Entra-ID-Tenant-Überprüfung für kirchliche Träger: Was die Diagnostiker-Überprüfung zum Festpreis liefert

Es gibt in fast jedem Erstgespräch bei einem kirchlichen Träger einen Moment, der sich immer gleich anfühlt. Man sitzt zu dritt oder zu viert zusammen — IT-Leitung, Verwaltungsleitung, vielleicht die örtlich Beauftragte für den Datenschutz —, der Kaffee ist okay, die Stimmung ist freundlich, und dann stellst du eine völlig harmlose Frage: Wie viele Konten in eurem Tenant haben eigentlich die Rolle Globaler Administrator?

Die Antwort ist selten null. Sie ist erstaunlich oft auch nicht zwei. Sie ist in aller Regel eine Zahl, die niemand im Raum vorher kannte, und sie kommt nicht als Zahl, sondern als Satz: „Das müsste ich nachschauen." Fünf Minuten später schaut jemand nach, und dann gibt es eine kurze, sehr konzentrierte Stille. Weil in der Liste ein Systemhaus steht, das seit drei Jahren nicht mehr für euch arbeitet. Weil da ein Konto mit dem Namen „admin2" auftaucht, das niemand angelegt haben will. Weil ein Pfarrer draufsteht, der seit anderthalb Jahren im Ruhestand ist und den Zugang damals bekommen hat, weil er sich „ein bisschen mit Computern auskennt".

Das ist kein Zeichen von Schlamperei. Es ist die völlig normale Folge davon, dass Microsoft 365 bei kirchlichen Trägern fast nie als Projekt eingeführt wurde, sondern als Reihe von Notwendigkeiten: erst die Pandemie und Teams, dann die Kita-Verwaltung, dann der Kirchenkreis, dann das diakonische Werk, das eigentlich einen eigenen Tenant wollte und dann doch nicht, dann der Dienstleisterwechsel. Jede dieser Etappen hat Spuren hinterlassen. Die Spuren hat nie jemand zusammengetragen.

Genau dafür gibt es die Diagnostiker-Überprüfung: eine strukturierte, werkzeuggestützte Bestandsaufnahme deines Entra-ID-Tenants, lesend durchgeführt, zum Festpreis, mit einem Ergebnisdokument, das Befunde nach kritisch, mittel und niedrig sortiert — und zu jedem Befund sagt, wo du klicken musst, um ihn loszuwerden. Kein Werkzeugverkauf, kein Dauerprojekt, kein Beratungsabonnement. Ein Blick, ein Dokument, eine Reihenfolge.

Dieser Beitrag gehört zur Reihe Microsoft 365 in Kirche, Diakonie und Caritas. Dort findest du die Einordnung, warum kirchliche Träger bei Microsoft 365 in einigen Punkten tatsächlich anders arbeiten müssen als Kommune und Mittelstand — und in vielen anderen Punkten eben gerade nicht.

FAKTEN · Worum es hier geht — und worum nicht

Eine Tenant-Überprüfung ist keine Sicherheitszertifizierung, kein Penetrationstest und keine Datenschutz-Folgenabschätzung. Sie ist die Inventur, die vor all dem kommen sollte und die in der Praxis übersprungen wird, weil niemand weiß, wie man sie anfängt.

Sie beantwortet eine einzige Frage vollständig: Was ist in diesem Tenant eigentlich konfiguriert — und wo weicht das von dem ab, was für einen kirchlichen Träger vertretbar ist?

Warum eine Tenant-Überprüfung bei kirchlichen Trägern besonders viel findet

Man könnte meinen, ein Tenant ist ein Tenant. Technisch stimmt das auch. Was sich unterscheidet, ist die Organisationsgeschichte, die in ihn hineingelaufen ist — und die ist bei kirchlichen Trägern mit einer Zuverlässigkeit unübersichtlich, die fast schon wieder beruhigend ist. Vier Ursachen tauchen immer wieder auf.

Gewachsene Strukturen: „historisch“ ist ein freundliches Wort

Ein evangelischer Kirchenkreis mit vierzig Gemeinden, drei Kitas in eigener Trägerschaft und einer Verwaltungsstelle hat selten einen Tenant, der von Anfang an so gedacht war. Er hat einen Tenant, der mit dem Kirchenkreisamt angefangen hat, dann Gemeinden aufgenommen hat, weil das günstiger war als eigene Lösungen, dann eine Jugendeinrichtung, dann die Friedhofsverwaltung. Auf katholischer Seite dasselbe Muster: Das Generalvikariat hat einen Tenant, die Dekanate haben Zugänge bekommen, ein Caritasverband auf Kreisebene wollte mitmachen, drei Kirchengemeinden sind aus einer Fusion dazugekommen und haben ihre alten Postfächer mitgebracht.

Jede dieser Aufnahmen war eine Einzelentscheidung, getroffen unter Zeitdruck, meist von einer Person, oft ohne schriftliches Konzept. Und jede hat eine Konfiguration hinterlassen: eine Ausnahmeregel, eine zusätzliche Rolle, eine Domäne, eine Gruppe, die „vorerst“ offen bleiben musste. Das Wort „vorerst“ ist in der IT das haltbarste Lebensmittel überhaupt.

Dienstleisterwechsel: das Erbe, das im Tenant bleibt

Kirchliche Träger wechseln ihre Systemhäuser seltener als Unternehmen, aber wenn sie wechseln, dann gründlich — nach einer Ausschreibung, nach einem Trägerwechsel, nach einer Fusion von Kirchenkreisen oder nach einer Verbundbildung in der Diakonie. Beim Wechsel werden Verträge übergeben, Geräte übergeben, Passwortlisten übergeben. Was fast nie übergeben wird, ist eine vollständige Liste der Zugänge, die der alte Dienstleister im Tenant hatte.

Das ist keine Böswilligkeit. Der alte Dienstleister hat über die Jahre Konten, Gastzugänge, App-Registrierungen und Partnerbeziehungen angelegt, weil sie für irgendetwas gebraucht wurden. Niemand hat mitgeschrieben. Beim Abschied denkt man an die Rechnungen, nicht an das Dienstkonto für die Backup-Überwachung von 2019. In einem katholischen Krankenhausverbund mit mehreren Standorten haben wir einmal eine App-Registrierung gefunden, die weitreichende Leserechte auf alle Postfächer hatte und deren Geheimnis vier Jahre zuvor von einem Dienstleister erzeugt worden war, den es in dieser Form nicht mehr gab. Das Geheimnis war noch gültig. Die Registrierung stand in keiner Dokumentation.

WARNUNG · Der Klassiker beim Dienstleisterwechsel

Der abgebende Dienstleister verliert den Zugriff auf die Konten, die im Vertrag standen. Er behält ihn bei allem, was daneben entstanden ist: Gastkonten mit privaten Adressen, Dienstkonten ohne Besitzerangabe, App-Registrierungen mit langlebigen Geheimnissen, delegierte Administratorbeziehungen aus der Partnerverwaltung.

Die Überprüfung listet genau diese Objekte auf — nicht als Vorwurf an irgendjemanden, sondern als Aufräumliste.

Ehrenamt: die Konten, die niemandem so richtig gehören

Hier liegt der Unterschied zur Kommune, und zwar ein echter. Eine Stadtverwaltung hat Beschäftigte, Auszubildende und gelegentlich externe Projektkräfte. Eine Kirchengemeinde hat dazu ein Presbyterium oder einen Kirchenvorstand, einen Pfarrgemeinderat, Chorleitungen, Lektorinnen und Lektoren, Küsterdienste, Konfirmandenarbeit, Besuchsdienste, einen Förderverein und drei Menschen, die den Gemeindebrief machen. Niemand davon steht auf einer Gehaltsliste. Alle brauchen irgendwann Zugriff auf irgendetwas.

Das Ergebnis im Tenant sind Konten, deren Lebenszyklus an keine Personalabteilung gekoppelt ist. Wenn eine Mitarbeiterin geht, merkt es die Personalstelle. Wenn ein Presbyterium neu gewählt wird, merkt es im Zweifel niemand im Tenant. Die Gastkonten der vorherigen Amtsperiode bleiben liegen, mitsamt ihren Mitgliedschaften in Teams, in denen Protokolle mit Personalangelegenheiten und Bauvorhaben liegen.

Wie man Ehrenamtliche sauber aufnimmt — Gastzugang, eigenes Konto oder bewusst gar nichts — ist ein eigenes Thema; ausführlich steht es in Ehrenamtliche in Microsoft 365: Gastzugang, eigene Konten, geteilte Postfächer oder besser gar nichts?. Für die Überprüfung zählt zunächst nur: Wie viele sind es, seit wann sind sie da, und wo kommen sie hin?

Nachweispflicht: Die Aufsicht fragt nicht nach deinem Bauchgefühl

Kirchliche Träger unterliegen nicht der DSGVO-Aufsicht der Länder, sondern einer eigenen Rechtsordnung mit eigener Aufsicht. Auf evangelischer Seite ist das das EKD-Datenschutzgesetz mit dem Beauftragten für den Datenschutz der EKD und den regionalen Datenschutzaufsichten, auf katholischer Seite das Gesetz über den Kirchlichen Datenschutz mit den Diözesandatenschutzbeauftragten und den gemeinsamen Datenschutzzentren. Inhaltlich liegen beide Gesetze nah an der DSGVO — sie sind aber eigenständige Gesetze mit eigener Paragrafenzählung, eigenen Auslegungshilfen und eigenen Prüfschwerpunkten.

Für eine Tenant-Überprüfung relevant sind vor allem drei Pflichten, die in beiden Rechtskreisen bestehen. Das Verzeichnis von Verarbeitungstätigkeiten ist im DSG-EKD in § 31 geregelt, im KDG ebenfalls in § 31. Die Pflicht zu geeigneten technischen und organisatorischen Maßnahmen steht im DSG-EKD in § 27, im KDG in § 26. Die Auftragsverarbeitung regelt das DSG-EKD in § 30, das KDG in § 29. Dazu kommt die Nachweispflicht aus den Verarbeitungsgrundsätzen: Die verantwortliche Stelle muss die Einhaltung nicht nur sicherstellen, sondern belegen können.

Und genau dort wird es unangenehm. Wenn die Aufsicht — ob auf Beschwerde hin oder anlasslos — fragt, welche technischen und organisatorischen Maßnahmen ihr für euren Microsoft-365-Tenant getroffen habt, ist die Antwort „wir haben MFA aktiviert“ keine Antwort. Die Antwort ist ein Dokument, das sagt, für welchen Anteil der Konten welche Authentifizierungsmethode registriert ist, welche Ausnahmen es gibt, wer sie beschlossen hat und wann sie überprüft wurden. Genau so ein Dokument fällt bei einer Überprüfung nebenbei ab.

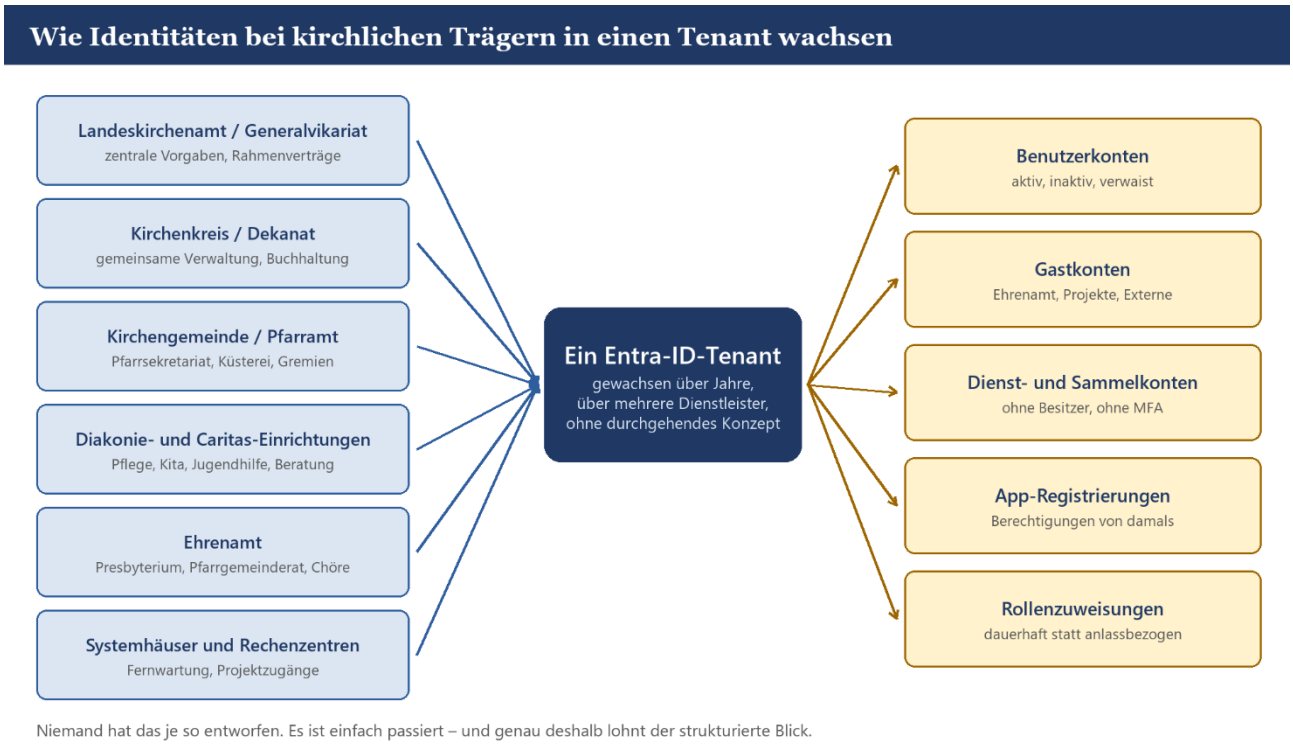
FAKTEN · Verifizierte Fundstellen, die in der Praxis gebraucht werden

Evangelisch: Verzeichnis von Verarbeitungstätigkeiten § 31 DSG-EKD, Sicherheit der Verarbeitung § 27 DSG-EKD, Auftragsverarbeitung § 30 DSG-EKD, Meldung von Schutzverletzungen an die Aufsicht § 32 DSG-EKD (unverzüglich), Datenschutz-Folgenabschätzung § 34 DSG-EKD.

Katholisch: Verzeichnis von Verarbeitungstätigkeiten § 31 KDG, technische und organisatorische Maßnahmen § 26 KDG, Verarbeitung im Auftrag § 29 KDG, Meldung an die Datenschutzaufsicht § 33 KDG (unverzüglich, möglichst binnen 72 Stunden), Datenschutz-Folgenabschätzung § 35 KDG.

Der Befundbericht einer Tenant-Überprüfung ersetzt keines dieser Dokumente. Er liefert aber die

technischen Angaben, ohne die sie nicht befüllbar sind.



Skizze 1: Aus wie vielen Richtungen Identitäten in den Tenant eines kirchlichen Trägers hineinlaufen — und was am anderen Ende liegen bleibt.

Kommt dazu, dass die Zuständigkeit bei kirchlichen Trägern selten so eindeutig ist wie im Organigramm. Eine Landeskirche verantwortet den Tenant, aber die Kirchengemeinden sind eigene juristische Personen. Ein Bistum stellt die Infrastruktur, aber der Caritasverband ist ein eigener Träger mit eigener Geschäftsführung. Wer ist dann verantwortliche Stelle? Diese Frage muss vor der Überprüfung geklärt sein, nicht danach — sonst weiß am Ende niemand, wer den Aktionsplan beschließt.

Wenn diese Frage bei euch noch offen ist, hilft Ein Tenant oder viele? Kirchengemeinde, Kirchenkreis, Landeskirche, Bistum und die Frage der Tenant-Architektur weiter. Und die Grundlagen der Identitätsverwaltung zwischen Landeskirche, Verband, Träger und Einrichtung stehen in Entra ID für kirchliche Träger: Identitäten zwischen Landeskirche, Verband, Träger und Einrichtung — dieser Beitrag hier setzt darauf auf und schaut nach, was davon in deinem Tenant tatsächlich umgesetzt ist.

Was wirklich anders ist als in der Kommune

Es lohnt sich, hier ehrlich zu sein, weil die Abgrenzung sonst zur Folklore wird. Der überwiegende Teil einer Tenant-Überprüfung ist bei einem Kirchenkreis genau dasselbe wie bei einem Stadtwerk: Rollen zählen, MFA prüfen, Altprotokolle suchen. Unterschiedlich sind wenige, dafür sehr konkrete Punkte.

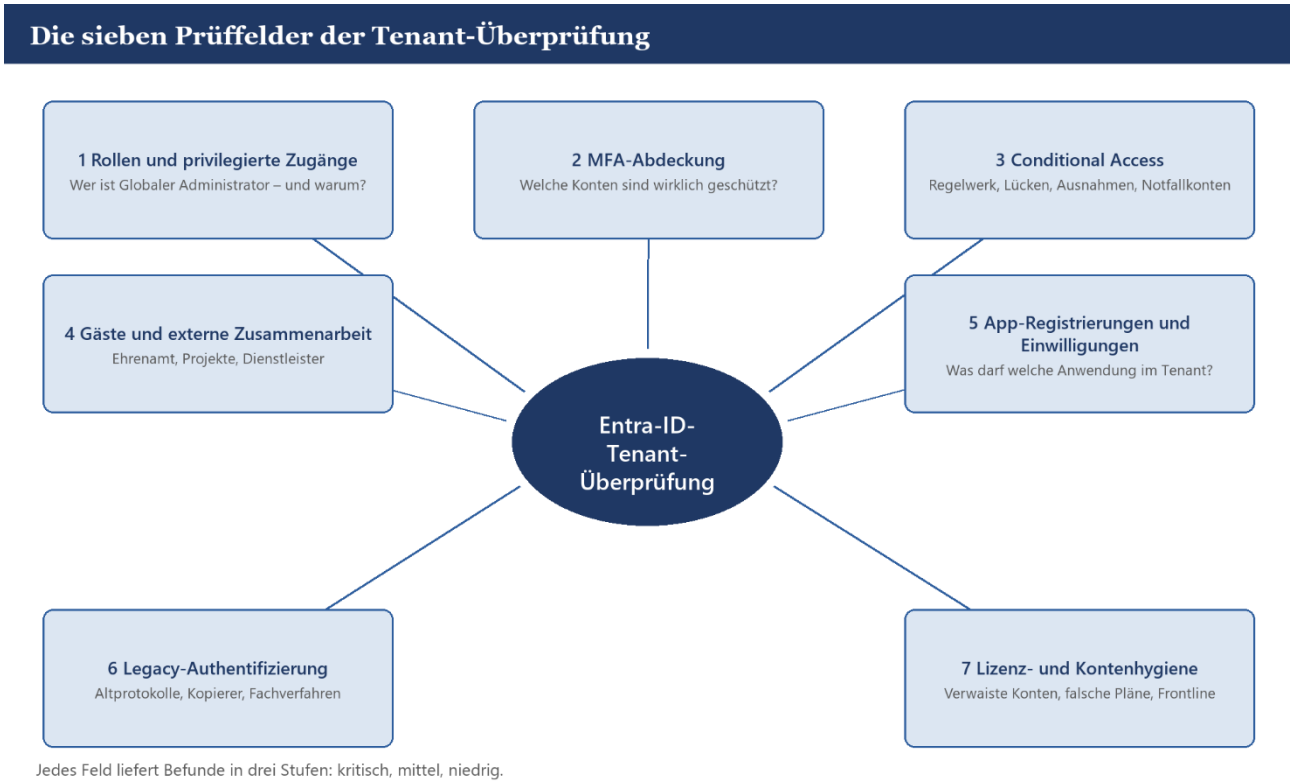
Thema	Kommunale Verwaltung	Kirchlicher Träger
Rechtsgrundlage	DSGVO und Landesdatenschutzgesetz	DSG-EKD oder KDG als eigenständige kirchliche Gesetze
Aufsicht	Landesbeauftragte für Datenschutz	BfD EKD und regionale Aufsichten bzw. Diözesandatenschutzbeauftragte und

Thema	Kommunale Verwaltung	Kirchlicher Träger
		Datenschutzzentren
Beteiligung der Beschäftigten	Personalrat nach Personalvertretungsrecht	Mitarbeitervertretung nach MVG-EKD oder MAVO, Dienstvereinbarung statt Dienstvereinbarung nach LPVG
Besonders schutzbedürftige Inhalte	Sozialdaten, Meldedaten, Ordnungsdaten	zusätzlich Seelsorge- und Beichtgeheimnis, Klientendaten in Beratung, Pflege und Jugendhilfe, Gemeindegliederdaten aus dem Meldewesen
Nutzerkreis	Beschäftigte und externe Projektkräfte	zusätzlich Ehrenamt in Gremien, Kirchenmusik, Jugendarbeit und Besuchsdiensten
Trägerlandschaft	eine Gebietskörperschaft mit Eigenbetrieben	Landeskirche oder Bistum, Kirchenkreis oder Dekanat, Gemeinden, Diakonie- und Caritasträger — oft mehrere juristische Personen in einem Tenant
Alles Übrige	normales Microsoft 365	normales Microsoft 365

Tabelle 1: Wo die Abgrenzung zur Kommune wirklich trägt — und wo sie aufhört. Die letzte Zeile ist ernst gemeint.

Die Prüffelder: Was angeschaut wird

Eine Überprüfung, die überall ein bisschen schaut, findet überall ein bisschen was und hilft niemandem. Deshalb arbeitet die Diagnostiker-Überprüfung mit einem festen Satz Prüffelder. Der Vorteil von festen Feldern: Du bekommst beim zweiten Durchlauf in zwölf Monaten vergleichbare Zahlen und kannst gegenüber Geschäftsführung, Presbyterium oder Verwaltungsrat belegen, dass sich etwas bewegt hat.



Skizze 2: Die sieben Prüffelder. Jedes liefert Befunde in drei Stufen — und jeder Befund bekommt einen Aktionsschritt.

Rollen und privilegierte Zugänge

Erste Frage, immer: Wer ist Globaler Administrator, und warum? Microsoft empfiehlt seit Jahren, diese Rolle auf eine sehr kleine Zahl von Konten zu begrenzen und für den Alltag stattdessen mit stärker eingegrenzten Rollen zu arbeiten — Exchange-Administration, Teams-Administration, Benutzerverwaltung, Helpdesk. In der Praxis bei kirchlichen Trägern sieht man das Gegenteil: Die Rolle wird vergeben, weil sie funktioniert, und Rollen, die funktionieren, nimmt niemand wieder weg.

Geprüft wird deshalb nicht nur die Anzahl, sondern der Zuschnitt: Sind die hochprivilegierten Konten reine Administrationskonten oder gleichzeitig Postfächer, mit denen jemand täglich Mails liest? Gibt es Notfallzugänge, die bewusst von den Anmelderichtlinien ausgenommen sind — und sind sie dokumentiert, hinterlegt und überwacht, oder ist das einfach ein Konto ohne MFA? Haben externe Personen dauerhaft Rollen, die sie nur projektweise bräuchten?

MFA-Abdeckung — die Zahl, die niemand kennt

„Wir haben MFA“ ist eine Aussage über eine Absicht, nicht über einen Zustand. Die belastbare Frage lautet: Für welchen Anteil der aktiven Konten ist tatsächlich eine starke Authentifizierungsmethode registriert, und bei welchen greift beim Anmelden auch wirklich eine Regel, die sie verlangt? Diese beiden Zahlen sind nicht dieselbe, und sie liegen bei gewachsenen Tenants oft erschreckend weit auseinander.

Dazu kommt eine Altlast, die in kirchlichen Tenants überdurchschnittlich häufig steckt: die alte Konfiguration pro Benutzer. Microsoft empfiehlt inzwischen ausdrücklich, diese benutzerbezogene MFA-Konfiguration zugunsten von Conditional Access aufzugeben, weil sich nur dort steuern lässt, wann eine zweite Stufe wirklich verlangt wird. Wo beides parallel existiert, entstehen Zustände, die niemand mehr erklären kann.

Die Rahmenbedingungen haben sich ohnehin verschoben: Microsoft hat die mehrstufige Authentifizierung für Anmeldungen an den Verwaltungsportalen verpflichtend gemacht, die Durchsetzung für das Azure-Portal wurde im März 2025 auf alle Tenants ausgerollt, die zweite Phase für Verwaltungsoperationen über Kommandozeile, PowerShell, Schnittstellen und Automatisierungswerkzeuge begann ab Oktober 2025. Wer noch Skripte oder Automatisierungen mit reinen Kennwortanmeldungen betreibt, merkt das spätestens jetzt. In der Überprüfung fällt so etwas auf, bevor am Montagmorgen die Lohnbuchhaltung stillsteht.

WICHTIG · Zwei Zahlen, die im Ergebnisdokument stehen sollten

- **Registrierungsquote:** Anteil der aktiven Konten mit mindestens einer phishing-resistenten oder zumindest starken Methode.
- **Durchsetzungsquote:** Anteil der Anmeldungen, bei denen eine Regel die zweite Stufe auch tatsächlich erzwingt — inklusive der Liste aller Ausnahmen.
- **Differenz:** genau diese Lücke ist das, was ein Angreifer sucht.

Conditional Access: das Regelwerk und seine Löcher

Conditional Access ist das Werkzeug, mit dem sich Anmeldebedingungen differenzieren lassen — anders für das Pfarrbüro als für den Pflegedienst, anders für Verwaltungskonten als für Ehrenamtliche. Es setzt eine Lizenzstufe voraus, die viele kirchliche Träger haben, ohne es zu wissen, weil sie in den Nonprofit-Angeboten mitkommt oder in einem E3- oder Business-Premium-Plan steckt.

Geprüft wird das Regelwerk als Ganzes, nicht Regel für Regel: Greifen die Regeln auf alle relevanten Anwendungen oder nur auf einige? Gibt es Regeln im Berichtsmodus, die seit zwei Jahren im Berichtsmodus stehen, weil sich niemand getraut hat, sie scharf zu schalten? Sind Ausnahmegruppen gepflegt, oder sind sie über die Jahre von drei auf achtzig Konten gewachsen? Und existieren überhaupt Notfallkonten, oder sperrt euch die nächste falsch gesetzte Regel komplett aus dem eigenen Tenant aus?

Ergänzend schaut die Überprüfung auf die von Microsoft selbst bereitgestellten Regeln: Microsoft hat in berechtigten Tenants Conditional-Access-Regeln im Berichtsmodus angelegt, unter anderem für die Anmeldung an Verwaltungsportalen und für Konten mit alter benutzerbezogener MFA-Konfiguration. Diese Regeln sind als Vorschlag gedacht und sollten bewusst übernommen, angepasst oder abgelehnt werden — nicht schweigend ignoriert.

Gäste und externe Zusammenarbeit

Wie viele Gastkonten hat euer Tenant? Bei einem diakonischen Werk in einer Großstadt war die geschätzte Zahl „vielleicht dreißig“. Die tatsächliche Zahl lag im hohen dreistelligen Bereich, davon über die Hälfte ohne Anmeldung in den letzten zwölf Monaten. Das ist kein Einzelfall, das ist der Normalfall, sobald eine Organisation ein paar Jahre mit Teams arbeitet und Einladungen an Kooperationspartner, Fachstellen, Beratungsgremien und Ehrenamtliche hinausgehen.

Geprüft wird, wer überhaupt einladen darf, ob Einladungen auf bestimmte Domänen begrenzt sind, welche Rechte Gäste im Verzeichnis haben, wie lange sie ohne Anmeldung bestehen bleiben und in welchen Teams sie Mitglied sind. Der unangenehmste Befund ist regelmäßig nicht die Zahl, sondern die Verteilung: ein einzelnes Gastkonto in einem Team, in dem der Vorstand einer diakonischen Einrichtung seine Aufsichtsratsunterlagen ablegt.

App-Registrierungen und erteilte Einwilligungen

Das ist das Prüffeld, bei dem in Erstgesprächen die Augenbrauen hochgehen, weil die wenigsten IT-Leitungen es je angesehen haben. Jede Anwendung, die auf euren Tenant zugreift — das Terminbuchungstool der Beratungsstelle, die Spendensoftware, das Belegungsprogramm der Kita, das Scan-Zusatzprogramm des Kopierers, die App eines früheren Praktikanten —, hinterlässt eine Registrierung mit Berechtigungen und in vielen Fällen ein Geheimnis oder ein Zertifikat.

Die Überprüfung listet auf: welche Registrierungen existieren, welche Berechtigungen sie haben, ob es sich um weitreichende Rechte auf Postfächer, Dateien oder das Verzeichnis handelt, wer die Einwilligung erteilt hat, wann Geheimnisse ablaufen — und welche längst abgelaufen oder im Gegenteil viel zu langlebig sind. Dazu die Frage, ob Nutzerinnen und Nutzer in eurem Tenant eigenständig Anwendungen zustimmen dürfen. Wenn ja: Dann hat faktisch jede Person in der Kita-Verwaltung eine Freigabeentscheidung getroffen, die eigentlich bei der IT-Leitung liegt.

WARNUNG · Warum dieses Prüffeld vor jedem Copilot-Rollout kommt

Anwendungen mit weitreichenden Leserechten auf Postfächer und Dateien sind schon für sich ein Risiko. In Verbindung mit einer Suchassistenz, die Inhalte über Standortgrenzen hinweg zusammenführt, wird daraus ein Oversharing-Problem mit Ansage.

Wer Copilot in einer diakonischen oder caritativen Einrichtung einführen will, sollte die App-Landschaft vorher kennen — nicht hinterher.

Ausführlich dazu: Copilot in Kirche und Diakonie: Nutzen, Grenzen, Oversharing und die Copilot-Überprüfung vor dem Rollout.

Legacy-Authentifizierung und Altprotokolle

Alte Anmeldeverfahren ohne zweite Stufe sind seit Jahren der bequemste Weg in einen Tenant. Microsoft hat die klassische Kennwortauthentifizierung in Exchange Online über mehrere Jahre abgeschaltet; der Vorgang war Ende 2022 im Wesentlichen abgeschlossen, mit der authentifizierten Client-Einlieferung per SMTP als letzter Ausnahme. Auch diese Ausnahme ist inzwischen beendet — Microsoft hat die Abschaltung für die SMTP-Client-Einlieferung auf Ende April 2026 terminiert. Wer bis dahin nicht auf moderne Authentifizierung umgestellt hat, merkt es daran, dass Geräte und Fachverfahren aufhören, Mails zu verschicken.

Und genau dort sitzen bei kirchlichen Trägern die Überraschungen: der Multifunktionskopierer im Pfarramt, der Scans per Mail verschickt. Die Alarmanlage im Gemeindehaus. Die Pflegesoftware, die Dienstpläne versendet. Das Spendenprogramm, das Zuwendungsbestätigungen verschickt. Das Gemeindebriefsystem. Die Überprüfung sucht diese Anmeldungen in den Protokollen und ordnet sie zu, bevor jemand vor dem stummen Kopierer steht und niemand mehr weiß, woran es liegt.

Lizenz- und Kontenhygiene

Das unspektakulärste Prüffeld und das mit dem verlässlichsten Ergebnis: Es bezahlt sich selbst. Bei kirchlichen Trägern findet sich regelmäßig eine Mischung aus zugewiesenen, aber ungenutzten Lizenzen, aus Konten ausgeschiedener Personen, die weiter lizenziert sind, aus Vollplänen für Menschen, die einen Frontline-Arbeitsplatz in Kita oder Pflege haben, und aus Nonprofit-Kontingenten, die nicht ausgeschöpft werden, weil niemand weiß, dass es sie gibt.

Geprüft wird der Kontenbestand insgesamt: aktive Konten ohne Anmeldung seit Monaten, deaktivierte Konten mit gültiger Lizenz, Sammelkonten ohne benannten Verantwortlichen, Postfächer ohne zugeordnete Person. Jedes dieser Objekte ist gleichzeitig ein Kostenpunkt und eine Angriffsfläche — eine ungewöhnlich angenehme Kombination, weil hier ausnahmsweise Sparsamkeit und Sicherheit in dieselbe Richtung zeigen.

Die Befundtabelle im Überblick

Prüffeld	Typischer Befund bei kirchlichen Trägern	Risiko
Rollen und privilegierte Zugänge	Zu viele dauerhafte Globale Administratoren; Rollen bei ausgeschiedenen Personen, früheren Systemhäusern und technikaffinen Ehrenamtlichen; Administrationsrechte auf Alltagskonten mit Postfach	Kritisch — ein übernommenes Konto reicht für den gesamten Tenant
MFA-Abdeckung	Registrierung deutlich höher als Durchsetzung; Sammel- und Dienstkonten grundsätzlich ausgenommen; alte benutzerbezogene MFA-Konfiguration parallel zu Conditional Access	Kritisch bis mittel — Kennwortangriffe treffen genau die Lücke
Conditional Access	Regeln seit Jahren im Berichtsmodus; gewachsene Ausnahmegruppen; keine dokumentierten Notfallkonten; von Microsoft vorgeschlagene Regeln unbeachtet	Mittel bis kritisch — je nachdem, ob die Lücke Verwaltungskonten trifft
Gäste und externe Zusammenarbeit	Deutlich mehr Gastkonten als vermutet; Gäste aus abgeschlossenen Projekten und früheren Amtsperioden von Presbyterium oder Pfarrgemeinderat; Gäste in Gremienteams mit Personalbezug	Mittel — hoch, sobald ein Gast in einem Gremien- oder Beratungsteam sitzt
App-	Registrierungen ohne benannten Besitzer;	Kritisch — Zugriff ohne

Prüffeld	Typischer Befund bei kirchlichen Trägern	Risiko
Registrierungen und Einwilligungen	weitreichende Postfach- oder Dateirechte für Fachanwendungen; langlebige Geheimnisse aus Dienstleisterzeiten; Nutzerzustimmung uneingeschränkt erlaubt	Anmeldung, ohne zweite Stufe, ohne Auffälligkeit
Legacy-Authentifizierung	Kopierer, Alarmanlagen, Pflege- und Spendensoftware mit reiner Kennwortanmeldung; SMTP-Einlieferung als Dauerprovisorium	Kritisch — und zusätzlich ein Betriebsrisiko durch die Abschaltung
Lizenz- und Kontenhygiene	Lizenzen bei ausgeschiedenen Personen; Vollpläne für Frontline-Arbeitsplätze in Kita und Pflege; ungenutzte Nonprofit-Kontingente; Sammelkonten ohne Verantwortliche	Niedrig bis mittel — Kosten, Angriffsfläche und unklare Zuständigkeit
Protokollierung und Nachweis	Anmeldeprotokolle nur in der Standardaufbewahrung, keine Auslagerung; keine Dokumentation, warum welche Ausnahme besteht	Mittel — bei einem Vorfall fehlt genau der Zeitraum, den man braucht

Tabelle 2: Prüffeld, typischer Befund und Risiko. Keine dieser Zeilen ist erfunden; alle stammen aus wiederkehrenden Mustern bei kirchlichen Trägern.

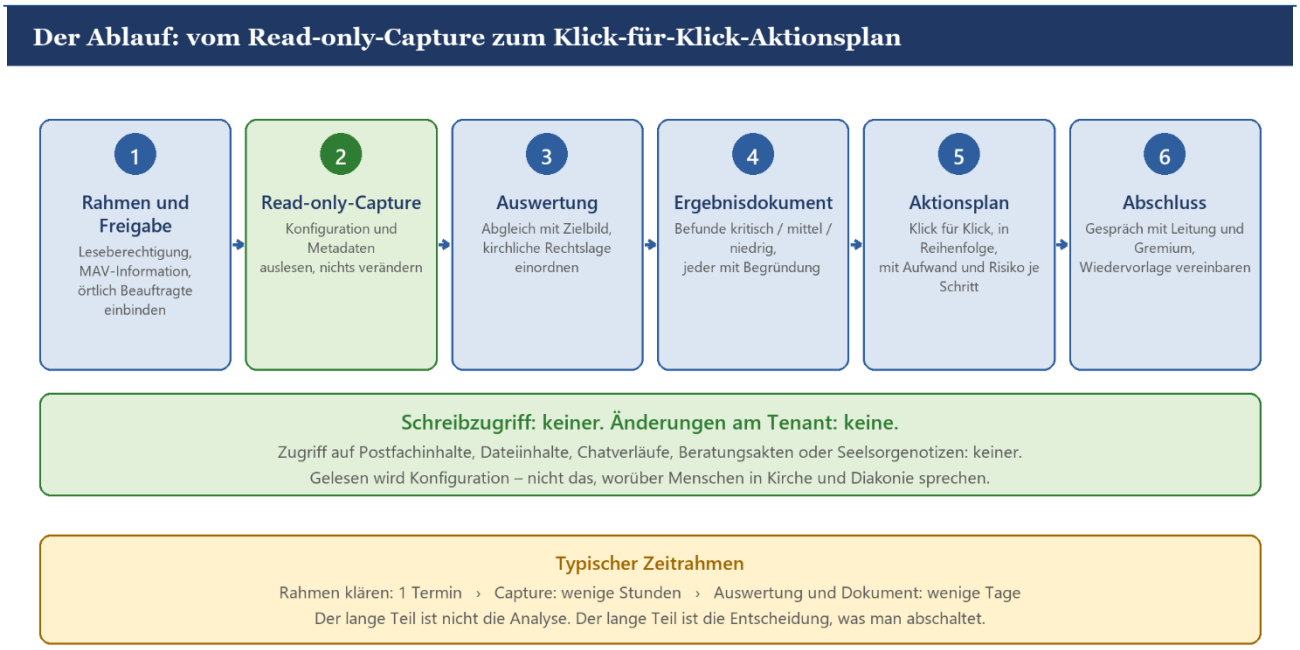
TIPP · Ein Hinweis zur Protokollaufbewahrung

Die Aufbewahrungsdauer der Anmelde- und Überwachungsprotokolle in Entra ID hängt an der Lizenzstufe: In der kostenfreien Stufe sind es sieben Tage, mit P1 oder P2 dreißig Tage. Wer längere Zeiträume braucht — und das braucht man bei einem Vorfall regelmäßig —, muss die Protokolle bewusst auslagern.

Für die Meldung einer Schutzverletzung an BfD EKD oder an den Diözesandatenschutzbeauftragten ist das kein Detail, sondern die Grundlage: Ohne Protokolle steht in der Meldung „Umfang unbekannt“, und das ist die Formulierung, die Rückfragen auslöst.

Der Ablauf: vom Read-only-Capture zum Aktionsplan

Der Ablauf ist bewusst kurz und bewusst berechenbar. Eine Überprüfung, die drei Monate dauert, beschreibt am Ende einen Tenant, den es so nicht mehr gibt.



Skizze 3: Sechs Schritte. Der einzige, bei dem etwas am Tenant passiert, ist der, den du selbst umsetzt.

Schritt 1: Rahmen klären, bevor irgendetwas ausgelesen wird

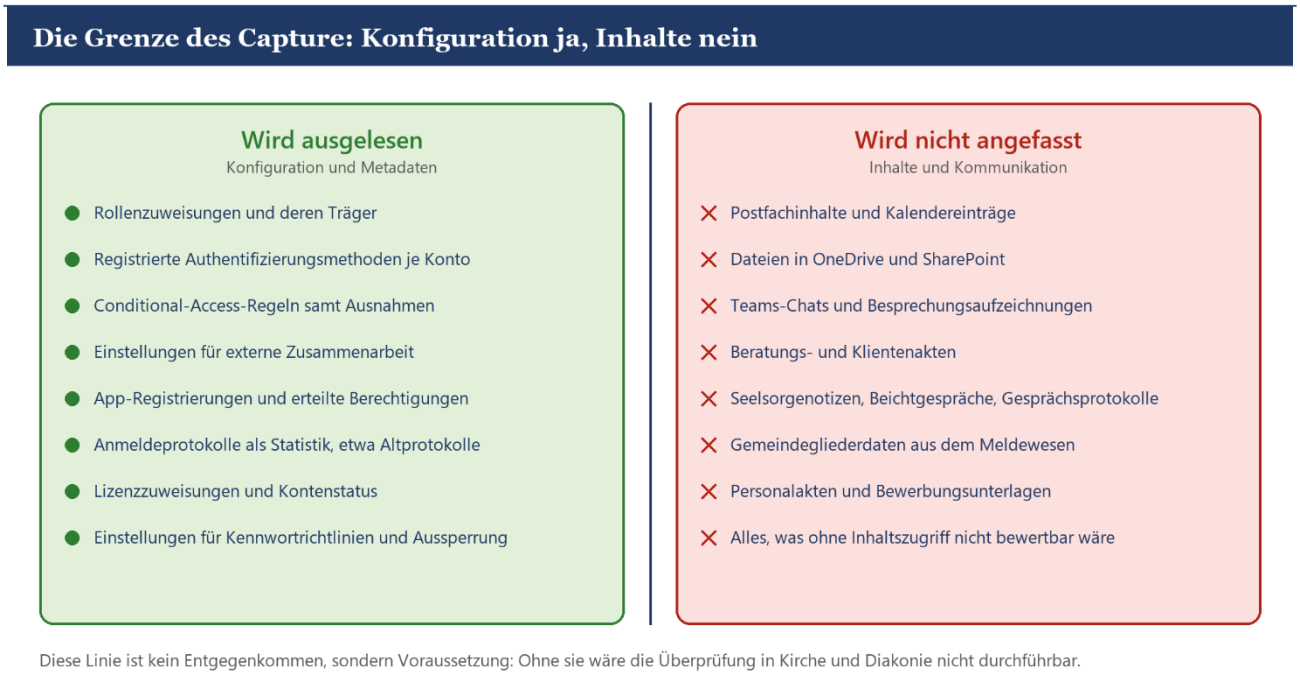
Zuerst wird geklärt, wer verantwortliche Stelle ist, wer die Leseberechtigung erteilt, welche örtlich Beauftragte für den Datenschutz zuständig ist und ob die Mitarbeitervertretung beteiligt werden muss. Das ist kein bürokratischer Vorlauf, sondern der Unterschied zwischen einer verwertbaren Untersuchung und einem Dokument, das später niemand verwenden darf.

In Trägerkonstellationen mit mehreren juristischen Personen in einem Tenant — Kirchenkreis plus Gemeinden, Bistum plus Caritasverband — gehört dazu die Frage, wessen Daten überhaupt in den Bericht dürfen. In der Regel lässt sich das sauber lösen, indem der Bericht auf Ebene von Zahlen und Konfiguration bleibt und personenbezogene Einzelauflistungen nur dort erscheinen, wo sie für die Bereinigung zwingend gebraucht werden — also bei Rollen, Gästen und App-Registrierungen.

Schritt 2: Read-only-Capture

Der eigentliche Erhebungsschritt läuft lesend. Ausgelesen werden Konfiguration und Metadaten über die regulären Verwaltungsschnittstellen — mit einer Berechtigung, die ausschließlich Leserechte umfasst. Es wird nichts geändert, nichts abgeschaltet, nichts „mal eben mitkorrigiert“. Das ist keine Bescheidenheit, sondern Methode: Eine Bestandsaufnahme, die während der Aufnahme den Bestand verändert, ist wertlos.

Ebenso wichtig ist, was nicht erhoben wird. Es gibt keinen Zugriff auf Postfachinhalte, Dateiinhalte, Chatverläufe, Besprechungsaufzeichnungen, Beratungsakten oder Notizen aus der Seelsorge. Diese Grenze ist bei kirchlichen Trägern nicht verhandelbar, und sie ist auch technisch nicht nötig: Alles, was die Überprüfung beantwortet, steht in der Konfiguration.



Skizze 4: Was das Capture liest und was es nicht anfasst. Die rechte Spalte ist der Grund, warum diese Überprüfung in Kirche und Diakonie überhaupt möglich ist.

Warum diese Grenze bei kirchlichen Trägern schärfer verläuft als anderswo, steht ausführlich in Seelsorgegeheimnis und Beichtgeheimnis in Microsoft 365: Was nie in Teams, OneNote oder Copilot landen darf.

Schritt 3: Auswertung und Einordnung

Die Rohdaten allein sind ein Zahlenfriedhof. Der Wert entsteht beim Abgleich mit einem Zielbild — und zwar einem, das zu einem kirchlichen Träger passt und nicht zu einem Softwarekonzern mit eigener Sicherheitsabteilung. Eine Kirchengemeinde mit vier Vollzeitstellen braucht kein rund um die Uhr besetztes Sicherheitszentrum. Sie braucht drei Administratoren statt elf, eine MFA-Durchsetzung ohne Löcher und eine Gästeliste, die jemand kennt.

Bei der Einordnung wird jeder Befund auf zwei Fragen abgeklopft: Erhöht er das Risiko eines tatsächlichen Zugriffs durch Unbefugte? Und berührt er eine Pflicht aus DSG-EKD oder KDG, die im Zweifel gegenüber der Aufsicht belegt werden muss? Befunde, die beides treffen, landen oben.

Schritt 4: Das Ergebnisdokument

Das Ergebnis ist ein Dokument, kein Werkzeugzugang und keine Weboberfläche, die du abonnieren musst. Es gehört dir, du darfst es an deine Aufsicht, deine Gremien, dein Systemhaus oder deine Versicherung weitergeben, ohne jemanden zu fragen.

Bestandteil	Was drinsteht
Kurzfassung für die Leitung	Zwei Seiten, allgemeinverständlich, für Geschäftsführung, Verwaltungsleitung, Presbyterium, Kirchenvorstand oder Verwaltungsrat — ohne Fachvokabular, mit klarer Aussage zur Lage
Kennzahlenblatt	Rollenverteilung, MFA-Registrierung und -Durchsetzung, Gastkonten, App-Registrierungen, Altprotokoll-Anmeldungen, Lizenz- und Kontenstatus — als Zahlen, die beim nächsten Durchlauf vergleichbar sind
Befundliste	Jeder Befund mit Klasse (kritisch, mittel, niedrig), Beschreibung, betroffenen Objekten, Begründung des Risikos und, wo einschlägig, Bezug

Bestandteil	Was drinsteht
	zur Pflicht aus DSG-EKD oder KDG
Aktionsplan	Zu jedem Befund der konkrete Weg: Portal, Menüpunkt, Einstellung, Reihenfolge — Klick für Klick, mit Hinweis auf Nebenwirkungen und geschätztem Aufwand
Beteiligungshinweise	Welche Maßnahmen die Mitarbeitervertretung berühren, welche in die Dokumentation für die Datenschutzaufsicht gehören und welche ausschließlich technischer Betrieb sind
Anhang mit Rohlisten	Vollständige Auflistungen zu Rollen, Gästen und App-Registrierungen als Arbeitsgrundlage für die Bereinigung

Tabelle 3: Lieferumfang der Überprüfung. Die Kurzfassung ist der Teil, der tatsächlich gelesen wird — deshalb steht sie vorn.

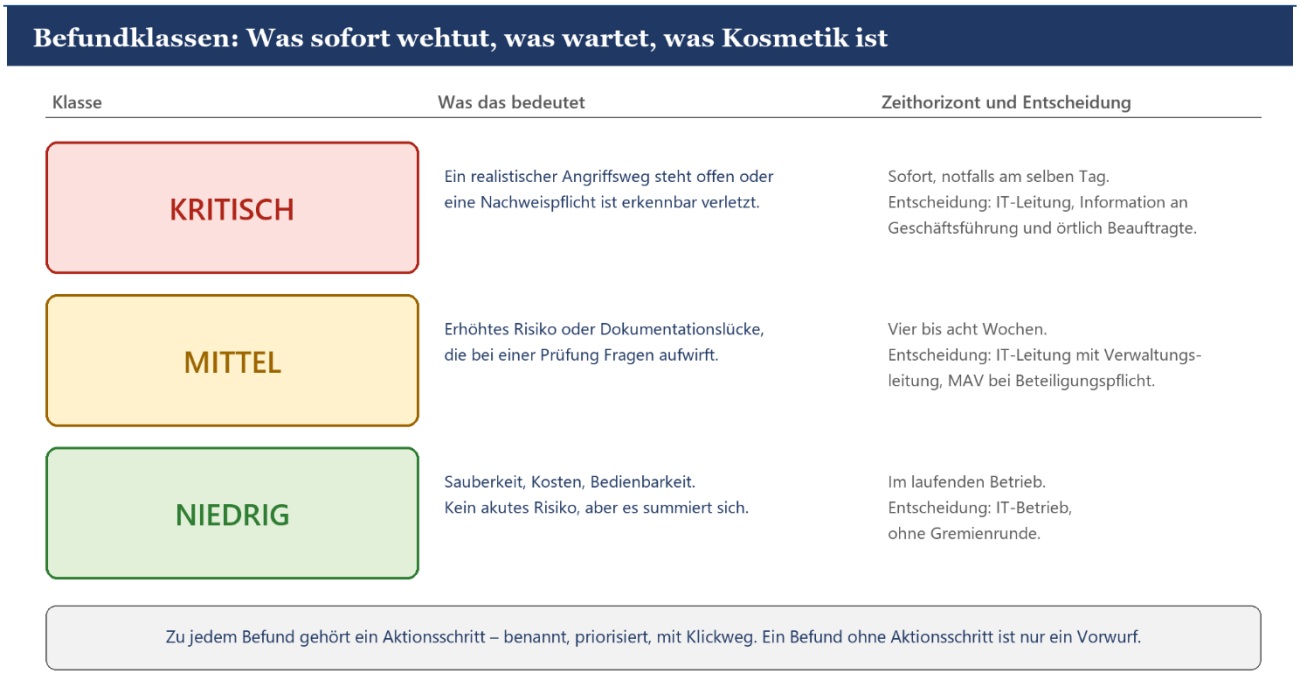
Schritt 5: Der Aktionsplan — Klick für Klick

Der Unterschied zwischen einem Befundbericht und einem nützlichen Befundbericht liegt in dieser einen Eigenschaft: Steht dort, was zu tun ist, oder steht dort nur, was falsch ist? Ein Satz wie „Die MFA-Abdeckung ist unzureichend“ hilft niemandem. Eine Anweisung, in welchem Portal unter welchem Menüpunkt welche Regel angelegt wird, in welcher Reihenfolge, mit welcher Testgruppe und mit welchem Rückfallweg, wenn am Montag das Pfarrbüro nicht mehr hineinkommt — die hilft.

Der Aktionsplan ist deshalb sortiert, nicht alphabetisch, sondern nach Wirksamkeit und Abhängigkeit. Notfallkonten werden vor der MFA-Erzwingung angelegt, nicht danach. Die Altprotokolle werden erst ausgewertet und den Geräten zugeordnet, bevor sie gesperrt werden. Gastkonten werden erst mit Verantwortlichen abgeglichen, bevor sie entfernt werden — sonst fehlt in der nächsten Presbyteriumssitzung der halbe Bauausschuss im Team.

Schritt 6: Abschlussgespräch und Wiedervorlage

Zum Schluss ein Gespräch, in dem die Befunde durchgegangen werden, Fragen geklärt und die kritischen Punkte terminiert werden. Wer will, lädt dazu die örtlich Beauftragte für den Datenschutz und die Mitarbeitervertretung ein; das spart später eine Runde. Und dann wird ein Wiedervorlagetermin vereinbart — üblicherweise zwölf Monate später, weil ein Tenant sich in zwölf Monaten zuverlässig wieder verändert hat.



Skizze 5: Die drei Befundklassen mit Zeithorizont und Entscheidungsebene. Die rechte Spalte verhindert, dass alles in der IT-Leitung hängen bleibt.

TIPP · Die Überprüfung zum Festpreis

Die Diagnostiker-Überprüfung des Entra-ID-Tenants gibt es als abgegrenzte Leistung zum Festpreis: fester Prüfumfang, feste Liefergegenstände, fester Preis, keine Tagessatz-Diskussion und kein Anschlussprojekt, das man vorher unterschreiben muss. Gerade bei kirchlichen Trägern ist das wichtig, weil Haushaltsmittel beschlossen und nicht geschätzt werden — ein Festpreis lässt sich einem Verwaltungsrat, einem Presbyterium oder einer Synode vorlegen, ein Aufwandsrahmen nicht.

- **Umfang:** die sieben Prüffelder plus Protokollierung und Nachweis.
- **Ergebnis:** Kurzfassung für die Leitung, Kennzahlenblatt, Befundliste, Klick-für-Klick-Aktionsplan, Rohlisten.
- **Vorgehen:** lesend, ohne Änderung am Tenant, ohne Zugriff auf Inhalte.

› Microsoft 365 Beratung für kirchliche Träger: Überprüfung, Konzepte und Begleitung zum Festpreis

Mitbestimmung, Datenschutz und Gremien: die Überprüfung sauber aufsetzen

Eine Tenant-Überprüfung ist technisch unspektakulär und organisatorisch sensibel. Wer sie ohne Vorlauf startet, bekommt hinterher eine Diskussion, die sich mit einer Mail vorher hätte vermeiden lassen.

Was die Mitarbeitervertretung wissen muss

Die Überprüfung selbst wertet keine Leistung und kein Verhalten von Beschäftigten aus. Sie schaut auf Konfiguration. Anmeldeprotokolle werden als Statistik betrachtet — wie viele Anmeldungen über Altprotokolle, aus welchen Anwendungen —, nicht als Bewegungsprofil einzelner Personen. Das lässt sich der MAV in zwei Sätzen erklären, und es stimmt auch.

Anders sieht es bei manchen Maßnahmen aus dem Aktionsplan aus. Sobald ein Regelwerk eingeführt wird, das zur Überwachung von Verhalten oder Leistung geeignet ist, greift auf evangelischer Seite die Mitbestimmung nach § 40 MVG-EKD — dort ist die Einführung und Anwendung von Maßnahmen oder technischen Einrichtungen erfasst, die dazu geeignet sind, Verhalten oder Leistung der Beschäftigten zu überwachen. Auf katholischer Seite ist es § 36 Absatz 1 Nummer 9 MAVO, der die Zustimmung der Mitarbeitervertretung zur Einführung und Anwendung technischer Einrichtungen verlangt, die zur Überwachung von Verhalten oder Leistung bestimmt sind. Die kirchliche Rechtsprechung legt „bestimmt“ dabei als „objektiv geeignet“ aus — die Absicht des Dienstgebers ist unerheblich.

Praktisch heißt das: Die Überprüfung selbst ist unproblematisch, der Aktionsplan enthält aber Punkte, bei denen die MAV an Bord gehört. Genau deshalb steht im Ergebnisdokument zu jeder Maßnahme, ob sie eine Beteiligung auslöst. Das ist keine Rechtsberatung — das ist eine Vorsortierung, damit ihr nicht bei jeder einzelnen Einstellung neu diskutiert.

Wie man daraus eine tragfähige Dienstvereinbarung macht — und was üblicherweise hineingehört —, steht in Mitarbeitervertretung und Microsoft 365: MVG-EKD, MAVO, Dienstvereinbarung und Mitbestimmung bei Teams, Copilot und Protokollierung. Für den evangelischen Bereich sieht das MVG-EKD Dienstvereinbarungen ausdrücklich vor; sie sind schriftlich zu fassen und von beiden Seiten zu unterzeichnen.

WICHTIG · Der Satz, der in der MAV-Information stehen sollte

„Die Überprüfung erhebt ausschließlich Konfigurationsdaten und statistische Angaben über Anmeldeverfahren. Es erfolgt kein Zugriff auf Inhalte von Postfächern, Dateien oder Chats und keine Auswertung des Verhaltens einzelner Beschäftigter. Maßnahmen aus dem Aktionsplan, die eine Beteiligung der Mitarbeitervertretung auslösen, sind im Ergebnisdokument gekennzeichnet.“

Dieser Satz hat in der Praxis mehr Sitzungen verkürzt als jede Präsentation.

Die örtlich Beauftragten für den Datenschutz einbinden

Die örtlich Beauftragte für den Datenschutz — auf katholischer Seite die betriebliche oder diözesane Datenschutzbeauftragung — hat an einer solchen Überprüfung ein natürliches Eigeninteresse, weil das Ergebnis genau die Angaben liefert, die im Verzeichnis von Verarbeitungstätigkeiten und in der Beschreibung der technischen und organisatorischen Maßnahmen fehlen. Die Beschreibung nach § 27 DSG-EKD beziehungsweise § 26 KDG ist in vielen Häusern ein Dokument, das einmal geschrieben und nie wieder angefasst wurde, weil niemand die Zahlen hatte, um es fortzuschreiben.

Wenn ihr die Überprüfung von vornherein als Zuarbeit für diese Dokumentation anlegt, bekommt ihr zwei Ergebnisse zum Preis von einem: einen sichereren Tenant und eine Nachweislage, die einer Prüfung standhält. In einer Landeskirche hat das dazu geführt, dass die Beschreibung der Maßnahmen erstmals seit der Einführung aktualisiert wurde — ausgelöst nicht von einer Beanstandung, sondern von einem Kennzahlenblatt.

Was die Aufsicht konkret erwartet und wie ein Prüfgespräch abläuft, steht in Kirchliche Datenschutzaufsicht in der Praxis: Was BfD EKD und Diözesandatenschutzbeauftragte von einem Microsoft-365-Tenant erwarten. Die rechtlichen Grundlagen findest du getrennt nach Konfession in DSG-EKD verständlich: Was das evangelische Datenschutzgesetz für Microsoft 365 konkret bedeutet und KDG verständlich: Microsoft 365 unter dem Kirchlichen Datenschutzgesetz der katholischen Kirche.

Was Leitung und Gremien davon haben

Für Geschäftsführungen, Verwaltungsleitungen, Presbyterien, Kirchenvorstände und Verwaltungsräte ist ein Tenant eine Blackbox. Sie beschließen Haushaltsmittel für etwas, dessen Zustand sie nicht beurteilen können, und sie tragen die Verantwortung, wenn es schiefgeht. Ein Befundbericht mit einer zweiseitigen Kurzfassung ändert daran mehr, als man vermuten würde: Er verwandelt ein diffuses Unbehagen in eine Liste mit Terminen.

Das hat einen angenehmen Nebeneffekt für die IT. Wer jahrelang erfolglos um Budget für Identitätsverwaltung gebeten hat, bekommt mit einem externen Befundbericht plötzlich Gehör — nicht, weil der Bericht klüger wäre, sondern weil er von außen kommt und eine Klassifizierung enthält, die ein Gremium verstehen kann. Das ist unbefriedigend und trotzdem wahr.

WARNUNG · Ein Wort zur Ehrlichkeit gegenüber den Gremien

Ein Befundbericht ist keine Freisprechung und keine Anklageschrift. Wenn er kritische Befunde enthält, heißt das nicht, dass jemand geschlampt hat — es heißt, dass eine gewachsene Umgebung einen Zustand erreicht hat, den niemand bewusst herbeigeführt hat.

Wer den Bericht in der Sitzung als Vorwurf gegen die eigene IT präsentiert, bekommt beim nächsten Mal keinen ehrlichen Bericht mehr, sondern einen gefälligen. Und der ist wertlos.

Was danach passiert — und was ausdrücklich nicht

Die Überprüfung ist kein Projektbeginn

Der häufigste Verdacht im Erstgespräch lautet: Das ist doch nur der Einstieg, damit anschließend ein großes Projekt verkauft wird. Verständlicher Verdacht, denn so funktioniert ein Teil der Branche. Hier funktioniert es anders, und zwar aus einem einfachen Grund: Der Aktionsplan ist so geschrieben, dass eure eigene IT ihn abarbeiten kann. Klick für Klick heißt Klick für Klick.

Es gibt Ausnahmen, ehrlicherweise. Wenn bei der Überprüfung herauskommt, dass eine Tenant-Konsolidierung ansteht, dass ein Verzeichnisabgleich neu aufgesetzt werden muss oder dass ein Regelwerk für vier verschiedene Nutzergruppen von Grund auf entworfen werden soll, dann ist das Arbeit, die über einen Aktionsplan hinausgeht. Aber das steht dann so im Bericht, mit Begründung, und ihr könnt damit auch zu jemand anderem gehen.

Was die Überprüfung nicht leistet

- **Keine Datenschutz-Folgenabschätzung.** Die Überprüfung liefert technische Zuarbeit, aber die Abschätzung nach § 34 DSG-EKD oder § 35 KDG ist ein eigenes Verfahren mit eigener Methodik.
- **Kein Penetrationstest.** Es wird nichts angegriffen, nichts ausprobiert, nichts umgangen. Wer wissen will, ob eine Konfiguration einem Angriff standhält, braucht eine andere Übung.
- **Keine Prüfung der Anwendungsebene.** Berechtigungen in SharePoint, Freigaben in OneDrive und die Konfiguration von Teams sind nicht Teil dieser Überprüfung. Das ist bewusst so — sonst wäre der Festpreis eine Lüge.
- **Keine Bewertung eurer Fachverfahren.** Das Krankenhausinformationssystem, die Pflegedokumentation, die Meldewesen-Anwendung und die Buchhaltung bleiben außen vor. Sie tauchen nur auf, wenn sie sich über Altprotokolle am Tenant anmelden.

- **Keine Aussage über Microsofts Verträge.** Ob eure Auftragsverarbeitung nach DSG-EKD oder KDG richtig aufgesetzt ist, ist eine Vertragsfrage, keine Konfigurationsfrage.

Die Wiedervorlage ist der eigentliche Wert

Eine einmalige Überprüfung ist eine Momentaufnahme. Ihr Wert entsteht beim zweiten Mal, weil dann die Kennzahlen vergleichbar werden. Wenn die Zahl der dauerhaften Globalen Administratoren von elf auf drei gesunken ist, wenn die Durchsetzungsquote der zweiten Anmeldestufe von siebenundsechzig auf neunundneunzig Prozent gestiegen ist und wenn die Zahl der inaktiven Gastkonten von vierhundert auf zwölf gefallen ist, dann hast du etwas, das du einem Verwaltungsrat, einer Synode oder einer Aufsicht zeigen kannst. Und zwar ohne Adjektive.

FAKTEN · Ein realistisches Bild aus der Praxis

Ein Caritasverband auf Kreisebene mit rund sechshundert Konten, verteilt über Verwaltung, zwei Pflegeeinrichtungen, vier Kitas und eine Beratungsstelle. Erste Überprüfung: neun dauerhafte Globale Administratoren, davon zwei bei einem früheren Dienstleister. Zweihundertdreiundsiebzig Gastkonten, davon einhundertneunzig ohne Anmeldung im letzten Jahr. Vierzehn App-Registrierungen, von denen drei niemand zuordnen konnte. Regelmäßige Anmeldungen über Altprotokolle aus zwei Kopierern und einer Dienstplansoftware.

Zwölf Monate später: drei Globale Administratoren, alle mit getrennten Administrationskonten. Achtundzwanzig Gastkonten mit benannten Verantwortlichen. Keine Altprotokoll-Anmeldungen mehr. Und — das war der Punkt, der die Geschäftsführung am meisten gefreut hat — vierundsechzig Lizenzen weniger.

Weiter zum Thema

› Entra ID für kirchliche Träger: Identitäten zwischen Landeskirche, Verband, Träger und Einrichtung — das Zielbild, gegen das die Überprüfung abgleicht

› Ein Tenant oder viele? Kirchengemeinde, Kirchenkreis, Landeskirche, Bistum und die Frage der Tenant-Architektur — wenn der Befund lautet: falsche Grundstruktur

› Ehrenamtliche in Microsoft 365: Gastzugang, eigene Konten, geteilte Postfächer oder besser gar nichts? — für das Prüffeld Gäste

› Mitarbeitervertretung und Microsoft 365: MVG-EKD, MAVO, Dienstvereinbarung und Mitbestimmung bei Teams, Copilot und Protokollierung — für die Beteiligung beim Aktionsplan

› Kirchliche Datenschutzaufsicht in der Praxis: Was BfD EKD und Diözesandatenschutzbeauftragte von einem Microsoft-365-Tenant erwarten — wofür die Kennzahlen gebraucht werden

› Microsoft-365-Lizenzierung für kirchliche Träger: Nonprofit-Angebote, Frontline-Pläne und die Frage, wer überhaupt berechtigt ist — für das Prüffeld Lizenzhygiene

› Microsoft 365 Einführungskonzept für kirchliche Träger: Die Kirchenedition zum Festpreis — wenn aus den Befunden ein Neuaufsatz wird

Häufige Fragen

Braucht unser kleines Pfarramt mit sechs Konten so etwas überhaupt?

Wenn ihr einen eigenen Tenant mit sechs Konten habt und nie ein Dienstleister daran gearbeitet hat, ist der Erkenntnisgewinn überschaubar. Die Realität sieht meist anders aus: Das Pfarramt hängt an einem Tenant des Kirchenkreises oder des Dekanats, in dem noch dreißig andere Stellen sitzen. Dann ist nicht euer Pfarramt der Prüfgegenstand, sondern der Tenant — und der ist groß genug.

Bekommt ihr dabei Zugriff auf unsere Daten?

Auf Konfigurationsdaten und Metadaten: ja, lesend, für die Dauer der Erhebung. Auf Inhalte: nein. Keine Postfächer, keine Dateien, keine Chats, keine Beratungsakten, keine Seelsorgenotizen, keine Gemeindegliederdaten. Die Leseberechtigung wird von euch erteilt, ist auf die benötigten Bereiche beschränkt und wird nach Abschluss entzogen. Die Erhebung ist im Protokoll eures Tenants nachvollziehbar — ihr könnt also selbst prüfen, was gelesen wurde.

Müssen wir die Mitarbeitervertretung vorher beteiligen?

Für die Erhebung selbst ist eine Beteiligung in aller Regel nicht erforderlich, weil weder Verhalten noch Leistung einzelner Personen ausgewertet werden. Eine Information an die MAV ist trotzdem sinnvoll und kostet zehn Minuten. Beteiligungspflichtig werden einzelne Maßnahmen aus dem Aktionsplan, wenn sie technische Einrichtungen einführen, die zur Überwachung geeignet sind — dann greifen § 40 MVG-EKD beziehungsweise § 36 Absatz 1 Nummer 9 MAVO.

Wir haben ein Systemhaus. Ist das nicht dessen Aufgabe?

Teilweise ja. Nur prüft ein Systemhaus ungern die Konfiguration, die es selbst angelegt hat — das ist keine Unterstellung, sondern eine strukturelle Frage. Hinzu kommt, dass die meisten Systemhäuser den kirchlichen Rechtsrahmen nicht im Blick haben und deshalb Befunde nicht einordnen können, die gegenüber BfD EKD oder Diözesandatenschutzbeauftragten relevant sind. Die Überprüfung ist ausdrücklich nicht gegen euer Systemhaus gerichtet; in der Praxis ist es oft dasjenige, das den Aktionsplan anschließend umsetzt.

Warum ein Festpreis und kein Tagessatz?

Weil kirchliche Haushalte beschlossen werden. Ein Kirchenkreis, ein Verwaltungsrat oder ein Trägerverbund kann eine feste Summe in den Haushalt einstellen und freigeben. Einen Aufwandsrahmen mit offenem Ende kann er nicht freigeben, jedenfalls nicht ohne Nachtragsdiskussion. Ein fester Prüfumfang mit festem Preis macht die Überprüfung beschlussfähig — und das ist bei kirchlichen Trägern der eigentliche Engpass, nicht das Geld.

Was, wenn dabei etwas richtig Unangenehmes herauskommt?

Dann steht es im Bericht. Wenn ein Befund den Verdacht begründet, dass bereits ein unbefugter Zugriff stattgefunden hat, wird das sofort besprochen und nicht erst im Abschlussdokument — dann geht es nämlich nicht mehr um Aufräumen, sondern um die Meldepflicht gegenüber der kirchlichen Aufsicht. Das DSG-EKD verlangt die unverzügliche Meldung an die Aufsicht, das KDG nennt dafür ausdrücklich die Frist von möglichst 72 Stunden ab Kenntnis. Beides sind Fristen, die man nicht mit einer Terminfindung verbringt.

Gilt das auch für Träger mit eigenem kirchlichem Rechenzentrum?

Ja, und dort ist es sogar häufig aufschlussreicher. Wenn Teile der Infrastruktur bei einem kirchlichen Rechenzentrum liegen und Microsoft 365 daneben betrieben wird, entstehen Übergaben, Verzeichnisabgleiche und Dienstkonten — und genau an diesen Nahtstellen sammeln sich Befunde. Die Überprüfung betrachtet dabei nur euren Tenant, nicht die Systeme des Rechenzentrums. Aber sie zeigt, was von dort in euren Tenant hineinreicht.

Wie oft sollte man das wiederholen?

Einmal jährlich ist ein guter Takt für einen mittleren Träger, und zusätzlich immer dann, wenn sich etwas Strukturelles ändert: nach einem Dienstleisterwechsel, nach einer Fusion von Kirchenkreisen oder Gemeinden, nach einer Verbundbildung in Diakonie oder Caritas, vor der Einführung einer Suchassistenz wie Copilot und nach einem Sicherheitsvorfall. Die Wiederholung ist deutlich schneller als der erste Durchlauf, weil das Zielbild steht.

Fazit

Ein Entra-ID-Tenant ist kein Gebäude, das man einmal baut und dann bewohnt. Er ist eher ein Gemeindehaus, in dem seit fünfzehn Jahren jede Gruppe irgendwo einen Schlüssel hinterlegt hat — im Blumenkasten, beim Küster, in der Schublade im Jugendraum. Jeder einzelne Schlüssel hatte einen guten Grund. In der Summe weiß niemand mehr, wer hineinkommt. Der Unterschied ist nur: Beim Gemeindehaus merkt man es, wenn nachts Licht brennt.

Die Diagnostiker-Überprüfung ist der strukturierte Blick auf die Schlüssel. Sie läuft lesend, sie fasst keine Inhalte an, sie respektiert die Grenze, die das Seelsorgegeheimnis zieht, und sie endet nicht mit einer Diagnose, sondern mit einem Aktionsplan, den eure eigene IT abarbeiten kann. Sie liefert nebenbei die Zahlen, die im Verzeichnis von Verarbeitungstätigkeiten und in der Beschreibung der technischen und organisatorischen Maßnahmen nach DSG-EKD und KDG fehlen — und damit genau das, wonach die kirchliche Aufsicht fragt, wenn sie fragt.

Der beste Zeitpunkt für eine solche Überprüfung war der Tag nach dem letzten Dienstleisterwechsel. Der zweitbeste ist heute. Der schlechteste ist der Montagmorgen, an dem die Verwaltung eines diakonischen Trägers feststellt, dass jemand anders die Schlüssel bereits gefunden hat — und man dann in der Meldung an die Aufsicht unter „Umfang der Betroffenheit“ schreiben muss, dass man es nicht sagen kann.

Gewachsene Strukturen sind kein Versagen. Sie nicht anzuschauen, schon.