Cassini I Guiding ahead

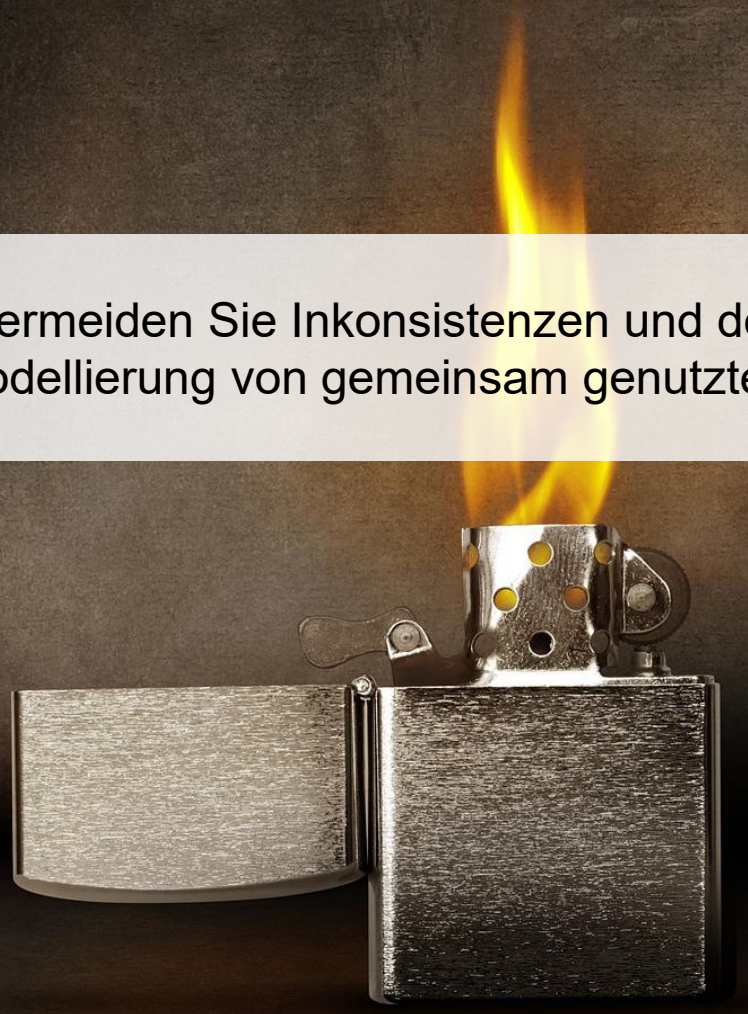
Modellierungsansätze für Basis-IT-Infrastruktur

Am Beispiel des ITDZ Berlin

Jan Graßhoff I Senior Consultant

cassini
GUIDING AHEAD

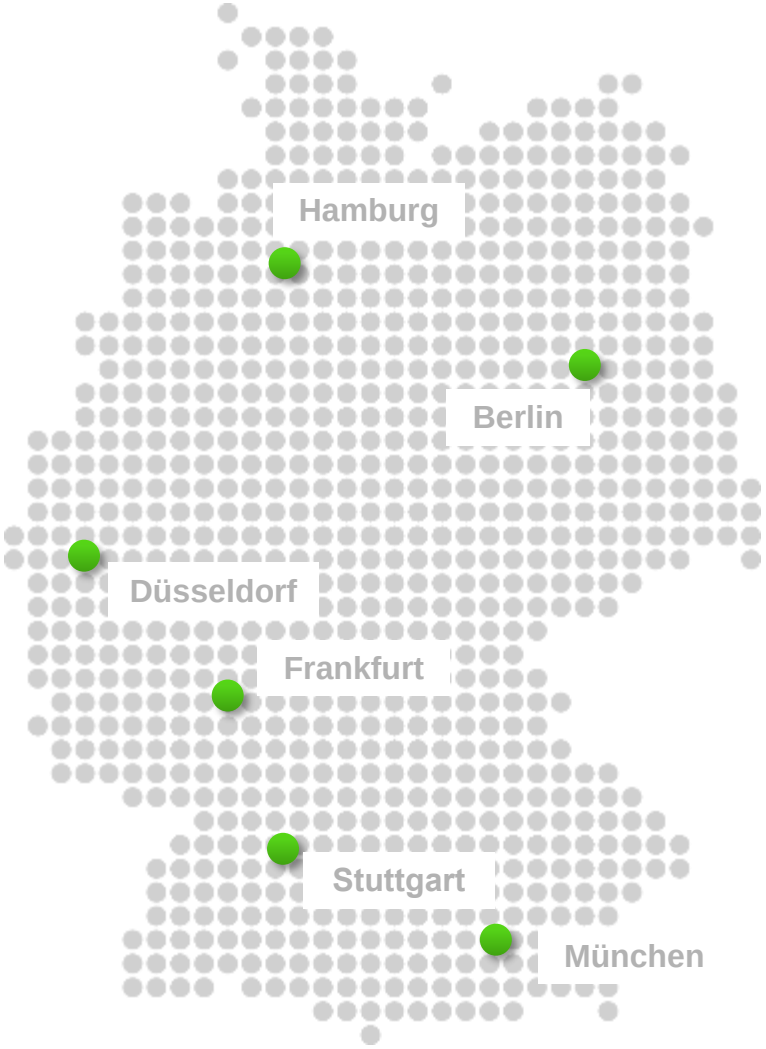
Wie vermeiden Sie Inkonsistenzen und doppelte Arbeit bei der Modellierung von gemeinsam genutzten Komponenten?



Cassini ist Management- und Technologieberatung

- Seit 2006 ist Cassini der Herausforderer und Innovationstreiber unter den Management- und Technologieberatungen
- Mitarbeiter: 170
- Standorte: Düsseldorf, Frankfurt, Berlin, Hamburg, Stuttgart und München
- Klienten: Jeder dritte DAX-Konzern, Bundes- und Landesbehörden, ambitionierte Mittelständler
- Rahmenvertragspartner des Bundes und mehrerer Länder
- Verinice.PARTNER
- Unser Anspruch heißt Guiding ahead:

  Wir führen Klienten durch Wissensvorsprung in die Zukunft

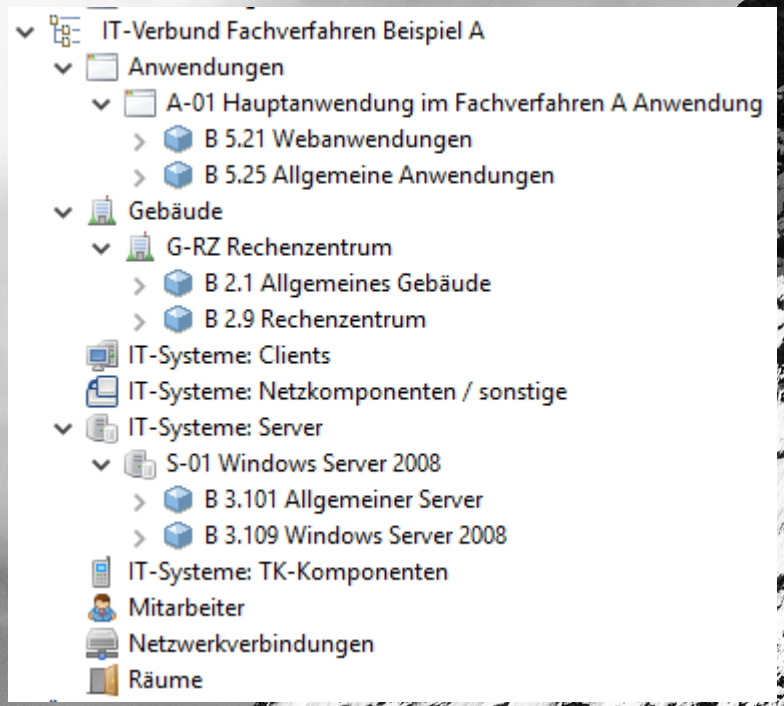


Agenda

1. Herleitung und Problemstellung
2. Zielbild: Beschreibung eines IT-Service
3. Infrastrukturbausteine im ITDZ Berlin
4. Technische Umsetzung in verinice

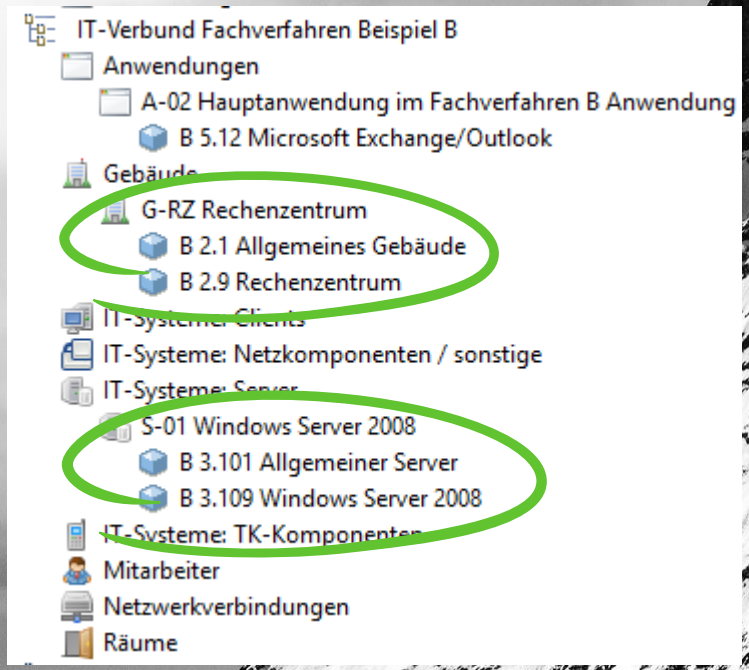
Herleitung und Problemstellung

Bei der Erstellung des ersten IT-Sicherheitskonzepts gibt es eine klare Abfolge von Arbeitsschritten



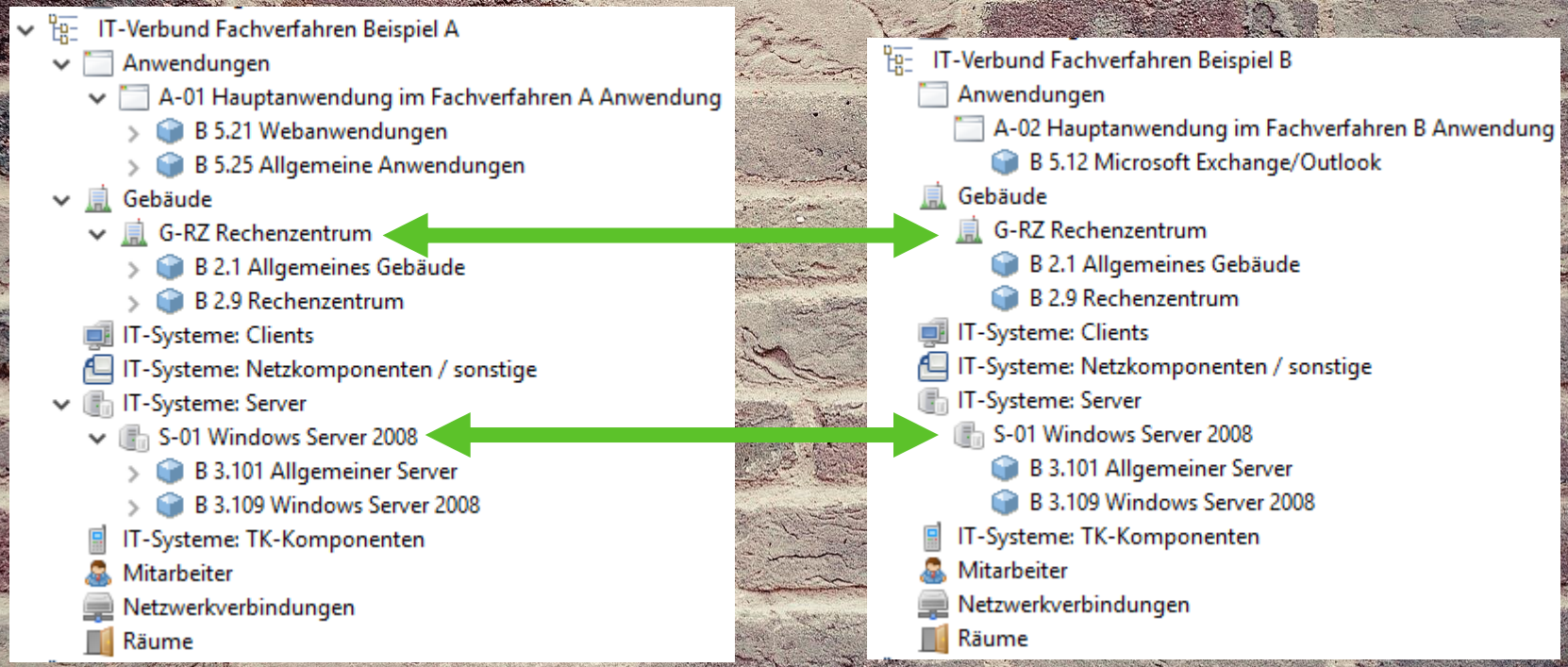
1. Strukturanalyse
2. Bausteinauswahl
3. Basis Sicherheitscheck
4. Umsetzung offener Maßnahmen

Das zweite IT-Sicherheitskonzept führt zu einer Doppelbelastung einzelner Bereiche



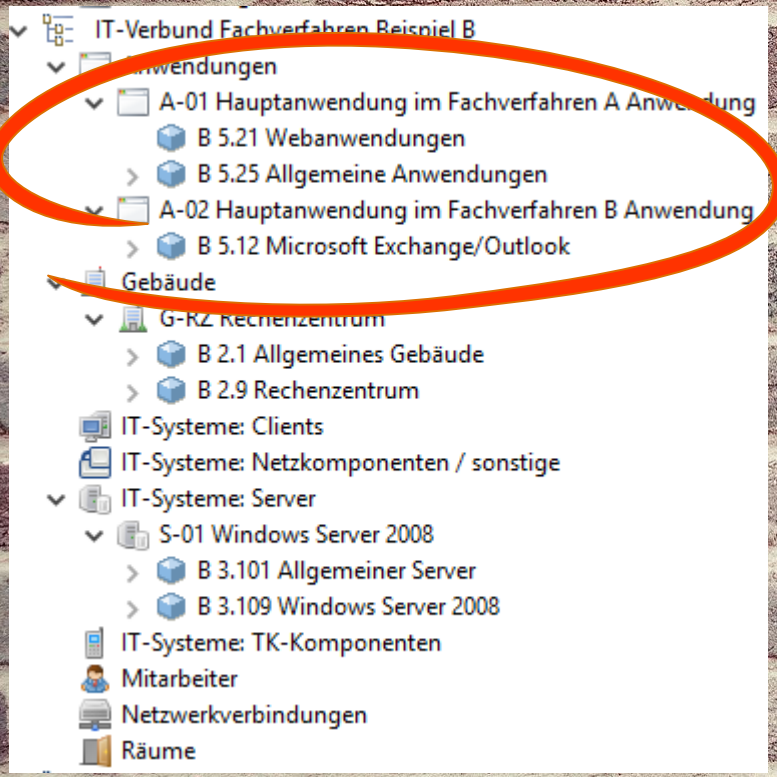
1. Strukturanalyse
2. Bausteinauswahl
3. Basis Sicherheitscheck
4. Umsetzung offener Maßnahmen

Möglichkeit 1: Modellierung von jeweils vollständigen und unabhängigen IT-Verbünden



Doppelte Datenhaltung führt zu Redundanzen
Mehraufwand durch Synchronisation

Möglichkeit 2: Alle Komponenten werden in einem IT-Verbund modelliert



✓ Keine redundante Datenhaltung

- Unübersichtlich: Welche Komponenten benötigt ein Verfahren?
- Fehlende Abgrenzung für eine Zertifizierung
- Kompliziertes Rechtekonzept
- Unklare Verantwortlichkeiten


Zielbild: Beschreibung eines IT-Service

Lösungsansatz: Aus mehrfach genutzten Komponenten werden IT-Services

Jeder IT-Service ist klar abgegrenzt

Fachverfahren können einzeln auditiert werden

IT-Services werden von Fachverfahren als Black-Box genutzt

Es gibt jeweils einen benannten Service-Manager

Infrastrukturbausteine im ITDZ Berlin

Bildquelle: http://www.rbb-online.de/content/dam/rbb/rbb/Bilder%20Infoportal-------/2015/2015_11/Presse/itdz-gebaeude.jpg.jpg/size=708x398.jpg

Beispiel ITDZ Berlin

IT-Dienstleister für die Berliner Landesverwaltung

Anbieter des Bürgertelefons 115

600 Mitarbeitende

Betreiber des Berliner Landesnetzes

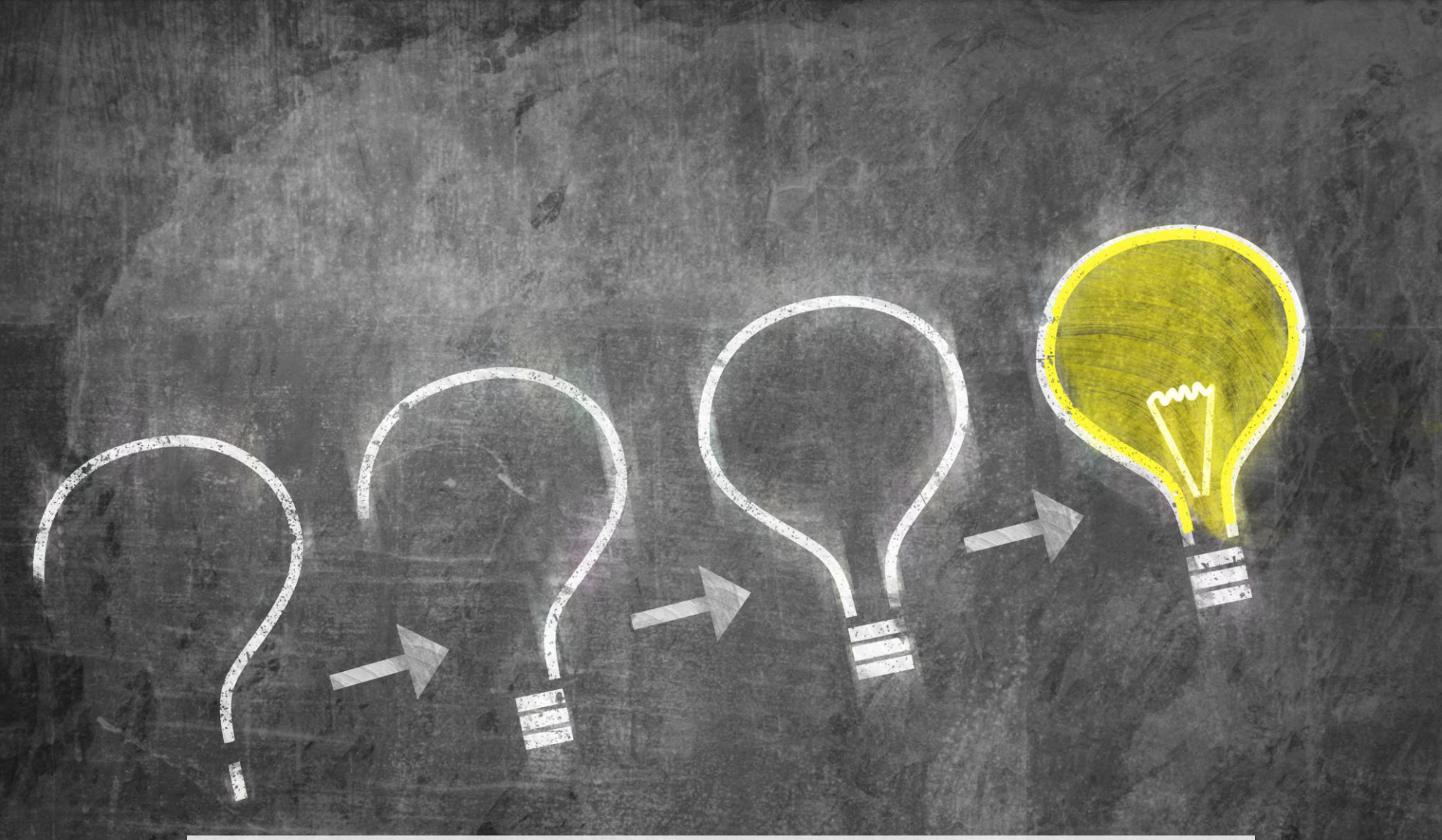
Kunden: u.a. Senats- und Bezirksverwaltungen, DRV

BSI-zertifiziertes Rechenzentrum

Bildquelle: http://www.rbb-online.de/content/dam/rbb/rbb/Bilder%20Infoportal-------/2015/2015_11/Presse/itdz-gebaeude.jpg.jpg/size=708x398.jpg

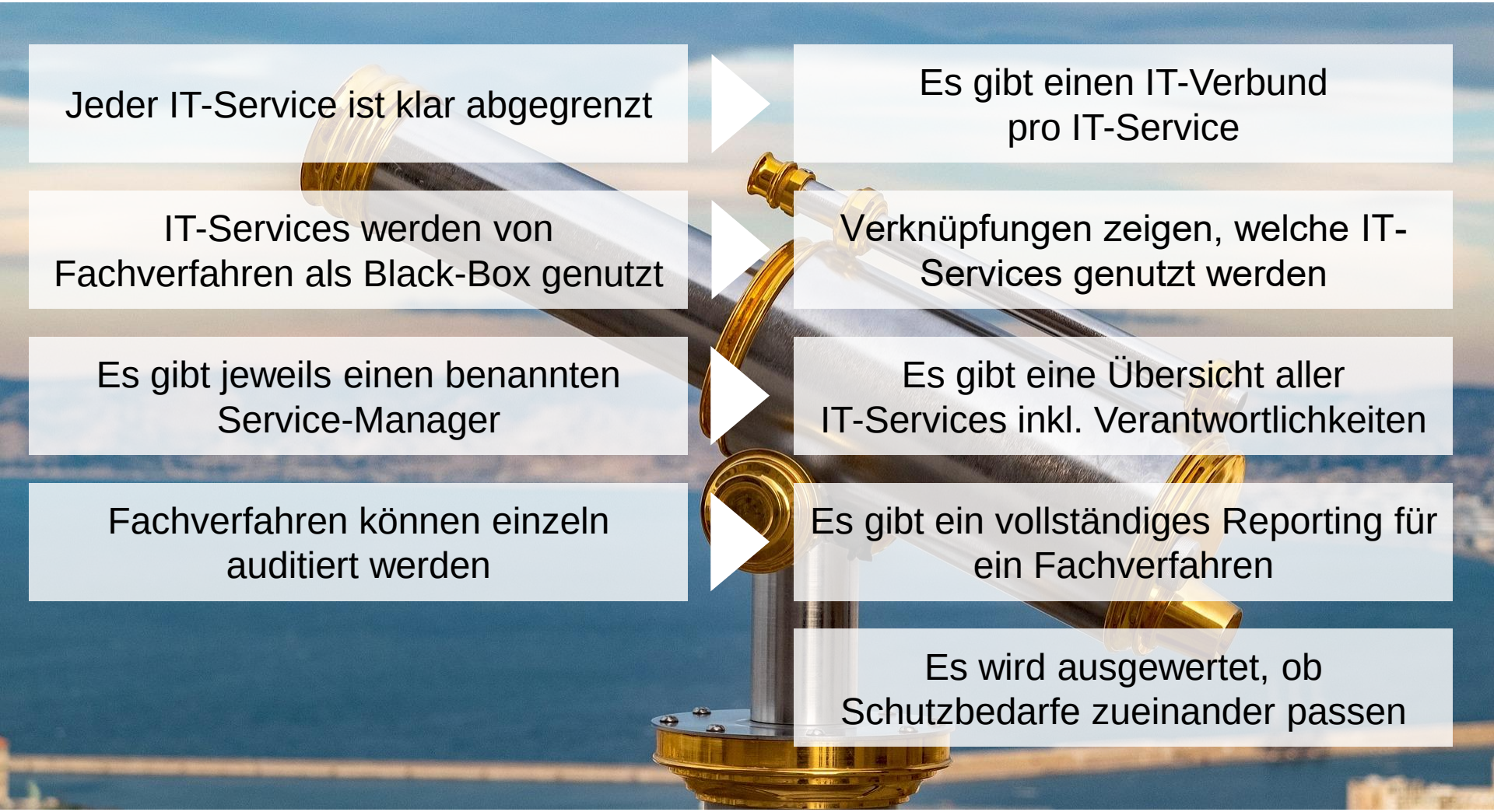
Im Servicekatalog vom ITDZ Berlin befinden sich 43 Infrastrukturbausteine

DC Facility	Netz	Server, Virtualisierung	Storage	Unifiy Communications	Basisdienste ohne Authentifizierung	Dienste mit Authentifizierung	Peripherie
Brandmelde-anlage	LAN	Server inkl. DHCP und BS	Datensicherung (alle Varianten)	Carrieranschluss Sprache und Carrier-Gateways	Firewall (alle Varianten)	VPN (alle Varianten)	Client System
Video-Überwachungs-system	BeLa	Cloud Infrastruktur	Datenspeicherung LAN-basiert	SC (Vermittlung, Auskunft, 115)	Monitoring (alle Varianten)	Administrative Zugänge	Drucken
Zugangskontroll-system	Carrieranschluss Daten	Legacy ESX Infrastruktur	Datenspeicherung SAN-basiert	UC-Service	Active Directory	SMTP Proxy	Transfer PC
KFS Kabelführungs-system	Wartungsnetz Notebook	ADM Terminalservice	SAN	Sprachendpunkte	DNS	Microsoft Exchange	
Leitungen und Kabel (passiv)		Citrix Terminalservice		TK Management	NTP	Datenschleuse	
Infrastruktur RZ (Storm, USV, Klima)				TK-Kopfanlagen TFA-Verbund, Kontaktcenter	PKI		
					HTTP Proxy		
					Softwareverteilung Windows		
					Malware Scanner		
					OS-Härtung		



Technische Umsetzung mit verinice

Für jedes Ziel wird eine technische Umsetzung abgeleitet



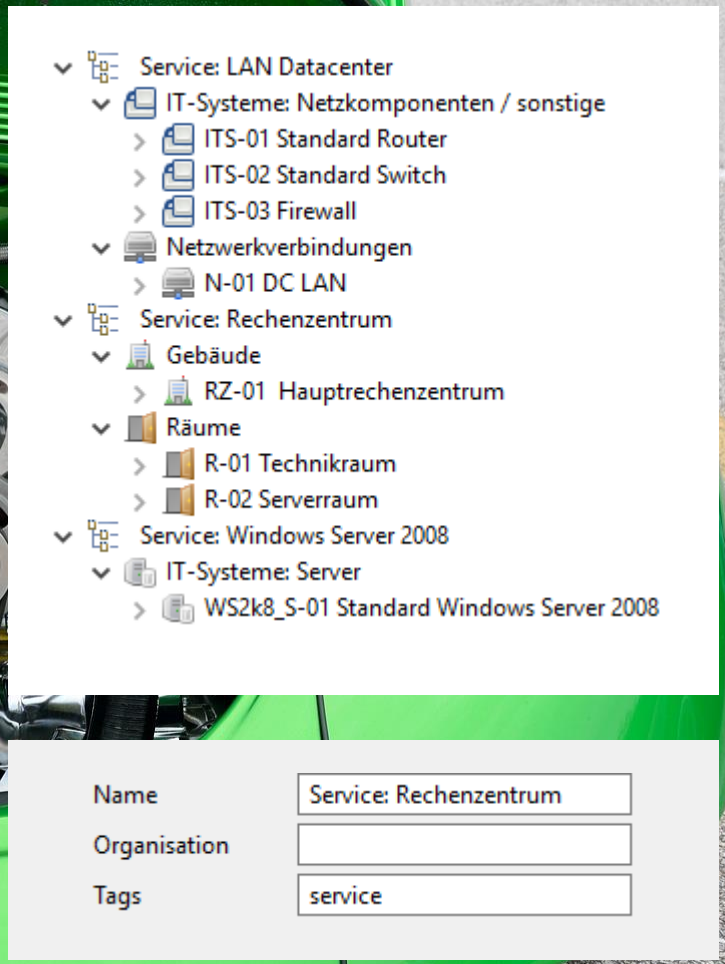
Jeder IT-Service ist klar abgegrenzt	Es gibt einen IT-Verbund pro IT-Service
IT-Services werden von Fachverfahren als Black-Box genutzt	Verknüpfungen zeigen, welche IT-Services genutzt werden
Es gibt jeweils einen benannten Service-Manager	Es gibt eine Übersicht aller IT-Services inkl. Verantwortlichkeiten
Fachverfahren können einzeln auditiert werden	Es gibt ein vollständiges Reporting für ein Fachverfahren
	Es wird ausgewertet, ob Schutzbedarfe zueinander passen

Jeder IT-Service erhält einen eigenen IT-Verbund in verinice

Präfix als Namenskonvention:
„Service“ im Titel

Im IT-Verbund sind alle Komponenten und Bausteine modelliert, die für die Serviceerbringung erforderlich sind

Hinterlegung eines Tags



Vorbereitung für die Verknüpfungen durch Anpassung der SNCA

```
<huientity
    name="IT-Verbund"
    id="itverbund" >

    <huirelation to="anwendung" id="service-relation"
        name="stellt Service bereit für" reversename="nutzt Service von" />

    <huirelation to="person" id="service_manager_relation"
        name="wird gemanagt von" reversename="Servicemanager von" />
```

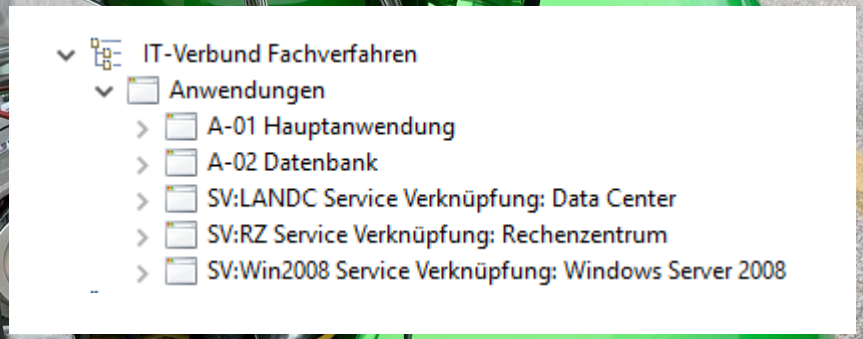
Verknüpfung von Fachverfahren mit IT-Services: Vorbereitung aufseiten des Fachverfahrens

Für jeden genutzten IT-Service wird ein neues Objekt vom Typ Anwendung angelegt

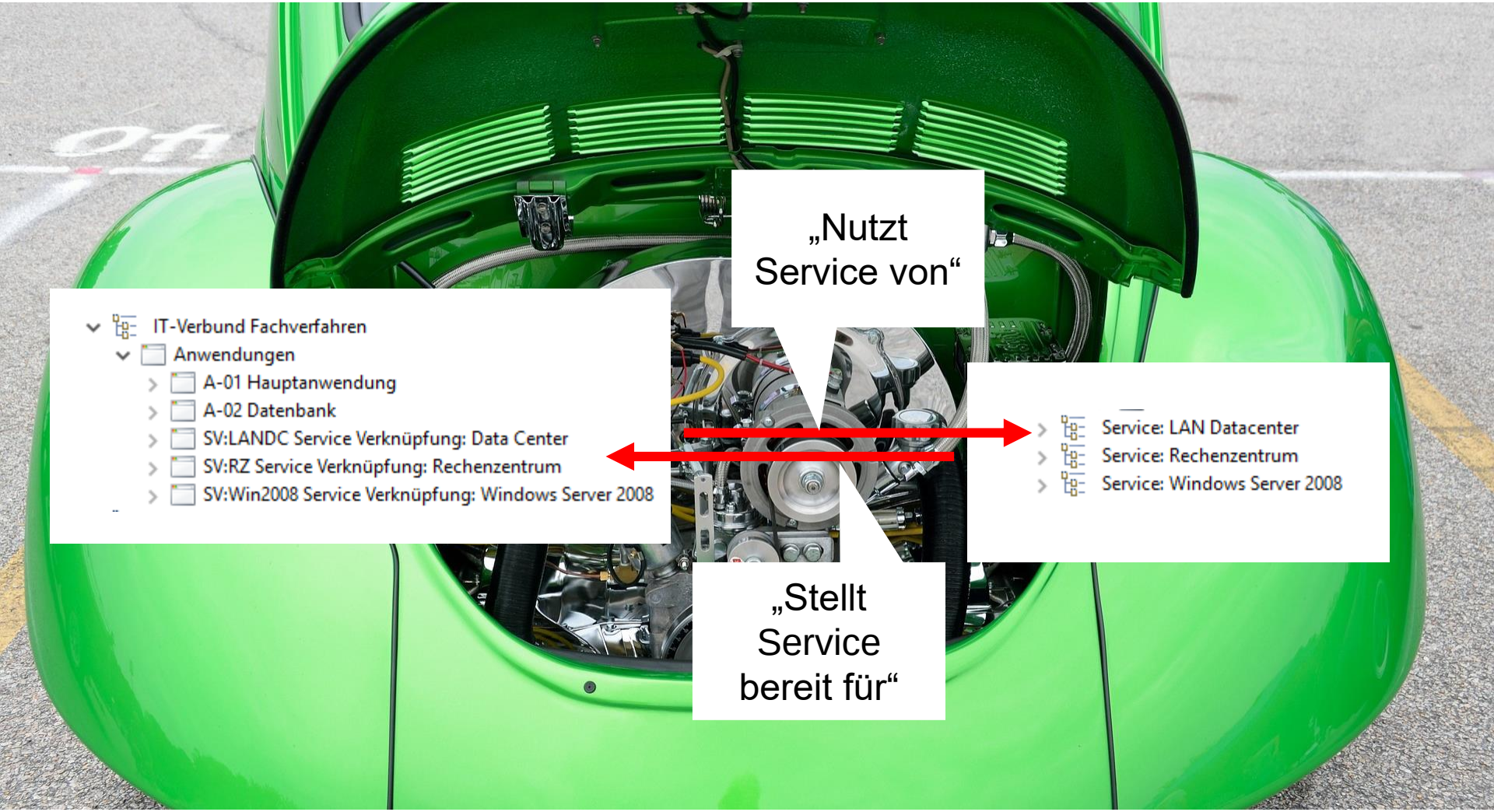
Präfix als Namenskonvention:

- „SV“ im Kürzel
- „Service Verknüpfung“ im Namen

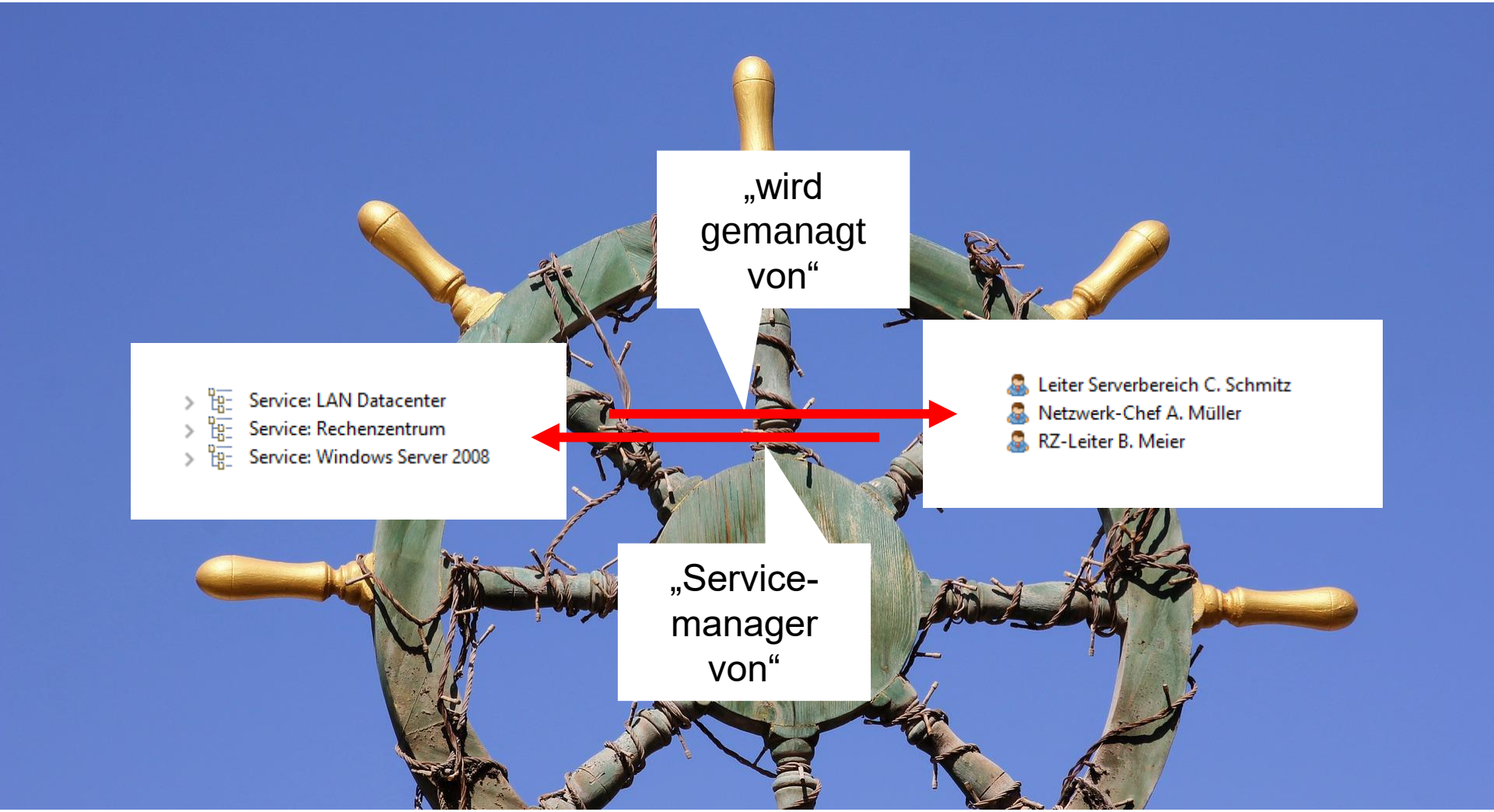
Felder nicht relevant*



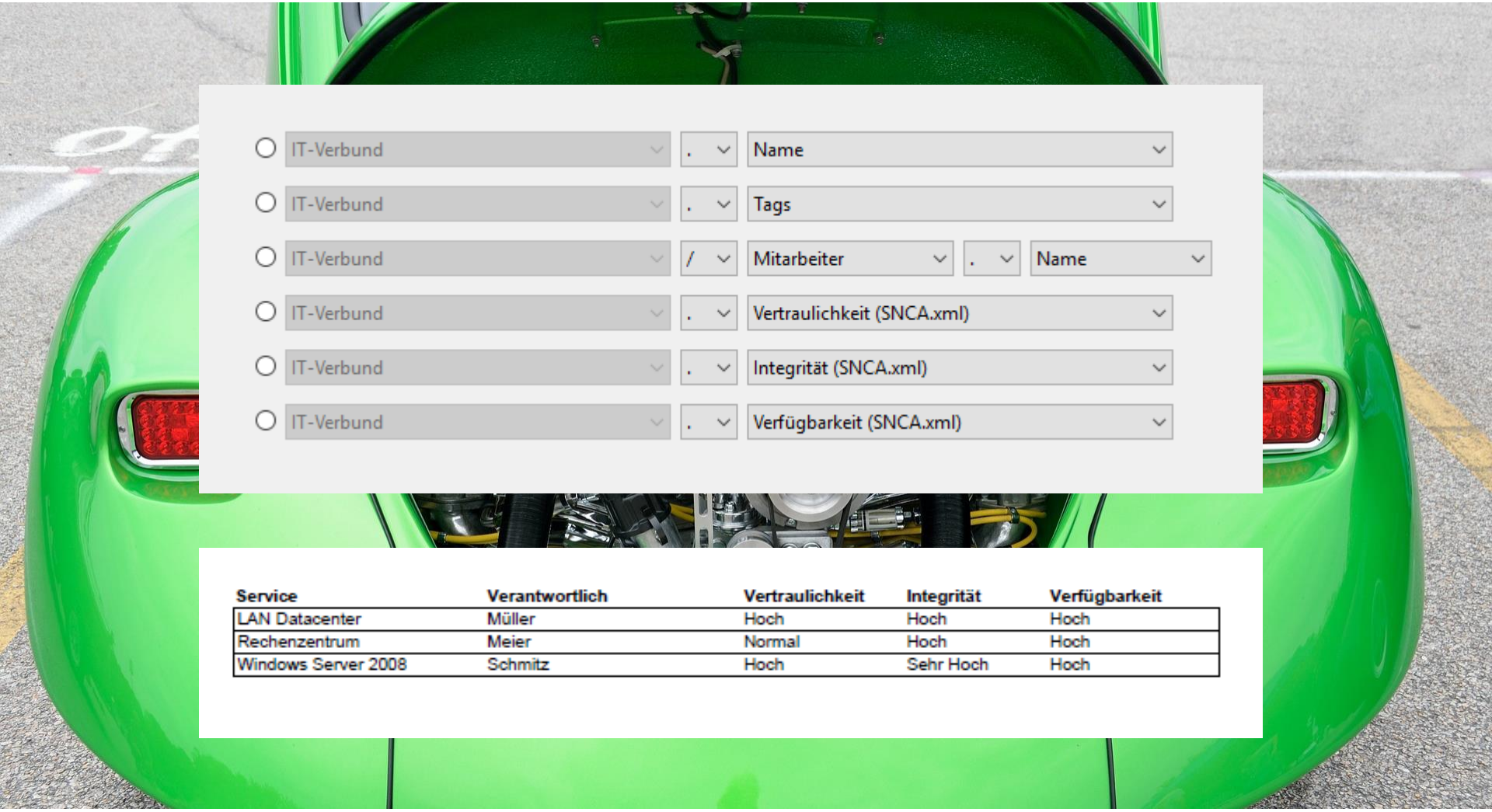
Die Verknüpfung zwischen Fachverfahren und IT-Service erlaubt den Zugriff auf die Maßnahmenumsetzung



Die Servicemanager werden mit den Services verknüpft

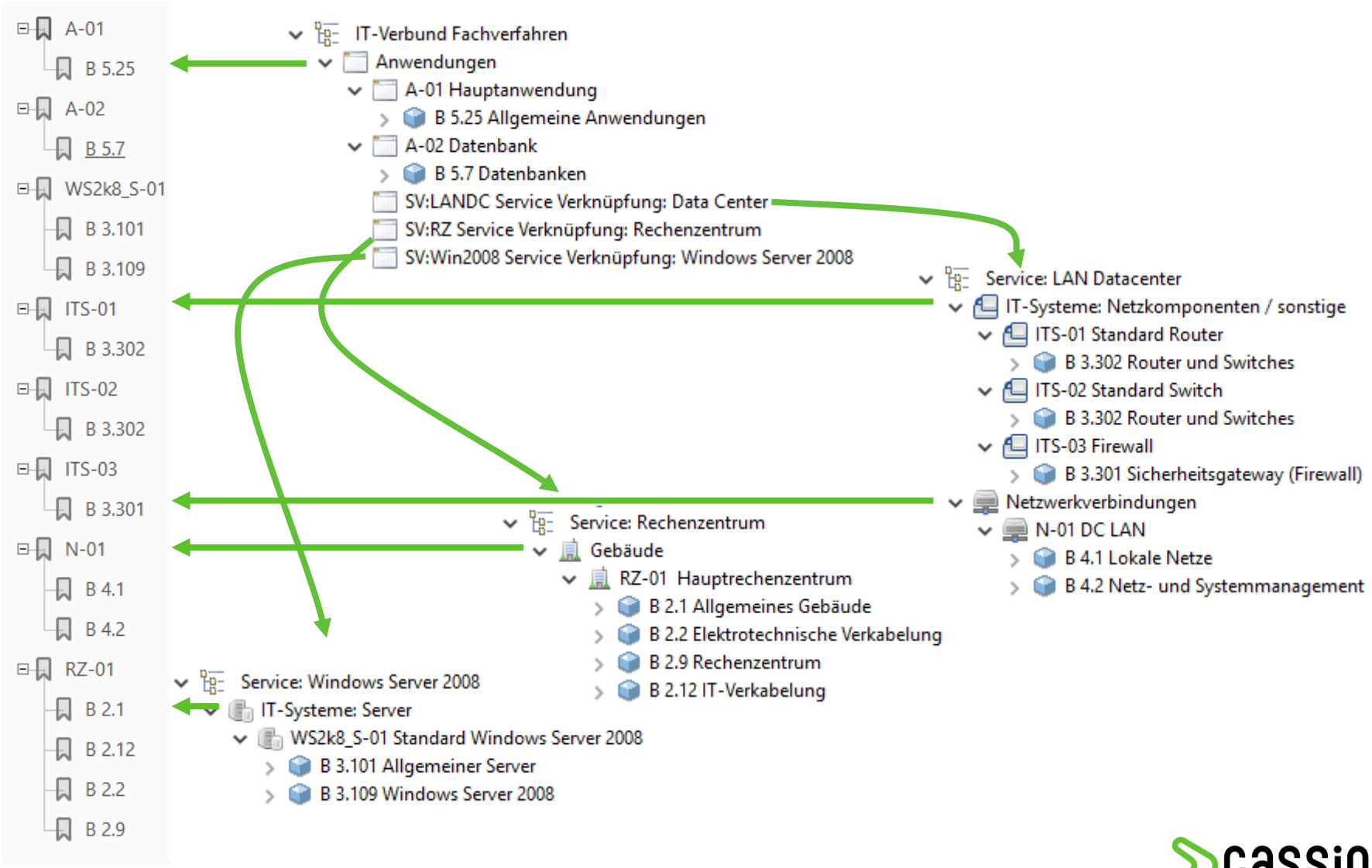


Eine einfache Abfrage ist die Grundlage für den Servicekatalog

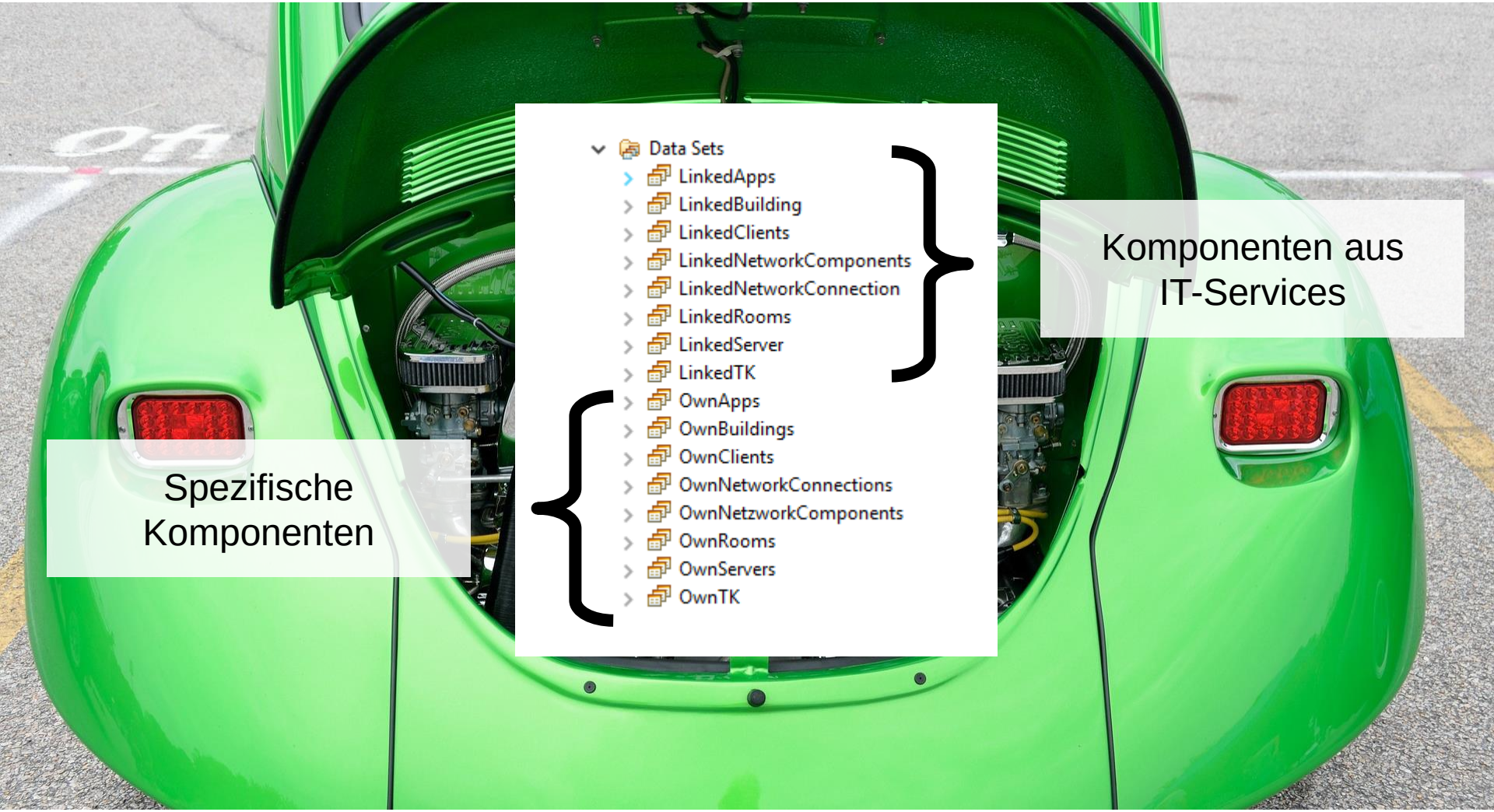


Service	Verantwortlich	Vertraulichkeit	Integrität	Verfügbarkeit
LAN Datacenter	Müller	Hoch	Hoch	Hoch
Rechenzentrum	Meier	Normal	Hoch	Hoch
Windows Server 2008	Schmitz	Hoch	Sehr Hoch	Hoch

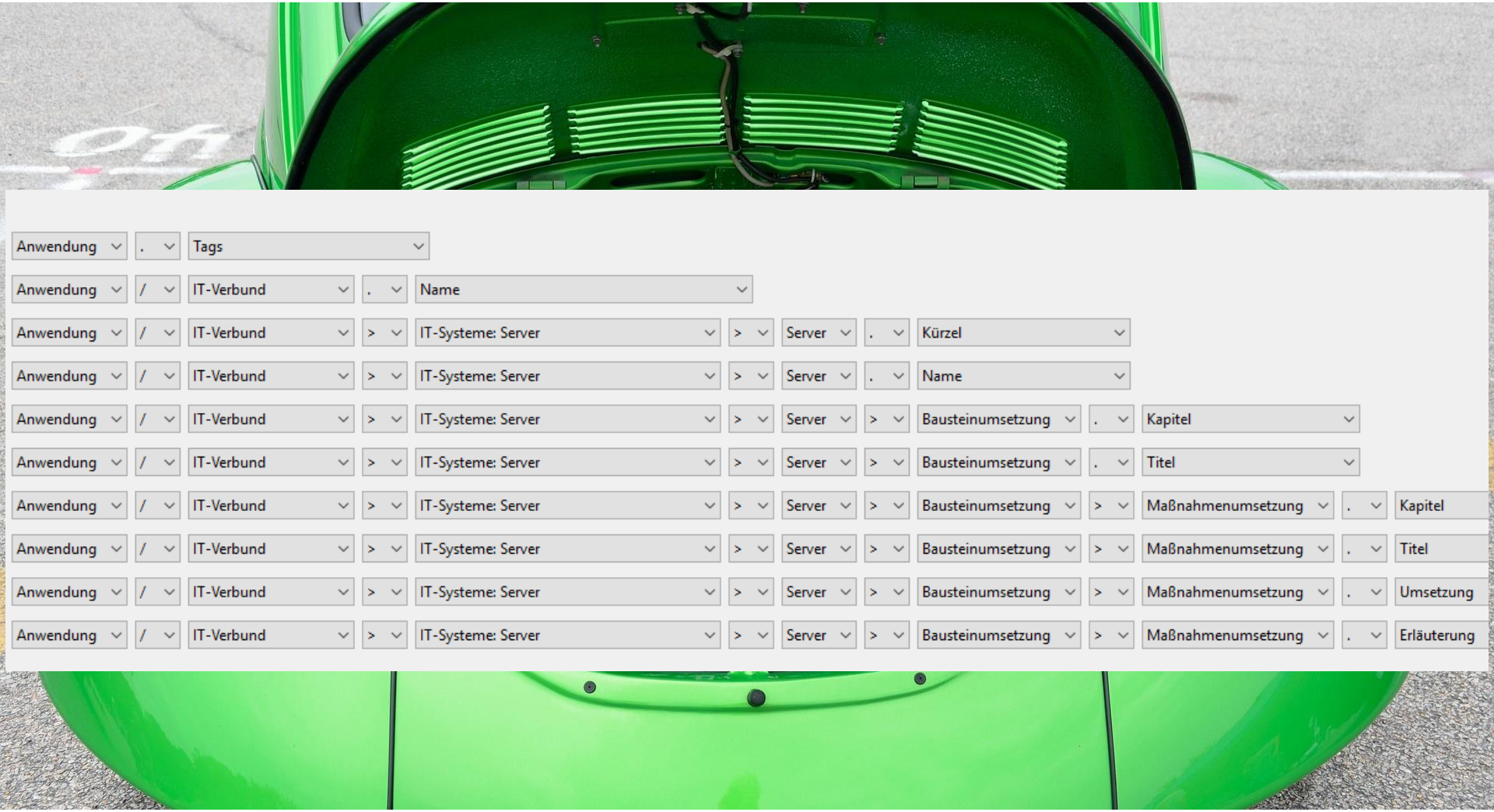
Ein Report muss alle für das Verfahren relevanten Maßnahmen darstellen



Im vdesigner werden für jede Kategorie zwei LTR Data Sets erstellt



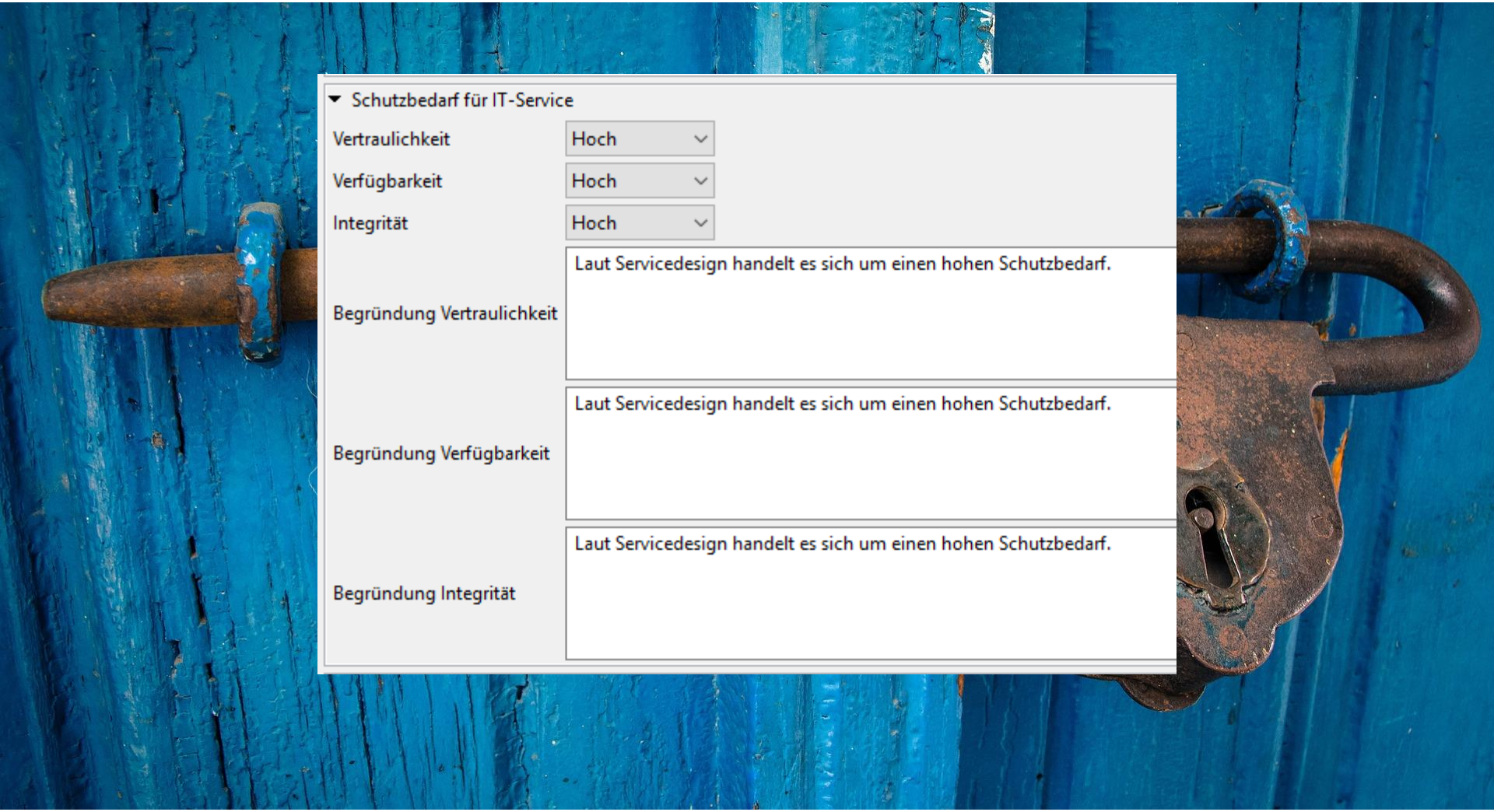
Innerhalb der Data Sets werden entsprechend der Verknüpfungen die Komponenten der IT-Services abgefragt



Für alle IT-Services werden die erfüllten Schutzbedarfe festgelegt und dokumentiert

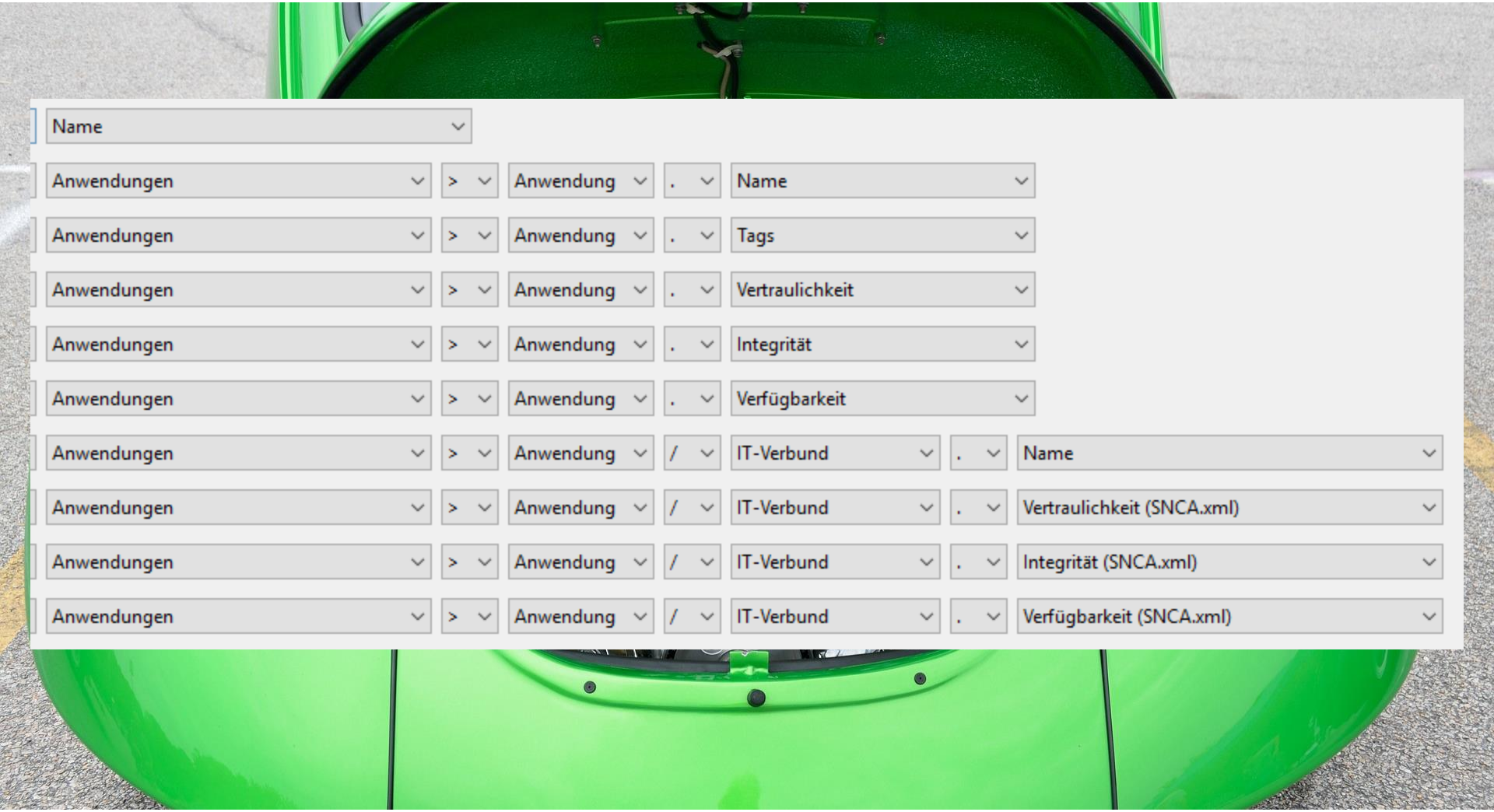
```
<huipropertygroup
    id="service_group_schutzbedarf"
    name="Schutzbedarf für IT-Service">
    <huiproperty
        id="service_vertraulichkeit"
        name="Vertraulichkeit"
        inputtype="singleoption">
        <option
            id="service_vertraulichkeit_normal"
            name="Normal" />
        <option
            id="service_vertraulichkeit_hoch"
            name="Hoch" />
        <option
            id="service_vertraulichkeit_sehrhoch"
            name="Sehr Hoch" />
    </huiproperty>
```

Nach der SNCA Änderung können Schutzbedarfe für IT-Services hinterlegt werden



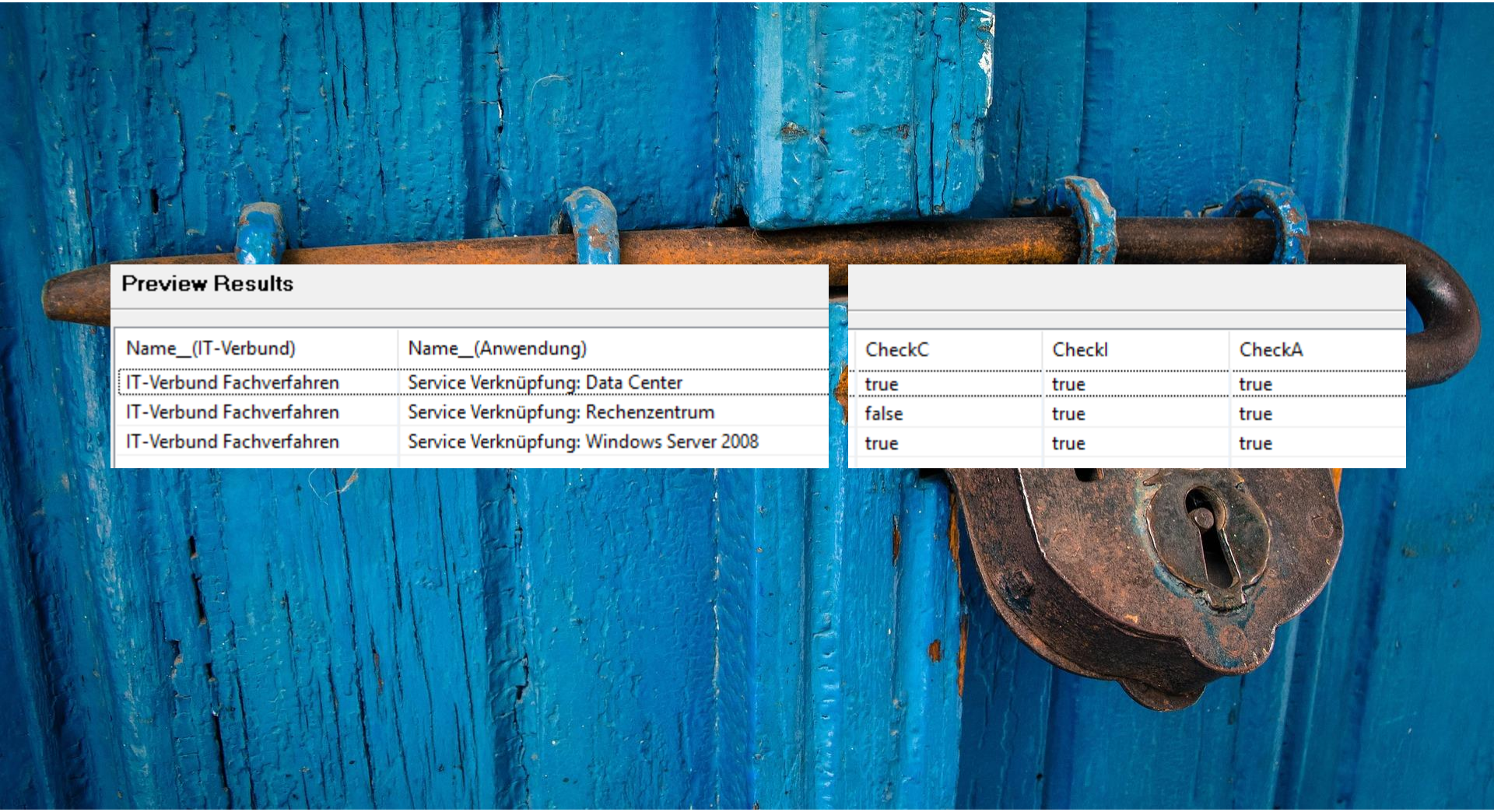
Der aus Sicht des Fachverfahrens benötigte Schutzbedarf wird an den Serviceverknüpfungen dokumentiert

Ein Data Set fragt die Schutzbedarfe von Serviceverknüpfungen und IT-Services ab



Name								
Anwendungen	>	Anwendung	.	Name				
Anwendungen	>	Anwendung	.	Tags				
Anwendungen	>	Anwendung	.	Vertraulichkeit				
Anwendungen	>	Anwendung	.	Integrität				
Anwendungen	>	Anwendung	.	Verfügbarkeit				
Anwendungen	>	Anwendung	/	IT-Verbund	.	Name		
Anwendungen	>	Anwendung	/	IT-Verbund	.	Vertraulichkeit (SNCA.xml)		
Anwendungen	>	Anwendung	/	IT-Verbund	.	Integrität (SNCA.xml)		
Anwendungen	>	Anwendung	/	IT-Verbund	.	Verfügbarkeit (SNCA.xml)		

Die ausgelesenen Schutzbedarfe werden innerhalb der Abfrage verglichen und bilden die Grundlage für einen Report



Preview Results

Name__(IT-Verbund)	Name__(Anwendung)
IT-Verbund Fachverfahren	Service Verknüpfung: Data Center
IT-Verbund Fachverfahren	Service Verknüpfung: Rechenzentrum
IT-Verbund Fachverfahren	Service Verknüpfung: Windows Server 2008

CheckC	CheckI	CheckA
true	true	true
false	true	true
true	true	true

Fazit: Mit kleinen Anpassungen und zusätzlichen Reports können IT-Services mit verinice modelliert werden

Technische Abbildung durch die Hintertür

Trotz sinnvoller Trennung von IT-Verbünden sind keine Redundanzen notwendig

Das Vorgehen ist zertifizierungssicher

Ziel erreicht: Die Anforderungen zur Modellierung von IT-Services sind erfüllt

Welche Fragen darf ich Ihnen beantworten?

Jan Graßhoff
Senior Consultant
Cassini Consulting
jan.grasshoff@cassini.de

Cassini Consulting
Niederlassung Berlin

Jan Graßhoff

Oberwallstraße 24
10117 Berlin
Deutschland
T +49 (0)151 11 44 68 67
F +49 (0)30 50 10 14 14
jan.grasshoff@cassini.de
visit www.cassini.de