnahme).
- Betroffene Apps/Clients identifizieren und auf Modern Auth migrieren.

> **Was bedeutet das?**
> Hohe Angriffsfläche: Legacy Clients nutzen oft schwächere Auth-Flows und umgehen MFA/Conditional Access teilweise.

EMPFOHLENE SCHRITTE

Konkret und umsetzbar

- CA Policy aktivieren: Legacy Clients blocken (mit Break-Glass Ausnahme).
- Betroffene User/Apps identifizieren (Top User/IPs/Client apps) und priorisieren.

DAUERHAFT SAUBER LOESEN

- Legacy Clients auf Modern Auth migrieren (IMAP/POP/SMTP/ActiveSync nur wenn wirklich nötig).
- Optional: Tenantweit Basic Auth in Exchange Online deaktivieren (falls relevant).

PRUEFEN OB ERLEDIGT

- Sign-in logs erneut prüfen: Legacy Client apps sollten auf 0 fallen.
- Zusätzlich: Check `conditional_access_legacy_block_present` muss OK sein.

SO FINDEST DU DAS IM ADMIN CENTER

- Entra Admin Center -> Monitoring -> Sign-in logs
- Filter: Client app = Other clients / IMAP / POP / SMTP / Exchange ActiveSync

KENNZAHLEN

Legacy Sign-ins (7d)	-

WARNUNG **Conditional Access: MFA Policy vorhanden** Geprueft: 14.7.2026, 10:51:36

BEFUND

Was wurde festgestellt?

Aktive CA Policies: - · MFA Policies: -. Ohne MFA-Enforcement steigt das Risiko von Kontoübernahmen deutlich.

- CA-Policy erstellen/aktivieren: Grant Controls enthält "Require multifactor authentication".
- Rollout mit Break-Glass Ausnahme planen.

> **Was bedeutet das?**
> Erhöhtes Risiko von Kontoübernahmen: MFA ist der wichtigste Basisschutz gegen Passwort-Angriffe.

EMPFOHLENE SCHRITTE

Konkret und umsetzbar

- CA-Policy erstellen/aktivieren: MFA als Grant Control (Break-Glass Ausnahme).

DAUERHAFT SAUBER LOESEN

- Rollout-Plan: erst Admins, dann alle User, Monitoring + Nutzerkommunikation.

PRUEFEN OB ERLEDIGT

- Nach Aktivierung: Check `conditional_access_mfa_present` = OK

SO FINDEST DU DAS IM ADMIN CENTER

- Entra Admin Center -> Protection -> Conditional Access -> Policies
- Policy prüfen: Grant Controls enthält "Require multifactor authentication"

WARNUNG **Anzahl Global Admins** Geprueft: 14.7.2026, 10:51:36

BEFUND

Was wurde festgestellt?

Es wurden mehrere Global Admin(s) erkannt. Zu viele Vollzugriffs-Konten erhöhen Risiko und Governance-Aufwand.

- Rollen reduzieren, JIT/PIM nutzen, Admin-Schutz (MFA/CA) erzwingen.

> **Was bedeutet das?**
> Je mehr Vollzugriffs-Konten, desto größer die Angriffsfläche und das Risiko von Fehlkonfigurationen.

EMPFOHLENE SCHRITTE

Konkret und umsetzbar

- Audit: Wer braucht wirklich Global Admin? Inaktive/überflüssige entfernen.

DAUERHAFT SAUBER LOESEN

- Least Privilege Rollen nutzen, JIT/PIM etablieren, separate Admin-Konten verwenden.

PRUEFEN OB ERLEDIGT

- Check `global_admin_count` sollte nach Reduktion OK/Warn-Grenze unterschreiten.

SO FINDEST DU DAS IM ADMIN CENTER

- Entra Admin Center -> Roles and administrators -> Global Administrator

KENNZAHLEN

Global Admins	-

WARNUNG **Gast-Accounts (extern) im Tenant** Geprueft: 14.7.2026, 10:51:36

BEFUND

Was wurde festgestellt?

Es wurden Gast-Accounts erkannt. Gäste sind oft nötig, müssen aber aktiv governanced werden.

- Access Reviews/Expiry einführen und Einladungsregeln restriktiv setzen.

> **Was bedeutet das?**
> Ohne Reviews/Expiry können externe Identitäten dauerhaft Zugriff behalten - oft unbemerkt.

EMPFOHLENE SCHRITTE

Konkret und umsetzbar

- Liste prüfen: braucht jeder Gast noch Zugriff? Inaktive/alte Gäste entfernen.

DAUERHAFT SAUBER LOESEN

- Access Reviews/Expiry einführen, Einladungsrechte restriktiv konfigurieren.

PRUEFEN OB ERLEDIGT

- Regelmäßig: Gäste-Liste + letzte Sign-ins prüfen.

SO FINDEST DU DAS IM ADMIN CENTER

- Entra Admin Center -> Users -> All users -> Filter: User type = Guest

KENNZAHLEN

Aktive Gäste	-