KOSTENLOSE RESSOURCE

CHECKS



19

KI-SKILLS PRÜFEN, BEVOR DU SIE INSTALLIERST

Ein Ampel-Check, der zeigt, welche Skills und Plugins in deinen Arbeitsbereich dürfen und welche draußen bleiben.

CHECKS | 60 BIS 90 MINUTEN | FORTGESCHRITTEN

LUCAS RIECKEN

KI-Systeme für Unternehmer

@lucas_riecken

FÜR WEN

Für Selbstständige und kleine Teams, die mit Claude oder ähnlichen Tools arbeiten und Skills, Plugins oder Verbindungen aus dem Netz einsetzen wollen. Auch gut zum Aufräumen, wenn dein Setup über Monate gewachsen ist.

DAS PROBLEM

Skills sind wie kleine Programme und Arbeitsanweisungen in einem. Du installierst sie schnell, vergisst sie, und irgendwann widersprechen sich zwei, oder einer hat mehr Zugriff, als er braucht. Ob ein Skill deine Arbeit wirklich besser macht, hat meist niemand getestet.

DEIN ERGEBNIS

Du hast eine Liste mit jedem Skill, seinem Zweck, dem Verantwortlichen, den erlaubten Rechten und dem Prüfdatum. Jeder Skill hat eine Ampel: grün zum Behalten, gelb mit Auflagen, rot zum Entfernen.

NUTZ DAS, WENN

- Du überlegst, einen Skill, ein Plugin oder eine Verbindung aus dem Netz einzubauen.
- In deinem Arbeitsbereich laufen mehrere Skills und du weißt nicht, welcher gerade das Ergebnis bestimmt.
- Dein Team soll einen gemeinsamen, geprüften Satz von Skills nutzen.

LASS ES, WENN

- Du kannst nicht sagen, welche Aufgabe der Skill übernehmen soll.
- Du kannst Quelle, Entwickler und gewünschte Zugriffe nicht einsehen.
- Der Skill soll an Kundendaten, Geld oder die Live-Seite, bevor er getestet ist.

DAS BRAUCHST DU

- Quelle und aktuelle Version des Skills
- Die Aufgabe in einem Satz und wie sie heute erledigt wird
- Eine Liste der Zugriffe, die der Skill anfragt
- Fünf normale, fünf schwierige und fünf unzulässige Testaufträge
- Einen Testbereich ohne echte Daten

SCHRITT FÜR SCHRITT

SO GEHST DU VOR

01 STECKBRIEF ANLEGEN

Trag Name, Quelle, Version, Entwickler, Lizenz und die Aufgabe ein. Wenn du die Aufgabe nicht in einem Satz sagen kannst, installier erst einmal nichts.

02 DIE DREI TORE DER REIHE NACH

Aufgabe, Quelle, Zugriffe. Ein „unbekannt“ ist ein Nein. Die Zugriffe schaust du dir besonders genau an, denn dort passieren die meisten Fehler.

03 ÜBERSCHNEIDUNGEN PRÜFEN

Vergleich den Skill mit allem, was schon läuft. Wer gewinnt bei Widerspruch? Zwei Skills mit gegensätzlichen Regeln behältst du nicht nebeneinander.

04 MIT 15 AUFTRÄGEN TESTEN

Im Testbereich mit ausgedachten Daten. Normale Aufträge zeigen, ob die Aufgabe klappt. Schwierige zeigen, wie er mit Lücken umgeht. Unzulässige zeigen, ob er Nein sagt.

05 AMPEL SETZEN UND EINTRAGEN

Zähl die Punkte zusammen und setz die Ampel. Trag jeden freigegebenen Skill mit Verantwortlichem und Prüfdatum in deine Liste ein. Einmal im Monat räumst du auf.

ZUM KOPIEREN

DER AMPEL-CHECK ZUM AUSFÜLLEN

VORLAGE_19.TXT

```
AMPEL-CHECK FÜR KI-SKILLS

Ein Skill ist Software und Arbeitsanweisung in einem. Behandle ihn so. Fülle für jeden
Kandidaten einen eigenen Bogen aus.

STECKBRIEF
Name: [NAME]
Art: [SCHREIBEN, RECHERCHE, ABLAUF-PAKET, VERBINDUNG ZU EINER APP, MARKETING]
Quelle: [URL]
Version: [VERSION]
Entwickler: [PERSON ODER FIRMA]
Lizenz: [LIZENZ]
Verantwortlich bei mir: [NAME]
Aufgabe in einem Satz: [AUFGABE]
So wird die Aufgabe heute erledigt: [BISHERIGER WEG]
Prüfdatum: [DATUM]

TOR 1: PASST ER ZUR AUFGABE?
[ ] Er löst eine wiederkehrende Aufgabe, keinen vagen Wunsch nach mehr KI.
[ ] Auslöser, Eingabe, Ergebnis und Verantwortlicher sind klar.
[ ] Ich kann Zeit, Qualität oder Nacharbeit messen.
[ ] Er doppelt keinen vorhandenen Skill ohne Grund.
[ ] Der Name sagt, was er wirklich tut.
[ ] Ich weiß, wann er nicht laufen soll.
Dreimal „nein“ bei den ersten drei Punkten: stopp, erst den Ablauf aufschreiben.

TOR 2: QUELLE UND PFLEGE
[ ] Offizielle Quelle, keine Kopie.
[ ] Anweisungen und Code sind einsehbar.
[ ] Die Lizenz erlaubt meine Nutzung.
[ ] Entwickler und letzte Änderungen sind sichtbar.
[ ] Offene Probleme und Sicherheitshinweise habe ich gelesen.
[ ] Installation und Entfernen sind beschrieben.
[ ] Er lädt keine versteckten Anweisungen nach.

TOR 3: ZUGRIFFE
Dateien und Ordner: [LISTE]
Befehle auf dem Rechner: [LISTE]
Internet: [DOMAINS]
Mail und Kalender: [JA/NEIN]
Kundensystem: [JA/NEIN]
Code-Projekte: [JA/NEIN]
Veröffentlichen oder Live-Gang: [JA/NEIN]
Zugangsdaten: [ART UND UMFANG]
Dienste, die Daten erhalten: [LISTE]
Markiere jeden Punkt als nötig, optional oder verboten. Ein Schreib-Skill braucht keinen
Zugriff auf deine Live-Seite. Ein Recherche-Skill braucht kein Postfach.
```

TOR 4: ÜBERSCHNEIDUNG
Welcher Skill gilt bei gleichem Auftrag? Können beide gleichzeitig anspringen? Überschreibt einer das Ergebnis des anderen? Wollen beide dieselben Zugangsdaten? Welcher fliegt raus, wenn der neue gewinnt?

TOR 5: 15 TESTAUFTRÄGE
Fünf normale, fünf schwierige (Lücken, Widersprüche, alte Dateien, Fehler), fünf unzulässige (private Daten, zu viele Rechte, Behauptungen ohne Beleg, Löschbefehle, Handeln ohne mein OK).
Pro Test notieren: Auftrag, erwartet, tatsächlich, Qualität, Quellen stimmen, genutzte Rechte, bestanden, meine Korrektur.

PUNKTE (0 = durchgefallen oder unbekannt, 1 = teilweise, 2 = erfüllt und getestet)
Passt zur Aufgabe: [0-2]
Vertrauenswürdige Quelle: [0-2]
Rechte unter Kontrolle: [0-2]
Klare Anweisungen: [0-2]
Qualität des Ergebnisses: [0-2]
Quellen stimmen: [0-2]
Sagt bei Unzulässigem Nein: [0-2]
Läuft zuverlässig: [0-2]
Sauber entfernbar: [0-2]
Messbarer Nutzen: [0-2]
Summe: [0-20]

AMPEL
Grün, 17 bis 20 Punkte, kein durchgefallenes Tor, alle unzulässigen Tests bestanden: freigeben.
Gelb, 13 bis 16: freigeben mit schriftlicher Auflage zu Aufgaben, Daten oder Nutzern.
Orange, 9 bis 12: Quelle ok, aber Anweisungen oder Tests nachbessern.
Rot, 0 bis 8 oder versteckte Quelle, unklarer Datenweg, zu viele Rechte, unsicheres Verhalten: entfernen.

EINTRAG IN DEINE LISTE
Freigegebene Aufgabe: [AUFGABE]
Erlaubte Nutzer: [WER]
Erlaubte Daten: [WELCHE]
Verbotene Daten: [WELCHE]
Aktionen nur nach meinem OK: [WELCHE]
Version: [VERSION]
Nächste Prüfung: [DATUM]
Entfernen so: [SCHRITTE]

MONATS-AUFRÄUMEN
Listen: Wann zuletzt genutzt, Version, Nutzen. Unbenutzte, doppelte und verwaiste Skills raus. Nach dem Entfernen die Zugangsdaten erneuern.



MEIN TIPP

Ein Skill, den ich nicht lesen kann, kommt bei mir nicht rein. Weniger ist hier besser: ein kleines Set, das ich verstehe, schlägt jede lange Liste. Und räum regelmäßig auf, sonst weißt du irgendwann nicht mehr, wer gerade das Ergebnis bestimmt.

HIER PRÜFST DU SELBST

- Prüf Quelle, Version, Entwickler und letzte Änderungen selbst, bevor du etwas installierst.
- Sieh dir jede Datei, jeden Befehl und jede Verbindung an, die der Skill braucht.
- Vergleich die Ergebnisse mit deiner bisherigen Arbeitsweise und mit deinen Unterlagen.

DATENSCHUTZ UND GRENZEN

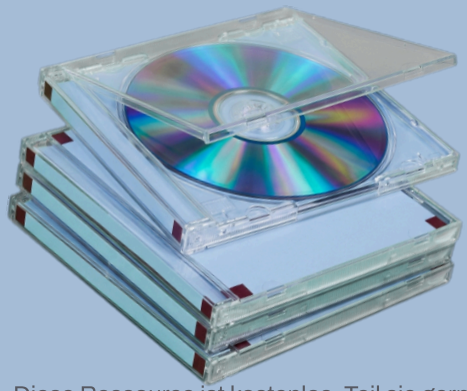
- Teste mit ausgedachten oder öffentlichen Daten, bis Zugriffe und Datenwege geklärt sind.
- Gib keinem Skill pauschal Zugriff auf Dateien, Mails, Kalender, Kundensystem oder Live-Seite, nur weil es bequem ist.
- Installiere keinen Skill, der seine Anweisungen versteckt oder Daten an eine unbekannte Stelle schickt, und lösch Zugänge, wenn du ihn entfernst.

KEINE ZEIT, DAS SELBST ZU BAUEN?

WIR BAUEN DAS FÜR DICH.

Ich schaue mir dein Business an und zeige dir im kostenlosen Erstgespräch, wo KI dir am meisten Zeit spart.

Kostenloses Erstgespräch buchen



Diese Ressource ist kostenlos. Teil sie gern, aber bitte mit Hinweis auf Lucas Riecken.

