die bank 17.10.2018
NEWSLETTER FÜR BANKPOLITIK UND PRAXIS

TOP-THEMA

©iStockphoto.com/iLexx

Aktuelles Lagebild

Cyber Crime: Schäden von über 70 Mio. Euro

71 statt zuletzt 50 Mio. Euro Schadensumme und ein genereller Anstieg der Fälle von Cyber Crime stehen einem deutlichen Rückgang beim Phishing im Online Banking entgegen, wo die Fallzahlen so niedrig sind wie zuletzt vor fünf Jahren. Die vielfältigen Schutz- und Erkennungsmaßnahmen der Banken zeigen Wirkung.

Cyber Crime, vereinfacht formuliert: Straftaten, die mithilfe von modernen Informations- und Kommunikationsstrukturen verübt werden, sind seit Jahren ein florierender Sektor des globalen Verbrechens. Trotz steigender Fallzahlen muss man davon ausgehen, dass die Dunkelziffer nicht gemeldeter bzw. angezeigter Fälle von Internetkriminalität wesentlich höher liegt als die Zahl bekannter Fälle. So veröffentlichte der Digitalverband Bitkom im Herbst 2017 eine Untersuchung, wonach jeder zweite Internetnutzer bereits Opfer von Cyber Crime wurde, aber nur 18 Prozent der Geschädigten hatten auch eine Anzeige bei der Polizei erstattet.

Vor diesem Hintergrund sind die Zahlen der Polizeilichen Kriminalstatistik mit gewissen Einschränkungen zu betrachten. Das Bundeskriminalamt (BKA) stellte in Wiesbaden sein aktuelles „Cybercrime Bundeslagebild“ für 2017 vor. Darin wurden 85.960 Fälle von Cybercrime „im engeren Sinn“ erfasst, eine Steigerung um 4 Prozent gegenüber 2016. Gestiegen ist auch die Aufklärungsquote, sie liegt aktuell bei 40,3 Prozent. Zum Tatbild „Cybercrime im engeren Sinne“ gehören Delikte im Rahmen des Computerbetrugs (u.a. Datenklau bei Kreditkarten, Überweisungsbetrug oder Abrechnungsbetrug im Gesundheitswesen), Ausspähen, Abfangen und Hehlerei von Daten, Com-

DIE BANK

Demnächst …

Es tut sich etwas hinter diesem Vorhang. Was, das wird noch nicht verraten.

Wir arbeiten dran.

Woran? An einem neuen Zusatzangebot.

Seien Sie gespannt! Wir halten Sie auf dem Laufenden.

Ihr Team von „die bank“

putersabotage, Datenveränderung, Fälschung von beweisrelevanten Daten und noch einiges mehr.

Der „typische" Täter ist dabei deutsch, männlich und zwischen 21 und 39 Jahren alt: Von den insgesamt 22.296 Tatverdächtigen aus dem Jahr 2017 waren 68 Prozent männlich, 77 Prozent besaßen die deutsche Staatsangehörigkeit und 58 Prozent sind im genannten Altersfenster. Nach den deutschen Staatsbürgern sind türkisch, rumänisch und polnisch die meistvertretenen Nationalitäten. Dabei ist vom Einzeltäter, der im alleine daheim programmiert, bis hin zu international organisierten Gruppen eine heterogene Tätergruppe vertreten. Das Spektrum reicht bis zu kriminellen Marktplätzen, wo „Cybercrime-as-a-Service"-Modelle florieren und entsprechende Produkte und Services in einer „Underground Economy" angeboten werden.

Die bekannte Schadensumme stieg von 50,9 Mio. Euro 2016 auf nunmehr 71,4 Mio. Euro, wobei die Summe pro Fall bei unveränderten 4.000 Euro blieb. Das Hauptbeschäftigungsfeld der Internet-Kriminellen ist die digitale Erpressung, sprich die Verbreitung von Ransomware, wobei Daten verschlüsselt werden bzw. der Zugriff darauf verwehrt wird und nur gegen Zahlung von Lösegeld – meist in digitalen Währungen – eine Freigabe erfolgt. „WannaCry" war der bekannteste Fall im letzten Frühling, mit der Deutschen Bahn als prominentestes Opfer. Das BKA zitiert in diesem Zusammenhang eine Studie des BSI, wonach im letzten Jahr 70 Prozent der befragten Wirtschaftsunternehmen in Deutschland von Cyber-Angriffen betroffen waren. Außerdem wurden viele weitere Arten von Schadsoftware registriert, wie Keylogger, Spyware und Banking-Trojaner.

G4C an Erstellung des Lagebilds beteiligt

Das BKA hat für die Erstellung des aktuellen Lagebilds intensiv mit dem G4C zusammengearbeitet. Das German Competence Centre against Cyber Crime e.V. ist ein Zusammenschluss, in dem neben dem BKA und dem BSI Banken (Commerzbank, ING-DiBa, HVB und KfW), Computer- und Softwareunternehmen sowie der Kölner Bank-Verlag ihre Erkenntnisse im Kampf gegen Internetkriminalität vernetzen. Diese Zusammenarbeit trug zu einer qualitativen Verbesserung des diesjährigen Lagebilds bei.

Auffällig ist der massive Anstieg bei mobiler Malware. Bei einer flächendeckenden Verbreitung von Smartphones und Tablets, die ständig online sind und E-Commerce-Aktivitäten ebenso abwickeln wie Transaktionen im Online-Banking, sind diese Geräte ein attraktives Angriffsziel für Kriminelle. G4C-Mitglied Symantec analysierte eine Zunahme von mobiler Malware um 54 Prozent im letzten Jahr mit 27.000 bekannten Varianten. Das BSI bestätigt diese Tendenz. Die größte Schwachstelle sind dabei die Nutzer selbst, die Apps aus unseriösen Quellen installieren, Sicherheitsupdates nicht ausführen und ihre Daten nicht genügend schützen und so den Cybergangstern den Angriff leicht machen.

Eine erfreuliche Veränderung zeigte sich im Bereich Phishing im Online Banking. Die Fallzahl sank im letzten Jahr um 34 Prozent auf 1.425 Fälle, das ist der niedrigste Stand seit fünf Jahren und bestätigt eine auch von Europol bereits festgestellte Tendenz. Außerdem darf man für diesen Deliktbereich davon ausgehen, dass das Dunkelfeld sehr gering ist. Der betrogene Kunde hat ein starkes Interesse, den Fall bei der Polizei anzuzeigen, denn nur in diesem Fall erstatten die Banken den durch das Phishing entstandenen Schaden.

Kampf der Banken erfolgreich – BaFin kündigt weitere Sicherheitstests an

Die Banken sind maßgeblich verantwortlich für den Rückgang dieser Angriffe. Sie haben die Möglichkeiten zum Entdecken solcher Angriffe konsequent weiterentwickelt und verfeinert und dabei auch Erkennungsmöglichkeiten zur Abwehr von malwarebasierten Abgriffen beim Online Banking installiert. Sie hatten viele Anforderungen aus den BAIT (Bankaufsichtliche Anforderungen an die IT) bereits antizipiert. Im Rahmen einer BAIT-Konferenz in Frankfurt kündigte BaFin-Exekutivdirektor Raimund Röseler in Frankfurt an, künftig noch stärker auf die Effektivität von Schutzmaßnahmen und auf geeignete Krisenreaktionsmechanismen zu achten. Die Behörde überlege, mit umfangreichen Sicherheitstests („Penetrationstests") die IT-Sicherheitssysteme der Banken auf Herz und Nieren zu testen, denn: „Software- oder Hardwarestörungen und Mängel in der ‚Cyber-Hygiene' sind viel häufiger die Ursache von Sicherheitsvorfällen als Attacken von außen", so Röseler.

Ebenfalls im Fokus von Cyber-Angriffen stehen die Betreiber Kritischer Infrastrukturen. Das potenziell hohe Schadenniveau, das beim Ausfall dieser Strukturen droht, ist nicht nur finanziell erheblich, sondern auch für politisch motivierte Täter verlockend. KRITIS-Unternehmen sind nach dem IT-Sicherheitsgesetz verpflichtet, festgestellte Vorfälle an das BSI zu melden. Dem Bundesamt für Sicherheit in der Informationstechnik lagen bis zum 30. Juni 2017 insgesamt 34 Meldungen vor, Schwerpunkt dabei war der Sektor Informationstechnik und Telekommunikation. (Anja U. Kraus)

Die komplette Statistik finden Sie auf der Webseite des Bundeskriminalamts.

Bitkom und BSI warnen: Starke Zunahme von Cyber-Attacken

Die Gefahr kommt aus dem Web

Wenn sich Unternehmen früher mit Wachmännern und Diensthunden vor illegalen Eindringlingen schützen konnten, sind heute andere Schutzmechanismen gefragt. Der reale Einbrecher, der auf dem Firmengelände Waren oder Werkzeuge stiehlt, ist harmlos im Vergleich zur Gefahr aus dem Internet.

Gut acht von zehn deutschen Industrieunternehmen berichten über eine Zunahme der Cyber-Attacken in den letzten beiden Jahren, mehr als Drittel verzeichnete sogar eine starke Zunahme von Datenklau, Spionage oder Sabotage. Quer durch alle Branchen stehe die deutsche Industrie unter „digitalem Dauerbeschuss“, sagte Bitkom-Präsident Achim Berg bei der Vorstellung einer Sicherheits-Studie. Der Querschnitt der Täter reiche dabei vom „digitalen Kleinkriminellen“ über die organisierte Kriminalität bis hin zu Hackern im Staatsauftrag. Und die weiteren Aussichten sind eher düster: „Qualität und Umfang der Cyber-Angriffe werden weiter zunehmen“, so Berg.

Seine Prognose deckt sich mit der Aussage der befragten Geschäftsführer und Sicherheitsverantwortlichen, die zu 82 Prozent mit einer Zunahme der Attacken rechnen. Schutz bieten neben technischen auch organisatorische und personelle Sicherheitsvorkehrungen, das wissen auch die Unternehmen. Sie schützen ihre Geräte mittlerweile flächendeckend durch Passwörter, installieren Firewalls und Virenscanner und machen regelmäßige Backups ihrer Daten. Immerhin ein Viertel simuliert zudem Angriffe von außen mithilfe von Penetrationstests. 5 Prozent der Unternehmen beschäftigen sich im Zusammenhang mit IT-Sicherheit bereits mit Künstlicher Intelligenz, um sich gegen Datendiebstahl und ähnliche Unbill zu schützen.


©iStockphoto.com/Henrik5000

Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat in den letzten Monaten eine erhöhte Gefährdungslage im Bereich der Cyber-Sicherheit wahrgenommen. Schadprogramme wie WannaCry, NotPetya oder Spectre/Meltdown zeigten eine neue Qualität von Cyber-Angriffen und IT-Sicherheitsvorfällen und richteten sich gegen die Grundpfeiler der Informationstechnologie, während gleichzeitig die Digitalisierung und Vernetzung von IT-Systemen, Alltagsgegenständen und Industrieanlagen voranschreite. Diese Kombination hebe die Gefährdungslage auf ein neues Niveau, heißt es im „Bericht zur Lage der IT-Sicherheit in Deutschland 2018.“ BSI-Präsident Arne Schönbohm stellte den Bericht gemeinsam mit Bundesinnenminister Horst Seehofer vor und erläuterte, die nationale Cyber-Sicherheitsbehörde müsse täglich neue Lösungen konzipieren und umsetzen. Der Lagebericht belege aber die Erfolge der Maßnahmen im Bereich der Prävention, Detektion und Reaktion, etwa mit der Umsetzung der Cyber-Sicherheitsstrategie der Bundesregierung oder des IT-Sicherheitsgesetzes.

Das BSI beobachtet eine hohe Dynamik der Angreifer bei der Weiterentwicklung von Schadprogrammen und Angriffswegen. Bereits bekannte Schadsoftware wird fortlaufend weiterentwickelt. Immerhin wurden im Berichtszeitraum keine größeren Angriffswellen mit Verschlüsselungs-Software registriert. Ransomware bleibe aber eine massive Gefährdung, die der deutschen Wirtschaft Schäden in Millionenhöhe beschere.

Als neue Gefährdung hat das BSI im Lagebericht das Thema illegales Krypto-Mining näher betrachtet. Aufgrund der hohen finanziellen Attraktivität und der Unauffälligkeit der Infektionen sei illegales Krypto-Mining als signifikant zunehmendes Cyber-Risiko zu bewerten.

Der aktuelle Lagebericht ist auf der Webseite des BSI unter https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html verfügbar, die Bitkom-Studie „Wirtschaftsschutz in der Industrie 2018“ unter https://www.bitkom.org/Bitkom/Publikationen/Wirtschaftsschutzstudie-2018.html

Europa schlechter vorbereitet als Asiaten und Amerikaner

Nur jedes zweite europäische Unternehmen verfügt über eine umfassende Cyber-Sicherheitsstrategie. Im internationalen Vergleich liegen sie damit auf dem vorletzten Platz, hinter Asien, Nord- und Südamerika und vor dem Nahen Osten.

©iStockphoto.com/imaginima

Die PwC-Studie „The Global State of Information Security 2018" untersuchte sechs Felder zur Abwehrfähigkeit von Unternehmen, und in allen landete Europa auf dem vierten Platz. Insgesamt wurden mehr als 9.500 Unternehmen analysiert, davon 2.416 in Europa. „In den meisten Bereichen haben 40 bis mehr als 50 Prozent der Unternehmen pro Region keine ausreichenden Maßnahmen ergriffen. Hinsichtlich der ständig zunehmenden Gefahr von Cyber-Angriffen stellt das ein hohes Risiko für die Wettbewerbsfähigkeit der einzelnen Unternehmen und je nach Relevanz dieser auch für die jeweiligen Volkswirtschaften dar", warnt Cyber-Security-Experte Jörg Asma von PwC.

53 Prozent der befragten 2.416 europäischen Unternehmen haben angegeben, dass sie ihre Mitarbeiter noch nicht intensiv hinsichtlich Datenschutz und Cybersicherheit trainieren würden (vgl. Asien: 43 Prozent, Nordamerika: 42 Prozent). Die gleiche Anzahl verfügt über keine präzise Übersicht persönlicher Daten in ihren Unternehmen. Nur 44 Prozent haben die Aussage getroffen, dass man das Sammeln, Archivieren und den Zugang zu Daten auf ein Minimum reduzieren würde. 42 Prozent lassen sich von Dritten auditieren, und 44 Prozent setzen durch Dritte spezifisch definierte Compliance-Vorschriften um.

Der Nahe Osten rüstet allerdings auf. Es gebe keine Region der Welt, die nach eigenen Angaben so umfangreich in das Thema Cyber-Sicherheit investiere wie der Nahe Osten, sagt Asma. Bei der PwC Global CEO Survey gaben fast zwei Drittel der Firmenlenker im Nahen Osten an, umfassend in Cyber-Sicherheit zu investieren, um Vertrauen bei Kunden aufzubauen. In den USA hat dies jeder zweite CEO angegeben, in Westeuropa 47 Prozent und in den zentralen und osteuropäischen Ländern 43 Prozent. Laut Asma tun sich bei Investitionen in Cyber-Sicherheit gerade auch in Deutschland viele Unternehmen noch schwer. Dafür sieht er drei Gründe: Zunächst das Fehlen von subjektiv empfundener Notwendigkeit und eines ausreichenden Präventiv-Gedankens. Zweitens: Unternehmen, die investieren, merkten rasch, dass diese Investition nicht beim Geld ende. ‚Security by Design' bedeute intensives Verweben von Sicherheit in Prozessen und Kultur und erfordere viele Ressourcen. Hinzu kommt Grund drei: Der Anbietermarkt für Cyber-Sicherheit sei in Deutschland und Europa zerklüftet zwischen Einzelberatern, internationalen Großanbietern und mittelständischen Anbietern, die teils exzellente Technologien besitzen, aber unbekannt sind. Die Qualität von Beratung, Software und Betrieb lasse sich kaum evaluieren.

Das Risikopotenzial der Cyber-Bedrohung liegt insgesamt so weit vorne auf der Agenda der CEOs wie noch nie. Im diesjährigen Global CEO Survey ist es von Platz zehn auf Platz drei gestiegen, gemeinsam mit geopolitischen Risiken. Nur Überregulierung und Terrorismus machen den CEOs weltweit mehr Sorgen. Cyber Security stehe also im Fokus. Entscheidend werde es nun sein, die individuell richtigen technischen wie prozessualen Maßnahmen zur Prävention, Detektion und Reaktion aufzusetzen. Unternehmen, denen das gelinge, verfüßgten damit über einen Wettbewerbsvorteil.

Corporate- und Investmentbanken:

Vorteile für US-Konkurrenz

Die europäischen Unternehmensbanken leiden unter der Konkurrenz aus Amerika. In den letzten zehn Jahren sank der Marktanteil der hiesigen Corporate- und Investment Banks (CIB) von 50 auf 33 Prozent, ihr Gesamtumsatz ging innerhalb von fünf Jahren um 25 Prozent zurück und sank von 82 auf 61 Mrd. Euro. Wie sich dieser gefährliche Trend begründen lässt, wird in einer aktuellen Studie von Eurogroup Consulting untersucht. Dabei werden mehrere Punkte deutlich.

Auffällig sind vor allem die starken Wettbewerbsvorteile der US-Banken, die einerseits auf den dortigen Markt selbst, andererseits aber auch auf das flexiblere Regulierungsumfeld zurückzuführen seien. Europäische Banken hingegen litten unter einem strengeren Rechtssystem. Zudem werde die in London erwartete Lockerung der Regulierung zugunsten der Banken in der City nach dem Brexit die Wettbewerbsfähigkeit der kontinentaleuropäischen Banken noch zusätzlich verstärken.

Die größte Bedrohung geht nach Ansicht der Berater jedoch von digitalen Transformation aus. Diese Revolution werde von Beginn an in den Vereinigten Staaten weitaus besser umgesetzt. Hier sei eine radikale Aufwertung von „kundenzentrierten" Geschäfts- und Betriebsmodellen gefragt, die nicht nur die IT-Systeme und die Organisation des Unternehmens, sondern auch deren hierarchische Strukturen und Kompetenzen einschließe. Die digitale Technologie sei heute mehr denn je ein wichtiger Treiber für die Unternehmensleistung, verändere die Arbeit des Unternehmensbankers und habe somit eine direkte Auswirkung auf die gesamte Wirtschaft des CIB-Sektors.

Die Bedrohung erreiche die traditionellen Investment- und Finanzierungsbanken auch im Bereich ihres einst unverzichtbaren Kerngeschäfts der Wirtschaftsfinanzierung. Der Eintritt neuer Player schwäche die einstigen Platzhirsche in Europa durch disruptive Marktveränderungen. Alternative Finanzierungen erwirtschafteten im Jahr 2017 bereits rund 550 Mrd. US-Dollar, bis 2022 soll diese Summe bei 1.000 Mrd. US-Dollar liegen. Trotz bereits begonnener Anpassungsmanöver, mit denen sich etablierte Banken auf alternativen Finanzmärkten zu positionieren versuchten, blieben zahlreiche Baustellen bestehen, sagt Pierre Reboul, Partner bei Eurogroup Consulting. „Die Investitions- und Finanzierungsbank der Zukunft muss neu erfunden werden, agil und widerstandsfähig." Die europäischen Banken müssten sich schneller anpassen, um den tiefgreifenden Veränderungen standzuhalten. Der zukünftige „Augmented Banker", mehrkanalig, allwissend, agil, „super compliant" und kundennah, stelle hier ein Ideal dar. Einige Banken hätten bereits damit begonnen, die notwendigen Rahmenbedingungen zu schaffen, z. B. mehr Zeit für Aufgaben mit hoher Wertschöpfung einzuräumen. Die Veränderung von Know-how, Erfahrung und Kompetenzen in großen Unternehmen bleibe jedoch ein langwieriges, gigantisches Unterfangen.

Investoren und Nachhaltigkeit

ESG drängt in den Mainstream

Die überwiegende Mehrheit der Investoren und Emittenten weltweit verfolgt bereits eine Nachhaltigkeitsstrategie nach den Kriterien „Environment", „Social" und „Governance" (ESG). Damit drängt ESG in den Mainstream. Das ist das Ergebnis einer von HSBC in Auftrag gegebenen Umfrage unter 1.731 Unternehmen und Investoren weltweit.

Im internationalen Vergleich sind die europäischen Investoren damit führend bei der Verfolgung einer Nachhaltigkeitsstrategie: Hier beziehen 85 Prozent entsprechende Kriterien in ihre Anlageentscheidungen ein, in Asien sind es nur 40 Prozent. Auch auf der Emittentenseite ist Europa vorne: Knapp 90 Prozent der Unternehmen – vor allem die mit einem Umsatz von über 10 Mrd. US-Dollar – verfolgen eine Nachhaltigkeitsstrategie, in den USA sind es 21 und in Hongkong nur 13 Prozent.

Im Vergleich zur letzten Umfrage aus dem Jahr 2017 zeigt sich, dass der Druck der Investoren offenbar Wirkung gezeigt hat. Vor allem in Europa wollten die Investoren schon damals verstärkt nachhaltig investieren, ihnen fehlten aber die Investitionsziele.

Beweggründe für ESG

Hauptbeweggrund für eine ESG-Strategie sind höhere finanzielle Returns, diese wurden in den persönlichen Interviews mit jeweils über 800 Vertretern von Unternehmen und institutionellen Investoren am häufigsten genannt. An zweiter Stelle stehen Steuervergünstigungen. Das zeigt, dass sich Bemühungen um Nachhaltigkeit immer häufiger in Euro und Cent auszahlen. Nur für Pensionsfonds und Staatsfonds steht die Regulierung an zweiter Stelle, wenn es um die Entscheidung geht, Nachhaltigkeitsaspekte einzubinden.

Für Unternehmen in Europa stehen außerdem selbstgesetzte Nachhaltigkeitsziele sowie der Druck von der Investorenseite ganz oben auf der Liste. Nachhaltige Lieferketten sind dagegen

für große Unternehmen (jenseits von 10 Mrd. Euro Umsatz) in China und Hongkong der zweitwichtigste Faktor, auf Nachhaltigkeit zu setzen.

Die Unternehmen investieren das Geld größtenteils intern, um ihre Geschäftsprozesse nachhaltiger aufzustellen. Zwei Drittel investieren in moderne Produktionsstätten, neue Maschinen oder in Stromquellen mit erneuerbaren Energien. Chinesische Unternehmen zeigen eine Besonderheit: 9 Prozent nutzen das Geld, um grüne Mergers & Acquisitions zu realisieren.

„Die Verschiebung in Richtung finanzieller Beweggründe zeigt, dass der Druck der Investoren wirkt und die Marktkräfte eine Verhaltensänderung erzeugt haben. Kurzum: ESG, klimagerechte Finanzierung und Risikomanagement nähern sich dem Mainstream“, schlussfolgerte Daniel Klier, bei HSBC verantwortlich für Strategien und nachhaltige Finanzierungsmodelle, aus den Ergebnissen der Studie.

Hindernisse

Unter den befragten Unternehmen sehen zwei Drittel keine Hürden, ihre Sustainable-Finance-Aktivitäten zu erhöhen. Bei den Investoren zeigt sich ein ähnliches Bild: Für 57 Prozent steht einem Ausbau ihrer Investitionen im ESG-Bereich nichts entgegen. Weniger als 10 Prozent der Investoren haben speziell für ESG vorgesehene Budgets.

Investoren, die Hürden erkennen, nennen meist die fehlenden Standards für ESG als Hindernisgrund. Gleiches hindert auch Emittenten weltweit daran, stärker auf Sustainable Finance zu setzen. Hier sind die europäischen Investoren keine Ausnahme. Investoren klagen zudem nach wie vor über fehlende Investitionsobjekte, die sich durch eine mangelhafte Datentransparenz bei den Unternehmen nochmal verschärft hätten.

Auch wenn das Engagement in ESG steigt und eine bessere Reputation ebenfalls ein Treiber für die Entwicklung ist, legen die wenigsten Investoren und Emittenten ihre Strategie offen. Die internationale Regulierung wird zwar als einer der Hauptgründe für mehr Offenlegung weltweit genannt, allerdings kennen nur 8 Prozent der Emittenten und 10 Prozent der Investoren die TCFD-Initiative. Die „Task Force of Climate-related Financial Disclosures“-Initiative, ein unabhängiger, freiwilliger Zusammenschluss des Financial Stability Boards und der Bank of England, hat es sich zum Ziel gesetzt, einheitliche Standards und global anwendbare Empfehlungen zur Offenlegung von Klimarisiken festzulegen. Damit soll die Transparenz gegenüber Investoren, Anlegern und Anteilseignern erhöht werden. Lediglich im Vereinigten Königreich wissen ein Fünftel der Unternehmen um die TCFD-Initiative. Dabei gilt: Je größer das Unternehmen, desto eher ist TCFD ein Begriff.

Da der Markt auf eine Regulierung hinarbeitet, um mehr Transparenz zu schaffen, gleichzeitig die Kapitalgeber eine verstärkte Offenlegung von Nachhaltigkeitsrisiken erwarten und die TCFD genau ein solches Rahmenwerk biete, sollte die Umsetzung der Handlungsempfehlungen global zu einer dringenden Priorität erkoren werden, empfiehlt Klier.

Brexit: Mindestens 8.000 Jobs für Frankfurt

Während die Brexit-Verhandlungen in ihre heiße Phase gehen und sich Großbritanniens Regierungschefin Theresa May mit ihren jüngsten Forderungen nach einem Sonderstatus wenig Freunde bei den EU-Länderchefs macht, werden in der Bankenbranche Tipps heiß gehandelt, welche Bank als erste den Umzug von London nach Frankfurt finalisiert.

„Aktuell haben 25 Brexit-Banken Frankfurt auserkoren – weit mehr als Paris oder andere Standorte“, heißt es im druckfrischen Papier „Finanzplatz Frankfurt“ der Helaba, indem Chefvolkswirtin Gertrud R. Traud diesmal den Brexit unter die Lupe nimmt und mit ihrem Team analysiert, bei welchen Londoner Banken so langsam das Kofferpacken beginnt. Helaba Research verhehlt dabei nicht, dass das Frankfurter Institut die Fortentwicklung des deutschen Finanzzentrums im Fokus hat und sich entsprechend engagiert, u. a. als Gründungsmitglied in der Initiative Frankfurt Main Finance.

Entsprechend freudig nimmt man es am Main zur Kenntnis, dass sich seit Jahresbeginn die Geschäftsverlagerungen bei immer mehr Instituten konkretisieren. Nach derzeitigem Planungsstand wollen jeweils sechs Banken ihren Standort von London nach Dublin bzw. Luxemburg verlagern, drei nach Amsterdam und neun Banken zieht es nach Paris. Da hat Frankfurt mit 25 hinzukommenden Banken ganz klar die Nase vorn, darunter Hochkaräter wie Barclays, CiCC, Citigroup, Goldman Sachs, JP Morgan oder Morgan Stanley. Die Helaba Volkswirte gehen davon aus, dass sich ab dem kommenden Jahr die Folgen des Brexits „deutlich positiv“ in der Beschäftigungsrate der Frankfurter Bankenszene auswirken werden. „Wir halten an unserer Prognose fest, dass durch den Brexit im Lauf der nächsten Jahre mindestens 8.000 Finanzjobs in Frankfurt geschaffen werden“, so Traut. Die vollständige Analyse steht auf der Website der Helaba bereit.

Zusatzpunkte im „War for Talents“

Hochschulabsolventen können sich ab sofort und bis zum 31. Dezember 2018 mit ihren Abschlussarbeiten aus dem Themenbereich „Banking & Finance“ für den 18. Karriere-Preis der DZ Bank Gruppe 2019 bewerben. Mit einem Preisgeld von insgesamt 24.000 € geht es hierbei um den höchstdotierten Hochschulpreis der deutschen Wirtschaft für akademische Abschlussarbeiten im diesem Bereich. Die Auszeichnung wird in zwei Kategorien vergeben: Master-Thesen und Bachelor-Thesen. Die eingereichten Arbeiten werden von einer Jury aus Wissenschaft und Praxis bewertet. Bewertungskriterien sind insbesondere Aufbau, Methodik, Originalität, Aktualität und Praxisrelevanz der Abschlussarbeiten.

Die Themen der eingereichten Arbeiten spiegeln in jedem Jahr die Themen wider, die aktuell die Bankenwelt beschäftigen. Die DZ Bank Gruppe sei einerseits sehr an Zukunftsthemen orientiert und suche deshalb den Austausch mit den Hochschulen, andererseits stärke sie mit dem Karriere-Preis aber auch die positive Wahrnehmung als attraktiver Arbeitgeber bei den vielfach umworbenen akademischen Nachwuchskräften, sagte Bereichsleiter Oliver Best. Der Preis wird gemeinsam von den Unternehmen der Bankgruppe ausgerichtet. Informationen zur Online-Bewerbung sind im Internet unter www.karrierepreis.de abrufbar.

Auf einen Kaffee in die Bankfiliale

Daten sind das Gold unserer Tage und Kunden, die für sich selbst einen klaren Mehrwert erkennen, sind durchaus bereit, ihrer Bank Daten zur Verfügung zu stellen. Dabei profitieren die Geldinstitute von dem hohen und in anderen Branchen unerreichten Vertrauensvorsprung: 72 Prozent der Bankkunden in Deutschland gehen davon aus, dass Kreditinstitute mit ihren persönlichen Daten sorgsam umgehen. Auf dieser Grundlage sollten es die Banken eigentlich leicht haben, Kontodaten systematisch auszuwerten. Scheu sei dabei fehl am Platz, denn rund die Hälfte der Bankkunden gehe – irrtümlich – davon aus, dass eine solche Auswertung ohnehin bereits stattfinde, heißt es in der „Bankkunden-Studie 2018 - Digitale Dienste“ der Unternehmensberatung Berg Lund & Company (BLC). Dafür wurden 2.000 deutsche Bankkunden befragt.

Banken gelten als erfahren und verlässlich im Umgang mit vertraulichen Informationen. Knapp drei von vier Deutschen geben an, dass sie ihrem Kreditinstitut in Bezug auf Datenschutz vertrauen. Bei Onlinehändlern sind es nur gut 40 Prozent der Befragten, bei sozialen Netzwerken wie Facebook gerade einmal 22 Prozent. Grundsätzlich fühlten sich die Kunden bei den Banken gut und sorgsam betreut. Thomas Nitschke von BLC geht deshalb davon aus: „Wenn Banken die Erlaubnis zur Datenauswertung erbitten und damit spürbare Vorteile versprechen, sind die Kunden in der Regel bereit, ihrem Geldinstitut relevante Daten bereitzustellen.“

Doch worin könnten diese Vorteile für den Kunden bestehen? Zum einen kann das die Vereinfachung von Bankgeschäften sein, wenn etwa Kontaktdaten freigegeben werden, um die Eingabe von IBAN zu ersparen, zum anderen können unmittelbare Dienstleistungen dazugehören, wie der Filial- und Geldautomatensucher auf Basis der eigenen Standortdaten. Knapp die Hälfte der Kunden ist laut BLC bereit, für solche Mehrwerte die eigenen Daten preiszugeben. Vier von zehn Kunden geben bereitwillig ihre Daten her, um persönlich zugeschnittene Angebote zu erhalten. „Mehrwertdienste und Werbeansprache lassen sich gut kombinieren“, rät Nitschke. „Hat etwa der Kunde sowohl die Standortbestimmung als auch den direkten Kontakt gestattet, so können Bankberater ihn zu Kaffee und Beratung einladen, wenn er in Filialnähe ist - am besten mit einem kundenbezogenen Anlass und einem Dankeschön.“

Generell sei die Bereitschaft zur Datenverwertung bei jüngeren Kunden stärker ausgeprägt: Bei den unter 40-Jährigen erlauben 51 Prozent persönlich zugeschnittene Angebote, bei den Kunden ab 50 Jahren sind es nur 36 Prozent. Ähnlich verhält es sich mit den Zustimmungsraten zur Datenfreigabe für die Vereinfachung von Bankgeschäften. Einer überwältigen Mehrheit der Kunden ist es aber wichtig, dass die Daten nur mit ihrer Erlaubnis für digitale Dienstleistungen verwendet werden. Bei der Auswertung von Kontobewegungen etwa sehen 96 Prozent der Bankkunden eine vorherige Erlaubnis als erforderlich an. In vielen Fällen haben die Banken ihre Kunden aber noch gar nicht nach dem Einverständnis für die Datenauswertung und Ansprache gebeten. Zurückhaltung hält Nitschke auch in diesem Punkt für falsch. Den Banken käme dabei ein weit verbreitetes Missverständnis bei Kunden zugute: Viele gingen davon aus, dass ihre Kontobewegungen ohnehin schon regelmäßig für Werbezwecke analysiert würden; immerhin 56 Prozent der Bankkunden glauben, dass ihre Daten entweder automatisch oder individuell durch ihren Bankberater ausgewertet werden. Eine solche Praxis ist jedoch verboten, sofern der Kunde nicht ausdrücklich zugestimmt hat.

AUS UNSERER MARKENWELT

Bankenverband macht Weg frei für Privatisierung der HSH Nordbank

Der Bundesverband deutscher Banken (BdB) hat eine Lösung im Streit um die HSH Nordbank erreicht. Der BdB habe sich nach intensiven Verhandlungen mit allen Beteiligten auf einen Übergang der HSH vom öffentlich-rechtlichen in den privaten Einlagensicherungsfonds geeinigt, sagte BdB-Präsident Hans-Walter Peters dem Handelsblatt. (...)

[Den vollständigen Text finden Sie hier.]

RISIKO MANAGER

Mehr unter: www.risiko-manager.com

Der schwierige Kampf der Banken gegen schmutziges Geld

Es sieht so aus, als sei alle paar Monate eine andere Bank in einen milliardenschweren Geldwäscheskandal verwickelt. Der jüngste Fall betrifft die Danske Bank, die offenbar mit schier unglaublicher Dreistigkeit 230 Mrd. US-Dollar an verdächtigen Geldbewegungen über ihre kleine Niederlassung fließen ließ. Die Banken zahlen ihre Strafe, versprechen Besserung, und der Skandal ist normalerweise vergessen.

Anleger sollten jedoch nicht den Fehler machen, die langfristigen Auswirkungen solcher Affären zu unterschätzen. Beim Kampf von Regierungen gegen eine ganze Reihe von Straftaten sind Banken mittlerweile zum Dreh- und Angelpunkt der Ermittlungen geworden. (...)

[Den vollständigen Text finden Sie hier.]

bank&compliance

Mehr unter: www.info-bank-compliance.de

Informationsfreiheitsgesetz – Rechtsmissbräuchliche Antragstellung

Anträge nach dem Informationsfreiheitsgesetz des Bundes (IFG) können wegen Unzulässigkeit abgelehnt werden, wenn sie rechtsmissbräuchlich gestellt sind.
Ein Rechtsmissbrauch kann vorliegen, wenn massenhaft identische Informationsanträge ohne jeden individuellen Bezug gestellt werden, die ausschließlich dem wirtschaftlichen Interesse der Verfahrensbevollmächtigten dienen, im Antrags- und anschließenden Gerichtsverfahren möglichst viele Anwaltsgebühren zu generieren.
(OVG Berlin-Brandenburg, Urt. v. 22.2.2018, Az. 12 B 16.17, WM 2018, S. 1174)

In dem die Entscheidung des OVG Berlin-Brandenburg zugrundeliegenden Fall hatte die Klägerin über ihre anwaltlichen Vertreter beim Bundesministerium der Finanzen in Bezug auf eine Wohnungsbaugesellschaft unter Berufung auf das Informationsfreiheitsgesetz eine schriftliche Auskunft zu insgesamt 24 Fragen sowie Akteneinsicht beantragt. Entsprechende Anträge hatten die anwaltlichen Vertreter der Klägerin zeitgleich für mehr als 500 weitere geschädigte Anleger der Wohnungsbaugesellschaft gestellt. Nachdem die Beklagte dem Auskunftsbegehren nur teilweise entsprochen hatte, hatten die anwaltlichen Vertreter der Klägerin Untätigkeitsklage erhoben, in der sie die bei der Behörde gestellten Informationsanträge weiter verfolgten. Parallel hierzu hatten die anwaltlichen Vertreter der Klägerin im Wesentlichen identische Informationsbegehren an die Bundesanstalt für Finanzdienstleistungsaufsicht gerichtet und anschließend auch hierzu zahlreiche Einzelklagen beim Verwaltungsgericht Frankfurt a. M. erhoben. (...)

[Den vollständigen Text finden Sie hier.]

BuB Alles, was Bankrecht ist.

Mehr unter: www.info-bub.de

UNSERE NÄCHSTEN VERANSTALTUNGEN AUF EINEN BLICK

TITEL	TERMIN	ORT
Zertifikatslehrgang „Informationssicherheitsbeauftragte (ISB) für Kreditinstitute“	6. bis 9. November 2018	Köln
Intensivseminar „Insolvenzrecht in der Bankpraxis: Update und Ausblick“	7. November 2018	Frankfurt am Main
RepRisk Forum 2018	15. November 2018	Köln
Fachtagung „FinTechs, Legal Techs und Bankrecht“	21. November 2018	Köln
Intensivseminar „Embargo und Finanzsanktionen in der aktuellen Bankpraxis“	22. November 2018	Köln
Fachtagung „Informationssicherheits-Compliance 2018“	27. November 2018	Köln
Fachtagung Bankrecht und Bankpraxis „Kollektiver Verbraucherrechtsschutz – konkrete Auswirkungen für die Finanzdienstleistungsbranche“	29. November 2018	Köln
Fachtagung „Compliance 2019“	7. Februar 2019	Köln
Fachkonferenz „Zahlungsverkehr der Zukunft 2019“	20. Februar 2019	Köln

WEITERE INFORMATIONEN UND ANMELDUNG

Stefan Lödorf
Telefon: 0221/5490-133
E-Mail: events@bank-verlag.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),
Michael Eichler,
Matthias Strobel

Bereichsleitung Medien:
Bernd Tretow

Mediaberatung:
Katrin Frese
Tel. 0221/54 90-327
E-Mail: katrin.frese@bank-verlag.de

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

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

Erscheinungsweise: mindestens 1 x pro Monat