

Entra-ID-Überprüfung für Hochschul-Tenants: Was sich nach zehn Jahren Wildwuchs findet

Microsoft 365 · Hochschule · Identität

Entra-ID-Überprüfung für Hochschul-Tenants: Was sich nach zehn Jahren Wildwuchs findet

Jeder Tenant hat einen Keller. Die Frage ist nur, wer zuletzt das Licht angemacht hat.

Verwaiste Konten

Gäste ohne Sponsor

Lehrstuhl-Apps

Globale Administratoren

Legacy-Authentifizierung

Notfallkonten

Benutzereinwilligung

Rein lesend

boddenberg.de

WISSEN

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

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

BERATUNG

Entra-ID-Überprüfung Ihres Hochschul-Tenants: rein lesend, werkzeuggestützt, mit Bewertung und Maßnahmenplan.

› [Beratung für Hochschulen und Forschung](#)

SCHULUNG

Für Rechenzentrum und Fakultäts-IT: Rollen, Apps, Gäste und Anmeldeprotokolle in Entra ID selbst prüfen.

› [Schulungen für Hochschulen und Forschung](#)

Irgendwann um 2015 hat jemand im Hochschulrechenzentrum den Tenant angelegt. Vielleicht für Office für Studenten, vielleicht für ein Pilotprojekt am Lehrstuhl für Wirtschaftsinformatik, vielleicht, weil das Präsidium nach einer Messe plötzlich Teams wollte. Die Person, die damals den ersten globalen Administrator angelegt hat, ist inzwischen in Pension, an einer anderen Hochschule oder in der freien Wirtschaft. Ihr Konto ist noch da. Es hat noch die Rolle. Und es hat, das ist die eigentliche Pointe, nie einen zweiten Faktor gesehen.

Zehn Jahre später ist der Tenant ein Gebäude mit vielen Anbauten. Jedes Semester sind Tausende neue Studenten eingezogen, Tausende andere ausgezogen, ohne dass jemand ihre Schlüssel eingesammelt hätte. Verbundprojekte haben Gäste mitgebracht, die nach Projektende einfach dageblieben sind. Lehrstühle haben sich eigene Anwendungen registriert, weil das Rechenzentrum zu langsam war oder weil niemand wusste, dass man fragen sollte. Und für den Scanner im Prüfungsamt, der Mails nur mit Kennwort verschicken kann, gibt es eine Ausnahme, die niemand mehr erklären kann.

Eine Entra-ID-Überprüfung macht im Keller das Licht an. Sie verändert dabei nichts, sie schaut nur hin: werkzeuggestützt, rein lesend, mit klarer Bewertung nach kritisch, mittel und niedrig und einem Maßnahmenplan, den das Hochschulrechenzentrum anschließend selbst umsetzen kann. Dieser Beitrag gehört zur Serie [Microsoft 365 in Hochschule und Forschung](#) und beschreibt, was sich in gewachsenen Hochschul-Tenants typischerweise findet, wie eine solche Überprüfung abläuft und was danach passieren sollte. Allgemeinbildende Schulen und Universitätsklinika haben eigene Rahmenbedingungen und sind hier nicht gemeint.

FAKTEN · Worum es in diesem Beitrag geht

Befundlage: verwaiste Konten, Gäste ohne Sponsor, selbst angelegte Apps, zu viele globale Administratoren, Legacy-Authentifizierung, fehlende Notfallkonten, offene Benutzereinstellung.
Vorgehen: rein lesende Bestandsaufnahme mit Werkzeugen, die nichts verändern.
Bewertung: kritisch, mittel, niedrig, mit nachvollziehbaren Kriterien.
Ergebnis: Maßnahmenplan mit Sofortmaßnahmen, 30 und 90 Tagen und Dauerbetrieb.
Beteiligung: Datenschutz und Personalrat, bevor die erste Abfrage läuft.

Warum Hochschul-Tenants schneller verwildern als andere

In einer Stadtverwaltung kommen und gehen pro Jahr ein paar Dutzend Mitarbeiterinnen und Mitarbeiter, die Personalabteilung meldet jeden Fall, und am Ende des Monats wird das Konto deaktiviert. An einer Hochschule wechselt mit jedem Semester ein spürbarer Teil der Benutzer. Dazu kommen Gruppen, die es in der Verwaltung so nicht gibt: Lehrbeauftragte mit Vertrag für ein Semester, Gastwissenschaftler für drei Monate, Emeriti, die ihre Mailadresse behalten sollen, studentische Hilfskräfte mit Verträgen, die kürzer sind als manche Kennwortrichtlinie, und Partner aus Verbundprojekten, die irgendwann als Gast eingeladen wurden.

Hinzu kommt die Struktur. Die Freiheit von Forschung und Lehre ist kein Lippenbekenntnis, sondern prägt die IT-Landschaft. Fakultäten, Institute und Lehrstühle betreiben eigene IT, haben eigene Administratoren und eigene Vorstellungen davon, was zentral zu regeln ist. Das ist legitim und oft gut begründet, erzeugt aber im gemeinsamen Tenant genau die Art von Ablagerungen, die eine Überprüfung findet. Wie man dezentrale Administration sauber organisiert, beschreibt der Beitrag [Dezentrale IT an der Hochschule: Lehrstuhl-Admins, Fakultäts-IT und ein Tenant für alle](#).

Und schließlich die Zeit. Viele Hochschul-Tenants sind älter als die Sicherheitsstandards, an denen sie heute gemessen werden. Was 2016 eine vernünftige Einstellung war, ist heute ein Befund. Niemand hat dabei etwas falsch gemacht. Es hat nur niemand nachgeschaut.

TYPISCHE SITUATION · Typische Situation, übertragen auf die Hochschule

In einer Stadtverwaltung fand sich bei einer Überprüfung ein globaler Administrator, der einem längst beendeten Dienstleistervertrag gehörte. Das Konto war aktiv, hatte ein Kennwort, das seit Jahren nicht geändert worden war, und keinen zweiten Faktor. Niemand hatte es bewusst stehen lassen; es war nur nie auf einer Liste aufgetaucht, weil es keine Personalnummer hatte.

An der Hochschule ist dieselbe Lage wahrscheinlicher, nicht unwahrscheinlicher: Einführungsprojekte, Dienstleister für die Migration des Mailsystems, Firmen für die Telefonanlage, ein Doktorand, der damals geholfen hat. Konten ohne Personalnummer und ohne Matrikelnummer fallen durch jedes Raster, das auf Personal- oder Studentendaten aufsetzt.

Was sich findet: die typische Befundlage

Die folgenden Befunde tauchen in gewachsenen Tenants so regelmäßig auf, dass man sie fast als Grundausstattung bezeichnen könnte. Nicht jeder Tenant hat jeden Befund, aber kaum einer hat keinen. Die Reihenfolge entspricht nicht der Schwere; die Einstufung folgt weiter unten.

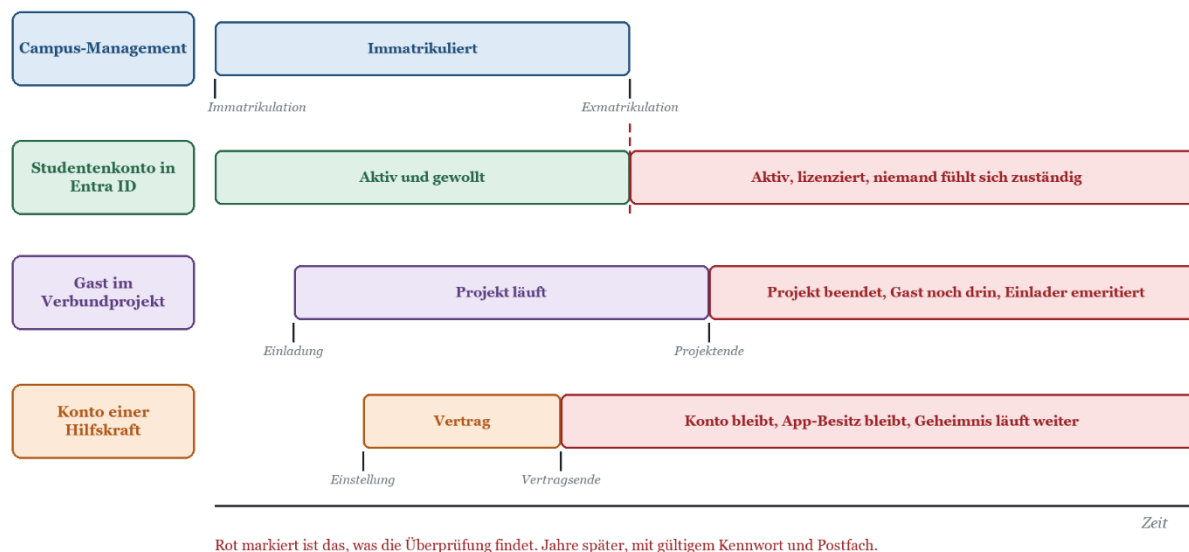
Verwaiste Konten ausgeschiedener Studenten und Gäste

Der Klassiker. Die Exmatrikulation wird im Campus-Management sauber erfasst, aber die Information erreicht Entra ID nicht oder nur halb. Das Konto bleibt aktiv, behält seine Lizenz, sein Postfach und seinen OneDrive. Wer das Kennwort kennt, kann sich weiter anmelden, und wer es per Phishing erbeutet, ebenfalls, ohne dass sich ein echter Mensch über ungewöhnliche Anmeldungen wundert. Verwaiste Konten sind die bevorzugte Beute, weil niemand sie vermisst.

Entra ID protokolliert für jedes Konto die letzte Anmeldung. Über Microsoft Graph stehen dafür drei Werte zur Verfügung: der letzte interaktive Anmeldeversuch, die letzte nicht interaktive Anmeldung und die letzte erfolgreiche interaktive Anmeldung. Für den letzten Wert verlangt Microsoft eine Lizenz für Entra ID P1 oder P2. Microsoft nennt für Inaktivität ein Zeitfenster zwischen 90 und 180 Tagen als üblich. An der Hochschule ist das zu kurz gedacht: Die vorlesungsfreie Zeit, ein Auslandssemester oder ein Forschungsfreisemester erzeugen legitime Pausen. Deshalb gehört zur Analyse immer der Abgleich mit dem Status im Campus-Management oder im Personalsystem.

Die Zombie-Phase

Das Campus-Management weiß, dass jemand gegangen ist. Entra ID erfährt es manchmal nie.



Skizze 2: Wo Konten nach dem Ende ihres Zwecks weiterleben

Wie der Lebenszyklus von der Immatrikulation bis zum Alumni-Konto automatisiert und damit an der Wurzel repariert wird, behandelt der Beitrag [Identity Lifecycle an der Hochschule: Von der Immatrikulation bis zum Alumni-Konto](#). Die Überprüfung liefert dafür die Ausgangsbasis: Wie viele Konten sind betroffen, aus welchen Jahrgängen, und welche Quelle hätte sie eigentlich abschalten müssen?

Gastkonten ohne Sponsor

Verbundprojekte, Gutachter in Berufungsverfahren, externe Prüfer, Kooperationen mit Unternehmen: Hochschulen laden ständig Gäste ein. Entra ID kann jedem Gast einen Sponsor zuordnen, also eine Person, die für die Einladung geradesteht. In gewachsenen Tenants ist dieses Feld meist leer, oder der Sponsor ist selbst längst ausgeschieden. Der Gast bleibt Mitglied in Teams, hat Zugriff auf Projektordner und bekommt im schlimmsten Fall noch Jahre später Sitzungsunterlagen.

Hinzu kommt die Frage, wer überhaupt einladen darf. Ist die Einstellung offen, kann jedes Mitglied Gäste einladen, und zwar ohne dass das Rechenzentrum davon erfährt. Für Microsoft 365 ist das bequem, für die Überprüfung ein Fundus. Wie Gastwissenschaftler, Lehrbeauftragte und Emeriti ordentlich abgebildet werden, erklärt der Beitrag [Gastwissenschaftler, Lehrbeauftragte, Emeriti: Sonderrollen in Entra ID sauber abbilden](#).

App-Registrierungen und Unternehmensanwendungen vom Lehrstuhl

In vielen Tenants dürfen alle Benutzer App-Registrierungen anlegen, weil das die Voreinstellung war und niemand sie geändert hat. Das Ergebnis ist eine Liste mit Hunderten Einträgen: Skripte

für den Versand von Kursmails, Anbindungen an selbst gebaute Webanwendungen, Experimente aus Abschlussarbeiten, Testanwendungen aus einem Hackathon. Viele davon sind harmlos. Einige wenige haben Anwendungsberechtigungen, die mandantenweit gelten, ein Client-Geheimnis mit sehr langer Laufzeit und als Besitzer ein Konto, das zu einer ehemaligen Hilfskraft gehört.

Gefährlich ist dabei der Unterschied zwischen delegierten Berechtigungen und Anwendungsberechtigungen. Eine delegierte Berechtigung handelt im Namen eines angemeldeten Benutzers und kann nicht mehr, als dieser darf. Eine Anwendungsberechtigung handelt ohne Benutzer, und wenn sie etwa Lesezugriff auf alle Postfächer gewährt, dann gilt das für das Postfach der Präsidentin ebenso wie für das Prüfungsamt. Wer das Geheimnis besitzt, besitzt den Zugriff.

Vom Lehrstuhl-Skript zum Zugriff auf alle Postfächer

Ein typischer Befundpfad bei selbst angelegten App-Registrierungen



Was die Überprüfung an jeder Station fragt



Skizze 3: Fünf Stationen, fünf Fragen, ein Befund der Kategorie kritisch

WARNUNG · Ein Geheimnis im Repository ist kein Geheimnis

Client-Geheimnisse landen erstaunlich oft in Quellcode, Konfigurationsdateien oder Wiki-Seiten des Lehrstuhls. Ist das Repository öffentlich oder wird es beim Lehrstuhlwechsel mitgenommen, ist der Zugang in fremden Händen, ohne dass eine Anmeldung eines Menschen jemals auffällt. Die Überprüfung kann nicht sehen, wo ein Geheimnis liegt. Sie kann aber zeigen, welche Anwendung welche Berechtigung mit welchem Geheimnis hat, und damit, welche Geheimnisse man besser heute als morgen erneuert.

Zu viele globale Administratoren

Microsoft empfiehlt ausdrücklich, die Rolle des globalen Administrators an weniger als fünf Personen zu vergeben, und blendet ab fünf Zuweisungen im Entra Admin Center einen Hinweis ein. Für alle privilegierten Rollen zusammen nennt Microsoft eine Obergrenze von weniger als zehn Zuweisungen. In Hochschul-Tenants finden sich regelmäßig deutlich mehr: das halbe Rechenzentrum, die Fakultäts-IT der Informatik, zwei Dienstleister, ein Funktionskonto für ein Synchronisationswerkzeug und der Kollege, der 2018 mal schnell etwas freischalten musste.

Hinzu kommen Administratorkonten, die aus dem lokalen Active Directory synchronisiert werden. Microsoft rät davon ab, weil eine Kompromittierung im lokalen Verzeichnis dann direkt in die Cloud durchschlägt. Und schließlich die Frage, ob privilegierte Rollen dauerhaft oder nur bei Bedarf aktiv sind. Privileged Identity Management setzt Entra ID P2 oder Entra ID Governance

voraus; welche Lizenzen Ihre Hochschule tatsächlich hat, klärt der Beitrag [Education-Lizenzen verstehen: A1, A3, A5 und der Student Use Benefit](#).

Legacy-Authentifizierung für Altgeräte

Multifunktionsgeräte im Dekanat, Messgeräte im Labor, die Ergebnisse per Mail verschicken, ein IMAP-Abruf für ein altes Ticketsystem, ein Skript, das seit Jahren SMTP mit Benutzername und Kennwort spricht. Legacy-Authentifizierung kann keinen zweiten Faktor, und deshalb ist sie bei Angriffen mit erratenen oder gestohlenen Kennwörtern der bevorzugte Weg. Exchange Online hat die Standardauthentifizierung für die meisten Protokolle längst abgeschaltet. Für den Mailversand per SMTP AUTH hat Microsoft den Termin mehrfach verschoben; maßgeblich ist der jeweils aktuelle Stand im Microsoft 365 Message Center.

Die Überprüfung zeigt in den Anmeldeprotokollen, welche Konten noch mit welchen Legacy-Clients unterwegs sind und ob eine Richtlinie für bedingten Zugriff sie blockiert. Das Ergebnis ist meist eine kurze Liste von Geräten, über die man reden muss, und eine lange Liste von Konten, bei denen Angreifer es versucht haben. Wie MFA und bedingter Zugriff an der Hochschule eingeführt werden, ohne dass das Helpdesk kollabiert, steht im Beitrag [MFA für 30.000 Studenten: Conditional Access an der Hochschule ohne Helpdesk-Kollaps](#).

Fehlende oder falsch gebaute Notfallkonten

Ein Notfallkonto ist das Konto, das man braucht, wenn alles andere nicht mehr geht: Die Föderation mit dem eigenen Identity Provider ist ausgefallen, eine Richtlinie für bedingten Zugriff sperrt versehentlich alle Administratoren aus, oder der Mobilfunk ist weg. Gerade an Hochschulen, die Entra ID an Shibboleth oder eine andere föderierte Anmeldung koppeln, ist das kein theoretischer Fall. Mehr dazu im Beitrag [Entra ID und Shibboleth: Microsoft 365 an die DFN-AAI-Welt anbinden](#).

Microsoft empfiehlt mindestens zwei Notfallkonten, die reine Cloudkonten mit der Domäne onmicrosoft.com sind, weder föderiert noch synchronisiert. Sie sollen mit einer phishingresistenten Methode geschützt sein, vorzugsweise einem Passkey auf einem FIDO2-Schlüssel, und zwar mit einer anderen Methode als die normalen Administratorkonten. Von Richtlinien, die die Anmeldung blockieren oder einschränken, werden sie ausgenommen; jede Anmeldung löst eine Benachrichtigung aus, und ihre Funktion wird mindestens alle 90 Tage getestet. In der Praxis findet die Überprüfung drei Varianten: kein Notfallkonto, ein Notfallkonto mit dem Smartphone des Rechenzentrumsleiters als zweitem Faktor, oder zwei vorbildliche Notfallkonten, deren Kennwort in einem Umschlag liegt, von dem niemand mehr weiß, in welchem Tresor.

FAKTEN • Notfallkonten nach Microsoft-Empfehlung

Mindestens zwei Konten, reine Cloudkonten mit onmicrosoft.com-Domäne.

Phishingresistente Anmeldung, bevorzugt Passkey auf FIDO2-Schlüssel, alternativ zertifikatbasiert, wenn eine eigene PKI vorhanden ist.

Andere Methode als bei den normalen Administratorkonten.

Ausgenommen von Richtlinien, die die Anmeldung blockieren oder einschränken; Richtlinien im Berichtsmodus brauchen keine Ausnahme.

Rolle des globalen Administrators dauerhaft aktiv, nicht nur berechtigt.

Alarm bei jeder Anmeldung, Funktionstest mindestens alle 90 Tage.

Benutzereinwilligung für Apps offen

Benutzer können Anwendungen den Zugriff auf eigene Daten erlauben, ohne dass ein Administrator gefragt wird. Das ist die Grundlage für Consent-Phishing: Eine freundlich benannte App bittet um Zugriff auf Postfach und Dateien, der Student klickt auf Akzeptieren, und die App liest fortan mit, ganz ohne gestohlenes Kennwort und unbeeindruckt vom zweiten Faktor.

Microsoft hat die Voreinstellung seit Juli 2025 auf eine von Microsoft verwaltete Richtlinie umgestellt, die die Einwilligung für Zugriff auf Dateien und Websites durch Drittanbieter-Apps einschränkt. Das ändert aber nichts an Tenants, in denen die Einstellung früher ausdrücklich auf die alte, offene Variante gesetzt wurde, und nichts an den Einwilligungen, die bereits erteilt sind: Eine Änderung der Einstellung wirkt nur für künftige Einwilligungen. Die Überprüfung schaut deshalb auf beides, die Einstellung und den Bestand.

Was sonst noch im Keller steht

- **Gruppen und Teams ohne Besitzer:** Kursteams vergangener Semester, Projektgruppen abgeschlossener Drittmittelprojekte, Teams, deren einziger Besitzer emeritiert ist.
- **Veraltete Geräteobjekte:** Laptops, die längst verschrottet sind, aber als registriertes Gerät weiterleben und die Aussagekraft gerätebasierter Regeln verwässern.
- **Rollen direkt an Personen statt an Gruppen:** jede Zuweisung einzeln, keine Gruppe, keine Rezertifizierung.
- **Mandantenerstellung durch Benutzer:** Wenn Benutzer eigene Tenants anlegen dürfen, entstehen Schatten-Tenants mit Hochschuldaten.
- **Selbst angelegte Richtlinien für bedingten Zugriff:** aus verschiedenen Jahren, mit Ausnahmen für Personen, die längst nicht mehr da sind.

Die Befunde auf einen Blick

Befund	Risiko	Sofortmaßnahme
Verwaiste Studenten- und Gastkonten	Übernahme ohne Bemerkung, Phishing aus dem Hochschulnamen heraus, unnötige Lizenzen	Konten ohne Anmeldung und ohne gültigen Status im Quellsystem deaktivieren, nicht löschen
Gäste ohne Sponsor	Zugriff auf Teams und Projektdaten nach Projektende, niemand fühlt sich zuständig	Gäste über Mitgliedschaften einem Verantwortlichen zuordnen, Rest anschreiben und sperren
Apps mit mandantenweiten Anwendungsberechtigungen	Zugriff auf alle Postfächer oder Dateien ohne Benutzeranmeldung	Fachlich Verantwortlichen ermitteln, Geheimnis erneuern, Berechtigung einschränken oder App deaktivieren
Zu viele globale Administratoren	Jedes Konto ist ein Generalschlüssel, jede Übernahme ein Totalschaden	Auf das Nötige reduzieren, spezifische Rollen vergeben, nur Cloudkonten
Legacy-Authentifizierung	Kennwortangriffe ohne zweiten Faktor	Nutzung auswerten, Richtlinie im Berichtsmodus, Ausnahmen benennen, dann sperren
Keine oder fehlerhafte Notfallkonten	Aussperrung bei Ausfall der Föderation oder Fehlkonfiguration	Zwei Cloudkonten mit FIDO2, Ausnahme in Richtlinien, Alarm, Test
Benutzereinwilligung offen	Consent-Phishing, dauerhafter Datenzugriff trotz MFA	Einwilligung einschränken, Workflow für Administratorzustimmung, bestehende Einwilligungen prüfen
Benutzer dürfen Apps registrieren	Unkontrolliertes Wachstum, Besitzer verschwinden	Registrierung auf Rolle beschränken, Bestand dokumentieren

So läuft die Überprüfung: werkzeuggestützt und rein lesend

Der wichtigste Grundsatz steht vor jeder Technik: Während der Erhebung wird im Tenant nichts verändert. Keine Richtlinie wird aktiviert, kein Konto deaktiviert, keine App gelöscht, auch dann nicht, wenn der Befund offensichtlich ist. Das hat zwei Gründe. Erstens weiß zu diesem Zeitpunkt niemand, was eine scheinbar verwaiste App in der Prüfungsverwaltung noch tut. Zweitens lässt sich ein Ergebnis nur sauber bewerten, wenn die Ausgangslage nicht unterwegs verschoben wurde. Wer beim Erheben repariert, hat am Ende weder einen vollständigen Befund noch eine nachvollziehbare Änderung.

Ablauf der Überprüfung

Sechs Schritte, ein Grundsatz: Während der Erhebung wird im Tenant nichts verändert.



Ergebnis: ein Bericht mit Befundliste, Einstufung und Maßnahmenplan. Keine stillen Korrekturen nebenbei.

Die Nachprüfung zeigt, ob die Maßnahmen gegriffen haben und ob neuer Wildwuchs nachgewachsen ist.

Skizze 1: Ablauf einer werkzeuggestützten, rein lesenden Überprüfung

Zugriff: so wenig wie möglich, so lange wie nötig

Für die Erhebung reichen lesende Rollen. Der globale Leser sieht fast alles, was ein globaler Administrator sieht, kann aber nichts ändern. Für Anmeldeprotokolle kommt der Berichtsleser oder der Sicherheitsleser hinzu. Die Werkzeuge verwenden Microsoft Graph mit Berechtigungen, die ausschließlich lesen. Der Zugang wird befristet vergeben, mit einem eigenen Konto und mit phishingresistenter Anmeldung, und nach Abschluss entzogen.

Bereich	Lesende Graph-Berechtigung	Wofür
Verzeichnis	Directory.Read.All	Konten, Gruppen, Gäste, Geräte, Sponsoren
Anmeldeaktivität	AuditLog.Read.All	Letzte Anmeldung, Legacy-Clients, Überwachungsprotokoll
Richtlinien	Policy.Read.All	Bedingter Zugriff, Einwilligung, Authentifizierungsmethoden
Rollen	RoleManagement.Read.Directory	Zuweisungen, dauerhaft oder bei Bedarf
Anwendungen	Application.Read.All	App-Registrierungen, Dienstprinzipale, Geheimnisse, Berechtigungen
Berichte	Reports.Read.All	Registrierungsstand der Authentifizierungsmethoden

Werkzeuge: Bordmittel, Microsoft-Module und Open Source

Eine Überprüfung braucht keine geheimen Spezialwerkzeuge. Sie braucht die richtigen Abfragen, eine saubere Dokumentation und jemanden, der die Ergebnisse im Hochschulkontext lesen kann. Die folgenden Werkzeuge ergänzen sich; keines deckt allein alles ab.

Werkzeug	Was es liefert	Einordnung
Entra Admin Center und Empfehlungen	Übersicht, Hinweise zu Rollen, Anwendungen und Konfiguration	Gut für den ersten Blick, wenig für die Dokumentation
Microsoft Secure Score	Gewichtete Liste von Konfigurationsempfehlungen	Nützlich als Maßstab, kennt aber keine Hochschulbesonderheiten
Zero Trust Assessment von Microsoft	PowerShell-Modul, prüft Hunderte Konfigurationspunkte, Bericht als HTML	Arbeitet lesend und lokal; der Bericht selbst ist vertraulich zu behandeln
Microsoft Graph PowerShell	Eigene Abfragen zu Anmeldeaktivität, Gästen, Apps, Rollen	Unverzichtbar für alles, was über Standardprüfungen hinausgeht
Open-Source-Prüfwerkzeuge	Testsammlungen gegen Entra ID und Microsoft 365, teils aus dem Behördenumfeld	Wertvolle Ergänzung, Ergebnisse brauchen trotzdem Einordnung

Das Zero Trust Assessment von Microsoft ist ein gutes Beispiel für die Haltung, die eine Überprüfung braucht: Das Modul lädt die Konfiguration mit lesenden Berechtigungen herunter und wertet sie lokal aus. Für die erste Einwilligung in die nötigen Berechtigungen ist allerdings ein globaler Administrator nötig, und der fertige Bericht enthält genug Details über den Tenant, um einem Angreifer die Arbeit zu erleichtern. Er gehört also nicht in den Mailverteiler des Senats.

TIPP · Erst die Rohdaten, dann die Bewertung

Sichern Sie die Rohdaten der Erhebung als Datei mit Datum, bevor jemand interpretiert. Bei der Nachprüfung nach 90 Tagen laufen dieselben Abfragen noch einmal, und der Vergleich zeigt, was sich bewegt hat und was nachgewachsen ist. Ohne diese Ausgangsbasis bleibt nur das Bauchgefühl, und das hat im Präsidium erfahrungsgemäß wenig Gewicht.

Datenschutz und Personalrat vor der ersten Abfrage

Anmeldeprotokolle sind personenbezogene Daten. Wer sie auswertet, um verwaiste Konten zu finden, sieht zwangsläufig auch, wann sich Mitarbeiterinnen und Mitarbeiter angemeldet haben. Das ist nicht der Zweck der Überprüfung, aber es ist technisch möglich, und genau darauf schauen Datenschutzbeauftragte und Personalräte zu Recht. Die Erhebung sollte deshalb vorab beschrieben werden: welche Daten, zu welchem Zweck, wer sieht sie, wann werden sie gelöscht, und dass keine Auswertung einzelner Personen nach Verhalten oder Leistung erfolgt.

Ob und in welcher Form der Personalrat mitbestimmt, regelt das jeweilige Landespersonalvertretungsgesetz, und die Rechtsgrundlage für die Verarbeitung ergibt sich aus Landesdatenschutzrecht und Hochschulgesetz des jeweiligen Landes. Das unterscheidet sich zwischen den Bundesländern spürbar. Häufig deckt eine bestehende Dienstvereinbarung zu Microsoft 365 die Administration und damit auch die Überprüfung bereits ab; dann genügt eine Information. Die Hintergründe stehen in den Beiträgen [Datenschutz und Microsoft 365 an Hochschulen: Zwischen DSK-Bewertung, Landesaufsicht und Campus-Realität](#) und [Personalrat und Microsoft 365 an der Hochschule: Dienstvereinbarung, wissenschaftliches Personal und die Verhaltenskontrolle](#).

HINWEIS • Keine Rechtsberatung

Die Hinweise zu Datenschutz und Mitbestimmung beschreiben die typische Lage und ersetzen keine rechtliche Prüfung. Ob für die Auswertung von Anmeldeprotokollen eine Information genügt, eine Zustimmung des Personalrats nötig ist oder eine Ergänzung der Dienstvereinbarung, hängt vom Landesrecht und von den Vereinbarungen Ihrer Hochschule ab. Beziehen Sie Justizariat, Datenschutzbeauftragte und Personalrat frühzeitig ein.

Wer an den Tisch gehört

Beteiligte	Beitrag zur Überprüfung
Hochschulrechenzentrum	Zugang, technische Ansprechpartner, Wissen über Ausnahmen und Altlasten
Fakultäts- und Institut-IT	Erklärung zu selbst angelegten Apps, Gruppen und Administratorkonten in ihrem Bereich
Campus-Management und Personalverwaltung	Abgleich: Wer ist noch immatrikuliert, wer noch beschäftigt, wer hat einen Lehrauftrag?
Datenschutzbeauftragte	Zweckbindung, Löschfristen, Umgang mit dem Bericht
Personalrat	Information oder Mitbestimmung nach Landesrecht
CIO oder Kanzler	Auftrag, Priorisierung, Entscheidung über Maßnahmen mit Folgen für Fakultäten

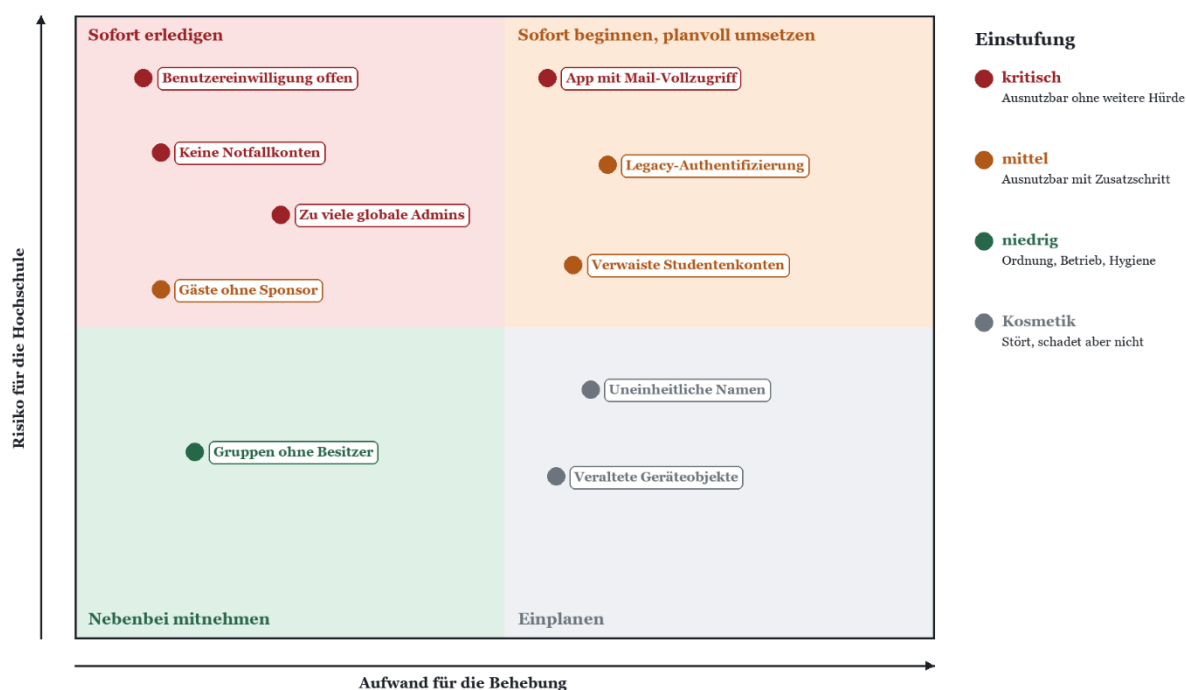
Bewertung und Maßnahmenplan

Eine Liste mit zweihundert Befunden ist kein Ergebnis, sondern eine Arbeitsverweigerung in Tabellenform. Den Wert der Überprüfung macht die Bewertung aus: Was ist gefährlich, was ist nur unordentlich, und was ist Absicht, die man dokumentieren sollte? Die Einstufung folgt dabei einer einfachen Frage: Wie weit ist ein Angreifer von einem Schaden entfernt, wenn er diesen Befund ausnutzt?

Stufe	Kriterium	Typische Beispiele	Frist
Kritisch	Ausnutzbar ohne weitere Hürde, Schaden für die ganze Hochschule	Kein Notfallkonto, globale Admins ohne MFA, App mit Vollzugriff auf Mail, offene Einwilligung	Sofort, innerhalb von Tagen
Mittel	Ausnutzbar mit einem Zusatzschritt oder begrenzter Wirkung	Legacy-Authentifizierung, verwaiste Konten, Gäste ohne Sponsor	Innerhalb von 30 Tagen
Niedrig	Betrieb, Ordnung, Nachvollziehbarkeit	Gruppen ohne Besitzer, veraltete Geräte, Rollen ohne Gruppen	Innerhalb von 90 Tagen oder im Dauerbetrieb

Bewertung: Risiko gegen Aufwand

Die Einstufung folgt dem Risiko. Der Aufwand entscheidet nur über die Reihenfolge.



Skizze 4: Typische Befunde, eingeordnet nach Risiko und Aufwand (schematisch, ohne Messwerte)

Die Skizze zeigt eine Eigenart, die in der Praxis oft übersehen wird: Viele kritische Befunde sind schnell behoben. Zwei Notfallkonten anzulegen dauert einen Nachmittag, die Einwilligung einzuschränken eine Viertelstunde plus die Kommunikation. Teuer sind meist die mittleren Befunde, weil sie Prozesse betreffen: Wer verwaiste Konten dauerhaft verhindern will, muss das Campus-Management anbinden, und wer Legacy-Authentifizierung abschaltet, muss mit dem Dekanat über den Scanner reden.

TYPISCHE SITUATION · Typische Situation, übertragen auf die Hochschule

In einem Krankenhausverbund fand sich eine App-Registrierung, die ein früherer Dienstleister für eine Schnittstelle angelegt hatte. Sie hatte mandantenweiten Lesezugriff auf alle Postfächer, ein Geheimnis mit mehrjähriger Laufzeit und keinen Besitzer mehr. Die Schnittstelle war seit Jahren außer Betrieb. Die Überprüfung stufte sie als kritisch ein; deaktiviert wurde sie erst nach einer Woche Beobachtung, in der sich niemand gemeldet hatte.

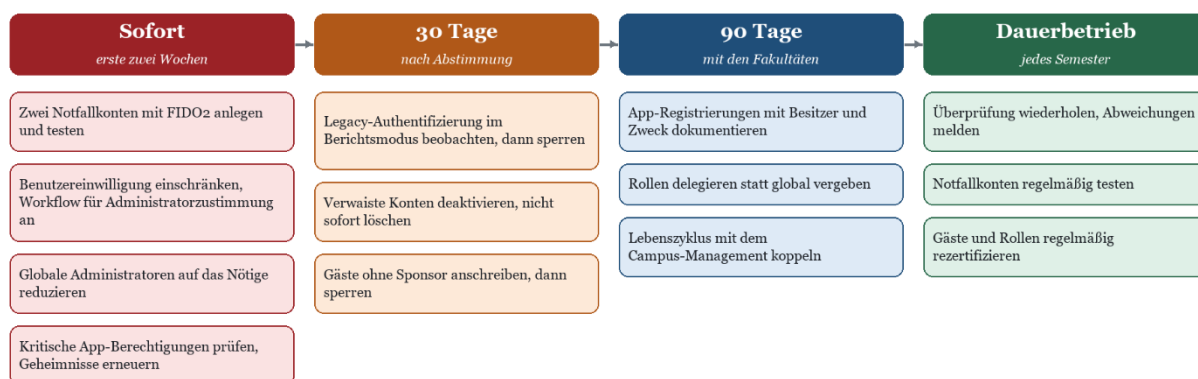
An der Hochschule ist der Dienstleister oft ein Lehrstuhl und die Schnittstelle ein Forschungsprototyp. Das Vorgehen ist dasselbe: erst deaktivieren und beobachten, dann löschen. Wer sofort löscht, erfährt beim nächsten Semesterstart, wofür die App doch noch gut war.

Vom Befund zum Maßnahmenplan

Der Maßnahmenplan ordnet jeden Befund einem Horizont zu und nennt für jede Maßnahme eine zuständige Stelle. Er ist so geschrieben, dass das Hochschulrechenzentrum ihn ohne externe Hilfe umsetzen kann. Wo eine Maßnahme Fakultäten oder Verwaltung betrifft, steht dabei, wer entscheiden muss: Ein Lehrstuhl verliert ungern eine App, und das Rechenzentrum sollte diese Diskussion nicht allein führen.

Vom Befund zum Maßnahmenplan

Vier Horizonte. Die kritischen Punkte warten nicht auf die nächste Senatssitzung.



Jede Maßnahme hat einen Namen daneben. Ein Plan ohne Zuständigkeit ist ein Wunschzettel.

Skizze 5: Der Maßnahmenplan in vier Horizonten

- **Sofort:** Notfallkonten, Einwilligung, globale Administratoren, kritische Apps. Diese Punkte brauchen keine Gremienentscheidung, sondern nur einen Termin.
- **30 Tage:** Legacy-Authentifizierung zuerst beobachten, dann sperren; verwaiste Konten deaktivieren; Gäste ohne Sponsor anschreiben.
- **90 Tage:** Apps dokumentieren, Rollen delegieren, Lebenszyklus mit dem Campus-Management koppeln. Das ist Projektarbeit mit den Fakultäten.
- **Dauerbetrieb:** Überprüfung jedes Semester wiederholen, idealerweise kurz vor Vorlesungsbeginn, wenn ohnehin aufgeräumt wird.

WARNUNG · Nicht zum Semesterstart aufräumen

Wer in der ersten Vorlesungswoche Tausende verwaiste Konten deaktiviert, erwischt mit Sicherheit auch ein paar, die gerade nach einem Urlaubssemester zurückkommen, und das Helpdesk erlebt eine Woche, über die man noch lange spricht. Massenänderungen gehören in die vorlesungsfreie Zeit, mit Ankündigung und mit einem Weg zurück.

Selbst prüfen oder prüfen lassen?

Ein Hochschulrechenzentrum, das sein Handwerk versteht, kann eine Überprüfung grundsätzlich selbst durchführen. Die Werkzeuge sind verfügbar, die Abfragen dokumentiert. Dass es trotzdem oft nicht passiert, hat drei Gründe: Im Tagesbetrieb fehlt die Zeit, der eigene Blick ist an die eigenen Altlasten gewöhnt, und ein Befund wie »zu viele globale Administratoren« lässt sich intern schwer vertreten, wenn man selbst einer davon ist.

Eine externe Überprüfung bringt den fremden Blick, die Vergleichserfahrung aus anderen öffentlichen Einrichtungen und einen Bericht, den Präsidium oder Kanzler als neutrale Grundlage lesen. Sie ersetzt das Rechenzentrum nicht, sie entlastet es. Entscheidend ist, dass die Überprüfung lesend bleibt und die Umsetzung bei denen liegt, die den Tenant auch danach betreiben.

WICHTIG · Entra-ID-Überprüfung für Ihre Hochschule

Wir führen die Entra-ID-Überprüfung für Hochschulen und Forschungseinrichtungen durch: rein

lesend, werkzeuggestützt, mit Bewertung nach kritisch, mittel und niedrig, einem Maßnahmenplan für Ihr Rechenzentrum und einer Zusammenfassung fürs Präsidium. Datenschutz und Personalrat beziehen wir von Anfang an ein. Details zum Ablauf finden Sie unter [Microsoft-365-Beratung für Hochschulen und Forschung](#).

Wenn Ihr Team die Überprüfung künftig selbst wiederholen möchte, zeigt die [Microsoft-365-Schulung für Hochschulen und Forschung](#) die Abfragen, Werkzeuge und Bewertungsmaßstäbe am eigenen Tenant.

Aspekt	Selbst durchgeführt	Extern begleitet
Zeitbedarf im Rechenzentrum	Hoch, konkurriert mit dem Tagesbetrieb	Gering, vor allem Gespräche und Abgleich
Blick auf Altlasten	Gewöhnt, blinde Flecken wahrscheinlich	Unbefangen, mit Vergleich aus anderen Einrichtungen
Wirkung im Präsidium	Interne Einschätzung	Neutraler Bericht als Entscheidungsgrundlage
Wissenstransfer	Bleibt im Haus	Muss bewusst eingeplant werden, etwa durch gemeinsame Auswertung
Wiederholung	Nach eigener Planung	Erste Runde extern, Folgeprüfungen intern möglich

Häufige Fragen zur Entra-ID-Überprüfung an Hochschulen

Verändert die Überprüfung etwas an unserem Tenant?

Nein. Die Erhebung arbeitet mit lesenden Rollen und lesenden Graph-Berechtigungen. Die einzige Ausnahme kann die einmalige Einwilligung in die Berechtigungen eines Prüfwerkzeugs sein, die ein globaler Administrator Ihrer Hochschule selbst erteilt und nach Abschluss wieder entfernt.

Wie lange dauert eine Überprüfung?

Das hängt vor allem von der Größe des Tenants und der Zahl der Fakultäten ab, deren Apps und Gruppen erklärt werden müssen. Die Datenerhebung selbst ist der kleinere Teil; die meiste Zeit fließt in den Abgleich mit dem Rechenzentrum und in die Bewertung.

Brauchen wir dafür Entra ID P1 oder P2?

Nicht zwingend, aber einige Auswertungen werden mit P1 genauer, etwa die letzte erfolgreiche Anmeldung. Privileged Identity Management und Zugriffsüberprüfungen setzen höhere Lizenzen voraus. Die Überprüfung zeigt auch, welche Funktionen Sie bereits lizenziert haben und nicht nutzen.

Muss der Personalrat zustimmen?

Das hängt vom Landespersonalvertretungsgesetz und von Ihrer Dienstvereinbarung ab. Informiert werden sollte er in jedem Fall, bevor die erste Abfrage läuft. Die Überprüfung wertet keine Personen nach Verhalten oder Leistung aus.

Was passiert mit dem Bericht?

Er ist vertraulich, weil er Schwachstellen beschreibt. Verteilt wird er an einen kleinen, vorab festgelegten Kreis; für Präsidium oder Kanzler gibt es eine Zusammenfassung ohne technische Details.

Dürfen wir verwaiste Konten einfach löschen?

Technisch ja, organisatorisch selten sofort. Löschfristen, Aufbewahrungspflichten für Prüfungs- und Personalvorgänge und Postfächer, die noch gebraucht werden, sprechen dafür, zuerst zu deaktivieren und erst nach einer festgelegten Frist zu löschen.

Wie oft sollte man die Überprüfung wiederholen?

Eine vollständige Überprüfung einmal, danach eine verkürzte Nachprüfung pro Semester. Die Notfallkonten testen Sie nach Microsoft-Empfehlung mindestens alle 90 Tage, unabhängig davon.

Gilt das auch für außeruniversitäre Forschungseinrichtungen?

Ja. Die Befunde sind ähnlich, nur die Ursachen unterscheiden sich: weniger Studentenkonten, dafür mehr Gastwissenschaftler, Verbundprojekte und häufig ein Spannungsfeld zwischen Institut und Zentrale.

Fazit: Licht anmachen, bevor es ein anderer tut

Ein Hochschul-Tenant nach zehn Jahren ist kein Skandal, sondern der Normalfall. Tausende Studenten sind gekommen und gegangen, Lehrstühle haben gebaut, was sie brauchten, und jede Ausnahme hatte zu ihrer Zeit einen guten Grund. Gefährlich wird es erst, wenn niemand mehr weiß, was im Keller steht, denn Angreifer machen dort sehr gern das Licht an, nur eben mit eigener Taschenlampe.

Eine werkzeuggestützte, rein lesende Überprüfung bringt Ordnung in diesen Bestand, ohne den Betrieb zu stören. Sie liefert eine ehrliche Liste, eine Bewertung, die Prioritäten setzt, und einen Maßnahmenplan, den das Rechenzentrum umsetzen kann. Die meisten kritischen Befunde sind in wenigen Tagen behoben. Der Rest ist Prozessarbeit, und die lohnt sich, weil der nächste Semesterwechsel bestimmt kommt.

WEITERLESEN · Weiterlesen

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

- › [Microsoft 365 in Hochschule und Forschung](#)
- › [MFA für 30.000 Studenten: Conditional Access an der Hochschule ohne Helpdesk-Kollaps](#)
- › [Gastwissenschaftler, Lehrbeauftragte, Emeriti: Sonderrollen in Entra ID sauber abbilden](#)
- › [Dezentrale IT an der Hochschule: Lehrstuhl-Admins, Fakultäts-IT und ein Tenant für alle](#)
- › [Identity Lifecycle an der Hochschule: Von der Immatrikulation bis zum Alumni-Konto](#)
- › [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](#)