Aqua-IT-Lab – IT-Sicherheit für kleine und mittlere Wasserversorger

Christof Thim

Forschungsprojekt:
Aqua-IT-Lab

Sektor Wasserversorgung: Verteilt und kleinteilig

Das Projekt Aqua-IT-Lab adressiert IT-Sicherheit im Sektor Wasserversorgung. Durch die Kleinteiligkeit und regionale Verankerung der Infrastruktur existieren hier viele kleine und mittlere Versorger. Anders als bei großen Versorgern, welche häufig Skaleneffekte bei der Investition in IT-Sicherheit nutzen können, stehen hier eher weniger Ressourcen zur Verfügung. Entsprechend ist der Umfang gängiger ISMS-Ansätze und Assessment-Verfahren nicht angemessen. Daher entwickelt das Projekt zwei Artefakte: Ein Schnelltest, der gängige Rahmenwerke kondensiert und zeiteffizient in Handlungsempfehlungen umsetzt, dient zur Selbstbewertung und zur Priorisierung von IT-Sicherheitsvorhaben. Eine Infrastruktursimulation ermöglicht die Durchführung von Security Assessments, z. B. Penetrationstests, ohne die Versorgung zu gefährden.

Schnelltest

Auf Basis der ISO2700x-Reihe, der IEC62443 sowie weiterer branchenspezifischer Sicherheitsstandards ermöglicht der Schnelltest eine Bewertung des Reifegrades der IT-Sicherheit in elf Dimensionen. Mit insgesamt 50 Fragen werden die größten Lücken in der IT-Sicherheit identifiziert und automatisiert Vorschläge zu deren Behandlung gegeben. Die Priorisierung der Handlungsempfehlung sorgt dafür, dass sie in handhabbaren Projekten mit flexiblem Ressourcenaufwand umgesetzt werden können.

Die Themenbereiche umfassen dabei nicht nur klassische Themen der Sicherheit der Office-IT, sondern greifen auch die Besonderheiten der Operational Technology auf. Der Umgang mit der Sicherheit der Steuerungstechnik im gesamten Komponentenlebenszyklus ist das Kernstück zum Erhalt der Versorgungssicherheit. Zur Verfeinerung der Schnelltestergebnisse wurde daher die Business-Impact-Analyse auf den Wasserversorgungsprozess angepasst, um Komponenten zu identifizieren, welche eines priorisierten Schutzes bedürfen. Der Schnelltest ergänzt somit den Branchenstandard des Wassersektors (W1060).

Testlabor

Mit dem Testlabor adressiert das Verbundprojekt eine weitere Herausforderung kleiner und mittlerer Versorger. Ihre Steuerungsinfrastruktur entwickelt sich sukzessive: Neue Technologien werden nach und nach integriert. Ein tiefgreifendes Assessment der IT-Sicherheit auf den Übertragungswegen und im Steuerungscode ist entweder nur oberflächlich oder unter der Gefährdung der Versorgung möglich.

Das Labor ermöglicht es den Versorgern nun, die kritischen Komponenten ihrer Infrastruktur oder Infrastrukturteile in einer gesicherten Umgebung zu testen. Hierfür werden Industriekomponenten (Firewalls, SPS, VPN, Vernetzung) und -systeme (SCADA, Leitsystem) mit den realen Konfigurationen eingerichtet. Nachrangige Systeme, wie z. B. einfache Input-Output-Steuerungen oder verteilte Sensoren werden simuliert.

Diese Umgebung kann je nach Umfang der Testfälle z. B. für Penetrationstests oder Code-Reviews genutzt werden, um verborgene Schwachstellen zu identifizieren und Hinweise zu deren Behebung zu geben.

Förderkennzeichen:
16KIS0202K , 16KIS0203 bis 16KIS0206

- Universität Potsdam
- HiSolutions AG
- Pretherm GmbH
- Stadtwerke Brandenburg/Havel GmbH
- Wasser- und Abwasserzweckverband Calau