PRESSEINFORMATION

Postadresse: Lyoner Straße 18
60528 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

Security by Design erreicht die Werkzeugmaschine

Verstärkte Nachfrage nach IT-Sicherheitslösungen auf der METAV 2022 erwartet

Frankfurt am Main, **03. Februar 2022**. – Wenn das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Cyber-Sicherheitswarnung der höchsten Warnstufe ausruft, ist die Industrie alarmiert: Eine „kritische Schwachstelle" in der weit verbreiteten Java-Bibliothek Log4j, so das BSI in seiner Warnmeldung vor wenigen Wochen, sei „trivial ausnutzbar" und ermögliche eine „vollständige Übernahme des betroffenen Systems". Dies bedeutet nicht weniger als ein gefundenes Fressen für Cyberkriminelle, zugleich der Albtraum vieler Unternehmen. Zwar steht das mögliche Ausmaß der Bedrohungslage noch nicht fest, weil Hacker zunächst einen Code im System ablegen und erst nach Wochen oder Monaten aktivieren könnten. Im VDW (Verein Deutscher Werkzeugmaschinenfabriken) ist der Alarm jedoch Wasser auf die Mühlen derjenigen, die gerade mit Hochdruck an einem Leitfaden zur methodischen Umsetzung von IT-Sicherheit an Werkzeugmaschinen arbeiten und branchenweit für mehr Security werben. Die Aussteller auf der kommenden METAV 2022 in Düsseldorf (neuer Termin 21. bis 24. Juni) können sich indes auf eine verstärkte Nachfrage nach Security-Lösungen einstellen.

Wachsende Bedrohungslage

Nach Angaben von Prof. Felix Hackelöer, Professor für Smart Automation an der Fakultät für Informatik und Ingenieurswissenschaften der Technischen Hochschule Köln, wirft die Sicherheitslücke von Log4j ein Licht auf die wachsende Bedrohungslage, die auch unmittelbar auf die Industrie zielt. In der Informationstechnik betreffen Fehler und Schwachstellen durch die große Zahl an Implementierungen schnell viele Systeme, so Hackelöer. Das gelte vor allem für nicht unmittelbar an der Wertschöpfung beteiligte Standardkomponenten, wie eben im Fall Log4j die Logging-Funktionen.

Eine Flucht in weniger verbreitete Software-Systeme ist für Hackelöer jedoch keine Option. „Der hohe Skalierungsfaktor der IT ist Fluch und Segen zugleich", erläutert der Wissenschaftler. Die millionenfache Verbreitung sorge neben einer hohen Kosteneffizienz schließlich auch dafür, dass entsprechend viele User mit der Software arbeiten und Schwachstellen relativ schnell erkannt und durch Updates geschlossen werden könnten. Es bleibt jedoch der ewige Wettlauf mit Hackern und der Gefahr, dass sensible Daten in falsche Hände geraten. In der Folge werden Unternehmen erpresst oder ausspioniert, beides könne existenzbedrohende Ausmaße annehmen. Dagegen helfe nur wirksamer Selbstschutz, und zwar nach außen und nach innen. Es gebe nämlich auch eine Bedrohungslage in den Unternehmen selbst, etwa durch allzu sorglosen Umgang mit Maschine und Peripherie sowie bewusst oder unbewusst hervorgerufene Manipulationen.

IT-Sicherheit geht alle an

Bereits im vergangenen Jahr wurde in der Abteilung Forschung und Technik des VDW ein erster Leitfaden „IT-Sicherheit an Werkzeugmaschinen" erarbeitet, der sich mit praktischen Tipps in erster Linie an Anwenderinnen und Anwender richtete. Daran beteiligt war auch Hackelöer als beratender Experte. Zugleich befasst sich der Arbeitskreis 2 *Steuerungs- und Systemtechnik* des VDW-Forschungsinstituts mit

Sicherheitsthemen. Inzwischen ist ein weiterer Leitfaden in Arbeit, der sich diesmal an Produzierende von Werkzeugmaschinen und Fertigungsanlagen richten soll.

„Wir hatten uns zunächst vor allem auf die funktionale Sicherheit, also die Sicherheit von Personen an der Maschine konzentriert und versucht, diesen von der IT-Security zu trennen“, erläutert Eberhard Beck, Leiter Steuerungstechnik der Index-Werke, Esslingen, und Vorsitzender des VDW-Arbeitskreises 2. Inzwischen sei jedoch klar, dass die funktionale Sicherheit einer Maschine nur aufrechterhalten werden kann, wenn die IT-Security funktioniert. „Das Thema dringt in alle Bereiche ein“, stellt Beck fest, „und ist weder abgrenzbar, noch auf andere abzuwälzen. Jeder muss sich damit befassen.“

Spannungsfeld durch heterogene Welt der Werkzeugmaschinen

Für den Arbeitskreis bedeutet dies nach Becks Angaben, dass er sich inzwischen fast ausschließlich mit Security-Themen befasst. Der Grund dafür liegt auf der Hand: Die digitale Transformation in der Fertigung, speziell auch von Werkzeugmaschinen und Anlagen, schreitet unaufhaltsam voran. Vormals als Insellösung betriebene Steuerungskomponenten werden unternehmensweit vernetzt, mit Hilfe des Internets miteinander verbunden oder interagieren mit Software-Services in der Cloud. Ein Spannungsfeld entstehe dadurch, dass die Welt der Werkzeugmaschinen viel heterogener sei als die IT-Welt, sagt Beck. „Während IT-Fachleute die Welt von einem handelsüblichen PC aus betrachten, der selten älter als zwei Jahre und mit aktuellem Betriebssystem ausgestattet ist, sind Werkzeugmaschinen speziell auf den Anwendungsfall zugeschnittene Unikate.“ Viele seien nach Jahrzehnten mechanisch noch völlig intakt und in der Produktion im Einsatz. Auch das Design einer Maschinensteuerung könne schon mal eine Dekade zurückliegen, als Cyberkriminalität noch kein Thema war.

Um Maschinen im Bestand zu schützen, könne man nicht mal eben ein neues Betriebssystem aufspielen, wenn der Software-Hersteller für die alte Version keine Sicherheits-Updates mehr anbietet, sagt Beck. Die Aufgabe ist anspruchsvoller, sodass sich hier sogar ein neues Geschäftsfeld etabliert hat. Es gibt Anbieter, wie auch auf

der METAV 2022 zu erleben, die das Retrofitting von Bestandsmaschinen anbieten. Für die Zukunft müsse es aber vor allem darum gehen, Security-Lösungen gleich in die Entwicklung einer Maschine einzubetten, und zwar so, dass sie über den gesamten Lebenszyklus resilient ist.

Security by Design

Aus der Software-Entwicklung ist eine Methode unter dem Begriff *Security by Design* bekannt. Sie wird bereits seit Jahren angewandt . Übertragen auf den Maschinen- und Anlagenbau, findet sie Anwendung in der internationalen Norm IEC 62443. Diese Norm hat sich als Maßstab zur Betrachtung von IT-Security über den gesamten Lebenszyklus von Automatisierungslösungen etabliert.

Bislang waren Maschinenbauer nach dieser Norm noch nicht gefordert, erläutert Hackelöer, weil sie das Umfeld der Maschine nicht in der Hand haben und die Norm zunächst für den Anlagenbau und kritische Infrastrukturen erstellt wurde. Zudem sei die Norm noch relativ neu. Hackelöer ist jedoch sicher, dass sie sich jetzt auch in der Werkzeugmaschinenindustrie durchsetzt. „Kundinnen und Kunden tragen das Thema in den Maschinenbau“, stellt er fest.

Kundinnen und Kunden als Security-Treiber

Eine verstärkte Nachfrage nach Security-Lösungen bestätigt auch Dr. Andreas Kahmen, Leiter Steuerungsentwicklung Maschinenplattformen bei Trumpf Werkzeugmaschinen. Kahmen ist Mitglied des VDW-Arbeitskreises 2 und mit Trumpf auf der METAV 2022 in Düsseldorf als Partnerunternehmen der *umati*-Initiative präsent. „Wir sind davon überzeugt, dass Vernetzung der Schlüssel ist, um Potenziale für die Produktion der Zukunft zu erschließen“, sagt Kahmen. Trumpf habe früh damit begonnen, Security-Lösungen anzubieten und sie vom BSI zertifizieren zu lassen. So wurde bereits Mitte der 2000er Jahre ein Security-Konzept entwickelt, mit dem das Maschinennetzwerk über eine Hardwarekomponente mit integrierter Firewall gegen unerlaubte Zugriffe geschützt wurde. Die Firewall erlaubte Teleservice-Zugriffe,

während alle anderen Zugriffe abgeblockt wurden. Damals seien Security-Lösungen kaum nachgefragt worden, doch das habe sich spürbar geändert. Die Nachfrage käme dabei nicht nur von Großunternehmen etwa der Automobilindustrie, sondern vor allem von kleineren Unternehmen. Die Sensibilisierung der Kunden für IT-Sicherheit habe deutlich zugenommen.

Dass sich die Security-Anstrengungen des Arbeitskreises 2 im VDW als „langer steiniger Weg" gestalten, wie es heißt, liegt weniger am mangelnden Interesse als an der Komplexität des Themas. Für Security-Themen muss Aufklärungsarbeit geleistet werden. Das gilt gegenüber Kundinnen und Kunden ebenso wie für Maschinen herstellende Firmen oder IT- Fachleute, nach deren Verständnis die Probleme doch einfach lösbar sein müssten. „Da muss man schon mal erklären, dass auf einer Werkzeugmaschine nicht einfach standardmäßig ein Virenscanner laufen kann, weil der temporär so viel Rechenleistung benötigt, dass er das Verhalten der Maschine beeinflussen könnte", sagt Kahmen. Auch Hackelöer stellt fest, dass ein wichtiger Teil wissenschaftlicher Arbeit an der Schnittstelle zwischen IT und Industrie darin besteht, „Übersetzungsarbeit" zu leisten. Wer IT-Security in die Werkzeugmaschinenindustrie bringen will, müsse dafür sorgen, dass sich Maschinenhersteller in ihrer Fachsprache wiederfinden.

Vom Fachwissen zum verständlichen Leitfaden

So soll im neuen „Leitfaden zur methodischen Umsetzung von IT-Sicherheit an Werkzeugmaschinen" anhand einer Werkzeugmaschine Schritt für Schritt die Vorgehensweise zur Ermittlung der notwendigen Security-Maßnahmen erläutert werden. Der Leitfaden wird federführend zusammengestellt von Ralf Reines, Referent in der Abteilung Forschung und Technik des VDW. Der Leitfaden dokumentiert, dass es in der gemeinsamen Verantwortung von Maschinen herstellenden Unternehmen, Kundinnen und Kunden sowie Komponentenlieferanten liegt, für die jeweilige Werkzeugmaschine ein Sicherheitsniveau zu erreichen, das den Erfordernissen im jeweiligen Betriebsumfeld und individuellen Anforderungen des Betreibenden genügt.

Hackelöer, der einmal mehr an der Entwicklung des Leitfadens beteiligt ist, sieht den Zeitpunkt als günstig an, jetzt und auch auf der METAV 2022 für Security-Themen zu werben und sich mit der Norm IEC 62443 auseinanderzusetzen. „Ein 100-prozentiger Schutz ist nicht erreichbar", räumt er ein. „Wichtig ist es jedoch, eine Risikoabwägung zu treffen, wie groß die Bedrohungslage für Cyberangriffe in einem bestimmten Anwendungsfall ist und welche Maßnahmen dagegen ergriffen werden können." Um dies in seiner Komplexität handelbar zu machen, sei das Wissen um Prozesse und Methoden unverzichtbar. „Es ist gut, dass sich der VDW dieses Themas annimmt und für Transparenz sorgt", sagt der Wissenschaftler. Die Aufmerksamkeit für das Thema könnte nach der jüngsten Alarmstufe Rot des BSI kaum größer sein.

10.239 Zeichen

Autorin: Cornelia Gewiehs, freie Journalistin, Rotenburg (Wümme)

Ansprechpartnerinnen und Ansprechpartner

VDW (Verein Deutscher Werkzeugmaschinenfabriken)
Gerda Kneifel
Presse- und Öffentlichkeitsarbeit
Lyoner Straße 18
60528 Frankfurt am Main
DEUTSCHLAND
Tel. +49 69 756081-32
g.kneifel@vdw.de
www.vdw.de

Index-Werke GmbH & Co. KG Hahn & Tessky
Eberhard Beck
Leiter Steuerungstechnik
Plochinger Straße 92
73730 Esslingen
DEUTSCHLAND
Tel. + 49 711 3191-0
eberhard.beck@index-werke.de
www.index-werke.de

Technische Hochschule Köln
Prof. Felix Hackelöer
Institut für Automation & Industrial IT
Campus Gummersbach, Steinmüllerallee 1
51643 Gummersbach
DEUTSCHLAND
Tel. +49 221 8275-6493
felix.hackeloer@th-koeln.de
www.th-koeln.de

Trumpf Werkzeugmaschinen GmbH + Co. KG
Dr. Andreas Kahmen
Leiter Steuerungsentwicklung Maschinenplattformen
Johann-Maus-Straße 2
71254 Ditzingen
DEUTSCHLAND
Tel. +49 7156 303-0
andreas.kahmen@trumpf.com
www.trumpf.com

Hintergrund

Die METAV 2022 findet vom 21. bis 24. Juni in Düsseldorf statt. Sie zeigt das komplette Spektrum der Fertigungstechnik. Schwerpunkte sind Werkzeugmaschinen, Werkzeuge, Zubehör, Messtechnik, Oberflächen- und Computertechnik für die Metallbearbeitung, Software, Maschinen und Systeme für die additive Fertigung, Produktionssysteme und Komponenten für die Medizintechnik. Zusätzlich stellt die METAV 2022 in vier Areas spezifische Lösungen zu den Themen Additive Manufacturing, Medical, Moulding und Quality heraus. Die METAV 2020 musste coronabedingt ausfallen und fand 2021 als Digitalveranstaltung statt.

Detaillierte Informationen, Angebote und Anmeldeunterlagen zur METAV 2022 finden Sie im Internet unter www.metav.de.

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

www.linkedin.com/company/metav-duesseldorf