

# 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>



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



[Klaus.bierschenk@cgi.com](mailto:Klaus.bierschenk@cgi.com)

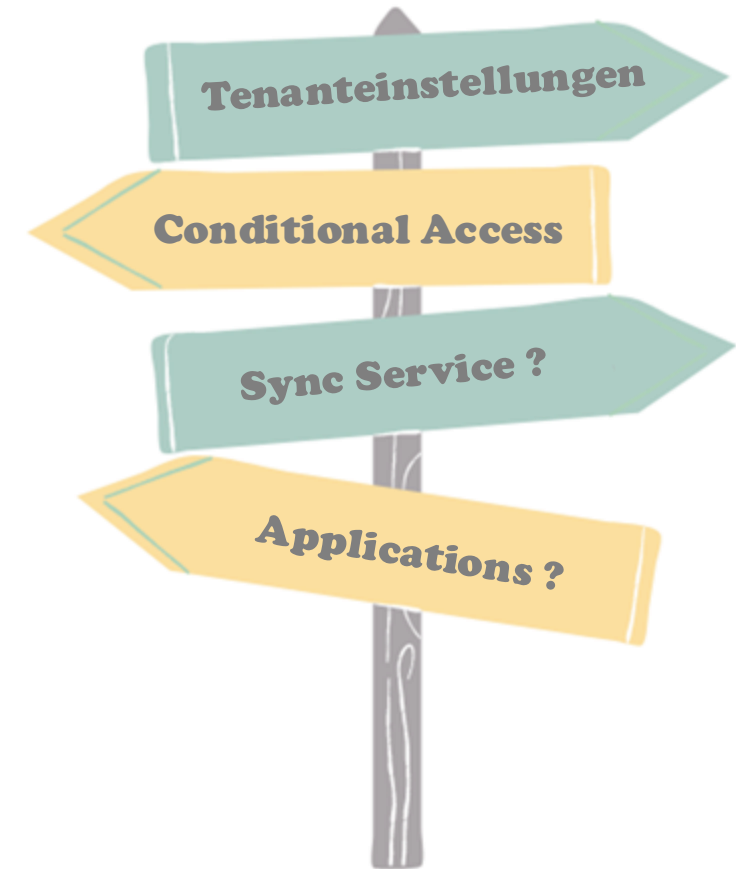


<https://nothingbutcloud.net/>

# Zero Trust und Identity – Warum Hoffnung keine Strategie ist

## AGENDA

- 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

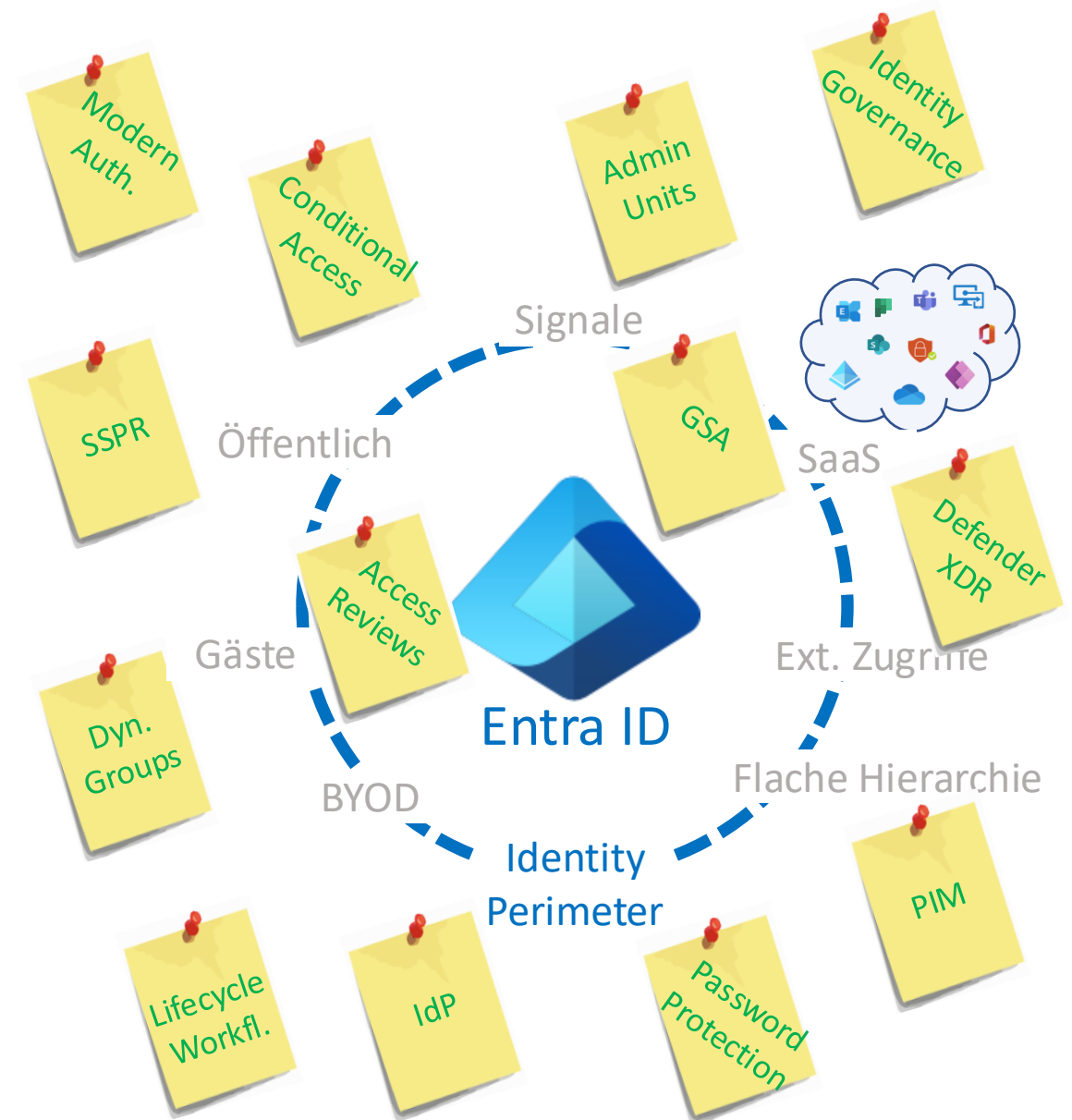
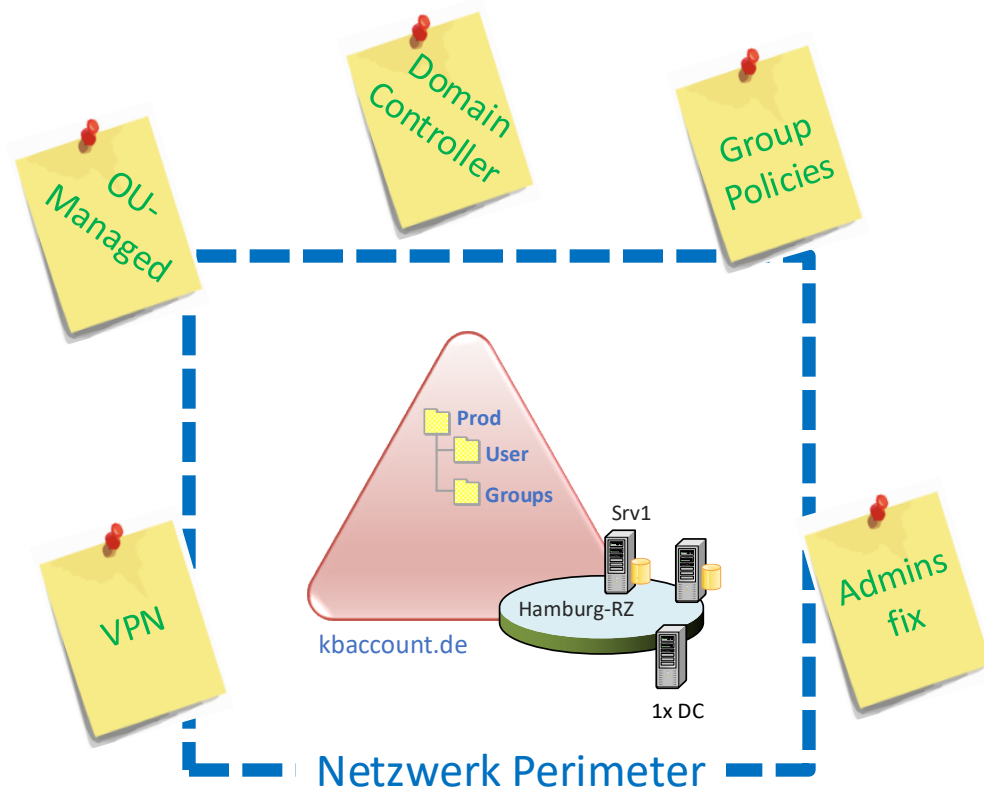
## AGENDA

- 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?

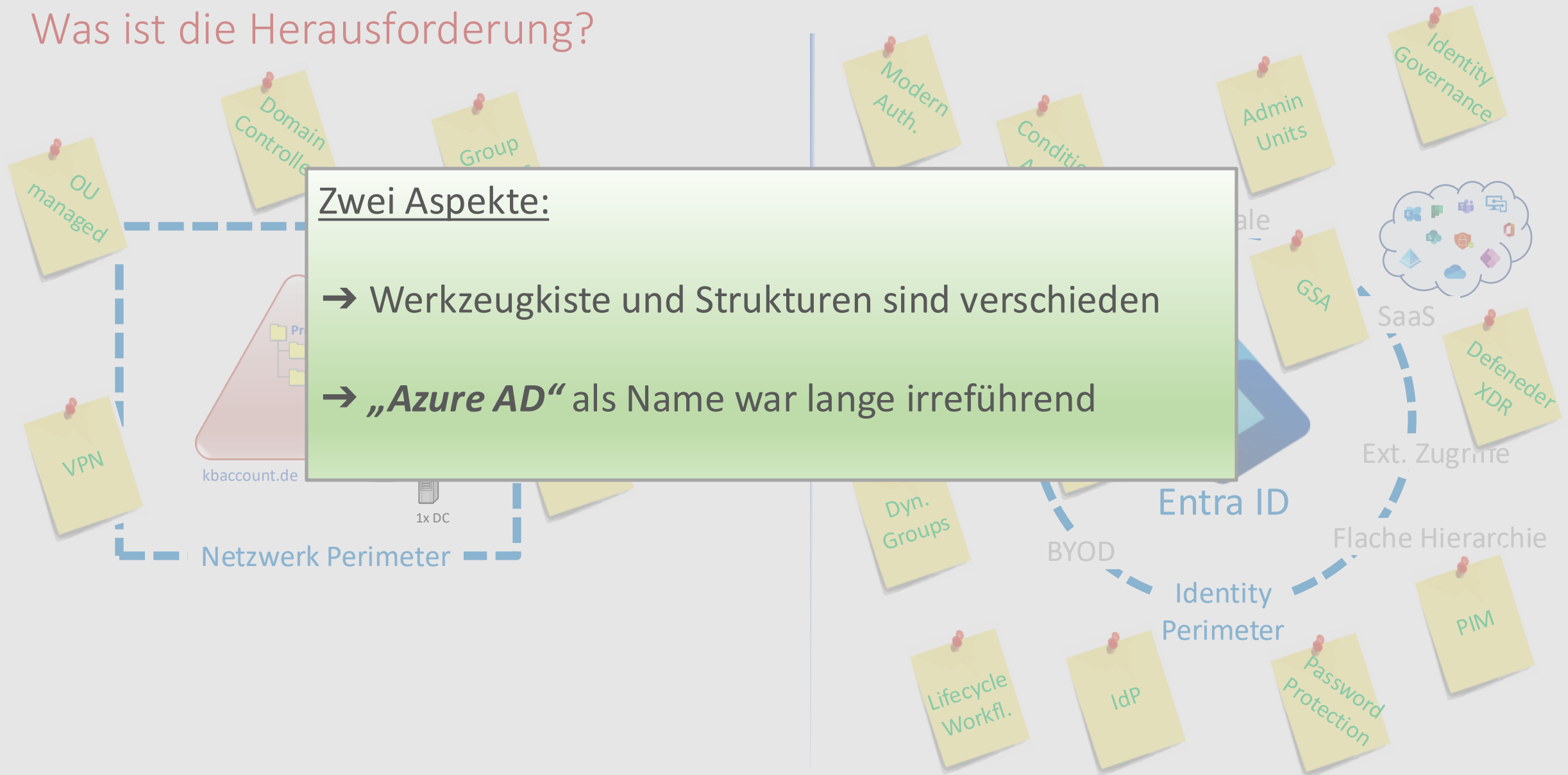


# Zero Trust und Identity – Warum Hoffnung keine Strategie ist

Was ist die Herausforderung?

Zwei Aspekte:

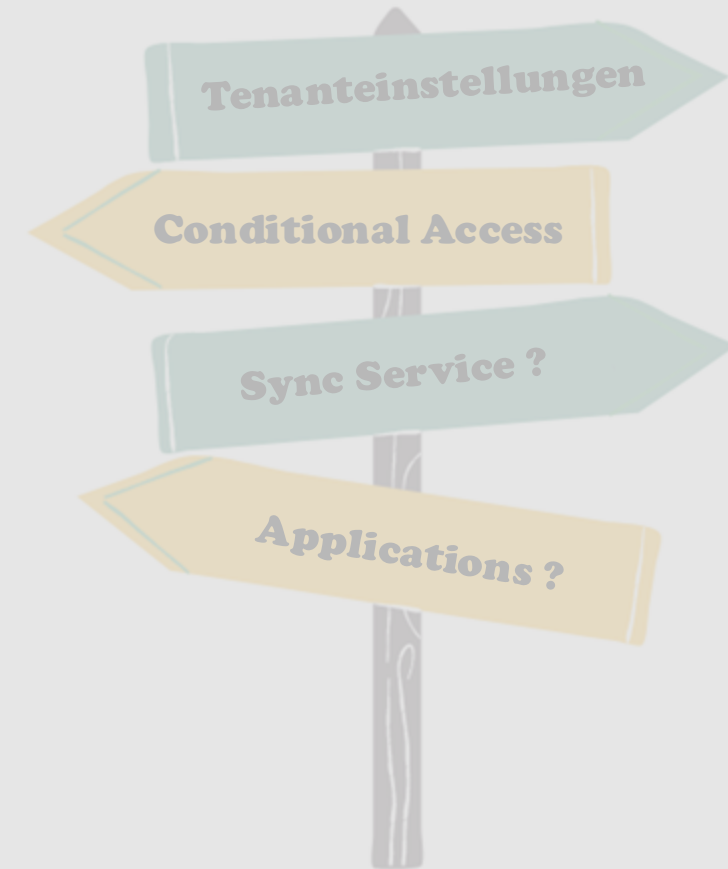
- Werkzeugkiste und Strukturen sind verschieden
- „**Azure AD**“ als Name war lange irreführend



# Zero Trust und Identity – Warum Hoffnung keine Strategie ist

## AGENDA

- 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
- ✓ Vorausschauende Planung
- ✓ Zuweisung entweder „active“ oder „eligible“
- ✓ Bedarfsgerechte Zuweisung (JIT/JEA) mit PIM



### Azure Admin Roles (619)

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

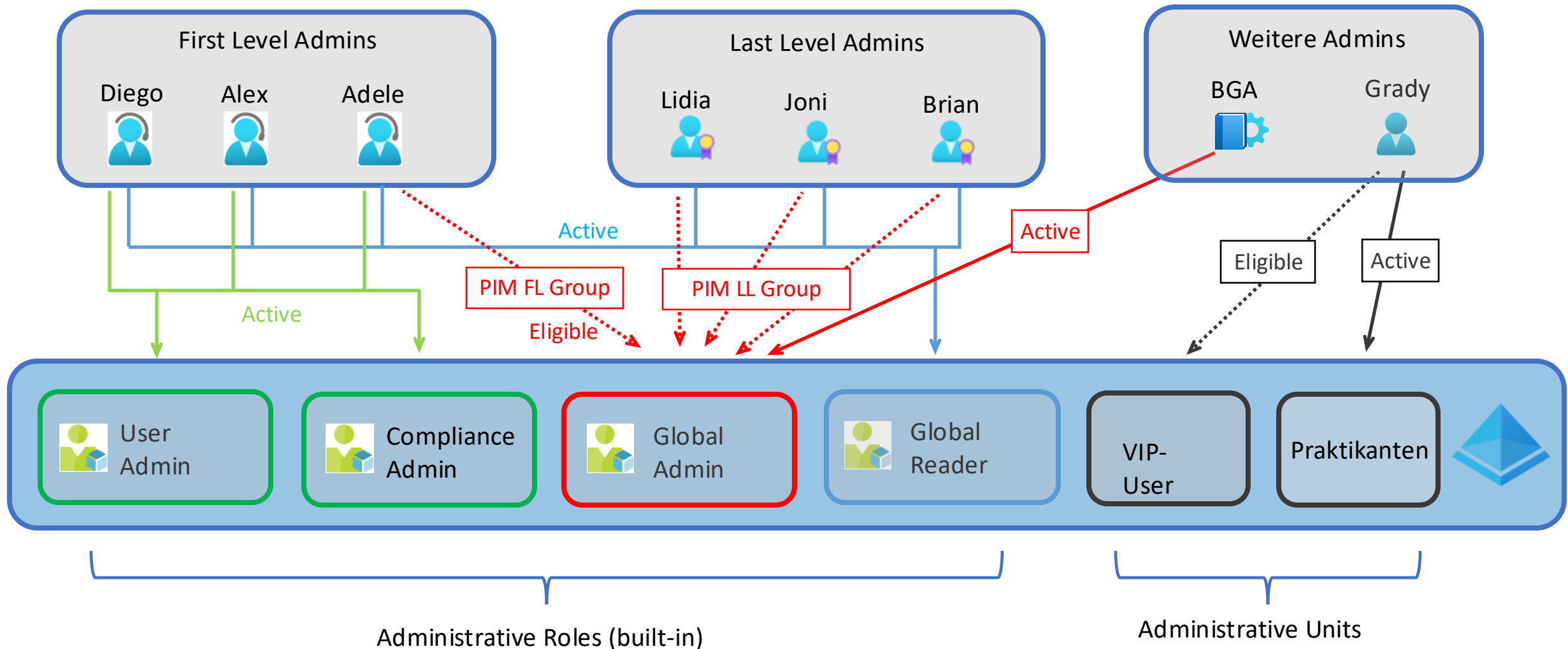
### Entra Admin Roles (117)

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

## AGENDA

- 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

## AGENDA

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



# Zero Trust und Identity – Warum Hoffnung keine Strategie ist

schwach

okay

besser

sehr gut

**Nur Password**

123456

Admin

qwertzuio

P@sw0rd2025%

\$%Ffer\$32“1??ß/  
86%fdrtg4\$\$“

**Password und ...**

SMS

Anruf

**Password und ...**

MS Authenticator  
Push Notification

Software Token OTP

Hardware Token OTP

**Noch besser  
Passwordless**

MS Authenticator  
Phone Sign-In

**Phishing-resistant**

Windows Hello for  
Business

FIDO Security Key

Certificate-based  
authentification  
(MFA)

Platform credential  
for MacOS

Passkey in MS  
Authenticator  
(device-bound)

schwach



Stärkere Authentifizierung



sehr gut

# 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](#)



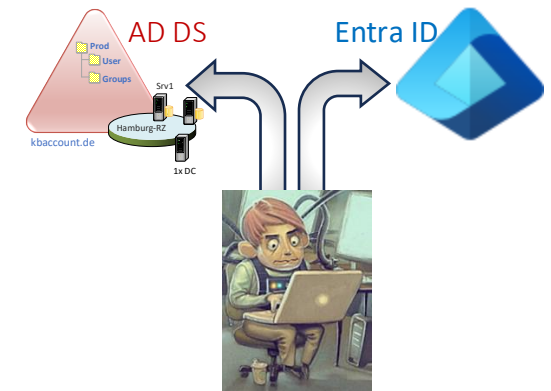
# Zero Trust und Identity – Warum Hoffnung keine Strategie ist

## 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 - Entra ID ist kein AD



- ➔ 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



# Zero Trust und Identity – Warum Hoffnung keine Strategie ist

---

Backup / Anhang

# Zero Trust und Identity – Warum Hoffnung keine Strategie ist

## Excellfile 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

Microsoft Entra admin center

Search resources, services, and docs (G+/)

klaus@kbrun.de  
IDENTITY LAB

Home > Conditional Access | Overview > Identity LAB > Users > Klaus Admin

Klaus Admin | Sign-in logs

User

Search

Download Export Data

Want to switch back to the default s

Date : Last 7 days Show date

User sign-ins (interactive) User s

Date	Request ID
2/7/2024, 8:38:34 AM	34a5bb52-f1
2/7/2024, 8:38:21 AM	8987c89f-80
2/6/2024, 9:06:26 PM	c13c65bb-89
2/6/2024, 2:38:26 PM	fb381d8c-a6
2/5/2024, 10:08:43 PM	a5ef19b4-84
2/5/2024, 7:50:38 PM	fb381d8c-a6
2/5/2024, 7:50:38 PM	528f646d-ac
2/5/2024, 7:50:38 PM	972682b9-15
2/5/2024, 7:50:35 PM	9830a159-57
2/5/2024, 7:40:50 PM	e1e4451b-d3
2/5/2024, 7:40:31 PM	84c640d6-22

Activity Details: Sign-ins

Basic info Location Device info Authentication Details Conditional Access Report-only

Search

Policy Name	Grant ...	Sessio...	Result
CA001-Global-BaseProtection-AllApps-AnyPlatform-BlockNonPersonas	Block		Not Applied
CA002-Global-BaseProtection-AllApps-AnyPlatform-SessionLifetime12h		Sign-in freq...	Success
CA003-Global-BaseProtection-AllApps-AnyPlatform-MFA			Disabled
CA004-Global-Compliance-AllApps-AnyPlatform-CompanyTermsPage	CA_Update...		Not Applied
CA005-Global-Compliance-MarketingApps-AnyPlatform-MarketingTermsPage	TermsPage...		Not Applied
CA006-Global-BaseProtection-AllApps-Android-Block	Block		Not Applied
CA006-Global-BaseProtection-AllApps-AnyPlatform-BlockLegacy	Block		Not Applied
CA100-Admins-BaseProtection-AllApps-AnyPlatform-MFAAuthStrengthPasswordless			Disabled
CA101-Admins-BaseProtection-AllApps-AnyPlatform-SignInFreqNonPersistent		Sign-in freq...	Success
CA103-GradyAdmin-CAProtection-Mac_Safari_CA_Delete_Protection-Block			Not Applied
CA400-GuestUser-BaseProtection-AllApps-AnyPlatform	Require m...		Not Applied
CA500-Developer-Compliance-AllApps-AnyPlatform-DeveloperTermsPage	CA_Update...		Not Applied

A sign-in can also be interrupted (e.g. blocked, multifactor authentication challenged) because of a user risk policy or sign-in risk policy. Currently, this tab only lists Conditional Access policies.

# Zero Trust und Identity – Warum Hoffnung keine Strategie ist

Conditional Access für Admins

Empfehlung:

Protected Actions ✓

Home > Conditional Access



## Conditional Access | Authentication contexts

Microsoft Entra ID

Overview

Policies

Insights and reporting

Diagnose and solve problems

Manage

Named locations

Custom controls (Preview)

Terms of use

Authentication contexts

Authentication strengths

Classic policies

+ New authentication context Refresh

Get started Authentication contexts

Manage authentication context to protect data as Conditional Access policies. [Learn more](#)

Name

Admin compliant

Home > Conditional Access | Policies >

## CA103-GradyAdmin-CAProtection-Mac\_Safari\_CA\_Delete\_Prot...

Conditional Access policy

Delete View policy information

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*

CA103-GradyAdmin-CAProtection-Mac\_Saf...

Assignments

Users

Specific users included and specific users excluded

Target resources

1 authentication context included

Conditions

1 condition selected

Control access based on all or specific network access traffic, cloud apps or actions. [Learn more](#)

Select what this policy applies to

Authentication context

Authentication context is used to secure application data and actions in apps like SharePoint and Microsoft Cloud App Security. [Learn more](#)

Select the authentication contexts this policy will apply to

☒ Admin compliant

CA Policy

Home > Privileged Identity Management | Microsoft Entra roles > Identity LAB | Roles >

## Edit role setting - Attack Payload Author

Privileged Identity Management | Microsoft Entra roles

Activation

Assignment

Notification

Activation maximum duration (hours)

8

On activation, require

☐ None

☐ Azure MFA

☒ Microsoft Entra Conditional Access authentication context

[Learn more](#)

Admin compliant

Label for Admin compliant computer

PIM Role

+ Add protected actions Refresh Manage view Remove Preview features Got feedback?

Protected actions enable permissions with Conditional Access applied for added security. Conditional Access requirements are enforced when a user performs the protected action. [Learn more](#)

Search by name or description

3 actions found

Permission	Description	Conditional Access authentication context
<input type="checkbox"/> microsoft.directory/conditionalAccessPolicies/basic/update	Update basic properties for Conditional Access policies	Admin compliant
<input type="checkbox"/> microsoft.directory/conditionalAccessPolicies/create	Create Conditional Access policies	Admin compliant
<input type="checkbox"/> microsoft.directory/conditionalAccessPolicies/delete	Delete Conditional Access policies	Admin compliant

# Zero Trust und Identity – Warum Hoffnung keine Strategie ist

Conditional  
Access  
für Admins

Empfehlung:

Authentication  
strength ✓



Microsoft Entra admin center

Search resources, services, and docs (G+)

Conditional Access | Policies

### CA100-Admins-BaseProtection-AllApps-AnyP

Conditional Access policy

Delete View policy information

Name \*

CA100-Admins-BaseProtection-AllApps-Any...

Assignments

Users

Specific users included and specific users excluded

Target resources

All cloud apps

Conditions

0 conditions selected

Access controls

Grant

1 control selected

Enable policy

Report-only On Off

Save

### Grant

Control access enforcement to block or grant access. [Learn more](#)

☐ Block access

☒ Grant access

☐ Require multifactor authentication

**"Require authentication strength" cannot be used with "Require multifactor authentication". [Learn more](#)**

☒ Require authentication strength

Passwordless MFA

**To enable all authentication strengths, configure cross-tenant access settings to accept claims coming from Microsoft Entra tenants for external users. Authentication strengths will only configure second factor**

Select