

Hochschulübergreifend zusammenarbeiten: B2B, mandantenübergreifender Zugriff und Verbundprojekte

Microsoft 365 · Hochschule · Verbund

Hochschulübergreifend zusammenarbeiten: B2B, mandantenübergreifender Zugriff und Verbundprojekte

Forschung kennt keine Tenant-Grenzen. Entra ID leider schon.

B2B-Gastkonten Geteilte Kanäle Zugriffseinstellungen MFA-Vertrauen Mehrmandantenorganisation

Verbundprojekte Industriepartner

boddenberg.de

WISSEN

Alle Beiträge der Serie zu Microsoft 365 in Hochschule und Forschung an einem Ort.

› [Microsoft 365 in Hochschule und Forschung](#)

BERATUNG

Mandantenübergreifende Zusammenarbeit für Verbünde und gemeinsame Rechenzentren planen, mit Datenschutz und Personalrat am Tisch.

› [Beratung für Hochschulen und Forschung](#)

SCHULUNG

Für Rechenzentrum und Fakultäts-IT: Zugriffseinstellungen, Gastkonten und geteilte Kanäle sicher betreiben.

› [Schulungen für Hochschulen und Forschung](#)

Kein Verbundprojekt dieser Welt endet an der Grundstücksgrenze der eigenen Universität. Die Konsortialführung sitzt in der einen Stadt, das Teilprojekt mit den Messdaten an einer Hochschule für angewandte Wissenschaften im Nachbarland, das Leibniz-, Fraunhofer- oder Max-Planck-Institut mit dem Großgerät irgendwo dazwischen, und der Industriepartner möchte bitte alles sehen, aber nichts selbst hochladen. Dazu kommen gemeinsame Studiengänge zweier Hochschulen, Kooperationen mit Kunst- und Musikhochschulen, Graduiertenkollegs mit Doktoranden aus drei Häusern und gemeinsame Rechenzentren, die mehrere Hochschulen eines Landes versorgen.

Microsoft 365 hat dafür eine eigentlich gute Antwort und ein strukturelles Problem. Die Antwort heißt B2B: Gastkonten, direkte Verbindungen, mandantenübergreifende Zugriffseinstellungen und, für Einrichtungen mit mehreren eigenen Tenants, die Mehrmandantenorganisation. Das Problem: Ein Tenant ist laut Microsoft-Dokumentation aus Sicht von Microsoft 365 die Standardgrenze für Zusammenarbeit und Lizenzierung. Wer drüber will, braucht eine Tür. Und jede Tür, die das Rechenzentrum nicht selbst einbaut, baut ein Lehrstuhl mit dem Knopf »Gast hinzufügen« ein, gern im Freitagnachmittagsmodus.

Dieser Beitrag gehört zur Serie [Microsoft 365 in Hochschule und Forschung](#). Er sortiert die Werkzeuge, ordnet sie typischen Szenarien im Hochschul- und Forschungsbetrieb zu, beantwortet die Frage nach einem gemeinsamen oder mehreren Tenants und zeigt, wo Datenschutz und Personalrat ins Spiel kommen. Allgemeinbildende Schulen und Universitätsklinikum haben eigene Rahmenbedingungen und bleiben hier außen vor.

FAKTEN · Das Wichtigste in fünf Sätzen

B2B-Zusammenarbeit mit anderen Entra-ID-Organisationen ist ab Werk erlaubt, die direkte B2B-Verbindung ab Werk blockiert.

Die direkte B2B-Verbindung funktioniert nur mit geteilten Kanälen in Teams, und Microsoft plant laut eigener Dokumentation keine Erweiterung auf andere Dienste.

Mit den mandantenübergreifenden Zugriffseinstellungen legen Sie pro Partner fest, wer hinein und hinaus darf und ob Sie dessen MFA- und Geräteansprüchen vertrauen.

Synchronisierung und Mehrmandantenorganisation sind für Tenants derselben Organisation gedacht, nicht für den Verbundpartner von nebenan.

Gäste kommen leicht herein und gehen schwer wieder. Das Enddatum gehört deshalb an den Anfang jedes Projekts.

Warum der Campus nie an der Tenant-Grenze endet

Unternehmen arbeiten auch mit Partnern, aber selten so dauerhaft, so gleichberechtigt und so unübersichtlich wie Hochschulen. In der Wissenschaft ist die Zusammenarbeit über Organisationsgrenzen nicht die Ausnahme, sondern das Geschäftsmodell. Drittmittelgeber verlangen Verbünde, Berufungsverfahren holen Professoren mit laufenden Projekten an anderen Häusern, und Gastwissenschaftler bringen ihr Heimatkonto mit. Wer im Rechenzentrum sitzt, kennt die typischen Konstellationen:

- **Verbundforschung:** mehrere Hochschulen und außeruniversitäre Institute, eine Konsortialführung, eine gemeinsame Ablage, eine Laufzeit mit Enddatum, das spätestens bei der Verlängerung niemand mehr kennt.
- **Gemeinsame Studiengänge:** Dozenten beider Hochschulen, Studenten mit Immatrikulation an der einen und Lehrveranstaltungen an der anderen, ein Prüfungsamt, das genau wissen will, wer welche Noten sieht.
- **Gemeinsame Rechenzentren:** eine Einrichtung betreibt Dienste für mehrere Hochschulen, etwa ein Landesrechenzentrum oder ein Verbund kleinerer Häuser, und stellt sich die Frage, ob dafür ein Tenant reicht.
- **Industriepartner:** Kooperationsverträge, Geheimhaltungsvereinbarungen, manchmal Exportkontrolle, und ein Partner mit eigener Entra-ID-Welt und eigenen Vorstellungen über MFA.
- **Einzelpersonen:** Gastwissenschaftler, Lehrbeauftragte und Emeriti, die mal mit Konto einer anderen Einrichtung, mal mit privater Adresse kommen.

Die Einzelpersonen behandelt ein eigener Beitrag der Serie ausführlich: [Gastwissenschaftler, Lehrbeauftragte, Emeriti: Sonderrollen in Entra ID sauber abbilden](#). Hier geht es um die Beziehungen zwischen Organisationen, also um die Frage, welche Tür zwischen zwei Tenants die richtige ist und wer sie abschließt, wenn das Projekt vorbei ist.

WARNUNG · Der Standard ist offen

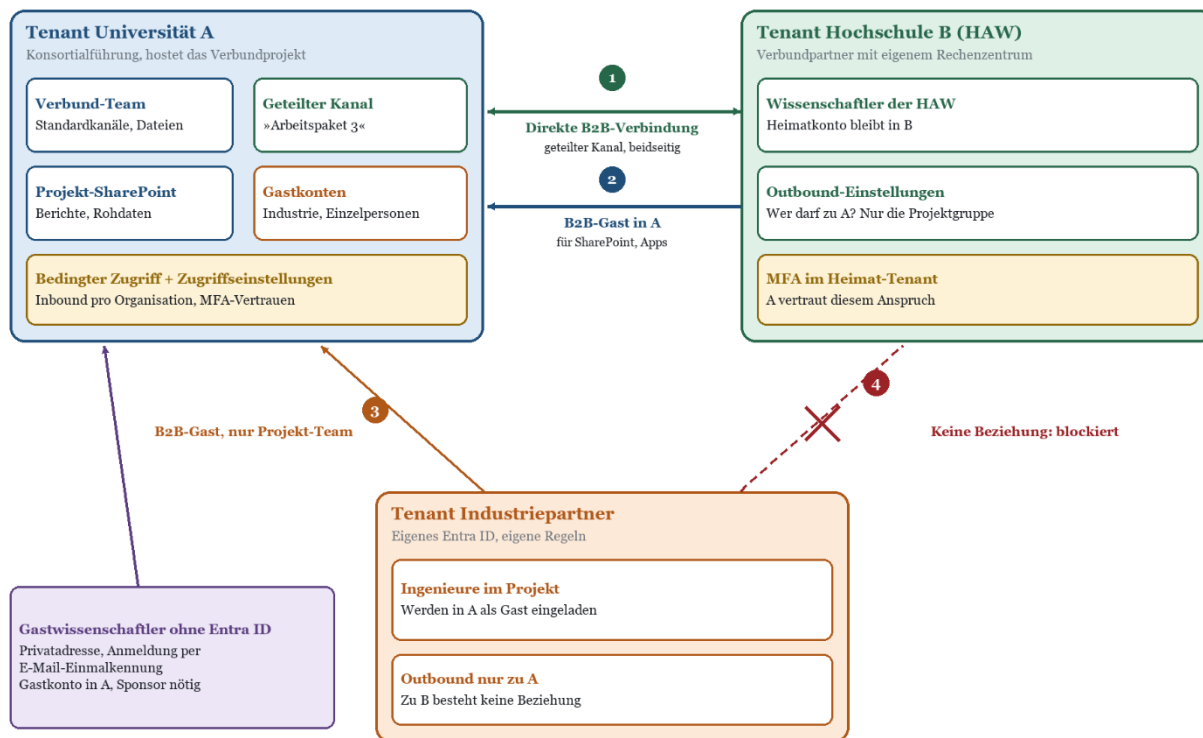
Ab Werk dürfen alle internen Konten Ihres Tenants mit allen anderen Entra-ID-Organisationen per B2B zusammenarbeiten: Ihre Leute dürfen Gäste einladen und selbst als Gast in fremde Tenants eingeladen werden. MFA- und Geräteansprüche anderer Organisationen werden dabei nicht vertraut. Wer nie hingeschaut hat, betreibt also bereits einen Hochschulverbund mit der ganzen Welt, nur ohne Vertrag.

Die Werkzeugkiste: vier Wege über die Grenze

Microsoft hat die Begriffe mehrfach umgebaut, die Oberflächen ebenfalls. Inhaltlich sind es vier Bausteine, die sich kombinieren lassen. Skizze 1 zeigt sie an einem typischen Verbund aus zwei Hochschulen und einem Industriepartner.

Zwei Hochschulen, ein Industriepartner, vier Wege

Welche Identität wo landet und wer die Tür aufschließt



Skizze 1: Je Weg eine andere Identität, ein anderes Protokoll und ein anderer Verantwortlicher fürs Aufräumen

B2B-Zusammenarbeit mit Gastkonten

Der Klassiker. Eine externe Person wird eingeladen und erhält im Ressourcen-Tenant ein eigenes Benutzerobjekt, standardmäßig vom Typ Gast. Angemeldet wird mit der Identität der Heimateinrichtung, wenn diese Entra ID nutzt, sonst über ein Microsoft-Konto, eine E-Mail-Einmalkennung oder einen SAML- beziehungsweise WS-Fed-Verbund mit einem externen Identitätsanbieter. Die Reihenfolge der zulässigen Anmeldewege lässt sich inzwischen konfigurieren, private Microsoft-Konten lassen sich als Rückfalloption abschalten, dann bleibt die E-Mail-Einmalkennung.

Gastkonten sind der universelle Weg: Sie funktionieren für Teams, SharePoint, OneDrive-Freigaben und für eigene oder fremde Anwendungen, die im Tenant registriert sind. Sie sind sichtbar, sie lassen sich in Gruppen stecken, mit Bedingtem Zugriff belegen und in Zugriffsüberprüfungen einbeziehen. Ihr Nachteil ist zugleich ihr Vorteil: Jedes Gastkonto ist ein Objekt in Ihrem Verzeichnis, und jedes Objekt will irgendwann gelöscht werden. Gastkonten sind darin Doktoranden nicht unähnlich: Geplant sind drei Jahre, geblieben wird zehn.

FAKTEN • Abrechnung von Gastkonten

Microsoft rechnet externe Identitäten nach monatlich aktiven Nutzern ab, also nach der Zahl unterschiedlicher externer Konten, die sich in einem Kalendermonat anmelden. Das Modell gilt für Konten vom Typ Gast. Konten vom Typ Mitglied, die aus anderen Tenants derselben Organisation stammen, zählen nach der Microsoft-Dokumentation nicht mit. Für die Abrechnung muss der Tenant mit einem Azure-Abonnement verknüpft sein. Wie viele Gäste kostenfrei bleiben und was darüber

hinaus anfällt, prüfen Sie bitte tagesaktuell bei Microsoft; Preise nennen wir hier bewusst nicht.

Direkte B2B-Verbindung und geteilte Kanäle

Die direkte B2B-Verbindung (B2B direct connect) ist das Gegenmodell: kein Gastkonto, kein Objekt im fremden Verzeichnis, keine Einladung. Zwei Organisationen vereinbaren gegenseitiges Vertrauen, und Personen der einen Seite arbeiten mit ihrer Heimatidentität in einem geteilten Kanal der anderen Seite, ohne in Teams den Tenant zu wechseln. Für Wissenschaftler, die in fünf Verbünden stecken, ist das eine echte Erleichterung, denn der Tenant-Wechsel in Teams gehört zu den Dingen, die niemand vermisst.

Der Haken steht im Kleingedruckten, und er ist groß: Die direkte Verbindung funktioniert ausschließlich mit geteilten Kanälen in Teams. Laut Microsoft gibt es keine Pläne, sie auf andere Dienste auszuweiten. Wer im Verbund also eine gemeinsame SharePoint-Website, ein Planner-Board außerhalb des Kanals oder eine Fachanwendung braucht, landet doch wieder beim Gastkonto. Außerdem muss die Verbindung auf beiden Seiten eingerichtet werden, Inbound bei Ihnen, Outbound beim Partner und umgekehrt. Ab Werk ist sie für alle Organisationen blockiert.

WICHTIG · Geteilte Kanäle und Gäste vertragen sich nicht

Gastkonten können geteilte Kanäle nicht sehen und nicht daran teilnehmen. Wer einen Industriepartner als Gast ins Verbund-Team holt und ihn dann in den geteilten Kanal »Arbeitspaket 3« einladen will, wird enttäuscht. Entscheiden Sie pro Partner, welcher Weg gilt, und schreiben Sie das in die Projektdokumentation.

Zweite Eigenheit: Mitglieder geteilter Kanäle verwaltet die Kanalbesitzerin oder der Kanalbesitzer direkt in Teams. Das Rechenzentrum sieht die externen Personen über Anmeldeprotokolle, Teams-Berichte und Zugriffsüberprüfungen, aber nicht als Benutzerobjekte im Verzeichnis.

Mandantenübergreifende Zugriffseinstellungen und Vertrauensstellung

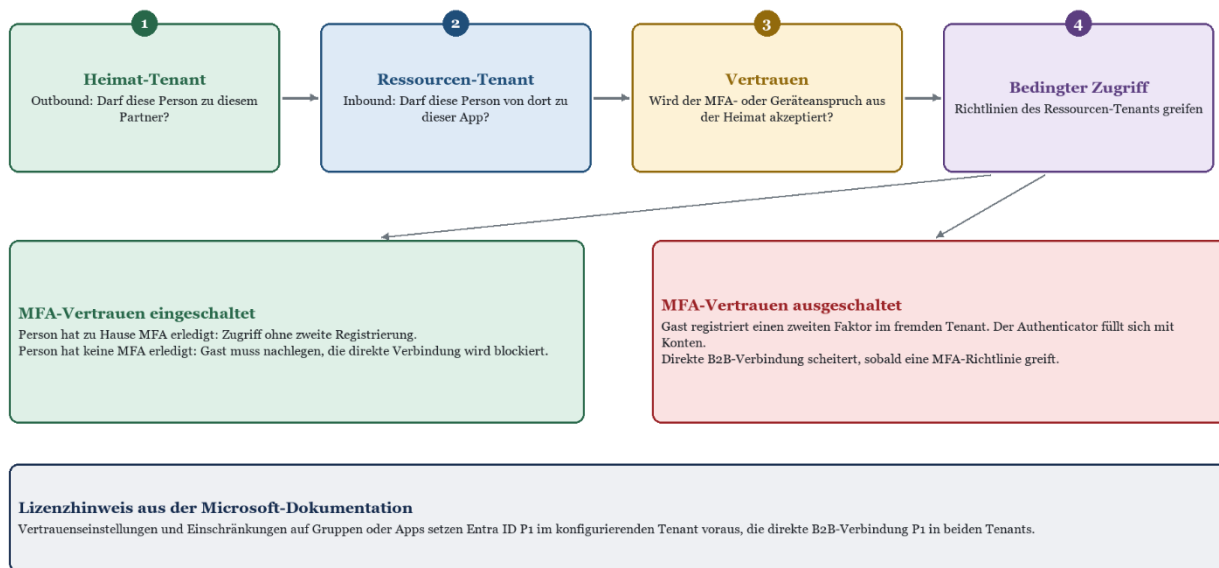
Die Zugriffseinstellungen (cross-tenant access settings) sind das Schaltpult über allen anderen Werkzeugen. Es gibt Standardeinstellungen, die für jede fremde Organisation gelten, und Organisationseinstellungen für einzelne Partner, die Vorrang vor dem Standard haben. Eine Obergrenze für die Zahl der Partner gibt es laut Microsoft nicht, was für einen Hochschul-Tenant mit Dutzenden Verbünden beruhigend ist. Je Partner legen Sie fest:

- **Inbound:** Wer aus der Partnerorganisation darf auf welche Ihrer Anwendungen zugreifen, getrennt für B2B-Zusammenarbeit und direkte Verbindung, auf Wunsch eingeschränkt auf bestimmte Gruppen der Gegenseite.
- **Outbound:** Welche Ihrer Personen dürfen beim Partner als Gast oder per direkter Verbindung arbeiten, und auf welche Anwendungen dort.
- **Vertrauen:** Akzeptiert Ihr Bedingter Zugriff die MFA, die die Person bereits zu Hause erledigt hat, und die Aussagen über konforme oder hybrid eingebundene Geräte?
- **Automatische Einlösung:** Entfällt die Zustimmungsabfrage beim ersten Zugriff? Das wirkt nur, wenn beide Seiten das Häkchen setzen, die Heimatseite Outbound und die Ressourcenseite Inbound.

Für Gruppen oder Anwendungen der Gegenseite brauchen Sie deren Objekt-IDs. Das klingt banal und ist in der Praxis der Moment, in dem das Verbundprojekt zum ersten Mal merkt, dass es auch zwischen den Rechenzentren einen Ansprechpartner braucht. Skizze 3 zeigt, in welcher Reihenfolge die Prüfungen bei einer Anmeldung greifen.

Was bei einer Anmeldung über die Tenant-Grenze geprüft wird

Beide Seiten müssen »ja« sagen, der Ressourcen-Tenant hat das letzte Wort



Skizze 3: Prüfreihenfolge bei mandantenübergreifenden Anmeldungen

TIPP · MFA-Vertrauen sauber einschalten

Wenn Sie der MFA eines Partners vertrauen, gelten Ihre MFA-Richtlinien weiterhin, die Person muss den zweiten Faktor aber nicht noch einmal bei Ihnen registrieren. Für die direkte B2B-Verbindung ist das Vertrauen sogar Pflicht, sobald Ihr Bedingter Zugriff MFA verlangt.

Microsoft empfiehlt, externe Konten in diesem Fall aus der MFA-Registrierungsrichtlinie von Entra ID Protection auszunehmen, weil sich beide Mechanismen sonst gegenseitig blockieren. Mehr zur Gestaltung der Richtlinien im Beitrag [MFA für 30.000 Studenten: Conditional Access an der Hochschule ohne Helpdesk-Kollaps](#).

Mandantenübergreifende Synchronisierung und Mehrmandantenorganisation

Die mandantenübergreifende Synchronisierung (cross-tenant synchronization) legt B2B-Konten automatisch an, aktualisiert sie und entfernt sie wieder. Sie ist ein Push-Verfahren: Der Quell-Tenant bestimmt, wer synchronisiert wird, der Ziel-Tenant erlaubt den Empfang und kann ihn jederzeit stoppen. Die Konten landen standardmäßig als externe Mitglieder statt als Gäste, Zustimmungsabfragen und Einladungsmails entfallen. Synchronisiert werden nur interne Konten der Quelle, keine Gäste, keine Geräte, keine Kontakte. Der Lauf startet in festen Abständen von etwa 40 Minuten; wer jemanden aus dem Bereich nimmt, sorgt für ein vorläufiges Löschen im Ziel.

Die Mehrmandantenorganisation (multitenant organization) setzt darauf auf. Sie zieht eine Klammer um Tenants, die einer Organisation gehören, und verbessert die Zusammenarbeit im neuen Teams und in Viva Engage, etwa durch Benachrichtigungen aus allen verbundenen Tenants und schnelleren Wechsel. Ein Tenant kann genau einer solchen Organisation angehören, aktiv sein dürfen nach aktueller Dokumentation bis zu 100 Tenants. Jeder bleibt dabei Herr im eigenen Haus und kann jederzeit austreten.

WICHTIG · Für die eigene Organisation gedacht, nicht für den Verbund

Microsoft beschreibt die Synchronisierung ausdrücklich als Werkzeug innerhalb einer Organisation. Für die organisationsübergreifende Nutzung weist die Dokumentation auf zusätzliche Pflichten nach Datenschutzrecht hin und empfiehlt für Partner außerhalb der eigenen Organisation stattdessen

Zugriffspakete aus der Berechtigungsverwaltung. Für eine Universität mit separatem Tenant eines An-Instituts oder ein Institut mit Zentrale kann das passen. Für zwei rechtlich selbstständige Hochschulen im Verbundprojekt ist es meistens das falsche Werkzeug.

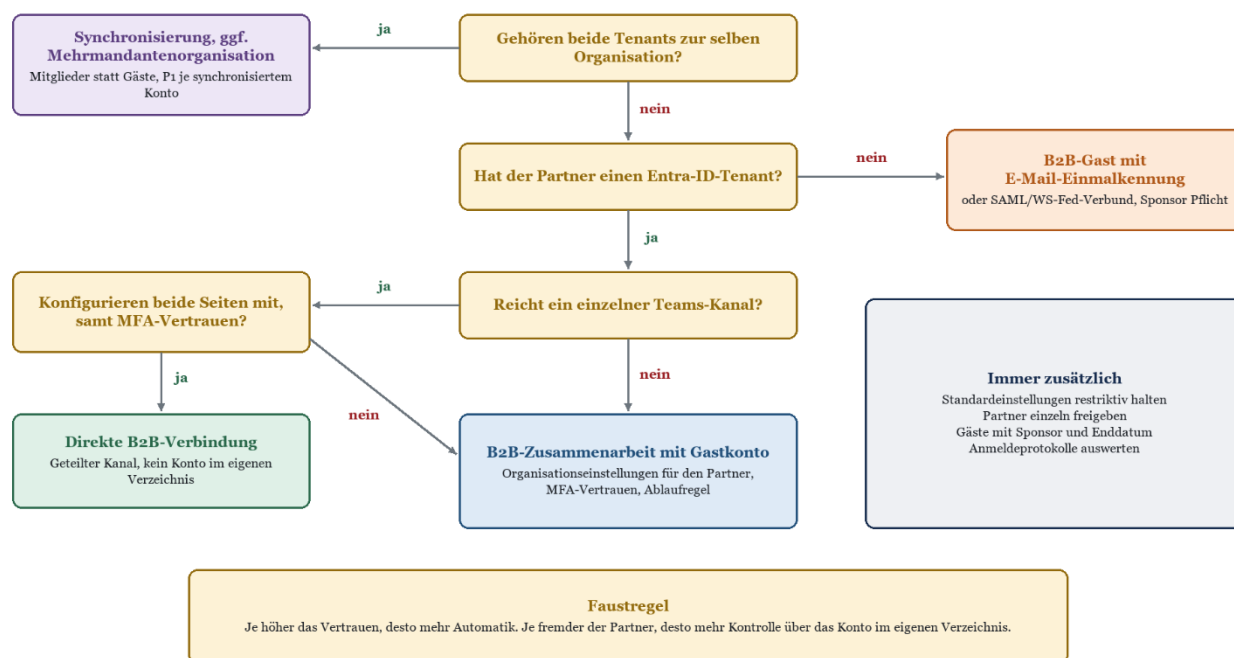
Merkmal	B2B-Gastkonto	Direkte Verbindung	Synchronisierung / Mehrmandantenorganisation
Objekt im Ressourcen-Tenant	Ja, Typ Gast (änderbar)	Nein	Ja, standardmäßig externes Mitglied
Einsatzbereich	Teams, SharePoint, OneDrive, Anwendungen	Nur geteilte Kanäle in Teams	Alle Microsoft-365-Dienste und Anwendungen
Einrichtung	Einseitig, Einladung je Person	Beidseitig, je Partner	Beidseitig, Quelle steuert den Umfang
Typische Vertrauensstufe	Niedrig bis mittel	Mittel	Hoch
Lizenzbedarf laut Dokumentation	Abrechnung nach aktiven Gästen; P1 für Vertrauen und feine Steuerung	P1 in beiden Tenants	P1 je synchronisiertem Konto im Quell-Tenant; Mehrmandantenorganisation zusätzlich mindestens eine P1 je Tenant
Aufräumen	Manuell oder per Zugriffsüberprüfung	Kanalbesitzer in Teams	Automatisch über den Synchronisierungsumfang

Welches Werkzeug für welches Szenario?

Die Werkzeugfrage entscheidet sich selten an der Technik, sondern an zwei organisatorischen Fragen: Gehören die Tenants zur selben Organisation? Und wie lange und wie eng soll die Zusammenarbeit dauern? Skizze 2 fasst den Weg als Entscheidungsbaum zusammen, die Tabelle darunter ordnet die häufigsten Szenarien zu.

Welches Werkzeug für welche Zusammenarbeit?

Ein Entscheidungsbaum für das Hochschulrechenzentrum



Skizze 2: Erst die Organisationsfrage klären, dann das Werkzeug wählen

Szenario	Werkzeug	Voraussetzung	Stolperfalle
Verbundprojekt mehrerer Hochschulen mit gemeinsamer Ablage	B2B-Gastkonten im Tenant der Konsortialführung, Organisationseinstellungen je Partner	Projektgruppe, Sponsor, Enddatum; MFA-Vertrauen zu den Partnern	Gäste überleben das Projekt; Partner-Tenant ändert MFA-Regeln ohne Absprache
Arbeitspaket mit intensivem Chat zwischen zwei Hochschulen	Direkte B2B-Verbindung mit geteiltem Kanal	Beide Rechenzentren konfigurieren mit, P1 beiderseits, MFA-Vertrauen	Nur Kanal, keine Website; Gäste aus dem übrigen Team bleiben außen vor
Industriepartner im Drittmittelprojekt	B2B-Gastkonten, nur für das Projekt-Team freigegeben	Kooperationsvertrag, Klärung vertraulicher Daten, ggf. Exportkontrolle	Freigabe »für alle mit dem Link«; Partner sieht mehr, als im Vertrag steht
Gemeinsamer Studiengang zweier Hochschulen	B2B-Gastkonten für Dozenten, Kursteams im Tenant der federführenden Hochschule	Klare Zuständigkeit für Prüfungsdaten, Absprache mit den Prüfungsämtern	Noten und Prüfungsunterlagen in Teams-Dateien eines fremden Tenants
Universität und eigenes An-Institut oder Tochter-gmbH mit eigenem Tenant	Synchronisierung, ggf. Mehrmandantenorganisation	Gleiche Organisation im Sinne der Dokumentation, P1 je Person	Rechtliche Selbstständigkeit des Instituts wird übersehen
Gemeinsames Rechenzentrum für mehrere Hochschulen	Gemeinsamer Tenant oder getrennte Tenants mit zentralem Betrieb	Vertrag zur Verantwortlichkeit, Lizenzklärung, Rollenmodell	Austritt einer Hochschule wird zur Migration
Gastwissenschaftler mit privater Adresse	B2B-Gastkonto mit E-Mail-Einmalkennung	Sponsor am Lehrstuhl, Ablaufdatum	Microsoft-Privatkonto als Anmeldeweg bleibt offen

Verbundprojekt mit Industriepartner

Im Verbund mit Unternehmen treffen zwei Kulturen aufeinander: Die Hochschule teilt gern, das Unternehmen schützt gern, und am Ende sitzen beide im selben Team und wundern sich über den jeweils anderen. Praktisch bewährt sich, das Verbundprojekt im Tenant der Konsortialführung zu hosten, den Industriepartner als Organisation in den Zugriffseinstellungen einzutragen und Inbound nur für die Projektgruppe des Partners zu öffnen. Die Gruppen-ID liefert dessen IT, ein Anruf genügt meistens, wenn man vorher den richtigen Menschen gefunden hat.

Sind vertrauliche Ergebnisse oder exportkontrollierte Güter im Spiel, reicht die Zugriffssteuerung allein nicht. Dann gehören Vertraulichkeitsbezeichnungen und Regeln gegen Datenabfluss dazu, und zwar bevor der erste Bericht hochgeladen ist. Und noch ein unscheinbarer Punkt: Wer Outbound standardmäßig alle Anwendungen sperrt, sperrt auch den Dienst, mit dem Ihre Leute verschlüsselte Mails des Partners lesen. Microsoft dokumentiert dafür eine Ausnahme, die Sie explizit freigeben müssen.

Gemeinsamer Studiengang

Bei gemeinsamen Studiengängen ist die technische Frage schnell beantwortet, die organisatorische nicht. Kursteams gehören in den Tenant der Hochschule, an der die Lehrveranstaltung verantwortet wird; Dozenten der Partnerhochschule kommen als Gast. Studenten, die an der Partnerhochschule eingeschrieben sind, ebenfalls. Kritisch wird es bei Prüfungsdaten: Wenn Klausuren, Bewertungen oder Noten in Teams-Dateien liegen, gilt das Regelwerk des Tenants, in dem sie liegen, nicht das des Prüfungsamts, das sie verantwortet. Das gehört vor Semesterbeginn geklärt, nicht nach der ersten Einsichtnahme.

Gemeinsames Rechenzentrum mehrerer Hochschulen

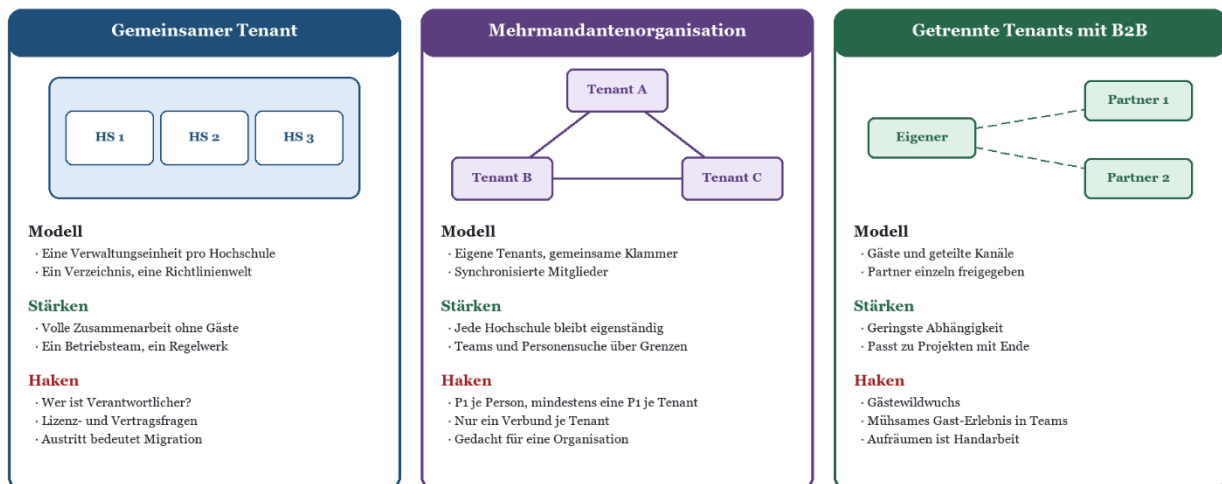
Kleinere Hochschulen, insbesondere Kunst- und Musikhochschulen, lassen ihre IT-Dienste mitunter von einer größeren Einrichtung oder einem gemeinsamen Rechenzentrum betreiben. Dann stellt sich die Grundsatzfrage: ein Tenant für alle oder ein Tenant je Hochschule mit gemeinsamer Betriebsmannschaft? Ihr widmet sich der nächste Abschnitt. Wer die Frage innerhalb einer einzigen Hochschule kennt, nämlich als Spannung zwischen zentralem Rechenzentrum und Fakultäts-IT, findet Parallelen im Beitrag [Dezentrale IT an der Hochschule: Lehrstuhl-Admins, Fakultäts-IT und ein Tenant für alle](#).

Ein gemeinsamer Tenant oder mehrere?

Die Frage klingt technisch und ist politisch. Ein Tenant ist nicht nur ein Verzeichnis, sondern eine Verantwortungsgrenze: Wer globale Administratoren stellt, kann alles sehen; wer die Richtlinien setzt, bestimmt für alle; und wer den Vertrag mit Microsoft hält, ist für die Lizenzierung aller verantwortlich. Skizze 4 stellt die drei Grundmodelle nebeneinander.

Ein Tenant, ein Verbund von Tenants oder lose Partner?

Drei Modelle für Hochschulen, die sich Infrastruktur teilen



Skizze 4: Die Topologie ist eine Organisationsentscheidung, keine Konfigurationsfrage

Was für einen gemeinsamen Tenant spricht

- Zusammenarbeit ohne Gäste: Alle sind Mitglieder, Personensuche, Kalender, Teams und Freigaben funktionieren ohne Umwege.
- Ein Regelwerk für Bedingten Zugriff, Aufbewahrung und Sicherheit, betrieben von einem Team, das die Sache auch wirklich beherrscht.
- Für kleine Einrichtungen, die allein kaum einen sicheren Tenant-Betrieb mit Notfallkonten, Protokollauswertung und Rollentrennung stemmen könnten, ist ein gemeinsamer Betrieb oft schlicht die sicherere Variante.

Was für mehrere Tenants spricht

- Rechtliche Selbstständigkeit: Jede Hochschule ist eigener Verantwortlicher im datenschutzrechtlichen Sinn, hat eigenen Personalrat, eigene Dienstvereinbarung und eigene Haushaltsführung.
- Administrative Trennung: Globale Administratoren der einen Hochschule sehen im gemeinsamen Tenant grundsätzlich auch die Daten der anderen. Verwaltungseinheiten mit eingeschränkten Rollen helfen, ersetzen die Trennung aber nicht.
- Austritt und Fusion: Aus einem gemeinsamen Tenant auszuziehen ist eine Migration mit Postfächern, Websites und OneDrives. Microsoft weist selbst darauf hin, dass die Synchronisierung kein Migrationswerkzeug ist.
- Hochschulgesetze und Landesdatenschutzrecht unterscheiden sich je Bundesland. Was in einem Land als gemeinsame Aufgabenwahrnehmung geregelt ist, verlangt anderswo einen eigenen Vertrag oder eine Rechtsgrundlage.

Und die Lizenzen?

Hier wird es schnell unseriös, wenn man nicht aufpasst. Belastbar aus der Microsoft-Dokumentation ist: Der Tenant ist die Standardgrenze für Lizenzierung, Lizenzen werden Konten in einem Tenant zugewiesen. Die Synchronisierung verlangt Entra ID P1 für jedes synchronisierte Konto im Heimat-Tenant, die Mehrmandantenorganisation eine P1-Lizenz je Person und Verbund sowie mindestens eine P1-Lizenz je Tenant. Gäste werden nach aktiven Konten abgerechnet. Welche Education-Pläne Entra ID P1 bereits enthalten, steht im Beitrag [Education-Lizenzen verstehen: A1, A3, A5 und der Student Use Benefit](#).

Ob eine Hochschule in ihrem Tenant Lizenzen für Angehörige einer anderen, rechtlich selbstständigen Einrichtung zuweisen darf, entscheidet dagegen nicht die Technik, sondern der Lizenzvertrag mit seinen Definitionen berechtigter Einrichtungen und Nutzer. Für Hochschulen, die über den Bundesvertrag beziehen, lohnt der Blick in den Beitrag [Microsoft-Bundesvertrag für Hochschulen: EES, Beitritt und was man damit wirklich bekommt](#).

HINWEIS • Keine Rechtsberatung

Ob ein gemeinsamer Tenant mehrerer Hochschulen lizenz-, haushalts- und datenschutzrechtlich zulässig ist, hängt vom konkreten Vertrag mit Microsoft oder dem Händler, vom Hochschulgesetz und vom Datenschutzgesetz des jeweiligen Landes sowie von den Vereinbarungen zwischen den Hochschulen ab. Klären Sie das mit Ihrem Vertragspartner, Ihrer Rechtsabteilung und den Datenschutzbeauftragten aller Beteiligten, bevor das erste Konto umzieht. Dieser Beitrag ersetzt diese Prüfung nicht.

TYPISCHE SITUATION • Mehr-Mandanten-Konsolidierung

Aus Projekten bei öffentlichen Auftraggebern kennen wir folgende Lage: Ein kommunaler Verband mit mehreren Mitgliedseinrichtungen hatte über die Jahre vier Tenants angesammelt, einen zentralen, zwei aus Pilotprojekten und einen, den eine Einrichtung in Eigenregie angelegt hatte. Gäste wurden kreuz und quer eingeladen, manche Personen existierten in drei Tenants mit drei Kennwörtern, und die Zugriffseinstellungen standen überall auf Werkseinstellung.

Die Lösung bestand nicht darin, alles in einen Tenant zu pressen. Zuerst wurde geklärt, welche Einrichtungen rechtlich und organisatorisch zusammengehören. Zwei Pilot-Tenants wurden aufgelöst und ihre Inhalte übernommen, die beiden verbleibenden Tenants per Synchronisierung verbunden, Gäste aus dem jeweils anderen Tenant durch synchronisierte Mitglieder ersetzt und die Standardeinstellungen für fremde Organisationen verschärft. Der aufwendigste Teil war nicht die Technik, sondern die Frage, wem welche Altdaten gehören.

Übertragen auf die Hochschule ist das die typische Situation eines gemeinsamen Rechenzentrums oder einer Universität mit eigenständig gewachsenen Tenants von An-Instituten, Graduiertenschulen oder Projekten. Die Reihenfolge bleibt dieselbe: Organisation klären, Altlasten zählen, dann erst Werkzeuge wählen.

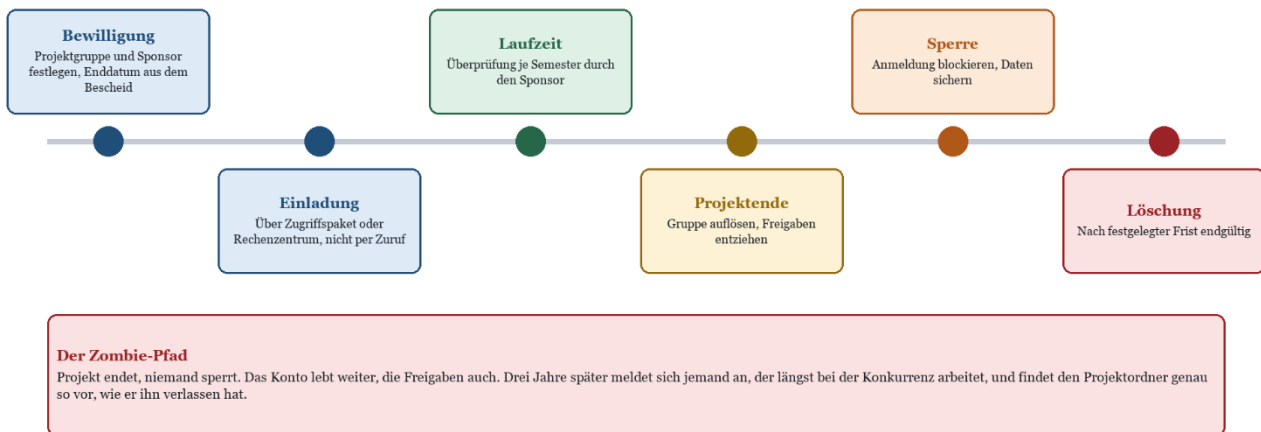
Betrieb: Lebenszyklus, Datenschutz und Personalrat

Der Lebenszyklus entscheidet über die Sicherheit

Die meisten Probleme mit mandantenübergreifender Zusammenarbeit sind keine Konfigurationsfehler, sondern vergessene Konten. Ein Verbundprojekt hat ein Enddatum, ein Gastkonto hat ab Werk keines. Skizze 5 zeigt den Lebenszyklus, wie er sein sollte, und den Pfad, den er ohne Pflege nimmt.

Lebenszyklus eines Gastkontos im Verbundprojekt

Das Konto sollte das Projekt nicht überleben. Tut es aber gern.



Skizze 5: Das Enddatum gehört an den Anfang, nicht ans Ende

- **Sponsor:** Jedes Gastkonto bekommt eine verantwortliche Person an der eigenen Hochschule, in der Regel die Projektleitung oder den Lehrstuhl.
- **Einladung über Zugriffspakete:** Wo die Lizenzlage es erlaubt, laufen Einladungen über die Berechtigungsverwaltung mit Ablaufdatum statt über einzelne Klicks in Teams.
- **Regelmäßige Überprüfung:** Einmal pro Semester bestätigt der Sponsor, dass das Konto noch gebraucht wird. Ohne Antwort wird gesperrt.
- **Sperren vor Löschen:** Nach Projektende erst die Anmeldung blockieren, dann nach festgelegter Frist löschen.
- **Protokolle sichern:** Anmeldeprotokolle stehen teils nur 30 Tage zur Verfügung. Wer wissen will, wer von außen zugreift, exportiert sie in ein eigenes Archiv oder SIEM.

Wie Gastwissenschaftler, Lehrbeauftragte und Emeriti mit Sponsoren und Ablaufdaten konkret abgebildet werden, beschreibt der Beitrag [Gastwissenschaftler, Lehrbeauftragte, Emeriti: Sonderrollen in Entra ID sauber abbilden](#); die Anbindung an Immatrikulation und Personalverwaltung steht im Beitrag [Identity Lifecycle an der Hochschule: Von der Immatrikulation bis zum Alumni-Konto](#). Wer wissen will, wie viele vergessene Gäste der eigene Tenant schon beherbergt, findet die Prüfschritte im Beitrag [Entra-ID-Überprüfung für Hochschul-Tenants: Was sich nach zehn Jahren Wildwuchs findet](#).

TIPP · Änderungen an den Zugriffseinstellungen absichern

Änderungen an den mandantenübergreifenden Zugriffseinstellungen gelten in Entra ID als geschützte Aktionen und lassen sich zusätzlich mit Bedingtem Zugriff absichern, etwa mit einer starken Authentifizierung. Im Überwachungsprotokoll finden Sie alle Änderungen unter der Kategorie CrossTenantAccessSettings. Für die Konfiguration reicht die Rolle Sicherheitsadministrator, ein globaler Administrator ist nicht nötig.

Datenschutz: Wer ist eigentlich verantwortlich?

Bei jeder Zusammenarbeit über Tenant-Grenzen fließen personenbezogene Daten zwischen Organisationen: Namen, Adressen, Anmeldeereignisse, Inhalte. Bei der direkten Verbindung erhält die Partnerorganisation nach Microsoft-Dokumentation zum Beispiel begrenzte Kontaktdaten Ihrer Personen, wenn diese über die vollständige Mailadresse gesucht werden. Organisationsspezifische Richtlinien werden in beiden Tenants gespeichert, unter Umständen auch außerhalb der eigenen Region.

Für Hochschulen heißt das: Der Verbundvertrag oder die Kooperationsvereinbarung sollte regeln, wer für die gemeinsame Ablage verantwortlich ist, wie Löschfristen aussehen und wer Auskunftersuchen beantwortet. Bei einem gemeinsamen Rechenzentrum kommt je nach Konstellation eine Auftragsverarbeitung oder eine gemeinsame Verantwortlichkeit in Betracht. Den Rahmen dafür beschreibt der Beitrag [Datenschutz und Microsoft 365 an Hochschulen: Zwischen DSK-Bewertung, Landesaufsicht und Campus-Realität](#).

HINWEIS · Hinweis zur rechtlichen Einordnung

Ob zwischen Verbundpartnern eine gemeinsame Verantwortlichkeit nach der DSGVO, eine Auftragsverarbeitung oder eine Übermittlung zwischen eigenständigen Verantwortlichen vorliegt, ist eine Einzelfallfrage. Sie hängt vom Zweck, von der Rollenverteilung und vom jeweiligen Landesdatenschutzgesetz ab. Beziehen Sie die Datenschutzbeauftragten aller beteiligten Einrichtungen frühzeitig ein.

Personalrat: Protokolle, die beim Partner liegen

Ein Aspekt, den Personalräte zu Recht ansprechen: Wenn Mitarbeiterinnen und Mitarbeiter Ihrer Hochschule als Gast in fremden Tenants arbeiten, entstehen Anmelde- und Nutzungsprotokolle beim Partner. Bei geteilten Kanälen liegen die Teams-Überwachungsereignisse laut Microsoft ausschließlich im Tenant, der den Kanal hostet; im Heimat-Tenant gibt es dazu keine. Ihre Dienstvereinbarung regelt also nur die halbe Welt.

Umgekehrt gilt das Gleiche: Ihre Administratoren sehen Anmeldungen fremder Wissenschaftler, die in keinem Dienstverhältnis zu Ihrer Hochschule stehen. Sinnvoll ist eine Regel in der Dienstvereinbarung, dass mandantenübergreifende Protokolle nur zu Sicherheits- und Betriebszwecken ausgewertet werden, und eine Abstimmung mit den Partnern im Verbundvertrag. Welche Mitbestimmungsrechte konkret greifen, regelt das jeweilige Landespersonalvertretungsgesetz unterschiedlich; Grundlagen dazu im Beitrag [Personalrat und Microsoft 365 an der Hochschule: Dienstvereinbarung, wissenschaftliches Personal und die Verhaltenskontrolle](#).

Wer Zugriffseinstellungen, Gastkonten und geteilte Kanäle nicht nur einrichten, sondern im Team dauerhaft betreiben will, findet passende Formate unter [Microsoft-365-Schulung für Hochschulen und Forschung](#). Für die Planung eines Verbunds oder einer Konsolidierung mehrerer Tenants mit allen Beteiligten am Tisch steht die [Microsoft-365-Beratung für Hochschulen und Forschung](#) zur Verfügung.

Häufige Fragen zur hochschulübergreifenden Zusammenarbeit

Ist B2B-Zusammenarbeit in unserem Tenant schon aktiv?

Sehr wahrscheinlich ja. Ab Werk ist B2B-Zusammenarbeit mit allen anderen Entra-ID-Organisationen erlaubt. Wer einladen darf, regeln die Einstellungen für externe Zusammenarbeit; welche Organisationen in Frage kommen, die mandantenübergreifenden Zugriffseinstellungen. Ein Blick in beide lohnt sich vor dem nächsten Semester.

Warum sehen unsere Gäste den geteilten Kanal nicht?

Weil Gastkonten geteilte Kanäle grundsätzlich nicht sehen können. Geteilte Kanäle mit externen Personen setzen die direkte B2B-Verbindung voraus, die beide Organisationen einrichten müssen.

Müssen Gäste bei uns noch einmal MFA einrichten?

Nur wenn Sie der MFA der Heimatorganisation nicht vertrauen. Mit eingeschaltetem Vertrauen gelten Ihre Richtlinien weiter, die bereits erledigte MFA wird aber anerkannt. Für das Einstellen des Vertrauens brauchen Sie Entra ID P1.

Können wir die Synchronisierung für ein Verbundprojekt nutzen?

Technisch ist das möglich, gedacht ist sie aber für Tenants derselben Organisation. Microsoft weist für den organisationsübergreifenden Einsatz auf zusätzliche datenschutzrechtliche Pflichten hin. Für Verbundpartner sind Gastkonten mit Zugriffspaketen meist der bessere Weg.

Lohnt sich ein gemeinsamer Tenant für mehrere kleine Hochschulen?

Betrieblich oft ja, rechtlich und vertraglich nur nach sorgfältiger Prüfung. Lizenzvertrag, Hochschulgesetz, Datenschutz und Personalvertretung des jeweiligen Landes entscheiden mit. Und der Austritt einer Hochschule ist später eine Migration.

Wie bekommen wir vergessene Gäste wieder los?

Mit Sponsoren, Ablaufdaten und regelmäßigen Zugriffsüberprüfungen für die Zukunft und mit einer einmaligen Bestandsaufnahme für die Vergangenheit: letzte Anmeldung, Gruppenmitgliedschaften, Freigaben. Erst sperren, dann löschen.

Was ist mit DFN-AAI und eduGAIN?

Föderierte Anmeldung über die DFN-AAI und Gastkonten in Entra ID lösen unterschiedliche Probleme und können nebeneinander bestehen. Wie Entra ID mit Shibboleth und der DFN-AAI zusammenspielt, beschreibt der Beitrag [Entra ID und Shibboleth: Microsoft 365 an die DFN-AAI-Welt anbinden](#).

Gilt das auch für außeruniversitäre Forschungseinrichtungen?

Ja, oft sogar verschärft: Institute großer Forschungsgesellschaften bewegen sich zwischen eigenem Tenant, zentralen Diensten der Gesellschaft und zahlreichen Hochschulkooperationen. Hintergründe im Beitrag [Microsoft 365 in außeruniversitären Forschungseinrichtungen: Institute zwischen Zentrale und Eigenständigkeit](#).

Fazit: Türen einbauen, bevor andere Löcher bohren

Hochschulen arbeiten über Grenzen, und das soll so bleiben. Microsoft 365 bietet dafür vier Werkzeuge mit sehr unterschiedlichen Stärken: Gastkonten für fast alles, die direkte Verbindung für geteilte Kanäle, Zugriffseinstellungen als Schaltpult darüber und Synchronisierung samt Mehrmandantenorganisation für Tenants, die wirklich zusammengehören. Keines davon ersetzt die Frage, wer mit wem in welcher Rolle und wie lange zusammenarbeitet.

Wer die Standardeinstellungen bewusst setzt, Partner einzeln freigibt, MFA-Vertrauen gezielt einschaltet und jedem Gast einen Sponsor und ein Enddatum mitgibt, hat die meisten Risiken im Griff. Der Rest ist Organisation: Verbundverträge, die IT mitdenken, Dienstvereinbarungen, die über die Tenant-Grenze schauen, und Rechenzentren, die einander kennen. Das klingt unspektakulär. Spektakulär wird es erst, wenn ein seit Jahren vergessenes Gastkonto plötzlich wieder Lebenszeichen sendet, und dann ist es meistens nicht mehr der ursprüngliche Inhaber.

WEITERLESEN · Weiterlesen

Die Serie zu Microsoft 365 in Hochschule und Forschung. Für diesen Beitrag besonders passend:

- › [Microsoft 365 in Hochschule und Forschung](#)
- › [Gastwissenschaftler, Lehrbeauftragte, Emeriti: Sonderrollen in Entra ID sauber abbilden](#)
- › [MFA für 30.000 Studenten: Conditional Access an der Hochschule ohne Helpdesk-Kollaps](#)

- › [Identity Lifecycle an der Hochschule: Von der Immatrikulation bis zum Alumni-Konto](#)
- › [Entra-ID-Überprüfung für Hochschul-Tenants: Was sich nach zehn Jahren Wildwuchs findet](#)
- › [Entra ID und Shibboleth: Microsoft 365 an die DFN-AAI-Welt anbinden](#)
- › [Microsoft-365-Beratung für Hochschulen und Forschung](#)
- › [Microsoft-365-Schulung für Hochschulen und Forschung](#)