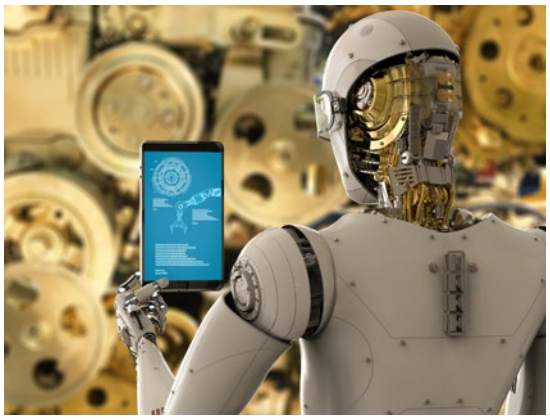
Focus

THE INVULNERABLE MACHINE



© Fotolia | phonlamaiphoto

A company suffering from a cyber attack: This is a scenario the new VDMA Competence Center Industrial Security will be dealing with. It is working on making machines invulnerable.

By Katrin Pudenz

“A cyber-attack recently halted a company’s production,” outlines Steffen Zimmermann, security expert at VDMA. “The interesting part is that the putative attack came from the IT administrator who was doing his job scanning for vulnerabilities,” he continues. One can only imagine what would happen if such an attack was really meant to do harm. These are the scenarios and issues Zimmermann and the new Competence Center Industrial Security will be dealing with. Zimmermann was made Head of the Competence Center.

“Industrie 4.0 and the digitalization of value-added processes lead to a dependence of industrial systems on software, data structure and communication networks,” says Zimmermann. “Manufacturers of components, mechanical engineering companies, integrators of production systems and services as well as the system operators need to consider how they can secure a network that includes several companies. We address the resulting and growing need for competency in the industry by establishing the VDMA Competence Center Industrial Security,” explains Zimmermann. He sees one of the central challenges for the industrial future being the reliable and secure operation of digitally linked production systems and services.

The purpose of industrial security is to protect industrial communication and production systems. “After all, the industry should be able to produce securely and reliably,” Zimmermann explains, adding that mechanical and plant engineering takes on a dual role in this regard. On the one hand, it is an operator of machines and systems, aiming to digitalize its own production processes. On the other, it develops new machines, systems, services and business models for its customers as integrator of Industrie 4.0. “Mechanical and plant engineers have great responsibility when defining security requirements and developing, implementing and updating measures,” Zimmermann emphasizes.

Why security is so important

In the VDMA security survey from 2013, 29 percent of the surveyed members reported a loss of production due to security problems such as viruses. Many companies in mechanical and plant engineering have since developed new services. One worthy of mentioning here is predictive maintenance. Predictive maintenance relies on operating data which must always be correct and available at the right time and place. If these requirements are not met, mechanical and plant engineers cannot offer predictive maintenance as a reliable and high-quality service. Two of the most important goals of industrial security are therefore integrity and availability.

VDMA member Siemens, for example, combined its expertize with Intel Security in order to protect industrial systems from cyber threats. Siemens experts use Intel Security solutions such as anti-virus software, whitelisting or security information and event management (SIEM). This way, experts can identify security-related incidents more quickly, inform plant operators faster and support countermeasures. The goal of this combination is to support industrial companies in minimizing risks and increasing the availability of systems with products and services.

In addition, mechanical and plant engineers must ensure confidentiality so that other competitors cannot carry out the service. This means that companies face the challenge of having to ensure integrity, availability and confidentiality over the entire duration of the service - starting out with the planning of the service on to the provision of the machine and finally the permanent operation.

At the same time companies need to embed their existing, often self-sufficient and statistical systems into agile communication structures. The machines and systems are not made for that purpose and often upgraded or converted under time pressure, but the legally and technically necessary requirements of standards and data security are often not adapted accordingly.

Compiling knowledge instead of actionism

Compilation of knowledge is more important in the context of industrial security than actionism. The earlier that companies integrate knowledge about potential threats, necessary measures and useful sources of information into the product lifecycle, the more sustainable and reliable the implementation measures will be.

Promoting the transfer of knowledge

“We have realized that industrial security is a core competence for the association and its members,” emphasizes Zimmermann. “We launched the Competence Center Industrial Security in order to pool the resources and skills needed here. Our goal is to establish a sustainable transfer of association-related and external topics such as the standardization or political representation of interests.” According to Zimmermann, the main task for the young committee will be to unite existing structures within VDMA and its trade associations. In the medium term, the Competence Center Industrial Security will be supported by a committee of mechanical engineers in regard to strategic issues. “This will make the Competence Center Industrial Security the first point of contact for members, authorities and policymakers,” explains Zimmermann.

Hygiene factor for future products

Industrial security is a strategic issue that affects all members and thus all trade associations of VDMA. Furthermore, knowledge deficits in politics and standardization confronts a host of knowledge, for example from experts in member companies. Last but not least, industrial security will become a hygiene factor for future products and services and will be included in the mechanical engineers’ operating instructions or the General Purchassing Conditions of the system operators.

Additional Information

VDMA has launched various committees on the topic of industrial security and information security. The VDMA Competence Center Industrial Security was founded in early 2017 and serves as a central contact for politics, science, standardization and member companies.

In addition, the VDMA task force Industrial Security forms the central network of manufacturers, integrators, operators, researchers and authorities. It serves the transfer of knowledge on security in production and automation.

Not least, the VDMA task force Information Security brings together information security officers from mechanical and plant engineering. In this committee, they exchange their expertise on traditional office IT and corporate security.

In 2016, VDMA published the Guideline Industrie 4.0 Security and created a digital learning course together with the start-up University4Industry from Munich. VDMA members can register on the company’s website and participate in the security learning course free of charge. ■

Further Information

VDMAimpulse | vdma.org: Industrial Security | VDMAimpulse 03-2017: “Securely networking existing machinery” | VDMAimpulse 03-2017: “Innovative risk management with CMDB” | VDMAimpulse 01-2016: “Security - A moving target”

Contact

Steffen Zimmermann, Head of VDMA Competence Center Industrial Security,
E-Mail: steffen.zimmermann@vdma.org

About VDMAimpulse

Read the magazine online: www.vdmaimpulse.org

VDMAimpulse is an international online magazine addressing the mechanical engineering and machine manufacturing industry. VDMAimpulse will be published every other months on or around the last Wednesday in January, March, May, July, September and November. If you want to receive an e-mail every time the new issue of the magazine is published, please contact the editorial office: VDMAimpulse@vdma.org