Conditional Access und MFA in Kirche und Diakonie: Ein Regelwerk für Pfarrbüro, Pflegedienst, Verwaltung und Ehrenamt

Es gibt in jedem Microsoft-365-Projekt bei einem kirchlichen Träger diesen einen Termin, in dem die Stimmung kippt. Bis dahin läuft alles rund: Teams begeistert, SharePoint ordnet das Chaos der Laufwerke, die Geschäftsführung nickt zufrieden. Dann sagt jemand das Wort „Mehrfaktor-Anmeldung“, und ab diesem Moment reden alle gleichzeitig. Die Verwaltungsleitung will Sicherheit. Die MAV will wissen, wer da eigentlich was protokolliert. Die Pfarrsekretärin fragt, ob sie jetzt ihr privates Handy hergeben soll. Und irgendwo hinten sagt der Küster leise, er habe gar kein Handy.

Das Unangenehme daran: Alle haben recht. Conditional Access und MFA sind bei einem kirchlichen Träger nämlich keine reine Technikentscheidung. Sie berühren Datenschutzrecht, das bei euch nicht DSGVO heißt. Sie berühren Mitbestimmung, die bei euch nicht über einen Personalrat läuft. Und sie berühren Menschen, die für ihren Dienst kein Firmengerät bekommen und trotzdem an die Gemeindedaten müssen. Wer das mit einer einzigen Richtlinie „MFA für alle“ erschlagen will, hat nach vierzehn Tagen entweder dreißig Ausnahmen im Tenant oder dreißig Kündigungsgespräche im Kalender.

Dieser Beitrag baut dir deshalb kein Sammelsurium aus Einzelfällen, sondern ein Regelwerk: einen überschaubaren Satz an Conditional-Access-Richtlinien, der vier sehr verschiedene Nutzergruppen abdeckt, MFA-Methoden verwendet, die im echten Leben funktionieren, und Ausnahmen so dokumentiert, dass du sie der Aufsicht auf den Tisch legen kannst, ohne rot zu werden. Evangelische wie katholische Seite, Verwaltung wie Einrichtung, Hauptamt wie Ehrenamt.

Dieser Beitrag gehört zur Serie Microsoft 365 in Kirche, Diakonie und Caritas. Dort findest du die Gesamtsicht auf Tenant, Datenschutz, Lizenzierung und Betrieb; hier geht es um die Zugriffsschicht, also um die Frage, wer unter welchen Bedingungen überhaupt an eure Daten kommt.

FAKTENCHECK · Warum das bei euch nicht „nur Microsoft 365“ ist

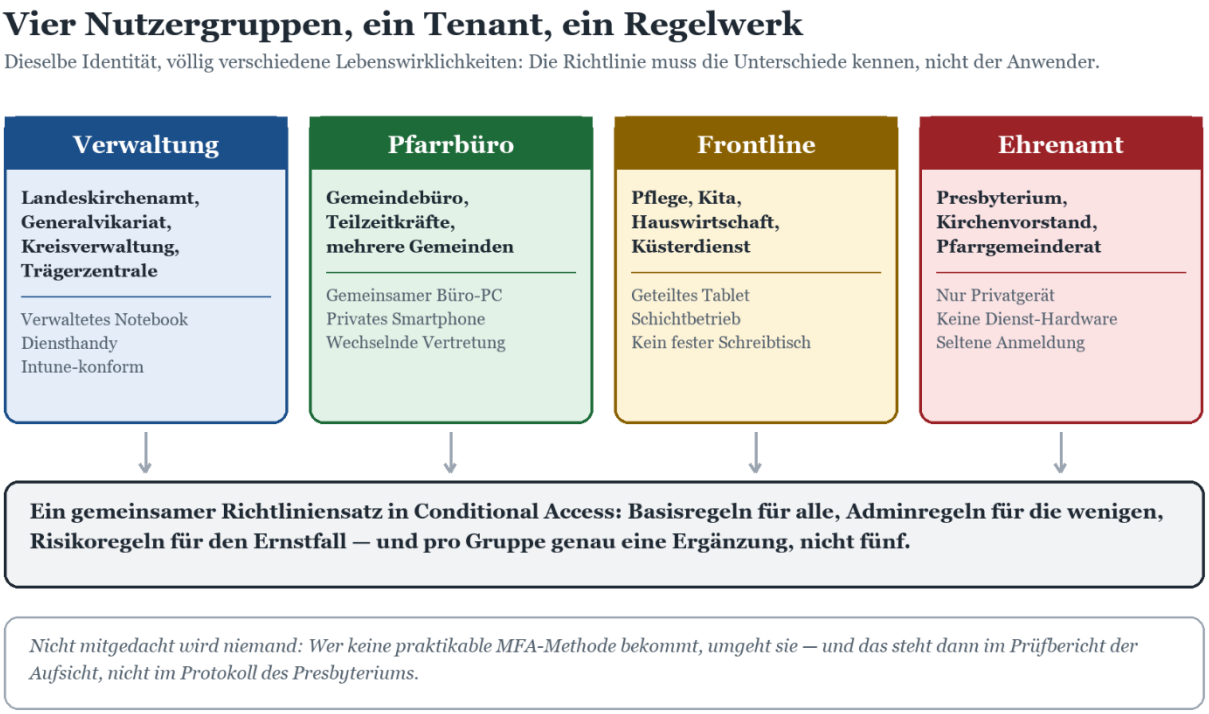
Kirchliche Träger unterliegen nicht der DSGVO, sondern eigenem Recht: auf evangelischer Seite dem Datenschutzgesetz der EKD (DSG-EKD), auf katholischer Seite dem Gesetz über den Kirchlichen Datenschutz (KDG). Beide verlangen geeignete technische und organisatorische Maßnahmen nach dem Stand der Technik — im DSG-EKD in § 27, im KDG in § 26. Beide Vorschriften nennen ausdrücklich die Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit sowie ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit.

Aufsicht führen nicht die Landesdatenschutzbehörden, sondern der Beauftragte für den Datenschutz der EKD beziehungsweise die Diözesandatenschutzbeauftragten und das Katholische Datenschutzzentrum. Mitbestimmung läuft über die Mitarbeitervertretung nach MVG-EKD oder MAVO, nicht über einen Personalrat nach Landespersonalvertretungsrecht. Der Rest — Entra ID, Intune, Purview — ist technisch identisch mit dem, was ein Mittelständler auch bekommt.

Vier Welten, ein Tenant: Wer sich bei euch eigentlich anmeldet

Bevor du eine einzige Richtlinie anlegst, brauchst du eine ehrliche Landkarte deiner Anwender. Nicht die aus dem Organigramm — die aus dem Alltag. Bei fast allen kirchlichen und diakonischen

Trägern fallen die Menschen in vier Gruppen, die sich technisch kaum ähnlicher sind als ein Kirchturm und ein Pflegebett.



Skizze 1: Vier Nutzergruppen mit völlig unterschiedlichen Gerätewelten — und ein gemeinsames Regelwerk darunter.

Die Verwaltung: der einfache Teil

Landeskirchenamt, Generalvikariat, Kreiskirchenamt, Dekanatsverwaltung, die Zentrale eines diakonischen Werks oder eines Caritasverbands auf Kreisebene: Hier sitzen Menschen mit eigenem Schreibtisch, eigenem Notebook und meistens einem Diensthandy. Die Geräte sind in Intune registriert, die Konformitätsrichtlinien greifen, die Belegschaft ist an Software gewöhnt. Diese Gruppe ist der Teil deines Rollouts, der reibungslos läuft — und genau deshalb die Gruppe, mit der du anfängst. Nicht weil sie am wichtigsten ist, sondern weil du an ihr lernst, ohne dass es wehtut.

Das Pfarrbüro: Teilzeit, Vertretung, Privatgerät

Im Pfarramt sieht es anders aus. Eine Kraft mit einer halben Stelle betreut drei Gemeinden, arbeitet an zwei Vormittagen in einem Büro, an einem dritten in einem anderen, und der Rechner dort wird auch von der Vertretung, vom Pfarrer und gelegentlich vom Kirchmeister benutzt. Ein Diensthandy gibt es nicht, weil der Haushalt es nicht hergibt. Das private Smartphone ist vorhanden, aber die Frage, ob die Person es dienstlich einsetzen muss, ist eine mitbestimmungsrelevante und arbeitsrechtliche, keine technische.

Hier entscheidet sich, ob dein Rollout gelingt. Wenn du dieser Gruppe keine Methode anbietest, die ohne Privatgerät funktioniert, bekommst du die Kennwörter auf gelben Zetteln unter der Tastatur zurück — und die sind noch nie durch eine Prüfung gekommen.

Frontline: Schichtbetrieb, geteilte Geräte, keine Zeit

Pflegedienst, Kita, Hauswirtschaft, Küsterdienst, Fahrdienst, Nachtwache. Diese Menschen haben keinen Schreibtisch, sondern eine Schicht. Sie teilen sich ein Tablet oder ein Stationstelefon, das

drei Kolleginnen vor ihnen in der Hand hatten. Microsoft nennt das Szenario Shared Device Mode: Eine Person meldet sich an, sieht ihre eigenen Daten in allen unterstützten Apps, meldet sich am Schichtende einmal ab und das Gerät ist wieder neutral. Conditional Access kann auf diesen Geräten gezielt andere Regeln durchsetzen als auf dem Notebook der Verwaltung — bei Android lässt sich der geteilte Modus mit Intune kombinieren, bei geteilten iPads solltest du die Einschränkungen der Plattform vorher genau prüfen, weil dort nicht jede Kombination aus Gerätekonformität und Conditional Access unterstützt wird.

Wie diese Arbeitsplätze insgesamt aussehen — von der Lizenz über die App-Auswahl bis zur Schichtplanung — steht im Beitrag Kita, Pflege, Jugendhilfe: Frontline-Arbeitsplätze in Microsoft 365 für Menschen ohne Schreibtisch. Hier geht es nur um die Anmeldung.

Ehrenamt: die Gruppe, die am schnellsten wieder weg ist

Presbyterium, Kirchenvorstand, Pfarrgemeinderat, Kirchenverwaltung, Gruppenleitungen, Besuchsdienst, Kollektenzähler. Ehrenamtliche haben ausschließlich Privatgeräte, melden sich unregelmäßig an und haben keinerlei Geduld für Technik, die ihnen den Abend verdirbt. Gleichzeitig sind sie die Gruppe, bei der ein kompromittiertes Konto besonders unangenehm wird, weil in Gremienunterlagen Personalvorgänge, Bauangelegenheiten und gelegentlich sehr persönliche Dinge stehen. Die Kunst besteht darin, den Zugriff eng zu halten, ohne ihn unbenutzbar zu machen.

Ob Ehrenamtliche überhaupt eigene Konten bekommen sollten oder ob ein Gastzugang die bessere Wahl ist, behandelt der Beitrag Ehrenamtliche in Microsoft 365: Gastzugang, eigene Konten, geteilte Postfächer oder besser gar nichts?. Das Regelwerk hier setzt voraus, dass die Entscheidung schon gefallen ist.

Die folgende Tabelle ist die Kurzfassung, die du in die Vorlage für Vorstand, Kirchenvorstand oder Geschäftsführung kopieren kannst. Sie beantwortet in einem Blick, was die häufigste Frage aus dem Gremium ist: „Und was heißt das jetzt für mich?“

Nutzergruppe	Gerätesituation	MFA-Methode	Richtlinie
Verwaltung Landeskirchenamt, Generalvikariat, Kreiskirchenamt, Trägerzentrale	Verwaltetes Notebook, Intune-konform, meist Diensthandy	Authenticator mit Number Matching; Ziel ist Windows Hello for Business auf dem verwalteten Gerät	Basisregel MFA; Zugriff bevorzugt vom konformen Gerät; normale Sitzungsdauer
Pfarrbüro Teilzeitkräfte, Vertretung, mehrere Gemeinden	Gemeinsam genutzter Büro-PC, privates Smartphone, kein Diensthandy	Authenticator nur freiwillig auf dem Privatgerät; sonst Hardware-Token oder FIDO2-Schlüssel vom Träger	Basisregel MFA; auf nicht verwalteten Geräten App-erzwungene Einschränkungen im Browser, kein Download
Frontline Pflege, Kita, Hauswirtschaft, Küsterdienst	Geteiltes Tablet oder Stationsgerät im Schichtbetrieb, Shared Device Mode	FIDO2-Schlüssel am Schlüsselbund oder OATH-Token; Authenticator nur bei persönlichem Diensthandy	Zugriff nur vom registrierten, konformen Gerät; kurze Sitzungsdauer; Abmeldung am Schichtende
Ehrenamt Presbyterium, Kirchenvorstand, Pfarrgemeinderat	Ausschließlich Privatgeräte, unregelmäßige Nutzung	Authenticator auf dem eigenen Smartphone; Temporary Access Pass für den Einstieg	MFA verpflichtend; nur Browserzugriff, keine persistente Sitzung; kein Zugriff auf Personal- und Klientendaten
Administration Tenant-	Dediziertes Adminkonto, möglichst eigene	Passkey (FIDO2) oder zertifikatsbasierte	Authentifizierungsstärke „Phishing-resistent“; Zugriff

Administration, Systemhaus, Rechenzentrum	Verwaltungsarbeitsstation	Authentifizierung — phishing-resistent, ohne Ausnahme	nur vom verwalteten Gerät; Anmeldung bei jedem Zugriff neu

Der rechtliche Rahmen: warum Conditional Access kein reines IT-Thema ist

In einem mittelständischen Betrieb entscheidet die IT-Leitung über MFA, informiert den Betriebsrat und schaltet scharf. Bei euch sind mindestens drei weitere Beteiligte im Raum, und alle drei können dir das Projekt anhalten — zu Recht.

Datenschutzrecht: eigene Gesetze, gleicher Maßstab

Das DSG-EKD verpflichtet verantwortliche Stellen und kirchliche Auftragsverarbeiter in § 27 auf geeignete technische und organisatorische Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Risiken für die Rechte und Freiheiten der betroffenen Personen. Ausdrücklich genannt sind Pseudonymisierung, Anonymisierung und Verschlüsselung, die Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit sowie ein Verfahren zur regelmäßigen Überprüfung und Bewertung der Wirksamkeit. Der Beauftragte für den Datenschutz der EKD hat dazu ein eigenes Kurzpapier zu technischen und organisatorischen Maßnahmen und IT-Sicherheit veröffentlicht.

Das KDG formuliert die Anforderung in § 26 praktisch wortgleich, samt derselben Aufzählung und demselben risikobasierten Ansatz: Maßnahmen sind dann geboten, wenn ihr Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht. Genau hier liegt dein Argument. MFA kostet bei Microsoft-365-Plänen in der Regel keine zusätzliche Lizenz, verhindert aber nach Microsofts eigener Auswertung den ganz überwiegenden Teil der Kontoübernahmen. Ein Träger, der Klientendaten, Personalakten und Seelsorgevorgänge in einem Tenant verarbeitet und auf MFA verzichtet, wird den Verhältnismäßigkeitstest nicht gewinnen.

Die Details beider Gesetze stehen in den Beiträgen DSG-EKD verständlich: Was das evangelische Datenschutzgesetz für Microsoft 365 konkret bedeutet und KDG verständlich: Microsoft 365 unter dem Kirchlichen Datenschutzgesetz der katholischen Kirche. Für dieses Regelwerk reicht die Erkenntnis, dass beide Kirchen an dieser Stelle denselben Maßstab anlegen — es gibt keine konfessionelle Abkürzung.

Mitbestimmung: die MAV sitzt früher am Tisch, als du denkst

Conditional Access erzeugt Anmeldeprotokolle. Anmeldeprotokolle enthalten Zeitpunkt, Ort, Gerät und Ergebnis jeder Anmeldung. Damit ist die Einführung eine Maßnahme, die geeignet ist, Verhalten oder Leistung zu überwachen — unabhängig davon, ob du das vorhast. Das MVG-EKD führt diesen Tatbestand in § 40 unter Nummer 11 als mitbestimmungspflichtige Angelegenheit, die MAVO in § 36 Absatz 1 Nummer 9. Beide Ordnungen sehen die Dienstvereinbarung als das Instrument vor, mit dem Dienstgeber und Mitarbeitervertretung diesen Punkt regeln; im MVG-EKD ist das in § 36 verankert. Die MAVO gilt als Rahmenordnung und wird diözesan in Kraft gesetzt, weshalb du bei mehreren Bistümern immer die jeweils geltende Fassung prüfen solltest.

Die gute Nachricht: Eine MAV, die früh eingebunden wird, ist bei MFA meistens ein Verbündeter. Sie hat nämlich dasselbe Interesse wie du — nur von der anderen Seite. Sie will, dass niemand sein Privatgerät hergeben muss, dass Protokolle nicht zur Leistungskontrolle zweckentfremdet werden und dass klar ist, wer die Anmeldeprotokolle wie lange sehen darf. Schreib das in die

Dienstvereinbarung und du bekommst die Zustimmung. Verschweig es und du bekommst die Einigungsstelle.

TIPP · Was in die Dienstvereinbarung gehört, damit MFA durchgeht

Zweckbindung: Anmeldeprotokolle dienen der IT-Sicherheit und der Aufklärung von Sicherheitsvorfällen, nicht der Verhaltens- oder Leistungskontrolle. Eine Auswertung zu Personalzwecken ist ausgeschlossen.

Freiwilligkeit beim Privatgerät: Wer kein dienstliches Gerät hat, bekommt auf Wunsch einen vom Träger gestellten Hardware-Token. Niemand muss ein privates Smartphone einsetzen, und wer es freiwillig tut, bekommt dafür keine Nachteile und keine Vorteile.

Rollen und Einsicht: Wer darf Anmeldeprotokolle sehen, wer darf Berichte erzeugen, wer wird bei Auffälligkeiten hinzugezogen, und wann wird die MAV informiert.

Aufbewahrung: Wie lange bleiben Anmelde- und Überwachungsprotokolle vorhanden, und was passiert danach.

Änderungsverfahren: Wie werden neue Richtlinien oder Änderungen an bestehenden angekündigt und beteiligt. Ein Satz dazu erspart dir bei jeder späteren Anpassung eine neue Verhandlungsrunde.

Vertiefung: Mitarbeitervertretung und Microsoft 365: MVG-EKD, MAVO, Dienstvereinbarung und Mitbestimmung bei Teams, Copilot und Protokollierung

Die Gremien: Beschlussfähigkeit ist keine Formsache

Presbyterium und Kirchenvorstand auf evangelischer Seite, Pfarrgemeinderat und Kirchenverwaltung auf katholischer Seite, dazu Verbandsvertretung, Kreissynode oder Dekanatsrat: Wenn Ehrenamtliche eigene Konten im Tenant bekommen, ist das eine Entscheidung mit Haftungsbezug, nicht nur eine Handreichung. Ein kurzer Beschlussvorschlag mit drei Sätzen — Zweck, Umfang, Methode — spart dir später die Diskussion, ob „das jemand so entschieden hat“. Er spart übrigens auch der Geschäftsführung eine unangenehme Frage, falls doch einmal etwas passiert.

MFA-Methoden praktikabel wählen: was funktioniert, was nur auf Folien funktioniert

Die Methodenwahl ist der Punkt, an dem Projekte scheitern. Nicht an der Technik — Entra ID kann alles — sondern daran, dass jemand die Methode für eine Gruppe festgelegt hat, ohne die Gruppe gefragt zu haben. Die folgende Reihenfolge hat sich in kirchlichen Umgebungen bewährt.

Skizze 2: Der Entscheidungsweg zur passenden MFA-Methode. Die erste Zeile, die zutrifft, gewinnt.

Microsoft Authenticator: der Standard für alle mit Smartphone

Die Push-Benachrichtigung im Microsoft Authenticator ist inzwischen durchgängig mit Number Matching abgesichert: Auf dem Anmeldebildschirm erscheint eine Zahl, die in der App eingegeben werden muss. Das ist kein kosmetisches Detail, sondern die Antwort auf die MFA-Ermüdungsangriffe der vergangenen Jahre, bei denen Angreifer so lange Push-Anfragen geschickt haben, bis jemand genervt auf „Genehmigen“ tippte. Number Matching lässt sich nicht abschalten, und wer eine zu alte App-Version betreibt, kann sich schlicht nicht mehr anmelden. Ergänzend zeigt die App den Anwendungsnamen und den ungefähren Standort der Anmeldung an — für die Belegschaft ist das die verständlichste Warnung, die es gibt: „Da will sich jemand aus einem Land anmelden, in dem ich nicht bin.“

Ein praktischer Nebeneffekt: Wenn Authenticator und die anzumeldende App auf demselben Gerät laufen, genügt eine Ja-Nein-Antwort statt der Zahleneingabe. Im Browser bleibt es bei der Zahl. Das erklärt die Rückfrage „Bei mir sieht das anders aus als bei der Kollegin“, bevor sie dich erreicht.

FIDO2 für Administration: die einzige Stelle ohne Kompromiss

Entra ID kennt drei eingebaute Authentifizierungsstärken, die du in Conditional Access direkt als Bedingung verwenden kannst. Für privilegierte Rollen nimmst du die stärkste, und zwar ohne Diskussion. Ein Trägerkonto mit globaler Administratorrolle, das per SMS abgesichert ist, ist der Grund, warum Ransomware-Vorfälle in der Sozialwirtschaft überhaupt noch funktionieren.

Methode	MFA-Stärke	Kennwortlos	Phishing-resistent	Praxisnote für kirchliche Träger
Passkey / FIDO2-Sicherheitsschlüssel	ja	ja	ja	Erste Wahl für Administration und Notfallkonten. Zwanzig bis fünfzig Euro

				pro Schlüssel, kein Abo, kein Akku.
Windows Hello for Business	ja	ja	ja	Kostenlos auf jedem verwalteten Windows-Gerät. Der unterschätzte Gewinner für die Verwaltung.
Zertifikatsbasierte Authentifizierung (mehrstufig)	ja	ja	ja	Sinnvoll, wenn im Landeskirchenamt oder Generalvikariat ohnehin eine PKI betrieben wird.
Authenticator (Telefonanmeldung ohne Kennwort)	ja	ja	nein	Sehr gute Alltagsmethode für alle mit dienstlichem Smartphone.
Temporary Access Pass	ja	nein	nein	Nur für Onboarding und Wiederherstellung gedacht — und genau dafür unverzichtbar.
Kennwort plus Push, SMS, Anruf oder OATH-Code	ja	nein	nein	Erfüllt die Pflicht, mehr nicht. Für Adminrollen und Klientendaten zu schwach.
SMS-Anmeldung oder Kennwort allein	nein	nein	nein	Erfüllt die MFA-Anforderung nicht. Taucht trotzdem in jedem zweiten Bestandstenant auf.

Für die Adminrichtlinie wählst du in Conditional Access nicht „Mehrstufige Authentifizierung erforderlich“, sondern „Authentifizierungsstärke erforderlich“ mit der eingebauten Stärke für phishing-resistente Verfahren. Beide Steuerungen zusammen in einer Richtlinie sind nicht zulässig — das ist der Fehler, an dem die erste Konfiguration regelmäßig hängen bleibt.

Temporary Access Pass: das Werkzeug für den ersten Tag

Der Temporary Access Pass ist ein zeitlich begrenzter Code, mit dem sich jemand anmelden kann, der noch gar keine Methode registriert hat. Damit löst du das Henne-Ei-Problem des Onboardings: Wie soll sich jemand mit MFA anmelden, um MFA einzurichten? In der Standardkonfiguration ist ein solcher Pass eine Stunde gültig, die maximale Lebensdauer steht auf acht Stunden, und der zulässige Bereich reicht von zehn Minuten bis zu dreißig Tagen. Du kannst festlegen, ob ein Pass nur einmal oder mehrfach verwendbar ist.

Für kirchliche Träger ist das Gold wert. Der neue Kollege im Kreiskirchenamt bekommt seinen Pass beim Personalgespräch. Die ehrenamtliche Gremienkraft bekommt ihn im Presbyteriumstermin, ausgedruckt auf einem Zettel, gültig bis zum Abend. Der Pflegemitarbeiter bekommt ihn zu Schichtbeginn. Ein Detail solltest du kennen: Wird ein Einmal-Pass verwendet, um eine kennwortlose Methode zu registrieren, muss die Registrierung innerhalb von zehn Minuten nach der Anmeldung abgeschlossen sein. Bei einem Geräte-Einrichtungsprozess, der länger dauert, brauchst du entweder zwei Einmal-Pässe oder einen mehrfach verwendbaren.

Wenn kein Smartphone da ist: Hardware statt Hilflosigkeit

Es gibt in jeder Gemeinde und jeder Einrichtung Menschen ohne Smartphone. Manche wollen keines, manche können keines bedienen, manche haben schlicht keines. Für diese Gruppe gibt es zwei ordentliche Antworten: einen FIDO2-Sicherheitsschlüssel — ein Stück Hardware, das man am Schlüsselbund trägt und in den USB-Anschluss steckt — oder einen Hardware-Token, der alle dreißig oder sechzig Sekunden einen neuen Zahlencode anzeigt. Beides stellt der Träger, beides kostet einmalig weniger als eine Stunde Supportaufwand, und beides beendet die Diskussion über Privatgeräte sofort.

Zur Verwaltung der Hardware-Token in der Richtlinie für Authentifizierungsmethoden solltest du wissen, dass Microsoft diesen Weg zum Redaktionsschluss noch als Vorschau kennzeichnet: Anlegen, Zuweisen und Aktivieren laufen über Microsoft Graph oder das Entra-Verwaltungsportal, die Aktivierung kann wahlweise die Administration übernehmen oder die Person selbst über ihre Sicherheitsinformationen. Plane bei der Ersteinrichtung ein, dass Richtlinienänderungen bis zu einer Stunde brauchen können, bevor der Token beim Anwender auftaucht. Das erspart dir drei aufgeregte Anrufe pro Gemeinde.

AUS DER PRAXIS · Die Küsterin ohne Diensthandy — und warum sie am Ende die Beste war

Eine Kirchengemeinde in einem größeren Kirchenkreis hatte den Rollout sauber geplant: Authenticator für alle, Stichtag, fertig. Dann kam die Küsterin. Sechzig Jahre, seit achtzehn Jahren im Dienst, verantwortlich für Schlüssel, Heizung, Glocken und die Abendmahlsvorbereitung. Kein Smartphone. Das private Gerät war ein Tastenhandy mit Prepaid-Karte, und der Vorschlag, sie möge doch eine App installieren, war schlicht gegenstandslos. Sie sagte höflich, aber sehr bestimmt: Für den Dienst stelle die Gemeinde die Werkzeuge, nicht sie.

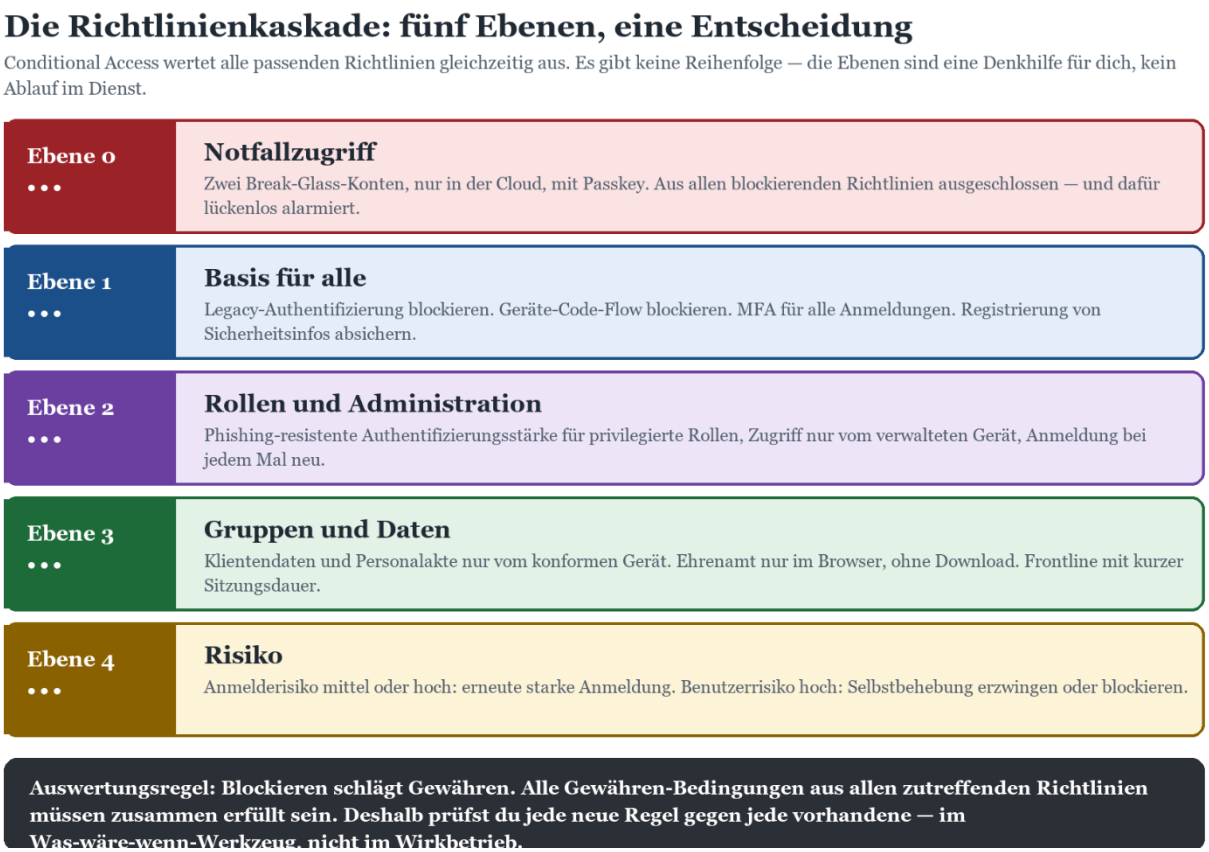
Die MAV gab ihr recht — und hatte recht. Der Rollout stand vier Wochen. In der Zwischenzeit kursierte im Gemeindebüro ein gemeinsames Kennwort, weil „das ja nur übergangsweise“ sei. So entstehen Befunde für die Aufsicht: nicht durch böse Absicht, sondern durch eine Richtlinie ohne Ausweg.

Die Lösung kostete achtundzwanzig Euro. Die Küsterin bekam einen FIDO2-Sicherheitsschlüssel, den sie an ihren ohnehin beeindruckenden Schlüsselbund hängte — sie trug bereits vierzig Schlüssel durch die Gegend, auf einen mehr kam es nicht an. Anmeldung am Büro-PC: Schlüssel einstecken, PIN eingeben, fertig. Kein Kennwort mehr, keine App, keine Zahlen abtippen. Nach zwei Wochen war sie die Person in der Gemeinde, die sich am schnellsten anmeldete, und beim nächsten Gemeindefest erklärte sie zwei Presbyterinnen ungefragt, wie das funktioniert.

Die eigentliche Lehre ist nicht der Schlüssel, sondern die Reihenfolge. Wer die Methodenwahl an der schwächsten Stelle beginnt statt an der bequemsten, hat am Ende ein Regelwerk ohne Ausnahmen. Wer bei der Verwaltung beginnt und den Rest „später regelt“, hat am Ende ein Ausnahmeregister, das länger ist als die Richtliniensammlung.

Der Richtliniensatz: Basis, Administration, Risiko — und pro Gruppe eine Ergänzung

Jetzt zum eigentlichen Regelwerk. Die wichtigste Gestaltungsentscheidung vorweg: Weniger Richtlinien sind besser als viele. Conditional Access wertet bei jeder Anmeldung alle zutreffenden Richtlinien gleichzeitig aus. Es gibt keine Reihenfolge, keine Priorität und kein „die speziellere gewinnt“. Blockieren schlägt Gewähren, und alle Gewähren-Bedingungen aus allen passenden Richtlinien müssen gemeinsam erfüllt sein. Wer fünfundzwanzig Richtlinien hat, kann nicht mehr vorhersagen, was bei einer bestimmten Anmeldung passiert — und erklärt das der Aufsicht dann im Konjunktiv.



Skizze 3: Die Richtlinienkaskade als Denkmodell. Die Ebenen ordnen deinen Kopf, nicht die Auswertungsreihenfolge im Dienst.

Ebene 1: Die Basisregeln, die in jedem kirchlichen Tenant stehen sollten

Vier Richtlinien bilden das Fundament, und sie gelten für alle — vom Landeskirchenamt bis zum Kollektenzähler. Microsoft legt einen Teil davon inzwischen selbst als verwaltete Richtlinien im Tenant an: Sie erscheinen zunächst im Nur-Bericht-Modus und werden frühestens dreißig Tage nach ihrer Einführung automatisch aktiviert, wobei betroffene Organisationen zwei Wochen vorher per Nachrichtencenter und E-Mail informiert werden. Du kannst sie früher einschalten, deaktivieren oder Ausschlüsse ergänzen — umbenennen oder löschen nicht. Wenn in deinem Tenant also plötzlich Richtlinien auftauchen, die als von Microsoft verwaltet gekennzeichnet sind: Das ist kein Fehler und auch kein Systemhaus, das ungefragt gearbeitet hat.

- Legacy-Authentifizierung blockieren. Alte Protokolle wie IMAP, POP3 und SMTP-Basisauthentifizierung kennen kein MFA. Nach Microsofts Analyse nutzen über 99 Prozent der Kennwort-Sprühangriffe genau diese Wege. In kirchlichen Beständen findet sich hier regelmäßig ein alter Scanner im Gemeindehaus oder eine Software für den Gemeindebrief-Versand — suchen, ersetzen, blockieren.
- Geräte-Code-Flow blockieren. Der Anmeldeweg, bei dem du auf einem Gerät startest und auf einem anderen bestätigst, wird von echten Anwendern selten und von Angreifern häufig genutzt. Ausnahme: Teams-Raumsysteme im Gemeindesaal oder Sitzungszimmer brauchen ihn eventuell — dann schließt du gezielt diese Konten aus, nicht die Richtlinie ab.
- MFA für alle Anmeldungen. Die Kernregel. Zielgruppe sind alle Konten, ausgenommen ausschließlich die Notfallkonten. Keine Ausnahme für „die Geschäftsführung, die das nicht mag“. Gerade nicht für die Geschäftsführung, denn deren Postfach ist das Ziel jeder zweiten Rechnungsmanipulation.

- Registrierung von Sicherheitsinformationen absichern. Die Registrierung neuer Anmeldemethoden ist der empfindlichste Vorgang überhaupt. Sie sollte nur von einem vertrauenswürdigen Standort, von einem konformen Gerät oder nach Anmeldung mit einem Temporary Access Pass möglich sein.

Ebene 2: Administration — wenige Konten, harte Regeln

Microsoft verpflichtet seit 2024 schrittweise zu MFA für die eigenen Verwaltungsoberflächen. In der ersten Phase betraf das ab Oktober 2024 das Azure-Portal, das Microsoft-Entra-Verwaltungscenter und das Intune-Verwaltungscenter, ab Februar 2025 kam das Microsoft-365-Admin-Center dazu. Die zweite Phase begann am 1. Oktober 2025 und erfasst Azure CLI, Azure PowerShell, die Azure-App, Infrastruktur-als-Code-Werkzeuge und REST-Aufrufe für alle ändernden Vorgänge; Lesevorgänge bleiben ausgenommen. Diese Durchsetzung kennt keine Ausnahme — auch nicht für Notfallkonten. Microsoft empfiehlt deshalb ausdrücklich, Notfallkonten mit Passkey oder zertifikatsbasierter Authentifizierung auszustatten, weil beide Verfahren die Anforderung erfüllen.

Deine eigene Adminrichtlinie geht darüber hinaus und fordert dreierlei: die Authentifizierungsstärke für phishing-resistente Verfahren, den Zugriff ausschließlich von einem konformen Gerät und eine Anmeldehäufigkeit, die bei jedem Zugriff eine frische Authentifizierung verlangt. Das ist unbequem. Es ist auch genau der Punkt, an dem ein diakonisches Werk in einer Großstadt nach einem Vorfall feststellte, dass drei Personen dauerhaft globale Administratorrechte hatten, von denen zwei seit über einem Jahr nicht mehr im Haus waren.

Ebene 3: Gruppen und Daten — hier wird es kirchlich

Die gruppenspezifischen Regeln sind der Teil, den du nicht aus einer Vorlage übernehmen kannst, weil er von eurem Datenbestand abhängt. Drei Muster begegnen einem immer wieder:

- Klientendaten und Personalakten nur vom konformen Gerät. Beratungsdokumentation, Pflegeplanung, Jugendhilfeakten, Personalvorgänge: Diese Inhalte gehören in SharePoint-Bereiche, die nur von verwalteten Geräten erreichbar sind. Nicht weil das Privatgerät böse ist, sondern weil du bei ihm keine Verschlüsselung, keinen Virenschutz und keine Löschmöglichkeit nachweisen kannst.
- Ehrenamt im Browser, ohne Spuren. Für Ehrenamtliche auf Privatgeräten sind app-erzwungene Einschränkungen das Mittel der Wahl: Der Zugriff läuft im Browser, Dateien lassen sich ansehen und bearbeiten, aber nicht herunterladen, drucken oder synchronisieren. Dazu keine dauerhafte Browsersitzung und eine Anmeldehäufigkeit, die nach spätestens einem Tag erneut fragt.
- Frontline mit kurzer Leine. Auf geteilten Geräten im Schichtbetrieb setzt du Gerätekonformität voraus und hältst die Sitzungsdauer kurz. Die eigentliche Sicherheit kommt hier aber nicht aus Conditional Access, sondern aus der Disziplin, sich am Schichtende abzumelden — und aus einem Gerätemodus, der das mit einem Fingertipp erledigt statt mit sieben.

Welche Inhalte überhaupt in welche Schutzklasse gehören, ist eine eigene Aufgabe; sie wird im Beitrag Klientendaten in Diakonie und Caritas: Sozialdaten, Schweigepflicht und Schutz mit Microsoft Purview behandelt. Für das Zugriffsregelwerk brauchst du daraus nur die Gruppenzuordnung.

Ebene 4: Risiko — die Regeln, die du hoffentlich nie bemerkst

Wenn eure Lizenzausstattung Identitätsschutz umfasst, kommen zwei Richtlinien dazu, die unauffällig im Hintergrund arbeiten: eine, die bei auffälligem Anmelderisiko eine erneute starke

Authentifizierung verlangt, und eine, die bei hohem Benutzerrisiko eine Selbstbehebung erzwingt oder den Zugriff blockiert. Auffällig heißt: unmöglicher Ortswechsel, Kennwort-Sprühangriff, Wiedereinspielen eines gestohlenen Tokens, geleakte Zugangsdaten aus einem fremden Datenleck. Letzteres ist in Gemeinden erstaunlich häufig, weil dienstliche Adressen gern für private Anmeldungen bei allerlei Portalen verwendet werden.

Welche Lizenzen welchen Funktionsumfang mitbringen und welche Nonprofit-Angebote für kirchliche Träger in Frage kommen, klärt der Beitrag Microsoft-365-Lizenzierung für kirchliche Träger: Nonprofit-Angebote, Frontline-Pläne und die Frage, wer überhaupt berechtigt ist. Die Risikoregeln setzen den höheren Plan voraus; Basis- und Adminregeln funktionieren auch ohne ihn.

Der komplette Satz sieht dann so aus. Die Kennungen sind Vorschläge — wichtig ist nur, dass du ein System hast und es durchhältst. Eine Richtlinie namens „Test neu Kopie 2 final“ ist in einem Prüftermin ein eigener Tagesordnungspunkt.

Kennung	Richtlinie	Zielgruppe	Steuerung
CA-001	Legacy-Authentifizierung blockieren	Alle Konten außer Notfallzugriff	Blockieren bei anderen Clients als moderner Authentifizierung
CA-002	MFA für alle Anmeldungen	Alle Konten außer Notfallzugriff	Authentifizierungsstärke: mehrstufige Authentifizierung
CA-003	Registrierung von Sicherheitsinformationen absichern	Alle Konten	Nur vom vertrauenswürdigen Standort, vom konformen Gerät oder mit Temporary Access Pass
CA-004	Geräte-Code-Flow blockieren	Alle Konten außer Besprechungsraumgeräten	Blockieren
CA-101	Phishing-resistente Anmeldung für privilegierte Rollen	Globale Administration und weitere privilegierte Rollen	Authentifizierungsstärke: phishing-resistent; Anmeldung bei jedem Zugriff neu
CA-102	Administration nur vom verwalteten Gerät	Privilegierte Rollen	Konformes oder in Entra eingebundenes Gerät erforderlich
CA-201	Erhöhtes Anmelderisiko	Alle Konten außer Notfallzugriff	Erneute starke Authentifizierung erforderlich
CA-202	Hohes Benutzerrisiko	Alle Konten außer Notfallzugriff	Selbstbehebung erzwingen oder Zugriff blockieren
CA-301	Klientendaten und Personalakten schützen	Gruppen Pflege, Beratung, Jugendhilfe, Personalwesen	Konformes Gerät für die betroffenen SharePoint-Bereiche
CA-302	Ehrenamt auf Privatgeräten	Gruppe Ehrenamt	App-erzwungene Einschränkungen, keine dauerhafte Browsersitzung, tägliche Neuanmeldung
CA-303	Frontline auf geteilten Geräten	Gruppe Frontline	Registriertes und konformes Gerät, kurze Sitzungsdauer
CA-901	Notfallzugriff	Gruppe Notfallzugriff (zwei Konten)	Ausschluss aus allen blockierenden Richtlinien; Passkey registriert; Alarmierung bei jeder Anmeldung

WARNUNG · Break-Glass-Konten ohne Überwachung sind keine Notfalllösung, sondern eine Hintertür

Microsoft empfiehlt mindestens zwei Notfallzugriffskonten. Sie sollen reine Cloud-Konten in der Standarddomäne sein, nicht föderiert, nicht aus einem lokalen Verzeichnis synchronisiert, an keine einzelne Person und an kein privates Gerät gebunden. Sie sollen ein anderes

Authentifizierungsverfahren nutzen als die regulären Adminkonten, ihre Anmeldedaten gehören an zwei getrennte, gesicherte Orte, und die Rollenzuweisung soll dauerhaft aktiv sein statt nur berechtigend.

Der Fehler, den man in kirchlichen Tenants am häufigsten sieht, ist nicht das Fehlen dieser Konten. Es ist ihr Fehlen im Überwachungskonzept. Die Konten werden angelegt, aus allen Richtlinien ausgeschlossen, das Kennwort wandert in einen Umschlag im Tresor der Kirchenkreisverwaltung — und dann passiert drei Jahre lang nichts. Niemand merkt, wenn sie benutzt werden. Niemand weiß, ob sie überhaupt noch funktionieren. Damit hast du ein privilegiertes Konto ohne MFA, ohne Protokollauswertung und ohne Eigentümer. Das ist exakt die Konstellation, die in einem Prüfbericht zu einem Befund wird — und in einem Ransomware-Vorfall zum Einstiegspunkt.

Microsoft verlangt für diese Konten drei Dinge, die du nicht weglassen darfst: Alarmierung bei jeder Anmeldung an mindestens zwei Personen, eine Nachschau nach jeder Nutzung mit der Frage, ob sie berechtigt war, und eine Überprüfung der Funktionsfähigkeit mindestens alle neunzig Tage. Dazu gehört auch, den Kreis der Berechtigten zu aktualisieren und die Tresorkombination zu ändern, wenn jemand das Haus verlässt. Das ist kein Misstrauen gegenüber der Dienstgemeinschaft, sondern die gleiche Selbstverständlichkeit, mit der ihr auch die Schlösser tauscht, wenn ein Generalschlüssel verschwindet.

Skizze 4: Die fünf Glieder der Break-Glass-Kette. Fehlt eines, ist das Konto kein Notfallzugriff mehr.

Ausnahmen, Dokumentation und der Blick der Aufsicht

Es wird Ausnahmen geben. Das ist keine Niederlage, sondern Realität: ein Fachverfahren im Krankenhaus, das noch nicht mit moderner Authentifizierung umgehen kann; ein Dienstleister, der aus einem Land zugreift, das eure Standortregel eigentlich sperrt; ein Besprechungsraumsystem, das den Geräte-Code-Flow braucht. Der Unterschied zwischen einem gut geführten und einem schlecht geführten Tenant liegt nicht darin, ob es Ausnahmen gibt, sondern ob jemand sie erklären kann.

Das Ausnahmeregister: eine Tabelle, die dir einen Prüftermin rettet

Führe die Ausnahmen außerhalb des Tenants, in einem Dokument, das auch dann noch lesbar ist, wenn gerade niemand im Verwaltungsportal angemeldet ist. Diese Struktur hat sich bewährt — sowohl gegenüber dem BfD EKD als auch gegenüber einem Diözesandatenschutzbeauftragten, denn beide stellen im Kern dieselben Fragen:

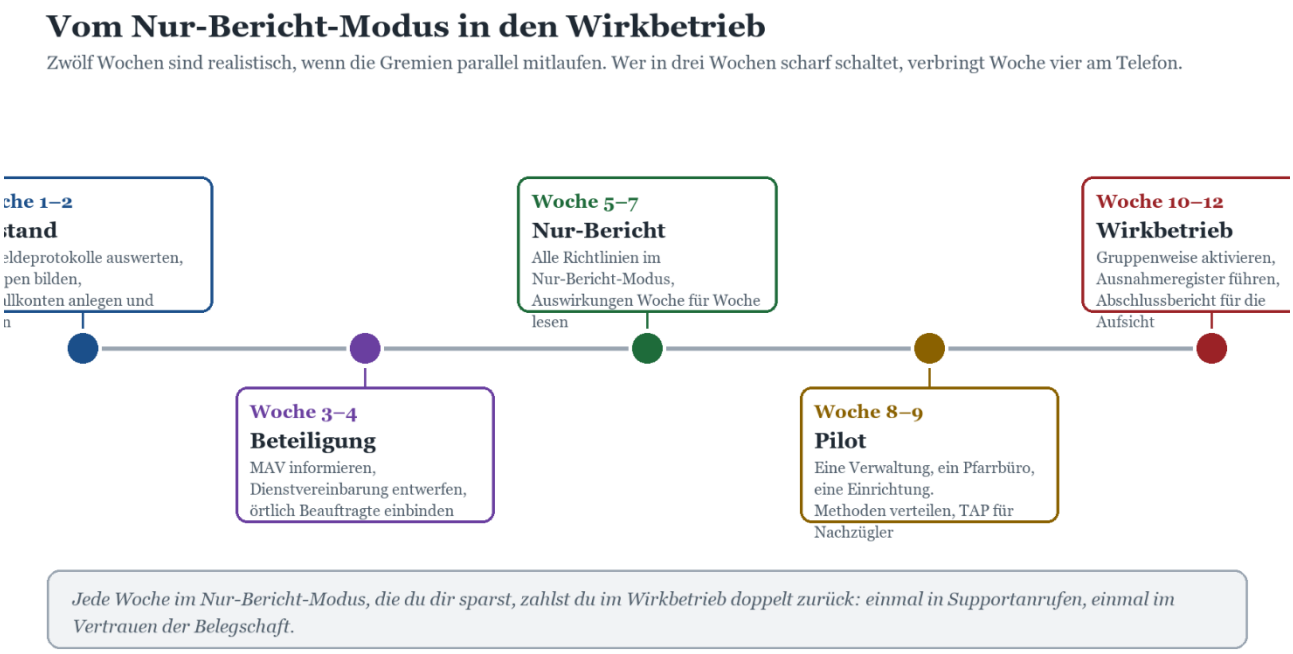
Feld	Was hineingehört	Typisches Beispiel
Kennung	Fortlaufende Nummer, die auch im Richtliniennamen auftaucht	AUS-2026-004
Betroffene Richtlinie	Kennung und Name der Richtlinie, aus der ausgeschlossen wird	CA-002 MFA für alle Anmeldungen
Personenkreis oder Konto	Gruppe oder Dienstkonto, niemals eine offene Sammelgruppe	Dienstkonto Schnittstelle Meldewesen
Fachliche Begründung	Warum die Ausnahme nötig ist, in einem Satz ohne Fachchinesisch	Schnittstelle unterstützt keine moderne Authentifizierung
Kompensierende Maßnahme	Was stattdessen schützt	Zugriff nur aus dem Rechenzentrumsnetz, keine interaktive Anmeldung, wöchentliche Protokollauswertung
Befristet bis	Immer ein Datum. Unbefristete Ausnahmen sind keine Ausnahmen, sondern Zustände	31.03.2027 (Ablösung des Fachverfahrens)
Freigabe durch	Wer entschieden hat — Leitung, nicht Administration	Verwaltungsleitung, im Benehmen mit der örtlich Beauftragten für den Datenschutz
Beteiligung	Ob und wann MAV und Datenschutz eingebunden waren	MAV informiert am 14.01.2026

Zwei Felder machen den Unterschied: das Ablaufdatum und die kompensierende Maßnahme. Eine Ausnahme mit beidem ist eine Risikoentscheidung. Eine Ausnahme ohne beides ist ein Versäumnis mit Aktenzeichen.

Was die kirchlichen Aufsichten sonst noch von einem Tenant sehen wollen, steht im Beitrag Kirchliche Datenschutzaufsicht in der Praxis: Was BfD EKD und Diözesandatenschutzbeauftragte von einem Microsoft-365-Tenant erwarten. Das Ausnahmeregister ist eines der Dokumente, nach denen dort regelmäßig als Erstes gefragt wird.

Die Einführung: Nur-Bericht-Modus ist nicht optional

Jede Conditional-Access-Richtlinie lässt sich im Nur-Bericht-Modus betreiben. Sie wird dann bei jeder Anmeldung ausgewertet und protokolliert, greift aber nicht ein. Das ist kein Testmodus für Vorsichtige, sondern der einzige verantwortbare Weg in einem Umfeld, in dem ein blockierter Zugriff bedeuten kann, dass der Pflegedienst um sechs Uhr morgens die Tourenplanung nicht öffnet. Lass die Richtlinien mindestens zwei, besser drei Wochen mitlaufen und lies die Auswertung wöchentlich. Du wirst Dinge finden, die niemand auf dem Zettel hatte — den Beamer im Gemeindesaal, das Scanner-Postfach, die Ehrenamtliche, die sich seit 2019 nur über ein altes Tablet anmeldet.



Skizze 5: Zwölf Wochen vom ersten Blick in die Anmeldeprotokolle bis zum Wirkbetrieb — mit Gremien im Takt.

WICHTIG · Reihenfolge der Aktivierung: erst das Netz, dann der Sprung

Aktiviere niemals die MFA-Richtlinie, bevor nicht jede Person eine registrierte Methode hat. Prüfe die Registrierungsberichte in Entra ID und arbeite die Liste ab, bevor du den Schalter umlegst. Wer am Stichtag noch nichts registriert hat, bekommt vorher einen Temporary Access Pass — nicht hinterher einen Anruf beim Bereitschaftsdienst.

Aktiviere zuerst die Notfallkonten samt Alarmierung, dann die Adminregeln, dann die Basisregeln, dann die Gruppenregeln. Die Reihenfolge klingt umständlich, hat aber einen Grund: Wenn dir bei den Adminregeln etwas um die Ohren fliegt, brauchst du die Notfallkonten. Wenn dir bei den Basisregeln etwas um die Ohren fliegt, brauchst du funktionierende Adminkonten.

Und teste im Was-wäre-wenn-Werkzeug, bevor du speicherst. Es beantwortet die Frage, welche Richtlinien bei einer konkreten Kombination aus Person, Anwendung, Gerät und Standort greifen würden. Das ist deutlich angenehmer als die Alternative, nämlich diese Frage von der Pflegedienstleitung telefonisch gestellt zu bekommen.

Wenn mehrere Träger im selben Tenant sitzen

Bei kirchlichen Strukturen ist die Tenant-Landschaft selten eine Landschaft, eher ein gewachsenes Gelände: Eine Landeskirche betreibt einen Tenant für die Verwaltung, die Kirchenkreise haben eigene, ein diakonisches Werk hat einen dritten, und ein katholischer Krankenhausverbund mit mehreren Standorten bringt gleich vier mit, weil jedes Haus einmal eigenständig war. Conditional Access wirkt immer pro Tenant. Wenn dein Regelwerk in mehreren Mandanten gelten soll, brauchst du entweder dieselbe Richtliniensammlung mehrfach — dann versioniere sie und halte sie synchron — oder du ziehst die Tenant-Frage grundsätzlich neu auf.

Für diese Entscheidung lohnt der Blick in Ein Tenant oder viele? Kirchengemeinde, Kirchenkreis, Landeskirche, Bistum und die Frage der Tenant-Architektur. Das Zugriffsregelwerk ist übrigens eines der besten Argumente für Konsolidierung: Fünf Tenants bedeuten fünf Ausnahmeregister, fünf Notfallkontenpaare und fünf Gelegenheiten, eine davon zu vergessen.

Die identitätsseitigen Grundlagen dieses Beitrags — Verzeichnisstruktur, Gruppen, Synchronisierung, Rollen zwischen Landeskirche, Verband, Träger und Einrichtung — stehen im Beitrag Entra ID für kirchliche Träger: Identitäten zwischen Landeskirche, Verband, Träger und Einrichtung. Wenn dort etwas schief steht, hilft dir das beste Richtlinienwerk nichts: Conditional Access ist immer nur so präzise wie die Gruppen, auf die es zielt.

Wer wissen will, wie der eigene Bestand tatsächlich dasteht, bevor er umbaut, findet in der Entra-ID-Tenant-Überprüfung für kirchliche Träger: Was die Diagnostiker-Überprüfung zum Festpreis liefert einen strukturierten Einstieg mit klarem Ergebnis.

Häufige Fragen

Brauchen wir für Conditional Access eine teure Lizenz?

Conditional Access setzt einen Entra-ID-Plan der ersten Stufe voraus, der in etlichen Microsoft-365-Paketen enthalten ist, unter anderem in Business Premium. Die risikobasierten Richtlinien brauchen die zweite Stufe. Ohne passenden Plan bleiben dir die Sicherheitsstandards, die pauschal MFA verlangen, ohne dass du Ausnahmen oder Gruppen steuern kannst — für ein Pfarrbüro mit drei Konten mag das reichen, für einen Träger mit Pflege, Kita und Verwaltung nicht.

Dürfen wir Beschäftigte verpflichten, ihr privates Smartphone für MFA zu nutzen?

Das ist keine technische, sondern eine dienstrechtliche Frage, und die Antwort lautet in der Praxis: eher nicht, und schon gar nicht ohne Beteiligung der Mitarbeitervertretung. Der saubere Weg ist, die Nutzung des Privatgeräts ausdrücklich freiwillig zu stellen und für alle anderen eine vom Träger gestellte Alternative bereitzuhalten. Das kostet dich einmalig ein paar Hardware-Token und spart dir eine Grundsatzdiskussion, die du nicht gewinnen kannst.

Was ist mit Pfarrerinnen und Pfarrern im Seelsorgekontext?

Conditional Access regelt den Zugang, nicht den Inhalt. Für das Seelsorgegeheimnis ist die entscheidende Frage nicht, wie sich jemand anmeldet, sondern was überhaupt im System liegt. MFA ist dafür notwendig und bei weitem nicht hinreichend. Das gehört in ein eigenes Konzept; siehe dazu Seelsorgegeheimnis und Beichtgeheimnis in Microsoft 365: Was nie in Teams, OneNote oder Copilot landen darf.

Wie viele Conditional-Access-Richtlinien sind zu viele?

Eine belastbare Faustregel: Wenn du nicht mehr aus dem Kopf sagen kannst, welche Richtlinien bei einer bestimmten Anmeldung greifen, sind es zu viele. Für einen mittleren kirchlichen Träger sind zehn bis vierzehn Richtlinien ein gutes Maß. Zwanzig gehen noch. Bei vierzig hat jemand jedes Einzelproblem mit einer eigenen Richtlinie erschlagen, und die Wechselwirkungen versteht niemand mehr.

Was passiert, wenn das Handy kaputt ist oder der Schlüssel im anderen Mantel steckt?

Genau dafür gibt es den Temporary Access Pass. Die Person ruft im Support an, weist sich nach einem definierten Verfahren aus — und dieses Verfahren solltest du vorher festlegen, denn der Anruf „Hier ist die Kollegin aus dem Pfarrbüro, ich brauche schnell einen Zugang“ ist der Standardeinstieg jedes Social-Engineering-Angriffs — und bekommt einen zeitlich eng begrenzten

Pass. Wichtig ist die zweite Methode: Wer nur eine registriert hat, ruft irgendwann an. Wer zwei hat, hilft sich selbst.

Muss die MAV jeder einzelnen Richtlinie zustimmen?

In der Regel nicht jeder einzelnen, wenn die Dienstvereinbarung einen Rahmen setzt und ein Änderungsverfahren beschreibt. Genau deshalb lohnt es sich, diesen Punkt beim ersten Mal sauber zu verhandeln. Ohne Rahmen wird jede neue Richtlinie zu einem eigenen Vorgang — und spätestens bei der dritten Anpassung wird das Verfahren zum eigentlichen Projektrisiko.

Unser Rechenzentrum betreut den Tenant. Wer legt die Richtlinien an?

Technisch derjenige mit der passenden Rolle. Verantwortlich bleibt der Träger — datenschutzrechtlich wie mitbestimmungsrechtlich. Dass ein kirchliches Rechenzentrum oder ein Systemhaus die Umsetzung übernimmt, ändert daran nichts. Lass dir die Richtliniensammlung mindestens jährlich als Bericht vorlegen, inklusive aller Ausschlüsse. Wer den eigenen Tenant nur vom Hörensagen kennt, wird irgendwann überrascht.

Wir haben kaum Ehrenamtliche im Tenant. Lohnt der Aufwand trotzdem?

Das Regelwerk skaliert nach unten. Basis- und Adminregeln brauchst du in jedem Fall, auch bei zwölf Konten in einer Kirchengemeinde. Die gruppenspezifischen Ebenen lässt du einfach weg, bis es sie braucht. Ein Regelwerk, das mit fünf Richtlinien anfängt und auf zwölf wächst, ist deutlich besser als eines, das mit dreißig anfängt und nie aufgeräumt wird.

Fazit

Conditional Access ist bei einem kirchlichen Träger kein Sicherheitsprojekt, sondern ein Organisationsprojekt mit technischem Anteil. Die Technik ist der einfache Teil: Entra ID kann alles, was du brauchst, die Richtlinien sind an einem Vormittag angelegt, und die eingebauten Authentifizierungsstärken nehmen dir die Feinarbeit ab. Der schwierige Teil ist die ehrliche Landkarte deiner Anwender und die Bereitschaft, für jede Gruppe eine Methode bereitzuhalten, die zu ihrem Alltag passt.

Halte dich an vier Sätze. Erstens: Beginne bei der schwächsten Stelle, nicht bei der bequemsten — die Küsterin ohne Smartphone entscheidet über den Erfolg, nicht die Verwaltung mit dem neuen Notebook. Zweitens: Wenige Richtlinien, klar benannt, in einem System, das du in einem Prüftermin vorlesen kannst. Drittens: Notfallkonten mit Passkey, mit Alarm, mit vierteljährlicher Probe — ein Notfallzugriff ohne Überwachung ist eine Hintertür mit gutem Gewissen. Viertens: Ausnahmen dokumentieren, befristen, kompensieren. Wer diese vier Dinge hat, besteht jede Prüfung durch den BfD EKD oder einen Diözesandatenschutzbeauftragten nicht deshalb, weil er nichts falsch gemacht hätte, sondern weil er jede Entscheidung erklären kann.

Und der Rest? Der Rest ist normales Microsoft 365. Die Zugriffsschicht ist technisch dieselbe wie bei einem Maschinenbauer im Sauerland. Anders sind die Gesetze, anders ist die Aufsicht, anders ist die Mitbestimmung, und anders sind die Menschen, die damit arbeiten — von der hauptamtlichen Verwaltungsleitung bis zur Ehrenamtlichen, die abends nach dem Gemeindekreis noch schnell ins Protokoll schaut. Ein Regelwerk, das diese Unterschiede kennt, macht die Arbeit sicherer, ohne sie mühsamer zu machen. Ein Regelwerk, das sie ignoriert, macht beides schlechter.

TIPP · Weiter im Thema

Wenn du das Regelwerk aufsetzen willst, ist die Reihenfolge dieser Beiträge hilfreich:

› Entra ID für kirchliche Träger: Identitäten zwischen Landeskirche, Verband, Träger und

Einrichtung

› Mitarbeitervertretung und Microsoft 365: MVG-EKD, MAVO, Dienstvereinbarung und Mitbestimmung bei Teams, Copilot und Protokollierung

› Ehrenamtliche in Microsoft 365: Gastzugang, eigene Konten, geteilte Postfächer oder besser gar nichts?

› Kita, Pflege, Jugendhilfe: Frontline-Arbeitsplätze in Microsoft 365 für Menschen ohne Schreibtisch

› Microsoft 365 in Kirche, Diakonie und Caritas: Was wirklich anders ist als in Kommune und Mittelstand

Wer das Regelwerk lieber gemeinsam mit jemandem aufsetzt, der schon ein paar kirchliche Tenants von innen gesehen hat: Das ist Gegenstand der Microsoft 365 Beratung für kirchliche Träger. Für die Einführung im Haus gibt es passend dazu die Microsoft 365 Schulung für kirchliche Träger.