Sicherheit für die Wasserwirtschaft

Categories : Messtechnik

Date : 13. Oktober 2017

In den automatisierten Anlagen der Wasserwirtschaft werden zur Steuerung der Prozesse Speicherprogrammierbare Steuerungen (ICS) verschiedener Hersteller eingesetzt. Die Betriebsführung wird von Prozessleitsystemen (SCADA, DCS) übernommen, die drüber hinaus oft mit Systemen zur Wahrnehmung des Berichtswesens ausgestattet sind. Die Leittechnik ist mit Standard IT-Komponenten ausgerüstet, sodass hier zwar durch Standardhardware kostengünstige Lösungen existieren, jedoch die Gefahren bestehen, die bereits aus der Office Welt bekannt sind.

Die Branche hat gesprochen

Um den Gefährdungen zu begegnen ist am 25.7.2015 das IT Sicherheitsgesetz in Kraft getreten. Die BSI IT KRITIS Verordnung folgte am 3.5.2016. Sie besagt, dass Kläranlagen ab einer Ausbaugröße von 500.000 EW und Wasserwerke ab einer Wassererzeugung von 22 Mio. m^3/a innerhalb 2 Jahren den Grundschutz sichergestellt, eine Kontaktstelle eingerichtet und die IT Systeme auf den Stand der Technik gebracht haben müssen. Um die Anwendbarkeit für die Branche pragmatisch zu gestalten und den Verantwortlichen einen Handlungsleitfaden zu geben, haben sich die Verbände DVGW und DWA zusammengeschlossen, um einen Branchenspezifischen Standard (B3S) zu erarbeiten. Dieser wurde durch das BSI geprüft und seine Eignung am 30.06.2017 festgestellt. Der IT-Standard für Wasser/Abwasser umfasst einen Sicherheitsleitfaden, in dem Anwendungsfälle, Gefährdungs- und Maßnahmenkataloge sowie Regularien zur Nachweisführung vorgeschlagen sind.

Handlungsleitfaden hilft, dem Ziel näher zu kommen

Das bereits in der Energiebranche etablierte integrierte Sicherheitsmanagement System (ISMS) verwendet die Vorgehensweise nach ISO/IEC 27001 und stellt damit zwar im Ergebnis einen höheren Umsetzungsgrad im Sinne des Grundschutzes dar, ist im Vergleich zum Branchenstandard jedoch deutlich abstrakter und damit variabler für die Etablierung eines wirksamen Systems. Der B3S hat den Vorteil der detaillierten Umsetzung von konkreten Maßnahmen und führt daher schneller zu einem wertbaren Resultat.

Hausaufgabe für die Geschäftsführung

Nach dem Vorgehensmodell des BSI Grundschutzes stellt ein abgestimmter IT Sicherheitsleitfaden die Grundlage für die Inangriffnahme eines ISMS dar. Hierin sind die Schutzziele des Unternehmens entsprechend §8a IT SichG nach Vertraulichkeit, Verfügbarkeit, Authentizität und Integrität zu definieren. Aus diesem leiten sich dann in Kenntnis der vorhandenen Prozesse der Organisation die weiteren Ziele ab. Auf diesem Fundament bringt die Strukturanalyse Aufschluss über den Zustand des IT Systems.

Alle machen mit

Wichtigster Aspekt bei der Umsetzung eines Schutzkonzeptes ist die Schulung, Sensibilisierung von Mitarbeitern. Nur durch entsprechende Akzeptanz und aktiver Unterstützung derjenigen, die am Prozess mitwirken, kann der angestrebte Grundschutz wirksam etabliert werden.

Konkret sind hier für die einzelnen Organisationseinheiten abgestimmte workshops vorzubereiten und durchzuführen. Diese werden nach disziplinarischen Ebenen aufgebaut, um alle Aspekte der Mitarbeiterführung des Unternehmens berücksichtigen zu können.

Kompetenzen für den Handlungsleitfaden

Zur Umsetzung der Maßnahme ist meist die Konsultation externer Spezialisten erforderlich. Grundschutz Experten erarbeiten für die spezifischen Aufgabenstellungen geeignete Handlungsleitfäden. Dabei ist die Kenntnis der Prozesse und der verfahrenstechnischen Anforderungen einerseits als auch das Expertenwissen der IT und speziell der Prozessleittechnik andererseits unabdingbar.

Fazit dem Ziel nähergekommen

Ein wirksamer Schutz vor den Gefährdungen aus dem Netz muss in allen Perspektiven Administrativ/Organisatorisch und Technisch substanziell aufgebaut werden, um erfolgreich zu wirken.