

# Information Barriers in Microsoft Purview: Wenn sich Abteilungen nicht finden dürfen

Microsoft 365 ist auf Offenheit gebaut. Jeder findet jeden, die Personensuche kennt die ganze Belegschaft, und der People Picker schlägt beim Freigeben freundlich Kolleginnen und Kollegen aus dem ganzen Konzern vor. Für die meisten Unternehmen ist das genau richtig. Für manche ist es ein Problem.

Spätestens wenn ein Pentest bemängelt, dass die Personensuche Menschen aus Bereichen anzeigt, die den Suchenden nichts angehen, wird es ernst. Oder wenn die Aufsicht verlangt, dass Research und Handel nachweislich nicht miteinander reden. Dann landest du bei Information Barriers, der „chinesischen Mauer“ in Microsoft Purview.

Dieser Artikel erklärt, wie Information Barriers funktionieren, was sie in Teams, SharePoint und OneDrive tatsächlich bewirken, wo die Mauer Löcher hat und wann du besser zu einem anderen Werkzeug greifst. Er gehört zum [Kompetenzbereich Microsoft Purview](#).

## Was Information Barriers sind und was nicht

Information Barriers schotten Benutzergruppen innerhalb eines Tenants voneinander ab. Abgeschottete Benutzer können einander nicht finden, nicht chatten, nicht telefonieren und nicht gemeinsam an Inhalten arbeiten. Ursprünglich wurde die Funktion für die Finanzbranche entwickelt, wo regulatorisch vorgeschrieben ist, dass bestimmte Abteilungen keine Informationen austauschen dürfen.

Heute begegnet sie uns in der Beratung aus ganz anderen Gründen: Konzerne mit Tochtergesellschaften, die sich nicht gegenseitig im Verzeichnis sehen sollen, Pentest-Befunde zur Personensuche, Schulen und Hochschulen, in denen Lernende nicht jede Lehrkraft anschreiben sollen. Der gemeinsame Nenner ist immer derselbe: ein Tenant, mehrere Welten.

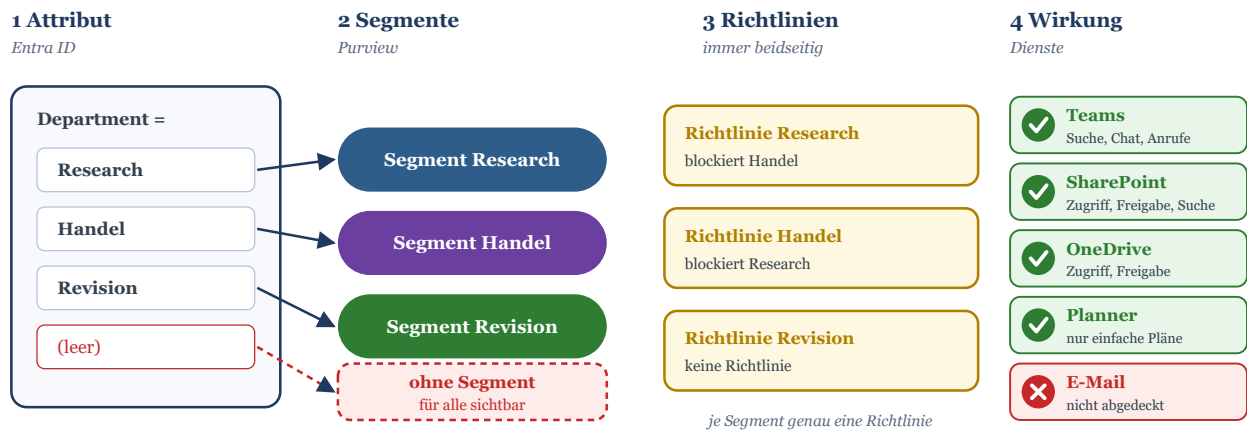
Ebenso wichtig ist, was Information Barriers nicht sind. Sie sind keine Berechtigungsverwaltung, kein Ersatz für saubere Freigaben und keine Lösung für Externe, die gar nicht erst im Verzeichnis stöbern sollen. Für Gäste gibt es in Entra ID ein eigenes, viel einfacheres Werkzeug, dazu später mehr.

### Fakten: Information Barriers im Steckbrief

- Wirken in Microsoft Teams, SharePoint, OneDrive und Planner (dort nur in einfachen Plänen).
- Wirken nicht in E-Mail: Exchange Online wird laut Microsoft nicht abgedeckt, dafür sind Mail-Flow-Regeln vorgesehen.
- Gelten immer nur innerhalb eines Tenants, tenantübergreifende Barrieren gibt es nicht.
- Lizenz: enthalten in Microsoft 365 E5, A5 und G5, in der Microsoft Purview Suite und im Insider-Risk-Management-Add-on, nicht aber im Add-on für Information Protection and Governance.

# Segmente und Richtlinien: So ist die Mauer gebaut

Information Barriers bestehen aus genau zwei Bausteinen, und beide sind schnell erklärt. Die Tücke steckt wie so oft im Detail.



Skizze 1: Vom Entra-Attribut über Segmente und Richtlinien zur Wirkung in den Diensten

## Segmente: Wer gehört wohin?

Ein Segment fasst Benutzer über einen Attributfilter zusammen, etwa alle mit Department gleich „Research“ oder alle Mitglieder einer bestimmten Gruppe. Damit steht und fällt die gesamte Lösung mit der Qualität deiner Entra-Attribute. Wenn die Personalabteilung Abteilungsnamen kreativ pflegt („Research“, „Research & Analytics“, „R&A“), hast du drei Segmente oder zwei Lücken. Segmente lassen sich nach dem Anlegen übrigens nicht mehr umbenennen.

## Richtlinien: Wer darf wen nicht sehen?

Eine Richtlinie hängt an genau einem Segment und legt fest, mit welchen anderen Segmenten es nicht kommunizieren darf (Block) oder ausschließlich kommunizieren darf (Allow). Microsoft empfiehlt für die meisten Szenarien Block-Richtlinien. Drei Regeln solltest du kennen, bevor du loslegst:

- Je Segment gibt es höchstens eine Richtlinie.
- Information Barriers unterstützen nur beidseitige Sperren. Soll Research den Handel nicht sehen, braucht es zwei Richtlinien: Research blockiert Handel und Handel blockiert Research.
- Der Typ einer Richtlinie (Block oder Allow) lässt sich nachträglich nicht ändern. Wer sich vertan hat, löscht und legt neu an.

## Organisationsmodus und Ausrollen

Ältere Tenants laufen teils noch im Legacy-Modus mit höchstens 250 Segmenten, einem Segment je Benutzer und Adressbuchrichtlinien als Unterbau. In den modernen Modi SingleSegment und MultiSegment sind bis zu 5.000 Segmente möglich, im MultiSegment-Modus darf ein Benutzer bis zu zehn Segmenten angehören. Welcher Modus gilt, verrät Get-PolicyConfig.

Richtlinien legst du inaktiv an, aktivierst sie und rollst sie dann aus. Vorher müssen das Audit-Log aktiv und die bereichsbezogene Verzeichnissuche in Teams eingeschaltet sein, und zwar mindestens 24 Stunden vor der ersten Richtlinie. Laut Microsoft vergehen nach dem Start rund 30 Minuten, danach werden etwa 5.000 Benutzer pro Stunde verarbeitet. Bei 20.000 Benutzern ist das also eher ein Nachmittag als eine Kaffeepause.

**Connect-IPPSession**

```
# Segmente anlegen
New-OrganizationSegment -Name 'Research' -UserGroupFilter "Department -eq 'Research'"
New-OrganizationSegment -Name 'Handel' -UserGroupFilter "Department -eq 'Handel'"

# je Segment eine Richtlinie, beidseitig, zunächst inaktiv
New-InformationBarrierPolicy -Name 'Research-Handel' -AssignedSegment 'Research' -SegmentsBlocked
'Handel' -State Inactive
New-InformationBarrierPolicy -Name 'Handel-Research' -AssignedSegment 'Handel' -SegmentsBlocked
'Research' -State Inactive

# aktivieren, ausrollen, Status prüfen
Get-InformationBarrierPolicy | ForEach-Object { Set-InformationBarrierPolicy -Identity $_.Identity -State
Active }
Start-InformationBarrierPoliciesApplication
Get-InformationBarrierPoliciesApplicationStatus
```

**Tipp: Die Gretchenfrage zuerst klären**

Bevor du das erste Segment anlegst: Gibt es Gruppen, die alle sehen müssen? Die IT, die Revision, die Geschäftsführung? In Skizze 1 ist das die Revision, die gar keine Richtlinie bekommt. Alternativ helfen Benutzer in mehreren Segmenten (nur im MultiSegment-Modus) oder eine Allow-Richtlinie. Wer das erst nach dem Ausrollen merkt, löscht Richtlinien und fängt von vorn an.

## Was die Barriere in Teams, SharePoint und OneDrive bewirkt

### Teams: die sichtbarste Wirkung

In Teams merkst du Information Barriers sofort. Blockierte Personen tauchen weder in der Suche noch im People Picker auf. Chats, Anrufe, Besprechungen und Bildschirmfreigaben zwischen blockierten Segmenten werden verhindert. Bei bestehenden Beziehungen greift die Barriere nachträglich: 1:1-Chats werden schreibgeschützt, unzulässige Mitglieder werden aus Gruppenchats und Teams entfernt.

### SharePoint und OneDrive: der Website-Modus entscheidet

In SharePoint und OneDrive steuern Information Barriers, wer einer Website hinzugefügt werden kann, wer auf Inhalte zugreift, wer sie freigeben darf und was in der Suche auftaucht. Wie streng das geschieht, legt der Modus der jeweiligen Website fest.



Teams-Websites werden innerhalb von 24 Stunden implizit; Websites von Benutzern mit Segment werden explizit.

Skizze 2: Die vier Website-Modi von offen bis streng

| Modus                     | Wer kommt hinein?                                                                                       | Wann gilt der Modus?                                                                                                                        |
|---------------------------|---------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Offen</b>              | Wer Berechtigungen hat; Freigabe nach der Richtlinie des Freigebenden                                   | Standard für Websites ohne Segment                                                                                                          |
| <b>Besitzer-moderiert</b> | Nur wen der Besitzer einlädt; Links für jeden und organisationsweite Links sind abgeschaltet            | Vom Administrator gesetzt, nur ohne Segmente möglich                                                                                        |
| <b>Implizit</b>           | Nur Mitglieder der verbundenen Microsoft-365-Gruppe                                                     | Teams-Websites, innerhalb von 24 Stunden automatisch                                                                                        |
| <b>Explizit</b>           | Nur wer ein passendes Segment und Berechtigungen hat; Benutzer ohne Segment erhalten eine Fehlermeldung | Sobald einer Website ein Segment zugeordnet wird, z. B. weil ein Benutzer mit Segment sie anlegt; bis zu 100 kompatible Segmente je Website |

Wichtig für die Planung: Information Barriers in Teams schützen die zugehörige SharePoint-Website nicht automatisch. SharePoint und OneDrive werden separat aktiviert, und das dauert nach Microsoft-Angaben rund eine Stunde, bis es wirkt.

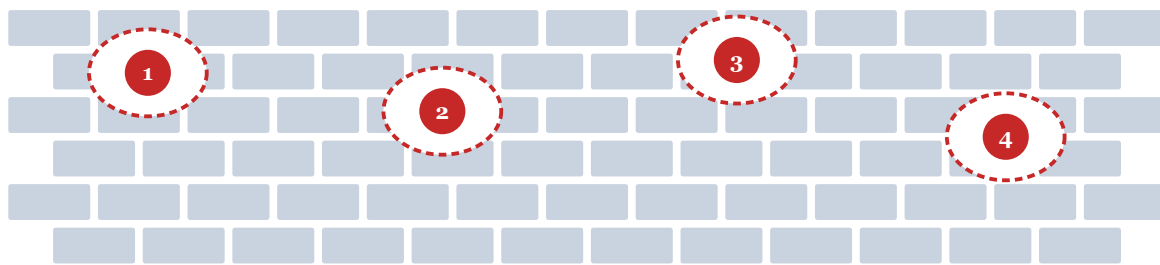
#### Fakten: Was nicht abgedeckt ist

- E-Mail: Wer Segmente auch im Postfach trennen will, braucht Mail-Flow-Regeln in Exchange Online.
- Verteilerlisten und Sicherheitsgruppen gelten als Nicht-IB-Gruppen, unterstützt werden nur Microsoft-365-Gruppen.
- Planner nur in einfachen Plänen, also Planner im Web und Planner in Teams.
- Federierte Benutzer aus anderen Organisationen unterliegen keinen Richtlinien.

## Die Löcher in der Mauer

Information Barriers sind ein ordentliches Werkzeug. Eine Mauer ist aber nur so dicht wie ihre schwächste Stelle, und vier Stellen sind in der Praxis immer wieder undicht.

### Die Barriere



**1 Benutzer ohne Segment**  
für alle sichtbar

**2 Alte Teams im Modus „Offen“**  
Richtlinien greifen nicht

**3 Suchtreffer aus Bestandszugriff**  
Titel und Vorschau rutschen durch

**4 E-Mail**  
von Barriers nicht erfasst

Skizze 3: Vier typische Lücken in einer Information-Barriers-Einführung

**Erstens: Benutzer ohne Segment.** In den modernen Modi gelten sie als Nicht-IB-Benutzer und sind für alle sichtbar. Jedes Konto mit leerem Department-Feld ist also ein Loch. Ein Bericht über Konten ohne Segmentattribut gehört deshalb in den Regelbetrieb, nicht nur in die Einführung.

**Zweitens: alte Teams.** Teams, die vor der Aktivierung angelegt wurden, laufen im Modus „Offen“, in dem keine Richtlinie greift. Sie müssen aktiv umgestellt werden, etwa mit Set-UnifiedGroup - InformationBarrierMode Implicit.

**Drittens: Suchtreffer aus Bestandszugriff.** Wer vor der Aktivierung Zugriff auf eine implizite oder besitzer-moderierte Website hatte, sieht deren Inhalte laut Microsoft weiterhin in der Suche. Erst beim Öffnen kommt die Ablehnung. Titel und Vorschauen können also durchrutschen.

**Viertens: E-Mail.** Die Barriere endet am Postfach. Wer das vergisst, hat eine Mauer mit offenem Tor.

#### Achtung: Migrationswerkzeuge und Sicherungen

Apps mit App-only-Zugriff, etwa Migrations- oder Backup-Werkzeuge, können an Websites mit Barriere scheitern. Microsoft sieht dafür die Ausnahme AppBypassInformationBarriers vor. Wer gleichzeitig nach SharePoint Online migriert und Information Barriers einführt, sollte das vor dem ersten Migrationslauf testen, nicht danach.

#### KI-Blick: Copilot sieht, was die Suche sieht

Microsoft 365 Copilot arbeitet auf denselben Berechtigungen wie die Suche. Die dritte Lücke betrifft deshalb auch Copilot: Inhalte aus impliziten oder besitzer-moderierten Websites, auf die jemand vor der Aktivierung Zugriff hatte, können laut Microsoft weiterhin in Copilot-Ergebnissen auftauchen, bis der Zugriff beim Öffnen scheitert. Wer Information Barriers als Teil einer Copilot-Einführung plant, sollte Bestandsberechtigungen vorher bereinigen. Mehr dazu im [Kompetenzbereich Copilot](#).

## Gäste, mehrere Tenants und Multi-Geo: wann Information Barriers passen

In Beratungsgesprächen höre ich oft die Frage, ob Information Barriers „das Problem mit der Personensuche“ lösen. Die ehrliche Antwort lautet: kommt darauf an, wer da sucht. Steht der Suchende als Gast, als synchronisiertes Mitglied oder als ganz normaler Benutzer im Verzeichnis? Daraus folgt, welches Werkzeug greift.

| Szenario                                                | Bestes Werkzeug                                                                            | Rolle der Information Barriers                          |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------|---------------------------------------------------------|
| Externe als Gäste im Tenant                             | Restriktive Gaststufe in Entra ID: Gäste sehen nur ihr eigenes Profil                      | <b>Ergänzung für einzelne Gastgruppen</b>               |
| Externe per Teams-Chat oder freigegebenem Kanal         | Positivlisten im externen Zugriff und in den mandantenübergreifenden Zugriffseinstellungen | <b>keine</b>                                            |
| Mehrere Tenants, Benutzer als Mitglieder synchronisiert | Scope und Attribute der Cross-Tenant-Synchronisierung                                      | <b>wertvoll über ein abgebildetes Herkunftsattribut</b> |
| Ein Tenant mit Multi-Geo                                | Information Barriers                                                                       | <b>einzigster echter Hebel</b>                          |
| Ein Tenant, interne Bereiche trennen                    | Information Barriers                                                                       | <b>Kernanwendung</b>                                    |

### Gäste

Für Gäste ist die Gaststufe in Entra ID das Mittel der Wahl. In der restriktiven Stufe sieht ein Gast nur sein eigenes Profil und kann andere Benutzer nicht einmal über deren Anmeldenamen abrufen, ganz ohne Zusatzlizenz. Information Barriers gelten in Teams zwar auch für Gäste, laut Teams-Dokumentation müssen diese dafür aber im Adressbuch auffindbar sein. Das ist ein Zielkonflikt, den du im Pilot klären solltest.

### Mehrere Tenants

Information Barriers wirken nur innerhalb eines Tenants. Eine Mauer über Tenant-Grenzen hinweg gibt es nicht. Spannend wird es bei der Cross-Tenant-Synchronisierung: Dort kommen Benutzer standardmäßig als Mitglieder im Ziel-Tenant an und sind damit normale Benutzer, die sich segmentieren lassen. Bildest du ein Herkunftsattribut wie companyName mit ab, kannst du im Ziel-Tenant gezielt Segmente bilden. Die Partner arbeiten nahtlos mit, finden bestimmte Bereiche aber nicht.

### Multi-Geo

Multi-Geo trennt Speicherorte, nicht Sichtbarkeit. Verzeichnis und Profile werden in jedes Geo repliziert, der People Picker zeigt alle Benutzer unabhängig vom Geo. Wer hier trennen will, kommt an Information Barriers nicht vorbei. Eine Besonderheit: Die SharePoint-Aktivierung muss laut Microsoft für jedes Geo einzeln erfolgen. Ein vergessenes Geo ist eine Lücke.

### Aus der Praxis: Der Pentest und die Personensuche

Ein typisches Szenario aus der Beratung: Ein Pentest bemängelt, dass die Personensuche Menschen aus Bereichen zeigt, die den Suchenden nichts angehen. On-premises war ein eigener Security Trimmer geplant, den es in SharePoint Online nicht gibt. Der erste Reflex lautet „Information Barriers“. Die erste Frage muss aber lauten: Wer sucht da eigentlich? Sind es Gäste, ist die Gaststufe in einer Viertelstunde umgestellt. Sind es interne Bereiche oder synchronisierte Gesellschaften, sind Information Barriers richtig, aber dann bitte mit sauberen Attributen, einer Prüfmatrix und einem Pilot. Den Nachweis für den Nachtest liefert die im Pilot ausgefüllte Prüfmatrix.

## Einführung, Betrieb und Monitoring

Information Barriers sind keine Einstellung, die man am Freitagnachmittag umlegt und dann vergisst. Die Einführung ist überschaubar, die eigentliche Arbeit beginnt danach: Menschen wechseln die Abteilung, neue Teams entstehen, Richtlinien ändern sich. Eine Mauer, um die sich niemand kümmert, bekommt Risse.

### Einführung in sieben Schritten

So gehe ich in Projekten vor:

1. **Segmentmodell fachlich festlegen:** Wer darf wen nicht sehen, in welche Richtung, und wer muss alle sehen?
2. **Attribute bereinigen:** Segmentmerkmal wählen, für alle Konten pflegen, Konten ohne Wert per Bericht aufdecken.
3. **Voraussetzungen schaffen:** Lizenz prüfen, Audit-Log aktivieren, bereichsbezogene Verzeichnissuche in Teams einschalten und 24 Stunden warten.
4. **Segmente und Richtlinien anlegen:** inaktiv, beidseitig, je Segment genau eine Richtlinie.
5. **Pilot:** mit Testbenutzern aus mindestens zwei Segmenten und einer Prüfmatrix für Teams, People Picker, Personensuche und SharePoint-Zugriff.
6. **Ausrollen:** Richtlinien aktivieren, anwenden, Status prüfen, SharePoint und OneDrive aktivieren (bei Multi-Geo je Geo), bestehende Teams auf „Implizit“ umstellen.
7. **Betrieb übergeben:** Prüfroutinen, Zuständigkeiten und Änderungsablauf festlegen, wie in den folgenden Abschnitten beschrieben.

### Betrieb: was die Mauer im Alltag verändert

Im Alltag merkst du Information Barriers vor allem dann, wenn sich etwas bewegt. Wechselt eine Person die Abteilung, ändert sich ihr Attribut und damit ihr Segment. Teams prüft bestehende Beziehungen laut Microsoft bei Profiländerungen neu: Die Person verschwindet dann aus Teams und Gruppenchats, die ihr neues Segment nicht mehr erlaubt, und alte 1:1-Chats werden schreibgeschützt. Technisch ist das korrekt. Für den Helpdesk ist es der Klassiker „Warum bin ich plötzlich aus meinem Team geflogen?“. Sag es dem Helpdesk vorher, dann wird aus dem Rätsel eine Standardantwort.

Ein zweiter Dauerbrenner sind neue Konten. Die Personalabteilung legt einen Neuzugang an, das Feld Department bleibt leer, und schon steht ein Benutzer ohne Segment im Tenant, für alle sichtbar und

alle sehend. Deshalb gehört das Segmentattribut in den Eintrittsprozess als Pflichtfeld, nicht in die Rubrik „pflegen wir später“.

## Monitoring: was du regelmäßig prüfen solltest

Microsoft liefert kein fertiges Dashboard für Information Barriers. Mit einer Handvoll PowerShell-Abfragen kommst du aber erstaunlich weit. Diese Prüfungen haben sich bewährt:

| Prüfung                                               | Werkzeug                                                | Rhythmus                       |
|-------------------------------------------------------|---------------------------------------------------------|--------------------------------|
| <b>Konten ohne Segmentattribut</b>                    | Get-MgUser mit Filter auf leeres Attribut (siehe unten) | wöchentlich                    |
| <b>Status der letzten Richtlinienanwendung</b>        | Get-InformationBarrierPoliciesApplicationStatus - All   | nach jeder Änderung            |
| <b>Teams, die noch im Modus „Offen“ laufen</b>        | Get-UnifiedGroup mit Filter auf InformationBarrierMode  | monatlich                      |
| <b>Websites mit unzulässigen Segmentkombinationen</b> | SharePoint-Compliance-Bericht für Information Barriers  | nach jeder Richtlinienänderung |
| <b>Segment eines einzelnen Benutzers</b>              | Get-Recipient mit den Segment-Eigenschaften             | bei Rückfragen                 |
| <b>Beziehung zwischen zwei Benutzern</b>              | Get-ExoInformationBarrierRelationship                   | bei Rückfragen                 |
| <b>Wirkung aus Sicht der Benutzer</b>                 | Prüfmatrix mit Testbenutzern aus dem Pilot              | halbjährlich                   |

```
# Konten ohne Segmentattribut (hier: Department)
Connect-MgGraph -Scopes User.Read.All
Get-MgUser -All -Property DisplayName,UserPrincipalName,Department,AccountEnabled |
    Where-Object { $_.AccountEnabled -and [string]::IsNullOrEmpty($_.Department) } |
    Select-Object DisplayName, UserPrincipalName

# Teams, für die noch keine Richtlinie greift (Exchange Online PowerShell)
Get-UnifiedGroup -ResultSize Unlimited |
    Where-Object { $_.InformationBarrierMode -eq 'Open' } | Select-Object DisplayName,
InformationBarrierMode

# Segment eines Benutzers und Beziehung zweier Benutzer
Get-Recipient -Identity anna.berg | Format-List Name,*segment*
Get-ExoInformationBarrierRelationship -RecipientId1 anna.berg -RecipientId2 jan.wolf

# SharePoint: Compliance-Bericht nach Richtlinienänderungen
Start-SPOInformationBarriersPolicyComplianceReport
Get-SPOInformationBarriersPolicyComplianceReport
$report = Get-SPOInformationBarriersPolicyComplianceReport -ReportId <ID>
$report.Content # u. a. IncompatibleSegmentsPairs und InvalidIBSegments
```

Der SharePoint-Bericht verdient einen zweiten Blick. Er zeigt Websites, deren zugeordnete Segmente nach einer Richtlinienänderung nicht mehr zusammenpassen, etwa wenn Research und Handel plötzlich gemeinsam auf einer Website hängen, oder Segmente, die es gar nicht mehr gibt. Mit dem Schalter -UpdateOneDriveSegments bringt der Bericht unzulässige OneDrive-Konten gleich selbst in Ordnung. Auf großen Tenants kann der Lauf allerdings lange dauern, also besser abends starten.

## Änderungen sicher durchführen

Für Änderungen an Segmenten und Richtlinien gilt eine einfache Regel: ändern, erneut anwenden, prüfen. Microsoft weist ausdrücklich darauf hin, dass Richtlinien nach dem Bearbeiten von Segmenten oder Richtlinien neu angewendet werden müssen. Bei großen Organisationen kann das 24 Stunden oder länger dauern.

- **Segment anpassen:** Set-OrganizationSegment mit neuem Filter, danach Start-InformationBarrierPoliciesApplication.
- **Richtlinie anpassen:** Nur die zugeordneten Segmente lassen sich ändern. Für einen anderen Typ die alte Richtlinie inaktiv setzen und eine neue anlegen.
- **Richtlinie entfernen:** erst inaktiv setzen, dann anwenden, erst danach mit Remove-InformationBarrierPolicy löschen.
- **Anwendung abbrechen:** Stop-InformationBarrierPoliciesApplication hält einen laufenden Durchlauf an, macht aber bereits angewendete Richtlinien nicht rückgängig.

Für die Nachvollziehbarkeit lohnt der Blick ins [Purview-Audit-Log](#). Wenn du die Einführung nicht allein stemmen willst: In der [Purview-Beratung](#) gehört das Segmentmodell zur Standortbestimmung, und in den [Purview-Schulungen](#) spielen wir Information Barriers im eigenen Tenant durch.

## Häufige Fragen zu Information Barriers

### Brauche ich für Information Barriers eine E5-Lizenz?

Information Barriers sind laut Microsoft in Microsoft 365 E5, A5 und G5 enthalten, außerdem in der Microsoft Purview Suite und im Insider-Risk-Management-Add-on. Im Add-on für Information Protection and Governance sind sie nicht enthalten. Wie viele Benutzer lizenziert sein müssen, klärst du am besten mit deinem Lizenzpartner.

### Blockieren Information Barriers auch E-Mails?

Nein. Microsoft stellt klar, dass Information Barriers die Kommunikation per Exchange Online nicht beschränken. Für E-Mail sind Mail-Flow-Regeln das passende Werkzeug, etwa eine Regel, die Nachrichten zwischen zwei Gruppen ablehnt.

### Kann ich festlegen, dass A den Bereich B nicht sieht, B aber A schon?

Nein. Information Barriers unterstützen nur beidseitige Sperren. Du legst zwar je Segment eine eigene Richtlinie an, die Wirkung muss aber in beide Richtungen gleich sein.

### Was passiert mit Benutzern, die keinem Segment angehören?

In den modernen Organisationsmodi sind sie für alle sichtbar. Das ist praktisch für zentrale Funktionen, aber gefährlich, wenn ein Segmentattribut einfach nur vergessen wurde. Ein regelmäßiger Bericht über Konten ohne Segment gehört deshalb zum Betrieb.

### Wirken Information Barriers auch über mehrere Tenants hinweg?

Nein, Segmente gelten immer nur innerhalb eines Tenants. Synchronisierte Mitglieder aus anderen Tenants lassen sich im Ziel-Tenant aber segmentieren, wenn die Synchronisierung ein passendes Attribut mitbringt.

## Wie lange dauert es, bis Richtlinien wirken?

Nach dem Start vergehen laut Microsoft rund 30 Minuten, danach werden etwa 5.000 Benutzer pro Stunde verarbeitet. Die Aktivierung in SharePoint braucht rund eine Stunde, die Umstellung von Teams-Websites auf den impliziten Modus bis zu 24 Stunden.

## Kann ich Information Barriers wieder abschalten?

Ja. Richtlinien lassen sich auf inaktiv setzen und erneut anwenden, SharePoint und OneDrive lassen sich mit `Set-SPOTenant -InformationBarriersSuspension $true` aussetzen. Was die Barriere zwischenzeitlich verändert hat, etwa aus Teams entfernte Mitglieder, solltest du danach gezielt prüfen.

### Weiter im Kompetenzbereich Microsoft Purview

- [Überblick Microsoft Purview](#)
- [Purview-Audit-Log](#)
- [Beratung Microsoft Purview](#)
- [Schulungen Microsoft Purview](#)