WELT 8: ANDOCKSTATION · MISSION 8.4

Connectors mit Verstand: der Rechte-Basar

Mail-Butler, Noten-Turbo, Kalender-Planer 2.0: Am Rechte-Basar wird jedes Werkzeug angepriesen. Ihr Team entscheidet, wer an Bord darf – und mit welchen Rechten.

Zur Mission

DAUER 60 Min. KOSTEN Gratis mit Konto WERKZEUGE Claude Desktop, Claude (Web), MCP-Server, Papier und Stift DATENAMPEL Grün – unbedenklich

Das Wichtigste

- Connector = Fernzugriff auf einen Dienst (Kalender, Cloud …); Desktop-Erweiterung = lokales Programm mit Ihren Benutzerrechten.
- Vier Prüffragen: Welche Daten? Welche Aktionen (lesen, schreiben, löschen, senden)? Ausgang nach aussen? Herkunft?
- Gefährliche Kombination: private Daten + fremde Inhalte + Kanal nach aussen. Eine Zutat weglassen.
- Werkzeugbeschreibungen sind für die KI Anweisungen – seltsame Beschreibung = Werkzeug entfernen (Tool Poisoning).
- Updates neu prüfen: Neue Werkzeuge brauchen einen neuen Entscheid.
- Pro Chat nur einschalten, was nötig ist; «immer erlauben» nie für Senden, Löschen, Ändern; im Research-Modus Schreibwerkzeuge vorher aus.
- Gratisplan: Connectors und Erweiterungen enthalten, ein eigener Custom Connector; Schulkonten nur mit Erlaubnis der Schule.
- Inventar führen und Unbenutztes trennen: Customize → Connectors, Einstellungen → Desktop app → Extensions.

Ihr Produkt

Eine im Team erarbeitete **Connector-Regel für Ihre Fachschaft** (drei Sätze, die jede Kollegin versteht), eine ausgefüllte **Connector-Prüfkarte** für ein echtes Werkzeug und ein **Inventar** aller Connectors und Erweiterungen in Ihrem Claude – mit allem getrennt, was Sie nicht brauchen.

Abnahme: Ihr Team hat alle 12 Karten mit Begründung entschieden, mindestens den Wolf im Schafspelz (Karte 11) und das Rechte-Update (Karte 12) erkannt, Sie haben Ihre eigenen Connectors und Erweiterungen inventarisiert, und die Fachschaft hat eine Connector-Regel mit drei klaren Sätzen.

So gehen Sie vor

1. Wer reist schon mit? Das Bord-Inventar
2. Der Rechte-Basar: 12 Händler, 90 Sekunden
3. Zweitgutachten von Claude – und wer hat recht?
4. Ein echter Connector – mit Lupe statt Klick
5. Schalter, die schützen
6. Die Connector-Regel der Fachschaft

Start-Prompt

Du bist Fachperson für Informationssicherheit und Datenschutz an einer Schweizer Berufsfachschule.
Eine Lehrperson mit privatem Gratiskonto will folgendes KI-Werkzeug verbinden:
[KARTENTEXT EINFÜGEN, z. B. «Mail-Butler: liest alle Mails, erstellt Entwürfe, sendet und löscht Mails»]
Beurteile es nach: Daten (Personendaten?), Aktionen (lesen, schreiben, löschen, senden), Ausgang nach aussen, Herkunft.
Prüfe besonders, ob die Kombination aus privaten Daten, nicht vertrauenswürdigen Inhalten und einem Kanal nach aussen entsteht.
Urteil: JA, JA MIT AUFLAGEN (welche?) oder NEIN, mit Begründung in höchstens 6 Sätzen.
Schweizer Rechtschreibung (immer «ss», kein Eszett).

Qualitätscheck

- Jede der 12 Karten hat einen Entscheid mit Begründung, nicht nur ein Kreuz.
- Karte 11 (Werkzeugbeschreibung mit Anweisung) und Karte 12 (Rechte-Update) sind als Risiko erkannt.
- Ihr Inventar listet alle Connectors und Erweiterungen; Unbenutztes ist getrennt.
- Kein Schulkonto wurde ohne Erlaubnis der Schule verbunden, und kein Werkzeug zum Senden oder Löschen steht auf «immer erlauben».
- Die Connector-Regel hat höchstens drei Sätze und ist ohne Informatikwissen verständlich.

Hängen Sie fest? Frag die KI

Ich bin Lehrperson an einer Schweizer Berufsfachschule und nutze Claude (Desktop-App, Gratisplan). Erkläre mir einfach den Unterschied zwischen einem Connector, einem eigenen «Custom Connector» und einer Desktop-Erweiterung (.mcpb): Wo läuft was, wer sieht welche Daten, und wo finde ich in den Einstellungen eine Übersicht, um nicht mehr Gebrauchtes zu trennen? Nenne die offiziellen Hilfeseiten von Anthropic als Suchbegriffe und markiere, was sich häufig ändert.

Klappt nicht? Der Rechte-Basar funktioniert komplett auf Papier, ohne Konto und ohne Installation. Die Schritte mit Claude gehen auch in jeder anderen Gratis-KI (ChatGPT, Gemini, Copilot): Kartentext einfügen und begutachten lassen. Den Blick in die eigenen Connector-Einstellungen machen Sie auf claude.ai im Browser.

Stand 19.11.2026 · CC BY 4.0 Alpasana GmbH · Werkzeuge ändern sich – prüfen Sie selbst.