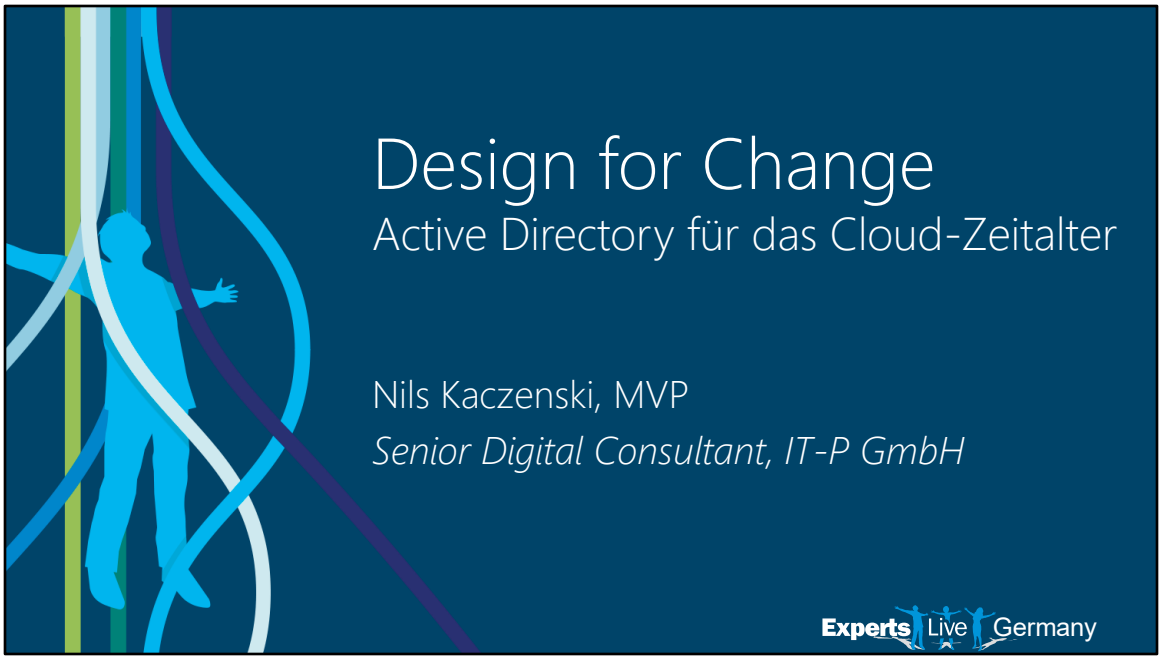


Nils Kaczenski
Strategy | Infrastructure
Senior Digital Consultant | Microsoft MVP

T: 0511 616 80 42 0
E: Nils.Kaczenski@it-p.de
W: https://www.it-p.de/
Li: https://www.linkedin.com/in/nils-kaczenski/
IT-P GmbH | Partner für erfolgreiche digitale Transformation


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

1

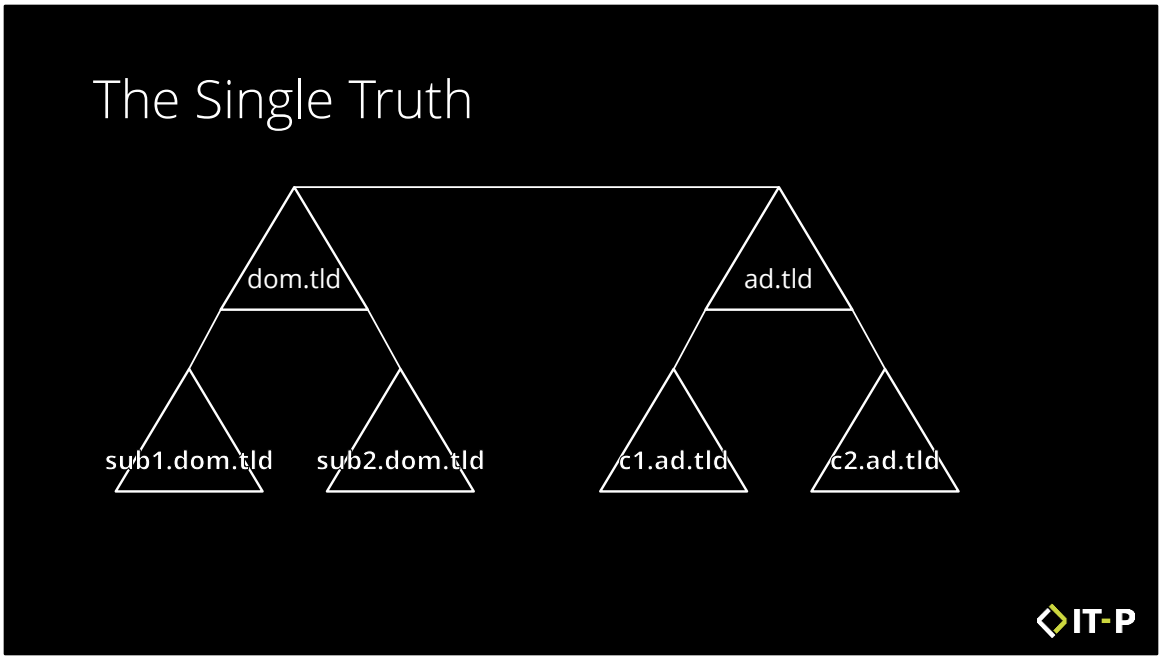
Design: Das Fundament für Identitäten

IT-P

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

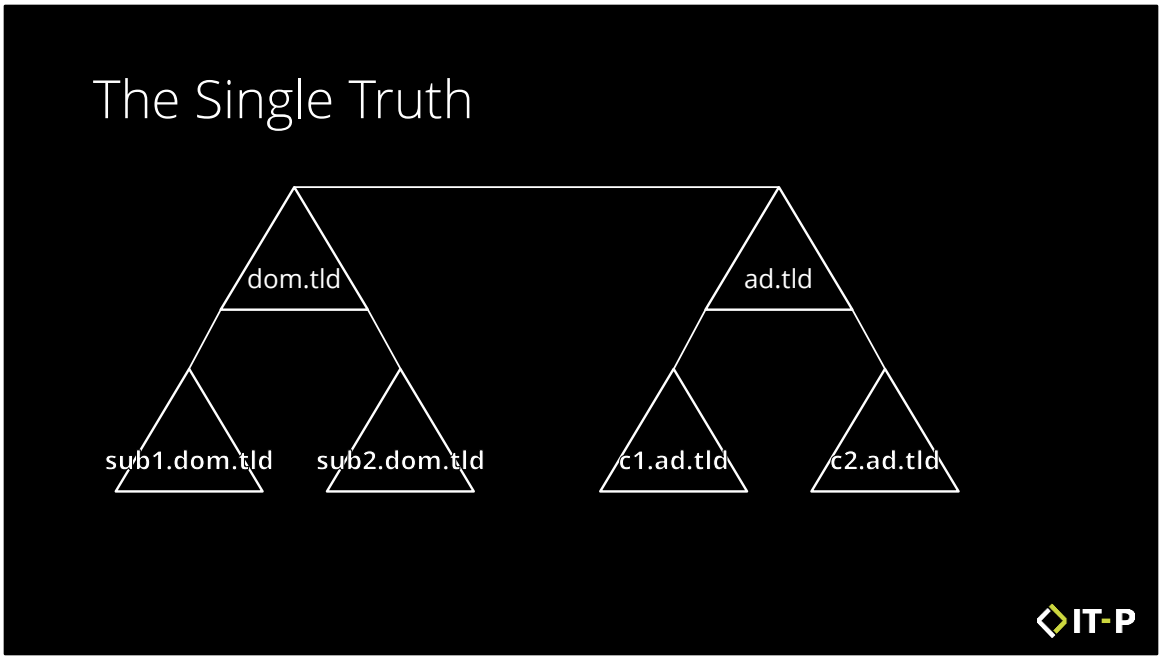
Abstrakter Name

Varianten gibt es einige, aber nur wenige sind gute Designs
https://www.faq-o-matic.net/2013/06/24/wie-nenne-ich-mein-active-directory/
Hinweis, was ein Rename bedeutet
Learning: Niemals eine Domäne migrieren, nur um sie umzubenennen. Wenn man aber neu aufbaut, gleich einen „richtigen“ Namen nehmen.

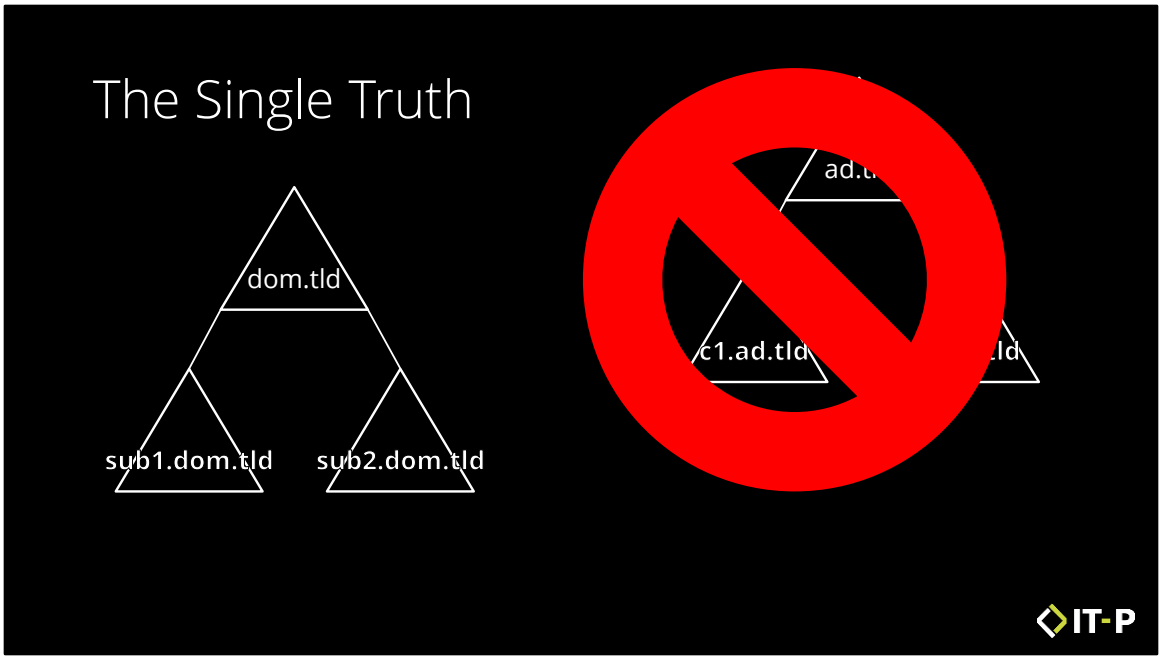


Single Domain Forest

Wiederholung: Domain, Tree, Forest

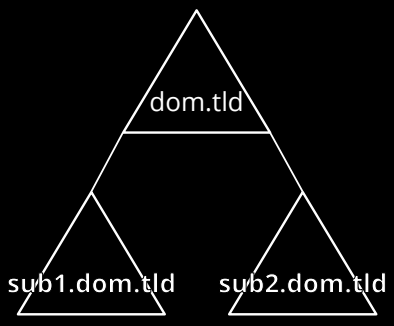


Annahme: Man kann aus einem Forest einen Tree herauslösen, falls man einen Unternehmensteil verkauft



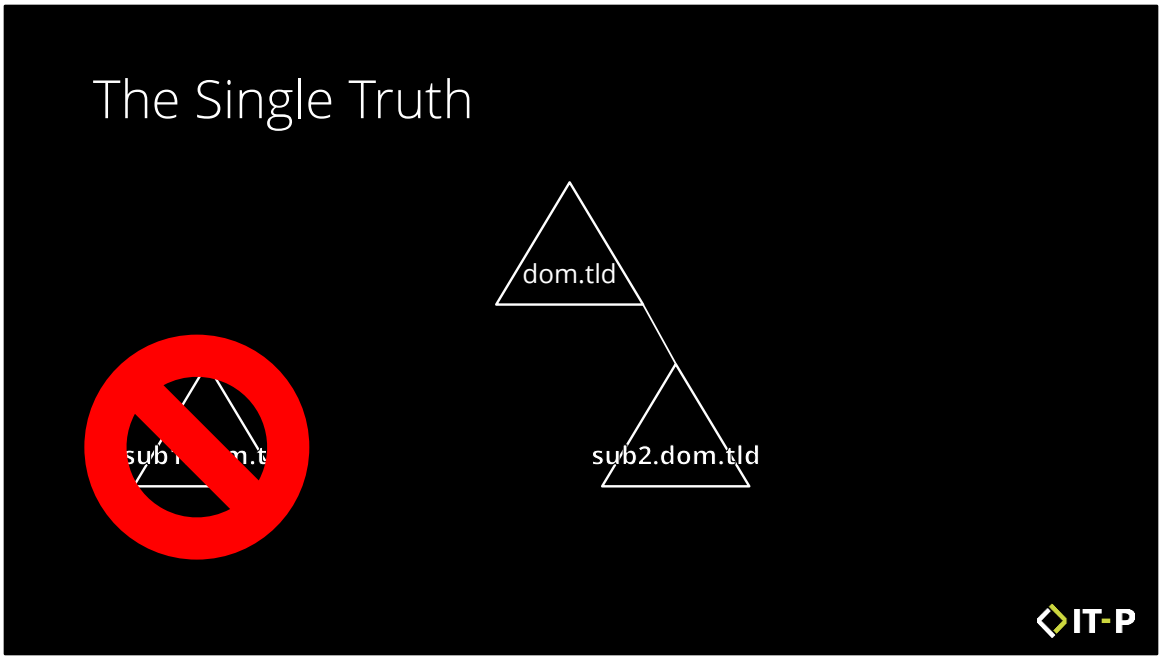
Realität: Genau das geht nicht. Einmal Teil des Forests, immer Teil des Forests.

The Single Truth

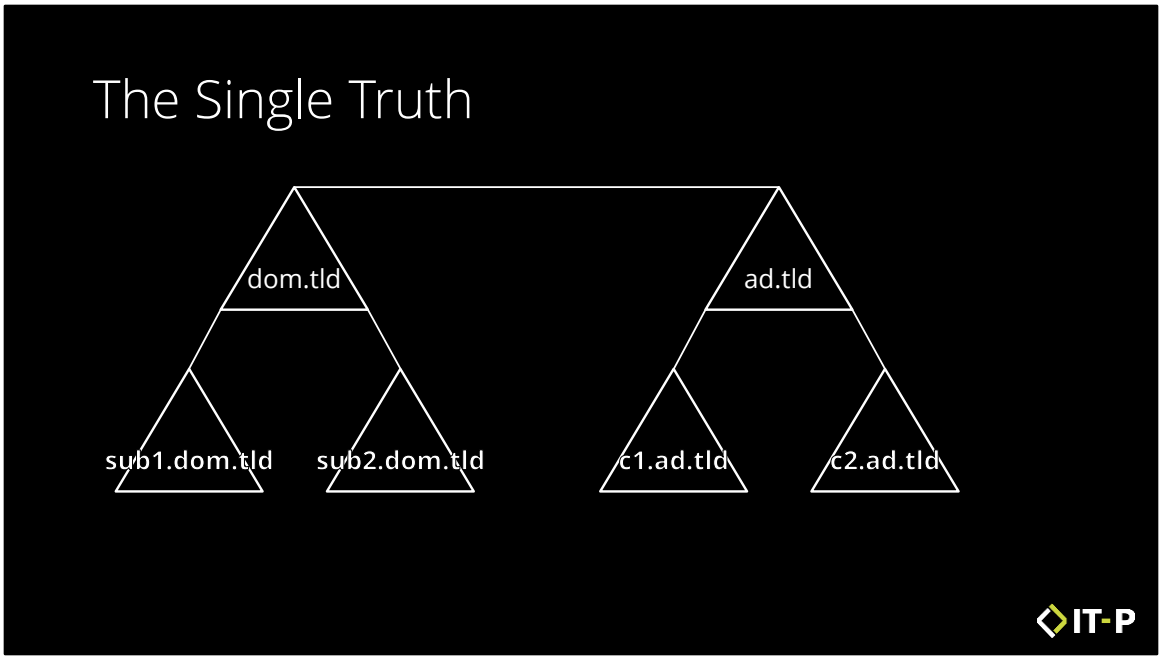


IT-P

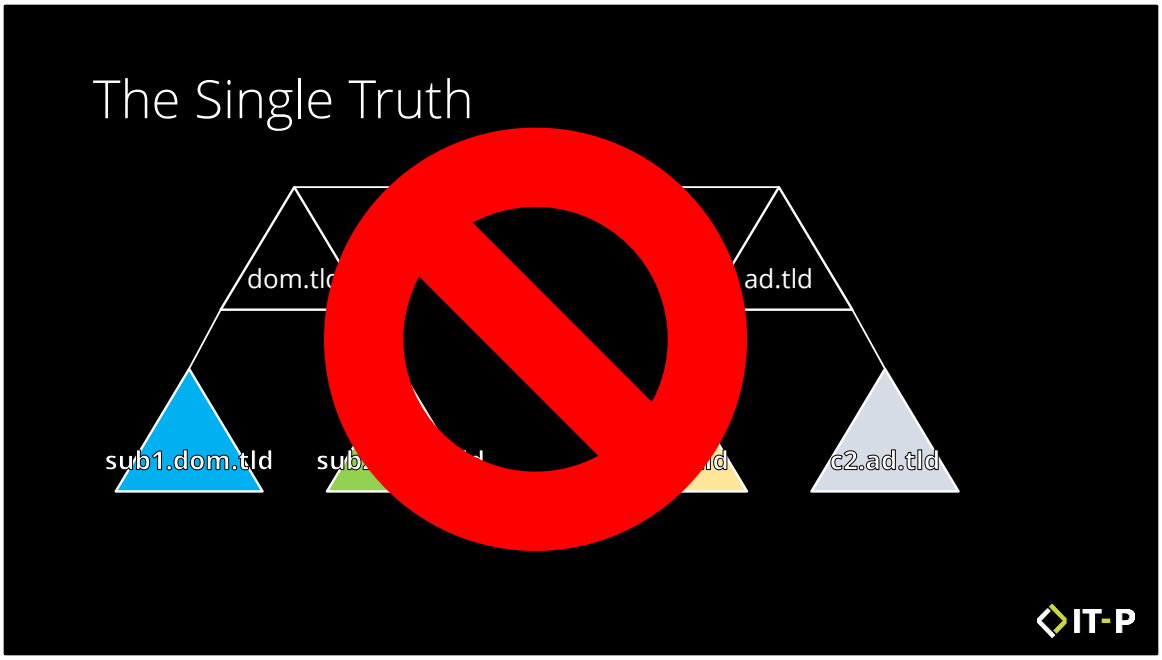
Annahme: Man kann aus einem Tree eine Domain herauslösen …



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



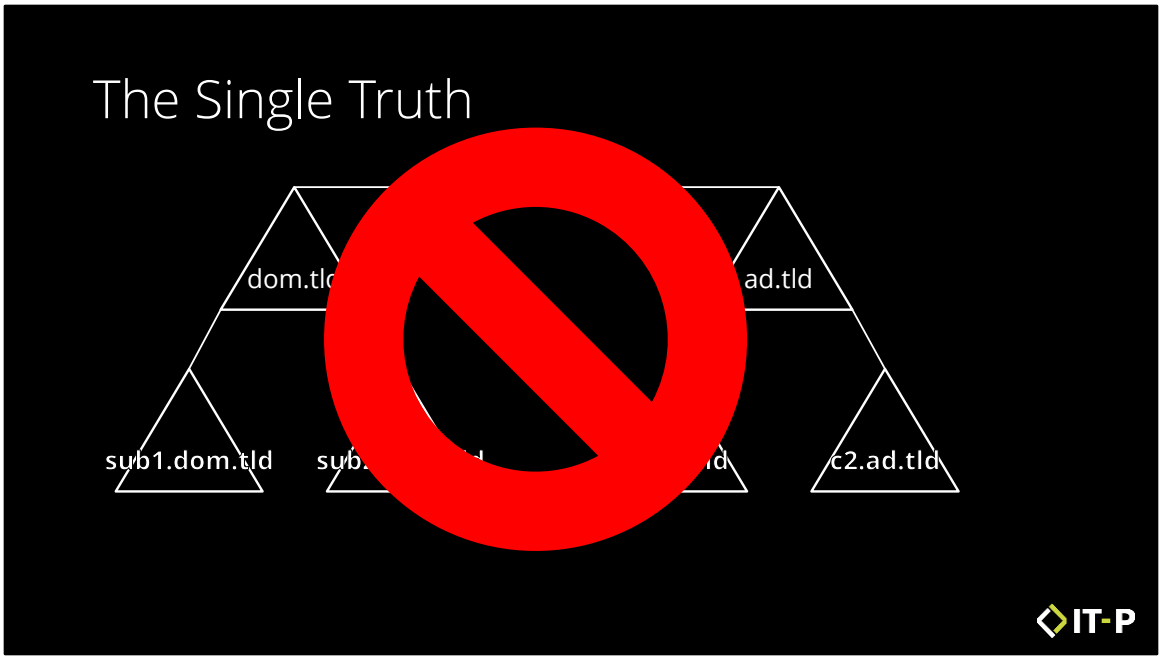
Annahme: Man kann ein AD in mehrere Domains aufteilen, um Sicherheitszonen für die Administration zu schaffen.



Realität: Nein, auch das geht nicht.

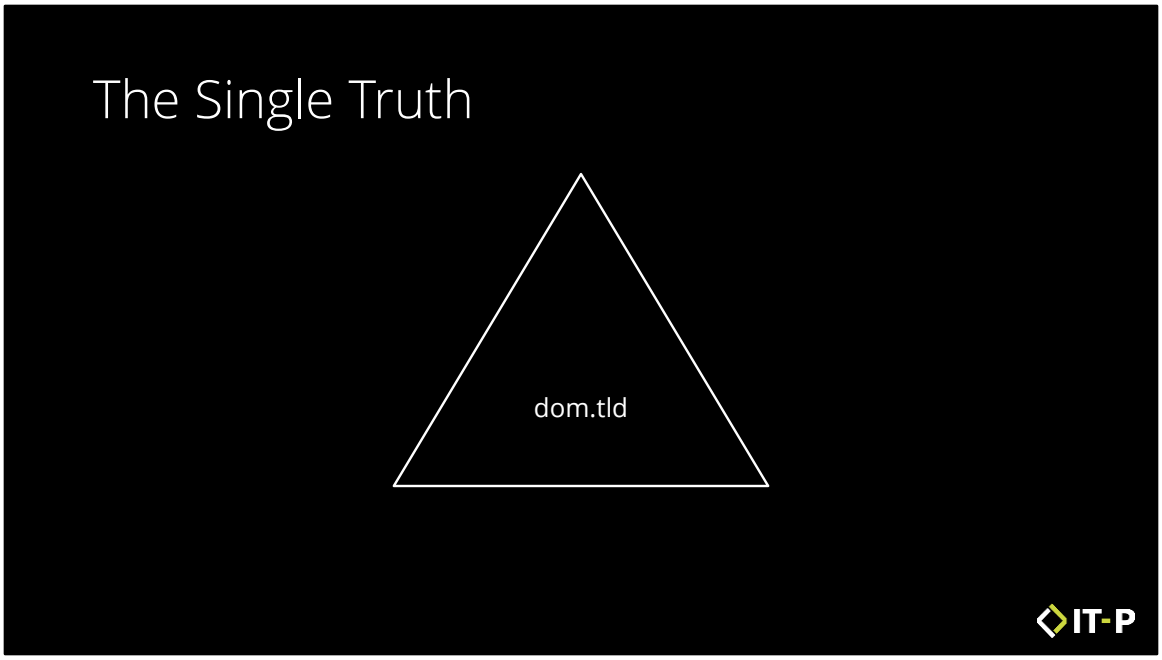
In einem Forest wird eine Sicherheitsaufteilung in Domänen wirkungslos (Enterprise Admins, automatische Trusts, Kerberos-Mechanismen, SID-Handhabung …).

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



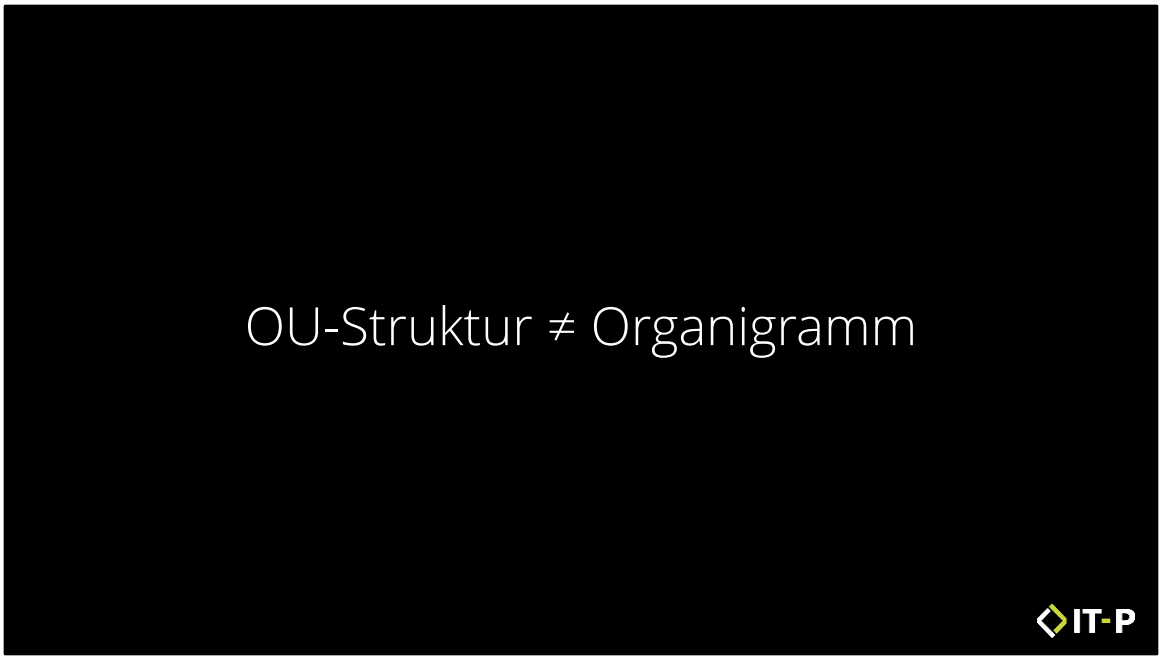
Ist ein Forest aus mehreren Domains also eine gute Idee?

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



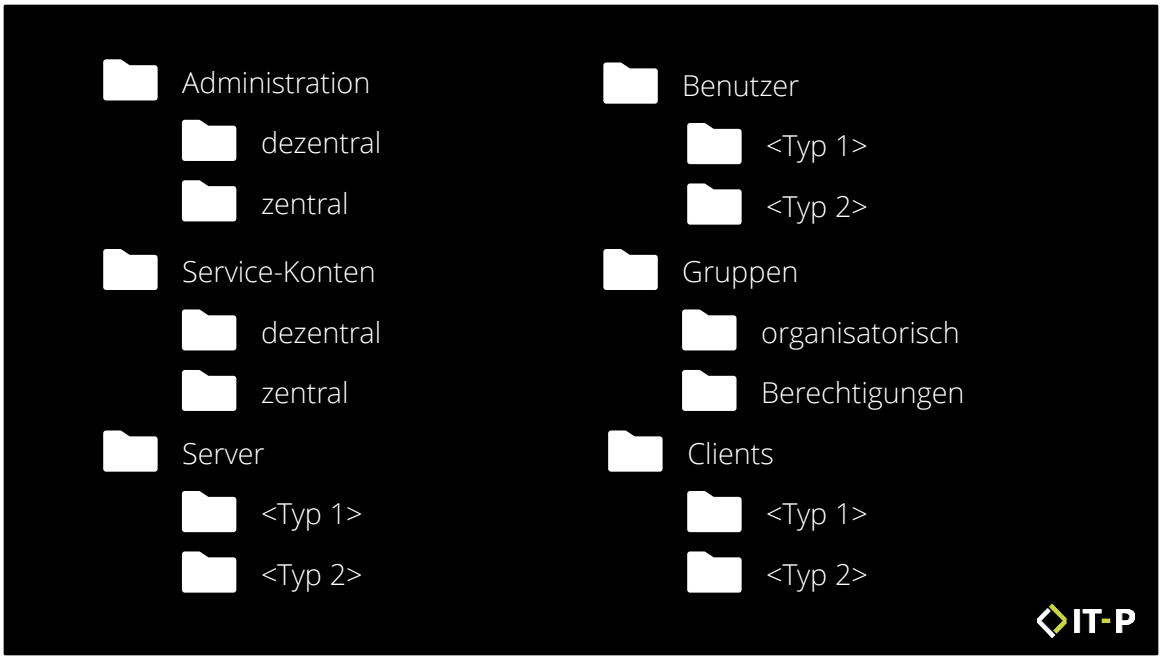
Für neue Entwürfe oder für Konsolidierungen gilt also: Single Domain ist das einzige valide Modell.

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



Objektorientierte OU-Struktur

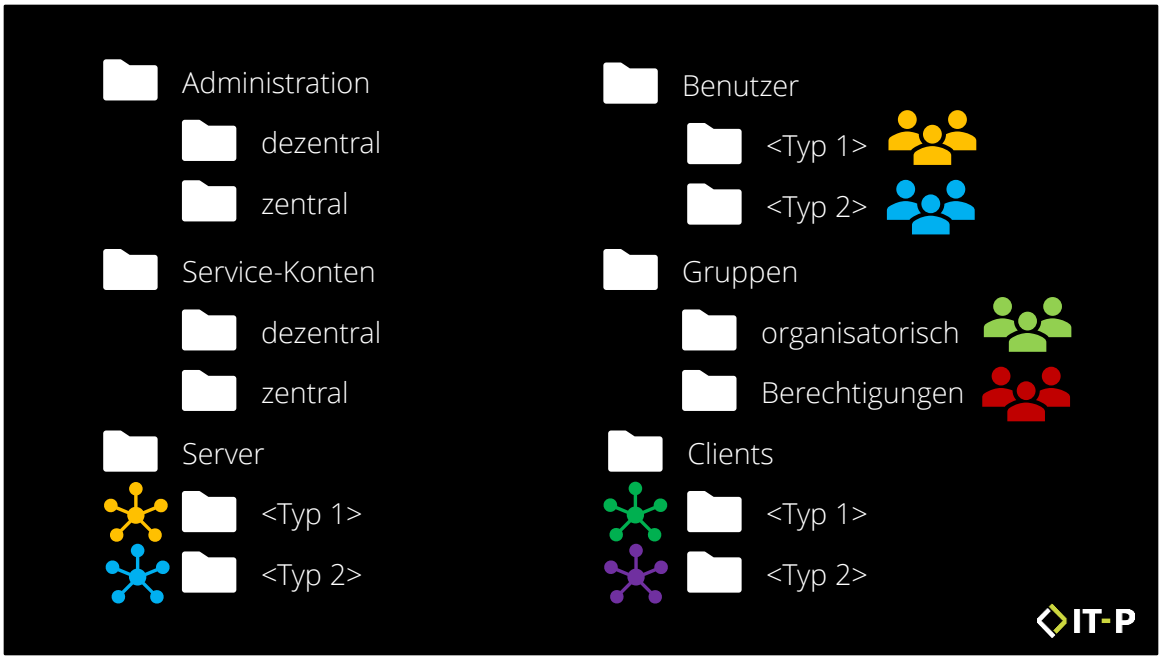
OU-Struktur ist nicht das Organigramm, sondern dient der AD-Administration



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

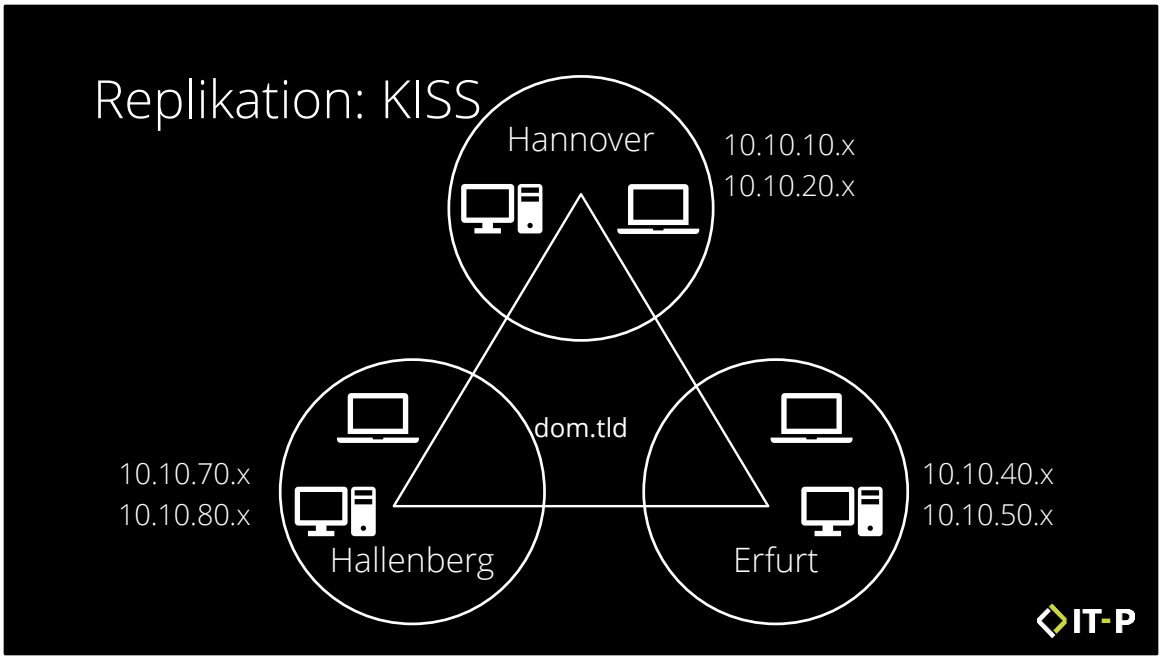
Hier ein Vorschlag für ein Standard-Design als Ausgangspunkt
https://www.faq-o-matic.net/2020/11/16/active-directory-best-practice-zur-ou-struktur/

Pro-Tipp: Integrierte Dokumentation über "description"



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

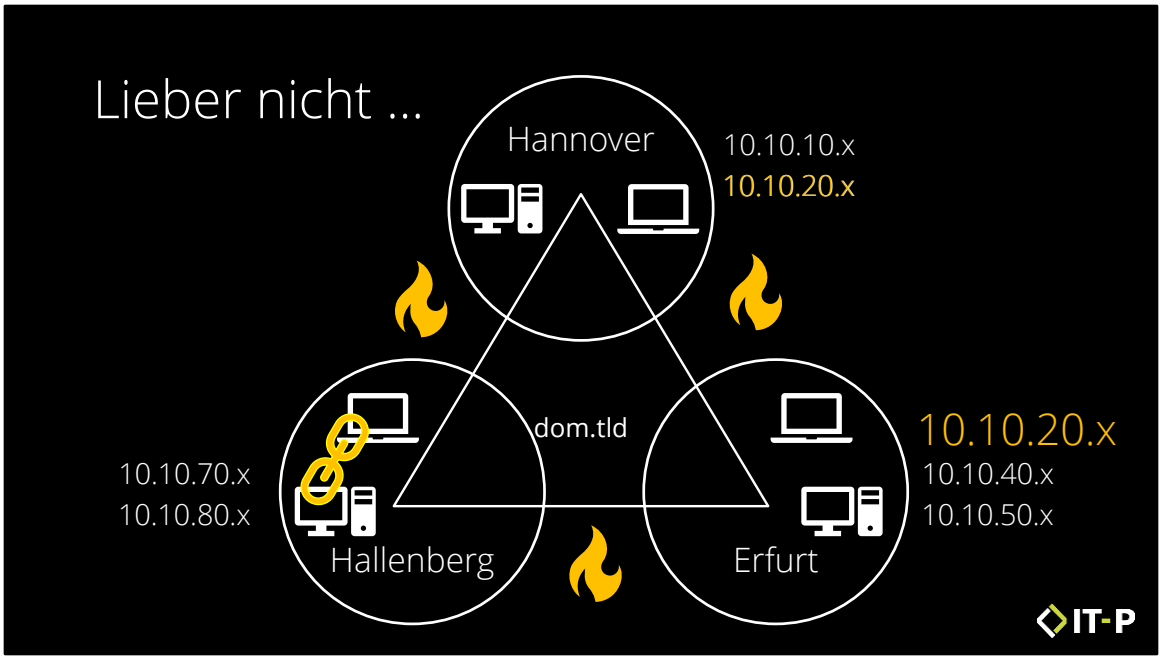


Replikationsstruktur: KISS

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

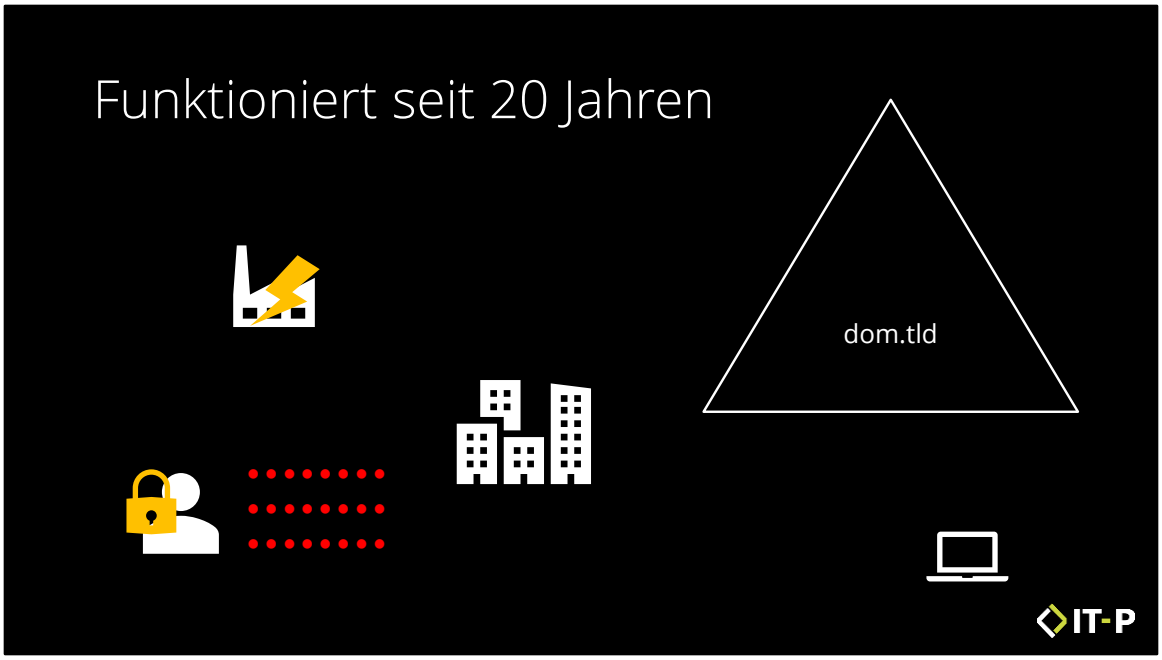
Special: Multi-Domain

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



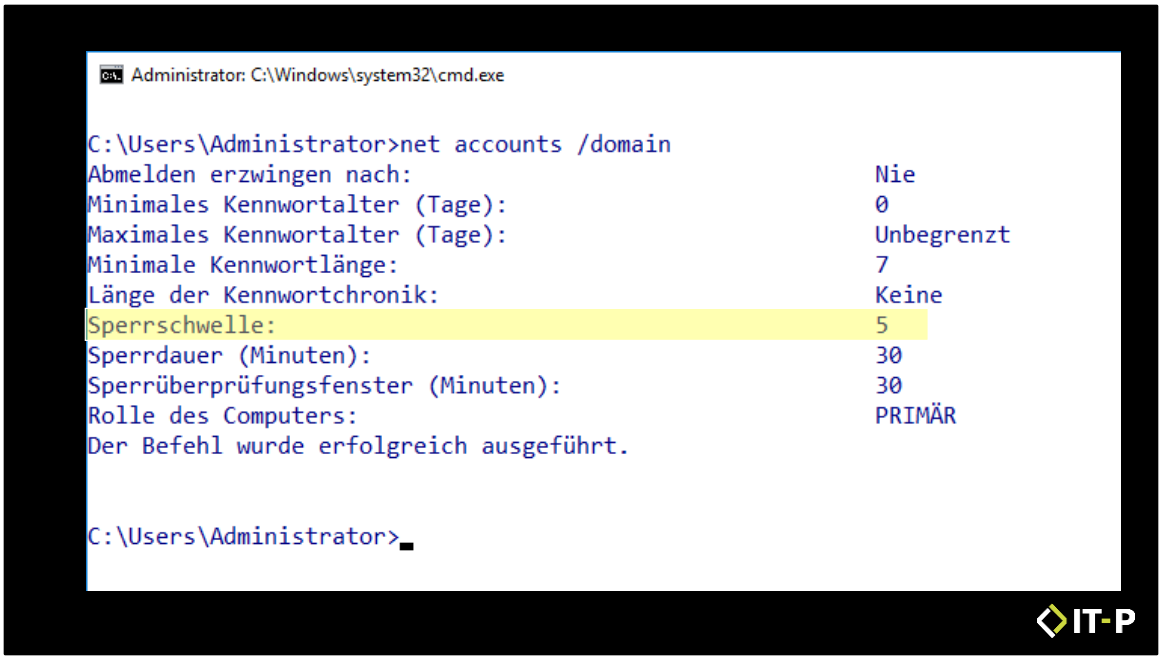
Was man vermeiden sollte
Uneindeutige Subnets
Firewalls (erfordert Konfig in der FW und in der AD-Konfig)
Einschränken der Replikation
Client-Manipulation, um die Anmeldung zu steuern

2 Sicherheit: Angriffe sind normal



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 …

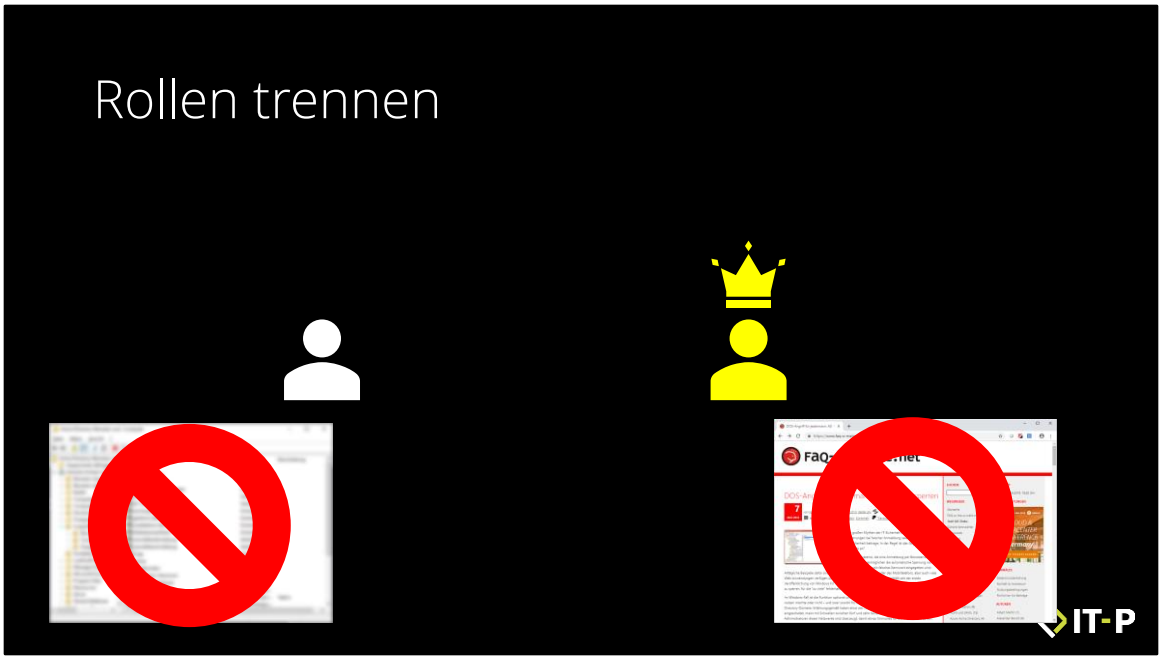
https://www.faq-o-matic.net/2013/08/07/dos-angriff-fr-jedermann-ad-konten-sperren/

Rollen trennen

IT-P

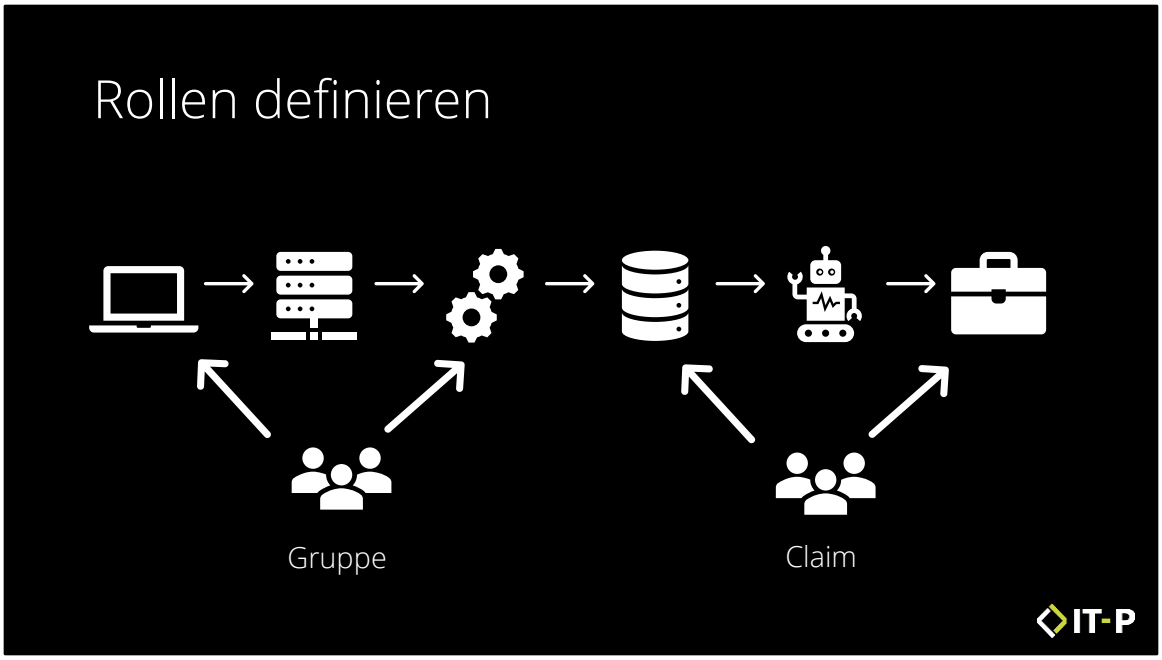
Moderne Sicherheitskonzepte beruhen auf der Rollentrennung

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

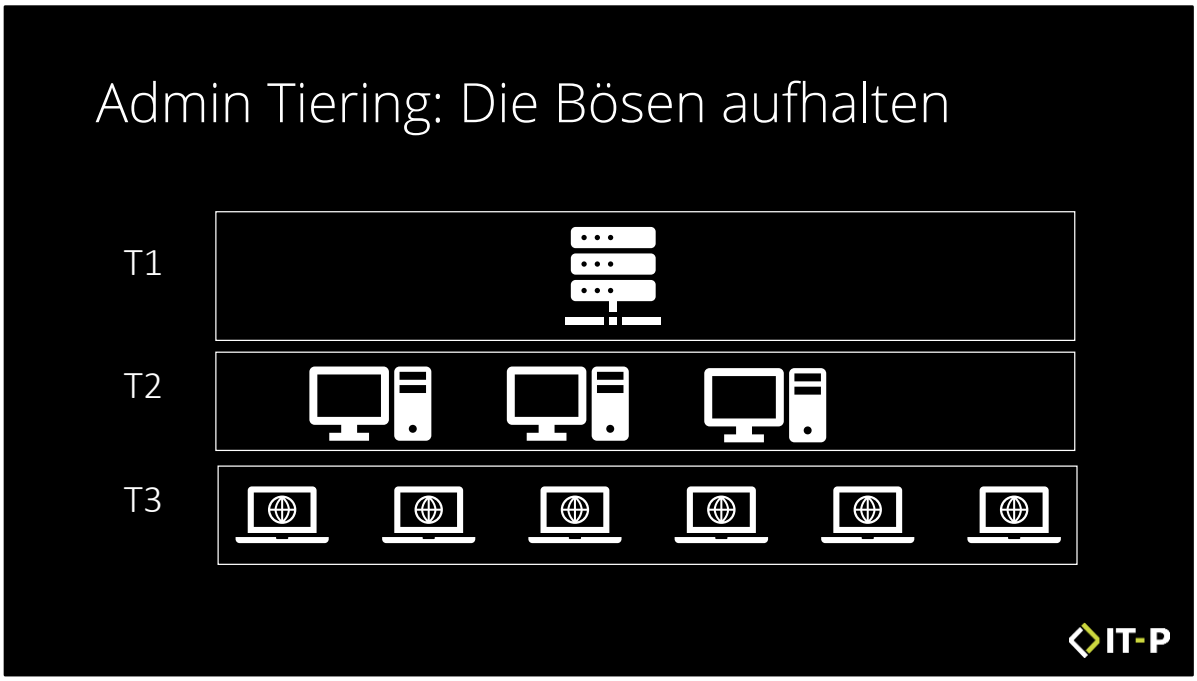


Ansatz: pro Sicherheitsbereich ein separates Konto.
Wer also mehr darf als andere, hat mehrere Konten dafür.

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

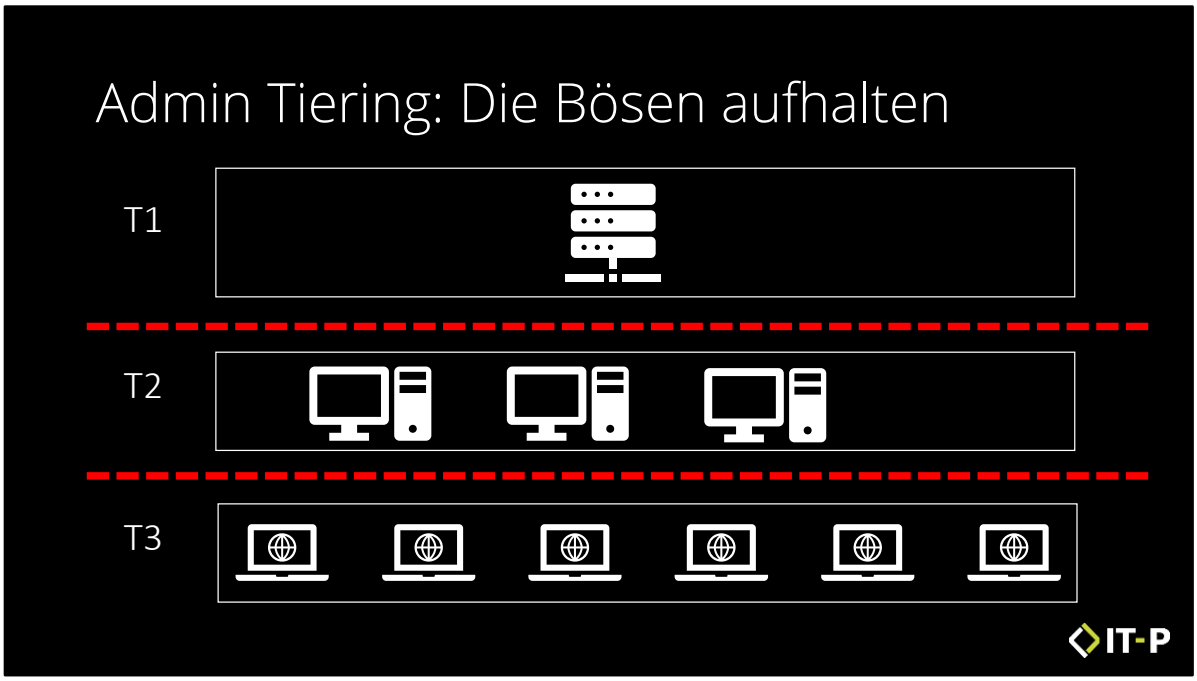


Wie kommt man zu einem Rollenkonzept?
Der Teil, den Admins nicht mögen: Man muss mit den Fachabteilungen sprechen
Frage: Wer braucht welche Daten und Funktionen?
Ableiten: Rollen und Zugriffe
Klassisch: Umsetzen mit Gruppen
Manchmal flexibler: Umsetzen mit Claims – erspart Anhäufung von Gruppen, ermöglicht 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

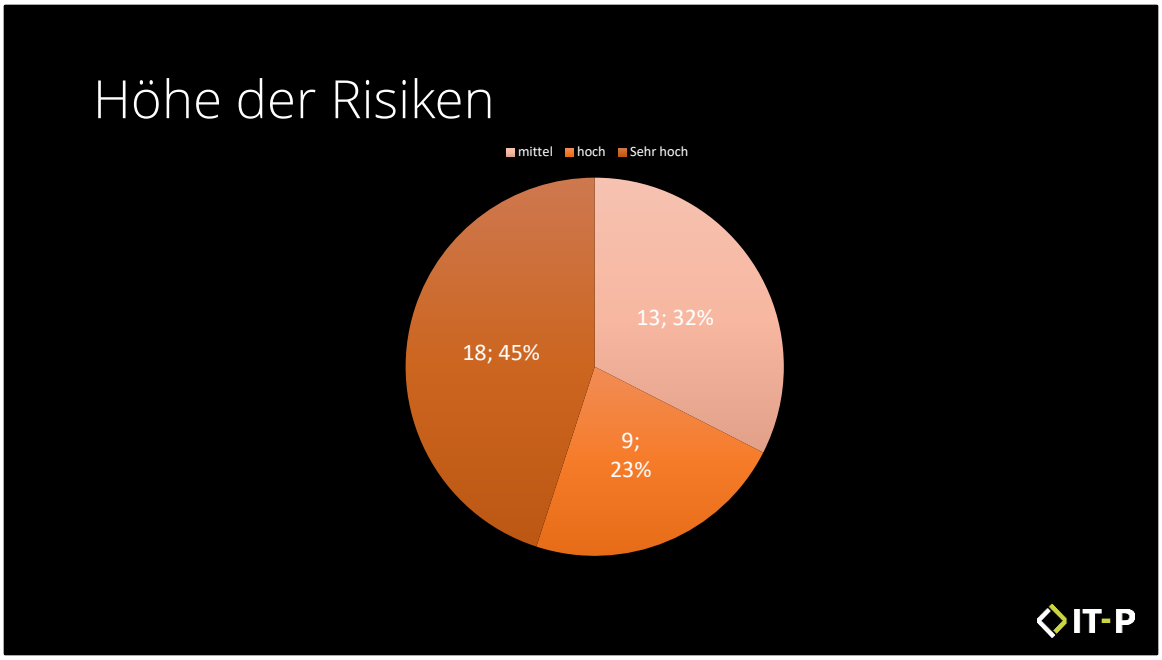
Rollentrennung ernst gemeint: Administrative Tiering

- 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

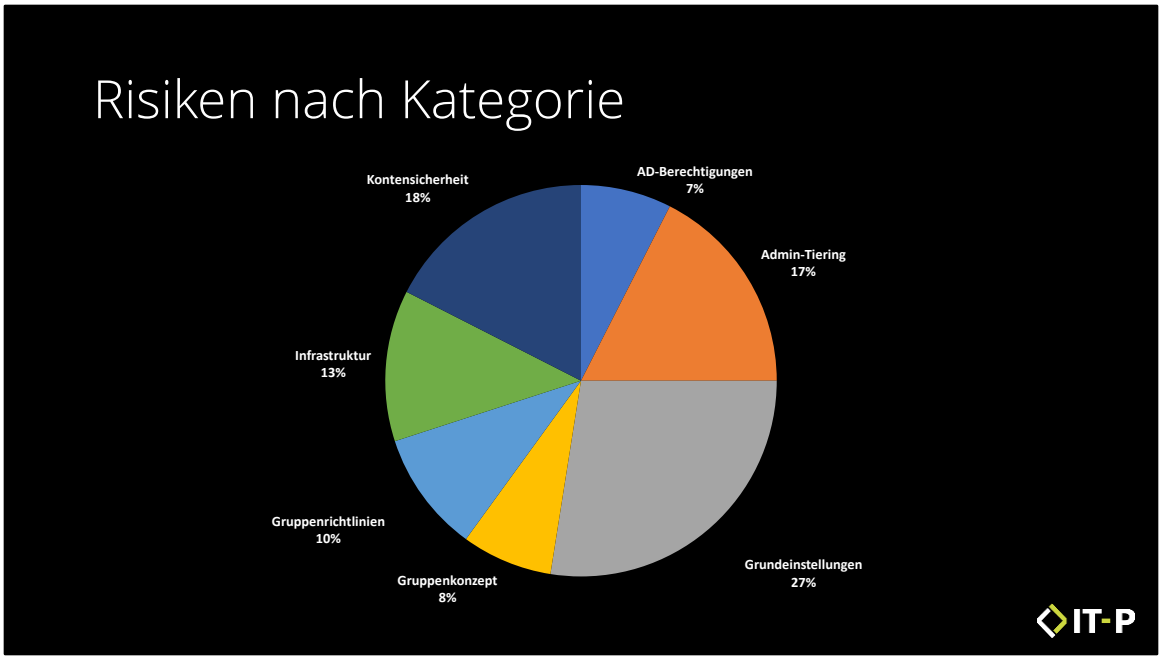
Warum der Mittelstand keine Pentests braucht

- Das typische „mittelständische“ Netzwerk ist durch Nachlässigkeit gekennzeichnet
  - Oft geht das durch Überlastung der IT auch gar nicht anders
- Daher sind diese Netze meist in einer Weise eingerichtet und betrieben, dass Pentests gar keinen Sinn ergeben: der Pentester wäre viel zu schnell drin, weil zu viele Grundlagen nicht beachtet sind

- Ein reales Fallbeispiel illustriert das gut:
  - Mittelständische Unternehmensgruppe
  - 2019 ein Major Incident: Ransomware-Befall
  - Kompletter Shutdown, Neuaufbau durch Dienstleister
  - IT denkt, sie sei nun sicher … aber da sind Zweifel …
  - Daher ein Audit 2022: wie sicher sind wir wirklich?



- Ein begrenztes Security-Audit (wenige Tage Budget, daher nur stichprobenartig) offenbarte gravierende Lücken
  - Weder Konzept noch Dokumentation vorhanden
  - Allein im untersuchten Bereich 40 relevante Findings …
  - … davon fast die Hälfte mit sehr hohem Risiko



Verteilung der gefundenen Risiken nach technisch-logischer Kategorie

3

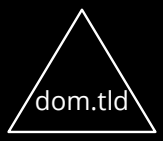
Hybrid-Design: Cloud und lokal

IT-P

Was heißt das nun für die Anbindung der Cloud?

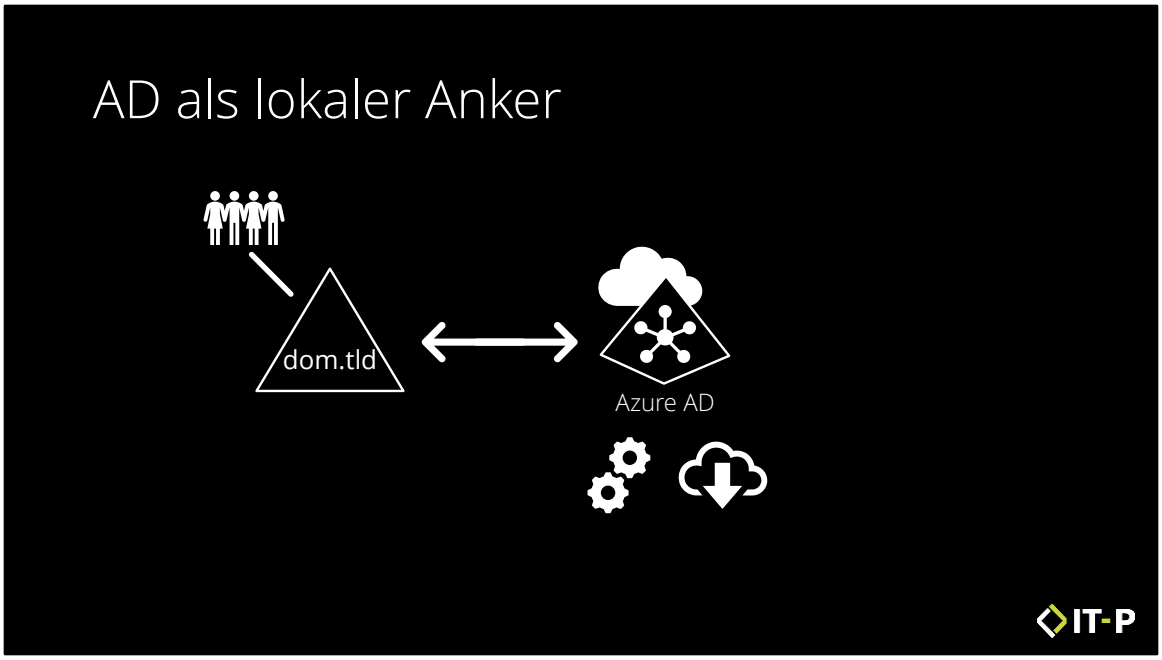
- Im Zentrum steht immer die Anmeldung, also die Identität. Habe ich die, so ist mein Zugriff definiert

AD als lokaler Anker



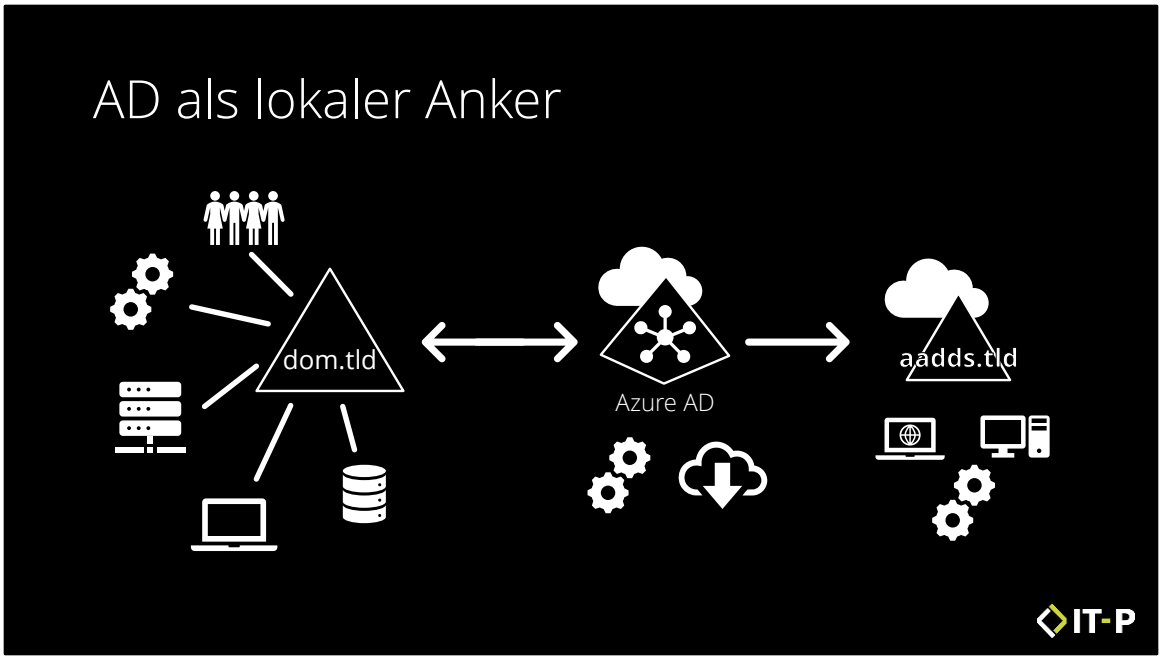
AD als lokaler Anker für alle Identitäten

Auf mittlere Sicht wird ein lokales Verzeichnis weiter genutzt



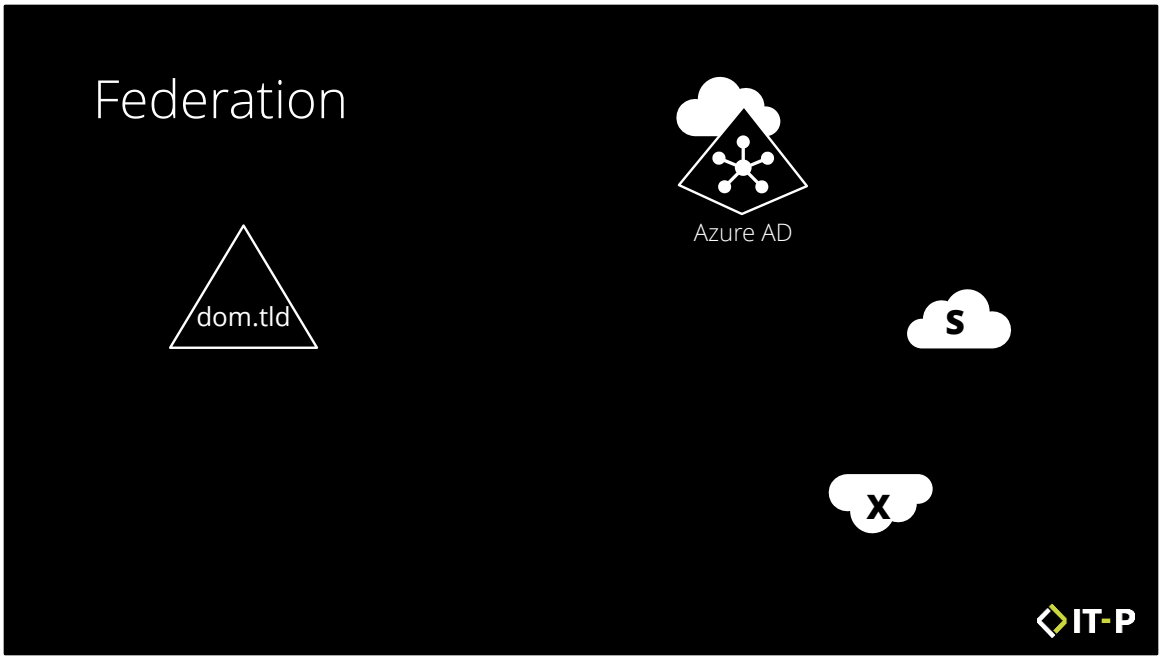
AD als lokaler Anker für alle Identitäten

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



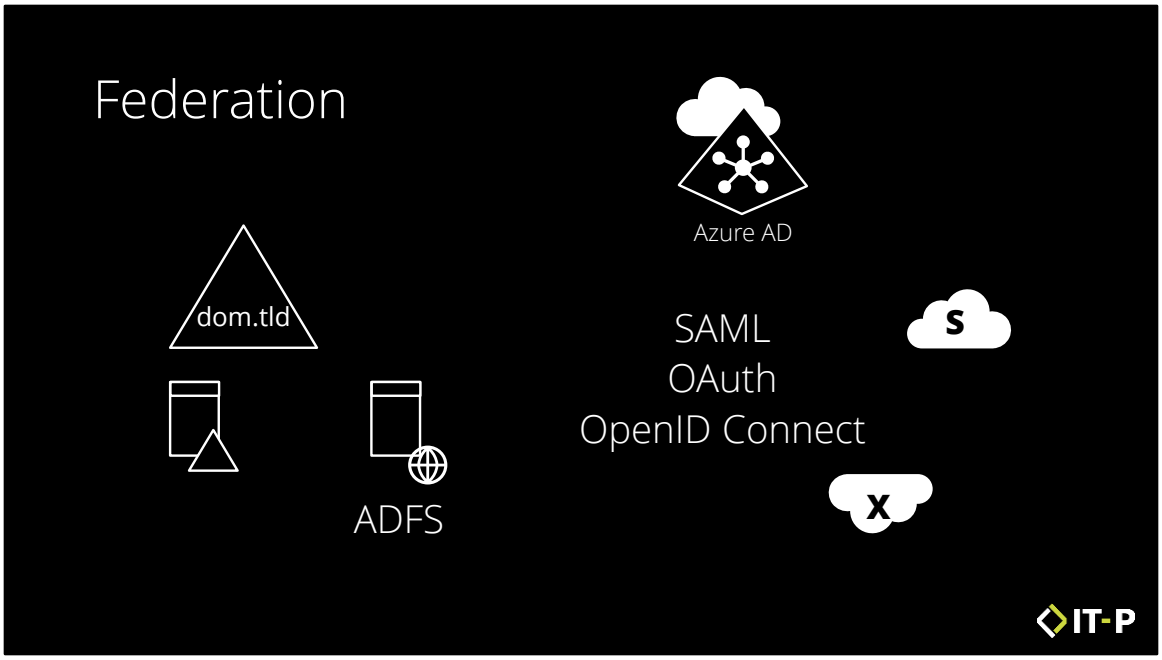
AD als lokaler Anker für alle Identitäten

- Auf mittlere Sicht wird ein lokales Verzeichnis weiter genutzt
- AAD und AADDS sind kein Ersatz, sondern nur eine partielle, flache Abbildung



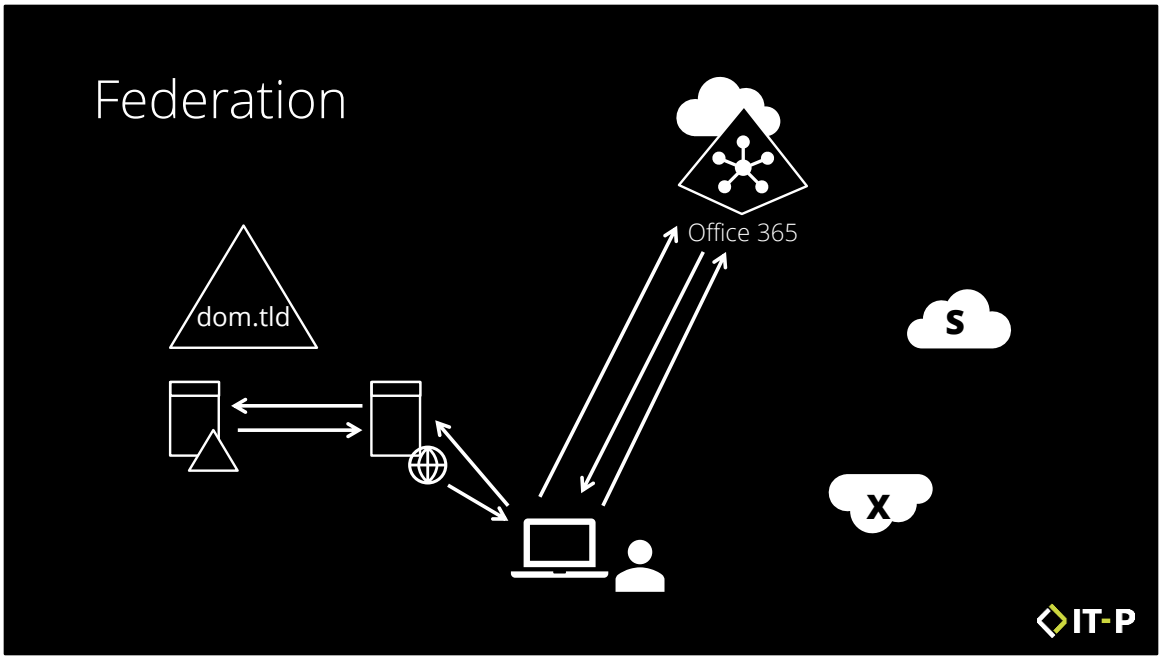
Federation und Authentifizierung

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

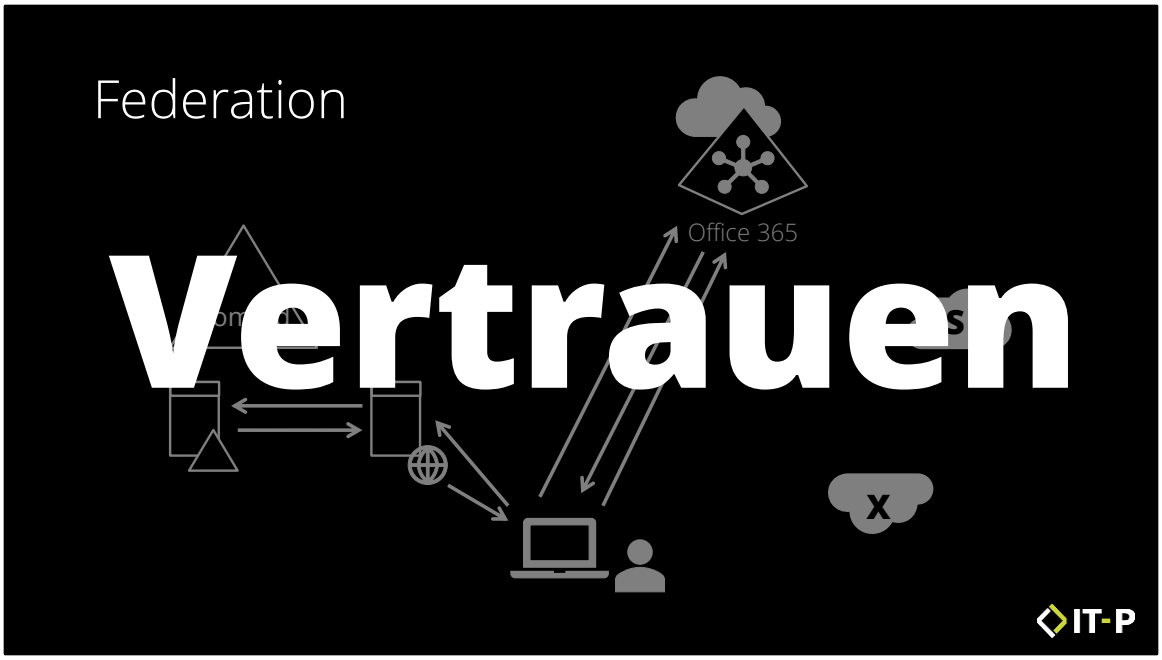


Federation und Authentifizierung: Lösungsansatz

- SAML, OAuth
- ADFS



Verfahren, hier am Beispiel SAML/ADFS

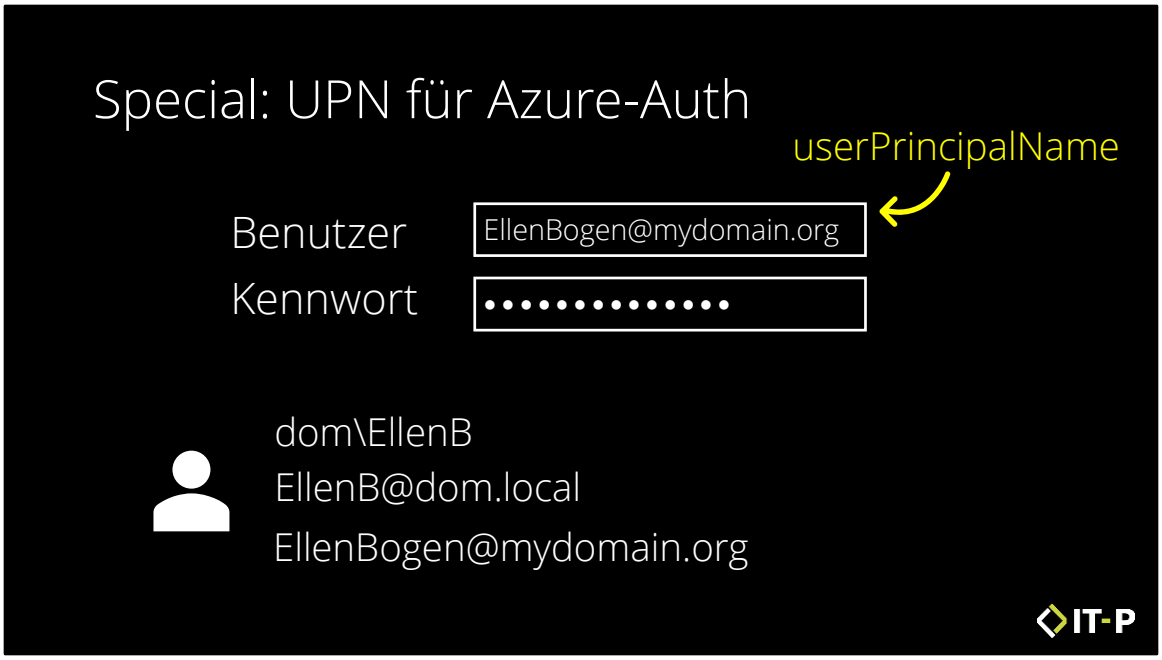


Im Kern steht: Vertrauen
Ich muss dem Provider vertrauen, dass er mit den Daten gut umgeht
Der Provider muss meiner Infrastruktur vertrauen, dass sie für eine ordentliche Auth sorgt
Wir müssen einander vertrauen, dass alles passt und wir schnell auf Fehler reagieren

Ist das nicht gegeben, dann: Finger weg!

Design for change

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



Vorteil: AD-Name = eigens registrierte Domain!
mydomain.org = in Azure für die Anmeldung nutzen

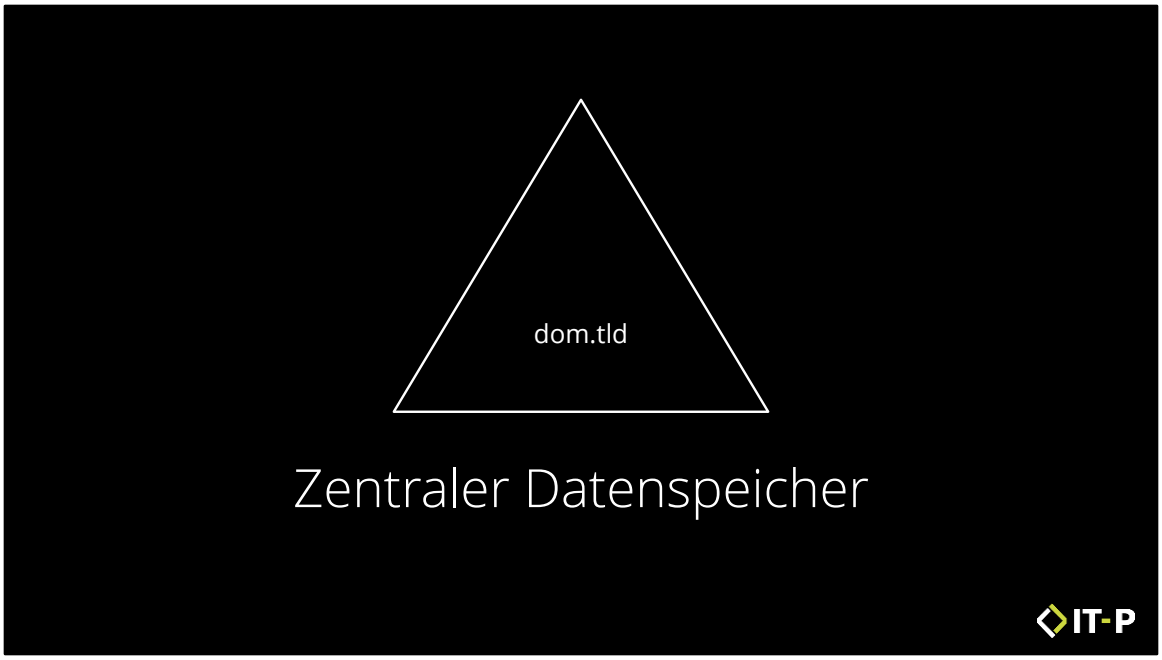
Oder: separate Domain (z.B. Maildomain) als zusätzliches UPN-Suffix
bestehende UPNs auf neues Suffix umstellen
Beispiel Animation:
SAM-Name DOM\EllenB
alter UPN: EllenB@dom.local
neuer UPN: EllenBogen@mydomain.org
Ausweg: AlternateLoginID

Learning: planen, bevor man loslegt!

4

Datenpool: Teile und herrsche

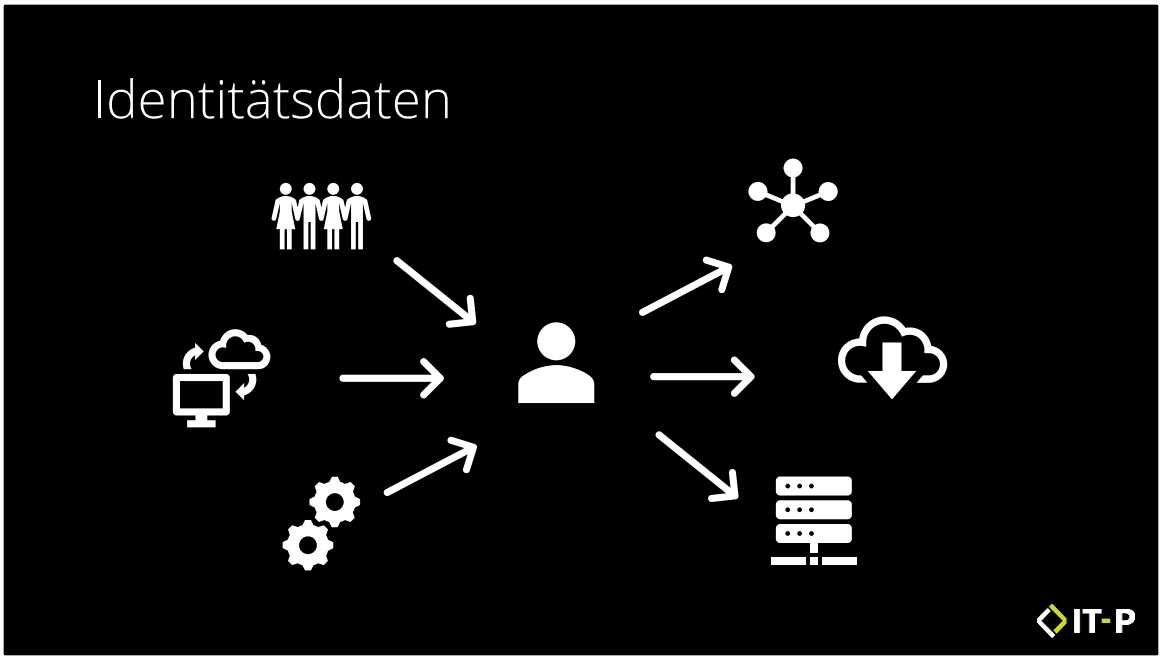
IT-P



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

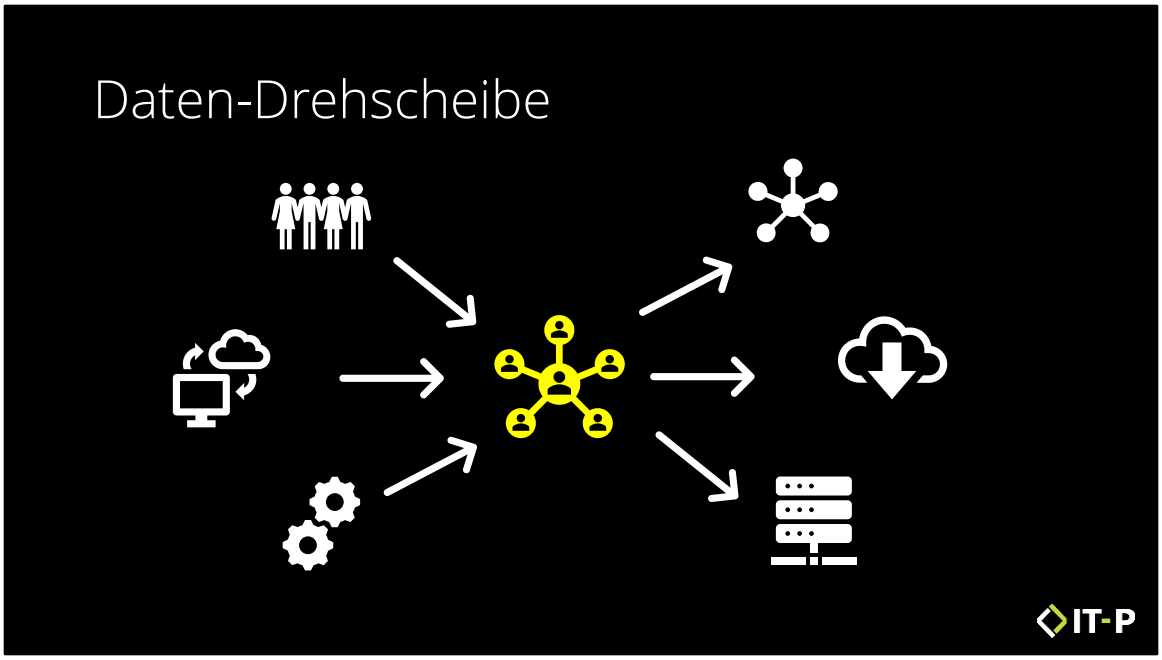
4 Datenpool: Teile und herrsche

- 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

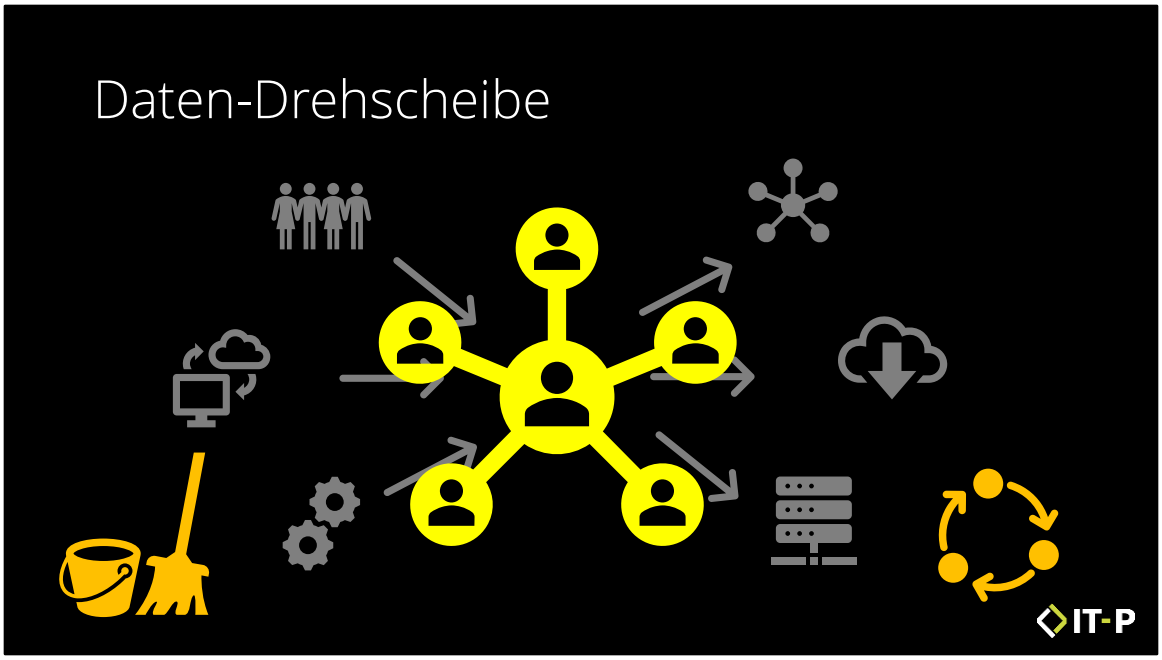


Identität setzt sich zusammen aus vielen Datenquellen …

… und wird an vielen verschiedenen Stellen verwendet



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



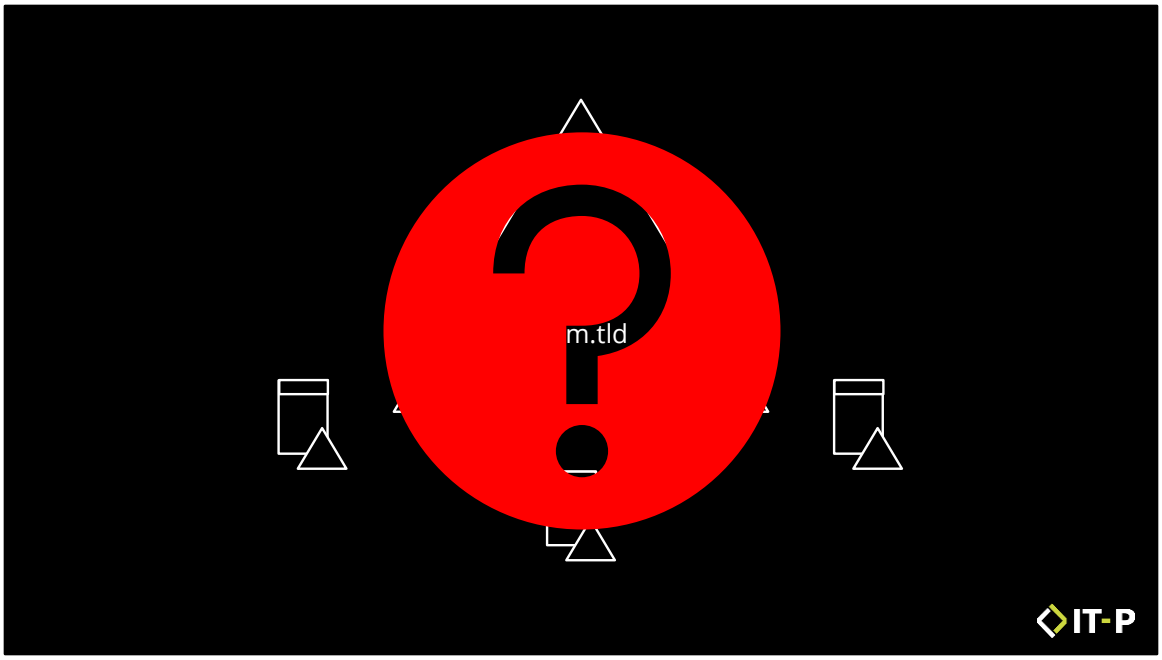
Wichtig in jedem Fall: Datenqualität

Prozesse etablieren, die Daten kontinuierlich zu pflegen

5

Notfall: Von hinten gedacht

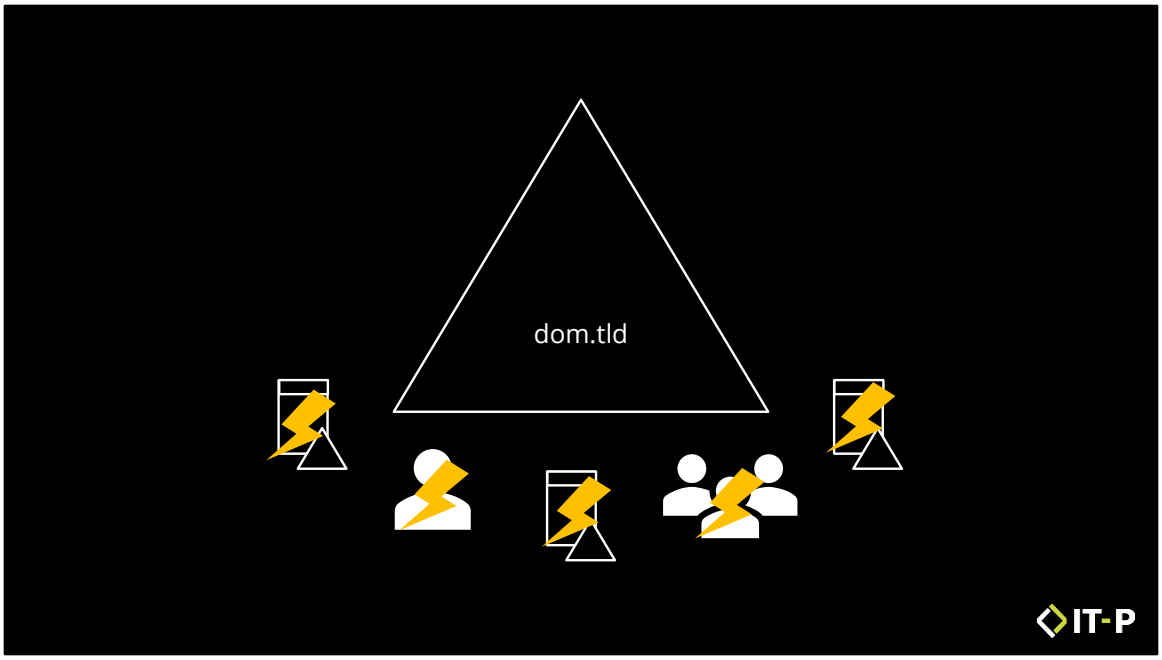
IT-P



Typischer Gedanke: Gegen „Desaster“ absichern

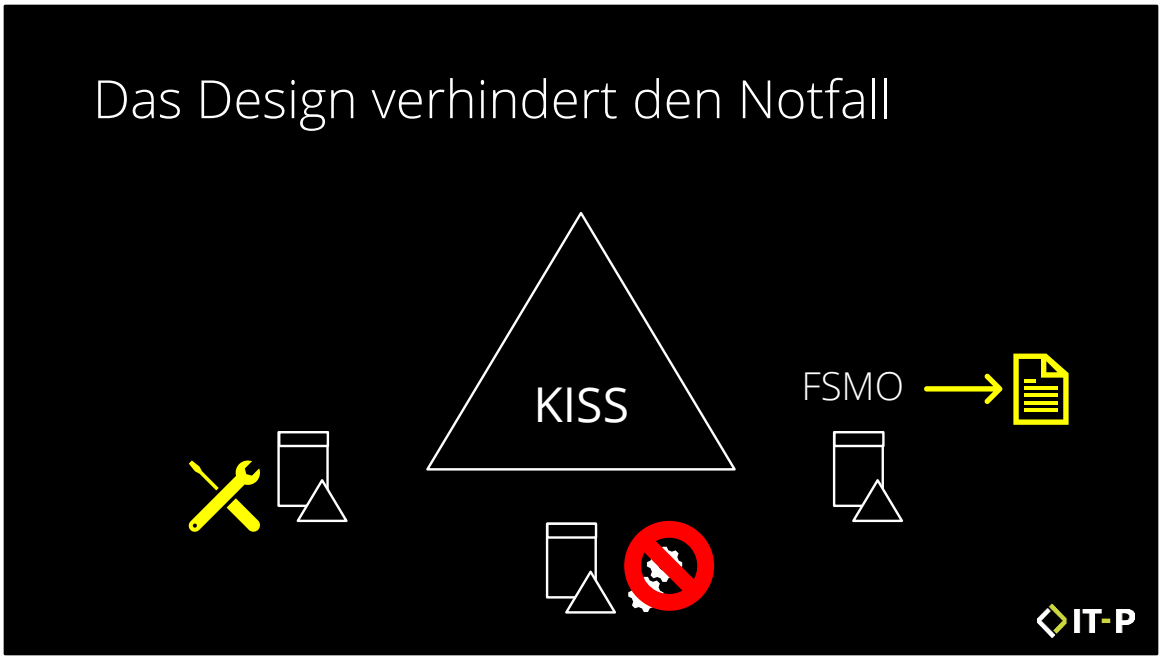
„was muss ich tun, wenn alles ausgefallen ist?“

Problem: In der Praxis kommt das selten vor …



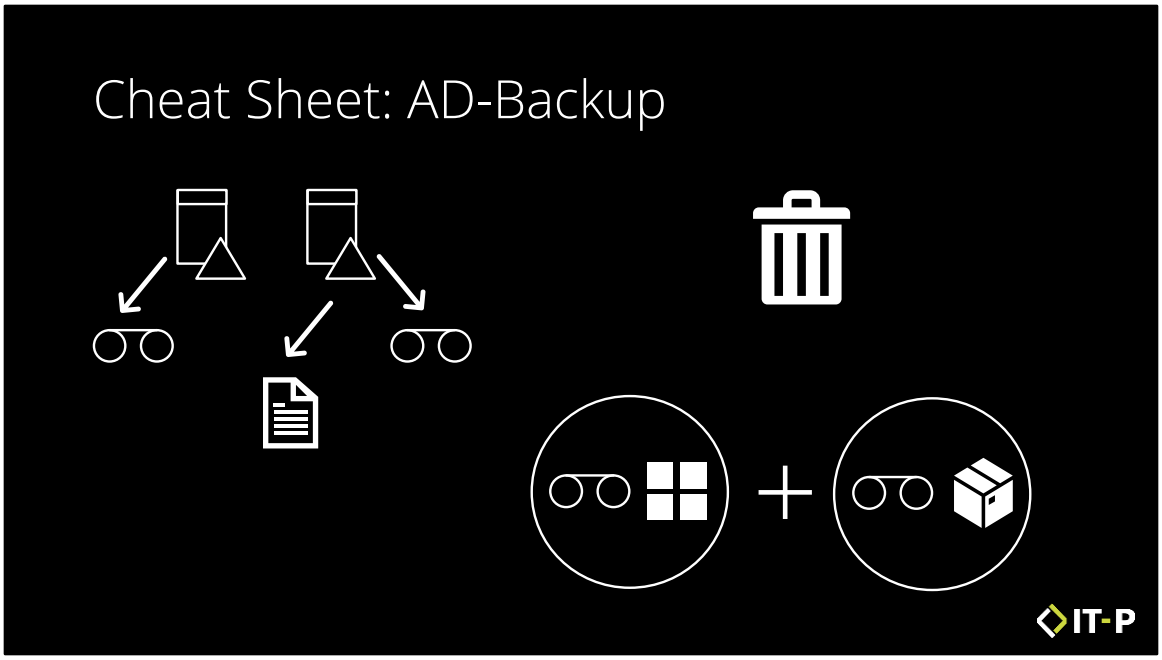
… viel häufiger als ein Komplettausfall sind Einzelstörungen

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

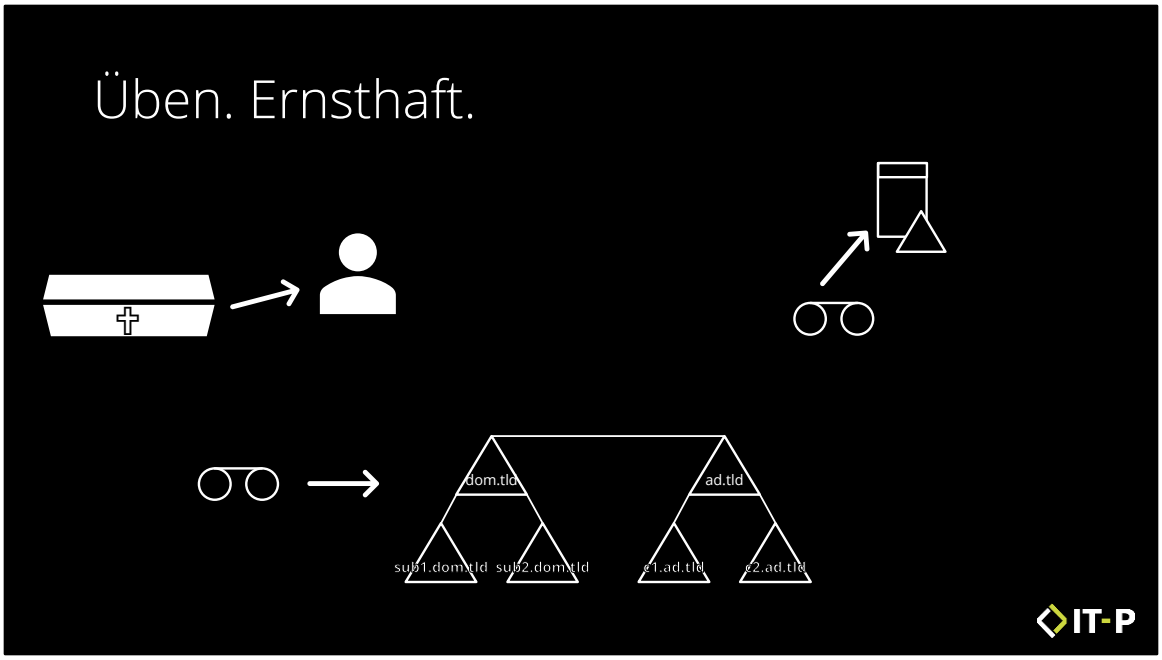
Cheat Sheet Cheat Sheet

- min. 2 DCs pro Domäne sichern
- Textexport aller Objekte bei jedem Backup

```
csvde -f C:\AD\exp.txt -u -l sAMAccountName,objectClass,description
```

- AD-Papierkorb aktivieren
- min. 1 Backup mit Windows Server Backup (Systemstate)
- Andere Produkte nur als Ergänzung

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)

Zum Mitnehmen

- 1 Design: Fundament für Identitäten
  - AD-Design prüfen: Einfach genug?
  - Objektorientiert aufbauen
- 2 Sicherheit: Angriffe sind normal
  - Rollen trennen
  - Admin Tiering – Zero Trust
- 3 Hybrid-Design: Cloud und lokal
  - AD ist der Identitäts-Anker
  - Namensräume planen
- 4 Datenpool: Teile und herrsche
  - Alle Daten an ihrem Platz
  - Datenverteilung steuern
- 5 Notfall: Von hinten gedacht
  - Das Design verhindert den Notfall
  - Recovery üben

IT-P

Nils.Kaczenski@it-p.de

IT-P

Vielen Dank an unsere Sponsoren!

Platinum

Mainzer Datenfabrik

Gold


Bitte gebt uns euer Feedback!
Feedback geben und Geschenk mitnehmen
Vielen Dank!
Experts Live Germany