IT Sicherheit -

Normen, Standards und die Digitalisierung

Thomas Geiz, Phoenix Contact

PHOENIX CONTACT
INSPIRING INNOVATIONS

IT-Sicherheit

Haben Sie sich schon einmal eine der folgende Fragen gestellt?

- Wie steht es um die Verfügbarkeit meiner Anlage ?
- Benötige ich ein IT-Securitykonzept ?
- Warum IT-Sicherheit notwendig ist ?
- Muss ich IT-Sicherheit umsetzen ?
- Was beinhaltet IT-Sicherheit ?
- Was hat IT-Security mit Digitalisierung zu tun ?
- Wer muss sich zertifizieren, und was ist mit den anderen ?
- Wonach soll ich mich zertifizieren lassen ?
- Was ist der Stand der Technik in der IT-Sicherheit ?

Dann sollten Sie bleiben …

PHOENIX CONTACT
INSPIRING INNOVATIONS

Was ist eigentlich Industrie 4.0

Allgemeine und eigene Sicht der Dinge

Allgemeine Definition

- **Industrie 4.0** ist die Bezeichnung für ein Zukunftsprojekt zur umfassenden Digitalisierung der industriellen Produktion, um sie für die Zukunft besser zu rüsten.
- Der Begriff geht zurück auf die Forschungsunion der
- **Produktion soll mit moderner Informations- und Kommunikationstechnik verbunden werden.**
- **Technische Grundlage hierfür sind intelligente und digital vernetzte Systeme.**
- Ermöglichen einer weitestgehend selbstorganisierte Produktion: Menschen, Maschinen, Anlagen, Logistik und Produkte kommunizieren und kooperieren in der Industrie 4.0 direkt miteinander.

Quelle: Wikipedia

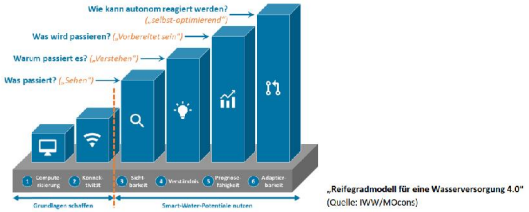
Was bedeutet es für mich…

- **Digitale Vernetzung der Anlagen schreitet voran**
- **IT und OT wachsen zusammen**
- Kommunikationsstandards sind unerlässlich
- Erkennen wo befinde ich mich mit meinem Unternehmen
- Wo will ich mit den einzelnen Geschäftsprozessen hin
- Veränderung - Changemanagement
- Was bringen mir moderne Technologien heute und Morgen
- **Wie gestallte ich die digitale Vernetzung sicher**
- KI – Notwendigkeiten und Ängste

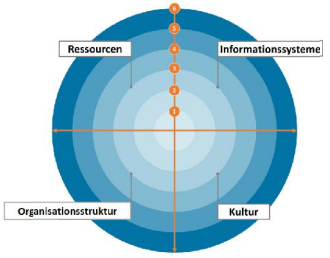
Bestimmung des Digitalisierungsgrads in meinem Unternehmen

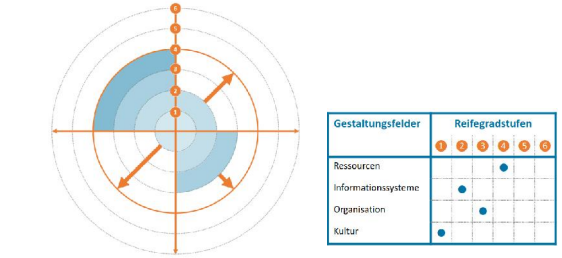
Das Reifegradmodell

- ☑ Methodik zur Bestimmung des Ist-Stands
  - § Schafft Übersicht über die Geschäftsfelder und deren Stand der Digitalisierung
- ☑ Gestaltungsmerkmale der Digitalisierung in Quadranten
  - § Organisationsstruktur
  - § Ressourcen
  - § **Informationssysteme**
  - § Unternehmenskultur
- ☑ Durchführung in den Phasen
  - § ***Bestimmung*** des Ist-Stands des Geschäftsfeldes
  - § ***Angleichung*** des Stands der einzelnen Quadranten
  - § ***Weiterentwicklung*** des Reifegrads



„Reifegradmodell für eine Wasserversorgung 4.0"
(Quelle: IWW/MOcons)





„Reifegradmodell für eine Wasserversorgung 4.0"
(Quelle: IWW/MOcons)

PHOENIX CONTACT
INSPIRING INNOVATIONS

Digitalisierungskonzept

Bestandteile eines Digitalisierungskonzepts

- Welche Bereiche des Unternehmens will ich voran bringen
- Schaffung der nötigen Organisationsstruktur
- Aufbau der Personalresourcen
- Ermittlung des Stand der Digitalisierung im Unternehmen
- Identifikation der Spannungsfelder (z.B. Veränderungen in Arbeitsabläufen)
- **IT-Sicherheitskonzept**
- Investitionsbedarf ermitteln

IT-Sicherheit *erfordert kontinuierliche Überwachung, Kontrolle und Information über*

Bedrohungslagen, Stand der Technik, aktuellen Normen

Informationssicherheit ist ein Weg kein Ziel…..

Verwendete Begrifflichkeiten

- **Kritische Infrastruktur:**
  - Einrichtungen, Anlagen oder Teile davon die den Industrien Energie, Informationstechnik, Telekommunikation, Transport und Verkehr, Gesundheit, Wasser (Trink-und Abwasser), Ernährung sowie Finanz- und Versicherungswesen angehören und von hoher Bedeutung für die Bevölkerung sind

- **Kritische Dienstleistungen:**
  - Dienstleistungen zur Versorgung der Bevölkerung in den kritischen Industrien erbracht werden

- **Trinkwasserversorgung:**
  - Versorgung mit Trinkwasser untergliedert in die Bereiche Gewinnung, Aufbereitung, Verteilung und Leitzentralen

- **Abwasserbeseitigung:**
  - Beseitigung von Abwasser der Allgemeinheit untergliedert in Siedlungsentwässerung, Abwasserbehandlung, Gewässereinleitung und Leitzentralen

Gesetzlicher Rahmen

- Bundesamt für Sicherheit in der Informationstechnik (BSI) hat die Branchenverbände DVGW / DWA beauftragt einen Branchenstandard zum Schutz der Anlagen in der Wasserwirtschaft zu erstellen.

- **Es ist nicht gesetzlich verpflichtend den Branchenstandard anzuwenden. Er stellt aber im Zusammenhang mit dem BSI-Grundschutzkatalog den Stand der Technik dar.**

- **Betreiber kritischer Infrastruktur sind dafür verantwortlich den Stand der Technik im Sinne der Informationssicherheit umzusetzen.**

- **Maßnahmen der Risikoabwendung sind schriftlich zu dokumentieren**

- **Die Durchführung der Maßnahmen kann delegiert werden (Intern / extern) die Prüfung auf Wirksamkeit und die Verantwortung hierfür bleiben beim Betreiber**

- **Verantwortlich ist immer die Geschäftsführung / Vorstand**. Abhängig von der Gesellschaftsform kann ein Betreiber auch persönlich haftend sein im Schadensfalle

IT-Sicherheitsgesetz

Gesetzliche Verankerung der Branchenstandards

[…]

Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach Absatz 1 vorschlagen. Das Bundesamt stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen nach Absatz 1 zu gewährleisten. Die Feststellung erfolgt,

- 1.im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe,
- 2.im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde

Warum ist IT Sicherheit nötig

Ziele der IT Sicherheit:

- **Versorgungssicherheit der Bürger**
- Schutz sensibler Daten (Kundendaten, geistiges Eigentum …)
- **Anlagenverfügbarkeit**
- Zugangsschutz bei Fernwartungskonzepten
- Schutz vor Cyberkriegsführung

Grundziel ist die Versorgungssicherheit der Bürger sicherstellen

Bedrohungen der IT-Sicherheit

Angriffe von außen

- Gezielte Angriffe auf ein Unternehmen aus dem Netz
- Nicht zielgerichtete Angriffe im Netz
- Einbruch / Unerlaubterer Zugang zu Anlagen
- Ungeschützte Fernwartungseinwahlsysteme
- Ungeschützte Fernwirk- und Übertragungssysteme
- E-Mail / Cyberkriegsführung …..

PHOENIX CONTACT
INSPIRING INNOVATIONS

Bedrohungen der IT-Sicherheit

Angriffe von Innen

- Umgang mit Wechseldatenträgern, Synchronisation mit Smartphone/Tablet…
- Mangelnde Softwarekonzepte / nicht durchgeführte Softwareupdates
- Hard und Software von Wartungsfirmen
- Mangelndes Wissen um IT Sicherheit beim Personal

Was beinhaltet IT-Sicherheit

IT-Security steht für Themen rund um den Schutz kritischer Infrastruktur wie…

- **Elementarschutz**
  - Personalausfall, Ausfall der Stromversorgung
- **Höhere Gewalt**
  - Überspannungsschäden
- **Organisatorische Mängel**
  - Wartungsmängel, fehlende Orga-Anweisungen
- **Menschliche Fehlhandlungen**
  - Fehlerhafte Nutzung von IT Systemen
- **Technische Mängel**
  - Ausfall einer Datenbank
- **Vorsätzliche Handlungen**
  - Systematisches Ausprobieren von Passwörtern

http://lustich.de/bilder/andere/obama-und-merkel

Was beinhaltet IT-Security ?

- Die dafür anzuwendenden Maßnahmen unterteilen sich in,
  - Organisatorische Maßnahmen
  - Technische Maßnahmen
  - Personelle Maßnahmen

Wer ist per Gesetz betroffen ...

- Energie
- Wasserwirtschaft
- Informationstechnik
- Ernährung

Planer, Errichter ,Hersteller, Anlagenbetreiber

Gründe für die Umsetzung der IT Sicherheit

- **Betreiber kritischer Infrastruktur**
  - Anlagenverfügbarkeit
  - Gesetzliche Verpflichtung der Umsetzung
  - Freiwillige Umsetzung da unterhalb der Größenvorgabe

- **Betreiber anderer Industrien**
  - Vermeidung von Produktionsausfällen (Anlagenverfügbarkeit)
  - Schutz geistigen Eigentums
  - Unternehmensrichtlinien

- **Dienstleister, Dienstleistungen**
  - Tätig für Unternehmen der kritischen Infrastruktur
  - Schutz geistigen Eigentums
  - Unternehmensrichtlinien

Verschiedene Zertifizierungswege, mit dem selben Ziel ?

- **DIN ISO 2700(1)**
  - Die ISO/IEC 27001 soll für verschiedene Bereiche anwendbar sein
    - **Wie Informationssicherheit, ISMS…**
  - Nicht Branchenspezifisch, Einsatzgebiet offen
  - Kernzielgruppe im Energiesektor, Stadtwerke, Verteilnetzbetreiber (einheitlicher Standard)
  - derzeitiger Branchenstandard Energieversorgung

- **IEC 62443 *Industrial communication networks – Network and system security***
  - Kernzielgruppen sind Industriebetreiber, Hersteller, Anlagenbau..
  - Vorrangig Betrachtung der Netzwerk und Automatisierungstechnik
  - Anomalie Erkennung im Netz
  - globale IEC-Norm

Verschiedene Zertifizierungswege, mit dem selben Ziel ?

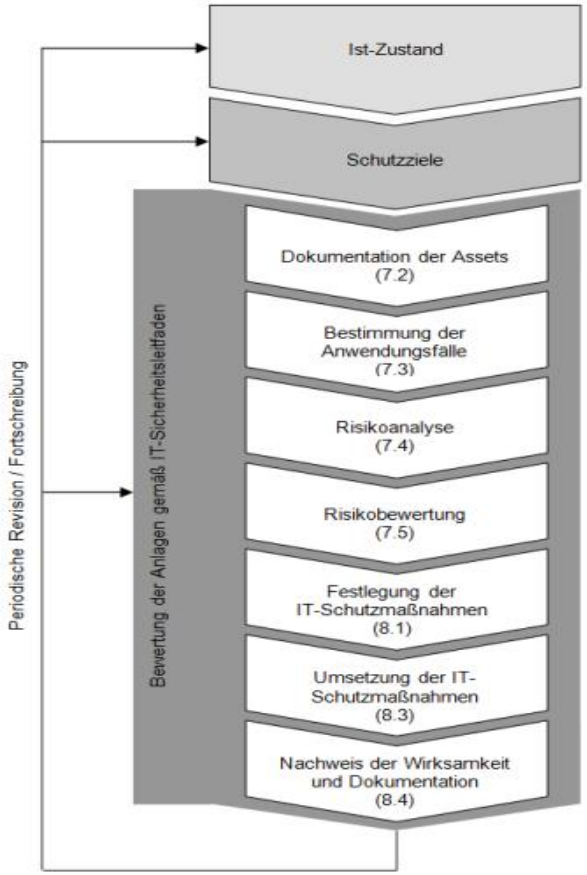
- **B3S Wasserwirtschaft**
  - Erarbeitet im Auftrag des BSI als speziell auf die Wasserwirtschaft angepasster Standard von DWA & DVGW
  - Erster durchs BSI akkreditierter Branchenstandard
  - Kernzielgruppe Wasserversorgung und Abwasserbehandlung in Deutschland
  - Zusammen mit dem BSI-Grundschutz stellt der B3S den Stand der Technik dar

- **BSI-Grundschutzkompendium**
  - Basiswerk des Bundesamt für Sicherheit in der Informationstechnologie
  - Bildet die Basis für die Branchen Standards in der kritischen Infrastruktur
  - Allgemeine Regeln der Informationssicherheit für alle Industrien, Betriebe…
  - Keine Zielgruppenausrichtung, Grundwerk für alle in Deutschland

Maßnahmen in der Umsetzung

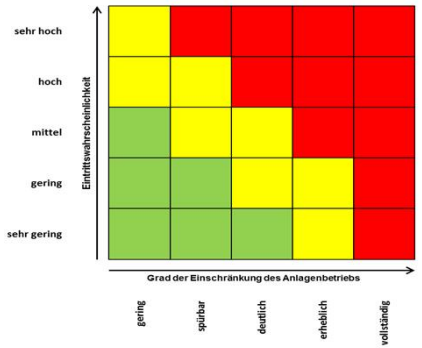
Grundsätzlich immer gleich

- ☑ Schaffung der nötigen Organisationsstruktur
- ☑ Aufbau der Personalressourcen und des Budgets
- ☑ Ermittlung des Ist-Zustands
- ☑ Festlegung der Schutzziele
- ☑ Dokumentation der Assets
- ☑ Risikoermittlung
- ☑ Festlegung der Maßnahmen
- ☑ Umsetzung
- ☑ Kontrolle auf Wirksamkeit



Risikoanalyse

- Grundlage der Gefährdungsbeurteilung zum Schutz der Prozesssteuer- und Überwachungssysteme sollten die Schutzziele nach DVGW W1001(H) sein
- Wahl der Methode der Gefährdungsanalyse liegt beim Betreiber
- Ob die Dokumentation auf Papier, mittels spezieller Software oder z.B. Excel geschieht ist nicht festgelegt
- Wichtig ist, das die Dokumentation für einen dritten Nachvollziehbar erfolgt
- Ist auch bei jeder Modernisierung oder einem neuen Anlagenteil durchzuführen
- Betreibern wird die Einführung eines ISMS empfohlen



Beispiel : B3S Wasserwirtschaft & BSI Grundschutzkompendium

- **B3S Wasserwirtschaft**
  - Erarbeitet im Auftrag des BSI als speziell auf die Wasserwirtschaft angepasster Standard von DWA & DVGW
  - Erster durchs BSI akkreditierter Branchenstandard
  - Kernzielgruppe Wasserversorgung und Abwasserbehandlung in Deutschland
  - Zusammen mit dem BSI-Grundschutz stellt der B3S den Stand der Technik dar

Branchenstandard Wasserwirtschaft

Der Branchenstandard besteht aus zwei Teilen, dem

Branchenleitfaden

- Inhalt:
  - Konkrete Anwendungsfälle (Usecases) mit Querverweise zu den Maßnahmen in den 27k Normen und dem BSI Grundschutz
  - Risikoabschätzung für verschiedene Bedrohungen auf Basis des BSI Grundschutz
  - Querverweise zu den Maßnahmen in den 27kNormen und dem BSI Grundschutz

Branchenstandard Wasserwirtschaft

Anwendungsfälle

Kürzel	Anwendungsfall	Beschreibung	Sicherheitsaspekt(e)
AR1	Dediziertes Netwerk	Alle Netzwerk-und Kommunikations-Infrastruktur ist ausschließlich dem SCADA-System zugeordnet. (Maßnahmen: Netzwerksegmentierung).	Niedrige Netzwerksicherheit ausreichend. Andere Themen, etwa Nutzung e Speichermedien wie USB-Sticks und DVDs, können zu einem Problem werde
AR2	Gemeinsame Nutzung des WAN mit anderen IT-Systemen	WAN-Kommunikationsinfrastruktur wird geteilt (mittels physischer (Medien) Trennung, VPN, VLAN, Firewall)	Hohe Sicherheit und Überwachung erforderlich. Auseinandersetzung mit der Netzwerktopologie notwendig; Kontrolle des Datenverkehrs im SPS-Netzwe
AR3	Gemeinsame Nutzung des LAN mit anderen IT-Systemen	LAN-Kommunikation (innerhalb der Anlage) wird geteilt (mittels VLAN, Firewall)	Sehr hohe Sicherheit und Überwachung erforderlich. Authentifizierung von E mit Zugriff aufdas SPS erforderlich.
NM1	Lokales Netzwerkmanagement	Zugriff auf die Konfiguration der Netzwerk-Infrastruktur aus der unmittelbaren Umgebung des Benutzers (seriell oder Netzwerk).	Grundlegende Zugriffskontrolle notwendig. Zugriff auf Netzwerkkomponent von SCADA-Einrichtungen verwaltet werden, über die SCADA-Netzwerkinfra
NM2	Anlagenweites Netzwerkmanagement	Zugriff auf die Konfiguration der Netzwerkinfrastruktur am jeweiligen Standort (LAN Access)	Mittlerer Schutz erforderlich.
NM3	Netzwerkmanagement über Remotezugriff (von anderem Standort aus)	Zugriff auf die Konfiguration der Netzwerk-Infrastruktur von einem anderen Standort aus.	Hohe Sicherheit notwendig. Hohe Anforderungen an die Verlässlichkeit der Authentifizierung von Benutzern.
OM1	Interne Verantwortung für IT-Sicherheit	Das Unternehmen verantwortet den Einsatz und die Nutzung der IT-Systeme.	Mögliches Organisationsverschulden. Daher: Organisatorische Verankerung Verantwortungen, Regeln und Aufgaben zur Sicherstellung der Durchführung

Gefährdungen | Maßnahmen | ICS-Referenzen | Normenreferenzen

Anwendungsfall

OM1 Interne Verantwortung für IT-Sicherheit

Das Unternehmen verantwortet den Einsatz und die Nutzung der IT-Systeme.

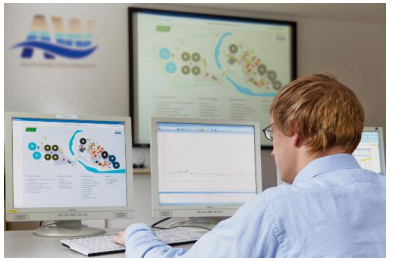
Gefährdungen

G 1.1	Personalausfall
G 1.2	Ausfall von IT-Systemen
G 1.10	Ausfall eines Weitverkehrsnetzes
G 1.18	Ausfall eines Gebäudes
G 1.19	Ausfall eines Dienstleisters oder Zulieferers
G 2.62	Ungeeigneter Umgang mit Sicherheitsvorfällen
G 2.66	Unzureichendes Sicherheitsmanagement
G 2.105	Verstoß gegen gesetzliche Regelungen und vertragliche Vereinbarungen
G 2.106	Störung der Geschäftsabläufe aufgrund von Sicherheitsvorfällen
G 2.107	Unwirtschaftlicher Umgang mit Ressourcen durch unzur
G 2.141	Nicht erkannte Sicherheitsvorfälle
G 2.142	Zerstörung von Beweisspuren bei der Behandlung von Sicherheitsvorfällen

Muster

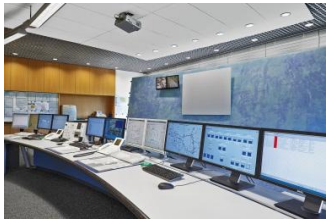
Betreiber kritischer Infrastruktur ist…

- Abwasserbetriebe / Anlagen unter …
  - Kläranlagen **ab** einer Ausbaugröße von 500.000 EW
  - Leitwarten **ab** einer angeschlossen Leistung von 500.000 EW
  - Kanalnetze **ab** einer angeschlossen Leistung von 500.000 EW



Betreiber kritischer Infrastruktur ist…

- Wasserversorgungsunternehmen …
  - Aufbereitungsanlagen mit einer Leistung **ab** 22 Mio. m³/Jahr
  - Transport / Verteilnetz (Fernleitung/Rohrnetz) mit einer Anschlussleistung ab 22 Mio. m³/Jahr
  - Leiteinrichtungen(Leitzentrale) mit einer Abgabe **ab** 22 Mio. m³/Jahr
  - Gewinnungsanlagen mit einer Abgabe **ab** 22 Mio. m³/Jahr
  - Wasserwerk mit einer Abgabe **ab** 22 Mio. m³/Jahr



Der Schwellwert 22 Mio. m³/Jahr errechnet sich aus der Formel

21,9 Mio. m³/Jahr = 43,8m³/(Einwohner x Jahr) x 500.000 Einwohner

Wer ist „nicht“ betroffen..

Die Insellösung ohne Verbindung nach Außen ?

- Eine wirkliche Insellösung ist heute nicht mehr möglich aus Gründen wie,
  - Systemupdates
  - Fremdwartungen
  - Unbeabsichtigte Kontamination durch Fehlverhalten
  - Vernetzung mit der Office-IT für die Betriebsführung
  - Vernetzte Feldgeräte
  - Anlagenbus der Automatisierung ins Feld gezogen

https://www.superlupo-magazin.de

PHOENIX CONTACT
INSPIRING INNOVATIONS

B3S Wasserwirtschaft –

Wer ist nun wirklich betroffen..

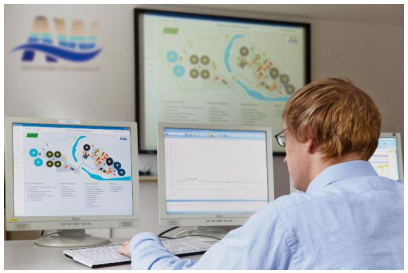
- **Betreiber => 500.000 EW (Abwasser/ 22Mio. M³/Jahr (Trinkwasser) „K“**
  - Zertifizierungspflicht
  - Umsetzungspflicht der Maßnahmen nach Kategorie A+K

- **Betreiber < 500.000 EW (Abwasser/ 22Mio. M³/Jahr (Trinkwasser) „A“**
  - Empfehlung zur Umsetzung der Maßnahmen nach Kategorie „A“
  - Zur Zeit **noch** keine Zertifizierungspflicht, **die Grenze wird sinken !**
  - Es besteht eine indirekte Umsetzungspflicht der Maßnahmen nach Kategorie A weil,
    - Der Branchenstandard ist mit dem BSI Grundschutz der Stand der Technik
    - **Im Schadenfalle bei behördlichen Untersuchungen wird geprüft entsprach die Anlage dem Stand der Technik !!**

Wer ist betroffen..

Jeder ist betroffen !!

Planer



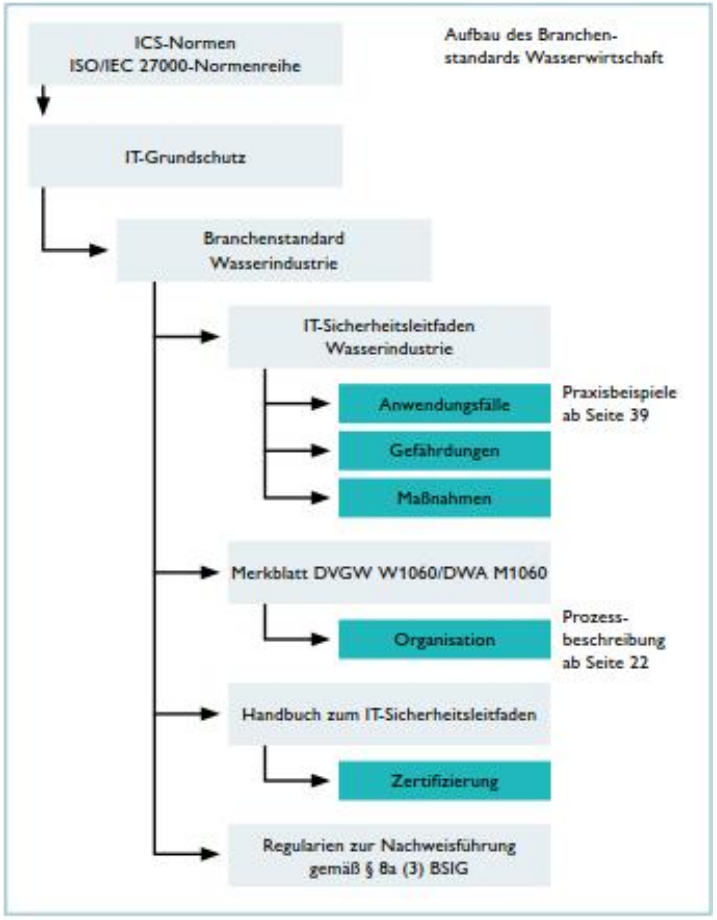
Hersteller

Betreiber

Anlagenbauer

PHOENIX CONTACT
INSPIRING INNOVATIONS

Aufbau des B3S Wasserwirtschaft



- **IT-Sicherheitsleitfaden**
  - Anwendungsfälle für den Praktiker

- **Merkblatt**
  - Anwendungsbereich
  - Normenverweise
  - Verwendete Begriffe

- **Handbuch zum IT-Sicherheitsleitfaden**
  - Praktische Arbeit mit dem Branchenstandard
  - Auditierung
  - Risikoanalyse

PHOENIX CONTACT
INSPIRING INNOVATIONS

Risikoanalyse

- Grundlage der Gefährdungsbeurteilung zum Schutz der Prozesssteuer- und Überwachungssysteme sollten die Schutzziele nach DVGW W1001(H) sein
- Wahl der Methode der Gefährdungsanalyse liegt beim Betreiber
- Ob die Dokumentation auf Papier, mittels spezieller Software oder z.B. Excel geschieht ist nicht festgelegt
- Wichtig ist, das die Dokumentation für einen dritten Nachvollziehbar erfolgt
- Ist auch bei jeder Modernisierung oder einem neuen Anlagenteil durchzuführen

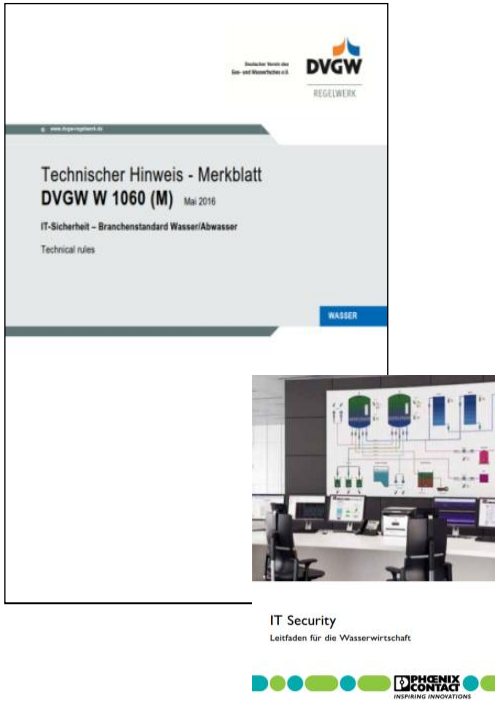
Aktuelle Möglichkeiten der Vorbereitung

- Dokumentation der Anlage und Anlagentechnik (z.B. Stromlaufpläne, Orga-Anweisung..)
- Zutrittsregelungen und Überwachungen
- Netzwerkanalyse
- Erstellen eines generischen Netzwerkplans
- Segmentierung von Netzwerken
- Softwareupdates zeitnah aufspielen und einen sicheren Prozess hierfür schaffen
- Regelung vorhandener Fernzugriffe (Firewall, Private Network, VPN…)
- Kontrolle der HW von Wartungsfirmen die sich ins Netz einloggen am Feldgerät oder Netzwerk

Was ist Stand der Technik in der IT-Sicherheit ?

- **B3S Wasserwirtschaft + BSI Grundschutz = Stand der Technik**
  - Man kann keinen dauerhaften Stand der Technik erreichen
  - Gültigkeit des B3S derzeit 2 Jahre, dann wird ein Update des Branchenstandard veröffentlicht und somit des Stand der Technik
  - Kontinuierliche Informationen über Veränderungen in der Bedrohungslage sind existentiell
  - Anpassungen an Organisation und Technik sind unumgänglich um die Wirksamkeit der Schutzmaßnahmen aufrecht zu erhalten
  - Um den Stand der Technik herstellen, Bedarf es immer,
    - Organisatorischen Maßnahmen
    - Personellen Maßnahmen
    - Technischen Maßnahmen

Branchenspezifische Dienstleistungen



- **IT-Sicherheit gem. den Normen**
  - B3S Wasserwirtschaft
    - DVGW W-1060
    - DWA M-1060
  - BSI-Grundschutz
  - DIN ISO 27001

mit den Leistungen

- Vorbereitung zur Zertifizierung
- Netzwerkanalyse und Segmentierung
- Netzwerkmonitoring und Security

- **Secure Cloud, Portallösungen**

Andere Aufgaben ? Sprechen sie uns an…

PHOENIX CONTACT
INSPIRING INNOVATIONS

Lassen Sie uns Zukunft gemeinsam gestalten!

PHOENIX CONTACT
INSPIRING INNOVATIONS