Die Welt der Metallbearbeitung
The world of metalworking

EMO Hannover
16-21·9·2019

# PRESSEINFORMATION


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


## Werkzeugmaschinen vor Cyberattacken schützen

### EMO Hannover 2019 zeigt Lösungen für komplexe vernetzte Anlagen

***Frankfurt am Main, 09. Juli 2019.*** *– Die Datensicherheit wird im Zuge von Industrie 4.0 immer wichtiger. Automation, Cloud-Applikationen sowie global vernetzte Maschinen und Komponenten spielen dabei mit Blick auf die Sicherheit vor externen Zugriffen eine wichtige Rolle.*

Mit der Digitalisierung, die sich in allen Branchen durchsetzt, nimmt auch die Notwendigkeit zu, sich vor Cyberrisiken zu schützen. Denn die deutsche Industrie steht immer häufiger im Fadenkreuz von Cyberkriminellen: Für gut acht von zehn Industrieunternehmen (84 Prozent) hat die Anzahl der Cyberattacken in den vergangenen zwei Jahren zugenommen, für mehr als ein Drittel (37 Prozent) sogar stark. Das ist das Ergebnis einer Studie des Digitalverbands Bitkom von 2018, für die 503 Geschäftsführer und Sicherheitsverantwortliche quer durch alle Industriebranchen repräsentativ befragt wurden. „Die deutsche Industrie steht unter digitalem Dauerbeschuss – von digitalen Kleinkriminellen über die organisierte Kriminalität bis zu Hackern im Staatsauftrag“, sagt Bitkom-Präsident Achim Berg. „Qualität und Umfang der Cyberangriffe werden weiter zunehmen.“

Fest steht: Cyberkriminalität ist ein weltweites Phänomen, das weder an Landesgrenzen noch vor verschlossenen Industrietoren Halt macht. Sie kann überall dort stattfinden, wo Menschen Computer, Smartphones und andere IT-Geräte benutzen.

**Reagieren auf Sicherheitslücken und Softwarefehler**

Einer der Global Player im Bereich Automation ist die Balluff Gruppe. Mit 4.000 Mitarbeitern weltweit bietet das Unternehmen ein umfassendes Portfolio an Sensor-, Identifikations-, Netzwerk- und Softwarelösungen für alle Bereiche der Automation. Der Schutz vor Cyberkriminalität ist bei der Entwicklung und Konzeption der Kundenlösungen eine wichtige Säule.

„Cyberkriminelle verwenden regelmäßig bekannte Sicherheitslücken oder Fehler in veralteter Software, um sich Zugriff auf ein System zu verschaffen. Das zeitnahe Einspielen angebotener Updates und Sicherheitspatches verringert das Risiko von Cyberangriffen ganz erheblich“, sagt Philipp Echteler, IIoT Strategy Manager bei Balluff. Mehr Transparenz schaffe hier auch die Nutzung von versionierten Soft- und Firmwareständen sowie das Überwachen dieser. „Vermeidbare Gefahren gehen auch von Geräten aus, die ursprünglich nicht für eine Anbindung an das Internet ausgelegt waren, sondern nur für die Kommunikation mit der Steuerung isolierter Netze. Viele dieser Ethernet-fähigen Automatisierungsgeräte bieten keinerlei Schutzmechanismen und öffnen Angreifern Tür und Tor“, so Echteler weiter.

**Anlagen vor Manipulationen und Cyberkriminalität schützen**

Doch auf was kommt es bei komplexen vernetzten Anlagen an, wenn diese sicher vor Manipulationen und Cyberkriminalität geschützt sein sollen? „Grundsätzlich stellt jede vernetze Anlage einen möglichen Angriffspunkt dar. Zum Schutz vor Manipulationen und Cyberkriminalität ist daher ein gut aufgesetztes Sicherheitskonzept unerlässlich“, sagt Juliane Schneider, Junior Productmanager bei symmedia. Seit 1997 entwickelt die symmedia GmbH aus Bielefeld Servicelösungen für den Maschinenbau. Die Digitalisierungskompetenz des Unternehmens wird durch die Allianz mit dem Maschinenbauer Georg Fischer, dem symmedia seit 2017 angehört, insbesondere mit Blick auf den Maschinen- und Anlagenbau gestärkt.

„Jede Art von menschlicher Nachlässigkeit im Umgang mit sensiblen Daten stellt ein Sicherheitsrisiko dar. Ob Opfer einer unbemerkten Cyberattacke, die leichtsinnige Mehrfachverwendung von Passwörtern oder die bewusste Weitergabe vertraulicher Daten – jede menschliche Handlungsweise kann massive Folgen und Schäden erwirken“, nennt Schneider einige naheliegende Risiken. Echteler ergänzt: „Risiken durch interne Bedrohungen sind nicht zu vernachlässigen. Mitarbeiter öffnen mangels besseren Wissens arglos E-Mail-

Anhänge und schleusen damit unbemerkt Viren ein oder sie versenden kritische Unternehmensinformationen ungeschützt per E-Mail.“ Auch schlecht gesicherte oder vergessene Wartungszugänge glichen einer Hintertür, die Angreifer gerne für ihre Zwecke ausnutzen.

**Firewall prüft automatisch auf Vertrauenswürdigkeit**

Um komplexe vernetzte Anlagen sicher vor Manipulationen und Cyberkriminalität zu schützen, sind zunächst standardmäßig Verschlüsselungsmechanismen wie SSL oder TLS einzusetzen. Damit wird der gesamte Datenverkehr zwischen den Servern, Computern und Anwendungen eines Netzwerkes verschlüsselt. Gängige Praxis ist es auch, alle Verbindungen, die auf einen Computer zugreifen wollen, von einer Firewall auf Vertrauenswürdigkeit prüfen zu lassen, um sich automatisiert vor Angriffen oder unbefugten Zugriffen zu schützen.
„Getrennte Netze für Produktion und Office bieten ein zusätzliches Plus an Sicherheit. Darüber hinaus empfiehlt es sich, die Zahl der Netzzugänge zu minimieren und den Datenstrom über ein zentrales, überwachtes Gateway zu leiten. Wenn man dann noch den Datenverkehr, die Last im Netz und den einzelnen Knoten kontinuierlich analysiert, lassen sich mögliche Bedrohungen häufig schon im frühen Stadium erkennen“, nennt Philipp Echteler weitere Umsetzungsmöglichkeiten, die die Sicherheit unterstützen helfen.

**Lösungsansätze zur Datensicherheit in der vernetzten Produktion**

Balluff hat ein eigenes Experten-Team etabliert, welches den weltweiten Kunden eine ganzheitliche Beratung anbietet. Einige der Balluff-Geräte verfügen mittlerweile zudem über eine Hardware-Verschlüsselung mittels Trusted Platform Modul.
Symmedia setzt neben Minimalanforderungen, wie die Absicherung durch Firewalls, ebenfalls auf HSM- und TPM Verfahren (Verfahren, die auf so genannten Hardware Security Modulen und Trusted Platform Modulen basieren) zur ausschließlichen Ausführung gesicherter Software. „Mit der Nutzung eines proprietären Netzwerkprotokolls setzen wir die Schwierigkeit des ungewollten Zugriffs zudem sehr hoch, da diese Verbindungen grundsätzlich nicht ohne Weiteres ‚gekapert‘ werden können“, sagt Schneider.

Bei der digitalen Serviceunterstützung setzt das Unternehmen auf eine sichere und workflowbasierte Punkt-zu-Punkt-Verbindung. „Die Nutzung gängiger Verschlüsselungs-, Authentifizierungs- und Autorisierungsverfahren für Clientanwendung, Server und Programmierschnittstellen, so genannte API, sind für uns ebenso selbstverständlich. Zudem

bieten wir viele weitere Sicherheitsmaßnahmen, so beispielsweise die individuelle Maschinen- und Benutzer-Zertifikatsstruktur nach PKI – die Public-Key-Infrastruktur – Passwortregeln, die irreversible Ablage der Zugangsdaten mit aktuellen Hashverfahren und die Mehrfaktor-Authentifizierungen“, beschreibt Juliane Schneider weiter.

**Cloud und Firmen-Cloud haben ihre Berechtigung**

Ein weiterer Punkt, der mit Blick auf das Datenhandling wichtig ist, ist der Ort der Datenspeicherung. Ob mögliche Kosteneinsparungen, die Entlastung der eigenen IT oder mehr Sicherheit: Drei von zehn Unternehmen (29 Prozent) nutzen eine Cloud-Lösung, die in ein zertifiziertes Rechenzentrum ausgelagert ist. Weitere zehn Prozent planen dies und 28 Prozent diskutieren darüber. Das zeigt der Digital Office Index 2018 – eine repräsentative Befragung von 1.106 Unternehmen ab 20 Mitarbeitern des Digitalverbands Bitkom. Demnach ist das so genannte Cloud-Hosting lediglich in weniger als drei von zehn Unternehmen (28 Prozent) überhaupt kein Thema. Betrachtet man die unterschiedlichen Branchen, ist der Maschinen- und Anlagenbau Vorreiter. Bereits fast jedes zweite Unternehmen aus dieser Branche (46 Prozent) greift nach Aussage von Bitkom auf externe Cloud-Dienstleister zurück.

Erste Wahl ist auch für Balluff die Public Cloud. „Für sie spricht eine hohe Verfügbarkeit, denn ihre Plattformen werden auf unabhängigen, häufig auch geografisch verteilten Rechenzentren repliziert. Weitere Vorteile sind zum Beispiel eine einfache Skalierbarkeit, ein hohes Maß an Sicherheit, die Nutzung neuester Technologien, die Servicekontinuität und Verschlüsselung. Damit ist das Funktionieren der Lösungen auch beim Eintreten negativer Szenarien garantiert“, unterstreicht IIoT Strategy Manager Echteler. Die Erfahrung zeige, dass sich eine Cloud nicht nebenher von den eigenen IT-Mitarbeitern betreiben ließe. Dies sei eine Aufgabe für ausgewiesene Spezialisten.

Symmedia dagegen bietet den Kunden hybride Lösungen an. „Dadurch erhalten diese Flexibilität, einhergehend mit außerordentlicher Sicherheit. Das heißt, die volle Datenhoheit obliegt hierbei unserem Kunden“, so Junior Productmanager Juliane Schneider. Dieser könne dann für sich entscheiden, ob und welche Daten er zentral, beispielsweise in einer Cloud oder nur lokal ablegen möchte. „Je nach Sensibilität der Daten haben wir die Erfahrung gemacht, dass unsere Kunden durchaus offen gegenüber zentralen Lösungen sind, sich jedoch immer das Recht vorbehalten, spezifische Daten nur lokal zu speichern.“

**Beispiele für Datensicherheit und Sicherheitskonzepte in Hannover**

Symmedia wird auf der EMO in Hannover anhand von praxisnahen Anwendungsmöglichkeiten am Beispiel einer Digital Factory zeigen, was die Software des Unternehmens für den Produktionsalltag leisten kann. Dabei werden beispielsweise Condition Monitoring, Alarming Szenarien und Remote Services live gezeigt. Zudem können sich die Messebesucher zu den Themen Predictive Maintenance, Datensicherheit und Sicherheitskonzepte, wie auch zum herstellerübergreifenden Einsatz der symmedia -Software informieren.

Balluff wird Lösungen präsentieren, mit denen sich die Produktivität in der Metallbearbeitung steigern lässt. Dazu gehören auch innovative Konzepte für intelligente Fertigungssysteme. Besondere Highlights sind beispielsweise ein einfach nachzurüstendes Werkzeugmanagementsystem sowie Lösungen für die kontinuierliche Prozessüberwachung an der Werkzeugmaschine.

*Autorin: Annedore Bose-Munde, Fachjournalistin aus Erfurt*
*Umfang: rund 9.800 Zeichen inkl. Leerzeichen*

**Ansprechpartner:**

VDW Verein Deutscher Werkzeugmaschinenfabriken
Gerda Kneifel
Presse- und Öffentlichkeitsarbeit
Corneliusstraße 4
60325 Frankfurt am Main
Deutschland
Tel. +49 69 756081 32
g.kneifel@vdw.de
www.vdw.de

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

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

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

Annedore Bose-Munde
Fachjournalistin für Wirtschaft und Technik
Am Elsterberg 13
99094 Erfurt
Deutschland
Tel. +49 171 2684 366
info@bose-munde.de
www.bose-munde.de

**EMO Hannover 2019 – Weltleitmesse der Metallbearbeitung**

Vom 16. bis 21. September 2019 präsentieren internationale Hersteller von Produktionstechnologie zur EMO Hannover 2019 smarte Technologien. Unter dem Motto „Smart technologies driving tomorrow's production!" zeigt die Weltleitmesse der Metallbearbeitung die gesamte Bandbreite moderner Metallbearbeitungstechnik, die das Herz jeder Industrieproduktion ist. Vorgestellt werden neueste Maschinen plus effiziente technische Lösungen, Produkt begleitende Dienstleistungen, Nachhaltigkeit in der Produktion u.v.m. Der Schwerpunkt der EMO Hannover liegt bei spanenden und umformenden Werkzeugmaschinen, Fertigungssystemen, Präzisionswerkzeugen, automatisiertem Materialfluss, Computertechnologie, Industrieelektronik und Zubehör. Die Fachbesucher der EMO Hannover kommen aus allen wichtigen Industriebranchen, wie Maschinen- und Anlagenbau, Automobilindustrie und ihren Zulieferern, Luft- und Raumfahrttechnik, Feinmechanik und Optik, Schiffbau, Medizintechnik, Werkzeug- und Formenbau, Stahl- und Leichtbau. Die EMO Hannover ist der wichtigste internationale Treffpunkt für die Fertigungstechnik weltweit. Zur EMO Hannover 2017 zogen fast 2.230 Aussteller aus 44 Ländern rd. 130.000 Fachbesucher aus 160 Ländern an. EMO ist eine eingetragene Marke des europäischen Werkzeugmaschinenverbands Cecimo.

Texte und Bilder zur EMO Hannover finden Sie im Internet unter www.emo-hannover.de/bilddatenbank.

Begleiten Sie die EMO Hannover auch auf unseren Social-Media-Kanälen

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

Wenn Sie unsere Presseinformationen nicht mehr erhalten wollen, klicken Sie bitte hier.