Transparency fordert Einführung eines Unternehmensstrafrechts

Nachricht vom 23.12.2014

Deutschland brauche ein Unternehmensstrafrecht, fordert die Antikorruptionsorganisation TI. Denn Korruption ist keine Ordnungswidrigkeit und dürfe demnach auch nicht als Kavaliersdelikt behandelt werden.

Die Einführung eines Unternehmensstrafrechts wird seit längerem kontrovers diskutiert. Nun scheint wieder etwas mehr Bewegung in das Thema zu kommen. Anfang Dezember fand eine erste Anhörung zum geplanten Gesetzesentwurf im Bundesjustizministerium statt.

„Haltet den Fahrraddieb!"

Im deutschen Recht existiert ein Missverhältnis. Hierauf weist die Geschäftsführerin von Transparency Deutschland, Anna-Maija Mertens, im Interview mit COMPLIANCEdigital (http://www.compliancedigital.de/ce/korruption-durch-unternehmen-ist-nur-eine-ordnungswidrigkeit/detail.html) hin. Unternehmen würden heute bei Korruptionsverstößen – wenn sie denn aufgedeckt werden – lediglich durch das Ordnungswidrigkeitenrecht belangt. Dagegen handelt es sich beim Fahrraddiebstahl um eine Straftat. „Ordnungswidrigkeit klingt nach Lappalie; man zahlt sein Bußgeld wie beim Falschparken. Das wird den wirtschaftlichen und gesellschaftlichen Schäden der Korruption nicht gerecht."

Korruption, so Mertens weiter, sei aber kein „Kavaliersdelikt". Hier sieht Transparency den Gesetzgeber gefordert. Korruption müsse endlich als echte Straftat behandelt werden, indem ein Unternehmensstrafrecht eingeführt wird, wie z.B. in den Niederlanden, Dänemark, Polen oder Frankreich. Dabei sollten nicht nur finanzielle Strafen in Betracht gezogen werden. Viel effektiver wäre es, wenn Unternehmen auch von öffentlichen Aufträgen ausgeschlossen werden könnten. Zudem ginge auch mit einem Strafurteil eines Gerichtes ein hoher Imageverlust einher.

Politik prüft Einführung eines Unternehmensstrafrechts

Die gute Nachricht ist, dass Transparency nicht ganz auf taube Politiker-Ohren stößt. So ist im Koalitionsvertrag zwischen CDU/CSU und SPD festgehalten, dass ein Unternehmensstrafrecht für multinationale Konzerne zumindest geprüft werde. Konkret heißt es dort: „Mit Blick auf strafbares Verhalten im Unternehmensbereich bauen wir das Ordnungswidrigkeitenrecht aus. Wir brauchen konkrete und nachvollziehbare Zumessungsregeln für Unternehmensbußen. Wir prüfen ein Unternehmensstrafrecht für multinationale Konzerne..." (Koalitionsvertrag 2013; 5. Moderner Staat, innere Sicherheit und Bürgerrechte).

Von Seiten der Regierungsparteien erhält die Antikorruptionsorganisation vor allem Unterstützung von den Sozialdemokraten. So hat NRW-Justizminister Thomas Kutschaty (SPD) bereits im Jahr 2013 einen Gesetzesentwurf für ein Unternehmensstrafrecht in den Bundesrat eingebracht. Beistand für seine Forderung erhält Kutschaty von Hamburgs Justizsenatorin Jana Schiedek (SPD), die die derzeitige Regelung ebenfalls für unzureichend hält.

Auch die beiden Oppositionsparteien Bündnis90/Die Grünen und Die Linke fordern die Einführung eines Unternehmensstrafrechts. Die Unionsparteien sind bei dem Thema reservierter. Man verschließe sich zwar nicht der Diskussion, stehe aber dem Entwurf von Kutschaty „etwas zurückhaltender" gegenüber, so die Justizministerin von Mecklenburg-Vorpommern, Uta-Maria Kuder (CDU).

Unternehmen stehen Verschärfung des Unternehmensstrafrechts kritisch gegenüber

Auch die Wirtschaft steht einer Verschärfung kritisch gegenüber. In der aktuellen Stellungnahme (http://www.dihk.de/presse/thema-der-woche/thema-der-woche/2014/tdw-04122014/at_download/file?mdate=1417703219647) wendet sich der Deutsche Industrie- und Handelskammertag (DIHK) gegen eine „pauschale Kriminalisierung von Unternehmen und von wirtschaftlichen Handeln". Laut Auffassung des DIHK würde ein Unternehmensstrafrecht „einen weiteren Baustein in der negativen Darstellung von Unternehmen in der Öffentlichkeit darstellen" (Siehe hierzu die Meldung vom 09.12.2014 auf COMPLIANCEdigital.de (http://www.compliancedigital.de/ce/dihk-mehr-compliance-weniger-strafrecht/detail.html)).

Was ist ein Benefit und was ist ein Vorteil?

Nachricht vom 22.12.2014

In einem Grundsatzurteil hat das U.S.-Berufungsgericht die strafrechtliche Verfolgung von Insider-Fällen neu geregelt. Die Entscheidung hat auch Auswirkungen auf die Arbeit der SEC.

Im Fall U.S. v. Newman, Case No. 13-1837 (2d Cir. Dec. 10, 2014) hat das U.S.-Berufungsgericht eine Grundsatzentscheidung gefällt. Die Entscheidung soll die strafrechtliche Verfolgung von sogenannten „Tipper"-Fällen eingrenzen.

Nach dem Urteil kann nur dann gegen den Empfänger einer Insiderinformation vorgegangen werden, wenn die Staatsanwaltschaft beweisen kann, dass dieser wusste, dass der Informant sich von den kursrelevanten Information einen persönlichen Vorteil („benefit") versprach.

Auch die Frage, was ein „Vorteil" ist, muss nach dem Urteil spezifiziert werden. Nach der neuen Regelung muss ein gewährter Vorteil „objektiv" und „messbar" sein.

Staatsanwaltschaft und SEC wird Arbeit erschwert

Die Entscheidung hat auch Auswirkungen auf die zukünftige Arbeit der Staatsanwaltschaft sowie der US-Börsenaufsicht (Security Exchange Commission – SEC). Beiden Behörden können nun nicht mehr so einfach gegen Informationsempfänger vorgehen, die nicht direkt in Beziehungen zu dem Informanten stehen. Die Vorsitzende der SEC, Mary Jo White, zeigt sich daher enttäuscht von dem Urteil. White bezeichnet die Entscheidung als „zu eng".

In dem hier entschiedenen Fall handelte es sich bei den Angeklagten nicht um Mitarbeiter oder Unternehmensinsider im traditionellen Sinn, sondern um externe Empfänger der kursrelevanten Insiderinformation ("downstream tippees"). Diese waren von der eigentlichen Informationsquelle mehrere Ebenen entfernt.

Anna Rode, Chefredakteurin Compliance Puls – Der US-Compliance Tracker (www.compliancepuls.com), anna.rode@compliancepuls.com

Sieben Sicherheits-Trends für die Cyber-World für 2015

Nachricht vom 19.12.2014

Unternehmen sind mit der Abwehr von Cyber-Angriffen überfordert. Unternehmen müssen daher in die IT-Compliance investieren. Für nächstes Jahr beschreibt der TÜV Rheinland sieben Cyber Security-Trends.

Erst diese Woche hat Sony Pictures den Film „The Interview" aufgrund einer Terrorwarnung zurückgezogen. Hacker aus Nordkorea sollen in die Firmennetze von Sony eingedrungen sein und über 100 Terabyte an Daten erbeutet haben. Der Schaden für Sony geht in die Millionen. Einige Kommentatoren sehen sogar die Zukunft von Sony Pictures als Filmstudio in Gefahr.

Angriffe auf Firmennetzwerke werden – so viel ist sicher – auch im nächsten Jahr viele IT-Sicherheitsabteilungen beschäftigen. Besonders im Fokus stehen dabei nach Meinung von Björn Haan, Geschäftsführer der TÜV Rheinland i-sec, vor allem Lieferanten und Medizin-Geräte.

Die Einschätzung basiert auf einer aktuellen Marktanalyse in Deutschland sowie weltweit von Security Analysts und Consultants bei TÜV Rheinland. Die TÜV-Experten für IT-Sicherheit heben sieben Themen hervor, die IT-Verantwortliche in den Unternehmen im Auge haben müssen.

Sieben Trends für 2015

1. IT-Compliance: Angesichts der zunehmenden Bedrohung und den verschärften Regeln – genannt seien hier das deutsche IT-Sicherheitsgesetz sowie die EU-Datenschutzreform – müssen und werden die Ausgaben in die IT-Sicherheit steigen.
2. Rückgriff auf externe Experten: Durch die Zunahme von gezielten komplexen Angriffen, genannt ATP (Advanced Persistent Threats) werden Unternehmen verstärkt auf externe Hilfe zurückgreifen müssen. Besonders bedroht sind vor allem Mittelständler, den vermeintlich schwächsten Glied in der Kette. Viele von ihnen sind nach Auffassung von Haan bereits schon „kompromittiert, ohne es zu ahnen".
3. IT Security für Medizin-Geräte: Als neue Gefahr identifizieren die TÜV-Experten vor allem medizinische Geräte. Bereits seit 2014 sind z.B. Hersteller in den USA dazu verpflichtet, IT-Sicherheit schon bei der Entwicklung der Geräte zu berücksichtigen. Nach Auffassung von Haan wird diese Regelung sehr bald auch auf europäische Hersteller zukommen. Zu groß ist die Gefahr, dass die Medizin-Geräte von externen Hackern gesteuert werden.
4. Internet der Dinge (IoT): Ein Trend, der bereits 2014 sich anbahnte, ist die Vernetzung unterschiedlichster Systeme, seien es Autos, Waschmaschinen oder ganze Versorgungssysteme. In diesem Bereich hinke das Problemverständnis für die „Bedrohungslage durch Cyber-Angriffe noch sträflich hinterher", so Olaf Siemens von TÜV Rheinland.
5. Industrie 4.0: Eng verknüpft mit dem IoT ist die Industrie 4.0. Aber auch hier, so die Studienautoren, seien wesentliche Sicherheitsfragen noch ungeklärt. Hier müsse die deutsche Industrie im nächsten Jahr investieren, wenn das Vertrauen in die Cyber-Sicherheit von Grundlagentechnologien wie dem Internet der Dinge und der Cloud in der Bevölkerung wachsen soll.
6. Vernetztes Fahren: IT-Sicherheit betrifft zunehmend auch die Mobilität. Nach Auffassung von Siemens, muss „die komplette Wertschöpfungskette in der Industrie mit Hochdruck an Lösungen arbeiten, die verhindern, dass gefährliche Eingriffe in die Fahrzeug-IT von außen überhaupt möglich sind".
7. Cloud- Private: „Der Trend zur Datenwolke ist unumkehrbar", so Haan. Aufgrund der Datenskandale im letzten Jahr, bauen Unternehmen verstärkt eigene Cloud-Systeme auf. Die Herausforderung bestehe in der Zukunft darin, die „Kombination von Consumer-Cloud-Lösungen mit mobilem Zugang und sozialer Authentifizierung (Social Login, z.B. über ein soziales Netzwerk wie Facebook) zu gewährleisten und sicherzustellen, dass hierdurch die Unternehmensdaten weiterhin sicher sind. (Quelle: TÜV Rheinland)

Hintergrund: IT-Compliance

Die sieben Cyber-Security-Trends zeigen, dass Unternehmen ihre IT-spezifische Risikolage neu überdenken müssen. Wie Unternehmen wesentliche regulatorische Anforderungen an die IT identifizieren, priorisieren und effizient steuern können, erläutern die Autoren Michael Rath und Rainer Sponholz in dem Band „IT-Compliance: Erfolgreiches Management regulatorischer Anforderungen (http://www.compliancedigital.de/ce/it-compliance-7/ebook.html)". Folgende Themen stehen im Mittelpunkt des Pionierwerks zur IT-Compliance, das bereits in der zweiten Auflage vorliegt:

- Prinzipien und Rechtsrahmen der IT-Compliance.
- Klassifizierung und Priorisierung notwendiger Schutzmaßnahmen
- CobiT-Framework: IT-Compliance unter Einsatz des ISACA-Rahmenwerks
- IT-Compliance-Management: Organisationsformen, Instrumente, Umsetzung
- Ergänzt wird der Band mit Praxisberichten von Unternehmen wie Capgemini oder der TÜViT.

„Korruption durch Unternehmen ist nur eine Ordnungswidrigkeit"

Nachricht vom 16.12.2014

Wo steht Deutschland und was kann Deutschland von anderen Ländern in Sachen Korruptionsbekämpfung lernen? Antworten auf diese Fragen gibt Dr. Anna-Maija Mertens, Geschäftsführerin von Transparency Deutschland, im Interview mit COMPLIANCEdigital.

Vor allem bei der Umsetzung internationaler Geldwäschestandards sieht Transparency Deutschland noch Nachholbedarf. Gerade hat die Organisation den Korruptionswahrnehmungsindex 2014 (http://www.transparency.de/Corruption-Perceptions-Index-2.2569.0.html) vorgestellt. Der Index, der in diesem Jahr bereits zum 20. Mal aufgelegt wurde, misst die bei Politkern und Beamten wahrgenommene Korruption. Er umfasst 175 Länder und Territorien und basiert auf einer Vielzahl von Expertenbefragungen.

COMPLIANCEdigital: Der diesen Monat von Transparency International vorgestellte Korruptionswahrnehmungsindex 2014 stellt Deutschland mit Platz 12 ein durchwachsenes Zeugnis aus. Warum kann Deutschland damit nicht zufrieden sein?

Dr. Anna-Maija Mertens: „Deutschland liegt im europäischen Vergleich nur im Mittelfeld. Hinsichtlich vergleichbarer Rahmenbedingungen und Möglichkeiten ist Europa für uns der entscheidende Referenzrahmen, daher kann dieses Ergebnis uns nicht zufrieden stellen.

COMPLIANCEdigital: Besonderen Schutz scheint hierzulande die Finanzwirtschaft zu genießen. Bei der Umsetzung internationaler Anti-Geldwäschestandards der OECD rangiert Deutschland auf Platz 28 von 34. Was muss sich konkret ändern?

Mertens: Der Korruptionswahrnehmungsindex 2014 zeigt, dass Geldwäsche, Steuerschlupflöcher und gestohlene Vermögen Entwicklungsländer bei der Ausübung solider Regierungsführung massiv behindern. Die Länder an der Spitze des Korruptionswahrnehmungsindex sind gefordert, sich für mehr Integrität in der Finanzwirtschaft einzusetzen und ihre Bemühungen im Kampf gegen intransparentes Finanzgebaren zu verstärken.

Transparency Deutschland fordert die Bundesregierung auf, sich für eine zeitnahe Verabschiedung der vierten EU-Anti-Geldwäscherichtlinie einzusetzen, um das Aufspüren von Geldern aus illegalen Geschäften zu erleichtern. Hier bietet sich eine einmalige Gelegenheit, den Aktivitäten von Kriminellen, Steuerflüchtlingen und korrupten Amtsträgern in Europa und der Welt einen Riegel vorzuschieben.

Auch der im Vergleich zum Finanzsektor zahlenmäßig wesentlich stärkere Nichtfinanzsektor, zu dem beispielsweise Immobilienmakler, Spielhallenbetreiber und Händler von Luxusgütern gehören, muss in diesem Kontext stärker berücksichtigt werden. Während die Geldwäscheaufsicht im finanziellen Sektor auf Bundesebene zentral durch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) wahrgenommen wird, ist sie im nicht-finanziellen Sektor Ländersache und uneinheitlich geregelt. Die Länder müssen die Kontrollen und ihre Aufsichtspflicht intensivieren und besser koordinieren.

COMPLIANCEdigital: Warum reicht die gesetzlich vorgeschriebene Geldwäschemeldung nach dem Geldwäschegesetz nicht aus?

Mertens: Nach § 2 Geldwäschegesetz (GwG) sind bestimmte Berufsgruppen des nicht-finanziellen Sektors hierzulande verpflichtet, Geldwäscheverdachtsmeldungen abzugeben. § 11 GwG gesteht den betreffenden Berufsgruppen, wie zum Beispiel Notaren und Wirtschaftsprüfern, allerdings weitgehende Verschwiegenheitspflichten bzw. Aussageprivilegien zu. Transparency Deutschland fordert, dass die derzeitigen Verschwiegenheitspflichten für bestimmte Berufsgruppen, die die Meldepflicht für Geldwäsche aushebeln, aufgehoben werden.

COMPLIANCEdigital: Die Koalition will ja die strafrechtliche Behandlung der Geldwäsche überarbeiten. Wie sollte aus Ihrer Sicht der Geldwäschetatbestand, also § 261 StGB, geändert werden?

Mertens: Die Bundesregierung hat sich im Koalitionsvertrag den internationalen Standards der Financial Action Task Force verpflichtet und angekündigt, den Geldwäschetatbestand (§ 261 StGB) entsprechend anzupassen. Wir begrüßen, dass die Bestechung im geschäftlichen Verkehr (§ 299 StGB) in den Vortatenkatalog des Geldwäschetatbestandes aufgenommen werden soll. Aber auch Eigengeldwäsche muss unter Strafe gestellt werden.

COMPLIANCEdigital: Wer könnte Deutschland im europäischen Vergleich der Korruptionsbekämpfung als Vorbild gelten?

Mertens: Der Europäische Integritätsbericht von Transparency International zeigt, dass weniger ganze Systeme als eher einzelne Beispiele Vorbilder sein können. Nachahmenswert sind z. B. die Regelungen Lettlands für die Veröffentlichung von Parteienspenden und Nebeneinkünften von Abgeordneten. Dort ist spätestens 15 Tage nach Eingang einer Parteispende die Stelle für Korruptionsprävention und Korruptionsbekämpfung zu informieren.

Auch in der Slowakei gibt es gute Ansätze, so ist z.B. der Zugang zu Informationen der Verwaltung besser als Deutschland geregelt. In der Slowakei wird Einzelpersonen und Organisationen das Recht auf Akteneinsicht innerhalb von zehn Tagen gewährt.

Und von der Schweiz können wir lernen, wie das Vergabewesen transparenter gestaltet werden kann. Dort werden auf der Onlineplattform www.simap.ch (http://www.simap.ch) öffentliche Ausschreibungen des Bundes und teilweise auch der Kantone detailliert dokumentiert. Es werden Auszeichnungen für das beste Preis-Leistungsverhältnis vergeben und es besteht die Möglichkeit, Anbieter auszuschließen, die falsche Angaben machen.

COMPLIANCEdigital: Gilt die Einschätzung Deutschlands auch für Compliance-Regeln in deutschen Unternehmen: Wie beurteilen Sie hier die aktuelle Situation?

Mertens: Unternehmen werden heute bei Korruption – wenn sie denn aufgedeckt wird – durch das Ordnungswidrigkeitenrecht belangt. Dagegen wird der Fahrraddiebstahl als echte Straftat angesehen. Ordnungswidrigkeit klingt nach Lappalie; man zahlt sein Bußgeld wie beim Falschparken. Das wird den wirtschaftlichen und gesellschaftlichen Schäden der Korruption nicht gerecht. Der Gesetzgeber muss sie in den Rang einer echten Straftat erheben und damit vom Geruch des sogenannten Kavaliersdeliktes befreien. Dabei kommen nicht nur finanzielle Strafen in Betracht, auch der – vorübergehende – Ausschluss von öffentlichen Aufträgen muss möglich sein. Mit einem echten Strafurteil eines Gerichtes ginge auch die immaterielle Strafe eines hohen Imageverlustes einher.

Transparency Deutschland fordert daher die Einführung eines Unternehmensstrafrechts, d.h. die Strafbarkeit eines Unternehmens, in Deutschland. Damit wäre Deutschland in guter Gesellschaft: Viele weitere kontinentaleuropäische Länder – kleinere wie die Niederlande und Dänemark, und auch größere wie Polen und Frankreich – kennen längst die Strafbarkeit von Unternehmen.

Zur Person: Dr. Anna-Maija Mertens

Dr. Anna-Maija Mertens (39) ist seit 01. Dezember 2014 neue Geschäftsführerin der Antikorruptionsorganisation Transparency International Deutschland e.V. Mertens studierte Politikwissenschaften an der Universität Münster. Von 2003 bis 2007 war sie als Ideen Mining Managerin bei der Transferstelle der Universität Münster tätig. Im Jahr 2007 wurde sie mit einer Arbeit zur Rolle der Präsidentschaft des Europäischen Rates an der Universität Münster promoviert, bevor sie zwei Jahre in einer Unternehmensberatung tätig war. Seit Januar 2010 leitete sie als Direktorin das Finnland-Institut in Berlin.

Hintergrund: Transparency International und Transparency Deutschland

Transparency International (TI) wurde 1993 vom ehemaligen Direktor der Weltbank für Ostafrika, Peter Eigen gegründet. Der Hauptsitz von Transparency International ist bis heute Berlin. TI agiert weltweit. Zurzeit verfüg TI über mehr als 90 nationale Organisationen, zu denen auch TI Deutschland gehört. Ziel von Transparency ist es, alle beteiligten Akteure aus Politik, Wirtschaft und Zivilgesellschaft zur Schaffung von Transparenz zusammen zu bringen. Transparency International Deutschland e.V. ist eine gemeinnützige und politische unabhängige Organisation. Sie wurde 2001 in München gegründet. Seit 2003 befindet sich die Geschäftsstelle in Berlin. Seit

2010 ist Prof. Dr. Edda Müller die Vorsitzende des Vereins.

Literaturhinweise

Das Buch „Korruption als Internationales Phänomen (http://www.compliancedigital.de/ce/korruption-als-internationales-phaenomen/search/korruption/target/search/ebook.html) ", herausgegeben von Prof. Dr. Matthias S. Fifka und Prof. Dr. Andreas Falke, gibt einen Überblick über die Ursachen und Auswirkungen. Zudem werden Strategien zur Bekämpfung von Korruption vorgestellt.

Das „Handbuch Compliance international" (http://www.esv.info/978-3-503-15649-8), herausgegeben von Dr. Malte Passarge und Prof. Dr. Stefan Behringer, beleuchtet die Grundlagen compliance-relevanter Rechtsgebiete. Compliance-Experten gehen besonders auf die Korruptionsbekämpfung in folgenden Ländern ein: Australien, Belgien, China, Deutschland, Frankreich, Großbritannien, Indien, Italien, Japan, Osttimor, Österreich, Polen, Russland, Schweiz, Südafrika, Südkorea, Tschechien, Türkei.

Rheinmetall hat in Griechenland Bestechungsgelder gezahlt

Nachricht vom 11.12.2014

Ob Zufall oder nicht. Einen Tag nach dem Anti-Korruptionstag der Vereinten Nationen, akzeptiert Rheinmetall einen Bußgeldbescheid. Der Vorwurf: Bestechung griechischer Offizieller.

Vorwürfe der Korruption gab es gegen die deutsche Rüstungsindustrie schon lange. Die Branche gehört aufgrund der Vielzahl von internationalen Geschäften zu den Anfälligsten. Im Mittelpunkt standen immer wieder Rüstungsgeschäfte in Griechenland. Seit dieser Woche ist es nun amtlich: Repräsentanten von Rheinmetall Defence Electronic (RDE), eine Tochtergesellschaft der Rheinmetall AG, haben griechische Offizielle Bestechungsgelder gezahlt, um an lukrative Aufträge in Griechenland zu gelangen.

Papperger: „Herumlavieren hätte nichts gebracht"

Der Vorwurf der Staatsanwaltschaft Bremen lautete, dass RDE verdächtige Zahlungen an Vertriebspartner nicht aufgedeckt und unterbunden hat. Insgesamt muss Rheinmetall eine Strafe in Höhe von 37,07 Millionen Euro zahlen. Mit der Zahlung des Bußgeldes endet das Unternehmensstrafverfahren. Das eigentliche Bußgeld betrage dabei lediglich 300.000 Euro. Der Großteil der Strafe wegen Korruption in Höhe von 36,77 Millionen Euro sind Gewinne, die beim Verkauf des Luftabwehrsystem Asrad angefallen sind. Da dieser Auftrag aufgrund von Korruption zustande gekommen ist, schöpft die Justiz diesen Gewinn nun ab. Laut Berechnungen der Süddeutschen Zeitung müsse der Konzern zudem mit einer Steuernachzahlung von 6,4 Millionen Euro rechnen, da die Bestechungsgelder unrechtmäßig als Betriebsausgaben abgerechnet wurden.

In einem Interview mit der Süddeutschen Zeitung gab sich Armin Papperger, Vorstandschef der Rheinmetall AG, einsichtig. Bei Rheinmetall seien Fehler gemacht worden, wofür das Unternehmen nun gerade stehen müsse. „Herumlavieren hätte nichts gebracht", so Papperger.

Rheinmetall kooperierte mit den Behörden

Neben den staatsanwaltlichen Ermittlungen bemühte sich auch Rheinmetall um Aufklärung der Vorwürfe. Die eigenen Ermittlungsergebnisse seien identisch mit denen der Staatsanwaltschaft, betonte der von Rheinmetall beauftrage Anwalt Hans-Peter Huber. Laut Papperger bescheinigte die Staatsanwaltschaft der Rheinmetall AG, dass sich das Unternehmen den Vorwürfen gestellt und zur Aufklärung beigetragen habe.

Mehrere Manager müssen nun mit Anklagen rechnen. Ferner hat Pappberger angekündigt, dass die Compliance-Abteilung bei Rheinmetall neu aufgestellt werde, „damit uns so etwas nicht wieder passiert". (Quelle: Rheinmetall, Süddeutsche Zeitung)

Der Fall zeigt, dass Korruption kein originäres griechisches, ukrainisches oder chinesisches Problem ist. Korruption ist vielmehr ein internationales Phänomen und könne daher auch nur gemeinsam bekämpft werden. (siehe hierzu auch die Nachricht auf COMPLIANCEdigital (http://www.compliancedigital.de/ce/praxisleitfaden-korruptionsbekaempfung/detail.html) vom 10. Dezember).

Hintergrund: Rheinmetall AG

Der 1889 gegründete Automobilzulieferer und Rüstungskonzern erwirtschaftete 2013 einen Umsatz von 4,613 Milliarden Euro. Insgesamt beschäftigte der Konzern zum Jahresende 2013 rund 21.000 Mitarbeiter. Die Rüstungssparte Rheinmetall Defence erwirtschaftete 2,155 Milliarden Euro und eine Rendite (EBIT) von 0,2 %.

Literaturhinweise

Ob „Korruption als internationales Phänomen", „Praxishandbuch Korruptionscontrolling", „Methoden der Korruptionsbekämpfung" – wer sich mit dem Problem Korruption befasst, findet auf COMPLIANCEdigital (http://www.compliancedigital.de/contenttyp_title_plural/eBooks/q/korruption/suche.html) einen reichhaltigen Literaturüberblick.

Praxisleitfaden Korruptionsbekämpfung

Nachricht vom 10.12.2014

Anlässlich des Welt-Anti-Korruptionstages der UNO hat das Deutsche Global Compact Netzwerk (DGCN) und das Deutsche Institut für Compliance (DICO) den Leitfaden zur Korruptionsbekämpfung aufgelegt.

Korruption ist nicht nur ein Problem sogenannter Dritte-Welt-Länder. Laut EU-Kommission entsteht allein in der Europäischen Union durch Korruption ein Schaden von 120 Milliarden Euro pro Jahr. Erst im November wurde der ehemalige portugiesische Ministerpräsident José Sócrates nach Ermittlungen wegen Steuerhinterziehung, Geldwäsche und Korruption festgenommen.

Auch Deutschland ist nicht frei von Korruption. Zwar belegt die Bundesrepublik laut des aktuellen Korruptionswahrnehmungsindex lediglich Platz zwölf. Großen Nachholbedarf sieht Transparency Deutschland (http://www.transparency.de/Corruption-Perceptions-Index-2.2569.0.html) aber vor allem noch beim Thema intransparentes Finanzgebaren.

Deutschland hat Korruption den Kampf angesagt

Die Korruptionsbekämpfung in Deutschland hat in diesem Jahr einen deutlichen Schub bekommen. Nachdem die Bundesregierung das Übereinkommen der Vereinten Nationen (UNO) gegen Korruption im Dezember 2003 unterzeichnet hat, dauerte es noch weitere elf Jahre, bis das Dokument am 12. November ratifiziert werden konnte. Eines der größten Hin-

dernisse war der Straftatbestand der Abgeordnetenbestechung. Nach einem jahrelangen parlamentarischen Gezerre wurde die Abgeordnetenbestechung im September vom Gesetzgeber konkretisiert.

Die Bundesrepublik war aufgrund der langen Verhandlungen eines der letzten Länder, die die Anti-Korruptionskonvention der Vereinten Nationen unterzeichnet hat (COMPLIANCEdigital (http://www.compliancedigital.de/ce/deutschland-schliesst-zum-rest-der-welt-auf/search/korruption/target/search/detail.html) berichtete).

First Aid Kid für Korruptionsbekämpfung

Unternehmen in Deutschland müssen daher die Aktivitäten bei derKorruptionsbekämpfung und Compliance ausweiten. Der vom DGCN und DICO gemeinsam aufgelegte Anti-Korruptionsleitfaden soll als eine Art „First Aid Kid" deutschen Unternehmen dabei helfen, fit zu werden bei der Anti-Korruptionsbekämpfung. Der Leitfaden vermittelt auf allgemeinverständlicher Weise die Grundlagen der Korruptionsbekämpfung. Konkret werden auch Aspekte wie Sponsoring oder der richtige Umgang mit Einladungen in VIP-Lounges thematisiert.

Den Leitfaden Korruptionsbekämpfung können Sie auf den Seiten des Deutsche Global Compact Netzwerk herunterladen (http://www.globalcompact.de/publikationen/korruptionspr%C3%A4vention-ein-leitfaden-f%C3%BCr-unternehmen). (Quelle: DGCN)

Literaturhinweise

Das Buch „Korruption als Internationales Phänomen (http://www.compliancedigital.de/ce/korruption-als-internationales-phaenomen/search/korruption/target/search/ebook.html)", herausgegeben von Prof. Dr. Matthias S. Fifka und Prof. Dr. Andreas Falke, gibt einen Überblick über die Ursachen und Auswirkungen. Zudem werden Strategien zur Bekämpfung von Korruption vorgestellt.

Das „Handbuch Compliance international" (http://www.esv.info/978-3-503-15649-8), herausgegeben von Dr. Malte Passarge und Prof. Dr. Stefan Behringer, beleuchtet die Grundlagen compliance-relevanter Rechtsgebiete. Compliance-Experten gehen besonders auf die Korruptionsbekämpfung in folgenden Ländern ein: Australien, Belgien, China, Deutschland, Frankreich, Großbritannien, Indien, Italien, Japan, Osttimor, Österreich, Polen, Russland, Schweiz, Südafrika, Südkorea, Tschechien, Türkei, USA.

DIHK: Mehr Compliance, weniger Strafrecht

Nachricht vom 09.12.2014

Der DIHK sieht die Einführung eines Unternehmensstrafrechts kritisch. In einer Stellungnahme fordert der Verband stattdessen mehr Anreize für Compliance.

Die Einführung eines Unternehmensstrafrechts steht seit langem auf der politischen Agenda. Bereits im September 2013 hatte Thomas Kutschaty (SPD), Justizminister in Nordrhein-Westfalen, den Gesetzesentwurf „Einführung der strafrechtlichen Verantwortlichkeit von Unternehmen und sonstigen Verbänden" vorgelegt. Bei den Kollegen aus den Ländern ist er auf positive Resonanz gestoßen (COMPLIANCEdigital (http://www.compliancedigital.de/ce/unternehmensstrafrecht-neue-gesetzesinitiative-aus-nrw-2/search/unternehmensstrafrecht/target/search/detail.html) berichtete).

Die Forderung nach einem eigenen Unternehmensstrafrecht floss auch in den Koalitionsvertrag ein. Dort heißt es, dass die Einführung eines Unternehmensstrafrechts „für multinationale Konzerne" geprüft werde. Eine erste Anhörung zum Gesetzesvorhaben wurde vom Bundesjustizministerium durchgeführt. Der Deutsche Industrie- und Handelskammertag (DIHK) als Interessensvertreter der deutschen Wirtschaft sieht die Einführung eines Unternehmensstrafrechts kritisch.

DIHK gegen pauschale Verurteilung durch ein Unternehmensstrafrecht

In der aktuellen Stellungnahme (http://www.dihk.de/presse/thema-der-woche/thema-der-woche/2014/tdw-04122014/at_download/file?mdate=1417703219647) des DIHK wendet sich der Interessensverband gegen eine „pauschale Kriminalisierung von Unternehmen und von wirtschaftlichen Handeln". Laut Auffassung des DIHK würde ein Unternehmensstrafrecht „einen weiteren Baustein in der negativen Darstellung von Unternehmen in der Öffentlichkeit darstellen". Wirtschaft sei aber nicht „gleichzusetzen mit Profiterhöhung um jeden Preis oder gar Ausbeutung". Vielmehr schaffe die Wirtschaft Wohlstand und Arbeitsplätze. Zudem sei die Wirtschaft ein integraler und wichtiger Bestandteil der Gesellschaft, so der DIHK.

Unternehmensstrafrecht bedroht Arbeitsplätze

Es bestehe zudem kein Regelungsbedarf. Zwar sei es richtig, dass „alle Täter, auch Unternehmen" bei Vergehen bestraft werden müssen. Jedoch wendet sich der DIHK gegen „strafrechtliche Gerichtsverfahren gegen ein Unternehmen selbst". Bemängelt wird vor allem, dass eine Anklage erhoben werden kann, ohne dass ein konkreter Täter benannt werden müsse. Dies würde ganze „Belegschaften an den Pranger" stellen, auch wenn es am Ende zu gar keiner Verurteilung kommt. Die Folgen eines solchen Szenarios seien nicht abschätzbar. So könne es passieren, dass aufgrund falscher Beschuldigungen „Arbeitsplätze vollkommen unbeteiligter Arbeitnehmer in den betroffenen Unternehmen und bei deren Vertragspartnern" gefährdet wären.

Nach Auffassung des DIHK reichen die „bisherigen Instrumente des Straf-, Gewerbe, und des Ordnungswidrigkeitsrechts (OWiG) vollkommen aus". Zwar gebe es noch Verbesserungspotenziale, jedoch bestünde keine Notwendigkeit für ein eigenes Unternehmensstrafrecht.

Anreize für Compliance erhöhen

Positiv bewertet der DIHK dagegen die Vorschläge, dass in Unternehmen angewandte Compliance-Maßnahmen sich im Strafrecht, OWiG oder Kartellrecht strafmildernd auswirken können. Unternehmen müssen demnach alles dafür tun, Straftaten zu verhindern.

Daher sei es sinnvoll, Anreize für Compliance-Systeme, gerade auch für kleinere und mittlere Unternehmen zu schaffen. Ziel müsse es sein, gemeinsam an Compliance-Systemen zu arbeiten, anstatt Unternehmen an den „medialen Pranger" zu stellen. Dies könne auch verhindern, dass „Unternehmen sich mit einem nur unzureichenden Compliance-System freikaufen können". Laut DIHK ist der „Balanceakt schwierig, aber dennoch lohnenswert".

Hintergrund zur NRW-Gesetzesinitiative zur Einführung eines Unternehmensstrafrechts

Der Vorschlag aus NRW wurde sowohl in der Öffentlichkeit als auch in der Fachwelt intensiv diskutiert. In der Ausgabe 1/2014 der Zeitschrift „Risk Fraud & Compliance" nehmen Dr. Wolfgang Hetzer (Pro) (http://www.compliancedigital.de/ce/pro-gesetzesvorschlag-zum-unternehmensstrafrecht-aus-nrw/detail.html) und RA Dr. Markus Rübenstahl (Contra) (http://www.compliancedigital.de/ce/contra-deutschland-

braucht-kein-solches-unternehmensstrafrecht/detail.html) Stellung zu der Gesetzesinitiative. Beide Beiträge stehen Abonnenten von COMPLIANCEdigital kostenfrei zur Verfügung.

Wie Geschäftsführer vergütet werden

Nachricht vom 04.12.2014

Die jetzt veröffentlichte Studie „Gehaltsindex Familienunternehmen 2014" ermöglicht seltene Einblicke in die Vergütung von Managern in deutschen Familienunternehmen.

Sie gehören zu den gut gehüteten Geheimnissen der deutschen Wirtschaft: Die Gehälter des Führungspersonals in Familienunternehmen. Gründe dafür dürften die nachhaltigen Strategien und das zurückhaltende Wirtschaften vieler Familienunternehmen sein.

Familienunternehmen fehlt der Vergleich

Diese gelebte Zurückhaltung führt auch dazu, dass die Inhaberfamilien selbst nur schwer einschätzen können, wo ihre Unternehmen im Vergleich zu anderen Marktteilnehmern einzuordnen sind. Das führt häufig zur Unklarheit über adäquate Vergütungsmodelle und die angemessene Gehaltshöhe potenzieller Geschäftsführer.

Das könnte sich nun ändern. „Der Gehaltsindex Familienunternehmen 2014 erhebt zum ersten Mal Daten über Höhe und Vergütungsmodell sowie Vertragsvarianten von Vorständen und Geschäftsführern in Familienunternehmen", sagt Dr. Detlef Keese vom Institut für Mittelstandsforschung der Universität Mannheim (ifm). Ohne vergleichbares Datenmaterial sei der „Marktwert" von Geschäftsführern nicht zu bestimmen, so Keese weiter.

„Gesellschafter können nun die Rahmenbedingungen zur Einstellung eines neuen Geschäftsführers viel besser einschätzen. So kann nun realistisch beurteilt werden, ab wann ein unbefristeter Vertrag angebracht ist oder einem Fremdgeschäftsführer Unternehmensanteile angeboten werden können", ergänzt Co-Autorin Gabriela Jaecker, Inhaberin der gleichnamigen Personal- und Nachfolgeberatung für Familienunternehmen.

Fixgehalt zwischen 121.000 und 150.000 Euro

An der nun vorgelegten Studie nahmen 310 Geschäftsführer von Familienunternehmen teil – mit teilweise überraschenden Ergebnissen: So werden 86 Prozent der Arbeitsverträge unbefristet aufgesetzt. Somit setzen Inhaberfamilien bei den Vertragsverhandlungen auf Vertrauen, Nachhaltigkeit und unternehmerische Stabilität. Die Vertragsart und Vergütungshöhe hängt dabei wesentlich mit der Unternehmensgröße, der Anzahl der Mitarbeiter, der Umsatzhöhe sowie der Exportquote zusammen. So erklärten drei Viertel der Teilnehmer, ihr Unternehmen habe eine Exportquote von über 50 Prozent.

Weitere Erkenntnis aus der Studie: Je kleiner das Unternehmen, desto höher ist die Wahrscheinlichkeit, einen unbefristeten Vertrag zu erhalten. Vergütungshöhe für Familienangehörige und Fremdgeschäftsführer Ein Jahressalär von über 200.000 Euro beziehen 54 Prozent der Befragten.

In der Regel erhalten Geschäftsführer ein Fixgehalt zwischen 121.000 und 150.000 Euro, der variable Anteil bewegt sich im Mittel zwischen 50.000 und 75.000 Euro. Unbefristet angestellte Geschäftsführer verdienen im Vergleich weniger als ihre Kollegen mit befristeten Verträgen. Dies wird jedoch durch die Langfristigkeit und Sicherheit des unbefristeten Beschäftigungsverhältnisses kompensiert. „Trotzdem sind überraschenderweise knapp 65 Prozent der Fremdgeschäftsführer unbefristet beschäftigt. Insgesamt sind 62 Prozent der befragten Geschäftsführer Angehörige der Inhaberfamilie", so Jaecker. Damit waren 38 Prozent der befragten Top-Manager Fremdgeschäftsführer.

Weitere Ergebnisse der Untersuchung:

- 90 Prozent der Geschäftsführer sind mehr als zehn Jahre im Unternehmen tätig.
- Jeder vierte Geschäftsführer ist sogar über 30 Jahre auf seiner Position.
- Knapp 75 Prozent der Befragten haben seit über fünf Jahren den Geschäftsführerposten inne.
- Lediglich ein Prozent wurde direkt als Geschäftsführer eingestellt.
- Externe Geschäftsführer erhalten im Vergleich zu den Eigengewächsen der Unternehmerfamilien aufgrund der oftmals fehlenden Firmenanteile ein deutlich höheres fixes Gehalt.

Akademischer Hintergrund ist keine Pflicht

Ein abgeschlossenes Studium ist dabei keine zwingende Voraussetzung, um als Geschäftsführer in einem Familienunternehmen Erfolg zu haben. 17 Prozent der Befragten verfügten nicht über ein abgeschlossenes Studium. Zwar wirkt sich ein akademischer Hintergrund positiv auf die Vergütung aus, aber es sind Werte wie Führungsstärke, Loyalität und Integrität sowie das Vertrauen in die Geschäftsführer, ein Unternehmen profitabel führen zu können, die höher gewertet werden.

Und umgekehrt: Was sind die Gründe bei einem Familienunternehmen anzuheuern? Flache Hierarchien, langfristige Verträge, nachhaltige Karrierewege sowie Übernahme von Verantwortung und gute Zukunftsaussichten mit unternehmerischen Entwicklungsperspektiven machen Familienunternehmen im Vergleich zu Publikumsgesellschaften bei potenziellen Managern zu attraktiven Optionen.

Literaturhinweise

Mit den unterschiedlichen Vergütungstypen im Arbeitsrecht befasst sich das Buch „Erfolgs- und leistungsorientierte Vergütung" (http://www.esv.info/978-3-503-10664-6) von Dr. Anja Mengel. Zielvereinbarungen für Mitarbeiter können mit variablen Vergütungsbestandteilen verknüpft werden. Das Buch „Arbeitsvertragliche Gestaltung von Zielvereinbarungen" (http://www.esv.info/978-3-503-09305-2) von Dr. Svenja Deich gibt darüber Auskunft.

SEC verhängt Strafe gegen HSBC

Nachricht vom 02.12.2014

Die US-Finanzaufsicht SEC geht gegen die Bank HSBC vor. Die Ermittler haben das Privatbankgeschäft von US-Kunden im Visier, in dem die Bank ohne die erforderliche SEC-Registrierung aktiv war.

Laut US-Finanzaufsichtsbehörde „Securities and Exchange Commission" (SEC) soll die schweizerische Tochter der HSBC Offshore-Konten für US-Kunden unterhalten haben, ohne jedoch über die hierfür erforderliche SEC-Registrierung zu verfügen. Insgesamt soll es sich um 368 Konten und einer Summe von insgesamt 775 Millionen Dollar gehandelt haben.

HSBC-Manager handelten ohne die erforderliche SEC-Registrierung

Die Bank hat sich nun zu der Regelverletzung bekannt und bereits die Strafe in Höhe von 12,5 Millionen Dollar akzeptiert. Die HSBC ist nicht die erste Bank, die für derartige Vergehen von der SEC belangt wurde. Im Februar dieses Jahres hatte sich die Credit Suisse mit der SEC verglichen. Damals musste die Schweizer Bank mit 196 Millionen Dollar allerdings eine deutliche höhere Strafzahlung an die SEC überweisen.

Unzureichende Compliance-Strukturen als Ursache für Gesetzesverletzungen

Als Ursache für die Gesetzesverletzung sieht die SEC darin, dass bei der HSBC Compliance-Strukturen unzureichend implementiert und überprüft worden waren. So konnten Relationship-Manager aus der Schweiz direkt mit US-Kunden verhandeln, ohne jedoch über die notwendigen US-Lizenzen zum Wertpapierhandel und Vermögensberatung zu verfügen. Bemühungen von US-Seiten der Bank, die Kunden direkt in den USA zu betreuen, wurde von den Schweizer Kollegen lange Zeit ignoriert. Sie hatten Sorge, den direkten Kundenkontakt zu verlieren.

Die Compliance-Verstöße liegt mehr als zehn Jahre zurück. Die HSBC hat sich zudem bereits 2010 aus dem grenzüberschreitenden US-Geschäft zurückgezogen und die US-Konten geschlossen bzw. entsprechend transferiert. (Quelle: SEC)

Anna Rode, Chefredakteurin Compliance Puls – Der US-Compliance Tracker (www.compliancepuls.com), anna.rode@compliancepuls.com

Korruptionsvermeidung in der Gesundheitsbranche

Nachricht vom 27.11.2014

Der Bundesverband Medizintechnologie tritt dafür ein, dass Kooperationen zwischen Unternehmen und Ärzten auch weiterhin möglich sein sollen. Jetzt wurde dazu der neue Kodex für Medizinprodukte vorgestellt.

Auch in der Gesundheitsbranche steht das Thema Compliance ganz oben auf der Tagesordnung. Der Grund hierfür ist u.a. die derzeit diskutierte neue Antikorruptionsregelung im Strafrecht. Healthcare Compliance, also das Einhalten von Regeln für die Zusammenarbeit in der Gesundheitswirtschaft, spiele daher auch in der alltäglichen Praxis eine immer größere Rolle.

Sinnvolle Kooperation darf nicht „kriminalisiert werden"

Auf der 6. BVMed-Healthcare Compliance-Konferenz in Berlin forderte die stellvertretende Vorstandsvorsitzende des Bundesverbandes Medizintechnologie (BVMed), Christiane Döring, dass die Zusammenarbeit zwischen Ärzten, medizinischen Einrichtungen und Unternehmen aus der Gesundheitsbranche nicht „kriminalisiert werden" dürfe.

Die neue Antikorruptionsregelung müsse nach Ansicht von Döring sicherstellen, „dass Kooperationen zwischen ärztlichen und nichtärztlichen Leistungserbringern, die der Verbesserung der Patientenversorgung dienen, auch weiterhin möglich sind". Insgesamt dürfen die neuen Anforderungen nicht zu „überzogenen Anforderungen führen, die die sinnvolle Zusammenarbeit zwischen Unternehmen und Ärzten" behindere.

Kodex für Medizinprodukte

Um Ärzten, medizinischen Einrichtungen und Unternehmen die gemeinsame Arbeit zu erleichtern, stellten Rechtsanwalt Peter Dieners und BVMed-Geschäftsführer Joachim M. Schmitt den überabeiteten Kodex Medizinprodukte vor. Der neue Kodex, den Sie hier (http://www.bvmed.de/download/kodex-medizinprodukte.pdf) einsehen können, enthalte konkrete Verhaltensregelungen für die Bereiche Forschung und Entwicklung, Drittmittelkonten, Fort- und Weiterbildung, Spenden, Geschenke und Beraterverträge. In dem Kodex sind die folgenden vier Grundprinzipien verankert:

- Trennungsprinzip: Zuwendungen dürfen nicht im Zusammenhang mit Beschaffungsentscheidungen stehen;
- Transparenzprinzip: Jede Zuwendung und Vergütung muss offengelegt werden;
- Dokumentationsprinzip: Alle Leistungen müssen schriftlich festgehalten werden;
- Äquivalenzprinzip: Leistung und Gegenleistung müssen in einem angemessenen Verhältnis stehen.

Neben dem Kodex seien für die MedTech-Unternehmen die Etablierung und die fortlaufende Überwachung eines effektiven Healthcare-Compliance-Systems von großer Bedeutung, so Dr. Adem Koyuncu von der internationalen Anwaltskanzlei Covington & Burling. „Ein Compliance-System muss auch gelebt werden", so Koyuncu. Sowohl das „Compliance Monitoring" als auch das „Compliance Auditing" durch unabhängige Auditoren müsse in Unternehmensrichtlinien abgebildet werden. Koyuncu: „Das ist in der Praxis häufig nicht oder nur unzureichend umgesetzt."

Healthcare Compliance: Nicht in den Verdacht von Korruption geraten

Damit Ärzte, medizinische Einrichtungen und Vertreter der Medizinprodukte-Industrie nicht in den Verdacht der Korruption geraten, betreibt der BVMed die Aufklärungskampagne „MedTech Kompass" (www.medtech-kompass.de). Mit diesem positiven Informationsansatz versuche der Verband, so Joachim M. Schmitt, die Prinzipien einer guten und transparenten Zusammenarbeit bekannter zu machen. Der neue Kodex kommuniziere dabei die wichtigsten Prinzipien der Healthcare Compliance. (Quelle: BVMed)

Meine Krankendaten sind sicher, oder?

Nachricht vom 26.11.2014

Die Frage, wie sicher sensible Krankendaten geschützt sind, wird allzu oft vernachlässigt, ist Stephan Brack überzeugt. Die Gesundheitsbranche muss daher dringend in IT-Sicherheit investieren.

Wie viel Google über einen weiß, lässt sich mittlerweile leicht herausfinden. (Siehe zu diesem Thema der Artikel: „Was weiß Google von mir?" auf Tagesspiegel (http://www.tagesspiegel.de/medien/digitale-welt/breite-datenspuren-was-weiss-google-von-mir/11014892.html). Einige Daten geben wir freiwillig in unseren Social-Media-Profilen preis. Andere Daten wiederum werden mit Hilfe von Bewegungsprofilen oder Suchverläufen erstellt. Heute weiß Google oftmals schneller als der Ehemann, ob z.B. Nachwuchs geplant ist oder eventuell schon unterwegs ist.

Und der Datenpool wird immer größer: Erste Versicherungen planen, Daten, die mit Hilfe von sogenannten Fitnessarm-

bändern oder anderen Devices gesammelt werden, direkt auszuwerten, um so maßgeschneiderte Angebote für die Versicherungsnehmer zu stricken – „Wer gesünder lebt, zahlt auch weniger".

Leichtsinniger Umgang mit Krankendaten

Doch was passiert, wenn Angaben zu Krankheiten in die Öffentlichkeit gelangen? An diesem Punkt kann es für Betroffene gefährlich werden, sobald die Daten in falsche Hände geraten. Sind die Krankendaten erst einmal öffentlich, können Versicherer, Arbeitgeber oder auch Vermieter darauf zugreifen. Wenn die „Daten erst einmal weg sind, können sie überall wieder auftauchen – ob man will oder nicht."

Noch schlimmer sei es allerdings, wenn die Daten gefälscht werden, wichtige Gesundheitsinformationen verschwinden oder die Daten dafür genutzt werden, ganze Identitäten zu stehlen, so Stephan Brack, CEO der Protected Networks GmbH.

Wie leicht man an sensible persönliche Krankendaten gelangen kann, hat im Sommer ein Test der Rheinischen Post (http://www.rp-online.de/wirtschaft/unternehmen/so-wird-meine-krankenversicherung-gekapert-aid-1.4341498) gezeigt. Mit nur wenigen Angaben, wie Name und Geburtsdatum, war es den Reportern möglich, an sensible Krankendaten von dritten Personen zu gelangen. Der Grund für die Sicherheitspannen liege in den mangelhaften IT-Sicherheitsvorkehrungen in Krankenhäusern, Versicherungen und Behörden.

Krankenhäuser müssen IT-Sicherheit überprüfen

Als erste präventive Maßnahme müssen Behörden und Unternehmen in der Gesundheitswirtschaft die interne IT-Infrastruktur überprüfen. „Nur so kann sich zum Beispiel eine Klinik in kurzer Zeit darüber im Klaren werden, wer auf die enorme Menge Patientendaten überhaupt Zugriff hat und hatte", sagt IT-Experte Brack. Anhand der ersten Überprüfung wird sehr schnell klar, wer alles noch Zugriff auf die Serverdaten hat.

Nach Meinung von Brack gehöre das „Risiko-Management und Datensicherheit in der Gesundheitsbranche zur Sicherheit des Patienten dazu. Sich zumindest ein Bild über die hausinternen IT-Strukturen zu machen kann die Augen öffnen". Sollte die Überprüfung eine saubere IT-Struktur zu Tage fördern, so Brack weiter, untermauert das nur die „Wirksamkeit des bisherigen Sicherheitskonzepts", und würde sicherlich auch viele Patienten beruhigen. (Quelle: Protected Networks)

Interne Revision zwischen Wunsch und Wirklichkeit

Nachricht vom 24.11.2014

Eine aktuelle Umfrage von PwC fragt nach den Erwartungen an die Interne Revision. Nur wenn diese bekannt sind, kann die Interne Revision einen hilfreichen Beitrag für das Unternehmen leisten.

Wie soll die Funktion der Internen Revision künftig ausgestaltet sein? Welche Ziele stehen auf der Agenda? Welchen Wertbeitrag kann sie leisten? Antworten auf diese zentralen Fragestellungen gibt die aktuelle PwC-Studie „State of the internal audit profession".

Nach Auffassung der Studienautorin Kathrin Kersten müsse die Interne Revision die Erwartung kennen, die die Unternehmensführung und der Aufsichtsrat an sie stellt. Nur so „kann sie einen signifikanten Wertbeitrag für das Unternehmen liefern".

Aufgaben und Ziele mit Interessen der Stakeholder abstimmen

Viele Unternehmen hätten zwar in der Vergangenheit „große Anstrengungen unternommen, um ihre Leistung zu verbessern". Diese reichten nach Auffassung von Kersten nicht aus, „um mit dem immer risikoreicher und komplexer werdenden Unternehmensumfeld Schritt zu halten".

Damit der Wert der Internen Revision im Unternehmen langfristig gesteigert werden kann, müssen die Ziele und Aufgaben mit den Interessen aller Stakeholder besser abgestimmt werden. „Nur so lassen sich langfristig die richtigen Ressourcen aufbauen sowie Leistung und Wertbeitrag der Internen Revision im Unternehmen steigern", so Kersten.

Wert der Internen Revision wird unterschätzt

Die Umfrage, welche unter 1.900 Unternehmensvertretern aus 24 Branchen in 37 Ländern durchgeführt wurde, zeigte zudem, dass die Interne Revision immer noch mit Zweifeln auf der Führungsebene zu kämpfen hat. Laut der Studie sehen 55 Prozent der Führungskräfte und 30 Prozent der Aufsichtsräte keinen wesentlichen Beitrag der Internen Revision am Wertzuwachs des Unternehmens. Zugleich gaben die Studienteilnehmer an, dass mit Hilfe der richtigen Ressourcen, die Interne Revision durchaus fähig wäre, den eigenen Stellenwert zu erhöhen und damit auch den Beitrag zum Unternehmenserfolg zu leisten.

Weiterhin wird die Leistung der Internen Revision von den Befragten kritisch beurteilt. So stellen nur 50 Prozent der Führungskräfte und zwei Drittel der Aufsichtsräte der Internen Revision ein gutes Zeugnis in Sachen Kundenorientierung, Ausrichtung auf die Stakeholder-Erwartungen, Kosteneffizienz und Fokussierung auf kritische Risiken aus. Das schlechte Abschneiden wird auch von Revisionsleitern so geteilt. Demnach sind nur 65 Prozent der Meinung, dass die Interne Revision in diesen Bereichen gute Arbeit abliefere.

Positiver fällt dagegen die Bewertung bei der Frage nach dem Wertbeitrag aus. Mehr als die Hälfte der Befragten gab an, dass die Interne Revision in der Rolle eines vertrauenswürdigen Beraters einen signifikanten Wertbeitrag leisten könne. Und immerhin ein Drittel ist der Meinung, dass die Interne Revision eher in ihrer klassischen Prüferrolle einen Wertbeitrag für das Unternehmen leiste.

Die Studie „State of the internal audit profession" finden Sie auf der Website von Pwc (http://www.pwc.com/en_M1/m1/publications/documents/pwc-state-of-the-internal-audit-profession-2014.pdf).

Deutsche Wirtschaft sorgt sich um den Datenschutz

Nachricht vom 21.11.2014

Die eigenen Mitarbeiter sowie Cloud-Dienste schaffen die Haupteinfallstore für Spionage- und Hackerangriffe. Der betriebliche Datenschutz gewinnt daher deutlich an Bedeutung.

Die Sicherheit der IT-Infrastrukturen gewinnt immer mehr an Bedeutung: Aufgeschreckt vom PRISM-Skandal verstärken 81 Prozent der Unternehmen aktuell ihre Anti-Ausspähmaßnahmen. Vor allem die Gefahren, die durch Hackerangriffe ent-

stehen können, haben die Verantwortlichen für das Thema sensibilisiert. Das ist das Ergebnis einer Studie der Nationalen Initiative für Informations- und Internet-Sicherheit (NIFIS). Auch die Frage, ob und welche Geheimdienste Zugriff auf sensible Daten haben können, beschäftigt viele IT-Sicherheitsverantwortliche in den Rechenzentren.

Die aktuelle NIFIS-Studie zeigt zudem, dass neben externen Bedrohungen auch der Datenklau im eigenen Unternehmen eine Bedrohung für die Zukunft der Unternehmen darstellt. 80 Prozent der Befragten gaben an, dass sie sich ausreichend vor den eigenen Mitarbeitern schützen. Als wichtige Gegenmaßnahme wurden Verhaltensregeln beim Umgang mit Social Networks (53 Prozent) und die Sicherheit bei Collaboration (59 Prozent) angeführt (siehe hierzu die Nachricht auf COMPLIANCEdigital (http://www.complianceedigital.de/ce/social-media-als-neue-aufgabe-fuer-die-interne-revision/detail.html) vom 29.10.).

Cloud-Dienste als Gefahrenquelle für die IT-Sicherheit

Cloud-Dienste entwickeln sich nach Meinung der Befragten zu einer immer ernster zunehmenden Bedrohung für die IT-Sicherheit. Zwei Drittel fordern bei diesem Thema mehr Schutz. Nicht zuletzt aufgrund des Schadens, der durch Datenklau entstehen kann, setzen die Firmen vor allem auf Cloud-Anbieter, die ihre Server in Deutschland oder im europäischen Ausland betreiben, so der NIFIS-Vorsitzende Dr. Thomas Lapp. Die Unternehmen verbinden damit die Hoffnung, so besser vor fremden Zugriffen geschützt zu sein, als wenn die Server in den USA oder in Asien stehen.

Die Sorge ist berechtigt. Auf Grund der Patriot-Act-Gesetzgebung sind amerikanische Cloud-Anbieter dazu verpflichtet, auf Anforderung auch Daten von Kunden aus Europa den Behörden zu übergeben. (Lesen Sie zu diesem aktuellen Thema auch die aktuelle Ausgabe (6/2014) der Zeitschrift Ping (http://www.pingdigital.de/inhalt.html).)

Thomas Lapp: „Entwicklung von neuen IT-Sicherheitsstandards ist nationale Aufgabe“

Die IT-Sicherheit ist vor allem auch ein Thema für die Bundesregierung. „Der Schutz vor massiver Wirtschaftsspionage muss in Wirtschaft, Staat, Wissenschaft und Gesellschaft einen noch weitaus höheren Stellenwert einnehmen als bisher.“ Dies müsse einhergehen mit einem umfassenden Förderungsprogramm für Innovationen im Bereich IT-Sicherheit und Datenschutz, so Lapp. Die aktuelle IT-Sicherheitssituation sei nach Auffassung von Lapp einer „modernen Informations- und Wissensgesellschaft wie Deutschland nicht angemessen“.

Ein erster richtiger Schritt sei daher das geplante IT-Sicherheitsgesetz. Im Rahmen des Projektes „Smart Service Welt“ will die Bundesregierung die deutsche Wirtschaft für die digitalen Herausforderungen fit machen.

Hintergrund: NIFIS

Die Nationale Initiative für Informations- und Internet-Sicherheit e.V. (NIFIS) ist eine neutrale Selbsthilfeorganisation, die die deutsche Wirtschaft im Kampf gegen die täglich wachsenden Bedrohungen aus dem Netz technisch, organisatorisch und rechtlich unterstützen möchte. Vornehmliches Ziel der Arbeit, der unter dem Dach der NIFIS organisierten Gremien ist es, Vertraulichkeit, Verfügbarkeit und Integrität sowie den sicheren Transport von Daten in digitalen Netzwerken sicherzustellen. Dazu entwickelt die NIFIS seit ihrer Gründung im Jahr 2005 unterschiedliche Konzepte und setzt diese in pragmatische Lösungen um. Zu den Schwerpunkten der Tätigkeit zählen die aktive Kommunikation und die Bereitstellung von Handlungsempfehlungen und Dienstleistungen.

BaFin: Deutsche Lebensversicherer für Solvency II gut gerüstet

Nachricht vom 14.11.2014

Laut BaFin sind die deutschen Lebensversicherer gut gerüstet, um die Kapitalanforderungen unter dem künftigen europäischen Aufsichtsregime Solvency II zu erfüllen.

Große Erleichterung bei den deutschen Versicherern. Im Rahmen der Umfrage „Vollerhebung Leben“ hat die BaFin alle 87 Marktteilnehmer zur voraussichtlichen Eigenmittelsituation unter Solvency-II-Bedingungen befragt. Das Ergebnis: Alle Lebensversicherer können die Solvency-II-Anforderungen auf Basis der Übergangsmaßnahmen und der Volatilitätsanpassung bewältigen.

Solvency-II-Übergangsregelungen zeigen Wirkung

Die Übergangsmaßnahmen und die Volatilitätsanpassung, die das Solvency-II-Regelwerk vorsieht, entfalten die gewünschte Wirkung. Laut BaFin konnten nur ein Prozent der Unternehmen trotz Anwendung der vorgesehenen Maßnahmen keine ausreichenden Eigenmittel nachweisen. Hier wird die BaFin das Gespräch mit den betroffenen Unternehmen suchen.

Herausforderung Niedrigzinsphase

Trotz des sehr guten Abschneidens der Versicherer dürfen die Gefahren, denen sich die Versicherungen gegenübersehen, nicht vernachlässigt werden. „Dauert die Niedrigzinsphase weiter an, müssen die Lebensversicherer in der 16-jährigen Übergangsphase erhebliche Anstrengungen unternehmen, um ihre Kapitalbasis zu stärken“, mahnt Felix Hufeld, Exekutivdirektor der Versicherungsaufsicht.

Laut der BaFin-Erhebung liegen die Eigenmittel zum Stichtag 31. Dezember 2013 bei etwa 25 Prozent der Unternehmen unter den Anforderungen. Zusammen kommen diese Unternehmen auf einen Marktanteil von rund 10 Prozent.

Die Niedrigzinsphase hat auch Auswirkungen auf das Eigenkapital der Versicherer. Die BaFin geht davon aus, dass die deutschen Lebensversicherer unter aktuellen Kapitalmarktbedingungen ohne Anwendung der Übergangsmaßnahmen eine Eigenmittellücke von etwa 15 Milliarden Euro aufweisen. Allerdings könne diese Zahl nur als Indikation dienen, da die Eigenmittellücke stark vom Niveau der Kapitalmarktzinsen sowie der Entwicklung der Vertragsbestände abhänge, so der Bericht der BaFin weiter.

Bedeckungsquoten unter Solvency II reagieren sensitiv auf Zinsänderungen

Die BaFin-Umfrage hat weiterhin gezeigt, dass die Bedeckungsquoten unter Solvency II sehr sensitiv auf Änderungen der Kapitalmarktzinsen reagieren. Dies hat zur Folge, dass die Eigenmittelsituation der Versicherer sehr volatil ist. Die BaFin erwarte daher von den Unternehmen, die die Bedeckungsquoten nur sehr knapp erreicht haben, dass diese geeignete Maßnahmen zur Stärkung der Kapitalbasis einleiten. (Quelle: BaFin)

Was veränderte Lieferketten für die Compliance bedeuten

Nachricht vom 07.11.2014

Der technologische Fortschritt verstärkt die Effekte der Globalisierung. Veränderte Lieferketten bedeuten zugleich neue Gefahren für die Compliance, so die GEXSO-Studie von BearingPoint.

„Radikale Technologiesprünge sind laut der GEXSO-Studie (Global Excellence in Supply Chain Operations) „der Katalysator für die Globalisierung von Produktion, Einkauf und Absatz." Vor allem die neuen technologischen Entwicklungen, wie elektrische Antriebe, Leichtbauwerkstoffe und das Internet der Dinge, verändern die Lieferketten der Unternehmen fundamental.

Sie beschleunigen die „regionalen Verschiebungen des Welthandels", so die BearingPoint-Studie weiter. Die Firmen seien immer mehr darauf angewiesen, ihre Lieferketten zu internationalisieren. Der Trend Richtung Asien und Osteuropa hält dabei laut der Studie unvermindert an.

72 Prozent der Befragten sehen „starken Technologiewandel"

Die Veränderungen treffen sowohl Mittelständler als auch die großen Konzerne. Laut der BearingPoint-Umfrage sprechen rund 72 Prozent der Teilnehmer von einem starken Technologiewandel in der eigenen Organisation. „Das sind vor allem jene Unternehmen, die Produktionsstandorte und Lieferanten vermehrt in anderen Regionen der Welt suchen", so Donald Wachs, Partner bei BearingPoint. „Ein mittelständischer Automobilzulieferer zum Beispiel ist durch die Elektrifizierung des Autos gezwungen, elektronische Komponenten vermehrt in den Herstellerländern Ostasiens einzukaufen. Er eröffnet ein Einkaufsbüro in Hongkong oder Shanghai – oder verlagert gleich die ganze Einkaufsfunktion ins Reich der Mitte."

Neue Lieferketten erhöhen das Risiko der Korruption

Mit der Verlagerung entstehen zugleich neue Herausforderungen, auch für die Compliance der Unternehmen. Neben den zu erwartenden Wechselkursschwankungen und Qualitätsproblemen in der Produktion sehen die Umfrageteilnehmer vor allem das Thema Korruption als großes Problem. Russland und China, gefolgt von Indien, werden von den befragten Unternehmen bei der Korruption als die mit Abstand schwierigsten Länder gesehen.

Doch nicht nur Asien und Osteuropa ist Korruption ein Thema. Aktuelle Studien beziffern den Schaden, der allein in Europa durch Korruption entsteht, auf über drei Milliarden Euro.

Aktiv gegen Korruption vorgehen

Umso wichtiger ist es, dass das Management aktiv gegen Korruption vorgeht. Dabei ist ein zielgerichtetes Korruptionscontrolling unerlässlich. Wie dies aufzubauen und mit dem Compliance-Management und der Internen Revision zu verzahnen ist, erläutern Jürgen Stierle und Helmut Siller. Sie sind Autoren des Praxishandbuchs „Korruptionscontrolling: Konzepte – Prävention – Fallbeispiele".

Stierle und Siller beleuchten wesentliche rechtliche, wirtschaftliche und soziale Dimensionen des Korruptions-Phänomens. Auf dieser Basis entwickeln die Autoren passgenaue Controlling-Instrumente, die Unternehmen dabei helfen, sich gegen Korruption zu wappnen.

Hintergrund zur BearingPoint-Studie

Für die GEXSO-Studie wurden insgesamt 57 Automobilzulieferer, Industriekomponentenhersteller sowie Maschinen- und Anlagenbauer aus Deutschland, Österreich und der Schweiz befragt.

Die Studie ist entstanden aus einer Kooperation der Managementberatung BearingPoint, der Technischen Universität Darmstadt sowie der Fachzeitschrift Logistik.

Steuerhinterziehung schwerer gemacht

Nachricht vom 30.10.2014

Auf der Berliner Tax Conference 2014 haben 50 Staaten einen automatischen steuerlichen Informationsaustausch beschlossen. Damit ist nach Schäuble das Bankgeheimnis Geschichte.

Die Finanzkrise hat den Druck auf die Länder mit einem strengen Bankgeheimnis enorm verstärkt. In Zeiten von Rezension, Arbeitslosigkeit und Haushaltskürzungen war es nicht länger hinnehmbar, dass Billionen in sogenannten „Steuerparadiesen" gebunkert werden.

Die Finanzminister waren daher aufgerufen, die Schlupflöcher zu schließen. Einen großen Schritt in Richtung Steuergerechtigkeit konnte nun auf der „Berlin Tax Conference 2014" vollzogen werden. In der „Berliner Erklärung" haben 50 Staaten beschlossen, ab 2017 Daten zu Finanzkonten von Steuerpflichtigen, die in einem Staat ansässig sind, an den betreffenden Staat zu übermitteln. Damit wird Finanzbehörden ermöglicht, Finanzinformationen von Steuerzahlern aus dem Ausland einzuholen.

In einem Bild-Interview hat der deutsche Finanzminister Wolfgang Schäuble (CDU) die Tragweite des Beschlusses dahingehend kommentiert, dass mit der Vereinbarung das „Bankgeheimnis in seiner alten Form damit ausgedient hat".

Deutschland geht im Kampf gegen Steuerhinterziehung voran

Die Erklärung beruht auf den von der OECD entwickelten Steuerstandards. Sie geht auf eine Initiative der „G5-Länder" Deutschland Frankreich, Italien, Großbritannien und Spanien aus dem Jahr 2013 zurück.

Ziel der sogenannten „Early Adopters", also der 50 Erstunterzeichner, ist es, dass sich der Vereinbarung, auch weitere Staaten anschließen. In dem Dokument, das Sie hier herunterladen (http://www.bundesfinanzministerium.de/Content/DE/Pressemitteilungen/Finanzpolitik/2014/10/2014-10-29-PM42-Anlage-Deutsch.pdf?) können, heißt es hierzu: „In der Erkenntnis, dass Steuerhinterziehung nur auf globaler Ebene wirksam bekämpft werden kann, hat die (...) Gruppe der Erstanwender (...) die frühzeitige Einführung des neuen, einheitlichen und globalen Standards für den automatischen Austausch von Informationen über Steuerpflichtige beschlossen. (...)

Als Gruppe sind wir entschlossen, unser globales Ziel weiter zu verfolgen, die Überwachung der Umsetzung dieses neuen Standards innerhalb des Global Forums zu unterstützen und zu gewährleisten, dass alle Länder die Vorteile des neuen Standards realisieren. Durch unser gemeinsames Vorgehen erkennen wir an, dass nur die Finanzplätze, die sich für die höchsten Transparenzstandards entscheiden und eng zusammenarbeiten, in Zukunft erfolgreich sein werden."

Nicht unterzeichnet haben u.a. die Schweiz und die USA. In der Schweiz bedarf es hierzu noch einer Volksabstimmung. Die USA dagegen haben im Rahmen der Fatca-Abkommen mit den be-

troffenen Ländern gesonderte Abkommen geschlossen.

Automatischer Informationsaustausch
Laut der Vereinbarung müssen Finanzinstitute mit Stichtag 31. Dezember 2015 den Altbestand ihrer Konten erfassen und ab dem 1. Januar 2016 bei Neukunden die steuerliche Ansässigkeit feststellen. Der erste automatische Informationsaustausch von Daten wird im September 2017 erfolgen. Bei diesem Austausch mit dem Ausland werden hohe deutsche Standards des Datenschutzes angelegt werden. Die vereinbarte Vorgehensweise zum automatischen Informationsaustausch wird mittlerweile von fast 100 Staaten und Jurisdiktionen unterstützt.

Die Finanzminister erhoffen sich, dass durch die Vereinbarung die Steuerhinterziehung weltweit zurückgedrängt wird. Zukünftig werden die Steuerverwaltungen weltweit, darunter auch die deutsche, die Information erhalten, die sie für eine korrekte Besteuerung aller Steuerpflichtigen benötigen.

Steuer-CDs bald wertlos
Nach Auffassung von Schäuble werden mit diesem Schritt die Finanzämter in Zukunft nicht mehr auf den Ankauf von sogenannten Steuer-CDs angewiesen sein, um Steuerflüchtlinge zu enttarnen. „Ich fand es immer problematisch, mit Hehlern zusammenarbeiten zu müssen, um Recht zu wahren“, so Schäuble in dem Bild-Interview.

Social Media als neue Aufgabe für die Interne Revision

Nachricht vom 29.10.2014

Social Media ist zunehmend auch ein Thema für die Interne Revision. Darauf wurde beim diesjährigen DIIR-Forum Kreditinstitute in Magdeburg in einem Vortrag von Volker Zieske (KPMG) hingewiesen.

Facebook, Twitter oder Instagram sind für viele Mitarbeiter wichtige Bestandteile ihres Alltags. Auf den Plattformen wird angefangen vom Beziehungsstatus bis hin zu den letzten Urlaubsfotos alles geteilt. Auch viele Unternehmen sind auf den Portalen präsent. Die direkte Kommunikation mit dem Kunden eröffnet für Unternehmen ungeahnte Möglichkeiten. Produktentwicklung und Marketing sind nur zwei Bereiche, die von dem direkten Draht zu den Kunden profitieren. Auch die Personalabteilungen setzen verstärkt auf Social Media (http://www.esv.info/978-3-503-15733-4), um neue Mitarbeiter für das Unternehmen zu gewinnen.

Zunehmend werden aber auch Informationen von Mitarbeitern gepostet, die nicht für die Öffentlichkeit bestimmt sind. Kommunikation aus dem Unternehmen heraus, so die Erkenntnis, kann kaum verhindert werden. Häufig ist es noch nicht einmal böse Absicht des Mitarbeiters. Viel zu oft existiert bei den Betroffenen kein Problembewusstsein, was eine Nachricht in der Social-Media-Welt auslösen kann. Und selbst in den Führungsetagen der Unternehmen fehlt es oftmals an der notwendigen Sensibilität im Umgang mit Nachrichten auf den Social-Media-Kanälen.

Die Probleme mit Social Media entstehen in den Grenzbereichen
Was passiert, wenn ein Finanzvorstand aus einem Board-Meeting twittert oder ein CEO privat eine Meldung auf Facebook postet, die nicht im Einklang mit der Politik des Hauses steht? Was sind die Folgen, wenn Mitarbeiter Fotos auf Instagram teilen, die vielleicht neue Produkte des Unternehmens zeigen? Auf diese Fragen haben viele Firmen keine klaren Antworten!

Social Media braucht klare Regeln
Nach Auffassung von Volker Zieske, Partner bei KPMG, müssen Unternehmen daher eine angemessene Social-Media-Strategie und Kontrolle entwickeln, um sich gegen Schäden abzusichern. Die Aufgabe der Internen Revision ist es, die Kontrollen zu validieren und sicherzustellen, dass diese effektiv sind und bleiben. In dem Vortrag wurden drei Handlungsfelder für Unternehmen aufgezeigt:

- Unternehmensrichtlinien: Sind alle Anforderungen an die Corporate Governance und Compliance in Bezug auf soziale Medien erfüllt?
- Unternehmensprozesse: Wie sind die Prozesse zur Erstellung, zum Monitoring und zum Reporting von sozialen Medien definiert?
- Mitarbeiter und externe Partner: Wie kann sichergestellt werden, dass die Unternehmenskultur richtig eingestellt ist, die Mitarbeiter richtig geschult und in die Social Media Prozesse integriert sind?

Social-Media-Revisionsansatz von Art des Unternehmens abhängig
Bei der Wahl des Revisionsansatzes sind nach Zieske wiederum vier Faktoren zu berücksichtigen.

- Branche und Geschäftsmodell
- Größe der Unternehmen
- Geschäftspartner
- Komplexität der Geschäftstätigkeit

Vor allem der Punkt Branche und Geschäftsmodell ist entscheidend: Wenn der Markenwert eines Unternehmens davon abhängt, dass der CEO ständig auf allen Kanälen präsent ist und der Firmenwert sich auch von der Anzahl der Twitter-Follower ablesen lässt, ist ein anderer Ansatz zu wählen als z.B. in einem Kreditinstitut, wo die Geschäftsführung eher gehalten ist, zurückhaltend zu kommunizieren.

Insgesamt besteht aber die Notwendigkeit, Social Media so einzusetzen, dass es dem Unternehmen nicht schadet. Für die Interne Revision ergeben sich hieraus vielseitige Handlungsfelder.

SEC verhängt Strafe gegen Hedgefund

Nachricht vom 28.10.2014

Die SEC verhängt zum ersten Mal eine Strafe wegen Manipulation des Hochfrequenzhandels. Die US-Behörde hat sich mit einem Hedgefund auf einen Vergleich in Höhe von einer Million US-Dollar geeinigt.

Das Aufräumen auf dem US-Finanzmarkt geht weiter. Nachdem in der Vergangenheit die großen Finanzakteure im Fadenkreuz der Ermittler standen, wenden sich die US-Behörden nun verstärkt den kleineren Marktteilnehmern zu. Die Ermittler haben dabei vor allem den Hochfrequenzhandel im Blickfeld.

„Banging the close“
Als einen der Ersten trifft es den Hedgefund Athena Capital Research LLC. Die US-Finanzaufsichtsbehörde (SEC) hat dem Hedgefund vorgeworfen, im Jahr 2009 komplizierte Algorithmen genutzt zu haben, um die Schlusskurse von Aktien mit massiven Kauf- und Verkaufsaufträgen in den letzten Sekunden eines Handelstages zu manipulieren. Dieses Vorgehen wird

in Fachkreisen als „banging the close" bezeichnet.

Vergleich akzeptiert

Mit der Kursmanipulation, so die SEC, habe Athena Capital Research LLC den § 10 (b) des Exchange Acts verletzt sowie gegen die entsprechende Richtlinie „Rule 10b-5", die jegliche Manipulation oder betrügerisches Vorgehen beim Kauf oder Verkauf von Wertpapieren verbietet, verstoßen. Athena Capital Research akzeptierte die Strafzahlung, um die Klage ohne Schuldeingeständnis beizulegen.

Anna Rode, Chefredakteurin Compliance Puls – Der US-Compliance Tracker (www.compliancepuls.com), anna.rode@compliancepuls.com

Industrie 4.0 und Soziale Marktwirtschaft verbinden

Nachricht vom 24.10.2014

Welche Rolle spielt CSR in Zeiten von Industrie 4.0? Jörg Hofmann von der IG Metall tritt in einem Gastbeitrag für das Handelsblatt für eine Humanisierungspolitik der Arbeitswelt ein.

Industrie 4.0 ist in aller Munde. Neben den vielen Chancen, welche sich nach Meinung von Wirtschaftsminister Sigmar Gabriel (SPD) für die deutsche Wirtschaft bieten, gibt es aber auch eine Vielzahl von gesellschaftlichen Herausforderungen, die nicht vernachlässigt werden dürfen. Darauf weist Jörg Hofmann, zweiter Vorsitzender der IG Metall, in einem Gastbeitrag für das Handelsblatt (http://www.igmetall.de/neue-arbeitswelt-braucht-faire-spielregeln-gastbeitrag-von-joerg-14602.htm) anlässlich des 8. Nationalen IT-Gipfels hin. Die Tagung, die in diesem Jahr am 21. Oktober in Hamburg stattfand, stand unter dem Motto: „Arbeiten und Leben im digitalen Wandel – gemeinsam. innovativ. selbstbestimmt".

Industrie 4.0 als Herausforderung für CSR

Weitestgehende Einigkeit – so kann vermutet werden – bestand auf dem 8. IT-Gipfel darin, dass die Industrie 4.0 die Zukunft der Arbeitswelt fundamental verändere. Die Bewertung der Folgen war indes nicht so einhellig. Neben der Betonung der vielen Möglichkeiten für Deutschland als „Ausrüster der Industrialisierung der Welt", so Wirtschaftsminister Gabriel, mischten sich auch kritische Töne. Kritiker befürchten, dass die Vorhersage von Carl Frey Wirklichkeit wird. Frey prognostiziert in der Studie „Die Zukunft der Beschäftigung", die im Frühjahr im Economist erschienen ist, dass fast 50 Prozent aller aktuellen Berufe durch die Digitalisierung der Produktion vom Aussterben bedroht sind. Vor allem die Dynamik der massiven Veränderungen in den Wertschöpfungsketten und Qualifikationsanforderungen, stellt, so Hofmann, eine große Gefahr für die Beschäftigteninteressen der Arbeitnehmer dar. Angesichts dieses Szenarios fordert der IG Metall Mann in dem Gastbeitrag, dass die Industrie 4.0 zwar die Wettbewerbsfähigkeit stärken soll, jedoch darf sie „nicht zu Ungleichheit und Unsicherheit der Beschäftigten beitragen".

Europa muss Normen des 21. Jahrhunderts bestimmen

Auf dem IT-Gipfel trat auch Bundeskanzlerin Angela Merkel (CDU) auf. Die Bundeskanzlerin betonte in ihrer Rede, dass Europa bei der Setzung der Normen für die Digitalisierung der Industrie nicht den Anschluss verlieren dürfe: „Am Anfang des 20. Jahrhunderts war man sehr davon überzeugt, dass eine Norm wie DIN natürlich nach Deutschland gehört. Dann war man der Überzeugung, dass manches nach Europa gehört. Inzwischen ist das nicht mehr so sicher. Gerade mit unserer starken Industrieproduktion wäre es aber ein guter Anspruch, dass Europäer auch die Normen der Industrie 4.0 wirklich mitbestimmen."

Neben technischen Normen und Regeln zählen hierzu auch soziale Aspekte. Merkel hob in ihrer Rede hervor, dass die digitale Welt kein Ort ohne jegliche Regularien ist: „Die Mechanismen der Sozialen Marktwirtschaft gelten – davon bin ich zutiefst überzeugt – auch in der digitalen Welt."

Unterstützung erhält Merkel für diese Position von Seiten der IG Metall: „Das ‚Modell Deutschland' kann trotz des bisherigen Erfolgs nicht einfach so bleiben, wie es ist. Anknüpfend an vorhandene Stärken – geschlossene Wertschöpfungsketten, qualifizierte Arbeitnehmer, soziale Stabilität durch Mitbestimmung und Tarifautonomie –, müssen neue Spielregeln für digitale Arbeitswelten gefunden werden", so Hoffmann in seinem Gastbeitrag für das Handelsblatt.

Industrie 4.0 nur mit sozialem Augenmaß

Hofmann tritt angesichts der aktuellen Veränderungen in der Industrie für einen Neustart in der Arbeitspolitik ein. Gefragt sei eine Humanisierungspolitik, deren Ziel eine Arbeitswelt ist, in der der Homo Faber – der handelnde und gestaltende Mensch – im Mittelpunkt stehe: „Er steuert die Systeme. Er erhält umfassende Weiterbildungsmöglichkeiten – etwa im Hinblick auf Software- und IT-Kenntnisse. Er erfährt Unterstützung – und nicht Delegation seiner Fähigkeiten – durch technische Assistenz, vor allem bei belastenden Routinetätigkeiten." Dies könne – als positiver Nebeneffekt – auch eine Antwort auf das Demografie Problem sein, ist sich Hofmann sicher.

Nach Meinung von Hofmann ist als Folge der aktuellen Entwicklungen zudem die Frage der Technikgestaltung neu zu stellen: „Ingenieursfantasie braucht soziale Erdung. Technik ist nicht vorbestimmt, und weil das so ist, muss sie im menschlichen Maß erforscht und erprobt werden." Seinen Appell verbindet Hofmann zugleich mit dem Aufruf zum Dialog in dieser Zukunftsfrage mit den Gewerkschaften und Betriebsräten.

COSO II wird überarbeitet

Nachricht vom 22.10.2014

Die US-amerikanische Organisation COSO überarbeitet gemeinsam mit der Wirtschaftsprüfungsgesellschaft PwC das ERM-Framework (COSO II) aus dem Jahr 2004.

Das Rahmenwerk COSO II hat sich in den vergangenen Jahren zu einem weltweit akzeptierten Tool etabliert. Gemeinsam mit dem Rahmenwerk für interne Kontrollsysteme (COSO I), dessen Update letztes Jahr in Kraft getreten ist, hilft es Führungskräften zu entscheiden, in welchem Umfang eine Organisation bereit und willens ist, im Zuge des Wertschöpfungsprozesses Risiken auf sich zu nehmen.

Krisensituationen stellen viele Unternehmen vor große Herausforderungen. Der souveräne Umgang mit unvorhergese-

henen Ereignissen ist daher für Unternehmen eine der zentralen Aufgaben. Um das Management aktiv beim Aufbau eines effizienten Risikomanagements zu unterstützen, hat das Committee of Sponsoring Organizations of the Treadway Commission, kurz COSO, das Framework „Unternehmensweites Risikomanagement – Übergreifendes Rahmenwerk" (ERM Framework) erarbeitet. Wie COSO nun bekanntgegeben hat, wird sie gemeinsam mit der Wirtschaftsprüfungsgesellschaft PwC das Rahmenwerk aus dem Jahr 2004 überarbeiten.

COSO II wird angepasst

Die Überarbeitung von COSO II sei notwendig, da sich auch die Anforderungen als auch die Erwartungshaltungen seitens der Stakeholder an das Risikomanagement in den vergangenen zehn Jahren geändert haben. Mit der Aktualisierung sollen Manager neue Tools an die Hand bekommen, um über Risiken adäquat zu informieren und um das unternehmensweite Risikomanagement zu überprüfen und zu evaluieren.

Umfangreiche Beteiligungsmöglichkeiten bei der Überarbeitung von COSO II geplant

Während der Überarbeitung wird das Team Beiträge und Feedback von Betroffenen sammeln. Ferner wird PwC eine Umfrage durchführen, um Ansichten zum aktuellen Rahmen zu erfassen und Verbesserungsvorschläge einzuholen.

Zudem plant COSO die Einrichtung eines Beirates. Dieser soll sicherstellen, dass die konzeptionellen und praktischen Herausforderungen des Risikomanagements möglichst aller Bereiche berücksichtigt werden. Neben Vertretern aus den Unternehmen aller Branchen sollen dem Beirat auch Personen aus Hochschulen und Non-Profit-Organisationen angehören.

Das Komitee wird in Kürze die Umfrage auf seiner Webseite freischalten. Unter folgender E-Mailadresse können Sie sich direkt an das Team wenden: COSO-ERM_Update@us.pwc.com. Weitere Informationen stehen auf der Seite von COSO (http://www.coso.org/ermupdate.html) zur Verfügung.

Bedeutung von Rahmenwerken für Compliance-Management-Systeme

Welche Bedeutung Rahmenwerke für Compliance-Management-Systeme haben, beantwortet Karl-Heinz Withus in seinem aktuellen Band „Betriebswirtschaftliche Grundsätze für Compliance-Management-Systeme". Das eBook steht Ihnen auf COMPLIANCEdigital (http://www.compliancedigital.de/ce/betriebswirtschaftliche-grundsaetze-fuer-compliance-management-systeme/ebook.html) zur Verfügung. Zum Thema Enterprise Risk Management (ERM) finden Sie in dem Handbuch Interne Kontrollsysteme (IKS) von Oliver Bungartz ebenfalls einen Beitrag. Das Kapitel können Sie hier herunterladen (http://www.compliancedigital.de/ce/enterprise-risk-management-erm-als-modell-zur-integration-von-internen-kontrollsystemen-iks-interner-revision-und-risikomanagement-3/search/coso+II/target/search/detail.html).

Transparency International mit neuer Führungsspitze

Nachricht vom 21.10.2014

Die Antikorruptionsorganisation Transparency International hat den Peruaner José Ugaz zum neuen Vorsitzenden ernannt. Als Stellvertreterin wurde die Russin Elena Panfilova gewählt.

Auf der diesjährigen Generalversammlung, die in Berlin abgehalten wurde, hat Transparency International ein neues Führungsduo gewählt. Mit José Ugaz und Elena Panfilova stehen ab sofort zwei profilierte Kämpfer gegen Korruption an der Spitze. Ugaz löst die Kanadierin Huguette Labelle ab, die der Organisation seit 2005 vorstand. Panfilova folgt dem Kameruner Akere Muna nach.

Über 200 Prozesse wegen Korruptionstatbeständen

Ugaz kann auf seine Erfahrungen als Sonderstaatsanwalt in Sachen Korruption in Peru zurückgreifen. Seit 2002 war José Ugaz Präsident von Proetica, der nationalen Organisation von Transparency International in Peru.

Als Staatsanwalt hat Ugaz hat mehrere Korruptionsprozesse auf höchster Ebene geführt. Bekannt geworden ist Ugaz durch die Korruptionsverfahren gegen den früheren peruanischen Präsidenten Alberto Fujimori und den ehemaligen Geheimdienst-Chef Vladimiro Montesinos.Auch sonst liest sich seine Bilanz beeindruckend: Zwischen 2000 und 2002 eröffnete die von ihm geleitete Einheit mehr als 200 Prozesse gegen 1.500 Regierungsbeamte und Partner von Fujimori. Es wurden Vermögen in Höhe von 205 Millionen US-Dollar im Ausland eingefroren und 75 Millionen US-Dollar zurückerlangt.

Zur stellvertretenden Vorsitzenden wurde Elena Panfilova gewählt, die Chefin von Transparency International Russland. Panfilova hat im Jahr 1999 Transparency Russland gegründet und war dessen Geschäftsführerin bis sie im Juli 2014 Vorsitzende wurde.

Korruption durch Offshore-Unternehmen verhindern

In seiner neuen Rolle will Ugaz vor allem gegen den Missbrauch von Offshore-Unternehmen vorgehen: „Es gibt immer noch zu viel Korruption, und wir müssen mehr dagegen tun. Zu oft kommen korrupte Personen davon und müssen keine Sanktionen fürchten. Der Missbrauch von Offshore-Unternehmen muss beendet werden". Sonst könnten korrupte Personen weiter in den Genuss unrechtmäßig erworbener Vermögen kommen, sich frei bewegen und ein Luxusleben führen, während die Armen die Rechnung zahlen müssten, so Ugaz.

Das neue Führungsduo wird in seinem Kampf gegen Korruption durch den zwölf-köpfigen internationalen Vorstand unterstützt. Auf der Generalversammlung wurden sechs neue Mitglieder in das Gremium gewählt: Sion Assidon (Marokko), Emile Carr (Sierra Leone), Jeremy Carver (Großbritannien), Mercedes de Freitas (Venezuela), Mark Mullen (Georgien) und Elisabeth Ungar Bleier (Kolumbien). Die Biographien der neuen Mitglieder finden Sie hier (https://www.transparency.org/files/content/feature/2014_New_Board_of_Directors.pdf).

ICC: Mit den richtigen Tools gegen Kartellrechtsverstöße vorgehen

Nachricht vom 17.10.2014

Die Internationale Handelskammer (ICC) hat soeben die deutsche Version des Handbuchs zur Kartellrechts-Compliance veröffentlicht. Es soll Unternehmen dabei unterstützen, die Compliance-Standards im Bereich Kartellrecht umzusetzen.

Kartellrechtsverstöße können schwerwiegende Folgen für Unternehmen haben.

Gerade für Unternehmen, die international engagiert sind, wird es immer schwieriger, alle Vorschriften im Blick zu behalten und sich Compliance-konform zu verhalten. Um auf die steigenden gesetzlichen Anforderungen reagieren zu können, hat die Internationale Handelskammer (ICC) das „ICC Antitrust Compliance Toolkit" entwickelt. Das Handbuch liegt nun auch in der deutschen Version vor.

Compliance-Systeme gegen Kartellrechtsverstöße

Die Internationale Handelskammer will mit dem Toolkit Firmen dabei helfen, ein auf ihre spezifischen Unternehmensbelange ausgerichtetes Compliance-System aufzubauen. Bereits laufende Compliance-Programme können mit Hilfe des Toolkits überprüft und angepasst werden.

Das Handbuch stellt den Unternehmen die Expertise von international anerkannten Kartellrechts-Experten zur Verfügung. Neben Vorschlägen für unternehmensinterne Richtlinien werden mit Hilfe von „Best Practice"-Beispielen auch konkrete Ratschläge formuliert, die Unternehmen dabei helfen, sich gegen Kartellrechtsverstöße abzusichern.

Konkret gibt das Toolkit Hinweise, wie

- die Führungsebene in Unternehmen bei dem Thema Kartellrecht am Ball bleibt,
- Schulungen zum Kartellrecht erfolgreich verlaufen,
- Mitarbeiter für das Thema Kartellrecht richtig motiviert werden sowie
- Unternehmen bei Whistleblowing-Verdachtsfällen und bei Ermittlungen durch Kartellbehörden im eigenen Haus angemessen reagieren können.

Die Tipps in dem Toolkit sind dabei so aufgebaut, dass die Unternehmen in den jeweiligen Ländern sie unabhängig von der jeweiligen Rechtsprechung und dem geltenden Kartellrecht anwenden können. Das Toolkit ergänzt zudem bestehende Instrumente und Empfehlungen der Internationalen Handelskammer.

Das Handbuch zur kartellrechtlichen Compliance können Sie auf den Seiten der ICC (http://www.icc-deutschland.de/fileadmin/ICC_Dokumente/Dokumente/ICC_Compliance_Toolkit_final.pdf) kostenlos herunterladen. Auf den Seiten der ICC (http://www.icc-deutschland.de/news/584-icc-handbuch-zur-kartellrechts-compliance-nun-auf-deutsch.html) finden Sie auch weitere Informationen zu dem Handbuch.

PwC: Unternehmen nicht ausreichend vor Hackerangriffen geschützt

Nachricht vom 15.10.2014

Die Wirtschaftsprüfungsgesellschaft PwC warnt in einer soeben vorgelegten Studie vor Hackerangriffen auf Unternehmen. Ungeachtet der steigenden Bedrohung reduzieren Firmen die Budgets für IT-Sicherheit.

Trotz der vielen Meldungen über Spionage und Hackerangriffe scheint das Thema IT-Sicherheit in den Unternehmen keine große Rolle zu spielen, denn die Budgets für IT-Sicherheit sind um vier Prozent gegenüber dem Vorjahr gesunken. Auf der anderen Seite steigt der Druck auf die Unternehmen kontinuierlich: Laut der PwC-Studie „Global State of Information Security 2015" sind Hackerangriffe auf Unternehmen im letzten Jahr weltweit im Vergleich zum Vorjahr um 48 Prozent auf 42,8 Millionen angestiegen. Auf einen Tag runtergebrochen sind das 117.300 Angriffe pro Tag!

Mängel in der IT-Sicherheit verursachen Milliarden Schäden

Auch die Schäden, die durch Hackerangriffe entstehen, gehen in die Billionen. Laut der Studie belief sich der Verlust pro Angriff auf rund 2,7 Millionen Dollar – das ist eine Steigerung von 34 Prozent im Vergleich zum Vorjahr. Wie die Ergebnisse der Studie weiter zeigen, sind große Verluste zunehmend an der Tagesordnung: So stieg die Zahl der Fälle mit einem Verlust von mehr als 20 Millionen Euro im Jahr 2013 um 92 Prozent. Insgesamt, so die Studienautoren, liegt der Schaden, der durch den Verlust von Geschäftsgeheimnissen entsteht, zwischen 749 Milliarden und 2,2 Billionen Dollar. Die Summe bezieht sich allerdings nur auf die offiziell gemeldeten Fälle. Die Dunkelziffer, so die Studienautoren, liege weitaus höher.

Europa steht im Visier der Hacker

Im letzten Jahr seien vor allem Firmen aus Europa ins Fadenkreuz der Hacker gerückt. Allein in Deutschland ist die Anzahl der aufgedeckten Angriffe im Vergleich zum Vorjahr auf 41 Prozent gestiegen. Größere Firmen sind dabei öfters betroffen als kleine und mittelständische Unternehmen. Besonders interessant für Hacker sind laut der Studie Handelsstrategien, geistiges Eigentum, wie Produktdesigns, und vor allem Kundendaten. Ein neuer Trend sei der Angriff auf vernetzte Verbrauchergeräte, wie Babyphones oder Fernseher. Hieraus entstehen nach Meinung von PwC völlig neue Bedrohungsszenarien, auch vor dem Hintergrund des „Internet der Dinge" (Internet of Things).

Mitarbeiter als Täter und Opfer mangelnder IT-Sicherheit

Als Haupttätergruppe identifizierte die Studie vor allem Mitarbeiter oder ehemalige Angestellte. Allerdings, so die Autoren, stecke dahinter oft keine kriminelle Absicht. Oft werden Mitarbeiter Opfer von Phishing-Mails. Ein weiteres Einfallstor für Hacker sind verlorengegangene mobile Endgeräten wie Smartphones oder Tablets. Hierauf sind, nach Aussage von Derk Fischer, PwC-Experte für Informationssicherheit, Unternehmen nicht vorbereitet: „Viele Organisationen übersehen gerade die Bedrohungen, die aus ihrem eigenen geschäftlichen Ökosystem stammen. Als Folge davon verfügen die wenigsten Unternehmen über eine geeignete Früherkennung und sind nicht in der Lage, auf den Ernstfall, der mit an Sicherheit grenzender Wahrscheinlichkeit eintreten wird, angemessen und schnell zu reagieren."

IT-Sicherheit ernst nehmen

Zu den gleichen Ergebnissen kommt auch der Verband der Internetwirtschaft in Europa (eco). Eco fordert ebenfalls von den Firmen, die IT-Sicherheit ernst zu nehmen. Das Problembewusstsein in den Unternehmen versuchte Eco mit einem Fünf-Punkte Plan zu schärfen. Der Plan soll Firmen dabei unterstützen, ihre IT-Sicherheit zu verbessern (siehe hierzu die Nachricht auf COMPLIANCEdigital (http://www.compliancedigital.de/ce/fuenf-punkte-plan-fuer-mehr-it-sicherheit/detail.html) vom 07.10.2014).

Informationen zu Studie

Die Studie „Global State of Information Security" wird jährlich von der Wirtschaftsprüfungsgesellschaft PwC in Zusammenarbeit mit den Fachmagazinen CIO und CSO durchgeführt. Für die aktuelle Studie wurden im Frühjahr 2014 rund 9800 IT-Verantwortliche in über 154 Länder quer durch alle Branchen befragt. Darunter waren rund 3300 europäische und 434 deutsche Unternehmen. Laut Aussage der Initiatoren handelt es sich hierbei um die größte Erhebung in Sachen IT-Sicherheit weltweit.

Weitere Informationen zur Studie finden Sie auf den Seiten von PwC (http://www.pwc.de/gsiss2015).

Transparency: Deutschland braucht legislative Fußspur

Nachricht vom 14.10.2014

Transparency Deutschland fordert in ihrem neuen Lobbyismus-Bericht von der Bundesregierung mehr Regulierung. Konkret schlägt die Antikorruptionsorganisation die Einführung einer „legislativen Fußspur" vor.

Wo viel Licht ist, da ist auch viel Schatten. So lässt sich aus Sicht der Antikorruptionsorganisation Transparency Deutschland die Situation in Sachen Lobbyismus in Deutschland beschreiben.

Unterzeichnung der UN-Antikorruptionskonvention ist Schritt in die richtige Richtung

Positiv hebt Transparency Deutschland die Ratifizierung der UN-Antikorruptionskonvention (COMPLIANCEdigital berichtete (http://www.compliancedigital.de/ce/deutschland-schliesst-zum-rest-der-welt-auf/detail.html)) sowie den Beschluss der Regierungskoalition hervor, eine Karenzzeit für Politker einzuführen, bevor sie nach ihrem Amt in die Wirtschaft wechseln. Auf der anderen Seite gibt es aber immer noch große Defizite im Bereich der Selbstregulierung durch die Interessenvertreter. Hier bestehe nach Meinung von Transparency weiterhin keine Alternative zu einer gesetzlichen Regelung:

„Die Bundesregierung hat letzte Woche verkündet, ein eigenes Gremium zu schaffen, das mögliche Interessenkonflikte beim Wechsel von ehemaligen Ministern und Parlamentarischen Staatssekretären beurteilt. Dieses Gremium muss auch für Transparenz und Lobbykontrolle zuständig sein. Dazu gehört die Überwachung eines einzuführenden aussagefähigen Lobbyistenregisters," so Prof. Dr. Edda Müller, Vorsitzende von Transparency Deutschland.

Einführung einer legislativen Fußspur gegen zu viel Schatten im Lobbyismus

Um wirksam gegen Korruption und Interessensverschränkungen vorgehen zu können, schlägt die Antikorruptionsorganisation die Einführung einer „legislativen Fußspur" vor. Die Idee dahinter ist, dass in jedem Gesetzesentwurf dokumentiert werden muss, wie das Gesetz entstanden ist und welche Positionen bei einzelnen Paragraphen dafür oder dagegen vorgebracht wurden. Die legislative Fußspur soll in der Gemeinsamen Geschäftsordnung der Bundesministerien fixiert werden. Nach Ansicht von Transparency würde dies dazu führen, dass alle Interessengruppen, die an dem Gesetzesentwurf mitgewirkt haben und dabei berücksichtigt oder auch abgelehnt wurden, bekannt wären.

„Die Öffentlichkeit muss über den Austausch von Politik und Interessen informiert werden. Unbestritten ist, dass es einen Unterschied zwischen starken und schwachen Interessen gibt. Welche Einflüsse in einen Gesetzgebungsprozess eingeflossen sind, muss offengelegt werden", so der Autor der Studie, Dr. Rudolf Speth.

Zum Hintergrund

Der Bericht ist Teil eines Projekts „Lifting the Lid on Lobbying: Taking Secrecy out of Politics in Europe" von Transparency International, das von der europäische Kommission finanziell unterstützt wird. Es hat zum Ziel, bestehende Regulierungen und Praktiken im Bereich des Lobbying in 19 europäischen Ländern darzustellen und Empfehlungen für Entscheidungsträger sowie Interessenvertreter zu formulieren.

Weitere Informationen finden Sie auf den Seiten von Transparency International (http://www.transparency.de/index.php?id=2535&type=98).

Fünf-Punkte Plan für mehr IT-Sicherheit

Nachricht vom 07.10.2014

Unternehmen vernachlässigen nach Ansicht des Verbandes der Internetwirtschaft in Europa (eco) das Thema IT-Sicherheit und Datenschutz. Der soeben vorgelegte Fünf-Punkte Plan soll hier Abhilfe schaffen.

Eine sichere IT-Infrastruktur zählt, zu den größten Herausforderungen der Industrie. Das gilt nicht erst seit den Ausspähaktionen ausländischer Geheimdienste. Die Schäden, die durch Datendiebstahl und Geheimnisverrat entstehen, können ganze Unternehmen und auch selbst Staaten ins Wanken bringen.

Grundsätzlich stehen „den deutschen Firmen eine Vielzahl von Maßnahmen zur Verbesserung des Datenschutzes und der IT-Sicherheit zur Verfügung". Würden diese besser umgesetzt, wäre die Bedrohung durch ausländische Geheimdienste und Cyberkriminelle in den Augen von Oliver Dehning, Leiter der eco Kompetenzgruppe Sicherheit, wesentlich geringer.

„Generell gilt es, IT-Sicherheit ernst zu nehmen"

Umso erstaunlicher ist der immer noch laxe Umgang mit dem Thema IT-Sicherheit. Nach Ansicht des IT-Sicherheitsexperten Oliver Dehning wird das Thema in den Unternehmen immer noch nicht ernst genug genommen: „Der meiste Schaden entsteht durch Fahrlässigkeit, die sich beispielsweise in offenen Accounts, leicht zu erratenden, offen herumliegenden oder seit Jahren nicht geänderten Kennwörtern, nicht aktivierten Verschlüsselungen sowie in der Speicherung wichtiger Daten in ungeschützten Cloud-Services widerspiegelt."

In vielen Unternehmen ist es nach Ansicht von Dehning nicht klar geregelt, welche Daten ins Netz gestellt werden dürfen. Um hier eine höhere Sensibilität zu erreichen, müssen Mitarbeiter durch Aufklärung, Transparenz und strikte Compliance-Regeln unterstützt werden.

Insgesamt fordert Dehning die Firmen auf, mehr Eigeninitiative bei dem Thema IT-Sicherheit an den Tag zu legen. Zudem müssen Datenschutz und IT-Sicherheit auch auf Verbands- und Branchenebene mehr in den Mittelpunkt gerückt werden. Das Ziel, so Dehning weiter, seien einheitliche Standards.

Fünf Punkte für mehr IT-Sicherheit

Um das Problembewusstsein in den Unternehmen zu schärfen, hat der Verband einen Fünf-Punkte Plan aufgelegt. Der Plan soll Firmen dabei unterstützen, ihre IT-Sicherheit zu verbessern:

1. Sorgfältiger und vorsichtiger Umgang mit sensiblen Firmendaten. Mitarbeiter durch Aufklärung, Transparenz und strikte Compliance-Richtlinien stärker sensibilisieren.
2. IT-Sicherheit bereits bei Beschaffung berücksichtigen.
3. Vorhandene IT-Sicherheitsmechanismen in den Firmen auch nutzen.
4. Bei Entwicklung der eigenen Produkte und Dienstleistungen IT-Sicherheit bereits berücksichtigen.

5. Zusammenarbeit auf Branchen- und Verbandsebene für Synergieeffekte, Erfahrungsaustausch und zur Standardisierung.

IT-Compliance aufbauen
Neben dem Aspekt der Gefahrenabwehr müssen die IT-Systeme auch grundlegenden regulatorischen Anforderungen genügen. Insbesondere die rasanten technologischen Veränderungen in den letzten Jahren haben zu einer grundlegenden Neubestimmung IT-spezifischer Risikolagen für Unternehmen geführt.

Wie Sie wesentliche regulatorische Anforderungen an die IT erkennen, priorisieren und deren Erfüllung einer effizienten Steuerung zuführen, erläutert der soeben erschiene Band „IT-Compliance" von Michael Rath und Rainer Sponholz. Das Buch steht Ihnen auf COMPLIANCEdigital (http://www.compliancedigital.de/ce/it-compliance-7/ebook.html) zur Verfügung.

Weitere Informationen zu IT-Sicherheit und Datenschutz finden sich auf den Internetseiten der eco Kompetenzgruppe Sicherheit (sicherheit.eco.de (http://sicherheit.eco.de)), die auch eine Umfrage zum Thema Internetsicherheit durchgeführt hat. Die Ergebnisse sollen Anfang 2015 veröffentlicht werden.

Informationen zum eco-Verband
eco ist nach eigener Darstellung mit mehr als 750 Mitgliedsunternehmen der größte Verband der Internetwirtschaft in Europa. Seit 1995 gestaltet der eco Verband maßgeblich die Entwicklung des Internets in Deutschland, fördert neue Technologien, Infrastrukturen und Märkte, formt Rahmenbedingungen und vertritt die Interessen der Mitglieder gegenüber der Politik und in internationalen Gremien. In den eco Kompetenzgruppen sind alle wichtigen Experten und Entscheidungsträger der Internetwirtschaft vertreten und treiben aktuelle und zukünftige Internetthemen voran.

Deutschland schließt zum Rest der Welt auf

Nachricht vom 02.10.2014

Als einer der letzten Staaten reiht sich die Bundesrepublik in die Liste der Unterzeichner der Anti-Korruptionskonvention ein. Der Bundestag hat Ende September den Weg für die Unterzeichnung freigemacht.

Einstimmig verabschiedete der Ausschuss für Recht und Verbraucherschutz in seiner Sitzung Ende September den Gesetzentwurf (BT.-Drs. 18/2138) zur Ratifikation des Übereinkommens der Vereinten Nationen gegen Korruption. Damit kann der Bundestag im Oktober dem Gesetz zustimmen. Mit der Unterzeichnung endet ein elfjähriges und unrühmliches parlamentarisches Gezerre.

UN-Konvention gegen Korruption
Bereits im Jahr 2003 hatten die Vereinten Nationen die Konvention beschlossen. Laut Bundesregierung sind aber erst jetzt die Rechtslage sowie das materielle Strafrecht in Deutschland soweit angepasst, dass die Unterzeichnung der UN-Konvention möglich ist. Erst im Februar dieses Jahres beschloss der Bundestag, dass Bestechung und Bestechlichkeit von Parlamentariern mit bis zu fünf Jahren Haft geahndet werden solle.

Mit dem Abkommen verpflichten sich die beteiligten Länder, Amtsträger für Korruptionstatbestände zu bestrafen. Ferner sieht die Konvention vor, dass die Vertragsstaaten zur Bekämpfung der Korruption sowohl präventive Maßnahmen fördern, zum Beispiel Verhaltenskodizes, als auch strafrechtliche Instrumente zur Verfolgung schaffen beziehungsweise schärfen. Weiterhin sieht die Konvention eine stärkere internationale Zusammenarbeit bei der Bekämpfung von Bestechung und Bestechlichkeit vor.

Parlamentarier sind erleichtert
Allgemein herrscht bei den Parlamentariern Erleichterung. Ein Vertreter der SPD-Fraktion äußerte sich zufrieden, dass man nach elf Jahren „nun endlich" die UN-Konvention umsetzen werde. Auch aus den Reihen der Opposition kommt weitgehend Zustimmung. Zwar halte man den Gesetzesentwurf der Regierung für unzureichend. Jedoch, so ein Vertreter von Bündnis 90/Die Grünen, sei es wichtig, dass das Übereinkommen nun endlich ratifiziert werde. Hinzu komme, dass der eigene Gesetzesentwurf (BT-Drs. 18/478) „mehr oder weniger deckungsgleich" sei. Andere Fraktionen haben sich bisher noch nicht geäußert.

Deutschland einer der letzten Unterzeichnerstaaten
Insgesamt fällt die Bilanz für die Bundesrepublik in Sachen UN-Antikorruptionskonvention bescheiden aus. Als einer der letzten Staaten, aber immerhin noch vor Syrien und Nordkorea, hat Deutschland das Ziel erreicht. Weitere Informationen finden Sie unter www.bundestag.de (http://www.bundestag.de/presse/hib/2014_09/-/330606).

Korruption ist internationales Phänomen
Informieren Sie sich über die Ursachen, Auswirkungen und Strategien zur Bekämpfung von Korruption in dem von Matthias S. Fifka und Andreas Falke herausgegebenen Band: „Korruption als internationales Phänomen". Die Autoren beleuchten das Phänomen Korruption vielseitig aus gesellschaftlichen, kulturellen, ethischen und ökonomischen Blickwinkeln. Das eBook steht Ihnen auf COMPLIANCEdigital (http://www.compliancedigital.de/ce/korruption-als-internationales-phaenomen/search/korruption/target/search/ebook.html) zur Verfügung.