/ MAURISEC.DE

FIELD NOTES / CHECKLIST 01

Entra ID: Identitäten, Anmeldung und Notfallzugriff prüfen

PRUEFEN. BELEGEN. NACHHALTEN.

Für einen eigenen Microsoft-Entra-Tenant. Bestand und Nachweise zuerst erfassen; Änderungen über einen freigegebenen Pilot durchführen. Benötigte Rollen, Lizenzen und vorhandene Richtlinien vorab prüfen. Quellenstand: 09.11.2026.

Pruefbereich / Team:

Datum:

- [ ] **01 / Zuständigkeit und aktuelle Entra-Konfiguration einschließlich Security Defaults und Conditional Access erfassen.**

  Nachweis: Datierter Konfigurationsexport mit verantwortlicher Person und Prüfbereich.

- [ ] **02 / Prüfen, ob MFA-Registrierung und tatsächlich erzwungener MFA-Schutz die vorgesehenen Benutzer und Administratoren abdecken.**

  Nachweis: Registrierungsbericht sowie passende erfolgreiche und abgewiesene Testanmeldungen.

- [ ] **03 / Für privilegierte Konten geeignete phishingresistente Methoden planen und deren tatsächliche Verwendung prüfen.**

  Nachweis: Methodenrichtlinie und Anmeldedetails eines autorisierten Testkontos.

- [ ] **04 / Legacy-Authentifizierung im Bestand identifizieren und die wirksame Sperre mit einem freigegebenen Negativtest belegen.**

  Nachweis: Anmeldeauswertung und dokumentiertes Blockierungsergebnis; notwendige Migrationen separat erfassen.

- [ ] **05 / Mindestens zwei cloudbasierte Notfallkonten mit unabhängigen, phishingresistenten Anmeldemitteln vorsehen und testen.**

  Nachweis: Notfallkonzept und Testprotokoll; keine Geheimnisse im Prüfbericht.

/ MAURISEC.DE

FIELD NOTES / CHECKLIST 01

- [ ] **06 / Notfallkonten vor sperrenden Anmelderichtlinien schützen und jede Nutzung oder Änderung überwachen.**

  Nachweis: Begründete Ausnahmen, funktionierender Alarm und dokumentierter Wiederherstellungstest.

- [ ] **07 / Benutzerzustimmung zu Anwendungen begrenzen und einen geregelten Prüfweg für weitergehende Berechtigungen festlegen.**

  Nachweis: Zustimmungsrichtlinie, zuständige Prüfpersonen und eine nachvollziehbare Beispielentscheidung.

- [ ] **08 / Bereits erteilte Anwendungsberechtigungen auf Erforderlichkeit, verantwortliche Person und ungewöhnliche Zugriffe prüfen.**

  Nachweis: Berechtigungsexport, begründete Freigaben und nachverfolgte Maßnahmen für Auffälligkeiten.

GEGENPROBE / AUTORISIERTE TESTUMGEBUNG

Mit einem freigegebenen Testkonto eine erwartete Anmeldung und eine erwartete Sperre prüfen; die tatsächlich angewendeten Kontrollen in den Anmeldedetails nachvollziehen.

GRENZEN UND VORAUSSETZUNGEN

MFA-Registrierung beweist keine durchgehende MFA-Erzwingung. Allgemeine MFA ist nicht automatisch phishingresistent. Security Defaults und individuelle Conditional-Access-Richtlinien sind alternative Betriebsmodelle; beim Wechsel keine Schutzlücke schaffen. Notfallkonten sind keine ungeschützten MFA-Ausnahmen. Diese Checkliste bestätigt weder einen kompromissfreien Tenant noch eine vollständige Härtung.

PRIMAERQUELLEN / STAND 09.11.2026

Microsoft Learn: Security defaults
learn.microsoft.com

Microsoft Learn: Emergency access accounts
learn.microsoft.com

Microsoft Learn: Authentication strengths
learn.microsoft.com

Microsoft Learn: Application consent management
learn.microsoft.com

Microsoft Learn: Review application permissions
learn.microsoft.com