FIRM

Frankfurter Institut für Risikomanagement und Regulierung

Liebe FIRM-Leser,

die Globalisierung ist tot. Es lebe die Globalisierung. So oder ähnlich könnte der Slogan bei einem Blick auf die aktuelle wirtschaftliche und politische Weltlage aussehen. Einerseits fordern Populisten mehr Eigensinn und bilaterale Verträge – Donald Trump und die Brexit-Befürworter machen es vor. Andererseits ist das Thema Wachstum im globalen Maßstab nicht vom Tisch. Im Klartext heißt das: Wachstum braucht offene Märkte, und das wissen auch Populisten. In diesem Sinne machte Rosa María Lastra von der Queen Mary University of London bei einer SAFE Policy Lecture klar, dass Populisten Zentralbanken als Teil des „politischen Establishments" sehen. Gleichzeitig fordern sie protektionistische Maßnahmen, wie zum Beispiel eine Begrenzung der Einwanderung. Überhaupt ist in vielen Bereichen ein globales Vorgehen zwingend notwendig, wie die Europäische Zentralbank mit ihrem Anfang Mai 2018 veröffentlichten europäischen Rahmenwerk für ethisches Hacking auf Basis von Threat Intelligence verdeutlichte. Ob diese Spielwiese gegen Hackerangriffe etwas bringt, steht indes auf einem anderen Papier.

Überhaupt tun sich Regierungen und Organisationen im Kampf gegen Hacker und Finanzkriminelle oft schwer. Zwei Beispiele: Eine aktuelle Studie kommt zu dem Schluss, dass E-Mail-Betrug ein Top-Sicherheitsrisiko ist. Und Transparency International sieht die Bemühungen der G20-Staaten zur Bekämpfung von Schattenfinanzplätzen und Geldwäsche nur teilweise umgesetzt. Das erste Beispiel ist kein neues Phänomen und doch ein stets aktuelles sowie organisationsinternes Risikomanagementthema. Beim zweiten Thema mangelt es wohl an internationaler Abstimmung – sprich viele Regierungen, viele Meinungen, viele Wege. Da passt es ins Bild, wenn eine aktuelle Studie unter Federführung des Zentrums für Europäische Wirtschaftsforschung (ZEW) zu dem Schluss kommt, dass ein europäischer Minister für Wirtschaft und Finanzen kein Weg sei. Denn dieser könne zentrale Probleme der fiskalischen Koordination in Europa nicht lösen.

Einigung verspricht dagegen FIRM. Denn seit dem 1. Mai ist Professor Udo Steffens neuer Vorstandsvorsitzender der Frankfurter Gesellschaft für Risikomanagement und Regulierung. Viel Glück für die neue Herausforderung an dieser Stelle. Apropos Glück – das brauchen auch jene Unternehmen, die sich bis dato noch nicht mit der ab 25. Mai in Kraft getretenen Datenschutzgrundverordnung (DSGVO) gebührend auseinandergesetzt haben. Und da wäre sie dann wieder die Globalisierung, zumindest im europäischen Maßstab.

Im diesem Kontext fordert in dem nachfolgenden Gastbeitrag Wolfgang Hartmann, Gründer und Ehrenvorsitzender des Frankfurter Instituts für Risikomanagement und Regulierung e.V. (FIRM), eine Stärkung der Corporate Governance in einer Welt neuer und alter Risiken.

Haben Sie viel Spaß mit der neuen FIRM-Publikation.
Es grüßt

Frank Romeike, verantwortlicher Chefredakteur und Mitglied des FIRM-Vorstands

INHALT

HERAUSGEBER

Gesellschaft für Risikomanagement und Regulierung e.V.

Walther-von-Cronberg-Platz 16
D 60594 Frankfurt am Main

Telefon: +49 69 87 40 20 00
Telefax: +49 69 87 40 20 09
Internet: www.firm.fm
E-Mail: info@firm.fm

Redaktion:
Frank Romeike (V.i.S.d.P.),
Andreas Eicher
E-Mail: redaktion@firm.fm

Erscheinungsweise:
10 x im Jahr als Einhefter in der Zeitschrift RISIKO MANAGER

FIRM
Frankfurter Institut für Risikomanagement und Regulierung

Veränderte Risikolandschaft braucht Stärkung der Corporate Governance

Jahrhundertelang bestimmte das mehr oder weniger professionelle Managen von Kredit-Ausfallrisiken das Wohl und Weh der Banken. Dagegen hat sich in den letzten 40 Jahren die Risikolandschaft der Banken dramatisch verändert. Einen wesentlichen Beitrag hierzu leistete der Regulator selbst. Mit der regulatorischen Zulassung interner Marktrisikomodelle für die Kapitalunterlegung durch den Baseler Ausschuss für Bankenaufsicht begann Mitte der 80er Jahre der Siegeszug des Investments Bankings. Handelsrisiken dominierten von nun an den Geschäftserfolg.
Aber erst im Rahmen der globalen Finanzmarktkrise 2008 wurde offenkundig, dass Kredit- und Handelsrisiken zwei Seiten der gleichen Medaille sind. Nicht die Verbuchung im Bank- oder Handelsbuch, sondern allein die Liquidität der Position bestimmt, ob die Position als Markt- oder als Kreditrisiko ausschlagend wird. Der Vertrauensverlust der großen internationalen Banken untereinander bewirkte einen Wegfall der Liquidität. In diesem Zuge verwandelte die Finanzmarktkrise quasi über Nacht Marktrisiken in 100-fach größere Kreditrisiken.

Vom Lehman-Crash zu schärferen Regularien

Die globale Vermarktung von US-amerikanischen Subprime-Asset Backed Securities (ABS) brachte viele europäische Institute an den Rand des Abgrunds. Dies betraf vor allem die Institute, die sich auf das externe Investment Grade Rating der Papiere blind verließen. Selbst AAA geratete Subprime-CDOs erlitten einen Totalausfall. Die Folge war, dass auch Ratings der großen drei internationalen Rating-Agenturen für andere strukturierte Finanzierungen nicht mehr vertraut wurde. Dies verstopfte bei Management Buy Outs und Leverage-Finanzierungen die Vertriebskanäle, wodurch große Originator-Institute auf den Klumpenrisiken sitzen blieben. Ohne die mutige, vom Financial Stability Board koordinierte, staatliche Rettungsaktion nach dem Lehman-Crash im Herbst 2008, wäre das internationale Bankensystem wohl zusammengebrochen.

In diesem Zuge wurde das internationale Bankensystem ständigen Wellen regulatorischer Nachschärfungen durch den Baseler Ausschuss unterworfen. Und das unter anderem mit der Schaffung von Bonus-Malus-Systemen bei der Managervergütung, der Neueinführung von zwei Liquiditätsratios und dem Leverage Ratio, höheren Kapitalanforderungen sowie der Begrenzung der Kapitalerleichterung durch die Verwendung interner Modelle. Nie wieder wollte sich die internationale Staatengemeinschaft in der Breite einem solch dramatischen „moral hazard"-Risiko gegenübersehen.

Ob diese regulatorischen Verschärfungen die Systemstabilität tatsächlich erhöht haben, werden wir erst in der nächsten Krise erfahren. Nach der längsten Niedrigzinsphase, die die Industrienationen weltweit je gesehen haben, dürfte ein Wiederanstieg der Zinsen – insbesondere, wenn dieser steil verläuft – die Asset-Blase

zum Platzen bringen und die Volatilität von „hot money flows“ erhöhen. Losgelöst von den vielen Einzelinvestments, die sich auf Basis höherer Zinsen und im Zuge technologischer Umbrüche dann nicht mehr rechnen werden. Dabei sollten wir eines nicht vergessen: In der Finanzindustrie sind die Banken die mit Abstand am stärksten „geleveragden“ Adressen.

Compliance und Cybercrime

In den letzten Jahren spielen internationale Compliance-Risiken eine immer größere Rolle. Auch die beiden größten deutschen Banken wurden durch zurückliegende internationale Rechtsverstöße und die sich hieraus ergebenden Strafzahlungen in Milliardenhöhe massiv betroffen. Wer in US-Dollar internationale Geschäfte betreibt, hat amerikanisches Recht zu beachten und zu fürchten – auch wenn die USA nicht unmittelbar tangiert sind.

Compliance-Risiken sind heutzutage die wahren Monster von Finanzgeschäften und verhalten sich wie die Hydra der griechischen Mythologie. Schlägt man einen Kopf ab, wachsen zwei neue nach. Zunächst war es nur der Insider-Handel. Dann kamen Geldwäsche, Korruption, Terror-Finanzierung, Steuer-Betrug, Kreditbetrug und Marktmanipulation hinzu. Das aktuelle Thema heißt Cybercrime. Wieso gehört Cybercrime zu den Compliance-Risiken? Der Schutz der Daten und die Sicherheit der Kunden sind entweder gesetzlich vorgeschrieben, oder sie gehören zum Moralkodex eines jeden Unternehmens. Fortschritt hat eben stets zwei Seiten – die Chance und das Risiko. Durch die zunehmende Überführung aller Bank- und Kundendaten auf IT-Plattformen (Stichwort: Digitalisierung) schaffte man die Voraussetzung für die moderne Banksteuerung nach Basel II und III.

Interne sowie externe Attacken auf die Geschäftsaktivitäten der Banken wurden hierdurch ermöglicht. Das Cybercrime-Risiko ist somit der Wegbegleiter der Digitalisierung. Dabei befinden wir uns erst am Anfang. Ohne Verlinken über das Internet und die Digitalisierung der Bankprozesse ist ein modernes Bankgeschäft heutzutage nicht mehr möglich. Online-Dienste sind das Gebot der Stunde, für alle Unternehmen. Moderner Zahlungsverkehr macht den Zugriff auf Kundendaten sowohl international über Server, die in Drittstaaten stehen, als auch über das Darknet möglich. Das Mobile-Banking via Smartphone sowie Kreditkarten eröffnet weitere Zugriffsmöglichkeiten für Kriminelle. Für die kriminelle „Intelligentia“ ist Cybercrime die Spielwiese der Zukunft. Hat man als krimineller Hacker erst einmal genug Erfahrungen gesammelt, kann man auch die Seiten wechseln. Dann wird aus dem „Saulus“ ein „Paulus“. Das heißt, man geht in die Abwehr von Cybercrime, sprich zu Unternehmen oder zu Behörden. Sei es das Cyber-Abwehrzentrum NCAZ (Nationale Cyber-Abwehrzentrum) unter Leitung des Bundesamts für Sicherheit in der Informationstechnik (BSI) oder zur Cyber-Truppe der Bundeswehr, der inzwischen 13.000 Soldaten unterstehen sollen.

Die potenziellen Gewinne von Kriminellen durch Cybercrime sind hoch. Das Gute daran ist, dass die handelnden Personen sich nicht mehr die Finger schmutzig machen müssen und auch nicht Leib und Leben Dritter gefährden. Im Ausland bleibt man häufig unerkannt, die Aufklärungsquote ist deshalb gering. Dass in Cybercrime auch Schurkenstaaten eine Spielwiese zum Geldverdienen oder der Schädigung von Gegnern sehen, liegt auf der Hand. Durch die Wahlmanipulation kann man gegnerische Staaten schwächen, ohne eine Kugel abzuschießen. Cybercrime ist somit das wahre Monster, der Leviathan, der die moderne Zivilisation bedroht. Hierbei befinden wir uns zweifellos erst am Anfang der Entwicklung, auch wenn die bekannten Schadensfälle sich jährlich bereits im Bereich von mehreren Milliarden Euro bewegen. Die Dunkelziffer ist hoch. Denn welches Unternehmen möchte zusätzlich seine Reputation dadurch ruinieren, dass es Cybercrime und damit Schadensfälle publik macht.

Für mich ist es deshalb nur noch eine Frage der Zeit, bis eine große Bank ihre Geschäftstätigkeit durch Ausfälle im Zuge eines Cybercrime-Angriffes wird einstellen müssen. Das Buch „Black Out“ von Marc Elsberg liefert einige Szenarien, welche Konsequenzen der Zusammenbruch der Stromversorgung im Zuge eines Cyberangriffs haben kann. Nicht auszudenken, was passieren kann, sollte es dem internationalen Terror einmal gelingen, eine Atombombe zu starten und hiermit eine Großstadt auszulöschen. Denn hierzu muss man keine Rakete mehr stehlen, es reicht der anonyme Zugriff auf die Steuerungssoftware. Undenkbar ist das alles nicht mehr.

Zurück vom Inferno der täglichen Bedrohung von Unternehmen. Die Abwehr von Cyberangriffen gehört bei Finanzdienstleistern und dem Geldtransfer von Unternehmen inzwischen zum Alltag; das gilt auch für den Mittelstand. Aber auch Privatpersonen rücken unmittelbar in den Focus. Durch gefälschte Webseiten werden Kontodaten erbeutet und in diesem Zuge die Konten der Privatpersonen geplündert. In ganz Europa gibt es heute frei zugängliches WLAN, das Cybercrime-Zugriffe stark vereinfacht. Gleiches gilt für Funk-Kreditkarten.

Insofern ist es für mich kaum nachvollziehbar, dass auch heute noch in vielen Banken für das Cybercrime-Risiko völlig unzureichende Governance-Strukturen existieren. Dabei vertrauen Vorstände bei der Absicherung ihrer Systeme ihren IT-Spezialisten. Getreu dem Motto: Diese werden es schon richten. Und wenn nicht?

Im Siemens Korruptionsskandal haben Gerichte die Verantwortung des Gesamtvorstands eines Unternehmens für die Schaffung einer leistungsfähigen Compliance-Organisation herausgestellt (Stichwort: Organ-Haftung). Es wurden hohe Geldbußen gegen Vorstandsmitglieder verhängt [vgl. hierzu vertiefend Hartmann/Romeike 2015]. Cybercrime-Risiken gehören zu den Compliance-Risiken. Dadurch ist absehbar, dass eine nachweislich unzureichende Überwachung durch den Vorstand bzw. eine hierfür geschaffene leistungsfähige Organisation in schweren Schadensfällen zu hohen Geldstrafen oder sogar zur Ablösung von Vorständen führen kann.

BJR: unzureichende Kenntnisse der Führungsebene

Seit Jahren kritisiere ich, dass Vorstände und Aufsichtsräte der deutschen Finanzindustrie völlig unzureichende Kenntnisse von der internationalen Grundregel für unternehmerische Entscheidungen haben. Dabei geht es um umfassende Kenntnisse der Business Judgement Rule (BJR). Nur deren Einhaltung kann die erste Managementebene und das Aufsichtsorgan vor der straf- und der zi-

vilrechtlichen Organhaftung schützen [vgl. hierzu Hartmann/Romeike 2015]. Kennen Sie die wesentlichen Kriterien dieser Leitlinie, und wissen Sie, was Sie bei strategischen unternehmerischen Entscheidungen zu beachten haben? Nur ein Hinweis: Es bedarf der Gegenüberstellung der 3-5-Jahresplanung sowohl der Alternative des „Status quo" als auch der Alternative „strategische Veränderung". Und zwar sowohl für den „most realistic case" als auch den „downside case". Das nicht nur für die Gewinn- und Verlustrechnung, sondern insbesondere bei Banken auch für Bilanzpositionen. Denn nur so lässt sich feststellen, ob die regulatorischen Mindestanforderungen auch im Rahmen der strategischen Veränderung eingehalten werden können. Erkennbar kannten viele Bankmanager die BJR nicht. Nur so konnte die Finanzmarktkrise ganze Institutsgruppen an den Rand des Abgrunds bringen. Durch global koordinierte gigantische Staatshilfen mussten viele systemrelevante Banken gerettet werden. Kann das wieder passieren? Ja, selbstverständlich kann es das.

Corporate Governance als Schwachstelle

Aus meiner Sicht ist die Corporate Governance bei vielen Unternehmen, insbesondere aber bei Banken, unverändert eine Schwachstelle. Daran ändern auch internationale Leitlinien nichts. Was wir dringend im Rahmen der Corporate Governance benötigen, professionell und kompetent agierende Aufsichtsräte und Vorstände. Ich empfehle einen Paradigmenwechsel bei den Kenntnissen, die zum Grundgerüst eines Bankvorstands und Aufsichtsrats gehören. Diese sollten regelmäßig an die aktuellen Anforderungen angepasst und alle zwei bis drei Jahre im Rahmen von „Fit and Proper" nachgewiesen, geschult und zertifiziert werden. Die Folge ist: Wer durchfällt, muss sein Mandat zurückgeben. Mit anderen Worten heißt das: Hier ist der Regulator gefragt. Zweifelsfrei unterliegt das professionelle Managen und Überwachen der Cyberrisiken der Organhaftung. Bei Bankvorständen und Aufsichtsräten ist das auch im Kreditwesengesetz (KWG) geregelt. Sofern ein Organ das Managen der Cyberrisiken alleine der Fachebene überlässt, haftet das Organ bei offenkundigem Versagen.

Zu kritisieren sind an dieser Stelle zudem die häufig zersplitterten Risikoverantwortlichkeiten in Banken. Geradezu klassisch zu nennen ist die Trennung zwischen dem Chief Risk Officer, der für die Financial Risks zuständig ist, und dem CFO, CEO oder COO. Letzte tragen häufig für Compliance-Risiken beziehungsweise die Non-Financial Risk die Verantwortung. Gelegentlich kommt noch ein gesonderter Vorstand für Legal Risk hinzu, der sich ausschließlich um die Schadensbegrenzung bei Altfällen kümmert. Durch diese Zersplitterung wird eine Gesamtschau durch das Risiko-Committee des Aufsichtsrats verhindert.

Und was macht die Regulierung? Nun, man beginnt das Thema Cybercrime zu entdecken. So erlangt am 25. Mai 2018 auf Ebene der Europäischen Union die „General Data Protection Regulation", kurz GDPR, nach einer zweijährigen Übergangsphase europaweit unmittelbar Gesetzeskraft. Einer Überführung in nationales Recht bedarf es somit nicht.

Gemäß den GDPR müssen bei Behörden und Unternehmen mit „certain risky processes" sogenannte „Data Protection Officer" (DPOs) installiert werden. National sind unabhängige „Supervisory Authorities" (SAs) zu schaffen, die europaweit durch einen „Data Protection Board" überwacht werden. Die SAs können bei schwerwiegenden Verstößen gegen die „Data Protection Rules" Geldbußen gegen die Data Controller von bis zu 20 Millionen Euro verhängen. Die DPOs müssen losgelöst von der operativen IT-Verantwortung agieren und ein „Data Protection Impact Assessment" for „all risky processing" installieren.

Auch die European Banking Authority (EBA) wurde aktiv und hat am 11. Mai 2017 „Guidelines on ITC Risk Assessment under the Supervisory Review of Evaluation Process", kurz SREP, veröffentlicht.

Die Europäische Zentralbank (ECB) hat ein „Reporting Framework for Significant Cyber Incidents" angestoßen. Dies wird nunmehr sukzessive bei allen unmittelbar beaufsichtigten, rund 130, Banken der Eurozone ausgerollt wird. Die Daten sollen vertraulich behandelt werden, die Richtlinie der ECB wurde leider nicht veröffentlicht. Man scheut also die Publizität bei diesem sensiblen Thema, möchte erst einmal Erfahrungen sammeln und offenkundig die Verbraucher nicht verunsichern.

Fazit

Die Bedrohung durch Cybercrime nimmt im Zuge der Digitalisierung der Industrie 4.0 exponentiell zu. Bei der Abwehr von Cybercrime-Risiken und deren Regulierung befinden wir uns noch im „stadium nascendi". Zwar bin ich optimistisch, dass durch ein besseres Managen der Compliance-Risiken die Milliardenstrafen für Marktmanipulationen durch Banken bald der Vergangenheit angehören werden. Dafür dürften sich die Cybercrime-Risiken als neuer Kopf der Hydra im Laufe der nächsten Jahre wohl zur teuersten Komponente im Bereich der Compliance-Risiken entwickeln.

Zur Begrenzung der Cyberrisiken sind prophylaktische Investitionen zur Schaffung sicherer Systeme unabdingbar. Hierzu zählt auch die Ausbildung von Experten und eine bessere organisatorische Aufstellung sowie eine professionelle Corporate Governance. Wer an falscher Stelle spart, dürfte früher oder später durch hohe Verluste aus Cybercrime-Schadensfällen bestraft werden und im Rahmen der Organhaftung möglicherweise auch seinen Job verlieren. Hinzu kommen Strafzahlungen sowie Reputationsverluste in der Öffentlichkeit und bei den Kunden.

Weiterführende Literaturhinweise

Hartmann, Wolfgang/Romeike, Frank [2015]: Business Judgement Rule, in: FIRM Jahrbuch 2015, Frankfurt/Main 2015, S. 157-160.

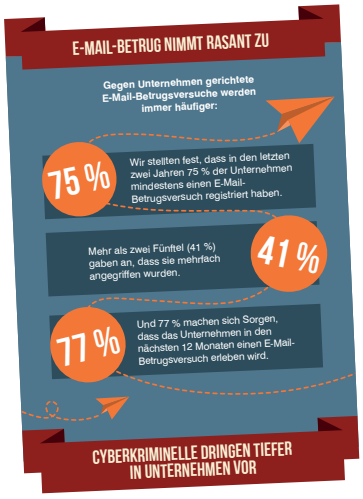
Elsberg, Marc [2012]: Blackout - Morgen ist es zu spät, Blanvalet Verlag, München 2012.

Autor

Wolfgang Hartmann, Ehrenvorsitzender des Vorstands des Frankfurter Instituts für Risikomanagement und Regulierung e.V. (FIRM). Er war bis 2009 Mitglied des Vorstands und Chief Risk Officer bei der Commerzbank.

Wissenschaft

Studie: E-Mail-Betrug ein Top-Sicherheitsrisiko



Die aktuelle Studie „Understanding Email Fraud Survey“ der Cybersecurity-Firma Proofpoint zeigt, dass 82 Prozent der weltweit befragten Unternehmen von E-Mail-Betrug betroffen sind und mehr als die Hälfte (59 Prozent) diese Cyberbedrohung als ein Top-Sicherheitsrisiko einstufen. E-Mail-Betrug, bei dem Cyberkriminelle sich beispielsweise als Vorgesetzte ausgeben, ist bereits heute weit verbreitet und für die Täter bestechend einfach einzusetzen. „Der E-Mail-Betrug, oftmals auch als Business Email Compromise (BEC) bezeichnet, ist aufgrund dieser Faktoren für klassische Sicherheitssoftware eine besondere Herausforderung. Cyberkriminelle setzen bei dieser Taktik auf die menschliche Naivität“, sagt Werner Thalmeier, Senior Director Systems Engineering EMEA bei Proofpoint. „Unsere Untersuchungsergebnisse unterstreichen daher, dass Organisationen und deren Vorstandsetagen angehalten sind, für ihre Belegschaft entsprechende Security-Lösungen bereitzustellen und diese Art der Bedrohung in Mitarbeiterschulungen zu thematisieren.“ Deutsche Organisationen waren in den letzten zwei Jahren im internationalen Vergleich unterdurchschnittlich von E-Mail-Betrug betroffen. So gaben lediglich 62 Prozent aller deutschen Befragten an, im Studienzeitraum mindestens einmal Opfer eines E-Mail-Betrugs gewesen zu sein (im weltweiten Durchschnitt 75 Prozent). Dennoch nannte ein Drittel (32 Prozent) der deutschen Befragten, dass ihr Unternehmen mehrfach Ziel eines derartigen Angriffs wurde. Für die Studie wurden 2.250 IT-Entscheider (USA, UK, Frankreich, Australien und Deutschland) zu ihren Erfahrungen aus den letzten beiden Jahren befragt.

Weitere Informationen unter: www.proofpoint.com

Auszeichnung für Dissertation: Bankenrestrukturierung und -abwicklung

Die internationale Kanzlei Baker McKenzie hat Anfang Mai 2018 den Preis für die beste wirtschaftsrechtliche Dissertation an Dominik Schöneberger verliehen. Er erhielt die Auszeichnung für seine Dissertation „Bankenrestrukturierung und Bankenabwicklung in Deutschland und den USA“. „Dominik Schönebergers Arbeit verknüpft in vorbildlicher Weise juristische Dogmatik, Rechtsvergleichung und ökonomische Analyse. Sie durchleuchtet nicht nur kritisch das geltende Recht, sondern entwickelt darüber hinaus eine Vielzahl konstruktiver rechtspolitischer Vorschläge“, kommentiert der betreuende Professor Andreas Cahn vom Institut für Zivil- und Wirtschaftsrecht der Goethe-Universität die Auswahl des Preisträgers. Jährlich vergibt die Kanzlei den Baker McKenzie-Preis für herausragende Dissertationen oder Habilitationen, die im Fachbereich Rechtswissenschaft der Goethe-Universität entstanden sind. Der Preis ist mit 6.000 Euro dotiert und kann auch auf zwei Preisträger aufgeteilt werden. Die bisherigen Preisträger sind heute unter anderem Universitätsprofessoren, Investmentbanker, Richter und Rechtsanwälte.

Studie zum Vorgehen gegen illegale Finanzgeschäfte

Ein Problem vieler Großbanken: Sie leiden unter zu komplexen und fehleranfälligen Prozessen bei der Bekämpfung von illegalen Finanztransaktionen. Dadurch steigt das Risiko, kriminelle Aktivitäten zu übersehen, seriöse Kunden zu verärgern und von den Aufsichtsbehörden sanktioniert zu werden. Zu diesem Schluss kommt die aktuelle Studie „How Banks Can Excel in Financial Crimes Compliance“ des Beratungsunternehmens Bain & Company in Zusammenarbeit mit der Parker Fitzgerald Group. Banken müssen viel mehr in moderne Datenanalyse, agile Kontrollabläufe und in die Kooperation mit hoch spezialisierten Regtech-Firmen investieren. Die Studie identifiziert vier Schlüsselkomponenten für den erfolgreichen Kampf gegen illegale Geldgeschäfte. Hierzu zählen: Prozesse komplett neu zu definieren, ein System für alle Daten, Advanced Analytics und Partnerschaften mit Regtechs. In Zukunft werden Banken gewisse Compliance-Prozesse an solch spezialisierte Regtechs auslagern, die zum Teil gemeinsam mit Wettbewerbern eigene Anti-Betrugs-Einheiten etablieren. „Damit die Zusammenarbeit mit den Regtechs erfolgreich ist, sollte der Compliance-Partner das Vertrauen der Aufsichtsbehörden genießen und die Bankdaten bestmöglich schützen“, erklärt Bain-Partner und Studien-Co-Autor Matthias Memminger. „Die Banken müssen sich außerdem den agilen Arbeitsweisen der Regtechs annähern, interne Abläufe abspecken und ihre IT-Architektur zügig den erforderlichen neuen Technologien anpassen.“ Auch gilt es für die Banken, in punkto Unternehmenskultur offener und im Projektmanagement flexibler zu werden.

Weitere Informationen unter: www.bain.de

Kurz notiert: Gastprofessur für Finanzgeschichte

Harold James, Princeton University, übernimmt in diesem Jahr die Gastprofessur für Finanzgeschichte am House of Finance der Goethe-Universität Frankfurt. Die Gastprofessur wird vom Bankhaus Metzler und der Friedrich-Flick-Förderungsstiftung finanziert. Die Forschungsschwerpunkte von Harold James liegen in den Bereichen Wirtschafts- und Finanzgeschichte sowie neue europäische Geschichte. James studierte an der Cambridge University.

Regulierungstrends

Populisten und die Unabhängigkeit von Zentralbanken

Nach den Worten Lastras betrachten Populisten Zentralbanken als Teil des „politischen Establishments". Bildquelle: SAFE.

Ende April 2018 präsentierte Rosa María Lastra von der Queen Mary University of London bei einer SAFE Policy Lecture ihre Ideen zu Populismus und der Unabhängigkeit von Notenbanken. Lastra: „Wenn es zuständige und spezialisierte Richter mit Expertise in Finanzfragen und Geldpolitik gäbe, die sich um die Rechtsprechung in Fällen in Zusammenhang mit der EZB kümmern, würde dies den rechtlichen Rahmen der Kontrolle der EZB im Lichte ihres beträchtlich ausgedehnten Mandats stärken." Nach den Worten Lastras betrachten Populisten Zentralbanken als Teil des „politischen Establishments". Sie setzten sich für schnelleres Wirtschaftswachstum ein und forderten zur selben Zeit protektionistische Maßnahmen, wie zum Beispiel eine Begrenzung der Einwanderung. Außerdem würde Ungleichheit zu Unzufriedenheit in der Öffentlichkeit führen, fügte Lastra hinzu. „Desillusionierte Menschen, die wenig zu verlieren haben, werden das politische Establishment abwählen, dagegen rebellieren oder protestieren". Die Angriffe von Populisten hätten die „soziale Legitimität" von Zentralbanken beschädigt. „Populismus ist eine Realität, der wir uns stellen müssen", so Lastra, die Professorin für internationales Finanz- und Währungsrecht am Centre for Commercial Law Studies an der Queen Mary University of London ist.

Weitere Informationen unter: www.safe-frankfurt.de

Bekämpfung von Finanzkriminalität nur teilweise umgesetzt

Auch zwei Jahre nach den Panama Papers haben die G20-Staaten ihre Zusagen zur Bekämpfung von Schattenfinanzplätzen und Geldwäsche nur teilweise umgesetzt. Zu diesem Schluss kommt der heute veröffentlichte Bericht „G20 Leaders or Laggards?" von Transparency International zu den Bemühungen der G20-Staaten im Kampf gegen Finanzkriminalität. „Wir sehen positive Entwicklungen auf europäischer und deutscher Ebene", so Gabriele C. Klug, Stellvertretende Vorsitzende von Transparency Deutschland. „Dennoch bleiben zu viele Schlupflöcher für Geldwäsche und Korruption insbesondere aufgrund mangelnder Transparenz von Finanzdaten bestehen." Elf der G20-Staaten besitzen nach wie vor nur unzureichende Regelungen zur Transparenz der sogenannten wirtschaftlich Berechtigten – trotz der 2014 gemachten Selbstverpflichtung im Rahmen der G20 High-Level Principles on Beneficial Ownership Transparency. Zwar konnten sich gegenüber einer Erhebung aus dem Jahr 2015 viele Staaten verbessern, darunter neben Deutschland auch Frankreich, Italien und Brasilien. Bis zur Erfüllung der Zusagen ist es jedoch noch ein weiter Weg. Nach den Panama Papers hatten die Staats- und Regierungschefs ihre Zusagen noch einmal bekräftigt, durch mehr Transparenz die Schattenfinanzplätze und die Steueroasen zu bekämpfen.

Weitere Informationen unter: www.transparency.de

Kurz notiert: Europäischer Minister für Wirtschaft und Finanzen keine Lösung

Ein „Europäischer Minister für Wirtschaft und Finanzen" (EMWF) könnte zentrale Probleme der fiskalischen Koordination in Europa nicht lösen. Das ist das Ergebnis einer aktuellen Studie, die von einem europäischen Team des Forschungsnetzwerks EconPol Europe unter Koordination des Zentrums für Europäische Wirtschaftsforschung (ZEW), Mannheim, verfasst und Anfang Mai 2018 bei der ZEW Lunch Debate in Brüssel zum Thema „Reform der Eurozone – Herausforderungen und Perspektiven" vorgestellt wurde.

Weitere Informationen unter: www.zew.de

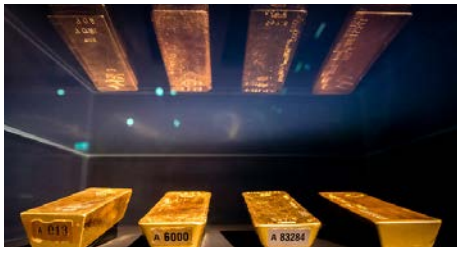
EZB mit Rahmenwerk für ethisches Hacking

Die Europäische Zentralbank (EZB) veröffentlicht Anfang Mai 2018 ein europäisches Rahmenwerk für ethisches Hacking auf Basis von Threat Intelligence (Threat Intelligence-based Ethical Red Teaming – TIBER-EU). Dabei handelt es sich um das erste Rahmenwerk auf europäischer Ebene für kontrollierte und individuell zugeschnittene Tests in Bezug auf Cyberangriffe auf den Finanzmarkt. TIBER-EU erleichtert einen europaweit harmonisierten Ansatz im Bereich erkenntnisgestützter Tests, die die Taktiken, Techniken und Vorgehensweisen echter Hacker nachahmen, die eine ernsthafte Bedrohung darstellen können. Mit den auf TIBER-EU basierenden Tests wird ein Cyberangriff auf die kritischen Funktionen und zugrunde liegenden Systeme eines Akteurs, wie beispielsweise Mitarbeiter, Prozesse und Technologien, simuliert. Dies ermöglicht es dem Unternehmen zu beurteilen, inwieweit es in der Lage ist, sich gegen mögliche Cyberattacken zu schützen, diese aufzuspüren und darauf zu reagieren.

Weitere Informationen unter: www.ecb.europa.eu

FIRM-News und Termine

Ausstellung zum Thema Gold



Gold als Ausstellungsobjekte
Bildquelle: Deutsche Bundesbank.

Die Deutsche Bundesbank hat im April 2018 in ihrem Geldmuseum eine Sonderausstellung zum Thema „Gold. Schätze in der Deutschen Bundesbank“ eröffnet. Für die Ausstellung wurden repräsentative Barren aus dem Bundesbank-Tresor ausgewählt. Die Auswahl reiche vom ältesten bis zu den jüngsten Goldbarren und ermögliche einen außergewöhnlichen Einblick, der sonst aus Sicherheitsgründen nicht möglich sei, so Vorstandsmitglied Carl-Ludwig Thiele. Die Ausstellung zeigt zudem bedeutsame Raritäten aus der numismatischen Sammlung der Bundesbank, vom Solidus über die Dukaten bis hin zu den Goldmünzen der Gegenwart. Die historische Bedeutung von Gold als Zahlungsmittel, die Eigenschaften des Edelmetalls, dessen weltweites Vorkommen, die Gewinnung und Weiterverarbeitung werden in der Ausstellung ebenso dargestellt wie die Hilfsmittel zur Echtheitserkennung der Goldbarren aus dem täglichen Einsatz in der Bundesbank. Die Ausstellung ist bis zum 30. September 2018 in Frankfurt am Main zu sehen.

Weitere Informationen unter: www.bundesbank.de

In eigener Sache: Udo Steffens neuer FIRM-Vorstandsvorsitzender

Professor Dr. Udo Steffens ist seit dem 1. Mai 2018 neuer Vorstandsvorsitzender der Frankfurter Gesellschaft für Risikomanagement und Regulierung (FIRM). Steffens, bislang Präsident der Frankfurt School, wird der erste Vertreter einer wissenschaftlichen Institution im Vorsitz dieses Gremiums sein. Damit bestärkt FIRM seinen Auftrag, eine der führenden Einrichtungen für die Förderung von Forschung und Lehre im Bereich Risikomanagement und Regulierung in Deutschland zu sein. Steffens übernimmt das Amt von Frank Westhoff, der den Vorstandsvorsitz im Jahr 2017 angetreten hatte. Westhoff ist als Vertreter der DZ BANK seit Vereinsgründung 2009 im Vorstand und wird diesem Gremium auch weiterhin angehören. Sein Rücktritt vom Vorsitz erfolgt aus privaten Gründen.

Weitere Informationen unter: www.firm.fm

Risikomanagement in Zahlen

12 Jahre Haft ...
wegen Korruption sitzt der ehemalige brasilianische Präsident Luiz Inácio Lula da Silva ab.

25. Mai ...
ist der Stichtag, an dem die neue Datenschutzgrundverordnung (DSGVO) in Kraft tritt.

110 Millionen US-Dollar ...
Strafe zahlt die Investmentbank Goldman Sachs wegen Aufsichtsversagens.

2,7 Milliarden US-Dollar ...
Rekordgewinn fuhr die Großbank Morgan Stanley im ersten Quartal ein.

Datum	Konferenz	Ort	Link
30. Mai 2018	6. Hanseatischer Compliance Tag	Hamburg	www.hanseatischer-compliance-tag.de
7. - 8. Juni 2018	International Risk Management Conference	Paris	www.therisksociety.com
17.- 22. Juni 2018	ACFE Global Fraud Conference	Las Vegas	www.fraudconference.com
19. - 20. Juni 2018	7. Messekongress „Finanzen & Risikomanagement“	Leipzig	www.assekuranz-messekongress.de