Sicherheit in industriellen Netzwerken durch intelligente Methoden zur Anomalieerkennung und Integritätsprüfung

Motivation

Durch die steigende Komplexität in verschiedenen Applikationsbereichen, wie z.B. Avionik, Automotive und der industriellen Anlagensteuerung, entstehen immer höhere Anforderungen an Verfügbarkeit, Integrität und der Anlagensicherheit. Im Projekt SiNeMA werden speziell industrielle Applikationen untersucht. Die eingesetzten Automatisierungs- bzw. Prozesssteuerungs- und -leitsysteme waren bis vor wenigen Jahren noch isolierte Elemente. Deswegen lag der Fokus vor allem auf der funktionalen Sicherheit (engl.: safety). Heutzutage sind diese, unter dem Begriff „Industrial Control Systems“ (ICS) zusammengefasste Systeme, aber immer stärker, sowohl untereinander als auch mit dem restlichen Firmennetzwerk, z.B. zum Auslesen von Messwerten, vernetzt. Dadurch ergibt sich ein wesentlich höheres Angriffspotential. Dies wird von den Herstellern sowie Integratoren, als auch Anwendern von ICS allmählich erkannt. Seit dem Auffinden von Stuxnet, Duqu und Flame kann ein stetiges Umdenken wahrgenommen werden. Diese zur Sabotage und Spionage eingesetzte Schadsoftware führt die Brisanz der Lage vor Augen und verdeutlicht den akuten Handlungsbedarf.

Vorgehen

Aufgrund der derzeitigen Situation ergibt sich die Notwendigkeit der Entwicklung von intelligenten Methoden zur Anomalieerkennung und Integritätsprüfung. Denn nur so können Angriffsmuster schnell und effizient erkannt werden. Durch integrierte Sicherheitsmechanismen wird die Unversehrtheit der Systeme im angestrebten Anwendungsfall, der zusammen mit den Partnern erarbeitet wird, gewährleistet. Wesentliche Bestandteile dabei sind die von der Trusted Computing Group spezifizierten Standards und Technologien (z.B. TPM, TNC), die als Basis dienen und eine Authentisierung im Netzwerk ermöglichen.

Um die Sicherheit der Daten zu gewährleisten können unvermeidbare Angriffe durch unterschiedliche Sicherheitsmaßnahmen, die in mehreren Schichten implementiert sind, eingedämmt werden.

Eckdaten

Kurztitel

SiNeMA

Forschungsschwerpunkt

Digital Technologies

Laufzeit

01.09.2013 - 31.08.2017

Fördergeber

Bundesministerium für Bildung und Forschung

Projektleitung

Prof. Dr.-Ing. Andreas Grzemba

Ziele

Das Projekt befasst sich mit der Entwicklung von intelligenten Methoden zur Anomalieerkennung und Integritätsprüfung in industriellen Netzwerken, um Angriffsmuster schnell und effizient zu erkennen und Sicherheit zu gewährleisten.