

Break-Glass-Konten anlegen und überwachen

Es gibt zwei Sorten von Administratoren: die, die schon einmal einen kompletten Tenant ausgesperrt haben, und die, denen es noch bevorsteht. Die erste Gruppe erkennst du daran, dass sie beim Stichwort Break-Glass nicht mehr grinst.

Das Szenario ist immer dasselbe und immer langweilig. Freitagnachmittag, eine neue Conditional-Access-Richtlinie, ein Häkchen bei „Alle Benutzer“, ein vergessener Ausschluss. Speichern. Dann meldest du dich ab, weil du feierabendmüde bist, und stellst dreißig Sekunden später fest, dass du dich nicht mehr anmelden kannst. Und deine Kollegin auch nicht. Und niemand sonst. Der Tenant läuft munter weiter, die Postfächer kommen an, Teams telefoniert fröhlich vor sich hin — nur ändern kann daran keiner mehr etwas. Ab hier hilft dir entweder ein Break-Glass-Konto oder ein Microsoft-Supportfall, dessen Bearbeitungszeit sich in Werktagen misst, nicht in Minuten.

Break-Glass-Konten sind das billigste Stück Sicherheitsarchitektur, das du in einem Microsoft-365-Tenant bauen kannst. Sie kosten keine Lizenz, ihre Einrichtung dauert eine halbe Stunde, und sie sind der Unterschied zwischen einer peinlichen Viertelstunde und einem Betriebsausfall. Die Betonung liegt allerdings auf **anlegen und überwachen**. Ein Break-Glass-Konto ohne Alarm ist kein Notausgang, sondern eine unbewachte Hintertür mit dauerhaft aktiver Rolle „Globaler Administrator“. Genau daran scheitern in der Praxis mehr Tenants als am fehlenden Konto.

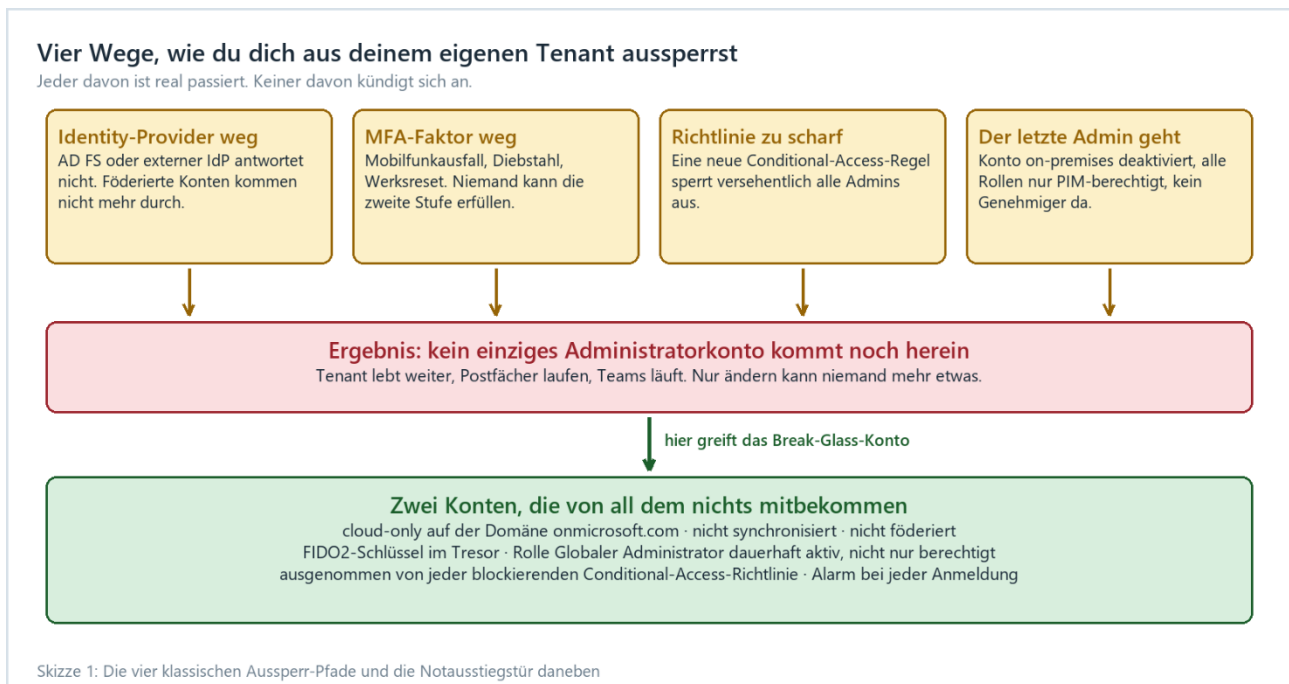
Dieser Beitrag gehört zur Serie [Microsoft 365 Security](#) und beschreibt Handlungsfeld A: was du konkret anlegst, wo du die Schlüssel hinlegst, wie du den Alarm baust und wie du beides am Leben hältst.

Warum zwei Konten, die niemandem gehören

Microsoft empfiehlt mindestens zwei Notfallzugangskonten. Nicht eines. Der Grund ist unspektakulär: Ein einzelnes Konto ist ein Einzelfehlerpunkt. Der Sicherheitsschlüssel geht kaputt, das Kuvert ist unauffindbar, der einzige Mensch mit der Tresorkombination liegt mit Grippe im Bett. Zwei Konten mit getrennten Schlüsseln an getrennten Orten kosten dich genau nichts extra und halbieren die Wahrscheinlichkeit, dass du im Ernstfall dumm dastehst.

Die Ausfälle, die dich wirklich treffen

Die Microsoft-Dokumentation zählt eine Handvoll Szenarien auf, in denen Notfallzugangskonten gebraucht werden. Sie klingen alle theoretisch, bis eines davon eintritt.



Skizze 1: Die vier klassischen Aussperr-Pfade — und die Notausstiegstür daneben.

Bemerkenswert ist der vierte Fall, weil er so gerne übersehen wird: Wenn alle Zuweisungen für „Globaler Administrator“ und „Administrator für privilegierte Rollen“ nur berechtigt statt aktiv sind, die Aktivierung eine Genehmigung erfordert und kein Genehmiger eingetragen ist, dann ist die Tenant-Verwaltung effektiv gesperrt. Aktive Inhaber dieser Rollen sind die Standardgenehmiger — aber es gibt keine aktiven Inhaber. Eine geschlossene Schleife, in die man sich mit lauter guten Absichten hineinkonfiguriert.

Warum ausgerechnet cloud-only

Die Notfallzugangskonten müssen reine Cloud-Konten auf der Domäne **onmicrosoft.com** sein. Nicht föderiert, nicht aus dem lokalen Verzeichnis synchronisiert, nicht auf deiner verifizierten Hausdomäne. Der Grund ist die Abhängigkeitskette: Ein Konto auf deiner eigenen Domäne kann von einem DNS-Problem, einer abgelaufenen Föderationsvertrauensstellung oder einer kaputten Verzeichnissynchronisierung mit in den Abgrund gerissen werden. Das Notfallkonto muss aber genau dann funktionieren, wenn alles andere kaputt ist. Es darf deshalb von gar nichts abhängen, was du selbst betreibst.

Dieselbe Logik gilt in die andere Richtung: Halte den Notfallzugang für die lokale Infrastruktur und den Notfallzugang für die Cloud strikt getrennt. Ein Notfallkonto, das in Active Directory gemastert wird, ist kein Notfallkonto, sondern eine Wette darauf, dass die Verzeichnissynchronisierung noch läuft.

Fakten: Die Leitplanken aus der Microsoft-Dokumentation

Mindestens zwei Notfallzugangskonten, ausschließlich cloud-only auf der Domäne onmicrosoft.com, ohne Abhängigkeit von einem föderierten Identitätsanbieter.

Phishing-resistente Authentifizierung — Passkey (FIDO2) empfohlen, alternativ zertifikatsbasierte Authentifizierung, wenn du ohnehin eine PKI betreibst. Und zwar bewusst eine andere Methode als bei deinen normalen Administratorkonten.

Rolle „Globaler Administrator“ dauerhaft aktiv zugewiesen, nicht nur berechtigt. Kein PIM, keine zeitgebundene Aktivierung, keine Genehmigungskette.

Anmeldedaten und Geräte dürfen nicht ablaufen und nicht in eine automatische Bereinigung wegen

Nichtnutzung geraten.

Ausschluss aus allen Conditional-Access-Richtlinien, die die Anmeldung blockieren oder einschränken. Richtlinien im Nur-Bericht-Modus brauchen keinen Ausschluss.

Alarm auf jede Nutzung, Funktionsprüfung mindestens alle 90 Tage.

Die Konten anlegen: Handlungsfeld A in dreißig Minuten

Das Folgende ist bewusst kurz gehalten, weil es kurz ist. Wer daraus ein Projekt macht, hat das Prinzip nicht verstanden.

Schritt 1: Zwei Cloud-Konten anlegen

Lege zwei Benutzer an, etwa **bg-01@deinetenant.onmicrosoft.com** und **bg-02@deinetenant.onmicrosoft.com**. Verwende keine Namen, die nach einem Menschen aussehen, und ordne die Konten niemandem persönlich zu. Notfallzugangskonten gehören der Organisation, nicht einer Person. Trage keine private Mobilnummer, keine private Mailadresse und keine persönliche Geräteregistrierung ein — sonst hängt der Notfallzugang am Handy eines Menschen, der im Ernstfall gerade im Flugzeug sitzt oder das Unternehmen vor drei Monaten verlassen hat.

Die Alternative, für die es gute Argumente gibt: personengebundene Notfallkonten pro Administrator. Das erhöht die Nachvollziehbarkeit und erlaubt den Zugriff aus dem Homeoffice. Es erhöht aber auch die Anzahl hochprivilegierter Konten und den Aufwand für Test und Dokumentation. Im Mittelstand fährst du mit zwei unpersönlichen Konten in aller Regel besser.

Schritt 2: FIDO2 statt Passwort

Das Passwort auf dem Zettel im Tresor war zehn Jahre lang der Standard. Es ist heute keiner mehr, und zwar nicht aus Geschmacksgründen, sondern weil es nicht mehr funktioniert. Microsoft empfiehlt für Notfallzugangskonten ausdrücklich einen Passkey (FIDO2) oder zertifikatsbasierte Authentifizierung. Beide Verfahren erfüllen die MFA-Anforderung, beide brauchen weder Mobilfunknetz noch Authenticator-App noch ein registriertes Telefon.

Praktisch heißt das: Du aktivierst in der Authentifizierungsmethoden-Richtlinie die Methode Passkey (FIDO2), registrierst für jedes der beiden Konten einen eigenen Hardware-Sicherheitsschlüssel und legst den Schlüssel samt PIN in den Tresor. Passkeys (FIDO2) sind in allen Entra-ID-Editionen enthalten, auch in der kostenfreien — dafür brauchst du keine Zusatzlizenz. Die einzige echte Ausgabe sind zwei Hardware-Schlüssel, und die kosten weniger als eine Stunde Beratung.

Wähle bewusst eine andere Methode als bei deinen regulären Administratorkonten. Wenn deine Admins mit der Authenticator-App arbeiten, nimm für Break-Glass Hardware-Schlüssel. Der Sinn der Übung ist ja gerade, dass ein Ausfall oder eine Fehlkonfiguration der einen Methode die andere nicht mitreißt. Wie du Passkeys darüber hinaus in der Breite einführst, steht in [Passwordless: FIDO2 und Passkeys in der Praxis](#).

Schritt 3: Rolle dauerhaft aktiv zuweisen

Weise beiden Konten die Rolle „Globaler Administrator“ zu — als dauerhaft aktive Zuweisung, nicht als berechnete. Das widerspricht allem, was du sonst über Just-in-Time-Zugriff gelernt hast, und das ist Absicht. Ein Notfallkonto, das erst über Privileged Identity Management aktiviert

werden muss, ist in genau dem Moment nutzlos, in dem PIM oder die Genehmigungskette Teil des Problems ist. Der Preis dafür sind zwei dauerhaft privilegierte Konten im Tenant — und den bezahlst du mit Überwachung, nicht mit Zugriffsbeschränkung.

Schritt 4: Ausschluss aus den Conditional-Access-Richtlinien

Lege eine Sicherheitsgruppe an, zum Beispiel **EmergencyAccess**, nimm die beiden Konten hinein und schließe diese Gruppe in jeder Conditional-Access-Richtlinie aus, die die Anmeldung blockiert oder einschränkt. Über eine Gruppe statt über Einzelkonten, weil du sonst beim nächsten Umbau eine Richtlinie vergisst. Wie du deine Richtlinien so schneidest, dass dieser Ausschluss überhaupt sauber möglich ist, steht in [Conditional Access: Baselines, die nicht nerven](#).

Art der Richtlinie	Ausschluss nötig?	Begründung
MFA erzwingen (Alle Benutzer)	Ja	Wenn die MFA-Registrierung des Kontos aus irgendeinem Grund nicht greift, sperrt die Richtlinie genau im Notfall aus.
Konformes Gerät verlangen	Ja	Der Notfall-Arbeitsplatz ist im Zweifel ein frisch aufgesetztes Gerät, das Intune nie gesehen hat.
Standort- oder IP-Beschränkung	Ja	Im Notfall sitzt niemand zwingend im Büronetz.
Anmeldehäufigkeit / Sitzungssteuerung	Ja	Zählt zu den einschränkenden Steuerungen.
Legacy-Authentifizierung blockieren	Nein	Blockiert nur veraltete Protokolle. Dein Break-Glass-Konto meldet sich modern an.
Richtlinie im Nur-Bericht-Modus	Nein	Blockiert nichts und braucht laut Microsoft keinen Ausschluss.
Risikobasierte Richtlinien	Ja	Eine Anmeldung aus dem Nichts nach Monaten der Ruhe sieht für die Risikobewertung verdächtig aus — zu Recht, aber unpassend.

Und danach: Prüfe die Ausnahme, statt sie zu glauben. Der Ausschluss steht in der Richtlinie, aber ob die Gruppenmitgliedschaft wirklich sitzt und ob nicht doch eine zweite Richtlinie dazwischenfunkt, siehst du erst beim Testlauf. Das ist der Grund, warum der halbjährliche Test weiter unten kein Bürokratie-Ritual ist.

Wichtig: Die Ausnahme hilft dir nur gegen deine eigenen Richtlinien

Microsoft erzwingt inzwischen MFA auf Plattformebene: seit Oktober 2024 für Azure-Portal, Microsoft Entra Admin Center und Intune Admin Center, seit Februar 2025 für das Microsoft 365 Admin Center, seit dem 1. Oktober 2025 für Azure CLI, Azure PowerShell, die Azure-Mobile-App, Infrastructure-as-Code-Werkzeuge und die Verwaltungs-REST-API bei schreibenden Vorgängen.

Die Antwort auf die Frage nach Ausnahmen ist in der Microsoft-Dokumentation unmissverständlich: Die Erzwingung gilt für alle Benutzerkonten, ausdrücklich auch für Break-Glass-Konten und ausdrücklich unabhängig von Benutzerausschlüssen. Es gibt kein Opt-out, nur einen Aufschub für Phase 2 — und der endet am 1. Juli 2026.

Was heißt das für dich? Ein Break-Glass-Konto mit einem langen Passwort auf einem Zettel ist seit der Erzwingung ein totes Konto. Es meldet sich am Portal an und fliegt an der Plattformregel auf. Passkey (FIDO2) oder zertifikatsbasierte Authentifizierung sind damit keine Kür mehr, sondern die Voraussetzung dafür, dass das Konto im Ernstfall überhaupt noch etwas tun kann.

Was die Conditional-Access-Ausnahme abschaltet — und was sie nicht abschaltet

Die Anmeldung eines Break-Glass-Kontos läuft von oben nach unten durch vier Prüfstellen.

1 Security Defaults

Entweder Security Defaults oder Conditional Access — beides zusammen geht nicht. Mit Security Defaults gibt es keine Ausnahmeliste. Break-Glass braucht deshalb Conditional Access.

je nach Tenant

2 Conditional Access

Deine Richtlinien: Gerätekonformität, Standort, Sitzungssteuerung, Anmeldehäufigkeit. Hier wird die Gruppe EmergencyAccess ausgeschlossen — und nur hier.

Ausnahme greift

3 Erzwungene Plattform-MFA

Microsoft erzwingt MFA für Azure-Portal, Entra Admin Center, Intune, Microsoft 365 Admin Center sowie Azure CLI, Azure PowerShell und die Verwaltungs-REST-API. Break-Glass-Konten sind ausdrücklich nicht ausgenommen.

Ausnahme greift NICHT

4 Authentifizierungsmethode

Passkey (FIDO2) oder zertifikatsbasierte Authentifizierung. Beides erfüllt die MFA-Anforderung ohne Telefon, ohne App, ohne Netz beim Nutzer.

kein Sicherheitsnetz

Merksatz: Die Ausnahme schützt dich vor deiner eigenen Richtlinie. Sie schützt dich nicht vor Microsofts Plattformregel. Ein Break-Glass-Konto, das nur ein Passwort kennt, ist an Schicht 3 tot — genau dann, wenn du es brauchst.

Skizze 2: Die vier Prüfstellen einer Break-Glass-Anmeldung

Skizze 2: Die vier Prüfstellen, die eine Break-Glass-Anmeldung passiert. Nur an Stelle 2 wirkt dein Ausschluss.

Phase	Ab wann	Betroffen	Vorgangsarten
Phase 1	Oktober 2024	Azure-Portal, Microsoft Entra Admin Center, Intune Admin Center	Alle Vorgänge, auch Lesen
Phase 1 (M365)	Februar 2025	Microsoft 365 Admin Center	Alle Vorgänge
Phase 2	1. Oktober 2025	Azure CLI, Azure PowerShell, Azure-Mobile-App, IaC-Werkzeuge, REST-API der Steuerungsebene	Anlegen, Ändern, Löschen — Lesen bleibt frei
Aufschub Phase 2	spätestens 1. Juli 2026	auf Antrag durch einen globalen Administrator	danach greift die Erzwingung endgültig

Schritt 5: Keine Lizenz zuweisen

Ein Notfallzugangskonto braucht keine Microsoft-365-Lizenz. Es soll kein Postfach haben, kein OneDrive, keinen Teams-Zugang. Es soll sich anmelden und verwalten können, und das kann es mit den Bordmitteln von Entra ID. Der Nebeneffekt ist angenehm: Zwei hochprivilegierte Konten ohne Postfach sind zwei Konten weniger, über die jemand Daten abziehen oder Mails versenden kann.

Tipp: Kein Postfach heißt nicht kein Kontakt

Weil das Konto kein Postfach hat, kann es auch keine Benachrichtigungen empfangen. Trage als

alternative Kontaktadresse deshalb nichts Persönliches ein und richte den Alarmweg konsequent über die Aktionsgruppe deiner Alarmregel ein, nicht über das Konto selbst.

Prüfe außerdem, ob das Konto in irgendeiner automatischen Bereinigung landet — etwa in einem Skript, das Konten ohne Anmeldung seit 180 Tagen deaktiviert. Ein Break-Glass-Konto ist definitionsgemäss inaktiv. Genau deshalb fällt es solchen Aufräumroutinen als Erstes zum Opfer.

Tipp: Weiter im Thema

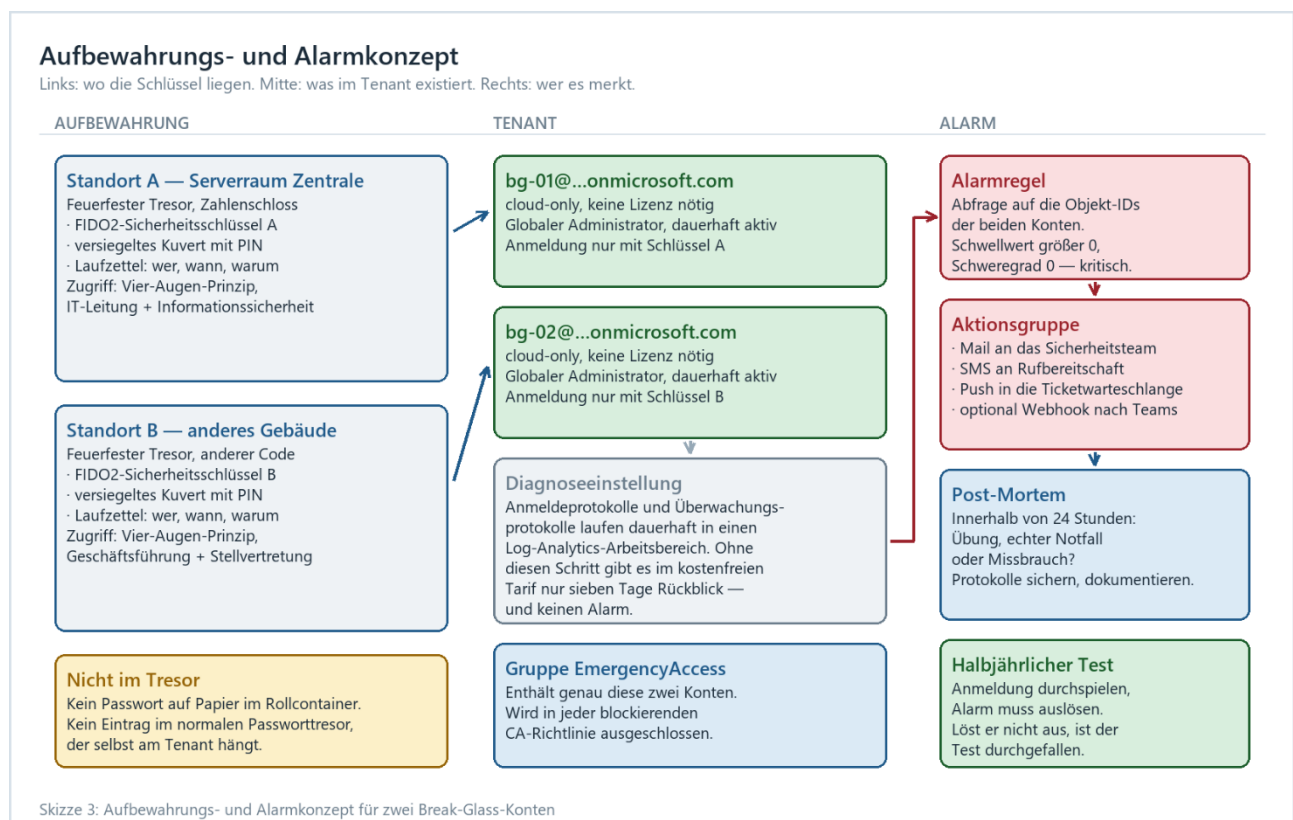
Break-Glass hängt nicht in der Luft. Diese drei Themen greifen direkt ineinander:

- › [Conditional Access: Baselines, die nicht nerven](#)
- › [Security Defaults oder Conditional Access?](#)
- › [Alert Policies und Benachrichtigungen richtig aufsetzen](#)

Aufbewahrung: der Tresor, nicht der Rollcontainer

Die Technik ist nach dreißig Minuten fertig. Die Aufbewahrung ist der Teil, an dem die meisten Konzepte in der Praxis scheitern — meist still und ohne dass es jemand merkt, bis der Ernstfall eintritt.

Microsoft formuliert das nüchtern: Bewahre die Anmeldedaten in sicheren, feuerfesten Behältnissen an **getrennten** Orten auf, zugänglich für mehrere Mitglieder des Administrationsteams. Zwei Tresore in demselben Serverraum sind ein Tresor. Ein Sicherheitsschlüssel im Schreibtisch der IT-Leitung ist kein Konzept, sondern eine Gewohnheit.



Skizze 3: Aufbewahrungs- und Alarmkonzept — Schlüssel getrennt, Konten getrennt, Alarmweg gemeinsam.

	Konto A	Konto B
Anmeldename	bg-01@...onmicrosoft.com	bg-02@...onmicrosoft.com

Anmeldemethode	FIDO2-Schlüssel A	FIDO2-Schlüssel B
Aufbewahrungsort	Feuerfester Tresor, Serverraum Zentrale	Feuerfester Tresor, zweites Gebäude
Zugriff	IT-Leitung und Informationssicherheit, Vier-Augen-Prinzip	Geschäftsführung und Stellvertretung, Vier-Augen-Prinzip
Kuvert	Versiegelt, mit PIN und Laufzettel	Versiegelt, mit PIN und Laufzettel
Testtermin	Januar	Juli
Rolle	Globaler Administrator, dauerhaft aktiv	Globaler Administrator, dauerhaft aktiv

Das versiegelte Kuvert ist kein Sicherheitsmechanismus, sondern ein Nachweismechanismus. Ein gebrochenes Siegel ohne Eintrag auf dem Laufzettel ist ein Vorfall — unabhängig davon, ob im Tenant irgendetwas passiert ist. Und die Kombination des Tresors änderst du regelmäßig sowie immer dann, wenn jemand mit Zugriff das Unternehmen verlässt.

Ein weiterer Punkt, der gerne untergeht: Wer ein Notfallkonto benutzt, soll das von einem dafür vorgesehenen, abgesicherten Arbeitsplatz aus tun — im Idealfall von einer Privileged Access Workstation. Im Mittelstand ist das oft ein einzelner, sauber aufgesetzter Laptop, der im selben Tresorraum liegt und sonst nichts tut. Das ist kein Luxus: Ein Notfallkonto auf einem Rechner, der seit Wochen ungepatcht im Netz hängt, ist ein sehr teurer Hardware-Schlüssel an einem sehr offenen Fenster.

Warnung: Der Passworttresor, der am Tenant hängt

Ein beliebter und wirklich unangenehmer Zirkelschluss: Die Zugangsdaten der Break-Glass-Konten liegen im zentralen Passwortmanager. Der Passwortmanager meldet sich per Single Sign-on gegen Entra ID an. Entra ID ist ausgesperrt. Ergebnis: Du kommst an die Notfallzugangsdaten nicht heran, weil du dafür genau den Zugang brauchst, den du gerade verloren hast.

Dasselbe gilt für die Dokumentation des Notfallprozesses. Wenn sie ausschließlich in SharePoint Online liegt, ist sie im Ernstfall genauso unerreichbar. Eine ausgedruckte Fassung im Tresor ist unmodern und funktioniert.

Alarm bei jeder Anmeldung

Warnung: Break-Glass ohne Alarm ist eine Hintertür

Du hast gerade zwei Konten mit dauerhaft aktiver Rolle „Globaler Administrator“ angelegt, sie aus allen einschränkenden Richtlinien ausgenommen und ihre Anmeldedaten an einen Ort gelegt, an den mehrere Personen herankommen. Das ist genau die Sorte Konto, die ein Angreifer sich wünscht: maximal privilegiert, minimal reglementiert, und niemand schaut hin.

Ohne Alarm ist das keine Notausstiegstür, sondern eine unbewachte Hintertür — und du hast sie selbst eingebaut, dokumentiert und mit einem Schild „Notfall“ versehen.

Die Regel ist deshalb einfach und kennt keine Ausnahme: Jede Anmeldung, jede Änderung an der Rolle, jede hinzugefügte Anmeldemethode dieser Konten löst einen Alarm mit höchster Priorität aus. Weil ein Break-Glass-Konto per Definition nie benutzt wird, ist jede Aktivität entweder ein geplanter Test, ein echter Notfall oder ein Vorfall. Drei Zustände, von denen zwei sofortige Aufmerksamkeit verlangen.

Der Weg der Signale

Bevor du eine Alarmregel baust, musst du verstehen, welche Kette da eigentlich hängt — denn getestet wird später die ganze Kette, nicht nur das Konto.



Skizze 4: Von der Anmeldung bis zum klingelnden Telefon — und die zwei Stellen, an denen es in der Praxis reißt.

Der entscheidende und am häufigsten vergessene Schritt ist die Diagnoseeinstellung. Die Anmeldeprotokolle von Entra ID sind im kostenfreien Tarif nur sieben Tage lang sichtbar, mit einer Lizenz Entra ID P1 oder P2 dreißig Tage. Erst wenn du die Protokolle per Diagnoseeinstellung dauerhaft in einen Log-Analytics-Arbeitsbereich schiebst, hast du überhaupt eine Datenquelle, auf die eine Alarmregel zugreifen kann — und nebenbei eine Aufbewahrung, die für Nachweiszwecke taugt.

Azure Monitor, Sentinel oder Alert Policy

Es gibt drei praktikable Wege, den Alarm zu bauen. Sie unterscheiden sich weniger in der Qualität als im Preis und in dem, was du sowieso schon betreibst.

Weg	Voraussetzung	Stärke	Schwäche	Passt zu
Azure Monitor Alarmregel	Log-Analytics-Arbeitsbereich, Diagnoseeinstellung	Genau eine Regel, volle Kontrolle über Abfrage, Schwellwert und Kanäle	Kosten für Datenaufnahme und Aufbewahrung, Einrichtung im Azure-Portal	Standardfall — der von Microsoft dokumentierte Weg
Microsoft Sentinel	Sentinel auf dem Arbeitsbereich aktiviert	Korrelation mit anderen Quellen, Fallverwaltung, Automatisierung, Aufbewahrung	Deutlich teurer, lohnt sich nicht allein für Break-Glass	Tenants, die Sentinel ohnehin betreiben
Alert Policy im Defender-Portal	Microsoft-365-Überwachung aktiv	Ohne Azure-Abonnement, schnell eingerichtet, Mailbenachrichtigung inklusive	Zielt auf Microsoft-365-Aktivitäten, nicht auf jede Entra-Anmeldung; größer als eine KQL-Abfrage	Kleine Tenants ohne Azure-Ressourcen

Für die Alarmregel in Azure Monitor brauchst du zuerst die Objekt-IDs der beiden Konten. Die stehen im Microsoft Entra Admin Center in den Benutzereigenschaften. Danach legst du unter

Monitor eine Alarmregel mit dem Signal „Benutzerdefinierte Protokollsuche“ an. Die Abfrage ist unspektakulär:

```
// Alle Anmeldungen der beiden Break-Glass-Konten
SigninLogs
| where UserId == "<Objekt-ID bg-01>" or UserId == "<Objekt-ID bg-02>"
| project TimeGenerated, UserPrincipalName, UserId, IPAddress,
    AppDisplayName, ResultType, ResultDescription
```

Als Alarmlogik setzt du den Schwellwerttyp auf statisch, den Operator auf „größer als“ und den Schwellwert auf 0. Übersetzt: Ein einziger Treffer reicht. Der Schweregrad gehört auf „0 – kritisch“, denn wenn diese Regel feuert, ist entweder Notfall oder Einbruch. Als Aktionsgruppe hinterlegst du mindestens zwei Kanäle, die nicht demselben Ausfall unterliegen: eine Mail an das Sicherheitsteam und eine SMS an die Rufbereitschaft. Eine Mailbenachrichtigung an ein Postfach im gerade ausgesperrten Tenant ist nur eingeschränkt hilfreich.

Tipp: Der Alarm braucht einen Weg, der ohne deinen Tenant funktioniert

Denk den Ausfall zu Ende. Wenn dein Tenant Probleme hat, kann auch die Mailzustellung Probleme haben. Eine SMS an eine Rufbereitschaftsnummer, eine Push-Benachrichtigung über einen externen Dienst oder ein Webhook in ein System außerhalb von Microsoft 365 sind deshalb keine Paranoia, sondern schlicht die zweite unabhängige Zustellstrecke.

Worauf du alarmierst

Die Anmeldung ist der offensichtliche Auslöser, aber nicht der einzige. Die Sicherheitsbetriebs-Leitlinien von Microsoft nennen vier Ereignisse, die jedes für sich auf einen Angriffsversuch hindeuten können.

Ereignis	Datenquelle	Priorität	Warum es zählt
Anmeldung, erfolgreich oder nicht	Anmeldeprotokolle	Kritisch	Das Konto wird per Definition nie benutzt. Jede Anmeldung ist erklärungsbedürftig.
Passwort geändert	Überwachungsprotokolle	Kritisch	Klassischer Übernahmeschritt. Legitim passiert das nur im Zuge eines geplanten Umbaus.
Rolle oder Berechtigung geändert	Überwachungsprotokolle	Kritisch	Wer dem Konto Rollen wegnimmt, sabotiert deinen Notausstieg. Wer welche hinzufügt, baut sich etwas auf.
Anmeldemethode hinzugefügt oder geändert	Überwachungsprotokolle	Kritisch	Ein zusätzlicher Sicherheitsschlüssel oder ein Temporary Access Pass an diesem Konto ist der stille Nachschlüssel.
Konto aus der Ausschlussgruppe entfernt	Überwachungsprotokolle	Hoch	Fällt sonst erst beim nächsten Testlauf auf — also im schlimmsten Fall Monate später.
Konto deaktiviert oder gelöscht	Überwachungsprotokolle	Hoch	Häufig kein Angriff, sondern eine gut gemeinte Aufräumaktion. Trotzdem ein Vorfall.

Wenn du ohnehin überlegst, deine Protokolle zusammenzuführen, ist Break-Glass ein guter Anlass, die Frage einmal grundsätzlich zu stellen — die Abwägung steht in [Microsoft Sentinel anbinden: wann es sich lohnt](#). Und wenn du gerade dabei bist, die Benachrichtigungswege im Microsoft-365-

Umfeld aufzuräumen, gehört [Alert Policies und Benachrichtigungen richtig aufsetzen](#) direkt daneben.

Was nach dem Alarm passiert

Ein Alarm, auf den niemand reagiert, ist ein teurer Weg, ein Postfach zu füllen. Lege deshalb vorab fest, wer bei Auslösung was tut. Microsoft empfiehlt ein Team für die Nachbetrachtung, das nach jeder Nutzung eines Notfallkontos drei Fragen beantwortet: War es eine geplante Übung? War es ein echter Notfall, in dem kein Administrator sein reguläres Konto nutzen konnte? Oder war es Missbrauch?

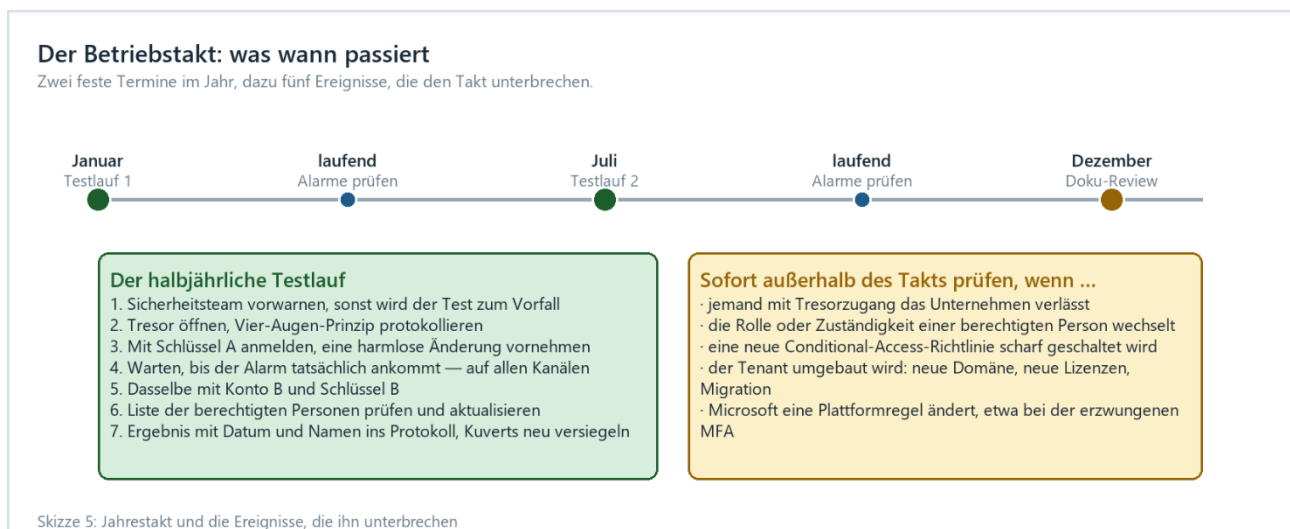
Anschließend werden die Protokolle gesichert und die durchgeführten Aktionen daraufhin geprüft, ob sie zum genehmigten Zweck passen. Das ist kein Misstrauen gegenüber den Kolleginnen und Kollegen, sondern der Grund, warum die Aufsicht dir bei der nächsten Prüfung glaubt. Wenn der dritte Fall eintritt, greift dein regulärer Ablauf — beschrieben in [Incident-Response-Plan für Microsoft 365](#) und, für die konkrete Aufräumarbeit, in [Kompromittiertes Konto erkennen und aufräumen](#).

Testen und dokumentieren: der Teil, der wehtut

Bis hierhin war alles Technik, und Technik ist einfach. Jetzt kommt der Teil, der Disziplin verlangt und deshalb in neun von zehn Tenants nach dem ersten Jahr eingeschlafen ist. Ein Break-Glass-Konzept ist kein Zustand, sondern eine Gewohnheit.

Der halbjährliche Testlauf

Microsoft empfiehlt eine Funktionsprüfung mindestens alle 90 Tage. Im Mittelstand ist ein fester halbjährlicher Termin realistischer und immer noch deutlich besser als der vierteljährliche Termin, den nach zwei Runden niemand mehr wahrnimmt. Setz ihn in den Kalender, mit Vertretung, und behandle ihn wie einen Wartungstermin an der Brandmeldeanlage: unspektakulär, verpflichtend, protokolliert.



Skizze 5: Zwei feste Termine im Jahr, dazu die Ereignisse, die eine außerplanmäßige Prüfung auslösen.

Schritt	Was du prüfst	Bestanden, wenn ...
1. Vorwarnen	Sicherheitsteam und Rufbereitschaft informieren	... alle Beteiligten wissen, dass gleich ein kritischer Alarm kommt
2. Tresor	Öffnen im Vier-Augen-Prinzip, Siegel	... Schlüssel, Kuvert und Laufzettel

	und Laufzettel prüfen	vollständig und unversehrt sind
3. Anmeldung	Mit Schlüssel A am Entra Admin Center anmelden	... die Anmeldung ohne Umweg gelingt, ohne Blockade durch eine Richtlinie
4. Handlungsfähigkeit	Eine harmlose Änderung vornehmen und wieder zurücknehmen	... das Konto tatsächlich schreiben darf, nicht nur lesen
5. Alarm	Warten, bis die Benachrichtigung eintrifft — auf jedem Kanal	... Mail und SMS ankommen, nicht nur die Regel im Portal einen Treffer zeigt
6. Zweites Konto	Schritte 2 bis 5 mit Konto B und Schlüssel B	... beide Wege unabhängig voneinander funktionieren
7. Personenkreis	Liste der Zugriffsberechtigten durchgehen	... niemand darauf steht, der das Unternehmen oder die Rolle verlassen hat
8. Protokoll	Ergebnis mit Datum, Namen und Auffälligkeiten festhalten	... das Protokoll unterschrieben ist und die Kuverts neu versiegelt sind

Der wichtigste Schritt ist Nummer 5, und er wird am häufigsten weggelassen, weil man ja schon in der Anmeldung war und es eilig hat. Wenn der Alarm nicht ankommt, ist der Test durchgefallen — auch dann, wenn die Anmeldung tadellos geklappt hat. Ein funktionierendes Konto ohne funktionierenden Alarm ist genau der Zustand, den du vermeiden wolltest. Wenn du solche Abläufe ohnehin regelmäßig übst, hängt der Break-Glass-Test hervorragend an einer [Feuerwehübung: Security-Notfälle im Team trainieren](#).

Was in die Dokumentation gehört

Die Dokumentation ist kein Selbstzweck. Sie ist das, was im Ernstfall ein Mensch liest, der nervös ist, unter Zeitdruck steht und vielleicht nicht derjenige ist, der das Konzept gebaut hat. Schreib sie entsprechend.

- **Wer darf entscheiden.** Namentlich benannte Personen und deren Vertretung, die die Nutzung eines Notfallkontos freigeben dürfen. Nicht „die IT“, sondern zwei Namen und zwei Telefonnummern.
- **Wann ist es ein Notfall.** Eine kurze Liste an Kriterien, damit niemand aus Bequemlichkeit das Break-Glass-Konto nimmt, weil sein eigenes gerade eine MFA-Abfrage stellt.
- **Wie kommt man an die Schlüssel.** Standort, Zugriffsberechtigte, Vier-Augen-Prinzip, Umgang mit dem Siegel und dem Laufzettel.
- **Der Anmeldeweg selbst.** Konkrete Schritte inklusive der Adresse des Portals und dem Hinweis, dass der Sicherheitsschlüssel eine PIN braucht. Im Stress vergisst man Erstaunliches.
- **Was danach passiert.** Meldung an das Sicherheitsteam, Nachbetrachtung innerhalb von 24 Stunden, Rückgabe des Schlüssels, neues Siegel, Eintrag im Protokoll.
- **Wo diese Dokumentation liegt.** Mindestens eine Fassung außerhalb des Tenants — ausgedruckt im Tresor, damit sie auch dann lesbar ist, wenn SharePoint Online gerade Teil des Problems ist.

Fakten: Was der Nachweis wert ist

Für regulierte Branchen ist der Notfallzugang kein Nice-to-have, sondern ein Prüfpunkt. Microsoft ordnet die Notfallzugangskonten ausdrücklich den Anforderungen an Notfallzugriffsverfahren zu und nennt drei Nachweise: die Überwachung der Anmelde- und Überwachungsprotokolle, die Nachbetrachtung nach jeder Nutzung und die regelmäßige Funktionsprüfung.

Das ist praktisch, weil du damit dieselbe Arbeit zweimal verwerten kannst. Wer im Rahmen von NIS2

oder einer ISO-Zertifizierung Belege für die Verwaltung privilegierter Zugänge braucht, hält mit dem Prüfprotokoll aus dem halbjährlichen Testlauf einen sauberen Nachweis in der Hand — vorausgesetzt, es existiert.

Wenn jemand geht

Der Personalwechsel ist der Klassiker, an dem Break-Glass-Konzepte still verrotten. Wer Zugriff auf den Tresor hatte und das Unternehmen verlässt, löst drei Dinge aus: Die Tresorkombination wird geändert, der Personenkreis in der Dokumentation wird aktualisiert, und es gibt einen außerplanmäßigen Testlauf. Dasselbe gilt bei einem Rollenwechsel innerhalb des Hauses. Das kostet eine halbe Stunde und ist der Unterschied zwischen einem gelebten Konzept und einem Ordner im Regal. Wenn du gerade dabei bist, den gesamten Tenant durchzugehen, findest du die Break-Glass-Konten übrigens auch auf der Liste in [Tenant-Härtung: die 20 wichtigsten Schrauben](#).

Häufige Fragen

Reicht nicht ein einziges Break-Glass-Konto?

Technisch funktioniert eines. Praktisch ist es ein Einzelfehlerpunkt: Der Sicherheitsschlüssel geht kaputt, das Kuvert ist weg, der Tresor klemmt, die eine Person mit der Kombination ist nicht erreichbar. Microsoft empfiehlt aus genau diesem Grund mindestens zwei. Das zweite Konto kostet dich einen zusätzlichen Hardware-Schlüssel und zehn Minuten Arbeit. Spar an etwas anderem.

Kann ich das Break-Glass-Konto von der erzwungenen MFA ausnehmen?

Nein. Die Microsoft-Dokumentation ist an dieser Stelle eindeutig: Die Erzwingung gilt für alle Benutzerkonten, ausdrücklich einschließlich Break-Glass-Konten, und Benutzerausschlüsse helfen nicht. Es gibt kein Opt-out. Für Phase 2 konnte ein globaler Administrator einen Aufschub bis spätestens 1. Juli 2026 beantragen — das war ein Aufschub, keine Ausnahme. Die Lösung ist nicht der Ausnahmeantrag, sondern ein Passkey (FIDO2) oder ein Zertifikat.

Brauchen die Konten eine Microsoft-365-Lizenz?

Nein. Ein Notfallzugangskonto verwaltet, es arbeitet nicht. Es braucht kein Postfach, kein OneDrive und keinen Teams-Zugang. Passkeys (FIDO2) sind in allen Entra-ID-Editionen enthalten, auch in der kostenfreien. Die einzige Einschränkung ohne Lizenz betrifft Conditional Access selbst — dafür brauchst du Entra ID P1 oder P2. Ohne diese Lizenz arbeitest du mit Security Defaults, und dann hast du ein anderes Problem, siehe nächste Frage.

Was, wenn ich Security Defaults statt Conditional Access nutze?

Dann kannst du keine Ausnahmen definieren — Security Defaults kennen keine Ausschlussliste, das ist genau ihr Prinzip. Für ein Break-Glass-Konzept im engeren Sinn brauchst du deshalb Conditional Access und damit Entra ID P1. Immerhin: Security Defaults erzwingen MFA für alle, auch für dein Notfallkonto, das damit wenigstens nicht an der Plattformregel scheitert. Die Abwägung im Detail steht in [Security Defaults oder Conditional Access?](#).

Wie oft muss ich wirklich testen?

Microsoft nennt als Mindestmaß alle 90 Tage. Ein halbjährlicher Termin, der tatsächlich stattfindet, ist mehr wert als ein vierteljährlicher, der im Kalender steht und verschoben wird.

Zusätzlich testest du immer dann außerplanmäßig, wenn sich der Personenkreis ändert, wenn du größere Änderungen an den Conditional-Access-Richtlinien vornimmst oder wenn Microsoft an den Plattformregeln dreht.

Kann ich Break-Glass-Konten in Privileged Identity Management verwalten?

Du kannst, aber du solltest die Rollenzuweisung dort als dauerhaft aktiv führen, nicht als berechtigt. Eine Aktivierung über PIM setzt voraus, dass PIM erreichbar ist, dass die MFA-Anforderung erfüllbar ist und dass gegebenenfalls ein Genehmiger antwortet. Drei Abhängigkeiten, die im Notfall genau die drei Dinge sind, die nicht funktionieren.

Was ist mit dem lokalen Active Directory?

Der Notfallzugang für die Cloud und der Notfallzugang für die lokale Umgebung werden getrennt gehalten, ohne gegenseitige Abhängigkeit. Für Windows Server Active Directory arbeitest du beispielsweise mit Smartcards und einem eigenen Verfahren. Wer sich mit der Authentifizierung auf der lokalen Seite grundsätzlich beschäftigen will, findet den Einstieg im Kompetenzbereich [Microsoft Kerberos](#).

Der Alarm hat ausgelöst — und es war der Testlauf. Muss ich trotzdem dokumentieren?

Ja, und zwar genau so sorgfältig wie bei einem echten Vorfall. Erstens ist die Dokumentation der Nachweis, dass der Test stattgefunden hat. Zweitens gewöhnst du dein Team damit an den Ablauf, den es im Ernstfall braucht. Und drittens ist ein Protokoll, in dem ausschließlich Tests stehen, das beste Argument dafür, dass die Überwachung funktioniert.

Fazit

Break-Glass-Konten sind unspektakulär, billig und in einem halben Vormittag erledigt. Zwei reine Cloud-Konten auf der onmicrosoft.com-Domäne, dauerhaft aktive Rolle „Globaler Administrator“, FIDO2-Sicherheitsschlüssel in zwei getrennten Tresoren statt eines Passworts auf einem Zettel, Ausschluss aus jeder blockierenden Conditional-Access-Richtlinie, keine Lizenz. Das ist der ganze Aufbau.

Der Teil, der über Erfolg oder Misserfolg entscheidet, kommt danach. Ein Break-Glass-Konto ohne Alarm bei jeder Anmeldung ist keine Notausstiegstür, sondern eine unbewachte Hintertür mit Verwaltungsrechten. Und ein Konzept ohne halbjährlichen Testlauf und ohne gepflegte Dokumentation ist ein Papier, das im Ernstfall niemandem hilft — weil der Schlüssel ausgetauscht wurde, die Ausschlussgruppe beim letzten Umbau verlorenging oder die Alarmmail seit anderthalb Jahren an ein Postfach geht, das niemand mehr liest.

Wenn du nur eine Sache aus diesem Beitrag mitnimmst: Prüfe heute, ob dein Tenant zwei solche Konten hat, und melde dich damit an. Wenn innerhalb weniger Minuten dein Telefon klingelt, ist alles in Ordnung. Wenn nicht, weißt du, was als Nächstes zu tun ist.

Beim Aufbau, bei der Prüfung eines bestehenden Konzepts oder bei der Frage, wie sich das Ganze in eine belastbare Gesamtarchitektur einfügt, unterstützen wir dich im Rahmen der [Microsoft 365 Security Beratung](#). Wenn dein Team das Thema lieber selbst in die Hand nimmt, ist die [Schulung Microsoft 365 Security](#) der schnellere Weg dorthin.