Christiane Schröder

Zunehmende **Digitalisierung** erfordert systematisches Compliance Management

Bedürfnisse von Kunden, die zunehmend digital agieren, führen zu neuen Zahlungs- und Kommunikationsdienstleistungen. So haben Banken und Sparkassen mit Paydirekt ein Onlinebezahlverfahren entwickelt, um Konkurrenten wie Paypal und Cringle auf einem zunehmend digital geprägten Markt etwas entgegenzusetzen. Nicht nur Direktbanken bieten eine breite Palette von Produkten an, die keine Beratung in der Filiale erfordern, auch Kreditinstitute, die in der Vergangenheit vorrangig auf ihre deutschlandweite physische Präsenz gesetzt haben, ziehen nach. Laut Angaben des Bankenverbandes nahm die Zahl der inländischen Zweigstellen seit dem Höhepunkt im Jahre 1995 stetig ab. Lag sie 1995 noch bei 68000, so wurden 2012 nur noch 36000 Zweigstellen verzeichnet. Laut Branchenkompass Banking von Sopra Steria Consulting plant jede dritte Bank in Deutschland bis 2017 Filialen in nennenswertem Umfang zu schließen.

Mit dem Wandel der Produkt- und Servicelandschaft verändern sich auch die Anforderungen an das Compliance Management. Durch Cybercrime entstehen Kreditinstituten Schäden in Millionenhöhe. Die Angriffsmuster werden zunehmend komplexer. Kaum ist ein Muster erkannt, werden neue Strategien entwickelt. Ein systematisches Management erfordert unter anderem die eingehende Analyse der sich verändernden Bedingungen, die Durchsetzung gezielter Maßnahmen sowie die Implementierung leistungsfähiger automatisierter IT-Lösungen.

Deutschland stark betroffen

Laut einer Studie des Center for Strategic and International Studies, die 2014 in Zusammenarbeit mit McAfee veröffentlicht wurde, ist Deutschland unter den mehr als fünfzig analysierten Ländern am stärksten von Cybercrime betroffen. Gemäß der Studie belaufen sich die Schäden, die beispielsweise durch Finanzverbrechen, den Verlust von geistigem Eigentum oder Marktmanipulationen entstehen, auf 1,6 Prozent des Bruttoinlandsprodukts. Viele Finanzdienstleister sind aufgrund ihres Leistungsspektrums besonders gefährdet.

Durch die Kombination unterschiedlicher Methoden werden die Angriffsstrategien immer komplexer. So entstand der Bank of Muscat im Jahr 2013 innerhalb von zehn Stunden ein Schaden über 30 Millionen Euro. Nach der Manipulation von Auszahlungslimits tätigten Mittelsmänner mit Duplikaten der gehackten Kreditkarten zirka 36000 Abhebungen in 24 Ländern. Laut einem Bericht der Welt machten Sicherheitslecks der Bank und einer indischen Filiale einer US-Firma für internationalen Zahlungsverkehr den Coup möglich.

Ringen um die besseren Strategien und Techniken – Beispiel Phishing

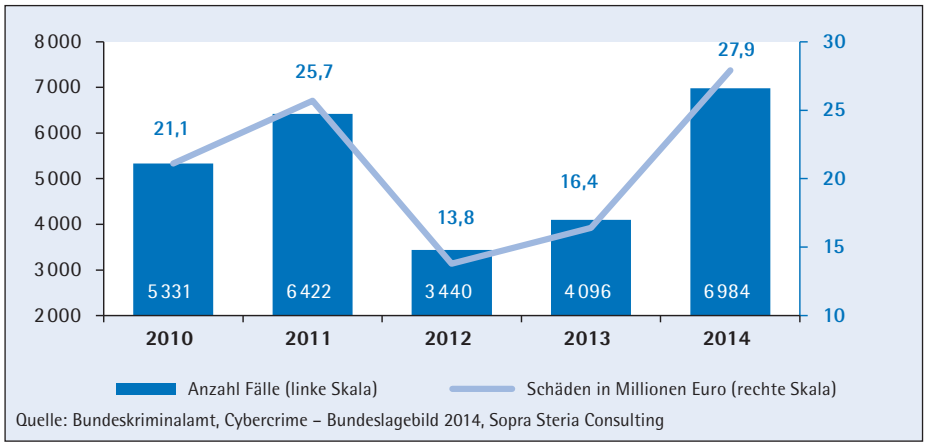
Doch nicht nur Täter nutzen neue Techniken, um immer wieder neue Angriffsstrategien zu ersinnen, auch die Banken entwickeln mit den neuen Produkten und Plattformen innovative Maßnahmen, um sich zu schützen. Die Entwicklung von Schadensfällen beim Phishing im Zusammenhang mit Onlinebanking in Deutschland spiegelt das stete Ringen um die passenden Bekämpfungsstrategien wider. 2012 konnten die Fallzahlen nach Schutzmaßnahmen, wie dem Einführen des auf mobilen Transaktionsnummern basierenden m-Tan-Verfahrens und der stärkeren Sensibilisierung der Anwender, im Vergleich zu 2011 von 6422 auf 3440 fast halbiert werden. Allerdings haben die Fallzahlen 2014 bei vergleichbaren durchschnittlichen Schadenshöhen wieder ein höheres Niveau von 6984 erreicht. Die 2012 etablierten Tan-Verfahren konnten durch Echtzeitmanipulation angegriffen werden. Die Software zur Manipulation von Smartphone-Betriebssystemen ist auf digitalen Schwarzmärkten wie Silk Road, Evolution oder Agora erhältlich (Abbildung 1).

Mit der zunehmenden Digitalisierung verändert sich auch die Bedrohungslage der Kreditinstitute. Das betrifft nicht nur das operative Risikomanagement, sondern auch die regulatorischen Themen, wie die Gefährdungsanalyse zur Verhinderung von Geldwäsche, Terrorismusfinanzierung und die sogenannten sonstigen strafbaren Handlungen. Die angeführten Beispiele verdeutlichen, dass aufgrund der dynamischen Entwicklung immer neuer Angriffsmuster kaum ein System geschaffen werden kann, das ein Kreditinstitut im Vorfeld vor allen denkbaren Angriffen schützt. Vielmehr geht es darum, ein Compliance-Management-System zu entwickeln, das der spezifischen Institutssituation gerecht wird. Dies erfolgt einerseits durch das Identifizieren potenzieller Risiken und Angriffsmuster auf Basis der Produkte, Kundengruppen, Vertriebskanäle und Länder, in denen das Institut aktiv ist, sowie

Christiane Schröder, Senior Consultant Banking, Sopra Steria Consulting, Hamburg

Aufgrund immer neuer Angriffsszenarien kann kein System geschaffen werden, das ein Kreditinstitut vor allen zukünftigen Bedrohungen aus dem virtuellen Raum zu 100 Prozent schützt. Um dieser Tatsache Rechnung zu tragen, dringt die Autorin darauf, dass Kreditinstitute regelmäßig die aktuelle Gefährdungslage prüfen, Datenverarbeitungssysteme auf institutsspezifische Parameter einstellen und angemessene IT-Lösungen, das heißt auch statistische Verfahren und Big-Data-Technologien zum Einsatz bringen. (Red.)

Abbildung 1: Phishing im Onlinebanking 2010 bis 2017



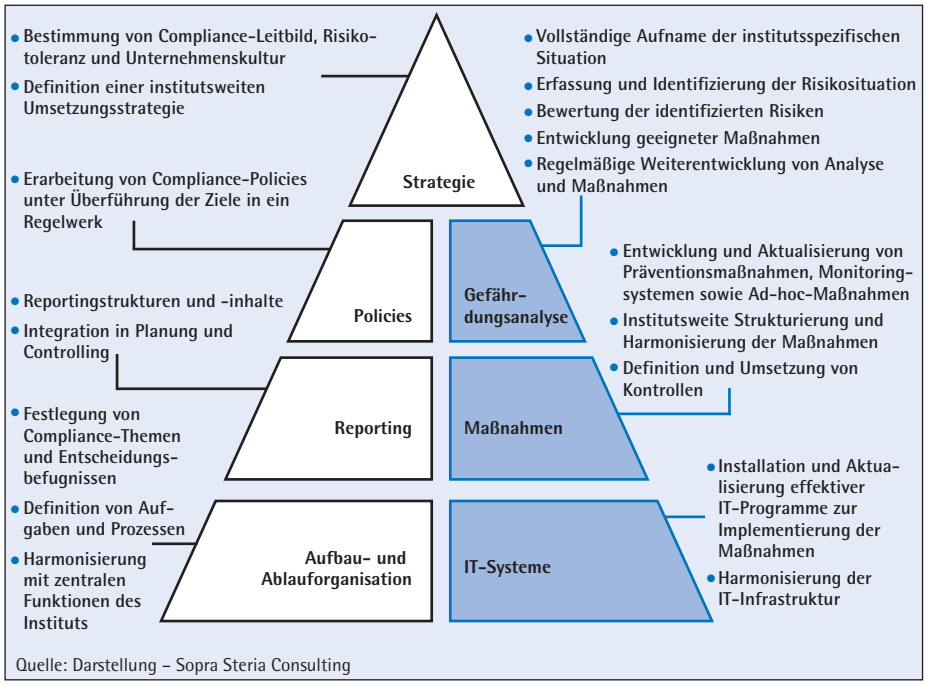
Quelle: Bundeskriminalamt, Cybercrime – Bundeslagebild 2014, Sopra Steria Consulting

andererseits durch das Lernen aus historischen Fällen und Schäden, die bei vergleichbaren Instituten aufgetreten sind.

Gefährdungsanalyse mindestens einmal pro Jahr

Ein zentrales Instrument für die Überprüfung der Ausrichtung des Compliance-Management-Systems ist die mindestens jährlich durchzuführende Gefährdungsanalyse. Um mit den neuen Anforderungen Schritt zu halten, müssen Compliance-Management-Systeme zudem laufend an die neuen Bedingungen angepasst werden. Ein wichtiges Element ist hierbei die ausreichende Berücksichtigung der an den digitalen Kundengruppen ausgerichteten Produkt- und Serviceangebote, insbesondere im Zahlungsverkehrsbereich. Die Reaktionsfähigkeit in der Abwehr von Angriffsszenarien hängt entscheidend von der Geschwindigkeit der Datenverarbeitung, von der Automatisierung der Prozesse sowie von der Vernetzung der unterschiedlichen Datensysteme ab. Auch steigende regulatorische Anforderungen, die aus den Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSi) und aus der überarbeiteten Zahlungsdiensterichtlinie (PSD II) erwachen, zeigen den Handlungsbedarf.

Abbildung 2: Bausteine eines Compliance-Management-Systems



Quelle: Darstellung – Sopra Steria Consulting

Die Anpassungserfordernisse betreffen die gesamte Compliance-Organisation von der Strategie bis zur Aufbau- und Ablauforganisation. Bei bestimmten Bausteinen des Compliance-Management-Systems können Investitionen besonders wirksam sein, um Effizienz und Effektivität zu steigern (siehe Abbildung 2).

Gefährdungsanalyse: Die Herausforderung für Kreditinstitute besteht in vielen Fällen darin, die Hauptrisikotreiber im Rahmen der Gefährdungsanalyse zu identifizieren und daraus wirtschaftlich sinnvolle Maßnahmen abzuleiten. Wie bereits im Kreditwesengesetz angelegt, erfordert die Digitalisierung eine stärkere Fokussierung auf Datenverarbeitungssysteme, insbesondere zur flächendeckenden Überwachung von Kundenkonten und Zahlungsvorgängen. Werden die größten Risiken erkannt, können Schäden effizient und effektiv abgewendet werden.

Sopra Steria Consulting hat 2013 einen **„Proof of Concept"** auf Basis von SAP HANA® durchgeführt. Darin wurde ein konventionelles Anti-Financial-Crime-Regelwerk bestehend aus 150 einzelnen Regeln implementiert. Während die konventionelle Lösung basierend auf relationaler Datenbanktechnologie für die Monatsverarbeitung von zehn Millionen Kunden und 110 Millionen Transaktionen bis zu 100 Stunden benötigt, schloss die In-Memory-Anwendung nach vier Minuten ab. Für eine komplette Tagesendverarbeitung wurden etwa elf Sekunden benötigt, für das Transaktionsvolumen einer Viertelstunde nur noch zirka 0,4 Sekunden. So ist der Abgleich von Massendaten mit Mustern nahezu in Echtzeit möglich. Die Transaktion kann angehalten werden, bevor das Geld die Bank verlässt.

Maßnahmen: Die Datenverarbeitungssysteme sollten auf angemessenen Parametern basieren, die auf anerkanntem Erfahrungswissen über die Prävention von Geldwäsche, Terrorismusfinanzierung oder sonstiger strafbarer Handlungen beruhen. Die Parametrisierung ist institutsspezifisch zu erstellen, hierbei sind insbesondere die neuen Produkte und Dienstleistungen zu berücksichtigen: Welche Nutzergruppen gibt es? Welche Transaktionen sind für die

unterschiedlichen Nutzergruppen zu erwarten, in Bezug auf Höhe, Frequenz sowie Sender und Empfänger? Welche spezifischen Risiken gibt es? Ist ein Schwellenwert ungünstig gesetzt, so kann es zu einem unverhältnismäßig hohen Bearbeitungsaufwand und gegebenenfalls auch zu Geldstrafen aufgrund von Bearbeitungsrückständen führen. Ziel einer adäquaten Parametrisierung ist es, ein wirtschaftlich sinnvolles Verhältnis zwischen Aufwand und verhindertem Schaden zu erzielen.

Statistische Verfahren und Big-Data-Technologien

IT-Systeme: Zur schnellen Erkennung von Anomalien und potenziellen Angriffen erfordert es den Einsatz adäquater IT-Lösungen. Eine verbesserte Detektion strafbarer Handlungen ist nur möglich, wenn sich der Kontext der Transaktion hinreichend beurteilen lässt. Um jährlich Milliarden von Transaktionen und die damit verbundenen Beziehungsnetze zu analysieren und Betrugsmuster zu antizipieren, kommen statistische Verfahren und Big-Data-Technologien wie „Predictive Analytics" zum Einsatz. Muster können über die Kombination von sachlichen, geografischen sowie persönlichen Eigenschaften von Transaktionen, Konten und Kunden erkannt werden.

Durch Softwareanwendungen, die mit In-Memory-Technologien arbeiten, kann der Analyseprozess um ein Vielfaches beschleunigt und auch bei großen Datenmengen auf wenige Minuten reduziert werden. Viele Kreditinstitute arbeiten noch mit konventionellen Verfahren, obwohl eine stufenweise Einführung eine sanfte Transformation ermöglicht.

Aufgrund der verstärkten Nutzung innovativer Zahlungsmethoden sowie steigender regulatorischer Anforderungen an die Sicherheit des Internetzahlungsverkehrs ist zu erwarten, dass der Druck auf Kreditinstitute weiter wächst. Wird ein systematisches Compliance Management durch leistungsfähige IT-Lösungen ergänzt und regelmäßig an die sich verändernden Bedingungen angepasst, können Schadenshöhen effektiv und effizient reduziert werden. Angesichts von Schäden in Millionenhöhe lohnt sich die Investition in eine systematische Analyse und die Implementierung von IT-Lösungen, die auf Big-Data-Technologien beruhen.