bank&compliance

bank&compliance-Newsletter

Ausgabe 10/2013 • November 2013

Inhaltsverzeichnis

Autoren: Max Colchester, Jason Douglas, Christian Grimm, Stefan Hirschmann, Andreas Kissler, Anja Kraus, Alexander Kolyandr, John Letzing, Jeannette Neumann, Madeleine Nissen, Andrey Ostroukh, Margot Patrick, Shayndi Raice

Im Land der Geldwäscher

Stefan Hirschmann

Schwächen in der derzeitigen Gesetzgebung machen Deutschland nach Meinung des Tax Justice Network zu einem Eldorado für Geldwäscher. Schätzungen gehen davon aus, dass zwischen 29 und 57 Mrd. € jährlich in Deutschland gewaschen werden. Zu den Quellen dieser enormen Summe gehören sowohl korrupte Politiker aus Ländern des globalen Südens als auch die organisierte Kriminalität. Die neue Bundesregierung und der neue Bundestag werden deshalb von mehreren NGOs aufgefordert, zügig für Abhilfe zu sorgen. Das ist im Kern natürlich eine richtige Forderung. Wer sollte da anderer Meinung sein? In der Praxis verhält es sich aber – wie so oft – etwas differenzierter. Betrug, Geldwäsche und Terrorismusfinanzierung, Korruption, Kartellrechtsverstöße oder Insiderbetrug – Wirtschaftskriminalität hat nämlich viele Gesichter. Wer durch kriminelle Handlungen in den Besitz von Financial Crime Money gelangt, steht schnell vor dem Problem der Geldwäsche, denn Schwarzgeld aus illegalen Geschäften muss wieder in den legalen Wirtschaftskreislauf eingeschleust werden. Verschiedene Delikte und strafbare Handlungen sind deshalb oft miteinander verkettet, sie treten im komplexen Organismus des Geldkreislaufs am deutlichsten zu Tage. Hier, im Bankwesen, bei der Bekämpfung von Geldwäsche anzusetzen, ist deshalb richtig. Den Instituten die ganze Last der gesetzlichen Verpflichtungen aufzuerlegen, ist es hingegen nicht. Das Gleichgewicht einer Lastenverteilung und gemeinsamen Zusammenarbeit von Politik, Strafverfolgungsbehörden und Verpflichteten ist aus der Perspektive vieler Banken nicht mehr gegeben. Bei einer vergleichenden Bewertung der 17 Euro-Länder hinsichtlich der Einhaltung der Empfehlungen der Financial Action Task Force (FATF) zur Bekämpfung der Geldwäsche schnitt Deutschland zuletzt ausgesprochen schlecht ab. Geldwäsche in Deutschland kann recht einfach sein. Doch das Problem sind nicht die Compliance-Maßnahmen der Banken und Sparkassen, sondern dringend verbesserungsbedürftig ist die Beaufsichtigung des Nichtfinanzsektors. Das Gesetz verpflichtet neben Finanzinstituten schließlich u.a. auch Juweliere, Rechtsanwälte und Wirtschaftsprüfer, Immobilienmakler, Spielbanken und Online-Casinos. Zudem sind noch immer organisatorische Probleme erkennbar. Eine dezentrale Organisation der Geldwäschebekämpfung, die eine parallele Bearbeitung durch Landeskriminalämter und BKA vorsieht und nicht – wie international weit verbreitet – nur durch eine allein zuständige zentrale Geldwäschebekämpfungsbehörde, ist nicht mehr zeitgemäß. Trotzdem sind harmonisierte Verwaltungsvorschriften, die alle Verpflichtetengruppen umfassen, bislang nicht geplant. So wird es keiner besonders ausgeprägten Beobachtungsgabe bedürfen, um zu erkennen, dass das bestehende Ungleichgewicht wohl auch in naher Zukunft erhalten bleiben wird. Im Jahr 2012 entfielen fast 97 % der Geldwäscheverdachtsanzeigen auf Banken, Versicherer und Finanzdienstleister. Seit 2008 hat sich die Anzahl auf annähernd 14.000 pro Jahr verdoppelt. Von den übrigen Teilen der Wirtschaft kommt hingegen fast nichts. Verdachtsmeldungen von Veranstaltern und Vermittlern von Glücksspiel im Internet sind beim Bundeskriminalamt bislang gar nicht eingegangen. Null. Gerade in diesem Segment wird das Compliancerisiko jedoch besonders hoch eingeschätzt. Vor den Leistungen der Kreditwirtschaft darf man dagegen ruhig einmal den Hut ziehen. Die Institute bilden das Rückgrat der Geldwäschebekämpfung in Deutschland. Zur Abwechslung liegt das Problem dieses Mal bei den anderen.

Open Source Intelligence

Bessere Ergebnisse in Betrugsermittlungen

Versicherungen in Deutschland haben zunehmend mit Betrugsfällen zu kämpfen. Ermittlungen lassen sich durch den Einsatz von Open Source Intelligence (OSINT) schneller und effektiver durchführen. Eine entscheidende Rolle bei der Aufklärung spielen Social Media. | Florian Peil

Die Zahlen sind alarmierend: Auf acht bis zwölf Milliarden Euro schätzt das Beratungsunternehmen Accenture den durch Betrug entstandenen Schaden bei Versicherungen pro Jahr in Europa – Tendenz steigend [vgl. Accenture 2013]. Laut der im Juni 2013 veröffentlichten Studie ist die Anzahl der Betrugsfälle in den vergangenen 36 Monaten um rund zehn Prozent gestiegen. Bei Betrügern besonders beliebt sind die Kfz- und die Haftpflichtversicherung. Angesichts der explodierenden Kosten durch Betrugsfälle sind die Versicherungen gezwungen, Betrugsversuche möglichst frühzeitig zu erkennen und effizient aufzuklären. Doch viele Unternehmen setzen laut Accenture noch immer auf veraltete Technik und überholte Analyse-Werkzeuge. Diese verhinderten in bis zu acht Prozent der Fälle eine Identifikation betrügerischer Handlungen.

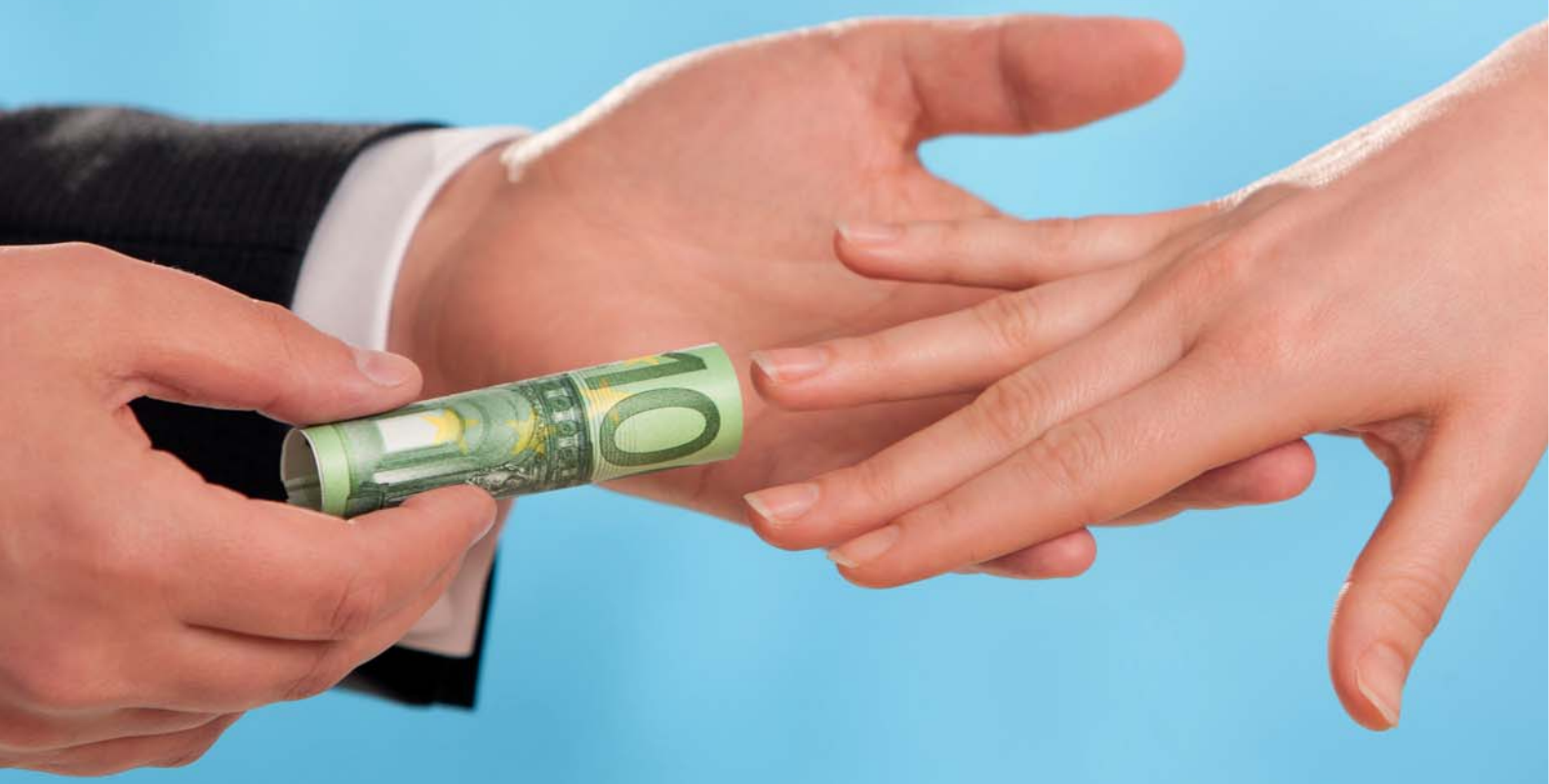
Dabei können die Versicherungen heute auf innovative Software-Lösungen zurückgreifen, die dazu beitragen, Betrugsermittlungen effizienter und erfolgreicher zu gestalten [vgl. SAS 2012, S. 3ff.]. Eine entscheidende Rolle kommt dabei Open Source Intelligence (OSINT) zu. Der Begriff entstammt ursprünglich der Welt der Nachrichtendienste und bezeichnet in diesem Kontext die systematische Sammlung und Aufbereitung von Informationen aus offen und legal zugänglichen Quellen, um den Informationsbedarf von Regierungen im Hinblick auf die nationale Sicherheit zu erfüllen [vgl. Störger/Schaurer 2010, S. 3]. Heute wird darunter vor allem die systematische Sammlung und Aufbereitung von Informationen aus offenen Quellen verstanden, die auch von Firmen oder Privatpersonen durchgeführt wird. Eine verbindliche Definition von OSINT gibt es also nicht.

„Big Data" im Kontext Betrugsermittlung

Immer mehr offen zugängliche Quellen sind heute im Internet verfügbar. Die Menschheit hat ungeheure Datenmengen angesammelt, die täglich weiter wächst: „Big Data" ist das Schlagwort der Stunde. Damit steigt auch die Zahl der für Ermittlungen relevanten Informationen. Doch die Datenflut hat auch eine Kehrseite: Die schiere Menge der im Internet verfügbaren Informationen erschwert oder verhindert immer häufiger den Sucherfolg. In der Folge sind relevante Informationen in dieser Datenflut immer schwerer zu lokalisieren. Hinzu kommt, dass Beiträge durch neuere Inhalte immer rascher verdrängt werden. Eine klassische Recherche über Suchmaschinen wie Google, Bing oder Yahoo bringt somit immer weniger substanzielle Ergebnisse. Zudem dauern die Ermittlungen tendenziell länger, bis relevante Ergebnisse vorliegen. Ein weiteres Hindernis bei einer OSINT-Recherche besteht darin, dass den Suchmaschinen der größte Teil des Internets verborgen ist – das so genannte „deep web". Einige Schätzungen gehen davon aus, dass Suchmaschinen gerade einmal ein Prozent der vorhandenen Datenmenge erfassen. Diese Entwicklungen erfordern also zweierlei: den Einsatz von Software-

Die SCHUFA-GwG-Auskunft

Drum prüfe, wer sich … bindet.



Einfach, schnell
und fallabschließend.

Jetzt bestellen

www.schufa-
gwg-auskunft.de

Mit der SCHUFA an Ihrer Seite schöpfen Sie die erweiterten Prüfungsmöglichkeiten des GwG kostengünstig und fallabschließend aus. Die SCHUFA-GwG-Auskunft ist mit Blick auf § 7 Abs. 2 GwG das Mittel Ihrer Wahl, wenn es um die Identifizierung des wirtschaftlich Berechtigten geht – ohne dass die Auskunftsdaten einer zusätzlichen Prüfung bedürfen. Erfahren Sie mehr unter **www.schufa-gwg-auskunft.de**.

Wir schaffen Vertrauen

schufa

Tools zur Unterstützung von Ermittlungen im Internet und geschulte Rechercheure, die diese Software zum Einen bedienen und zum Anderen die Ergebnisse zu analysieren wissen. Inzwischen ist eine ganze Industrie rund um die gezielte Nutzung von Big Data entstanden. Verschiedene Methoden und Ansätze zur Analyse der Datenberge existieren. Davon eignet sich eine besonders zur Tiefenrecherche: das so genannte „Information Retrieval".

Bei der entsprechenden OSINT-Lösungen handelt es sich im Kern um ein Web-Monitoring-System, das Suchmaschinen-Technologie mit semantischen und statistischen Analysen verknüpft. Damit lässt sich jede öffentliche Webseite durchsuchen und indexieren. Auch Inhalte von Social Media lassen sich über Schnittstellen einbinden und verarbeiten. Somit sind praktisch alle offen im Internet vorhandenen Inhalte durchsuchbar – und auch tief im Internet vergrabene Informationen lassen sich aufspüren.

Social Media liefern wertvolle Erkenntnisse bei Ermittlungen

Ihre Fähigkeiten voll ausspielen kann diese Software bei der Recherche in sozialen Medien. Diese liefern häufig besonders wertvolle Erkenntnisse im Rahmen von Ermittlungen, allen voran Facebook. Der Grund: Immer mehr Menschen offenbaren in diesen Netzwerken freiwillig Details aus ihrem Privatleben. Youtube, Twitter und Facebook ermöglichen mitunter tiefe Einblicke in das Leben potenzieller Täter und geben Aufschluss über Persönlichkeit und Verhalten. Auch Kriminelle nutzen Facebook – und besprechen dort auch ihre Aktivitäten. Ein Beispiel: Ein 22-Jähriger hatte seiner Versicherung sein iPhone als kaputt gemeldet. Ein Freund sei darauf getreten. Was den Ermittler skeptisch machte: Wenige Tage zuvor war das neue iPhone 5 erschienen. Zudem hatte der 22-Jährige bereits im Vorjahr ein Notebook als kaputt gemeldet – Schuld sei ebenfalls ein Freund gewesen. Eine mittels OSINT-Software durchgeführte Recherche ergab, dass der Betroffene auf seiner Seite öffentlich zugängliche Fotos von sich und seinem neuen iPhone gepostet hatte. Aufschlussreich waren insbesondere die zugehörigen Kommentare: Glückwünsche mehrerer Freunde zu der „gelungenen Aktion"; der Dank des 22-Jährigen für die Hilfe; die Verabredung, die Tat bei einem anderen Freund zu wiederholen. Ein gefundenes Fressen für die Ermittler.

In einem anderen Fall hatte ein 42 Jahre alter Dachdecker Berufsunfähigkeit durch Personenschaden bei seiner Versicherung beantragt: Sein rechtes Knie sei infolge eines Autounfalls zerschmettert, sodass er ohne Krücke nicht mehr laufen könne. Die Versicherung stimmte zu, nachdem ein ärztliches Gutachten vorlag. Doch auf Facebook veröffentlichte der 42-Jährige wenige Wochen später Fotos, die er von sich auf einem Berggipfel in den Alpen per Smartphone aufgenommen hatte, inklusive der Metadaten wie Orts- und Zeitangabe. Im Rahmen der Ermittlungen via Software stellte sich heraus, dass der in den fingierten Unfall verwickelte Kfz-Fahrer ein Freund des Mannes war - ebenso wie der Arzt, der das entscheidende Gutachten ausgestellt hatte. Beide Mittäter waren mit dem Täter auf Facebook befreundet und hatten, wie im ersten Beispiel, die Freizeitaktivitäten des Mannes kommentiert.

Die Nutzung einer OSINT-Software durch einen erfahrenen Rechercheur konnte diese Ergebnisse in kurzer Zeit zutage fördern. Eine manuelle Recherche durch einen Ermittler hingegen hätte vermutlich mehrere Stunden bis Tage gedauert – Erfahrung bei der Recherche in sozialen Netzwerken vorausgesetzt.

Heute sind also bei Ermittlungen im Internet die Kombination von OSINT-Software und entsprechenden Recherche-Fähigkeiten vonnöten. Auf diese Weise lassen sich schnell gute Ergebnisse erzielen.

Fazit

Immer mehr Betrugsfälle belasten die Versicherungen. Eine schnelle und effiziente Aufklärung ist notwendig. Dies ermöglicht der Einsatz von erfahrenen OSINT-Rechercheuren zusammen mit einer entsprechenden Software. Dieses Vorgehen trägt dazu bei, Ermittlungen schneller und effizienter abzuwickeln. Zugleich ermöglicht es eine Entlastung von Mitarbeitern. Damit bleiben bei der Schadenabwicklung mehr Zeit und Ressourcen für die Betreuung ehrlicher Kunden – was wiederum die Kundenbindung stärkt.

Quellenverzeichnis sowie weiterführende Literaturhinweise:

Accenture (Hrsg.) (2013): Betrug bei Sach- und Haftpflichtversicherungen europaweit auf dem Vormarsch. Kronberg im Taunus, 2013.

Störger, Jan/Schaurer, Florian (2010): OSINT Report 3/2010: The Evolution of Open Source Intelligence. ISN ETH Zürich, 2010.

SAS (Hrsg.) (2012): Combating Insurance Claims Fraud. How to Recognize and Reduce Opportunistic and Organized Claims Fraud. White Paper, 2012.

Autor:
Florian Peil, Head of Intelligence,
Riskworkers GmbH, München.

Russische Bank wegen Geldwäsche geschlossen

Die russische Zentralbank greift unter neuer Führung hart gegen Geldwäsche und andere illegale Finanzgeschäfte durch. Wegen fehlerhafter Bilanzen und wiederholter Verletzung der Geldwäsche-Gesetze hat die Notenbank dem mittelgroßen Kreditinstitut Master Bank in Moskau die Banklizenz entzogen. Das Geldhaus ist in Russland auch dafür bekannt, dass im Verwaltungsrat ein Verwandter von Präsident Wladimir Putin sitzt. Die Stilllegung des Instituts ist bislang die auffälligste Aktion der Notenbank unter der neuen Gouverneurin Elvira Nabiullina. Die erste Frau an der Spitze der Behörde hatte im Juli die Führung übernommen. Das Vorgehen gegen die Master Bank könnte ein Fanal sein im Kampf Russlands gegen das chronische Problem mit der Geldwäsche. Igor Putin sitzt immer noch im Verwaltungsrat der Master Bank, für kurze Zeit war er sogar Vizepräsident des Instituts. Ein Kreml-Sprecher versicherte, Igor Putin sei zwar ein „entfernter Verwandter" des russischen Präsidenten, aber dass „die beiden nichts gemeinsam haben außer dem Namen" und keine geschäftlichen Verbindungen unterhalten. Im Übrigen spiele der Kreml keine Rolle bei der Entscheidung der Zentralbank. Gouverneurin Nabiullina habe von Beginn ihrer Amtszeit an gesagt, dass sie sich auf die Bankenregulierung konzentrieren werde. Sie folge ihrer Linie konsequent. Die Gouverneurin hatte der Duma, dem Unterhaus des russischen Parlaments, erklärt, die Bank weise eine Kapitallücke von mindestens 2 Mrd. Rubel auf, umgerechnet etwa 45 Mio. €. „Die Bank hat ihre wahre Verfassung verschleiert, indem die falsche Berichte eingereicht hat". Sie habe Geschäfte in der Schattenwirtschaft gemacht, illegale Transaktionen durchgeführt und die Geldwäsche-Gesetze wiederholt verletzt. „Wir waren gezwungen, zu dieser Ultima-Ratio-Maßnahme zu greifen", sagte Nabiullina. Bei der Master Bank war niemand für einen Kommentar zu erreichen. Die Büros der Bank waren zuletzt geschlossen. Die Polizei teilte mit, sie durchsuche die Zentrale des Instituts. In den letzten Jahren hatte die Zentralbank regelmäßig kleinere Banken wegen ähnlicher Vorwürfe dichtgemacht. Die Master Bank ist aber das größte Institut, das seit der Finanzkrise 2008/09 seine Lizenz verloren hat. Nach Bilanzsumme steht die Master Bank in Russland an 75. Stelle. Sie hat zentrale Filialen in Moskau und St. Petersburg. Nach eigenen Angaben hat sie das drittgrößte Netz von Geldautomaten in dem Land. Die Regulierungsbehörden teilten mit, die Sparer würden ihr Geld aus dem nationalen Einlangensicherungsfonds wiederbekommen, der Ausfälle bis zu einem gewissen Limit abdeckt. Regierungsvertreter gehen nicht davon aus, dass der Staat weiteres Geld zuschießen muss, um die Forderungen abzudecken. Dabei ist die Master Bank der bislang größte Fall für den Fonds, die Summe der Forderungen liegt bei geschätzten 30 Milliarden Rubel. Die Bank verwaltet private Einlagen in Höhe von 47 Mrd. Rubel, die gesamten Vermögenswerte belaufen sich auf 74 Mrd. Rubel. Schon vor einem Jahr stand die Master Bank im Visier polizeilicher Ermittlungen. Sie konnte aber ohne Einschränkungen weiter Geschäfte machen und warb in den vergangenen eineinhalb Jahren aggressiv um neue Kunden. Das Innenministerium teilte am Mittwoch mit, die Zentrale sei durchsucht worden. Die Behörden untersuchten illegale Geschäfte, darunter Transaktionen über 2 Mrd. Rubel. Der Vorgänger der Zentralbank-Gouverneurin Nabiullina, Sergej Ignatjew, hatte im Februar seine Befürchtungen hinsichtlich massiver Geldwäschegeschäfte in Russlands Bankensystem geäußert. Er ging dabei aber nicht auf einzelne Institute ein. Auf das Bankensystem Russlands werde die Schließung der Master Bank nur einen sehr begrenzten Einfluss haben, sagten die Analysten der VTB, Russlands zweitgrößter Bank. Es sei denn, der Lizenzentzug

löse den Einlagenabzug von anderen kleineren Banken aus. Sie sagten, dass die Bank eine zu vernachlässigende Präsenz auf dem Interbankenmarkt habe, der Effekt auf andere Institute dementsprechend gering sei.

Zu wenig Schutz für Whistleblower

Wer hierzulande auf Missstände hinweist, begibt sich auf Glatteis: Deutschland – ebenso wie 14 andere EU-Staaten – biete Whistleblowern nur geringen Schutz, urteilt die Antikorruptionsorganisation Transparency International in ihrem jüngsten Bericht. Nur vier Ländern in der EU bescheinigt die Organisation, dass sie die Aufdecker von Verfehlungen gut schütze: Neben Großbritannien sind dies Luxemburg, Rumänien und Slowenien. In Deutschland fehlten klare rechtliche Regelungen, sodass Whistleblower die Konsequenzen ihres Tuns nicht abschätzen können, sagte Edda Müller, Vorsitzende von Transparency Deutschland. „Whistleblower sind auf Seiten der Machtlosen. Sie biedern sich gerade nicht bei den Mächtigen an. Diese Zivilcourage verdient unsere Unterstützung“, so Müller weiter. Lediglich Beamte genössen hierzulande einen guten Schutz vor arbeitsrechtlichen Konsequenzen. Anders als Tarifbeschäftigte in der öffentlichen Verwaltung und Arbeitnehmer in der Privatwirtschaft dürfen sie sich bei Korruptionsverdacht nämlich an die Staatsanwaltschaft wenden. OECD, G20 und Europarat fordern Deutschland seit Langem auf, den Schutz für Whistleblower in der Privatwirtschaft zu verbessern. Die OECD hatte Deutschland daher bereits Anfang 2011 eine Zweijahresfrist eingeräumt, ihre Empfehlungen umzusetzen - leider ohne Erfolg. Jetzt sei Deutschland erneut aufgefordert, bis März 2014 über Fortschritte zu berichten, erläuterte die Antikorruptionsorganisation. Rainer Frank, Leiter der Arbeitsgruppe Hinweisgeber, hat festgestellt, dass in deutschen Unternehmen eine immer stärkere Bereitschaft bestehe, interne Whistleblower-Systeme einzurichten. Allerdings sei die Wirtschaft sehr zögerlich, einen gesetzlichen Schutz für Whistleblower einzufordern. Wie ein guter Schutz auszusehen habe, erläuterte er so: Wer Dinge wahrnehme, von denen er Schäden für Personen, Umwelt oder Vermögen fürchten könne, müsse das Recht haben, gegenüber dem Arbeitgeber oder dessen Beauftragten darauf hinzuweisen, ohne vor arbeitsrechtlichen oder anderen Konsequenzen Angst haben zu müssen. Wenn offensichtlich sei, dass dem Hinweis nicht nachgegangen werde, müsse der Whistleblower auch die zuständigen Stellen außerhalb des Unternehmens ansprechen können. Der letzte Versuch einer Neuregelung wurde unter der Großen Koalition im Jahr 2008 als Reaktion auf den Gammelfleischskandal unternommen. Ein gemeinsamer Gesetzesvorschlag von Justiz-, Verbraucher- und Arbeitsministerium wurde jedoch nie vom Kabinett verabschiedet. Transparency Deutschland hatte kürzlich gemeinsam mit der Vereinigung Deutscher Wissenschaftler und der deutschen Sektion der IALANA den Whistleblower-Preis an Edward Snowden verliehen. Mit diesem Preis wurde der Mut eines Mannes geehrt, der auf gravierende Missstände in den Reihen der Mächtigen hingewiesen hat.

Steueroase Deutschland?

Das Tax Justice Network hat den Schattenfinanzindex 2013 mit einem Ranking der Schattenfinanzzentren vorgestellt. Darin nimmt Deutschland mit Rang 8 wieder einen Platz unter den Top 10 internationaler Steueroasen ein. Die dritte Ausgabe des Schattenfinanzindex zeigt unter

anderem, dass das Vereinigte Königreich der größte und wichtigste Player im weltumspannenden Netz finanzieller Geheimhaltungspraktiken ist. Obwohl Großbritannien selbst nur Platz 21 der Rangliste einnimmt, unterstützt und kontrolliert die britische Regierung ein Konglomerat von Schattenfinanzentren in seinen Überseegebieten und Kronkolonien – von den Kaimaninseln über Bermuda bis Jersey und Gibraltar. Aggregiert man die Werte für alle diese Gebiete, übertrifft das britische Netzwerk auch den Spitzenreiter des Index, die Schweiz, bei weitem. Insgesamt zeigt der Index, dass sich in Sachen Geheimhaltung und Verschleierung nur wenig getan hat – trotz der vollmundigen Ankündigungen durch die Regierungen im Rahmen der G20 und der OECD. Und selbst der Druck, der beispielsweise durch die USA auf die Schweiz ausgeübt wurde, hat lediglich Löcher in das dichte Netz der Geheimniskrämerei gerissen.

Die Top 10 des Schattenfinanzindex 2013

Rang	Land	FSI-Score
1	Schweiz	1.765,3
2	Luxemburg	1.454,5
3	Hongkong	1.283,4
4	Kaimaninseln	1.233,6
5	Singapur	1.216,9
6	USA	1.213,0
7	Libanon	747,9
8	**Deutschland**	**738,3**
9	Jersey	591,7
10	Japan	513,1

Razzia bei Infinus

Der Dresdner Finanzdienstleister Infinus und die Tochterunternehmen der Unternehmensgruppe sind in das Visier der Ermittler geraten. Polizeikräfte und Staatsanwaltschaft haben sämtliche Büroräume durchsucht und Unterlagen sowie elektronische Datenträger und Computer sichergestellt. Grund für die bundesweite Aktion ist der Vorwurf des Betrugs und der Schädigung von Anlegern und Investoren. Es soll Unregelmäßigkeiten beim Handel mit Finanzprodukten gegeben haben. Möglicherweise war das Unternehmen an einem Schneeballsystem beteiligt. Mehrere Personen aus der Unternehmensführung wurden festgenommen. Prof. Dr. Kewan Kadkhodai, Vorstandsmitglied der Infinus-Gruppe, erachtet die Vorwürfe als haltlos und sicherte in einer Pressemitteilung eine schnelle Aufklärung zu. Das Unternehmen habe sich absolut auf dem Boden der Gesetze bewegt, hieß es.

EECH: Haftstrafen wegen Betrugs

Die Hamburger Strafkammer hat die beiden ehemaligen Vorstände der European Energy Consult Holding AG (EECH), Tarik Ersin Yoleri und Michael Bode, zu empfindlichen Freiheitsstrafen verurteilt. Die Hamburger EECH-Gruppe warb bei mehreren tausend Kleinanlegern rund 100 Mio. € für Investments in erneuerbare Energien ein. Die Gelder sollten für Windkraft- und Photovoltaikprojekte in Deutschland, Frankreich und Italien verwendet werden. Stattdessen entpuppte sich der ehemalige Vorstandsvorsitzende Yoleri als glühender Kunstliebhaber und kaufte nach Angaben der Hamburger Rechtsanwälte Gröpper & Köpke für rund 25 Mio. € Kunstgegenstände. Als das bekannt wurde, stürmten die Anleger das

Emissionshaus und machten Schadensersatzansprüche geltend. Das Emissionshaus ging in die Insolvenz. Jetzt hat die Hamburger Strafkammer zwei der ehemaligen Unternehmensverantwortlichen wegen schweren Betrugs zum Nachteil der Anleger verurteilt. Yoleri bekam fünf Jahre, Bode kam mit zwei Jahren davon; seine Strafe wurde auf Bewährung ausgesetzt.

„Königreich Deutschland" ist am Ende

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) hat dem Wittenberger Peter Fitzek aufgegeben, das im Namen des nicht eingetragenen Vereins „Königreich Deutschland" ohne Erlaubnis betriebene Versicherungsgeschäft sofort einzustellen und durch Kündigung der geschlossenen Verträge abzuwickeln. Die von dem selbst ernannten „obersten Souverän" Fitzek angebotenen Krankenversicherungen des „Königreich Deutschland" begründen nach Auffassung der BaFin keinen Anspruch auf Absicherung im Krankheitsfall. Die Krankenversicherungspflicht entfällt auch nicht durch die „Staatsangehörigkeit" genannte Mitgliedschaft im „Königreich Deutschland". Dies könnte für diese Personen dazu führen, dass sie zur Zahlung von gegebenenfalls beträchtlichen Prämienzuschlägen verpflichtet werden, deren Höhe auch von der Dauer der Zeiten der Nichtversicherung abhinge. Für Fitzek besteht das Risiko einer Strafverfolgung im Falle einer Nichtbeachtung der finanzaufsichtlichen Vorgaben.

Rabobank zahlt wegen Libor-Manipulation

Die Rabobank Groep hat im Skandal um manipulierte Zinsen eine teure Einigung mit den Aufsichtsbehörden weltweit erzielt. Das niederländische Geldhaus zahlt eine Strafe von insgesamt 774 Mio. €. Der Vergleich hat zudem auch personelle Konsequenzen: Rabobank-Chef Piet Moerland gibt sein Amt auf. Die Niederländer sind das fünfte Institut weltweit, das die seit Jahren laufenden Ermittlungen zum mutmaßlichen Zinspfusch mit einem Vergleich beendet hat. Im Vergleich zu anderen Einigungen ist der Deal mit den Behörden aus den USA, den Niederlanden, Japan und Großbritannien aber hoch. Es ist die zweitteuerste Einigung bisher. Einige Mitarbeiter der Bank seien durch Fehlverhalten aufgefallen. Sie hätten versucht, die Referenzzinssätze Libor und Euribor zu beeinflussen. Insgesamt seien 30 Mitarbeiter betroffen, die Bank beschäftigt weltweit mehr als 60.000 Mitarbeiter. „Dies hätte niemals passieren dürfen", entschuldigte sich Rabobank-Chef Moerland. Angesichts der Tragweite des Vorgangs legte Moerland sein Amt nieder. Nachfolger soll vorläufig Rinus Minderhoud werden.

RBS zahlt wegen Hypothekenpapieren

Die Royal Bank of Scotland (RBS) legt einen Rechtstreit mit der US-Börsenaufsicht über Hypothekenpapiere gegen Zahlung von 153,7 Mio. US-$ bei. Die betroffene RBS-Tochter gestehe weder ihre Schuld ein noch weise sie Vorwürfe der SEC zurück, hieß es. Die Aufseher hatten der RBS Securities Inc, seinerzeit als Greenwich Capital Markets bekannt, vorgeworfen, Investoren gegenüber irreführende Angaben zu Subprime-Papieren gemacht zu haben. Betroffen waren Residential Mortgage Backed Securities (RMBS) im Volumen von 2,2 Mrd. US-$ aus dem Jahr 2007. Für die Zahlung hat die Bank bereits Rücklagen gebildet.

Milliardenstrafe für die Bank of America

Im Streit um die Qualität von Hypothekenpapieren nehmen die Strafen für die Banken immer größere Ausmaße an. Nachdem J. P. Morgan sich Informanten zufolge mit dem US-Hypothekenkreditregulierer FHFA auf eine Milliardenstrafe geeinigt hat, könnte es für die Bank of America noch dicker kommen. Die Behörde will dem Institut eine Strafe von mehr als 6 Mrd. US-$ aufbrummen. Diese Summe hatte die Behörde ursprünglich auch von J. P. Morgan eingefordert, die FHFA gab sich dann aber mit 4 Mrd. US-$ zufrieden. Hintergrund für die Strafe sind Anschuldigungen, die Bank habe die Hypothekenfinanzierer Fannie Mae und Freddie Mac über die Qualität von Hypotheken in die Irre geführt, die das Kreditinstitut während des Immobilienbooms an die beiden Hypothekenbanken verkauft hatte.

Insgesamt muss J.P. Morgan sogar 13 Mrd. US-$ berappen, neben dem Geld für die FHFA fallen 4 Mrd. US-$ zur Entschädigung von Kunden an, dazu kommen 5 Mrd. US-$ Strafe an weitere Behörden. Die FHFA hat insgesamt 17 Institute verklagt wegen der Hypothekengeschäfte mit Fannie und Freddie. Die Bank of America weist dabei mit 57 Mrd. US-$ das größte Geschäftsvolumen auf. J. P. Morgan kommt lediglich auf 33 Mrd. US-$. Bei der Bank of America war zunächst keine Stellungnahme zu erhalten.

Milliardenstrafe gegen HSBC verhängt

Die britische Bank HSBC muss wohl in einer juristischen Auseinandersetzung, die auf einen elf Jahre alten Fall zurückgeht, Milliarden berappen. Ein Distriktgericht im US-Bundesstaat Illinois verurteilte die mittlerweile zu der britischen Bank gehörende Household International Inc zu einer Zahlung von insgesamt 2,46 Mrd. US-$. Zuvor hatte eine Jury das Unternehmen des Betrugs für schuldig befunden. Die Summe umfasst 1,48 Mrd. US-$ an Entschädigungen für 10.902 Anspruchsteller, die sich zu einer Sammelklage zusammengeschlossen hatten.

Dazu kommen 986 Mio. US-$ an zusätzlichen Kosten. Zahlen müssen sowohl die HSBC-Tochter als auch drei ehemalige Manager des Unternehmens. Vor mehr als vier Jahren war eine Jury bereits zu dem Schluss gekommen, dass das Unternehmen Anfang des vergangenen Jahrzehnts gegen das US-Wertpapiergesetz verstoßen habe. So seien für die Investoren wichtige Informationen im Kleingedruckten versteckt und die Anleger über die Kreditqualität in die Irre geführt worden. Außerdem prangerte die Jury die Buchführung des Unternehmens an. Die Vergehen geschahen zwischen März 2001 und Oktober 2002. HSBC hat Household International 2002 übernommen. Zu dem Zeitpunkt war das Unternehmen der zweitgrößte Anbieter von Konsumentenkrediten in den USA, vor allem für Kreditnehmer mit niedriger Bonität. Ein Sprecher von HSBC kündigte an, in Berufung gehen zu wollen. Zudem habe die Bank die Investoren in ihren Veröffentlichungen stets auf dem Laufenden gehalten.

Das Urteil sei nur der nächste Schritt in einem 11 Jahre alten Fall. Die Gegenseite sprach von überwältigenden Beweisen für den Betrug, den man der Jury habe darlegen können. Man habe gezeigt, wie die Investoren unter dem Betrug gelitten haben, sagte ein Anwalt des Klageführers.

Deutsche Börse muss zahlen

Der Streit mit den USA wegen eines Verstoßes gegen Iran-Sanktionen wird für die Deutsche Börse wohl nur halb so teuer wie zunächst gedacht. Im Januar war noch eine Strafzahlung von 340 Mio. US-$ im Gespräch, nun ist eine Reduzierung der Summe auf 152 Mio. US-$ möglich, wie der Frankfurter Börsenbetreiber mitteilte. In dem Streit geht es um das Konto eines Kunden der Deutsche-Börse-Tochter Clearstream. Dieser Kunde hatte iranische Investoren, und Clearstream wurde von den Amerikanern vorgeworfen, mit der Kontoführung gegen Iran-Sanktionen verstoßen zu haben. Diese waren in den 80er-Jahren nach einem Bombenanschlag auf US-Truppen verhängt worden. Die USA hatten den Iran als Urheber verurteilt. Clearstream befand sich wegen dieser Vorgänge seit Jahren im Streit mit der amerikanischen Exportkontrollbehörde OFAC. Im Januar hatte sich dann eine Lösung in dem Streit abgezeichnet, allerdings war der Deutschen Börse die damals im Raum stehende Strafe zu hoch. Nun teilte die OFAC mit, eine zu verhängende Strafe würde nach aktuellem Stand 168,8 Mio. US-$ betragen. Clearstream könne den Streit nun beenden, wenn sich die Deutsche-Börse-Tochter auf einen Vergleich einlässt.

Diese gütliche Einigung würde die Strafe nochmals um 10 % reduzieren. Damit würde die Strafe auf knapp 152 Mio. US-$ sinken. Die Deutsche Börse will über das Angebot der US-Behörde nun nachdenken. Eine Entscheidung werde in den kommenden Tagen gefällt, sagte ein Sprecher. Teuer wird es aber dennoch: Der DAX-Konzern kündigte an, im dritten Quartal eine Rückstellung entsprechend der nun diskutierten Strafe zu bilden. Im Vorquartal hatte die Deutsche Börse einen Nettogewinn von 171 Mio. € erzielt. Die Rückstellung dürfte somit einen Großteil der Gewinne im dritten Quartal aufzehren. Clearstream war nicht das einzige Unternehmen, das sich gegen Vorwürfe der US-Behörden wegen Iran zu wehren hatte. Im Visier der Ermittler standen mehrere europäische Institute. Auch die Deutsche Bank und die UniCredit-Tochter HypoVereinsbank zählten dazu. Die Deutsche Bank hatte sich 2007 selbst verpflichtet, keinerlei neue Geschäfte im Iran zu tätigen und alte so schnell wie möglich auslaufen zu lassen. Ihre Repräsentanz in Teheran hat die Bank geschlossen. Einige Institute mussten bereits tief in die Tasche greifen. So hatte die britische Standard Chartered insgesamt 667 Mio. US-$ gezahlt, um Anschuldigungen wegen illegaler Iran-Geschäfte aus der Welt zu räumen.

Banken stemmen sich gegen Verschuldungsquote

In den USA lassen sich Banken vorrangig an ihrer Verschuldungsquote messen, hierzulande wehren sich Privatbanken noch heftig dagegen. Die geplante Leverage Ratio habe keinen Einfluss auf die Finanzmarktstabilität und sei eine Belastung für die Wirtschaft, sagte Jürgen Fitschen, Präsident des Bankenverbands BdB.

Die Regulatoren haben bislang im Regelwerks Basel III ab 2018 eine Leverage Ratio von mindestens drei Prozent geplant. Die Bilanzsumme kann damit maximal auf das 33,3-Fache des Kapitals gehebelt werden. Die Deutsche Bank hat derzeit eine Quote von 3,1 Prozent, die Commerzbank von 4,1 Prozent. Umgekehrt ist es bei der Kapitalausstattung: Während die Deutsche Bank bei voller Anwendung von Basel III auf eine Eigenkapitalquote von 9,7 Prozent kommt, schafft die Commerzbank erst 8,6 Prozent. Mit Blick auf die Leverage Ratio sind die US-Banken deutlich besser ausgestattet

als ihre europäischen Wettbewerber. Das hängt mit den deutlich höheren Kreditrisiken in den USA zusammen.

Die Deutschen sind im Vergleich zu den Amerikanern deutlich weniger verschuldet. Entsprechend geringer ist hierzulande das Kreditausfallrisiko. Die Aussage von Fitschen, wonach die Leverage Ratio keinen Einfluss auf die Stabilität der Finanzmärkte hat, ist gleichwohl heftig umstritten. Viele Experten verweisen darauf, dass die Finanzierung mit zuviel Fremdkapital Grund für die Finanzkrise war. Sie halten diese Risikokennziffer für besonders aussagekräftig, weil sie nicht zwischen Anlageformen wie Unternehmenskredite und Staatsanleihekäufen unterscheidet.

UBS lässt ihr Devisengeschäft intern prüfen

Die Schweizer Großbank UBS stellt die Praxis ihrer Devisengeschäfte auf den Prüfstand. Es sei eine interne Untersuchung eingeleitet worden, teilte die Schweizer Großbank bei Vorlage der Drittquartalszahlen mit. Damit erhöht sich die Sorge, dass dem Geldhaus weitere Rechtsstreitigkeiten in Haus stehen könnten. Die UBS verweist darauf, dass die Bank wie andere Wettbewerber auch in der Sache Anfrage von Behörden bekommen habe. Man habe im Juni nach zahlreichen Medienberichten über Unregelmäßigkeiten bei Fremdwährungskursen eine hauseigene Prüfung auf den Weg gebracht. Auch in den USA und Großbritannien stehen die möglichen Devisenkursmanipulationen auf dem Radar der Behörden. Die Briten hatten im Juni eine Untersuchungen wegen möglicher Manipulationen auf dem Devisenmarkt eingeleitet. Unter anderem hatte die Financial Times berichtet, dass Banken Informationen über geplante große Devisengeschäfte genutzt haben sollen, die sie im Auftrag ihrer Kunden abwickelten, um dabei für sich selbst Vorteile zu erzielen.

US-Prozesse belasten Deutsche Bank

Angesichts massiver neuer Rückstellungen für Prozessrisiken ist der Gewinn der Deutschen Bank im dritten Quartal unerwartet deutlich eingebrochen. Auch das Investmentbanking lief schwach. Der Überschuss sank um 95 % auf gerade einmal 41 Mrd. €. Damit verfehlte die Bank die Erwartungen der Analysten klar - sie hatten im Schnitt mit 376 Millionen Euro gerechnet. Im vorbörslichen Handel bricht die Aktie um 4 % ein. Die Rückstellungen für Rechtsrisiken stiegen auf 4,1 Mrd. €, einschließlich zusätzlicher Kosten von 1,2 Mrd. € im dritten Quartal. Analysten hatten nur mit rund 500 Mrd. € zusätzlichen Kosten gerechnet. Vor allem in den USA kommen auf die Deutsche Bank hohe Prozesskosten zu. Die Frankfurter gehören unter den ausländischen Banken zu den großen Playern auf dem Hypothekenmarkt. Die nicht abreißende Klageflut aus den Anfangsjahren der Finanzkrise macht der Bank massiv zu schaffen. Zwar haben die beiden Vorstände Anshu Jain und Jürgen Fitschen gleich zu Beginn ihrer Amtszeit einen Kulturwandel ausgerufen. Aber es sind die Sünden der Vergangenheit, die die Bank noch jagen. In den Rückstellungen sind neben den Streitigkeiten in den USA auch Kosten für drohende Strafzahlungen im Zinsskandal und andere Prozesse enthalten. Die hohen Kosten für Rechtsstreitigkeiten belasteten insbesondere die Investmentbank stark, da hier auch die meisten Klagen anhängig sind. Die Erträge in der Investmentbank fielen im dritten Quartal um ein Viertel. Das Anleihegeschäft war unter Druck geraten, nachdem die US-Notenbank im Frühsommer begonnen hatte, Anleger

Compliance. Auf einen Blick.

Embargo-Filter

Die Vorgaben der sich ständig ändernden internationalen Sanktionslisten tagesaktuell einzuhalten bedeutet für Finanzinstitute eine stetige Herausforderung. SWIFT Sanctions Screening ist für kleinere und mittelgroße Banken die schnelle, kosteneffektive Lösung zur Realtime-Prüfung ihrer Transaktionen. Nähere Informationen erhalten Sie unter +49 69 7541 2240 oder Hubertus.KRAEHE@swift.com.

www.swift.com

Common Challenges.
Unique Solutions.

auf einen Ausstieg aus der lockeren Geldpolitik vorzubereiten. Das sorgte für Nervosität und Turbulenzen an den Finanzmärkten, einzelne Banken wurden offenbar auf dem falschen Fuß erwischt. Mit schwachen Zahlen steht die Deutsche Bank nicht alleine da. So machten etwa der Credit Suisse und Barclays ebenfalls das schwache Anleihengeschäft zu schaffen. In den USA litten Banken wie J. P. Morgan Chase und die Citigroup darüber hinaus unter der trägen Wirtschaft und einer sinkenden Hypothekennachfrage. Anderen Banken – wie der UBS – setzt die schwache Entwicklung im Investmentbanking ebenfalls zu. Allerdings haben die Schweizer ihren Schwerpunkt auf das Geschäft mit den vermögenden Kunden gelegt, was sich als weiches Kissen im dritten Quartal erwiesen hat. Ähnlich lief es hier bei der Deutschen Bank: Sie erhöhte den Vorsteuergewinn in der Vermögensverwaltung um 150 %. Zu dem starken Anstieg verhalfen auch sehr hohe Kosteneinsparungen. Als recht stabiler Gewinnbringer erweist sich für die Frankfurter Bank einmal mehr das Privatkundengeschäft, allerdings war die Entwicklung nicht so stark wie von von Analysten erwartet. Der Vorsteuergewinn fiel wegen der gesunkenen Erträge um 15 %. Hier hat sich die Strategie der Bank ausgezahlt, das Geschäft durch die Postbank-Übernahme auszuweiten. Das Privatkundengeschäft galt lange als langweilig. Auch die starke Konkurrenz und die damit einhergehenden dünnen Margen sprachen nicht für dieses Segment. Gleichwohl hat es sich als stabile Säule in schwierigen Zeiten erwiesen.

Wirtschaft stark von Banken abhängig

Die Wirtschaft der Eurozone ist nach Einschätzung der Europäischen Zentralbank (EZB) zu sehr von der Finanzierung durch Banken abhängig. EZB-Direktor Benoit Coeure sagte in Peking, eine Lehre aus der aktuellen Krise sei auch, dass in Europa neue Wege für eine bankunabhängige Finanzierung gefunden werden müssten. „Der Anleihe- und Aktienkapitalmarkt in Europa muss entwickelt werden“, sagte Coeure laut vorab verbreitetem Redetext. Der EZB-Direktor bemängelte, dass 75 % der externen Unternehmensfinanzierung im Euroraum von den Banken komme, was die Wirtschaft besonders anfällig für Krisen mache, die sich über das Bankensystem ausbreiteten. Die EZB wird im kommenden Jahr die Bankenaufsicht im Euroraum übernehmen und im Vorfeld die Bilanzen der Institute überprüfen und einem Stresstest unterziehen. Sie hat eine rigide Prüfung jener 128 Institute angekündigt, die sie demnächst direkt überwachen wird. Die europäischen Geldhäuser sind weitaus weniger robust als die in den USA, weil sie noch viele notleidende Kredite in den Büchern haben und unter dem schwächeren Wirtschaftswachstum leiden. Zudem gibt es in Europa vergleichsweise viele Institute. Die europäischen Banken sind der wichtigste Adressat der EZB-Krisenpolitik. Die EZB begründet das für gewöhnlich mit der herausgehobenen Rolle, die die Institute für die Realwirtschaft spielen. Forderungen nach einer Begrenzung ihrer Rolle sind von der EZB normalerweise nicht zu hören. Coeure sagte in Peking: „Wenn wir diese Krise hinter uns lassen wollen, dann müssen wir uns auch fragen: Was finanziert dieser Sektor wirklich?“

Panne beim Facebook-IPO für Nasdaq günstiger

Börsenbetreiber Nasdaq OMX muss deutlich weniger Geld als befürchtet als Entschädigung an Kunden zahlen, die beim Börsengang von Facebook Geld verloren hatten. Der Börsenbetreiber rechnet momentan mit einer Summe von 41,6 Mio. US-$, ein Betrag, den die Organisati-

on für die Selbstregulierung der Finanzbranche (FINRA) ermittelt habe. Die Zahlung liegt damit deutlich unter dem Betrag, den die Börse als Entschädigung erwartet hatte. Insgesamt hatte die Nasdaq 62 Mio. US-$ für fällige Entschädigungen auf die hohe Kante gelegt. Aufgrund technischer Probleme hatten Investmentfirmen und ihre Kunden beim Facebook-Börsengang im Mai 2012 viele Millionen US-$ verloren. Investoren wussten beim Handelsstart der Aktie des sozialen Netzwerks teilweise über Stunden nicht, ob ihre Aufträge erfüllt worden waren. Einige Aufträge wurden gar nicht ausgeführt. Die Fehler der Technologiebörse kosteten die Wall Street Schätzungen zufolge gut 500 Mio. US-$. Die Nasdaq will nun einen Bericht bei der US-Börsenaufsicht SEC einreichen, in dem die Berechnung der FINRA dargestellt wird. Auszahlungen an Kunden sind dann innerhalb von 60 Tagen zu erwarten, nachdem der Bericht von der SEC abgesegnet wurde.

BoE-Geld nicht nur für Banken?

Mark Carney, Chef der Bank of England (BoE), will in zukünftigen Finanzkrisen die Liquiditätsversorgung anpassen. In seiner ersten großen Rede zur Zukunft des Finanzplatzes London kündigte der seit Juli amtierende Carney an, sein Haus prüfe derzeit, im Ernstfall auch Broker-Firmen, Clearing-Häusern und anderen Finanzunternehmen den Zugang zur Notversorgung mit Zentralbankgeld zu öffnen. Englands Notenbankchef bekannte sich trotz Bankenkrise und zahlreicher Skandale und Verfehlungen in den Chefetagen der Geldhäuser zur Londoner City als bedeutendem Finanzzentrum. „Die Aufgabe der Bank of England ist es, sicherzustellen, dass Großbritannien einen großen und wachsenden Finanzplatz besitzt, der finanzielle Stabilität begünstigt“, sagte Carney vor Bankern. Er versuchte die versammelte Branche davon zu überzeugen, dass nur eine robuste Finanzindustrie die Rolle Londons als globaler Finanzplatz gewährleisten könne. Der Währungshüter erneuerte gleichzeitig sein Versprechen, die Zinsen in diesem und im nächsten Jahr niedrig zu halten. Nach seiner Rede wollte er aber vor Journalisten den Eindruck widerlegen, dass die Notenbank ein reiner Förderer der Finanzindustrie sei. „Das System muss sowohl auf der Banken- als auch auf der Marktseite auf Widerstandsfähigkeit organisiert werden.“ Carney kündigte außerdem an, auch die Spitzenrefinanzierungsfazilität stärker öffnen zu wollen. Aktuell geht der BoE-Gouverneur nicht davon aus, dass die Banken mehr Liquidität brauchen. Wenn die Notenbank aber beginne, ihre während der Krise für 375 Mrd. GB-£ gekauften Staatsanleihen wieder auf den Markt zu bringen, rechnet Carney damit, dass die Spitzenrefinanzierungsfazilität stärker angezapft wird.

Abwicklungsfonds für Pleitebanken

Der Zeitplan ist ambitioniert, aber das Ziel erreichbar, sagt EZB-Direktor Jörg Asmussen im Hinblick auf die angepeilte Bankenaufsicht in der Eurozone unter dem Dach der EZB. „Wir wollen die gemeinsame Aufsicht im November nächsten Jahres startklar haben“, sagte der frühere deutsche Finanzstaatssekretär. Der Währungshüter schätzt, dass der Aufbau eines gemeinsamen Abwicklungsfonds für Pleitebanken zehn Jahre dauern werde. Bis dahin könnte der ESM diese Funktion erfüllen. „Das würde eine Änderung des ESM-Vertrages erfordern. Das ist aber die kleinere Hürde als eine Änderung der EU-Verträge“, so Asmussen. Der EZB-Direktor bewertet den Euro im Vergleich zu anderen Währungen

nicht als überteuert. Sowohl nominal als auch real liege der Euro im Rahmen der vergangenen zehn Jahre. Die EZB mache sich keine übermäßigen Sorgen um den Wechselkurs. Asmussen verwies im Interview mit einer italienischen Zeitung darauf, dass die EZB kein spezielles Mandat für diese Thematik habe. Der Euro hat sich zuletzt nachhaltig von der Marke von 1,38 US-$ gelöst und steht auf dem höchsten Stand seit fast zwei Jahren. Der Anstieg verteuert Exporte aus der Eurozone. In Frankreich und Italien wird deshalb beklagt, dass der Anstieg die Reformerfolge zunichtemache.

Weitere Ermittlungen bei britischer Skandalbank

Der britische Schatzkanzler George Osborne hat eine formale Untersuchung bei der strauchelnden Co-operative Bank eingeleitet. Der Schritt folgte nur Stunden, nachdem der ehemalige Chairman des britischen Kreditinstituts, Paul Flowers, im Zuge von Ermittlungen wegen Drogenhandels festgenommen wurde. In der nun angeordneten Untersuchung soll nun die Zeit von 2008 bis heute beleuchtet werden. Dabei soll ermittelt werden, wie die Co-op Bank über die Jahre in die Krise gerutscht war, wie sie dabei geführt wurde und wie die Personalentscheidungen getroffen wurden. Zudem soll die Rolle der Regulierer in diesem Fall unter die Lupe genommen werden. Gleichzeitig erklärten die Finanzregulierer Prudential Regulation Authority und die Financial Conduct Authority, eigene Ermittlungen zu erwägen.

Die Bank wird gerade mit 1,56 Milliarden britischen Pfund (rund 1,86 Milliarden Euro) gerettet. Im Zuge dieser Rettung muss sie einen Großteil des Aktienkapitals ihres derzeitigen Eigentümers Co-operative Group an eine Gruppe von US-Hedgefonds aushändigen. Die früher als „ethisch korrekt" geltende und von Politikern insbesondere der Labour Party gerne als Musterbeispiel angeführte Co-op Bank hatte faule Immobilienkredite angehäuft und sich zudem mit einer missglückten Expansionsstrategie verhoben. Seit Flowers Abgang im Juni haben sich die Verluste der Bank ausgeweitet und bedrohen nun den Mutterkonzern Co-operative Group Ltd., der eine Reihe verschiedener Geschäfte betreibt - von Supermärkten bis hin zu Bestattungsunternehmen. Die Co-operative Group und die Co-op Bank kündigten an, jede Untersuchung zu unterstützen. Flowers, ehemaliger Chairman des Kreditinstituts, war verhaftet, sein Haus durchsucht worden. Zuvor war ein Bericht der Mail on Sunday erschienen, der besagte, Flowers hätte in der nordenglischen Stadt Leeds Kokain und Crystal Meth gekauft. Die Zeitung untermauerte ihre Behauptungen mit Fotos und einem Video. In dem belastenden Material ist zu sehen, wie Flowers offensichtlich mit jemandem bespricht, welche Drogen er kaufen möchte und dann 300 britische Pfund in Geldscheinen zwischen den Fingern zählt. Darüber hinaus veröffentlichte die Zeitung SMS-Nachrichten, in denen Flowers mit einem Bekannten über den mutmaßlichen Drogenkauf und die Einnahme der Drogen spricht. Flowers war bereits im Juni von seinem Posten zurückgetreten und hatte erst Anfang November vor dem Parlamentsausschuss über die Situation der Bank aussagen müssen. Im Zuge der Affäre um Flowers war bereits der Chefaufseher des Mutterkonzerns, Lex Wardle, zurückgetreten.

EU will SWIFT-Abkommen aussetzen

Als Konsequenz aus Medienberichten über Spähprogramme des US-Geheimdienstes NSA hat das Europaparlament die Aussetzung des SWIFT Ab-

kommens zur Übermittlung von Bankkundendaten an die USA gefordert. Das Abkommen solle so lange auf Eis gelegt werden, bis vollständig geklärt sei, ob sich US-Dienste unter Verletzung der Vereinbarung einen nicht genehmigten Zugang zu Finanzdaten verschafft haben, verlangte das Parlament in einer Entschließung. Nach Informationen des brasilianischen Fernsehsenders TV Globo vom September zapft die NSA das SWIFT-Kommunikationsnetzwerk an, in dem die Bankdaten von Millionen von Bürgern und Unternehmen in der EU gespeichert sind. Diese Angaben seien von den USA bisher nicht widerlegt worden, stellte das Europaparlament fest. Zugleich verlangte die EU-Volksvertretung, dass ihr „unverzüglich alle maßgeblichen Informationen und Unterlagen" zur Prüfung des Sachverhalts übermittelt werden. Im September hatte das Parlament seinen Ausschuss für bürgerliche Freiheiten damit beauftragt, den Vorwürfen nachzugehen. Das nach langen und zähen Verhandlungen zwischen Brüssel und Washington zustandegekommene Abkommen, das nach dem Finanzdienstleister SWIFT mit Sitz in Belgien benannt ist, soll einen Beitrag zur Bekämpfung des internationalen Terrorismus leisten. Es wurde zunächst für fünf Jahre geschlossen. Betroffen sind Geldtransfers, die europäische Bürger und Unternehmen mit Drittstaaten außerhalb der EU tätigen. Im Februar 2010 hatte das Europaparlament ein geplantes erstes SWIFT-Interimsabkommen wegen datenschutzrechtlicher Bedenken gekippt. Daraufhin billigten die US Behörden einige Nachbesserungen. So wurde die europäische Polizeibehörde Europol beauftragt, Anfragen aus den USA auf ihre Stichhaltigkeit hin zu überprüfen. Außerdem wurden zwei EU-Beamte nach Washington entsandt, um über die Verwendung der Daten zu wachen. Aufgrund dieser Nachbesserungen stimmte die EU-Volksvertretung dem Abkommen schließlich im Juni 2010 zu - gegen die Stimmen der Grünen und einiger Vertreter der Linken.

Schweizer rebellieren gegen FATCA

Die Schweizer Bürgerorganisation „Le Lobby des Citoyens" (LLDC) will mit allen Mitteln das FATCA-Abkommen zwischen der Schweiz und den USA verhindern. Angestrebt wird ein Referendum gegen den Bundesbeschluss vom 27. September 2013 über die Genehmigung des FATCA-Abkommens zwischen der Schweiz und den Vereinigten Staaten. Die Referendumsfrist läuft noch bis 14. Januar 2014. Die LLDC-Aktivisten kritisieren, dass FATCA unter enormem politischem und ökonomischem Druck entstanden sei, dem die Schweiz nachgegeben habe, ohne zu kämpfen. Mit FATCA verfolge der amerikanische Fiskus nicht nur seine Staatsbürger und US-Firmen in der ganzen Welt, sondern auch Doppelbürger und Schweizer Ehepartner von US-Staatsangehörigen. Bereits ein Studium in den USA reiche aus, um aus ihnen einen US-Steuerpflichtigen zu machen, heißt es in der Referendumsbegründung. Die Übermittelung von Bankdaten an die US-amerikanischen Steuerbehörden bedeute die Aufhebung des Schweizer Bankkundengeheimnisses als Instrument zum Schutz der Personen. Amerikanische Unternehmen, die in der Schweiz angesiedelt seien und ausschließlich Schweizer Personal beschäftige, könnten demnach von Schweizer Gerichten nach amerikanischem Recht beurteilt werden, befürchten die Westschweizer Bürgerrechtsvertreter.

Suche nach Devisenmanipulation

Der Druck auf die Banken zur Aufarbeitung möglicher Währungsmanipulationen steigt. Großbanken wie die Deutsche Bank und die Citigroup wurden nun von der US-Finanz-

marktaufsicht CFTC aufgefordert, ihre sämtlichen Daten und Aufzeichnungen nach Hinweisen auf Manipulationen am Devisenmarkt zu durchforsten und diese der Aufsichtsbehörde auszuhändigen. Eine der informierten Personen sagte, die Deutsche Bank nehme gegenwärtig Millionen von Dollar in die Hand, um die E-Mails und Chat-Aktivitäten ihrer Devisenhändler nach bestimmten Schlagwörtern und anderen Hinweisen zu durchkämmen. Bislang hätten jedoch weder die Deutsche Bank noch die Citigroup derartiges Material an die CFTC übergeben. Die Aufsichtsbehörde selber wollte sich dazu nicht äußern. Neben der Commodity Futures Trading Commission gehen noch weitere Aufsichtsbehörden rund um den Globus dem Verdacht auf Währungsmanipulationen nach. Eine Reihe von Großbanken sind von den Untersuchungen betroffen.

Das Wall Street Journal hatte bereits berichtet, dass J.P. Morgan und die Royal Bank of Scotland mit der britischen Finanzdienstleistungsaufsicht Financial Conduct Authority (FCA) zusammenarbeiten und interne Untersuchungen durchführen. Nach Auskunft einer informierten Person soll die Royal Bank of Scotland in diesem Zusammenhang bereits entsprechendes Material an die FCA übergeben haben. Ein zentraler Bestandteil der Untersuchungen ist laut informierten Personen das sogenannte Devisen-Fixing - tägliche Momentaufnahmen des Handels, die unter anderem von Disponenten dazu genutzt werden, um ihre Bestände zu bewerten. Das am häufigsten genutzte Fixing ist das um 16.00 Uhr Londoner Zeit. Die „Fixes“ werden aus den Kursbewegungen in einem kurzen Zeitraum berechnet. Die Untersuchungen in London, einer der Drehscheiben des weltweiten Devisenhandels, konzentrieren sich teilweise auf einen elektronischen Chatroom, in dem eine Gruppe von Devisenhändlern unter verschiedenen Spitznamen wie „The Club“, „The Bandits‘ Club“, „The Dream Team und „The Cartel“ operiert haben soll. Die schweizerische Finanzaufsicht hatte ebenfalls einer Untersuchung der Banken in die Wege geleitet.

In einem Zeitungsinterview hatte Urs Rohner, Chef der Schweizer Großbank Credit Suisse, Anfang des Monats bereits erklärt, in seinem Haus bislang keine Hinweise auf mögliches Fehlverhalten von Händlern gefunden zu haben. Laut Insidern soll auch das FBI in den USA ein strafrechtliches Ermittlungsverfahren eingeleitet haben, um mögliche Manipulationen der internationalen Devisenmärkte zu untersuchen. Die Untersuchungen an den Devisenmärkten wurden durch einen Skandal um Zinsmanipulationen an der Wall Street und der City of London ausgelöst. Nach Einschätzung einer mit den internen Nachforschungen bei der Citigroup vertrauten Person werden die Untersuchungen auf die Frage hinauslaufen, ab welchem Punkt aus einem normalen Informationsaustausch unter Händlern unangemessenes Verhalten wird. Führende Banker einiger großer Geldhäuser schlossen nicht aus, dass es Devisenhändler ihren Job kosten könnte, Kurse in Absprache mit anderen Händlern zu Lasten von Kunden absichtlich nach oben getrieben zu haben.

Neue Datenschutz-Grundverordnung in der Kritik

Während sich die Fraktionen im EU-Parlament auf eine gemeinsame Linie für die neue Datenschutz-Grundverordnung geeinigt haben, fordern Wirtschaftsverbände noch etliche Nachbesserungen. Auch die deutsche Politik sieht die Bemühungen um Harmonisierung des europäischen Datenschutzrechts noch nicht am Ziel. „Es ist noch viel handwerkliche Arbeit nötig, um die Verordnung so auszugestalten, dass sie die

hohen deutschen Datenschutzstandards widerspiegelt, praxistauglich ist und zugleich auf die Herausforderungen des Internetzeitalters vernünftige Antworten gibt", sagte Bundesinnenminister Hans-Peter Friedrich. Der Bundesverband mittelständische Wirtschaft (BVMW) und die Berliner Datenschutzrunde sehen vor allem die Bedürfnisse der kleinen und mittleren Unternehmen (KMU) nicht ausreichend berücksichtigt. Die Pflicht zur Datenschutz-Folgenabschätzung verursacht erhebliche Mehrkosten. „Die vorgesehenen Dokumentationspflichten gefährden die Wettbewerbsfähigkeit des Mittelstands, da gerade kleinere Mittelständler durch die Pflicht zur Dokumentation sämtlicher betrieblicher Datenverarbeitungsprozesse erheblich belastet würden", so Mario Ohoven, Präsident des BVMW und des europäischen Mittelstandsdachverbandes CEA-PME.

Eine Überarbeitung der Regelungen sei notwendig, um den neuen Herausforderungen gerecht zu werden. Die Unternehmen dürften jedoch nicht durch unverhältnismäßige Regulierungen im Datenschutzrecht geschwächt werden. „Hier muss mit Augenmaß ein sachgerechter Ausgleich zwischen den Interessen des Verbraucherschutzes und der Wirtschaft geschaffen werden", so Ohoven. Auch der Bundesverband Digitale Wirtschaft (BVDW) kritisierte den verabschiedeten Kompromiss des Europaparlaments. Insbesondere mit den erstmals verankerten Anreizelementen für pseudonyme Datenverarbeitung werde zwar europaweit ein Modell eingeführt, das in Deutschland bereits seit langem erfolgreich eingesetzt wird. Diese Regelungen seien vor allem für kleine Diensteanbieter im Wettbewerb überlebenswichtig. Jedoch fehlte dem Parlament der Mut, diesen „privacy by design"-Ansatz im Gesetzestext in aller Deutlichkeit zu regeln. Stattdessen wurde er in so genannten Erwägungsgründen versteckt und damit Rechtsunsicherheit provoziert. Als kontraproduktiv bewertet der BVDW die Regelung zum so genannten Profiling. Der Kompromiss führe in der jetzigen Fassung dazu, dass sich das geplante Verbot auch auf Daten erstreckt, die keinen Personenbezug haben. Dies stelle weder eine angemessene, abgestufte Lösung dar, die das tatsächliche Risiko und die Sensibilität der betroffenen Daten berücksichtige, noch sei dieser Vorschlag geeignet, in der Praxis für mehr Datenschutz zu sorgen. Matthias Ehrlich, Präsident des BVDW: „Das Dossier kann auch nicht annähernd als Antwort auf die Enthüllungen flächendeckender staatlicher Internetüberwachung durch Geheimdienste gesehen werden. Ein hastig nachgetragener Artikel, der für gesetzliche Kooperationspflichten letztlich Unternehmen haftbar machen will, ist kein politischer Vorschlag, sondern klarer Ausdruck politischer Rat- und Hilflosigkeit in Sachen PRISM & Co." Darüber hinaus bekräftigt Ehrlich die Bedeutung des Zusammenspiels von Gesetzgebung und Selbstregulierung: „Als Digitalindustrie haben wir die Aufgabe, einen fundierten Regulierungsrahmen durch branchenweite Standards mit Leben zu füllen, wie dies mit dem Deutschen Datenschutzrat Online-Werbung (DDOW) und der European Interactive Digital Advertising Alliance (EDAA) bereits geschehen ist. Leider setzen die Vorschläge des Parlaments praktisch keine Anreize für die Schaffung solcher gemeinsamer Standards."

Jeder Zehnte bereits Betrugsopfer

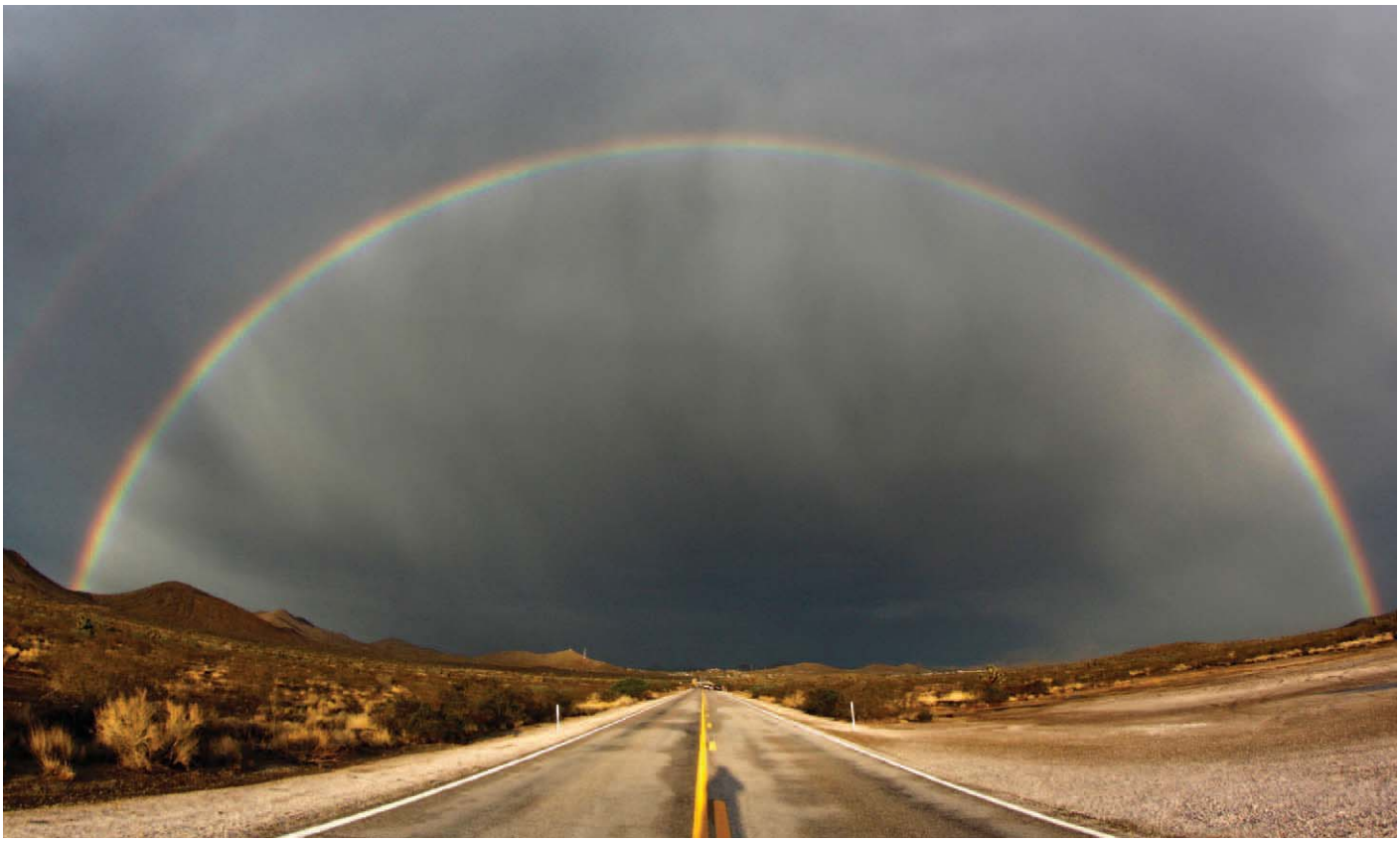
Eine aktuelle Studie zum Thema Online-Sicherheit zeigt: Weltweit hat mehr als jeder zehnte Verbraucher bereits Online-Betrug erlebt und dadurch einen finanziellen Schaden erlitten. In Deutschland bezeichneten sich 14 % der Befragten selbst als Online-Betrugsopfer oder gaben an, ihnen seien schon einmal Kreditkartendaten

gestohlen worden. Die USA und Malaysia vermelden mit jeweils 20 % die höchste Opferquote, innerhalb Europas ist Großbritannien mit 17 % Geschädigten an der Spitze. Mit den niedrigeren Raten an Leidtragenden geht einher, dass die Europäer im Vergleich zu Brasilien, USA und Malaysia wesentlich geringere Ängste und Sicherheitsbedenken in Sachen Online-Kriminalität haben. So fürchten in Deutschland 62 %, beim Online-Shopping ein Betrugsopfer zu werden, 64 % haben Befürchtungen beim Online-Banking. In den außereuropäischen Ländern liegen die entsprechenden Werte mit 87 beziehungsweise 84 % wesentlich höher. Bei der Nutzung von mobilen Geräte oder Tablets haben die meisten Anwender dabei weniger Angst als bei der Verwendung von PC-Systemen. Die Sorge um die Online-Sicherheit bei Alltagsaktivitäten wie Surfen, Einkaufen, Lesen oder Mail-Versand teilen in Deutschland 69 % der Anwender bei der Benutzung von PC oder Laptop, bei mobilen Geräten sind es lediglich 53 %, bei der Verwendung von Tablets sogar nur 39 %. Trotzdem sind PC immer noch die verbreitetsten Zugangsgeräte für den Online-Zugang. In Deutschland nutzen 90 % Windows-basierte PCs und Notebooks, 37 % Android-Smartphones. Bei anderen mobilen Geräten liegen die deutschen Anwender deutlich unter dem europäischen Durchschnitt. Nur 16 % (im Vergleich zu europaweit 24 %) gehen mit iPhones online, 14 % (Europa: 22 %) mit Android Tablets, 13 % (Europa: 20 %) nutzen ein iPad. Auch Apple-Computer sind in Deutschland weniger verbreitet und werden nur von 8 % genutzt, europaweit liegt der Anteil bei 16 %. Egal, womit gearbeitet wird: Die Mehrheit der Befragten weiß um die Wichtigkeit, die Software durch Updates auf dem aktuellen Stand zu halten. 77 % kennen die Gefahr von Sicherheitslücken durch unterlassene Updates, 86 % versicherten, ihre Software regelmäßig nachzurüsten. In seiner aktuellen Verbraucherbefragung „Digital Lifestyle Survey“ gibt F-Secure auch Tipps zur Vermeidung von Online-Betrug. Dazu gehört, für jeden Account einzelne sichere Passwörter, kombiniert aus Buchstaben, Zahlen und Sonderzeichen, zu verwenden. Persönliche oder Bank-Daten sollte man grundsätzlich nur auf vertrauenswürdigen Webseiten eingeben, die man leicht an der „https”-URL erkennt. Wer online einkauft oder Geldgeschäfte betreibt, sollte dies möglichst nicht an öffentlich zugänglichen Rechnern oder in einem öffentlichen WLAN tun. Besondere Vorsicht ist bei Phishing-Mails geboten. Bei Mails, die angeblich von der eigenen Bank etc. kommen, sollte man niemals Anhänge öffnen oder auf Links im Text klicken. Und auf dem Rechner schützen beispielsweise Virenschutzprogramme vor unerwünschten Eindringlingen.

Kriminelle nutzen SEPA-Umstellung

Kriminelle nutzen die Einführung neuer Regeln für Überweisungen und Lastschriften, um Spam zu verbreiten. Das hat das Bundesamt für Sicherheit in der Informationstechnik beobachtet. Die Betrüger tarnen ihre E-Mails als Informationsschreiben der Bank zur SEPA-Umstellung, tatsächlich schmuggelt die E-Mail aber einen Trojaner auf den Rechner des Opfers. Dagegen hilft den Angaben nach ein Virenscanner: Die meisten aktuellen Programme können solche Schädlinge erkennen und unschädlich machen. Nutzer sollten die gefährlichen E-Mails am besten direkt löschen und mitgelieferte PDF- oder ZIP-Dateien auf keinen Fall öffnen. Im Zuge der Umstellung auf die in der EU-weiten Standards der SEPA (Single Euro Payments Area) gelten für Überweisungen und Lastschriften ab dem 1. Februar 2014 bekanntlich neue Regeln. Ab diesem Zeitpunkt werden nicht mehr die gewohnten Kontonummern und Bankleitzahlen gebraucht, sondern IBAN und BIC, die internationale Bankleitzahl.

THOMSON REUTERS
ACCELUS™



MARKTFÜHRENDE LÖSUNGEN FÜR UNTERNEHMENSWEITES GOVERNANCE, RISK UND COMPLIANCE MANAGEMENT (GRC)

INTEGRIEREN. VEREINFACHEN. AUSSFÜHREN.

Proaktive Unternehmen erkennen, daβ ein ganzheitlicher Ansatz für Governance, Risk und Compliance nicht nur entscheidend für die Einhaltung gesetzlicher Vorschriften ist, sondern auch zu einer guten Geschäftspraxis gehört.

Thomson Reuters Accelus bietet marktführende Lösungen für unternehmensweites Governance, Risk und Compliance Management (GRC), Risiko-, Richtlinien- und Audit-Management, globale aufsichtsrechtliche Informationen im Zusammenhang mit Wirtschaftskriminalität, Anti-Korruption und -Bestechung, Lieferkettenrisiken, verstärkter Due Dilligence , Schulungen und e-Learning sowie Dienstleistungen für den Vorstand und der Offenlegungspflicht an.

Wir erreichen dies durch eine einzigartige Kombination von regulatorischen und risikoorientierten Inhalten, Taxonomie und konfigurierbare Workflow-Technologie, die Governance-, Risiko- und Compliance-Prozesse in einem ganzheitlichen und integrierten Ansatz in Ihrem Unternehmen verbindet.

Thomson Reuters Accelus wurde im Leaders Quadrant von Gartner, Inc. als führend im "Enterprise Governance, Risk and Compliance Platforms Magic Quadrant" prositioniert. Ebenso wurde Accelus als einer der Branchenführer im Chartis RiskTech Quadrant ™ für operationelle Risikomanagement-Systeme und unternehmensweite Governance, Risk and Compliance-Systeme ernannt.

Besuchen Sie uns auf unserer Website und erfahren Sie mehr:
http://accelus.thomsonreuters.com/de

THOMSON REUTERS™

Geldwäsche: Commerzbank soll strenger kontrollieren

Die US-Notenbank fordert von der Commerzbank strengere Vorkehrungen zur Verhinderung von Geldwäsche-Aktivitäten. Das deutsche Geldinstitut und seine US-Tochter seien nun aufgefordert worden, sich einer unabhängigen Überprüfung zu unterziehen, teilte die Federal Reserve (Fed) in Washington mit. Im Rahmen dieser Kontrolle soll geklärt werden, ob sich die Bank zwischen Mai und Oktober 2012 an die US-Vorschriften zur Meldung „verdächtiger Aktivitäten" gehalten habe. Im Juni 2012 hatten sich die Commerzbank und ihre New Yorker Filiale gegenüber der Fed verpflichtet, die internen Kontrollen zu verbessern. Die Bank habe es aber versäumt, angemessene Kontrollmechanismen beizubehalten, kritisierte die US-Notenbank nun. Die Fed verhängte kein Bußgeld, forderte die Commerzbank aber auf, innerhalb von 30 Tagen einen unabhängigen Berater zu engagieren. Die Ergebnisse der Untersuchung sollen genutzt werden, um die Maßnahmen des Geldinstituts in diesem Bereich zu verbessern. In den USA wurde gegen die Commerzbank bereits im Zusammenhang mit früheren Transaktionen in Länder wie dem Iran oder Nordkorea wegen möglicher Verstöße gegen US-Sanktionen ermittelt.

US-Behörde verklagt Barclays

Der Streit der britischen Bank Barclays mit der US-Energiemarktaufsicht FERC geht in die nächste Runde. Nachdem die Bank sich geweigert hat, eine Strafe von 435 Mio. US-$ wegen Manipulationen auf dem kalifornischen Strommarkt zu bezahlen, hat die Behörde nun Klage eingereicht. Die FERC hatte die Rekordstrafe im Juli verhängt. Barclays hatte sogleich angekündigt, sich dagegen zur Wehr zu setzen. Die Behörde wirft der Bank vor, Händler des Geldhauses hätten die Preisbildung auf dem kalifornischen Strommarkt in den Jahren 2006 bis 2008 manipuliert. Vier Händler hätten am Derivatemarkt gleichzeitig gegen einen steigenden Energiepreis gewettet. Barclays war für einen Kommentar nicht zu erreichen. Die Behörde war auch schon gegen weitere Banken vorgegangen. Eine Tochter der Deutschen Bank wurde in diesem Jahr ebenfalls mit einer Strafe versehen, sie kam mit 1,7 Mio. US-$ aber vergleichsweise glimpflich davon. Deutlich härter traf es da J.P. Morgan. Das New Yorker Institut musste 410 Mio. US-$ berappen.

Manipulationsvorwürfe gegen Großbanken

Den Großbanken könnten nach dem Libor-Skandal neue Manipulationsvorwürfe ins Haus stehen. Aufsichtsbehörden prüfen derzeit, ob die Institute an den Devisenmärkten Kurse absichtlich nach oben oder unten getrieben haben. Die Geldhäuser durchforsteten daraufhin zahlreiche E-Mails und andere elektronische Kommunikation ihrer Mitarbeiter, wie mit der Sache vertraute Personen. Die Royal Bank of Scotland (RBS) händigte bereits die elektronische Korrespondenz eines früheren Angestellten an die britische Finanzmarktaufsicht FCA aus, wie eine der Personen sagte. Der Mitarbeiter habe die Bank aber nicht wegen der Ermittlungen, sondern aus anderen Gründen verlassen. Die US-Bank J.P. Morgan ist laut einem Insider in Gesprächen mit der FCA und anderen Aufsehern. Und im Rahmen der FCA Ermittlung, die im Juni begann, untersuchen auch andere Großbanken ihre Handelsak-

tivitäten und durchleuchten ihre interne und externe Kommunikation. Zu den Geldhäusern zählen laut anderen informierten Personen die Deutsche Bank, Citigroup und Barclays. An den Maßnahmen wird deutlich, dass die Überprüfung der Devisenmärkte in der Schweiz, Großbritannien und Brüssel Fahrt aufnimmt. Der potenzielle Skandal rief vorläufig schon die Politik auf den Plan. Die Schweizer Finanzministerin Eveline Widmer-Schlumpf sorgte jüngst für Stirnrunzeln, als sie vor Reporten erklärte, eine Manipulation von Devisenkursen habe stattgefunden. Später ruderte das Finanzministerium zurück. Die Ministerin habe lediglich sagen wollen, dass die Schweizer Marktaufsicht den Fall prüfe, stellte ein Sprecher klar. Die wichtigste Schweizer Aufsichtsbehörde Finma hatte ihre Ermittlungen wegen des Verdachts auf Manipulation von Devisenkursen am Freitag bekannt gegeben. Außer der Schweizer Aufsicht hat sich auch noch die EU Wettbewerbsbehörde den Fall vorgeknöpft. Die Untersuchung sei aber in einem sehr frühen Stadium, erklärte Sprecher Antoine Colombani. Zum Großteil dreht sich die Untersuchung um das sogenannte „Devisen-Fixing“, bei dem zu bestimmten Zeiten im täglichen Handelsverlauf die aktuellen Devisenkurse festgestellt werden. Einige Anleger meiden bereits Käufe und Verkäufe um die Fixing-Zeitpunkte herum. Sie fürchten, dann für Währungstransaktionen nachteilige Preise zu erhalten. Überhaupt ist ihnen der gesamte Prozess zu undurchsichtig. Da Währungen rund um den Globus 24 Stunden lang gehandelt werden, gibt es keinen Zeitpunkt, zu dem der Markt schließt und sich eine tägliche Benchmark bestimmen ließe. Stattdessen geben die Unternehmen, die die Daten liefern, regelmäßig Wasserstände an. Am beliebtesten ist der Kurs, der um 16 Uhr Londoner Zeit vom Gemeinschaftsunternehmen WM/Reuters ermittelt wird. Dieses Fixing dient als Referenzwert und viele Anleger weisen ihre Banken an, genau zu diesem Kurs die Transaktionen abzuschließen. Allerdings betrachten mehrere Marktteilnehmer diesen Referenzkurs argwöhnisch. Sie beschweren sich über unerklärliche Kursausschläge und schwankende Liquidität. Eine Sprecherin des Datenservices WM verwies auf die Unternehmenswebseite, wo die Methodologie des Computerfixing erklärt würde. Sein Unternehmen liefere lediglich die Daten, mit denen WM den Benchmark berechne, sagte ein Thomson-Reuters-Sprecher. Die Experten von WM/Reuters errechnen das Fixing, indem sie kurz vor 16 Uhr Handelsdaten aus mehreren Ausführungsorten über einen Zeitraum von 60 Sekunden betrachten. Die wichtigsten Währungspaare – wie Euro-Dollar oder Pfund-Dollar – werden kräftig gehandelt. Das dürfte Kursmanipulationen eigentlich erheblich erschweren. Für weniger stark gehandelte Währungen nutzt das Joint Venture Verkaufs- und Kaufgebote und setzt dabei nach Angaben von WM „weitere Qualitätschecks“ ein. Das Devisenfixing ist besonders beliebt bei Indexfonds, die den breiteren Markt abbilden. Indem sie ihre Währungsgeschäfte zum Fix-Preis abschließen, schützen sie sich vor Kursfluktuationen, durch die sich ihre Transaktionen vom Index unterscheiden könnten. Aber einige Investoren und Anlageberater halten die undurchsichtige Art und Weise der Berechnungen für eine Gefahr. Es sei unmöglich zu ermitteln, welche großen Handelsaufträge das Fixing letztlich nach oben oder unten drückten. „Unsere Kunden, etwa lokale Pensionsfonds, wollen bei uns explizit zum Fixing handeln. Auch weil ihre Investmentberater ihnen das empfehlen. Aber wir haben ernsthafte Bedenken“, warnte der Handelschef einer Vermögensverwaltung, der nicht genannt werden wollte. „Dieses Verfahren garantiert nicht immer den transparentesten Kurs.“ Auch James Cochrane, Direktor von ITG Analytics, empfiehlt seinen Kunden keinen Handel zu den Fix-Kursen. „Zunächst einmal sind die Preise nicht besonders gut. Außerdem überwacht nie-

mand das Fixing. Es gibt keinen Aufseher. Es ist eine unregulierte Benchmark."

Cybercrime verursacht Riesenschäden

Die Risiken durch Cyberkriminalität werden von den meisten deutschen Mittelständlern grob unterschätzt. Nur knapp 6 % der Leiter mittelständischer Betriebe sehen ihr Unternehmen als mögliches Ziel von Hacker-Angriffen und ähnlichen Risiken, weltweit sind es sogar nur 4 % der Unternehmer, stellte die Zurich Versicherung nun im Rahmen einer einer repräsentativen Umfrage unter Geschäftsführern und Vorstandsmitgliedern mittelständischer Betriebe fest. Damit hinke das Risikoempfinden dem faktischen Risiko weit hinterher, denn laut polizeilicher Kriminalstatistik habe die Cyber-Kriminalität mit 64.000 Fällen im Jahr 2012 einen neuen Höchststand erreicht, sagte Ralph Brand, Vorstandsvorsitzender von Zurich in Deutschland. Die Zahl der Fälle sei im Vergleich zu 2011 um 7,5 % gestiegen, gegenüber 2007 stellen die Zahlen sogar eine Zunahme um 87 % dar. Die Risiken der digitalen Arbeitswelt würden für viele Unternehmer bislang kaum eine Rolle spielen, kritisierte Brand. Er rät, die Unternehmen sollten ihre internen IT-Risikolücken identifizieren und schließen, um Angriffe aus dem Netz bestmöglich abzuwehren. Eine Absicherung für den Ernstfall könne zudem finanzielle Schäden auffangen. Einer Studie von HP zufolge kostet Cyberkriminalität deutsche Unternehmen im Schnitt 5,7 Mio. € im Jahr, das ist ein Anstieg von 16 % gegenüber 2012, wie aus der jährlichen Erhebung „Cost of Cyber Crime" hervorgeht. Damit liegt Deutschland im weltweiten Vergleich auf Platz zwei hinter den USA. In Deutschland hatte das Ponemon Institut für diese Untersuchung 398 Fach- und Führungskräfte aus 47 deutschen Organisationen ausführlich befragt und in seine Studie auch die Analyseergebnisse aus tatsächlichen Cyberangriffen einfließen lassen. Dabei stellte sich heraus, dass die Beseitigung der Folgen eines Cyber-Crime-Angriffs im Mittel 22 Tage dauern und 352.500 € kosten. Jedes der untersuchten deutschen Unternehmen verzeichnete im vergangenen Jahr 1,3 erfolgreiche Angriffe pro Woche, das sind 21 % mehr als im Vorjahr. Die höchsten Kosten verursachen in Deutschland Cyberangriffe von Insidern, Denial-of-Service- sowie Phishing-Attacken. Zusammen verursachen diese drei Angriffstypen 50 % aller Kosten, die pro Unternehmen und Jahr durch Cyberkriminalität entstehen. Schadcodes und Botnetze spielen hingegen eine nachgeordnete Rolle: Im internationalen Vergleich werden deutsche Unternehmen am wenigsten durch diese Angriffsmethoden attackiert. Die teuerste Folge von Cyberkriminalität bleibt weiterhin Datenverlust, dicht gefolgt von Umsatzeinbußen durch Betriebsstörungen. Auf ein Jahr gesehen macht der Schaden durch Datenverlust einen Anteil von 43 % der gesamten externen Kosten aus. Umsatzeinbußen durch Betriebsstörungen und reduzierte Produktivität legten um 2 % auf 27 % der externen Kosten zu. Die teuersten Gegenmaßnahmen sind die Entdeckung und Beseitigung von Angriffen, resultierend vor allem in Produktivitätsverlust und Arbeitskosten. Der übrige Aufwand verteilte sich auf das Isolieren schadhafter Systembestandteile oder Software, auf Nachforschungen, Incident Management sowie nachgelagerte Maßnahmen. Die Studienergebnisse zeigen einen Zusammenhang zwischen Unternehmensgröße und den Kosten durch Cyberangriffe: Kleinere Unternehmen verzeichnen deutlich höhere Kosten pro Kopf (durchschnittlich 974 €) als größere Unternehmen (durchschnittlich 251 €). Grundsätzlich sind jedoch Unternehmen aller Branchen von Cyberkriminalität betroffen, wenn auch in unterschiedlichem Umfang. Unternehmen aus den Bereichen Energie und Versorgung, Finanzdienstleistungen und Technologie verbuchen jährlich deutlich höhere Cybercrime-Kosten als solche

aus den Bereichen Handel, Medien und Konsumgüter. Trotz der steigenden Bedrohungslage durch Cyberattacken zeigt die Studie, dass moderne Security-Intelligence-Werkzeuge dabei helfen können, die Bedrohungen und die dadurch verursachten Kosten deutlich zu reduzieren. Genannt wurden hier vor allem Lösungen für das Sicherheitsinformations- und Event-Management (SIEM), Intrusion-Prevention-Systeme, Sicherheitstests für Applikationen sowie Lösungen für Governance, Risikomanagement und Compliance in Unternehmen. Unternehmen und Behörden, die solche Sicherheitstechniken anwenden, konnten Cyberattacken effizienter erkennen und eindämmen und haben – laut Studie – damit im Durchschnitt 1,4 Mio. € im Jahr eingespart. Die Studie untersuchte außerdem den ROI von sieben unterschiedlichen Security-Technologien. Das Resultat: Unternehmen erzielten im Schnitt eine Investitionsrendite von 25 % durch den umfassenden Einsatz von Verschlüsselungstechnologien. Auf den weiteren Plätzen folgen Security-Intelligence-Systeme (20 %) sowie fortschrittliche Perimeter-Kontrollen und Firewall-Technologien.

Höhere Strafen für Korruption gefordert

Deutschland wird neben Großbritannien, der Schweiz und den USA im neuesten „Exporting Corruption"-Bericht der Antikorruptionsorganisation Transparency International eine „aktive Verfolgung der Auslandsbestechung" bescheinigt. Die Vereinigung berichtet in dem Papier über den Stand der Strafverfolgung der Auslandsbestechung von Amtsträgern im Geschäftsverkehr in OECD-Ländern. Dies sei zwar gut, aber noch nicht genug, um Unternehmen effektiv von Korruption abzuhalten, urteilt Transparency International. Die Organisation beruft sich auf Untersuchungen, die zeigten, dass die Bereitschaft deutscher Unternehmen, im Ausland zu bestechen, in den letzten Jahren nicht zurückgegangen sei. Auf dem „Bestechungszahlungsindex", der dies aufliste, verharre Deutschland seit 2008 bei 8,6 von 10 möglichen Punkten. Neben einer aktiven Strafverfolgung sei die Frage des Strafmaßes entscheidend dafür, ob sich Unternehmen auf korrumpierende Geschäfte einlassen. Deutschland hat zwar die mögliche Geldbuße, die gegen Unternehmen verhängt werden kann, von einer auf zehn Millionen Euro angehoben, doch bliebe das Strafmaß weiterhin zu gering, so Transparency. NRW-Justizminister Thomas Kutschaty hat angekündigt, Eckpunkte für die Einführung eines Unternehmensstrafrechts in der nächsten Justizministerkonferenz Mitte November vorzustellen. Edda Müller, Vorsitzende von Transparency Deutschland, erwartet diese Vorschläge mit Spannung: „Die OECD fordert dies seit langem. In einer globalisierten Wirtschaftswelt können wir uns nicht erlauben, internationale Empfehlungen zu unterminieren." Ein weiterer Faktor zur Prävention gegen Korruption sei die Frage nach der Wahrscheinlichkeit der Entdeckung. Dazu empfiehlt der Bericht „Exporting Corruption", den Schutz für Hinweisgeber in Deutschland zu stärken. International gebe es diesbezüglich Druck: OECD, G20 und Europarat forderten Deutschland auf, den Hinweisgeberschutz in der Privatwirtschaft zu verbessern. Die OECD hatte Deutschland Anfang 2011 eine Zweijahresfrist eingeräumt, die entsprechenden Empfehlungen umzusetzen. Jetzt, so Transparency abschließend, sei Deutschland erneut aufgefordert, bis März 2014 über Fortschritte zu berichten.

10.000 Selbstanzeigen in NRW

Bei der Finanzverwaltung Nordrhein-Westfalen sind im September 2013 insgesamt 601 Selbstanzeigen von Bürgerinnen und Bürgern mit Bezug

zur Schweiz eingegangen. Dies ist der höchste Zuwachs innerhalb eines Monats seit Mai 2010. Damit steigt die Zahl der Eingaben von Schwarzgeldbesitzern bei der Finanzverwaltung NRW auf 10.545 seit Februar 2010. „Die Zahlen zeigen, dass es richtig ist, den Druck auf Steuerhinterzieher aufrecht zu erhalten“, sagte Finanzminister Norbert Walter-Borjans. „Wir werden weiterhin alle Möglichkeiten nutzen, um Schwarzgeldbesitz aufzudecken. Aber wir wollen auch genauso konsequent gegen Steuerschlupflöcher im In- und Ausland vorgehen“, so der Minister. „Dazu brauchen wir einen internationalen Informationsaustausch, der seinen Namen wirklich verdient.“

CRIM-Komitee analysiert EU-Kriminalität

Insgesamt treiben rund 3.600 kriminelle Organisationen in der Europäischen Union ihr Unwesen und verursachen jährliche Schäden in Höhe von 290 Mrd. €. Das geht nach Informationen des „Spiegel“ aus einem Bericht des CRIM-Komitees hervor. Der Sonderausschuss des Europäischen Parlaments für organisierte Kriminalität, Korruption und Geldwäsche (CRIM) wurde im März 2012 eingerichtet und dient dazu, kriminelle Aktivitäten zu untersuchen und zu analysieren sowie einen umfassenden und strukturierten Plan zu deren Bekämpfung auf europäischer Ebene zu entwerfen. Ein Kernproblem ist offenbar die grassierende Korruption. Allein in öffentlichen Einrichtungen zählt der Bericht rund 20 Millionen Fälle mit einem Gesamtschaden von 120 Mrd. €. Das CRIM-Komitee fordert u.a. die Bekämpfung europäischer Steueroasen, höhere Strafen bei Geldwäsche oder Korruption sowie einen europaweiten gesetzlichen Schutz von Whistleblowern.

Konsequenzen aus der Abhöraffäre gefordert

Hightech-Spezialisten fordern Konsequenzen aus den Abhör- und Ausspähaktionen ausländischer Geheimdienste. „Die informationelle Selbstbestimmung deutscher Verbraucher wird derzeit ebenso verletzt wie die Integrität wettbewerbsrelevanter Informationen in Unternehmen und vertraulicher Kommunikation in der Politik“, sagte BITKOM-Präsident Prof. Dieter Kempf. „Das Vertrauen von Internetnutzern und Unternehmen in die Sicherheit und den Schutz ihrer Daten ist beschädigt. Es ist zu befürchten, dass sich dies nachteilig auf die Nutzung neuer Technologien auswirkt und Schaden für Wirtschaft und Gesellschaft entsteht.“ Es sei höchste Zeit, in aller Konsequenz Maßnahmen einzuleiten. Dabei dürfe man sich nicht allein von den aktuellen Berichten leiten lassen, sondern müsse ebenso mögliche Aktivitäten derzeit nicht genannter Geheimdienste, die Organisierte Kriminalität sowie Angriffe extremistischer Organisationen im Auge behalten. Der Verband fordert von der Politik unter anderem eine Befreiung der Unternehmen von der derzeit weitgehenden Verschwiegenheitspflicht über Abhörmaßnahmen, Verhandlungen über ein No-Spy-Abkommen, eine internationale Übereinkunft für Zugriffe der Behörden auf Daten und einen zumindest europaweiten Schutz für Privatverbraucher vor Ausspähung durch befreundete Geheimdienste. Letzteres könne dadurch erreicht werden, dass alle EU-Bürger in den EU-Mitgliedstaaten unter Aspekten der informationellen Selbstbestimmung als Inländer gelten. Damit würden sehr viel strengere Regeln für ihre Überwachung gelten. Kempf: „In einem vereinten Europa ist das gegenseitige Ausspähen der jeweiligen nationalen Staatsbürger ein absoluter Anachronismus. Ein kollusives Zusammenwirken der nationalen Behörden untereinander und damit eine faktische Aushebelung des verfassungsrechtlich garantierten Fernmeldegeheimnisses und des Rechts auf informationelle Selbstbestimmung darf es nicht geben.“ Kempf betonte anlässlich der Vorstellung eines Positionspapiers in Berlin, dass die Unternehmen der Netzwirtschaft zur Kooperation mit Sicherheitsbehörden gesetzlich verpflichtet seien. Weder für Anlass noch für Umfang oder Ausgestaltung von Abhörmaßnahmen seien die Unternehmen verantwortlich. Welche Daten unter welchen Bedingungen wo und wie erhoben, gesammelt, verarbeitet und gespeichert würden, entschieden allein die hierfür zuständigen staatlichen Stellen und der Gesetzgeber. Kempf: „Die Unternehmen der Netzwirtschaft haben keinerlei Interesse daran, sich an der Ausspähung ihrer Kunden oder anderer Internetnutzer zu beteiligen. Sie haben das alleinige Interesse, ihren Kunden sichere und hoch vertrauenswürdige Dienste anbieten zu können. Dabei sind sie bestrebt, den Schutz von Daten und Kommunikation und die Unversehrtheit der Privatsphäre jederzeit sicherzustellen und Angriffe und Zugriffe von außen zu verhindern. In die Sicherheit der Daten ihrer Kunden investieren die Unternehmen der Netzwirtschaft jährlich weltweit einen zweistelligen Milliardenbetrag.“ Die Vorschläge im Einzelnen:

1 Transparenz:

Die Bundesregierung sollte schnellstmöglich über den Umfang der tatsächlichen Abhörmaßnahmen der Geheimdienste aufklären und darlegen, auf welcher Rechtsgrundlage in den jeweiligen Ländern Abhörmaßnahmen durchgeführt werden, in welcher Form die rechtlichen Vorgaben jeweils in die Praxis umgesetzt werden und welche Kontrollmechanismen greifen, um das behördliche Vorgehen jeweils

zuverlässig zu überprüfen und im Bedarfsfall einzuschränken. Unternehmen sollten die Möglichkeit erhalten, in aggregierter Form regelmäßig über einschlägige Maßnahmen zu berichten.

2 Rechtssicherheit:

International aktive Unternehmen dürfen nicht der Unsicherheit ausgesetzt werden, sich zwischen widersprechenden Anforderungen an die Herausgabe von Daten entscheiden zu müssen und damit zwangsläufig gegen die eine oder andere Rechtsordnung zu verstoßen. BITKOM fordert die Bundesregierung und die Mitgliedstaaten der Europäischen Union deshalb auf, innerhalb der EU und mit wichtigen Partnerländern wie den USA eine internationale Übereinkunft darüber zu erzielen, welche Auskunftsersuchen von wem und unter welchen Umständen zulässig sind und nach welchen international zu standardisierenden Verfahren Datenweitergaben erfolgen müssen – und wann sie zu unterbleiben haben. Ohne Vorliegen eines entsprechenden Abkommens sollte die Herausgabe von Daten europäischer Nutzer unzulässig sein. Etwaige Auskunftsersuche müssen dabei im Wege eines Amtshilfeersuchens gegenüber Staaten und nicht direkt gegenüber Unternehmen erfolgen. Die Politik ist dringend aufgefordert, hier für Rechtssicherheit zu sorgen. Die Bundesregierung soll darauf hinwirken, dass die Verhandlungen über die Datenschutz-Grundverordnung unverzüglich zum Abschluss gebracht werden. Außerdem muss es auf internationaler Ebene so schnell wie möglich Verhandlungen für ein Antispy-Abkommen geben. Die Bundesregierung sollte sich für die Neuverhandlung und nachhaltige Verbesserung des Safe Harbour Agreements und dessen Vollzug in den USA einsetzen. Darüber hinaus sollten bei den Verhandlungen zur Datenschutzgrundverordnung, zur Transatlantischen Handels- und Investitionspartnerschaft und zum Datenschutzrahmenabkommen zwischen der USA und der Europäischen Union die Belange des Datenschutzes und des Datenmanagements berücksichtigt werden. Nach Abschluss dieser Verhandlungen sollten bestehende Vereinbarungen dahingehend geprüft werden, ob sie eventuell entbehrlich sind.

3 Europaweiter Schutz vor Ausspähung:

Die Regierungen der EU-Mitgliedstaaten müssen einen gemeinsamen Ansatz für die Aktivitäten ihrer Geheimdienste entwickeln. Alle EU-Bürger müssen in den EU-Mitgliedstaaten unter entsprechenden Aspekten als Inländer gelten. Ein kollusives Zusammenwirken der nationalen Behörden untereinander und damit eine faktische Aushebelung des verfassungsrechtlich garantierten Fernmeldegeheimnisses und des Rechts auf informationelle Selbstbestimmung darf es nicht geben.

4 Legitimation und Umfang nachrichtendienstlicher Überwachung klären:

Legitime Interessen wie etwa Strafverfolgung und Gefahrenabwehr sind anzuerkennen und können ein Informationsbedürfnis staatlicher Stellen grundsätzlich rechtfertigen. Diese Rechtfertigung staatlicher Überwachung gilt aber nicht schrankenlos. Es ist originäre Aufgabe der Politik, eine Balance zwischen der Sicherheit auf der einen und Freiheit des Einzelnen sowie der Berufsausübungsfreiheit der betroffenen Unternehmen auf der anderen Seite zu finden. Ziel der Bundesregierung sollte es sein, sich auf internationaler Ebene für angemessene Regelungen nachrichtendienst-

licher Tätigkeiten einzusetzen, um elementare Grundrechte zu schützen und das Vertrauen in die digitale Welt zu stärken.

5 Routing:

Es ist zu prüfen, welche Beiträge zu mehr Datenschutz und Datensicherheit Maßnahmen im Bereich des Routings grundsätzlich leisten können. Im Besonderen ist dabei zu untersuchen, welche entsprechenden Beiträge von einem nationalen Routing oder einem Routing im Schengen-Raum ausgehen können.

6 Wirtschaftsspionage:

Ein unbefugter Zugriff auf Unternehmensgeheimnisse in der Datenverarbeitung und -übertragung muss als strafrechtlicher Tatbestand auch international konsequent verfolgt und mit angemessenen Schadensersatzansprüchen unterlegt werden – auch gegenüber staatlichen Stellen. Ziel sollte hier auch eine Erweiterung der vorhandenen Bündnisse um einen gegenseitigen Verzicht auf Staats- und Wirtschaftsspionage sowie Sabotage von kritischen Infrastrukturen und IT-Systemen sein. Darüber hinaus sollte sich die Bundesregierung dafür stark machen, dass Wirtschaftsspionage international geächtet und ein Abkommen verabschiedet wird, dessen Unterzeichnerstaaten verbindlich erklären, zumindest untereinander künftig auf jedwede Wirtschaftsspionage zu verzichten und sich bei der grenzüberschreitenden Strafverfolgung einschlägiger Tatbestände gegenseitig bestmöglich zu unterstützen.

7 Sicherheitsbewusstsein:

Die Unternehmen in Deutschland und in Europa müssen jederzeit im Stande sein, ihre Daten und die Daten ihrer Kunden in der Art zu schützen. Sinnvolle Mittel dazu können z.B. die Nutzung von verschlüsseltem Datenverkehr oder die Ablage von Daten nur in geschützten Bereichen sowie Data Leakage Prevention sein. Eine weitere Sensibilisierung, Medienkompetenz, öffentliche und private Initiativen zur Erhöhung der Sicherheit ist zu begrüßen. Die Allianz für Cybersicherheit und der Verein Deutschland Sicher im Netz tritt für eine Stärkung der Sicherheitskultur in Deutschland ein und leistet Beiträge, alle privaten und geschäftlichen IT-Nutzer zum Selbstschutz zu befähigen. Es werden auch Schulungen oder Weiterbildungsmaßnahmen unterstützt, die Unternehmensmitarbeiter und Bürger in die Lage versetzen, mit sensiblen Daten richtig umzugehen und auch etwa bei der Datenspeicherung oder deren Bekanntgabe über mögliche Folgen informiert sind.

8 IT-Strategie:

Die neu gebildete Bundesregierung sollte gemeinsam mit den Branchenvertretern eine Strategie zur Stärkung des IT-Standorts Deutschland entwickeln und umsetzen. Damit sollen die enormen Chancen, die sich mit der Digitalisierung für den Standort Deutschland verbinden, betont und genutzt werden.

9 Nationaler Rat:

BITKOM regt an, ähnlich dem Nationalen Ethikrat einen Kreis von Persönlichkeiten einzurichten, der in der Lage ist, Orientierungshilfe bei der Weiterentwicklung der digitalen Welt und der Ausformulierung des entsprechenden Rechtsrahmens und seiner Umsetzung zu geben.

Ex-Banker der UBS in Italien festgenommen

Ein ehemaliger Spitzenbanker der Schweizer Großbank UBS ist in Italien wegen mutmaßlicher Beihilfe zur Steuerflucht festgenommen worden. Gegen Raoul Weil, einst die Nummer drei in der Führungsriege der UBS, lag nach Angaben eines US-Vertreters ein internationaler Haftbefehl vor. Ihm droht nun die Auslieferung an die USA, wo ihm der Prozess gemacht werden soll. Weil war im Jahr 2008 vor einem US-Gericht in Florida angeklagt worden, an Steuerhinterziehung in Milliardenhöhe beteiligt gewesen zu sein. Der Banker war zwischen 2002 und 2007 für das grenzüberschreitende Privatkundengeschäft der UBS zuständig gewesen und soll in dieser Funktion reichen Amerikanern geholfen haben, ihr Vermögen am Fiskus vorbei in der Schweiz zu verstecken. Ein US-Bundesrichter erklärte Weil später als Flüchtigen und ließ ihn auf die Interpol-Fahndungsliste setzen. Laut Anklageschrift sollen rund 20 Mrd. US-$ vor den Steuerbehörden verheimlicht worden sein. Die Festnahme in Italien zeigt nach Ansicht von Dan Levy, einem ehemaligen US-Bundesstrafverfolger, dass „es eine reale Gefahr für Schweizer Banker im Fadenkreuz der US-Ermittler sei, in ein anderes Land zu reisen“. Im Kampf gegen die Steuerhinterziehung zeige sich, „wie geduldig und beharrlich das US-Justizministerium“ solche Fälle verfolge. Weil, der in seiner Sparte rund 20.000 US-Kunden betreute, soll das grenzüberschreitende Geschäft der UBS als „Giftmüll“ bezeichnet haben. Er ordnete laut Anklageschrift an, dass Mitarbeiter in der Schweiz ihre grenzüberschreitenden Dienstleistungen ausweiten, obwohl er wusste, dass die Banker damit gegen US-Gesetze verstoßen. Weils Anwalt stand für einen Kommentar nicht zur Verfügung. Im Jahr 2009 hatte ein Anwalt Weils dem Wall Street Journal gesagt, dass sein Mandant ein unschuldiges Opfer eines politischen Streits zwischen den USA und der Schweiz sei.

Eine UBS-Sprecherin teilte mit, dass Weil nach der Anklage von seinen Pflichten bei der Bank entbunden worden war. UBS hatte im Jahr 2009 zugegeben, US-Steuerzahlern dabei geholfen zu haben, Geld im Ausland zu verstecken. Die Bank zahlte 780 Mio. US-$ Strafe und händigte die Namen von mehr als 4.400 Amerikanern aus, die in der Schweiz geheime Konten unterhielten. Im Gegenzug dafür, dass sie das Schweizer Bankgeheimnis in dem Fall lüftete, entging sie einem Strafverfahren. Seitdem haben sich mehr als 38.000 US-Steuerzahler freiwillig beim Fiskus gemeldet und geheime Auslandskonten angezeigt. Die US-Regierung hat dadurch mehr als 5,5 Mrd. US-$ hinterzogener Steuern eingetrieben und weitere 5 Milliarden Dollar dürften noch folgen. Das älteste Bankhaus der Schweiz, Wegelin & Co, musste jüngst schließen, nachdem es sich der Beihilfe zur Steuerflucht in Höhe von mehr als 1,2 Mrd. US-$ schuldig bekannt hatte. Im August stellten die USA und die Schweiz ein neues Programm vor, nach dem Schweizer Banken, gegen die bisher noch keine Ermittlungen laufen, versteckte Vermögen von Amerikanern freiwillig offenlegen und entsprechende Strafen zahlen können. Hunderte von Banken dürften sich an dem Programm beteiligen.

Compliance-Profi Renz verlässt Helaba

Nach mehr als zehn Jahren als Compliance-Beauftragter der Landesbank Hessen-Thüringen

Girozentrale (Helaba) hat sich Hartmut Renz dazu entschieden, die Bank zum 31.10.2013 zu verlassen. Das Frankfurter Institut verliert damit einen der profiliertesten Compliance-Experten, der insbesondere im Bereich der Wertpapier-Compliance Pionierarbeit geleistet hat. Renz hat in Heidelberg Rechtswissenschaften studiert. Er ist Rechtsanwalt und war seit 2003 als Leiter der Compliance-Stelle Kapitalmarkt bei der Helaba tätig. Davor leitete er die Investment Banking-Grundsatzabteilung der DZ Bank AG und war für die Betreuung kapitalmarktrechtlicher Fragestellungen verantwortlich. Seine berufliche Karriere begann Renz beim BVI Bundesverband Investment und Asset Management, wo er sich mit Fragen zur Altersversorgung auf Investmentfondsbasis beschäftigte. Hartmut Renz hält seit Jahren Seminare zu kapitalmarktrechtlichen Themen und Grundsatzfragen des Wertpapiergeschäfts, publiziert regelmäßig zu diesen Fragestellungen und ist u.a. Mitherausgeber einer Praxiskommentierung zur Wertpapiercompliance. Darüber hinaus ist er Dozent an der Frankfurt School of Finance and Management im Rahmen des „Certified Compliance Professional Programs (CCP)“ sowie an der Universität St. Gallen, Schweiz, im Rahmen des „Executive Master of Business Law Programs (M.B.L.)“. Ferner ist er Mitglied des Sanktionsausschusses der Frankfurter Wertpapierbörse.

Neuer Compliance-Chef bei Paymill

Jorge Camacho (Foto) ist neuer Head of Risk & Compliance des Online-Payment-Dienstleisters Paymill. Er kommt von Facebook, wo er in den vergangenen drei Jahren das Risikomanagement sowie Legal & Compliance verantwortete. Zu seinen neuen Aufgaben gehören insbesondere die Risikosteuerung und -überwachung sowie

die Betrugsprävention. Camacho kann auf über sieben Jahre Erfahrungen im Risikomanagement und in der Betrugsanalyse zurückblicken. Der 35-jährige Jurist war zuletzt Leiter EMEA für den Compliance-Bereich des Social Networks Facebook. Davor arbeitete er bei PayPal, wo er umfangreiche Erfahrung in der Online-Payment-Branche sammelte. Innerhalb des Credit Risk Departments betreute er große Händler in Sachen Betrugsprävention im Raum DACH, Großbritannien und Spanien. Der Münchner Online-Payment-Anbieter Paymill freut sich über den kompetenten Risk Management-Experten: „Mit Jorge holen wir uns einen extrem erfahrenen Spezialisten mit ins Boot. Wir sind überzeugt, dass unser Team mit dieser Verstärkung den Service im Bereich Risk Management weiter ausbauen kann und wir auch hier neue Wege gehen können“, erklärt Mark Fabian Henkel, Mitgründer und Geschäftsführer von Paymill.

CCO Göres geht zur Deutschen Bank

Dr. Ulrich Göres (40), Chief Compliance Officer (CCO) & Group General Counsel der Erste Group Bank AG, steht vor einem Wechsel zur Deutschen Bank, wo er die weltweite Verantwortung für Anti-Geldwäsche und Financial Crime übernehmen soll. In dieser Funktion wird er direkt an den Vorstand Dr. Stephan Leithner berichten. Andreas Born, bislang Konzerngeldwäsche-Beauf-

tragter der Deutschen Bank, geht nach mehr als 30 Jahren bei der Bank zum Jahresende auf eigenen Wunsch in den Ruhestand. Göres wechselte 2010 von der Commerzbank nach Wien zur Erste Group, wo er konzernweit die Bereiche Compliance, Legal, Security, Datenschutz und das Management von Reputationsrisiken restrukturiert hat und verantwortet. Für die Commerzbank war er im Geschäftsbereich Group Compliance in verschiedenen Führungspositionen im In- und Ausland tätig, u.a. als Regional Head in den USA, zuletzt als stellvertretender Head of Group Compliance. Von 2005 bis 2007 war er bei der WestLB AG in Düsseldorf tätig. Als Global Head Private Banking Compliance war er global zuständig für die Betreuung sämtlicher Private-Banking-Aktivitäten des WestLB-Konzerns aus Compliance-Sicht.

Barclays verliert Compliance-Chef

Bei der britischen Großbank Barclays geht Compliance-Chef Hector Sants von Bord. Sants fehlte bei Barclays wegen Krankheit schon seit einigen Wochen. Als Grund hatte er damals den hohen Stresspegel genannt, weshalb er überarbeitet gewesen sei. Eigentlich sollte er nach einer Auszeit im Januar seinen Job weiter machen. Nun hieß es, dass er kurzfristig nicht in der Lage sei, die Arbeit wieder aufzunehmen. Aus diesem Grund habe er sich zur Kündigung entschieden. Bis auf Weiteres soll die Arbeit von Sants, zu der im Wesentlichen die Einhaltung von Richtlinien und Gesetzen zählte, Allen Meyer übernehmen. Meyer ist Compliance-Chef der Investmentbank von Barclays. Der endgültige Rückzug Sants folgt nur zehn Monate auf seinen Einstieg bei der britischen Großbank. Sants sollte als ehemaliger Chef der britischen Finanzmarktaufsicht FSA die angeknacksten Bande zu den Behörden wieder kitten. Er war in den Vorstand der Bank eingezogen und berichtete direkt an CEO Jenkins.

RBS-CCO wird Berater

Ashley Kovas, zuletzt Head of Compliance Policy bei der Royal Bank of Scotland (RBS), ist bei der auf Regulierungsfragen spezialisierte Beratungsgesellschaft Bovill eingestiegen. Bei der RBS Group war Ashley auch federführend an der Entwicklung und Implementierung eines unternehmensweiten Risk Framework beteiligt. Zuvor war er u.a. für Prudential und KPMG tätig und arbeitete acht Jahre bei der britischen Finanzaufsicht FSA.

Zimmerli neuer Compliance-Chef der SFAMA

Thomas Zimmerli (43) ist neuer Senior Legal Counsel und stellvertretender Geschäftsführer bei der Swiss Funds & Asset Management Association (SFAMA). Er folgt damit auf Hans Tschäni, der Ende 2013 pensioniert wird. Zimmerli ist ein ausgewiesener Experte in Compliance- und Rechtsfragen im Bereich kollektiver Kapitalanlagen. Er arbeitete zuletzt als Leiter Compliance Executive Director, bei der UBS Fund Management (Switzerland) AG, wo er seit 1999 verschiedene Funktionen ausübte. Er verfügt über das Anwaltspatent des Kantons Bern und absolvierte den Nachdiplomkurs DAS Compliance Management am Institut für Finanzdienstleistungen IFZ Zug der Hochschule Luzern. Zudem ist er Dozent an der Swiss Fund Academy und am IFZ.

Führungswechsel beim LKA-NRW

Die NRW-Polizei bekämpft konsequent die Computer- und Internetkriminalität. „Cyber-Crime ist eine wachsende Gefahr für die Gesellschaft. Deshalb setzen wir hier einen strategischen Schwerpunkt. Im Cybercrime-Kompetenzzentrum des Landeskriminalamtes wird mit rund 100 spezialisierten Polizeibeamten, Wissenschaftlern und Technikern das Expertenwissen gebündelt“, sagte NRW-Innenminister Ralf Jäger bei der Verabschiedung des bisherigen Direktors des Landeskriminalamtes Wolfgang Gatzke und der Amtseinführung des Nachfolgers Uwe Jacob. „Dazu haben wir in allen 47 Kreispolizeibehörden spezielle Ermittlungsdienststellen eingerichtet und IT-Fachleute eingestellt. Darüber hinaus intensivieren wir die Aus- und Fortbildung aller Polizeibeamtinnen und -beamten zum Thema Cybercrime.“ In den ersten zehn Monaten dieses Jahres gab es 23.104 Fälle von Computerkriminalität in NRW. Das sind 22 Prozent mehr als im gleichen Zeitraum des Vorjahres (+ 4.273 Fälle). Insbesondere bei Straftaten der Datenveränderung und Computersabotage gab es einen deutlichen Anstieg um rund 60 Prozent auf nunmehr 5.963 Fälle. „Es gibt mittlerweile kaum noch eine Straftat, die ohne Nutzung moderner Informations- und Kommunikationstechnik begangen wird. Und wenn es nur das Mobiltelefon ist“, erklärte der Innenminister. Das Cybercrime-Kompetenzzentrum im LKA Düsseldorf hilft mit modernster Technik, Kriminelle aus der Anonymität des Internets zu bringen, die früher unentdeckt geblieben wären. Für Unternehmen und Behörden in NRW ist das Kompetenzzentrum zentrale Ansprechstelle. Knapp 500 Mal nutzten Unternehmen und Behörden bis Ende Oktober das Wissen der Cybercrime-Experten bei Hacking- oder DDOS-Attacken. Im Jahr zuvor waren es zum gleichen Zeitpunkt rund 200 Anfragen. Die Experten beraten kompetent im Schadensfall und bei einer vermuteten Straftat. Sie leiten erste Schritte ein, um weitere Schäden zu verhindern und Straftaten zu verfolgen. „Mit dem erfahrenen Kriminalisten Uwe Jacob ist ein Garant dafür gegeben, dass das LKA weiterhin bei der Kriminalitätsbekämpfung des sich rasant entwickelnden Cybercrime Schritt hält“, hob Jäger hervor. Im LKA ist der 57-jährige Jacob kein Unbekannter. Er leitete dort bereits 2007 das Dezernat Kriminalitätsangelegenheiten und ab 2009 die Abteilung für Ermittlungsunterstützung. Seit 2010 ist Jacob im Innenministerium für Kriminalitätsbekämpfung und die strategische Ausrichtung der Kriminalpolizei zuständig. „Uwe Jacob besitzt herausragende kriminalpolizeiliche Kompetenz und praktische Erfahrungen aus vielen Bereichen der Polizei“, charakterisierte Jäger den neuen LKA-Chef. Jäger dankte dem scheidenden LKA-Direktor Wolfgang Gatzke für seine erfolgreiche Arbeit. „Wolfgang Gatzke ist ein souveräner und anerkannter Fachmann im In- und Ausland in allen Bereichen der Kriminalitätsbekämpfung, ein brillanter Analytiker und ein stets sachlich und fachlich argumentierender Gesprächspartner“. Unter seiner Leitung hat sich auch das Kriminalwissenschaftliche und -technische Institut (KTI) des LKA auf neue Anforderungen ausgerichtet. So wurde der DNA-Untersuchungsbereich von 30 auf 70 Wissenschaftler und technische Assistenten ausgeweitet, um die ständig steigende Anzahl der DNA-Untersuchungsanträge qualifiziert zu bewältigen. Mit dem Cybercrime-Kompetenzzentrum setzte Gatzke einen deutlichen Schwerpunkt in diesem Bereich. Diesem Vorbild folgten mittlerweile fast alle anderen Länder und das BKA. Uwe Jacob will an der erfolgreichen Arbeit von Wolfgang Gatzke anknüpfen.

Termine

Zertifikatkurs: Basis Seminar Compliance 2013

Termin: 10. – 11. Dezember 2013
Ort: Münster
Gebühr: 1.290 EUR
Info: www.ca-seminare.de

Zertifikatkurs: Compliance Officer (Univ.)

Termin: 14. März 2014
Ort: Universität Augsburg (ZWW)
Gebühr: 6.250 EUR (inkl. Prüfungsunterlagen)
Info: www.zww.uni-augsburg.de/finance

Veranstaltung: Fraud Prevention

Termin: 20. März 2014
Ort: Frankfurt/Main
Gebühr: 1.050 EUR (inkl. Prüfungsunterlagen)
Info: www.forum-institut.de

Fachtagung: Compliance for Banks

Termin: 26. – 27. März 2014
Ort: Köln
Gebühr: 149 EUR (für Banker)
Info: www.compliance-fachtagung.de

Impressum

Verlag und Redaktion:
Bank-Verlag GmbH
Postfach 450209, 50877 Köln
Wendelinstraße 1, 50933 Köln

Tel. 0221/54 90-0
Fax 0221/54 90-315
E-Mail: medien@bank-verlag.de

Geschäftsführer:
Wilhelm Niehoff (Sprecher),
Matthias Strobel

Gesamtleitung Kommunikation und Redaktion:
Dr. Stefan Hirschmann
Tel. 0221/54 90-221
E-Mail: stefan.hirschmann@bank-verlag.de

Objektleitung:
Bernd Tretow

Layout & Satz:
Cathrin Schmitz
Tel. 0221/54 90-132
E-Mail: cathrin.schmitz@bank-verlag.de

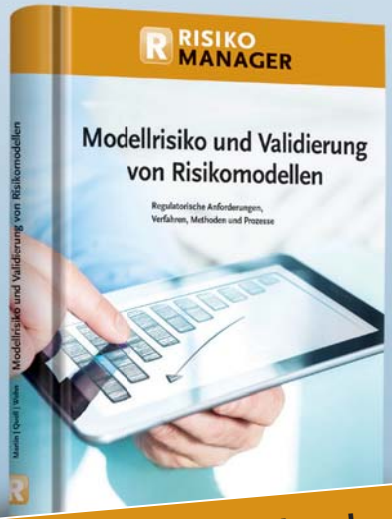
Mediaberatung
Nicola Lipmann
Tel. 0221/54 90-133
E-Mail: nicola.lipmann@bank-verlag.de

Redaktion:
Anja Kraus
Tel. 0221/54 90-542
E-Mail: anja.kraus@bank-verlag.de

Erscheinungsweise: 10 x jährlich
Der nächste bank&compliance-Newsletter 1-2014 erscheint in der KW 03.

ISSN: 2195-4488

Fachbücher für Risikomanagement-Profis



Neues Standardwerk

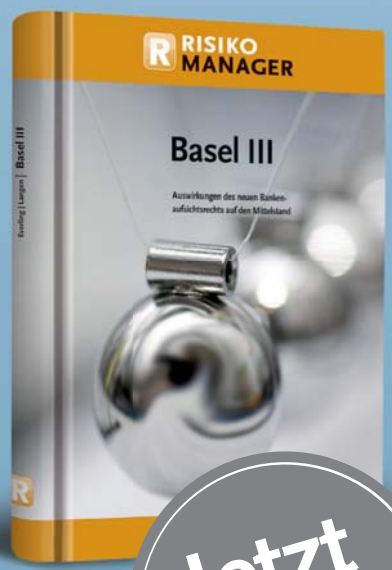
Marcus R. W. Martin | Peter Quell | Carsten S. Wehn (Hrsg.)

Modellrisiko und Validierung von Risikomodellen

Regulatorische Anforderungen, Verfahren, Methoden und Prozesse

ISBN 978-3-86556-381-1
Art.-Nr. 22.496-1300
368 Seiten, gebunden

69,00 Euro



Jetzt bestellen

Oliver Everling | Rainer Langen (Hrsg.)

Basel III

Auswirkungen des neuen Bankenaufsichtsrechts auf den Mittelstand

ISBN 978-3-86556-354-5
Art.-Nr. 22.486-1300
200 Seiten, gebunden

59,00 Euro

Weitere Fachbücher in unserem Shop:
www.bank-verlag-shop.de

RISIKO MANAGER

Bank-Verlag GmbH | Wendelinstraße 1 | 50933 Köln | Tel. +49-221-5490-500 | E-Mail: medien@bank-verlag.de