Die Welt der Metallbearbeitung
The world of metalworking

EMO Hannover
16-21·9·2019

PRESS RELEASE

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

Protecting machine tools from cyber attacks

EMO Hannover 2019 showcasing solutions for complex networked systems

Frankfurt am Main, 09. July 2019. *– Data security is gaining in importance as Industry 4.0 takes shape. Automation, cloud applications and globally networked machines and components play key roles when it comes to shielding systems from external threats.*

As digitalisation becomes more prevalent across industries, there is a growing need for companies to safeguard against cyber risks. This is because German industry is increasingly becoming a target for cybercriminals: more than eight in ten industrial companies (84 per cent) have reported an increase in the number of cyber attacks in the past two years, with more than a third (37 per cent) reporting a strong increase. This is the result of a 2018 survey conducted by the Bitkom digital association, which interviewed 503 managing directors and security officers from all sectors of industry. "German industry is under constant digital fire – from petty digital criminals, organised crime and even state-backed hackers," says Bitkom President Achim Berg. "The nature and scale of the cyber attacks is set to increase."

One thing is certain, however: cybercrime is a worldwide phenomenon that does not stop at national borders or at locked factory gates. It can happen wherever people use computers, smartphones or other IT devices.

Responding to security vulnerabilities and software bugs

The Balluff Group is a global player in the automation sector. With its workforce of 4,000 employees the company offers a comprehensive portfolio of sensor, identification, network and software solutions for all areas of automation. Protecting against cybercrime is a key aspect in the development and design of customer solutions.

"Cybercriminals often use known vulnerabilities or bugs in outdated software to gain access to a system. "Promptly installing updates and security patches considerably reduces the risk of cyber attacks," says Philipp Echteler, IIoT Strategy Manager at Balluff. Using versioned software and firmware and monitoring these help create greater transparency. "Avoidable dangers also emanate from devices that were originally only designed for communication with the controller of isolated networks, and not for connection to the Internet. Many of these Ethernet-enabled automation devices have no protection features, which leaves them vulnerable to attack," continues Echteler.

Protecting systems from manipulation and cybercrime

But what are the best ways to protect complex networked systems against manipulation and cybercrime? "In principle, any networked system represents a possible point of attack. a well-designed security concept is therefore indispensable for safeguarding such systems against manipulation and cybercrime," says Juliane Schneider, Junior Product Manager at Symmedia. Symmedia GmbH from Bielefeld has been developing service solutions for the mechanical engineering sector since 1997. The company's digitalisation expertise – especially in the field of mechanical and plant engineering – is strengthened by its alliance with Georg Fischer, a mechanical engineering company to which Symmedia has belonged since 2017.

"When it comes to handling sensitive data, any human negligence poses a security risk. An unnoticed cyberattack, the reckless multiple use of passwords or the deliberate divulgence of confidential data – any human action can have major consequences and cause significant damage," says Schneider, listing just some of the more obvious risks. Echteler adds: "The risks which arise from internal threats should not be underestimated. Employees unthinkingly open email attachments which can be used to smuggle in viruses unnoticed, or they send critical company information in unencrypted form by email." Poorly protected or forgotten maintenance access routines represent back doors that attackers can then use for their own purposes.

Firewalls that automatically conduct trustworthiness checks

Encryption mechanisms such as SSL or TLS must be deployed as standard in order to protect complex networked systems from manipulation and cybercrime. These encrypt all data traffic between servers, computers and applications in a network. Another common practice is to install a firewall which checks the trustworthiness of all parties seeking access to a computer in order to automatically protect it from attacks or unauthorised access.

"Having separate production and office networks offers additional security. Further recommendations include minimising the number of network accesses and routing the data stream via a central, monitored gateway. Potential threats can often be identified at an early stage if data and network traffic levels and individual nodes are also continuously analysed," says Echteler, citing further options that can help increase security.

Solutions for data security in networked production

Balluff has established its own team of experts to offer comprehensive consulting services to customers all over the world. Some of the Balluff devices now also feature hardware encryption based on the Trusted Platform module. In addition to minimum requirements such as firewall protection, Symmedia also uses HSM and TPM procedures (based on so-called hardware security and Trusted Platform modules) to ensure that only secure software is run. "We also use a proprietary network protocol to provide very high level protection against unwanted access. It is virtually impossible to hack into these connections," says Schneider.

The company uses a secure and workflow-based point-to-point link for digital service support. "The use of common encryption, authentication and authorisation procedures for client applications, servers and programming interfaces, so-called APIs, is also a matter of course for us. In addition, we offer many other security measures, including a PKI (public key infrastructure)-based individual machine and user certificate structure, password rules, the irreversible storage of access data with up-to-date hash procedures and multi-factor authentication," continues Juliane Schneider.

Clouds and corporate clouds have a role to play

Another major point with regard to data handling is the location of the data storage. Three in ten companies (29 per cent) use a cloud solution that is outsourced to a certified data centre – either to achieve possible cost savings, to relieve the strain on their own IT staff or to obtain greater security. Another ten per cent plan to do so and 28 per cent are discussing this as an

option. This is shown by the Digital Office Index 2018 – a representative survey of 1,106 Bitkom companies with 20 or more employees. According to the Index, fewer than three in ten companies (28 per cent) state that cloud hosting is of no concern to them. A comparison of the different industries reveals that the mechanical engineering and plant construction sector is the frontrunner in this field. According to Bitkom, almost half of all companies in this industry (46 per cent) are already using external cloud service providers.

For Balluff, too, the public cloud is the first choice. "Its high availability is attractive because its platforms are replicated in independent, geographically distributed data centres. Other advantages include its easy scalability, its high level of security, its use of state-of-the-art technologies and encryption, and its service continuity. These guarantee that the solutions will work even in the event of negative scenarios," emphasises IIoT Strategy Manager Echteler. From experience we know that it is not possible for a company's own IT staff also to run a cloud. This is a task for suitably qualified specialists.

Symmedia, on the other hand, offers its customers hybrid solutions. "This gives our customers flexibility combined with outstanding security. And this in turn gives them full data sovereignty," says Junior Product Manager Juliane Schneider. They can decide for themselves which data they want to store centrally, for example in a cloud, and which is only to be stored locally. "We have found that our customers are open to central solutions, but always want to be able to store specific data locally, depending on how sensitive it is."

Examples of data protection and security concepts at the EMO

At the EMO Hannover, Symmedia will be showcasing a digital factory to demonstrate its software's capabilities and show its practical applications in daily production. There will be live demonstrations, for example, of condition monitoring, alarm scenarios and remote services. Visitors will also be able to find out about predictive maintenance, data protection and security concepts, and pick up information on the use of Symmedia software across systems made by different manufacturers.

Balluff will be presenting productivity enhancement solutions in the metalworking field. These include innovative concepts for intelligent manufacturing systems. Chief among these are a retrofit tool management system and solutions for continuous machine tool process monitoring.

Author: Annedore Bose-Munde, specialist journalist from Erfurt

Size: around 9,800 characters including blanks

Contact persons

VDW German Machine Tool Builders' Association
Gerda Kneifel
Press and Public Relations
Corneliusstraße 4
60325 Frankfurt am Main
Germany
Tel. +49 69 756081-32
g.kneifel@vdw.de
www.vdw.de

symmedia GmbH
Nicole Wimmer, Press
Turnerstraße 27
33602 Bielefeld
Germany
+49 521 96655-50
wimmer@symmedia.de
www.symmedia.de

Balluff GmbH
Dr. Detlef Zienert, Specialised Press
Schurwaldstraße 9
73765 Neuhausen a.d.F
Germany
+49 7158 173-418
detlef.zienert@balluff.de
www.balluff.com

Bitkom - Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V
Andreas Streim, Press Spokesperson
a.streim@bitkom.org
Albrechtstraße 10
10117 Berlin-Mitte
Germany
+49 30 27576-0
bitkom@bitkom.org
www.bitkom.org

Annedore Bose-Munde
Specialist Journalist for Economics and Technology
Am Elsterberg 13
99094 Erfurt
Germany
Tel. +49 171 2684 366
info@bose-munde.de
www.bose-munde.de

EMO Hannover 2019 – the world's premier trade fair for the metalworking sector

From 16 to 21 September 2019, international manufacturers of production technology will be spotlighting smart engineering at the EMO Hannover 2019. Under the motto of "Smart technologies driving tomorrow's production!", the world's premier trade fair for the metalworking industry will be showcasing the entire bandwidth of modern-day metalworking technology, which is the heart of every industrial production process. The fair will be presenting the latest machines, plus efficient technical solutions, product-supportive services, sustainability in the production process, and much, much more. The principal focus of the EMO Hannover is on metal-cutting and forming machine tools, production systems, high-precision tools, automated material flows, computer technology, industrial electronics and accessories. The trade visitors to the EMO come from

all major sectors of industry, such as machinery and plant manufacturers, the automotive industry and its component suppliers, the aerospace sector, precision mechanics and optics, shipbuilding, medical technology, tool and die manufacture, steel and lightweight construction. The EMO Hannover is the world's most important international meeting point for production technology specialists from all over the planet. The EMO Hannover 2017 attracted almost 2,230 exhibitors from 44 different countries, and around 130,000 trade visitors from 160 nations. EMO is a registered trademark of the European Association of the Machine Tool Industries Cecimo.

You will find texts and images relating to the EMO Hannover 2019 on the internet at:
https://www.emo-hannover.de/en/press/press-releases/press-releases/press-releases.xhtml.
You can also follow the EMO Hannover using our social media channels

http://twitter.com/EMO_HANNOVER


https://de.industryarena.com/emo-hannover

www.linkedin.com/company/emo-hannover

http://www.youtube.com/metaltradefair


http://facebook.com/EMOHannover

If you no longer wish to receive our press releases, please click here.