

Dezentrale IT an der Hochschule: Lehrstuhl-Admins, Fakultäts-IT und ein Tenant für alle



WISSEN

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

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

BERATUNG

Delegationsmodell, Administrative Units und Regeln für Teams und Sites gemeinsam mit Rechenzentrum und Fakultäten entwerfen.

› [Beratung für Hochschulen und Forschung](#)

SCHULUNG

Für Fakultäts-IT und Lehrstuhl-Admins: delegierte Rollen, PIM und Gruppenpflege sicher im Alltag nutzen.

› [Schulungen für Hochschulen und Forschung](#)

Jede Hochschule hat ein Rechenzentrum. Viele haben außerdem eine Fakultäts-IT, ein paar Institutsadmins mit eigenem Serverraum und mindestens einen Lehrstuhl, an dem ein promovierter Physiker seit 2009 nebenher „die Rechner macht“. Das ist kein Versagen der Organisation, das ist ihre DNA. Fakultäten waren schon autonom, bevor irgendjemand das Wort Tenant buchstabieren konnte, und sie werden es noch sein, wenn Microsoft das Admin Center zum siebten Mal umbenannt hat.

Microsoft 365 trifft diese gewachsene Vielstaaterei mit einem unbequemen Detail: Es gibt einen Tenant. Einen Verzeichnisdienst, eine Conditional-Access-Ebene, eine Gastrichtlinie, eine Ablaufrichtlinie für Gruppen. Wer dort globaler Administrator ist, kann alles, auch Dinge, die man sich lieber nicht ausmalt. Die Frage ist also nicht, ob dezentral administriert wird, sondern wie man aus dutzenden IT-Fürstentümern eine föderale Ordnung macht, in der jeder seinen Landstrich verwaltet, ohne dem Nachbarn die Brunnen zu vergiften.

Dieser Beitrag beschreibt die Werkzeuge, mit denen das gelingt: Administrative Units, rollenbasierte Delegation, Privileged Identity Management, Namenskonventionen, Regeln für die Anlage von Teams und Sites und den Lebenszyklus von Gruppen. Er widmet sich außerdem dem Schatten-Tenant, also dem Lehrstuhl, der sich mal eben einen eigenen Mandanten angelegt hat, und der Frage, wie man die Freiheit von Forschung und Lehre ernst nimmt, ohne dass jede Regel an ihr zerschellt. Er gehört zur Serie [Microsoft 365 in Hochschule und Forschung](#).

Allgemeinbildende Schulen und Universitätsklinikum bleiben außen vor; beide haben eigene Regeln und eigene Sorgen.

FAKTEN · Das Wichtigste in Kürze

Ein Tenant kennt tenantweite Einstellungen, die sich nicht delegieren lassen. Was delegierbar ist, betrifft Konten, Gruppen und Geräte, also Objekte, nicht Richtlinien.

Administrative Units grenzen den Wirkungsbereich von Rollen ein. Sie lassen sich nicht verschachteln; eine Gruppe in einer AU bringt ihre Mitglieder nicht mit.

Für Administratoren mit AU-bezogener Rolle verlangt Microsoft eine Entra ID P1 Lizenz; für dynamische Mitgliedschaftsregeln in AUs auch für die Mitglieder.

Privileged Identity Management macht aus Daueradmins Admins auf Abruf, mit Begründung, Zeitlimit und auf Wunsch mit Freigabe.

Namensrichtlinie und Ablaufrichtlinie für Gruppen sind tenantweit: genau eine Namensrichtlinie, genau eine Ablaufrichtlinie.

Schatten-Tenants entstehen meist ohne böse Absicht. Wer sie findet, braucht einen Plan, keine Strafexpedition.

Ein Tenant, dutzende Fürstentümer: Warum der Campus anders delegiert

In einem Unternehmen ist die Hierarchie der IT meist eine Linie: zentrale IT, vielleicht ein paar Standortverantwortliche, fertig. In einer Stadtverwaltung gibt es Ämter mit Eigenleben, aber am Ende unterschreibt der Oberbürgermeister. An einer Universität dagegen hat das Präsidium formal die Leitung, die Fakultäten verwalten ihre Angelegenheiten aber weitgehend selbst, und die Professoren genießen ein Grundrecht, das in keinem Organigramm einer Firma vorkommt. Die IT spiegelt das: Sie ist nicht hierarchisch, sondern föderal, mit allen Vor- und Nachteilen, die Föderalismus so mit sich bringt.

Für die Administration von Microsoft 365 heißt das: Es wird nie genügen, alles zentral zu machen. Das Rechenzentrum hätte weder das Personal noch das Fachwissen, um dem Lehrstuhl für Musikwissenschaft die richtige Kanalstruktur für seine Editionsprojekte zu bauen. Es wird aber auch nie funktionieren, alles freizugeben. Dann gibt es nach drei Semestern 4.000 Teams namens „Test“, 200 Gäste mit unbekannter Herkunft und eine Fakultät, die versehentlich den Gastzugang für den ganzen Tenant geöffnet hat, weil ihr Admin zu viele Rechte hatte.

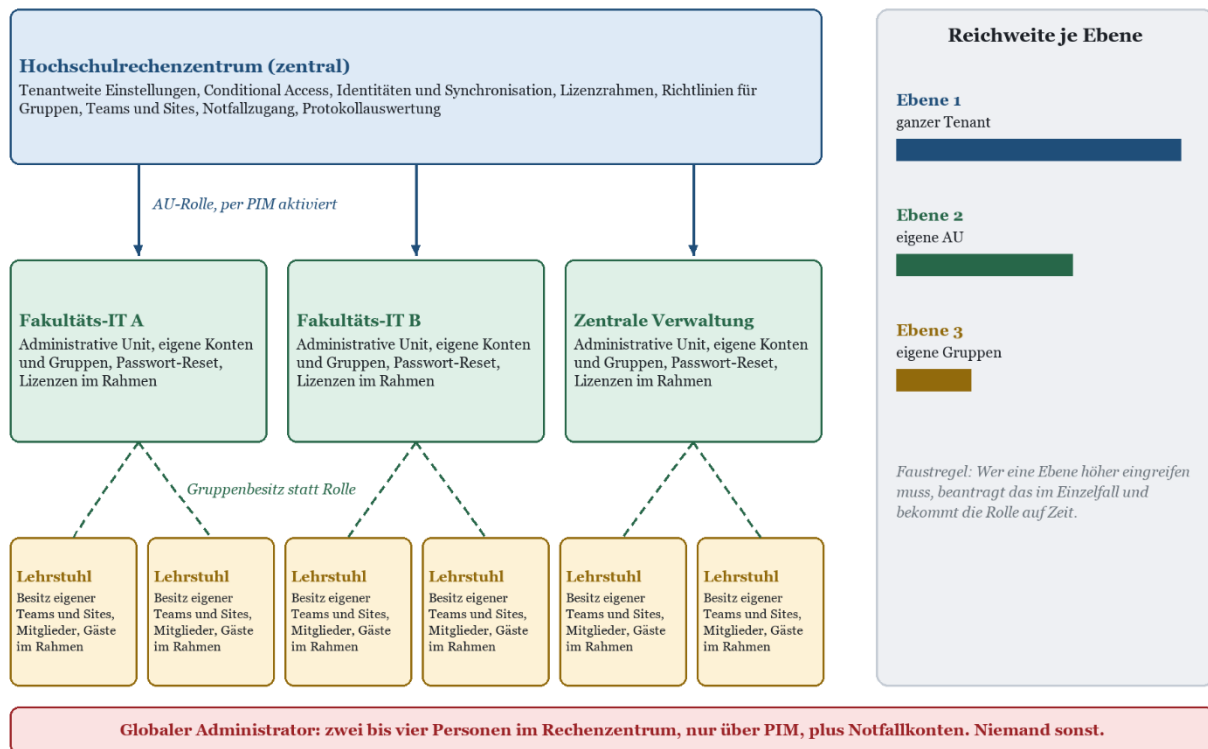
Die drei Ebenen: Rechenzentrum, Fakultäts-IT, Lehrstuhl

In der Praxis bewährt sich ein Modell mit drei Ebenen. Das Hochschulrechenzentrum verantwortet alles, was tenantweit wirkt: Identitäten und deren Synchronisation aus dem Campus-Management und der Personalverwaltung, Conditional Access, Gastrichtlinien, Lizenzrahmen, Aufbewahrung, die Richtlinien für Gruppen, Teams und Sites sowie die Protokollauswertung. Die Fakultäts-IT bekommt einen klar umrissenen Ausschnitt des Tenants und darin die Rechte, die sie für den Alltag braucht: Konten pflegen, Passwörter zurücksetzen, Lizenzen im vorgegebenen Rahmen zuweisen, Gruppen verwalten. Der Lehrstuhl schließlich administriert gar nicht im engeren Sinn, er besitzt: seine Teams, seine Sites, seine Mitgliederlisten.

Der entscheidende Gedanke steckt in dieser letzten Ebene. Der Lehrstuhl braucht in aller Regel keine Verzeichnisrolle. Was er will, ist Kontrolle über die eigene Zusammenarbeit, und die bekommt er als Besitzer von Gruppen, Teams und Sites. Das ist ein Unterschied wie zwischen Hausrecht und Generalschlüssel: Mit dem Hausrecht entscheiden Sie, wer in Ihre Wohnung darf. Mit dem Generalschlüssel kommen Sie in alle Wohnungen, und irgendwann fragt jemand, warum Sie das getan haben.

Skizze 1: Das Delegationsmodell in drei Ebenen

Oben wenige Schlüssel mit großer Reichweite, unten viele Schlüssel mit kleiner. Nicht umgekehrt.



Vereinfachte Darstellung. Zusschnitt der Ebenen je nach Organisation der Hochschule bzw. Forschungseinrichtung.

Freiheit von Forschung und Lehre: ernst nehmen, nicht als Joker spielen

Früher oder später fällt in jeder Governance-Runde der Satz: „Das verstößt gegen die Freiheit von Forschung und Lehre.“ Manchmal stimmt das. Wenn das Rechenzentrum vorschreiben will, mit welchen Partnern ein Lehrstuhl forscht, welche Inhalte in einer Vorlesung behandelt werden oder ob ein Wissenschaftler ein Werkzeug überhaupt benutzen darf, das für seine Methode unverzichtbar ist, dann berührt das den Kern der Wissenschaftsfreiheit. Wenn es dagegen um ein Präfix im Teamnamen, eine Ablauffrist für ungenutzte Gruppen oder die Pflicht zu einer Mehrfaktor-Anmeldung geht, dann ist das ungefähr so freiheitsgefährdend wie die Brandschutzordnung im Labor.

Hilfreich ist eine einfache Unterscheidung. Regeln, die das Wie der Zusammenarbeit betreffen, also Sicherheit, Ordnung, Nachvollziehbarkeit und Datenschutz, sind organisatorische Rahmenbedingungen und gehören in die Zuständigkeit der Hochschulleitung. Regeln, die das Ob und das Was der Forschung betreffen, gehören nicht in ein IT-Regelwerk. Wer diese Linie in der Governance-Ordnung sauber zieht und sie im Senat erklärt, hat das Argument entschärft, bevor es als Joker auf den Tisch kommt. Und er hat sich selbst verpflichtet, keine Regel zu schreiben, die tatsächlich in Methode oder Inhalt eingreift. Diese Selbstbindung ist mehr wert als jede technische Sperre.

HINWEIS · Kein Rechtsrat, aber ein Hinweis

Die Wissenschaftsfreiheit nach Art. 5 Abs. 3 GG und die Organisationsregeln der Hochschulgesetze der Länder bestimmen, wer in der Hochschule was entscheiden darf. Die Kompetenzverteilung zwischen Präsidium bzw. Rektorat, Kanzler, Senat und Fakultäten ist von Land zu Land unterschiedlich geregelt, ebenso die Frage, ob eine IT-Ordnung als Satzung, als Richtlinie des Präsidiums oder als Dienstanweisung erlassen wird. Klären Sie Form und Zuständigkeit mit dem Justizariat, bevor Sie eine Benutzungsordnung für Microsoft 365 in Kraft setzen.

Was ein Tenant nicht delegieren kann

Bevor es an die Werkzeuge geht, eine Ernüchterung. Es gibt Einstellungen, die existieren genau einmal pro Tenant. Dazu gehören die Gastrichtlinien in Entra ID, die Einstellungen für mandantenübergreifenden Zugriff, die Namensrichtlinie und die Ablaufrichtlinie für Microsoft-365-Gruppen, die meisten Conditional-Access-Richtlinien in ihrer Wirkung, die Freigabeeinstellungen auf Organisationsebene in SharePoint und die Teams-Einstellungen für externe Kommunikation. Microsoft schreibt in der Dokumentation zu Administrative Units ausdrücklich, dass AU-bezogene Rollen keine organisationsweiten Funktionen erhalten. Ein Gruppenadministrator mit AU-Bereich kann also die Gruppen seiner Fakultät pflegen, aber weder die Namensrichtlinie noch die Ablaufrichtlinie ändern.

Das klingt nach Einschränkung, ist aber ein Geschenk. Denn die Diskussion „Fakultät A will Gäste ohne MFA, Fakultät B will gar keine Gäste“ lässt sich technisch nicht durch zwei unterschiedliche Tenantschalter lösen. Sie muss entschieden werden, und zwar einmal, für alle, in einem Gremium. Wer das akzeptiert, spart sich jahrelange Stellvertreterkriege im Admin Center.

Der Werkzeugkasten: Administrative Units, Rollen und PIM

Microsoft liefert für dezentrale Organisationen erstaunlich passende Werkzeuge. In der Dokumentation zu Administrative Units ist das Beispiel sogar wörtlich eine große Universität mit autonomen Schools, jede mit eigenem IT-Team. Das ist erfreulich, sollte aber nicht darüber hinwegtäuschen, dass die Werkzeuge Grenzen haben, die man kennen muss, bevor man der Fakultät für Chemie etwas verspricht.

Administrative Units: Die Fakultät als Verwaltungsbereich

Eine Administrative Unit, kurz AU, ist in Entra ID ein Container für Konten, Gruppen und Geräte. Eine Rolle, die Sie mit dem Bereich einer AU zuweisen, wirkt nur auf deren Mitglieder. Die Fakultäts-IT der Physik bekommt also beispielsweise die Rolle Helpdesk-Administrator, Benutzeradministrator oder Gruppenadministrator für die AU „Fakultät für Physik“ und kann dort Passwörter zurücksetzen, Konten pflegen oder Gruppen verwalten, aber nicht in der Philosophie.

Dabei gibt es ein paar Eigenheiten, die in jeder Planung auftauchen und ebenso zuverlässig vergessen werden:

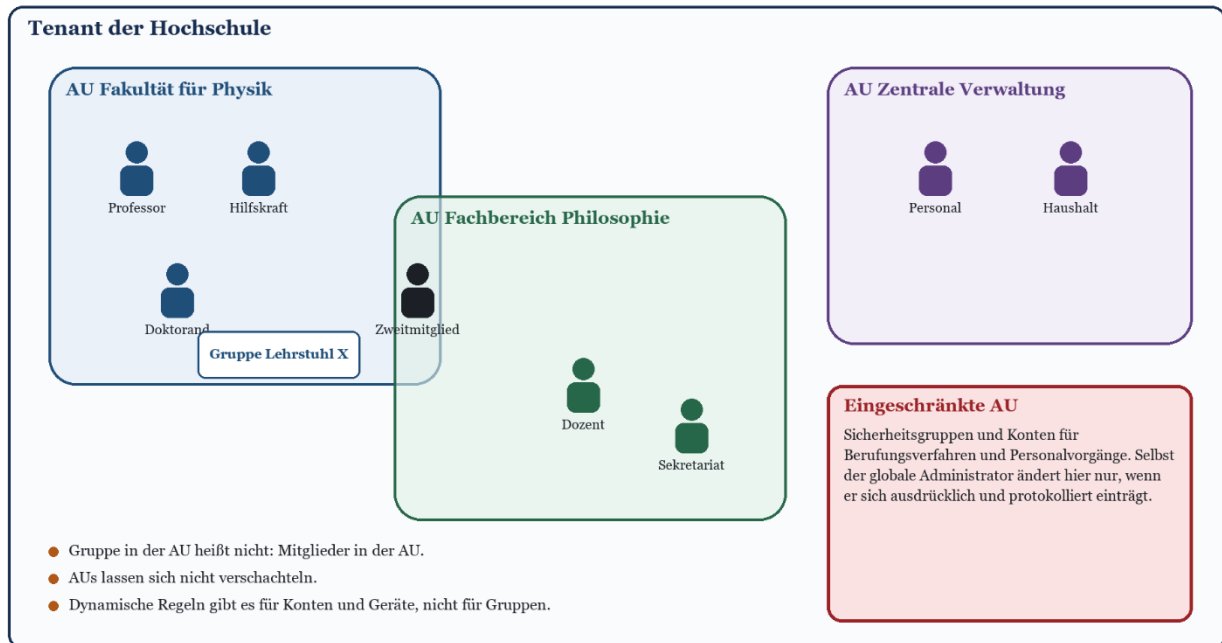
- **Keine Verschachtelung.** AUs lassen sich nicht ineinander schachteln. Eine Hierarchie Fakultät, Institut, Lehrstuhl müssen Sie also flach abbilden, etwa indem ein Konto Mitglied mehrerer AUs ist. Das geht, denn Konten dürfen in beliebig vielen AUs liegen.
- **Gruppe ist nicht gleich Mitglieder.** Nehmen Sie eine Gruppe in eine AU auf, kann der AU-Admin die Gruppe verwalten, also Name und Mitgliedschaft, nicht aber die Konten der Mitglieder. Die müssen separat in die AU.
- **Dynamische Regeln nur für Konten und Geräte.** AU-Mitgliedschaft lässt sich über Regeln steuern, etwa nach Abteilungsattribut. Für Gruppen gibt es das nicht.
- **Lesen bleibt erlaubt.** AUs begrenzen nur Verwaltungsrechte. Wer im Tenant ist, kann über Standardberechtigungen weiterhin andere Konten und Gruppen sehen. Wer eine Fakultät vor Blicken anderer verstecken will, ist mit AUs falsch beraten.
- **Intune ist außen vor.** Für die Geräteverwaltung in Intune gelten AUs nicht; dort steuern Sie Delegation über Bereichsmarkierungen und eigene Intune-Rollen.

Damit hängt die Qualität Ihrer AUs vollständig an den Attributen, die aus dem Quellsystem kommen. Steht in der Personalverwaltung bei der Hälfte des wissenschaftlichen Personals keine Organisationseinheit, oder führt das Campus-Management Studenten mit Zweitfach in zwei

Fakultäten, dann wird Ihre dynamische Regel genau das abbilden: Chaos, nur schneller. Die Pflege der Quelldaten ist deshalb die eigentliche Vorarbeit für jede Delegation.

Skizze 2: Administrative Units schneiden den Tenant in Zuständigkeiten

Kein Ordnerbaum, sondern Mengen. Ein Konto darf in mehreren liegen, eine AU nicht in einer anderen.



Prinzipdarstellung. Funktionsumfang laut Microsoft-Dokumentation zu Administrative Units in Entra ID, Stand Oktober 2026.

Eingeschränkte AUs für das wirklich Vertrauliche

Eine Variante verdient besondere Aufmerksamkeit: die AU mit eingeschränkter Verwaltung. Objekte darin können nur von Administratoren geändert werden, die ausdrücklich für genau diese AU eingetragen sind. Selbst ein globaler Administrator kann dort nichts ändern, solange er sich nicht selbst einträgt, und dieser Vorgang landet im Überwachungsprotokoll. Für Sicherheitsgruppen, die den Zugriff auf Berufsakten, Personalvorgänge oder Prüfungsunterlagen steuern, ist das genau das richtige Werkzeug: Die Fakultäts-IT mit tenantweiter Gruppenrolle, die es eigentlich nicht geben sollte, die es aber aus historischen Gründen fast immer gibt, kommt hier nicht mehr heran.

Die Einschränkungen laut Microsoft: Die Eigenschaft muss beim Anlegen der AU gesetzt werden und lässt sich danach nicht mehr ändern. Microsoft-365-Gruppen, E-Mail-aktivierte Sicherheitsgruppen und Verteilerlisten können nicht Mitglied werden, nur Konten, Geräte und Sicherheitsgruppen. Objekte in einer solchen AU lassen sich nicht mit den Funktionen von Entra ID Governance wie PIM für Gruppen, Zugriffsüberprüfungen oder Lebenszyklus-Workflows verwalten. Und pro Tenant sind höchstens 100 solcher AUs möglich, was für eine Hochschule reicht, wenn man sie nicht als Allzweckwaffe missbraucht.

WARNUNG · Eingeschränkte AU kann Workflows brechen

Microsoft weist selbst darauf hin: Wer Objekte in eine eingeschränkte AU legt, schränkt den Kreis derer, die sie ändern dürfen, drastisch ein. Bestehende Provisionierungen, Skripte mit Graph-Anwendungsberechtigungen und Abläufe des Helpdesks laufen dann ins Leere. Anwendungen brauchen eine Rolle mit dem Bereich genau dieser AU. Testen Sie mit einem Pilotobjekt, nicht mit der Gruppe, an der am Montag die Berufungskommission hängt.

Rollen: Kleinste Werkzeuge statt Generalschlüssel

Nicht jede Rolle lässt sich auf eine AU begrenzen. Laut Microsoft gehören unter anderem Benutzeradministrator, Gruppenadministrator, Helpdesk-Administrator, Kennwortadministrator, Authentifizierungsadministrator, Lizenzadministrator und Cloudgeräteadministrator dazu, außerdem benutzerdefinierte Rollen mit Berechtigungen für Konten, Gruppen oder Geräte. Spannend für Hochschulen sind zwei Spezialfälle: Teams-Administrator und SharePoint-Administrator lassen sich zwar mit AU-Bereich zuweisen, erlauben dann aber nur die Pflege der Microsoft-365-Gruppen in der AU und einiger Eigenschaften über das Microsoft 365 Admin Center. Das Teams Admin Center und das SharePoint Admin Center bleiben verschlossen. Wer der Fakultäts-IT „Teams-Admin für die Fakultät“ verspricht, sollte vorher genau nachlesen, was das konkret heißt.

Daraus folgt eine Grundhaltung: Delegieren Sie Aufgaben, nicht Rollen. Fragen Sie die Fakultäts-IT, was sie im Alltag tatsächlich tut, und suchen Sie dann die kleinste Rolle, die das abdeckt. Meist sind das Passwort-Reset, Authentifizierungsmethoden zurücksetzen, Lizenzen zuweisen und Gruppen pflegen. Selten ist es mehr. Für alles andere gibt es einen Antrag beim Rechenzentrum, und das ist kein Misstrauensvotum, sondern die einzige Art, wie man nach zehn Jahren noch weiß, wer was warum eingestellt hat.

Privileged Identity Management: Admin auf Abruf

Privileged Identity Management, kurz PIM, verwandelt dauerhafte Rollenzuweisungen in berechnete. Wer berechnete ist, aktiviert die Rolle bei Bedarf für eine festgelegte Zeit, gibt eine Begründung an, meldet sich mit mehreren Faktoren an und braucht auf Wunsch eine Freigabe. Zuweisungen können befristet werden, und über Zugriffsüberprüfungen lässt sich regelmäßig fragen, ob jemand eine Rolle überhaupt noch braucht. Das passt hervorragend zu einem Umfeld, in dem Verträge befristet sind, Projektstellen auslaufen und der Lehrstuhl-Admin von heute der Postdoc in Kanada von morgen ist.

PIM ist eine Funktion von Entra ID P2 bzw. Entra ID Governance. Welche Education-Pläne das enthalten und für wen Sie dann lizenzieren müssen, steht im Beitrag [Education-Lizenzen verstehen: A1, A3, A5 und der Student Use Benefit](#). Für die Governance zählt vor allem: PIM funktioniert auch mit AU-bezogenen Rollen. Die Fakultäts-IT kann also berechnete sein, die Rolle Benutzeradministrator für die eigene AU zu aktivieren, und hat sie ansonsten nicht. Fällt ein Konto der Fakultäts-IT in falsche Hände, ist der Schaden damit deutlich kleiner.

WARNUNG · „Nur kurz“ globaler Administrator

Der häufigste Sündenfall in dezentralen Tenants: Eine Fakultäts-IT braucht für eine Einrichtung „nur kurz“ globale Rechte, bekommt sie dauerhaft, und vier Jahre später stellt sich heraus, dass das Konto nie MFA hatte. Globale Administratoren gehören ins Rechenzentrum, in kleiner Zahl, ausschließlich über PIM, plus zwei Notfallkonten, die von Conditional Access ausgenommen und gut verwahrt sind. Alles andere ist kein Vertrauensbeweis, sondern ein Einbruchswerkzeug mit Vorschuss.

Wer macht was: Die Aufgabenverteilung im Überblick

Die folgende Tabelle ist ein Ausgangspunkt für die eigene Zuständigkeitsmatrix. Sie ersetzt keine Abstimmung mit Fakultäten und Personalrat, verkürzt sie aber erheblich, weil alle über dieselbe Liste reden.

Aufgabe	Zentral (Rechenzentrum)	Delegiert an	Werkzeug
Identitäten anlegen	Ja, aus Campus-	Nein, höchstens	Provisionierung,

und sperren	Management und Personalverwaltung	Sonderkonten nach Antrag	Synchronisation
Passwort und MFA zurücksetzen	Rückfallebene	Fakultäts-IT für die eigene AU	Helpdesk- bzw. Authentifizierungsadministrator mit AU-Bereich
Kontoeigenschaften pflegen	Rahmen, Attribute aus Quellsystem	Fakultäts-IT für nicht synchronisierte Felder	Benutzeradministrator mit AU-Bereich, PIM
Lizenzen zuweisen	Lizenzrahmen, gruppenbasierte Standardzuweisung	Fakultäts-IT für Sonderfälle	Lizenzadministrator mit AU-Bereich
Gruppen und Teams anlegen	Richtlinie, Namensregel, Vorlagen	Fakultäts-IT bzw. berechnigte Personen	Einstellung für Gruppenerstellung, Antragsprozess
Mitglieder und Gäste in Teams	Gastrichtlinie tenantweit	Besitzer am Lehrstuhl	Gruppenbesitz
Gruppen-Lebenszyklus	Ablaufrichtlinie, Ersatzadresse	Besitzer verlängern	Ablaufrichtlinie für Microsoft-365-Gruppen
Vertrauliche Gruppen	Ja	Nur benannte Admins	AU mit eingeschränkter Verwaltung
Geräteverwaltung	Basisrichtlinien	Fakultäts-IT für eigene Geräte	Intune-Rollen mit Bereichsmarkierungen
Conditional Access, Gastrichtlinie	Ja	Nein	Entra ID, nur zentral
Globale Rollen	Ja, wenige Personen	Nein	PIM mit Freigabe, Notfallkonten
Protokolle auswerten	Ja, nach Regelung mit Personalrat	Nein	Überwachungsprotokoll, Zweckbindung

Teams, Sites und Gruppen: Anlage, Namen und Lebenszyklus

Wenn Administrative Units die Verfassung sind, dann sind die Regeln für Gruppen die Straßenverkehrsordnung. Sie betreffen jeden, jeden Tag, und genau deshalb lösen sie die heftigsten Debatten aus. Hinter jedem Team, jeder Gruppen-Site und jedem Planner-Plan steckt eine Microsoft-365-Gruppe. Wer die Gruppe steuert, steuert also das meiste, was Nutzer als „Teams“ oder „SharePoint“ wahrnehmen.

Wer darf anlegen? Drei Modelle mit Nebenwirkungen

Standardmäßig darf in Entra ID jedes Mitglied des Tenants Microsoft-365-Gruppen anlegen und damit auch Teams. Über die Einstellung zur Gruppenerstellung lässt sich das auf niemanden oder auf eine ausgewählte Gruppe beschränken. Damit sind die drei Grundmodelle schon beschrieben:

Modell	So funktioniert es	Vorteil	Nebenwirkung
Offen	Alle Mitarbeiterinnen und Mitarbeiter dürfen anlegen, oft auch Studenten	Keine Wartezeit, hohe Akzeptanz	Wildwuchs, Dubletten, verwaiste Teams nach Projektende
Antrag	Anlage nur über ein Formular, das Rechenzentrum oder ein Automat legt an	Saubere Namen, Metadaten, Besitzer garantiert	Wartezeit, Umgehung über private Werkzeuge
Delegiert	Eine Gruppe pro Fakultät darf anlegen, etwa Fakultäts-IT und Sekretariate	Nähe zum Bedarf, Verantwortung vor Ort	Unterschiedliche Sorgfalt je Fakultät

Mischform	Wissenschaftliches Personal und Verwaltung offen, Studenten nur über Kursteams oder Antrag	Passt zu den Rollen am Campus	Regelwerk muss erklärt werden
------------------	--	-------------------------------	-------------------------------

Aus Erfahrung in dezentral organisierten öffentlichen Einrichtungen lässt sich sagen: Das restriktivste Modell erzeugt nicht weniger Wildwuchs, es verlagert ihn nur. Wer drei Wochen auf ein Team warten muss, gründet eine Gruppe in einem Messenger oder legt einen Ordner bei einem privaten Cloudanbieter an. Ein Antragsprozess ist nur so gut wie seine Durchlaufzeit. Wenn er automatisiert binnen Minuten ein Team mit sauberem Namen, zwei Besitzern und hinterlegter Kostenstelle liefert, wird er angenommen. Wenn er per E-Mail an ein Funktionspostfach geht, das im Semesterstress niemand liest, dann nicht.

Namenskonventionen: Präfixe, die etwas bedeuten

Entra ID bietet eine Namensrichtlinie für Microsoft-365-Gruppen. Sie kann feste Präfixe und Suffixe erzwingen und Attribute des anlegenden Kontos einsetzen. Unterstützt sind laut Microsoft Abteilung, Firma, Büro, Bundesland bzw. Region, Land und Titel; Erweiterungs- und benutzerdefinierte Attribute nicht. Der gesamte Name inklusive Präfix und Suffix darf höchstens 63 Zeichen lang sein. Daneben gibt es eine Liste gesperrter Wörter mit bis zu 5.000 Einträgen; gesperrt wird nur bei exakter Übereinstimmung, nicht bei Teilwörtern. Die Richtlinie wirkt in Teams, Outlook, SharePoint, Planner und weiteren Diensten.

Für Hochschulen ist das Abteilungsattribut der naheliegende Kandidat, um die Fakultät automatisch in den Namen zu bringen. Das funktioniert aber nur, wenn das Attribut flächendeckend und knapp gepflegt ist. „Fakultät für Mathematik, Informatik und Naturwissenschaften, Institut für Theoretische Physik“ als Abteilung frisst das Zeichenbudget, bevor der eigentliche Teamname beginnt. Kürzel sind hier keine Bürokratie, sondern Notwendigkeit. Drei Dinge sollten Sie außerdem wissen:

- Globale Administratoren und Benutzeradministratoren sind von der Richtlinie ausgenommen. Gruppen, die das Rechenzentrum anlegt, folgen ihr also nur, wenn es sich selbst daran hält.
- Bestehende Gruppen werden nicht umbenannt. Die Regel greift erst, wenn ein Besitzer den Namen bearbeitet.
- Es gibt nur eine Namensrichtlinie pro Tenant. Fakultätsspezifische Präfixe entstehen also über Attribute, nicht über mehrere Richtlinien.

TIPP · Ein Präfix, das man auch nach zehn Jahren versteht

Bewährt hat sich ein kurzes Schema aus Typ und Organisationseinheit, etwa „LV“ für Lehrveranstaltung, „PJ“ für Projekt, „OE“ für Organisationseinheit, gefolgt vom Fakultäts- oder Institutskürzel. Ein Team heißt dann zum Beispiel „PJ-PHY-Quantensensorik“. Das Semester gehört bei Kursteams in den Namen, bei Projekten das Ende der Laufzeit in eine Beschreibung oder ein Attribut. Und veröffentlichen Sie die Kürzelliste an einer Stelle, an der sie auch gefunden wird.

FAKTEN · Lizenzhinweis zur Namensrichtlinie

Laut Microsoft setzt die Namensrichtlinie voraus, dass Sie für jede Person, die Mitglied in mindestens einer Microsoft-365-Gruppe ist, eine Entra ID P1 Lizenz oder eine Entra Basic EDU Lizenz besitzen; zugewiesen werden muss sie nicht. Für die Ablaufrichtlinie gilt sinngemäß dasselbe mit P1 oder P2 für die Mitglieder der betroffenen Gruppen. Prüfen Sie das gegen Ihren Vertragsbestand, bevor das Präsidium eine Richtlinie beschließt, die Sie nicht einschalten dürfen.

Lebenszyklus: Das Semester als Taktgeber

Gruppen sterben nicht von selbst. Ohne Lebenszyklus sammelt ein Hochschul-Tenant Teams wie ein Dachboden Kartons: alles irgendwann wichtig gewesen, nichts davon beschriftet. Die Ablaufrichtlinie für Microsoft-365-Gruppen setzt eine Laufzeit von mindestens 30 Tagen. Gruppen mit Aktivität, etwa ein Kanalbesuch in Teams oder ein Dateizugriff in SharePoint, verlängern sich automatisch. Wo das nicht greift, erhalten die Besitzer 30, 15 und einen Tag vor Ablauf eine Erinnerung. Nicht verlängerte Gruppen werden gelöscht und sind 30 Tage lang wiederherstellbar. Für Gruppen ohne Besitzer gehen die Hinweise an eine Ersatzadresse, die Sie hinterlegen.

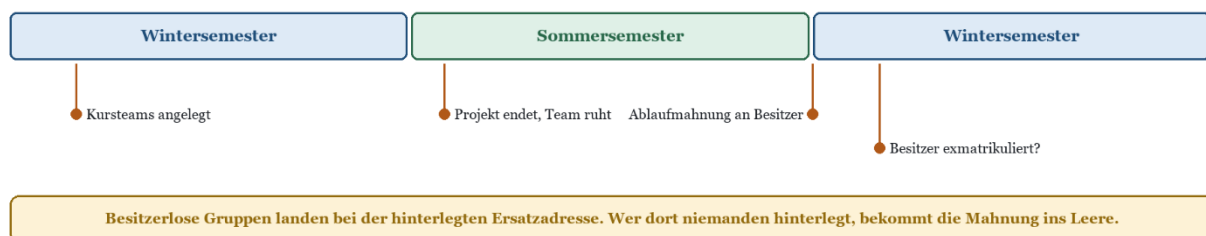
Die Richtlinie gilt wahlweise für alle oder für ausgewählte Gruppen, im zweiten Fall für höchstens 500. Für eine Hochschule mit tausenden Teams ist die Auswahlvariante daher eher eine Pilotphase als ein Dauerzustand. Beim ersten Einschalten bekommen ältere Gruppen eine Galgenfrist von 35 Tagen, sofern sie nicht aktiv sind. Das ist der Moment, in dem Sie besser vorher kommuniziert haben, sonst erfährt der Emeritus über eine automatische E-Mail, dass sein Lebenswerk demnächst entsorgt wird.

Skizze 3: Lebenszyklus einer Microsoft-365-Gruppe

Vom Antrag bis zur endgültigen Löschung. Die Uhr läuft, ob jemand hinsieht oder nicht.



Und so sieht das im Hochschuljahr aus:



Zeiten laut Microsoft-Dokumentation zur Ablaufrichtlinie für Microsoft-365-Gruppen. Laufzeit selbst ist frei wählbar, mindestens 30 Tage.

Wichtiger als die Löschaufomatik ist die Besitzerfrage. Jedes Team braucht mindestens zwei Besitzer, idealerweise aus dem Stammpersonal und nicht nur studentische Hilfskräfte oder Doktoranden mit Vertragsende in sechs Monaten. Wenn ein Lehrstuhl wechselt, ein Professor emeritiert wird oder eine Projektstelle ausläuft, muss jemand die Besitzrechte übernehmen. Daran hängt der Identity Lifecycle aus der Personalverwaltung und dem Campus-Management, und daran hängt auch die Frage, wie lange Inhalte nach dem Ende einer Gruppe aufbewahrt werden. Aufbewahrungsrichtlinien greifen nach der Löschung weiter, wenn sie eingerichtet sind; ohne sie ist nach Ablauf der Wiederherstellungsfrist schlicht Schluss.

WICHTIG · Löschen ist auch eine Datenschutzfrage

Ein Lebenszyklus, der Gruppen nach Projektende löscht, dient der Datenminimierung. Er kann aber mit Aufbewahrungspflichten für Forschungsdaten, Prüfungsunterlagen oder Drittmittelnachweise kollidieren. Stimmen Sie Laufzeiten und Aufbewahrungsrichtlinien mit Datenschutzbeauftragten, Archiv und Drittmittelverwaltung ab. Hintergründe stehen im Beitrag [Datenschutz und Microsoft 365 an Hochschulen: Zwischen DSK-Bewertung, Landesaufsicht und Campus-Realität](#).

Schatten-Tenants: Der Lehrstuhl mit dem eigenen Mandanten

Irgendwann stößt jedes Rechenzentrum auf ihn: einen Tenant, der nicht ihm gehört, aber den Namen der Hochschule trägt. Manchmal verrät er sich über eine DNS-Anfrage für einen TXT-Eintrag unter einer Subdomain, manchmal über eine Rechnung in der Drittmittelverwaltung, manchmal über einen Gastwissenschaftler, der fragt, warum er sich bei der Hochschule zweimal anmelden muss. Und manchmal über einen Anruf von Microsoft, weil der Tenant auf eine Adresse lautet, deren Inhaber vor drei Jahren die Hochschule verlassen hat.

Wie Schatten-Tenants entstehen

Die Entstehungsgeschichten sind meist harmlos, und das ist wichtig für den Umgang. Ein Doktorand wollte Power Platform ausprobieren und hat einen Entwicklertenant registriert. Ein Verbundprojekt brauchte schnell eine gemeinsame Arbeitsumgebung, und der Projektpartner hat einen Tenant mit Testlizenzen spendiert. Ein Institut hat vor der zentralen Einführung von Microsoft 365 eigene Lizenzen über einen Händler gekauft, weil es nicht warten wollte. Oder ein Lehrstuhl hat über ein Azure-Guthaben für die Forschung einen eigenen Verzeichnismandanten bekommen und dort mit der Zeit Konten für das ganze Team angelegt.

Technisch gibt es dafür mehrere Wege. Einer davon steht im eigenen Tenant: Entra ID erlaubt Mitgliedern standardmäßig, neue Tenants anzulegen, und macht sie dort automatisch zu globalen Administratoren. Mit der Einstellung, die Erstellung von Tenants durch Nicht-Administratoren zu beschränken, geht das nur noch mit der Rolle Mandantenersteller. Jede Erstellung landet im Überwachungsprotokoll als Aktivität „Create Company“, auch wenn sie erlaubt ist. Das ist ein guter, billiger Frühwarnmechanismus.

Der Bezug zur Hochschuldomain entsteht über DNS. Um eine Domain oder Subdomain in einem Tenant zu verifizieren, muss jemand einen TXT- oder MX-Eintrag in der entsprechenden Zone setzen können. An Hochschulen, an denen Institute eigene DNS-Zonen für ihre Subdomains betreiben, ist das kein Hindernis. Ob eine Subdomain in einem fremden Tenant verifiziert werden kann, wenn die übergeordnete Domain bereits im zentralen Tenant liegt, hängt von Reihenfolge und Konstellation ab; verlassen Sie sich nicht darauf, dass Entra ID das für Sie verhindert. Die wirksamste Kontrolle sitzt da, wo sie schon immer saß: bei der Frage, wer Einträge in Ihren DNS-Zonen anlegen darf.

WARNUNG · Subdomain im fremden Tenant

Ist eine Subdomain der Hochschule in einem Schatten-Tenant verifiziert, laufen dort Konten mit Adressen, die nach Hochschule aussehen, Mail kann im Namen der Hochschule versendet werden, und Gäste in anderen Tenants halten diese Konten für offiziell. Wer die Subdomain später zentral nutzen will, muss sie zuerst aus dem fremden Tenant herauslösen. Ohne einen greifbaren Administrator dort wird das zu einem langwierigen Verfahren. Dokumentieren Sie deshalb jede Delegation einer DNS-Zone und prüfen Sie regelmäßig, welche Verifikationseinträge darin stehen.

Warum sie zum Problem werden

Ein Schatten-Tenant ist nicht per se gefährlich. Er wird gefährlich, weil er außerhalb aller Prozesse steht, die Sie mühsam aufgebaut haben. Die Konten dort werden bei der Exmatrikulation oder beim Ausscheiden aus dem Dienst nicht gesperrt. MFA ist eine Option, kein Standard. Niemand prüft die Protokolle. Für personenbezogene Daten fehlt oft die Grundlage, die der zentrale Tenant mit Verarbeitungsverzeichnis, Datenschutz-Folgenabschätzung und Dienstvereinbarung hat. Wer gegenüber Microsoft Vertragspartner ist, wenn der Tenant mit der privaten Kreditkarte eines

Professors bezahlt wurde, ist eine Frage, die man lieber nicht vor einem Datenschutzvorfall beantworten möchte.

Hinzu kommt die Wiederholungsgefahr. Der Lehrstuhl-Admin, der den Tenant aufgebaut hat, geht. Seine Nachfolgerin findet ein Konto namens admin, dessen Passwort in einer Tabelle stand, die gelöscht wurde. Der Tenant läuft weiter, Lizenzen werden verlängert, Daten liegen darin, aber niemand kommt mehr hinein. Das ist der Moment, in dem Schatten-Tenants von lästig zu teuer werden.

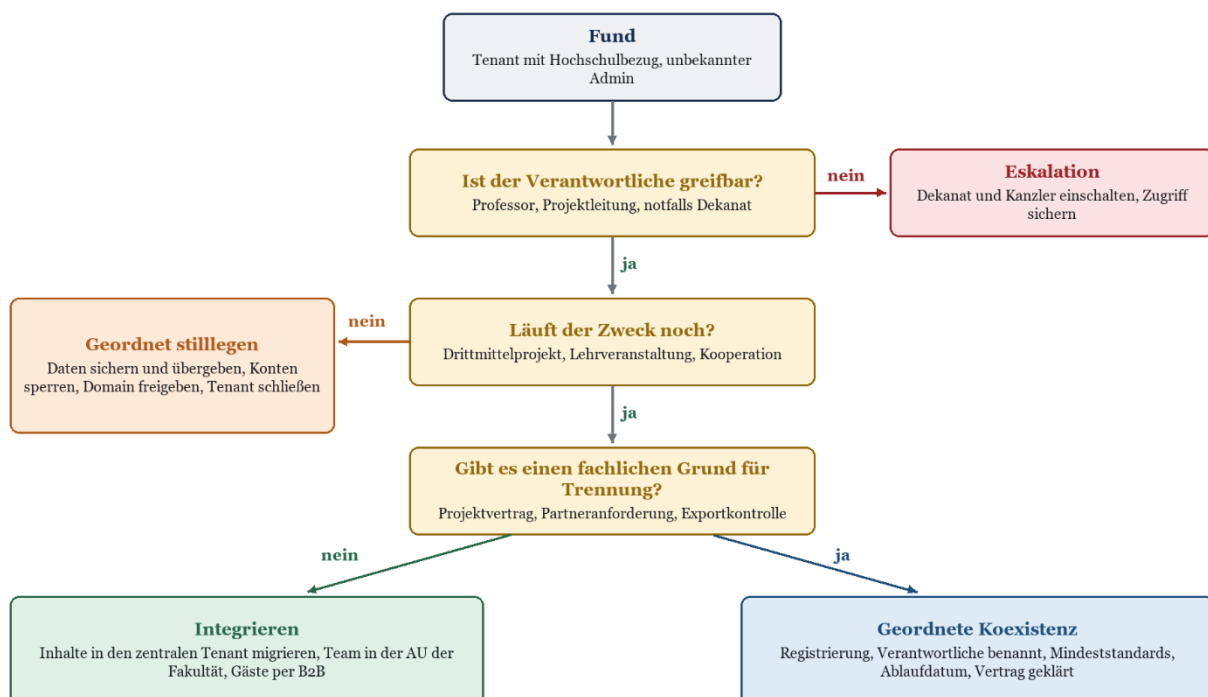
Umgang: Inventur, Amnestie, Entscheidung

Der erfolgreichste Umgang mit Schatten-Tenants beginnt mit einem Satz, der vielen Rechenzentren schwerfällt: „Wir wollen niemanden bestrafen, wir wollen wissen, was es gibt.“ Eine befristete Amnestie, angekündigt über Präsidium und Dekanate, bringt mehr Tenants ans Licht als jede technische Suche. Parallel lohnt sich die Suche in DNS-Zonen, im Überwachungsprotokoll, in den Rechnungen der Drittmittelverwaltung und in den Anmeldeprotokollen, wo Konten der Hochschule sich bei fremden Tenants als Gast anmelden.

Danach wird entschieden, Tenant für Tenant. Drei Ausgänge sind realistisch. Erstens die Integration: Inhalte wandern in den zentralen Tenant, das Team kommt in die AU der Fakultät, externe Partner werden als Gäste eingeladen. Zweitens die geordnete Koexistenz: Es gibt einen fachlichen Grund für einen eigenen Tenant, etwa weil ein Verbundprojekt ihn vertraglich verlangt oder weil Anforderungen der Exportkontrolle eine harte Trennung sinnvoll machen. Dann wird der Tenant registriert, bekommt benannte Verantwortliche, Mindeststandards für MFA und Protokollierung und ein Ablaufdatum. Drittens die geordnete Stilllegung: Daten sichern, Konten sperren, Domain freigeben, Tenant schließen.

Skizze 4: Ein Schatten-Tenant ist aufgetaucht. Und jetzt?

Erst verstehen, dann entscheiden. Löschen ist die letzte Option, nicht die erste.



Entscheidungshilfe, kein Automatismus. Rechtliche Fragen (Auftragsverarbeitung, Verantwortlichkeit) gesondert klären.

Für die Zukunft brauchen Sie dann eine Regel, und sie sollte erstaunlich kurz sein: Neue Tenants mit Hochschulbezug werden beim Rechenzentrum angezeigt, Hochschuldomains werden nur nach Freigabe in anderen Tenants verifiziert, und für Verbundprojekte gibt es einen dokumentierten

Standardweg über Gastzugriff oder mandantenübergreifende Synchronisation. Wenn dieser Standardweg schneller ist als ein eigener Tenant, ist das Problem zu zwei Dritteln gelöst. Das letzte Drittel ist Gewohnheit, und Gewohnheiten ändern sich an Hochschulen etwa im Rhythmus von Berufungsverfahren.

TYPISCHE SITUATION · Wenn jedes Amt seinen eigenen Mandanten hat

Aus anonymisierter Projekterfahrung bei einem kommunalen Verband: Bei der Bestandsaufnahme vor einer zentralen Einführung fanden sich neben dem offiziellen Tenant mehrere weitere, angelegt von einzelnen Fachbereichen für Projekte, Tests und eine Kooperation mit externen Partnern. Zwei liefen auf Subdomains des Verbands, einer auf die persönliche Adresse eines inzwischen ausgeschiedenen Mitarbeiters. Lizenzen wurden aus Sachmitteln bezahlt, Konten nie gesperrt.

Gelöst wurde das nicht mit einem Verbot, sondern mit einer Inventur ohne Schuldzuweisung, einem einfachen Formular zur Registrierung und einer klaren Entscheidung pro Fund. Zwei Tenants wurden integriert, einer blieb für die Dauer einer Kooperation mit Mindeststandards bestehen, der verwaiste wurde nach Sicherung der Daten über den Microsoft-Support stillgelegt. Das dauerte Monate, nicht Wochen.

Übertragen auf die Hochschule: Ersetzen Sie Fachbereich durch Lehrstuhl, Kooperation durch Verbundprojekt und den ausgeschiedenen Mitarbeiter durch einen Postdoc, der jetzt in Übersee forscht. Die Lage ist dieselbe, nur die Zahl der Funde ist meist höher.

Governance, die eine Senatssitzung übersteht

Technik ist an dieser Stelle der leichtere Teil. Administrative Units sind an einem Nachmittag eingerichtet, PIM an zwei. Was Monate dauert, ist die Einigung darüber, wer was entscheidet. Und weil an Hochschulen viele Stellen mitreden dürfen und es auch tun, braucht die Governance eine Form, die diese Stellen einbindet, statt sie zu umgehen.

Delegationsvereinbarung statt Dekret

Bewährt hat sich eine schriftliche Delegationsvereinbarung zwischen Rechenzentrum und jeder Fakultät bzw. jedem Fachbereich, die das Dekanat mitzeichnet. Darin steht, welche Rollen die Fakultäts-IT bekommt, für welche AU, über welchen Aktivierungsweg und mit welchen Pflichten: MFA mit phishingresistenten Verfahren für Admin-Konten, getrennte Admin-Konten, Teilnahme an Schulungen, Meldung von Sicherheitsvorfällen, Mitwirkung bei Rezertifizierungen. Im Gegenzug sagt das Rechenzentrum Reaktionszeiten für Anträge und Transparenz bei tenantweiten Änderungen zu.

Für außeruniversitäre Forschungseinrichtungen gilt das sinngemäß zwischen Zentrale und Instituten, mit dem Unterschied, dass die Institute oft eigene Rechtsträger oder zumindest eigene Haushalte haben. Die Spannungen dort beschreibt der Beitrag [Microsoft 365 in außeruniversitären Forschungseinrichtungen: Institute zwischen Zentrale und Eigenständigkeit](#).

Personalrat und Protokolle

Dezentrale Administration hat eine Seite, die gern übersehen wird: Wer Konten verwaltet, sieht Anmeldedaten, Gerätedaten und häufig auch Nutzungsprotokolle. Fakultäts-IT und Lehrstuhl-Admins sitzen oft im selben Flur wie die Menschen, deren Protokolle sie sehen können. Das macht die Frage nach Verhaltens- und Leistungskontrolle konkreter als in einem zentralen Rechenzentrum. Regeln Sie deshalb in der Dienstvereinbarung nicht nur, welche Daten erhoben werden, sondern auch, welche delegierten Rollen welche Protokolle sehen dürfen und zu welchem Zweck. Wie das in den Personalvertretungsgesetzen der Länder unterschiedlich ausgestaltet ist und wie wissenschaftliches Personal dort vertreten wird, behandelt der Beitrag [Personalrat und](#)

Microsoft 365 an der Hochschule: Dienstvereinbarung, wissenschaftliches Personal und die Verhaltenskontrolle.

Die Schrittfolge für den Einstieg

Wer mit einem gewachsenen Tenant startet, kann sich an dieser Reihenfolge orientieren:

1. **Bestand erheben:** Wer hat heute welche Rolle, dauerhaft oder befristet, tenantweit oder begrenzt? Welche Gruppen haben keinen oder nur einen Besitzer?
2. **Quelldaten prüfen:** Sind Organisationseinheiten im Personal- und Studentendatensatz so gepflegt, dass dynamische AU-Regeln funktionieren?
3. **Zuständigkeitsmatrix abstimmen:** Aufgabe, zentral, delegiert, Werkzeug, mit Fakultäten, Kanzler und Personalrat.
4. **AUs und Rollen einrichten:** Zuerst eine Pilotfakultät, dann die übrigen. Vertrauliche Gruppen in eingeschränkte AUs.
5. **PIM einschalten:** Globale Rollen zuerst, dann die delegierten Rollen der Fakultäts-IT.
6. **Gruppenregeln festlegen:** Anlagemodell, Namensrichtlinie, Ablaufrichtlinie, Ersatzadresse für besitzerlose Gruppen.
7. **Tenant-Erstellung beschränken und Schatten-Tenants inventarisieren:** mit Amnestie und klaren Ausgängen.
8. **Rezertifizieren:** Mindestens jährlich, besser zum Semesterwechsel, prüfen, wer welche Rolle noch braucht.

TIPP · Schulung ist Teil der Delegation

Wer Rechte delegiert, delegiert Verantwortung. Fakultäts-IT und Lehrstuhl-Admins, die PIM, AU-Rollen und Gruppenpflege nur aus Screenshots kennen, machen Fehler an genau den Stellen, die später teuer werden. Eine kurze, praxisnahe Einweisung vor der Freischaltung zahlt sich aus. Passende Formate finden Sie unter [Microsoft-365-Schulung für Hochschulen und Forschung](#).

Wer das Modell mit externer Unterstützung entwerfen möchte, findet Hinweise zur [Microsoft-365-Beratung für Hochschulen und Forschung](#). Die Grundsatzfragen, warum der Campus überhaupt anders funktioniert als Verwaltung und Wirtschaft, behandelt der Beitrag [Microsoft 365 an Hochschulen: Wo der Campus anders tickt als Verwaltung und Wirtschaft](#).

FAQ: Häufige Fragen zur dezentralen IT im Hochschul-Tenant

Können wir jeder Fakultät einen eigenen Tenant geben?

Technisch ja, praktisch selten sinnvoll. Mehrere Tenants bedeuten mehrere Identitäten pro Person, getrennte Adressbücher, Gastzugriffe zwischen den eigenen Fakultäten und vervielfachten Verwaltungsaufwand. Für Hochschulen ist ein Tenant mit Administrative Units der Normalfall; eigene Tenants bleiben die gut begründete Ausnahme.

Kann die Fakultäts-IT eigene Conditional-Access-Richtlinien bauen?

Nein, nicht im Sinne eigener Zuständigkeit. Conditional Access wird tenantweit verwaltet. Richtlinien lassen sich zwar auf Gruppen einer Fakultät ausrichten, verwaltet werden sie aber zentral. Wünsche der Fakultäten fließen über einen Antrag ein.

Brauchen Lehrstühle Administratorrollen, um ihre Teams zu verwalten?

In aller Regel nicht. Besitzer eines Teams können Mitglieder und Gäste im Rahmen der Gastrichtlinie verwalten, Kanäle anlegen und Einstellungen des Teams ändern. Eine Verzeichnisrolle ist dafür nicht nötig.

Verstößt eine Namenskonvention gegen die Freiheit von Forschung und Lehre?

Ein Präfix im Teamnamen regelt die Organisation der Zusammenarbeit, nicht Inhalt oder Methode der Forschung. Rechtlich verbindlich beurteilen kann das nur das Justizariat Ihrer Hochschule; in der Praxis ist eine gut begründete und transparent beschlossene Konvention selten strittig.

Was tun, wenn wir einen Schatten-Tenant ohne erreichbaren Administrator finden?

Zuerst klären, wer fachlich verantwortlich ist und welche Daten betroffen sein könnten. Anschließend gibt es Verfahren, mit denen der Inhaber einer verifizierten Domain die Kontrolle übernehmen oder die Domain freibekommen kann; die Details unterscheiden sich je nach Konstellation und laufen häufig über den Microsoft-Support. Datenschutzbeauftragte früh einbinden.

Wie viele globale Administratoren sind vernünftig?

So wenige wie möglich, aber nicht einer allein. Üblich sind einige wenige Personen im Rechenzentrum, die die Rolle ausschließlich über PIM aktivieren, plus zwei Notfallkonten, die gesondert gesichert und überwacht werden.

Gilt die Ablauffrichtlinie auch für Kursteams?

Wenn sie für alle Gruppen eingeschaltet ist, ja. Kursteams werden in der Regel im Semester genutzt und damit automatisch verlängert. Nach dem Semester greift die Erinnerung an die Besitzer. Ob ein Kursteam danach archiviert, gelöscht oder für Nachprüfungen erhalten bleibt, sollte die Hochschule vorher festlegen.

Fazit: Föderalismus mit Generalschlüssel-Verbot

Dezentrale IT ist an Hochschulen kein Betriebsunfall, den man mit einer zentralen Plattform endlich beheben könnte. Sie ist Ausdruck dessen, wie Hochschulen funktionieren. Microsoft 365 zwingt sie in einen gemeinsamen Tenant, und das ist gleichzeitig Zumutung und Chance. Zumutung, weil tenantweite Entscheidungen gemeinsam getroffen werden müssen. Chance, weil Administrative Units, fein geschnittene Rollen und PIM eine Delegation ermöglichen, die sicherer ist als die meisten gewachsenen Strukturen davor.

Die Formel ist schlicht: Das Rechenzentrum hält die Richtlinien, die Fakultäts-IT hält ihren Ausschnitt, der Lehrstuhl hält seine Teams, und niemand hält einen Generalschlüssel auf Dauer. Dazu eine Namensregel, die man versteht, ein Lebenszyklus, der niemanden überrascht, und ein gelassener Umgang mit Schatten-Tenants. Das klingt nicht spektakulär. Aber wenn in zehn Jahren jemand eine Entra-ID-Überprüfung macht und nur die üblichen Sünden findet statt einer archäologischen Grabungsstätte, dann hat sich die Mühe gelohnt.

WEITERLESEN · Weiterlesen

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

- › [Microsoft 365 in Hochschule und Forschung](#)
- › [Microsoft 365 an Hochschulen: Wo der Campus anders tickt als Verwaltung und Wirtschaft](#)
- › [Microsoft 365 in außeruniversitären Forschungseinrichtungen: Institute zwischen Zentrale und Eigenständigkeit](#)
- › [Personalrat und Microsoft 365 an der Hochschule: Dienstvereinbarung, wissenschaftliches Personal und die Verhaltenskontrolle](#)
- › [Datenschutz und Microsoft 365 an Hochschulen: Zwischen DSK-Bewertung, Landesaufsicht und Campus-Realität](#)
- › [Education-Lizenzen verstehen: A1, A3, A5 und der Student Use Benefit](#)
- › [Microsoft-365-Beratung für Hochschulen und Forschung](#)

› [Microsoft-365-Schulung für Hochschulen und Forschung](#)