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

Vigilance – The best protection against hacking

METAV 2020 offering expert knowledge on data security – Cybersecurity Congress highlighting challenges facing the office and production environments

Frankfurt am Main, 27 November 2019 - Digitalisation has its price. The networking of people, machines and companies not only increases productivity and sustainability, but also raises the risk of a cyber attack. The VDMA Cybersecurity Congress at METAV 2020 on 11 March 2020 offers potential ways of resolving this dilemma. Heinz-Uwe Gernhard is head of the VDMA Security working group and in his principal occupation is responsible for IT security at Robert Bosch in Stuttgart. In an interview he reveals his recipe for success: vigilance training for cyber attacks.

Mr Gernhard, has cyber security awareness increased?

Heinz-Uwe Gernhard: Yes, but not to the extent that I expected when we launched the Security Working Group in 2012. There is still urgent need for action because Germany and the EU are demanding measures for greater protection against cyber attacks, including in production, in the form of laws and

regulations. Deploying additional IT is certainly one way of achieving this. But without the necessary knowledge and organisational skills, this alone will not be enough to reach the necessary security levels. Industry 4.0 developments are certainly helpful here, but unfortunately cyber security is just one of many aspects.

What do you recommend to newcomers in this field?

Heinz-Uwe Gernhard: Just start taking precautions, both technical and organisational. It's a bit like the annual flu epidemic. You have a higher risk of getting it without a flu job. In today's networked world, no one is safe from cyber attacks. There needs to be a change of heart here.

Cyber attacks on the rise

What measures should companies that are currently undergoing an Industry 4.0 digital transformation process take?

Heinz-Uwe Gernhard: This is a task for management – clear and simple. The managers must identify the risks that are attached to networking and then define suitable measures. With regard to production technology availability, they must understand the risk of considerable damage being done. Interconnectivity means that nobody is immune. If you follow the trade press, there is a constant stream of news items on this – such as that of a cyber attack practically paralysing the IT of a specialist safety and control technology company. The company decided to go public with the incident. I think that's important and it's the right approach because we are all in the same boat.

Nevertheless, openness is still the exception when it comes to cyber attacks. To what extent can networks such as the VDMA Security Working Group, which you spearhead, help in this? By getting network members to talk openly to each other about cyber attacks?

Heinz-Uwe Gernhard: We take a proactive approach by clearly identifying the risks and providing assistance on a wide range of issues. I think it is crucial that we work together to ensure transparency across association boundaries. The Industry 4.0 platform link also offers a good starting point www.plattform-i40.de.

In many cases there is a lack of awareness.

Some companies are now starting to alert their employees to different fraud scenarios. What do you think of the new buzzword "cyber resilience" which is now making the rounds?

Heinz-Uwe Gernhard: This is the right approach, because awareness offers the best protection for this type of threat. Every user of cyber technologies should be cyber resilient.

Where do you think we are right now with security IT?

Heinz-Uwe Gernhard: Let me make a comparison with road vehicles. In 1920, motorists needed a completely different level of risk awareness to today's drivers because cars now demand much less attention as a result of all the built-in systems. The vehicles themselves and the infrastructure make driving today much less risky. Our IT is currently at the level of a 1920s car in terms of the inherent risks. It requires a high level of attention from users and a wide range of knowledge. Awareness is a key topic right now.

Isn't that scaremongering?

Heinz-Uwe Gernhard: No, it's not scaremongering, at all. Marc Elsberg's novel Blackout plays through various scenarios. The technical aspects he includes are not fictional, but reflect the current realities. He has merely packaged them in an exciting fictional work. The Government is also getting involved in the form of the IT Security Act (Kritis), which is currently being revised.

The IT expert Peter Turczak told VDMA magazine: "I would never put critical data into a cloud." However, companies need data in order to implement Industry 4.0 and need to store it securely. What belongs in the cloud and what doesn't?

Heinz-Uwe Gernhard: My IT colleague here is addressing the central requirement of OT (?) for availability. As a communications engineer, I am well aware of the competition between bandwidth, local computing power and, of course, cost. With the right bandwidth, the cloud can facilitate the provision of a centralised application with a great deal of computing power to a large number of users. Users must weigh the type of cloud usage against their willingness to take risks, their availability requirements, and their technical and organisational capabilities. Another important question, of course, is how to guarantee the dependability or trustworthiness of the provider.

So it's a question of trust?

Heinz-Uwe Gernhard: Yes, I need to ask myself whom I trust to do what. Do the technical measures, contracts and service provider certifications offer sufficient legal protection?

Most machine tools at METAV 2020 have Internet connections: What should trade fair visitors be looking out for here?

Heinz-Uwe Gernhard: Hopefully the link is not via an open Internet connection, but a trustworthy one, as I just mentioned. Don't just ask about the technical solution itself, but also about the provider's organisational capabilities. From a technical point of view, private VPN networks based on an appropriate contract are best here.

Standards can help

How can trade fair visitors prepare for their meetings?

Heinz-Uwe Gernhard: Help is provided by ISO/IEC 62443. Part 2-4 contains the "Security program requirements for IACS service providers" and provides a framework for the key aspects when considering offers. Otherwise, regulations and standards, even if they are often inflexible, can be helpful and effective here.

Mr Gernhard, thank you for talking to us.

VDMA - Cyber security through targeted interaction

Information technologies are a key element of almost every production plant today. "IT not only makes machines smart and interactive, but also more susceptible to cyber attacks," observes Steffen Zimmermann, Head of the VDMA's Industrial Security Competence Center. "In order to guarantee high machine availability and data integrity levels over the entire product life cycle, the suppliers of automation solutions and machines must also interact with the plant operator. Operators have to be aware of the constant threat of a cyber attack. This means they should take basic precautions to ensure their own cyber resilience as a means of reducing the impact of a cyber attack. The Cybersecurity Congress of VDW and VDMA at METAV 2020 on 11 March 2020, which focuses on the convergence of the office and production environments, will present the current state-of-the-art. The topics include: Regulation, remote maintenance/international networking, live hacking and basic measures for IT network restoration.

Curriculum vitae: Heinz-Uwe Gernhard

After studying Communications Engineering at TH Darmstadt, the young graduate Heinz-Uwe Gernhard (born 1957) joined the SEL electronics group as a developer In 1983,. From 1987 to 2017 Gernhard worked on the development of control technology at today's Bosch Rexroth Electric Drives and Controls GmbH in Erbach. He has been working in the central IT Security and Application (C/TED1) department at Robert Bosch GmbH in Stuttgart since 2017. Gernhard specialises in risk management and IT security for manufacturing.

((Size: around 8,160 characters incl. blanks))

Author: Nikolaus Fecht on behalf of the VDW

Contact persons

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

Robert Bosch GmbH
Heinz-Uwe Gernhard
IT Security and Application (C/TED1)
Robert-Bosch-Platz 1
70839 Gerlingen-Schillerhöhe
Tel. +49 711 400 40990

VDMA
Steffen Zimmermann
Head of Competence Center Industrial Security
Lyoner Straße 18
60528 Frankfurt
Tel. +49 69 6603-1978
steffen.zimmermann@vdma.org

Press Agency Nikolaus Fecht
Technik-Texte à la carte - wenn Ihnen die Worte fehlen
Husemannstraße 29

45879 Gelsenkirchen
Tel. +49 209 26575
fecht@erzfreunde.de

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 www.metav.de
https://www.metav.com/en/Press/Press_material/VDW_Press_Releases

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