PRESS RELEASE

Cyber security in industrial plants still recklessly neglected - the Open Industry 4.0 Alliance provides a practical framework for action

European companies can learn how to implement deep security from the factory floor to the cloud through the Cyber Security Design Principles policy paper.

Reinach, Switzerland, 23 February 2021 - the Open Industry 4.0 Alliance has published a strategic paper on "Cyber Security Design Principles" in industrial plants. The paper shows which ISO/IEC standards on cyber security are integrated and which practices of other bodies and alliances, such as Cloud Security Alliance, FIRST, MITRE or OWASP, the Open Industry 4.0 Alliance relies on for the implementation of deep cyber security across all layers. As always, the Alliance is also concerned with practical instructions on how to implement "security by design" in a transformed supply chain. (See download link below) .

Little cyber security in industrial plants

Blackmail, sabotage and industrial espionage are the main motivations for attacks on companies and their infrastructure. Cyber attacks on production facilities that trigger a production standstill are absolutely crucial. The industry is in a dilemma: on the one hand, the digital transformation requires the opening of production and IT systems, but on the other hand, there is a lack of knowledge and practice to implement standards and routines to appropriately protect the facilities that are now accessible via the internet. A 2020 study by KPMG shows that only a quarter of the 16,000 companies surveyed worldwide actively defend their industrial control systems. Moreover, 58 per cent of the companies stated that they lack in-house security expertise.

"Since the publication of Stuxnet in 2010 and the subsequent attacks on production plants and component manufacturers in the recent past, it has become clear that we will not be able to manage without solid protection of industrial plants in the future," explains Matthias Schmidt, Co-Lead Technical Committee Cyber Security of the Open Industry 4.0 Alliance and Product Manager Industrial Security at ifm solutions. "In the Open Industry 4.0 Alliance, we are now providing members with a strategy on how they can implement the existing security standards. In doing so, we bring ISO/IEC standards, MITRE's lists of common weaknesses, recommendations from the Cloud Security Alliance or OWASP on cloud and app security and the FIRST Forum into a strategic framework."

"The Alliance defines four layers, two each on the factory floor and in the cloud," explains Dr Stephan Theis, Co-Lead Cyber Security Group of the Open Industry 4.0 Alliance and Managing Director of nekst one GmbH. "Cyber security takes place in all layers. A pure software application based on a container, for example, cannot contain or guarantee any security functionalities of the layers below and above it. The Full Stack Secure Solution Architecture we have defined therefore encompasses all layers, starting with egde computing and connectivity on the factory floor and extending to the cloud with the Open Operator Cloud Platform and Common Cloud Central. This approach provides Alliance members with a sound and solid basis for systematically implementing and offering the principle of 'security by design' in their products and solutions."

Safety for the operational technology of industrial plants

Where IT is already struggling to keep up with developments in cyber security, companies seem overwhelmed with plant technology (OT; Operational Technology) and industrial control system (ICS; Industrial Control ICS) security. The Open Industry 4.0 Alliance white paper on "Industrial Cyber Security Design Principles" is divided into the following contents:

- Roles of stakeholders such as providers of apps, connectivity and other technology as well as manufacturers, system integrators and finally end users and service providers.
- Security by Design across all layers with the Full Stack Secure Solution Architecture
- a table on the integrated standards and best practices of other cyber security organisations
- and a structuring of the requirements for security compliance across the four layers of the Alliance from the edge to the cloud.

The strategy paper can be downloaded here: https://openindustry4.com/de/Your-Downloads.html

Picture material:



Cybersecurity on the factory floor: difficult balancing act between IT and Operational Technology (OT) © KUKA Group
Matthias Schmidt Co-Lead Technical Comitee Cyber Security of the Open Industry 4.0 Alliance and Product Manager Industrial Security at ifm solutions
Stephan Theis, Co-Lead Cyber Security Group of the Open Industry 4.0 Alliance and Managing Director of nekst one GmbH

Please request high-resolution images from Berkeley.

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

Media contacts:
Karl H. Mayer, Berkeley Communications
Phone +49 89-747262-12 / mobile +49 172-8415419
E-mail: karl.mayer@berkeleypr.com

Ulrike Götz, Open Industry 4.0 Alliance PR Lead
Tel. +49 170 70 69 613
E-Mail: Ulrike.Goetz@kuka.com

Nils Herzberg
Spokesman of the Executive Board Open Industry 4.0 Alliance
Global Head Strategic Partnerships for Digital Supply Chain and Industry 4.0 SAP
E-mail: info@openindustry4.com

About the Open Industry 4.0 Alliance

The Open Industry 4.0 Alliance acts as a partnership of leading European industrial companies that pragmatically participate in the implementation of cross-vendor industry 4.0 solutions and services for manufacturing facilities and automated warehouses. The alliance was launched in April 2019. The association is headquartered in Reinach, Switzerland.

Further information can be found at https://www.openindustry4.com/