Korruption, Kartelle und Schwarzarbeit

Nachricht vom 06.09.2019

Eine Unternehmensbefragung des Instituts der deutschen Wirtschaft hat sich mit der Frage beschäftigt, welche Einbußen die deutsche Wirtschaft aufgrund von Korruption, Kartellen und Schwarzarbeit erleidet.

Bestechungsvorwürfe, illegale Beschäftigung und Preisabsprachen schaden der nationalen Wirtschaft – denn einerseits schädigen sie langfristig das Grundvertrauen der Bürger in die Unabhängigkeit, Unbestechlichkeit und Handlungsfähigkeit des Staates bzw. die Integrität der Wirtschaft. Andererseits sorgen diese Wirtschaftsdelikte aber auch für unmittelbare monetäre Verluste, die im Mittelpunkt der Studie standen.

Einschätzung der Schwarzarbeit
Ca. die Hälfte der befragten Unternehmen leidet überhaupt nicht unter Schwarzarbeit: 49,5 Prozent gaben an, dass ihrem Unternehmen kein Umsatz durch die Schwarzarbeit der Konkurrenz verloren geht. Im Durchschnitt liegt die Zahl jedoch bei ca. 4,7 Prozent. Vor allem Unternehmen der Baubranche klagten über die illegale Konkurrenz. Verglichen mit Korruption und unerlaubten Absprachen verursacht Schwarzarbeit allerdings noch die geringsten Umsatzeinbußen.

Einschätzung von Kartellen und Korruption
Keine Probleme mit Preisabsprachen oder Bestechung der Konkurrenten haben nach eigenen Angaben rund ein Drittel der befragten Unternehmen. Umsatzverluste bis zu zehn Prozent durch Korruption befürchtet knapp die Hälfte der Unternehmen; durch verbotene Kartellbildung knapp 40 Prozent. Weitere jeweils 15 Prozent der Betriebe beziffern ihre Umsatzverluste durch unerlaubte Geschenke oder Absprachen auf bis zu 30 Prozent.

Unternehmen mit mehr als 250 Mitarbeitern leiden hierbei deutlich mehr unter der illegalen Kartellbildung und Korruption als kleinere. Drei von vier Großunternehmen gehen von Erlöseinbußen zwischen einem und 30 Prozent durch Bestechung und/oder Preis- und Mengenabsprachen aus.

Schaden nach Branchen
Am meisten von Schwarzarbeit (Durchschnitt: 9,1 Prozent Umsatzverlust), Korruption (8,7 Prozent) und Kartellabsprachen (7,7 Prozent) betroffen ist laut Umfrage die Baubranche, während sich die Industrie nur überdurchschnittlich stark mit Bestechung auseinandersetzen muss.

Auswirkungen auf den Umsatz
Die in der Umfrage erfassten Branchen erwirtschafteten 2017 einen Umsatz von 5,4 Billionen Euro (Statistisches Bundesamt, 2018). Der Umsatzverlust durch Korruption in diesen Branchen beträgt 6,2 Prozent. Dies entspricht Umsatzeinbußen von rund 335 Milliarden Euro jährlich. Der Umsatzverlust durch Schwarzarbeit lag schätzungsweise bei rund 4,7 Prozent (254 Mrd. Euro) im Jahr 2017 für die untersuchten Branchen. Am gravierendsten werden die Schäden durch Kartelle eingeschätzt. Es werden Umsatzeinbußen in Höhe von durchschnittlich 7,1 Prozent befürchtet und damit insgesamt von 383 Mrd. Euro jährlich für die befragten Branchen. Zusammengenommen werden basierend auf diesen unternehmenseigenen Schätzungen durch die Delikte durchschnittlich 18 Prozent weniger Umsätze legal erzielt.

Die gesamte Studie können Sie hier [1] herunterladen.

Quellen

[1] https://www.iwkoeln.de/fileadmin/user_upload/Studien/Kurzberichte/PDF/2019/IW-Kurzbericht-2019_Wirtschaftskriminalitaet.pdf

Radieschen, Schokolade und Compliance

Nachricht vom 30.08.2019

Werden Sie schwach bei Schokolade? Oder eher bei Radieschen? Mit der Bedeutung der Willenskraft für die Compliance hat sich Thomas Schneider in seinem neuen Beitrag der Serie „Compliance anders" auseinandergesetzt.

Tests sind notwendig, um theoretische Überlegungen in der Realität zu überprüfen. Allerdings können sie für die Teilnehmer auch durchaus unangenehm sein. In einem Versuch (s. hierzu Baumeister/Tierney: Die Macht der Disziplin, 2012, S. 31–33) durften die Versuchsteilnehmer einen ganzen Tag lang nichts essen und kamen entsprechend hungrig in den Versuchsraum. Vor ihnen standen drei Schlüsseln mit verschiedenem Inhalt: ofenwarme Plätzchen, Schokolade und Radieschen.

Willenskraft ist gefragt
Einige Testteilnehmer durften die Plätzchen essen, andere die Schokolade, eine weitere Gruppe musste mit den Radieschen vorlieb nehmen. Letzeres fiel auch deshalb besonders schwer, weil die Teilnehmer einige Zeit alleine im Raum blieben und die Radieschen-Esser Plätzchen und Schokolade betrachten mussten, ohne zugreifen zu dürfen. Es gelang den Teilnehmern, der Versuchung zu widerstehen. Dass dazu aber erhebliche Willenskraft erforderlich war, bedarf keiner weiteren Erläuterung.

Anschließend wurden alle Testteilnehmer in einen anderen Raum gebracht und aufgefordert, eine Geometrieaufgabe zu lösen, die in Wahrheit unlösbar war. Ein geeigneter Test, um die Ausdauer eines Menschen zuverlässig zu ermitteln. Diejenigen, die Plätzchen oder Schokolade essen durften, versuchten sich zwanzig Minuten an den Aufgaben, die Radieschenesser dagegen nur acht Minuten lang, also weniger als die Hälfte. Der Grund war vermutlich relativ einfach: Sie hatten ihre Willenskraft bereits in großem Maße dazu eingesetzt, den Plätzchen und der Schokolade zu widerstehen. Willenskraft ist keine statische, sondern eine dynamische Größe, welche sich wie ein Muskel erschöpfen kann.

Empfehlungen für die Compliance
Die Empfehlung, die die Compliance hieraus an ihre Ansprechpartner generiert, ist einfach: Treffen Sie keine Compliancerelevanten Entscheidungen, wenn ihre Willenskraft geschwächt ist. Besser ein wenig zögern und am nächsten Morgen entscheiden, als nach einem stressigen Arbeitstag einen vielleicht verhängnisvollen Fehler zu begehen, bei dem sich im Nachhinein nicht nur der Betroffene fragt, wie es dazu kommen konnte.

- Teil 1: Compliance Officer: Fortune müssen sie haben! [1]
- Teil 2: Nur wenn gesprochen wird, wird der offene Dialog zur Routine [2]
- Teil 3: Wenn der Kollege Marotten zeigt [3]
- Teil 4: Mit Empathie mehr erfahren [4]
- Teil 5: Einordnung von Gerüchten in der Compliance [5]
- Teil 6: Konkretisierung von Gerüchten in der Compliance [6]
- Teil 7: Macht und Moral [7]
- Teil 8: Das Nutella-Prinzip [8]
- Teil 9: Kreativität und Standardlösungen [9]
- Teil 10: Netzwerke der Compliance [10]
- Teil 11: Neue Wege gehen [11]
- Teil 12: Der Anteil des Glücks am Erfolg [12]

Thomas Schneider

Quellen

[1] https://www.compliancedigital.de/ce/compliance-officer-fortune-muessen-sie-haben/detail.html
[2] https://www.compliancedigital.de/ce/nur-wenn-gesprochen-wird-wird-der-offene-dialog-zur-routine/detail.html
[3] https://www.compliancedigital.de/ce/wenn-der-kollege-marotten-zeigt/detail.html
[4] https://www.compliancedigital.de/ce/mit-empathie-mehr-erfahren/detail.html
[5] https://www.compliancedigital.de/ce/einordnung-von-geruechten-in-der-compliance/detail.html
[6] https://www.compliancedigital.de/ce/konkretisierung-von-geruechten-in-der-compliance-2/detail.html
[7] https://www.compliancedigital.de/ce/macht-und-moral/detail.html
[8] https://www.compliancedigital.de/ce/das-nutella-prinzip/detail.html
[9] https://www.compliancedigital.de/ce/kreativitaet-und-standardloesungen/detail.html
[10] https://compliancedigital.de/ce/netzwerke-der-compliance/detail.html
[11] https://compliancedigital.de/ce/neue-wege-gehen-1/detail.html
[12] https://www.compliancedigital.de/ce/der-anteil-des-gluecks-am-erfolg/detail.html

Cybersicherheit unterstützt von Künstlicher Intelligenz

Nachricht vom 29.08.2019

Das Internetzeitalter schreitet voran, und immer mehr Unternehmen setzen auf Künstliche Intelligenz, um die Sicherheit vor Angriffen aus dem Cyberspace zu erhöhen.

Viele Unternehmen setzen vermehrt auf Künstliche Intelligenz (KI), um die Produktivität und den Umsatz zu steigern oder die Erlebnisqualität zu verbessern. Zunehmend bedienen sie sich auch der KI, um die Sicherheit vor Angriffen aus dem Cyberspace zu erhöhen, denn mit der Anzahl der Einfallstore wächst auch die Gefahr. In der Studie Reinventing Cybersecurity with Artificial Intelligence [1] hat das Capgemini Research Institute 850 Führungskräfte aus den Bereichen IT-Informationssicherheit, Cybersicherheit und IT-Betrieb in sieben Branchen und aus zehn Ländern befragt, sowie vertiefende Gespräche mit Branchenexperten und Wissenschaftlern geführt.

KI ist Notwendigkeit

Die Ergebnisse der Studie sind eindeutig: Die befragten Unternehmen halten es für zunehmend notwendig, die Cybersicherheit mit KI zu stärken – 69 Prozent der Unternehmen glauben nicht daran, dass sie kritische Bedrohungen ohne KI identifizieren können. Insbesondere Telekom- und Konsumgüterhersteller (80 bzw. 78 Prozent) zählen auf die KI, um Bedrohungen zu identifizieren und Angriffe zu vereiteln. Versorger und Versicherer (mit 59 bzw. 61 Prozent) haben den geringsten, aber immer noch hohen Zustimmungswert. Diese Zahlen stimmen mit dem geschätzten Schaden überein, den Unternehmen in der jeweiligen Branche bereits erlitten haben – Spitzenreiter waren Telekommunikationsdienstleister vor den Konsumgüterherstellern, während Versichererer und Versorger am Ende des Rankings rangieren.

Nutzen nach Anwendungsart und Tempo der Einführung

Den höchsten Nutzen beim Einsatz von KI versprechen sich die Unternehmen laut Studie bei der Entdeckung von Cyber-Angriffen. 51 Prozent sehen hier einen hohen Nutzen. Während die Mehrheit der Unternehmen der Prävention einen mittleren Nutzen zuspricht, beurteilen die Unternehmen die Reaktionsmöglichkeiten durch KI zu 35 Prozent mit einem geringen Nutzen.

Und das Tempo bei der Einführung von KI in der Cybersicherheit steigt – fast drei Viertel der Unternehmen testen KI bereits in konkreten Anwendungsfällen. Sie erkennen dabei einen starken Geschäftsnutzen – denn drei von fünf Unternehmen gaben an, dass der Einsatz von KI die Präzision und Effizienz der Cyberanalysten erhöht.

Quellen

[1] https://www.capgemini.com/de-de/wp-content/uploads/sites/5/2019/07/Report_AI_in_Cybersecurity_Capgemini_Research_Institute.pdf

Weber: „Compliance ist in vielen Hochschulen ein Thema“

Nachricht vom 23.08.2019

Compliance gewinnt für Hochschulen, Universitäten und außeruniversitäre Forschungseinrichtungen stetig an Relevanz. Welchen besonderen Herausforderungen diese bei der Einführung von Compliance Management Systemen gegenüberstehen und welchen Compliance-Risiken sie begegnen, darüber gaben Prof. Dr. Beatrix Weber und Dr. Stefanie Lejeune der ESV-Redaktion im Interview Auskunft.

Sie haben ein Buch über Compliance in Hochschulen, Universitäten und außeruniversitären Forschungseinrichtungen geschrieben. Vor welchen besonderen Herausforderungen stehen diese Institutionen bei der Einführung von Compliance Management Systemen?

Beatrix Weber: Hochschulen für angewandte Wissenschaften und Universitäten sind einerseits Behörden, die mit hoheitlichen Aufgaben wie der Prüfungsdurchführung betraut sind. Andererseits stehen sie in verschiedenen Märkten wie dem der Forschungsdienstleistungen im Wettbewerb mit anderen Hochschulen. Als „Wissenschaftsbetriebe“ sind sie hybride Organisationen, die in ihrer Compliance-Struktur die verwaltungsrechtlichen Verfahren wie auch risikoorientierte Prozesse abbilden müssen.

Die außeruniversitären Forschungseinrichtungen sind in der Regel als eingetragene Vereine organisiert. Damit unterfallen sie bei wirtschaftlicher Tätigkeit an sich den Compliance-Strukturen wie Unternehmen. Als Empfänger öffentlicher Förderung sind sie aber zur Einhaltung der öffentlich-rechtlichen Vorgaben verpflichtet und damit auch beispielsweise Prüfgegenstand der Rechnungshöfe.

Inwiefern unterscheiden Sie sich von Unternehmen?

Beatrix Weber: Unternehmen dienen primär der Gewinnerzielung. Hochschulen haben die gesetzlichen Aufgaben von Lehre, Forschung, Weiterbildung und Wissenstransfer. Sie sind an Recht und Gesetz durch die Verfassung gebunden und den Grundsätzen der Wirtschaftlichkeit und Sparsamkeit verpflichtet. Der Spielraum zum Eingehen von Risiken im Rahmen von Compliance als rechtlichem Risikomanagement ist daher deutlich geringer als in Unternehmen.

Wie weit sind die Hochschulen bereits allgemein bei der Einhaltung von Compliance?

Beatrix Weber: Es gibt wenig verlässliche Zahlen hierzu. Eine Untersuchung im Jahr 2015 hat gezeigt, dass Compliance in vielen Hochschulen ein Thema ist, aber nur wenige konkrete Umsetzungsschritte für ein strukturiertes Compliance Management System ergreifen. Positive Ausnahmen gibt es immer: Zu nennen ist hier die TUM, das KIT und natürlich die Hochschule für Angewandte Wissenschaften Hof. Bei den außeruniversitären Forschungseinrichtungen tritt die Fraunhofer Gesellschaft positiv hervor, die sich nach dem freiwilligen Prüfstandard IDW PS 980 prüfen lässt. Sehr viel Know-how und Compliance-Aktivitäten verzeichnet trotz vieler einzelner Verwerfungen auch die Max-Planck-Gesellschaft, was nicht zuletzt auf ihren außerordentlich kompetenten Compliance-Beauftragten zurückzuführen ist.

In welchen Bereichen sehen Sie besonderen Nachholbedarf?

Beatrix Weber: Das Beispiel Max-Planck-Gesellschaft hat gezeigt, dass wir die Risikomanagementsysteme für Hochschulen und außeruniversitäre Forschungseinrichtungen ganzheitlich betrachten müssen. Technische, wirtschaftliche und rechtliche Risiken greifen ineinander. Die Verantwortung liegt bei den Hochschulen und Einrichtungen selbst. Die Wissenschaftsministerien haben sich im Zuge des New Public Management zugunsten der Eigenverantwortung und Selbststeuerung der Hochschulen weit zurückgezogen. Daher sind die Hochschulen selbst aufgerufen, Compliance Management Systeme aufzubauen und kompetente Compliance-Verantwortliche zu benennen. Zum anderen ist die Einrichtung eines internen Kontrollsystems sowie einer unabhängigen Internen Revision unabdingbar. Hier haben sehr viele Hochschulen, große und kleine, deutlichen Nachholbedarf. Neben einer unabhängigen Innenrevision ist die Rolle von externen, unabhängigen Prüforganen nicht zu unterschätzen. Den Rechnungshöfen kommt dabei eine wichtige Funktion zu. Im Zusammenspiel mit der Rechtsaufsicht durch die zuständigen Wissenschaftsministerien könnten sie Garant für eine unabhängige Prüfung werden, deren Empfehlungen an Hochschulen und die Rechtsaufsicht ein besonderes Gewicht zukommt.

Welchen Risiken sind Hochschulen insbesondere ausgesetzt?

Stefanie Lejeune: Neben den strategischen und politischen Risiken sind es vor allem operative Risiken, mit denen sich Hochschulen und außeruniversitäre Forschungseinrichtungen auseinandersetzen müssen. Man unterscheidet in der Risikokategorie der operativen Risiken verschiedene Risikoarten, wie Prozess-, Projekt-, technologische, soziale oder finanzielle Risiken, die unter dem Gesichtspunkt von Ursache und Wirkung untereinander in vielfältige Wechselbeziehungen treten können. Das komplexe, da hybride System von Hochschulen und außeruniversitären Forschungseinrichtungen lässt sich am besten über Risikofelder abbilden. Typische, aber keineswegs ausschließliche Risikofelder einer Hochschule sind das Beschaffungs- und Vergabewesen, das IT-Wesen, insbesondere Datenschutz und Datensicherheit, das Personalwesen, insbesondere Bewerbungsverfahren, sowohl von Lehrenden als auch Studierenden, die Abnahme von Prüfungen und Gewährung akademischer Abschlüsse, das Haushaltswesen, die Mittelbeschaffung, die Drittmittel und das Allgemeine Betriebswesen.

Welche Organe der Hochschulverwaltung tragen eine besondere Verantwortung für die Compliance?

Beatrix Weber: Compliance Management Systeme fügen sich weder in die klassischen Strukturen der akademischen Selbstverwaltung noch in die weisungsgeprägten Verwaltungshierarchien ein. Wissenschafts- und insbesondere Forschungsprozesse sind auf Offenheit, Kommunikation auf Augenhöhe und Inhaltsorientierung angelegt. Compliance in Hochschulen muss also neue Wege der Zusammenarbeit jenseits der althergebrachten Schranken gehen. Der Hochschulleitung und ihrer Präsidentin oder ihrem Präsidenten kommt für die Compliance-Kultur in einer Hochschule eine entscheidende Bedeutung zu. Compliance ist Leitungsaufgabe. Die Delegation an eine Compliance-Beauftragte oder einen Compliance-Beauftragten sollte im Sinne der Best Practice als Stabsstelle zur Präsidentin bzw. zum Präsidenten erfolgen. Andererseits geht Compliance alle an. Und: Compliance ist Change Management. Compliance-Richtlinien und Prozesse sollten daher in gemeinsamen Projekten von Forschung, Lehre und Verwaltung erarbeitet und schlussendlich von der Hochschulleitung beschlossen werden.

Hinweisgebersysteme sind ein wesentlicher Bestandteil von Compliance Management Systemen. Welche relevanten Punkte zur Gestaltung haben Hochschulen zu berücksichtigen?

Stefanie Lejeune: Die Hochschule und außeruniversitäre Forschungseinrichtung muss zunächst entscheiden, ob sie ein personalisiertes Hinweisgebersystem – mittels einer oder eines internen Compliance-Beauftragten sowie externen Ombudsperson – oder ein elektronisches Hinweisgebersystem – telefonische Hotline, Voicemail oder internetbasiert – implementieren oder beide Systeme miteinander verbinden möchte. Sie muss festlegen, welche rechtlichen Verfehlungen – ob nur bestimmte oder alle Straftatbestände, auch untergesetzliche Regelverstöße – gemeldet werden sollen oder – von den Beschäftigten – sogar gemeldet werden müssen. Und wie die Kommunikationskanäle

laufen sollen und welche Kommunikationswege potentiellen Hinweisgebern zur Verfügung stehen. Das Thema Anonymitätsschutz für potentielle Hinweisgeber muss ebenso geklärt werden wie der Kreis potentieller Hinweisgeber. Sollen nur Beschäftigte oder Studierende Hinweise geben dürfen oder alle, die irgendeinen Bezugspunkt zur Hochschule haben?

Muss jede Hochschule ein Hinweisgebersystem einrichten?

Stefanie Lejeune: Abgesehen vom Geldwäschegesetz und Kreditwesengesetz gibt es in Deutschland aktuell noch keine rechtliche Pflicht, ein Hinweisgebersystem zu implementieren. Allerdings haben die EU Kommission und der Rat im März 2019 einen einheitlichen Schutz für Whistleblower in der ganzen EU beschlossen und darin auch bestimmt, dass private wie öffentlich-rechtliche Institutionen, so auch Hochschulen, klare und sichere Meldekanäle für potentielle Hinweisgeber zur Verfügung stellen müssen. Es ist zu erwarten, dass dieser Beschluss auch für die Mitgliedstaaten der EU Wirkung zeigen wird. Dann steht für jede Hochschule, größere und kleinere, nicht mehr die Frage im Raum, ob sie ein Hinweisgebersystem implementieren will, sondern wie dieses konkret aussehen wird. Doch bereits jetzt empfiehlt sich im Hinblick auf das hohe Dunkelfeld von Korruptionsdelikten und anderen, nur schwer erkennbaren Verfehlungen die Zurverfügungstellung eines Hinweisgebersystems.

Welche rechtlichen Anforderungen sind für die Einrichtung eines Hinweisgebersystems besonders zu berücksichtigen?

Stefanie Lejeune: Da Hinweise nur dann relevant sein können, wenn die Hinweisgeberin bzw. der Hinweisgeber detaillierte Informationen über handelnde Personen geben kann, setzt das Datenschutzrecht klare Grenzen für die Implementierung und die Anwendung von Hinweisgebersystemen. Regelmäßig werden personenbezogene Daten von der Hinweisgeberin oder dem Hinweisgeber übermittelt bzw. im anschließenden internen Ermittlungsverfahren im Sinne der DSGVO verarbeitet. Das ist nur möglich mit dem Einverständnis der Betroffenen oder aufgrund einer ausdrücklichen gesetzlichen Grundlage, wie etwa § 26 Abs. 1 S. 2 BDSG. Auch die Auswahl einer externen Ombudsperson bzw. eines Kooperationspartners, der etwa ein internetbasiertes Hinweisgebersystem zur Verfügung stellt, muss datenschutzrechtlichen Anforderungen genügen.

Das Einwerben von Drittmitteln wird für Hochschulen, Universitäten und außeruniversitäre Forschungseinrichtungen immer wichtiger. Welche Compliance-Anforderungen sind dabei insbesondere zu beachten?

Beatrix Weber: Die Mittel für Forschung der Hochschulen sind in den letzten Jahren nicht gesunken. Gleichzeitig zieht sich der Staat aber immer mehr aus der Finanzierung zurück, d.h. der Anteil von einzuwerbenden Drittmitteln steigt immer weiter und damit auch der Wettbewerb um die verfügbaren Mittel. Das Vergabe-und Beihilferecht sowie das Rechte- und Datenmanagement werden immer komplexer. Alle forschenden Kolleginnen und Kollegen verdienen mit persönlichen und sachlichen Ressourcen ausreichend ausgestattete Transfer- oder Drittmittelstellen, die sie beim Einwerben der Mittel rechtlich und ökonomisch kompetent unterstützen. Ziel ist, einen wissenschaftsadäquaten Prozess zu gestalten, der die Forschungsfreiheit der Wissenschaftler schützt, die rechtlichen Vorgaben beachtet und Risiken für die Hochschule einbezieht und bewertet.

Zu den Personen

Prof. Dr. Beatrix Weber, MLE, beschäftigt sich mit Compliance in der Hochschulpraxis, Forschung und Lehre. Sie ist Professorin für Gewerblichen Rechtsschutz und IT-Recht an der Hochschule Hof, leitet dort die Stabsstelle Compliance, die Transferstelle Recht und Lizenzen sowie die Forschungsgruppe Recht in Nachhaltigkeit, Compliance und IT. Sie konzipiert und implementiert seit Jahren Compliance Management Systeme direkt aus der Forschung in diversen Organisationen und vermittelt in Schulungen anwendungsbezogene Erkenntnisse.

Dr. Stefanie Lejeune ist Rechtsanwältin in der überörtlichen Sozietät Göhmann in Berlin und langjährige Lehrbeauftragte der Humboldt-Universität zu Berlin im Fachbereich Rechtswissenschaften. Zuvor war sie Richterin am Sozialgericht, Staatssekretärin im Ministerium der Justiz Rheinland-Pfalz und Landtagsabgeordnete. Sie ist u.a. spezialisiert auf die Beratung von Behörden und Unternehmen in den Bereichen Corporate Governance, Compliance und Korruptionsprävention.

Viele deutsche Unternehmen von e-Crime betroffen

Nachricht vom 06.08.2019

Eine aktuelle KPMG-Studie belegt, wie groß die Gefahren für die deutsche Wirtschaft sind, die durch Computerkriminalität und Cyberangriffe entstehen. Und wie unvorsichtig viele Unternehmen agieren.

Bereits zum fünften Mal seit 2010 beleuchtet KPMG das Thema e-Crime. In der diesjährigen Studie wurden 1.001 Unternehmen zu ihren Erfahrungen mit Computerkriminalität befragt.

Erhebliches Dunkelfeld

Ein sehr interessantes Ergebnis der Befragung ist, dass die Studienteilnehmer die Gefahr für deutsche Unternehmen allgemein als hoch oder sehr hoch einstufen. 92 Prozent der Unternehmen teilten im Jahr 2019 diese Einschätzung. Das Risiko für das eigene Unternehmen beurteilen allerdings nur 52 Prozent als hoch oder sehr hoch. Ein Grund für diese Diskrepanz in der Wahrnehmung des Risikos könne an den eigenen Erfahrungen liegen: Schließlich waren in den vergangenen beiden Jahren 39 Prozent der Unternehmen von e-Crime betroffen. Bei diesen Unternehmen könnte die Sensibilisierung daher erhöht sein.

Die Identifikation der Täter bereitet hierbei große Schwierigkeiten. In fünf von sechs Fällen können die Täter lediglich als „unbekannt extern" zugeordnet werden. Ein Umstand, der die Autoren der Studie den Verdacht äußern lässt, dass nicht nur die Täter, sondern auch ganze Delikte unerkannt bleiben.

Menschliche Faktoren von entscheidender Bedeutung

Mailserver sind dabei das häufigste Angriffsziel von Computerkriminellen. Das unterstreiche, wie sehr der Geschäftsverkehr und unternehmensinterne Abläufe inzwischen von der Nutzung von E-Mails abhängen und sich auf den zugehörigen Servern eine Vielzahl hochattraktiver Informationen für die Angreifer befinden. Phishing-Mails seien eine verhältnismäßig unkomplizierte Methode, Zugang zu erhalten. Aber auch der Erfolg von Ransomware-Angriffen sei zumeist darauf zurückzuführen, dass Kriminelle die Mitarbeiter mit betrügerischen E-Mails zu

folgenschweren Handlungen verleiten können.

Als begünstigender Faktor für e-Crime wird in der Studie insbesondere auf die Unachtsamkeit der Mitarbeiter (90 Prozent) hingewiesen. Aber auch eine mangelnde Sicherheitskultur, das Nicht-Erkennen von Verdachtsfällen sowie unzureichend geschultes Personal werden als e-Crime förderliche Faktoren genannt. Auf technischer Seite stellt die zunehmende Komplexität der in Unternehmen eingesetzten Technologie einen wesentlichen Faktor für den Erfolg von Computerkriminalität dar. Auch die ungenügende Sicherheit der IT-Systeme vor Angriffen und die zunehmende Professionalisierung der Angreifer („Hacking-as-a-service") begünstige den Erfolg.

Der Stellenwert vorbeugender Maßnahmen nimmt zu

Ein Lösungsansatz bestehe laut der Studie darin, die Mitarbeiter in Schulungen gezielt zu sensibilisieren (88 Prozent). Aber auch die Verschlüsselung von Daten und Datenträgern (87 Prozent) sehen die befragten Unternehmen als wesentliche Präventionsmaßnahme an sowie die regelmäßige Identifizierung des Schutzbedarfs von Daten und Systemen (79 Prozent). Auf den Austausch mit Behörden (36 Prozent) sowie Whistleblower-Systeme (32 Prozent) legen die Befragten weniger ihr Augenmerk.

Die vollständige Studie können Sie hier [1] anfordern.

Quellen

[1] https://hub.kpmg.de/studie-e-crime-in-der-deutschen-wirtschaft-2019?utm_campaign=KPMG%20-%20Studie%20-%20e-Crime%20in%20der%20deutschen%20Wirtschaft%202019&utm_source=AEM

Supply Chain Risk Management auf dem Prüfstand

Nachricht vom 29.07.2019

„Handelspartner, der." *Nach Duden-Definition ein „Land, seltener auch Unternehmen, mit dem ein anderes Land oder Unternehmen Handel treibt."* *Soweit zur theoretischen Bedeutung des Begriffs nach Auffassung des Dudens. In der Realität sieht das Ganze indes vielfach anders aus – gerade mit Blick auf die aktuelle wirtschaftspolitische Lage im globalen Maßstab.*

Die ist gekennzeichnet durch protektionistische Strömungen, Handelsbeschränkungen bis hin zu Sanktionen. Sprich, wir leben in einer instabilen Zeitenwende, in der bis dato gültige Handelsvereinbarungen nicht mehr bestehen oder von heute auf morgen aufgekündigt werden. Unternehmen müssen sich auf diese wirtschaftspolitischen Fliehkräfte einstellen und ihren Weg finden, um in diesen unruhigen Zeiten zu bestehen.

Kaum ein Tag vergeht, ohne Meldungen zu den drei großen Ländern – USA, China und Russland – und deren Ringen um weltweiten Einfluss. Den Beteiligten geht es darum, ihre wirtschaftliche und militärische Position im globalen Maßstab weiter auszubauen und vor allem zu festigen. Und auch innerhalb der EU gewinnen nationalistische und protektionistische Haltungen an Bedeutung – von Großbritannien über Italien bis nach Ungarn. Kurzum, die geopolitische Welt hat sich verändert, von einer bipolaren Welt alten Zuges hin zu einer multipolaren Unordnung, in der sich Staaten und Unternehmen schneller auf wechselnde Bündnisse sowie Marktgegebenheiten einstellen müssen. Vor allem produzierende Unternehmen und Zulieferer sind von diesen weltpolitischen Schwankungen betroffen. Gut beraten ist, wer in diesen volatilen Zeiten flexibel auf sich verändernde Märkte und deren Rahmenbedingungen reagieren kann und frühzeitig die richtigen Weichen stellt. Hilfreich ist ein Supply Chain Risk Management, um Planungs- und Handlungssicherheit zu gewinnen.

Von der Geopolitik über Naturkatastrophen bis zur Insolvenz

Wenn die US-Administration Strafzölle gegen den Iran oder China als Sanktion verhängt, so ist dies längst kein bilateraler Konflikt mehr. Denn im Zuge der weltweiten Verflechtung und Vernetzung im Finanz-, Waren- und Rohstoffaustausch können diese scheinbar zwischenstaatlichen Aggressionen Zulieferketten sprengen. Wer auf Öl aus dem Iran angewiesen ist oder chinesische High-Tech-Produkte für die eigene Produktion benötigt, hat schnell das Nachsehen. Sprich, im schlimmsten Fall droht ein kompletter Produktionsstopp. Dabei müssen es nicht immer die großen weltpolitischen Spannungen sein, die zu Zulieferproblemen führen. Deutlich wurde das im Jahr 2011 als der isländische Vulkan Eyjafjallajökull ausbrach und zu massiven Flugausfällen führte, was wiederum Teile der weltweiten Industrie über Wochen behinderte.

Dass der Fehler im Detail stecken kann, das zeigt sich in den Billigfertigungen der Armenhäuser dieser Welt. Steht eine Bekleidungsfabrik in Asien in Flammen, so kommt in Europa die Weiterverarbeitung oder Auslieferung ganzer Bekleidungsserien ins Stocken. Hinzu kommen weitere Risiken, wie LKW-Streiks, Demonstrationen oder die Insolvenz eines (Sub-)Lieferanten. Von daher brauchen Unternehmen, die zwingend von funktionierenden Lieferketten abhängig sind, neue Wege und Lösungen im Risikomanagement.

Alle unter einen Hut: (Supply Chain Risk) Management ist Chefsache

Wie umrissen, stehen Unternehmen heute vor einer Vielzahl an Herausforderungen in puncto möglicher Ausfallrisiken von Lieferketten. Angefangen bei geopolitischen Risiken, wie Protektionismus, Sanktionen und Kriege, über Finanz- und Compliance-Risiken bis zu Cybergefahren und Naturkatastrophen. Dementsprechend groß ist der Radius verantwortlicher Personen und Bereiche, die in diesem Umfeld involviert sein müssen.

Diese reichen von der Führungsebene, dem Einkauf und der Logistik sowie dem Risikomanagement und der Informationssicherheit bis hin zu Compliance-Experten und dem Business Continuity Management.

Alle unter einen Hut zu bekommen ist Führungs- und Risikomanagementaufgabe zugleich. Denn Ziel muss es sein, zu einer organisationsweiten sowie auf das jeweilige Unternehmen abgestimmten Vorgehensweise im kompletten Zuliefermanagement zu gelangen.

Vielfach scheitert das Supply Chain Management bereits an dieser Einstiegshürde. Die Gründe dafür sind vielfältig und reichen von einer mangelnden Kommunikation zwischen den Abteilungen und über den initiierten Risikomanagementprozess. Hinzu kommt eine fehlende Unternehmenskultur im offenen Umgang mit Risiken und Chancen. Daraus resul-

tiert eine Art Wagenburgmentalität, in der sich Abteilungen abschotten, Wissen und Know-how nicht weitergeben und auf Insellösungen setzen. Gepaart mit dem Glauben, die jeweilige Software wird den notwendigen Überblick ermöglichen, werden potenzielle Risiken in der Zulieferkette oft in einer Art Häkchenmentalität behandelt und abgearbeitet.

Ein Supply Chain Risk Management muss in der Gesamtorganisation fest verankert und die handelnden Personen müssen mit dem dafür notwendigen Mandat und Wissen ausgestattet sein. Denn das Risikomanagement kann nur so gut sein wie die Personen, die es ausfüllen müssen. Von daher trifft der alte Spruch nach wie vor zu: (Supply Chain) Risk Management ist Chefsache.

Wie ein aktives Supply Chain Risk Management in der Praxis aussehen kann, zeigen die folgenden Beispiele:

Praxisbeispiele: Zulieferketten stärken dank Nachhaltigkeit, Resilienz und Standards

- Wie ein aktives Risikomanagement im Zuliefererbereich aussehen kann, das will der **VW- Konzern** mit seiner neuen Selbstverpflichtung zeigen. Bis dato kein Garant für Integrität, verordnen sich die Wolfsburger Autobauer seit dem 1. Juli 2019 ein „weltweites Sustainability Rating (Nachhaltigkeitsprüfung) für seine Lieferanten". In einer Meldung des Konzerns heißt es hierzu: „Beim Sustainability Rating geben die Zulieferer auf Basis eines Fragebogens und mitgelieferter Dokumente zunächst eine Selbsteinschätzung zu ihrem Nachhaltigkeitsverhalten ab. Die Angaben und Dokumente werden von qualifizierten Dritten überprüft. Bei Zweifeln finden Kontrollen vor Ort statt. Kommt es zu Verfehlungen in den Bereichen Umwelt/Soziales oder Korruption, führen diese zum Ausschluss von der Auftragsvergabe." Basis der Nachhaltigkeitsstrategie und zugleich verpflichtend für alle Firmen in der VW-Lieferkette ist der neue „Code of Conduct für Geschäftspartner" des Konzerns. Zur Pressemitteilung [1].
- Die **DHL** setzt auf ein verbessertes Lieferkettenmanagement. So kommt innerhalb des Konzerns die Lösung „DHL Resilience360" zum Einsatz. Mit der cloudbasierten Risikomanagementlösung sollen bessere Wetterdaten und -warnungen zu Hurrikanen die Lieferketten schützen. Basierend auf einem Algorithmus analysiert die Lösung den vorhergesagten Weg eines Hurrikans oder Zyklons. Nutzer sollen damit „über mögliche Auswirkungen auf ihre spezifischen Lieferketten" informiert werden. Und weiter heißt es bei der DHL: „Mit den neuen Funktionen können Kunden eine bessere Analyse der betroffenen Standorte erhalten und beurteilen, inwieweit Produktion oder Belieferungen an Endkunden beeinflusst werden." Zur Pressemitteilung [2].
- Und auch bei der **Zurich-Versicherung** setzen die Verantwortlichen auf Analysen. Zurich Supply Chain Risk Management Services baut auf eine automatisierte Überwachung und Risikoidentifikation der kompletten Lieferkette. Neben Online-Datenquellen und Datenbanken kommen Technologien zum Einsatz, die auf künstlicher Intelligenz basieren. Im Fokus stehen neben geopolitischen Risiken auch Naturkatastrophen oder Cybergefahren. Das Ziel ist, vorausschauend auf mögliche Risiken zu blicken und eine bessere Entscheidungsgrundlage zu besitzen. So kommt das Unternehmen zu dem Schluss: „Gemeinsam mit dem Versicherer können Unternehmen durch eine Analyse der komplexen Lieferketten Ausweichszenarien für bestimmte Vorfälle entwickeln und die Widerstandsfähigkeit des Unternehmens erhöhen – bis hin zu einem Transfer der Restrisiken." Zum Bericht [3].
- Das **VDA QMC**, Qualitäts Management Center im Verband der Automobilindustrie e. V., veröffentlichte zusammen mit der **AIAG** (Automotive Industry Action Group) im Juni 2019 ein Failure Mode and Effects Analysis (FMEA-) Handbuch zum neuen Standard der Risikoanalyse in der automobilen Lieferkette. Hintergrund ist, dass einschlägige Normen in der automobilen Lieferkette die Durchführung technischer Risikoanalysen in Form einer FMEA voraussetzen – vertraglich gefordert. Dabei dient FMEA als teamorientierte und systematische Analyse-Methode im technischen Risikomanagement. Das Ziel ist es, Risiken zu identifizieren und zu reduzieren. Inhaltlich basiert das Ganze auf einem Sieben-Schritt-Ansatz – von der Planung und Vorbereitung, einer Struktur- und Funktionsanalyse über die Fehler- und Risikoanalyse bis zur Optimierung und Ergebniskommunikation inklusive der Risikokommunikation. Mit dem neuen Standard sollen Lieferanten in die Lage versetzt werden, mithilfe eines einheitlichen Prozesses zur FMEA sowohl die Bedürfnisse als auch die Erwartungen der Kunden zu erfüllen. Zum Newsletter (S. 22ff.) [4].

Big Data und der Mensch

Überhaupt muss es für Unternehmen darum gehen, neue Methoden in ihr Supply Chain Risk Management zu integrieren. Dabei spielen neue Analyseverfahren und Auswertungen im Big-Data-Umfeld eine wichtige Rolle, um beispielsweise mithilfe von Szenarien zu validen Aussagen über die Risikolage in einzelnen Ländern, Regionen oder weltweit zu gelangen. Damit lassen sich Komplexitäten in der kompletten Zulieferkette reduzieren und wertvolle Informationen für das eigene Handeln gewinnen. Dies setzt aber Experten voraus, die in der Lage sind, Daten zu überprüfen und vor allem die richtigen Schlüsse für das weitere Vorgehen zu ziehen. Denn die größte und beste Datengrundlage wird nutzlos, wenn Unternehmen intern nicht in der Lage sind, diese zu interpretieren und auf Kausalität zu prüfen.

Doch dies alleine genügt nicht. Unternehmen müssen in unseren sensiblen Zeiten regelmäßig die eigene Zulieferkette und Fertigungsstrategie auf den Prüfstand stellen. Dabei spielen unter anderem Fragen nach den Fertigungsbedingungen in Offshore-Ländern eine Rolle, aber auch Just-in-Time-Lieferungen sowie Produktionsstandorte, die in Erdbebenregionen liegen oder durch Terror und Krieg bedroht sind. In diesem Kontext bringt es Dr. Ulrich Kater, Chefvolkswirt der Deka Bank, in einem Interview [5] auf den folgenden Nenner: „Die Welt als eine einzige Fabrikhalle zu begreifen, ist vorbei. Das bedeutet, dass Produktionen, die bislang im Ausland angesiedelt waren, zurückkommen könnten (...)". Als Gründe nennt er neben Zöllen und der sich ändernden Kalkulationsbasis auch den technischen Fortschritt in der heimische Produktion. Faktoren, die durchaus neue Denkmodelle in der gesamten Produktions- und Zuliefererkette zulassen. Hinzu kommt ein weiterer Schwerpunkt, nämlich das Thema Nachhaltigkeit und Reputation.

Unternehmen, die auf schlechte Produktionsbedingungen setzen und damit rein den Kostenfaktor im Blick haben, werden zukünftig das Nachsehen haben. Diesem politischen und gesellschaftlichen Druck können sich Unternehmensverantwortliche nicht mehr entziehen. Von daher gilt es, die Sensibilität und Awareness auch in diesen Bereichen auszubauen, um den Faden in der Zulieferkette nicht zu verlieren. Oder anders formuliert: Zum Einblick muss der Aus- und Weitblick im gesamten Prozess des Supply Chain Risk Management kommen.

Michael Jahn-Kozma

RMA-Leitfaden: Supply Chain Risk Management

Der Arbeitskreis Supply Chain Risk Management der RMA hat einen eigenen Leitfaden zum Supply Chain Risk Management erstellt. Dieser setzt auf eine ganzheitliche Betrachtung strategischer, operativer und finanzieller Risiken in der Supply Chain – auch unter Berücksichtigung von Compliance-Fragestellungen. Dazu gehören auch geeignete Methoden zur Risikoidentifizierung und -bewertung, die Definition von Messinstrumenten zur Risikoüberwachung und Analyse von Maßnahmen zur Risikosteuerung. Weitere Informationen finden Sie hier [6].

Den Leitfaden – Supply CRM können Sie über die Homepage der RMA kostenfrei bestellen [7].

Quellen

[1] https://www.volkswagenag.com/de/news/2019/06/volkswagen-group-commits-suppliers-to-sustainability.html
[2] https://www.dpdhl.com/content/dam/dpdhl/de/media-relations/press-releases/2019/pm-r360-hurricane-report-20190529.pdf
[3] https://www.zurich.de/de-de/branchenwissen/supply-chain%20
[4] https://vda-qmc.de/fileadmin/redakteur/newsletter/2019_Newsletter_Juni.pdf
[5] https://www.sparkasse.de/themen/mittelstand/strafzoelle-usa.html
[6] https://rma-ev.org/verein/arbeitskreise/supply-chain-risk-management/
[7] https://rma-ev.org/news-publikationen/publikationen-rma-spezial/

Meseke: „Nichts ist sicher“

Nachricht vom 28.05.2019

Mit Bodo Meseke, Cybercrime-Experte und Autor des neuen Buchs „Digitale Forensik – Praxiswissen Cybercrime für Manager“, sprach die ESV-Redaktion über Cybergefahren und wie sich Unternehmen besser schützen können.

Das neue Buch „Digitale Forensik – Praxiswissen Cybercrime für Manager“ richtet sich nicht nur an IT-Spezialisten, sondern vor allem an das Management. Führungskräfte sollten die wichtigsten Maßnahmen kennen, um ihr Unternehmen und seine Werte zu schützen.

Kein Monat vergeht, in dem nicht ein neuer Hack bekannt wird. Ständig werden Unternehmen angegriffen. Wo sind sensible Daten heute eigentlich noch sicher?

Bodo Meseke: Wenn der Speicherort mit anderen Systemen verbunden ist? Nirgends! Machen Sie sich eines bewusst: Die Frage ist längst nicht mehr, ob ein Unternehmen angegriffen wird, sondern wann.

Das klingt dramatisch. Was können Führungskräfte tun, um das neue Gold – ihre Firmendaten und Geschäftsgeheimnisse – bestmöglich zu schützen?

Bodo Meseke: Sie sollten möglichst früh anfangen, eine IT-Sicherheitsstrategie aufzubauen, die alle wesentlichen Abteilungen einbezieht. Ganz wichtig ist neben der technischen Komponente der menschliche Faktor: Mitarbeiter, die im Ernstfall wissen, was zu tun ist, können größeren Schaden abwenden. Auch die Unternehmenskultur spielt eine große Rolle. Wer Fehler vertuscht, weil er Strafen fürchtet, macht die Sache womöglich noch schlimmer.

Ihr Buch geht genau auf diese Faktoren ein. An wen richtet es sich und was können die Leser erwarten?

Bodo Meseke: Digitale Forensik – Praxiswissen Cybercrime für Manager [1] ist für Führungskräfte und Compliance-Verantwortliche, ebenso wie IT-Mitarbeiter geschrieben. Doch ist es kein technisch orientiertes Werk. Mein Ziel ist es, das Management „abzuholen“ und durch Hinweise zu sensibilisieren: was im Ernstfall zu tun ist, wie Maßnahmen ablaufen können und was im Vorfeld beachtet werden sollte.

Im Ernstfall habe ich aber keine Zeit, lange Texte zu lesen...

Bodo Meseke: Genau. Deshalb enthält mein Buch auch erste Anregungen für alltagsnahe Checklisten, FAQs und ein Glossar. Wen muss ich ansprechen, wenn der Verdacht eines Angriffs besteht etc. Griffige Beispiele aus der Praxis zeigen, wie mit anderen Vorfällen umgegangen wurde. Und am besten ist es, Führungskräfte fangen schon jetzt an, eine individuelle Strategie für ihr Unternehmen zu entwickeln – und nicht erst, wenn die IT-Systeme blockiert sind.

Haben Sie ein alltagsnahes Beispiel für erste Schritte?

Bodo Meseke: Wie bei jedem Notfall ist es hilfreich, zuerst folgende W-Fragen zu beantworten, um sich einen Überblick zu verschaffen:

- Was ist geschehen?
- Wo ist es passiert?
- Wann ist es passiert?
- Wer hat den Angriff entdeckt?
- Wer muss informiert werden?
- Was wurde beschädigt/verändert/gelöscht/gestohlen?

Entlang dieses Rasters greift dann ein zuvor entwickelter Notfallplan, der natürlich nicht nur digital, sondern auch in gedruckter Form schnell zugänglich sein muss.

Sie beschreiben, was passiert, wenn Ermittler ins Haus kommen. Wie läuft denn so eine digitalforensische Untersuchung generell ab?

Bodo Meseke: Ein jeweils passendes Team aus Experten wird zusammengestellt. Jede digitalforensische Untersuchung lässt sich in sechs Schritte gliedern: von der strategischen zur organisatorischen Vorbereitung über das Suchen und Erkennen von Beweisen bis hin zu ihrer Prüfung und Analyse sowie dem abschließenden Bericht. Dieses Grundgerüst ist flexibel und wird je nach Vorfall um geeignete Maßnahmen ergänzt.

Seit über 20 Jahren leiten Sie IT-forensische Teams. Was hat sich in der Zeit geändert?

Bodo Meseke: Wir arbeiten heute natürlich mit wesentlich leistungsfähigeren digitalen Tools bei der Datenanalyse. Zudem ist das Datenvolumen enorm gestiegen: Bei einer eDiscovery beispielsweise werden oft Riesenmengen – wir reden teilweise von Millionen – an E-Mails, PowerPoint-Präsentationen, Verträgen oder Protokollen ausgewertet. Manchmal parallel an mehreren Standorten auf verschiedenen Kontinenten.

Und wenn wir auf Cybercrime ganz grundsätzlich schauen: Cyberkriminelle tragen heute Anzug. Und der Ort des Geschehens sind keine „nerdigen" Zimmer mit chaotischer Technik, es sind vorzeigbare Büros mit teils Dutzenden „Arbeitsplätzen". Hier gibt es – wie auch in anderen „Firmen" – ein planvolles Vorgehen mit definierten Zuständigkeiten. Auch das Darknet ist mitunter besser organisiert als große bekannte Verkaufsplattformen.

Bin ich sicher, wenn ich meine innersten Systeme gar nicht nach außen vernetze?

Bodo Meseke: Unternehmensnetzwerke komplett abzuschotten, gelingt nicht, zumindest nicht, wenn Sie ihre Wettbewerbsfähigkeit nicht drastisch reduzieren wollen. Heute ist alles abhängig von Technologien. Digitale Systeme gehören zum Herzstück jedes Unternehmens, deswegen ist und bleibt Cybersicherheit ein Topthema. Egal, ob es um Steuerungsprozesse oder das Intranet geht. Mit allen digitalen Verbesserungen entwickeln sich auch die Risiken weiter – teilweise mit unabsehbaren Folgen.

Gibt es Besonderheiten für den deutschen oder europäischen Markt?

Bodo Meseke: Die rechtlichen Regularien für sein Land sollte man unbedingt kennen. Bei uns ist die DSGVO ein großes Thema: Heute muss z.B. jeder Vorfall, bei dem der Schutz personenbezogener Daten verletzt wurde, innerhalb von 72 Stunden der Aufsichtsbehörde gemeldet werden – es sei denn, diese Verletzung führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen. Mein Buch enthält einen Überblick zu den rechtlichen Vorgaben bezüglich IT-Sicherheit und Datenschutz.

Erfahrene Dienstleister kennen all diese Rahmenbedingungen und beraten die Unternehmensleitung zu den wesentlichen Maßnahmen. Sie unterstützen zudem behördliche Ermittlungen und bereiten Daten gerichtssicher auf. So ein Vorfall stört den normalen Geschäftsablauf erheblich. Das Ziel ist deshalb, den Schaden zu begrenzen und so zügig wie möglich zur Normalität zurückzukehren.

Zur Person

Bodo Meseke arbeitet seit über 20 Jahren in der Digitalen Forensik. Als Cybercrime-Ermittler beim Bundeskriminalamt hat er spektakuläre Fälle gelöst; später leitete er computerforensische Abteilungen und gründete ein Dienstleistungsunternehmen für IT-Forensik.
Heute ist Bodo Meseke als Partner bei Ernst & Young (EY) verantwortlich für die Forensic Technologies in Deutschland, Österreich und der Schweiz (GSA). Der Diplom-Verwaltungswirt erstellt regelmäßig Gutachten für Strafverfolgungsbehörden, Industrie und Wirtschaft.
Sein Buch zur Digitalen Forensik hilft Managern, die Risiken, die Cybercrime für ihr Unternehmen darstellt, zu verstehen und vorzubeugen – mit praxisnahen Beispielen und Checklisten.

Quellen

[1] https://www.esv.info/978-3-503-18267-1

Einkauf: Wo sehen Unternehmen die größten Risiken?

Nachricht vom 10.05.2019

Für den Einkauf hat die Versorgungssicherung höchste Relevanz. Eine zuverlässige Sicherung wird durch klassisches Risikomanagement jedoch immer schwieriger. Auf welche Maßnahmen setzen Unternehmen?

In einer Umfrage unter 93 Teilnehmern hat die Unternehmensberatung INVERTO im Zeitraum November – Dezember 2018 die Herausforderungen und Maßnahmen zur Risikoprävention untersucht. Teilgenommen haben Unternehmen unterschiedlichster Umsatzgrößen und Branchen.

Aktuell relevante Risiken

Auf die Frage, welche aktuellen politischen und wirtschaftlichen Themen für ihr Unternehmen ein Risiko darstellen, nannten 54 Prozent den Protektionismus (17 Prozent im Vorjahr) und 45 Prozent den Brexit (nach 19 Prozent). Auch IT-Kriminalität (49 Prozent), veraltete digitale Technologien (45 Prozent) und die Lieferantenabhängigkeit (41 Prozent) nahmen die Unternehmen als wesentliche Risken wahr. Als Risiko mit der höchsten Priorität schätzten die Unternehmen das Versorgungsrisiko ein, d.h. die Gefahr, nicht alle benötigten Waren rechtzeitig beschaffen zu können (65 Prozent). Aber auch Preisrisiken (48 Prozent) sowie Lieferantenausfall- und Qualitätsrisiken (jeweils 46 Prozent) wurden häufig genannt. Compliance- und Nachhaltigkeitsrisiken räumen die Unternehmen in diesem Jahr nur eine geringere Priorität ein (18 Prozent bzw. 14 Prozent).

Risikomanagement der Teilnehmer

Laut Umfrage werden Risiken dabei nur von etwas mehr als der Hälfte der Unternehmen systematisch erfasst und bewertet – von großen Unternehmen dabei aber noch deutlich häufiger als von kleinen. Dennoch definieren die meisten Unternehmen Gegenmaßnahmen. Am häufigsten wurden hierbei eine regelmäßige Lieferantenbewertung genannt (81 Prozent) sowie der Abschluss langfristiger Rahmenverträge (69 Prozent). Auf die Frage, welche Erfolge mit dem Risikomanagement im Einkauf erzielt wurden, gaben 71 Prozent die Sicherung der zuverlässigen Versorgung an sowie die Verringerung von Lieferantenausfällen (54 Prozent). Im Vergleich zum Vorjahr gelang dies aber in diesem Jahr weniger Unternehmen (88 Prozent bzw. 58 Prozent in 2017/2018).

Handlungsempfehlungen

Als Handlungsempfehlungen geben die Autoren der Studie mit, sich einen Überblick über potenzielle Risiken für die Supply Chain und Ihr Unternehmen zu verschaffen, insbesondere vor dem Hintergrund aktueller Entwicklungen auf den Beschaffungsmärkten – aber auch gesamtwirtschaftlich. Auch die Bewertung des möglichen Schadens (Umsatzausfall, verlorene Marge etc.) bei Eintreten der Risiken sowie Transparenz bei Aufwand und Ertrag von Maßnahmen helfen, eine gesamtunternehmerische Entscheidung zu treffen.

Die gesamte Studie können Sie hier [1] anfordern.

Quellen

[1] https://www.inverto.com/publikationen/studienergebnisse-risikomanagement/

Dax-Aufsichtsratsvergütung 2018: Gestiegen, trotz rückläufiger Gewinne

Nachricht vom 29.04.2019

Die durchschnittliche Vergütung von Aufsichtsratsvorsitzenden der Dax-Unternehmen stieg im Geschäftsjahr 2018 um 3,9 Prozent auf 424.000 Euro.

Damit lag sie etwas unterhalb des Durchschnitts, der seit 2006 rund 4,3 Prozent pro Jahr beträgt. Die Vergütungsniveaus der Vorstandsvorsitzenden in den gleichen Unternehmen liegt laut Studie etwa bei dem Fünfzehnfachen.

Keine Augenhöhe mit dem Vorstand

Den immensen Unterschied in der Vergütungshöhe von Aufsichtsratsvorsitzenden und Vorstandsvorsitzenden kritisieren die Studienautoren: „Ein Aufsichtsratsvorsitz ist heute mehr denn je auch mit Strategiebegleitung und intensivem Sparring für den Vorstand verbunden. Keine nennenswerte Investition oder sonstige Entscheidung von größerem Ausmaß kann heute ohne Einbindung des Aufsichtsratsvorsitzenden getätigt werden. Die Vergütung für das Amt sollte daher so ausgelegt sein, um sich auf Augenhöhe begegnen zu können. Davon sind wir aber weit entfernt“, bilanziert Nina Grochowitzki von der Unternehmensberatung hkp, die die Untersuchung vorgelegt hat.

Entkopplung der Vergütung

Angesichts der von den Unternehmen fortgesetzten Umstellung der Aufsichtsratsvergütung auf reine Fixbezüge haben sich die Vergütungen von der Geschäftsentwicklung entkoppelt. So werde der aktuelle Vergütungsanstieg durch sinkende Unternehmensgewinne kontrastiert, beschreiben die Autoren: Der durchschnittliche Konzernjahresüberschuss der Dax-Unternehmen ist 2018 um drei Prozent gesunken. Mit BMW, Continental, Deutsche Bank, Fresenius und Fresenius Medical Care setzen laut Studie nur noch fünf Unternehmen auf eine Kombination von fixer und langfristig variabler Vergütung für ihre Aufsichtsräte. Eine kurzfristig variable Vergütung auf Basis des Geschäftsergebnisses eines Jahres findet sich in keinem Dax-Unternehmen mehr. Vorschriften zum Erwerb und langfristigen Halten eines signifikanten Anteils an Aktien des eigenen Unternehmens finden sich nur bei BASF, Bayer, Daimler und RWE.

Regine Siepmann, Partnerin bei hkp, betrachtet den manifestierten Trend zur ausschließlichen Fixvergütung kritisch: „Wenn schon eine reine Fixvergütung gezahlt wird, dann sollte diese zwingend durch eine Aktienkaufverpflichtung ergänzt werden. Der Aufsichtsrat als Vertreter der Aktionäre braucht mehr „Skin in the Game“, fordert die Corporate Governance-Expertin.

Die Deutsche Bank ist Spitzenreiter

Mit rund 858.000 Euro belegt der Aufsichtsratsvorsitzende der Deutschen Bank wie in den Geschäftsjahren zuvor die Spitze der Vergütungsrangliste der ganzjährig im Amt tätigen Dax-Kontrolleure. Auf den Plätzen zwei und drei folgen die Chefaufseher von BMW und Fresenius mit jeweils 640.000 Euro Vergütung. Die geringsten Vergütungen erhalten die Aufsichtsratsvorsitzenden von Merck (237.000 Euro), HeidelbergCement (232.000 Euro) und Beiersdorf (228.000 Euro).

Weitere Informationen zur Studie finden Sie hier [1].

Quellen

[1] https://www.hkp.com/article/387

5. EU-Geldwäscherichtlinie – Neue Anforderungen

Nachricht vom 17.04.2019

Dr. Tim Nikolas Müller, Counsel bei der internationalen Anwaltskanzlei Allen & Overy LLP, gibt im Interview Auskunft über die wesentlichen Änderungen durch die 5. EU-Geldwäscherichtlinie.

Die 5. EU-Geldwäscherichtlinie ist im Juli 2018 bereits in Kraft getreten und bis zum 10. Januar 2020 von den EU-Mitgliedstaaten umzusetzen. Weshalb die schnelle Änderung ggü. der 4. EU-Geldwäscherichtlinie, die bis Juni 2017 umzusetzen war?

Tim Müller: Die Methoden der Geldwäsche und Terrorismusfinanzierung unterliegen einem steten Wandel. Die gesetzlichen Regelungen zur Prävention dieser Delikte müssen daher regelmäßig aktualisiert werden, um wirksam zu sein. Ein Beispiel: Die Richtlinie nimmt mit Kryptowährungen eine technologische Neuerung ins Visier, die anonyme Transaktionen ermöglicht und deshalb besonders leicht für kriminelle Zwecke missbraucht werden kann.

Diese wesentliche Änderung betrifft insbesondere den Kreis der Verpflichteten. Wer wurde neu in den Kreis aufgenommen?

Zukünftig werden insbesondere Kryptowährungsbörsen und Wallet-Anbieter in den Kreis der Verpflichteten aufgenommen. Kryptowährungsbörsen sind Unternehmen, die den Tausch zwischen offiziellen Zahlungsmitteln und virtuellen Währungen ermöglichen. Wallet-Anbieter sind Unternehmen, die ihren Kunden elektronische Geldbörsen für virtuelle Währungen zur Verfügung stellen. Weiterhin werden Kunsthändler/-vermittler ab einem bestimmten Transaktionswert als Verpflichtete erfasst. Immobilienmakler sind in Zukunft nicht nur beim Verkauf von Immobilien zur Geldwäscheprävention verpflichtet, sondern auch bei deren Vermietung, wenn die monatliche Miete einen bestimmten Schwellenwert erreicht. Neben dem bereits heute erfassten Steuerberater werden zukünftig auch weitere Personen, die Hilfe oder Unterstützung in Steuerfragen leisten, als Verpflichtete gelten.

Kryptowährungsbörsen und Wallet-Anbieter haben ihren Sitz derzeit häufig nicht in der EU. Sind sie auch dann verpflichtet?

Kryptowährungsbörsen und Wallet-Anbieter werden – wie andere Verpflichtete auch – von den spezifischen Vorschriften zur Geldwäscheprävention nur erfasst sein, wenn sie ihren Sitz oder eine Niederlassung in einem EU-Mitgliedstaat

haben. Anonyme Transaktionen in virtuellen Währungen werden daher nur eingedämmt und nicht etwa vollständig verhindert.

Weshalb hat man die Kunsthändler als Verpflichtete erst jetzt aufgenommen?

Kunsthändler waren nach der bisherigen Gesetzeslage bereits als Güterhändler zur Geldwäscheprävention verpflichtet. Für Güterhändler gelten allerdings verschiedene Erleichterungen, die für Kunsthändler durch die eigenständige Erfassung als Verpflichtete wegfallen werden.Die eigenständige Erfassung von Kunsthändlern geht insbesondere darauf zurück, dass internationale terroristische Vereinigungen den Verkauf von erbeuteten Kunstwerken und Kulturgütern – etwa aus Syrien – als Finanzierungsquelle entdeckt haben.

Welche Neuerungen beinhaltet die 5. EU-Geldwäscherichtlinie in Bezug auf KYC-Checks?

Bei Geschäftsbeziehungen zu bestimmten Gesellschaften werden Verpflichtete im Rahmen ihrer KYC-Checks in Zukunft zur Einsichtnahme in das Transparenzregister verpflichtet. Die Richtlinie harmonisiert außerdem die verstärkten Sorgfaltspflichten, die Verpflichtete bei Geschäftsbeziehungen in Drittländer mit einem hohen Geldwäscherisiko anwenden müssen. Weiterhin wird es zukünftig EU-weite Listen zu Ämtern und Funktionen geben, deren Inhaber als politisch exponierte Personen im Sinne des Geldwäscherechts zu behandeln sind.

Wer darf Einsicht in das Transparenzregister nehmen und welche Informationen finden sich dort?

Das Transparenzregister enthält Informationen zu den wirtschaftlich Berechtigten von juristischen Personen, Personengesellschaften und weiteren Rechtsgestaltungen, z.B. Trusts. Die Einsichtnahme war bislang vom Vorliegen eines berechtigten Interesses abhängig. Die Richtlinie erleichtert den Zugang zum Transparenzregister und hebt das Erfordernis eines berechtigten Interesses auf. Nur in Bezug auf Trusts und vergleichbare Rechtsvereinbarungen wird auch zukünftig ein berechtigtes Interesse an der Einsichtnahme gefordert.

Was ist zu tun, wenn man Unstimmigkeiten beim Blick in das Register feststellt?

Verpflichtete müssen das Transparenzregister in Zukunft informieren, wenn die ihnen vorliegenden Informationen zu den wirtschaftlich Berechtigten ihres Vertragspartners nicht mit den Angaben im Transparenzregister übereinstimmen. Personen, die keine Verpflichteten sind, werden von dieser Pflicht nicht erfasst – zum Beispiel Journalisten, die im Rahmen einer Recherche das Transparenzregister einsehen.

Sind nationale Transparenzregister nicht völlig unzureichend in Anbetracht der globalen Vernetzung der Wirtschaft – gerade auch in Bezug auf Sprachbarrieren?

Die EU hat diese Schwierigkeit erkannt. Die Richtlinie sieht daher vor, dass die EU-Kommission gemeinsam mit den EU-Mitgliedstaaten dafür sorgt, dass die nationalen Register bis zum 10. März 2021 miteinander vernetzt werden.

Welche Änderungen hält die Richtlinie für die Behörden bereit?

Die Richtlinie erweitert die Befugnisse der zentralen Meldestellen, den Financial Intelligence Units. Diese erhalten zukünftig unter anderem Zugriff auf Register, in denen die Inhaber von Immobilien in den EU-Mitgliedstaaten verzeichnet sind. Zudem wird die Zusammenarbeit zwischen den zentralen Meldestellen erleichtert, indem etwa Hindernisse beim Informationsaustausch abgebaut werden.

Zur Person

Dr. Tim Nikolas Müller ist Counsel im Frankfurter Büro der internationalen Anwaltskanzlei Allen & Overy LLP. Er berät nationale und internationale Unternehmen zu allen Fragen des Wirtschaftsstrafrechts und der Compliance. Er verfügt über große Erfahrung in der Verteidigung von Unternehmen in komplexen Straf- und Ordnungswidrigkeitenverfahren. Ein weiterer Schwerpunkt seiner Praxis ist die Beratung zu Wirtschafts- und Finanzsanktionen und Fragen der Geldwäscheprävention. Zudem ist er auf die Durchführung von internen Untersuchungen spezialisiert.

Der Anteil des Glücks am Erfolg

Nachricht vom 15.04.2019

Dem Compliance Officer gelingt vieles, aber nicht immer alles. Woran liegt es? An den eigenen Fähigkeiten? Am Fleiß? Am Glück? Welches Bild wird den Ansprechpartnern vermittelt?

Zwei Gruppen ließ Robert H. Frank ein Interview mit einer Person lesen, wobei die Inhalte fiktiv waren: Ein intelligente, kompetente, selbstsichere, aber nicht unbedingt liebenswerte Person beschrieb darin ihren beruflichen Erfolgsweg (Frank: Ohne Glück kein Erfolg, 2018, S. 182 – 187).

Beide Texte enthielten die gleichen dreihundert Worte. Am Ende stand jedoch ein kurzer, unterschiedlicher Abschnitt. Eine Version mit einem kompetenten Interviewpartner, die andere mit einem glücklichen. Der kompetente Mensch betonte: „Allerdings ist uns der Erfolg nicht so einfach in den Schoß gefallen. Wir haben hart dafür gearbeitet ... und ich bin wahrscheinlich der Einzige, dem das gelingen konnte."

Während der Glückliche festhielt: „Wir haben hart gearbeitet, aber wir hatten auch Glück ... und wäre nicht zufällig dieser Investor anwesend gewesen ... weiß ich nicht, ob sich irgendetwas von der realen Magie überhaupt ereignet hätte."

Glück oder Kompetenz?

Auf die Frage, ob sie den Glücklichen oder Kompetenten einstellen würden, bevorzugten Frauen den Ersteren, während Männer zum Zweiten tendierten. Befragte mit höherem Bildungsabschluss tendierten zum Glücklichen, solche mit niedrigerem Bildungsabschluss zum Kompetenten. Bei der Frage, mit wem sie lieber befreundet wären, bevorzugten alle Versuchsteilnehmer den Glücklichen. Sie vermuteten u.a., dass diesem Freundlichkeit wichtiger wäre.

Glück hat hohe Relevanz

Dass Talent und Einsatz als positive Eigenschaften die Grundlage des Erfolgs sind, bedarf nicht der Erklärung. Es gibt allerdings noch einen anderen Faktor, der wesentlichen Einfluss darauf hat, wie Menschen als attraktive Teamteilnehmer wahrgenommen werden: das Glück. Glück besitzt deshalb eine hohe Relevanz,

weil ehrgeizige Menschen geschätzt werden und Dinge voranbringen, ein Übermaß an Ehrgeiz dagegen rasch zur einseitigen Durchsetzung der eigenen Interessen führt, ein Team schwächt und deshalb negativ wahrgenommen wird. Dabei handelt es sich nicht um ein „Wohlfühlthema" als vielmehr einen harten Faktor, werden doch sympathisch wahrgenommen Menschen mit sehr viel größerer Wahrscheinlichkeit innerhalb eines Themas Zustimmung für ihre Themen finden.

Es wird also durchaus die Zusammenarbeit mit anderen positiv beeinträchtigen, wenn bereitwillig auch dem Glück ein Anteil am Erfolg eingeräumt wird. Auch als Compliance-Officer.

Serie „Compliance anders"

- Teil 1: Compliance Officer: Fortune müssen sie haben! [1]
- Teil 2: Nur wenn gesprochen wird, wird der offene Dialog zur Routine [2]
- Teil 3: Wenn der Kollege Marotten zeigt [3]
- Teil 4: Mit Empathie mehr erfahren [4]
- Teil 5: Einordnung von Gerüchten in der Compliance [5]
- Teil 6: Konkretisierung von Gerüchten in der Compliance [6]
- Teil 7: Macht und Moral [7]
- Teil 8: Das Nutella-Prinzip [8]
- Teil 9: Kreativität und Standardlösungen [9]
- Teil 10: Netzwerke der Compliance [10]
- Teil 11: Neue Wege gehen [11]

Thomas Schneider

Quellen

[1] https://www.compliancedigital.de/ce/compliance-officer-fortune-muessen-sie-haben/detail.html
[2] https://www.compliancedigital.de/ce/nur-wenn-gesprochen-wird-wird-der-offene-dialog-zur-routine/detail.html
[3] https://www.compliancedigital.de/ce/wenn-der-kollege-marotten-zeigt/detail.html
[4] https://www.compliancedigital.de/ce/mit-empathie-mehr-erfahren/detail.html
[5] https://www.compliancedigital.de/ce/einordnung-von-geruechten-in-der-compliance/detail.html
[6] https://www.compliancedigital.de/ce/konkretisierung-von-geruechten-in-der-compliance-2/detail.html
[7] https://www.compliancedigital.de/ce/macht-und-moral/detail.html
[8] https://www.compliancedigital.de/ce/das-nutella-prinzip/detail.html
[9] https://www.compliancedigital.de/ce/kreativitaet-und-standardloesungen/detail.html
[10] https://compliancedigital.de/ce/netzwerke-der-compliance/detail.html
[11] https://compliancedigital.de/ce/neue-wege-gehen-1/detail.html

Fachtagung Compliance 2019

Nachricht vom 08.04.2019

Neben der Digitalisierung standen die Themen Geldwäsche, Tax Compliance und Praxiserfahrungen zum US-Monitorship im Fokus der 5. Fachtagung Compliance.

Zum Auftakt betonte Paul Nemitz, Principal Advisor bei der Europäischen Kommission, in seinem Vortrag, dass Digitalfirmen nicht über dem Recht stünden, wie auch aktuelle Strafzahlungen der EU verdeutlichen. Auch wenn diese Firmen für disruptive Innovationen stehen, dürfe es kein „disrupt the law" geben. Dies sei unabdingbar für das Funktionieren der Demokratie. Geltendes Recht wie die DSGVO müsse eingehalten werden. Allerdings wies Nemitz darauf hin, dass Künstliche Intelligenz die Gesetzgebung vor bisher unbekannte Probleme stellen werde, insbesondere der Umgang mit generierten Daten selbstlernender Systeme. Der Mensch müsse dabei stets die Kontrolle behalten und dürfe nicht blind der Technologie vertrauen.

Vorhanden GRC-Strikturen nutzen

Christian Gräser und Harald Diebel von EY stellten im Anschluss die wichtigsten Faktoren für ein wirksames Tax Compliance Management System vor. Die Referenten empfahlen eine sinnvolle Verzahnung von Tax Compliance mit dem u.U. bereits vorhandenen GRC-System. Sie betonten, dass Tax Compliance keine Standalone-Lösung im Unternehmen sein dürfe und im Idealfall an vorhandene Kontrollsysteme wie das IKS, das Compliance Management System und das Risikomanagementsystem angehängt werden sollte.

Know your customer (KYC)

Die neuen Anforderungen an die Geldwäscheprävention gem. der 5.EU-Geldwäscherichtlinie stellte Dr. Tim Nikolas Müller von Allen & Overy vor. Im Gegensatz zur 4. EU-Geldwäscherichtlinie wurde die Gruppe der Verpflichteten um Kryptowährungsbörsen, Wallet-Anbieter, Kunsthändler und -vermittler (ab einem Schwellenwert über 10.000 Euro) und Personen erweitert, die geschäftlich oder gewerblich Unterstützung bei Steuerfragen leisten. Wichtige Änderungen stellen in der 5. Richtlinie die Sorgfaltspflichten (KYC-Checks) wie die Pflicht zur Einsichtnahme in das Transparenzregister oder verstärkte Sorgfaltspflichten bei Geschäftsbeziehungen in Drittländer mit hohem Risiko dar. Die Zusammenarbeit zwischen Behörden der EU-Mitgliedstaaten soll verbessert werden und der Schutz von Whistleblowern im Beschäftigungsverhältnis gestärkt werden.

Compliance Tech

Christan Götz von Warth & Klein Grant Thornton stellte moderne Analyse-Techniken und Anwendungen zur Sicherstellung der Compliance vor. Möglichst große Datenbestände zu analysieren sei einerseits wünschenswert, um qualitativ die besten Rückschlüsse ziehen zu können, andererseits müsse besonderes Augenmerk auf die Einhaltung von gesetzlichen und ethischen Vorgaben gelegt werden. Es gehe um die Fragen, welche Daten überhaupt miteinander verknüpft werden dürfen und wie heterogene Daten erfasst werden können. Clustering sei ein geeignetes Mittel, um Reviews deutlich zu beschleunigen. Gerade bei personenbezogenen Daten sei die gründliche Pseudonymisierung aber unerlässlich für DSGVO-konforme Compliance-Analysen.

Podiumsdiskussion und parallele Foren

Im Anschluss diskutierten Dr. Gisa Ortwein (Norma SE), Dr. Burkhard Schmitt (Fujitsu), Ulrich Rothfuchs (DEKRA) und Dietmar Will (AUDI AG) über Maßnahmen und Erfolgsfaktoren für eine gute Unternehmenskultur. Die Diskussion veranschaulichte, wie schwierig die Thematik aufgrund der großen Bandbreite an Mitarbeiter-Werten ist. Einigkeit herrschte, dass Führungspersönlichkeiten als Role Model vorangehen müssen und der „Tone from/at the top" stimmen müsse. Außerdem müsse man beachten, dass infor-

melle Prozesse häufig wichtiger für die Unternehmenskultur seien als formelle. Ein verstärkter Dialog in Klein(st)gruppen führe zu einer positiven Beeinflussung der Unternehmenskultur. Das Vorgehen im persönlichen Austausch „face-to-face" mit den Mitarbeitern sei hierbei am wirksamsten, allerdings komme man gerade in Großkonzernen ohne „face-to-monitor" nicht aus.

An die Podiumsdiskussion schlossen sich parallele Foren zu den Themen ePrivacy-Verordnung, Kartellrechts-Compliance und Scheinselbständigkeit an.

Die Journey der AUDI AG

Dietmar Will, Leiter Compliance/Integrität bei der Audi AG, berichtete den Teilnehmern über die Arbeit mit dem US-Monitorship im Hause. Er führte dazu aus, dass die Zahl der für die Compliance-Themen eingesetzten Mitarbeiter dafür signifikant erhöht wurde und weiter ansteigen werde, um den vielfältigen inhaltlichen und organisatorischen Aufgaben nachkommen zu können. Darüber hinaus setze man auf einen verstärkten Dialog mit Führungskräften und Mitarbeitern zum Thema, um eine genaue Diagnose stellen zu können und Fehlentwicklungen zukünftig besser zu vermeiden. Besondere Herausforderungen mit dem US-Monitorship seien insbesondere die unterschiedlichen Blickwinkel und Gesetze, die Sprache, die Mitbestimmung in Deutschland sowie eine „Flut an neuen zusätzlichen Aufgaben" wie dem Einreichen von Dokumentationen, Teilnahme an Meetings sowie der Anfertigung zahlreicher Berichte.

Compliance 2030

Zum Abschluss der Fachtagung Compliance 2019 nahm Dr. Alexander Löw, CEO der Data-Warehouse GmbH, die Teilnehmer mit auf eine Reise in das Jahr 2030. Der Fortschritt der Digitalisierung werde dafür sorgen, dass für heutige Verhältnisse unvorstellbar viele Sensoren die Menschen überall umgeben werden und „alles" online erfassen. Der ungesteuerte Informationsaustausch werde dabei eine Veränderung der Werte nach sich ziehen und steigende Rechenleistungen werden Künstliche Intelligenz und Machine Learning auf ein neues Level heben. Unternehmen werden sich an diese neue Realität anpassen müssen, der Markt werde eine hohe Geschwindigkeit vorgeben. Entsprechend werde sich auch das Berufsbild des Compliance-Officers ändern. Der Umgang mit Daten und das Thema Cybersecurity werden einen wesentlich höheren Stellenwert erreichen. Große Aufgaben sah Löw in der Lieferkettensteuerung, aufgrund der Internationalisierung und Demokratisierung von Wertedefinitionen und der IT-Kompetenz auf die Compliance zukommen.

Fachtagung Compliance 2019 in Berlin

Am 3. April 2019 fand in Berlin bereits die 5. Fachtagung Compliance statt. Christoph Bertling, Geschäftsführer der Handelsblatt Fachmedien und Dr. Joachim Schmidt, Geschäftsführer des Erich Schmidt Verlags, stimmten die Gäste auf die zahlreichen aktuellen Herausforderungen für die Compliance ein: Rechtliche Rahmenbedingungen, notwendige Wirtschaftlichkeit und technische Umsetzung der Maßnahmen. Birgit Galley, Direktorin der School of Governance, Risk & Compliance, führte durch die Veranstaltung. Das Programm können Sie sich hier [1] noch einmal anschauen.

Quellen

[1] https://www.esv.info/lp/esv-akademie/Tagungsprogramm_FachtagungCompliance2019.pdf

Neue IFRS-Standards mit Implikationen für alle Unternehmensbereiche

Nachricht vom 02.04.2019

Die internationalen Rechnungslegungsnormen IFRS sind von jeher geprägt von permanenter Weiterentwicklung und hoher Dynamik. Insbesondere die drei neuen Standards IFRS 9, IFRS 15 und IFRS 16 beinhalten wesentliche Veränderungen, die Unternehmen vor große Herausforderungen stellen können.

Die ESV-Autoren Prof. Dr. Isabel von Keitz, Rainer Grote und Marc Hansmann beleuchten diese Thematik aus unterschiedlichen Perspektiven.

IFRS 9 zu Finanzinstrumenten (incl. Hedge Accounting,) sowie IFRS 15 zu Erlösen aus Kundenverträgen waren verpflichtend bereits auf Geschäftsjahre anzuwenden, die am oder nach dem 1.1.2018 begannen. Was waren hier die größten Herausforderungen für die Bilanzierer? Welche Erfahrungen konnten Sie in der Praxis sammeln?

Isabel von Keitz: Die Unternehmen mussten in ihren Konzernabschlüssen 2018 mit IFRS 9 und IFRS 15 zwei „gewichtige" Neuregelungen erstmalig anwenden, die mit einem Umfang von 976 Seiten über 20 Prozent des gesamten Regelwerks des IASB ausmachen. Da grundsätzlich alle Unternehmen Finanzinstrumente und Erlöse aus Kundenverträgen zu bilanzieren haben, hat sich die Mehrheit der Unternehmen zusammen mit ihren Beratern bzw. Wirtschaftsprüfern mit den umfangreichen Änderungen beschäftigen müssen.

Die tatsächlichen Auswirkungen auf den Konzernabschluss waren hingegen grundsätzlich – abhängig von Ausmaß und Komplexität z.B. der Finanzinstrumente – sehr unterschiedlich. So haben Auswertungen der Halbjahresabschlüsse gezeigt, dass das Ausmaß der Auswirkungen der Erstanwendung von IFRS 9 auf das Eigenkapital von 0 Prozent bis knapp 40 Prozent beträgt.

Welche Erfahrungen konnten Sie in der Praxis sammeln?

Marc Hansmann: Eine Herausforderung in der Praxis bei der Erstanwendung der neuen IFRS bestand darin, dass die Anwendung nicht nur Implikationen für das Rechnungswesen, sondern auch für andere Unternehmensbereiche hat. Die Umstellung auf das „expected loss"-Modell wirkt sich z.B. in weiten Teilen eines Unternehmens aus, da auch „normale" Forderungen gegenüber Kunden betroffen sind. Für eine korrekte Bilanzierung bedarf es nun unter Umständen des Inputs von Kundenmanagern, die bislang kaum Berührungspunkte mit der Rechnungslegung hatten.

Welche Rolle spielt dabei das jeweilige Geschäftsmodell eines Unternehmens?

Rainer Grote: Im Rahmen der Erstanwendung des IFRS bestand in der Praxis eine große Herausforderung in der Würdigung der Geschäftsmodelle ihres Unternehmens sowie der prüfungssicheren Do-

kumentation der IFRS 15-Anwendung auf diese Modelle. Die Umsetzung des IFRS 15 führte hier z.T. zu erheblichem Mehraufwand, obwohl sich die Darstellung der VFE-Lage im Resultat nicht ändert.

Der IFRS 16 zu Leasingverhältnissen ist seit dem 01.01.2019 verpflichtend. Insbesondere Leasingnehmer sind von den Novellierungen betroffen. Wie können diese sich auf die IFRS 16 vorbereiten?

Marc Hansmann: In der Praxis stellt insbesondere die systematische und zentrale Erfassung aller Leasingverhältnisse im Unternehmen eine Herausforderung dar. Während Mietverträge über Gebäude regelmäßig zentral administriert werden, gilt es nun auch z.B. die gemieteten Drucker und Kopiergeräte zentral zu erfassen. Die umfangreichere Bilanzierung beim Leasingnehmer verursacht insofern erhebliche Umstellungskosten und erfordert frühzeitige Maßnahmen zur Anpassung der Prozesse und Systeme innerhalb des Unternehmens.

Rainer Grote: Mit IFRS 9, 15 und 16 haben die Unternehmen innerhalb kurzer Zeit drei wichtige neue Standards umzusetzen, die zahlreiche Implikationen auch für Funktionen außerhalb des Rechnungswesens mit sich bringen. Die Unternehmen mussten bzw. müssen noch für IFRS nicht nur in der Bilanzierungsabteilung und den jeweiligen IT-Systemen neue Anforderungen umsetzen, sondern sahen und sehen sich auch mit einem verstärkten Kommunikations- und Schulungsbedarf innerhalb ihrer Organisation konfrontiert.

Mit welchen Änderungen ist in der Zukunft zu rechnen? An welchen Aktualisierungen arbeitet der IASB momentan?

Isabel von Keitz: Nachdem der IASB sein Regelwerk in den letzten Jahren zunächst mit IFRS 10, 11 und 12, die die Konzernrechnungslegung betreffen, und in den Jahren 2018 und 2019 dann mit IFRS 9, 15 und 16 umfangreich geändert hat, sind vergleichbar umfassende Änderungen aktuell für die kommenden Perioden (noch) nicht in Sicht. Dies ist nicht nur aus Sicht der IFRS-Anwender zu begrüßen, für die jede Änderung mit zum Teil erheblichen Aufwand verbunden ist, sondern auch aus Sicht der Adressaten, da die Änderungen auch bei retrospektiver Anwendung eine Zeitreihenanalyse der Abschlüsse erschweren.

Marc Hansmann: Dennoch sollten die Anwender den Work-Plan des IASB weiterhin genau im Auge behalten und frühzeitig prüfen, welche Agendapunkte ggf. Auswirkungen auf das eigene Unternehmen haben könnten. Neben den regelmäßigen „Annual Improvements" an bestehenden Standards sind dies aktuell vor allem die sogenannte „Disclosure Initiative" sowie der IFRS 17 zu Versicherungsverträgen.

Ihr gemeinsames Buch „IFRS auf einen Blick" stellt eine gelungene Verknüpfung von Wissenschaft und Praxis dar. Welche Erfahrungen konnten Sie in den jeweiligen Bereichen machen und wie hat sich dies auf die Inhalte und die Aufbereitung dieses Buches ausgewirkt?

Marc Hansmann: Die IFRS sind in der Unternehmenspraxis an weit mehr Stellen von Bedeutung, als dies auf den ersten Blick offensichtlich ist. Natürlich sind im externen Rechnungswesen eines Konzerns IFRS-Kenntnisse unabdingbar und regelmäßig auch in großem Umfang vorhanden.

Aber auch ein Controller muss IFRS-Zahlen zumindest „lesen" können. Gleichfalls sind IFRS-Grundkenntnisse für Produkt- oder Kundenmanager wichtig, um bei der Vor- und Nachkalkulation von Kundenaufträgen einen sinnvollen Plan-Ist-Vergleich zu ermöglichen. Ganz aktuell kann z.B. der IFRS 15 für einen Vertriebsmanager Auswirkungen haben, wenn Einmalzahlungen des Kunden ggf. nicht mehr in der Periode, in der sie gezahlt werden, auch als Umsatz gezeigt werden, sondern stattdessen über die Projektlaufzeit zu verteilen sind. Letztendlich werden auch die Kennzahlen, die in die Bonusberechnung einfließen, regelmäßig basierend auf IFRS-Werten ermittelt, so dass in der Personalabteilung entsprechende Kenntnisse notwendig sind. Unser Werk richtet sich an all diese und weitere Funktionen im Unternehmen. Das Ziel dieses Buches ist es, diesen Personen schnell und fundiert ein Verständnis der IFRS zu ermöglichen.

Isabel von Keitz: Bei der didaktischen Aufbereitung des Werkes kam uns die Erfahrung in der Lehre sehr zugute. Ebenso wie jene Mitarbeiter eines Unternehmens, die nicht in der Grundsatzabteilung zur Bilanzierung arbeiten, müssen auch die meisten Studierenden die mittlerweile fast 4.000 Seiten umfassenden Regelungen des IASB nicht alle im Detail kennen. Vielmehr sollten diese die grundlegende Systematik des IASB-Regelwerkes und die wichtigsten Bilanzierungs- und Bewertungsregeln kennen und auf Beispiele anwenden können. Daher haben wir uns bewusst für eine konsequente Verwendung von Grafiken und Beispielen sowie einen modularen Aufbau entschieden: Studierende wie auch Praktiker können sich so zielgerichtet und effizient mit den für sie relevanten Themen auseinandersetzen.

Zu den Personen

Prof. Dr. Isabel von Keitz war nach ihrer Promotion zunächst einige Jahre bei einem DAX-Unternehmen und einer Wirtschaftsprüfungsgesellschaft tätig, wo sie jeweils u.a. IFRS-Projekte betreute. Seit 2001 hat sie eine Professur für BWL, insb. internationales Rechnungswesen, an der FH Münster inne. Sie ist Autorin zahlreicher Fachpublikationen und weiterhin beratend für Unternehmen und Wirtschaftsprüfungsgesellschaften tätig.

WP/StB Rainer Grote war zunächst in einer internationalen Wirtschaftsprüfungsgesellschaft tätig und anschließend als Bereichsleiter für die Rechnungslegung nach internationalen Rechnungslegungsstandards bei einem Joint Venture von zwei DAX-Unternehmen verantwortlich. Nunmehr leitet er als Gesellschaftergeschäftsführer einer renommierten mittelständischen Wirtschaftsprüfungsgesellschaft den Bereich internationale Abschlussprüfungen.

Marc Hansmann begann seine Laufbahn in der IFRS-Grundsatzabteilung eines großen deutschen Medienkonzerns. Anschließend unterstützte er als Unternehmensberater verschiedene Großkonzerne in Fragen der IFRS-Konzernrechnungslegung. Nach Studien u.a. in Berkeley, Münster und Wuppertal ist er aktuell im Bereichscontrolling eines Dienstleistungsunternehmens tätig. Parallel unterrichtet er seit vielen Jahren als Lehrbeauftragter für externes und internes Rechnungswesen.