Bundesverband

TeleTrusT
Pioneers in IT security.

TeleTrusT – Bundesverband IT-Sicherheit e.V.

Allianz für Sicherheit der Wirtschaft e.V. - ASW Bundesverband

TeleTrusT/ASW-Workshop "IT-Sicherheit in der Wirtschaft"

Berlin, 23.09.2015

Cyber-Security-Strategie einer Kritischen Infrastruktur

Michael Böttcher, IT-Sicherheitsingenieur Wasserversorgung, Berliner Wasserbetriebe

Cyber-Security-Strategie einer Kritischen Infrastruktur

Michael Böttcher IT-Sicherheitsingenieur Wasserversorgung

Agenda

I. Das Unternehmen

II. Standpunkt zur Sicherheit

III. Grundsätze und Leitlinien

IV. Fazit

I. Das Unternehmen

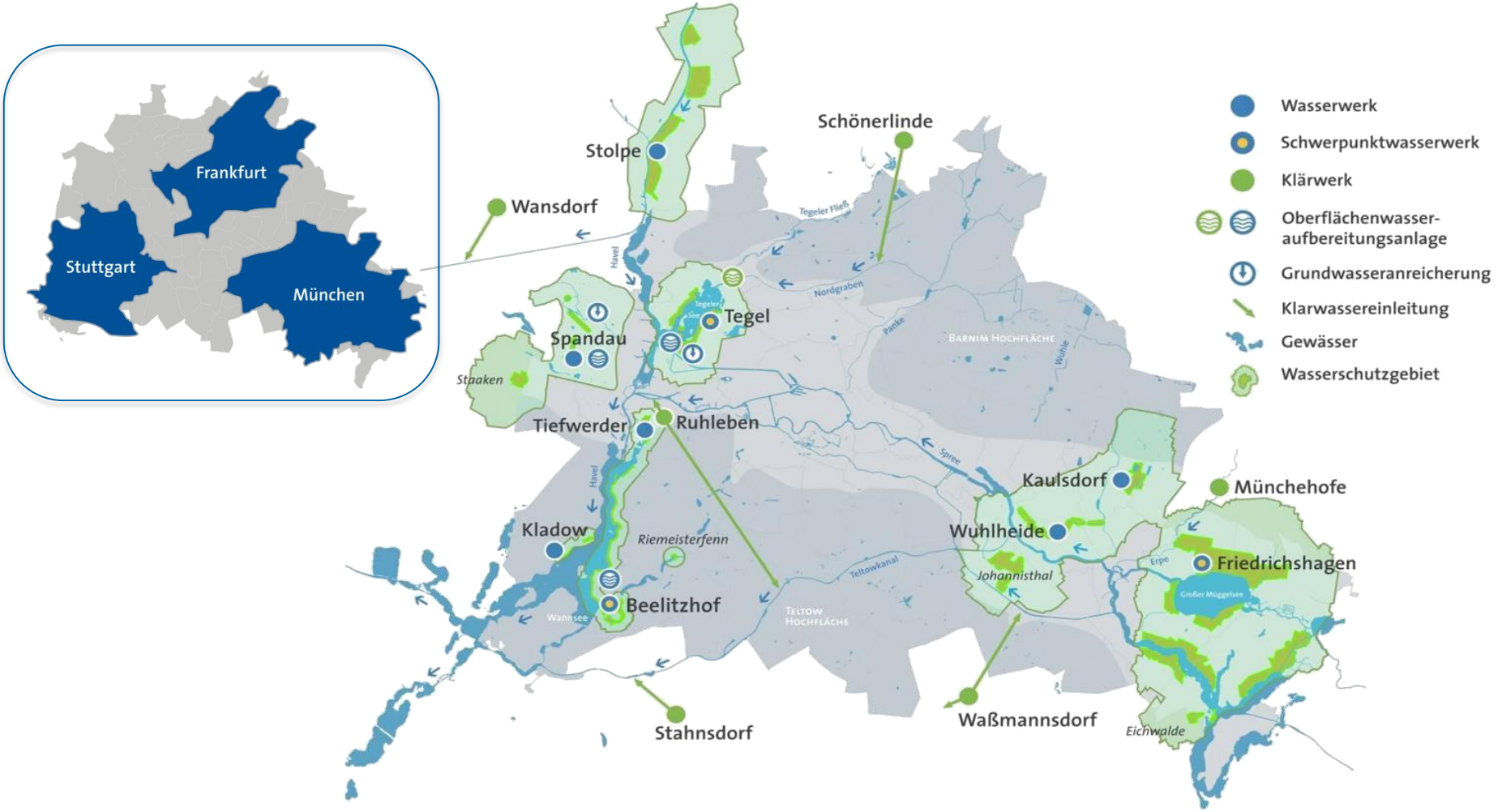
Die Berliner Wasserbetriebe in Zahlen

Trinkwasserversorgung	Abwasserentsorgung	Wirtschaftliche Kennziffern
Wasserverkauf:	*Reinigungsleistung:*	1,1 Mrd. € Umsatz
190 Mio. m³	234 Mio. m³	138 Mio. € Jahresüberschuss
7.900 km Rohrnetz	9.700 km Kanalnetz	264 Mio. € Investitionen
9 Wasserwerke	1.200 km Druckleitungen	5,8 Mrd. € Anlagevermögen
700 Brunnen	6 Klärwerke	4.523 Beschäftigte
	158 Pumpwerke	

Zahlen des Geschäftsjahres 2014

I. Das Unternehmen

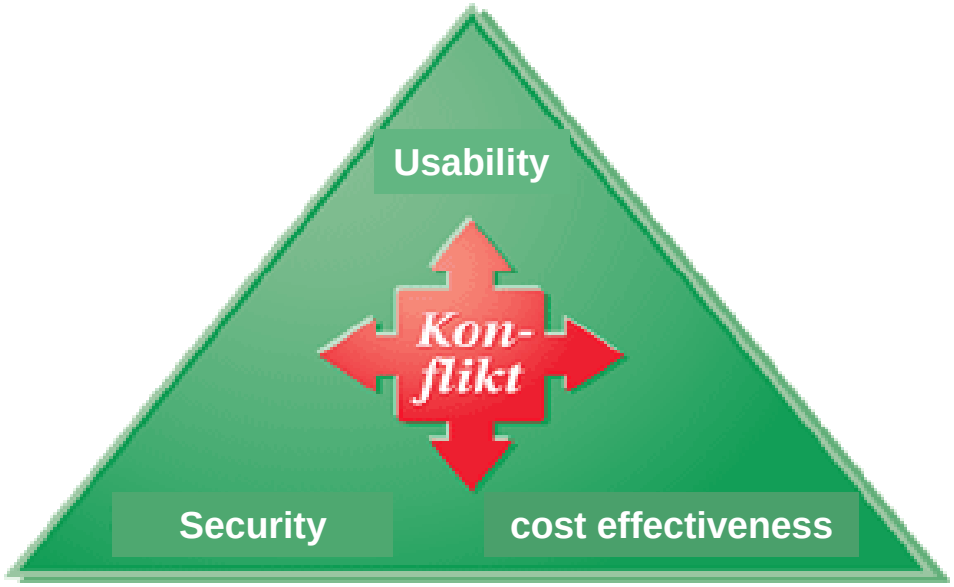
Wasser für Berlin



II. Standpunkt zur Sicherheit

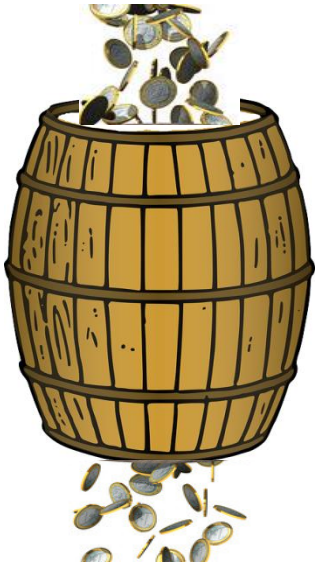
Risiken und Konflikte im Spannungsfeld

- Sicherheit versus Usability/Komfort
- Sicherheit versus Kosten
- Usability/Komfort versus Kosten

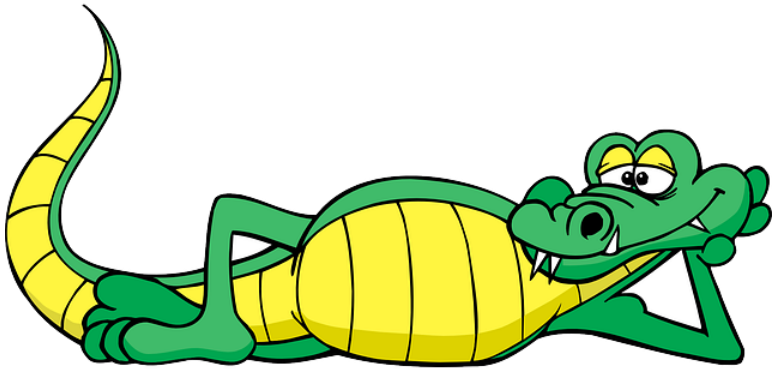


II. Standpunkt zur Sicherheit

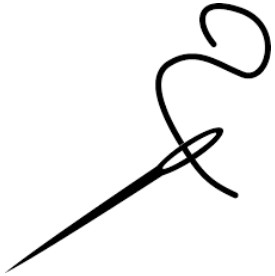
Wozu Sicherheit ?



- Sicherheit kostet Geld



- Sicherheit verschlingt Personalressourcen



- Sicherheit engt ein (Regelwerke)

II. Standpunkt zur Sicherheit

Trends - Risiken und Gefährdungen

Cyberkriminalität

Social Engineering

Stromausfall (Blackout)

Hochwasser / Überflutungen

Organisierte Kriminalität

Unwetterzunahme Wasser / Schnee / Hagel

Vandalismus / grober Unfug

Brandstiftung / Brandanschläge

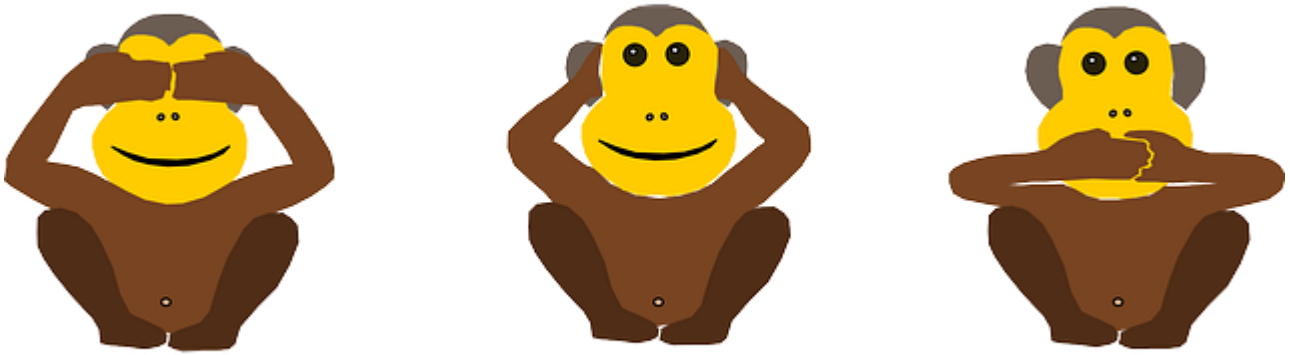
Einbruch / Diebstahl

Terror

II. Standpunkt zur Sicherheit

Individuelle Gefahrenwahrnehmung:

- Ich sehe nichts!
- Ich höre nichts!
- Ich schmecke nichts!
- Es tut mir nichts weh!
- Es wird schon einen anderen treffen!



II. Standpunkt zur Sicherheit

Was ist Ihnen sicherer?

Wieviel Prozent werden in privaten Ausgaben für die Absicherung von Türen und Fenstern ausgegeben?

Wie hoch sind die Ausgaben für Sicherheit, speziell IT - Sicherheit in den Unternehmen?

II. Standpunkt zur Sicherheit

Ups - Wie konnte das passieren?

Berliner Wasserbetriebe

HACKER-ATTACKE IM BUNDESTAG

BILD zeigt das brisante Geheim-Protokoll

30 Provinzen betroffen

Stromausfall legt große Teile der Türkei lahm

Ein großflächiger Stromausfall hat weite Teile der Türkei getroffen. In Istanbul und Ankara stoppten die U-Bahnen. Der türkische Energieminister hält selbst einen Cyber-Angriff für möglich.

31.03.2015

n-tv

Suchen auf n-tv.de

Rheinland-Pfalz 22.06.2015

Hackerangriff auf Kfz-Zulassungsstellen - Dienststellen in Rheinland-Pfalz und Hessen betroffen

POLITIK

Samstag, 20. Dezember 2014

Hackerangriff auf Sony

Cyberangriff entwickelt sich zur Staatsaffäre

Mit der Hacker-Attacke auf Sony könnte Nordkorea den Bogen überspannt haben. US-Präsident Obama plant eine "angemessene Reaktion" auf den Einschüchterungsversuch aus Pjöngjang. Die Filmkonzerne warnt er vor Selbstzensur.

iX MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK

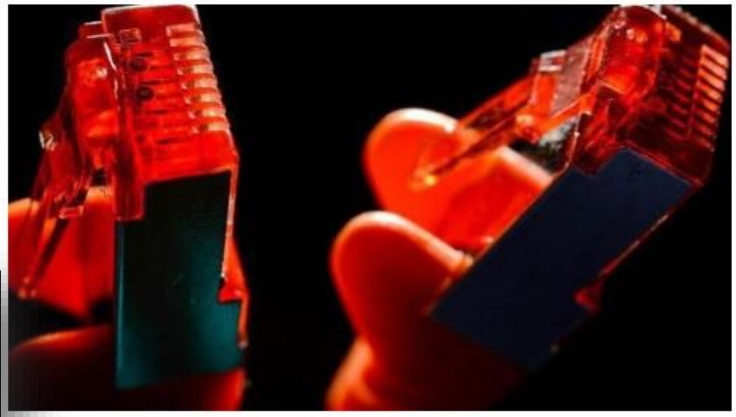
News Artikel Apps Aktuelles He

iX > 7-Tage-News > 2015 > KW 31 > Honeynet-Projekt analysiert Gefahren für Industrie 4.0

« Vorige | Nächste »

Honeynet-Projekt analysiert Gefahren für Industrie 4.0

28.07.2015 14:44 Uhr – Ute Roos vorlesen



(Bild: dpa, David Ebener++)

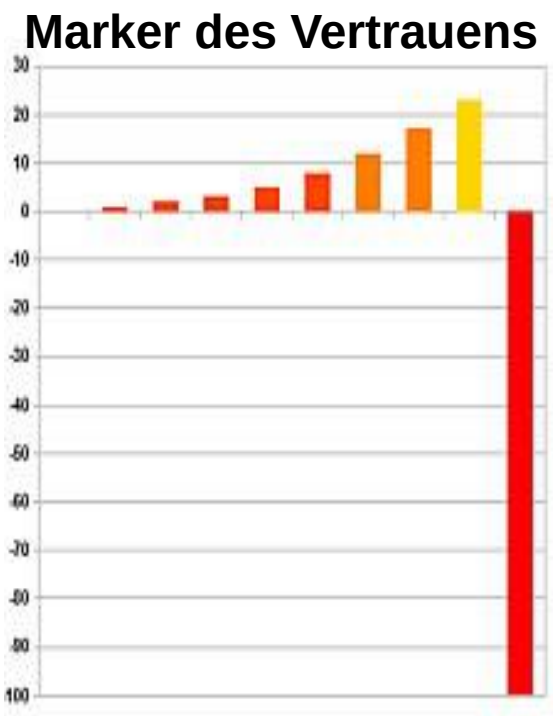
Acht Monate lang beobachteten Experten des TÜV SÜD, welche Angriffe von wo aus auf ihr simuliertes Wasserwerk erfolgten. Ihre Erkenntnisse sollten arglose Unternehmen spätestens jetzt wachrütteln.

Infrastrukturen und Produktionsstätten werden gezielt angegriffen, potenzielle Angreifer lauern überall. Den Nachweis dafür lieferte die Analyse der 60.000 Zugriffe auf eine virtuelle Infrastruktur, die der TÜV SÜD während der achtmonatigen Laufzeit seines Honeynet-Projektes verzeichnen konnte. Das Honeynet kombinierte reale Hardware und Software mit einer simulierten Umgebung eines kleineren Wasserwerks. Die Experten beobachteten Zugriffe von Servern aus der ganzen Welt, teilweise unter verschleierten IP-Adressen.

II. Standpunkt zur Sicherheit

Die Truthahn-Illusion
oder der Nachteil einer vergangenheitsbasierten Risikobetrachtung

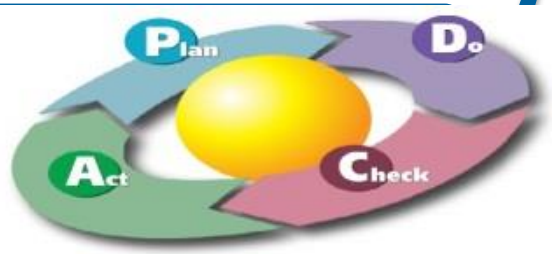
Es wird gerne übersehen, dass der sogenannte schlimmste Fall zu der Zeit, da er sich ereignete, schlimmer war als der damals geltende „schlimmste Fall“.



III. Grundsätze und Leitlinien

Vorgehensweise Sicherheitsprozess

1.	**Schutzbedarf**	1.	analysieren
2.	**Risiko**	2.	betrachten und definieren
3.	**Daten & Systeme**	3.	klassifizieren
4.	**zentrale Vorgaben**	4.	entwickeln
5.	**Maßnahmen**	5.	entwickeln und anwenden
6.	**Sicherheit**	6.	prüfen



III. Grundsätze und Leitlinien

Weg und Methode der „kritische Pfad“

Prozesstransparenz herstellen

Benutzerberechtigungskonzepte erarbeiten

Anforderungen / Leitlinie definieren

Sicherheitskonzepte entwickeln

Zugänge und Zugriffe absichern

Systeme und Daten schützen

Abhängigkeiten von einzelnen Komponenten minimieren

Notfall und Wiederanlaufpläne definieren

Awarness schaffen

Sicherheitsniveau prüfen

III. Grundsätze und Leitlinien

Sicherheit braucht Organisation

Sicherheitsmodell der BWB (³Säulenmodell)

Unternehmenssicherheit

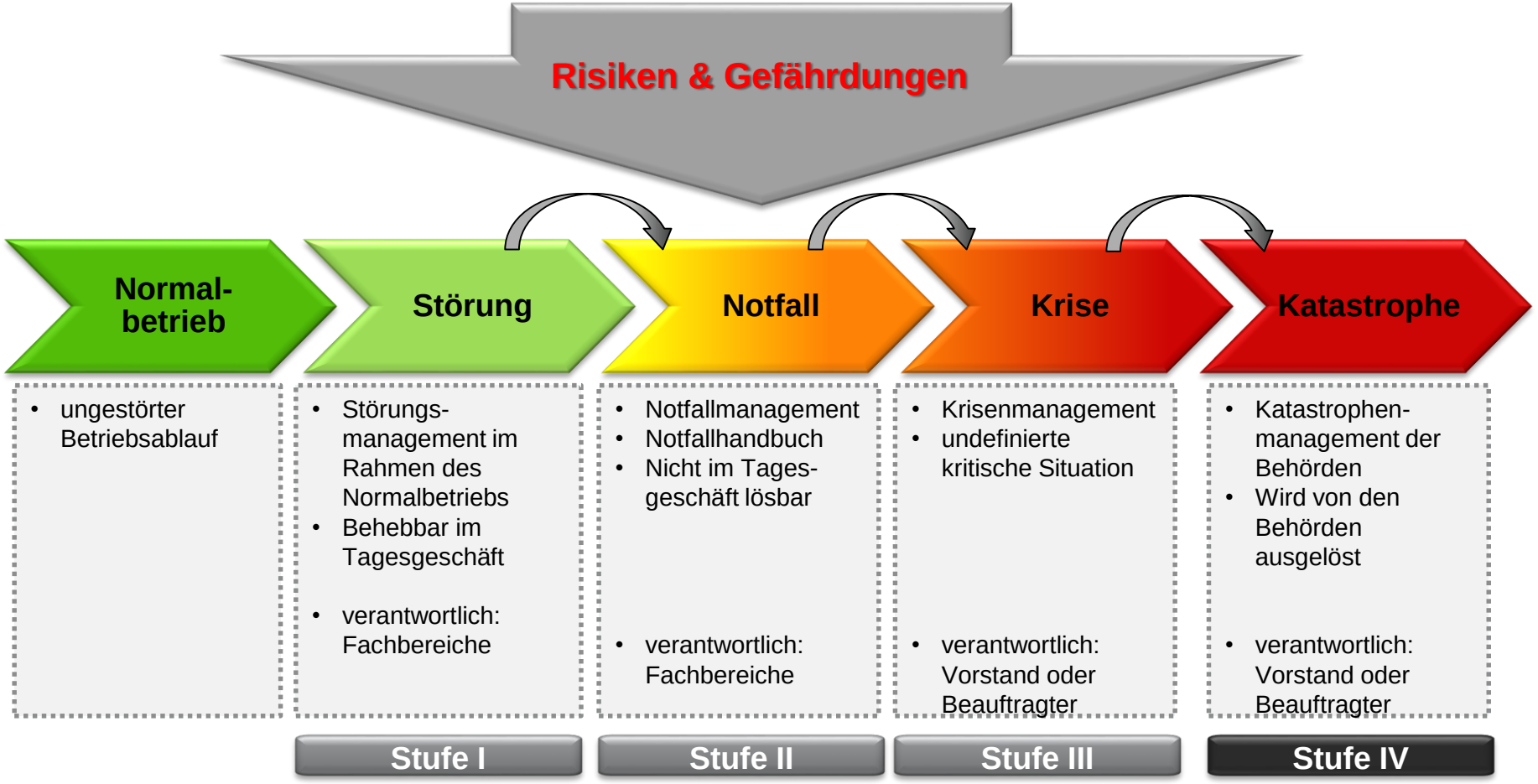
Personelle Sicherheit	Physische Sicherheit	Betriebs-Sicherheit	IT-Sicherheit	Krisen-schutz	Katastrophen-schutz
Grundschutz		**Anwendungen**		**Krisenmanagement**	
Zutritts-management	Perimeter- & Gebäudeschutz	Wasserversorgung / Abwasserentsorgung	Datensicherheit	Krisenstab	
Sicherheitsleitstand & Gefahrenmanagementsystem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

Sicherheits-management

Sicherheitsstrategie
Konzepte & Policy & Standards
Risiko-Monitoring
Awareness

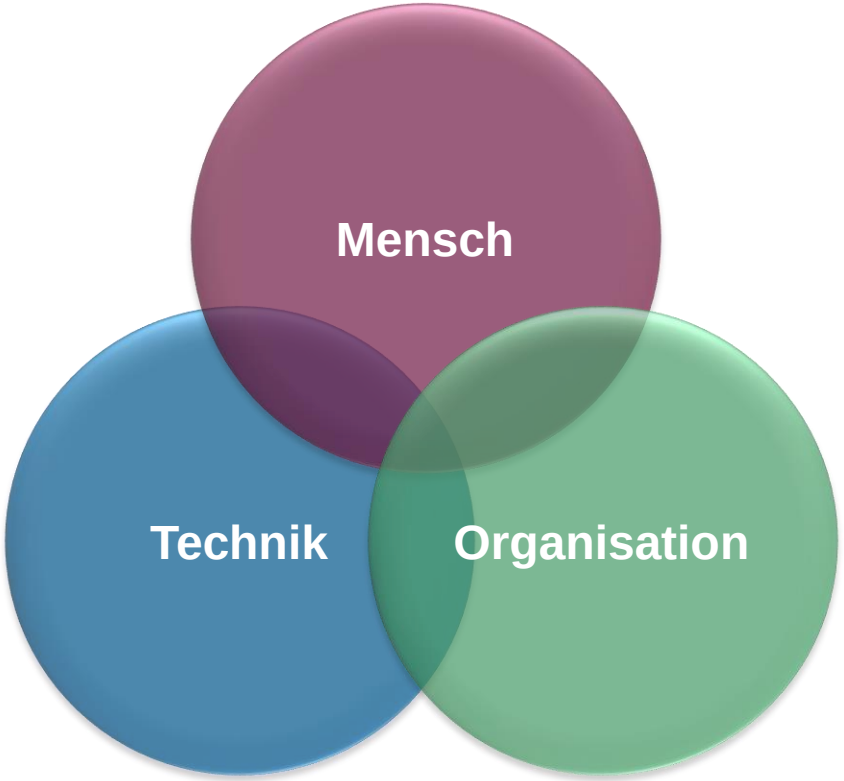
III. Grundsätze und Leitlinien

Begriffsdefinitionen



III. Grundsätze und Leitlinien

Grundsatz Sicherheit braucht Struktur
ganzheitliche Betrachtung Technik, Mensch und Organisation



Organisation
- Definition Standards
- Integration IT-Sicherheit in bestehendes Sicherheitsmanagement

Mensch
- Mitarbeiter/Innen schulen
- Sicherheitsbewusstsein schaffen
- Sicherheit als Prozess begreifen

Technik
- Installation von Virenscannern, Firewalls, DMZ, etc.
- Redundanzen
- Sicherheit bei Systemänderungen anpassen

III. Grundsätze und Leitlinien

Sicherheit benötigt Transparenz

- automatisierte Überwachung laufender Prozesse zur Detektion von Anomalien
- Kenntnis
  - der Systemtopologie
  - der Schnittstellen und Übertragungswege
  - der eingesetzten Hardwarekomponenten
  - der eingesetzten Software
  - der verwendeten Prozesse und ihrer gegenseitigen Abhängigkeiten

Wer seine Prozesse nicht kennt, hat keine Chance, den Ausnahmefall zu erkennen!

? *Über welche Schnittstellen kann auf Ihr Leitsystem zugegriffen werden?*

? *Wie werden ihre Daten übertragen und wie ist die Übertragung abgesichert ?*

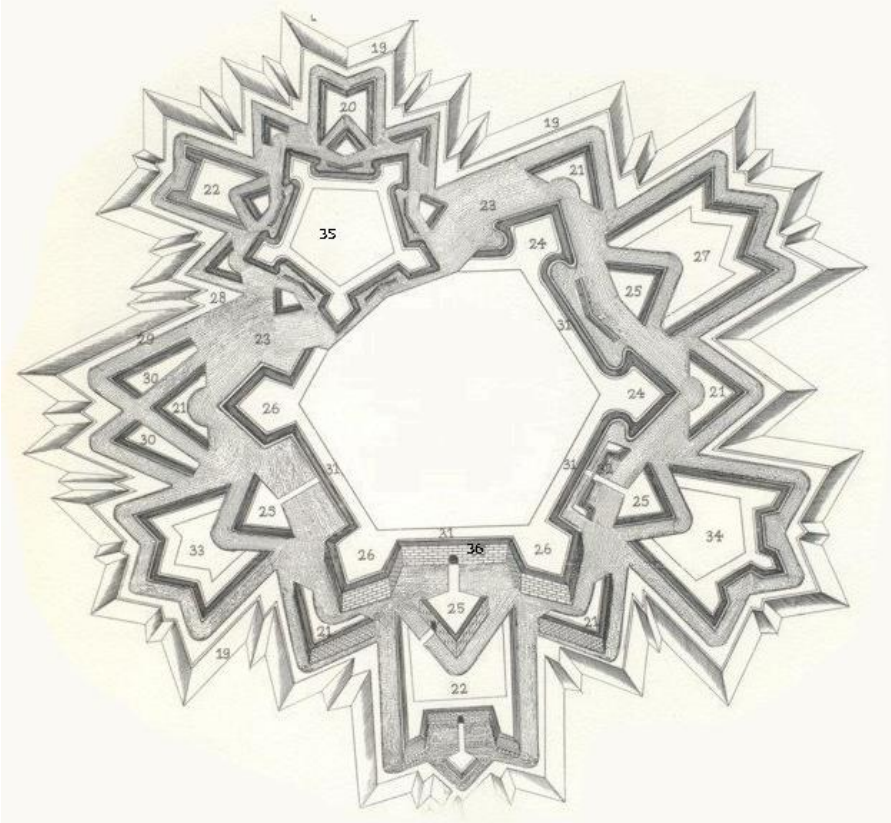
? *Wie alt ist die Firmware Ihrer SPSen?*

? *Was passiert bei Ausfall einer bestimmten SPS?*

III. Grundsätze und Leitlinien

Defense in Depth
(ergänzende ineinander greifende Sicherheitsmaßnahmen) am Beispiel Leittechniknetzwerk

- keine Internetanbindung
- abgesicherte Fernzugänge
- Kapselung
- Firewalls
- NAC aktive Port-Security
- Netzwerkssegmentierung
- Autorisierung der Netzwerksteilnehmer
- Überwachung des Netzwerksverkehrs
- DMZ-Technologie an Netzübergängen
- Prozessfingerabdrucküberwachung



III. Grundsätze und Leitlinien

Berechtigungskonzept “Minimal need to know”

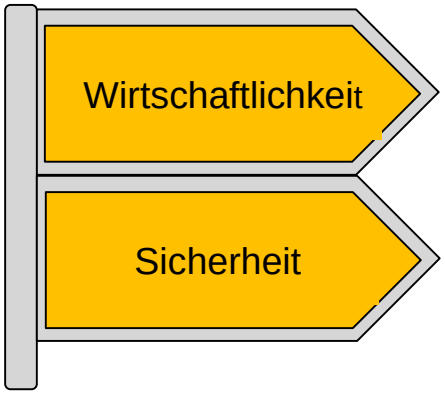
- jeder erhält nur genau die Berechtigungen, die zur Erfüllung seiner Aufgabe notwendig sind
- ausschließlich rollenbasierte Berechtigungen, keine Individualrechte!
- ausschließlich personenbezogen (auch in der Leittechnik)

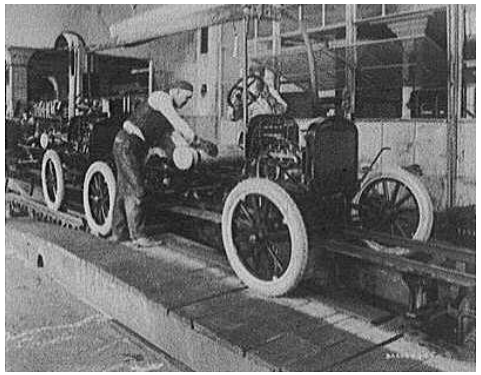
- Berechtigungen werden nach den vier Augenprinzipien erstellt Antragsteller> Umsetzer>Prüfer/ Freigebender
- Dokumentation aller Berechtigungen
- regelmäßige Prüfung vorhandener Benutzerberechtigungen
- automatisierte Überwachung der Einhaltung von Berechtigungen

III. Grundsätze und Leitlinien

Security per Design

- Berücksichtigung des Grundsatzes „Security per Design“ in der Planung
  - Aufwandsoptimierung während einer Erneuerungsphase
  - spätere Implementierung setzt aufwendige Testszenarien voraus
  - Vermeidung von Gewährleistungsproblemen
- Tests von Veränderungen der Hard- und Software vorab
  - in gekapselter nichtkritischer Umgebung mit standardisierten Checklisten





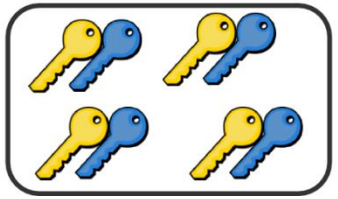
III. Grundsätze und Leitlinien

Sicherheitsanforderungen externe Dienstleister:

- Anerkenntnis der Anforderungen des BWB-Sicherheitskonzeptes als obligatorischer Angebotsbestandteil für Fremdfirmen
- Bereitstellung von Hard- und Software für interne und externe Dienstleister durch BWB
- Arbeitsanmeldeverfahren und Zugang zu Automatisierungsanlagen für externe Dienstleister
  nur in Begleitung hauseigener Mitarbeiter
- Nachweis des gesicherten Datenaustausches und der sicheren Kundendokumentenablage und Datenzugriffsrechte
- Vertraulichkeitserklärung zur Datenweitergabe
- Festlegung eines Arbeitsanmeldeverfahrens
- Hinterlegung von Quellcode für Customizing Lösungen

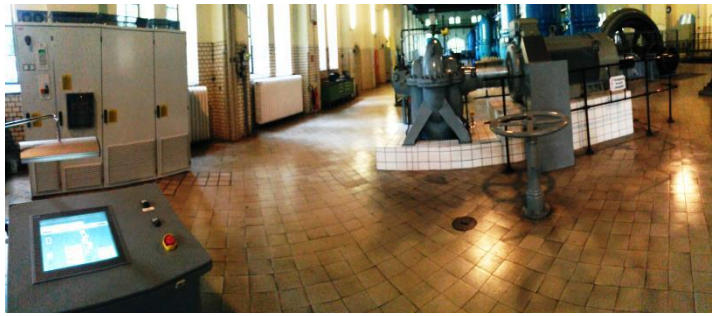
III. Grundsätze und Leitlinien

Redundanzprinzip



- Safety als “last Line of Defense” (Plan B)
- unabhängige Steuerungstrukturen der Kernprozesse

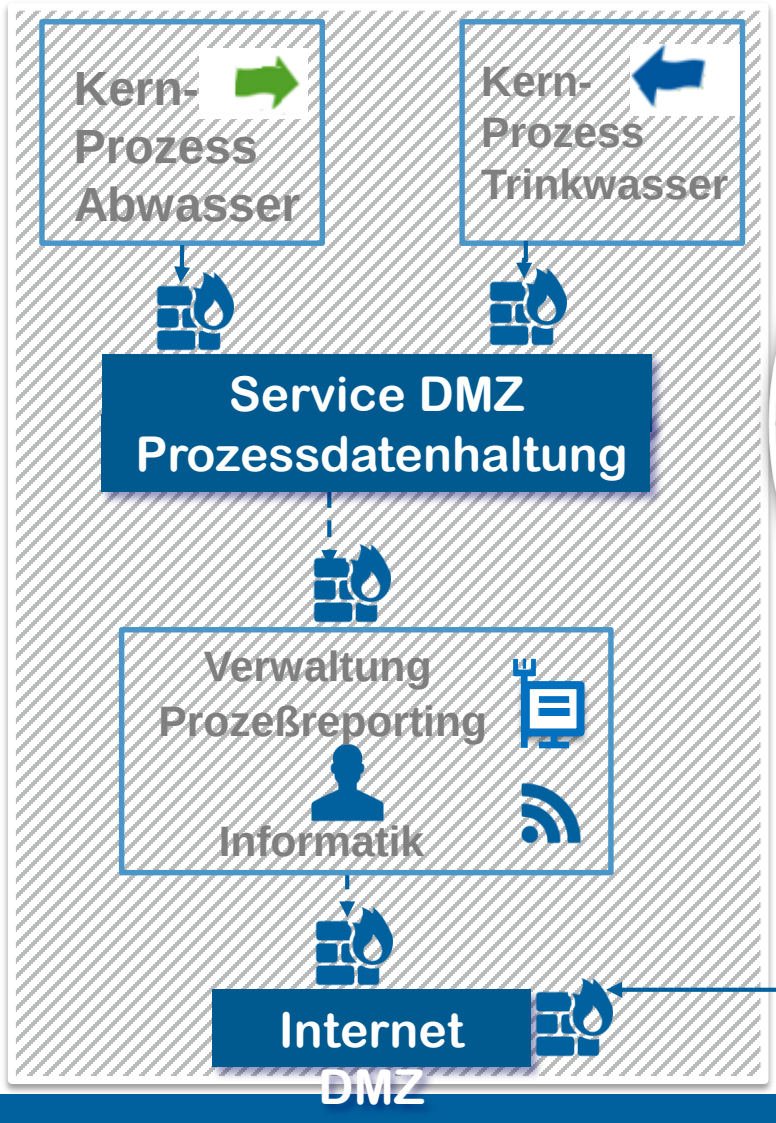
Beispiel:
unabhängige Bedienmöglichkeit
einer Reinwasserpumpe

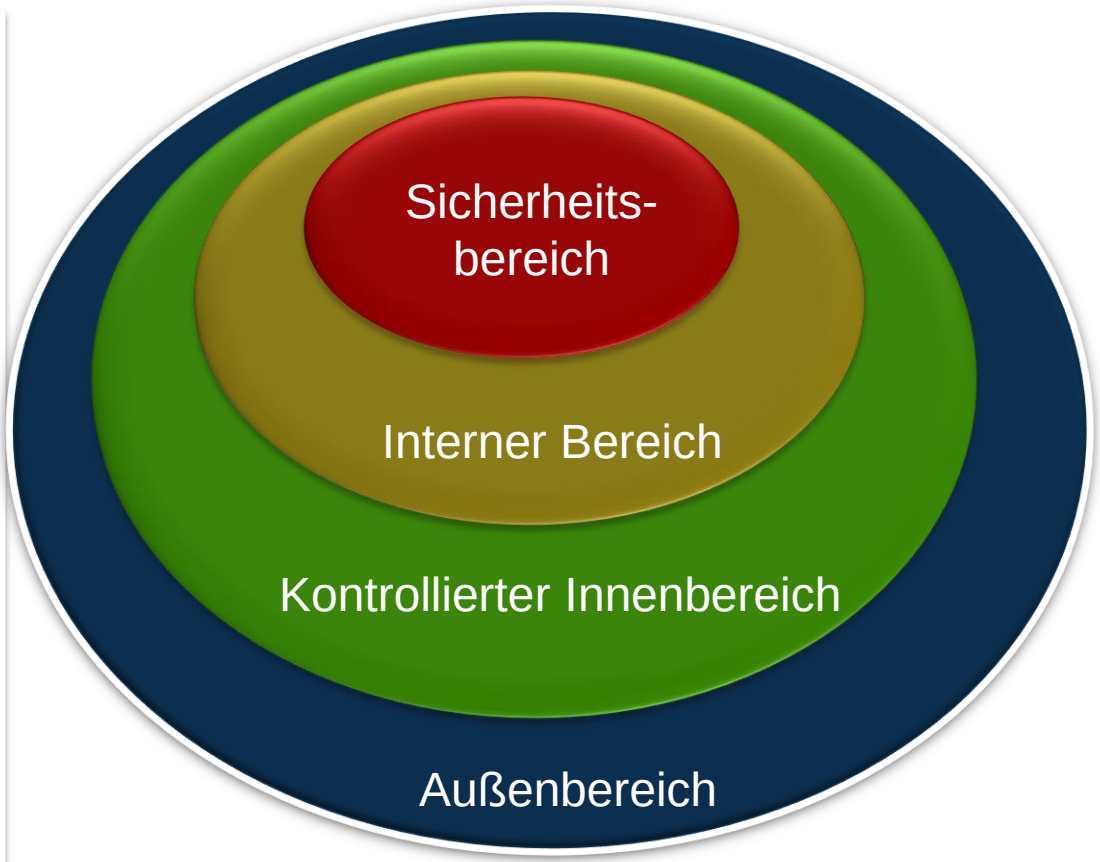


- Redundanzen in Datenwegen und technischen Systemen
- Abhängigkeiten
  von externen Strukturen berücksichtigen

III. Grundsätze und Leitlinien

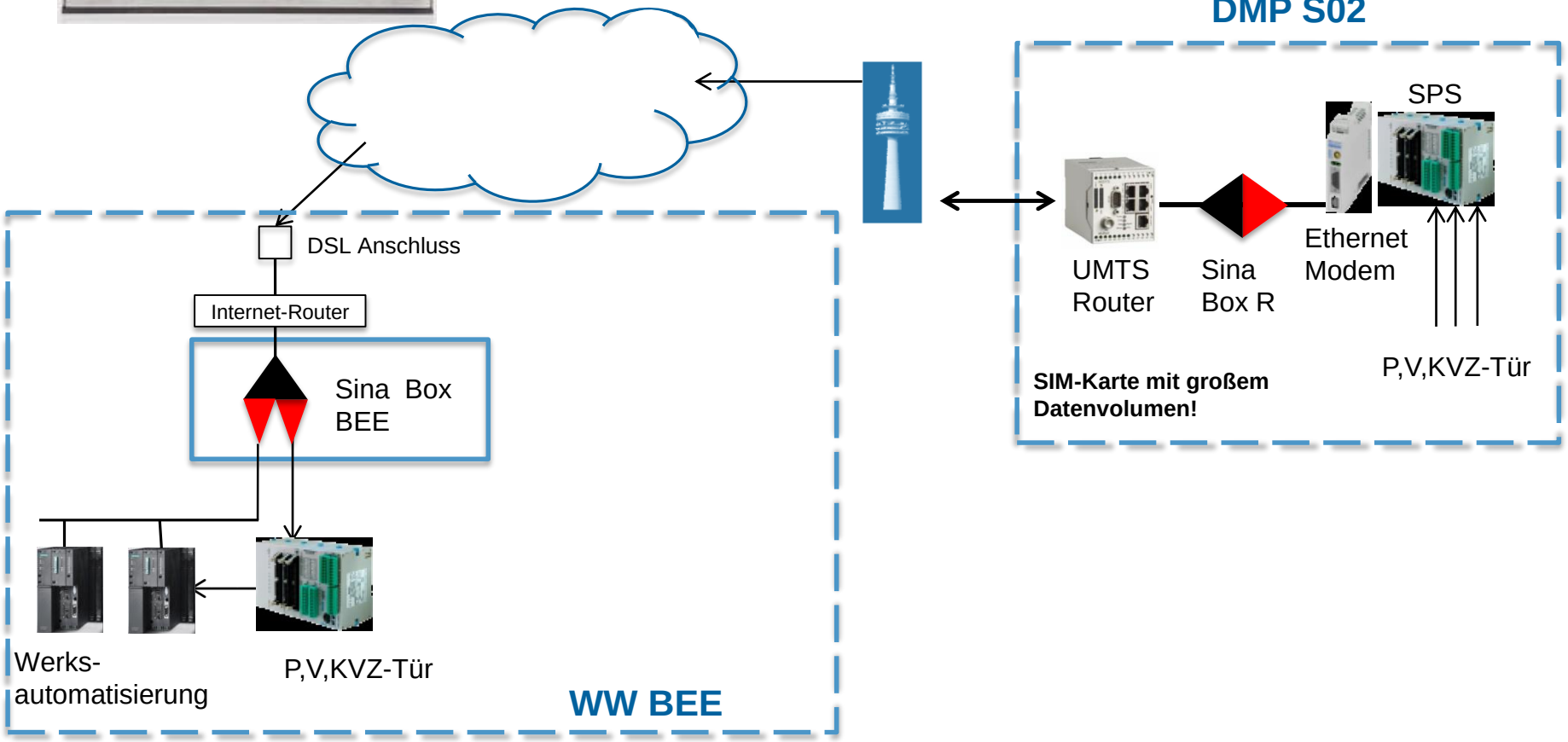
IT Sicherheit Sicherheitszonen





III. Grundsätze und Leitlinien

Fernzugänge in der aktiven Leittechnik

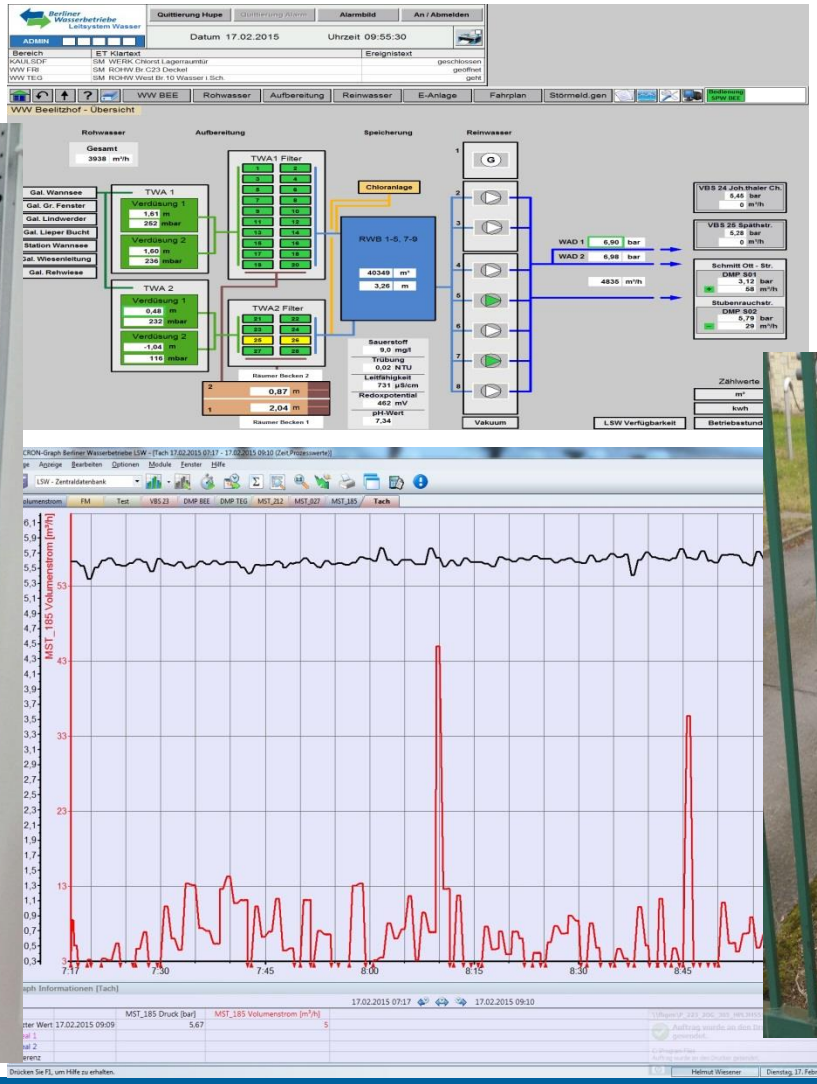


III. Grundsätze und Leitlinien

Fernzugänge in der aktiven Leittechnik

Berliner Wasserbetriebe

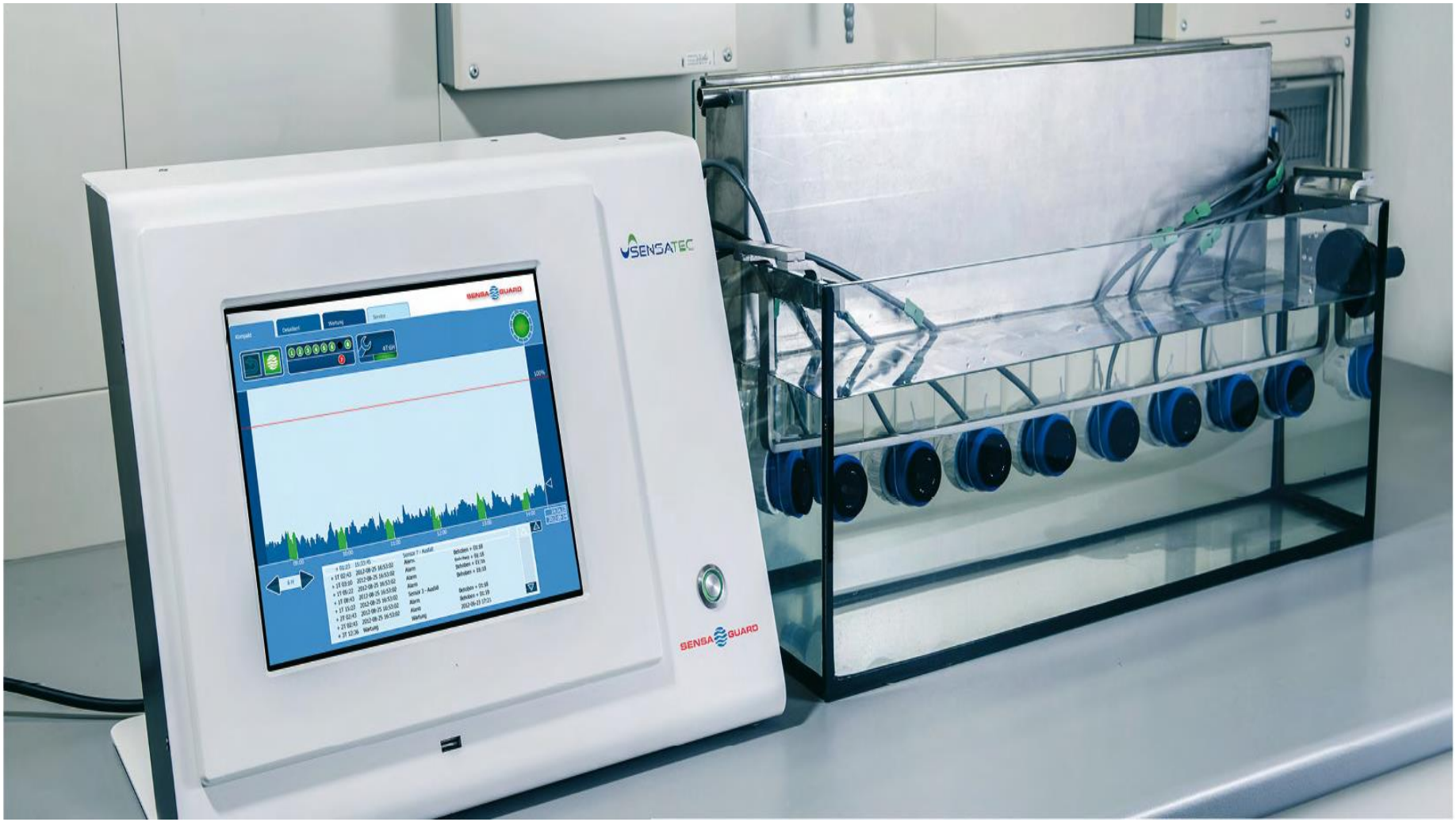
Werksserver



Druckmesspunkt

III. Grundsätze und Leitlinien

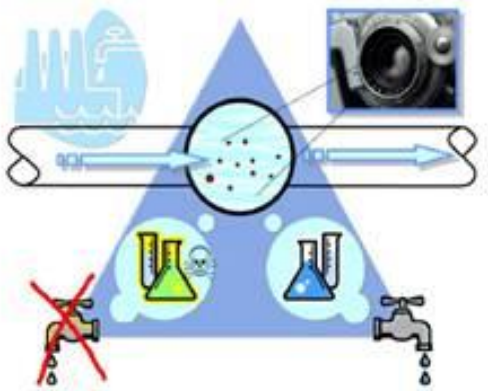
Biomonitoring

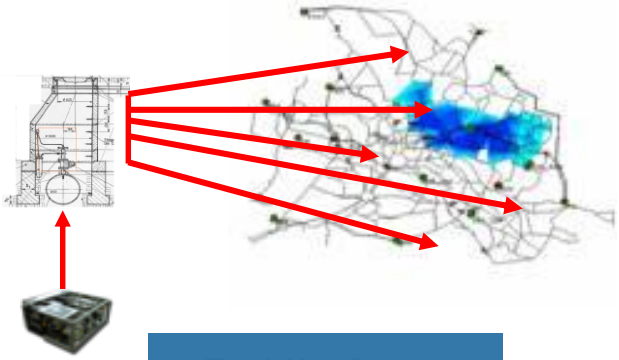


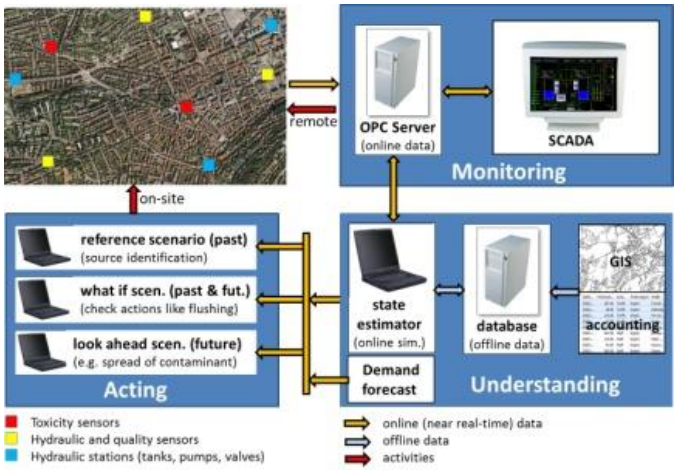
III. Grundsätze und Leitlinien

Krisenmanagement / Notfallvorsorge / Forschung

- Auqabiotox
- SimKas 3D
- SmartOnline
- TankNotStrom
- STEUERUNG
- Alphakomm
- Biomonitore
- RESI-Water







III. Grundsätze und Leitlinien

Krisenmanagement / Notfallvorsorge
Beispiel Notwasserversorgung - Trinkwasser

III. Grundsätze und Leitlinien

Erfahrungsaustausch im Sektor Verbände, Institutionen und Forschung

Berliner Wasserbetriebe

- Branchenverbände

bdew Energie. Wasser. Leben. VKU DWA DVGW

- Institutionen und Sicherheitsverbände

UP KRITIS Bundesamt für Sicherheit in der Informationstechnik Allianz für Cyber-Sicherheit

- Forschung

Technische Universität Berlin SECT Fraunhofer IPK Fraunhofer Heinrich Hertz Institute

III. Grundsätze und Leitlinien

Sicherheit ermöglicht auch neue Chancen

IV. Fazit auf einen Blick

- definierte Verantwortlichkeiten und strukturiertes Vorgehen zur IT Sicherheit sowie regelmäßige Überprüfung des Sicherheitsniveaus
- Abgesicherte Netzwerke mit sicheren Fernzugängen und ausschließlich definierten, dokumentierten und abgesicherten Schnittstellen.
- Systemhärtung und Systempflege
- dokumentierte Funktionstests in nichtkritischer Umgebung bei Veränderungen
- rollenbasiertes personenbezogenes Benutzerberechtigungskonzept nach dem Minimal Need to know Prinzip
- Security Awarness

Spezifisch Messbar Attraktiv Realistisch Terminiert

Vielen Dank für Ihre Aufmerksamkeit!

Michael Böttcher IT-Sicherheitsingenieur Wasserversorgung