Informationstag "Umsetzung des IT-Sicherheitsgesetzes in der Unternehmenspraxis"

Gemeinsame Veranstaltung von TeleTrusT, bevh und BISG

Berlin, 29.11.2016

"Vor der Meldung steht die Vorfallerkennung – ein Praxisbericht aus den KRITIS-Sektoren Energie und Wasser"

Dieter Meyer, Stadtwerke Delmenhorst GmbH

Stefan Menge, Achtwerk GmbH & Co. KG

Agenda

1. Geschäftsfelder der StadtWerkegruppe
2. Anforderungen an den Energienetzbetrieb
3. Schritte zu einem ISMS nach IT-Sicherheitskatalog
4. IS-Vorfallerkennung und Security-Monitoring im Gasnetz

Geschäftsfelder der StadtWerkegruppe

- Gas- und Wasserversorgung
- Stromvertrieb
- Entwässerung (Schmutz- und Niederschlagswasser) inkl. Betrieb der Kläranlage, diverser Pumpwerke usw.
- Betrieb von Blockheizkraftwerken > 500 kW
- Betrieb von Windenergie- und Photovoltaikanlagen
- Betrieb der Bäder- und Wellnessanlage (Grafttherme)
- Abfuhr, Behandlung und Entsorgung von Abfall
- Straßenbeleuchtung
- Dienstleistungen, Contracting

http://www.stadtwerkegruppe-del.de/

Anforderungen an den Energienetzbetrieb

- BNetzA erstellt IT-Sicherheitskatalog mit Mindestanforderungen an Energienetzbetreiber und überwacht dessen Einhaltung
- Gesetzliche Vorgabe durch das Energiewirtschaftsgesetz (ENWG)
- Energienetzbetreiber muss ein Informationssicherheits-managementsystem (ISMS) nach DIN ISO/IEC 27001 einführen
- Darüber hinaus Verpflichtung, bis zum 31.01.2018 nachzuweisen, dass die Anforderungen des IT Sicherheitskataloges der BNetzA umgesetzt wurden
- Entsprechende Zertifizierung zwingend erforderlich
- Etablierung eines angemessenen Schutzes für IKT-Systeme, die für einen sicheren Energienetzbetrieb notwendig sind
- **Erhebliche Herausforderung für Netzbetreiber**

Anforderungen an den Energienetzbetrieb

- SWD betreibt druckgeregeltes Gasnetz in Delmenhorst
- 2 Gasübergabestationen und rd. 45 GDR-Anlagen
- Keine klassische, besetzte Leitwarte
- Netzwerkverbindungen über Internet, Fernwirktechnik, GSM, Funk, etc.
- Betreuung der Steuerungsanlagen dezentral im Netzbereich
- Ziel der zunehmenden Automatisierung war in erster Linie hohe Verfügbarkeit und Optimierung der Betriebsabläufe
- Sicherheitsanforderungen nach heutigem Stand nicht ausreichend, müssen permanent hinterfragt und angepasst werden
- **Änderung der Organisation und Verantwortlichkeiten unbedingt notwendig**

Schritte zu einem ISMS nach IT-Sicherheitskatalog

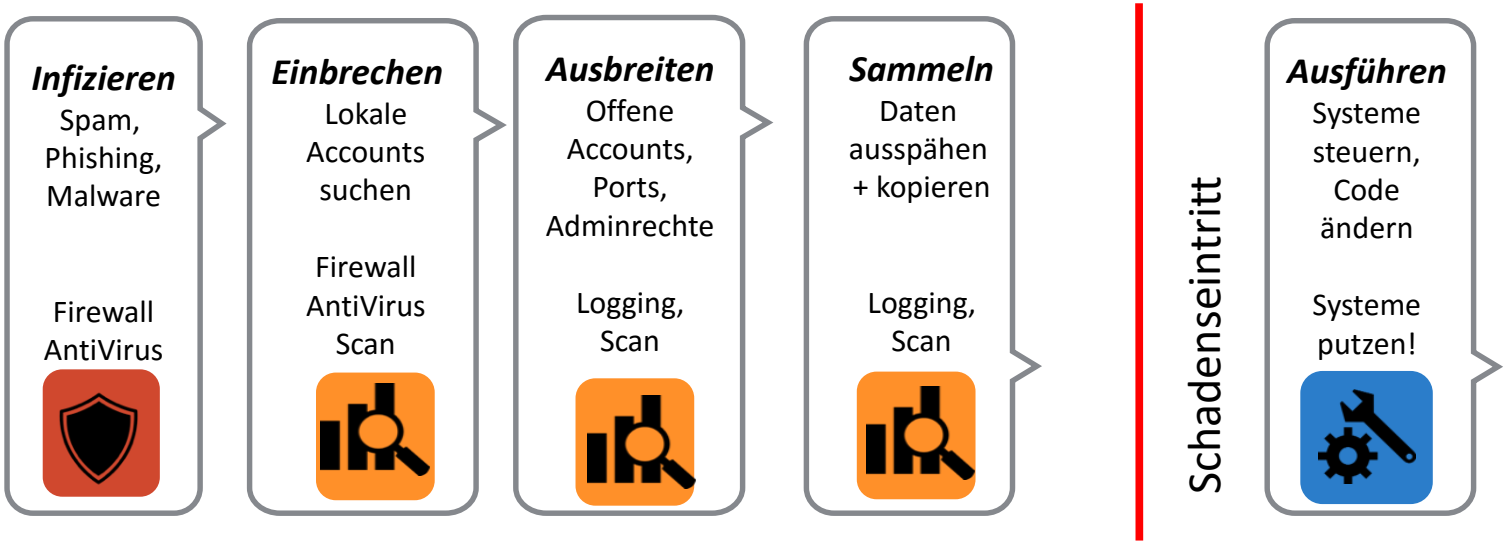
- Statusaufnahme und Festlegung des Anwendungsbereichs
- Inventarisierung der Werte (Assets)
  - Erkennen von Assets
  - Erstellung Netzstrukturplan
- Analysieren und Behandeln von Risiken
  - Erkennen von Schwachstellen und Bedrohungen
  - Behandeln der Risiken
- Maßnahmen festlegen und umsetzen
  - Technische und organisatorische Sicherheitsmaßnahmen planen, bewerten und kontrollieren
- Regelmäßiges Review und kontinuierliche Verbesserung
  - Kontinuierliche Überwachung des Datenverkehrs
  - Erkennen von Anomalien
  - Alarmieren bei Vorfallerkennung

Security-Monitoring im Gasnetz

- Trennung der Steuerungsnetze Gas, Wasser, Abwasser
- Integration einer Sensorik jeweils im PLS der Gas-und Wasserversorgung
- Kontinuierliche Überwachung der Systeme
- Erkennung bisher nicht bekannter Assets
- Falschkonfigurationen, interne Manipulationen und Cyberangriffe werden in Echtzeit-Überwachung gemeldet
- Erfüllung wesentlicher Controls der ISO/IEC 27001
- Umfangreiches Reporting
- Direkte Meldung von Sicherheitsvorfällen an die Behörden möglich
- Risiko eines Systemausfalls wird erheblich minimiert
- **Etablierung eines effektiven Frühwarnsystems**

Zeit und Informationen effizient nutzen

Ablauf eines Angriffes sowie die passende Sicherheitstechnologie



Diese intelligenten Angriffe lassen sich nur durch eine kontinuierliche Überwachung identifizieren und erfolgreich bekämpfen.

Security-Anforderungen durch Industrial Ethernet

- Aktueller **Netzplan** für die Risikoanalyse
- Maximale **Nutzung** der vorhandenen Security-Funktionen zum Schutz und zur Detektionsfähigkeit
- **Reaktionsfähigkeit** durch frühzeitiges Erkennen und Alarmieren von IT-Sicherheitsvorfällen
- **Bediener-Freundlichkeit**: Security-Funktionen ohne Experten-Knowhow
- Einzel-Lösungen sind **nicht** ausreichend…

Wie müssen die neuen Sicherheitskonzepte sein?

dynamisch | kontinuierlich | automatisiert

Der Security-Monitoring Prozess

Produktions-IT analysieren

- Assets automatisch identifizieren
- Verwalten: z.B. Asset-name, -owner, Standort, Gruppieren
- Verbindungen beurteilen, Schwellwerte setzen
- Validieren

Risiken managen

- Schwachstellen
- Bedrohungen
- Risiken
- Maßnahmen
- Reports

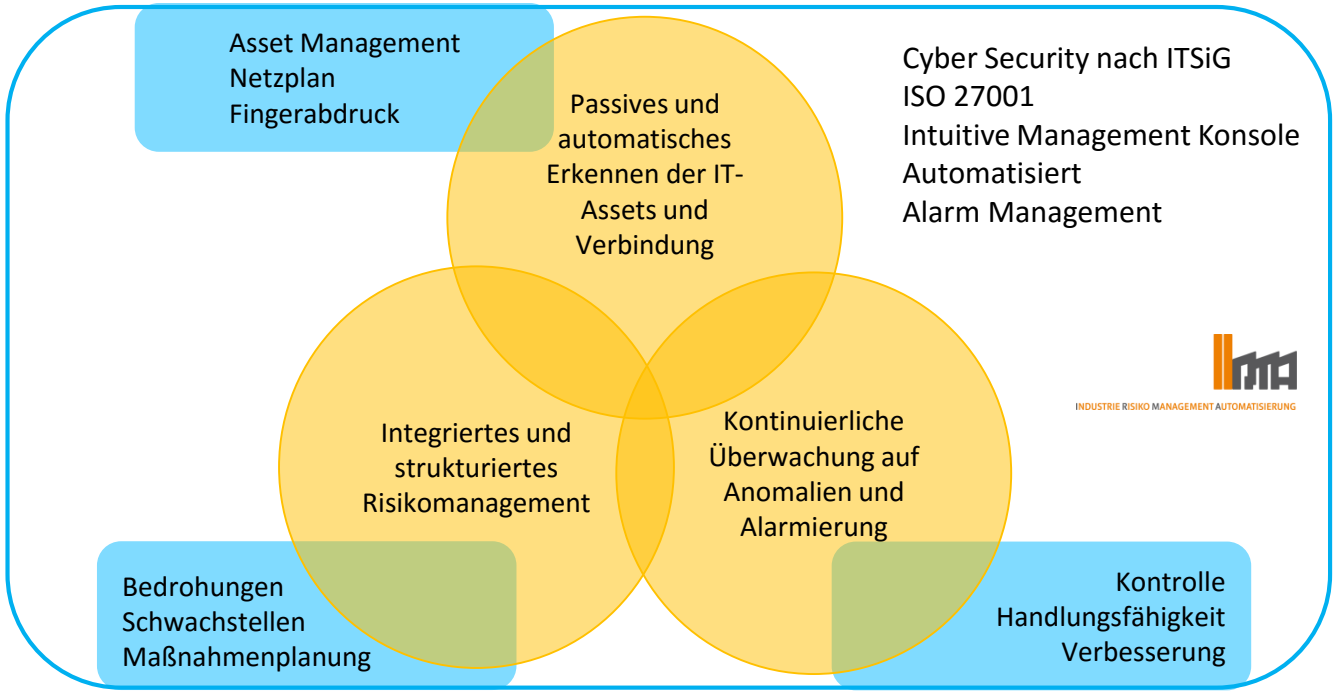
Anomalien erkennen

- Assets
- Verbindungen
- Daten
- Attacken / Schwachstellen
- Kontrollieren

Kontinuität gewährleisten

- Status Quo prüfen
- Soll / Ist Abgleich
- Attacken / Schwachstellen
- Alarme

Vertrauen ist gut, Kontrolle ist wesentlich



Fazit

- Der Einsatz von IRMA bietet eine sehr gute Möglichkeit, die hohen Ansprüche der StadtWerkegruppe Delmenhorst an die Prozess- und IT-Sicherheit und damit an die Versorgungssicherheit langfristig sicherzustellen
- Neben der Erhöhung des allgemeinen Sicherheitsniveaus werden wesentliche controls der DIN ISO/IEC 27001 erfüllt
- Das Zertifizierungsverfahren nach§ 11 Abs. 1a EnWG wird durch den Einsatz von IRMA erheblich erleichtert
- **Deutliche Sensibilisierung der Mitarbeiter und Anpassung der Organisation**
- **Damit zunehmender Anstieg der Organisationssicherheit für die StadtWerkegruppe**

Vielen Dank für Ihre Aufmerksamkeit!