Datum: 10.05.2021 | Kategorie: Sonstige

Konsultation der Zahlungsdiensteaufsichtlichen Anforderungen an die IT von Zahlungs- und E-Geld-Instituten (ZAIT)

Am 12. April 2021 hat die BaFin die Konsultation eines geplanten Rundschreibens mit ?Zahlungsdiensteaufsichtlichen Anforderungen an die IT von Zahlungs- und E-Geld-Instituten ? ZAIT? veröffentlicht. Die BaFin hat damit neben den bisher gültigen Vorgaben für Kapitalverwaltungsgesellschaften, Versicherungen und Banken - der KAIT, VAIT bzw. der BAIT - letztere wurde zum 26. Oktober 2020 von der BaFin in einer Novelle als Entwurf konsultiert -, nun auch IT-Anforderungen speziell für Zahlungs- und E-Geld-Institute konkretisiert. Die ZAIT gilt auch für Zweigniederlassungen deutscher Institute im Ausland i. S. v. § 38 ZAG. Hingegen ist sie nicht anzuwenden auf Zweigniederlassungen mit Sitz in einem anderen Staat des EWR (Europäischer Wirtschaftsraum) nach § 39 ZAG.

Die ZAIT orientiert sich dabei an den IT-Anforderungen für Banken (BAIT) und stützt sich hierbei insbesondere auf die EBA Anforderungen aus den EBA-Leitlinien für IKT und Sicherheitsrisikomanagement (GL/2017/17) sowie den EBA-Leitlinien zu Auslagerungen (GL/2019/02).

Die ZAIT verpflichtet die Institute dazu, sich bei der Ausgestaltung der IT-Systeme und den dazugehörigen IT-Prozessen an gängigen Standards (i. e. S. ISO/IEC270XX sowie der BSI-Grundschutz) zu orientieren. Zugleich nennt die ZAIT noch die Payment Card Industry Data Security Standards (PCI-DSS) als möglichen Standard.

Die ZAIT sieht in der Konsultation u. a. folgende Anforderungen vor:

Erstellung einer IT-Strategie mit definierten Mindestinhalten,
Quantitativ und qualitativ angemessene Personalausstattung des Informationsrisikomanagement, des Informationssicherheitsmanagement, des IT-Betrieb und der Anwendungsentwicklung,
Festlegung eines Informationsverbundes sowie Ermittlung des Schutzbedarfs für Bestandteile dieses Verbundes nach den Schutzzielen ?Integrität?, ?Vertraulichkeit?, ?Verfügbarkeit? und ?Authentizität?,
Beschluss einer Informationssicherheitsleitlinie durch die Geschäftsleitung,
Mindestens vierteljährliche Berichterstattung an die Geschäftsleitung in Form einer Risikoanalyse und eines Statusberichtes, letzteres durch den Informationssicherheitsbeauftragten,
Einrichtung der unabhängigen Funktion des Informationssicherbeauftragten (ISB), der grundsätzlich im eigenen Haus vorzuhalten ist
Richtlinie zum Testen und Überprüfen von Sicherheitsmaßnahmen
Genehmigungs-, Kontroll- und regelmäßige Überprüfungsprozesse für Benutzerberechtigungen
Angemessene Steuerung von IT-Projekten und regelmäßige Berichterstattung über IT-Projekte und Projektrisiken an die Geschäftsleitung,
Festlegung von Prozessen für die Anwendungsentwicklung,
Testen von IT-Systemen vor ihrem erstmaligen Einsatz und bei wesentlichen Veränderungen mit einer definierten Methode,
Anforderungen an den Umgang mit Individueller Datenverarbeitung (z. B. wesentliche Excel-Dateien in den Fachbereichen)

Durchführung von Auswirkungsanalysen zur Identifikation von zeitkritischen Aktivitäten und Prozessen
Erstellung von Notfallkonzepten, welche mindestens vier vorgegebene Notfallszenarien berücksichtigen
Nachweis der Wirksamkeit und Angemessenheit des Notfallkonzepts für zeitkritische Aktivitäten und Prozesse für alle relevanten Szenarien mindestens jährlich und anlassbezogen.
Automatisierte und regelbasierte Überwachung der Sicherheit von Anwendungssystemen anhand von Protokolldaten,

Meldungen und Störungen, welche Hinweise auf Verletzung der Schutzziele geben können.

Zugleich legt die ZAIT in dem Kapitel ?Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen? aufbau- und ablauforganisatorische Regelungen zu Auslagerungen fest, die in der BAIT so nicht vorhanden sind, sondern aus dem AT 9 der MaRisk stammen. Sie betreffen insbesondere konkrete Vorgaben für die Analyse, Beurteilung, Vertragsgestaltung, Steuerung und Kontrolle von IT-Auslagerungen und dem sonstigen Fremdbezug von IT-Dienstleistungen. Die ZAIT fordert in Tz. 9.12 die Einrichtung eines zentralen Auslagerungsbeauftragten im Institut selbst, sobald das Institut Auslagerungen von IT-Aktivitäten und IT-Prozessen vornimmt.

Die Anforderungen in der ZAIT sind sehr umfangreich (48 Seiten). In der oben genannten Auflistung sind bei weitem nicht alle Anforderungen enthalten, sondern nur die wesentlichsten. Eine risikoorientierte Herangehensweise ist für alle Institute zu empfehlen, die sich mit der Umsetzung der Anforderungen beschäftigen. Institute sollten im ersten Schritt ihren IST-Zustand mit den Anforderungen der ZAIT vergleichen, und eine ?GAP-Analyse? erarbeiten. Aufgrund unserer Erfahrungen mit kleineren Instituten sowie mit Instituten, welche die BAIT bereits erfolgreich umgesetzt haben, können wir Sie dabei optimal unterstützen.

Eine konkrete Umsetzungsfrist wurde im Entwurf nicht genannt. Es ist damit zu rechnen, dass die endgültige Fassung ohne Umsetzungsfrist in Kraft treten wird, was dem Vorgehen bei der Veröffentlichung der BAIT entsprechen würde.

Stellungnahmen zum Entwurf der ZAIT werden bis zum 14.05.2021 von der BaFin entgegengenommen.

Quellen / Verweise

Konsultation 03/2021 ? ZAIT
EBA-Leitlinien zu Auslagerungen (GL/2019/02)
EBA-Leitlinien für IKT und Sicherheitsrisikomanagement (GL/2017/17)