Alexander Frank · Identity & Endpoint Management

BEISPIELBERICHT · FIKTIVE DATEN

Identity-Check Microsoft 365 & Entra ID

Wer kommt mit welchem Konto, von welchem Gerät, an welche Daten? Bestandsaufnahme, Risiken und ein umsetzbarer Maßnahmenplan.

4	7	2	16
Befunde hoch	Befunde mittel	Befunde niedrig	Prüfpunkte in Ordnung

AUFTRAGGEBER
Musterbau Nord GmbH (fiktiv)

UMGEBUNG
1 Mandant · 85 Benutzer · Business Premium

STAND
11.11.2026 · Version 1.0

Dieser Bericht ist ein Muster. Firma, Personen, Zahlen und Befunde sind erfunden. Aufbau, Prüfmethode und Detailtiefe entsprechen einem echten Identity-Check. Für Systemhäuser kann der Bericht im eigenen Design und unter eigenem Namen geliefert werden.

1 · MANAGEMENT-ZUSAMMENFASSUNG

Ein gestohlenes Passwort reicht heute noch aus.

Die Microsoft-365-Umgebung der Musterbau Nord GmbH ist gut lizenziert, aber nur zum Teil abgesichert. Die vorhandene Lizenz (Business Premium mit Entra ID P1 und Intune) enthält fast alles, was nötig ist. Es ist nur nicht eingeschaltet.

9 von 85
Konten ohne registrierte Mehrfaktor-Anmeldung

143
Anmeldeversuche über veraltete Protokolle in 30 Tagen, aus 6 Ländern

6
globale Administratoren, empfohlen sind höchstens 2 bis 4 plus Notfallkonten

Die drei wichtigsten Risiken in Klartext

1. **Rechnungsbetrug über ein gekapertes Postfach.** Neun Konten lassen sich allein mit einem Passwort übernehmen, zwei davon in der Buchhaltung. In einem Postfach der Buchhaltung leitet eine Regel E-Mails an eine externe Adresse weiter. Genau dieses Muster wird für Betrug mit geänderter IBAN genutzt.
2. **Angriffe laufen bereits, sie werden nur noch nicht gesehen.** Über veraltete Protokolle (IMAP, SMTP-Authentifizierung) wird automatisiert durchprobiert, welches Passwort passt. Bisher ohne Erfolg, aber diese Protokolle umgehen die Mehrfaktor-Anmeldung.
3. **Zu viele Schlüssel zum ganzen Haus.** Sechs Personen haben volle Administratorrechte, zwei davon arbeiten mit demselben Konto täglich im Postfach. Wird eines dieser Konten übernommen, gehört dem Angreifer der gesamte Mandant.

Bedeutung für Versicherung und Kunden: Cyberversicherer fragen Mehrfaktor-Anmeldung für alle Konten und den Schutz administrativer Zugänge regelmäßig ab. Auftraggeber im NIS2-Umfeld verlangen von Lieferanten zunehmend Nachweise zum Zugriffsschutz. Mit dem aktuellen Stand wären diese Fragen nicht guten Gewissens mit „Ja“ zu beantworten.

Empfehlung

Die vier hohen Befunde lassen sich in **etwa einer Woche** schließen, ohne Zusatzlizenzen und ohne Ausfall für die Mitarbeitenden. Danach folgt eine Conditional-Access-Basis, die zuerst im Berichtsmodus läuft und nach Kontrolle der Auswirkungen scharf geschaltet wird. Den Plan dafür zeigt Kapitel 5.

BEREICH	BEWERTUNG	KURZBEGRÜNDUNG
Anmeldung & MFA	kritisch	Lücken in der MFA-Abdeckung, Legacy-Protokolle offen, Sicherheitsstandards ohne Ersatz abgeschaltet
Privilegierte Konten	kritisch	Zu viele globale Administratoren, keine Trennung von Alltags- und Admin-Konto, kein Notfallkonto
Lebenszyklus (Eintritt/Austritt)	kritisch	Konten ehemaliger Mitarbeitender aktiv und lizenziert
Gäste & Anwendungen	verbesserungswürdig	Inaktive Gäste, langlebige App-Geheimnisse, Benutzer dürfen Apps selbst freigeben
E-Mail-Absicherung	verbesserungswürdig	DMARC nur beobachtend, DKIM nicht aktiv, externe Weiterleitung
Geräte	verbesserungswürdig	Gut ein Drittel der Windows-Geräte nicht in Intune, Gerätezustand fließt nicht in die Zugriffsentscheidung ein

2 · UMFANG UND METHODE

Nur lesen, nichts verändern.

Der Check wurde remote und ausschließlich mit Leserechten durchgeführt. In der Umgebung wurde keine Einstellung geändert.

Geprüft

- Microsoft Entra ID: Benutzer, Gruppen, Rollen, Authentifizierungsmethoden, Conditional Access, Sicherheitsstandards, Gäste, App-Registrierungen und Unternehmensanwendungen, Zustimmungseinstellungen
- Anmelde- und Auditprotokolle der letzten 30 Tage
- Exchange Online: Weiterleitungen, Posteingangsregeln, Authentifizierungsprotokolle
- Mail-Domain: SPF, DKIM, DMARC
- Intune: registrierte Geräte, Compliance-Richtlinien

Nicht geprüft

- Lokales Active Directory und Server
- Firewall, Netzwerk, Endgeräte-Virenschutz (EDR) im Detail
- Inhalte von Postfächern und Dateien
- Penetrationstest oder aktive Angriffe

Diese Bereiche können in einem Folgeauftrag oder durch das betreuende Systemhaus geprüft werden.

Vorgehen

SCHRITT	INHALT	DAUER
1 Zugang	Der Kunde legt ein zeitlich begrenztes Konto mit den Rollen *Globaler Leser* und *Sicherheitsleser* an (für Exchange: *View-Only Organization Management*). Anmeldung nur mit FIDO2-Schlüssel.	15 Minuten beim Kunden
2 Automatisch	Prüfläufe mit Maester (Open Source, Testsammlungen nach EIDSCA, CISA SCuBA und CIS) und eigenen Microsoft-Graph-PowerShell-Abfragen. Ergebnisse werden lokal gespeichert und nach Projektende gelöscht.	½ Tag
3 Manuell	Bewertung jeder Abweichung im Kontext: Ist sie Absicht? Gibt es eine Ausnahme mit Grund? Welche Konten sind wirklich betroffen? Abgleich mit den Anmeldeprotokollen.	½ Tag
4 Bericht	Befunde mit Risiko, Nachweis und Empfehlung, Maßnahmenplan mit Aufwand, Zusammenfassung für die Geschäftsführung.	½ Tag
5 Gespräch	Vorstellung der Ergebnisse (60 Minuten), Fragen, Entscheidung über die nächsten Schritte. Danach wird das Lesekonto entfernt.	1 Stunde

Bewertungsmaßstab

hoch	Ermöglicht ohne weitere Hürde die Übernahme von Konten oder Daten. Innerhalb von 1–2 Wochen beheben.
mittel	Erhöht das Risiko deutlich oder erschwert die Erkennung eines Angriffs. Innerhalb von 4–6 Wochen beheben.
niedrig	Verbesserung für Betrieb oder Nachweisbarkeit. Im Rahmen der laufenden Betreuung.

3 · BEFUNDE IM ÜBERBLICK

13 Befunde, 4 davon dringend.

ID	RISIKO	BEFUND	EMPFEHLUNG	AUFWAND
F01	hoch	9 von 85 aktiven Konten ohne registrierte MFA-Methode, davon 2 in der Buchhaltung. Sicherheitsstandards sind deaktiviert, eine Conditional-Access-Regel zur MFA fehlt.	MFA-Pflicht für alle Benutzer per Conditional Access (CA01), Registrierungskampagne mit Authenticator bzw. Passkey.	0,5 PT
F02	hoch	Veraltete Authentifizierung nicht blockiert. 143 fehlgeschlagene Anmeldeversuche über IMAP und SMTP-Authentifizierung in 30 Tagen, aus 6 Ländern, typisches Passwort-Spray-Muster.	Legacy-Authentifizierung per CA blockieren (CA02), SMTP-AUTH mandantenweit abschalten, Ausnahme nur für ein dokumentiertes Scan-Gerät.	0,25 PT
F03	hoch	6 globale Administratoren, 2 davon nutzen dasselbe Konto für E-Mail und Alltag. Keine Notfallkonten.	Getrennte Admin-Konten, Rollen nach minimalem Bedarf, phishingresistente MFA für Admins (CA03), 2 Notfallkonten mit FIDO2 und Überwachung.	0,5 PT
F04	hoch	3 Konten ausgeschiedener Mitarbeitender sind aktiv und lizenziert, letzte Anmeldung bei einem davon vor 11 Tagen.	Sofort sperren, Sitzungen widerrufen, Anmeldungen seit Austritt prüfen. Austrittsprozess als Checkliste bzw. Skript festlegen.	0,25 PT
F05	mittel	2 Posteingangsregeln leiten E-Mails an externe Adressen weiter, eine davon aus der Buchhaltung an ein privates Postfach.	Regel mit Fachbereich klären und entfernen, externe automatische Weiterleitung organisationsweit unterbinden.	0,25 PT
F06	mittel	37 Gastkonten, 21 davon seit über 180 Tagen ohne Anmeldung.	Inaktive Gäste entfernen, Einladungen auf Rollen beschränken, Zugriffsüberprüfung für Gäste vierteljährlich.	0,25 PT
F07	mittel	4 App-Registrierungen mit Geheimnissen über 12 Monate Laufzeit, eine davon mit Anwendungsberechtigung *Mail.ReadWrite* für alle Postfächer.	Berechtigung auf benötigte Postfächer begrenzen, Zertifikat statt Geheimnis, Laufzeit max. 6 Monate, Verantwortliche je App festlegen.	0,5 PT
F08	mittel	Benutzer dürfen Drittanbieter-Apps selbst Zugriff auf ihre Daten erteilen.	Benutzerzustimmung einschränken, Genehmigungsworkflow für App-Anfragen.	0,25 PT
F09	mittel	DMARC steht auf *p=none*, DKIM ist für die Hauptdomain nicht aktiviert.	DKIM aktivieren, DMARC-Berichte auswerten, schrittweise auf *quarantine* bzw. *reject*.	0,25 PT
F10	mittel	31 von 72 Windows-Geräten sind nicht in Intune. Der Gerätezustand wird bei der Zugriffsentscheidung nicht berücksichtigt.	Geräte aufnehmen, Compliance-Richtlinie, CA05 zuerst im Berichtsmodus.	2–3 PT
F11	mittel	Anmeldungen mit Gerätecode-Fluss sind erlaubt, werden aber nicht genutzt.	Gerätecode-Fluss per CA blockieren (CA04).	0,1 PT
F12	niedrig	Self-Service-Kennwortzurücksetzung ist nicht aktiviert.	SSPR mit den bereits registrierten MFA-Methoden einschalten.	0,1 PT
F13	niedrig	Anmeldeprotokolle stehen nur 30 Tage zur Verfügung, keine Benachrichtigung bei Änderungen an Rollen.	Protokolle exportieren (z. B. Log Analytics), Warnung bei Rollenänderungen.	0,5 PT

PT = Personentag. Aufwand geschätzt für Umsetzung inklusive Test und Dokumentation.

Was genau gefunden wurde und wie.

F01 · Konten ohne Mehrfaktor-Anmeldung

hoch

Ein Passwort allein schützt ein Konto nicht mehr, wenn es bei einem Phishing-Angriff oder aus einem Datenleck bekannt wird. Neun aktive Konten haben keine zweite Methode registriert und können deshalb auch nicht dazu gezwungen werden.

```
# Nachweis: Registrierungsstatus aller Mitglieder (nur lesen)
Connect-MgGraph -Scopes "AuditLog.Read.All","UserAuthenticationMethod.Read.All"
Get-MgReportAuthenticationMethodUserRegistrationDetail -All |
  Where-Object { -not $_.IsMfaRegistered -and $_.UserType -eq "member" } |
  Select-Object UserPrincipalName, MethodsRegistered

# Ergebnis (gekürzt, Namen pseudonymisiert)
UserPrincipalName              MethodsRegistered
-----------------              -----------------
buchhaltung.01@musterbau.example   {}
buchhaltung.02@musterbau.example   {}
… 7 weitere
```

Ursache Die Sicherheitsstandards wurden 2024 abgeschaltet, um ein Scan-Gerät anzubinden. Eine Ersatzregel wurde nie angelegt.

Empfehlung Richtlinie CA01 „MFA für alle Benutzer“ mit Ausnahme der Notfallkonten, zuerst 7 Tage im Berichtsmodus. Vorher Registrierungskampagne über das Microsoft-Authenticator-Onboarding.

F02 · Passwort-Spray über veraltete Protokolle

hoch

Die Anmeldeprotokolle zeigen gleichmäßig verteilte Fehlversuche gegen viele Konten mit wenigen, häufigen Passwörtern. Diese Versuche laufen über IMAP und SMTP-Authentifizierung. Diese Protokolle können keine Mehrfaktor-Anmeldung abfragen. Hat ein Konto ein schwaches Passwort, ist es damit offen, auch wenn MFA registriert ist.

PROTOKOLL (CLIENTAPPUSED)	VERSUCHE	KONTEN	LÄNDER	ERFOLGREICH
IMAP4	96	41	5	0
Authenticated SMTP	47	22	4	0
Exchange ActiveSync	0	0	0	0

Einordnung Bisher wurde kein Konto übernommen. Das Risiko liegt darin, dass ein einziger Treffer genügt und dieser in den Protokollen nach 30 Tagen nicht mehr nachweisbar wäre.

Empfehlung CA02 „Legacy-Authentifizierung blockieren“ sofort aktiv schalten (keine legitime Nutzung gefunden außer einem Scan-Gerät, das auf eine App-spezifische Lösung umgestellt wird).

F05 · Externe Weiterleitung aus der Buchhaltung

mittel

Eine Posteingangsregel im Postfach „buchhaltung.02“ leitet alle E-Mails mit „Rechnung“ im Betreff an eine private Adresse weiter. Ob die Regel von der Mitarbeiterin selbst oder von einem Angreifer stammt, lässt sich aus der Konfiguration allein nicht sagen. Genau solche Regeln werden bei Rechnungsbetrug angelegt, um mitzulesen und Antworten abzufangen.

Empfehlung Mit der Mitarbeiterin klären, Regel entfernen, Anmeldungen des Kontos der letzten 30 Tage prüfen, Passwort zurücksetzen und MFA registrieren lassen. Danach externe automatische Weiterleitung organisationsweit sperren.

5 · MASSNAHMENPLAN

In drei Schritten zu einer belastbaren Basis.

Der Plan ist so geschnitten, dass die dringenden Punkte zuerst geschlossen werden und niemand im Betrieb ausgesperrt wird. Jede Richtlinie läuft vor dem Scharfschalten im Berichtsmodus.

Schritt 1 Woche 1	• Konten Ausgeschiedener sperren (F04) • Notfallkonten anlegen, Admin-Konten trennen (F03) • Legacy-Authentifizierung blockieren (F02) • Externe Weiterleitung klären und sperren (F05)	**ca. 1,5 PT**
Schritt 2 Woche 2–4	• Conditional-Access-Basis CA01–CA05 im Berichtsmodus, Auswertung, dann aktiv (F01, F11) • MFA-Registrierung aller Benutzer, SSPR (F12) • App-Zustimmung einschränken, App-Geheimnisse ersetzen (F07, F08) • DKIM aktivieren, DMARC schrittweise verschärfen (F09)	**ca. 3 PT**
Schritt 3 ab Monat 2	• Geräte in Intune aufnehmen, Compliance, CA05 aktiv (F10) • Gäste-Review vierteljährlich (F06) • Protokollexport und Warnungen (F13) • Monatliche Kontrolle: neue Admins, neue Apps, Abweichungen von der Basis	**2–3 PT** + laufend

Richtlinien der Conditional-Access-Basis

NAME	WIRKUNG	START
`CA01-MFA-AlleBenutzer`	Mehrfaktor-Anmeldung für alle Benutzer und Anwendungen	Berichtsmodus 7 Tage
`CA02-BlockLegacyAuth-AlleBenutzer`	Blockiert Protokolle ohne MFA-Fähigkeit	sofort aktiv
`CA03-StarkeMFA-Admins`	Phishingresistente Anmeldung (FIDO2/Passkey) für Administratorrollen	nach Registrierung
`CA04-BlockDeviceCode-AlleBenutzer`	Blockiert den Gerätecode-Anmeldefluss	sofort aktiv
`CA05-KonformesGeraet-Pilot`	Zugriff nur von konformen Geräten, zunächst für eine Pilotgruppe	Berichtsmodus

Alle Richtlinien schließen die Gruppe `GRP-CA-Exclude-BreakGlass` aus. Jede Änderung wird mit Datum, Grund und Ergebnis im Änderungsprotokoll festgehalten.

Umsetzung: Schritt 1 und 2 entsprechen dem Paket *Identity-Baseline* (Festpreis). Schritt 3 kann als Projekt oder in der laufenden Betreuung *Managed Identity* erfolgen. Alles wird so dokumentiert, dass das interne Team oder das betreuende Systemhaus die Umgebung danach selbst weiterführen kann.

ANHANG A · PRÜFKATALOG (AUSZUG)

32 Prüfpunkte, Ergebnis je Punkt.

PRÜFPUNKT	ERGEBNIS
MFA für alle Benutzer erzwungen	×
Legacy-Authentifizierung blockiert	×
Phishingresistente MFA für Administratoren	×
Anzahl globaler Administratoren ≤ 4	×
Mindestens 2 Notfallkonten, aus CA ausgeschlossen, überwacht	×
Keine aktiven Konten ausgeschiedener Mitarbeitender	×
Externe automatische Weiterleitung gesperrt	×
Gäste: Inaktive Konten unter 10 %	×
Benutzerzustimmung für Apps eingeschränkt	×
App-Geheimnisse mit Laufzeit ≤ 6 Monate	teilweise
DKIM aktiv, DMARC mindestens quarantine	teilweise
Gerätecode-Fluss blockiert	×
Geräte vollständig in Intune, Compliance in CA	teilweise

PRÜFPUNKT	ERGEBNIS
SSPR aktiviert	×
Warnung bei Änderungen an privilegierten Rollen	×
Sicherheitsstandards oder gleichwertige CA-Regeln aktiv	×
Kennwortablauf deaktiviert (Empfehlung NIST/Microsoft)	✓
Benutzer dürfen keine Mandanten anlegen	✓
Benutzer dürfen keine App-Registrierungen anlegen	✓
Gastzugriff auf Verzeichnisobjekte eingeschränkt	✓
Microsoft-Authenticator mit Nummernabgleich	✓
SMS als Methode nicht für Administratoren	✓
Smart Lockout aktiv	✓
Benannte Orte gepflegt	✓
Weitere 8 Prüfpunkte in Ordnung	✓

Anhang B · Begriffe für die Geschäftsführung

MFA	Anmeldung mit zweitem Faktor, z. B. Bestätigung in einer App oder Sicherheitsschlüssel. Ein gestohlenes Passwort reicht dann nicht mehr.
Conditional Access	Regeln in Microsoft Entra ID, die bei jeder Anmeldung entscheiden: Wer, von welchem Gerät, von wo, auf welche Anwendung, und ob zusätzlich MFA nötig ist.
Legacy-Authentifizierung	Ältere Anmeldeverfahren (z. B. IMAP), die keine MFA kennen und deshalb gern für Angriffe genutzt werden.
Notfallkonto	Zwei streng geschützte Konten, mit denen man den Mandanten auch dann noch verwalten kann, wenn eine Regel versehentlich alle aussperrt.

Erstellt von
Alexander Frank · Identity & Endpoint Management
SC-300 · MD-102 · Okta Certified Administrator
alexander-frank.org

Hinweis
Muster mit fiktiven Daten. Ein echter Bericht enthält die vollständige Befundliste mit Nachweisen und wird vertraulich übergeben. Für Systemhäuser auf Wunsch im eigenen Design und unter eigenem Namen.