
IT-P
IT-P
Design for Change:
Active Directory for the Cloud Age
Nils Kaczenski
Director Competence Center Microsoft
MVP Cloud & Datacenter Management
www.IT-P.de

IT-P


FAQ-O-MATIC.net
IT-P
MVP
Microsoft
Most Valuable
Professional

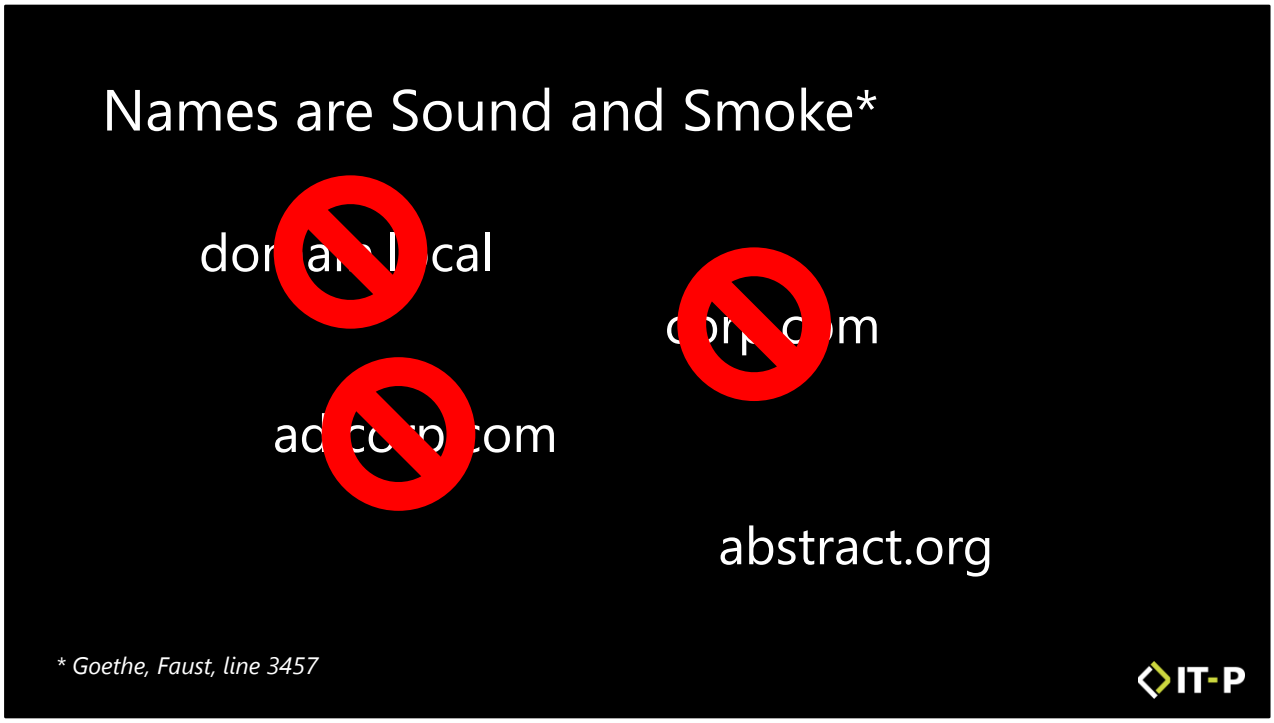
Aber was ist jetzt ein „wirklich gutes AD-Design“?

1

Design: The Foundation for Identities

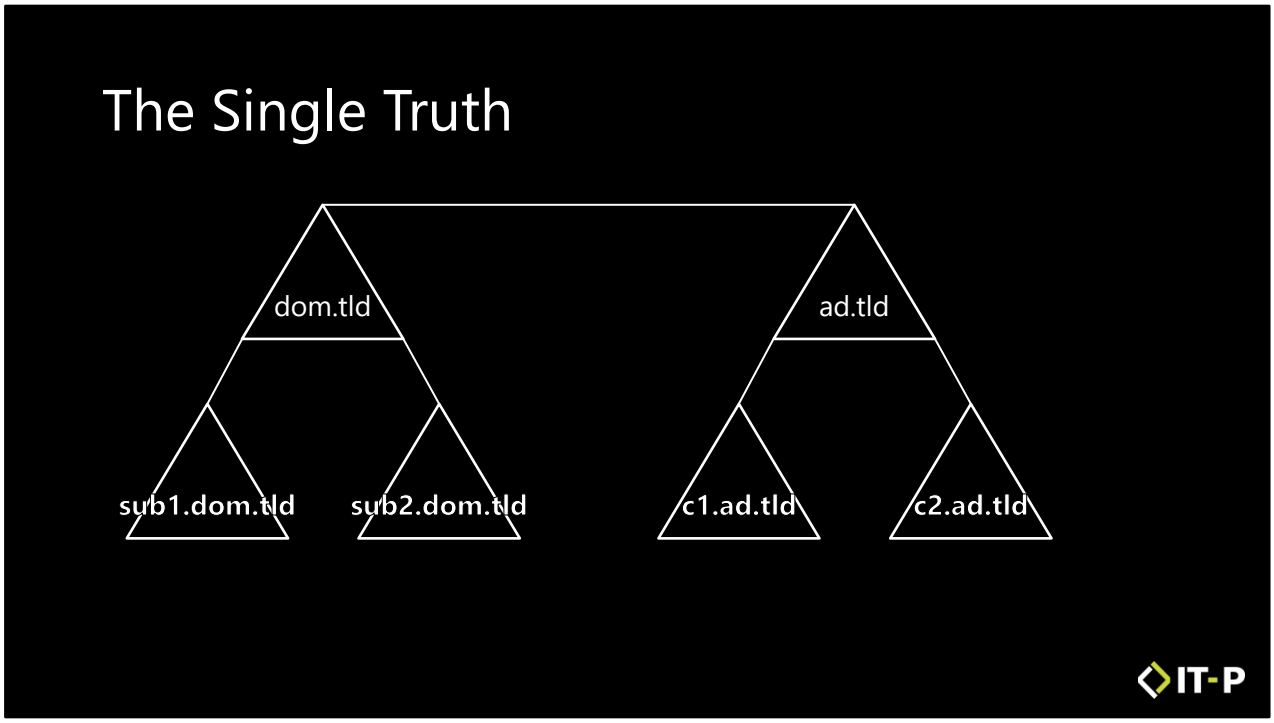
Aber was ist jetzt ein „wirklich gutes AD-Design“?

4



Abstrakter Name

- Varianten aufzählen
- Hinweis, was ein Rename bedeutet
- Learning: Niemals eine Domäne migrieren, nur um sie umzubenennen. Wenn man aber neu aufbaut, gleich einen „richtigen“ Namen nehmen.

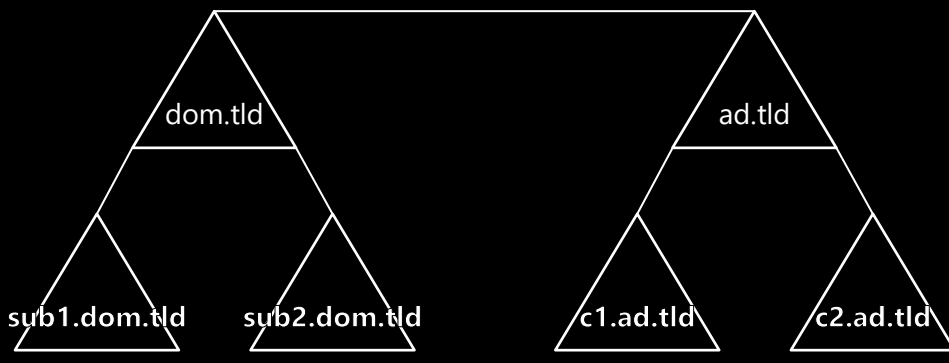


Single Domain Forest

Wiederholung: Domain, Tree, Forest

6

The Single Truth

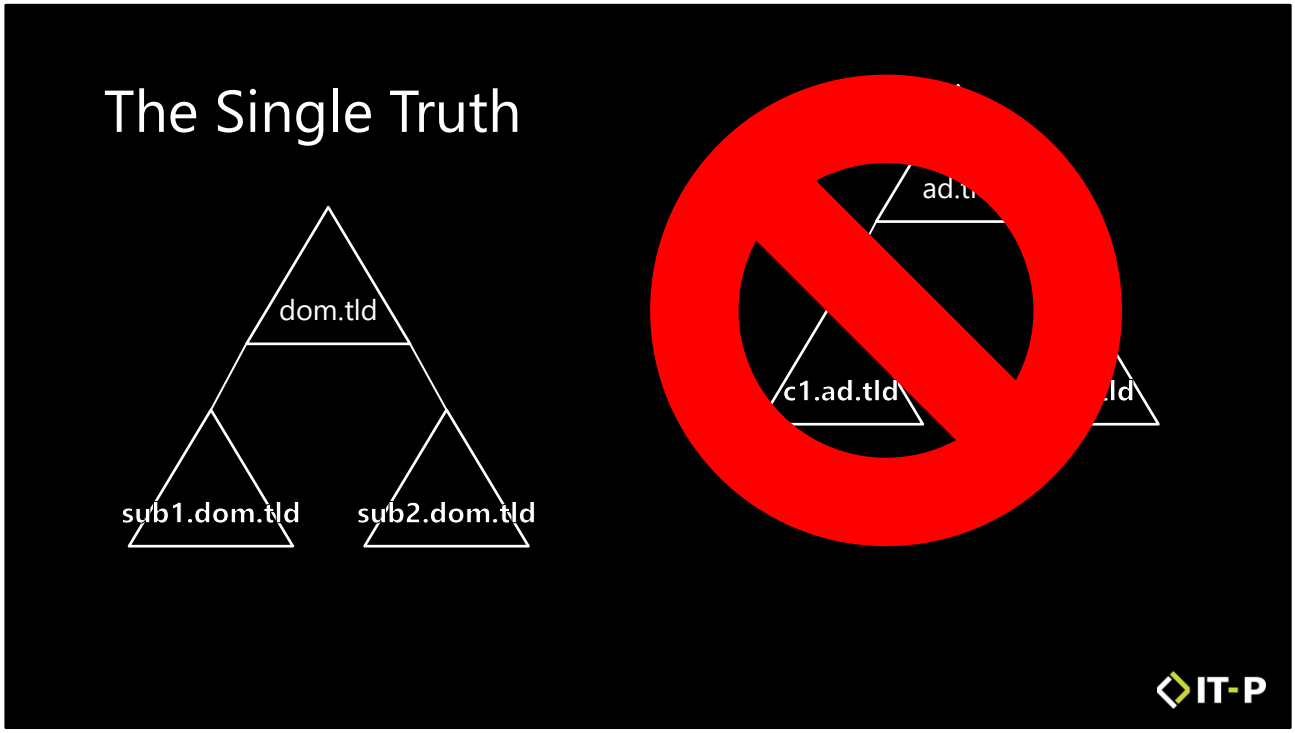


IT-P

Annahme: Man kann aus einem Forest einen Tree herauslösen, falls man einen Unternehmensteil verkauft

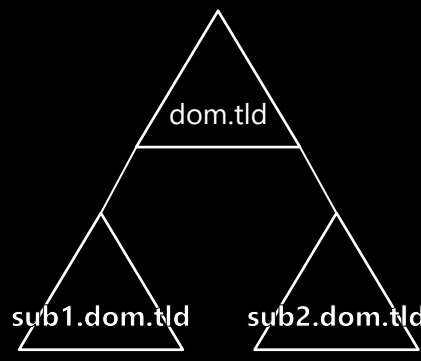
7

IT-P



Realität: Genau das geht nicht. Einmal Teil des Forests, immer Teil des Forests.

The Single Truth

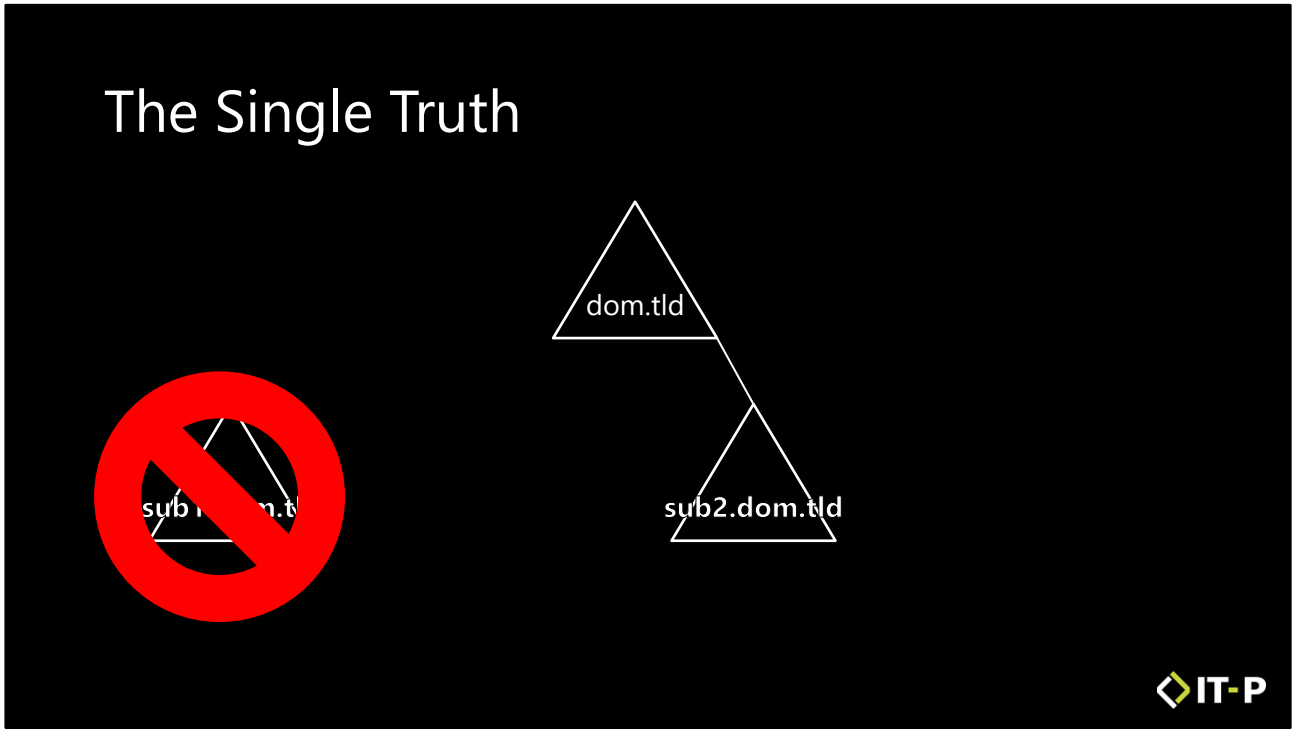


IT-P

Annahme: Man kann aus einem Tree eine Domain herauslösen …

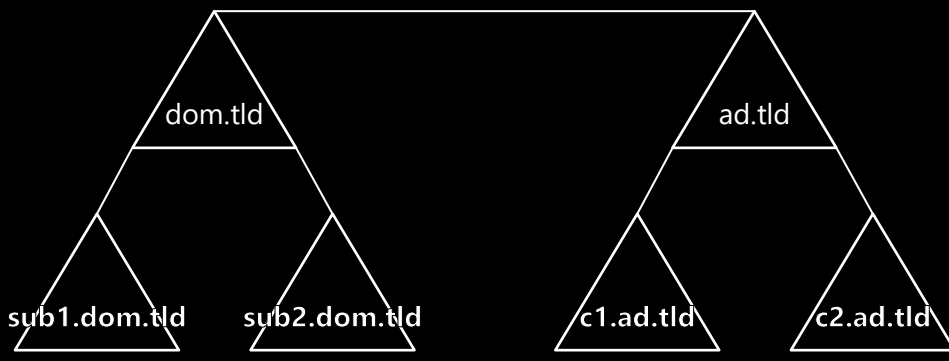
9

IT-P



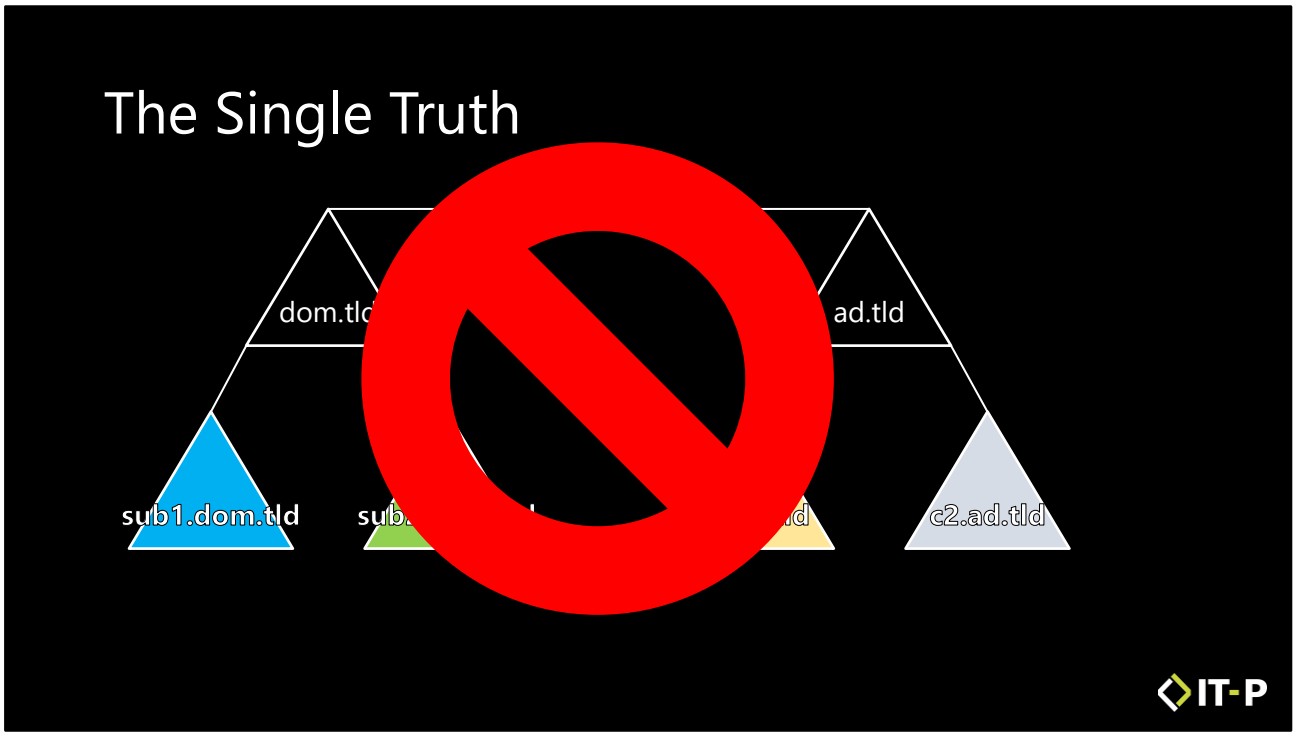
Nein, auch das geht nicht. Einmal Tree, immer Tree.

The Single Truth



IT-P

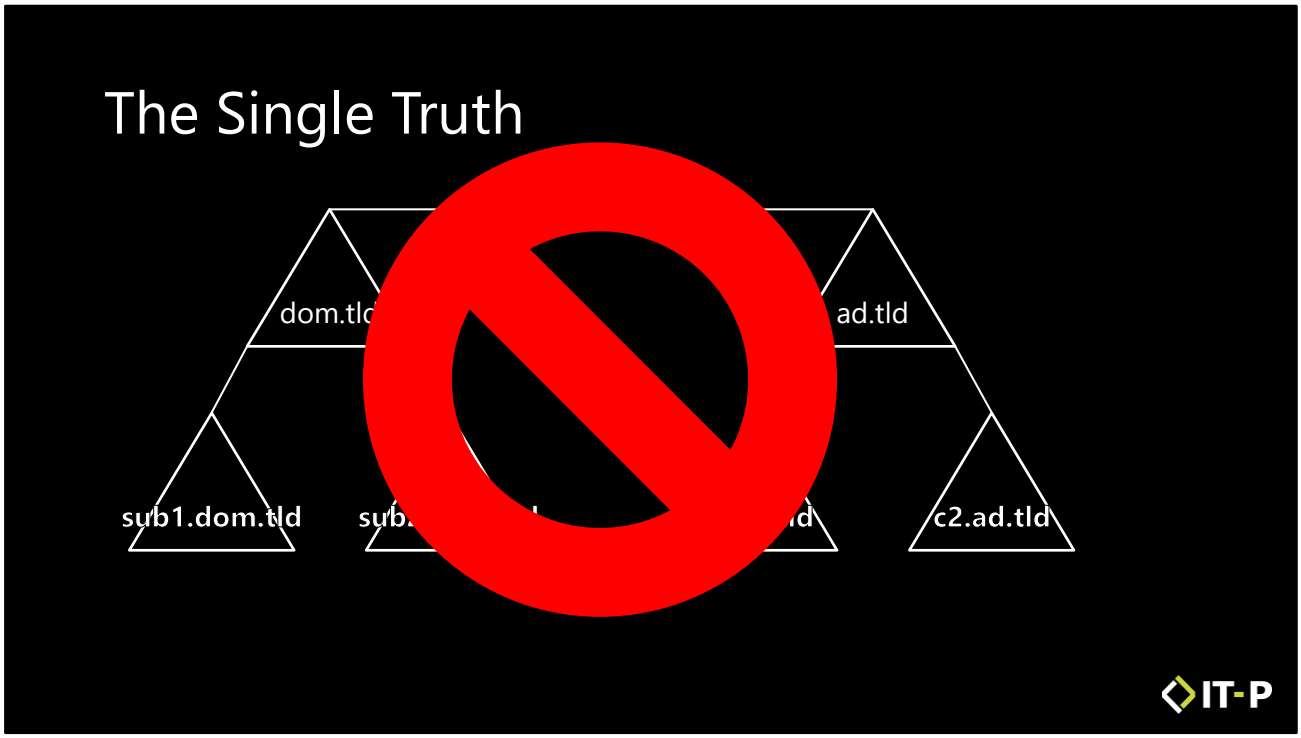
Annahme: Man kann ein AD in mehrere Domains aufteilen, um Sicherheitszonen für die Administration zu schaffen.



Realität: Nein, auch das geht nicht.

In einem Forest wird eine Sicherheitsaufteilung in Domänen wirkungslos (Enterprise Admins, automatische Trusts, Kerberos-Mechanismen, SID-Handhabung …).

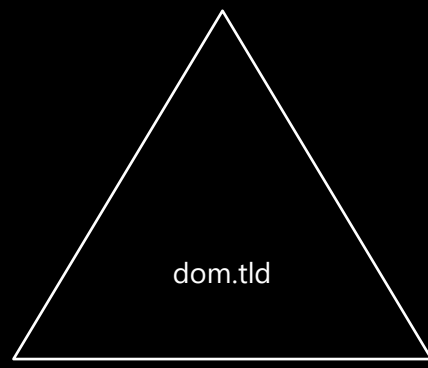
Die Domain ist keine Sicherheitsgrenze. Nur der Forest ist eine wirksame Grenze.



Ist ein Forest aus mehreren Domains also eine gute Idee?

Nein. Er hat keine Vorteile gegenüber den Strukturen, die man innerhalb einer Domäne bauen kann.

The Single Truth



Für neue Entwürfe oder für Konsolidierungen gilt also: Single Domain ist das einzige valide Modell.

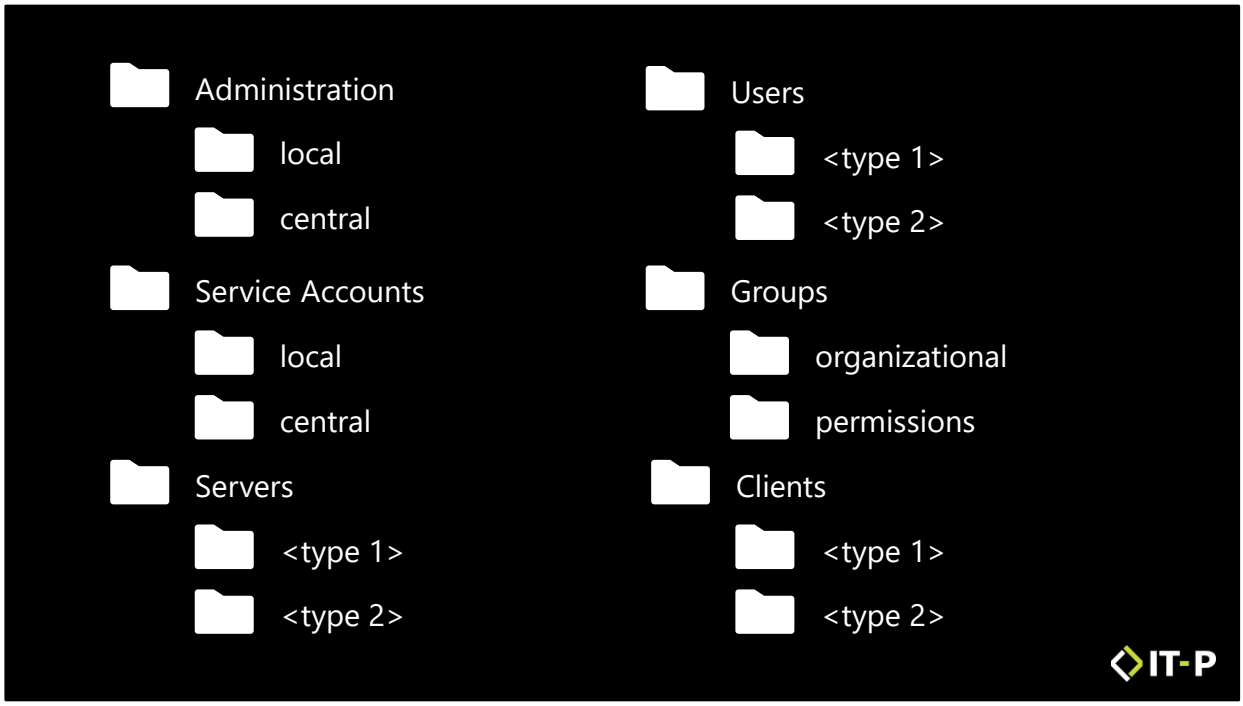
Einzige Ausnahme: Red Forest – aber da ist eben auch der Forest abgetrennt!

OU Tree ≠ Organization Chart

Objektorientierte OU-Struktur

- OU-Struktur ist nicht das Organigramm, sondern dient der AD-Administration

15

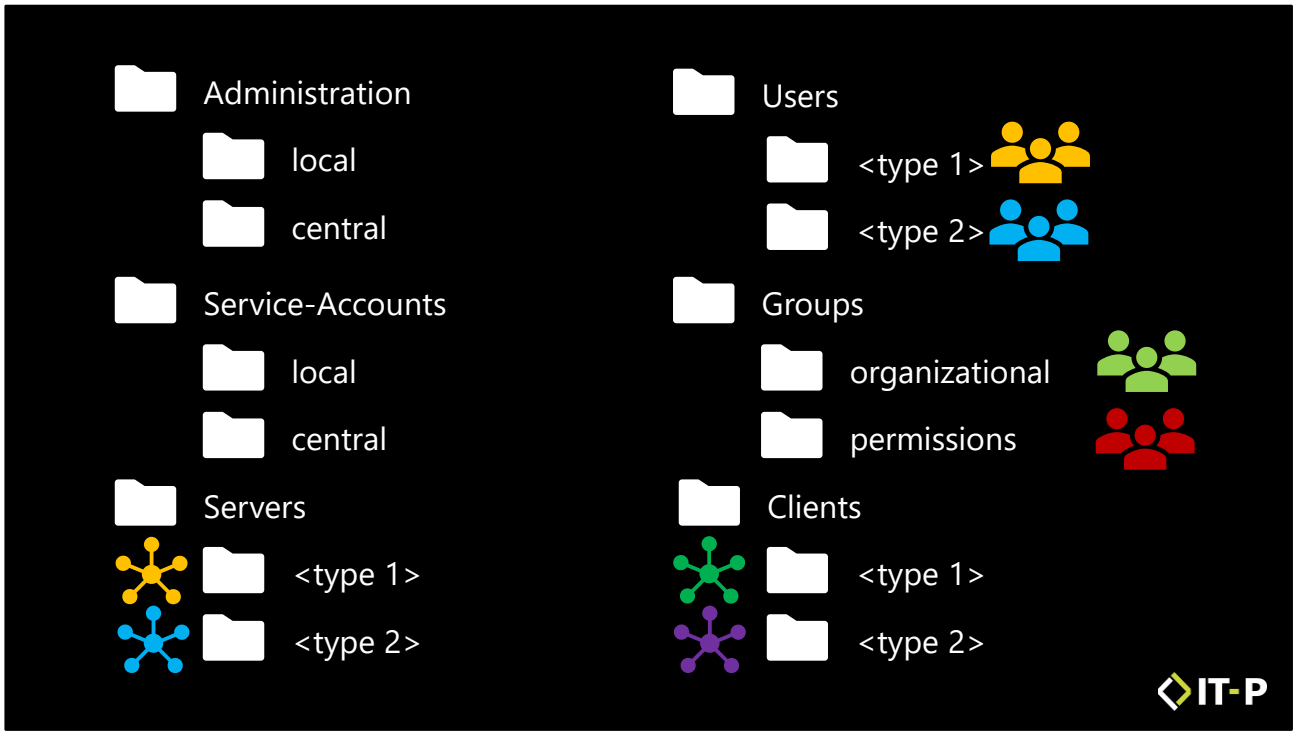


Bewährt hat sich: OUs nach Objektklassen aufbauen, alle weiteren Kriterien folgen optional als weitere Ebenen

Hier ein Vorschlag für ein Standard-Design als Ausgangspunkt

Pro-Tipp: Integrierte Dokumentation über "description"

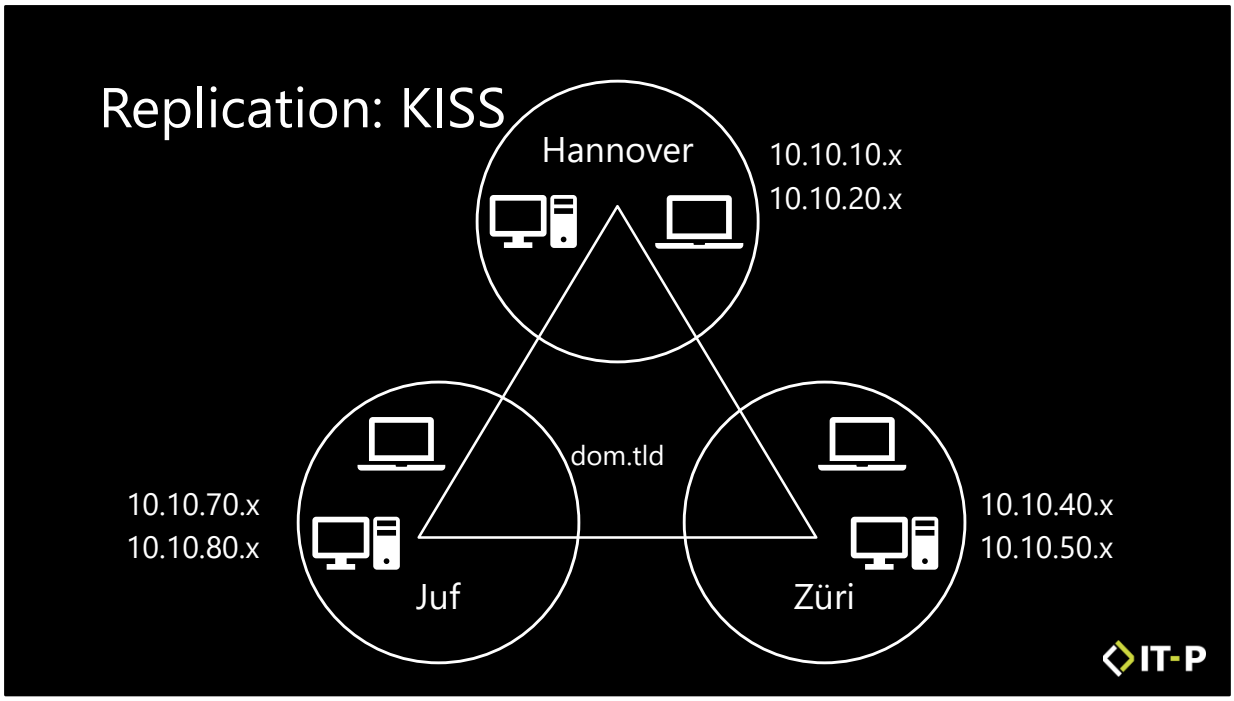
16



- Ansatz: Typen von Objekten –Sicherheitskriterien oder administrative Anforderungen
- Admin-Berechtigungen i.d.R. leichter und mit weniger Ausnahmen
- GPOs: Einstellungen leichter zuordnen
- Das gilt natürlich nicht immer – aber sehr oft so ein Modell

Und mein Organigramm?

- Zuordnung des „Managers“ (Vorgesetzte/r) beim User
- besser: Gar nicht im AD, weil dort nicht von Relevanz



Replikationsstruktur: KISS

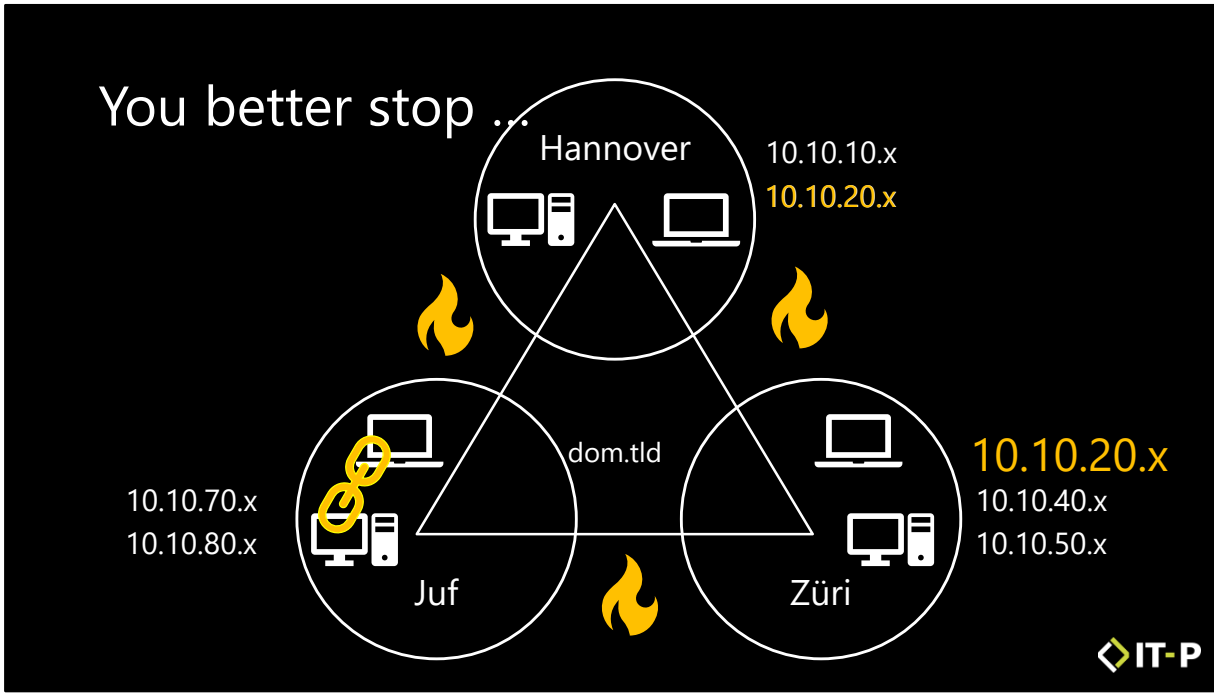
Grundlagen

Standards

- AD-Site nur wenn nötig
- Alle Subnets zuordnen
- Repl-Intervall 15 Minuten 24/7

Special: Multi-Domain

AD-Sites müssen gleiche Namen haben, um die Anmeldung zu steuern



Was man vermeiden sollte

- Uneindeutige Subnets
- Firewalls (erfordert Konfig in der FW und in der AD-Konfig)
- Einschränken der Replikation
- Client-Manipulation, um die Anmeldung zu steuern

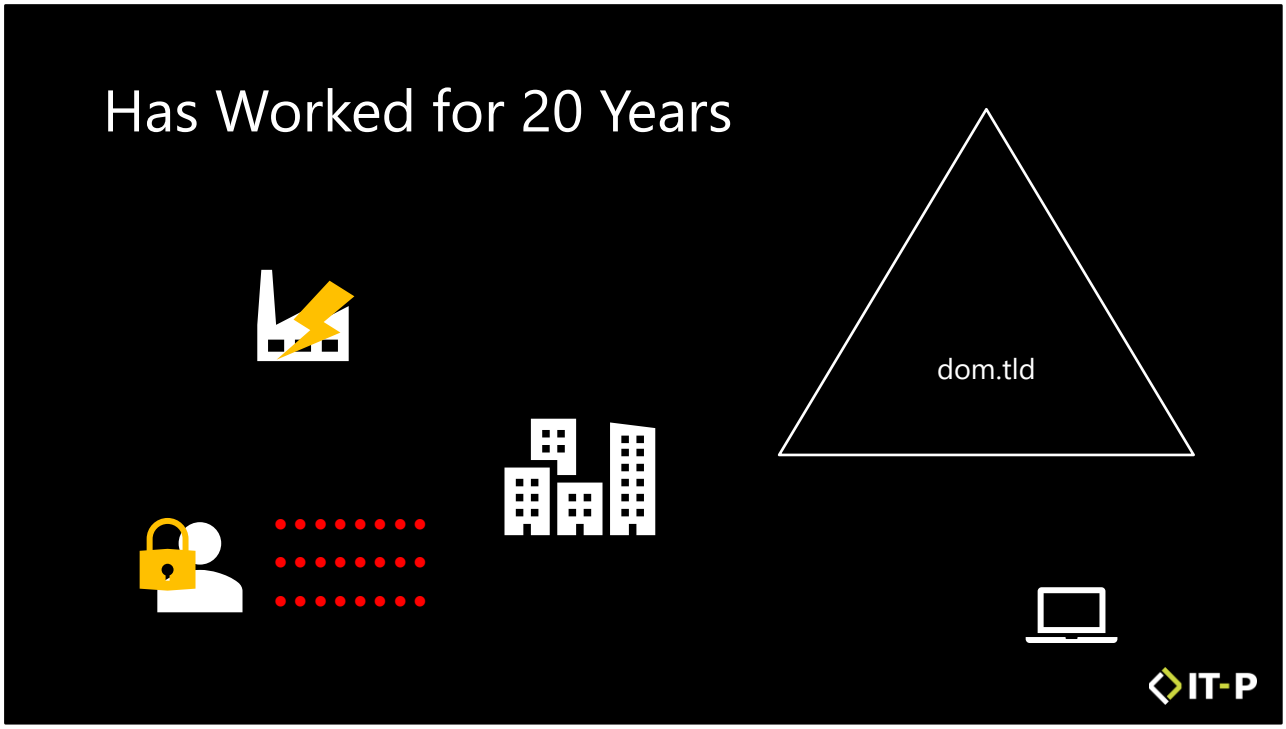
2

Security: (Attack -eq normal)

2 Sicherheit: Angriffe sind normal

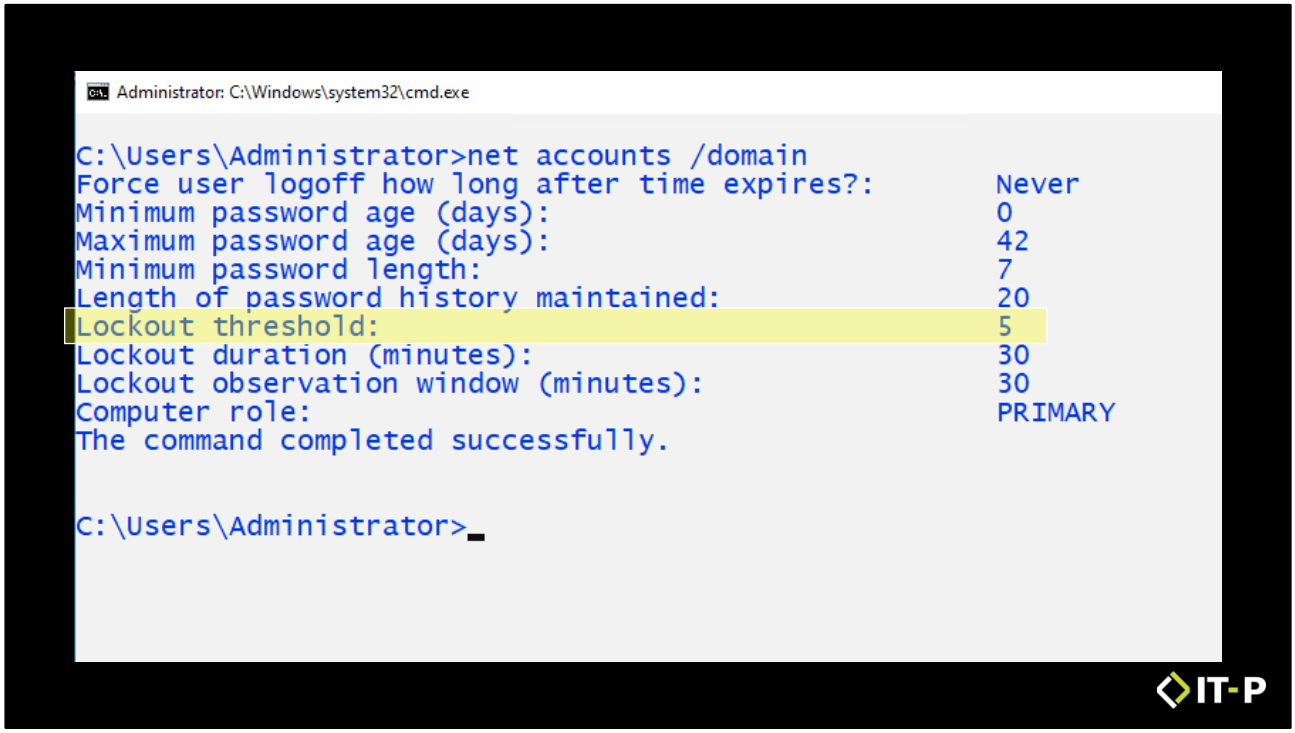
- Passwörter sind böse
- Der Browser und das Handy: Einfallstor für simple Angriffe (zu simple Kennwörter aus Bequemlichkeit)

20



Alt und bewährt: Angriffe, die seit 20 Jahren funktionieren

- Die Niederlassung als Extremrisiko
- Windows-Rechner in die Domäne aufnehmen
- Kontensperrung: DoS ernst gemeint



Wie der Kontensperrungs-DoS funktioniert …

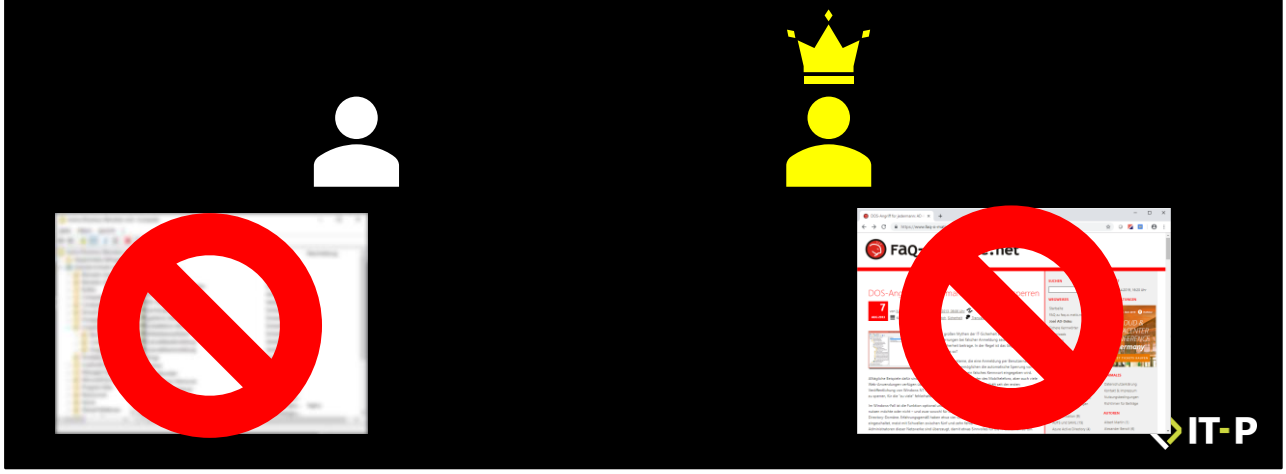
Separate Roles

Moderne Sicherheitskonzepte beruhen auf der Rollentrennung

Es gibt nicht mehr einen Account pro User, der im Zweifel alles darf

23

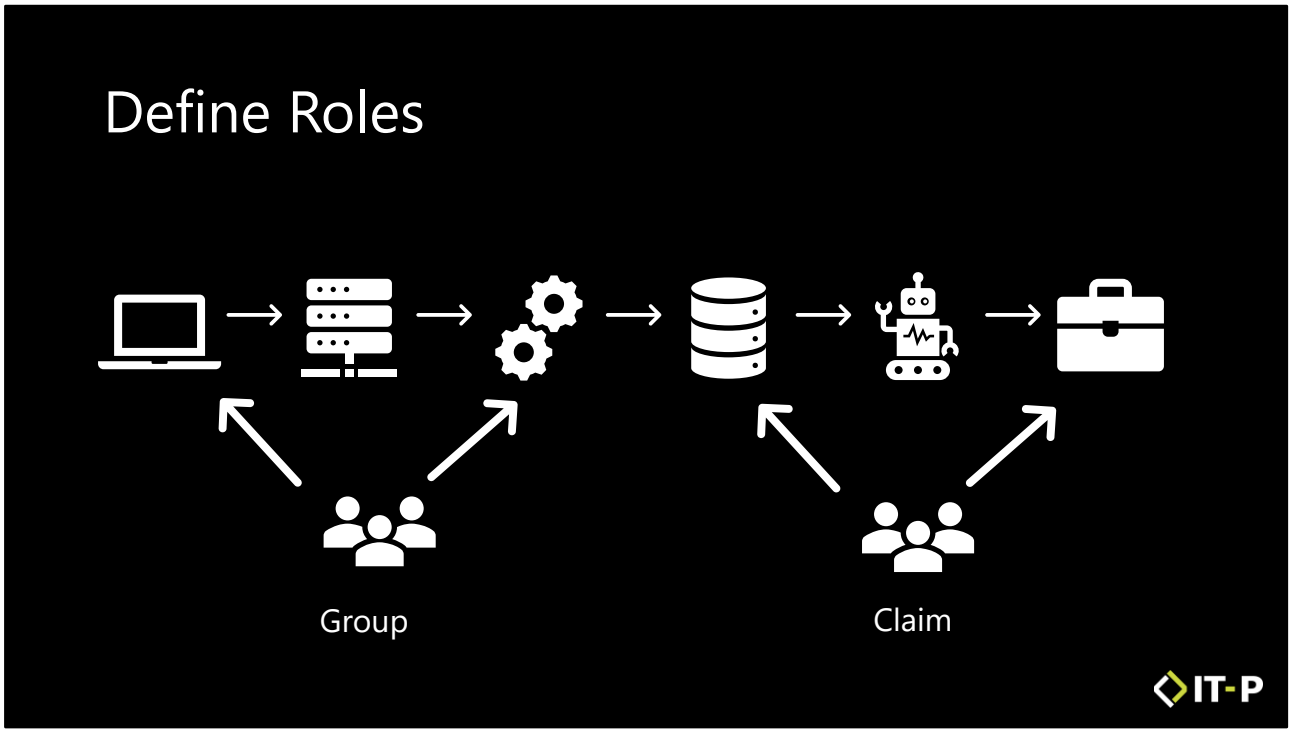
Separate Roles



Ansatz: pro Sicherheitsbereich ein separates Konto.
Wer also mehr darf als andere, hat mehrere Konten dafür.

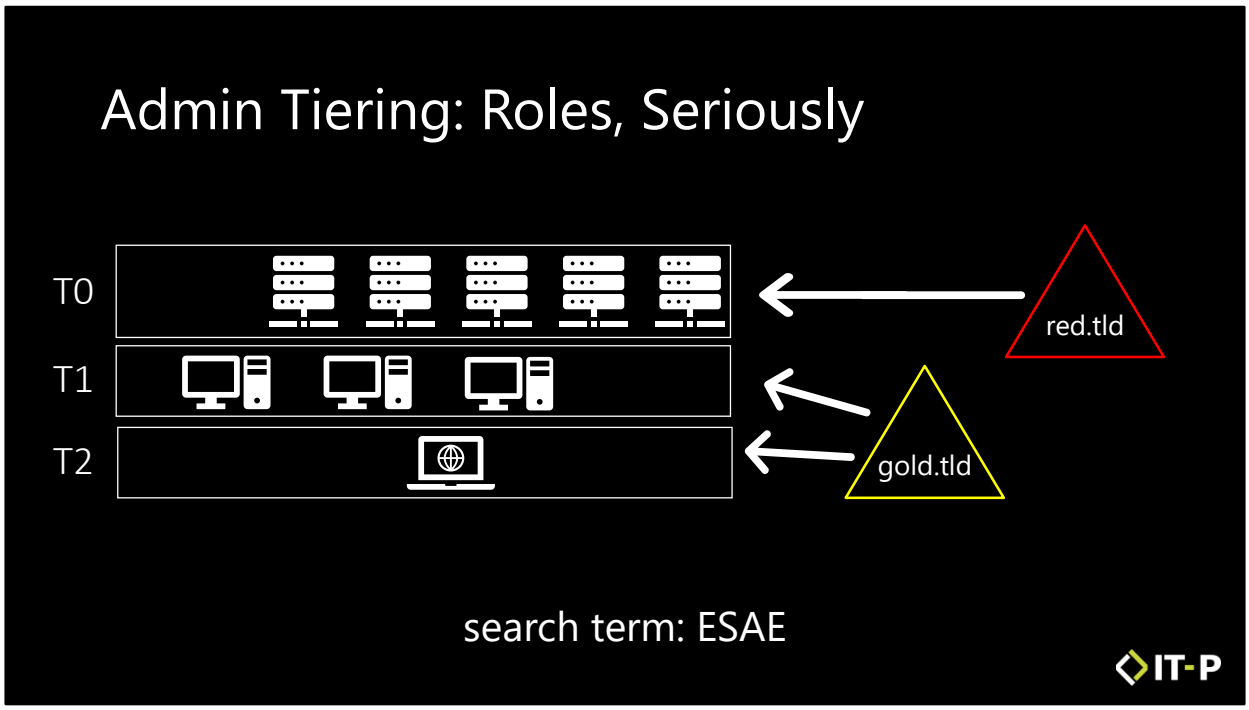
Minimal:

1. Konto für die Alltagsarbeit, „Office“ –keine administrativen Aufgaben, egal wo
2. Konto für die Administration – darf keine (anfälligen) Office-Aufgaben ausführen (kein Internet, keine Mailbox …)



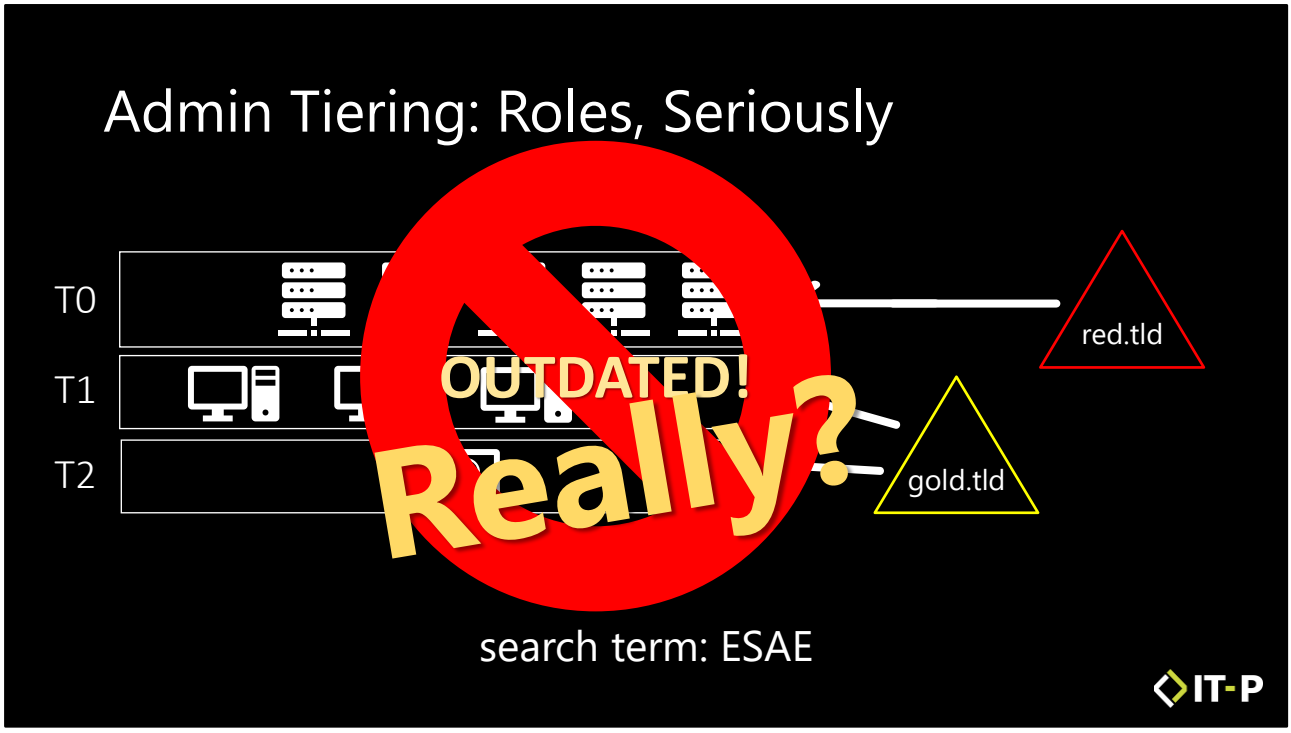
Wie kommt man zu einem Rollenkonzept?

- Der Teil, den Admins nicht mögen: Man muss mit den Fachabteilungen sprechen
- Frage: Wer braucht welche Daten und Funktionen?
- Ableiten: Rollen und Zugriffe
- Klassisch: Umsetzen mit Gruppen
- Manchmal flexibler: Umsetzen mit Claims – erspart Anhäufung von Gruppen, ermöglicht Szenarien, die mit Gruppen schwierig sind – kann aber technisch aufwändig werden



Rollentrennung ernst gemeint: Administrative Tiering

- Netzwerk in Sicherheits-Ebenen unterteilen
- Empfehlung: 3 Ebenen
- Ergänzend können Sicherheitszonen (vertikal) nützlich sein
- Jeder Account wird nur in einer Ebene (ggf. einer Ebene/Zone) verwendet



Rollentrennung ernst gemeint: Administrative Tiering

- Netzwerk in Sicherheits-Ebenen unterteilen
- Empfehlung: 3 Ebenen
- Ergänzend können Sicherheitszonen (vertikal) nützlich sein
- Jeder Account wird nur in einer Ebene (ggf. einer Ebene/Zone) verwendet

3

Hybrid Design: Cloud and Local

Was heißt das nun für die Anbindung der Cloud?

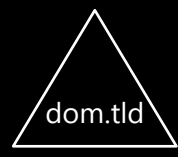
28

Identity is the New Perimeter

- Im Zentrum steht immer die Anmeldung, also die Identität. Habe ich die, so ist mein Zugriff definiert

29

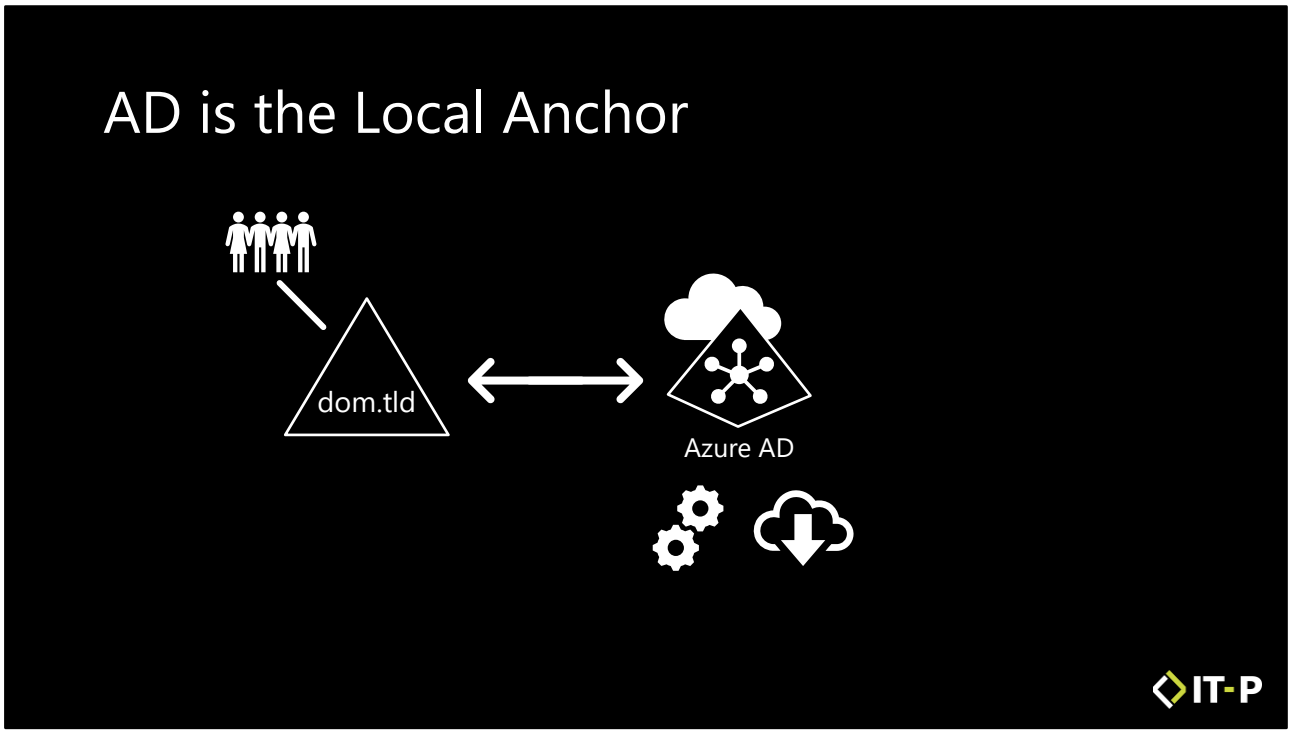
AD is the Local Anchor



AD als lokaler Anker für alle Identitäten

Auf mittlere Sicht wird ein lokales Verzeichnis weiter genutzt

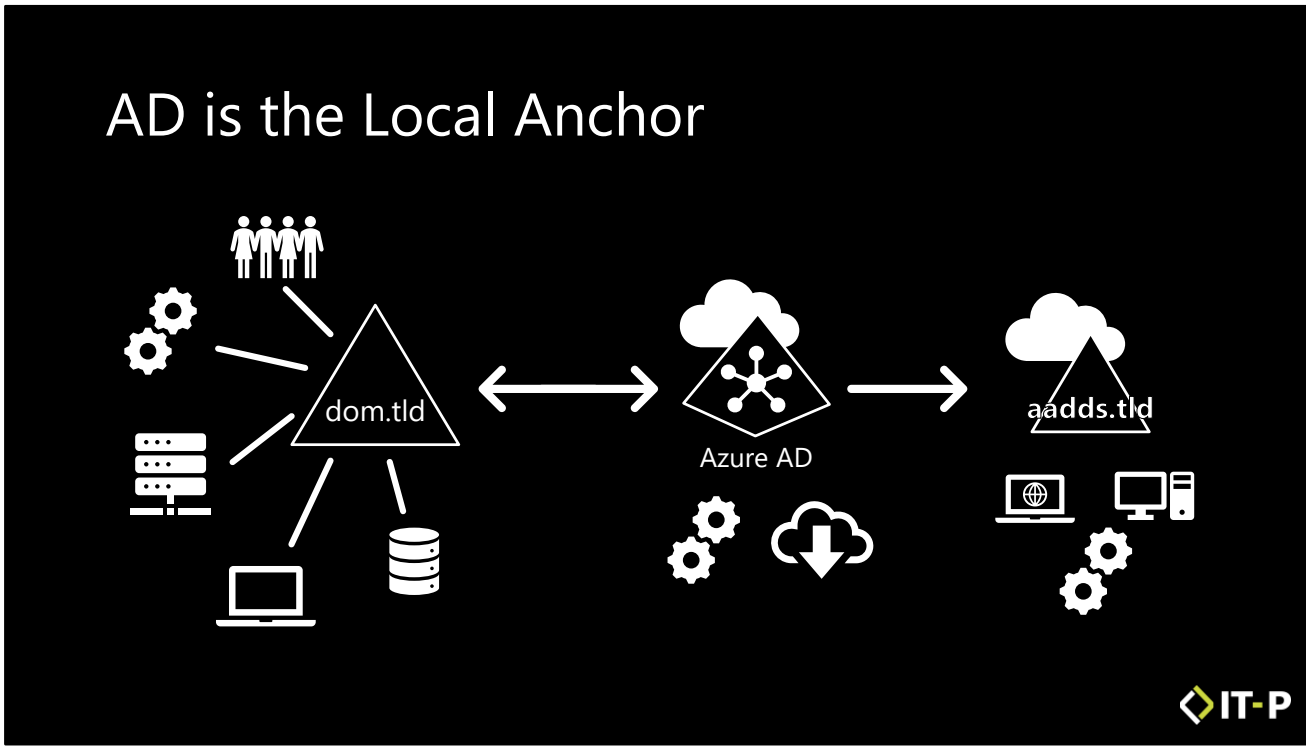
30



AD als lokaler Anker für alle Identitäten

AAD und AADDS sind kein Ersatz, sondern nur eine partielle, flache Abbildung

31

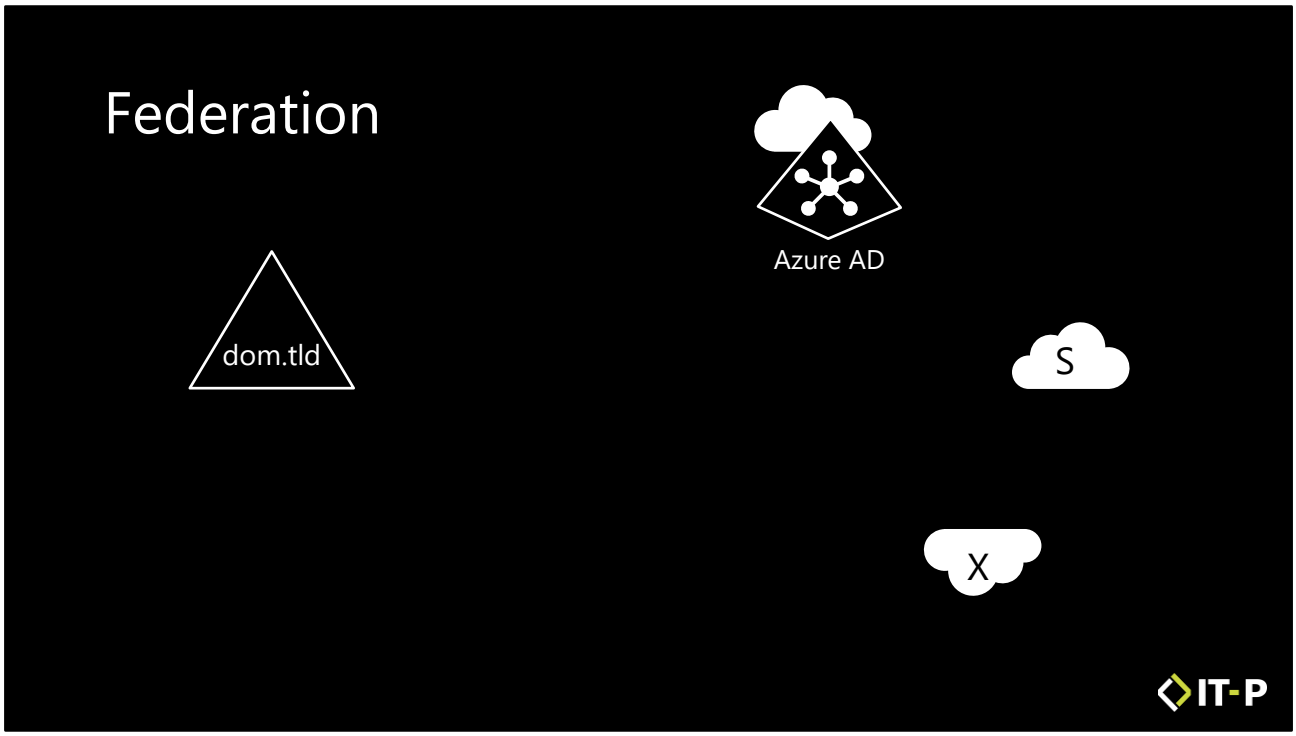


AD als lokaler Anker für alle Identitäten

Auf mittlere Sicht wird ein lokales Verzeichnis weiter genutzt

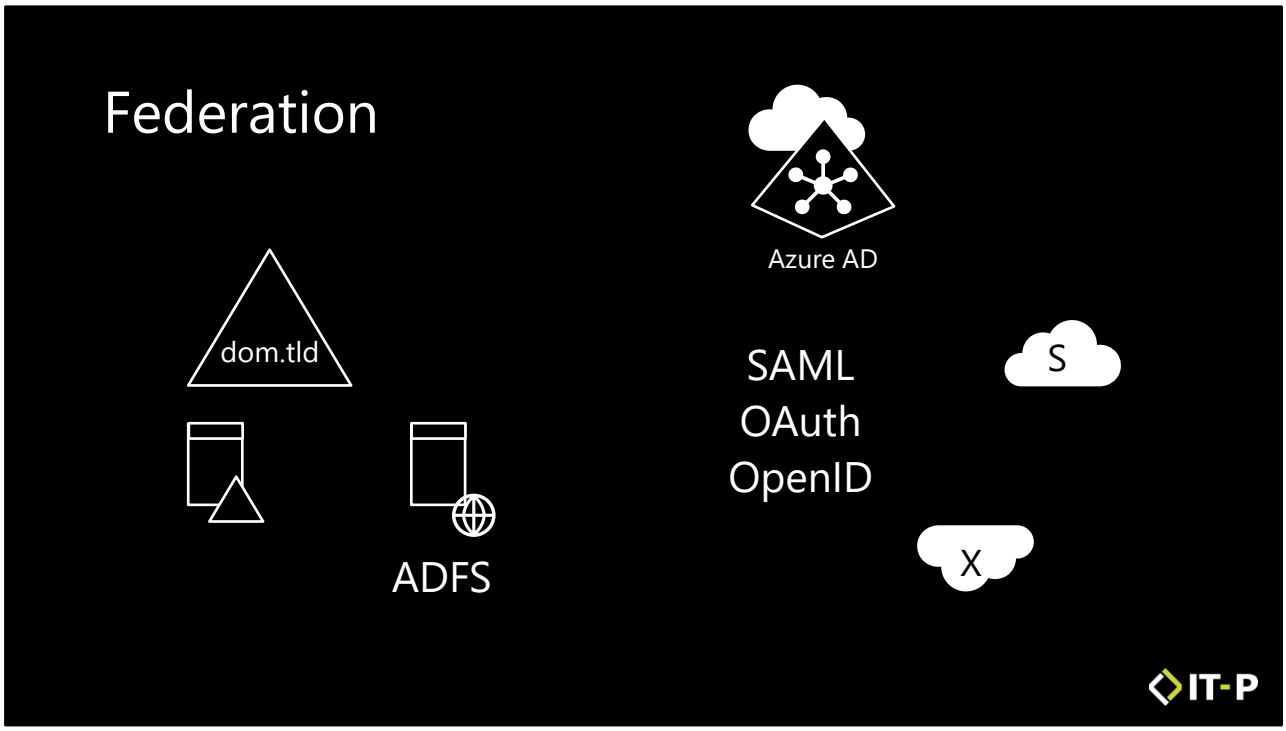
AAD und AADDS sind kein Ersatz, sondern nur eine partielle, flache Abbildung

32



Federation und Authentifizierung

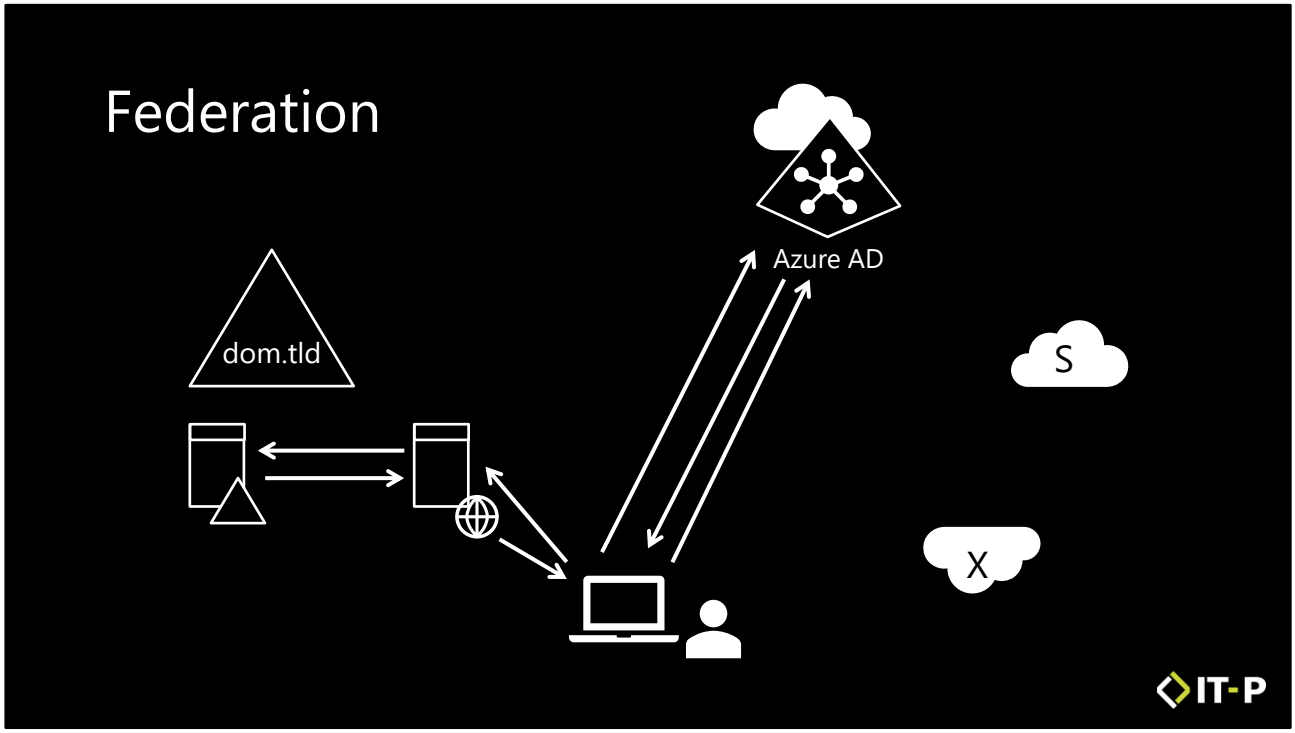
- Die Idee: Jeder Cloud-Service verlangt eine Anmeldung des Users
- Problem mit herkömmlichen Konten beim Provider: Steuerung liegt beim Provider



Federation und Authentifizierung: Lösungsansatz

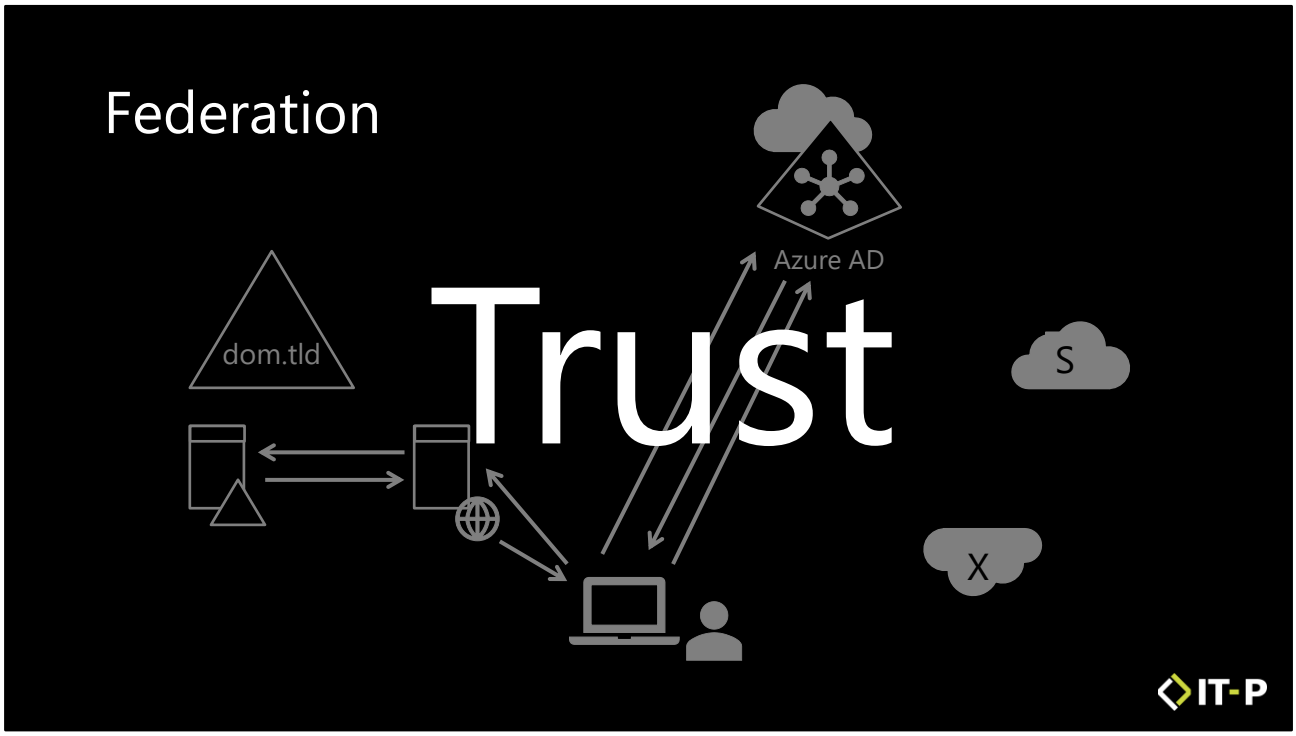
- SAML, OAuth
- ADFS

34



Verfahren, hier am Beispiel SAML/ADFS

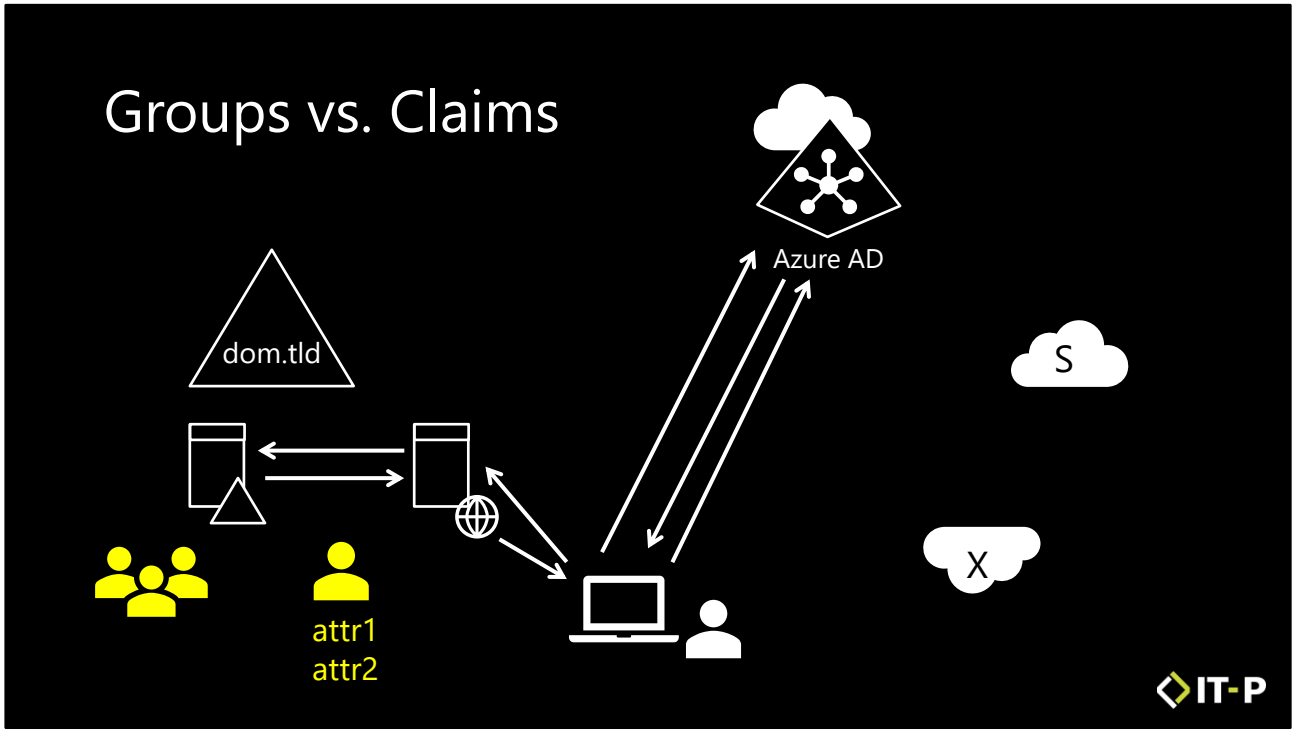
35



Im Kern steht: Vertrauen

- Ich muss dem Provider vertrauen, dass er mit den Daten gut umgeht
- Der Provider muss meiner Infrastruktur vertrauen, dass sie für eine ordentliche Auth sorgt
- Wir müssen einander vertrauen, dass alles passt und wir schnell auf Fehler reagieren

Ist das nicht gegeben, dann: Finger weg!



Bei Federation kommen wieder Claims ins Spiel

- Oft bessere Alternative als Gruppen
- Claims lassen schnellere und flexiblere Zuordnungen zu
- Selbst wenn man intern Gruppen sieht, übermittelt SAML (…) immer Claims
- Daher: Es lohnt, Aufwand in den Ablauf zu stecken, damit der Provider nur das sieht, was er braucht
- Oft zu beobachten: Kunden senden „alle“ Informationen, Gruppenmitgliedschaften usw.

Design for Change*

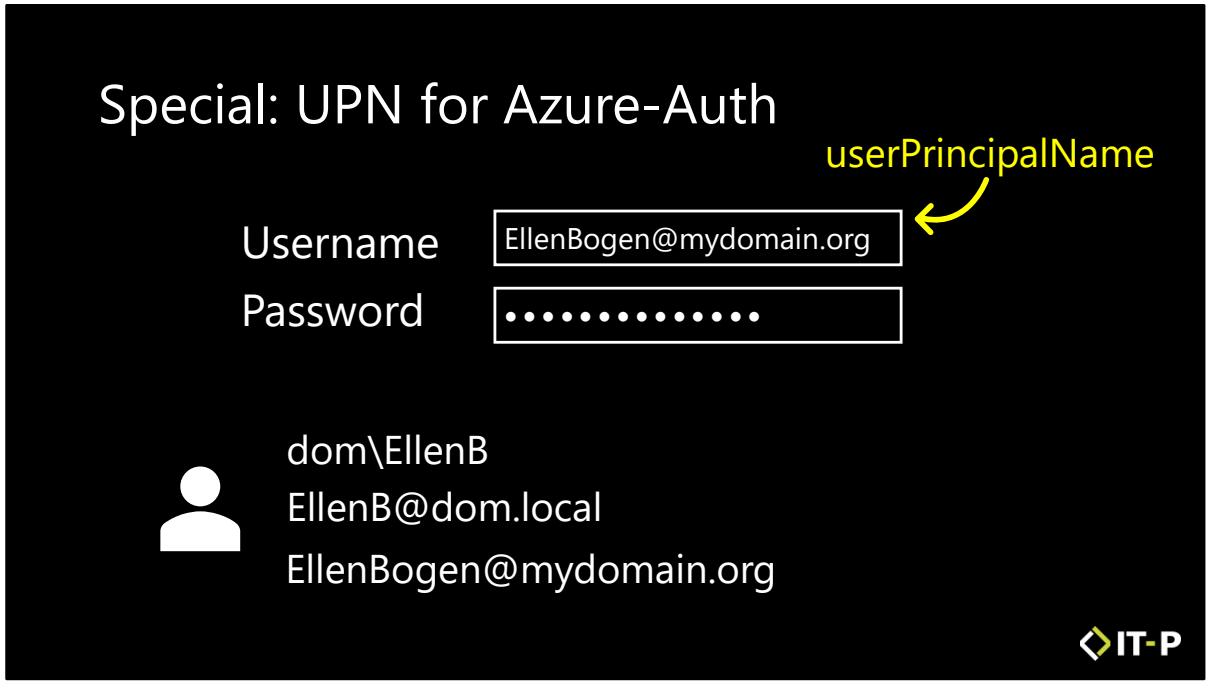
** no, I don't mean a pocket full of change*

IT-P

- Im Cloud-Geschäft kann sich alles sehr schnell ändern – das ist ja der Witz daran
- der Ansatz ist heute nicht mehr, für alle Zeit Strukturen vorzugeben, das Design muss Flexibilität ermöglichen

38

IT-P



Vorteil: AD-Name = eigens registrierte Domain!

- mydomain.org = in Azure für die Anmeldung nutzen

Oder: separate Domain (z.B. Maildomain) als zusätzliches UPN-Suffix

- bestehende UPNs auf neues Suffix umstellen
- Beispiel Animation:
- SAM-Name DOM\EllenB
- alter UPN: EllenB@dom.local
- neuer UPN: EllenBogen@mydomain.org

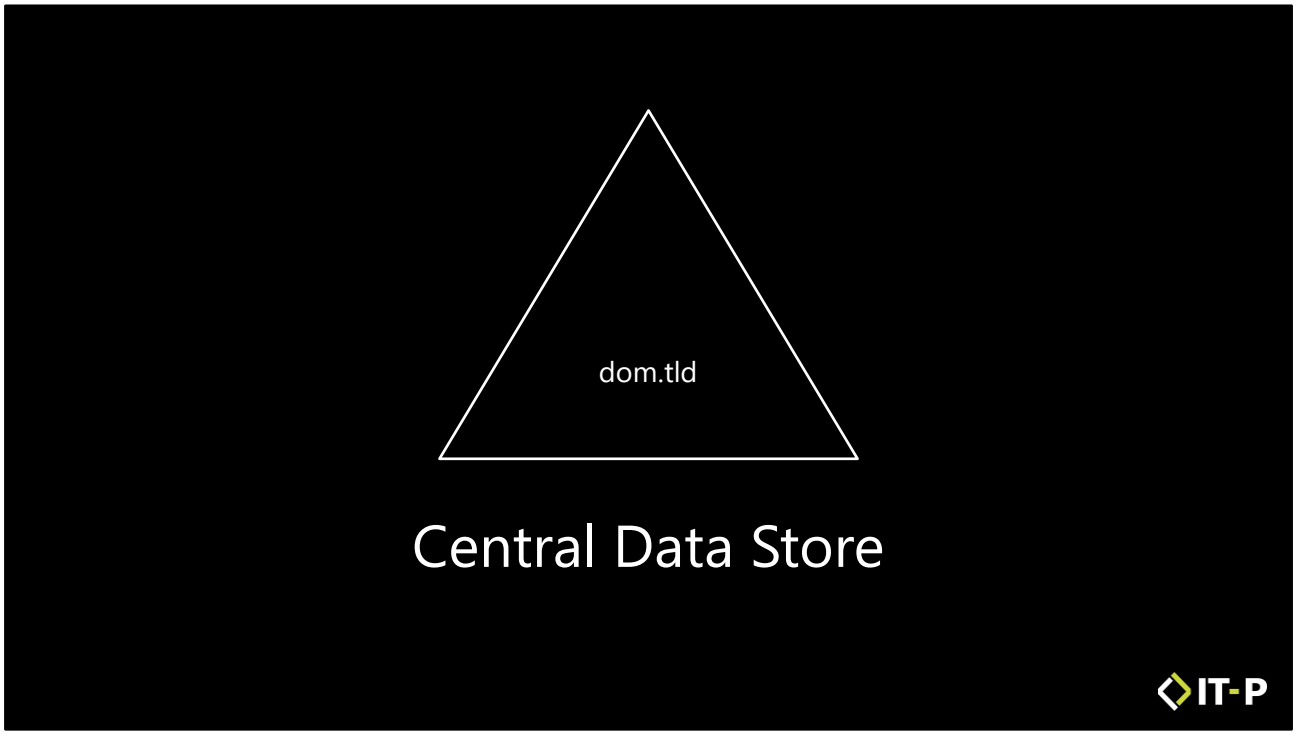
Ausweg: AlternateLoginID

Learning: planen, bevor man loslegt!

39

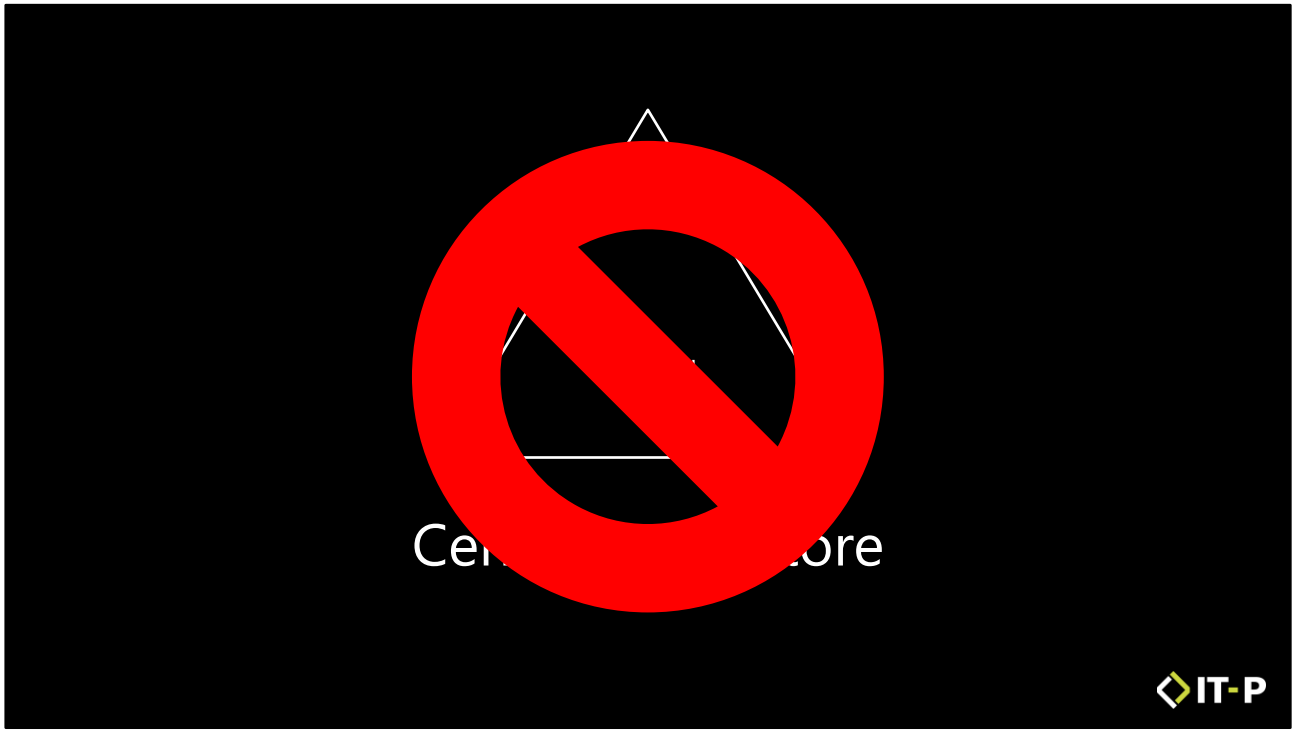
4

Data Pool: Divide and Conquer



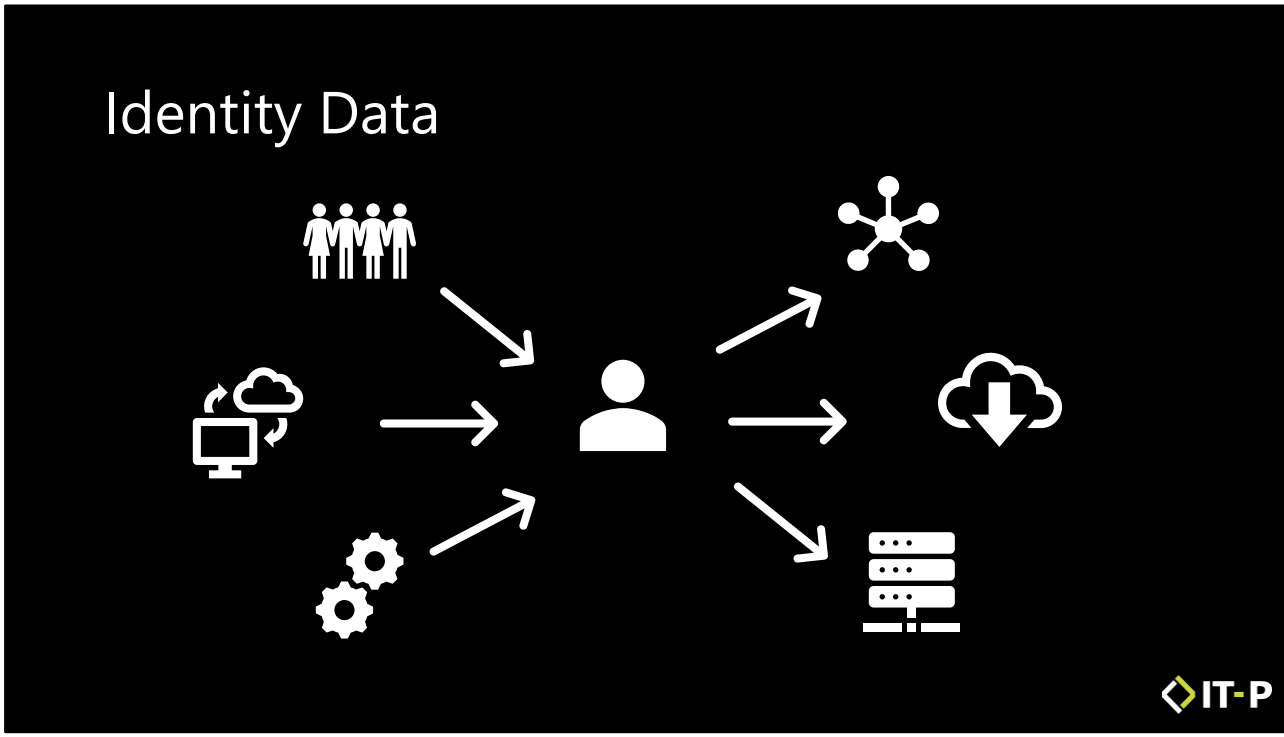
4 Datenpool: Teile und herrsche

- Zentraler Verzeichnisdienst = überholte Idee
- AD nicht als Identity Store "für alles" geeignet
- In der Praxis nutzen wenige Applikationen LDAP
- Datenmenge = Problem mit Datenpflege
- Sicherheits- und Datenschutzbedenken
- Redundante Daten führen zu Inkonsistenzen



4 Datenpool: Teile und herrsche

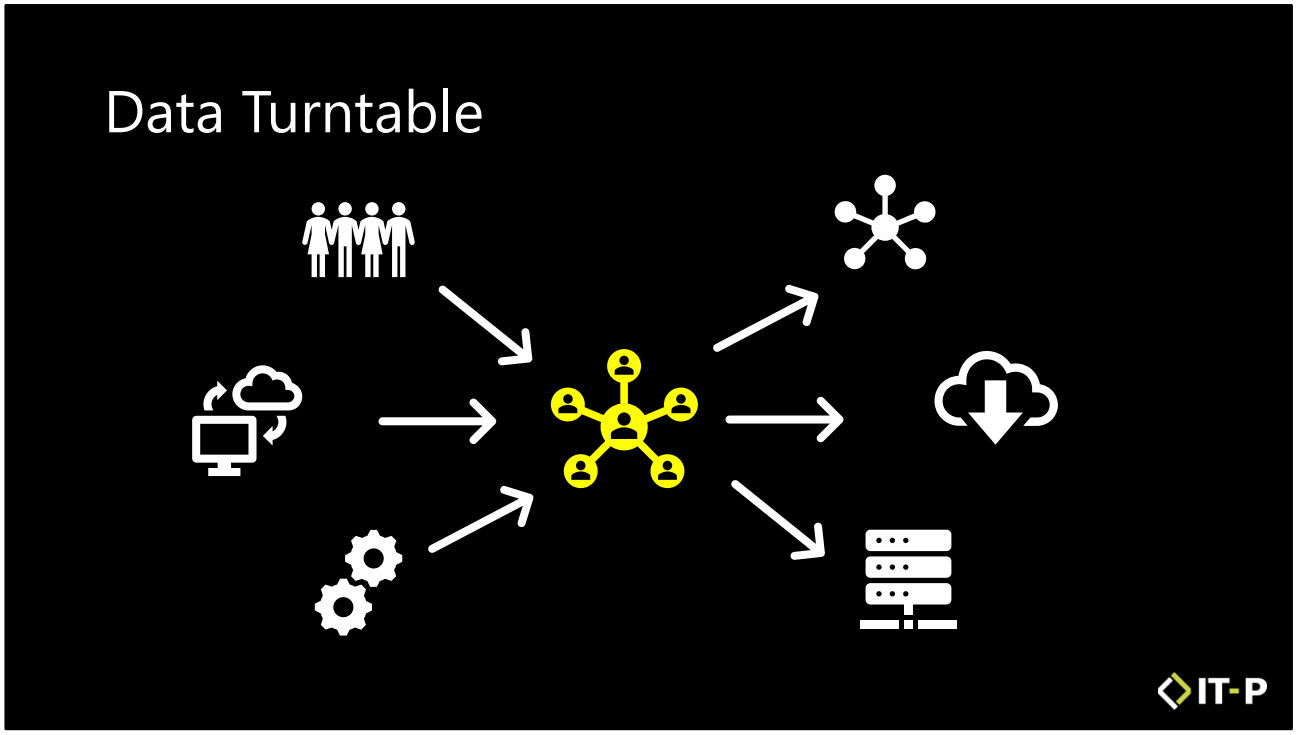
- Zentraler Verzeichnisdienst = überholte Idee
- AD nicht als Identity Store "für alles" geeignet
- In der Praxis nutzen wenige Applikationen LDAP
- Datenmenge = Problem mit Datenpflege
- Sicherheits- und Datenschutzbedenken
- Redundante Daten führen zu Inkonsistenzen



Identität setzt sich zusammen aus vielen Datenquellen …

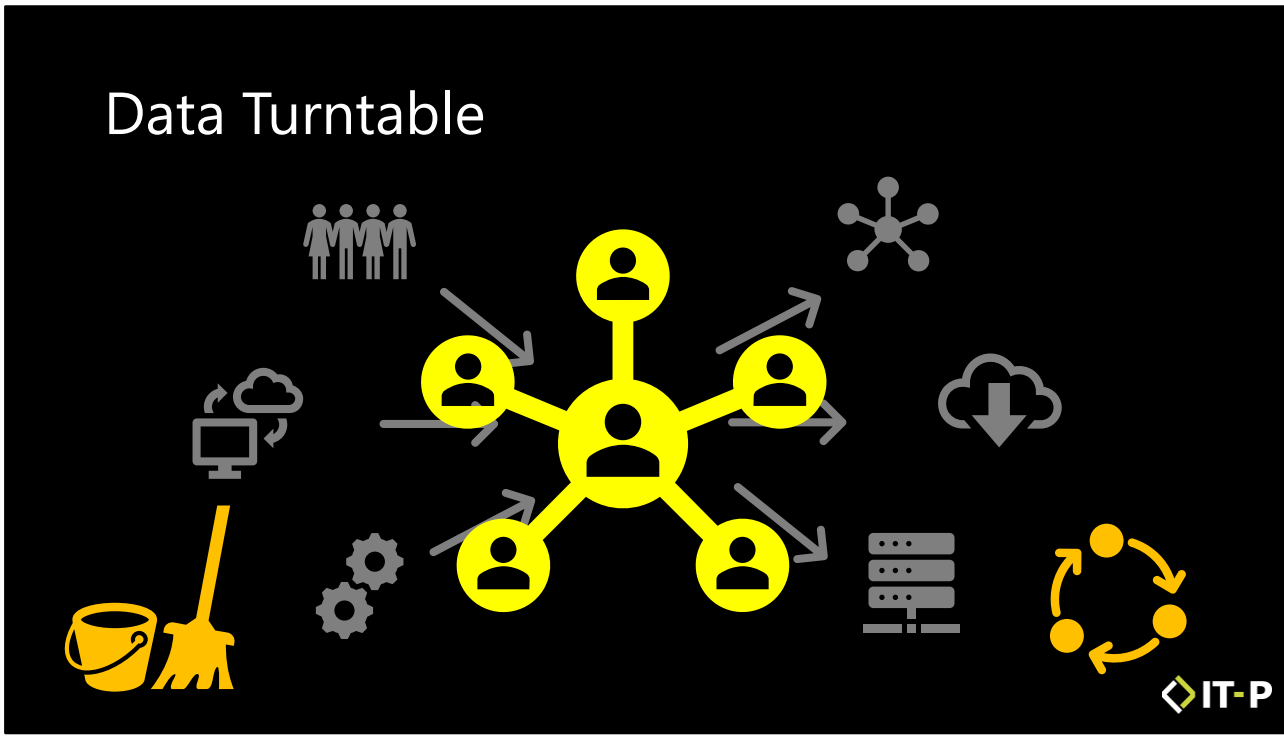
… und wird an vielen verschiedenen Stellen verwendet

43



Daten liegen in den Systemen, wo sie hingehören. Eine IdM-Drehscheibe sorgt dafür, sie nach Bedarf zuzuordnen.

44

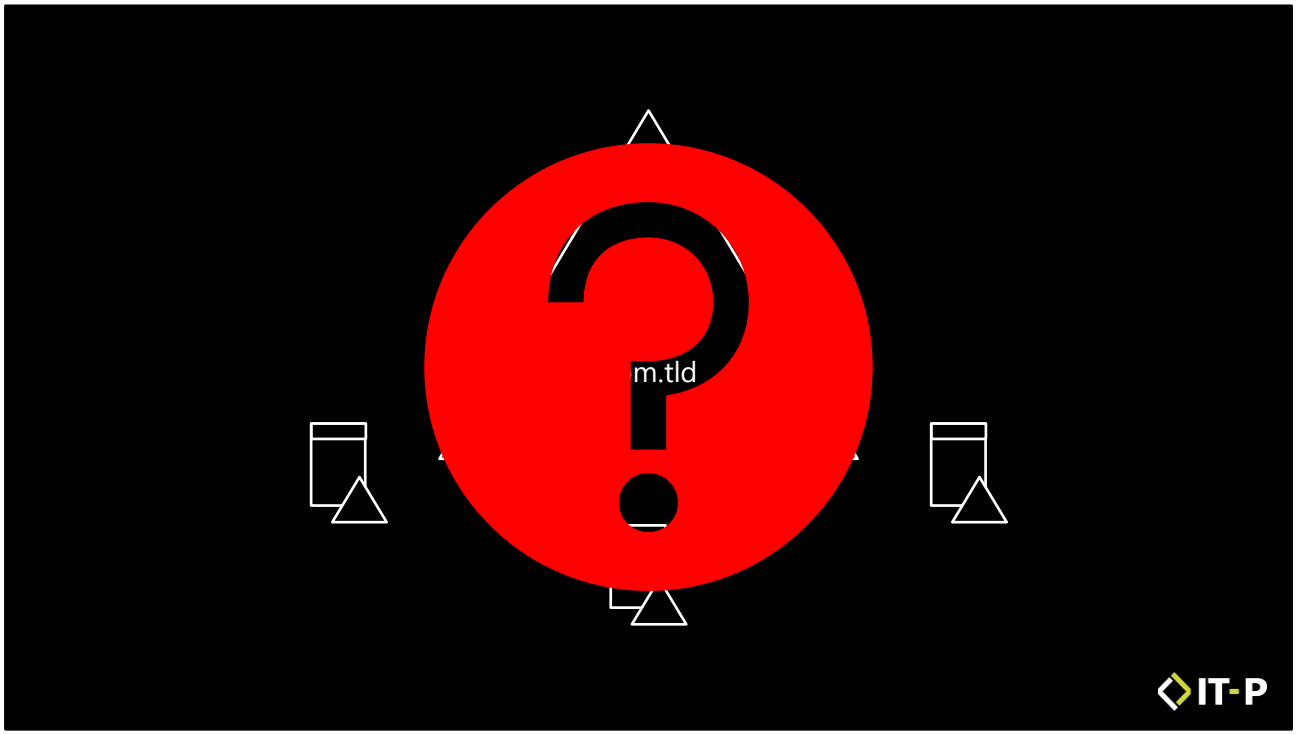


Wichtig in jedem Fall: Datenqualität

Prozesse etablieren, die Daten kontinuierlich zu pflegen

5

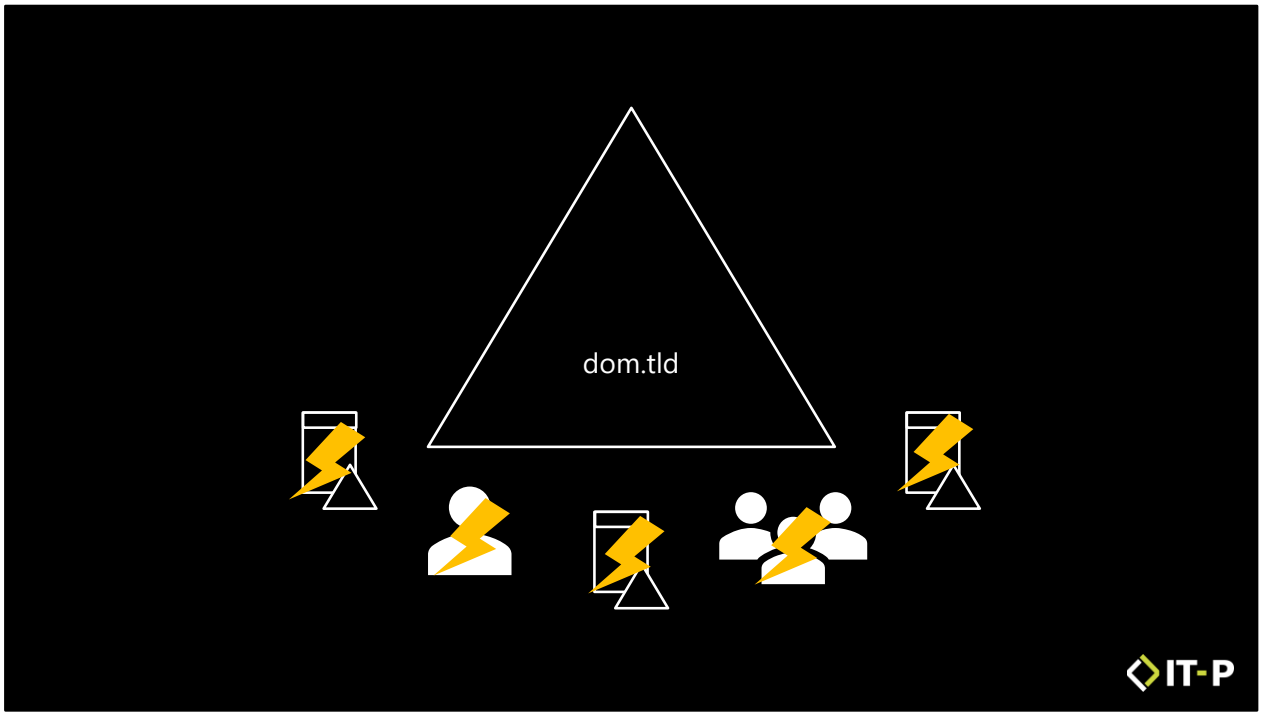
Emergency: Conceived from the End



Typischer Gedanke: Gegen „Desaster“ absichern

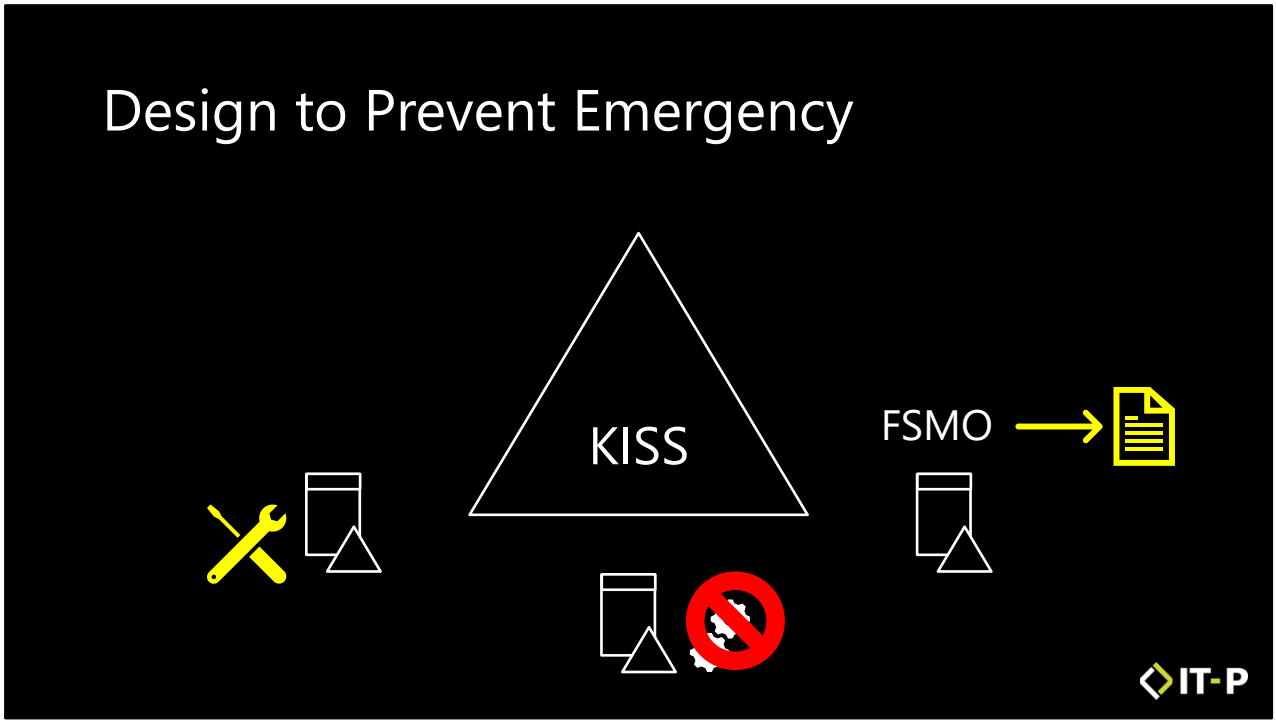
„was muss ich tun, wenn alles ausgefallen ist?“

Problem: In der Praxis kommt das selten vor …



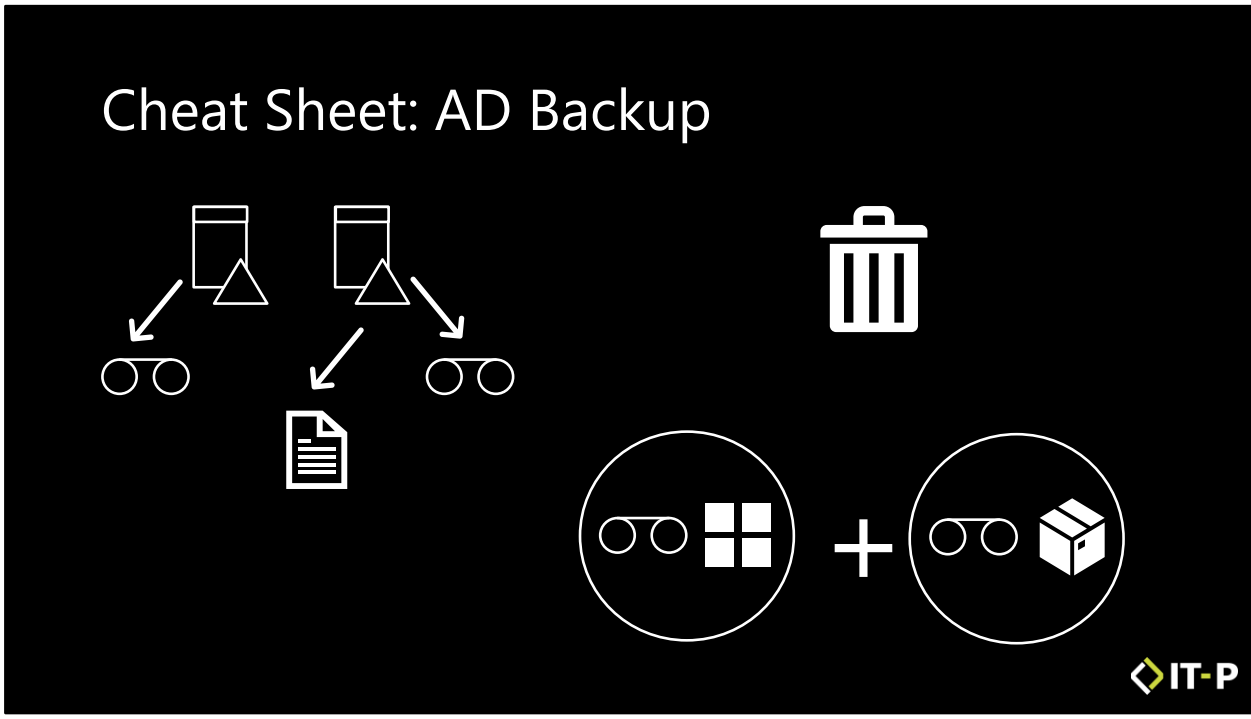
… viel häufiger als ein Komplettausfall sind Einzelstörungen

- Ein DC fällt aus
- Alle DCs fallen aus
- Ein User wird gelöscht
- Eine Gruppe bzw. anderes Objekt wird gelöscht – oder komplexer: wird manipuliert



AD-Design für Wiederherstellbarkeit

- Simples Design
- FSMO-Rollen dokumentiert
- DC nur DC
- Min. 1 DC physisch
- Ausreichende Redundanz



AD-Backup

- Systemstate von min. 2 DCs
- Textexport bei jedem Backup: gelöschte Objekte identifizieren
- Papierkorb
- Andere Backups nur zusätzlich zum Systemstate

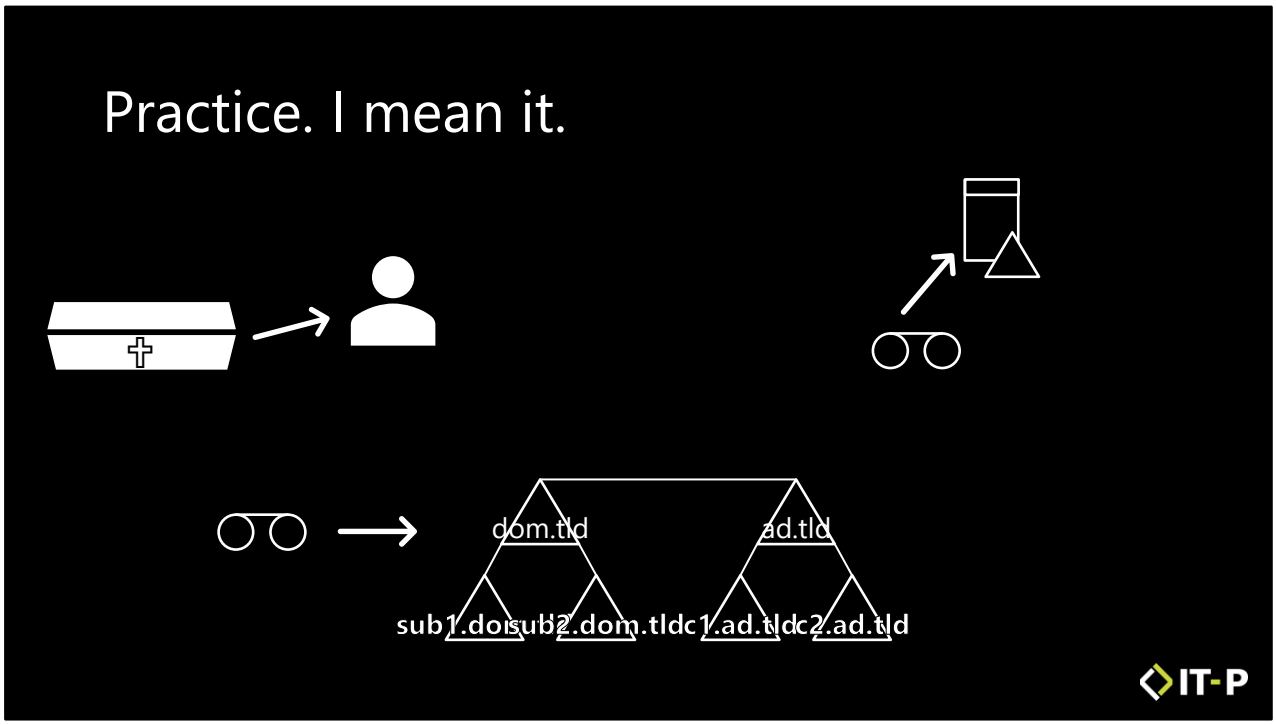
Cheat Sheet Cheat Sheet

- Backup 2+ DCs per domain
- Do a text export of all objects with each backup
  - csvde -f C:\AD\exp.txt -u -l sAMAccountName,objectClass,description
- Enable the AD Recycle Bin
- Do 1+ backup with Windows Server Backup (Systemstate)
- Other products just in addition

IT-P

51

IT-P



Wichtige Szenarien vorplanen und üben

- Objekte wiederherstellen
- Einzelnen DC ersetzen
- Forest-Recovery - Zeit einplanen und Schritte genau dokumentieren (z.B. Entfernen der Replikationspartner)

Food Takeaway

- 1 Design: Foundation for Identities
  - Check AD design: simple enough?
  - Build object-oriented trees
- 2 Security: Attack is Normal
  - Separate roles
  - Red Forest Design
- 3 Hybrid Design: Cloud and Local
  - AD is the identity anchor
  - Plan your name spaces
- 4 Data Pool: Divide and Conquer
  - All data in its location
  - Control data spread
- 5 Emergency: Conceived from the End
  - Design to prevent emergency
  - Practice recovery actions

IT-P

tea-age-axe

ScriptRunner®

IT-P

IT-P

Nils.Kaczenski@it-p.de

Stay safe. Stay secure.

IT-P Information Technology-Partner GmbH