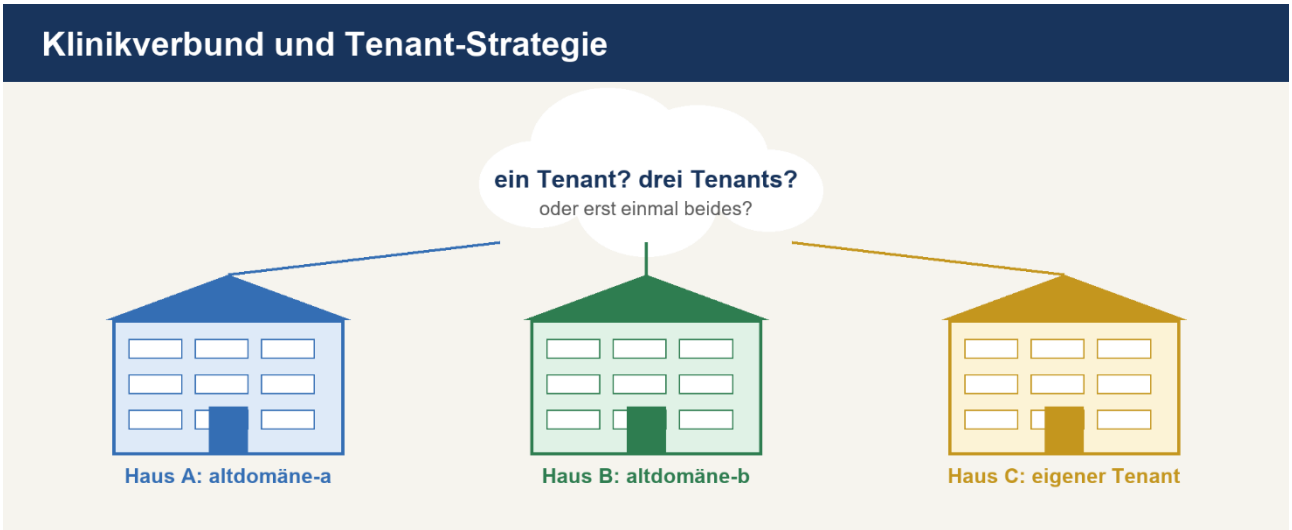
Klinikverbund und Tenant-Strategie: Ein Mandant, mehrere Häuser, gewachsene Domänen



Wissen

Der Überblick zur ganzen Serie: Recht, Technik und Organisation in der Klinik.

› **Microsoft 365 im Krankenhaus**

Beratung

Tenant-Strategie für Ihren Verbund – mit Kriterien, Varianten und Vorlage für die Geschäftsführung.

› **Microsoft-365-Beratung für Krankenhäuser**

Schulung

Administratoren fit machen für Verwaltungseinheiten, Mehrmandantenorganisation und Synchronisierung.

› **Microsoft-365-Schulung für Krankenhäuser**

Im Krankenhauswesen ist die Fusion kein Ereignis, sondern ein Aggregatzustand. Kaum ist ein Haus in den Verbund integriert, steht das nächste vor der Tür: ein kommunales Haus, dessen Träger die Defizite nicht mehr tragen will, eine Rehaklinik, die ins Portfolio passt, eine Fachklinik, die ein freigemeinnütziger Träger abgibt. Mit jedem neuen Standort kommen Patienten, Betten, eine Belegschaft – und eine IT-Landschaft, die man sich nicht ausgesucht hat. Eine eigene Active-Directory-Domäne gehört praktisch immer dazu, eine eigene Mailwelt meistens, und immer öfter auch ein eigener Microsoft-365-Tenant, den irgendjemand vor Jahren mit einer Kreditkarte und guten Absichten angelegt hat.

Spätestens dann stellt die Geschäftsführung die Frage, die nach einer Formalie klingt und doch eine Grundsatzentscheidung ist: Wie viele Tenants braucht der Verbund? Bei der Frage **Klinikverbund Microsoft 365 Tenant** geht es um weit mehr als um Technik. Es geht um Gesellschaftsrecht, Datenschutz zwischen rechtlich selbstständigen Häusern, um die Frage, ob die IT gemeinsam oder getrennt betrieben wird – und um die unbequeme Wahrscheinlichkeit, dass ein Haus, das heute integriert wird, in fünf Jahren wieder verkauft oder ausgegliedert wird. Wer schon einmal einen Standort aus einem gemeinsamen Tenant herausgelöst hat, weiß: Das Einsteigen ist ein Projekt, das Aussteigen eine Operation am offenen Herzen. Nur ohne Anästhesie.

Dieser Beitrag beschreibt die drei grundlegenden Varianten – einen gemeinsamen Tenant mit Verwaltungseinheiten je Haus, mehrere Tenants als Mehrmandantenorganisation mit

mandantenübergreifender Synchronisierung und die Mischform für die Übergangszeit – und legt die Kriterien für die Entscheidung offen. Und er vergisst die lokale Seite nicht: Vertrauensstellungen zwischen Domänen, Altdomänen, die noch Jahre weiterleben, und Teilmigrationen, bei denen nur Verwaltung und Finanzwesen umziehen. Er gehört zur Serie Microsoft 365 im Krankenhaus.

Fakten: Was ein Tenant ist – und was nicht

Ein Tenant (deutsch: Mandant) ist die Organisationseinheit in Microsoft Entra ID und Microsoft 365: ein Verzeichnis mit Benutzern, Gruppen, Geräten, Lizenzen, Richtlinien und den Daten in Exchange Online, SharePoint, OneDrive und Teams.

- Eine eigene Domäne (etwa klinik-a.example) kann nur in genau einem Tenant als verifizierte Domäne eingetragen sein.
- Ein Objekt aus dem lokalen Active Directory wird über Entra Connect bzw. Cloud Sync in einen Tenant synchronisiert. Mehrere Gesamtstrukturen in einen Tenant sind ein unterstützter Normalfall, eine Gesamtstruktur in mehrere Tenants nur mit Einschränkungen.
- Ein Tenant ist keine AD-Domäne. Vertrauensstellungen wie im lokalen AD gibt es in Entra ID nicht; das Pendant sind mandantenübergreifende Zugriffseinstellungen und B2B-Zusammenarbeit.

Warum der Klinikverbund überhaupt eine Tenant-Strategie braucht

In einem mittelständischen Unternehmen ist die Frage schnell beantwortet: eine Firma, ein Tenant, fertig. Im Klinikverbund ist das anders, und zwar aus Gründen, die mit IT wenig zu tun haben. Die Struktur eines Verbunds bildet selten ein einziges Unternehmen ab, sondern ein Geflecht: eine Holding oder Muttergesellschaft, darunter mehrere Krankenhausgesellschaften als gGmbH oder GmbH, eine Servicegesellschaft für Reinigung und Speisenversorgung, ein MVZ, manchmal eine eigene IT-Gesellschaft. Jede dieser Gesellschaften ist datenschutzrechtlich zunächst ein eigener Verantwortlicher. Und jede hat ihre eigene Geschichte.

Was ein übernommener Standort typischerweise mitbringt

Wer die Integration eines übernommenen Hauses plant, findet in der Bestandsaufnahme fast immer dieselben Zutaten, nur in wechselnder Dosierung:

- **Eine eigene AD-Domäne**, häufig als eigene Gesamtstruktur, mit eigenem Namensraum, eigenen Gruppenrichtlinien und Dienstkonten, deren Kennwort zuletzt geändert wurde, als das Haus noch einen anderen Träger hatte.
- **Eine eigene Mailwelt**: lokales Exchange, Exchange Hybrid, ein Hoster des früheren Trägers oder bereits Exchange Online in einem eigenen Tenant.
- **Ein eigenes KIS** oder zumindest eine eigene Instanz, dazu Subsysteme wie LIS, RIS und PACS, deren Schnittstellen auf die lokale Domäne, lokale Namen und lokale Zertifikate gebaut sind.
- **Medizintechnik**, die an Domänenkonten, NTLM, alte Protokolle und feste Hostnamen gebunden ist und deren Hersteller jeder Änderung mit der Begeisterung eines Notaufnahme-Teams am Samstagabend entgegensehen.
- **Einen eigenen Microsoft-365-Tenant** – manchmal sauber betrieben, manchmal während der Pandemie in drei Tagen für Videokonferenzen aufgesetzt und seitdem nie wieder angefasst. Mit Gastzugängen, die niemand mehr zuordnen kann.

- **Eine eigene Arbeitnehmervertretung** mit eigenen Dienst- oder Betriebsvereinbarungen zu IT-Systemen, je nach Trägerschaft Betriebsrat, Personalrat oder MAV.

Das ist keine Mängelliste, das ist der Normalzustand. Die Frage ist nicht, ob diese Vielfalt existiert, sondern wie lange Sie sie parallel betreiben wollen und in welche Richtung sie sich entwickeln soll.

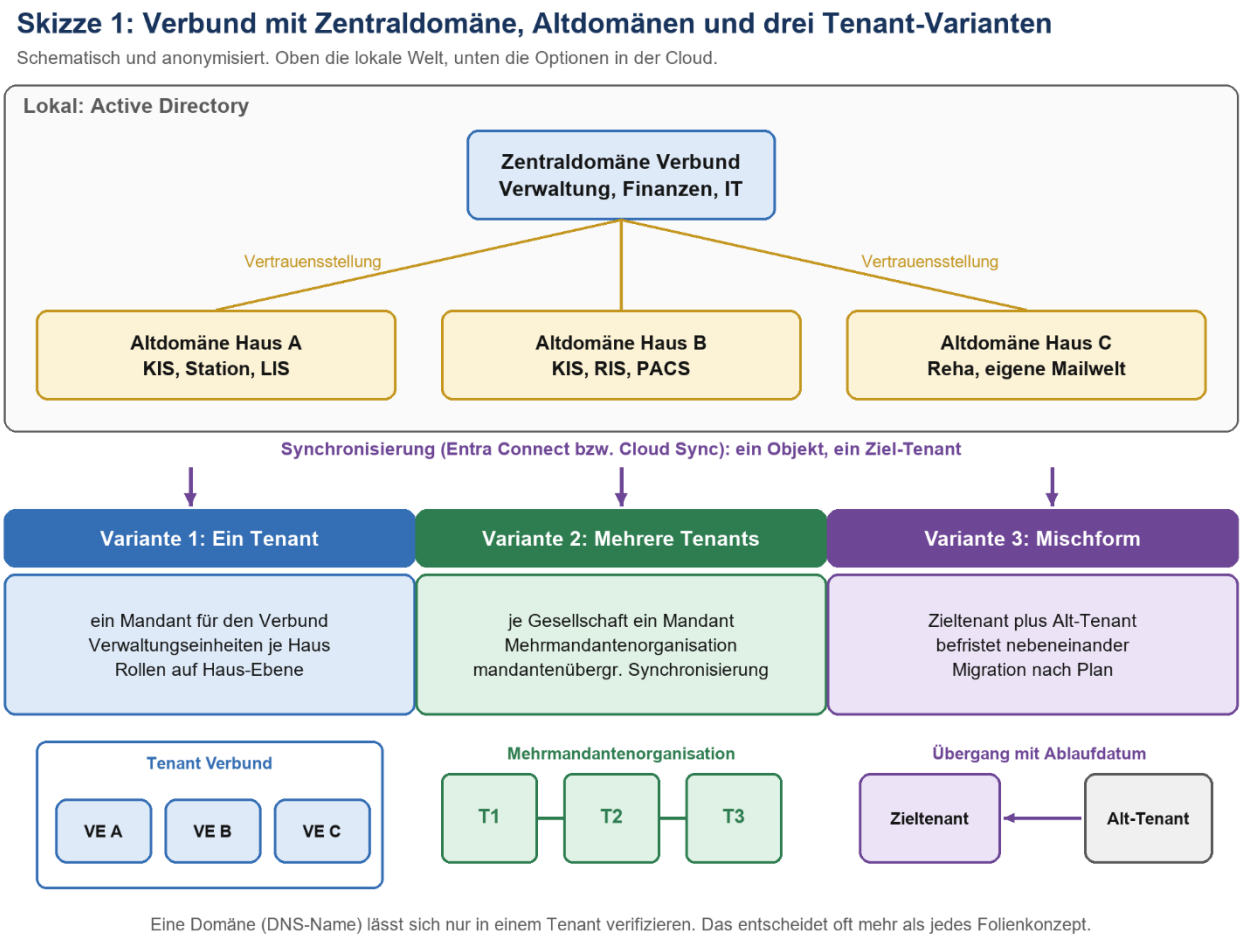
Die Grundhaltung: Microsoft 365 ist nicht das KIS

Bevor es um Tenants geht, eine Klarstellung, die in jedem Beitrag dieser Serie steht und hier besonders wichtig ist: Patientendaten gehören ins KIS und seine Subsysteme. Microsoft 365 ist das Werkzeug für Verwaltung, Organisation, Qualitätsmanagement und Zusammenarbeit. Die Tenant-Frage betrifft also vor allem Postfächer, Gremien-Teams, QM-Handbücher, Verfahrensanweisungen, Controlling-Auswertungen und Dienstplan-Absprachen. Das KIS bleibt, wo es ist, und folgt seinem eigenen Integrationsfahrplan.

Ja, wir wissen auch, dass in so manchem Teams-Kanal eine Excel-Liste mit Patientennamen für die Bettenbelegung oder die Entlassplanung liegt. Wer zwei Häuser in einen Tenant zusammenführt, führt diese Listen gleich mit zusammen – und vergrößert damit den Kreis derer, die sie theoretisch finden können. Das ist kein Argument gegen den gemeinsamen Tenant, aber ein starkes Argument dafür, vor der Zusammenführung aufzuräumen. Wo die Grenze verläuft, beschreibt der Beitrag Patientendaten und Microsoft 365: Wo das KIS endet und das Office anfängt.

Warnung: Excel-Listen mit Patientenbezug wandern mit

Bei jeder Tenant-Zusammenführung und jeder Migration werden auch Inhalte bewegt, die dort nie hätten liegen dürfen. Lassen Sie vor der Migration die Teams, SharePoint-Websites und OneDrive-Bereiche der betroffenen Häuser auf Patientenbezug prüfen – mit Purview-Klassifizierung, Stichproben und vor allem mit Gesprächen auf Station und im Funktionsbereich. Was nicht mitmigriert wird, muss auch nicht erklärt werden.



Skizze 1: Lokale Domänenlandschaft eines Verbunds und die drei Tenant-Varianten (schematisch, anonymisiert)

Die drei Varianten im Überblick

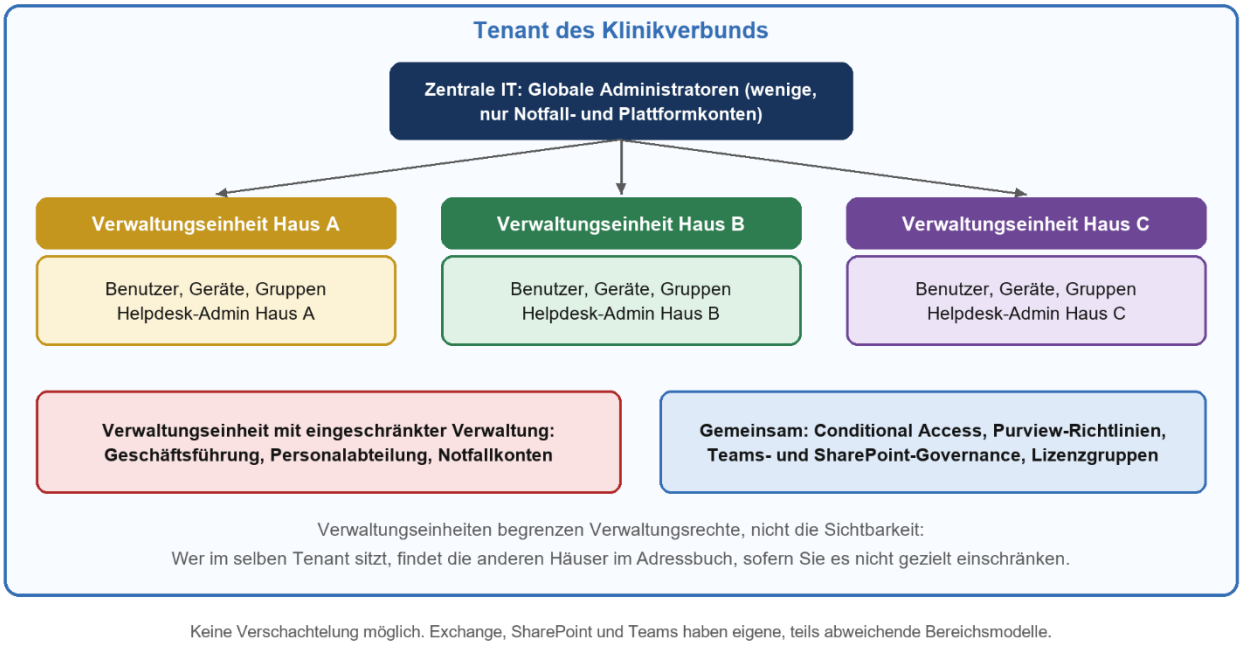
Für den Klinikverbund kommen im Kern drei Modelle infrage. Sie schließen sich nicht dauerhaft aus: Viele Verbünde starten in der Mischform und landen nach einigen Jahren bei einem der beiden anderen Modelle. Wichtig ist, dass das Ziel bewusst gewählt und dokumentiert wird, statt sich aus der Summe der letzten drei Übernahmen zu ergeben.

Variante 1: Ein gemeinsamer Tenant mit Verwaltungseinheiten je Haus

Alle Häuser und Gesellschaften teilen einen Tenant. Die Abgrenzung erfolgt über Verwaltungseinheiten (Administrative Units) in Microsoft Entra ID: Je Haus gibt es eine Verwaltungseinheit mit den Benutzern, Gruppen und Geräten dieses Standorts, und die lokale IT des Hauses erhält Rollen wie Helpdesk- oder Benutzeradministrator nur für diesen Bereich. Microsoft beschreibt genau dieses Szenario: Organisationen aus weitgehend selbstständigen Einheiten, deren IT-Teams nur ihre eigenen Benutzer verwalten sollen.

Für besonders schützenswerte Konten – Geschäftsführung, Personalabteilung, Notfallkonten – gibt es Verwaltungseinheiten mit eingeschränkter Verwaltung. Deren Objekte können selbst globale Administratoren mit Tenant-Bereich nicht ändern, solange sie sich nicht ausdrücklich für diese Einheit berechtigen; und genau das wird im Überwachungsprotokoll festgehalten. Die Einstellung muss beim Anlegen der Einheit gesetzt werden und lässt sich nachträglich nicht ändern.

Skizze 2: Ein Tenant, mehrere Häuser: Verwaltungseinheiten statt Mauern



Skizze 2: Ein Tenant für den Verbund, Abgrenzung über Verwaltungseinheiten

Fakten: Verwaltungseinheiten in Microsoft Entra ID

- Verwaltungseinheiten enthalten Benutzer, Gruppen und Geräte und begrenzen den Wirkungsbereich von Administratorrollen.
- Sie lassen sich nicht verschachteln. Ein Benutzer kann aber Mitglied mehrerer Einheiten sein, etwa „Haus B“ und „Verwaltung“.
- Sie begrenzen Verwaltungsrechte, nicht die Sichtbarkeit: Benutzer und Administratoren können mit ihren Standardrechten weiterhin andere Benutzer und Gruppen im Verzeichnis sehen.
- Lizenz: Microsoft Entra ID P1 für jeden Administrator mit Rolle im Bereich einer Verwaltungseinheit; für Mitglieder genügt Free, außer bei dynamischer Mitgliedschaft – dann P1 für jedes Mitglied.
- Verwaltungseinheiten mit eingeschränkter Verwaltung: höchstens 100 je Tenant; Funktionen von Entra ID Governance wie Zugriffsüberprüfungen oder Lebenszyklus-Workflows greifen für ihre Mitglieder nicht.

Der Haken: Verwaltungseinheiten sind ein Entra-Konstrukt. Exchange Online, SharePoint, Teams, Intune und Purview haben eigene, teils abweichende Bereichsmodelle – Verwaltungsbereiche in Exchange, Bereichs-Tags in Intune, Verwaltungseinheiten in Purview, Website-Administratoren in SharePoint. Ein „Haus-Administrator“, der nur sein Haus sieht, ist deshalb kein Häkchen, sondern ein Berechtigungskonzept über mehrere Dienste. Ein globaler Administrator bleibt global; mit ihm sollten Sie sparsam umgehen wie mit Betäubungsmitteln: wenige, dokumentiert, doppelt verschlossen.

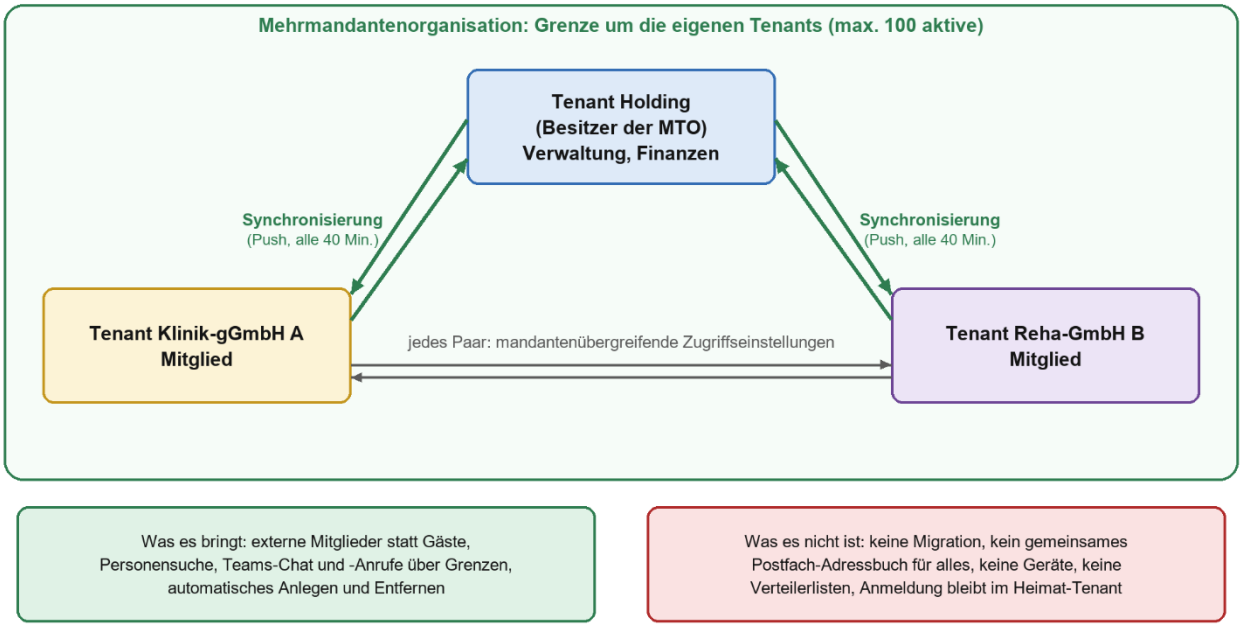
Variante 2: Mehrere Tenants als Mehrmandantenorganisation

Jede Gesellschaft – oder jede Gruppe von Gesellschaften mit gemeinsamer Verantwortung – behält ihren eigenen Tenant. Damit die Zusammenarbeit trotzdem funktioniert, verbinden Sie die

Tenants zu einer Mehrmandantenorganisation (Multitenant Organization, MTO). Ein Tenant legt sie als Besitzer an, die anderen treten bei; ab dann gelten die Tenants als zusammengehörig. Microsoft betont dabei das Prinzip der Gleichrangigkeit: Jeder Tenant-Administrator behält die Kontrolle über seinen Tenant und kann die Organisation jederzeit verlassen.

Die eigentliche Arbeit erledigt die mandantenübergreifende Synchronisierung (Cross-Tenant Synchronization). Sie legt die Benutzer eines Quell-Tenants automatisch als B2B-Benutzer im Ziel-Tenant an, aktualisiert sie und entfernt sie wieder, wenn sie den Bereich verlassen. Standardmäßig werden sie als „externe Mitglieder“ angelegt, nicht als Gäste. Das klingt nach Wortklauberei, ist aber für Teams, Personensuche und Richtlinien ein deutlicher Unterschied. Zusammen ergeben MTO und Synchronisierung das, was viele sich unter „ein Verbund, mehrere Tenants“ vorstellen: Die Ärztin aus Haus A findet den Controller der Holding in Teams, chattet mit ihm, ohne den Tenant umständlich zu wechseln, und verliert den Zugriff automatisch, wenn sie das Haus verlässt.

Skizze 3: Mehrere Tenants als Mehrmandantenorganisation



Skizze 3: Mehrere Tenants, verbunden als Mehrmandantenorganisation mit gegenseitiger Synchronisierung

Fakten: Mehrmandantenorganisation und Synchronisierung laut Microsoft Learn (Stand Oktober 2026)

- Ein Tenant kann genau einer Mehrmandantenorganisation angehören; bis zu 100 aktive Tenants je Organisation.
- Lizenz: Microsoft Entra ID P1 – je Person eine P1-Lizenz je Mehrmandantenorganisation, mindestens eine P1-Lizenz je Tenant. Für die Synchronisierung von Benutzern braucht jeder synchronisierte Benutzer P1 im Quell-Tenant; für die Synchronisierung von Gruppen ist Entra ID Governance oder die Entra Suite nötig.
- Die Synchronisierung ist ein Push vom Quell- in den Ziel-Tenant, startet in festen Abständen von 40 Minuten und überträgt Benutzer und Sicherheitsgruppen – keine Geräte, keine Kontakte, keine Verteilerlisten, keine Microsoft-365-Gruppen im Ziel.
- Synchronisiert werden nur interne Mitglieder des Quell-Tenants, keine Gäste. Die Anmeldung findet immer im Heimat-Tenant statt.
- Microsoft stellt klar: Die mandantenübergreifende Synchronisierung ist kein

Migrationswerkzeug.

Die Grenzen sollte man kennen, bevor man der Geschäftsführung „nahtlose Zusammenarbeit“ verspricht. Ein externes Mitglied ist technisch immer noch ein B2B-Konto. Freigaben, Teams-Mitgliedschaften und Berechtigungen funktionieren, aber nicht jede Anwendung behandelt externe Mitglieder wie interne. Ein gemeinsamer Exchange-Adressbuch-Raum mit Ressourcenpostfächern, Verteilerlisten und Frei/Gebucht-Informationen über alle Häuser entsteht nicht von selbst, sondern braucht zusätzliche Konfiguration auf Exchange-Seite. Und jede Richtlinie – bedingter Zugriff, Aufbewahrung, Vertraulichkeitsbezeichnungen – gibt es so oft, wie es Tenants gibt. Wer drei Tenants betreibt, betreibt drei Sicherheitskonfigurationen. Das ist keine Katastrophe, aber eine Daueraufgabe.

Variante 3: Die Mischform für die Übergangszeit

Die ehrlichste Variante ist die, die in der Praxis am häufigsten vorkommt: Ein Zieltenant ist definiert, ein übernommenes Haus bringt seinen eigenen Tenant mit, und beide laufen für eine begrenzte Zeit nebeneinander. In dieser Zeit sorgen B2B-Zusammenarbeit oder eine vorläufige Mehrmandantenorganisation dafür, dass man sich findet und gemeinsam arbeiten kann. Parallel werden Postfächer, OneDrive-Inhalte, SharePoint-Websites und Teams geordnet in den Zieltenant verschoben. Am Ende wird der Alt-Tenant stillgelegt.

Das Wort, auf das es ankommt, ist „begrenzt“. Eine Mischform ohne Enddatum ist keine Übergangslösung, sondern eine dauerhafte Variante 2 ohne deren Konzept. Legen Sie deshalb gleich zu Beginn fest, wer über das Ende entscheidet, woran man es erkennt und was passiert, wenn es sich verschiebt. Ein Termin im Gremium hilft. Ein Termin, an dem auch die Lizenzverträge des Alt-Tenants auslaufen, hilft noch mehr.

Fakten: Mandantenübergreifende Migration von Postfächern und OneDrive

Microsoft bietet für den Umzug zwischen Tenants eine eigene Postfach- und OneDrive-Migration an. Sie setzt je migriertem Benutzer eine einmalige Zusatzlizenz „Cross Tenant User Data Migration“ voraus, die im Quell- oder im Ziel-Tenant zugewiesen werden kann; ohne sie schlägt die Migration fehl. Teams-Besprechungen müssen nach dem Umzug neu angelegt werden, weil ihre Links im Ziel-Tenant ungültig sind. Prüfen Sie die aktuellen Voraussetzungen vor der Planung auf der Seite

Mandantenübergreifende Postfachmigration bei Microsoft Learn

.

Die Varianten im direkten Vergleich

Variante	Vorteile	Nachteile	Passt zu
Ein Tenant mit Verwaltungseinheiten	Eine Sicherheitskonfiguration, ein Adressbuch, eine Teams- und SharePoint-Landschaft; Lizenzen und Richtlinien zentral; Zusammenarbeit ohne B2B-Umwege;	Herauslösen eines Hauses bei Verkauf aufwendig; Abgrenzung nur über Rollen und Berechtigungen; gemeinsame Sichtbarkeit im Verzeichnis; Datenschutz zwischen Gesellschaften muss	Verbünde mit gemeinsamer IT-Gesellschaft, stabiler Struktur, einheitlicher Trägerschaft und geringer Verkaufswahrscheinlichkeit.

Variante	Vorteile	Nachteile	Passt zu
	Copilot und Suche sehen den ganzen Verbund (Vorteil und Risiko zugleich).	vertraglich und organisatorisch abgesichert werden.	
Mehrere Tenants als Mehrmandantenorganisation	Klare Trennung je Gesellschaft; Verkauf oder Ausgliederung ohne Datenmigration; eigene Verantwortung und eigene Admins; Zusammenarbeit über externe Mitglieder dennoch komfortabel.	Mehrfache Richtlinien, Lizenzverträge und Sicherheitskonfigurationen; Zusammenarbeit bleibt B2B mit Einschränkungen; zusätzliche Lizenzanforderungen für Synchronisierung; höherer Betriebsaufwand.	Verbünde aus eigenständigen Gesellschaften, unterschiedlichen Trägerschaften oder mit absehbaren Portfolio-Bewegungen.
Mischform mit Zieltenant und befristetem Alt-Tenant	Arbeitsfähigkeit vom ersten Tag; Migration in eigenem Tempo; Zeit zum Aufräumen und zur Klärung mit Gremien.	Doppelter Betrieb, doppelte Kosten, doppelte Angriffsfläche; Gefahr des Dauerprovisoriums; Benutzer leben zeitweise in zwei Welten.	Jede frische Übernahme, bis das Zielbild steht und die Migration abgeschlossen ist.

Die Kriterien: Wer entscheidet eigentlich über die Zahl der Tenants?

Die Tenant-Frage wird gern in der IT-Abteilung entschieden, weil sie dort zuerst auftaucht. Das ist nachvollziehbar und trotzdem falsch. Die maßgeblichen Kriterien liegen bei Geschäftsführung, Träger, Datenschutz und Gremien. Die IT liefert die Optionen und die Folgen, nicht die Antwort.

Trägerrecht und Gesellschaftsstruktur

Wem gehören die Häuser, und wie sind sie organisiert? Ein kommunaler Verbund mit einer Holding und mehreren Tochter-gGmbHs, ein kirchlicher Träger mit rechtlich selbstständigen Einrichtungen, ein privater Konzern mit Dutzenden Klinik-GmbHs – jede dieser Strukturen hat eigene Regeln dafür, was die Mutter darf und was die Tochter selbst entscheiden muss. Bei kommunalen Trägern kommen kommunalrechtliche Vorgaben hinzu, bei kirchlichen Trägern das kirchliche Datenschutzrecht. Wie unterschiedlich das aussehen kann, zeigen die Beiträge Microsoft 365 im kirchlichen Krankenhaus: KDG, DSG-EKD und die MAV am Tisch und – für die kommunale Seite – der Kompetenzbereich Microsoft 365 in der öffentlichen Verwaltung.

Datenschutz zwischen Gesellschaften

Im Datenschutzrecht gibt es kein Konzernprivileg. Wenn Haus A und Haus B eigenständige Gesellschaften sind, ist die Übermittlung personenbezogener Daten zwischen ihnen rechtfertigungsbedürftig – auch dann, wenn beide im selben Tenant liegen und es technisch nur ein Klick ist. Ein gemeinsamer Tenant braucht deshalb ein Gerüst aus Verträgen: Auftragsverarbeitung, wenn eine IT-Gesellschaft für alle Häuser betreibt, gegebenenfalls Vereinbarungen über gemeinsame Verantwortlichkeit für gemeinsam genutzte Verzeichnisse und Kollaborationsräume, und klare Regeln, wer auf welche Daten zugreifen darf. Für Inhalte, die der

Schweigepflicht unterliegen, gelten zusätzlich die Anforderungen aus § 203 StGB und aus dem jeweiligen Landeskrankenhausgesetz; die Einzelheiten unterscheiden sich je Bundesland erheblich. Mehr dazu im Beitrag Schweigepflicht und Cloud: § 203 StGB, Landeskrankenhausgesetze und Auftragsverarbeitung.

Wichtig: Keine Rechtsberatung

Ob ein gemeinsamer Tenant für rechtlich selbstständige Krankenhausgesellschaften zulässig ist und welche Verträge dafür nötig sind, hängt von Gesellschaftsstruktur, Trägerschaft, Landesrecht und gegebenenfalls kirchlichem Datenschutzrecht ab. Dieser Beitrag beschreibt technische Optionen und typische Fragen. Die rechtliche Bewertung gehört zu Ihrem Datenschutzbeauftragten, zur Rechtsabteilung des Trägers oder zu einer spezialisierten Kanzlei.

Gemeinsame IT oder getrennte IT

Ein gemeinsamer Tenant ohne gemeinsame IT ist wie eine gemeinsame Station ohne gemeinsamen Dienstplan: theoretisch möglich, praktisch eine Quelle ständiger Missverständnisse. Gibt es eine zentrale IT-Gesellschaft oder Abteilung, die für alle Häuser Verantwortung übernimmt, spricht vieles für Variante 1. Arbeiten die Häuser mit eigenen IT-Teams, eigenen Dienstleistern und eigener Rufbereitschaft, wird ein gemeinsamer Tenant zur Dauerbaustelle der Abstimmung – oder zur Machtfrage, wer globaler Administrator sein darf. Dann sind mehrere Tenants mit klarer Zusammenarbeit oft die ehrlichere Lösung.

Dazu kommt die Sicherheitsverantwortung. Krankenhäuser müssen nach § 391 SGB V angemessene Vorkehrungen für ihre IT-Sicherheit treffen; seit dem NIS2-Umsetzungsgesetz vom 6. Dezember 2025 gilt die Vorschrift in neuer Fassung, und für Betreiber kritischer Anlagen treten an ihre Stelle die Pflichten des BSIG. Der branchenspezifische Sicherheitsstandard „Medizinische Versorgung“ der DKG liegt in Version 1.3.1 vom 10. Oktober 2025 vor. In einem gemeinsamen Tenant ist ein Sicherheitsvorfall in Haus C potenziell auch ein Vorfall in Haus A. Wer die Verantwortung dafür trägt, muss vor der Zusammenführung geklärt sein. Einzelheiten im Beitrag NIS2, § 391 SGB V und B3S: Was die Sicherheitspflichten für Microsoft 365 bedeuten.

Wie wahrscheinlich ist ein Verkauf oder eine Ausgliederung?

Die unbequemste Frage, und deshalb die, die am häufigsten übersprungen wird. Niemand plant gern den Ausstieg, während der Einstieg noch gefeiert wird. Aber die Krankenhauslandschaft ist in Bewegung: Standorte werden zusammengelegt, Häuser in Gesundheitszentren umgewandelt, an andere Träger abgegeben oder in neue Gesellschaften ausgegliedert. Wenn ein Haus in einem gemeinsamen Tenant lebt, heißt Verkauf: Postfächer, OneDrive-Inhalte, SharePoint-Websites, Teams und Identitäten herauslösen, Domäne aus dem Tenant entfernen, Richtlinien im neuen Tenant nachbauen. Ein Projekt von vielen Monaten, das unter Zeitdruck läuft, weil der Kaufvertrag einen Stichtag hat. Mit einem eigenen Tenant heißt Verkauf: Mehrmandantenorganisation verlassen, Synchronisierung beenden, fertig – zumindest auf Microsoft-365-Seite.

Tipp: Den Ausstieg in die Vorlage für die Geschäftsführung schreiben

Nehmen Sie in jede Entscheidungsvorlage zur Tenant-Strategie einen Absatz „Was passiert bei Verkauf oder Ausgliederung eines Hauses?“ auf, mit grober Aufwandsschätzung für jede Variante. Nicht, weil der Verkauf wahrscheinlich ist, sondern weil die Geschäftsführung die Folgekosten der Integration erst dann wirklich bewerten kann. Wie eine solche Vorlage in einer kompakten Konzeptionsphase entsteht, beschreibt die

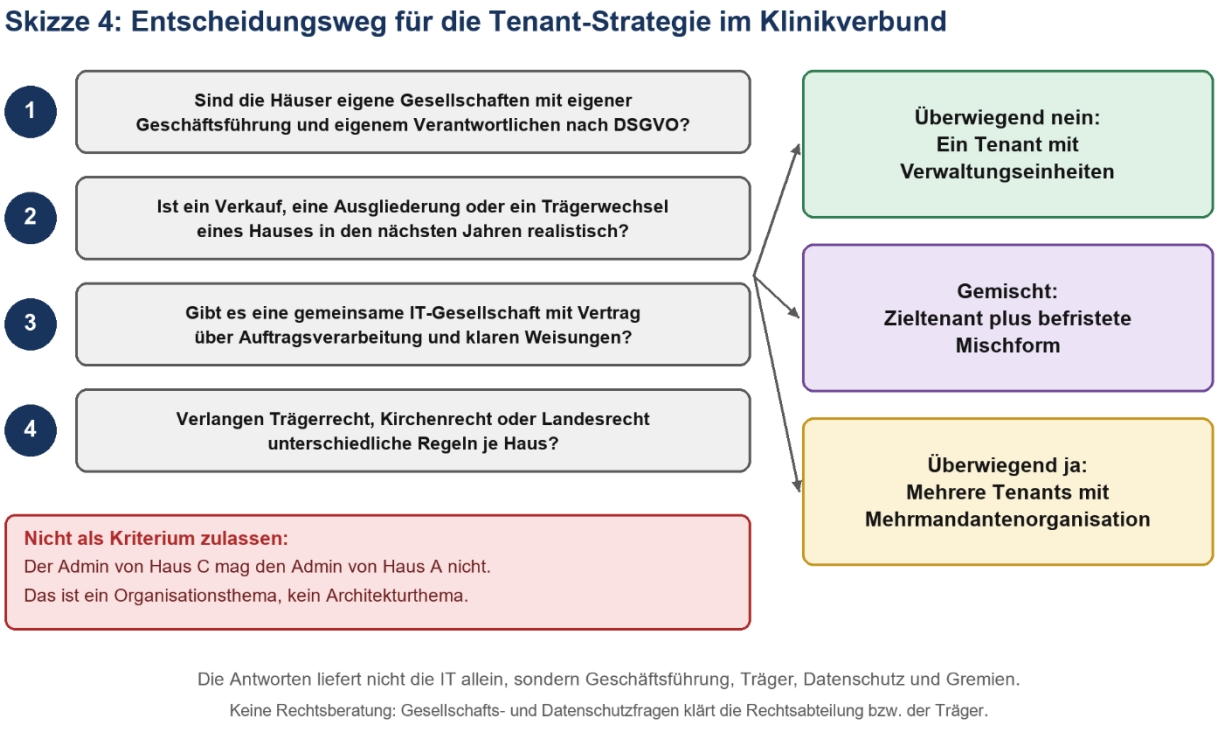
Microsoft-365-Beratung für Krankenhäuser

.

Arbeitnehmervertretung, Lizenzen und Landesrecht

Ein gemeinsamer Tenant bedeutet häufig auch: gemeinsame Auswertungsmöglichkeiten über Gesellschaftsgrenzen hinweg, etwa in Überwachungsprotokollen oder Nutzungsberichten. Das berührt die Mitbestimmung, und zwar je Gesellschaft: Ein Haus mit Betriebsrat, eines mit Personalrat und eines mit MAV können zu drei unterschiedlichen Vereinbarungen führen. Das Personalvertretungsrecht ist zudem Landesrecht und unterscheidet sich je Bundesland. Wer hier früh alle Gremien an einen Tisch holt, spart später Monate; mehr dazu im Beitrag Betriebsrat, Personalrat oder MAV: Mitbestimmung bei Microsoft 365 je nach Trägerschaft. Bei den Lizenzen gilt: Mehrere Tenants bedeuten mehrere Verträge oder zumindest eine sorgfältige Zuordnung, und ob Nonprofit-Angebote für gemeinnützige Gesellschaften greifen, prüft Microsoft je Organisation. Der Beitrag Lizenzen im Krankenhaus: Frontline für die Pflege, Vollausstattung für die Verwaltung ordnet das ein.

Und dann ist da noch § 393 SGB V: Seit dem 1. Juli 2025 dürfen Sozial- und Gesundheitsdaten in Cloud-Diensten nur verarbeitet werden, wenn ein aktuelles C5-Typ-2-Testat oder ein nach der Verordnung gleichwertiges Testat oder Zertifikat vorliegt. Das gilt unabhängig davon, ob Sie einen oder fünf Tenants betreiben. Welche Microsoft-Dienste von welchem Testat erfasst sind, prüfen Sie im Service Trust Portal und dokumentieren es – für jeden Tenant und jeden Dienst, den Sie dort für solche Daten vorsehen. Der Beitrag § 393 SGB V und C5-Testat: Was Krankenhäuser beim Cloud-Einsatz nachweisen müssen beschreibt den Nachweis.



Skizze 4: Entscheidungsweg mit den vier Leitfragen für die Tenant-Strategie

Kriterium	Spricht für einen Tenant	Spricht für mehrere Tenants
Gesellschaftsstruktur	eine Gesellschaft oder enge Organschaft mit zentraler Steuerung	mehrere eigenständige Gesellschaften mit eigener Geschäftsführung

Kriterium	Spricht für einen Tenant	Spricht für mehrere Tenants
Trägerschaft	einheitlicher Träger, einheitliches Datenschutzregime	gemischte Trägerschaften, kirchliches und staatliches Datenschutzrecht nebeneinander
IT-Organisation	zentrale IT-Gesellschaft mit Auftragsverarbeitung für alle Häuser	eigene IT je Haus, eigene Dienstleister, eigene Rufbereitschaft
Portfolio	langfristig stabiler Verbund	absehbare Verkäufe, Ausgliederungen oder Kooperationen auf Zeit
Zusammenarbeit	viele hausübergreifende Gremien, Kommissionen, gemeinsames QM	Zusammenarbeit punktuell, überwiegend über Holding und Verwaltung
Mitbestimmung	eine Arbeitnehmervertretung oder Konzern- bzw. Gesamtvereinbarung	unterschiedliche Gremien und Rechtsgrundlagen je Haus

Die lokale Seite: Domänen, Vertrauensstellungen und Teilmigrationen

Wer nur über Tenants spricht, hat die Hälfte vergessen. In fast jedem Klinikverbund ist das lokale Active Directory die eigentliche Quelle der Identitäten, und dort sieht die Welt selten so aufgeräumt aus wie im Entra Admin Center. Eine Zentraldomäne des Verbunds, mehrere Altdomänen der übernommenen Häuser, dazwischen Vertrauensstellungen – teils sauber eingerichtet, teils als „vorübergehende“ Lösung, die inzwischen ihr zehnjähriges Jubiläum feiert.

Vertrauensstellungen sind eine Brücke, keine Wohnung

Vertrauensstellungen zwischen Domänen oder Gesamtstrukturen sind das klassische Werkzeug, um nach einer Übernahme schnell arbeitsfähig zu werden: Benutzer aus der Zentraldomäne erhalten Zugriff auf Dateiserver und Anwendungen im übernommenen Haus und umgekehrt. Das ist legitim und oft der richtige erste Schritt. Problematisch wird es, wenn die Vertrauensstellung zur Dauerlösung wird. Dann erbt die Zentraldomäne die Altlasten des Hauses: schwache Kennwortrichtlinien, NTLM-Abhängigkeiten, Dienstkonten mit zu vielen Rechten. Ein Angreifer, der in der Altdomäne Fuß fasst, sucht als Erstes genau diese Brücke.

Praktisch heißt das: Vertrauensstellungen so eng wie möglich konfigurieren – selektive Authentifizierung, SID-Filterung, nur die Richtung, die wirklich gebraucht wird – und mit einem Ablaufdatum versehen. Und parallel die Authentifizierung modernisieren: Kerberos statt NTLM, wo immer es geht, saubere Dienstprinzipalnamen, eine PKI, die über Domänengrenzen hinweg vertrauenswürdige Zertifikate ausstellt. Die Kompetenzbereiche Kerberos und PKI mit ADCS beschreiben die Grundlagen.

Mehrere Gesamtstrukturen, ein Tenant

Für Variante 1 ist die gute Nachricht: Mehrere AD-Gesamtstrukturen in einen Tenant zu synchronisieren, ist ein unterstützter Standardfall für Entra Connect und Cloud Sync. Sie müssen die Häuser also nicht erst lokal konsolidieren, bevor sie den gemeinsamen Tenant nutzen können. Wichtig ist, dass jede Person genau einmal im Tenant erscheint. Wer in mehreren Domänen ein Konto hat – etwa ein Arzt mit Konto im Stammhaus und im Partnerhaus –, braucht eine klare Regel, welches Konto das führende ist. Sonst sitzen im Tenant zwei Dr. Müller, und beide bekommen eine Lizenz.

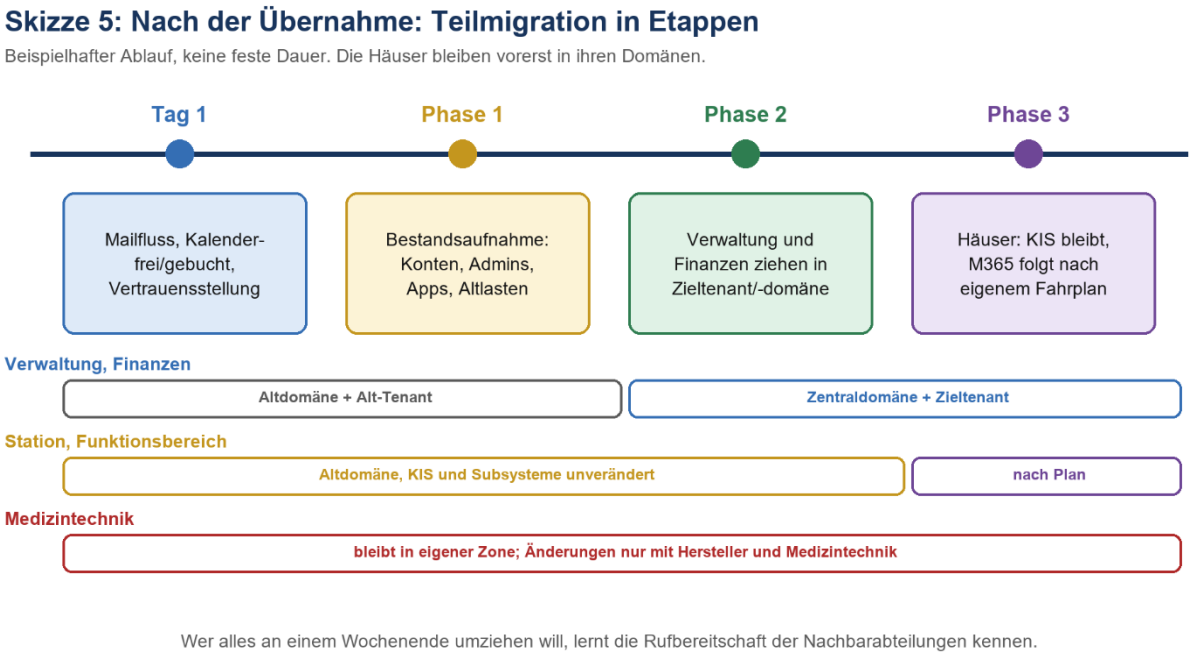
Umgekehrt gilt: Eine Gesamtstruktur in mehrere Tenants zu synchronisieren, ist nur eingeschränkt möglich, und ein einzelnes Objekt landet grundsätzlich in genau einem Tenant. Wenn Sie also

Variante 2 wählen, muss sich die lokale Struktur daran orientieren – oder Sie trennen über Organisationseinheiten und Filter sehr sauber, welches Konto wohin gehört.

Teilmigration: Verwaltung und Finanzen ziehen um, die Häuser bleiben

In der Praxis ist die Teilmigration oft der klügste Weg. Verwaltung, Finanzwesen, Personalabteilung, Controlling und Einkauf werden ohnehin zentralisiert und arbeiten künftig mit der Holding zusammen. Sie ziehen in die Zentraldomäne und in den Zieltenant. Die Häuser mit Station, Funktionsbereich und KIS bleiben vorerst in ihren Domänen – denn dort hängen KIS, Subsysteme und Medizintechnik dran, und eine Domänenmigration im laufenden Klinikbetrieb ist etwas, das man nicht nebenbei macht.

Technisch bedeutet das: Die Benutzer der Häuser werden aus ihren Altdomänen in den gemeinsamen Tenant synchronisiert, während die Verwaltung bereits aus der Zentraldomäne kommt. Für Microsoft 365 sehen beide gleich aus. Das KIS merkt davon nichts. Die lokale Konsolidierung der Häuser folgt später, eigenständig geplant, mit Herstellern, Medizintechnik und einem Notfallkonzept.



Skizze 5: Teilmigration in Etappen – Verwaltung zuerst, Häuser nach eigenem Fahrplan

Tipp: Exchange Hybrid nicht unterschätzen

Wenn ein übernommenes Haus noch ein lokales Exchange betreibt, ist der Weg über Exchange Hybrid in den Zieltenant meist planbarer als ein Umweg über den Alt-Tenant. Aber: Eine lokale Exchange-Organisation wird in aller Regel mit genau einem Tenant hybrid verbunden, Konstellationen mit mehreren Tenants sind nur eingeschränkt möglich. Klären Sie deshalb vor der Hybrid-Konfiguration, welcher Tenant das Ziel ist – sonst richten Sie die Brücke zum falschen Ufer ein.

Wichtig: Praxis: Begleitung eines Krankenhausverbunds mit mehreren Altdomänen

Aus der langjährigen Begleitung eines Krankenhausverbunds mit mehreren Standorten (anonymisiert): Der Verbund war über Jahre durch Übernahmen gewachsen, jeder Standort

brachte seine eigene Domäne mit. Verbunden waren sie über Vertrauensstellungen, die irgendwann für den Übergang eingerichtet worden waren – der Übergang hatte sich verstetigt.

- Erste Erkenntnis: Die Vertrauensstellungen waren breiter als nötig, und über sie lief noch erstaunlich viel NTLM. Bevor irgendetwas konsolidiert werden konnte, mussten die Anmeldewege sichtbar gemacht werden: Wer authentifiziert sich wo, mit welchem Protokoll, gegen welchen Dienst?
- Zweite Erkenntnis: Ein beträchtlicher Teil der Abhängigkeiten steckte in Klinik- und Medizintechnik-Anwendungen, die fest verdrahtete Konten und Namen verwendeten. Die Umstellung auf Kerberos und die Abschaltung von NTLM gelangen nur Schritt für Schritt, gemeinsam mit den Fachabteilungen und den Herstellern.
- Dritte Erkenntnis: Ohne eine saubere PKI geht nichts. Zertifikate für Server, Geräte und Anmeldung müssen über Domänengrenzen hinweg vertrauenswürdig sein. Der Aufbau und die Härtung der PKI waren deshalb kein Nebenprojekt, sondern Voraussetzung.
- Vierte Erkenntnis: Exchange Hybrid war der Taktgeber für die Cloud-Seite. Erst als klar war, welche Identität in welchem Tenant führend ist, ließ sich der Mailfluss sauber planen.

Die Lehre: Die Tenant-Entscheidung war der einfachere Teil. Die eigentliche Arbeit lag in der lokalen Identitätslandschaft – und die lässt sich nicht an einem Wochenende aufräumen.

Entra ID als Klammer

Welche Variante Sie auch wählen: Microsoft Entra ID ist die Klammer, die den Verbund in der Cloud zusammenhält. Bedingter Zugriff, privilegierte Rollen, Verwaltungseinheiten, mandantenübergreifende Zugriffseinstellungen, Synchronisierung, Lebenszyklus von Konten – all das entscheidet darüber, ob die gewählte Strategie im Alltag trägt. Einen Überblick über die Möglichkeiten und typische Stolpersteine bietet der Kompetenzbereich Microsoft Entra ID. Für die Sicherheitsseite, von Defender bis zum Schutz privilegierter Konten, lohnt der Blick in den Kompetenzbereich Microsoft 365 Security.

Warnung: Alt-Tenants nicht verwaisen lassen

Ein stillgelegter Alt-Tenant, in dem noch globale Administratoren ohne MFA, alte App-Registrierungen mit gültigen Geheimnissen und Gastkonten existieren, ist kein Archiv, sondern ein Einfallstor. Planen Sie die Stilllegung als eigenen Arbeitsschritt: Daten migrieren oder nach Aufbewahrungsregeln sichern, Konten deaktivieren, Domänen entfernen, Abonnements kündigen, Administratorzugänge dokumentiert übergeben – und erst dann löschen.

FAQ: Klinikverbund und Microsoft 365 Tenant

Ist ein einziger Tenant für den Klinikverbund immer die beste Lösung?

Nein. Ein gemeinsamer Tenant ist am einfachsten zu betreiben und ermöglicht die beste Zusammenarbeit. Er passt aber nur, wenn Gesellschaftsstruktur, Datenschutz, IT-Organisation und Portfolio-Planung dazu passen. Bei eigenständigen Gesellschaften, gemischten Trägerschaften oder absehbaren Verkäufen sind mehrere Tenants oft die ehrlichere Wahl.

Können verschiedene Krankenhausgesellschaften rechtlich überhaupt einen Tenant teilen?

Technisch ja, rechtlich hängt es vom Einzelfall ab. Es gibt kein Konzernprivileg im Datenschutz; Sie brauchen ein tragfähiges Vertragsgerüst und klare Zugriffsregeln. Die Bewertung gehört zu Datenschutzbeauftragtem und Rechtsabteilung, nicht zur IT allein.

Was unterscheidet eine Mehrmandantenorganisation von normaler Gastzusammenarbeit?

In einer Mehrmandantenorganisation erkennt Microsoft 365 die verbundenen Tenants als zusammengehörig. Synchronisierte Benutzer erscheinen als externe Mitglieder statt als Gäste, werden automatisch angelegt und entfernt und erhalten in Teams eine bessere mandantenübergreifende Erfahrung. Normale Gastzusammenarbeit arbeitet mit Einladungen und manueller Pflege.

Brauche ich für die Mehrmandantenorganisation zusätzliche Lizenzen?

Microsoft nennt Entra ID P1 als Voraussetzung, für die Synchronisierung von Gruppen Entra ID Governance oder die Entra Suite. Viele Enterprise-Pakete enthalten P1 bereits. Prüfen Sie den aktuellen Stand bei Microsoft vor der Planung, Preise nennen wir bewusst nicht.

Kann ich mit der mandantenübergreifenden Synchronisierung einen Tenant in einen anderen migrieren?

Nein. Microsoft stellt ausdrücklich klar, dass sie kein Migrationswerkzeug ist – die Benutzer melden sich weiterhin im Quell-Tenant an. Für Postfächer und OneDrive gibt es eine eigene mandantenübergreifende Migration mit Zusatzlizenz; für SharePoint und Teams kommen weitere Werkzeuge hinzu.

Müssen die Altdomänen der Häuser vor dem gemeinsamen Tenant aufgelöst werden?

Nein. Mehrere Gesamtstrukturen in einen Tenant zu synchronisieren, ist unterstützt. Die lokale Konsolidierung kann später und unabhängig erfolgen – was angesichts von KIS, Subsystemen und Medizintechnik meist auch sinnvoll ist.

Was passiert mit dem KIS, wenn wir den Tenant wechseln?

In aller Regel nichts. Das KIS und seine Subsysteme hängen am lokalen Active Directory und an der eigenen Infrastruktur, nicht am Microsoft-365-Tenant. Achten Sie aber auf Schnittstellen, etwa Mailversand aus Subsystemen oder Single Sign-on über Entra ID.

Wie lange darf eine Mischform dauern?

So lange wie nötig, so kurz wie möglich – und vor allem mit festem Enddatum. Eine Mischform ohne Ende ist kein Übergang, sondern eine Variante 2 ohne Konzept, mit doppelten Kosten und doppelter Angriffsfläche.

Betrifft die Tenant-Frage auch Teams-Telefonie?

Ja, am Rande. Teams-Telefonie ist im Krankenhaus in aller Regel eine Unteranlage für Verwaltung und ärztliche Leitungspositionen hinter der Klinik-TK-Anlage, die für Station, DECT, Zentrale und Patienten führend bleibt. Bei mehreren Tenants braucht jede Unteranlage ihre eigene Anbindung; mehr dazu unter Teams-Telefonie im Krankenhaus und in der Pflege.

Fazit: Erst die Struktur klären, dann den Tenant bauen

Die Tenant-Strategie eines Klinikverbunds ist keine IT-Entscheidung mit organisatorischen Folgen, sondern eine organisatorische Entscheidung mit IT-Folgen. Ein gemeinsamer Tenant mit

Verwaltungseinheiten ist die effizienteste Lösung für Verbünde mit gemeinsamer IT, stabiler Struktur und einheitlicher Trägerschaft. Mehrere Tenants als Mehrmandantenorganisation sind die robustere Lösung für eigenständige Gesellschaften und bewegliche Portfolios. Die Mischform ist legitim – wenn sie ein Enddatum hat.

Vergessen Sie die lokale Seite nicht. Vertrauensstellungen, Altdomänen, NTLM, Zertifikate und Exchange Hybrid entscheiden oft mehr über den Projekterfolg als die Wahl der Cloud-Variante. Und die Teilmigration – Verwaltung zuerst, Häuser nach eigenem Fahrplan – ist in vielen Verbünden der Weg, der den Klinikbetrieb am wenigsten stört. Wenn Sie die Tenant-Strategie für Ihren Verbund mit Geschäftsführung, Datenschutz und Gremien strukturiert erarbeiten möchten, unterstützt Sie die Microsoft-365-Beratung für Krankenhäuser; für Administratoren, die Verwaltungseinheiten, Mehrmandantenorganisation und Synchronisierung betreiben sollen, gibt es die Microsoft-365-Schulung für Krankenhäuser.

Weiter: Passende Beiträge und Kompetenzbereiche

› Schweigepflicht und Cloud: § 203 StGB, Landeskrankenhausgesetze und Auftragsverarbeitung

› NIS2, § 391 SGB V und B3S: Was die Sicherheitspflichten für Microsoft 365 bedeuten

› Microsoft 365 im kirchlichen Krankenhaus: KDG, DSG-EKD und die MAV am Tisch

› Microsoft Entra ID

› Kerberos

› PKI mit ADCS