

Safeguard Your Admin Identities: Mastering Active Directory and Azure AD Account Security

Johannes Blohberger | base-IT





Johannes Blohberger

- OnPrem Security
 - Active Directory Tiering
 - OS Hardening
- Cloud Security
 - Microsoft 365 E5
- Managed Service Security
 - Service Delivery Management

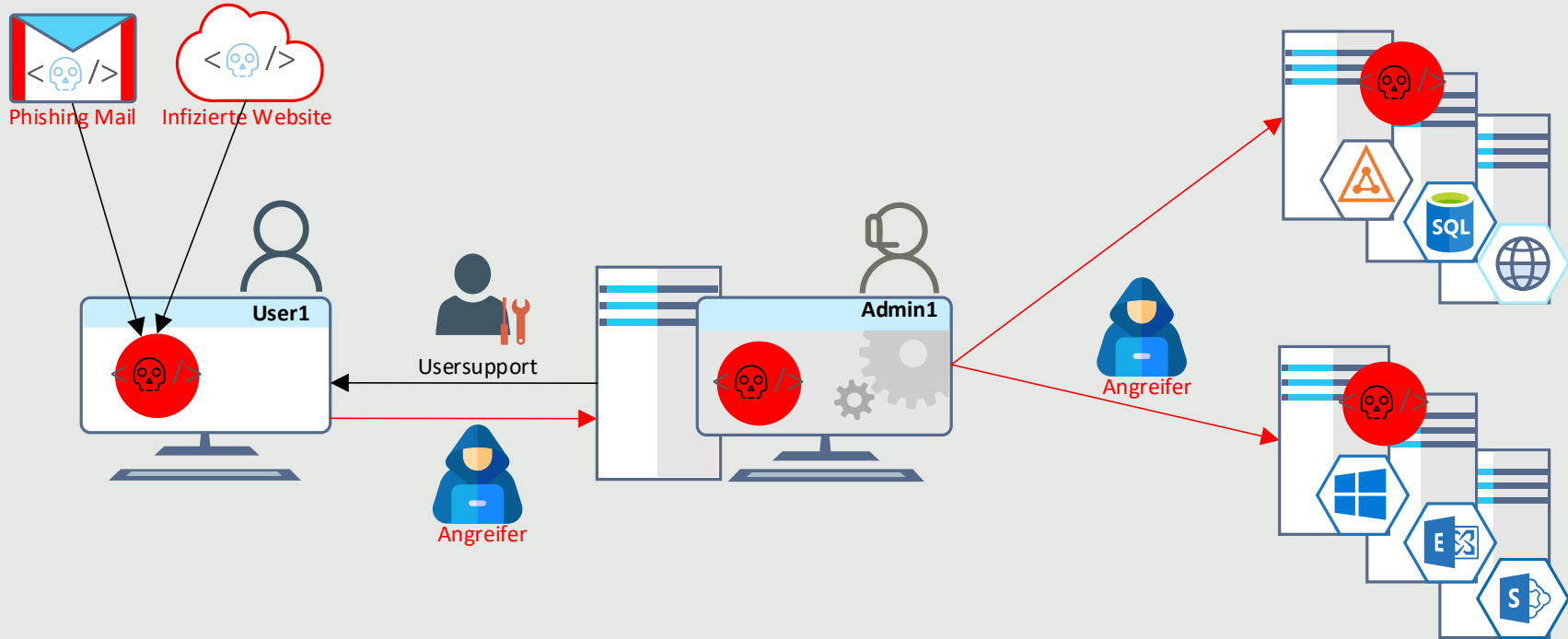


OnPrem Administration

Herausforderung:

- „Domain Admins“ per Default lokale Administratoren
- ein User pro Admin für alles
- Legacy Protokolle ohne MFA

Lateral Movement





Active Directory Tiering

Lösung:

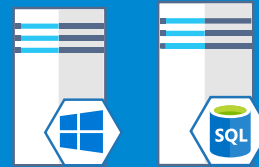
- Unterteilung der *Assets* in *Tier-Levels*
- pro *Tier-Level* eigene Admin Accounts
- Absicherung des Eintrittspunktes mittels MFA

AD Tiering - Tier Levels

Tier 0 – Authentication Services



Tier 1 – App Services



Tier 2 – End User Devices



AD Tiering - Tier Levels

Admin Access (Login)

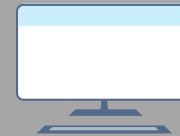
Tier 0 – Authentication Services



Tier 1 – App Services

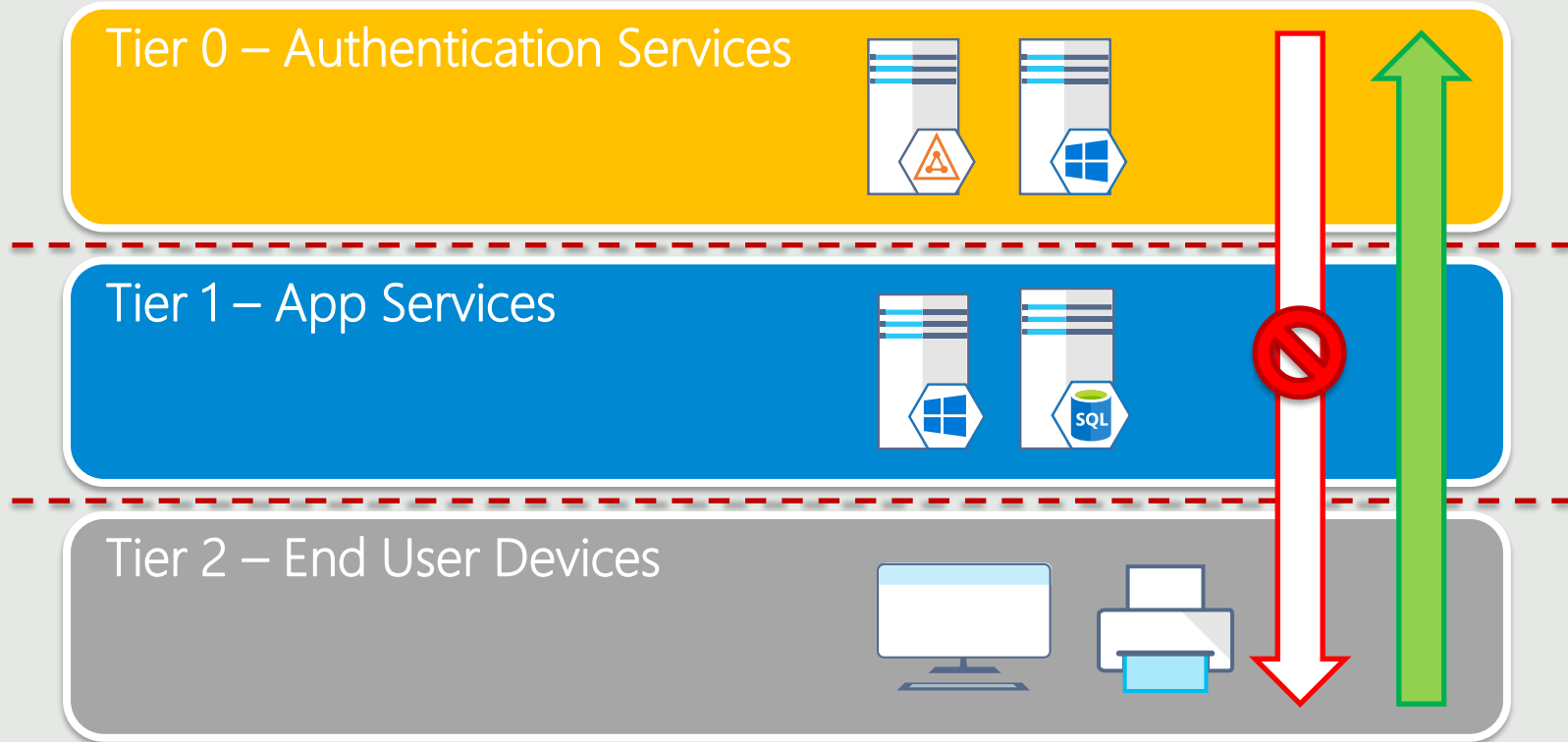


Tier 2 – End User Devices



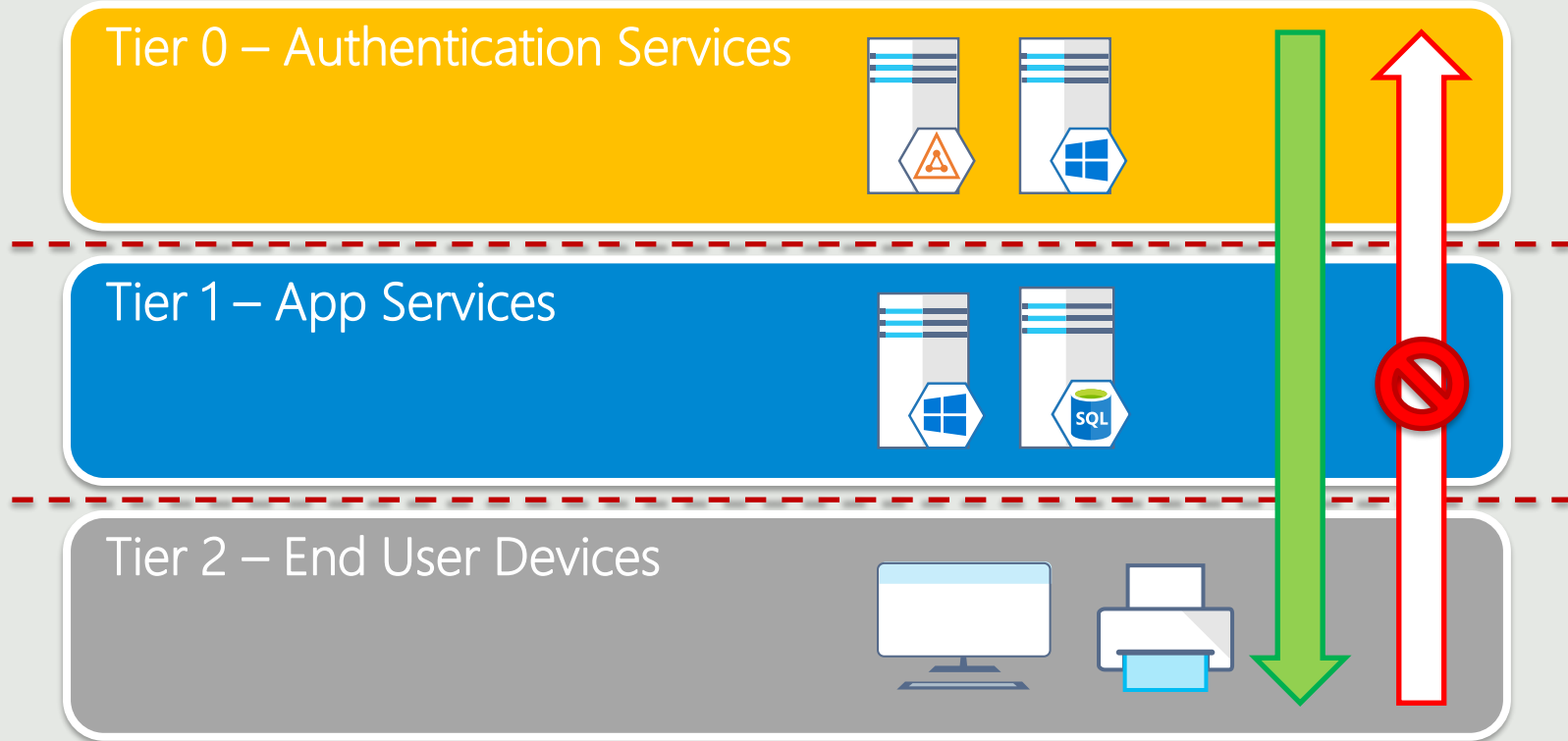
AD Tiering - Tier Levels

Service Access



AD Tiering - Tier Levels

AD Administration





AD Tiering - Tier Levels

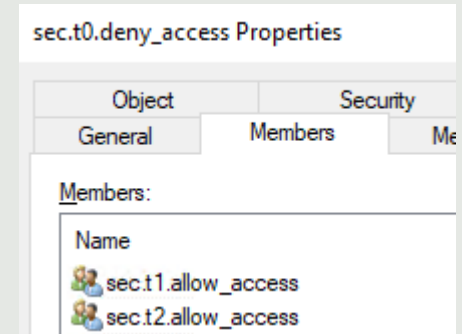
Technische Umsetzung:

- GPO zur Steuerung der lokalen Gruppe „Administrators“
- **allow** & **deny** access Gruppen inkl. Verschachtelung
- LockOut von Admins anderer *Tier-Level*

AD Tiering - Tier Levels

Gruppenverschachtelung:

LockOut via GPO:



| Local Policies/User Rights Assignment | | hide |
|---------------------------------------|-----------------------|------|
| Policy | Setting | |
| Deny log on locally | AD\sec.t0.deny_access | |
| Deny log on through Terminal Services | AD\sec.t0.deny_access | |

User in >1 allow access Gruppe = LockOut



AD Tiering – AD Security

- Domain Controller ohne weiterer Rollen/Tools
- Prüfung der Security relevanten AD Einstellungen und Delegations
- Hardening der Admin Accounts (Protected Users, sichere Kennwörter,...)



MFA Absicherung OnPrem

Herausforderung:

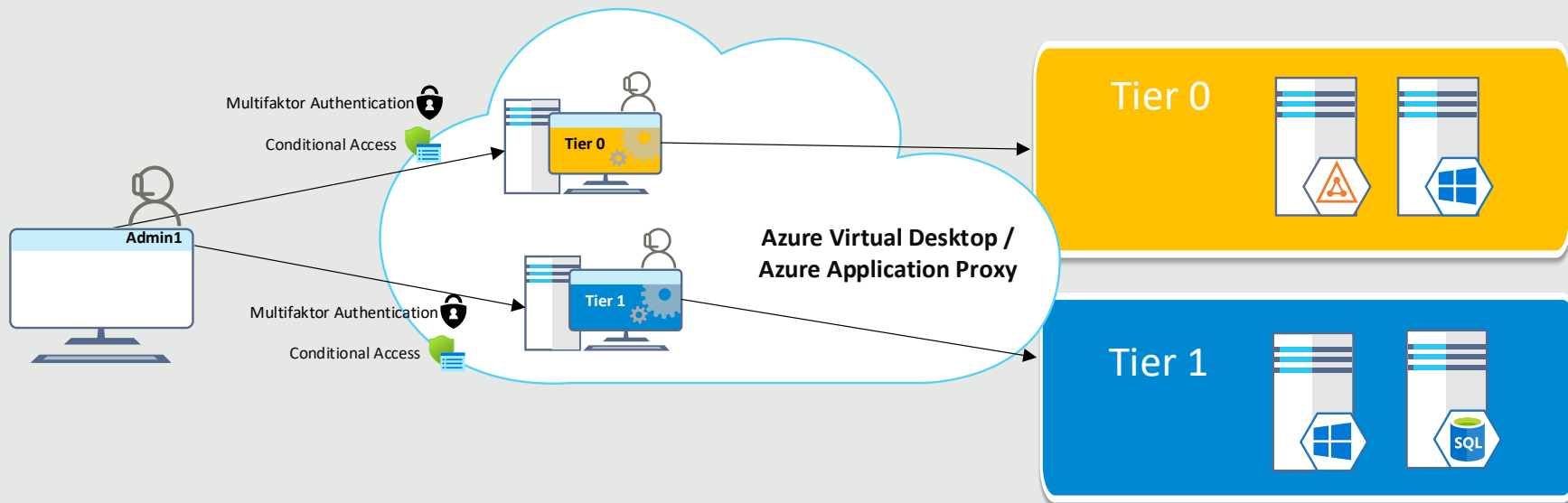
- Legacy Protokolle (Kerberos & NTLM) unterstützen kein MFA
- Werden Hashes oder Tickets gestohlen, kann die Nutzung nicht revalidiert werden



Privileged Access Workstations

- best practice: eigenständiges, physisches Gerät bzw. pro Tier-Level separates Gerät
- **Kompromisslösung:**
 - VM pro Tier-Level
 - Erzwingen von MFA für Zugriff
 - OS Hardening

Privileged Access Workstations





Privileged Access Workstations

- Erzwingen von MFA für Zugriff
- multi-session nur für User mit gleichen Rechten
- lokale Adminrechte ausschließlich mit überwachten Service Accounts
- OS Hardening (MS Security Baselines)

Azure Active Directory

Empowering the Modern Era



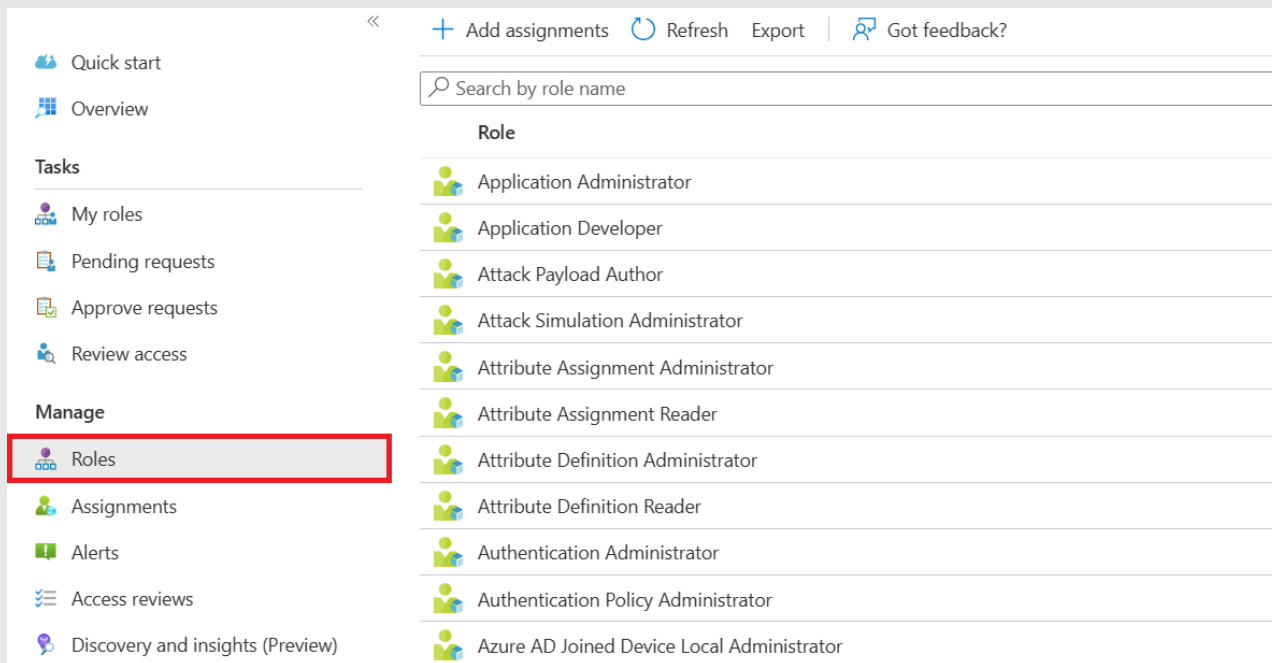


Privileged Identity Management

- Azure AD Feature (Premium P2)
- just-in-time access
- time-bound access
- enforce MFA
- approval, justification, notifications...

Privileged Identity Management

Konfiguration von Rollen:



The screenshot displays the Microsoft Privileged Identity Management (PIM) console interface. The left-hand navigation pane is visible, with the 'Roles' option highlighted by a red rectangular box. The main content area on the right shows a list of roles, each preceded by a person icon. At the top of the main area, there are links for 'Add assignments', 'Refresh', 'Export', and 'Got feedback?'. Below these links is a search bar labeled 'Search by role name'.

Navigation Pane:

- Quick start
- Overview
- Tasks**
- My roles
- Pending requests
- Approve requests
- Review access
- Manage**
- Roles** (highlighted)
- Assignments
- Alerts
- Access reviews
- Discovery and insights (Preview)

Top Actions:

- + Add assignments
- Refresh
- Export
- Got feedback?

Search: Search by role name

Role List:

| Role |
|--|
| Application Administrator |
| Application Developer |
| Attack Payload Author |
| Attack Simulation Administrator |
| Attribute Assignment Administrator |
| Attribute Assignment Reader |
| Attribute Definition Administrator |
| Attribute Definition Reader |
| Authentication Administrator |
| Authentication Policy Administrator |
| Azure AD Joined Device Local Administrator |

Privileged Identity Management

Konfiguration von Gruppen (preview):

Privileged Identity Management | Groups (Preview)

<< Refresh | Got feedback?

Tasks

My roles

Pending requests

Approve requests

Manage

Roles

Assignments

Settings

Search by role name

| Role | ↑↓ | Modified | ↑↓ |
|--------|----|----------|----|
| Member | | Yes | |
| Owner | | No | |



Privileged Identity Management

Rolleneinstellungen:

Activation

Setting

Activation maximum duration (hours)

On activation, require

Require justification on activation

Require ticket information on activation

Require approval to activate

Approvers

Assignment

Setting

Allow permanent eligible assignment

Expire eligible assignments after

Allow permanent active assignment

Expire active assignments after

Require Azure Multi-Factor Authentication on active assignment

Require justification on active assignment



Thanks to our Sponsors!

basee it

ACP IT for
innovators.



INFOTECH
[IT & Communication]



Lenovo



secureguard

ACP IT for
innovators.