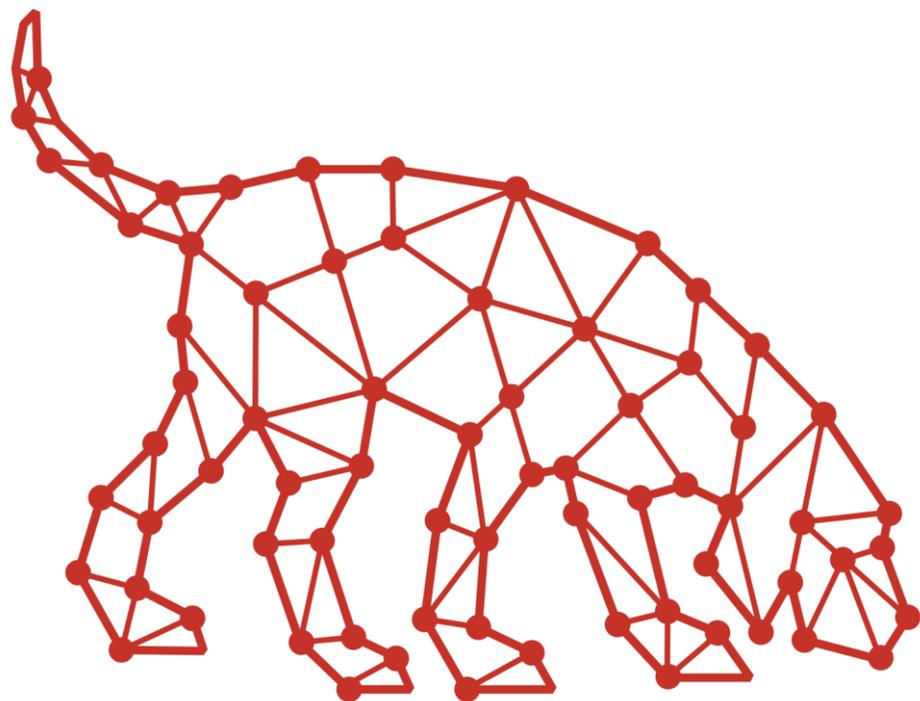




Who Let the Hounds Out

Fehler in der Implementierung vom Active Directory Tier Modell



VidraSec - Schwachstellen finden, bevor Angreifer sie ausnutzen



Um was geht es heute?

Was ist Active
Directory Tiering



Warum Tiering?



Fehler bei der
Implementierung



Kurze Erklärung zum Anfang

- Neuer ist das **Enterprise Access Model**
- Kurzfassung:
 - Enterprise Access Model ist eine Weiterentwicklung und basiert immer noch auf dem Tier Modell
 - Schwerer zu verstehen
- Mehr dazu am Ende



Martin Grottenthaler

Founder & IT Security Consultant
VidraSec 🦫

✉ martin@vidrasec.com

🌐 <https://www.vidrasec.com>

🔗 <https://www.linkedin.com/in/mgrottenthaler/>



Was ist VidraSec 🦫 ?

Penetrationstests und IT-Security Consulting

Schwachstellen finden, bevor Angreifer sie ausnutzen

- 🚨 Fokus auf echte Probleme
- 🎯 Umsetzbare Lösungen liefern
- 🌱 Sinnvolle & effiziente Projekte durchführen



Los geht's!

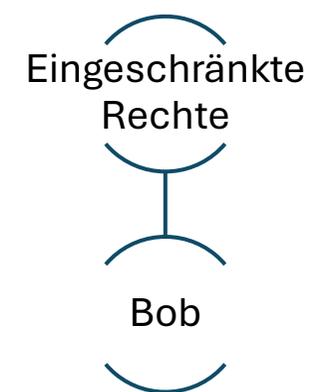
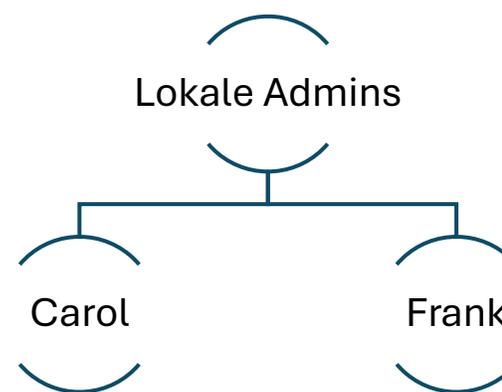
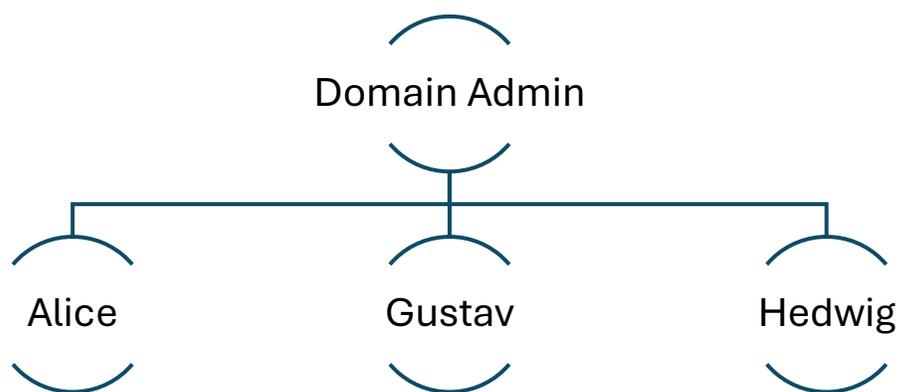


BusyBeaverGroup

Person	Funktion
Alice	Head of IT / Domain Admin
Bob	Billing
Carol	CEO
Frank	CFO
Gustav	General Admin
Hedwig	Helpdesk



Ausgangslage





Problem?



ass.jpg.exe



Was passiert?

Wana Decrypt0r 2.0

Ooops, your files have been encrypted! English

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

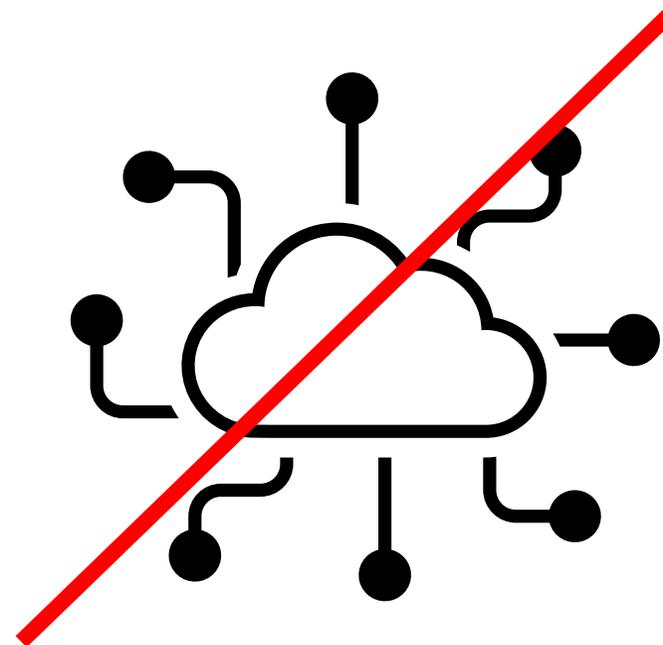
Send \$300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw Copy

Check Payment Decrypt



Nie mit dem Domain Admin

- Im Internet surfen
- Mails lesen
- usw.



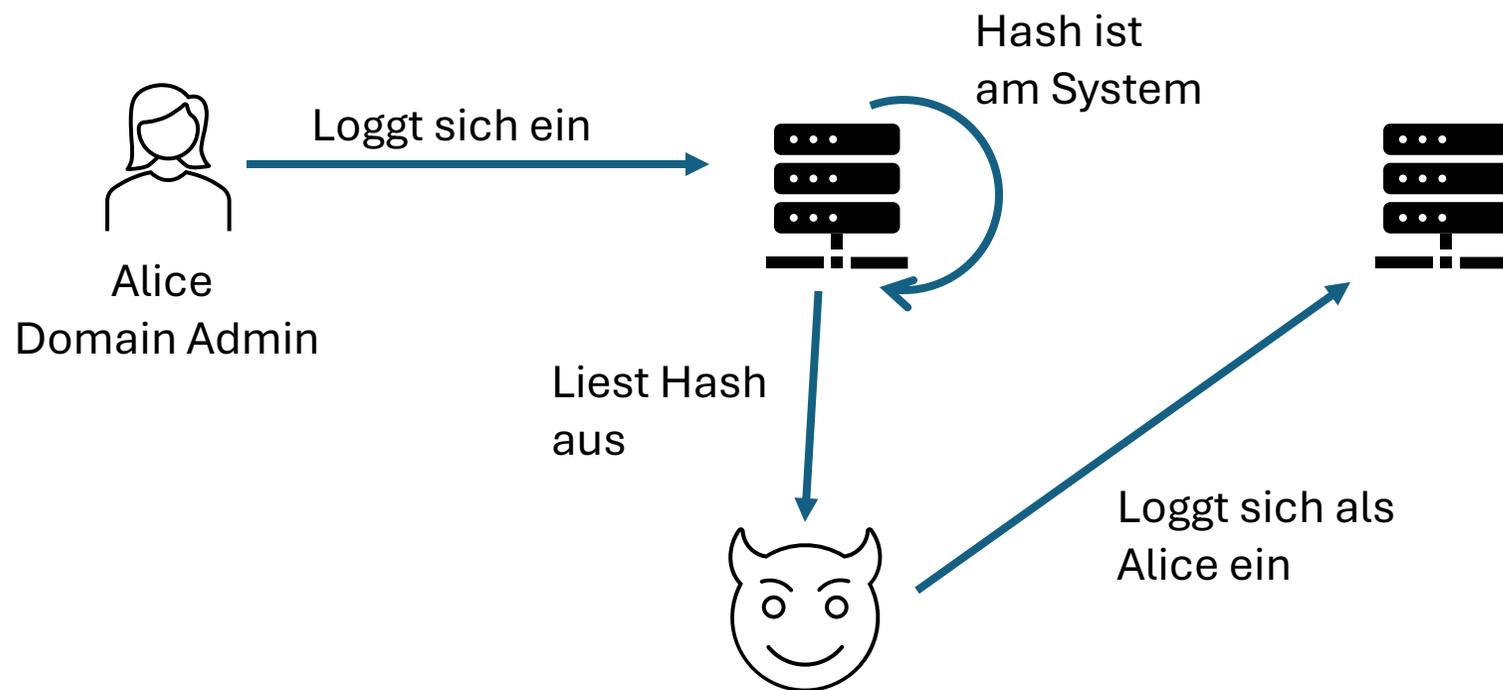


Was darf ein Domain Admin machen?

1. Domain Admin Tätigkeiten
2. DOMAIN ADMIN TÄTIGKEITEN
3. That's it!

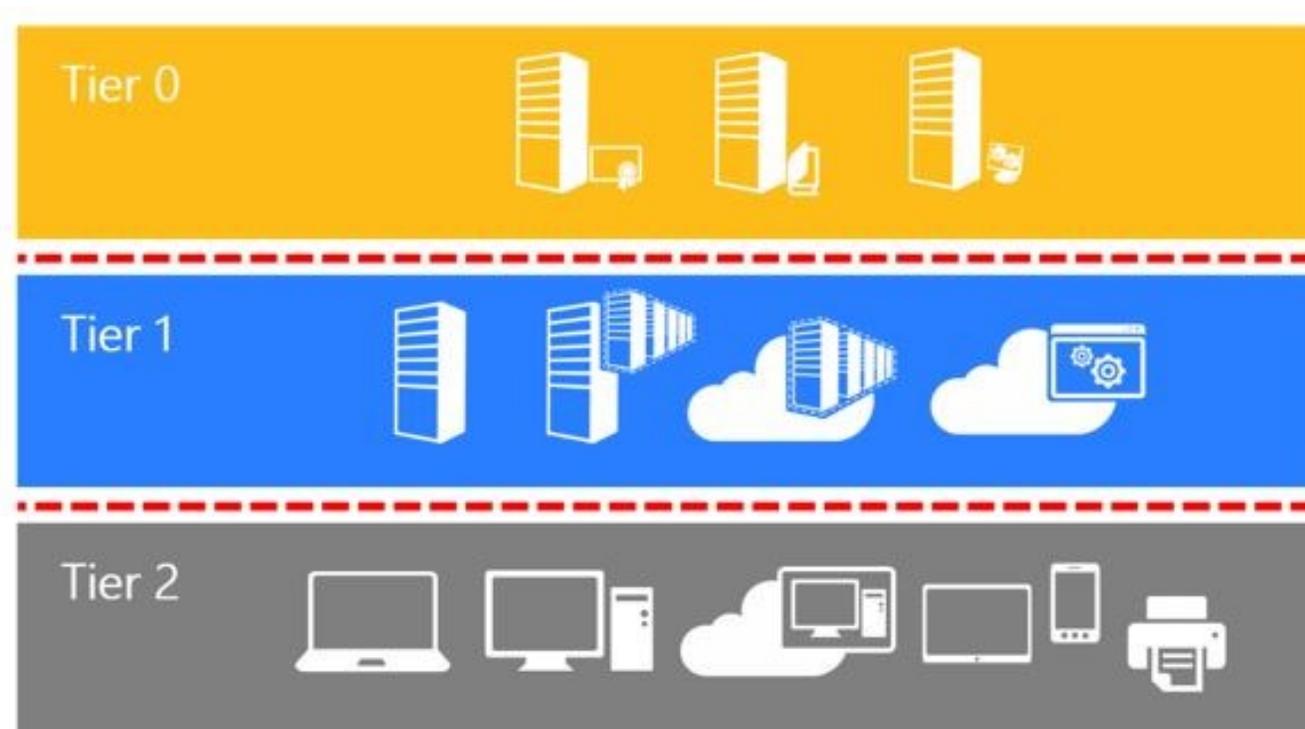


Weiteres Problem – Pass the Hash





Active Directory Tier Model



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

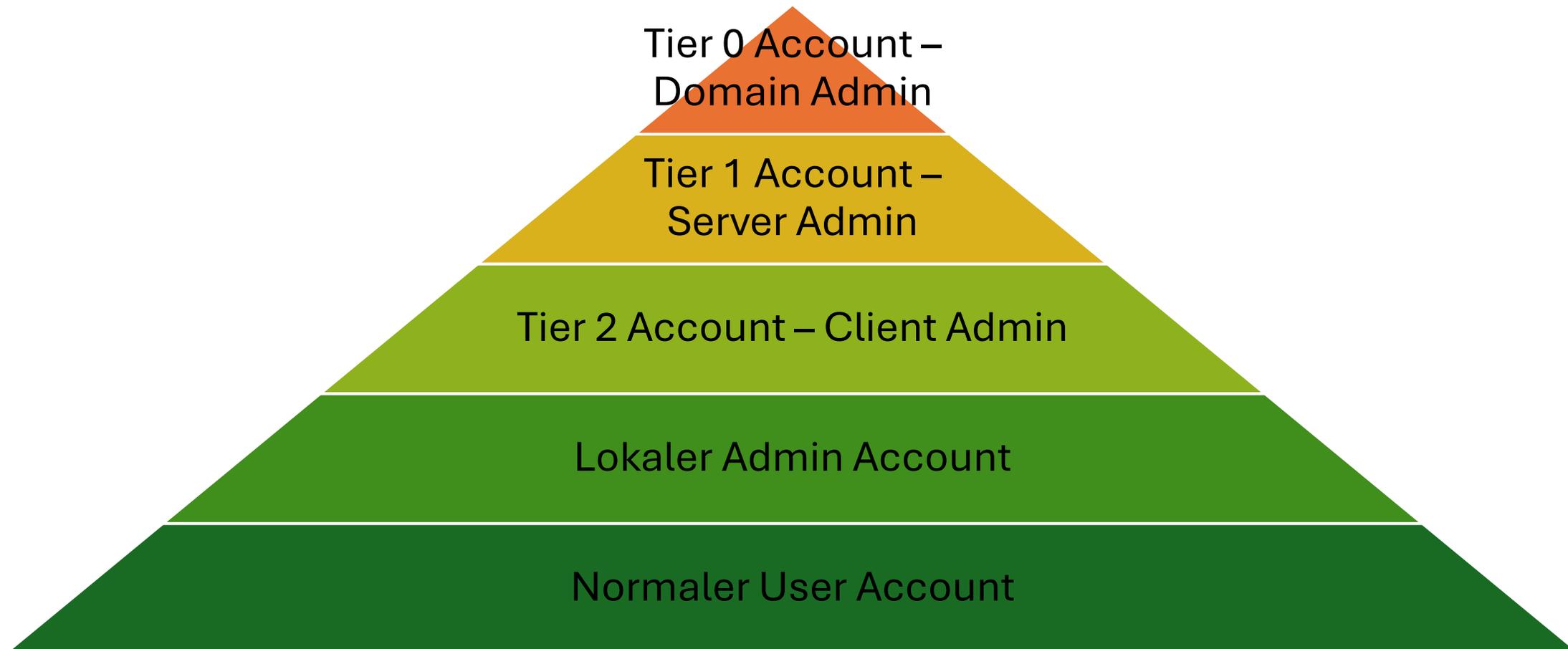


Wir brauchen viele neue Accounts

Das wird ein bisschen aufwändig



Beispiel: Alice – Domain Admin



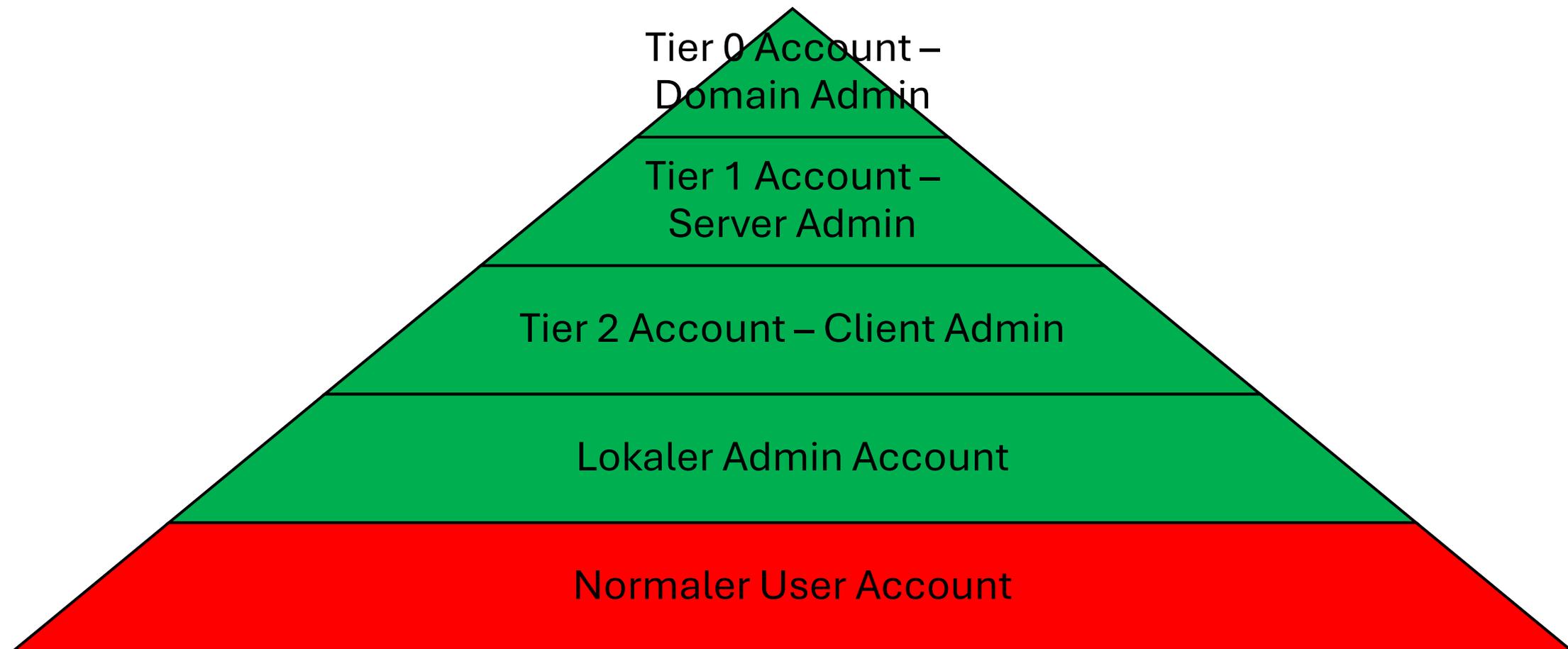


Nochmal unser Problem





Auswirkung



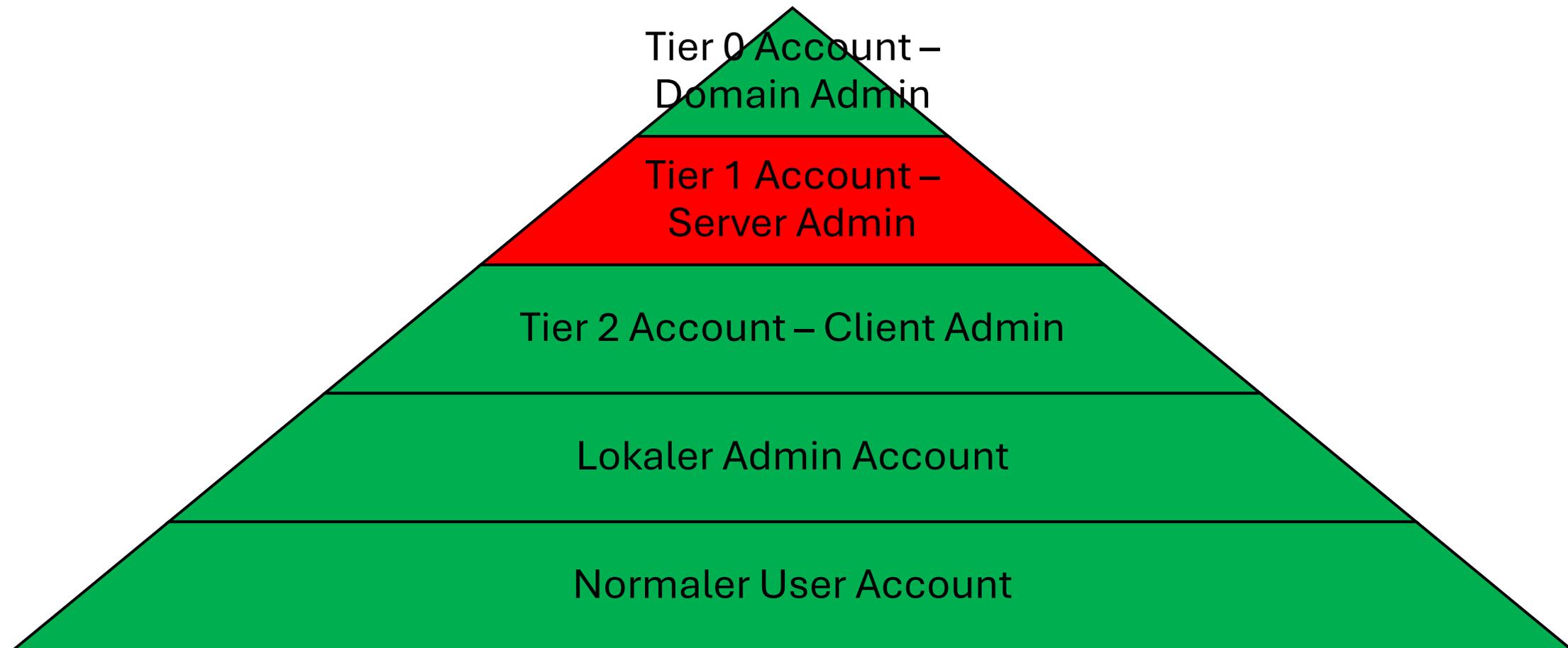


Anderes Problem





Auswirkung





Ein paar Anmerkungen

- LAPS-Passwort auslesen besser als Client Admin
- **Wichtig:** wo gebe ich mein Admin Passwort ein?
 - Jump Server
 - Privileged Access Workstations (PAW)
 - Privileged Access Management (PAM)
- Wo speichere ich meine Passwörter?



Fragen bis hierhin?



Der nächste Part baut darauf auf



Fehler bei Umsetzung

Brüche im Tier Modell



Tiering ist nicht immer genug

Hedwig ist **Helpdesk**

Helpdesk ist **Tier 2 (Client Admins)**

Helpdesk darf außerdem
Passwörter zurücksetzen

Fragen:

- Darf Hedwig das Passwort eines Domain Admins zurücksetzen?
- Darf Hedwig das Passwort von Carol (CEO) zurücksetzen?
- Darf Hedwig einen DA Client administrieren?



Lösung

1. Keine Rechte auf Konten in höheren Tiers

z.B. Domain Admin Konten dürfen nur von Domain Admins bearbeitet werden (was ist mit normalen Konten von DAs)

2. Gewisse Personen sind wichtig fürs Business, auch wenn sie keine speziellen Rechte im AD haben

Z.B. CEO, CFO, ... Passwörter nur von Domain Admins rücksetzbar machen

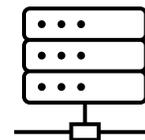


Terminalserver sind ...?

(Normale User loggen sich ein, um einen virtuellen Desktop zu bekommen)



Clients
Tier 2



Server
Tier 1



Terminalserver sind Clients!

Warum?

- Dort loggen sich normale User ein
- Normale User sind böse!

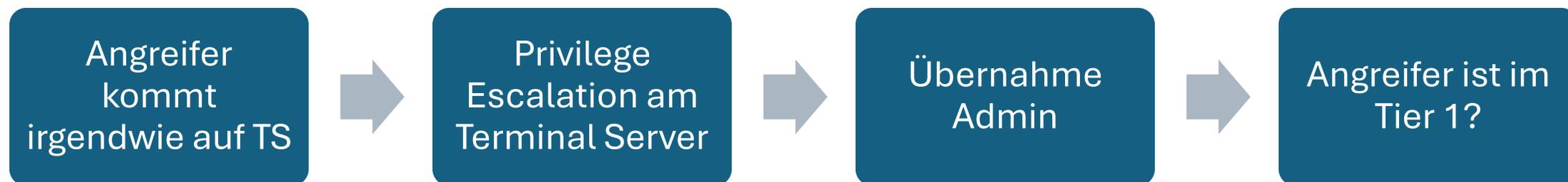
Daher

- Terminalserver → Tier 2

Trifft auch auf Citrix oä. zu



Angriffsweg





Tier 0 muss abgesichert werden

- Tier 1 Admins dürfen keine Schreibrechte auf Tier 0 Gruppen haben
- Tier 1 Admins dürfen keine Group Policies die auf Domain Admins oder Domain Controller greifen bearbeiten dürfen
- ... usw. oft sehr individuell



Exchange by default mit hohen Rechten

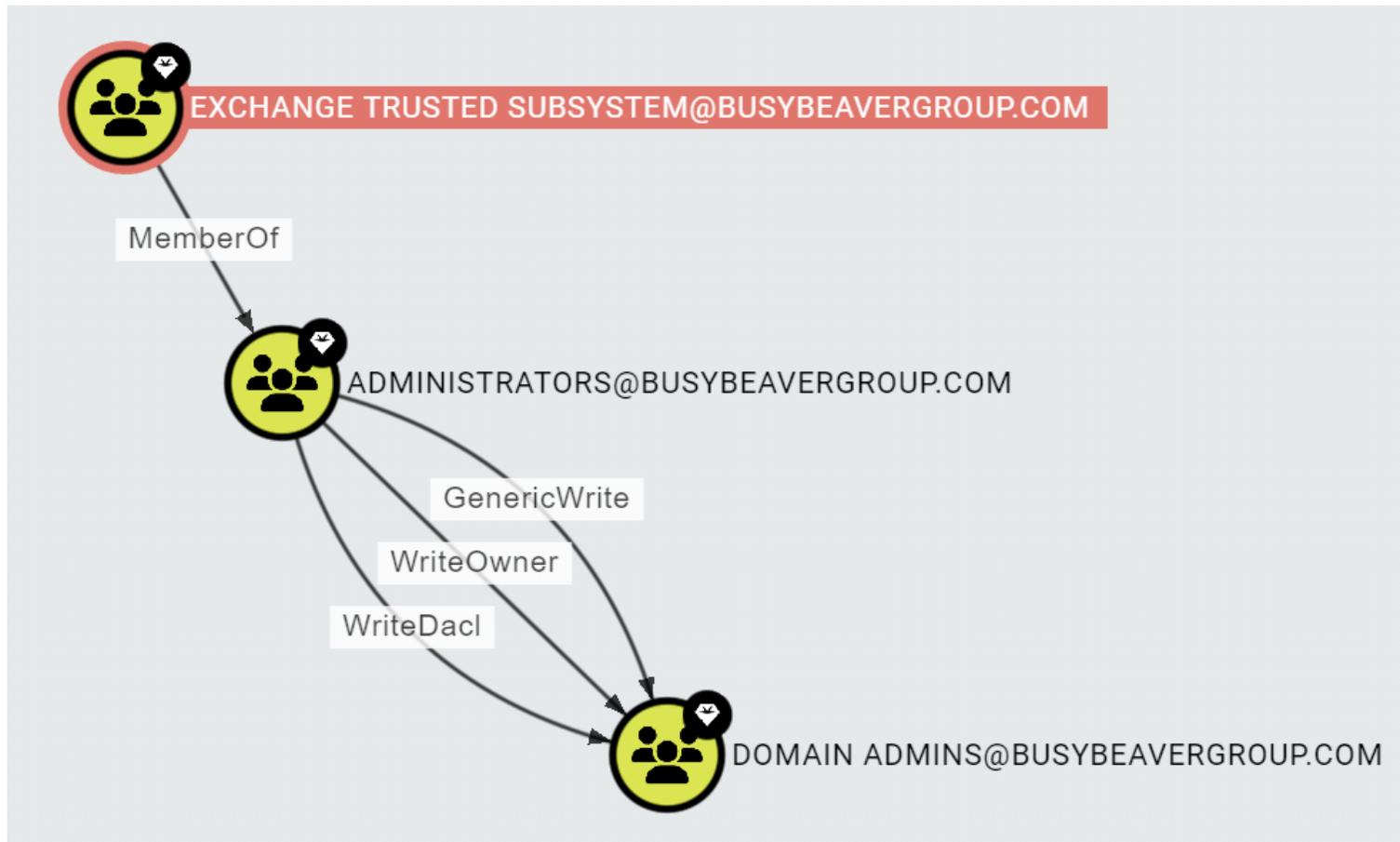
- Exchange by default mit Tier 0 Rechten
- Aber eigentlich ein Tier 1 System

- Behebung: Exchange Split Permissions

<https://learn.microsoft.com/en-us/exchange/permissions/split-permissions/configure-exchange-for-split-permissions>



Exchange by default mit hohen Rechten





Tier 0 ist nicht nur der Domain Controller

- Z.B. auch der Active Directory Certificate Service (ADCS)
- Warum? Der stellt Zertifikate für Login aus

Die TierZeroTable checken:

<https://specterops.github.io/TierZeroTable/>



Dasselbe Passwort

User in verschiedenen Tiers

```
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:b2fec3265736640ff52c20311e05253e:::  
service-user:1125:aad3b435b51404eeaad3b435b51404ee:633511530c37f48ea04b238466b6e995:::  
alice:1117:aad3b435b51404eeaad3b435b51404ee:3e24dcead23468ce597d6883c576f657:::  
aliceT0:1127:aad3b435b51404eeaad3b435b51404ee:3e24dcead23468ce597d6883c576f657:::  
aliceT1:1128:aad3b435b51404eeaad3b435b51404ee:3e24dcead23468ce597d6883c576f657:::
```



Dasselbe Passwort

Lokaler Admin von verschiedenen Maschinen (in verschiedenen Tiers)

→ Pass-the-Hash

Lösung: LAPS

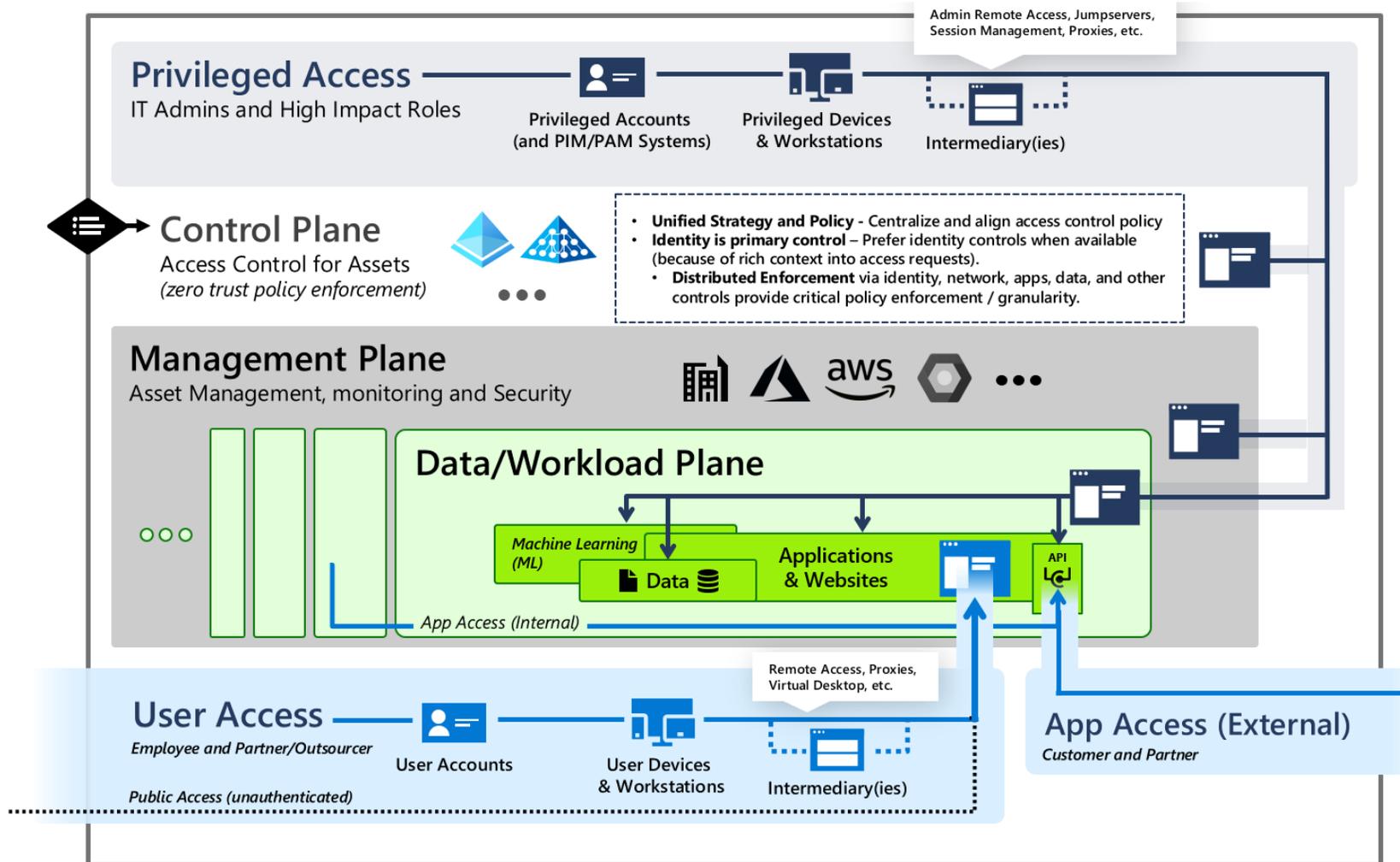


Ausblick

Was gibt es noch?



Enterprise Access Model



Privileged Access

Enables IT administrators and other high impact roles to access sensitive systems and data. *Stronger security for higher impact accounts*

Control and Management Planes

Provide unified access and management for workloads and assets (*and provide attackers shortcut for illicit objectives*)

Data/Workloads

Create and store business value in

- Business processes (in apps/workloads)
- Intellectual property (in data and apps)

User and App Access

How employees, partners, and customers access these resources



Weiteres

- Die Anzahl der Stufen (Tiers) ist unbegrenzt
- Aber: zu viel Komplexität ist auch kontraproduktiv
 - Dann brauch ich kein AD mehr



Andere Modelle

- Red Forest und Shadow Forest
- Extrem komplex zu implementieren
- Kenne ich nur aus der Theorie → hier gerne eure Erfahrungen

- Mittlerweile nicht mehr empfohlen!



Zusammenfassung

- Konten mit vielen Rechten sind gefährlich
- Rechte müssen aufgeteilt werden
- Vertikale Privilege Escalation () darf nicht möglich sein

 Prüfen! Sonst bringt es nichts.

 Meldet euch da gerne!



Danke!

Martin Grottenthaler
Founder & IT Security Consultant
VidraSec 🦫

✉ martin@vidrasec.com

🌐 <https://www.vidrasec.com>

🔗 <https://www.linkedin.com/in/mgrottenthaler/>