Neue aufsichtsrechtliche Anforderungen für Cyber Security bei Kredit- und Finanzdienstleistungsinstituten

Hinweise für Outsourcing-Verträge

Cyber Security – Top-Thema auf der Agenda der Aufsichtsbehörden

Die Bankaufsichtsbehörden in Deutschland, der EU und den USA haben das Thema Cyber Security seit Anfang dieser Woche verschärft im Fokus:

Die Bundesbank prüft, ob sie spezielle „Hacker-Stresstests" für Institute zur Pflicht macht, so Bundesbank-Vorstand Andreas Dombret am 21.6. in einem Vorabbericht. In Großbritannien und weiteren EU-Mitgliedsstaaten sind Cyber Resilience-Tests bereits Standard. Nachdem Hacker von der Zentralbank Bangladesch letztes Jahr die Rekordsumme von 81 Mio. USD erbeutet haben, hat zuletzt die European Banking Authority (EBA) gefordert, nunmehr den Instituten in allen EU-Mitgliedsstaaten Stresstests zur Absicherung gegen Cyber-Attacken aufzuerlegen.

Auch die Europäische Zentralbank (EZB) verschärft die Anforderungen: Bereits ab diesem Sommer müssen Institute unter der Aufsicht der EZB signifikante Cyber-Vorfälle melden. Darüber hinaus will die EZB eine Datenbank für Cyber-Vorfälle einrichten, die als Frühwarn- und Analysesystem dienen soll.

Schließlich haben am 20.6. US-Banken wie die Bank of America, Citigroup und J.P. Morgan Chase bekannt gemacht, dass sie unter der Ägide der U.S. Chamber of Commerce mit Cicso, Microsoft, Verizon und weiteren Stakeholdern derzeit Security Ratings (ähnlich wie FICO Score) entwickeln. Auch die BaFin beobachtet die Bemühungen zur Schaffung von Mindeststandards für die Cyber-Sicherheit in der Finanzdienstleistungsbranche aufmerksam (siehe Arbeitsschwerpunkte zur IT-Aufsicht 2016/2017, 16. März 2017). Neben den geplanten neuen Regeln wird die BaFin künftig verstärkt im Nationalen Cyber-Abwehrzentrum (Cyber-AZ) mitwirken.

Praxisfolgen für Outsourcing Verträge

Es zeichnet sich ab, dass „Hacker-Stresstests" – d.h. sog. Schwachstellen- und Penetrationstests, die dazu dienen, die Sicherheit und Resilienz von IT-Systemen zu testen – ein elementarer Baustein des Aufsichtsrechts und damit auch von Outsourcing Verträgen werden.

Derzeit arbeitet die BaFin mit Hochdruck daran, die Bankaufsichtlichen Anforderungen an die IT(-Sicherheit) (BAIT) auszuformulieren (siehe Konsultation 02/2017 - Bankaufsichtliche Anforderungen an die IT (BAIT)). Die Veröffentlichung der BAIT per BaFin-Rundschreiben ist für Mitte des Jahres angekündet. Die BAIT sollen die Mindestanforderungen an das Risikomanagement der Banken (MaRisk) konkretisieren. Ein erklärtes Ziel der BAIT ist, insbesondere das IT-Risikobewusstsein in den Instituten gegenüber den Auslagerungsunternehmen zu erhöhen. Dabei ist zu beachten, dass die BAIT die adressierten Themen nicht abschließend regeln. Das heißt, dass Institute gemäß § 25a Abs. 1 Nr. 4 KWG i. V. m. AT 7.2 Tz. 2 MaRisk verpflichtet sind, bei der Ausgestaltung der IT-Systeme und der dazugehörigen IT-Prozesse grundsätzlich auf gängige Standards (z.B. der Grundschutzkatalog des Bundesamtes für Sicherheit in der Informationstechnik und der internationale Sicherheitsstandard ISO/IEC 2700X) abzustellen. Das BSI hat gerade kürzlich einen Leitfaden für Penetrationstests veröffentlicht; Penetrationstests sind somit im Blickfeld der Behörden.

Institute sollten die geplanten aufsichtsrechtlichen Pflichten daher vor allem auch bei Auslagerungen von Leistungen an Dienstleister im Blick haben. Das gilt für bestehende und künftige Outsourcing Verträge. Denn bei Auslagerungen bleiben Institute für die Umsetzung und das Monitoring der erforderlichen IT-Sicherheitssysteme verantwortlich: Zum einen sind die vorgenommenen Risikobewertungen der ausgelagerten Leistungen regelmäßig und anlassbezogen zu überprüfen und ggf. inkl. der Vertragsinhalte anzupassen; zum anderen ist die Leistungserbringung angemessen zu überwachen (vgl. BAIT-Entwurf vom 23.02.2017, 8 Tz. 58 und 59). Damit werden Penetrationstest-Vereinbarungen zu einem wichtigen Bestandteil von künftigen Outsourcing Verträgen. Bestehende Outsourcing Verträge sollten daraufhin geprüft werden, ob ein Recht zu Stresstests der IT-Sicherheitssysteme besteht.

Nicht nur ein aufsichtsrechtliches Thema: Die DS-GVO

Die Pflicht zur Implementierung einer widerstandsfähigen IT-Sicherheitsarchitektur bei Dienstleistern ist eine zentrale Pflicht unter der EU-Datenschutz-Grundverordnung (DS-GVO). Ein auslagerndes Institut hat als datenschutzrechtlich Verantwortlicher geeignete technische und organisatorische Maßnahmen zum Datenschutz zu treffen: Dazu zählt, sicherzustellen, dass Systeme und Dienste im Zusammenhang mit der Datenverarbeitung insb. „auf Dauer“ (Prüfungspflicht) „belastbar“ (d.h. widerstandsfähig) sind (Artikel 32 Abs. 1 lit. b DS-GVO). Die Aufsichtsbehörde kann einen Verstoß gegen die Anforderungen des Artikel 32 DS-GVO mit einer Geldbuße von bis zu 10 Mio. EUR oder (bei Unternehmen) von bis zu 2% des gesamten weltweit erzielten Unternehmens-Jahresumsatzes des vorangegangenen Geschäftsjahrs (je nachdem, welcher der Beträge höher ist) ahnden (Art. 83 Abs. 4 lit. a DS-GVO).

Fazit

Die IT-Sicherheit ist in den Scope der Aufsichtsbehörden gerückt. Neben den geplanten neuen Regeln wird die BaFin künftig verstärkt im Nationalen Cyber-Abwehrzentrum (Cyber-AZ) mit dem BSI mitwirken. Neue regulatorische Anforderungen für die IT-Sicherheit – die BAIT; Stresstests, Meldepflichten und auch die DS-GVO – kommen. Die Umsetzung der aufsichtsrechtlichen Cyber Sicherheits-Anforderungen im internen Management und in Verträgen mit Dienstleistern stellt somit ein wesentliches To-do dar.

Bei Fragen stehen wir Ihnen gerne jederzeit zur Verfügung.

Dr. Lars Lensdorf

Tel: +49 (69) 768063-30

Mobile: +49 (160) 90704902

E-Mail: l.lensdorf@heylaw.de

Dr. Moritz Hüsch, LL.M.

Tel: +49 (69) 768063-453

Mobile: +49 (151) 12577724

E-Mail: m.huesch@heylaw.de