

Gäste in Teams und SharePoint: Planungsbüros, Träger und Gremienmitglieder sicher einbinden

Die gefährlichste Formulierung in der Verwaltungs-IT lautet nicht „Cyberangriff“. Sie lautet „nur ganz kurz“. Das Bauamt braucht das Architekturbüro nur ganz kurz im Projektkanal. Das Jugendamt möchte den freien Träger nur ganz kurz an die Sachstandsliste lassen. Und die Ratsfraktion hätte nur ganz kurz Zugriff auf die Unterlagen zur nächsten Sitzung, natürlich vom privaten Tablet, natürlich am Sonntagabend, natürlich sofort.

Aus „nur ganz kurz“ wird in der Praxis ein Gastkonto, das drei Jahre später immer noch existiert, weil die Person, die es angelegt hat, inzwischen im Ruhestand ist und die Person, die es hätte beenden müssen, nie erfahren hat, dass sie zuständig war. Externe Zusammenarbeit scheitert in Verwaltungen fast nie an der Technik. Sie scheitert daran, dass niemand den Vorgang als Vorgang behandelt: mit Anlass, Zuständigkeit, Frist und Abschluss.

Dieser Beitrag ordnet die vier Mechanismen ein, mit denen Microsoft 365 externe Personen einbindet, vergleicht sie nach Kontrolle und Risiko und beschreibt einen Gastlebenszyklus, den Sie einer Verwaltungsspitze und einem Rechnungsprüfungsamt erklären können. Er ist Teil unserer Reihe [Microsoft 365 in der öffentlichen Verwaltung](#), in der wir die Einführungsfragen von Kommunen, Kreisen, Landesbehörden, Zweckverbänden und kirchlichen Trägern der Reihe nach durchgehen. Wenn Sie die Informationsarchitektur Ihrer Ämter noch gar nicht gebaut haben, lesen Sie besser zuerst [Microsoft Teams in der Verwaltung einführen: Informationsarchitektur entlang der Ämter](#) – Gäste in einer unsortierten Landschaft sind kein Zugriffsproblem, sondern ein Ordnungsproblem mit Zugriffsfolgen.

FAKTEN • Was Sie über Gäste in Microsoft 365 wissen sollten

Vier Mechanismen, nicht einer. Gastkonto (B2B Collaboration), Freigabelink in SharePoint und OneDrive, freigegebener Kanal über B2B Direct Connect und das Extranet-Muster mit Zugriffspaketen aus der Identitätsgovernance. Sie unterscheiden sich fundamental darin, was in Ihrem Tenant entsteht.

Ein Gastkonto ist ein Verzeichnisobjekt. Es wird in Entra ID angelegt, unterliegt Ihren Richtlinien für bedingten Zugriff und Ihrer Protokollierung – und es bleibt bestehen, wenn die Person das Team verlässt. Nur eine administrative Löschung entfernt es.

Ein freigegebener Kanal erzeugt kein Verzeichnisobjekt. Externe Teilnehmer arbeiten mit ihrem eigenen Arbeitsplatz-Account. Dafür müssen beide Organisationen die mandantenübergreifenden Zugriffseinstellungen gegenseitig freigeben. Standardmäßig ist das in beide Richtungen blockiert.

Zusätzliche Microsoft-365-Lizenzen braucht ein Gast nicht. Für den Gastzugang in Teams gilt das Abrechnungsmodell von Entra External ID; ein eigenes Nutzerkonto mit Lizenz ist nicht erforderlich.

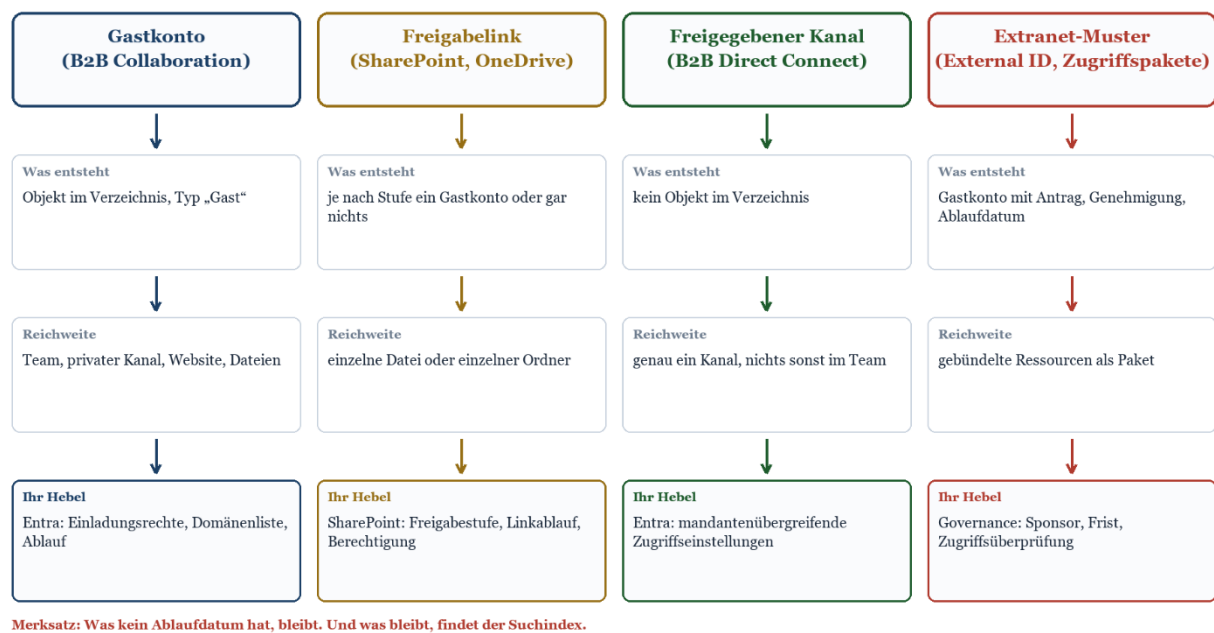
Gäste sind sichtbar gekennzeichnet. In Teams trägt der Name den Zusatz „Gast“, und der Kanal zeigt an, dass Externe beteiligt sind. Das ist eine Hilfe, aber kein Schutz: Gelesen wird der Zusatz meist erst, wenn die Datei schon hochgeladen ist.

Die vier Mechanismen und was sie wirklich tun

Bevor wir über Regeln reden, muss die Unterscheidung sitzen. In neun von zehn Verwaltungen, in die wir kommen, wird „Gast“ als Sammelbegriff für alles benutzt, was von außen kommt. Das führt zu Regelwerken, die entweder zu viel verbieten oder zu wenig – und in beiden Fällen umgangen werden.

Vier Türen ins Rathaus

Wie externe Personen an Inhalte kommen – und was dabei im Tenant entsteht



Merksatz: Was kein Ablaufdatum hat, bleibt. Und was bleibt, findet der Suchindex.

Skizze 1: Die vier Wege, auf denen externe Personen an Inhalte gelangen, mit dem jeweiligen Verzeichnisobjekt, der Reichweite und dem administrativen Hebel.

Das Gastkonto: der Klassiker mit Verzeichnisobjekt

Bei der B2B-Zusammenarbeit legt Entra ID für die externe Person ein Benutzerobjekt vom Typ „Gast“ an. Die Person meldet sich mit ihrer eigenen Identität an – ein Arbeitsplatz-Account, ein Microsoft-Konto oder, wenn nichts davon vorhanden ist, eine per E-Mail zugestellte Einmalkennung. Seit dem Umbau des Anmeldeerlebnisses, den Microsoft im Juli 2025 begonnen und bis Ende 2025 abgeschlossen hat, wird die Person dabei zur Anmeldeseite ihrer eigenen Organisation umgeleitet und sieht deren Erscheinungsbild, nicht Ihres. Für die Beschäftigten im Amt ist das unsichtbar, für Rückfragen aus dem Planungsbüro erklärt es einiges.

Der entscheidende Punkt für Sie: Ein Gastkonto ist ein Objekt in Ihrem Verzeichnis. Es lässt sich mit bedingtem Zugriff steuern, in Zugriffsüberprüfungen aufnehmen, protokollieren und auditieren. Es taucht in Gruppenmitgliedschaften auf, es kann zu Teams, privaten Kanälen, Websites und einzelnen Dateien berechtigt werden. Und es verschwindet nicht von selbst. Wenn ein Gast das Team über die Teams-Oberfläche verlässt, ist er aus dem Team raus – das Konto bleibt im Verzeichnis, bis jemand es administrativ entfernt. Genau hier entstehen die Karteileichen, die im Prüfbericht später „nicht nachvollziehbare Zugriffsberechtigungen Externer“ heißen.

Ein zweites Detail, das Erwartungsmanagement erspart: Nachdem ein Gast einem Team hinzugefügt wurde, kann es bis zu zwölf Stunden dauern, bis der Zugriff vollständig wirkt. Wer das

nicht weiß, legt in der Zwischenzeit ein zweites Konto an, teilt zur Sicherheit noch einen Link und schickt die Datei am Ende doch per Mail. Drei Wege, ein Dokument, kein Nachweis.

Der Freigabelink: der schnellste Weg und der unauffälligste

SharePoint und OneDrive kennen vier Freigabestufen: „Jeder“ mit anonymen Links, „neue und vorhandene Gäste“, „nur vorhandene Gäste“ und „nur Personen in Ihrer Organisation“. Die Stufe auf Ebene der einzelnen Website darf nur gleich oder strenger sein als die Tenant-Einstellung; die restriktivere Einstellung gewinnt immer. Für OneDrive gilt dasselbe Verhältnis zur SharePoint-Einstellung.

„Jeder“-Links sind der Grund, warum die Freigabediskussion in Verwaltungen emotional wird. Sie funktionieren ohne Anmeldung, sie funktionieren beim Weiterleiten, und Sie können hinterher nicht feststellen, wer den Inhalt tatsächlich geöffnet hat. Wenn Sie diese Stufe überhaupt zulassen, dann mit erzwungenem Ablaufdatum und ausschließlich mit Leserecht. In den meisten Verwaltungen ist die richtige Antwort schlicht: nicht zulassen. Es gibt kaum einen Vorgang im Rathaus, der einen anonymen Link zwingend braucht, und es gibt sehr viele, die ihn nicht überleben würden.

Wichtig für die Steuerung: Wenn die Integration mit Entra B2B aktiv ist, entsteht auch bei der Datei- und Ordnerfreigabe immer ein Gastkonto, und die Entra-Regeln für Einladungen und Domänen greifen. Ohne diese Integration kann eine Dateifreigabe an der Verzeichnissteuerung vorbeilaufen. Das ist einer der wenigen Schalter, bei denen wir in Verwaltungen praktisch immer dieselbe Empfehlung geben.

Der freigegebene Kanal: elegant, aber mit Voraussetzung auf beiden Seiten

Freigegebene Kanäle über B2B Direct Connect sind der sauberste Mechanismus, wenn Ihr Gegenüber selbst mit Entra ID arbeitet – also bei einem Landesbetrieb, einem Nachbarkreis, einem Zweckverband, einem größeren Planungsbüro oder einem Wohlfahrtsverband mit eigener Microsoft-365-Umgebung. Die externen Personen bleiben in ihrem eigenen Mandanten angemeldet, sehen den Kanal in ihrer eigenen Teams-Oberfläche und wechseln nirgends hin. In Ihrem Verzeichnis entsteht kein Objekt.

Der Preis dafür ist Abstimmung. B2B Direct Connect ist standardmäßig in beide Richtungen für alle Organisationen blockiert. Beide Seiten müssen einander in den mandantenübergreifenden Zugriffseinstellungen freigeben – eingehend bei Ihnen, ausgehend beim Partner. Sie können die Freigabe auf einzelne Gruppen des Partners beschränken, wenn Sie dessen Gruppenkennung erhalten. Änderungen an diesen Einstellungen können bis zu zwei Stunden brauchen, bis sie wirken; das ausgestellte Token ist eine Stunde gültig. Wer diese Zeiten nicht einkalkuliert, verabredet eine Videokonferenz zur Freischaltung und sitzt dann gemeinsam vor einer Fehlermeldung.

Zwei Grenzen sollten Sie kennen, bevor Sie den Mechanismus als Universallösung verkaufen. Erstens: Externe Teilnehmer in freigegebenen Kanälen haben Zugriff auf genau diesen Kanal – nicht auf das übrige Team, nicht auf andere Kanäle, nicht auf Dateifreigabelinks Ihrer Organisation. Zweitens: Gäste im Sinne der B2B-Zusammenarbeit können freigegebene Kanäle weder sehen noch nutzen. Beide Mechanismen schließen sich im selben Kanal gegenseitig aus. Ein Projektteam, in dem ein Planungsbüro als Gast und ein Nachbarkreis über Direct Connect mitarbeiten sollen, braucht deshalb zwei getrennte Konstruktionen.

Wenn Sie den bedingten Zugriff bereits scharf gestellt haben, kommt hier eine Stolperstelle dazu: Verlangt Ihre Richtlinie eine Mehrfaktor-Anmeldung für externe Personen, müssen Sie in den eingehenden Vertrauenseinstellungen ausdrücklich festlegen, dass Sie den Mehrfaktor-Nachweis des Partnermandanten akzeptieren. Sonst werden die externen Teilnehmer blockiert, obwohl sie sich in ihrer eigenen Organisation ordnungsgemäß stark authentifiziert haben. Wie ein tragfähiges Regelwerk aussieht, haben wir in [Conditional Access für Verwaltungen: Regelwerk für Rathaus, Bauhof und Homeoffice](#) ausgearbeitet.

Entra External ID und das Extranet-Muster

Entra External ID ist der Produktname, unter dem Microsoft die externen Identitäten zusammengefasst hat. Für Verwaltungen sind zwei Ausprägungen relevant. Die eine ist die B2B-Zusammenarbeit im eigenen Arbeitsplatz-Mandanten – das ist der Gastzugang, über den wir bisher gesprochen haben. Die andere ist der Aufbau eines echten Extranets mit Zugriffspaketen aus der Identitätsgovernance: Die externe Person stellt einen Antrag, eine benannte Stelle im Fachamt genehmigt, das Paket bündelt Team, Website und Anwendung, und die Zuweisung hat ein Ablaufdatum.

Das ist der Mechanismus, der einem Verwaltungsvorgang am nächsten kommt, und er liefert nebenbei den Nachweis mit. Läuft die letzte Paketzugewweisung einer Person aus, wird sie in der Standardkonfiguration von der Anmeldung ausgeschlossen und das Gastkonto nach dreißig Tagen entfernt. Ein Sponsor – intern oder auf der Partnerseite – erhält die Ablaufmeldung und kann verlängern oder es laufen lassen. Genau diese Rollenzuweisung fehlt in fast jeder gewachsenen Gästelandschaft.

Der Haken ist die Lizenzierung: Identitätsgovernance mit Zugriffspaketen und wiederkehrenden Zugriffsüberprüfungen ist nicht in jeder Ausstattung enthalten. Bevor Sie ein Konzept darauf aufbauen, klären Sie die Ausstattung – die Behördenkonditionen und ihre Fallstricke haben wir in einem eigenen Beitrag auseinandergenommen.

Für die Einordnung der Stufen und dessen, was in E3, E5 und F3 tatsächlich enthalten ist, siehe [Microsoft 365 Lizenzen für Verwaltungen: E3, E5, F3 und die Behördenkonditionen](#).

Mechanismus, Kontrolle, Risiko: die Übersicht

Die folgende Tabelle ist die Kurzfassung, mit der wir in Workshops arbeiten. Sie eignet sich als Anlage zur Beschlussvorlage, weil sie ohne Produktschulung lesbar ist.

Mechanismus	Was Sie kontrollieren können	Wo das Risiko liegt
Gastkonto im Team (B2B Collaboration)	Einladungsberechtigung je Rolle, Domänen-Positiv- oder Negativliste, Verzeichnissichtbarkeit, bedingter Zugriff, Ablauf über Zugriffspakete, Zugriffsüberprüfung, vollständige Protokollierung	Das Konto überlebt den Anlass. Gast im falschen Team sieht alle Kanäle und die gesamte Dateiablage. Ohne Ablaufdatum keine Beendigung.
Freigabelink „vorhandene Gäste“	Freigabestufe je Website, Standard-Linktyp, Ablauf des Gastzugriffs in Tagen, Domänenbeschränkung, Protokoll über die Freigabe	Berechtigungen wandern an der Teamstruktur vorbei. Niemand sieht auf einer Website, wie viele Einzelfreigaben bestehen.
Freigabelink „Jeder“ (anonym)	Erzwungenes Ablaufdatum, Beschränkung auf Leserecht, vollständige Abschaltung auf Tenant- oder Websiteebene	Keine Authentifizierung, keine Zuordnung, unbegrenzte Weiterleitbarkeit. Für schutzbedürftige Verwaltungsinhalte ungeeignet.

Freigegebener Kanal (B2B Direct Connect)	Freigabe je Partnerorganisation ein- und ausgehend, Beschränkung auf einzelne Gruppen, Vertrauen in fremde Mehrfaktor- und Gerätenachweise, Protokoll im Ressourcen-Mandanten	Vertrauen wird an eine fremde Organisation delegiert. Sicherheitsniveau des Partners wird zu Ihrem. Ganze Teams als Kanalmitglied entziehen sich der Zugriffsüberprüfung.
Zugriffspaket (Identitätsgovernance)	Antrag, Genehmigung, Sponsor, Ablauf, automatische Entfernung, wiederkehrende Überprüfung, Nachweis für die Rechnungsprüfung	Setzt Ausstattung und Pflege voraus. Ein Paket ohne benannten Genehmiger ist nur ein umständlicheres Gastkonto.
Externer Zugriff für Chat und Besprechung	Zulassung je Domäne, getrennt vom Gastzugang steuerbar	Kein Zugriff auf Inhalte – dafür entsteht regelmäßig der Irrtum, damit sei die Zusammenarbeit geregelt.

Tabelle 1: Mechanismus, Kontrolle, Risiko. Die Zeilen schließen sich nicht gegenseitig aus – die meisten Verwaltungen brauchen drei davon parallel.

TIPP · Die Faustregel, die sich in Workshops bewährt hat

Ein Kanal, eine Organisation, ein Arbeitsplatz-Account beim Partner? Freigegebener Kanal.

Ein Dokument, eine Person, ein Termin? Freigabelink mit Ablauf.

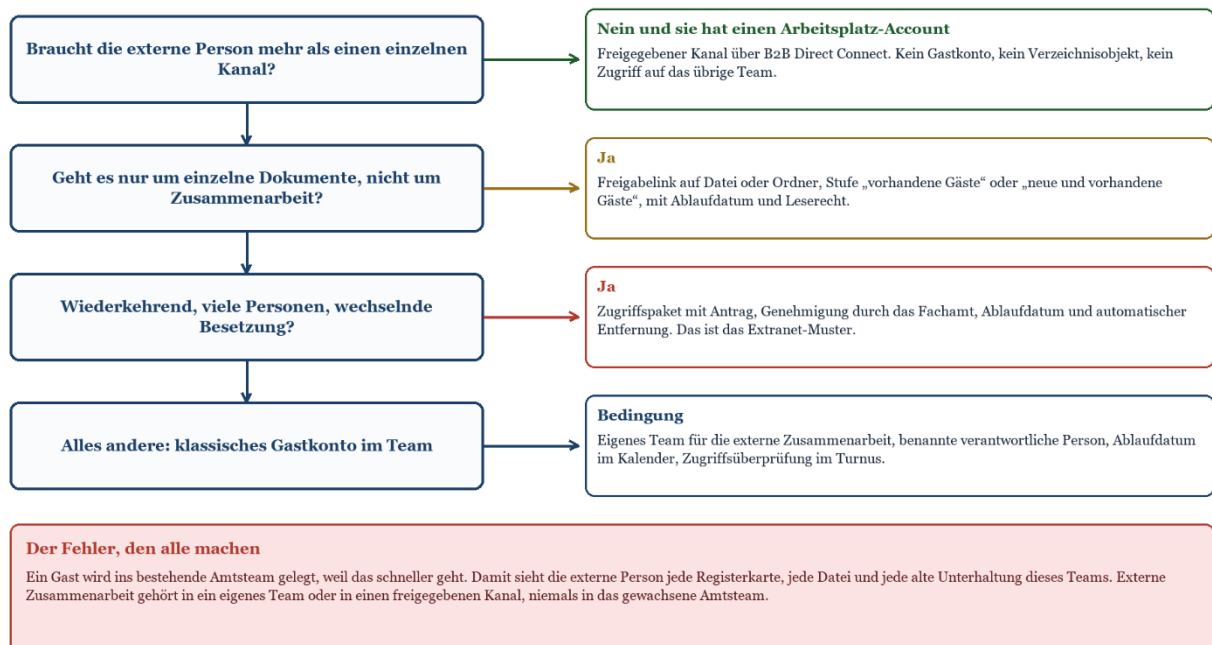
Ein Projekt, mehrere Externe, mehrere Monate? Eigenes Team mit Gastkonten und Ablaufdatum.

Wiederkehrend, wechselnde Besetzung, viele Partner? Zugriffspaket mit Sponsor.

Nie: Gäste in ein bestehendes Amtsteam legen, weil es schneller geht.

Entscheidungsbaum: Welcher Mechanismus für welchen Fall

Vier Fragen, die Sie vor jeder externen Zusammenarbeit beantworten



Skizze 2: Vier Fragen führen zum passenden Mechanismus. Der Entscheidungsbaum gehört in die Dienstanweisung, nicht in ein Handbuch, das niemand liest.

Drei Fälle aus der Verwaltungspraxis

Theorie überzeugt keine Amtsleitung. Die folgenden drei Konstellationen decken erfahrungsgemäß rund achtzig Prozent dessen ab, was in einer Kommune oder einem Landschaftsverband an externer Zusammenarbeit tatsächlich anfällt. Alle drei sind anonymisiert.

Das Planungsbüro im Vergabe- und Bauvorhaben

Eine Stadtverwaltung mit rund tausend Rufnummern führt ein Bauvorhaben mit wechselnden Fachplanern durch. Die Vergabestelle braucht eine saubere Trennung: Der Vergabevorgang selbst – Eignungsprüfung, Angebote, Wertung, Vergabevermerk – gehört in die Vergabeakte und in die dafür vorgesehene Fachanwendung, nicht in einen Teams-Kanal. Die Bauabwicklung nach Zuschlag dagegen ist ein Abstimmungsprozess, der von gemeinsamer Ablage profitiert.

Die tragfähige Konstruktion ist ein eigenes Projektteam pro Vorhaben, in dem die Fachplaner Gastkonten erhalten, mit einem Ablaufdatum, das an der geplanten Bauzeit hängt und mit Puffer verlängert wird, nicht mit Kulanz. Die Kämmererei bekommt keinen Gast, sondern einen internen Zugang. Die Rechnungsprüfung braucht am Ende nachvollziehbar: Wer war wann berechtigt, wer hat welche Version hochgeladen und wo liegt der aktenrelevante Stand.

Was in der Leistungsbeschreibung und in den Vergabeunterlagen zu Microsoft 365 selbst geregelt gehört, ist ein eigenes Thema; wir haben es in [Microsoft 365 rechtssicher beschaffen: Vergabe, Leistungsbeschreibung, Rahmenverträge](#) behandelt. Wertgrenzen, Fristen und Schwellenwerte richten sich nach dem jeweiligen Landesrecht und der einschlägigen Vergabeordnung – prüfen Sie das mit Ihrer Vergabestelle, nicht anhand eines Fachartikels.

Der freie Träger im Sozialbereich

Eine Stadtverwaltung, die SharePoint im Sozialbereich einsetzt, arbeitet mit freien Trägern der Jugendhilfe zusammen. Hier wird es unangenehm, und zwar aus einem guten Grund: In diesem Umfeld sind Sozialdaten im Spiel, teilweise mit besonderem Schutzniveau. Die Frage lautet nicht, wie man den Träger schnell in den Kanal bekommt, sondern welche Informationen überhaupt geteilt werden dürfen und in welcher Granularität.

Die Praxislösung war eine strikte Zweiteilung: eine gemeinsame Ebene für Planungsdaten, Belegungsübersichten ohne Personenbezug, Terminabstimmung und Konzepte – und eine getrennte, gastfreie Umgebung für alles Fallbezogene. Technisch abgesichert wurde das über Container-Kennzeichnungen: Teams und Websites, die Fallbezug haben, tragen eine Kennzeichnung, die Gäste in der Gruppe schlicht nicht zulässt und externe Freigabe ausschließt. Das ist wirksamer als jede Schulungsfolie, weil es nicht auf Aufmerksamkeit setzt.

Für kirchliche Träger, die im Sozialbereich häufig die Gegenseite sind, gelten eigene Datenschutzregime; die Besonderheiten haben wir in [Microsoft 365 in Kirche, Diakonie und Caritas: DSG-EKD, KDG und Mitarbeitervertretung](#) zusammengetragen. Für die Frage, wer bei einer solchen Zusammenarbeit datenschutzrechtlich verantwortlich ist und ob eine Auftragsverarbeitung oder eine gemeinsame Verantwortlichkeit vorliegt, gehört Ihre oder Ihre kirchliche Datenschutzaufsicht an den Tisch – das ist keine Frage der Tenant-Konfiguration.

Das Ratsmitglied mit privatem Tablet

Der schwierigste Fall ist nicht der professionellste, sondern der ehrenamtliche. Gremienmitglieder sind keine Beschäftigten. Sie haben in der Regel kein Dienstgerät, keine dienstliche Identität und keinen Vorgesetzten, der eine Regelung durchsetzt. Sie haben ein privates Tablet, ein privates Postfach und die berechtigte Erwartung, dass die Sitzungsunterlagen funktionieren.

In den meisten Ländern gibt es dafür ein Ratsinformationssystem, und in den meisten Verwaltungen ist genau das der richtige Ort für Sitzungsunterlagen. Microsoft 365 sollte hier nicht das Ratsinformationssystem ersetzen, sondern die Fälle abdecken, die es nicht abbildet: die Arbeitsgruppe zur Haushaltskonsolidierung, den Arbeitskreis zur Schulentwicklung, den nicht-öffentlichen Abstimmungsstrang zu einer Beschlussvorlage in Vorbereitung.

Wenn Sie Gremienmitglieder in Teams einbinden, gilt: Gastkonto, eigenes Team, Multifaktor-Anmeldung ohne Ausnahme, Zugriff nur über Browser oder verwaltete App mit unterbundenem lokalem Herunterladen, Ablaufdatum am Ende der Wahlperiode – und ein Onboarding, das nicht aus einer PDF-Anleitung besteht. Die Erfahrung aus Landschaftsverbänden und großen Kreisen: Der technische Aufwand ist klein, der kommunikative ist erheblich. Wer hier spart, produziert Screenshots von Sitzungsunterlagen in privaten Nachrichtengruppen.

Wenn Sie Onboarding und Begleitung nicht nebenbei stemmen können, ist eine strukturierte [Microsoft-365-Schulung für Verwaltungen](#) für die Gremienbetreuung meist billiger als der dritte Anlauf mit einem improvisierten Merkblatt.

WARNUNG · Personalunterlagen im Kanal mit Gästen

Der häufigste ernsthafte Zwischenfall bei externer Zusammenarbeit ist banal: In einem Projektteam mit Gästen liegt eine Datei, die dort nichts zu suchen hat. Eine Anwesenheitsliste mit Krankheitszeiten. Ein Vermerk zu einer Personalmaßnahme. Ein Organigramm-Entwurf mit Namen und Bewertungsvermerken. Eine Vertretungsregelung mit Gesundheitsdaten im Kommentarfeld.

Niemand hat das absichtlich getan. Die Datei wurde in einen Chat gezogen, weil der Chat gerade offen war. Der Kanal war der falsche. Und der Kanal hatte Gäste.

Was daraus folgt: Personalunterlagen gehören in keinen Zusammenarbeitsraum, der Gäste zulässt – auch nicht kurz, auch nicht als Entwurf, auch nicht in der Registerkarte „Dateien“ eines Chats. Technisch heißt das: Container-Kennzeichnung, die Gäste ausschließt, für alle Personalbereiche; Verlustvermeidungsrichtlinien, die auf Personalkennzeichnungen und typische Muster reagieren; und eine Kennzeichnungspflicht für Dokumente aus dem Personalamt.

Organisatorisch heißt es: Ein Team mit Gästen wird bei Einrichtung als solches gekennzeichnet, es hat eine benannte verantwortliche Person, und in der Kanalbeschreibung steht in einem Satz, was dort nicht abgelegt werden darf. Der Personalrat wird das unterstützen – meist ist er der Erste, der diese Frage stellt.

Und wenn es passiert ist: Datei entfernen reicht nicht. Prüfen Sie über das Protokoll, wer in welchem Zeitraum Zugriff hatte und ob heruntergeladen wurde, dokumentieren Sie den Vorgang und binden Sie die oder den Datenschutzbeauftragten ein. Ob eine Meldepflicht besteht, entscheidet sich nach der Datenschutz-Grundverordnung und dem jeweils anwendbaren Landes- oder kirchlichen Recht, nicht nach Bauchgefühl.

Warum ein zu großzügiger Gästekanal spätestens mit Copilot zum Problem wird, haben wir gesondert beschrieben: [Oversharing im Verwaltungs-Tenant: Warum Copilot die Personalakte findet](#). Kurzfassung: Berechtigungen, die jahrelang unauffällig zu weit waren, werden durch eine gute Suchfunktion sichtbar. Das ist kein Copilot-Problem, sondern ein Berechtigungsproblem mit neuem Publikum.

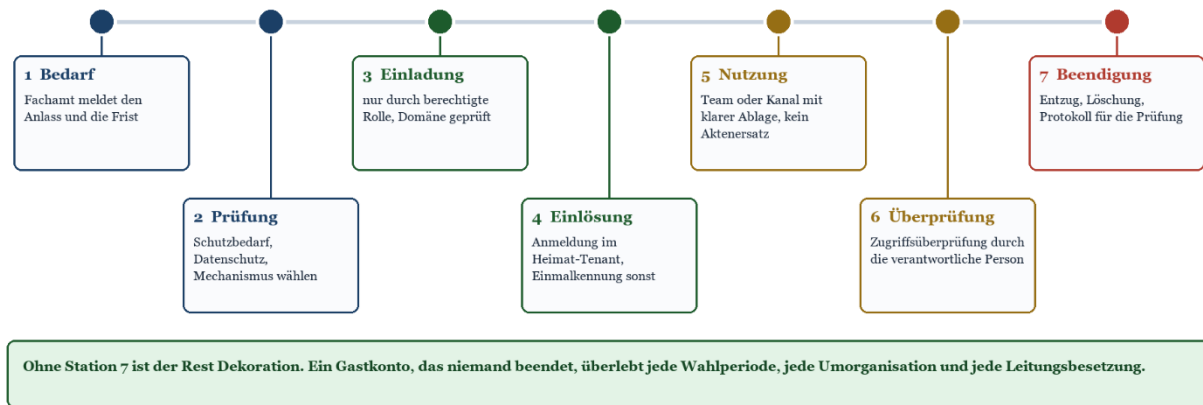
Der Gastlebenszyklus als Verwaltungsvorgang

Jetzt der Teil, der über Erfolg oder Misserfolg entscheidet – und der in fast jedem Konzept fehlt, das wir zur Zweitmeinung auf den Tisch bekommen. Der Lebenszyklus eines Gastzugangs ist kein

IT-Prozess. Er ist ein Vorgang mit Anlass, Zuständigkeit, Frist, Abschluss und Nachweis. Behandeln Sie ihn wie einen solchen, dann funktioniert er auch mit den Mitteln, die eine Verwaltung kennt.

Der Gastlebenszyklus als Verwaltungsvorgang

Sieben Stationen – jede mit einer zuständigen Stelle und einem Nachweis



Skizze 3: Sieben Stationen von der Bedarfsmeldung bis zur dokumentierten Beendigung. Ohne Station sechs und sieben ist der Rest Kosmetik.

Eintritt: Wer darf einladen und wen

Standardmäßig darf in Entra ID jeder Benutzer Gäste einladen – einschließlich der Gäste selbst. Für eine Verwaltung ist das die falsche Ausgangslage. Sie haben vier Stufen zur Auswahl, von „alle einschließlich Gäste“ bis „niemand, auch keine Administratoren“. Der brauchbare Mittelweg für die meisten Häuser ist die dritte Stufe: Nur Personen mit bestimmten Rollen laden ein. Die Rolle „Gasteinladender“ existiert genau dafür und lässt sich vergeben, ohne jemandem Administratorrechte zu geben.

Praktisch heißt das: In jedem Fachamt gibt es ein bis zwei Personen mit dieser Rolle. Sie sind nicht IT, sie sind Fachseite, und sie kennen den Anlass. Das ist auch der Punkt, an dem eine Domänenliste sinnvoll wird: Sie können Einladungen auf bestimmte Domänen beschränken oder einzelne sperren. Eine Positivliste ist in einem Landschaftsverband mit stabilen Partnern realistisch; in einer Kommune mit hundert wechselnden Handwerksbetrieben ist sie Verwaltungsaufwand ohne Sicherheitsgewinn. Dann arbeiten Sie besser mit einer kurzen Sperrliste und strenger Nachverfolgung.

Vergessen Sie die Verzeichnissichtbarkeit nicht. Die Voreinstellung gibt Gästen eingeschränkten Zugriff auf Eigenschaften und Mitgliedschaften von Verzeichnisobjekten; sie können damit die Mitgliedschaft aller nicht ausgeblendeten Gruppen sehen. Die restriktivste Stufe beschränkt einen Gast auf sein eigenes Objekt. Für Verwaltungen ist das in aller Regel die richtige Einstellung: Ein Architekturbüro muss nicht wissen, wer alles im Personalamt in welcher Gruppe ist.

Laufzeit: Ablauf, Sponsor und Zugriffsüberprüfung

Ein Gastzugang ohne Ablaufdatum ist ein Dauerzugang. Sie haben mehrere Hebel, und sie ergänzen sich:

- **Ablauf des Gastzugriffs auf Websiteebene:** In den SharePoint-Freigabeeinstellungen können Sie festlegen, dass der Zugriff eines Gastes auf eine Website oder freigegebene Inhalte nach einer bestimmten Anzahl von Tagen automatisch endet.
- **Ablauf von Links:** „Jeder“-Links lassen sich mit einer erzwungenen Höchstdauer versehen. Wird die Frist verkürzt, ziehen bestehende Links nach; wird sie verlängert, behalten sie ihre alte Frist.
- **Ablauf der Zuweisung im Zugriffspaket:** Die saubere Variante, weil sie den gesamten Bündelzugriff beendet und einen Sponsor benachrichtigt, statt einzelne Berechtigungen zu zerpflücken.
- **Wiederkehrende Zugriffsüberprüfung:** Ein Turnus, in dem eine benannte Person bestätigt, dass ein Zugang noch gebraucht wird. Sie können die Prüfung an die Teambesitzerin oder den Teambesitzer, an das Fachamt oder an die Gäste selbst richten.

Zur Zugriffsüberprüfung noch ein Detail, das man kennen muss: Sie erfasst interne Personen, Gäste und externe Teilnehmer aus freigegebenen Kanälen. Sie erfasst aber nicht ganze Teams, die einem freigegebenen Kanal hinzugefügt wurden. Wenn Sie mit Team-zu-Team-Freigaben arbeiten, muss die Kanalbesitzerin oder der Kanalbesitzer diese Mitgliedschaften in Teams selbst kontrollieren. Das gehört in die Handreichung, sonst entsteht eine Prüflücke, die niemandem auffällt – bis sie auffällt.

Konstellation	Turnus der Überprüfung	Wer bestätigt	Nachweis
Projektteam mit Planungsbüro	vierteljährlich, zusätzlich zum Projektmeilenstein	Projektleitung im Fachamt	Protokoll der Überprüfung, Vermerk in der Projektakte
Freier Träger, dauerhafte Kooperation	halbjährlich	Amtsleitung oder benannte Fachkraft	Überprüfungsbericht, Abgleich mit dem Kooperationsvertrag
Gremienmitglieder	einmal jährlich, verpflichtend zum Ende der Wahlperiode	Gremienbetreuung, Hauptamt	Liste der Zugänge mit Beendigungsdatum
Freigegebener Kanal mit Partnerbehörde	halbjährlich, plus Prüfung der mandantenübergreifenden Einstellungen	IT-Leitung gemeinsam mit dem Fachamt	Auszug der Partnerkonfiguration, Kanalmitgliederliste
Externe im Bereich mit hohem Schutzbedarf	monatlich oder gar kein Gastzugang	Fachamt und Datenschutzbeauftragte	Vollständige Nachweiskette, Vorlage beim Rechnungsprüfungsamt

Tabelle 2: Ein Turnusmodell, das sich am Schutzbedarf orientiert und nicht am Kalender der IT. Die Turnusangaben sind Erfahrungswerte, keine Rechtsvorgabe.

Austritt: Beenden, löschen, nachweisen

Das Ende eines Gastzugangs hat drei Ebenen, die regelmäßig verwechselt werden. Erstens die Mitgliedschaft: Die Person wird aus dem Team, dem Kanal oder der Website entfernt. Zweitens das Konto: Das Gastobjekt wird im Verzeichnis gelöscht. Drittens der Nachweis: Es wird dokumentiert, dass beides geschehen ist, mit Datum und veranlassender Stelle.

Nur die dritte Ebene interessiert das Rechnungsprüfungsamt, und nur die erste erledigt sich manchmal von selbst. Bei der zweiten kommt eine unangenehme Eigenschaft dazu: Wenn Sie die externe Freigabe abschalten und später wieder einschalten, erhalten Gäste ihren Zugriff zurück.

Der Zugriff verschwindet nach einer Abschaltung typischerweise binnen einer Stunde – aber er ist nicht gelöscht, er ist stillgelegt. Wer einen sauberen Schnitt braucht, muss die Berechtigungen und die Konten entfernen, nicht nur den Hauptschalter umlegen.

Was an Protokolldaten verfügbar ist und wie Sie daraus einen prüffesten Nachweis machen, steht in [Microsoft 365 Audit-Log und Rechnungsprüfung: Nachweise, die Verwaltungen liefern müssen](#). Wichtig für freigegebene Kanäle: Die Prüfergebnisse zum Kanal – Anlegen, Löschen, Mitglieder hinzufügen und entfernen – entstehen im Mandanten, der den Kanal beherbergt. Im Heimatmandanten der externen Person gibt es keine Protokolleinträge über deren Aktivität in Ihrem Kanal. Wenn Sie Nachweise brauchen, müssen Sie den Kanal also selbst hosten.

WICHTIG · Zwei Zahlen, die Ihre Erwartung sortieren

Bis zu zwölf Stunden, bis ein neu hinzugefügter Gast vollen Zugriff auf ein Team hat. Planen Sie das ein, statt in der Zwischenzeit Ersatzwege zu bauen.

Bis zu zwei Stunden, bis Änderungen an den mandantenübergreifenden Zugriffseinstellungen für freigegebene Kanäle wirken. Legen Sie den Termin mit der Partnerbehörde nicht auf denselben Vormittag.

Das Regelwerk: Was Sie einmal einstellen und dann prüfen

Die technische Konfiguration ist überschaubar, wenn man sie als Schichtenmodell denkt. Sechs Kontrollpunkte greifen nacheinander, und die restriktivste Einstellung gewinnt. Das ist eine gute Nachricht: Sie können konservativ starten und gezielt öffnen, statt großzügig zu starten und hinterher zu suchen.

Sechs Kontrollpunkte, die nacheinander greifen

Der Zugriff eines Gastes muss jede Schicht passieren – die restriktivste gewinnt

1 Entra: Externe Zusammenarbeit

Wer darf einladen, welche Domänen sind erlaubt, was sieht ein Gast im Verzeichnis

2 Entra: Mandantenübergreifende Einstellungen

Ein- und ausgehende Freigabe je Partnerorganisation, Vertrauen in fremde Mehrfaktor-Nachweise

3 Bedingter Zugriff

Mehrfaktor-Pflicht für Gäste, Gerätezustand, Standort, Sitzungssteuerung im Browser

4 Container-Kennzeichnung

Erlaubt dieses Team überhaupt Gäste, ist die Website privat, ist Freigabe zulässig

5 SharePoint: Freigabestufe

Vier Stufen im Tenant, je Website gleich oder strenger, Ablauf für Links und Gastzugriff

6 Purview und Protokoll

Vertraulichkeit, Verlustvermeidung, Aufbewahrung, Prüfprotokoll für das Rechnungsprüfungsamt

Was oft fehlt

Schicht 3 und Schicht 4. Viele Verwaltungen konfigurieren Entra sauber und SharePoint streng, lassen den bedingten Zugriff aber ohne Regel für Gäste und vergeben keine Kennzeichnung auf Teams. Ergebnis: Ein Gastkonto ohne zweiten Faktor auf einem unbekannten Privatgerät in einem Team, das nie für Gäste gedacht war.

Skizze 4: Sechs Schichten, die ein externer Zugriff nacheinander passieren muss. In der Praxis fehlen meist die Schichten drei und vier.

Die Grundkonfiguration, die wir empfehlen

Die folgende Tabelle ist unser Ausgangspunkt in Konzeptionsworkshops. Sie ist bewusst restriktiv – jede Abweichung nach oben soll begründet und dokumentiert werden, nicht umgekehrt.

Einstellung	Empfehlung für Verwaltungen	Begründung
Wer darf Gäste einladen	Nur Personen mit der Rolle „Gasteinladender“ oder Benutzerverwaltung	Fachliche Nähe zum Anlass ohne Administratorrechte; erzeugt eine namentliche Zuständigkeit.
Verzechnissichtbarkeit für Gäste	Restriktivste Stufe: Zugriff nur auf eigene Objekte	Externe brauchen keine Übersicht über Ihre Gruppen und Mitgliedschaften.
Entra-B2B-Integration in SharePoint	Aktiviert	Sonst laufen Dateifreigaben an Einladungsregeln und Domänenlisten vorbei.
SharePoint-Freigabestufe Tenant	„Neue und vorhandene Gäste“, „Jeder“ abgeschaltet	Authentifizierung bleibt Pflicht; anonyme Links entfallen als Fehlerquelle.
Standard-Linktyp	„Bestimmte Personen“	Verhindert die versehentlich weitergeleitete Berechtigung im Alltag.
Ablauf des Gastzugriffs auf Websiteebene	Aktiviert, Frist am Anwendungsfall orientiert	Setzt eine harte Grenze auch dort, wo der organisatorische Prozess versagt.
Gäste dürfen Fremdinhalte weitergeben	Deaktiviert	Ein Gast soll Ihre Inhalte nutzen, nicht weiterverteilen.
B2B Direct Connect	Standard bleibt blockiert, Freigabe nur je Partnerorganisation	Vertrauen in eine fremde Organisation ist eine bewusste Entscheidung, kein Voreinstellungsergebnis.
Eingehendes Vertrauen in fremde Mehrfaktor-Nachweise	Nur für geprüfte Partnerbehörden	Ohne Vertrauensstellung blockiert Ihre Richtlinie sonst legitime Zugriffe.
Bedingter Zugriff für Gäste	Mehrfaktor-Pflicht, Sitzungssteuerung im Browser, kein Herunterladen auf unverwalteten Geräten	Deckt genau den Fall des privaten Tablets ab, der sich sonst nicht regeln lässt.
Container-Kennzeichnung	Für Personal-, Sozial- und Sicherheitsbereiche verpflichtend, ohne Gastzulassung	Wirkt beim Anlegen, nicht erst bei der Kontrolle.
Externe dürfen die Organisation selbst verlassen	Aktiviert, sobald der Datenschutzkontakt hinterlegt ist	Reduziert Karteileichen; die Einstellung ist ohne hinterlegte Datenschutzinformationen gar nicht verfügbar.

Tabelle 3: Ausgangskonfiguration für externe Zusammenarbeit. Jede Abweichung nach oben braucht einen dokumentierten Anlass.

Der Sonderfall der unverwalteten Geräte

Das Gremienmitglied mit dem privaten Tablet ist kein Randfall, sondern der Regelfall der ehrenamtlichen Mitarbeit. Sie werden dieses Gerät nicht verwalten, und Sie sollten es auch nicht versuchen – niemand übergibt sein privates Tablet der Kreisverwaltung. Was bleibt, ist die

Sitzungssteuerung: Zugriff im Browser mit eingeschränkter Sitzung, kein lokales Herunterladen, kein Drucken, kein Ausschneiden und Einfügen aus geschützten Anwendungen heraus.

Das ist unbequem, und es wird Beschwerden geben. Die Alternative sind Sitzungsunterlagen im privaten Download-Ordner eines Geräts, das die Verwaltung nie gesehen hat. Wo die Grenzen des bedingten Zugriffs liegen und welche Ausnahmen sich rechtfertigen lassen, haben wir im Detail beschrieben; im Zusammenspiel mit privilegierten Konten lohnt zusätzlich ein Blick auf [Privilegierte Konten in der Verwaltungs-IT: Rollen, PIM und der Fall des einen Admins](#) – denn die Rolle „Gasteinladender“ ist zwar harmlos, die Rollen daneben sind es nicht.

Was der Schutzbedarf dazu sagt

Externe Zugriffe sind in der Schutzbedarfsbetrachtung ein eigener Punkt und gehören nicht in eine Fußnote. Die Frage ist nicht, ob Microsoft 365 externe Zusammenarbeit sicher kann – die Frage ist, welche Informationen mit welchem Schutzbedarf Sie überhaupt in einen Raum legen, in dem Personen außerhalb Ihrer Organisationshoheit lesen. Den systematischen Abgleich haben wir in [Schutzbedarf und Microsoft 365: IT-Grundschutz-Abgleich für die Praxis](#) aufbereitet.

Für Verfahren mit hohem Schutzbedarf ist die ehrliche Antwort oft: kein Gastzugang. Nicht, weil es technisch nicht ginge, sondern weil der organisatorische Aufwand für die belastbare Kontrolle den Nutzen übersteigt. Diese Entscheidung darf man treffen. Sie muss nur dokumentiert und mit einer Alternative versehen sein, sonst wird sie unterlaufen.

Personalrat, Datenschutz und die Grenze zur Akte

Was in eine Dienstvereinbarung gehört – und was nicht

Externe Zusammenarbeit ist selten der Kern einer Dienstvereinbarung, aber sie berührt zwei Punkte, die den Personalrat zu Recht interessieren. Erstens: In Räumen mit Gästen wird die Arbeit von Beschäftigten für Externe sichtbar – wer wann welche Datei bearbeitet hat, wer im Kanal aktiv ist, wer auf eine Frage nicht antwortet. Zweitens: Protokolldaten über Gastzugriffe enthalten unvermeidlich auch Daten über interne Personen, die mit ihnen zusammenarbeiten.

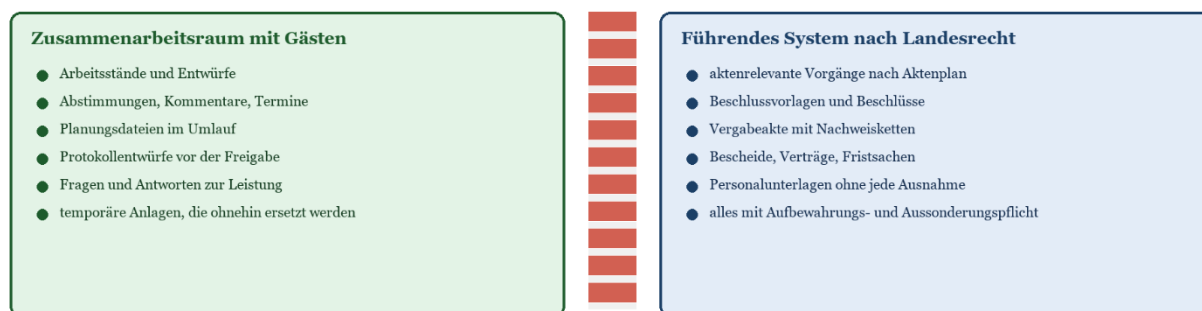
Beides lässt sich regeln, wenn man es benennt: Zweckbindung der Protokolldaten, Ausschluss der Verhaltens- und Leistungskontrolle, Verfahren bei Verdachtsfällen, Beteiligung bei der Einführung neuer Freigabemechanismen. Bausteine dafür haben wir in [Copilot und Personalrat: Bausteine einer Dienstvereinbarung](#) zusammengestellt; die Systematik trägt auch für den Gastzugang. Was nicht in eine Dienstvereinbarung gehört, sind technische Konfigurationswerte. Eine Vereinbarung, die eine konkrete Freigabestufe festschreibt, ist nach dem nächsten Funktionsupdate entweder falsch oder blockierend.

Die Grenze zur E-Akte: klar ziehen, einmal, schriftlich

Hier kommt der Punkt, an dem viele Konzepte weich werden. Ein Teams-Kanal mit Gästen ist ein Raum für die laufende Zusammenarbeit. Er ist kein System der Schriftgutverwaltung, und er ist in aller Regel keine E-Akte im Sinne der E-Government-Gesetze der Länder. Ob und ab wann Sie zur elektronischen Aktenführung verpflichtet sind, welches System dafür führend ist und welche Anforderungen an Aktenplan, Vollständigkeit, Integrität und Aussonderung gelten, richtet sich nach dem jeweiligen Landesrecht und Ihrer Aktenordnung.

Die Grenzlinie: Gästekanal ist kein Aktenersatz

Was in der Zusammenarbeit entstehen darf und was in die führende Akte gehört



Übergabe erfolgt bewusst, dokumentiert und einmal – nicht durch Zufall

Wer die Linie nicht zieht, führt am Ende zwei Akten. Eine davon kennt die Registratur nicht.

Skizze 5: Links der Zusammenarbeitsraum mit Gästen, rechts das führende System nach Landesrecht. Die Übergabe muss ein bewusster Schritt sein.

Praktisch bedeutet das: Der aktenrelevante Stand wird an einer definierten Stelle in das führende System übernommen – als Vorgang mit Aktenzeichen, nicht als Sammlung von Dateiversionen. Wann SharePoint dafür überhaupt in Frage kommt und wo die Grenze verläuft, haben wir in [SharePoint als E-Akte? Was geht, was nicht und wo die Grenze nach Landesrecht liegt](#) ausführlich behandelt. Die Übersetzung vom Aktenplan in Aufbewahrungsbezeichnungen steht in [Schriftgutverwaltung mit Microsoft 365: Vom Aktenplan zur Aufbewahrungsbezeichnung](#), die Mechanik von Fristen, Disposition und Vernichtungsnachweis in [Aufbewahrung und Aussonderung mit Purview: Fristen, Disposition, Vernichtungsnachweis](#).

Für den Gastzugang folgt daraus eine sehr konkrete Regel: Bevor Sie einen Projektraum mit Externen schließen, wird geklärt, was aktenrelevant ist und wohin es gehört. Sonst löschen Sie entweder zu früh – und verlieren Schriftgut, das aufbewahrungspflichtig war – oder Sie löschen nie, und der Raum wird zur Schattenakte, die bei der nächsten Auskunftsanfrage niemand kennt.

Auftragsverarbeitung, Verantwortlichkeit, Zuständigkeit

Wenn ein freier Träger, ein Planungsbüro oder ein Zweckverband in Ihrem Tenant arbeitet, verarbeitet er Daten in einem System, für das Sie verantwortlich sind. Ob daraus eine Auftragsverarbeitung, eine gemeinsame Verantwortlichkeit oder eine getrennte Verantwortlichkeit wird, hängt vom Einzelfall ab und ist keine Frage, die eine Konfigurationstabelle beantwortet. Klären Sie es vorab mit der oder dem Datenschutzbeauftragten und halten Sie das Ergebnis in der Kooperationsvereinbarung fest – nicht in einer E-Mail an die IT.

Was Sie technisch beitragen können, ist Nachvollziehbarkeit: wer wann berechtigt war, worauf, durch wen veranlasst und wie lange. Diese vier Angaben decken die meisten Rückfragen ab, die aus Datenschutzprüfungen und aus dem Rechnungsprüfungsamt kommen.

TIPP · Die Zusammenarbeit mit dem kommunalen Rechenzentrum

Viele Kommunen betreiben Microsoft 365 nicht allein, sondern gemeinsam mit ihrem kommunalen Rechenzentrum oder einem Systemhaus. Für den Gastzugang lohnt sich eine ausdrückliche Rollenklärung: Wer stellt die Tenant-Grundeinstellungen ein, wer vergibt die Rolle „Gasteinladender“, wer führt die Zugriffsüberprüfungen durch, und wer liefert die Nachweise, wenn die Prüfung anklopft.

Diese Zuordnung gehört in die Leistungsbeschreibung, nicht in die mündliche Absprache. [Microsoft](#)

[365 und das kommunale Rechenzentrum: Rollen, Schnittstellen, Zweitmeinung](#) geht die typischen Schnittstellen durch.

Häufige Fragen zum Teams-Gastzugang in der Verwaltung

Brauchen Gäste eine eigene Microsoft-365-Lizenz?

Nein. Der Gastzugang lässt sich mit den gängigen Microsoft-365-Abonnements für Unternehmen, Enterprise und Bildung nutzen, ohne dass für die externe Person eine zusätzliche Microsoft-365-Lizenz erworben werden muss. Für Gäste gilt das Abrechnungsmodell von Entra External ID. Beachten Sie aber, dass Funktionen der Identitätsgovernance – Zugriffspakete, wiederkehrende Zugriffsüberprüfungen – an eine eigene Ausstattung gebunden sind. Genau diese Funktionen sind es, die den Lebenszyklus tragen. Rechnen Sie das im Konzept mit, statt es später zu entdecken.

Kann ein Gast in einem freigegebenen Kanal mitarbeiten?

Nein. Gäste im Sinne der B2B-Zusammenarbeit können freigegebene Kanäle weder sehen noch nutzen. Umgekehrt haben externe Teilnehmer aus freigegebenen Kanälen keinen Zugriff auf das übrige Team und keine Berechtigungen aus Dateifreigabelinks. Die beiden Mechanismen sind Alternativen, keine Ergänzung im selben Kanal. Wenn Sie in einem Vorhaben beide Partnerarten haben, brauchen Sie zwei Konstruktionen – und eine klare Ansage, welche Information wo liegt.

Wie verhindern wir, dass Gäste in Bestandsteams landen?

Über Container-Kennzeichnungen. Eine Sensitivitätskennzeichnung auf der Gruppe legt fest, ob Gäste überhaupt Mitglied werden dürfen, ob die Website privat ist und ob externe Freigabe zulässig ist. Vergeben Sie diese Kennzeichnungen beim Anlegen, nicht im Nachgang. Ergänzend hilft eine Namenskonvention, die Teams mit externer Beteiligung erkennbar macht – das ist keine Sicherheitsmaßnahme, aber es senkt die Fehlerquote im Alltag erheblich.

Was ist der Unterschied zwischen Gastzugang und externem Zugriff?

Der externe Zugriff, oft auch Verbund genannt, erlaubt Chat, Anruf und Besprechung mit Personen aus anderen Organisationen. Er gibt keinen Zugriff auf Teams, Kanäle oder Dateien. Der Gastzugang dagegen bindet eine externe Person in Ihre Zusammenarbeitsräume ein. Beide Schalter sind unabhängig voneinander. Der häufigste Irrtum in Verwaltungen: Man aktiviert den externen Zugriff, hält damit die Zusammenarbeit für geregelt und wundert sich, warum weiter Dateien per Mail verschickt werden.

Sollen wir Gäste über eine Positivliste von Domänen steuern?

Das hängt von Ihrer Partnerstruktur ab. Eine Positivliste ist sinnvoll, wenn Sie mit wenigen, stabilen Partnern arbeiten – etwa ein Zweckverband mit fünf Mitgliedskommunen oder ein Landschaftsverband mit festen Trägern. Bei wechselnden Auftragnehmern erzeugt sie einen Pflegeaufwand, der irgendwann durch Ausnahmen unterlaufen wird. Dann ist eine kurze Sperrliste plus konsequenter Lebenszyklus wirksamer. Die Domänenbeschränkung existiert auf beiden Ebenen: in Entra für Einladungen und in SharePoint für Freigaben. Konfigurieren Sie beide konsistent, sonst suchen Sie Fehler an der falschen Stelle.

Wir betreiben ADFS. Ändert das etwas am Gastzugang?

Für den Gast selbst nicht – er authentifiziert sich bei seinem eigenen Identitätsanbieter. Für Ihre Steuerung schon: Richtlinien für bedingten Zugriff entfalten ihre Wirkung dort, wo Entra ID die Anmeldung verantwortet. Wenn Ihre internen Anmeldungen noch über einen Verbunddienst laufen, prüfen Sie, ob Ihre Gastregeln greifen wie gedacht. Die Entscheidungslinien entlang der Fachverfahren haben wir in [ADFS oder Entra ID in der Verwaltung: Die Entscheidung entlang der Fachverfahren](#) beschrieben.

Was bedeutet Delos Cloud für die externe Zusammenarbeit?

Delos Cloud ist ein für die öffentliche Verwaltung in Deutschland vorgesehenes Angebot, das Microsoft-Dienste in einer souverän betriebenen Umgebung bereitstellen soll. Für die Frage des Gastzugangs ist der nüchterne Stand: Funktionsumfang, Verfügbarkeit einzelner Dienste und die Möglichkeiten mandantenübergreifender Zusammenarbeit sind gesondert zu prüfen und lassen sich nicht pauschal aus dem öffentlichen Angebot ableiten. Wir empfehlen, das Zielbild für externe Zusammenarbeit unabhängig vom Betriebsmodell zu beschreiben und die Umsetzungsvarianten daran zu messen. Eine Einordnung des Angebots finden Sie in [Delos Cloud für Kommunen: Was das Angebot ist, wen es betrifft und was fehlt](#), die Betriebsmodellfrage in [Standard-Tenant oder Hybrid: Die Betriebsmodell-Entscheidung für Verwaltungen](#).

Wie oft sollten Zugriffsüberprüfungen laufen?

So oft, wie es der Schutzbedarf verlangt, und so selten, dass die prüfende Person sie noch ernst nimmt. Eine monatliche Überprüfung für unkritische Projekträume erzeugt Klickroutine ohne Erkenntnis. Ein Jahresrhythmus für einen Bereich mit Sozialdaten ist zu lang. Tabelle 2 in diesem Beitrag ist unser Ausgangsraster; passen Sie es an Ihre Schutzbedarfsfeststellung an und halten Sie die Begründung fest – das ist genau die Art von Nachweis, die eine Prüfung sehen will.

Was passiert mit den Inhalten, wenn ein Gastkonto gelöscht wird?

Die Inhalte bleiben. Dateien, die eine externe Person in einer Bibliothek hochgeladen hat, gehören der Website, nicht der Person. Beiträge in Kanälen bleiben erhalten, die Urheberangabe wird nach der Löschung des Kontos weniger aussagekräftig dargestellt. Das ist aus Sicht der Schriftgutverwaltung erwünscht – es ist aber ein Argument dafür, die Übergabe aktenrelevanter Stände vor der Beendigung zu erledigen und nicht danach.

Wer entscheidet in der Verwaltung eigentlich über die Gästeregeln?

Idealerweise nicht die IT allein. Die Grundsatzentscheidung – welche Mechanismen zugelassen sind, welche Bereiche gastfrei bleiben, wer einladen darf – ist eine Organisationsentscheidung mit Beteiligung von Organisationsamt, Datenschutz, Personalrat und Verwaltungsspitze, und sie gehört in vielen Häusern in eine Beschlussvorlage oder eine Dienstanweisung. Die IT liefert die Optionen und die Folgen, nicht die Entscheidung. Wie sich das in einer kompakten Konzeptionsphase bündeln lässt, beschreibt [Microsoft-365-Einführung in der Verwaltung: Konzeptionsphase in 4,5 Tagen und die Beschlussvorlage](#).

Fazit

Externe Zusammenarbeit ist in Microsoft 365 kein technisches Problem. Die vier Mechanismen sind vorhanden, sie sind steuerbar, und sie sind für Verwaltungen tauglich – wenn man sie unterscheidet und nicht alles „Gast“ nennt. Der freigegebene Kanal ist die eleganteste Lösung mit Partnern, die selbst Entra ID nutzen. Das Gastkonto bleibt der Arbeitspferd-Mechanismus für alles

andere. Der Freigabelink ist für das einzelne Dokument da und nicht für Projekte. Und das Zugriffspaket ist die einzige Variante, die den Lebenszyklus von sich aus mitbringt.

Das eigentliche Problem liegt woanders. Es liegt in dem Gastkonto ohne Ablaufdatum, in dem Projektteam, das niemandem gehört, in der Personaldatei, die versehentlich im falschen Kanal gelandet ist, und in der Frage, die niemand beantworten kann: Wer war eigentlich zuständig? Wenn Sie externe Zugänge wie Verwaltungsvorgänge behandeln – mit Anlass, Zuständigkeit, Frist, Abschluss und Nachweis –, dann ist die Technik der einfache Teil.

Fangen Sie klein an: eine Liste aller heute bestehenden Gastkonten, eine Spalte „wer braucht das noch“, eine Frist. Die Erfahrung sagt, dass in dieser Liste bei einer mittleren Stadtverwaltung ein Drittel der Einträge niemandem mehr zuzuordnen ist. Das ist kein Grund für schlechte Laune, sondern der beste denkbare Anlass für eine Regelung. Die zweite Bereinigung fällt deutlich kleiner aus – vorausgesetzt, es gibt inzwischen einen Prozess, der die dritte überflüssig macht.

Wenn Sie diesen Prozess nicht auf der grünen Wiese entwerfen wollen, sondern an einer gewachsenen Landschaft mit Fachämtern, Vergabestelle, Kämmerei und Registratur ansetzen: Genau dafür gibt es die [Microsoft-365-Beratung für Verwaltungen](#). Zweitmeinung inklusive, auch gegenüber dem eigenen Konzept.

WEITER IM THEMA · Passend zu diesem Thema

- › [Microsoft Teams in der Verwaltung einführen: Informationsarchitektur entlang der Ämter](#)
- › [Conditional Access für Verwaltungen: Regelwerk für Rathaus, Bauhof und Homeoffice](#)
- › [Oversharing im Verwaltungs-Tenant: Warum Copilot die Personalakte findet](#)
- › [SharePoint als E-Akte? Was geht, was nicht und wo die Grenze nach Landesrecht liegt](#)
- › [Microsoft 365 Audit-Log und Rechnungsprüfung: Nachweise, die Verwaltungen liefern müssen](#)
- › [Microsoft 365 in der Kommune: Was Sie wirklich entscheiden müssen \(und was nicht\)](#)