PRESSEMITTEILUNG

Cyber Security in Industrieanlagen immer noch sträflich vernachlässigt – die Open Industry 4.0 Alliance liefert einen praktischen Handlungsrahmen

Europäische Unternehmen können sich mittels des Strategiepapiers zu „Cyber Security Design Principles" informieren, wie sie eine tiefgehende Sicherheit von der Werkshalle bis zur Cloud umsetzen

Reinach, Schweiz, 23. Februar 2021 – die Open Industry 4.0 Alliance hat ein strategisches Papier zu „Cyber Security Design Principles" in Industrieanlagen herausgegeben. Das Papier zeigt auf, welche ISO-/IEC-Standards zur Cyber Security eingebunden werden und auf welche Praktiken anderer Gremien und Allianzen wie etwa Cloud Security Alliance, FIRST, MITRE oder OWASP die Open Industry 4.0 Alliance bei der Umsetzung einer tiefgehenden, über alle Schichten reichenden Cyber Security setzt. Wie immer geht es der Allianz auch bei diesem Thema um praktische Handlungsanweisungen, wie „Security by Design" in einer transformierten Supply Chain umzusetzen ist. (Siehe Downloadlink unten) .

Cyber Security in Industrieanlagen nur wenig gegeben

Erpressung, Sabotage und Industriespionage sind die Hauptmotivation bei Angriffen auf Unternehmen und deren Infrastruktur. Absolut an die Substanz gehen Cyberangriffe auf Produktionsanlagen, die einen Produktionsstillstand auslösen. Die Industrie steckt in einem Dilemma: einerseits erfordert die digitale Transformation die Öffnung der Produktions- und IT-Systeme, andererseits fehlt es an Wissen und Praxis zur Umsetzung von Standards und Routinen, um die via Internet nun zugänglichen Anlagen entsprechend zu schützen. Eine Studie der KPMG von 2020 zeigt, dass erst ein Viertel der weltweit befragten 16.000 Unternehmen ihre industriellen Kontrollsysteme aktiv verteidigen. 58 Prozent der Unternehmen gaben überdies an, dass ihnen die Sicherheitskompetenz im Haus fehlt.

„Seit Veröffentlichung von Stuxnet in 2010 und der darauffolgenden Angriffe auf Produktionsanlagen und Komponentenhersteller in jüngster Vergangenheit ist klar, dass wir in Zukunft nicht ohne solide Absicherung von Industrieanlagen auskommen werden", erklärt Matthias Schmidt Co-Lead Technical Comitee Cyber Security der Open Industry 4.0 Alliance und Produktmanager Industrial Security bei ifm solutions. „In der Open Industry 4.0 Alliance geben wir den Mitgliedern jetzt eine Strategie an die Hand, wie sie die vorhandenen Security-Standards bei sich umsetzen können. Dabei bringen wir ISO-/IEC-Standards, Aufstellungen der MITRE zu Common Weaknesses, Empfehlungen der Cloud Security Alliance oder OWASP zur Cloud- und App-Sicherheit sowie des FIRST-Forums in einen strategischen Rahmen."

„Die Alliance definiert vier Schichten, jeweils zwei in der Werkshalle und in der Cloud", erklärt Dr. Stephan Theis, Co-Lead Cyber Security Group der Open Industry 4.0 Alliance und Geschäftsführer der nekst one GmbH. „Cyber Security findet in allen Schichten statt. Eine reine Software-Applikation auf Basis eines Containers kann beispielsweise keine Sicherheitsfunktionalitäten der darunter und darüber liegenden Schichten enthalten oder garantieren. Die von uns definierte Full Stack Secure Solution Architecture umfasst deshalb alle Ebenen, angefangen beim Egde Computing und Connectivity in der Werkshalle bis zur Cloud mit der Open Operator Cloud Platform und Common Cloud Central. Mittels dieses Ansatzes bekommen die Mitglieder der Alliance eine fundierte und solide Grundlage, um das Prinzip ‚Security by Design' in ihren Produkten und Lösungen systematisch umsetzen und anbieten zu können."

Sicherheit für die Operational Technology der Industrieanlagen

Wo es der IT schon schwer fällt, mit der Entwicklung im Cybersicherheitsbereich Schritt zu halten, scheinen die Unternehmen bei der Anlagentechnologie (OT; Operational Technology) und mit der Sicherheit bei Industriekontrollsystemen (ICS; Industrial Control ICS) überfordert. Das Whitepaper der Open Industry 4.0 Alliance zu „Industrial Cyber Security Design Principles" gliedert sich in folgende Inhalte:

- Rollen der Beteiligten wie Provider von Apps, Connectivity und weiterer Technologie sowie Herstellern, Systemintegratoren und schließlich Endanwendern und Service Providern
- Security by Design über alle Schichten mit der Full Stack Secure Solution Architecture
- eine Tabelle zu den eingebundenen Standards und Best Practices anderer Cyber Security Organisationen
- und einer Strukturierung der Anforderungen zur Security Compliance über die vier Schichten der Alliance von der Edge bis zur Cloud

Das Strategiepapier kann hier herunter geladen werden: https://openindustry4.com/de/Your-Downloads.html

Bildmaterial:



Cybersecurity in der Werkshalle: Schwieriger Spagat zwischen IT und Anlagentechnik (OT) © KUKA Group
Matthias Schmidt Co-Lead Technical Comitee Cyber Security der Open Industry 4.0 Alliance und Produktmanager Industrial Security bei ifm solutions
Stephan Theis, Co-Lead Cyber Security Group der Open Industry 4.0 Alliance und Geschäftsführer der nekst one GmbH

Bilder in hoher Auflösung bitte bei Berkeley anfordern.

LinkedIn: Besuchen Sie https://www.linkedin.com/company/open-industry-4-0-alliance/
Hashtag: #OI4Alliance

Ansprechpartner für die Presse:
Karl H. Mayer, Berkeley Kommunikation
Tel. +49 89-747262-12 / derzeit lieber mobil +49 172-8415419
E-Mail: karl.mayer@berkeleypr.com

Ulrike Götz, Open Industry 4.0 Alliance PR Lead
Tel. +0170 70 69 613
E-Mail: Ulrike.Goetz@kuka.com

Nils Herzberg

Sprecher des Vorstands Open Industry 4.0 Alliance
Global Head Strategic Partnerships for Digital Supply Chain and Industry 4.0 SAP
E-Mail: info@openindustry4.com

Über die Open Industry 4.0 Alliance

Die Open Industry 4.0 Alliance agiert als ein partnerschaftlicher Zusammenschluss führender, europäischer Industrieunternehmen, die sich pragmatisch an der Umsetzung herstellerübergreifender Industrie-4.0-Lösungen und -Services für Fertigungsanlagen und automatisierte Warenlager beteiligen. Die Allianz wurde im April 2019 ins Leben gerufen. Der Vereinssitz ist Reinach, Schweiz.

Weitere Informationen finden Sie unter https://www.openindustry4.com/