Anlage 2

Anforderungen an die IT-Sicherheit bei den Stadtwerken Norderstedt und wilhelm.tel

IT-Sicherheit und Datenschutz bei den Stadtwerken

Bislang wurden unterschiedliche Compliance-Anforderungen aus verschiedenen Gesetzen wie

- Bundesdatenschutzgesetz (BDSG),
- Telekommunikationsgesetz (TKG),
- Telemediengesetz (TMG) usw.

betrachtet. Dies führte zur Umsetzung einer Reihe von Maßnahmen:

- Bestellung eines Datenschutzbeauftragten,
- Durchführung von Schulungen zu Datenschutz und IT-Sicherheit,
- Erstellung von Sicherheitsrichtlinien,
- Erstellung der Verfahrensübersicht usw.

Darüber hinaus wurden eine Reihe von Anforderungen aufgrund von Kundenwünschen umgesetzt, z.B. im Rechenzentrum.

→ Bislang aber keine Umsetzung eines

Information Security Management System (ISMS)

als Voraussetzung für eine mögliche Zertifizierung.

Aktuelle Anforderungen an die IT-Sicherheit

Smart Meter Gateway Administrator wie in §21 ff EnWG gefordert:

- Umsetzung der technischen Richtlinie **BSI TR 03109-1**
- Umsetzung des BSI Grundschutzkataloges
- Zertifizierung nach BSI **ISO 27001 Grundschutz**

Entwurf der BNetzA zum Sicherheitskatalog gem. §11a ENWG:

- Umsetzung eines ISMS nach DIN ISO/IEC 27001 für den Netzbetrieb
- Zertifizierung des ISMS durch eine unabhängige Zertifizierungsstelle

Anforderungen aus KRITIS

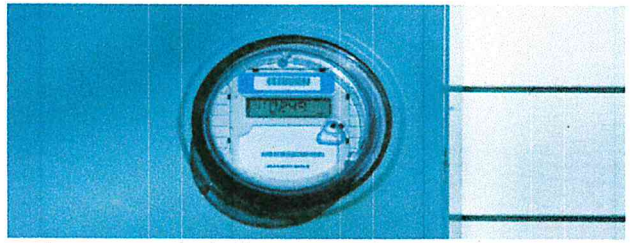
(Nationale Strategie zum Schutz Kritischer Infrastrukturen)

Anforderungen an den Betrieb des Rechenzentrums

- Zertifizierung als Wettbewerbsvorteil
- Zertifizierung als Voraussetzung zum Betrieb ?

Aktuelle Anforderungen an die IT-Sicherheit

Smart Meter Gateway Administrator



in der technischen Richtlinie TR 03109-1 des BSI heißt es:

„Der SMGW-Admin MUSS ein ISMS nach [ISO 27001] implementieren, betreiben und dokumentieren. Ergänzend dazu MUSS [DIN 27009, ISO/IEC TR 27019] „Leitfaden für das Informationssicherheits-Management von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002“ berücksichtigt werden, soweit die dort genannten Maßnahmen (Controls) auf die Aufgaben und Betriebsprozesse des SMGW-Admins anwendbar sind.

Zur Erfüllung der vorgenannten Anforderungen MUSS der IT-Grundschutz verwendet werden. Grundlage dafür ist der BSI Standard 100. Der Standard [BSI 100-1] KANN unterstützend zu [ISO 42 27001] zum Aufbau des ISMS herangezogen werden. Die IT-Grundschutz-Vorgehensweise nach [BSI 100-2] sowie die [IT-GS Kataloge] MÜSSEN angewendet werden. Für Risikoanalysen KANN die Methodik nach [BSI 100-3] verwendet werden.“

Wer muss zertifiziert werden ?

- Eine mögliche Betreibergesellschaft der IVU, DNMG, DZG und ggf. Stadtwerke Norderstedt?
- Der Rechenzentrumsdienstleister (Stadtwerke Norderstedt ?)
- die Gesellschafter des Betreibers ?
- eventuelle Unterauftragnehmer ?

Aktuelle Anforderungen an die IT-Sicherheit

Entwurf der BNetzA zum Sicherheitskatalog gem. §11 Abs. 1a ENWG:

„Der Betrieb eines sicheren Energieversorgungsnetzes umfasst insbesondere auch einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die der Netzsteuerung dienen. Die Regulierungsbehörde erstellt hierzu im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik einen Katalog von Sicherheitsanforderungen und veröffentlicht diesen. Ein angemessener Schutz des Betriebs eines Energieversorgungsnetzes wird vermutet, wenn dieser Katalog der Sicherheitsanforderungen eingehalten und dies vom Betreiber dokumentiert worden ist."

<u>Konkret heißt dies nach derzeitigem Entwurf:</u>

- Umsetzung eines ISMS nach DIN ISO/IEC 27001 für den Netzbetrieb
- Umsetzung der DIN ISO/IEC 27002 (Leitfaden für das Informationssicherheits-Management)
- Umsetzung der DIN SPEC 27009 (Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002)
- Zertifizierung des ISMS durch eine unabhängige Zertifizierungsstelle

Aktuelle Anforderungen an die IT-Sicherheit

KRITIS: Nationale Strategie zum Schutz Kritischer Infrastrukturen

Infrastrukturen gelten dann als „kritisch", wenn sie für die Funktionsfähigkeit moderner Gesellschaften von wichtiger Bedeutung sind und ihr Ausfall oder ihre Beeinträchtigung nachhaltige Störungen im Gesamtsystem zur Folge hat.

Dies betrifft die technische Basisinfrastrukturen

- Energieversorgung
- Informations- und Kommunikationstechnologie
- Transport und Verkehr
- (Trink-) Wasserversorgung und Abwasserentsorgung

Gefordert wird von Unternehmen insbesondere die Erarbeitung von Schutzkonzepten unter Berücksichtigung geltender Standards, Normen und Regelwerke (z.B. die BSI-Standards zur Informationssicherheit als grundlegende Handlungsempfehlung für Betreiber kritischer Infrastrukturen oder das Regelwerk des DVGW zum Risikomanagement im Bereich der Trinkwasserversorgung).

Information Security Management Systeme

Das **Information Security Management System** (**ISMS**, engl. für „Managementsystem für Informationssicherheit“) ist eine Aufstellung von Verfahren und Regeln innerhalb eines Unternehmens, welche dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

Verschiedene Normen:

- BSI Grundschutz nach ISO 27001 Standards 100-1, 100-2, 100-3 und 100-4
- DIN ISO/IEC 27001 in Verbindung mit DIN ISO/IEC 27002 und DIN SPEC 27009
- COBIT: *(Control Objectives for Information and Related Technology)* ist das international anerkannte Framework zur IT-Governance und gliedert die Aufgaben der IT in Prozesse und Kontrollziele)
- PCI-DSS: Der Payment Card Industry Data Security Standard, ist ein Regelwerk im Zahlungsverkehr, das sich auf die Abwicklung von Kreditkartentransaktionen bezieht und von allen wichtigen Kreditkartenorganisationen unterstützt wird.

Die Normenfamilie ISO/IEC 270xx

Die internationale Norm **ISO/IEC 27001** *Informationstechnik– IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen* spezifiziert die Anforderungen für

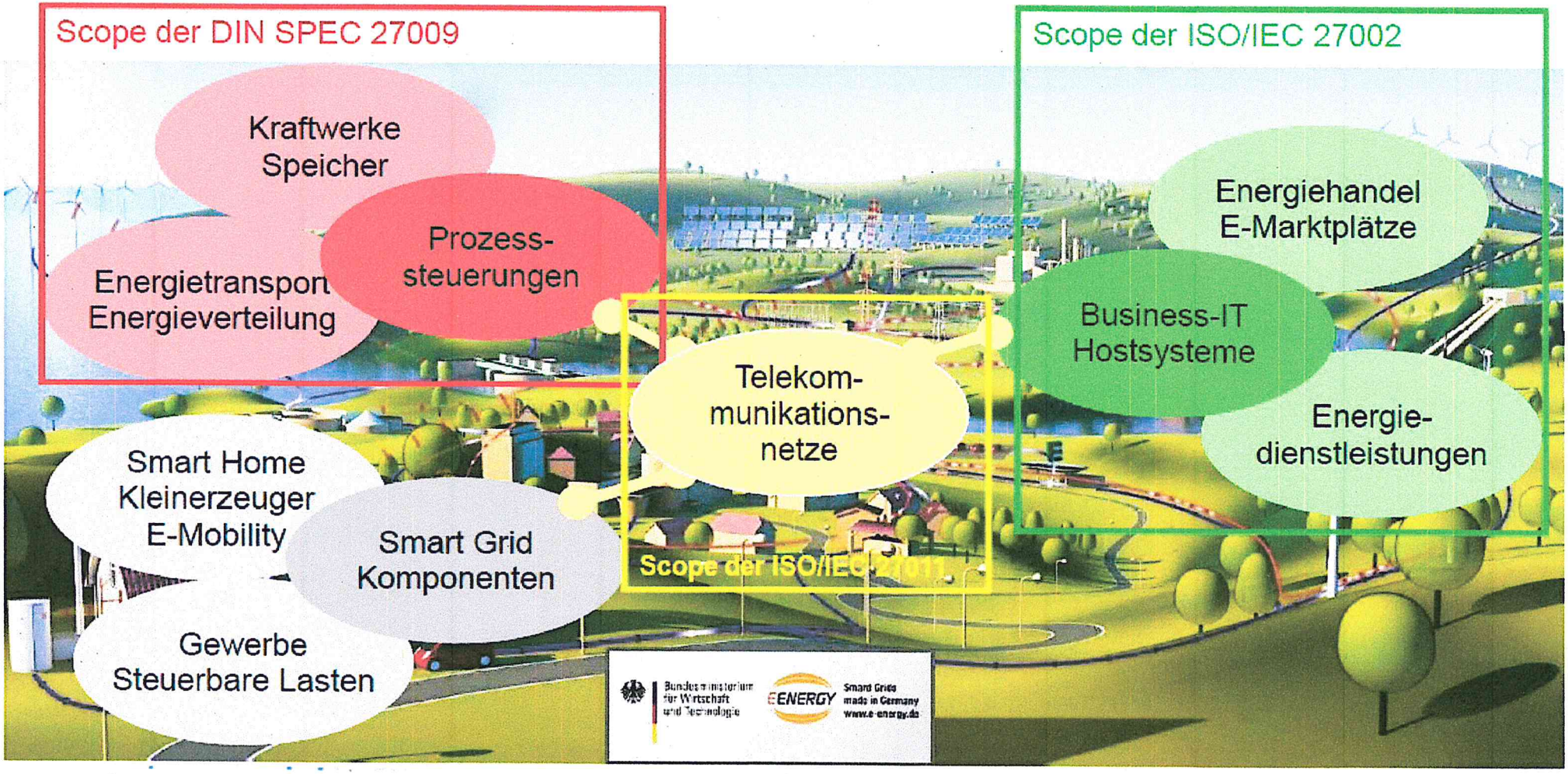
- Herstellung, Einführung, Betrieb,
- Überwachung, Wartung und
- Verbesserung

eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung der IT-Risiken innerhalb der gesamten Organisation.

Die **ISO/IEC 27002** ist ein internationaler Standard, der Empfehlungen für diverse Kontrollmechanismen für die Informationssicherheit beinhaltet. Dabei geht es um Sicherheit gegen Angriffe. Eine Zertifizierung nach ISO/IEC 27002 ist grundsätzlich nicht möglich, da es sich bei der Norm um eine Sammlung von Vorschlägen und nicht Forderungen handelt. Soll ein Informationssicherheitsmanagementsystem (ISMS) zertifiziert werden, ist dies nur über die Erfüllung der Anforderungen nach ISO/IEC 27001 möglich.

Die **DIN SPEC 27009:2012-04** ist ein Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002.

Zuordnung der verschieden Normen ISO 270xx



Aufbau eines ISMS (1)

Zu einem ISMS gehören folgende grundlegende Komponenten

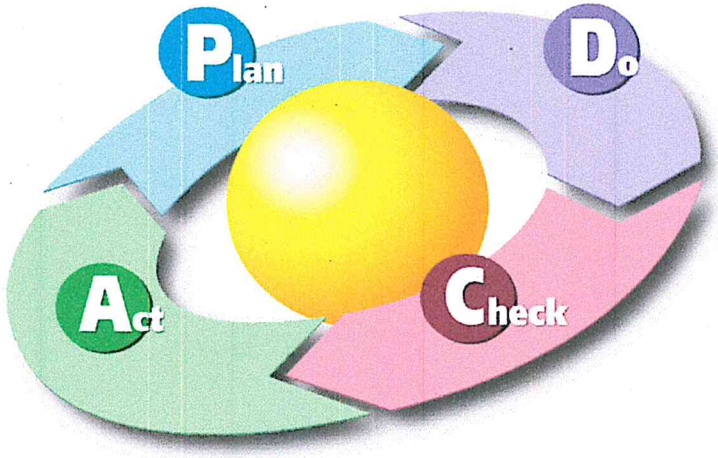
- Management-Prinzipien
- Ressourcen
- Mitarbeiter
- Sicherheitsprozess
  - Leitlinie zur Informationssicherheit, in der die Sicherheitsziele und die Strategie zu ihrer Umsetzung dokumentiert sind
  - Sicherheitskonzept
  - Informationssicherheitsorganisation

→ Eine wesentliche Funktion beim Aufbau und Betrieb eines ISMS kommt dem IT-Sicherheitsbeauftragten zu.

Aufbau eines ISMS (2)

Prozessbeschreibung und Lebenszyklus-Modell

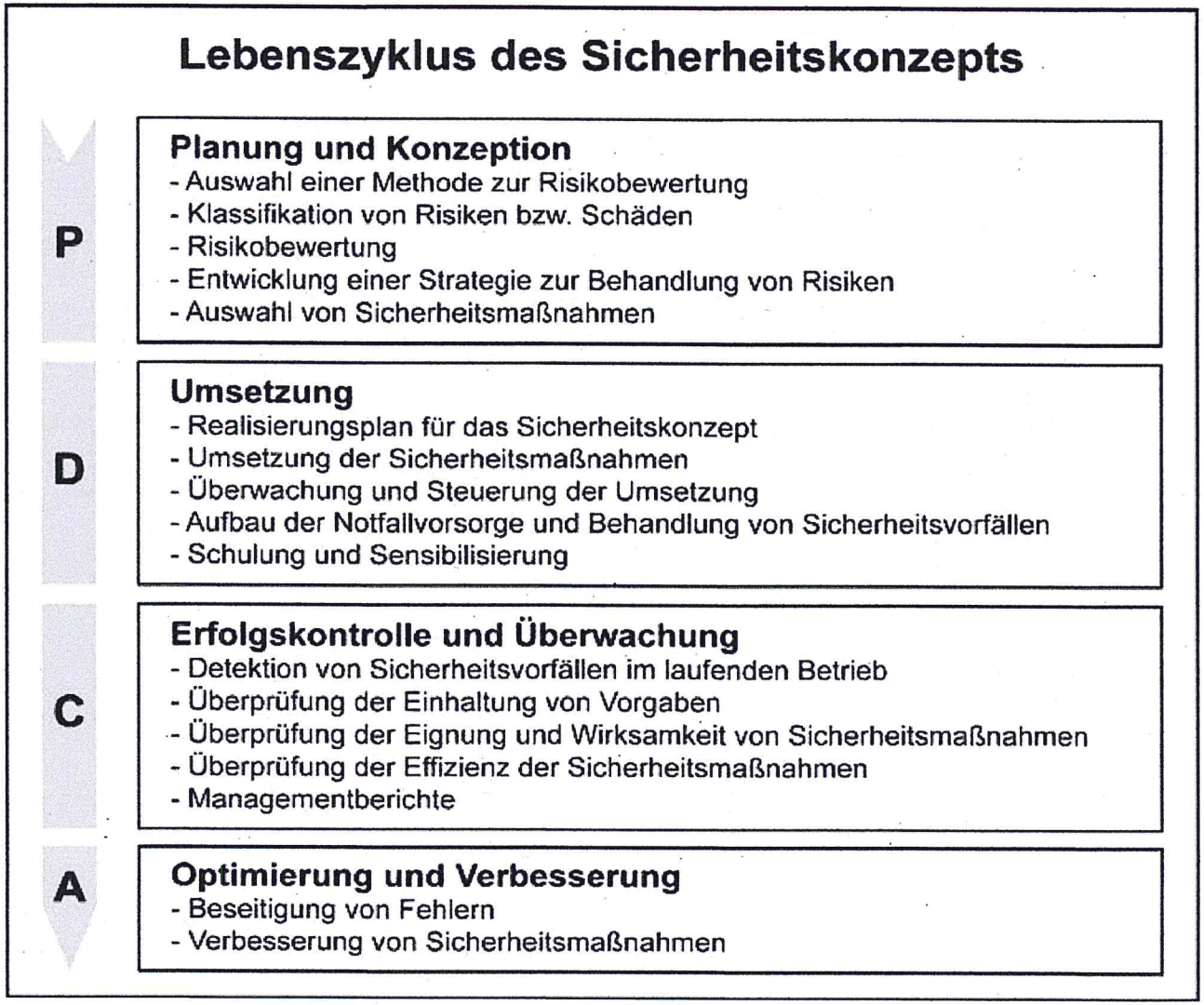
Um ein erreichtes Sicherheitsniveau zu erhalten, ist es erforderlich Anforderungen und ihre Umsetzung im Rahmen eines sog. "kontinuierlichen Verbesserungsprozesses" (KVP) regelmäßig zu überprüfen. Der KVP ist elementarer Bestandteil der Normen ISO 9000, ISO 27001 und des BSI-Standards 100-1. Der kontinuierliche Verbesserungsprozess erfolgt mit Hilfe des sog. „PDCA-Zyklus“.



"PDCA" steht für die englischen Begriffe:

- Plan: Planung, d.h. Festlegung der Anforderungen.
- Do Umsetzung der Planung bzw. Umsetzung der Anforderungen im Betrieb.
- Check: Erfolgskontrolle bzw. Überwachung ob die Anforderungen umgesetzt wurden und eingehalten werden.
- Act: Beseitigung von erkannten Mängeln und Schwächen bzw. Optimierung sowie Verbesserung.

Aufbau eines ISMS (3)



Kritische Erfolgsfaktoren bei der Einführung eines ISMS

- Sicherheitspolitik, Sicherheitsziele und Sicherheitsmaßnahmen sind als Folge der Geschäftsziele oder einzelner „Geschäftsprozesse“ zu formulieren
- Implementierung von Sicherheit in Übereinstimmung mit der vorhandenen Organisationskultur
- Offenkundige Unterstützung und Engagement seitens der Geschäftsleitung (mental und finanziell!)
- Eingehende Kenntnis der Sicherheitsanforderungen, der Risikoanalyse/Risikobewertung und des Risikomanagements
- Effektives „Marketing der Informationssicherheit“ gegenüber allen Managern und Mitarbeitern
- Bekanntmachung der Informationssicherheits-Politik sowie zugehöriger Maßnahmen an alle Angestellten und Auftragnehmer
- Ermittlung des Schulungsbedarfs und Angebot an Schulungen (intern/extern)
- Regelmäßige Durchführung von internen Audits und Management-Reviews
- Kontinuierlicher Verbesserungs-Prozess („KVP“)

Regelungsbereich Personalsicherheit

A.8 Personalsicherheit
- A.8.1 Vor der Anstellung
  - A.8.1.1 Aufgaben und Verantwortlichkeiten
  - A.8.1.2 Überprüfung
  - A.8.1.3 Arbeitsvertragsklauseln
- A.8.2 Während der Anstellung
  - A.8.2.1 Verantwortung des Managements
  - A.8.2.2 Sensibilisierung, Ausbildung und Schulung für Informationssicherheit
  - A.8.2.3 Disziplinarverfahren
- A.8.3 Beendigung oder Änderung der Anstellung
  - A.8.3.1 Verantwortlichkeiten bei der Beendigung
  - A.8.3.2 Rückgabe von organisationseigenen Werten
  - A.8.3.3 Aufheben von Zugangsrechten

Regelungsbereich Beschaffung IT-Systeme

A.12 Beschaffung, Entwicklung und Wartung von Informationssystemen
- A.12.1 Sicherheitsanforderungen von Informationssystemen
  - A.12.1.1 Analyse und Spezifikation von Sicherheitsanforderungen
- A.12.2 Korrekte Verarbeitung in Anwendungen
  - A.12.2.1 Überprüfung von Eingabedaten
  - A.12.2.2 Kontrolle der internen Verarbeitung
  - A.12.2.3 Integrität von Nachrichten
  - A.12.2.4 Überprüfung von Ausgabedaten
- A.12.3 Kryptografische Maßnahmen
  - A.12.3.1 Leitlinie zur Anwendung von Kryptografie
  - A.12.3.2 Verwaltung kryptografischer Schlüssel
- A.12.4 Sicherheit von Systemdateien
  - A.12.4.1 Kontrolle von Software im Betrieb
  - A.12.4.2 Schutz von Test-Daten
  - A.12.4.3 Zugangskontrolle zu Quellcode
- A.12.5 Sicherheit bei Entwicklungs- und Unterstützungsprozessen
- A.12.6 Schwachstellenmanagement
- A.12.6.1 Kontrolle technischer Schwachstellen

Beispiele für bereits umgesetzte Maßnahmen

- IT-Sicherheitsleitlinie ist formuliert und durch die Werkleitung freigegeben.
- Ein IT-Sicherheitsbeauftragter ist ernannt. Eine entsprechende Aufgabenbeschreibung liegt vor.
- verschiedene Sicherheitsrichtlinien sind von der Werkleitung in Kraft gesetzt und den MA bekannt gemacht worden.
- in verschiedenen Sicherheitskategorien sind bereits verschiedene Maßnahmen und Regelungen umgesetzt. z.B.:
  - Physische und umgebungsbezogene Sicherheit:
    - Sicherheitsbereiche sind definiert.
    - Zutrittskontrollen (Hausausweise, Besucherausweise, Logging von Zutritten, Einsatz von Chipkarten und Handvenen-Scan) sind umgesetzt.
    - Es existieren Regelungen zum Schutz von Betriebsmitteln (Rauchverbote, USV, Notstromversorgung usw.)
  - Zugangskontrolllen:
    - Regelungen zum Passwortverfahren,
  - und weitere ....

Quo Vadis ? – wo wollen die Stadtwerke hin ?

- Werden Zertifizierungen angestrebt ?
- Wenn ja, mit welchem Zeithorizont ?
- Welche Bereiche sollen zertifiziert werden ?
- Wer wird die Projekte vorantreiben ?
- Ist externe Unterstützung notwendig ?

Vielen Dank für
Ihre Aufmerksamkeit!