Microsoft-365-Security an Hochschulen: Offene Netze, private Geräte und Konten als Beute



WISSEN

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

› **Microsoft 365 in Hochschule und Forschung**

BERATUNG

Sicherheitsbestandsaufnahme für Ihren Hochschul-Tenant: MFA, Conditional Access, privilegierte Konten, Legacy-Protokolle, Lizenzabgleich.

› **Beratung für Hochschulen und Forschung**

SCHULUNG

Für Hochschulrechenzentrum, Fakultäts-IT und Helpdesk: Conditional Access, Entra-Rollen und Vorfallsbearbeitung im Tenant.

› **Schulungen für Hochschulen und Forschung**

Wenn Angreifer einen Wunschzettel schreiben dürften, sähe er ungefähr so aus: ein Netz, in das sich jeder mit irgendeinem Gerät einbuchen darf. Zehntausende Laptops und Telefone, die niemand kennt und niemand patcht. Jedes Semester ein paar tausend neue Konten, deren Inhaber noch nicht wissen, wie die echte Mail des Prüfungsamts aussieht. Administratorrechte, verteilt über Fakultäten und Lehrstühle wie Freikarten. Und hinter all dem Forschungsdaten, Drittmittelverträge, Berufungsakten und eine Finanzbuchhaltung, die regelmäßig Rechnungen von Verbundpartnern bezahlt. Herzlichen Glückwunsch: Sie betreiben diesen Wunschzettel. Man nennt ihn Hochschule.

Das ist keine Kritik an der Hochschulkultur. Offenheit ist der Auftrag, und die Freiheit von Forschung und Lehre ist kein Konfigurationsfehler. Sie bedeutet aber, dass die Sicherheitsmechanismen, die in einem Unternehmen per Arbeitsanweisung durchgesetzt werden, auf dem Campus über Technik, Überzeugung und sehr viel Geduld kommen müssen. Dieser Beitrag beschreibt, warum Hochschulen ein so dankbares Ziel sind, wie eine typische Angriffskette vom gephishten Studentenkonto bis in die Verwaltung verläuft und welche Maßnahmen in Microsoft 365 am meisten bringen, sortiert nach Wirkung und nicht nach Hochglanzbroschüre.

Er gehört zur Serie Microsoft 365 in Hochschule und Forschung und richtet sich an Leitungen von Hochschulrechenzentren und IT-Servicezentren, CIOs, Kanzlerinnen und Kanzler, Dezernate, Datenschutzbeauftragte und Personalräte sowie an IT- und Verwaltungsleitungen außeruniversitärer Forschungseinrichtungen. Schulen und Universitätsklinika spielen in eigenen Ligen und bleiben hier außen vor.

FAKTEN · Das Wichtigste in Kürze

Hochschulen sind nicht deshalb ein beliebtes Ziel, weil sie schlecht administriert wären, sondern weil Offenheit, Fluktuation und dezentrale Verantwortung zum Geschäftsmodell gehören. Übernommene Studentenkonten sind dabei selten das Ziel, sondern die Eintrittskarte.

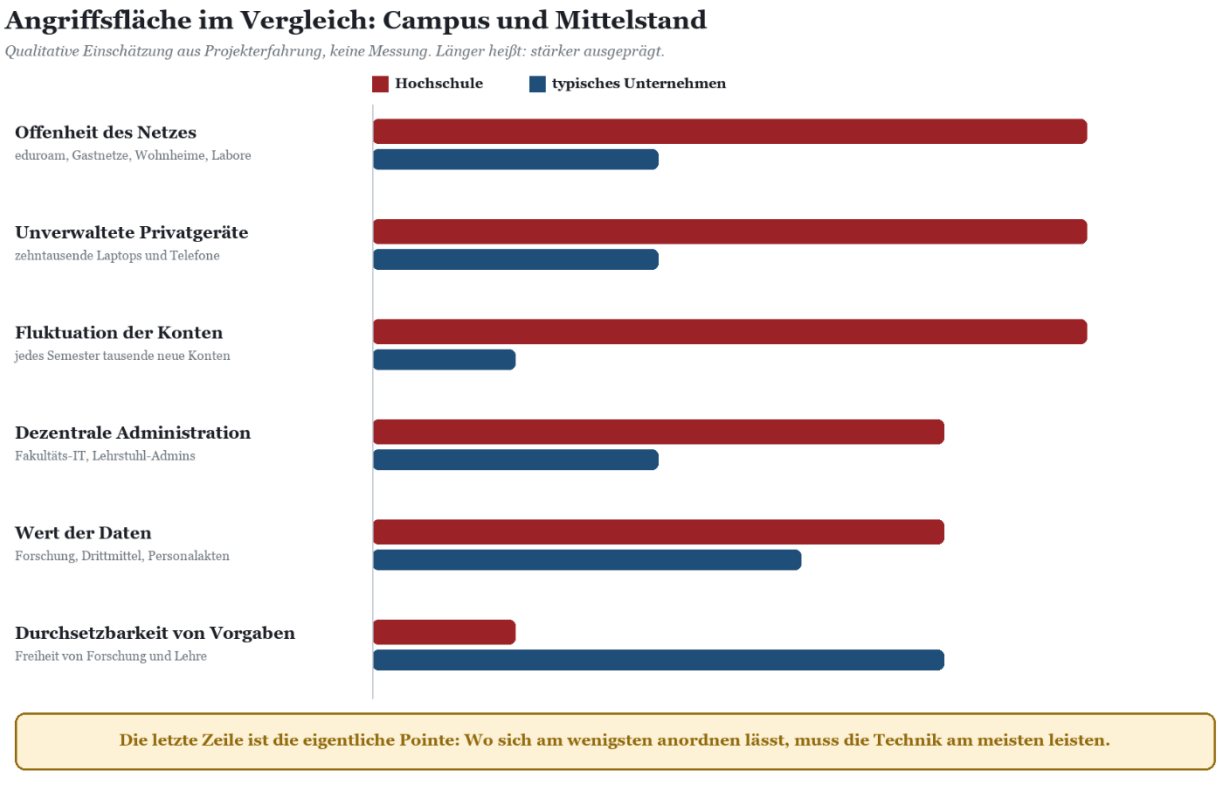
Die drei wirksamsten Maßnahmen kosten kaum Lizenzgeld: MFA für wirklich alle Konten, Legacy-Authentifizierung abschalten und privilegierte Konten konsequent trennen und schützen.

Conditional Access setzt Microsoft Entra ID P1 voraus. Die Office-365-A-Pläne enthalten laut Servicebeschreibung weder Entra ID P1 noch Intune; Microsoft 365 A3 enthält beides, Microsoft 365 A5 zusätzlich Entra ID P2 und Defender for Office 365 Plan 2.

Für Privatgeräte ist App-Schutz (MAM) die realistische Wahl, nicht die vollständige Geräteverwaltung.

Warum Hochschulen ein dankbares Ziel sind

Wer im Hochschulrechenzentrum arbeitet, kennt die Situation: Der Kollege aus der Industrie erzählt auf der Konferenz, dass bei ihm kein Gerät ohne Registrierung ins Netz kommt. Man nickt höflich und denkt an das Wohnheim, die Gastwissenschaftler aus vierzig Ländern, den Lehrstuhl mit dem selbst gebauten Messrechner und die Erstsemesterwoche, in der sich an einem Vormittag mehr neue Geräte anmelden als beim Industriekollegen im ganzen Jahr. Die Angriffsfläche einer Hochschule ist nicht größer, weil jemand geschlampt hat, sondern weil sie so gebaut ist.



Skizze 1: Der Campus ist offen gebaut. Das ist gewollt und trotzdem ein Sicherheitsproblem.

Offene Netze: eduroam, Wohnheim, Labor

Hochschulnetze sind traditionell offen. eduroam erlaubt Studenten und Wissenschaftlern aus aller Welt die Anmeldung, dazu kommen Gastnetze für Tagungen, Wohnheimnetze, Labornetze mit Messgeräten aus der Zeit, als Windows XP noch modern war, und Forschungsnetze mit eigenen Regeln. Das Netz als Vertrauensgrenze taugt auf dem Campus deshalb wenig. Für Microsoft 365

heißt das: Eine Regel wie „aus dem Hochschulnetz ohne MFA“ ist an einer Hochschule ungefähr so sicher wie ein Fahrradschloss aus Lakritz. Das IP-Netz der Hochschule ist kein vertrauenswürdiger Ort im Sinne von Conditional Access, solange jeder Wohnheimbewohner und jeder Tagungsgast darin unterwegs ist.

Ein zweiter Punkt wird gern übersehen: An vielen Hochschulen dient dieselbe Benutzerkennung für eduroam, VPN, Campus-Management, Bibliothek und die Anmeldung über die DFN-AAI. Ein gephishtes Passwort öffnet dann nicht nur das Postfach, sondern auch das Netz und die Prüfungsanmeldung. MFA in Entra ID schützt Microsoft 365 und alles, was über Entra ID angemeldet wird. Für die anderen Dienste braucht es eigene Antworten. Die Kette endet nicht am Rand des Tenants.

Zehntausende unverwaltete Privatgeräte

Studenten bringen ihre eigenen Geräte mit, und das ist auch gut so. Auch ein großer Teil des wissenschaftlichen Personals arbeitet mit privaten oder aus Drittmitteln beschafften Geräten, die nie ein Hochschulrechenzentrum gesehen haben. Lehrbeauftragte kommen mit dem Laptop ihres eigentlichen Arbeitgebers, Emeriti mit dem Tablet der Enkelin. Eine Geräteverwaltung für all diese Geräte ist weder rechtlich noch organisatorisch durchsetzbar, und niemand sollte es ernsthaft versuchen. Die Konsequenz: Die Sicherheit muss an der Identität und an den Apps hängen, nicht am Gerät.

Hohe Fluktuation und das Kontenleben nach der Exmatrikulation

Jedes Wintersemester werden tausende Konten angelegt, jedes Semester enden Verträge von studentischen Hilfskräften, wissenschaftliche Mitarbeiterinnen und Mitarbeiter wechseln nach der Befristung die Hochschule, Gastwissenschaftler kommen und gehen. Wo der Identity Lifecycle nicht sauber automatisiert ist, entstehen verwaiste Konten mit gültigem Passwort und ohne Besitzer, der eine verdächtige Anmeldung bemerken würde. Genau diese Konten sind besonders beliebt: Niemand vermisst sie, niemand liest ihre Warnmails. Wie der Lebenszyklus von der Immatrikulation bis zum Alumni-Konto aussehen sollte, beschreibt der Beitrag Identity Lifecycle an der Hochschule: Von der Immatrikulation bis zum Alumni-Konto.

Dezentrale Administration

Kaum eine Organisation verteilt Administrationsrechte so großzügig wie eine Hochschule. Fakultäts-IT, Institutsadministratoren, Lehrstuhl-Admins und engagierte Doktoranden mit „vorübergehenden“ Rechten aus dem Jahr 2016: Jede dieser Rollen ist für sich begründbar, zusammen ergeben sie eine Liste privilegierter Konten, die niemand vollständig kennt. Hinzu kommen App-Registrierungen, denen irgendwann jemand weitreichende Berechtigungen erteilt hat, und Dienstkonten mit Passwörtern, die älter sind als die aktuelle Hochschulleitung. Wie sich das in einem gemeinsamen Tenant ordnen lässt, ohne die Fakultäten zu entmündigen, zeigt der Beitrag Dezentrale IT an der Hochschule: Lehrstuhl-Admins, Fakultäts-IT und ein Tenant für alle.

Wertvolle Forschungsdaten und eine zahlende Verwaltung

Forschungsdaten, Patentvorbereitungen, Ergebnisse aus Industriekooperationen und exportkontrollierte Projekte sind für staatlich gesteuerte Angreifer interessant. Für die weniger ambitionierte, aber zahlreichere Kundschaft ist die Verwaltung lohnender: Eine Hochschule überweist regelmäßig hohe Beträge an Verbundpartner, Lieferanten und Gastwissenschaftler, und eine gefälschte Mail mit geänderter Bankverbindung aus einem echten, übernommenen Konto ist deutlich glaubwürdiger als jede Absenderfälschung. Wie Sie vertrauliche Drittmittelprojekte zusätzlich abschirmen, beschreibt der Beitrag Exportkontrolle und vertrauliche Drittmittelprojekte: Sensitivity Labels und DLP in der Forschung.

Übernommene Studentenkonten als Spam- und Phishing-Schleudern

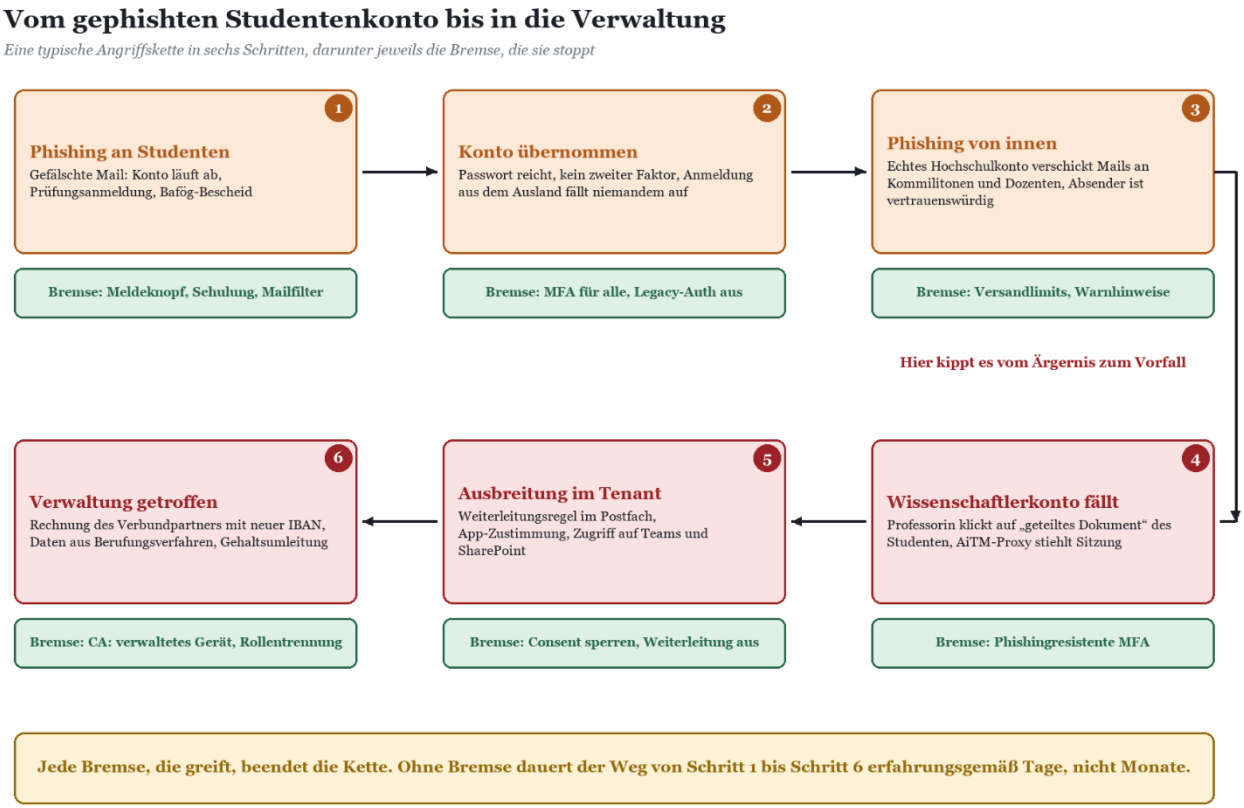
Ein übernommenes Studentenkonto ist für Angreifer ein Werkzeug mit drei Eigenschaften: Es verschickt Mails von einer seriösen Hochschuldomain, es hat Zugriff auf das Adressbuch der Hochschule und es steht in tausenden Teams und Kursgruppen. Typischerweise wird es zunächst für Spam- und Phishingwellen nach außen genutzt, bis die Versandlimits von Exchange Online greifen und das Konto für den Versand gesperrt wird. Der eigentliche Schaden entsteht aber nach innen: Phishingmails an Kommilitonen und Dozenten, die von einem bekannten Absender kommen und deshalb geöffnet werden. Nebenbei leidet der Ruf der Maildomain, und plötzlich landen auch die echten Mails des Prüfungsamts bei externen Empfängern im Spam.

WICHTIG · Vorfälle und Zahlen

Deutsche Hochschulen und Forschungseinrichtungen sind in den vergangenen Jahren wiederholt Ziel schwerer Cyberangriffe geworden, teilweise mit wochenlangen Ausfällen. Dieser Beitrag nennt bewusst keine einzelnen Einrichtungen. Wenn Sie Präsidium oder Senat überzeugen wollen, greifen Sie auf die Veröffentlichungen der betroffenen Hochschulen selbst und auf die Lageberichte des BSI zurück. Die Geschichten aus der Nachbarschaft wirken ohnehin stärker als jede Statistik.

Die typische Angriffskette

Die folgende Skizze zeigt eine Kette, wie sie in ähnlicher Form in vielen Organisationen mit offener Benutzerbasis abläuft. Keiner der Schritte erfordert besondere Raffinesse. Die Kunst des Angreifers besteht vor allem darin, geduldig zu sein und die Vertrauensbeziehungen der Hochschule auszunutzen.



Skizze 2: Das Studentenkonto ist selten das Ziel. Es ist die Eintrittskarte.

Bemerkenswert ist Schritt 4. Gegen klassisches Phishing hilft MFA sehr gut. Gegen sogenannte Adversary-in-the-Middle-Angriffe, bei denen ein Proxy zwischen Opfer und echter Anmeldeseite die Sitzung abgreift, helfen SMS-Codes und einfache Push-Bestätigungen dagegen wenig. Hier

wirken nur phishingresistente Verfahren wie Passkeys nach FIDO2 oder Windows Hello for Business, ergänzt um Regeln, die die gestohlene Sitzung auf einem fremden Gerät nutzlos machen. Für alle 30.000 Studenten ist das unrealistisch, für Verwaltung und Administratoren dagegen Pflicht.

TYPISCHE SITUATION · Wenn das echte Konto die Rechnung schickt

Aus einem kommunalen Verband kennen wir folgende Situation: Ein Postfach im Einkauf wurde übernommen, der Angreifer las wochenlang mit, legte eine Regel an, die Antworten eines bestimmten Lieferanten in einen unscheinbaren Ordner verschob, und schickte zum passenden Zeitpunkt eine Mail mit neuer Bankverbindung. Aufgefallen ist es erst, als der echte Lieferant mahnte.

Übertragen auf die Hochschule ist die Lage eher schlimmer: Verbundprojekte mit Partnern im Ausland, wechselnde Ansprechpartner, Zahlungen an Gastwissenschaftler und eine Drittmittelverwaltung, die an Ausnahmen gewöhnt ist. Ein Rückruf unter einer bekannten Nummer bei jeder Änderung der Bankverbindung ist keine IT-Maßnahme, verhindert aber mehr Schaden als manches Lizenzpaket.

Angriffswege im Überblick

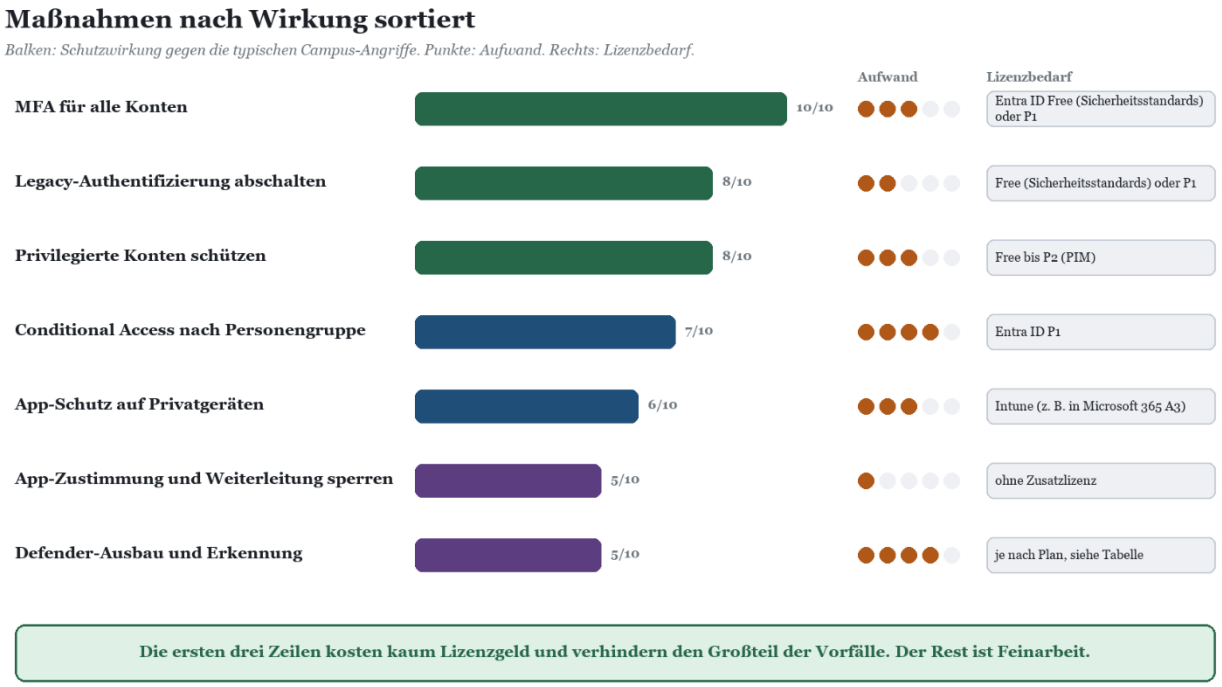
Die Tabelle fasst die häufigsten Angriffswege zusammen, jeweils mit dem Grund, warum sie an einer Hochschule besonders gut funktionieren, der passenden Gegenmaßnahme und dem Lizenzbedarf. Die Lizenzangaben beziehen sich auf die Funktion, nicht auf ein bestimmtes Paket; welche Pläne welche Funktionen enthalten, zeigt die Tabelle im dritten Abschnitt.

Angriffsweg	Warum an der Hochschule leicht	Gegenmaßnahme	Lizenzbedarf
Phishing mit Passwortdiebstahl	Viele neue Konten pro Semester, Absender wie Prüfungsamt oder Bafög-Amt sind leicht nachzuahmen	MFA für alle, Meldeknopf, Schulung zum Semesterstart	Entra ID Free (Sicherheitsstandards) oder P1
Password Spraying	Kennungen folgen einem bekannten Schema, Startpasswörter oft vorhersehbar	MFA, Smart Lockout, gesperrte Passwortlisten, kein Startpasswort per Brief ohne Ablauf	Entra ID Free; eigene gesperrte Passwörter ab P1
Legacy-Protokolle (IMAP, POP, SMTP AUTH mit Basic Auth)	Mailclients unter Linux, Skripte am Lehrstuhl, Multifunktionsgeräte, die per SMTP scannen	Legacy-Authentifizierung blockieren, OAuth oder Relay-Connector für Geräte	Sicherheitsstandards oder Conditional Access (P1)
AiTM-Phishing mit Sitzungsdiebstahl	Wissenschaftler erwarten geteilte Dokumente von Unbekannten	Phishingresistente MFA für Verwaltung und Admins, verwaltete Geräte für sensible Apps	Entra ID P1 (Authentifizierungsstärke), Intune
Consent-Phishing über bösartige Apps	Nutzerzustimmung zu Apps ist an vielen Hochschulen historisch offen	Benutzerzustimmung einschränken, Workflow für Administratorzustimmung	ohne Zusatzlizenz
Verwaiste Konten	Exmatrikulation, Vertragsende, Gastaufenthalte ohne automatisches Ende	Automatisierter Lifecycle, Zugriffsüberprüfungen, Ablauf für Gäste	Lifecycle über IDM; Zugriffsüberprüfungen ab P2
Überprivilegierte Admin-Konten	Lehrstuhl-Admins mit globalen Rollen, Rechte	Getrennte Admin-Konten, Rollen mit geringsten Rechten,	Verwaltungseinheiten ab P1, PIM ab P2

	ohne Ablaufdatum	Verwaltungseinheiten, PIM	
Datenabfluss über Privatgeräte	Kein Zugriff auf die Geräte, keine Durchsetzung per Weisung	App-Schutzrichtlinien, Sitzungsregeln für Browser	Intune, Entra ID P1
Missbrauch als Spamschleuder	Seriöse Domain, großes Adressbuch, Mitgliedschaft in vielen Teams	Ausgehende Spamrichtlinie, Weiterleitung nach extern sperren, Warnungen auswerten	Exchange Online Protection (in Exchange Online enthalten)

Maßnahmen nach Wirkung: was zuerst kommt

Sicherheitskonzepte für Hochschulen scheitern selten an fehlenden Ideen, sondern an der Reihenfolge. Wer mit dem Security Operations Center und der KI-gestützten Bedrohungsanalyse anfängt, während die Hälfte der Konten noch ohne zweiten Faktor unterwegs ist, kauft eine Alarmanlage für ein Haus ohne Tür. Die folgende Reihenfolge ist nach Schutzwirkung pro Aufwand sortiert.



Skizze 3: Wirkung schlägt Werkzeugvielfalt. Erst die Tür abschließen, dann die Alarmanlage kaufen.

1. MFA für alle, wirklich alle

Multifaktor-Authentifizierung ist die Maßnahme mit der größten Wirkung, und an Hochschulen zugleich die mit dem meisten Widerstand. Die Einwände kennen Sie: Studenten ohne Smartphone, Professoren, die keine dienstliche App auf ihr privates Telefon laden wollen, Emeriti, die seit zwanzig Jahren dasselbe Passwort nutzen und das als Ausweis von Zuverlässigkeit verstehen. Keiner dieser Einwände rechtfertigt ein Konto ohne zweiten Faktor. Sie rechtfertigen aber Alternativen: Hardware-Sicherheitsschlüssel nach FIDO2, Einmalpasswort-Token oder ein temporärer Zugangspass für die Erstregistrierung.

Microsoft hat einen Teil der Diskussion ohnehin entschieden: Seit Oktober 2024 verlangt Microsoft für Anmeldungen am Azure-Portal, am Microsoft Entra Admin Center und am Intune Admin Center MFA, seit Februar 2025 schrittweise auch für das Microsoft 365 Admin Center. Seit dem 1. Oktober 2025 folgt in einer zweiten Phase die Durchsetzung für Azure CLI, Azure

PowerShell und weitere Verwaltungswerkzeuge bei ändernden Operationen. Ausnahmen für Notfallkonten oder Studentenkonten gibt es dabei ausdrücklich nicht. Wer Administratoren noch ohne MFA arbeiten lässt, erfährt es spätestens jetzt.

Für Hochschulen, die Entra ID an einen Shibboleth-Identitätsanbieter föderieren, kommt ein Detail hinzu: Wird MFA im föderierten Identitätsanbieter erledigt, muss dieser Entra ID die erfolgte MFA per Claim mitteilen, sonst fordert Entra ID erneut oder die Anforderung bleibt unerfüllt. Wie die Anbindung an die DFN-AAI-Welt sauber gelingt, beschreibt der Beitrag Entra ID und Shibboleth: Microsoft 365 an die DFN-AAI-Welt anbinden. Wie Sie MFA für zehntausende Studenten ausrollen, ohne dass der Helpdesk in der ersten Semesterwoche kapituliert, steht in MFA für 30.000 Studenten: Conditional Access an der Hochschule ohne Helpdesk-Kollaps.

TIPP · MFA-Einführung zum Semesterstart

Verknüpfen Sie die MFA-Registrierung mit der Kontoaktivierung nach der Immatrikulation. Wer das Konto ohnehin zum ersten Mal einrichtet, registriert den zweiten Faktor im selben Schritt. Ein temporärer Zugangspass für die Erstanmeldung erspart Ihnen Startpasswörter, die als Brief oder PDF durch die Gegend reisen. Und: Planen Sie den Helpdesk für die ersten zwei Wochen des Wintersemesters großzügig, nicht für den Durchschnitt.

2. Legacy-Authentifizierung abschalten

Alte Protokolle mit Benutzername und Passwort kennen keinen zweiten Faktor. Solange sie funktionieren, ist MFA eine Haustür mit Sicherheitsschloss neben einem offenen Kellerfenster. In Exchange Online hat Microsoft die Basic-Authentifizierung für Exchange ActiveSync, POP, IMAP, EWS, Remote PowerShell und Outlook bereits abgeschaltet; sie lässt sich nicht wieder aktivieren. Übrig ist SMTP AUTH für den Mailversand. Nach dem aktuellen Zeitplan von Microsoft wird Basic Auth für SMTP AUTH Ende Dezember 2026 in bestehenden Tenants standardmäßig deaktiviert, Administratoren können sie dann aber noch wieder einschalten. Den endgültigen Abschalttermin will Microsoft in der zweiten Jahreshälfte 2027 bekanntgeben.

An Hochschulen hängen an SMTP AUTH typischerweise Multifunktionsgeräte, Laborsoftware, Monitoring-Skripte und das eine Webformular des Instituts, das seit 2014 Mails verschickt. Nutzen Sie die Zeit bis zur Umstellung für eine Inventur: Die Anmeldeprotokolle in Entra ID zeigen, welche Konten noch mit alten Protokollen arbeiten. Geräte gehören auf einen Relay-Connector oder auf OAuth, Skripte auf die Graph-API. Danach blockieren Sie Legacy-Authentifizierung tenantweit per Conditional Access oder über die Sicherheitsstandards. Wer noch lokale Exchange-Server oder Alt-Mailsysteme betreibt, findet Hinweise im Beitrag Exchange an der Hochschule: Hybrid, Alt-Mailserver und die Studenten-Mail.

WARNUNG · Das Kellerfenster heißt oft IMAP

IMAP ist an Hochschulen beliebter als anderswo, weil Mailclients unter Linux und selbst gepflegte Mailfilter zur Kultur gehören. Moderne Clients wie Thunderbird beherrschen OAuth für IMAP; ältere Konfigurationen tun es nicht. Bevor Sie blockieren, sollten Sie wissen, wer betroffen ist, und eine Anleitung bereitstellen. Sonst erfahren Sie es vom Dekan persönlich.

3. Privilegierte Konten schützen

Ein übernommenes Studentenkonto ist ärgerlich, ein übernommenes Konto mit der Rolle Globaler Administrator ist das Ende des Tenants, wie Sie ihn kennen. Privilegierte Konten verdienen deshalb eine Sonderbehandlung, die konsequent und ohne Ausnahmen für verdiente Professoren gilt:

- **Getrennte Admin-Konten:** Administrative Rollen hängen an eigenen, reinen Cloud-Konten ohne Postfach, nicht am Alltagskonto, mit dem Mails gelesen und Dokumente geöffnet werden.
- **Wenige globale Administratoren:** Microsoft empfiehlt weniger als fünf Konten mit der Rolle Globaler Administrator. Alles andere läuft über Rollen mit geringeren Rechten, etwa Exchange-, Teams- oder Benutzeradministrator.
- **Verwaltungseinheiten für die Fakultäts-IT:** Administrative Einheiten erlauben, Rollen auf die Konten und Gruppen einer Fakultät zu beschränken. Der Lehrstuhl-Admin setzt dann Passwörter für sein Institut zurück, nicht für das Präsidium.
- **Rollen nur bei Bedarf:** Privileged Identity Management (Entra ID P2) aktiviert Rollen zeitlich begrenzt, mit Begründung und optional mit Genehmigung.
- **Phishingresistente MFA:** Für Admin-Konten sind Passkeys oder FIDO2-Sicherheitsschlüssel Pflicht, durchgesetzt über eine Authentifizierungsstärke in Conditional Access.
- **Notfallzugänge:** Mindestens zwei Notfallkonten, von den meisten Regeln ausgenommen, aber ebenfalls mit MFA, idealerweise per FIDO2-Schlüssel im Tresor, und mit Alarm bei jeder Anmeldung.

Wie viele privilegierte Konten, verwaiste App-Registrierungen und vergessene Dienstkonten sich in einem über Jahre gewachsenen Hochschul-Tenant finden, überrascht regelmäßig auch erfahrene Rechenzentrumsleute. Eine systematische Bestandsaufnahme beschreibt der Beitrag Entra-ID-Überprüfung für Hochschul-Tenants: Was sich nach zehn Jahren Wildwuchs findet.

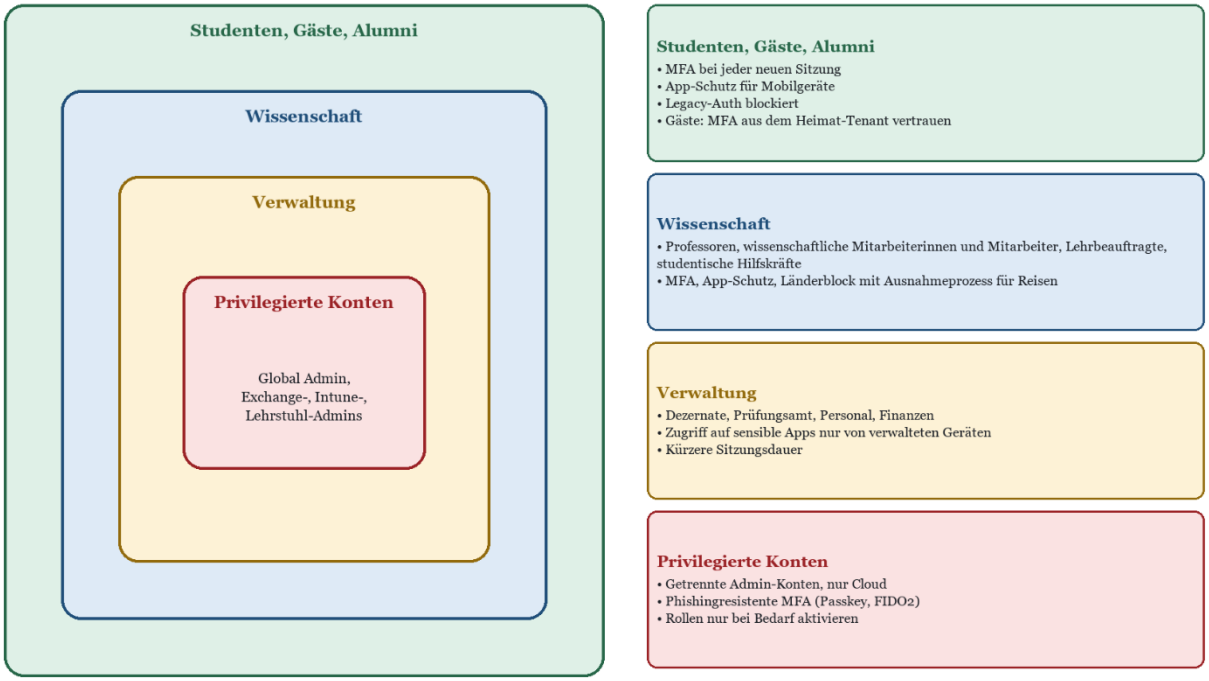
4. Conditional Access nach Personengruppe

Conditional Access ist das Regelwerk, mit dem Entra ID bei jeder Anmeldung entscheidet: zulassen, blockieren oder zusätzliche Bedingungen verlangen. Die Funktion setzt Microsoft Entra ID P1 voraus, risikobasierte Regeln auf Basis von Anmelde- und Benutzerrisiko zusätzlich Entra ID P2. Ohne P1 bleiben die Sicherheitsstandards, die für alle Kunden verfügbar sind und MFA sowie das Blockieren alter Protokolle tenantweit einschalten, allerdings ohne jede Differenzierung.

An einer Hochschule passt eine Einheitsregel selten. Die Studentin im Wohnheim, der Gastwissenschaftler aus dem Verbundprojekt und die Sachbearbeiterin im Personaldezernat haben unterschiedliche Risiken und unterschiedliche Zugriffsrechte. Bewährt hat sich ein Zonenmodell nach Personengruppe, das sich aus dem Identitätsmanagement speist: Gruppenmitgliedschaften entstehen automatisch aus dem Status im Campus-Management und im Personalsystem, nicht per Hand.

Conditional Access nach Personengruppe: vier Zonen

Je weiter innen, desto strenger. Niemand landet ohne MFA im Tenant.



Skizze 4: Zonen statt Einheitsregel. Die Studentin im Wohnheim ist nicht der Kanzler am Dienstrechner.

Personengruppe	Mindestanforderung	Zusätzlich sinnvoll	Typischer Stolperstein
Studenten	MFA, Legacy-Auth blockiert	App-Schutz auf Mobilgeräten, Sitzungsdauer begrenzen	Lizenz: Entra ID P1 nicht in jedem Plan enthalten
Wissenschaftliches Personal	MFA, Legacy-Auth blockiert, App-Schutz	Länderblock mit dokumentiertem Ausnahmeprozess für Dienstreisen und Feldforschung	Messrechner und Skripte mit Benutzerkonto
Verwaltung	Phishingresistente MFA oder verwaltetes Gerät für sensible Apps	Zugriff auf Finanz- und Personaldaten nur von konformen Geräten	Homeoffice mit Privatgerät ohne Plan B
Gäste und Verbundpartner	MFA, vertrauenswürdige MFA aus dem Heimat-Tenant	Ablaufdatum, Zugriffsüberprüfung	Mandantenübergreifende Vertrauenseinstellungen fehlen
Privilegierte Konten	Phishingresistente MFA, getrennte Konten	Admin-Arbeitsplätze, PIM, Anmeldung nur von bestimmten Geräten	Notfallkonten vergessen oder ungeschützt

Zwei Hinweise aus der Praxis: Starten Sie jede neue Regel im Modus „Nur Bericht“ und werten Sie die Anmeldeprotokolle mindestens zwei Wochen aus, besser über einen Semesterwechsel hinweg. Und schließen Sie Notfallkonten von blockierenden Regeln aus, bevor Sie die erste scharf schalten. Für Gäste aus Partnerhochschulen lohnt ein Blick auf die Einstellungen für den mandantenübergreifenden Zugriff, mit denen Sie MFA aus dem Heimat-Tenant anerkennen, statt Gäste doppelt registrieren zu lassen. Details dazu im Beitrag Hochschulübergreifend zusammenarbeiten: B2B, mandantenübergreifender Zugriff und Verbundprojekte.

HINWEIS · Personalrat, Datenschutz und Landesrecht

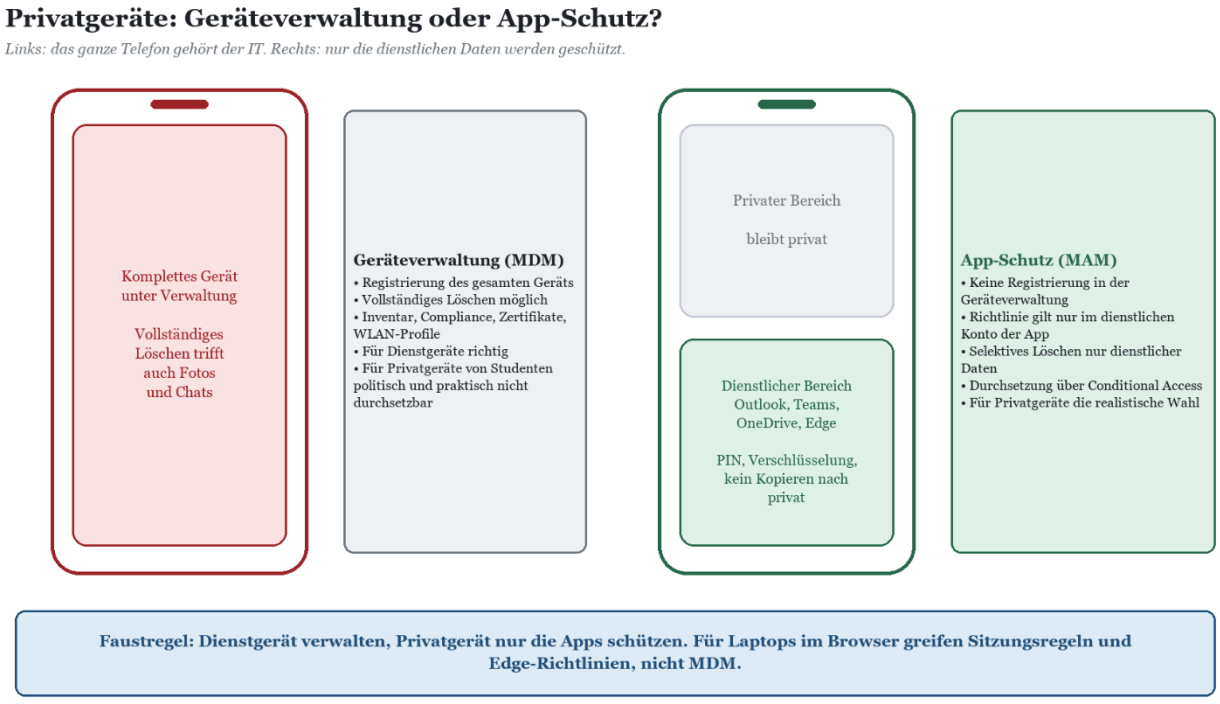
MFA auf privaten Telefonen, Anmeldeprotokolle und Regeln nach Personengruppe berühren Mitbestimmungsrechte und Datenschutz. Ob eine Dienstvereinbarung nötig ist, ob Mitarbeiterinnen und Mitarbeiter ihr privates Telefon als zweiten Faktor verwenden müssen oder die Hochschule Alternativen wie Sicherheitsschlüssel bereitstellt, regeln Personalvertretungsgesetze und Landesdatenschutzgesetze je Bundesland unterschiedlich. In Forschungseinrichtungen privater Rechtsform ist statt des Personalrats ein Betriebsrat zuständig. Dieser Beitrag ist keine Rechtsberatung; beziehen Sie Personalrat, Datenschutzbeauftragte und Justitiariat früh ein.

Hintergründe zur Mitbestimmung finden Sie im Beitrag Personalrat und Microsoft 365 an der Hochschule: Dienstvereinbarung, wissenschaftliches Personal und die Verhaltenskontrolle.

5. App-Schutz statt Geräteverwaltung für Privatgeräte

Für Dienstgeräte ist die Sache klar: Sie gehören in die Geräteverwaltung, ob mit Intune, mit einem anderen Werkzeug oder in Koexistenz mit der bewährten Linux- und Mac-Verwaltung des Rechenzentrums. Für Privatgeräte ist Intune-MDM der falsche Ansatz. Niemand möchte, dass die Hochschule das ganze Telefon löschen kann, und kein Personalrat wird dem zustimmen.

App-Schutzrichtlinien (Mobile Application Management, kurz MAM) setzen eine Ebene tiefer an: Sie gelten für Outlook, Teams, OneDrive, Edge und die Office-Apps, aber nur im dienstlichen Konto. Sie verlangen eine PIN für die App, verschlüsseln dienstliche Daten, verhindern das Kopieren in private Apps und erlauben ein selektives Löschen nur der dienstlichen Daten. Laut Microsoft funktionieren sie auch auf Geräten, die in keiner Geräteverwaltung registriert sind. Durchgesetzt werden sie über Conditional Access mit der Bedingung „App-Schutzrichtlinie erforderlich“. Voraussetzung ist eine Intune-Lizenz für die betroffenen Konten; auf Android braucht es zusätzlich die App Unternehmensportal, ohne dass das Gerät registriert werden muss.



Skizze 5: Niemand muss das Urlaubsfoto der Doktorandin verwalten, um ihr Postfach zu schützen.

Für private Laptops greift App-Schutz nur eingeschränkt. Dort helfen Sitzungsregeln: Zugriff über den Browser ohne Download, begrenzte Sitzungsdauer und für besonders sensible Bereiche schlicht kein Zugriff von unverwalteten Geräten. Das ist für Prüfungsamt und Personaldezernat zumutbar, für den Doktoranden im Labor eher nicht. Welche Bestände eine solche

Sonderbehandlung verdienen, beschreibt der Beitrag Prüfungsdaten, Berufungsakten, Personalvorgänge: Besonders schützenswerte Daten im Hochschul-Tenant.

TYPISCHE SITUATION · Die Krankenhaus-Lösung für das Telefon

In einem Krankenhausverbund stellte sich die Frage, wie Ärztinnen, Ärzte und Pflegekräfte mit privaten Telefonen auf dienstliche Mail und Teams zugreifen dürfen. Die Geräteverwaltung scheiterte am Widerstand der Belegschaft, nach dem Wechsel auf App-Schutz war das Thema nach wenigen Wochen erledigt: Die Dienst-Apps verlangen eine PIN, Kopieren nach privat ist gesperrt, das Gerät bleibt privat.

An der Hochschule ist die Situation typischerweise dieselbe, nur mit mehr Gerätetypen und weniger Weisungsbefugnis. Gerade deshalb ist App-Schutz der Kompromiss, der sich vor Personalrat und Senat vertreten lässt.

6. Die kleinen Schalter mit großer Wirkung

Einige Einstellungen kosten weder Lizenz noch Projekt, werden aber erstaunlich oft übersehen:

- **Benutzerzustimmung zu Apps einschränken:** Studenten und Wissenschaftler sollten nicht beliebigen Apps Zugriff auf Postfach und Dateien gewähren können. Ein Workflow für Administratorzustimmung hält den Weg für legitime Werkzeuge offen.
- **Automatische Weiterleitung nach extern:** Die ausgehende Spamrichtlinie steuert, ob Postfachregeln Mails nach außen weiterleiten dürfen. Prüfen Sie, ob das aus Bequemlichkeit für alle freigegeben wurde, und erlauben Sie Ausnahmen gezielt.
- **Versandlimits und Warnungen:** Exchange Online sperrt Konten, die Versandgrenzen überschreiten. Sorgen Sie dafür, dass die zugehörigen Warnungen jemand liest, und zwar nicht erst am Montag.
- **Selbstregistrierung von Mandanten und Geräten:** Prüfen Sie, wer neue App-Registrierungen anlegen, Geräte beitreten lassen und Gäste einladen darf.
- **Meldeknopf für Phishing:** Ein sichtbarer Melde-Button in Outlook macht aus 30.000 potenziellen Opfern 30.000 Sensoren. Einige davon melden sogar echtes Phishing.

Defender und Lizenzstufen: was in welchem Plan steckt

Bei der Frage, welche Schutzfunktionen tatsächlich lizenziert sind, gehen die Meinungen im Rechenzentrum, in der Beschaffung und beim Microsoft-Vertrieb gern auseinander. Die folgende Übersicht basiert auf der Servicebeschreibung für Microsoft 365 Education auf learn.microsoft.com, Stand Oktober 2026. Lizenzpläne ändern sich, prüfen Sie den aktuellen Stand vor jeder Entscheidung. Preise nennen wir bewusst nicht. Eine ausführliche Einordnung der Pläne und des Student Use Benefit finden Sie im Beitrag Education-Lizenzen verstehen: A1, A3, A5 und der Student Use Benefit.

Funktion	Office 365 A1, A3, A5	Microsoft 365 A3	Microsoft 365 A5	Student Use Benefit (Microsoft 365 A3 / A5)
Exchange Online Protection (Basisschutz für Mail)	ja	ja	ja	ja / ja
Microsoft Entra ID P1 (Conditional Access)	nein	ja	über P2 enthalten	ja / ja
Microsoft Entra ID P2 (ID Protection, PIM)	nein	nein	ja	nein / ja

Intune (App-Schutz, Geräteverwaltung)	nein	ja	ja	ja / ja
Defender for Office 365 Plan 2	nein	nein	ja	nein / ja
Defender for Endpoint	nein	Plan 1	Plan 2	nein / nein
Defender for Identity	nein	nein	ja	nein / ja
Defender for Cloud Apps	nein (A3, A5: Office 365 Cloud App Security)	Office 365 Cloud App Security	ja	nein / ja

FAKTEN · Was die Tabelle bedeutet

Eine Hochschule, die ausschließlich Office-365-A-Pläne einsetzt, hat laut Servicebeschreibung weder Conditional Access noch Intune. Ihr bleiben die Sicherheitsstandards, also MFA und Blockade alter Protokolle für alle, ohne Differenzierung nach Personengruppen.

Microsoft 365 A3 ist die Stufe, ab der das Zonenmodell aus diesem Beitrag vollständig umsetzbar ist: Entra ID P1 für Conditional Access, Intune für App-Schutz, Defender for Endpoint Plan 1 für die Dienstgeräte.

Microsoft 365 A5 bringt die Erkennungs- und Reaktionsseite: Entra ID P2 mit risikobasierten Regeln und PIM, Defender for Office 365 Plan 2 mit Angriffssimulation und automatisierter Untersuchung, Defender for Identity für das lokale Active Directory.

Gemischte Lizenzierung: der Normalfall

Kaum eine Hochschule lizenziert alle Personengruppen gleich. Typisch ist ein Mix aus Microsoft 365 A3 oder A5 für Mitarbeiterinnen und Mitarbeiter, einem Student-Use-Benefit- oder A1-Plan für Studenten und Sonderfällen für Gäste, Lehrbeauftragte und Emeriti. Für die Sicherheitsarchitektur hat das eine einfache Konsequenz: Regeln, die eine Lizenz voraussetzen, gelten lizenzrechtlich nur für lizenzierte Konten. Prüfen Sie deshalb vor dem Entwurf des Zonenmodells, welche Gruppe welche Pläne hat. Wer Studenten ohne Entra ID P1 hat, landet bei einer Entscheidung zwischen tenantweiten Sicherheitsstandards und einer Lizenzergänzung.

Defender ist kein Ersatz für Hygiene

Defender-Produkte erkennen Angriffe, untersuchen Vorfälle und reagieren teilweise automatisch. Sie entfalten ihren Wert aber nur, wenn jemand die Warnungen liest und handeln darf. An vielen Hochschulen ist das der wunde Punkt: Ein Rechenzentrum mit wenigen Stellen für Sicherheit, keine Rufbereitschaft am Wochenende, und die Warnung über das verdächtige Postfach liegt bis Montag im Sammelpostfach. Bevor Sie A5 nur wegen Defender beschaffen, klären Sie, wer die Konsole betreut. Ein ungelesenes Dashboard schützt genauso gut wie kein Dashboard. Unterstützung beim Aufbau von Betriebsprozessen und Rollen bietet die Microsoft-365-Beratung für Hochschulen und Forschung, die Qualifizierung des Teams die Microsoft-365-Schulung für Hochschulen und Forschung.

TIPP · Erst messen, dann kaufen

Microsoft Secure Score und die Berichte zu Authentifizierungsmethoden und Anmeldungen stehen in jedem Tenant zur Verfügung. Sie zeigen ohne Zusatzlizenz, wie viele Konten MFA registriert haben, wer noch alte Protokolle nutzt und welche Empfehlungen offen sind. Diese Zahlen sind für das Präsidium überzeugender als jede Herstellerfolie, und sie zeigen, ob eine teurere Lizenzstufe das eigentliche Problem überhaupt löst.

Ein realistischer Fahrplan für das Hochschulrechenzentrum

Sicherheit an der Hochschule ist ein Marathon mit Semesterrhythmus. Große Umstellungen gehören in die vorlesungsfreie Zeit, nicht in die erste Woche des Wintersemesters und nicht in die Prüfungsphase. Der folgende Fahrplan hat sich als Gerüst bewährt und lässt sich an Größe und Ausgangslage anpassen.

Phase	Maßnahmen	Beteiligte	Ergebnis
Bestandsaufnahme (vier bis sechs Wochen)	Privilegierte Konten, Legacy-Anmeldungen, MFA-Abdeckung, App-Zustimmungen, Lizenzen je Gruppe	Hochschulrechenzentrum, Fakultäts-IT	Belastbare Zahlen für das Präsidium
Sofortmaßnahmen	Notfallkonten, getrennte Admin-Konten, MFA für alle Admins, App-Zustimmung einschränken, Weiterleitung prüfen	Hochschulrechenzentrum	Die größten Löcher sind zu
Beteiligung	Personalrat, Datenschutz, Kanzler, Senatsausschuss für IT	Präsidium, Personalrat, Datenschutzbeauftragte	Freigabe für MFA und Regelwerk
MFA-Rollout	Verwaltung und Wissenschaft zuerst, Studenten zum Semesterstart mit der Kontoaktivierung	Rechenzentrum, Helpdesk, Studentensekretariat	MFA-Abdeckung nahe hundert Prozent
Legacy-Auth und Conditional Access	Inventur der Altprotokolle, Regeln im Berichtsmodus, dann scharf	Rechenzentrum, Fakultäts-IT	Zonenmodell aktiv
Ausbau	App-Schutz, phishingresistente MFA für Verwaltung, PIM, Defender-Prozesse	Rechenzentrum, Verwaltung	Erkennung und Reaktion im Regelbetrieb

Überzeugen statt anordnen

Kein Präsidium kann einer Professorin vorschreiben, wie sie forscht. Es kann aber festlegen, wie man sich an den zentralen Diensten der Hochschule anmeldet. Diese Unterscheidung ist der Schlüssel für die Diskussion im Senat: Die Freiheit von Forschung und Lehre schützt den Inhalt der Arbeit, nicht das Recht auf ein Passwort ohne zweiten Faktor. Erfahrungsgemäß hilft es, das Thema nicht als IT-Vorgabe, sondern als Schutz der Wissenschaft zu formulieren: Die Forschungsdaten und Drittmittelprojekte der Fakultäten sind das, was Angreifer wollen.

TYPISCHE SITUATION · Die Stadtverwaltung und der Bürgermeister

In einer Stadtverwaltung scheiterte die MFA-Einführung zunächst an genau einer Person: dem Bürgermeister, der keine App auf sein Telefon laden wollte. Gelöst wurde es mit einem Sicherheitsschlüssel am Schlüsselbund und dem Hinweis, dass gerade sein Postfach das lohnendste Ziel im Haus ist. Danach war das Thema für die restliche Belegschaft keines mehr.

An der Hochschule übernimmt diese Rolle typischerweise ein Mitglied des Präsidiums oder ein prominenter Lehrstuhlinhaber. Wer die Leitung zuerst überzeugt und mit gutem Beispiel vorangehen lässt, spart sich viele Einzeldiskussionen.

Häufige Fragen

Reichen die Sicherheitsstandards von Microsoft für eine Hochschule?

Für den Anfang sind sie deutlich besser als nichts: Sie erzwingen MFA und blockieren alte Protokolle für alle Konten. Sie lassen sich aber nicht nach Personengruppen differenzieren und vertragen sich nicht mit eigenen Regeln in Conditional Access. Für eine Hochschule mit Verwaltung, Wissenschaft, Studenten und Gästen ist Conditional Access mit Entra ID P1 auf Dauer die bessere Wahl.

Brauchen wir für Conditional Access Microsoft 365 A5?

Nein. Conditional Access setzt Entra ID P1 voraus, das laut Servicebeschreibung in Microsoft 365 A3 enthalten ist. A5 bringt mit Entra ID P2 zusätzlich risikobasierte Regeln und Privileged Identity Management. Die Office-365-A-Pläne enthalten Entra ID P1 dagegen nicht.

Was machen wir mit Studenten ohne Smartphone?

Bieten Sie Alternativen an: FIDO2-Sicherheitsschlüssel, Einmalpasswort-Token oder eine Authenticator-App auf dem Laptop. Für die Erstregistrierung hilft ein temporärer Zugangspass. Ein Konto ohne zweiten Faktor ist keine Alternative.

Ist das Hochschulnetz ein vertrauenswürdiger Ort für Conditional Access?

In aller Regel nicht. eduroam, Wohnheime und Gastnetze machen das Campusnetz zu einem Ort, an dem sich jeder aufhalten kann. Ausnahmen von MFA auf Basis der IP-Adresse der Hochschule öffnen genau den Angreifern die Tür, die bereits ein Passwort erbeutet haben und sich ins WLAN setzen.

Können wir Privatgeräte von Mitarbeiterinnen und Mitarbeitern mit Intune verwalten?

Technisch ja, praktisch ist es selten sinnvoll. App-Schutzrichtlinien schützen die dienstlichen Daten in Outlook, Teams und OneDrive, ohne das Gerät zu registrieren. Das ist für Personalrat und Belegschaft deutlich leichter vermittelbar und deckt die meisten Risiken ab.

Wann wird SMTP AUTH mit Basic Auth abgeschaltet?

Nach dem aktuellen Zeitplan von Microsoft wird Basic Auth für SMTP AUTH Ende Dezember 2026 in bestehenden Tenants standardmäßig deaktiviert, lässt sich aber zunächst wieder einschalten. Den endgültigen Termin will Microsoft in der zweiten Jahreshälfte 2027 bekanntgeben. Planen Sie die Umstellung trotzdem jetzt.

Wie gehen wir mit Lehrstuhl-Admins um, die globale Rechte haben?

Entziehen Sie globale Rollen und vergeben Sie Rollen mit geringeren Rechten, beschränkt auf Verwaltungseinheiten der jeweiligen Fakultät oder des Instituts. Admin-Tätigkeiten laufen über getrennte Konten mit phishingresistenter MFA. Das nimmt der Fakultäts-IT keine Arbeit weg, nur das Risiko.

Gilt das auch für außeruniversitäre Forschungseinrichtungen?

Weitgehend ja. Die Zahl der Studentenkonten ist kleiner, dafür sind Gäste, Verbundpartner und internationale Kooperationen oft noch zahlreicher, und der Wert der Forschungsdaten ist mindestens so hoch. Je nach Rechtsform ist statt des Personalrats ein Betriebsrat zu beteiligen.

Fazit: Die Tür abschließen, bevor man die Alarmanlage kauft

Hochschulen werden nicht angegriffen, weil sie schlechter administriert wären als andere Organisationen, sondern weil Offenheit, Fluktuation und dezentrale Verantwortung zu ihrem Wesen gehören. Das lässt sich nicht abstellen und soll es auch nicht. Es lässt sich aber so

absichern, dass ein gephishtes Studentenkonto ein Ärgernis bleibt und nicht zum Einstieg in die Verwaltung wird.

Die Reihenfolge entscheidet: MFA für alle, Legacy-Authentifizierung abschalten, privilegierte Konten trennen und schützen. Danach Conditional Access nach Personengruppe, App-Schutz für Privatgeräte und erst dann der Ausbau von Erkennung und Reaktion. Die ersten drei Schritte kosten vor allem Überzeugungsarbeit und Helpdesk-Kapazität, kaum Lizenzgeld. Wer sie hinter sich hat, kann über A5 und Security Operations reden. Wer sie überspringt, kauft eine sehr teure Alarmanlage für ein Haus, dessen Tür offen steht. Wenn Sie dabei Unterstützung wollen, finden Sie die passenden Angebote in der Microsoft-365-Beratung für Hochschulen und Forschung.

WEITERLESEN · Weiterlesen

Für diesen Beitrag besonders passend aus der Serie:

› MFA für 30.000 Studenten: Conditional Access an der Hochschule ohne Helpdesk-Kollaps
› Entra-ID-Überprüfung für Hochschul-Tenants: Was sich nach zehn Jahren Wildwuchs findet
› Dezentrale IT an der Hochschule: Lehrstuhl-Admins, Fakultäts-IT und ein Tenant für alle
› 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
› Hochschulübergreifend zusammenarbeiten: B2B, mandantenübergreifender Zugriff und Verbundprojekte