

MFA für 30.000 Studenten: Conditional Access an der Hochschule ohne Helpdesk-Kollaps

Microsoft 365 · Hochschule · Identität

MFA für 30.000 Studenten: Conditional Access an der Hochschule ohne Helpdesk-Kollaps

Der zweite Faktor ist schnell eingeschaltet. Das Telefon am Helpdesk klingelt trotzdem dreißigtausendmal.

Authenticator Passkeys und FIDO2 Zugriffspass Conditional Access Wellenplanung

eduroam ist nicht vertrauenswürdig Helpdesk

boddenberg.de

WISSEN

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

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

BERATUNG

Methodenwahl, Richtlinienset und Wellenplan für Ihren Tenant, abgestimmt auf Semesterkalender und Helpdesk-Kapazität.

› [Beratung für Hochschulen und Forschung](#)

SCHULUNG

Für Rechenzentrum, Fakultäts-IT und Helpdesk: Conditional Access, Authentifizierungsmethoden und Zugriffspass in der Praxis.

› [Schulungen für Hochschulen und Forschung](#)

Multifaktor-Authentifizierung einzuschalten dauert in Entra ID ungefähr so lange wie ein Kaffee aus dem Automaten im Foyer des Rechenzentrums. Eine Richtlinie anlegen, alle Benutzer auswählen, MFA verlangen, aktivieren. Fertig. Am nächsten Morgen stellen Sie dann fest, dass 30.000 Studenten, 4.000 Mitarbeiterinnen und Mitarbeiter, ein paar hundert Lehrbeauftragte und eine unbekannte Zahl von Emeriti gleichzeitig beschlossen haben, dass das Helpdesk ab sofort ihr persönlicher Ansprechpartner für Lebensfragen ist. Die Warteschleife spielt Vivaldi, aber nur die ersten zwei Takte, dann bricht die Verbindung ab.

Dass MFA an der Hochschule kommen muss, bestreitet in den Rechenzentren kaum noch jemand. Hochschulkonten sind Beute: für Phishing-Kampagnen, die aus einem übernommenen Studentenpostfach an den ganzen Fachbereich gehen, für den Zugriff auf Forschungsdaten und für die Erpressung, die mit einem einzigen Administratorkonto beginnt. Die Frage ist nicht ob, sondern wie: mit welchen Methoden, mit welchen Richtlinien für welche Personengruppe und vor allem in welcher Reihenfolge, damit das Semester weiterläuft und das Helpdesk das Semesterende erlebt.

Dieser Beitrag ist ein Rollout-Artikel. Er gehört zur Serie [Microsoft 365 in Hochschule und Forschung](#) und behandelt die Methodenwahl zwischen Authenticator-App, Passkeys, FIDO2-Schlüsseln und befristetem Zugriffspass, den Umgang mit Studenten ohne Smartphone oder mit grundsätzlicher Abneigung gegen jede App, das Conditional-Access-Grundset nach Personengruppe, die Wellenplanung entlang von Semesterstart und Prüfungsphasen und die Vorbereitung des Helpdesks. Allgemeinbildende Schulen und Universitätsklinika haben eigene Rahmenbedingungen und sind hier nicht gemeint.

FAKTEN · Worum es in diesem Beitrag geht

Lizenzgrundlage: Conditional Access braucht Entra ID P1, risikobasierte Richtlinien brauchen Entra ID P2. Was davon in A3, A5 und im Student Use Benefit steckt.

Methoden: Authenticator-App, TOTP-Apps anderer Hersteller, Passkeys, FIDO2-Schlüssel, befristeter Zugriffspass für die Erstregistrierung.

Richtlinien: Grundset für Studenten, Personal, Administratoren und Gäste, mit Tabelle zur Ausnahmebehandlung.

Netz: Warum eduroam und Campusnetz kein vertrauenswürdiger Standort sind.

Rollout: Registrierungskampagne, Wellen nach Fachbereich, Zeitstrahl über ein Semester, Helpdesk-Vorbereitung.

Ausgangslage: 30.000 Studenten sind keine 30.000 Angestellten

Wer MFA in einem Unternehmen oder einer Stadtverwaltung eingeführt hat, kennt das Muster: Die Belegschaft ist bekannt, hat einen Arbeitsvertrag, oft ein Diensthandy, und lässt sich über Vorgesetzte, Intranet und Dienstanweisung erreichen. An der Hochschule fehlt fast alles davon. Studenten haben keinen Vorgesetzten und kein Diensthandy, lesen ihre Hochschulmail sporadisch und wechseln jedes Semester zu einem Viertel. Dazu kommen die Personengruppen, die in keinem Organigramm sauber stehen: studentische Hilfskräfte mit Doppelrolle, Lehrbeauftragte mit einem Lehrauftrag pro Semester, Gastwissenschaftler für drei Monate und Emeriti, deren Mailadresse älter ist als die heutige Firewall.

Hinzu kommt die Freiheit von Forschung und Lehre, die im Rechenzentrumsalltag gerne als Argument gegen jede Vorgabe auftaucht. Sie schützt die Inhalte von Forschung und Lehre, nicht das Recht auf ein Konto ohne zweiten Faktor. Trotzdem gilt: Ein MFA-Rollout, der Professoren mitten im Berufungsverfahren oder kurz vor dem Drittmittelantrag aussperrt, wird politisch teurer als jeder Angriff. Das Präsidium sollte den Rollout deshalb beschließen, nicht nur zur Kenntnis nehmen. Wie man eine solche Vorlage aufbaut, steht im Beitrag [Microsoft-365-Einführung an der Hochschule: Konzeptionsphase in 4,5 Tagen und die Vorlage fürs Präsidium](#).

Die Lizenzfrage zuerst

Bevor Sie über Methoden reden, klären Sie, was Ihr Tenant darf. Conditional Access setzt laut Microsoft Entra ID P1 voraus. Risikobasierte Richtlinien, also Anmelderrisiko und Benutzerrisiko aus Entra ID Protection, sind eine Funktion von Entra ID P2. Im Bildungsbereich steckt Entra ID P1 in Microsoft 365 A3, Entra ID P2 in Microsoft 365 A5. Über den Student Use Benefit erhalten Studenten auf Grundlage der Zahl bezahlter Lizenzen für Personal Zugriff auf die entsprechenden Studentenlizenzen, einschließlich Entra ID P1 beziehungsweise P2, sofern die Hochschule über einen qualifizierenden Vertrag wie EES lizenziert. Office 365 A1 enthält dagegen kein Entra ID P1.

Für die Praxis heißt das: Eine Hochschule, die Personal mit A3 und Studenten nur mit A1 ausstattet, hat für den größten Teil ihrer Konten keine Lizenz für Conditional Access. Technisch lassen sich die Richtlinien zwar auch auf diese Konten anwenden, lizenzrechtlich verlangt Microsoft aber eine passende Lizenz für jede Person, die von der Funktion profitiert. Die Sicherheitsstandards (Security Defaults) sind kostenlos, gelten aber nur ganz oder gar nicht für den gesamten Tenant und schließen Conditional Access aus. Ein Mischbetrieb ist also nicht vorgesehen. Wie die Pläne zusammenhängen, erklärt der Beitrag [Education-Lizenzen verstehen: A1, A3, A5 und der Student Use Benefit](#).

Funktion	Ohne Premium	Entra ID P1 (A3, A3-SUB)	Entra ID P2 (A5, A5-SUB)
----------	--------------	--------------------------	--------------------------

Sicherheitsstandards (ganz oder gar nicht)	ja	möglich, aber nicht sinnvoll	möglich, aber nicht sinnvoll
Conditional Access mit Gruppen, Apps, Geräten	nein	ja	ja
Authentifizierungsstärken (z. B. phishingresistent)	nein	ja	ja
Registrierungskampagne, Zugriffspass, Passkeys	ja	ja	ja
Anmelde- und Benutzerrisiko als Bedingung	nein	nein	ja
Privileged Identity Management für Admin-Rollen	nein	nein	ja

FAKTEN · Lizenzlage, gegen Microsoft Learn geprüft

Conditional Access erfordert Entra ID P1. Risikobasierte Richtlinien (Anmelderisiko, Benutzerrisiko) erfordern Entra ID Protection und damit Entra ID P2.

Microsoft 365 A3 enthält Entra ID P1, Microsoft 365 A5 enthält Entra ID P2. Der Student Use Benefit gewährt Studenten diese Produkte auf Basis der bezahlten Lizenzen für Personal, unter qualifizierenden Verträgen wie EES.

Laufen Lizenzen für Conditional Access aus, bleiben bestehende Richtlinien aktiv, lassen sich aber nicht mehr bearbeiten, nur noch ansehen und löschen.

Lizenzpreise nennt dieser Beitrag bewusst nicht. Sie hängen vom Vertrag ab.

Sicherheitsstandards, MFA pro Benutzer, Conditional Access

In vielen Hochschul-Tenants findet man bei der ersten Bestandsaufnahme alle drei Generationen gleichzeitig: ein paar Konten mit der alten MFA pro Benutzer, die irgendwann für die Verwaltung aktiviert wurde, Sicherheitsstandards, die bei der Tenant-Erstellung eingeschaltet und später wieder deaktiviert wurden, und eine Handvoll Conditional-Access-Richtlinien mit Namen wie "Test Max". Räumen Sie das vor dem Rollout auf. Die MFA pro Benutzer kennt keine Gruppen und keine Bedingungen. Die Sicherheitsstandards verlangen die Registrierung der Authenticator-App oder einer TOTP-App, eine Schonfrist für die Registrierung gibt es seit 2024 nicht mehr. Für einen Tenant mit Entra ID P1 empfiehlt Microsoft selbst Conditional Access statt der Sicherheitsstandards.

Prüfen Sie außerdem, ob die Authentifizierungsmethoden bereits vollständig in der zentralen Richtlinie für Authentifizierungsmethoden verwaltet werden. Die alten Einstellungen für MFA und Self-Service-Kennwortzurücksetzung laufen sonst parallel weiter und erzeugen Kombinationen, die niemand mehr erklären kann. Der Migrationsassistent im Entra Admin Center erledigt das in wenigen Schritten und ist umkehrbar.

Wenn Shibboleth die Anmeldung übernimmt

Viele Hochschulen föderieren ihre Domäne nicht direkt in Entra ID, sondern lassen die Anmeldung über den eigenen Shibboleth-Identity-Provider laufen, der ohnehin für die DFN-AAI betrieben wird. Dann stellt sich die Frage, wo der zweite Faktor stattfindet: im Identity Provider der Hochschule, der das Ergebnis an Entra ID meldet, oder in Entra ID nach der föderierten Anmeldung. Beides geht, gesteuert über die Föderationseinstellung für das MFA-Verhalten. Entscheiden Sie sich bewusst, sonst müssen Studenten zwei Faktoren an zwei Stellen pflegen. Ein Detail mit Wirkung auf die Erstregistrierung: Ein befristeter Zugriffspass hat bei föderierten

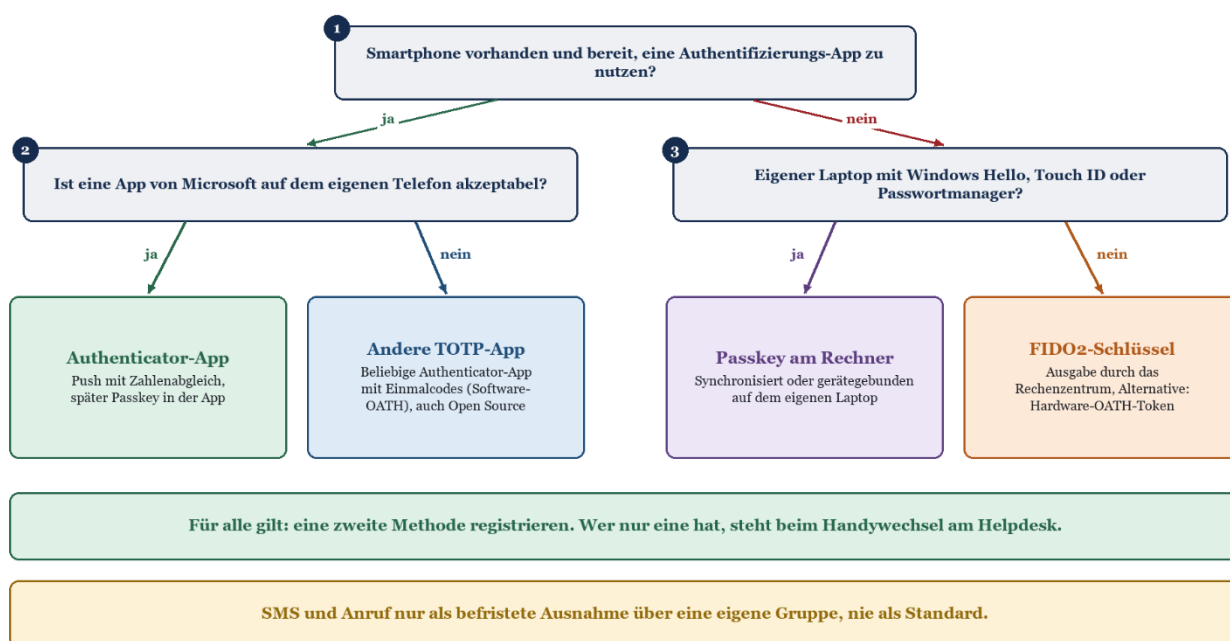
Domänen Vorrang, die Person wird dann nicht an den Identity Provider umgeleitet. Hintergründe zur Anbindung finden Sie im Beitrag [Entra ID und Shibboleth: Microsoft 365 an die DFN-AAI-Welt anbinden](#).

Methodenwahl: Was Studenten, Personal und Admins bekommen

Die beste Methode ist die, die ein Student nach drei Bier und einem verlorenen Handy noch wiederherstellen kann, ohne das Helpdesk anzurufen. Das klingt zynisch, beschreibt aber das Designziel ziemlich genau. Microsoft empfiehlt phishingresistente Verfahren wie Passkeys, FIDO2-Schlüssel und Windows Hello for Business, weil Codes und Push-Benachrichtigungen per Phishing abgegriffen werden können. Gleichzeitig muss die Methode auf einem privaten Android-Telefon von 2019 genauso funktionieren wie auf dem MacBook aus dem Elternhaus. Die Lösung ist kein Entweder-oder, sondern ein Methodenmix je Personengruppe.

Skizze 1: Welche Methode für welchen Studenten?

Drei Fragen, vier Ausgänge. Niemand fällt durch, auch nicht ohne Smartphone.



Schematisch. Welche Methoden im Tenant erlaubt sind, regelt die Richtlinie für Authentifizierungsmethoden.

Methode	Stärke	Für wen	Haken
Authenticator-App (Push mit Zahlenabgleich)	MFA, nicht phishingresistent	Standard für Studenten und Personal mit Smartphone	Smartphone und Bereitschaft zur Installation nötig; Handywechsel ohne Sicherung erzeugt Tickets
TOTP-App anderer Hersteller (Software-OATH)	MFA, nicht phishingresistent	Wer keine Microsoft-App möchte	Codes sind abgreifbar; Methode muss eigens freigeschaltet werden
Passkey in der Authenticator-App	phishingresistent	Personal und interessierte Studenten	Gerätegebunden; bei Verlust neu registrieren
Synchronisierter Passkey (z. B. im Passwortmanager)	phishingresistent	Studenten mit eigenem Laptop oder Smartphone	Sicherheit hängt am Konto des Passwortmanagers; über Passkey-Profil steuerbar
FIDO2-Sicherheitsschlüssel	phishingresistent	Admins, Prüfungsamt, Studenten ohne Smartphone	Logistik: Ausgabe, Ersatz, Verlust

Windows Hello for Business	phishingresistent	Personal an verwalteten Geräten	Nur auf dem jeweiligen Gerät
Hardware-OATH-Token	MFA, nicht phishingresistent	Sonderfälle ohne USB oder NFC	Derzeit als Vorschau gekennzeichnet; Tokenverwaltung
SMS und Anruf	schwächste MFA-Stufe	Befristete Ausnahme	Ausland, SIM-Tausch, Phishing; nicht als Standard

Authenticator-App als Brot-und-Butter-Methode

Für die Masse der Studenten wird die Authenticator-App mit Push-Benachrichtigung und Zahlenabgleich der Standard sein. Der Zahlenabgleich, bei dem die am Bildschirm angezeigte Zahl in der App eingetippt wird, entschärft die berüchtigte MFA-Müdigkeit: Wer um drei Uhr nachts zum zwanzigsten Mal eine Anfrage bekommt, kann nicht mehr reflexhaft auf Genehmigen drücken. Zusätzlich sollten Sie den Kontext in der Benachrichtigung anzeigen lassen, also Anwendung und ungefähren Ort. Ein Student in Gießen, der eine Anfrage aus einem anderen Kontinent sieht, versteht das ohne Schulung.

Die App lässt sich später zum Passkey-Träger ausbauen. Wer sie einmal mit Push-Benachrichtigung registriert hat, kann in derselben App einen Passkey anlegen. Für einen Rollout im ersten Schritt reicht der Push, die phishingresistente Stufe kommt mit der nächsten Kampagne.

Passkeys und FIDO2

Passkeys sind die eigentliche Zielmethode, auch an der Hochschule. Entra ID unterscheidet inzwischen zwischen gerätegebundenen Passkeys, etwa auf einem FIDO2-Schlüssel oder in der Authenticator-App, und synchronisierten Passkeys, die ein Passwortmanager oder das Betriebssystem über Geräte hinweg verteilt. Über Passkey-Profile legen Sie je Gruppe fest, welche Art erlaubt ist. Ein sinnvolles Muster: Für Studenten sind synchronisierte Passkeys erlaubt, weil sie den Handywechsel überleben. Für Administratoren gelten nur gerätegebundene Passkeys mit erzwungener Attestierung, also FIDO2-Schlüssel bekannter Hersteller.

FIDO2-Schlüssel sind außerdem die Antwort auf zwei Gruppen, die in jedem Rollout auftauchen: Studenten ohne Smartphone und Bereiche, in denen Smartphones nichts verloren haben, etwa Reinräume, Sicherheitslabore oder Prüfungsräume. Planen Sie die Ausgabe wie eine Bibliotheksausleihe: mit Ausweiskontrolle, Eintrag im Ausgabesystem und einem Ersatzprozess für verlorene Schlüssel.

Der befristete Zugriffspass für die Erstregistrierung

Das unterschätzte Problem jedes MFA-Rollouts ist der erste Faktor beim ersten Mal. Wer noch keine Methode registriert hat, meldet sich mit dem Kennwort an und registriert dann seine App. Genau das kann aber auch ein Angreifer, der das Kennwort bereits kennt: Er registriert seine eigene App und ist danach vollwertig mit zwei Faktoren angemeldet. Der befristete Zugriffspass, im Admin Center als Temporary Access Pass geführt, schließt diese Lücke. Er ist ein zeitlich begrenzter Code, der als starke Anmeldung zählt und mit dem die Person ihre eigentlichen Methoden registriert.

FAKTEN · Befristeter Zugriffspass in Zahlen

Die Standardgültigkeit beträgt eine Stunde, die maximale Lebensdauer ist in der Richtlinie zwischen zehn Minuten und dreißig Tagen einstellbar.

Ein Pass kann für einmalige oder mehrfache Nutzung innerhalb der Gültigkeit ausgestellt werden. Bei einmaliger Nutzung muss die Registrierung einer kennwortlosen Methode innerhalb von zehn

Minuten nach der Anmeldung abgeschlossen sein.

Die Länge ist zwischen acht und 48 Zeichen konfigurierbar. Jede Person hat höchstens einen gültigen Pass, ein neuer ersetzt den alten.

Externe Gäste können keinen Pass aus dem Ressourcen-Tenant erhalten. Der Pass funktioniert nicht mit der NPS-Erweiterung und dem AD-FS-Adapter.

Ausstellen dürfen mindestens Authentifizierungsadministratoren, für Konten mit Admin-Rollen privilegierte Authentifizierungsadministratoren.

Für Erstsemester bietet sich an, den Zugriffspass in den Prozess der Immatrikulation einzubauen. Das Identitätsmanagement legt das Konto an, erzeugt über Microsoft Graph einen Pass mit einigen Tagen Gültigkeit und liefert ihn mit den Zugangsdaten aus. Seien Sie dabei ehrlich zu sich selbst: Ein Pass, der im selben Brief steht wie das Kennwort, ist genau so sicher wie dieser Brief. Besser ist ein getrennter Kanal, etwa der Pass im Campus-Management-Portal nach Anmeldung mit dem Kennwort und eine Ausgabe gegen Ausweis am Infostand der Orientierungswoche für alle, bei denen das nicht klappt. Mehr zum Prozess rund um Immatrikulation und Kontoerstellung steht im Beitrag [Identity Lifecycle an der Hochschule: Von der Immatrikulation bis zum Alumni-Konto](#).

Studenten ohne Smartphone oder mit Verweigerungshaltung

Es gibt sie, und sie sind nicht nur Querulanten. Manche haben schlicht kein Smartphone, manche ein Diensthandy des Arbeitgebers, auf dem sie nichts installieren dürfen, manche wollen grundsätzlich keine Software eines bestimmten Herstellers auf ihrem privaten Gerät. Und dann gibt es den Informatikstudenten im fünften Semester, der Ihnen in einer vierseitigen Mail erklärt, warum TOTP kryptografisch ohnehin überholt ist. Er hat übrigens recht, nur nicht mit der Schlussfolgerung, dass er deshalb gar keinen zweiten Faktor braucht.

Für alle diese Fälle gibt es eine Methode, die ohne Microsoft-App auskommt. Schalten Sie in der Richtlinie für Authentifizierungsmethoden TOTP-Apps anderer Hersteller frei, dann reicht jede Authenticator-App, auch eine quelloffene. Wer einen eigenen Laptop hat, kann einen Passkey im Betriebssystem oder im Passwortmanager ablegen. Wer gar nichts hat, bekommt einen FIDO2-Schlüssel. SMS und Anruf bleiben die Rückfallebene für eine befristete Ausnahmegruppe, etwa während eines Auslandssemesters, nicht der Standard. Wichtig für die Registrierungskampagne: Wer bewusst eine Alternative gewählt hat, gehört in eine Ausschlussgruppe, sonst nervt ihn das System bei jeder Anmeldung mit der Aufforderung, doch die Microsoft-App zu installieren. Wie Microsoft-Dienste und offene Werkzeuge auf dem Campus nebeneinander bestehen, beschreibt der Beitrag [Microsoft 365 oder Open Source? Koexistenz mit BigBlueButton, Nextcloud, Moodle und Matrix](#).

HINWEIS · Private Geräte und Pflicht zur MFA: keine Rechtsberatung

Ob eine Hochschule Studenten oder Mitarbeiterinnen und Mitarbeiter verpflichten kann, für die Anmeldung ein privates Gerät einzusetzen, regeln Landesrecht, Hochschulsatzungen und Benutzungsordnungen des Rechenzentrums unterschiedlich. Für das Personal kommen die Personalvertretungsgesetze der Länder hinzu, die bei technischen Einrichtungen in der Regel ein Mitbestimmungsrecht vorsehen, und der Arbeits- oder Dienstvertrag. Eine gerätefreie Alternative wie ein FIDO2-Schlüssel entschärft die Frage in der Praxis erheblich.

Die Verarbeitung von Anmelde- und Gerätedaten gehört in das Verzeichnis der Verarbeitungstätigkeiten und gegebenenfalls in eine Datenschutz-Folgenabschätzung. Stimmen Sie sich mit Datenschutzbeauftragten, Justizariat und Personalrat ab. Dieser Kasten ersetzt keine rechtliche Prüfung.

Für das Personal lohnt sich ein Blick in den Beitrag [Personalrat und Microsoft 365 an der Hochschule: Dienstvereinbarung, wissenschaftliches Personal und die Verhaltenskontrolle](#), denn MFA-Anmeldeprotokolle sind technisch geeignet, Verhalten und Leistung zu überwachen. Die Einordnung der Datenflüsse aus Sicht der Aufsichtsbehörden finden Sie im Beitrag [Datenschutz und Microsoft 365 an Hochschulen: Zwischen DSK-Bewertung, Landesaufsicht und Campus-Realität](#).

Conditional-Access-Grundset nach Personengruppe

Conditional Access ist im Kern eine Sammlung von Wenn-dann-Regeln: Wenn diese Person auf diese Anwendung zugreift, unter diesen Bedingungen, dann muss sie dies tun. Der häufigste Fehler an Hochschulen ist nicht eine falsche Regel, sondern die vierzigste. Richtlinien wachsen mit jeder Ausnahme, jede Fakultät bekommt ihre eigene, und nach drei Jahren weiß niemand mehr, welche Regel welchen Zugriff erlaubt. Halten Sie das Grundset klein, benennen Sie die Richtlinien nach einem festen Schema und ändern Sie es nur über einen dokumentierten Weg.

Wichtig für das Verständnis: Treffen mehrere Richtlinien auf eine Anmeldung zu, müssen alle erfüllt sein. Eine studentische Hilfskraft, die gleichzeitig in der Gruppe der Studenten und in der Gruppe des Personals steht, erfüllt also immer die strengere Anforderung. Das ist gewollt, sollte aber vorher in der Kommunikation an die Hilfskräfte stehen, nicht erst im Ticket.

Skizze 2: Das Conditional-Access-Grundset nach Personengruppe

Eine Basisschicht für alle, darüber eine Säule je Gruppe. Es gelten immer alle zutreffenden Richtlinien.

Basis für alle Konten: Legacy-Authentifizierung blockieren · Gerätecodefluss blockieren · Registrierung der Sicherheitsinformationen schützen			
Studenten	Personal	Administratoren	Gäste
MFA für alle Cloud-Apps	MFA für alle Cloud-Apps	Getrennte Admin-Konten, nur in der Cloud	MFA hier oder aus dem Heimat-Tenant vertraut
Methoden: App, TOTP, Passkey, Schlüssel	Prüfungs- und Personaldaten: verwaltetes Gerät oder phishingresistent	Phishingresistent: FIDO2, Windows Hello	Nur freigegebene Apps
Moderate Anmeldehäufigkeit	Kürzere Sitzungen in Verwaltungsportalen	Keine dauerhafte Browsersitzung	Ablauf über Zugriffspaket
Mit P2: Anmelde- und Benutzerrisiko	Mit P2: Risiko-Richtlinien	Rollen nur bei Bedarf (PIM, P2)	Kein Zugriffspass für externe Gäste

— Studentische Hilfskraft: beide Säulen gelten, die strengere Anforderung gewinnt. —

Ausgenommen und überwacht Zwei Notfallkonten ohne Personenbezug, nur in der Cloud, mit eigener Alarmierung bei jeder Anmeldung
--

Kein vertrauenswürdiger Standort im Grundset. Weder Campusnetz noch eduroam noch VPN-Adressbereich.
--

Schematisch. Lizenzbedarf: Conditional Access ab Entra ID P1, Risiko-Richtlinien und PIM ab Entra ID P2.

Gruppen aus dem Identitätsmanagement, nicht aus Handarbeit

Die Richtlinien sind nur so gut wie die Gruppen, auf die sie zielen. Bauen Sie die Zielgruppen als dynamische Gruppen auf Basis von Attributen, die aus dem Identitätsmanagement kommen: Personentyp, Status, Fakultät oder Fachbereich. Dann wandern Studenten mit der Exmatrikulation automatisch aus der Gruppe, und eine Welle nach Fachbereich ist nichts weiter als eine Gruppenregel. Für Sonderrollen wie Gastwissenschaftler, Lehrbeauftragte und Emeriti brauchen Sie eigene Attribute, sonst landen sie zufällig in irgendeiner Säule. Wie man diese Rollen sauber

abbildet, beschreibt der Beitrag [Gastwissenschaftler, Lehrbeauftragte, Emeriti: Sonderrollen in Entra ID sauber abbilden](#).

Das Grundset im Überblick

Die folgende Tabelle zeigt ein Grundset, das sich in Projekten bei öffentlichen Auftraggebern bewährt hat und sich auf die Hochschule übertragen lässt. Sie ist eine Ausgangsbasis, keine Vorlage zum Abtippen. Prüfen Sie jede Zeile gegen Ihre Lizenzlage, Ihre Anwendungen und Ihre Dienstvereinbarungen.

Personengruppe	Richtlinie	MFA-Methode	Ausnahmebehandlung
Alle Konten	Legacy-Authentifizierung blockieren; Gerätecodefluss blockieren; Registrierung der Sicherheitsinformationen schützen	Registrierung nur mit MFA oder befristetem Zugriffspass	Gerätecodefluss nur für eine eng gefasste Gruppe, etwa Konferenzraumsysteme; Notfallkonten ausgenommen
Studenten	MFA für alle Cloud-Apps; moderate Anmeldehäufigkeit; mit P2 Anmelde- und Benutzerrisiko	Authenticator-App, TOTP-App, Passkey, FIDO2-Schlüssel	Befristete Ausnahmegruppe mit SMS für Nachzügler und Auslandssemester; Gruppe läuft automatisch ab
Studentische Hilfskräfte	Gelten Studenten- und Personalrichtlinien, die strengere gewinnt	Wie Personal	Keine eigene Ausnahme; Hinweis in der Kommunikation
Wissenschaftliches Personal	MFA für alle Cloud-Apps; sensible Anwendungen nur mit verwaltetem Gerät oder phishingresistenter MFA	Authenticator-App, Passkey, Windows Hello	Labore und Reinräume ohne Smartphone: FIDO2-Schlüssel statt Ausnahme
Verwaltung und Prüfungsamt	Wie Personal; Prüfungs- und Personaldaten mit Authentifizierungsstärke phishingresistent; kürzere Sitzung	Passkey, FIDO2-Schlüssel, Windows Hello	Keine dauerhafte Ausnahme; Vertretungsregel für verlorene Schlüssel
Lehrbeauftragte, Emeriti	Wie Personal, ohne Zugriff auf Verwaltungsanwendungen	Authenticator-App, TOTP-App, FIDO2-Schlüssel	Konto mit Ablauf aus Lehrauftrag oder Status; kein MFA-Verzicht aus Höflichkeit
Administratoren	Eigene Admin-Konten nur in der Cloud; phishingresistente MFA bei jeder Anmeldung; Rollen nur bei Bedarf (PIM, P2)	FIDO2-Schlüssel, Windows Hello	Keine; Ersatzschlüssel im Tresor
Gäste (B2B)	MFA verlangen; MFA aus Heimat-Tenant über mandantenübergreifende Zugriffseinstellungen vertrauen, wo vereinbart	Methode des Heimat-Tenants oder Registrierung im Ressourcen-Tenant	Kein befristeter Zugriffspass für externe Gäste; Zugriff über Zugriffspaket mit Ablauf
Notfallkonten	Von allen Richtlinien ausgenommen	Phishingresistent, Schlüssel im Tresor	Alarm bei jeder Anmeldung; regelmäßiger Test

TIPP • Report-only und What-If vor jeder Scharfschaltung

Jede neue Richtlinie läuft zuerst im Modus "Nur Bericht". Werten Sie die Anmeldeprotokolle mindestens zwei Wochen aus, bevor Sie einschalten. Das What-If-Werkzeug im Admin Center zeigt für einzelne Konten, welche Richtlinien greifen würden.

Testen Sie mit echten Konten aller Gruppen, auch mit dem der studentischen Hilfskraft und dem des

Emeritus. Die Überraschungen sitzen fast immer an den Rändern.

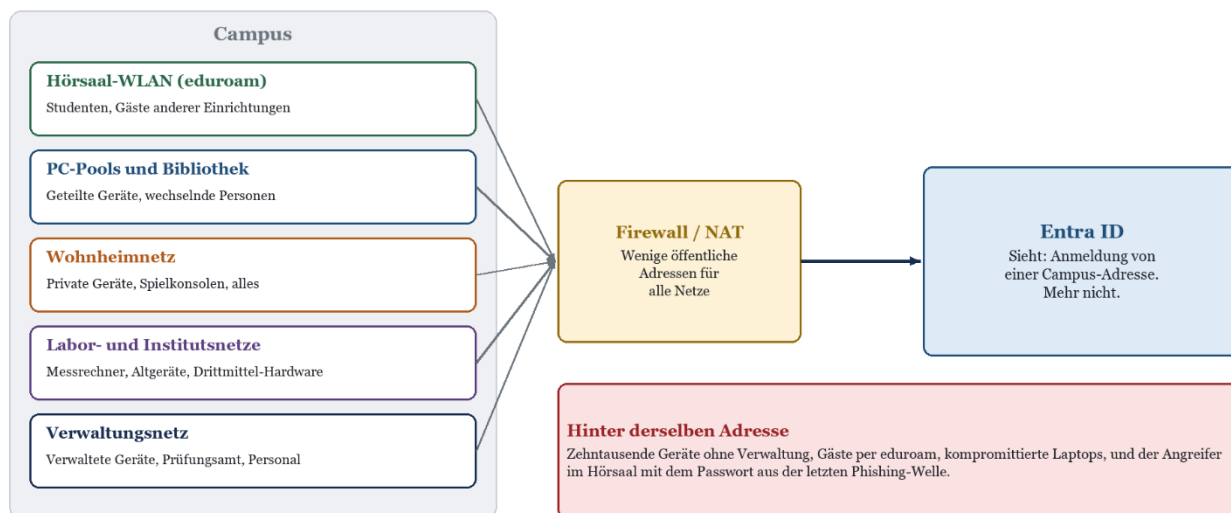
eduroam und Campusnetz sind kein vertrauenswürdiger Standort

In jedem zweiten Workshop kommt der Vorschlag, das Campusnetz als vertrauenswürdigen Standort zu markieren und dort auf MFA zu verzichten. Er kommt meist von Menschen, die noch nie gesehen haben, was hinter der Campus-Adresse alles ins Internet geht. Entra ID sieht nicht das Gerät im Hörsaal, sondern die öffentliche Adresse nach der Adressumsetzung. Hinter dieser Adresse stehen Hörsaal-WLAN, PC-Pools, Wohnheimnetze, Laborrechner aus drei Drittmittelgenerationen und über eduroam auch Angehörige jeder anderen teilnehmenden Einrichtung, die gerade zufällig auf Ihrem Campus sitzen.

Wer diese Adressen als vertrauenswürdige markiert, schaltet MFA genau dort ab, wo am meisten angemeldet wird, und schenkt jedem Angreifer mit einem abgephischten Kennwort einen bequemen Weg: in die Bibliothek setzen, einloggen, fertig. Die eduroam-Anmeldung am WLAN selbst läuft über die RADIUS-Infrastruktur Ihrer Einrichtung und ist von Conditional Access nicht betroffen. Sie sagt aber nichts darüber aus, wer anschließend mit welchem Kennwort an Microsoft 365 anklopft.

Skizze 3: Warum das Campusnetz kein vertrauenswürdiger Standort ist

Entra ID sieht eine Handvoll öffentlicher Adressen. Dahinter steckt eine Kleinstadt.



Campusnetz als vertrauenswürdige markieren heißt: keine MFA genau dort, wo am meisten angemeldet wird.

Erlaubt: Campus-Adressen als Signal für Sonderfälle, etwa den Prüfungsraum mit verwalteten Geräten. Nie als pauschale MFA-Ausnahme.

Schematisch. Netzaufbau, Adressbereiche und NAT unterscheiden sich je Hochschule.

WARNUNG · Kein MFA-Verzicht für Campus-Adressen

Markieren Sie weder das Campusnetz noch eduroam noch den Adressbereich des VPN als vertrauenswürdigen Standort, um MFA zu umgehen. Die Option der vertrauenswürdigen IP-Adressen in den alten MFA-Diensteinstellungen empfiehlt Microsoft ohnehin nicht mehr.

Benannte Standorte bleiben trotzdem nützlich: als Signal in der Auswertung, zum Blockieren von Ländern, in denen Ihre Hochschule nachweislich nicht tätig ist, und für eng umrissene Sonderfälle wie den Prüfungsraum, dort aber immer in Kombination mit einem verwalteten Gerät.

Prüfungsraum, PC-Pool und die Klausur ohne Handy

Ein Sonderfall, der in keiner Herstellerdokumentation steht: die elektronische Klausur im PC-Pool. Die Prüfungsordnung verlangt, dass Smartphones ausgeschaltet in der Tasche liegen, die Lernplattform verlangt eine Anmeldung, und Conditional Access verlangt einen zweiten Faktor. Die schlechteste Lösung ist eine pauschale Ausnahme für den Raum. Bessere Lösungen sind verwaltete Prüfungsrechner, auf denen die Anmeldung über ein eigenes Prüfungskonto oder über eine Richtlinie mit Gerätefilter läuft, oder FIDO2-Schlüssel, die für die Klausur ausgegeben werden. Klären Sie das mit Prüfungsamt und Dekanaten vor der ersten Prüfungsphase unter MFA, nicht in der Nacht davor.

Notfallkonten und Benennung

Legen Sie vor der ersten Richtlinie zwei Notfallkonten an, die nur in der Cloud existieren, dauerhaft die Rolle des globalen Administrators tragen, von allen Richtlinien ausgenommen sind und mit phishingresistenten Schlüsseln aus dem Tresor angemeldet werden. Jede Anmeldung an diesen Konten löst einen Alarm aus. Das ist keine Paranoia, sondern die Versicherung gegen die eine Richtlinie, die versehentlich alle Administratoren aussperrt. Wer schon einmal einen Freitagabend mit dem Support von Microsoft verbracht hat, um wieder in den eigenen Tenant zu kommen, legt diese Konten freiwillig an.

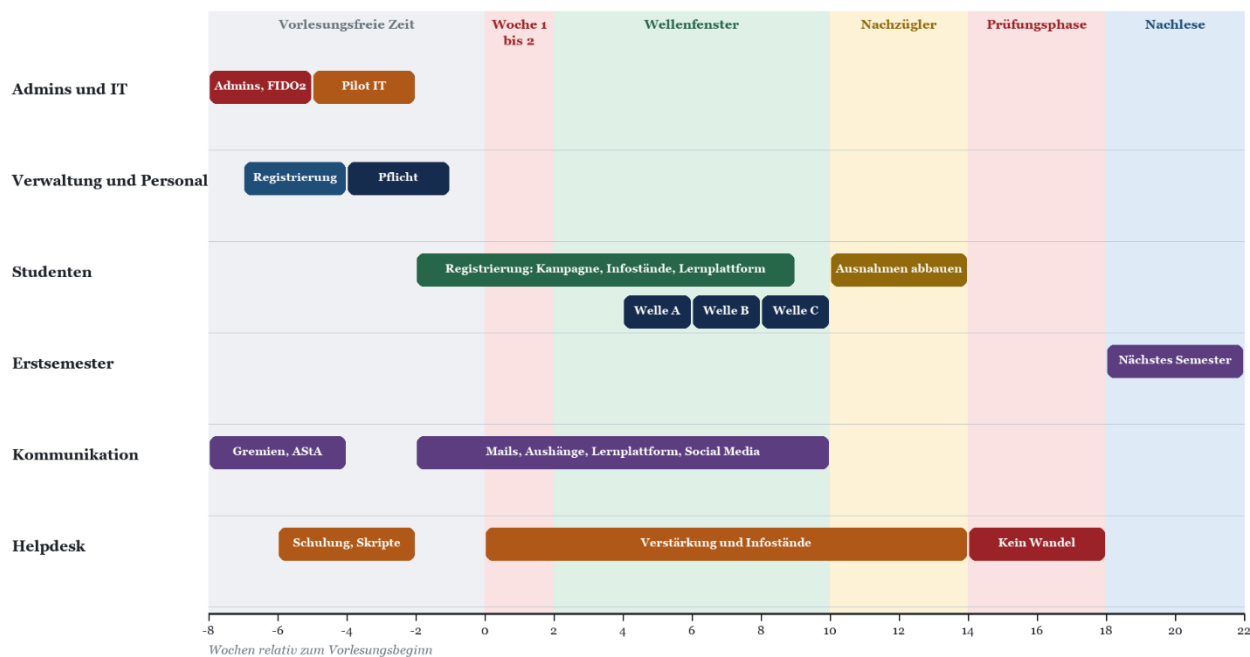
Benennen Sie die Richtlinien nach einem festen Schema mit Nummer, Zielgruppe, Anwendung und Wirkung, etwa "CA110 Studenten Alle Apps MFA". Dann erkennt man in jedem Anmeldeprotokoll sofort, was gegriffen hat. Wenn Fakultäts-IT und Lehrstuhl-Admins Teile der Verwaltung übernehmen, gehören Änderungen an Conditional Access trotzdem ausschließlich ins zentrale Rechenzentrum. Wie Sie Zuständigkeiten über Verwaltungseinheiten verteilen, ohne die Richtlinien freizugeben, beschreibt der Beitrag [Dezentrale IT an der Hochschule: Lehrstuhl-Admins, Fakultäts-IT und ein Tenant für alle](#).

Rollout über ein Semester: Kampagne, Wellen, Kalender

Der Semesterkalender ist Ihr wichtigstes Planungswerkzeug, wichtiger als jedes Projektmanagement-Tool. Es gibt Zeiten, in denen ein MFA-Rollout funktioniert, und Zeiten, in denen er zur Katastrophe wird. Die Vorlesungszeiten und Prüfungsphasen liegen an Universitäten, Hochschulen für angewandte Wissenschaften sowie Kunst- und Musikhochschulen unterschiedlich, und sie unterscheiden sich zwischen den Ländern. Der folgende Zeitstrahl rechnet deshalb in Wochen relativ zum Vorlesungsbeginn.

Skizze 4: Rollout-Zeitstrahl über ein Semester

Woche 0 ist der erste Vorlesungstag. Scharf geschaltet wird nur im grünen Fenster.



Woche 1 bis 2 und Prüfungsphase: keine Scharfschaltung, keine Richtlinienänderung, kein Experiment.

Schematisch. Lage von Vorlesungs- und Prüfungszeiten unterscheidet sich je Hochschule und Hochschulart.

WARNUNG · MFA-Pflicht nie in der ersten Vorlesungswoche scharf schalten

In der ersten Vorlesungswoche ändern sich Stundenpläne, Kurszuordnungen und Raumbelegungen, Erstsemester suchen ihre Hörsäle, und das Helpdesk kämpft mit vergessenen Kennwörtern und vollen Postfächern. Wer in diese Woche die MFA-Pflicht legt, bekommt jedes Ticket doppelt und jeden Fehler in der Hochschulöffentlichkeit.

Registrieren lassen dürfen Sie in dieser Zeit, Infostände sind sogar ideal. Scharf geschaltet wird frühestens ab der dritten Woche, und vor der Prüfungsphase wird eingefroren: keine neuen Richtlinien, keine Änderungen an Methoden.

Die Wellen

Fangen Sie bei denen an, die es am meisten brauchen und am besten aushalten: Administratoren und Rechenzentrum. Danach Verwaltung und Personal, noch in der vorlesungsfreien Zeit, weil das Helpdesk dann Luft hat und die Verwaltung erreichbar ist. Die Studenten folgen in Wellen nach Fachbereich, jeweils mit zwei Wochen Abstand, sodass jede Welle aus den Tickets der vorigen lernt. Beginnen Sie mit einem Fachbereich, der technisch eher gelassen ist, und heben Sie sich die Fakultät mit den meisten Erstsemestern für die Mitte auf, wenn die Skripte eingespielt sind.

Welle	Zeitpunkt	Zielgruppe	Erfolgskriterium vor der nächsten Welle
0	Vorlesungsfreie Zeit, früh	Notfallkonten, Administratoren, Rechenzentrum	Alle Admin-Konten mit FIDO2; Notfallkonten getestet; Alarmierung läuft
1	Vorlesungsfreie Zeit	Pilot: IT-Personal, freiwillige Fachbereichs-IT	Skripte für Helpdesk erprobt; Report-only ohne Überraschungen
2	Vorlesungsfreie Zeit,	Verwaltung,	Registrierungsquote hoch; Sonderfälle

	spät	wissenschaftliches Personal, studentische Hilfskräfte	(Labor, Reinraum) gelöst
3a bis 3c	Woche 3 bis 10	Studenten nach Fachbereich	Registrierungsquote je Fachbereich vor Scharfschaltung hoch; Ticketvolumen unter Kapazität
4	Woche 10 bis 14	Nachzügler aus der Ausnahmegruppe	Ausnahmegruppe vor der Prüfungsphase möglichst leer
Erstsemester	Ab dem nächsten Semester	Neue Konten aus der Immatrikulation	MFA ab Kontoerstellung; Registrierung mit Zugriffspass vor Vorlesungsbeginn

Die Registrierungskampagne

Entra ID bringt eine Registrierungskampagne mit, die Personen nach einer MFA-Anmeldung auffordert, eine stärkere Methode einzurichten. Sie kann entweder die Authenticator-App oder Passkeys als Ziel haben, aber nicht beides gleichzeitig. Im von Microsoft verwalteten Zustand legt Microsoft Zielmethode und Aufschubregeln fest. Im Zustand "Aktiviert" bestimmen Sie selbst, wie viele Tage zwischen zwei Aufforderungen liegen, zwischen null und vierzehn, und ob die Registrierung nach drei Aufschüben verpflichtend wird.

Zwei Details sind für die Hochschule wichtig. Erstens greift die Kampagne erst nach einer MFA-Anmeldung. Für Konten, die noch gar keine Methode haben, ist sie also nicht das Werkzeug der Erstregistrierung. Dafür sorgt die Conditional-Access-Richtlinie selbst, die bei fehlender Methode in die Registrierung umleitet, abgesichert durch die Richtlinie für die Registrierung der Sicherheitsinformationen. Zweitens wird die Aufforderung zur Authenticator-App nicht auf Mobilgeräten angezeigt, die Passkey-Kampagne dagegen auch im mobilen Browser. Für die Phase nach dem Rollout ist die Kampagne damit ideal, um Studenten von SMS auf App und später von App auf Passkey zu bewegen. Microsoft stellt die Kampagne gerade auf eine neue Version um, das Verhalten im Tenant kann deshalb vorübergehend von der Dokumentation abweichen.

Kommunikation, die tatsächlich ankommt

Eine Rundmail an alle Studenten erreicht ungefähr so viele Menschen wie ein Aushang im Keller des Physikgebäudes. Nutzen Sie die Kanäle, die Studenten wirklich lesen: die Startseite der Lernplattform, die Kurse der Erstsemester, die Fachschaften und den AStA, Aushänge an den Druckern und Bildschirme in Mensa und Bibliothek. Bitten Sie Dozenten, in der zweiten Vorlesungswoche eine Folie zu zeigen. Ein QR-Code auf die Anleitung, drei Sätze Begründung und das Datum der eigenen Welle reichen. Für das Personal gehört die Ankündigung in die Dekanate, die Dezernate und in die Personalversammlung.

TYPISCHE SITUATION · Der Stichtag, an dem alle gleichzeitig kamen

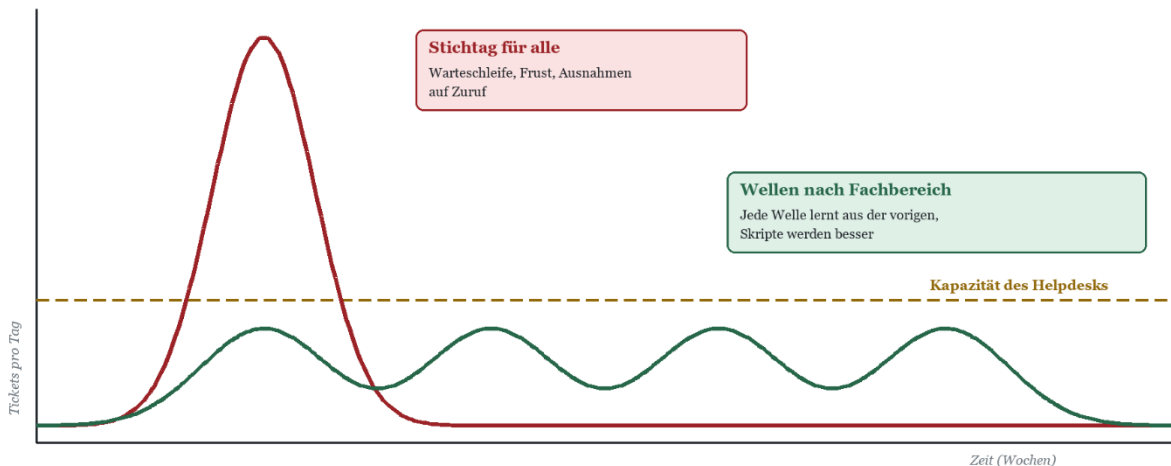
In einer Stadtverwaltung wurde MFA an einem Montag um sieben Uhr für alle Mitarbeiterinnen und Mitarbeiter scharf geschaltet. Bis neun Uhr lagen mehr Tickets vor als sonst in einem Monat, darunter ein Bauhof, dessen Belegschaft gar keine dienstlichen Smartphones hatte, und eine Leitstelle, in der private Telefone verboten waren. Gelöst wurde beides mit FIDO2-Schlüsseln, aber erst nach zwei Wochen mit Ausnahmen auf Zuruf, von denen einige ein Jahr später noch aktiv waren. Übertragen auf die Hochschule ist das die typische Situation: Der Bauhof heißt dort Reinraum oder Prüfungsraum, die Leitstelle heißt Labor. Wer die Sonderfälle vor der Welle sammelt, braucht keine Ausnahmen danach.

Helpdesk-Vorbereitung: Der eigentliche Engpass

Die Technik ist an einem Nachmittag konfiguriert, das Helpdesk braucht Wochen. Es muss Methoden erklären, Zugriffspässe ausstellen, Identitäten prüfen und dabei unterscheiden, ob am Telefon ein verzweifelter Student sitzt oder ein Angreifer, der genau so klingt. Die Kapazität des Helpdesks bestimmt das Tempo der Wellen, nicht umgekehrt.

Skizze 5: Helpdesk-Last bei Stichtag und bei Wellen

Ähnlich viele Tickets, anders verteilt. Nur eine Kurve bleibt unter der Kapazitätsgrenze.



Was über der Kapazitätsgrenze liegt, wird nicht gelöst, sondern per Ausnahme weggeklickt. Und Ausnahmen bleiben.

Schematische Darstellung ohne Messwerte.

Identität prüfen, bevor zurückgesetzt wird

Sobald MFA eingeführt ist, wird das Helpdesk zum attraktivsten Ziel im ganzen Tenant. Wer dort anruft und glaubhaft macht, sein Handy verloren zu haben, bekommt im schlechtesten Fall einen Zugriffspass und damit die Möglichkeit, eine eigene Methode zu registrieren. Legen Sie deshalb fest, auf welchen Wegen ein Pass ausgegeben wird: persönlich gegen Studentenausweis oder Personalausweis, per Rückruf an eine im Identitätsmanagement hinterlegte Nummer oder über einen Self-Service, der eine bereits bestehende starke Anmeldung voraussetzt. Am Telefon ohne Rückruf gibt es keinen Pass, auch nicht für den Dekan.

TYPISCHE SITUATION · Der freundliche Anrufer

In einem kommunalen Verband rief ein angeblicher Amtsleiter im Helpdesk an, er sei auf Dienstreise, das Handy sei weg, die Sitzung beginne in zehn Minuten. Der Kollege im Helpdesk wollte helfen, und das Verfahren sah nur eine Rückfrage nach dem Geburtsdatum vor. Dass der echte Amtsleiter im Nebenraum saß, fiel erst am nächsten Tag auf.

Typische Situation an der Hochschule: Ein Professor auf einer Tagung, ein Drittmittelantrag mit Frist, ein Helpdesk mit studentischen Hilfskräften am Telefon. Ein festes Verfahren mit Rückruf schützt beide Seiten, auch die Hilfskraft, die sonst die Entscheidung allein treffen müsste.

Rollen und Werkzeuge für das Helpdesk

Für das Ausstellen von Zugriffspässen und das Zurücksetzen von Methoden reicht die Rolle des Authentifizierungsadministrators, beschränkt auf Konten ohne Admin-Rollen. Wer Fakultäts-IT einbindet, kann die Rolle über Verwaltungseinheiten auf einen Fachbereich begrenzen. Die Rolle des privilegierten Authentifizierungsadministrators bleibt beim zentralen Rechenzentrum. Geben

Sie dem Helpdesk außerdem Lesezugriff auf die Anmeldeprotokolle, damit es den häufigsten Satz der ersten Wochen beantworten kann: "Ich habe nichts gemacht, und jetzt geht nichts mehr."

Ticketart	Häufigkeit im Rollout	Lösung	Vorbeugung
Neues Handy, alte App weg	sehr häufig	Identität prüfen, Zugriffspass, neu registrieren	Zweite Methode, Sicherung der App, synchronisierte Passkeys
Kein Smartphone	regelmäßig	TOTP-App am Rechner, Passkey oder FIDO2-Schlüssel	Alternativen in der Anleitung vorne nennen, nicht im Kleingedruckten
Push kommt nicht an	häufig	Benachrichtigungen und Akkusparmodus prüfen, Code statt Push	Anleitung je Betriebssystem
Code wird abgelehnt	gelegentlich	Uhrzeit des Geräts prüfen	Hinweis auf automatische Zeiteinstellung
Auslandssemester ohne Mobilfunk	saisonal	App-Codes funktionieren offline; SMS nur über Ausnahmegruppe	Vor Abreise zweite Methode einrichten
Unerwartete MFA-Anfrage	selten, aber wichtig	Als Sicherheitsvorfall behandeln, Kennwort ändern, Sitzungen widerrufen	Meldeweg in jeder Anleitung

Kapazität planen, ohne Zahlen zu erfinden

Wie viele Tickets eine Welle erzeugt, hängt von Vorbereitung, Kommunikation und Zielgruppe ab. Ein belastbarer Weg ist, die erste Pilotwelle genau zu zählen und die Quote auf die folgenden Wellen hochzurechnen, mit einem Sicherheitsaufschlag für Erstsemester. Planen Sie für die Wellen der Studenten zusätzliche Kräfte ein, etwa geschulte studentische Hilfskräfte an Infoständen in Bibliothek und Mensa. Ein Infostand mit zwei Menschen und einem Stapel Anleitungen löst in einer Stunde mehr Probleme als ein Ticketsystem an einem Tag, weil die meisten Fragen in dreißig Sekunden beantwortet sind, wenn jemand auf das Display schauen kann.

TIPP · Drei Dinge, die vor der ersten Studentenwelle fertig sein müssen

Eine Anleitung pro Methode mit Bildschirmfotos, auf einer Seite, mit QR-Code. Die Alternativen ohne Smartphone stehen auf derselben Seite, nicht in einem Anhang.

Ein Helpdesk-Skript mit Entscheidungsbaum, wann ein Zugriffspass ausgegeben wird und wann nicht.

Eine Ausnahmegruppe mit Ablaufdatum, die das Helpdesk selbst befüllen darf, und eine Auswertung, die jede Woche zeigt, wer noch drinsteht.

TYPISCHE SITUATION · Smartphones verboten, Anmeldung trotzdem nötig

In einem Krankenhausverbund durften in bestimmten Funktionsbereichen keine privaten Telefone mitgeführt werden, die Anmeldung an Microsoft 365 war aber auch dort nötig. Die Lösung waren verwaltete Geräte mit Windows Hello und eine kleine Zahl FIDO2-Schlüssel für wechselnde Arbeitsplätze, ausgegeben und zurückgenommen wie Generalschlüssel.

Typische Situation an der Hochschule: Sicherheitslabore, Reinräume und Werkstätten. Die Logik ist dieselbe, nur dass die Schlüssel am Institut statt an der Pforte ausgegeben werden.

Für die Schulung von Helpdesk, Fakultäts-IT und Rechenzentrum zu Conditional Access, Authentifizierungsmethoden und Zugriffspass gibt es die [Microsoft-365-Schulung für Hochschulen und Forschungseinrichtungen](#). Wer Methodenwahl, Richtlinienet und Wellenplan gemeinsam mit einem externen Blick aufsetzen möchte, findet das Angebot unter [Microsoft-365-Beratung für Hochschulen und Forschung](#).

FAQ: MFA und Conditional Access an der Hochschule

Brauchen wir für MFA überhaupt Entra ID P1?

Für MFA an sich nicht, die Sicherheitsstandards sind kostenlos. Sie gelten aber nur für den gesamten Tenant, lassen sich nicht nach Personengruppen steuern und schließen Conditional Access aus. Für ein Grundset nach Personengruppe brauchen Sie Entra ID P1, enthalten in Microsoft 365 A3 und im zugehörigen Student Use Benefit. Für risikobasierte Richtlinien brauchen Sie Entra ID P2 aus A5.

Können wir das Campusnetz nicht wenigstens für die Verwaltung als vertrauenswürdig markieren?

Auch das Verwaltungsnetz verlässt den Campus meist über dieselben öffentlichen Adressen wie Hörsaal-WLAN und Wohnheim. Für die Verwaltung ist ein verwaltetes Gerät die bessere Bedingung: Es weist nach, dass das Gerät dazugehört, nicht nur die Adresse.

Was machen wir mit Studenten, die kein Smartphone haben?

Eine TOTP-App am eigenen Rechner, ein Passkey im Betriebssystem oder Passwortmanager oder ein FIDO2-Schlüssel aus dem Rechenzentrum. SMS ist nur für eine befristete Ausnahmegruppe gedacht.

Dürfen wir von Studenten verlangen, eine App auf dem privaten Handy zu installieren?

Das hängt von Landesrecht, Satzungen und Benutzungsordnung ab und ist eine rechtliche Frage, die Sie mit Justizariat und Datenschutz klären sollten. In der Praxis entschärft eine gerätefreie Alternative wie ein FIDO2-Schlüssel die Diskussion erheblich.

Funktioniert der befristete Zugriffspass, wenn unsere Domäne an Shibboleth föderiert ist?

Ja. Bei föderierten Domänen hat der Zugriffspass Vorrang, die Anmeldung wird dann in Entra ID abgeschlossen, ohne Umleitung an den Identity Provider.

Ist eduroam von der MFA-Pflicht betroffen?

Die Anmeldung am WLAN läuft über die RADIUS-Infrastruktur Ihrer Einrichtung und nicht über Conditional Access. Betroffen ist die anschließende Anmeldung an Microsoft 365, und für die ist eduroam ausdrücklich kein vertrauenswürdiger Standort.

Wann ist der richtige Zeitpunkt für den Start?

Administratoren und Personal in der vorlesungsfreien Zeit, Studenten in Wellen ab der dritten Vorlesungswoche, Abschluss vor der Prüfungsphase. Nie in der ersten Vorlesungswoche und nie während der Prüfungen.

Wie verhindern wir, dass das Helpdesk ausgetrickst wird?

Mit einem festen Verfahren: Zugriffspass nur persönlich gegen Ausweis, per Rückruf an eine hinterlegte Nummer oder per Self-Service mit bestehender starker Anmeldung. Unerwartete MFA-Anfragen werden als Sicherheitsvorfall behandelt.

Fazit: Der zweite Faktor ist einfach, der erste Montag nicht

MFA an der Hochschule scheitert selten an der Technik. Entra ID bringt alles mit, was ein Campus braucht: Methoden für jede Lebenslage, einen Zugriffspass für die Erstregistrierung, Passkey-Profile für unterschiedliche Gruppen, eine Registrierungskampagne und Conditional Access für ein schlankes Grundset. Es scheitert am Kalender, an der Kommunikation und am Helpdesk. Wer den Semesterplan ernst nimmt, Campusnetz und eduroam nicht als Abkürzung missbraucht, die Sonderfälle vor der Welle sammelt und das Helpdesk mit Verfahren statt mit Durchhalteparolen ausstattet, bringt 30.000 Studenten durch den Rollout, ohne dass jemand die Warteschleife auswendig kann.

Und der Informatikstudent mit der vierseitigen Mail? Er bekommt einen FIDO2-Schlüssel und ist danach der zufriedenste Mensch auf dem Campus. Phishingresistent, ohne Microsoft-App, mit einem Stück Hardware am Schlüsselbund. Manchmal ist die Lösung für die lauteste Beschwerde zugleich die sicherste Methode.

WEITERLESEN • Weiterlesen

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

- › [Microsoft 365 in Hochschule und Forschung](#)
- › [Education-Lizenzen verstehen: A1, A3, A5 und der Student Use Benefit](#)
- › [Entra ID und Shibboleth: Microsoft 365 an die DFN-AAI-Welt anbinden](#)
- › [Identity Lifecycle an der Hochschule: Von der Immatrikulation bis zum Alumni-Konto](#)
- › [Gastwissenschaftler, Lehrbeauftragte, Emeriti: Sonderrollen in Entra ID sauber abbilden](#)
- › [Dezentrale IT an der Hochschule: Lehrstuhl-Admins, Fakultäts-IT und ein Tenant für alle](#)
- › [Datenschutz und Microsoft 365 an Hochschulen: Zwischen DSK-Bewertung, Landesaufsicht und Campus-Realität](#)
- › [Personalrat und Microsoft 365 an der Hochschule: Dienstvereinbarung, wissenschaftliches Personal und die Verhaltenskontrolle](#)
- › [Microsoft-365-Beratung für Hochschulen und Forschung](#)
- › [Microsoft-365-Schulung für Hochschulen und Forschungseinrichtungen](#)