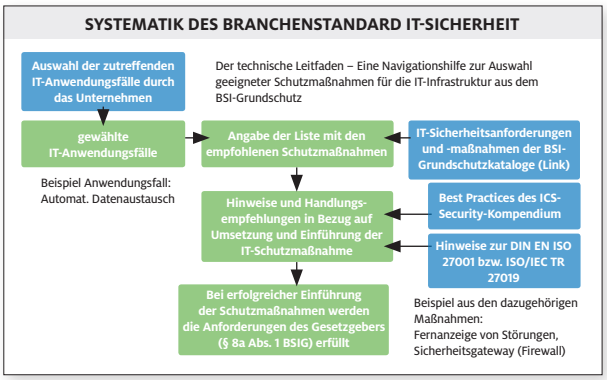
IT-Sicherheit in der Trink-/Abwasserwirtschaft konkret: Der Branchenstandard – W1060 – kommt.

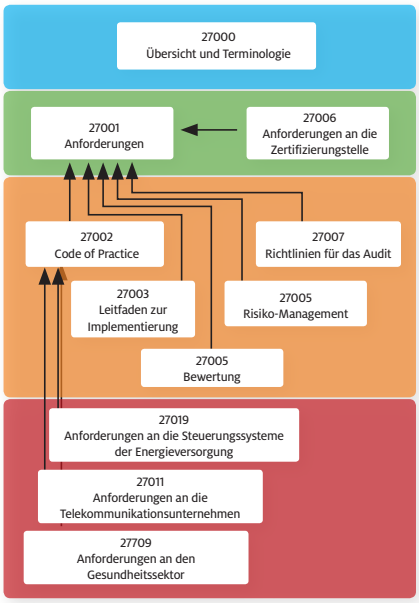
Rechtliche Anforderung

Der Gesetzgeber hat das IT-Sicherheitsgesetz in 2015 und die daraus abgeleitete Rechtsverordnung u.a. für den Sektor Wasser am 3. Mai 2016 in Kraft gesetzt. Damit sind die zeitlichen Vorgaben für den Bereich Ab-/Wasser klar definiert. Exakt zwei Jahre nach dem in Kraft treten müssen Wasserversorgungsunternehmen, die festgelegten Schwellenwerte erreichen bzw. überschreiten, haben angemessene Vorkehrungen zur Vermeidung von Störungen ihrer Informationstechnologie zu treffen. Unternehmen, die diese Schwellenwerte zwar unterschreiten, haben im Sinne einer angemessenen Risikovorsorge und vor dem Hintergrund der aktuellen Cyber-Sicherheitslage ebenfalls geeignete Schutzmaßnahmen nach dem Stand der Technik zu ergreifen. Zum Stand der Technik existiert z.B. eine Handreichung des TeleTrusT e.V. (https://www.teletrust.de/fileadmin/docs/fachgruppen/ag-stand-der-technik/TeleTrusT-Handreichung_Stand_der_Technik.pdf).

DWA und DVGW wurden vom Bundesamt für Sicherheit in der Informationstechnik (BSI) mit der Erstellung des branchenspezifischen Sicherheitsstandards für den Sektor Wasser beauftragt. Das Merkblatt u.a. zu organisatorische Maßnahmen wird nach den Richtlinien des DVGW erstellt und wird dort unter DVGW W 1060 zu finden sein. Der Leitfaden mit den Umsetzungshinweisen zu konkreten Anwendungsfälle wird nach DWA Standard erstellt und vom DVGW übernommen. Voraussichtliche Bestätigung und Veröffentlichung erfolgt im 1. Quartal 2017 durch das BSI.

Bereits heute ist klar, dass darin die sicherheitstechnischen Anforderungen zur Risikoverminderung entsprechend dem BSI IT-Grundschutz formuliert sind. Um für Querverbundunternehmen, die auch Energienetzbetreiber sind, die Umsetzung zu erleichtern, wird auf die entsprechenden Maßnahmen der DIN ISO/IEC 27001 bzw. der ISO/IEC TR 27019 als Vorgabe der Bundesnetzagentur referenziert.





Wo unterstützt IRMA den Automatisierer und ISMS Verantwortliche:

- Zeitersparnis zur Aufnahme und Inventarisierung der IT-Assets ohne wesentlichen Beratungsaufwand
  - → Erforderlich für das initiale Scoping im ISO27000,
  - → Erforderlich für die Identifikation der notwendigen Maßnahmen nach dem BSI Grundschutz und ICS Kompendium
- wirtschaftliche Aufbereitung des geforderten Netzstrukturplanes durch automatisierte Erstellung im Analyseprozess
  - → Übersichtlich und jederzeit aktuell
- Erfüllen der BSI-/BNA-Meldevorgaben da das Erkennen von Sicherheitsvorfällen kontinuierlich durch die Beobachtung der IT-Infrastruktur erfolgt und automatisiert alarmiert
  - → Angriffserkennung und somit unmittelbare, direkte Handlungsfähigkeit für die Betriebsleitung
  - → schnelle Ursachen und Datenerfassung für ein unkomplizierte Meldung

Des Weiteren natürlich die Erhöhung der Verfügbarkeit der gesamten Automatisierung der Anlagen

VIDEC.

Anforderungen an die IT-Sicherheit

Die DWA/DVGW-Umsetzungshinweise (Leitfaden und Merkblatt) beinhalten Handlungsempfehlungen u.a. für konkrete Anwendungsfälle, sogenannte Usecases, und Risikoabschätzungen für verschiedene Bedrohungen. Referenziert auf konkrete Prüfvorgaben (controls) aus der DIN ISO/IEC 27001 und ISO/IEC TR 27019 zu:

- Inventarisierung der Werte (Assets)
  IRMA hilft bei einer ersten Bestandsaufnahme und zeigt ALLE Komponenten und Datenverbindungen, die u.U. weder dokumentiert noch bekannt sind.
- Kontrollmaßnahmen gegen Schadsoftware
  IRMA hilft bestimmte Schadsoftware-Aktivitäten zu erkennen.
- Ereignisprotokollierung
  IRMA zeichnet Störungen bzw. Informationssicherheitsvorfälle auf und meldet diese.
- Meldung von Informationssicherheitsereignissen
  IRMA meldet Anomalien und potenzielle Informationssicherheitsereignisse.
- Überprüfung der Einhaltung von technischen Vorgaben
  IRMA überwacht kontinuierlich als permanentes Kontrollorgan im Unterschied zur Einmaligkeit von sogenannten Penetrationstests.
- Sicherung der Prozessdatenkommunikation
  Maßnahmen zur Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit der internen und externen Prozessdatenkommunikation sind in Abhängigkeit der Sensibilität der übertragenen Daten zu konzipieren, zu entwickeln und umzusetzen.

IRMA Dashboard

Darstellung eines Netzplans

Kundenzitate aus dem Sektor Wasser, Energie und Stadtwerke

- „Der Einsatz von IRMA bietet eine sehr gute Möglichkeit, unsere hohen Ansprüche 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 mit IRMA deutlich erleichtert."
- „Es erfolgt damit ein zunehmender Anstieg der Organisationssicherheit für die Stadtwerke."

Einfach, kontinuierlich und wirksam!

VIDEC GmbH
Contrescarpe 1 · DE-28203 Bremen · Phone +49(0)421 - 33 950-0 · Fax +49(0)421 - 33 950-50
info@videc.de · www.videc.de
Niederlassungen und internationale Vertretungen entnehmen Sie bitte unserer Website.