/ MAURISEC.DE

FIELD NOTES / CHECKLIST 13

Der IdP fällt aus: Notfallzugang ohne zirkuläre Abhängigkeiten

PRUEFEN. BELEGEN. NACHHALTEN.

Für einen eigenen Entra-Tenant mit föderierter Anmeldung und abhängigen Verwaltungsdiensten. Richtwert: 90 Minuten für einen vorbereiteten Zugangspfad; Neubau, Beschaffung und Behebung zusätzlich. Prioritäten gelten für dieses Ausfallszenario, nicht als allgemeine Compliance-Vorgabe.

Pruefbereich / Team:

Datum:

- [ ] **01 / Ausfallvarianten getrennt modellieren: Föderation, MFA-Methode, PIM-Genehmigung, Verwaltungsgerät und Entra-Dienst selbst.**

  Nachweis: Abhängigkeitsmatrix mit erreichbaren Ressourcen und verbleibendem Zugangsweg je Variante.

- [ ] **02 / Mindestens zwei cloudbasierte Notfallkonten auf der onmicrosoft.com-Domäne mit dauerhaft aktiver Global-Administrator-Rolle prüfen.**

  Nachweis: Objekt- und Rollenexport; keine Synchronisierung, Föderation oder notwendige PIM-Aktivierung.

- [ ] **03 / Unabhängige phishingresistente Anmeldemittel bereitstellen; Ablauf, Wiederbeschaffung und sichere getrennte Aufbewahrung prüfen.**

  Nachweis: Methoden- und Verwahrnachweis ohne Geheimnisse; keine Abhängigkeit vom privaten Telefon eines einzelnen Administrators.

- [ ] **04 / Sperrende Conditional-Access-Bedingungen für die Notfallkonten ausschließen und den tatsächlich verbleibenden MFA-Schutz prüfen.**

  Nachweis: Richtlinienabgleich und erfolgreiche Anmeldedetails; eine CA-Ausnahme wird nicht als pauschale MFA-Befreiung behandelt.

- [ ] **05 / Runbook, Freigabeverantwortliche, Schlüsselzugang und sichere Verwaltungsstation ohne Anmeldung am ausgefallenen IdP erreichbar halten.**

  Nachweis: Abruf- und Zugangstest einschließlich Tresor, Kontaktliste und benötigter Netzwerkverbindung.

☐ **06 / Für lokale Infrastruktur und kritische SaaS-Dienste herstellerseitig unterstützte Wiederherstellungswege gesondert festlegen.**

Nachweis: Dienstbezogene Ablaufpläne mit Befugnissen und Rücknahme; Cloud- und lokale Notfallzugänge hängen nicht gegenseitig voneinander ab.

☐ **07 / Jede Notfallanmeldung und relevante Kontoänderung an einen im Ausfallszenario erreichbaren Reaktionsweg melden.**

Nachweis: Empfangener Testalarm mit Zeitstempel, Konto-ID, Vertretung und dokumentierter Reaktion.

☐ **08 / Zugriff und notwendige Verwaltungsfunktion mindestens alle 90 Tage sowie nach relevanten Änderungen erproben; jede Nutzung nachbesprechen.**

Nachweis: Übungsprotokoll, offene Abhängigkeiten, Wiederherstellungszeit und kontrollierte Rücknahme der Übungsänderung.

GEGENPROBE / AUTORISIERTE TESTUMGEBUNG

In einer freigegebenen Übung den regulären IdP-Zugang im Ablauf als nicht verfügbar behandeln. Über die vorbereitete sichere Station mit einem Notfallkonto anmelden, eine vorher benannte leere Testgruppe umbenennen und zurückbenennen. Bestehen: kein reguläres SSO, keine PIM-Freigabe und kein gesperrter Tresor erforderlich; beide Änderungen und der Nutzungsalarm sind nachweisbar.

GRENZEN UND VORAUSSETZUNGEN

Ein cloudbasiertes Entra-Notfallkonto hilft bei Ausfall eines vorgeschalteten IdP, nicht bei vollständiger Unerreichbarkeit von Entra. Zertifikatsauthentifizierung kann eigene PKI-Abhängigkeiten mitbringen. Keine produktive Föderation oder Schutzrichtlinie für eine Übung global abschalten. Auch Notfallgeräte und Anmeldemittel benötigen Pflege.

PRIMAERQUELLEN / STAND 09.11.2026

Microsoft Learn: Manage emergency access accounts
learn.microsoft.com

Microsoft Learn: Create a resilient access control management strategy
learn.microsoft.com

NIST SP 800-34 Rev. 1: Contingency Planning Guide
nvlpubs.nist.gov