

MICROSOFT 365 COPILOT

Mehr Sicherheit durch Copilot

- ▶ Copilot-Architektur & Integration im Unternehmen
- ▶ Sicherheit & Compliance mit Microsoft Purview
- ▶ Praxisnahe SharePoint & Dokumentenverwaltung



Über den Autor

Aaron Siller

Als ich 2014 als IT-Dienstleister startete, stand ich vor denselben Herausforderungen, mit denen heute viele meiner Kunden zu mir kommen: Komplexe Microsoft-Systeme, ständig neue Security-Anforderungen und nie genug Zeit, um alles richtig zu konfigurieren.

Was als klassische IT-Beratung begann, entwickelte sich schnell zu einer klaren Mission: **Microsoft 365**

Umgebungen sicherer machen, ohne dass Admins dafür Wochenenden opfern müssen.



Heute werde ich von führenden Instituten wie der Heise Academy und Golem Karrierewelt als Trainer für Microsoft 365 Security eingesetzt. Meine Expertise bestätigt sich in der Zusammenarbeit mit Unternehmen vom handwerklichen Mittelstand bis hin zu internationalen Konzernen. Schau Dir gerne meine Referenzen auf meiner Website an.

 E-MAIL aaron@siller.consulting

 WEBSITE siller.consulting

 LINKEDIN [Aaron-Siller](#)

 YOUTUBE [Aaron-Siller-YT](#)

Inhaltsverzeichnis

Microsoft 365 Copilot Architektur	9
Grounding dem Microsoft Graph: Informationsgrundlage.....	10
Datenquellen: OneDrive und Freigaben	10
Technischer Rahmen: Microsoft 365 Copilot Umgebung	10
Dokumentenklassifizierung & Output	11
Rechenzentrums-Fallback & Datenverarbeitung	11
Prompt-Verarbeitung & Architektur	12
Data-at-Rest vs. Data-in-Transit	13
Taxonomie und standardisierte Dokumentenbenennung	14
Rollen im Datenmanagement: Data Stewards und Data Guards.....	14
Indexierung der Zugriffe und Berechtigungen	15
Struktur des semantischen Index.....	15
Tenant-Level Semantischer Index	16
User-Level Semantischer Index.....	17
Validierung und Ablauf von Gastzugriffen	17
Synchronisierung und Indexierung von Berechtigungen	17
Connected Experiences.....	18
Copilot und Sharepoint-Daten zum Antworten	19
Navigation im Microsoft 365 Admin Center	20
Übersicht über SharePoint-Sites	21
Organisationseinstellungen im Admin Center	22
Berichte und Pseudonymisierung in Copilot.....	24
Self-Service-Testversionen und -Käufe.....	26
Empfohlene Einstellungen für Self-Service	27
Konfiguration von SharePoint-Freigaben	28
Risiken durch Jeder-Links	29
Microsoft 365 Installation und Risiken.....	30
Microsoft 365 Installation und Risiken.....	31

Lizenzmodell und Installationsanzahl	32
Gerätekontrolle durch Intune und Conditional Access	33
Speicherlimits Einstellungen	34
Speicherzuteilung: Automatisch vs. Manuell.....	36
Versionierung und Speichernutzung.....	37
OneDrive: Speichergrenzen verstehen und steuern	39
Zugriffsvalidierung und OneDrive-Synchronisation	39
SharePoint, OneDrive und erweiterte Ansichten.....	41
Optionen zur externen Freigabe	43
Interne und externe Freigaben steuern	45
Jeder-Link und Copilot-Auswirkungen	45
Zugriffssteuerung und Conditional Access.....	46
Verknüpfung und Speicherverbrauch	47
Zugriffsmanagement in der Praxis	48
Seitenaufrufe und Aktivitätsdaten verstehen	49
Bewertung von Anzeigefehlern und Datenlücken	50
Beliebteste geteilte Webseiten	50
Erweiterte Verwaltung und Berichterstattung.....	51
Berichte zur Datenzugriffs-Governance und Linknutzung	52
Interne Freigabe und Copilot-Indexierung.....	54
Side Lifecycle Management und Site Level Access Restriction	54
Inactive Site Policy und Berichtserstellung	55
Site Ownership Policies und Berichtserstellung.....	59
Änderungen nachvollziehen und SharePoint-Aktivitäten überwachen.....	61
Überwachung durchgeführter Änderungen	62
Unterstützung durch AI Insights.....	63
Regelmäßige Kontrolle der Nutzeraktivität.....	64
Weitere Änderungen im Admin Center nachvollziehen	65
Site Level Access Restriction unter Access Control aktivieren.....	66

Gastzugriffe in Entra ID und Microsoft Teams verwalten	72
Regelungen zum Einladen von Gästen in Teams.....	73
Automatisierung und Gastzugriffsverwaltung	73
Wirkung und Anwendungsbereiche.....	79
Erstellung von Sicherheitsgruppen einschränken.....	80
Erstellung von Microsoft 365 Gruppen zentral steuern.....	80
Ablaufsteuerung für Microsoft 365 Gruppen aktivieren	81
Beispielansicht für Zugriffsüberprüfungen	82
App-Zugriffe im Bereich „Enterprise Applications“ steuern	83
Ungenutzte Anwendungen finden und verwalten.....	84
Cloud Discovery zur Erkennung von Schatten-IT nutzen	86
Konfiguration von Conditional Access für Copilot	87
Enterprise Copilot als Zielressource sichtbar machen	88
Empfohlene Richtlinien zur praktischen Umsetzung mit Copilot	90
Any-Any-Richtlinie mit Ausschluss des Break-Glass-Accounts.....	90
Benutzer- und Anmelderisiko im CA richtig konfigurieren	92
Zugriff nach Geräteplattformen steuern	93
Zugriff auf Copilot nach Land oder IP gezielt einschränken.....	94
Absicherung mit modernen MFA-Methoden.....	96
Anmeldehäufigkeit zur erneuten Authentifizierung definieren	98
Copilot im Admin Center vorbereiten.....	99
SharePoint Search: Suchergebnisse gezielt einschränken	99
Nutzung des Nachrichtencenters für Microsoft 365 Updates	105
Richtliniensteuerung für Microsoft Copilot in der Office-Suite	106
Dokumentenerstellung durch Copilot.....	109
Sichtbarkeit des Copilot-Buttons steuern	110
Copilot Agents: Auswahl, Sicherheit und Datenschutz.....	111
Datensicherheit und Compliance im Microsoft Purview Portal.....	112
Automatische Bildgenerierung aktiviert lassen	113

Copilot in Microsoft Teams-Besprechungen	114
Aufzeichnungsrichtlinien separat verwalten	115
Copilot in Microsoft Edge und Office	116
Connected Experiences als technische Voraussetzung	116
Konfigurationen im Compliance-Portal.....	117
Datensicherheit mit Microsoft Purview und DSPM for AI	117
Information Barriers in Microsoft Purview	118
Alternative: Granulare Steuerung mit Sensitivity Labels	119
Schwellwerte richtig definieren	130
Zuweisung und Veröffentlichung von Labels	133
Einsatz von eDiscovery zur Analyse digitaler Aktivitäten.....	135
Compliance-Prüfung vor dem Einsatz.....	139
IT-Tasks: Microsoft 365 Umgebung vorbereiten	139
Risikominimierung und Optimierung in Sharepoint	140
Optimierung der SharePoint-Sicherheit und -Verwaltung.....	140
Strukturierung und Datenhygiene in Microsoft 365	140
Datenrichtlinien, Verantwortlichkeiten und Audits	140
Effektive Zugriffs- und Validierungsprozesse	141
"Just Enough Access" mit Microsoft Purview und Entra.....	141
Zuweisung der Microsoft 365 Copilot Lizenz	141
Definierung und Erstellung von Copilot Agents	142

Einleitung

Microsoft 365 Copilot ist ein starkes Tool, sofern die technischen Grundlagen klar definiert und die organisatorischen Weichen richtig gestellt sind.

Dieser Leitfaden zeigt, wie Unternehmen ihre Microsoft-365-Umgebung auf Copilot vorbereiten – mit einem starken Fokus auf Sicherheit, Struktur und Compliance.

Denn klar ist: Der Einsatz von KI in produktiven Systemen funktioniert nicht ohne Ordnung. Was oft fehlt, sind verbindliche Datenrichtlinien, saubere Berechtigungskonzepte und eine klar strukturierte Informationsarchitektur.

Das Problem?

Copilot wirkt auf den ersten Blick einfach – eine Leiste in Word, ein Fenster in Teams. Die dahinterliegende Technik greift aber tief in Ihre Infrastruktur ein: Berechtigungen, Indizes, Klassifizierungen und auch Sicherheitsrichtlinien müssen stimmen. Wird das ignoriert, sind Datenschutzpannen und Fehlinformationen vorprogrammiert.

Mit diesem Leitfaden schaffe ich Klarheit.

In den folgenden Kapiteln erfahren Sie unter anderem:

- wie die Copilot-Architektur funktioniert und welche Datenquellen genutzt werden.
- wie Sie Dokumente klassifizieren und Zugriffe sicher verwalten.
- wie Sie den semantischen Index strukturieren und SharePoint-Daten gezielt bereitstellen.
- wie Sie Conditional Access, MFA und Gerätezugriffe für Copilot absichern.
- wie Sie mit Compliance-Richtlinien und Sensitivity Labels den Überblick über Ihre Daten behalten.

Besonders wichtig?

Microsoft 365 erfordert einen **ganzheitlichen** Sicherheitsansatz.

Copilot ist keine einfache App. Es handelt sich um einen Dienst, der auf die bestehende Microsoft-365-Struktur aufsetzt – und sie spiegelt. Wer unstrukturierte, ungesicherte Daten verwaltet, erhält unstrukturierte, unsichere Antworten.

Unser Fokus liegt daher auf technischer Vorbereitung, sicherer Bereitstellung und praxisnahen Empfehlungen. Sie erfahren nicht nur, welche Stellschrauben wichtig sind – sondern auch, wo und wie Sie sie konfigurieren.

Legen wir los!

Microsoft 365 Copilot Architektur

Microsoft 365 Copilot nutzt Daten aus dem Microsoft Graph, OneDrive und SharePoint, verarbeitet sie innerhalb deutscher Rechenzentren und liefert Antworten über einen semantischen Index.

Microsoft 365 Copilot bewegt sich innerhalb der **Microsoft 365 Service Boundary**. Diese Service Boundary beschreibt, in welchen Rechenzentren und in welchen Services wir unterwegs sind.



Abbildung 001

(Quelle: <https://www.redeszone.net/app/uploads-redeszone.net/2025/02/copilot-1.jpg>)

Für die optimale Nutzung dieses eBooks und Microsoft 365 Copilot ist es entscheidend zu verstehen, dass wir uns in einem deutschen Tenant bewegen. Das bedeutet konkret: Die Datenbasis, das sogenannte **Grounding**, auf der Microsoft 365 Copilot alle Informationen stützt, wird primär aus dem *Microsoft Graph* des Rechenzentrums in Frankfurt und sekundär aus dem Rechenzentrum in Berlin bezogen.

Grounding dem Microsoft Graph: Informationsgrundlage

Microsoft Graph spielt eine zentrale, wenngleich indirekte Rolle beim Grounding. Copilot sammelt über Graph relevante Informationen aus verschiedenen **Microsoft 365 Online-Diensten**. Dazu gehören nicht nur das primäre Exchange-Postfach, sondern auch freigegebene Postfächer und andere zugängliche Datenquellen.

Diese Informationen bilden die Grundlage für die Antworten und Aktionen von Copilot.

Tipp: Graph selbst speichert keine Daten, sondern ermöglicht lediglich den Zugriff.

Datenquellen: OneDrive und Freigaben

Um die volle Leistungsfähigkeit von Microsoft 365 Copilot auszuschöpfen, greifen wir auf eine breite Datenbasis zu. Das umfasst alle Informationen aus unserem OneDrive; entsprechend unsere eigenen Dateien als auch Freigaben von anderen.

Ebenso werden unsere Microsoft Teams-Daten einbezogen: sämtliche Inhalte aus Kanälen – seien es öffentliche, private oder geteilte –, die zugehörigen SharePoint-Seiten und Chats, bestehend aus Einzel- und Gruppenchats.

Hinzu kommen alle Inhalte, die in unserem SharePoint Online gespeichert sind. Sobald wir eine **Microsoft 365 Copilot-Lizenz** aktivieren, beginnt dieser Prozess.

Microsoft Graph dient dabei als Schnittstelle, um Daten zu erfassen und dem **Azure OpenAI-Modell** zur Verfügung zu stellen. Dieses Modell, eine speziell für Microsoft angepasste Version des öffentlichen OpenAI, lernt so im Large-Language-Model, welche Antworten auf unsere Anfragen am besten passen. Es analysiert die gesammelten Informationen, um uns relevante und hilfreiche Antworten auf unsere Prompts zu liefern.

Technischer Rahmen: Microsoft 365 Copilot Umgebung

Sobald wir die Copilot-Lizenz aktivieren, werden alle unsere Inhalte in einen **semantischen Index** überführt. Das bedeutet, Copilot bewegt sich innerhalb dieser Service Boundary und analysiert alles, worauf wir Zugriff haben – und das innerhalb unseres Tenants und der Rechenzentren Frankfurt und Berlin.

Tipp: Microsoft betont, dass die Qualität und Menge der Ergebnisse entsprechend der Menge an Daten steigt, die Copilot zur Verfügung hat.

Die Herausforderung besteht darin, festzulegen, welche Daten wir Copilot zugänglich machen wollen. Standardmäßig greift er auf alle Informationen zu, für die wir **Leseberechtigungen** haben, auf unsere zuletzt abgerufenen Daten und auf alle tenantweiten, öffentlich zugänglichen Informationen.

Dokumentenklassifizierung & Output

Die korrekte Dokumentenklassifizierung und ein klar definierter Output sind unersetzlich. Rechenzentrums-Fallback sichert die Datenverarbeitung, während die Prompt-Architektur die Ausgabe beeinflusst. Zudem ist der Unterschied zwischen Data-at-Rest und Data-in-Transit zu beachten.

Wir können Datenklassifizierungsstufen auf Dokumentebene anwenden, um die Verarbeitung sensibler Informationen zu steuern. Copilot nutzt diese **Klassifizierungen**, um innerhalb unserer Anwendungen – sei es bei der Zusammenfassung von Meetings, der Erstellung von Präsentationen oder der Bearbeitung von Dokumenten – die richtigen Informationen bereitzustellen.

Ein weiterer wichtiger Punkt ist die Nutzung von Copilot auf **Endgeräten**. Hier müssen wir entscheiden, ob wir Mitarbeitern die Nutzung auf nicht verwalteten Geräten gestatten. Die Ausgabe von Copilot, die aus unserer definierten Service Boundary stammt, kann sensible Informationen enthalten, die auf ungesicherten Geräten ein Sicherheitsrisiko darstellen könnten.

Bei der Nutzung von **Office Suite** und der **Microsoft 365 Apps** stellt sich die Frage nach möglichen Einschränkungen für Benutzer, die über Office.com auf Copilot zugreifen. Besonders relevant ist hier das Thema **Conditional Access**. Microsoft bestätigt, dass Copilot diese Richtlinien und Zugriffsrechte berücksichtigt.

Das bedeutet, dass die von Copilot abgerufenen und angezeigten Informationen innerhalb der definierten Service Boundary durch unsere **Zugriffsrichtlinien** gesteuert werden. Wenn wir also Richtlinien haben, die den Zugriff auf bestimmte Daten von bestimmten Orten oder Geräten aus einschränken, gelten diese auch für Copilot.

Rechenzentrums-Fallback & Datenverarbeitung

Der Copilot indiziert zunächst alle zugänglichen Daten. Microsoft weist darauf hin, dass bei Spitzenlasten, also wenn nicht genügend Leistung zur Verfügung steht, Copilot auf Daten außerhalb unserer definierten Service Boundary zugreifen kann.

Nach Deutschland kommt der europäische Tenant mit seinen Rechenzentren in Amsterdam und Dublin. Wir als User erhalten dazu keine Benachrichtigung zur externen Verarbeitung. Das bedeutet, dass wir keine Garantie dafür bekommen, dass eine Prompt-Abfrage oder die Bearbeitung durch das Large Language Model ausschließlich innerhalb unserer eigenen Rechenzentren erfolgt.

Prompt-Verarbeitung & Architektur

Der Prozess des Abfragens und Erstellens von Prompts folgt einem konsistenten Aufbau, der in der untenstehenden Grafik sehr deutlich dargestellt ist.

Schritt 1: Der User-Prompt innerhalb der Copilot-App, die in Office integriert ist, wird eingegeben (Punkt 1).

Schritt 2: Dieser Prompt initiiert das sogenannte **Grounding oder Crawling**.

Dieses Grounding, das über *Microsoft Graph Connector* in unserem Tenant abläuft, verwendet stets eine **TLS-Verschlüsselung**, um die Daten während der Übertragung zu schützen. Die dabei gesammelten Informationen stammen aus verschiedenen Quellen, darunter unsere Online-Services, Plugins, Add-ins, Bing-Metasuche, Power Platform und Dataverse. All diese Quellen tragen dazu bei, den potenziellen Output von Copilot zu erweitern.

Schritt 3: Sollen unsere Prompt-Abfragen und die durch das Grounding gesammelten Daten an das Large Language Model zurückgegeben werden? Modell Azure OpenAI generiert dann Antworten und ergänzt diese gegebenenfalls mit Web-Ergebnissen.

Schritt 4: Je nach Art der Anfrage kann der Copilot uns vorschlagen, weitere Informationen aus dem Web einzuholen und entsprechende Links bereitzustellen.

Diese Integration von Web-Ergebnissen führt zu einem umfassenderen und informativeren Output für den Benutzer.

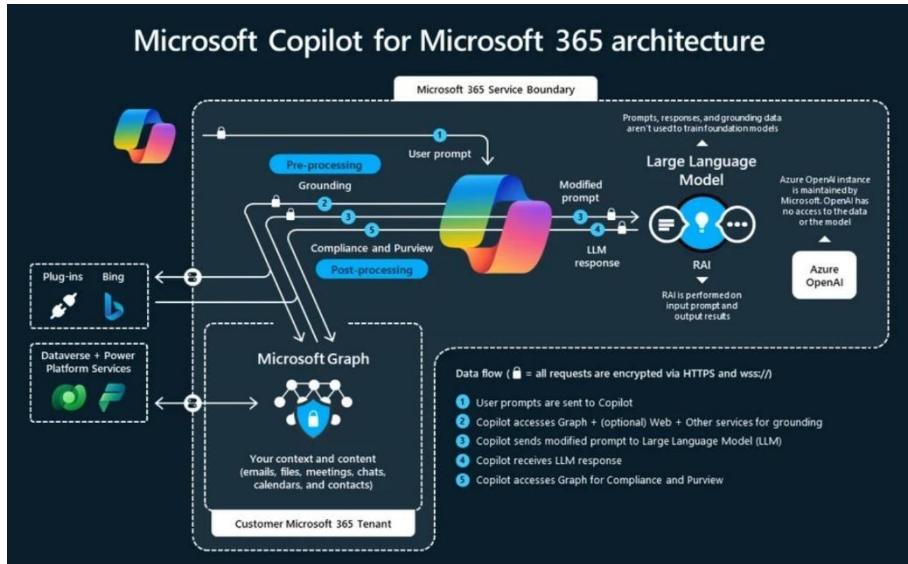


Abbildung 002

(Quelle: <https://www.reddit.com/media?url=https%3A%2F%2Fpreview.redd.it%2Fhow-to-stop-grounding-in-microsoft-graph-prompting-settings-v0-2yg973ij3g2e1.png%3Fwidth%3D1080%26crop%3Dsmart%26auto%3Dwebp%26s%3Dc0dcceaf4abc24646d3f6baabb508ed07d37004>)

Schritt 5: Copilots' Ergebnis wird durch *Compliance- und Purview-Richtlinien* validiert. Das bedeutet, dass bei Abfragen über die Graph API nicht nur die Berechtigungen von SharePoint, OneDrive oder Teams geprüft werden, sondern auch Data-Loss-Prevention-Richtlinien und Information-Protection-Klassifizierungsstufen.

So kann Copilot erkennen, dass ein Benutzer zwar Zugriff auf eine SharePoint-Seite hat, ihm aber bestimmte Ordner oder Dokumente innerhalb dieser Seite aufgrund von Richtlinien nicht angezeigt werden dürfen. Diese Daten werden entsprechend zwar indiziert, sind aber für den Benutzer **nicht zugänglich**.

Tipp: Das Large Language Model selbst ist nicht für die Datensammlung zuständig. Diese Aufgabe übernimmt **Graph** mit dem Grounding-Prozess. Die Abfragen an das Large Language Model können, wie bereits erwähnt, auch außerhalb unserer eigenen Rechenzentren verarbeitet werden.

Data-at-Rest vs. Data-in-Transit

Wir nutzen nicht die öffentlich zugänglichen OpenAI-Dienste, sondern unseren speziell angepassten Azure OpenAI-Dienst. Das bedeutet, dass keine Kundendaten außerhalb der

Heimatregion des Benutzers gespeichert werden. Deswegen ist es wichtig, grundlegend zwischen Data-in-Transit und Data-at-Rest zu unterscheiden.

Data-at-Rest (ruhende Daten): Werden mit einer 256-Bit-AES-Splitting-Verschlüsselung geschützt und verbleiben ausschließlich in unseren Rechenzentren.

Data-in-Transit (Daten während der Übertragung): Anfragen dürfen auch außerhalb unserer eigenen Rechenzentren verarbeitet werden.

Taxonomie und standardisierte Dokumentenbenennung

Eine klare Taxonomie und standardisierte Dokumentenbenennung sind entscheidend für effizientes Datenmanagement. Data Stewards und Data Guards spielen wichtige Rollen. Zudem ist die Indexierung von Zugriffen und Berechtigungen relevant.

Die Qualität der Copilot-Erfahrung hängt entscheidend von den in Microsoft 365 **indexierten Datenquellen** ab. Hierbei ergibt sich ein wichtiger Aspekt, der in der Praxis oft eine Herausforderung darstellt: der Aufbau einer Taxonomie. Es ist wahrscheinlich, dass die IT-Abteilung hierbei nicht allein agieren kann.

Der Aufbau einer Taxonomie beinhaltet die **Verwendung von Tags in Teams, Hashtags in Chats und die Bearbeitung von Dokumenteigenschaften**. Dazu gehören Informationen wie Autor, Dokumentkategorie (z. B. Verkaufs-, Finanz- oder Vertragsdokument) und die Einhaltung einer einheitlichen Namenskonvention.

Tipp: Anstatt Dokumente als "Version 4, 5, 6, 7, 8" zu benennen, empfiehlt es sich, eine standardisierte Namenskonvention zu verwenden, die idealerweise vom Allgemeinen zum Spezifischen übergeht.

Auch ohne eine solche Taxonomie liefert Copilot Ergebnisse, jedoch sind diese nachweislich besser, wenn eine einheitliche Namenskonvention im Unternehmen etabliert ist.

Rollen im Datenmanagement: Data Stewards und Data Guards

Die Verantwortung für eine effektive Datenorganisation liegt nicht allein bei der IT-Abteilung. Hier kommen sogenannte Data Guards oder Data Stewards ins Spiel. Das sind **designierte Personen** innerhalb des Unternehmens, die als Besitzer von Teams oder SharePoint-Seiten fungieren und die Zugriffe sowie die Struktur der Dokumente und Dateien in ihren jeweiligen Bereichen **überwachen und validieren**.

Tipp: Diese Aufgabe sollte nicht von der IT-Abteilung allein übernommen werden.

Empfehlung: Es ist wichtig, zu prüfen, ob in unserem Unternehmen bereits Data Stewards oder Datenverantwortliche etabliert sind. Oftmals, und das ist ein häufiges Problem, sind Administratoren mit ihren Admin-Konten in zahlreichen SharePoint-Seiten oder Teams Mitglied, nur um die Verwaltung zu erleichtern, obwohl sie die Inhalte **nie einsehen**. Das kann zu unerwünschten Ergebnissen in Copilot führen, da Mitarbeiter möglicherweise Inhalte sehen, die ihnen nicht zugänglich sein sollten.

Indexierung der Zugriffe und Berechtigungen

Microsoft 365 führt automatisch **alle acht Stunden** eine Indexierung durch. Nach der initialen Vollsynchonisierung bei der Aktivierung des Copilot-Dienstes werden Zugriffe und Berechtigungen regelmäßig überprüft.

Das bedeutet, wenn wir Änderungen an Zugriffsrechten vornehmen, kann es bis zu acht Stunden dauern, bis diese in Copilot sichtbar werden; eben erst, wenn der **nächste Synchronisationsintervall** stattfindet.

Der Timer wird immer auf die UTC-Zeit null gesetzt. Die Indexierung erfolgt entsprechend um 8 Uhr, 16 Uhr und 24 Uhr, also wieder um Mitternacht.

Struktur des semantischen Index

*Der semantische Index ist auf Tenant- und Nutzerebene strukturiert.
Gastzugriffe werden validiert und Berechtigungen synchronisiert. "Connected Experiences" und Copilot nutzen SharePoint-Daten.*

Oftmals sind Aspekte wie die Anzahl der Besitzer von SharePoint-Seiten, die Anzahl der Personen, die Teams oder SharePoint-Seiten erstellen dürfen, und die Art der freigegebenen Links über die Jahre gewachsen, ohne dass klare Prozesse oder Verantwortlichkeiten definiert wurden.

Semantic Index for Copilot explained



Abbildung 003

(Quelle: https://media.licdn.com/dms/image/v2/D5612AQFvBNGgi84hqQ/article-cover_image-shrink_720_1280/article-cover_image-shrink_720_1280/0/1724750286496?e=1751500800&v=beta&t=2rf2AfNAetvquCYIF3XumW6VOuGfQ1MNnUCI6VnFgF8)

Der semantische Index, der für Copilot verwendet wird, durchsucht unseren **gesamten Tenant** und greift **auf alle relevanten Daten** zu. Wir müssen daher unsere Datenstruktur und Zugriffsrechte überprüfen und optimieren, um die bestmöglichen Ergebnisse mit Copilot zu erzielen.

Um zu verstehen, wie der semantische Index funktioniert, ist es wichtig, seine Unterteilung zu betrachten: den User-Level-Semantic-Index und den Tenant-Level-Semantic-Index.

Tenant-Level Semantischer Index

Die Basis hierfür bildet SharePoint. Es ist jedoch wichtig zu verstehen, was alles auf SharePoint aufbaut: **OneDrive, Teams und Microsoft 365 Gruppen**. Alle sind Tools, die von unseren Benutzern täglich verwendet werden.

Oftmals werden Abteilungsdateien fälschlicherweise in OneDrive gespeichert, was nicht der vorgesehene Zweck ist. Hier ist es wichtig, Klarheit zu schaffen.

Innerhalb von SharePoint werden **Seiten, Webparts, Sites, Bibliotheken, Aktivitäten** (wie zuletzt aufgerufene Inhalte) und **Listen** indiziert. Microsoft Lists ist eine Anwendung, die in Teams bereitgestellt werden kann und zur Erstellung verschiedener Listen dient. Obwohl Lists auf den

ersten Blick nichts mit SharePoint zu tun haben scheint, basiert es darauf und wird daher ebenfalls indiziert.

Empfehlung: Gehen Sie bei der Vergabe von Zugriffsrechten für Anwendungen in Microsoft Teams, insbesondere für solche mit Datenablage auf SharePoint-Basis, sorgfältig vor.

User-Level Semantischer Index

Der User-Level Index umfasst vom Benutzer selbst abgelegte **Dokumente, geteilte Inhalte** (sowohl direkt als auch über Gruppen), Dokumente, in denen der Benutzer erwähnt wurde, und Kommentare in Dokumenten, an denen er mitgearbeitet hat.

Ein weiterer wichtiger Aspekt ist die Integration von **E-Mails**. Copilot berücksichtigt, auf welche Postfächer der Benutzer Zugriff hat, und zeigt die entsprechenden E-Mail-Inhalte an.

Validierung und Ablauf von Gastzugriffen

Es ist entscheidend zu verstehen, dass die Inhalte, auf die Copilot zugreift, vollständig auf den Daten in unserem Tenant basieren. Copilot greift nicht auf Daten zu, die in Cross-Tenant-Synchronisierungen oder Gastzugriffen liegen. Diese Daten werden **weder indiziert noch in den Ergebnissen angezeigt**. So müssen wir nicht um die Verwaltung und Freigabe von Daten außerhalb unseres Tenants kümmern.

Tipp: Microsoft empfiehlt, die Gastzugriffe in unserem Tenant zu überprüfen. Gastzugriffe bleiben in der Regel bestehen, auch wenn Berechtigungen geändert werden.

Auch wenn der semantische Index auf unseren internen Daten basiert, ist es im Rahmen der Administration wichtig, die Gastzugriffe zu validieren.

Synchronisierung und Indexierung von Berechtigungen

Zum Überprüfen der technischen Konfiguration in unseren Systemen, insbesondere den On- und Offboarding-Prozess für Gastobjekte, ist die **Konfiguration des Gastzugriffs in Microsoft Teams** von zentraler Bedeutung. Wie ist dieser Prozess bei uns implementiert? Gibt es angemessene Restriktionen, um die Sicherheit unseres Tenants zu gewährleisten?

Eine Validierung der aktuellen Konfiguration ist erforderlich. Obwohl der semantische Index auf unseren internen Daten basiert, ist eine Überprüfung der administrativen Konfiguration notwendig.

Wir müssen außerdem die Anzahl der Gastzugriffe und deren Notwendigkeit in unserem Tenant überprüfen. Im Hinblick auf die Verschlüsselung ist zu beachten, dass Microsoft die Kategorien *Data-in-Transit* und *Data-at-Rest* unterscheidet.

Data-in-Transit Encryption: Daten, die zwischen Services und Endpoints, wie z.B. Teams-Nachrichten und E-Mails, übertragen und durch TLS-Verschlüsselung geschützt werden.

Data-at-Rest Encryption: Ruhende Daten, die in SharePoint, OneDrive und Teams gespeichert sind, und durch 256-Bit-AES-Splitting-Verschlüsselung geschützt werden.

Bezüglich erweiterter Verschlüsselung ist zu beachten, dass die Nutzung der *Double-Key-Encryption* von Microsoft Office 365 Copilot **nicht** unterstützt wird. Ebenso führt die Datenverschlüsselung mit einem lokal verwalteten PKI-Schlüssel dazu, dass die entsprechenden Dokumente nicht in die Bewertung durch Microsoft Office 365 Copilot einbezogen werden.

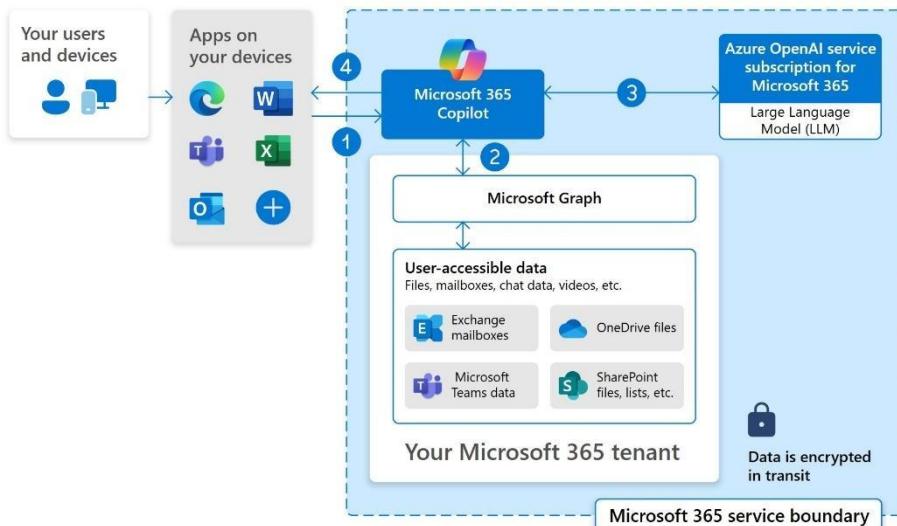


Abbildung 004

(Quelle: <https://learn.microsoft.com/fi-fi/copilot/microsoft-365/media/microsoft-365-copilot-architecture/copilot-query-flow.svg>)

Connected Experiences

Die *Connected Experiences* sind eine wesentliche Voraussetzung für die Nutzung von Copilot in der Microsoft Office Suite. Es gibt zwei Kategorien dieser verbundenen Erfahrungen:

Connected Experiences that analyze your content: verbundene Erfahrungen, die Ihre Inhalte analysieren

Connected Experiences that download content: verbundene Erfahrungen, die Inhalte herunterladen

Die Designvorschlagsfunktion in PowerPoint, die zusätzliche Designideen aus dem Internet abrufen kann, ist eine *Connected Experience*. Auch die Wetteranzeige gehört zu diesen verbundenen Erfahrungen.

Tipp: Der Copilot-Dienst in den Office-Anwendungen ist nicht verfügbar, wenn die *Connected Experiences deaktiviert* sind. Überprüfen Sie daher Konfiguration dieser Einstellungen.

Copilot und Sharepoint-Daten zum Antworten

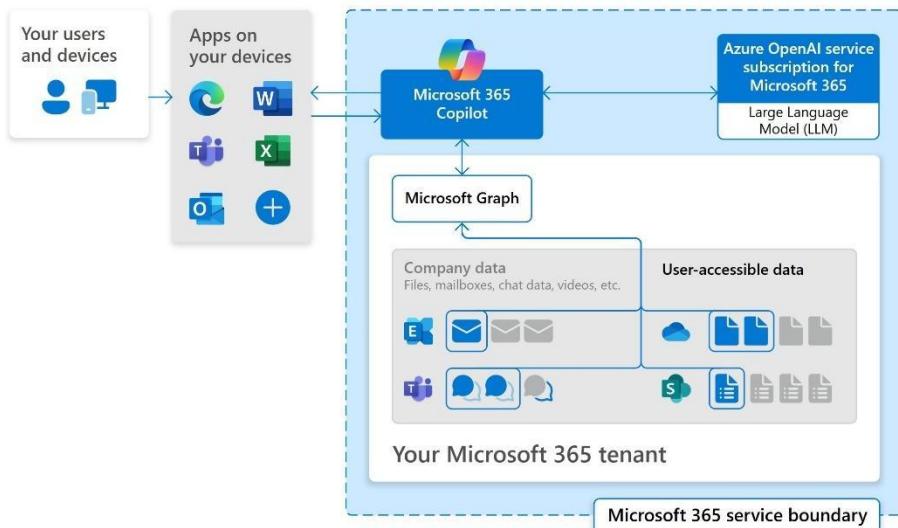


Abbildung 005

(Quelle:<https://learn.microsoft.com/fi-fi/copilot/microsoft-365/media/microsoft-365-copilot-architecture/copilot-user-access.svg>)

Microsoft 365 Copilot greift zusätzlich zu Office-Anwendungen auf SharePoint-Daten für die Beantwortung von Fragen zu, wobei ein großes Sprachmodell (**Large Language Model**) mit Microsoft Graph-Daten kombiniert wird.

Die Rolle des AI-Administrators (im N2ID) gewinnt zunehmend an Bedeutung. Dieser muss mit verschiedenen Bereichen und administrativen Werkzeugen zusammenarbeiten, da Copilot Daten aus digitalen Word-Dokumenten, PowerPoint-Meeting-Aufzeichnungen und OneDrive auswertet.

Die **Zugriffsvalidierung** durch Microsoft 365 Copilot ist dabei entscheidend. Technisch gesehen sollte Copilot nur auf Informationen zugreifen, für die der Benutzer berechtigt ist. Dies betrifft Dateien in OneDrive (eigene und geteilte), Exchange-Postfächer, Chat-Nachrichten (ohne gelöschte) und SharePoint-Inhalte.

Navigation im Microsoft 365 Admin Center

Das Microsoft 365 Admin Center navigiert durch SharePoint-Einstellungen, Berichte und Self-Service. Die Konfiguration von Freigaben, Installationsrisiken, Speicherlimits und Zugriffsmanagement werden behandelt. Aktivitätsdaten geben Einblicke.

Pfad: admin.microsoft.com → Teams und Gruppen → **Aktive Teams und Gruppen**

Anbei eine Veranschaulichung unserer Teams, Microsoft 365 Gruppen, Verteilergruppen und Sicherheitsgruppen. Für uns sind insbesondere Sicherheitsgruppen und Microsoft 365 Gruppen relevant.

Types of groups and where they are created

Groups can be created in several of the admin centers and by users from within apps.

Type of group	Security group	Microsoft 365 group	Mail-enabled security group	Distribution group	Shared mailbox
	Used for granting access to resources and for managing devices.	Used for collaboration. Includes a group email and shared workspaces.	Includes the ability to send mail to a group. Cannot be dynamically managed. Cannot contain devices.	Used for sending notifications to a group of people.	Used when multiple people need to access the same mailbox, such as a support email address.
Where groups can be created					
Azure AD					
Microsoft 365 admin center					
Exchange admin center					
Outlook					
Teams					
SharePoint					
Planner					
Yammer					
Stream					
Power BI (classic)					
Roadmap					
Project for the web					

Abbildung 006

(Quelle:https://media.licdn.com/dms/image/v2/D4E22AQHQbUj2WNQ1mQ/feedshare-shrink_1280/feedshare-shrink_1280/0/1684947518752?e=1748476800&v=beta&t=yrXXqBx6riltnBwUT2E7jKalkhrslaxji-e3LhacwB2A)

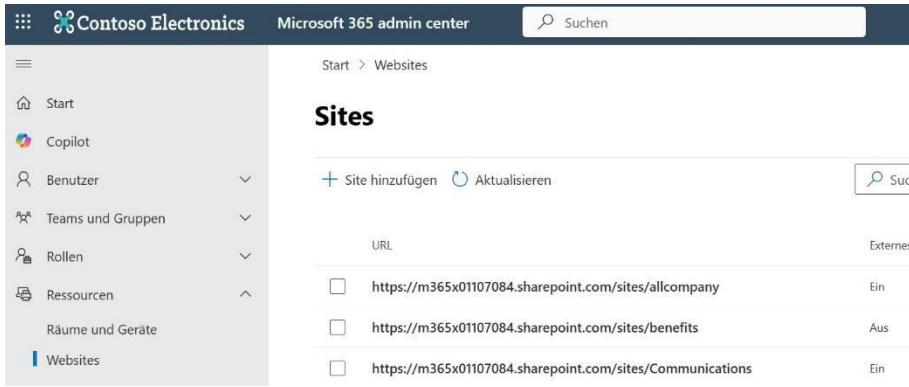
Eine Microsoft 365 Gruppe umfasst entsprechend ein Teams, eine E-Mail-Adresse und weitere Komponenten. Technisch gesehen wird im Backend eine Microsoft 365 Gruppe aufgebaut, während im Frontend ein Teams genutzt wird.

Die Microsoft 365 Gruppe ist eine zentrale Komponente, die verschiedene Dienste integriert. Dazu gehören SharePoint-Speicher, OneDrive-Aufnahmeordner, Planner-Aufgaben, Kommentare, freigegebene Postfächer, Teams-Inhalte, SharePoint-Inhalte und Yammer-Inhalte. Power BI und Project sind **nicht direkt** integriert, Streaming-Transkripte können jedoch genutzt werden.

Es ist wichtig, die Konfiguration der Teams- und Microsoft 365 Gruppenanlage zu überprüfen. Eine Microsoft 365 Gruppe kann ohne Teams angelegt werden, ein Teams jedoch nicht ohne Microsoft 365 Gruppe.

Übersicht über SharePoint-Sites

Pfad: admin.microsoft.com → Ressourcen→ Websites



URL	Externes
<input type="checkbox"/> https://m365x01107084.sharepoint.com/sites/allcompany	Ein
<input type="checkbox"/> https://m365x01107084.sharepoint.com/sites/benefits	Aus
<input type="checkbox"/> https://m365x01107084.sharepoint.com/sites/Communications	Ein

Abbildung 007

Aktuell gibt es eine Auflistung von SharePoint-Seiten, die nicht im SharePoint Admin Center selbst enthalten ist und alle Bibliotheken umfasst. Im SharePoint Admin Center werden private Kanäle und Chat-Kanäle, die ebenfalls SharePoint-Seiten sind, **nicht** angezeigt.

Um diese Seiten zu verwalten, muss man den Bereich **Sites** aufrufen. Ein wichtiger Aspekt ist die Überprüfung der Anzahl der vorhandenen Sites, deren Nutzung und die Konfiguration externer Freigaben. Wir müssen überprüfen, welche externen Zugriffe erlaubt sind und welche nicht, sowie welche möglicherweise nicht mehr benötigt werden.

Obwohl das SharePoint Admin Center zur Verwaltung dient, fehlen dort einige Seiten. Um eine vollständige Übersicht über die SharePoint-Sites zu erhalten, navigieren wir zu → **Einstellungen**.

Organisationseinstellungen im Admin Center

Pfad: admin.microsoft.com → Einstellungen → Einstellungen der Organisation → **Kontoverknüpfung**

Die Konfiguration selbst wird später betrachtet. Wir überprüfen zunächst, ob wir die Option **Kontoverknüpfung** haben. Sie wird je nach vorherigen Konfigurationen möglicherweise nicht in allen Tenants angezeigt.

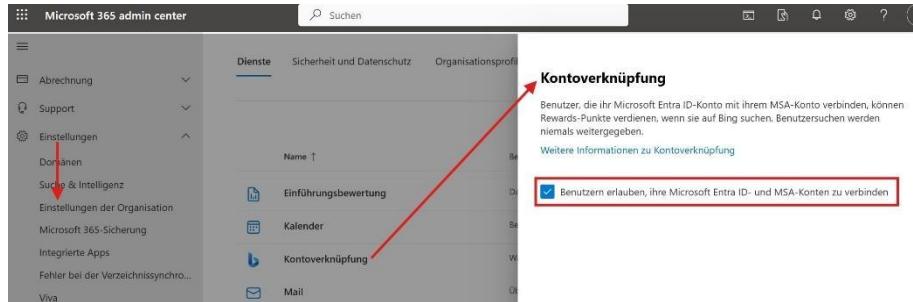


Abbildung 008

Kontoverknüpfung ermöglicht die Verknüpfung von Microsoft Entra ID-Konten mit MSA-Konten, um bei Bing-Suchen Belohnungspunkte zu sammeln. Hierbei handelt es sich nicht um eine reine Sicherheitskonfiguration, sondern um ein Compliance-Thema. Der Bing-Suchdienst ist in Microsoft 365 Copilot integriert.

Durch die Verknüpfung kann der Bing-Suchdienst Metadaten auswerten, um zwischen privaten und geschäftlichen Suchen zu unterscheiden. Zu diesen Metadaten gehören Suchinhalte, IP-Adressen und Browserversionen. Die Daten werden zur Verbesserung der Bing-Suchergebnisse verwendet, die auch in Microsoft 365 Copilot angezeigt werden.

Tipp: Trennen Sie zwischen geschäftlichen und privaten Konten. Die geschäftliche Nutzung von Copilot sollte ausschließlich mit geschäftlichen Konten erfolgen, die private Nutzung von Bing oder Copilot nur mit privaten Konten.

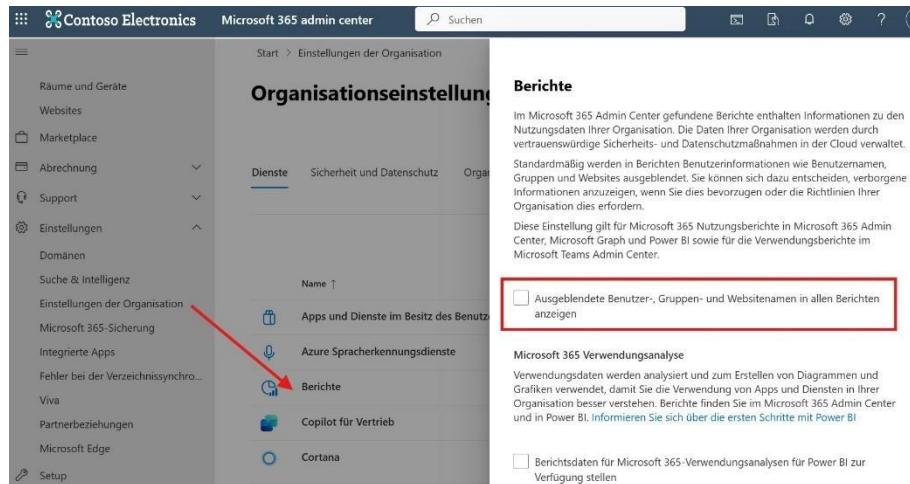
Empfehlung: Falls **Kontoverknüpfung** aktiviert ist, deaktivieren Sie es. Das hat in der Regel keine Auswirkungen auf die meisten Benutzer. Benutzer, die zuvor eine Verknüpfung hatten, werden jedoch möglicherweise aufgefordert, sich mit einem geschäftlichen Konto anzumelden, um den geschäftlichen Bereich nutzen zu können.

Im Bereich **Einstellungen der Organisation** gibt es weitere Konfigurationsoptionen, die im Rahmen einer Tenant-Härtung überprüft werden sollten. Für Copilot sind insbesondere drei Optionen relevant:

- Berichte
- Self-Service-Testversionen und -Käufe
- SharePoint

Berichte und Pseudonymisierung in Copilot

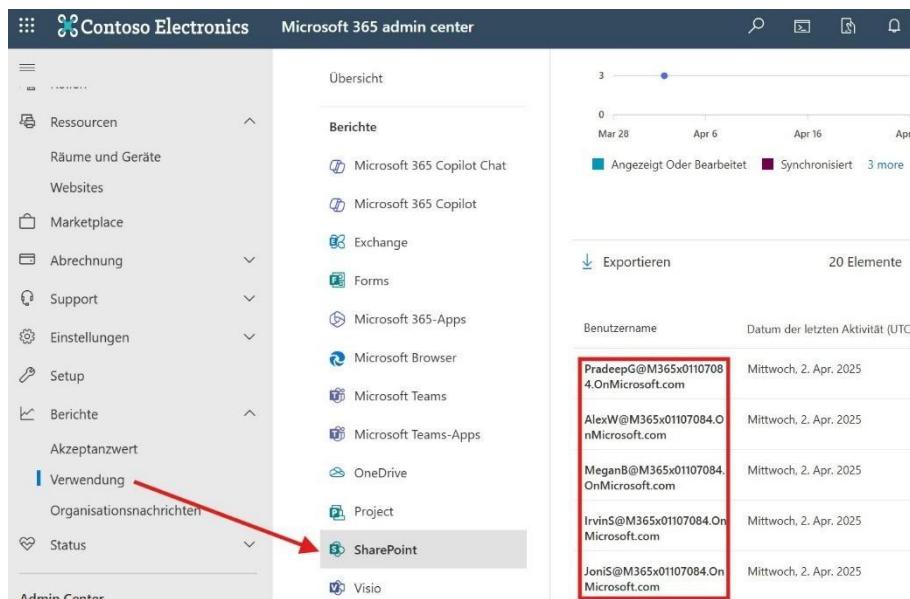
Wenn der Haken unter Pfad: admin.microsoft.com → Einstellungen → Einstellungen der Organisation → **Berichte** nicht gesetzt ist,



The screenshot shows the Microsoft 365 Admin Center interface. On the left, there's a navigation sidebar with various categories like 'Raume und Geräte', 'Websites', 'Marketplace', etc. Under 'Einstellungen', there are several sub-options including 'Einstellungen der Organisation'. In the main content area, the 'Organisationseinstellung' page is displayed. A red arrow points from the 'Einstellungen der Organisation' link in the sidebar to the 'Berichte' link in the center. The 'Berichte' section contains a paragraph about reports and a checkbox labeled 'Ausgebendete Benutzer-, Gruppen- und Websitenamen in allen Berichten anzeigen'. Another red box highlights this checkbox.

Abbildung 009

erscheinen die Namen unter Pfad: admin.microsoft.com → Berichte → Verwendung → **Sharepoint** (ganz unten) unter als *Klarnamen*.



This screenshot shows the Microsoft 365 Admin Center with the 'Berichte' section selected in the navigation. A red arrow points from the 'Verwendung' link in the left sidebar to the 'SharePoint' link in the center content area. The right side displays a list of users with their names listed under the 'SharePoint' heading. A red box highlights the entire list of names.

Benutzername	Datum der letzten Aktivität (UTC)
PradeepG@M365x01107084.OnMicrosoft.com	Mittwoch, 2. Apr. 2025
AlexW@M365x01107084.OnMicrosoft.com	Mittwoch, 2. Apr. 2025
MeganB@M365x01107084.OnMicrosoft.com	Mittwoch, 2. Apr. 2025
IrvinS@M365x01107084.OnMicrosoft.com	Mittwoch, 2. Apr. 2025
JoniS@M365x01107084.OnMicrosoft.com	Mittwoch, 2. Apr. 2025

Abbildung 010

Auch innerhalb der Copilot-Auswertungen werden diese Namen entsprechend sichtbar dargestellt. Aus **datenschutzrechtlicher Sicht** – insbesondere im Hinblick auf eine DSGVO-konforme Konfiguration – ist jedoch eine Pseudonymisierung vorgesehen.

Dabei sprechen wir ausdrücklich von **Pseudonymisierung**, nicht von Anonymisierung. In der praktischen Umsetzung bedeutet das: Die Klartextnamen werden durch automatisch generierte Buchstaben-Zahlen-Kombinationen ersetzt.

Aktiviert man nun die Funktion in Pfad: admin.microsoft.com → Einstellungen → Einstellungen der Organisation → **Berichte**

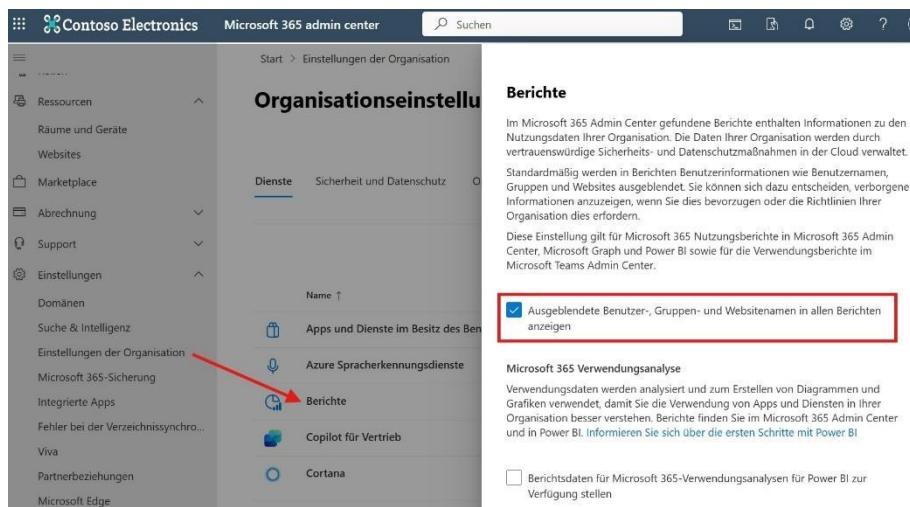


Abbildung 011

sehen wir unter admin.microsoft.com → Berichte → Verwendung → **SharePoint** deutlich, dass die Nutzer nun als Zahlen- und Buchstabenkombination, eben einer Pseudonymisierung, angezeigt werden.

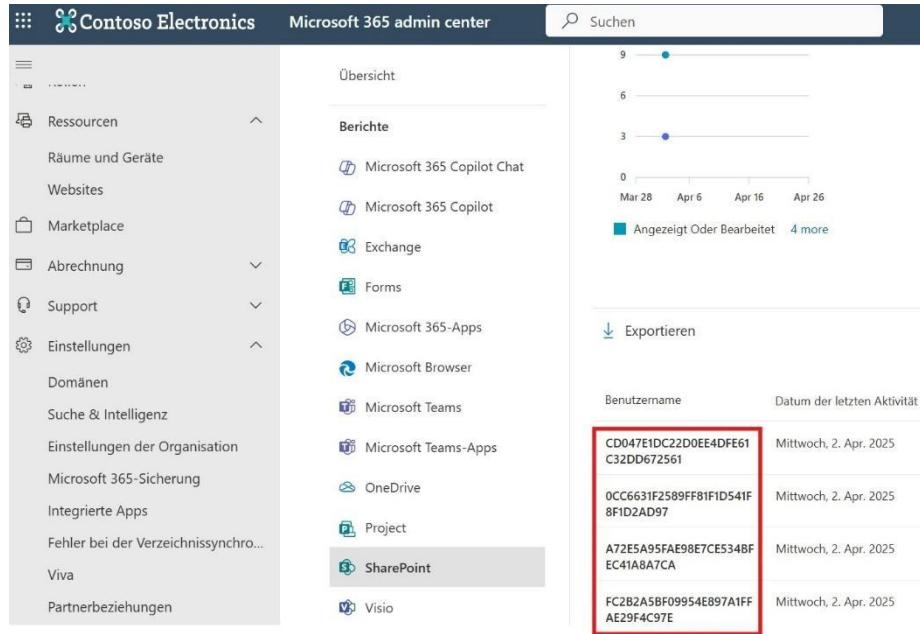


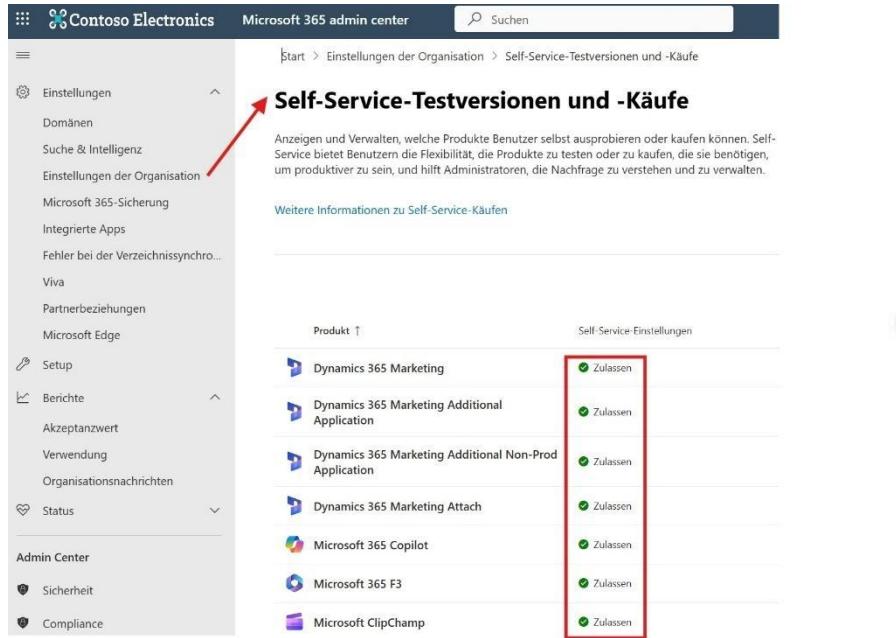
Abbildung 012

Diese Einstellung führt häufig zu einem gewissen Spannungsfeld: Auf der einen Seite möchten wir nachverfolgen, wie intensiv einzelne Nutzer bestimmte Microsoft 365-Dienste wie SharePoint, Teams oder Copilot verwenden – etwa im Rahmen von **Compliance-Analysen**. Auf der anderen Seite wollen wir eine potenzielle **Mitarbeiterüberwachung** unbedingt vermeiden.

Die Entscheidung für oder gegen die Pseudonymisierung ist daher keine reine technische Frage, sondern betrifft grundlegend auch datenschutzrechtliche und unternehmenskulturelle Überlegungen.

Self-Service-Testversionen und -Käufe

Unter Pfad: admin.microsoft.com → Einstellungen → Einstellungen der Organisation → **Self-Service-Testversionen und -Käufe** gibt es verschiedene Self-Service-Testversionen und Kaufoptionen. In den meisten Fällen stehen diese Einstellungen standardmäßig auf **Zulassen** oder **Nicht zulassen**.



Start > Einstellungen der Organisation > Self-Service-Testversionen und -Käufe

Self-Service-Testversionen und -Käufe

Anzeigen und Verwalten, welche Produkte Benutzer selbst ausprobieren oder kaufen können. Self-Service bietet Benutzern die Flexibilität, die Produkte zu testen oder zu kaufen, die sie benötigen, um produktiver zu sein, und hilft Administratoren, die Nachfrage zu verstehen und zu verwalten.

Weitere Informationen zu Self-Service-Käufen

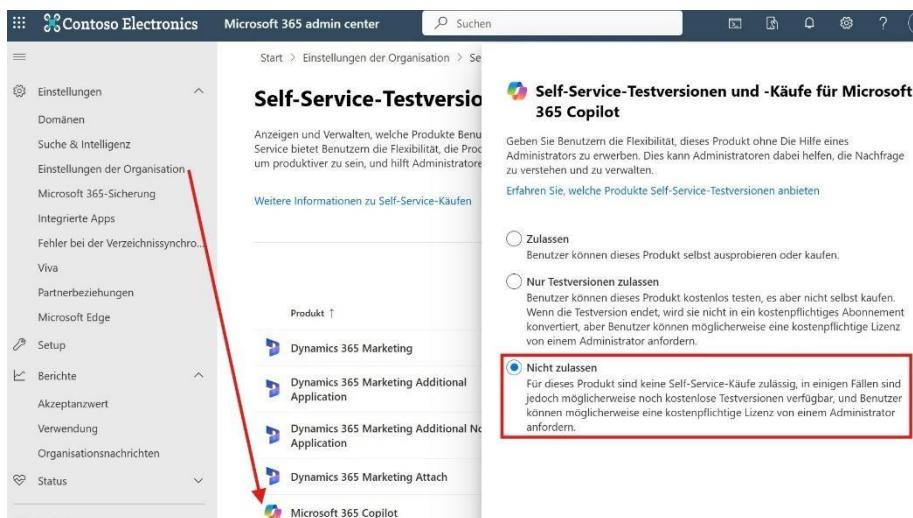
Produkt ↑	Self-Service-Einstellungen
Dynamics 365 Marketing	<input checked="" type="checkbox"/> Zulassen
Dynamics 365 Marketing Additional Application	<input checked="" type="checkbox"/> Zulassen
Dynamics 365 Marketing Additional Non-Prod Application	<input checked="" type="checkbox"/> Zulassen
Dynamics 365 Marketing Attach	<input checked="" type="checkbox"/> Zulassen
Microsoft 365 Copilot	<input checked="" type="checkbox"/> Zulassen
Microsoft 365 F3	<input checked="" type="checkbox"/> Zulassen
Microsoft ClipChamp	<input checked="" type="checkbox"/> Zulassen

Abbildung 013

Empfohlene Einstellungen für Self-Service

Bei einigen Tenants ist bereits alles auf **Nicht zulassen** gesetzt, mit Ausnahme einzelner Punkte wie dem **Teams Exploratory Upgrade Request**, der möglicherweise noch nicht deaktiviert wurde.

Es wird empfohlen, alle Self-Services, die nicht aktiv genutzt werden sollen, konsequent auf **Nicht zulassen** zu stellen. Die verfügbaren Optionen sind:



Start > Einstellungen der Organisation > Self-Service-Testversionen und -Käufe für Microsoft 365 Copilot

Self-Service-Testversionen und -Käufe für Microsoft 365 Copilot

Geben Sie Benutzern die Flexibilität, dieses Produkt ohne die Hilfe eines Administrators zu erwerben. Dies kann Administratoren dabei helfen, die Nachfrage zu verstehen und zu verwalten.

Erfahren Sie, welche Produkte Self-Service-Testversionen anbieten

Nicht zulassen
Benutzer können dieses Produkt selbst ausprobieren oder kaufen.

Nur Testversionen zulassen
Benutzer können dieses Produkt kostenlos testen, es aber nicht selbst kaufen. Wenn die Testversion endet, wird sie nicht in ein kostenpflichtiges Abonnement konvertiert, aber Benutzer können möglicherweise eine kostenpflichtige Lizenz von einem Administrator anfordern.

Dynamics 365 Marketing
Dynamics 365 Marketing Additional Application
Dynamics 365 Marketing Additional Non-Prod Application
Dynamics 365 Marketing Attach
Microsoft 365 Copilot

Abbildung 014

Gerade in einer gehärteten Umgebung sollte die Entscheidung über die Freigabe von Applikationen, Add-ins oder Programmen zentral **durch die IT** getroffen werden – nicht durch einzelne User.

Microsoft 365 hat sich im Laufe der Zeit von einem geschlossenen zu einem sehr offenen System entwickelt. Dadurch ist es notwendig geworden, dass wir neue Funktionen wie Self-Service-Käufe aktiv konfigurieren – sei es durch Erlauben oder gezieltes Sperren. Diese Prüfung sollte für sämtliche Services erfolgen.

Beispiel: Teams Exploratory Upgrade

Wenn ein User eine Testversion aktiviert, erscheint diese unter Pfad: admin.microsoft.com → Abrechnung → **Ihre Produkte**. Ein typisches Beispiel ist der **Teams Exploratory Plan**, der insbesondere während der Corona-Zeit bereitgestellt wurde. Er ermöglichte ein Jahr lang die Nutzung der vollwertigen Teams-Version – danach war ein Wechsel auf eine kostenpflichtige Lizenz oder die Free-Version erforderlich.

In der Praxis kann es sinnvoll sein, generell **keine Self-Service-Funktionen zuzulassen**. Dies sollte allerdings gut geplant und in einen klaren Prozess eingebettet sein. Es ist nachvollziehbar, dass sich solche Konfigurationen nicht immer leicht und schnell umsetzen lassen.

Konfiguration von SharePoint-Freigaben

Pfad: admin.microsoft.com → Einstellungen → Einstellungen der Organisation → **SharePoint**

Hier sehen wir eine Auswahlmöglichkeit mit den Optionen:

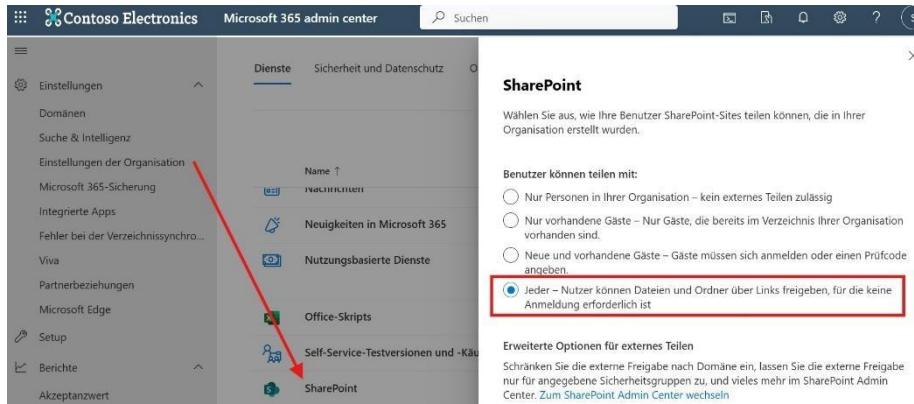


Abbildung 015

Bei einigen Tenants steht die Auswahl noch auf **Jeder** – was in der Praxis mit erheblichen Risiken verbunden ist.

Risiken durch Jeder-Links

Teilen wir eine Datei oder einen Ordner über einen Jeder-Link, kann theoretisch jede Person mit dem Link auf die Inhalte zugreifen – unabhängig davon, ob sie **intern oder extern** ist. Auch wenn die Freigabe ursprünglich auf einen bestimmten Personenkreis beschränkt war, haben wir keine Kontrolle darüber, ob diese Nutzer den Link nicht weitergeben.

Für Microsoft 365 Copilot bedeutet das: **Sobald ein Link mit Jeder-Freigabe besteht, wird der Inhalt indexiert** und kann Copilot als potenzielle Datenquelle zur Verfügung stehen. Diese Inhalte erscheinen dann bei Suchanfragen, sofern sie durch Berechtigungen gedeckt sind.

Empfehlung: Wir deaktivieren die Option *Jeder* und wählen stattdessen eine restriktivere Einstellung aus. Damit wird sichergestellt, dass Inhalte nicht unbeabsichtigt in größerem Umfang freigegeben werden.

Hier haben wir einige Optionen:

Neue und vorhandene Gäste als Alternative

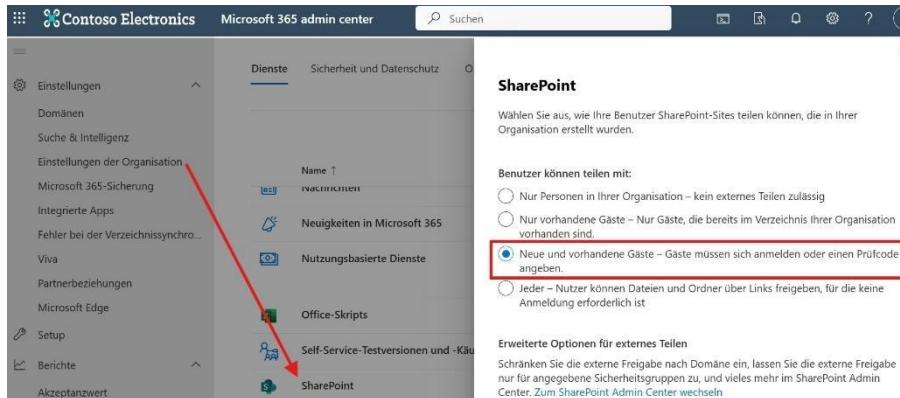


Abbildung 016

Die Option **Neue und vorhandene Gäste** bietet mehr Kontrolle, erfordert aber eine strukturierte Umsetzung. In diesem Fall kann ein Benutzer eine externe Person selbst zur Zusammenarbeit einladen. Die eingeladene Person erhält eine E-Mail mit einem Verifizierungscode und muss diesen bestätigen, um Zugriff zu erhalten.

Vorteil: Die Einladung kann ohne IT-Abteilung erfolgen.

Nachteil: Jeder eingeladene Gast durchläuft denselben Onboarding-Prozess, was bei vielen externen Nutzern zu einem hohen Aufwand führen kann.

Auch intern ist durch diese Einstellung sichergestellt, dass Inhalte **nicht mehr mit allen im Unternehmen** geteilt werden können, sondern nur noch mit einer explizit ausgewählten Gruppe. Das betrifft sowohl SharePoint- als auch OneDrive-Inhalte.

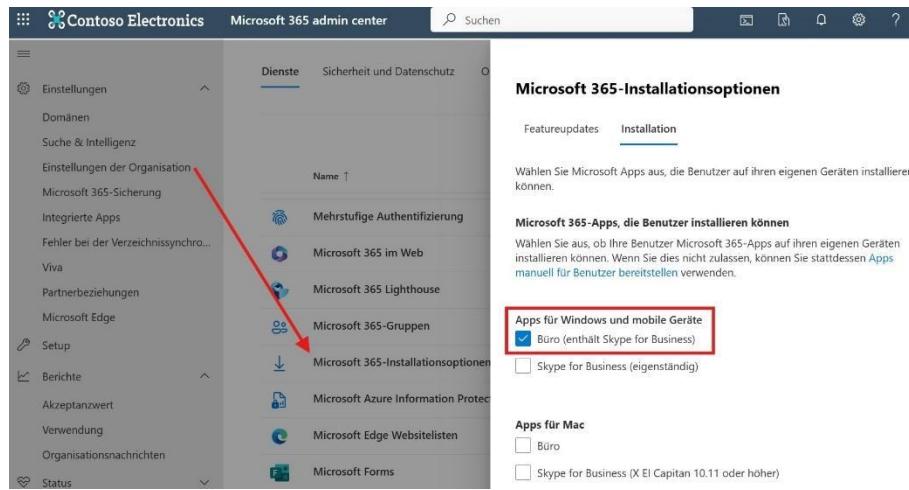
Übergang von Jeder auf restriktivere Optionen

Ein sofortiger Wechsel von *Jeder* auf *Neue und vorhandene Gäste* sollte **vorab kommuniziert werden**. Sobald diese Änderung aktiviert ist, verlieren bestehende Jeder-Links nach kurzer Zeit ihre Gültigkeit – oft innerhalb von zwei bis drei Stunden.

Das bedeutet: **Alle bisherigen Freigaben müssen neu gesetzt werden.** Hier lohnt sich ein vorbereitender Hinweis an die betroffenen Nutzer.

Microsoft 365 Installation und Risiken

Pfad: admin.microsoft.com → Einstellungen → Einstellungen der Organisation → **Microsoft 365-Installationsoptionen** → Installation

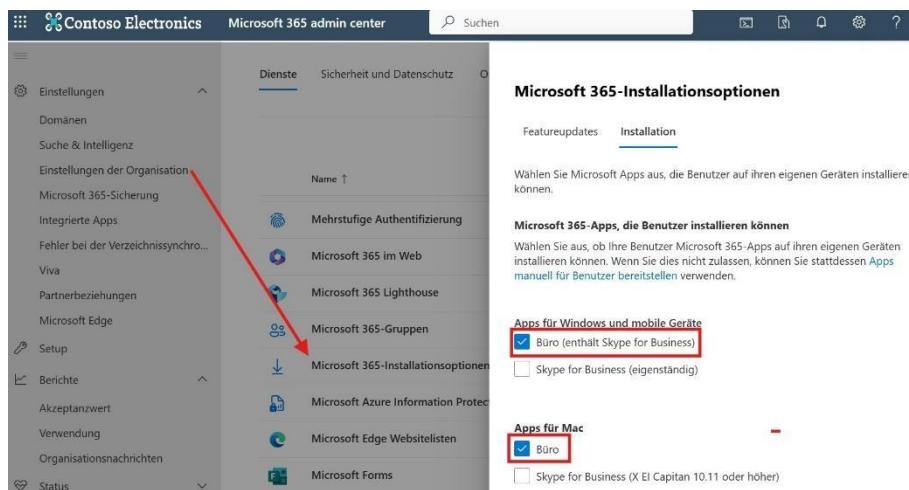


The screenshot shows the Microsoft 365 admin center interface for 'Contoso Electronics'. The left sidebar has sections like Einstellungen, Dienste, Sicherheit und Datenschutz, and Reports. The 'Dienste' section is selected. In the main pane, under 'Microsoft 365-Installationsoptionen', there are tabs for Featureupdates and Installation. The 'Installation' tab is selected. It lists apps for Windows and mobile devices, including 'Büro (enthalt Skype for Business)' which is checked. There's also a section for Mac apps.

Abbildung 017

Microsoft 365 Installation und Risiken

Pfad: admin.microsoft.com → Einstellungen → Einstellungen der Organisation → **Microsoft 365-Installationsoptionen** → Installation



This screenshot is identical to Abbildung 017, showing the Microsoft 365 admin center for 'Contoso Electronics'. The 'Dienste' section is selected in the sidebar. The main content shows the 'Microsoft 365-Installationsoptionen' page with the 'Installation' tab selected. It lists apps for Windows and mobile devices, including 'Büro (enthalt Skype for Business)' which is checked. There's also a section for Mac apps.

Abbildung 018

Wenn wir die Installationsoptionen für Microsoft 365 nicht explizit eingeschränkt haben, erlauben wir es Benutzern, über **office.com** oder **m365.copilot.com** die Office Suite eigenständig auf nicht verwalteten Geräten zu installieren. Auch unter www.m365.cloud.microsoft.com finden wir auf der rechten Seite die folgende Option:



Abbildung 019

Sobald sich diese Möglichkeit in der Organisation herumspricht, wird sie häufig genutzt – oft auch **auf privaten Geräten**. Das birgt auf mehreren Ebenen ein Risiko.

Im Zusammenhang mit Microsoft 365 Copilot bedeutet das: Die Indexierung, die Generierung von Suchergebnissen und die Ausgabe von Inhalten erfolgen potenziell auf **nicht verwalteten Endgeräten**. Damit stellen wir Unternehmensinformationen, auch klassifizierte Inhalte, außerhalb kontrollierter Umgebungen zur Verfügung.

Empfehlung: Wir müssen uns aktiv die Frage stellen: Wollen wir das zulassen – ja oder nein? In den allermeisten Fällen lautet die Antwort: Nein.

Lizenzmodell und Installationsanzahl

Die Installation der Office Suite sollte idealerweise zentral durch die IT-Abteilung erfolgen – und nicht durch die Benutzer selbst. Microsoft erlaubt mit einer Microsoft 365 Lizenz insgesamt **15 Installationen**:

- 5 × Windows oder Mac
- 5 × Smartphone
- 5 × Tablet

Ob es sich dabei um geschäftliche oder private Geräte handelt, spielt für Microsoft technisch keine Rolle. Die entscheidende Frage ist vielmehr: **Wie viele Installationen sind erforderlich – und auf welchen Geräten erlauben wir sie?**

Tipp: Die meisten Benutzer benötigen maximal drei Geräte: Smartphone, Tablet und ein Arbeitsgerät.

Gerätekontrolle durch Intune und Conditional Access

Es liegt in unserer Verantwortung, sicherzustellen, **wo unsere Unternehmensdaten innerhalb der Office Suite verarbeitet werden dürfen**. Die Installationsfunktion selbst prüft nicht, ob es sich um ein verwaltetes Gerät handelt – sie unterscheidet nicht zwischen einem Gerät in Intune oder einem privaten Rechner im Heimnetzwerk.

Ein möglicher, erster Schritt ist es, die Option zu deaktivieren; dazu einfach die Häkchen entfernen.

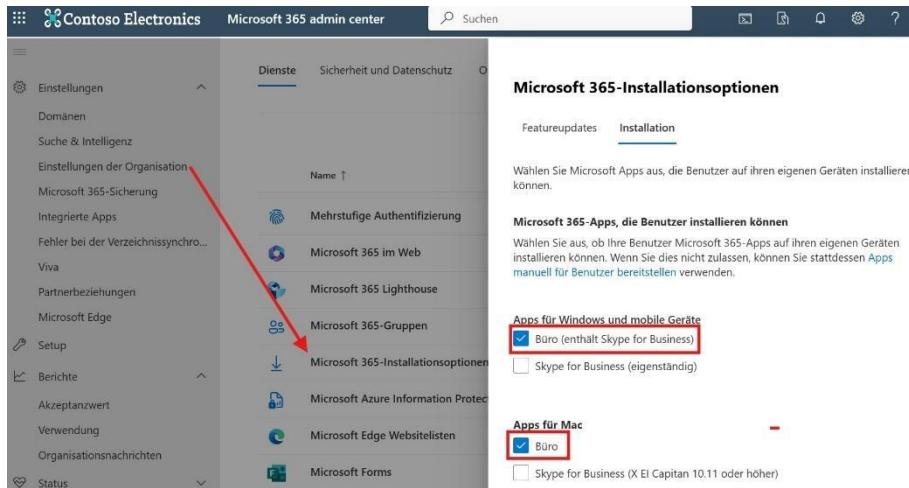


Abbildung 020

Bleibt eine Reaktion aus, wissen wir: Es bestand kein konkreter Bedarf. Falls sich hingegen jemand meldet, können wir den Anwendungsfall im Detail betrachten.

Ziel ist es, unsere **Datenfluss-Strategie** zu kontrollieren: Inhalte mit hoher Klassifizierung oder besonderer Unternehmensrelevanz sollen nicht auf unkontrollierten Geräten verarbeitet

werden. Das ist ein zentraler Baustein im Sicherheitskonzept rund um Copilot – und ein Schritt in Richtung verantwortungsvoller Datenverarbeitung.

Falls wir dennoch entscheiden, die Installationsoption aktiv zu lassen, empfiehlt sich die Kombination mit **Conditional Access** und idealerweise **Intune**. Damit können wir zumindest steuern, **wo und wie** die Office Suite verwendet wird.

Wenn jedoch die Option aktiviert bleibt und keine Conditional Access-Richtlinien greifen, ist **alles offen**: Jeder kann alles installieren – auf jedem Gerät.

Speicherlimits Einstellungen

Pfad: admin.microsoft.com → **SharePoint**

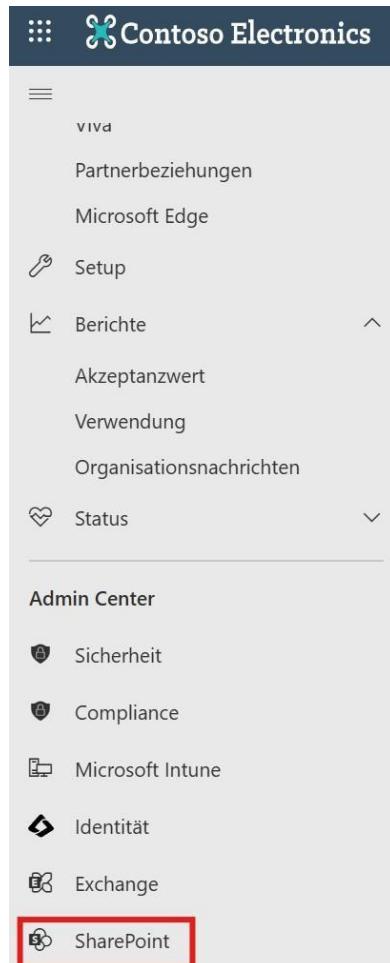
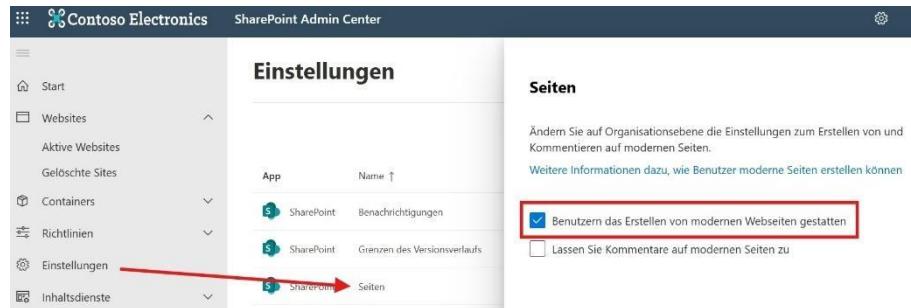


Abbildung 021

In diesem Kapitel werden wir uns zeitgleich verschiedene Einstellungen ansehen, die miteinander verknüpft. Dazu zunächst die beiden folgenden.

Pfad: admin.sharepoint.com → Einstellungen → **Seiten**



The screenshot shows the SharePoint Admin Center interface. The left sidebar has a 'Einstellungen' link under 'Inhaltsdienste' which is highlighted with a red arrow. The main content area is titled 'Einstellungen' and 'Seiten'. It contains a table with two rows: 'SharePoint Benachrichtigungen' and 'SharePoint Grenzen des Versionsverlaufs'. Below the table, there are two checkboxes: 'Benutzen das Erstellen von modernen Webseiten gestatten' (which is checked and highlighted with a red box) and 'Lassen Sie Kommentare auf modernen Seiten zu'.

Abbildung 022

Hier lässt sich steuern, ob Benutzer eigene Seiten erstellen dürfen. Direkt darunter befindet sich die Option Webseiterstellung – ein Punkt mit besonderer Bedeutung.

Pfad: admin.sharepoint.com → Einstellungen → **Websiteeinstellungen**

Die allermeisten Benutzer erstellen keine SharePoint-Seiten direkt über office.com oder die App. In der Praxis geschieht das meist im Rahmen der Zusammenarbeit über Microsoft Teams – was völlig legitim ist. Dennoch sollten wir die Erstellung von SharePoint-Seiten nicht dem Zufall überlassen, sondern **gezielt** steuern.

Idealerweise legen wir diese Seiten zentral an, entscheiden also selbst:

- wann eine Seite angelegt wird,
- mit welchen Berechtigungen und
- unter welchen Konfigurationsvorgaben.

Also kurz: Wie sieht das Lifecycle Management dahinter aus?

Benutzer sollten nicht selbstständig eigene SharePoint-Seiten erstellen können; es sei denn, sie haben konkrete Vorgaben.

Ein strukturierter Prozess – etwa über ein Ticketsystem oder einen Change-Prozess – ist hier besonders bei größeren Unternehmen sinnvoll. Ab einer Größenordnung von etwa 600 bis 1000 Benutzern aufwärts zeigt sich, wie wichtig es ist, klare Regeln für das Erstellen und Verwalten von SharePoint-Seiten zu definieren.

Empfehlung: Wenn wir die Webseiterstellung nicht aktiv gesteuert haben, empfiehlt es sich, die Option zu deaktivieren.

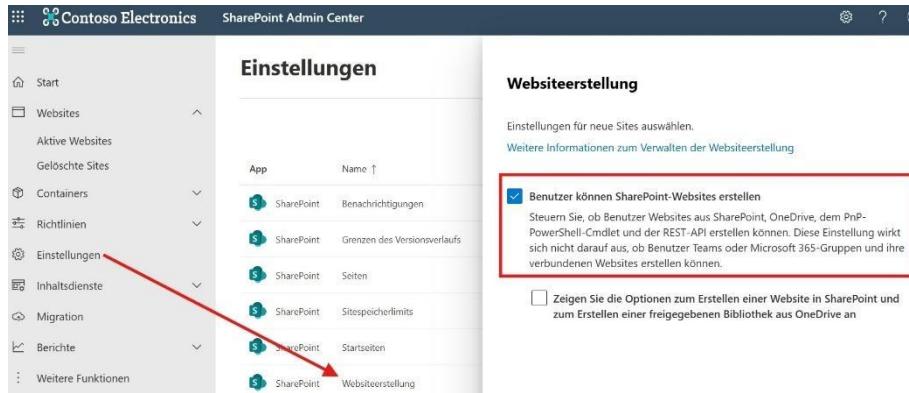


Abbildung 023

Sobald jemand eine neue SharePoint-Seite benötigen, können wir diese gezielt erstellen.

Vorteil: Während wir den aktuellen Ist-Bestand validieren, verhindern wir gleichzeitig, dass ungewollte neue Seiten oder Datenbestände entstehen.

Ziel ist es, **den Zuwachs unkontrollierter Inhalte zu unterbinden**, während wir unseren Bestand analysieren. In manchen Umgebungen wurde die Freigabe nie angepasst – in diesem Fall ist es sinnvoll, diese nun zurückzunehmen.

In der Praxis zeigt sich oft, dass viele Benutzer diese Option gar nicht vermissen. Falls sich doch jemand meldet, kann jederzeit individuell reagiert werden.

Speicherzuweisung: Automatisch vs. Manuell

Pfad: admin.sharepoint.com → Einstellungen → **Sitespeicherlimits**

Ein weiterer wichtiger Aspekt ist die Konfiguration der **Sitespeicherlimits**. Hier lässt sich festlegen, ob SharePoint den verfügbaren Speicher automatisch oder manuell zuteilt. In der Standardeinstellung steht die Option oft auf **Automatisch**.

Werfen wir dazu einen Blick auf den aktuell verfügbaren SharePoint-Speicher: Pfad: admin.sharepoint.com → Websites → **Aktive Websites**

Die Berechnung beläuft sich wie folgt:

Ein Terabyte Basis-Speicher für die Organisation plus **10 GB je lizenziertem Benutzer**. Optional kann zusätzlicher Speicher hinzugebucht werden.

Wenn wir die Speicherverteilung auf **Automatisch** belassen, besteht das Risiko, dass einzelne SharePoint-Seiten unverhältnismäßig viel Speicherplatz belegen. Gerade in einer noch unkontrollierten Umgebung können dadurch Datenablageorte und Freigaben entstehen, die wir so nicht vorgesehen haben.

Empfehlung: Setzen Sie diese Option zunächst auf **Manuell**. So behalten Sie die Kontrolle darüber, wie viel Speicher einzelnen Seiten zur Verfügung steht.

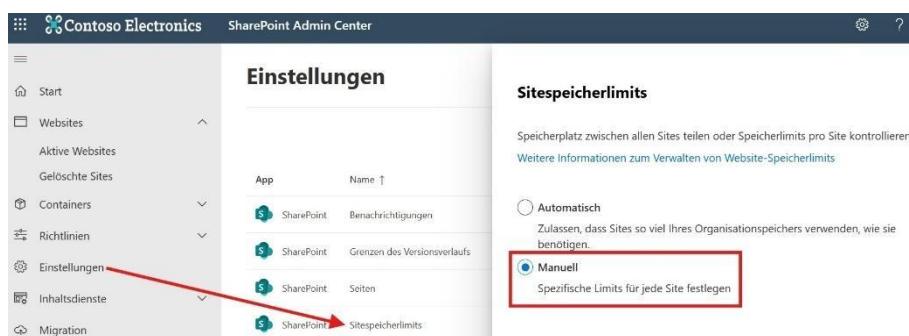


Abbildung 024

Versionierung und Speichernutzung

Pfad: admin.sharepoint.com → Einstellungen → **Grenzen des Versionsverlaufs**

The screenshot shows the SharePoint Admin Center interface. In the left sidebar, under 'Einstellungen', the 'Grenzen des Versionsverlaufs' (Version history limits) option is selected. The main content area displays a table of limits for different components. The 'Manuell' (Manual) row for OneDrive is highlighted with a red box. Below it, the 'Anzahl der Hauptversionen' (Number of major versions) field is set to '500'. The 'Zeit' (Time) dropdown is set to 'Nie (Standard)' (Never (Standard)).

Abbildung 025

Hier können wir festlegen, wie viele Versionen gespeichert werden und wie lange.

Standardmäßig wird empfohlen, die Option auf **Automatisch** zu setzen – der Speicher wird dabei durch einen intelligenten Algorithmus optimiert.

Die Option **Manuell** ist auf **500 Versionen ohne Ablaufdatum** gesetzt. Diese Einstellung kann in vielen Fällen überdimensioniert sein – insbesondere bei größeren Dateien wie PowerPoint-Präsentationen oder Projektarchiven.

Empfehlung: Setzen Sie die maximale Anzahl an Versionen manuell auf **100** und definieren Sie gleichzeitig ein Ablaufdatum – etwa nach **sechs Monaten** oder einem Jahr. Auch benutzerdefinierte Werte sind möglich.

Warum das sinnvoll ist, zeigt ein einfaches Rechenbeispiel: Wenn wir eine PowerPoint-Datei mit 100 MB bearbeiten, entsteht mit jeder Änderung eine neue Version – bei 5 Versionen sprechen wir bereits von 500 MB. Bei 500 möglichen Versionen wird der Speicherverbrauch schnell kritisch, insbesondere wenn mehrere Benutzer gleichzeitig große Dateien bearbeiten.

Deshalb sollten wir frühzeitig Rahmenbedingungen setzen, die den Speicherverbrauch aktiv begrenzen. Die Standardeinstellung von **500 Versionen ohne Ablaufdatum** kann für viele Szenarien zu großzüig sein.

OneDrive: Speichergrenzen verstehen und steuern

Pfad: admin.sharepoint.com → Einstellungen → OneDrive **Speicherlimit**

Der Standardwert liegt bei 1024 MB, der Mindestwert bei 1 TB. Ab dem fünften lizenzierten Benutzer stellt Microsoft bis zu 5 TB pro Benutzer zur Verfügung. Hier stellt sich jedoch die Frage: Ist das tatsächlich notwendig? In vielen Fällen reichen deutlich kleinere Speicherbereiche aus.

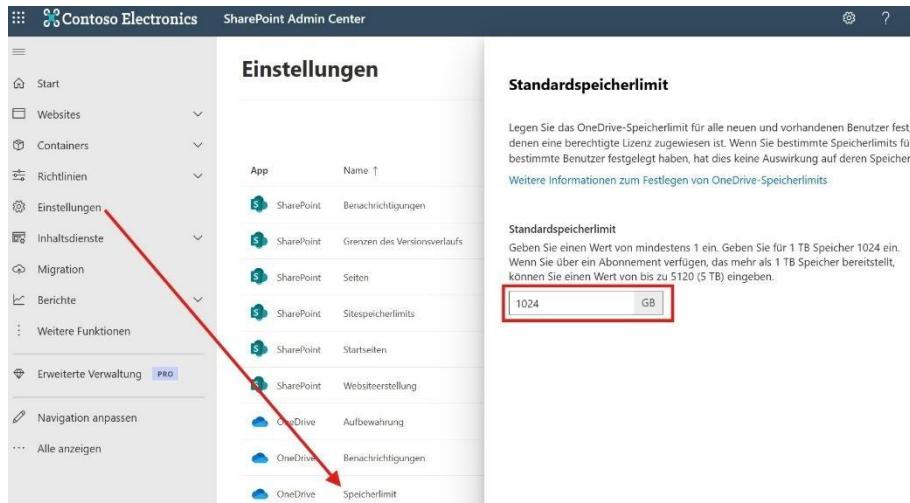


Abbildung 026

Tipp: Wir sollten genau überlegen, wie viel Speicher wir zur Verfügung stellen wollen – denn jede zusätzliche Kapazität bringt Verwaltungs- und Sicherheitsaufwand mit sich. Zugriffe müssen überwacht, Daten klassifiziert und entsprechend verarbeitet werden.

Diese Überlegungen gelten nicht nur für SharePoint, sondern ebenso für OneDrive. Auch hier sollten wir unsere Strategie bewusst definieren.

Empfehlung: Die allermeisten Benutzer benötigen in der Praxis nicht einmal 1 TB Speicherplatz – in Ausnahmefällen kann man mehr Speicherplatz zuweisen. Es lohnt sich, die Speichergrenzen bewusst zu setzen und nicht nur auf Basis der maximal möglichen Werte zu entscheiden.

Zugriffsvvalidierung und OneDrive-Synchronisation

Die folgenden Einstellungen betreffen weniger Copilot direkt, sondern vielmehr die Validierung von Zugriffen und den Schutz unserer Daten.

Pfad: admin.sharepoint.com → Einstellungen → OneDrive Synchronisieren

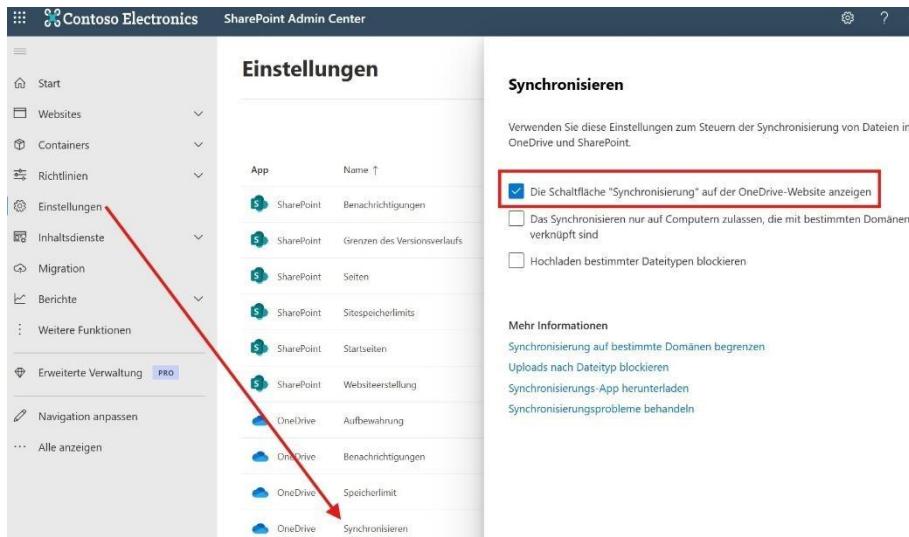


Abbildung 027

Die zentrale Frage lautet: Wollen wir es zulassen, dass Benutzer über den Web-Zugriff auch Daten herunterladen dürfen? Entscheidend ist dabei, ob der Zugriff technisch auf **verwaltete Unternehmensgeräte** beschränkt ist.

Wenn das nicht der Fall ist, kann es sinnvoll sein, die Synchronisierungsfunktion zunächst zu deaktivieren – und schrittweise wieder zu aktivieren, sobald klar ist, wie die Zugriffssituation geregelt ist.

Diese Einschränkung scheint auf den ersten Blick sehr restriktiv, sorgt jedoch für mehr Kontrolle und reduziert das Risiko unkontrollierter Datenflüsse.

Tipp: Wir könnten auch grundsätzlich einschränken, **wer überhaupt auf OneDrive zugreifen darf**. Hier bietet das Admin Center unter dem Pfad: admin.sharepoint.com → **Richtlinien** die drei Optionen:

- Teilen
- Zugriffssteuerung
- Website-Lebenszyklusverwaltung

Der Bereich **Website-Lebenszyklus-Verwaltung** wird jedoch nur angezeigt, wenn die **Erweiterte Verwaltung** aktiviert ist bzw. die Lizenz dafür erworben wurde.

Empfehlung: Ich empfehle, diese Lizenz für Ihr Unternehmen zu erwerben, sollte sie, zum Zeitpunkt dieses eBooks, nicht bereits Bestandteil der Copilot-Lizenz sein. Ohne diese Funktion lassen sich bestimmte Richtlinien nicht umsetzen, die für eine saubere und konforme Copilot-Einführung erforderlich sind.

Wer Reports, Richtlinien und weiterführende Konfigurationen für Copilot plant, wird auf diese Funktion nicht verzichten können. Sie wird zum **zentralen Bestandteil einer sicheren, steuerbaren Umgebung**.

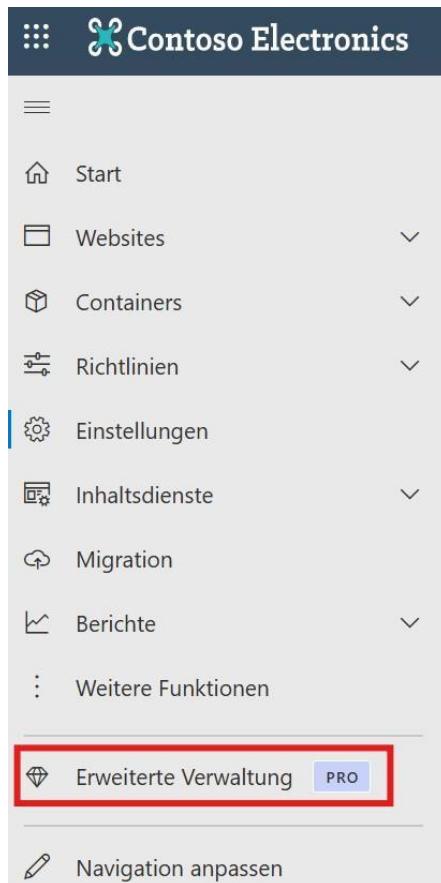


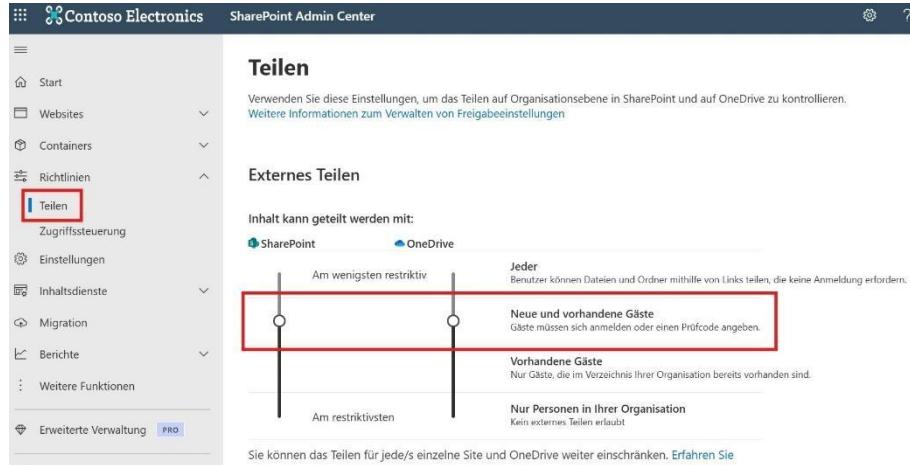
Abbildung 028

SharePoint, OneDrive und erweiterte Ansichten

Pfad: admin.sharepoint.com → Richtlinien → Teilen

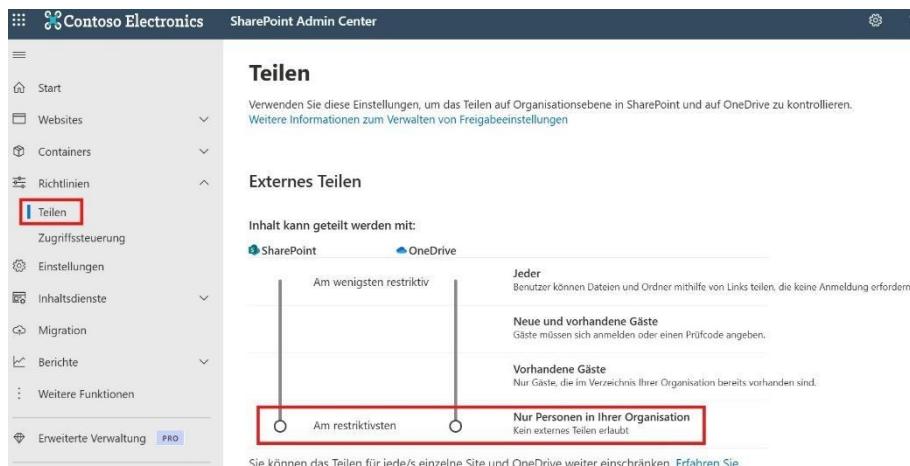
Die bekannten Optionen wie **Jeder**, **Neue und vorhandene Gäste**, **Vorhandene Gäste** und **Nur Personen in Ihrer Organisation** sind Teil der erweiterten Ansicht, die wir bereits in den Organisationseinstellungen gesehen haben.

Hier können wir zudem im SharePoint den Zugriff herunterregeln, der dann automatisch für OneDrive angepasst wird. **OneDrive kann nicht höher eingestuft werden als SharePoint** – das wird systemseitig abgelehnt.



The screenshot shows the SharePoint Admin Center interface under the 'Teilen' (Share) section. On the left, there's a navigation menu with 'Teilen' selected. The main content area is titled 'Teilen' and contains instructions about using these settings to control sharing at the organization level in SharePoint and OneDrive. It highlights the 'Externes Teilen' (External Sharing) section. A diagram shows a spectrum from 'Am wenigsten restriktiv' (Least restrictive) to 'Am restriktivsten' (Most restrictive). The 'Jeder' (Everyone) option is at the most restrictive end, which is highlighted with a red box. Other options shown are 'Neue und vorhandene Gäste' (New and existing guests), 'Vorhandene Gäste' (Existing guests), and 'Nur Personen in Ihrer Organisation' (Only people in your organization).

Abbildung 029

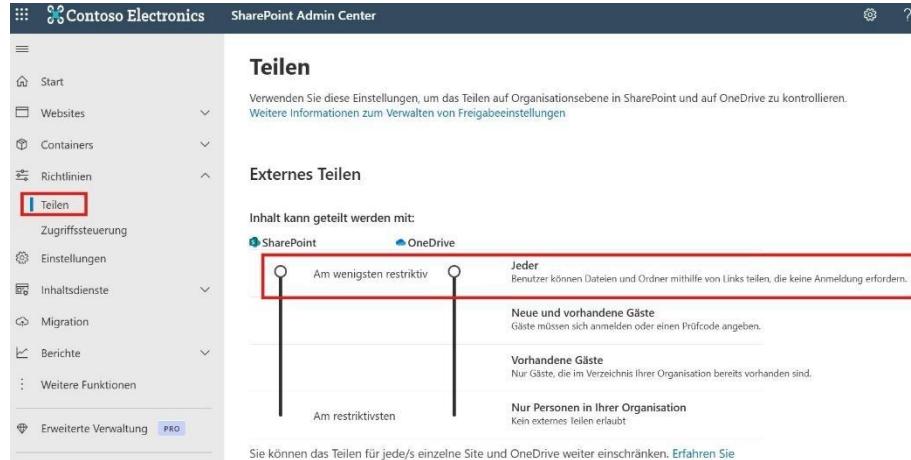


This screenshot is identical to Abbildung 029, showing the 'Teilen' (Share) settings in the SharePoint Admin Center. The 'Nur Personen in Ihrer Organisation' (Only people in your organization) option is highlighted with a red box, indicating it is the most restrictive setting available.

Abbildung 030

Optionen zur externen Freigabe

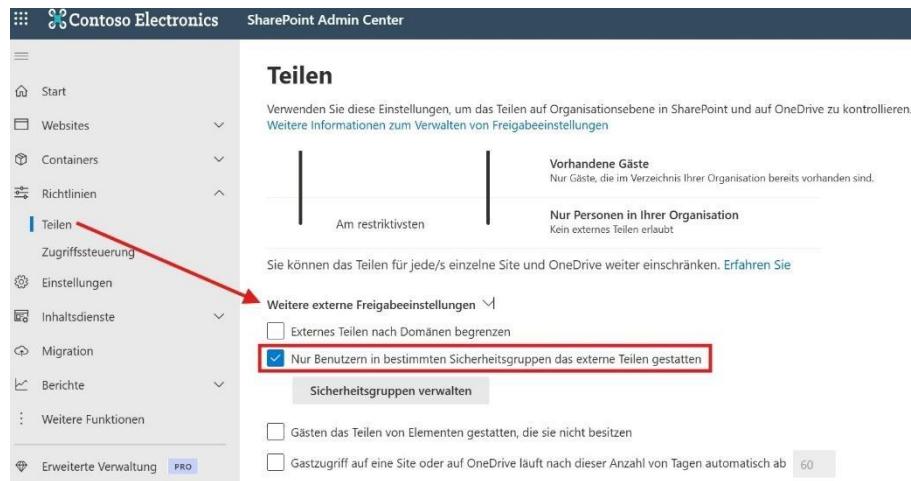
Setzen wir die Option auf **Jeder** werden uns alle Möglichkeiten zur Freigabe angezeigt.



The screenshot shows the SharePoint Admin Center under the 'Teilen' (Sharing) section. It displays sharing options for both SharePoint and OneDrive. The 'Jeder' (Everyone) option is selected, highlighted with a red box. Below it, other options like 'Neue und vorhandene Gäste' (New and existing guests) and 'Vorhandene Gäste' (Existing guests) are shown. A note at the bottom says 'Sie können das Teilen für jede/s einzelne Site und OneDrive weiter einschränken. Erfahren Sie' (You can further restrict sharing for each individual site and OneDrive. Learn more).

Abbildung 031

Einige Punkte, über die wir dabei jedoch nachdenken sollten:



This screenshot shows the same 'Teilen' (Sharing) section, but with a red arrow pointing to the 'Weitere externe Freigabeeinstellungen' (Additional external sharing settings) dropdown. Inside, the checkbox 'Nur Benutzern in bestimmten Sicherheitsgruppen das externe Teilen gestatten' (Allow external sharing only to users in specific security groups) is checked and highlighted with a red box. Other options like 'Externes Teilen nach Domänen begrenzen' (Restrict external sharing by domain) and 'Gästen das Teilen von Elementen gestatten, die sie nicht besitzen' (Allow guests to share items they don't own) are also visible.

Abbildung 032

- **Externes Teilen nach Domänen begrenzen:** Diese Option ist oft sinnvoll, um den Zugriff gezielt einzuschränken.

- **Sicherheitsgruppen verwenden:** Wer mit vielen Partnerunternehmen arbeitet, kann durch Sicherheitsgruppen besser definieren, wer überhaupt extern teilen darf.

In der Praxis kann es schwierig sein, eine vollständige Domänenliste zu pflegen – vor allem bei vielen externen Kontakten. Aber wenn wir nicht in dieser Situation sind, ist die Einschränkung über Sicherheitsgruppen ein valider Ansatz. Mitglieder einer Sicherheitsgruppe können gezielt vom Teilen ausgeschlossen oder eingeschränkt werden – eine Funktionalität, die sich in vielen Szenarien bewährt hat.

Empfehlung: Die Option **Gästen das Teilen von Elementen gestatten, die sie nicht besitzen** ist standardmäßig aktiviert. Deaktivieren Sie diese Option – Inhalte sollten ausschließlich durch aktive Freigabe interner Benutzer geteilt werden.



Abbildung 033

Der nächste Punkt dreht sich um Gastzugriffe einer Site oder OneDrive – ergänzt durch den nächsten Punkt; eine erneute **Re-Authentifizierung**. Wie geht man richtig vor?

Das Prinzip lautet:

So wenig Zugriff wie nötig – nur so lange wie nötig.

Idealerweise aktivieren wir beide Optionen, um sicherzustellen, dass Gastzugriffe nicht unbegrenzt bestehen. Wenn beispielsweise ein Guest nach 30 Tagen erneut einen Prüf-Code eingeben muss, ist das bereits ein Schutzmechanismus.

Interne und externe Freigaben steuern

Auch die interne Freigabe sollte strukturiert erfolgen. Ich empfehle, die folgenden Optionen auszuwählen:

Pfad: admin.sharepoint.com → Richtlinien → Teilen



Abbildung 034

Eine externe Freigabe – oder eine Freigabe mit Schreibrechten – sollte nur **bewusst** erfolgen. Der Benutzer sollte sich aktiv dafür entscheiden, statt standardmäßig volle Berechtigungen zu vergeben. Nur so lässt sich verhindern, dass Inhalte unnötig oder ungewollt bearbeitet oder weitergegeben werden. Das gilt auch für Leserechte.

Empfehlung: Freigaben sollten grundsätzlich **restriktiv** voreingestellt sein. Es ist nicht praktikabel, sich darauf zu verlassen, dass Benutzer immer an den richtigen Freigabetyp denken. Wir müssen als Organisation den Rahmen vorgeben, der standardmäßig die sicherste Variante nutzt. So schaffen wir Verlässlichkeit und vermeiden unbeabsichtigte Datenfreigaben.

Wenn wir mit dem **Jeder-Link** arbeiten (z. B. aus organisatorischen Gründen), sollten wir **mindestens ein Ablaufdatum** definieren. Auch bei notwendiger externer Freigabe – etwa bei Ordnern oder Einzeldokumenten – sollte der Zugriff zeitlich befristet sein.

Jeder-Link und Copilot-Auswirkungen

Die Nutzung des **Jeder-Links** bringt zusätzliche Herausforderungen mit sich – insbesondere im Zusammenspiel mit Microsoft 365 Copilot.

Wird ein Dokument oder Ordner intern über den Jeder-Link geteilt, kann Copilot **auf diese Inhalte zugreifen**. Sobald in einem Prompt Schlagwörter verwendet werden, die zu diesem Dokument passen, besteht die Möglichkeit, dass Copilot es als Ergebnis einblendet – **selbst wenn der ursprüngliche Zugriff nicht bewusst eingerichtet wurde**.

Deshalb spreche ich nochmal die klare Empfehlung aus, **auf den Jeder-Link zu verzichten** – auch intern. Die potenziellen Auswirkungen auf Datenschutz, Transparenz und Berechtigungsstruktur sind nicht zu unterschätzen.

Zugriffssteuerung und Conditional Access

Pfad: admin.sharepoint.com → Richtlinien → **Zugriffssteuerung**

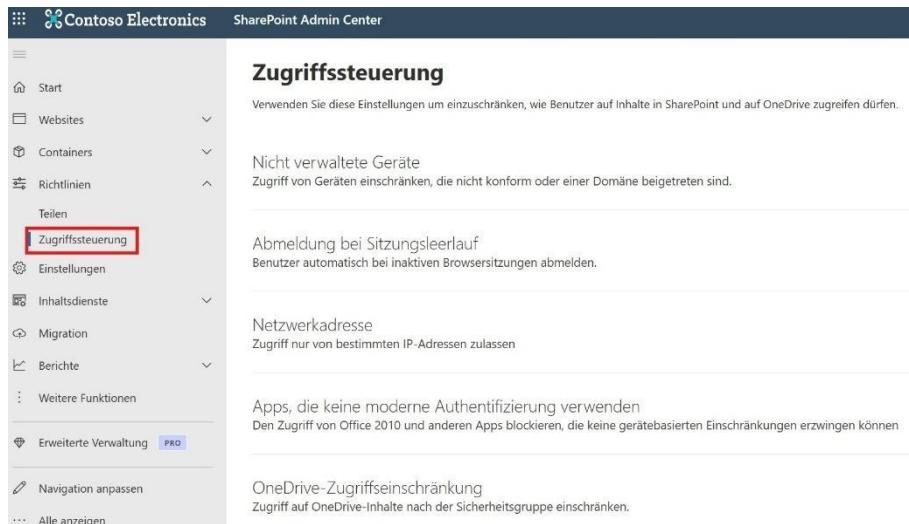


Abbildung 035

Durch das Klicken der einzelnen Optionen lassen sich **individuelle** Richtlinien festsetzen. Diese Regeln können bereits ohne Conditional Access konfiguriert werden und bieten grundlegenden Schutz – vor allem für Umgebungen, die über keine Conditional Access-Lizenzen verfügen.

Auch hier nochmal der Hinweis, dass verschiedene Optionen, wie *Zugriffeinschränkung auf Websiteebene* nur mit der Lizenz zur *Erweiterten Verwaltung* im Tenant aktiviert wurde.

Ich empfehle dennoch, diesen Bereich im Zusammenspiel mit Conditional Access weiter auszubauen, um granulare Steuerung zu ermöglichen. Conditional Access ist Stand April 2025 das

mächtigste Werkzeug zur Absicherung der Microsoft 365 Umgebung – insbesondere im Kontext von Microsoft 365 Copilot.

Verknüpfung und Speicherverbrauch

Pfad: admin.sharepoint.com → Websites → Aktive Websites → **Verwendeter Speicher** → sortieren von groß nach klein

Hier sehen wir die Übersicht der SharePoint-Seiten mit zugehörigem Webseitennamen und URL – inklusive Information, ob sie an ein Microsoft 365 Team gekoppelt sind oder als Einzelseite bestehen.

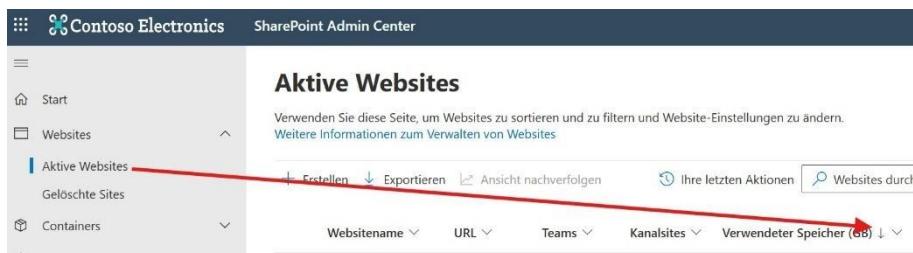


Abbildung 036

Ein oft unterschätzter Aspekt ist dabei der **Speicherverbrauch** dieser Seiten. Gerade bei der Entscheidung, ob Seiten weitergeführt oder bereinigt werden sollen, ist die Kopplung an Teams sowie die Speichermenge ein wichtiger Indikator.

In der Speicheranalyse zeigt sich häufig folgendes Bild: Einzelne Seiten belegen 500 MB, 400 MB, 150 MB – danach folgen kleinere Sprünge: 82 MB, 4 MB, 2 MB, 1 MB oder weniger.

Diese Entwicklung lässt sich nutzen, um gezielt zu prüfen, welche Seiten **aktiv genutzt** werden – und welche möglicherweise **überflüssig geworden sind**.

Viele Unternehmen nutzen automatisiert erstellte Projektseiten. Auch hier ist die ursprüngliche Idee nachvollziehbar: Projekte sollen einen gemeinsamen Raum zur Zusammenarbeit erhalten. In der Realität zeigt sich jedoch oft, dass diese Seiten **nicht aktiv genutzt werden**. Eine Alternative ist, von einer automatischen Erstellung auf ein **Opt-in-Modell** umzusteigen: Projektseiten entstehen nur noch auf Wunsch – nicht mehr automatisch.

Wichtig ist dabei auch das Thema **Lifecycle-Management**:

- Wann wird eine Seite archiviert oder gelöscht?
- Was passiert mit ungenutzten Daten?
- Wie lange bleiben inaktive Seiten bestehen?

Diese Fragen sollten bei jeder Governance-Strategie für SharePoint einbezogen werden – idealerweise durch **klare Richtlinien und automatisierte Prozesse**.

Zugriffsmanagement in der Praxis

Zugriffsmanagement spielt auch bei Projektseiten eine Rolle. Wenn niemand mehr aus dem ursprünglichen Projektteam im Unternehmen ist, kann nur ein Administrator Zugriffe neu freigeben.

Die eigentliche Datenmenge – ob in Gigabyte oder Terabyte – ist nicht das Entscheidende. Entscheidend ist: **Wie gut lassen sich diese Daten verwalten?**

Schon 100 MB können problematisch sein, wenn sie sensible Informationen enthalten.

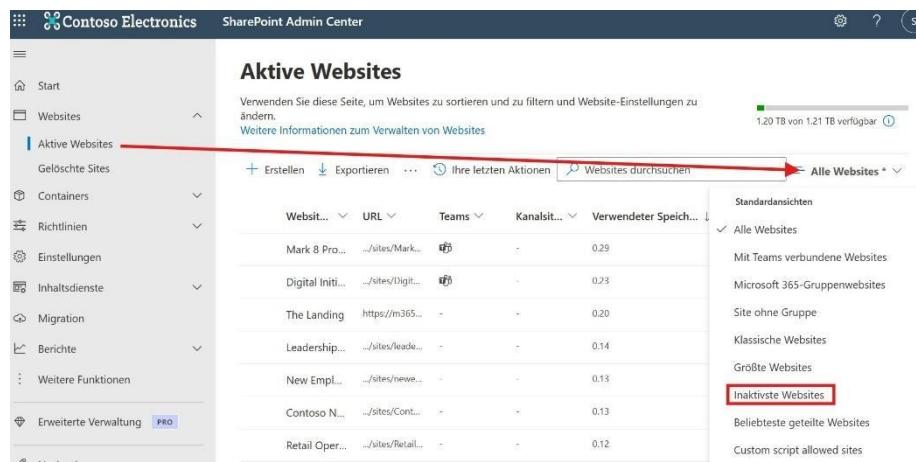
Wenn darin beispielsweise ein zentrales Firmengeheimnis gespeichert ist, ist es kritischer als 10 Terabyte an Bildern vom letzten Teamevent.

Diese Unterscheidung hilft, Prioritäten bei der Speicher- und Zugriffsverwaltung richtig zu setzen.

Seitenaufrufe und Aktivitätsdaten verstehen

Auf der rechten Seite können wir die Websites filtern:

Pfad: admin.sharepoint.com → Websites → **Aktive Websites** → Alle Websites



Website	URL	Teams	Kanäle	Verwendeter Speicher
Mark 8 Pro...	./sites/Mark...	-	-	0.29
Digital Initi...	./sites/Digit...	-	-	0.23
The Landing	https://m365...	-	-	0.20
Leadership...	./sites/leader...	-	-	0.14
New Empl...	./sites/newe...	-	-	0.13
Contoso N...	./sites/Conto...	-	x	0.13
Retail Oper...	./sites/Retail...	-	-	0.12

Abbildung 037

Hier können wir über die Ansicht **Aktive Websites** auf der rechten Seite verschiedene Filter nutzen – zum Beispiel nach **größten Websites** oder **inaktivsten Websites**.

Durch die Kombination aus **Seitenaufrufen**, **letztem Aktivitätsdatum** und **verwendetem Speicher** ergibt sich ein aussagekräftiges Bild. So lässt sich schnell erkennen, welche Seiten wahrscheinlich **nicht mehr benötigt werden** – insbesondere solche ohne Pageaufrufe, ohne Aktivität und ohne Speicherverbrauch.

Das Aktivitätsdatum wird durch verschiedene Vorgänge ausgelöst:

- Hochladen von Dateien
- Bearbeiten von Inhalten
- Hinzufügen von Benutzern

Die Verlässlichkeit dieser Daten liegt laut Erfahrungswerten bei etwa **60 %** – ein guter Richtwert, aber kein absoluter Beweis für Relevanz.

Bewertung von Anzeigefehlern und Datenlücken

In der Praxis kann es zu **Anzeigefehlern** kommen: Seiten mit realer Nutzung erscheinen als inaktiv, weil die Erfassung nicht korrekt war. Fehlt zum Beispiel ein Wert im Feld Seitenaufrufe – obwohl die Seite intensiv genutzt wird – liegt mit hoher Wahrscheinlichkeit ein Fehler in der Darstellung vor.

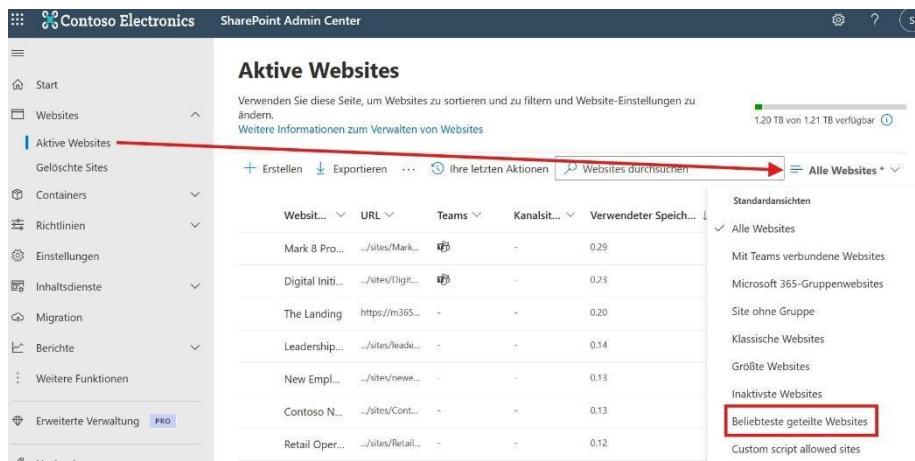
Deshalb ist eine rein datengetriebene Entscheidung **nicht ausreichend**. Wir müssen zusätzlich überlegen:

- Welche Seiten erfüllen noch einen Zweck?
- Was könnte übersehen worden sein?

Diese Art von **Cleanup-Aktion** braucht Zeit. **Datenbereinigung ist ein fortlaufender Prozess**, der Planung und saubere Validierung erfordert.

Beliebteste geteilte Webseiten

Pfad: admin.sharepoint.com → Websites → **Aktive Websites** → Alle Websites



Website	URL	Teams	Kanäle	Verwendeter Speicherplatz
Mark 8 Pro...	.../sites/Mark...	✗	-	0.29
Digital Initi...	.../sites/Digit...	✗	-	0.23
The Landing	https://m365...	-	✗	0.20
Leadership...	.../sites/leader...	-	✗	0.14
New Empl...	.../sites/newem...	-	✗	0.13
Contoso N...	.../sites/Conto...	-	✗	0.13
Retail Oper...	.../sites/Retail...	-	✗	0.12

Abbildung 038

Im nächsten Schritt lohnt es sich, die **Spalten „Seitenbesuche“ und „Externe Freigaben“** zu aktivieren. Hier können wir nachverfolgen, welche Seiten kürzlich besucht wurden und bei welchen externen Freigaben bestehen.

Diese Informationen helfen, die Bedeutung einzelner Seiten einzuordnen: Seiten mit vielen Besuchen und aktiven Freigaben werden **vermutlich weiterhin benötigt**, während Seiten ohne Aktivität **potenziell obsolet sind**.

Diese Übersicht ist entsprechend ein hilfreicher Indikator für die Entscheidung, **welche SharePoint-Seiten aktiv bleiben sollen** und welche entfernt oder archiviert werden können.

Erweiterte Verwaltung und Berichterstattung

Berichte unterstützen bei der Kontrolle von Datenzugriffen und Linkfreigaben. Sie ermöglichen die Bewertung der Copilot-Indexierung, das Lifecycle-Management von Sites sowie die Definition von Ownership- und Inaktivitätsrichtlinien.

Pfad: admin.sharepoint.com → **Erweiterte Verwaltung**

Im Bereich **Erweiterte Verwaltung** stehen uns zusätzliche Optionen zur Verfügung, die aktuell möglicherweise nicht sichtbar sind, weil die Funktion noch nicht aktiviert wurde.

Hier erscheint zunächst ein sogenanntes **Started File**, das den Zugriff auf weiterführende Funktionen ermöglicht.

Nach dem Aufruf zeigt die Übersicht verschiedene Inhalte, die teilweise Verlinkungen in andere Admin-Center enthalten. In der Regel erfolgt an dieser Stelle keine Konfiguration, sondern eine Weiterleitung oder eine vorbereitende Information.

Berichtswesen zur Analyse von Veränderungen

Ziel dieser Oberfläche ist der Aufbau eines strukturierten **Berichtswesens**. Es geht darum, nachzuvollziehen:

- Welche Änderungen wurden an SharePoint-Websites vorgenommen?
- Welche Seiten sind neu entstanden, wurden gelöscht oder verändert?
- In welcher Form und Intensität wird die Umgebung durch Benutzer genutzt?

Diese Informationen dienen uns als Grundlage für fundierte Entscheidungen zur **Ressourcenbewertung und Governance**. Sie unterstützen uns dabei, die Ergebnisse vorheriger Prüfungen – wie Seitenaktivität oder Speicherverbrauch – mit konkreten Verwaltungsdaten zu verknüpfen und strategisch einzuordnen.

Berichte zur Datenzugriffs-Governance und Linknutzung

Pfad: admin.sharepoint.com → **Erweiterte Verwaltung**

In der erweiterten Verwaltung steht uns der Bereich **Datenzugriffs-Governance** zur Verfügung. Hier können wir über den Eintrag **Berichte zu Datenzugriffs-Governance** direkt zu den zugehörigen Reports wechseln.

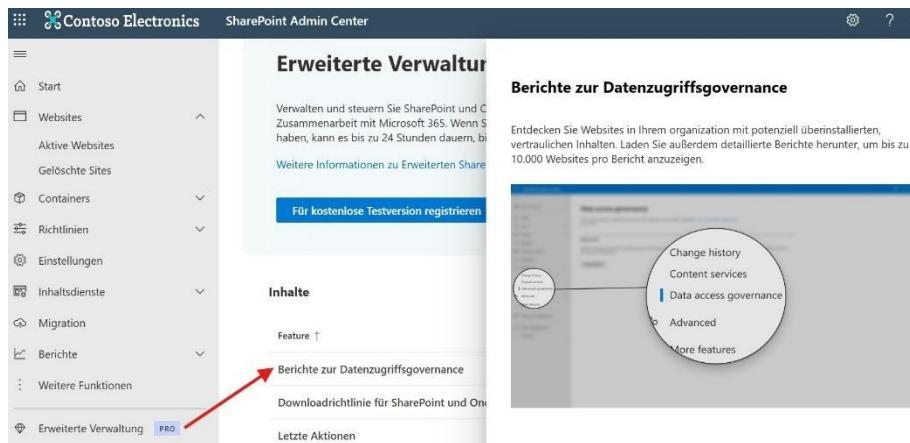
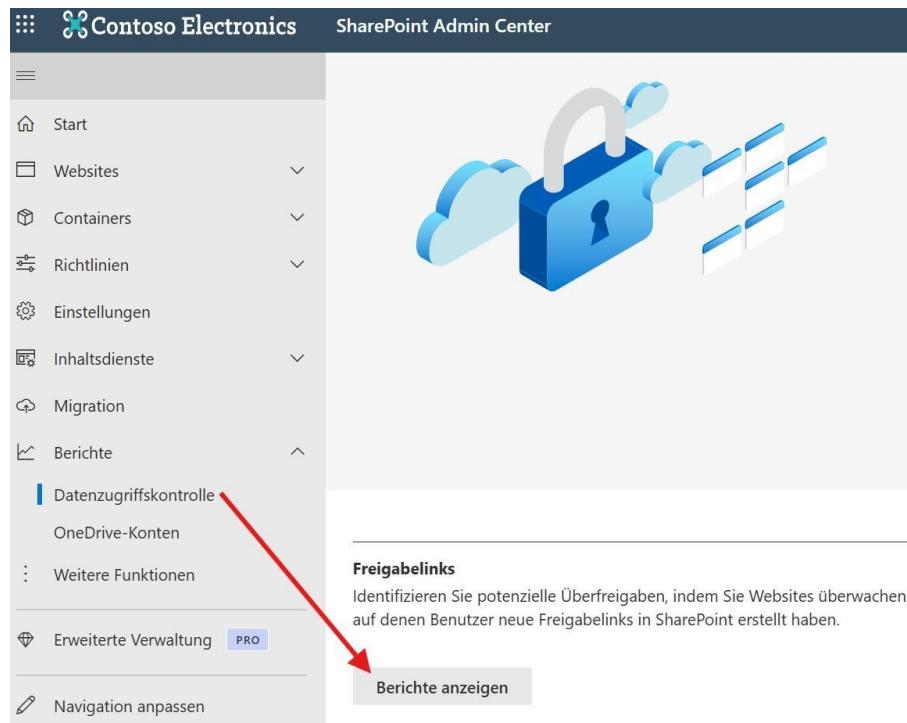


Abbildung 039

Pfad: admin.sharepoint.com → Berichte → Datenschutzkontrolle → Freigabelinks → **Berichte anzeigen**

Unter dem Punkt **Datenzugriffs-Kontrolle** sehen wir Berichte wie **Freigabe-Links** sowie Inhalte, die mit bestimmten Benutzergruppen geteilt wurden.

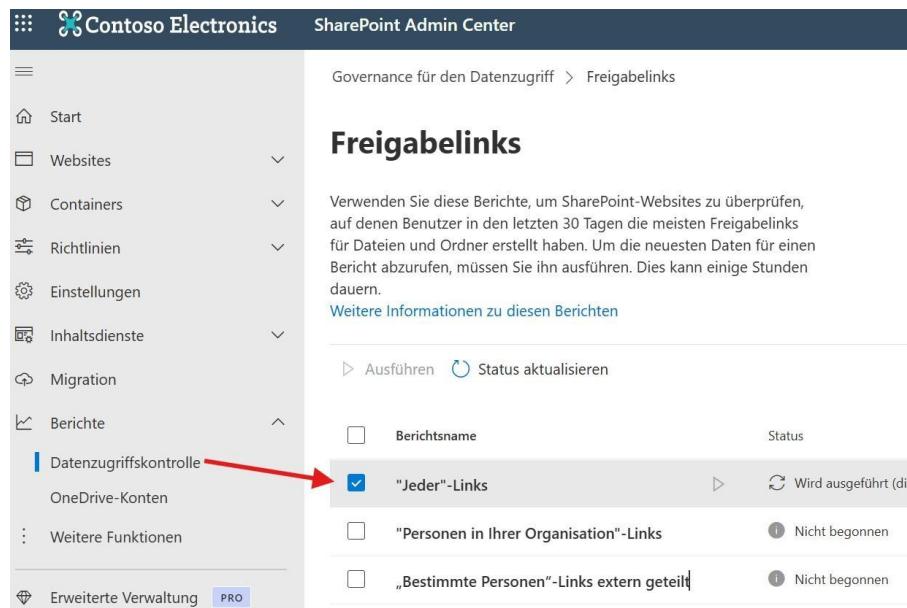
Wir haben damit die Möglichkeit, zentral zu prüfen, welche Arten von Freigabelinks in unserem Tenant aktiv verwendet werden.



The screenshot shows the SharePoint Admin Center interface for Contoso Electronics. On the left, there's a navigation menu with items like Start, Websites, Containers, Richtlinien, Einstellungen, Inhaltsdienste, Migration, Berichte, and Erweiterte Verwaltung. The 'Berichte' item is expanded, showing 'Datenzugriffskontrolle' (which is highlighted with a blue bar) and other options like OneDrive-Konten and Weitere Funktionen. A red arrow points from the 'Datenzugriffskontrolle' link down to the 'Berichte anzeigen' button on the right. The main content area features a lock icon and the text 'Freigabelinks'.

Abbildung 040

Alternativ zu PowerShell-Skripten lässt sich die Analyse **komfortabel über die Weboberfläche** durchführen. Wir können einzelne oder alle Berichte auswählen und hier direkt über das Symbol *Bericht ausführen* starten.



The screenshot shows the 'Freigabelinks' report page in the SharePoint Admin Center. The left navigation menu is identical to Abbildung 040. The main content area is titled 'Freigabelinks' and contains instructions on how to use the reports to check SharePoint websites for potential over-sharing. It includes a 'Weitere Informationen zu diesen Berichten' link, an 'Ausführen' button, and a 'Status aktualisieren' button. Below this, a table lists reports with their names and statuses. The first report, "'Jeder'-Links", is checked and has a status of 'Wird ausgeführt (dies)', indicated by a grey bar. A red arrow points from the 'Datenzugriffskontrolle' link in the navigation to this checked report row.

Berichtsname	Status
"Jeder"-Links	Wird ausgeführt (dies)
"Personen in Ihrer Organisation"-Links	Nicht begonnen
„Bestimmte Personen“-Links extern geteilt	Nicht begonnen

Abbildung 041

Nach Auswahl eines Berichts erhalten wir Informationen darüber,

- welche Seiten betroffen sind
- wie häufig bestimmte Linktypen verwendet wurden

Die Ergebnisse stehen als **CSV-Datei** zur Verfügung und lassen sich anschließend weiterverarbeiten.

Interne Freigabe und Copilot-Indexierung

Pfad: admin.sharepoint.com → Berichte → Datenschutzkontrolle → Für „Jeder außer externen Benutzern“ freigegebenen Inhalte → **Berichte anzeigen**

Ein kritischer Punkt betrifft Inhalte, die mit **allen Personen in der Organisation** geteilt wurden. Auch wenn kein externer Zugriff besteht, werden diese Dokumente von **Copilot indexiert**, sobald der Benutzer dafür lizenziert ist.

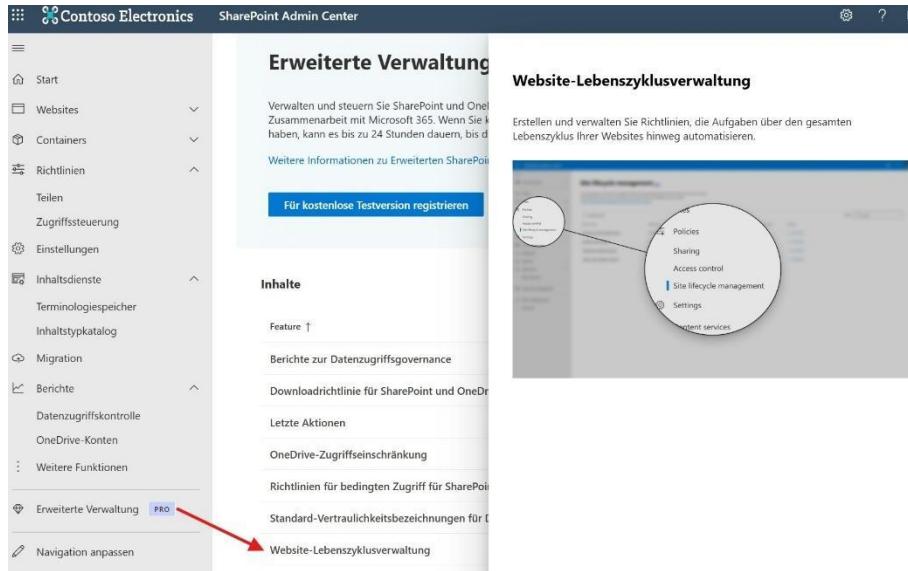
Die Frage ist daher: **Wollen wir das?**

In vielen Fällen nicht. Selbst wenn kein Missbrauch vorliegt, möchten wir möglicherweise nicht, dass bestimmte Inhalte intern **flächendeckend auffindbar** sind.

Beim Erstellen eines Berichts wird standardmäßig der Zeitraum der **letzten 28 Tage** berücksichtigt. In diesem Rahmen sehen wir, welche Inhalte mit *Jeder* geteilt, aber noch nicht von Externen aufgerufen wurden.

Side Lifecycle Management und Site Level Access Restriction

Pfad: admin.sharepoint.com → Erweiterte Verwaltung → **Website-Lebenszyklusverwaltung**



The screenshot shows the SharePoint Admin Center interface. On the left, there's a navigation pane with various options like Start, Websites, Containers, Richtlinien, Teilen, Zugriffssteuerung, Einstellungen, Inhaltsdienste, Migration, Berichte, and Erweiterte Verwaltung (which has a 'PRO' badge). The main content area is titled 'Erweiterte Verwaltung' and contains sections for 'Weiteren Informationen zu Erweiterten SharePoint-Richtlinien', 'Für kostenlose Testversion registrieren', and 'Inhalte'. Below these are links for 'Feature', 'Berichte zur Datenzugriffsgovernance', 'Downloadrichtlinie für SharePoint und OneDrive', 'Letzte Aktionen', 'OneDrive-Zugriffseinschränkung', 'Richtlinien für bedingten Zugriff für SharePoint', 'Standard-Vertraulichkeitsbezeichnungen für Dokumente', and 'Website-Lebenszyklusverwaltung'. A red arrow points from the 'Erweiterte Verwaltung' link in the navigation to the 'Website-Lebenszyklusverwaltung' section.

Abbildung 042

Hier können wir zwei Richtlinien definieren:

- Inactive Site Policy
- Site Ownership Policy.

Inactive Site Policy und Berichtserstellung

Über **Inactive Site Policy** können wir nun via → **Create Policy** einen neuen Bericht erstellen.



The screenshot shows the 'Website-Lebenszyklusverwaltung' page. It has two main sections: 'Inactive site policies' (with 3 policies listed) and 'Richtlinien zum Besitz von Websites' (with 1 policy listed). Each section has a 'Create and configure policies to:' list and an 'Öffnen' button. A red box highlights the 'Öffnen' button under 'Inactive site policies'.

Abbildung 043

Wir sehen zunächst auf der linken Seite eine Übersicht, die uns durch den Prozess leiten wird.



Abbildung 044

Im **ersten Schritt** können wir die Daten aus den **Active Sites** über eine erweiterte Konfiguration validieren. Hier lassen sich Richtlinien definieren, wie mit inaktiven Seiten verfahren werden soll.

Wir haben die Möglichkeit festzulegen, dass bei fehlender Aktivität eine **Benachrichtigung an die jeweiligen Site-Administratoren oder -Owner** versendet wird. Darüber hinaus lässt sich automatisieren, ob die betroffene Seite beispielsweise **archiviert** oder in den **Read-only-Modus** versetzt werden soll.

Im **zweiten Schritt** *Bereich* geht es um die Einrichtung der *Inactive Site Policy*. Wir legen zunächst fest, nach welchem Zeitraum ohne Aktivität eine Seite als inaktiv gilt. Zur Auswahl stehen: 1, 2, 3 oder 6 Monate.

Empfehlung: Beginnen Sie mit 6 Monaten. Auf dieser Basis lassen sich erste Erfahrungen sammeln.

Anschließend können wir den Zeitraum auf 3 Monate reduzieren und die Kriterien schärfen.

Dann definieren wir, welche Arten von Seiten in die Prüfung einbezogen werden sollen.

Dazu zählen:

Richtlinienbereich festlegen

Wie lange nach der letzten Aktivität sollte eine Website als inaktiv betrachtet werden?

Umfasst Aktivitäten auf der Website, Dateien und alle verbundenen Ressourcen wie Microsoft Teams, Viva Engage oder Exchange.

3 Monate ▾

Which sites should be checked for inactivity? *

OneDrive sites are excluded automatically.

Websitevorlagen auswählen

Alles auswählen

Klassische Websites

Kommunikationswebsites

Verbundene Websites ohne Teams gruppieren

Teamwebsites ohne Microsoft 365-Gruppe

Mit Teams verbundene Websites

Is this section helpful in setting the scope of this policy?  

Abbildung 045

Auch wenn wir bestimmte Seitentypen – etwa Classic Sites – aktuell nicht nutzen, sollten wir sie in die erste Analyse einbeziehen. Das verschafft uns einen **vollständigen Überblick**.

Schritt 3: Konfiguration. Jetzt definieren wir, wer bei Inaktivität per E-Mail benachrichtigt werden soll.

Hier stehen zwei Optionen zur Verfügung:

- Site-Owner
- Admins

Tipp: Site-Owner und Administratoren müssen nicht identisch sein. Diese Unterscheidung sollten wir bei der Auswahl berücksichtigen – abhängig davon, wer in unserem Unternehmen die Verantwortung für das weitere Vorgehen trägt.

Richtlinie konfigurieren

Who should be notified via email if site has been inactive? *

Recipients will be able to certify the site to keep it active.

 Site owners Site admins

What action should the policy take on inactive sites that have not been certified by site owners or site admins after 3 notifications? *

(i) Enforcement actions cannot be edited after policy creation

 Do nothing Take an enforcement

Abbildung 046

Im Anschluss legen wir fest, welche Maßnahmen ergriffen werden sollen, wenn eine Seite als inaktiv erkannt wurde. Zur Auswahl stehen:

- **Do nothing** – es erfolgt keine Aktion
- **Take an enforcement** – Auswahl zwischen:
 - **Read-only access**: Die Seite bleibt zugänglich, kann aber nicht mehr bearbeitet werden
 - **Archive sites after mandatory read-only period**: Die Seite wird nach Ablauf des *Read-only*-Zeitraums archiviert

Besonders zu beachten ist:

Die Archivierung von SharePoint-Seiten ist **kostenpflichtig**. Sie ist nicht Bestandteil einer Microsoft 365-Lizenz, sondern erfordert separate Abrechnung pro Speicherbedarf.

Vor diesem Hintergrund kann es sinnvoll sein, zunächst mit *Read-only access* zu arbeiten. Diese Option bewahrt den Zugriff, reduziert aber das Risiko unkontrollierter Änderungen – und verursacht keine zusätzlichen Kosten.

Site Ownership Policies und Berichtserstellung

Die ersten beiden Schritte unterscheiden sich nicht von der Berichterstellung für *Inactive Sites*. Im **dritten** Schritt jedoch, können wir nun festlegen, wer informiert werden soll: Owner oder Admin.

Richtlinie konfigurieren

Wer sollte für die einzelnen Websites verantwortlich sein? *

Besitzer der Website

Administratoren der Website

Mindestanzahl von Besitzern oder Administratoren, die für jede Website erforderlich sind *

2

Abbildung 047

Diese Einstellung wird im System mit dem Wert 2 (*Recommended*) hinterlegt – und genau das ist auch meine Empfehlung. Ein zweiter Owner sorgt für Redundanz und Kontinuität, besonders wenn eine Person das Unternehmen verlässt oder nicht verfügbar ist. Administrative Aufgaben und Entscheidungen können weiterhin getroffen werden.

Owner übernehmen in der täglichen Praxis eine zentrale Rolle – sie agieren als Data Stewards oder Data Guards. Das bedeutet konkret: Sie tragen die **Verantwortung** dafür, zu prüfen, welche Zugriffe bestehen und wer auf welche Inhalte Zugriff hat.

Prüfen Sie daher, wie viele Owner in Ihrem System aktuell hinterlegt sind – sowohl in **Microsoft Teams**, als auch in Ihren **Microsoft 365 Gruppen** und **SharePoint-Seiten**. Fügen Sie wo notwendig einen zweiten Owner hinzu.

Im nächsten Schritt legen wir fest, wer benachrichtigt werden soll, wenn Änderungen erfolgen oder Maßnahmen notwendig sind.

Zur Auswahl stehen:

Wer soll (per E-Mail) benachrichtigt werden, um die Verantwortung der Website zuzuweisen oder in Anspruch zu nehmen? *

Wenn eine Website weniger als die Mindestanzahl von Besitzern oder Administratoren aufweist, werden ausgewählte Empfänger benachrichtigt. Es wird empfohlen, sicherzustellen, dass mindestens 3 Optionen ausgewählt sind, um die Wahrscheinlichkeit zu erhöhen, dass ein Besitzer gefunden wird.

- Aktuelle Websitebesitzer, falls vorhanden
- Aktuelle Websiteadministratoren, falls vorhanden
- Manager*in des vorherigen Websitebesitzers oder -administrators (i)
- Aktive Websitemitglieder (i)

Abbildung 048

Auch die Anzahl **Aktiven Websitemitglieder** kann hier definiert werden.

Zusätzlich können wir konfigurieren, welche Aktion ausgelöst wird – zum Beispiel **keine Änderung** oder eine **Umstellung auf schreibgeschützt**. Diese Konfiguration trägt dazu bei, den Zugriff auf nicht verwaltete oder inaktive Inhalte gezielt zu steuern.

Welche Aktion möchten Sie ausführen, wenn eine Website länger als 3 Monate besitzerlos bleibt?

(i) Erzwangsaktionen können nach der Richtlinienerstellung nicht bearbeitet werden

Die ausgewählte Aktion wird auf der Website ausgeführt, wenn die Empfänger den Besitz nicht akzeptieren oder niemand benachrichtigt werden kann.

Zugriff auf schreibgeschützt festlegen	▼
<small>Zugriff auf schreibgeschützt festlegen</small> <small>Benutzer können Websiteinhalte anzeigen, aber nicht bearbeiten.</small>	
<small>Keine Änderung beim Zugriff</small> <small>Benutzer können die Website weiterhin verwenden, auch wenn kein Besitzer vorhanden ist.</small>	
Zurück	Weiter

Abbildung 049

Von der Priorisierung her gilt: zunächst solltet Sie eine Ist-Aufnahme machen, dann die Datenbestände validieren. Die Einrichtung der Owner-Struktur ist wichtig – sie folgt jedoch auf diese **beiden vorbereitenden Schritte**.

Änderungen nachvollziehen und SharePoint-Aktivitäten überwachen

Änderungen in SharePoint lassen sich gezielt nachverfolgen – von administrativen Anpassungen bis hin zu Nutzeraktivitäten. AI Insights und regelmäßige Prüfungen unterstützen dabei, Auffälligkeiten frühzeitig zu erkennen.

Nach der Validierung der aktuellen Konfiguration empfehle ich, in das Admin Center zurückzukehren. In der erweiterten Verwaltung steht uns unter *Berichte* der Bereich **Änderungsverlauf** zur Verfügung. Hier können wir über den Verweis direkt zu den zugehörigen Reports wechseln.

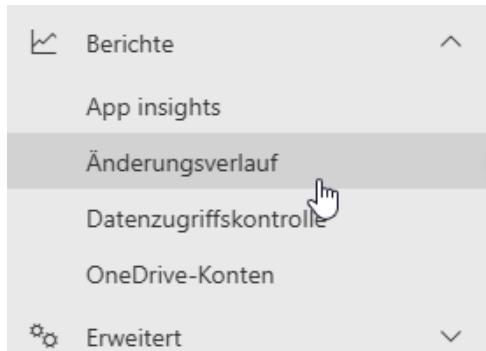


Abbildung 050

Sie können auch den folgenden Pfad verwenden: admin.sharepoint.com → Berichte → Änderungsverlauf

Klicken Sie auf **Neuer Bericht**. Hier lässt sich im Bereich der Seiten- oder Organisationseinstellungen festlegen, welche Administratorrollen in Auswertungen berücksichtigt werden sollen; etwa globale Administratoren oder SharePoint-Administratoren, jedoch keine Site-Administratoren.

Berichtsart auswählen

Websiteeinstellungen

Änderungen nachverfolgen, die in den letzten 180 Tagen von globalen Administratoren, SharePoint-Administratoren oder Websiteadministratoren an Websites vorgenommen wurden.

Organisationseinstellungen

Änderungen nachverfolgen, die in den letzten 180 Tagen von globalen Administratoren oder SharePoint-Administratoren an organization Einstellungen vorgenommen wurden.

Abbildung 051

Überwachung durchgeföhrter Änderungen

Pfad: admin.sharepoint.com → Berichte → Änderungsverlauf → Change history

Zusätzlich lässt via *Change history* nachvollziehen, welche Änderungen durchgeführt wurden. Die sogenannte Lifecycle-Zeit wird an anderer Stelle angezeigt und gibt Hinweise auf den Verlauf einzelner Seiten.

X

Changes SharePoint Sites

[Schließen](#)[Eine Kopie erstellen](#) [Abrufen von AI-Erkenntnissen](#) [Löschen](#)**Berichtstyp**

Websiteeinstellungen

Berichtsstatus

Abgeschlossen

Änderungen insgesamt

4.100

Erstellt von

Aaron Siller ADM

Erstellungsdatum

2. März 2025

Berichtsbereich (UTC)

24. Februar 2025 - 3. März 2025

Ausgewählte Websites

Alle Websites

Änderungen vorgenommen von

Alle globalen Administratoren, SharePoint-Administratoren und Websiteadministratoren

Abbildung 052

Unterstützung durch AI Insights

Pfad: admin.sharepoint.com → Berichte → **Änderungsverlauf** → AI insights

AI Insights liefert Ihnen zusätzlich **automatische Hinweise** auf relevante Ereignisse – zum Beispiel, wenn Seiten gelöscht wurden oder größere Änderungen vorgenommen wurden.

Im folgenden Beispiel wies das System darauf hin, dass am 25. Februar mehrere Seiten entfernt und bestimmte Inhalte angepasst wurden.

Auch **Änderungen an Freigabeeinstellungen oder Speicherlimits** werden hier aufgeführt. Diese Informationen helfen dabei, im Anschluss an die Validierung der Seitenstruktur gezielt nachzuvollziehen, welche Eingriffe im System stattgefunden haben.

- **Site deletions:** Multiple sites were deleted on 2/25/2025, including "EXT-IBB-Workshop-IBBIntern" and "EXT-IBB-Workshop". This could lead to accidental data loss if these deletions were not intentional. Consider reviewing the deletion logs and ensuring that these actions were authorized and necessary.
- **IB mode changes:** There were changes to the IB mode for several sites, including "EXT-P-ContentPlanning" and "Nouman-Aaron", moving from "Open" to "Implicit". This indicates a tightening of access controls, which can help prevent oversharing. Ensure that these changes align with your organization's security policies.
- **Storage settings adjustments:** The storage limit warning for the site "EXT-P-ContentPlanning" was set to 85% on 2/19/2025. This can help in managing storage limits effectively by providing early warnings before the storage limit is reached. Regularly monitor storage usage to prevent any disruptions in access.

 Copy

AI-generated content may be incorrect



Abbildung 053

Regelmäßige Kontrolle der Nutzeraktivität

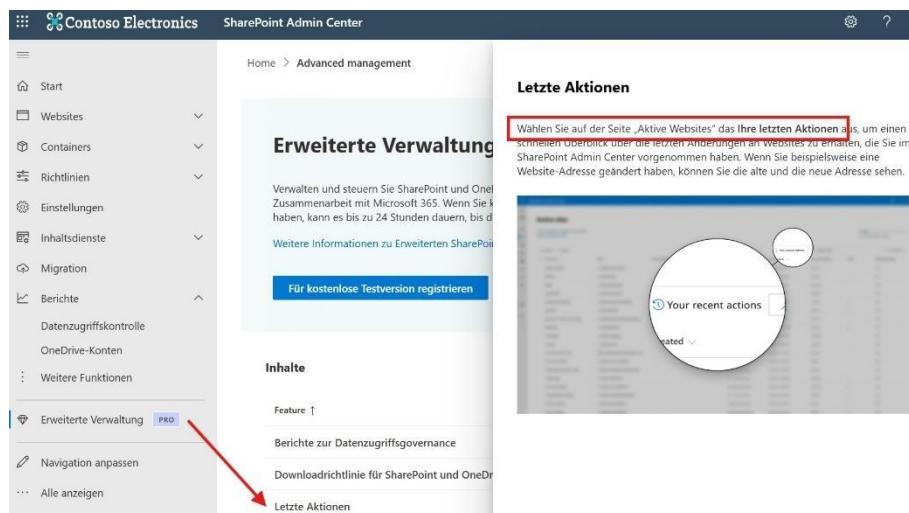
Nicht jeder Hinweis führt zwangsläufig zu einem konkreten Task – dennoch lohnt es sich, diese Berichte regelmäßig zu prüfen. Sie bieten einen Überblick darüber, wie aktiv Ihre Benutzer im SharePoint arbeiten und ob bestimmte Entwicklungen eine weitere Maßnahme erfordern.

Weitere Änderungen im Admin Center nachvollziehen

Auch abseits klassischer Berichte bietet das Admin Center wertvolle Einblicke. Die Aktivierung der Site Level Access Restriction ist dabei ein zentraler Schritt zur Absicherung geschäftskritischer Inhalte.

Pfad: admin.sharepoint.com → Berichte → **Letzte Aktionen**

Im Microsoft 365 Admin Center finden Sie unter **Letzte Aktionen** eine Übersicht über kürzlich durchgeführte administrative Änderungen. Hier wird angezeigt, ob Sie selbst oder ein Kollege eine Konfiguration angepasst haben.



The screenshot shows the SharePoint Admin Center interface. On the left, there's a navigation sidebar with various sections like Start, Websites, Containers, Richtlinien, Einstellungen, Inhaltsdienste, Migration, Berichte, and Erweiterte Verwaltung (Advanced Management). The 'Erweiterte Verwaltung' section is highlighted with a red arrow pointing from the sidebar to the 'Letzte Aktionen' link at the bottom of the main content area. The main content area has a heading 'Erweiterte Verwaltung' and a sub-section 'Inhalte'. At the bottom of this section, there's a link 'Letzte Aktionen' which also has a red arrow pointing to it. To the right of the main content, there's a separate window titled 'Letzte Aktionen' with a descriptive text and a circular preview image.

Abbildung 054

Auch wenn diese Liste gelegentlich leer ist – etwa, weil aktuell keine Änderungen vorgenommen wurden – lohnt sich, regelmäßig reinzuklicken. Selbst kleinere Änderungen können wichtige Hinweise auf laufende Aktivitäten liefern und helfen dabei, die Übersicht zu behalten.

Ihre letzten Aktionen PRO

Überprüfen Sie die letzten Websiteänderungen, die Sie in den letzten 30 Tagen aus dem SharePoint Admin Center vorgenommen haben. Um die von anderen Benutzern vorgenommenen Websiteänderungen zu überprüfen, zur Seite „Änderungsverlauf“ wechseln.

Weitere Informationen zu aktuellen Aktionen

 Exportieren

04:34

 Site gelöscht.

.../sites/team_identities

04:34

 Site gelöscht.

.../sites/PartnerMarketing-Broker

04:28

 Site gelöscht.

.../sites/assistenz

00:56

 Site gelöscht.

.../sites/ALLCTO

Abbildung 055

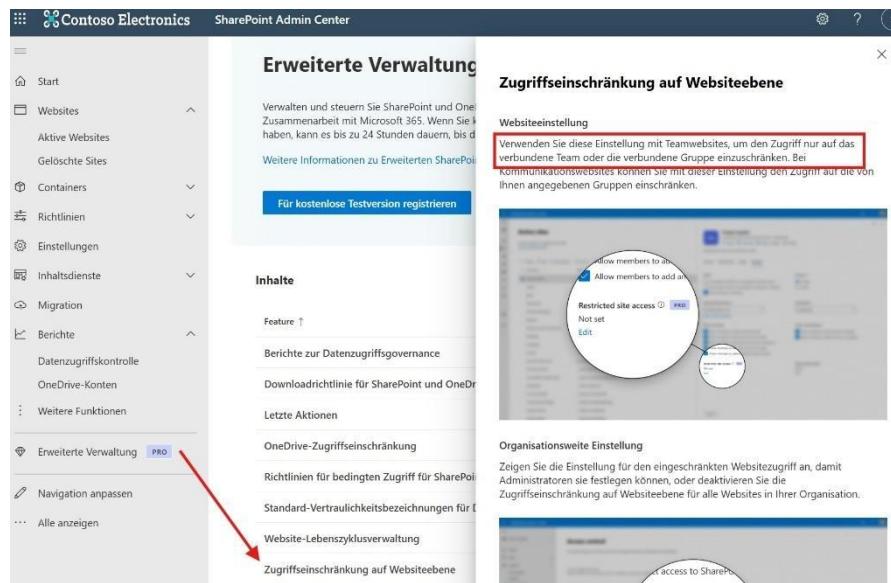
Site Level Access Restriction unter Access Control aktivieren

Pfad: admin.sharepoint.com → Erweiterte Verwaltung → **OneDrive Zugriffseinschränkung**

Hier wählen wir in den *Erweiterte Verwaltung* die Kategorie **OneDrive Zugriffseinschränkung** und klicken auf den angegebenen Verweis.

Inhalte

Feature ↑	Speicherort
Berichte zur Datenzugriffsgovernance	Berichte > Datenzugriffsgovernance
Downloadrichtlinie für SharePoint und OneDrive blockieren	Microsoft PowerShell
Letzte Aktionen	Aktive Websites > Letzte Aktionen
OneDrive-Zugriffeinschränkung	> OneDrive-Zugriffeinschränkung

Abbildung 056


The screenshot shows the SharePoint Admin Center interface. On the left, the navigation menu includes 'Start', 'Websites' (with 'Aktive Websites' and 'Gelöschte Sites' sub-options), 'Containers', 'Richtlinien', 'Einstellungen', 'Inhaltsdienste', 'Migration', 'Berichte' (with 'Datenzugriffskontrolle', 'OneDrive-Konten', and 'Weitere Funktionen' sub-options), 'Erweiterte Verwaltung' (highlighted with a red arrow), 'Navigation anpassen', and 'Alle anzeigen'. The main content area is titled 'Erweiterte Verwaltung' and contains sections for 'Inhalte' (with links to 'Berichte zur Datenzugriffsgovernance', 'Downloadrichtlinie für SharePoint und OneDrive blockieren', 'Letzte Aktionen', and 'OneDrive-Zugriffeinschränkung') and 'Zugriffeinschränkung auf Websiteebene'. The 'Zugriffeinschränkung auf Websiteebene' dialog box is open, showing 'Websiteeinstellung' (with a note about using it for Team sites) and 'Organisationsweite Einstellung' (with a note about using it for communication sites). A red box highlights the note in 'Websiteeinstellung'.

Abbildung 057

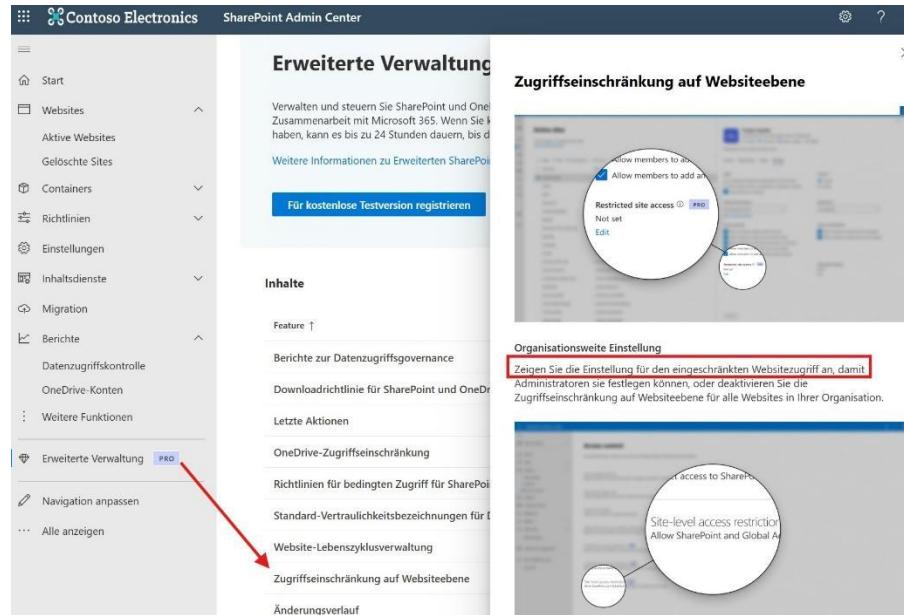


Abbildung 058

Nun aktivieren wir die **OneDrive Zugriffseinschränkung**, in dem wir das Häkchen setzen.

OneDrive-Zugriffseinschränkung

Verwenden Sie diese Einstellung, um nur Benutzern in bestimmten Sicherheitsgruppen den Zugriff auf OneDrive-Inhalte zu ermöglichen. Sie können bis zu 10 Sicherheitsgruppen hinzufügen. Benutzer, die sich nicht in diesen Sicherheitsgruppen befinden, verlieren den Zugriff auf alle OneDrive-Inhalte.

[Weitere Informationen zur Einschränkung des Zugriffs auf OneDrive](#)

- Beschränken des OneDrive-Zugriffs auf Benutzer in bestimmten Sicherheitsgruppen

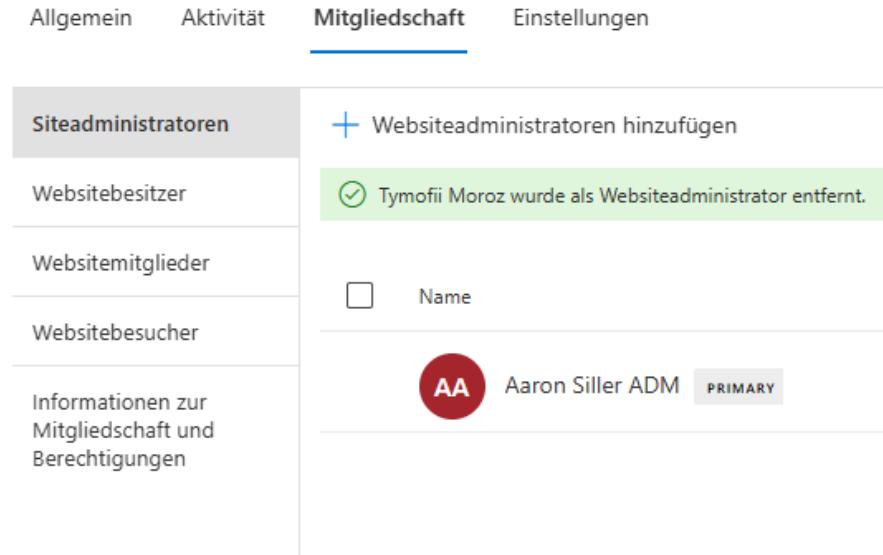
Sicherheitsgruppen hinzufügen

Sicherheitsgruppen durchsuchen

Abbildung 060

Jetzt ist es uns möglich, verschiedene Einstellungen einzusehen. Dazu wählen wir eine beliebige aktive Seite über den Pfad: admin.sharepoint.com → Websites → **Aktive Websites**.

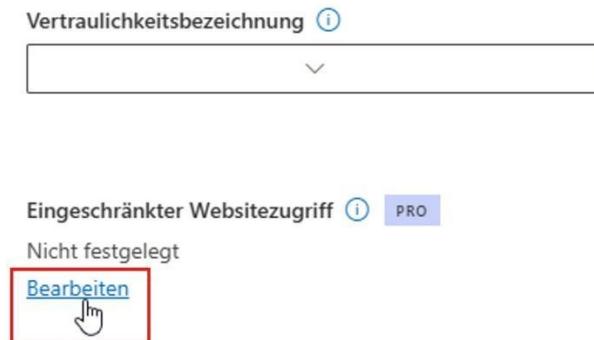
In diesem Beispiel die Seite für *G-Workshop*. Über den Menüpunkt → **Mitgliedschaft** können wir nun mittels der verschiedenen seitlich angezeigten Kategorien die jeweiligen Rollen einsehen.



The screenshot shows the 'Mitgliedschaft' tab selected in the top navigation bar. On the left, a sidebar lists categories: Siteadministratoren (highlighted), Websitebesitzer, Websitemitglieder, Websitebesucher, and Informationen zur Mitgliedschaft und Berechtigungen. The main area displays a list of website administrators. A green message box at the top right says: 'Tymofii Moroz wurde als Websiteadministrator entfernt.' Below it is a form field for adding a new administrator with a placeholder 'Name'. A user card for 'Aaron Siller ADM' is shown with the status 'PRIMARY'.

Abbildung 061

Über den Menüpunkt → **Einstellungen** haben wir zusätzlich die Möglichkeit, den **Eingeschränkten Websitezugriff** zu aktivieren.



The screenshot shows the 'Einstellungen' page. In the 'Vertraulichkeitsbezeichnung' section, there is a dropdown menu. In the 'Eingeschränkter Websitezugriff' section, the status is set to 'Nicht festgelegt' (Not defined). A red box highlights the 'Bearbeiten' button, which has a hand cursor icon over it.

Abbildung 062

Dazu setzen wir das Häkchen. Was bedeutet das?

Eingeschränkter Websitezugriff

Verwenden Sie diese Einstellung, um nur Benutzern bestimmter Gruppen den Zugriff auf diese SharePoint-Website zu ermöglichen. Sie können bis zu 10 Sicherheitsgruppen oder Microsoft 365-Gruppen hinzufügen. Benutzer, die diesen Gruppen nicht angehören, verlieren den Zugriff auf diese SharePoint-Website.

Weitere Informationen zur eingeschränkten Zugriffssteuerung für SharePoint-Websites

Beschränken des Zugriffs auf SharePoint-Websites auf Benutzer in bestimmten Gruppen

Gruppe hinzufügen

Gruppen durchsuchen

Abbildung 063

Öffnen Sie dazu eine beliebige Site in Ihrem System und klicken Sie via der rechten Seite zu den Einstellungen, dann auf → **Websiteberechtigungen**.



Abbildung 064

Wir sehen die Einstellung: **Restricted Site Access is on**. Das bedeutet: Nur Mitglieder einer bestimmten Gruppe – mit den entsprechenden Site-Berechtigungen – haben Zugriff auf die Seite. Der Gruppenname wird dabei explizit angezeigt.

Idealerweise wählen Sie für diese Gruppe denselben Namen wie für die zugehörige SharePoint-Seite. Das erleichtert die Zuordnung und erfüllt gleichzeitig eine wichtige Funktion: **eine Art Notfallzugriff**. Sollte es zu Unklarheiten bei den Berechtigungen kommen, lässt sich so schnell überprüfen, wer Zugriff haben sollte – und wer nicht.

Gerade bei Seiten mit **geschäftskritischen Daten** ist diese Konfiguration essenziell. Mit wenigen Klicks können Sie sicherstellen, dass **ausschließlich Gruppenmitglieder Zugriff erhalten**.

Alle anderen – etwa externe Benutzer oder individuell berechtigte Personen außerhalb der Gruppe – **verlieren den Zugriff automatisch**. Nur Mitglieder der definierten Gruppe behalten Zugriffsrechte, alle anderen haben **keine Möglichkeit mehr**, auf die Inhalte zuzugreifen.

Permissions X

Manage who has access to this site.

ⓘ Restricted site access is on - Only owners and members of the following group with site permissions can access this site:
5.01_Sales_Global

Add members ▾

▼ Site owners - full control ⓘ
▼ Site members - limited control ⓘ
▼ Site visitors - no control ⓘ

Site Sharing
Change how members can share

Guest Expiration
Your organization does not require guest access to expire.
Manage

There are additional groups or people with permissions on this site. To see them, please visit [Advanced permissions settings](#).

Abbildung 065

Empfehlung: Wenn Sie einzelne Seiten aus der Indexierung innerhalb des Microsoft 365 Group Piloten herausnehmen möchten, öffnen Sie über die *Site Settings* die Option *Search and Offline Availability*. Setzen Sie **Allow this site to appear in Search Results** auf **No**.

Gastzugriffe in Entra ID und Microsoft Teams verwalten

Gastzugriffe, Gruppenverwaltung und App-Berechtigungen zählen zu den kritischsten Bereichen im Microsoft 365 Umfeld. Klare Regeln, automatisierte Prozesse und gezielte Zugriffskontrolle sorgen für Sicherheit – auch im Einsatz mit Copilot.

Pfad: entra.microsoft.com → Identität → Benutzer → Alle Benutzer → Filter

Hier sehen Sie die Gesamtzahl aller Benutzer in Ihrem Tenant.

Um gezielt nach Gastnutzern zu filtern, wählen Sie **Filter** aus. Geben Sie dann den **Benutzertyp** ein und setzen Sie den Filter auf **Gast**. So erhalten Sie eine Übersicht aller externen Nutzer in Ihrer Umgebung.

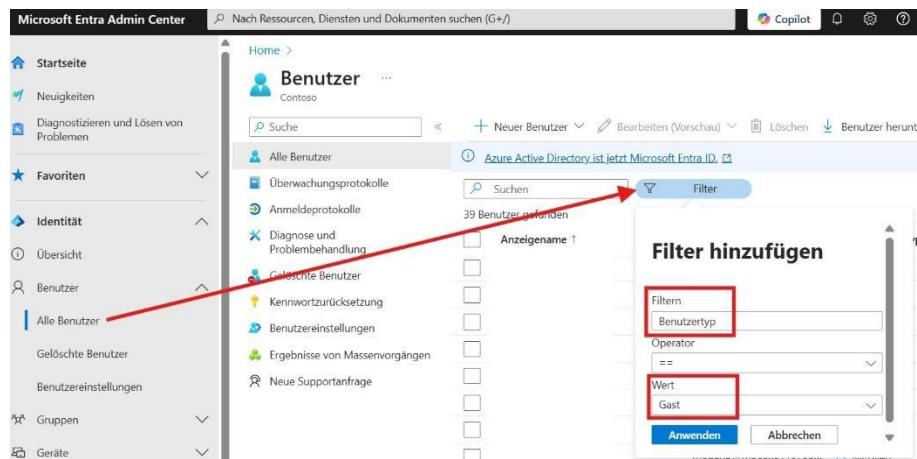


Abbildung 066

Gäste gelangen nicht nur über SharePoint oder OneDrive in Ihr System, sondern auch über **Microsoft Teams**. Deshalb ist es entscheidend, dort ebenfalls klare Regelungen zu treffen.

Regelungen zum Einladen von Gästen in Teams

Wie Gäste in Microsoft Teams eingeladen werden dürfen, ist in der Praxis sehr unterschiedlich geregelt. In einer Umgebung dürfen Mitglieder Gäste vorschlagen, die Einladung muss jedoch durch einen **Besitzer des Teams** bestätigt werden. Die Besitzerrolle übernehmen in der Regel Teamleiter oder Projektverantwortliche.

Es ist auch möglich, ein **formalisiertes Antragsverfahren** zu nutzen: Nur Gäste von **zugelassenen Domänen** dürfen eingeladen werden. Der Antrag zur Freigabe einer Domäne wird vom **IAM-Team geprüft und freigegeben**. Erst danach kann der Owner eines Teams eigenständig Gäste einladen.

Ziel ist es, die Abläufe rund um externe Zugriffe transparent zu machen. Microsoft Teams ist häufig der Einstiegspunkt für Gäste – darum ist es wichtig zu klären:

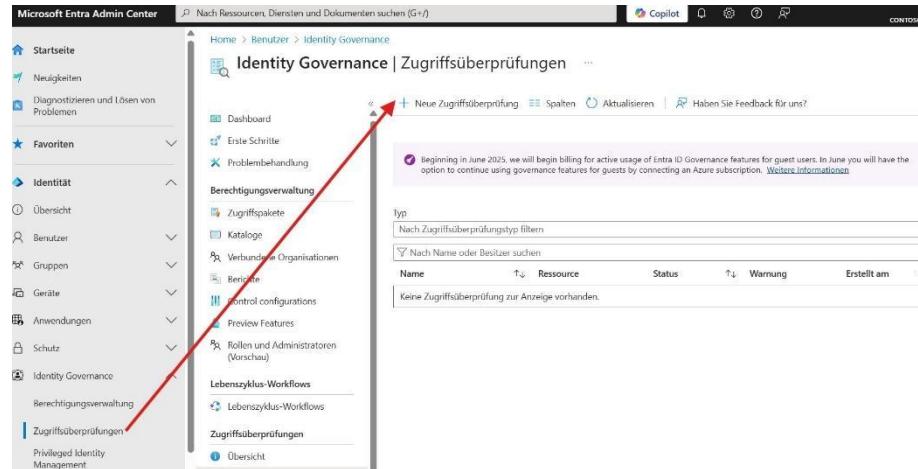
- **Wer darf Gäste einladen?**
- **Wie wird der Zugriff wieder entzogen?**

Denn: Gäste, die im System angelegt werden, **bleiben dauerhaft aktiv**, sofern nichts anderes konfiguriert wurde. Microsoft 365 bietet **standardmäßig keinen automatischen Ablaufmechanismus** für Gastkonten.

Für eine strukturierte Steuerung müssen Sie diesen Prozess selbst definieren. Hier kommt die Funktion **Zugriffsüberprüfungen** ins Spiel. Damit können Sie regelmäßig prüfen, ob Gastkonten noch benötigt werden. Diese Funktion steht jedoch erst ab einer **Microsoft E5- bzw. P2-Lizenz** zur Verfügung.

Automatisierung und Gastzugriffsverwaltung

Pfad: entra.microsoft.com → Identität → Identity Governance → **Zugriffsüberprüfungen** → Neue Zugriffsüberprüfung

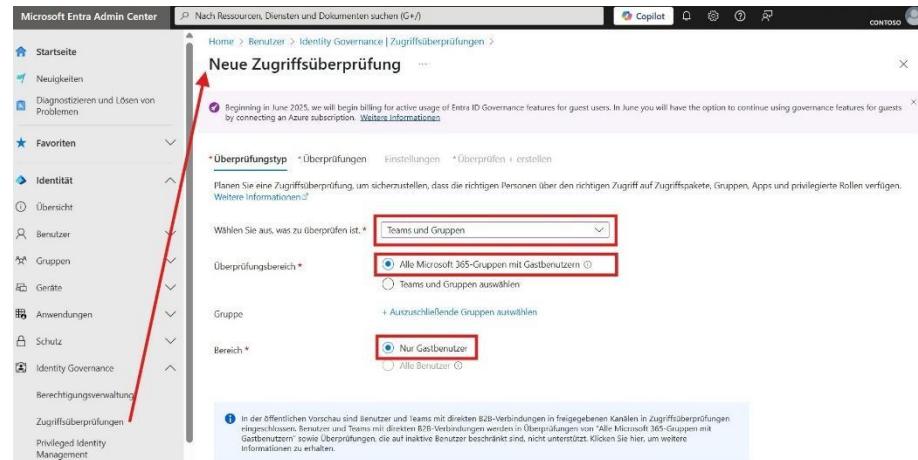


The screenshot shows the Microsoft Entra Admin Center interface. The left sidebar has a tree view with 'Identity Governance' selected, and 'Zugriffsüberprüfungen' is highlighted. The main content area is titled 'Identity Governance | Zugriffsüberprüfungen'. At the top right, there is a button labeled '+ Neue Zugriffsüberprüfung'. A red arrow points from the left sidebar towards this button.

Abbildung 067

Der **erste Schritt** der Konfiguration ist **Überprüfungstyp**. Hier können wir nun zwischen zwei Optionen wählen. Für unsere Datenstände im Microsoft Copilot sind **Teams und Gruppen** entscheidend. Anschließend definieren wir, ob wir die Automatisierung auf alle Gruppen und Gäste legen wollen, oder nur auf bestimmte.

Ich empfehle, **Alle Microsoft 365-Gruppen mit Gastbenutzern** zu wählen und ebenfalls den **Bereich** auf **Nur Gastbenutzer** zu setzen. So erzielen wir eine flächendeckende Sicherung unserer Umgebung.



The screenshot shows the 'Neue Zugriffsüberprüfung' configuration dialog. The left sidebar is visible, and the main dialog has several sections: 'Überprüfungstyp' (selected), 'Überprüfungen', 'Einstellungen', and 'Überprüfen + erstellen'. The 'Wählen Sie aus, was zu überprüfen ist.' dropdown is set to 'Teams und Gruppen'. The 'Überprüfungsbereich' section contains a radio button for 'Alle Microsoft 365-Gruppen mit Gastbenutzern' (which is highlighted with a red box). The 'Bereich' section also contains a radio button for 'Nur Gastbenutzer' (which is also highlighted with a red box). A note at the bottom states: 'In der öffentlichen Vorschau sind Benutzer und Teams mit direkten B2B-Verbindungen in freigegebenen Kanälen in Zugriffsüberprüfungen eingeschlossen. Benutzer und Teams mit direkten B2B-Verbindungen werden in Überprüfungen von "Alle Microsoft 365-Gruppen mit Gastbenutzern" sowie Überprüfungen, die auf aktive Benutzer beschränkt sind, nicht unterstützt. Klicken Sie hier, um weitere Informationen zu erhalten.'

Abbildung 068

Im **zweiten Schritt** definieren wir die **Überprüfungen**. Es gibt hier zwei Möglichkeiten: Die Voreinstellung, mit der eine Person geprüft wird, oder die Überprüfungswiederholung. Diese wird durch Auswählen des Häckchens betätigt, erfordert jedoch eine weitere Person.

Bei der Voreinstellung zur einmaligen Überprüfung gibt es vier Gruppen, die wir konfigurieren können:

- **Gruppenbesitzer:** Beste Wahl.
- **Ausgewählte Benutzer und Gruppen:** Neutral.
- **Benutzer überprüfen ihren eigenen Zugriff:** Nicht zu empfehlen.
- **Vorgesetzte von Benutzern:** Erfordernd, dass die Stammdaten gepflegt sind und keine Vorgesetzten oder externe Nutzer wie Sponsoren hinterlegt sind.

The screenshot shows the Microsoft Entra Admin Center interface. The left sidebar navigation includes 'Startseite', 'Neuigkeiten', 'Diagnostizieren und Lösen von Problemen', 'Favoriten', 'Identität', 'Übersicht', 'Benutzer', 'Gruppen', 'Geräte', 'Anwendungen', 'Schutz', and 'Identity Governance' (which is currently selected). Under 'Identity Governance', there are links for 'Berechtigungsverwaltung', 'Zugriffsüberprüfungen', 'Privileged Identity Management', and 'Lebenszyklus-Workflows'. The main content area is titled 'Neue Zugriffsüberprüfung' (New Access Review). It displays a message about billing starting in June 2025. Below this, there are tabs for 'Überprüfungstyp' (Review Type), 'Überprüfung' (selected), 'Einstellungen', and 'Überprüfen + erstellen'. A note says 'Legen Sie nachstehend die Überprüfungsphasen, die Prüfer und die Zeitachse fest.' (Define the review phases, reviewers, and timeline below). There are sections for 'Überprüfung in mehreren Phasen' (Multi-phase review) with a checkbox, 'Prüfer angeben' (Specify reviewer) with a dropdown menu containing 'Gruppenbesitzer' (highlighted with a red box), 'Wiederholung der Überprüfung ar...' (Review repetition), 'Dauer (in Tagen)' (Duration in days), 'Wiederholung der Überprüfung *' (Review repetition *), 'Startdatum' (Start date), and a date input field showing '29.04.2025'.

Abbildung 069

Die **Dauer (in Tagen)** ist mit sechs Tagen vordefiniert – ein guter Zeitraum. Setzen Sie **Wiederholung der Überprüfung** zunächst auf monatlich; nach guter Einarbeitung genügen auch quartalsweise.

Microsoft Entra Admin Center Copilot

Nach Ressourcen, Diensten und Dokumenten suchen (G+)

Startseite
Neuigkeiten
Diagnosieren und Lösen von Problemen
Favoriten
Identität
Übersicht
Benutzer
Gruppen
Geräte
Anwendungen
Schutz
Identity Governance
Berechtigungsverwaltung
Zugriffsüberprüfungen
Privileged Identity Management
Lebenszyklus-Workflows
Externe Identitäten

Home > Benutzer > Identity Governance | Zugriffsüberprüfungen > Neue Zugriffsüberprüfung ...

Beginning in June 2025, we will begin billing for active usage of Entra ID Governance features for guests by connecting an Azure subscription. [Weitere Informationen](#)

* Überprüfungstyp ***Überprüfungen** Einstellungen * Überprüfen + erstellen

Legen Sie nachstehend die Überprüfungsphasen, die Prüfer und die Zeitachse fest.

Überprüfung in mehreren Phasen

Prüfer angeben

Prüfer auswählen * Gruppenbesitzer

Alternative Prüfer [+ Alternative Prüfer auswählen](#)

Wiederholung der Überprüfung angeben

Dauer (in Tagen) * 3

Wiederholung der Überprüfung * Monatlich
Wöchentlich
Monatlich
Vierteljährlich
Halbjährlich
Jährlich

Startdatum * Ende *

Abbildung 070

Ich empfehle zudem, mindestens eine Richtlinie zu konfigurieren, die niemals endet – wir setzen **Ende** entsprechend auf **Nie**. So gehen wir sicher, dass wir immer wieder zur Überprüfung herangezogen werden und die Umgebung sicherer halten.

Microsoft Entra Admin Center Copilot

Nach Ressourcen, Diensten und Dokumenten suchen (G+)

Startseite ...

Neuigkeiten

Diagnostizieren und Lösen von Problemen

Favoriten

Identität

Übersicht

Benutzer

Gruppen

Geräte

Anwendungen

Schutz

Identity Governance

Berechtigungsverwaltung

Zugriffsüberprüfungen

Privileged Identity Management

Lebenszyklus-Workflows

Externe Identitäten

Home > Benutzer > Identity Governance | Zugriffsüberprüfungen > Neue Zugriffsüberprüfung ...

Beginning in June 2025, we will begin billing for active usage of Entra ID Governance features for guest users by connecting an Azure subscription. [Weitere Informationen](#)

* Überprüfungstyp *** Überprüfungen** Einstellungen * Überprüfen + erstellen

Legen Sie nachstehend die Überprüfungsphasen, die Prüfer und die Zeitachse fest.

Überprüfung in mehreren Phasen

Prüfer angeben

Prüfer auswählen * Gruppenbesitzer

Alternative Prüfer [+ Alternative Prüfer auswählen](#)

Wiederholung der Überprüfung angeben

Dauer (in Tagen) * 3

Wiederholung der Überprüfung * Monatlich

Startdatum * 29.04.2025

Ende *

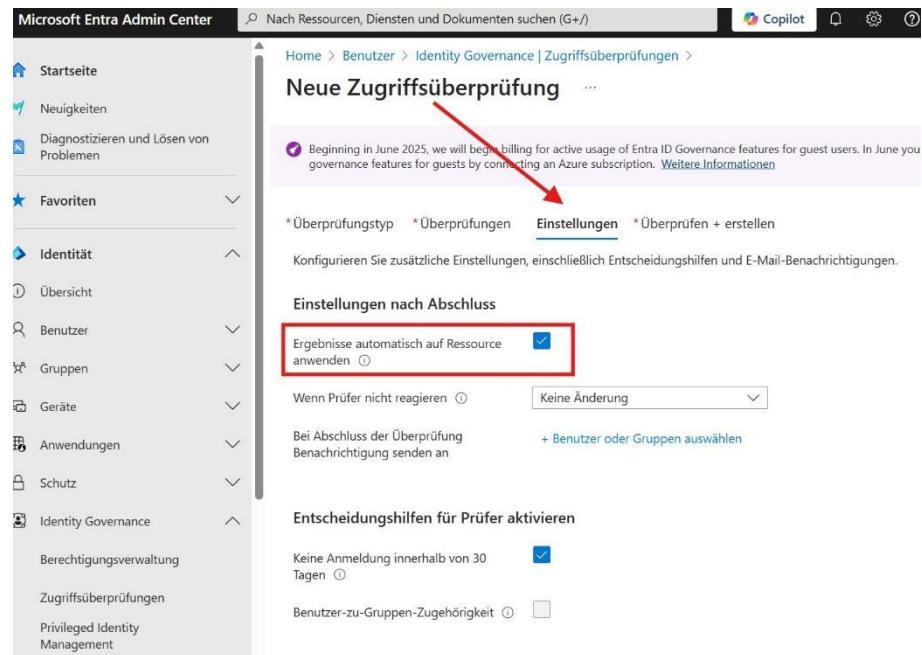
Nie

An bestimmtem Datum beenden

Nach Anzahl von Vorkommen beenden

Abbildung 071

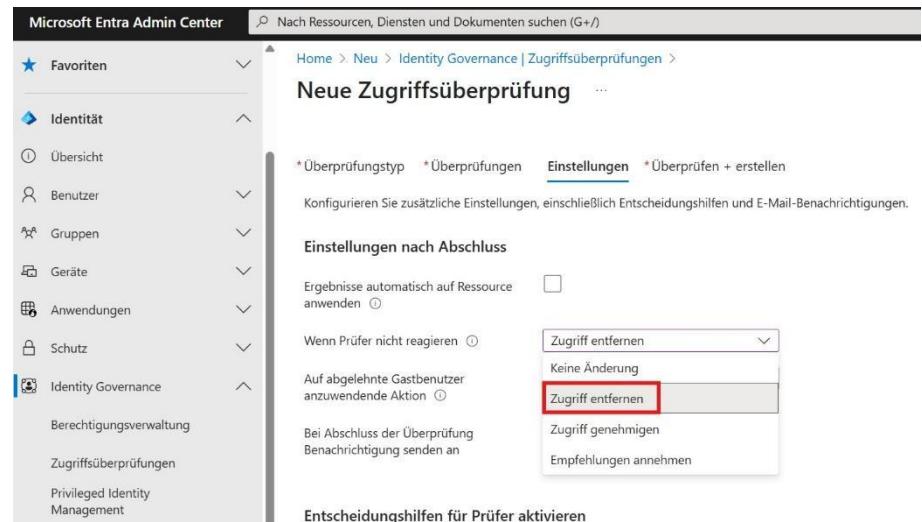
Im **dritten Schritt** schauen wir uns in den **Einstellungen** den Punkt *Ergebnisse automatisch auf Ressource anwenden* an. Lassen Sie da Häkchen, dass in der Voreinstellung gesetzt ist, drin. Somit erhalten wir nicht nur die Information, dass ein User keinen Zugriff mehr möchte, sondern können den Nutzer dann auch aktiv entfernen.



The screenshot shows the Microsoft Entra Admin Center interface. On the left, there's a navigation sidebar with categories like Startseite, Neuigkeiten, Diagnosieren und Lösen von Problemen, Favoriten, Identität, Übersicht, Benutzer, Gruppen, Geräte, Anwendungen, Schutz, Identity Governance, Berechtigungsverwaltung, Zugriffsüberprüfungen, and Privileged Identity Management. The 'Identity Governance' section is expanded. The main content area is titled 'Neue Zugriffsüberprüfung'. At the top, there's a note about billing for active usage of Entra ID Governance features for guest users starting in June 2025. Below the note, there are tabs for Überprüfungstyp (*Überprüfungen), Einstellungen (selected), and Überprüfen + erstellen. A red arrow points to the 'Einstellungen' tab. Under 'Einstellungen nach Abschluss', there's a checkbox for 'Ergebnisse automatisch auf Ressource anwenden' which is checked and highlighted with a red box. Other options include 'Wenn Prüfer nicht reagieren' (Keine Änderung selected) and 'Bei Abschluss der Überprüfung Benachrichtigung senden an' (+ Benutzer oder Gruppen auswählen). In the 'Entscheidungshilfen für Prüfer aktivieren' section, there are checkboxes for 'Keine Anmeldung innerhalb von 30 Tagen' (checked) and 'Benutzer-zu-Gruppen-Zugehörigkeit'.

Abbildung 072

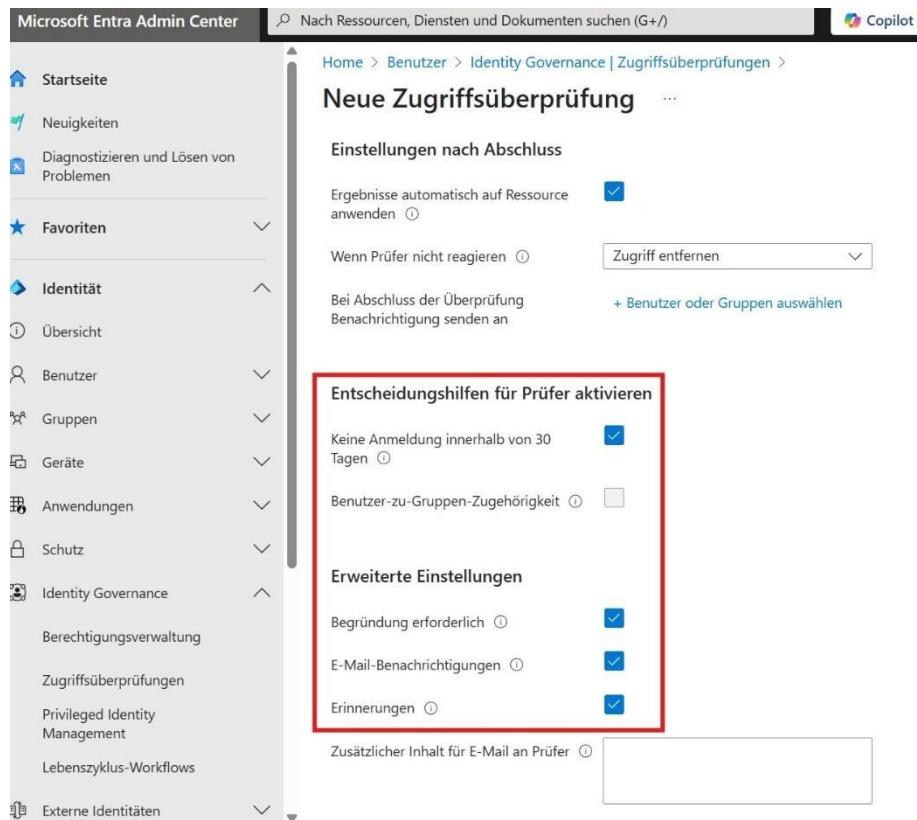
Anschließend definieren wir, was passiert, wenn ein Prüfer nicht auf die Benachrichtigung antwortet. Setzen Sie die Option auf **Zugriff entfernen**, damit der Zugriff auch wirklich entzogen wird.



This screenshot is similar to Abbildung 072 but focuses on the 'Entscheidungshilfen für Prüfer aktivieren' section. It shows the 'Einstellungen nach Abschluss' section with the 'Ergebnisse automatisch auf Ressource anwenden' checkbox unchecked. In the 'Wenn Prüfer nicht reagieren' dropdown, the 'Zugriff entfernen' option is selected and highlighted with a red box. Other options in the dropdown are 'Keine Änderung' and 'Zugriff genehmigen'. Below the dropdown, there are additional options: 'Auf abgelehnte Gastbenutzer anzuwendende Aktion' (Keine Änderung selected), 'Bei Abschluss der Überprüfung Benachrichtigung senden an' (Zugriff genehmigen selected), and 'Empfehlungen annehmen'.

Abbildung 073

Empfehlung: Alle weiteren Voreinstellungen sind optimal eingerichtet.



The screenshot shows the Microsoft Entra Admin Center interface. On the left, there's a navigation sidebar with various categories like Startseite, Neuigkeiten, Diagnosieren und Lösen von Problemen, Favoriten, Identität, Benutzer, Gruppen, Geräte, Anwendungen, Schutz, Identity Governance, Berechtigungsverwaltung, Zugriffsüberprüfungen, Privileged Identity Management, Lebenszyklus-Workflows, and Externe Identitäten. The main content area is titled 'Neue Zugriffsüberprüfung'. It contains sections for 'Einstellungen nach Abschluss' (Settings after review), 'Entscheidungshilfen für Prüfer aktivieren' (Enable reviewer decision aids), and 'Erweiterte Einstellungen' (Advanced settings). Each section has several checkboxes, many of which are checked.

Abbildung 074

Schritt 4 ist lediglich eine Zusammenfassung alle gewählten Einstellungen. Mit einem Klick auf **Überprüfen und erstellen** wird der Access Review aktiviert.

Wirkung und Anwendungsbereiche

Wird ein Zugriff nicht validiert, wird er automatisch entfernt. Vergessene oder ungewollte Berechtigungen geraten so wieder in den Fokus.

Access Reviews lassen sich für **SharePoint** und **Microsoft Teams** einsetzen. Ich empfehle, dieses Verfahren in Ihre Umgebung zu integrieren. Die Funktion ist Teil der **kostenpflichtigen E5- bzw. P2-Lizenz**.

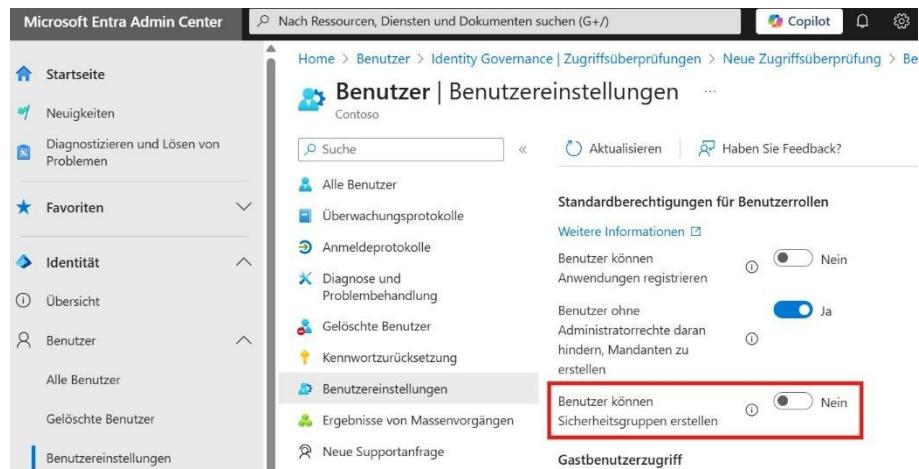
In einem Beispiel wurde ein Access Review bereits konfiguriert. In den Einstellungen finden sich die zugehörige **Review History** sowie **Audit Logs**, die alle Änderungen nachvollziehbar dokumentieren.

Erstellung von Sicherheitsgruppen einschränken

Pfad: entra.microsoft.com → Benutzer → **Benutzereinstellungen**

Die Einstellung *Benutzer können Sicherheitsgruppen erstellen* empfehle ich grundsätzlich auf **Nein** zu setzen. So stellen Sie sicher, dass nur autorisierte Personen – in der Regel Ihre IT – Sicherheitsgruppen erstellen dürfen. Das gilt für klassische Sicherheitsgruppen, aber auch für solche, die Sie im SharePoint Online oder für den Zugriff auf Microsoft Teams verwenden möchten.

Diese Einschränkung **reduziert die Anzahl unkontrolliert erstellter Gruppen** und erleichtert die zentrale Verwaltung von Berechtigungen.



The screenshot shows the Microsoft Entra Admin Center interface. The left sidebar navigation includes: Startseite, Neuigkeiten, Diagnostizieren und Lösen von Problemen, Favoriten (Übersicht, Benutzer), Identität (Alle Benutzer, Gelöschte Benutzer, Benutzereinstellungen), and Benutzer (Alle Benutzer, Gelöschte Benutzer, Benutzereinstellungen). The main content area is titled 'Benutzer | Benutzereinstellungen' for the 'Contoso' tenant. It displays several configuration options under 'Standardberechtigungen für Benutzerrollen': 'Benutzer können Anwendungen registrieren' (Nein), 'Benutzer ohne Administratorrechte daran hindern, Mandanten zu erstellen' (Ja), and 'Benutzer können Sicherheitsgruppen erstellen' (Nein, highlighted with a red box). There is also a 'Gastbenutzerzugriff' section.

Abbildung 075

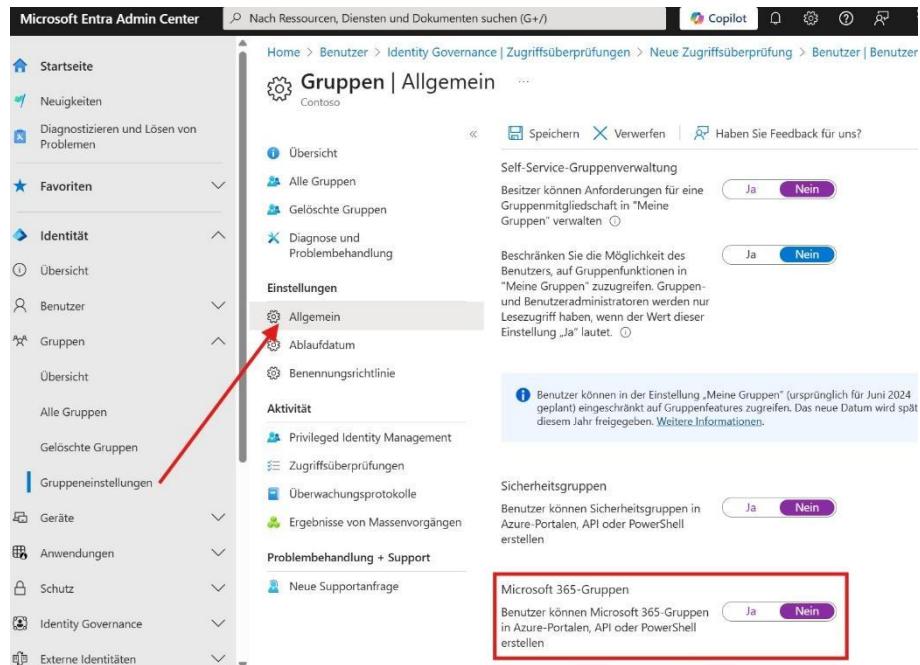
Erstellung von Microsoft 365 Gruppen zentral steuern

Pfad: entra.microsoft.com → Gruppen → Gruppeneinstellungen → **Allgemein**

Wir schauen uns die Option an und validieren, ob Benutzer selbstständig **Microsoft 365 Gruppen** erstellen dürfen. Auch hier empfehle ich, diese Funktion auf **Nein** zu setzen.

Wie bei der Erstellung von Teams sollte die Einrichtung neuer Microsoft 365 Gruppen **zentral durch Ihre IT-Abteilung** erfolgen. In der Praxis haben Benutzer selten das Bedürfnis, Gruppen selbst zu erstellen. Wenn ein entsprechender Anwendungsfall entsteht, sollte dieser gezielt und nachvollziehbar durch die zuständigen Personen bearbeitet werden.

Eine zentrale Steuerung hilft dabei, **Dublettten, verwaiste Gruppen und Berechtigungschaos zu vermeiden** – und sorgt für eine klare, wartbare Struktur.



The screenshot shows the Microsoft Entra Admin Center interface. The left sidebar navigation includes: Startseite, Neuigkeiten, Diagnostizieren und Lösen von Problemen, Favoriten, Identität (Übersicht, Benutzer, Gruppen, Übersicht, Alle Gruppen, Gelöschte Gruppen, Gruppeneinstellungen), Geräte, Anwendungen, Schutz, Identity Governance, and Externe Identitäten. The main content area is titled 'Gruppen | Allgemein' (Contoso). It displays several sections: 'Übersicht', 'Alle Gruppen', 'Gelöschte Gruppen', 'Diagnose und Problembehandlung', 'Einstellungen' (with 'Allgemein' selected, highlighted by a red arrow), 'Ablaufdatum', 'Benennungsrichtlinie', 'Aktivität' (Privileged Identity Management, Zugriffsüberprüfungen, Überwachungsprotokolle, Ergebnisse von Massenvorgängen), 'Problembehandlung + Support' (Neue Supportanfrage). There are two callout boxes: one for 'Sicherheitsgruppen' (Ja, Nein) and one for 'Microsoft 365-Gruppen' (Ja, Nein), which is highlighted with a red border.

Abbildung 076

Ablaufsteuerung für Microsoft 365 Gruppen aktivieren

Pfad: entra.microsoft.com → Gruppen → Gruppeneinstellungen → **Ablaufdatum**

Hier definieren wir, ob und wann **Microsoft 365 Gruppen automatisch ablaufen** sollen. Falls diese Funktion bei Ihnen noch nicht aktiviert ist, empfehle ich ausdrücklich, sie zu konfigurieren.

Über die Ablaufsteuerung definieren Sie eine **Lebensdauer für Gruppen** – zum Beispiel 180, 365 oder einen benutzerdefinierten Zeitraum. Wird innerhalb dieser Zeit **keine Aktivität** verzeichnet, wird die Gruppe automatisch gelöscht. Eine Wiederherstellung ist **innerhalb von 30 Tagen** möglich.

Tipp: Der Ablauf gilt nicht nur für die Gruppe selbst, sondern auch für das damit verknüpfte **Microsoft Team** – inklusive aller Freigaben und Datenablagen. Das betrifft auch Inhalte, auf die **Microsoft Copilot** zugreifen kann. So vermeiden Sie, dass nicht mehr genutzte Strukturen bestehen bleiben und Ressourcen binden.

Die Besitzer der Gruppe werden **30, 15 und 1 Tag vor Ablauf** per E-Mail informiert. Gibt es keinen Besitzer, kann alternativ eine **Sammeladresse** hinterlegt werden.

Bereits minimale Aktivitäten – etwa das Senden einer Nachricht, das Bearbeiten einer Datei oder das Hinzufügen eines Mitglieds – **setzen den Ablauf-Timer automatisch zurück**. Das System reagiert sehr sensibel, sodass die Gefahr, dass eine tatsächlich genutzte Gruppe versehentlich gelöscht wird, **äußerst gering** ist.

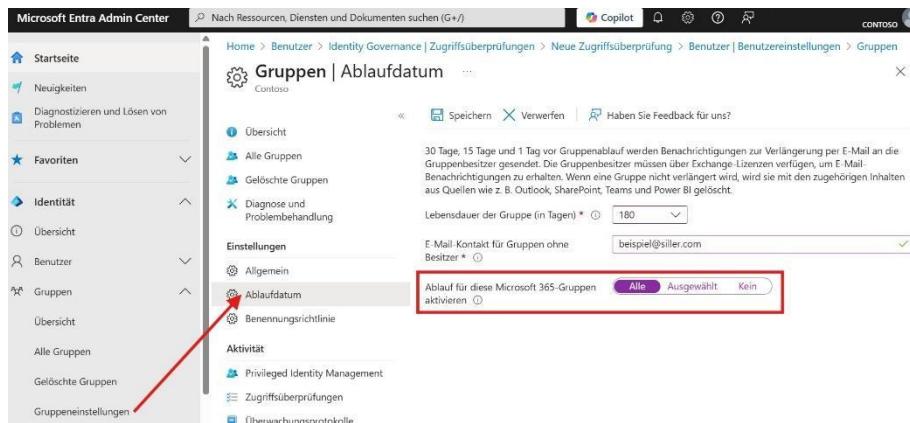


Abbildung 077

Beispielansicht für Zugriffsüberprüfungen

Pfad: myaccess.microsoft.com → **Zugriffsüberprüfungen**

Wenn Sie Zugriffsüberprüfungen noch nicht im Einsatz haben, ist es hilfreich, sich die Oberfläche einmal im Vorfeld anzusehen. Über die Zugriffsüberprüfungen sehen Sie die geplanten Überprüfungen, inklusive der zugewiesenen Person, die für die Validierung zuständig ist.

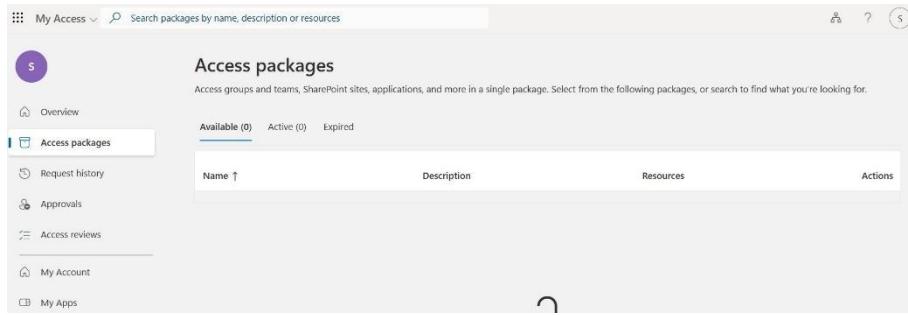


Abbildung 078

App-Zugriffe im Bereich „Enterprise Applications“ steuern

Pfad: entra.microsoft.com → Anwendungen → Unternehmensanwendungen → **Einstellungen für die Benutzereinwilligung**

Ich empfehle hier, zunächst mit der Standardeinstellung **Benutzereinwilligung nicht zulassen** zu arbeiten. So stellen Sie sicher, dass ausschließlich autorisierte Administratoren Anwendungen genehmigen und bereitstellen dürfen.

Für Microsoft 365 Copilot ist diese Einstellung besonders relevant: Sie verhindert, dass Benutzer **eigenständig** Anwendungen registrieren, die anschließend Zugriff auf sensible Inhalte erhalten könnten. Solche Anwendungen – technisch betrachtet Agents – würden sonst direkt im Copilot-Kontext auftauchen.

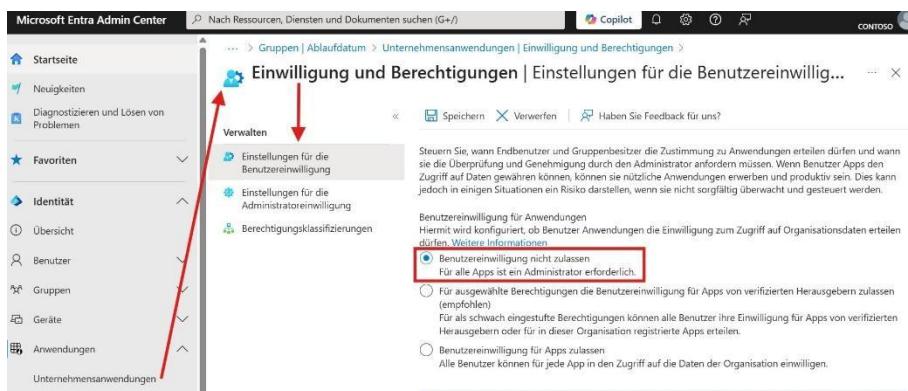
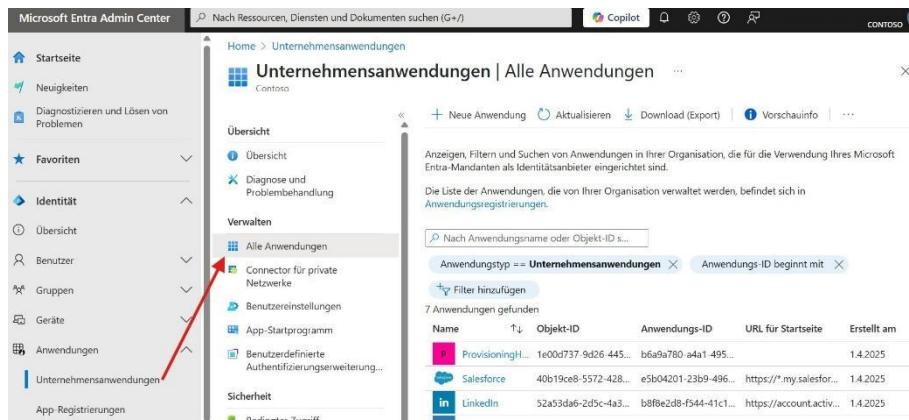


Abbildung 079

Ungenutzte Anwendungen finden und verwalten

Es lohnt sich, regelmäßig die Nutzung von registrierten Unternehmensanwendungen in Ihrer Umgebung zu überprüfen.

Pfad: [entra.microsoft.com](#) → Anwendungen → Unternehmensanwendungen → Alle Anwendungen

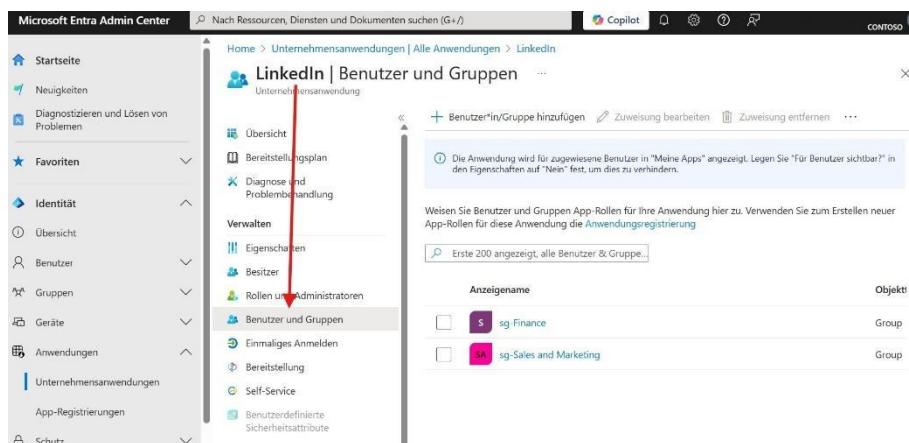


The screenshot shows the Microsoft Entra Admin Center interface. The left sidebar has a 'Favoriten' section with 'Unternehmensanwendungen' selected. The main area is titled 'Unternehmensanwendungen | Alle Anwendungen'. It shows a table with columns: Name, Objekt-ID, Anwendungs-ID, URL für Startseite, and Erstellt am. There are three entries: ProvisioningH..., Salesforce, and LinkedIn. A red arrow points to the 'Alle Anwendungen' link in the sidebar.

Name	Objekt-ID	Anwendungs-ID	URL für Startseite	Erstellt am
ProvisioningH...	1eb004737-9d26-445...	b6a9a780-a4a1-495...		1.4.2025
Salesforce	40b19ce8-5572-428...	e5b04201-23b9-496...	https://*.my.salesfor...	1.4.2025
LinkedIn	52a53da6-2d5c-4a3...	b8f8e2d8-f544-41c1...	https://account.activ...	1.4.2025

Abbildung 080

Klicken wir auf eine Anwendung, können wir im Bereich **Benutzer und Gruppen** prüfen, welche Benutzer die jeweilige Anwendung registriert haben. Ist kein Benutzer mehr hinterlegt, kann das ein Hinweis darauf sein, dass das zugehörige Objekt **nicht mehr aktiv** ist – und die Anwendung möglicherweise **nicht mehr benötigt** wird.

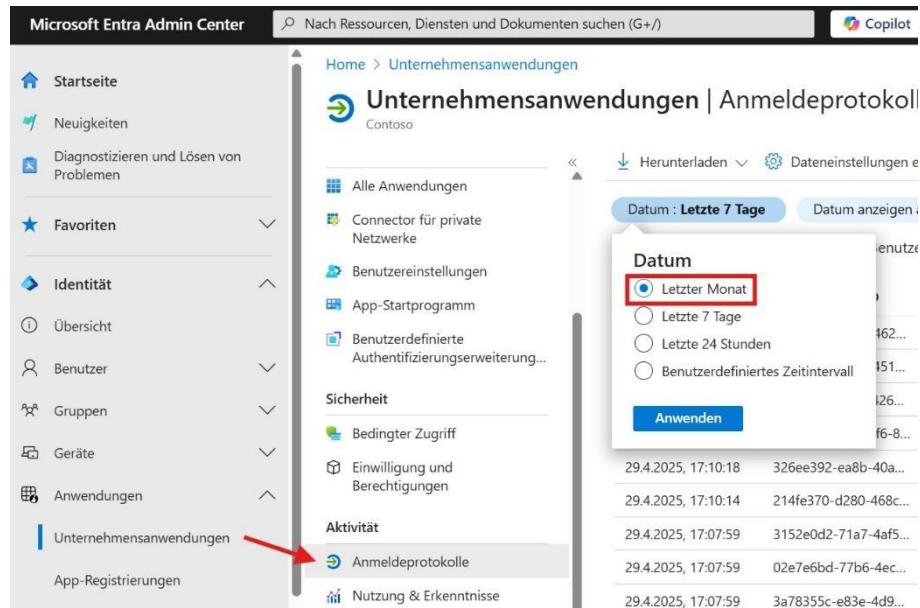


The screenshot shows the Microsoft Entra Admin Center interface for the LinkedIn application. The left sidebar has a 'Verwalten' section with 'Benutzer und Gruppen' selected. The main area is titled 'LinkedIn | Benutzer und Gruppen'. It shows a table with columns: Anzeigename, Objekttyp, and Group. There are two entries: sg-Finance and sg-Sales and Marketing. A red arrow points to the 'Benutzer und Gruppen' link in the sidebar.

Anzeigename	Objekttyp
sg-Finance	Group
sg-Sales and Marketing	Group

Abbildung 081

Zusätzlich empfehle ich, die **Anmeldeprotokolle** zu prüfen – zum Beispiel rückblickend auf den letzten Monat.



Datum	Zeit	ID
29.4.2025, 17:10:18	326ee392-ea8b-40a...	
29.4.2025, 17:10:14	214fe370-d280-468c...	
29.4.2025, 17:07:59	3152e0d2-71a7-4af5...	
29.4.2025, 17:07:59	02e7e6bd-77b6-4ec...	
29.4.2025, 17:07:59	3a78355c-e83e-4d9...	

Abbildung 082

Wenn auch dort keine Anmeldungen mehr registriert wurden, können Sie unter **Eigenschaften** die Einstellung **Aktiviert für die Benutzeranmeldung?** auf **Nein** setzen. So wird der Zugriff zunächst gesperrt, ohne die Anwendung sofort zu löschen.

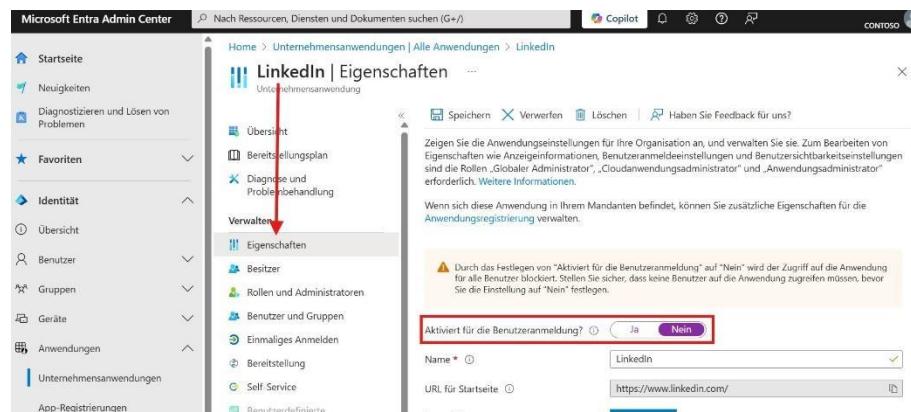


Abbildung 083

In der Praxis hat sich folgender Ablauf bewährt:

1. Anwendung sperren
2. Erinnerung in 30 Tagen setzen
3. Wird die App weiterhin nicht genutzt → Löschung vornehmen

Mit diesem Vorgehen halten Sie Ihre Umgebung **aktuell und übersichtlich** – und vermeiden es, Altlasten im Applikationsbestand mitzuschleppen.

Cloud Discovery zur Erkennung von Schatten-IT nutzen

Pfad: security.microsoft.com → Cloud Apps → Cludentdeckung → **Ermittelte Apps**

Im **Microsoft 365 Defender Portal** haben Sie über **Cloud Discovery** die Möglichkeit zu prüfen, welche Anwendungen in Ihrer Umgebung tatsächlich genutzt werden.

Diese Auswertungen basieren unter anderem auf:

- Daten aus Defender for Endpoint
- Protokollen Ihrer Firewall
- Informationen aus einem vorhandenen Web Application Proxy
- sowie ggf. weiteren Netzwerkproxies.

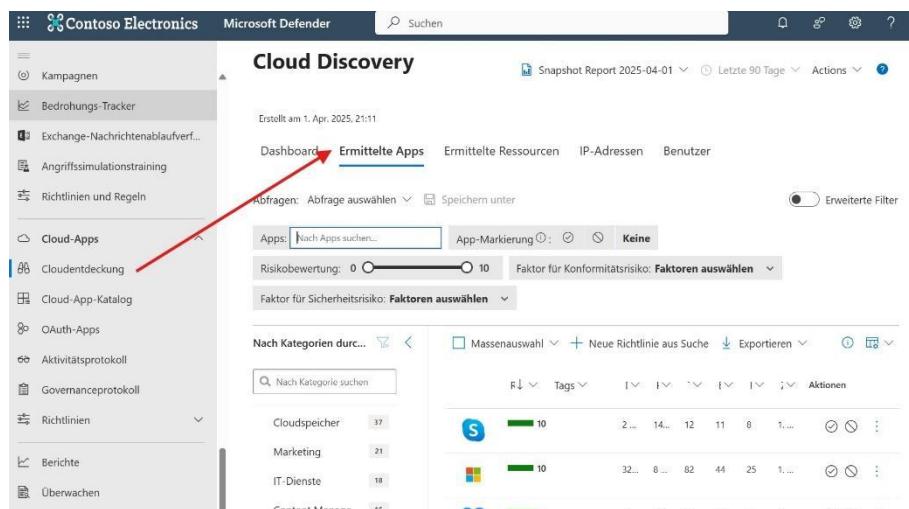


Abbildung 084

Alle gesammelten Daten werden **visuell aufbereitet** und bieten uns einen klaren Überblick über die eingesetzten Anwendungen und Dienste.

Zusätzlich zur Entra ID empfiehlt es sich, auf dieser Grundlage zu prüfen, **welche Applikationen und Services tatsächlich gewünscht sind** – und welche möglicherweise unautorisiert verwendet werden.

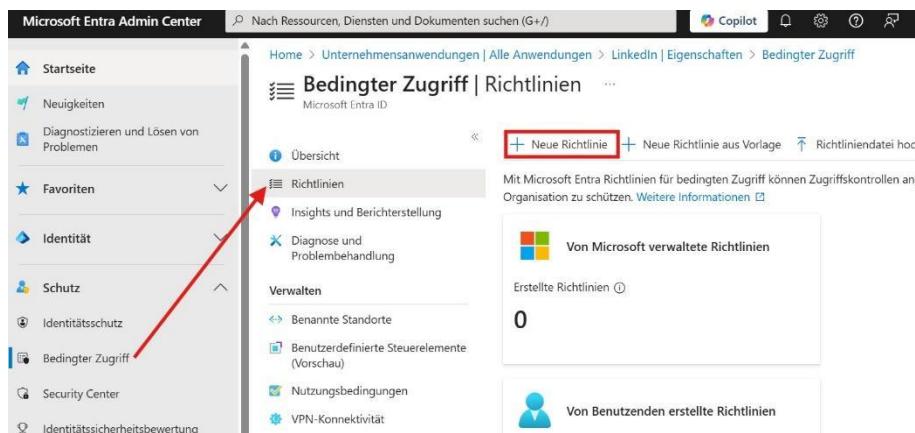
Die zugrunde liegende Technologie ist ein sogenannter **Cloud Access Security Broker (CASB)**. Ziel ist es, **Schatten-IT zu erkennen und zu verhindern** – also Anwendungen, die ohne Genehmigung eingesetzt werden und an der zentralen Benutzerverwaltung (z. B. Entra ID) vorbeilaufen.

Wenn wir **Netzwerk-Logs vollständig bereitstellen**, erhalten wir ein deutlich umfassenderes Bild der tatsächlichen Nutzung. So ergänzen wir unsere Sicherheitsstrategie um eine **weitere, tiefgreifende Kontrolle** über die eingesetzten Cloud-Dienste.

Konfiguration von Conditional Access für Copilot

Ein zentraler Aspekt für die sichere Nutzung von Microsoft 365 Copilot ist der Einsatz von **Conditional Access**. Diese Funktion erlaubt es uns, den Zugriff auf bestimmte Dienste gezielt zu steuern – abhängig von Gerät, Standort oder Benutzerrolle.

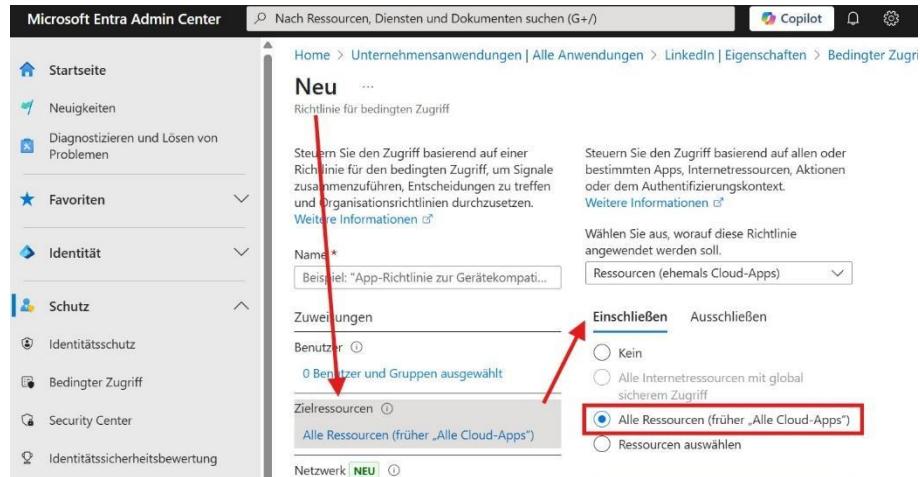
Pfad: entra.microsoft.com → Schutz → Bedingter Zugriff → Richtlinien → Neue Richtlinie



The screenshot shows the Microsoft Entra Admin Center interface. The left sidebar has a red arrow pointing from the 'Bedingter Zugriff' link to the 'Richtlinien' link in the main content area. The main content area is titled 'Bedingter Zugriff | Richtlinien' and contains a list of navigation links: Übersicht, Richtlinien (highlighted with a red box), Insights und Berichterstellung, Diagnose und Problembehandlung, Verwalten, Benannte Standorte, Benutzerdefinierte Steuerelemente (Vorschau), Nutzungsbedingungen, and VPN-Konnektivität. Below these are two sections: 'Von Microsoft verwaltete Richtlinien' (Erstellte Richtlinien: 0) and 'Von Benutzenden erstellte Richtlinien' (0). At the top right, there are buttons for 'Neue Richtlinie', 'Neue Richtlinie aus Vorlage', and 'Richtliniendatei hochladen'. The URL in the address bar is 'Home > Unternehmensanwendungen | Alle Anwendungen > LinkedIn | Eigenschaften > Bedingter Zugriff'.

Abbildung 085

Hier klicken wir über **Neue Richtlinie** weiter zu **Zielressourcen**, um zu bestimmen, auf welche Dienste sich die Richtlinie beziehen soll.

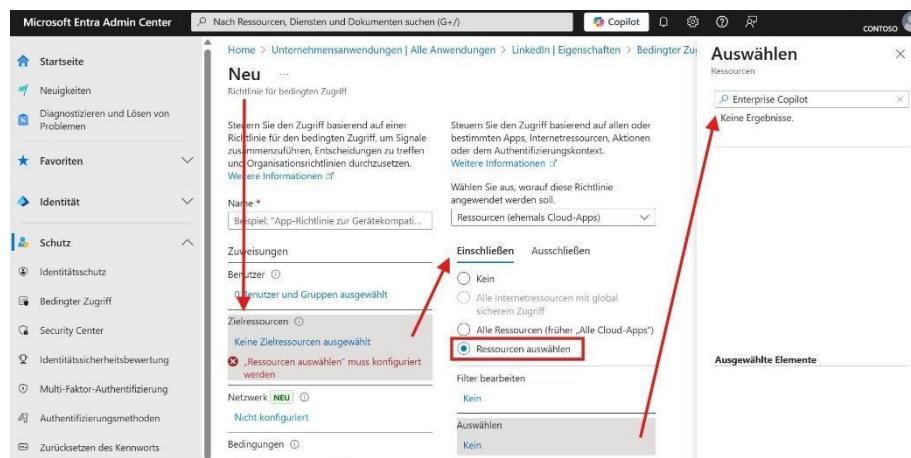


The screenshot shows the Microsoft Entra Admin Center interface. On the left, there's a navigation sidebar with links like Startseite, Neuigkeiten, Diagnosieren und Lösen von Problemen, Favoriten, Identität, Schutz, Identitätsschutz, Bedingter Zugriff, Security Center, and Identitätssicherheitsbewertung. The main area is titled 'Neu' and describes a 'Richtlinie für bedingten Zugriff'. It includes sections for 'Name' (with a placeholder 'Beispiel: "App-Richtlinie zur Gerätekompat...")', 'Zuweisungen' (User assignment), and 'Zielressourcen' (Target resources). Under 'Zielressourcen', the option 'Alle Ressourcen (früher „Alle Cloud-Apps“)' is selected. Below this, there are buttons for 'Einschließen' (Include) and 'Ausschließen' (Exclude), with radio buttons for 'Kein', 'Alle Internetressourcen mit global sicherem Zugriff', and 'Alle Ressourcen (früher „Alle Cloud-Apps“)', where the last one is checked. A red arrow points to the 'Alle Ressourcen' button.

Abbildung 086

Enterprise Copilot als Zielressource sichtbar machen

Weiter unten wählen wir nun **Auswählen** und geben im Suchfeld als Beispiel **Enterprise** ein. Falls **Enterprise Copilot** nicht angezeigt wird, liegt das daran, dass dieser Dienst noch **nicht als Service Principal** in unserer Umgebung hinterlegt ist.



The screenshot shows the Microsoft Entra Admin Center interface. The main blade is identical to Abbildung 086. On the right, a modal dialog box titled 'Auswählen' (Select) is open. It has a search bar containing 'Enterprise Copilot'. Below the search bar, it says 'Keine Ergebnisse.' (No results). At the bottom of the dialog, there's a section labeled 'Ausgewählte Elemente' (Selected elements) which is currently empty. A red arrow points from the 'Zielressourcen' section in the main blade to the 'Auswählen' dialog, and another red arrow points to the search bar in the dialog.

Abbildung 087

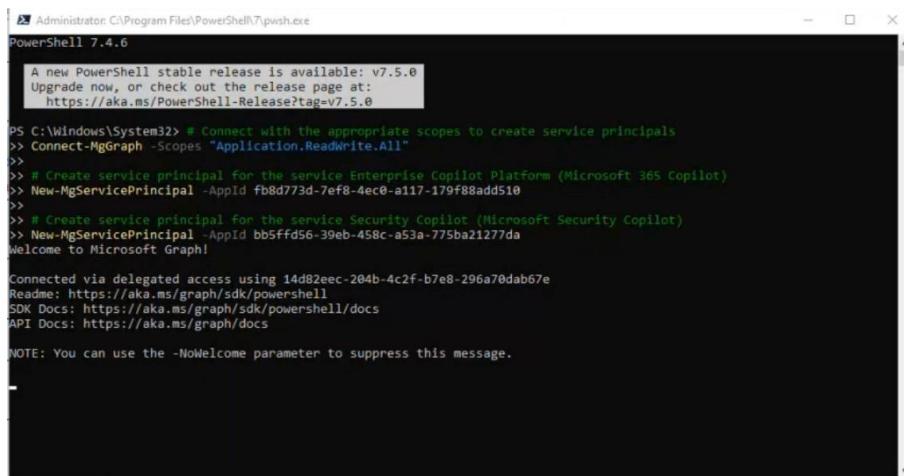
Damit Copilot über Conditional Access gezielt angesprochen werden kann, muss er zunächst als **Service Principal** registriert werden. Dieser Eintrag bildet die technische Grundlage dafür, um Zugriffsregeln für den Copilot festzulegen – beispielsweise

- von welchen Standorten darauf zugegriffen werden darf
- welche Benutzergruppen Zugriff erhalten und/oder
- ob bestimmte Gerätekonfigurationen erforderlich sind.

Sobald der Service Principal angelegt wurde, kann Copilot **wie jeder andere Cloud-Dienst** in einer Conditional Access Richtlinie verwendet werden.

Mit dem folgenden **Script-Link** können wir diesen Schritt via PowerShell gezielt ausführen. Die entsprechenden Befehle lassen sich direkt anwenden, um die Registrierung durchzuführen.

So stellen Sie sicher, dass Microsoft 365 Copilot von Beginn an **in Ihre Zugriffsstrategie eingebunden** ist.



```
A new PowerShell stable release is available: v7.5.0
Upgrade now, or check out the release page at:
https://aka.ms/PowerShell-Release?tag=v7.5.0

PS C:\Windows\System32> # Connect with the appropriate scopes to create service principals
>> Connect-MgGraph -Scopes "Application.ReadWrite.All"
>>
>> # Create service principal for the service Enterprise Copilot Platform (Microsoft 365 Copilot)
>> New-MgServicePrincipal -AppId fb8d773d-7ef8-4ec0-a117-179f88add510
>>
>> # Create service principal for the service Security Copilot (Microsoft Security Copilot)
>> New-MgServicePrincipal -AppId bb5ffd56-39eb-458c-a53a-775ba21277da
Welcome to Microsoft Graph!

Connected via delegated access using 14d82eec-204b-4c2f-b7e8-296a70dab67e
Readme: https://aka.ms/graph/sdk/powershell
SDK Docs: https://aka.ms/graph/sdk/powershell/docs
API Docs: https://aka.ms/graph/docs

NOTE: You can use the -NoWelcome parameter to suppress this message.
```

Abbildung 088

Nach Ausführung dieser Befehle sollte der Enterprise Copilot im Suchfeld angezeigt werden.

Empfohlene Richtlinien zur praktischen Umsetzung mit Copilot

Sorgfältig konfigurierte Richtlinien für Conditional Access stärken die Sicherheit beim Einsatz von Microsoft 365 Copilot. Geräte, Standorte, Risiken und Authentifizierung lassen sich gezielt steuern – inklusive Ausnahmen für Notfallzugriffe.

Pfad: entra.microsoft.com → Schutz → Bedingter Zugriff → Richtlinien → Neue Richtlinie

Im Folgenden erhalten Sie einige Ansätze, die Sie möglicherweise bereits in Teilen umgesetzt haben. Ziel ist es, diese vorhandenen Strukturen gezielt darauf auszurichten, wie sie für den Einsatz von Microsoft 365 Copilot weiter genutzt oder angepasst werden können.

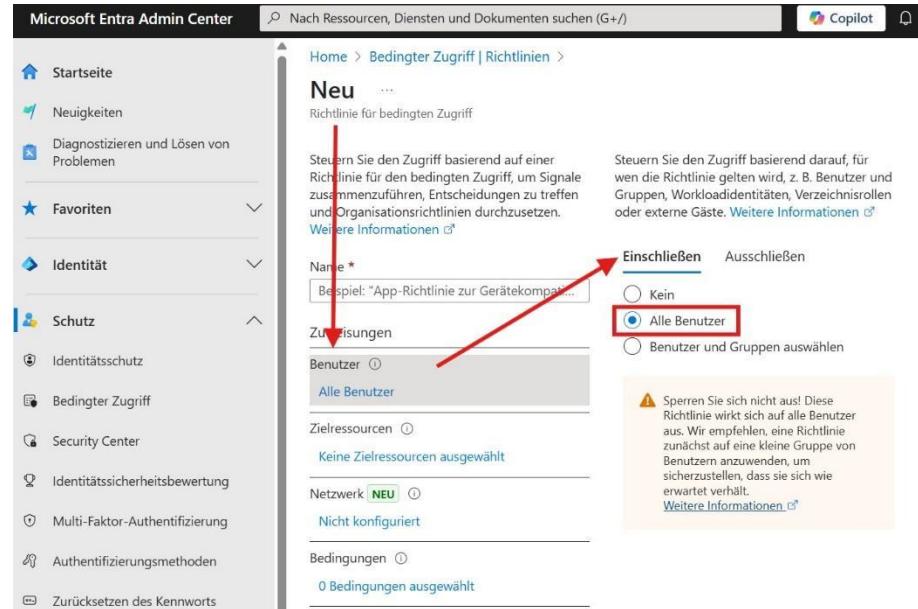
Any-Any-Richtlinie mit Ausschluss des Break-Glass-Accounts

Microsoft empfiehlt, **mindestens eine** sogenannte Any-Any-Richtlinie in unserer Umgebung zu konfigurieren. Diese umfasst grundsätzlich alle Benutzer im Tenant, um einheitliche Sicherheitsstandards zu gewährleisten.

Dabei gilt jedoch ein wichtiger Grundsatz: Unser Break-Glass-Account **darf niemals** von solchen Richtlinien erfasst werden. Dieser spezielle administrative Notfallzugang muss jederzeit verfügbar bleiben – auch dann, wenn alle anderen Zugänge durch eine Fehlkonfiguration oder technische Probleme blockiert sind.

Dazu gehen wir wie folgt vor:

Wir starten eine neue Richtlinie. Unter **Einschließen** wählen wir **Alle Benutzer**; unter **Ausschließen** schließen wir den Break-Glass-Account aus, indem wir **Benutzer und Gruppen** auswählen.

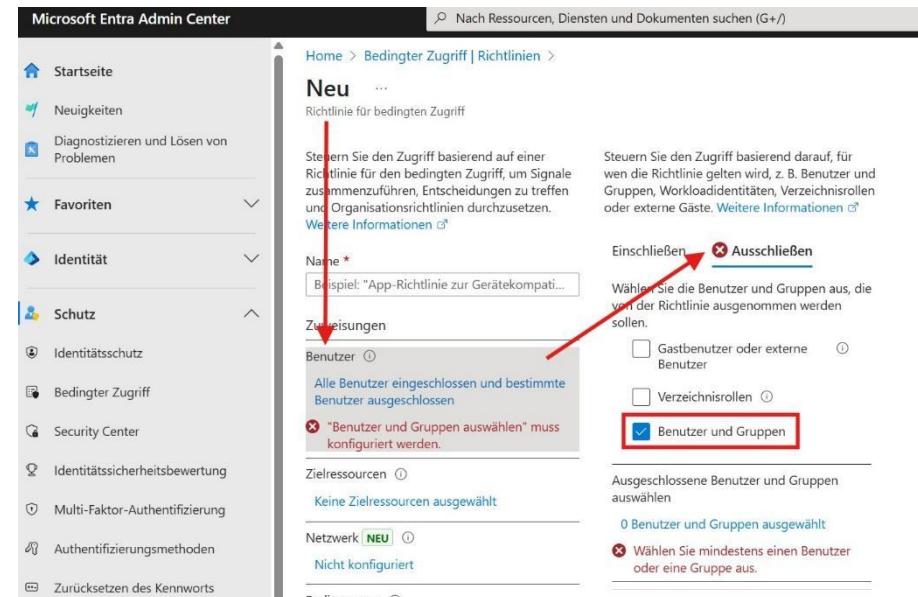


The screenshot shows the Microsoft Entra Admin Center interface. On the left, there's a navigation sidebar with categories like Startseite, Neuigkeiten, Diagnostizieren und Lösen von Problemen, Favoriten, Identität, Schutz (Identity Protection, Bedingter Zugriff, Security Center, Identitätssicherheitsbewertung, Multi-Faktor-Authentifizierung, Authentifizierungsmethoden, Zurücksetzen des Kennworts), and others.

The main content area is titled "Neu" and "Richtlinie für bedingten Zugriff". It includes a description: "Steuern Sie den Zugriff basierend auf einer Richtlinie für den bedingten Zugriff, um Signale zusammenzuführen, Entscheidungen zu treffen und Organisationsrichtlinien durchzusetzen." Below this is a "Name" field with the placeholder "Beispiel: 'App-Richtlinie zur Gerätekompat...'" and a "Zuweisungen" section where "Alle Benutzer" is selected.

On the right, there are two tabs: "Einschließen" (selected) and "Ausschließen". Under "Einschließen", "Alle Benutzer" is selected. A warning message states: "Sperren Sie sich nicht aus! Diese Richtlinie wirkt sich auf alle Benutzer aus. Wir empfehlen, eine Richtlinie zunächst auf eine kleine Gruppe von Benutzern anzuwenden, um sicherzustellen, dass sie sich wie erwartet verhält." Under "Ausschließen", "Benutzer und Gruppen auswählen" is selected, and a note says: "* 'Benutzer und Gruppen auswählen' muss konfiguriert werden." There are also checkboxes for "Gastbenutzer oder externe Benutzer" and "Verzeichnisrollen".

Abbildung 089



This screenshot is identical to Abbildung 089, but the "Ausschließen" tab is now selected instead of "Einschließen". The "Alle Benutzer" selection is now highlighted with a red arrow. The warning message about locking users out is still present. The "Benutzer und Gruppen auswählen" note is also visible, along with the checkboxes for "Gastbenutzer oder externe Benutzer" and "Verzeichnisrollen".

Abbildung 090

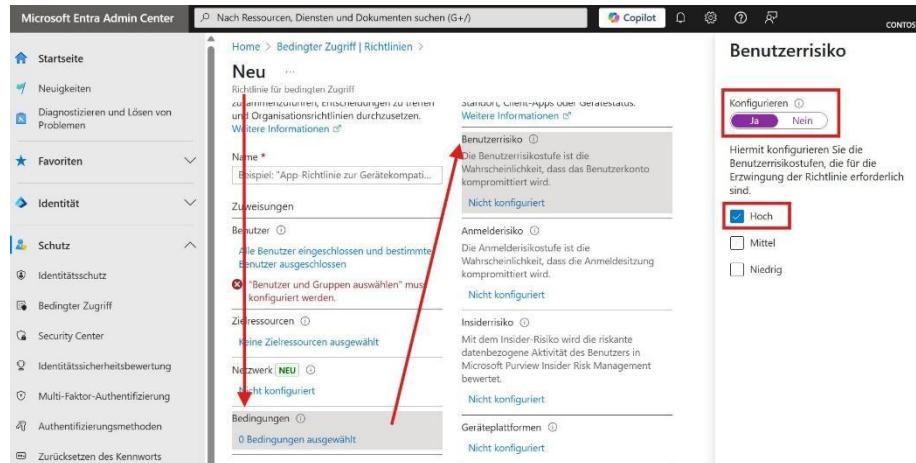
Auch wenn der Ausschluss des Break-Glass-Accounts technisch korrekt und sicherheitsseitig notwendig ist, hat das **Auswirkungen auf den Microsoft Secure Score**. Dieser Score bewertet die Sicherheit unserer Tenant-Konfiguration – und durch den Ausschluss des Break-Glass-Accounts kann es zu einer **niedrigeren Bewertung** kommen.

Dieses Risiko wird jedoch bewusst in Kauf genommen, da es **keine Alternative gibt**, um die **dauerhafte Verfügbarkeit des Notfallzugangs** sicherzustellen.

Benutzer- und Anmelderisiko im CA richtig konfigurieren

Pfad: entra.microsoft.com → Schutz → Bedingter Zugriff → Richtlinien → Neue Richtlinie → Bedingungen → **Benutzerrisiko** und **Anmelderisiko**

Bei der Konfiguration von Conditional Access ist besondere Vorsicht geboten – vor allem bei den Bedingungen **Benutzerrisiko** und **Anmelderisiko**. Viele setzen beispielsweise das Benutzerrisiko auf **Hoch** und kombinieren das mit einem auf **Niedrig** gesetzten Anmelderisiko oder wählen in beiden Kategorien **alle Optionen außer Kein Risiko** aus.



The screenshot shows the Microsoft Entra Admin Center interface. On the left, the navigation menu includes 'Startseite', 'Neuigkeiten', 'Durchsuchen und Lösen von Problemen', 'Favoriten', 'Identität', 'Schutz' (selected), 'Identitätsschutz', 'Bedingter Zugriff' (selected), 'Security Center', 'Identitätssicherheitsbewertung', 'Multi-Faktor-Authentifizierung', 'Authentifizierungsmethoden', and 'Zurücksetzen des Kennworts'. The main content area shows a 'Neu' (New) dialog for creating a rule. It includes fields for 'Name' (e.g., 'App-Richtlinie zur Gerätekompat...'), 'Zuweisungen' (Assignments), 'Benutzer' (Users), 'Zielressourcen' (Target resources), 'Netzwerk' (Network), and 'Bedingungen' (Conditions). The 'Bedingungen' section has a note: 'Alle Benutzer eingeschlossen und bestimmte Benutzer ausgeschlossen' (All users included and specific users excluded). The 'Benutzerrisiko' section shows 'Hoch' (High) is selected. The 'Anmelderisiko' section shows 'Niedrig' (Low) is selected. The right panel, titled 'Benutzerrisiko', contains configuration options for user risk levels: 'Ja' (Yes) is selected for 'Hoch' (High), while 'Mittel' (Medium) and 'Niedrig' (Low) are unselected. A note states: 'Hiermit konfigurieren Sie die Benutzerrisikostufen, die für die Erzwingung der Richtlinie erforderlich sind.'

Abbildung 091



The screenshot shows the Microsoft Entra Admin Center interface for creating a new conditional access rule. The rule is titled 'Neu' and applies to all users while excluding specific ones. It does not target any specific licenses. Under 'Bedingungen', there are no conditions applied. On the right, the 'Anmelderisiko' (Login Risk) section is configured with 'Ja' (Yes) selected. The 'Insiderisiko' (Insider Risk) section has 'Niedrig' (Low) selected.

Abbildung 092

Das wirkt auf den ersten Blick vollständig – führt aber in der Praxis dazu, dass die Richtlinie **nicht mehr greift**. Denn: Wenn ein Benutzer z. B. ein hohes **Benutzerrisiko** hat, aber **kein erhöhtes Anmelderisiko**, wird die kombinierte Bedingung **nicht erfüllt** – die Richtlinie wird ignoriert.

Empfehlung: Konfigurieren Sie **separate Richtlinien** – eine für Benutzerrisiko und eine für Anmelderisiko. So vermeiden Sie, dass sich beide Bedingungen gegenseitig ausschließen. Auch für Microsoft 365 Copilot gelten diese Regeln.

Tipp: Hoch schließt Mittel und Niedrig nicht automatisch ein – diese Stufen müssen explizit ausgewählt werden, wenn gewünscht.

Zugriff nach Geräteplattformen steuern

Neben **Benutzerrisiko** und **Anmelderisiko** sollten wir auch den Faktor **Geräteplattformen** in Ihre Sicherheitsrichtlinien einbeziehen. Diese Einstellung ermöglicht es, den Zugriff auf Microsoft 365 – einschließlich Copilot – nur von **bestimmten Gerätetypen** zuzulassen.

Arbeiten wir beispielsweise im Unternehmen ausschließlich mit Windows und Android, sollten Sie **alle nicht genutzten Plattformen gezielt blockieren**.

Schritt 1: Pfad: entra.microsoft.com → Schutz → Bedingter Zugriff → Richtlinien → Neue Richtlinie → Bedingungen → **Geräteplattformen**

The screenshot shows the Microsoft Entra Admin Center interface. On the left, the navigation menu includes 'Startseite', 'Neuigkeiten', 'Diagnosieren und Lösen von Problemen', 'Favoriten', 'Identität', 'Schutz', 'Identitätschutz', 'Bedingter Zugriff', 'Security Center', 'Identitätsicherheitsbewertung', 'Multi-Faktor-Authentifizierung', 'Authentifizierungsmethoden', and 'Zurücksetzen des Kennworts'. The main pane displays a 'Neu' (New) configuration page for a 'Richtlinie für bedingten Zugriff'. The 'Bedingungen' (Conditions) section shows '1 Bedingung ausgewählt' (1 condition selected). A red arrow points from this section to the 'Geräteplattformen' (Device platforms) configuration panel on the right. This panel has a title 'Geräteplattformen' with a note 'Wenden Sie die Richtlinie auf ausgewählte Gerätetypen an.' Below it are two tabs: 'Konfigurieren' (Configure) with a 'Ja' (Yes) button highlighted with a red box, and 'Weitere Informationen' (More information). The 'Einschließen' (Include) tab is selected, showing options like 'Jedes Gerät' (Every device), 'Geräteplattformen auswählen' (Select device platforms), and checkboxes for 'Android', 'iOS', 'Windows Phone' (which is checked), 'Windows', 'macOS', and 'Linux'.

Abbildung 093

Schritt 2: Pfad: entra.microsoft.com → Schutz → Bedingter Zugriff → Richtlinien → Neue Richtlinie → Gewähren

The screenshot shows the Microsoft Entra Admin Center interface. The left navigation menu is identical to Abbildung 093. The main pane displays a 'Neu' configuration page for a 'Richtlinie für bedingten Zugriff'. The 'Gewähren' (Grant) section shows '0 Steuerelemente ausgewählt' (0 controls selected). A red arrow points from this section to the 'Gewähren' configuration panel on the right. This panel has a title 'Gewähren' with a note 'Steuern Sie die Zugriffserzwingung, um den Zugriff zu blockieren oder zu gewähren. Weitere Informationen'. It contains two radio buttons: 'Blockzugriff' (Block access) (selected) and 'Zugriff gewähren' (Allow access). Below these are several checkboxes: 'Multi-Faktor-Authentifizierung erfordern' (Multi-factor authentication required), 'Authentifizierungsstärke erforderlich' (Authentication strength required), 'Markieren des Geräts als kompatibel erforderlich' (Mark device as compatible required), 'In Microsoft Entra hybrid eingebundenes Gerät erforderlich' (Hybrid device in Microsoft Entra required), 'Genehmigte Client-App erforderlich' (Required approved client app), 'Liste der genehmigten Client-Apps anzeigen' (Show list of approved client apps), 'App-Schutzrichtlinie erforderlich' (Required app protection policy), 'Liste der durch Richtlinien geschützten Client-Apps anzeigen' (Show list of protected client apps), and 'Kennwortänderung anfordern' (Require password change).

Abbildung 094

Zugriff auf Copilot nach Land oder IP gezielt einschränken

Über Conditional Access haben wir die Möglichkeit, den Zugriff auf Microsoft 365 Copilot basierend auf **geografischen Standorten** oder IP-Adressen gezielt zu steuern. In der Praxis spricht man hierbei von einem Blacklisting.

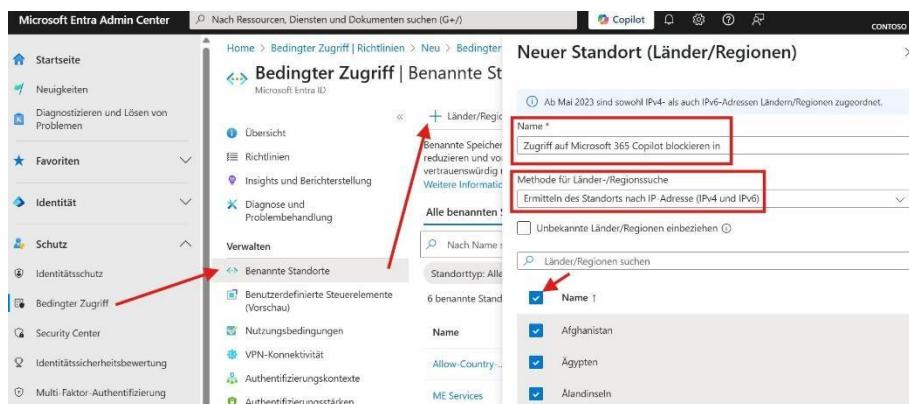
Wir können definieren, **aus welchen Ländern oder Regionen** Anmeldungen und Zugriffe auf den Copilot-Dienst **erlaubt oder blockiert** werden sollen. Besonders im Rahmen einer gezielten Tenant-Sicherheit ist es empfehlenswert, **nur die Länder freizuschalten, aus denen tatsächlich gearbeitet wird.**

Ein pauschales Blockieren *aller bösen Länder* ist dabei wenig sinnvoll – zumal sich politische oder rechtliche Einschätzungen schnell ändern können. Stattdessen sollten wir analysieren: **Wo befinden sich unsere Benutzer, und von wo aus sind Zugriffe berechtigt?**

Entsprechend konfigurieren wir eine neue Richtlinie:

Pfad: entra.microsoft.com → Schutz → Bedingter Zugriff → Benannte Standorte → **Länder/Regionen**

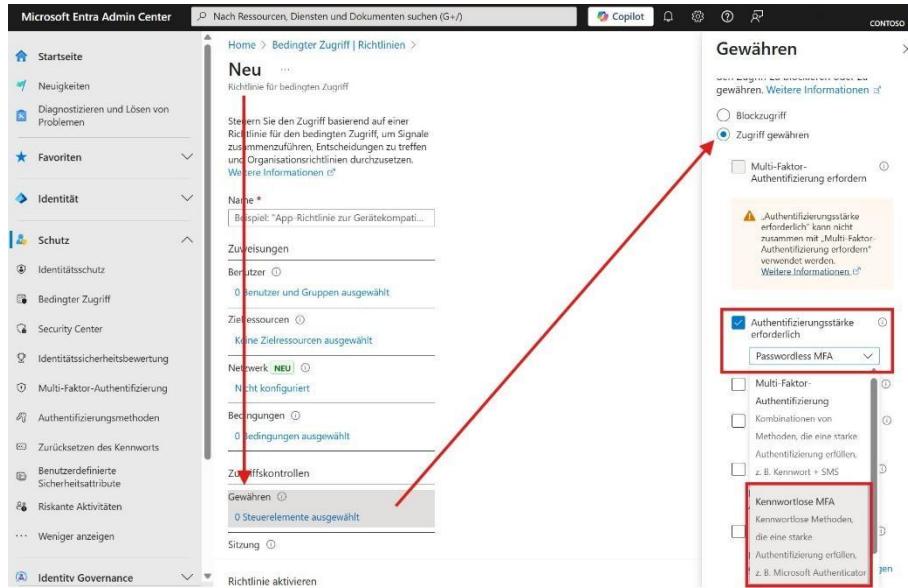
Hier definieren wir nun, von welchen Ländern aus der Zugriff erfolgen darf. Das eigene Land (z. B. **Germany**) wird dann **explizit ausgeschlossen**, um den Zugriff zuzulassen.



The screenshot shows the Microsoft Entra Admin Center interface. In the left sidebar under 'Schutz', the 'Bedingter Zugriff' option is selected. The main content area displays the 'Bedingter Zugriff | Benannte Standorte' configuration screen. A red arrow highlights the 'Bedingter Zugriff' link in the sidebar. Another red arrow points to the 'Name' input field in the 'Neuer Standort (Länder/Regionen)' dialog, which contains the text 'Zugriff auf Microsoft 365 Copilot blockieren in'. The dialog also includes a dropdown for 'Methode für Länder-/Regionsuche' and a checkbox for 'Unbekannte Länder/Regionen einbeziehen'.

Abbildung 095

Anschließend wählen wir via Pfad: entra.microsoft.com → Schutz → Bedingter Zugriff → Neue Richtlinie → **Gewähren** die Option **Zugriff gewähren** für alle übrigen Standorte, allerdings mit der weiteren Konfiguration: **Authentifizierungsstsärke erforderlich**, die Sie auf **Kenntwortlose MFA** zu setzen.



The screenshot shows the Microsoft Entra Admin Center interface. On the left, the navigation menu includes 'Startseite', 'Neigkeiten', 'Diagnosieren und Lösen von Problemen', 'Favoriten', 'Identität', 'Schutz' (selected), 'Identity Protection', 'Bedingter Zugriff', 'Security Center', 'Identity Security Assessment', 'Multi-Factor-Authentifizierung', 'Authentifizierungsmethoden', 'Zurücksetzen des Kennworts', 'Benutzerdefinierte Sicherheitsattribute', 'Risikosituationen', 'Weniger anzeigen', and 'Identity Governance'. The main pane shows a 'Neu' (New) configuration for a conditional access rule named 'Beispiel: "App-Richtlinie zur Gerätekompat...".' It lists 'Zuweisungen' (Assignments) with '0 Benutzer und Gruppen ausgewählt' (0 users and groups selected). Under 'Zielressourcen' (Target resources), it says 'Keine Zielressourcen ausgewählt' (No target resources selected). In the 'Netzwerk' (Network) section, 'NEU' is selected with 'Nicht konfiguriert' (Not configured). The 'Bedingungen' (Conditions) section shows '0 Bedingungen ausgewählt' (0 conditions selected). The 'Zugriffskontrollen' (Access controls) section is highlighted with a red box and contains 'Gewähren' (Grant) with '0 Steuerelemente ausgewählt' (0 policy elements selected) and 'Sitzung' (Session). The right pane, titled 'Gewähren' (Grant), has a red arrow pointing to the 'Zugriff gewähren' (Grant access) radio button. Below it, a warning message states: 'Authentifizierungsstärke erforderlich. Weitere Informationen.' (Required authentication strength. See more information.) A dropdown menu under 'Authentifizierungsstärke erforderlich' (Required authentication strength) shows 'Passwortlose MFA' (Passwordless MFA) selected. Other options include 'Multi-Faktor-Authentifizierung' (Multi-factor authentication), 'Kombinationen von Methoden, die eine starke Authentifizierung erfüllen' (Combinations of methods that meet strong authentication requirements), and 'z. B. Kennwort + SMS' (e.g. password + SMS). A red box highlights the 'Passwortlose MFA' option.

Abbildung 096

Empfehlung: Definieren Sie eine weitere Einschränkung über **IP-Adressbereiche**, um ungewollte Zugriffe – insbesondere auf Dienste wie Copilot – wirksam zu verhindern.

Pfad: entra.microsoft.com → Schutz → Bedingter Zugriff → **Richtlinien**

Sobald eine Richtlinie erstellt wurde finden wir den Punkt unter: Zugriffskontrollen → Gewähren → Authentifizierungsstärke erforderlich

Absicherung mit modernen MFA-Methoden

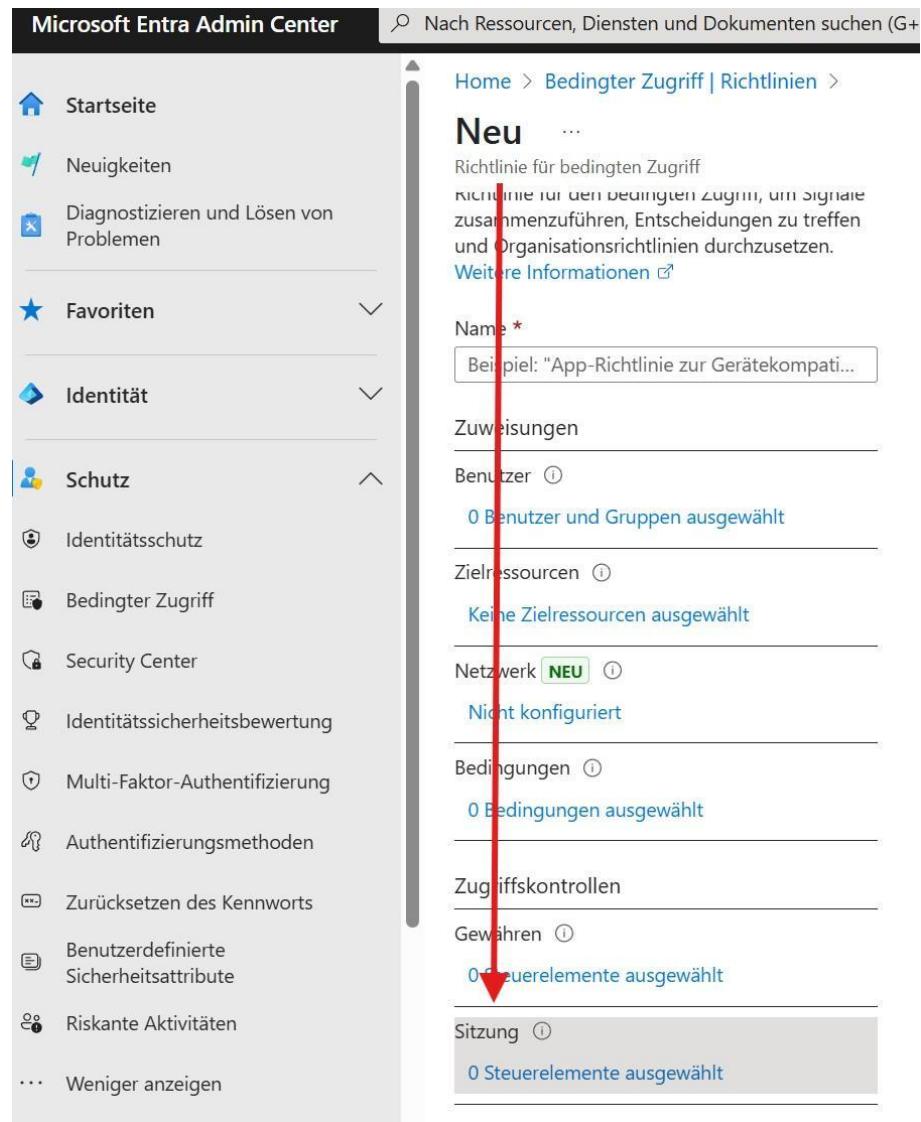
Microsoft empfiehlt mittlerweile klar den Einsatz des **Microsoft Authenticators mit Number Matching** und rät davon ab, weiterhin auf **SMS oder Telefonanrufe** als zweiten Faktor zu setzen. Diese gelten als vergleichsweise **unsichere MFA-Methoden**.

Solange in Ihrer Umgebung jedoch keine konkreten Einschränkungen vorgenommen wurden, können Benutzer unter Umständen dennoch auf **schwächere Methoden** zurückgreifen – selbst wenn stärkere Optionen technisch verfügbar wären.

Empfehlung: Statt einzelne MFA-Methoden zuzulassen oder zu verbieten, konfigurieren Sie **Authentication Strengths**. Diese definieren gezielt, welche Authentifizierungsverfahren erlaubt sind – etwa ausschließlich die Authenticator-App mit Number Matching.

Sie finden die Konfiguration unter **Authentifizierungsmethoden** im Microsoft Entra Admin Center. Dort lassen sich auch **User Registration Details** einsehen, um zu prüfen, welche Methoden bereits registriert wurden. Selbst wenn SMS und Anrufe technisch möglich sind, bedeutet das nicht automatisch, dass sie bereits verwendet werden – ein kurzer Abgleich kann Klarheit schaffen.

Pfad: entra.microsoft.com → Schutz → Bedingter Zugriff → Neue Richtlinie → **Sitzung**



The screenshot shows the Microsoft Entra Admin Center interface. On the left, there's a navigation sidebar with links like Startseite, Neuigkeiten, Diagnostizieren und Lösen von Problemen, Favoriten, Identität, and Schutz (which is expanded). Under Schutz, there are sub-links: Identitätsschutz, Bedingter Zugriff (which is selected and highlighted in blue), Security Center, Identitätssicherheitsbewertung, Multi-Faktor-Authentifizierung, Authentifizierungsmethoden, Zurücksetzen des Kennworts, Benutzerdefinierte Sicherheitsattribute, Riskante Aktivitäten, and Weniger anzeigen. The main content area is titled 'Neu' and describes a 'Bedingter Zugriff' rule. It includes sections for Name (with a placeholder 'Beispiel: "App-Richtlinie zur Gerätekompati...)'), Zuweisungen (User assignments: 0 Benutzer und Gruppen ausgewählt), Zielressourcen (Target resources: Keine Zielressourcen ausgewählt), Netzwerk (Network: NEU, Nicht konfiguriert), Bedingungen (Conditions: 0 Bedingungen ausgewählt), Zugriffskontrollen (Access controls: 0 Steuerelemente ausgewählt), and Sitzung (Session: 0 Steuerelemente ausgewählt). A red arrow points from the 'Authentifizierungsmethoden' section in the sidebar down to the 'Sitzung' section in the main content area.

Abbildung 097

Anmeldehäufigkeit zur erneuten Authentifizierung definieren

Pfad: entra.microsoft.com → Schutz → Bedingter Zugriff → Neue Richtlinie → **Sitzung**

Über den gleichen Pfad können wir nun ebenfalls die **Anmeldehäufigkeit** konfigurieren, die regelmäßig eine neue Authentifizierung erzwingt.

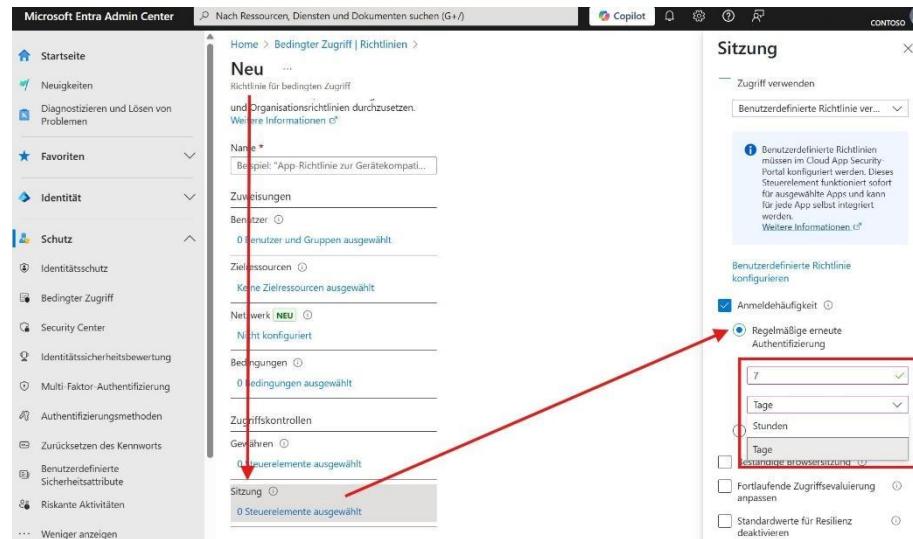
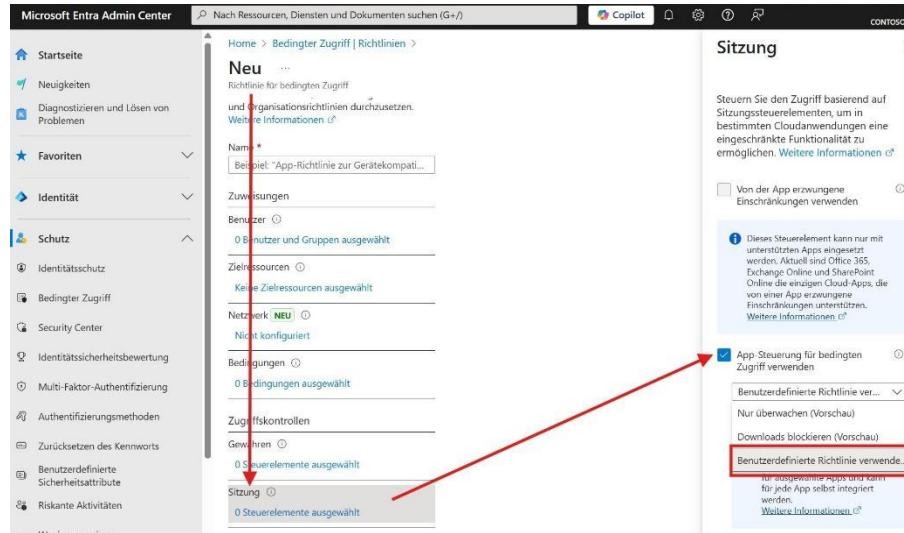


Abbildung 098

Darüber hinaus lässt sich über **App-Steuerung für bedingten Zugriff** festlegen, dass **Downloads blockiert werden**, wenn Copilot außerhalb des Unternehmensnetzwerks verwendet wird.

Gerade bei Nutzung auf privaten Geräten – etwa im Homeoffice – kann es sinnvoll sein, zu verhindern, dass **Ausgaben über Copilot heruntergeladen oder kopiert werden**. So bleibt die Kontrolle über sensible Inhalte auch in externen Nutzungsszenarien erhalten.



The screenshot shows the Microsoft Entra Admin Center interface. On the left, the navigation menu includes 'Startseite', 'Neuigkeiten', 'Diagnosieren und Lösen von Problemen', 'Favoriten', 'Identität', 'Schutz', 'Identitätschutz', 'Bedingter Zugriff', 'Security Center', 'Identitätsicherheitsbewertung', 'Multi-Faktor-Authentifizierung', 'Authentifizierungsmethoden', 'Zurücksetzen des Kennworts', 'Benutzerdefinierte Sicherheitsattribute', and 'Risikante Aktivitäten'. The main panel shows a 'Bedingter Zugriff | Richtlinien' configuration page for a new policy named 'Neu'. The policy settings include 'Richtlinie für bedingten Zugriff' (Conditional Access policy), 'Zuweisungen' (Assignments), 'Benutzer' (Users), 'Zielressourcen' (Target resources), 'Netzwerk' (Network), 'Bedingungen' (Conditions), 'Zugriffskontrollen' (Access controls), 'Gewähren' (Grant), and 'Sitzung' (Session). A red arrow points from the 'Sitzung' section to the 'Benutzerdefinierte Richtlinie ver...' dropdown, which is highlighted with a red border.

Abbildung 099

Copilot im Admin Center vorbereiten

Die effektive Nutzung von Copilot erfordert eine präzise Steuerung über das Admin Center. Dazu gehören Richtlinien zur Websuche, Agent- und Button-Verwaltung, Datenschutz sowie Einstellungen für Office, Teams und Edge.

Zur Vorbereitung von Microsoft 365 Copilot empfiehlt es sich, verschiedene Richtlinien im Admin Center zu definieren, um Zugriff, Sicherheit und Datenindexierung gezielt zu steuern.

SharePoint Search: Suchergebnisse gezielt einschränken

Die *Restricted SharePoint Search* ist eine sinnvolle Funktion, um die Indexierung und Darstellung von Inhalten in Microsoft 365 Copilot gezielt zu steuern. Sie definiert, **welche SharePoint-Seiten in die Suche einbezogen werden sollen** – alles andere bleibt außen vor.

Wenn Sie beispielsweise 100 spezifische Seiten für die Indexierung freigeben, **werden ausschließlich diese Inhalte von Copilot berücksichtigt**. Seiten, die nicht in der Freigabeliste enthalten sind, werden weder indexiert noch in Suchergebnissen vorgeschlagen.

Diese Funktion ist besonders relevant für Organisationen, die Copilot bereits nutzen, aber **nachträglich die Kontrolle über dessen Datenbasis stärken möchten** – etwa, wenn nicht klar ist, welche Inhalte bislang verarbeitet wurden.

Copilot zeigt dann nur noch Inhalte an, für die Benutzer entweder **explizit berechtigt** sind oder die Teil der freigegebenen Seitenliste sind. Es entfallen automatisch Vorschläge zu Inhalten, auf die kein gezielter Zugriff besteht.

Außerdem erhält der Benutzer einen **klaren Hinweis**, dass eine eingeschränkte Suche aktiv ist und ihm nicht alle Ergebnisse angezeigt werden.

Die Konfiguration erfolgt vollständig über PowerShell – es ist **keine zusätzliche Lizenz erforderlich**.

Bestehende Berechtigungen bleiben unaufgetastet, aber die Sichtbarkeit über die Suche wird entsprechend begrenzt.

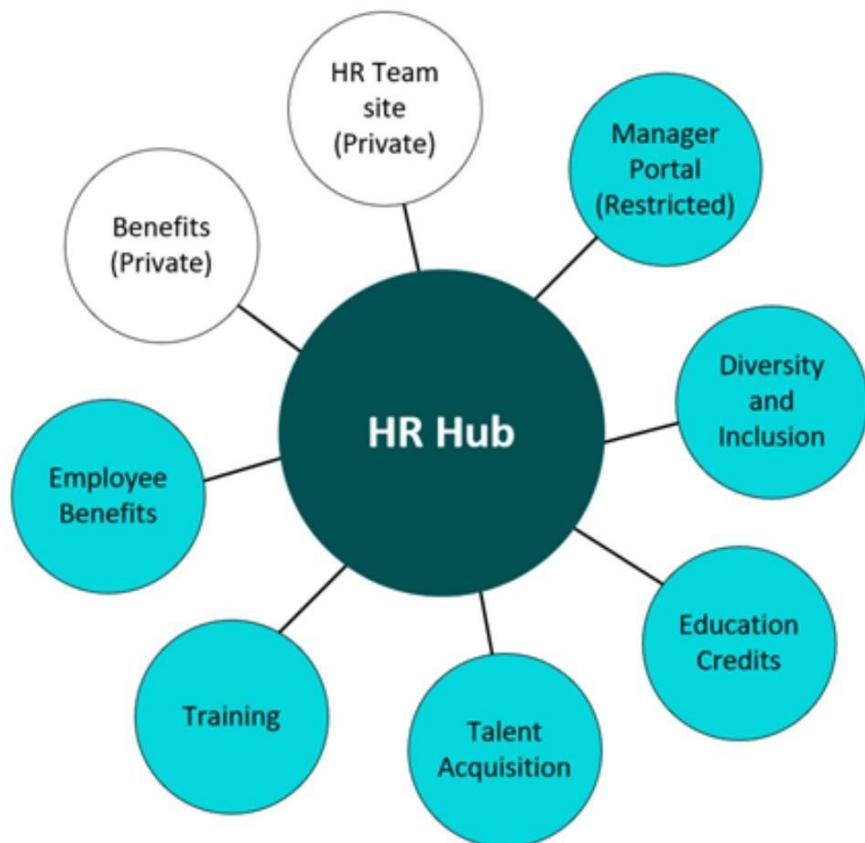


Abbildung 100

(Quelle: <https://learn.microsoft.com/de-de/sharepoint/sharepointonline/media/hub-nav.png>)

Beachten Sie bei der Verwendung der *Restricted SharePoint Search*: Die Begrenzung auf maximal 100 SharePoint-Seiten umfasst auch Hub Sites.

Tipp: Eine Hub Site mit mehreren Unterseiten zählt dennoch nur als **ein Eintrag in der Freigabeliste**. Das vereinfacht die Verwaltung erheblich – insbesondere, wenn Sie größere Inhaltsbereiche strukturiert zusammenfassen möchten.

So haben Sie die Möglichkeit, über die Auswahl einzelner Hubs eine deutlich größere Datenbasis freizugeben, **ohne** das Limit technisch auszureißen. Das verschafft Ihnen mehr Flexibilität bei der gezielten Indexierung von Inhalten für Microsoft 365 Copilot.

Die folgenden Links und Screenshots helfen bei der Konfiguration:

- **Connect to your SharePoint Online environment:** Connect-SPOService -Url <https://yourdomain-admin.sharepoint.com>
- **Enablement Restricted SharePoint Search:** Set-SPOTenantRestrictedSearchMode -Mode Enabled
- **Restricted SharePoint Search Status:** Get-SPOTenantRestrictedSearchMode
- **Hinzufügen von Seiten zur Allow-List:** Add-SPOTenantRestrictedSearchAllowedList -SitesList @ <https://yourdomain.sharepoint.com/sites/Site1> & <https://yourdomain.sharepoint.com/sites/Site2>



1.04 TB available of 1.05 TB

All sites

Standard views

- ✓ All sites
- Sites connected to Teams
- Microsoft 365 group sites
- Sites without a group
- Classic sites
- Largest sites
- Least active sites
- Most popular shared sites
- Active sites by page views
- Custom script allowed sites
- Save view as
- Set current view as default

Abbildung 101

Pfad: admin.sharepoint.com → Websites → Aktive Websites → Alle Websites

- **Ansicht aktueller Allowed Sites:** Get-SPOTenantRestrictedSearchAllowedList
- **Entfernung von SharePoint Seiten aus der Allowed List:** Remove-SPOTenantRestrictedSearchAllowedList -SitesList @
<https://yourdomain.sharepoint.com/sites/SiteToRemove>
- **Deaktivierung Restricted SharePoint Search:** Set-SPOTenantRestrictedSearchMode -Mode Disabled
- **Anmeldung SharePoint Online:**

```
o load this module into PowerShell please use 'Import-Module -SkipEditionCheck' syntax.
PS C:\Windows\System32> Connect-SPOService -Url https://sillerconsulting2017-admin.sharepoint.com/
>>
PS C:\Windows\System32> Get-SPOTenantRestrictedSearchMode
```

Abbildung 102

- **Validierung Status:**

```
PS C:\Windows\System32> Get-SPOTenantRestrictedSearchMode  
Restricted search mode is currently not set.
```

Abbildung 103

- **Aktivierung Restricted SharePoint Search:**

```
PS C:\Windows\System32> Set-SPOTenantRestrictedSearchMode -Mode Enabled  
>>  
PS C:\Windows\System32> Get-SPOTenantRestrictedSearchMode  
Enabled
```

Abbildung 104

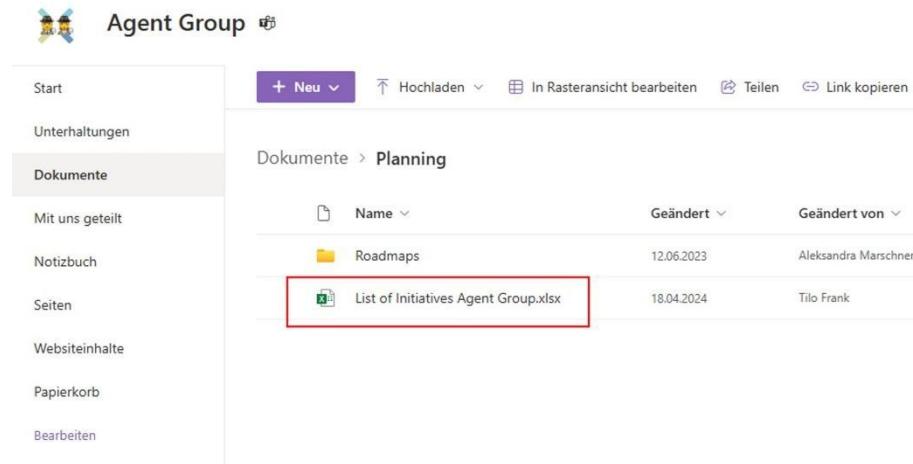
- **Hinzufügen von Seiten & Ansicht der Restricted Search:#**

```
PS C:\Windows\System32> Add-SPOTenantRestrictedSearchAllowedList -SitesList https://sillerconsulting2017.sharepoint.com/sites/EXT-P-Workshop  
PS C:\Windows\System32> Get-SPOTenantRestrictedSearchAllowedList  
>>  
https://sillerconsulting2017.sharepoint.com/sites/EXT-P-Workshop  
PS C:\Windows\System32>
```

Abbildung 105

- **Link zu allen Parametern in der Restricted SharePoint Search:** [Restricted SharePoint Search Admin PowerShell Scripts - SharePoint in Microsoft 365 | Microsoft Learn](#)

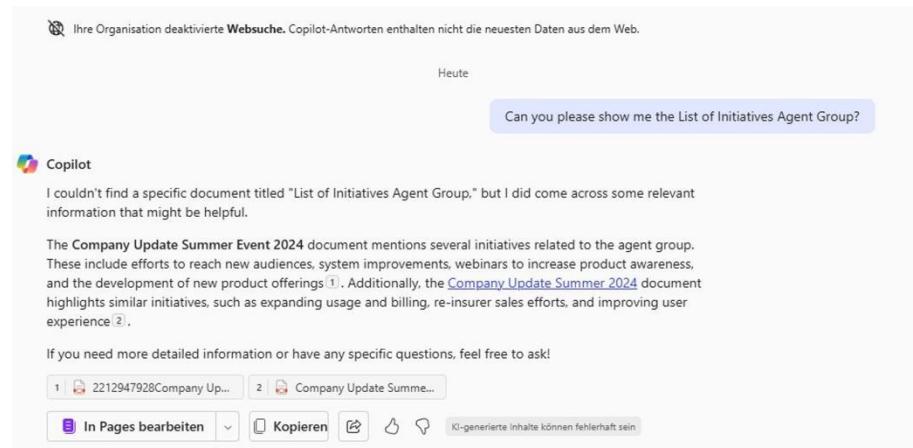
- User hat keinen Zugriff im SharePoint Online:



The screenshot shows a SharePoint Online interface. On the left, there's a navigation bar with links like Start, Unterhaltungen, Dokumente, Mit uns geteilt, Notizbuch, Seiten, Websiteinhalte, Papierkorb, and Bearbeiten. The 'Dokumente' link is currently selected. In the center, there's a list of documents under the 'Planning' category. One document, 'List of Initiatives Agent Group.xlsx', is highlighted with a red border. The list includes a folder named 'Roadmaps' and the highlighted document.

Abbildung 106

- Output im Microsoft 365 Copilot:



The screenshot shows the Microsoft 365 Copilot interface. At the top, it says 'Ihr Organisation deaktivierte Websuche. Copilot-Antworten enthalten nicht die neuesten Daten aus dem Web.' Below that is a timestamp 'Heute'. A user input box contains the text 'Can you please show me the List of Initiatives Agent Group?'. The Copilot response starts with 'I couldn't find a specific document titled "List of Initiatives Agent Group," but I did come across some relevant information that might be helpful.' It then provides a summary from a document about Company Update Summer 2024, mentioning initiatives related to the agent group. At the bottom, there are several interaction buttons and a note about AI-generated content being仅供参考 (for reference).

Abbildung 107

Hinweis zur Anzeige der Restricted Search Warnung: „The notification in Microsoft 365 Copilot appears when users attempt to access content that is not included in the allowed list. If all sites a user interacts with are permitted, the notification may not display.“

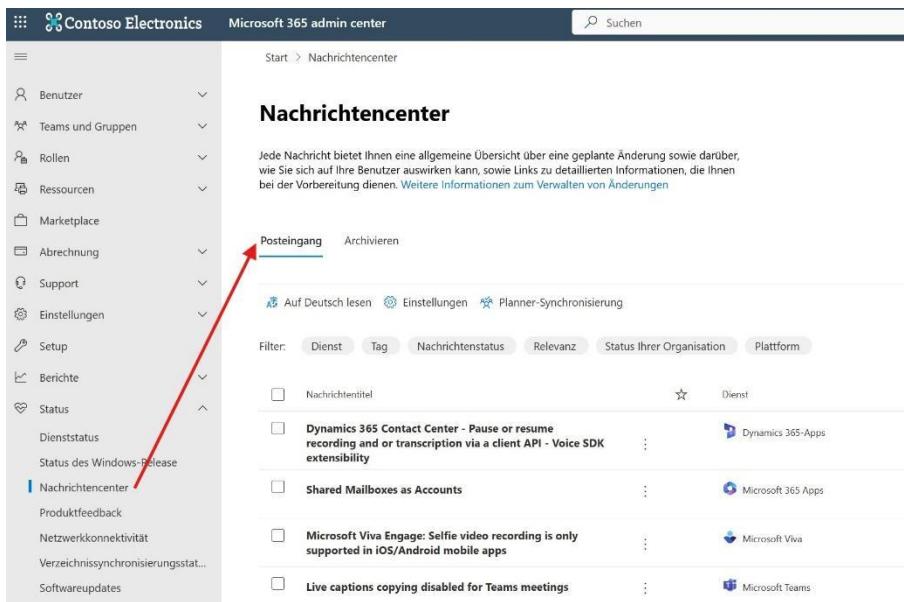
Die Aktivierung der *Restricted SharePoint Search* erfolgt technisch in wenigen Sekunden. Die tatsächliche Umsetzung im Hintergrund kann jedoch **bis zu 21 Tage dauern**, bevor sie vollständig wirksam wird.

Daher gilt: Wenn Sie die Einführung von Microsoft 365 Copilot planen, sollten Sie bereits im Vorfeld prüfen, **welche Inhalte indexiert werden sollen**. Sobald die Daten validiert sind, können Sie gezielt festlegen, welche Seiten in die Indexierung aufgenommen werden – und so eine kontrollierte, datenschutzkonforme Copilot-Nutzung sicherstellen.

Nutzung des Nachrichtencenters für Microsoft 365 Updates

Pfad: admin.microsoft.com → Status → **Nachrichtencenter**

Über das Nachrichtencenter können wir uns zentral über alle **aktuellen Microsoft 365 Updates** informieren lassen. Die Inhalte stammen direkt von Microsoft – nicht von Drittanbietern – und bieten somit eine verlässliche Quelle für Produktneuigkeiten, Funktionsänderungen und sicherheitsrelevante Hinweise.

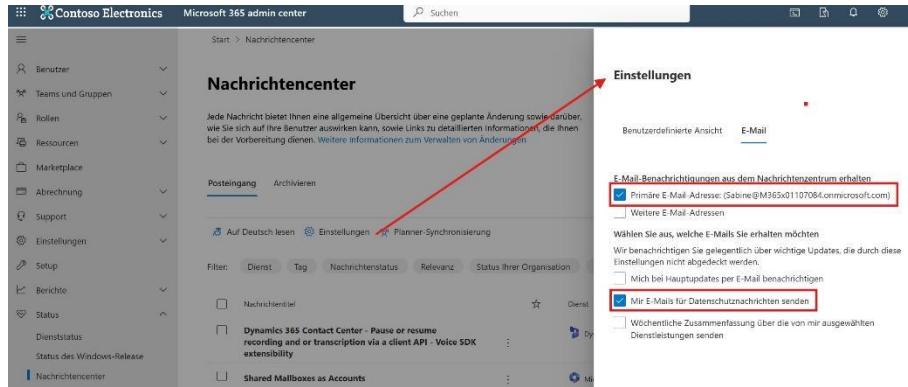


The screenshot shows the Microsoft 365 Admin Center interface for 'Contoso Electronics'. The left sidebar includes links for Benutzer, Teams und Gruppen, Rollen, Ressourcen, Marketplace, Abrechnung, Support, Einstellungen, Setup, Berichte, Status, Dienststatus, and Softwareupdates. The 'Nachrichtencenter' link is highlighted with a blue box. The main content area is titled 'Nachrichtencenter' and contains a summary about updates. Below it is a list of recent changes, each with a checkbox, a title, a service icon, and a brief description. The first item is 'Dynamics 365 Contact Center - Pause or resume recording and/or transcription via a client API - Voice SDK extensibility'.

Titel	Dienst
Dynamics 365 Contact Center - Pause or resume recording and/or transcription via a client API - Voice SDK extensibility	Dynamics 365-Apps
Shared Mailboxes as Accounts	Microsoft 365 Apps
Microsoft Viva Engage: Selfie video recording is only supported in iOS/Android mobile apps	Microsoft Viva
Live captions copying disabled for Teams meetings	Microsoft Teams

Abbildung 108

Wir können uns zudem E-Mail-Benachrichtigungen aus dem Nachrichtencenter einrichten. Auch wenn das nicht den regelmäßigen Blick in das Portal ersetzt, hilft es dabei, **relevante Änderungen frühzeitig mitzubekommen**.



The screenshot shows the Microsoft 365 admin center interface. On the left, there's a navigation menu with items like Benutzer, Teams und Gruppen, Rollen, Ressourcen, Marketplace, Abrechnung, Support, Einstellungen, Setup, Berichte, Status, Dienststatus, and Status des Windows-Release. The 'Nachrichtencenter' item is selected. In the main content area, there's a 'Nachrichtencenter' section with tabs for Posteingang and Archivieren. Below that, there are several news items listed. On the right, there's a sidebar titled 'Einstellungen' with tabs for Benutzerdefinierte Ansicht and E-Mail. Under E-Mail, there's a section for 'E-Mail-Benachrichtigungen aus dem Nachrichtenzentrum erhalten'. It includes a checkbox for 'Primäre E-Mail-Adresse: Sabine@M365x01107084.onmicrosoft.com' which is checked. Other options include 'Weitere E-Mail-Adressen', 'Wählen Sie aus, welche E-Mails Sie erhalten möchten', 'Mir E-Mails für Datenschutzbenachrichtigen' (which is checked), and 'Wöchentliche Zusammenfassung über die von mir ausgewählten Dienstleistungen senden'.

Abbildung 109

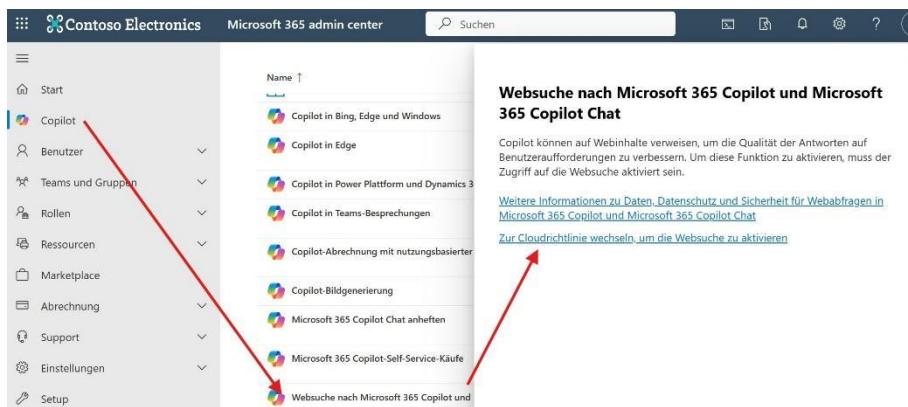
Wenn es darum geht, in Microsoft 365 stets auf dem neuesten Stand zu bleiben, ist das **Nachrichtencenter Ihre zentrale Anlaufstelle**.

Richtliniensteuerung für Microsoft Copilot in der Office-Suite

Pfad: admin.microsoft.com → Copilot: Websuche nach **Microsoft 365 Copilot und Microsoft 365 Copilot Chat**

Im Microsoft 365 Admin Center finden wir einen wichtigen Punkt für Copilot: **Websuche nach Microsoft 365 Copilot und Copilot Chat**. Ein Klick auf diese Option leitet uns weiter zur Cloud-Richtlinie, die über config.office.com verwaltet wird.

Dort haben Sie die Möglichkeit, spezifische Richtlinien für die Office-Suite und die darin integrierten Copilot-Funktionen zu konfigurieren.



The screenshot shows the Microsoft 365 admin center interface. On the left, there's a navigation menu with items like Start, Copilot (which is selected), Benutzer, Teams und Gruppen, Rollen, Ressourcen, Marketplace, Abrechnung, Support, Einstellungen, and Setup. The 'Copilot' item is highlighted with a red arrow. In the main content area, there's a search bar with the query 'Websuche nach Microsoft 365 Copilot und Microsoft 365 Copilot Chat'. Below the search bar, there's a list of results. One result, 'Websuche nach Microsoft 365 Copilot und Microsoft 365 Copilot Chat', has a red arrow pointing to it. At the bottom of the search results page, there's a link 'Zur Cloudrichtlinie wechseln, um die Websuche zu aktivieren' with another red arrow pointing to it.

Abbildung 110

Pfad: config.office.com → Anpassung → **Richtlinienkonfiguration**

Nach dem Login bei **config.office.com** können wir eine neue Richtlinie anlegen.

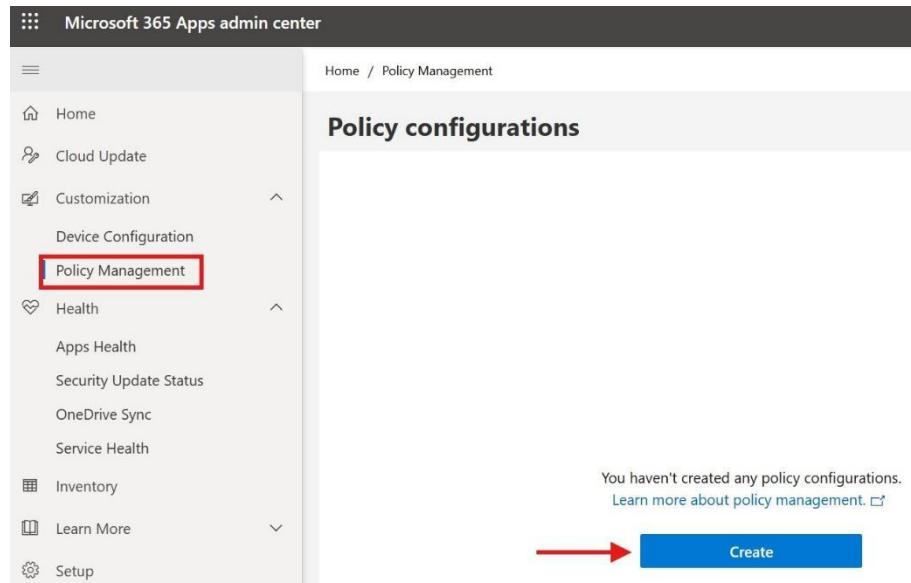


Abbildung 111

Schritt 1 – Grundlagen: Wir benennen die neue Richtlinie mit einem aussagekräftigen Titel.

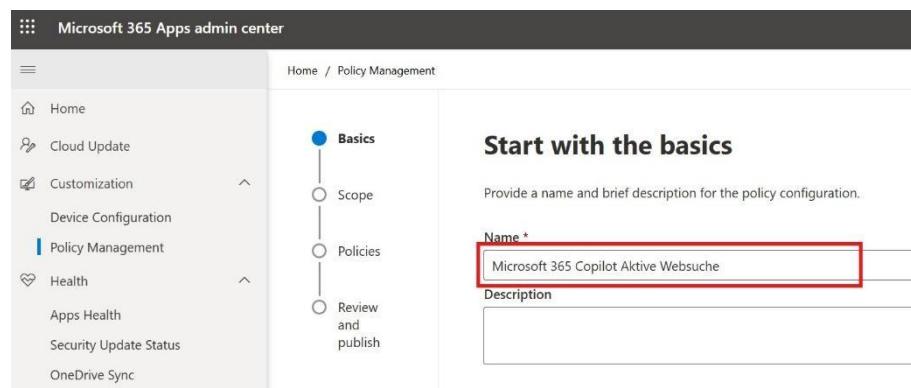


Abbildung 112

Schritt 2 – Bereich: Wir definieren für **welche Benutzergruppen oder Office-Versionen** sie gelten soll – etwa für alle Benutzer oder ausschließlich für Office Online.

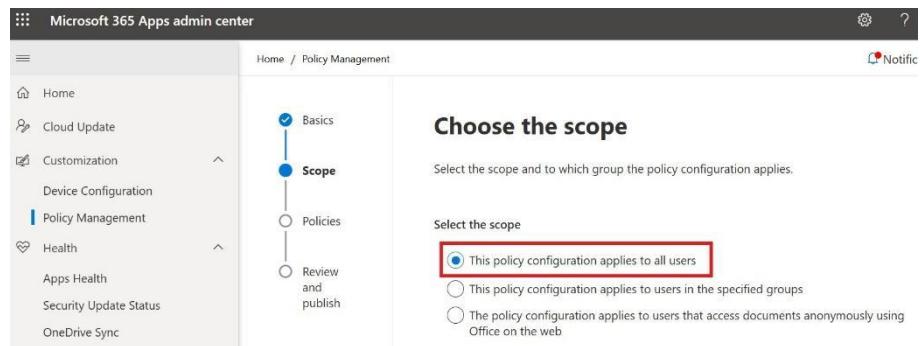


Abbildung 113

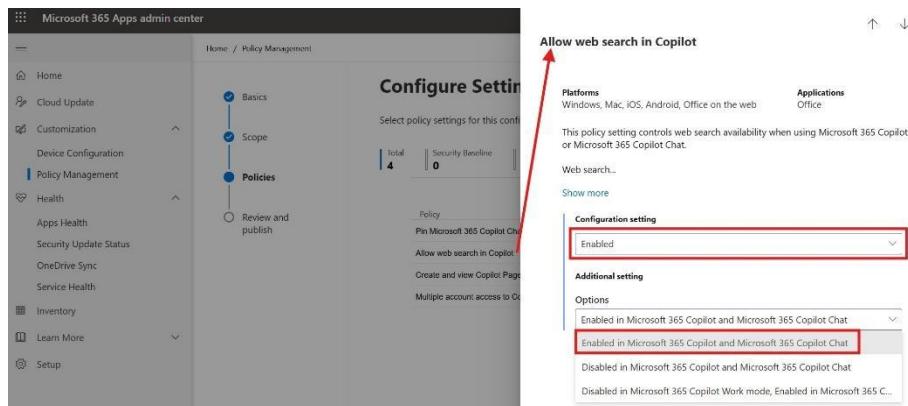
Schritt 3 – Richtlinien: Wir geben im Suchfeld auf der rechten Seite **Copilot** ein, wodurch uns alle bereits definierten Copilot-Richtlinien angezeigt werden.



Abbildung 114

Als Beispiel konfigurieren wir nun die Richtlinie: **Allow-Web-Search**. Diese bestimmt, ob **Web-Ergebnisse in Copilot und Copilot Chat eingeblendet werden dürfen**.

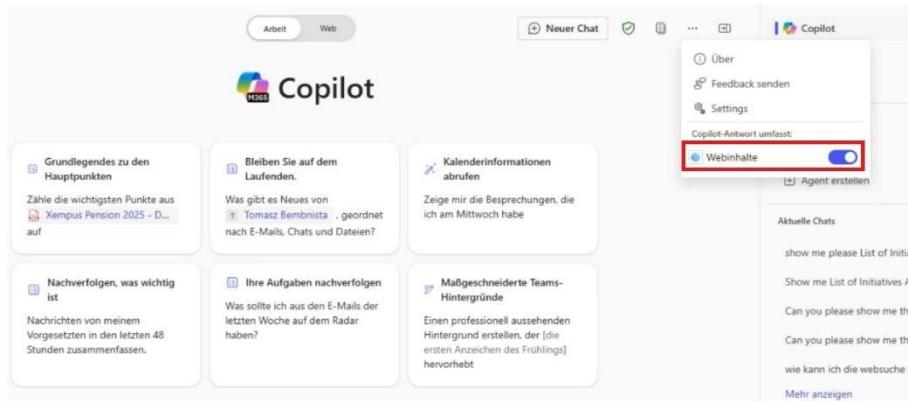
Standardmäßig ist diese Option aktiviert. Wenn Sie nicht möchten, dass Benutzer Web-Inhalte in Copilot angezeigt bekommen, müssen Sie die Option **explizit deaktivieren**.



The screenshot shows the Microsoft 365 Apps admin center interface. On the left, there's a navigation sidebar with various options like Home, Cloud Update, Customization, Device Configuration, Policy Management, Health, Apps Health, Security Update Status, OneDrive Sync, Service Health, Inventory, Learn More, and Setup. The main area is titled 'Configure Settings' under 'Policy Management'. It shows a summary of policy settings: 4 items, 0 security baseline, and a policy named 'Pin Microsoft 365 Copilot Chat'. Below this, there's a section for 'Allow web search in Copilot' with a red arrow pointing to it. The configuration setting dropdown is set to 'Enabled', and the additional settings dropdown is also set to 'Enabled in Microsoft 365 Copilot and Microsoft 365 Copilot Chat'. Other options in the dropdown include 'Disabled in Microsoft 365 Copilot and Microsoft 365 Copilot Chat' and 'Disabled in Microsoft 365 Copilot Work mode; Enabled in Microsoft 365 C...'.

Abbildung 115

In der Benutzeroberfläche m365.cloud.microsoft wird der Bereich **Web-Inhalte** dann ausgegraunt – das bedeutet, der User kann **nicht mehr auf Web-Ergebnisse zugreifen** oder diese einbeziehen.



The screenshot shows the Microsoft Copilot interface. At the top, there are tabs for 'Arbeit' and 'Web'. Below that is a 'Copilot' logo. The main area contains several cards with prompts: 'Grundlegendes zu den Hauptpunkten', 'Bleiben Sie auf dem Laufenden.', 'Kalenderinformationen abrufen', 'Nachverfolgen, was wichtig ist', 'Ihre Aufgaben nachverfolgen', and 'Maßgeschneiderte Teams-Hintergründe'. To the right, there's a sidebar with options like 'Über', 'Feedback senden', 'Settings', and a toggle switch for 'Copilot-Antwort umfasst: Webinhalte' which is turned on. Below the sidebar, there's a section for 'Aktuelle Chats' with some sample messages.

Abbildung 116

Dokumentenerstellung durch Copilot

Pfad: config.office.com → Anpassung → **Richtlinienkonfiguration**

Wir bleiben in der gleichen Location und definieren die Richtlinie zur **automatisierten Dokumentenerstellung**. Diese Funktion erlaubt es Copilot, nach einem entsprechenden Prompt ein Dokument zu erstellen.

Das Ergebnis kann je nach Eingabe unterschiedlich ausfallen, stellt jedoch eine nützliche Unterstützung im Arbeitsalltag dar – etwa bei der Strukturierung oder Formulierung von Inhalten.

Empfehlung: Diese Richtlinie **nicht deaktivieren**. Sie bietet einen echten Mehrwert und lässt sich gut in den bestehenden Copilot-Workflow integrieren.

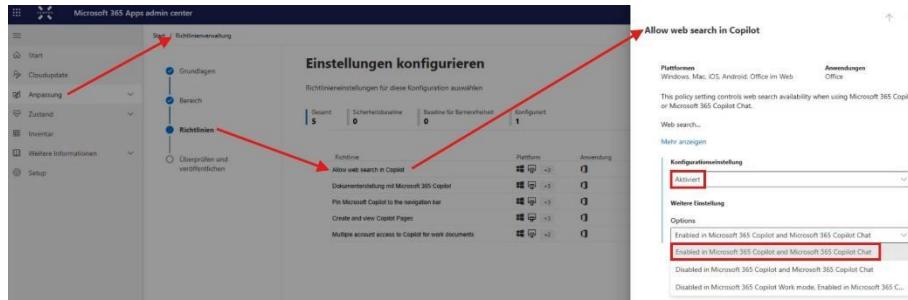


Abbildung 117

Sichtbarkeit des Copilot-Buttons steuern

Pfad: config.office.com → Anpassung → **Richtlinienkonfiguration**

Ein weiterer Konfigurationspunkt betrifft die Frage, **ob Copilot prominent in der Navigationsleiste angezeigt werden soll** – zum Beispiel in Teams, Outlook oder anderen Office-Anwendungen.

Diese Integration lässt sich **schrittweise aktivieren**, um zu testen, wie sie von den Benutzerinnen und Benutzern angenommen wird. So behalten wir die Kontrolle über die Sichtbarkeit und können gezielt entscheiden, ob und wann Copilot aktiv beworben werden soll.

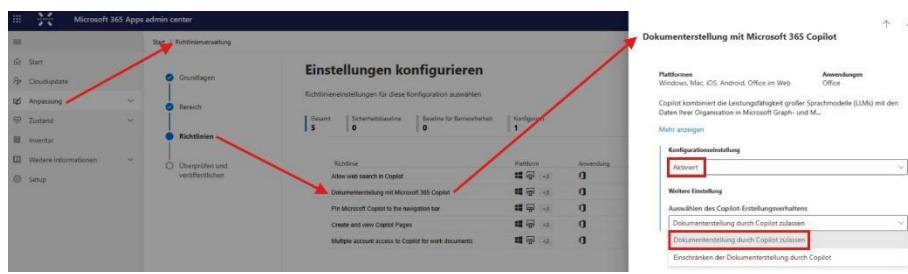


Abbildung 118

Empfehlung: Die Sichtbarkeit des Copilot-Buttons können Sie auch über das Admin Center steuern – dort ist die Einstellung allerdings global: entweder **für alle aktiviert oder deaktiviert**. Ich empfehle, diese Konfiguration über **config.office.com** vorzunehmen. Dort haben Sie die

Möglichkeit, Copilot gezielt **auf Gruppenbasis bereitzustellen**. Das erlaubt Ihnen eine granularere Steuerung, zum Beispiel für Copilotgruppen oder bestimmte Fachbereiche, bevor Sie den Dienst unternehmensweit ausrollen.

Copilot Agents: Auswahl, Sicherheit und Datenschutz

Pfad: admin.microsoft.com → Copilot → Agents

Ein weiterer wichtiger Aspekt in der Konfiguration von Microsoft 365 Copilot betrifft die **Copilot Agents** – also Zusatzfunktionen oder Dienste, die innerhalb der Oberfläche m365.cloud.microsoft/ eingebunden werden können.

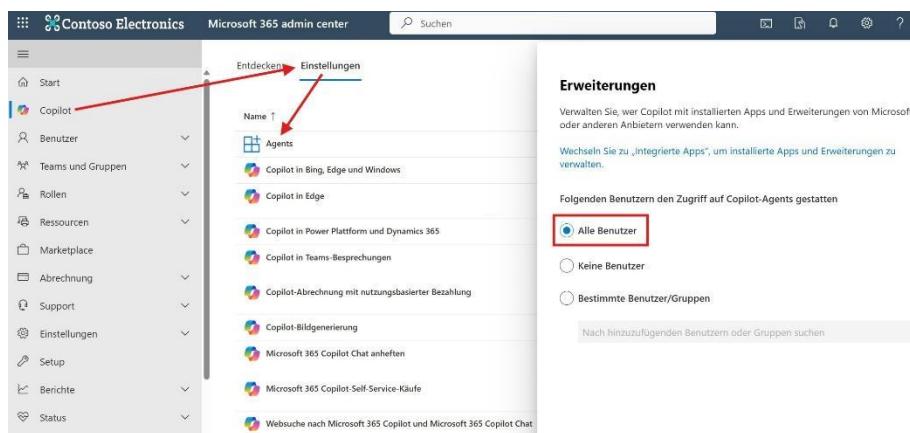
Die zentrale Frage lautet: Sollen Benutzer **selbstständig** Copilot Agents aktivieren oder auswählen dürfen?

Diese Entscheidung sollte nicht allein unter Sicherheitsaspekten getroffen werden, sondern auch im Hinblick auf **Datenschutz** und eine **datensparsame Konfiguration**.

Wie beim Microsoft Teams App Store sollten wir genau prüfen:

- Welche Agents sollen zugelassen werden?
- Welche Metadaten werden verarbeitet?
- Auf welche Informationen im Tenant greifen die Agents zu?

Empfehlung: Treffen Sie die Auswahl kontrolliert, um die Freigabe solcher Agents gezielt zu steuern – so kommen **nur geprüfte und sichere Erweiterungen** im Unternehmen zum Einsatz.



The screenshot shows the Microsoft 365 Admin Center interface. On the left, there's a navigation sidebar with various options like Start, Copilot, Benutzer, Teams and Groups, etc. The 'Copilot' option is highlighted with a red arrow. In the main content area, there's a search bar at the top. Below it, there are two tabs: 'Entdecken' (Discover) and 'Einstellungen' (Settings). The 'Entdecken' tab is active. A red arrow points to the 'Agents' section under the 'Entdecken' tab. The 'Agents' section lists several items: Copilot in Bing, Edge and Windows, Copilot in Edge, Copilot in Power Platform and Dynamics 365, Copilot in Teams-Besprechungen, Copilot-Abrechnung mit nutzungsbasierter Bezahlung, Copilot-Bildgenerierung, Microsoft 365 Copilot Chat anheften, Microsoft 365 Copilot Self-Service-Käufe, and Websuche nach Microsoft 365 Copilot und Microsoft 365 Copilot Chat. To the right of the 'Agents' section, there's a 'Erweiterungen' (Extensions) section. It says 'Verwalten Sie, wer Copilot mit installierten Apps und Erweiterungen von Microsoft oder anderen Anbietern verwenden kann.' and 'Wechseln Sie zu „Integrierte Apps“, um installierte Apps und Erweiterungen zu verwalten.' Below this, there's a section titled 'Folgenden Benutzern den Zugriff auf Copilot-Agents gestatten' (Allow access to Copilot Agents for the following users). It has three radio buttons: 'Alle Benutzer' (All users), 'Keine Benutzer' (No users), and 'Bestimmte Benutzer/Gruppen' (Selected users/groups). The 'Alle Benutzer' radio button is selected and highlighted with a red box. There's also a link 'Nach hinzuzufügenden Benutzern oder Gruppen suchen' (Search for added users or groups).

Abbildung 119

Datensicherheit und Compliance im Microsoft Purview Portal

Pfad: admin.microsoft.com → Copilot: **Datensicherheit und Compliance**

Im Admin Center finden wir unter dem Punkt **Datensicherheit und Compliance** eine Weiterleitung zum **Microsoft Purview Compliance Portal**.

Dieses Portal bildet den **letzten wichtigen Baustein** in der Konfiguration von Microsoft 365 Copilot. Hier können Sie sicherstellen, dass auch Compliance-Vorgaben und Datenschutzrichtlinien im Zusammenhang mit Copilot ordnungsgemäß berücksichtigt werden.

Datensicherheit und Compliance

Schützen und schützen Sie Copilot Interaktionen und Daten über Microsoft 365 hinweg mithilfe von Lösungen im Microsoft Purview Portal.

Datensicherheitstatus-Management für KI

Wenden Sie Richtlinien mit nur einem Klick an, um Ihre Daten zu schützen und Einblicke in die KI-Nutzung innerhalb Ihrer organization zu erhalten.

[Wechseln Sie zu Microsoft Purview DSSM für KI](#)

Insider-Risikomanagement,

Erkennen potenziell riskanter KI-Nutzung in Microsoft Copilot Erfahrungen und Webversionen anderer generativer KI-Apps.

[Wechseln Sie zu Microsoft Purview, um verwalten Sie Insider-Risikomanagement-Richtlinien](#)

Vertraulichkeitsbezeichnungen

Bezeichnung, und schützen Sie die Daten Ihrer organization, die von Copilot verarbeitet und generiert werden, während Sie sicherstellen, dass die Benutzerproduktivität nicht beeinträchtigt wird.

[Wechseln Sie zu Microsoft Purview, um Vertraulichkeitsbezeichnungen](#)

Aufbewahrungsrichtlinien zu verwalten,

Verwalten Sie Ihren Datenlebenszyklus, indem Sie entscheiden, wie lange Copilot Interaktionen beibehalten werden sollen und ob sie nach einer bestimmten Zeit gelöscht werden sollen.

[Wechseln Sie zu Microsoft Purview, um Aufbewahrungsrichtlinien zu verwalten](#)

Kommunikationscompliance

Erfassen Copilot Interaktionen zur Überprüfung potenzieller Verstöße gegen behördliche und geschäftliche Verhaltensweisen.

[Wechseln Sie zu Microsoft Purview, um die Kommunikationscompliance zu verwalten](#)

Überwachen

Suchen Sie nach Überwachungsdatensätzen Copilot Interaktionen, die von Benutzern und Administratoren ausgeführt wurden.

[Wechseln Sie zu Microsoft Purview, um Überwachungsdatensätze](#)

eDiscovery-

Durchsuchen Copilot Interaktionsinhalten innerhalb Ihrer organization, Inhalte erhalten und Suchergebnisse zur weiteren Analyse exportieren

[Wechseln Sie zu Microsoft Purview, um eDiscovery- zu verwalten.](#)

Abbildung 120

Automatische Bildgenerierung aktiviert lassen

Pfad: admin.microsoft.com → Copilot: **Copilot-Bildgenerierung**

Ich empfehle, die Standardeinstellung zur Copilot-Bildgenerierung aktiviert zu lassen, da es sich hierbei um eine nützliche Funktion handelt.

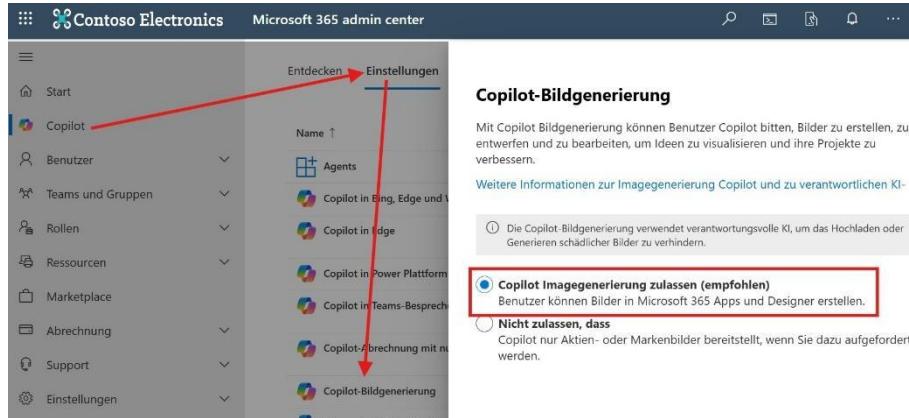


Abbildung 121

Copilot in Microsoft Teams-Besprechungen

Pfad: admin.microsoft.com → Copilot: **Copilot in Teams Besprechungen**

Klicken wir auf Copilot in Teams Besprechungen:

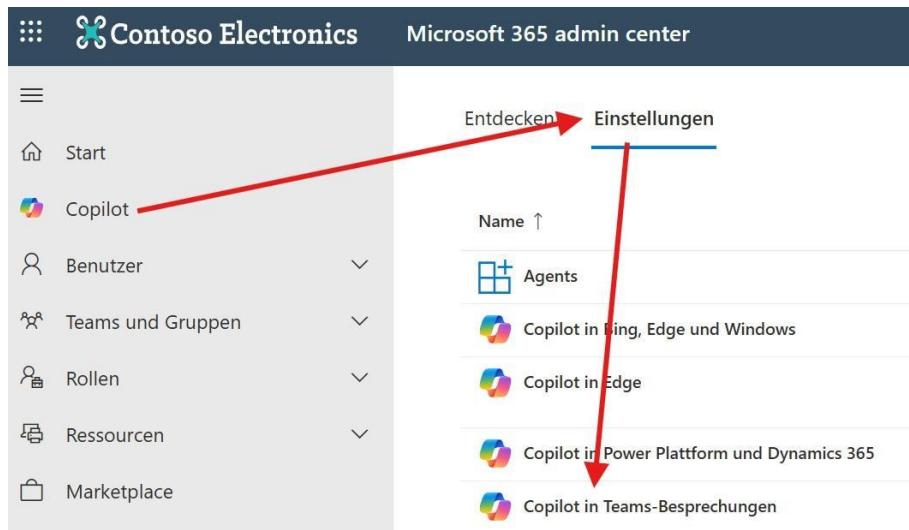
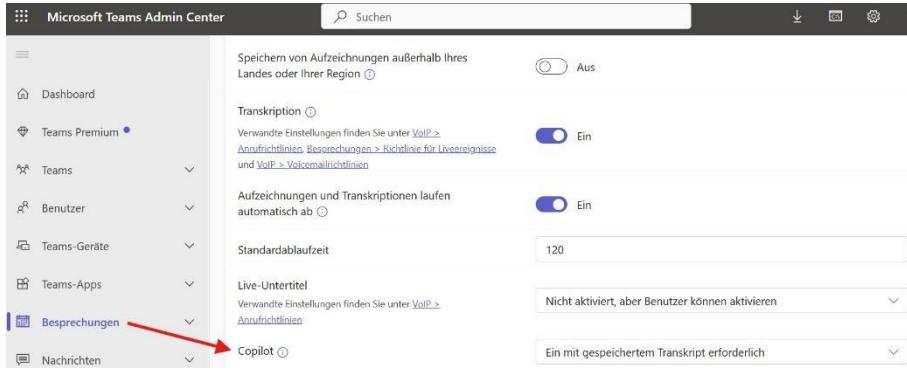


Abbildung 122

werden wir idealerweise ins admin.teams.microsoft.com zur Option **Copilot** weitergeleitet.



The screenshot shows the Microsoft Teams Admin Center interface. On the left, there's a navigation sidebar with options like Dashboard, Teams Premium, Teams, Benutzer, Teams-Geräte, Teams-Apps, Besprechungen (which is highlighted with a red arrow), and Nachrichten. The main content area has several configuration sections:

- Speichern von Aufzeichnungen außerhalb Ihres Landes oder Ihrer Region: A switch set to "Aus" (Off).
- Transkription: A switch set to "Ein" (On). A note below says: "Verwandte Einstellungen finden Sie unter VoIP > Anrufrichtlinien, Bezeichnungen > Richtlinie für Liveaufnahmen und VoIP > Voicemailrichtlinien".
- Aufzeichnungen und Transkriptionen laufen automatisch ab: A switch set to "Ein" (On). A note below says: "Standardablaufzeit" with a value of "120".
- Live-Untertitel: A note says: "Verwandte Einstellungen finden Sie unter VoIP > Anrufrichtlinien". A dropdown menu shows "Nicht aktiviert, aber Benutzer können aktivieren".
- Copilot: A note says: "Ein mit gespeichertem Transkript erforderlich".

Abbildung 123

Hier legen wir fest, ob standardmäßig Transkripte erstellt und Besprechungen zusammengefasst werden dürfen.

Der **automatische Start von Transkripten** sorgt bei einigen Unternehmen – insbesondere im Bereich Compliance – allerdings für Bedenken.

Empfehlung: Der Besprechungsorganisator sollte **aktiv zustimmen müssen**, bevor ein Transkript erstellt wird. So behalten wir die Kontrolle darüber, wann und wie gesprochene Inhalte aufgezeichnet werden.

Wird das Transkript automatisch gestartet, kann dies dazu führen, dass Namen und Aussagen protokolliert werden, **ohne dass alle Teilnehmenden vorab ausdrücklich zugestimmt haben** – ein potenzielles Risiko im Hinblick auf Datenschutz und Dokumentationspflichten.

Aufzeichnungsrichtlinien separat verwalten

Unabhängig von Copilot, gibt es in Microsoft Teams auch **eigene Richtlinien für Aufzeichnungen**. Diese bestimmen beispielsweise

- ob Aufzeichnungen grundsätzlich erlaubt sind.
- ob Benutzer aktiv zustimmen müssen, bevor eine Besprechung aufgezeichnet werden darf.

Die technische Umsetzung erfolgt ebenfalls im Teams Admin Center.

Ergänzend gilt: Wenn Copilot über **Microsoft Edge** verwendet wird, greifen auch dort Richtlinien, die berücksichtigt werden sollten.

Copilot in Microsoft Edge und Office

Pfad: admin.microsoft.com → Copilot: **Copilot in Edge**

Mittlerweile ist die **Nutzung von Copilot auch im Microsoft Edge Browser möglich**. Über entsprechende Edge-Policy-Konfigurationen können wir festlegen, wie und ob Websuchfunktionen in Verbindung mit Copilot zugelassen werden.

Sobald Copilot im Edge-Browser verwendet wird, greift er ebenfalls auf **Web-Ergebnisse** zurück – ähnlich wie innerhalb der Office-Anwendungen.

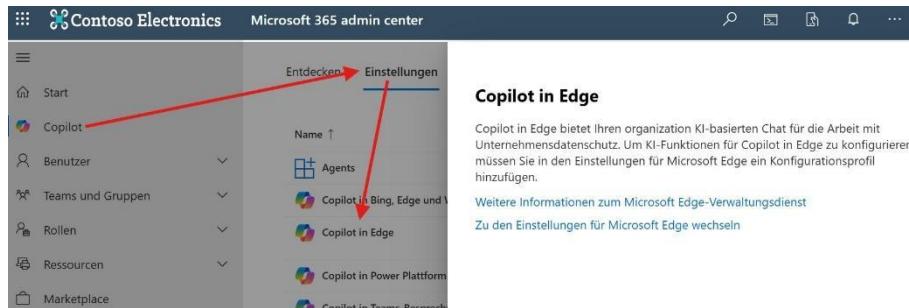


Abbildung 124

Connected Experiences als technische Voraussetzung

Pfad: admin.microsoft.com → Copilot: **Copilot in Bing, Edge und Windows**

Für die Nutzung von Copilot in der Office-Suite müssen die sogenannten Connected Experiences aktiviert sein.

Nur wenn diese Funktion aktiv ist, kann Copilot **innerhalb von Word, Excel, Outlook und anderen Office-Apps** korrekt arbeiten.

Ohne diese aktivierte Verbindung stehen die erweiterten KI-Funktionen von Copilot nicht zur Verfügung.

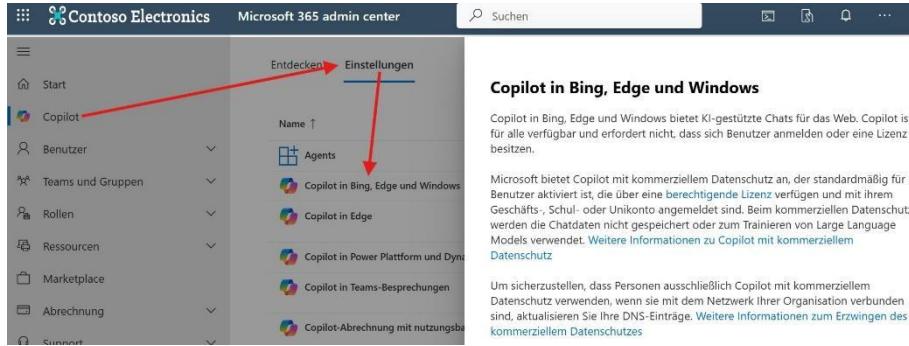


Abbildung 125

Konfigurationen im Compliance-Portal

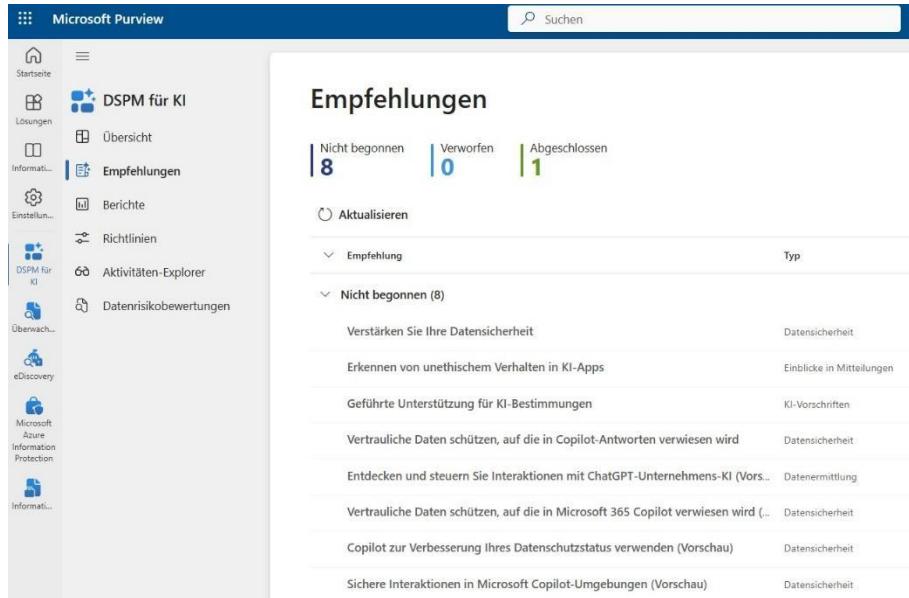
Microsoft Purview stellt zentrale Werkzeuge bereit, um Copilot datenschutzkonform einzusetzen. Dazu zählen Information Barriers, Sensitivity Labels, eDiscovery und Prüfmechanismen zur Einhaltung gesetzlicher Vorgaben.

Durch Klicken auf Pfad: admin.microsoft.com → **Compliance** landen wir im **Compliance-Portal** auf **purview.microsoft.com**

Datensicherheit mit Microsoft Purview und DSPM for AI

Pfad: purview.microsoft.com → Lösungen → DSPM für KI → **Empfehlungen**

Hier finden wir konkrete Vorschläge zur Absicherung unserer Umgebung, insbesondere im Kontext der KI-Nutzung.



Empfehlungen		
Nicht begonnen	Verworfen	Abgeschlossen
8	0	1
Aktualisieren		
Empfehlung		
Nicht begonnen (8)		
Verstärken Sie Ihre Datensicherheit Erkennen von unethischem Verhalten in KI-Apps Geführte Unterstützung für KI-Bestimmungen Vertrauliche Daten schützen, auf die in Copilot-Antworten verwiesen wird Entdecken und steuern Sie Interaktionen mit ChatGPT-Unternehmens-KI (Vorschau) Vertrauliche Daten schützen, auf die in Microsoft 365 Copilot verwiesen wird (Vorschau) Copilot zur Verbesserung Ihres Datenschutzstatus verwenden (Vorschau) Sichere Interaktionen in Microsoft Copilot-Umgebungen (Vorschau)		
<small>Type</small>		
<small>Datensicherheit</small>		
<small>Einblicke in Mitteilungen</small>		
<small>KI-Vorschriften</small>		
<small>Datenermittlung</small>		
<small>Datensicherheit</small>		
<small>Datensicherheit</small>		
<small>Datensicherheit</small>		

Abbildung 125a

Als Basis dienen hier **Information Protection Policies**. Diese Richtlinien helfen uns, Datenklassifizierungen zu definieren und die Kontrolle über sensible Informationen zu behalten.

Information Barriers in Microsoft Purview

Pfad: purview.microsoft.com → Lösungen → **Informationsschranken**

Hier haben wir die Option, eine **Segmentierung der Kommunikation** innerhalb unserer Organisation vorzunehmen. Das bedeutet, dass bestimmte Gruppen – etwa Mitarbeitende der Personalabteilung – **nicht mit anderen Bereichen**, wie z. B. der IT, kommunizieren dürfen.

Diese Einschränkung bezieht sich auf:

- Microsoft Teams
- E-Mail-Kommunikation
- sowie mögliche **Copilot-Prompts**, die abteilungsübergreifende Daten betreffen

Microsoft sieht den Haupteinsatzbereich dieser Funktion im **Finanzsektor**, etwa für Broker oder Handelsabteilungen mit regulatorischen Trennpflichten.

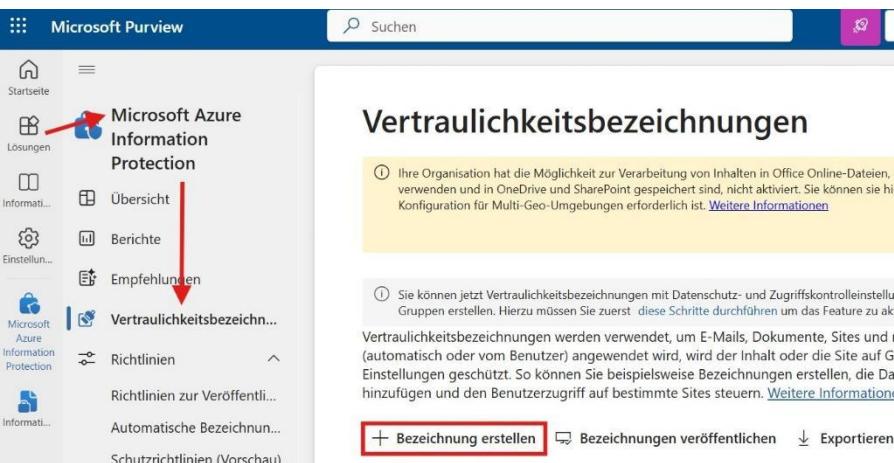
In der Praxis zeigt sich jedoch: Für die **meisten Unternehmen ist diese Funktion nicht erforderlich.**

Alternative: Granulare Steuerung mit Sensitivity Labels

Statt die Kommunikation vollständig zu segmentieren, setzen viele Unternehmen auf **granulare Datenklassifikation über Sensitivity Labels**.

Diese Labels ermöglichen eine flexible, datenschutzkonforme Steuerung von Zugriffen – ohne Kommunikationsgrenzen zwischen Abteilungen zu erzwingen.

Pfad: purview.microsoft.com → Lösungen → Microsoft Azure Information Protection → Vertraulichkeitsbezeichnungen → **Bezeichnung erstellen**



The screenshot shows the Microsoft Purview interface. On the left, there's a sidebar with various navigation options like 'Startseite', 'Lösungen', 'Informati...', 'Einstellun...', 'Microsoft Azure Information Protection', and 'Schutzrichtlinien (Vorschau)'. The 'Microsoft Azure Information Protection' section is highlighted with a red box and an arrow. Below it, under 'Vertraulichkeitsbezeichnungen', there's a sub-menu with 'Übersicht', 'Berichte', 'Empfehlungen', and 'Richtlinien'. A red arrow points to the 'Richtlinien' link. The main content area is titled 'Vertraulichkeitsbezeichnungen'. It contains two informational boxes: one about handling Office Online files and another about creating labels. At the bottom, there are buttons for '+ Bezeichnung erstellen' (which is highlighted with a red box), 'Bezeichnungen veröffentlichen', and 'Exportieren'.

Abbildung 126

Im Folgenden erstellen wir ein neues Label und definieren grundlegende Einstellungen.

Schritt 1 – Bezeichnungsdetails: Hier legen wir zunächst einen **administrativen Namen** sowie einen **Anzeigenamen** fest. Zusätzlich können wir eine **Beschreibung für Benutzer** hinzufügen – diese wird beim Klassifizieren von Dokumenten in Word, Excel oder PowerPoint angezeigt.

Der Beschreibungstext sollte kurz und prägnant sein, idealerweise **ein bis zwei Zeilen** – auch bei mehreren Hundert oder Tausend Nutzern. Beispiel:
 „Dieses Label erlaubt Lesezugriff für ausgewählte Benutzer.“

Parallel lässt sich eine **Admin-Beschreibung** sowie eine **Farbe** für das Label definieren, z. B. Rot für „Streng vertraulich“.

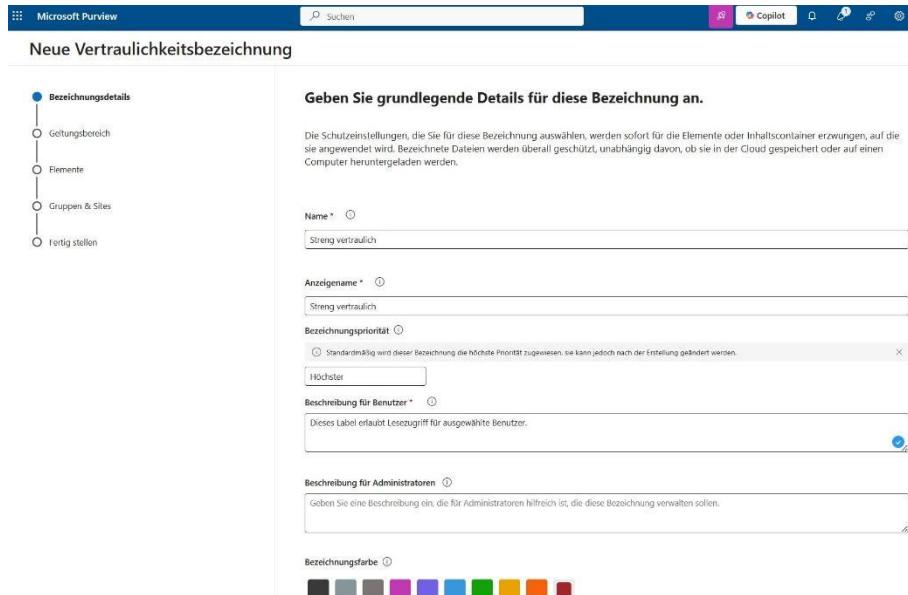


Abbildung 127

Schritt 2 – Geltungsbereich: Nun wählen wir den Bereich, auf den das Label angewendet werden soll. Standardmäßig gilt dieser zunächst für **Dateien und E-Mails** – der wichtigste Bereich für den Einsatz mit **Microsoft Copilot**.

Erweiterte Szenarien ermöglichen den Einsatz von Vertraulichkeits-bezeichnungen auch in **Microsoft Teams**, **Microsoft 365 Gruppen** oder **SharePoint**. In der Praxis empfiehlt es sich jedoch, zunächst mit **Dateien zu starten**, da dies bereits einen erheblichen Aufwand mit sich bringt.

Wichtig: Hat ein Dokument eine Vertraulichkeitsbezeichnung, die dem Benutzer **keinen mindestens lesenden Zugriff** gewährt, wird es **nicht im Copilot angezeigt** – selbst wenn der Benutzer Zugriff auf die SharePoint-Seite hat.

Damit gelten Labels als zugriffssteuernde Komponente auf Dateiebene – entscheidend für den Erfolg der Copilot-Nutzung.

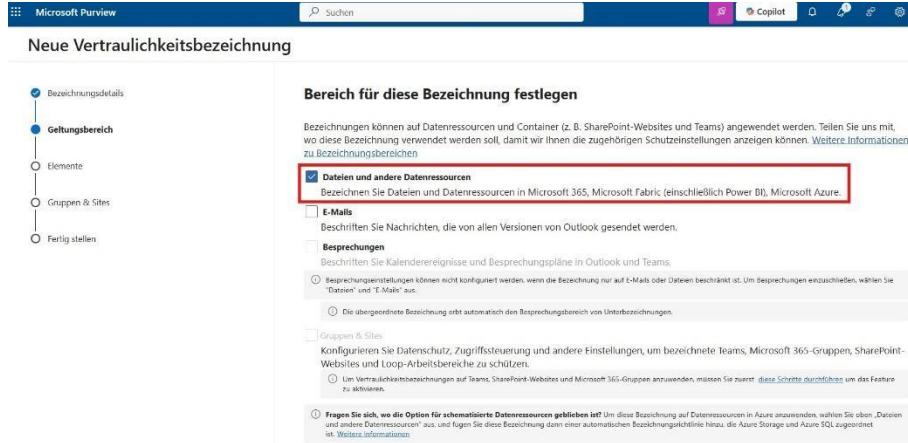


Abbildung 128

Schritt 3 – Elemente: Zusätzlich können wir über das Label folgende Optionen konfigurieren:

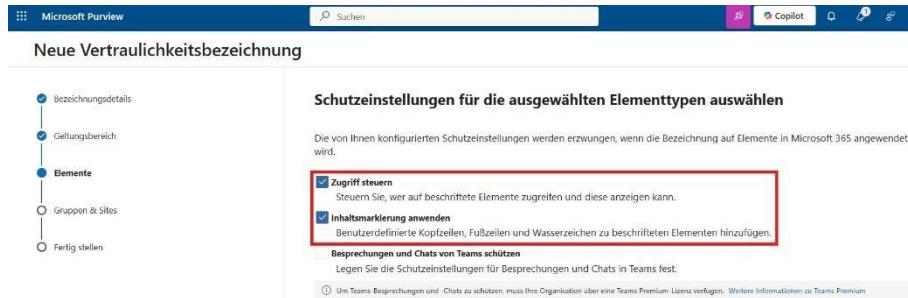


Abbildung 129

Beide Funktionen lassen sich **in Kombination nutzen**, um sowohl visuell als auch technisch eine eindeutige Klassifikation durchzusetzen.

Einige Unternehmen setzen ausschließlich auf **optische Markierungen** – etwa sichtbare Hinweise wie „Vertraulich“ – verzichten dabei jedoch auf tatsächliche Zugriffseinschränkungen. Aus Sicht der Sicherheit und Compliance ist das **nicht empfehlenswert**. Labels entfalten ihre Schutzwirkung erst dann vollständig, wenn sie **auch technische Zugriffsmechanismen enthalten**.

Schritt 4 – Elemente → Zugriffssteuerung: Es ist wichtig, bereits zu Beginn einen **klaren Zugriffsmechanismus** zu definieren – auch wenn dieser zunächst nur grundlegend ist.

Ein besonders wichtiger Konfigurationspunkt ist die **Zugriffsverweigerung**: Diese Option sollte immer aktiviert werden – auch wenn keine konkreten Einschränkungen gesetzt sind.

Hintergrund: Wird ein Label ohne Restriktionen erstellt und später durch ein anderes ersetzt, das ebenfalls keine Restriktionen enthält, wird eine frühere Verschlüsselung nicht automatisch entfernt, es sei denn, die Zugriffsverweigerung ist aktiviert. Das kann zu **unerwarteten Zugriffsbeschränkungen** führen und sollte vermieden werden.

Im Bereich **Berechtigungen jetzt zuweisen oder Benutzer entscheiden lassen?** stehen zwei Optionen zur Verfügung:

- **Berechtigungen jetzt zuweisen:** Berechtigungen werden durch die IT zentral definiert
- **Benutzer entscheiden lassen:** Benutzer dürfen selbst festlegen, wer auf Inhalte zugreifen darf (z. B. Lese- oder Schreibzugriff)

Empfehlung: Starten Sie mit **Berechtigungen jetzt zuweisen** – insbesondere, wenn die Kontrolle über Zugriffsrechte unternehmensweit konsistent bleiben soll. Nach Auswahl dieser Option werden weitere Einstellungen sichtbar, darunter z. B. die Gültigkeitsdauer von Zugriffsrechten.

Im Rahmen der Zugriffskontrolle können wir auch festlegen, ob und wann eine Berechtigung abläuft. Unter dem Punkt **Benutzerzugriff auf Inhalt läuft ab?** stehen uns drei Optionen zur Verfügung:

- Ein bestimmtes Datum
- Anzahl bestimmter Tage
- Nie

Diese Optionen sind hilfreich, wenn Dokumente – etwa Verträge – **zeitlich befristet bereitgestellt werden** sollen.

Standardmäßig ist jedoch **Nie** ausgewählt. In diesem Fall bleibt die erteilte Berechtigung bestehen, bis sie manuell geändert oder widerrufen wird.

Zusätzlich können wir entscheiden, ob Benutzer auf klassifizierte Inhalte auch **offline** zugreifen dürfen. Die Einstellung **Offlinezugriff zulassen** ist vor allem dann relevant, wenn Dokumente nicht in Teams, SharePoint oder OneDrive abgelegt sind, sondern lokal geöffnet werden sollen.

Neue Vertraulichkeitsbezeichnung

- Bezeichnungsdetails
- Geltungsbereich
- Elemente**
- Zugriffsteuerung
- Inhaltsmarkierung
- Automatisches Bezeichnen von Dateien und E-Mails
- Gruppen & Sites
- Fertig stellen

angegebenen Bereich können die Elemente E-Mails, Office-, Fabric- und Power BI-Dateien sowie Besprechungseinladungen umfassen.
[Weitere Informationen zu Zugriffssteuerung](#)

Zugriffssteuerungsinstellungen entfernen, wenn sie bereits auf Elemente angewendet wurden
 Zugriffssteuerungsinstellungen konfigurieren

Aktivieren Sie die gemeinsame Dokumenteneinstellung für Office-Desktop-Apps, damit mehrere Benutzer gleichzeitig beschreibte Dokumente bearbeiten können, auf die Zugriffssteuerungsinstellungen angewendet wurden. [Weitere Informationen zu dieser Einstellung](#)

[Zur Einstellung zur gemeinsame Dokumenteneinstellung wechseln](#)

Berechtigungen jetzt zuweisen oder Benutzer entscheiden lassen?
 Berechtigungen jetzt zuweisen

Die von Ihnen ausgewählten Einstellungen werden automatisch erzwungen, wenn die Bezeichnung auf E-Mails und Office-Dateien angewendet wird.

Benutzerzugriff auf Inhalt läuft ab:

Nie

Offlinezugriff zulassen

Immer

Bestimmten Benutzern und Gruppen Berechtigungen erteilen *

Berechtigungen zuweisen

Abbildung 130

Nun können wir die Berechtigungen via **Berechtigungen zuweisen** festlegen, in dem wir

- konkret einzelne Benutzer oder Gruppen berechtigen oder
 - die Option **Hinzufügen aller Benutzer und Gruppe in Ihrer Organisation bzw. Alle authentifizierten Benutzer hinzufügen** verwenden.

Hinzufügen aller Benutzer und Gruppe in Ihrer Organisation betrifft ausschließlich Benutzer innerhalb unseres eigenen Tenants. **Alle authentifizierten Benutzer hinzufügen** hingegen schließt alle Benutzer mit einem vertrauenswürdigen (federierten) Login ein – etwa aus anderen Microsoft-Tenants, Google-Accounts oder Apple-ID-Umgebungen.

Das bedeutet: Jeder, der sich erfolgreich authentifizieren kann, unabhängig von unserer Organisation, erhält Zugriff – sofern wir diese Option aktivieren. Diese Einstellung sollte daher mit besonderer Vorsicht genutzt werden.

Die Option **Alle authentifizierten Benutzer hinzufügen** umfasst nicht nur Benutzer aus federierten Umgebungen, sondern auch externe Empfänger, die sich über einen Einmalcode authentifizieren – beispielsweise mit einer Gmail-Adresse.

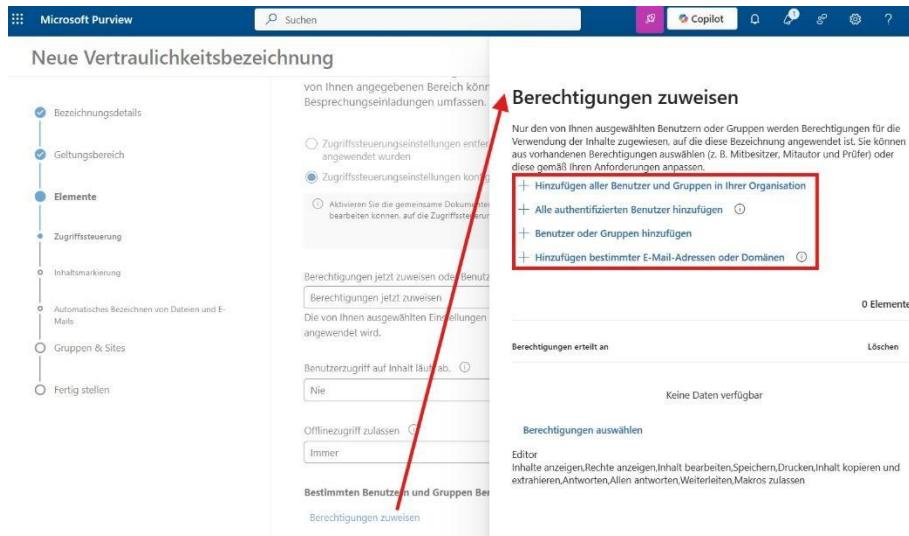
Das bedeutet: Auch nicht verwaltete Konten können Zugriff auf Inhalte erhalten, sofern sie erfolgreich ihre Identität bestätigen.

Diese Funktion ist nützlich, wenn gezielte Freigaben an externe Partner erfolgen sollen – sollte aber mit Vorsicht eingesetzt werden, wenn der Inhalt nicht für Außenstehende bestimmt ist.

Alternativ können wir auch:

- konkrete Benutzer oder Gruppen oder
- spezifische E-Mail-Adressen oder Domänen

zur Berechtigung hinzufügen.



Neue Vertraulichkeitsbezeichnung

von Ihnen angegebener Bereich kann Besprechungsseitladungen umfassen.

Zugriffsteuerungseinstellungen entfernt angewendet werden

Zugriffsteuerungseinstellungen konfiguriert werden

Aktivieren Sie die gemeinsame Dokumentbearbeitung, auf die Zugriffsteuerung angewendet wird.

Berechtigungen jetzt zuweisen oder Benutzern ausgewählte Berechtigungen zuweisen

Berechtigungen jetzt zuweisen Die von Ihnen ausgewählten Einstellungen angewendet werden.

Benutzerzugriff auf Inhalt läuft ab: Nie

Offlinezugriff zulassen Immer

Bestimmten Benutzern und Gruppen Berechtigungen zuweisen

Berechtigungen zuweisen

Nur den von Ihnen ausgewählten Benutzern oder Gruppen werden Berechtigungen für die Verwendung der Inhalte zugewiesen, auf die diese Bezeichnung angewendet ist. Sie können aus vorhandenen Berechtigungen auswählen (z. B. Mitbesitzer, Mitautor und Prüfer) oder diese gemäß Ihren Anforderungen anpassen.

+ Hinzufügen aller Benutzer und Gruppen in ihrer Organisation

+ Alle authentifizierten Benutzer hinzufügen

+ Benutzer oder Gruppen hinzufügen

+ Hinzufügen bestimmter E-Mail-Adressen oder Domänen

0 Elemente

Berechtigungen erteilt an Löschen

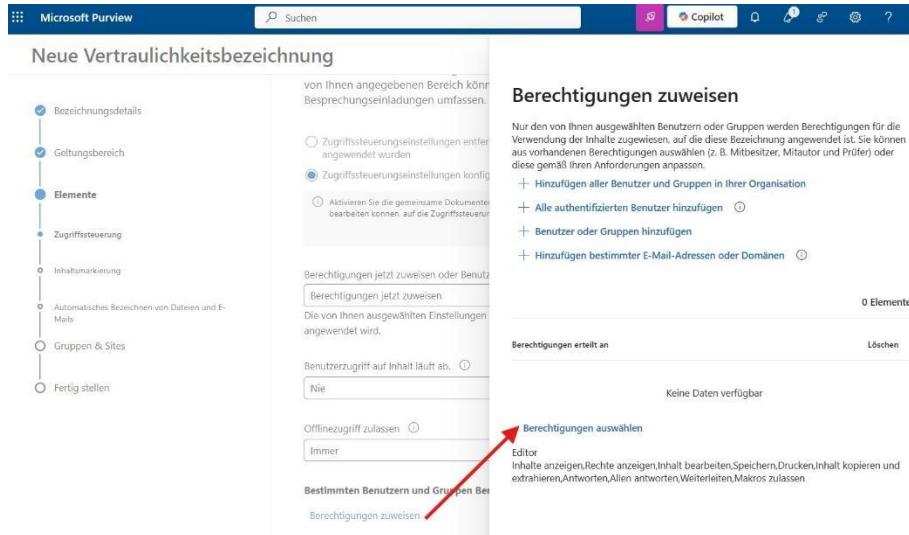
Keine Daten verfügbar

Berechtigungen auswählen

Editor
Inhalte anzeigen, Rechte anzeigen, Inhalt bearbeiten, Speichern, Drucken, Inhalt kopieren und extrahieren, Antworten, Allen antworten, Weiterleiten, Makros zulassen

Abbildung 131

Wenn wir z. B. ein Label wie **Streng vertraulich** nur intern nutzen möchten, wählen wir ausschließlich interne Gruppen und vergeben dann gezielt Rechte wie **Lesen**, **Drucken** oder **Bearbeiten**.

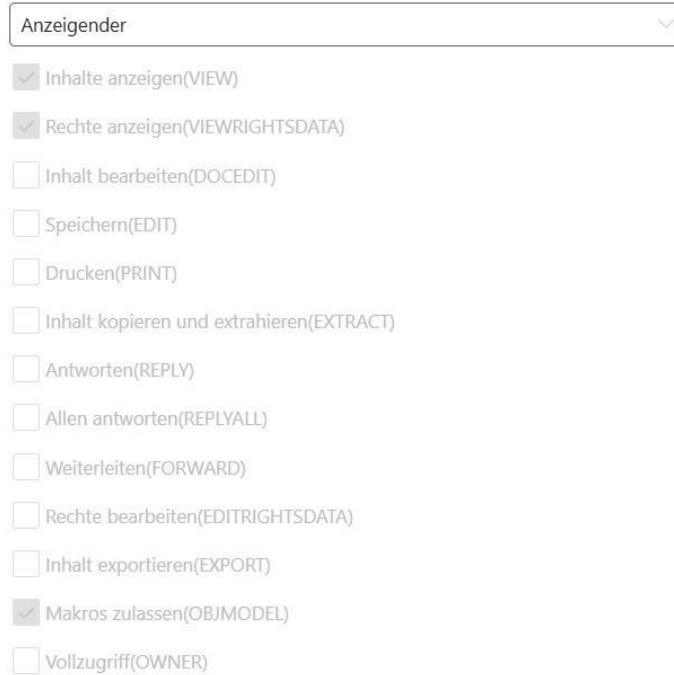


The screenshot shows the Microsoft Purview interface for creating a new confidentiality label. The left sidebar has a tree structure with 'Bezeichnungsdetails', 'Geltungsbereich', and 'Elemente' expanded. Under 'Elemente', there are 'Zugriffssteuerung', 'Inhaltsmarkierung', 'Automatisches Bezeichnen von Dateien und E-Mails', 'Gruppen & Sites', and 'Fertig stellen'. The right panel shows configuration options for the label, including 'von Ihnen angegebener Bereich kann Besprechungsseminar umfassen.' and 'Zugriffssteuerungseinstellungen konfigurieren'. Below this is a section for assigning permissions, with a red arrow pointing to the 'Berechtigungen auswählen' button. The permission list includes 'Inhalt anzeigen(VIEW)', 'Rechte anzeigen(VIEWRIGHTSDATA)', 'Inhalt bearbeiten(DOCEDIT)', etc.

Abbildung 132

Berechtigungen auswählen

Auswählen, welche Aktionen für diese/n Benutzer/Gruppe zulässig wären. [Weitere Informationen zu Berechtigungen](#)



The screenshot shows a list of permissions for a user or group. The 'Anzeigender' dropdown is set to 'Anzeigender'. The list includes:

- Inhalte anzeigen(VIEW)
- Rechte anzeigen(VIEWRIGHTSDATA)
- Inhalt bearbeiten(DOCEDIT)
- Speichern(EDIT)
- Drucken(PRINT)
- Inhalt kopieren und extrahieren(EXTRACT)
- Antworten(REPLY)
- Allen antworten(REPLYALL)
- Weiterleiten(FORWARD)
- Rechte bearbeiten(EDITRIGHTSDATA)
- Inhalt exportieren(EXPORT)
- Makros zulassen(OBJMODEL)
- Vollzugriff(OWNER)

Abbildung 133

Diese Berechtigungen sollten mit der Beschreibung und dem Namen des Labels konsistent sein, um Verwirrung bei den Nutzern zu vermeiden.

Es ist wichtig zu verstehen, dass die Gruppe, die Labels anwenden darf, **nicht zwingend dieselbe** ist wie die Gruppe, die Zugriffsrechte auf die Inhalte erhält.

So kann z. B. eine kleinere, kontrollierte Gruppe für die Anwendung des Labels zuständig sein, während eine größere Zielgruppe später Lese- oder Schreibzugriff erhält.

Diese Trennung zwischen *Label Publisher* und *Berechtigungsnehmer* bietet mehr Flexibilität in der Umsetzung von Datenklassifikationsstrategien.

Bei der Erstellung eines Labels können wir zusätzliche Schutzfunktionen aktivieren:

- **Dynamische Wasserzeichen verwenden:** Dokumente werden automatisch mit dem Namen des Anwenders versehen. Diese Funktion ist optional – viele Unternehmen verzichten darauf.
- **Nutzen Sie Doppelschlüsselverschlüsslung:** Neben dem Microsoft-Schlüssel wird ein eigener Schlüssel des Unternehmens verwendet. Diese Option erhöht die Datensicherheit, schränkt jedoch die Nutzung innerhalb von Microsoft 365 Copilot ein – Inhalte mit DSV können dort nicht verarbeitet werden.

Microsoft Purview Suchen

Neue Vertraulichkeitsbezeichnung

- Bezeichnungsdetails
- Geltungsbereich
- Elemente**
- Zugriffssteuerung
- Inhaltsmarkierung
- Automatisches Bezeichnen von Dateien und E-Mails
- Gruppen & Sites
- Fertig stellen

Zugriffssteuerungseinstellungen entfernen, wenn sie angewendet wurden
 Zugriffssteuerungseinstellungen konfigurieren

(i) Aktivieren Sie die gemeinsame Dokumenterstellung für Office bearbeiten können, auf die Zugriffssteuerungseinstellungen

Berechtigungen jetzt zuweisen oder Benutzer entscheider

Die von Ihnen ausgewählten Einstellungen werden automatisch angewendet wird.

Benutzerzugriff auf Inhalt läuft ab. (i)

Offlinezugriff zulassen (i)

Bestimmten Benutzern und Gruppen Berechtigungen

Berechtigungen zuweisen

Benutzer und Gruppen

admin@M365x01107084.onmicrosoft.com

Dynamische Wasserzeichen verwenden (i)

Nutzen Sie Doppelschlüsselverschlüsselung (i)

URL Ihres Diensts für Doppelschlüsselverschlüsselung

Abbildung 134

Schritt 5 – Elemente → Inhaltsmarkierung: Hier legen wir fest, ob ein Dokument durch einen Kopf, Fuß oder ein Wasserzeichen **optisch als klassifiziert gekennzeichnet** werden soll.

Die Gestaltung kann flexibel angepasst werden:

- Freitext (z. B. „Streng vertraulich“)
- Schriftgröße und -farbe
- Positionierung (z. B. mittig, oben oder unten)

Einige Unternehmen setzen Wasserzeichen nur dann ein, wenn Inhalte **außerhalb** des Unternehmens freigegeben werden – als zusätzlicher Hinweis auf die Vertraulichkeit.

Bleiben die Daten intern und sind über Zugriffsbeschränkungen geschützt, wird oft auf eine sichtbare Kennzeichnung verzichtet, da das Label selbst bereits für Klarheit sorgt.

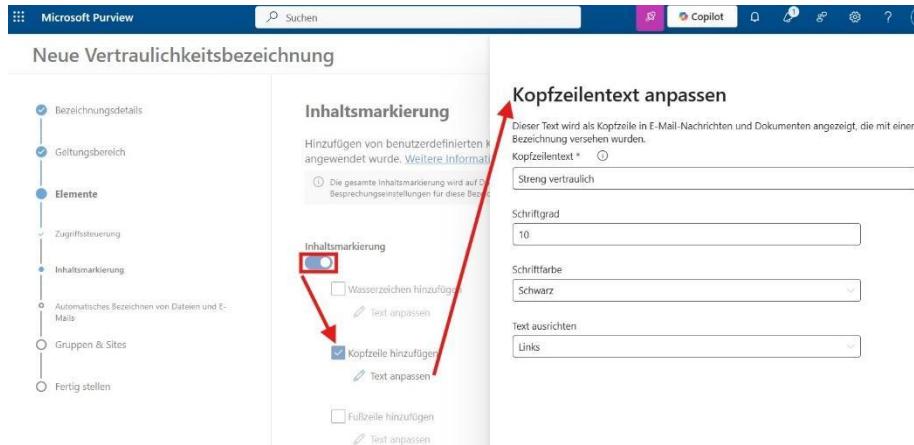


Abbildung 135

Schritt 6 – Elemente → Automatisches Bezeichnen von Dateien und E-Mails: Ein weiteres leistungsstarkes Feature ist das Autolabeling, das große Vorteile in der Skalierung und Automatisierung der **Datenklassifizierung** bietet – besonders in großen Umgebungen mit hohem Dokumentenvolumen.

Hierbei werden Dokumente **automatisch mit einer Vertraulichkeits-bezeichnung** versehen, sobald bestimmte Inhalte erkannt werden – zum Beispiel:

- Typen vertraulicher Informationen; zum Beispiel Kreditkartennummern, Personalausweise oder IBANs
- Trainierbare Klassifizierer, die auf maschinellem Lernen basieren

Grundlage sind entweder:

- **vordefinierte Typen vertraulicher Informationen** (z. B. IBAN, Personalausweis, Gesundheitsdaten) oder
- **eigene Wörterbuchdefinitionen**, die über die Microsoft Graph API eingebunden werden.

Dabei wird geprüft, ob Inhalte bestimmte Kriterien erfüllen – und wenn ja, wird das entsprechende Label automatisch angewendet.

Wichtig: Diese Funktion steht nur mit einer E5-Lizenz oder einer entsprechenden Microsoft Purview Add-on-Lizenz zur Verfügung.

Viele Unternehmen entscheiden sich zunächst für die manuelle Klassifizierung, um **Fehlklassifikationen (False Positives) zu vermeiden**. Der Benutzer entscheidet entsprechend, das Label einzusetzen.

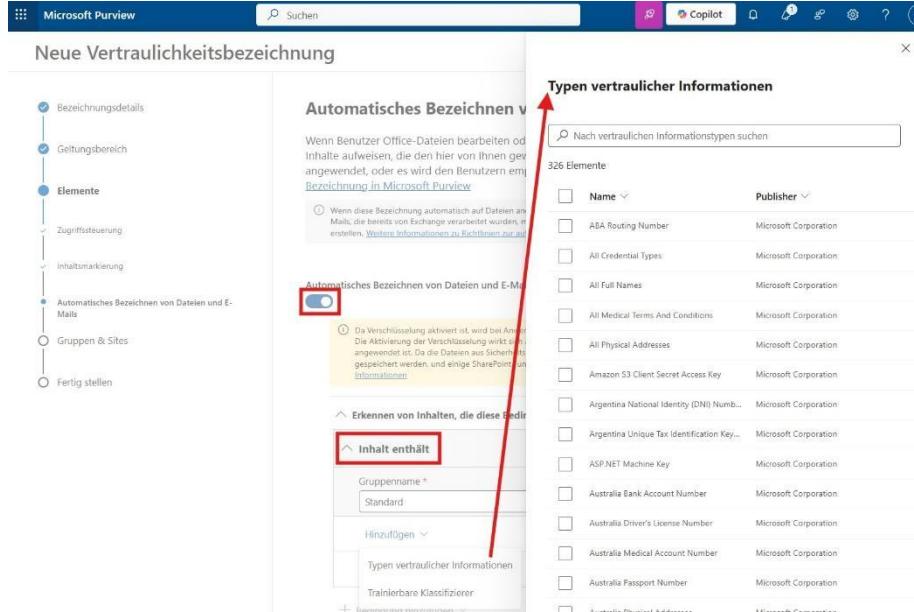
Microsoft stellt derzeit rund **326 Sensitive Information Types** bereit. Diese decken u. a. Anforderungen aus der DSGVO (GDPR) und anderen Datenschutzverordnungen ab.

Trainierbare Klassifizierer bieten darüber hinaus die Möglichkeit, unternehmensspezifische Inhalte zu erkennen. Allerdings ist:

- für das Training dieser Klassifizierer ein Set von mindestens 50.000 Wörtern nötig (z. B. über SharePoint-Dokumente) und
- ihre Nutzung lizenziert – das Anlegen ist kostenlos, der Einsatz erfordert jedoch eine zusätzliche Microsoft-Lizenz.

Empfehlung: Überprüfen Sie die Einstellungen zum Autolabelling genau bzw. gestuft. Beginnen Sie mit einer manuellen Klassifizierung, und validieren Sie im Anschluss die Trefferqualität automatischer Regeln, bevor Sie diese großflächig aktivieren.

Auch wenn Microsoft die Möglichkeit bietet, Labels automatisch anwenden zu lassen, empfiehlt es sich in der Praxis häufig, zunächst mit **manuellen Klassifizierungen** zu starten. So behalten die Benutzerinnen und Benutzer die **Kontrolle** über die Zuweisung – was insbesondere bei sensiblen Daten oder komplexen Inhalten Missverständnisse vermeidet.



The screenshot shows the Microsoft Purview interface for creating a new confidentiality label. On the left, there's a navigation tree with options like 'Bezeichnungsdetails', 'Geltungsbereich', 'Elemente' (which is selected), 'Zugriffsteuerung', 'Inhaltsmarkierung', 'Automatisches Bezeichnen von Dateien und E-Mails' (also selected), 'Gruppen & Sites', and 'Fertig stellen'. The main content area has sections for 'Automatisches Bezeichnen von Dateien und E-Mails' (with a note about automatic labeling on shared files) and 'Erkennen von Inhalten, die diese Bedeutung haben' (with a sub-section 'Inhalt enthält'). A sidebar titled 'Typen vertraulicher informationen' lists 326 elements, such as 'ABA Routing Number', 'All Credential Types', 'All Full Names', etc. A red arrow highlights the connection between the sidebar and the 'Automatisches Bezeichnen' section.

Abbildung 136

Statt Labels automatisch anzuwenden, lässt sich die Option **Bezeichnung empfehlen** aktivieren. In diesem Fall erscheint z. B. in Word ein Hinweis wie: „*Basierend auf dem Inhalt empfehlen wir das Label 'Vertraulich'.*“

Die Entscheidung bleibt beim Benutzer, wodurch die Wahrscheinlichkeit von **Fehlklassifizierungen reduziert** wird. In Projekten zeigt sich jedoch, dass auch solche Empfehlungen zu Rückfragen und Tickets führen können – etwa wenn ein vorgeschlagenes Label nicht zur beabsichtigten Nutzung passt.

Schwellwerte richtig definieren

Ein zentraler Aspekt bei empfohlenen Labels sind die **Schwellwerte**, also die Bedingungen, unter denen ein Label vorgeschlagen wird.

Beispiel: Ein Label wird erst vorgeschlagen, wenn mindestens 50 Kreditkartennummern im Text erkannt wurden.

Hier stellt sich die Frage:

- Soll der Schwellwert niedrig sein, um möglichst viel zu erfassen?
- Oder eher hoch, um nur in wirklich relevanten Fällen einzutreten?

Die Entscheidung hängt von Ihrer Zielsetzung ab – und davon, wie viel Transparenz und Automatisierung Ihre Benutzerinnen und Benutzer verkraften, ohne überfordert zu werden.

Ein Pilotbetrieb mit angepasstem Schwellwert ist in jedem Fall ratsam.

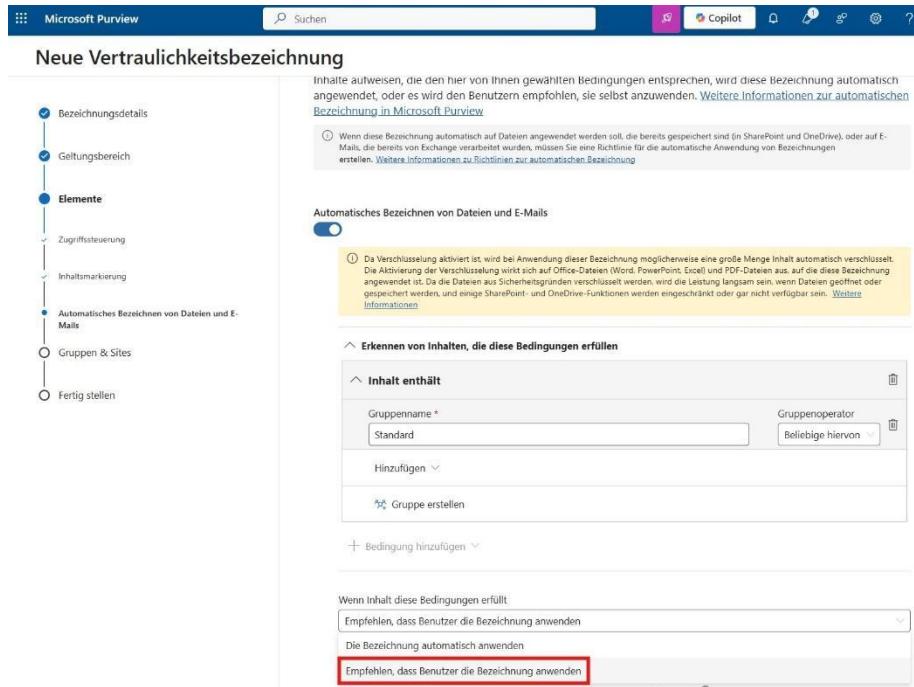


Abbildung 137

Schritt 7 – Gruppen & Sites: Beim Erstellen einer Vertraulichkeitsbezeichnung lässt sich optional festlegen, ob diese auch auf **Microsoft 365 Gruppen und SharePoint Sites** angewendet werden soll.

Falls diese Option in Ihrer Umgebung derzeit nicht aktiv genutzt wird, können Sie diesen Schritt zunächst überspringen und sich auf Dateien und E-Mails konzentrieren.



Abbildung 138

Schritt 8 – Fertig stellen: Hier überprüfen wir alle Konfigurationen und erstellen die neue Bezeichnung. Nachdem sie angelegt wurde, zeigt das System eine Zusammenfassung Ihrer Konfiguration. Mit einem Klick auf **Bezeichnung erstellen** wird die Bezeichnung gespeichert – allerdings ist sie damit **noch nicht automatisch verfügbar**.



Abbildung 139

Jetzt legen wir fest, ob und an wen das Label veröffentlicht werden soll. Dies geschieht über die Option **Veröffentlichen von Bezeichnungen für Benutzer Apps**.

Hier definieren Sie

- welche Benutzergruppen Zugriff auf das Label erhalten und

- in welchen Anwendungen (z. B. Word, Outlook, Teams) es verwendet werden darf.

Dieser Veröffentlichungsprozess sorgt dafür, dass nur autorisierte Nutzerinnen und Nutzer die Möglichkeit erhalten, das Label aktiv auf Inhalte anzuwenden.

Zuweisung und Veröffentlichung von Labels

Pfad: purview.microsoft.com → Lösungen → Microsoft Azure Information Protection → Richtlinien → **Richtlinien zur Veröffentlichung**

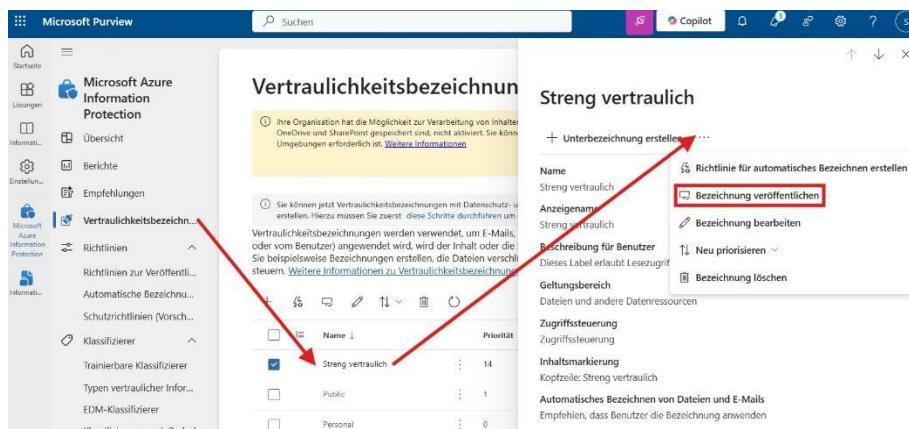
Sobald eine Vertraulichkeitsbezeichnung erstellt wurde, müssen wir ihr **über eine Richtlinie zur Veröffentlichung** den entsprechenden Benutzergruppen zur Verfügung stellen.

Wir legen fest,

- welche Benutzergruppen oder Admin Units die Labels erhalten und
- ob bestimmte Labels standardmäßig vorgeschlagen oder verpflichtend angewendet werden sollen.

So entsteht eine klare Trennung zwischen

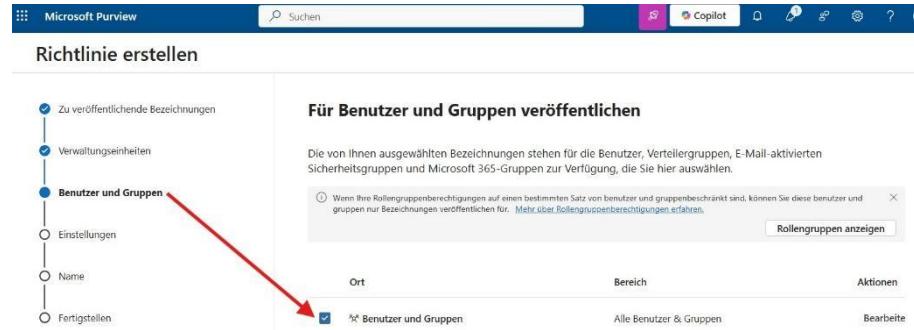
- den **Berechtigungen**, die ein Label definiert und
- der **Zielgruppe**, die dieses Label tatsächlich verwenden darf.



The screenshot shows the Microsoft Purview interface with the 'Microsoft Azure Information Protection' section selected. In the left sidebar, under 'Richtlinien', the 'Richtlinien zur Veröffentlichung' option is highlighted. The main content area displays a 'Vertraulichkeitsbezeichnung' (Classification Label) named 'Streng vertraulich'. A red arrow points from the 'Richtlinien' section in the sidebar to the 'Bezeichnung veröffentlichen' (Publish Label) button in the main content area. Another red arrow points from the 'Streng vertraulich' label entry in the list below to the same button.

Name	Priority
Streng vertraulich	14
Public	1
Personal	0

Abbildung 140



Zu veröffentlichte Bezeichnungen

Verwaltungseinheiten

Benutzer und Gruppen

Einstellungen

Name

Fertigstellen

Für Benutzer und Gruppen veröffentlichen

Die von Ihnen ausgewählten Bezeichnungen stehen für die Benutzer, Verteilergruppen, E-Mail-aktivierten Sicherheitsgruppen und Microsoft 365-Gruppen zur Verfügung, die Sie hier auswählen.

Wenn Ihre Rollengruppenberechtigungen auf einen bestimmten Satz von benutzer und gruppenbeschränkt sind, können Sie diese benutzer und gruppen nur Bezeichnungen veröffentlichen für. [Mehr über Rollengruppenberechtigungen erfahren.](#)

Rollengruppen anzeigen

Ort	Bereich	Aktionen
<input checked="" type="checkbox"/> Benutzer und Gruppen	Alle Benutzer & Gruppen	Bearbeiten

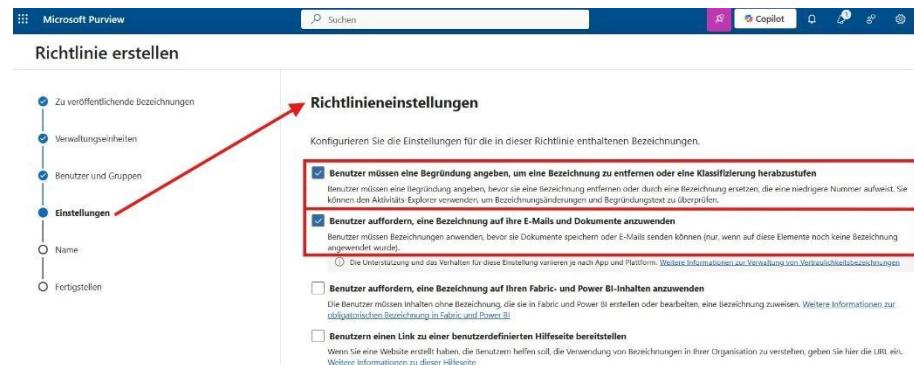
Abbildung 141

In der Richtlinien-Konfiguration können wir zusätzliche Regeln aktivieren:

- Benutzer müssen eine Begründung angeben, um eine Bezeichnung zu entfernen oder eine Klassifizierung herabzustufen.
- Benutzer auffordern, eine Bezeichnung auf ihre E-Mails und Dokumente anzuwenden.

Viele Unternehmen starten zunächst mit optionalen Labels und **führen die Pflicht zur Klassifizierung stufenweise ein**, um die Akzeptanz im Unternehmen zu erhöhen.

Auch wenn Datenklassifizierung für viele Unternehmen **noch nicht etabliert ist**, gilt: **Jedes Unternehmen in Deutschland sollte über ein Klassifizierungskonzept verfügen** – unabhängig davon, ob dies technisch umgesetzt ist oder nur in Richtlinienform vorliegt.



Zu veröffentlichte Bezeichnungen

Verwaltungseinheiten

Benutzer und Gruppen

Einstellungen

Name

Fertigstellen

Richtlinieneinstellungen

Konfigurieren Sie die Einstellungen für die in dieser Richtlinie enthaltenen Bezeichnungen.

Benutzer müssen eine Begründung angeben, um eine Bezeichnung zu entfernen oder eine Klassifizierung herabzustufen
Die Benutzer müssen eine Begründung angeben, bevor sie eine Bezeichnung entfernen oder durch eine Bezeichnung ersetzen, die eine niedrigere Nummer aufweist. Sie können den Akthubs Explorer verwenden, um Bezeichnungsänderungen und Begründungen zu überprüfen.

Benutzer auffordern, eine Bezeichnung auf ihre E-Mails und Dokumente anzuwenden
Die Benutzer müssen Bezeichnungen anwenden, bevor sie Dokumente speichern oder E-Mails senden können (nur, wenn auf diese Elemente noch keine Bezeichnung angewendet wurde).

Benutzer auffordern, eine Bezeichnung auf ihren Fabric- und Power BI-Inhalten anzuwenden
Die Benutzer müssen Inhalte ohne Bezeichnung, die in Fabric und Power BI erstellen oder bearbeiten, eine Bezeichnung zuweisen. Weitere Informationen zur obligatorischen Bezeichnung in Fabric und Power BI.

Benutzen einen Link zu einer benutzerdefinierten Hilfeseite bereitstellen
Wenn Sie eine Website erstellt haben, die Benutzern helfen soll, die Verwendung von Bezeichnungen in Ihrer Organisation zu verstehen, geben Sie hier die URL ein. Weitere Informationen zu dieser Hilfeseite.

Abbildung 142

Innerhalb der **Richtlinie zur Veröffentlichung** können wir außerdem **Default-Labels für verschiedene Typen** definieren – darunter:

- Dokumente
- E-Mails
- Meetings
- Microsoft Teams Sites
- Power BI
- Microsoft Fabric

Auch wenn Labels für Power BI oder Fabric **selten genutzt werden**, besteht die Möglichkeit, diese ebenfalls in Ihre Klassifizierungsstrategie einzubeziehen.

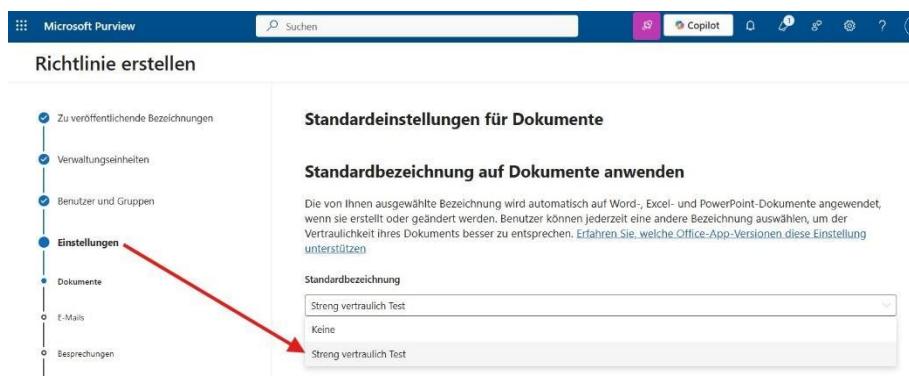


Abbildung 143

Zum Schluss geben Sie der Richtlinie einen Namen, klicken auf **Weiter** und **Fertigstellen**.

Damit wird das Label für die ausgewählten Gruppen **bereitgestellt** und ist in der Benutzeroberfläche – z. B. in Word oder Outlook – verfügbar.

Einsatz von eDiscovery zur Analyse digitaler Aktivitäten

Wenn es darum geht, ein umfassendes digitales Abbild von Benutzeraktivitäten zu erstellen – z. B. zur Beweissicherung oder Dokumentation – bietet sich die Nutzung von **eDiscovery in Microsoft 365** an.

Dieses Werkzeug ermöglicht die Suche und Archivierung von:

- E-Mails
- Chatnachrichten

- Dateien
- Teams-Kommunikation und mehr

Auch im Kontext von Microsoft Copilot lässt sich eDiscovery einsetzen.

Pfad: purview.microsoft.com → eDiscovery → Fälle

Wir wählen nun einen beliebigen Fall und klicken uns durch zu **Bedingungen hinzufügen**.

Über Copilot Search können wir gezielt nach Inhalten oder Aktionen innerhalb des Copilot-Kontextes suchen – z. B. anhand von Parametern wie **Autor, Absender oder Dateityp**.

Abbildung 144

Abbildung 145

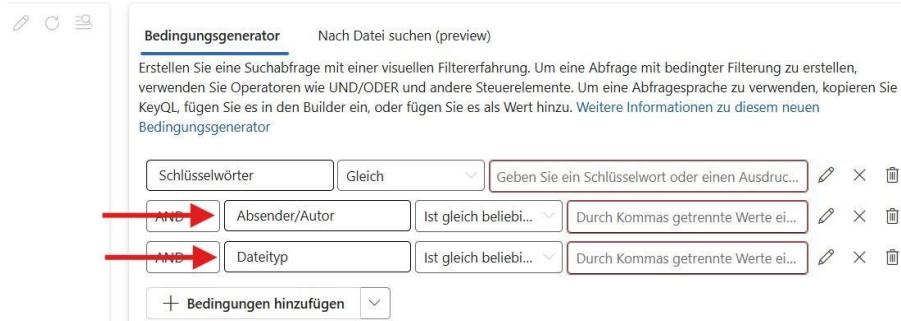


Abbildung 146

Pfad: purview.microsoft.com → Lösungen → **Überwachen**

Ergänzend zur eDiscovery bietet die Funktion **Überwachen** in Microsoft Purview eine sehr **feingranulare Nachverfolgung von Benutzeraktivitäten** – auf Klick-Ebene.

Hier können wir nachvollziehen,

- welche Dateien geöffnet, geändert oder gelöscht wurden,
- ob und wann Nachrichten versendet oder weitergeleitet wurden,
- und spezifisch für Copilot: **Welche Prompts eingegeben wurden.**

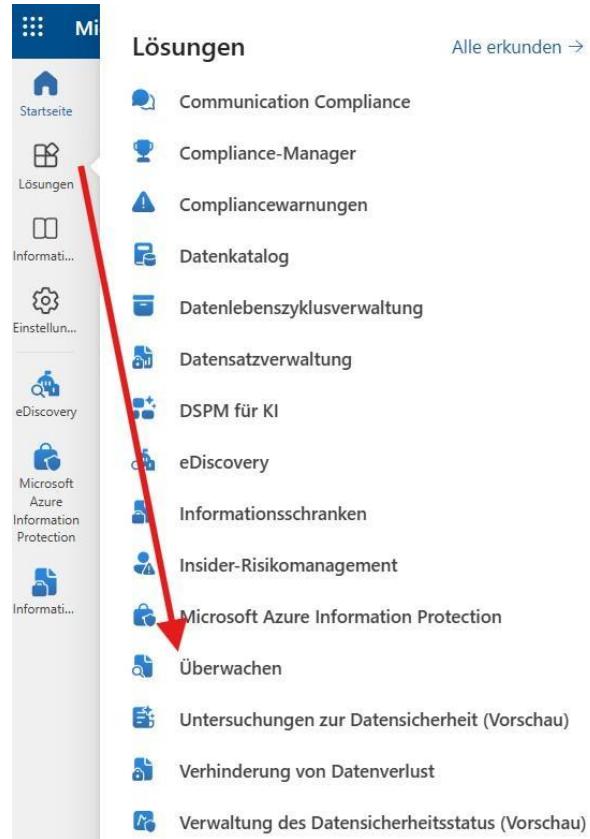
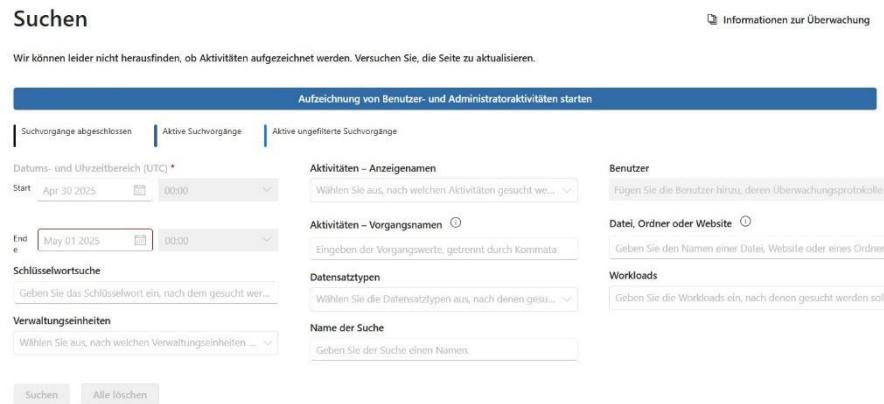


Abbildung 147



The screenshot shows the 'Suchen' (Search) page in the Microsoft 365 Admin Center. The search bar contains 'Aufzeichnung von Benutzer- und Administratoraktivitäten starten'. The search results show several filters: 'Datums- und Uhrzeitbereich (UTC)' (Start: April 30 2025, End: May 01 2025), 'Schlüsselwortsuche', 'Verwaltungseinheiten', 'Aktivitäten – Anzeigenamen' (with a placeholder 'Wählen Sie aus, nach welchen Aktivitäten gesucht werden...'), 'Aktivitäten – Vorgangsnamen' (with a placeholder 'Eingeben der Vorgangswerte, getrennt durch Komma...'), 'Datensatztypen' (with a placeholder 'Wählen Sie die Datensatztypen aus, nach denen gesucht werden...'), 'Name der Suche' (with a placeholder 'Geben Sie der Suche einen Namen...'), 'Benutzer' (with a placeholder 'Fügen Sie die Benutzer hinzu, deren Überwachungsprotokolle si...'), 'Datei, Ordner oder Website' (with a placeholder 'Geben Sie den Namen einer Datei, Website oder eines Ordners...'), and 'Workloads' (with a placeholder 'Geben Sie die Workloads ein, nach denen gesucht werden soll...'). At the bottom are 'Suchen' and 'Alle löschen' buttons.

Abbildung 148

Gerade für sicherheitskritische Umgebungen stellt das Überwachen eine **wertvolle Ergänzung zur eDiscovery** dar – mit höherer Detailtiefe.

Trotz der technischen Möglichkeiten bestehen bei vielen Organisationen **datenschutzrechtliche und mitbestimmungsrelevante Vorbehalte** gegenüber dem Einsatz von eDiscovery und Überwachen – insbesondere zur Überwachung von Copilot-Aktivitäten.

Während IT-Abteilungen diese Tools gern zur **Absicherung oder Fehleranalyse** einsetzen würden, verweigern Datenschützer und Betriebsräte mitunter die Freigabe. Daher ist eine **frühzeitige Abstimmung mit den zuständigen Gremien** (z. B. Datenschutzbeauftragten oder dem Betriebsrat) essenziell, bevor solche Lösungen implementiert werden.

Compliance-Prüfung vor dem Einsatz

Bevor Überwachungsfunktionen aktiv genutzt werden, sollte intern geprüft werden, ob der Einsatz **datenschutzkonform** möglich ist.

Auch wenn Tools wie eDiscovery oder Überwachen technisch viel ermöglichen, gilt: **Transparenz, Dokumentation und Zustimmung relevanter Gremien (z. B. Datenschutz, Betriebsrat)** sind unerlässlich.

Das Überwachungstool erlaubt sehr **detaillierte Einblicke** in verschiedene Benutzeraktivitäten:

- Welche Datei wurde wann geöffnet, verändert oder gelöscht?
- Wer hat wem Berechtigungen erteilt?

IT-Tasks: Microsoft 365 Umgebung vorbereiten

Das IT-Team spielt eine Schlüsselrolle bei der Vorbereitung der Microsoft 365 Umgebung für Copilot. Von Governance und Sicherheit über Datenhygiene bis zur Lizenzzuweisung gilt es, Standards zu setzen und Risiken zu minimieren.

Werfen wir nun einen Blick auf alle Maßnahmen zur Microsoft 365 Copilot Governance, die ich Ihnen nun schrittweise empfehle.

Risikominimierung und Optimierung in Sharepoint

- Unbenutzte Sites bereinigen, um Content Sprawl zu reduzieren
- Sites mit freigegebenem Inhalt identifizieren bzw. analysieren
- Download-Richtlinien für SharePoint- und OneDrive-Sites blockieren
- Bedingten Zugriff für SharePoint und OneDrive einrichten

Optimierung der SharePoint-Sicherheit und -Verwaltung

- Zugriff auf (SharePoint-)Inhalte kontrollieren
- Zugriffsberechtigungen für SharePoint einrichten
- Suchberechtigungen für SharePoint aktivieren
- „Proaktive Maßnahmen“ für (geschäfts-)kritische SharePoint-Sites ergreifen
- Sicherstellen, dass alle SharePoint-Sites gültige Besitzer haben
- SharePoint-Sites in den Lese-Modus setzen, löschen oder archivieren

Strukturierung und Datenhygiene in Microsoft 365

- Überprüfung aller Dokumente, E-Mails, Chats und Wikis auf Relevanz und Löschung von nicht benötigten Inhalten
- Entwicklung einer **klaren Taxonomie** für die Kategorisierung von Dokumenten, E-Mail, SharePoint-Seiten etc.
- Kategorisierung mit Labels, Hashtags und Metadaten
- Festlegung einer **organisationsweiten Namenskonvention** (Q1 2025 Earnings Report.docx statt Q3Rep_v4final(1).docx)
- Versionierung für SharePoint und OneDrive bearbeiten
- Schulung und Change Management zur Einhaltung einer „Datenhygiene“

Datenrichtlinien, Verantwortlichkeiten und Audits

- Ernennung eines Data Stewards, der für die Vorbereitung, Pflege und Qualitätssicherung von Daten zuständig ist.
- Datenrichtlinien und Nutzungspraktiken für Microsoft 365 und Copilot dokumentieren, um klare Standards zu setzen.

- Regelmäßige Audits:
 - Identifikation neuer Datenquellen, die Zugriffsbeschränkungen oder Freigabeänderungen erfordern.
 - Analyse von Berechtigungen und externen Freigaben, um „Datenbreaches“ zu reduzieren.

Effektive Zugriffs- und Validierungsprozesse

- Implementierung der *Microsoft SharePoint Advanced Management Tools*
- Berichte zur Datenzugriffsgovernance
 - Zugriffsbeschränkungen
 - Überprüfung des Websitezugriffs
 - Eingeschränkte Inhaltsermittlung
- Zugriffsüberprüfungen im Entra ID und SharePoint anwenden
- Validierung der Suchergebnisse (Kreuztest mit Nutzern)

“Just Enough Access” mit Microsoft Purview und Entra

- Erarbeitung eines „just enough access“-Konzeptes:
 - Microsoft Purview Information Protection
 - Microsoft Purview Vertraulichkeitsbezeichnungen
 - Microsoft Entra Conditional Access Richtlinien
 - (Microsoft Entra – Verwaltung privilegierter Identitäten (PIM))
 - Microsoft Graph-Konnektoren und -Erweiterungen

Zuweisung der Microsoft 365 Copilot Lizenz

- Microsoft 365 Copilot Usage Report: [Usage- Microsoft 365 admin center](#)

The screenshot shows the Microsoft 365 Copilot setup guide dashboard. On the left, a sidebar lists various Microsoft 365 services. The main area has two main sections: 'Make sure your users are eligible for Copilot' and 'Track your organization's available Copilot licenses'. The 'Copilot Chat' service is highlighted in the sidebar.

Make sure your users are eligible for Copilot

- Total prerequisite licenses: 5
- Users on an eligible update channel: 1

This is not a complete list of requirements. To view all requirements and get assistance rolling out Copilot to your organization, go to the Microsoft 365 Copilot setup guide.

Recommendations

- Pin Copilot for all of your users: Go to Settings to pin Copilot. Make it easier for everyone to find and use Copilot in apps like Teams and Outlook. [Show me](#)
- Deliver insights to your IT leader with the Microsoft Copilot Dashboard: Give your leaders access to explore Copilot readiness, adoption, and impact in Viva Insights. [Open the Copilot Dashboard](#)

Enable active users of Microsoft 365 apps

Active Microsoft 365 app users

App	Count
Teams meetings	2
Teams chat	3
Outlook email	4
Office docs	1
Any of these	7

To get the most out of Copilot, users should be actively using Microsoft 365 apps in Microsoft Teams and Outlook.

Abbildung 149

Definierung und Erstellung von Copilot Agents

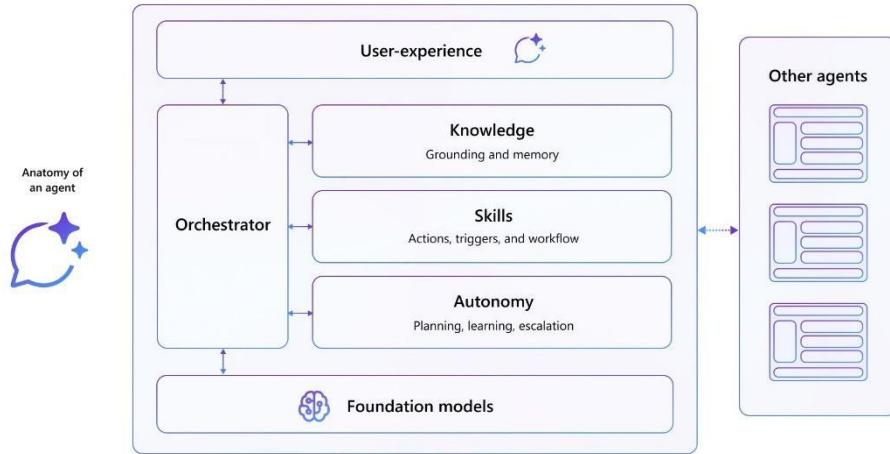


Abbildung 150

(Quelle <https://learn.microsoft.com/de-de/microsoft-365-copilot/extensibility/assets/images/anatomy-agents.png>)