Interview: Industrie 4.0 auch vor Cyber Risiken nicht gefeit

Der Maschinen- und Anlagenbau ist einer der führenden Industriezweige der deutschen Wirtschaft. Alleine 80 Prozent der Produktion hierzulande gehen in den Export. Umso relevanter ist für diese Schlüsselbranche ihr Know-how, um Produktion und Technik zu schützen. In der heutigen digitalen Welt, in der viele Anlagen hochtechnologisiert arbeiten und möglicherweise durch Schnittstellen vernetzt sind, spielt die Thematik Cyberrisiken zwischenzeitlich eine große Rolle. Gemeinsam mit dem Branchenverband der deutschen Maschinen- und Anlagenbauer VDMA beziehungsweise dessen Tochterunternehmen, dem Versicherungsmakler VSMA GmbH, hat Chubb eine speziell auf die Bedürfnisse der Branche ausgerichtete Cyber-Police konzipiert. Kerstin Hartung Alexandre, Chefredakteurin der Face, sprach über die Besonderheiten der Branche sowie deren Bewusstsein für Cyberrisiken sowie über die Speziallösung mit Birger Jeurink, Geschäftsführer der VSMA, und Natalie Kress-Happel, Cyber Line Manager bei Chubb in Deutschland.

Herr Jeurink, welche besonderen Merkmale zeichnen den deutschen Maschinen- und Anlagenbau aus und weshalb sollte sich dieser besonders gut vor der Gefahr aus der Cyberwelt schützen?

Der Maschinen- und Anlagenbau ist eine wichtige Schlüsselbranche und Motor für die deutsche Wirtschaft. Mit einem Umsatz in 2018 von rund 232 Milliarden Euro und 1,3 Millionen Beschäftigten ist die Branche der größte industrielle Arbeitgeber und einer der führenden deutschen Industriezweige. Die Produkte und Dienstleistungen des Maschinenund Anlagenbaus genießen weltweit hohes Ansehen. Das Thema Industrie 4.0 zeigt, wie weit die Branche mit dem Thema

Digitalisierung bereits ist, und wie weit der Einsatz der künstlichen Intelligenz bereits fortgeschritten ist, sieht man daran, dass Maschinen mittlerweile in der Lage sind, eigenständig anhand von Algorithmen dazuzulernen. Sie tragen zu einer effizienteren Produktion und damit zu mehr Wettbewerbsfähigkeit bei. Die zunehmende Vernetzung hat auch ihre Schattenseiten – sie wird zur Angriffsfläche für Hackerangriffe. Um diese wachsende Bedrohung im Zaum zu halten, bietet der VDMA verschiedene Unterstützungsleistungen an.

Welches sind die größten beziehungsweise gefährlichsten Cyberrisiken für die Branche?

Eine aktuelle VDMA-Studie kommt zu folgendem Ergebnis: Rund 60 Prozent der Unternehmen rechnen für die kommenden Jahre mit einer Steigerung der Security-Vorfälle im eigenen Unternehmen. Von Security-Vorfällen betroffene Unternehmen verzeichnen zumeist Kapitalschäden (50 Prozent) und Produktionsausfälle (31 Prozent). Zu den Bedrohungen mit der höchsten Risikoeinschätzung gehören nach wie vor menschliches Fehlverhalten und Sabotage (Platz 1) und das Einschleusen von Schad-Software (Platz 2). Neu hinzugekommen in der Liste der Top 10 Bedrohungen ist unter anderem „social engineering and pishing“ (Platz 3).

Wie verhält es sich mit dem Bewusstsein hinsichtlich Cyber bei den deutschen Maschinen- und Anlagebauern? Lässt sich ein bestimmter Trend für die kommenden Jahre erkennen?

Industrial Intelligence lautete das Leitmotiv der Hannover-Messe in 2019. Unter anderen standen Fragen im Bereich Cyber Security im Fokus. Es ist völlig unbestritten, dass automatisierte Systeme, die digitalisiert miteinander kommunizieren, anfälliger für Hackerangriffe werden. Die Bedrohung steht zwar in keinem Verhältnis zu den Chancen, die der Maschinen- und Anlagenbau aus der Digitalisierung ziehen

kann, muss aber durchaus ernst genommen werden. Diesbezüglich sind mehr Aufklärungs- und Unterstützungsangebote gefragt. Nicht jeder Unternehmer schätzt sein Cyberrisiko zurzeit richtig ein.

Welche Rolle kommt Ihnen beziehungsweise dem VDMA hierbei zu?

Der VDMA bietet Mitgliedsunternehmen umfassende Unterstützung an. Im Mittelpunkt steht hierbei die Hilfe zur Selbsthilfe, zum Gedankenaustausch sowie zur politischen Unterstützung auf nationaler und internationaler Ebene. Mehrere Gremien im VDMA befassen sich mit dem Thema Security, umfassende Publikationen und Veranstaltungen stehen den Mitgliedern offen. Das VDMA-Kompetenzcenter Industrial Security bündelt die Verbandsaktivitäten des VDMA zur Informationssicherheit, zur Security in der Produktion und zu Security in den Maschinenbau-Produkten. Mit dem Kompetenzcenter stehen den Mitgliedsunternehmen Ansprechpartner für alle Bereiche zur Verfügung. Um den Maschinen- und Anlagenbauern bei der Minimierung der Cyberrisiken zur Seite zu stehen, bietet die VSMA ein Cyberrisiko-Tool an. Mit diesem web-basierten Tool können die Mitgliedsunternehmen auf unkomplizierte Weise ihr Gefahrenpotential überprüfen. Ebenfalls exklusiv für Mitgliedsunternehmen steht die neue Broschüre „Tipps für den Cyber-Schadenfall“ zur Verfügung, die wichtige Hinweise und Handlungsleitfäden zum Umgang mit Cyberangriffen bietet. Zur optimalen Absicherung gegen die wachsende Bedrohung aus dem world wide web bietet die VDMACyber-Police (VCP) außerdem eine speziell für die Branche entwickelte Versicherungslösung.

Warum haben Sie als VSMA sich für eine spezielle Branchenlösung entschieden – hätte eine „reguläre“ Cyberdeckung nicht ausgereicht?

Im Mai 2017 haben wir gemeinsam mit dem VDMA eine Umfrage bei den VDMA-Mitgliedsunternehmen durchgeführt. Wir wollten wissen, wie halten es die deutschen Maschinenund Anlagenbauer

mit ihrem Einsatz für die IT-Sicherheit in ihrem Betrieb konkret? Wieviel Einfluss haben die IT-Verantwortlichen in der Unternehmens-Hierarchie? Auf wessen Rat von außen legen sie wert? Was denken sie über Cyber-Versicherungen? Anhand der Antworten, die in einer Studie „Cyber-Risiken im Maschinen- und Anlagenbau“ veröffentlicht wurden, haben wir die Erkenntnis gezogen, zusammen mit unserem Kooperationspartner FINLEX GmbH eine Branchenlösung für Cyber-Risiken zu entwickeln. Die bis zu diesem Zeitpunkt gebotenen Versicherungslösungen waren nicht auf die speziellen Risiken unserer Branche abgestellt. So wie in allen anderen Versicherungsbereichen haben wir uns daher auf das Wesentliche für unsere Maschinenbauer konzentriert. Alle führenden Cyber-Versicherer haben wir kontaktiert und nach einer Lösung gesucht. Wir freuen uns mit dem nunmehr bestehenden Konsortium eine wirklich branchengerechte Versicherungslösung bieten zu können.

Frau Kress-Happel, wie schätzen Sie aus Versicherersicht und der bisherigen Erfahrungen den Status bezüglich Cyberrisiken im deutschen Maschinenund Anlagenbau ein?

In den letzten Jahren konnten wir auch aufgrund der zunehmenden Digitalisierung und Vernetzung einen Umbruch innerhalb der Branche beobachten. Viele Maschinenbauer wenden sich einem hybriden Geschäftsmodell zu: sie produzieren Maschinen- und Anlagen, statten diese auch mit entsprechender Software aus, bieten ihren Kunden IT-Dienstleistungen und warten die Maschinen und Anlagen remote. Dies führt dazu, dass sich die Unternehmen eingehend mit allen Themen rund um Industrie 4.0 beschäftigen. Dazu gehört zum einen das Erstellen sicherer Anwendungen und Anlagen, zum anderen schwenkt es aber auch den Fokus aufs eigene Unternehmen und damit auf die eigene IT und Datensicherheit. Das Thema IT-Sicherheit hat daher mehr denn je einen hohen Stellenwert – sowohl was die unternehmenseigene Cyber Security angeht als

auch jene der Produkte –, denn die hieraus entstehenden Risiken können für das Unternehmen weitreichende Folgen haben. Das gilt einerseits im Hinblick auf die Reputation und Haftung aus Produkten, zum anderen aber auch für eigene Produktionsausfälle – bedingt durch eine zunehmend vernetzte Produktion – oder sonstigen Kosten, die bei einer Cyberattacke entstehen können. Ferner lassen sich die Risiken eines Maschinen- und Anlagenbauers nicht mit denen eines reinen Bürobetriebes vergleichen. Der Fokus liegt hier ganz klar auf der OT (operational technology) und auch die Angriffsvektoren sind in diesem Umfeld besonders. Als plakatives Beispiel zur Verdeutlichung können die sogenannten Legacy-Systeme dienen: Aus den meisten Bürobetrieben wurden diese längst verbannt, aber in der Produktion ist dies nicht immer möglich, da mit diesen Systemen Produktionsanlagen gesteuert werden und ein Austausch dieser Systeme entweder wirtschaftlich nicht zumutbar oder technisch schlicht unmöglich ist. Dies ist eine besondere Risikosituation und führt dazu, dass man diesem Thema im Underwriting eine gewisse Bedeutung beimessen muss.

Welche Maßnahmen hinsichtlich des Risikomanagements können Maschinenund Anlagenbauer ergreifen?

Der Maßnahmenkatalog zur Risikominimierung in der IT kann nicht abschließend definiert werden, da es mittlerweile unzählige Standards und Zertifizierungen gibt, die ein Unternehmen umsetzen kann. Oftmals sind es ressourcenverzehrende und langwierige Zertifizierungswege, vor denen sich insbesondere der Mittelstand scheut. Umso wichtiger ist es, branchenübliche Standards zu definieren, die durch den Verband von fachkundigen Mitgliedern für Mitglieder herausgegeben werden, wie es zum Beispiel bei dem VDMA Kompetenzcenter Industrial Security der Fall ist. Aus Versicherersicht ist neben den allgemeinen Maßnahmen für IT- und Datensicherheit insbesondere auf folgende Themen Augenmerk zu legen: Härtung, Authentifizierung, solides Patchmanagement,

Segmentierung zwischen Büro- und Produktions-IT, Remote-Zugänge und Notfallpläne.

Speziell für die finanzielle Risikominimierung kann die Cyberdeckung hilfreich sein – welche speziellen Merkmale enthält die VSMA-Police?

Die Besonderheit der VCP-Police liegt darin, dass es sich hierbei um ein für die Branche maßgeschneidertes und exklusives Produkt handelt, das auf Grundlage der Bedürfnisse ebendieser Branche – untermauert mit der besagten Umfrage – geschaffen wurde. Dies spiegelt sich selbstverständlich auch im Bedingungswerk wider. Weiterhin ist hier hervorzuheben, dass mit Unterstützung der FINLEX GmbH der Abschluss- und Underwriting-Prozess digital gestützt ist. Dies erleichtert das Handling im Tagesgeschäft und schont Ressourcen.

Das Interview führte

Kerstin Hartung Alexandre
für Face, 2019 Ausgabe 2

Beitragsbild: ipopba / iStock

Kontakt:
Herr Thomas Völker
VSMA GmbH – ein Unternehmen des VDMA
Telefon +49 69 6603-1520
tvoelker@vsma.org

VDMA Cyber-Police