TECHNISCHE UNIVERSITÄT WIEN

Information & Software
Engineering Group
Favoritenstraße 9
1040 Wien, Österreich
www.ifs.tuwien.ac.at

Mehr IT-Sicherheit für die Industrie 4.0

Schutz vor Cyber-Attacken durch maßgeschneiderte Sicherheitslösungen für Produktionssysteme – auch bereits in der Entwicklungsphase

Der Computerwurm Stuxnet sabotierte vor einigen Jahren ganze Industrieanlagen. Er griff vor allem iranische Atomanlagen an und machte erstmals breit und medienwirksam bekannt, wie Schadprogramme – sogenannte Malware – gezielt für einen Angriff auf Produktionsbetriebe verwendet werden können. Stuxnet bewirkte ein lang überfälliges Umdenken für mehr Informationssicherheit in dieser Domäne.

Seit Stuxnet ist es in der Öffentlichkeit um Cyberattacken auf Industrieanlagen wieder ruhig geworden, tatsächlich hat sich die Bedrohungslage jedoch verschlechtert. Laut dem Jahresbericht 2016 der US-Behörde ICS-CERT stieg in den vier Jahren davor die Zahl der aufgedeckten und gemeldeten Angriffe von ca. 140 auf über 220 pro Jahr. Die Dunkelziffer dürfte weit höher liegen, da entsprechende Vorkommnisse aus Angst vor Reputationsschäden oft nicht gemeldet werden.

Mit der breiten Einführung vernetzter Produktionssysteme für die Industrie 4.0 eröffnen sich nun neue Angriffswege für Cyberkriminelle auf Industrieanlagen, die vormals weitgehend abgekapselt waren.

Neben bereits in Betrieb stehenden Produktionssystemen ist zunehmend auch die Planungsphase gefährdet. Durch einen gezielten Angriff während des Entwicklungsprozesses von Anlagen können Kriminelle unbemerkt Schwachstellen in Systeme einschleusen, die erst nach deren Inbetriebnahme ausgenutzt werden. Diese Vorgehensweise erlaubt es Hackern, ohne späteren Angriff von außen, Produktionsprozesse lahmzulegen. Es kann auch Malware verbreitet werden, um andere Systeme zu infizieren.

Stuxnet war zwar hoch komplex, mit einem frühen Zugang in der Entwicklungsphase wird eine ähnliche Attacke aber weit einfacher und kann beliebige Anlagen der Industrie 4.0 betreffen. Damit Unternehmen sich mit geeigneten Sicherheitsmaßnahmen gegen diese neuartige Bedrohung rüsten können, entwickelt die TU Wien wirksame Schutzmechanismen für den Entwicklungsprozess von Industrieanlagen und Produktionssystemen (Production Systems Engineering – PSE).

Zielsetzung

Um digitale Fabriken sicher betreiben zu können, muss sowohl Daten- und Informations- als auch Produktionssicherheit gewährleistet sein. Dazu muss ein ganzheitliches Sicherheitskonzept über den gesamten Entwicklungsprozess verfolgt werden. Dies bedeutet vor allem, dass Informationsprozesse bereits in der Konzeptionsphase abgesichert sind.

Ein zentraler Aspekt ist der Zugriff auf gemeinsame Dokumente und Datensätze durch mehrere Parteien. Er wird durch vernetzte Datenrepositorien ermöglicht. Mit deren zunehmender Verwendung und durch die steigende Anzahl von einzubeziehenden Partnern – die von unterschiedlicher Vertrauenswürdigkeit sind – wird die Absicherung dieser schutzwürdigen Ressourcen erschwert. Es gilt daher, Informationsprozesse mit einem Höchstmaß an Sicherheit zu entwerfen, die weder die Funktionalität der Repositorien einschränken, noch das effiziente Arbeiten der Entwickler behindern.

Lösung

Der Lösungsansatz der TU Wien umfasst: einzelne gezielte Sicherheitsmaßnahmen für Informationsprozesse, den Einsatz erprobter Methoden für ein sicheres Design von Produktionssystemen (Security by Design) sowie die Erstellung angepasster Testverfahren zur raschen Identifizierung von Sicherheitslücken.

Bewährte Sicherheitskonzepte aus der Softwareentwicklung werden auf die Planung von Industrieanlagen übertragen. Daraus ergeben sich folgende wesentliche Einzelmaßnahmen:

- Integration von Sicherheitsfunktionalitäten in Industrie-Datenformate wie AutomationML
- effiziente Sicherung zentraler Datenrepositorien für den Engineering-Prozess
- maßgeschneiderte Modellierung realistischer Bedrohungsszenarien für Produktionssysteme
- Risikoabschätzung für geplante sowie bestehende Industrieanlagen (Security-Ontologie)
- Konzeption und Durchführung von Sicherheitstests im Rahmen der Test- und Verifikationsphase des Produktionssystems

Notizen

Ergebnisse

Erfahrungswerte aus der Softwarebranche zeigen, dass die Einführung eines sicheren Entwicklungszyklus nachweislich die Informations- und Betriebssicherheit verbessert. Ein solcher „Secure Software Development Lifecycle“ (SDLC) wurde beispielsweise von Microsoft im Jahr 2002 eingeführt. Bis zum Jahr 2008 hat sich die Anzahl an Schwachstellen in den neuen Betriebssystemen um 60% verringert. Es ist naheliegend, eine derart ganzheitliche und wirkungsvolle Sicherheitsstrategie auch für die Entwicklung und Planung von Produktionssystemen als neuen Stand der Technik zu etablieren.

Nutzen für Sie

Um Ihr Unternehmen vor Produktionsstillstand oder Imageschaden durch Schadprogramme zu bewahren, bietet die TU Wien Unterstützung und Projektkooperation bei folgenden Schritten an:

- Beratung bei der Einführung eines sicheren Entwicklungszyklus für Produktionssysteme
- Konzeption von sicheren Informationsprozessen
- Sicherheitsanalyse von Industrie-Komponenten
- Sicherheitsberatung für bereits bestehende Produktionssysteme
- Schulungen in der Netzwerkanalyse für die Erkennung von Angriffen auf eine Industrieanlage

Kontakt

Dr. Edgar Weippl
TU Wien - Information & Software Engineering Group
www.ifs.tuwien.ac.at
T: +43 1 58801 18888
edgar.weippl@tuwien.ac.at