

PRESSEINFORMATION

von Sylke Becker
Telefon +49 69 756081-33
Telefax +49 69 756081-11
E-Mail 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



Aufmerksamkeit schützt vor Hackern

METAV 2020 bietet Expertenwissen zur Datensicherheit – Cybersecurity-Kongress zeigt Herausforderungen in der Office- und Produktionswelt

Frankfurt am Main, 21. November 2019 - Die Digitalisierung hat ihren Preis: Die Vernetzung von Menschen, Maschinen und Unternehmen erhöht nicht nur Produktivität und Nachhaltigkeit, sondern steigert auch das Risiko einer Cyberattacke. Wege aus dem Dilemma bietet der Kongress Cybersecurity des VDMA auf der METAV 2020 am 11. März 2020. Ein Erfolgsrezept verrät vorab Heinz-Uwe Gernhard, Leiter des VDMA-Arbeitskreises Security und im Hauptberuf bei Robert Bosch in Stuttgart zuständig für IT-Security im Interview: Schulung der Aufmerksamkeit für Cyberattacken.

Herr Gernhard, hat das Bewusstsein für Cybersecurity zugenommen?

Heinz-Uwe Gernhard: Ja, aber nicht in dem Ausmaß, den ich damals beim Start des Arbeitskreises Security im Jahr 2012 erwartet habe. Es besteht nach wie vor dringender Handlungsbedarf, denn Deutschland und die EU werden mit Gesetzen und Regelungen Maßnahmen zum besseren Schutz, auch der Produktion, vor Cyberangriffen einfordern. Ein Mittel zum Zweck ist sicherlich der

Einsatz von zusätzlicher IT. Aber ohne das dazugehörige Wissen und die organisatorischen Fähigkeiten wird das allein nicht ausreichen, um für eine Erhöhung der notwendigen Sicherheit zu sorgen. Hilfreich in diesem Zusammenhang sind sicherlich die Bemühungen im Kontext von Industrie 4.0, aber dort ist Cybersecurity leider auch nur ein Thema von vielen.

Was empfehlen Sie einem Einsteiger?

Heinz-Uwe Gernhard: Einfach anfangen und Vorsorge treffen, sowohl technisch als auch organisatorisch. Das ist genauso wie bei der alljährlichen Grippe-Epidemie. Das Risiko, sie zu bekommen, ist nun mal ohne Gripeschutzimpfung höher. In der heutigen vernetzten Welt ist keiner mehr vor einer Cyberattacke sicher. Hier muss ein Sinneswandel stattfinden.

Cyberattacken nehmen zu

Welche Maßnahmen sollten Unternehmen ergreifen, die sich jetzt mitten in der digitalen Transformation – Stichwort Industrie 4.0 – befinden?

Heinz-Uwe Gernhard: Es ist eine klare und eindeutige Managementaufgabe. Die Verantwortlichen müssen die Risiken, die durch die Vernetzung drohen, ganz klar erkennen und Maßnahmen definieren. Mit Blick auf die Verfügbarkeit der Produktionstechnik müssen sie verstehen, dass ihnen erhebliche Schäden drohen. Davor ist auf Grund der Vernetzung niemand gefeit. Wer die Fachpresse verfolgt, findet immer wieder Nachrichten, wie zum Beispiel, dass eine Cyberattacke sogar die IT einer Spezialfirma für Sicherheits- und Steuerungstechnik weitestgehend lahmlegte. Die Firma hat diesen Vorfall publik gemacht. Das ist für mich richtig und wichtig, denn wir sitzen alle im selben Boot.

Doch noch ist Offenheit in Sachen Cyberattacken eher die Ausnahme: Inwiefern können Netzwerke wie der von Ihnen geleitete VDMA-Arbeitskreis Security dabei helfen – indem man untereinander offen über Cyberattacken spricht?

Heinz-Uwe Gernhard: Wir gehen das Thema proaktiv an, in dem wir die Risiken klar adressieren und Hilfestellungen zu den vielfältigen Fragen bieten. Mir geht es insbesondere darum, dass wir über Verbandsgrenzen hinweg gemeinsam für Transparenz sorgen. Eine gute Ausgangsbasis bietet auch die Plattform Industrie 4.0 mit ihrem Link www.plattform-i40.de.

Oft fehlt das richtige Bewusstsein

Manche Firmen beginnen nun ganz gezielt, bei ihren Mitarbeitern das Bewusstsein für Betrugsszenarien zu wecken. Was halten Sie von dem neuen Zauberwort Cyberresilienz, das gerade die Runde macht?

Heinz-Uwe Gernhard: Das ist der richtige Weg, denn Aufmerksamkeit bietet für diese Bedrohungsart den besten Schutz. Das ist eine Fähigkeit, die jeder Anwender von Cybertechnologien besitzen sollte.

Wie beurteilen Sie den Stand der Sicherheits-IT?

Heinz-Uwe Gernhard: Vergleichen wir es mit dem Verkehr. Ein Autofahrer brauchte im Jahr 1920 ein ganz anderes Risikobewusstsein als ein heutiger Pkw-Lenker, dessen Fahrzeug eine deutlich geringere Aufmerksamkeit erfordert, weil es ihm vieles abnimmt. Fahrzeuge und Infrastruktur machen das Autofahren heute sehr viel risikoärmer. Im Vergleich dazu ist der Reifegrad unserer gegenwärtigen IT in Bezug auf ihre inhärenten Risiken auf dem Stand eines Autos von 1920. Es erfordert vom Benutzer eine hohe Aufmerksamkeit und vielfältiges Wissen. Awareness oder auf gut Hessisch „uffpasse!“ ist aktuell ein zentrales Thema.

Ist das nicht Angstmacherei?

Heinz-Uwe Gernhard: Nein, es ist keine Angstmacherei. Beispielhaft werden Szenarien im Roman Blackout von Marc Elsberg durchgespielt. Die technischen Aspekte darin sind eben keine Fiktion, sondern entsprechen den Realitäten und sind nur von ihm romanhaft und spannend verpackt worden. Hier wurde ja auch

der Gesetzgeber mit dem IT-Sicherheitsgesetz (Kritis) aktiv, das sich gerade in Überarbeitung befindet.

Der IT-Experte Peter Turczak sagte im VDMA Magazin: „In eine Cloud würde ich niemals Daten ablegen, ohne die unser Betrieb stillstehen würde.“ Unternehmen benötigen aber Daten für die Umsetzung von Industrie 4.0 und müssen sie sicher speichern. Was gehört in die Cloud und was nicht?

Heinz-Uwe Gernhard: Der IT-Kollege spricht die zentrale Forderung der OT (?) nach Verfügbarkeit an. Als Nachrichtentechniker sehe ich immer den Wettbewerb zwischen Bandbreite, Rechnerleistung vor Ort und natürlich den Kosten. Die Cloud bietet vielen eine zentralisierte Anwendung mit viel Rechenleistung, wenn die Bandbreite stimmt. Der Anwender muss die Art des Cloud-Einsatzes mit Blick auf seine Risikobereitschaft und Verfügbarkeitsanforderungen und seinen technischen und organisatorischen Fähigkeiten abwägen. Eine andere wichtige Frage ist natürlich das Vertrauen bzw. die Vertrauenswürdigkeit des Anbieters und deren Sicherstellung.

Es ist also eine Vertrauensfrage?

Heinz-Uwe Gernhard: Genau, ich muss mich fragen, wem ich wie vertraue. Reichen im gegebenen Rechtsraum technische Maßnahmen, Verträge und Zertifizierungen von beteiligten Dienstleistern aus?

Auf der Metav 2020 verfügen die meisten Werkzeugmaschinen über Internetanschlüsse: Worauf sollten Messebesucher achten?

Heinz-Uwe Gernhard: Es handelt sich hoffentlich nicht um einen offenen Internetanschluss, sondern um eine, auch hier wieder, vertrauenswürdige Verbindung. Fragen Sie hierzu nicht nur nach der technischen Lösung, sondern auch nach den organisatorischen Fähigkeiten des Anbieters. Technisch bieten sich private VPN-Netze mit entsprechender vertraglicher Absicherung an.

Eine Norm bietet Hilfestellung

Wie kann sich der Messebesucher auf das Gespräch vorbereiten?

Heinz-Uwe Gernhard: Hilfe bietet die Norm ISO/IEC 62443, die im Teil 2-4 mit den „Anforderungen an das IT-Sicherheitsprogramm von Dienstleistern für industrielle Automatisierungssysteme“ den Rahmen vorgibt, worauf er bei Angeboten achten sollte. Ansonsten sind Regelungen und Standards, auch wenn sie oft etwas spröde sind, hilfreich und zielführend.

Herr Gernhard, wir bedanken uns für das Gespräch.

VDMA: Cybersicherheit durch gezieltes Zusammenspiel

Informationstechnologien sind heute ein wichtiger Teil nahezu jeder Produktionsanlage. „IT macht Maschinen nicht nur schlau und interaktiv, sondern auch anfälliger für Cyberangriffe“, beobachtet Steffen Zimmermann, Leiter Competence Center Industrial Security beim VDMA. „Um hohe Maschinenverfügbarkeit und Integrität der Daten über den gesamten Produktlebenszyklus zu garantieren, bedarf es des Zusammenspiels der Anbieter von Automatisierungslösungen und Maschinen mit dem Betreiber der Anlage.“ Zudem müssten sich Betreiber darauf einstellen, dass die Gefahr einer Cyberattacke immer besteht. Daher sollten Betreiber mit grundlegenden Maßnahmen ihre Cyberresilienz sicherstellen, um die Auswirkungen eines Cyberangriffs zu verringern. Den aktuellen Stand der Dinge vermittelt am 11. März 2020 der Cybersecurity-Kongress von VDW und VDMA auf der METAV 2020, bei dem das Zusammenwachsen von Office- und Produktionswelt im Mittelpunkt steht. Zu den Themen zählen unter anderem: Regulierung, Fernwartung/internationale Vernetzung, Live Hacking und Basic-Maßnahmen zur Wiederherstellung eines IT-Netzwerkes.

Vita: Heinz-Uwe Gernhard

Heinz-Uwe Gernhard (Jahrgang 1957) wechselte als junger Diplom-Ingenieur (Nachrichtentechnik) nach seinem Studium an der TH Darmstadt 1983 als Entwickler zum Elektronikkonzern SEL. 1987 bis 2017 entwickelte Heinz-Uwe Gernhard Steuerungstechnik bei der heutigen Bosch Rexroth Electric Drives and Controls GmbH in Erbach. Seit 2017 arbeitet der Diplom-Ingenieur im Zentralbereich IT Security and Application (C/TED1) bei der Robert Bosch GmbH in Stuttgart. Sein Spezialgebiet ist das Risikomanagement und IT-Security für die Fertigung.

((Umfang: rund 8.800 Z. inkl. Leerz.))

Autor: Nikolaus Fecht im Auftrag des VDW

Ansprechpartner

VDW - Verein Deutscher Werkzeugmaschinenfabriken e.V.
Gerda Kneifel
Presse und Öffentlichkeitsarbeit
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
Leiter Competence Center Industrial Security
Lyoner Straße 18
60528 Frankfurt
Tel. +49 69 6603-1978
steffen.zimmermann@vdma.org

Presseagentur Nikolaus Fecht
Technik-Texte à la carte - wenn Ihnen die Worte fehlen

Husemannstraße 29
45879 Gelsenkirchen
Tel. +49 209 26575
fecht@erzfreunde.de

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 im Bereich Presse. https://www.metav.de/cgi-bin/md_metav/lib/pub/tt.cgi?oid=3615&lang=1&ticket=g_u_e_s_t

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>