Foto: privat

Die größte Herausforderung bei der IT-Sicherheit liegt in der praktischen Umsetzung

Das BSI warnt Energieversorgungsunternehmen und Netzbetreiber schon seit einigen Jahren davor, Ziel von Hackerangriffen zu werden. Dr. Michael Conrad, Software-Architekt bei IDS ist Experte für IT-Sicherheit in der Energieversorgung. Im Interview erläutert er die Herausforderungen beim Thema IT-Sicherheit für EVU und Netzbetreiber und zeigt auf, welchen Beitrag Normen und Standards für Safety und Security leisten.

Herr Dr. Conrad, in Ihrem Vortrag im Rahmen der Session „Security in der Energieversorgung“ stellen Sie gemeinsam mit einem Fachkollegen von Schneider Electric ein Einsatzszenario nach IEC 62351 vor. Diese Norm ist ein Standard für die Sicherheit in Energiemanagementsystemen und dem zugehörigen Datenaustausch. Mit welchen Themen befasst sich die IEC 62351?

Conrad: Die Normenreihe IEC 62351 befasst sich vor allem damit, wie bestehende Sicherheitsprotokolle – etwa TLS, RFC 8446 – korrekt angewendet werden. Ziel dabei: die sichere Kommunikation zwischen den einzelnen Komponenten eines Energiemanagementsystems. In meinem Vortrag erläutere ich dies etwas ausführlicher. Zusätzlich deckt die IEC 62351 aber auch Aspekte wie rollenbasierten Zugriffsschutz, Monitoring und Schlüsselmanagement ab. Diese Aspekte spielen schon heute in bestimmten Szenarien, zum Beispiel bei der Stationsautomatisierung, eine wichtige Rolle.

Wo liegen heute die Schwerpunkte bei der Sicherheit in Energiemanagementsystemen? Betrifft das Thema eher Hersteller oder auch Anwender?

Conrad: Für eine erfolgreiche Umsetzung von IT-Sicherheit in der Energieversorgung sind beide Gruppen gleichermaßen verantwortlich. Einerseits müssen Hersteller notwendige Sicherheitsfunktionen wie Zugriffsschutz oder Verschlüsselung in ihre Geräte integrieren und diese passend zu den jeweils gültigen technischen und regulatorischen Anforderungen aktualisieren. Andererseits ist es Aufgabe der Anwender, diese Sicherheitsfunktionen auch korrekt anzuwenden und ein sicheres Umfeld in der eigenen Organisation zu schaffen.

Wo sehen Sie dann heute die größte Herausforderung?

Conrad: Die größte Herausforderung sehe ich in der praktischen Umsetzung. Hersteller müssen notwendige Updates zeitnah bereitstellen. Anwender sind aber genauso in der Pflicht, diese Updates auch kurzfristig auf die vorhandenen Geräte

auszurollen. In beiden Fällen verursacht dies zusätzlichen Aufwand, der jedoch insgesamt zu einer höheren Systemsicherheit führt.

In der öffentlichen Diskussion werden in erster Linie Energieversorgungsunternehmen und Netzbetreiber beim Thema Sicherheit der Managementsysteme genannt. Sind diese auch aus Ihrer Sicht die Hauptbetroffenen oder ist das Thema beispielsweise auch für Industriebetriebe relevant?

Conrad: Der Fokus liegt momentan auf den Betreibern kritischer Infrastrukturen. Die Dezentralisierung fordert aber, dass auch die anderen Beteiligten am Energiesystem, also Anlagenbetreiber, Vermarkter oder Aggregatoren, genauso in die Verantwortung zur IT-Sicherheit mit einbezogen werden. Als wichtige Zielgruppe sehe ich die Anlagenbetreiber und darunter auch die angesprochenen Industriebetriebe, die schon jetzt oder künftig ihre steuerbaren Lasten oder Erzeuger in das Energiesystem integrieren. Neben der sicheren Kommunikation in Richtung Netzbetreiber müssen sie sich auch mit Themen wie sicherer Wartung und Diagnose beschäftigen, um die notwendige IT-Sicherheit auch im Anlagenbereich garantieren zu können.

Unter dem Slogan »Intelligenz statt Kupfer« werden immer mehr Ortsnetzstationen mit Fernwirktechnik und Überwachungsinstrumenten ausgestattet. Das ist sicherlich ebenfalls ein Thema für die IEC 62351?

Conrad: Gerade im Szenario „Intelligente Ortsnetzstation“ werden die Themen Zugriffsschutz und sichere Kommunikation aus der IEC 62351 eine wichtige Rolle spielen. Derzeit wird aufgrund fehlender privater Kommunikationsinfrastruktur meist auf öffentliche Kommunikationssysteme, also zum Beispiel den Mobilfunk, zurückgegriffen. Hierzu bietet die Normenreihe IEC 62351 sowohl für den Austausch von Prozessdaten mittels IEC 60870-5-104, als auch IEC 61850 entsprechende Vorgaben. Einzig im Bereich sichere Wartung und Diagnose solcher abgesetzter Anlagen gibt es aktuell nur wenige direkte Vorgaben durch die IEC 62351. Hier besteht noch Handlungsbedarf.

Demnächst soll der lang erwartete Rollout intelligenter Messsystemen – Stichwort Smart Metering – starten. Dabei soll es für die FNN-Steuerbox ein Protokoll für Steuerungslösungen geben. Wie weit sind hier die Standards beschrieben und die Vorgaben geklärt?

Conrad: Anfang 2018 wurde die erste Version des Lastenheftes für die FNN-Steuerbox durch das Expertenteam des FNN veröffentlicht. Dort ist bereits die herstellerübergreifende Kommunikationsschnittstelle der FNN-Steuerbox mittels des etablierten Kommunikationsprotokolls IEC 61850 und die prioritätsbasierte Steuerung von elektrischen Anlagen für die verschiedenen Marktrollen beschrieben. Hinsichtlich der IT-Sicherheit hält die FNN-Steuerbox die Anforderungen der Technischen Richtlinie TR-03109-1 des BSI aus dem Umfeld des intelligenten Messsystems ein.

Die aktuelle Arbeit des Expertenteams umfasst vor allem einheitliche administrative Funktionen wie Firmware- oder Parameter-Updates.

Dr. Michael Conrad, Software-Architekt bei IDS, präsentiert im Rahmen des Forums „Security in der Energieversorgung“ beim VDE Tec Summit 2018 ein Einsatzszenario der IEC 62351. Seien Sie dabei, wenn am 13. und 14. November in der STATION Berlin Energieexperten aus EVU und Wissenschaft, Netzbetreiber und Energiewirtschaft sowie Politik über die Zukunft der Energieversorgung diskutieren und bringen Sie Ihre Perspektive ein: https://tecsummit.vde.com**.**