PRESS RELEASE

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

Corneliusstraße 4
60325 Frankfurt am Main
GERMANY
Telefon +49 69 756081-0
Telefax +49 69 756081-11
E-Mail presse@vdw.de
www.metav.de

IT security in production – A major challenge for machine manufacturers

Cyber Security Congress at METAV 2020 aims to shed light

Frankfurt am Main, 29 January 2020. – Almost daily reports of hacker attacks are unnerving the public. According to the results of a Deutsche Telekom survey, nearly two thirds of German companies have fallen victim to hacking at least once. The mechanical engineering industry, too, is experiencing a significant increase in attacks on its production facilities. Steffen Zimmermann, Head of the VDMA Industrial Security Competence Center, explains how, in a recent VDMA survey, more than a third of the members who responded reported suffering production losses due to hacker attacks, and more than half the companies complained of capital losses. The alarm bells should now be ringing in every company. Better prevention is called for – as is a list of experts who can quickly be called in to provide support in the event of an attack.

Natalia Oropeza, Chief Cyber Security Officer of Siemens AG, says: "You have to be aware of the risks associated with infrastructure products – and also be prepared to respond to them. Ignoring them can destroy your business." Oropeza is set to give the keynote speech at the VDMA and VDW Cyber Security Congress on 11 March 2020 at METAV in Düsseldorf. She will talk about security in the age of Industry 4.0 and the importance of Security by Design. This must include the entire supply chain if trustworthiness is to be ensured. Industry, manufacturers and users need technological transparency and homogeneous requirements across different markets.

Who carries responsibility for data security?

The majority of machines will be linked to the Internet in the future. This will confront all the relevant parties – machine manufacturers, component suppliers, machine operators and possibly also service providers – with completely new challenges. Productivity, robustness, longevity and reliability were once the main priorities, whereas IT security is now gaining in significance. Practical experience shows that there are many different potential security vulnerabilities. "In many cases it isn't major hacker attacks that pose the greatest threat in everyday production," says Dr. Alexander Broos, Head of Research and Technology at the VDW. "Rather it's the regular and unavoidable exchange of data via the USB interface of the controller, for instance, which provides the gateway into the system." It is relatively easy for IT experts to offer instant solutions, such as simply closing the USB interface. "However, this prevents efficient use of the machine," Broos continues. Service technicians, for example, need to be able to read out error logs and install updates. This is because automatic updating of the control software, as happens in the operating system of the office PC, is relatively unusual in production equipment. Life cycles of ten years and more are by no means a rarity in machines and control systems. In

addition, the control software for complex products like machine tools is highly customised and is specially adapted to particular applications. The question therefore arises as to who is responsible for closing security gaps. "The responsibility is shared to varying degrees between the machine manufacturers, control suppliers and operators," Broos continues. "Ultimately, however, the responsibility can only be met by all these together."

Bernd Gehring, in charge of Industrial Security at Voith AG in Heidenheim, adds: "There is a risk of the software in older machines being completely outdated, and of the manufacturers providing no further updates. Accordingly, companies are well advised to prepare for digital maintenance of their machines at an early stage." The operators, whose safety requirements machine manufacturers have to meet, are increasing the pressure, he believes, as are the standards that stipulate secure IT systems. These are indispensable in areas such as remote maintenance. He also points out that major investment is sometimes necessary in order to ensure machine security. However, there is often no initial return on such investment.

Cyber Security Congress at METAV aiming to raise transparency levels and sensitivity to security gaps

At the VDMA and VDW Cyber Security Congress to be held during METAV 2020, high-calibre speakers – e.g. from Siemens, the ZF Group, the German Federal Office for Information Security, Voith, Trumpf and Deutsche Telekom – will be talking about particular cyber security challenges in the automotive industry, the potential opportunities of security systems, and risk management solutions.

"We are particularly targeting managing directors and product managers from industrial companies with a strong culture of innovation.

They are especially at risk, and security needs to be tackled at the highest level," summarises Steffen Zimmermann. Nevertheless, there is no such thing as 100 per cent security, given that the target is constantly moving and that hackers are constantly adapting their methods. Machine manufacturers need to collaborate with component suppliers and operators to make production processes more secure. The Industry 4.0 business model can only work if digital services are made absolutely secure. All the contributing partners share a strong and common interest in this.

((Box Text))

Cyber Security Congress

When:	Wednesday, 11 March 2020, 10:30 until 14:30
Where:	METAV 2020, Düsseldorf Exhibition Centre, Stockumer Kirchstraße 61, Hall 1, Room 14
Fee:	€ 89.00 plus VAT.
Bookings:	v.hoffmann@vdw.de
Further information:	metav.de or https://www.metav.com/en/METAV_2020/Supporting_Programme/Cyber_Security_Congress

Background – METAV 2020 in Düsseldorf

METAV 2020 - 21st International Trade Fair for Metalworking Technologies displays the full spectrum of manufacturing technology. The focus is on machine tools, manufacturing systems, precision tools, automated material flows, computer technology, industrial electronics and accessories. Added to this are new topics such as Moulding, Medical, Additive Manufacturing and Quality. They are firmly established in so-called Areas in the METAV exhibition programme, each with its own nomenclature. The target group of METAV visitors includes all branches of industry that process metals, in particular mechanical and plant engineering, the automotive and supply industry, the aerospace sector, the electrical industry, energy and medical technology, tool and mould making as well as metalworking and trades.

Articles and pictures relating to METAV can be found in the Press section at https://www.metav.com/en/Press/Overview_Press

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