Cyber-Kriminalität, ein schwer zu bewältigendes Risiko

Eva Tronberend
Cyber Underwriter

Sich schnell ändernde technologische und regulatorische Faktoren machen Cyber-Kriminalität zu einem unberechenbaren Risiko. Mit mehr Erfahrung und besseren Hilfsmitteln kann diese Gefahr jedoch besser kontrolliert werden.

Überblick

Cyber-Kriminalität ist unter den heutigen Risiken eine der größten Bedrohungen. Umfragen[1] unter weltweiten Führungskräften ergaben, dass neben geopolitischer Instabilität und dem Klimawandel Cyber-Risiken weit oben auf der Liste rangieren, wohingegen europäische Risikomanager in einer Umfrage Cyber-Kriminalität als größtes Risiko angaben.

800 Millionen

der derzeitigen Arbeitsplätze verschwunden sein bis 2030

Technologie ist ein wichtiger Aspekt des politischen und wirtschaftlichen Wandels, die beiden Hauptgründe für die steigende Unberechenbarkeit für Unternehmen, wie es der Unvorhersagbarkeitsindex (Unpredictability Index) von QBE zeigt. Soziale Medien verändern die politische Debatte während gleichzeitig erwartet wird, dass neue Technologien, wie z. B. selbstfahrende Autos, Roboter und künstliche Intelligenz das Leben der Menschen spürbar beeinflussen werden. McKinsey zufolge werden ca. 60 % aller Berufe in irgendeiner Weise von der Automatisierung betroffen sein. Gleichzeitig könnten bis 2030 bis zu 800 Millionen der derzeitigen Arbeitsplätze verschwunden sein.

Technologie steht derzeit für die meisten Unternehmen im Mittelpunkt. Sie treibt den Betrieb, die Lieferketten und den Vertrieb voran. Das Tempo, mit dem neue Technologien angenommen werden, scheint jedoch die technischen Fähigkeiten und die im Bereich der Cyber-Sicherheit der meisten Nutzer und Unternehmen zu übertreffen. Viele verstehen weder, was Cyber-Kriminalität für sie bedeutet, noch ahnen sie, welchen Einfluss diese auf ihr Unternehmen haben wird, sollte etwas schiefgehen.

Rückblickend erscheinen viele Cyber-Vorfälle vorhersehbar und sogar vermeidbar. Und doch ist es im Vergleich zu Risiken, wie Naturkatastrophen oder Feuer, mit denen wir vertraut sind und für die auf der Grundlage historischer Daten Modelle erstellt werden können, besonders schwer, das Cyber-Risiko zu ermitteln. Es ist sehr schwer vorherzusagen, wann, wo und wie ein Cyber-Vorfall auftreten wird. Selbst wo wahrscheinliche Szenarien identifiziert werden können, kann es schwierig sein, die wahrscheinlichen Folgen und möglichen finanziellen Verluste vorauszusehen und zu berechnen.

(1) Weltwirtschaftsforum Globale Risiken, 2019 PwC-Umfrage, https://www.ferma.eu/2018-european-risk-manager-report

Unzählige Unbekannte

Technologie und Cyber-Vorfälle bedeuten viele unbekannte Faktoren. Cyber-Vorfälle stammen aus vielen verschiedenen Quellen und haben viele Auslöser, wie z. B. böswillige Cyber-Angriffe, technische Störungen, Schwachstellen in der Lieferkette oder einen unaufrichtigen Mitarbeiter.

Unternehmen können nicht wissen, wie stark sie betroffen sein werden oder welche Auswirkungen ein Cyber-Vorfall auf sie haben wird. Und da jedes Unternehmen seine eigene IT-Umgebung hat, ist es schwierig, von der Erfahrung anderer zu lernen.

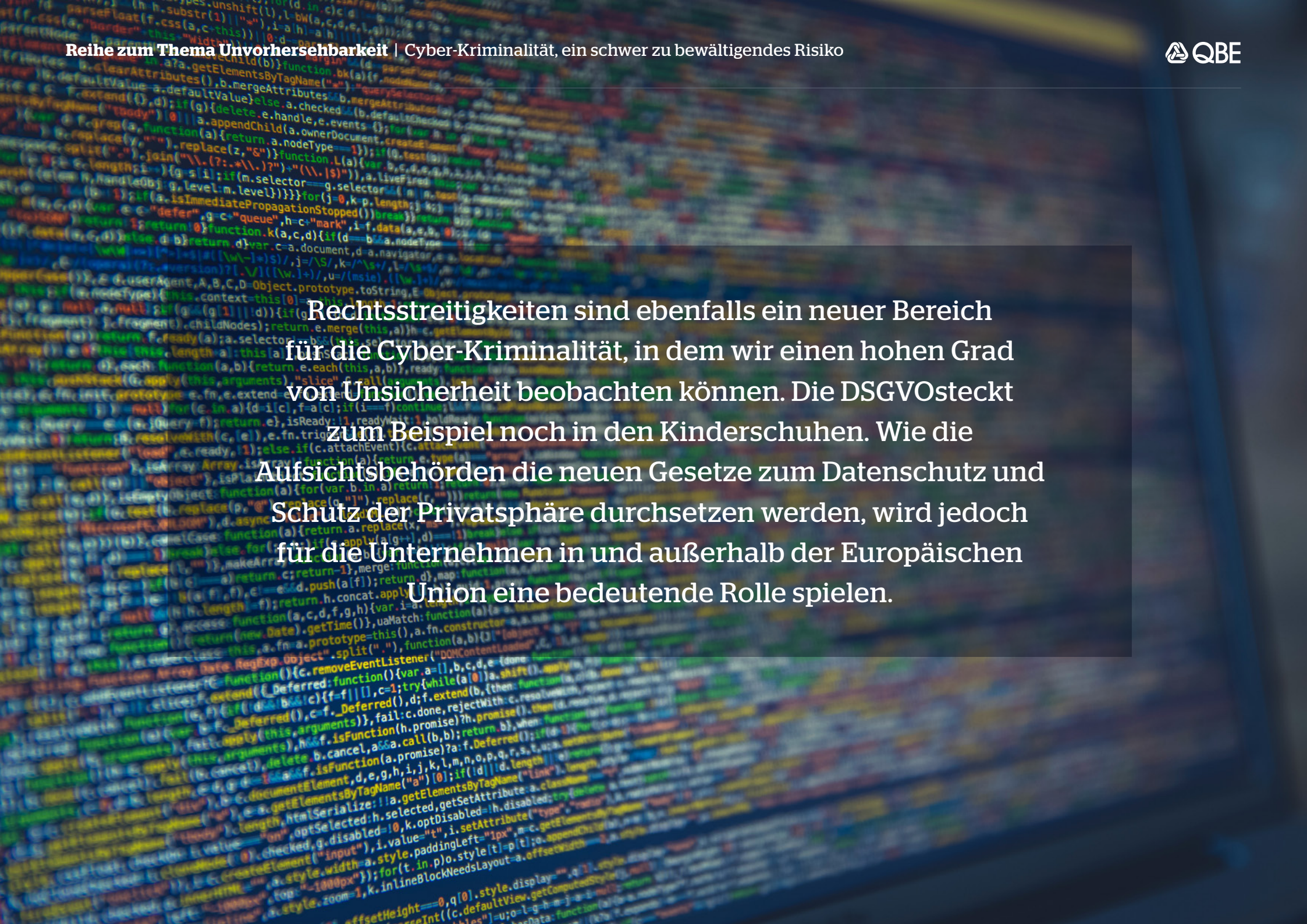
Mit Cyber-Risiken mitzuhalten ist ebenfalls eine Herausforderung. Cyber-Kriminalität ist ein nie endendes Rennen, in dem Hacker immer einen Schritt voraus sind und neue Schwachstellen an unerwarteten Stellen auftreten können. Das Ausnutzen von

> Cyber-Kriminalität ist ein nie endendes Rennen, in dem Hacker immer einen Schritt voraus sind und neue Schwachstellen an unerwarteten Stellen auftreten können.

IdD-Geräten und Schwachstellen in der Hardware (wie z. B. die Bedrohung durch Meltdown und Spectre im Jahr 2018) gehört zu den zunehmenden Gefahren, während sich nun die Aufmerksamkeit auch auf Cyber-Angriffe durch künstliche Intelligenz richtet. Wie gut die Schutzvorrichtungen eines Unternehmens auch sein mögen, es wird nie immun gegen Cyber-Angriffe sein.

Die Auswirkungen eines Cyber-Angriffs vorauszusagen ist besonders schwer, da selbst die Folgen für den gleichen Vorfall von Unternehmen zu Unternehmen stark variieren. Der NotPetya-Malware-Angriff im Jahr 2017 führte zum Beispiel bei einer Reihe von Unternehmen zu massiven Unterbrechungen, während andere Unternehmen in der gleichen Branche nicht betroffen waren.

Umfang und Interkonnektivität verstärken die Unvorhersehbarkeit, die Verletzung der Datensicherheit in den Marriott-Hotels betraf im letzten Jahr 500 Millionen Menschen und der Angriff durch die WannaCry-Ransomware im Jahr 2017 betraf geschätzte 300.000 Computer in 150 Ländern. Nach einer kürzlich durchgeführten Untersuchung von Lloyd‘s of London könnte ein großer weltweiter Malware-Angriff mehr als 600.000 Unternehmen weltweit betreffen und über 193 Milliarden USD kosten, d. h. so viel wie eine schwere Naturkatastrophe.



Rechtsstreitigkeiten sind ebenfalls ein neuer Bereich für die Cyber-Kriminalität, in dem wir einen hohen Grad von Unsicherheit beobachten können. Die DSGVOsteckt zum Beispiel noch in den Kinderschuhen. Wie die Aufsichtsbehörden die neuen Gesetze zum Datenschutz und Schutz der Privatsphäre durchsetzen werden, wird jedoch für die Unternehmen in und außerhalb der Europäischen Union eine bedeutende Rolle spielen.

Störung des Geschäftsbetriebs

Vorfälle wie WannaCry und NotPetya unterstreichen das Potenzial für durch Cyber-Angriffe verursachte Störungen des Geschäftsbetriebs und die damit verbundenen Verluste, welche angesichts der Komplexität und der Konzentration des Risikos auf die physischen und digitalen Lieferketten besonders schwer hervorzusehen und zu beziffern sind.

Ein Hersteller könnte z. B. in der Lage sein, einen Produktionsausfall auszugleichen, ihm könnten aber zusätzliche Kosten für Ausweichlösungen entstehen oder Geschäftsmöglichkeiten entgehen. Im vergangenen Jahr war der Halbleiterhersteller TSMC von einer Malware betroffen, was zu einem geschätzten Umsatzverlust von 3 % und zusätzlichen Kosten führte. Der Reederei Maersk und dem Logistikunternehmen FedEx entstanden durch den NotPetya-Angriff durch die Unterbrechung des Geschäftsbetriebs und den damit verbundenen zusätzlichen Kosten Verluste von je 300 Millionen USD, der Lebensmittelhersteller Mondelez wies im Zusammenhang mit dem Angriff Verluste von über 100 Millionen USD aus.

Als Versicherungsgesellschaft für Cyber-Risiken sehen wir viele Vorfälle, bei denen Unternehmen die Konsequenzen eines Cyber-Vorfalls nicht vollständig verstanden haben. Auch wenn sich ein Unternehmen auf mögliche Angriffe vorbereitet, ist es in der Praxis schwer, die Leistung der Kontinuitätspläne von Unternehmen vorherzusagen. So ist z. B. der Neustart von Systemen in einer kontrollierten Umgebung völlig anders als der Neustart nach einem Ausfall oder einem Angriff einer Erpressersoftware.

Rechtliche Unsicherheiten

Die Technologie ändert sich so schnell, dass sich auch die rechtlichen und regulatorischen Rahmenbedingungen ständig ändern. Das gilt insbesondere für Gesetze zum Schutz von Daten und der Privatsphäre, betrifft aber auch Anforderungen in Bezug auf den Schutz vor Cyber-Angriffen und Haftungsregelungen – z. B. werfen die Einführung von selbstfahrenden Autos, IdD und künstliche Intelligenz regulatorische und rechtliche Fragen auf.

Neue Vorschriften und ungeprüfte Gesetze schaffen für viele Unternehmen Ungewissheit, von der Größe der Strafen bis hin zur Entschädigung der betroffenen Personen. Das ist bereits in der Datenschutz-Grundverordnung der EU (DSGVO) erkennbar, die im Mai 2018 strenge Vorschriften für den Datenschutz und den Schutz der Privatsphäre eingeführt hat. Die DSGVO verleiht Aufsichtsbehörden größere Befugnisse und den Verbrauchern bessere Rechte. Es wird jedoch mehrere Jahre dauern, bis die Auswirkungen der DSGVO vollständig verstanden werden.

Rechtsstreitigkeiten sind ebenfalls ein neuer Bereich für die Cyber-Kriminalität, in dem wir einen hohen Grad von Unsicherheit beobachten können. Die DSGVOsteckt zum Beispiel noch in den Kinderschuhen. Wie die Aufsichtsbehörden die neuen Gesetze zum Datenschutz und Schutz der Privatsphäre durchsetzen werden, wird jedoch für die Unternehmen in und außerhalb der Europäischen Union eine bedeutende Rolle spielen. Die DSGVO gilt für Unternehmen, die überall in der Welt Daten aus der EU verarbeiten. Eine steigende Anzahl von Ländern versucht nunähnliche Anforderungen einzuführen.

Gerichtsverfahren sind ein sich ebenfalls entwickelndes Gebiet im Cyber-Bereich. Bisher haben wir noch kein großes Volumen an Rechtsstreitigkeiten gesehen, aber es besteht für die Zukunft eindeutig das Potenzial für eine weitaus größere Haftung gegenüber Dritten. Gesetze wie die DSGVO erleichtern es dem Einzelnen nach einem Cyber-Vorfall eine Entschädigung einzufordern. Dazu gehört auch Schadenersatz für nicht-finanzielle Schäden, wie seelisches Leid. Die Einstellung zur Privatsphäre und Betriebsunterbrechung ändert sich und eine wachsende Anzahl von Cyber-Vorfällen führt zu Sammelklagen, mit denen Investoren und Verbraucher Schadenersatz für die erlittenen Schäden fordern.

In Kürze...

Zu den Ersten gehören, die gleich nach der Veröffentlichung eine Kopie des QBE-Unpredictability Index erhalten

qbe.de

Prävention

Es ist klar, dass Cyber-Risiken nicht von der Bildfläche verschwinden werden. Ein robustes Risikomanagement und Versicherungen können jedoch die Wahrscheinlichkeit eines Angriffs verringern und Unternehmen bei der besseren Bewältigung der Auswirkungen unterstützen.

Versicherungsprodukte für den Bereich Cyber-Sicherheit werden kontinuierlich verbessert und bringen zusätzliche Gewissheit, wenn Unternehmen in neue Technologien und digitale Geschäftsmodelle investieren.

93 %

der Risikomanager eng mit ihren Kollegen in den Bereichen IT und Cyber-Sicherheit zusammenarbeiten

37 %

bereits vor der Einführung neuer Technologien durch das Unternehmen Risiken identifizieren und einschätzen

Bewährte Methoden für das Risikomanagement können zum Beispiel Unternehmen und Ihren Vorständen helfen, wenn diese sich für den Einsatz neuer Technologien und die Digitalisierung entscheiden. Eine Umfrage der Federation of Risk Management Associations (FERMA - Verbund der Risikomanagementverbände) unter Risikomanagern ergab, dass nun 93 % der Risikomanager eng mit ihren Kollegen in den Bereichen IT und Cyber-Sicherheit zusammenarbeiten und 37 % bereits vor der Einführung neuer Technologien durch das Unternehmen Risiken identifizieren und einschätzen.

Die Digitalisierung steht noch ganz am Anfang. Aber mit zunehmender Erfahrung werden Unternehmen Cyber-Risiken und Präventionen besser verstehen. In der Zwischenzeit gibt es Maßnahmen, die Unternehmen ergreifen können, um das Risiko zu reduzieren. Neben den grundlegenden Maßnahmen im Bereich der Cyber-Sicherheit, wie z. B. Penetrationstests, Patches und Schulungen, kann die Vorbereitung auf einen Cyber-Vorfall, wie einen Ausfall oder eine Verletzung der Datensicherheit, die Auswirkungen erheblich mindern.

Auf der Führungsebene sollten Unternehmen die Was-wäre-wenn-Fragen einer Verletzung der Datensicherheit oder eines Ausfalls durchspielen und Daten, Dienste und Dritte ausmachen, die für ihr Unternehmen entscheidend sind. Es ist lohnenswert , sich rechtzeitig die Zeit zu nehmen und mögliche Szenarien durchzuspielen, Maßnahmen für den Ernstfall vorzubereiten und Kontinuitätspläne

auszuarbeiten. Erfahrungen haben gezeigt, dass eine gute Vorbereitung die Auswirkungen einer Verletzung der Datensicherheit wesentlich reduzieren kann. Durch die Verbesserung der allgemeinen Widerstandsfähigkeit sollte ein Unternehmen in der Lage sein, auf einen Cyber-Vorfall zu reagieren, egal wie unerwartet dieser auch eintreffen mag.

Technologie kann Unternehmen ebenfalls helfen, indem sie Mittel bereitstellt, mit denen Cyber-Risiken eingeschätzt und quantifiziert werden können. Plattformen für die Einschätzung von Cyber-Risiken können bereits jetzt das Risiko eines Cyber-Angriffs auf ein Unternehmen und die Sicherheitsstruktur des Unternehmens einschätzen und dabei helfen, Verluste zu quantifizieren oder Lieferketten aufzuzeichnen. Solche Hilfsmittel befinden sich in der frühen Entwicklungsphase, werden jedoch in den kommen Jahren mit Sicherheit unverzichtbar werden.

Unternehmen können das Risiko auch auf die Versicherungsbranche übertragen, ihre Dienstleistungen nutzen und auf ihr Fachwissen zurückgreifen. Versicherungsprodukte für den Bereich Cyber-Sicherheit werden kontinuierlich verbessert und bringen zusätzliche Gewissheit, wenn Unternehmen in neue Technologien und digitale Geschäftsmodelle investieren.

Maßnahmen, die Sie ergreifen können, um das Cyber-Risiko zu reduzieren:

Grundlegende Cybersicherheitshygiene:

- Penetrationstests
- Patchen
- Training

Planung für ein Cyber-Event:

- ein Ausfall
- Datenschutzverletzung

In Kontakt bleiben

Sollten Sie sich nicht bereits zum Erhalt aus der Reihe zum Thema Unvorhersehbarkeit angemeldet haben, so können Sie dies hier vornehmen unter:

qbe.de

April 2019

QBE Insurance (Europe) Limited
Breite Straße 31
40213 Düsseldorf
Karte anzeigen

T: +49 (0) 211 99419 0 | F: +49 (0) 211 99419 88
info@de.qbe.com