bitkom

Auf einen Blick

BaFin Konsultation 03/2021 – ZAIT:

Ausgangslage

Nachdem die BaFin die BAIT – Bankaufsichtliche Anforderungen an die IT – bereits novelliert hat, zieht die Finanzaufsicht nun mit den Zahlungs- und E-Geld-Instituten nach. Institute, die bisher keine Berührungspunkte mit den BAIT hatten, dürften mit an Sicherheit grenzender Wahrscheinlichkeit mit dem ZAIT Anforderungskatalog vor erhebliche Herausforderungen gestellt werden.

Bitkom-Bewertung

Wir empfehlen daher im Rahmen der Veröffentlichung eine realistische Erwartungshaltung für den Zeitrahmen der Umsetzung der ZAIT Anforderungen zu kommunizieren. Klarheit zu einer ZAIT-Umsetzungsfrist würde auch Auditoren dabei unterstützen, die mittel- bis langfristigen Pläne der Institute zu würdigen.

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Kevin Hackl
Referent Digital Banking & Financial Services
T +49 175 5848805
k.hackl@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Bitkom BaFin Konsultation 03/2021 – ZAIT: Konsultation eines geplanten Rundschreibens "Zahlungsdiensteaufsichtliche Anforderungen an die IT von Zahlungs- und E-Geld-Instituten - ZAIT"

14. Mai 2021

Konkrete Anmerkungen und Änderungsempfehlungen

Stelle im Text	BaFin Text mit den gewünschten Änderungsvorschlägen Streichungen: ~~rot~~ / Ergänzungen: blau	Anmerkungen
I.2	Mindestinhalte der IT-Strategie sind:	Hier wäre ein Verweis hilfreich, welche Standards und Normen diese Mindestinhalte bereits abdecken (z.B. ISO27001 Zertifizierung). So könnten die betroffenen Institute gezielt und schnell erfassen, welche Punkte für sie relevant sind.
1.4	Die IT-Strategie sowie erforderliche Anpassungen der IT-Strategie sind dem Aufsichtsorgan des Instituts zur Kenntnis zu geben ~~und mit diesem zu erörtern.~~	Dies halten wir für einen sehr hohen bürokratischen Aufwand; insbesondere dann wen die Aufsicht keine Empfehlungen abgibt.
3.11	Die Geschäftsleitung ist regelmäßig, mindestens jedoch vierteljährlich oder anlassbezogen, insbesondere über die Ergebnisse der Risikoanalyse sowie die Veränderungen an der Risikosituation zu unterrichten.	Hier sollte der Grundsatz eines risikobasierten Ansatzes der Proportionalität stärker berücksichtigt werden.
4.4	[...] Sie stellt sicher, dass die in der IT-Strategie, der Informationssicherheitsleitlinie und den Informationssicherheitsrichtlinien des Instituts festgelegten Ziele und Maßnahmen hinsichtlich der Informationssicherheit sowohl intern als auch gegenüber ~~Dritten~~ Parteien mit berechtigtem Interesse transparent gemacht und deren Einhaltung regelmäßig sowie	Eine entsprechende Einschränkung bzw. Klarstellung wäre hier angebracht, damit Mitbewerber hier nicht ohne Einschränkung Informationen mit Verweis auf diese Richtlinie verlangen können.

	anlassbezogen überprüft und überwacht werden. […] - als Ansprechpartner für Fragen der Informationssicherheit innerhalb des Instituts und für ~~Dritte~~ Parteien mit berechtigtem Interesse bereitzustehen	
5.2	Das Institut hat auf Basis der Informationssicherheitsleitlinie und Informationssicherheitsrichtlinien angemessene, risikobasierte, ~~dem Stand der Technik entsprechende,~~ operative Informationssicherheitsmaßnahmen und Prozesse zu implementieren, die den Stand der Technik berücksichtigen.	Eine Klarstellung bzw. Neuformulierung, die einen risikobasierten Zugang ins Zentrum rückt, wäre hier zu begrüßen. Weiter soll sichergestellt werden, dass die Formulierung innovationsfreundlich getroffen wird.
8.2	[…] Zu den Bestandsangaben zählen insbesondere: […] - ~~Standort der Komponenten der IT-Systeme~~ Standort oder Benennung kritischer Drittdienstleister im Falle einer Auslagerung	Eine entsprechend Neuformulierung wäre wichtig um die Machbarkeit von Auslagerungen zu garantieren.
9.10	[…] **Sonstige Sicherheitsanforderungen** Regelungen zu sonstigen Sicherheitsanforderungen sollten für alle, also auch nicht wesentliche Auslagerungen, vertraglich vereinbart werden. Zu den sonstigen Sicherheitsanforderungen zählen vor allem Zugangsbestimmungen zu Räumen und Gebäuden (z. B. bei Rechenzentren) sowie Zugriffsberechtigungen auf Softwarelösungen zum Schutz wesentlicher Daten und Informationen. Die Einhaltung dieser Anforderungen ist regelmäßig ~~fortlaufend~~ zu überwachen.	Im Falle von Rechenzentren und den Zugangsbestimmungen erfolgt eine anlassbezogene Prüfung (Review von Zertifikaten und/oder Vorgaben, Prüfungsberichte über interne Kontrollen oder Vor-Ort-Prüfungen). Hier kann somit grundsätzlich nicht von einer fortlaufenden Überwachung im Sinne einer kontinuierlichen Überwachung gesprochen werden. Selbstverständlich müssen die Sicherheitsanforderungen fortlaufend implementiert sein und bei Dritten effektiv wirken.
10.8	Das Institut hat nachzuweisen, dass bei Ausfall eines Rechenzentrums die zeitkritischen Aktivitäten und Prozesse aus einem ausreichend entfernten Rechenzentrum und für eine angemessene Zeit sowie für die anschließende Wiederherstellung des IT-Normalbetriebs erbracht werden können.	Bitte um Klarstellung bzw. Definition zu „ausreichend entfernte[s] Rechenzentrum“.

10.9	Die Geschäftsleitung hat sich mindestens ~~quartalsweise~~ jährlich und ~~anlassbezogen~~ in zeitlicher Abstimmung zu den Notfalltests über den Zustand des Notfallmanagements schriftlich berichten zu lassen.	Eine Anpassung an die jährlich stattfindenden Notfalltests wäre angemessen.
11.5	Falls das Institut mit dem Zahlungsdienstnutzer Betragsobergrenzen vereinbart hat, ist dem Zahlungsdienstnutzer die Möglichkeit zu geben, die vereinbarten Grenzen auf geringere Beträge im Rahmen der Risikosteuerung anzupassen.	
11.6	Zur Erkennung von betrügerischer oder nicht autorisierter Nutzung der Zahlungskonten des Zahlungsdienstnutzers hat das kontoführende Institut dem Zahlungsdienstnutzer die Möglichkeit einzuräumen, Benachrichtigungen über getätigte und fehlgeschlagene Transaktionen zu erhalten.	Dies kann durch einen Zahlungsauslösungsauslösedienst alleinig nicht sichergestellt werden, sondern muss in der Verantwortung des kontoführenden Instituts liegen. Grundsätzlich ist dabei auch darauf hinzuweisen, dass hierfür die technische Realisierbarkeit fehlt und datenschutzrechtliche Schranken bestehen.