Yardwork

KI-Agenten: Zugriffscheck

Aufgabe, Konto und wirksame Rechte zusammen prüfen. Entzug löscht keine schon gespeicherten Daten.

- [ ] **Verbindungen inventarisieren**
  Öffnen Sie die Einstellungen für Drittanbieter-Zugriff Ihres Kontos. Im Google-Konto ist das der Bereich für Drittanbieter-Apps und -Dienste, in Slack die Liste der installierten Apps des Workspace. Jede verbundene App wird mit ihren Scopes aufgeführt.

- [ ] **Die Scopes lesen, nicht den App-Namen**
  Ein Tool namens „Meeting-Notizen" kann drive.readonly halten. Vergleichen Sie jeden erteilten Scope mit dem, was das Tool für seine Aufgabe braucht.

- [ ] **Nach dem Konto fragen**
  Dokumentieren Sie Konto und Scopes zusammen. Ein eigenes Konto trennt die Arbeit, seine Rechte und Aktionsprotokolle müssen trotzdem geprüft werden.

- [ ] **Das Gate finden**
  Klären Sie, welche Aktionen unbeaufsichtigt laufen und welche eine Person erfordern. Lautet die Antwort „der Prompt sagt ihm, er soll es nicht tun", gibt es kein Gate.

- [ ] **Veraltetes entziehen**
  Entfernen Sie Verbindungen zu Tools, die nicht mehr genutzt werden. Ein Entzug stoppt künftigen Zugriff; er löscht keine bereits vorhandenen Daten. Fragen Sie danach getrennt.

- [ ] **Einen Wiedervorlagetermin setzen**
  Berechtigungen driften, wenn sich Workflows ändern. Eine für eine Aufgabe erteilte Verbindung überlebt diese Aufgabe meist.

Konkrete Rechte vergleichen

Recht	Zu prüfende Grenze
gmail.send	Senden ohne Postfachlesen
gmail.compose	Entwürfe verwalten und senden; kein allgemeiner Postfacheingang
drive.file	Angelegte oder per Dateiauswahl geteilte/geöffnete Dateien
Sites.Selected	Zustimmung und Ressourcenzuweisung; delegiert zusätzlich Nutzerrechte

Gmail/Drive-Kurznamen tragen normalerweise das Präfix https://www.googleapis.com/auth/. Prüfen Sie in Slack den Token-Typ; bei Microsoft delegierte und Anwendungsrechte separat.

Quellen

Gmail API - Choose Auth Scopes: https://developers.google.com/workspace/gmail/api/auth/scopes

Google Drive API - API-specific authorization: https://developers.google.com/workspace/drive/api/guides/api-specific-auth

Microsoft Graph permissions reference: https://learn.microsoft.com/en-us/graph/permissions-reference

Selected permissions: https://learn.microsoft.com/en-us/graph/permissions-selected-overview