funk*forum*

SPIONAGE

Wenn Staaten Daten klauen

Seite 14

LIECHTENSTEIN

Ein Gesetz zu Blockchain

Seite 26

SONDERAUSGABE · CYBER · SONDERAUSGABE

UNTERSCHÄTZTE GEFAHR

Cyber-Risiken – größer, als man denkt

Seite 16

140 JAHRE | Die beste Empfehlung. Funk.

Gerüstet für neue Risiken

Dr. Anja Funk-Münchmeyer,
Mitglied der Geschäftsleitung

Wann waren Sie das letzte Mal einen Tag oder länger offline? Digitale Helfer wie Smartphone und PC gehören längst zu unserem Alltag. Auch Unternehmen sind heute permanent online: Der Kontakt zum Kunden läuft per E-Mail, Produktionsmaschinen werden aus der Ferne gesteuert und Rohstoffe auf Online-Portalen geordert. Durch die neuen technischen Möglichkeiten laufen Geschäftsprozesse effizient und Mitarbeiter sind optimal vernetzt. Aber die Digitalisierung hat auch Schattenseiten: In der schönen neuen Welt tummeln sich Cyber-Kriminelle und Wirtschaftsspione.

Wie Sie in dieser Sonderausgabe unseres Kundenmagazins lesen werden, müssen Hacker nur eine kleine Schwachstelle im System finden – und die gibt es in nahezu jedem Unternehmen – oder einen Mitarbeiter täuschen. Schon haben sie Zugriff auf fremde Rechner, können Daten erbeuten und Netzwerke infizieren. Ist die IT erst einmal lahmgelegt, stehen schnell auch die Maschinen still. Die von Cyber-Angriffen verursachten Schäden sind enorm und können sogar zur existenziellen Bedrohung werden. Dabei sind es nicht zwingend Kriminelle, die die Schäden verursachen, sondern oft die eigenen Mitarbeiter.

Damit Sie optimal für die neuen Risiken gerüstet sind, haben wir in dieser Ausgabe alles Wissenswerte zum Thema Cyber zusammengefasst: Woher die Gefahren kommen, wo Risiko- und Versicherungsmanagement ansetzen und wie Sie im Ernstfall mit der Hilfe von Cyber-Experten die IT wieder zum Laufen bringen. Und weil Cyber-Kriminelle vor Ländergrenzen nicht haltmachen, tun wir dies auch nicht. Funk-Experten aus Deutschland, Österreich und der Schweiz sowie ausgewählte Partner und Gastautoren beleuchten das Thema Cyber aus unterschiedlichen Perspektiven.

Viel Spaß bei der Lektüre!

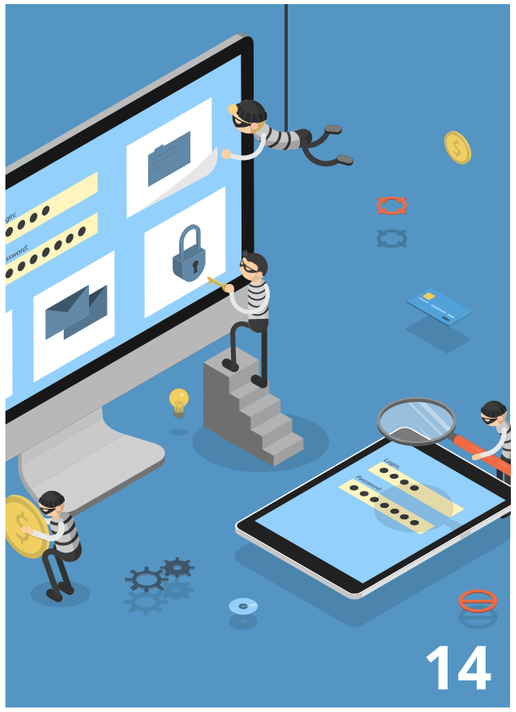
Ihre

Dr. Anja Funk-Münchmeyer

Die beste Empfehlung. Funk.

Inhalt

Zahlen , Daten , Fakten: woher Cyber-Schäden kommen und welche Unternehmen am häufigsten von Attacken betroffen sind .



Spionage-Angriffe auf Unternehmen sind längst keine Seltenheit mehr. Wir haben das Bundesamt für Verfassungsschutz dazu befragt.

In Österreich ist Cyber-Schutz Sache des Bundesheers. Dieses sieht den Schlüssel zum Erfolg vor allem in Sicherheitsforschung.

Die letzte Meile ist oft die kniffligste , auch beim Versicherungsschutz. Mit dem Funk Cyber Risk Calculator erkennen Sie die Restrisiken.

3 Dinge,

die Sie in diesem funk*forum* überraschen werden.

Ein Blockchain-Gesetz aus Liechtenstein
Unsere Wirtschaft wird immer digitaler, auch im Finanzbereich. Das Fürstentum Liechtenstein arbeitet deshalb an einem Blockchain-Gesetz. Regierungschef Adrian Hasler erläutert in einem exklusiven Gastkommentar die Hintergründe.

› Seite 26

Leichtgläubige Mitarbeiter
Cyber-Kriminelle haben den Enkeltrick für sich entdeckt und leicht abgewandelt: Betrüger geben sich dabei als Chef aus und bitten um die Überweisung von Geld. Warum das leider oft funktioniert und wie Sie Ihr Unternehmen schützen können.

› Seite 32

Cyber-Soforthilfe
Eine Cyber-Police von Funk ist wie eine Mitgliedschaft im Automobilclub: Im Schadenfall erreichen Sie unter einer Hotline rund um die Uhr Experten, die Soforthilfe geben. Ein Incident Response Team sorgt dafür, dass Cyber-Schäden klein bleiben.

› Seite 36

Risikoprävention mit Funk Beyond Insurance

Durch technische Innovationen im Kontext der Digitalisierung entstehen für das Risikomanagement neue Möglichkeiten. Vor diesem Hintergrund ist Funk Beyond Insurance entstanden – eine Dienstleistung, bei der intelligente Risikoprävention im Mittelpunkt steht. Technologien wie Künstliche Intelligenz und Sensorik werden dabei zur vorausschauenden Schadenvermeidung eingesetzt. Informationen über Maschinen, Anlagen oder Gebäude werden ermittelt und zum Zweck der Frühindikation von Schwachstellen erhoben. Auf Basis des gewonnenen Datenmaterials können potenzielle Schäden frühzeitig erkannt und abgewendet werden.

Funk Beyond Insurance nutzt Künstliche Intelligenz und Sensorik zur Schadenvermeidung.

Dafür arbeitet Funk mit Start-ups und mit etablierten Unternehmen zusammen. Momentan wird diese neue Dienstleistung im Rahmen verschiedener Pilotprojekte aufgebaut. Den Mehrwert für den Kunden beschreibt Hendrik Löffler, Mitglied der Geschäftsleitung bei Funk, so:

„Funk Beyond Insurance bietet die Möglichkeit der Schadenverhinderung sowie die Optimierung von Wartungs- und Qualitäts- sowie Energieprozessen. Konsequent angewandt kann die neue Technik dazu beitragen, viele Frequenzschadenpotenziale zu reduzieren."

Funk Mitherausgeber von „Insurance & Innovation"

Wer sich über die aktuellen Strömungen in der Versicherungswirtschaft informieren will, der findet seit 2011 zuverlässige Inspiration im Jahrbuch „Insurance & Innovation". Seit 2016 fungiert Funk als Mitherausgeber.

Thematisch spielt die Digitalisierung die zentrale Rolle in der neuen Ausgabe. Unter anderem geht es um Künstliche Intelligenz, um das Potenzial von Apps oder um Spracherkennung. Außerdem werden Risiken aus der Digitalisierung, wie z. B. Cyber-Gefahren, beleuchtet.

Das Fachbuch präsentiert Einblicke in aktuelle Trends der Versicherungswirtschaft.

Darüber hinaus finden sich in dem Buch Artikel zu Change-Prozessen in Unternehmen der Versicherungswirtschaft. Die Verfasser stammen aus der gesamten Branche.

Seitens Funk haben drei Experten Artikel beigesteuert: Dr. Alexander Skorna schreibt über das Thema Blockchain im Risikomanagement, während Thomas Wang und Stephan Kuntner sich in ihrem gemeinsamen Artikel mit Versicherungslösungen bei Unternehmensübernahmen (M&A) für chinesische Unternehmen auseinandersetzen.

Dr. Anja Funk-Münchmeyer, Mitglied der Geschäftsleitung bei Funk, sagt über das Buch: „Als internationaler Versicherungsmakler und Risk Consultant wollen wir unseren Kunden mit innovativen Produkten und Dienstleistungen heute und in Zukunft die beste Empfehlung aussprechen. Unser Engagement für das Buch ist dafür ein fester Baustein, denn es soll die Transparenz über unterschiedlichste Innovationsansätze in der gesamten Branche fördern und die Innovationsentwicklung unterstützen."

Die Mitherausgeber Axel Liebetrau und Dr. Andreas Eckstein kommentieren: „Das Engagement von Funk bringt den Sammelband nicht nur inhaltlich voran, sondern unterstreicht auch den an der Praxis orientierten Wert des Buches."

CYBER-SICHERHEIT IM HEILWESEN

Passwort „Behandlung"

Daten von Patienten sind nicht sicher. Der Grund dafür ist, dass in Arztpraxen teilweise wenig Phantasie aufgebracht wird, wenn es um Passwörter geht.

Fragen Sie Ihren Arzt oder Apotheker – dieser sonst so sinnvolle Ratschlag gilt offenbar nicht, wenn es um die Sicherung vertraulicher Daten geht. Denn im Heilwesen werden vielfach Passwörter genutzt, die nicht sicher sind. Das ergibt eine aktuelle Untersuchung zur IT-Sicherheit im Gesundheitswesen im Auftrag des Gesamtverbandes der Deutschen Versicherungswirtschaft (GDV). Laut dieser Untersuchung verlassen sich nicht weniger als 90 Prozent der Ärzte auf leicht zu erratende Passwörter wie „Behandlung" oder den eigenen Namen. Leichtes Spiel für Hacker! Die Sorglosigkeit erstaunt umso mehr, da Daten gerade im Heilwesen besonders sensibel sind. Ein weiteres Risiko entsteht durch Phishing-Angriffe. Diese waren im Test immerhin bei 6 von 25 der attackierten Arztpraxen erfolgreich. Mitarbeiter klickten auf den Link in einer Mail – und hinter dem Link lauerte ein Schadprogramm.

Laut GDV häufen sich Hackerangriffe auf Ärzte und Apotheken. Schließlich handelt es sich um eine Berufsgruppe, die für Erpresser besonders interessant ist. Die Masche der Kriminellen besteht meist darin, Patientendaten zu kopieren und nur gegen Lösegeld von einer Veröffentlichung abzusehen. Laut GDV wird die Gefahr dadurch vergrößert, dass sich Ärzte zu sicher fühlen, wenn es um ihre eigene Cyber-Sicherheit geht. Die Studie diagnostiziert das Gegenteil. ■

AUSGEWÄHLTE SCHADENFÄLLE

Wenn Daten verschwinden und Maschinen stillstehen

Ob Weltkonzern, Mittelständler oder Privatperson, vor Cyber-Attacken ist keiner gefeit. Und manchmal kann schon ein simpler Tippfehler zum Computer-Chaos führen. Wir zeigen prominente Cyber-Vorfälle aus den vergangenen drei Jahren.

Eine Reederei arbeitet ohne IT

Ging es um Lösegeld oder um reine Sabotage? Im Sommer 2017 fielen zahlreiche Unternehmen einem breit angelegten Hacker-Angriff zum Opfer. Der Erpressungstrojaner NotPetya erwischte auch die dänische Reederei Maersk. Wochenlang kam die Containerschifffahrt von Maersk zum Erliegen. Es entstand ein Schaden von mehreren hundert Millionen Dollar. Wie der Vorsitzende Jim Hagemann Snabe berichtete, mussten 45.000 Client-Rechner und 4.000 Server neu installiert werden. Bis die Technik wieder lief, behalfen sich die Mitarbeiter mit Zettel und Stift.

Tippfehler führt zu Computerchaos

Ein Cyber-Vorfall muss nicht immer eine gezielte Attacke sein: Der Tippfehler eines Technikers in einem Amazon-Rechenzentrum führte Anfang 2017 zu einem Domino-Effekt, weil Dienste untereinander verbunden waren. Hunderte Internetangebote des US-amerikanischen Online-Versandhändlers waren nicht oder nur eingeschränkt erreichbar. Der Neustart dauerte deutlich länger als erwartet.

Krankenhäuser stellen die Behandlung ein

Eine der berühmtesten Cyber-Attacken ging vom Schadprogramm WannaCry aus, das im Mai 2017 zahlreiche Unternehmen angriff. Betroffen waren unter anderem der französische Automobilhersteller Renault, der US-Logistiker FedEx, die Deutsche Bahn sowie Ministerien in Russland. Besonders ernst wurde die Lage in Großbritannien, wo der staatliche Gesundheitsdienst National Health Service attackiert worden war. In Krankenhäusern konnten Laborberichte und Patientendaten nicht mehr eingesehen werden. Viele Kliniken mussten vorübergehend schließen.

Pharma-Konzern geht der Impfstoff aus

Der Pharma-Riese Merck war ebenfalls vom NotPetya-Angriff betroffen. Auch hier führten die verseuchten Computer zu Produktionsausfällen. Da die Maschinen stillstanden, konnte unter anderem die Nachfrage nach dem Gardasil-Impfstoff kurzfristig nicht mehr bedient werden, der z. B. vor Gebärmutterhalskrebs schützen soll. Um lieferfähig zu bleiben, kaufte Merck der US-Gesundheitsbehörde Bestände des eigenen Produkts ab. Die Kosten der Cyber-Attacke sollen im Milliardenbereich liegen.

Druckerei-Chef verhandelt um Lösegeld

Auch der Mittelstand ist für Cyber-Kriminelle interessant. Ende 2018 hatte die Druckerei Braun und Klein aus dem Saarland plötzlich keinen Zugriff mehr auf Kundendaten, Lohnprogramm und Banksoftware. Hacker hatten die Daten mit einer Schadsoftware verschlüsselt und forderten ein Lösegeld für die Entschlüsselung. Die Druckerei sollte 4.500 Euro in Bitcoin bezahlen, handelte die Erpresser dann aber auf 3.500 Euro herunter. Der wahre Schaden: die Betriebsunterbrechung. Wochenlang konnten Maschinen nicht bedient werden. Das kostete die Druckerei nach eigenen Angaben mehr als 70.000 Euro.

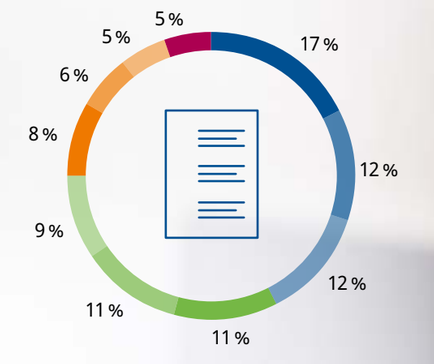
Adventskalender mit gestohlenen Daten

Die breite Öffentlichkeit interessierte sich für Cyber-Vorfälle, als das soziale Netzwerk Facebook im Herbst 2018 meldete, dass die Daten von rund 30 Millionen Kunden gehackt worden waren. Im Januar 2019 war dann der „Kinderzimmertäter“ in den Medien: Ein 20-Jähriger hatte sich Zugang zu persönlichen Daten von Politikern und anderen Prominenten verschafft und die Daten im Dezember 2018 nach und nach veröffentlicht – in einem digitalen Adventskalender.

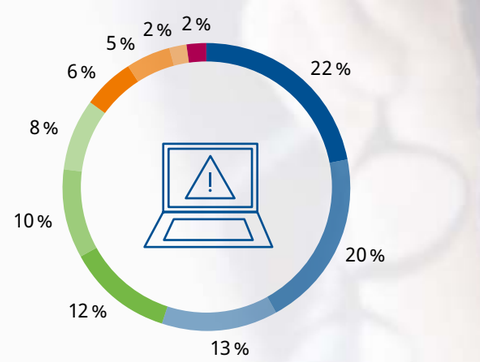
Versicherbar oder nicht?

Nicht alle finanziellen Schäden und Kosten aus den beschriebenen Schadenfällen sind versicherbar. Was die am Markt erhältlichen Versicherungskonzepte leisten und wo die Grenzen der Versicherbarkeit sind, zeigen Ihnen die Cyber-Experten von Funk gern auf; sie beraten Sie zu individuellen Risiken und zum passenden Schutz.

Top 10 der wertvollsten Informationen für Cyber-Kriminelle



Top 10 der größten Cyber-Bedrohungen für Organisationen



Quelle: Global Information Security Survey 2018–19

FUNK CYBER-SCHADENSPIEGEL 2019

Cyber-Gefahren weltweit: ein Überblick

Wir haben für Sie aktuelle Studien und Schadenstatistiken gesichtet: Anhand konkreter Zahlen erfahren Sie, wie groß die Cyber-Gefahren derzeit sind und welche Branchen am stärksten betroffen sind.

Cyber-Risiken sind ein zunehmendes internationales Problem. Schäden werden aus nahezu allen industrialisierten Ländern berichtet, Unternehmen weltweit sind betroffen. Spezifische Attacken mit Schadprogrammen können nicht an internationalen Grenzen aufgehalten werden. Zurückliegende Cyber-Angriffe wie WannaCry, ein Erpressungstrojaner, infizierten im Jahr 2017 IT-Systeme in mehr als 150 Ländern. Nur wenig später betraf der Angriff NotPetya mit einer Schadsoftware rund 65 Länder. Cyber-Attacken sind zu einem weitläufigen Risiko mit potenziell hohen finanziellen Schäden geworden, die aktuell ein weltweites und systemisches Problem darstellen.

Fast jeder dritte Mittelständler war bereits Opfer von Cyber-Angriffen, so das Kernergebnis einer Forsa-Umfrage aus dem Jahr 2018 unter 300 Unternehmern, beauftragt vom Gesamtverband der deutschen Versicherer. In fast jedem zweiten betroffenen Unternehmen (43 Prozent) resultierten aus dem Cyber-Angriff auch zeitweise Betriebsstillstände. Viele Unternehmer hoffen jedoch, dass es sie nicht treffen wird, und agieren zurückhaltend: 72 Prozent der Befragten sehen ein hohes Risiko für Cyber-Kriminalität im Mittelstand, doch nur 37 Prozent schätzen das Cyber-Risiko für das eigene Unternehmen als hoch ein.

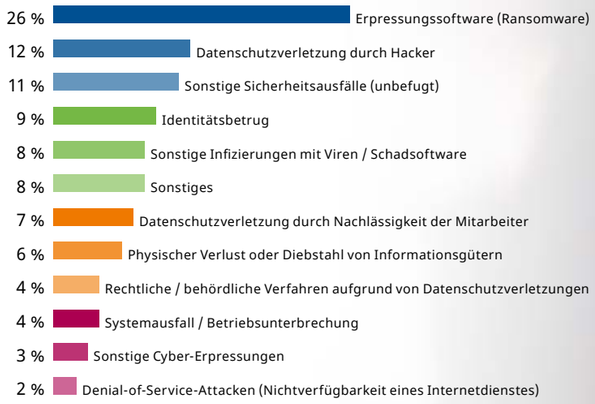
„Ein Umdenken beginnt meist erst, wenn Unternehmen selbst betroffen sind, es also zu einem Cyber-Schaden gekommen ist.“

Dr. Alexander Skorna,
Leiter Business Development

Schaden in Milliardenhöhe

Bei Befragungen der IT-Branche zeigt sich ein differenzierteres Bild. Hier gaben in einer Studie unter 500 Industrieunternehmen des IT-Branchenverbandes Bitkom zum Herbst 2018 sieben von zehn befragten Unternehmen an, von Datendiebstahl, Industriespionage oder Sabotage betroffen gewesen zu sein. Cyber-Angriffe haben bei 47 Prozent der Industrieunternehmen finanzielle Schäden verursacht. Die Bitkom geht von einem Gesamtschaden von 43,4 Milliarden Euro aus den letzten zwei Jahren aus. Jeweils rund 20 Prozent der

Cyber-Schäden nach gemeldeten Vorfällen



Quelle: AIG EMEA für das Schadenjahr 2017

Gezielte Angriffe oder Nachlässigkeit der Mitarbeiter: Cyber-Vorfälle können viele Ursachen haben. Die Folgen sind oft gravierend.

Kosten stammen von Imageschäden und Patentrechtsverletzungen. Betriebsunterbrechungen sind für 15 Prozent der Kosten verantwortlich und rangieren damit an dritter Stelle, gefolgt von Ermittlungs- bzw. Aufklärungskosten.

Eine große Schwachstelle ist der Mensch. Hauptquellen der Cyber-Angriffe sind nach Einschätzung der Bitkom-Studie überwiegend ehemalige oder derzeitige Mitarbeiter sowie das unternehmerische Umfeld, also Kunden, Lieferanten, Dienstleister und Wettbewerber. Das bestätigt eine Studie des Versicherers Hiscox aus dem Jahr 2018, der zufolge sich rund zwei Drittel aller Cyber-Schäden auf eine Form von menschlichem Versagen zurückführen lassen. „Aufmerksame Mitarbeiter sind hier der beste Schutz und geben bei entsprechender Sensibilisierung gute Hinweise, erst dann unterstützt ein professionelles IT-Sicherheitssystem“, sagt Dr. Alexander Skorna.

Werfen wir einen Blick in die Schadenstatistiken. In den vergangenen zwei Jahren haben viele Unternehmen ihre individuelle Risikosituation beleuchten lassen und als Folge Cyber-Deckungen abgeschlossen. Gleichzeitig stieg das Risiko vor allem durch die Verbreitung von Ransomware (Verschlüsselungstrojaner) und Malware (Schadsoftware) erheblich. Eine Übersicht über die Ursachen versicherter Cyber-Schäden finden Sie in der Grafik oben auf dem Bild.

Schadenfälle nehmen zu

Entsprechend steigen aktuell die versicherten Schäden, bei manchen Versicherern um bis zu 50 Prozent pro Jahr. Alleine im Jahr 2017 erfasst die American International Group in ihrem aktuellen Schadenreport vom Mai 2018 so viele Schadenfälle wie in den Jahren von 2013 bis 2016 zusammen. Entsprechend groß ist die Sorge der Versicherer vor Kumulschäden die durch großflächige Angriffe von Hackern oder durch Würmer bei vielen Unternehmen gleichzeitig entstehen können. „Wir sehen im Markt derzeit eine Kürzung von Kapazitäten sowie in Teilen auch eine allgemeine Zurückhaltung der Versicherer bei hochexponiertem Neugeschäft“, fasst Dr. Alexander Skorna die Marktsituation zusammen.

„In Deutschland steigen die Schadenkosten für Cyber von Jahr zu Jahr besonders stark an.“

Dr. Alexander Skorna,
Leiter Business Development

Die Schadenhöhen unterscheiden sich je nach Größe des Unternehmens stark. Laut einer Studie des Ponemon Institute von 2018 liegt die durchschnittliche Schadenhöhe einer Datenverletzung weltweit bei 3,86 Millionen US-Dollar – ein Anstieg von 6,4 Prozent im Vergleich zum Vorjahr (bei einer Verletzung von einer Million oder mehr Datensätzen schnellen die Kosten laut Studie jedoch hoch und betragen durchschnittlich rund 40 Millionen US-Dollar). Diese Zahlen beziehen sich lediglich auf Kosten, die durch Datenschutzverletzungen entstehen. Die Kosten eines durchschnittlichen Cyber-Vorfalls liegen laut einer KPMG-Studie bei 6,1 Millionen Euro. „Bei kleinen und mittelständischen Unternehmen sind die Schadensummen durch Cyber-Vorfälle meist deutlich niedriger, aber auch hier ist ein klarer Aufwärtstrend zu beobachten“, sagt Dr. Skorna. „In Deutschland steigen die Schadenkosten für Cyber von Jahr zu Jahr besonders stark an.“ Kostentreiber sind sowohl bei Großkonzernen als auch bei Mittelständlern Betriebsunterbrechungsschäden, Benachrichtigungskosten betroffener Kunden bei Datenpannen sowie Kosten zur Schadenfeststellung.

Bei den betroffenen Branchen zeigt sich in den Studien ein relativ einheitliches Bild. Die meisten Schäden (Anzahl) entfallen auf Finanzdienstleister, Rechts-/Unternehmensberater, Unternehmen aus dem Gesundheitswesen sowie auf Einzelhändler. Die in Deutschland starke industrielle Maschinenbauproduktion befindet sich in den Schadenstatistiken im Mittelfeld – etwa jeder zehnte Schadenfall betrifft den Maschinenbau. Die höchsten finanziellen Schäden verursachen Cyber-Angriffe in der Finanzwirtschaft, der Energiewirtschaft sowie in der Luftfahrt-/Verteidigungsindustrie. Die industrielle Produktion und der Handel (vor einigen Jahren noch am stärksten betroffen) sind gemessen an der Schadenhöhe aktuell eher im Mittelfeld anzusiedeln.

Kunden machen Druck

Schlussendlich bleibt ein Blick auf die Treiber für einen Abschluss von Cyber-Versicherungen. Gemäß einer Studie der PartnerRe zusammen mit Advisen im Jahr 2018 schließen Unternehmen Versicherungen gegen Cyber-Risiken überwiegend auf externen Druck Dritter – meist Kunden – ab. Weitere Treiber sind die Verschärfung der Datenschutzgrundverordnung und das größere Haftpflichtrisiko. Auch die mediale Präsenz sowie die eigene Betroffenheit von Unternehmen führen zu vermehrten Abschlüssen.

Die Prämien sind derzeit volatil und unterscheiden sich je nach Versicherer stark. „Ein Versicherungsmakler wie Funk hat hier den Mehrwert, eine Marktkonsistenz durch eine einheitliche Police sicherzustellen und das beste Preis-Leistungs-Verhältnis im Sinne des Kunden zu bieten“, sagt Dr. Skorna. Grundvoraussetzung für einen effizienten Cyber-Schutz ist jedoch, dass Unternehmen ihre Risikogefährdung einschätzen können. Hierzu kann eine Risk-Analyse beitragen. Zudem sollten sich Unternehmen mit Notfallplänen oder einem Business Continuity Management auf Betriebsunterbrechungen in Folge eines Cyber-Angriffs vorbereiten. Erst die ganzheitliche Absicherung von Cyber-Angriffen wird Unternehmen helfen, den Vorfall möglichst unbeschadet zu überstehen. ■

Ihr Ansprechpartner
Dr. Alexander Skorna
a.skorna@funk-gruppe.de

Cyber-Attacken stellen auch für die Nachrichtendienste vieler Staaten ein hocheffizientes Mittel dar, um sich Informationen zu beschaffen.

SPIONAGE-ANGRIFFE AUF UNTERNEHMEN

Wenn Staaten Daten klauen

Die Entwicklung der Informationstechnologie bietet fremden Nachrichtendiensten zahlreiche Möglichkeiten zur Spionage. Dr. Felor Badenberg vom Bundesamt für Verfassungsschutz (BfV) erklärt, worauf deutsche Unternehmen achten müssen.

Frau Dr. Badenberg, es vergeht kaum eine Woche ohne eine Meldung über einen Cyber-Angriff auf eine staatliche oder private Einrichtung in Deutschland. Wie hoch ist das Risiko für Unternehmen hierzulande, Opfer einer Cyber-Attacke eines fremden Nachrichtendienstes zu werden? Und welche Branchen sind besonders gefährdet?

❮ Eine pauschale Aussage ist hier nur schwer zu treffen. Allerdings ist die Bundesrepublik Deutschland aufgrund ihrer geopolitischen Lage, ihrer Rolle in der Europäischen Union und der NATO sowie als Standort zahlreicher Unternehmen der Spitzentechnologie für fremde Nachrichtendienste besonders attraktiv. Das Risiko, Opfer eines Cyber-Angriffs zu werden, hängt insbesondere davon ab, welcher Branche das jeweilige Unternehmen angehört. Gefährdet sind hier, wie bereits erwähnt, der Bereich der Hoch- und Spitzentechnologie, außerdem Rüstungsunternehmen, Elektronik- und Elektrotechnikkonzerne sowie Unternehmen der Luft- und Raumfahrt. Darüber hinaus geraten auch solche Firmen verstärkt in den Fokus staatlicher Cyber-Kampagnen, die zu kritischen Infrastrukturen (KRITIS) gerechnet werden. Dazu zählen beispielsweise die Energie- und Wasserversorgung, aber auch Krankenhäuser oder Banken. Wichtig ist, dass nicht nur Großkonzerne Opfer eines Spionage- oder Sabotageangriffs werden können. Auch mittelständische Unternehmen sind davon betroffen.

Bei welchen Fällen wird die Cyber-Abwehr des Verfassungsschutzes aktiv und wie ist das Prozedere?

❮ Das BfV als eine Cyber-Sicherheitsbehörde ist verantwortlich für die Aufklärung und Abwehr von politisch sowie islamistisch motivierten und staatlich gesteuerten Cyber-Angriffen. Seinem gesetzlichen Auftrag nach fungiert der Verfassungsschutz dabei als eine Art Frühwarnsystem. Nachrichtendienstliche Erkenntnisse werden hier zu Lageeinschätzungen verdichtet, die der Bundesregierung bei politischen Entscheidungsprozessen helfen. Allerdings können sich auch Unternehmen der Privatwirtschaft an die Cyber-Abwehr des BfV wenden, wenn sie den Verdacht hegen, betroffen zu sein. Je nach Gefährdungslage werden dann mobile Cyber-Teams zu den entsprechenden Einrichtungen geschickt und Sensibilisierungsgespräche geführt. Zusätzlich bekommen betroffene, aber auch potentiell gefährdete Unternehmen eine Warnmeldung (sog. Cyber-Brief), die Informationen über die aktuelle Angriffswelle, den Angriffsvektor inklusive technischer Indikatoren (sog. Indicators of Compromise), über die Angreifer sowie ihr Aufklärungsinteresse enthält. Mithilfe der technischen Indikatoren können die Unternehmen feststellen, ob sie von den Aktivitäten der Cybergruppierung betroffen sind, und entsprechende Schutzvorkehrungen treffen, um einer Infizierung ihrer Systeme vorzubeugen. Der Cyber-Brief wird auch auf der Internetseite des BfV veröffentlicht.

Welchen Arten von Spionage- und Sabotageangriffen begegnen Sie bei der Cyber-Abwehr am häufigsten?

❮ Die Art des Cyber-Angriffs – der sogenannte Angriffsvektor – hängt vom Modus Operandi der jeweiligen Angreifergruppierung ab. Häufig können zwei Vektoren festgestellt werden: zum einen Angriffe mit „Spear-Phishing-Mails“, also personalisierte E-Mails mit infizierten Links oder Schadanhängen, die sich an Mitarbeiter von Unternehmen richten. Die Nachrichten werden von einer vermeintlich vertrauenswürdigen Quelle verschickt, die Inhalte sind in der Regel gut recherchiert und enthalten teilweise Insiderwissen. Dies zeigt, dass der Angreifer professionelles Social Engineering betreibt, sich also zuvor intensiv mit dem Umfeld der Zielperson auseinandersetzt. Eine weitere Angriffsmethode ist die „Watering-Hole-Attacke“. Hier handelt es sich um einen Cyber-Angriff, bei dem der Angreifer eine anhand der Vorlieben des Opfers ausgewählte Webseite manipuliert und mit Schadcode infiziert. Die Infizierung ist meist durch unbekannte Sicherheitslücken, sogenannte Zero-Day-Schwachstellen, möglich.

Gibt es Staaten, die in erhöhtem Maße mit diesen Methoden arbeiten?

❮ Die Nachrichtendienste vieler Staaten haben Cyber-Angriffe als Mittel für sich entdeckt. Besonders die Nachrichten- und Sicherheitsdienste der Russischen Föderation und der Volksrepublik China entfalten in großem Umfang Spionageaktivitäten. Ihre Schwerpunkte orientieren sich an den politischen Vorgaben ihrer Regierungen. Hierzu gehört auch der gesetzliche beziehungsweise staatliche Auftrag, die eigene Volkswirtschaft mit Informationen zu unterstützen, die auf nachrichtendienstlichem Wege beschafft wurden.

Weiterführende Informationen zur Arbeit des Bundesamtes für Verfassungsschutz und der Abteilung Cyber-Abwehr finden Sie unter:

verfassungsschutz.de

Dr. Felor Badenberg

Dr. Felor Badenberg leitet im Bundesamt für Verfassungsschutz (BfV) die Abteilung für operative Aufklärung und Abwehr von staatlich gesteuerten Cyber-Angriffen gegen die Bundesrepublik Deutschland.

Was macht Cyber-Angriffe für die Täter so attraktiv?

❮ Die Vorteile liegen auf der Hand: Cyber-Angriffe stellen ein vergleichsweise kostengünstiges, aber hocheffizientes Mittel dar, sich Informationen über Staaten, Unternehmen oder Institutionen zu beschaffen. So können mit Cyber-Angriffen Daten erbeutet werden, die sonst nur mit gut platzierten menschlichen Quellen unter ungleich höherem Aufwand zu erlangen sind. Darüber hinaus sind die Attacken international einsetzbar und eine Attribution – das heißt eine Zuordnung zum Täter – ist in der Regel schwierig.

Wird Wirtschaftsspionage in Zukunft nur noch digital stattfinden? Oder müssen sich Unternehmen auch weiterhin auf analoge Angriffe einstellen?

❮ Aus Sicht der Angreifer gibt es keine Trennung zwischen digitaler oder analoger Spionage. Es geht immer um bestimmte Aufklärungsziele, die auf dem Weg verfolgt werden, der sich am einfachsten anbietet. Insofern spielen ganz klassische nachrichtendienstliche Methoden – zum Beispiel das Anbahnen von persönlichen Kontakten oder das Abhören von Räumen oder Telefonen – nach wie vor eine nicht zu unterschätzende Rolle. Eine wesentliche Erkenntnis sollte man allerdings nicht aus dem Blick verlieren: Das mit Abstand häufigste Einfallstor für Spionage – selbst bei hochkomplexen Cyber-Angriffen – ist der Mensch. Sich ausschließlich auf die technische Komponente zu konzentrieren, ist also in hohem Maße fahrlässig. ■

CYBER IM JAHR 2019

Das unterschätzte Risiko

Wie lange kann Ihr Unternehmen ohne IT arbeiten? In der digitalisierten Welt von heute können Cyber-Schäden schnell zur existenziellen Bedrohung werden. Woher die Angriffe kommen und wie Unternehmen sich wappnen können.

Der amerikanische Geheimdienst späht das Handy von Bundeskanzlerin Angela Merkel aus: Über diesen Skandal berichteten im Jahr 2013 zahlreiche Medien und machten das Thema Cyber-Risiko einer breiten Öffentlichkeit bekannt. Seitdem gab es zahlreiche weitere prominente Vorfälle, zum Beispiel Attacken mithilfe von Krypto- oder Erpressungstrojanern wie Ryuk, WannaCry, Petya, Cerber, CryptoLocker und Locky. Dabei greifen Hacker auf fremde Daten zu und verschlüsseln diese. Oft bieten die Kriminellen dann an, die Daten gegen Zahlung eines Lösegelds wieder freizugeben. Opfer dieser Angriffe sind nicht nur Privatpersonen, sondern auch Unternehmensnetzwerke und Einrichtungen der öffentlichen Infrastruktur, etwa Energieversorger, Wasserwerke und Krankenhäuser. Cyber-Angriffe stellen somit ein erhebliches Gefahrenpotenzial dar.

Selbst Angriffe aus dem Kinderzimmer sind möglich

Wer die Initiatoren solcher Angriffe sind, bleibt oft unklar. Bei einigen Attacken wird vermutet, dass internationale Verbrecherorganisationen am Werk waren, die mit einer eigenen „Digitalabteilung“ gezielt Unternehmen mit Schadsoftware infizieren. In anderen Fällen geraten ganze Staaten in Verdacht, die Unternehmen in anderen Ländern ausspionieren und sich sensible Informationen beschaffen.

Wie ein aktueller Fall zur Jahreswende 2018/2019 in Deutschland gezeigt hat, braucht es aber gar keine organisierten Verbrecherbanden oder staatliche Geheimdienste, um ein Datenskandal zu verursachen. Einem Schüler ist es gelungen, aus seinem Kinderzimmer heraus an sensible Daten von Politikern und Prominenten zu gelangen. Augenscheinlich ist die Sensibilität für Cyber-Risiken auch einige Jahre nach dem Handyskandal von Angela Merkel noch lange nicht ausreichend hoch. Vor diesem Hintergrund mag man sich gar nicht ausmalen, wer möglicherweise ganz still und heimlich in Firmennetzwerken unerkannt mitliest. Es gibt sicherlich genügend Interessenten für Informationen über Patente, technische Zeichnungen, Kunden- und Lieferantenbeziehungen, Preisstrategien, Marktanteile, Deckungsbeiträge und vieles weitere mehr.

Wenn der Betrieb stillsteht

Die IT-Infrastruktur stellt heute das zentrale Nervensystem eines jeden Unternehmens dar. Einzelne Maschinen sind ebenso durch IT verbunden wie auch die gesamten Produktions- und Logistikabläufe miteinander vernetzt sind. Gleiches gilt für viele weitere Subsysteme im Unternehmen. „Nichts funktioniert ohne IT. Der Ausfall dieser vielfach untrennbar miteinander verwobenen Netzwerkstrukturen führt zwangsläufig zum Stillstand einzelner Abteilungen bis hin zum Stillstand des ganzen Betriebs“, sagt Hendrik F. Löffler, Mitglied der Geschäftsleitung von Funk. „Ausfallszenarien von wenigen Minuten über Stunden bis hin zu Tagen und Wochen sind möglich.“

> *„Nichts funktioniert ohne IT. Der Ausfall führt zum Stillstand einzelner Abteilungen bis hin zum Stillstand des ganzen Betriebs.“*
>
> **Hendrik F. Löffler,**
> Mitglied der Geschäftsleitung von Funk

Selbst wenn Unternehmen die Zeichen der Zeit erkannt haben und hochwertige Schutzmechanismen installiert haben, ist kein Unternehmen vollständig vor Schäden aus dem Cyber-Kontext geschützt. Denn Unternehmen müssen sich nicht nur gegen Attacken von außen wappnen. Löffler: „Unaufmerksamkeit und Fahrlässigkeit der eigenen Mitarbeiter oder schlichte Fehlbedienung kann genauso dazu führen, dass die IT ausfällt – und in der Folge der ganze Betrieb stillsteht.“

Für die Bilanz und die Gewinn-und-Verlust-Rechnung eines Unternehmens ist es völlig irrelevant, ob der Schaden intern oder extern entstanden ist. Da konventionelle Betriebsunterbrechungsversicherungen nur in den seltensten Fällen für solche Schäden eintreten, bleiben die Unternehmen oft auf den Kosten sitzen.

Die IT allein kann diese Herausforderung nicht lösen

Welche Vorkehrungen können Unternehmen treffen? Die IT-Abteilung schützt die eigenen Systeme natürlich nach bestem Wissen und mit den gegebenen Möglichkeiten. Dies geschieht jedoch in aller Regel nur aus dem Fokus der IT und nicht unter Berücksichtigung der unternehmensweiten Wertschöpfungszusammenhänge. Da sich große Cyber-Risikoschadenpotenziale in vielen Fällen aber erst aus den Wechselwirkungen der einzelnen Unternehmensbereiche untereinander ergeben, kann die Unternehmens-IT alleine keine ganzheitliche Schadenkalkulation vornehmen.

Ein Beispiel: Um beurteilen zu können, in welcher Größenordnung sich ein Deckungsbeitragsausfall für eine bestimmte Produktlinie bewegt, wenn das ERP-System für fünf Tage ausfällt, bedarf es zwangsläufig auch der Kompetenzen aus dem Controlling und aus der Produktion. Die Ursachen liegen auch häufig gar nicht im Einflussbereich der IT-Abteilung: Ein Produktionsmitarbeiter kann einen großen Schaden anrichten, wenn er zum Beispiel ein Maschinensoftware-Update falsch aufspielt. Oder der externe Maschinenlieferant infiziert das Produktionsnetzwerk per Fernwartung unbeabsichtigt mit einem Virus.

Sind Sie vorbereitet, wenn es Ihr Unternehmen trifft?

Das Cyber-Risiko bleibt aktuell und wird in absehbarer Zeit auch nicht mehr von der Tagesordnung verschwinden. Umso erschreckender ist das Ergebnis des Cyber Security Reports 2018: In jedem dritten Unternehmen setzt sich die Geschäftsführung nicht intensiv – sofern überhaupt – und höchstens anlassbezogen mit dem Thema Cyber-Sicherheit auseinander.

Kennen Sie die Cyber-Risiken Ihres Unternehmens? Wissen Sie, welche Auswirkungen die vielfältigen Gefahren auf Ihren Geschäftserfolg haben können? Mit einer spezifischen Risikoanalyse erhalten Sie mehr Transparenz und ein besseres

Die IT-Infrastruktur stellt heute das zentrale Nervensystem eines jeden Unternehmens dar.

Funk Cyber-Risk-Analyse

Ziel: Risikotransparenz und Überblick über die IT-Gefahrensituation durch Aufzeigen von Schwachstellen aus Open-Source-Informationen

2-tägige betriebswirtschaftliche Analyse
durchgeführt von Funk

- Interdisziplinärer Workshop zur Risikoidentifikation
- Einschätzung/Überprüfung bereits vorhandener Informationen
- Erstellung einer individuellen Risikocheckliste
- Bewertung der Risiken
- Definition von Risikosteuerungsmaßnahmen
- Zusammenfassung der identifizierten Risiken
- Aufzeigen der bereits bestehenden Risikosteuerungsmaßnahmen sowie Empfehlungen für weitere Maßnahmen

IT-Security-Quick-Check
durchgeführt von RadarServices

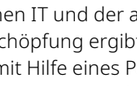
- Externes Footprinting
  - Analyse von extern erreichbaren Ressourcen Ihres Unternehmens
  - Aufdeckung von IT-Schwachstellen
- RadarServices RiskCheck Fragenkatalog
  - Behandlung sicherheitsrelevanter Themen Ihrer Unternehmens-IT

Ergebnis: Zwei individuelle Abschlussberichte liefern optimale Transparenz über das individuelle Cyber-Risiko auf betriebswirtschaftlicher und technischer Ebene.

Risikoverständnis. Daher ist sie ein wichtiger Schritt für das effektive Management von Cyber-Gefahren.

Ein Workshop beleuchtet die Prozesse im Unternehmen

Funk bietet Ihnen eine individuelle Analyse im Rahmen eines interdisziplinären Workshops. In der Vorbereitung werden die Projektziele und das dazugehörige Projektteam verbindlich festgelegt. Um alle Unternehmensbereiche abzubilden, nehmen üblicherweise neben dem IT-Leiter auch die Leiter von Einkauf, Controlling/Finanzen, Vertrieb, der Produktionsleiter sowie das Versicherungswesen und Risikomanagement an der Risikoanalyse teil. Die Teilnehmer diskutieren gemeinsam mit den Experten von Funk mögliche Risikoszenarien entlang der Wertschöpfungskette und priorisieren die Risiken. Mittels einer Geschäftsauswirkungsanalyse können die vorhandenen Prozesse im Unternehmen im Zusammenwirken mit den Risiken in ihrer Kritikalität beurteilt werden. Dabei werden sämtliche Risikofelder, vorhandene Maßnahmen, Wechselwirkungen und Ausfallzeiten berücksichtigt, sodass sich ein transparentes Bild über die aktuelle Risikosituation und über die Wechselwirkungen zwischen IT und der analogen Wertschöpfung ergibt. Optional kann mit Hilfe eines Penetrationstests unseres exklusiven Kooperationspartners RadarServices ein konkreter Einblick in die tatsächlich vorhandenen IT-Security-Schwachstellen gewonnen werden. Cyber-Experte Löffler: „Unternehmen gewinnen mit der Funk Cyber-Risk-Analyse nicht nur eine erhöhte Risikotransparenz, sondern auch eine fundierte Grundlage für Versicherungslösungen.“ Mit den gewonnenen Daten können zudem Notfall- oder Business-Continuity-Pläne erstellt werden. So sind Cyber-Schäden zwar immer noch lästig, aber keine existenzielle Bedrohung mehr. ■



Ihr Ansprechpartner
Hendrik F. Löffler
h.loeffler@funk-gruppe.de

STRAFGELDER

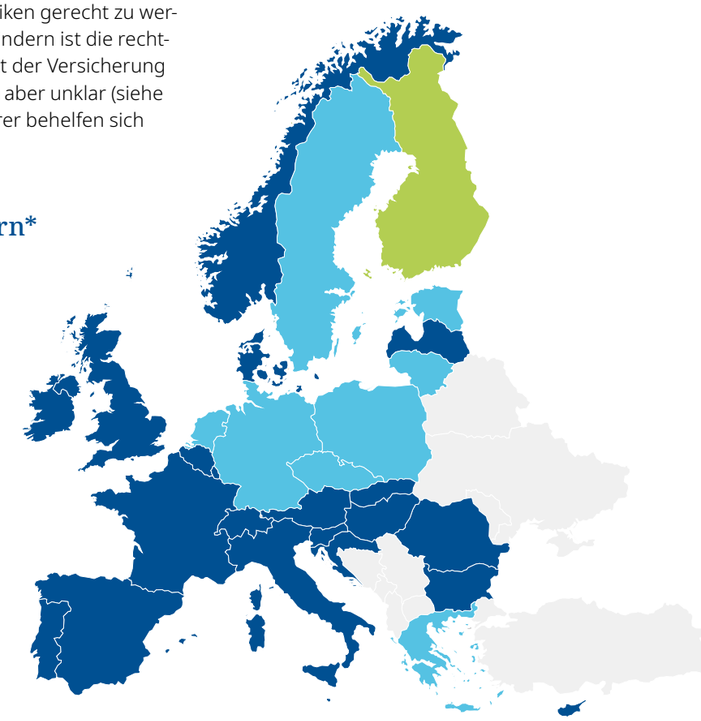
Sanktionen aus Europa

Die EU hat die Pflichten rund um Verarbeitung, Speicherung und Weitergabe personenbezogener Daten deutlich erweitert. Bei einem Verstoß drohen Bußgelder. Unternehmen können dieses Risiko versichern – aber nicht in allen Ländern.

Datenschutzpannen können richtig teuer werden. In der neuen EU-Datenschutzgrundverordnung wurde die bisherige Bußgeld-Obergrenze von 300.000 Euro auf 20 Millionen Euro angehoben (oder 4 Prozent des gesamten weltweiten Jahresumsatzes). Wenn Unternehmen den deutlich gestiegenen Anforderungen zu beispielsweise Datensicherung, Melde-, Lösch- und Dokumentationspflichten nicht nachkommen, können sie zur Kasse gebeten werden. In Deutschland wurden bereits erste Strafen verhängt. Auch Frankreich hat schon ein Exempel statuiert und einen Technologiekonzern wegen mehrerer Verstöße bei der Datenverarbeitung belangt. Das Bußgeld: 50 Millionen Euro. Der Versicherungsmarkt bietet verschiedene Lösungen, um den gestiegenen Risiken gerecht zu werden. In vielen Ländern ist die rechtliche Zulässigkeit der Versicherung von Bußgeldern aber unklar (siehe Karte). Versicherer behelfen sich damit, die Sanktionen durch D&O- oder Cyber-Policen abzusichern, soweit dies rechtlich zulässig ist. Solange kein ausdrückliches Verbot besteht, nehmen Versicherer eine Regulierung vor. Wir behalten für Sie die Entwicklungen im Blick und beraten Sie gern dazu. ■

Versicherbarkeit von direkten Bußgeldern*

1	Belgien	3	Malta
3	Bulgarien	1	Niederlande
2	Dänemark	1	Norwegen
1	Deutschland	1	Österreich
2	Estland	1	Polen
2	Finnland	1	Portugal
1	Frankreich	2	Rumänien
2	Griechenland	1	Schweden
1	Großbritannien	1	Schweiz
1	Irland	2	Slowakei
1	Italien	2	Slowenien
3	Kroatien	1	Spanien
2	Lettland	2	Tschechien
3	Litauen	2	Ungarn
2	Luxemburg	2	Zypern



Stand: März 2019
* Die Übersicht bezieht sich auf die Versicherbarkeit eines direkten Bußgeldes, nicht auf einen möglichen Bußgeldregress.

Datenschutzniveau:
1 = hoch | 2 = mittelmäßig | 3 = niedrig

Länder:
nicht versicherbar | Rechtslage unklar | versicherbar

INDIVIDUELLE VERSICHERUNGSKONZEPTE

Deckungs-Duo für Ihr Risiko

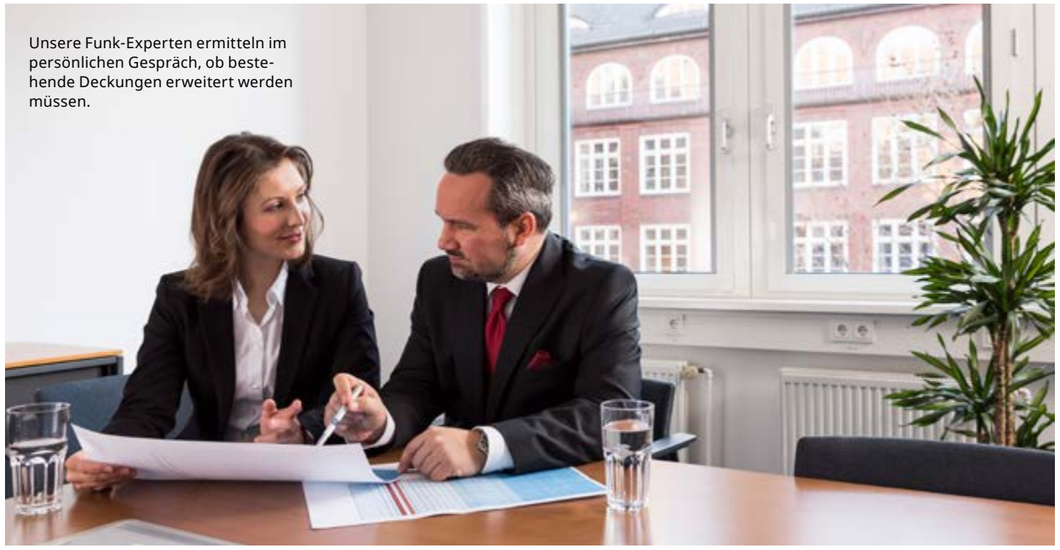
IT-Sicherheit hat in der heutigen Zeit für jedes Unternehmen eine hohe Priorität. Dabei hat jede Branche eigene Risiken, weshalb es keine Musterlösung gibt. Je nach individueller Risikolage sollten Unternehmen zwei Deckungen sinnvoll kombinieren: Cyber- und Vertrauensschaden-Versicherung.

Die rasante Entwicklung der Informations- und Kommunikationstechnologie führt zu einer weltweiten Vernetzung. Gleichzeitig steigen die rechtlichen Anforderungen an Unternehmen, zum Beispiel durch die Datenschutzgrundverordnung. Die Unternehmensleitung ist zunehmend gefordert: Sie muss unternehmensweite Sicherheitslücken identifizieren, gemeinsam mit der IT-Abteilung technische und organisatorische Maßnahmen ergreifen und Notfallpläne aufstellen. Doch die Anforderungen variieren stark, jede Branche sieht sich mit individuellen Risiken konfrontiert.

Die Begrifflichkeit „Cyber" führt leicht in die Irre, da sie suggeriert, es ginge nur um „Cyber Crime". Die aktuelle Bedrohungslage geht jedoch weit darüber hinaus. Die steigende Komplexität der IT-Systeme führt generell zu einer erhöhten Anfälligkeit. Dies gilt nicht nur für Sabotagehandlungen durch Dritte, sondern auch für technische Probleme oder Fehlbedienungen durch Mitarbeiter. Hinzu kommen Unternehmensstrukturen über Ländergrenzen hinweg, welche die Implementierung interner Kontroll- und Informationssicherheits-Managementsysteme erschweren. Die Folge: eine erhöhte Verwundbarkeit. „Die Allgegenwärtigkeit von Informationen über Menschen und Unternehmen macht es Tätern leicht, sich zielgerichtet vorzubereiten. Sie identifizieren den Menschen als schwächstes Glied der (IT-)Sicherheitskette und nutzen das entsprechend aus", sagt Alexandra Köttgen, Expertin für Vertrauensschaden-Versicherungen bei Funk. Dabei gehen die Täter online und offline vor.

„Die Täter identifizieren den Menschen als schwächstes Glied der (IT-)Sicherheitskette und nutzen das entsprechend aus."

Alexandra Köttgen,
Expertin für Vertrauensschaden-Versicherungen



Unsere Funk-Experten ermitteln im persönlichen Gespräch, ob bestehende Deckungen erweitert werden müssen.

Bei der Gestaltung der Versicherungskonzepte ist es wichtig, sowohl branchenspezifische Aspekte als auch individuelle Unternehmenssituationen zu berücksichtigen. „Wir prüfen auf Basis des bestehenden Versicherungskonzeptes, inwieweit eine Erweiterung des Deckungsschutzes um risikospezifische Konzepte sinnvoll und umsetzbar ist. Hierbei stehen die Cyber- und die Vertrauensschaden-Versicherung im Fokus", sagt Michael Winte, Fachbereichsleiter Cyber, Technology & Crime bei Funk. Aufgrund der Bandbreite der bestehenden Risiken und damit einhergehender Schadenkonstellationen ergänzen sich beide Deckungskonzepte.

„Wir prüfen auf Basis des bestehenden Versicherungskonzeptes, inwieweit eine Erweiterung des Deckungsschutzes sinnvoll ist."

Michael Winte,
Fachbereichsleiter Cyber, Technology & Crime

„Überschneidungen existieren aufgrund der abweichenden Deckungsauslöser kaum", so Winte.

Es kommt auf den Schaden an

Um diesen Ausprägungen gerecht zu werden, hat Funk eigenständige Konzepte entwickelt, die optimal ineinandergreifen und modular aufgebaut sind. Risiken aus dem Bereich der Wirtschaftskriminalität, wie etwa der Fake-President-Betrug (siehe S. 32), stehen meist nicht in einem unmittelbaren Zusammenhang mit einer Informationssicherheitsverletzung. In diesen Fällen greift die Vertrauensschaden-Versicherung Funk CrimeSecure. Entscheidend ist daher stets die Schadenursache, welche eine klare Trennung der Deckungskonzepte ermöglicht.

Losgelöst daneben steht im Falle einer Informationssicherheitsverletzung die Cyber-Versicherung. Hier hat Funk neben der CyberSecure für Industrieunternehmen (S. 22) weitere Sonderdeckungen für spezielle Branchenbedürfnisse entwickelt, wie die Funk CyberProfessional für Gewerbetreibende oder ein Spezialkonzept für Rechtsanwälte und Wirtschaftsprüfer (S. 24). ■

Abgrenzung von Cyber- und Vertrauensschaden-Versicherung

	Cyber-Versicherung	Vertrauensschaden-Versicherung
Gegenstand der Deckung	Versichert sind Schäden, die durch eine Verletzung der Informationssicherheit, verursacht durch benannte Ereignisse, entstehen.	Versichert sind Vermögensschäden, die dem versicherten Unternehmen durch unerlaubte vorsätzliche Handlungen einer Vertrauensperson und im definierten Umfang durch Dritte entstehen.
Leistungselemente	› Drittansprüche › Eigenschäden in Form umfangreicher Kostenbausteine (u. a. IT-Forensik, Datenwiederherstellung, Krisen- und Rechtsberatung, Informationskosten) › Betriebsunterbrechung › Lösegeldzahlungen	› Vermögensschäden durch Vertrauenspersonen › Vermögensschäden durch Dritte (z. B. Betrug (Fake President), Raub oder Diebstahl) › Kostenpositionen (u. a. Schadenermittlungs-, Rechtsverfolgungskosten, PR-Kosten)

Ihre Ansprechpartnerin
Alexandra Köttgen
a.koettgen@funk-gruppe.de

Ihr Ansprechpartner
Michael Winte
m.winte@funk-gruppe.de

Im Nachhinein sind Cyber-Angriffe nur schwer nachzuweisen. Das Versicherungskonzept der Funk CyberSecure inkludiert daher eine Beweislastumkehr im Schadenfall.

RISIKOTRANSFER

Das ist Funk CyberSecure

Cyber-Risiken bedrohen die Wirtschaft. Funk bietet mit der Funk CyberSecure eine exklusive und individualisierbare Versicherungslösung.

Mit der medialen Berichterstattung und der damit verbundenen Aufmerksamkeit rückt das Thema „IT-Risiken“ mehr und mehr in den Fokus. Einer der primären Gründe hierfür ist die Tatsache, dass sich die IT von einem reinen Unterstützungsprozess zu einer zentralen Ressource im Unternehmen entwickelt hat. Dieser Wandel und die entsprechend gesteigerte Bedeutung führen gleichermaßen auch zu einer Veränderung der Bedrohungslage. Neben Datenschutz- oder Integritätsverletzungen kann gerade auch die Nichtverfügbarkeit von Daten und IT-Systemen zu erheblichen Beeinträchtigungen des Geschäftsbetriebes und damit einhergehenden beträchtlichen Schäden führen.

Immense Schäden durch Fehlbedienungen

„Die Ursachen hierfür sind vielfältig und beschränken sich nicht auf Cyber-Kriminalität und Datenschutzverletzungen. Gerade auch Fehlbedienungen durch Mitarbeiter oder technische Probleme können zu immensen Schäden führen. Die Folgen sind im Vorwege kaum kalkulierbar“, führt Michael Winte, Fachbereichsleiter Cyber, Technology & Crime bei Funk, aus. Die schadenauslösenden Ursachen orientieren sich bei der Funk CyberSecure an dem Gefahrenkatalog des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und stellen nicht lediglich auf CyberCrime und Datenschutzverletzungen ab. Damit verfolgt die Funk CyberSecure einen deutlich weitergehenden Ansatz als viele andere am Markt erhältliche Cyber-Policen. Klassische Versicherungsprodukte gewähren für drohende Schäden aufgrund einer Informationssicherheitsverletzung (Verletzung der Vertraulichkeit oder Integrität von Daten sowie Verfügbarkeit von Daten und IT-Systemen) keinen oder allenfalls unzureichenden Schutz, da sie der Vielfältigkeit der Risiken und möglichen Schadenfolgen nicht in ausreichendem Maße begegnen können.

Versicherte Gefahren

- Netzwerksicherheitsverletzung
  - Hacker, Viren, Trojaner
  - DoS-Schaden
- Datenschutz-Vertraulichkeitsverletzung
- Fehlbedienung/Sabotage durch Mitarbeiter
- Technische Probleme
  - Bspw.: Überspannung, Spannungsabfall, Ausfall der Stromversorgung vor Ort, interner Netzwerkfehler, Hardwarefehler

Die Funk CyberSecure bietet bei einer Informationssicherheitsverletzung Versicherungsschutz für Eigenschäden im Rahmen umfangreicher Kostenbausteine für Eigenschäden, Erpressung, Betriebsunterbrechungen sowie die Freistellung oder Abwehr von Haftpflichtansprüchen. Darüber hinaus weist die Funk CyberSecure weitere Besonderheiten auf, hierzu zählt insbesondere eine Beweislastumkehr im Schadenfall zu Gunsten des Versicherungsnehmers. Viele Cyber-Angriffe sind im Nachhinein schwer oder kaum nachzuweisen. Durch die Beweislastumkehr wird dem Versicherten diese oftmals schwierige Beweisführung erspart.

Leistungen Funk CyberSecure

- Drittschäden
  - Abwehr/Befriedigung von Ansprüchen Dritter
  - Entschädigung mit Strafcharakter oder Gebühren
  - Vertragsstrafen und Bußgelder
- Eigenschäden
  - Dienstleistungs-, Beratungs-, Überwachungs-, Informations-, Monitoringkosten
  - Kosten für Wiederherstellung Reputation, Krisenberatung
- Betriebsunterbrechungsschäden
  - Fortlaufende Kosten und Betriebsgewinn
  - Definierte Mehrkosten
- Sonstige Deckungsbausteine
  - Cyber-Kriminalität (z. B. Fehlleiten von Geldern)
  - Lösegeldzahlungen
  - Sacheigenschaden

Branchenübergreifendes Bedürfnis

Die Nachfrage nach Versicherungslösungen für Cyber-Risiken ist enorm; das Bedürfnis nach Sicherheit und Risikotransfer in diesem Bereich besteht branchenübergreifend und unabhängig von der Größe der Unternehmen. Michael Winte sagt dazu: „Für das steigende Risikobewusstsein gibt es diverse Gründe, hierbei können sicherlich die DSGVO, die zunehmende globale Vernetzung und die mediale Berichterstattung angeführt werden. Hinzu kommt die Tatsache, dass sich die Verantwortlichkeit für organisatorische und technische IT-Security-Maßnahmen und einen etwaigen Risikotransfer im Unternehmen aufgrund der aktuellen Bedrohungslage mehr und mehr in die Führungsetagen der Unternehmen verlagert und sich die Verantwortlichen bei Mängeln erheblichen Haftungsrisiken ausgesetzt sehen.“ ■

Ihr Ansprechpartner
Michael Winte
m.winte@funk-gruppe.de

FUNK CYBERPROFESSIONAL

Schutz für Local Heroes

Kleinere Unternehmen und Freiberufler wähnen sich vor Hackern häufig in Sicherheit. Doch auch hier kann eine Cyber-Versicherung sinnvoll sein. Die Funk CyberProfessional ist für Kleinbetriebe die richtige Wahl.

Ob Rechtsanwalt, Zahnarzt oder Immobilienmakler – die Funk CyberProfessional, das jüngste Cyber-Spezialprodukt von Funk, richtet sich an Gewerbetreibende und Freiberufler mit einem jährlichen Umsatz von regelmäßig bis zu 10 Millionen Euro. Denn auch für diese sind Cyber-Risiken allgegenwärtig, trotz der häufigen Annahme, sie seien im Vergleich zu Großunternehmen für Kriminelle nicht attraktiv. Das Gegenteil ist der Fall: Bei entsprechender Arglosigkeit sind kleine Unternehmen oft einfache Ziele, vor allem für Cyber-Erpressungen.

Im Rahmen der CyberProfessional können Kunden mit Versicherungssummen von 100.000 bis 2 Millionen Euro Eigen- und Drittschäden absichern. „Die Spezialdeckung ist dabei wie ihre große Schwester, die CyberSecure, im Marktvergleich besonders leistungsstark“, sagt Johann Ulferts, Referent der Geschäftsführung bei Funk. Sie gewährleistet Schutz für alle Schäden, die aus der Verletzung der Verfügbarkeit, Integrität und Vertraulichkeit von Daten entstehen. Zudem profitieren Kunden von Elementen wie der Beweiserleichterung im Schadenfall und einem weitgehenden Verzicht auf den Selbstbehalt, etwa für IT-Dienstleistungskosten oder bei Straf- und OWi-Verfahren.

Back-up für die DSGVO

Ein Fokus der CyberProfessional liegt darüber hinaus auf der EU-Datenschutzgrundverordnung (EU-DSGVO), die seit Mai 2018 in Kraft ist. Auch Gewerbetreibende und Freiberufler müssen durch die erhöhten Anforderungen an die Informationssicherheit ihre datenschutzrelevanten Prozesse optimieren. Die EU-DSGVO sieht vielfältige Pflichten sowie weitreichende, bewusst abschreckende Geldbußen vor. Daher besteht zurzeit ein großes Maß an Verunsicherung, denn es drohen Konsequenzen, die bei kleineren Unternehmen schnell zu finanziellen Schwierigkeiten führen können. Die Funk CyberProfessional bietet hier eine maßgeschneiderte Deckungslösung, die interne Datenschutzprozesse sinnvoll ergänzt. Im Schadenfall steht Gewerbetreibenden und Freiberuflern ein verlässliches Dienstleister-Netzwerk zur Seite, das bei Cyber-Krisen effektive Unterstützung sicherstellt. ■

Ihr Ansprechpartner
Johann Ulferts
j.ulferts@funk-gruppe.de

Die CyberProfessional bietet Schutz für kleine Betriebe, aber auch für Arztpraxen und freie Berufe, wie Rechtsanwälte oder Architekten.

Ob in Deutschland oder weltweit: Funk kennt die Rechtslage vor Ort und empfiehlt Unternehmen so immer die passende Cyber-Deckung.

INTERNATIONALE CYBER-LÖSUNGEN

Expertise für Global Player

Cyber-Schäden kennen keine Grenzen und können im Ausland zu einem unangenehmen Problem werden. Mit Funk sind Sie international umfassend abgesichert.

Andere Länder, anderes Recht – das gilt auch für Cyber-Versicherungen. Die Funk CyberSecure ist weltweit gültig, sofern eine grenzüberschreitende Versicherung im jeweiligen Staat rechtlich zulässig ist. In Verbotsländern wie zum Beispiel Mexiko oder China benötigt ein Versicherer jedoch eine lokale Zulassung, um vor Ort Schutz zu bieten, ohne gegen geltendes Recht zu verstoßen.

Angesichts dieser Problematik empfiehlt Funk zwei unterschiedliche Varianten: den Abschluss von Lokalpolicen oder das Absichern des „finanziellen Interesses der Muttergesellschaft“ im Mastervertrag über eine sogenannte FInC-Deckung (Financial Interest Cover). Letztere ersetzt finanzielle Einbußen, die durch einen Cyber-Schaden bei einer ausländischen Tochter entstehen, und ist deutlich kostengünstiger.

„Der Abschluss einer Lokalpolice kann im Schadenfall klare Vorteile bieten.“

Peter Schneider,
Leiter Key Account Division

„Der Abschluss einer Lokalpolice kann im Schadenfall aber auch klare Vorteile bieten“, betont Peter Schneider, Leiter der Funk Key Account Division. Denn trotz FInC-Klausel dürfen fremde Versicherer in Verbotsländern keine Leistungen zur Schadenabwicklung, etwa die Betreuung von Schäden oder die Auszahlung von Versicherungssummen, durchführen. Bei Cyber-Vorfällen entstehen die Kosten für IT-Services aber häufig direkt vor Ort, und auch bei Haftungsfragen im Kontext personenbezogener Daten lohnt sich lokaler Schutz. Ob FInC-Deckung oder Lokalpolice: Funk und sein internationales Broker-Netzwerk Funk Alliance sind in über 100 Ländern Ihr kompetenter Cyber-Partner. ■

Ihr Ansprechpartner
Peter Schneider
p.schneider@funk-gruppe.de

IMPULSE AUS DEM FÜRSTENTUM LIECHTENSTEIN

Gesetz für Blockchain

Mit seinen Plänen rund um die Blockchain-Technologie hat das Fürstentum Liechtenstein weltweit für Aufsehen gesorgt. Im exklusiven Gastkommentar im Forum zeigt Regierungschef Adrian Hasler, welche Vorteile die Regulierung von neuen Technologien bietet – und warum Bitcoin nur der Anfang ist.

Im März 2018 habe ich auf dem „Finance Forum Liechtenstein“ angekündigt, dass Liechtenstein ein Blockchain-Gesetz erarbeitet. Diese Nachricht ging innerhalb kurzer Zeit durch die weltweite Blockchain-Community. Die vielen positiven Rückmeldungen, die wir in der Zwischenzeit erhalten haben, zeigen sehr deutlich, dass in der Blockchain-Welt ein großes Bedürfnis nach einer Regulierung besteht. Wieso ist das so? Ich bin überzeugt, dass neue Technologien und Innovationen Treiber der Wirtschaft sind und damit nachhaltig die Gesellschaft verändern. Klar, die Digitalisierung kennt nicht nur Sonnenseiten, dennoch dürfen wir uns als Staat nicht hinter Vorsicht und Regulierungen verstecken, sondern müssen die Innovationskraft der neuen Technologien für unseren Standort nutzen.

Mehr als nur Kryptowährungen

Aus diesem Grund habe ich mit „Impuls Liechtenstein“ vor rund fünf Jahren eine Plattform eingerichtet, welche uns den Puls der Zeit fühlen lässt. Wir haben damit einen übergeordneten Innovationsprozess zur Weiterentwicklung der staatlichen Rahmenbedingungen für die Wirtschaft initiiert.

Das geplante Blockchain-Gesetz ist unter anderem aus Inputs dieser Initiative entstanden. Die Arbeiten am Gesetz haben vor rund zwei Jahren begonnen. Dies zeigt, dass wir durch den intensiven Kontakt mit innovativen Unternehmen sehr früh Problemfelder erkennen und umgehend agieren können. Dabei ist relativ schnell klar geworden, dass das Potenzial der Blockchain nicht nur im Finanzdienstleistungsbereich, zum Beispiel bei Bitcoin, liegt. Vielmehr bietet sich die Blockchain an, um eine viel größere Palette an Vermögensobjekten digital abzubilden und für jede erdenkliche Dienstleistung zur Verfügung zu stellen. Dieses breite Feld, welches im Prinzip die gesamte Wirtschaft umfasst, wird üblicherweise unter dem Begriff Token-Ökonomie zusammengefasst. Ein Token repräsentiert hier ein Vermögensobjekt oder ein Wirtschaftsgut. Die Token-Ökonomie ist der nächste logische Schritt in der Digitalisierung unserer Wirtschaft, einschließlich der Finanzdienstleistungen.

Die Blockchain-Technologie

Die Blockchain (dt. „Blockkette“) ist eine Kette von digitalen Datenblöcken. Jeder Block fasst komplexe Informationen zu Transaktionen zusammen, zum Beispiel zu Bestellungen oder Überweisungen. Die einzelnen Blöcke werden auf einer Vielzahl dezentraler Rechner gespeichert. So sind die Datenketten unveränderbar, transparent und besonders sicher.

Von analogem zu digitalem Recht

Im Blockchain-Gesetz geht es um zwei große Themenbereiche: Einerseits muss geklärt werden, wie die Abbildung eines Rechts aus der bestehenden Rechtsordnung, beispielsweise des Eigentumsrechts an einem Fahrzeug, in einem digitalen Transaktionssystem funktioniert. Wir müssen herausfinden, wie diese Schnittstelle zwischen den beiden Welten rechtssicher gewährleistet werden kann. Diese Fragen gehen weit über die Abbildung eines Wertpapiers auf der Blockchain hinaus. Mit der Einführung des Token als neues Rechtselement schafft Liechtenstein ein Instrument, mit dem jedes beliebige Recht aus der analogen Welt digital abgebildet werden kann. Und das ist aus meiner Sicht eine der wichtigsten Innovationen des Blockchain-Gesetzes.

Finanziellem Missbrauch entgegenwirken

Andererseits muss ein Staat klarstellen, welche Anforderungen an die Dienstleister einer Token-Ökonomie gestellt werden, sobald das Finanzmarktrecht nicht anwendbar ist. Denn auch hier werden in Zukunft Unternehmen für ihre Kunden vermögensrelevante Tätigkeiten ausführen, welche schutzwürdig sind. Ohne eine Regulierung besteht ein erhöhtes Missbrauchsrisiko. Dieses soll mit dem Blockchain-Gesetz reduziert werden. Es werden Mindeststandards für Dienstleister definiert, um einerseits die Kunden zu schützen und andererseits die Interessen des Staates zu gewährleisten. Dies beinhaltet auch Fragen zur Anwendung der Geldwäschereibekämpfung und der Kundeninformation, welche über die Finanzmarktgesetze nicht gedeckt sind.

Liechtenstein wird mit dem Blockchain-Gesetz als erstes Land diese zentralen Fragen geklärt haben. Damit bieten wir sowohl Unternehmen als auch deren Kunden ein hohes Maß an Rechtssicherheit in diesem wichtigen Feld der Digitalisierung. Ich bin daher überzeugt, dass andere Staaten schon bald dem Beispiel Liechtensteins folgen werden. ■

Adrian Hasler

Seit 2013 ist Adrian Hasler Regierungschef des Fürstentums Liechtenstein. Ihm obliegt die Führung des Ministeriums für Präsidiales und Finanzen.

Die Kernaufgaben im Bereich Finanzen sind der Staatshaushalt sowie die Steuer- und Finanzmarktpolitik. Ziel von Regierungschef Hasler ist es, optimale und verlässliche Rahmenbedingungen zu schaffen, um die internationale Konkurrenz- und Innovationsfähigkeit Liechtensteins zu erhalten und zu stärken.

WIE SIEHT DAS ÖSTERREICHISCHE BUNDESHEER DIE CYBER-RISIKEN?

Aufbruch in neue Gefilde

Cyber-Gefahren bringen auch für das Militär neue Herausforderungen mit sich. Das österreichische Bundesheer will sich für die Zukunft wappnen – und investiert in Forschung.

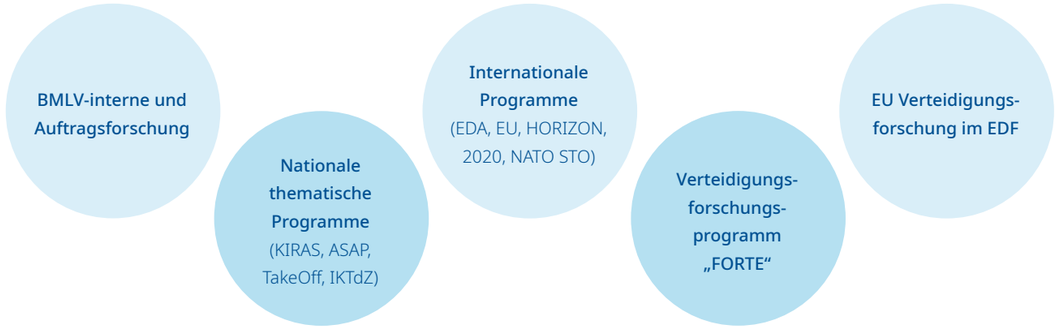
Der Technologiewandel der letzten Jahrzehnte hat nicht nur zu einem grundlegenden gesellschaftlichen Wandel geführt, sondern auch die Streitkräfte vor neue Herausforderungen gestellt. Neu entstandene Konfliktformen und „hybride" Bedrohungsbilder erfordern umfassende Lösungsansätze und stellen neue Anforderungen an die Entwicklung und die Fähigkeiten der Streitkräfte, um auch zukünftig als „strategische Handlungsreserve" der Republik Österreich im gesamten Aufgabenspektrum wirksam werden zu können.

Die Verteidigungsforschung folgt dabei den Anforderungen an die militärische Leistungsfähigkeit in Abhängigkeit von rüstungs- und sicherheitstechnischer Kompetenz. Sie etabliert dabei neue Formen der Zusammenarbeit zur Innovations- und Technologieentwicklung, und das sowohl auf europäischer als auch auf nationaler Ebene. Sie stützt sich dabei auf fünf Säulen, die Sie in der Grafik auf der nächsten Seite sehen.

Forschungsprogramm FORTE

Neben der Auftragsforschung und der aktiven Teilnahme an anderen nationalen Forschungsförderprogrammen wurde im Herbst 2018 erstmals das Verteidigungsforschungsprogramm FORTE (FORschung und TEchnologie) ausgeschrieben. Es bildet gemeinsam mit dem Sicherheitsforschungsprogramm KIRAS die sogenannte „Sicherheitsklammer" in Österreich und ist primär auf den militärischen Bedarf ausgerichtet. Im Rahmen von FORTE werden militärische Forschungsvorhaben im naturwissenschaftlichen und technischen Bereich, die der Fähigkeitenentwicklung für zukünftige Bedrohungsszenarien sowie dem Ausbau von Innovationsfähigkeit der Streitkräfte dienen sollen, im Volumen von 5 Mio. Euro gefördert. Das BMLV/ÖBH ist dabei als Nutzer und Expertisenträger für die inhaltliche und thematische Gestaltung des Förderprogramms verantwortlich. Die Priorisierung auf die zentralen Forschungsthemenbereiche (FTB) „Cyber Defence", „Führungsinformationssysteme", „ABC-Abwehr", „Counter IED", „Schutz kritischer Infrastrukturen gegen UAVs" und „Robotics" folgt daher der strategischen Ausrichtung und den damit verbundenen notwendigen Fähigkeiten moderner, innovativer und zukunftsorientierter Streitkräfte.

Die fünf Säulen der Verteidigungsforschung in Österreich



KIRAS = österreichisches Sicherheitsforschungsprogramm, ASAP = Austrian Space Applications Programme, EDA = European Defence Agency, NATO STO = NATO Science And Technology Organization, EDF = European Defence Fund

Cyber-Sicherheit ist in Österreich Sache des Bundesheers.

Robuste IKT-Lösungen

Im Bereich „Cyber Defence und Führungsinformationssysteme" werden beispielsweise besondere Anforderungen an robuste IKT-Lösungen und den Schutz eigener sowie externer Systeme gestellt. Die permanente Verfügbarkeit von Information sowie das Gewinnen der Informationsüberlegenheit und in weiterer Folge der Führungsüberlegenheit ist für den militärischen Erfolg im Einsatz von zentraler Bedeutung. Dies erfordert auch die Entwicklung und den Betrieb von C4I(STAR)-Systemen wie Führungs- und Fachinformationssystemen, Aufklärungs- und Überwachungssystemen, Lagebilddarstellungen, Entscheidungsunterstützungssystemen, Sensorsystemen usw. unter den Aspekten der Interoperabilität und Netzwerkfähigkeit der Streitkräfte. Die inhaltliche Ausrichtung des FTB „Cyber Defence und Führungsinformationssysteme" folgt dabei den Schwerpunktthemen „Cyber Situational Awareness & Cyber Range", „Security & Crypto", „Interoperabilität", „heterogene Informationsquellen" und „Sensornetzwerke".

Diese Ziele verfolgt das Programm FORTE

1. Forschungsrelevante Beiträge, primär im Bereich der Wehrtechnik, zur Unterstützung der militärischen Auftragserfüllung sicherstellen
2. Das BMLV und das ÖBH als Partner der Wirtschaft für Forschung, Innovation und Technologieentwicklung positionieren (jenseits von KIRAS)
3. Die nationalen Verteidigungsforschungskompetenzen derart stärken, dass nationale Forschungsinstitutionen auch im internationalen Wettbewerb zur Verteidigungsforschung (Forschungsprogramme der EU) konkurrenzfähig bleiben bzw. werden

FORTE soll aber nicht nur einen wesentlichen Beitrag zur militärischen Auftragserfüllung leisten, sondern auch das BMLV und das ÖBH als Partner der Wirtschaft für Forschung, Innovation und Technologieentwicklung positionieren. Als Forschungsförderprogramm hat FORTE daher auch zum Ziel, neue Akzente in der Forschungslandschaft Österreichs zu setzen und in weiterer Folge die nationalen Kompetenzen so zu stärken, dass nationale Forschungsorganisationen und Unternehmen auch im internationalen Umfeld wettbewerbsfähig sind.

Auf europäischer Ebene eröffnet sich demgegenüber ein noch höheres Potenzial. Mit dem European Defence Fund (EDF) steht ab 2021 erstmals in der Geschichte der EU ein signifikantes Budget aus dem gemeinsamen EU-Haushalt für den Verteidigungsbereich und die Stärkung der europäischen technologischen und industriellen Basis (EDTIB) zur Verfügung: 4,1 Mrd. Euro für Forschung (mit 100 %-Finanzierung) und 8,9 Mrd. Euro für Entwicklung i. S. von technologischer Entwicklung mit einer Förderung zwischen 20 % und 100 %, je nach Entwicklungsphase.

Strategische Entwicklungen anstoßen

Für Österreich ergibt sich dabei ein potentielles Investitionsvolumen von etwa 100 bis 150 Mio. Euro p. a., vorwiegend im Hochtechnologiebereich, sodass strategische Entwicklungen in ausgewählten Industriesektoren angestoßen werden und damit mittel- bis langfristig eine bessere strategische Positionierung österreichischer Unternehmen im europäischen Kontext gefördert und erreicht wird.

Dazu müssen naturgemäß aber auch die dafür nötigen Rahmenbedingungen geschaffen werden. Die Grundlagen dazu wurden bereits in der „österreichischen Strategie zur EU-Verteidigungsforschung" erarbeitet. Diese wurde im August des vergangenen Jahres durch den Ministerrat beschlossen. Damit liegt eine klare politische Absichtserklärung zur optimierten Nutzung der Potentiale des European Defence Fund in Österreich vor, um zu einer gesamtheitlichen Weiterentwicklung des Wirtschafts-, Forschungs- und Technologiestandortes Österreich beizutragen. ■

Gastbeitrag von Dipl.-Ing. Christian Meurers

Forschungsmanager für den Bereich „Cyber-Defence und Führungsinformationssysteme" im Bundesministerium für Landesverteidigung, Abteilung Wissenschaft, Forschung und Entwicklung

CYBER AN ERSTER STELLE

Steigendes Interesse an Deckungen

Ein Blick über die Alpen: Wie ist es um das Thema Cyber-Security in Österreich bestellt?

Dem Allianz Risiko-Barometer 2019 zufolge wächst die Angst vor wirtschaftspolitischen Risiken. Handelskriege, Wirtschaftssanktionen, Brexit und die damit verbundene Destabilisierung verunsichern auch die österreichische Wirtschaft. Rechtliche Veränderungen im wirtschaftlichen Umfeld werden ambivalent wahrgenommen: Einerseits werden gesetzliche Vorgaben wie die NIS-Richtlinie zur IT-Sicherheit und Datenschutzgrundverordnung (DSGVO) als nützlich erachtet. Andererseits verunsichern die möglichen rechtlichen Konsequenzen, wenn ein Unternehmen – aus welchem Grund auch immer – die gesetzlichen Vorgaben nicht 100-prozentig umgesetzt hat.

In Österreich rangiert die Angst vor Cyber-Vorfällen laut Risiko-Barometer sogar an erster Stelle – noch vor Naturkatastrophen und Betriebsunterbrechung. Dabei darf nicht übersehen werden, dass Cyber- und BU-Risiken oftmals korrelieren. Zahlreiche Datenskandale, Hackerangriffe und IT-Pannen haben dazu beigetragen, dass Cyber-Risiken in den Fokus rücken. Alle Branchen, unabhängig von der Unternehmensgröße, waren in Österreich von Cyber-Angriffen betroffen.

Doch wie reagiert Österreichs Wirtschaft? Noch vor Kurzem sahen Unternehmen das Thema Cyber-Sicherheit überwiegend im Verantwortungsbereich ihrer IT-Abteilung. Mittlerweile hat sich das Cyber-Security-Management aber einen Platz in den obersten Chefetagen erobert. Der Schwerpunkt der Risikominimierung liegt in der Prävention. Hier wiederum stand bisher die Abwehr von Hackerangriffen durch technische Vorkehrungen im Vordergrund. Zunehmend rückt jedoch der Faktor Mensch ins Zentrum des Interesses der Angreifer. Hacker nutzen äußerst subtil die Sorglosigkeit und Neugierde von Angestellten aus. Die meisten bisherigen Sicherheitskonzepte der Unternehmen reichen daher nicht mehr aus. Notwendig ist es, die Risiko-Awareness der Mitarbeiter zu schärfen.

> *„In Österreich rangiert die Angst vor Cyber-Vorfällen an erster Stelle – noch vor Naturkatastrophen und Betriebsunterbrechungen."*
>
> **Gabriele Zsitek,**
> Leiterin Broking/Financial Lines Funk Internat. Austria

Und während die Risiko-Awareness der Mitarbeiter das Fundament darstellt, sollte eine passgenaue Versicherungslösung als Dach eines Cyber-Sicherheitskonzepts fungieren.

Das Interesse an solchen Versicherungslösungen steigt in Österreich. Wie wichtig es dabei für Unternehmen ist, sich im Vorfeld von Cyber-Versicherungsexperten beraten zu lassen, zeigt das Beispiel Mondelez: Mondelez wurde 2017 durch einen Trojanerangriff erheblich geschädigt. Der Versicherer weigert sich jedoch zu zahlen und begründet dies damit, dass dieser Cyber-Angriff als „feindliche oder kriegsähnliche Aktion" zu werten sei. Schäden, die im Krieg eintreten, sind nicht vom Versicherungsschutz umfasst. Die Klärung der Frage, ob ein Versicherungsfall vorliegt, kann viel Zeit und Kosten in Anspruch nehmen. Diese Unsicherheiten dürfen sich im Schadenfall jedoch nicht zulasten der Versicherungsdeckung auswirken. ■

Ihre Ansprechpartnerin
Gabriele Zsitek
g.zsitek@funk-austria.com

Täter wenden sich unter falscher Identität an Mitarbeiter, um an Geldbeträge zu gelangen.

VERTRAUENSCHADEN-VERSICHERUNG

Die Masche mit dem falschen Chef

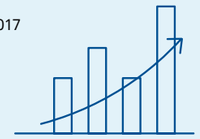
Unternehmen werden immer häufiger Opfer des sogenannten „CEO-Fraud“ oder auch „Fake-President-Fraud“. Die Grundidee gleicht dem bekannten „Enkeltrick“. Durch immer weitergehende Professionalisierung der Täter wird es jedoch trotz der medialen Aufmerksamkeit schwerer, sich zu schützen.

Der Fake-President-Fraud hat in den vergangenen Jahren mehrfach für Schlagzeilen gesorgt, Unternehmen wurden teilweise um zweistellige Millionenbeträge betrogen. Die Täter wenden sich unter falscher Identität an Mitarbeiter, um diese gezielt zum Überweisen mitunter erheblicher Geldbeträge – in der Regel auf ausländische Konten – zu verleiten. Der Vorwand für die Überweisung kann beispielsweise der Kauf von Unternehmensanteilen sein. Hierfür nutzen die Täter zumeist durch Social Engineering erlangte Informationen über interne Abläufe, Kommunikationswege und Geschäftsbeziehungen. Dabei wird die bereits vorhandene Freigabe für die Transaktion durch einen Vorgesetzten (wie z. B. den CEO) oder die Anweisung durch den Vorgesetzten selbst durch gefälschte E-Mails und/oder per Telefonanruf vorgetäuscht. Häufig sind angebliche Anwälte involviert, die das Unternehmen bei der streng vertraulichen Transaktion unterstützen und so das Vertrauen des getäuschten Mitarbeiters stärken. Das überwiesene Geld kann in der Regel nicht zurückgeholt werden, die Täter lösen die Konten binnen kürzester Zeit auf und transferieren die erbeutete Summe auf verschiedenste weitere Konten, um so eine Nachverfolgbarkeit zu erschweren.

Regelmäßige Schulungen und die Sensibilisierung der Mitarbeiter können das Risiko eines erfolgreichen Betruges deutlich minimieren. Einen allumfassenden Schutz gewährleisten jedoch auch diese Maßnahmen nicht. Solange Zahlungsprozesse nicht ausnahmslos vollautomatisiert in einem Unternehmen durchgeführt werden, bleibt die Eingriffsmöglichkeit über die Beeinflussung von Mitarbeitern ein Risiko. Hinzu kommt, dass die Täter dieses Szenario stetig weiterentwickeln: Jüngst wurden beispielsweise angebliche Mitarbeiter der IT eingebunden, die nach dem Anruf des falschen Chefs den Mitarbeiter über einen versuchten Fake-President-Betrug in Kenntnis setzen. Zum Schein solle die geforderte Summe überwiesen werden, um die Täter auf frischer Tat zu ertappen. Auch hier war das erbeutete Geld für das betrogene Unternehmen verloren.

+ 60 Prozent der Fälle allein in Deutschland (2015 vs. 2016)

BKA, 2017



Diese und weitere Betrugsmaschen – wie beispielsweise der Fake-Identity-Fraud oder das Fehlleiten von Geldern oder Waren – haben sich längst zu einer etablierten Form der Wirtschaftskriminalität entwickelt. Nicht nur in Unternehmen gewinnt das Thema an Brisanz, auch die Versicherungswirtschaft listet Schäden durch den Fake-President-Fraud inzwischen auf den oberen Rängen aktueller und besonders schadenträchtiger Szenarien. Der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) beziffert den im Zeitraum von 2016 bis 2018 entstandenen Schaden auf über 150 Millionen Euro. Die Dunkelziffer dürfte deutlich höher liegen, da die Statistik lediglich Versicherern gemeldete Fälle erfasst.

„Mit der Funk CrimeSecure gibt es eine eigenständige Lösung, welche aktuelle Bedrohungslagen absichert.“

Alexandra Köttgen,
Expertin für Vertrauensschaden-Versicherungen

Risikotransfer als Ergänzung

Als Ergänzung der Risikoprävention besteht auch die Möglichkeit eines Risikotransfers. Versicherbar sind diese Schäden über eine Vertrauensschaden-Versicherung. Neben den geschilderten Betrugsszenarien bietet diese Versicherungslösung Schutz vor Schäden durch unternehmensfremde Dritte, die durch andere Straftaten wie beispielsweise Raub, Diebstahl oder Unterschlagung entstehen. „Mitversichert sind daneben auch Schäden durch unerlaubte Handlungen eigener Mitarbeiter, die häufig ein noch deutlich weiter reichendes Schädigungspotential besitzen und über einen langen Zeitraum immense Schäden verursachen können“, so Alexandra Köttgen, Expertin für Vertrauensschaden-Versicherungen bei Funk, „die Motive sind vielfältig, angefangen bei persönlicher Not, Frustration oder Habgier bis hin zu Vergeltung.“

Die Folgen für Unternehmen erschöpfen sich nicht in den entstandenen Schäden in Form des Abhandenkommens von Geldern: Regelmäßig fallen Kosten, beispielsweise im Rahmen der Schadenermittlung oder Rechtsverfolgung, an, es werden Vertragsstrafen fällig oder die Täter verursachen Schäden durch den Verrat von Geschäfts- oder Betriebsgeheimnissen.

„Viele Versicherungsprodukte werden den Risiken nicht vollumfänglich gerecht, aus diesem Grund haben wir mit der Funk CrimeSecure eine eigenständige Lösung entwickelt. Neben der Berücksichtigung der aktuellen Bedrohungslage haben wir auch unsere Erfahrungswerte aus vielfältigen Schadenfällen in die Gestaltung des Produktes einfließen lassen“, so Köttgen. ■

Ihre Ansprechpartnerin
Alexandra Köttgen
a.koettgen@funk-gruppe.de

40 % der Unternehmen waren in den letzten zwei Jahren vom CEO-Fraud betroffen.

Dabei waren 5 % der Angriffe erfolgreich.

PwC-Studie
zur Wirtschaftskriminalität 2018

CYBER-RESTRISIKEN ABSICHERN

So gehen Sie die letzte Meile

Ein technisch sicheres IT-System oder Datenschutzkonformität stellen nur einen Teil des Weges zum ganzheitlichen Cyber-Risikomanagement dar. Wie Sie den Zieleinlauf effizient und erfolgreich meistern, zeigt Funk Schweiz.

Bei der Teilnahme an einem Marathon muss alles stimmen: Läufer sollten körperlich wie auch psychisch mit der richtigen Einstellung ins Rennen gehen – und einen kompetenten Trainer haben, der sie motiviert, wenn die Kraft einmal nachlässt. Ähnlich verhält es sich beim ganzheitlichen Management von Cyber-Risiken. Eine hastig abgeschlossene Versicherungslösung hilft einem Unternehmen genauso wenig weiter wie der alleinige Fokus auf die Optimierung der IT-Sicherheit oder die Sensibilisierung der Mitarbeitenden. Da Angreifer stetig neue Methoden entwickeln, kann ein hundertprozentiger Schutz auch bei umfassenden Präventionsmaßnahmen nicht erreicht werden.

„Die Quantifizierung des Cyber-Restrisikos ist der letzte Schritt eines ganzheitlichen Risikomanagements."

Max Keller,
Lead Funk RiskLab
Funk Insurance Brokers AG

„Die Quantifizierung der Cyber-Restrisiken ist der letzte Schritt eines ganzheitlichen IT-Risikomanagements", sagt Max Keller, Lead Funk RiskLab bei Funk Schweiz. Die Funk-Experten ermitteln finanzielle Restrisiken und transferieren diese bei Bedarf in den Versicherungsmarkt.

Versteckte Risiken finden

Der Fokus liegt dabei unter anderem auf meist unerkannten Risiken, wie zum Beispiel dem Datenschutz beim Outsourcing von IT-Services. Im Schadenfall haftet hier sowohl in der EU als auch in der Schweiz der rechtlich Verantwortliche – also jenes Unternehmen, das die Daten erhebt, und nicht der externe Dienstleister (Auftragsverarbeiter). Je mehr Outsourcing-Partner involviert sind, desto höher ist die Wahrscheinlichkeit, dass Daten trotz Vorsichtsmaßnahmen nicht datenschutzkonform verarbeitet werden und es zum Haftungsfall kommt. Ein Restrisiko, das abgesichert werden sollte.

„Wichtig ist beim Cyber-Restrisiko vor allem, dass sich die Unternehmensleitung für die Absicherung zuständig fühlt", betont Keller. Da deren Zeit erfahrungsgemäß begrenzt ist, nutzt Funk effiziente Tools und Prozesse: In zwei Fragebögen wird das unternehmensspezifische Risikoprofil erhoben, anhand dessen der Cyber Risk Calculator (siehe Kasten) potenzielle Schadenwerte ermittelt. Im Anschluss folgt ein persönlicher Risikodialog, bei dem die Ergebnisse des CRC diskutiert werden.

Die Unternehmensleitung erhält damit eine konkrete Entscheidungsgrundlage, ob ein Risikotransfer sinnvoll ist und zu welchen Konditionen die ermittelten Cyber-Restrisiken versichert werden können. Zudem ist die vollständige Abarbeitung des IT-Risikomanagement-Prozesses gewährleistet. Führungskräfte sind so vollständig abgesichert – und können gemeinsam mit ihren Mitarbeitenden die Ziellinie zum ganzheitlichen Cyber-Risikomanagement erfolgreich überqueren. ■

Der Funk Cyber Risk Calculator

Der Cyber Risk Calculator (CRC), entwickelt vom Funk RiskLab in der Schweiz, unterstützt Unternehmen bei der Quantifizierung ihrer Cyber-Restrisiken. Das Tool kombiniert unternehmensspezifische Risikodaten logisch mit Schadendaten und Erfahrungswerten. So erhalten Entscheider eine Berechnung ihrer individuellen Risikopotenziale. Zudem können die ermittelten Risiken direkt im CRC in die entsprechenden Versicherungssummen umgewandelt werden.

Über 100 Funk-Kunden nutzen den CRC bereits erfolgreich; darüber hinaus ist im Schweizer Kundenportal eine Betaversion verfügbar. Mithilfe dieses Tools sind Unternehmen zukünftig in der Lage, Veränderungen im Zusammenhang mit Cyber-Risiken eigenständig festzustellen und zu erfassen. Funk erhält in einem solchen Fall eine Benachrichtigung, sodass Risikoveränderungen unmittelbar bei bestehenden Versicherungslösungen berücksichtigt werden können.

Ihr Ansprechpartner
Max Keller
max.keller@funk-gruppe.ch

Das letzte Stück ist oft das schwerste, auch beim Versicherungsschutz.

Im Falle eines Cyber-Schadens müssen viele Experten zusammenarbeiten.

INCIDENT RESPONSE TEAM

Verhalten im Schadenfall

Was tun im Falle eines Cyber-Schadens? Für betroffene Unternehmen ist es wichtig, besonnen zu reagieren – und dennoch schnell zu sein.

Wenn der Worst Case eintritt, die Systeme ausfallen und der Betrieb stillsteht oder eine Datenpanne öffentlich bekannt wird, gilt es, besonnen und zielgerichtet zu reagieren. Verschiedene Studien und Erfahrungen aus Schadenszenarien kommen zu der Erkenntnis, dass die Geschwindigkeit und die Qualität der Reaktion einen signifikanten Einfluss auf das Ausmaß des Vorfalles haben.

Implementierung von Maßnahmen

Es ist daher zu empfehlen, sich auf einen potenziellen Schadenfall dezidiert vorzubereiten. Der Erfahrung nach wirkt sich die Implementierung von Maßnahmen zur Krisenbewältigung im Vorfeld sehr positiv auf Dauer und Höhe des Schadens aus. Wichtig ist die vorherige Festlegung und Benennung von Verantwortlichkeiten auf sämtlichen Hierarchieebenen. Zudem sollte ebenfalls im Vorfeld ein Incident Response Team mit Mitarbeitern aus unterschiedlichen Bereichen (IT-Sicherheit, IT-Administration, Recht und Datenschutz, Finanzwesen, Marketing und Kommunikation sowie insbesondere den jeweiligen Fachbereichen im Unternehmen) zusammengestellt werden, um damit auch die Auswirkungen auf das operative Geschehen einschätzbar zu machen. Achten Sie auf Vertretungsregelungen und Erreichbarkeit! Empfehlenswert sind insbesondere auch das Erarbeiten eines Krisenplans und die Implementierung eines Notfallmanagements. Halten Sie in diesem Rahmen, sofern diese Ressourcen nicht intern abgebildet werden, Dienstleister z. B. für den Bereich IT-Administration vor. Viele Schadenfälle lassen sich mittels interner Ressourcen nur schwer oder gar nicht unter Kontrolle bringen, insoweit bedarf es kostspieliger externer Unterstützung durch Experten. Insbesondere externe Spezialisten aus den Bereichen Incident Response Management, spezialisierte Rechtsanwälte sowie Krisen- und Kommunikationsberater müssen häufig eingeschaltet werden. Hier setzt die Versicherungslösung Funk CyberSecure (für eine ausführliche Darstellung der Funk Cyber Secure siehe Seite 22) im Schadenfall an: Bereits im Verdachtsfall steht die der Police hinterlegte Krisenberatung zur Verfügung. Unter der Hotline ist eine Erreichbarkeit rund um die Uhr gewährleistet. Dort werden zunächst die ersten Informationen zu dem potentiellen Schadenfall aufgenommen. Anhand dieser Erkenntnisse wird dann umgehend ein Incident Response Manager durch den Dienstleister benannt, der sich binnen kürzester Zeit mit konkreten Handlungsempfehlungen zurückmeldet und erste Sofortmaßnahmen einleitet. Sodann wird ein Incident Response Team gebildet. Dieses Team ist für die erforderlichen Reaktions- und Wiederherstellungsmaßnahmen zuständig. Dies kann je nach Schadenumfang und -ausmaß in unterschiedlicher Form erfolgen: telefonischer Support, Vor-Ort-Unterstützung durch Experten, Tiefenanalyse in Form forensischer Untersuchungen unter Berücksichtigung sämtlicher Beweismittel sowie Bewertung der rechtlichen Rahmenbedingungen.

Michael Winte, Fachbereichsleiter Cyber, Technology & Crime bei Funk, betont: „Im Rahmen der Funk CyberSecure findet ein etwaiger Selbstbehalt auf diese Leistungen keine Anwendung. Sollte sich im Nachhinein herausstellen, dass der Schadenfall auf eine nichtversicherte Ursache zurückzuführen ist, verzichtet der Versicherer überdies auf die Rückerstattung bis zu diesem Zeitpunkt angefallener Kosten.“ ■

» Sieben Empfehlungen für den Schadenfall

Florian Sättler, Cyber Incident Manager bei Crawfort & Company, benennt die aus seiner Erfahrung nach wichtigsten Grundsätze im Falle eines Cyber-Schadens.

Crawford & Company ist ein international renommierter Schadendienstleister. Aufgrund der langjährigen Etablierung am Markt und der umfassenden Erfahrungen im Incident Response Management ist Crawford der von Funk bevorzugte Dienstleister im Rahmen der Cyber-Secure.

1 Handeln Sie ruhig und besonnen nach Maßgabe des erarbeiteten Notfall-Managementkonzepts / Krisenplans und ziehen Sie den externen Incident Response Manager so schnell wie möglich hinzu.

2 Prüfen Sie mögliche Sofortmaßnahmen und bringen Sie den Informationsfluss unter Kontrolle.

3 Sofern möglich und sinnvoll, stimmen Sie alle Maßnahmen mit dem internen Incident Response Manager ab, der für die Kommunikation mit dem externen Incident Response Management verantwortlich ist.

4 Agieren Sie vorsichtig und versuchen Sie alle Beweise nach Möglichkeit zu sichern oder unverändert zu lassen.

5 Im Falle einer Erpressung / Lösegeldforderung oder eines Vorfalls mit strafrechtlicher Relevanz bringen Sie den Fall unbedingt zur Anzeige.

6 Soweit personenbezogene Daten betroffen sind, melden Sie den Vorfall den zuständigen Datenschutzbehörden.

7 Prüfen Sie auch, ob und inwieweit der Vorfall Benachrichtigungsverpflichtungen gegenüber sonstigen Behörden oder an Vertragspartnern auslöst.

RISIKOREPORTS ZUM KOSTENLOSEN DOWNLOAD

Projekt der Funk Stiftung

Cyber-Risiken gestalten sich in jedem Land unterschiedlich. Wer eine Investitionsentscheidung treffen will, findet in den Risikoreports fundierte Informationen.

Welche Ansprüche kann ein Unternehmer in Ländern wie China, Russland oder der Türkei an die Cyber-Sicherheit stellen? Welche technischen Voraussetzungen gibt es dort, die ausländische Unternehmen und Personen schützen? Und wie sind die Rahmenbedingungen, um sich juristisch gegen eine Cyber-Attacke zu wehren? „Für Unternehmen, die Investitionen im Ausland erwägen, sind diese Fragen höchst relevant", weiß Hendrik Löffler, Vorstandsvorsitzender der Funk Stiftung, und merkt an, dass die entsprechenden Risikodaten bislang wenig transparent waren und nur mit hohem eigenen Aufwand oder mit Beauftragung eines Dienstleisters zu erwerben waren. „Praxisorientierte Antworten verspricht nun die Publikationsreihe *Risiko Report – Politische Risikoszenarien*", so Löffler.

Für 25 Länder (siehe unten), die für die deutsche Wirtschaft besonders relevant sind, wird die Frage nach den Cyber-Risiken untersucht. Datengrundlage sind unter anderem der „Cyber Power Index" und der „Global Cybersecurity Index". Darüber hinaus wurden zahlreiche weiteren Quellen herangezogen, die am Ende eines jeden Reports genannt werden. Neben den Cyber-Risiken finden sich in den Reports außerdem Einschätzungen über die politische Stabilität oder die Marktstruktur des Landes.

So entsteht eine faktenbasierte Grundlage für Entscheidungen über eine etwaige Erschließung neuer Märkte, den Abschluss neuer Lieferantenaufträge oder vergleichbare Themen. Erstellt wurden die Reports von CONIAS Risk Intelligence; die Funk Stiftung hat das Projekt gefördert. ■

Zu diesen 25 Ländern gibt es jeweils einen Risikoreport:

- Ägypten
- Argentinien
- Belarus
- Brasilien
- China
- Indonesien
- Iran
- Italien
- Kasachstan
- Katar
- Kolumbien
- Marokko
- Mexiko
- Polen
- Russland
- Saudi-Arabien
- Südafrika
- Südkorea
- Thailand
- Türkei
- Tunesien
- Ukraine
- USA
- Vereinigtes Königreich
- Vietnam

Laden Sie die Risikoreports kostenlos herunter:

funk-stiftung.org/risikoreports

Einen ersten Überblick zu den Reports gibt es hier:

funk-stiftung.org/Broschuere-risk-reports.pdf

BITCOIN-ERPRESSUNG IN DER SCHWEIZ

„Der Vorfall hat uns die Augen geöffnet“

Was passiert, wenn plötzlich der Großteil der eigenen Dateien verschlüsselt ist? Ein Schweizer Unternehmen hat genau diesen Fall im Juli 2018 erlebt.

Der Sommer 2018 ging als eine Anomalie in die europäische Wetteraufzeichnung ein. Einem etablierten mittelständischen Unternehmen in der deutschsprachigen Schweiz wird diese Zeit aber nicht nur aufgrund der Hitze in Erinnerung bleiben, sondern auch wegen einer Anomalie im eigenen IT-System: ein zielgerichteter Cyber-Angriff, der zum Umdenken der Führungskräfte und zur nachhaltigen Umstellung der IT-Sicherheitsorganisation führte.

An einem Mittwoch im Juli fiel dem IT-Support eine Unregelmäßigkeit in der Auslastung der Server auf, Stunden später fiel der Mail-Server kurzfristig aus. Trotzdem ging niemand vom Schlimmsten aus. Am Donnerstagmorgen folgte jedoch das böse Erwachen. „Der IT-Support musste feststellen, dass die Dateien auf 17 der insgesamt 22 Server vollständig verschlüsselt waren“, so der CFO des betroffenen Unternehmens. Der Angriff war besonders heimtückisch, denn neben den Core-Applikationen waren teilweise auch die Dateien der Backup-Applikationen verschlüsselt. Eine sofortige Wiederherstellung des Systems war deshalb unmöglich. In den verschlüsselten Dateien war die Forderung der Cyber-Kriminellen enthalten: Das Unternehmen sollte 24 Bitcoins für die Entschlüsselung der Daten und somit für die sofortige Fortführung der Geschäftstätigkeiten bezahlen.

Der Angriff war kein Zufall

Drei Indizien deuteten auf einen zielgerichteten und lange geplanten Cyber-Angriff hin: Erstens begann dieser genau in dem Moment, als sich der IT-Leiter in den Sommerferien befand. Zweitens sollte nach der Abwesenheit des IT-Leiters das Datensicherungskonzept überarbeitet werden. Drittens veränderten die Angreifer die Konfigurationen der Backups insofern, als dass die Spezialisten im Nachgang nur eine unvollständige Datensicherung vorfanden.

Da das Führungsteam nicht vorhatte, das Lösegeld zu bezahlen, meldete es den Vorfall direkt bei den zuständigen Behörden. Gleichzeitig bildete sich ein Krisenstab, der aus Vertretern des Unternehmens sowie einem IT-Service- und einem IT-Security-Provider bestand.

Kommunikation im Fokus

Inzwischen begannen die Aufräumarbeiten. Am Wochenende wurden alle Laptops und Clients mit einem DeepScan überprüft und von Schadprogrammen bereinigt. Um die vitalen Kommunikationsfunktionen wiederherzustellen, konfigurierte die IT-Abteilung bis Montag einen Notserver und stellte den Datenserver wieder zur Verfügung. Nun war das Unternehmen zumindest in der Lage, in gewohnter Art mit den Kunden zu kommunizieren. Demgegenüber lief die Produktion langsam leer, da die Arbeitsvorbereitung nur mittels spezifischer Applikationen erfolgen konnte. Der CFO erinnert sich an die neuen Herausforderungen: „Die interne und externe Kommunikation war in dieser Phase besonders wichtig, um Sicherheit an die Mitarbeitenden und die Kunden auszustrahlen.“

„Unsere ‚business first‘-Einstellung machte es den Angreifern zu einfach, unsere IT-Systeme zu kompromittieren.“

CFO des betroffenen Unternehmens

Der Krisenstab erlangte unterdessen die ernüchternde Erkenntnis, dass bei diesem Cyber-Vorfall weder Backups noch eine passende Decryptor-Software genutzt werden konnten. Um die Reputation des Unternehmens zu schützen, mandatierten die Verantwortlichen daher einen spezialisierten amerikanischen Unterhändler. Dieser nahm am folgenden Freitag im Darknet die Verhandlungen mit den Cyber-Kriminellen auf. Tatsächlich gelang es ihm, das Lösegeld von 24 auf 12 Bitcoins zu senken und am Montag in den Besitz des Schlüssels zu gelangen. Trotz des engagierten Einsatzes des IT-Teams dauerte die Entschlüsselung der Dateien jedoch noch zusätzliche 48 Stunden, sodass die Geschäftstätigkeit erst am Donnerstag wieder vollständig hergestellt wurde.

„Rückblickend haben wir bei der IT-Sicherheit zu stark auf klassische Methoden vertraut“, resümiert der CFO. „Unsere ‚business first‘-Einstellung machte es den Angreifern zu einfach, unsere IT-Systeme zu kompromittieren.“ Seiner Erfahrung nach achten die Angreifer nicht auf die Attraktivität des Ziels, sondern suchen den Weg des geringsten Widerstandes. „Ich bin überzeugt, dass 99 von 100 Unternehmen die Möglichkeiten von professionellen Cyber-Kriminellen unterschätzen. Der Vorfall hat uns die Augen geöffnet, die IT Security ist jetzt genauso wichtig wie das Tagesgeschäft.“

Sicherheit hat ihren Preis

Der zweiwöchige Ausfall der IT-Systeme kostete das Unternehmen rund 400.000 Schweizer Franken. Während der Verschlüsselung schlugen etwa 10.000 verlorene produktive Stunden, das Lösegeld, das Beratungshonorar und die Kosten für den Notserver zu Buche. Im Nachgang investierte das Unternehmen noch einmal circa 200.000 Schweizer Franken in ein Security Operation Center (SOC) und weitere IT-Security-Maßnahmen.

Einen finanziellen Lichtblick gab es am Ende aber doch: Das Lösegeld und die Beratungskosten waren im Rahmen einer Kidnap & Ransom-Versicherung abgedeckt. ■

funkforum Cyber 2019

RADAR SMART SOLUTION UND RISK CHECK

Lösungen speziell für KMU

RadarServices ist der bevorzugte Kooperationspartner von Funk beim Thema IT-Sicherheit. Da dieses Thema nicht nur große Unternehmen betrifft, gibt es nun eine spezielle Lösung für kleinere und mittlere Unternehmen, mit denen IT-Risiken erkannt und erfolgreich vermieden werden können.

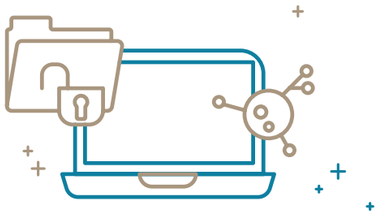
Ein umfassendes, kontinuierliches IT-Security-Monitoring war für kleine und mittlere Unternehmen (KMU) bislang in aller Regel zu ressourcenintensiv. Die IT-Experten von RadarServices, einem Funk-Kooperationspartner, machen nun aber auch diese Unternehmen sicherer – mit Radar Smart Solution sowie dem Risk Check. Die Lösungen wurden speziell für Unternehmen mit bis zu 500 Mitarbeitern entwickelt. Oft wird in Unternehmen dieser Größenordnung die neue Gefahr der Cyber-Attacken noch unterschätzt. Dabei geraten aber beispielsweise Kundendaten verstärkt ins Visier von Kriminellen. Das verschärft die Bedrohungslage und führt dazu, dass KMU bei Erpressung viel häufiger zahlen, um ihre Systeme zu entsperren. Wie Christian Polster, Chief Portfolio Officer von RadarServices, betont, „stehen nicht nur große Konzerne im Fokus der Cyber-Angreifer. Kleine und mittelständische Unternehmen trifft es dann besonders hart. Wenn die Produktion plötzlich stillsteht, das Abrechnungssystem nicht mehr verbunden ist oder die E-Mail-Kommunikation ausfällt, kostet das Geld, Reputation und es ist schnell existenzbedrohend.“ Radar Smart Solution lässt sich reibungslos in die vorhandene IT-Infrastruktur von Unternehmen bis zu 500 Mitarbeitern integrieren. Teil von Radar Smart Solution ist die „Radar Smart Box“ – diese sammelt potenziell sicherheitsrelevante Daten aus den wichtigsten Quellen sowohl innerhalb des Netzwerks als auch von extern. Die gewonnenen Daten werden im nächsten Schritt automatisiert analysiert und die Erkenntnisse im Radar Smart Cockpit dargestellt. Diese Übersicht ist nach einer Prioritätenliste geordnet und mit Informationen zu den konkreten nächsten Schritten versehen. Das Cockpit bildet für Kunden die Basis, um schnell die richtigen Maßnahmen zu ergreifen, die vorhandenen personellen Ressourcen optimal einzusetzen und insgesamt die IT-Sicherheit des Unternehmens zu erhöhen.

Bislang gab es für KMU wichtigere Themen als die Sicherheit der IT. Doch nun setzt ein Umdenken ein.

Risk Check für kleine Betriebe

Neben Radar Smart Solution gibt es den Risk Check. Der Risk Check ist speziell für kleine Firmen mit bis zu 50 Mitarbeitern gedacht. Besonders attraktiv ist die denkbar einfache Handhabung, zum Beispiel sind keine Schritte für die Integration in die vorhandene IT notwendig. Via Webinterface haben Kunden Zugriff auf aktuelle und historische Daten. Diese Lösung bietet eine automatisierte Überprüfung. Die Überprüfung umfasst sowohl einen externen als auch einen internen Schwachstellenscan für sämtliche PCs, Laptops und Server inklusive eines Fragebogens zur Selbstbeurteilung der eigenen IT-Landschaft. „Wir wollen kleinen und mittleren Unternehmen Lösungen bieten, die IT-Sicherheit steigern und gleichzeitig schlank und leistbar sind. Aus dieser Überlegung heraus entstanden Radar Smart Solution und Risk Check“, sagt Harald Reisinger, Geschäftsführer von RadarServices. „Mit diesen Lösungen bieten wir erstmals in Europa effizientes IT-Security-Monitoring für KMU an.“ ■

Die Top-10-Risiken für KMUs



1. Mitarbeiter sind nicht ausreichend geschult, mit Angriffen korrekt umzugehen
2. Oft einmalige Investition in IT-Sicherheit (Antivirensoftware, Firewall) – ohne weitere Vorkehrungen oder Updates
3. Fehlende Investitionen in IT und IT-Security
4. Nur ein (unsicheres) Passwort für alle Geräte/Konten
5. Keine IT-Abteilung bzw. kein IT-Verantwortlicher
6. Risiken und Attacken schwer einschätzbar
7. Regularien – Überblick über Gesetze und Vorgaben ist schwierig
8. Fehlender Überblick über Geräte und Infrastruktur
9. Phishingangriffe – kleine Firmen sind eher angreifbar und Folgen sind schwerwiegender
10. Keine Sicherheitsabläufe etabliert

Kooperation im Sinne der Kunden

Beim Thema IT-Sicherheit kooperiert Funk im Rahmen von Funk Beyond Insurance (siehe Seite 6 in diesem Heft) mit dem österreichischen IT-Dienstleister RadarServices.

RadarServices hat sich auf die Erkennung von Risiken für die Sicherheit der IT in Unternehmen spezialisiert und nutzt dafür eine eigens entwickelte Technologieplattform.

Passgenau dazu bietet Funk eine Cyber-Risikoanalyse und das Versicherungskonzept Funk CyberSecure an. Damit stellen beide Unternehmen gemeinsam ein IT-Sicherheitskonzept zur Verfügung, welches einzigartig auf dem Markt ist. Angesichts der IT-Bedrohungen, denen Unternehmen heute gegenüberstehen, bietet diese Lösung effizienten Schutz.

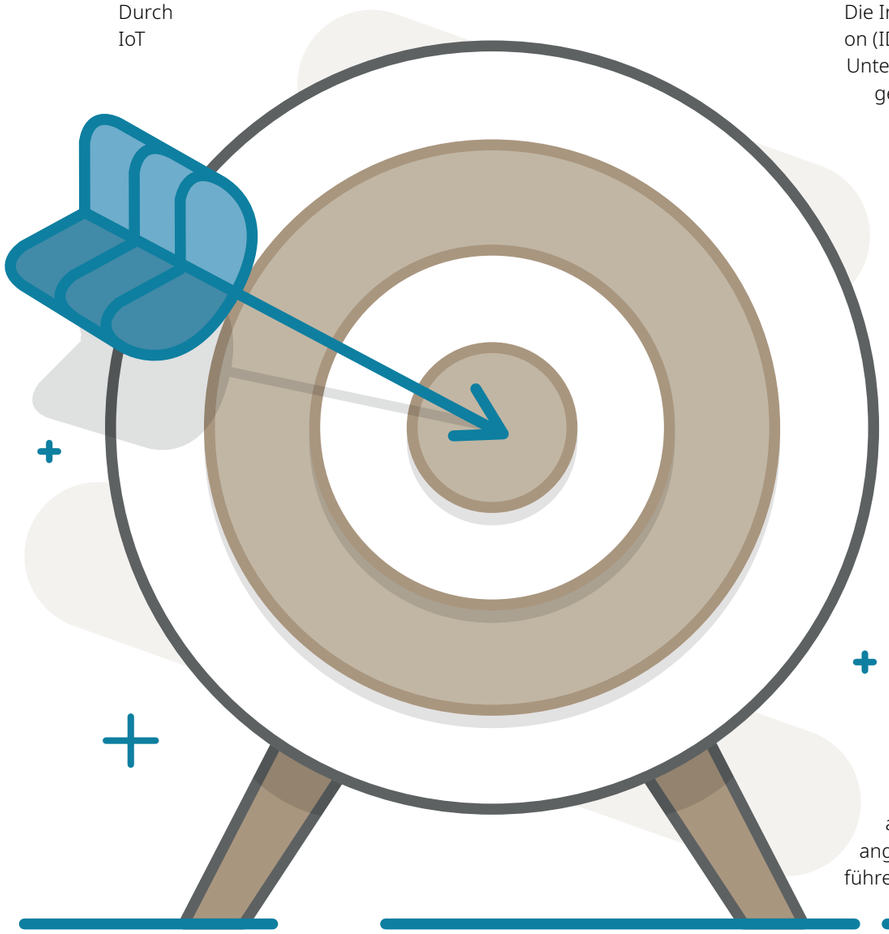
RADAR SERVICES

STUDIEN ZUR IT-SICHERHEIT

Vergrößerte Angriffsfläche

Studien zählen Cyber-Risiken zu den Top-Risiken der Zukunft. Doch Unternehmen können sich aktiv schützen – mit diesen zehn Tipps für mehr Cyber-Sicherheit.

Technologie durchdringt mittlerweile jeden Arbeits- und Unternehmensbereich. Sie ermöglicht, unterstützt und beschleunigt jeden Prozess. Diese digitale Durchdringung ist so fortgeschritten, dass der Geschäftserfolg von Unternehmen unmittelbar von der Sicherheit der eingesetzten Technologien abhängt. Durch IoT und weitere Applikationen, Anwendungen, Software und Hardware wird das Arbeiten effizienter – die Angriffsfläche von Unternehmen für Cyber-Attacken aber auch immer größer. So ist es nicht verwunderlich, dass das World Economic Forum Cyber-Angriffe zu den Top 3 der weltweit größten Risiken zählt. Auch die Studie zu Cyber-Attacken und IT-Sicherheit im Jahr 2025, eine Expertenbefragung zu den Zukunftstrends und -herausforderungen der IT-Sicherheit von RadarServices, unterstreicht dieses Risiko. So werden nach Meinung der Experten des Wiener Cyber-Security-Unternehmens Angriffe in Zukunft dramatisch ansteigen.



Die International Data Corporation (IDC) erwartet, dass 74 % der Unternehmen im Laufe des Jahres gehackt werden. Mit der eigens entwickelten Cybersecurity Detection Technologie beobachtet RadarServices diesen dramatischen Anstieg jeden Tag in seinem 600 Quadratmeter großen Security Operation Center, kurz SOC genannt, in Wien. In dem ausgebauten und sich auf mittlerweile zwei Stockwerken erstreckenden SOC werden Datenmengen von 933 Petabyte pro Jahr verarbeitet (1 Petabyte = 1.000 Terrabyte).

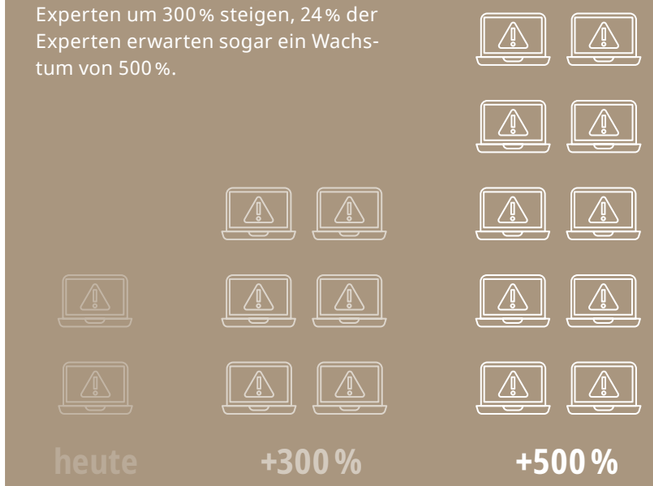
IT-Sicherheit ist für viele Unternehmen zum zentralen Thema geworden und dementsprechend auch schon in den Chefetagen angekommen. Für Geschäftsführer und IT-Abteilungen bringen neue Möglichkeiten auch neue Risiken mit sich. Die stetig steigende Zahl an Systemen, Geräten und Datenaufkommen erschwert die Übersicht und gleichzeitig auch den Schutz in Unternehmen erheblich. Mit dem digitalen Fußabdruck in internen und externen Netzwerken sowie Datenbanken vergrößert sich die Angriffsfläche für Cyber-Angriffe. Fehlendes Patchmanagement und fehlendes Bewusstsein im Bereich Sicherheit und Angriffsszenarien sind die größten Risiken, die von den IT-Experten von RadarServices 2018 beobachtet wurden.

So können Unternehmen Reputationsverlust vermeiden

Es gibt aber auch gute Nachrichten zu vermelden: Denn zur effizienten Verbesserung der Cyber-Security gilt es laut RadarServices einige grundlegende Aspekte und Maßnahmen umzusetzen, die die Sicherheit von Firmen deutlich verbessern. Wer diese beachtet und die entsprechende Vorkehrungen trifft, kann Risiken und Schäden, wie zum Beispiel Reputationsverlust, drastisch minimieren. Dann dürfen Unternehmen auch in Zukunft auf Vertrauen und Glaubwürdigkeit von Kunden als auch Partnern bauen. Damit Firmen ihre IT-Sicherheit im Jahr 2019 gezielt vorantreiben können, haben die IT-Experten von RadarServices zehn praxisorientierte Anwendungstipps für mehr Cyber-Security im Unternehmen zusammengestellt. Diese finden Sie in unten stehender Grafik. ■

Cyber-Attacken werden dramatisch steigen

Pro Jahr werden die Angriffe laut Experten um 300 % steigen, 24 % der Experten erwarten sogar ein Wachstum von 500 %.



Die Top-10-Tipps für mehr Cyber-Security von den RadarServices-Experten

1. Kontinuierliches IT-Monitoring und Risk Detection sämtlicher Systeme
2. Überblick über Systeme und Berechtigungen verschaffen (IT, OT, IoT, IIoT)
3. Etablierung Patchmanagement und -zyklen
4. Umfassende Sicherheitsstrategie samt Verantwortlichkeiten und deren regelmäßige Überprüfung
5. Eingesetzte Technologie entsprechend und korrekt konfigurieren
6. Schwachstellen erkennen und umgehend schließen
7. Datensicherungskonzept sowie Datenschutzerklärung (für Mitarbeiter, Partner und Dienstleister) sowie Zutrittskontrolle
8. Geschäfts- und Kundendaten regelmäßig sichern – denn diese Daten alleine können von großem Wert für Unternehmen sein
9. Sichere Entsorgung von Informationen (Papier und Datenträger)
10. Multi-Faktor-Authentifizierung und Verschlüsselung der Daten und Kommunikation

Veranstaltungen

Branchentreffen: Risikomanagement für die Automobilzulieferindustrie

Zulieferer in der Autoindustrie müssen umdenken, denn Endverbraucher wollen künftig immer flexibler und nachhaltiger unterwegs sein. Die Folge: Wertschöpfungskette und Risikomanagement müssen neu und ganzheitlich gedacht werden. Das Branchentreffen, organisiert von Funk Risk Consulting und dem Cluster Automotive des Netzwerks Bayern Innovativ, stellt die Herausforderungen der Branche in den Fokus. Die Redner thematisieren zum Beispiel Betriebsunterbrechungen oder Standortrisiken und geben Einblicke in die Praxis.

» 2. Juli 2019 in Nürnberg

it-sa: Fachmesse für IT Security

Ob Top-Themen wie Cloud Security und Biometrie oder Basis-Informationen zum Virenschutz: Auf der it-sa 2019 dreht sich alles um das Thema IT-Sicherheit. Auch Funk ist dieses Jahr gemeinsam mit Kooperationspartner RadarServices vor Ort – schauen Sie vorbei!

» 8. bis 10. Oktober 2019 in Nürnberg

Funk organisiert regelmäßig Veranstaltungen zu aktuellen Fachthemen. Auf der Website (s. u.) sehen Sie die aktuellen Termine.

Das Funk-Team am Cyber-Day: Friederike Burkhardt, Ulrike Meyer, Michael Winte, Alexandra Köttgen (von links).

Rückblick: Funk-Experten auf der Hannover Messe vor Ort

Die Hannover Messe ist die weltgrößte Industriemesse und präsentiert aktuelle Trends und Innovationen. Funk war in diesem Jahr dabei und stellte den Besuchern im persönlichen Gespräch aktuelle Risikolösungen vor, zum Beispiel Versicherungsschutz für Cyber-Attacken und die neue entwickelte Risikomanagementsoftware RIMIKS X.0.

Zweitägiges Best-Practise-Seminar zum Risikomanagement

Die Steuerung von Risiken ist eine der Kernaufgaben jedes Unternehmers. Das ist eine komplexe Angelegenheit, denn die Risikolandschaft ist volatil. Besonders Risiken aus den Themenbereichen Cyber, Compliance und Supply-Chain stellen Unternehmen heutzutage vor große Herausforderungen. Kennen Sie bereits die Risikotragkraft Ihres Unternehmens? Im Rahmen unseres zweitägigen Seminars lernen Sie den Aufbau und die Elemente des Risikomanagement-Prozesses kennen.

» 12. bis 13. September 2019 in München

Ihre Ansprechpartnerin:
Ulrike Meyer
u.meyer@funk-gruppe.de

Anmeldung unter:
funk-gruppe.com/veranstaltungen

Webinare

Cyber-Risiken im Fokus

Die Informations- und Kommunikationstechnik hat sich in den vergangenen Jahrzehnten rasant verdichtet und weiterentwickelt. Damit einher gehen Cyber-Risiken, die teilweise schneller entstehen, als Vorschriften und IT-Abteilungen darauf reagieren können. Wir informieren Sie über Schutzmöglichkeiten, wie zum Beispiel detaillierte Risikoanalysen und maßgeschneiderte Bewältigungskonzepte.

» 17. Oktober 2019

Betriebsunterbrechungsanalyse

Eine Störung der Lieferkette und die daraus resultierende Betriebsunterbrechung kann schnell dramatische Folgen haben, etwa Produktionsstillstand, Umsatzeinbrüche, Kundenverlust und Imageschäden. Das kann schnell zur existenziellen Bedrohung werden. In unserem Webinar erfahren Sie, wie die Risiken entlang der Wertschöpfungskette analysiert, bewertet und gesteuert werden.

» 28. August oder 20. November 2019

Business Continuity Management

Ob der Ausfall eines Lieferanten, ein Maschinenschaden oder ein Großbrand im Warenlager – wenn der Geschäftsbetrieb eines Unternehmens maßgeblich gestört ist, muss gehandelt werden. Für Überlegungen bleibt keine Zeit, Entscheidungen müssen schnell getroffen werden. Worauf Sie achten sollten und was die ersten Schritte sind, möchten wir Ihnen anhand verschiedener Praxisbeispiele aufzeigen.

» 11. Juni, 10. September oder 12. Dezember 2019

Versicherungsvergleichsportal proMIT

Mit dem Versicherungsvergleichsportal proMIT erhalten Mitarbeiter, Mitglieder und Mieter Informationen über Versicherungen, können Bedingungen vergleichen, Verträge direkt online abschließen und Schäden melden. Funk bietet in vielen Sparten besondere Bedingungen und Sondertarife. Das Portal lässt sich dabei problemlos in Ihr Intranet integrieren. Im Webinar können Sie einen Blick in das Vergleichsportal werfen und erhalten Informationen zu speziellen Serviceleistungen.

» 12. September oder 14. November 2019

Risikomanagement-Systeme

Das Thema Risikomanagement gewinnt für Unternehmen fortlaufend an Bedeutung. Neben formalen Anforderungen und hieraus resultierenden Haftungstatbeständen für die Geschäftsführung spielen auch Forderungen von Kapitalgebern, Zulieferern und Kunden eine zunehmende Rolle. Hier erfahren Sie, wie Sie Krisen vorbeugen können, indem Sie ein Risikomanagement-System implementieren.

» 22. August oder 7. November 2019

Management von politischen Risiken

Die internationalen politischen Verhältnisse sind unberechenbarer geworden. Geschäftsbeziehungen mit Unternehmen aus gefährdeten Regionen oder Ländern bergen daher viele Risiken. So können zum Beispiel umstürzende Machtverhältnisse Investitionen bedrohen. Im Webinar lernen Sie das Gefahrenpotenzial von politischen Risiken kennen sowie den ganzheitlichen Beratungsansatz von Funk Risk Consulting.

» 8. Oktober 2019

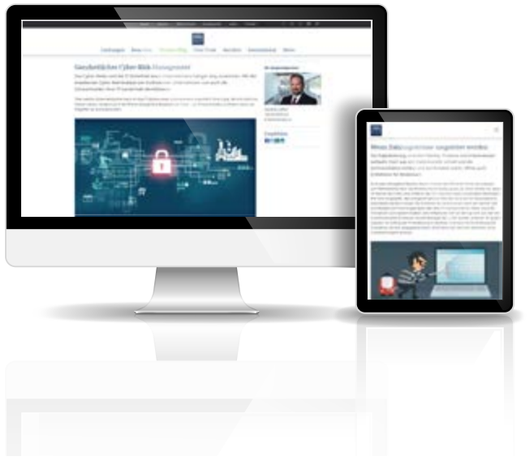
Ihre Ansprechpartnerin:
Diana Gelwer
d.gelwer@funk-gruppe.de

Anmeldung unter:
funk-gruppe.com/webinare

Mehr Informationen zu Cyber-Themen

Cyber-Broschüre

Alle Infos auf einen Blick: Welche Arten von cyberbedingten Vorfällen es gibt, welche Auswirkungen Cyber-Risiken haben und was Funk CyberSecure alles für Ihr Unternehmen leistet, steht übersichtlich zusammengefasst in unserer Cyber-Broschüre. Fragen Sie gern Ihren Kundenberater nach einem Exemplar oder kontaktieren Sie einen unserer Experten (siehe rechts).



News auf der Webseite

Sie lesen lieber digital? Auf unserer Webseite finden Sie spannende Inhalte, die laufend aktualisiert werden. Dort können Sie sich auch für einen unserer informativen Newsletter anmelden – damit Sie in Zukunft keine Entwicklungen rund um Cyber-Versicherungen mehr verpassen.

Artikel zu Cyber:
funk-gruppe.de/cyber

Videos unserer Experten

Unsere Cyber-Experten beziehen auch gern vor der Kamera Stellung. In zwei kurzen Videos gewinnen Sie einen guten Einblick in Cyber-Risiken. Ideal, um z. B. den Chef auf das Thema aufmerksam zu machen.

Filme in der Funk Mediathek:
funk-gruppe.de/filme

Kontaktieren Sie unsere Cyber-Experten

Deutschland

Hendrik F. Löffler
Mitglied der Funk Geschäftsleitung der Funk Gruppe
und Geschäftsführer Funk Risk Consulting
fon +49 40 35914-642
h.loeffler@funk-gruppe.de

Michael Winte
Fachbereichsleiter Cyber, Technology & Crime
fon +49 40 35914-582
m.winte@funk-gruppe.de

Philipp Seebohm
ISMS Lead Auditor nach ISO 27001
fon +49 40 35914-949
p.seebohm@funk-gruppe.de

Österreich

Mario Heinisch
Geschäftsführer/CEO Funk International Austria
fon +43 15 89 10 202
m.heinisch@funk-austria.com

Gabriele Zsitek
Leiterin Broking/Financial Lines Funk International Austria
fon +43 15 89 10 219
g.zsitek@funk-austria.com

Schweiz und Liechtenstein

Max Keller
Lead RiskLab Funk Insurance Brokers
fon +41 58 311 05 51
max.keller@funk-gruppe.ch

Funk-Zeichen

Impressum

Herausgeber
Funk Gruppe
Valentinskamp 20, 20354 Hamburg
Fon +49 40 35914-0

Redaktion
Dr. Anja Funk-Münchmeyer (v. i. S. d. P.),
Larissa Schier, Sarah Seyfried, Ansgar Vaut

Kontakt
Über Anregungen, Hinweise oder den Wunsch nach weiteren Informationen freuen wir uns. Wenden Sie sich bitte an Sarah Seyfried (s.seyfried@funk-gruppe.de)

Grafik
Carolin Krüger, Hauke Kaden

Druckerei
MOD Offsetdruck GmbH
Gewerbestraße 3, 23942 Dassow
Auflage: 13.800 Exemplare

Bildnachweise
Jakob Boerner (S. 3, 20), Dirk Meissner Cartoons (S. 50), stock.adobe.com: adimas (S. 1, 18), artinspiring (S. 4, 14), SFIO CRACHO (S. 4, 10, 12), Joerg Huettenhoelscher (S. 5, 28), Maridav (S. 5, 34), AndSus (S. 6), Rostislav (S. 7), irinastrel123 (S. 8, 9), Gorodenkoff Productions OU (S. 16), Jacob Ammentorp Lund (S. 22, 23), mavoimages (S. 24), yellowj (S. 24), pressmaster (S. 24), Drobot Dean (S. 25), 2017 Phive Imaging Studio (S. 27), 騰龙 郭 (S. 31), NWM (S. 32), David Crockett (S. 36, 38), Anja Kaiser (40, 41), seventyfour (S. 42), Maksim Pasko (S. 48), indysystem (S. 48), sidop (S. 52). Funk (Rest)

Funk in den digitalen Medien

Die letzte Seite im Heft ist die erste im Netz. Das digitale Angebot von Funk hält Sie auf dem Laufenden – jederzeit und überall! In unserem Themen-Blog finden Sie aktuelle Beiträge aus den Bereichen Versicherungsmanagement, Vorsorge, Risikomanagement, Karriere, Internationales und Mittelstand.

funk-gruppe.com

Wofür steht Funk? Was bedeutet „die beste Empfehlung“? Kundenzitate und Praxisbeispiele geben einen unmittelbaren Einblick in die Zusammenarbeit mit Funk. Klicken Sie rein unter:

die-beste-empfehlung.com

Unsere Vision. Unsere Mission. Erfahren Sie mehr über unsere Strategie:

strategie.funk-gruppe.com

Abonnieren Sie unsere Newsletter:

funk-gruppe.com/newsletter

Die beste Empfehlung. Funk.

Durchstarten in die Zukunft
Innovationsmanagement bei Funk

In Zeiten des raschen Wandels von Märkten und sich ändernder Risiken wie auch Chancen entwickelt Funk innovative Risikolösungen für Unternehmen.

Mehr zum Thema: funk-gruppe.com/innovationen