BaFin
Bundesanstalt für
Finanzdienstleistungsaufsicht

Bundesamt
für Sicherheit in der
Informationstechnik

An die Geschäftsleitungen der Unternehmen, die gemäß
BSI-Kritisverordnung Betreiber Kritischer Infrastrukturen
im Sektor Finanz- und Versicherungswesen sind

Bankaufsichtliche Anforderungen an die IT Kritischer Infrastrukturen 03.08.2018

Sehr geehrte Damen und Herren,

zu den spezifischen Anforderungen an den Sektor Finanz- und Versicherungswesen, der neben der langjährig institutionalisierten Aufsicht des Bundes über Kreditinstitute durch die BaFin und die Deutschen Bundesbank nunmehr auch durch eine europäische Bankenaufsicht im Rahmen des SSM geprägt ist, kommen mit den §§ 8a und 8b BSI-Gesetz für Betreiber Kritischer Infrastrukturen gemäß BSI-Kritisverordnung (KRITIS-Betreiber) weitere gesetzliche Anforderungen hinzu.

BSI, BaFin und Vertreter der KRITIS-Betreiber haben im vergangenen Jahr intensive und konstruktive Diskussionen über die Umsetzung dieser Anforderungen geführt. BaFin und BSI begrüßen diesen kooperativen Austausch ausdrücklich. Diese Arbeit wird uns gemeinsam auch in diesem Jahr weiter beschäftigen.

Auf nationaler Ebene führt das Hinzutreten der §§ 8a und 8b BSI-Gesetz zu Überschneidungen in den Anforderungen im Hinblick auf Unternehmen, die der Aufsicht der BaFin unterfallen und zugleich KRITIS-Betreiber sind.

Um eine zusätzliche materielle Belastung dieser KRITIS-Betreiber im Rahmen des rechtlich Vertretbaren möglichst gering zu halten, weisen wir auf Folgendes hin:

Gemäß den finanzsektorspezifischen Normen müssen die Aufsichtsobjekte der BaFin stets über eine ordnungsgemäße Geschäftsorganisation verfügen, die die Einhaltung der zu beachtenden Gesetze, Verordnungen und aufsichtsbehördlichen Anforderungen gewährleistet. Mit der Veröffentlichung des Rundschreibens 10/2017 (BA) „Bankaufsichtliche Anforderungen an die IT (BAIT)“ im vergangenen Jahr hat die BaFin für den Bankenbereich die einschlägigen Normen in Bezug auf die Anforderungen an eine ordnungsgemäße IT-Geschäftsorganisation interpretiert.

Zu den aufsichtsrechtlichen Anforderungen an eine ordnungsgemäße Geschäftsorganisation gehören auch Anforderungen an Auslagerungen, die sich mittelbar auch auf Auslagerungsunternehmen auswirken, die IT-Dienstleistungen für die BaFin-Aufsichtsobjekte erbringen (IT-Dienstleister).

Für Aufsichtsobjekte der BaFin, die zugleich KRITIS-Betreiber sind, plant die BaFin in Abstimmung mit dem BSI, zeitnah ein KRITIS-Modul zu veröffentlichen.

Das KRITIS-Modul soll beschreiben, welche zusätzlichen Anforderungen zu berücksichtigen sind, um den Nachweis gemäß § 8a Abs. 3 BSI-Gesetz durch den Jahresabschlussprüfer zu erbringen, der im Rahmen der Prüfung des Risikomanagements und der Geschäftsorganisation des Unternehmens gleichzeitig die Erfüllung der Anforderungen des § 8a Abs. 1 BSI-Gesetz überprüft und bestätigt.

Alternativ können die KRITIS-Betreiber einen unternehmensindividuellen Ansatz verfolgen oder einen branchenspezifischen Sicherheitsstandard (B3S) gemäß § 8a Abs. 2 BSI-Gesetz erstellen. Der Nachweis gemäß § 8a Abs. 3 BSI-Gesetz ist in diesen Fällen unter Hinzuziehung einer geeigneten Prüfstelle (vgl. "Orientierungshilfe zu Nachweisen gemäß § 8a (3) BSIG") zu erstellen.

Im Hinblick auf die Meldepflicht gemäß § 8b Abs. 4 BSI-Gesetz weisen wir vorsorglich darauf hin, dass diese unverändert gegenüber dem BSI einzuhalten ist.

Es ist unser gemeinsamer Wille, auch künftig – neben dem Aufsichtshandeln beider Behörden – mit Ihnen einen intensiven fachlichen Austausch insbesondere im Rahmen der auf Fachebene etablierten Gremien zu Fragen der Sicherheit der IT-Systeme durchzuführen.

Felix Hufeld
Präsident BaFin

Arne Schönbohm
Präsident BSI