Zero Trust und Identity – Warum Hoffnung keine Strategie ist

Klaus Bierschenk

Director Consulting Expert – CGI Deutschland

- Identity-Enthusiast seit über 20 Jahren
- Wohnhaft in Murnau am Staffelsee (Garmisch-Partenkirchen)
- Zusammen mit meiner Familie, zwei Schlangen und zwei Katzen
- Mit den Bergen vor der Haustür verbringe ich dort viel Zeit

http://www.linkedin.com/in/klabier

Klaus.bierschenk@cgi.com

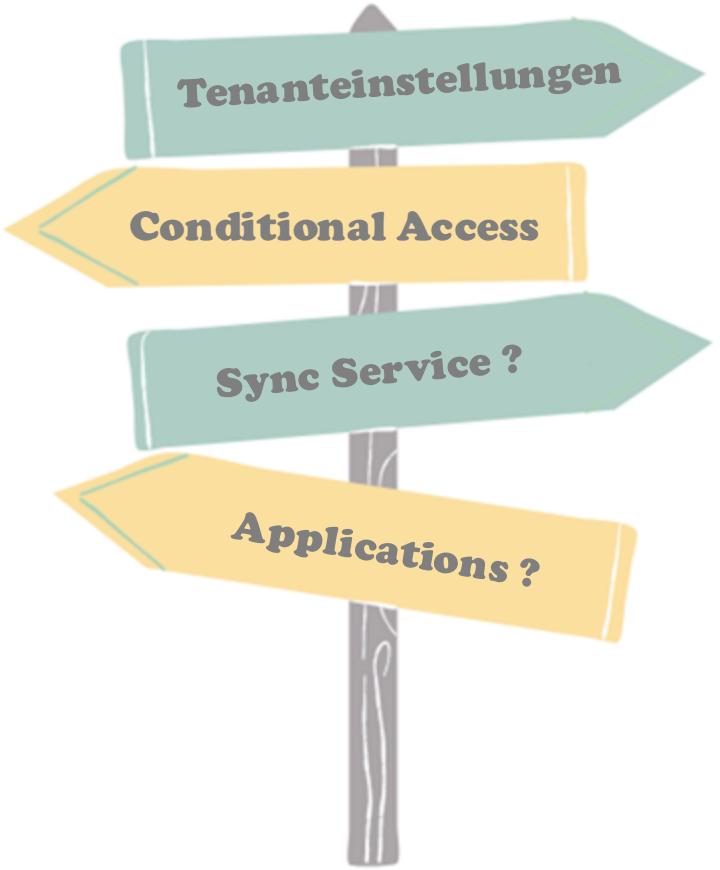
https://bsky.app/profile/klabier.bsky.social

https://nothingbutcloud.net/

Zero Trust und Identity – Warum Hoffnung keine Strategie ist

- Was ist die Herausforderung?
- „PIMp my Administration“
- Strategien für den Notfall
- Endbenutzer-Authentifizierung

- *Ask-Me-Anything am Stand E0 der heise academy - 12:00 Uhr*



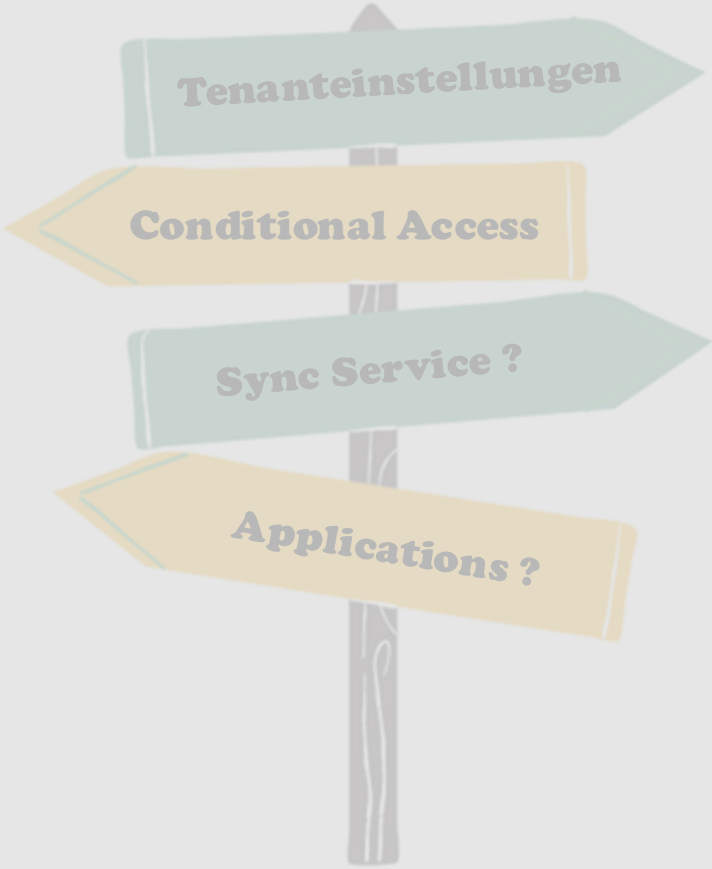
Zero Trust und Identity – Warum Hoffnung keine Strategie ist

Gartner prognostiziert, dass bis 2025 über 99% der Cloud-Sicherheitsverletzungen auf vermeidbare Fehlkonfigurationen oder Fehler von Endbenutzern zurückzuführen sein werden.

https://venturebeat.com/business/takeaways-fromgartners-2021-hype-cycle-for-cloud-security-report

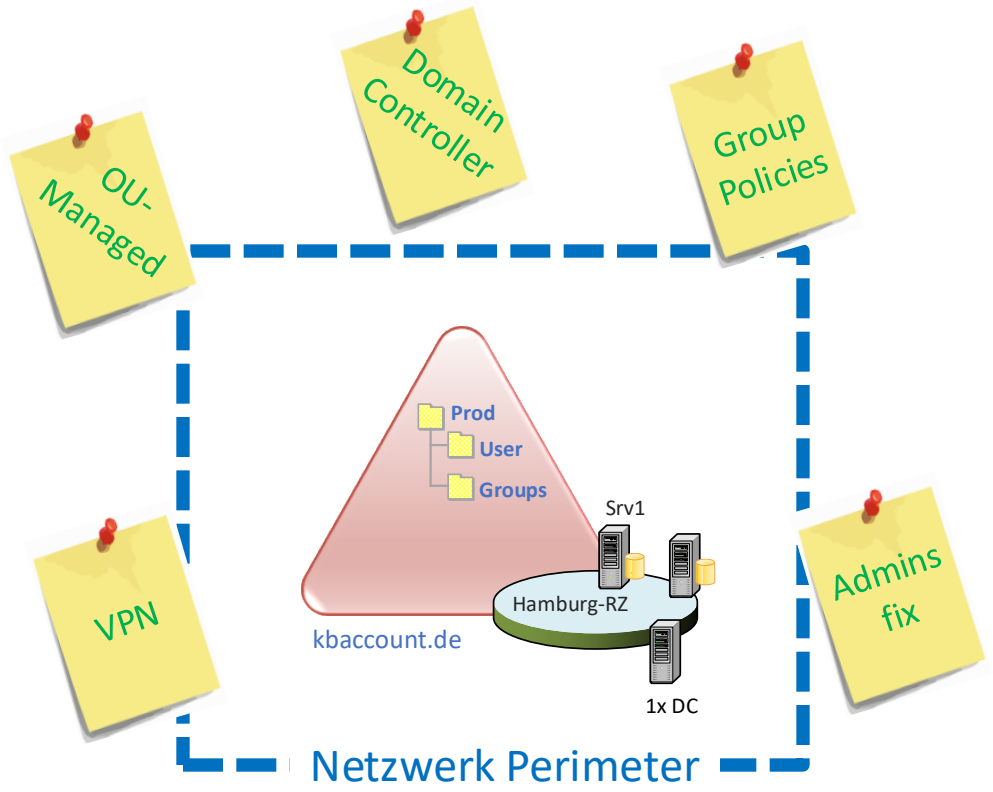
Zero Trust und Identity – Warum Hoffnung keine Strategie ist

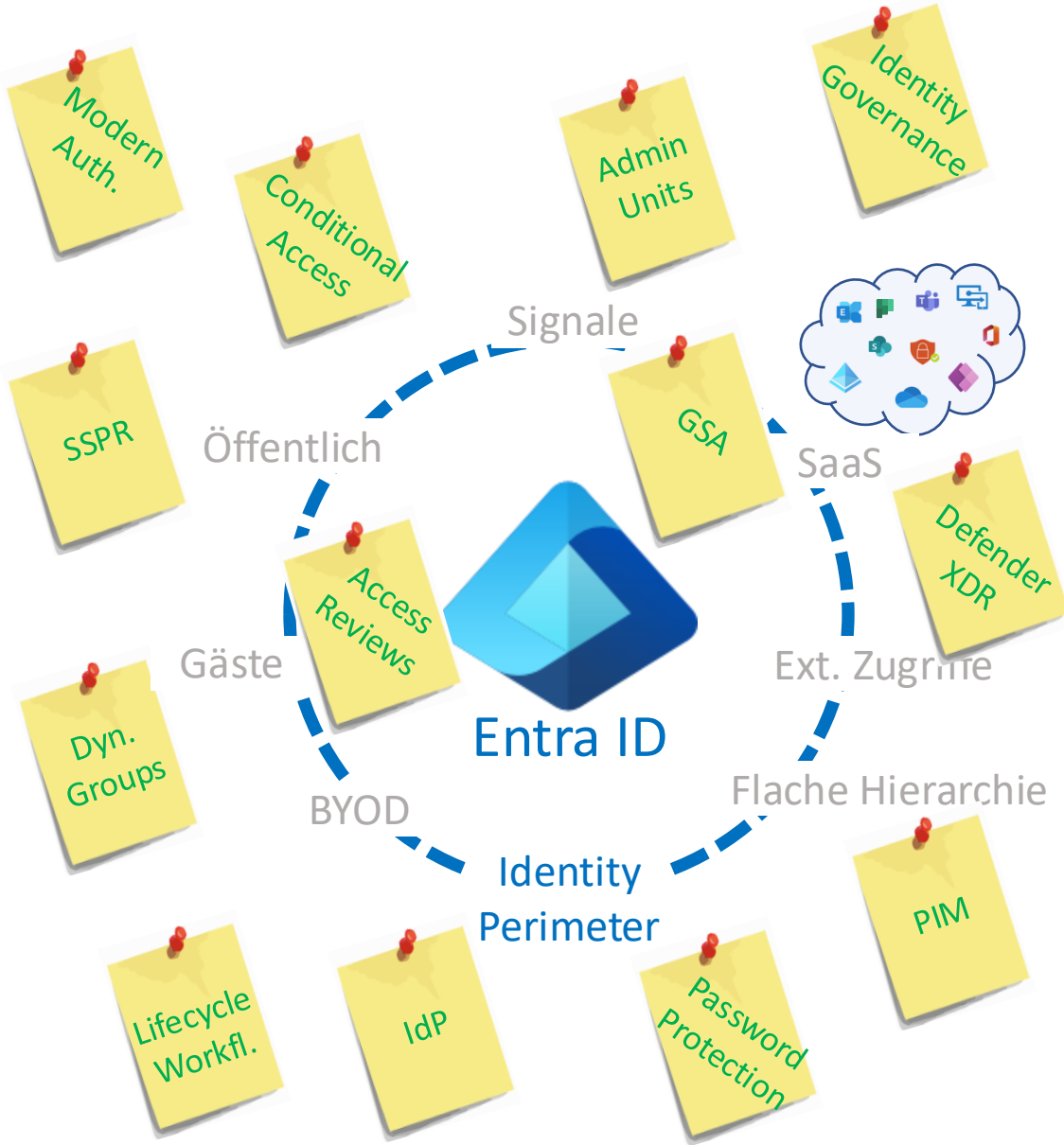
- Was ist die Herausforderung?
- „PIMp my Administration“
- Strategien für den Notfall
- Endbenutzer-Authentifizierung



Zero Trust und Identity – Warum Hoffnung keine Strategie ist

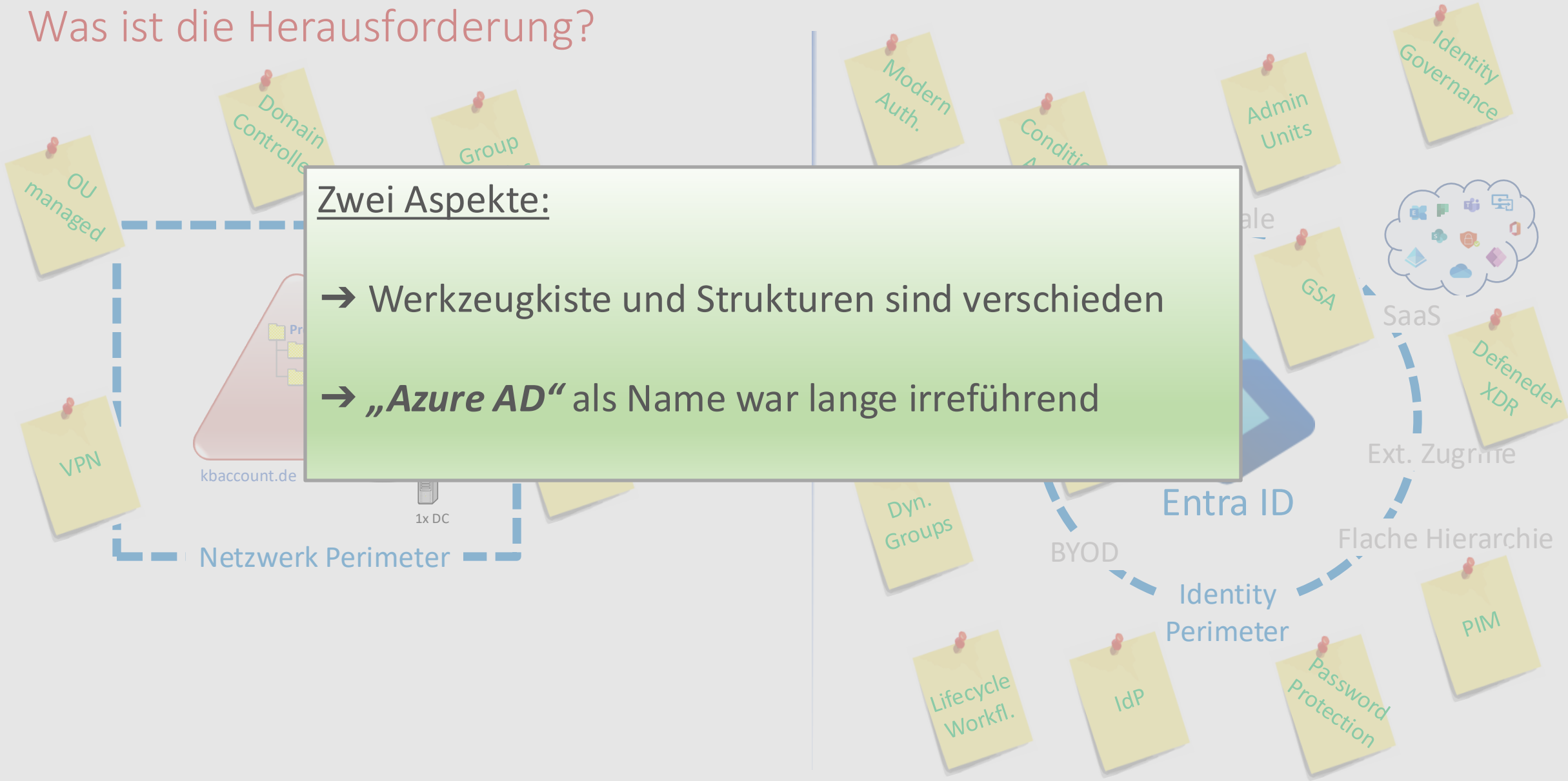
Was ist die Herausforderung?





Zero Trust und Identity – Warum Hoffnung keine Strategie ist

Was ist die Herausforderung?



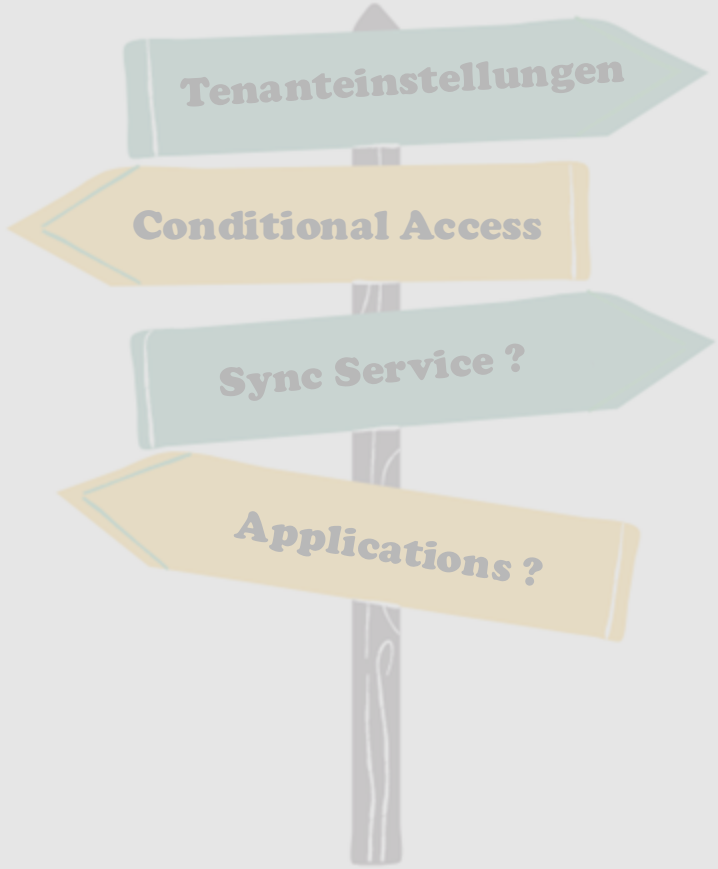
Zwei Aspekte:

➔ Werkzeugkiste und Strukturen sind verschieden

➔ ***„Azure AD“*** als Name war lange irreführend

Zero Trust und Identity – Warum Hoffnung keine Strategie ist

- Was ist die Herausforderung?
- „PIMp my Administration“
- Strategien für den Notfall
- Endbenutzer-Authentifizierung



Zero Trust und Identity – Warum Hoffnung keine Strategie ist

Privileged Identity Management (PIM)

Administration heute:
Nicht mehr als erforderlich (Just-Enough-Access)

… und auch nicht länger als nötig (Just-in-Time)

Zero Trust und Identity – Warum Hoffnung keine Strategie ist

Rollenmanagement in der Microsoft Cloud

Administrative Rollen

- ✓ Azure / Entra Rollen getrennt
- ✓ Vorrausschauende Planung
- ✓ Zuweisung entweder „active“ oder „eligible“
- ✓ Bedarfsgerechte Zuweisung (JIT/JEA) mit PIM

Azure Admin Roles (619)

	Azure Role
1	Azure Role
2	AcrPush
3	API Management Service Contributor
4	AcrPull
5	AcrImageSigner
6	AcrDelete
7	AcrQuarantineReader
8	AcrQuarantineWriter
9	API Management Service Operator Role
10	API Management Service Reader Role
11	Application Insights Component Contributor
12	Application Insights Snapshot Debugger
13	Attestation Reader
14	Automation Job Operator
15	Automation Runbook Operator
16	Automation Operator
17	Avere Contributor
18	Avere Operator
19	Azure Kubernetes Service Cluster Admin Role

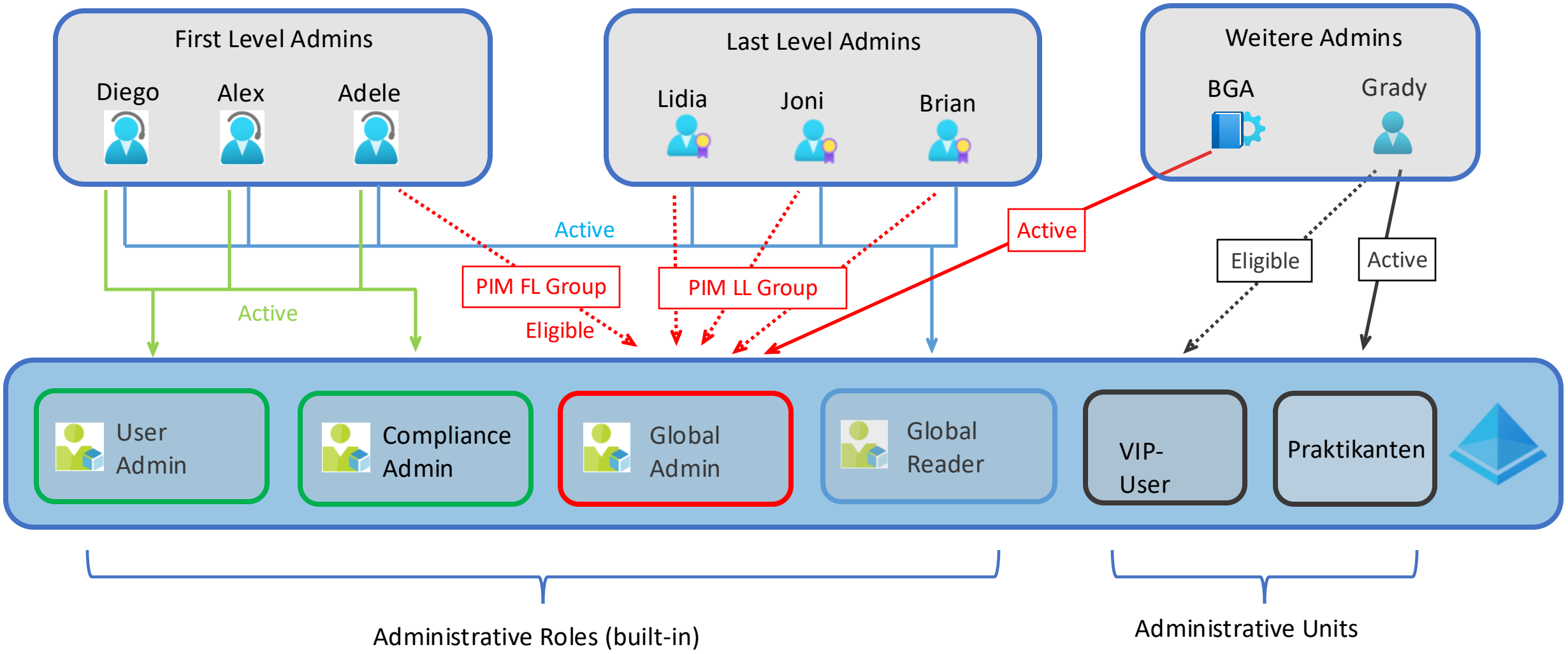
Entra Admin Roles (117)

Entra Role
Global Administrator
Guest User
Restricted Guest User
Guest Inviter
User Administrator
Helpdesk Administrator
Service Support Administrator
Billing Administrator
User
Partner Tier1 Support
Partner Tier2 Support
Directory Readers
Directory Writers
Exchange Administrator
SharePoint Administrator
Skype for Business Administrator
Device Users
Azure AD Joined Device Local Administrator

Cmdlets im Anhang

Zero Trust und Identity – Warum Hoffnung keine Strategie ist

PIM-Praxisszenarien



Zero Trust und Identity – Warum Hoffnung keine Strategie ist

Wichtige Fakten zu PIM …

- Separates Setup für jede Admin-Rolle
- Leistungsstark: PIM-for-Groups
- Analyse kritischer Rollen
- „MFA“ oder „Protected-Action“ bei Rollenaktivierung
- P2 Lizenz erforderlich für Role-Member, Approver, PIM-Admin
- Integration in Access Reviews (Link)
- Rolle aktivieren über PIM-Dashboard, PS, MS Graph API

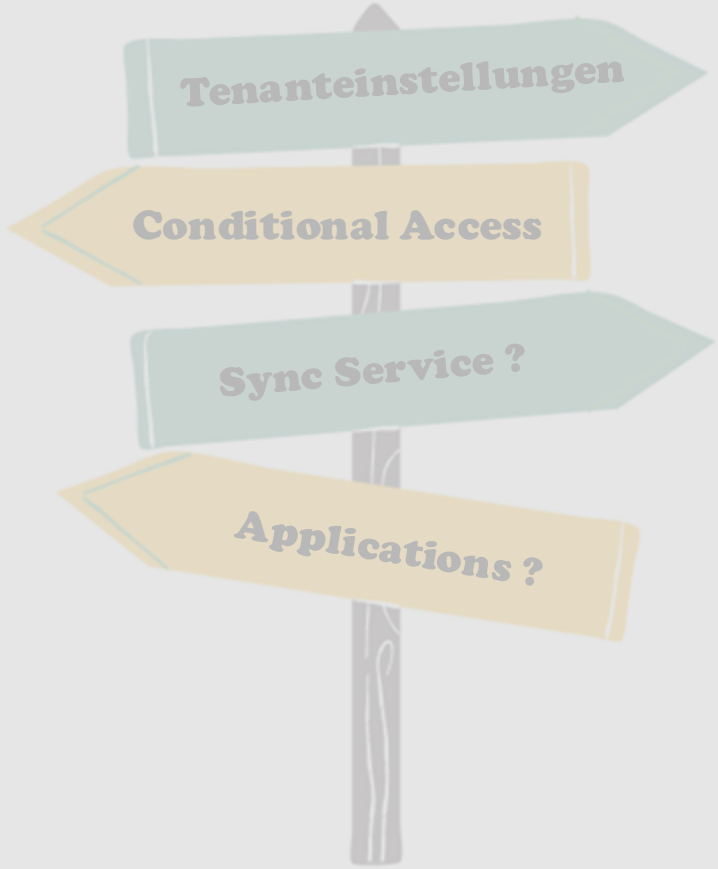
Zero Trust und Identity – Warum Hoffnung keine Strategie ist

It is time for a demo …

Privileged Identity Management:
PIM Groups und Einstellungen

Zero Trust und Identity – Warum Hoffnung keine Strategie ist

- Was ist die Herausforderung?
- „PIMp my Administration“
- **Strategien für den Notfall**
- Endbenutzer-Authentifizierung



Zero Trust und Identity – Warum Hoffnung keine Strategie ist

Strategien für den Notfall:

- Aussperren aus dem Tenant ist möglich und übles Szenario
- Wichtig bei PTA wegen notwendiger Verbindung zu On-Prem AD
- Mögliche Gründe für einen „Notfall“:

➔ Gelöschte Admin-Konten

➔ Fehlerhafte Konfigurationen

➔ Policies zu restriktiv (Conditional Access)

➔ Keine Verbindung zu On-Premises mehr

Zero Trust und Identity – Warum Hoffnung keine Strategie ist

Design und Implementierung

Keine synchronisierten Benutzerkonten

„Cloud Only“-User erstellen (nicht personalisiert)

Analyse des Risikos notwendig, denn …

BGA-Konten haben maximale Berechtigungen (GA)

BGA-Konten bei Exclude einsetzen (Policies)

Aufbewahrung des Passwortes? Geteiltes Passwort?

Wirklich eine dedizierte Gruppe für diese Konten?

Administrative Aspekte (BHB)

Notfallprozess dokumentieren

Regelmäßige Tests planen. OpsGuide (BHB)

BGA-Aktivitäten überwachen (Warnregeln)

Funktioniert Anmeldung? Rechte ok? Alerts ok?

Prüfen, ob „Excludes“ bei den Richtlinien passen

Regelmäßig Warnungsregel prüfen

Neues Passwort bei MA-Wechsel im Admin-Team

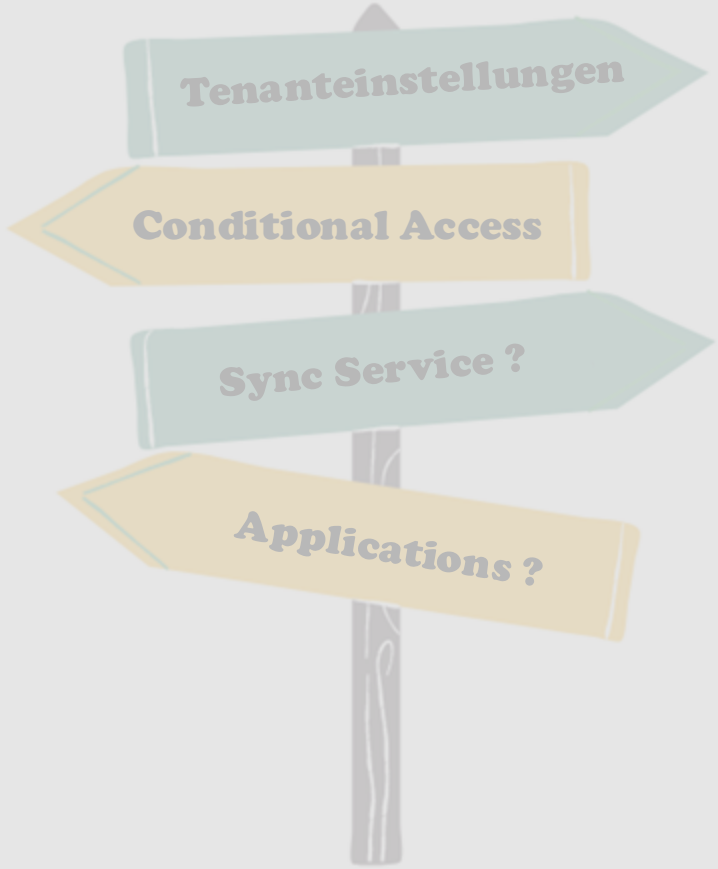
Zero Trust und Identity – Warum Hoffnung keine Strategie ist

It‘s time for a demo …

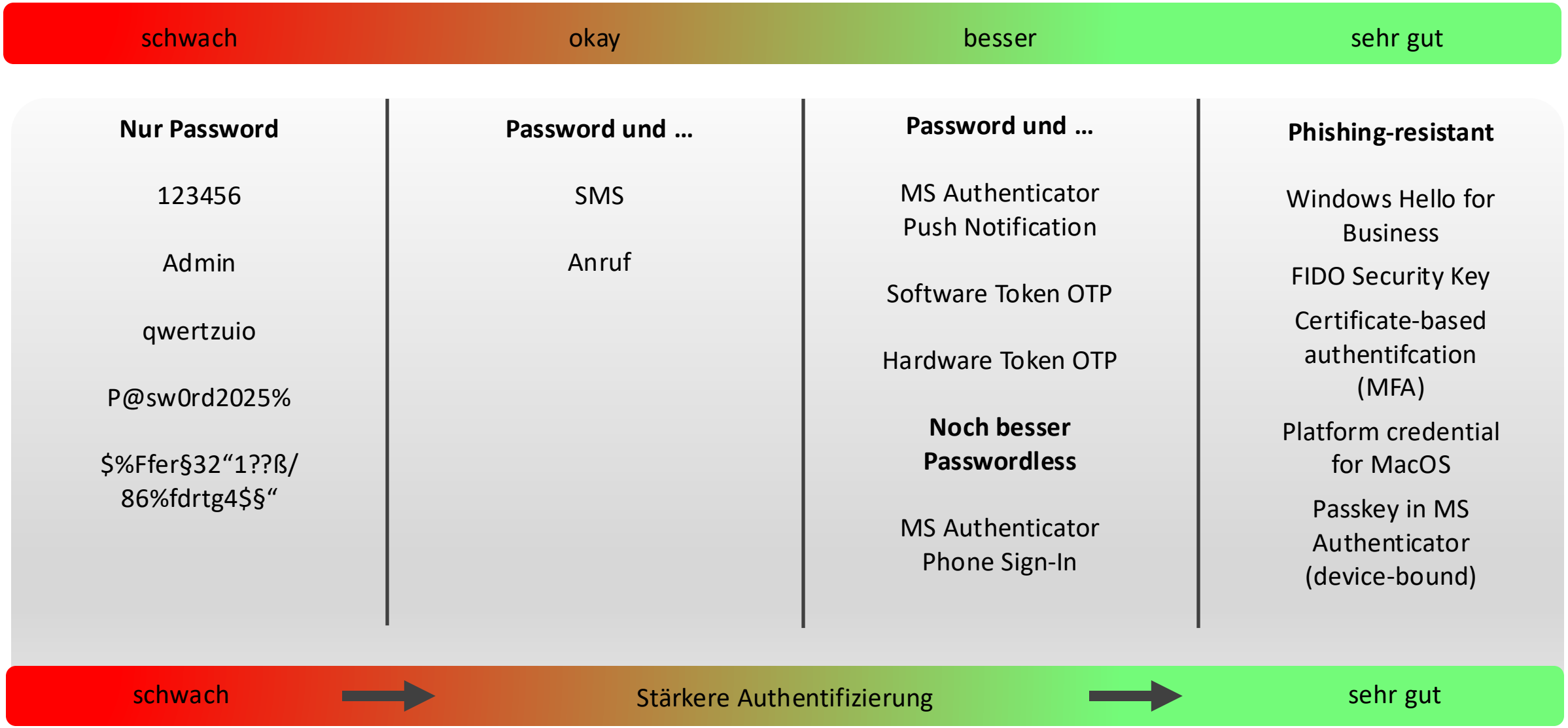
`BGA-Warnungen handgemacht`

Zero Trust und Identity – Warum Hoffnung keine Strategie ist

- Was ist die Herausforderung?
- „PIMp my Administration“
- Strategien für den Notfall
- Endbenutzer-Authentifizierung



Zero Trust und Identity – Warum Hoffnung keine Strategie ist



Zero Trust und Identity – Warum Hoffnung keine Strategie ist

Letzte und gute Änderungen im Bereich Authentifizierung …

Februar 2025 (Public Preview)
QR based authentication TechCommunity Beitrag

Februar 2025 (General available)
Authentication methods migration wizard (Was, wo?)

Dezember 2024 (Public Preview)
Temporary Access Pass (TAP) support for internal guest users

Dezember 2024 - Ignite (Public Preview)
Security Copilot embedded in Microsoft Entra

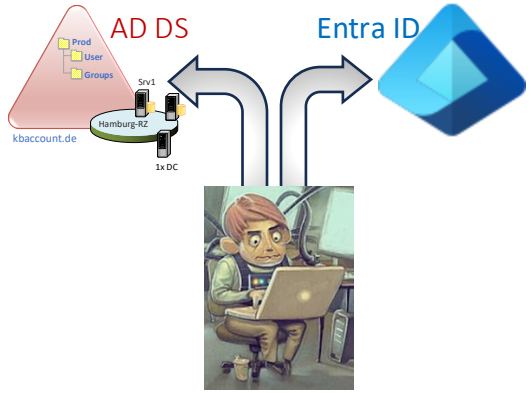
April 2024 (Public Preview)
Enable passkeys in Authenticator

Zero Trust und Identity – Warum Hoffnung keine Strategie ist

Zusammenfassung - Was haben wir gelernt?

➔ Nichts dem Zufall überlassen.
Hoffnung und Zero Trust passen nicht zusammen

➔ Active Directory Domain Services (AD DS) ist eine über Jahrzehnte ausgereifte und leistungsstarke Technologie aber verwalten Sie Ihr Entra ID nicht wie das lokale AD - <u>Entra ID ist kein AD</u>



➔ Bleiben Sie auf dem Laufenden! Informieren Sie sich regelmäßig über Neuigkeiten und Änderungen in Entra ID (siehe Folie mit Links)

Zero Trust und Identity – Warum Hoffnung keine Strategie ist

Weiterführende Informationen

Ergänzendes Material:

Create an access review of PIM for Groups in Microsoft Entra ID (preview)

Kontrovers diskutiert: Warum der Namenswechsel von Azure AD zu Entra ID problematisch ist

Aktivieren von Passkeys in Authenticator

Gute Quellen für Neuigkeiten rund um Entra ID:

Merill Fernando Entra News

Microsoft Entra-Versionen und Ankündigungen

Heise Academy - Neuerungen in Entra ID - Serie

secIT by heise

HANNOVER 2025

heise academy

ASK ME ANTHING
19. März – 12 Uhr

Zero Trust und Identity – Warum Hoffnung keine Strategie ist

Backup / Anhang

Zero Trust und Identity – Warum Hoffnung keine Strategie ist

Excelfile mit allen Adminrollen erstellen

Cmdlets und
Infos in meinem
Github Repository:

https://github.com/KlaBier/Powershell

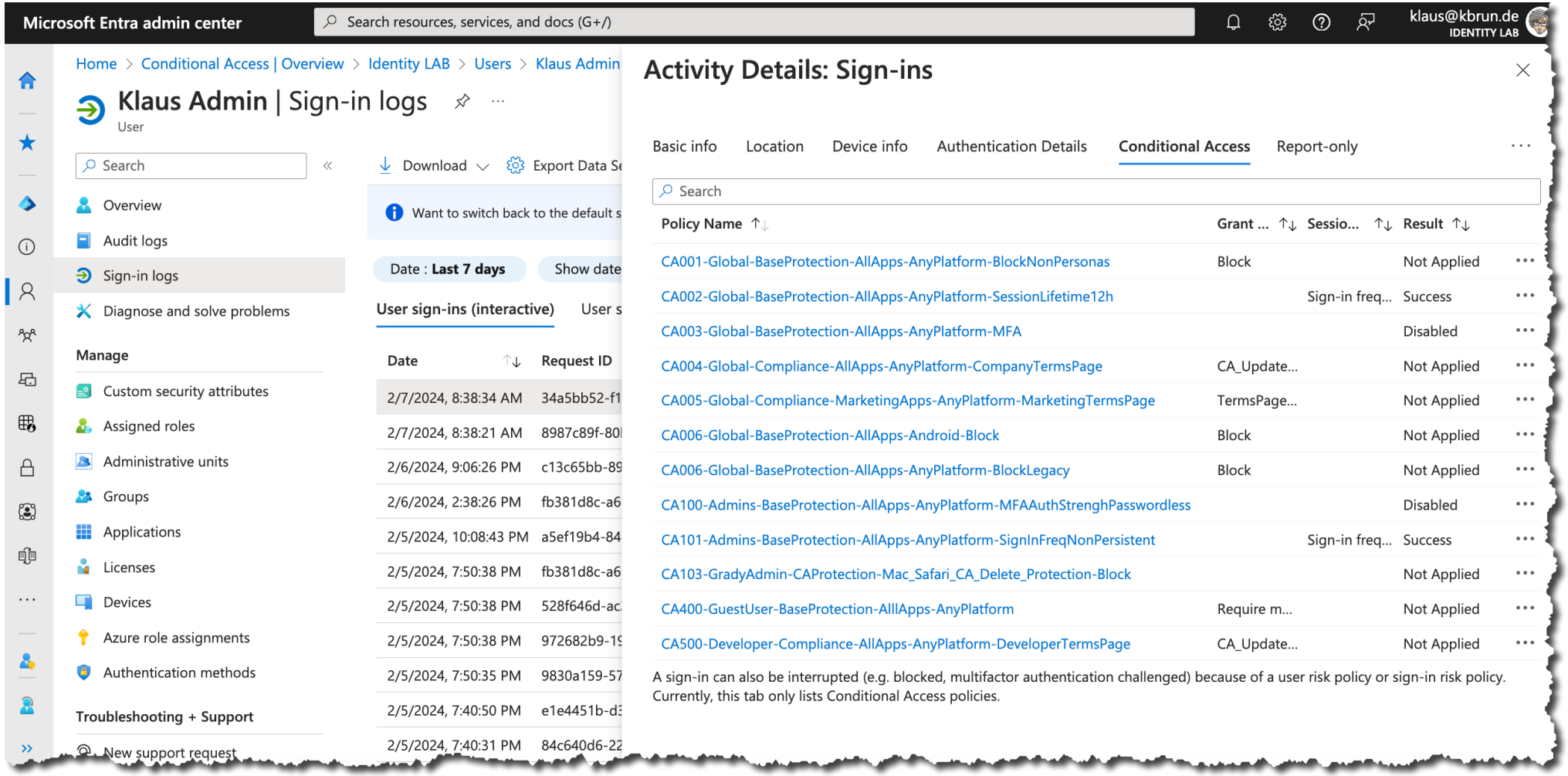
```
# ... use Excel stuff from Doug Finke
Install-Module -Name ImportExcel

#### Entra Roles ...
# Login
Connect-MgGraph -Scopes "RoleManagement.Read.All"

# Get all roles
$roles = Get-MgRoleManagementDirectoryRoleDefinition

# ... and write it to excel
$roles | select-object -property DisplayName, Description `
| Export-Excel .\roles.xlsx -WorksheetName "Roles" -AutoSize

#### Azure Roles ...
# Login
Connect-AzAccount

# Get all roles
$azroles = Get-AzRoleDefinition

$azroles | select-object -property Name, Description `
| Export-Excel .\roles.xlsx -WorksheetName "AZRoles" -AutoSize
```

Zero Trust und Identity – Warum Hoffnung keine Strategie ist

Empfehlung: Gutes „Naming“ ✓

Must read:

Conditional Access framework and policies - Azure Architecture Center | Microsoft Learn

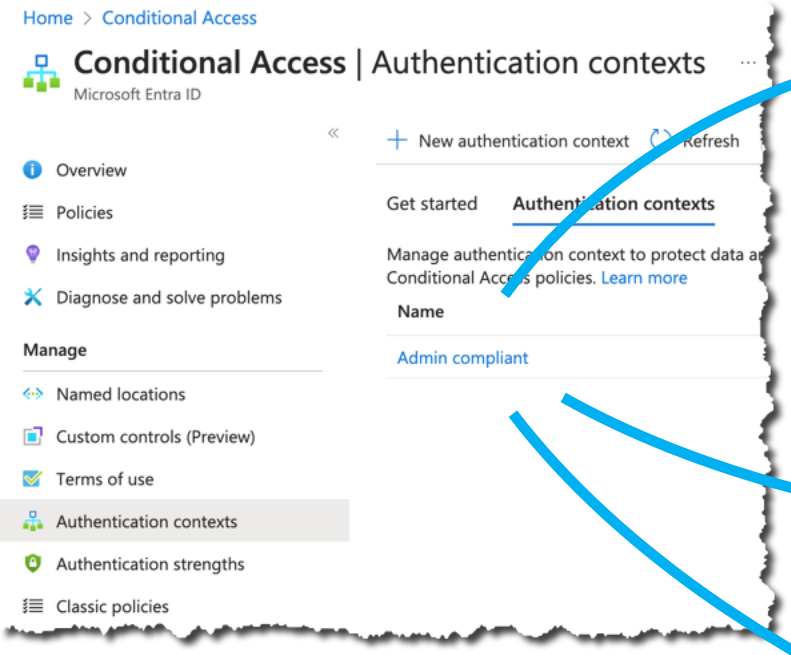


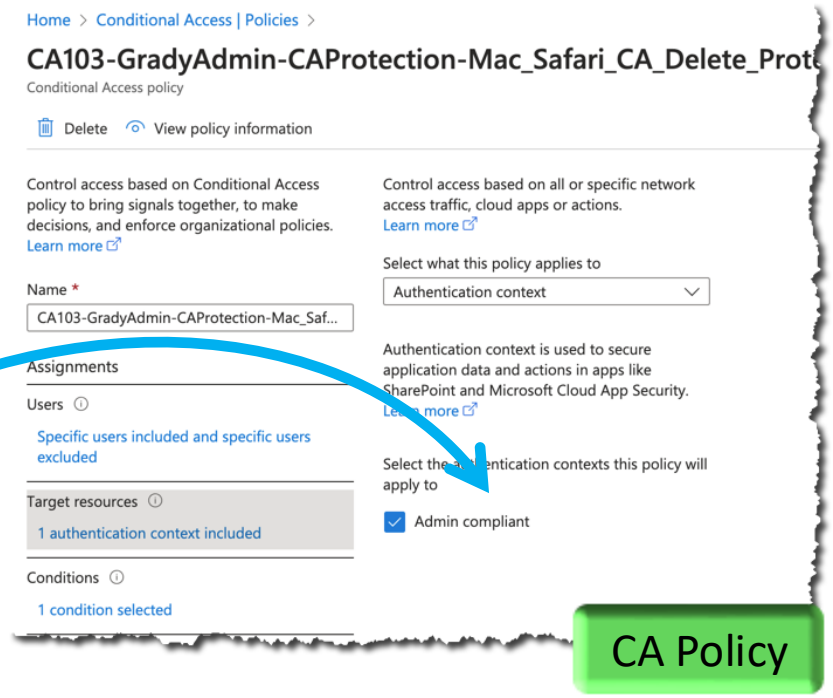
Zero Trust und Identity – Warum Hoffnung keine Strategie ist

Conditional Access für Admins

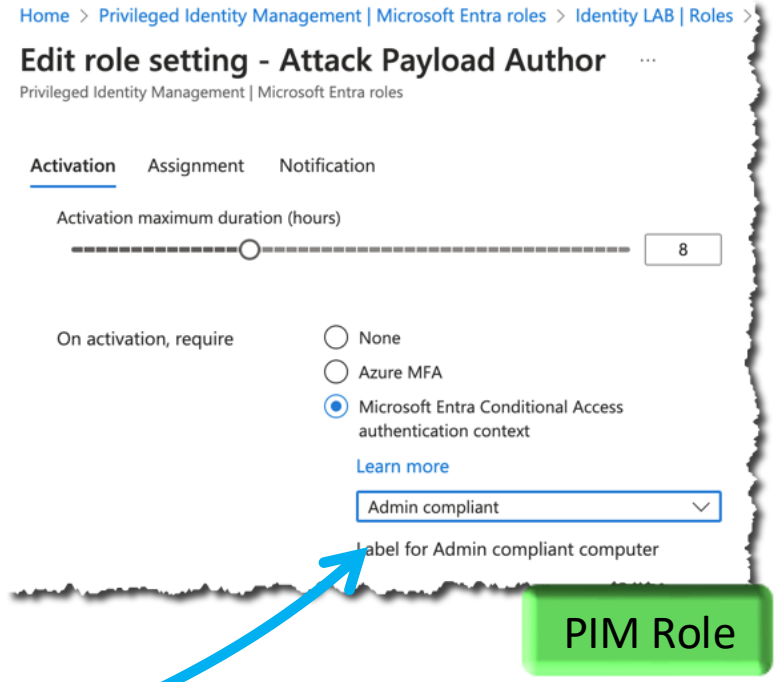
Empfehlung:

Protected Actions ✓

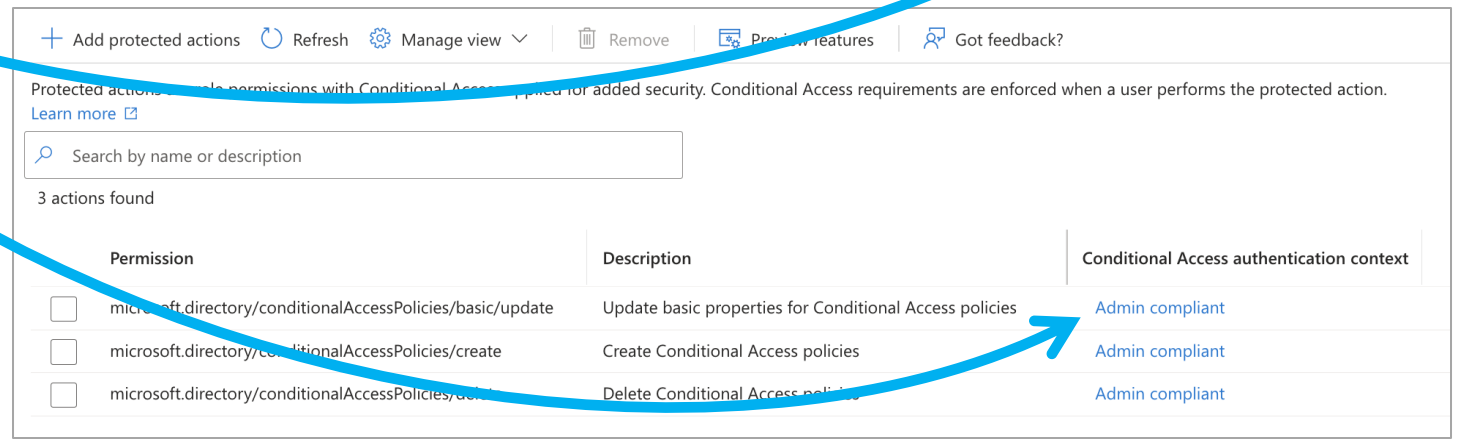




CA Policy



PIM Role



Zero Trust und Identity – Warum Hoffnung keine Strategie ist

Conditional Access für Admins

Empfehlung:

Authentication strength ✓