



THOMAS
KRENN®

Active Directory besser absichern

Webinar am 25.11.2021

Christoph Mitasch, Thomas-Krenn.AG

THOMAS
KRENN®



Christoph Mitasch

- seit 2005 bei der Thomas-Krenn.AG, Niederlassung Österreich
- Diplomstudium Computer- und Mediensicherheit
- Erfahrung in Web Operations, Linux und HA
- Cyber-Security-Practitioner (v1)

Agenda

Grundlagen Active Directory
Empfehlungen
3-Tier-Modell und PAW
Sicherheits-Scanner
Windows 2FA mit privacyIDEA

Agenda

Grundlagen Active Directory

Empfehlungen

3-Tier-Modell und PAW

Sicherheits-Scanner

Windows 2FA mit privacyIDEA

Grundlagen Active Directory



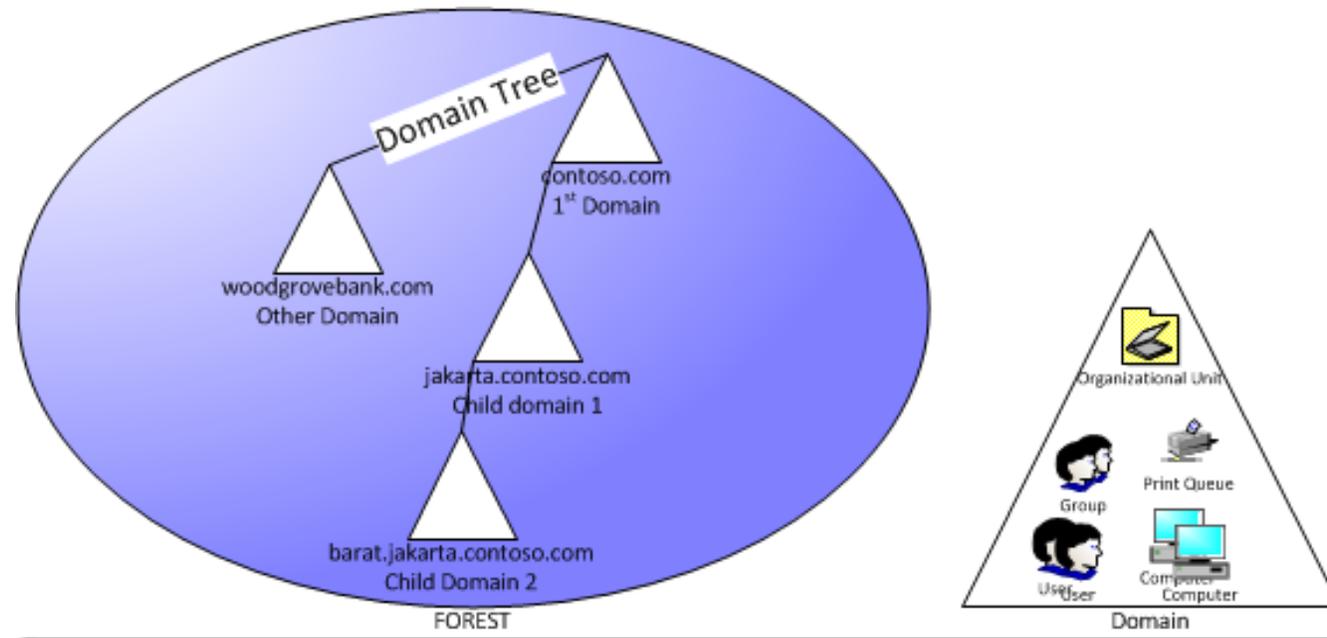
- Verzeichnisdienst von Windows Server
- 5 Server-Rollen:
 - Domain Services (AD DS)
 - Lightweight Directory Services (AD LDS, früher ADAM)
 - Federation Services (ADFS)
 - Rights Management Services (AD RMS)
 - Certificate Services (AD CS)
- 4 Protokolle
 - LDAP
 - Kerberos
 - SMB/CIFS
 - DNS
- relationale Jet Blue Datenbank “NTDS.dit”, Secret-Key in Registry, Achtung bei Backup!
- seit Windows 2000 Multimaster Replikation, davor PDC/BDC

Grundlagen Active Directory



- Objekt = Datensatz
 - Konten (Benutzer, Gruppen, Computer)
 - Ressourcen (Datei und Druckerfreigaben)
- Eigenschaften = Attribute
- Organisation der Objekte in OUs (Containern)
- DN = distinguished name
Bsp: „CN=Franz Mustermann,OU=Marketing,DC=example,DC=org“
- Loginname
traditionell: EXORG\FMustermann
UPN: FMustermann@example.org
- Zugriffssteuerungsliste - ACL (Access Control List)
- Gruppenrichtlinien – GPO (Group Policy Object)

Grundlagen Active Directory



Quelle: <https://social.technet.microsoft.com/wiki/contents/articles/16969.active-directory-concepts-part-2.aspx>

Umfrage

Verwendung Active Directory

1. nur lokal, kein Sync
2. mit Azure AD Connect Pass-Through
3. mit Azure AD Connect Hash-Sync
4. mit AD-FS Verbund zu Azure AD



Recommended

AAD Connect Password Hash Sync

- Seamless SSO
- Cloud MFA
- Simple and Cheap
- 1 Server

Keep Passwords On-Prem

AAD Connect Pass-Through Auth

- Seamless SSO
- Cloud MFA
- Simple and Cheap
- 1 Server

Works with On-Prem MFA

ADFS

- Federated SSO
- Password on-prem
- Complex and Expensive
- Server Farm



Agenda

Grundlagen Active Directory

Empfehlungen

3-Tier-Modell und PAW

Sicherheits-Scanner

Windows 2FA mit privacyIDEA

Empfehlungen

APP.2.2: Active Directory (Edition 2021)

Datum 01.02.2021

- BSI Grundschatz Kompendium „APP.2.2: Active Directory“
 - Gefährdungslagen
 1. Unzureichende Planung der Sicherheitsgrenzen
 2. Zu viele oder nachlässige Vertrauensbeziehungen
 3. Fehlende Sicherheitsfunktionen durch ältere Betriebssysteme und Domain Functional Level
 4. Betrieb weiterer Rollen und Dienste auf Domänencontrollern
 5. Unzureichende Überwachung und Dokumentation von delegierten Rechten
 6. Unsichere Authentisierung
 7. Zu mächtige oder schwach gesicherte Dienstkonten
 8. Nutzung desselben lokalen Administratorpassworts auf mehreren IT-Systemen
 - Anforderungen
 - **Basis:** Planung der AD-Administration, Planung der Gruppenrichtlinien, Härtung des AD, Aufrechterhaltung der Betriebssicherheit, Umsetzung sicherer Verwaltungsmethoden
 - **Standard:** Konfiguration des „Sicheren Kanals“ unter Windows, Schutz der Authentisierung beim Einsatz von AD, Sicherer Einsatz von DNS für AD, Überwachung der AD-Infrastruktur, Datensicherung für Domänen-Controller
 - **Erhöhtem Schutzbedarf:** Verwendung dedizierter privilegierter Administrationssysteme, Trennung von Administrations- und Produktionsumgebung

Empfehlungen

- Microsoft – Best Practices

- <https://docs.microsoft.com/de-de/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory>

- Schützen von Domänencontrollern vor Angriffen

- <https://docs.microsoft.com/de-de/windows-server/identity/ad-ds/plan/security-best-practices/securing-domain-controllers-against-attack>
- Physische Sicherheit: TPM, Bitlocker Verschlüsselung, dedizierte sichere Racks
- Virtualisierte Domänencontroller: separate physische Hosts, shielded VMs
- RODC = Read Only Domain Controller für unsichere Standorte
- Domänen Controller mit alten Windows-Versionen priorisiert außer Betrieb nehmen
- Windows Server Core wird empfohlen, Verwaltung mit PAWs

- Einführung
- Angriffswege
- Attraktive Konten für den Diebstahl von Anmeldeinformationen
- Reduzieren der Active Directory-Angriffsfläche
- Implementieren von Verwaltungsmodellen der geringsten Rechte
- Implementieren sicherer Verwaltungshosts
- Schützen von Domänencontrollern vor Angriffen
- Überwachen von Active Directory auf Anzeichen einer Sicherheitsgefährdung
- Empfehlungen zu Überwachungsrichtlinien
- Planen der Kompromittierung
- Warten einer sichereren Umgebung
- Anhänge
- Anhang B: Privilegierte Konten und Gruppen in Active Directory
- Anhang C: Geschützte Konten und Gruppen in Active Directory
- Anhang D: Schützen integrierter Administratorkonten in Active Directory
- Anhang E: Schützen von Organisationsadministratorgruppen in Active Directory
- Anhang F: Schützen von Domänenadministratorgruppen in Active Directory
- Anhang G: Schützen von Administratorgruppen in Active Directory
- Anhang H: Schützen lokaler Administratorkonten und -gruppen
- Anhang I: Erstellen von Verwaltungskonten für geschützte Konten und Gruppen in Active Directory
- Anhang L: Zu überwachende Ereignisse
- Anhang M: Links zu Dokumenten und empfohlene Lektüre

- Microsoft Security Baselines - GPOs

- <https://www.microsoft.com/en-us/download/details.aspx?id=55319>
- Windows 10 Version 1809 and Windows Server 2019 Security Baseline.zip
- Microsoft Security Configuration Toolkit (SCT)
- Policy Analyzer - GPOs vergleichen und verbessern
- CIS Benchmarks (Level 1,2,3) als Alternative

Empfehlungen

- Lessons Learned @ Thomas-Krenn

- NTFS Berechtigungen genau prüfen
sind auch bei Logon/Logoff-Skripten sowie GPOs (SYSVOL\Policies) relevant
- möglichst wenig Rollen auf Domänen-Controllern (z.b. keine Zertifizierungsstelle)
-> hilft auch bei Windows Upgrades
- Printer Spooler deaktivieren
- 2FA in Azure AD verhindert sehr oft Angriffe
- eigenes VLAN für Domänen-Controller
- cpassword in GPOs
- lokale Administrator-Passwörter auf Domänen-Member Servern
-> lokale Admin-Accounts führen häufig zu Verlust des Domänen-Admins
- regelmäßige Überprüfung macht Sinn
- Zentrale Logs essentiell für Angriffserkennung und -analyse
 - Windows Event Forwarding (WEF)
 - z.b. Graylog oder Winlogbeat von Elastic
- Auftrennung Admin Accounts für Azure AD und OnPrem -> siehe auch MS Videos <https://docs.microsoft.com/en-us/security/compass/administration-videos-and-decks>



In this article

Part 1: Introduction (05:40)

Part 2: Admin Quantity (03:14)

Part 3: Managed and Separate Admin Accounts (03:38)

Part 4: Emergency Access (02:28)

Part 5: Containing Attack Pivot Risk (02:42)

Part 6: Admin Account Protection (05:25)

Part 7: Admin Workstation Security (04:09)

Part 8: Enforcing Access Security (03:13)

Part 9: Simplify Permissions (03:31)

Part 10: Admin Account Lifecycle (02:53)

Next steps

Von: [redacted]
Gesendet: Dienstag, 9. November 2021 11:47
An: [redacted] <[redacted]@thomas-krenn.com>
Betreff: Arbeitsabläufe in Mannschaften =0
Priorität: Hoch

Microsoft Mannschaften

Hallo

Deine Teamkollegen versuchen, dich in **Microsoft Mannschaften**

GP Neues Dokument, das für Sie in Team freigegeben wurde

In Teams
anzeigen

Jetzt Microsoft Teams installieren

IOS

ANDROID

Microsoft Körperschaft, Eins Microsoft Weg, Redmond Wa

https://refid-2login.website.yandexcloud.net/#[redacted]@thomas-krenn.com

 Microsoft

← [redacted]@thomas-krenn.com

Enter password

Password

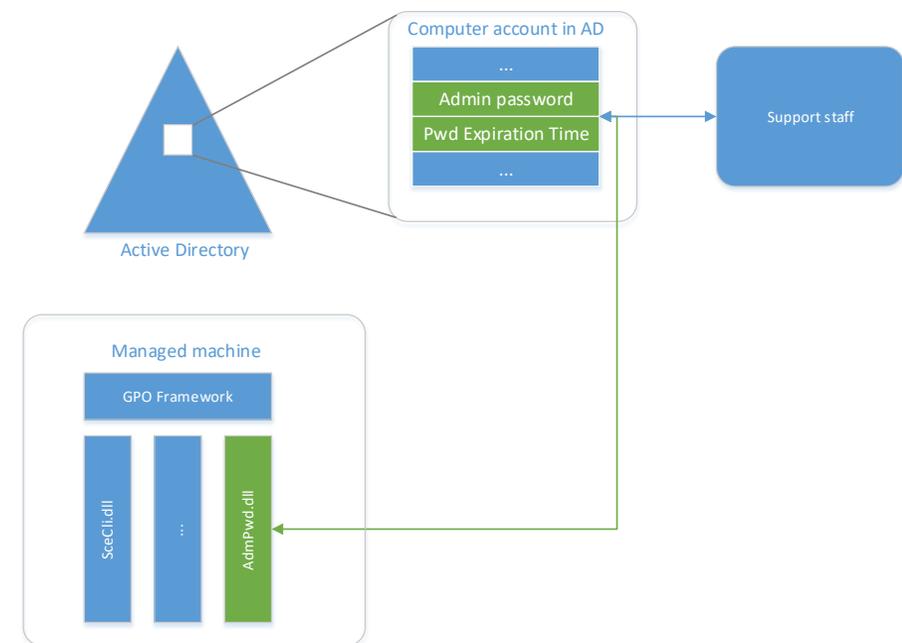
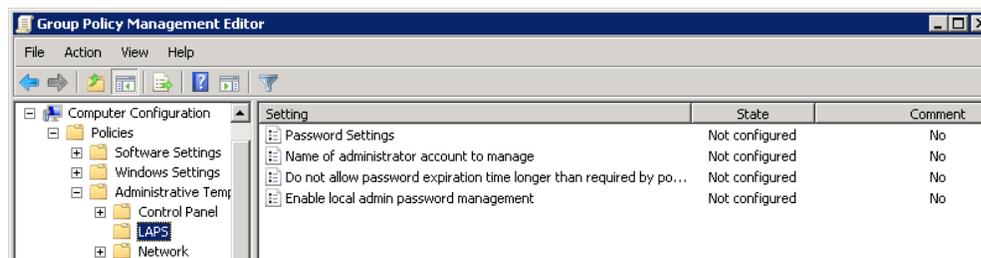
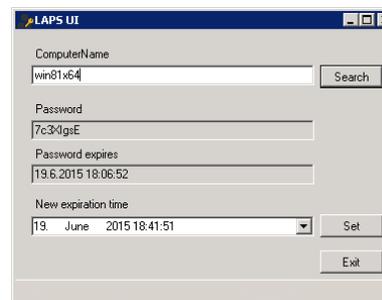
[Forgot my password](#)

Sign in

- Nach Eingabe des Passwortes gab es sofort Loginversuche von einer russischen IPv6 Adresse

Local Administrator Password Solution (LAPS)

- lokale Administrator Passwörter werden zentral über das AD verwaltet
- nur kurze Zeit gültig (Default: 30 Tage, min: 1 Tag), Agent ändert automatisch
- AD Schema Anpassung
- über Gruppenrichtlinie aktiviert
- Achtung: für DCs nicht relevant, haben keine lokalen Konten
- Download: <https://www.microsoft.com/en-us/download/details.aspx?id=46899>



Quelle: <https://www.microsoft.com/en-us/download/details.aspx?id=46899>

Agenda

Grundlagen Active Directory

Empfehlungen

3-Tier-Modell und PAW

Sicherheits-Scanner

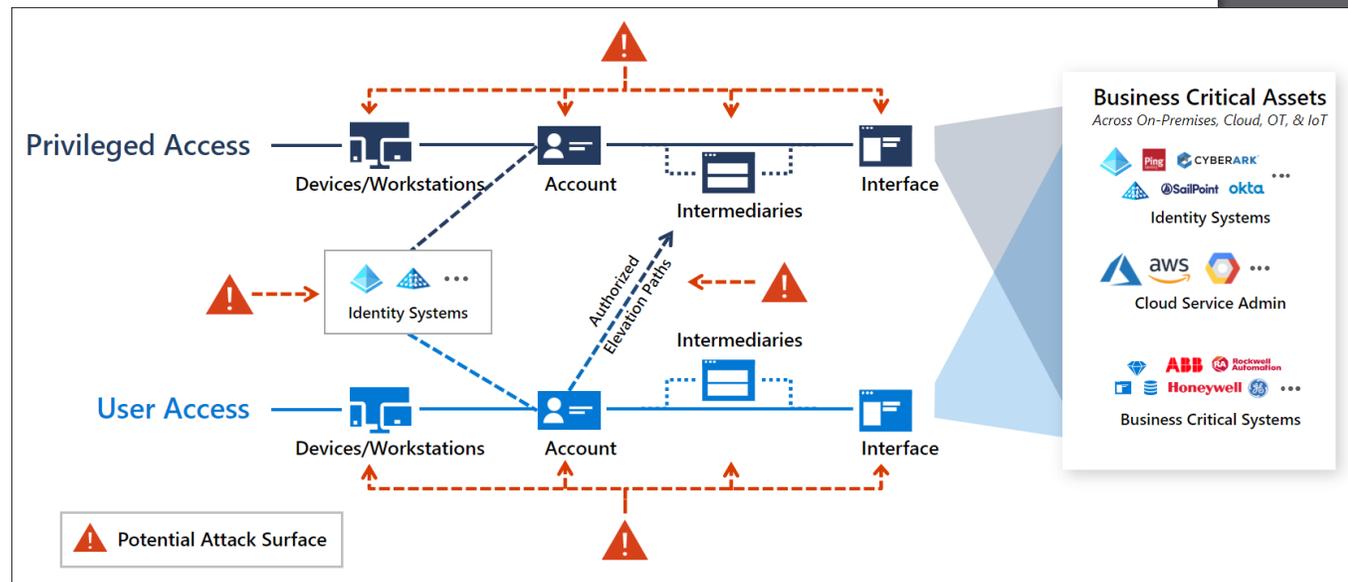
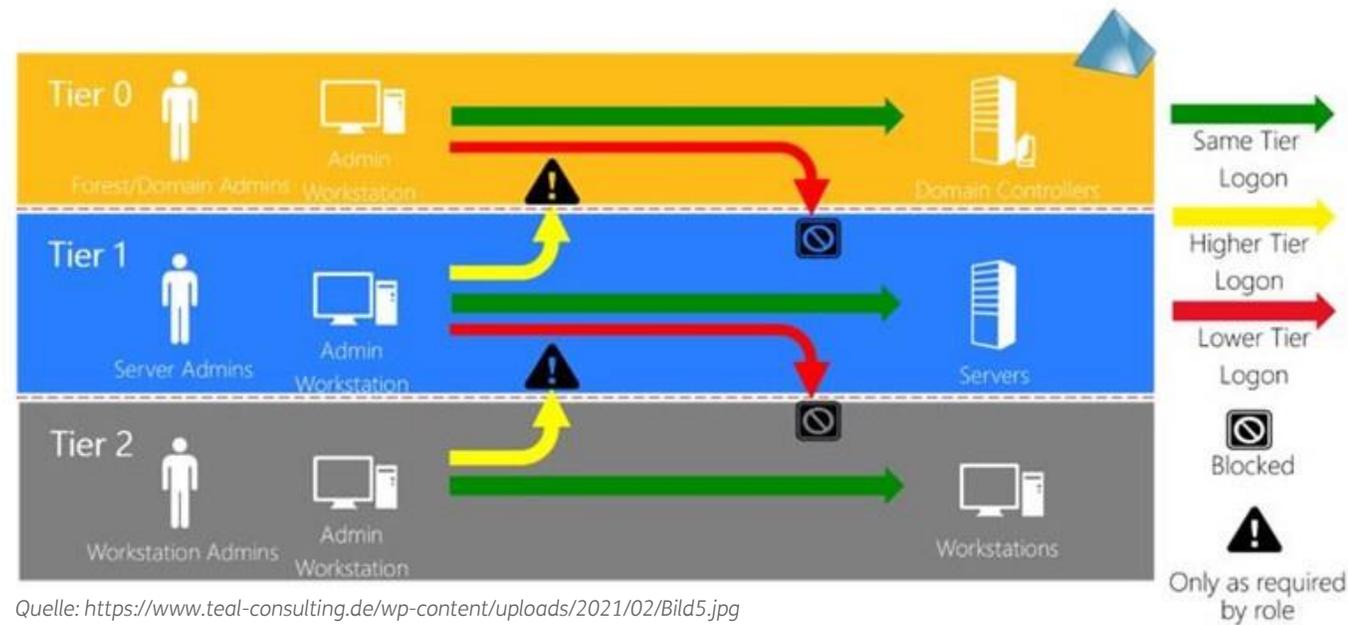
Windows 2FA mit privacyIDEA

3 Tier Modell

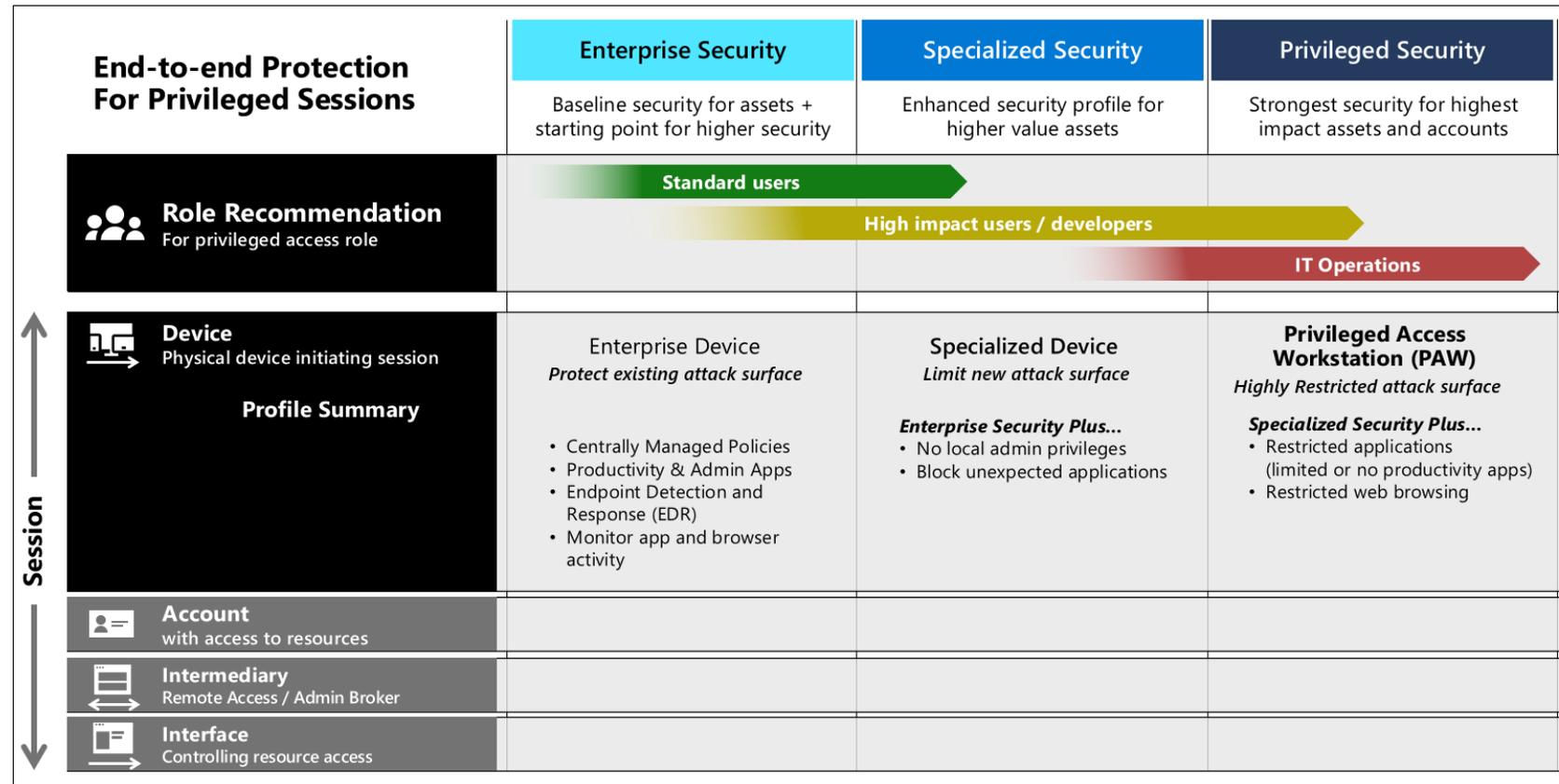
- Tier 0:
 - DCs, Domain Admins
- Tier 1:
 - restlichen Server
- Tier 2:
 - Workstations

<https://www.frankysweb.de/active-directory-einfache-manahmen-fr-mehr-sicherheit-teil-1/>

- mittlerweile durch Privileged Access Strategy und RAMP (Rapid Modernization Plan) abgelöst (davor gab es noch ESAE)
- „Strategic assumption - Cloud is a source of security“



Privileged Access Workstations (PAW)



Quelle: <https://docs.microsoft.com/en-us/security/compass/privileged-access-devices>

Agenda

Grundlagen Active Directory

Empfehlungen

3-Tier-Modell und PAW

Sicherheits-Scanner

Windows 2FA mit privacyIDEA

PingCastle

- kostenlos (“as long as you do not derive any revenue from it”), Non-Profit OSL, “Enterprise Version“
- normale Benutzerrechte ausreichend
- Abfrage via LDAP, ADWS, SMB
- Kommandozeile

```
.\. PingCastle (Version 2.10.0.0 06.08.2021 08:19:57)
| #. Get Active Directory Security at 80% in 20% of the time
# @@ > End of support: 31.07.2023
| @@@:
| .# Vincent LE TOUX (contact@pingcastle.com)
| .: twitter: @mysmartlogon https://www.pingcastle.com
What do you want to do?
=====
Using interactive mode.
Do not forget that there are other command line switches like --help that you can use
1-healthcheck-Score the risk of a domain
2-conso -Aggregate multiple reports into a single one
3-carto -Build a map of all interconnected domains
4-scanner -Perform specific security checks on workstations
5-export -Export users or computers
6-advanced -Open the advanced menu
0-Exit
=====
This is the main functionality of PingCastle. In a matter of minutes, it produces a report which will give you an overview of your Active Directory security. This report can be generated on other domains by using the existing trust links.
```

- HTML- und XML-Report
- ~150 Checks

Indicators



Domain Risk Level: 100 / 100

It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better



State Objects rule details [5 rules matched]

1 domain(s) used in SIDHistory	+ 15 points
Presence of wrong primary group: 1	+ 15 points
Non admin users can add up to 1 computer(s) to a domain	+ 10 points
The subnet declaration is incomplete [1 ip of DC not found in declared subnets]	+ 5 points
SMB v1 activated on 1 DC	+ 1 points
SMB v1 activated on 1 DC	+ 1 points

DC Vulnerability (SMB v1)

Description:
The purpose is to verify if Domain Controller are vulnerable to the SMB v1 vulnerability

Technical explanation:
The SMB downgrade attack is used to obtain credentials or executing commands on behalf of a user by using SMB v1 as protocol. Indeed, because SMB v1 supports old authentication protocol, the integrity can be bypassed

Advised solution:
It is highly recommended by Microsoft to disable SMB v1 whenever it is possible on both client and server side. Do note that if you are still not following best practices regarding the usage of deprecated OS (Windows 2000, 2003, XP, CE), regarding Network printer using SMBv1 scan2shares functionalities, or regarding software accessing Windows share with a custom implementation relying on SMB v1, you should consider fixing this issues before disabling SMB v1, as it will generates additional errors.

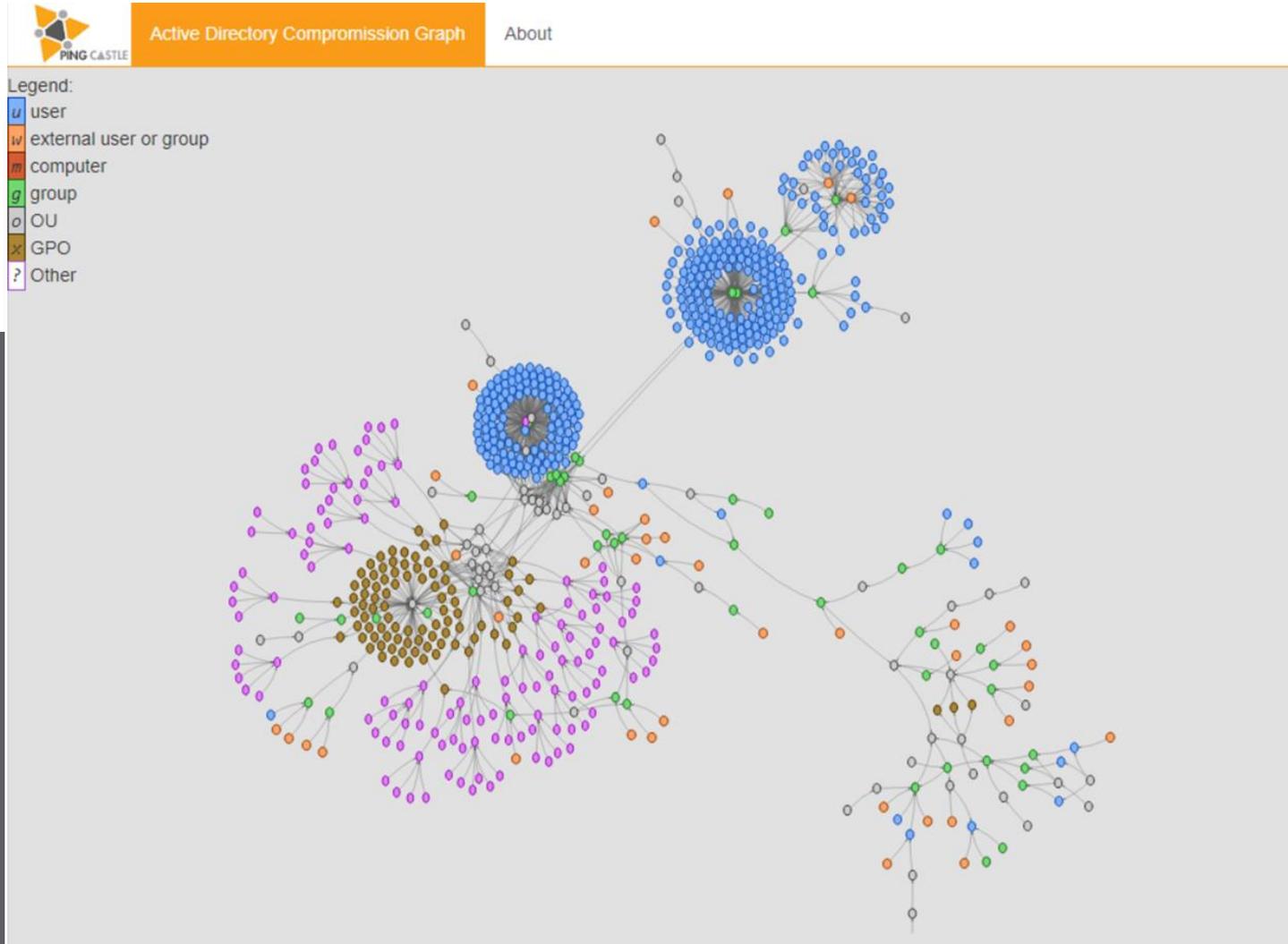
Points:
1 points if present

Documentation:
<https://github.com/fgandx/Responder-Windows>
<https://blogs.technet.microsoft.com/josebda/2015/04/21/the-deprecation-of-smb1-you-should-be-planning-to-get-rid-of-this-old-smb-dialect>
<https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012>

Details:
Domain controller: WIN-PGAH2EC18E

Quelle: <https://www.pingcastle.com/documentation/>

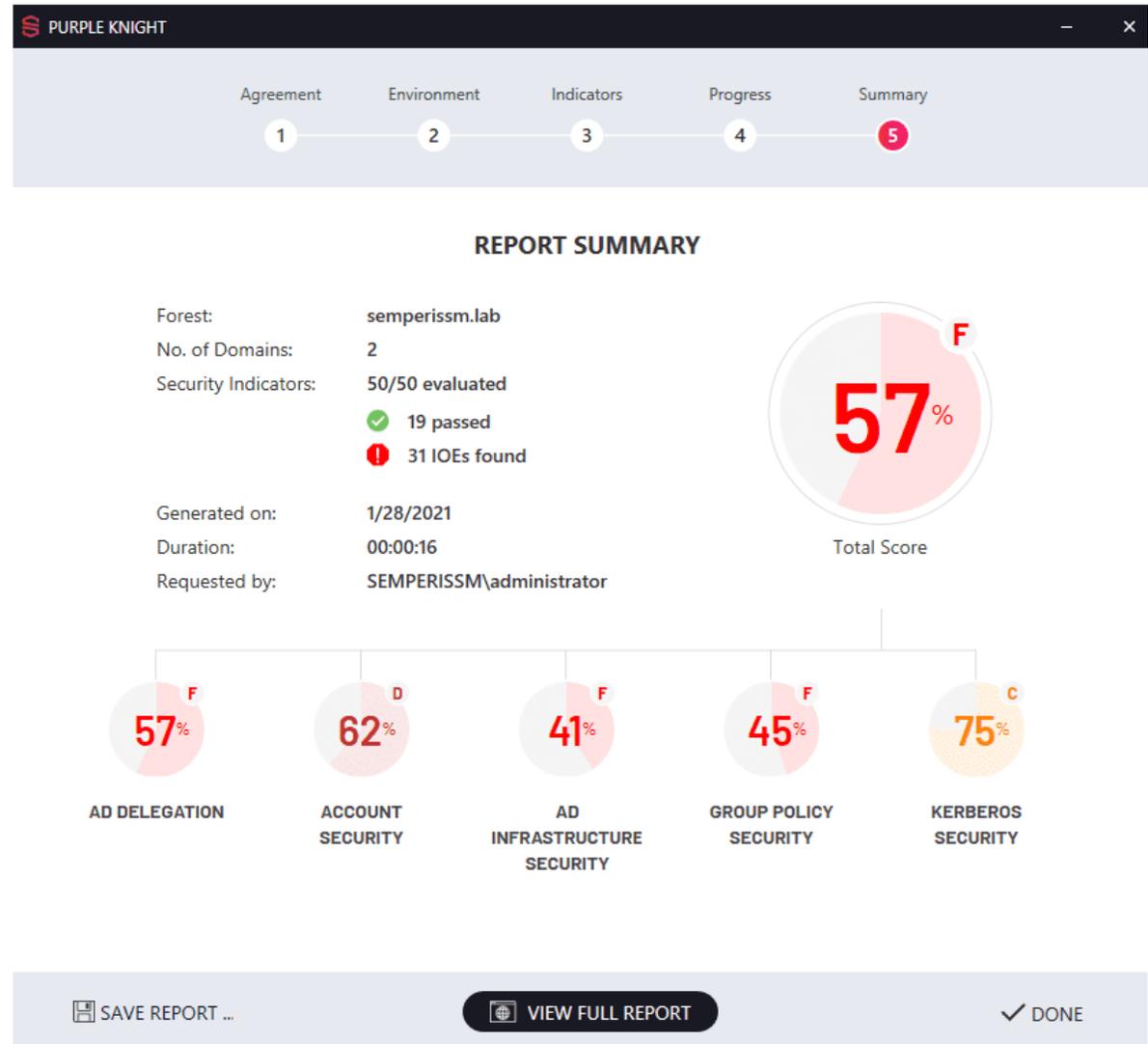
PingCastle



Quelle: <https://www.pingcastle.com/documentation/>

Purple Knight

- kostenlos nach Registrierung
- normale Benutzer-Rechte ausreichend
- Abfrage via LDAP, SMB
- >70 Checks
- MITRE ATT&CK Zuordnung



Quelle: <https://www.purple-knight.com/>

Specops Password Auditor

- kostenlos nach Registrierung
- Richtlinien mit Specops Password Policy sind kostenpflichtig
- ~700 Mio bekannte Passwörter
- PDF Report

The screenshot displays the Specops Password Auditor interface with the following sections:

- Blank Passwords (1):** KioskUser
- Breached Passwords (97):** Adam Admin, Adam Patria, Alasteir Blance, Albrecht Jessett, Ailyn Conlon, Augy Sargood, Bealle Mollen, Brant Neilson, Brew Adamovsky
- Identical Passwords (4):** Adam Admin, Adam Patria, Demo Admin, SQL Service
- Admin Accounts:** Adam Admin, Administrator, Demo Admin
- Stale Admin Accounts (2):** Adam Admin, Administrator
- Password Not Required (2):** KioskUser, MSOLService
- Password Never Expires (7):** Adam Admin, Administrator, App Service, Demo Admin, KioskUser, MSOLService, SQL Service
- Expiring Passwords:** Jere Peschet, Winne Skrzynski, Reidar Dingivan, Staford Guillot, Wheeler Acock, Alyda Tine, Mellie Gregoriou, Jacklyn Iacabucci
- Expired Passwords (9):** Donia Momery, Ailyn Conlon, Delora Shorto, Myrwyn Jendrich, Sandy Lepper, Odie Furphy, Phillis McMenamy, Reid Stallan, Janela Sherburn
- Password Policies:** specopsdemo1.local, Admins Password Policy, Service Accounts Password Policy
- Password Policy Usage:** A pie chart showing usage distribution.
- Password Policy Compliance:** Admins Password Policy (yellow), specopsdemo1.local (yellow), Service Accounts Password Policy (red)

At the bottom, there are buttons for "Back" and "Get PDF Report".

Quelle: <https://www.youtube.com/watch?v=4ekhMYMEhRI>

Agenda

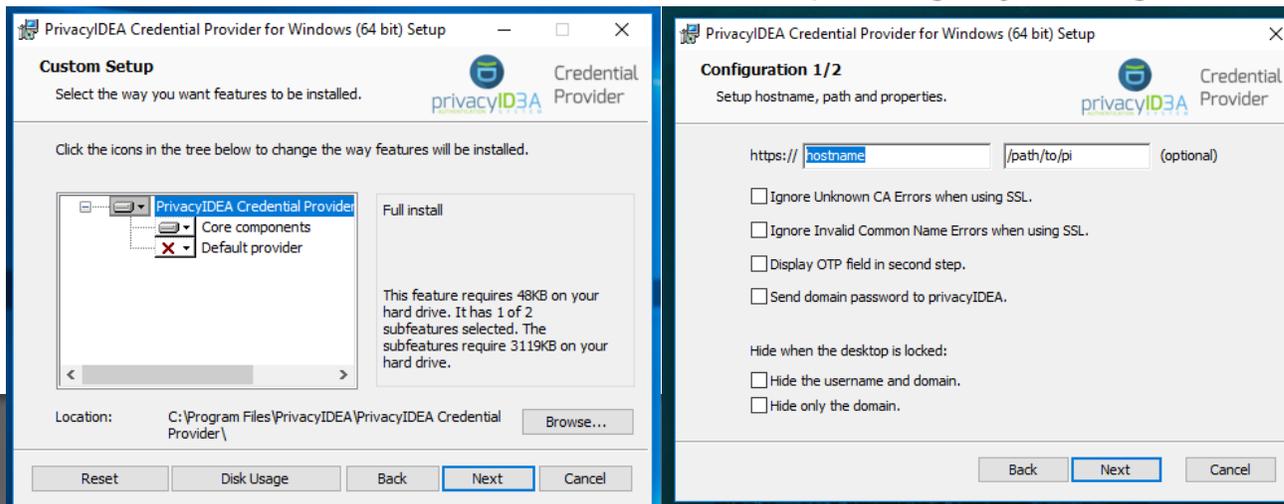
Grundlagen Active Directory
Empfehlungen
3-Tier-Modell und PAW
Sicherheits-Scanner
Windows 2FA mit privacyIDEA

Windows 2FA mit privacyIDEA



privacyID3A
AUTHENTICATION SYSTEM

- Webinterface für Token-Verwaltung
 - OpenSource
 - viele verschiedene Token-Typen (TOTP/HOTP, Push, Email, FIDO, Yubikey, ...)
 - Anbindung via RADIUS, SAML, LDAP-Proxy
 - funktioniert ohne Azure/Cloud und auch ohne Internet-Anbindung
 - Windows Credential Provider
 - <https://github.com/privacyidea/privacyidea-credential-provider/releases/tag/v3.1.2>
 - kostenpflichtig mit Lizenz-Datei (wird im Webinterface hinterlegt)
 - MSI-Datei oder manuelle Installation (DLL-Datei plus Registry-Einträge)

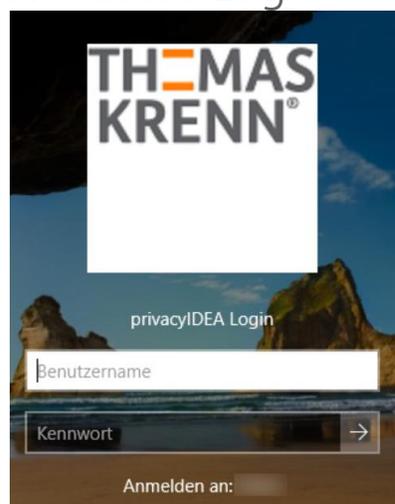


le: <https://privacyidea-credential-provider.readthedocs.io/en/latest/>

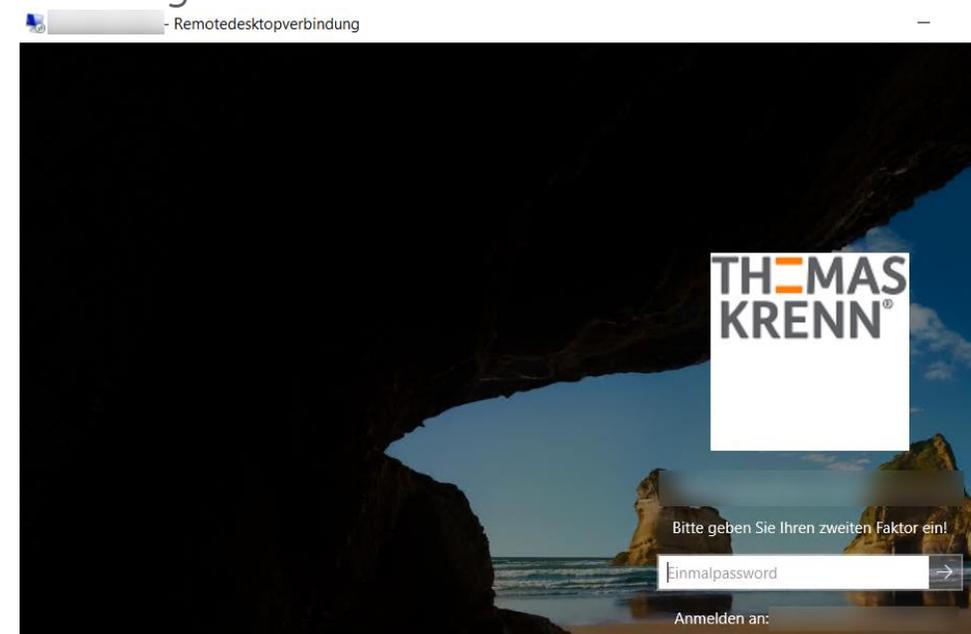


Windows 2FA mit privacyIDEA

- für RDP „two_step_hide_otp“ in Registry aktivieren
- default_realm, show_domain_hint, excluded_account (z.B. „\Administrator“)
- Windows Login



RDP-Login



Quelle: <https://privacyidea-credential-provider.readthedocs.io/en/latest/>

SAVE THE DATE:
Jahresrückblick
am 20.1.2022
10 Uhr

**THOMAS
KRENN®**

Vielen Dank für Ihre
Aufmerksamkeit!

