Conditional Access für Verwaltungen: Regelwerk für Rathaus, Bauhof und Homeoffice

Es gibt einen Moment in jedem Projekt, in dem der Charme des Themas endgültig verfliegt. Bei Conditional Access ist das der Moment, in dem jemand aus der Kämmerei fragt, ob das dann auch für die Kassenaufsicht gilt, die am Monatsende gelegentlich von zu Hause aus freigibt. Bis dahin haben alle genickt. Ab dieser Frage wird verhandelt.

Das ist auch richtig so. Conditional Access ist keine Technikentscheidung, die man in der IT unter sich ausmacht. Es ist ein Regelwerk, das festlegt, wer unter welchen Umständen an welche Daten kommt – und damit ein Stück Organisationsrecht, das zufällig in einem Verwaltungsportal konfiguriert wird. Wer es als reine Technik behandelt, bekommt am Ende ein technisch sauberes Regelwerk, das im Bauhof niemand benutzen kann und für das der Personalrat nachträglich eine Erklärung verlangt.

Gleichzeitig ist die Ausgangslage in Verwaltungen unangenehm eindeutig. Die Angriffe auf Kommunen der letzten Jahre begannen fast alle gleich: ein Konto, ein Kennwort, kein zweiter Faktor, ein altes Protokoll, das nie jemand abgeschaltet hat. Der Rest ist bekannt – Bürgerbüro geschlossen, Wochen ohne Fachverfahren, Pressemitteilungen in einem Tonfall, den man kein zweites Mal formulieren möchte. Conditional Access ist die eine Maßnahme, die genau diesen Einstieg zumacht.

Dieser Beitrag beschreibt ein Regelwerk, das in einer Verwaltung tatsächlich funktioniert. Nicht das Maximum, das technisch möglich wäre, sondern die Stufen, die sich in Rathäusern, Kreisverwaltungen und Zweckverbänden umsetzen lassen, ohne dass der Winterdienst um vier Uhr morgens vor einer Anmeldeaufforderung steht, die er nicht beantworten kann.

Der Beitrag gehört zur Reihe Microsoft 365 in der öffentlichen Verwaltung. Dort finden Sie den Überblick über die Themen, die bei einer Einführung zusammenhängen: Betriebsmodell, Vergabe, Schriftgut, Datenschutz. Conditional Access ist der Baustein, der alle anderen absichert – und derjenige, der am häufigsten zu spät angefasst wird, nämlich erst dann, wenn die Fachämter schon produktiv arbeiten und jede Regeländerung Betroffene hat.

Warum das Regelwerk einer Verwaltung anders aussieht

Drei Arbeitswelten, ein Tenant

Ein mittelständisches Unternehmen mit 800 Beschäftigten hat im Zweifel 800 ähnliche Arbeitsplätze: Notebook, Büro, Homeoffice, fertig. Eine Stadtverwaltung mit 800 Beschäftigten hat mindestens fünf grundverschiedene Arbeitswelten im selben Tenant, und die Unterschiede sind nicht kosmetisch.

Da ist erstens das Rathaus: feste Arbeitsplätze, verwaltete Rechner, kabelgebundenes Netz, Sachbearbeitung mit Fachverfahren. Zweitens der Außendienst – Bauhof, Grünflächen,

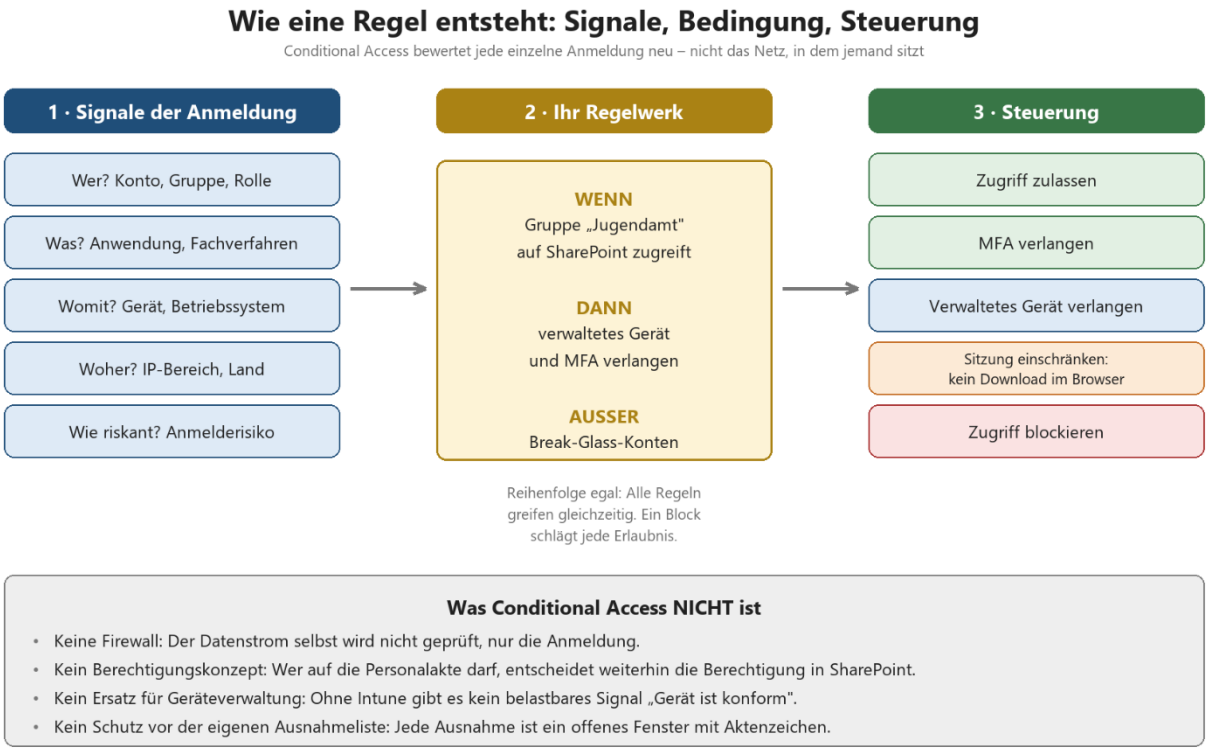
Winterdienst, Ordnungsamt, Feuerwehr –, wo mit Tablets im Fahrzeug gearbeitet wird, oft über Mobilfunk, oft mit Handschuhen, gelegentlich mit einem Gerät, das drei Leuten gleichzeitig gehört. Drittens das Homeoffice, das seit der Dienstvereinbarung kein Ausnahmezustand mehr ist, sondern Regelbetrieb für ganze Fachämter. Viertens die besonders schutzbedürftigen Bereiche: Jugendamt, Sozialamt, Personalamt, Gesundheitsamt, Kasse. Und fünftens die Gruppe, die in keinem Organigramm auftaucht und trotzdem Zugriff braucht: Ratsmitglieder, sachkundige Bürger, ehrenamtliche Wehrführungen, Aufsichtsratsmitglieder kommunaler Gesellschaften.

Diese fünfte Gruppe ist der Grund, warum Standardvorlagen in Verwaltungen scheitern. Ein Ratsmitglied ist rechtlich kein Beschäftigter. Es bekommt kein Diensthandy, es unterliegt keiner Dienstanweisung im arbeitsrechtlichen Sinn, und es wird sein privates Tablet nicht in die Geräteverwaltung der Verwaltung aufnehmen lassen. Trotzdem muss es die Sitzungsunterlagen lesen können, darunter regelmäßig nichtöffentliche Vorlagen mit Personalbezug oder Grundstücksdaten. Jedes Regelwerk, das diese Gruppe nicht sauber löst, wird an ihr aufgeweicht – meist durch eine Ausnahme, die jemand abends „nur mal kurz" setzt und die dann acht Jahre bleibt.

Was Conditional Access leistet – und was nicht

Conditional Access sitzt an genau einer Stelle: bei der Anmeldung. Es bewertet, wer sich anmeldet, an welcher Anwendung, mit welchem Gerät, aus welchem Netz, mit welchem erkannten Risiko – und entscheidet daraufhin, ob der Zugriff durchgeht, ob ein zweiter Faktor kommt, ob ein verwaltetes Gerät verlangt wird, ob die Sitzung eingeschränkt wird oder ob schlicht Schluss ist.

Was es nicht leistet, ist mindestens genauso wichtig, weil es in Beschlussvorlagen regelmäßig zu großzügig beschrieben wird. Conditional Access ersetzt kein Berechtigungskonzept: Wer nach bestandener Anmeldung auf die Personalakte zugreifen darf, entscheidet weiterhin die Berechtigung in SharePoint – ein Thema, das seine eigene Sprengkraft hat, sobald eine Suche über den ganzen Tenant läuft. Es ersetzt auch keine Geräteverwaltung: Ohne Intune oder eine vergleichbare Verwaltung gibt es schlicht kein belastbares Signal, ob ein Gerät verschlüsselt und aktuell ist. Und es schützt nicht vor der eigenen Ausnahmeliste.



Skizze 1: Jede Anmeldung wird neu bewertet. Die Kunst liegt nicht in den Regeln, sondern darin, die Ausnahmen zählbar zu halten.

Wer die Berechtigungsseite unterschätzt, findet sie spätestens bei der ersten KI-gestützten Suche wieder. Warum das so ist, steht in Oversharing im Verwaltungs-Tenant: Warum Copilot die Personalakte findet. Conditional Access und Berechtigungen sind zwei Schlösser an zwei verschiedenen Türen; keines ersetzt das andere.

Die Lizenzfrage, kurz und schmerzlos

Bevor jemand ein Regelwerk entwirft, das die Verwaltung nicht bezahlen kann: Conditional Access setzt Microsoft Entra ID P1 voraus. P1 steckt in Microsoft 365 E3, in F3 und in F1, also in genau den Plänen, die in Verwaltungen ohnehin üblich sind. Risikobasierte Regeln – also Regeln, die auf ein erkanntes Anmelde- oder Benutzerrisiko reagieren – setzen dagegen P2 voraus, wie es in E5 enthalten ist. Wer kein P1 hat, kann nur mit den Sicherheitsstandards arbeiten: ein pauschales Alles-oder-nichts ohne Gruppen, ohne Standorte, ohne Ausnahmen. Für einen Kleinstverband mit zwölf Konten mag das reichen. Für eine Kreisverwaltung ist es keine Grundlage.

Funktion	Entra ID P1 (in E3, F3, F1)	Entra ID P2 (in E5)
Regeln nach Gruppe, App, Plattform	enthalten	enthalten
MFA erzwingen, Legacy blockieren	enthalten	enthalten
Verwaltetes bzw. konformes Gerät verlangen	enthalten	enthalten
Benannte Standorte, Ländersperren	enthalten	enthalten
Sitzungssteuerung, Anmeldehäufigkeit	enthalten	enthalten

Authentifizierungsstärke, phishing-resistente MFA	enthalten	enthalten
Regeln nach Anmelde- und Benutzerrisiko	nicht enthalten	enthalten
Zeitlich befristete Rollenaktivierung (PIM)	nicht enthalten	enthalten

Die Mischkalkulation aus E3, E5 und F3 ist in Verwaltungen der Normalfall und keineswegs ein Zeichen von Unordnung – sie muss nur bewusst geschnitten sein. Welche Rolle welchen Plan braucht und wie die Behördenkonditionen dabei wirken, behandelt Microsoft 365 Lizenzen für Verwaltungen: E3, E5, F3 und die Behördenkonditionen. Für dieses Regelwerk gilt die praktische Konsequenz: Die Stufen 1 bis 5 laufen vollständig mit P1. Nur die risikobasierte Kür braucht E5 – und zwar nicht flächendeckend, sondern für die Konten, bei denen es sich lohnt.

FAKTEN · Die Pflicht kommt ohnehin

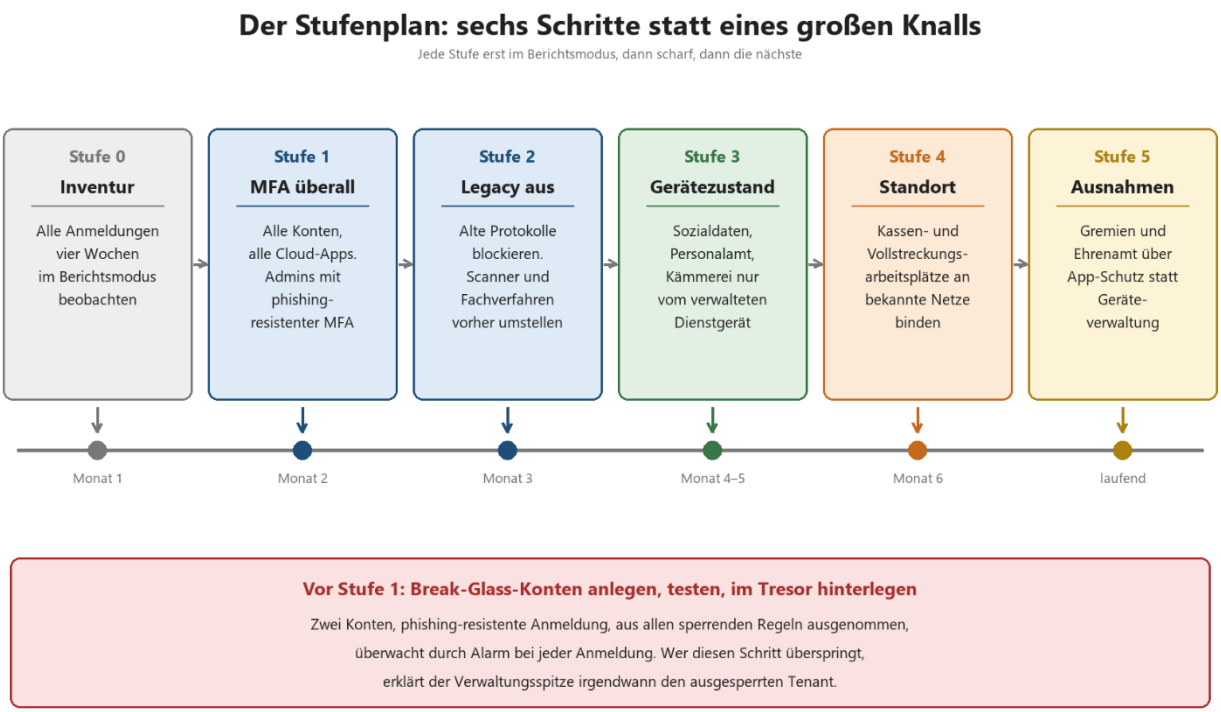
Microsoft erzwingt Mehrfaktor-Anmeldung inzwischen selbst, unabhängig von Ihrem Regelwerk. Seit Oktober 2024 gilt sie für Anmeldungen am Azure-Portal, am Entra-Verwaltungsportal und am Intune-Verwaltungsportal, seit Februar 2025 rollend auch für das Microsoft-365-Verwaltungsportal. Seit dem 1. Oktober 2025 folgt Phase 2: Azure CLI, Azure PowerShell, die Azure-App, Infrastrukturwerkzeuge und REST-Aufrufe an die Azure-Verwaltungsschnittstelle verlangen MFA für alle schreibenden Vorgänge; reine Leseoperationen bleiben ausgenommen.

Zwei Punkte, die in Verwaltungen regelmäßig übersehen werden: Erstens gilt diese Pflicht ausdrücklich auch für Break-Glass-Konten – wer dort nur ein langes Kennwort hinterlegt hat, hat im Ernstfall kein funktionierendes Notfallkonto mehr. Zweitens sind Dienstkonten, die als normale Benutzerkonten für Automatisierung angelegt wurden, voll betroffen; echte Workload-Identitäten dagegen nicht.

Wer mehr Zeit brauchte, konnte den Start pro Tenant verschieben – für Phase 2 bis zum 1. Juli 2026. Diese Fenster sind inzwischen zu. Die Frage lautet also nicht mehr, ob MFA kommt, sondern nur noch, ob Sie sie selbst gestalten oder von der Plattform gestaltet bekommen.

Das Regelwerk in Stufen

Der häufigste Fehler ist nicht die falsche Regel, sondern der falsche Zeitpunkt. Regelwerke, die an einem Freitagnachmittag vollständig scharf geschaltet werden, produzieren am Montag eine Warteschlange im Bürgerbüro und im Verwaltungsvorstand die dauerhafte Überzeugung, dass Sicherheit den Betrieb stört. Deshalb: Stufen, jede einzeln, jede zuerst im Berichtsmodus.



Skizze 2: Sechs Stufen über etwa ein halbes Jahr. Der Zeitplan ist ambitioniert, aber realistisch – vorausgesetzt, Stufe 0 wird nicht übersprungen.

Stufe 0: Vier Wochen zusehen

Jede Regel in Entra lässt sich im Berichtsmodus anlegen. Sie greift dann nicht, protokolliert aber für jede Anmeldung, was sie getan hätte. Das ist der wichtigste Schalter des ganzen Themas, und er kostet nichts außer vier Wochen Geduld.

In diesen vier Wochen finden Sie die Dinge, die in keiner Dokumentation stehen. Das Multifunktionsgerät im dritten Stock, das Scans über ein altes Protokoll verschickt. Das Fachverfahren der Vergabestelle, das nächtlich Berichte mailt – unter dem Konto einer Kollegin, die 2021 in Elternzeit ging und deren Konto seither niemand anzufassen wagte. Die Zeiterfassung, die sich über einen Anmeldeweg meldet, den es offiziell nicht mehr gibt. In einer Stadtverwaltung mit rund 1.000 Rufnummern fanden wir in dieser Phase vierzehn solcher Fälle. Zwölf ließen sich in zwei Wochen umstellen. Zwei brauchten den Hersteller, und einer davon brauchte ihn ein halbes Jahr.

Nebenbei liefert diese Phase das, was später niemand mehr rekonstruieren kann: eine belastbare Aussage darüber, wie viele Anmeldungen die Regel betroffen hätte. Das ist das Argument, mit dem man in den Verwaltungsvorstand geht. „Wir haben es geprüft, es betrifft 23 Konten, hier ist die Liste" schlägt jede Sicherheitsargumentation.

TIPP · Die Inventur, die sich in jedem Fall lohnt

Bevor Sie Regeln bauen, ziehen Sie drei Listen: alle Konten mit Administratorrollen, alle Konten ohne registrierte Anmeldemethode, alle Anmeldungen über alte Protokolle der letzten 30 Tage. Diese drei Listen passen zusammen auf wenige Seiten und beantworten neunzig Prozent der Fragen, die später im Projekt gestellt werden.

Die erste Liste ist erfahrungsgemäß die unangenehmste. In einem Zweckverband ergab sie elf Konten

mit globaler Administratorrolle bei sieben Beschäftigten in der IT – darunter zwei Konten eines Dienstleisters aus einem beendeten Projekt und ein Sammelkonto namens „admin2", dessen Kennwort drei Personen kannten.

Stufe 1: MFA überall – und für Admins etwas Besseres

Die erste scharfe Regel ist die einzige, über die man nicht diskutieren sollte: Mehrfaktor-Anmeldung für alle Benutzerkonten, für alle Cloud-Anwendungen. Nicht für eine Pilotgruppe, nicht für die Verwaltungsspitze, nicht „erst mal für die, die wollen". Für alle. Alles andere ist eine Liste von Konten, die man später sucht.

Für privilegierte Konten reicht die normale MFA allerdings nicht mehr. Ein Anruf oder eine SMS lässt sich abfangen, eine Bestätigungsmeldung lässt sich durch penetrantes Wiederholen erzwingen, und eine Anmeldeseite lässt sich nachbauen. Für alle Konten mit Administratorrollen gehört deshalb eine eigene Regel mit phishing-resistenter Authentifizierungsstärke ins Regelwerk – Sicherheitsschlüssel, Passkey oder zertifikatsbasierte Anmeldung. Das kostet pro Schlüssel etwa so viel wie ein Aktenordner mit Registerblättern und ist die beste Einzelinvestition im ganzen Projekt.

Wie viele Administratorkonten eine Verwaltung wirklich braucht, welche Rollen dauerhaft vergeben werden und welche nur auf Zeit aktiviert werden sollten, behandelt Privilegierte Konten in der Verwaltungs-IT: Rollen, PIM und der Fall des einen Admins. Für Stufe 1 gilt die kurze Fassung: Je weniger dauerhafte Rollen es gibt, desto kleiner ist die Gruppe, die einen Sicherheitsschlüssel braucht – und desto überschaubarer wird die Ausnahmeliste.

Ein Sonderfall, der in föderierten Umgebungen für böse Überraschungen sorgt: Wenn die Anmeldung über einen eigenen Verzeichnisdienst läuft und die MFA dort geleistet wird, muss dieser Dienst die entsprechende Bestätigung auch tatsächlich mitschicken. Tut er das nicht, sieht die Cloud nur eine gewöhnliche Kennwortanmeldung – und die Regel greift, obwohl der zweite Faktor längst geleistet wurde. Das ist einer der Gründe, warum die Föderationsfrage vor dem Regelwerk geklärt gehört.

Diese Weichenstellung ist Thema von ADFS oder Entra ID in der Verwaltung: Die Entscheidung entlang der Fachverfahren. Wenn Sie beides gleichzeitig anfassen – Föderation abbauen und Regelwerk aufbauen –, planen Sie die Reihenfolge sehr bewusst. Zwei bewegliche Teile in derselben Woche sind ein Fehler, den man nur einmal macht.

Stufe 2: Alte Anmeldeverfahren abschalten

Alte Anmeldeverfahren – im Portal firmieren sie als „andere Clients" – sind der Grund, warum MFA allein nicht reicht. Ein Protokoll, das nur Benutzername und Kennwort kennt, kann keinen zweiten Faktor abfragen. Wer diese Wege offen lässt, hat MFA eingeführt und gleichzeitig eine Tür daneben offen gelassen, an der ein Schild hängt: „Hier ohne".

Die Regel selbst ist trivial – zwei Klicks. Die Vorarbeit ist es nicht. Betroffen sind in Verwaltungen typischerweise: Multifunktionsgeräte mit Scan-to-Mail, Fachverfahren mit eigenem Mailversand, Zeiterfassungssysteme, Ratsinformationssysteme älterer Bauart, Alarmierungssysteme der

Feuerwehr, Frankiermaschinen und in einem denkwürdigen Fall ein Getränkeautomat, der Störungsmeldungen per Mail verschickte.

WICHTIG · Die Uhr läuft ohnehin ab

Für den Mailversand über das alte Verfahren hat Microsoft einen festen Fahrplan veröffentlicht: Ab dem 1. März 2026 wird ein wachsender Anteil solcher Übermittlungen abgewiesen, bis Ende April 2026 vollständig. Zum Jahresende 2026 wird das Verfahren für bestehende Tenants standardmäßig abgeschaltet; Administratoren können es dann noch einmal aktiv einschalten. Für Tenants, die nach diesem Zeitpunkt neu entstehen, steht es von vornherein nicht mehr zur Verfügung.

Praktisch heißt das: Die Umstellung Ihrer Multifunktionsgeräte und Fachverfahren findet ohnehin statt. Sie können sie im eigenen Projektplan erledigen oder in einer Störungsmeldung. Der zweite Weg ist erfahrungsgemäß der teurere.

Zwei Auswege haben sich bewährt. Erstens: Geräte und Verfahren, die es können, auf moderne Anmeldung umstellen. Zweitens: Geräte, die es nicht können, gar nicht erst anmelden lassen – Multifunktionsgeräte können in aller Regel über einen internen Weiterleitungsdienst ohne eigene Anmeldung versenden. Der dritte, häufig gewählte Weg ist die dauerhafte Ausnahme für ein Dienstkonto. Er ist zulässig, er ist manchmal unvermeidlich, aber er gehört befristet, dokumentiert und in einer Gruppe, deren Name erklärt, warum es sie gibt.

Stufe 3: Gerätezustand für Sozialdaten

Ab hier wird das Regelwerk verwaltungsspezifisch. Die Anforderung lautet: Auf Daten mit erhöhtem Schutzbedarf kommt man nur von einem Gerät, das die Verwaltung kennt und verwaltet. In der Praxis betrifft das Jugendamt, Sozialamt, Gesundheitsamt, Personalamt, die Kämmerei und – je nach Zuschnitt – Teile des Ordnungsamts und der Rechtsabteilung.

Die Regel verlangt ein konformes oder verzeichnisgebundenes Gerät. Sie ist unbequem, weil sie hart ist: Ohne Diensthardware kein Zugriff. Genau das ist ihr Zweck. Ein Sozialbericht hat auf einem privaten Laptop mit unbekanntem Verschlüsselungsstatus nichts verloren, und diese Aussage lässt sich gegenüber Personalrat, Datenschutzbeauftragten und Kommunalaufsicht gleichermaßen begründen.

In einer Stadtverwaltung, die den Sozialbereich mit SharePoint abbildet, haben wir diese Regel bewusst nicht auf ganze Fachämter gelegt, sondern auf die Anwendungen und Gruppen, die die betreffenden Bereiche nutzen. Der Unterschied klingt akademisch, ist aber betrieblich erheblich: Eine Kollegin, die für zwei Wochen in der Poststelle aushilft, verliert dadurch nicht ihren gesamten Zugang, sondern nur den zu dem Bereich, für den die Regel gilt. Regeln, die an Aufgaben hängen statt an Organigrammen, überleben Umorganisationen. Und Umorganisationen gibt es in Verwaltungen häufiger als Regelwerksrevisionen.

Welcher Bereich welchen Schutzbedarf hat, ist keine Frage des Bauchgefühls, sondern das Ergebnis einer Schutzbedarfsfeststellung. Wie sich diese mit den Bausteinen des IT-Grundschutzes gegen die Microsoft-365-Wirklichkeit abgleichen lässt, steht in Schutzbedarf und Microsoft 365: IT-Grundschutz-Abgleich für die Praxis. Die dortige Einstufung ist die Begründung für die Regeln dieser Stufe – und das Dokument, nach dem das Rechnungsprüfungsamt fragen wird.

WARNUNG · Konform ist nicht gleich sicher

„Gerät ist konform" bedeutet exakt: Das Gerät erfüllt die Bedingungen, die Sie selbst in Ihrer Geräterichtlinie definiert haben. Wenn diese Richtlinie nur prüft, ob ein Gerät registriert ist, dann bestätigt das Signal genau das – und sonst nichts.

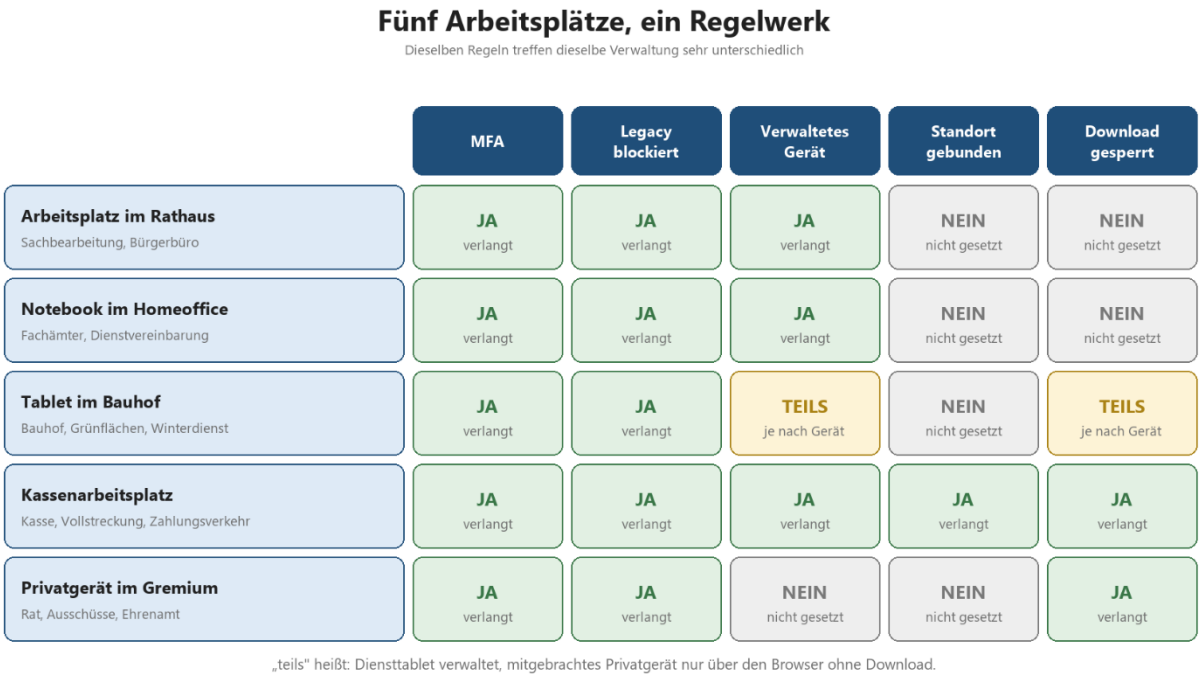
Prüfen Sie deshalb, was Ihre Konformitätsrichtlinie tatsächlich verlangt: Festplattenverschlüsselung, aktueller Patchstand, aktiver Virenschutz, gesperrter Bildschirm nach kurzer Zeit, keine Freischaltung der Administratorrechte für Anwendende. Ein Regelwerk, das ein nichtssagendes Signal abfragt, erzeugt Prüfsicherheit ohne Schutzwirkung. Das ist der unangenehmste aller Zustände: Es sieht in der Beschlussvorlage gut aus und hält im Ernstfall nichts.

Stufe 4: Standortregeln für Kassenarbeitsplätze

Standort ist ein schwaches Signal, und man sollte es genau deshalb sehr sparsam einsetzen. Die Cloud erkennt den Standort über die öffentliche IP-Adresse oder – wenn man es ausdrücklich einschaltet – über die Ortung der Authentifizierungs-App. Beides ist manipulierbar. Ein Angreifer mit gültigen Zugangsdaten und einem Zugang über einen deutschen Anbieter sieht aus wie ein Kollege im Homeoffice.

Für einen Bereich lohnt es sich trotzdem: die Kasse. Zahlungsverkehr, Vollstreckung, Anordnungsbefugnis. Hier ist der Schaden bei Missbrauch unmittelbar finanziell, hier ist der Personenkreis klein, hier sind die Arbeitsplätze fest. Eine Regel, die den Zugriff auf die Kassenanwendungen auf die bekannten Netze der Verwaltung beschränkt, ist verhältnismäßig, erklärbar und im Zweifel auch gegenüber der Rechnungsprüfung leicht zu begründen. Sie ersetzt keine Vier-Augen-Freigabe im Verfahren selbst – aber sie schließt den Fall aus, dass jemand mit erbeuteten Zugangsdaten aus dem Ausland eine Anordnung anfasst.

Zwei Fallstricke aus der Praxis. Erstens: Der Adressbereich Ihres Internetzugangs ändert sich – bei Anbieterwechsel, bei Umstellung auf einen anderen Netzübergang, bei Notfallumschaltung auf eine Ersatzleitung. Wenn niemand die benannten Standorte nachzieht, sperrt sich die Kasse am Monatsende selbst aus. Hinterlegen Sie die Pflege dieser Liste dort, wo auch die Netzänderungen verantwortet werden. Zweitens: Ländersperren wirken nur, wenn sie als Erlaubnisliste gebaut sind. Eine Sperrliste einzelner Länder ist Symbolpolitik – die Umleitung über ein erlaubtes Land ist keine Hürde, sondern ein Häkchen in einer Software.



Skizze 3: Dieselben fünf Regeln, fünf sehr verschiedene Arbeitsplätze. Wer diese Matrix nicht vorab füllt, füllt sie später im Störungsbetrieb.

Stufe 5: Gremienmitglieder mit Privatgeräten

Und nun zum Fall, an dem sich entscheidet, ob Ihr Regelwerk Bestand hat. Ein Ratsmitglied hat ein privates Tablet. Es wird dieses Gerät nicht in die Geräteverwaltung geben, und es hat dafür gute Gründe: Auf dem Gerät sind private Fotos, private Mails und möglicherweise die Kommunikation aus einer politischen Funktion, die die Verwaltung nichts angeht. Die Forderung „verwaltetes Gerät oder kein Zugriff" ist hier keine Lösung, sondern eine Konfliktankündigung.

Die tragfähige Antwort besteht aus drei Teilen. Erstens: MFA gilt auch hier, ohne Ausnahme – wer Sitzungsunterlagen mit nichtöffentlichen Inhalten liest, meldet sich mit zweitem Faktor an. Das ist niemandem zu viel zugemutet und lässt sich in einer Fraktionssitzung in zehn Minuten erklären. Zweitens: Statt Gerätezustand tritt Anwendungsschutz. In den mobilen Apps von Microsoft 365 lässt sich erzwingen, dass Verwaltungsdaten nur innerhalb der geschützten Apps bleiben, dass eine PIN abgefragt wird, dass kein Kopieren in private Apps möglich ist und dass sich die Daten aus der Ferne löschen lassen, ohne das private Gerät anzufassen. Drittens: Am Rechner läuft der Zugriff über den Browser, mit einer Sitzungsregel, die das Herunterladen unterbindet. Gelesen wird online, gespeichert wird nichts.

Diese Konstruktion ist kein Kompromiss aus Bequemlichkeit, sondern die verhältnismäßige Lösung: Sie schützt die Daten, ohne in das Privatgerät einzugreifen. Genau diese Begründung braucht man später gegenüber dem Datenschutz – und gegenüber dem Ratsmitglied, das wissen will, was die Verwaltung auf seinem Tablet sehen kann. Die Antwort lautet: die Verwaltungsdaten in den geschützten Apps, sonst nichts. Diese Antwort sollte schriftlich vorliegen, bevor die Frage gestellt wird.

Wie Gremienmitglieder, Planungsbüros und freie Träger technisch sauber eingebunden werden – als Gäste, als eigene Konten oder über einen getrennten Bereich –, behandelt Gäste in Teams und SharePoint: Planungsbüros, Träger und Gremienmitglieder sicher einbinden. Die dortige

Entscheidung bestimmt, an welcher Stelle Ihre Regeln aus Stufe 5 überhaupt greifen können: Bei Gastkonten aus fremden Tenants gelten teilweise andere Bedingungen als bei eigenen Konten.

Das Regelwerk auf einer Seite

Die folgende Tabelle ist der Kern dieses Beitrags. Sie ist bewusst so gebaut, dass sie in eine Beschlussvorlage passt: eine Regel je Zeile, mit Zielgruppe, zulässiger Ausnahme und dem Risiko, das die Regel selbst erzeugt. Diese vierte Spalte ist die wichtigste. Jede Sicherheitsregel bringt ein neues Risiko mit, und wer das nicht aufschreibt, wird beim ersten Vorfall gefragt, warum niemand daran gedacht hat.

Regel	Zielgruppe	Zulässige Ausnahme	Risiko der Regel
1 · MFA für alle Cloud-Anwendungen	Alle Benutzerkonten, auch Gäste und Gremien	Ausschließlich die beiden Break-Glass-Konten	Beschäftigte ohne Diensthandy brauchen ein Alternativverfahren, sonst entsteht eine Schatten-Ausnahmeliste
2 · Phishing-resistente Anmeldung	Alle Konten mit Administratorrollen, Zugang zu Kassenverfahren	Keine; Break-Glass nutzt Sicherheitsschlüssel	Verlorener Schlüssel sperrt aus – Ersatzschlüssel gehört in den Tresor, nicht in die Schreibtischschublade
3 · Alte Anmeldeverfahren blockieren	Alle Konten	Befristet einzelne Dienstkonten für Geräte, die noch nicht umgestellt sind	Scan-to-Mail, Fachverfahrensmails und Alarmierung fallen ohne Vorarbeit sofort aus
4 · Verwaltetes und konformes Gerät	Jugend-, Sozial-, Gesundheits-, Personalamt, Kämmerei	Keine; stattdessen Diensthardware bereitstellen	Externe Prüfer, Dolmetscher und kurzfristige Vertretungen stehen ohne Gerät vor der Tür
5 · Zugriff nur aus bekannten Netzen	Kasse, Vollstreckung, Zahlungsverkehr	Notfallfreigabe für 24 Stunden, gezeichnet von Kämmerei und IT-Leitung	Adresswechsel beim Anbieter oder Umschalten auf Ersatzleitung sperrt die Kasse am Monatsende aus
6 · Anwendungsschutz statt Geräteverwaltung	Gremienmitglieder, Ehrenamt, mitgebrachte Geräte im Außendienst	Lesender Zugriff über den Browser ohne Herunterladen	Kein Signal über den Gerätezustand; gegen Abfotografieren des Bildschirms hilft keine Regel
7 · Sitzung ohne Herunterladen	Alle Zugriffe von nicht verwalteten Geräten	Einzelne freigegebene Anwendungen, etwa das Ratsinformationssystem	Beschäftigte weichen auf Umwege aus, wenn kein praktikabler Arbeitsweg angeboten wird
8 · Anmeldehäufigkeit begrenzen	Bürgerbüro-Poolrechner, Schichtarbeitsplätze, Kasse	Leitstelle und Rufbereitschaft mit längerem Intervall	Zu kurz gesetzt entsteht ein Anmeldemarathon – und die Bereitschaft, Kennwörter aufzuschreiben
9 · Anmeldung aus unbekannten Ländern blockieren	Alle Konten, als Erlaubnisliste gebaut	Dienstreisen und Partnerschaftsbesuche, vorab befristet freigegeben	Vergessene Dienstreise erzeugt einen Anruf beim Bürgermeister statt beim Servicedesk
10 · Risikobasierte Prüfung	Nur Konten mit E5, vorrangig Leitungsebene	Fachverfahrenskonten mit maschinellem	Fehlalarme treffen nachts; ohne erreichbare

	und Administration	Anmeldemuster	Rufbereitschaft steht der Betrieb bis zum Morgen

WARNUNG · Break-Glass-Konten: Das Kapitel, das niemand überspringen darf

Ein Regelwerk kann sich selbst aussperren. Das ist kein theoretisches Risiko, sondern der häufigste ernsthafte Zwischenfall bei der Einführung: Eine Regel greift weiter als gedacht, trifft auch die Administration, und niemand kommt mehr in den Tenant, um sie zurückzunehmen. Der Weg über den Herstellersupport dauert Stunden bis Tage. In dieser Zeit steht Ihr Regelwerk – und damit Ihre Verwaltung.

Deshalb gilt vor der ersten scharfen Regel: Legen Sie zwei Notfallkonten an. Nicht eines, denn eines kann verloren gehen. Nicht drei oder mehr, denn jedes weitere ist ein zusätzliches Ziel. Diese Konten sind reine Cloud-Konten ohne Bezug zu einer Person, ohne Postfach, ohne Verzeichnissynchronisierung, mit dauerhafter globaler Administratorrolle.

Die Anmeldung: Ein langes Kennwort reicht nicht mehr. Microsoft verlangt inzwischen auch für Notfallkonten eine Mehrfaktor-Anmeldung an den Verwaltungsportalen und empfiehlt ausdrücklich Passkey beziehungsweise Sicherheitsschlüssel oder zertifikatsbasierte Anmeldung. Zwei Sicherheitsschlüssel, versiegelt, an zwei getrennten Orten – beispielsweise im Tresor der Kämmerei und in einem zweiten verschlossenen Behältnis mit dokumentiertem Zugriffsverfahren.

Die Ausnahme: Diese Konten werden aus allen sperrenden Regeln ausgenommen. Aus allen. Eine Regel, die während eines Vorfalls das Notfallkonto blockiert, ist genau der Fall, für den das Konto existiert.

Die Gegenkontrolle: Jede Anmeldung eines Break-Glass-Kontos löst einen Alarm aus, der bei mindestens zwei Personen ankommt – IT-Leitung und eine unabhängige Stelle. Und alle sechs Monate wird die Anmeldung getestet, protokolliert und das Protokoll aufbewahrt. Ungetestete Notfallkonten sind Dekoration.

Ob dieses Verfahren im Ernstfall wirklich trägt, stellt sich nicht in der Dokumentation heraus, sondern in der Übung. Ein Ablauf dafür – Tenant übernommen, SharePoint verschlüsselt, Bürgertelefon tot – steht in Notfallübung für die Verwaltungs-IT: SharePoint verschlüsselt, Admin-Konto übernommen, Bürgertelefon tot. Die Frage „Wer holt den Schlüssel aus dem Tresor, wenn die Kämmerei geschlossen ist und der Kämmerer im Urlaub?" beantwortet man besser an einem Übungstermin als an einem Sonntagabend.

Ausnahmen, Beteiligung und die Frage, wer eigentlich entscheidet

Jede Ausnahme bekommt ein Verfallsdatum

Ausnahmen sind nicht das Problem. Ausnahmen ohne Gedächtnis sind das Problem. In jedem Tenant, den wir uns nach ein paar Betriebsjahren ansehen, gibt es mindestens eine Gruppe mit einem Namen wie „CA-Ausnahme-temp", in der Konten liegen, die niemand mehr zuordnen kann. Die Kollegin, für die sie angelegt wurde, ist längst in einem anderen Amt. Die Regel, von der sie ausnimmt, ist inzwischen die wichtigste im ganzen Werk.

Behandeln Sie Ausnahmen deshalb wie Verwaltungsvorgänge, denn genau das sind sie. Schriftlicher Antrag aus dem Fachamt mit Begründung und Befristung. Mitzeichnung durch IT-Leitung und die datenschutzbeauftragte Person. Eine eigene Gruppe je Ausnahmegrund, nie eine Sammelgruppe. Ein sprechender Name, der auch in zwei Jahren noch erklärt, worum es ging. Ein Ablaufdatum, das technisch hinterlegt ist – Entra kann Mitgliedschaften in Gruppen automatisch auslaufen lassen, und diese Funktion ist die zuverlässigste Wiedervorlage, die Sie bekommen können. Und ein Verzeichnis, das jederzeit vorzeigbar ist.

Skizze 4: Eine Ausnahme ist ein Vorgang mit Anfang und Ende. Ohne die Wiedervorlage nach 90 Tagen wird aus der Ausnahme eine stille Regeländerung.

Personalrat und Dienstvereinbarung

Conditional Access erzeugt Protokolldaten über das Anmeldeverhalten von Beschäftigten: wann, von wo, mit welchem Gerät, mit welchem Ergebnis. Ob und in welchem Umfang das der Mitbestimmung unterliegt, hängt vom jeweiligen Landespersonalvertretungsrecht ab – und im kirchlichen Bereich von der Mitarbeitervertretungsordnung. Die Regelungen unterscheiden sich zwischen den Ländern erheblich; das ist eine Frage für die Rechtsabteilung und gegebenenfalls für externe rechtliche Beratung, nicht für die IT-Leitung und nicht für diesen Beitrag.

Was sich unabhängig davon sagen lässt: Der Personalrat gehört früh in dieses Thema, und zwar nicht als Empfängerkreis einer fertigen Konfiguration. Die Regeln aus Stufe 3 und Stufe 5 greifen unmittelbar in die Arbeitsbedingungen ein – wer nur vom Diensttablet auf Sozialdaten kommt, arbeitet anders als vorher. Umgekehrt ist die Personalvertretung oft ein guter Verbündeter, wenn es darum geht, den Anwendungsschutz auf Privatgeräten als das darzustellen, was er ist: eine Grenze, die auch die Beschäftigten schützt.

Der wichtigste Satz für die Beteiligung lautet: Diese Auswertungen dienen der Sicherheit, nicht der Leistungs- und Verhaltenskontrolle. Wer diesen Satz in eine Dienstvereinbarung schreibt, muss

ihn auch technisch halten – also festlegen, wer die Anmeldeprotokolle einsehen darf, zu welchem Anlass, mit welcher Aufbewahrungsdauer und unter welcher Gegenkontrolle. Ein Vier-Augen-Prinzip für personenbezogene Auswertungen kostet nichts und nimmt der Debatte die Schärfe.

Bausteine für eine solche Vereinbarung – Zweckbindung, Auswertungsverbot, Beteiligungsverfahren, Revisionsklausel – finden Sie in Copilot und Personalrat: Bausteine einer Dienstvereinbarung. Die dortige Systematik lässt sich weitgehend auf Anmeldeprotokolle übertragen; die Datenarten sind andere, die Konfliktlinien dieselben. In Einrichtungen unter kirchlicher Trägerschaft kommen zusätzlich die Besonderheiten aus Microsoft 365 in Kirche, Diakonie und Caritas: DSG-EKD, KDG und Mitarbeitervertretung hinzu.

Wer entscheidet was

Die unangenehmste Frage im Projekt ist selten technisch. Sie lautet: Wer darf eine Regel ändern? Die ehrliche Antwort in vielen Verwaltungen lautet derzeit: derjenige, der gerade die Berechtigung dafür hat und angerufen wurde. Das ist auf Dauer nicht haltbar, weil eine Regeländerung eine Entscheidung über den Zugang zu geschützten Daten ist – und die trifft nicht der Dienst habende Administrator, sondern die Organisation.

Bewährt hat sich eine schlichte Dreiteilung. Das Regelwerk selbst – welche Regeln es gibt und wen sie treffen – wird von der Verwaltungsleitung beschlossen, auf Vorschlag der IT-Leitung und mit Beteiligung von Datenschutz und Personalvertretung. Änderungen am Regelwerk laufen über ein Änderungsverfahren mit Mitzeichnung. Die technische Umsetzung liegt bei der IT beziehungsweise beim Betriebsdienstleister – und dort ausschließlich als Umsetzung, nicht als Entscheidung.

Wenn der Betrieb ganz oder teilweise bei einem kommunalen Rechenzentrum oder einem Systemhaus liegt, muss diese Grenze in der Leistungsbeschreibung stehen, sonst wird sie im Alltag verwischt. Welche Rollen sich dafür sauber schneiden lassen, behandelt Microsoft 365 und das kommunale Rechenzentrum: Rollen, Schnittstellen, Zweitmeinung. Beide Seiten profitieren von Klarheit: Der Dienstleister will nicht die Verantwortung für eine Zugangsentscheidung tragen, und die Verwaltung will sie nicht abgeben.

Einführen, ohne das Bürgerbüro anzuhalten

Reihenfolge, Pilot, Rückfallweg

Die Einführung folgt immer demselben Muster, und zwar für jede einzelne Stufe: Regel im Berichtsmodus anlegen, mindestens zwei Wochen beobachten, Auswertung lesen, Ausnahmen klären, Pilotgruppe scharf schalten, eine Woche warten, dann in Wellen ausrollen. Als Pilotgruppe eignet sich die IT selbst am wenigsten – sie ist zu geübt und findet die Fehler nicht, die alle anderen finden. Nehmen Sie ein Fachamt mit gemischter Technikaffinität und guter Gesprächskultur. Das Bauamt ist erfahrungsgemäß eine gute Wahl, das Bürgerbüro die schlechteste – dort ist die Fehlertoleranz null, weil vor dem Schalter jemand wartet.

Zu jeder scharf geschalteten Stufe gehört ein dokumentierter Rückfallweg: Wer darf die Regel wieder in den Berichtsmodus setzen, unter welchen Voraussetzungen, mit welcher Meldung an wen. Das klingt banal, ist aber der Unterschied zwischen einer kontrollierten Rücknahme und einer hektischen Nacht. Und es gehört in die Betriebsdokumentation, nicht in den Kopf einer Person.

TIPP · Der Satz, der die meisten Anrufe verhindert

Kommunizieren Sie vor jeder Stufe genau drei Dinge, in genau dieser Reihenfolge: Was ändert sich für mich konkret? Ab wann? Wen rufe ich an, wenn es nicht funktioniert?

Nicht kommunizieren sollten Sie: die Bezeichnung der Regel, die Technik dahinter und die Zahl der betroffenen Konten. Diese Angaben interessieren im Fachamt niemanden und erzeugen nur das Gefühl, es handele sich um ein IT-Projekt statt um eine Verwaltungsentscheidung.

Praktisch bewährt: eine halbe Seite je Stufe, in der Sprache des Hauses, freigegeben vom Organisationsamt. Dazu ein Kurzformat für die Beschäftigten – zehn Minuten Registrierung der Anmeldemethode, gemeinsam, im Sitzungsraum, mit jemandem daneben. Wie sich solche Formate für Verwaltungen zuschneiden lassen, zeigt die Microsoft-365-Schulung für Verwaltungen. Der Aufwand ist gering, die Wirkung auf das Beschwerdeaufkommen erheblich.

Was das Rechnungsprüfungsamt sehen will

Irgendwann kommt die Prüfung, und sie kommt mit Fragen, die auf den ersten Blick unbequem allgemein klingen: „Ist der Zugang zu schutzbedürftigen Daten angemessen abgesichert?" Die Antwort darauf ist kein Screenshot aus einem Verwaltungsportal, sondern eine kleine Sammlung von Nachweisen. Wenn Sie diese Sammlung während der Einführung anlegen, kostet sie fast nichts. Wenn Sie sie hinterher rekonstruieren müssen, kostet sie eine Arbeitswoche.

Frage der Prüfung	Nachweis	Woher
Nach welchen Regeln wird der Zugang gesteuert?	Beschlossenes Regelwerk mit Datum, Fassung und Mitzeichnung	Aktenplan, Vorgang der IT-Leitung
Sind die Regeln wirksam?	Auswertung der Anmeldeprotokolle mit angewandten Regeln je Anmeldung	Anmeldeprotokolle im Entra-Portal, Export
Welche Ausnahmen bestehen?	Ausnahmeverzeichnis mit Begründung, Befristung und Mitzeichnung	Eigene Vorgangsakte, halbjährlich fortgeschrieben
Wer darf Regeln ändern?	Rollenkonzept und Änderungsverfahren	Betriebsdokumentation, Leistungsbeschreibung des Dienstleisters
Sind Notfallzugänge geregelt?	Verfahrensbeschreibung und Protokoll des letzten Tests	Notfallhandbuch, Tresorprotokoll
Werden Änderungen nachvollziehbar protokolliert?	Auszug aus dem Überwachungsprotokoll für Regeländerungen	Einheitliches Überwachungsprotokoll des Tenants

Welche Protokolle Microsoft 365 überhaupt führt, wie lange sie vorgehalten werden und was das für Prüfungsanfragen bedeutet, steht in Microsoft 365 Audit-Log und Rechnungsprüfung: Nachweise, die Verwaltungen liefern müssen. Ein Hinweis vorweg, weil er regelmäßig für Ärger sorgt: Die Vorhaltedauer der Protokolle hängt vom Plan ab. Wer im Nachhinein einen zwei Jahre zurückliegenden Vorgang belegen soll, aber nur die Standardvorhaltung hat, kann diesen Nachweis nicht führen – unabhängig davon, wie gut das Regelwerk war.

Der Sonderfall Delos Cloud

In Gesprächen mit Kommunen kommt regelmäßig die Frage, ob sich all das erübrigt, wenn man auf die für die deutsche Verwaltung vorgesehene souveräne Cloud-Umgebung setzt. Die nüchterne Antwort: Die Identitäts- und Zugangssteuerung ist konzeptionell dieselbe. Ein Regelwerk, das Sie heute entwerfen – MFA für alle, alte Verfahren abgeschaltet, Gerätezustand für schutzbedürftige Bereiche, Ausnahmen mit Befristung –, ist keine verlorene Arbeit. Es ist die Ordnungsleistung, die Sie in jeder Umgebung brauchen, und der schwierige Teil daran ist ohnehin nicht die Technik, sondern die Abstimmung im Haus.

Was das Angebot inhaltlich umfasst, welche Dienste zu welchem Zeitpunkt verfügbar sind und wo derzeit Lücken bestehen, behandelt Delos Cloud für Kommunen: Was das Angebot ist, wen es betrifft und was fehlt. Was hier nicht steht, ist ein Terminversprechen – aus gutem Grund. Planungen dieser Größenordnung verschieben sich, und ein Regelwerk, das auf einen Termin wartet, schützt in der Zwischenzeit niemanden.

Häufige Fragen

Brauchen wir für ein sinnvolles Regelwerk Microsoft 365 E5?

Nein. Die Stufen 1 bis 5 dieses Beitrags laufen vollständig mit Entra ID P1, das in E3, F3 und F1 enthalten ist. E5 beziehungsweise Entra ID P2 brauchen Sie für risikobasierte Regeln und für die zeitlich befristete Aktivierung von Administratorrollen. Beides ist wertvoll, beides ist aber ein Aufbau auf einem Fundament, das erst einmal stehen muss. Verwaltungen, die zuerst E5 beschaffen und danach über das Regelwerk nachdenken, haben in der Regel Geld ausgegeben, ohne Sicherheit zu gewinnen.

Was passiert, wenn die Anmeldung beim Anbieter gestört ist?

Dann kommt niemand hinein, auch nicht ins Bürgerbüro – und zwar unabhängig von Ihrem Regelwerk, weil die Anmeldung ohnehin über den Anbieterdienst läuft. Genau deshalb gehört dieser Fall in die Notfallplanung und nicht in die Diskussion über Regeln. Die relevanten Vorkehrungen sind: ein Verfahren für den Papierbetrieb an den Schaltern für einige Stunden, klare Kommunikationswege zu den Fachämtern und die Kenntnis darüber, welche Fachverfahren lokal weiterlaufen. Break-Glass-Konten helfen bei einer Störung des Anmeldedienstes ausdrücklich nicht – sie helfen gegen ein Regelwerk, das sich selbst ausgesperrt hat.

Dürfen Ratsmitglieder wirklich mit Privatgeräten auf Vorlagen zugreifen?

Technisch ist es lösbar, wie in Stufe 5 beschrieben. Ob es zulässig ist, hängt von der Einstufung der Unterlagen, von der Geschäftsordnung des jeweiligen Gremiums und von landesrechtlichen Vorgaben ab, die sich zwischen den Ländern unterscheiden. Das ist eine Frage für die Rechtsabteilung und die datenschutzbeauftragte Person, nicht für die IT-Leitung allein. Was die IT liefern kann und sollte, ist eine belastbare Beschreibung der technischen Schutzmaßnahmen – auf dieser Grundlage lässt sich die rechtliche Bewertung überhaupt erst treffen.

Wie viele Regeln sind normal?

In einer mittleren Kommunalverwaltung landen wir typischerweise bei zwölf bis achtzehn Regeln. Weniger als acht bedeutet meist, dass die Fallunterscheidungen fehlen und einzelne Bereiche unnötig hart oder unnötig lasch behandelt werden. Mehr als fünfundzwanzig bedeutet fast immer, dass historisch gewachsene Sonderfälle nie zusammengeführt wurden. Die aussagekräftigere Kennzahl ist ohnehin nicht die Zahl der Regeln, sondern die Zahl der Ausnahmen. Wenn diese nicht auf eine Seite passt, hat das Regelwerk seine Schutzwirkung verloren.

Können wir Ländersperren einsetzen?

Ja, und in Verwaltungen ist das häufig verhältnismäßig, weil Dienstreisen selten und planbar sind. Wichtig ist die Bauweise: als Erlaubnisliste weniger Länder, nicht als Sperrliste einzelner Herkunftsländer. Eine Sperrliste umgeht man mit einem Häkchen in einer beliebigen Umleitungssoftware. Ergänzen Sie ein einfaches Verfahren für Dienstreisen und Partnerschaftsbesuche: befristete Aufnahme in eine Ausnahmegruppe, beantragt über das Fachamt, automatisch auslaufend. Ohne dieses Verfahren erzeugt die Regel genau einen Vorgang – einen Anruf aus dem Ausland, meist an einem Feiertag.

Was machen wir mit Multifunktionsgeräten, die Scans versenden?

Am besten gar nicht anmelden lassen. Die meisten Geräte können über einen internen Weiterleitungsdienst versenden, der die Anmeldung übernimmt; das Gerät selbst braucht dann keine Zugangsdaten. Wo das nicht geht, hilft ein Dienstkonto mit sehr eng gezogenen Berechtigungen und einer befristeten, dokumentierten Ausnahme. Und in beiden Fällen gilt der Fahrplan des Anbieters: Der Mailversand über das alte Verfahren wird ab März 2026 schrittweise abgewiesen und Ende 2026 für bestehende Tenants standardmäßig abgeschaltet. Wer die Geräte jetzt umstellt, macht es einmal statt zweimal.

Muss der Personalrat zustimmen?

Das richtet sich nach dem Personalvertretungsrecht des jeweiligen Landes beziehungsweise nach der einschlägigen Mitarbeitervertretungsordnung im kirchlichen Bereich, und die Regelungen unterscheiden sich erheblich. Die Einordnung nimmt die Rechtsabteilung vor. Unabhängig von der formalen Antwort ist die praktische Empfehlung eindeutig: früh beteiligen, den Zweck der Protokollierung schriftlich begrenzen und das Auswertungsverfahren festlegen. Projekte, die diesen Schritt überspringen, verlieren später mehr Zeit, als die Beteiligung je gekostet hätte.

Wie lange dauert die Einführung realistisch?

Für eine Verwaltung mit 500 bis 1.500 Konten sind sechs Monate von der ersten Inventur bis zum vollständig scharf geschalteten Regelwerk ein realistischer, aber sportlicher Zeitplan. Der zeitkritische Pfad verläuft dabei fast nie über die Technik. Er verläuft über die Umstellung der Geräte und Fachverfahren in Stufe 2 und über die Bereitstellung von Diensthardware in Stufe 3. Wenn dafür eine Beschaffung nötig ist, addieren Sie die Vergabefristen – und zwar ehrlich, nicht optimistisch.

FAKTEN · Fünf Zahlen für die Beschlussvorlage

Sechs Stufen, ein halbes Jahr, zwei Break-Glass-Konten, ein Ausnahmeverzeichnis auf einer Seite – und mindestens vier Wochen Berichtsmodus vor der ersten scharfen Regel.

Wenn eine dieser Zahlen aus dem Projektplan verschwindet, verschwindet meist die vierte zuerst. Das ist die, die man am Ende am meisten vermisst.

Fazit

Conditional Access ist die wirksamste einzelne Maßnahme, die eine Verwaltung im Microsoft-365-Umfeld ergreifen kann, und gleichzeitig diejenige, die am wenigsten mit Technik zu tun hat. Die Regeln sind in einer Woche gebaut. Die Entscheidungen dahinter – welcher Bereich welchen Schutz braucht, welche Ausnahme wer verantwortet, wie Gremienmitglieder eingebunden werden – brauchen Monate, weil sie durch Fachämter, Personalrat, Datenschutz und Verwaltungsspitze müssen.

Deshalb der Rat, der sich in Projekten immer wieder bestätigt hat: Fangen Sie mit den Stufen an, die nicht verhandelbar sind. MFA für alle und das Abschalten alter Anmeldeverfahren sind keine Abwägungsfragen, sie sind Hausaufgaben – und die Plattform erzwingt sie ohnehin schrittweise. Diese beiden Stufen schließen die Tür, durch die praktisch alle bekannten Angriffe auf Kommunen gegangen sind. Alles, was danach kommt, ist Feinschliff und braucht Beteiligung.

Und behalten Sie die Ausnahmen im Blick. Nicht die Regeln entscheiden über die Sicherheit eines Tenants, sondern die Liste derer, für die sie nicht gelten. Diese Liste wächst leise, sie wächst immer freitagnachmittags, und sie wächst mit den besten Absichten. Ein Regelwerk, dessen Ausnahmen halbjährlich vorgelegt und gezeichnet werden, ist nach drei Jahren noch wirksam. Eines ohne dieses Verfahren ist nach drei Jahren ein Dokument, das gut aussieht.

Wenn Sie das Regelwerk mit einer neutralen Zweitmeinung gegenprüfen lassen möchten – vor der Beschlussvorlage oder vor der nächsten Prüfung –, ist das ein überschaubarer Termin: Die Microsoft-365-Beratung für Verwaltungen geht die Stufen mit Ihnen durch, einschließlich der Ausnahmeliste und der Frage, welche Nachweise das Rechnungsprüfungsamt tatsächlich sehen will.

TIPP · Weiter in dieser Reihe

› Privilegierte Konten in der Verwaltungs-IT: Rollen, PIM und der Fall des einen Admins – wie viele Administratorkonten eine Verwaltung wirklich braucht.

› Microsoft 365 Lizenzen für Verwaltungen: E3, E5, F3 und die Behördenkonditionen – welcher Plan welche Regel überhaupt zulässt.

› Schutzbedarf und Microsoft 365: IT-Grundschutz-Abgleich für die Praxis – die Begründung für die Regeln aus Stufe 3.

› Notfallübung für die Verwaltungs-IT: SharePoint verschlüsselt, Admin-Konto übernommen, Bürgertelefon tot – der Test, ob die Break-Glass-Konten wirklich funktionieren.

› Microsoft 365 in der Kommune: Was Sie wirklich entscheiden müssen (und was nicht) – die Einordnung, wenn das Vorhaben insgesamt noch am Anfang steht.