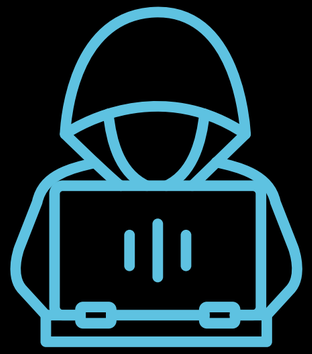
T.I.S.P. Community Meeting 2023

Berlin, 07. - 08.11.2023

Active Directory Security

Dipl.-Ing.
Carsten Vossel
CEO @ CCVOSSEL

Dipl.-Inform. Dipl.-Wi.-Ing.
Oliver Falkenthal
Lead Defensive Security @ CCVOSSEL
T.I.S.P.-Trainer



Offensive Security (RED)

- Penetrationtest
- Active Directory Hacking
- Red Teaming
- Phishing

Defensive Security (BLUE)

- Analyse & Konzepte
- Härtung & Cloud Security
- Active Directory und Identity Protection
- Organisatorische Sicherheit und Awareness

24/7 Secure Operations

- Sicherheitskritische Applikationen
- Businessprozesskritische Applikationen

Mitglied im TeleTrusT und aktiv im Arbeitskreis “Stand der Technik” seit 2019

Allgemeine Fakten

90 %

der untersuchten Angriffe haben das Active Directory als Angriffsvektor ausgenutzt.

50 %

der Unternehmen sind in den letzten 1–2 Jahren Opfer eines Cyberangriffs geworden.

40 %

der Angriffe waren erfolgreich.

Unsere Erfahrungen

90 %

der untersuchten Unternehmen konnten während des Penetrationstests übernommen werden.

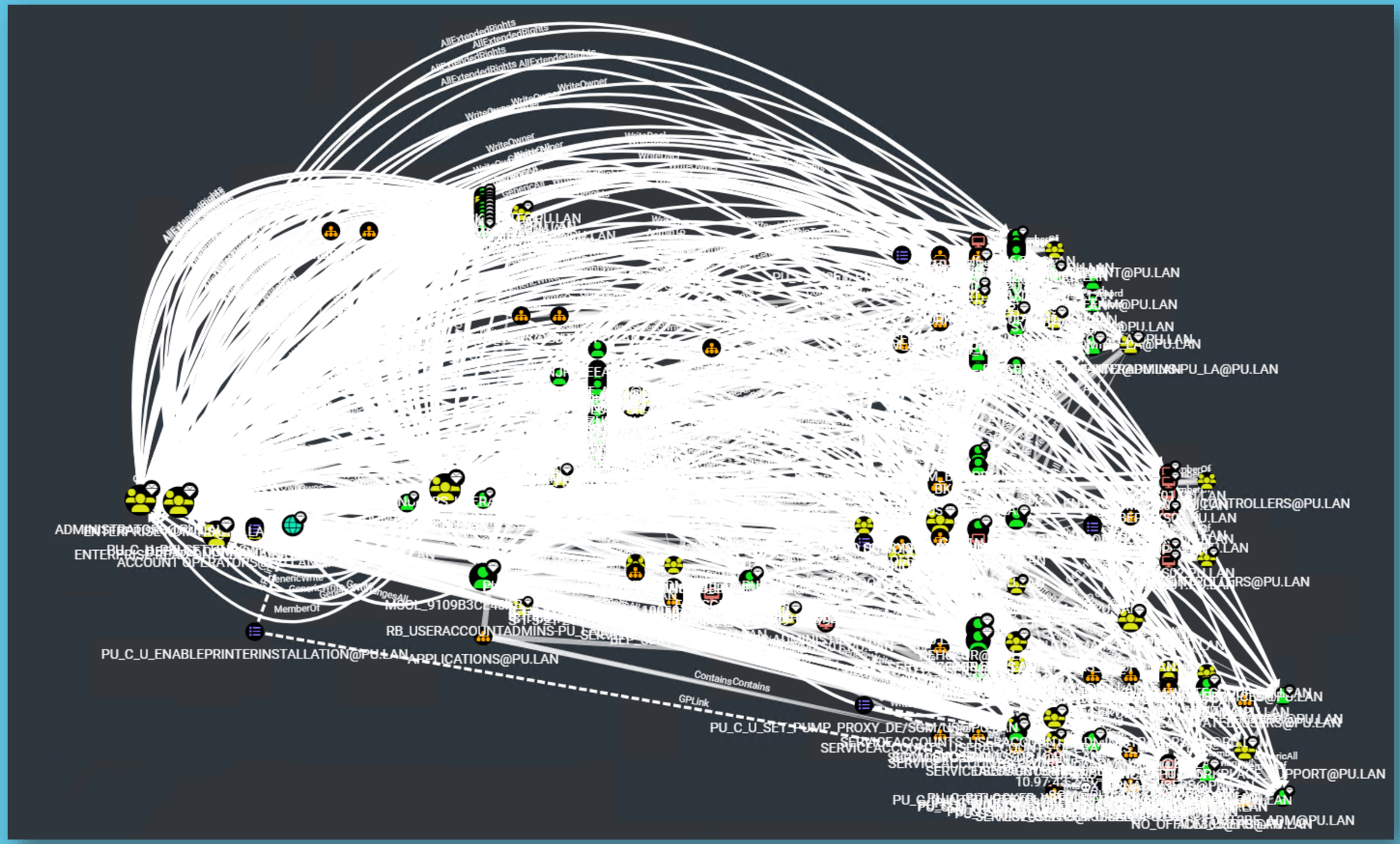
50 %

der Passwörter von Unternehmen werden innerhalb von 24 Stunden entschlüsselt

40 %

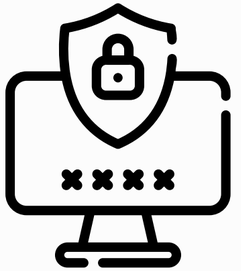
der Unternehmen waren konfiguriert, dass jeder Mitarbeiter administrative Berechtigung besaß oder erlangen konnte.

Übersichtliche Ansicht der Angriffsmöglichkeiten?

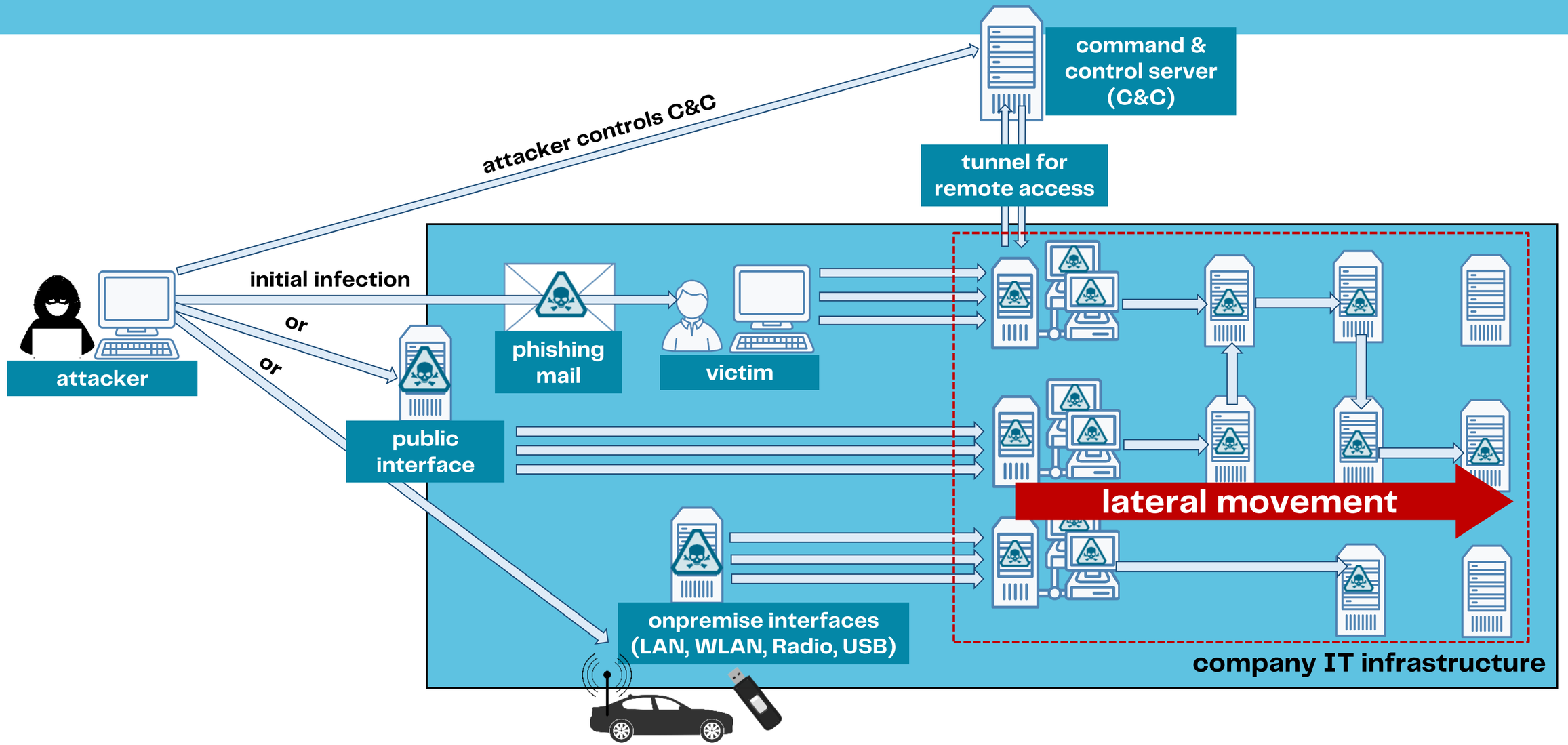


Das Active Directory Tier Model

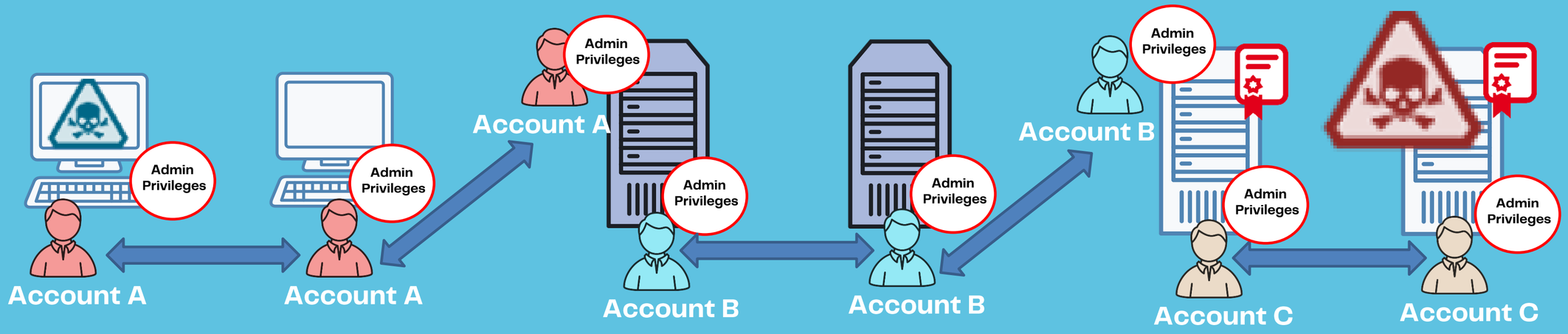
Active Directory wird zur Festung



Assume-Breach



Das Problem



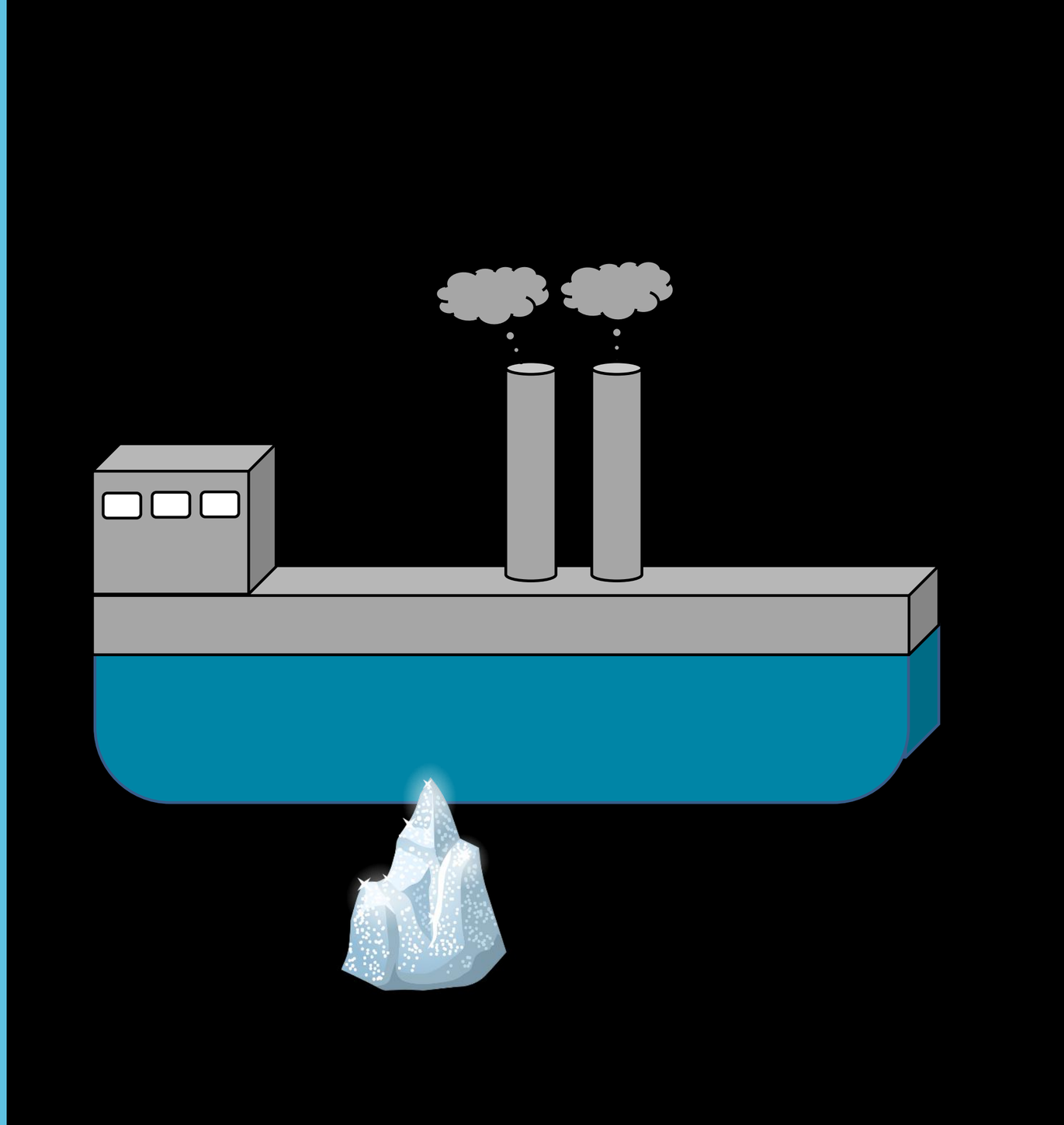
„Lateral Movement“ über mehrere Zwischensysteme zum Zielsystem

Admin-Rechte führen zur Aufdeckung von Passwörtern anderer Konten

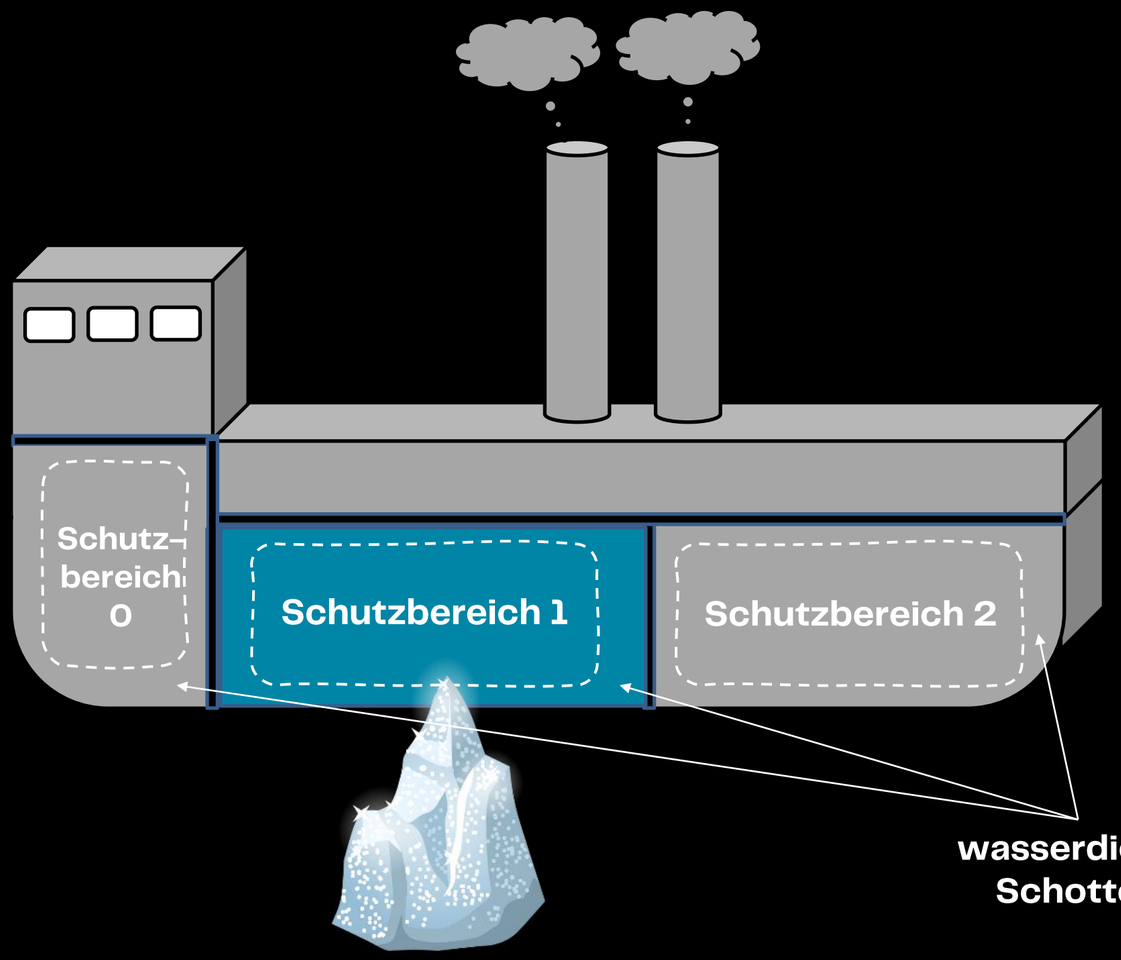
Ziel

Infrastruktursysteme (DNS, DC, PKI usw.) zu kompromittieren, um die gesamte IT-Infrastruktur zu übernehmen.

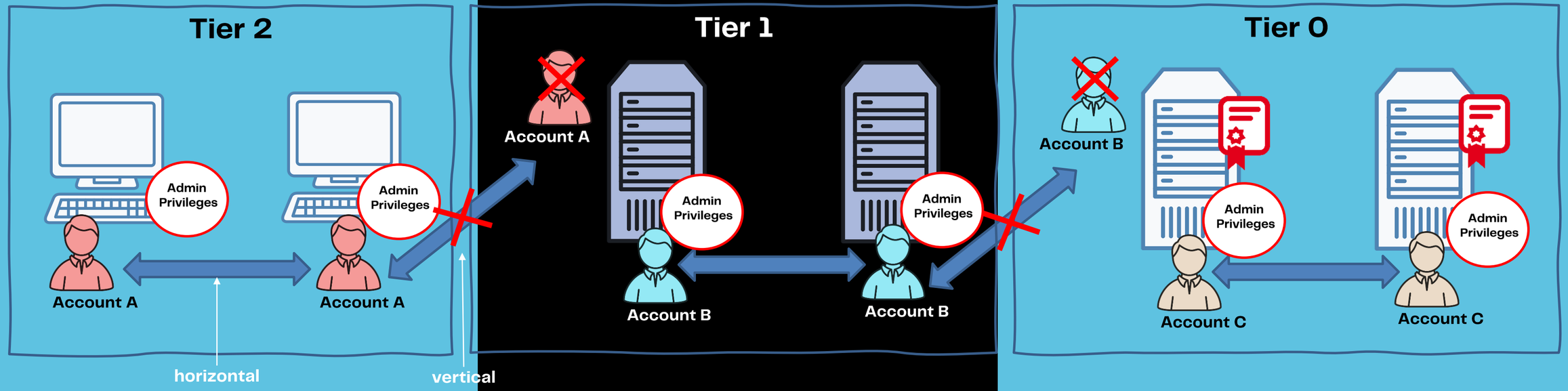
Wenn Informatiker Schiffe zeichnen...



Einführung von Schutzbereichen



Tier Model

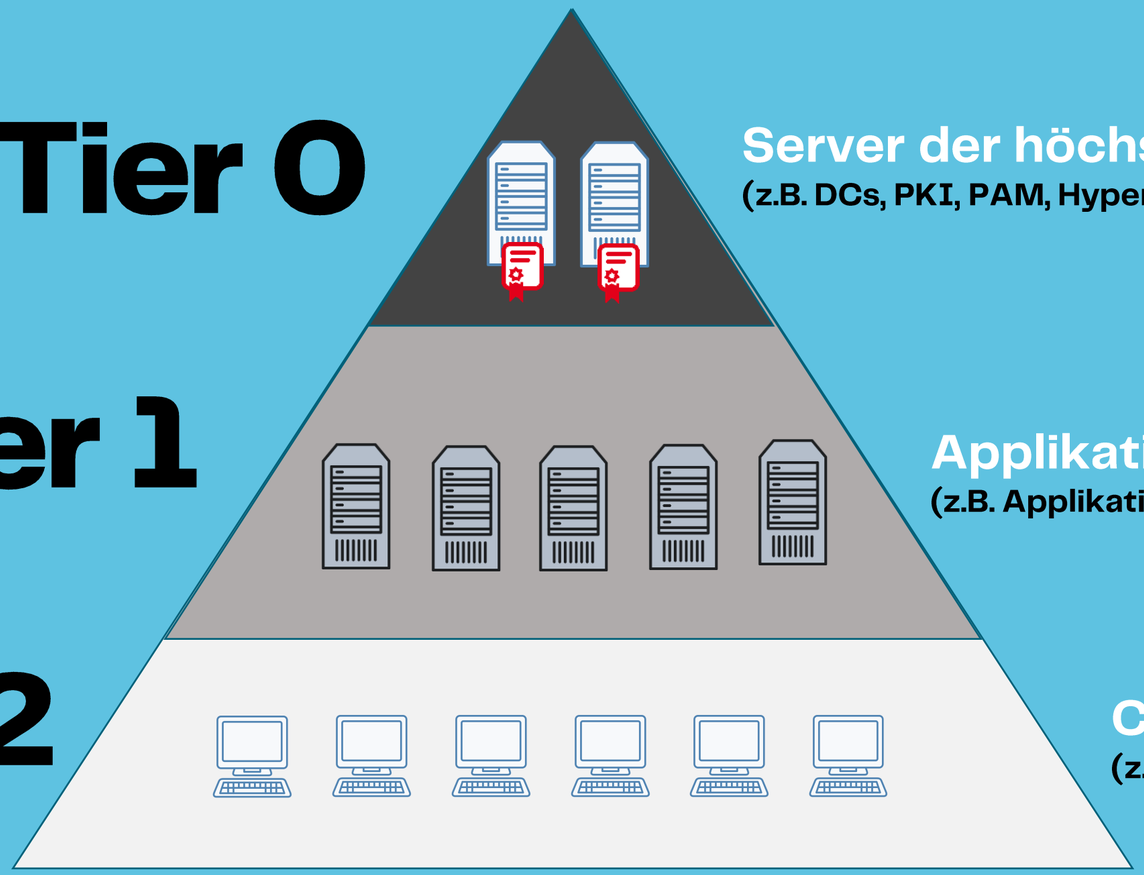


Unterteilung des Active Directory in mehrere Schutzbereiche (inkl. Zuordnung der Objekte)

Verhinderung vom Lateral Movement über die Tiergrenzen hinweg

Lateral Movement innerhalb des Tiers ist weiterhin möglich

Systeme im Tier Model (onPrem)



Tier 0

Server der höchsten Stufe
(z.B. DCs, PKI, PAM, Hypervisoren etc.)

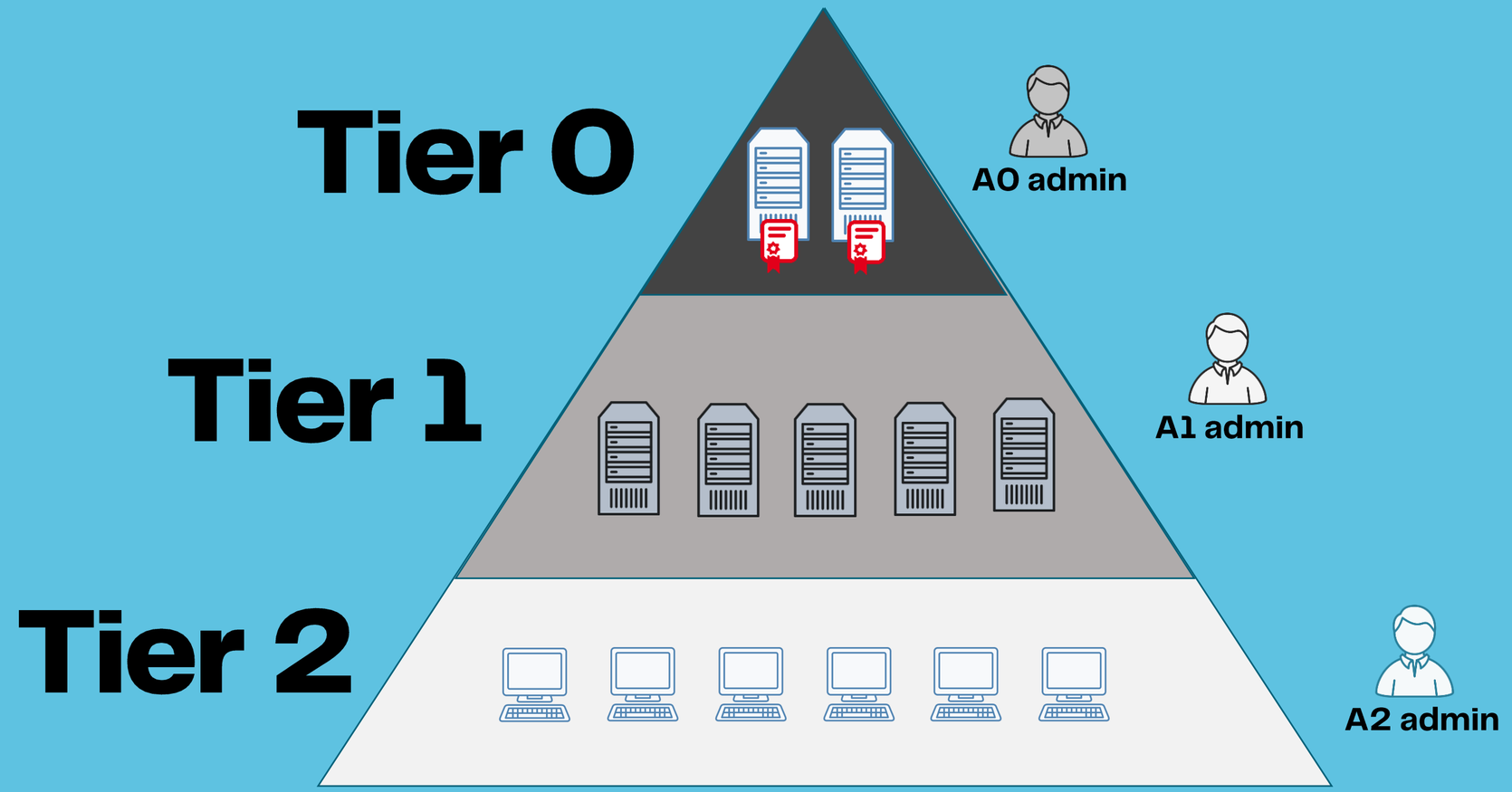
Tier 1

Applikationsserver
(z.B. Applikationsserver, Datenbankserver, Mailserver etc.)

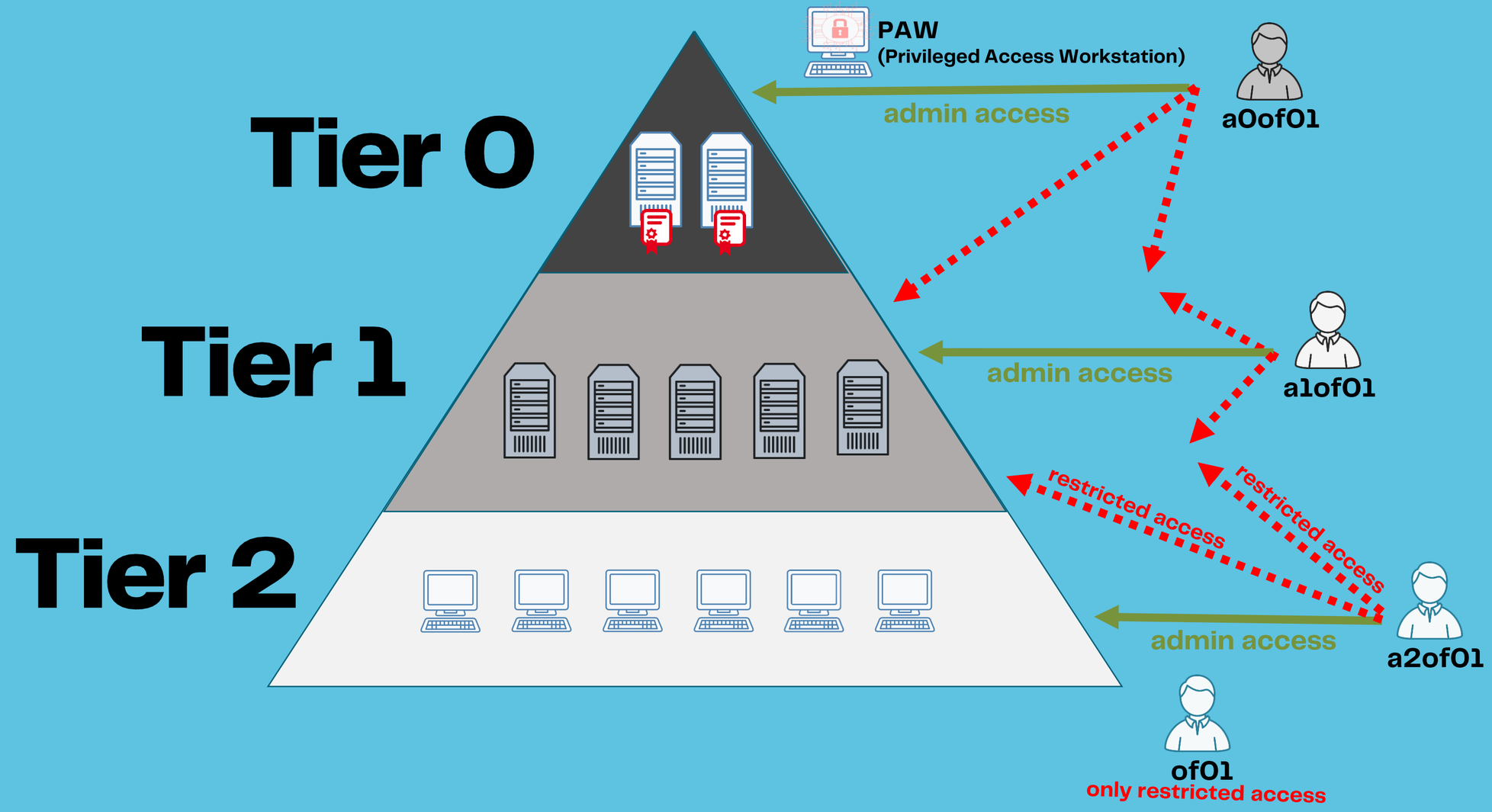
Tier 2

Clients
(z.B. Notebooks, Desktops)

Accounts im Tier Model

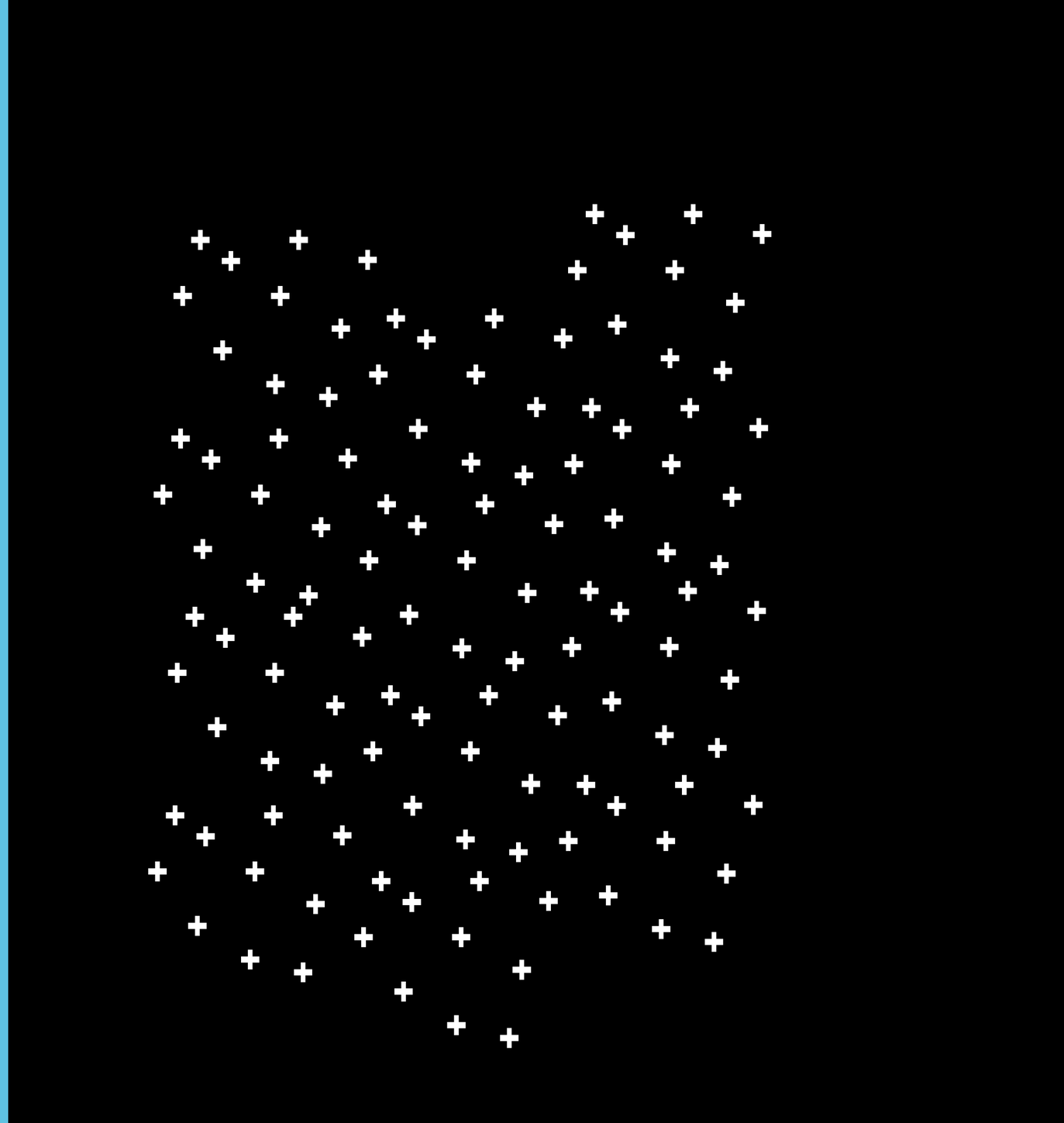


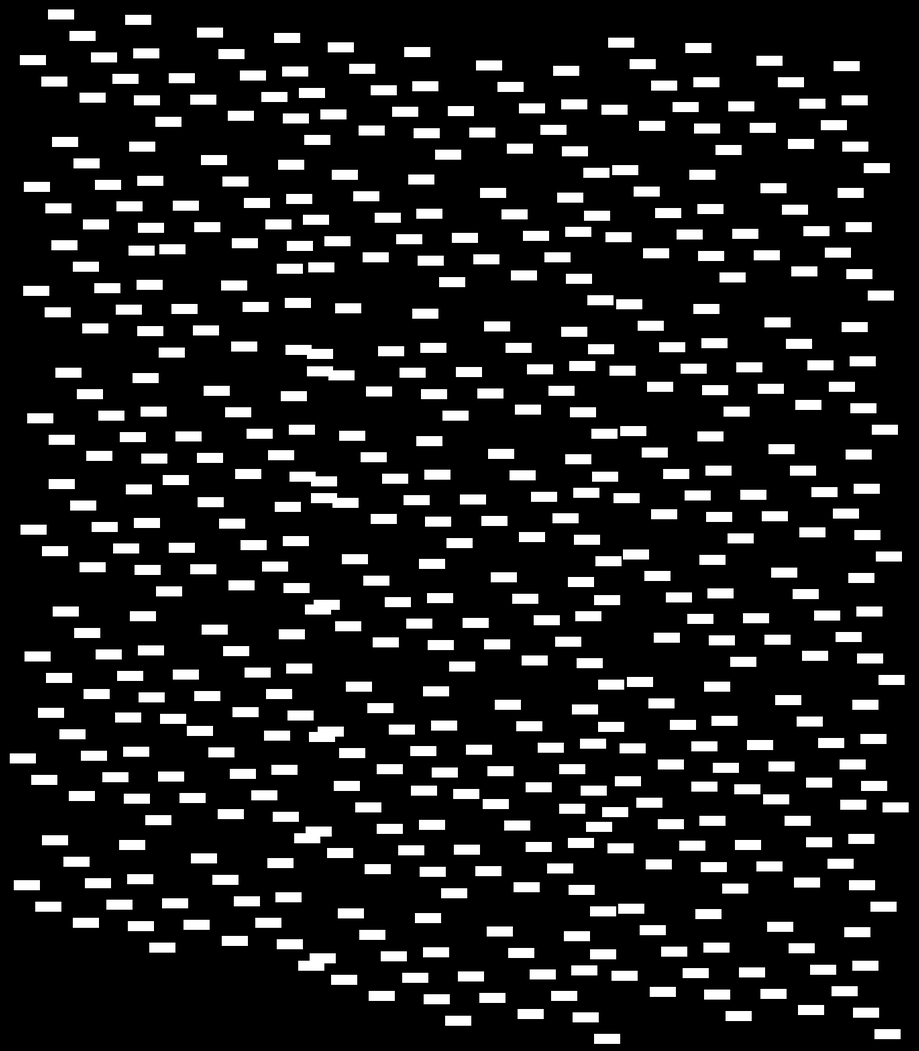
Accounts im Tier Model



Vorteile

- In jedem Unternehmen möglich
- Limitierung des Schadens
- Verhindert Vollübername
- Einfachere Segregation of Duty (Funktionstrennung)
- Einfache Implementierung
- Erweiterungsmöglichkeiten
  (4-Tier, 6-Plane, Entra ID)

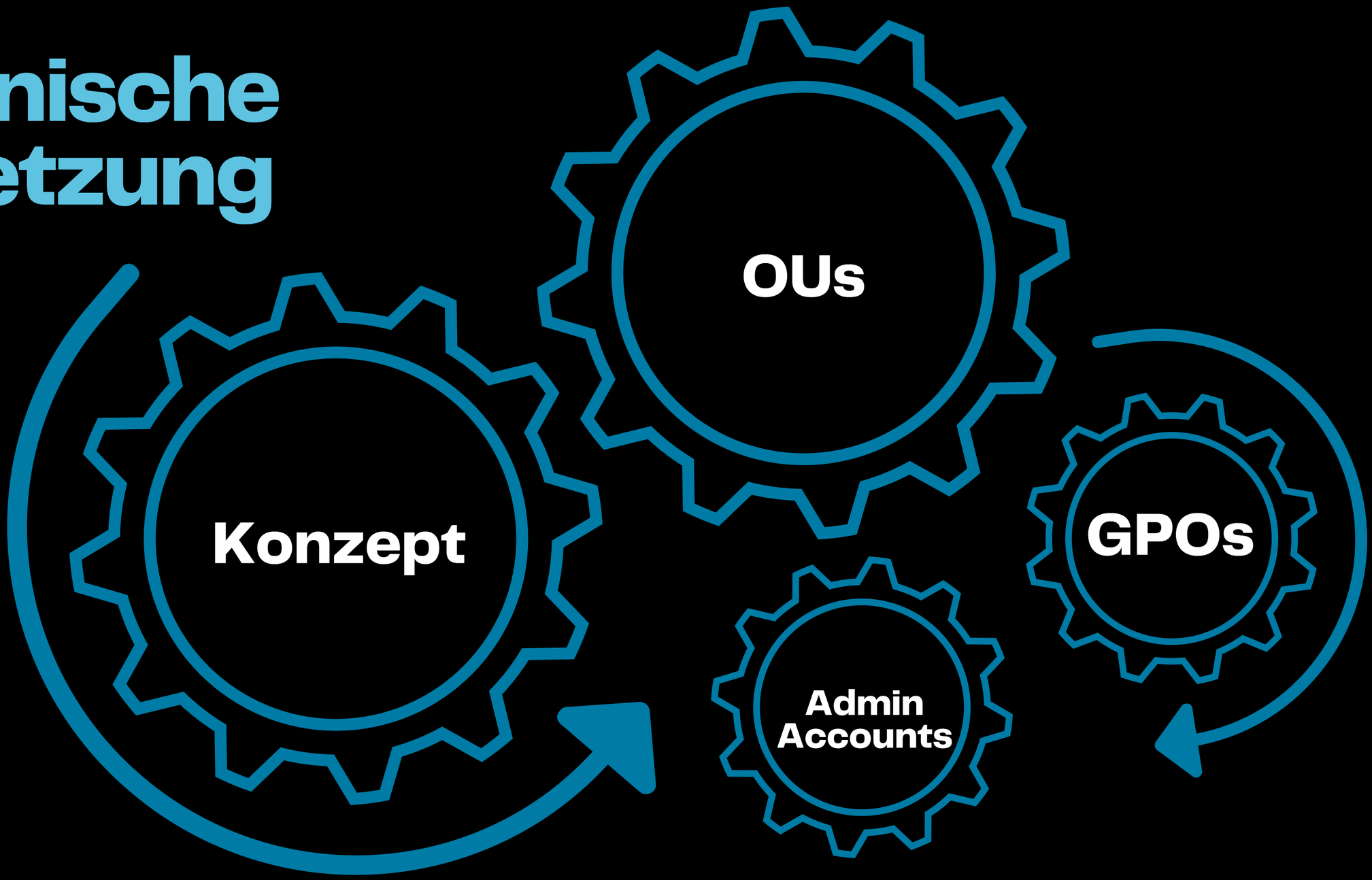




Nebenwirkungen

- Konzept und Namenskonvention notwendig
- Umdenken erforderlich
  (Überadmins werden Teiladmins)
- Mehr Accounts für den Admin
- Ggf. mehrere Clients für den Admin (z.B. Notebook + PAW)

Technische Umsetzung



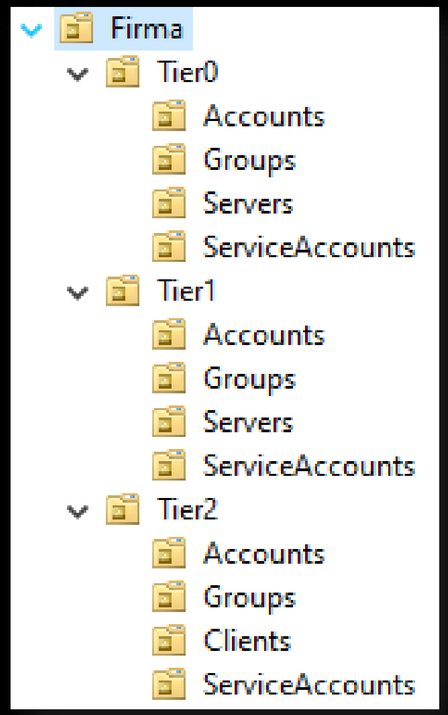
Umsetzung

Konzept
(inkl. Namenskonvention)

Namenskonvention	
1.1	**Server**
1.1.1	Schema
1.1.2	Details
1.2	**Clients**
1.2.1	Schema
1.2.2	Details
1.3	**Drucker**
1.3.1	Schema
1.3.2	Details
1.4	**Benutzer**
1.4.1	Schema
1.4.2	Details
1.5	**Administratorenkonten OnPrem**
1.5.1	Schema
1.5.2	Details
1.6	**Administratorenkonten Cloud**
1.6.1	Schema
1.6.2	Details
1.7	**Task & Service Accounts**
1.7.1	Dokumentationspflicht
1.7.2	Schema
1.7.3	Details
1.8	**Group Managed Service Accounts**
1.8.1	Dokumentationspflicht
1.8.2	Schema
1.8.3	Details
1.9	**Gruppen**
1.9.1	Dokumentationspflicht
1.9.2	Schema

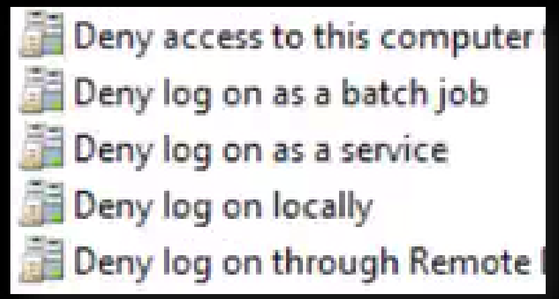
+

OU-Struktur



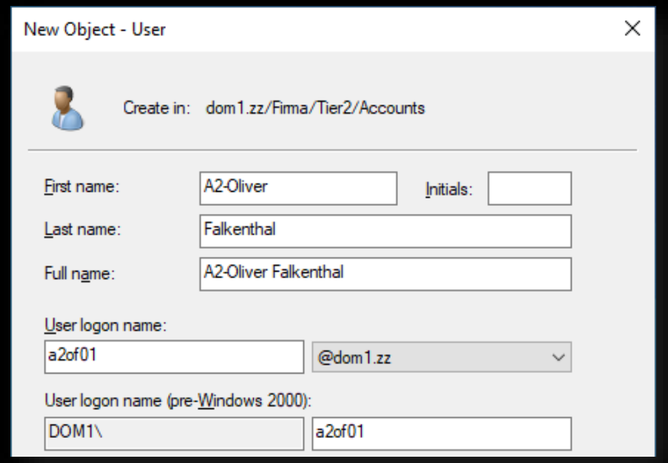
+

GPOs



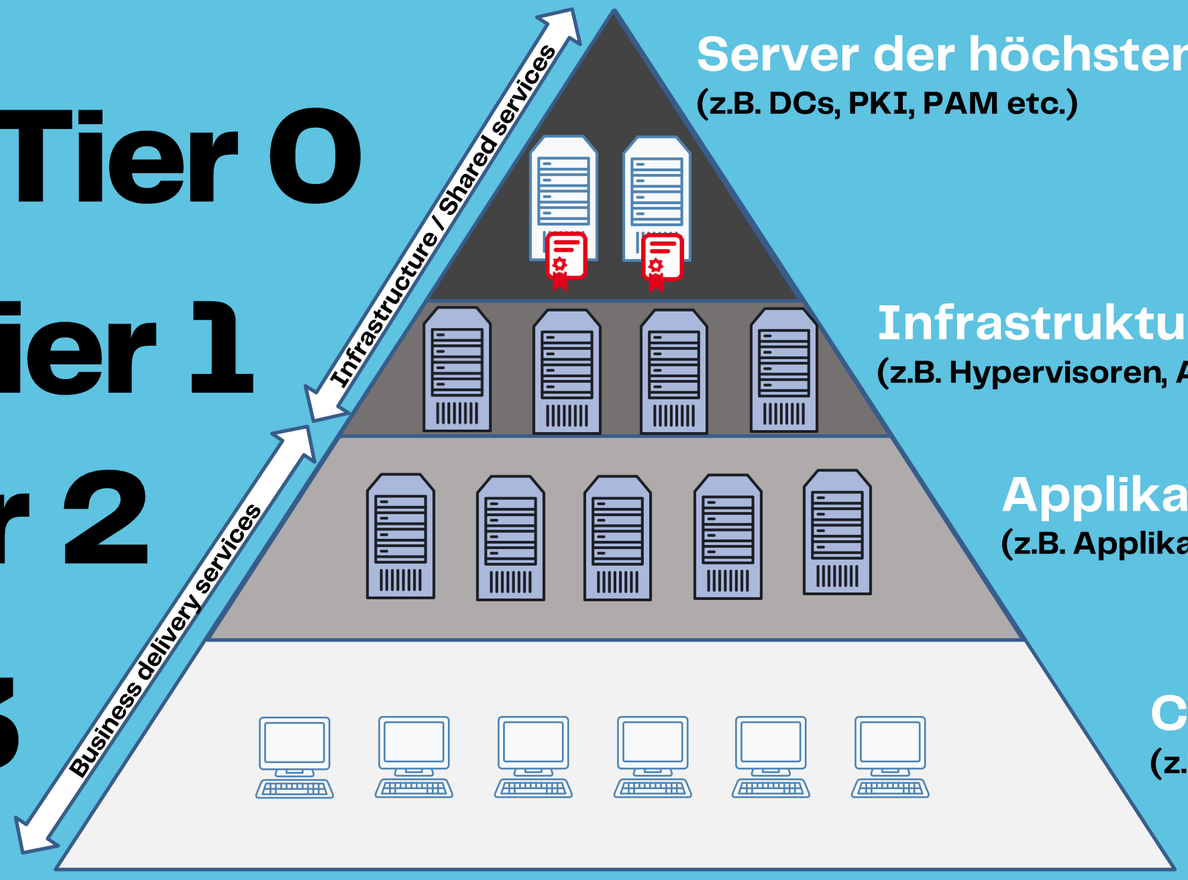
+

Admin-Konten anlegen



Erweiterungen des Tier-Modells

4-Tier Model



Tier 0

Server der höchsten Stufe
(z.B. DCs, PKI, PAM etc.)

Tier 1

Infrastrukturserver
(z.B. Hypervisoren, AV, SIEM, ILO etc.)

Tier 2

Applikationsserver
(z.B. Applikationsserver, Datenbankserver, Mailserver etc.)

Tier 3

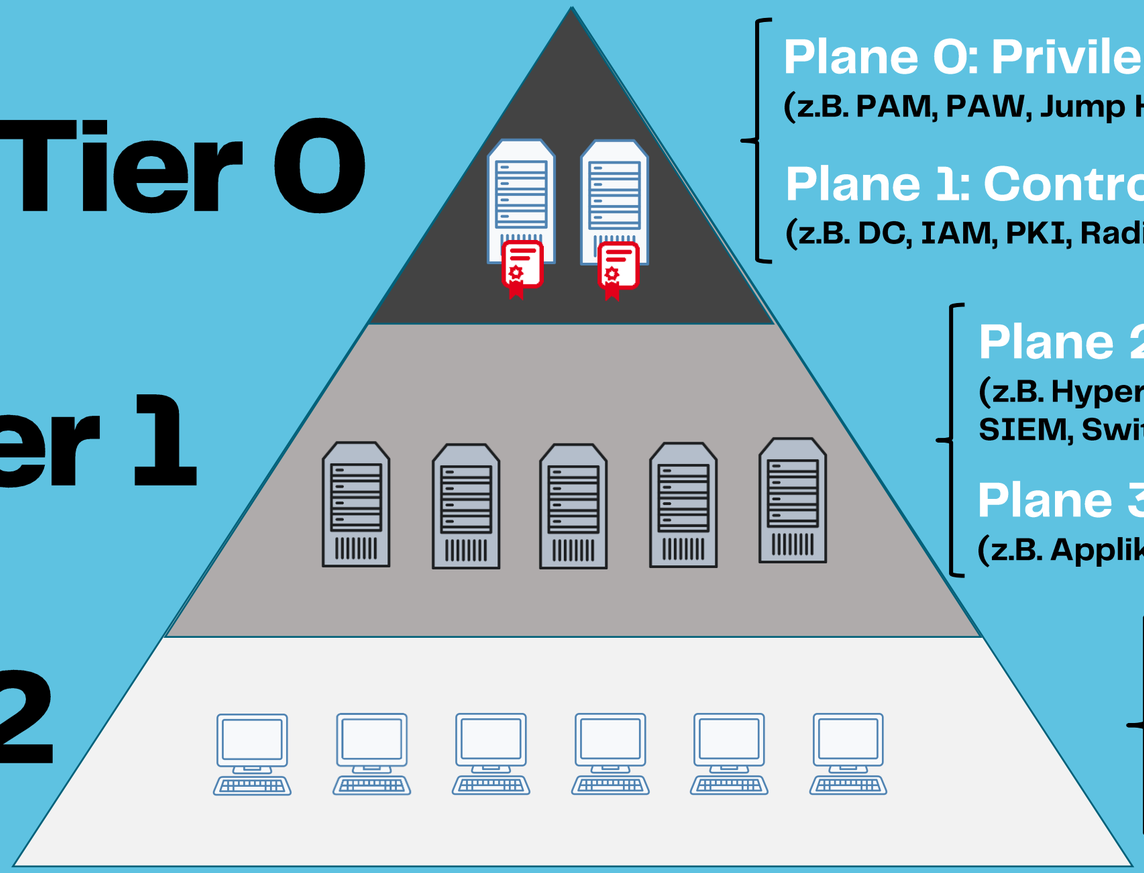
Clients
(z.B. Notebooks, Desktops, VDI)

6-Plane Model

Tier 0

Tier 1

Tier 2



Plane 0: Privileged Access Plane
(z.B. PAM, PAW, Jump Hosts etc.)

Plane 1: Control Plane
(z.B. DC, IAM, PKI, Radius, AD-DNS etc.)

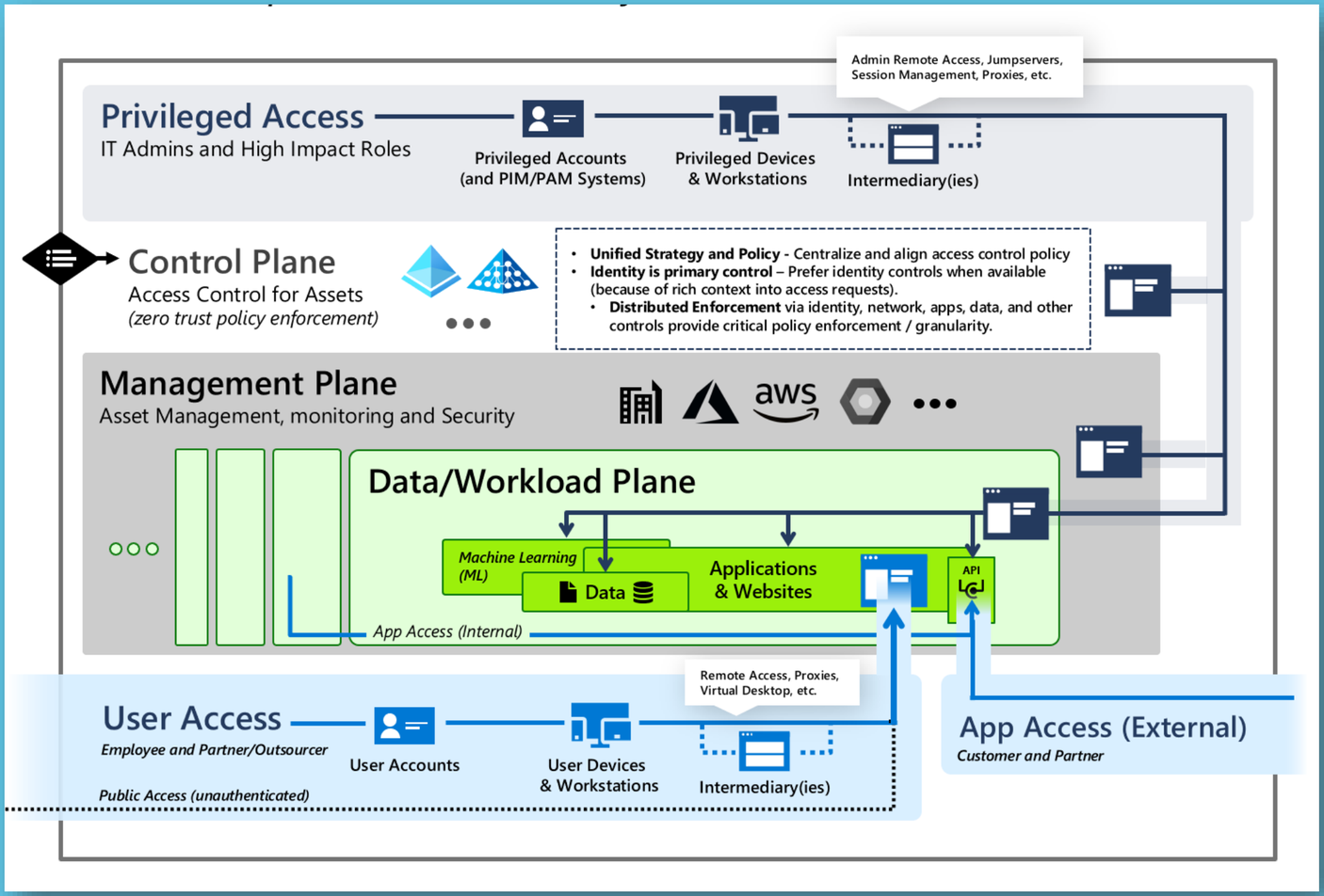
Plane 2: Management Plane
(z.B. Hypervisoren, DCHP, DNS, Proxy, Backup, ILO, SIEM, Switches, Firewalls, ILO etc.)

Plane 3: Data Workload Plane
(z.B. Applikationsserver, Datenbankserver, Mailserver etc.)

Plane 4: User Access Plane
(z.B. Notebooks, Desktops, VDI etc.)

Plane 5: App Access Plane
(z.B. externe APIs)

6-Plane Model



https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-access-model

Plane 0: Privileged Access Plane
(z.B. PAM, PAW, Jump Hosts etc.)

Plane 1: Control Plane
(z.B. DC, IAM, PKI, Radius, AD-DNS etc.)

Plane 2: Management Plane
(z.B. Hypervisoren, DCHP, DNS, Proxy, Backup, ILO, SIEM, Switches, Firewalls, ILO etc.)

Plane 3: Data Workload Plane
(z.B. Applikationsserver, Datenbankserver, Mailserver etc.)

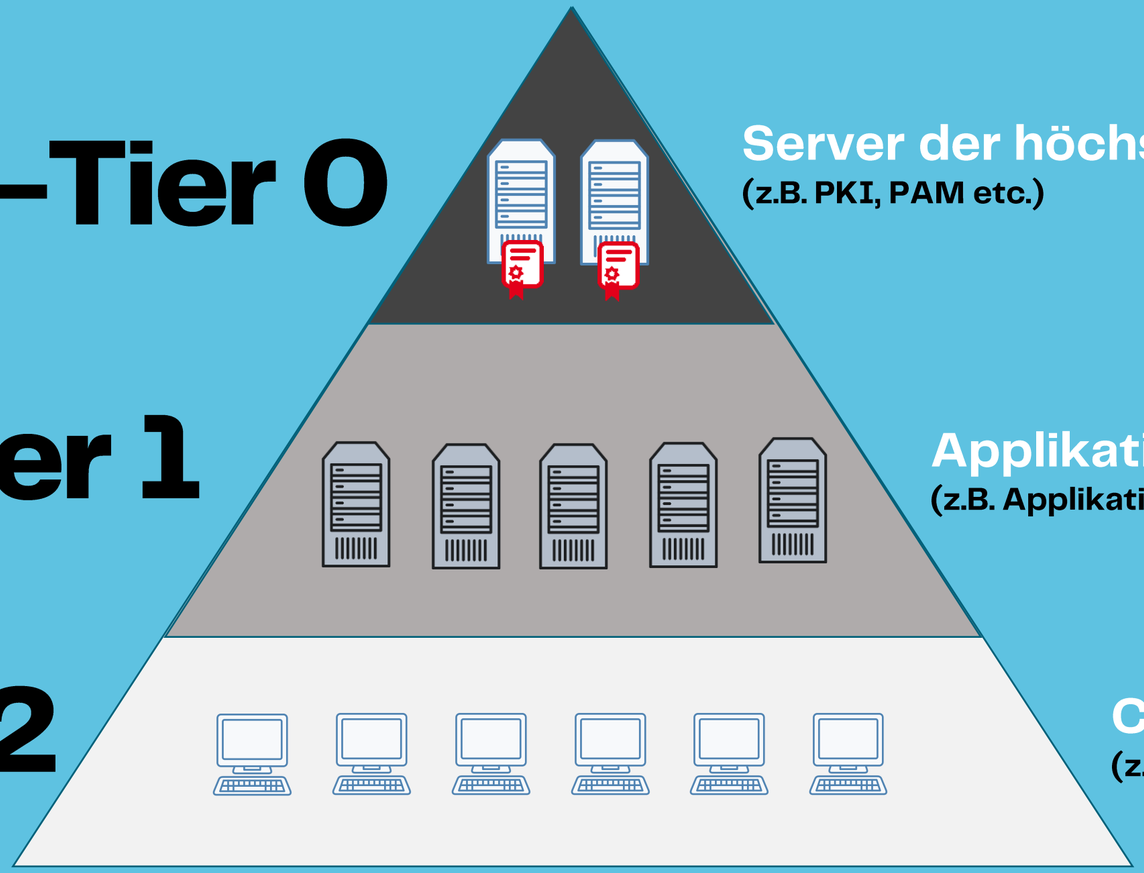
Plane 4: User Access Plane
(z.B. Notebooks, Desktops, VDI etc.)

Plane 5: App Access Plane
(z.B. externe APIs)

Tier-Modell in der MS Azure Cloud

Tier Model in Azure (IaaS)

IaaS-Tier 0



Server der höchsten Stufe
(z.B. PKI, PAM etc.)

IaaS-Tier 1

Applikationsserver
(z.B. Applikationsserver, Datenbankserver, Mailserver etc.)

IaaS-Tier 2

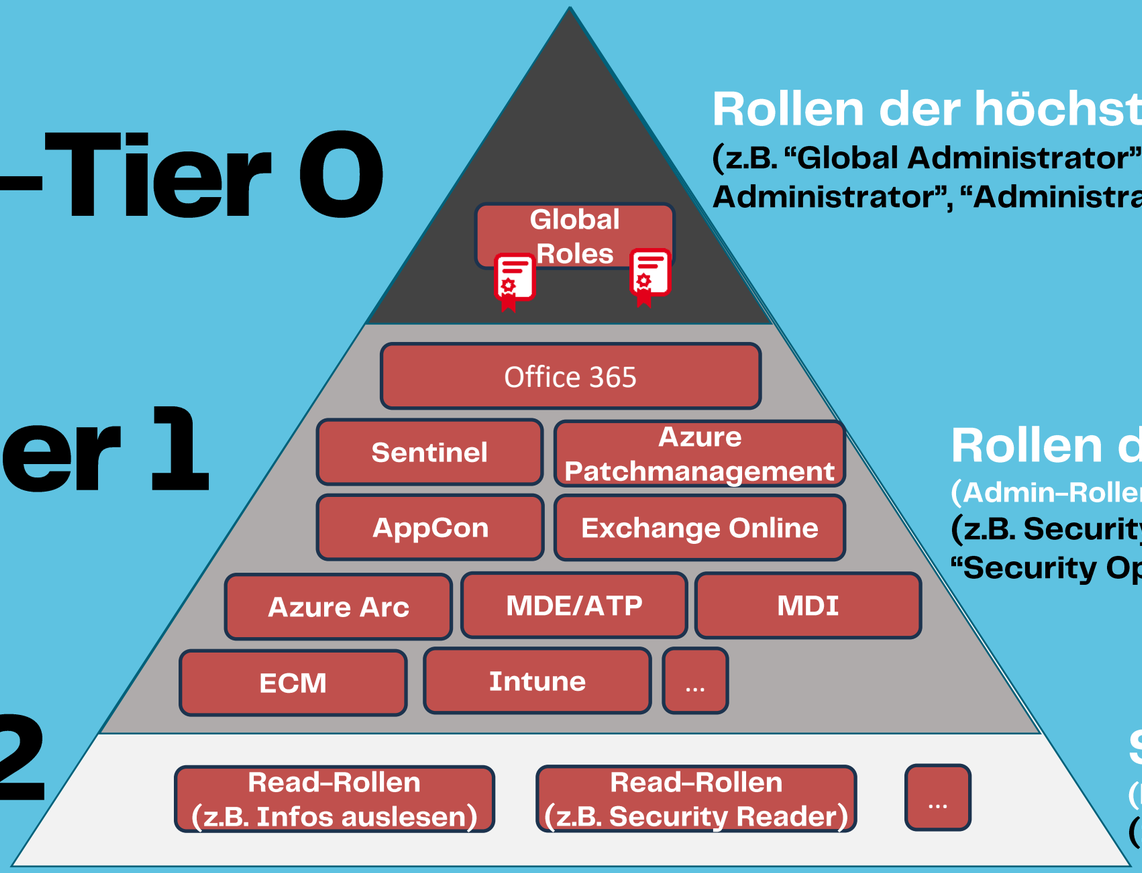
Clients
(z.B. VDI)

Tier Model in Azure (SaaS)

SaaS-Tier 0

SaaS-Tier 1

SaaS-Tier 2



Rollen der höchsten Stufe
(z.B. "Global Administrator", "Privileged Role Administrator", "Billing Administrator", "Administrator für die Berechtigungsverwaltung")

Rollen der Sicherheitsdienste
(Admin-Rollen)
(z.B. Security Admin Roles, "Global Reader", "Security Operator")

Sonstige Rollen
(keine Admin-Rollen)
(z.B. Read Roles oder "Mitwirkende")

Rollen siehe hier: https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference
(privileged = mind. Tier 1)

CCVOSSEL

We ♥ being a hacker's nightmare

CCVOSSEL

Ihre Ansprechpartner

Dipl.-Ing.

Carsten Vossel

CEO

c.vossel@ccvossel.de
+49 30 60 98 40 910
ccvossel.de

Ihr Ansprechpartner

Dipl.-Inform. Dipl.-Wi.-Ing.

Oliver Falkenthal

Lead Defensive Security (BLUE)

o.falkenthal@ccvossel.de
+49 30 60 98 409 33
ccvossel.de