(Secure) Active Directory concepts

(Marc Grote)
Consultant, Trainer, Buchautor, Mensch

Version 1.0 – 01.01.0001

Über www.IT-Visions.de

- Expertennetzwerk mit Schwerpunkt auf Web & Microsoft:
  - HTML5, JavaScript, .NET, Visual Studio, TFS, Xamarin
  - SQL Server, SharePoint, BizTalk, CRM, Azure, Sicherheit
  - Windows Client & Server, Exchange Server, PowerShell
  - OOAD, ALM, Scrum, Design & Usalibity, Java, MySQL, Oracle, Linux
- Top-Experten mit großer Praxiserfahrung (viele davon Buch- und Fachzeitschriftenautoren, Konferenzredner, MVPs)
- Gegründet 1996
- Geleitet von Dr. Holger Schwichtenberg (MVP)
- Tätigkeiten
  - Softwareentwicklung
  - Strategische und technische Beratung
  - Individuelle, maßgeschneiderte technische Schulungen
  - Strategie-Vorträge (Management-Level)
  - Coaching bei Entwicklungsprojekten und Prototyp-Workshops
  - Support (Telefon/Online)
- Telefon: 0201 / 649590-0 (Mo-Fr, 9 bis 17 Uhr)

(MARC GROTE)

Kundenbeispiele

SIEMENS
ERGO
Roche
Continental
T
MAN
Niedersachsen
COMMERZBANK
ZEISS
thyssenkrupp
HUK-COBURG
eurofins
Deutsche Post
BOSCH
BAYER
RWE
Dräger
DB
AIRBUS GROUP
arvato BERTELSMANN

Unsere Kunden (Auswahl)

SIEMENS
ZEISS
AIRBUS GROUP
arvato BERTELSMANN
Niedersachsen
ZF
BAYER
Roche
Dräger
BOSCH
sage
GROB
ERGO
thyssenkrupp
Microsoft
VOITH
Deutsche Post
Merckle
T
MAN
UNISYS
eurofins
CONCORDIA Versicherungen
Sparda-Banken freundlich & fair
OBI
HUK-COBURG Aus Tradition günstig
REWE
ABB
Lufthansa
QIAGEN
AXA
JENOPTIK
MTU Aero Engines
HESSEN
Atos
Buderus
DB
RWE
HILTI
INTERNATIONALE LKW WALTER TRANSPORTORGANISATION AG
BREMER LANDESBANK
AOK Die Gesundheitskasse.
SMA
KARSTADT
WEMPE
GDV DIE DEUTSCHEN VERSICHERER
stratec biomedical
EVONIK INDUSTRIES
Fraunhofer
universa VERSICHERUNGEN
UBS
adesso business. people. technology.
CLAAS
FESTO
viega
TÜV SÜD
BOMBARDIER the evolution of mobility
Continental
Alles Gute. KVBW
Imperial College London
POLIZEI BAYERN
HUGO BOSS
LS telcom
DEA Deutsche Erdöl AG
ING DiBa Die Bank und Du
DACHSER Intelligent Logistics
GAGFAH GROUP
COMMERZBANK

Referentenvorstellung

- Marc Grote
- Erster Rechner 1984 / seit 1989 hauptberuflich ITler / Seit 1995 Selbststaendig / ab 2022 Rentner
- MVP Forefront (2004-2014), MVP Hyper-V (2014), MVP Cloud and Datacenter (2015-2017), Microsoft MCT/MCSE Messaging/Security/Server/MCLC /MCITP*/MCTS*/MCSA*/MC*
  MCSE Private Cloud, Productivity, Cloud Platform and Infrastructure, Server Infrastructure, Exchange
  MCS Server Virtualization Hyper-V / System Center/ Azure
  MCITP Virtualization Administrator
- Buchautor und Autor fuer Fachzeitschriften
- Schwerpunkte:
  - Windows Server Hochverfuegbarkeit/Virtualisierung/Security
  - Exchange Server seit Version 5.0
  - System Center VMM/SCEP/DPM
  - von *.Forefront reden wir nicht mehr ☹

(MARC GROTE)

Vorstellungsrunde

- Wer sind Sie?
- Was ist Ihre Taetigkeit hier?
- Welche Vorkenntnisse haben Sie (Active Directory / Security)?
- Was erwarten Sie von diesem Workshop?

Workshopzeiten

- 09:00 – 10:30
  - Pause 15 Minuten
- 10:45 – 12:15
  - Pause 15 Minuten
- 12:30 – 13:00
  - Mittagspause 0,5 Stunden
- 13:30 – 15:00
  - Pause 15 Minuten
- 15:15 – 16:00

(MARC GROTE)

Schulungs-FAQ

Folienpräsentation?	Nein
Live-Vorführungen („Demos")?	Nein
Teilnehmerübungen („Hands On")?	Nein
Bekommen wir die Folien?	Ja, wenn es sich lohnt?
Zwischenfragen?	Gerne, jederzeit ☺ → ggf. Fragenspeicher
Wunschthemen?	Ja, sofern es die Zeit erlaubt!
Zeit für Fragen am Ende?	Ja!
Bekommen wir Teilnehmerzertifikate?	Ja, der Auftraggeber der Maßnahme hat einen Link zu unserem Webportal bekommen, wo er die Zertifikate anfordern kann. Wenn er dort Ihren Namen einträgt, bekommt er ein Zertifikat für Sie zugeschickt.

(MARC GROTE)

Noch irgendwas unklar?

(MARC GROTE)

Ok, dann:

Auf die Plätze, fertig…

(MARC GROTE)

Gliederung des Workshop

- Sichtung des IST Zustands
- Spezielle Fragestellungen
- Active Directory Security Design
- Vorstellung Active Directory Admin Modelle
- Betrachtung ganzheitlicher Ansatz
- Diskussion / Entscheidung weitere Vorgehensweise

Sichtung des IST Zustands

- AD
- Applikationen
- Third Party

Spezielle Fragestellungen

- Single Sign On (SSO)
- Multi Faktor Authentifizierung
- Admin Tier Modell besprechen
- Microsoft ESAE
- Exchange Anbindung an die Cloud

Multi Faktor Authentifizierung

- Azure MFA
- Third Party MFA (Duo Security u. a.) – moegliche Cloud Anbindung beruecksichtigen

Exchange Anbindung an die Cloud

- Cloud only (https://docs.microsoft.com/de-de/office365/enterprise/office-365-integration)
- Hybrid Bereitstellung (https://docs.microsoft.com/de-de/exchange/hybrid-deployment-prerequisites)

Active Directory Security Design

Active Directory Security Design

Clean Source – PAW – Reduzierung Admin Konten – FGPP fuer Admin- / Servicekonten – Dedizierte Service Accounts – Einsatz von MSA und/oder GMSA – Domain Controller Hardening – RODC? – Monitoring – regelmaessige Health Checks – AD Risk Assessment – Netzwerk Separierung - Backup und Wiederherstellung – Secure Time Source – AdminSDHolder - AD Delegation nutzen – Security mit GPO – sichere Protokolle (LDAPS, Kerberos, Zertifikate, Cipher Hardening) - SIEM (MS ATA) verwenden – Client Hardening – LAPS einsetzen – Secure RDS – AD Cleanup - Credential Caching verhindern – Patching – Windows Firewall – Kennwortrichtlinien – Klartextprotokolle vermeiden – Ueberwachungsrichtlinien - Microsoft Security Compliance Toolkit

Vorstellung Active Directory Admin Modelle

- Basic (Secure) Design – Single CORP Forest
- Tier Modell - Single CORP Forest – mit Tier
- PAM/MIM – PRIV Forest – CORP Forest - mit Tier
- ESAE – PRIV Forest – ESAE Admin Forest - mit Tier

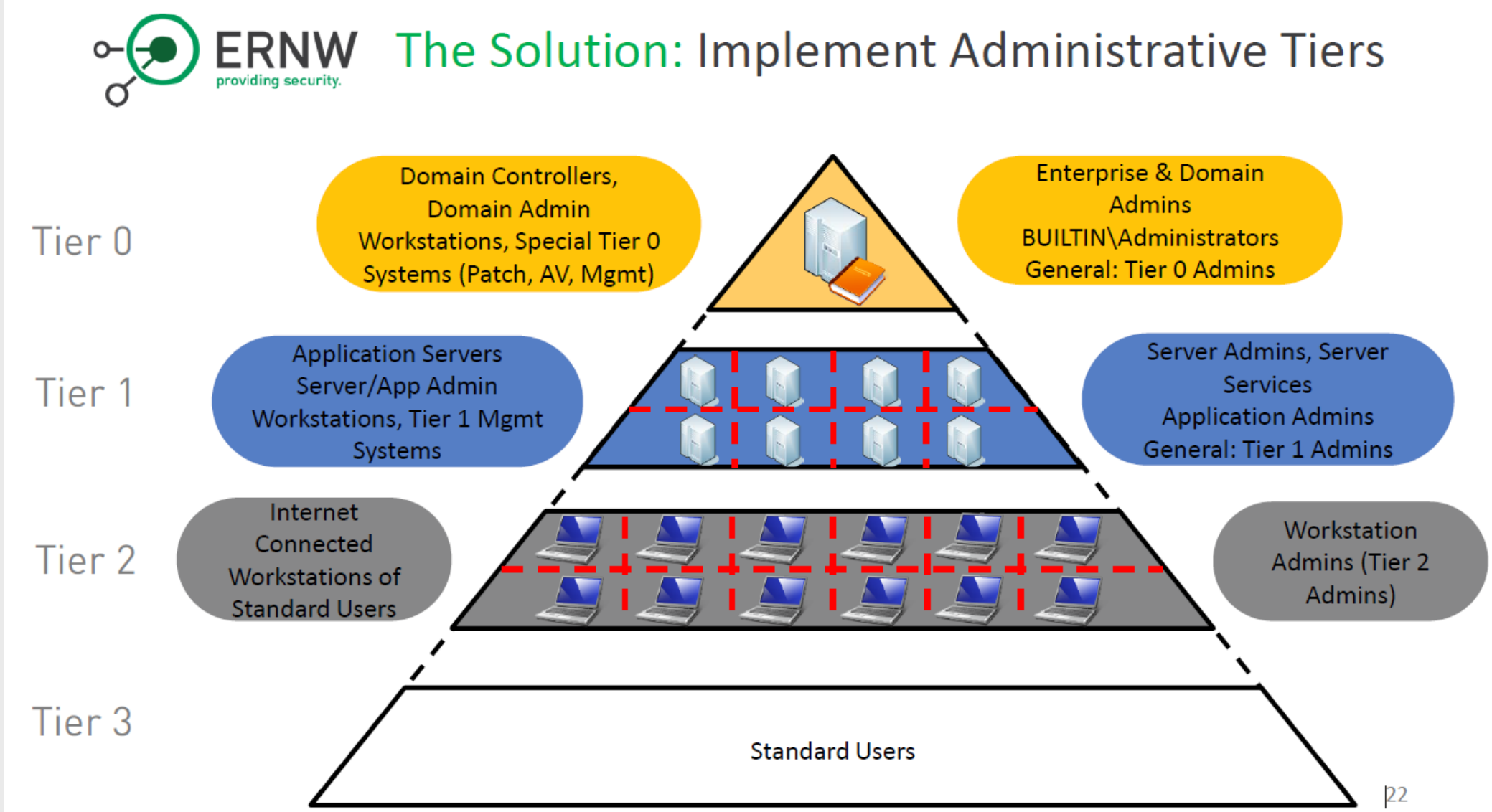
Basic (Secure) Design

- Least Privileged Permisson/Access Design
- Reduzierte Admin Accounts (Protected User Group)
- Admin Accounts von User Accounts trennen
- AD Delegation verwenden
- Service Accounts einsetzen
- Group Policies sinnvoll einsetzen
- Ueberwachungsrichtlinien
- PAW Workstation
- Windows Firewall
- Netzwerk Separierung (Server/Clients/Infrastruktur)

Tier Modell

- Die Administrationshoheit des Allmacht Admins wird aufgeteilt/unterbunden auf einzelne Ebenen
- Die Berechtigungen im Active Directory werden „partitioniert"
- Standard = Tier0 / Tier1 / Tier2
- Tier0 = Enterprise Admin, Domain Admin, Domain Controller
- Tier1 = Server Admins, Anwendungs Admins, Exchange Tier0 wenn kein RBAC bei Installation!!, Anwendungs-Server
- Tier2 = Workstation Admins, Standard User / Workstation
- Single Forest
- https://www.frankysweb.de/active-directory-einfache-manahmen-fr-mehr-sicherheit-teil-1/

Tier Modell


ERNW
providing security.
The Solution: Implement Administrative Tiers
Tier 0
Domain Controllers, Domain Admin Workstations, Special Tier 0 Systems (Patch, AV, Mgmt)
Enterprise & Domain Admins BUILTIN\Administrators General: Tier 0 Admins
Tier 1
Application Servers Server/App Admin Workstations, Tier 1 Mgmt Systems
Server Admins, Server Services Application Admins General: Tier 1 Admins
Tier 2
Internet Connected Workstations of Standard Users
Workstation Admins (Tier 2 Admins)
Tier 3
Standard Users

Tier Modell

ERNW providing security. Tier Model Principles

Classify: *Every single* security principal, system, or application **has to be classified as belonging *only* to one tier**

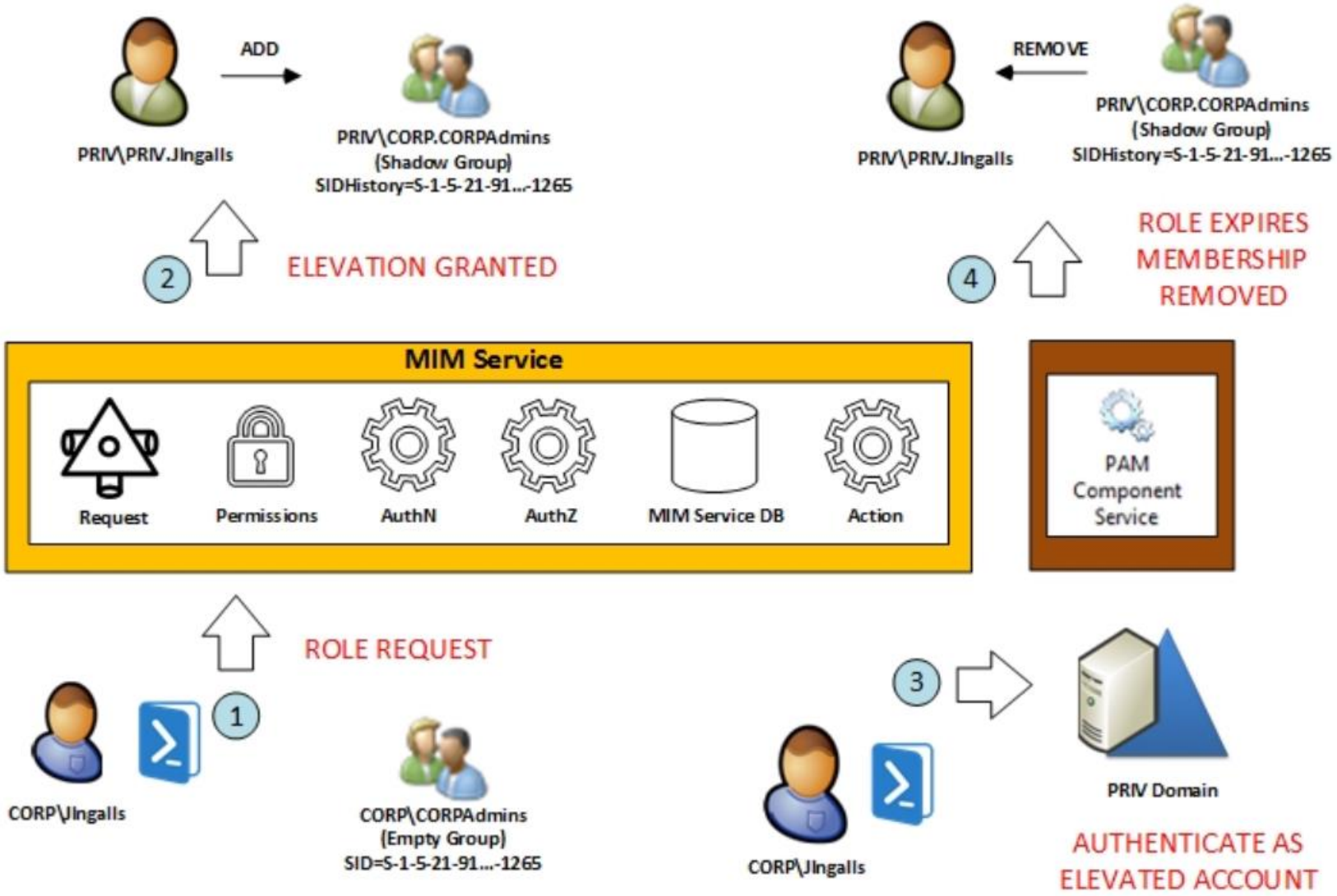
Restrict Logons: Security principals of a higher tier ***must never log on to* a resource on a lower tier** (→ Implement logon restrictions)

Restrict Control: Security principals of a lower tier ***must never control* resources of a higher tier** (→ Implement control restrictions)

PAM / MIM

- Privileged Access Management (PAM)
- PRIV Forest mit sensitiven Admin Accounts
- CORP Forest mit den normalen Ressourcen
- Verwendung von Shadow Security Principals
- Microsoft Identity Manager (MIM) provisioniert sensitive Admin Accounts von PRIV in CORP Forest
- JIT und JIA
- https://docs.microsoft.com/de-de/microsoft-identity-manager/pam/principles-of-operation

PAM / MIM

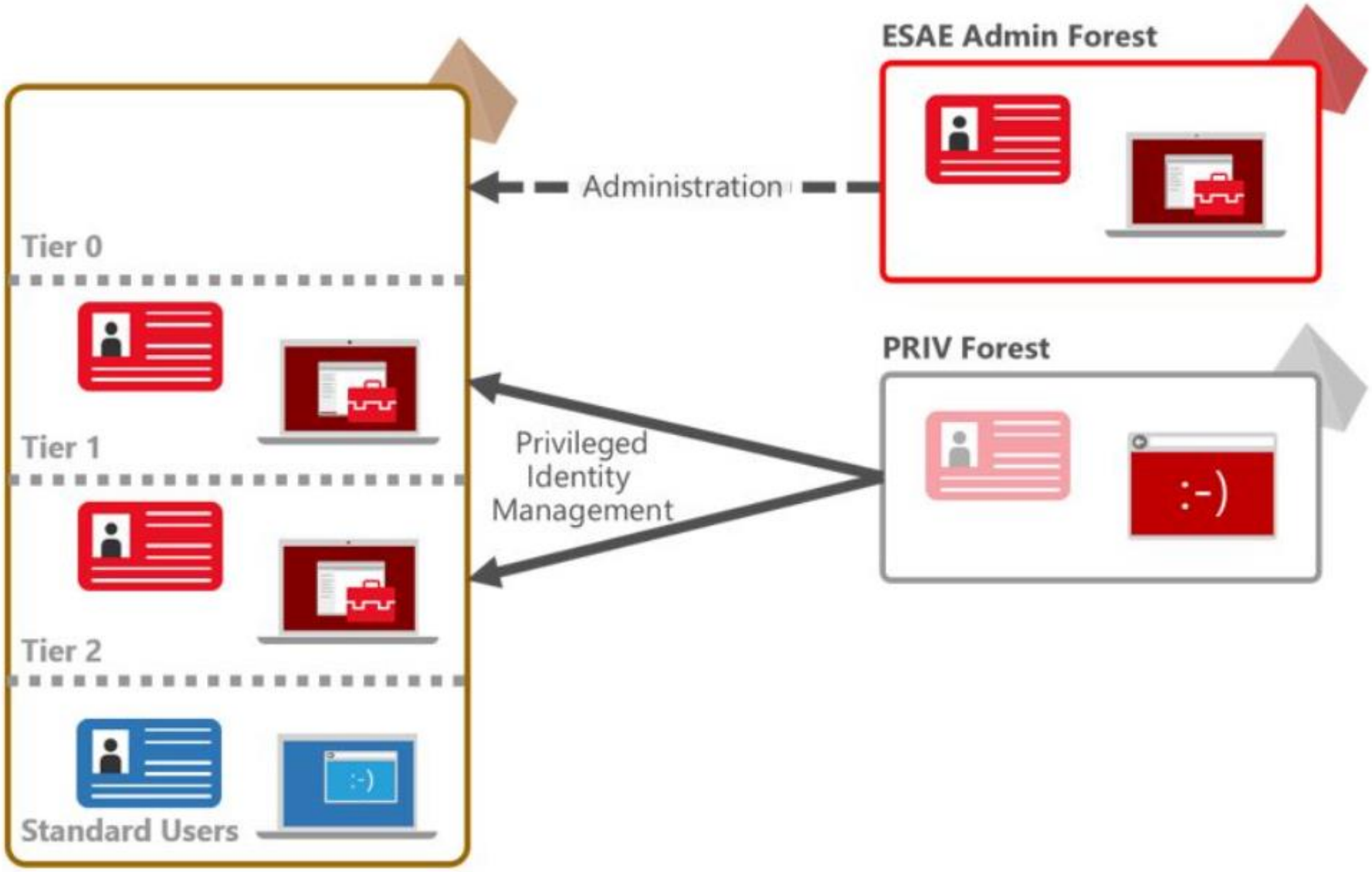


Quelle: https://social.technet.microsoft.com/wiki/contents/articles/33363.mim-2016-privileged-access-management-pam-faq.aspx

ESAE

- Enhanced Security Administrative Environment
- PRIV Forest – ESAE Admin Forest - mit Tier
- https://www.ntsystems.de/asai.html

ESAE



Quelle: https://docs.microsoft.com/de-de/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

AD-Ablaufplan-HighLevel-v1.docx

Betrachtung ganzheitlicher Ansatz

- Security 101
- Physikalischer Schutz
- Organisation / Management
- Awareness / Schulung
- Client Schutz / Hardening
- DLP/DRM
- Backup und Wiederherstellung
- Firewall/Proxy/Content Handling
- Cim-endpoint.pptx

Diskussion / Entscheidung weitere Vorgehensweise

- Am Ende des Tages sollte ein Fahrplan fuer die weitere Vorgehensweise existieren
- Klarheit ueber das zukuenftige Konzept existiert

Brauchen Sie Unterstützung?

- .NET, Silverlight, WinRT, SQL Server, SharePoint, Windows Server, BizTalk, CRM, u.v.a. Microsoft-Produkte sowie HTML, JavaScript, Oracle, MySQL, PHP und Java u.v.m.
- Beratung bei Einführung, Migration und Betrieb
- (Vor-Ort-)Schulungen, Workshops
- Coaching (Vor-Ort | Telefon | E-Mail | Online-Meeting)
- Support (Vor-Ort | Telefon | E-Mail | Online-Meeting)
- Entwicklung von Prototypen und Lösung

http://www.IT-Visions.de
http://www.5minds.de
Telefon 0201/649590-0
info@IT-Visions.de

www.IT-Visions.de®
Dr. Holger Schwichtenberg

5Minds
IT-SOLUTIONS