

PRESS RELEASE

Postadresse: Lyoner Straße 18
60528 Frankfurt am Main
GERMANY
Telefon +49 69 756081-0
Telefax +49 69 756081-11
E-Mail presse@vdw.de
www.metav.de

From Sylke Becker
Phone +49 69 756081-33
Telefax +49 69 756081-11
Email s.becker@vdw.de

Security by Design now in machine tools

Increased demand for IT security solutions expected at METAV 2022

Frankfurt am Main, 3 February 2022. – When the German Federal Office for Information Security (BSI) issues a top-level cyber security alert, industry sits up and takes note. A "critical vulnerability" in the widely used Java library Log4j was "readily exploitable" and allowed "the affected system to be completely taken over," the BSI wrote in its warning a few weeks ago. This is just what cybercriminals have been waiting for – and a nightmare for many companies. The extent of the potential threat has not yet been determined, as hackers could potentially smuggle a code into the system but then wait weeks or months before activating it. At the VDW (German Machine Tool Builders' Association), however, the warning arrived right on cue for those currently working urgently on promoting greater security throughout the industry and on producing a guideline for the systematic Incorporation of IT security into machine tools. Meanwhile, exhibitors at the upcoming METAV 2022 in Düsseldorf (new dates: June 21-24) are expecting increased demand for security solutions.

Growing threat

According to Prof. Felix Hackelöer, professor of Smart Automation in the Faculty of Computer Science and Engineering Science at TH Köln, the Log4j security flaw provides a good example of the growing threat which is directly targeting industry. In information technology, errors and vulnerabilities can quickly affect multiple systems due to the large number of different systems involved, Hackelöer said. This is especially true for standard components not directly involved in value creation, such as the logging functions in the case of Log4j.

However, deploying less common software systems is not a viable option for Hackelöer. "The high scaling factor of IT is both a curse and a blessing," explains the scientist. In addition to being highly cost-efficient, the software is deployed by millions of users. This ensures that vulnerabilities can be detected and updates offered relatively quickly. However, the never-ending race against hackers and the danger of sensitive data falling into the wrong hands remain. Companies can be blackmailed or spied on as a result, both of which can threaten their very existence. The only way to counter this is for the companies to protect themselves effectively, both externally and internally. The companies can pose a potential threat themselves through careless handling of machines and peripherals, as well as through conscious or unconscious manipulation.

IT security – a concern for all

Last year, the VDW's Research and Technology department produced the first version of a guide. Entitled "IT Security in Machine Tools", it contained practical tips and was aimed primarily at users. Hackelöer was involved in this, too, as a consulting expert. Working Group 2 *Control and Systems Engineering* of the VDW Research Institute deals with safety and security issues. A further guide is in the works, this time aimed at producers of machine tools and manufacturing equipment.

"We initially focused on functional safety, i.e. the safety of people using the machine, and tried to separate this from IT security," explains Eberhard Beck, head of Control Technology at Index-Werke, Esslingen, and Chairman of VDW Working Group 2. In the meantime, however, it has become clear that the functional safety of a machine can only be maintained if it has fully functioning IT security. "It's an issue that affects all areas," Beck notes. "You can neither define its limits nor shift responsibility for it to others. It affects everyone."

Situation compounded by heterogeneity of machine tools

According to Beck, the consequence is that the working group is now dealing almost exclusively with security issues. And the reasons are obvious. Manufacturing in general, and machine tools and systems in particular, are undergoing an inexorable process of digital transformation. Control components that previously functioned as stand-alone solutions are now networked throughout the company, interconnected via the Internet, or interacting with software services in the cloud. Compounding the problem is the fact that the world of machine tools is much more heterogeneous than the IT world, says Beck. "IT professionals view the world from a PC that typically is rarely more than two years old and runs on the latest operating system, while machine tools are unique products tailored specifically to a particular application." Many are still mechanically intact and in use even after decades in production, he said. And the machine control systems could be based on a design which is a decade or so old, when cybercrime was not yet an issue.

In order to protect existing machines, it isn't enough simply to install a new operating system if the software provider no longer offers security updates for the old version, says Beck. The task is so challenging that an entirely new business field has developed in response. There are now suppliers which specialize in the retrofitting of existing machines, as can also be experienced at METAV 2022. In the future, however, the main focus must be on integrating security solutions into the development of a machine in such a way as to ensure its resilience over its entire life cycle.

Security by Design

A software development method known as *Security by Design* has taken root. It has been in use for several years now. In mechanical and plant engineering it is applied in the international standard IEC 62443. This standard has established itself as the benchmark for IT security over the entire lifecycle of automation solutions.

Until now, machine builders have not been required to comply with this standard, explains Hackelöer. This is because they have no control over the environment in which the machine is operated and the standard was initially created for plant engineering and critical infrastructures. Furthermore, the standard is still relatively new. Hackelöer is certain, however, that it is now set to gain acceptance in the machine tool industry. "Customers are now applying it in mechanical engineering," he notes.

Customers driving demand for increased security

Dr. Andreas Kahmen, Head of Control Development for Machine Platforms at Trumpf Werkzeugmaschinen, also confirms the increased demand for security solutions. Kahmen is a member of VDW Working Group 2 and will be present on the Trumpf stand at METAV 2022 in Düsseldorf as a partner company of the *umati initiative*. "We are convinced that networking is the key to unlocking potential for production in the future," says Kahmen. From an early stage, Trumpf began offering BSI-certified security solutions. As early as the mid-2000s, a security concept based on a hardware component with an integrated firewall was developed to protect the machine network from unauthorized access. The firewall allowed access for remote service, but blocked all other access. At that time, there was very little demand for security solutions, but that has changed noticeably. Demand came not only from large companies in the automotive industry, for example, but also – and primarily – from smaller companies. Customers are now increasingly aware of IT security.

The fact that the security work conducted by VDW Working Group 2 has proved to be a "long and rocky road" is due more to the complexity of the issue than any lack of

interest. Awareness levels need to be raised on such security matters. This applies not only to customers but also to machine manufacturing companies and IT experts, some of whom believe rather naively that the problems are easy to solve. "That's when you have to explain that it isn't possible simply to run a virus scanner on a machine tool by default. That requires so much short-term computing power that it could affect the machine's behavior," says Kahmen. Hackelöer also notes that "translation work" represents an important aspect of the scientific work at the interface between IT and industry. Anyone seeking to raise IT security levels in the machine tool industry must ensure that they speak the technical language of the machine manufacturers, he says.

From expert knowledge to comprehensible guide

The new "Guide to the Systematic Implementation of IT Security in Machine Tools", for example, explains step by step how to determine the necessary security measures for a particular machine tool. Work on the guide is being spearheaded by Ralf Reines, an expert in the VDW's Research and Technology department. The guide states that machine manufacturing companies, customers and component suppliers carry joint responsibility for ensuring that each machine tool has a safety/security level that meets the requirements of the respective operating environment and operator.

Hackelöer, who is also involved in the development of the guide, believe that the time is ripe for promoting security topics – including at METAV 2022 – and for considering the sector's response to the IEC 62443 standard. "You can never have 100 percent protection," he acknowledges. "However, it is important to assess the threat of cyberattacks in particular use cases and to identify what measures can be taken against them." A sound knowledge of the processes and methods is indispensable for coping with the complexity involved. "It is good that the VDW is addressing this issue and ensuring transparency," says the scientist. IT security is attracting maximum attention following the BSI's latest red alert.

9.535 characters

Author: Cornelia Gewiehs, freelance journalist, Rotenburg (Wümme)

Contact persons

VDW (German Machine Tool Builders' Association)

Gerda Kneifel

Press and Public Relations

Lyoner Straße 18

60528 Frankfurt am Main

GERMANY

Tel. +49 69 756081-32

g.kneifel@vdw.de

www.vdw.de

Index-Werke GmbH & Co. KG Hahn & Tessky

Eberhard Beck

Head of Control Engineering

Plochinger Straße 92

73730 Esslingen

GERMANY

Tel. + 49 711 3191-0

eberhard.beck@index-werke.de

www.index-werke.de

Technische Hochschule Köln

Prof. Felix Hackelöer

Institute for Automation & Industrial IT

Campus Gummersbach, Steinmüllerallee 1

51643 Gummersbach

GERMANY

Tel. +49 221 8275-6493

felix.hackeloer@th-koeln.de

www.th-koeln.de

Trumpf Werkzeugmaschinen GmbH + Co. KG

Dr. Andreas Kahmen

Head of Control development machine platforms

Johann-Maus-Straße 2

71254 Ditzingen

GERMANY

Tel. +49 7156 303-0

andreas.kahmen@trumpf.com

www.trumpf.com

Background

METAV 2022 will take place from 21 to 24 June in Düsseldorf. It will showcase the entire spectrum of production technology. The main focuses are on machine tools, tools, accessories, measuring technology, surface and computer technology for metalworking, software, machines and systems for additive manufacturing, production systems and components for medical technology. In addition, METAV 2022 will highlight specific solutions in four theme areas: Additive Manufacturing, Medical, Moulding and Quality. METAV 2020 had to be cancelled due to the COVID pandemic and was held as a digital event in 2021.

Detailed information, offers and registration documents for METAV 2022 are available at www.metav.de

https://www.metav.com/en/Press/Latest_Information/VDW_Press_Releases

<https://medianet.messe-duesseldorf.de/press/metav>

You can also visit the METAV via our social media channels



<http://twitter.com/METAVonline>



<http://facebook.com/METAV.fanpage>



<http://www.youtube.com/metaltradefair>



<https://de.industryarena.com/metav>



www.linkedin.com/company/metav-duesseldorf