T.I.S.P./T.P.S.S.E. Community Meeting 2026

Berlin, 10. - 11.11.2026

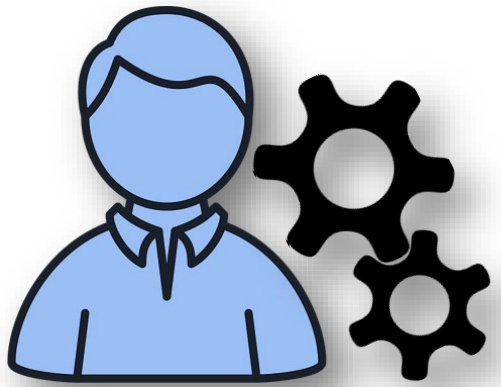
Alt, aber immer noch kritisch! Strategien zum Umgang mit Service Accounts im KRITIS-Umfeld.

Oliver Falkenthal, CCVOSSEL

Vertraulichkeit: Intern

Ein zentraler Schlüssel

für großflächige Angriffe auf Windows-Infrastrukturen sind…



Service Accounts
&
Task Accounts

Vertraulichkeit: Öffentlich

Angreifer suchen Zugänge von Konten, die folgendes bieten…



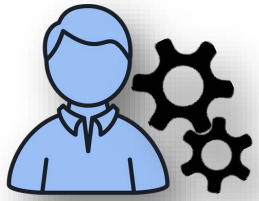
Admin Accounts

Service Accounts

Service Accounts bieten eine **viel größere Angriffsfläche** als Admin-Accounts!

Vertraulichkeit: Öffentlich

Das größte Problem…



Service Accounts
&
Task Accounts

direkt auslesbare Kennwörter

Kennwörter mit Adminrechten auslesbar

- gespeichert in der **Registry**
- **Adminrechte** oder **Debug-Privilegien** können **unmittelbar entschlüsseln**!
  (z.B. mittels „Mimikatz“ → in Klartext!)

Vertraulichkeit: Öffentlich

Das Problem

Mimikatz im Einsatz

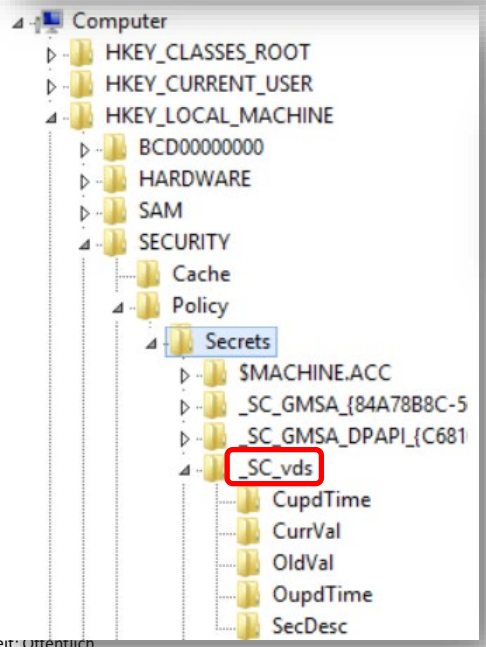


Services (Local)

Virtual Disk

Stop the service
Restart the service

Name	Description	Status	Startup Type	Log On As
UPnP Device H...	Allows UPn...		Disabled	Local Service
User Access Lo...	This service ...	Running	Automatic (D...	Local System
User Profile Ser...	This service ...	Running	Automatic	Local System
Virtual Disk	Provides m...	Running	Manual	ServiceAccount01@sec.demo.local



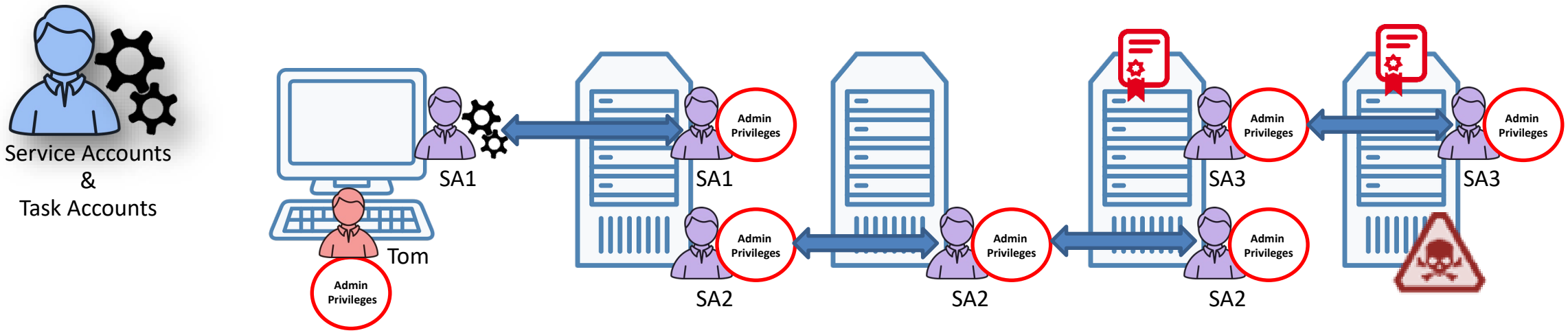

```
mimikatz.exe "privilege::debug" "token::elevate" "lsadump::secrets"
```

```
Secret  :  _SC_vds / service 'vds' with username : ServiceAccount01@sec.demo.local
cur/text: SuperSecret1000
```

Klartext-Kennwort

Auch Sicherheitsfeatures wie „**Credential Guard**“ schützen hiervor nicht!

Lateral Movement



„Lateral Movement“ über mehrere Zwischensysteme zum Zielsystem

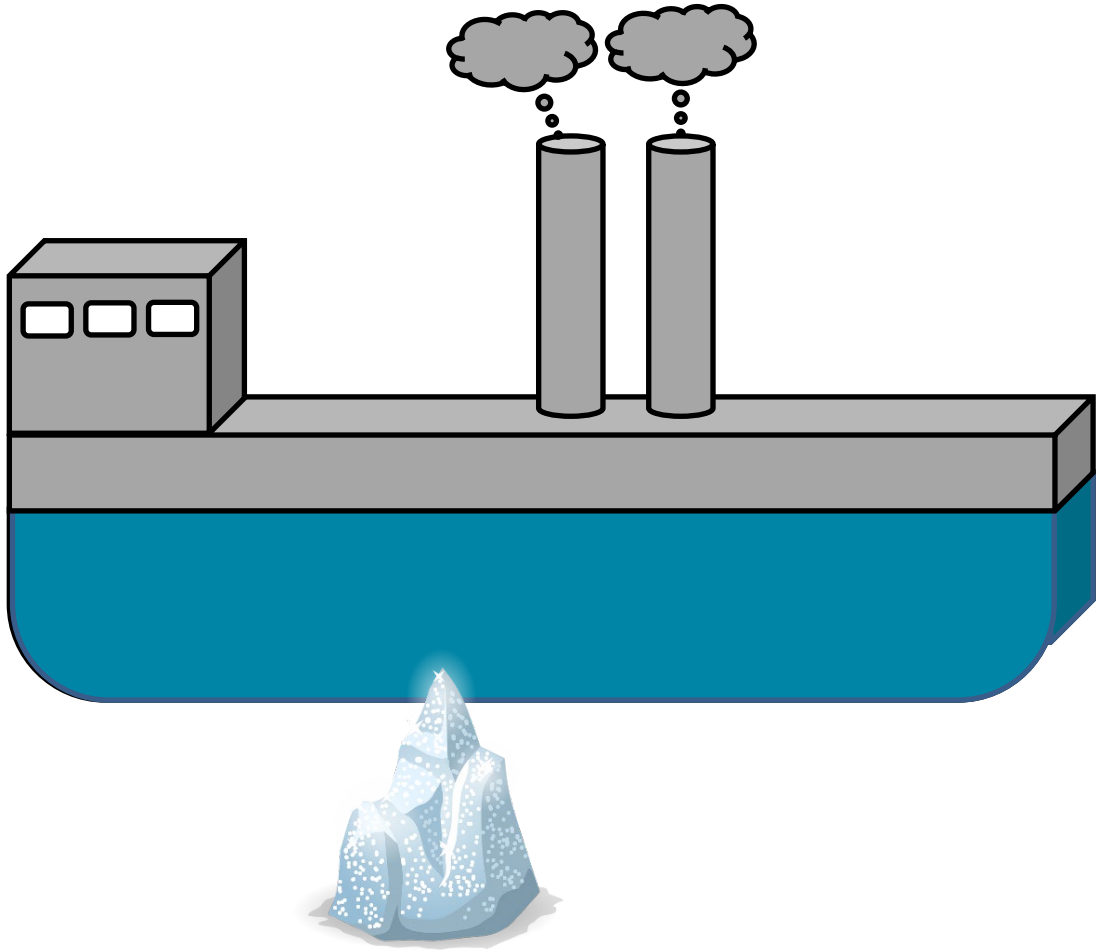
Admin-Rechte führen zur Aufdeckung von Passwörtern anderer Konten

Ziel

Zentrale Infrastruktursysteme zu kompromittieren, um die gesamte IT-Infrastruktur zu übernehmen.

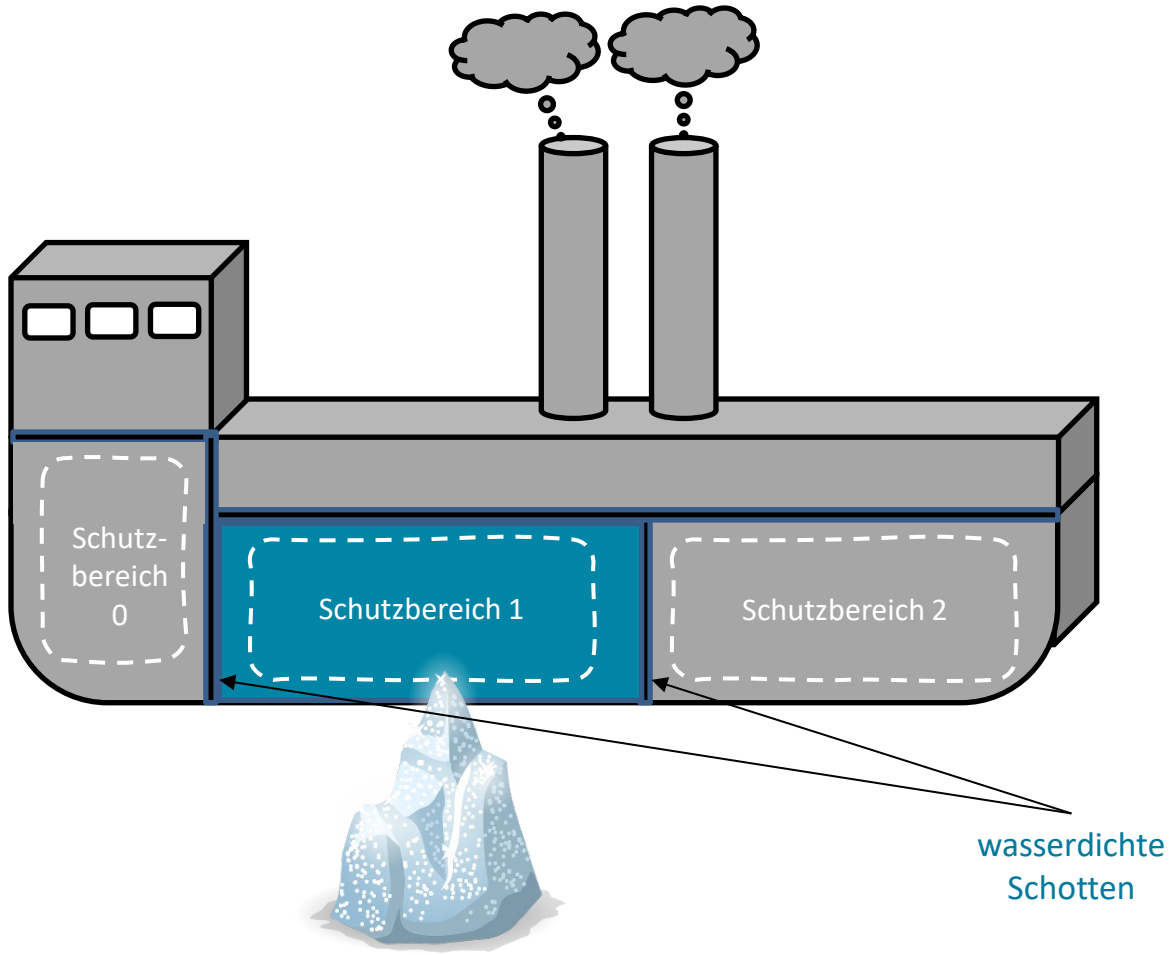
Vertraulichkeit: Öffentlich

Wenn Informatiker Schiffe zeichnen…



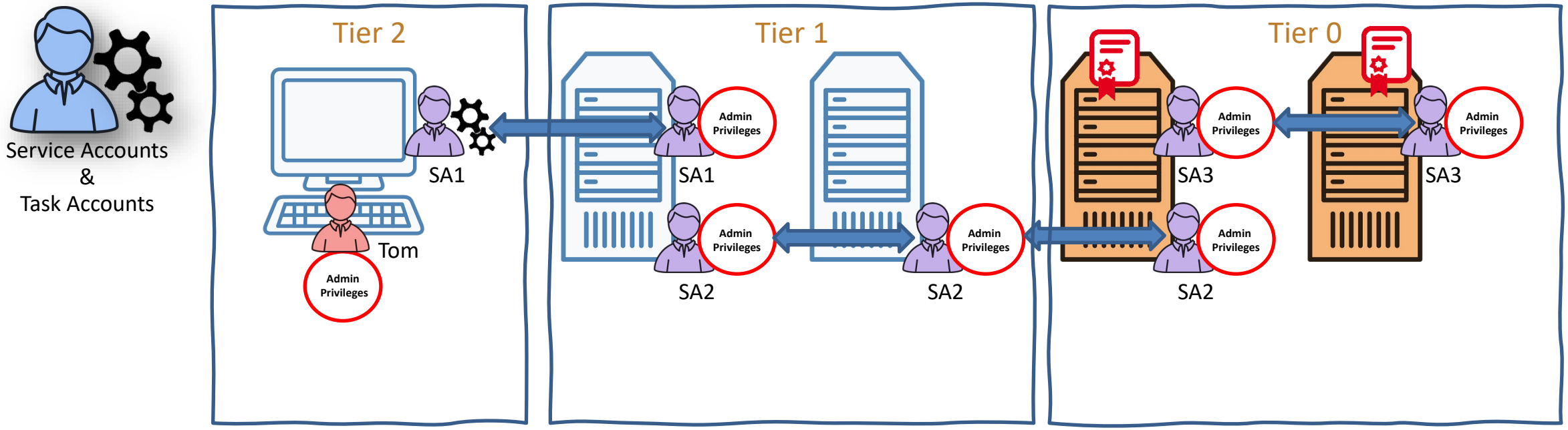
Vertraulichkeit: Öffentlich

Einführung von Schutzbereichen



Vertraulichkeit: Öffentlich

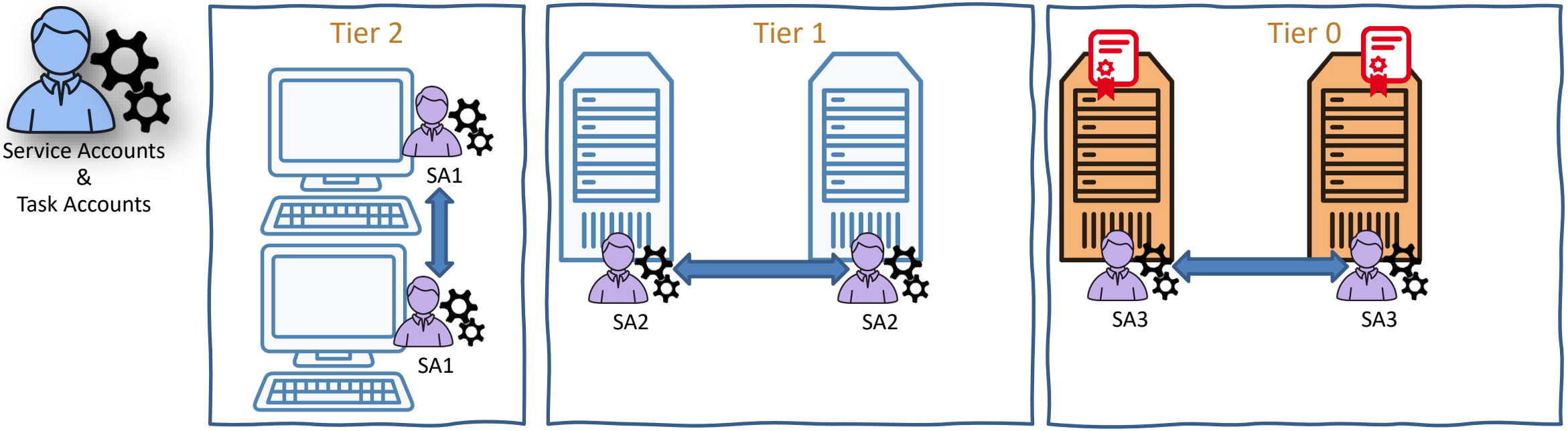
Lateral Movement über Tiers (Tier-Modell)



- Empfehlung: **Tier-Modell** zur **Aufteilung von Accounts und Systemen in Schichten („Tiers“)**
- z.B. **Tier 2** für die **Clients**, **Tier 1** für die **Applikationsserver** und **Tier 0** für die **kritischen Systeme**

Vertraulichkeit: Öffentlich

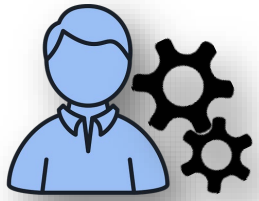
Empfehlung: Segmentierung nach Tiers (Tier-Modell)



- **Tierbreaker werden verboten**! Privilegierte Accounts einer Schicht dürfen nicht in anderen Schichten verwendet werden.
- **Lateral Movement über Tiers** hinweg **wird verhindert.**

Vertraulichkeit: Öffentlich

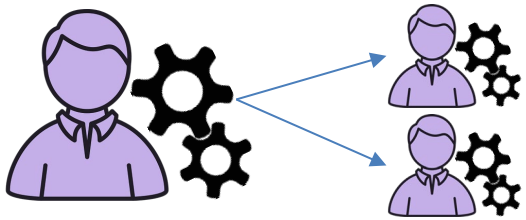
Analyse und Segmentierung



Service Accounts
&
Task Accounts

- Über Tier-Grenzen hinweg → Admin-Berechtigungen in mehreren Tiers (Tier-Modell)
- viele Zwecke → Nutzung für viele Zwecke (oft nicht dokumentiert)

Lösung



Segmentierung

Tool



Service Account
Scanner
(„**TSA-Scanner**“)

Vertraulichkeit: Öffentlich

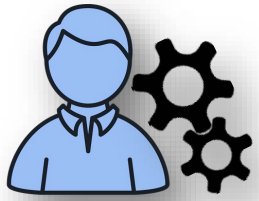


Service Accounts
&
Task Accounts

brauchen keine Adminrechte!

Vertraulichkeit: Öffentlich

Hinfort mit den Adminrechten…



Service Accounts
&
Task Accounts

hohe Privilegien auf vielen Systemen

Adminrechte (o. Ä.) auf einem oder mehreren Systemen

Lösung

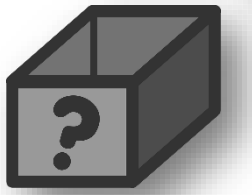


POLP (Principle of Least Privilege)

- Erste Versuche ohne Adminrechte
- Anfrage beim Hersteller
- Blackbox-Analyse

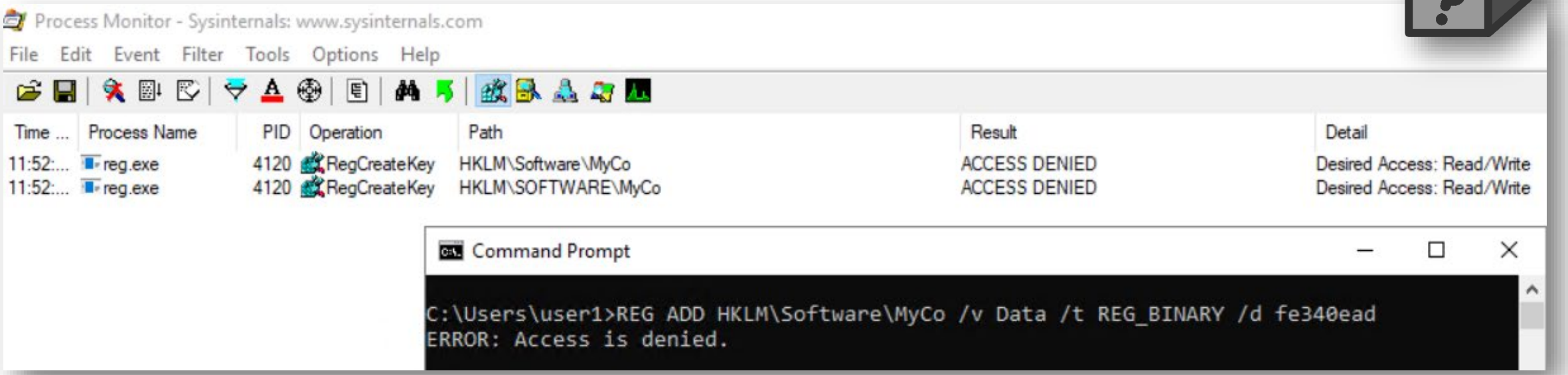






Vertraulichkeit: Öffentlich

Blackbox-Analyse (z.B. mittels Tool „ProcMon“)



- **Datei-**, **Registry-** und Netzwerkzugriffe lassen sich in Echtzeit überwachen → und **Schritt-für-Schritt freischalten**
- **Spezialfälle** sind ebenfalls lösbar (z.B. DCOM-Rechte, Dienstkontrolle etc.)

Vertraulichkeit: Öffentlich

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

CCVOSSEL

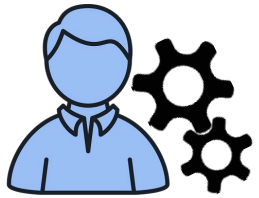
Na dann mal los…

Widerstand!

(aus den Fachabteilungen)

Vertraulichkeit: Öffentlich

Interaktive Anmeldung

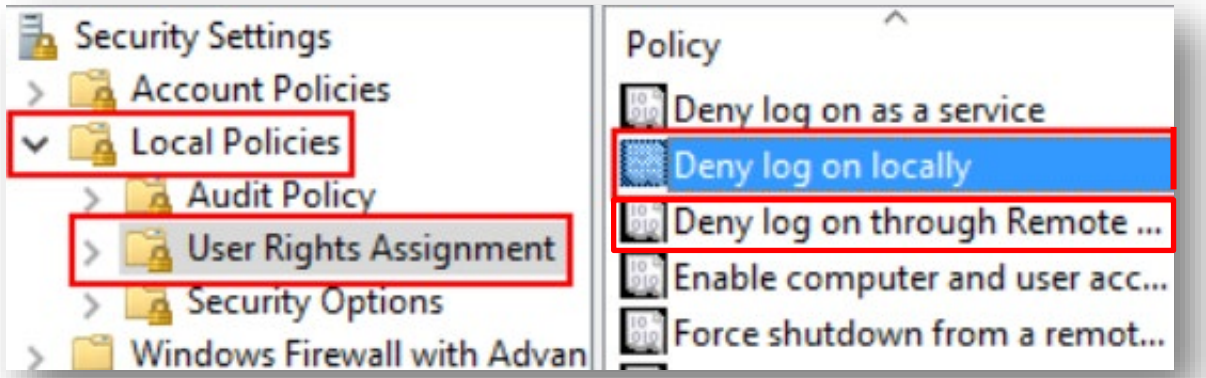


Service Accounts
&
Task Accounts

Interaktive Anmeldung → Interaktive Anmeldung (lokal/RDP) stellen Risiko dar

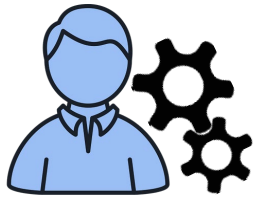
Lösung

Gruppenrichtlinie, die die **lokale** und die **RDP-Anmeldung** verbietet



Vertraulichkeit: Öffentlich

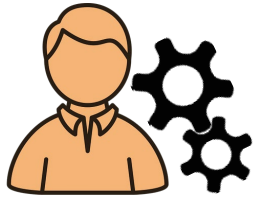
Da waren noch andere Probleme… Jetzt kommen die gMSAs!



Service Accounts
&
Task Accounts

langlebige Kennwörter	Keine Kennwortänderungspflicht / Änderung mühsam
simple Kennwörter	Neue Kennwortrichtlinien wirken nicht auf alte Accounts
verteiltes Kennwortwissen	Unklar, welcher Personenkreis Kennwortkenntnis hat
Kennwörter im Klartext	In Dokumentationen, Notizzetteln, Ex-&Ext-Mitarbeiter etc.

Lösung

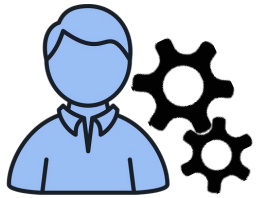


Group Managed
Service Account
(gMSA)

- **Automatische Kennwortverwaltung**, (Wechsel alle 30 Tage)
- **Kennwortlänge** = 240 Bytes
- Für **alle Scheduled Tasks** einsetzbar
- **Allerdings nur für ausgewählte Dienste** einsetzbar (meist MS-Dienste)

Vertraulichkeit: Öffentlich

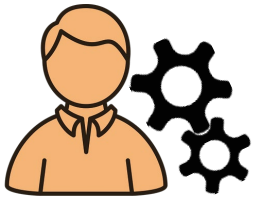
dMSAs sind die beste Lösung! Keine Kennwörter mehr!



Service Accounts
&
Task Accounts

Kennwörter der gMSAs können innerhalb 30 Tage ausgelesen und wiederverwendet werden

Lösung



Delegated Managed Service Account (dMSA)

- **Gerätegebundene Identitäten**
- Kerberos only
- erst einsetzbar ab **Windows Server 2025 als Domänencontroller** und als **Member-Server**.

Vertraulichkeit: Öffentlich

Bereinigungsprozess



- Analyse und **Bereinigung sämtlicher Service & Task Accounts** im Unternehmen
- **Risk-Score** pro Service Account
- Unterstützung der **Fachabteilungen**
- Es bedarf einer **kontinuierlichen Überwachung, Reports** und der **Berichterstattung** an das Management (z.B. CIO, ISOs, BISOs)
- automatisierte **Analysetools**
- Automatisierte **Prozess-Workflows**
- **zentrale Reportingsysteme** (z.B. **SIEM**)

Vertraulichkeit: Öffentlich

Fazit



- ✓ **Stark gestiegenes Sicherheitsniveau** im gesamten Konzern
- ✓ Durch **Segmentierung** wird der Nutzen für Angreifer vermindert
- ✓ Durch **Entfernung von Admin-Berechtigungen** wird **Lateral Movement verhindert**
- ✓ **gMSA**-Kennwörter durch automatische Verwaltung geschützt, **dMSA-Accounts** sind langsam im kommen
- ✓ **Tierbreaker** und Berechtigungen werden **kontinuierlich überwacht**

Vertraulichkeit: Öffentlich

CCVOSSEL



We ♥ being a hacker's nightmare