Protokoll

der Sitzung des Fachgremiums IT am Freitag, 14.10.2016, 10:30 Uhr bis 16 Uhr im Hause der Bundesanstalt für Finanzdienstleistungsaufsicht, Bonn.

TOP 1: Begrüßung und Vorstellung
RL BA 51 begrüßte die Teilnehmer und wies auf den gegenüber der letzten Sitzung erweiterten Teilnehmerkreis hin. Es folgte eine kurze Vorstellungsrunde.

TOP 2: Annahme des Protokolls der letzten Sitzung
Das Protokoll der letzten Sitzung wurde angenommen.

TOP 3: Besprechung eines Entwurfs des BAIT-Moduls „Informationssicherheitsmanagement"
Zu Beginn der Diskussion wurden von Seiten der Kreditwirtschaft zwei Folien vorgestellt, die sich mit der Abgrenzung der Begriffe „Informationssicherheitsrisiken", „IT-Risiken" und „Cyber-Risiken" bzw. dem Unterschied zwischen „Informationssicherheits-management" und „IT-Sicherheitsmanagement" beschäftigten. Danach widme sich das IT-Sicherheitsmanagement dem Schutz elektronisch gespeicherter Informationen, während das Informationssicherheitsmanagement auch Informationen umfasse, die auf Papier oder nur in den Köpfen der Mitarbeiter vorhanden seien.

Von Seiten der Aufsicht wurde erläutert, dass das entsprechende Modul den Titel „Informationssicherheitsmanagement" trage, weil dieser Begriff sich zunehmend durchsetze und beispielsweise auch vom BSI verwendet werde. Von Seiten der Kreditwirtschaft wurde angemerkt, dass man prüfen müsse, ob dieser Begriff für alle Module passe, da Sicherheitsfragen ganz ohne IT-Bezug wohl nicht in den BAIT geregelt werden sollen. Auch wurde der Wunsch nach klaren Begriffsdefinitionen, bspw. in einem Glossar, geäußert.

Auch wurde von Vertretern der Kreditwirtschaft angemerkt, dass es ihnen schwerfalle, den Entwurf dieses Moduls in die Gesamtstruktur der BAIT einzuordnen, da noch nicht Entwürfe für alle Module vorlägen. Von Seiten der Aufsicht wurde versichert, dass bis zur geplanten zweitägigen Sitzung im Dezember Entwürfe zu allen Modulen vorliegen sollten; dann bestehe auch Gelegenheit, über das weitere Vorgehen zu sprechen.

In diesem Zusammenhang wurde auch das Thema Proportionalität angesprochen. Von Seiten der Aufsicht wurde hierzu bemerkt, dass dieser Gesichtspunkt in einer Präambel zu den Modulen angesprochen werden wird. Grundsätzlich liege es in der Verantwortung der Geschäftsleitung, die Anforderungen der BAIT in einer zu Größe, Geschäftsmodell und Risiko des Instituts proportionalen Art und Weise umzusetzen.

Im Folgenden wurden die einzelnen Textziffern des Entwurfs besprochen. Soweit Einigkeit über Änderungen erzielt wurde oder die Aufsicht Nachbesserungsbedarf bei einzelnen Punkten identifizierte, wurden unmittelbar in der Sitzung entsprechende Änderungen oder Kommentare in ein elektronisches Dokument eingefügt. Nachfolgend werden deshalb nur die wichtigsten Punkte der Diskussion erwähnt.

Es bestand Konsens, dass die Informationssicherheitsleitlinien nicht nur im Einklang mit der IT-Strategie des Instituts, sondern mit allen seinen Strategien stehen müssen.

Kontrovers wurde über den Begriff „Stand der Technik" diskutiert. Von Seiten der Kreditwirtschaft wurde zum Teil argumentiert, dass es im Bereich der IT keine allgemein anerkannte Definition des Terminus „Stand der Technik" gebe. Von Seiten der Aufsicht

wurde betont, dass man mit dieser Formulierung nicht verlangen wolle, stets die neuesten auf dem Markt verfügbaren Produkte zu verwenden, wenn Abweichendes unter Risikogesichtspunkten zu vertreten sei. Die Formulierung solle aber noch einmal überprüft werden.

In Bezug auf den Informationssicherheitsbeauftragten wurde diskutiert, wie das an verschiedenen Stellen verwendete Wort „Mitwirkung" zu verstehen sei. Es geht nach Auskunft der Aufsicht nicht darum, dass der Beauftragte zum Beispiel als Projektbeteiligter mitarbeitet; er sei vielmehr zu beteiligen, so dass er die Belange der Informationssicherheit einbringen könne. Die entsprechenden Formulierungen sollen noch einmal überprüft werden.

Einige Vertreter der Kreditwirtschaft baten um Klarstellung, wie die Anforderung, dass der Informationssicherheitsbeauftragte nicht in die Hierarchie der operativen IT einbezogen sein soll, zu verstehen sei; auch hier sollen noch Klarstellungen, zum Beispiel im Glossar, erfolgen.
Von Seiten der Aufsicht wurde erläutert, dass – je nach Institut – die Tätigkeit des Informationssicherheitsbeauftragten keine Vollzeitstelle ausfüllen müsse; eine Kombination mit anderen Funktionen wie z.B. Geldwäsche-Beauftragter oder WpHG-Compliance-Beauftragter sei grundsätzlich möglich.

Anschließend wurde eine Formulierung diskutiert, die bestimmten Instituten, die nicht über wesentliche eigenbetriebene IT verfügen, die Möglichkeit geben würde, einen gemeinsamen Informationssicherheitsbeauftragten zu benennen. Einigen Teilnehmer aus der Kreditwirtschaft merkten an, dass diese Formulierung relativ stark auf verbundangehörige Institute zugeschnitten sei; die Belange der Auslandsbanken, die die die IT ihres Stammhauses verwendeten, so wie die der konzernangehörigen Banken seien nicht ausreichend berücksichtigt. Die Aufsicht sagte eine Prüfung dieser Anliegen zu.

Schließlich wurde noch beschlossen, die Formulierung der Meldeschwelle für Informationssicherheitsvorfälle zu schärfen.

TOP 4: Besprechung eines Entwurfs des BAIT-Moduls „Benutzerberechtigungsmanagement"

Auch in Bezug auf dieses Modul wurden die einzelnen Textziffern des Entwurfs besprochen. Soweit Einigkeit über Änderungen erzielt wurde oder die Aufsicht Nachbesserungsbedarf bei einzelnen Punkten identifizierte, wurden unmittelbar in der Sitzung entsprechende Änderungen oder Kommentare in ein elektronisches Dokument eingefügt. Nachfolgend werden wiederum nur die wichtigsten Punkte der Diskussion erwähnt:

Zu Anfang wurde diskutiert, ob sich das Modul nur auf die Berechtigungen zur Nutzung elektronisch gespeicherter Informationen beziehe, oder z.B. auch auf in Informationen in Papierform. Als Arbeitshypothese wurde eine Beschränkung auf elektronische Informationen vereinbart; im Nachgang ist zu prüfen, ob eine Erweiterung auf anderweitig gespeicherte Informationen sinnvoll sei.

Anschließend wurde die Frage diskutiert, welcher Grad von Granularität für das Berechtigungskonzept nötig sei; nach Ansicht der Aufsicht ist eine Ausführung bis auf die Ebene der Einzelberechtigungen (Soll/Ist) notwendig; fachlich reiche es grundsätzlich aus, wenn sich das Berechtigungskonzept auf die von der Software bereitgestellten

Benutzerrollen beschränke; eine Abbildung beispielsweise bis auf die hinter einzelne Transaktionen stehenden Datenbankzugriffe sei nicht notwendig.
Der Begriff „Laufzeit" in Bezug auf Berechtigungen wird gestrichen; von Seiten der Aufsicht wird klargestellt, dass es nicht erforderlich sei, alle Berechtigungen zu befristen.

Die Bedeutung der Begriffe persönliche und technische Berechtigungen wird bspw. im Glossar erklärt werden.

Es darf Nutzerkonten („Accounts") mit mehreren Nutzern geben, solange nachvollziehbar ist, wer das Konto in einer bestimmten Situation genutzt hat.

Die Formulierung „Interessenkonflikte" bezieht sich nur auf aufsichtlich relevante Interessenkonflikte.

Die Überprüfung des Berechtigungskonzepts hat vornehmlich anlassbezogen und unabhängig davon auch regelmäßig zu erfolgen. Bei der regelmäßig stattfindenden Prüfung soll vor allem eine Vergewisserung erfolgen, ob es seit dem Zeitpunkt der letzten Überprüfung Veränderungen oder Vorfälle gegeben hat, die eine Änderung des Benutzerberechtigungskonzepts notwendig machen. Wenn diese Änderung nichts bereits anlassbezogen erfolgt ist, ist sie dann nachzuholen.

Die Anforderung, dass die Benutzerkennungen die Nachvollziehbarkeit von Aktivitäten gewährleisten müssen, wurde gestrichen, da sie eine nicht gewollte Vollprotokollierung aller Tätigkeiten suggeriert.

In Bezug auf die Anforderung der technisch korrekten Umsetzung des Benutzerberechtigungen wurde klargestellt, dass – risikoorientiert – in manchen Konstellationen ein gewisser zeitlicher Versatz bei der Änderung von Benutzerberechtigungen möglich sein kann.

Anschließend fand eine längere Diskussion zum Prozessumfang bei der Rezertifizierung statt. Die Tendenz der Diskussion ging dahin, dass die Rezertifizierung nicht den Umfang eines Neuantrags haben müsse, es jedoch erforderlich sei, dass der Linienvorgesetzte zustimme. Die einzelnen Berechtigungsrollen sind regelmäßig zu überprüfen.

Im Hinblick auf die Notwendigkeit, nach Maßgabe des Schutzbedarfs Protokollierungs- und Überwachungsprozesse einzurichten, wurde von Seiten der Kreditwirtschaft angeregt klarzustellen, dass die Aufsicht keine umfassende Mitarbeiterüberwachung vorschreibe; es müsse um den Schutz gegen die betrügerische (alternativ: „unrechtmäßige" bzw. „missbräuchliche") Benutzung von Berechtigungen gehen (genaue Formulierung ist noch zu klären). Auch sollten statt der Überwachung angemessene andere Maßnahmen zulässig sein.

TOP 5: Sonstiges
Es wurde beschlossen, dass die nächste Sitzung des Fachgremiums IT zweitägig am 15. und 16. Dezember 2016 stattfindet.

Von Seiten der Aufsicht wurde auf die gerade angelaufene Konsultationsperiode für die EBA-Leitlinien zur Beurteilung von IT-Risiken im Rahmen des SREP hingewiesen.

Schließlich berichtete die Aufsicht noch, dass sie eine Reihe von Bürgeranfragen zur aufsichtlichen Beurteilung des iTAN-Verfahrens erhalten habe. In diesem Zusammenhang betonte die Aufsicht, dass dieses Verfahren nicht den Anforderungen der Zweiten

Zahlungsdiensterichtlinie (PSD2) entspreche. Diese Anforderungen werden im Laufe des Jahres 2018 in Kraft treten. Die Aufsicht würde es daher begrüßen, wenn die Kreditinstitute bereits jetzt Projekte initiierten, die eine vollständige Umstellung auf andere Authentifizierungsverfahren zum Ziel hätten.

Anlage 1: Teilnehmer

Hans Köster	FinanzInformatik
Dr. Andreas Abel	Fiducia & GAD IT AG
André Nash	BdB
Michael Schwirten	DSGV
Dr. Friedrich Zuther	BVR
Michael Rabe	VÖB
Elke Willy	VAB
Oliver Semmler	BWF
Lothar Galonska	VdB
Dr. Judith Wunschik	DiBa
Hinrich Voelker	Deutsche Bank
Stefan Böse	DZ Bank
Christopher Nolte	CoBa
Ulrich Haumann	UniCredit
Arne Tieves	HSH Nordbank
Andreas Fichelscher	KfW
Stefan Finkenzeller	Bayern LB
Christoph Bernius	Helaba
Daniel Konrad	LBBW
Dr. Heino Gärtner	Nord-LB
Dr. Thomas Mangel	Postbank Systems
Felix Kaiser	BHS
Peter Höges	IKB
Jakob Mayer	RBB

Thorsten Stichter	MKB
Tino Behrends	GSV
Dr. Michael Paust (Co-Vorsitz)	Deutsche Bundesbank
Andreas Vogel	Deutsche Bundesbank
Rainer Englisch	Deutsche Bundesbank
Jörg Bretz	Deutsche Bundesbank
Dr. Rainer Janlewing	Deutsche Bundesbank
Renate Essler	BaFin
Dr. Felix Reinshagen	BaFin
Dr. Jens Gampe	BaFin
Dr. Sebastian Silberg	BaFin
Christoph Ruckert	BaFin