Total IT-Security

Fortgeschrittenes Sicherheitsmanagement und durchgängige Durchsetzung von Sicherheitspolitiken für komplexe IT-Infrastrukturen

Thomas J. Wilke, tub@tjw.li

Gliederung

- Begriffe
- Ausgangssituation / Ziele / Anforderungen
- Problemstellungen
- Strategien
- Element Identification Authority (EIA)
- Wirkverbindliche Elemente (Trusted Points)
- Zusammenfassung

Begriffe

- Elemente
  - Subjekte: aktive Entitäten (z. B. Personen, Rechner, …)
  - Objekte: passive Entitäten (z.B. Dokumente, Software, …)

- Sicherheit

  Sicherheit ist ein Maß für die Schutzbedürftigkeit von Objekten oder Subjekten in einem definierten Umfeld.
  Die Schutzbedürftigkeit korreliert mit der (wirtschaftlichen) Bedeutung, die dem Objekt oder Subjekt im jeweiligen Umfeld zugeschrieben wird.

Begriffe

- Offene Systeme

  Systeme, deren Funktionalität im regulären Betrieb aufgrund ihrer Architektur prinzipiell verändert werden kann.

- IT-Infrastruktur

  Eine IT-Infrastruktur ist eine Menge von Subjekten und Objekten, die im Zusammenhang mit der technischen Darstellung und Verarbeitung von Daten steht und die der hoheitlichen Verantwortung einer (natürlichen oder juristischen) Person zugeordnet ist.

Ausgangssituation: technische Aspekte

- Etablierte und akzeptierte technische Systeme
- Hohe Heterogenität der technischen Strukturen
- Unterschiedliche Wirkebenen und hohe Funktionsvernetzung
- Offene Systeme zur Verarbeitung sicherheitsrelevanter Funktionalität
- Sicherungsmechanismen mit sehr begrenztem Sicherungsfokus, die isoliert voneinander wirken.

Ausgangssituation: organisatorische Aspekte

- Mangelnde Festlegung und Formalisierung von Organisations- und Kompetenzstrukturen
- Mangelnde Sicherheitsregelwerke und Risikovorsorge
- Zu erfüllende ökonomische und gesetzliche Vorgaben
- Outsourcing
- Geringe Transparenz der technischen Gegebenheiten

Ziele

- Optimierung existierender und/oder Etablierung neuartiger Geschäftsprozesse zur Effizienzsteigerung und/oder Wertsteigerung des Betriebs
- Funktionale Flexibilität, um auf marktwirtschaftliche und gesetzliche Veränderungen angemessen reagieren zu können
- Kosten/Nutzen Maximierung des IT-Betriebs.
- Wahrung der Betriebssicherheit beim Einsatz von IT-Systemen

Anforderungen

- Schutz von Werten innerhalb der IT-Systeme
- Verankerung von Mechanismen in IT-Systemen zur Wahrung wirtschaftlicher & gesetzlicher Regeln
- „Skalierbare“ Sicherheit, mit der Schutzwirkung und Gefährdungslage in Übereinstimmung gebracht werden können
- Wirkungsverzahnte Sicherungsverfahren, die Prävention, Erkennung und Reaktion auf verschiedenen Wirkebenen realisieren

Problemstellungen

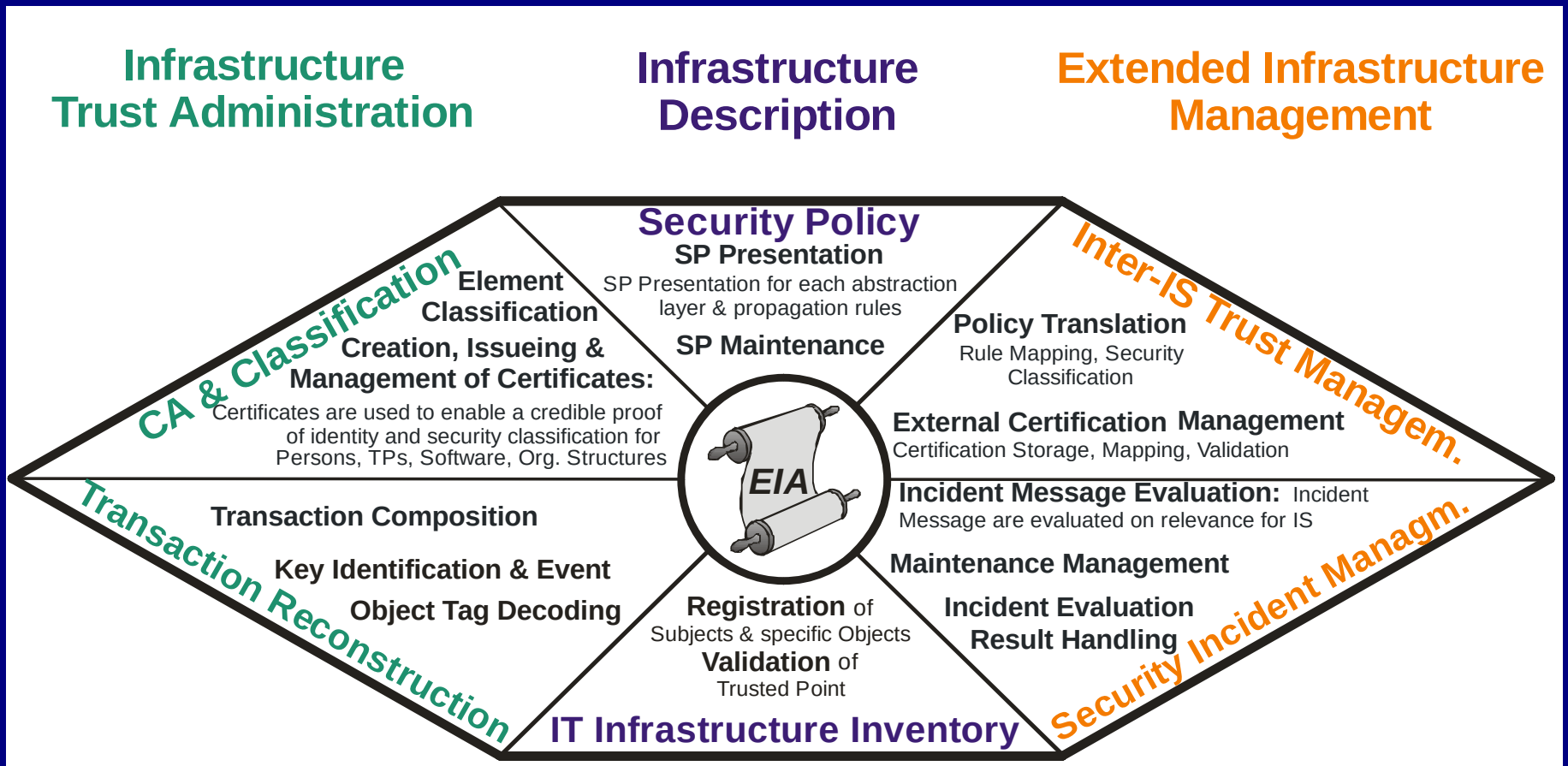
- Homogene Durchsetzung von Sicherheitsregelwerken innerhalb der IT-Systeme
- Verbindliche Nachvollziehbarkeit der Vorgänge innerhalb der IT-Systeme
- Direkte Durchsetzung der organisatorischen Kompetenzstrukturen innerhalb der IT-Systeme
- Datenschutz
- Erkennung und Behandlung von unbekannten Bedrohungssituationen

Strategien

Komplexitätsreduzierung

- Identifizierbarkeit der Elemente einer IT-Infrastruktur
- Funktionale Isolierbarkeit der Elemente einer IT-Infrastruktur
- Strategische Informationsverteilung

Element Identification Authority



Wirkverbindliche Elemente (TPs)

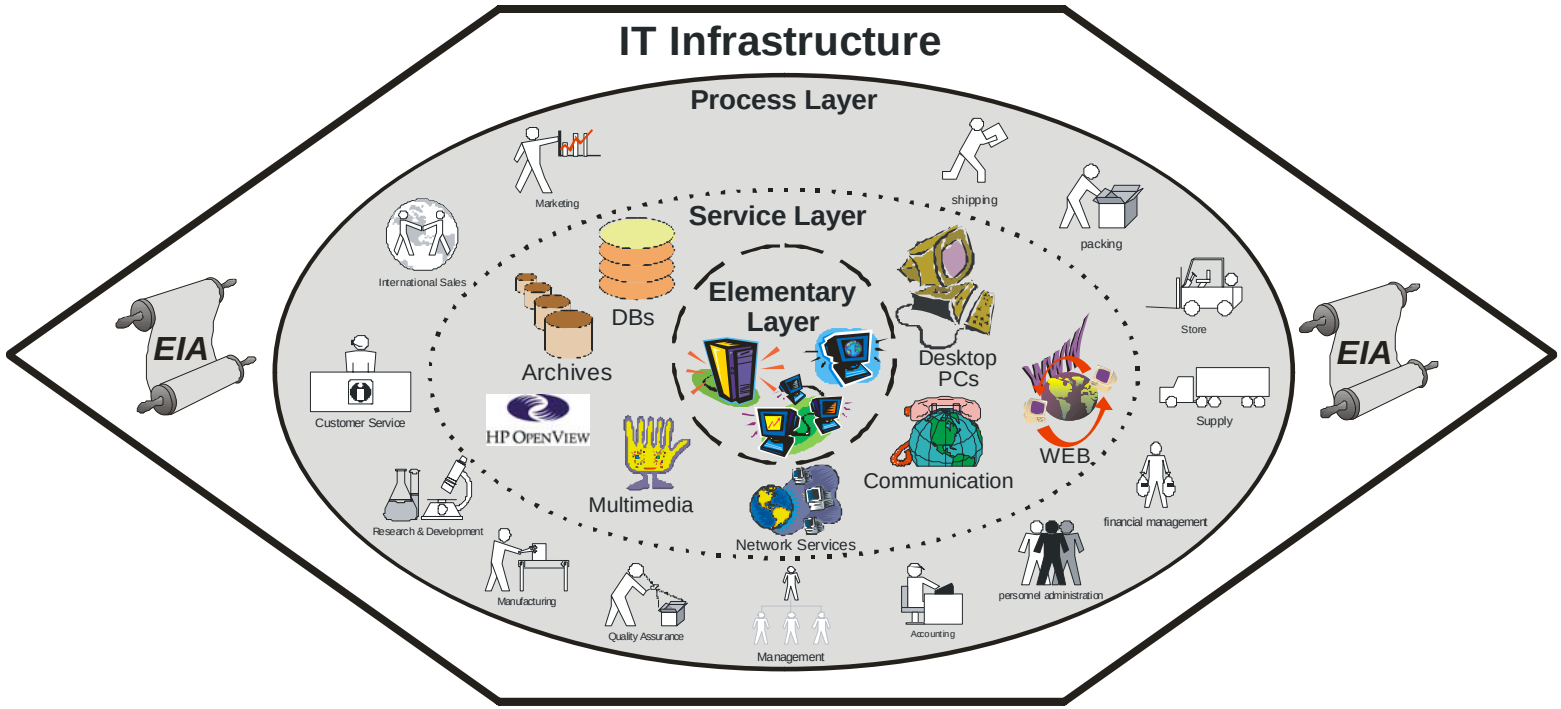
Wirkverbindliche Elemente sind Subjekte, die eine beschränkte, wohldefinierte und verifizierte Funktionalität verlässlich bereitstellen.
Sollte ihre funktionale Integrität nicht mehr gegeben sein, so stellen diese Elemente ihren Betrieb ein und zeigen ihre Kompromittierung für ihre Umgebung erkennbar an. Sie sind vorzugsweise als geschlossene, dedizierte Systeme technisch realisiert.

Wirkebenen

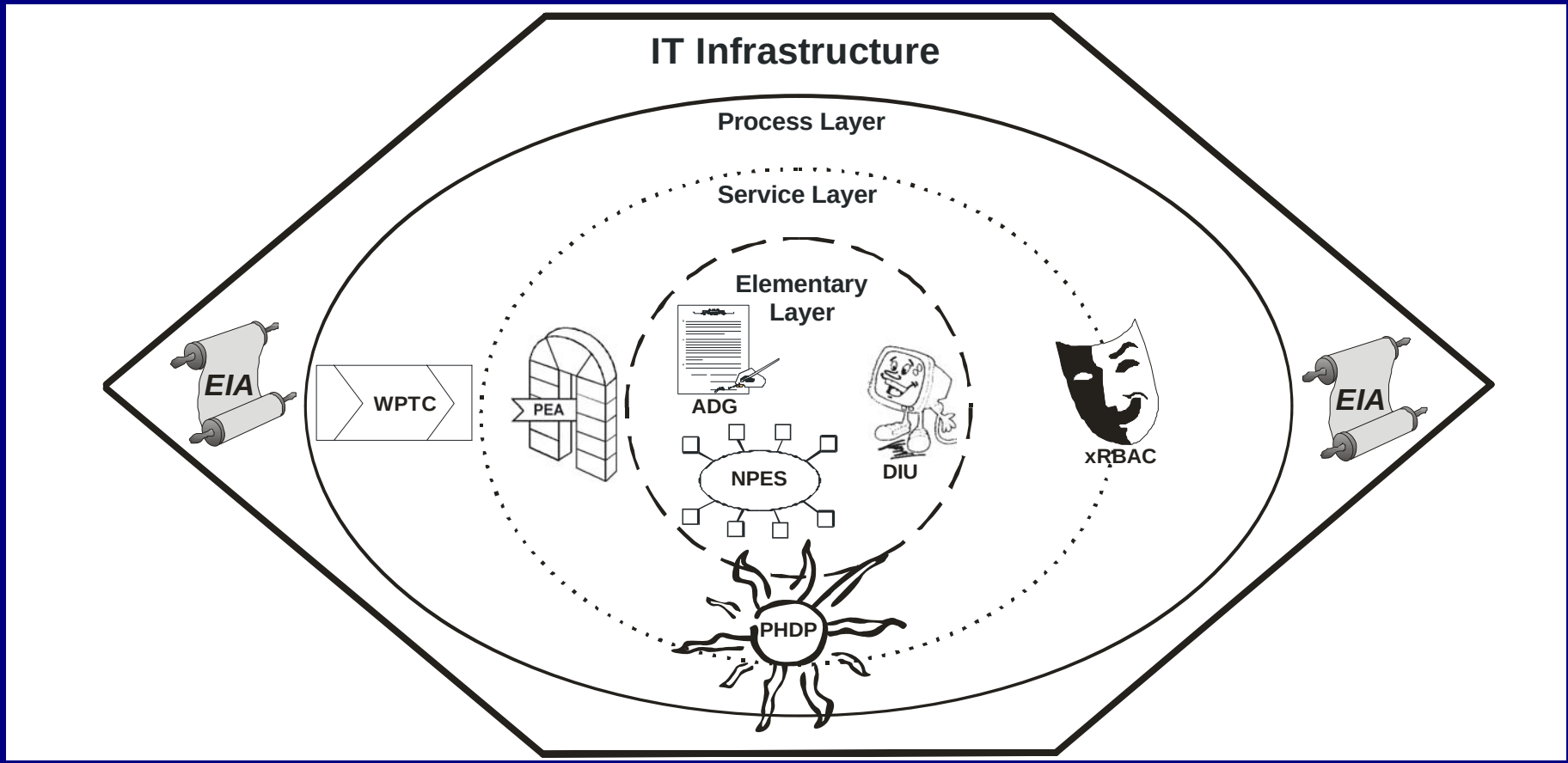
Process Layer
Process description with workflows and roles

Service Layer
Desription of Services: Dektop Pcs, DB, DNS, Mail, WEB, HP OV...

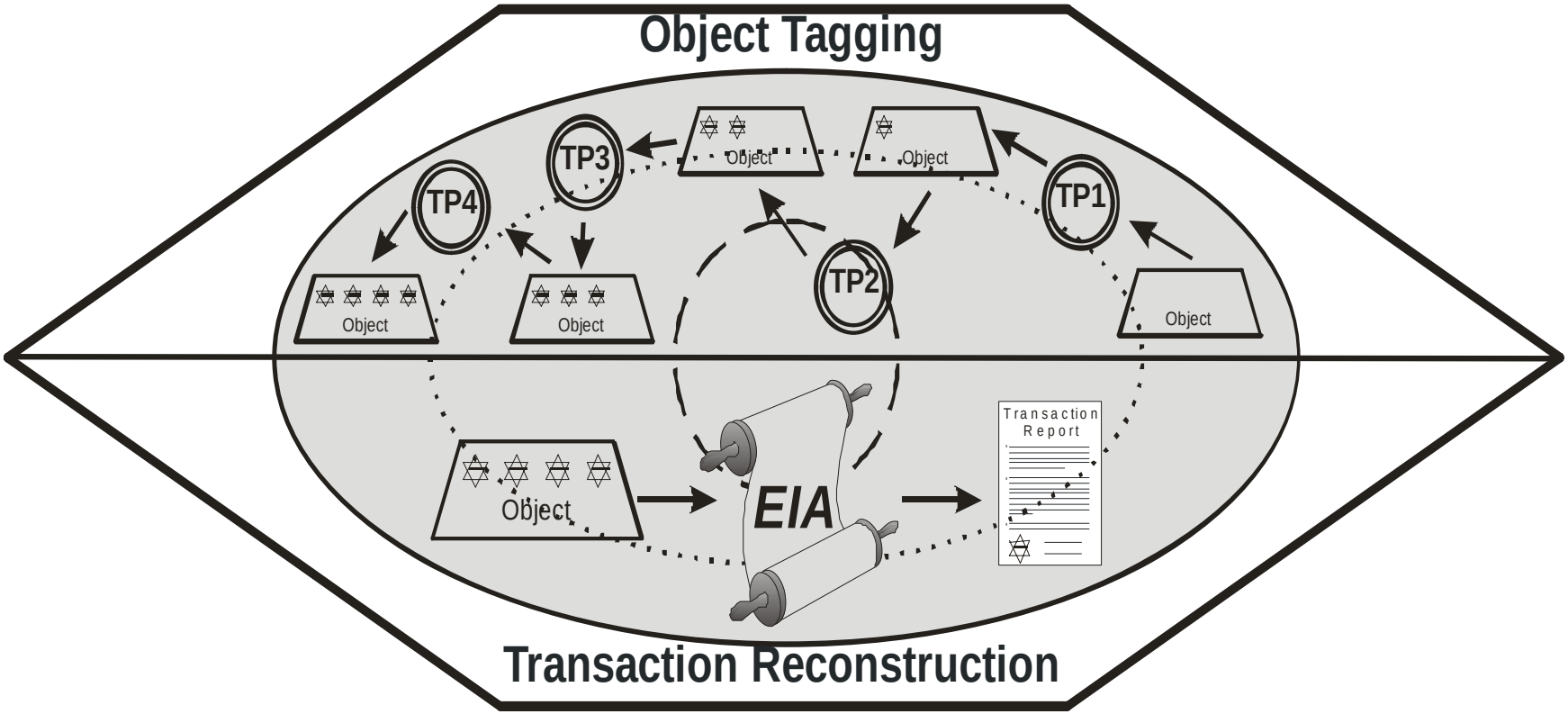
Elementary Layer
Description of Hardware Elements



Wirkverbindliche Elemente: Wirkebenen



Wirkverbindliche Elemente: Object Tagging



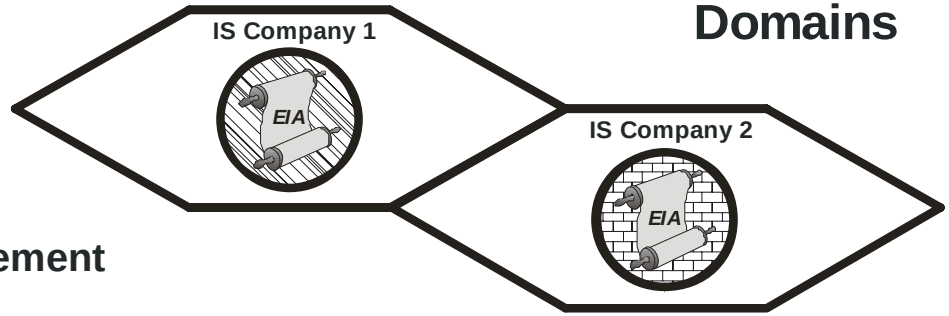
IT-Infrastrukturen Kopplung

Inter-Infrastructure Trust Establishment
- Exchange of Policy Rules and Explicit Restrictions
- Exchange of Certificates

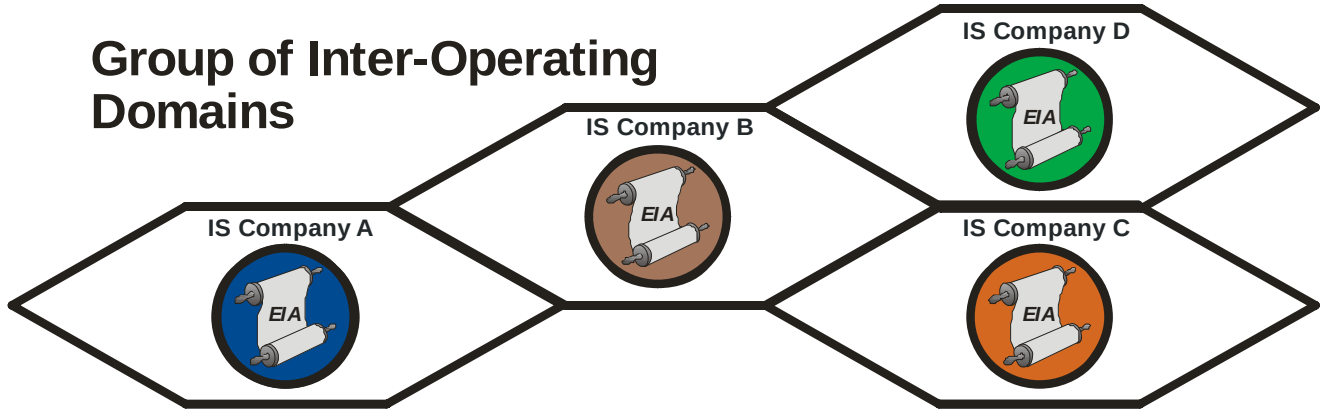
Policy Translation
- Exchange of Policy Rules & Explicit Restrictions
- Exchange of Certificates

External Certificate and Incident Management
- Certificate repository and control
- External Security Incident Message Handling

Couple of Inter-Operating Domains



Group of Inter-Operating Domains



Zusammenfassung (1/2)

- Voraussetzung zur Durchsetzung einer Sicherheitspolitik ist die Identifizierbarkeit von Elementen einer Infrastruktur
- Vorgänge mit hoher sicherheitstechnischer Relevanz dürfen ausschließlich auf wirkverbindlichen Elementen verarbeitet werden
- Für alle Abstraktionsebenen müssen ebenenspezifische Sicherungsverfahren zum Einsatz kommen

Zusammenfassung (2/2)

- Einheitliche Sicherheitsbezeichner und deren spezifische Bedeutungsfestsetzung für jede Abstraktionsebene, bilden die Voraussetzung für eine vertikale Durchsetzung einer Sicherheitspolitik
- Horizontale und vertikale Wirkverzahnung von Sicherungsverfahren bilden die Voraussetzung zur verbindlichen Nachvollziehbarkeit von Vorgängen innerhalb von IT-Infrastrukturen

Ausblick

- Verfahren zur Durchsetzung von Regelwerken außerhalb der technischen Ebene von IT-Systemen (Context Related Security)
- Methodik für die umfassende und konsistente Anwendung des Instrumentariums der IT-Sicherheit
- Methodik zum angemessen Einsatz von IT-Systemen die Wirkung auf den zivilisatorischen Kontext entfalten können (IT-Security Engineering)

Kontakt

Ansprechpartner: Thomas J. Wilke
tub@tjw.li
+49 (30) 74740929
www.Total-IT-Security.de