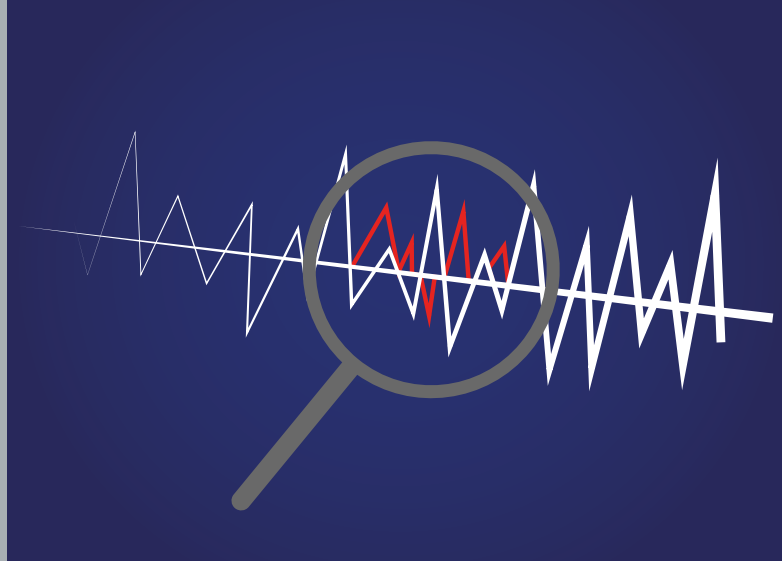
Fraunhofer
SIT

FRAUNHOFER-INSTITUT FÜR
SICHERE INFORMATIONSTECHNOLOGIE



FRÜHWARNSYSTEM FÜR INDUSTRIELLE NETZE

GEFAHREN ERKENNEN, ANGRIFFE ABWEHREN, NETZE SICHERN

Fraunhofer-Institut für Sichere Informationstechnologie SIT

Kontakt:
Sinisa Dukanovic
Rheinstraße 75
64295 Darmstadt

Telefon 06151 869-153
Fax 06151 869-224
sinisa.dukanovic@sit.fraunhofer.de
www.sit.fraunhofer.de

In industriellen Internet of Things-Umgebungen kommunizieren viele unterschiedliche Maschinen, die miteinander vernetzt sind. Über diese Kommunikationsflüsse lassen sich frühzeitig Abweichungen und Gefahren feststellen: Die Experten des Fraunhofer-Instituts für Sichere Informationstechnologie SIT nutzen den Netzwerkverkehr eines Industrial Control Systems (ICS) als Frühwarnsystem für Angriffe und andere Veränderungen, indem sie Netzwerkdaten mit Methoden des maschinellen Lernens und Big Data-Technologien analysieren. So können frühzeitig Gefahren der Industrie 4.0 abgewehrt und Ausfälle vermieden werden.

Industrielle Steuernetzwerke bestehen aus vielen miteinander vernetzten Maschinen und Geräten wie Routern, Anlagenteilen, Netzwerkknoten, Switches etc., die permanent Daten austauschen. Die meisten Unternehmen haben dieses Netzwerk nach außen mit mehreren Netzwerksicherheitsanwendungen wie etwa einer Firewall abgesichert, die bekannte Bedrohungen erkennen und gängige Angriffe abwehren. Bei Attacken mit neuartigem Angriffsmuster ist die Erkennungsrate solcher Anwendungen allerdings schwach. Darüberhinaus erschwert die zunehmende Komplexität von Industrienetzwerken – durch wachsende Anzahl von Kommunikationsteilnehmern und steigende Netzwerkaktivität – die Überwachung von ICS und die Erkennung von Anomalien. Hier kann ein bisher unbekanntes Schadprogramm bereits die Steuerung beeinträchtigen oder Daten stehlen, ohne dass dies bemerkt wird, wie es bei den Computerwürmern Stuxnet oder Duqu der Fall war.

Netzwerkanalyse mit künstlicher Intelligenz

Die Sicherheitsexperten des Fraunhofer SIT nutzen deshalb Methoden des maschinellen Lernens und Big Data-Technologien, um unbekannte Gefahren, unbefugte Zugriffe, Netzwerkfehler und andere Unregelmäßigkeiten innerhalb eines ICS zu identifizieren: Zunächst wird auf Grundlage des normalen Standardnetzwerkverkehrs des Unternehmens mittels Machine Learning ein Modell trainiert, das als Ausgangspunkt für den Analyseprozess dient. Das Anomalieerkennungssystem nutzt dann dieses Modell und wendet es auf den laufenden neuen Netzwerkverkehr an. Dabei wird sämtlicher Datenverkehr mit einbezogen, etwa aus Feldbus-, Sensor-, Fertigungs- oder ERP-Daten. Wenn hierbei Ereignisse gefunden werden, die vom zuvor trainierten Modell abweichen (also eine Anomalie darstellen), werden diese Vorgänge identifiziert und an einen Sicherheitsleitstand gemeldet.

Das Fraunhofer SIT hilft damit Netzwerkbetreibern, mehr Transparenz über ihre Datenflüsse innerhalb des Industrial Control Systems zu bekommen und nicht nur bekannte Gefahren zu erkennen, sondern auch bisher unbekannte Anomalien zu entdecken, die eine Gefahr darstellen könnten.

Unser Angebot

- Anomalieerkennung in ICS mittels Machine Learning und Big Data-Technologien
- Individuelle Netzwerkdatenanalyse
- Analyse von Feldbus-, Sensor-, Fertigungs- und ERP-Dateien