

# Informationssicherheitsma- nagementsystem (ISMS) MVV Netze GmbH

Reinhard Aichele

Mannheim, 29.11.2017

# Agenda

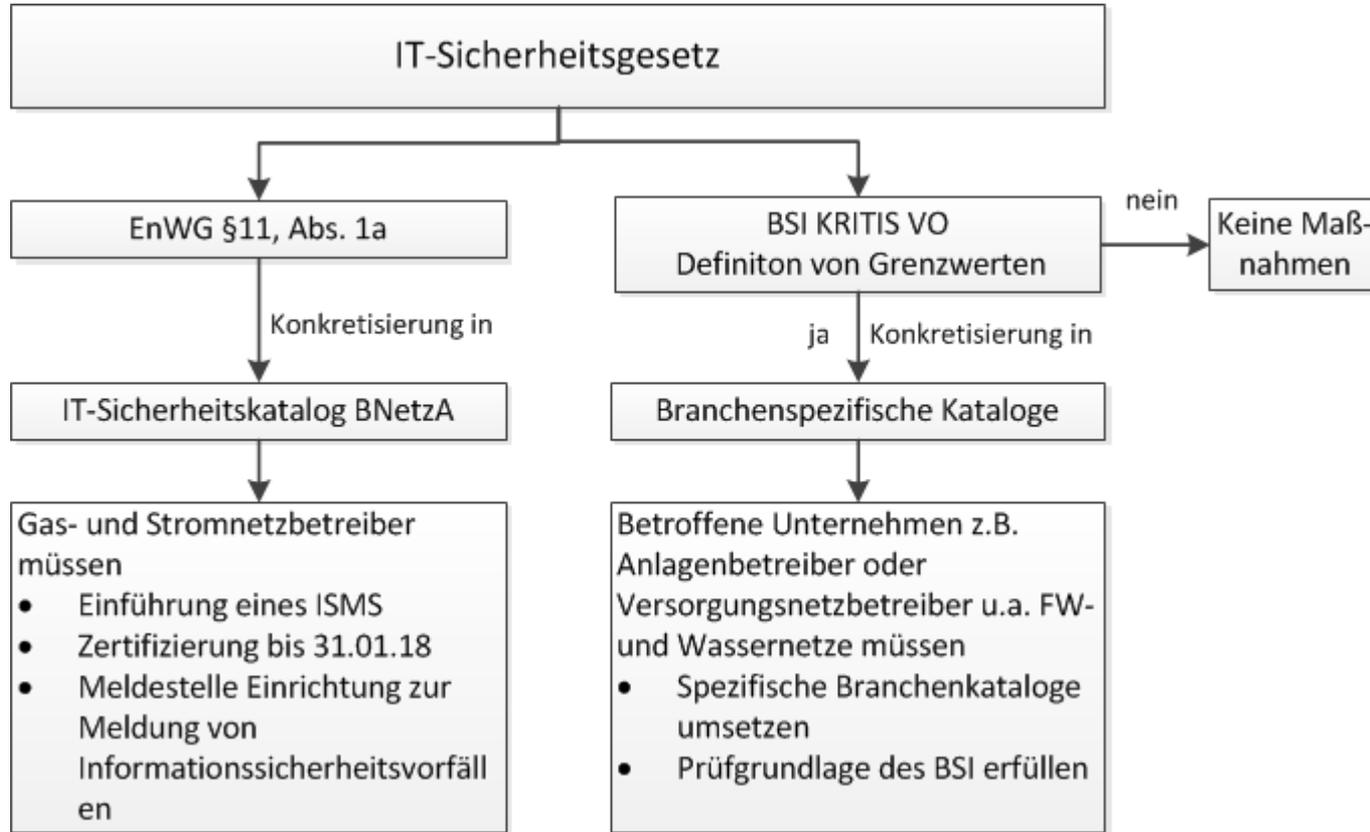
- Was ist ein ISMS
- Gesetzliche Grundlage für ein ISMS
- Normen
- IT-Sicherheitskatalog
- Vorgehensweise im Projekt
- Audit S1
- Audit S2
- Zukünftige Audits
- Ausblick

# Was ist ein ISMS?

## **ISMS** = Informationssicherheitsmanagementsystem

- Informationssicherheit hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. IT-Sicherheit beschäftigt sich an erster Stelle mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung.
- Informationssicherheit umfasst alle Maßnahmen, welche dem Schutz von Informationen dienen.
- Dies beinhaltet neben den Virenschutz, Firewall... auch den Zutritt und Zugang zu den entsprechenden Informationen (technische und organisatorische Maßnahmen).

# Gesetzliche Grundlage für ein ISMS



# Grundforderungen IT-Sicherheitskatalog

- Sicherstellung eines angemessenen Schutzes gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind.
- Aufbau eines ISMS und Zertifizierung bis 31.01.2018  
Unter Betrachtung von:
  - Leitsystem und Systembetrieb
  - Übertragungstechnik/Kommunikation
  - Sekundär-, Automatisierungs- und Fernwirktechnik
- Erstellung eines Netzstrukturplans über alle Technologiekategorien
- Benennung eines Ansprechpartners IT Sicherheit ggü. BNetzA 30.11.2015
- Einrichtung einer Meldestelle ggü. BSI Nov. 2016

# Normen für Netzbetreiber (Strom/Gas)

- [DIN EN ISO/IEC 27001:2017-06](#)

Legt die Anforderungen an Aufstellen, Umsetzen, Betrieb, Überwachung, Bewertung, Wartung und Verbesserung von dokumentierten Informationssicherheits-Managementssystemen in Bezug auf die allgemeinen Geschäftsrissen einer Organisation fest.

- [DIN EN ISO/IEC 27002:2017-06](#)

Gibt Empfehlungen für das Informationssicherheitsmanagement zur Anwendung durch diejenigen Personen, die in einer Organisation für die Einführung, Implementierung und Erhaltung der Sicherheit verantwortlich sind.

- [ISO/IEC 27019:2017-10](#)

Diese Spezifikation stellt einen Leitfaden für die Anwendung eines Informationssicherheitsmanagement-Systems nach ISO/IEC 27002 in der Systemleittechnik in der Energieversorgung bereit.

# Vorgehen bei MVV Netze

- Start des Projekts ISMS-Einführung 18.7.2016
- Ernennung eines ISMS-Sicherheitsbeauftragten als Kontaktstelle zur BNetzA und Einrichtung einer Meldestelle zu BSI
- Aufbau der Projektorganisation über die Bereiche Netzführung, Planung und Bau und Netzbetrieb
- Auswahl eines Beratungsunternehmens zum Aufbau eines ISMS
- Erstellung einer GAP Analyse = Prüfung der vorhandenen Prozesse, Dokumentationen und Richtlinien gegenüber den Normforderungen
- Erstellung einer Schutzbedarfsanalyse = Einstufung der Prozesse und Daten im Netzbetrieb nach kritisch/hoch/mäßig

# Vorgehen bei MVV Netze

- Erstellung von Richtlinien für Informations- und Kommunikationstechnik (IKT) im Bereich der Prozess-IT
- Ernennung von Anlagenverantwortlichen IKT, die sich um das Thema Informationssicherheit in ihren Bereichen kümmern
- Erstellung von Netzstrukturplänen und Dokumentationen, die den Anforderungen der Normen entsprechen
- Aufbau eines der Norm entsprechenden Risikomanagement zur Informationssicherheit
- Definition von Riskowner zur Freigabe von Risikoakzeptanzen/Maßnahmen
- Internes Audit im Sep./Okt. 2017 als Voraussetzung des Zertifizierungsaudits

# Audit S1 17/18.Okt. 2017

- Dokumentenaudit durch einen externen Auditor

Prüfung des Managementrahmen nach DIN EN ISO/IEC 27001:

- Beschreibung des Geltungsbereichs/Politik/Geschäftsbereich/Organisation/
- Netzstrukturpläne
- Dokumentation zu Risikomanagement/Freigaben/Restrisiken
- Managementbewertung
- Interne Audits
- .....

# Audit S2 13. – 15.11. und 20. – 22.11.2017

- Prüfung der Normumsetzung DIN EN ISO/IEC 27002/27019 und Forderungen der BNetzA aus dem IT-Sicherheitskatalog
- Prüfung aller Normvorgaben auf angemessene Anwendung und Umsetzung
- Frage an die jeweiligen Fachabteilungen über die Umsetzung
- Prüfung der Netzstrukturpläne durch ext. Fachexperten Strom und Gas
- Prüfung des Risikomanagement durch ext. Fachexperten Strom und Gas
- Anlagenbegehungen Strom- und Gasstationen
- Prüfung Leitsystem und Rechnerinfrastruktur
- .....

# Zukünftige Audits

- Jährliches Internes Audit durch den ISMS-Beauftragten
- Jährliches Überwachungsaudit durch externen Auditor
- Alle 3 Jahre Rezertifizierungsaudit durch externen Auditor

# Ausblick - Wasserbereich

- Geplanter Projektstart Wasserbereich Dez. 2017
- Aufbau einer Projektorganisation
- Ausweitung des bestehenden ISMS (Strom/Gas) auf den Wasserbereich
- Erstellung und Erweiterung von Dokumentationen entsprechend der Normen DIN EN ISO/IEC 27001/27002
- Umsetzung der Anforderungen des Branchenkatalogs Wasser
- Überprüfung der Umsetzung bis 4.5.2018 durch einen externen Prüfer

MVV Netze GmbH

Reinhard Aichele

Telefon +49 621 290 2119

Telefax +49 621 290 2877

Reinhard.aichele@mvv-  
netze.de



*Metropolregion  
Rhein-Neckar*