Umfassende Risikoabsicherung & Prävention
bei Schäden aus der Digitalisierung im Maschinen- und Anlagenbau

Risikotransfer im Bereich Smart Factory & Industrial IoT

? Digitalisierung sowie Industrie 4.0 sind brennende Themen, wenn es um die Zukunft unserer Gesellschaft in der globalisierten Welt geht. Parallel dazu steigt die Zahl der Cyberattacken weiter signifikant an. Die Risiken und Gefahren für einzelne Unternehmen aber auch für die ganze Gesellschaft sind real. Wie schätzen Sie das Bewusstsein der Industrieunternehmen in diesem Zusammenhang ein?

Nun, die Entwicklung ist in der Tat äußerst kritisch zu betrachten. In erster Linie sind es insbesondere die Softwareunternehmen und IT-Dienstleister, welchen hier eine besondere Verantwortung hinsichtlich der Sicherheit ihrer Produkte zukommt. Verfolgt man die Medienberichterstattung beschränkt sich diese allerdings fast ausschließlich auf die Gefahren von Cyberrisiken. Auch wenn dies ein wesentlicher Bestandteil des »Gefahrenpotenzials« darstellt, ist mir diese Sichtweise zu kurz gedacht. Schließlich können nicht nur Cyberrisiken zu massiven Schäden führen, sondern auch menschliches Versagen oder fehlerhafte Entwicklung im Bereich der Softwareprogrammierung.

Ganzheitliches IT-Sicherheitsmanagement in Unternehmen besteht aus den vier Säulen Technik, Organisation, Menschen und Absicherung des Restrisikos. Im Interview erläutert Peter Janson, Prokurist der Dr. Hörtkorn München GmbH, wie sich Maschinenbauer gegen die Risiken der industriellen IoT absichern können.

Die Kombination aus technischen, organisatorischen und personellen Maßnahmen sind wesentlicher Bestandteil eines ganzheitlichen IT-Sicherheitsmanagements in Unternehmen. Doch erst wenn die vierte Säule, nämlich der Risikotransfer in Form der Absicherung von verbleibenden Restrisiken über adäquaten Versicherungsschutz hinzukommt, ist das IT-Sicherheitsmanagement vollständig.

Und genau hier gibt es noch viele »weiße Flecken«, welche teils mangelnder Bereitschaft der Unternehmen sich mit diesem Thema zu beschäftigen, teils aufgrund nicht vorhandenen geeigneten Versicherungslösungen eine große Herausforderung darstellen.

? Können Sie das etwas konkretisieren?

Versetzen wir uns zunächst in die Welt der IT-Unternehmen. Deren Produkte und Dienstleistungen sind ja quasi der »Motor« der Digitalisierung.

Betrachten wir mögliche Schadensszenarien müssen wir zunächst in drei Kategorien unterscheiden: Personen-, Sach- und/oder reine Vermögensschäden. Der Fokus für IT-Unternehmen liegt dabei eindeutig in der Absicherung von reinen Vermögensschäden.

So ist es heute bei vielen Versicherungen Usus, nicht nur die obligatorische Haftung bei Verschulden, sondern auch die verschuldensunabhängige Haftung, insbesondere bei Abweichen von vereinbarten Beschaffenheiten von Produkten und Leistungen, wie etwa im Rahmen von Service Level Agreements oder Dauerschuldverhältnissen abzusichern. Selbst bei den durch Versicherer bislang sehr zurückhaltend behandelten Themen wie »pauschalierter Schadensersatz« oder »Vertragsstrafen« gibt es inzwischen Bewegung.

Unter den Versicherungsschutz fallen dabei nicht nur die zivilrechtlichen Schadensersatzansprüche Dritter infolge mangelhafter Produkte oder Leistungen, sondern auch Haftpflichtansprüche in Zusammenhang mit »Cyberschäden«.

Darüber hinaus kann sich das IT-Unternehmen durch Assistance-Dienstleistungen auch Forensik-Spezialisten sowie die Absicherung von Eigenschäden, etwa bei Ertragsausfall oder Cybererpressung, in Form einer Cyberpolice einkaufen.

Zusammengefasst soll das heißen, dass es für Softwareentwickler und IT-Dienstleister inzwischen ausreichende Lösungen gibt, um sich selbst aber auch Dritte vor selbst- oder fremdverschuldeten Schadensszenarien hinreichend zu versichern.

Gehen wir jedoch in die Welt der »Smart Factory beziehungsweise Industrial IoT« sieht das Bild ganz anders aus. Bisher waren die IT und die IoT zwei getrennte Bereiche. Das hat sich mittlerweile komplett geändert.

Die Integration der Operation Technology (OT) in die Welt des Internets – was häufig auch unter dem Stichwort Industrie 4.0 zusammengefasst wird – bringt in Sachen Sicherheitsmanagement völlig neue Anforderungen. In diesem Zusammenhang ist auch ein »neues Denken« im Bereich des Risikotransfers dringend erforderlich.

Gerade die Bereiche Maschinenbau, Robotik und Automation stehen in Verbindung mit Industrie 4.0 vor großen Aufgaben. Um im internationalen Wettbewerb bestehen zu können, muss diese »klassische Industrie« in Sachen Digitalisierung massiv investieren und aufrüsten. Ziel ist es mit digitalisierten Wertschöpfungsketten zusätzliche Effizienzsteigerung zu erreichen, aber auch durch zusätzliche Services wie Prozessüberwachung, Prozessoptimierung, Fernwartung, regelmäßige Updates oder

Upgrades bisher unerschlossene Umsatzpotenziale neu zu erschließen.

Doch der unvermeidlich weiter anwachsende Einfluss der Digitalisierung in diesen Branchen erhöht auch deren Störanfälligkeit. Neue digitale Gefahren und neue Services brauchen auch neue Lösungen zur Schadenverhütung. Schnelle und kompetente Reaktion bei Störungen sind erforderlich, um existenziellen Schaden von Unternehmen fernzuhalten. Versicherer setzen aktuell jedoch noch immer auf das gängige Produkthaftpflichtmodell aus dem letzten Jahrtausend, welches sich in erster Linie mit Personen- und Sachschäden aus der »analogen« Welt beschäftigt. Zwar werden auch heute schon gewisse Vermögensschäden aus IT-Risiken mitversichert, dies deckt den neu entstandenen Bedarf jedoch nicht ansatzweise ab. Insbesondere setzt die Leistung des Versicherers erst dann ein, wenn der Schaden schon eingetreten ist. Unterstützung im Rahmen einer schnellen und wirksamen forensischen Ursachenforschung, um Schäden in einem frühen Stadium einzufangen und klein zu halten, »Fehlanzeige«. Gleiches gilt auch für die aufgrund der Digitalisierung erforderlichen und bereits erwähnten neuen Services.

Die Maschinenbaubranche verfügt zwar meist über eigene Servicetechniker, diese sind in aller Regel aber eher analog ausgerichtet und mit Problemen wie beispielsweise bei der Steuerungssoftware überfordert. Stellen wir uns nur einmal vor was passiert, wenn ein international tätiges Maschinenbauunternehmen über eine eigene zentrale Cloudlösung alle Maschinen, welche bei Kunden weltweit im Einsatz sind, steuert. Aufgrund einer digitalen Störung fallen nun die Maschinen zeitgleich aus. Ein Horrorszenario, bei dem es ganz schnell um die Existenz des Unternehmens gehen kann. Schnelle forensische Untersuchung der Ursache ist hier von elementarer Bedeutung. Doch was, wenn die eigenen Servicetechniker das Problem nicht in den Griff bekommen?

? Welche Lösungsansätze bietet die Versicherungsbranche derzeit?

Aktuell können Maschinenbauunternehmen hinsichtlich ihrer digitalen Risiken bereits eine Cyberversicherung abschließen, welche neben Eigenschäden auch eine Vermögensschadenhaftpflicht bei Drittschäden bietet. Im Fokus stehen dabei Informations- und Netzwerksicherheitsverletzungen, welche gegenüber Dritten entstehen können.

Wie eine kürzlich erschienene Auswertung des Gesamtverbandes der Deutschen Versicherungswirtschaft im Rahmen eines Branchenchecks aufzeigt, ist im Bewusstsein hinsichtlich der Notwendigkeit sich gegenüber Cyberrisiken im Maschinenbau abzusichern noch deutlich Luft nach oben. Demnach ist jeder dritte Maschinenbauer bereits Ziel von Cyberkriminalität geworden, 10 % davon sogar schon mehrmals. Ungeachtet dessen halten immer noch 38 % der Maschinenbauunternehmen in Deutschland das Risiko von einem Cyberangriff getroffen zu werden für »eher beziehungsweise sehr gering«. Frei nach dem Sankt-Florian-Prinzip sehen sogar 55 % die Risiken als »eher beziehungsweise sehr gering« an, wenn es um die Einschätzung für das eigene Unternehmen geht.

Eine »klassische« Betriebs- und Produkthaftpflichtversicherung gehört dagegen für den deutschen Maschinenbau zur »Grundausstattung«.

? Was müsste aus Ihrer Sicht von Seiten der Versicherer getan werden, um gegen die neuen digitalen Risiken im Bereich »Smart Factory« gerüstet zu sein?

Im Prinzip ist die Maschinenbaubranche mit zunehmendem Anteil der Digitalisierung versicherungstechnisch wie ein IT-Unternehmen zu sehen. Nur eben zusätzlich mit den klassischen Risiken eines Maschinenbauers.

Nehmen wir einmal an, wir verknüpfen die IT-Vermögensschadenhaftpflicht mit einer industriellen klassischen Betriebshaftpflicht. Nehmen wir ferner an, dass wir im Rahmen dieser neuartigen Haftpflichtpolice auch eine Assistancedienstleistung nach ISO 27001 integrieren, welche die Anforderungen zur Behandlung sicherheitsrelevanter Pro bleme nach IEC 62443-4.1 erfüllt. Diese Assistance hat eine 24/365 Erreichbarkeit und ist in der Lage sich innerhalb kürzester Zeit unterstützend in die Forensik einzuschalten.

? Sie meinen also, eine Haftpflichtpolice analog eines IT-Unternehmens mit integrierter Schadenprävention? Um im Bedarfsfall den Schaden schnellstmöglich zu identifizieren und die Auswirkungen klein zu halten?

Genau so etwas meine ich.

? Das klingt spannend, aber ist so etwas in absehbarer Zeit realistisch?

Die Versicherer sind, was neue Risiken angeht, grundsätzlich immer eher zurückhaltend, weil man diese statistisch schwer oder überhaupt nicht erfassen kann. Dies ist jedoch die Voraussetzung für das sogenannte Underwriting und Pricing eines Versicherers. Doch wenn Deutschland im Bereich Industrie 4.0 nicht den Anschluss verlieren will, wird auch der Versicherungsmarkt reagieren müssen.

Als spezialisierter Versicherungsmakler für IT-Unternehmen und Cyberrisiken haben wir vor geraumer Zeit genau ein solches Produkt mit einem auf IT-Risiken spezialisierten Versicherer sowie einem vom BSI als APT-Response-Dienstleister qualifizierten Krisenmanagementunternehmen auf den Markt gebracht. Der Startschuss ist also bereits gefallen. Wenn dieses Haftpflichtprodukt, wovon wir überzeugt sind, sich in absehbarer Zeit erfolgreich am Markt positioniert, werden andere Versicherer sicherlich nachziehen. Schließlich existiert in der Versicherungsbranche auch eine sehr große Begehrlichkeit nach Marktanteilen.

Das sind ja wirklich interessante Neuigkeiten. Vielen Dank für das Gespräch.