Sabrina Wrobel

Handout - Oversharing

Szenarien, mögliche Folgen und wie man sie abfangen kann

Merksatz: Copilot erzeugt keine neuen Berechtigungen. Er macht aber vorhandene Zugriffe sehr viel sichtbarer, weil er Inhalte über mehrere Quellen hinweg findet, zusammenfasst und kombiniert.

Szenario	Wodurch entsteht es?	Mögliche Folgen	Abfangen / Gegenmaßnahmen
Zu weit gefasste Gruppenmitgliedschaften	Große Gruppen wie „Alle Mitarbeitenden“, alte dynamische Gruppen oder Sammelgruppen werden für Sites, Teams oder Ordner berechtigt.	Personen sehen Inhalte außerhalb ihrer Rolle. Copilot kann diese Inhalte in Antworten einbeziehen und dadurch sensible Informationen leichter auffindbar machen.	Gruppen nach Rollen und Zweck schneiden, Mitgliedschaften regelmäßig prüfen, Access Reviews aktivieren und „Least Privilege“ als Standard verwenden.
Unkontrollierte Datei- oder Ordnerfreigaben	Einzelne Dateien oder ganze Ordner werden spontan geteilt, oft ohne Ablaufdatum, ohne Besitzerprüfung oder mit zu breiten Linktypen.	Alte Freigaben bleiben aktiv. Ergebnisse aus ehemals geteilten Dokumenten tauchen später unerwartet in Suche oder Copilot-Antworten auf.	Standard-Link auf „bestimmte Personen“ setzen, Ablaufdaten erzwingen, anonyme Links begrenzen und Freigabeberichte regelmäßig auswerten.
Vererbte Berechtigungen in SharePoint	Berechtigungen werden von Site, Bibliothek oder Ordner nach unten vererbt. Einzelne Bereiche bekommen dadurch mehr Zugriff als fachlich nötig.	Oversharing bleibt unsichtbar, weil der Zugriff nicht direkt am Dokument vergeben wurde. Betroffene wissen oft nicht, woher der Zugriff kommt.	Berechtigungsvererbung gezielt dokumentieren, eindeutige Site-Strukturen verwenden und Ausnahmen auf Ordner- oder Bibliotheksebene minimieren.
Historisch gewachsene Rechte nach Rollenwechsel	Beschäftigte wechseln Teams oder Projekte, behalten aber alte Gruppen, Teams, Sites oder Postfachberechtigungen.	Informationen aus früheren Tätigkeiten bleiben sichtbar. In Copilot können alte Projekt-, Personal- oder Finanzkontexte wieder auftauchen.	Joiner-Mover-Leaver-Prozess pflegen, automatische Gruppenregeln nutzen, Rechte beim Rollenwechsel entziehen und Projektzugriffe befristen.
Externe Gäste mit zu breitem Zugriff	Partner, Lieferanten oder Freelancer werden in Teams oder Sites eingeladen und bleiben nach Projektende aktiv.	Externe Konten können weiter auf interne Dokumente zugreifen. Das erhöht Risiko für Datenabfluss und Compliance-Verstöße.	Gastzugriff nur projektbezogen vergeben, Gastablauf und Access Reviews aktivieren, externe Freigabe je Site begrenzen und Gäste nach Projektende entfernen.
Sensible Daten im falschen Teams-Kanal	Vertrauliche Informationen werden im allgemeinen Team, im falschen Kanal oder in einem Kanal mit breiter Mitgliedschaft abgelegt.	Dateien, Chats und Notizen sind für alle Teammitglieder sichtbar. Copilot kann Inhalte aus Kanaldateien und Konversationen zusammenführen.	Private oder geteilte Kanäle bewusst einsetzen, Teammitgliedschaften klein halten, Kanalregeln definieren und sensible Dateien in passende Sites verschieben.

Oversharing-Szenarien (Fortsetzung)

Szenario	Wodurch entsteht es?	Mögliche Folgen	Abfangen / Gegenmaßnahmen
Fehlende oder falsche Sensitivity Labels	Dokumente werden nicht klassifiziert oder tragen Labels, die nicht zum Schutzbedarf passen.	Schutzlogik wie Verschlüsselung, Wasserzeichen, DLP oder Einschränkung externer Freigaben greift nicht zuverlässig.	Label-Strategie festlegen, Standard- und Pflichtlabels verwenden, automatische Label-Vorschläge prüfen und besonders sensible Inhalte verschlüsseln.
OneDrive als Schattenablage	Teams speichern Arbeitsstände, Exporte oder Kopien dauerhaft in persönlichen OneDrive-Bereichen und teilen sie manuell weiter.	Dubletten und alte Versionen bleiben auffindbar. Beim Austritt oder Rollenwechsel ist unklar, welche Kopien noch geteilt sind.	Gemeinsame Dateien in SharePoint/Teams ablegen, OneDrive-Freigaben regelmäßig prüfen, Aufbewahrung regeln und veraltete Kopien löschen.
Meetingnotizen, Transkripte und Chatverläufe	Besprechungen erzeugen automatisch Notizen, Aufzeichnungen oder Transkripte, deren Ablage und Berechtigungen nicht bewusst geprüft werden.	Aussagen, Entscheidungen oder personenbezogene Details werden später über Suche oder Copilot wiedergefunden.	Aufzeichnungs- und Transkriptionsrichtlinien definieren, vertrauliche Meetings kennzeichnen, Ablageorte prüfen und Löschfristen anwenden.
Fehlender Datenlebenszyklus	Alte Projektablagen, Exportdateien, Testdaten oder temporäre Listen bleiben ohne Verantwortliche bestehen.	Veraltete oder falsche Informationen fließen in Entscheidungen ein. Zusätzlich wächst die Angriffsfläche, weil unnötige Daten weiter zugänglich sind.	Retention- und Löschkonzepte einsetzen, Site Lifecycle Management nutzen, Besitzer benennen und archivierte Bereiche von aktiven Arbeitsräumen trennen.
Zu breite administrative oder privilegierte Rollen	Adminrollen, Site-Owner-Rechte oder Postfachrechte werden dauerhaft vergeben, obwohl sie nur kurzfristig benötigt werden.	Privilegierte Personen können mehr Inhalte oder Einstellungen sehen und verändern als nötig. Fehler wirken dadurch tenantweit oder siteübergreifend.	PIM/JIT-Zugriff einsetzen, Adminrollen trennen, regelmäßige Rollenreviews durchführen und privilegierte Konten getrennt halten.
Copilot als Verstärker vorhandener Berechtigungen	Copilot respektiert Berechtigungen, kann aber über viele Quellen hinweg schneller finden, zusammenfassen und kombinieren.	Ein Zugriff, der vorher nur theoretisch vorhanden war, wird praktisch sichtbar. Kleine Berechtigungslücken bekommen größere Wirkung.	Vor Copilot-Rollout Berechtigungen bereinigen, Search- und SharePoint-Berichte prüfen, Pilotgruppen verwenden und Nutzer für sichere Prompts sensibilisieren.

Schnellcheck vor Freigabe oder Copilot-Rollout

Nutze die Fragen als kurze Prüfung, bevor neue Teams, Sites, Bibliotheken oder Copilot-Pilotgruppen freigegeben werden.

□ Wer braucht den Zugriff wirklich für seine aktuelle Aufgabe?	□ Ist der Zugriff befristet oder regelmäßig überprüft?
□ Gibt es eine verantwortliche Person für Site, Team oder Bibliothek?	□ Ist externe Freigabe bewusst erlaubt und dokumentiert?
□ Sind besonders schützenswerte Daten korrekt gelabelt?	□ Würden Copilot-Antworten mit diesen Quellen fachlich und datenschutzrechtlich passen?

Empfohlene Reihenfolge in der Praxis

1. Inventarisieren	Sites, Teams, Gruppen, Gäste und besonders sensible Bibliotheken sichtbar machen.
2. Bereinigen	Offene Links, alte Projektgruppen, unnötige Gäste und vererbte Ausnahmen entfernen.
3. Begrenzen	Standardfreigaben, externe Zusammenarbeit, Adminrollen und Ablaufdaten restriktiv einstellen.
4. Schützen	Sensitivity Labels, DLP, Verschlüsselung und Aufbewahrung passend zum Schutzbedarf anwenden.
5. Überwachen	Access Reviews, Audit-Logs und Besitzerverantwortung regelmäßig nutzen.

Praxisformel: Erst Berechtigungen bereinigen, dann Copilot breit ausrollen. Je sauberer Gruppen, Labels und Freigaben gepflegt sind, desto weniger Überraschungen entstehen in KI-Antworten.