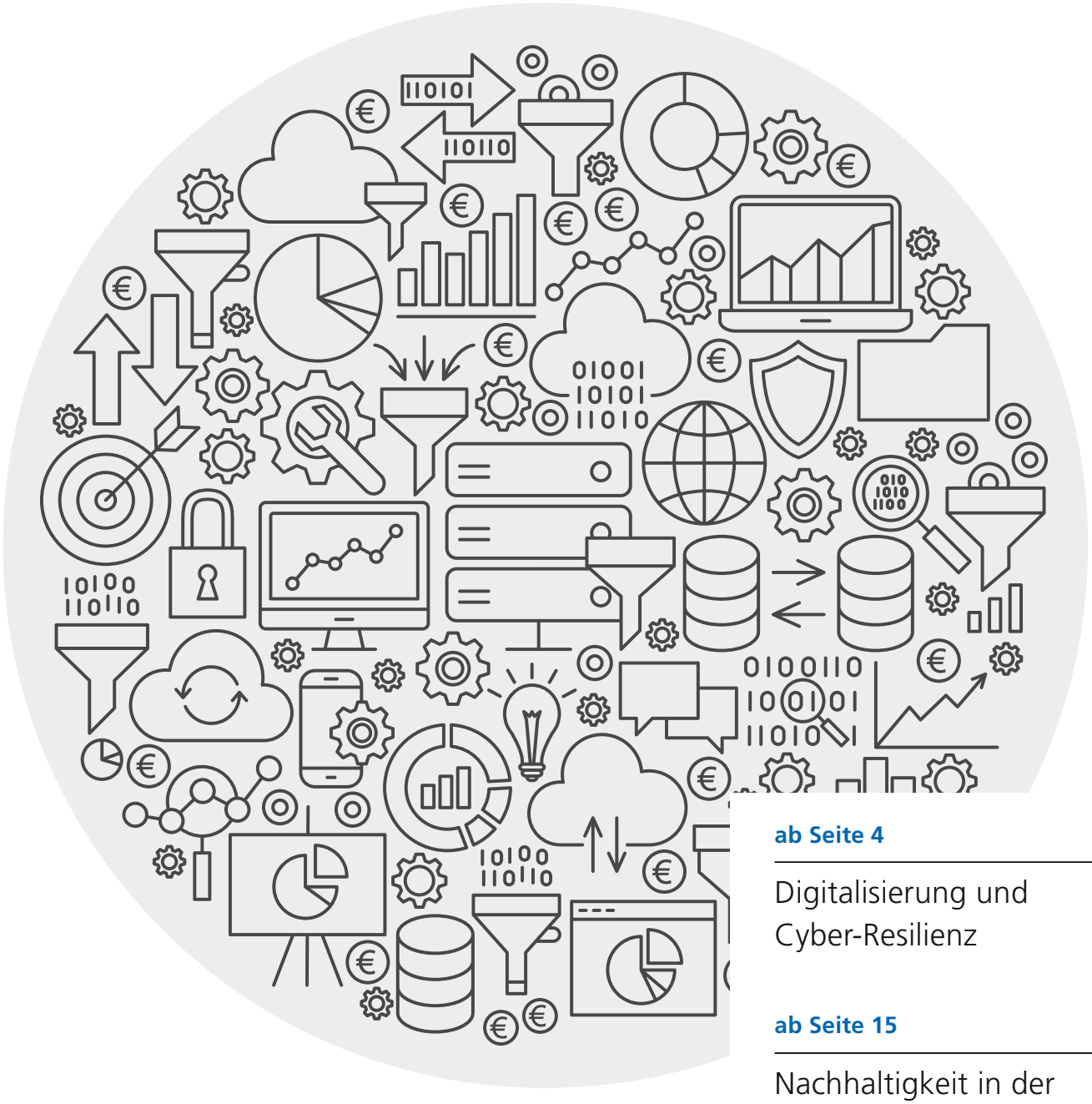
DZ CompliancePartner

Point of Compliance

Das Risikomanagement-Magazin für unsere Kunden und Geschäftspartner

AUSGABE 3/2019



Digitalisierung und Klimawandel

sind in der aufsichtsrechtlichen Praxis angekommen. „Cyber-Resilienz", die Widerstandsfähigkeit von Unternehmen gegen Angriffe auf die Daten- und Informationssicherheit, rückt immer mehr in den aufsichtsrechtlichen Fokus (S. 4) und auch „Nachhaltigkeitsrisiken" werden zum Ende dieses Jahres namentlich und voraussichtlich umfassend Eingang in die MaRisk finden (S. 15). Beide Themen werden Auswirkungen auf Ihr Institut haben.

Jens Saenger
Sprecher der Geschäftsführung

Ist das gut? Auf den ersten Blick nicht, weil damit auf operativer Ebene ganz neue Anforderungen verbunden sind, die zum Teil auch einen erheblichen Mehraufwand bedeuten.

Andererseits wird erstmals ein aufsichtsrechtlicher Orientierungsrahmen zu den Megathemen Digitalisierung und Klimawandel gesetzt. Die Bank kann innerhalb dieses Rahmens ihre diesbezüglichen Risiken sicher(er) identifizieren, benennen und steuern. Und, wenn man so will, gewinnt sie unternehmerische Freiheit (zurück), um ihr Geschäftsmodell vor dem Hintergrund der Digitalisierung und des Klimawandels weiterzuentwickeln.

Ob die Entwicklung nun als schlecht oder gut zu bewerten ist: Die Themen sind so oder so gesetzt, alles ist im Fluss. Wir, als Ihr Spezialist im Beauftragtenwesen, als Ihr Beauftragter, haben die Anforderungen schlicht umzusetzen. Dies werden wir sicher, kunden- und praxisorientiert zusammen mit Ihnen angehen. Die gute Nachricht ist: Über den gemeinsamen Antritt, den Mehrmandantenansatz, können und werden wir dies ressourcenschonend realisieren. Das mag ich schon heute versprechen. In diesem Sinne stehen wir Ihnen, auch und insbesondere in Bezug auf die anstehenden Herausforderungen, mit unseren Erfahrungen, unserem Know-how und vor allem auch mit abgesicherten und abgestimmten Prozessen zur Seite.

Ich wünsche eine spannende Lektüre,

Ihr Jens Saenger

Daten- und Informationsmanagement

Das Gold einer di

Daten, ganz gleich ob mit oder ohne Personenbezug, sind das unverzichtbare Fundament der Digitalisierung von Big Data, Cloud-Computing, Facebook und Co. Ob als Firma, Beauftragter oder Privatperson: Das Sammeln, Auswerten, Nutzen von Daten und Informationen wird immer verlockender und einfacher. Der Schutz sowie der verantwortungsbewusste Umgang hatten mit dieser Entwicklung leider nicht in gleichem Maße Schritt.

Verfolgt man die öffentliche Berichterstattung, rücken sowohl der Umgang mit personenbezogenen Daten wie auch ihr Schutz immer mehr ins Blickfeld. Der Gesetzgeber hat hierfür seit über einem Jahr eine neue Verordnung mit dem vielsagenden Namen „Datenschutz-Grundverordnung" ins Leben gerufen.

Was im Sinne der Sache gut gemeint ist, kommt jedoch längst nicht bei jedermann gut an. Bei unseren Nachbarn in Österreich hat es das Wort Datenschutz-Grundverordnung (DSGVO) sogar zum Unwort des Jahres 2018 geschafft. Begründung: „Dieses Wortungetüm steht für die an sich wichtige Zielsetzung des Schutzes der privaten elektronischen Daten. Seine überaus komplizierte und mit hohem bürokratischen Aufwand verbundene Umsetzung – in Kombination mit der Tatsache, dass die großen internationalen Akteure im Umgang mit Daten von den Regelungen kaum betroffen sind – macht die Sache zu einer Perversion des gut gemeinten Vorhabens und den Begriff damit zu einem Unwort." Demnach wären die Vorgaben der DSGVO kompliziert, deren Umsetzung mit hohem bürokratischem Aufwand verbunden, die Regelungen teilweise nicht relevant (gerade für internationale Akteure) und somit das eigentlich positive Ziel eines wirksamen Datenschutzes pervertiert.

Aber: Selbst wenn uns die Umsetzung so mancher Vorgabe Kopfschmerzen bereitet und uns entsprechend fluchen lässt: Wie sieht die Realität ein Jahr nach Inkrafttreten der DSGVO aus? Wer ist für die operative Umsetzung zum Schutz der Daten verantwortlich? Und wird die der Umsetzung zugrunde liegende Grundhaltung den Zielen des Schutzes von Daten gerecht? Kann auf so einer Grundlage ein effektiver und ernst gemeinter Schutz von Daten stattfinden?

Fluch und Segen

Es lohnt sich, an dieser Stelle einmal kurz innezuhalten und darüber nachzudenken, worum es hier eigentlich geht.

Daten und Informationen sind das Gold des digitalen Zeitalters. Sie sind der Schmierstoff gut laufender Geschäftsmodelle. Korrekte Daten sind der Garant für Zuverlässigkeit und geschäftliche Erfolge. Sowohl kleine Fintechs wie auch große Konzerne sind hinter den Daten von Kunden her wie der Teufel hinter der armen Seele. Daher ist der Schutz von Daten eigentlich das Synonym für das Recht des Einzelnen auf informelle Selbstbestimmung.

Der Schutz von Daten und Informationen bei juristischen Personen ist heute mehr denn je im Zusammenhang mit ihrer korrekten und jederzeitigen Verfügbarkeit sowie der Verhinderung ihrer unlauteren Erlangung zu sehen. Dargelegt sind solche Szenarien in diversen Gesetzen. Bei sogenannten „kritischen Infrastrukturen" des öffentlichen Interesses sind zudem Aufsichtsbehörden und Staaten als „Gatekeeper" aktiv oder treten mittelbar in Erscheinung. Denn schlussendlich kann das Wohl einer ganzen Firma, ihrer Kunden und Mitarbeiter oder aber einer ganzen Bevölkerungsschicht (oder alternativ: eines Staates) gefährdet sein: Wenn Daten missbraucht werden, sie urplötzlich und unwiderruflich nicht mehr für Entscheidungsfindungen zur Verfügung stehen oder ggf. falsch verknüpft werden und in der Folge unzutreffende Analysen mit verhängnisvollen Entscheidungen getroffen werden.

gitalen Welt

Datenschutz bei natürlichen Personen ist sogar im Grundgesetz verankert. Der Schutz unserer Daten ist ein Grundrecht, auf dessen Einhaltung wir alle beharren können, sollen und im Zeitalter fortschreitender Digitalisierungen sogar müssen.

Mehr als ein Kostenfaktor

Warum wird der sich auf den Datenschutz beziehende Aufwand als so bürokratisch und realitätsfern beschrieben? Warum müssen sich Firmen bzw. Datenschützer und Informationssicherheitsbeauftragte für ihre Tätigkeit oder ihren angemessenen Aufwand rechtfertigen?

Liegt es vielleicht daran, dass noch immer kein angemessenes Maß für eine akzeptierte „Best Practice" gefunden wurde? Oder ist es einfach fehlende Konsequenz, dass der Schutz der Daten von vielen Firmen zwar einerseits als in höchstem Maße wichtig und sogar als verkaufsförderndes Marketinginstrument angesehen wird, andererseits aber in der Umsetzungsrealität kaum Beachtung findet, weil der Aufwand schlichtweg als zu teuer und bisweilen unnötig angesehen wird?

Das Ziel von Informationssicherheit und Datenschutz in seiner aktuellen Form ist, den Nachweis tatsächlich wirksamer Maßnahmen zu initiieren. Der Gesetzgeber bzw. die Aufsicht will nachvollziehen können, dass angemessene und wirksame Maßnahmen getroffen wurden. Das ist vor dem Hintergrund der faktischen Risiken und gemachten Erfahrungen nachvollziehbar und durchaus legitim.

Jeder Bürger, dessen Identität oder dessen Bankkonto schon einmal in betrügerischer Weise missbraucht wurde, weiß um die Notwendigkeit wirksamer Schutzmechanismen. Jede Firma, die aufgrund falscher, unvollständiger oder vielleicht sogar gestohlener Daten einen unternehmerischen Schaden hat erleiden müssen, kann den betriebswirtschaftlichen Wert eindeutig beziffern. Somit ist der Schutz von Daten gerade nicht der so oft kolportierte Hemmschuh des Fortschritts digitaler Entwicklungen, sondern im Gegenteil: Er ist die Voraussetzung für einen nachhaltigen digitalen Fortschritt. Ohne wirksamen Schutz von Daten und Informationen in einer Firma kein Vertrauen, ohne Vertrauen in diese Firma kein Geschäft.

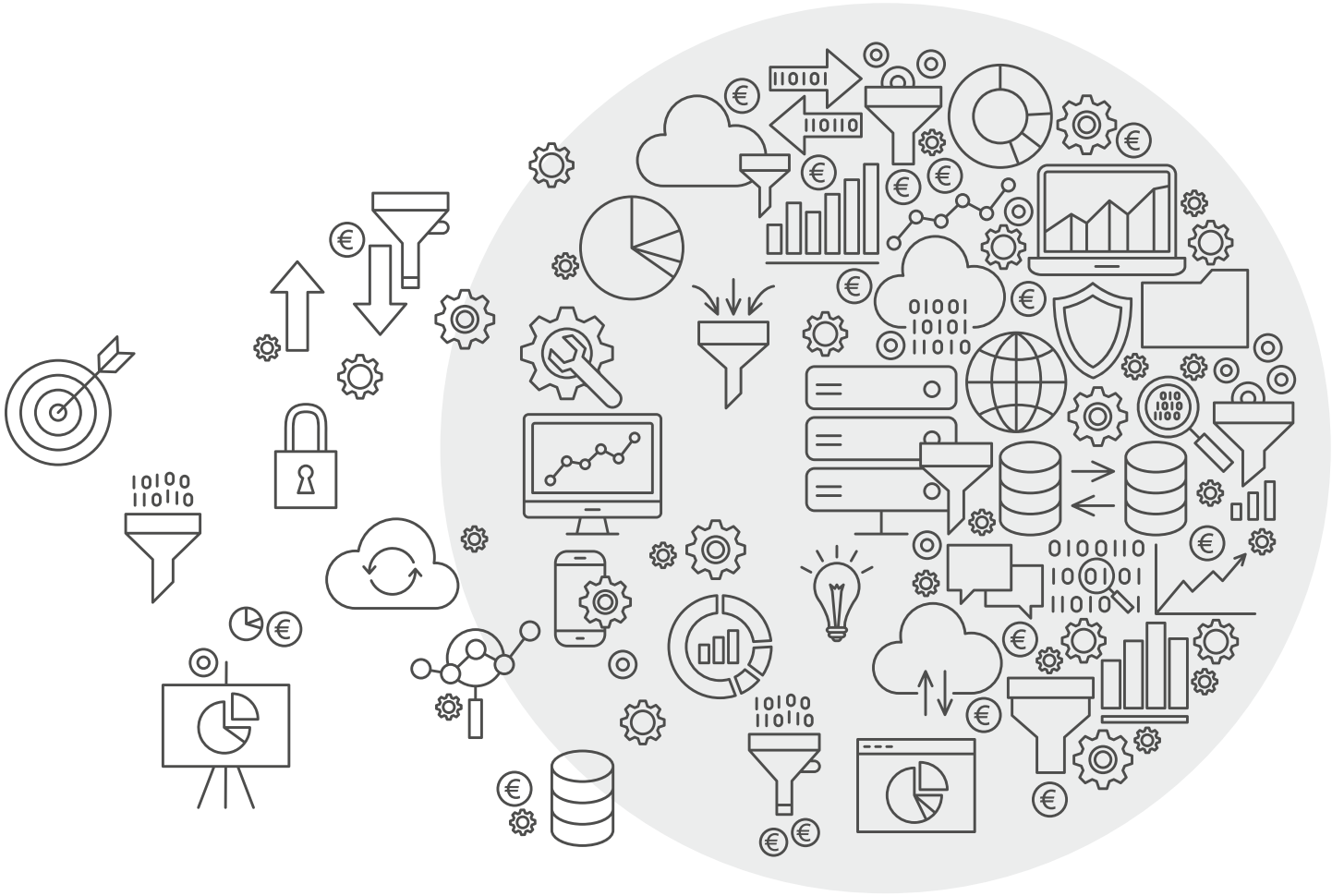
Und gerade deshalb ist es eine große Herausforderung für Beauftragte in ihrer Rolle als Schützer von Informationen und Daten, die Aufwände für diese Aufgaben zu erklären. Sie sind eben nicht als reiner Kostenfaktor zu betrachten. Sie sind vielmehr elementarer Bestandteil erfolgreicher Geschäftsmodelle und als solche glaubwürdig zu integrieren. Immerhin gilt es, wichtige Geschäftsgeheimnisse und den Geschäftsbetrieb der Firma und das Grundrecht der Kunden der Firma gleichermaßen zu schützen. Dies gelingt nur, wenn eine transparente, belastbare Verbindung zwischen regulatorisch und gesetzlich relevanten Informationen und Datenhaushalten, dem entsprechend konformen Umgang damit und den zu ihrer Nutzung vorgesehenen Geschäftsprozessen und Systemen hergestellt werden kann.

Wirksame Daten- und Informationssicherheit

Voraussetzung ist eine Detailtiefe in Bezug auf Abläufe und Prozesse, die schon im Stellenprofil der Beauftragten verankert sein muss. Eine ausschließlich theoretische Betrachtungsweise gesetzlicher Vorgaben wird nur bedingten operativen Erfolg haben. Eine gewisse Begeisterung für die Inhalte und Ziele des Datenschutzes und der Informationssicherheit erhöht die Chancen für pragmatische und zugleich effiziente Lösungen dagegen ungemein. Dies ist im Übrigen auch ein Argument dafür, auf externe Unterstützung zurückzugreifen: Für externe Beauftragte ist der Schutz von Informationen und Daten absolutes Kerngeschäft. Sie machen bei vielen verschiedenen Mandanten nichts anderes und bauen somit ein Qualifikationsprofil auf, das den hohen aufsichtsrechtlichen und gesetzlichen Anforderungen entspricht. Sie „brennen" erfahrungsgemäß auch für ihr Thema. Das kann insbesondere für kleinere und mittlere Häuser interessant werden. Sie verschaffen sich somit einen betriebswirtschaftlich optimierten Zugang zu fachlicher und prozessualer Intelligenz und damit zu einem wirksam(er)en Schutz.

Eine weitere Voraussetzung für eine wirksame Daten- und Informationssicherheit liegt in einem integrativen Ansatz.

Grundlage für die geschäftlichen Operationen der Finanzdienstleistungsbranche ist seit jeher das, was heute die „Schätze des digitalen Zeitalters" sind: die Informationen und Daten >



zu ihren Kunden. Aktualität, Korrektheit, jederzeitige Verfügbarkeit und Schutz gegen „Angriffe“ von außen sind von nachhaltiger Bedeutung, denn:

- Geschäftsmodelle sind nur mit korrekten Daten wirklich erfolgreich.
- Kunden bekommen nur auf Basis korrekter Analysen individuelle und bestmögliche Lösungen angeboten.
- Vertrauen ist das Kernkapital einer gesunden Kunde-Bank-Beziehung: Ein sorgsamer Umgang mit Daten gehört deshalb zu den ersten Pflichten.

Eine der Kernaufgaben des modernen Beauftragtenwesens ist die Absicht, diese vorgenannten Zielsetzungen durch eine nachhaltige Aufgabenerledigung zu erreichen.

Vor dem Hintergrund, dass Daten- und Informationssicherheit heute – ohne Zweifel – elementar für die Bankenbranche ist, ist es nur schwer nachvollziehbar, dass sich Datenschutz- oder Informationssicherheitsbeauftragte für ihre Initiativen und Aufwände rechtfertigen müssen, weil diese den geschäftlichen Erfolg schmälern könnten. Oder anders formuliert: Es ist schlicht kontraproduktiv, wenn immer noch – insbesondere digitale – Geschäftsmodelle ohne die Integration regulatorischer Zielvorgaben gedacht werden und die Regulatorik als „Feindbild“ geschäftlicher Opportunitäten betrachtet wird. Geschäftsmodelle und die Ziele von Regulatorik dürfen sich nicht gegenseitig ausschließen, sondern sind idealerweise als Einheit zu betrachten.

AUTOR UND ANSPRECHPARTNER

Andreas Marbeiter
Geschäftsführung,
E-Mail: andreas.marbeiter@dz-cp.de

Das bedingt, dass die Zielsetzungen der jeweiligen Geschäftsmodelle einerseits und der Regulatorik andererseits pragmatisch und integrativ aufbereitet werden. Dies an sich ist schon eine sehr herausfordernde eigene Exzellenz, die – unter anderem – der Beauftragte ins Unternehmen einbringen muss.
Der Beauftragte benötigt dazu

- fundierte Kenntnisse der rechtlichen Rahmenbedingungen und dessen, was möglich ist,
- professionelle Erfahrung in Bezug auf relevante Arbeitsabläufe im Unternehmen,
- eine nachhaltige Expertise in Bezug auf prozessuale Ausgestaltungen sowie
- eine klare Lösungsorientierung.

Idealerweise liefert ihm die Organisation, in der er arbeitet, entsprechend unterstützende Rahmenbedingungen. Ohne diese Grundvoraussetzungen wird es schwierig, einen finanziell lohnenden Trade-off zwischen dem Aufwand der Regulatorik und dem Erfolg von Geschäftsmodellen zu gestalten.

Beauftragtentätigkeit als Erfolgsfaktor

Als Mehrmandantendienstleister optimiert die DZ CompliancePartner fortlaufend ihre Unterstützungsleistung

- mit Blick auf neue regulatorische Anforderungen (Stichwort DSGVO, BAIT etc.), aber auch
- hinsichtlich gesellschaftspolitischer Anforderungen, insbesondere der Digitalisierung, und
- der betriebswirtschaftlichen, bankenindividuellen Anforderungen (Stichwort Prozessintelligenz, Lernkurveneffekte, Kosten-Nutzen-Balance etc.).

Auch für uns ist dies ein Prozess, der langfristig angelegt und auch nicht ohne Rückschläge ist.

Als Ihr Beauftragter verstehen wir uns als Sparringspartner, wenn es darum geht, Ihr Geschäftsmodell für die digitalen und aufsichtsrechtlichen Herausforderungen abzusichern und auch fit zu machen. Wir wollen Ihnen

- aufsichtlich akzeptierte Vorgehensmodelle zur Gestaltung des Beauftragtenwesens bieten,
- Zugang zu der gesammelten Expertise und idealen Lösungen in der Genossenschaftlichen FinanzGruppe durch optimales Wissensmanagement verschaffen,
- ein Team von Kolleginnen und Kollegen zur Verfügung stellen, die sich für die Umsetzung dieser Aufgaben begeistern.

Schlussendlich können wir als Mehrmandantendienstleister dem Mehraufwand Prozessintelligenz entgegensetzen. Standardisierung und Automatisierung sorgen nicht nur für Transparenz und Sicherheit in der Funktion, sondern auch in der betriebswirtschaftlichen Steuerung. Ihnen steht ein gleichermaßen angemessenes wie wirksames Vorgehen zur Verfügung, das die nötigen Aufwände an den tatsächlichen Erfordernissen ausrichtet. Die Eintrittswahrscheinlichkeit für sanktionierbares Fehlverhalten kann deutlich reduziert werden.

Datenschutz und Informationssicherheit sind zur Zeit einer der regulatorischen Kernthemen, der alle Marktteilnehmer, Unternehmen ebenso wie Kunden, beschäftigt und auch weiterhin beschäftigen wird. Organisatorisch und strukturell richten wir aktuell unseren Fachbereich auf genau diese Anforderungen aus, um unsere Dienstleistungen im Sinne unserer Kunden auch zukünftig erfolgreich zu gestalten.

Die DZ CompliancePartner unterstützt diese Prozesse bereits inhaltlich für die von ihr selbst angebotenen Auslagerungsdienstleistungen. Ferner stellen wir auch Arbeitsmittel für das Auslagerungsmanagement zur Verfügung, damit Ihr Haus das Auslagerungsmanagement in dem geforderten Umfang und betriebswirtschaftlich sinnvoll erfüllen kann. ▬

4. EU-Geldwäscherichtlinie

Regierungsentwurf zur Umsetzung der Änderungsrichtlinie

Das Bundeskabinett hat am 31. Juli 2019 den Entwurf eines Gesetzes zur Umsetzung der Änderungsrichtlinie zur 4. EU-Geldwäscherichtlinie [Richtlinie (EU) 2018/843] beschlossen. Das Gesetz soll zum 1. Januar 2020 in Kraft treten.

Das Gesetz soll in erster Linie das Geldwäschegesetz (GwG) ändern. Die neuen Regelungen sehen insbesondere vor:

- die Erweiterung des geldwäscherechtlichen Verpflichtetenkreises, insbesondere im Bereich virtueller Währungen,
- die Erweiterung der Anwendungsfälle verstärkter Sorgfaltspflichten bei Hochrisikoländern,
- die Konkretisierung des Personenkreises „politisch exponierte Personen“ (PEP) durch Listen der Mitgliedsstaaten und der Europäischen Kommission zu Funktionen bzw. Ämtern,
- den öffentlichen Zugang zum elektronischen Transparenzregister sowie die Vernetzung der europäischen Transparenzregister.

Erweiterung des Verpflichtetenkreises, insbesondere im Bereich virtueller Währungen

Der Anwendungsbereich des GwG wird um einige Verpflichtete erweitert, so dass diese Berufsgruppen erstmalig nach geldwäscherechtlichen Maßstäben ein Risikomanagement einrichten, Sorgfaltspflichten erfüllen und Verdachtsmeldungen abgeben müssen.

Aus dem Finanzsektor sind dies:

- Anbieter von elektronischen Geldbörsen (sogenannte „Wallet Provider“), mit denen virtuelle Währungen (z. B. „Bitcoin“) verwahrt werden
- Umtauschplattformen: Dienstleister, die gesetzliche Zahlungsmittel in virtuelle Währungen und umgekehrt tauschen bzw. die den Tausch virtueller Währungen untereinander anbieten
- Zahlungs- und E-Geld-Institute mit Sitz im Ausland, die im Inland über Vertriebshelfer („Agenten“) tätig werden

Aus dem Nichtfinanzsektor:

- Immobilienmakler nun auch bei der Vermittlung von Mietverträgen, wenn die monatliche Miete oder Pacht mindestens 10.000 EUR beträgt
- Neben den nach der bisherigen Regelung verpflichteten Wirtschaftsprüfern, vereidigten Buchprüfern, Steuerberatern und Steuerbevollmächtigten unterliegen zukünftig alle Dienstleister in Steuerangelegenheiten geldwäscherechtlichen Pflichten, soweit sie als wesentliche geschäftliche Tätigkeit Hilfe in Steuerangelegenheiten leisten (insbesondere Lohnsteuerhilfevereine nach § 4 Nummer 11 des Steuerberatungsgesetzes)
- Im Kunstsektor über Kunsthändler und -vermittler hinaus zukünftig auch Lagerer von Kunst (nur in Zollfreigebieten) ab einem Transaktionswert von 10.000 EUR

Erweiterung der Anwendungsfälle verstärkter Sorgfaltspflichten bei Hochrisikoländern

Der Gesetzentwurf definiert zusätzlich ein höheres Risiko, wenn es sich um eine Geschäftsbeziehung oder Transaktion handelt, an der ein von der Europäischen Kommission ermittelter Drittstaat mit hohem Risiko oder eine in diesem Drittstaat ansässige natürliche oder juristische Person beteiligt ist. In diesen Fällen haben die Verpflichteten nun einen fest definierten Katalog von verstärkten Sorgfaltspflichten zu erfüllen.

AUTOR UND ANSPRECHPARTNER

Norbert Schäfer
Geschäftsführung,
E-Mail: norbert.schaefer@dz-cp.de

Darüber hinaus wurde im Rahmen der Nationalen Risikoanalyse „Bekämpfung von Geldwäsche und Terrorismusfinanzierung“ (NRA) Versteigerungen ein erhöhtes Geldwäscherisiko zugeschrieben. Der Gesetzentwurf sieht daher vor, Versteigerungen durch die öffentliche Hand geldwäscherechtlichen Pflichten zu unterwerfen.

Für Korrespondenzbankbeziehungen innerhalb des Europäischen Wirtschaftsraums (EWR) sieht der Gesetzentwurf künftig auch bei grenzüberschreitenden Korrespondenzbankbeziehungen innerhalb des EWR verstärkte Sorgfaltspflichten vor, sofern die Beurteilung des Verpflichteten zu dem Ergebnis führt, dass hiermit ein höheres Risiko verbunden ist.

Daneben sollen die Faktoren für ein potenziell höheres Risiko (Anlage 2 zum GwG) erweitert werden um Transaktionen in Bezug auf Öl, Waffen, Edelmetalle, Tabakerzeugnisse, Kulturgüter und andere Artikel von archäologischer, historischer, kultureller oder religiöser Bedeutung oder von außergewöhnlichem wissenschaftlichen Wert sowie Elfenbein und geschützte Arten.

Schließlich soll der Schwellenbetrag, ab dem Güterhändler geldwäscherechtlichen Pflichten unterliegen, als Ergebnis der NRA in Bezug auf den Edelmetallhandel von 10.000 EUR auf 2.000 EUR abgesenkt werden.

Konkretisierung des Personenkreises „politisch exponierte Personen“ (PEP) durch Listen der Mitgliedsstaaten und der Europäischen Kommission zu Funktionen bzw. Ämtern

Die Mitgliedsstaaten haben der EU-Kommission bis zum 10. Januar 2020 Listen mit konkreten Ämtern, die den PEP-Status begründen, vorzulegen. Die EU-Kommission erstellt daraus eine gemeinsame Liste, auf die künftig im GwG verwiesen werden soll. Die Liste für Deutschland soll begleitend zum Gesetzgebungsverfahren erstellt werden.

Zugang zum elektronischen Transparenzregister sowie Vernetzung der europäischen Transparenzregister

Das Transparenzregister wird künftig für die „Öffentlichkeit“ zugänglich sein. Weitere Änderungen in Bezug auf das Transparenzregister sind die verpflichtende Meldung von festgestellten Unstimmigkeiten durch Verpflichtete und Behörden sowie die Beibringung eines Registrierungsnachweises oder Registerauszuges bei Begründung einer neuen Geschäftsbeziehung mit mitteilungspflichtigen Unternehmen. Daneben ist ein europäisches System der Registervernetzung vorgesehen.

Sonstige Neuregelungen von Bedeutung

Bei Personen, die als **wirtschaftlich Berechtigte** gelten, sollen zudem die Maßnahmen zur Überprüfung der Identität und etwaige Schwierigkeiten, die während des Überprüfungsvorgangs aufgetreten sind, aufgezeichnet werden.

Aufzeichnungen und sonstige Belege sollen zukünftig mindestens fünf Jahre aufbewahrt und spätestens nach zehn Jahren vernichtet werden.

Für die **Verarbeitung personenbezogener Daten** durch Verpflichtete sieht der Gesetzentwurf eine Klarstellung vor, dass Verpflichtete personenbezogene Daten in Erfüllung ihrer Sorgfalts- und Meldepflichten auf Grundlage dieses Gesetzes ausschließlich für Zwecke der Verhinderung von Geldwäsche und Terrorismusfinanzierung verarbeiten dürfen. >

Der Gesetzentwurf sieht eine Stärkung der **Befugnisse der Zentralstelle für Finanztransaktionsuntersuchungen (FIU)** dahingehend vor, dass die FIU bei automatisiertem Datenabgleich mit der gemeinsamen Datenbank der Polizeien (INPOL Bund) von Treffern im Bereich besonders geschützter Daten (beispielsweise organisierte Kriminalität, Staatsschutz) Kenntnis erhält und dass die FIU zukünftig über einen Zugriff auf das Zentrale Staatsanwaltschaftliche Verfahrensregister (ZStV) auch Zugang zu strafrechtlich relevanten Informationen der Bundesländer haben soll.

Die bisherige Regelung des GwG zur **Privilegierung freier Berufe** in Bezug auf die Verdachtsmeldepflicht soll stärker an die Formulierung der Richtlinienvorgaben angeglichen werden (Privilegierung bei Tätigkeiten der Rechtsberatung und Prozessvertretung). Der Gesetzentwurf sieht darüber hinaus die Erweiterung der **Verdachtsmeldepflicht freier Berufe bei Immobilientransaktionen** (Erwerbsvorgänge nach Grunderwerbssteuergesetz) vor, die angesichts des bestehenden hohen Geldwäscherisikos im Immobiliensektor und der geringen Zahl der Verdachtsmeldungen von Notaren geboten ist.

Die in dem Anschreiben des Bundesministeriums der Finanzen zur Verbändekonsultation zum Referentenentwurf vom 20. Mai 2019 angekündigte **Ergänzung des Strafgesetzbuchs** (StGB), wonach der Abgabe einer Verdachtsmeldung nach § 43 GwG auch die strafbefreiende Wirkung nach § 261 Absatz 9 StGB zukommen soll, hat auch im Wortlaut des nun vorliegenden Regierungsentwurfs leider keinen Niederschlag gefunden.

Steht die Person, die eine Meldung nach § 43 Absatz 1 GwG abgegeben hat oder die dem Verpflichteten intern einen solchen Sachverhalt gemeldet hat, in einem Beschäftigungsverhältnis zum Verpflichteten, so darf ihr aus der Meldung **keine Benachteiligung im Beschäftigungsverhältnis** entstehen. Der Gesetzentwurf sieht vor, dass Beschäftigte berechtigt sind, bei der Aufsichtsbehörde Beschwerde zu erheben, wenn sie sich im Zusammenhang mit ihrem Beschäftigungsverhältnis aufgrund der Abgabe einer Meldung benachteiligt fühlen.

Der Gesetzentwurf sieht die Aufnahme zahlreicher weiterer **Bußgeldtatbestände** in das GwG vor. Der Verschuldungsgrad für die Bußgeldbewehrungen wurde nicht, wie noch im Referentenentwurf vorgesehen, auf „fahrlässig“ herabgesetzt. Somit muss nach wie vor ein Bußgeldtatbestand entweder vorsätzlich oder zumindest leichtfertig verwirklicht werden, um entsprechende Sanktionen gegen Verpflichtete oder deren Mitarbeiter zu begründen.

Schließlich enthält der Gesetzentwurf einen klarstellenden Hinweis, dass ein **Mitglied der Führungsebene** nicht in jedem Fall ein Mitglied der Leitungsebene sein muss.

Die DZ CompliancePartner wird das Gesetzgebungsverfahren weiter verfolgen und die von ihr angebotenen Dienstleistungen in der Geldwäsche- und Betrugsprävention an den neuen gesetzlichen Vorschriften ausrichten. ▬

Geldwäsche- und Betrugsprävention

Warum Vor-Ort-Kontrollen

Vor-Ort-Kontrollen erhöhen das Schutzniveau der Bank bedarfsorientiert bzw. themenspezifisch. Die Banken schätzen insbesondere die Möglichkeit, im persönlichen Gespräch detailliert und unmittelbar Fragen abschließend klären zu können.

Die DZ ComliancePartner bietet im Bereich der Geldwäsche- und Betrugsprävention eine breite Palette von maßgeschneiderten Lösungen an. Diese reichen von Coaching- und Beratungsleistungen über eine Teilauslagerung bis hin zur vollständigen Übernahme der Funktion des Geldwäschebeauftragten.

Mit all diesen Dienstleistungen verfolgen wir das Ziel, unsere Kunden – die Bank, den Vorstand, die Mitarbeiter und auch die Kunden der Bank – zu schützen. Dabei gibt es keine „one size fits all"-Lösung (siehe Tabelle Abb. 1).

Standardisierter Risikomanagement-Prozess

Ab dem Zeitpunkt der vollständigen Übernahme der Funktion des Geldwäschebeauftragten werden alle gesetzlichen Anforderungen zur Geldwäsche- und Betrugsprävention vollumfänglich durch die DZ CompliancePartner erfüllt. Sämtliche Prozesse wurden durch die langjährige enge Zusammenarbeit mit den Prüfungsverbänden und die umfangreiche Gremienarbeit fortlaufend optimiert. Dies wird nicht zuletzt durch die regelmäßigen Testate der Prüfungen nach PS 951 bestätigt.

Die Geldwäsche- und Betrugsprävention ist in das Compliance Management System (CMS) eingebunden und folgt dem dargestellten Risikomanagement-Prozess (Abb. 2, S. 12).

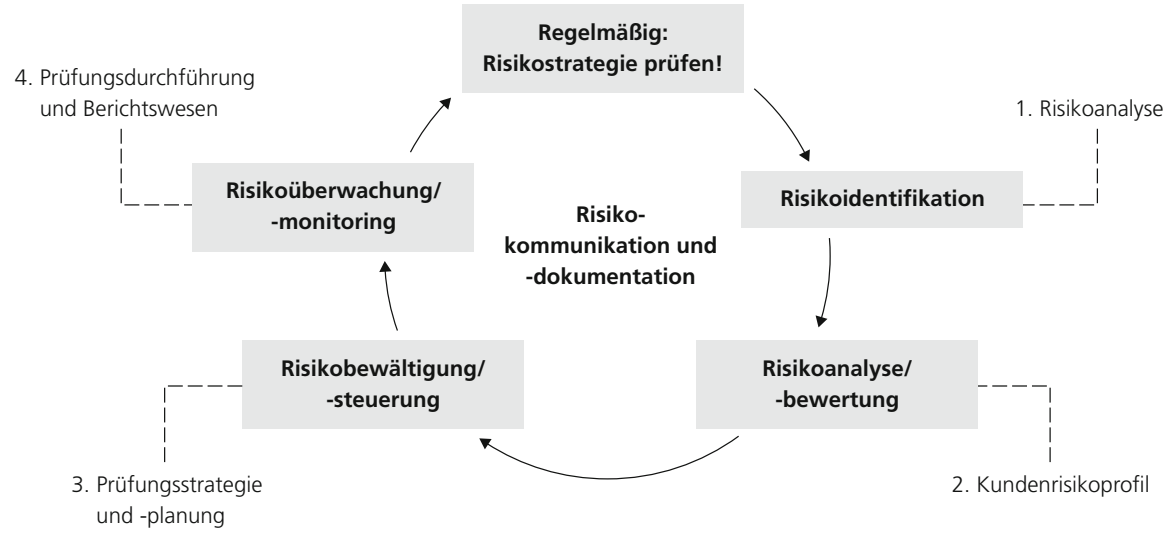
Auf Basis der individuellen Risikoanalyse wird zunächst ein Kontrollplan erstellt. Die Themen für den Kontrollplan ergeben sich zum einen aus der Risikoanalyse selbst. Jedes nicht geringe Risiko wird zwingend betrachtet. Zum anderen fließen unsere Erkenntnisse als Mehrmandantendienstleister ein. Die am häufigsten aufgetretenen Schadensfälle werden ebenso berücksichtigt wie neue oder ungewöhnliche Betrugs- oder Schadensmuster bzw. neue Typologien. Aus diesem Kontrollplan leiten sich schließlich die konkreten Kontrollmaßnahmen ab.

Neben dem Geldwäschebeauftragten steht der Bank auf Wunsch ein Team von Compliance-Spezialisten zur Verfügung. Diese kommen immer dann zum Einsatz, wenn das Schutzniveau einer Bank über das gesetzlich geforderte Maß hinaus erhöht werden soll. So entscheiden sich viele Banken, ihre Risiken – bedarfsorientiert und themenspezifisch – (unter anderem) durch Vor-Ort-Kontrollen abzusichern. >

1 GELDWÄSCHE- UND BETRUGSPRÄVENTION

	Auslagerung	Teilauslagerung	Coaching/ Beratung	Interims-Management	Werkzeug	WBT, Schulung
Geldwäsche-/Betrugsprävention	✔	✔	✔	✔	✗	✔

2 RISIKOMANAGEMENT-PROZESS



Erfahrungsberichte

An zwei Beispielen kann das konkrete Vorgehen skizziert werden.

Beispiel 1: Sprengung von Geldautomaten
In dem Bericht des Bundeskriminalamtes (BKA) „Bundeslagebild Angriffe auf Geldautomaten 2018“ wird von einem Anstieg der Fallzahlen von versuchten und vollendeten Sprengungen von Geldautomaten um 38 % berichtet. Folgende Statistik des BKA (Abb. 3) belegt die Gefährdungssituation eindrucksvoll: Teilweise waren von der DZ CompliancePartner betreute Banken selbst betroffen. Oder die Vorfälle ereigneten sich in unmittelbarer Nähe zu Filialen der Banken. Die Brisanz des Angriffs mit Explosivstoffen liegt darin, dass die ausgelöste Explosion in der Regel nicht kontrolliert abläuft. Dies bedeutet, dass neben dem eigentlichen Schaden am Geldautomaten mit einer erheblichen Schädigung des unmittelbaren und mittelbaren Umfeldes und auch Personenschäden gerechnet werden muss.

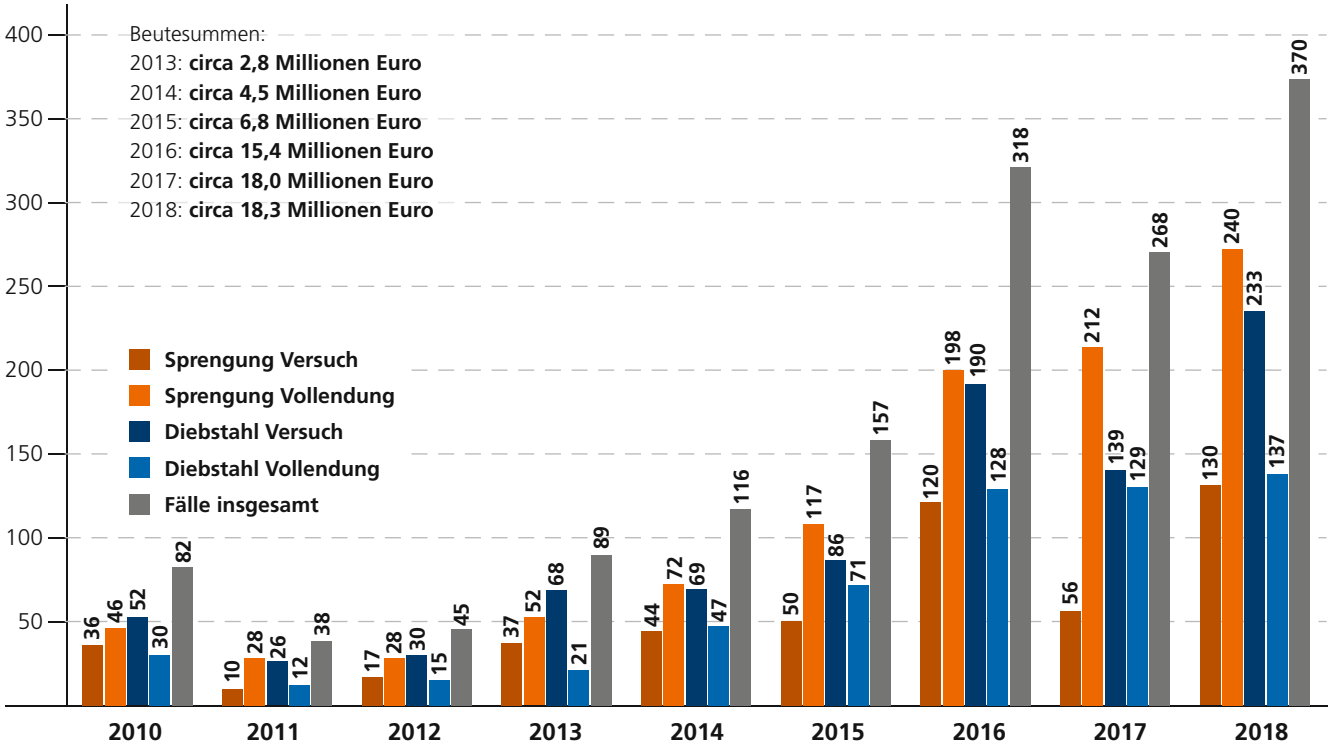
Ziel einer Vor-Ort-Kontrolle ist es, eine Beurteilung möglicher Gefährdungen hinsichtlich von Sprengungen sowie Entwendungen von Geldautomaten vorzunehmen und risikominimierende Maßnahmen festzulegen. Durch unsere Spezialisten werden dabei eine Vielzahl auf den ersten Blick vielleicht nicht unmittelbar geldwäscherelevanter Informationen und Unterlagen aus den verschiedenen Bereichen der Bank ausgewertet. Gemeinsam mit den zuständigen Mitarbeitern werden Gespräche geführt, situativ indizierte Risikoanalysen durchgeführt, Ortsbegehungen vorgenommen, Maßnahmen abgeleitet und natürlich werden auch die Mitarbeiter für das jeweilige Thema sensibilisiert. Als Ergebnis der Kontrollen erhält die Bank darüber hinaus einen Bericht, in dem die getroffenen Maßnahmen zur Risikominimierung sowie Hinweise und Empfehlungen dargestellt werden.

Vorteile zusammengefasst: Der Geldwäschebeauftragte der Bank wird aktiv und unmittelbar eingebunden. Das weitere Vorgehen findet in enger Abstimmung statt. Der Geldwäschebeauftragte wird auch über die Ergebnisse der Kontrollen, die Umsetzung der empfohlenen Maßnahmen und ggf. über den weiteren Handlungsbedarf informiert. Das Schutzniveau ist deutlich erhöht worden.

Beispiel 2: Umsetzung neuer gesetzlicher Anforderungen
Eine besondere Herausforderung für alle Banken als Verpflichtete nach dem Geldwäschegesetz (GwG) ist die stetig steigende Dynamik der regulatorischen Neuerungen. So wurde Mitte 2017 die 4. EU-Geldwäscherichtlinie in deutsches Recht umgesetzt. Das Bundeskabinett hat am 31. Juli 2019 den Entwurf eines Gesetzes zur Umsetzung der Änderungsrichtlinie zur 4. EU-Geldwäscherichtlinie beschlossen. Das Gesetz soll zum 1. Januar 2020 in Kraft treten.

Mit Inkrafttreten des Gesetzes zur Umsetzung der 4. EU-Geldwäscherichtlinie verdreifachte sich die Anzahl der Paragraphen des GwG. Es galten unmittelbar diverse neue Regelungen, deren Umsetzung erheblichen Aufwand bei den Banken verursachte. Beispielhaft seien hier die Einführung des Konstrukts des „fiktiven wirtschaftlich Berechtigten“ und die Ausweitung der Anwendbarkeit der „gruppenweiten Sorgfaltspflichten“ gemäß § 9 GwG genannt. Faktisch waren die Verpflichteten unter einem immensen zeitlichen und organisa- >

3 FALLZAHLEN 2018



AUTOR UND ANSPRECHPARTNER

Thomas Wagener
Leiter Compliance-Spezialisten,
E-Mail: thomas.wagener@dz-cp.de

torischen Druck, die Neuerungen fristgerecht umzusetzen. Erschwerend kamen zwei weitere Aspekte hinzu: Zum einen bestand bis zum Dezember 2018, also dem Zeitpunkt der Veröffentlichung der Auslegungs- und Anwendungshinweise (AuA) der BaFin, teils rechtliche Unsicherheit hinsichtlich der Auslegung einiger gesetzlicher Anforderungen. Zum anderen traten mit dem Gesetz drastische Verschärfungen der Bußgeldvorschriften in Kraft.

Im Rahmen des Auslagerungsverhältnisses Geldwäsche- und Betrugsprävention konnten für die Kunden der DZ CompliancePartner (ehemals DZ BANK bzw. GenoTec) alle Prozesse überarbeitet und angepasst werden. Durch den jeweils zuständigen Geldwäschebeauftragten wurden alle nötigen Schritte unternommen, um die gesetzlichen Anforderungen umzusetzen.

Darüber hinaus äußerten viele Banken weitergehende Informations- und Unterstützungsbedarfe, die zum Teil nur mittelbar in der Zuständigkeit des Geldwäschebeauftragten lagen. Auch in diesen Fällen wissen die Banken zu schätzen, dass unsere Spezialisten direkt vor Ort ansprechbar sind. So wurde beispielsweise eine Vielzahl von themenspezifischen Präsenzschulungen durchgeführt. In Workshops wurden die Änderungen in kleineren Gruppen anhand konkreter Fälle besprochen. Oder es wurden anhand der bankindividuellen Prozesse bedarfsorientierte Lösungen erarbeitet. Selbstverständlich wurde die Umsetzung der Neuerungen kontrolliert und, sofern nötig, wurden Feinjustierungen und Korrekturen der Prozesse gemeinsam mit den Banken erarbeitet.

Vorteile zusammengefasst: Durch direkte Einbindung des Geldwäschebeauftragten konnten die durch die gesetzlichen Neuerungen mittelbar tangierten bankspezifischen Prozesse identifiziert und angepasst werden. Auch hier profitiert die Bank, weil die rechtlichen Neuerungen in allen Bereichen der Bank zügig und weitreichend Anwendung fanden.

Unsere Leistung – Ihr Nutzen

- Durch die Vor-Ort-Betreuung übernimmt die DZ CompliancePartner bankindividuelle – bedarfsorientierte und themenspezifische – Tätigkeiten, wie beispielsweise die risikoorientierte Beratung in Ihrem Haus/vor Ort,
- das Aufspüren von Verdeckungsrisiken durch ergänzende, prozessorientierte Unterstützung,
- die Reduzierung von Schadensfällen, indem Risiken frühzeitig und angemessen behandelt werden, sowie
- erweiterte Kontrollen und
- Mitarbeitersensibilisierungen.

Diese Tätigkeiten werden in der Regel durch den „Compliance-Spezialisten“ vor Ort übernommen. Sie steigern insgesamt das Schutzniveau Ihrer Bank, das Risiko aufsichtsrechtlicher Sanktionen reduziert sich noch einmal. Im Übrigen kann die Bank dokumentieren, dass sie nicht nur ihre geldwäsche- und betrugspräventionsrelevanten Prozesse mit einem Compliance-Management-System steuert, das nach dem IDW-Prüfungsstandard 951 Typ 2 geprüft wird, sondern auch, dass sie eine Compliance-Kultur vor Ort zusätzlich stärkt.

Das Feedback der Banken spricht eine deutliche Sprache. Sie schätzen insbesondere die Möglichkeit, im persönlichen Gespräch detailliert und unmittelbar ihre speziellen Fragen abschließend klären zu können, was sich allein aus der Lektüre der umfangreichen Fachliteratur einschließlich aller einschlägigen Arbeitsanweisungen nicht immer und schon gar nicht auf die Schnelle erreichen lässt. ▬

MaRisk

Nachhaltigkeit in der Finanzwirtschaft

Das Thema „Nachhaltigkeit" ist in aller Munde. Doch ändert sich auch etwas? Diese Frage wird nun seitens der Finanzaufsicht überraschend klar beantwortet: Voraussichtlich noch in diesem Jahr sind erste Maßnahmen zu ergreifen, die erhebliche Auswirkungen haben werden.

„Als Finanzaufsicht ist es unser Auftrag, Risiken für das Finanzsystem zu erkennen und die von uns beaufsichtigten Unternehmen aufzufordern, sie angemessen zu berücksichtigen", erklärte BaFin-Präsident Felix Hufeld zum Auftakt der ersten Konferenz „Nachhaltige Finanzwirtschaft", die am 9. Mai im Umweltforum Berlin stattfand.

Der nachfolgende Artikel will einen kurzen Überblick zur Nachhaltigkeit in der Finanzwirtschaft geben.

Nachhaltigkeitsbegriff

Nachhaltige Finanzwirtschaft bezieht sich nach einem breiten Verständnis auf ein Spektrum finanzwirtschaftlicher Ansätze und Instrumente, die sich nicht nur an ökonomischen Kriterien orientieren, sondern – simultan und systematisch – auch sogenannte **„Nachhaltigkeitskriterien",** wie die 17 Ziele der Vereinten Nationen für nachhaltige Entwicklung (17 Sustainable Development Goals – SDGs)[1], berücksichtigen.

Die G20-Staats- und -Regierungschefs haben daher in der Erklärung von Buenos Aires 2018 die Mobilisierung nachhaltiger Finanzierung als wichtig für das globale Wachstum herausgestellt. Vorangegangen war die Weltklimaschutzkonferenz in Paris 2015, die mit dem Pariser Klimaabkommen schloss. Ziel des Pariser Klimaabkommens ist es, die Erderwärmung auf unter 2 Grad Celsius, nach Möglichkeit auf unter 1,5 Grad Celsius gegenüber vorindustriellen Werten zu beschränken. Dies ist notwendig, da jede der drei letzten Dekaden wärmer war als jede andere Dekade zuvor. Die gesamtwirtschaftlichen Schäden durch Naturkatastrophen steigen weltweit[2]. 2018 war das viertteuerste Jahr gemessen an den Schäden seit 1980; die Schäden beliefen sich auf 160 Mrd. US-Dollar. In diesem Zusammenhang ändert sich auch das Risiko bzw. der mögliche Risikoeinschlag: Es sind Mehrfach-Hits wahrscheinlich, d. h., ein Naturereignis schlägt aus Bankensicht nicht nur in einen Risikobereich ein, sondern kann Mehrfachauswirkungen haben. Wird beispielsweise durch einen Hagelschaden nicht nur die vorfinanzierte Ernte vernichtet, sondern auch das für einen Kredit als Sicherheit dienende Gewächshaus, so kann die Wirtschaftsgrundlage des Betreibers und daher auch das Geschäft der Bank gefährdet sein.

Der Klimawandel wird existierende Risiken verstärken und zusätzliche Risiken für Mensch und Umwelt schaffen.

Um dieser Risikoentwicklung im Bankensektor entgegenzuwirken, hat sich zwei Jahre nach dem Pariser Klimaabkommen das **Network for Greening the Financial System (NGFS)** gegründet. Das NGFS besteht aus 42 Mitgliedern und acht Beobachtern und setzt sich im Wesentlichen aus Zentralbanken und Aufsichtsbehörden zusammen, darunter auch die Deutsche Bundesbank und die BaFin[3].

Das NGFS ruft zu konzentriertem Handeln auf und schlägt den Zentralbanken und Aufsichtsbehörden vier mögliche Vorgehensweisen (Best Practices) vor, mit denen der Finanzsektor dazu beitragen kann, die Pariser Klimaschutzziele zu erreichen. Zu den Best Practices gehört u. a. die stärkere Einbindung von Klima- und Umweltrisiken ins Risikomanagement[4,5]. >

[1] https://www.un.org/sustainabledevelopment/sustainable-development-goals/.

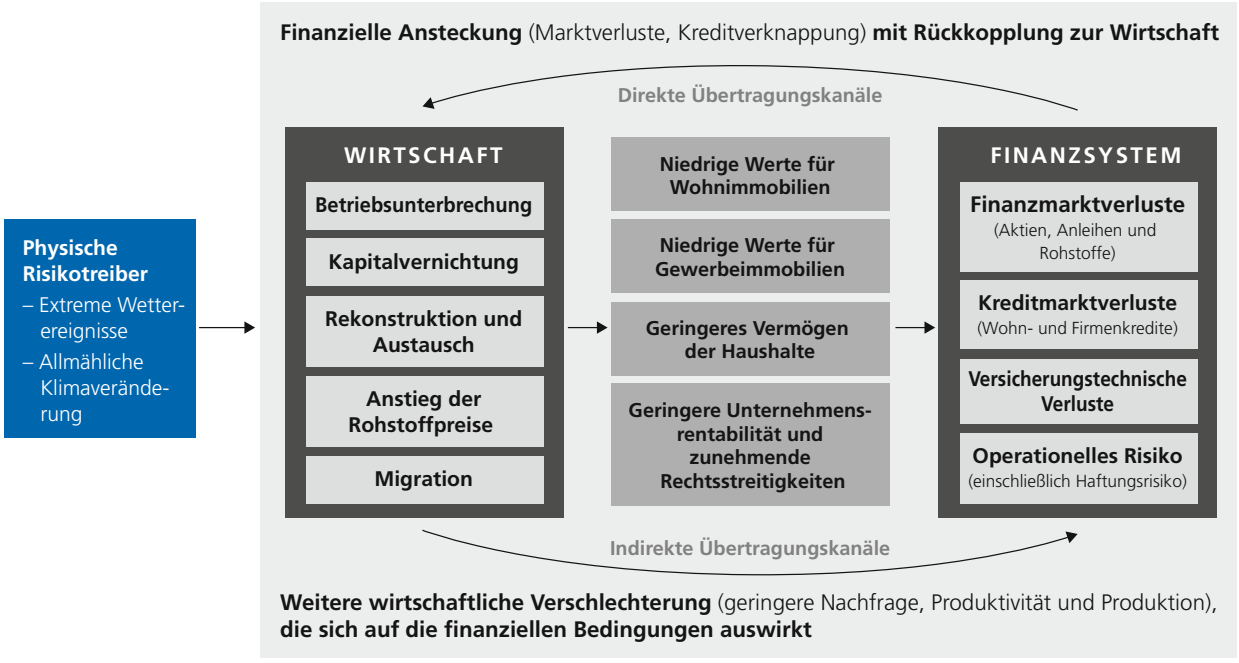
[2] Munich Re, Homepage, abgerufen am 18.07.2019.

[3] https://www.banque-france.fr/en/financial-stability/international-role/network-greening-financial-system/about-us.

[4] https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2019/meldung_190418_NGFS_Report.html.

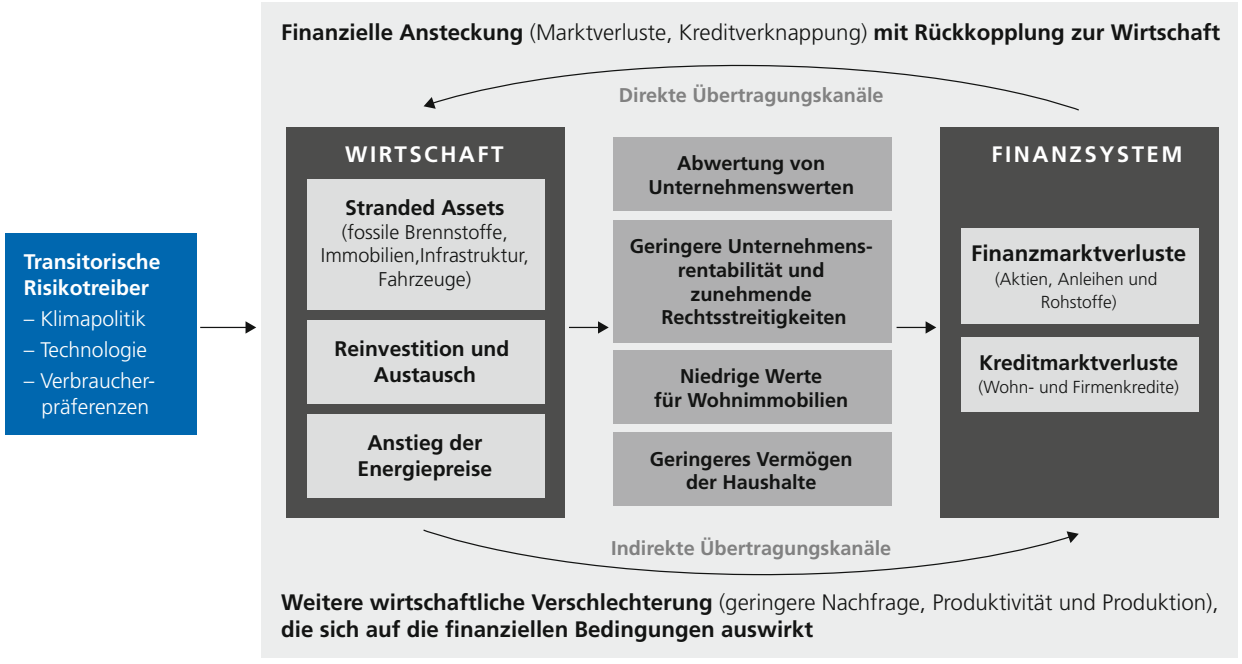
[5] Hierzu flankierend hat das NFGS mit „A call for action – Climate change as a source of financial risk" einen Bericht darüber veröffentlicht, wie sich Klima- und Umweltrisiken auf die Finanzmärkte auswirken.

1 VON **PHYSISCHEN RISIKEN** ZU RISIKEN FÜR DIE FINANZSTABILITÄT



Quelle: Network for Greening the Financial System (NGFS), First Comprehensive Report, S. 14.

2 VON **TRANSITORISCHEN RISIKEN** ZU RISIKEN FÜR DIE FINANZSTABILITÄT



Quelle: Network for Greening the Financial System (NGFS), First Comprehensive Report, S. 17.

Das Fachgremium MaRisk hat sich im Mai 2019 mit dem Thema beschäftigt und Vorschläge zur Berücksichtigung von Nachhaltigkeitsrisiken in den MaRisk gemacht. Es ist davon auszugehen, dass diese in der für Ende 2020 vorgesehenen Konsultation der MaRisk-Novelle enthalten sein werden.

Die BaFin veranstaltete in Berlin ebenfalls im Mai 2019 eine Nachhaltigkeitskonferenz, um das Bewusstsein des Finanzsektors für die Risiken und Chancen zu schärfen, die sich aus klimatischen, ökologischen oder sozialen Veränderungen sowohl für den einzelnen Finanzmarktakteur als auch für den Finanzmarkt als Ganzes ergeben[6].

Im Rahmen dieser Nachhaltigkeitskonferenz wurde auch das Thema **Environment, Social, Governance (ESG)** diskutiert.

Nachhaltigkeit ist demnach nicht nur ein reines Umweltthema, wie bei der Erstbetrachtung oftmals vermutet wird. Es umfasst ebenso z. B. den Umgang eines Unternehmens mit seinen Mitarbeitern, das Thema Menschenrechte und wie bei Entscheidungen von Unternehmen ökologische und sozialgesellschaftliche Aspekte beachtet beziehungsweise bewertet werden.

In der Summe lässt sich anhand des ESG-Ansatzes prüfen, wie nachhaltig ein Unternehmen arbeitet und welche Nachhaltigkeitsrisiken unter Umständen bestehen.

Nachhaltigkeitsrisiken im Finanzmarkt

Die Nachhaltigkeitsrisiken im Finanzmarkt untergliedern sich in physische und transitorische Risiken sowie Finanzstabilitätsrisiken. Hinter der Begrifflichkeit des Nachhaltigkeitsrisikos versteckt sich grundsätzlich kein neues Risiko. Das Central Banks and Supervisors Network for Greening the Financial System (NGFS) hat in seinem „First Comprehensive Report“ aus April 2019 die Auswirkungen von physischen und transitorischen Risiken für die Finanzstabilität graphisch dargestellt (siehe S. 16).

Finanzstabilitätsrisiken

Die erwarteten volkswirtschaftlichen Auswirkungen bei unterschiedlichen Erwärmungsphasen sind enorm und stellen immense Risiken für die Finanzstabilität dar.

Eine Erderwärmung um drei Grad Celsius im Vergleich zu einer konstanten Erdtemperatur würde gemäß den Prognosen des Chief Risk Officers Forum zu einem Rückgang des weltweiten Bruttoinlandsprodukts um bis zu 23 Prozent führen. Bestimmte Regionen der Erde werden in diesem Fall für Menschen zum Teil nicht mehr bewohnbar sein. Würde sich die Temperatur sogar um fünf Grad Celsius erwärmen, hätte dieses zur Folge, dass der Meeresspiegel schon bis zur nächsten Jahrhundertwende um bis zu zwei Meter steigen könnte. In der Folge würde sich das weltweite Bruttoinlandsprodukt nahezu halbieren.

Perspektive der Kreditwirtschaft

Der Klimawandel und die damit einhergehenden Nachhaltigkeitsbestrebungen fordern die Kreditwirtschaft heraus: Die EU-Kommission hat allein für Europa einen jährlichen Finanzierungsbedarf von 180 Mrd. EUR identifiziert, um die EU-Klima- und -Energieziele bis 2030 zu verwirklichen[7]. Weltweit wird der jährliche Investitionsrückstand in den Bereichen Verkehr, Energie und Ressourcenmanagement auf 270 Mrd. EUR geschätzt[8]. Daraus kann eine steigende Nachfrage nach nachhaltigen Geldanlagen abgeleitet werden.

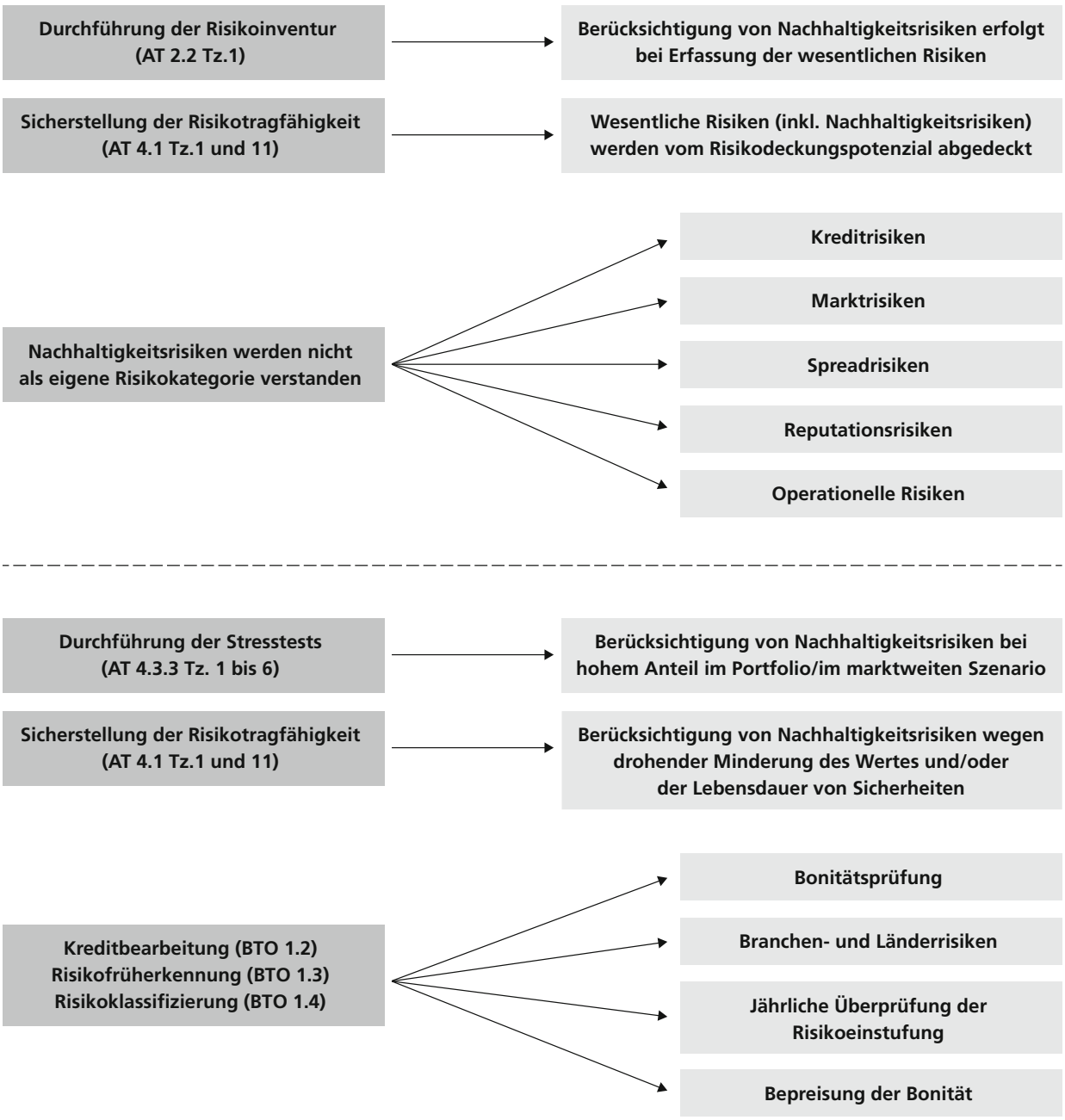
Neben den Instituten beschäftigen sich auch die Aufsicht und einschlägige Gremien mit dem Thema, so z. B. im regulatorischen Umfeld das Fachgremium MaRisk. >

[6] https://www.bafin.de/SharedDocs/Veranstaltungen/DE/190509_sustainable_finance.html.

[7] Europäische Kommission: Aktionsplan „Finanzierung nachhaltigen Wachstums“ vom 08.03.2018, S. 3.

[8] EU-Kommission, a.a.O.

3 BERÜCKSICHTIGUNG VON NACHHALTIGKEITSRISIKEN IN DEN MARISK



Quelle: Fachgremium MaRisk am 03.05.2019

AUTOREN UND ANSPRECHPARTNER

Jörg Scharditzky
Beauftragter MaRisk-Compliance, E-Mail: joerg.scharditzky@dz-cp.de

Axel Hofmeister
Beauftragter MaRisk-Compliance, E-Mail: axel.hofmeister@dz-cp.de

Nachhaltigkeitsrisiken in den MaRisk

Das Fachgremium MaRisk hat sich am 3. Mai 2019 mit dem Thema Nachhaltigkeitsrisiken in den aktuellen Mindestanforderungen an das Riskomanagement (MaRisk) eingehend beschäftigt. Dem Fachgremium gehören Experten aus kleineren und größeren Instituten, Prüfer, Verbandsvertreter und Aufseher an. Im Ergebnis wurde eine Kurzübersicht erstellt, die die Berücksichtigung von Nachhaltigkeitsrisiken in den MaRisk darstellt (siehe S. 18).

Nachhaltigkeitsansatz der BaFin

Ausgehend von den drei Säulen Regulierung, Risk-Management und Marktbeobachtung/Offenlegung & Meldewesen adressiert die BaFin Nachhaltigkeit über alle Sektoren hinweg. Sie wird Nachhaltigkeit in den risikobasierten Aufsichtsansatz einbeziehen und – voraussichtlich – im Dezember 2019 ein Merkblatt zum Umgang mit Nachhaltigkeitsrisiken veröffentlichen.

Das Merkblatt zur Nachhaltigkeit wird sich u. a. mit folgenden Themen befassen[9]:

- Strategien
- Verantwortung der Unternehmensführung
- Geschäftsorganisation
- Risikomanagement
- Stresstests/Szenarioanalysen
- Auslagerung/Ausgliederung
- Gruppensachverhalte
- Verwendung von Ratings

Die Banken müssen damit rechnen, dass die BaFin zukünftig auch Themen aus dem Merkblatt im Rahmen von Prüfungen einbeziehen wird. Als Bank kann man sich dem Thema Nachhaltigkeit daher nicht verschließen.

Fazit

Es ist sicher nicht das Risiko von kostspieligen Schäden aufgrund der zunehmenden Wetterextreme, das nationale und internationale Aufsichtsbehörden und Zentralbanken auf den Plan ruft. Vielmehr sind es die indirekten Risiken, also die Risiken, die sich aus der Struktur der Kunden von Banken und Versicherern ergeben.

Gerade die dargelegten physischen und transitorischen Risiken von Versicherern und Banken können gebündelt geeignet sein, die Stabilität des Finanzmarktes zu gefährden. In der Gesamtbetrachtung werden Nachhaltigkeitsrisiken somit langsam, aber sicher zur einer gesamtwirtschaftlichen Bedrohung. Folglich sind die nationalen und internationalen Regulierer und Aufsichten sensibilisiert, diese Herausforderung anzugehen.

Wie groß das ökonomische Potenzial ist, zeigt eine Studie der EU-Kommission, die den Investitionsbedarf zur Erreichung der Klimaziele allein im Energiesektor auf jährlich 180 Mrd. EUR beziffert. Genau hier liegen die großen Chancen für die Finanzwirtschaft, wenn sie sich früh genug bei der Generierung und Umleitung von Mitteln zur Erfüllung von Nachhaltigkeitszielen positioniert.

Es ist davon auszugehen, dass die geplanten Änderungen der Finanzaufsicht Auswirkungen auf das gesamte Institut, einschließlich der Compliance-Funktion, haben werden. ▬

[9] So der Chief Sustainable Finance Officer der BaFin auf dem Norddeutschen Bankentag 2019 in Lüneburg in dem Vortrag „Nachhaltigkeit – Die Rolle der Regulierer".

Security Awareness

Mensch vs. Trojaner 1:0

Die Heise Gruppe wurde Opfer der Schadsoftware Emotet. Was wir daraus lernen können: 1. Niemand ist davor sicher. 2. Besser kann man kommunikativ mit einem Schadensfall nicht umgehen. 3. Ein Schadenfall ist sehr teuer. 4. Security Awareness zahlt sich aus.

Man könnte annehmen, dass ein Verlag, in dem sich so viel IT-Know-how vereint, bestens gegen derartige Angriffe geschützt sein müsste. Gleiches könnte man wohl auch von der Informationsverarbeitung im Bankensektor annehmen – und es wäre ebenso falsch! Denn IT-Know-how allein reicht nicht aus, es muss in konkrete organisatorische Vorgaben und Prozesse gegossen werden. Und auch diese schützen nur, wenn Informationssicherheit im Unternehmen gelebt wird, wenn Informationssicherheit zu einem Teil der Unternehmenskultur geworden ist.

In diesem Artikel soll beispielhaft an dem „Banking-Trojaner" Emotet und der Heise Gruppe gezeigt werden, welche Methoden moderne Trojaner nutzen, um einen Zugang zu Ihrem Unternehmensnetzwerk zu erlangen[1].

Bericht der Infektion von Heise

Am Montag, den 13. Mai 2019 wurde einem Mitarbeiter von Heise eine E-Mail zugestellt, welche sich auf eine real existierende Geschäftsbeziehung bezog. Es wurde darum gebeten, falls sich Daten geändert haben sollten, diese doch bitte zu ändern. Zu diesem Zweck befand sich im Anhang eine Word-Datei. Die E-Mail war unauffällig. Weder fiel sie durch übliche Rechtschreib- noch durch Logikfehler auf, wie man sie bei Phishing-E-Mails oft beobachten kann. Es schien sich um eine reguläre Kommunikation mit einem Geschäftspartner zu handeln. Mit dem Öffnen der Word-Datei wurde jedoch das Ausführen von Makros bestätigt, die dann den Schadcode aus dem Internet nachgeladen haben. Der nun mit Emotet infizierte Rechner des Mitarbeiters begann sofort, auch die Rechner von Kollegen anzugreifen und zu infizieren.

Dieses löste in Folge mehrere Alarme in der Anti-Viren-Software aus, woraufhin die Systemadministratoren die betroffenen Systeme reinigten. Zunächst schien es, als ob das Problem damit unter Kontrolle sei, bis am Mittwoch, den 15. Mai 2019 die Firewall Alarmmeldungen erzeugte. Mehrere Rechner hatten Verbindung mit einem Emotet Command- & Control-Server hergestellt. Die Systemadministratoren versuchten diese Verbindungen zu blockieren und die infizierten Rechner zu isolieren. Gegen Mittwochabend zeichnete sich ab, dass dieses Wettrennen nicht zu gewinnen war. Sie führten einen kompletten Lockdown der Systeme und Netzwerke durch. Der normale Geschäftsbetrieb kam vollständig zum Erliegen.

Ab Donnerstag begann dann eine systematische Analyse der Netzwerke mit forensischen Methoden im Rahmen des Incident-Response-Prozesses. Dabei wurde offensichtlich, dass das Ausmaß der Infektion zu umfangreich war, um es mit den internen Fachkräften bewältigen zu können. Es wurden externe Berater engagiert, um bei der Analyse zu unterstützen. Ergebnis war: Mindestens fünf verschiedene Versionen von Emotet haben mehr als 100 Rechner infiziert. Das Active Directory war derart beschädigt, dass es neu aufgebaut werden musste.

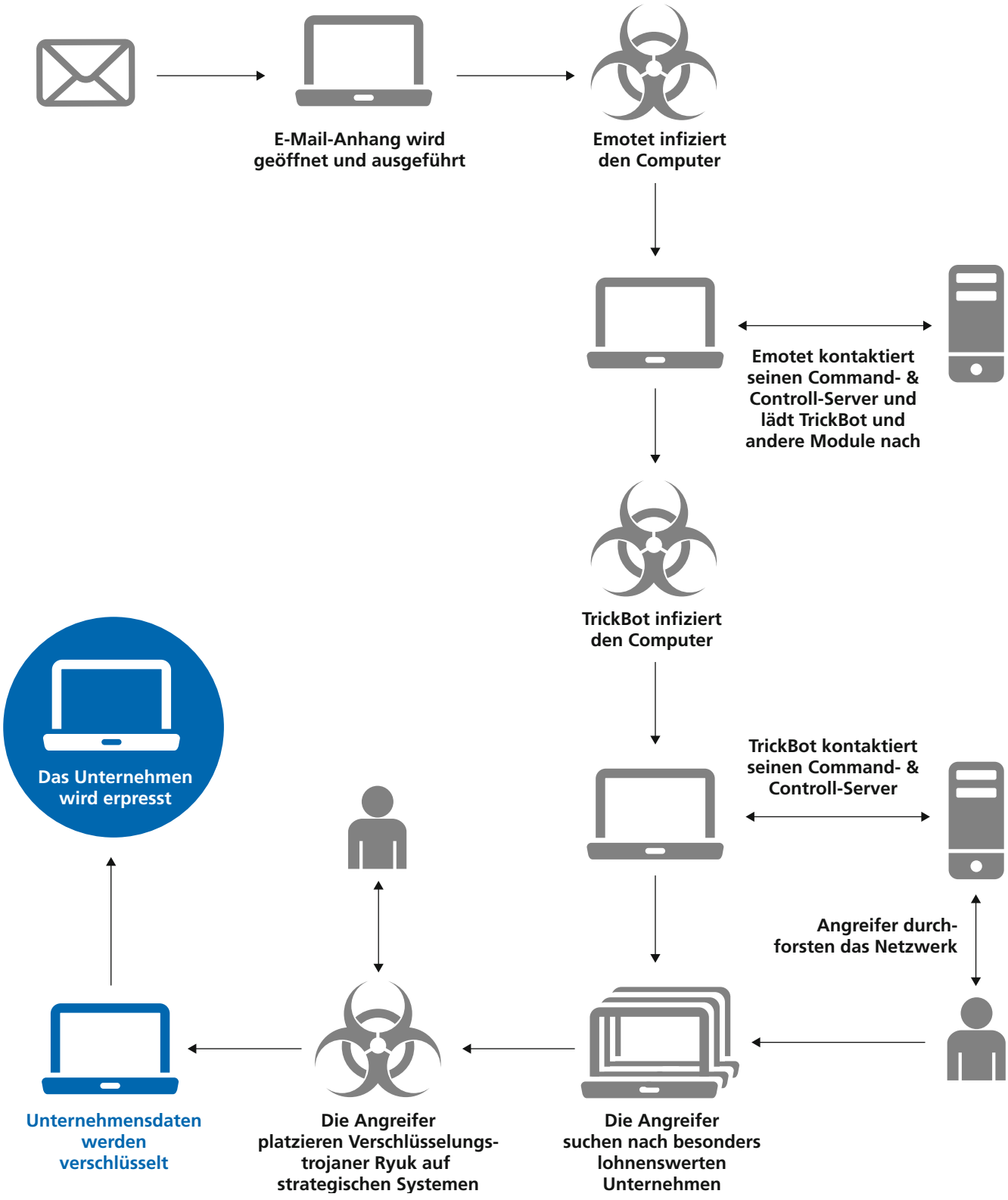
Der Wiederaufbau dauerte mehrere Tage an. Die Kosten: ca. 50.000 EUR zzgl. Umsatzeinbußen durch Produktionsausfälle sowie Kosten für verbesserte Security.

Die Wirkweise von Emotet und Co.

Wie aber konnte ein Trojaner wie Emotet trotz Viren-Scanner, Firewalls, fein abgestimmter Berechtigungsstrukturen sowie Mitarbeitersensibilisierung so erfolgreich ein ganzes Unternehmensnetzwerk infiltrieren? Die Antwort: Auch die Angreifer werden geschickter und rüsten auf.

Emotet ist nicht neu. Erstmals wurde dieser Trojaner im Juni 2014 identifiziert. Damals waren hauptsächlich Kunden österreichischer und deutscher Banken betroffen. Da Emotet den Kommunikationspartnern vortäuscht, das jeweilige Gegenüber zu sein, kann er nahezu beliebige Änderungen im Datenstrom vornehmen, ohne dass der Kunde oder die Bank etwas davon bemerken. Denn anders als beim Phishing handelt es sich beim Kunden-PC und der Onlinebanking-Webseite um die echten Systeme dieser Kommunikationsverbindung. >

[1] https://www.heise.de/security/meldung/Emotet-bei-Heise-Aufzeichnung-des-heisec-Webinars-jetzt-verfuegbar-4464045.html


E-Mail-Anhang wird geöffnet und ausgeführt
Emotet infiziert den Computer
Emotet kontaktiert seinen Command- & Controll-Server und lädt TrickBot und andere Module nach
TrickBot infiziert den Computer
TrickBot kontaktiert seinen Command- & Controll-Server
Angreifer durch-forsten das Netzwerk
Das Unternehmen wird erpresst
Unternehmensdaten werden verschlüsselt
Die Angreifer platzieren Verschlüsselungs-trojaner Ryuk auf strategischen Systemen
Die Angreifer suchen nach besonders lohnenswerten Unternehmen

AUTOR UND ANSPRECHPARTNER

Florian Brüderle
Beauftragter Informationssicherheit & Datenschutz,
E-Mail: florian.bruederle@dz-cp.de

Emotet wurde seitdem immer weiter entwickelt, bis er seit Ende 2018 auch in der Lage ist, E-Mails auszulesen und zu verwenden. Wie schon im konkreten Fall bei der Heise Gruppe beschrieben, versendet Emotet nun E-Mails mit authentisch aussehenden, aber frei erfundenen Inhalten an Personen, mit denen der infizierte Rechner bereits in Kontakt steht. Dabei werden die Signatur der ausgelesenen E-Mail, der Betreff und der Absender stimmig eingesetzt, so dass auch sensibilisierte Mitarbeiter Schwierigkeiten haben, dies als Angriff zu erkennen. Dieses sogenannte „E-Mail-Harvesting" ist der Klasse automatisierter und für den massenhaften Einsatz konzipierter APT-Angriffe (Advanced Persistent Threat) zuzuordnen.

Unter APT-Angriffen versteht man komplexe, zielgerichtete Angriffe auf lohnende Infrastrukturen. Dabei nehmen die Angreifer über einen langen Zeitraum großen, oft auch personellen Aufwand auf sich, um möglichst lange in dem Netzwerk des Opfers handlungsfähig zu bleiben. Ein in der Öffentlichkeit wahrgenommener APT war der Angriff auf den deutschen Bundestag zwischen Dezember 2014 und Mai 2015.

Nun handelt es sich bei APTs wie den oben beschriebenen und dem Angriff auf Heise zwar um unterschiedliche Angriffs- und auch Gefährdungsklassen. Der Hauptunterschied ist die hohe Automatisierung von Emotet, die zwar erstaunlich geschickt vorgeht, menschlichen Angreifern aber immer noch weit unterlegen ist. Dies ist aber kein Grund, solche Angriffe als weniger bedrohlich einzustufen. Denn zum einen können sich Gruppen, die einen APT planen, bekannter Schädlinge wie Emotet bedienen, um im Falle der frühen Entdeckung als „normale" Infektion eingeordnet zu werden. Zum anderen besitzt Emotet einen weiteren Angriffsmechanismus.

Sobald Emotet einen Computer infiziert hat, kontaktiert er seinen Command- & Control-Server. Der lädt im Hintergrund weitere Module und sogar Banking-Trojaner, wie etwa TrickBot, nach.

TrickBot wurde 2016 entwickelt und zählt zu den derzeit modernsten Banking-Trojanern. Emotet übernimmt in dieser Symbiose dann mehr die Verbreitung über das bereits beschriebene E-Mail-Harvesting. Er agiert also wie ein Wurm und unterstützt dadurch die Verbreitung von TrickBot. Sobald TrickBot installiert ist, nimmt dieser ebenfalls Verbindung zu seinem Command- & Control-Server auf und könnte damit der Beginn eines APT sein. Denn ab diesem Moment beginnen die Eigentümer des Command- & Control-Servers das Netzwerk des Opfers zu untersuchen.

Bei besonders interessanten und lukrativen Opfern werden die Angreifer dann auch manuell tätig. Sie analysieren das Netzwerk, identifizieren Backupsysteme, löschen Backups und platzieren Verschlüsselungstrojaner. Im Falle einer Emotet-/TrickBot-Infektion würde dann der Verschlüsselungstrojaner Ryuk zum Einsatz kommen. Da sich aber zuvor bereits Emotet umfassende Rechte im Active Directory des Unternehmens gesichert hat und die TrickBot-Administratoren gegebenenfalls manuell das Netzwerk untersucht haben, hat die Verschlüsselung mittels Ryuk meist katastrophale Folgen für das Unternehmen.

Die Entschlüsselung muss dann teuer bezahlt werden: Die Höhe der Summe hängt von der Finanzkraft des Opfers ab. Eine Bank müsste also tiefer in die Tasche greifen als eine Privatperson. Aber auch die Nationalität kann eine Rolle spielen. Der IT-Sicherheitsexperte Linus Neumann berichtete kürzlich in seinem Podcast „Logbuch Netzpolitik (Folge 307)", wie mittels russischer Sprachkenntnisse und eines russischen Passes ein mit dem Verschlüsselungstrojaner GandCrap verschlüsselter PC kostenlos entschlüsselt werden konnte.

Schutzmaßnahmen gegen solche Angriffe

Nach all den bedrohlichen Berichten: Kann man sich vor Emotet und Co. überhaupt schützen? Die gute Nachricht: Ja, es gibt zahlreiche Maßnahmen, die das Risiko einer Infektion verringern.

Es gibt aber nicht die „eine" wirksame Lösung. Heise hat aus dem Angriff gelernt und sechs Verteidigungslinien definiert, in denen sie sich verbessern wollen:

1. Security Awareness
2. Perimetersicherheit: Die zentralen Fragen in diesem Punkt lauten: Nutzen wir geeignete Firewalls, Web- und E-Mail-Filter? Ist es wirklich notwendig, dass wir Office-Dokumente mit Makros erhalten? Und arbeiten unsere Nutzer noch mit lokalen Administratorrechten?
3. Netzwerksicherheit: Netzwerk- und Rechtemanagement ist zentral bei der Verteidigung, deshalb die Frage: Ermöglichen wir unseren IT-Administratoren Weiterbildungen auf höchstem Niveau und haben sie in der täglichen Arbeit die notwendigen zeitlichen Ressourcen, dieses Wissen anzuwenden?
4. Monitoring: Monitoringsysteme helfen die Integrität des Netzwerkes zu überwachen. Aber auch hier benötigt man gut geschultes Personal mit ausreichend zeitlichen Ressourcen. Ansonsten droht man in einer Flut von Fehlalarmen unterzugehen, die kaum mehr jemand ernst nimmt.
5. Backups: Emotet, TrickBot und Ryuk verschlüsseln alles, auch und gerade Online-Backups. Machen sie daher offline Backups auf externen Datenträgern und testen sie diese regelmäßig.
6. Notfallmanagement: Bereiten Sie sich auf den Ernstfall vor. Denn mit kühlem Kopf und einem Plan kann man jede Krise meistern. Es ist nicht die Frage, ob sie angegriffen werden, sondern wann.

Punkt 1 der Liste, Security Awareness, ist insbesondere hervorzuheben. Wie sieht es bei Ihnen aus: Was tun Sie im Unternehmen ganz konkret für Ihre Security Awareness?

Bei einem Angriff mit Emotet, TrickBot, Ryuk sind jene Unternehmen gut geschützt, deren MitarbeiterInnen den Trick durchschauen und den verhängnisvollen Anhang nicht öffnen.

Tragischerweise ist Mitarbeitersensibilisierung genau der Bereich, den Unternehmen oft mit ungenügenden finanziellen Ressourcen ausstatten. Und lassen Sie uns Klartext reden: Web Based Trainings sind nur ein kleiner Bestandteil einer wirksamen Security-Awareness-Strategie. Nicht vergessen: Wir sprechen hier von unserer 1. Verteidigungslinie.

Deshalb betrifft Mitarbeitersensibilisierung nicht nur die normalen Computernutzer, sie richtet sich zunächst an das Management. Die Botschaft lautet: Informationssicherheit kostet Geld. Die meisten betroffenen Unternehmen erhöhen erst nach einem Vorfall ihr Budget für Informationssicherheit. Klug, wenn man es bereits zuvor getan hat und kein Opfer geworden ist.

Der nächste Adressat von Security Awareness ist die IT-Abteilung. Hier ist die Botschaft: Wir haben Probleme, und wir müssen uns ständig verbessern. Dies betrifft nicht zwangsläufig Hard- und Software. Zu oft arbeiten Administratoren mit zu hohen Rechten oder umgehen gar lästige technische Richtlinien wie globale Passwortrichtlinien. Administratoren sollten sich ständig bewusst sein, dass sie auch nur User sind. Angesichts ihrer Rechte in den Systemen sind aber gerade sie besonders gefährliche und vor allem lohnenswerte Ziele.

Und last but not least richtet sich Security Awareness an alle Mitarbeiter mit folgender Botschaft: Ich bin wichtiger Teil der Informationssicherheit meines Unternehmens. Nur mit meiner Hilfe kann das Unternehmen effektiv geschützt werden!

Fazit

Wenn alle sechs Verteidigungslinien greifen, dann wird Ihr Unternehmen zwar dennoch irgendwann angegriffen werden, aber die Auswirkungen werden erträglich sein. Stellen Sie sich die Alternative vor. Alle Ihre Unternehmensdaten, auch Ihre Backups sind unwiederbringlich verloren. Eventuell werden durch Sie auch noch Kunden oder Geschäftspartner infiziert. Können Sie den Schaden für Ihr Unternehmen beziffern? Angesichts dieses Szenarios erscheint es gar nicht mehr so schlimm, sich proaktiv auf Angriffe dieser Art vorzubereiten, oder? ▬

▶ **IT-Revision**

Auslagerung IT-Revision – (un)wesentlich?

Vor dem Hintergrund der steigenden Bedeutung von IT ist auch die „third line of defense", die IT-Revision, heutzutage besonders gefordert. Eine Auslagerung ist oft ein sehr guter Weg. Dabei stellt sich die Frage: Ist die Auslagerung der IT-Revision eigentlich als wesentlich oder unwesentlich zu betrachten?

Ihren Ursprung hat die IT-Revision in der Betriebswirtschaft bzw. dem Prüfungswesen. Durch die gestiegenen Anforderungen ist die IT-Revision ein spezieller Bestandteil der Internen Revision geworden. Allerdings setzt eine effektive IT-Revision interdisziplinäres Fachwissen voraus und damit kosten- und zeitintensive Seminare, um die zunehmende Komplexität der Prüfungsfelder bewältigen zu können.

Die IT-Revision muss in ihrer Rolle als dritte Verteidigungslinie unabhängig von den operativ Verantwortlichen oder den Beauftragtenfunktionen prüfen, dass alle IT-bezogenen normativen Bestimmungen eingehalten werden. IT-Revision setzt somit einen Schlusspunkt in der Schadensabwehr im Bereich der IT. Dazu gehören u. a.

- die Prüfung der Einhaltung unternehmensexterner und -interner Regelungen in der und für die IT – und somit der Schutz vor unsachgemäßem IT-Gebrauch (Datenverlust, Datendiebstahl etc.),
- die Prüfung auf Einhaltung der Regelungen des Datenschutzes,
- die Prüfung des Schutzes und der Sicherheit aller Informationssysteme, insbesondere der rechnungslegungsrelevanten IT-Systeme und Anwendungen – und damit die Identifizierung und Minimierung von Risiken und Ineffizienzen der IT-Infrastruktur sowie
- die Erstellung von Handlungsempfehlungen für das Management unter Berücksichtigung von Risikobewertungen und Schwachstellenanalysen.

Aufgrund der immer höheren Komplexitäten dieser Aufgaben bedienen sich viele Häuser mittlerweile der Expertise externer Fachleute. So ist z. B. das Angebot der DZ CompliancePartner GmbH zur Auslagerung der IT-Revision ein probates Mittel.

Auslagerung der IT-Revision

Für die Auslagerung gelten die Vorgaben der §§ 25a, 25b Kreditwesengesetz (KWG) sowie der AT 9 der Mindestanforderungen an das Risikomanagement (MaRisk). Für wesentliche – künftig wohl gemäß EBA-Guideline „kritische" oder „wichtige" – Auslagerungen gelten darüber hinaus noch besondere Anforderungen an die Vertragsgestaltung, die Beendigung des Auslagerungsverhältnisses sowie die Steuerung und Überwachung. Ergänzend dazu sind noch die Bankaufsichtlichen Anforderungen an die IT (BAIT) zu beachten.

Die Gesamtverantwortung für eine bereits durchgeführte bzw. geplante Auslagerung obliegt nach AT 3 Tz. 1 MaRisk der gesamten Geschäftsleitung und besteht in der Erstellung und Umsetzung eines angemessenen und wirksamen Risikomanagements im Sinne des § 25a Abs. 1 KWG.

Die Geschäftsleitung benötigt zur Steuerung und Überwachung der mit der Auslagerung verbundenen Risiken einen Gesamtüberblick über die ausgelagerten Aktivitäten und Prozesse. Dazu wird künftig ein zentrales Register vorzuhalten sein, wobei z. B. das Tool „Auslagerungsmanagement kompakt" der DZ CompliancePartner eine gute Unterstützung darstellt.

Eine Auslagerung darf nicht dazu führen, dass die Ordnungsmäßigkeit des Geschäftsbetriebes, die Steuerungs- und Kontrollmöglichkeiten der Geschäftsleitung oder gar die Prüfungsrechte und Kontrollmöglichkeiten der Finanzaufsicht eingeschränkt werden. Die Auslagerung von Funktionen wie z. B. des Risikocontrollings, der Compliance-Funktion nach WpHG oder MaRisk oder der Internen Revision (= besondere Funktionen) ist grundsätzlich unter Beachtung der Voraussetzungen des AT 9 Tz. 5 MaRisk erlaubt.

Die IT-Revision ist eine spezielle Kategorie im Rahmen der Internen Revision und kann somit als Teilkontrollfunktion der Internen Revision gemäß den MaRisk unter Berücksichtigung einer MaRisk-konformen Vertragsgestaltung sowie einer angemessenen Überwachung der Leistungserstellung ausgelagert werden.

Risikoanalyse zur Auslagerung

Eine Antwort auf die Frage, ob die Auslagerung der IT-Revision wesentlich oder unwesentlich ist, liefern die MaRisk jedoch nicht. Sie überlassen die Bewertung der Risiken für den Geschäftsbetrieb und damit die Einwertung der Auslagerung den Häusern selbst.

Die Art der Auslagerung – wesentlich oder unwesentlich – wird somit

- auf Grundlage einer Risikoanalyse nach AT 9 Tz. 2 MaRisk,
- im Vorfeld der Auslagerung und
- unter Beachtung der individuellen Situation, d. h., welche Risiken mit der geplanten Maßnahme überhaupt verbunden sind, entschieden.

Die Ausprägung, Tiefe oder Methodik der Risikoanalyse liegen dabei im Ermessen des jeweiligen Instituts und sollen eine Beurteilungsgrundlage schaffen, welches Risikopotenzial im Sinne der MaRisk von einer Auslagerung ausgeht, und ob sie demzufolge insgesamt als wesentlich oder als nicht wesentlich zu bewerten ist.

Die MaRisk verzichten auf detaillierte Vorgaben zu notwendigen Inhalten der Risikoanalyse. Das Institut führt diese eigenverantwortlich unter Risikogesichtspunkten aus und wiederholt diese regelmäßig, falls es zu der Auslagerung gekommen ist. Dabei sind zudem die maßgeblichen Organisationseinheiten sowie im Rahmen ihrer Aufgaben auch die Interne Revision bei der Erstellung mit einzubeziehen (vgl. AT 9 Tz. 2 MaRisk).

Bei der Risikoanalyse können unterschiedlichste Aspekte eine Rolle spielen: der konkrete Gegenstand der Auslagerung, welche Auswirkungen die Maßnahme auf das Institut hat, der Ort der Leistungserbringung, die Komplexität der geplanten Maßnahme, die Eignung potenzieller Dienstleister etc. Die Intensität der Analyse hängt somit von Art, Umfang, Komplexität und Risikogehalt der ausgelagerten Aktivitäten und Prozesse ab.

Unwesentlich oder wesentlich?

Für einige der zu bewertenden, relevanten Kriterien werden seitens des BVR Vorschläge unterbreitet. Dabei werden die Vorteile von Auslagerungen innerhalb der Genossenschaftlichen FinanzGruppe positiv berücksichtigt. So kann z. B. bei Auslagerungen innerhalb der Genossenschaftlichen FinanzGruppe das Risiko, keinen Ersatzanbieter zu finden, unberücksichtigt bleiben. Gleiches gilt für die Herausforderung, die Tätigkeit ggf. nicht wieder eingliedern zu können. Auch die Risikokonzentration ist bei Auslagerungen innerhalb der Gruppe aufgrund der Governance-Strukturen grundsätzlich mit gering vorzubelegen. Als wichtig werden aber auch hier die Anforderungen an das Qualitätsniveau der Auslagerung, die Komplexität oder der mögliche Verstoß gegen spezialgesetzliche Vorgaben angesehen. Demzufolge sind sowohl die Risiken der Auslagerung selbst wie auch die Eignung des Auslagerungsunternehmens vorab zu berücksichtigen.

Hinsichtlich der Bewertung der Auslagerungsrisiken per se ist es ratsam, die von der Auslagerung betroffenen Prozesse zu bewerten, sich ein Bild über die betriebsinternen Abläufe vor und nach der Auslagerung zu machen und abzuklären, inwieweit es möglich ist, klare Definitionen über die Aufgabenallokationen zwischen Auftraggeber und Auftragnehmer zu treffen.

In Bezug auf die Wahl des Anbieters wären vor dem Hintergrund möglicher rechtlicher Risiken und/oder Ausfallrisiken bei der Bewertung des Auslagerungsunternehmens Nachfragen zur Kapitalausstattung, zum Reputationsrisiko oder dem Risiko aus möglichen Weiterverlagerungen indiziert.

Wurde die Risikoanalyse abgeschlossen, ist anhand der gewonnenen Erkenntnisse final die Frage zu beantworten, ob es sich um eine wesentliche oder nicht wesentliche Auslagerung handelt.

Dies fordert auch § 9 Abs. 3 Prüfberichtsverordnung (PrüfbV) als Anforderung für den Abschlussprüfer: „Dabei ist eine Aussage darüber zu treffen, ob die Einstufung von >

Auslagerungen als wesentlich oder unwesentlich unter Gesichtspunkten des Risikos, der Art, des Umfangs und der Komplexität nachvollziehbar ist."

Insgesamt verweist auch der BVR in seiner Übersicht zu ausgelagerten Geschäftsprozessen in Anlehnung an den § 9 Abs. 3 PrüfbV vom 3. Juli 2019 darauf, dass auf alle Fälle eine Prüfung durch die Institute im Einzelfall vorzunehmen ist. Seine grundsätzliche Annahme lautet, dass „eine solche Auslagerung regelmäßig als ‚wesentlich' einzustufen sein dürfte".

Somit verbleibt die grundsätzliche Beurteilung, ob wesentlich oder unwesentlich, letztendlich doch bei dem einlagernden Unternehmen selbst. Relevant ist diese Entscheidung vor allen Dingen in Bezug auf den Umfang der Maßnahmen und Kontrollen, die sich zur Steuerung der Auslagerung ergeben. Sollte das Unternehmen nach Abwägung aller geforderten Parameter zu dem Schluss kommen, dass die Auslagerung der IT-Revision unwesentlich ist, dann muss dies gut begründet sein.

Eventuell ergeben sich künftig durch die neuen EBA-Guidelines, deren Geltung die BaFin für 2020 auf ihr Programm genommen hat („comply or explain"), erleichternde Aspekte in Bezug auf Gruppen- oder Konzernauslagerungen.

Bewertung der Auslagerungsdienstleistung der DZ CompliancePartner

Hinsichtlich der Risikoeinschätzung im Rahmen einer Auslagerung der IT-Revision an die DZ CompliancePartner könnte eine Bewertung auf Basis folgender Annahmen vorgenommen werden:

- Das Ausfallrisiko der DZ CompliancePartner als Auslagerungsdienstleister wird gemäß einem Gutachten der AWA-DO Deutsche Audit GmbH vom 15. März 2019 als gering eingestuft.
- Rechtliche Risiken sind aufgrund der Nutzung eines Auslagerungsvertrages nach BVR-Vorgaben überschaubar.
- Die DZ CompliancePartner setzt in diesem Bereich ausschließlich spezialisierte IT-Revisoren mit langjähriger Expertise ein und stellt deren laufende Aus- und Weiterbildung sicher.
- Die Durchführung der Prüfung wird in das Revisionskonzept der Bank integriert.
- Die Erkenntisse der Prüfungen werden durch die Bank aufgenommen und final geschlossen.
- Alle Arbeitspapiere der Prüfung verbleiben in der Bank. Der Vorstand wird unmittelbar und direkt informiert.
- Die IT-Systemlandschaft der Banken ist aufgrund der Nutzung der Systeme der Fiducia & GAD IT AG klar definiert und somit die Komplexität reduziert.
- Das Risiko einer Weiterverlagerung wird ausgeschlossen.

Diese Vorgehensweise ermöglicht es den Banken, einen externen IT-Revisor auch unmittelbar in das IKS der Bank einzubinden. Dadurch hat auch der Vorstand des Unternehmens die Möglichkeit (und die Verpflichtung), die Qualität der Dienstleistungserbringung direkt zu beurteilen, da der Bank sämtliche relevante Informationen zur Bewertung der Auslagerung zur Verfügung stehen. Gleichwohl bleibt die Erkenntnis, dass das jeweilige Institut, das einen externen IT-Revisor langfristig beauftragen möchte, eine Entscheidung hinsichtlich der Auslagerung der IT-Revision – unwesentlich oder wesentlich – bewusst und dokumentiert treffen muss. ▬

AUTOR UND ANSPRECHPARTNER

Thomas Grebe
Leiter IT-Audit,
E-Mail: thomas.grebe@dz-cp.de

Auslagerung

Nicht monetäre Motivationen für Auslagerungen

Sind Auslagerungen nur ein Rechenexempel? Spielen nur finanzielle Erwägungen für eine Auslagerungsentscheidung eine Rolle? Oder welche Beweggründe könnte es denn neben der monetären Sicht geben, Auslagerungen als vorteilhaft zu beurteilen?

Stöbert man in der Literatur zu diesem Thema, werden zwar vielfältige Gründe aufgezählt, eine nachhaltige Systematik oder Einordnung von nicht finanziellen Erwägungen findet sich aber nicht. Wie könnte man sich nun diesem Thema nähern?

Banken bzw. Unternehmen müssen in einem wettbewerbsintensiven Marktumfeld versuchen, Wettbewerbsvorteile gegenüber ihren Konkurrenten zu erzielen. Wie Wettbewerbsvorteile generiert werden können, wurde intensiv erforscht. Eine der einflussreichsten Publikationen dazu verfasste Michael E. Porter[1], ein renommierter, amerikanischer Wirtschaftswissenschaftler. Er formulierte die These, dass sich Unternehmen nur auf zwei Wegen Vorteile verschaffen können: Entweder sie realisieren Kostenvorteile (Strategie der Kostenführerschaft) oder sie konzentrieren sich auf die Erzielung von Leistungsvorteilen (Strategie der Qualitätsführerschaft). Ergänzt werden diese beiden Differenzierungsmerkmale durch das Konzept der Kernkompetenzen, das maßgeblich von den beiden amerikanischen Ökonomen Hamel und Prahalad[2] entwickelt wurde.

Auslagerungen können demnach der Bank bzw. einem Unternehmen Wettbewerbsvorteile verschaffen, wenn sie

- die Kostenposition und/oder
- die Qualität verbessern und/oder
- die Kernkompetenzen stärken.

Der erste Punkt verweist auf die monetären Gründe für eine Auslagerungsentscheidung. Eine Bank lagert dann aus, wenn der Auslagerer preiswerter produziert bzw. verkauft als man selber. Im Folgenden soll auf die beiden anderen Komponenten „Qualität“ und „Kernkompetenz“ näher eingegangen werden.

[1] Wettbewerbsvorteile (Competitive advantage), Michael E. Porter, Frankfurt, M.: Campus-Verl., 2014, 8., durchges. Aufl.

[2] Wettlauf um die Zukunft: wie Sie mit bahnbrechenden Strategien die Kontrolle über Ihre Branche gewinnen und die Märkte von morgen schaffen, Gary Hamel/C. K. Prahalad, Wien: Ueberreuter, 1997

Qualitätssteigerung

Können Auslagerungen bei Banken im aufsichtsrechtlichen Beauftragtenwesen die Qualität fördern?

Funktionen im aufsichtsrechtlichen Beauftragtenwesen sind bei Genossenschaftsbanken selten Fulltime-Jobs. Meist ist die Hauptfunktion des Beauftragten eine andere. Oder er vereinigt auf seine Stelle gleich mehrere Beauftragtenfunktionen, sofern daraus kein Interessenkonflikt erwächst. In beiden Fällen ist die Spezialisierung des Stelleninhabers nicht optimal. Er oder sie erledigt diese Aufgabe „nur“ nebenher oder zusätzlich. Dieser Teilzeit-Beauftragte wird qualitativ immer einem Vollzeit-Profi unterlegen sein, der sich seiner Aufgabe rund um die Uhr und ausschließlich widmen kann. Hat dieser Profi dann noch den Vorteil, dass er bei seinen Aufgaben über den Tellerrand blicken kann, weil er für andere Banken ebenfalls tätig ist, wird der Qualitätsvorsprung noch ausgeprägter.

Es ist also unmittelbar einsichtig, dass im Beispiel des aufsichtsrechtlichen Beauftragtenwesens durch die Auslagerung Qualitätsvorteile erzielt werden können.

Das trifft regelmäßig auf Tätigkeiten zu, die das auslagernde Unternehmen aufgrund ihres zeitlichen Umfanges oder ihrer Spezifik nicht so professionell – bezogen auf die zur Verfügung stehende Zeit, aber auch hinsichtlich der fachlichen Qualifizierung und Erfahrung – ausüben kann wie ein Auslagerungsunternehmen, das sich genau auf dieses Segment konzentriert.

Stärkung der Kernkompetenz

Wie steht es nun um die Kernkompetenzen? Können Auslagerungen die Kernkompetenzen einer Bank stärken?

Eine Kernkompetenz wird durch vier Eigenschaften charakterisiert: >

1. Kundennutzen: Kann die Bank auf Basis dieser Kernkompetenz einen nachhaltigen Mehrwert für den Kunden erzielen?
2. Imitationsschutz: Beherrscht die Bank die Kernkompetenz exklusiv, oder kann sie vom Wettbewerber leicht imitiert werden?
3. Differenzierung: Führt die Kernfähigkeit zu einem nachhaltigen Vorteil gegenüber der Konkurrenz?
4. Diversifikation: Bietet die Kernfähigkeit potenziellen Zugang zu neuen Märkten?

Betrachten wir wieder die Auslagerung von aufsichtsrechtlichen Beauftragtenfunktionen, konkret die Auslagerung der WpHG-Compliance.

Wenn die örtliche Genossenschaftsbank die beste WpHG-Compliance in der Region hat, verschafft sie sich dadurch einen Wettbewerbsvorteil, den der Kunde honoriert? Wechselt der Sparkassen-Kunde oder der Großbankkunde am Ort seine Bankverbindung, weil die Genossenschaftsbank die beste WpHG-Compliance bietet? Der Kunde wird leider in der Mehrzahl der Fälle überhaupt nicht wissen, was eine WpHG-Compliance ist, geschweige denn, was sie ihm bietet. Der Aufbau eines Kundennutzens ist also schwer möglich, wenn er in der Erfahrungswelt eines Kunden nicht einmal vorkommt.

Und wie steht es mit dem Imitationsschutz? Bleiben wir bei der WpHG-Compliance. Von Exklusivität kann keine Rede sein, denn durch die Auslagerung kann sie jeder Wettbewerber ebenfalls einkaufen. Auch wenn die Bank die Beauftragtenfunktion selber darstellt, ist durch die gesetzliche Normierung ein Imitationsschutz geradezu untersagt.

Bei der Differenzierung sieht es ähnlich aus. Auch hier sorgt die gesetzliche Normierung für gleiche Wettbewerbsbedingungen („level playing field“). Eine Differenzierung ist quasi gesetzlich verboten, unabhängig davon, ob eine Auslagerung stattfindet oder die Bank die Funktion selber ausführt.

Die letzte Chance wäre nun die Diversifizierung. Kann die Bank sich durch die Auslagerung von aufsichtsrechtlichen Beauftragtenfunktionen neue Märkte erschließen? Auch hier ist die Antwort wieder negativ. Entweder unterliegen die neuen Märkte aufsichtsrechtlichen Anforderungen oder nicht. Wenn ja, sind alle Wettbewerber verpflichtet, diese Funktionen in gefordertem Umfang anzubieten. Wenn nein, können alle Wettberber darauf verzichten.

AUTOR UND ANSPRECHPARTNER

Martin Hierlemann
Leiter Vertrieb,
E-Mail: martin.hierlemann@dz-cp.de

Im Ergebnis heißt das, dass Banken zumindest bei Auslagerungen im aufsichtsrechtlichen Beauftragtenwesen keine Kernkompetenzen aufbauen oder verlieren können. Zumindest im betriebswirtschaftlichen Sinne. Das ist aber auch andererseits tröstlich, da viele Banken befürchten, sie gäben (betriebswirtschaftliche) Kernkompetenzen aus der Hand, wenn sie Funktionen im Beauftragtenwesen auslagern. Dies ist zumindest nach der obigen Argumentationslinie eindeutig widerlegbar.

Fazit

Im aufsichtsrechtlichen Beauftragtenwesen sind also letztlich zwei Komponenten für die Auslagerungsentscheidung maßgebend: eine finanzielle Komponente und eine nicht finanzielle Komponente. Bei der finanziellen Sicht spielen die Kosten/Preise der Auslagerung die entscheidende Rolle und bei der nicht finanziellen Sicht die Qualität.

Ob eine der beiden Komponenten eine stärkere Rolle spielt als die andere, oder ob beide gleichgewichtig in die Entscheidungsfindung einfließen, muss jede Bank für sich entscheiden. Preise und Qualität sind auf jeden Fall die entscheidenden Treiber der Auslagerungsentscheidung im aufsichtsrechtlichen Beauftragtenwesen, die (betriebswirtschaftlichen) Kernkompetenzen spielen hierbei keine Rolle. ▬

Informationssicherheit

Kapitalverwaltungsaufsichtliche Anforderungen an die IT

Die BaFin hat den Entwurf des Rundschreibens „Kapitalverwaltungsaufsichtliche Anforderungen an die IT (KAIT)“ zur Konsultation gestellt.

AUTOR UND ANSPRECHPARTNER

Michael Switalla
Leiter Informationssicherheit & Datenschutz,
E-Mail: michael.switalla@dz-cp.de

Die BaFin hat sich in den vergangenen Jahren in ihren Bankaufsichtlichen Anforderungen an die IT (BAIT) bereits dazu geäußert, wie Banken ihre IT-Ressourcen, ihre Informationsrisiken und ihre Informationssicherheit organisieren und überwachen sollen. Nun konsultiert sie auch ihre Kapitalverwaltungsaufsichtlichen Anforderungen an die IT (KAIT).

Das BaFin-Rundschreiben zielt darauf ab, die IT-Sicherheit im Markt zu erhöhen und das IT-Risikobewusstsein in den Kapitalverwaltungsgesellschaften (im Sinne des § 17 Kapitalanlagegesetzbuch (KAGB), soweit diese über eine Erlaubnis nach § 20 Absatz 1 KAGB verfügen) zu schärfen. Es enthält Hinweise zur Auslegung der nationalen und europarechtlichen Vorschriften über die Geschäftsorganisation, soweit sie sich auf die technisch-organisatorische Ausstattung der Kapitalverwaltungsgesellschaften beziehen.

Mit dem Rundschreiben will die BaFin eigenen Angaben zufolge einen „flexiblen und praxisnahen Rahmen für die technisch-organisatorische Ausgestaltung der IT“ vorgeben, insbesondere für das Management der IT-Ressourcen und für das IT-Risikomanagement. Darüber hinaus regelt das Rundschreiben den Umgang mit Auslagerungen von IT-Aktivitäten und IT-Prozessen.

Dem Rundschreiben zufolge müssen künftig alle Kapitalverwaltungsgesellschaften (KVG) Leitlinien zur Informationssicherheit (IT-Strategie und IT-Governance) definieren und dokumentieren. Die wichtigsten Neuerungen sind zusammengefasst:

- Auch KVG müssen nun die Informationsrisiken aktiv managen, d. h., die jeweiligen Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen und Kommunikationswege zu definieren, aufeinander abzustimmen, zu überwachen und zu steuern.
- Das Informationssicherheitsmanagement obliegt dabei einem Beauftragten für Informationssicherheit, den die KVG zu ernennen hat. Er stellt innerhalb seiner Funktion sicher, dass die in der IT-Strategie, in der Informationssicherheitsleitlinie und in den Informationssicherheitsrichtlinien der KVG niedergelegten Ziele und Maßnahmen – sowohl intern als auch gegenüber Dritten – transparent gemacht werden und deren Einhaltung überprüft und überwacht wird.
- Ein Benutzerberechtigungsmanagement soll gewährleisten, dass den Benutzern eingeräumte Berechtigungen so ausgestaltet sind und genutzt werden, wie es den organisatorischen und fachlichen Vorgaben der KVG entspricht.
- Wesentliche Veränderungen in den IT-Systemen im Rahmen von IT-Projekten, deren Auswirkung auf die IT-Aufbau- und IT-Ablauforganisation sowie die dazugehörigen IT-Prozesse sind vorab im Rahmen einer Analyse des Risikogehalts zu bewerten.
- Der IT-Betrieb inkl. Datensicherung wird geregelt, ebenso wie Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen.

Zusammenfassend zollt das Rundschreiben dem faktischen Bedeutungszuwachs der Informationstechnik in den Kapitalverwaltungsgesellschaften Rechnung. Letztlich steht dahinter die zu begrüßende Intention, die IT- und Datensensibilität, die Datenmengen und die unterschiedlichen beteiligten Systeme mithilfe von (Mindest-)Standards in den Griff zu bekommen. Wir stehen Ihnen dabei gerne mit unseren Erfahrungen beratend bzw. als ausgelagerte Funktion zur Verfügung, sprechen Sie uns an. ▬

Interne Revision

Seit der letzten Berichterstattung in der Point of Compliance (2/2019, S. 23) wurden folgende Berichte veröffentlicht:

- als letzter aus der Jahresprüfungsplanung 2018: „Innenrevision im IT-Bereich“,
- aus der aktuellen Jahresprüfungsplanung im Juni 2019: „IT & Projekte/Allgemeine Betriebsorganisation/Dienstleistersteuerung“ und „WpHG-Compliance“.

Letzterer wurde als dienstleistungsbezogener Bericht an unsere Mandantschaft versandt. Der Bericht für den Bereich MaRisk-Compliance ist derzeit in der Endabstimmung. Zudem wurden die Quartalsberichte zum ersten und zweiten Quartal 2019 erstellt und versandt.

Die Abarbeitung des internen Jahresprüfungsplanes für 2019 verläuft weiterhin planmäßig. Von den aus dem Jahr 2018 übertragenen Prüfungen wurde „IT & Projekte“ bereits abgeschlossen (siehe oben), die der Bereiche „Informationssicherheit & Datenschutz“ und „IT-Audit“ sind für das zweite Halbjahr 2019 vorgesehen.

Die externe Prüfung der Geschäftsbereiche MaRisk-Compliance, WpHG-Compliance und Zentrale Stelle nach IDW PS 951 (Typ 2) wurde von der Ernst & Young GmbH Wirtschaftsprüfungsgesellschaft durchgeführt. Es wurde jeweils ein Testat ohne wesentliche Einschränkung erteilt.

Die externe Prüfung der Funktion Hinweisgebersystem nach IDW PS 331 – ebenfalls durch die Ernst & Young GmbH Wirtschaftsprüfungsgesellschaft – wurde mit einem uneingeschränkten Testat beendet.

Darüber hinaus wurde turnusgemäß je ein Follow-up-Quartalsbericht für das erste und zweite Quartal 2019 erstellt und der Geschäftsführung der DZ CompliancePartner fristgerecht vorgelegt. In den Follow-up-Berichten wird die Abarbeitung der von internen und externen Prüfern getroffenen Maßnahmen/Empfehlungen dokumentiert. Insgesamt ist die Anzahl der offenen Punkte gesunken, obwohl – sowohl von internen als auch von externen Berichten – neue Feststellungen in die Gesamtbewertung einflossen. Dies zeigt, dass die in vorangegangenen Prüfungen gemachten Feststellungen konsequent abgearbeitet werden.

Als weiterer Informationsaustausch finden zwischen dem Sprecher der Geschäftsführung der DZ CompliancePartner und der Internen Revision regelmäßige Jours fixes statt. ▬

Ansprechpartner: ***Lars Schinnerling,*** *Leiter Interne Revision, E-Mail: lars.schinnerling@dz-cp.de*

Wirtschaftliche Lage

Auch das zweite Quartal 2019 ist für die DZ CompliancePartner positiv verlaufen. Die Erträge lagen bei 3.956 TEUR und damit 164 TEUR, d. h. 4 %, über Plan. Die Planüberschreitung war u. a. von unterstützenden Dienstleistungen und Teilauslagerungen wie Geno-SONAR®- und MAR-Trefferanalytiken, Risikoanalysen sowie Datenschutz- bzw. BAIT-Checkups getragen.

Die Aufwände (inkl. außerordentlicher Aufwand) lagen bei –3.142 TEUR und damit +292 TEUR unter Plan. Die Planunterschreitung resultiert u. a. aus Verschiebungen von Aufwänden vom zweiten Quartal in die folgenden Monate. Insbesondere die mit der Integration des Geschäftsfeldes Geldwäsche-Insourcing der DZ BANK erforderlichen „Investitionen“ in das Rechenzentrum und die Dienstleistungsprozesse werden erst im zweiten Halbjahr (und auch noch im Folgejahr) wirksam.

Die Liquiditätssituation ist unverändert entspannt, die wirtschaftliche Lage der DZ CompliancePartner stabil. ▬

Ansprechpartner: ***Jens Saenger,*** *Sprecher der Geschäftsführung, E-Mail: jens.saenger@dz-cp.de*

IMPRESSUM

Point of Compliance
Das Risikomanagement-Magazin für unsere Kunden und Geschäftspartner, Ausgabe 21, 3/2019
ISSN: 2194-9514
Herausgeber: DZ CompliancePartner GmbH, Wilhelm-Haas-Platz, 63263 Neu-Isenburg, Telefon 069 6978-3324, Telefax 069 6978-3322, www.dz-cp.de
Handelsregister HRB 11105, Amtsgericht Offenbach, USt.-IdNr.: DE201150917
Geschäftsführung: Jens Saenger (Sprecher), Andreas Marbeiter, Norbert Schäfer

Verantwortlich i. S. d. P. : Jens Saenger
Redaktion: Gabriele Seifert, Leitung (red.)
Redaktionsanschrift: DZ Compliance-Partner GmbH, Redaktion Point of Compliance, Wilhelm-Haas-Platz, 63263 Neu-Isenburg, Telefon 069 6978-3188, Telefax 069 6978-3322, E-Mail: poc@dz-cp.de
Weitere Autoren dieser Ausgabe:
Florian Brüderle, Thomas Grebe, Martin Hierlemann, Axel Hofmeister, Andreas Marbeiter, Norbert Schäfer, Jörg Scharditzky, Lars Schinnerling, Michael Switalla, Thomas Wagener

Bildnachweise: DZ CompliancePartner GmbH, iStockphoto (Titel, Seite 6, Seite 21)
Gestaltung: EGENOLF DESIGN, Wiesbaden, studio@egenolf-design.de
Druck: odd GmbH & Co. KG · Print und Medien, www.odd.de

Redaktionsschluss: 15. August 2019
Auflage: 2.600 Exemplare
Die aktuellen Mediadaten finden Sie im Internet unter www.dz-cp.de/poc