Informationssicherheit bei Stadtwerken - Herausforderungen und Lösungen

TÜVRheinland®
Genau. Richtig.

Agenda

1. **Stadtwerke**
2. **Rechtliche Herausforderungen für Stadtwerke**
3. **ISMS als Lösung?!**
4. **Forschungsprojekt SIDATE**

TÜVRheinland®
Genau. Richtig.

Stadtwerke

Stadt- und Gemeindewerke (manchmal zusammengefasst unter dem Oberbegriff Kommunalwerke) sind kommunale Unternehmen (d. h. öffentliche oder gemischtwirtschaftliche Unternehmen im mehrheitlichen Besitz einer oder mehrerer Kommunen), die im öffentlichen Auftrag technische Dienstleistungen und Versorgungsleistungen, insbesondere im Bereich der Grundversorgung und der Daseinsvorsorge der Bevölkerung, erbringen oder kommunale Infrastruktur bereitstellen.

Leistungsspektrum

- Energieversorgung
- Wasserversorgung
- Entsorgung
- Infrastruktur
- Öffentlicher Verkehr

Große Heterogenität

- 100 – 10.000 MAs
- Lediglich Teilversorgung - Vollversorger

Quelle: Wikipedia

TÜVRheinland®
Genau. Richtig.

Agenda

1. **Stadtwerke**
2. **Rechtliche Herausforderungen für Stadtwerke**
3. **ISMS als Lösung?!**
4. **Forschungsprojekt SIDATE**

TÜVRheinland®
Genau. Richtig.

Anforderungen. Herausforderungen.

TÜVRheinland®
Genau. Richtig.

Herausforderung – Ziel des IT-Sicherheitsgesetzes

Das „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ hat zum Ziel eine **signifikante Verbesserung der Sicherheit informationstechnischer Systeme** (IT-Sicherheit) in Deutschland zu erreichen.

TÜVRheinland®
Genau. Richtig.

Herausforderung – Ziel des IT-Sicherheitsgesetzes

Das „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ hat zum Ziel eine **signifikante Verbesserung der Sicherheit informationstechnischer Systeme** (IT-Sicherheit) in Deutschland zu erreichen.

Der Schutz der Systeme soll im Hinblick auf die Schutzgüter der IT-Sicherheit

- **Verfügbarkeit,**
- **Integrität,**
- **Vertraulichkeit**
- und **Authentizität**

verbessert werden um den **aktuellen und zukünftigen Gefährdungen** der IT-Sicherheit wirksam begegnen zu können.

TÜVRheinland®
Genau. Richtig.

Herausforderung – Ziel des IT-Sicherheitsgesetzes

Das „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ hat zum Ziel eine **signifikante Verbesserung der Sicherheit informationstechnischer Systeme** (IT-Sicherheit) in Deutschland zu erreichen.

Der Schutz der Systeme soll im Hinblick auf die Schutzgüter der IT-Sicherheit

- **Verfügbarkeit,**
- **Integrität,**
- **Vertraulichkeit**
- und **Authentizität**

verbessert werden um den **aktuellen und zukünftigen Gefährdungen** der IT-Sicherheit wirksam begegnen zu können.

Ziel des Gesetzes ist die **Verbesserung der IT-Sicherheit von Unternehmen**, der verstärkte **Schutz der Bürgerinnen und Bürger im Internet** und in diesem Zusammenhang auch **die Stärkung von BSI und Bundeskriminalamt** (BKA).

TÜVRheinland®
Genau. Richtig.

Herausforderung – Ziel des IT-Sicherheitsgesetzes

Das „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ hat zum Ziel eine **signifikante Verbesserung der Sicherheit informationstechnischer Systeme** (IT-Sicherheit) in Deutschland zu erreichen.

Der Schutz der Systeme soll im Hinblick auf die Schutzgüter der IT-Sicherheit

- **Verfügbarkeit,**
- **Integrität,**
- **Vertraulichkeit**
- und **Authentizität**

verbessert werden um den **aktuellen und zukünftigen Gefährdungen** der IT-Sicherheit wirksam begegnen zu können.

Ziel des Gesetzes ist die **Verbesserung der IT-Sicherheit von Unternehmen**, der verstärkte **Schutz der Bürgerinnen und Bürger im Internet** und in diesem Zusammenhang auch **die Stärkung von BSI und Bundeskriminalamt** (BKA).

„**Besondere Bedeutung** kommt im Bereich der IT-Sicherheit denjenigen Infrastrukturen zu, die für das Funktionieren unseres Gemeinwesens zentral sind. Der Schutz der IT- Systeme von solchen **Kritischen Infrastrukturen** …“ [1]

TÜVRheinland®
Genau. Richtig.

Herausforderung – Ziel des IT-Sicherheitsgesetzes (steht im Einklang mit geplanter EU-Richtlinie)

Das „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ hat zum Ziel eine **signifikante Verbesserung der Sicherheit info[illegible]echnischer Systeme** (IT-Sicherheit) in Deutschland zu erreichen.

Der Schutz der Systeme soll im Hinblick auf die Schu[illegible]cherheit

- **Verfügbarkeit,**
- **Integrität,**
- **Vertraulichkeit**
- und **Authentizität**

verbessert werden um den **aktuellen und [illegible]gen** der IT-Sicherheit wirksam begegnen zu können.

Ziel des Gesetzes ist die **Ver[illegible] IT-Sicherheit von Unternehmen**, der verstärkte **Schutz der [illegible] und Bürger im Internet** und in diesem Zusammenhang auch [illegible] **BSI und Bundeskriminalamt** (BKA).

„**Besondere Bed[illegible]** [illegible]nt im Bereich der IT-Sicherheit denjenigen Infrastrukturen zu, die für das [illegible]ionieren unseres Gemeinwesens zentral sind. Der Schutz der IT- Systeme von solchen **Kritischen Infrastrukturen** …“ [1]

TÜVRheinland®
Genau. Richtig.

Herausforderung – Die Lösung

Lösung des Gesetzgebers:

„Defizite im Bereich der IT-Sicherheit sind abzubauen !“

TÜVRheinland®
Genau. Richtig.

Herausforderung – Anforderungen aus dem IT-SiG

Lösung des Gesetzgebers:

„Defizite im Bereich der IT-Sicherheit sind abzubauen. Insbesondere **Betreiber Kritischer Infrastrukturen** sind wegen der weitreichenden gesellschaftlichen Folgen, die ein Ausfall oder eine Beeinträchtigung ihrer Infrastrukturen nach sich ziehen kann, und ihrer insoweit besonderen Verantwortung für das Gemeinwohl zu verpflichten, ein **Mindestniveau an IT-Sicherheit einzuhalten** und dem **BSI IT-Sicherheitsvorfälle** zu **melden**. … Telekommunikationsanbieter, die eine Schlüsselrolle für die Sicherheit des Cyberraums haben, verpflichtet, **IT-Sicherheit nach dem Stand der Technik** nicht nur zum **Schutz des Fernmeldegeheimnisses** und **zum Schutz personenbezogener Daten**, sondern auch im Hinblick auf die **Verfügbarkeit ihrer Telekommunikations- und Datenverarbeitungssysteme zu gewährleisten**.“ [1]

TÜVRheinland®
Genau. Richtig.

Herausforderung – Anforderungen aus dem IT-SiG

Lösung des Gesetzgebers:

„Defizite im Bereich der IT-Sicherheit sind abzubauen. Insbesondere **Betreiber Kritischer Infrastrukturen** sind wegen der weitreichenden gesellschaftlichen Folgen, die ein Ausfall oder eine Beeinträchtigung ihrer Infrastrukturen nach sich ziehen kann, und ihrer insoweit besonderen Verantwortung für das Gemeinwohl zu verpflichten, ein **Mindestniveau an IT-Sicherheit einzuhalten** und dem **BSI IT-Sicherheitsvorfälle** zu **melden**. … Telekommunikationsanbieter, die eine Schlüsselrolle für die Sicherheit des Cyberraums haben, verpflichtet, **IT-Sicherheit nach dem Stand der Technik** nicht nur zum **Schutz des Fernmeldegeheimnisses** und **zum Schutz personenbezogener Daten**, sondern auch im Hinblick auf die **Verfügbarkeit ihrer Telekommunikations- und Datenverarbeitungssysteme zu gewährleisten**.“ [1]

Die Verfügbarkeit der ITK stellt somit eine erweiterte, bislang nicht vorhandene Anforderung durch den Gesetzgeber dar.

Hinzu kommt eine Meldepflicht ggü. dem BSI oder der BNetzA und Ansprechpartner bzw. Sicherheitsbeauftragte sind zu ernennen.

TÜVRheinland®
Genau. Richtig.

Herausforderung – Adressaten des IT-SiG

- **Änderung des BSI-Gesetzes**
- **Änderung des Energiewirtschaftsgesetzes**
- **Änderung des Atomgesetzes** **für SW nicht relevant**
- **Änderung des Telemediengesetzes**
- **Änderung des Telekommunikationsgesetzes**
- **Änderung des Bundesbesoldungsgesetzes** **für SW nicht relevant**
- **Änderung des Bundesbesoldungsgesetzes** **für SW nicht relevant**

TÜVRheinland®
Genau. Richtig.

Änderung des BSI-Gesetzes

- Das BSI wird zur nationalen Informationssicherheitsbehörde, §1 BSIG
- Das BSI bekommt erweiterte Befugnisse, insbesondere als „zentrale Meldestelle in Angelegenheiten der Sicherheit in der Informationstechnik“, §4 BSIG
- Begriffsbestimmung (Legal-Definition) „Kritischen Infrastrukturen“, §2 Abs. 10 BSIG
- Sektorspezifische Einordnung der „Kritischen Infrastrukturen“, §2 Abs. 10 BSIG
- Verweis auf eine Rechtsverordnung zur Konkretisierung, § 10 Abs.1 BSIG
- Verweis auf Zertifizierungspflicht über obige Rechtsverordnung, §9 BSIG

TÜVRheinland®
Genau. Richtig.

Herausforderung – Begriffsbestimmung „Kritischen Infrastrukturen“

„ §2 BSIG - Begriffsbestimmungen

….

(10) **Kritische Infrastrukturen** im Sinne dieses Gesetzes sind **Einrichtungen, Anlagen oder Teile davon**, die

1. den Sektoren **Energie**, **Informationstechnik** und **Telekommunikation**, **Transport und Verkehr**, **Gesundheit**, **Wasser**, **Ernährung** sowie **Finanz- und Versicherungswesen** angehören und

2. von **hoher Bedeutung für das Funktionieren des Gemeinwesens** sind, weil durch ihren Ausfall oder **ihre Beeinträchtigung erhebliche Versorgungsengpässe** oder Gefährdungen **für die öffentliche Sicherheit** eintreten würden.

Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 BSIG näher bestimmt.“

Gem. §10 BSIG werden durch das BMI per Rechtsverordnung der sog. „**Versorgungsgrad“** anhand **von branchenspezifischen Schwellenwerte** genau spezifiziert.

Dies erfolgt in Abstimmung mit der Wirtschaft, der Wissenschaft und der betroffenen Betreiber sowie weiterer.

TÜVRheinland®
Genau. Richtig.

Herausforderung – Normenkomplex der §8a, 8b und 8c BSIG

Der Normenkomplex der §8a,b,c BSIG hat einige Verwirrung gestiftet.

Wichtigste Erkenntnis:

§8c BSIG stellt Ausnahmen zum Anwendungsbereiches des BSIG (§8a,b) dar:

Kleinstunternehmen fallen nicht in den Anwendungsbereich:

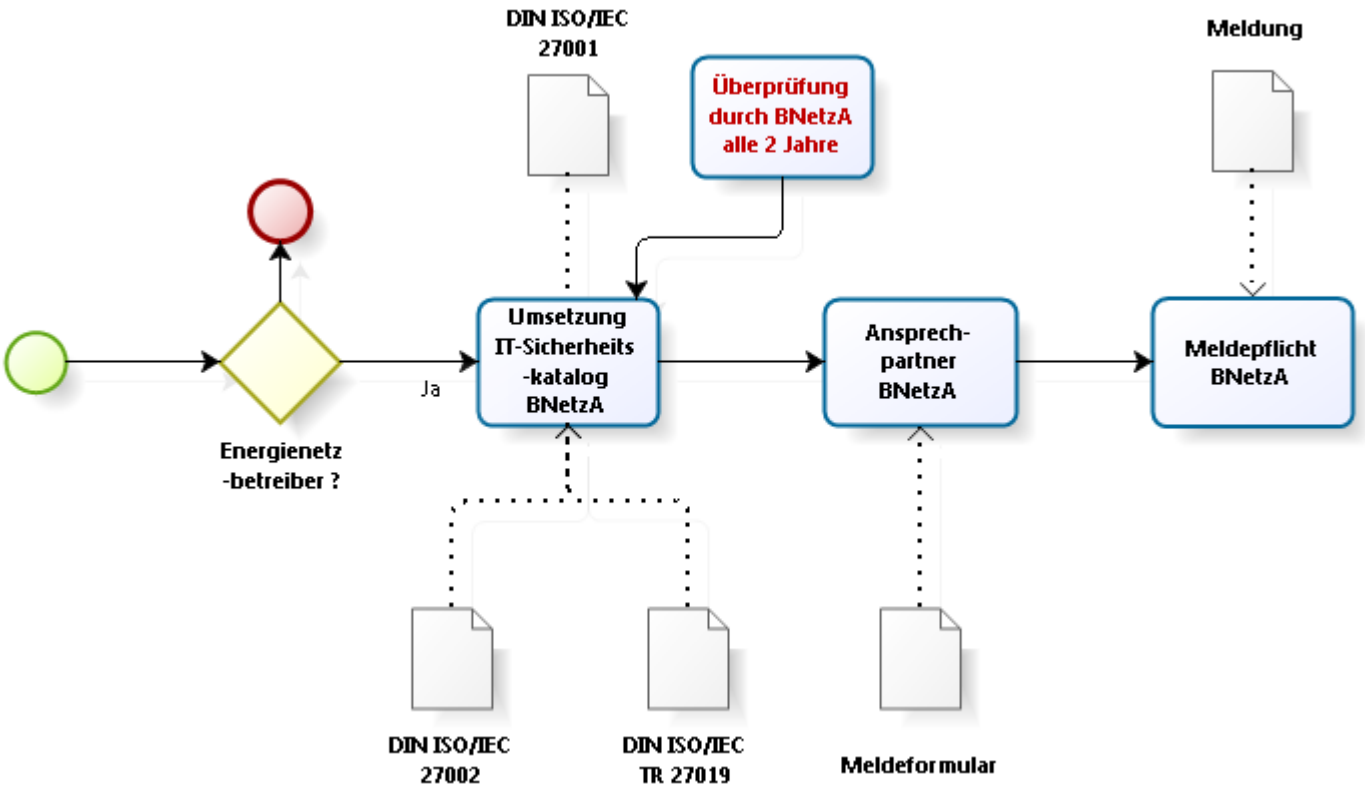
Kleinstunternehmen im Sinne der Empfehlung 2003/361/EC der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen [2]

- **weniger als 10 Personen beschäftigt**
- **und dessen Jahresumsatz bzw. Jahresbilanz 2 Mio. EUR nicht überschreitet.**

TÜVRheinland®
Genau. Richtig.

Herausforderung – Energienetzbetreiber IT-Sicherheitskatalog BNetzA

Netzbetreiber haben ein ISMS zu implementieren, das den Anforderungen der DIN ISO/IEC 27001 genügt. Es sind die Telekommunikations- und EDV-Systeme, die für einen sicheren Netzbetrieb notwendig sind zu berücksichtigen.



TÜVRheinland®
Genau. Richtig.

Herausforderung – Benennung Ansprechpartner IT-Sicherheit bzw. Sicherheitsbeauftragte (TKG KRITIS)

Offen ist Ansprechpartner oder Sicherheitsbeauftragter in der Energiebranche im Rahmen KRITIS ! Anders TKG, hier ist Sicherheitsbeauftragter notwendig !

- **IT-Sicherheitskatalog für Energienetzbetreiber fordert Ansprechpartner**
- **KRITIS TKG fordert Sicherheitsbeauftragten**
- **Ist nicht zu Vergleichen mit Datenschutzbeauftragten (BDSG), da keine persönliche Eignung gefordert und BNetzA hat keine Kontrollbefugnis**
- **Fachliche Eignung jedoch erforderlich**
- **Er muss durchzuführende Schutzmaßnahmen beurteilen können**
- **Ihm steht daher ggf. ein Recht auf umfassende Information über alle Sicherheitsrelevanten Vorgänge im Unternehmen zu**

TÜVRheinland®
Genau. Richtig.

Herausforderung – Benennung Ansprechpartner IT-Sicherheit bzw. Sicherheitsbeauftragte (TKG KRITIS)

Offen ist Ansprechpartner oder Sicherheitsbeauftragter in der Energiebranche im Rahmen KRITIS ! Anders TKG, hier ist Sicherheitsbeauftragter notwendig !

- **IT-Sicherheitskatalog für Energ[illegible] Ansprechpartner**
- **KRITIS TKG fordert Si[illegible]**
- **Ist nicht zu Verg[illegible] (BDSG), da keine persönliche [illegible] Kontrollbefugnis**
- **Fachliche [illegible]**
- **Er muss durchzuführen[illegible]utzmaßnahmen beurteilen können**
- **Ihm steht daher ggf. ein Recht auf umfassende Information über alle Sicherheitsrelevanten Vorgänge im Unternehmen zu**

Frist
Ansprechpartner IT-Scherheitskatalog
BNetzA gem. §11 Abs.1a EnWG
30.11.2015
Meldeformular bei BNetzA

TÜVRheinland®
Genau. Richtig.

Herausforderung – IT-Sicherheitskatalog Überblick

IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz

	IT-Sicherheitskatalog	Zertifizierung	Ansprechpartner IT-Sicherheit
Betreiber von Energieversorgungsnetzen	anwendbar	gefordert	BNetzA
Betreiber von Energieanlagen	nicht anwendbar	empfehlenswert	nicht erforderlich
Telekommunikations-netzbetreiber	nicht anwendbar	empfehlenswert	nicht erforderlich
Telemediendiensteanbieter	nicht anwendbar	empfehlenswert	nicht erforderlich

TÜVRheinland®
Genau. Richtig.

Herausforderung – IT-Sicherheitskatalog Überblick

IT-Sicherheitskatalog gemäß § 11 Absatz 1a En

	IT-S	Ansprechpartner IT-Sicherheit
Betreiber von Energieversorgungsnetz		**BNetzA**
Betreiber von Energieanlagen		**nicht erforderlich**
Telekommunikati treiber	**wert**	**nicht erforderlich**
Telemediendiens	**hlenswert**	**nicht erforderlich**

Frist 31.01.2018

Nachweis durch Vorlage des Zertifikats bei BNetzA

TÜVRheinland®
Genau. Richtig.

Aufwand – Überblick der Umsetzungsanforderungen

I. INFORMATIONSSICHERHEITS-MANAGEMENTSYSTEM

II. SICHERHEITSKATEGORIEN UND MAßNAHMEN

III. ORDNUNGSGEMÄßER BETRIEB DER BETROFFENEN ITKT-SYSTEME

IV. NETZSTRUKTURPLAN

V. RISIKOEINSCHÄTZUNG

VI. RISIKOBEHANDLUNG

VII. ANSPRECHPARTNER IT-SICHERHEIT

VIII. ZERTIFIZIERUNG

TÜVRheinland®
Genau. Richtig.

Agenda

1. **Stadtwerke**
2. **Rechtliche Herausforderungen für Stadtwerke**
3. **ISMS als Lösung?!**
4. **Forschungsprojekt SIDATE**

TÜVRheinland®
Genau. Richtig.

Informationssicherheitsmanagementsystem (ISMS)

Das Informationssicherheitsmanagementsystem wahrt die

- Vertraulichkeit,
- Integrität
- und Verfügbarkeit

von Informationen

unter Anwendung eines Risikomanagementprozesses

und verleiht interessierten Parteien

das Vertrauen in eine angemessene Steuerung von Risiken.

Das ISMS ist Teil der Abläufe einer Organisation

Quelle: DIN ISO/IEC 27001:2015-03

TÜVRheinland®
Genau. Richtig.

IS Management durch ein ISMS.

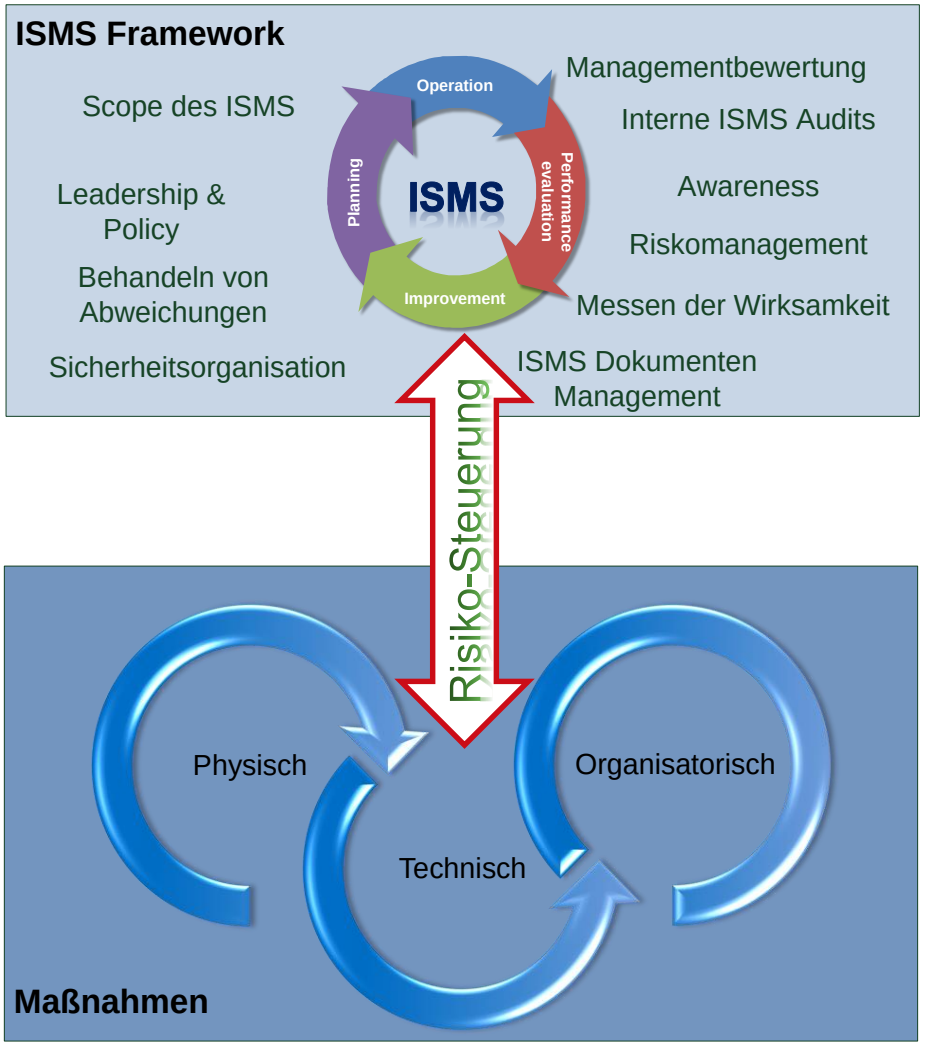
Organisation		ISMS
Management	Strategien, Planungen, Visionen	Management Commitment
Bereich Organisation	Prozesse, Rollen, Strukturen	Security Forum, Policies
Fachbereiche	Verfahren, Lösungen	Technische/Organisatorische Maßnahmen
Informationstechnik	Prozesse, Kommunikation, Daten	Technische/Organisatorische Maßnahmen
Infrastruktur-Technik	Gebäude, Infrastruktur	Technische Maßnahmen

Ca. 80% der Maßnahmen bei der Einführung eines ISMS sind organisatorischer Art!

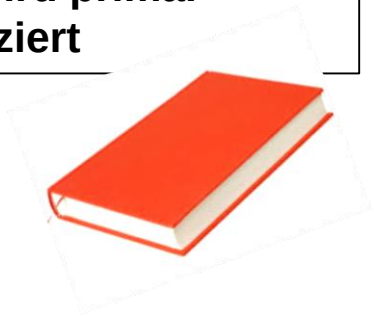
▲ Dienstleistung ▼ ISMS-Forderungen ▼ Betriebliche Anforderungen

TÜVRheinland®
Genau. Richtig.

Aufwand – Einführung Informationssicherheit-Managementsystem



- **ISO/IEC 27001**
- **Das ist das ISMS**
- **Das wird primär zertifiziert**



- **ISO/IEC 27001 Anh. A bzw. ISO/IEC 27002**
- **Weitere frei definierbare Maßnahmen z.B. ISO/IEC TR 27019, IT-Sicherheitskatalog BNetzA**

TÜVRheinland®
Genau. Richtig.

Aufwand – Informationssicherheit im Energiemanagement. Ein Lösungsansatz.

Strategische Ausrichtung

- Informationssicherheits-Managementsystem (ISMS)
  - Z.B. ISO 27001, IT-Grundschutz
  - Ergänzend: ISO 27019 oder ISO 27011 (Sektorspezifischen Normen)
- Richtlinien und Standardisierung (intern)
- Standards und Richtlinien für den Anlagenhersteller

Technische Maßnahmen

- Z.B. Segmentierung des IT-Netzes von Anlagen- oder Netzbetreibern
- Fernwartungskonzept
- Systemsicherheit durch Härtung
- Threat Management auf Perimeterebene

Organisatorische und Betriebliche Maßnahmen

- Verfahrens- und Arbeitsanweisungen
- Sicherheitsbewusstsein schaffen – Awareness
- Betriebsprozesse in Office- und Steuerungsumgebung synchronisieren
- Z.B. Berechtigungsmanagement, Patchmanagement, etc.

Zielsetzung: GANZHEITLICHE LÖSUNG.

TÜVRheinland®
Genau. Richtig.

Aufwand - Vorgehensmodell. Aufbau ISMS.

Evaluierung Ausgangssituation

- Zielsetzung / Motivation
- Vorgaben / Anforderungen (z.B. §11 Abs 1a EnWG, IT-Sicherheitsgesetz, Kooperationspartner)
- Grundlegende Definitionen
- Auswahl anzuwendender Standards (z.B. IT-GS, ISO27001, ISO27019)

Die Projekt-Planung

- Definition des Anwendungsbereiches
- Definition und Abgrenzung des Projektes
- Projektorganisation
- Definition der Aktivitäten
- Aufwandsschätzung

ISMS Konzeption

- Methodik und Dokumentation
- Sicherheits-Organisation (Rollen und Verantwortlichkeiten)
- Richtlinien und Anweisungswesen
- Maßnahmen-Management
- Berichtswesen

TÜVRheinland®
Genau. Richtig.

Aufwand - Vorgehensmodell. Aufbau ISMS.

Implementierung

- Transformation in Denken und Handeln
- Implementierung der Methoden
- Umsetzen von Maßnahmen
- Zielgruppenkonforme Kommunikation
- Sensibilisierung aller Mitarbeiter
- Regelmäßige Überprüfungen / Bewertungen

Regelbetrieb

- Fortlaufende Sensibilisierung aller Mitarbeiter
- Regelmäßige Umsetzung aller ISMS Aktivitäten
- Bewertung aller Aktivitäten und Ergebnisse
- Ableiten von Maßnahmen zu Verbesserung
- Ressourcenbereitstellung in allen betroffenen Bereichen

TÜVRheinland®
Genau. Richtig.

Aufwand – Risikoeinschätzung

Die Risikoeinschätzung hat sich an den **Schadenskategorien**

- „kritisch“ (die Schadensauswirkungen können ein existentiell bedrohliches,
- katastrophales Ausmaß erreichen),

- „hoch“ (die Schadensauswirkungen können beträchtlich sein) und

- „mäßig“ (die Schadensauswirkungen sind begrenzt und überschaubar)

zu orientieren.

Für die Komponenten, Systeme und Anwendungen, die für einen sicheren Netzbetrieb notwendig sind, ist **grundsätzlich von einer Einstufung** in die Kategorie „**hoch**“ auszugehen.

Eine vom Grundsatz abweichende Einstufung als „mäßig“ ist ausführlich zu begründen und zu dokumentieren.

TÜVRheinland®
Genau. Richtig.

Aufwand – Risikoeinschätzung

Bei der Einstufung in die **Schadenskategorien** sind durch den Netzbetreiber mindestens die folgenden Kriterien zu berücksichtigen:

- Beeinträchtigung der Versorgungssicherheit,
- Einschränkung des Energieflusses,
- Betroffener Bevölkerungsanteil,
- Gefährdung für Leib und Leben,
- Auswirkungen auf weitere Infrastrukturen (z. B. vor- und nachgelagerte Netzbetreiber, Wasserversorgung),
- Gefährdung für Datensicherheit und Datenschutz durch Offenlegung oder Manipulation,
- Finanzielle Auswirkungen.

TÜVRheinland®
Genau. Richtig.

Aufwand – Risikoeinschätzung - Ursachen

vorsätzliche Gefährdungen

- **Gezielte IT-Angriffe,**
- **Computer-Viren, Schadsoftware,**
- **Abhören der Kommunikation,**
- **Diebstahl von Rechnern usw.**

nicht vorsätzliche Gefährdungen

- **Elementare Gefährdungen,**
- **Höhere Gewalt,**
- **Organisatorische Mängel,**
- **Menschliche Fehlhandlungen,**
- **Technisches Versagen,**
- **Versagen oder Beeinträchtigung anderer für die Netzsteuerung relevanter Infrastrukturen und externer Dienstleistungen,**
- **Ungezielte Angriffe und Irrläufer von Schadsoftware.**

TÜVRheinland®
Genau. Richtig.

Aufwand - Kernfragen. Aufbau Managemensystem.

Der Schwarzfall als SuperGAU

- Was sind meine Kernprozesse?
- Was ist mein Schutzbedarf?
- Was sind die wirklichen Bedrohungen?
- Wer greift mich an?
- Wo sind meine Schwachstellen?
- Wie hoch ist die Gefahr?
- Wie können Risiken bewertet werden?
- Welcher Schaden kann entstehen?
- Wie können entsprechende Gegenmaßnahmen abgeleitet werden?

TÜVRheinland®
Genau. Richtig.

Aufwand - Netzstrukturpläne

Der Netzbetreiber hat eine Übersicht über die vom Geltungsbereich des IT-Sicherheitskatalogs betroffenen Anwendungen, Systeme und Komponenten mit den anzutreffenden Haupttechnologien und deren Verbindungen zu erstellen.

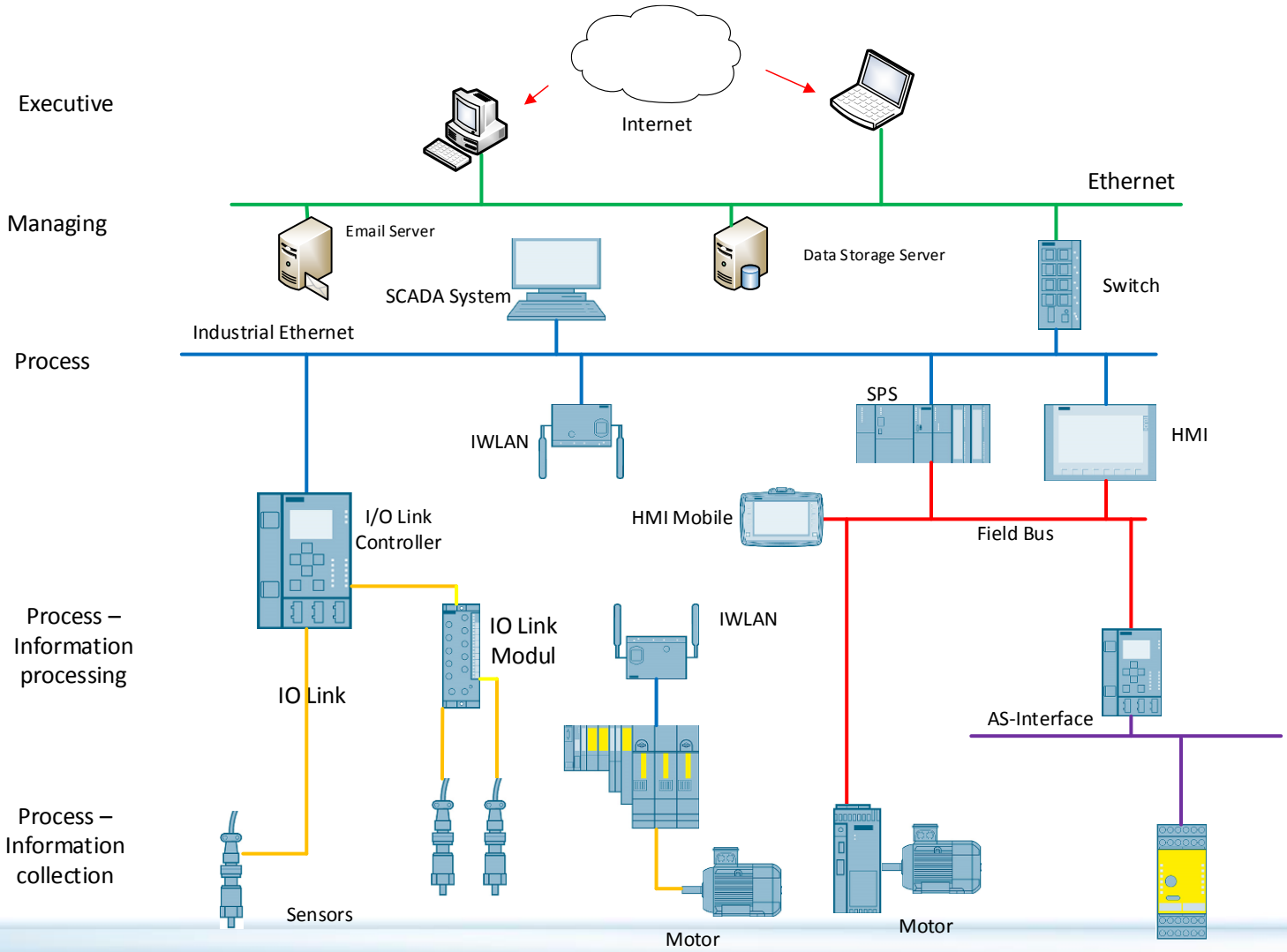
Die Übersicht ist nach den Technologiekategorien

- **Leitsysteme und Systembetrieb**
- **Übertragungstechnik/Kommunikation**
- **Sekundär-, Automatisierungs- und Fernwirktechnik**

zu unterscheiden

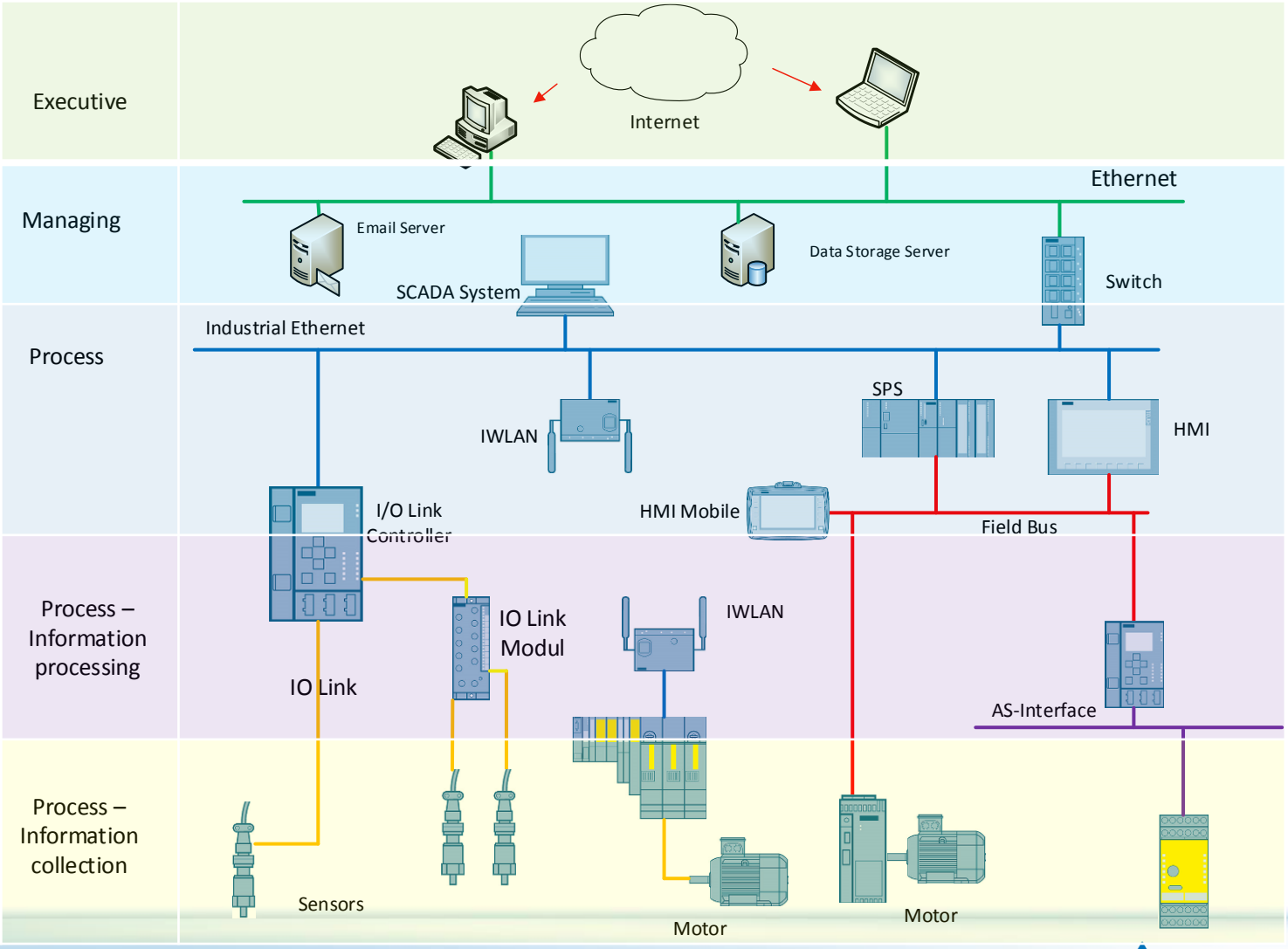
TÜVRheinland®
Genau. Richtig.

Aufwand – Beispiel Netzstrukturpläne



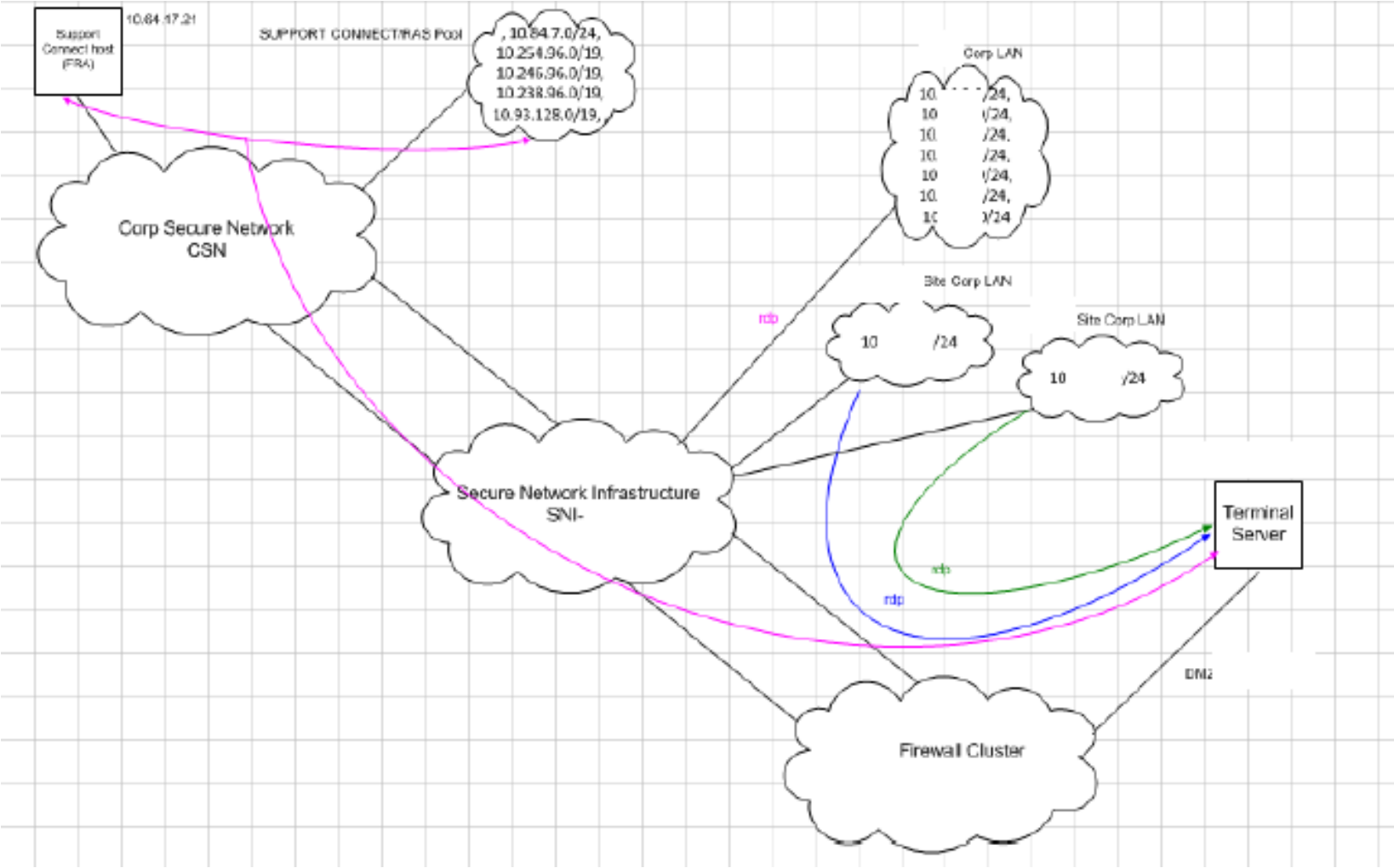
TÜVRheinland®
Genau. Richtig.

Aufwand - Beispiel Netzstrukturpläne (Betriebshoheiten)



TÜVRheinland®
Genau. Richtig.

Aufwand - Beispiel Netzstrukturpläne (Kommunikationsnetze ITK)



TÜVRheinland®
Genau. Richtig.

Aufwand – Risikobehandlung

- **Auswahl geeigneter und angemessener Maßnahmen nach erfolgter Risikoabschätzung.**

- **Maßnahmen der ISO TR 27019 sind zwingend umzusetzen**

- **Bei der Angemessenheit einer Maßnahme ist insbesondere deren technischer und wirtschaftlicher Aufwand zu berücksichtigen. Dieser sollte nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung des sicheren Netzbetriebs stehen.**

TÜVRheinland®
Genau. Richtig.

Aufwand – Risikobehandlung

- **Auswahl geeigneter und angemessener Maßnahmen nach erfolgter Risikoabschätzung.**

- **Maßnahmen der ISO TR 27019 sind zwingend umzusetzen**

- **Bei der Angemessenheit einer Maßnahme ist insbesondere deren technischer und wirtschaftlicher Aufwand zu berücksichtigen. Dieser sollte nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung des sicheren Netzbetriebs stehen.**

Fazit:

Abzuwägen ist der Aufwand in Bezug zur Beeinträchtigung der Öffentlichkeit

TÜVRheinland®
Genau. Richtig.

Aufwand – Ansprechpartner IT-Sicherheit

- **Nennung des Ansprechpartners und Vertreters bei der BNetzA**
- **Einbindung des Ansprechpartners in den betrieblichen Ablauf des Netzbetriebes (Unverzüglichkeit)**
- **Fachliche Expertise gefordert**
- **Aussagefähigkeit kann nur gegeben sein, wenn dokumentierte Prozesse und Verfahren existieren**
- **Berichtswesen erforderlich**
- **Incident-Management muss etabliert sein (Grundvoraussetzung ISO 27001)**
- **Fungiert als Treiber und steuert / koordiniert den Regelbetrieb**

TÜVRheinland®
Genau. Richtig.

Aufwand – Zertifizierung

- **Zertifizierungsvorgaben befinden sich derzeit in der Abstimmung zwischen BNetzA und der DAAKS (deutsche Akkreditierungsstelle)**

- **Unabhängige Zertifizierung gefordert (Trennung Beratung / Zertifizierung)**

- **Netzbetreiber der Bundesnetzagentur bis zum 31.01.2018 den Abschluss des Zertifizierungsverfahrens durch Vorlage einer Kopie des Zertifikats mitzuteilen.**

- **Aufwende für Zertifizierung hängen von der Größe der Personen im Anwendungsbereich ab, der Anzahl der Standorte und Anzahl der zu betrachtenden ITK Systeme**

TÜVRheinland®
Genau. Richtig.

Aufwand – Nutzen für die Öffentlichkeit

- **Erhöhung der Versorgungssicherheit ?**
- **Steigerung des öffentlichen Vertrauen in die Daseinsvorsorge durch den Staat ?**
- **Ist der öffentliche Nutzen tatsächlich sichtbar oder Messbar ?**

TÜVRheinland®
Genau. Richtig.

Aufwand – Nutzen für die Stadtwerke

- **ISMS als Governance-Instrument zur Resourcen- und Investitionsentscheidung**
- **Bessere Planbarkeit anstehender Investitionen**
- **Transparenz der Kosten des IT-Betriebs**
- **Definierte Geschäfts- und IT-Prozesse**
- **Haftungsminimierung durch Zertifizierung „… Ein angemessener Schutz des Betriebs von Energieanlagen im Sinne von Satz 1 liegt vor…“**

TÜVRheinland®
Genau. Richtig.

Agenda

1. **Stadtwerke**
2. **Rechtliche Herausforderungen für Stadtwerke**
3. **ISMS als Lösung?!**
4. **Forschungsprojekt SIDATE**

TÜVRheinland®
Genau. Richtig.

Förderlinie IT-Sicherheit für Kritische Infrastrukturen

cklu thoden und Werkzeugen für eine
e Ab der lebenswichtigen IT-Systeme,
das ngsleistungen, die über kritische
Infrastrukturen e rden, jederzeit garantiert werden können.“

AQUA-IT-Lab	Cyber-Safe	INDI	ITS.APT
MoSaIK	PREVENT	RiskViz	SecMaaS
SICIA	SIDATE	SURF	VeSiKi

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

TÜVRheinland®
Genau. Richtig.

SIDATE Forschungsprojekt

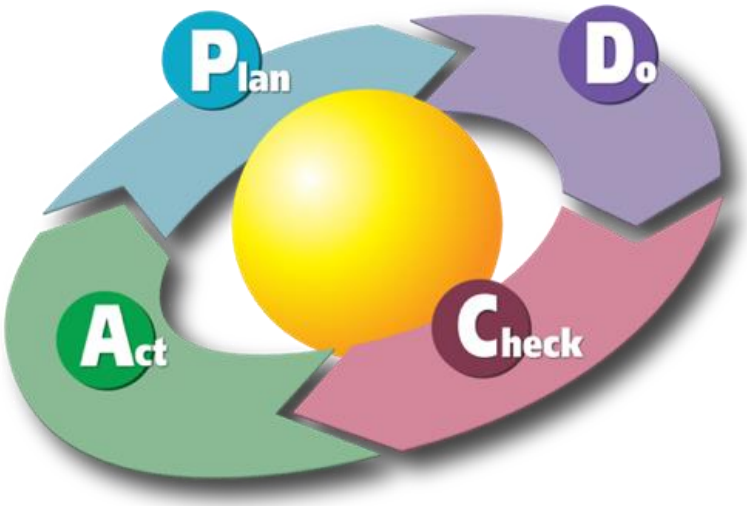
Sichere Informationsnetze
bei kleinen und mittleren Energieversorgern

technische Unterstützung kleiner und mittelgroßer Energieversorger (z.B. Stadtwerke) bei der Verbesserung ihrer IT-Sicherheit.

Laufzeit: 08/2015 – 07/2018

Problemstellung

- Standardkonformes ISMS sehr komplex
- Anforderungen insbesondere für kleine und mittelgroße Netzbetreiber sehr hoch
  - Kleine IT-Abteilungen
  - Begrenzte personelle und finanzielle Ressourcen
  - Fehlende Qualifikation
  - Herausforderungen bei der Risikoanalyse und Auswahl geeigneter Maßnahmen



TÜVRheinland®
Genau. Richtig.

Projektziel

Das Projekt setzt sich zum Ziel, kleine und mittlere Energieversorger in die Lage zu versetzen **Risiken** hinsichtlich der Sicherheit ihrer IT-Infrastruktur **selbst zu identifizieren** zu **analysieren und zu bewerten**, sowie die **Nützlichkeit**, **Anwendbarkeit** und **Wirtschaftlichkeit** möglicher Lösungsalternativen **einzuschätzen**. Die Kernidee ist die Identifikation und nachhaltige Verfolgung technischer und organisatorischer Schwachstellen und zugehöriger Gegenmaßnahmen.

TÜVRheinland®
Genau. Richtig.

Projektkonsortium

TÜVRheinland® Genau. Richtig.

Forschungsinhalte

Analyse und Bewertung

Entwicklung von **Werkzeugen**, die Stadtwerke dabei unterstützen **das eigene Sicherheitsniveau selbst zu analysieren und zu bewerten**.

- Laufen Sicherheits-Maßnahmen effektiv?
- Wo besteht akuter Handlungsbedarf? (z.B. Softwareupdates)
- Wo stehe ich im Vergleich zu anderen Netzbetreibern (Benchmarking)?
- Welche weiteren Maßnahmen sollten geplant und eingeführt werden?

TÜVRheinland®
Genau. Richtig.

Analyse und Bewertung

Entwicklung von **Werkzeugen**, die Stadtwerke bei der **Auswahl geeigneter Sicherheitsmaßnahmen unterstützen**

- Welche Auswirkung hat eine Maßnahme auf das eigene Sicherheitsniveau?
  - Mit welchen Kosten ist eine Maßnahme verbunden?
    - Anschaffung, Wartung, Personal, Schulungen ...
- Welche Auswirkungen hat eine Maßnahme für die Arbeitspraxis in meinem Unternehmen? Werden Mitarbeiter in Ihrer Arbeitsweise beeinträchtigt?

→ Welche Maßnahme bietet die optimale Balance zwischen diesen Kategorien

TÜVRheinland®
Genau. Richtig.

Kooperation und Wissensaustausch

Entwicklung einer **Kooperationplattform** für Energienetzbetreiber für eine nachhaltige, organisationsübergreifende Verbesserung des IT-Sicherheitsniveaus

- gegenseitige Information zu sicherheitskritischen Vorfällen und identifizierten Schwachstellen
- Gemeinsame Ausarbeitung neuer Best-Practice Sammlungen
- Sensibilisierung für das Thema IT-Sicherheit und neue Bedrohungspotentiale
- Einbeziehung externer Experten für kosteneffiziente Unterstützungs- und Beratungsleistungen

TÜVRheinland®
Genau. Richtig.

SIDATE Portal

https://portal.sidate.org

SIDATE

Questions & Answers

filtered by: isms, network

Best | New

- Questions & Answers
- Security Assessment
- Security Measures

Should our office network be in the scope of our ISMS?
Tags: isms, network
Controls: Compliance, Communications and Operations Mgmt.

Automatically generate and/or update network topology map? ✔
Tags: isms, network, software
Controls: Compliance, Communications and Operations Mgmt.

Are backup-servers in the scope of the IT-Security catalogue? ✔
Tags: isms, network, server
Controls: Compliance

Ask a Question

Tags

software, asset-management, isms, network, server, legal, it-security commissioner

Controls

Security Policy, Asset Management, Info. Security Organization, Compliance, HR Security, Access Control, Physical and Environmental Security, Communications and Operations Mgmt., IS Acquisition, Development & Maintenance, Information Security Incident Mgmt., Business Continuity Management

TÜVRheinland®
Genau. Richtig.

SIDATE Portal

https://portal.sidate.org

SIDATE

Questions & Answers

Security Assessment

Security Measures

Security Assessment ▸ Management of IT-Security Incidents

Do you have an information security emergency plan?

- ◉ Yes
- ○ No
- ○ I do not know

Previous Question | Next Question

More on this topic

Top Questions asked by the Community

1. Are there any guidelines on how to create an emergency plan?
2. Which aspects should an IT security emergency plan address?
3. Is it really necessary to have an emergency plan?

How other people have answered this question

- Yes: 61%
- No: 28%
- I do not know: 11%

TÜVRheinland®
Genau. Richtig.

SIDATE Portal

https://portal.sidate.org

SIDATE

Questions & Answers

Security Assessment

Security Measures

Security Measures ▸ Network segmentation

An ICS network should consist of several network segments with individual protection requirements. The data traffic between the different levels (see 3) should be limited to the operationally required extent by means of data flow control, e.g. firewall.

If the protection requirements are correspondingly high, a demilitarised zone (DMZ) should be included between the production management and the operational/process management. A DMZ is an intermediate network located between the Intranet and the Internet, but not included in either network. It is a separate network not protected as strongly as the network actually to be protected. It consists of two physically separated firewalls and an application level gateway. Proxy services with filtering options up to layer 7 should control and monitor the data traffic.

In addition to the network segmentation with different functionalities (for vertical integration, see 1), networks at all geographic sites or generally organisationally independent machines/plants should also be segmented among each other (for horizontal integration, see 2). This prevents, for example, malware from spreading to all machines in an unhindered manner. The connection should always be established from the network segment with the higher protection requirements into the network segment with the lower

Ratings

Efficacy ★★★★☆

Usability ★★☆☆☆

Cost ★★☆☆☆

Overall Rating ★★★★☆

Tags

network

Controls

Communications and Operations Mgmt.

This is one of the most important network security measures. It was hard to change our existing network topolgy to accomplish a physical segmentation though.

Posted 2016-02-22

Overall Rating ★★★★☆

Jane Doe

Stadtwerke Musterstadt

Write a Comment

TÜVRheinland®
Genau. Richtig.

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Regelmäßig aktuelle Informationen im
Newsletter und unter **www.tuv.com/informationssicherheit**

TÜVRheinland®
Genau. Richtig.