# Aqua-IT-Lab

## Bewertung der Handlungsempfehlungen und Labortests


**Lehrstuhl für Wirtschaftsinformatik**
**Prozesse und Systeme**
*Universität Potsdam*

**Chair of Business Informatics**
**Processes and Systems**
*University of Potsdam*

Univ.-Prof. Dr.–Ing. habil. Norbert Gronau
*Lehrstuhlinhaber* | *Chairholder*

August-Bebel-Str. 89 | 14482 Potsdam | Germany

*Tel* +49 331 977 3322
*Fax* +49 331 977 3406

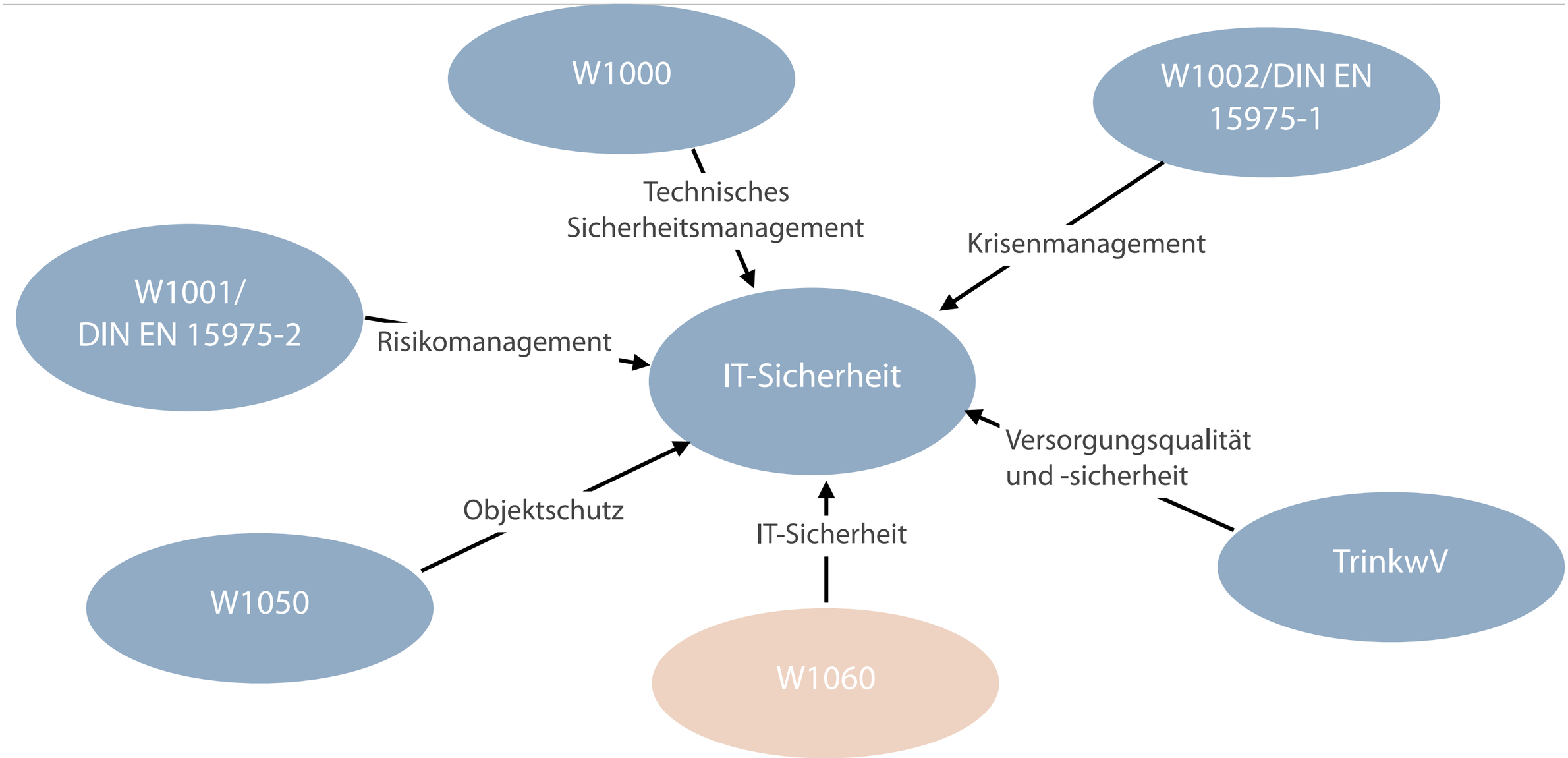
*E-Mail* ngronau@lswi.de
*Web* lswi.de

# IT-Sicherheit in der Wasserversorgung

Wirtschaftliche Umsetzung von Schutzmaßnahmen

Überprüfung der Sicherheit im Laborkontext

# Abgeleitete Verpflichtungen von Wasserversorgern zur IT-Sicherheit




**Kleine und mittlere Versorger sind nicht direkt vom IT-Sicherheitsgesetz und dem Branchenstandard betroffen. IT-Sicherheit ist aber mittelbar über bestehende Normen und Gesetze zu beachten.**

# IT-Sicherheit in der Wasserversorgung

## **Wirtschaftliche Umsetzung von Schutzmaßnahmen**

Überprüfung der Sicherheit im Laborkontext

# Self Assessment Tool

# Auswertungen

## Numerische Auswertung

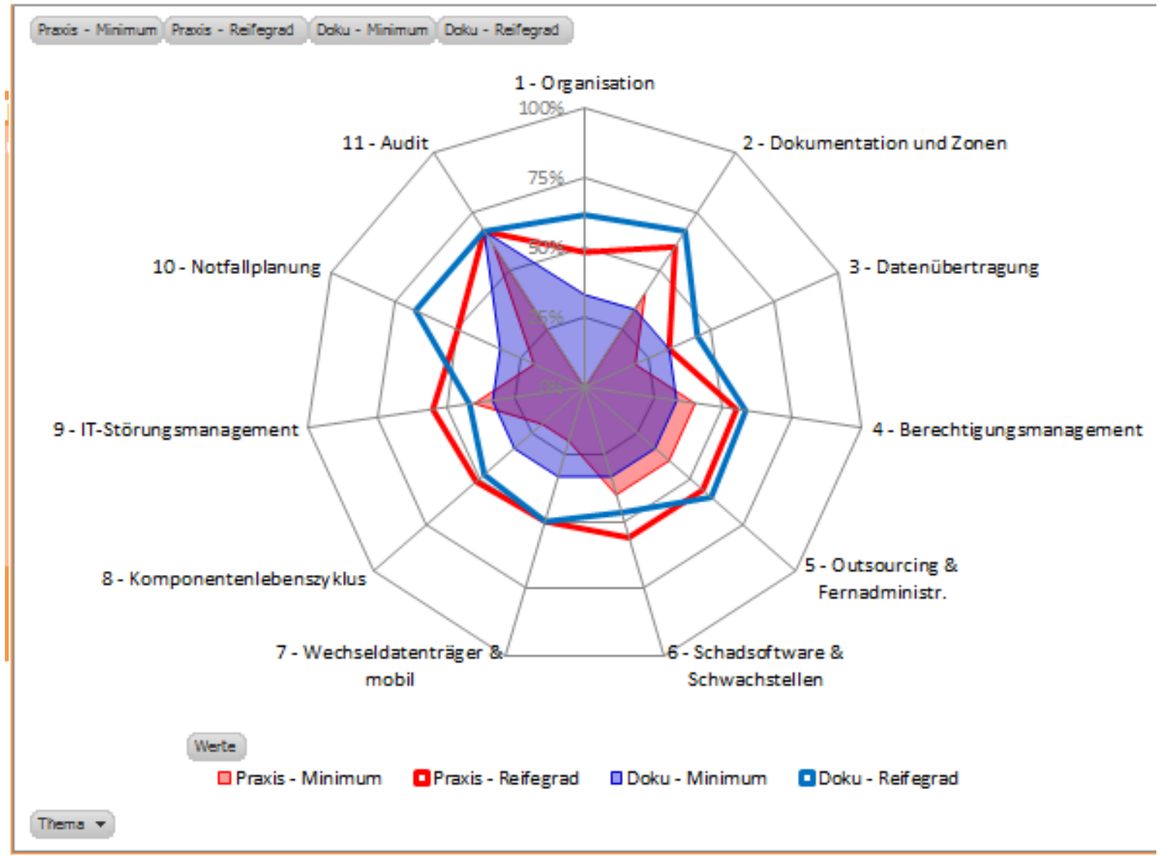
ool

uswertung - Reifegrad

| Thema | Praxis - Minimum | Praxis - Reifegrad | Doku - Minimum | Doku - Reifegrad |
|---|---|---|---|---|
| 1 - Organisation | 0% | 49% | 33% | 62% |
| 2 - Dokumentation und Zonen | 40% | 60% | 33% | 67% |
| 3 - Datenübertragung | 20% | 33% | 33% | 44% |
| 4 - Berechtigungsmanagement | 40% | 55% | 33% | 58% |
| 5 - Outsourcing & Fernadministr. | 40% | 56% | 33% | 60% |
| 6 - Schadsoftware & Schwachstellen | 40% | 56% | 33% | 47% |
| 7 - Wechseldatenträger & mobil | 20% | 50% | 33% | 50% |
| 8 - Komponentenlebenszyklus | 20% | 51% | 33% | 48% |
| 9 - IT-Störungsmanagement | 40% | 55% | 33% | 42% |
| 10 - Notfallplanung | 20% | 50% | 33% | 67% |
| 11 - Audit | 60% | 67% | 67% | 67% |
| Gesamtergebnis | 0% | 53% | 33% | 56% |

Der Wert Minimum gibt den niedrigsten erreichten Reifegrad je Bereich an. Hier liegt bei niedrigen
Als Faustregel gilt: Bei normalem Schutzbedarf sollte mindestens ein Reifegrad von 50% erreicht werden,

## Grafische Auswertung




**Über 52 Fragen in 11 Kategorien können Versorger ermitteln, in welchen Bereichen der größte Handlungsbedarf besteht.**

# Self Assessment Tool

# Handlungsempfehlungen

| Thema | Titel | Beschreibung | Handlungsempfehlungen | Dokumentationsvorschlag |
|---|---|---|---|---|
| 1 1 - Organisation | Verantwortung der Leitungsebene | Die Leitungsebene bekennt sich dazu, dass die Herstellung und Aufrechterhaltung der IT-Sicherheit ein relevantes Ziel beim Betrieb der kritischen Wasserinfrastruktur ist. | Die oberste Leitungsebene muss IT-Sicherheit als wesentlich erklären | IT-Sicherheits-Leitlinie |
| 2 1 - Organisation | Kenntnis der Vorgaben | Gesetzliche, regulatorische und sonstige besonderen Vorgaben für den ICS-Bereich sowie den Wassersektor sind bekannt und ihre Auswirkungen auf den Betreiber werden ausgewertet. | Kontakt zu relevanten behördlichen Stellen (BSI, ...); Liste mit allen Anforderungen mit jeweils Auswirkungen auf das Unternehmen, periodische Überarbeitung | Wir erabeiten generische Liste. - Arbeitsschutz, KontraG, ...) |
| 3 1 - Organisation | Verantwortlicher für IT-Sicherheit | Es ist ein Verantwortlicher (z.B. "IT-Sicherheitsbeauftragter") für die IT-Sicherheit im Automatisierungsbereich bestimmt und innerhalb der Organisation bekannt gemacht. | Leitungsebene benennt IT-Sicherheitsbeauftragten offiziell und macht diesen z. B. im Intranet bekannt | Wo? |
| 4 1 - Organisation | Kompetenz | Der IT-Sicherheitsbeauftragte verfügt über die Kompetenzen, IT-Bedrohungen und -Risiken im ICS-Bereich zu kennen, erkennen zu bewerten und geeignete Maßnahmen auszuwählen. | Der IT-Sicherheitsbeauftragte sollte einmal zu Beginn seiner Tätigkeit einen mindestens dreitägigen einschlägigen Kurs besuchen, wenn entsprechende Erfahrungen noch nicht vorhanden sind. Dieser sollte neben allgemeiner Informationssicherheit auch die Besonderheiten von Security im ICS-Bereich umfassen. Jährlich sollten Auffrischungen für neue Thematiken und Bedrohungen stattfinden. | Stellenbeschreibung des IT-Siche Fortbildungsplan |
| 5 1 - Organisation | Ressourcen | Der IT-Sicherheitsbeauftragte verfügt über ausreichend Ressourcen (zeitlich und finanziell), um die als notwendig erkannten und mit der Leitungsebene abgestimmten Maßnahmen umsetzen. | Das Management muss entprechend der Sicherheitsanforderungen bedarfsgerecht ein Budget sowie die notwendige Zeit für alle Beteiligten zur Verfügung stellen (in Höhe von mindestens 8-10% des IT-Budgets). | IT-Sicherheitsbudget und mittelfristi |
| 6 1 - Organisation | Dienstanweisungen | Der Umgang mit der Unternehmens-IT wird in Dienstanweisungen geregelt, welche den Mitarbeitern vermittelt werden. Neue Mitarbeiter werden in Aspekte der IT-Sicherheit eingeführt. | Die IT-Sicheheit sollte durch allgemeine Dienstanweisungen und spezielle objektbezogene Dienstanweisungen verbindlich gemacht werden. Sie enthalten ein Datum der Inkraftsetzung. Sie sollten den Mitarbeitern gegen Unterschrift ausgehändigt werden. Neue Mitarbeiter werden jeweils mit dem kompletten Set von Dienstanweisungen ausgestattet. | Dienstanweisungen sind im ggf. vorh Unternehmens zu dokumentieren, in aufzubewahren. |

**Aus den Antworten ergeben sich Handlungsbedarfe, welche in den Handlungsempfehlungen automatisiert ausgegeben und priorisiert werden.**

# Wirtschaftlichkeitsbetrachtung

# Verknüpfung mit Schnelltest und Handlungsempfehlungen

- Aus einer Vielzahl von Ansätzen zur Bewertung von Maßnahmen in der IT wird das „Konzept zur Durchführung von Wirtschaftlichkeitsbetrachtungen in der Bundesverwaltung, insbesondere beim Einsatz der IT“ (**WiBe 5.0**) bevorzugt
- Bestimmung der Vorteilhaftigkeit und des **wirtschaftlichen Profils der Maßnahme**
- Zwei Module:
  - **Kapitalwertbetrachtung:** alle Kosten- und Nutzengrößen, die monetär quantifizierbar sind (WiBe KW)
  - **Nutzwertbetrachtung:** qualitativ-strategischen Wirkungen der IT-Maßnahme (WiBe Q) und externen Effekte der IT-Maßnahme (WiBe E)
- Handlungsempfehlungen des Schnelltests und die Maßnahmen aus Berücksichtigung der Regelwerke werden den **Kategorien der WiBe zugeordnet.**

| 0 | 2 | 4 | 6 | 8 | 10 |
|---|---|---|---|---|---|
| Nicht von Bedeutung | Wichtig für einige Fachaufgaben, später | Wichtig für einige Fachaufgaben, zeitnah | Wichtig für alle Fachaufgaben, später | Wichtig für alle Fachaufgaben, zeitnah | Unabdingbar für die IT-Strategie der Behörde |

# Wirtschaftlichkeitsbetrachtung
# Umgang mit Ergebnissen

- fast immer ein **negativer Kapitalwert** der erforderlichen Maßnahmen (monetäre Belastungen sind ermittelbar, die monetäre Nutzen nur bewertbar)
- negativen Kapitalwert steht regelmäßig ein **positiver Nutzwert** entgegen (WiBe Q)

## Gesetzliche Verpflichtung

- Maßnahme ist zwingend durchzuführen
- WiBe Q – Bedeutung für die IT-Strategie wird mit 10 Punkten bewertet
- Bei kleinen und mittleren jedoch (noch) nicht der Fall

## Nutzwert über 50

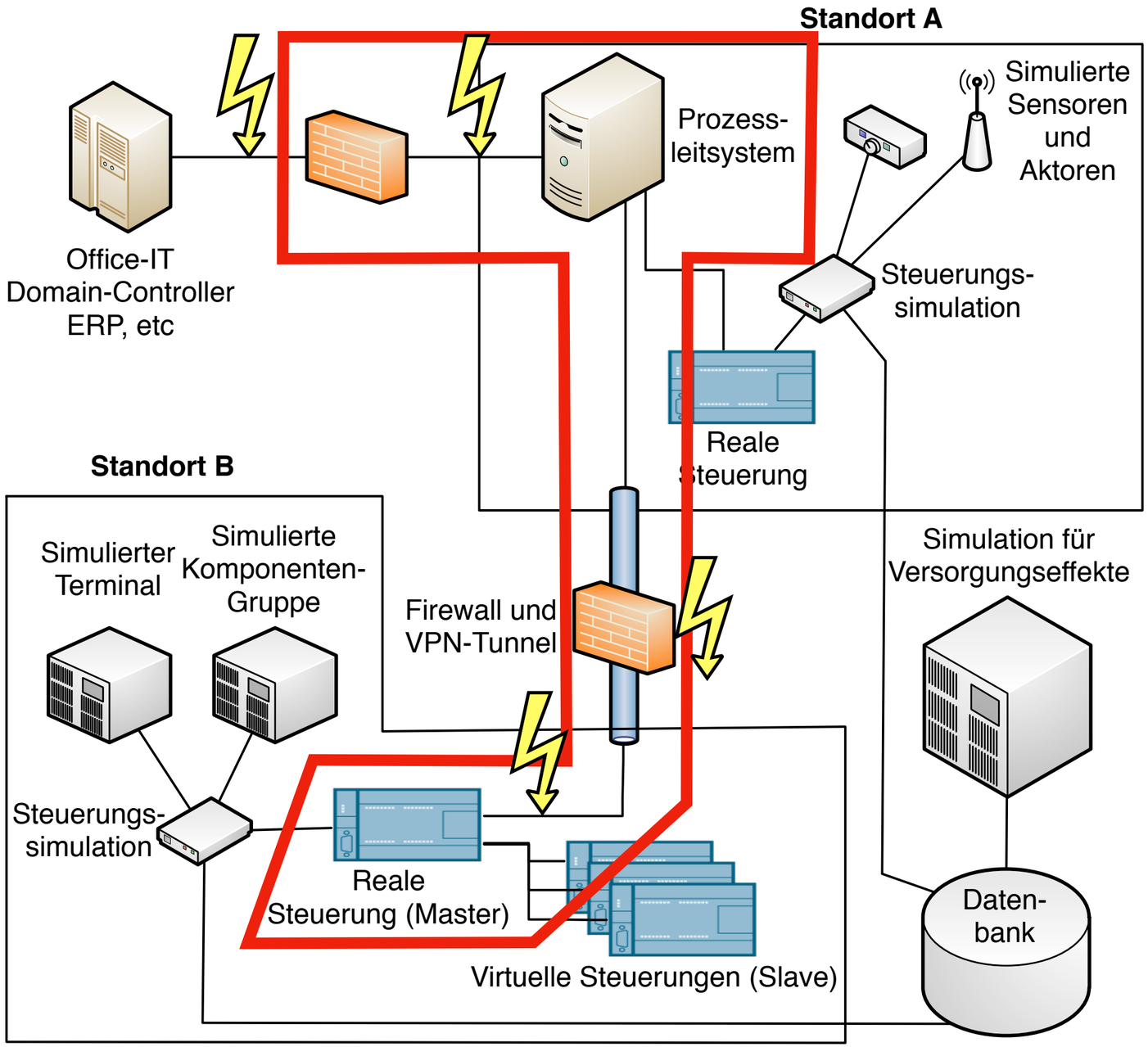
- Maßnahme kann durchgeführt werden
- Maßstab kann der **Quotient NW/KW** sein
- Je niedriger umso stärker wird Maßnahme präferiert
- Abarbeiten der Maßnahmen je nach Budgetdeckung

IT-Sicherheit in der Wasserversorgung

Wirtschaftliche Umsetzung von Schutzmaßnahmen

**Überprüfung der Sicherheit im Laborkontext**

# Angriffsszenario „Remotekommunikation zwischen Leitstelle und Wasserwerk“



# Vier Angriffspunkte innerhalb des Szenarios

### Angreifer innerhalb des Officenetzes

- Innentäterproblematik der Büromitarbeiter
- Überprüfung der Erreichbarkeit und Manipulationsmöglichkeiten

### Angreifer aus dem Internet

- Überprüfung der Konfiguration des VPN
- Auswertung der eingesetzten Komponenten

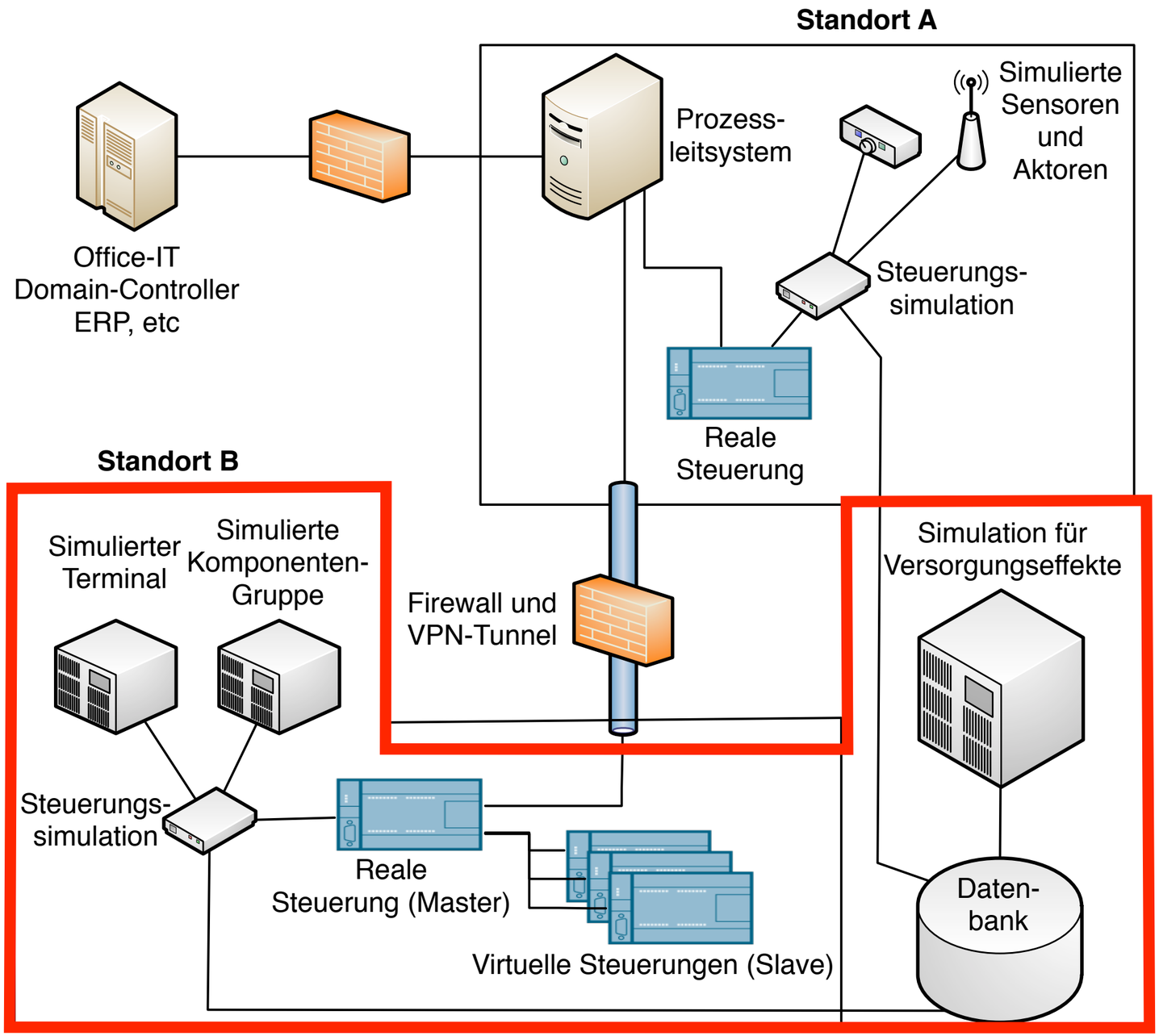
### Angreifer innerhalb des Wasserwerkes

- Auswertung des Zugriffs auf die SPS
- Überprüfung der Erreichbarkeit und Manipulationsmöglichkeiten

### Angriff innerhalb des Leitsystems

- Auswertung des Zugriffs auf das SCADA-System
- Überprüfung der Manipulationsmöglichkeiten

# Angriffsszenario „Kommunikationsmanipulation durch internen Angreifer“



# Mögliche Kommunikationsmanipulation durch internen Angreifer

## Replay-Angriffe

- Angreifer nimmt Kommunikation auf und spielt diese wieder
- Erlaubt Kommunikationsstörung auch ohne Protokollverständnis

## Man-in-the-Middle (MIM) Angriffe

- Angreifer befindet sich zwischen zwei Steuerunggeräten
- Manipuliert Datenverkehr zwischen den beiden Geräten
- Bsp: Manipulation einer Wasserstandsanzeige durch Veränderung der Füllstandwerte

## Denial/Degradation of Service (DoS) Angriffe

- Verzögern/Überlasten der Kommunikation zwischen Steuerungsgeräten
- Kann zu Ausfall kritischer Komponenten führen
- Hohes Schadenspotential bei kritischer Infrastruktur

## Authentication Bypass Angriffe

- PLCs in seltenen Fällen passwort-gesichert
- Angreifer lauscht auf Datenverkehr zur Authentisierung legitimer Netzteilnehmer
- Kann so erhaltenes Authentisierungstoken wiederverwenden

**Sobald ein Angreifer sich im internen Netz befindet, stehen ihm vielfältige Angriffsmöglichkeiten offen.**