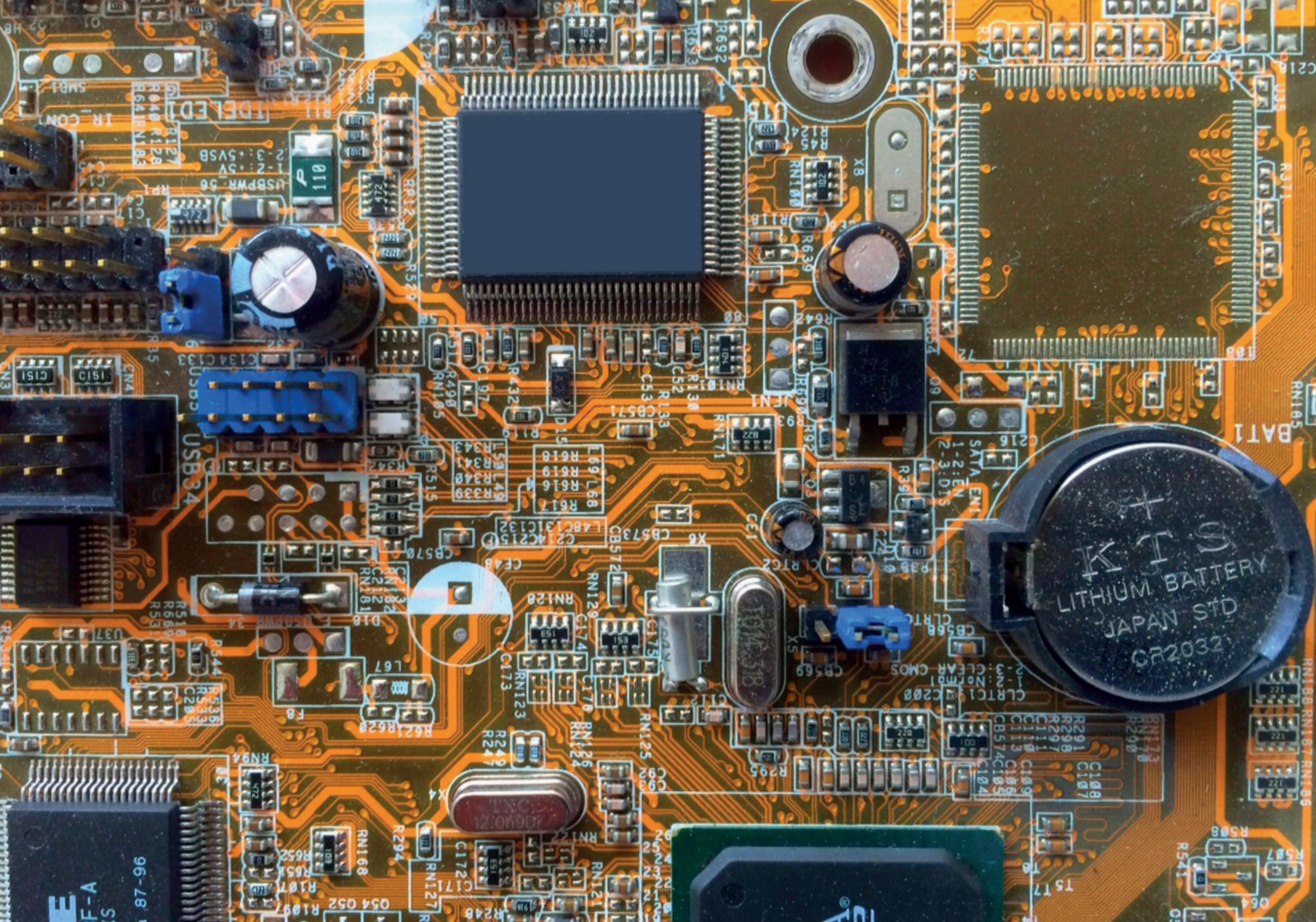
CYBER-SICHERHEIT

MAPRA
ASSEKURANZKONTOR

Cy|ber-|Sich|er|heit [saɪbɐzɪçɐhaɪt], die, (~;~), *Zustand der voraussichtlich gefahren- und störungsfreien Funktion von →Computern, →Peripheriegeräten, →mobilen Geräten, →Software, →technischen Netzwerken →Kommunikationseinrichtungen und durch das →Internet erreichbaren →Informationsinfrastrukturen;*


K T S
LITHIUM BATTERY
JAPAN STD
CR2032

DIGITALER WANDEL

Wir befinden uns in einer Zeit großer Veränderungen des Privat- und Wirtschaftslebens, deren Treiber der technische Fortschritt und die Digitalisierung sind.
Aber wieso ist das so? Der Computer kann nur digitale Informationen verarbeiten. Mittlerweile lassen sich nahezu alle analogen Werte (Töne, Bilder, Temperatur, Gewicht etc.) in digitale Informationen überführen. Die Leistungsfähigkeit von Computern ist enorm gestiegen bei gleichzeitiger Miniaturisierung der Prozessoren und sinkenden Herstellungskosten. Leistungsfähigere Computer können diese Informationen schneller verarbeiten bei gleichzeitiger Steigerung der zu verarbeitenden Datenmenge. Fortschritte bei der drahtlosen Kommunikation sowie der Ausbau des Breitbanddatennetzes sind weitere Grundlagen der Verbreitung der Informationstechnologie (kurz IT).

Diese Entwicklungen erlauben es, neue Produkte und Dienstleistungen zu entwickeln. Das Internet, E-Mail, Smartphones, Cloud-Dienste, digitale Steuerungstechnik, Automatisierung von Arbeitsabläufen, Online-Handel und das digitale Büro sind nur einige Beispiele für diesen Wandel, deren Verwendung aus unserer Arbeitswelt nicht mehr wegzudenken sind. Schlagworte wie etwa Internet der Dinge, Industrie 4.0 und Big Data sind allgegenwärtig. Wir müssen uns darauf einstellen, dass der Umgestaltungsprozess noch lange anhalten, und die Komplexität von IT-Systemen zunehmen wird; das Rad wird sich nicht zurückdrehen.
Diese mitunter tiefgreifenden Veränderungen der Gegenwart eröffnen neue Räume für unternehmerisches Handeln, da der Einsatz von IT viele Vorzüge bietet. Gewichtige Vorteile sind insbesondere die Steigerung der Produktivität und die Eröffnung neuer Geschäftsfelder sowie Absatzmärkte und –wege.

PERSPEKTIVEN/ WECHSEL

Die Vorzüge des Einsatzes von IT machen wir uns schon seit längerem zu Nutze - bspw. hat die E-Mail schon seit Jahren einen festen Platz in der Kommunikation. Mit dem wachsenden Einsatz von IT steigt aber auch die Abhängigkeit – und damit der unternehmerische Erfolg – von deren Funktionsfähigkeit.
Weitgehend sorgenfrei wurde die Verwendung von IT vorangetrieben, ohne dabei auf die IT-Sicherheit ein größeres Augenmerk gelegt zu haben. Das ist auch verständlich, da IT-Sicherheit kein Unternehmensziel ist, und daher oft erst bei einem Vorfall die Aufmerksamkeit erlangte, die sie verdiente. Allerdings waren die Gefahren und die Schadenanfälligkeit in der Vergangenheit geringer, da auch die Abhängigkeiten weniger ausgeprägt waren.

Heute sieht es anders aus. Digitalisierung kann ohne IT-Sicherheit nicht zum Erfolg beitragen.
Neue und teilweise bekannte Risiken gewinnen mit der Digitalisierung an Bedeutung.
Das erfordert einen Perspektivenwechsel auf allen Seiten: bei den Unternehmen und deren Kunden sowie bei den Versicherern, die Deckungen für den veränderten Bedarf zur Verfügung stellen müssen, und den Versicherungsmaklern, die bei der Beratung die geänderte Lage berücksichtigen müssen. Dieser Aufgabe haben wir uns angenommen und stellen Ihnen unsere Expertise zur Verfügung.

Da wir uns aber nicht als Bedenkenträger, sondern als Problemlöser verstehen, und Sie nicht verängstigt zurücklassen wollen, gibt es die gute Nachricht vorweg: Man kann die Gefahren durch Risikomanagement deutlich reduzieren! Für Restrisiken kann eine Cyber-Versicherung eine sinnvolle Ergänzung sein. Auf beide Gesichtspunkte kommen wir im weiteren Verlauf der Broschüre noch zurück.

SICHERHEITS/ RISIKEN

Welchen Risiken muss man unter den geänderten Verhältnissen Aufmerksamkeit schenken?
Man kann die maßgeblichen Faktoren für die Beeinträchtigung der IT-Sicherheit in drei Kategorien einteilen: Technisches und menschliches Versagen sowie Cyber-Kriminalität

Zum technischen Versagen gehören Umstände wie bspw. Softwareausfälle aufgrund von Programmierungsfehlern oder Überlastung der Systeme, die begrenzte Lebensdauer und der Ausfall von Hardwarekomponenten. Ferner spielen auch Gefahren wie Feuer, Wasser, Überspannung oder Stromausfall in diesem Zusammenhang eine Rolle.

Dem menschlichen Versagen kann man die Fehlbedienung aufgrund von Unachtsamkeit oder Unwissenheit zuordnen, sowie fahrlässiges Verhalten beim Verlust von Daten (bspw. aufgrund einer unterlassenen Datensicherung) oder dem Verlust von Datenträgern (bspw. Notebook, Smartphone oder Papierakte im Zug vergessen). Auch die unzureichende Sensibilität für Sicherheitsrisiken im Umgang mit IT ist hier zu nennen.

Durch Cyber-Kriminalität werden jährlich zweistellige Milliardenschäden verursacht. Es geht dabei um kriminelle Handlungen, die mit Hilfe von IT begangen werden, oder sich gegen die IT des Opfers richten. Aufgrund der enormen Verdienstmöglichkeiten bei vergleichsweise geringem Aufwand sowie erheblicher Schwierigkeiten, der Täter habhaft zu werden, ist es eine attraktive Verdienstmöglichkeit für Kriminelle. Die Cyber-Kriminalität ist bereits heute mitunter sehr professionell am Werk, und wird in Zukunft noch weitaus professioneller werden.


01000011 01111001
01110010 00101101
01100010 01100101
01000011 01111001 01100010 01100101 01110010 00101101 01110011
01110100 00001101 00001010
01110011 01101001
01101000
01100101
01110010
01101001 01110100
01000011 01111001 01100010 01100101 01110010 00101101 01110011 01101001 01100011 01101000 01100101 01110010 01101000 01100101 01101001 01110100 00001101 00001010

SCHADEN/ POTENTIAL

Wir möchten Ihnen auf den nachfolgenden Seiten anhand von Beispielen veranschaulichen, mit welchen Risiken sich die Unternehmen heute auseinandersetzen müssen.
Allen Beispielen gemeinsam ist, dass die Tätigkeiten vor der Digitalisierung auch in „analoger" Form durchgeführt worden sind. Nunmehr unterstützt oder ersetzt die IT sogar vormals „analoge" Tätigkeiten.
In der einen oder anderen Form betrifft dies jedes Unternehmen – ganz gleich, ob Kleingewerbe, Mittelstand oder Industrie, und unabhängig davon, ob es sich um einen Dienstleistungs- oder Produktionsbetrieb handelt.
Die Beispiele greifen vier Themen auf, die bei vielen Unternehmen eine wachsende Bedeutung einnehmen. Es geht um die Themen digitale Steuerungssysteme, digitale Buchhaltung bzw. Online-Banking, Schäden durch Fehlbedienung sowie um Cyber-Kriminalität. Die Schadenausmaße lassen sich nicht pauschal beziffern, sondern sind individuell zu betrachten.

Im Anschluss an die Beispiele geben wir Ihnen einen Überblick über die Cyber-Versicherung, die ergänzend zu den aus dem Risikomanagement abgeleiteten Maßnahmen im Schadenfall eine wichtige Stütze sein kann.
Die Schadenbeispiele greifen wir anschließend auf, um zu veranschaulichen, was eine Cyber-Versicherung in diesen Situationen leisten kann.


CYBER
ATTACKS
AHEAD

CYBER/ SCHÄDEN

Das erste Beispiel befasst sich mit digitaler Steuerungstechnik und den Folgen des Ausfalls: Kriminelle schleusten Software in das Netzwerk einer Keksfabrik ein, um diese auszuforschen. Die Software beeinträchtigte aber auch die Steuerungssoftware der Produktionsanlagen. Es kam zum Betriebsstillstand. Vorproduzierter Teig vertrocknete in den Leitungen, so dass diese letztlich herausgeschnitten werden mussten. Vor dem Schaden ging man davon aus, dass der größte Schaden durch eine Cyberattacke ein versalzener Teig sein könnte.
Ein großes Sicherheitsproblem der Gegenwart ist, dass bestehende Anlagen mit Digitaltechnik nachgerüstet werden. Selbst die Steuerungen von Kirchturmuhren lassen sich heute über das Internet erreichen. In Deutschland sollen zeitweise über 30.000 Steuerungssysteme über das Internet erreichbar gewesen sein – ungesichert.

Das nächste Beispiel befasst sich mit der digitalen Buchhaltung bzw. dem Online Banking. Überweisungen werden zunehmend elektronisch über Buchungssysteme in der Firma durchgeführt oder die Überweisungsdaten elektronisch an eine Bank übermittelt. Kriminelle wollten an die Buchungssysteme eines Unternehmens, um Gelder an sich umzuleiten. Das Netzwerk war sehr gut gesichert. Die Angreifer beobachteten daher das Verhalten der Angestellten. Diese aßen in dem Restaurant auf der anderen Straßenseite zu Mittag und schauten regelmäßig auf der Internetseite des Restaurants auf die Speisekarte. Also manipulierten die Kriminellen die Internetseite des Restaurants und schleusten so ein Schadprogramm ein, als die Angestellten aus der Buchhaltung die Seite besuchten. Dann manipulierten sie Überweisungen und täuschten vor, dass alles in bester Ordnung sei, so dass der Diebstahl über einen längeren Zeitraum möglich war. Cyber-Kriminelle betreiben mitunter erheblichen Aufwand und sind dabei sehr kreativ - die einzige Frage für sie ist, ob es sich für sie lohnen wird.

CYBER/ SCHÄDEN

Im vorletzten Beispiel geht es um einen Schaden aufgrund von fahrlässigem Verhalten eines Angestellten. Durch ein Versehen eines Mitarbeiters wurde ein Virus eingeschleust, der die Datenbank eines Hochregallagers durcheinanderbrachte. Die Waren konnten nicht mehr geortet werden. Es kam zur Betriebsunterbrechung. Daneben entstanden Kosten durch die Wiederherstellung der Datenbank, teilweise musste die Ware manuell neu erfasst werden. Hinzu kamen Schadenersatzansprüche der Kunden.
Menschliches Fehlverhalten ist mit Abstand der häufigste Grund für Cyber-Schäden. Hierzu gehört auch das Social-Engineering. Täter erschwindeln sich Informationen von den Opfern, die zu vertrauensselig oder unvorsichtig sind. Hier ist das Bewusstsein der Angestellten zu sensibilisieren, so dass die Mitarbeiter aus eigenem Antrieb aufmerksamer und risikobewusster sind.

Das letzte Beispiel befasst sich mit der Nichtverfügbarkeit der Unternehmensdaten aufgrund von Cyber-Kriminalität. Die Täter verschlüsselten die Patientendatenbank einer Klinik über einen so langen Zeitraum, dass auch alle Datensicherungen von der Verschlüsselung betroffen waren. Die Klinik konnte ohne die Daten nicht weiterarbeiten, da die Patientenakten nur noch digital vorlagen. Um wieder Zugriff auf die Daten zu erhalten, musste die Klinik ein Lösegeld zahlen. Es wurden Krisenmanager, Rechtsanwälte, IT-Forensiker und Detektive beauftragt. Angriffe dieser Art haben stark zugenommen. Für Kriminelle ist die Erpressung eine simple Art, an Geld zu kommen. Bezahlt wird mit der Internetwährung Bitcoins.

Cyber-Schäden kann aber auch vorgebeugt werden, indem im Unternehmen Risikomanagement betrieben wird. Aus der Pflicht der Unternehmensleitung zur ordnungsgemäßen Geschäftsführung ergibt sich die Pflicht zur Schaffung und Aufrechterhaltung einer angemessenen IT-Sicherheit. Das heißt IT-Sicherheit ist Aufgabe der Unternehmensführung und darf nicht allein IT-Spezialisten überlassen werden, da der Geschäftserfolg betroffen ist. Schäden, die im Zusammenhang mit der Vernachlässigung dieser Pflicht entstehen, sind D&O-relevant. Eine D&O-Versicherung wird aber nicht den Schutz bieten, den Sie bei einem Cyber-Vorfall benötigen.

Zunächst ist eine Risikoanalyse des Unternehmens im Hinblick auf die IT-Sicherheit vorzunehmen. Festzustellen ist, welche Bedeutung den Daten und Produktionsmitteln im Einzelnen beigemessen werden muss, um das Schadenpotential bei deren Störung oder Ausfall abschätzen zu können. Dabei ist zu gewichten, welche Bereiche besonders schützenswert sind, und welche weniger, da eine umfassende IT-Sicherheit weder erreichbar noch finanzierbar ist. Gleichzeitig müssen die Sicherheitsrisiken in den Blick genommen werden, etwa technisches Versagen, Virenbefall, Erpressung, Fehlbedienung etc. Im Anschluss daran können Schutzmaßnahmen zur Risikoverringerung abgeleitet werden, d. h. es muss ein IT-Sicherheitskonzept erstellt werden.

Ein IT-Sicherheitskonzept muss für jedes Unternehmen individuell erstellt werden. Lassen Sie uns kurz einige Punkte eines solchen Konzepts anreißen. Bestandteile eines Sicherheitskonzepts sind beispielsweise das Berechtigungsmanagement bzgl. der Nutzungsrechte der IT. Jeder Nutzer soll nur die Rechte erhalten, die er auch wirklich benötigt. So werden Fehlerquellen verringert und Einfallstore für Kriminelle verkleinert.

RISIKO/
MANAGEMENT

Die Sicherheit der digitalen Kommunikation ist ein wichtiger Gesichtspunkt. Denn woher soll man wissen, dass „auf der anderen Seite der Leitung" auch tatsächlich die Person sitzt, die man dort vermutet. Ein wichtiger Schritt zu mehr Sicherheit sind daher gesicherte Kommunikationsverbindungen, etwa durch E-Mail-Verschlüsselung oder VPN-Verbindungen zum Unternehmensnetzwerk. Datensicherungskonzepte sind für viele Unternehmen von zentraler Bedeutung - es reicht nicht allein, die Daten zu sichern. Vielmehr ist regelmäßig zu prüfen, ob die gesicherten Daten im Bedarfsfall auch wieder zurückgespielt und verwendet werden können. Denn das beste Konzept kann nur dann helfen, wenn es auch gelebt wird.

Risikomanagement ist der erste wichtige Schritt zu mehr IT-Sicherheit!

Alle Softwaresysteme, die sich im Einsatz befinden, müssen mit Updates versehen werden. Denn häufig schließen Updates Lücken, durch die Angreifer Zugang zu dem System finden. Im Konzept sollte daher das Update-Management berücksichtigen, d. h. wer sich wann um das Aktualisieren der Systeme kümmert, und wer dies kontrolliert. Zentraler Bestandteil eines effektiven IT-Sicherheitskonzepts sind die Mitarbeiter des Unternehmens. Ihnen muss bewusst sein, wo welche Gefahren bestehen, und wie ihnen begegnet werden kann. Die Mitarbeiter müssen daher geschult und motiviert werden, mehr IT-Sicherheit leben zu können und zu wollen. Nicht zuletzt gehört auch ein Notfallplan zu dem Konzept, um nicht erst im Schadenfall darüber nachzudenken, was von wem zu tun ist. Ein gutes Notfallmanagement beinhaltet sowohl, schnell reagieren zu können, als auch mit Bedacht. Ist beides gewährleistet, können Schäden häufig in ihrem Ausmaß begrenzt werden.

CYBER/ VERSICHERUNG

Im Rahmen des Risikomanagements wird man feststellen, dass sich alle Risiken lediglich theoretisch ausräumen lassen. Dies wäre jedoch weder wirtschaftlich noch praktisch vertretbar. Für Restrisiken kann eine Cyber-Versicherung eine sinnvolle Ergänzung darstellen.
Die Anfänge dieser Versicherung liegen etwa vier Jahre zurück. Mit der Digitalisierung hat sich unser Wirtschaftsleben verändert. Teils bekannte, aber auch neue Risiken gewinnen an Gewicht. Die Versicherungskonzepte der Vergangenheit wurden den neuen Verhältnissen nicht mehr gerecht, und es war höchste Zeit, darauf mit neuen Deckungskonzepten zu reagieren.

Eine Cyber-Versicherung deckt Haftpflichtschäden, also solche Schäden, die Sie Dritten zufügen bzw. zugefügt haben sollen, etwa durch eine Datenrechtsverletzung. Der Versicherer wehrt unbegründete Ansprüche ab oder stellt sie von begründeten Forderungen frei. Die Versicherung beinhaltet ferner eine Eigenschadendeckung. Insbesondere Schäden durch den Ausfall und die Wiederherstellung der Systeme können erhebliche Ausmaße erreichen. Die Cyber-Versicherung zeichnet sich vor allem durch die Gewährung von Dienstleistungen aus, da einer schnellen und professionellen Reaktion entscheidende Bedeutung im Schadenfall zukommen kann. Im Krisenfall kommen dann Spezialisten aus den folgenden Bereichen zum Einsatz: IT-Dienstleistungen, Rechtsberatung, Public-Relations-Beratung und Krisenberatung bei Erpressungen.

Die Expertise dieser Dienstleister lässt sich schwerlich durch eigene Mitarbeiter gewährleisten. Die hausinternen oder die beauftragten IT-Dienstleister sind nicht dafür ausgebildet, auf einen Cyber-Vorfall zu reagieren. Daraus darf man ihnen auch keinen Vorwurf machen.
Versicherer schließen Rahmenvereinbarungen mit diesen Dienstleistern, auf die Sie im Schadenfall zurückgreifen können. Sie wissen vor dem Schaden, an wen Sie sich im Notfall wenden können.
IT-Dienstleister werden bspw. benötigt, um die Schadenursache zu ermitteln und die IT-Systeme wiederherzustellen. Rechtsanwälte sind insbesondere in Datenschutzvorfällen, aber auch bei der Abwehr unbegründeter Ansprüche tätig. Public-Relations-Berater unterstützen bei der Öffentlichkeitsarbeit, damit im Schadenfall einem Reputationsschaden vorgebeugt, oder dieser vermindert werden kann. Krisenberater stellen ihre Erfahrung zur Verfügung, um professionell auf Erpressungsfälle reagieren zu können.

Lassen Sie uns nun die Beispiele aus dem Kapitel „Cyber-Schäden" aufgreifen, um aufzuzeigen, welchen Versicherungsschutz eine Cyber-Police gewährt.

Im Fall der Keksfabrik ist der Betriebsunterbrechungsschaden versichert, ferner die IT-Dienstleistungen zur Wiederherstellung der Soft- und Hardware. Der Sachschaden aufgrund der Leitungen, die herausgeschnitten werden mussten, ist über eine Cyber-Police nicht versichert. Hier müsste mit dem Sachversicherer eine Sonderdeckung vereinbart werden, die gegenwärtig nicht standardmäßig angeboten wird.

Im Beispiel der Überweisungen mit Hilfe von Software, die in die digitale Buchhaltung eingeschleust wurde, sind die IT-Dienstleistung zur Findung der Schadsoftware und zur Wiederherstellung der IT versichert. Ferner lässt sich in begrenztem Umfang auch der Diebstahl der Gelder versichern. Auch bestehen zwischen der Cyber- und der Vertrauensschadenversicherung Überschneidungen, die man bei der Prüfung des Versicherungsschutzes beachten muss.

Eine Cyber-Versicherung ergänzt die Risikovorsorge in Ihrem Unternehmen.

Im Fall des Hochregallagers lassen sich über die Cyber-Versicherung die Betriebsausfallschäden ebenso abdecken, wie der erhöhte Personalaufwand zur Erfassung der Ware sowie die IT-Dienstleistungen zur Wiederherstellung des Systems. Nicht versicherbar – auch nicht über eine Cyber-Versicherung - sind Schadenersatzansprüche von Abnehmern aufgrund verspäteter Lieferung.

Im Erpressungsfall ist die Lösegeldforderung ebenso gedeckt, wie das Tätigwerden eines Krisenberaters, der bei den Verhandlungen mit den Tätern unterstützt. Ferner sind die Leistungen von IT-Dienstleistern gedeckt, die unter anderem auch prüfen, ob die Forderung der Täter überhaupt Substanz hat. Schließlich sind auch die Rechtsanwaltskosten versichert.
Lassen Sie uns über den Bedarf in Ihrem Unternehmen sprechen.

PRESSUM

Bildnachweise:
Digitaler Wandel: Computerteile, © O. F. Lützenkirchen
Perspektivenwechsel: Netzwerk-Switch, © Xiaoliangge - Fotolia.com
Sicherheitsrisiken: Hacker at work with graphic user interface around, © Glebstock - Fotolia.com
Schadenpotential: Grafik: Binäres System, © Mapra
Cyber Schäden: Fotopool Martens & Prahl, © M&P
Risikomanagement: Fotopool Martens & Prahl, © M&P
Cyber Versicherung: Fotopool Martens & Prahl, © M&P

Entwurf, Layout und Texte: MAPRA Lübeck
Auch als Druckversion erhältlich.

MAPRA/
ASSEKURANZKONTOR

www.mapra.de