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

"T.I.S.P. Community Meeting 2021"

Berlin, 03.-04.11.2021

Least-Privilege-Prinzip in Konzernen

Oliver Falkenthal, CCVOSSEL GmbH

CCVOSSEL

We know IT.

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

Oliver Falkenthal

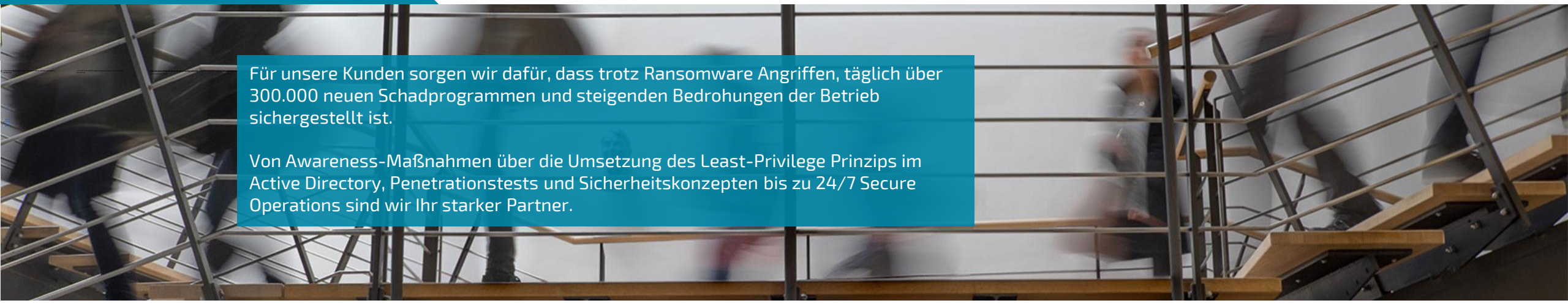
Teamleiter IT-Security

- TeleTrusT Information Security Professional (T.I.S.P.)
- Autor im TeleTrusT-AK „Stand der Technik“
- Certified Security Hacker
- Microsoft Certified Professional (MCSA, MCSE)
- VdS-anerkannter Berater für Cyber-Security
- CQURE Certified Windows Security Master 2021

o.falkenthal@ccvossel.de

CCVOSSEL
We know IT.

CCVOSSEL GmbH



Für unsere Kunden sorgen wir dafür, dass trotz Ransomware Angriffen, täglich über 300.000 neuen Schadprogrammen und steigenden Bedrohungen der Betrieb sichergestellt ist.

Von Awareness-Maßnahmen über die Umsetzung des Least-Privilege Prinzips im Active Directory, Penetrationstests und Sicherheitskonzepten bis zu 24/7 Secure Operations sind wir Ihr starker Partner.

ISO/IEC 27001 www.isocert.de zertifiziert

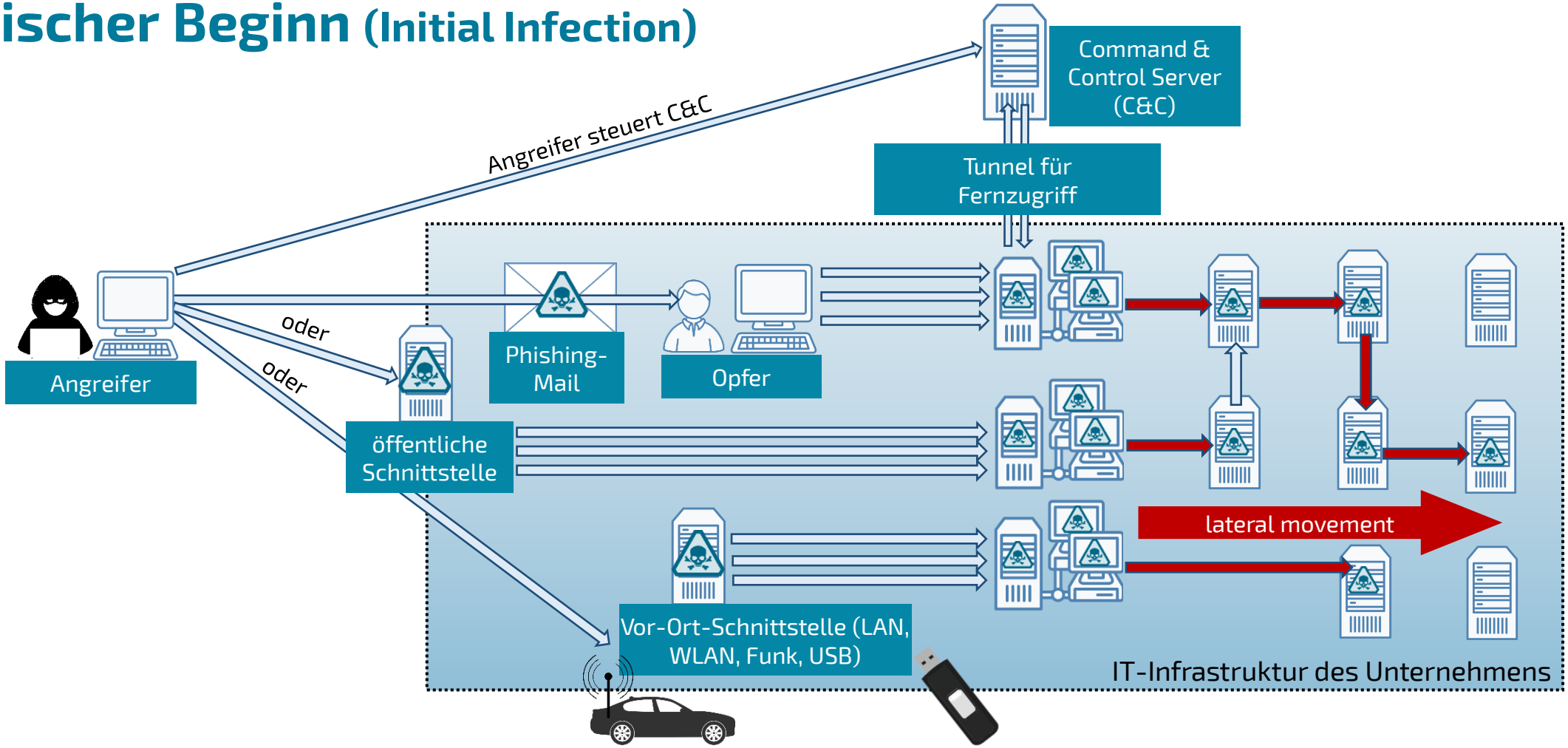
ISO 9001 www.isocert.de zertifiziert

CCVOSSEL
We know IT.

Unzählige Angriffsmöglichkeiten innerhalb von Konzernen

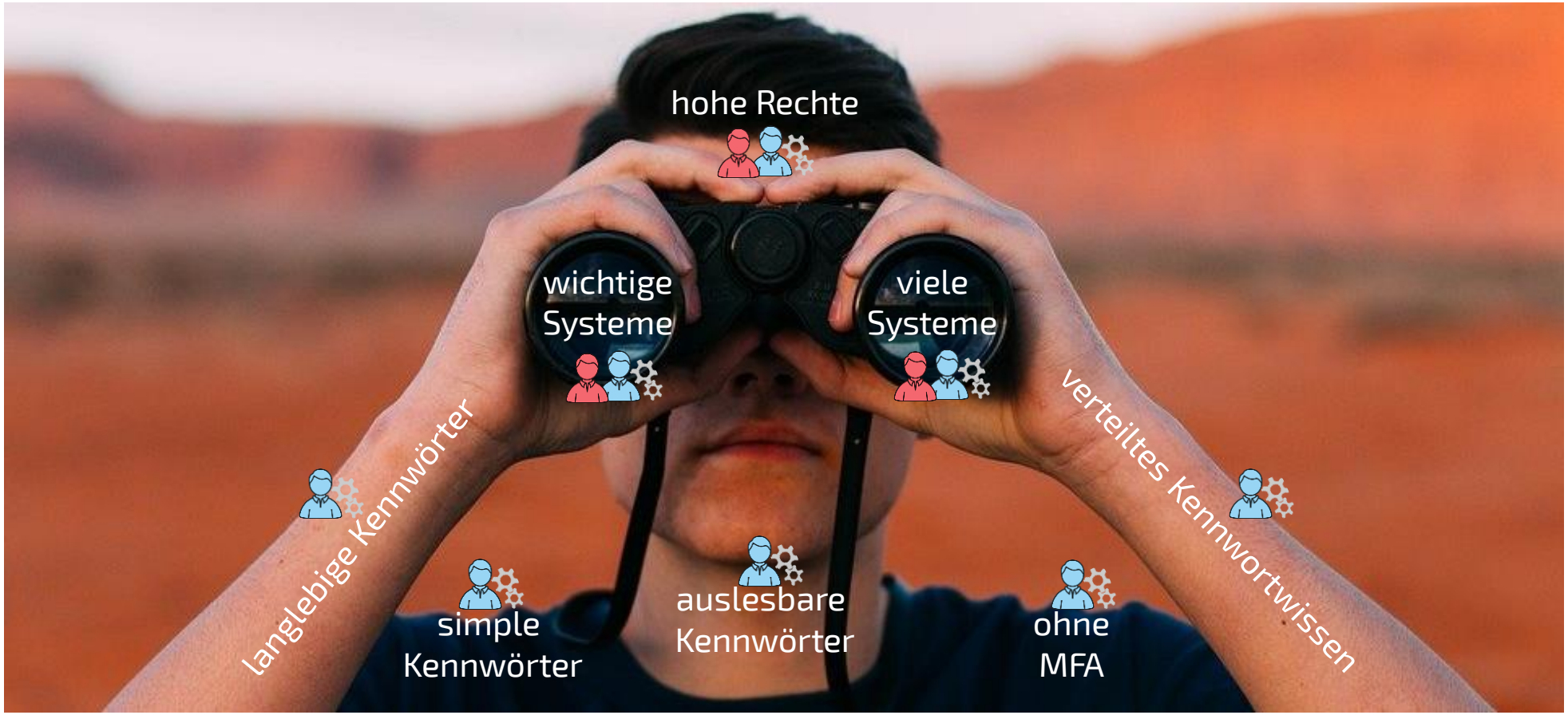
CCVOSSEL
We know IT.

Typischer Beginn (Initial Infection)



CCVOSSEL
We know IT.

Angreifer suchen Zugänge von Konten, die folgendes bieten…



Admin Accounts

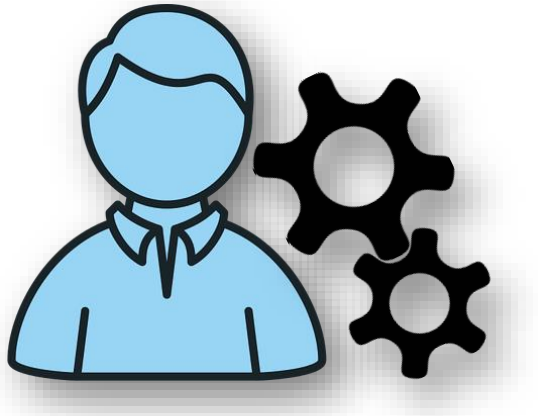
Service Accounts

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

CCVOSSEL
We know IT.

Angriffsvektor Nr.1

für großflächige Angriffe auf Windows-Infrastrukturen sind…

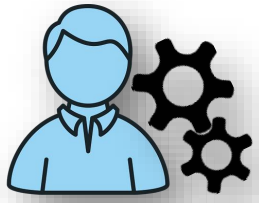


Service Accounts & Task Accounts

IT-Sicherheit
✓ BSI-Grundschutz 2.1
✓ AD-Härtung
✓ Group Managed Accounts
✓ POLP
✓ Gefährdungskategorien, z.B.: G 0.23, G 0.30, G 0.31, G 0.32

CCVOSSEL
We know IT.

Das größte Problem…



Service Accounts
&
Task Accounts

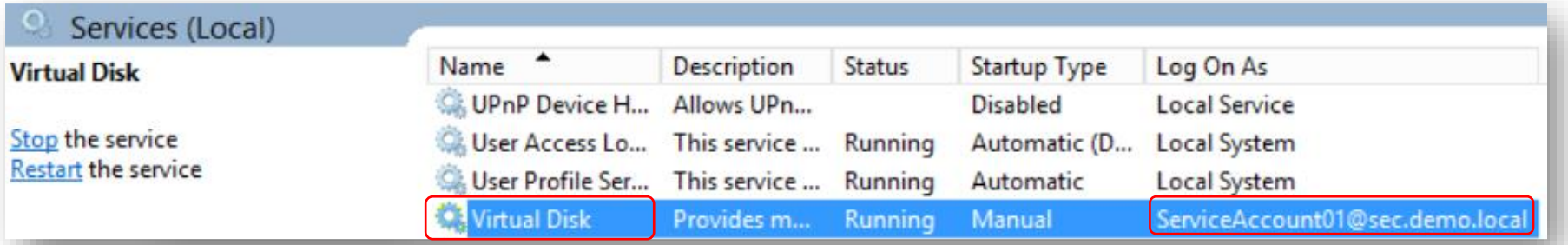
direkt auslesbare Kennwörter

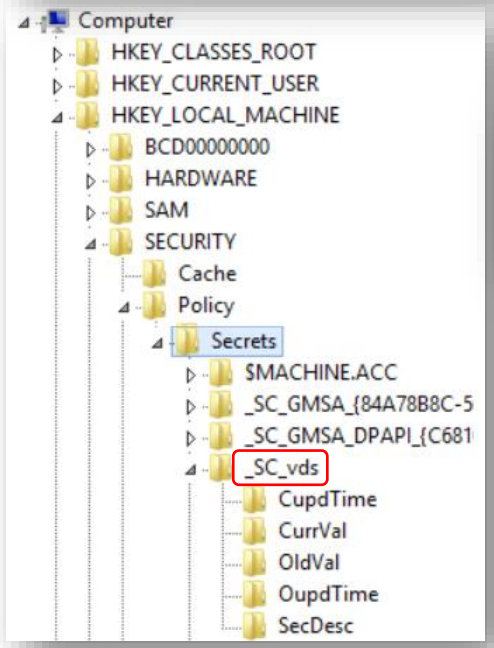
Kennwörter mit Adminrechten auslesbar

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

CCVOSSEL
We know IT.

Mimikatz im Einsatz






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

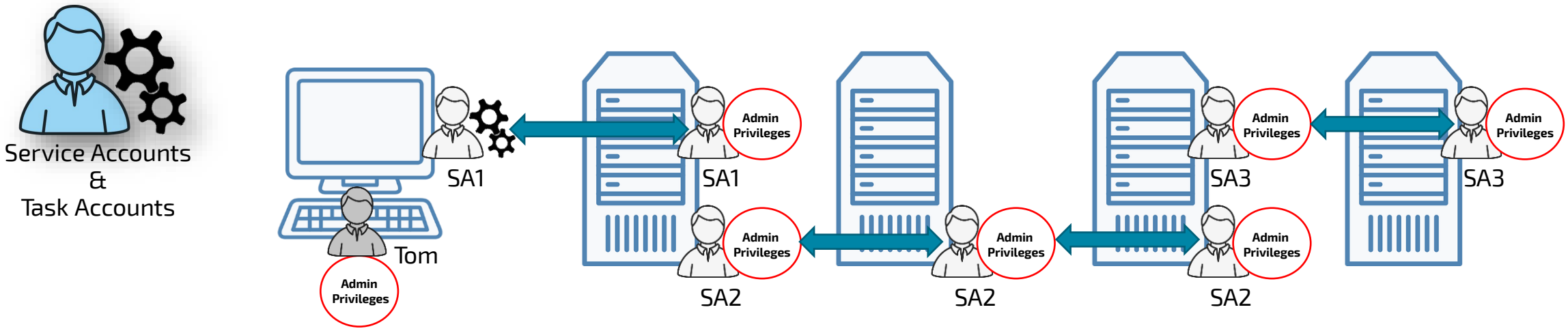
```
Secret  : _SC_vds / service 'vds' with username : ServiceAccount01@sec.demo.local
cur/text: SuperSecret1000
```

Klartext-Kennwort

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

CCVOSSEL
We know IT.

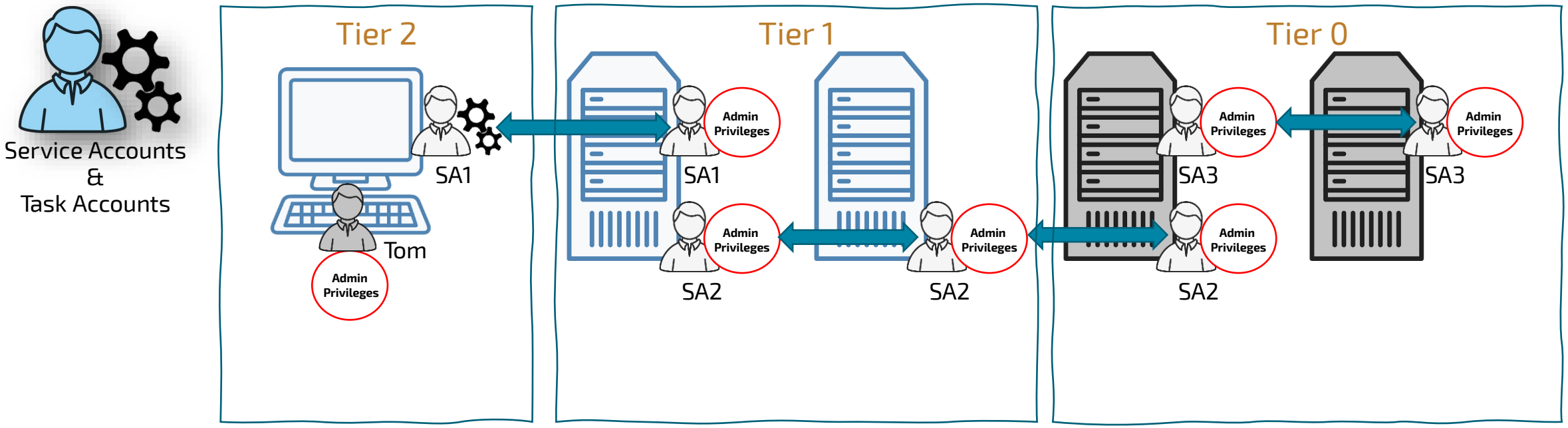
Lateral Movement



- **Admin-Privilegien** führen zu **Anmeldedaten** anderer Service Accounts
- **Fortbewegung** (**Lateral Movement**) über mehrere Zwischenstationen zum Ziel wird möglich
- oft zu Infrastruktursystemen (DC, DNS, PKI etc.) mit dem Ziel der **vollständigen Übernahme** der IT

CCVOSSEL
We know IT.

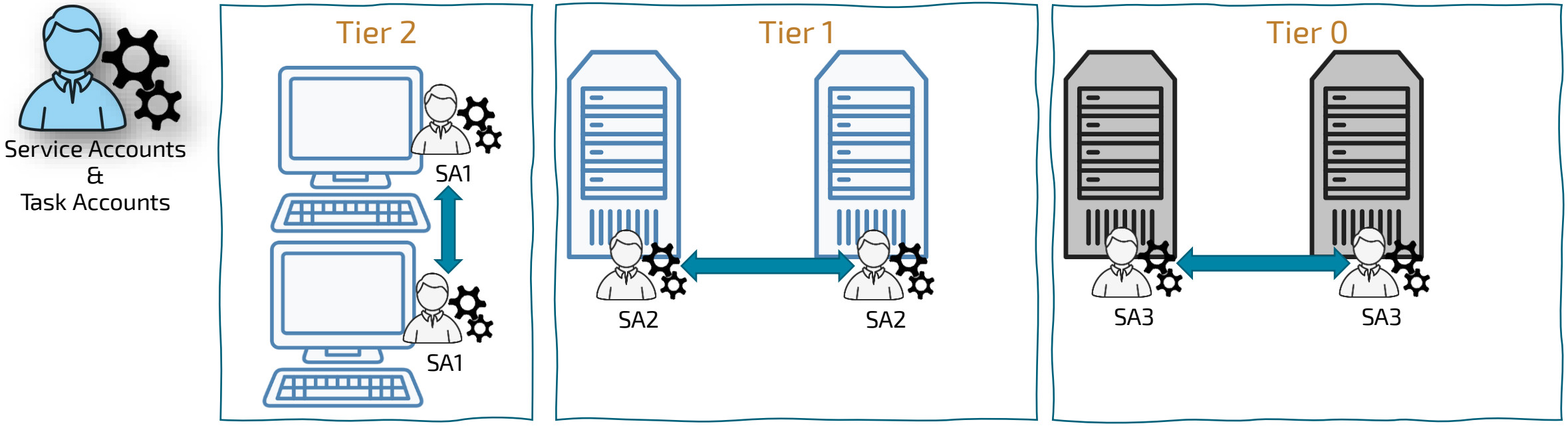
Lateral Movement über Tiers (Tier-Modell)



- Empfehlung: **Tier-Modell** zur **Aufteilung von Accounts und Systemen in Schichten („Tiers“)**

CCVOSSEL
We know IT.

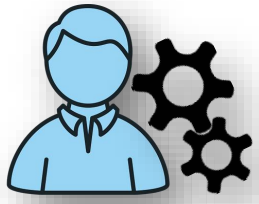
Empfehlung: Segmentierung nach Tiers (Tier-Modell)



- z.B. **Tier 2** für die **Clients**, **Tier 1** für die **Applikationsserver** und **Tier 0** für die **kritischen Systeme**
- Es muss sichergestellt werden, dass Accounts einer Schicht nicht in anderen Schichten verwendet werden. **Lateral Movement über Schichten hinweg** kann damit **verhindert werden.**

CCVOSSEL
We know IT.

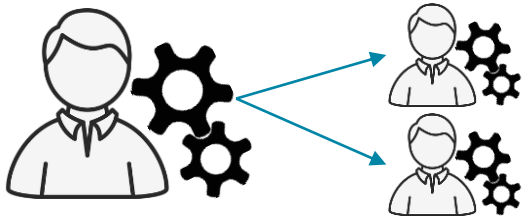
Analyse und Segmentierung



Service Accounts
&
Task Accounts

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

Lösung



Segmentierung

Tool

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

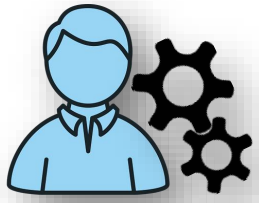
CCVOSSEL
We know IT.

Service Accounts
&
Task Accounts

brauchen keine Adminrechte!

CCVOSSEL
We know IT.

Hinfort mit den Adminrechten…



Service Accounts
&
Task Accounts

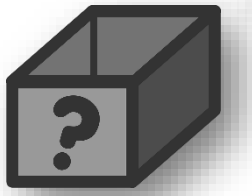
hohe Privilegien auf vielen Systemen

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

Lösung

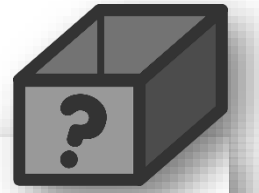
POLP (Principle of Least Privilege)

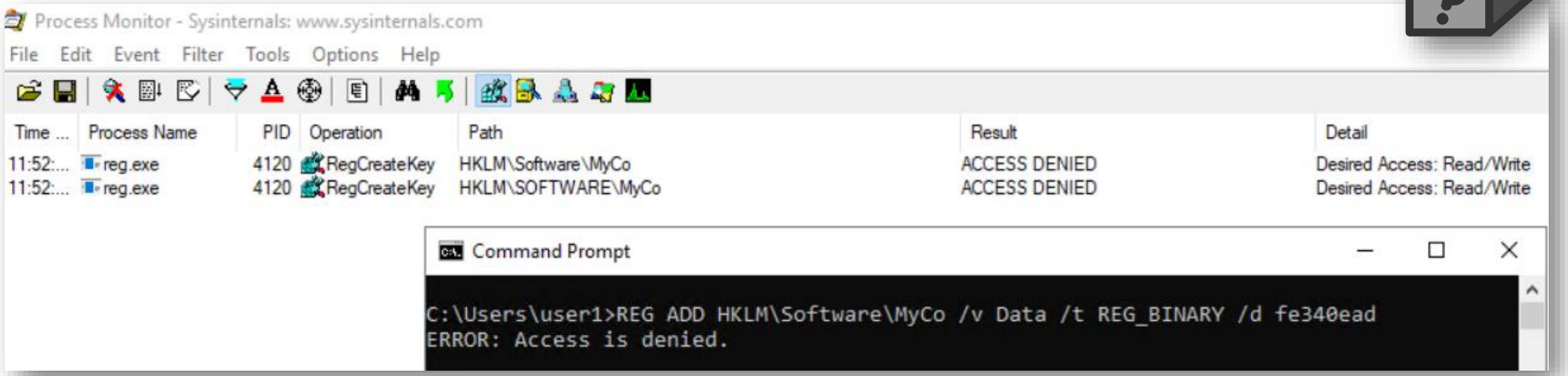
- Erste Versuche ohne Adminrechte
- Anfrage beim Hersteller
- Blackbox-Analyse



CCVOSSEL
We know IT.

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.)

CCVOSSEL
We know IT.

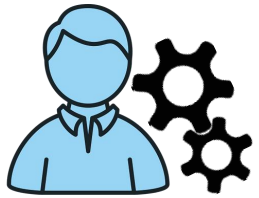
Na dann mal los…

Widerstand!

(aus den Fachabteilungen)

CCVOSSEL
We know IT.

Interaktive Anmeldung



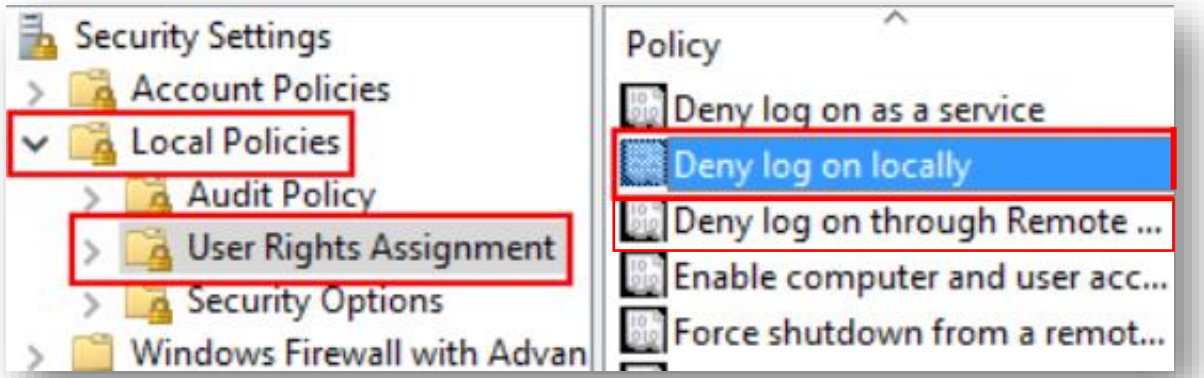
Service Accounts
&
Task Accounts

Interaktive Anmeldung

Interaktive Anmeldung (lokal/RDP) stellen Risiko dar

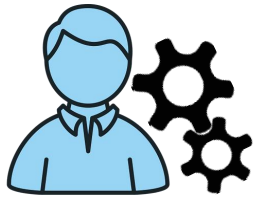
Lösung

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



CCVOSSEL
We know IT.

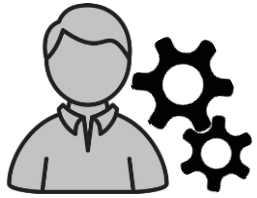
Da waren noch andere Probleme… Jetzt kommen die gMSAs!



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

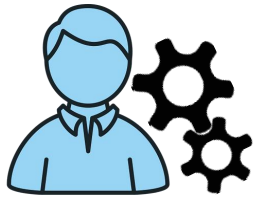


Group Managed
Service Account
(gMSA)

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

CCVOSSEL
We know IT.

Kennwörter in Skripten? Sollten nicht sein! Die PowerShell kann es!



Service Accounts
&
Task Accounts

Kennwörter im Klartext → Klartext-Kennwörter in Skripten

Lösung

- Möglichst entfernen
- **„Secure Strings“** in Powershell-Skripten

Verschlüsseln

```
$strEncrypted = ConvertFrom-SecureString -SecureString (Read-Host “Enter password to decrypt" -AsSecureString)
```

Entschlüsseln

```
$strEncrypted = "01000000d08c9ddf0115d1118c7a00c04fc297eb01000000d29105a690ce4fb19b6415cd153ade0002..."

$strDecrypted = [System.Runtime.InteropServices.Marshal]::PtrToStringAuto(`
 [System.Runtime.InteropServices.Marshal]::SecureStringToBSTR(`
 (ConvertTo-SecureString -String $strEncrypted)))
```

Prozessablauf

CCVOSSEL
We know IT.

A. **IST-Zustand**
Gefahrenszenario/
Angriffsvektoren

Basischeck

Task-/Service Account Scanner

Erweiterte Analyse

Bewertung,
Risk Scores,
Projektvorbereitung,
Checkliste

High Risk | Middle Risk | Low Risk

B. **Prozesserarbeitung** auf Grundlage der Kundeninfrastruktur/-bedarfe
+ Projektdurchführung

Management Reporting/Prozessfortschrittsbericht

1. Checkliste

Bearbeiten der Findings aus dem APR-Scan

(Interviews mit den Ownern der Serviceaccounts)

2.

Durchführung AD Bereinigung (POLP Prozess)

Account-Segmentierung

Account-Bereinigung

3.

APR-Scanner

Ergebnis-prüfung durch erneuten Scan

Anbindung Monitoring

C. **Maintenance**

Wöchentliche Re-Scans zur kontinuierlichen Bereinigung des AD durch das kundeninterne Team (z.B. SOC)

CCVOSSEL
We know IT.

Bereinigungsprozess

- Analyse und **Bereinigung sämtlicher Service & Task Accounts** im Unternehmen
- Unterstützung der **Fachabteilungen**
- Es bedarf einer **kontinuierlichen Überwachung, Reports** und der **Berichterstattung** an das Management (z.B. CIO, ISOs, BISOs)

CCVOSSEL
We know IT.

Werkzeuge

- **Interview-Konzepte** (**Checkliste**)
- selbstentwickelte automatisierte **Schwachstellenanalysetools (APR-Scanner)**
- **zentrale Reportingsysteme** (z.B. **SIEM**) mit komplexen Daten-Korrelationen
- Automatisierte **Prozess-Workflows**

CCVOSSEL
We know IT.

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
- ✓ **Minimale Berechtigungen** werden **kontinuierlich überwacht** (mittels APR-Scanner)

CCVOSSEL

We know IT.