

Entra ID für kirchliche Träger: Identitäten zwischen Landeskirche, Verband, Träger und Einrichtung

Es gibt einen Moment in jedem Einführungsprojekt, in dem die Stimmung kippt. Man sitzt im Besprechungsraum eines Landeskirchenamts oder eines Generalvikariats, auf dem Tisch liegen Zeitplan und Lizenzangebot, alle sind guter Dinge — und dann fragt jemand harmlos: „Woher kommen eigentlich die Konten?“ Danach redet zwei Stunden lang niemand mehr über Teams.

Der Grund ist, dass diese Frage in kirchlichen Strukturen keine technische ist. In einem Industrieunternehmen gibt es ein Personalsystem, ein Active Directory, eine Wahrheit. In einer Landeskirche gibt es das zentrale Verzeichnis des Landeskirchenamts, daneben das gewachsene Verzeichnis des diakonischen Werks, daneben die Personalabrechnung des Krankenhausverbunds, daneben ein Kirchenkreis, der vor acht Jahren „mal eben schnell“ einen eigenen Tenant aufgemacht hat, und daneben zweitausend Ehrenamtliche, die in keinem einzigen dieser Systeme stehen und trotzdem den Gemeindebrief setzen, die Kollekte zählen und im Presbyterium über Bauvorhaben abstimmen. Jede dieser Quellen hat eine eigene Rechtsperson dahinter, einen eigenen Haushalt, ein eigenes Leitungsorgan und häufig eine eigene Meinung dazu, wer ihre Leute verwalten darf.

Dieser Beitrag gehört zur Serie [Microsoft 365 in Kirche, Diakonie und Caritas](#). Dort findest du die Übersicht von Datenschutz über Lizenzierung bis Telefonie. Hier geht es um die Schicht darunter: das Identitätsmodell. Wer es einmal sauber aufsetzt, spart sich Jahre. Wer es nicht tut, merkt es spätestens dann, wenn die örtlich Beauftragte für den Datenschutz fragt, warum eine Kollegin, die vor vierzehn Monaten in Rente gegangen ist, noch immer Zugriff auf das Laufwerk der Beratungsstelle hat.

Vorab eine Abgrenzung, damit wir uns nicht verfransen: Der Zuschnitt der Mandantengrenze — ein Tenant für alle oder viele kleine — ist eine eigene Entscheidung mit eigener Logik. Sie ist die Voraussetzung für alles, was hier folgt.

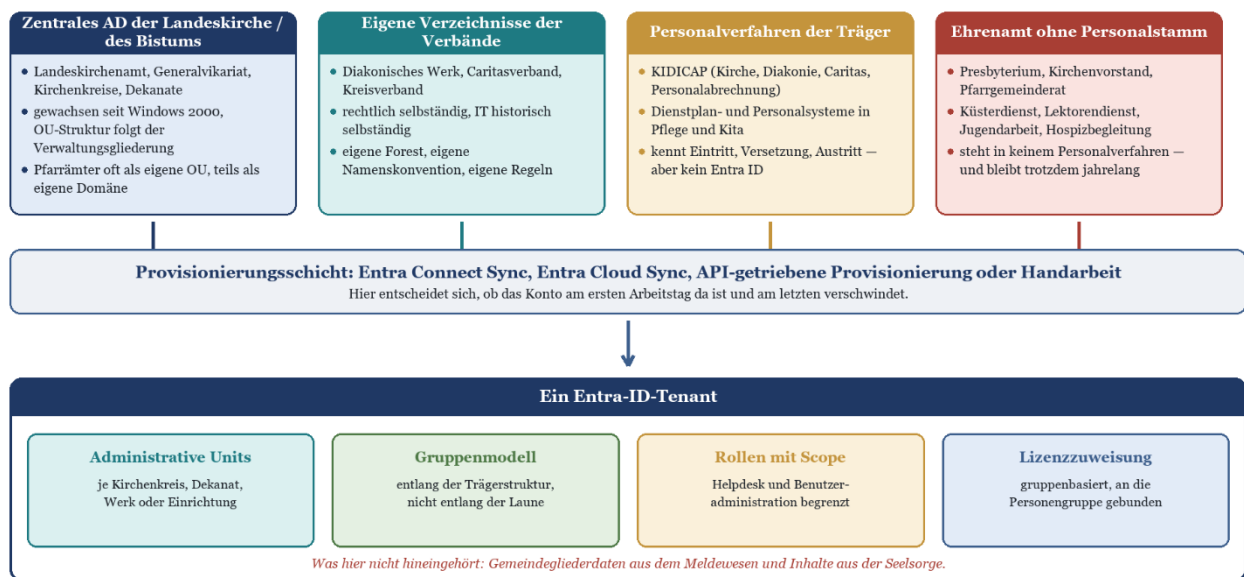
Wenn diese Frage bei dir noch offen ist, fang dort an: [Ein Tenant oder viele? Kirchengemeinde, Kirchenkreis, Landeskirche, Bistum und die Frage der Tenant-Architektur](#). Dieser Beitrag setzt voraus, dass die Entscheidung gefallen ist, und beantwortet die nächste: Wie kommen die Menschen hinein — und wie kommen sie wieder heraus?

Woher die Identitäten kommen: die Landschaft bei kirchlichen Trägern

Bevor man über Entra Connect, Cloud Sync oder Lifecycle Workflows redet, muss man eine unspektakuläre Vorarbeit leisten: aufschreiben, welche Personengruppen es überhaupt gibt und wo deren Stammdaten heute liegen. Das klingt nach einer Nachmittagsaufgabe. In der Praxis ist es der Punkt, an dem die meisten Projekte zum ersten Mal ehrlich werden.

Woher die Identitäten kommen

Vier Quellen, ein Tenant — und keine davon ist von Haus aus für Microsoft 365 gebaut



Skizze 1: Identitätsquellen kirchlicher Träger und ihr Weg in einen gemeinsamen Tenant.

Skizze 1: Identitätsquellen kirchlicher Träger und ihr Weg in einen gemeinsamen Tenant.

Das zentrale Verzeichnis der Landeskirche oder des Bistums

In fast jeder Landeskirche und in fast jedem Bistum gibt es ein Active Directory, das irgendwann um die Jahrtausendwende entstanden ist und dessen OU-Struktur die Verwaltungsgliederung abbildet: oben das Landeskirchenamt beziehungsweise das Generalvikariat, darunter Kirchenkreise oder Dekanate, darunter Pfarrämter. Manchmal sauber, häufiger als Archäologie mehrerer Reorganisationen, bei denen die alten Organisationseinheiten nie gelöscht wurden, weil ja „vielleicht noch etwas darin hängt“.

Dieses Verzeichnis ist der naheliegende Ausgangspunkt, und in den meisten Projekten wird es das auch. Aber es hat eine Eigenschaft, die man kennen sollte: Es kennt nur die Menschen, für die irgendwann jemand ein Windows-Konto gebraucht hat. Die Küsterin, die Reinigungskraft, die Erzieherin im Springerdienst, der Krankenhausseelsorger im Nebenamt — die stehen oft nicht darin. Sie stehen im Personalverfahren, aber nicht im Verzeichnis. Und sie sind die Gruppe, die sich am lautesten meldet, sobald Teams eingeführt wird.

Die eigenen Verzeichnisse der Verbände

Diakonische Werke und Caritasverbände sind rechtlich selbständig, und ihre IT ist es historisch ebenfalls. Ein Kreisverband der Caritas mit Sozialstation, Kita-Trägerschaft und Schuldnerberatung hat in aller Regel eine eigene Domäne, eine eigene Namenskonvention und einen eigenen Dienstleister. Wenn dieser Verband und die verfasste Kirche in einen gemeinsamen Tenant gehen, treffen zwei Verzeichnisse aufeinander, die nie füreinander gebaut wurden.

Der klassische Konflikt heißt UPN-Suffix. Die Landeskirche hätte gern alle unter einer Domäne, weil das in der Adressliste hübscher aussieht. Der Verband besteht auf seiner eigenen, weil seine Klientinnen und Klienten ihn unter dieser Adresse kennen und weil er nicht als Abteilung der Landeskirche wahrgenommen werden will. Beide haben recht. Technisch ist die Sache trivial — ein

Tenant verträgt viele verifizierte Domänen —, politisch kann sie ein Projekt um Monate verzögern. Klär das früh und schriftlich.

Die Personalverfahren der Träger

Hier liegt die eigentliche Wahrheit über Eintritt, Versetzung und Austritt. In Kirche, Diakonie und Caritas ist das häufig KIDICAP — ein Kunstwort aus Kirche, Diakonie, Caritas und Personalabrechnungssystem, entstanden Mitte der Neunziger genau für dieses Umfeld und heute bei Landeskirchen, Bistümern, Krankenhausverbünden und großen sozialen Trägern im Einsatz. Daneben stehen Dienstplan- und Personalsysteme aus der Pflege, eigene Lösungen in der Kita-Verwaltung und, in größeren Häusern, klassische HR-Suiten.

Diese Systeme wissen, dass jemand zum Ersten des Monats anfängt und zum Letzten des Jahres aufhört. Sie wissen nur nichts von Entra ID, und Entra ID weiß nichts von ihnen. Die Brücke dazwischen ist entweder ein Provisionierungsverfahren oder ein Mensch mit einer Excel-Liste. Es gibt kein Drittes. Microsoft bietet für die Brücke zwei ernstzunehmende Wege an: die vorkonfigurierte Anbindung an eine HR-Anwendung und die API-getriebene Provisionierung, bei der das Personalverfahren Datensätze per Schnittstelle einliefert. Beide setzen mindestens Entra ID P1 voraus. Beide brauchen jemanden, der auf der Personalseite zuständig ist — und das ist regelmäßig die härtere Anforderung.

Das Ehrenamt, das in keinem Personalstamm steht

Und dann sind da die, um die es in der Kirche eigentlich geht. Das Presbyterium, der Kirchenvorstand, der Pfarrgemeinderat, die Kirchenverwaltung, der Lektorendienst, die Hospizbegleitung, die Konfi-Teamerinnen und -Teamer. Menschen mit Zugriffsbedarf, Verantwortung und oft jahrzehntelanger Bindung an die Einrichtung — aber ohne Arbeitsvertrag, ohne Personalnummer, ohne Eintrag in irgendeinem System, das man synchronisieren könnte.

Für diese Gruppe gibt es kein automatisches Provisionieren, weil es keine Quelle gibt. Es gibt nur bewusste Entscheidungen: eigenes Konto, Gastzugang, gemeinsam genutztes Postfach oder gar kein digitaler Zugang. Welcher Weg wann trägt, ist ein eigenes Thema, und zwar ein größeres, als es aussieht: [Ehrenamtliche in Microsoft 365: Gastzugang, eigene Konten, geteilte Postfächer oder besser gar nichts?](#) Fürs Identitätsmodell zählt hier nur eines: Auch Ehrenämter enden. Sie enden nur leiser als Arbeitsverhältnisse — niemand gibt einen Schlüssel zurück, niemand füllt ein Formular aus. Deshalb brauchen ehrenamtliche Konten zwingend ein Ablaufdatum und eine regelmäßige Bestätigung durch einen benannten Menschen aus dem Gremium. Sonst wächst die Gruppe monoton.

Die Übersicht, die am Anfang steht

Bring die vier Quellen in eine Tabelle, bevor du irgendein Werkzeug auswählst. Diese Tabelle ist kein Dokumentationsselbstzweck: Sie ist später die Anlage zum Berechtigungskonzept, und sie ist das erste, was die Aufsicht sehen will.

Identitätsquelle	Personengruppe	Provisionierung	Deprovisionierung
Zentrales AD der Landeskirche bzw. des Bistums	Landeskirchenamt, Generalvikariat, Kirchenkreis- und Dekanatsverwaltung, Pfarrämter	Entra Connect Sync oder Cloud Sync, gefiltert auf die produktiven Organisationseinheiten	Konto im AD deaktivieren; die Deaktivierung wird synchronisiert, Lizenz fällt über die Gruppe weg

Identitätsquelle	Personengruppe	Provisionierung	Deprovisionierung
Verzeichnis des diakonischen Werks bzw. Caritasverbands	Verwaltung, Leitungen, Fachdienste des Verbands	Cloud Sync mit eigenem Agenten, auch aus einer nicht verbundenen Gesamtstruktur	im Quellverzeichnis des Verbands; Zuständigkeit gehört in die Vereinbarung zwischen den Trägern
Personalverfahren des Trägers (z. B. KIDICAP)	Beschäftigte in Pflege, Kita, Jugendhilfe, Beratung, Küche, Hauswirtschaft — auch ohne bisheriges IT-Konto	API-getriebene oder HR-getriebene Provisionierung ins AD oder direkt ins Entra ID; Attribute steuern Gruppen und Lizenz	Austrittsdatum aus dem Personalverfahren löst den Leaver-Ablauf aus, idealerweise über Lifecycle Workflows
Kein Verzeichnis: Ehrenamt	Presbyterium, Kirchenvorstand, Pfarrgemeinderat, Küster-, Lektoren- und Besuchsdienst, Jugendarbeit	manuell oder über einen Antragsprozess, immer mit Ablaufdatum und benanntem Bürgen aus dem Gremium	Ablaufdatum läuft ab; Verlängerung nur durch aktive Bestätigung, nicht durch Schweigen
Externe: Dienstleister, Systemhaus, Rechenzentrum	Administration, Wartung, Projektbeteiligte	Gastkonto oder eigenes Konto mit Kennzeichnung, befristet, vertraglich hinterlegt	Ende des Auftrags ist das Ende des Kontos — im Vertrag geregelt, im Kalender hinterlegt

Tabelle 1: Identitätsquellen, Personengruppen und die beiden Richtungen, die beide funktionieren müssen.

Fakten: Die Rechtsgrundlage, die hinter alldem steht

Beide kirchlichen Datenschutzgesetze verlangen angemessene technische und organisatorische Maßnahmen und den Nachweis darüber: auf evangelischer Seite § 27 DSG-EKD („Sicherheit der Verarbeitung“), auf katholischer Seite § 26 KDG („Technische und organisatorische Maßnahmen“). Beide sind im Wortlaut eng an die DSGVO angelehnt.

Ein Berechtigungskonzept ist damit keine Kür. Es ist die Dokumentation, mit der du die Angemessenheit deiner Maßnahmen belegst. Und ein Identitätsmodell, das niemand aufgeschrieben hat, ist kein Konzept, sondern eine Erzählung.

› [DSG-EKD verständlich: Was das evangelische Datenschutzgesetz für Microsoft 365 konkret bedeutet](#)

› [KDG verständlich: Microsoft 365 unter dem Kirchlichen Datenschutzgesetz der katholischen Kirche](#)

Entra Connect Sync, Cloud Sync oder gleich cloud-only?

Diese Frage wird in kirchlichen Häusern besonders gern verschleppt, weil sie unangenehm ist: Sie berührt nämlich die Frage, ob das lokale Verzeichnis überhaupt noch eine Zukunft hat. Und daran hängen Arbeitsplätze, Dienstleisterverträge und manchmal das Selbstverständnis einer ganzen IT-Abteilung. Trotzdem muss sie beantwortet werden, und zwar zeitnah.

Der Stichtag, den viele überlesen haben

Warnung: Entra Connect Sync unterhalb Version 2.5.79.0 stellt am 30. September 2026 die Synchronisierung ein

Microsoft hat diese Hürde nicht als Empfehlung formuliert, sondern als harte Abschaltung: Läuft dein Connect-Server unter einer älteren Version, synchronisiert er ab diesem Datum nicht mehr. Keine neuen Konten, keine Kennwortänderungen, keine Deaktivierungen mehr — und zwar still, ohne dass jemand

eine Meldung auf einem Bildschirm sieht, auf den regelmäßig jemand schaut.

Dazu kommt die reguläre Regel: Jede Version 2.x wird zwölf Monate nach dem Erscheinen einer neueren Version zurückgezogen. Alle 1.x-Versionen sind längst tot und synchronisieren nicht mehr.

Wenn du diesen Beitrag im September 2026 liest und nicht aus dem Kopf sagen kannst, welche Version auf deinem Connect-Server läuft: Das ist die Aufgabe für heute Nachmittag, nicht für das nächste Quartal. Prüf sie besonders dort, wo der Server bei einem Dienstleister steht, der ihn „mitbetreut“ — das ist erfahrungsgemäß die Formulierung, hinter der sich niemand zuständig fühlt.

Was Cloud Sync kann — und was es weiterhin nicht kann

Microsoft entwickelt neue Synchronisierungsfunktionen inzwischen vorrangig auf der Cloud-Sync-Plattform. Für kirchliche Träger ist vor allem eine Eigenschaft interessant, die Connect Sync schlicht nicht hat: Cloud Sync kann aus mehreren nicht miteinander verbundenen Gesamtstrukturen in denselben Tenant synchronisieren. Genau das ist die Lage, wenn Landeskirche, diakonisches Werk und Krankenhausverbund zusammengehen, ohne dass irgendjemand vorhat, die Verzeichnisse zu verheiraten. Man setzt in jede Struktur einen leichtgewichtigen Agenten, konfiguriert alles in der Cloud, und die Träger behalten ihre Autonomie.

Ebenso praktisch: Cloud Sync erlaubt mehrere aktive Agenten gleichzeitig. Der einzelne Connect-Server als heimlicher Single Point of Failure — der, der immer dann ausfällt, wenn die zuständige Person im Urlaub ist — entfällt.

Es gibt allerdings Grenzen, und die muss man vor der Entscheidung kennen, nicht danach:

Fähigkeit	Entra Connect Sync	Entra Cloud Sync	Bedeutung für kirchliche Träger
Nicht verbundene Gesamtstrukturen	nein	ja	der entscheidende Punkt beim Zusammengehen von Landeskirche, Werk und Verband
Mehrere aktive Synchronisierungsinstanzen	nein	ja	kein einzelner Server mehr, an dem alles hängt
Gerätesynchronisierung (Hybrid Join)	ja	nein	wer domänenbeigetretene Rechner ins Entra ID bringen will, braucht Connect Sync oder den Weg über Cloud Kerberos Trust
Objekte je Domäne	unbegrenzt	150.000	für praktisch jeden kirchlichen Träger irrelevant — die Grenze erreicht selbst eine große Landeskirche nicht
Mitglieder je Gruppe	250.000	50.000	ebenfalls unkritisch
Kennwort-Hash-Synchronisierung und Rückschreiben	ja	ja	Selbstbedienung beim Kennwort funktioniert in beiden Welten
Komplexe Synchronisierungsregeln	ja	nein	wer über Jahre Sonderregeln gebaut hat, muss sie auf den Ausdruckseditor übersetzen — das ist die eigentliche Arbeit
Filterung nach Attributen	vollständig	eingeschränkt	Filterung über Organisationseinheiten geht in beiden; feingranulare Attributfilter nur in Connect Sync
Verweise über Gesamtstrukturgrenzen hinweg	ja	nein	relevant nur bei echten Vertrauensstellungen zwischen den Verzeichnissen

Fähigkeit	Entra Connect Sync	Entra Cloud Sync	Bedeutung für kirchliche Träger
Bereitstellung von Gruppen ins lokale AD	nein	ja	praktisch, wenn lokale Fachverfahren weiter über AD-Gruppen gesteuert werden — etwa das Meldewesen

Tabelle 2: Die Unterschiede, die in kirchlichen Konstellationen tatsächlich eine Rolle spielen.

Cloud-only: die Antwort, die häufiger richtig ist, als man denkt

Es gibt eine Gruppe von Trägern, für die die ganze Debatte gegenstandslos ist: den Kreisverband mit vierzig Beschäftigten in drei Beratungsstellen, den Kita-Verbund mit zwölf Einrichtungen, das Bildungswerk. Diese Häuser haben oft ein lokales Verzeichnis, weil vor fünfzehn Jahren jemand einen Dateiserver brauchte. Sie haben keine Anwendung mehr, die es zwingend benötigt. Sie betreiben es, weil es da ist.

Für sie ist cloud-only die ehrlichere Antwort. Kein Sync-Server, keine Version, die im September abläuft, keine Vertrauensstellung, kein Dienstleister, der einmal im Jahr die Zertifikate erneuert. Die Identitäten entstehen direkt im Entra ID, gespeist aus dem Personalverfahren über die API-getriebene Provisionierung oder, bei kleinen Zahlen, aus einem sauberen manuellen Ablauf mit Vier-Augen-Prinzip.

Ein diakonisches Werk in einer Großstadt hat auf diesem Weg in einem knappen Jahr zwei Windows-Server, eine Sicherungslösung und einen Wartungsvertrag abgeschafft. Das eingesparte Geld ist in Lizenzen für die Beschäftigten in der Pflege geflossen, die vorher gar kein Konto hatten. Das ist nicht immer die richtige Rechnung, aber es ist eine, die man aufmachen sollte.

Tipp: Die Prüffrage, die die Diskussion abkürzt

Frag nicht „Können wir das lokale AD abschalten?“. Frag: „Welche Anwendung meldet sich heute noch gegen das lokale Verzeichnis an, und wer benutzt sie wie oft?“ Schreibe die Antworten auf. In kirchlichen Häusern bleiben typischerweise drei Kandidaten übrig: das Meldewesen, ein Finanzverfahren und ein Dateiserver, auf dem seit 2011 niemand mehr etwas abgelegt, aber auch nichts gelöscht hat.

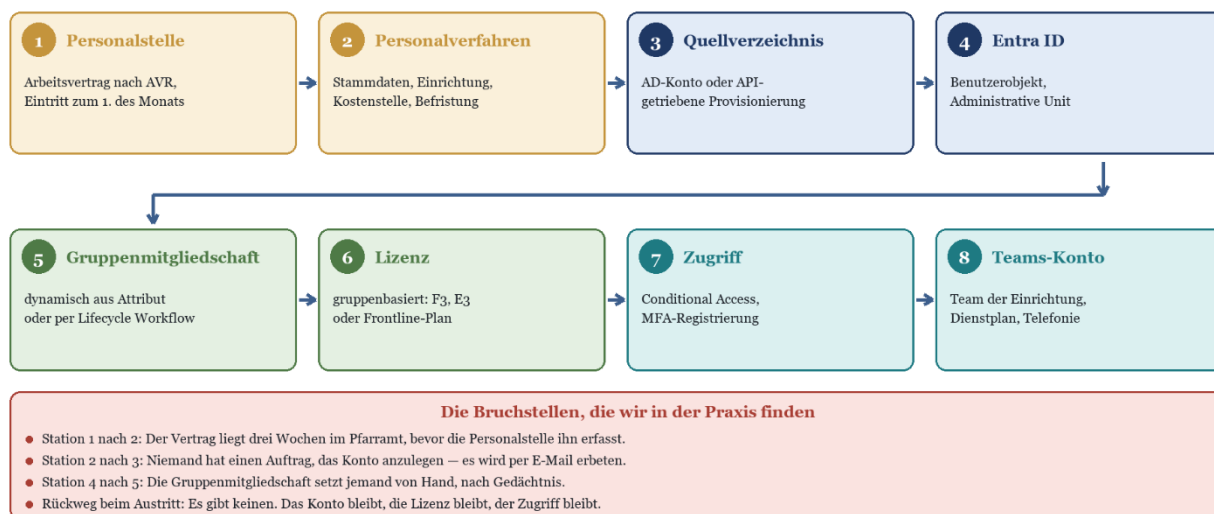
Für die ersten beiden gibt es meist eine Lösung. Der dritte ist kein technisches, sondern ein Aufräumproblem — und gehört in die Aufbewahrungs- und Kassationsfrage, nicht in die Identitätsarchitektur.

Vom Arbeitsvertrag zum Teams-Konto: Eintritt, Versetzung, Austritt

Jetzt zum eigentlichen Betrieb. Die Architektur ist das eine, der Alltag das andere: Eine Erzieherin fängt am Ersten an, eine Verwaltungsmitarbeiterin wechselt vom Kirchenkreis in die Geschäftsstelle des Werks, ein Pflegehelfer geht nach der Probezeit wieder. Diese drei Fälle heißen in der Lehrbuchsprache Joiner, Mover und Leaver. In der kirchlichen Praxis heißen sie meistens „Kannst du der neuen Kollegin mal schnell ein Konto machen?“, „Ach, die ist jetzt woanders?“ und gar nicht.

Von der Personalstelle bis zum Teams-Konto

Der Weg einer neuen Kollegin in der Pflege — acht Stationen, sieben Bruchstellen



Skizze 2: Identitätsfluss von der Personalstelle bis zum Teams-Konto.

Skizze 2: Identitätsfluss von der Personalstelle bis zum Teams-Konto — und die Stellen, an denen er in der Praxis reißt.

Der Eintritt: Warum das Konto am ersten Tag da sein muss

Es gibt einen betriebswirtschaftlichen Grund und einen kulturellen. Der betriebswirtschaftliche ist banal: Eine Pflegefachkraft, die am ersten Tag keinen Dienstplan aufrufen kann, kostet Zeit bei allen anderen. Der kulturelle ist gewichtiger. In Häusern, die sich auf die Dienstgemeinschaft berufen, ist der erste Arbeitstag ein Signal. Wer da mit „Ihre Kennung kommt in ein bis zwei Wochen“ empfangen wird, hat die erste Erfahrung mit der Organisation gemacht, und sie war nicht gut.

Technisch ist der Eintritt der einfachste der drei Fälle, weil jemand ein Interesse daran hat. Die Kette lautet: Personalverfahren erfasst den Eintritt mit Datum, Einrichtung und Funktion; die Provisionierung legt das Objekt an; ein Attribut steuert die Mitgliedschaft in einer dynamischen Gruppe; die Gruppe trägt die Lizenz; die Lizenz erzeugt Postfach und Teams-Konto. Jedes Glied der Kette funktioniert. Die Ketten reißen in kirchlichen Häusern fast nie an der Technik, sondern an der Zuständigkeit: Die Personalstelle hält sich nicht für die IT-Abteilung, und die IT-Abteilung erfährt vom Eintritt, wenn die Kollegin schon davorsteht.

Lifecycle Workflows: der automatisierte Teil — und seine Rechnung

Microsoft hat für genau diese Abläufe Lifecycle Workflows gebaut: Vorgänge, die zu einem definierten Zeitpunkt relativ zum Eintritts- oder Austrittsdatum automatisch laufen. Sieben Tage vor dem Eintritt ein temporäres Zugangspaket erzeugen und der Führungskraft zuschicken. Am Eintrittstag Gruppen zuweisen und eine Willkommensnachricht senden. Am letzten Arbeitstag die Anmeldung sperren, alle Gruppenmitgliedschaften entfernen und die Aufgaben an die Vertretung übergeben. Dreißig Tage später das Konto löschen.

Das ist genau das, was ein kirchlicher Träger braucht, und es hat einen Preis, den man kennen muss: Lifecycle Workflows sind weder in Entra ID P1 noch in P2 enthalten. Sie brauchen Entra ID Governance oder die Entra Suite, und zwar rechnerisch für jede Person, die von einem Workflow erfasst wird — nicht nur für die Administration. Wer zweihundert Beschäftigte über einen Joiner-Workflow laufen lässt, braucht zweihundert Lizenzen plus eine für die verwaltende Person. Das

Kontingent liegt bei fünfzig Workflows und bis zu hundert eigenen Aufgabenerweiterungen; das reicht auch für komplexe Trägerstrukturen reichlich.

Ob sich das rechnet, hängt an der Fluktuation. In einem Pflegeverbund mit hoher Personalbewegung amortisiert sich die Investition schnell, weil jeder nicht gelöschte Zugang ein Risiko und jede unnötig weiterlaufende Lizenz bares Geld ist. In einem Kirchenkreis mit dreißig Beschäftigten und drei Wechseln im Jahr ist ein sauber dokumentierter manueller Ablauf mit Checkliste die ehrlichere Antwort. Die Lizenzfrage insgesamt — Nonprofit-Angebote, Frontline-Pläne, Berechtigung — steht in [Microsoft-365-Lizenzierung für kirchliche Träger: Nonprofit-Angebote, Frontline-Pläne und die Berechtigungsfrage](#).

Der Mover-Fall: die Versetzung, die niemand meldet

Der unterschätzte der drei Fälle. Jemand wechselt von der Kita-Leitung in die Fachberatung des Verbands, von der Verwaltung des Kirchenkreises ins Landeskirchenamt, von der Station in die Pflegedienstleitung. Das Konto bleibt, die E-Mail-Adresse bleibt, der Mensch bleibt — und die Rechte sammeln sich an wie Kalk im Wasserkocher.

Nach fünf Jahren und drei Wechseln hat diese Person Zugriff auf drei Teams, in denen sie nichts mehr zu suchen hat, und ist womöglich noch immer Eigentümerin eines SharePoint-Bereichs, den sie seit Jahren nicht geöffnet hat. Das ist die Situation, aus der später Befunde bei der Datenschutzaufsicht entstehen, und es ist die Situation, die Copilot gnadenlos sichtbar macht: Was eine Person lesen darf, kann Copilot ihr zusammenfassen — auch die Beratungsdokumentation aus dem vorletzten Arbeitsplatz.

Die Gegenmittel sind unspektakulär. Erstens: Mitgliedschaften möglichst dynamisch aus Attributen ableiten, die sich beim Wechsel ohnehin ändern — dann fällt die alte Zugehörigkeit von selbst weg. Zweitens: alles, was nicht dynamisch geht, mit einem Wiedervorlagedatum versehen. Drittens: Zugriffsüberprüfungen für die sensiblen Bereiche, vor allem dort, wo Klientendaten liegen. Wie man Beratungs- und Sozialdaten darüber hinaus technisch absichert, steht in [Klientendaten in Diakonie und Caritas: Sozialdaten, Schweigepflicht und Schutz mit Microsoft Purview](#).

Der Austritt: der Fall, an dem sich alles entscheidet

Deprovisionierung ist die unbeliebteste Disziplin der IT, weil niemand dafür gelobt wird. Sie ist gleichzeitig die, nach der die Aufsicht als Erstes fragt. Und sie hat in kirchlichen Häusern eine Besonderheit, die man nicht übergehen darf: Nicht alles darf sofort weg.

Schritt	Zeitpunkt	Was passiert	Worauf du achten musst
Anmeldung sperren	letzter Arbeitstag, Dienstschluss	Konto deaktivieren, laufende Sitzungen widerrufen, MFA-Methoden entfernen	Deaktivieren, nicht löschen — das Konto ist noch Anker für Postfach und Dateien
Zugehörigkeiten lösen	letzter Arbeitstag	Gruppen, Teams, Administrative Unit, Rollen und Eigentümerschaften abräumen	verwaiste Eigentümerschaften an Teams und SharePoint-Bereichen vorher an eine Person mit Dienstbezeichnung übergeben
Lizenz einziehen	nach kurzer Karenz	gruppenbasierte Lizenz endet mit der Gruppenmitgliedschaft	zu frühes Entziehen kann Postfachinhalte gefährden; die Karenz gehört ins Konzept, nicht in die Improvisation
Postfach und	innerhalb weniger	Vertretung erhält Zugriff, Inhalte	Seelsorgliches bleibt außen vor — es

Schritt	Zeitpunkt	Was passiert	Worauf du achten musst
Dateien regeln	Wochen	werden umgehängt oder archiviert	hatte in den allgemeinen Ablagen ohnehin nichts zu suchen
Aufbewahrung sicherstellen	vor dem Löschen	Aufbewahrungsrichtlinie greift unabhängig vom Kontostatus	kirchliche Aufbewahrungs- und Kassationsregeln gehen der Aufräumlust vor
Konto löschen	nach der festgelegten Frist	Objekt entfernen, Protokoll behalten	Frist im Konzept festlegen und einhalten — beides, nicht eines von beidem

Tabelle 3: Ein Austrittsablauf, der sowohl die Sicherheit als auch die Aufbewahrung berücksichtigt.

Wichtig: Provisionierung und Deprovisionierung sind ein Thema für die Mitarbeitervertretung

Wer automatisiert Konten anlegt, Attribute aus dem Personalverfahren überträgt und Anmeldevorgänge protokolliert, verarbeitet Beschäftigtendaten in einer Weise, die nach MVG-EKD und nach MAVO die MAV angeht. Das ist kein Störfeuer, sondern der ganz normale Dritte Weg.

Praktisch heißt das: Die MAV gehört an den Tisch, bevor die Attributzuordnung steht — nicht danach. Regelbar ist das in einer Dienstvereinbarung, die beschreibt, welche Attribute übertragen werden, wozu sie dienen, wie lange Protokolle aufbewahrt werden und wer sie auswerten darf. Wer das früh und offen macht, bekommt in aller Regel eine Vereinbarung. Wer es nachreicht, bekommt eine Diskussion.

› [Mitarbeitervertretung und Microsoft 365: MVG-EKD, MAVO, Dienstvereinbarung und Mitbestimmung](#)

Delegation ohne Global-Admin-Inflation

Kommen wir zu dem Teil, bei dem in Überprüfungen am häufigsten kurz Stille im Raum eintritt.

Warnung: Vierzehn Global Administrators bei zweihundert Beschäftigten

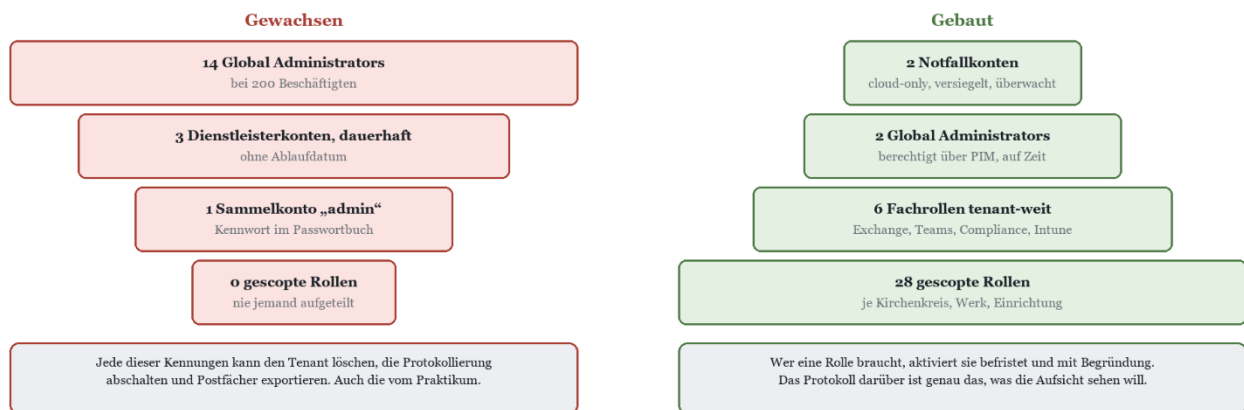
Der Befund stammt aus einer Tenant-Überprüfung bei einem diakonischen Träger: zweihundert Beschäftigte, vierzehn Konten mit der Rolle Global Administrator. Darunter drei Konten des Systemhauses, angelegt bei der Einführung vor fünf Jahren und seither nie überprüft. Ein Sammelkonto namens „admin“, dessen Kennwort in einem Passwortbuch stand, auf das sechs Leute Zugriff hatten. Und zwei Konten von Personen, die im Haus gar nicht mehr arbeiteten.

Niemand hatte das böswillig gebaut. Jede einzelne Vergabe hatte im Moment ihrer Entstehung einen nachvollziehbaren Grund: Jemand brauchte kurzfristig eine Berechtigung, niemand wusste, welche kleinere ausgereicht hätte, also wurde die größte vergeben — „das räumen wir später auf“. Später ist bekanntlich ein Ort, den niemand je erreicht.

Die Bewertung ist unangenehm schlicht: Jedes dieser vierzehn Konten kann den gesamten Tenant umkonfigurieren, die Protokollierung abschalten, jedes Postfach exportieren und den Datenschutzbeauftragten aussperren. Microsoft empfiehlt, die Rolle Global Administrator an weniger als fünf Personen zu vergeben. Vierzehn ist fast das Dreifache davon — und das bei einem Träger, der Klientendaten verarbeitet, die dem Sozialgeheimnis unterliegen.

Der Rechtekegel: wie viele dürfen wie viel?

Links der Zustand, den wir vorfinden. Rechts der, den die Aufsicht sehen möchte.



Skizze 3: Rollenverteilung vor und nach dem Aufräumen.

Skizze 3: Rollenverteilung vor und nach dem Aufräumen — dieselbe Organisation, dieselbe Arbeitsfähigkeit.

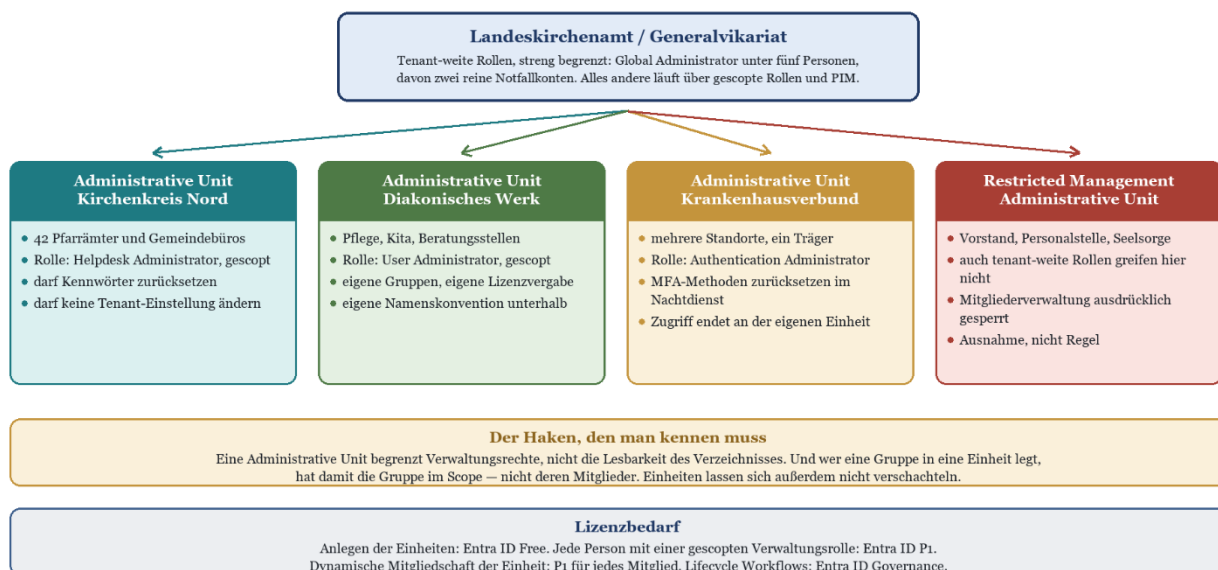
Administrative Units: Delegation entlang der kirchlichen Gliederung

Das Werkzeug gegen die Rolleninflation heißt Administrative Unit. Eine solche Einheit ist ein Behälter für Benutzer, Gruppen oder Geräte, und sie beschränkt eine Rolle auf ihren Inhalt. Wer als Helpdesk Administrator im Geltungsbereich der Einheit „Kirchenkreis Nord“ eingesetzt ist, kann für die Menschen dort Kennwörter zurücksetzen — und für niemanden sonst. Er kann keine Tenant-Einstellung ändern, keine Richtlinie anfassen und im Nachbarkirchenkreis gar nichts.

Für kirchliche Träger ist das der passgenaue Baustein, weil er sich an der Gliederung orientiert, die es ohnehin gibt: eine Einheit je Kirchenkreis oder Dekanat, eine je Werk, eine je größerer Einrichtung. Die örtliche IT, die es an vielen Stellen ohnehin gibt und die sowieso angerufen wird, bekommt damit genau die Rechte, die sie für ihre Leute braucht. Das ist nicht nur sicherer — es entspricht auch dem Selbstverständnis der Ebenen, die sich zu Recht nicht gern von oben verwalten lassen.

Administrative Units statt Vollzugriff

Delegation entlang der kirchlichen Gliederung — jeder verwaltet seine Leute, niemand alle



Skizze 4: Delegation über Administrative Units entlang der Trägerstruktur.

Skizze 4: Administrative Units entlang der Trägerstruktur, mit gescopten Rollen statt Tenant-Vollzugriff.

Drei Eigenschaften muss man kennen, bevor man das Modell aufsetzt. Erstens lassen sich Administrative Units nicht verschachteln — eine Einheit „Kirchenkreis“ mit Untereinheiten je Gemeinde gibt es nicht. Zweitens bringt eine Gruppe, die man in eine Einheit legt, ihre Mitglieder nicht mit: Man darf die Gruppe verwalten, nicht die Menschen darin. Wer beides will, muss beides hineinlegen. Drittens begrenzen Einheiten nur Verwaltungsrechte, nicht das Lesen des Verzeichnisses — die Adressliste bleibt tenant-weit sichtbar, sofern du das nicht getrennt einschränkst.

Für wenige, wirklich sensible Personenkreise gibt es die Sonderform der Restricted Management Administrative Unit: Wer hier hineingelegt wird, ist auch für tenant-weite Administrationsrollen nicht mehr verwaltbar; die Mitgliederverwaltung ist ausdrücklich gesperrt. Das kann für Vorstand, Personalstelle oder Konten der Seelsorge sinnvoll sein. Behandle es als Ausnahme mit gutem Grund und nicht als Standard — sonst bearbeitet am Ende niemand mehr das Kennwortproblem am Sonntagabend.

Welche Rolle du stattdessen vergibst

Die häufigste Ursache für Global-Admin-Inflation ist Unkenntnis: Man weiß nicht, welche schmalere Rolle gereicht hätte. Die folgende Tabelle deckt die Anliegen ab, die in kirchlichen Häusern tatsächlich vorkommen.

Das Anliegen im Alltag	Die passende Rolle	Geltungsbereich	Was damit nicht geht
„Ich muss der Küsterin das Kennwort zurücksetzen.“	Helpdesk Administrator	Administrative Unit des Kirchenkreises oder der Einrichtung	keine Kennwörter von Personen mit Administrationsrollen, keine Tenant-Einstellungen
„Wir legen neue Beschäftigte selbst an und vergeben Lizenzen.“	User Administrator	Administrative Unit des Werks oder Verbands	keine Rollenvergabe über den eigenen Bereich hinaus
„Im Nachtdienst muss jemand die MFA-Methode zurücksetzen können.“	Authentication Administrator	Administrative Unit der Einrichtung	keine Authentifizierungsrichtlinien ändern
„Die Verteiler und Postfächer betreue ich.“	Exchange Administrator	tenant-weit	keine Benutzerkonten, keine Richtlinien außerhalb Exchange
„Teams, Kanäle und Telefonie liegen bei mir.“	Teams Administrator	tenant-weit	kein Zugriff auf Postfächer oder Compliance-Werkzeuge
„Ich bin örtlich Beauftragte für den Datenschutz und muss nachvollziehen können.“	Global Reader, ergänzt um lesende Compliance-Rechte	tenant-weit, ausschließlich lesend	keinerlei Änderung — und genau das ist der Punkt
„Aufbewahrung, Label und Auswertungen gehören zu meiner Aufgabe.“	Compliance Administrator	tenant-weit	keine Benutzerverwaltung, keine Verzeichniseinstellungen
„Das Systemhaus betreut uns im Betrieb.“	die jeweils kleinste passende Fachrolle, befristet über PIM	so eng wie möglich	keine dauerhafte Global-Administrator-Rolle, kein Sammelkonto

Tabelle 4: Für fast jedes Anliegen gibt es eine Rolle, die kleiner ist als Global Administrator.

Tipp: Die zwei Konten, die es trotzdem geben muss

Microsoft empfiehlt zwei reine Cloud-Konten als Notfallzugänge, dauerhaft mit der Rolle Global Administrator, keiner konkreten Person zugeordnet, ausschließlich für den Fall gedacht, dass die normalen Wege nicht funktionieren — die Verbindung zum lokalen Verzeichnis ist weg, der Verschlüsselungsvorfall läuft, oder die einzige Person mit Zugang ist im Urlaub in einem Funkloch.

Diese Konten gehören nicht in ein Passwortbuch im Schrank des Pfarramts. Sie gehören in einen versiegelten Umschlag im Tresor, mit dokumentiertem Zugriffsverfahren, mit Alarmierung bei jeder Anmeldung und mit einer Ausnahme in den Conditional-Access-Regeln, die verhindert, dass genau die Regel, die dich schützen soll, dich im Ernstfall aussperrt. Prüf einmal im Jahr, ob sie funktionieren. Ein Notfallkonto, das im Notfall nicht geht, ist schlimmer als keines, weil man sich darauf verlassen hat.

Was die Aufsicht davon sehen will

BfD EKD und Diözesandatenschutzbeauftragte beziehungsweise das Katholische Datenschutzzentrum fragen bei einem Microsoft-365-Tenant sehr verlässlich nach denselben Dingen: nach dem Berechtigungskonzept, nach der Liste der privilegierten Konten, nach dem Nachweis, dass ausgeschiedene Personen keinen Zugriff mehr haben, und nach der Protokollierung, mit der du das belegst. Nichts davon ist überraschend, und nichts davon lässt sich am Abend vor dem Termin erzeugen. Was genau erwartet wird, steht in [Kirchliche Datenschutzaufsicht in der Praxis: Was BfD EKD und Diözesandatenschutzbeauftragte von einem Microsoft-365-Tenant erwarten](#).

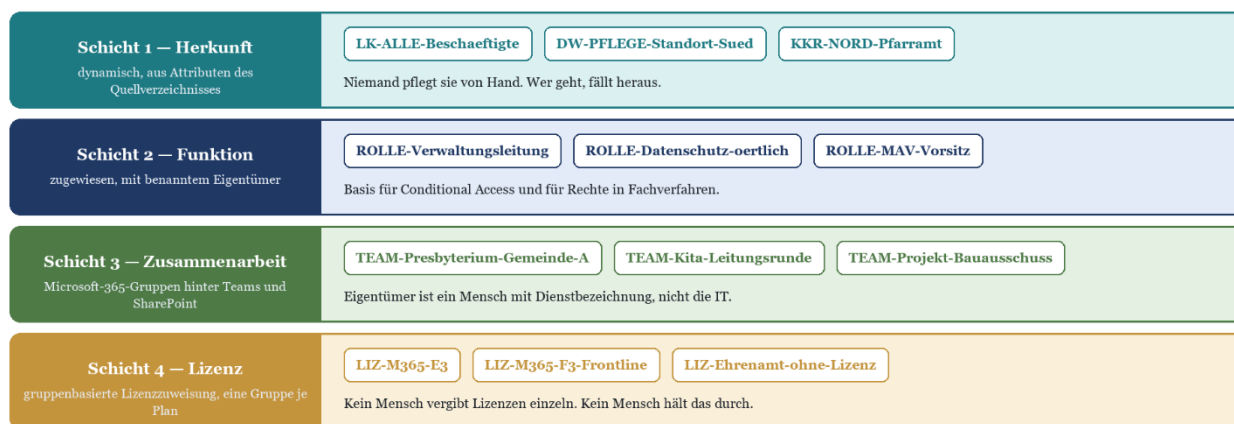
Der praktische Rat: Führe eine Rollenmatrix als Anlage zum Berechtigungskonzept — wer hat welche Rolle, in welchem Geltungsbereich, seit wann, auf welcher Grundlage, bis wann. Zwei Seiten reichen. Und lass sie einmal im Jahr von den Verantwortlichen der jeweiligen Ebene bestätigen, nicht von der IT. Die IT weiß, wer welche Rechte hat. Nur die Leitung der Einrichtung weiß, wer sie noch braucht.

Ein Gruppenmodell, das die Trägerstruktur abbildet

Gruppen sind in Microsoft 365 die Währung, in der Rechte ausgezahlt werden. Wenn das Gruppenmodell nicht stimmt, stimmt hinterher nichts: nicht die Lizenzierung, nicht der Conditional Access, nicht die Berechtigung in SharePoint, nicht die Zielgruppe im Intranet. Und da man Gruppen so leicht anlegen kann, entsteht in jedem Tenant nach spätestens achtzehn Monaten ein Unterholz aus Gruppen, die niemand mehr zuordnen kann.

Ein Gruppenmodell, das die Trägerstruktur abbildet

Vier Schichten, klar getrennte Aufgaben — und ein Name, aus dem man die Zuständigkeit ablesen kann



Skizze 5: Gruppenschichten entlang der Trägerstruktur.

Skizze 5: Vier Gruppenschichten entlang der Trägerstruktur — getrennte Aufgaben, sprechende Namen.

Vier Schichten, vier Aufgaben

- **Herkunft.** Wer gehört wozu? Diese Gruppen leiten sich dynamisch aus Attributen des Quellverzeichnisses ab — Einrichtung, Kostenstelle, Dienstort, Beschäftigungsart. Niemand pflegt sie von Hand, und genau darin liegt ihr Wert: Wer geht, fällt automatisch heraus. Dynamische Mitgliedschaft setzt Entra ID P1 für jede erfasste Person voraus.
- **Funktion.** Wer hat welche Aufgabe? Verwaltungsleitung, örtlich Beauftragte für den Datenschutz, MAV-Vorsitz, Pflegedienstleitung, Kita-Leitung. Diese Gruppen werden zugewiesen, nicht abgeleitet, und sie haben zwingend einen benannten Eigentümer. Sie sind die Grundlage für Conditional Access und für Rechte in Fachverfahren.
- **Zusammenarbeit.** Die Microsoft-365-Gruppen hinter Teams und SharePoint-Bereichen: das Presbyterium, die Leitungsrunde der Kitas, der Bauausschuss. Eigentümer ist ein Mensch mit Dienstbezeichnung, nicht „die IT“. Wer keinen Eigentümer hat, wird nicht angelegt.
- **Lizenz.** Je Plan eine Gruppe, an die die Lizenz gebunden ist. Wer in die Gruppe kommt, bekommt die Lizenz; wer herausfällt, verliert sie. Manuelle Einzelzuweisung von Lizenzen hält kein Mensch über Jahre durch, und in einem Verbund mit mehreren Trägern erst recht nicht.

Die Namenskonvention, die du nur einmal festlegst

Ein Gruppenname sollte von links nach rechts lesbar machen, wer zuständig ist: Träger oder Ebene, dann Bereich, dann Zweck. „DW-PFLEGE-Standort-Sued“ sagt einem Menschen im dritten Jahr noch, worum es geht. „Gruppe_neu2“ sagt niemandem etwas, und zwar schon ab dem zweiten Tag.

Zwei Regeln aus der Praxis, die sich auszahlen. Erstens: Verzichte in Gruppennamen auf Umlaute und Sonderzeichen, obwohl sie technisch möglich sind — irgendein nachgelagertes System wird damit Schwierigkeiten haben, und du findest erst heraus welches, wenn es zu spät ist. Im Anzeigenamen dürfen sie stehen, im technischen Namen besser nicht. Zweitens: Häng ein Präfix an, das die Schicht kennzeichnet. Dann sieht jeder auf einen Blick, ob eine Gruppe abgeleitet, zugewiesen, für Zusammenarbeit oder für Lizenzen da ist — und niemand kommt auf die Idee, eine dynamische Herkunftsgruppe als Verteiler zu missbrauchen.

Wie sich dasselbe Prinzip in der Ablagestruktur fortsetzt — Pfarramt, Gremien, Ausschüsse, Gebäude —, steht in [SharePoint-Informationsarchitektur für Kirchengemeinde und Kirchenkreis](#).

Was welcher Baustein kostet

Damit die Planung nicht an einer Überraschung scheitert: eine Übersicht der Voraussetzungen. Sie ist der Grund, warum manche Träger das Modell in zwei Stufen bauen — erst das, was mit P1 geht, später der Rest.

Baustein	Voraussetzung	Wofür die Lizenz gezahlt wird
Administrative Units anlegen	Entra ID Free	keine gesonderte Zählung
Geschopte Rolle in einer Administrative Unit	Entra ID P1	je Person mit einer solchen Verwaltungsrolle
Dynamische Mitgliedschaft (Gruppen und Einheiten)	Entra ID P1	je Person, die Mitglied mindestens einer dynamischen Gruppe oder Einheit ist
Gruppenbasierte Lizenzzuweisung	Entra ID P1	je Person, die auf diesem Weg eine Lizenz erhält
Conditional Access	Entra ID P1	je Person, für die eine Richtlinie gilt
HR-getriebene und API-getriebene Provisionierung	Entra ID P1	je Identität, die auf diesem Weg entsteht
Lifecycle Workflows	Entra ID Governance oder Entra Suite	je Person im Geltungsbereich eines Workflows, plus die verwaltende Person
Zugriffsüberprüfungen und Zugangspakete	Entra ID P2 für den Grundumfang, Entra ID Governance für die erweiterten Funktionen	je überprüfte und je überprüfende Person
Privileged Identity Management	Entra ID P2 oder Entra ID Governance	je Person mit berechtigter Rollenzuweisung, plus die genehmigenden Personen

Tabelle 5: Welcher Baustein welche Lizenzstufe braucht — und wie gezahlt wird.

Fakten: Was Entra ID P2 nicht mehr bekommt

Microsoft hat die Governance-Funktionen aus dem P2-Plan herausgelöst und in eine eigene Produktfamilie überführt. Die Funktionen, die in P2 allgemein verfügbar waren, bleiben dort. Neue Funktionen aus dem Bereich Identity Governance kommen aber ausdrücklich nicht mehr in den P2-Plan. Für die Planung bedeutet das: Wer den Lebenszyklus in den nächsten Jahren automatisieren will, plant mit Entra ID Governance oder der Entra Suite. Wer heute P2 kauft in der Erwartung, dass die Funktionen schon nachwachsen, plant an der Wirklichkeit vorbei.

Ein letzter Punkt, der in kirchlichen Häusern regelmäßig zu Missverständnissen führt: Gemeindegliederdaten aus dem kirchlichen Meldewesen gehören nicht ins Entra ID. Die Meldewesenverfahren der Landeskirchen und Bistümer sind eigene Fachanwendungen mit eigener Rechtsgrundlage, eigenen Zugriffsregeln und einem sehr begrenzten Kreis von Berechtigten. Wer Gemeindeglieder als Kontakte oder gar als Benutzer in den Tenant spiegelt, weil „man sie dann im Adressbuch hat“, baut ein Datenschutzproblem, das sich später nur mit erheblichem Aufwand zurückdrehen lässt. Dasselbe gilt für alles aus der Seelsorge — siehe [Seelsorgegeheimnis und Beichtgeheimnis in Microsoft 365: Was nie in Teams, OneNote oder Copilot landen darf](#).

Häufige Fragen

Brauchen wir wirklich Entra ID P1 für alle, oder reicht das, was in Microsoft 365 Business Premium steckt?

Business Premium enthält Entra ID P1. Wenn dein Träger klein genug für Business Premium ist und alle Beschäftigten diesen Plan haben, brauchst du nichts zusätzlich. Die Falle liegt woanders: bei gemischten Beständen. Sobald ein Teil der Belegschaft auf einem Plan ohne P1 sitzt — etwa in der Pflege oder in der Kita —, musst du für die Zählung genau hinsehen. Dynamische Mitgliedschaft und Conditional Access werden je erfasster Person gezählt, nicht je verwaltender. Wer zweihundert Beschäftigte über eine dynamische Gruppe steuert, braucht rechnerisch zweihundert P1-Lizenzen, auch wenn nur drei Leute die Gruppe administrieren.

Wir haben drei getrennte Gesamtstrukturen: Landeskirche, diakonisches Werk, Krankenhausverbund. Müssen wir die zusammenlegen?

Nein, und das ist die gute Nachricht dieses Beitrags. Entra Cloud Sync kann aus nicht miteinander verbundenen Gesamtstrukturen in denselben Tenant synchronisieren, ohne dass es zwischen den Verzeichnissen eine Vertrauensstellung geben muss. Jede Struktur bekommt ihre eigenen Agenten, die Konfiguration liegt zentral in der Cloud, die Autonomie der Träger bleibt erhalten. Rechne trotzdem mit Arbeit an zwei Stellen: bei den UPN-Suffixen und bei der Vermeidung doppelter Objekte für Personen, die für zwei Träger tätig sind — den Fall gibt es in der Kirche häufiger, als die Werkzeuge vorsehen.

Was machen wir mit Menschen, die für zwei Träger arbeiten?

Die Pfarrerin, die zu einem Teil in der Gemeinde und zu einem anderen in der Klinikseelsorge tätig ist. Die Verwaltungsmitarbeiterin, die anteilig für Kirchenkreis und Werk arbeitet. Technisch sauber ist ein Konto mit zwei Gruppenzugehörigkeiten. Das erfordert allerdings eine Einigung darüber, welches Verzeichnis führend ist und wer die Lizenz bezahlt. Die technische Antwort ist einfach, die organisatorische nicht — und sie gehört in die Vereinbarung zwischen den Trägern, nicht in die Synchronisierungsregel. Zwei Konten für einen Menschen sind die schlechtere Lösung: Sie verdoppeln Lizenzkosten, Angriffsfläche und Verwirrung, und beim Austritt wird zuverlässig eines übersehen.

Können wir Administrative Units je Kirchengemeinde anlegen?

Technisch ja, praktisch selten sinnvoll. Bei mehreren hundert Gemeinden entsteht ein Verwaltungsaufwand, den niemand trägt, und jede Einheit braucht mindestens eine Person mit einer gescopten Rolle und damit einer P1-Lizenz. Der Schnitt auf Ebene Kirchenkreis, Dekanat oder Werk trifft in fast allen Projekten besser — dort sitzt die IT-Unterstützung ohnehin. Und weil sich Einheiten nicht verschachteln lassen, kannst du die feinere Gliederung nicht unter der gröberen abbilden. Du müsstest sie nebeneinanderstellen, und dann verwaltest du am Ende doppelt.

Unser Systemhaus sagt, es braucht dauerhaft Global Administrator. Stimmt das?

In aller Regel nicht. Für den laufenden Betrieb reichen Fachrollen — Exchange, Teams, Intune, Benutzerverwaltung. Für die seltenen Vorgänge, die tatsächlich tenant-weite Rechte brauchen, gibt

es die befristete Aktivierung über Privileged Identity Management, mit Begründung und Protokoll. Dauerhafte Global-Administrator-Rechte für ein externes Unternehmen sind gegenüber der kirchlichen Aufsicht schwer zu begründen und gehören ohnehin in den Vertrag zur Auftragsverarbeitung — einschließlich der Frage, was mit den Konten passiert, wenn der Vertrag endet. Wenn ein Dienstleister an dieser Stelle hart bleibt, ist das eine Aussage über den Dienstleister.

Wie lange darf ein Konto nach dem Austritt bestehen bleiben?

Dafür gibt es keine kirchenrechtlich festgelegte Zahl, die man zitieren könnte. Was es gibt, ist die Pflicht, personenbezogene Daten nicht länger zu verarbeiten als nötig, und die Pflicht, kirchliche Aufbewahrungs- und Kassationsregeln einzuhalten. Beides zusammen führt zu einem zweistufigen Ablauf: Die Anmeldung endet am letzten Arbeitstag, sofort und ohne Ausnahme. Das Objekt bleibt danach so lange bestehen, wie du für die geordnete Übergabe von Postfach und Ablage brauchst — und keinen Tag länger. Leg diese Frist selbst fest, schreib sie ins Konzept und halt sie ein. Die Aufsicht fragt nicht nach der Zahl. Sie fragt, ob du eine hast und ob du dich daran hältst.

Wir haben zweitausend Ehrenamtliche. Bekommen die alle ein Konto?

Vermutlich nicht, und das ist keine Geringschätzung des Ehrenamts, sondern eine Frage der Verhältnismäßigkeit. Ein Konto ist eine Dauerbeziehung mit Pflichten auf beiden Seiten: Kennwort, zweiter Faktor, Schulung, Überprüfung, Deprovisionierung. Für das Presbyterium, das regelmäßig mit Vorlagen arbeitet, lohnt sich das. Für die Helferin, die zweimal im Jahr beim Gemeindefest mitmacht, ist ein Gastzugang zu einem einzelnen Team die angemessenere Lösung — oder gar nichts. Die Abwägung im Einzelnen steht in [Ehrenamtliche in Microsoft 365: Gastzugang, eigene Konten, geteilte Postfächer oder besser gar nichts?](#).

Wie fangen wir an, wenn der Tenant schon läuft und unaufgeräumt ist?

In dieser Reihenfolge, und sie ist bewusst so gewählt. Erstens: Liste aller Konten mit privilegierten Rollen ziehen und jede einzelne Zuweisung schriftlich begründen lassen — nicht durch die IT, sondern durch die jeweilige Leitung. Was sich nicht begründen lässt, fällt weg. Zweitens: zwei Notfallkonten einrichten und testen. Drittens: Administrative Units entlang der Gliederung anlegen und die gescopten Rollen vergeben. Viertens: das Gruppenmodell aufsetzen und die Lizenzen darauf umstellen. Fünftens: den Austrittsablauf schreiben und ihn einmal an einem echten Fall durchspielen. Erst dann lohnt sich das Nachdenken über Automatisierung. Wer mit Schritt fünf anfängt, automatisiert das Chaos — und zwar zuverlässig.

Fazit

Das Identitätsmodell ist die Schicht, auf der alles andere steht. Wenn es stimmt, merkst du davon nichts: Konten sind am ersten Tag da, verschwinden am letzten, Rechte folgen der Aufgabe, und die Rollenmatrix passt auf zwei Seiten. Wenn es nicht stimmt, merkst du es an allen anderen Stellen gleichzeitig — bei den Lizenzkosten, beim Oversharing in SharePoint, beim ersten Copilot-Versuch, bei der Prüfung durch die Aufsicht und spätestens dann, wenn ein Konto missbraucht wird, das seit achtzehn Monaten niemandem mehr gehört.

Für kirchliche Träger kommt eine Besonderheit hinzu, die man nicht wegorganisieren kann: Die Identitätsquellen gehören verschiedenen Rechtspersonen. Das Verzeichnis der Landeskirche, das Personalverfahren des Werks und die Mitgliederliste des Presbyteriums sind nicht drei

Abteilungen eines Hauses, sondern drei Verantwortliche mit eigenen Pflichten. Ein Identitätsmodell, das diese Struktur abbildet statt sie einzuebnen, ist deshalb nicht nur rechtlich sauberer — es wird auch akzeptiert. Und Akzeptanz ist in kirchlichen Strukturen kein weicher Faktor, sondern die Voraussetzung dafür, dass überhaupt jemand mitmacht.

Die drei Dinge, die du aus diesem Beitrag mitnehmen solltest: Prüf heute die Version deines Connect-Servers, wenn du einen hast. Zieh diese Woche die Liste deiner privilegierten Konten und erschrick kurz. Und schreib auf, welche Personengruppen es gibt und woher ihre Daten kommen — diese eine Tabelle ist mehr wert als jedes Werkzeug, das du danach auswählst.

Weiter im Thema: Wenn du an dieser Stelle weiterlesen willst

Die Nachbarthemen, die am engsten an das Identitätsmodell grenzen:

- › [Ein Tenant oder viele? Kirchengemeinde, Kirchenkreis, Landeskirche, Bistum und die Frage der Tenant-Architektur](#)
- › [Ehrenamtliche in Microsoft 365: Gastzugang, eigene Konten, geteilte Postfächer oder besser gar nichts?](#)
- › [Kita, Pflege, Jugendhilfe: Frontline-Arbeitsplätze in Microsoft 365 für Menschen ohne Schreibtisch](#)
- › [Mitarbeitervertretung und Microsoft 365: MVG-EKD, MAVO, Dienstvereinbarung und Mitbestimmung](#)
- › [Microsoft 365 in Kirche, Diakonie und Caritas: Was wirklich anders ist als in Kommune und Mittelstand](#)
- › [Microsoft-365-Schulungen für kirchliche Träger](#)
- › [Microsoft 365 Beratung für kirchliche Träger](#)