Maschinenidentitäten: Wer handelt ohne Benutzerkonto?

PRUEFEN. BELEGEN. NACHHALTEN.

Für einen abgegrenzten Dienst mit CI/CD, Cloud-Ressourcen und maschinellen API-Zugriffen. Richtwert: 90 Minuten für einen vorhandenen Dienstpfad; Migrationen und vollständige Inventarisierung zusätzlich. Entra-Begriffe sind Beispiele und müssen auf die eingesetzte Plattform übertragen werden.

Pruefbereich / Team:

Datum:

- [ ] **01 / Identität, technische Instanz, aufrufenden Workload und fachlichen Eigentümer verbinden; App-ID und tenantlokale Objekt-ID nicht verwechseln.**

  Nachweis: Inventar mit Zweck, Umgebung, Ressourcen, letzter belegter Nutzung und zuständiger Vertretung.

- [ ] **02 / Authentifizierung ohne selbst verwaltetes dauerhaftes Geheimnis für unterstützte Pfade bevorzugen; verbleibende Ausnahmen begründen.**

  Nachweis: Entscheidung zwischen Managed Identity, Workload-Föderation, Zertifikat und Secret einschließlich Betriebsabhängigkeiten.

- [ ] **03 / Bei föderierten Workloads den zulässigen Aussteller, Subject und Audience exakt an den freigegebenen Workflow binden.**

  Nachweis: Vertrauenskonfiguration und tatsächlich verwendete Claims; keine unbewertete Erweiterung auf andere Repositories oder Umgebungen.

- [ ] **04 / Effektive Rechte auf Kontroll- und Datenebene prüfen; zusätzliche Gruppen, Rollen und direkte Ressourcenfreigaben einbeziehen.**

  Nachweis: Aufgaben-Rechte-Matrix mit erfolgreichem Sollzugriff und verweigertem Zugriff außerhalb des Zwecks.

- [ ] **05 / Produktions- und Testidentitäten trennen und Wiederverwendung über unabhängige Anwendungen nur begründet zulassen.**

  Nachweis: Zuordnung der ausführenden Ressourcen zu Identitäten und geprüfte Trennung der erreichbaren Daten.

/ MAURISEC.DE

FIELD NOTES / CHECKLIST 16

☐ **06 / Wer Credentials, Föderationsregeln oder ausführbaren Workload ändern darf, als möglichen Nutzer der Maschinenidentität bewerten.**

Nachweis: Berechtigungsprüfung der App-Eigentümer, Deployment-Pipeline und verbundenen Rechenressourcen.

☐ **07 / Nutzung und Vertrauensänderungen überwachen; Token, private Schlüssel und Secrets aus Logs und Prüfbelegen heraushalten.**

Nachweis: Zuordenbare Anfrage mit Identitäts-ID und Ergebnis sowie Alarm für eine freigegebene Teständerung.

☐ **08 / Stilllegung und Notfallsperre mit abhängigen Diensten erproben; Rechteänderungen nicht mit sofortigem Tokenverlust gleichsetzen.**

Nachweis: Entzugsablauf, gemessene Wirklatenz, Restzugänge und Abschlussprüfung nach dem dokumentierten Cache- beziehungsweise Tokenfenster.

GEGENPROBE / AUTORISIERTE TESTUMGEBUNG

In der eigenen Testumgebung mit der tatsächlichen Test-Workload-Identität genau einen Lesezugriff auf eine benannte Dummy-Ressource außerhalb ihres erlaubten Bereichs versuchen. Bestehen: Die Ressource verweigert die Autorisierung und protokolliert die richtige Identität; ein Fehler durch DNS, fehlendes Objekt oder abgelaufenes Token genügt nicht.

GRENZEN UND VORAUSSETZUNGEN

Managed Identities entfernen die Secret-Verwaltung, nicht die Folgen eines kompromittierten Workloads. Benutzer-MFA schützt keine App-only-Anmeldung. Bei Managed Identities können Gruppen- oder Rollenänderungen wegen Caches erst nach Stunden wirksam werden. Plattform, Ressource und Tokentyp bestimmen die tatsächliche Entzugswirkung.

PRIMAERQUELLEN / STAND 09.11.2026

Microsoft Learn: Securing service principals
learn.microsoft.com

Microsoft Learn: Workload identity federation
learn.microsoft.com

Microsoft Learn: Federated identity credential considerations
learn.microsoft.com

Microsoft Learn: Managed identity best practice recommendations
learn.microsoft.com

OWASP: Non-Human Identities Top 10
owasp.org