BISG bevh TeleTrusT
Pioneers in IT security.

Informationstag "Umsetzung des IT-Sicherheitsgesetzes in der Unternehmenspraxis"

Gemeinsame Veranstaltung von TeleTrusT, bevh und BISG

Berlin, 29.11.2016

IT-Sicherheitsgesetz, was nun?

Was bedeutet das für Betreiber Kritischer Infereastrukturen?

Michael Böttcher, Berliner Wasserbetriebe

Agenda

1. Vorstellung des Umfeldes
2. unser Umgang mit dem Stand der Technik und den Branchenstandards
3. Umsetzung der Meldepflicht
4. Vorbereitung auf die Zertifizierung

1. Vorstellung des Umfeldes

Die Berliner Wasserbetriebe in Zahlen

Trinkwasser-versorgung

199 Mio. m³ Wasserverkauf

7.900 km Rohrnetz

9 Wasserwerke

700 Brunnen

Abwasser-entsorgung

242 Mio. m³ Reinigungsleistung:
9.700 km Kanalnetz

1.200 km Druckleitungen

6 Klärwerke

158 Pumpwerke

Wirtschaftliche Kennziffern

1,1 Mrd. € Umsatz
321 Mio. € Jahresüberschuss

254 Mio. € Investitionen

352 Mio. € Beschaffungsvolumen, davon 80 % an regionale Firmen

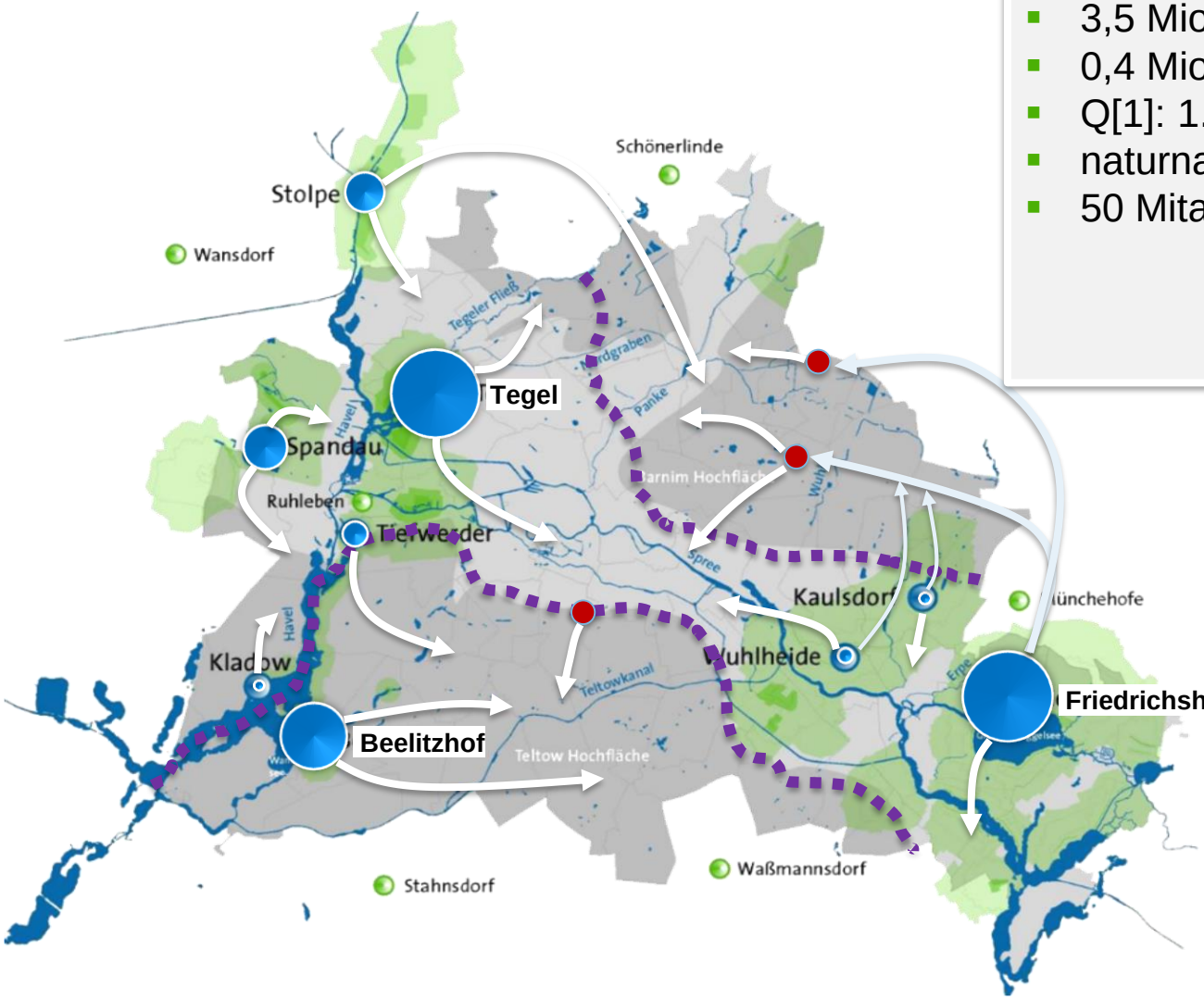
4.430 Beschäftigte

Zahlen des Geschäftsjahres 2015

1. Vorstellung des Umfeldes

Trinkwasserversorgung in Berlin

- 3,5 Mio. Einwohner Berlins
- 0,4 Mio. Bürger im Umland
- Q[1]: 1.100.000 m³/d
- naturnah und ohne Desinfektion
- 50 Mitarbeiter Schichtbetrieb



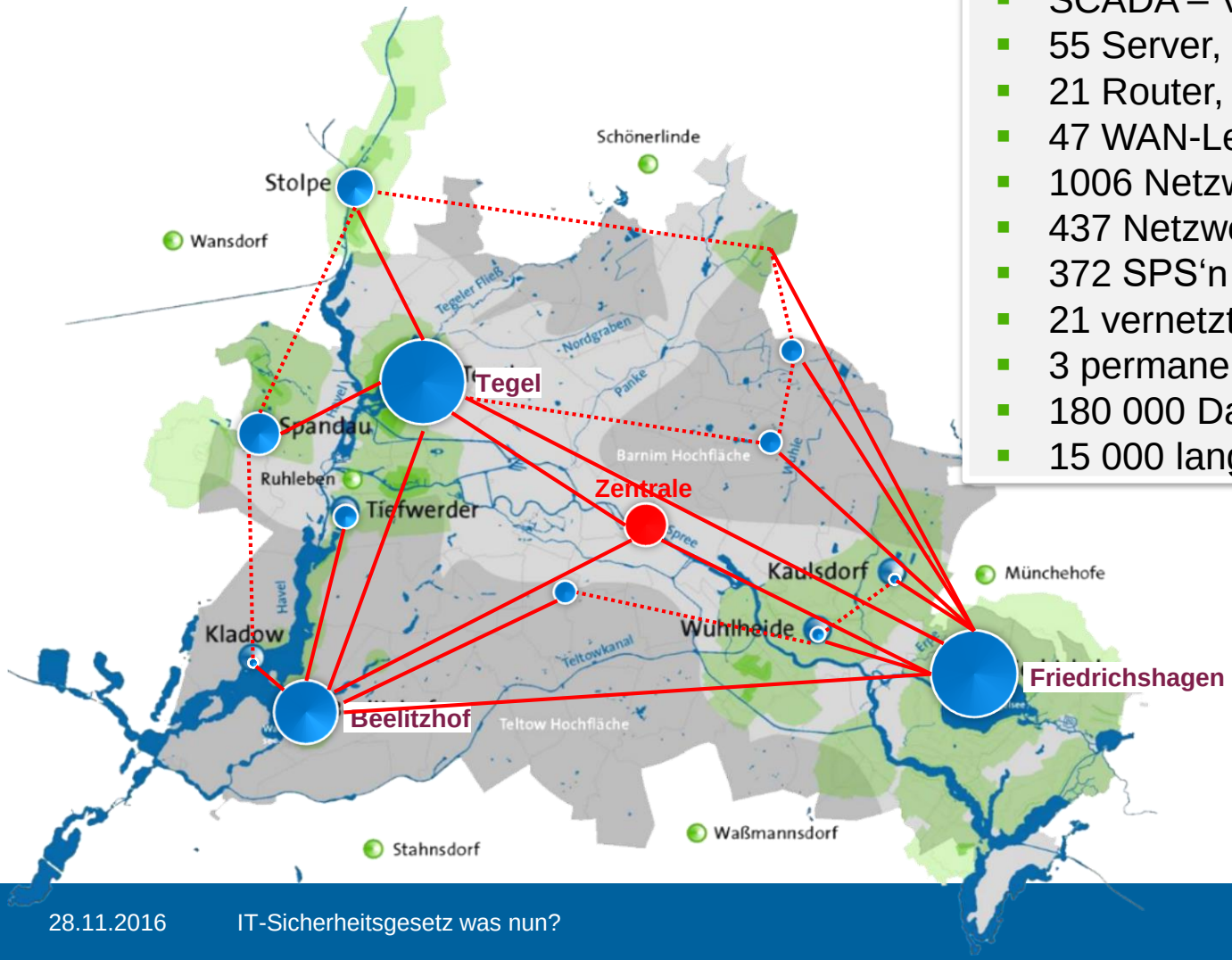
1. Vorstellung des Umfeldes

Leitsystemverbundsystem Wasserversorgung

Berliner Wasserbetriebe

Technische Kennzahlen

- SCADA – Verbund aller Werke
- 55 Server, 88 Clients
- 21 Router, 44 Switche
- 47 WAN-Leitungen
- 1006 Netzwerksports
- 437 Netzwerksdevices
- 372 SPS‘n
- 21 vernetzte Standorte
- 3 permanent besetzte Warten
- 180 000 Datenpunkte
- 15 000 langzeitarchivierte DP



SIEMENS
Intellution
ABB
Cegelec
ViDEC
Microsoft
GE Intelligent Platforms

1. Vorstellung des Umfeldes

Sicherheit benötigt Organisation

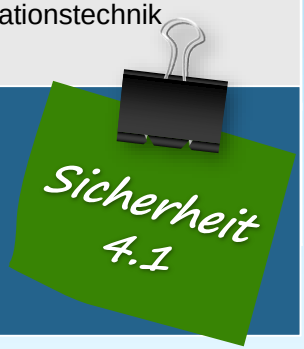
Berliner Wasserbetriebe

Unternehmenssicherheit

Personelle Sicherheit	Physische Sicherheit	Betriebs-Sicherheit	IT-Sicherheit	Krisen-schutz	Katastrophen-schutz
Grundschutz		**Anwendungen**		**Krisenmanagement**	
Zutritts-management	Perimeter- & Gebäudeschutz	Wasserversorgung / Abwasserentsorgung	Datensicherheit	Krisenstab	
Sicherheitsleitstand & Gefahrenmanagementsystem		Prozessleittechnik	Kommunikations- & Netztechnologie	Ereignismanagement → Koordination & Maßnahmen	
Objektschutz	Rohr- & Kanalnetz	Informationstechnologie & Cybersicherheit		Kommunikation	
Brandschutz		Notfallmanagement / Funkleitzentrale	Datenschutz	Kommunikationstechnik	

Sicherheitsstrategie
Konzepte & Policies & Standards
Risikomanagement
Sicherheitsbewusstsein
Sicherheitsorganisation

Sicherheits-management



2. Branchenstandards

IT Sicherheitsgesetz Regelungsbestandteile

Berliner Wasserbetriebe

Schlagwort	BSIG	Beschreibung
Standards	§8a Abs. 1	Im BSIG Verweis auf "Stand der Technik". Ausgestaltung durch DVGW im Rahmen UP-Kritis. Umsetzung innerhalb von 2 Jahren.
Meldepflicht	§8b Abs. 3	Meldung von erheblichen Störungen an das Bundesamt für Sicherheit in der Informationstechnik.
Erreichbarkeit	§8b Abs. 3	Jederzeit erreichbare Kontaktstelle ist einzurichten.
Audits	§8a Abs. 3	Mindestens alle 2 Jahre Nachweis der Erfüllung durch Audits, Prüfungen oder Zertifizierungen.
Unterstützung	§3 Abs. 3	BSI kann auf Ersuchen beraten und unterstützen

2. Stand der Technik & Branchenstandards
Was kommt ?

Branchenstandard
Grundlagen

- Branchenstandard
  - IT-Sicherheitsgesetz
  - Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV)
  - Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a (2) BSIG
- Verankerung
  - DVGW-Regelwerk (Wasser), DWA-Regelwerk (Abwasser)

Branchenstandard Wasser/ Abwasser: Erläuterungen (Stand: 03.08.2016) 03.08.2016 || 4

2. Stand der Technik & Branchenstandards

Systemsicherheit

- Trennung vom Internet
- verbindliche Nutzung eines Test und Entwicklungslabors z. B.
  für Signatur und Patchmanagement sowie Qualitätssicherung in der Entwicklung
- verbindliche Anforderungen an externe Dienstleister z. B.
  externer Auszug des Sicherheitskonzeptes als verbindlicher Angebotsbestandteil
- Systemhärtung
- Nutzung eines Schwachstellenscanners
- netzinterner industrial Honeypot als Alarmanlage

- Versionierung mit Online Soll-Ist-Vergleich der SPS Programme
- Sperrung von Wechseldatenträgern z.B. USB Sticks (Stuxnet)

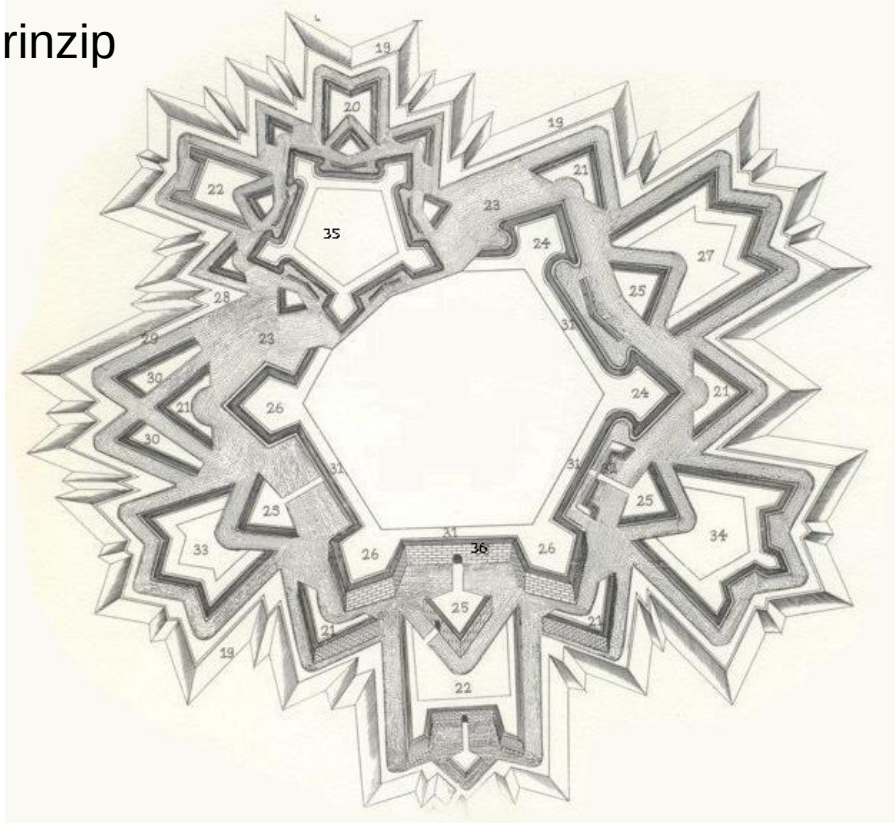
- Download von Dateien nur über separates Netzwerk mit Virenprüfung

2. Stand der Technik & Branchenstandards

Defense in Depth am Beispiel Zugang & Zugriff

Extern

- Deklaration von Zutrittsberechtigungen nach dem Sicherheitszonen (Zwiebel) Prinzip
- Überwachung der Liegenschaften über Brand- und Einbruchsmeldeanlagen



BWB intern

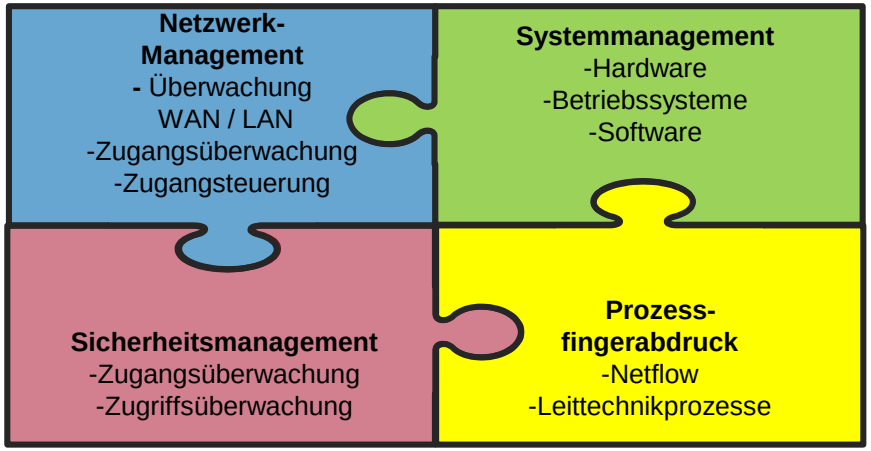
- Elektronisches Schließsystem
- Für hochsensible Bereiche Türkontakte und Bewegungsmelder
- Leittechnikschaltschränke mit Türmelder versehen

Systemintern

- zentrale personenbezogene Benutzersteuerung
- Überwachung von Logins und der Anwendung von Benutzerrechten

2. Stand der Technik & Branchenstandards
Netz- und Systemsicherheit: Monitoring

- Überwachung der Netzwerksteilnehmer
- Überwachung des Konnektivitätsstatus
- Überwachung der Fernzugänge
- Überwachung der Firewall-Konfiguration
- Autorisierung der Netzwerksteilnehmer
- aktive Port-Security
  automatische Alarmierung und Blockierung



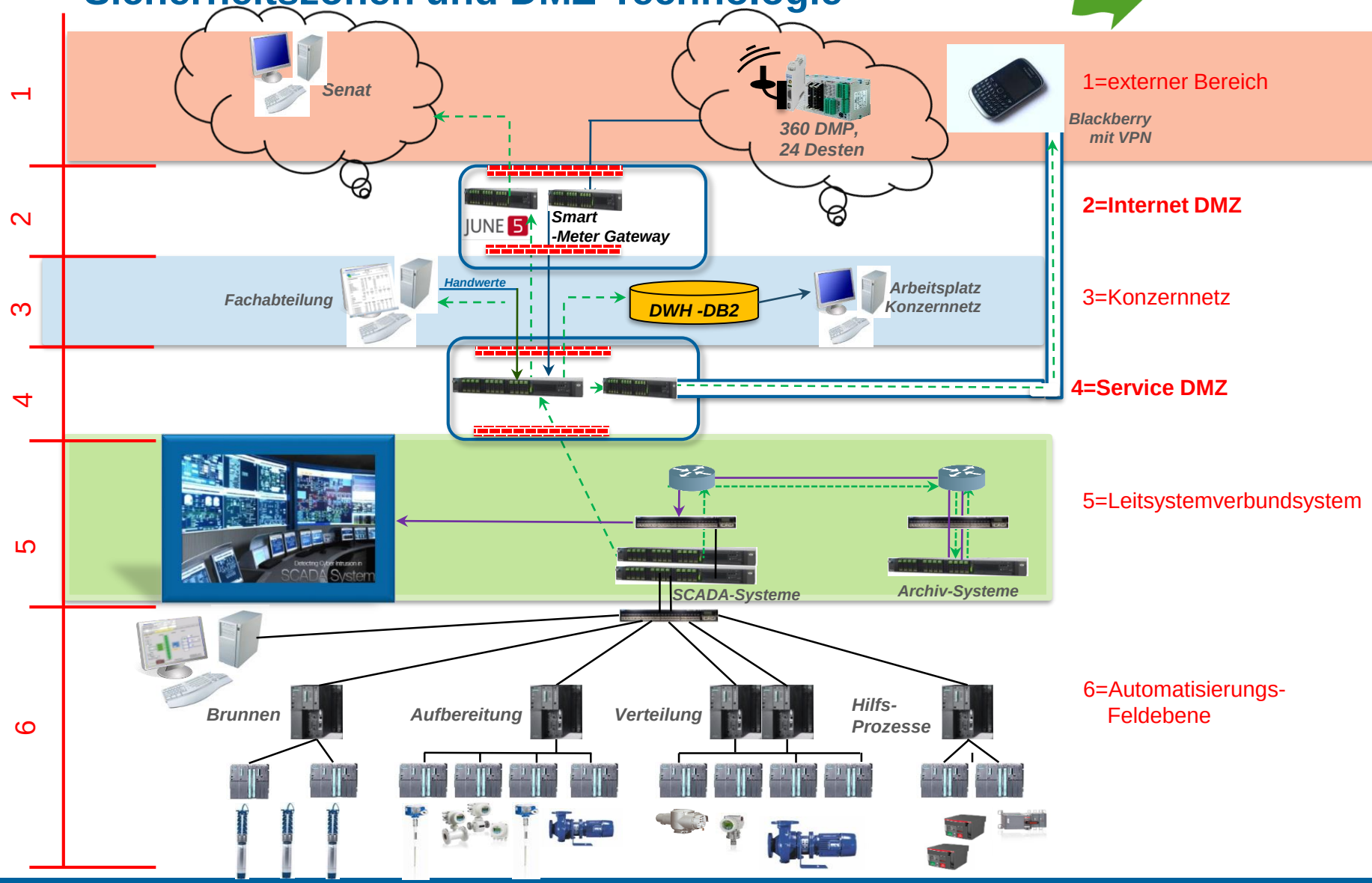
- Überwachung des Netzwerksfingerabdruckes
- Überwachung des Prozessfingerabdrucküberwachung

- Überwachung der Hardware und der Betriebsysteme
- aktive Alarmierung und automatische Eskalation auf Prozessebene

- Schaltschranktürüberwachung
- Überwachung Logins & des Anwendens von Benutzerrechten

2. Stand der Technik & Branchenstandards

Sicherheitszonen und DMZ-Technologie



2. Stand der Technik & Branchenstandards

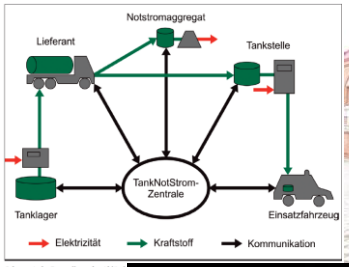
"Plan B" als Pflicht

vom Leitsystem unabhängige Bedienebene

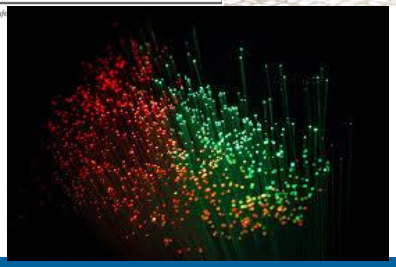
Katastrophenschutz

Redundanzen in Datenwegen und technischen Systemen und Abhängigkeiten von externen Strukturen berücksichtigen

Tanknotstrom



Eigenbewirtschaftete Darkfiber



2. Stand der Technik & Branchenstandards

SINA=sichere Ferneinwahl

- Fernzugriffe auf die Leittechnik ausschließlich in Eigenregie der BWB

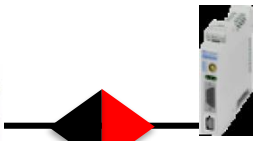
- *Seit 2013 – Nutzung von* SINA (Ablösung von ISDN)
- Nutzung bei Rufbereitschaft und externen Dienstleistern für Zugriff auf
  - Leitsystem Wasserversorgung
  - Leit- und Informationssystem Abwasserentsorgung

- Online-Managementfunktion bietet
  - aktive Freischaltung für Fernzugriffe
  - Möglichkeit der Soforttrennung in Gefahrensituationen

2. Stand der Technik & Branchenstandards

SINA=sichere Remoteeinbindungen unsere Vorbereitung auf Industrie 4.0

Druckmesspunkt



SPS

UMTS Router

SINA Box R

Ethernet Modem

P,V,KVZ-Tür

SIM-Karte mit großem Datenvolumen!

DSL Anschluss

Internet-Router

SINA Box L3

Werks-automatisierung

P,V,KVZ-Tür

Wasserwerk

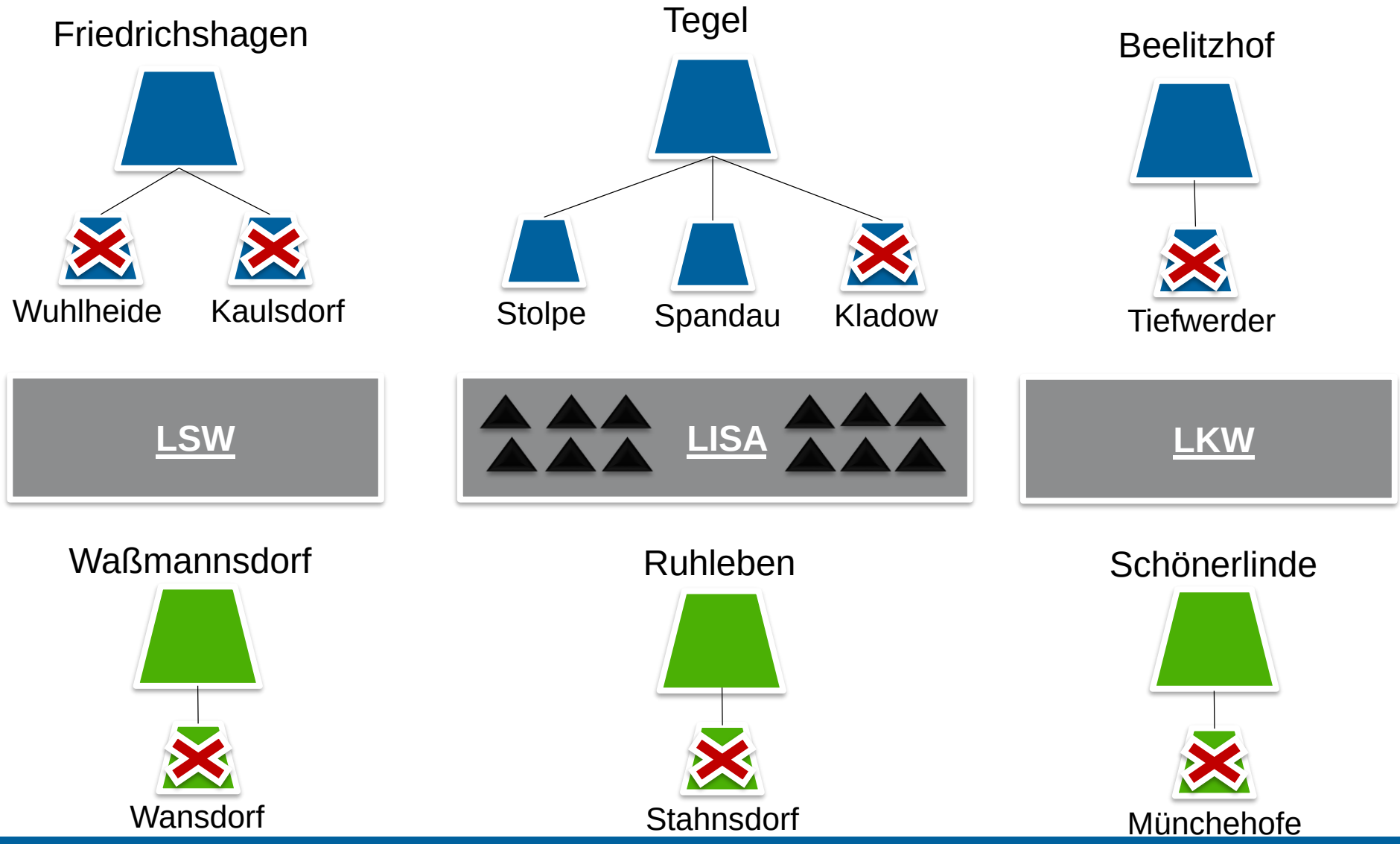
3. Meldepflicht

IT Sicherheitsgesetz Regelungsbestandteile

Schlagwort	BSIG	Beschreibung
Standards	§8a Abs. 1	Im BSIG Verweis auf "Stand der Technik". Ausgestaltung durch DVGW im Rahmen UP-Kritis. Umsetzung innerhalb von 2 Jahren.
Meldepflicht	§8b Abs. 3	Meldung von erheblichen Störungen an das Bundesamt für Sicherheit in der Informationstechnik.
Erreichbarkeit	§8b Abs. 3	Jederzeit erreichbare Kontaktstelle ist einzurichten.
Audits	§8a Abs. 3	Mindestens alle 2 Jahre Nachweis der Erfüllung durch Audits, Prüfungen oder Zertifizierungen.
Unterstützung	§3 Abs. 3	BSI kann auf Ersuchen beraten und unterstützen

3. Meldepflicht

anlagenbezogene meldepflichtige Anlagen



3. Meldepflicht
Grundprinzip Erstmeldung mit Filterfunktion

3. Meldepflicht
Vereinfachte Fragen zur Feststellung der Meldepflicht

Berliner Wasserbetriebe

Welche Anlage(n) bzw. Systeme sind Betroffen?

- LISA
- HPW Chab
- HPW Köp
- LKW
- KW Ruh
- KW Mün
- .....
- .....
- .....

Textfeld

Hält die Störung noch an?

- Ja
- Nein

Der Vorfall

- führt(e) zum vollständigen Ausfall der Anlage oder Systems: → BSI Meldung!
- zu einer Beeinträchtigung der Anlage oder Systems mit Auswirkung auf die Entsorung in Menge oder Qualität. → BSI Meldung!
- hätte zu einer Beeinträchtigung oder einem Ausfall führen können. → BSI Meldung?
- hatte in keinerlei Hinsicht Auswirkungen auf die Abwasserentsorgung. → Interne Meldung
- im Moment nicht absehbar.

Textfeld

4. Vorbereitung auf die Zertifizierung

IT Sicherheitsgesetz Regelungsbestandteile

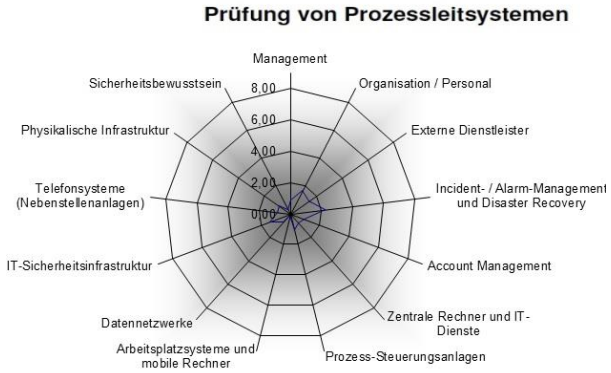
Schlagwort	BSIG	Beschreibung
Standards	§8a Abs. 1	Im BSIG Verweis auf "Stand der Technik". Ausgestaltung durch DVGW im Rahmen UP-Kritis. Umsetzung innerhalb von 2 Jahren.
Meldepflicht	§8b Abs. 3	Meldung von erheblichen Störungen an das Bundesamt für Sicherheit in der Informationstechnik.
Erreichbarkeit	§8b Abs. 3	Jederzeit erreichbare Kontaktstelle ist einzurichten.
Audits	§8a Abs. 3	Mindestens alle 2 Jahre Nachweis der Erfüllung durch Audits, Prüfungen oder Zertifizierungen.
Unterstützung	§3 Abs. 3	BSI kann auf Ersuchen beraten und unterstützen

4. Vorbereitung auf die Zertifizierung

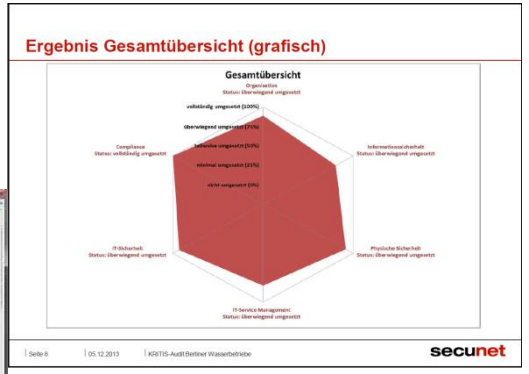
bisherige Prüfschritte

- Überprüfung der Sicherheit des LSW durch die Innenrevision

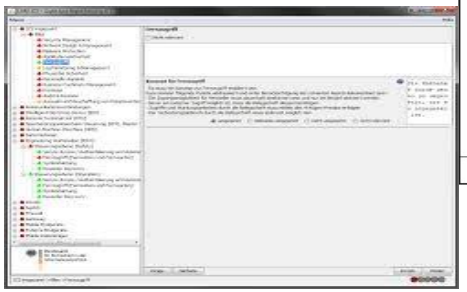
- Internes Security-Audit über KRITIS-Standortcheck



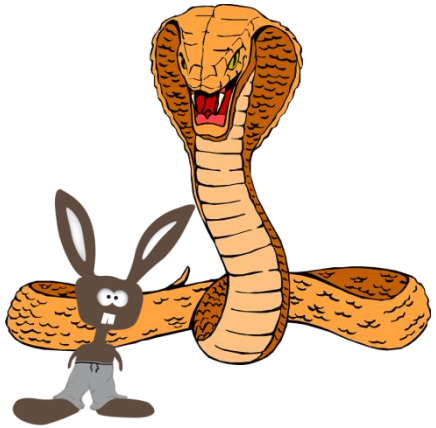
- externes KRITIS-Testat



- internes Security Audit über LARS



4. Vorbereitung auf die Zertifizierung
Maßnahmen der BWB



- Benennung von Produktions-IT Sicherheitsingenieuren
- Erarbeitung einer Information Security Policy
- Festlegung von Sicherheitskonzepten
- Aufbau einer Schutzbedarfsfeststellung
- Ausbau des Risikomanagements
- Aufbau der Notfallplanung und Ausbau des Krisenmanagement
- unabhängige Überprüfung des Sicherheitsniveaus (externe Sicht)
- Planung eines Penetrationstests zur Überprüfung des technischen Sicherheitsniveaus
- Umsetzung des Standes der Technik
- Definition von Anforderungen / Regeln für Externe
- Awarness-Schulungen

Vielen Dank
für ihre Aufmerksamkeit

…noch Fragen?