itsecurity
DEZEMBER 2019

DAS SPEZIAL

VERSICHERUNGSSCHUTZ FÜR UNTERNEHMEN

RISIKO CYBERKRIMINALITÄT

Tobias von Mäßenhausen, AXA Konzern AG

FÜHRUNGSKRÄFTE & IT SICHERHEIT

Mangelnde Unterstützung

ZERO TRUST-PLATTFORM

Never Trust, always verify

IIOT-SCHWACH-STELLEN

Unterstützung für IT und OT

ab Seite 20

IAM CONNECT 2020

Die Brücke zu neuen Geschäftsmodellen

16. bis 18. März 2020
Berlin Marriott Hotel – Inge-Beisheim-Platz

www.iamconnect.de

Save the Date!

Eine Veranstaltung von itmanagement & itsecurity

4
COVERSTORY

INHALT

WIR BIETEN UNTERNEHMEN EIN VERSICHERUNGSKONZEPT AN, DAS DANK EINES MODULAREN BAUSTEINPRINZIPS GENAU DER ERFORDERLICHEN VERSICHERUNGSLEISTUNG ENTSPRICHT.

Tobias von Mäßenhausen,
Leiter Technische und Cyber-Versicherungen,
AXA Konzern AG, www.axa.de

RISIKO CYBERKRIMINALITÄT

VERSICHERUNGSSCHUTZ FÜR UNTERNEHMEN

Unternehmen sind zunehmend Bedrohungen und Risiken aus Cyberspace und durch IT ausgesetzt. Dabei kann Cyberkriminalität jedes Unternehmen teuer zu stehen kommen. Mit einer Cyber-Versicherung kann das finanzielle Risiko reduziert werden. Was aber, wenn trotzdem etwas passiert? Darüber sprach Ulrich Parthier, Herausgeber it-security, mit Tobias von Mäßenhausen, Leiter Technische und Cyber-Versicherungen bei AXA.

? **Ulrich Parthier:** Ein Unternehmen ist Opfer eines Cyberangriffs geworden und nicht mehr handlungsfähig. AXA kann hier Abhilfe schaffen?

Tobias von Mäßenhausen: Ja, genau hier tritt AXA auf den Plan. Im Falle eines Cyberangriffes ist sehr schnell das gesamte IT-System betroffen, wodurch der unternehmerische Schaden enorm sein kann.

Als Versicherung ist unser Kerngeschäft die Sicherheit. Das bedeutet nicht, dass wir nur eine „Zahlstelle" sind, wenn es zum Schaden gekommen ist, sondern dass wir unsere Kunden in diesen kritischen Momenten begleiten. Es geht darum, kurzfristig Maßnahmen zu ergreifen und einen Schaden zu verhindern oder zu begrenzen. Hierfür haben wir ein Netz aus Dienstleistern und Kooperationspartnern aufgebaut, mit denen wir schnelle Unterstützung und Beratung bei der Wiederherstellung des Betriebes leisten können.

? **Ulrich Parthier:** Jeder Cyberangriff ist unterschiedlich - woher kann ein Unternehmen im Vorfeld wissen, wogegen es sich absichern muss?

Tobias von Mäßenhausen: Hierbei gilt es, drei wichtige Aspekte zu betrachten:

1. Woraus können die größten Schäden resultieren? Sprich, welche Cybergefahren sind für mein Unternehmen am wahrscheinlichsten.

2. Wo werden die größten Auswirkungen erwartet? Die letzten Jahre zeigen, dass dies insbesondere im Bereich der Betriebsunterbrechung und der Datenwiederherstellung der Fall ist.

3. Wie teuer wird es, den Schaden und seine Auswirkungen zu beheben?

Hieraus ergibt sich, welche Maßnahmen für Unternehmen sinnvoll sind. AXA bietet Unternehmen ein individuelles Versicherungskonzept an, das dank eines modularen Bausteinprinzips so individu-

ell zusammengestellt werden kann, dass es genau der erforderlichen Versicherungsleistung entspricht.

Somit können Schäden durch Cyber-Angriffe zwar nicht vollständig verhindert werden, im Schadensfall erhalten versicherte Unternehmen jedoch schnelle und individuelle Unterstützung.

? **Ulrich Parthier:** Sind präventive Schutzmaßnahmen im Zweifel nicht sinnvoller, als die Absicherung eines eventuellen Schadenfalls?

Tobias von Mäßenhausen: Das eine schließt das andere nicht aus. Ich trage als Unternehmer immer die Verantwortung für die Sicherheit in meinem Unternehmen, aber gegen alle Cyber-Risiken kann man sich nun mal nicht schützen. Es gilt abzuwägen, welche Absicherung für ein Unternehmen sinnvoll ist und welche eher nicht.

Man sollte ganz konkret schauen, welche Kosten in Abhängigkeit vom Risiko entstehen können und dann entscheiden, ob und in welcher Höhe eine Investition in eine Cyber-Versicherung betriebswirtschaftlich Sinn ergibt.

? **Ulrich Parthier:** Und gibt es Möglichkeiten, durch entsprechende Schutzmaßnahmen Einfluss auf den letztendlichen Versicherungsbeitrag zu nehmen?

Tobias von Mäßenhausen: Wir honorieren, wenn Kunden proaktiv mit ihren Risiken umgehen und mitwirken. Kunden, die sich allein auf ihre Versicherung verlassen möchten, werden vorher geprüft und nicht ohne Weiteres versichert. Wir legen Wert auf ein hohes und homogenes Sicherheitsniveau unserer Versichertengemeinschaft, sodass ein Ausgleich des guten Vertrags für den schlechten Vertrag nicht in Frage kommt.

Wir setzen zudem bei allen unseren Kunden grundlegende Maßnahmen zur IT-Sicherheit voraus. Dazu gehören sowohl technische als auch organisatorische Maßnahmen, wie beispielsweise eine Firewall und Antivirensoftware, ein Patchmanagement-System zur Schließung von Sicherheitslücken sowie – besonders wichtig – regelmäßige Back-Ups der Daten.

? **Ulrich Parthier:** Worauf kommt es also beim Risikomanagement an?

Tobias von Mäßenhausen: Das Wichtigste ist erstmal das Bewusstsein innerhalb des Unternehmens – insbesondere der Geschäftsleitung – dass IT-Sicherheit ein wichtiges Thema ist. Denn ein effektiver Schutz gegen Hackerangriffe und vergleichbare Attacken kann in der Regel nur durch das Unternehmen selbst gewährleistet werden.

Risikomanagement ist am Anfang erstmal ganz losgelöst von der Versicherung, sondern fängt mit anderen Dingen an – beispielsweise:

1. Wie wir der Datenschutz sichergestellt?
2. Wie ist meine Internetseite dargestellt?
3. Wie erfolgen Back-Ups?
4. Und vor allem: Ist Budget für Cyber-Risikomanagement vorhanden?

Wir sehen allerdings, dass dieses Bewusstsein in kleineren Unternehmen deutlich abnimmt, wobei gerade hier die Attacken am erfolgreichsten sind.

? **Ulrich Parthier:** Wenn aber trotz aller Sicherheitsvorkehrungen der Schadenfall eintritt - das Unternehmen also nicht mehr arbeitsfähig ist. Wie kann AXA hier ganz konkret unterstützen?

Tobias von Mäßenhausen: Wir bieten eine 24/7 Hotline an, mit der unser Kunde mit einem IT-Dienstleister die Situation direkt analysieren und umgehend Maßnahmen einleiten kann.

Oft ist es leider so: Der Kunde wird gehackt und versucht direkt mit seinem Back-Up zu retten, was zu retten ist. Wenn er jetzt die Back-Up-Festplatte an das infizierte System anschließt, ist das Back-Up befallen und nicht mehr nutzbar. Deswegen ist es wichtig, im ersten Schritt schnelle professionelle Hilfe und einen Expertenrat einzuholen, um Bedienungsfehler und eine Ausweitung des Schadens zu verhindern und die richtigen Maßnahmen anzustoßen.

Im zweiten Schritt erfolgt dann die Sicherung und Wiederherstellung der Daten – dies wird dann häufig vor Ort vorgenommen.

Alternativ haben unsere Kunden auch die Möglichkeit, direkt mit ihrem eigenen IT-Dienstleister zu arbeiten und Sofortmaßnahmen ohne vorherige Absprache mit uns einzuleiten. Da der eigene Dienstleister die Kunden-IT bereits kennt, kann damit das Schadenausmaß häufig schnell und effektiv reduziert werden.

! **Ulrich Parthier:** Herr von Mäßenhausen, wir danken für dieses Gespräch.

RISIKEN DER DIGITALISIERUNG

KÖNNEN CYBER-VERSICHERUNGEN ABHILFE SCHAFFEN?

Der digitale Wandel vollzieht sich immer rasanter und das Verlangen nach Effizienzsteigerung treibt konsequent Veränderungen voran. Auch Unternehmen bekommen diesen Wandel zu spüren: Um wettbewerbsfähig zu bleiben, werden Prozesse digitalisiert und automatisiert, Abteilungen vernetzt und Geschäftsinformationen in der Cloud gesichert. Neben massiven Vorteilen bringt diese Entwicklung auch große Gefahren mit sich.

Die Schattenseiten des digitalen Zeitalters

Cyber-Kriminalität ist auf dem Vormarsch. Cyber-Attacken richten sich dabei nicht unbedingt direkt gegen ein bestimmtes Unternehmen. Oft führen nicht zielgerichtete Angriffe auf eine Vielzahl von Unternehmen ebenfalls zum Ziel. So steigt die Zahl der sich im Umlauf befindlichen Schadprogramme seit Jahren kontinuierlich an und lag im Jahr 2018 bereits bei circa 800 Millionen – 200 Millionen mehr als ein Jahr zuvor. Tagtäglich registrieren IT-Sicherheitsunternehmen viele Hunderttausende Cyber-Attacken. Wo früher nur das Betriebssystem oder der Browser angreifbar waren, ergeben sich heute weitreichende Möglichkeiten. Informationen zu Überwachungskameras, Smart Homes oder IoT-Geräten können schnell und unkompliziert online erbeutet werden – der Hack ist meist nur noch einen Mausklick entfernt. Laut einer Umfrage des BSI waren bereits 70 Prozent der deutschen Unternehmen Opfer von Cyber-Angriffen – hierbei konnte sich jeder zweite Angreifer Zugriff auf IT-Systeme verschaffen, jeder vierte führte zu teilweise verheerenden und kostspieligen Produktions- und Betriebsausfällen sowie weiteren Kosten für die Wiederherstellung der IT, Imageschäden oder Drittansprüchen.

Auch der Netzwerkausrüster Cisco kommt in einer Studie mit Teilnehmern aus 26 Ländern zu dem Ergebnis, dass mehr als die Hälfte der mittelständischen Unternehmen im Jahr 2018 eine Datenpanne erlitten hatten, insbesondere durch Phishing, also betrügerische Angriffe auf Mitarbeiter, aber auch durch Malware und DDos-Attacken. Nicht selten bekommen Angreifer erst über die ungewollte Mitwirkung von Mitarbeitern Zugang zur geschützten Infrastruktur eines Unternehmens. Das BSI rät derzeit erneut vor der „weltweit gefährlichsten Schadsoftware Emotet", die Nutzer dazu bringt, infizierte E-Mail-Anhänge zu öffnen und hierdurch Malware zu installieren. Erst kürzlich sorgte eine neue Angriffswelle binnen weniger Tage für erhebliche Schäden in der deutschen Wirtschaft, bei Behörden und Organisationen. Für Unternehmen stellt sich daher nicht die Frage, ob sondern wann sie Opfer einer Cyber-Attacke sein wird.

Wie kann sich ein Unternehmen schützen?

Unternehmen werden sich des Risikos immer bewusster, der Markt um IT-Experten boomt. Gezielte Maßnahmen können das Risiko eines Cyber-Angriffs bereits wesentlich einschränken. Durch das Verwenden von professionellen Firewalls und Antivirenprogrammen erlangt das Unternehmen einen Grundschutz. Sicherheitslücken sollten durch regelmäßige Softwareaktualisierungen geschlossen werden. Tägliche Datensicherungen und regelmäßige Wiederherstellungstests können vor großen Datenverlusten schützen. Ein Berechtigungsmanagement verwehrt unbefugten Personen Zugang zu kritischen Geschäftsprozessen und kann die Reichweite des Angriffs einschränken. Auch der Faktor Mensch sollte nicht zu kurz kommen. Regelmäßige Schulungen zur IT Sicherheit sensibilisieren Mitarbeiter und können Fehlentscheidungen minimieren. Genaue Handlungsanweisungen und Notfallmaßnahmen sollten für Worst-Case-Szenarien bereits vorab in einem Notfallplan klar definiert sein, um Chaos im Krisenfall zu vermeiden.

Cyber-Versicherung als Ergänzung zur IT-Sicherheit

Leider bietet keine Maßnahme einen allumfassenden Schutz gegen Cyber-Kriminalität, ein Restrisiko verbleibt. Dies haben auch die Versicherer erkannt und in den letzten Jahren zunehmend neue Versicherungsprodukte auf den Markt gebracht. Zwar gibt es Unterschiede in Bedingungen und Deckungsumfang, im Kern haben sie jedoch dasselbe Ziel: Eine Cyber-Versicherung soll Unternehmen vor Vermögensschäden als Folge von Hacker-Angriffen oder sonstigen Akten der Cyber-Kriminalität schützen. Hierbei werden sowohl Eigen- als auch Drittschäden versichert, darunter fallen zum Beispiel Daten-, Betriebsunterbrechungs- und Haftpflichtschäden.

Die Deckungsinhalte sind umfangreich, unter anderem werden folgende Kosten ersetzt:

- Betriebsunterbrechungsschäden, insbesondere Ertragsausfälle und Mehrkosten. Einige Anbieter übernehmen

ebenfalls Rückwirkungsschäden durch Ausfall eines Clouddienstleisters

- IT-Forensikkosten zur Schadenermittlung und Schadensuche

- Kosten für die Wiederherstellung von Daten und Programmen in den früheren, betriebsfertigen Zustand. Hierunter fallen die Wiederbeschaffung und Wiedereingabe von Daten oder die Beseitigung von Schadsoftware

- Kosten eines Krisenmanagements, rechtliche Beratungen oder externe Kommunikation durch Pressearbeit zur Abwendung oder Minderung eines Reputationsschadens

- Aufwendungen, die durch gesetzlich geforderte Maßnahmen anfallen, insbesondere auch Kosten eines behördlichen Meldeverfahrens oder die Einrichtung eines Call-Centers für Betroffene bei Datenschutzvorfällen

- Kosten für die Abwehr von Haftpflichtansprüchen Dritter z.B. aus Datenschutzverletzungen, aufgrund eines Hacker-Angriffs oder aus unberechtigter Verbreitung von Daten und Programmen

- Kosten, die durch Schäden eines Identitätsdiebstahls oder Manipulation entstehen können

Eine schnelle Reaktionsfähigkeit kann im Krisenfall in vielerlei Hinsicht den Schaden drastisch minimieren. Daher bieten Cyber-Versicherer zusätzlich zum Deckungsumfang wichtige Serviceleistungen an. So besteht die Möglichkeit als Versicherungsnehmer rund um die Uhr über eine Notfallhotline an fachkompetente IT-Dienstleister zu gelangen, die im Krisenfall Soforthilfe leisten. Insbesondere kleine und mittelständische Unternehmen schätzen diesen Service sehr. Ein weiterer Service wird im Rahmen der Präventionsmaßnahmen angeboten. So können Mitarbeiter durch kostenfreie Awareness-Schulungen sensibilisiert werden und Unterstützung beim Ausbau der IT-Sicherheit kann, etwa durch Mithilfe bei der Erstellung eines Notfallplans, angefragt werden.

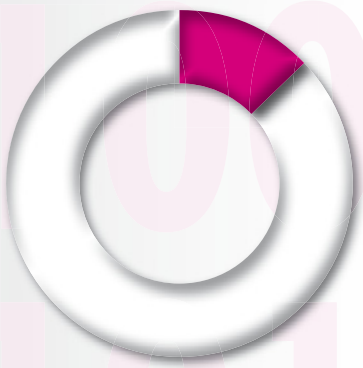
Der Nutzen einer Cyber-Versicherung ist für Unternehmen immens, insbesondere vor dem Hintergrund, dass die vielfältige finanzielle Absicherung und die angebotenen Serviceleistungen bereits für wenige Hundert Euro im Jahr erhältlich sind. Als Grundvoraussetzung für den Abschluss einer Versicherung verlangen die Versicherer einen gewissen Reifegrad der bereits umgesetzten technischen, organisatorischen und prozessualen Maßnahmen. Da die Geschäftsführung oft mit der Bewältigung von IT-Risiken überfordert ist, sollte der IT-Leiter im Rahmen des Risikomanagementprozesses mit der Geschäftsführung Risiken identifizieren und zu ergreifende Bewältigungsmaßnahmen auswählen. Es sollte geklärt werden, welche Informationen und Unternehmensdaten besonders schützenswert und auf welche Art und Weise diese bereits abgesichert sind. Im letzten Schritt kann dann entschieden werden, ob das verbleibende finanzielle Restrisiko eines Cyber-Vorfalls durch das Unternehmen selbst getragen werden soll oder durch den Abschluss einer Cyber-Versicherung auslagert wird.

Donja Torabian, www.axa.de

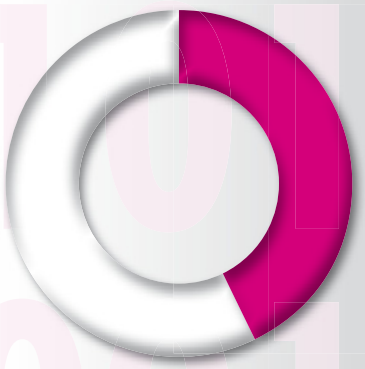
BYTE PROTECT 5.0 VON AXA

- **sichert Cyber-Risiken wirkungsvoll ab**
- **versichert Eigenschäden und Drittschäden**
- **ist durch das flexible Bausteinprinzip individuell an Unternehmensbedürfnisse anpassbar**
- **ist für jede Unternehmensbranche und -größe geeignet**
- **bietet sowohl die freie Wahl des IT-Dienstleisters im Krisenfall, als auch die Möglichkeit der Nutzung einer 24/7 Notfallhotline**

RISIKOMANAGEMENT IM UNTERNEHMEN



13 %
der Unternehmen erklären, dass derzeit ein Risikomanagement implementiert wird



43 %
der Unternehmen betreiben aktuell kein gezieltes Risikomanagement

(Quelle: AXA Konzern AG)

IIOT-SCHWACHSTELLEN MANAGEMENT

UNTERSTÜTZUNG FÜR IT UND OT BEI DER EINFÜHRUNG EINER GEMEINSAMEN SPRACHE

Es ist höchste Zeit, dass sich IT- und OT-Profis beim Schwachstellenmanagement in der Industrie 4.0 auf eine gemeinsame Sprache verständigen, um ihre Systeme zu schützen.

IT- und Produktions-Betriebstechnik (OT) Teams sind sich der Hemmnisse bewusst, die es im Bereich Cybersecurity zu überwinden gilt, um eine erfolgreiche Implementierung des Industrial Internet of Things (IIoT) zu erreichen. Trotzdem gehen in vielen Fällen die einzelnen Abteilungen an diese Bedrohungen mit sehr unterschiedlichen Prioritäten heran.

Für IT-Teams erfordert das Endpunktmanagement ein sehr Detailorientiertes Arbeiten. Denn in der IT besteht das Ziel darin, autorisierten Netzwerkbenutzer sicheren und zuverlässigen Dateizugriff zu ermöglichen. Auf der anderen Seite ist für die OT-Teams die oberste Priorität eine stabile Produktionslinie aufrechtzuerhalten. Aus diesem Grund ist bei den OT-Teams eher die Mentalität verbreitet: „Wenn es nicht kaputt ist, lass die Finger davon". Ein Beispiel für diesen Zwiespalt ist die Kohleindustrie, wo es einfach keine „schnellen Lösungen" für Sensoren, Maschinen und Steuerungssysteme gibt. Änderungen können hier das gesamte System zum Stillstand bringen, wodurch die gesamte Produktionslinie ins Stocken kommen kann.

In einem aktuellen Bericht der Beratungsgruppe McKinsey & Co. haben sich Unterschiede auf der „letzten Meile" in der IT/OT als große Hürde für Unternehmen erwiesen, die versuchen, IIoT-Programme aus der Pilotphase in eine unternehmensweite Implementierungen umzusetzen. Hier besteht die Herausforderung darin, den beiden Teams zu helfen, die Sprache des jeweils anderen zu verstehen und gleichzeitig das für ihre Arbeitsumgebung passende Verfahren für Schwachstellenmanagement anzuwenden.

Probleme (zu) patchen

Innerhalb des Bereichs Patch-Management sind die deutlichsten Unterschiede in der Sprache des IIoT für IT- und OT-Pro-

WHILE PILOTS ARE COMMON, COMPANY-WIDE WOLL OUT IS STILL RAE.
Percent of solutions by type at each stage of development

Quelle: McKinsey Industry 4.0 Global Expert Survey 2018