# Privilegierte Konten in der Verwaltungs-IT: Rollen, PIM und der Fall des einen Admins

In fast jeder Verwaltung, die wir betreten, gibt es diesen einen Menschen. Er hat den Tenant vor Jahren angelegt, kennt jede Ausnahme im Verteilerverzeichnis, weiß auswendig, warum die Vergabestelle einen eigenen Freigabepfad hat, und er ist der Grund, warum die Verwaltung überhaupt funktioniert. Er ist ausdrücklich nicht das Problem. Das Problem ist, dass die gesamte handlungsfähige Administration eines Hauses mit siebenhundert Beschäftigten an einem einzigen Benutzerkonto hängt, das alles darf, und an einem einzigen Kalender, in dem irgendwann Jahresurlaub steht.

Verwaltungen sind es gewohnt, Zuständigkeiten sauber zu trennen. Die Kämmerei bucht nicht, was sie selbst anordnet. Die Vergabestelle vergibt nicht an sich selbst. Das Rechnungsprüfungsamt prüft, was andere entschieden haben. In der Aufbauorganisation ist die Funktionstrennung selbstverständlich. In der Berechtigungsstruktur des Microsoft-365-Tenants ist sie es erstaunlich oft nicht. Dort sitzt eine Person mit der Rolle **Globaler Administrator**, die zugleich Postfächer öffnen, Aufbewahrungsrichtlinien abschalten, Konten anlegen, Protokolle löschen und die eigene Genehmigung erteilen kann. Wäre das eine Kassenanordnung, hätte das Rechnungsprüfungsamt längst einen Vermerk geschrieben.

Dieser Beitrag beschreibt, wie Sie aus dem gewachsenen Zustand ein Rollenmodell machen, das eine Prüfung übersteht: mit dem Prinzip der geringsten Rechte, mit zeitlich begrenzten Rechten über Privileged Identity Management, mit getrennten Adminkonten, mit Notfallkonten und mit einem Vier-Augen-Prinzip, das nicht nur in der Dienstanweisung steht, sondern technisch erzwungen wird. Und er beschreibt, was passiert, wenn der eine Admin in den Urlaub fährt — einmal ohne Modell und einmal mit.

## Der Befund: ein Konto, das alles kann

Der Zustand ist selten das Ergebnis einer Entscheidung. Er ist das Ergebnis einer Historie. Wer einen Microsoft-365-Tenant anlegt, bekommt die Rolle des Globalen Administrators automatisch zugewiesen. In der Pilotphase war das praktisch. Aus der Pilotphase wurde ein Wirkbetrieb, aus dem Wirkbetrieb wurden acht Jahre, und aus der einen Zuweisung wurden fünf, weil das Systemhaus, die Telefonie-Betreuung und die Fachanwendungsbetreuung ja auch mal etwas brauchen.


*Skizze 1: Der übliche Ausgangszustand. Ein Konto verbindet alle Dienste, und keine Verbindung ist dokumentiert.*

## Warum das in der Verwaltung besonders unangenehm ist

In einem mittelständischen Unternehmen ist ein überdimensioniertes Adminkonto ein Sicherheitsrisiko. In einer Verwaltung ist es zusätzlich ein Organisationsproblem, ein Datenschutzproblem und ein Mitbestimmungsproblem. Ein Konto, das alle Postfächer öffnen und alle SharePoint-Bibliotheken lesen kann, hat technischen Zugriff auf die Beschlussvorlage vor der Sitzung, auf die Bieterunterlagen vor dem Submissionstermin, auf den Vermerk der Personalabteilung zu einem laufenden Verfahren und auf die Fallakte im Sozialamt. Ob dieser Zugriff jemals genutzt wurde, ist zweitrangig. Erklären müssen Sie schon, dass er möglich war.

Bei einer Stadtverwaltung mit rund tausend Rufnummern haben wir genau diese Frage im Personalrat erlebt. Nicht als Vorwurf, sondern als sachliche Erkundigung: Wer kann eigentlich in mein Postfach schauen? Die ehrliche Antwort lautete damals: drei Personen, jederzeit, ohne dass es jemandem auffällt. Die Antwort, die man nach einem Rollenprojekt geben kann, lautet: niemand dauerhaft, im Bedarfsfall eine benannte Person nach Genehmigung durch eine zweite, mit Protokolleintrag und Ablaufdatum. Das ist derselbe technische Dienst, aber eine andere Verwaltung.

**FAKTEN | Was Microsoft selbst als Obergrenze nennt**

**Weniger als fünf** Personen sollten die Rolle Globaler Administrator besitzen. Ab fünf privilegierten Zuweisungen dieser Rolle blendet das Entra Admin Center einen Hinweis auf der Übersichtsseite ein.

**Weniger als zehn** privilegierte Rollenzuweisungen insgesamt. Rollen mit besonders kritischen Berechtigungen, etwa dem Ändern von Anmeldeinformationen, tragen im Portal die Kennzeichnung „PRIVILEGED“. Wird die Zahl zehn überschritten, erscheint eine Warnung auf der Seite der Rollen und Administratoren.

**Über 65 integrierte Rollen** stehen in Entra ID zur Verfügung, dazu kommen benutzerdefinierte Rollen. Für nahezu jede Verwaltungsaufgabe existiert eine passendere Rolle als die des Globalen Administrators.

**Zwei reine Cloud-Konten** für den Notfall empfiehlt Microsoft ausdrücklich — dauerhaft aktiv, nicht an Personen gebunden, nicht aus dem lokalen Verzeichnis synchronisiert.

Dieser Beitrag gehört zur Reihe Microsoft 365 in der öffentlichen Verwaltung. Dort finden Sie die übergreifende Einordnung, in welcher Reihenfolge Verwaltungen die Themen Betriebsmodell, Schutzbedarf, Berechtigungen und Beschaffung sinnvoll angehen. Wenn Sie an dieser Stelle einsteigen, ist das vollkommen in Ordnung: Ein Rollenmodell lässt sich auch nachträglich einziehen, es ist nur unbequemer.

## Die Risiken, sortiert nach dem, was der Verwaltung wirklich weh tut

| Risiko | Was konkret passiert | Wer es merkt | Was es beendet |
|---|---|---|---|
| Ausfall der einzigen Person | Kein Konto anlegbar, keine Kennwortrücksetzung, keine Regeländerung; das Haus ist verwaltungstechnisch handlungsfähig, aber IT-seitig eingefroren | Fachämter am zweiten Tag, die Verwaltungsspitze am fünften | Benannte Vertretung mit eigener Berechtigung, nicht mit geteiltem Kennwort |
| Übernahme des Kontos | Ein einziger erfolgreicher Angriff genügt für Postfachzugriff, Datenabfluss, Abschalten von Protokollierung und Aufbewahrung | Im schlechten Fall niemand, im guten die Sicherheitsüberwachung | Keine stehenden Rechte, phishing-resistente Anmeldung, getrennte Konten |
| Fehlbedienung im Alltag | Eine unbedachte Änderung in Conditional Access sperrt den Bauhof aus, eine gelöschte Gruppe reißt eine Bibliothek mit | Sofort, sehr laut, meist freitags | Rechte nur für den Anlass, Zweitfreigabe bei kritischen Rollen |
| Fehlender Nachweis | Das Rechnungsprüfungsamt fragt, wer eine Änderung veranlasst hat; es gibt Protokolle, aber keinen Antrag und keine Genehmigung | Bei der nächsten Prüfung | Antrag, Begründung, Genehmigung und Ablauf als Teil des Vorgangs |
| Vermischung der Sphären | Dasselbe Konto liest Mails, klickt Links, öffnet Anhänge und verwaltet nebenbei das Verzeichnis | Nach dem Vorfall | Getrenntes Adminkonto ohne Postfach und ohne Alltagsnutzung |

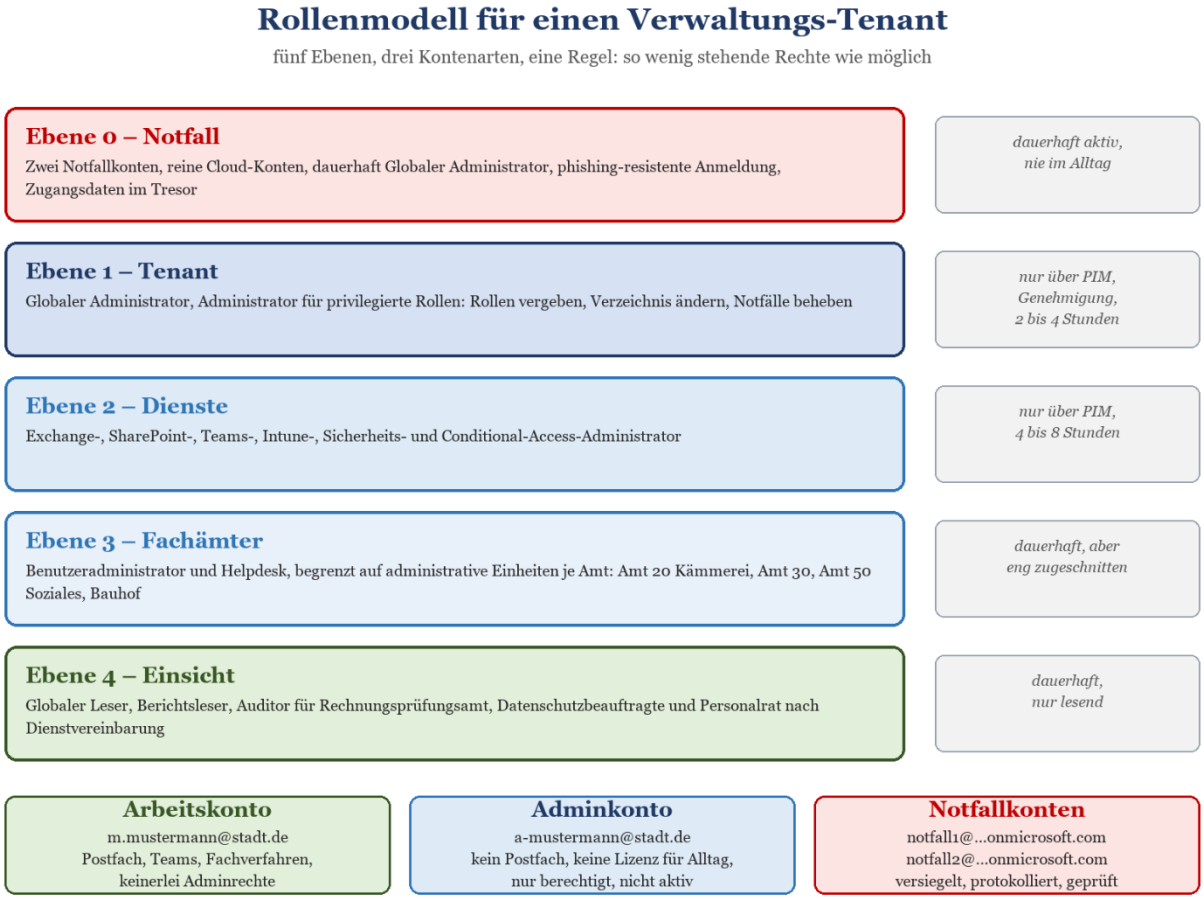
*Tabelle 1: Fünf Risiken des Ein-Konto-Betriebs. Nur das erste ist ein Personalthema, alle anderen sind Organisationsthemen.*

**WARNUNG | Die Rechnung, die niemand aufmacht**

Der Ein-Konto-Betrieb ist nicht billig, er ist nur unsichtbar teuer. Solange nichts passiert, kostet er nichts. Wenn etwas passiert, kostet er die Handlungsfähigkeit des Hauses. Bei einer Stadtverwaltung, die ihr Bürgertelefon über Teams betreibt, ist der gesperrte Administrator kein IT-Vorfall, sondern eine Erreichbarkeitsstörung mit politischer Öffentlichkeit. Führen Sie diese Abhängigkeit im Risikoregister und berichten Sie sie der Verwaltungsspitze. Ein Risiko, das nur die IT kennt, ist organisatorisch nicht existent.

# Das Rollenmodell: geringste Rechte, übersetzt in Verwaltungssprache

Ein Rollenmodell ist kein Sicherheitsprodukt, sondern ein Organisationsdokument. Es beschreibt, welche Aufgabe welche Berechtigung braucht, in welchem Umfang und für welchen Zeitraum. Diese drei Dimensionen — Menge der Berechtigungen, Umfang des Geltungsbereichs, Dauer — sind genau die Stellschrauben, die Microsoft in seinen eigenen Empfehlungen zum Prinzip der geringsten Rechte nennt. Verwaltungen sind darin gut, weil sie es aus dem Aktenplan und aus der Zeichnungsberechtigung kennen. Der Rollenkatalog ist im Kern nichts anderes als eine Zeichnungsordnung für den Tenant.




*Skizze 2: Rollenmodell in fünf Ebenen. Die roten und blauen Ebenen sind die Ausnahme, die hellen Ebenen sind der Alltag.*

## Fünf Ebenen, die sich in jeder Verwaltung wiederfinden

- **Ebene 0 — Notfall.** Zwei reine Cloud-Konten mit dauerhafter Zuweisung der Rolle Globaler Administrator. Sie gehören niemandem, sie werden nie im Alltag benutzt, und ihre Nutzung löst einen Alarm aus. Dazu gleich mehr.
- **Ebene 1 — Tenant.** Globaler Administrator und Administrator für privilegierte Rollen. Diese Ebene ändert das Verzeichnis selbst und vergibt Rechte. Sie darf niemand dauerhaft besitzen. Zwei bis drei Personen sind hierfür berechtigt, aktiv sind sie nur für die Dauer eines Vorgangs.
- **Ebene 2 — Dienste.** Exchange-, SharePoint-, Teams-, Intune-, Sicherheits- und Conditional-Access-Administrator. Diese Rollen erledigen den technischen Betrieb. Auch sie werden zeitlich begrenzt aktiviert, aber ohne den ganz strengen Genehmigungsweg.

- **Ebene 3 — Fachämter.** Benutzeradministration und Helpdesk, eingegrenzt auf administrative Einheiten. Eine administrative Einheit bildet ein Amt, einen Standort oder einen Bereich ab. Die Person im Amt 10 setzt Kennwörter im Amt 10 zurück und nirgendwo sonst.
- **Ebene 4 — Einsicht.** Globaler Leser, Berichtsleser und vergleichbare lesende Rollen für das Rechnungsprüfungsamt, für Datenschutzbeauftragte und — soweit die Dienstvereinbarung das vorsieht — für den Personalrat. Diese Rechte dürfen dauerhaft sein, weil sie nichts verändern können.

Der Reflex, zunächst alles in Ebene 1 zu belassen, weil es dort schneller geht, ist verständlich und falsch. Die Verwaltung, die uns erklärt hat, sie habe „eigentlich nur drei Global Admins“, hatte tatsächlich drei Personen und neun weitere Zuweisungen über Dienstkonten, Integrationen und ein längst vergessenes Migrationswerkzeug. Die erste Amtshandlung eines Rollenprojekts ist deshalb nie das Modell, sondern die Inventur.

## Kontentrennung: drei Konten, ein Mensch

Die wirksamste Einzelmaßnahme kostet keine Lizenz und keine Projektwoche: Administrative Tätigkeiten laufen über ein eigenes Konto. Das Arbeitskonto liest Mails, sitzt in Teams-Besprechungen, öffnet Anhänge aus dem Posteingang der Poststelle und trägt damit das übliche Risiko des Büroalltags. Das Adminkonto hat kein Postfach, empfängt keine Nachrichten, surft nicht und wird ausschließlich für Verwaltungsaufgaben im Tenant benutzt. Microsoft empfiehlt für diese Adminkonten ausdrücklich reine Cloud-Konten, also keine aus dem lokalen Verzeichnis synchronisierten Konten: Wird das lokale Active Directory kompromittiert, wandert der Schaden sonst direkt in den Tenant.

Genau an dieser Stelle hängt die Frage, ob Ihre Anmeldung noch über eine lokale Föderation läuft. Wer per ADFS anmeldet, hat eine zusätzliche Abhängigkeit im Anmeldepfad seiner Administration. Die Abwägung entlang der Fachverfahren haben wir in ADFS oder Entra ID in der Verwaltung: Die Entscheidung entlang der Fachverfahren ausführlich beschrieben; für das Rollenmodell gilt in jedem Fall: Die Konten der Ebenen 0 und 1 dürfen nicht von einem lokalen System abhängen.

**TIPP | Namenskonvention, die Prüfungen überlebt**

Vergeben Sie Adminkonten nach einem erkennbaren Muster, etwa mit vorangestelltem Kürzel: **a-nachname** für administrative Konten, **n-1** und **n-2** für Notfallkonten. Das klingt banal, hat aber drei Effekte: Die Konten sind in Protokollen sofort erkennbar, sie lassen sich sauber in Conditional-Access-Regeln adressieren, und das Rechnungsprüfungsamt kann die Liste der privilegierten Konten ohne Rückfrage lesen. Halten Sie die Konvention in der Dienstanweisung fest, nicht nur im Kopf.

## Aufgaben und passende Rollen

| Verwaltungsaufgabe | Geeignete Rolle | Geltungsbereich | Zuweisung |
|---|---|---|---|
| Kennwort zurücksetzen, neue Kraft im Amt anlegen | Benutzeradministrator oder Helpdesk-Administrator | Administrative Einheit des jeweiligen Amtes | Dauerhaft, eng begrenzt |
| Verteiler, Raumpostfächer, Postfachberechtigungen | Exchange-Administrator | Gesamter Tenant | Über PIM, 4 bis 8 Stunden |
| Teams anlegen, Websitesammlungen, Freigabeeinstellungen | Teams-Administrator, SharePoint-Administrator | Gesamter Tenant | Über PIM, 4 bis 8 Stunden |

| | | | |
|---|---|---|---|
| Regelwerk für Anmeldung, Gerätezustand, Standorte | Conditional-Access-Administrator | Gesamter Tenant | Über PIM, Genehmigung erforderlich |
| Aufbewahrung, Aussonderung, eDiscovery | Compliance-Administrator und passende Purview-Rollengruppe | Gesamter Tenant | Über PIM, Genehmigung erforderlich |
| Rollen vergeben, Verzeichnis grundlegend ändern | Administrator für privilegierte Rollen, Globaler Administrator | Gesamter Tenant | Über PIM, 2 Stunden, Genehmigung |
| Prüfung, Innenrevision, Datenschutzaufsicht | Globaler Leser, Berichtsleser | Gesamter Tenant, ausschließlich lesend | Dauerhaft |
| Betreuung durch Systemhaus oder Rechenzentrum | Rolle nach Leistungsbeschreibung, kein Globaler Administrator | So eng wie fachlich möglich | Über PIM, mit Genehmigung durch die Verwaltung |

*Tabelle 2: Aufgabenbezogene Rollenzuordnung. Die letzte Spalte ist die wichtigste: Sie unterscheidet zwischen dauerhaftem Besitz und zeitweiliger Wirkung.*

Die letzte Zeile verdient einen eigenen Satz, weil sie erfahrungsgemäß zu Missverständnissen führt. Dass ein kommunales Rechenzentrum oder ein Systemhaus administrative Rechte braucht, ist selbstverständlich und richtig; diese Häuser leisten Betrieb, den die Verwaltung selbst nicht vorhalten kann. Die Frage ist nicht, ob sie Rechte bekommen, sondern welche, in welchem Umfang und mit welcher Nachvollziehbarkeit. Ein Dienstleister mit einer passgenauen Rolle und einem protokollierten Aktivierungsweg ist für beide Seiten die bessere Konstruktion: Die Verwaltung behält die Kontrolle, der Dienstleister hat einen Nachweis, was er wann getan hat.

Wie sich die Schnittstellen zwischen Verwaltung und Rechenzentrum sauber beschreiben lassen, welche Rollen dort typischerweise verhandelt werden und wann eine Zweitmeinung sinnvoll ist, behandelt Microsoft 365 und das kommunale Rechenzentrum: Rollen, Schnittstellen, Zweitmeinung. Für die Rollenzuweisung selbst genügt eine Regel: Der Dienstleister erhält keine Rolle, die er nicht in der Leistungsbeschreibung begründen kann.

**WICHTIG | Administrative Einheiten sind der unterschätzte Hebel**

Administrative Einheiten begrenzen eine Rollenzuweisung auf eine Teilmenge von Benutzern, Gruppen oder Geräten. Für Verwaltungen ist das die natürliche Abbildung der Ämterstruktur: Amt 20, Amt 32, Amt 50, Bauhof, Feuerwehr, Volkshochschule. Wer den Helpdesk in den Fachämtern verankern will — und viele größere Häuser wollen das —, kommt ohne administrative Einheiten nicht aus.

Für den besonders sensiblen Bereich gibt es zusätzlich **eingeschränkt verwaltete administrative Einheiten**. Objekte darin können nur von ausdrücklich zugewiesenen Personen geändert werden, selbst Globale Administratoren müssen sich dafür explizit zuweisen — und dieser Vorgang wird protokolliert. Für Konten der Amtsleitung oder des Personalbereichs ist das eine ernst zu nehmende Option. Beachten Sie dabei: PIM unterstützt Gruppen innerhalb solcher eingeschränkt verwalteten Einheiten nicht.

## PIM: Rechte mit Verfallsdatum

Privileged Identity Management, kurz PIM, dreht die Logik der Rechtevergabe um. Statt einer dauerhaften Zuweisung erhält eine Person eine **Berechtigung**: Sie ist für eine Rolle vorgesehen, besitzt sie aber nicht. Braucht sie die Rolle, fordert sie die Aktivierung an, weist sich aus, begründet

den Anlass, lässt sich gegebenenfalls von einer zweiten Person freigeben und erhält die Rolle für ein definiertes Zeitfenster. Danach verschwindet sie wieder, ohne dass jemand daran denken muss. Genau dieses Vergessen ist in Verwaltungen der häufigste Grund für gewachsene Rechte.


*Skizze 3: Aus einem stehenden Recht wird ein Vorgang. Die Balken unten zeigen, wie stark sich die Angriffsfläche über die Zeit unterscheidet.*

## Die Einstellungen, die Sie tatsächlich entscheiden müssen

PIM-Rolleneinstellungen werden je Rolle festgelegt und gelten dann für alle Zuweisungen dieser Rolle. Sie brauchen also keine individuellen Sonderregelungen, sondern eine Entscheidung pro Rolle — das passt gut zu einer Dienstanweisung. Die maximale Aktivierungsdauer lässt sich zwischen einer und vierundzwanzig Stunden einstellen. Für die Genehmigung gilt: Wählen Sie mindestens einen, besser zwei Genehmiger. Wird kein Genehmiger benannt, werden aktive Administratoren für privilegierte Rollen beziehungsweise Globale Administratoren zu Standardgenehmigern.

| Rolle | Max. Dauer | Nachweis bei Aktivierung | Genehmigung | Begründung |
|---|---|---|---|---|
| Globaler Administrator | 2 Stunden | Authentifizierungskontext mit phishing-resistenter Methode | Ja, zwei Genehmiger | Pflicht, mit Ticketnummer |
| Administrator für privilegierte Rollen | 2 Stunden | Authentifizierungskontext | Ja, zwei Genehmiger | Pflicht, mit Ticketnummer |
| Conditional-Access-Administrator | 4 Stunden | Authentifizierungskontext | Ja | Pflicht |
| Compliance-Administrator | 4 Stunden | Mehrstufige Authentifizierung | Ja | Pflicht |
| Exchange-, SharePoint-, Teams-Administrator | 8 Stunden | Mehrstufige Authentifizierung | Nein | Pflicht |
| Intune-Administrator | 8 Stunden | Mehrstufige Authentifizierung | Nein | Pflicht |

| | | | | |
|---|---|---|---|---|
| Benutzeradministrator, auf Amt begrenzt | Dauerhaft aktiv | Anmeldung nach Regelwerk | Entfällt | Entfällt |
| Globaler Leser | Dauerhaft aktiv | Anmeldung nach Regelwerk | Entfällt | Entfällt |

*Tabelle 3: Ein praxistauglicher Ausgangswert für die Rolleneinstellungen. Die Zahlen sind Vorschläge, keine Vorgaben — sie müssen zu Ihren Dienstzeiten und zu Ihrer Rufbereitschaft passen.*

## Der Unterschied zwischen mehrstufiger Anmeldung und Authentifizierungskontext

Ein Detail, das in Konzepten regelmäßig untergeht: Die Einstellung „bei Aktivierung mehrstufige Authentifizierung verlangen“ führt nicht zwingend zu einer erneuten Abfrage. Hat die Person sich bereits stark angemeldet, trägt sie den Nachweis im Token, und die Aktivierung läuft ohne weitere Rückfrage durch. Wer eine echte, frische Bestätigung im Moment der Aktivierung will, verwendet einen **Conditional-Access-Authentifizierungskontext** in Verbindung mit einer Authentifizierungsstärke und setzt in der zugehörigen Richtlinie die Anmeldehäufigkeit auf „jedes Mal“. Erst dann ist die Aktivierung eine bewusste Handlung und nicht ein Nebeneffekt der Morgenanmeldung.

Vorsicht bei einem Nebeneffekt: Nach einer erneuten Authentifizierung gilt ein Zeitfenster von zehn Minuten. Aktiviert dieselbe Person innerhalb dieses Fensters eine weitere berechtigte Rolle, wird sie nicht noch einmal zur Bestätigung aufgefordert. Das ist gewollt und bequem, sollte aber bei der Festlegung Ihrer Rollentrennung bekannt sein.

Weil PIM in diesem Punkt auf dem Regelwerk der bedingten Zugriffssteuerung aufsetzt, gehören beide Themen in dieselbe Konzeptphase. Das passende Regelwerk für Rathaus, Bauhof, Außenstellen und Homeoffice — einschließlich der Frage, welche Ausnahmen eine Verwaltung wirklich braucht — finden Sie in Conditional Access für Verwaltungen: Regelwerk für Rathaus, Bauhof und Homeoffice. Wer PIM einführt, ohne die Regeln für die bedingte Zugriffssteuerung sortiert zu haben, baut ein Türschloss in eine Wand ohne Tür.

**WARNUNG | Der Klassiker: sich selbst aussperren**

Es gibt eine Konstellation, die eine Verwaltung zuverlässig handlungsunfähig macht, und sie entsteht mit den besten Absichten: **Alle** Zuweisungen für Globaler Administrator und Administrator für privilegierte Rollen sind nur berechtigt, keine ist aktiv; für die Aktivierung ist eine Genehmigung erforderlich; ein Genehmiger ist nicht ausdrücklich benannt oder wurde inzwischen aus dem Verzeichnis entfernt. Dann kann niemand mehr genehmigen, und niemand kann mehr aktivieren.

Der Schutz dagegen besteht aus zwei Dingen, die Sie beide brauchen: ausdrücklich benannte Genehmiger — mindestens zwei — und Notfallkonten mit dauerhafter, aktiver Zuweisung. Prüfen Sie diese Konstellation, bevor Sie die letzte dauerhafte Zuweisung entfernen, nicht danach.

## Die Lizenzfrage, nüchtern betrachtet

PIM ist kein Bestandteil der Grundausstattung. Jede Person mit berechtigten oder zeitgebundenen Zuweisungen benötigt eine Lizenz für Microsoft Entra ID P2 oder Microsoft Entra ID Governance. Das gilt auch für Zuweisungen über PIM für Gruppen. Die gute Nachricht für Verwaltungen: Es geht nicht um die gesamte Belegschaft, sondern um die Handvoll Personen mit administrativen Aufgaben. Benutzerdefinierte Rollen und bedingte Zugriffssteuerung setzen Entra ID P1 voraus, administrative Einheiten benötigen P1 für Administratoren, die auf eine Einheit begrenzt sind. Zugriffsüberprüfungen gehören in den Bereich Entra ID Governance beziehungsweise Entra Suite.

Ob Sie diese Lizenzen über eine flächige E5-Ausstattung, über gezielte Zusatzlizenzen für den Administrationskreis oder über die Behördenkonditionen abbilden, ist eine Beschaffungsentscheidung und keine technische. Die Varianten und ihre Fallstricke haben wir in Microsoft 365 Lizenzen für Verwaltungen: E3, E5, F3 und die Behördenkonditionen durchgerechnet. Für die Vergabeunterlage genügt zunächst die Feststellung: Das Rollen- und Berechtigungskonzept erzeugt einen klar abgrenzbaren, kleinen Lizenzbedarf mit erheblicher Risikowirkung.

**FAKTEN | Warum die Diskussion um Adminkonten ohnehin kommt**

Microsoft erzwingt inzwischen mehrstufige Authentifizierung für die Anmeldung an den Verwaltungsportalen. Die erste Stufe betraf ab Oktober 2024 das Azure-Portal, das Entra Admin Center und das Intune Admin Center, ab Februar 2025 kam das Microsoft 365 Admin Center hinzu. Die zweite Stufe mit Azure CLI, Azure PowerShell, der Azure-App, Werkzeugen für Infrastruktur als Code und REST-Endpunkten begann ab dem 1. Oktober 2025; reine Lesevorgänge sind ausgenommen.

Für Verwaltungen heißt das: Die Frage, wie sich Ihre administrativen Konten anmelden, ist keine Kür mehr. Wer sie ohnehin beantworten muss, kann bei der Gelegenheit gleich das Rollenmodell mitnehmen. Prüfen Sie dabei besonders technische Konten und Automatisierungen — dort tut die Umstellung erfahrungsgemäß am meisten weh.

## Notfallkonten und Vertretung: der Fall des einen Admins

Jetzt zum eigentlichen Thema, denn alles Bisherige war Vorbereitung. Ein Rollenmodell mit zeitbegrenzten Rechten löst das Sicherheitsproblem. Es löst nicht das Verfügbarkeitsproblem. Im Gegenteil: Wer stehende Rechte abschafft, ohne die Vertretung zu regeln, hat das Risiko nur verschoben. Deshalb gehören Notfallkonten und Vertretungsregelung in dieselbe Beschlussvorlage wie das Rollenmodell.

### Notfallkonten nach Lehrbuch

| Anforderung | Ausgestaltung | Warum das so ist |
|---|---|---|
| Anzahl | Mindestens zwei | Redundanz; ein einzelnes Notfallkonto ist wieder ein einzelner Ausfallpunkt |
| Herkunft | Reine Cloud-Konten in der Domäne onmicrosoft.com | Keine Abhängigkeit von lokalem Verzeichnis oder Föderation, die gerade ausgefallen sein könnte |
| Zuweisung | Globaler Administrator dauerhaft aktiv, nicht nur berechtigt | Im Notfall darf keine Genehmigung nötig sein, die niemand erteilen kann |
| Anmeldung | Phishing-resistent, etwa Passkey oder zertifikatsbasiert | Andere Methode als bei den regulären Adminkonten, damit nicht ein Ausfall beide Wege trifft |
| Regelwerk | Aus sperrenden Regeln der bedingten Zugriffssteuerung ausgenommen | Sonst greift die Sperre genau in dem Fall, für den das Konto gedacht ist; reine Prüfrichtlinien brauchen keine Ausnahme |
| Aufbewahrung | Zugangsmittel in getrennten, gesicherten und feuerfesten Behältnissen | Ein Schlüssel im Schreibtisch des Administrators ist kein Notfallkonzept |
| Überwachung | Alarm bei jeder Anmeldung, Nachbetrachtung durch ein benanntes | Der Unterschied zwischen Notfall, Übung und Missbrauch muss belegbar sein |

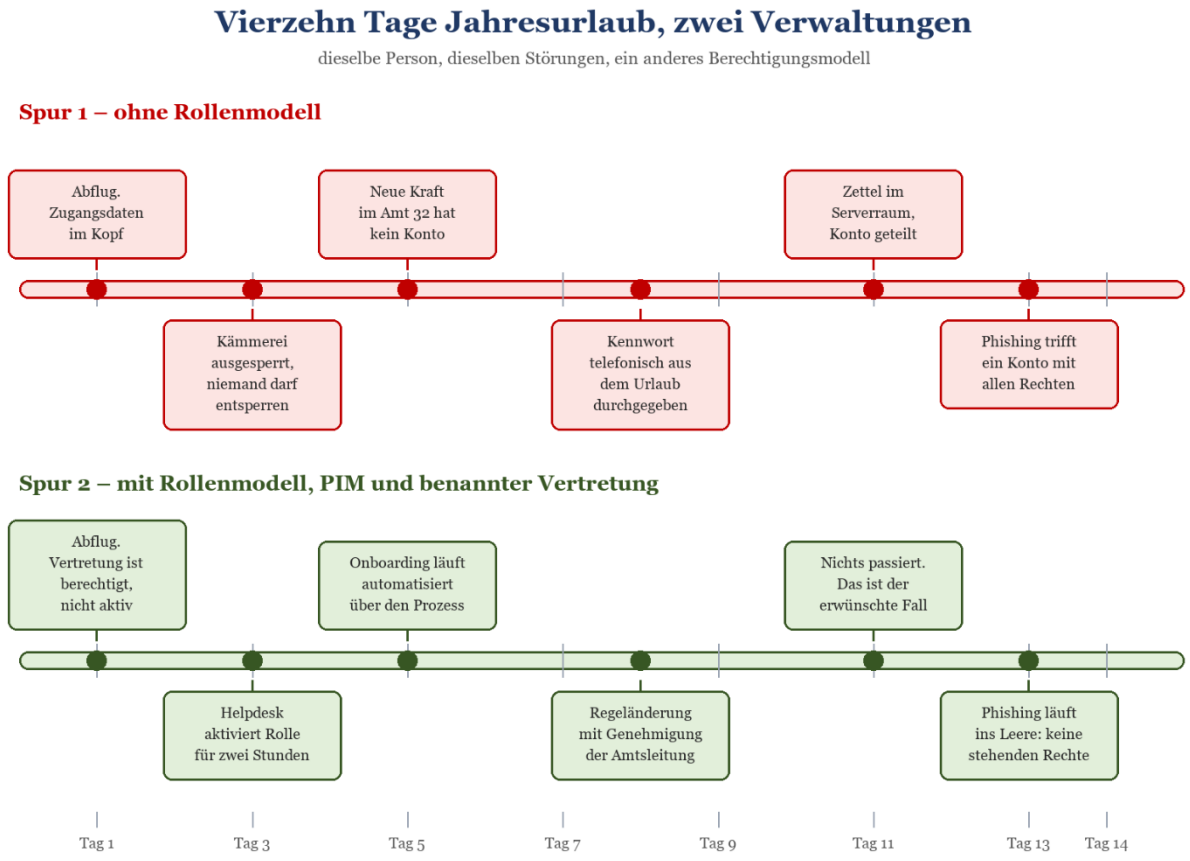
| | | |
|---|---|---|
| | Team | |
| Prüfung | Mindestens alle 90 Tage, zusätzlich bei Personalwechsel | Ein Notfallkonto, das im Ernstfall nicht funktioniert, ist schlimmer als keines, weil man sich darauf verlassen hat |

*Tabelle 4: Anforderungen an Notfallkonten. Die letzte Zeile ist die, die in der Praxis am häufigsten liegen bleibt.*

**WICHTIG | Der Tresor gehört nicht in die IT**

Notfallkonten sind keine IT-Angelegenheit, sondern eine Angelegenheit der Verwaltungsführung. Legen Sie in einer Dienstanweisung fest, wer Zugriff auf die Zugangsmittel hat, wie die Entnahme dokumentiert wird und wer nach einer Nutzung Bericht erstattet. Bewährt hat sich eine Zwei-Personen-Regel analog zum Umgang mit Zahlungsmitteln: eine Person aus der IT, eine aus dem Hauptamt oder der Verwaltungsleitung. Ändern Sie die Kombination des Behältnisses, wenn eine zugriffsberechtigte Person das Haus verlässt.

## Praxisfall: Was passiert, wenn der eine Admin in den Urlaub fährt




*Skizze 4: Zwei Verläufe desselben Jahresurlaubs. Der Unterschied liegt nicht in der Person, sondern im Modell.*

**AUS DER PRAXIS | Vierzehn Tage, ein Landschaftsverband und ein Zettel im Serverraum**

Bei einem großen Landschaftsverband haben wir den Verlauf in der linken Spur der Skizze in Varianten mehrfach erlebt. Der zuständige Kollege war fachlich hervorragend und hatte alles im Griff — solange er da war. Am zweiten Urlaubstag brauchte die Kämmerei eine Kennwortrücksetzung für einen Zugang, der an eine Fristsache gebunden war. Es gab niemanden

mit dem Recht dazu. Am vierten Tag rief die Amtsleitung beim Systemhaus an, das aus guten Gründen ablehnte, weil es keine Beauftragung für diesen Vorgang hatte.

Am achten Tag wurde der Kollege im Urlaub angerufen, gab telefonisch die Zugangsdaten seines administrativen Kontos durch, und ab diesem Moment gab es keine Zurechenbarkeit mehr. Am elften Tag klebte ein Zettel an der Innenseite des Serverschranks, weil sich niemand die Zeichenfolge merken konnte. Das ist die Stelle, an der aus einem Organisationsmangel ein meldepflichtiger Vorfall werden kann. Es ist nichts passiert. Passieren hätte es können, und genau das ist der Punkt.

Im zweiten Anlauf, nach Einführung des Rollenmodells, sah derselbe Urlaub anders aus. Zwei Personen aus dem Anwenderservice waren für die Rolle Benutzeradministrator berechtigt, begrenzt auf die administrativen Einheiten ihrer Bereiche. Sie aktivierten die Rolle im Bedarfsfall für zwei Stunden, mit Begründung und Ticketnummer. Für die eine wirklich kritische Änderung an einer Anmelderegel aktivierte die Vertretung die entsprechende Rolle, ein zweiter Berechtigter gab frei. Der Kollege im Urlaub erfuhr davon nach seiner Rückkehr aus dem Protokoll. Das ist die Definition einer funktionierenden Vertretung: Sie merkt man erst hinterher.

### Vertretung ist eine Organisations-, keine Technikaufgabe

Die Berechtigung in PIM ist der einfache Teil. Der schwierige Teil ist die Befähigung. Eine Person, die zwar berechtigt ist, eine Rolle zu aktivieren, aber noch nie eine Aufbewahrungsrichtlinie gesehen hat, ist keine Vertretung, sondern eine Haftungsfrage. Planen Sie deshalb drei Dinge ein, die nichts mit Technik zu tun haben: eine schriftliche Vertretungsregelung mit Namen und Zeiträumen, eine dokumentierte Übergabe der wiederkehrenden Vorgänge, und regelmäßige Übungen, bei denen die Vertretung tatsächlich einmal handelt — am besten, während die Hauptperson danebensteht und nichts sagt.

Für den Aufbau dieser Befähigung eignen sich zugeschnittene Formate deutlich besser als Standardkurse, weil die Verwaltungsfälle — Aktenplan, Fristen, Gremienarbeit, Fachverfahren — in Herstellerkursen schlicht nicht vorkommen. Wie wir das aufsetzen, beschreibt Microsoft-365-Schulung für Verwaltungen. Wichtiger als der Anbieter ist allerdings, dass die Vertretung Zeit im Dienstplan bekommt. Eine Vertretung, die zusätzlich zum Tagesgeschäft stattfinden soll, findet nicht statt.

Und noch ein Hinweis, weil er in Verwaltungen erfahrungsgemäß gebraucht wird: Üben Sie den Ernstfall, bevor er eintritt. Wie eine solche Übung aufgebaut sein kann — mit verschlüsselter Bibliothek, übernommenem Adminkonto und ausgefallenem Bürgertelefon — beschreibt Notfallübung für die Verwaltungs-IT: SharePoint verschlüsselt, Admin-Konto übernommen, Bürgertelefon tot. Die Übung deckt regelmäßig genau die Lücke auf, die im Konzept so überzeugend aussah.

## Vier-Augen-Prinzip und die Nachweise für die Rechnungsprüfung

Verwaltungen kennen das Vier-Augen-Prinzip aus dem Haushaltsrecht: Anordnung und Ausführung liegen nicht in einer Hand. Für administrative Tätigkeiten im Tenant gilt derselbe Gedanke, und er lässt sich technisch abbilden. Die Genehmigungsfunktion in PIM ist genau das: Eine Person fordert die Rolle an, eine zweite gibt frei, beide Vorgänge sind protokolliert. Der Genehmiger braucht dafür selbst keine Rolle zu besitzen — das ist wichtig, weil es Ihnen erlaubt, die Genehmigung organisatorisch anzusiedeln statt technisch.


*Skizze 5: Die Nachweiskette von der Dienstanweisung bis zur Aussonderung. Die Bruchstelle liegt fast immer bei der Aufbewahrung der Protokolle.*

## Was das Rechnungsprüfungsamt tatsächlich fragt

| Prüffrage | Woher der Nachweis kommt | Turnus |
|---|---|---|
| Wer darf welche Rolle und seit wann? | Übersicht der berechtigten und aktiven Zuweisungen in PIM, abgeglichen mit dem Rollenkatalog der Dienstanweisung | Laufend, Auszug quartalsweise |
| Wurde eine Rolle im Prüfzeitraum aktiviert und warum? | PIM-Verlauf mit Begründung, Ticketnummer und Genehmiger | Anlassbezogen |
| Was wurde mit der aktivierten Rolle konkret getan? | Einheitliches Überwachungsprotokoll des Tenants, verknüpft über Zeitfenster und Konto | Anlassbezogen |
| Sind Rechte noch erforderlich? | Zugriffsüberprüfung mit dokumentierter Entscheidung je Person und Rolle | Quartalsweise oder halbjährlich |
| Wurden Notfallkonten benutzt? | Alarmierung bei Anmeldung, Nachbetrachtung, Vermerk | Jede Nutzung, Funktionsprüfung alle 90 Tage |
| Wer hat Zugriff auf die Protokolle selbst? | Rollenzuweisung für lesende Rollen, getrennt von den ändernden Rollen | Jährlich |

*Tabelle 5: Prüffragen und ihre Quellen. Wer diese sechs Zeilen beantworten kann, hat ein belastbares Berechtigungskonzept.*

Die dritte Zeile ist die anspruchsvollste, weil sie zwei Systeme verbindet: die Aktivierung in PIM und die eigentliche Änderung im Protokoll des Tenants. Welche Protokolle es gibt, wie lange sie vorgehalten werden und wie Sie daraus einen prüffesten Nachweis machen, behandelt Microsoft 365 Audit-Log und Rechnungsprüfung: Nachweise, die Verwaltungen liefern müssen im Detail. Der wichtigste Punkt vorab: Die Vorhaltedauer im Dienst ist begrenzt und richtet sich nach Lizenzierung und Konfiguration. Wenn Ihre Aufbewahrungsfristen darüber hinausgehen, brauchen Sie einen Export und eine Ablage.

## Rezertifizierung: die unbeliebte, aber wirksame Übung

Berechtigungen wachsen. Menschen wechseln vom Amt 32 ins Amt 20 und behalten ihre alten Rechte, weil niemand sie entzieht. Zugriffsüberprüfungen sind das Gegenmittel: In festen Abständen bestätigt eine benannte Person, dass eine Berechtigung noch gebraucht wird, oder sie entzieht sie. Microsoft empfiehlt diesen Turnus ausdrücklich, und für Verwaltungen hat er einen zusätzlichen Vorteil: Die Entscheidung ist dokumentiert und lässt sich einer Amtsleitung zuordnen. Aus einer IT-Aufgabe wird eine Führungsaufgabe mit Aktenzeichen.

Setzen Sie den Turnus realistisch an. Quartalsweise für die Ebenen 0 bis 2, halbjährlich oder jährlich für die Ebenen 3 und 4 ist in Häusern mit einigen hundert bis wenigen tausend Konten machbar. Eine monatliche Rezertifizierung klingt gründlich und führt in der Praxis dazu, dass alle Einträge ungelesen bestätigt werden. Damit haben Sie den Nachweis, aber nicht die Wirkung.

**FAKTEN | Einordnung in den IT-Grundschutz**

Der Baustein **ORP.4 Identitäts- und Berechtigungsmanagement** des BSI adressiert genau dieses Thema. Zu den Basis-Anforderungen gehört unter anderem die Aufgabenverteilung und Funktionstrennung; als Standard-Anforderung ist der Schutz privilegierter Konten mit Mehr-Faktor-Authentisierung benannt. Bei erhöhtem Schutzbedarf kommt das Vier-Augen-Prinzip für administrative Tätigkeiten hinzu.

Das ist eine fachliche Orientierung, keine Rechtsberatung: Welche Anforderungen für Ihr Haus verbindlich sind, ergibt sich aus Ihrer Schutzbedarfsfeststellung, aus landesrechtlichen Vorgaben und gegebenenfalls aus Vorgaben Ihres Trägers oder Zweckverbands. Prüfen Sie das mit Ihrem Informationssicherheitsbeauftragten.

› Schutzbedarf und Microsoft 365: IT-Grundschutz-Abgleich für die Praxis

## Berechtigungen und die Frage, was Copilot findet

Ein Randthema, das kein Randthema ist: Rollen im Verzeichnis und Berechtigungen auf Inhalte sind zwei verschiedene Dinge. Ein Konto ohne jede administrative Rolle kann trotzdem Zugriff auf eine SharePoint-Bibliothek mit Personalvorgängen haben, wenn dort einmal breit freigegeben wurde. Bei einer Stadtverwaltung mit SharePoint im Sozialbereich haben wir beides in einem Zug aufgeräumt, weil die Fragen im Personalrat ohnehin gemeinsam gestellt wurden. Das ist auch fachlich sinnvoll: Ein sauberes Rollenmodell im Verzeichnis nützt wenig, wenn die Inhaltsberechtigungen dahinter beliebig sind.

Warum das mit dem Einsatz von Copilot dringlich wird — die Suchfunktion findet eben genau das, was technisch freigegeben ist — beschreibt Oversharing im Verwaltungs-Tenant: Warum Copilot die Personalakte findet. Für das Berechtigungsprojekt heißt das schlicht: Nehmen Sie die Inhaltsberechtigungen in dieselbe Bestandsaufnahme auf wie die Verzeichnisrollen.

**TIPP | Der Personalrat ist Verbündeter, nicht Hürde**

Ein Rollenmodell mit zeitbegrenzten Rechten ist für die Interessenvertretung ein gutes Angebot, weil es genau die Frage beantwortet, die dort gestellt wird: Wer kann unter welchen Bedingungen auf welche Daten zugreifen? Führen Sie das Thema aktiv ein, bevor Sie gefragt werden. Halten Sie in einer Dienstvereinbarung fest, welche Auswertungen der Protokolle zulässig sind, wer sie durchführen darf und dass sie nicht der Verhaltens- oder Leistungskontrolle dienen. Bausteine für solche Regelungen finden Sie hier:

› Copilot und Personalrat: Bausteine einer Dienstvereinbarung

# Häufige Fragen

## Wir haben nur eineinhalb Stellen in der IT. Ist das Modell nicht überdimensioniert?

Nein, es ist dann sogar wichtiger. Je dünner die Personaldecke, desto größer das Ausfallrisiko einer Einzelperson. Sie können das Modell verschlanken: zwei Notfallkonten, getrennte Adminkonten, zwei bis drei Personen mit Berechtigung statt dauerhafter Zuweisung, und eine Vertretung, die zumindest die häufigsten Vorgänge beherrscht. Der Aufwand für diesen Kern liegt bei wenigen Tagen, nicht bei Monaten. Auf Genehmigungsketten und feingliedrige administrative Einheiten können Sie in kleinen Häusern zunächst verzichten.

## Brauchen wir für PIM zwingend eine E5-Ausstattung?

Nein. Erforderlich ist Microsoft Entra ID P2 oder Microsoft Entra ID Governance, und zwar nur für die Personen mit berechtigten oder zeitgebundenen Zuweisungen. In einer Verwaltung mit tausend Beschäftigten sind das typischerweise fünf bis fünfzehn Lizenzen. Ob Sie diese einzeln beschaffen oder ohnehin über eine höherwertige Suite abgedeckt sind, ist eine Frage Ihrer Vertragslage.

## Was ist mit unserem Systemhaus? Das braucht doch Vollzugriff.

Es braucht Zugriff, aber selten Vollzugriff, und praktisch nie dauerhaft. Beschreiben Sie in der Leistungsbeschreibung, welche Aufgaben der Dienstleister übernimmt, und leiten Sie daraus die Rollen ab. Für die Aktivierung gilt derselbe Weg wie intern: Anforderung, Begründung, Genehmigung durch die Verwaltung, Zeitfenster, Protokoll. Seriöse Dienstleister begrüßen das, weil es sie im Streitfall entlastet.

## Wie viele Personen sollten die Rolle Globaler Administrator aktivieren dürfen?

Microsoft empfiehlt weniger als fünf Zuweisungen dieser Rolle insgesamt. In der Praxis hat sich bewährt: zwei Notfallkonten mit dauerhafter Zuweisung und zwei bis drei Personen, die berechtigt sind und die Rolle über PIM aktivieren können. Ein Haus mit einer Person in dieser Konstellation ist zu dünn aufgestellt, ein Haus mit acht zu breit.

## Können wir Notfallkonten nicht einfach in den Passwortsafe legen?

Ein Passwortsafe ist besser als ein Zettel, aber er ist eine Abhängigkeit. Wenn der Safe über dasselbe Verzeichnis authentifiziert, das gerade ausgefallen ist, hilft er nicht. Microsoft empfiehlt für Notfallkonten phishing-resistente Verfahren, also Passkeys oder zertifikatsbasierte Anmeldung, und die getrennte Verwahrung der Zugangsmittel an gesicherten Orten. Halten Sie die Zugangswege des Notfallkontos unabhängig von allem, was ausfallen kann.

## Wie oft müssen Notfallkonten geprüft werden?

Mindestens alle 90 Tage, zusätzlich bei personellen Veränderungen im Kreis der Zugriffsberechtigten und bei Änderungen an der Lizenzierung. Die Prüfung umfasst mehr als eine Anmeldung: Aktualisieren Sie die Liste der berechtigten Personen, prüfen Sie, ob die Alarmierung ausgelöst hat, und stellen Sie sicher, dass der dokumentierte Ablauf noch zur aktuellen Konfiguration passt.

### Dürfen wir dem Personalrat lesenden Zugriff auf Protokolle geben?

Das ist eine Frage der Dienstvereinbarung und des jeweils geltenden Personalvertretungsrechts, das sich zwischen den Ländern und bei kirchlichen Trägern zwischen den Regelungswerken unterscheidet. Technisch ist ein rein lesender Zugriff über eine geeignete Rolle problemlos abbildbar. Ob und in welchem Umfang er zulässig oder geboten ist, klären Sie mit Ihrer Rechtsabteilung und Ihrer Interessenvertretung; dieser Beitrag ersetzt keine Rechtsberatung.

### Was ändert sich am Rollenmodell, wenn wir später in Richtung Delos Cloud gehen?

Die Grundlogik bleibt. Ein Rollenkatalog, getrennte Adminkonten, benannte Vertretung, Notfallzugänge, Vier-Augen-Prinzip und Rezertifizierung sind Organisationsleistungen, die in jeder Umgebung gebraucht werden. Welche einzelnen Rollen und Funktionen in einer souveränen Umgebung in welchem Umfang zur Verfügung stehen, ist gesondert zu prüfen und hängt vom jeweiligen Leistungsstand ab. Arbeiten Sie deshalb im Konzept mit Rollenbeschreibungen und Zuständigkeiten, nicht mit Produktnamen.

### Wir haben Rollen über Gruppen vergeben. Ist das schlecht?

Im Gegenteil, es kann sehr sinnvoll sein. Rollenzuweisbare Gruppen erlauben es, die Rollenvergabe an eine Gruppenverwaltung zu delegieren, und sie lassen sich ebenfalls über PIM steuern, so dass es keine dauerhaften Mitglieder oder Besitzer gibt. Wer mehrere Rollen gleichzeitig braucht, kann über eine solche Gruppe mit einer einzigen Aktivierung mehrere Rollen erhalten. Achten Sie darauf, dass die Gruppe beim Anlegen als rollenzuweisbar gekennzeichnet wird — das lässt sich später nicht mehr ändern.

### Womit fangen wir konkret an, wenn wir nächste Woche beginnen wollen?

Mit der Inventur: Wer hat heute welche privilegierte Rolle, seit wann und warum? Danach die beiden Notfallkonten, weil sie die Voraussetzung für alles Weitere sind. Dann die Kontentrennung für die Personen mit administrativen Aufgaben. Erst danach das eigentliche Rollenmodell und PIM. Wer die Reihenfolge umdreht und mit PIM beginnt, riskiert genau die Aussperrung, die weiter oben beschrieben ist.

## Fazit

Der eine Admin, der alles kann, ist kein Personalproblem und kein Vorwurf an eine einzelne Person. Er ist ein Organisationszustand, der entstanden ist, weil niemand ihn je entschieden hat. Genau deshalb lässt er sich auch mit einer Entscheidung beenden — nicht mit einem Produkt, sondern mit einem Rollenkatalog, einer Dienstanweisung und einer Beschlussvorlage.

Die vier wirksamen Schritte in der Reihenfolge, in der sie sich bewährt haben: **Erstens** zwei Notfallkonten, sauber eingerichtet und regelmäßig geprüft. **Zweitens** getrennte Adminkonten ohne Postfach und ohne Alltagsnutzung. **Drittens** ein Rollenmodell entlang der Ämter, das administrative Einheiten nutzt und die Ebenen 0 bis 2 möglichst leer hält. **Viertens** PIM mit Zeitbegrenzung, Begründung und Genehmigung für alles, was verändern kann. Die Rezertifizierung kommt danach und hält den Zustand.

Für die Verwaltungsspitze lässt sich der Nutzen in einem Satz zusammenfassen: Danach kann die Verwaltung eine Frage beantworten, die sie heute nicht beantworten kann — wer hat wann, mit welcher Begründung und mit wessen Genehmigung etwas in der zentralen Arbeitsumgebung des Hauses verändert. Das ist kein IT-Thema. Das ist dieselbe Anforderung, die im Haushaltsrecht seit Jahrzehnten selbstverständlich ist.

Wenn Sie das Thema aufsetzen wollen und eine strukturierte Bestandsaufnahme, einen Rollenkatalog und die passende Beschlussvorlage brauchen: Wie wir Verwaltungen dabei begleiten, beschreibt Microsoft-365-Beratung für Verwaltungen. Die Bestandsaufnahme der privilegierten Konten ist in aller Regel an einem Tag erledigt — was danach kommt, ist eher eine Frage der Abstimmung im Haus als eine Frage der Technik.

**WEITERLESEN | Passend zu diesem Thema**

Diese Beiträge greifen einzelne Punkte auf, die hier nur gestreift werden konnten:

› Conditional Access für Verwaltungen: Regelwerk für Rathaus, Bauhof und Homeoffice
› ADFS oder Entra ID in der Verwaltung: Die Entscheidung entlang der Fachverfahren
› Microsoft 365 Audit-Log und Rechnungsprüfung: Nachweise, die Verwaltungen liefern müssen
› Notfallübung für die Verwaltungs-IT: SharePoint verschlüsselt, Admin-Konto übernommen, Bürgertelefon tot
› Backup und Wiederherstellung in Microsoft 365: Die Risikoentscheidung fürs Rechnungsprüfungsamt
› Schutzbedarf und Microsoft 365: IT-Grundschutz-Abgleich für die Praxis
› Oversharing im Verwaltungs-Tenant: Warum Copilot die Personalakte findet
› Microsoft 365 und das kommunale Rechenzentrum: Rollen, Schnittstellen, Zweitmeinung
› Microsoft-365-Einführung in der Verwaltung: Konzeptionsphase in 4,5 Tagen und die Beschlussvorlage