Shadow AI & Copilot Oversharing

Wie Verwaltungen KI-Nutzung sichtbar, steuerbar und sicher machen

Philipp Hunold, isolutions AG | Cloud and Workplace Day 2026

isolutions

Shadow AI

KI-Nutzung, die niemand freigegeben hat

1 Was das Problem ist

2 Was wir in der Praxis sehen

3 Was wir empfehlen

isolutions

1 · DAS PROBLEM

Gleiche Bedrohungen, neue Physik

Schatten-IT

Ungeprüfte Werkzeuge

Nicht freigegebene Apps und Dienste.

Shadow AI

Versteckte Produktivität

Nicht freigegebene KI-Nutzung: Einfügen, Hochladen, und Verbindungen, die mit dem Arbeitskonto bestehen bleiben.

Der Antrieb ist unverändert: der offizielle Weg war zu langsam. Neu sind Tempo, Reichweite und ein Zugriff, der weiterläuft, wenn längst niemand mehr hinschaut.

Angreifer setzen KI von aussen ein, Ihre Organisation von innen. Beide Wege laufen über Identitäten.

1 · DAS PROBLEM

Drei Fragen, die den Zustand zeigen

1. Wissen Sie, welche KI-Werkzeuge bei Ihnen genutzt werden – und mit welchen Daten?

2. Gibt es verbindliche Regeln, wie KI im Arbeitsalltag eingesetzt werden darf?

3. Ist geregelt, wer eine KI-Anwendung freigibt und wer dafür geradesteht?

2 · WAS WIR SEHEN

Eine Beispiel-Auswertung (30 Tage)

~60
KI-Apps im Einsatz

10
davon offiziell freigegeben

~150
Personen mit KI-Traffic

~1'000
Geräte mit KI-Traffic

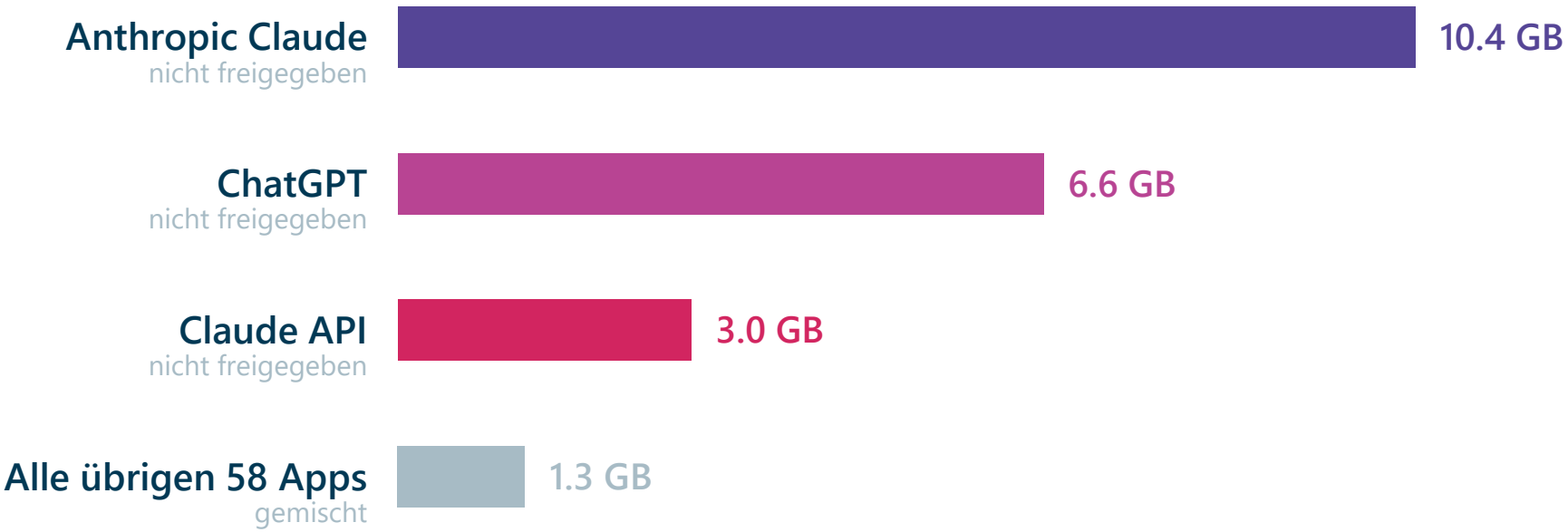
21 GB
ausgehender KI-Traffic

89%
der Apps nie geprüft

Die IT dieser Organisation hatte mit 10 bis 15 Personen gerechnet.
30 Tage – Kleinere Finanzdienstleistung

2 · WAS WIR SEHEN

Drei Anwendungen, 89 Prozent des Volumens



Die meistgenutzte Anwendung war nicht die, über die alle reden. Wer nur ChatGPT sperrt, hat zwei Drittel des Volumens nicht angefasst.

2 · WAS WIR SEHEN

Warum bisher niemand Alarm geschlagen hat

Der Traffic ist unauffällig	Eine verschlüsselte Verbindung zu einer Website unter tausenden pro Tag.
Monitoring schaut auf Bekanntes	Überwacht wird, was freigegeben wurde. Der Rest fällt aus dem Raster.
Gerät und Konto sind entkoppelt	Privates Konto auf verwaltetem Gerät. Oder verwaltetes Konto auf privatem Gerät.
«Entfernen» ist nicht «Entziehen»	Wer eine App aus seiner Oberfläche löscht, widerruft nicht die Zustimmung im Verzeichnis. Der Zugriff bleibt.

Sie können nicht entziehen, was Sie nie erteilt zu haben glaubten.

isolutions

3 · UNSERE EMPFEHLUNG

Erkennen, regeln, schützen, überwachen

1

Erkennen

Auswertung aus Logs oder Endpoint Detection Response (EDR).

Ergebnis: die genutzten Werkzeuge, nach Risiko sortiert.

2

Regeln

Welche Daten dürfen in KI-Werkzeuge? Wer gibt frei, in welcher Frist? Eine Seite, nicht vierzig.

Ergebnis: eine Regel, die man auswendig sagen kann.

3

Schützen

Klassifizierung auf Inhaltsebene, Regeln für Zustimmungen, und ein offizieller Weg, der schneller ist als der inoffizielle.

Ergebnis: die Regel gilt auch dann, wenn niemand hinschaut.

4

Überwachen

Neue Apps, auffällige Muster, Regelverstösse. Fester Rhythmus, definierter Ablauf für den Ernstfall.

Ergebnis: Sie erfahren es im Review, nicht aus einer Medienanfrage.

Für die Verwaltung zusätzlich: Amtsgeheimnis, kantonales Datenschutzrecht und Beschaffung. Ein Werkzeug, das niemand beschafft hat, hat auch niemand geprüft.

isolutions

Copilot Oversharing

Was ein freigegebener Assistent auf Ihren eigenen Ablagen findet

1 Was das Problem ist

2 Was wir in der Praxis sehen

3 Was wir empfehlen

isolutions

TEIL 2 · COPILOT OVERSHARING

1 · DAS PROBLEM

Der M365 Copilot erbt Ihre Berechtigungen

> **Er umgeht keine Berechtigung. Er nutzt sie zum ersten Mal vollständig aus.**

Was sich ändert	Was gleich bleibt
Suchen dauert Sekunden statt Stunden.	Die Berechtigungen sind unverändert.
Inhalte werden zusammengefasst und weiterverwendet.	Kein Konto sieht mehr als vorher.
Was schwer auffindbar war, steht in der Antwort.	Es entsteht keine neue Freigabe.

Das Oversharing ist nicht neu. Neu ist, wie einfach die Abfrage wird.

isolutions

1 · DAS PROBLEM

Wie ein Oversharing-Problem entsteht

«Jeder ausser externe Benutzer» EEEU

Eine Security-Gruppe, die automatisch alle internen Mitarbeiter beinhaltet, aber nicht externe Gäste ausschliesst um Dokumente schnell mit dem gesamten Unternehmen zu teilen.

Gebrochene Vererbung

Jemand vergibt einmalig eigene Rechte auf einer Bibliothek oder einem Ordner. Ab dann wirkt keine Korrektur auf Site-Ebene mehr dort.

Provisionierung ohne Vorgaben

Teams und Sites entstehen ohne Klassifizierung, ohne Freigaberegel und ohne benannte Verantwortlichkeiten.

Freigabelinks ohne Ablauf

«Alle in der Organisation» einmal erzeugt, unbefristet gültig, in Chats und Mails weitergereicht.

Verwaiste und inaktive Sites

Der Eigentümer hat die Organisation verlassen. Niemand entfernt Rechte, niemand archiviert – durchsuchbar bleibt alles.

Migrationen vom Fileserver

Berechtigungen wurden pauschal übernommen, nach dem Muster «erst mal alle rein, aufräumen später».

Jede dieser Ursachen ist harmlos für sich. Über zehn Jahre summieren sie sich zu einer Ablage, die niemand mehr überblickt.

isolutions

2 · WAS WIR SEHEN

Herausforderungen in langjährig genutzten Microsoft-Umgebungen

«Bei uns ist alles sauber berechtigt.»

Die Berechtigungen waren beim Anlegen korrekt. Seither sind zehn Jahre vergangen, Teams sind gewachsen, Leute haben gewechselt, Projekte wurden geteilt.

Ohne wiederkehrende Überprüfung ist «einmal korrekt» kein Zustand, sondern ein Datum.

«Das sind nur ein paar alte Sites.»

Inaktive Sites sind für die Suche genauso sichtbar wie aktive. Alter macht Inhalte nicht unsichtbar, es macht nur, dass niemand mehr hinschaut.

Verwaiste Sites ohne Eigentümerschaft sind der zweithäufigste Befund.

«Wir haben doch migriert.»

Migrationen sind die häufigste Ursache, nicht die Lösung. Berechtigungen wurden pauschal übernommen, weil der Umzug sonst nicht fertig geworden wäre.

Wer migriert hat und nie nachbereinigt, hat das Problem mitgenommen.

Erfahrungswert: Wer Zugriffe auf Sites und Teams nie regelmässig überprüft hat, hat mit hoher Wahrscheinlichkeit ein Oversharing-Problem. Die Frage ist nicht ob, sondern wo.

2 · WAS WIR SEHEN

Der Test, der eine halbe Stunde kostet

> Setzen Sie sich mit dem Konto einer normalen Sachbearbeiterin hin – nicht mit einem Administratorkonto – und suchen Sie nach «Lohn», «Kündigung», «vertraulich», «Strafanzeige».

Was dabei zurückkommt, findet ein Assistent auch. Nur schneller, und ohne dass jemand danach fragen muss.

Wenn das Ergebnis unangenehm ist, haben Sie kein KI-Problem. Sie haben ein Berechtigungsproblem, das Sie ab heute kennen.

isolutions

3 · UNSERE EMPFEHLUNG

Zuerst eindämmen, dann aufräumen

Eindämmen

Tage

Heikle Sites von der Auffindbarkeit durch den Assistenten ausnehmen. Klassifizierte Inhalte von der Verarbeitung ausschliessen. Danach prüfen, dass nichts Eingeschränktes mehr in Antworten auftaucht.

Aufräumen

Wochen bis Monate

Zugriffsprüfungen durch die Eigentümer: organisationsweite Gruppen und Links entfernen, gebrochene Vererbung reparieren, Eigentümerschaft zuweisen. Danach die Notbremse Site für Site lösen.

Standard setzen

dauerhaft

Eingeschränkter Zugriff als Voreinstellung für geschäftskritische Sites. Organisationsweite Freigabegruppen und offene Links abschalten. Klassifizierung beim Anlegen erzwingen.

Die Reihenfolge ist der ganze Trick. Wer mit dem Aufräumen beginnt, bleibt so lange offen, wie das Aufräumen dauert.

Vorgehen analog dem Microsoft-Leitfaden zur Absicherung von M365 Copilot, Stand März 2026.

isolutions

3 · UNSERE EMPFEHLUNG

Sieben Stellschrauben, die es bereits gibt

Eindämmen

wirkt sofort, ändert keine Rechte

Eingeschränkte Suche

Suche und Assistent auf freigegebene Sites begrenzen.

Restricted SharePoint Search

Sites verbergen

Einzelne Sites ausnehmen, ohne Rechte zu ändern.

Restricted Content Discovery

Klassifizierung und DLP

Sensitiv gekennzeichnete Inhalte mittels DLP gezielt von Copilot ausschliessen.

Microsoft Purview

Aufräumen

findet und bereinigt Befunde

Zugriffsberichte

Überteilte und sensible Sites systematisch finden.

Data Access Governance Reports

Inaktive Sites

Inaktive Sites erkennen, Eigentümer zur Bestätigung auffordern, def. Folgeaktionen auslösen.

Inactive Site Policy

Standard setzen

gilt dauerhaft, auch für Neues

Freigabekontrollen

Links für bestimmte Personen, Freigaben je Site begrenzen.

SharePoint Built-in Controls

Eingeschränkter Zugriff

Zugriff auf Gruppen begrenzen, überschreibt frühere Rechte.

Restricted Access Control

Keine dieser Stellschrauben verlangt ein neues Berechtigungsmodell.

Oversharing-Kontrollen für M365 Copilot, Microsoft Learn, Stand März 2026.

isolutions

3 · UNSERE EMPFEHLUNG

Nachweisbarkeit sichern, Wirkung überprüfen

Nachweisbarkeit

- Aufbewahrungsfrist für Interaktionen festlegen, abgestimmt auf Archivrecht und interne Vorgaben
- Auffindbarkeit für Audit, Aufsicht und Rechtsbegehren sicherstellen
- Inaktive und veraltete Inhalte archivieren, damit sie nicht mehr in Antworten auftauchen

Laufender Betrieb

- Auswerten, welche sensiblen Daten der Assistent tatsächlich berührt
- Neue Oversharing-Quellen erkennen, bevor sie sich einnisten
- Einschränkungen zurücknehmen, sobald eine Site bereinigt ist

Verfahrensrelevante KI-Interaktionen können akten- und nachweispflichtig sein. Aufbewahrung und Auffindbarkeit sind organisationsspezifisch zu regeln.

isolutions

ZUM WEITERDISKUTIEREN

Anregungen

TEIL 1

Wissen Sie, welche KI-Werkzeuge bei Ihnen laufen – oder wissen Sie, welche Sie erlaubt haben?

TEIL 2

Wann wurden die Zugriffe auf Ihre Sites und Teams zuletzt systematisch überprüft?

Wenn Sie auf die letzte Frage eine Antwort haben, fangen Sie dort an.

isolutions

Danke.

Ich vergleiche gerne Erfahrungen – auch ohne Projekt dahinter.

Philipp Hunold | Senior Security Consultant, Cloud Services | isolutions AG

linkedin.com/in/phunold