Sicherheit für sensible Infrastrukturen: AREVA schützt industrielle Anlagen gegen Cyber-Attacken mit einer IT-Security-Lösung aus der Kerntechnik

Erlangen, 29. November 2016

Das Schlagwort „Industrie 4.0“ steht für die zunehmende Vernetzung von Industrieanlagen mit dem Internet. Die Kehrseite dieses Trends bilden neue Manipulationsmöglichkeiten von außerhalb. Spätestens seit „Stuxnet“ geraten auch sogenannte speicherprogrammierbare Steuerungen ins Visier von Hackern aller Couleur. Entsprechende Anlagen befinden sich weltweit in tausenden Betrieben in der Industrie, der Energieversorgung und anderer kritischer Infrastrukturen. Ungesicherte Schnittstellen zum Internet bilden ein Einfallstor für das Auslesen oder die Manipulation von Programmcodes oder Konfigurierungsdaten.

In Kernkraftwerken sichern bereits seit Jahren speziell entwickelte und zertifizierte Softwarelösungen sensible Anlagen wie etwa die Lademaschine vor einem unbefugten Zugriff. Diese ausgereiften Lösungen stehen für alle SPS-Steuerungen auch außerhalb der Kerntechnik zur Verfügung und können mit verhältnismäßig geringem Aufwand in bestehende Industrieanlagen und Infrastruktureinrichtungen integriert werden.

„Wir implementieren unsere Sicherheitssoftware individuell in jede dieser Steuerungen und können so sensible Systeme zuverlässig überwachen. Das haben umfangreiche Tests auch von externen Gutachtern und kerntechnischen Aufsichtsbehörden bestätigt“, sagt Holger Hoppe, IT-Security-Spezialist bei AREVA in Erlangen, und ergänzt: „Durch den jahrelangen Einsatz in Kernkraftwerken können wir attraktive Lizenzlösungen für andere Branchen anbieten.“

Die AREVA-Software OPANASec verriegelt und überwacht die Integrität der Systeme gleichermaßen. Während der Integritätsschutz verhindert, dass die Software in speicherprogrammierbaren Steuerungen gelesen und überschrieben wird, sorgt die Integritätsüberwachung kontinuierlich dafür, dass Änderungen zuverlässig erkannt und gemeldet werden. Das System informiert den Betreiber der Anlage bei jeglichem Eingriff in das System. Daraufhin kann die Veränderung entweder freigegeben oder Gegenmaßnahmen ergriffen werden. Unbemerkte Eingriffe sind damit ausgeschlossen.

Pressekontakt:
Stefan Pursche, Tel.: +49 9131 – 900 93304, Fax: +49 9131 – 900 94411, stefan.pursche@areva.com
AREVA GmbH, Paul-Gossen-Str. 100, 91052 Erlangen, Deutschland