Interview

Redaktionsgespräch mit Jens Obermöller

„Nur auf Basis einer Sicherheitskultur lässt sich dauerhaft ein angemessener Grad an IT-Sicherheit erreichen“

Der neue Leiter des Referates zur IT-Sicherheit beim Bundesamt für Finanzdienstleistungsaufsicht, Jens Obermöller, äußert sich im Redaktionsgespräch zu den prinzipienbasierten Vorschriften MaRisk, die Kreditinstitute im Hinblick auf ihre IT-Sicherheit zu erfüllen haben. Seine Behörde arbeitet kontinuierlich daran, diese weiter zu konkretisieren. Er spricht sowohl den umfangreichen Einsatz von IT-Dienstleistern als auch die hohe Zahl von historisch gewachsenen technischen Altsystemen als Faktoren an, die zu einer Asymmetrie zwischen agilen Angreifern aus dem virtuellen Raum und den Unternehmen, die sich verteidigen, führen können. Zwar seien viele Einzelmaßnahmen möglich, insbesondere aber sei der Aufbau einer Sicherheitskultur in den Kreditinstituten nötig, so seine Forderung. (Red.)

Welche Anforderungen hat die BaFin an die IT-Sicherheit der Kreditinstitute?

Die grundlegenden Anforderungen der BaFin an die IT-Sicherheit der Institute leiten sich aus der in § 25 a Kreditwesengesetz kodifizierten Verpflichtung zur ordnungsgemäßen Geschäftsführung ab. Im Zusammenspiel mit den einschlägigen prinzipienbasierten Vorschriften der Mindestanforderungen an das Risikomanagement sind die Institute angehalten, gängige Standards der IT-Sicherheit zu beachten. Zu solchen Standards zählen zum Beispiel der IT-Grundschutzkatalog des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und der internationale Sicherheitsstandard ISO/IEC 2700X der International Organization for Standardization.

Aufgrund der wachsenden Bedeutung des Themas denken wir natürlich darüber nach, in welcher Form sich die Erwartungen der Aufsicht an die IT-Sicherheit der Institute künftig weiter konkretisieren lassen.

Spezielle Anforderungen ergeben sich auch heute schon beispielsweise aus dem im Mai 2015 veröffentlichten Rundschreiben der BaFin zu den Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSi).

Werden diese Anforderungen auch detailgetreu erfüllt?

Natürlich bestehen für die Institute in Abhängigkeit etwa von Geschäftsmodell, Größe und Komplexität Freiheitsgrade bei der Umsetzung der Anforderungen nach § 25 a Kreditwesengesetz. Daher lässt sich

© BaFin/Eschweiler

Jens Obermöller, Leiter des Referates zur IT-Sicherheit, Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Bonn

die Frage nach einer detailgetreuen Umsetzung nur schwerlich beantworten. Aus meiner Sicht befinden sich die deutschen Kreditinstitute auf einem guten Weg, den wir als Aufsicht so eng wie möglich zu begleiten versuchen. Die Erfüllung der Anforderungen an Ordnungsmäßigkeit der IT-Organisation wird jährlich durch den Jahresabschlussprüfer und auch im Rahmen von bankaufsichtlichen Vor-Ort-Prüfungen überprüft. Sollten sich Hinweise auf Mängel ergeben, so werden diese durch die zuständigen Fachaufseher aufgegriffen.

Eine absolute Sicherheit von Systemen scheint im weltweiten Datennetz nicht zu existieren – nur eine relative. Was bedeutet das für die Bankenbranche?

Eine absolute Sicherheit werden wir im weltweiten Datennetz nicht erreichen können, da haben Sie recht. Umso wichtiger ist es, dass die Institute über eine angemessene Risikosteuerung- und -controlling für IT-Risiken verfügen. Hierbei spielen insbesondere die Feststellung des notwendigen Schutzbedarfs und die Ableitung von Sicherheitsanforderungen konkreter Sicherheitsmaßnahmen eine wesentliche Rolle. Auch sollten Vorkehrungen und Regelungen für entsprechende Notfälle existieren.

Mit dem Fortschreiten der Digitalisierung auf Produkt- und Vertriebsebene der Banken wächst die Zahl der Schnittstellen in den IT-Systemen. Deren sicherer Betrieb verursacht durchaus Aufwand für die Banken. Stimmt nach Ihrer Wahrnehmung das Verhältnis zwischen den Chancen der Digitalisierung und deren Kosten und Risiko?

Natürlich stellt das Fortschreiten der Digitalisierung die Banken vor große Herausforderungen, insbesondere auch finanzieller Natur. Es bieten sich aber auch genügend Chancen. Dies belegen die zahlreichen Fintech-Unternehmen, die versuchen, etablierte Finanzdienstleistungen wie die Zahlungsabwicklung oder die Kreditvergabe durch die Nutzung neuer Technologien kostengünstiger oder kundenfokussierter anzubieten.

Das Verhältnis von Kosten und Nutzen der Digitalisierung wird aber jedes Institut individuell für sich herausarbeiten müssen.

Wo liegen Ihren Erkenntnissen nach die größten Probleme/Herausforderungen der Finanzbranche im Hinblick auf die IT-Sicherheit?

In den letzten Jahren lässt sich ein starker Anstieg von Cyberangriffen beobachten. Unternehmen der Finanzbranche stellen attraktive Ziele solcher Angriffe dar. Neben finanziellen und operationellen Risiken drohen betroffenen Instituten bei einem erfolgreichen Angriff unter Umständen auch handfeste Reputationsrisiken. Die starke IT-Abhängigkeit der Geschäfts- und Wertschöpfungsprozesse im Finanzbereich, der umfangreiche Einsatz von IT-Dienstleistern und IT-Zulieferern sowie ein signifikanter Anteil historisch gewachsener Altsysteme treten verstärkend hinzu und führen zu einer deutlichen Asymmetrie zu den flexibel und mit verblüffend geringem finanziellem Aufwand durchführbaren Cyberangriffen.

> „Eine absolute Sicherheit werden wir im weltweiten Datennetz nicht erreichen können."

Welche Maßnahmen können und müssen noch ergriffen werden? Welche Schwerpunkte sollten Banken und Sparkassen in Ihren Augen mit Blick auf ihre IT-Sicherheit legen?

Neben vielfältigen Einzelmaßnahmen, die Institute ergreifen können, möchte ich doch die Bedeutung betonen, die der Etablierung einer entsprechenden Sicherheitskultur in jedem Institut zukommt. Nur auf dieser Basis lässt sich dauerhaft ein angemessener Grad an IT-Sicherheit erreichen.

Ist die Kreditwirtschaft in der digitalen Welt ähnlich gut abgesichert, wie sie es in der realen Welt ist? Im realen Leben beispielsweise mit Tresoren, Schließfächern, Verzögerungsmechanismen und genauen Vorgaben für Auszahlungen.

Die Kreditwirtschaft ist als regulierte Branche mit Blick auf das erreichte Sicherheitsniveau schon sehr weit fortgeschritten – eine vollständige Sicherheit werden wir in der digitalen wie auch realen Welt nicht erreichen.

Anforderungen an die technisch-organisatorische Ausstattung von Banken sind im MaRisk-Rundschreiben 10-2012 festgelegt. Wichtige IT-Sicherheitsstandards für Banken sind in der ISO27001/27002 Norm geregelt sowie im BSI-Grundschutz vom Bundesamt für Sicherheit in der Informationstechnik. Kreditinstitute scheinen angemessen geschützt zu sein, wenn sie diese Vorgaben erfüllen?

Die MaRisk verweisen auf gängige Sicherheitsstandards. Die von Ihnen angeführten ISO-Normen und der BSI-Grundschutz sind grundsätzlich geeignete Standards, um ein gewisses Maß an IT-Sicherheit zu erreichen.

Ist und bleibt daher menschliches Versagen das größte IT-Sicherheitsrisiko für eine Bank?

Fragt man einen Mitarbeiter der IT wird dieser vermutlich auf diese Frage antworten „ja, die größte Sicherheitslücke sitzt immer noch vor dem Bildschirm". Und auch aus unserer Erfahrung stellen mangelnde Grundkenntnisse im Bereich der IT-Sicherheit und ein fehlendes Risikobewusstsein ein wesentliches IT-Sicherheitsrisiko für die Bank dar. Moderne Angriffstechniken wie beispielsweise das „Spear-Phishing" nutzen dies gezielt aus, indem Social-Engineering-Techniken und der Einsatz von Schadsoftware kombiniert werden. Allerdings gibt es neben dem Faktor „Mensch" noch weitere wesentliche IT-Risikofaktoren. IT-Sicherheit wird sich folglich immer nur im Zusammenspiel von technisch-organisatorischen Abwehrmaßnahmen und der Schulung und Sensibilisierung der Mitarbeiter und Kunden erreichen lassen.

> „Die Kreditwirtschaft ist mit Blick auf das erreichte Sicherheitsniveau schon sehr weit fortgeschritten."

Müssen die Banken mehr für eine Sicherheitskultur tun? Wie können Kunden diesbezüglich sensibilisiert werden?

IT-Sicherheit ist ja leider kein Produkt, das man kaufen kann, sondern ein fortlaufender Prozess, der im Unternehmen gelebt und immer wieder aufs Neue eingeübt werden muss. Dies gelingt nur auf der Basis einer entsprechenden Sicherheitskultur. Jedes Institut sollte individuell prüfen, wie es um diese im eigenen Hause bestellt ist. Wie in anderen Bereichen der Unternehmenskultur prägt das Management den „tone at the top" und sollte auch mit Blick auf die IT-Sicherheit den Mitarbeitern als Vorbild dienen.

Zur Sensibilisierung von Kunden existieren aus meiner Sicht eine Vielzahl etablierter Instrumente, die Institute nutzen können, um ihren Kunden Unterstützung und Orientierung zu relevanten Sicherheitsthemen zu bieten. Auch die BaFin versucht hier einen Beitrag zu leisten. So haben wir im August 2015 im BaFin-Journal und auf der Homepage der BaFin ausführlich über Sicherheitsaspekte des Onlinebankings aus Verbrauchersicht berichtet.

Die Einrichtung von Prozessen für eine angemessene IT-Berechtigungsvergabe wird in dem MaRisk-Rundschreiben 10-2012 besonders hervorgehoben. Verzeichnen Sie hier Fortschritte in der Branche?

Neben der angesprochenen Betonung der aufsichtlichen Anforderungen an eine angemessene IT-Berechtigungsvergabe wird das Thema regelmäßig in Vor-Ort-Prüfungen aufgegriffen. Unsere Erkenntnisse zeigen, dass die Institute Prozesse für eine angemessene Berechtigungsvorgabe eingerichtet haben oder in entsprechenden Projekten zur weiteren Verbesserung der Prozesse weit fortgeschritten sind. Wir werten dies als Fortschritt – auch wenn das Thema IT-Berechtigungsvergabe in einem technologisch und organisatorisch dynamischen Umfeld sicherlich immer eine Herausforderung bleiben wird.

Inwiefern lässt sich IT-Sicherheit bei kleineren Kreditinstituten auslagern? Welche Kompetenzen und Kapazitäten müssen in jedem Haus vorgehalten werden?

Grundsätzlich lassen sich entsprechend der MaRisk alle Aktivitäten und Prozesse auslagern, solange dadurch die Ordnungsmäßigkeit der Geschäftsorganisation nicht beeinträchtigt wird. Das gilt auch für Aktivitäten im Bereich der Informationssicherheit. Allerdings erwarten wir – und das wird auch jeder Kunde von seinem Institut erwarten –, dass sich auch in kleinen Instituten jemand verantwortlich um das Thema Informationssicherheit kümmert und über grundsätzliche Kompetenzen in diesem Bereich verfügt. Wir sprechen uns daher klar dafür aus, dass jedes Institut einen Informationssicherheitsbeauftragten benennen sollte, der diese Rolle übernimmt. Der Informationssicherheitsbeauftragte kann sich bei der Durchführung seiner Aufgaben natürlich in dem erforderlichen Umfang extern unterstützen lassen.

„IT-Sicherheit ist ein fortlaufender Prozess, der im Unternehmen gelebt und immer wieder aufs Neue eingeübt werden muss."

Wie genau beobachtet die BaFin die Fintech-Branche im Hinblick auf deren IT-Sicherheit, vor allem auch an den Schnittstellen zur Finanzwirtschaft?

Fintech-Unternehmen unterliegen nicht der Aufsicht der BaFin, soweit sie keine erlaubnispflichtigen Produkte oder Dienstleistungen anbieten. Insofern haben wir im Regelfall allenfalls einen indirekten Blick auf die IT-Sicherheit der Fintech-Branche, der sich aus öffentlich zugänglichen Quellen speist.

„Wir haben im Regelfall allenfalls einen indirekten Blick auf die IT-Sicherheit der Fintech-Branche."

Allerdings gibt es auch Bereiche, in denen wir ganz konkret versuchen, entsprechende Sicherheitsanforderungen mit zu gestalten. So wird es im Rahmen der Arbeiten zur Umsetzung der Zahlungsdiensterichtlinie 2 (PSD2) unter anderem auch darum gehen, auf europäischer Ebene IT-technische Anforderungen für die Sicherheit bei Internetzahlungen zu erarbeiten. Beispiele sind eine starke Kundenauthentifizierung oder eine sichere Kommunikation zwischen Zahlungsdienstleistern, Händlern und Kunden bei der Auslösung von Zahlungen.

Klappt die institutsübergreifende Zusammenarbeit der Branche beim Informationsaustausch zu Bedrohungen aus dem virtuellen Raum?

Wir haben hier natürlich keinen statistisch belastbaren Überblick, aber die Erfahrungen aus einzelnen Gremien oder unserer eigenen Informationsveranstaltung zur IT-Sicherheit stimmen in jedem Fall optimistisch in Bezug auf die Offenheit mit der hier Informationen ausgetauscht werden.

Hypovereinsbank, ING-Diba und Commerzbank haben gemeinsam das German Competence Center against Cyber Crime aus der Taufe gehoben. Als wie wirksam schätzen Sie solche gemeinsamen Initiativen der Kreditwirtschaft ein?

„Es ist schwierig, eine Aussage zu treffen, aus welchen Ländern Angriffe tatsächlich durchgeführt werden."

Aus unserer Sicht begrüßen wir natürlich ausdrücklich Initiativen, die über einen Austausch von Informationen oder die Entwicklung und Verbreitung von Best Practices einen Beitrag zur Erhöhung der Sicherheit im Cyberraum leisten.

Allerdings wird erst die Erfahrung zeigen, welche Strukturen oder Kooperationsformen – auch grenzüberschreitend – benötigt werden, um den weltweit vernetzten und flexiblen Strukturen gerecht zu werden, derer sich Angreifer aus dem Cyberraum bedienen können.

Was sind die häufigsten Arten von Cyberangriffen? Kann man auch sagen, aus welchen Regionen der Welt diese bevorzugt kommen?

Besonders häufig beobachten wir sogenannte Distributed-Denial-of-Service-Angriffe (DDoS), die darauf abzielen, die Verfügbarkeit von Diensten, Webseiten oder sogar Netzen einzuschränken. Sehr häufig werden diese Angriffe mit erpresserischen Geldforderungen unterlegt. Ebenfalls gehäuft treten Phishing-Angriffe auf, bei denen die Angreifer versuchen, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten wie Kreditkartendaten eines Internetnutzers zu gelangen. Da Cyberangreifer sich nicht an nationale Grenzen halten, ist es schwierig, eine Aussage zu treffen, aus welchen Ländern Angriffe tatsächlich durchgeführt werden.

Im vergangenen Jahr wurde eine Taskforce der Europäischen Bankenaufsichtsbehörde zu IT-Risiken gebildet. Die EZB beschäftigte sich im vergangenen Jahr mit der Widerstandsfähigkeit der bedeutenden Banken gegen Cyberattacken. Wie stark ist IT-Sicherheit (noch) ein Thema der nationalen Aufseher BaFin und Bundesbank?

Die bewährte Zusammenarbeit der nationalen Aufsichtsbehörden mit der EZB im Rahmen des SSM gilt natürlich ebenso für den Bereich der IT-Sicherheit. Die Tatsache, dass das Thema IT-Sicherheit nun auch in zahlreichen europäischen und internationalen Gremien aufgegriffen wurde, erfordert auch eine Vertretung der deutschen Aufsichtsinteressen in eben diesen Gremien. Daneben gibt es aber auch beispielsweise noch das IT-Sicherheitsgesetz als das zentrale deutsche Regelungswerk mit dem Ziel, die IT der kritischen Infrastrukturen, zu denen auch der Finanzsektor gehört, zu schützen.

Die nationalen Aufsichtsbehörden können hier einen wesentlichen Beitrag leisten, wenn es darum geht, umfassende Standards für die IT-Sicherheit in der Finanzdienstleistungsbranche zu schaffen, die den Schutz von Daten, Instituten, Systemen und Infrastrukturen sowie der Verbraucher sicherstellt. Hierzu dient nicht zuletzt die Zusammenarbeit mit anderen relevanten Institutionen für Cybersicherheit im Finanzdienstleistungsbereich wie beispielsweise dem BSI oder dem UP KRITIS.