PRESSEINFORMATION

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

von Sylke Becker
Telefon +49 69 756081-33
Telefax +49 69 756081-11
E-Mail s.becker@vdw.de

IT-Sicherheit in der Produktion ist große Herausforderung für Maschinenhersteller

Cyber Security Kongress auf der METAV 2020 will aufklären

Frankfurt am Main, 29. Januar 2020. – Fast täglich schrecken Meldungen über Hackerangriffe die Öffentlichkeit auf. Nahezu zwei Drittel der deutschen Unternehmen wurden bereits mindestens einmal gehackt, so das Ergebnis einer Befragung der Deutschen Telekom. Auch der Maschinenbau verzeichnet einen deutlichen Anstieg von Angriffen auf seine Produktionsanlagen. Steffen Zimmermann, Leiter Competence Center Industrial Security im VDMA, spricht von mehr als einem Drittel der befragten Mitglieder in einer VDMA-Umfrage, die von Produktionsausfällen berichten und mehr als der Hälfte der Firmen, die Kapitalschäden aufgrund von Hackerangriffen beklagen. Spätestens jetzt müssten bei den Unternehmen alle Alarmglocken schrillen. Bessere Prävention lautet das Gebot der Stunde. Und im Schadensfall sollten die Kontaktdaten von Experten, die schnell helfen können, griffbereit vorliegen.

Natalia Oropeza, Chief Cyber Securitiy Officer der Siemens AG, sagt: „Man muss die Risiken von Infrastrukturprodukten kennen – und auch auf sie eingehen. Sie zu ignorieren, kann das Geschäft vernichten." Oropeza hält die Keynote auf dem Cyber Security Kongress von VDMA und VDW am 11. März 2020 auf der METAV in Düsseldorf. Sie wird über Security im Zeitalter von Industrie 4.0 sprechen und die Notwendigkeit, Security by Design zu gewährleisten. Das gelte für die gesamte Lieferkette, um Vertrauenswürdigkeit sicherzustellen. Die Industrie, Hersteller und Anwender, benötigen dafür Transparenz der Technologien und möglichst homogene Anforderungen in unterschiedlichen Märkten.

Wer trägt die Verantwortung für Datensicherheit?

Weil künftig die Mehrzahl der Maschinen an das Internet angeschlossen sein wird, stehen alle Beteiligten, das sind Maschinenhersteller, Komponentenlieferanten, Maschinenbetreiber und ggf. auch Dienstleister, vor ganz neuen Herausforderungen. Ging es bisher in erster Linie um Produktivität, Robustheit, Langlebigkeit und Zuverlässigkeit, rückt nunmehr zusätzlich die IT-Sicherheit in den Blick. Die Praxis zeigt, dass vielfältige Sicherheitsschwachstellen bestehen können. „Im Produktionsalltag stellt häufig nicht der große Hackerangriff die Gefährdung dar", sagt Dr. Alexander Broos, Leiter Forschung und Technik im VDW. „Vielmehr ist es der tägliche, unvermeidliche Datenaustausch, z.B. über die USB-Schnittstelle der Steuerung, der das Einfallstor bietet." IT-Experten hätten hier sehr schnell Lösungen parat, indem sie beispielsweise die USB-Schnittstelle einfach dicht machen. „Das behindert dann jedoch die effiziente Nutzung der Maschine", sagt Broos weiter. So sind beispielsweise Servicetechniker darauf angewiesen, darüber Fehlerprotokolle auszulesen und Updates einzuspielen. Denn im Produktionsalltag seien permanente Updates der Steuerungssoftware, wie etwa beim Betriebssystem im Büro-PC, eher unüblich. Lebenszyklen

von Maschinen und Steuerungen erreichen leicht zehn Jahre und mehr. Außerdem ist die Steuerungssoftware bei einem so komplexen Produkt wie der Werkzeugmaschine hochgradig individualisiert und auf die jeweilige Anwendung angepasst. Nicht zuletzt deshalb entsteht die Frage, wer denn nun für die Schließung von Sicherheitslücken zuständig ist. „Es besteht ein Spannungsfeld zwischen Maschinenherstellern, Steuerungsanbietern und Betreibern," erläutert Broos weiter. „Letztendlich wird man dieser Verantwortung nur gemeinsam gerecht werden können."

Bernd Gehring, bei der Voith AG in Heidenheim für die industrielle Security zuständig, ergänzt: „Ältere Maschinen tragen das Risiko in sich, dass die Software auf einem völlig veralteten Stand ist und Hersteller oft keine Updates mehr zur Verfügung stellen. Deshalb sind Unternehmen gut beraten, sich frühzeitig auf die digitale Wartung ihrer Maschinen vorzubereiten." Er sieht steigenden Druck einerseits von den Betreibern, deren Sicherheitswünsche Maschinenhersteller erfüllen müssen, andererseits über Normen, die sichere IT-Systeme fordern. Bei Themen wie Fernwartung seien sie beispielsweise unabdingbar. Allerdings weist er darauf hin, dass für die Absicherung der Maschinen zum Teil größere Investitionen notwendig seien, die zunächst keinen zusätzlichen Cent abwerfen würden.

Cyber Security Kongress auf der METAV will Transparenz und Sensibilität für Sicherheitslücken erhöhen

Beim Cyber Security Kongress von VDMA und VDW auf der METAV 2020 sprechen hochkarätige Referenten von Siemens, der ZF Group, vom Bundesamt für Sicherheit in der Informationstechnik, von Voith, Trumpf und der Deutschen Telekom u.a. über besondere Herausforderungen in der Automobilindustrie im Hinblick auf Cyber Security, über

Chancenpotenziale von Sicherheitssystemen und Lösungen zur Risikobewältigung.

„Wir sprechen insbesondere Geschäftsführer und Produktverantwortliche aus Industrieunternehmen mit einer hohen Innovationskultur an. Sie sind besonders gefährdet, und Security ist Chefsache“, fasst Steffen Zimmermann zusammen. Gleichwohl gebe es keine 100-Prozent-Sicherheit, zumal sich das Ziel permanent verändert, weil Hacker ihre Methoden ständig anpassen. Maschinenhersteller müssten im Verbund mit Komponentenlieferanten und Betreibern gemeinsam daran arbeiten, Produktionsprozesse sicherer zu machen. Das Industrie 4.0-Geschäftsmodell könne nur funktionieren, wenn digitale Dienste dauerhaft abgesichert seien. Und daran haben alle beteiligten Partner höchstes Interesse.

((im Kasten))

Cyber Security Kongress

Wann:	Mittwoch, 11. März 2020, 10.30 bis 14.30 Uhr
Wo:	METAV 2020, Messegelände Düsseldorf, Stockumer Kirchstraße 61, Halle 1, Raum 14
Teilnahmegebühr:	89 Euro zzgl. MwSt.
Anmeldung:	v.hoffmann@vdw.de
Weitere Informationen:	metav.de bzw. https://www.metav.de/de/METAV_2020/Rahmenprogramm/Cybersecurity_Kongress

Hintergrund METAV 2020 in Düsseldorf

Die METAV 2020 – 21. Internationale Messe für Technologien der Metallbearbeitung zeigt das komplette Spektrum der Fertigungstechnik. Schwerpunkte sind Werkzeugmaschinen, Fertigungssysteme, Präzisionswerkzeuge, automatisierter Materialfluss, Computertechnologie, Industrieelektronik und Zubehör. Hinzu kommen die neuen Themen Moulding, Medical, Additive Manufacturing und Quality. Sie sind in so genannten Areas mit eigener Nomenklatur fest im METAV-Ausstellungsprogramm verankert. Zur Besucherzielgruppe der METAV gehören alle Industriezweige, die Metall bearbeiten, insbesondere der Maschinen- und Anlagenbau, die Automobil- und Zulieferindustrie, Luft- und Raumfahrt, Elektroindustrie, Energie- und Medizintechnik, der Werkzeug- und Formenbau sowie Metallbearbeitung und Handwerk.

Texte und Bilder zur METAV finden Sie im Internet unter
www.metav.de/de/Presse/ Übersicht_Presse

Besuchen Sie die METAV auch über unsere Social Media Kanäle

http://twitter.com/METAVonline

http://facebook.com/METAV.fanpage

http://www.youtube.com/metaltradefair

https://de.industryarena.com/metav