Starke Partnerschaft: AREVA und secunet

Das neue IT-Sicherheitsgesetz soll mehr Sicherheit schaffen für Kritische Infrastrukturen. Verantwortlich für die Umsetzung bleibt allerdings weiterhin der Betreiber

Der Angriff auf den französischen Fernsehsender TV5Monde Anfang April ist nur ein Beispiel für eine Art von Kriminalität, die mehr und mehr Lebensbereiche bedroht. Die Cyberattacke richtete enormen Schaden an: Stundenlang war der Sendebetrieb der Station unterbrochen, auch über die Internetseite und die meisten Konten in den sozialen Netzwerken hatte der Sender lange Zeit keine Kontrolle. Es dauerte Tage, um zu einem Normalbetrieb zurückzukehren.

>>>

Die Auswirkungen wären noch gravierender, wenn ein solcher Angriff auf lebenswichtigere Bereiche wie die Strom- oder Wasserversorgung erfolgreich wäre! Wie ab Seite 10 beschrieben, soll nun das IT-Sicherheitsgesetz für diese Bereiche der Kritischen Infrastrukturen (KRITIS) mehr und umfassendere Sicherheit schaffen. Verantwortlich für die Umsetzung bleibt allerdings weiterhin der Betreiber.

Sicherheit für digitale Steuerungsanlagen

AREVA ist nicht nur Lieferant für Nuklear- und Windkraftanlagen, sondern bietet auf Basis jahrelanger Erfahrung im Umfeld Kritischer Infrastrukturen auch ein breites Spektrum an Produkten und Dienstleistungen, wenn es um die Sicherheit von digitalen Steuerungsanlagen geht. Im engen Schulterschluss mit Partnern wie secunet wird hierbei die IT-Sicherheit nicht erst beim Betrieb einer Anlage berücksichtigt, sondern fängt schon bei der Produktentwicklung an. So können ausgereifte Ansätze angeboten werden: sei es beim grundlegenden Aufbau eines ISMS, beim Gesamtkonzept oder bei der konkreten Implementierung spezieller Hardware- und Softwarelösungen. Alle Leistungen zum Thema Industrial Security werden in einem integrativen Ansatz zusammengefasst, so dass nukleare und nicht nukleare Kunden gleichermaßen von den Best Practices mit weltweit höchsten Schutzklassen profitieren:

- Aufbau von ISMS inklusive Risikobewertung bis hin zur Auditierung, zum Beispiel nach ISO/IEC 27000
- Industrial Security, mit Security-Zonen und Security Grading, zum Beispiel nach IEC 62443
- Security Modellierung und Simulation
- Prozessleitsysteme und Netzleittechnik
- SIEM (Security Information and Event Management)
- Automation Security, z. B. PCS7, WINCC, SIPROTEC
- Intrusion Detection und Intrusion Prevention, Whitelisting, Security Tests …
- Laufende Bedrohungserfassung, -bewertung, -analyse und -abwehr ■

Mehr Informationen:
Holger Hoppe
holger.hoppe@areva.com

Christoph Schambach
christoph.schambach@secunet.com

Zuverlässige Integritätsüberwachung

AREVA

Mit der Lösung OPANASec™ entwickelte AREVA für diverse Steuerungssysteme verschiedene, einfach einsetzbare Softwaremodule, mit denen eine Integritätsüberwachung realisiert wird. Einerseits sind damit Änderungen am Programm nur nach Betätigung eines Schlüsselschalters möglich, andererseits werden Angriffe, die die Anwendersoftware oder die Konfigurationsdaten manipulieren, zuverlässig entdeckt und sofort gemeldet. Das hat der TÜV SÜD zertifiziert, Patente dafür sind angemeldet.