Informationssicherheit bei PostMail und PostLogistics

SGRP-Veranstaltung im BZ Härkingen vom 8. September 2016

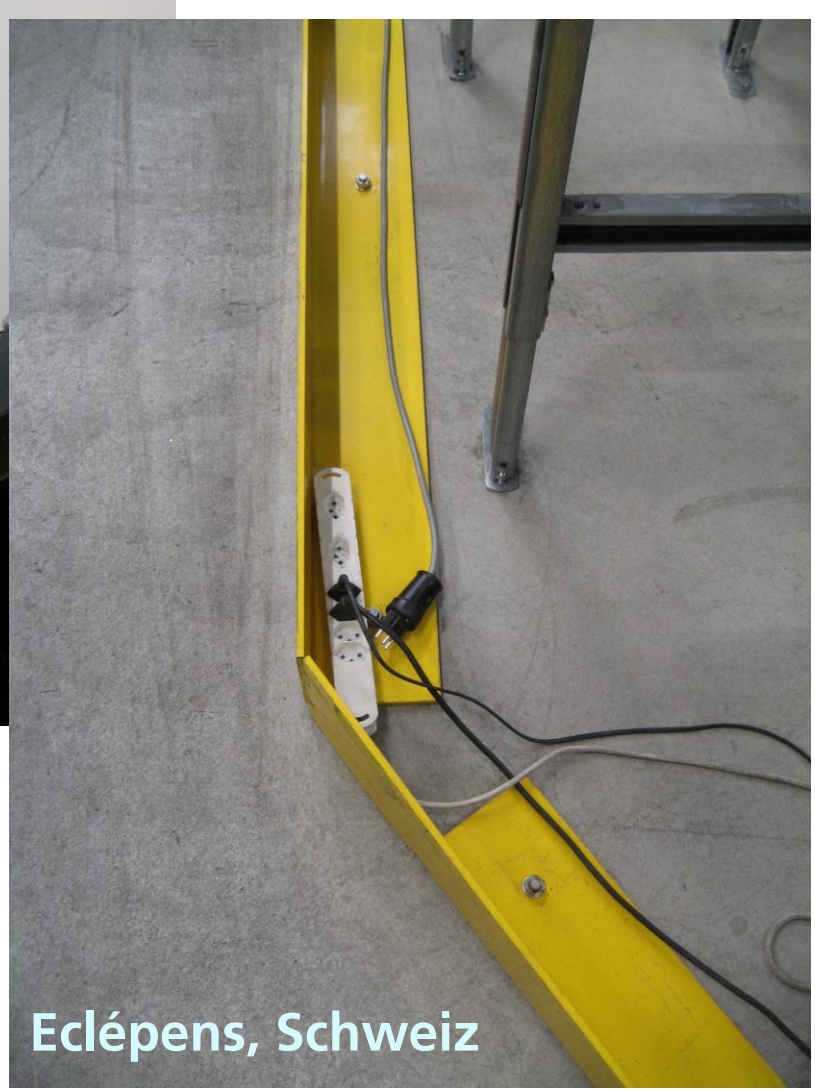
Markus Stopper CISO PL/PM / David Aeschlimann, IT-SIBE PL/PM

Gelb bewegt.

DIE POST

Vergleich der Kulturen - Installationstechnik

Vergleich der Kulturen - Wo gibt’s Strom?



Vergleich der Kulturen – Sicherheit….

Pokhara, Nepal

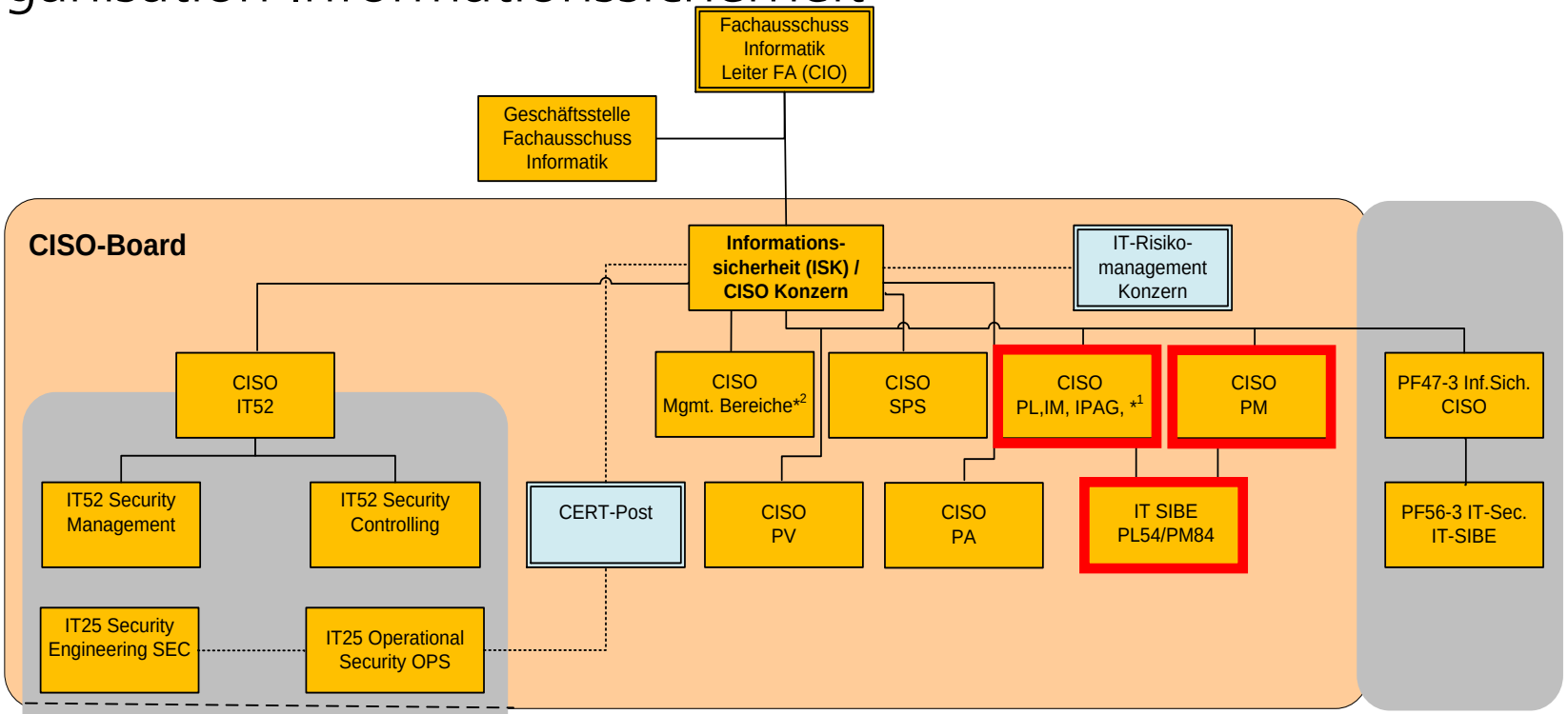
Härkingen, Schweiz

Ablauf Informationssicherheitsschulung

- Kurz in eigener Sache
- Grundpfeiler der Informationssicherheit und IT-Sicherheit
- Information Security Management System ISMS
- Informationssicherheit SCADA-Gewerke am Beispiel Zugriffsschutz
- Das IT-Portfolio und dessen Abdeckungsgrad
- Grundlagen, damit dies auch funktioniert
- Zusammenfassung - Position des CISO und IT-SIBE bei PostMail und PostLogistics
- Fragen

Kurz in eigener Sache

Organisation Informationssicherheit



*1 MoSAG und SecurePost
*2 Mgmt. Bereiche = F, P, K, IR

Kurz in eigener Sache 2/5

Aktuelle und zukünftige Tätigkeiten Informationssicherheit

CISO Bereich PM und PL

Markus Stopper
PL51_PM81
CISO PL
CISO IMS
Stv. CISO PM
Stv. DSB PM

Martin Sax
PM81_PL51
CISO PM
Stv. CISO PL
Stv. CISO IMS
Stv. DSB PL

- Vorhaben
  - Schutzbedarfsanalysen
  - Geschäftskritische Anwendungen
  - Securityaspekte in den SLAs
  - Identity and Accessmanagement

- Tägliche Arbeiten
  - Begleitung und Unterstützung von Projekten und Audits
  - Beurteilung von Ausnahmeanträgen (EWEM)
  - Schulungen und Sensibilisierung

Kurz in eigener Sache 3/5

Aktuelle und zukünftige Tätigkeiten Informationssicherheit

IT-SIBE Bereich PM und PL für Sortierinformatik

David Aeschlimann
PM84_PL54

- Vorhaben
  - Einhaltung der Sicherheitsvorgaben
  - Benutzerkonzepte / Benutzerverwaltung
  - Enge Zusammenarbeit mit den CISOs

- Tägliche Arbeiten
  - Ansprechpartner für IT Sicherheit
  - Zutrittsverwaltung Server- und Technikräume
  - Prüfung der IT-Sicherheitsaspekte bei Projekten und Aufträgen

Kurz in eigener Sache

Kurz in (fast) eigener Sache - Organisation Datenschutz

DSB Konzern

DSB F & K & PA | DSB IM | DSB IT | DSB E | DSB MoS AG

DSB SecurePost | DSB P | DSB P US (Video) | DSB SPS

DSB PV | DSB PL | DSB PM

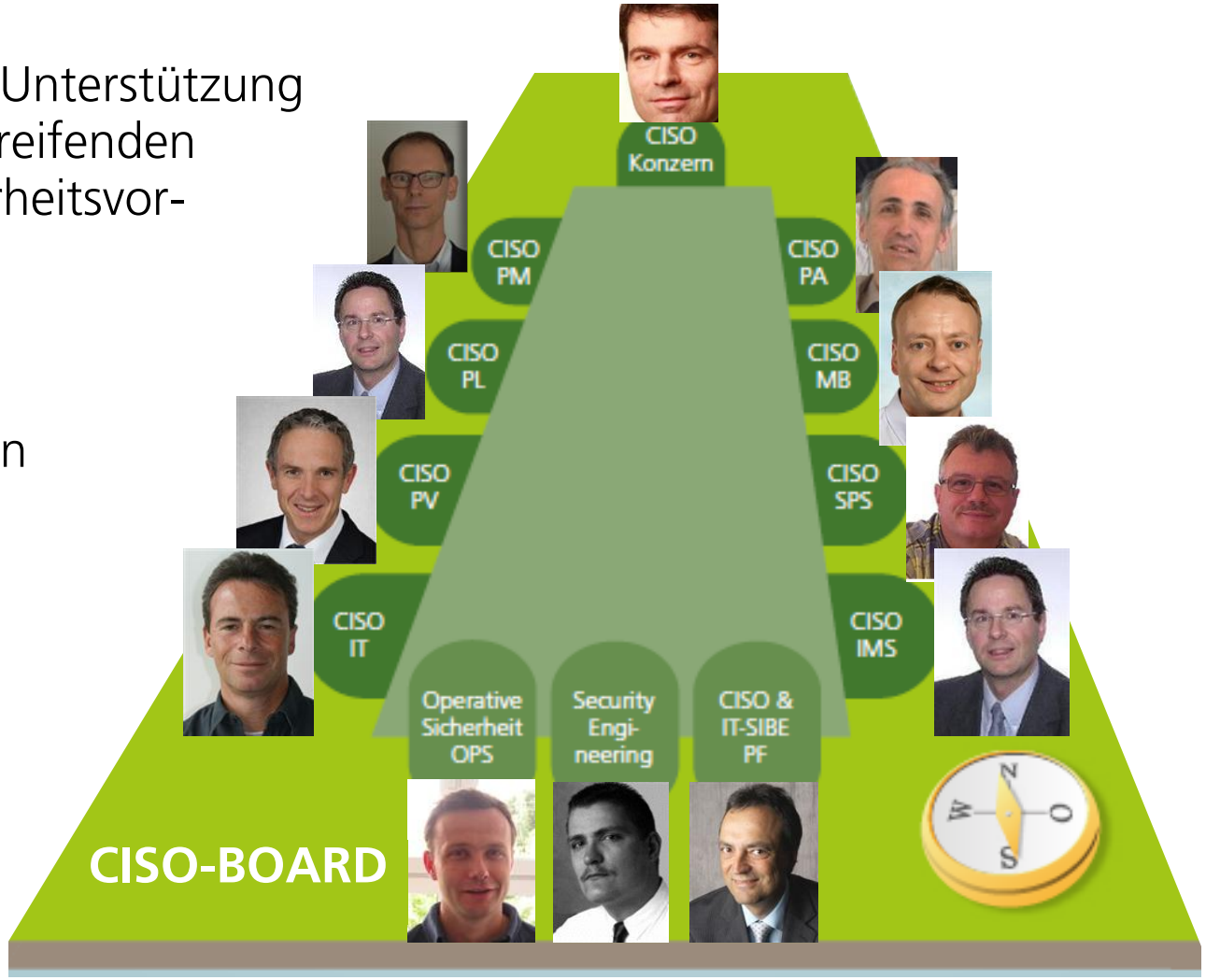
Monika Hollenstein
PL83-1
DSB PL

Patrick Sprecher
PM7
DSB PM

Kurz in eigener Sache

CISOs des Konzern Post - Wer sind wir?

- Koordination und Unterstützung der bereichsübergreifenden Informationssicherheitsvor-haben
- Abstimmung und Wissensaustausch zwischen Bereichen
- Erarbeiten von Empfehlungen z. H. FA ICT



Grundpfeiler der Informationssicherheit und IT-Sicherheit

EINWANDFREI FUNKTIONIERENDE INFRASTRUKTUR, NAMENTLCH HLKSE (HEIZUNG, LÜFTUNG, KLIMA, SANITÄR UND ELEKTRO) UND DIE SORTIERGEWERKE

Information Security Management System ISMS 1/4

Vorgaben der Informationssicherheit 2/4

Vorgaben der Informationssicherheit 3/4

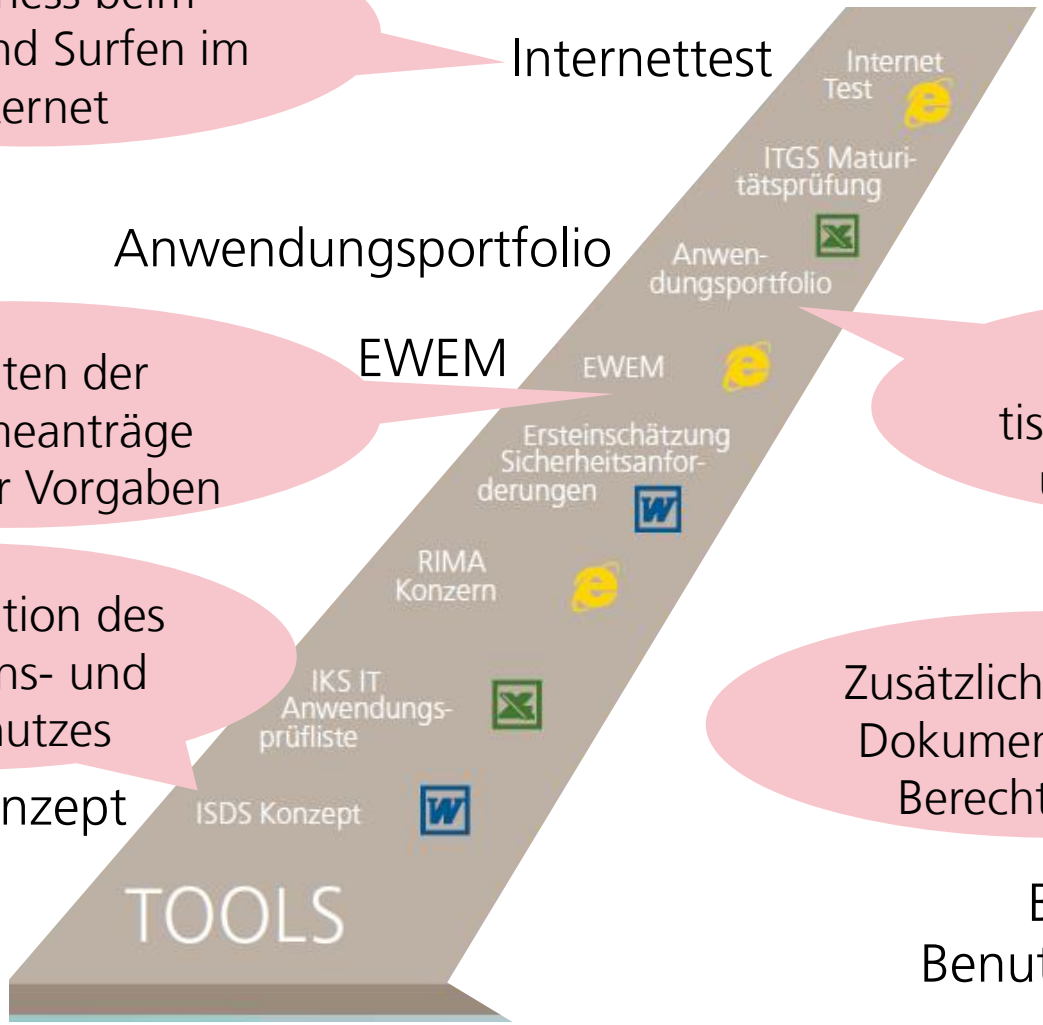
Regelt den Schutz der Personen-daten (Einhaltung DSG) sowie wertvollen und schützens-werten Informationen

Grundsätze wie die Informatik geführt und organisiert ist. Entscheidungsbefugnisse und Verantwortlichkeiten

Definiert die **Schutzziele** Verfüg-barkeit, Integrität, Vertraulichkeit, und Nachvollziehbarkeit sowie die **Grundsätze** Risikoorientierung, IT-Grundschutz, Eigenverant-wortlichkeit und Eignerschaft

Vorgaben der Informationssicherheit 4/4

Werkzeuge zur Umsetzung der Informationssicherheit



Awareness beim Mailen und Surfen im Internet

Internettest

Anwendungsportfolio

Verwalten der Ausnahmeanträge gegenüber Vorgaben

EWEM

Liste geschäftskritischer Anwendungen und ISA KEP&Mail

Dokumentation des Informations- und Datenschutzes

ISDS Konzept

Zusätzlich bei PM/PL: Dokumentation der Berechtigungen

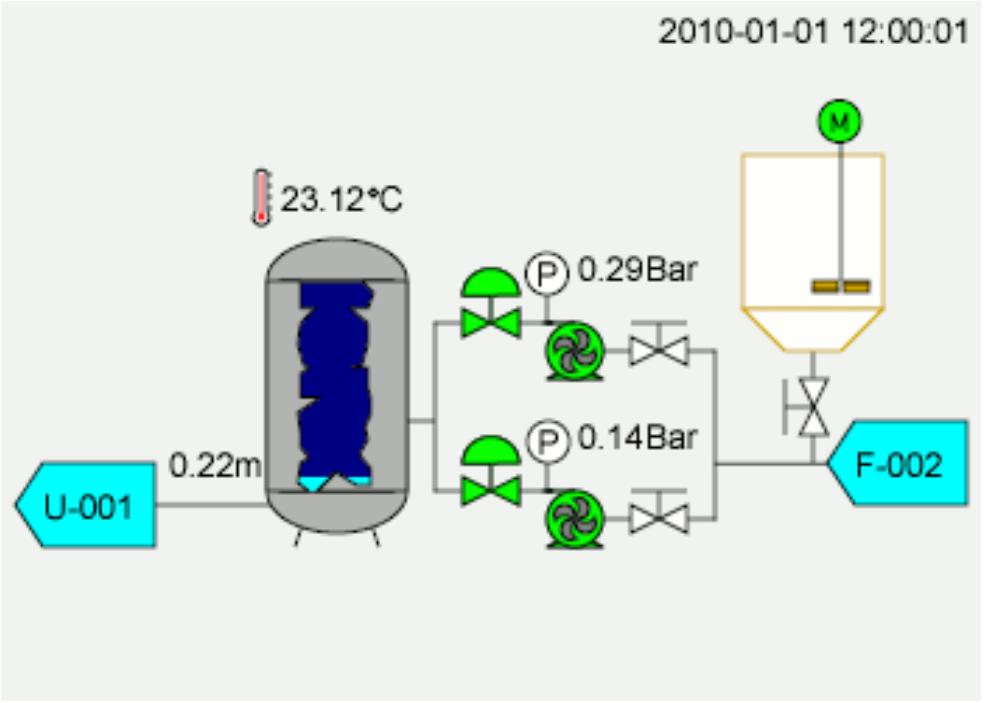
Berechtigungs- und Benutzerdokumentation

Informationssicherheit SCADA-Gewerke am Beispiel Zugriffsschutz 1/7

Und wie Informationssicherheit am Beispiel von SCADA-Gewerken gehandhabt wird, zeigt Ihnen nun der IT-SIBE.

Per Definition:

Unter **Supervisory Control and Data Acquisition** (**SCADA**) versteht man das Überwachen und Steuern technischer Prozesse mittels eines Computer-Systems.



Informationssicherheit SCADA-Gewerke am Beispiel Zugriffsschutz 2/7

Wie der Zugriffsschutz in der Praxis aussieht, werde ich anhand des RDP-Zugriffs auf einen Beispielserver aufzeigen.

Situation:

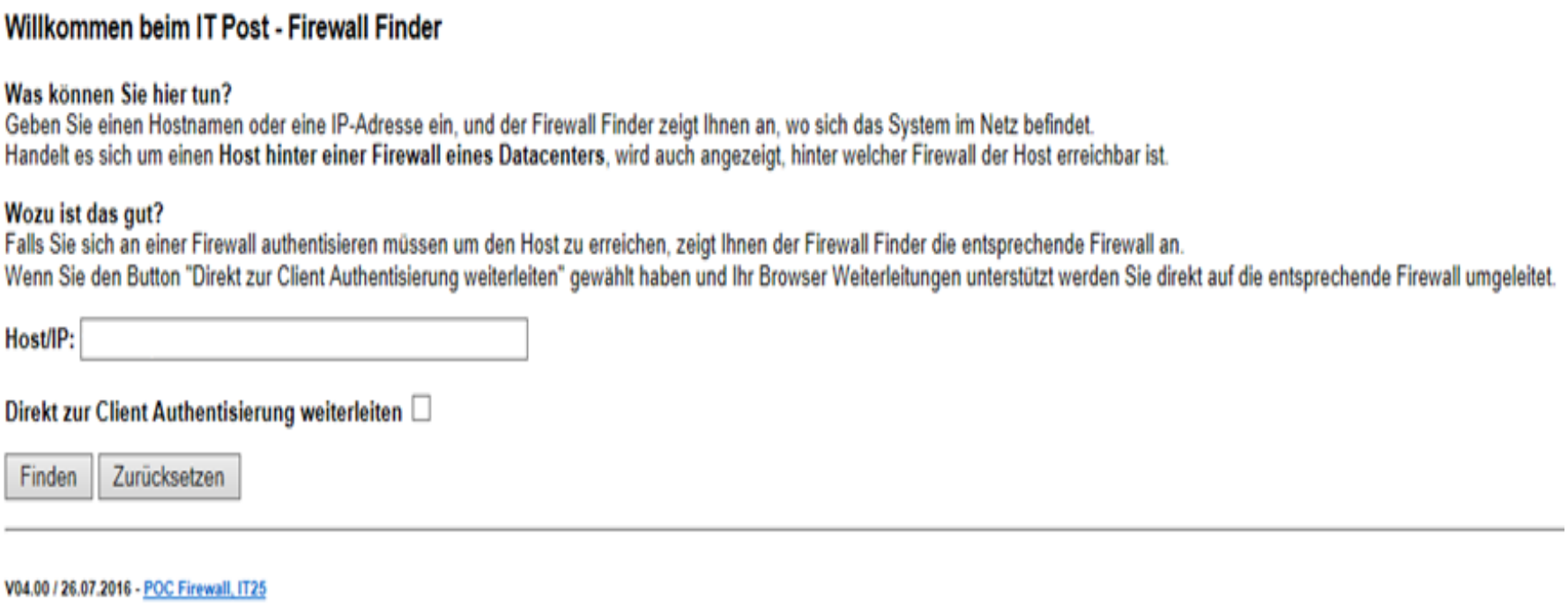
- Der User arbeitet regulär an seinem Arbeitsplatz und muss zu Supportzwecken auf einen Server eines SCADA-Systems zugreifen.

Bedingungen:

- Der User ist in einer der Administratorengruppen (Serverbetrieb oder Applikationsbetrieb)
- Der User verfügt über die Berechtigung, sich an der entsprechenden Domäne anzumelden
- Der User ist im Besitz einer SecureID mit gültiger Synchronität

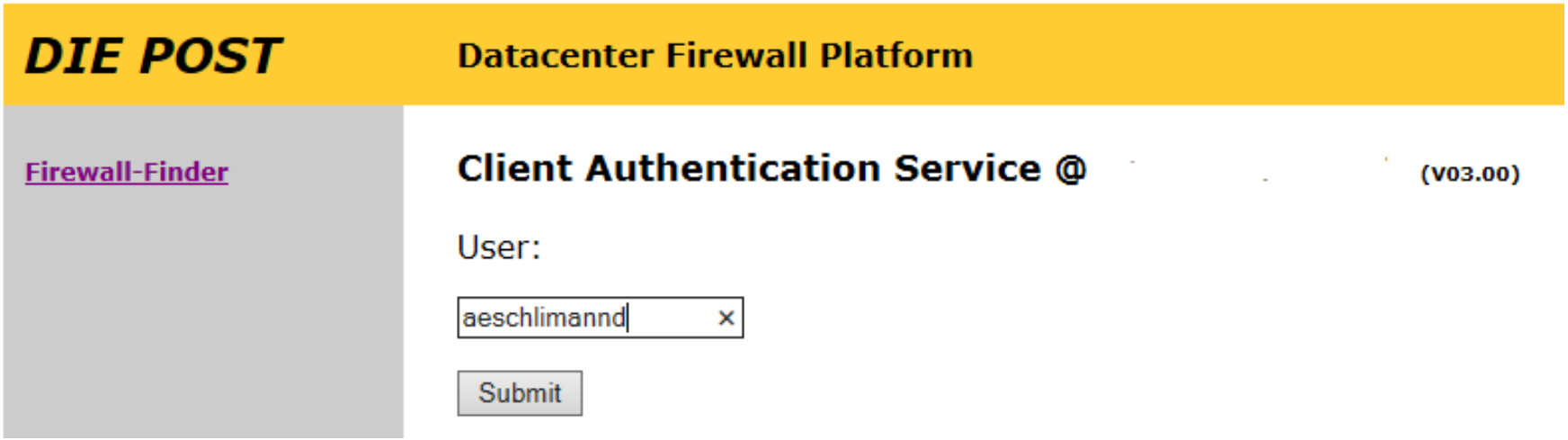
Informationssicherheit SCADA-Gewerke am Beispiel Zugriffsschutz 3/7

Schritt 1: Finden der Firewall des jeweiligen Datacenters



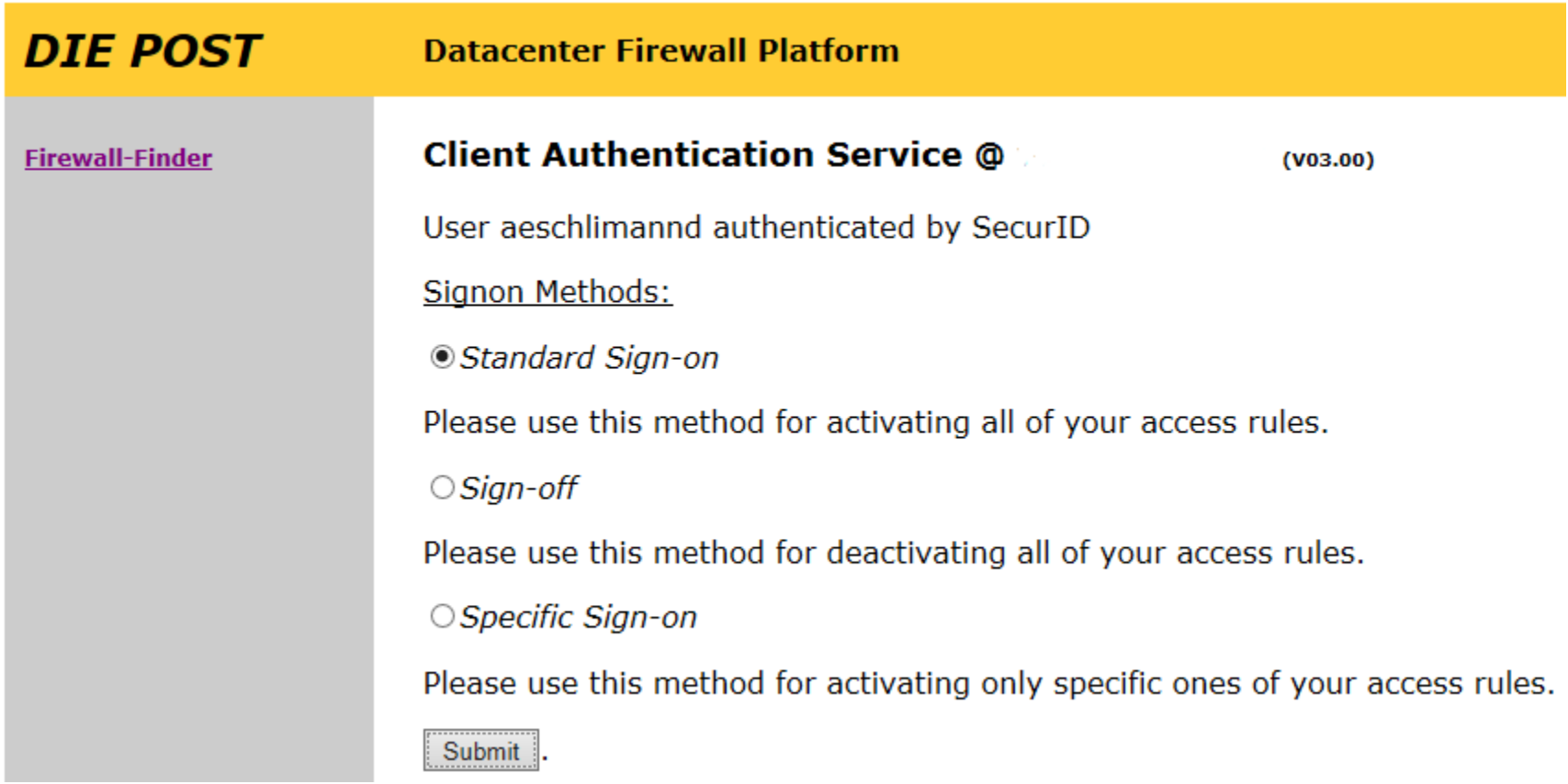
Informationssicherheit SCADA-Gewerke am Beispiel Zugriffsschutz 4/7

Schritt 2: Authentifizieren mittels AD Account, PIN und PRN



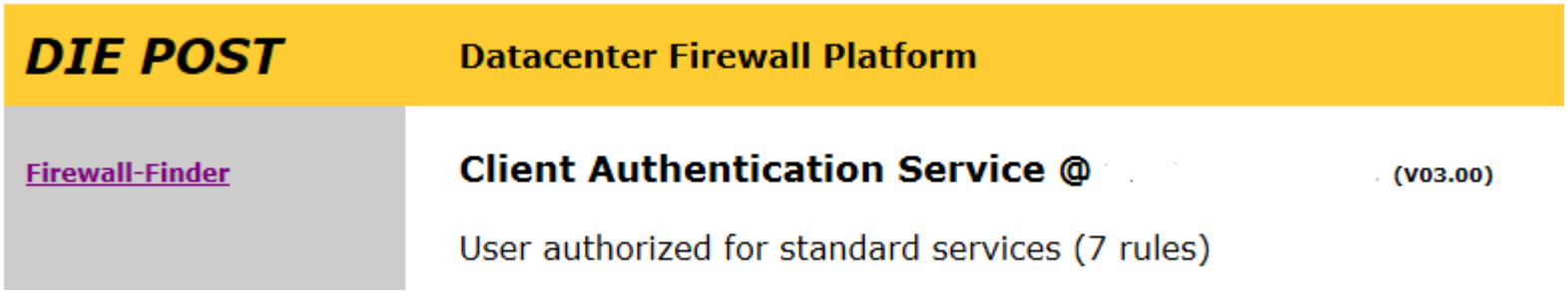
Informationssicherheit SCADA-Gewerke am Beispiel Zugriffsschutz 5/7

Schritt 3: Temporäre Freischaltung von persönlichen Firewallrules
Die Freischaltungs-Seite ist maximal eine Minute gültig.

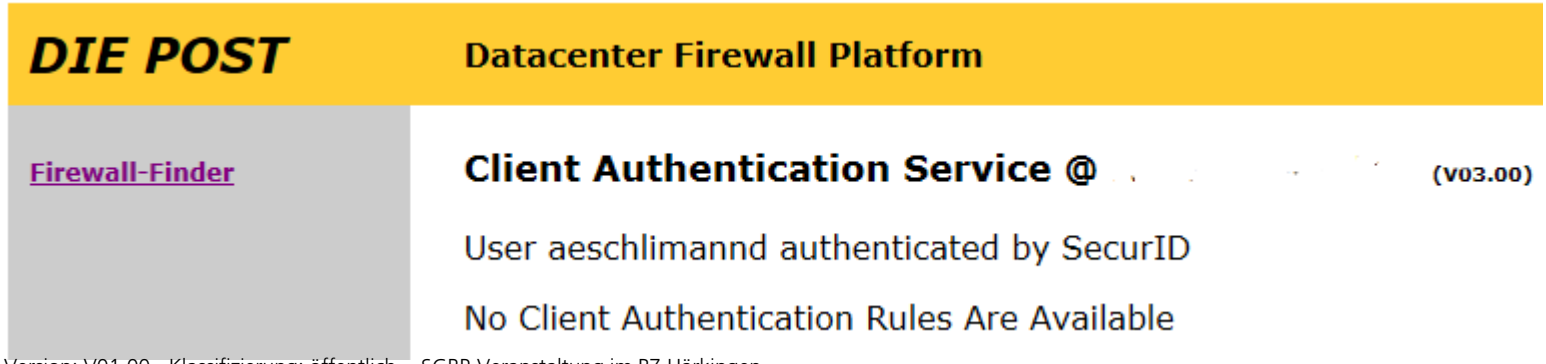


Informationssicherheit SCADA-Gewerke am Beispiel Zugriffsschutz 6/7

Schritt 4: Rules werden freigeschaltet.
Die Freischaltung ist zeitlich auf einige Stunden begrenzt.



Entsprechende Rules werden nur freigeschaltet, wenn der User einen begründeten Antrag gestellt hat und diese freigeschaltet wurden. Andernfalls ist zwar die Authentifizierung erfolgreich, aber es werden keine Rules geschaltet.



Informationssicherheit SCADA-Gewerke am Beispiel Zugriffsschutz 7/7

Schritt 5: Fertig! Der User kann nun während der nächsten Stunden über RDP auf den Server zugreifen.

Fazit:

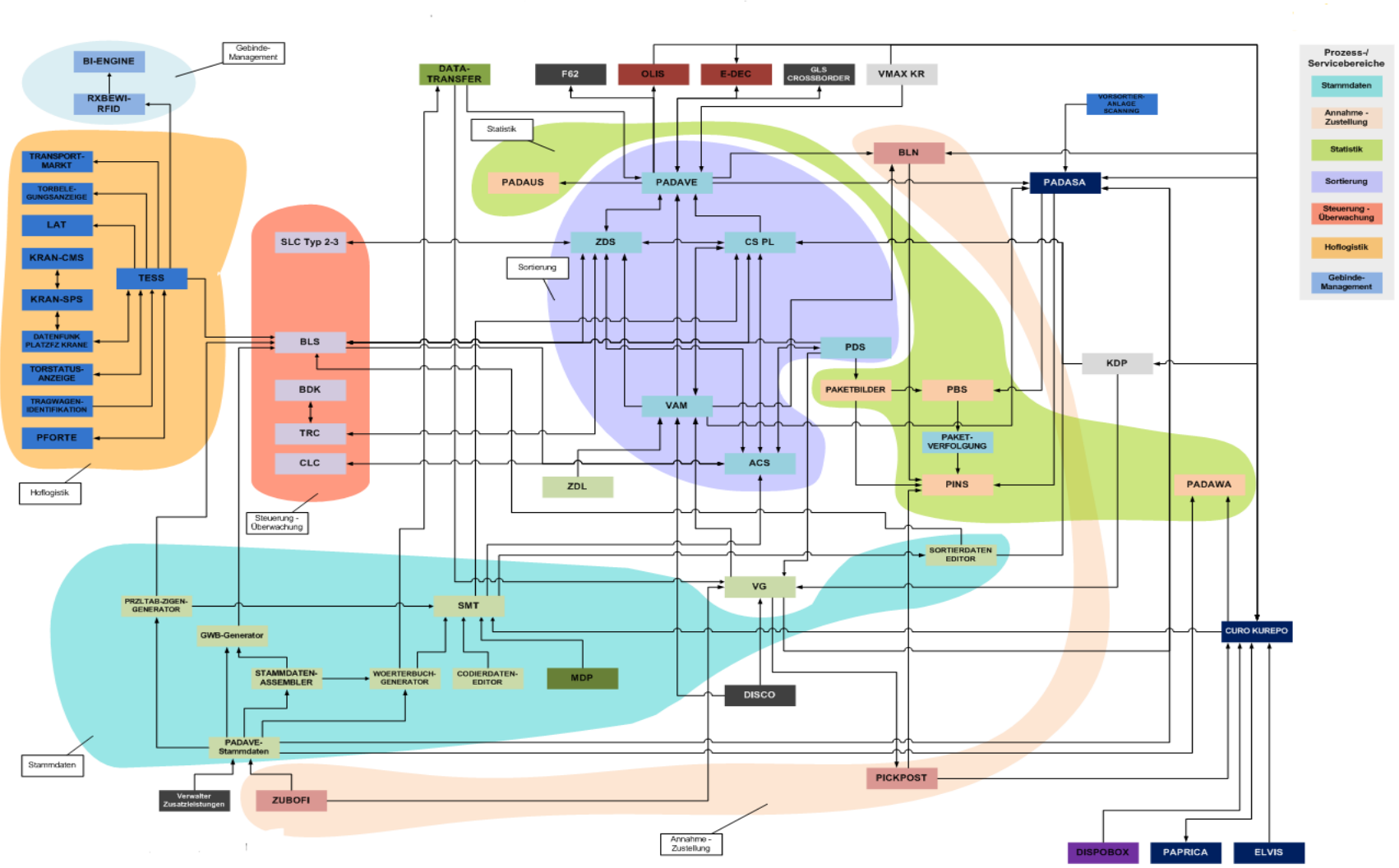
- Das Verfahren ist anders als bei regulären Applikations- und Datenbankservern, denn bei diesen entfällt die Freischaltung der temporären Firewall Rules
- Restriktive Handhabung
- Jederzeit eine Nachvollziehbarkeit sichergestellt

Das IT-Portfolio und dessen Abdeckungsgrad 1/4

- Das IT-Portfolio umfasst mittlerweile 581 Anwendungen, welche dokumentiert sind
- Die Abbildung erfolgt nach dem Prinzip «vom Groben ins Detail» in einer eigenen Informations System Architektur
- Es wird bis Stufe Applikation abgebildet und deren direkten Umsysteme
- Die zugrunde liegende Technologie wird berücksichtigt
- Die Informationen der Vertraulichkeit, Verfügbarkeit, Nachvollziehbarkeit und Integrität sind hinterlegt
- Die zuständigen Verantwortlichen (Fachbereich, Applikationsverant-wortlicher, Betreiber, Lieferant…) sind dokumentiert

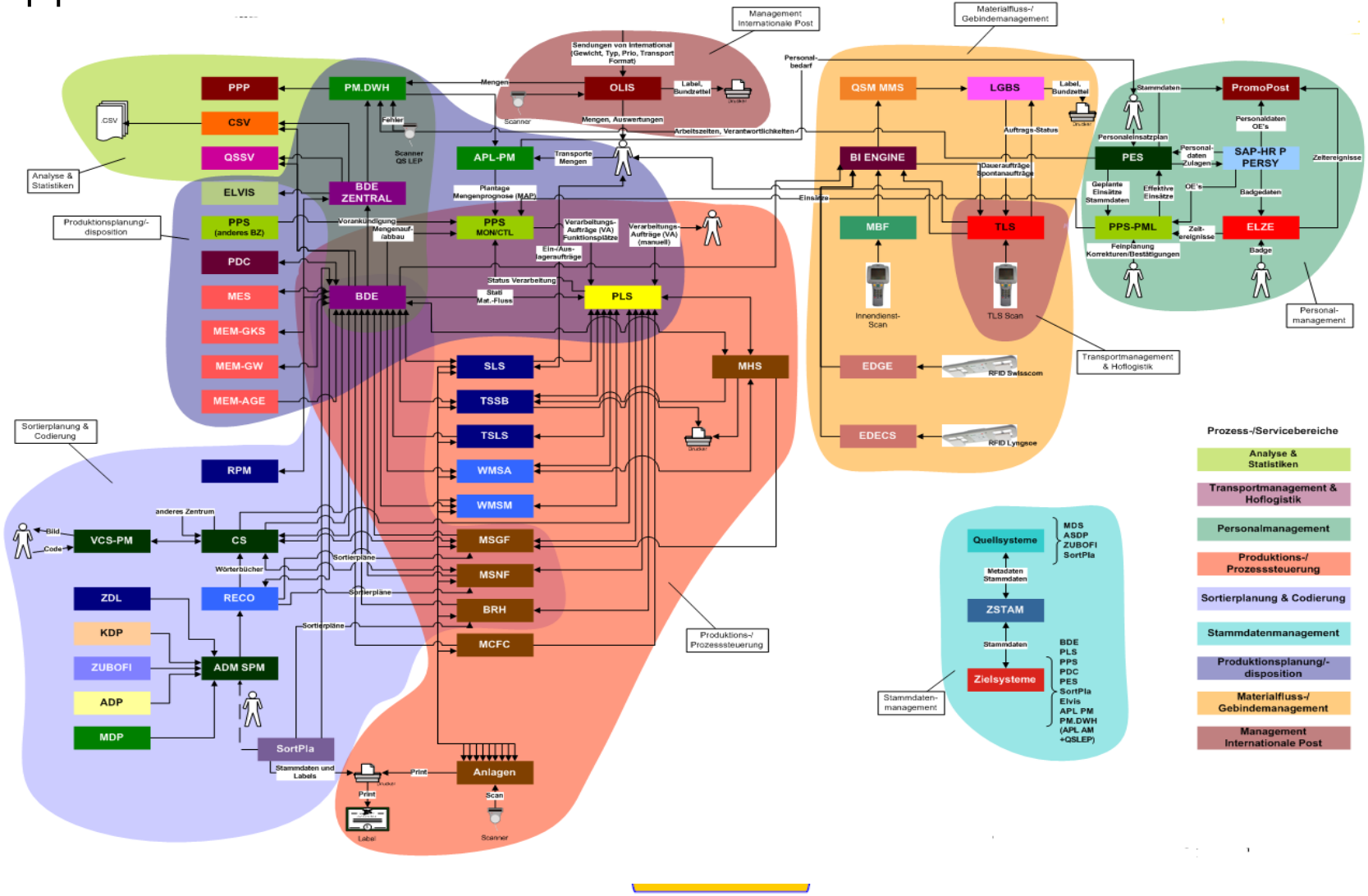
Das IT-Portfolio und dessen Abdeckungsgrad 2/4

Applikationslandschaft PostLogistics



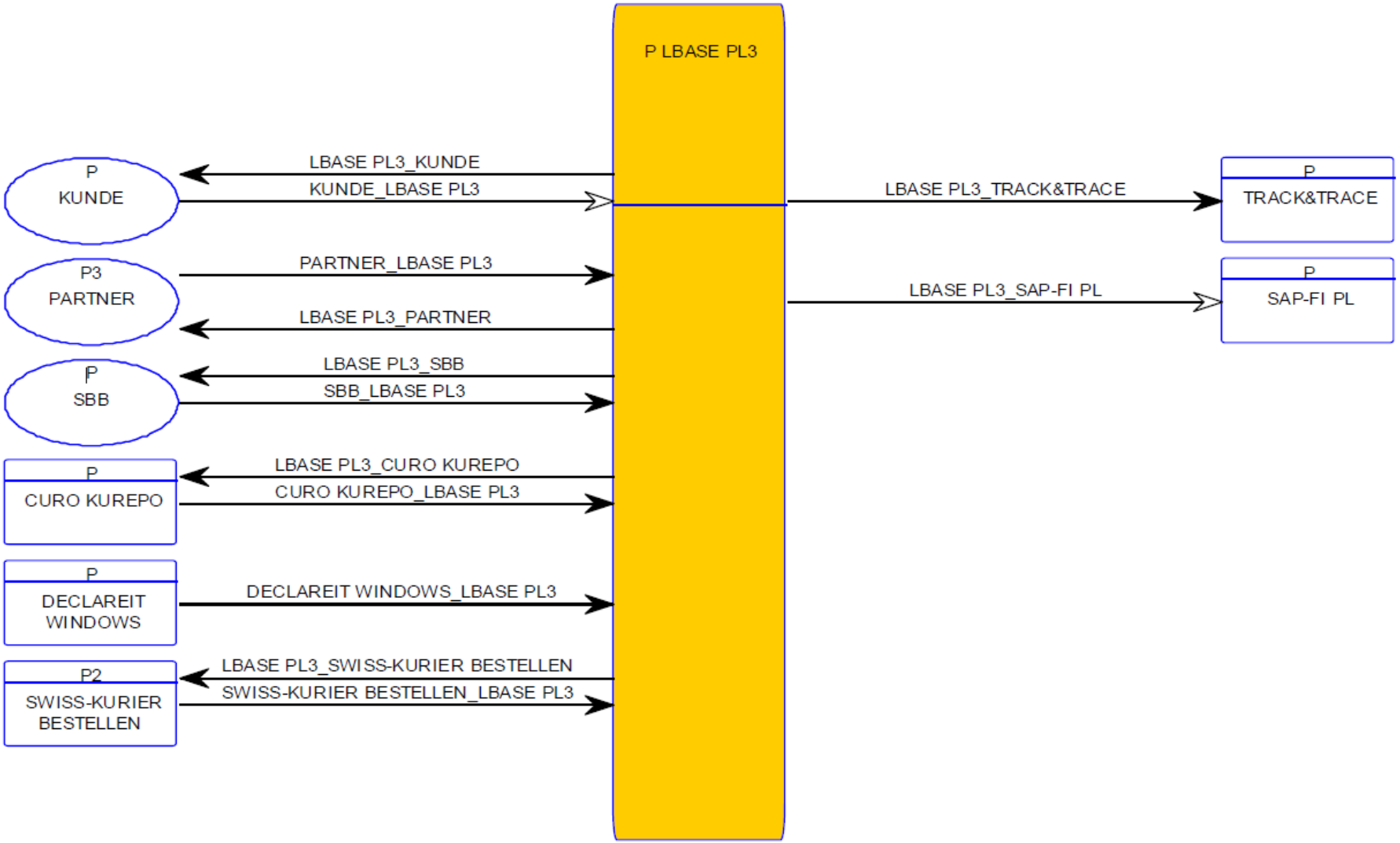
Das IT-Portfolio und dessen Abdeckungsgrad ¾

Applikationslandschaft PostMail



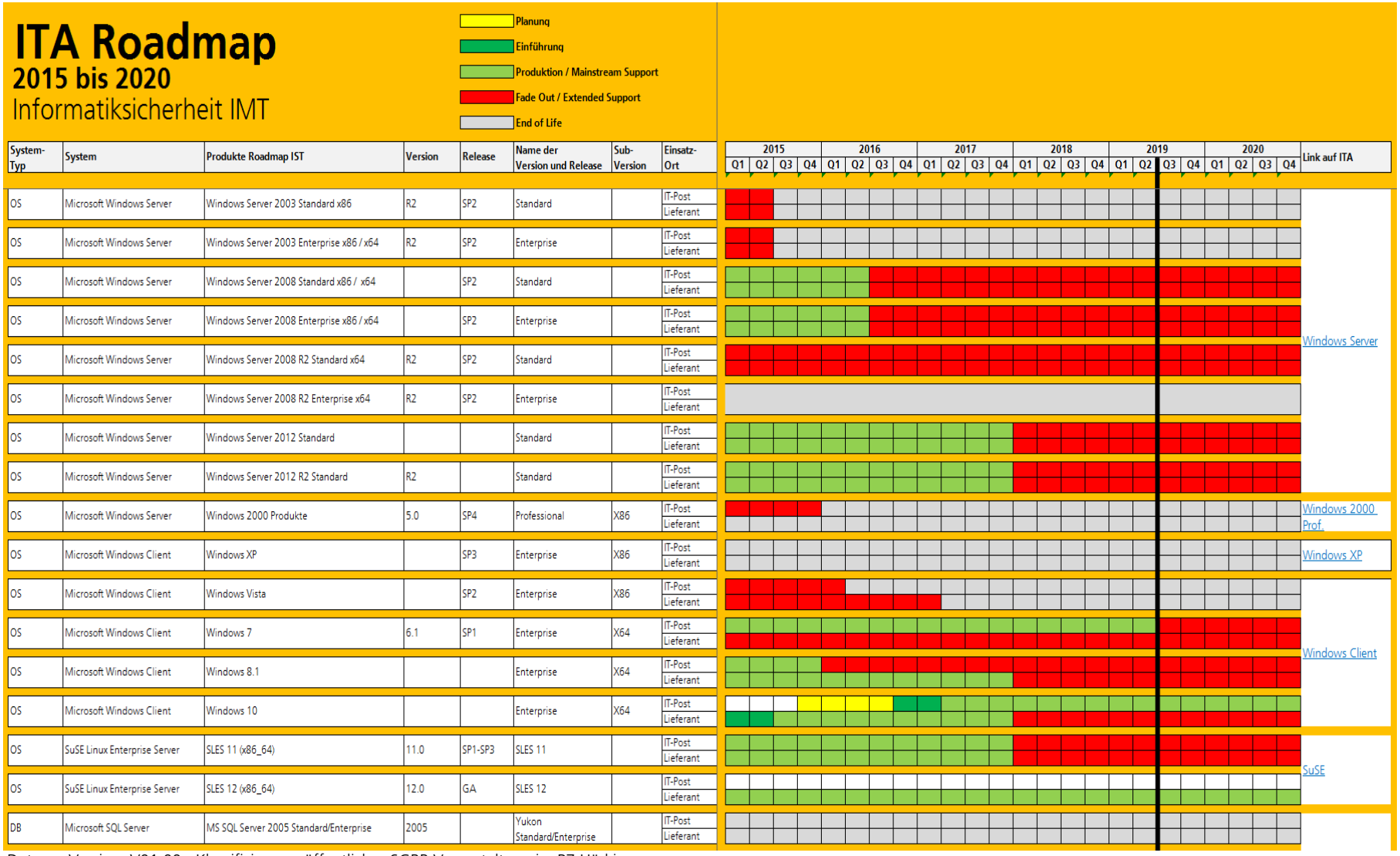
Das IT-Portfolio und dessen Abdeckungsgrad ¾

Einzelapplikation mit den Beziehungen zu den Umsystemen



Das IT-Portfolio und dessen Abdeckungsgrad 4/4

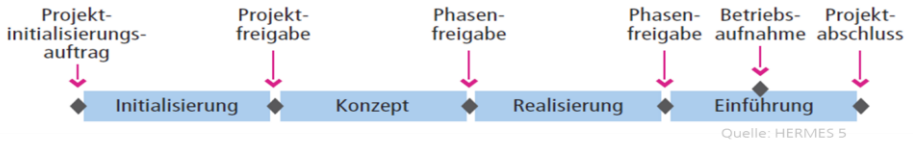
Informations Technologie Architektur - Roadmap



System-Typ	System	Produkte Roadmap IST	Version	Release	Name der Version und Release	Sub-Version	Einsatz-Ort	Link auf ITA
OS	Microsoft Windows Server	Windows Server 2003 Standard x86	R2	SP2	Standard		IT-Post Lieferant	
OS	Microsoft Windows Server	Windows Server 2003 Enterprise x86 / x64	R2	SP2	Enterprise		IT-Post Lieferant	
OS	Microsoft Windows Server	Windows Server 2008 Standard x86 / x64		SP2	Standard		IT-Post Lieferant	
OS	Microsoft Windows Server	Windows Server 2008 Enterprise x86 / x64		SP2	Enterprise		IT-Post Lieferant	
OS	Microsoft Windows Server	Windows Server 2008 R2 Standard x64	R2	SP2	Standard		IT-Post Lieferant	Windows Server
OS	Microsoft Windows Server	Windows Server 2008 R2 Enterprise x64	R2	SP2	Enterprise		IT-Post Lieferant	
OS	Microsoft Windows Server	Windows Server 2012 Standard			Standard		IT-Post Lieferant	
OS	Microsoft Windows Server	Windows Server 2012 R2 Standard	R2		Standard		IT-Post Lieferant	
OS	Microsoft Windows Server	Windows 2000 Produkte	5.0	SP4	Professional	X86	IT-Post Lieferant	Windows 2000 Prof.
OS	Microsoft Windows Client	Windows XP		SP3	Enterprise	X86	IT-Post Lieferant	Windows XP
OS	Microsoft Windows Client	Windows Vista		SP2	Enterprise	X86	IT-Post Lieferant	
OS	Microsoft Windows Client	Windows 7	6.1	SP1	Enterprise	X64	IT-Post Lieferant	
OS	Microsoft Windows Client	Windows 8.1			Enterprise	X64	IT-Post Lieferant	Windows Client
OS	Microsoft Windows Client	Windows 10			Enterprise	X64	IT-Post Lieferant	
OS	SuSE Linux Enterprise Server	SLES 11 (x86_64)	11.0	SP1-SP3	SLES 11		IT-Post Lieferant	
OS	SuSE Linux Enterprise Server	SLES 12 (x86_64)	12.0	GA	SLES 12		IT-Post Lieferant	SuSE
DB	Microsoft SQL Server	MS SQL Server 2005 Standard/Enterprise	2005		Yukon Standard/Enterprise		IT-Post Lieferant	

Grundlagen, damit dies auch funktioniert

- Konsequentes Durchsetzen einer einheitlichen Methode



Schutzbedarf abklären

ISDS-Konzept

Berechtigungs- und Benutzer-dokumentation

Datenschutzblatt

Architektur-review

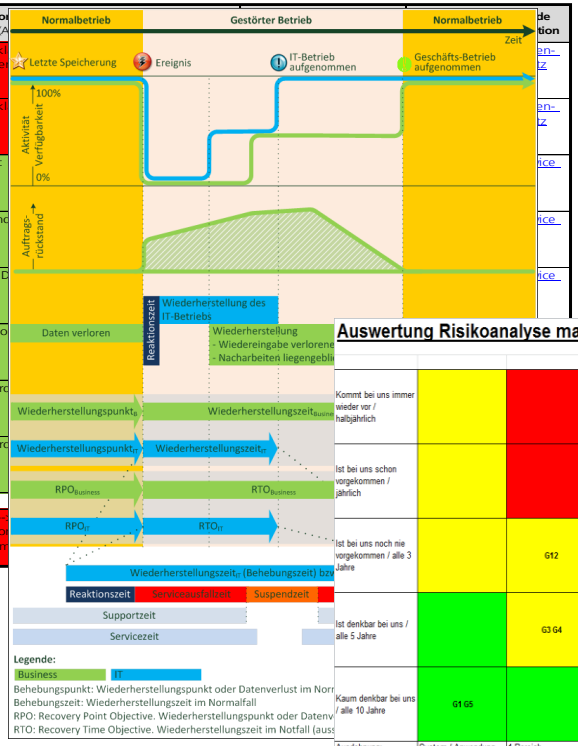
SLA

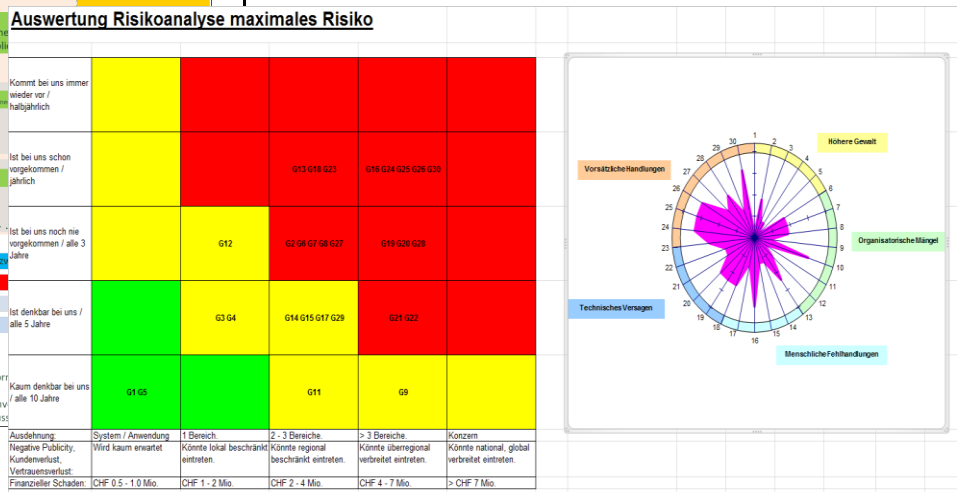
Abnahme

WebPenTest

- Klare Lieferergebnisse definieren

Kriterien	Fragen	Anfo
Vertraulichkeit	Welche Art von Personendaten werden bearbeitet (nach Weisung Daten- und Informationsschutz der Schweizerischen Post)?	Schutzkl Personer
	Wie sind die Informationen einzustufen (nach Weisung Daten- und Informationsschutz der Schweizerischen Post)?	Schutzkl
Verfügbarkeit	In welchem Zeitraum muss die Dienstleistung mindestens verfügbar sein? (Betriebszeiten)	Level 1:
	Max. zulässige Ausfalldauer? Bzw. wie lange darf die maximale Wiederherstellungsdauer sein?	32 Stund
	Max. zulässige Datenverlustzeit? Bzw. auf welchen Stand vor dem Ereignis müssen die Daten wiederhergestellt werden können? (Z. B. letztes Backup)	Klasse D
	Bedarf nach Katastrophenvorsorge (Business Continuity Management)?	Katastro
Integrität	Muss die Echtheit, Korrektheit und/oder Unversehrtheit der Daten nachgewiesen werden können?	Standard
Nachvollziehbarkeit	Müssen bestimmte Arbeitsvorgänge nachgewiesen werden können?	Standard
Schutzbedarf	Gesamtbeurteilung (Wird automatisch ausgefüllt)	Hoch ISDS-Kor und dem





- Rechtzeitiger Miteinbezug des CISO

Zusammenfassung - Position des CISO und IT-SIBE bei PostMail und PostLogistics

- Der CISO und IT-SIBE sind bei Projektbeginn bereits dabei
- Dieser Paradigma-Wechsel dauerte über 8 Jahre
- Der CISO und IT-SIBE sind der Coach des Fachbereichs
- «Geht nicht, gibt's nicht!» → CISO und IT-SIBE sind «Enabler

Vielen Dank für die Aufmerksameit


DIE POST
Gelb bewegt.