Informationssicherheit

Kapitalverwaltungsaufsichtliche Anforderungen an die IT

Die BaFin hat den Entwurf des Rundschreibens „Kapitalverwaltungsaufsichtliche Anforderungen an die IT (KAIT)“ zur Konsultation gestellt.

AUTOR UND ANSPRECHPARTNER

Michael Switalla
Leiter Informationssicherheit & Datenschutz,
E-Mail: michael.switalla@dz-cp.de

Die BaFin hat sich in den vergangenen Jahren in ihren Bankaufsichtlichen Anforderungen an die IT (BAIT) bereits dazu geäußert, wie Banken ihre IT-Ressourcen, ihre Informationsrisiken und ihre Informationssicherheit organisieren und überwachen sollen. Nun konsultiert sie auch ihre Kapitalverwaltungsaufsichtlichen Anforderungen an die IT (KAIT).

Das BaFin-Rundschreiben zielt darauf ab, die IT-Sicherheit im Markt zu erhöhen und das IT-Risikobewusstsein in den Kapitalverwaltungsgesellschaften (im Sinne des § 17 Kapitalanlagegesetzbuch (KAGB), soweit diese über eine Erlaubnis nach § 20 Absatz 1 KAGB verfügen) zu schärfen. Es enthält Hinweise zur Auslegung der nationalen und europarechtlichen Vorschriften über die Geschäftsorganisation, soweit sie sich auf die technisch-organisatorische Ausstattung der Kapitalverwaltungsgesellschaften beziehen.

Mit dem Rundschreiben will die BaFin eigenen Angaben zufolge einen „flexiblen und praxisnahen Rahmen für die technisch-organisatorische Ausgestaltung der IT“ vorgeben, insbesondere für das Management der IT-Ressourcen und für das IT-Risikomanagement. Darüber hinaus regelt das Rundschreiben den Umgang mit Auslagerungen von IT-Aktivitäten und IT-Prozessen.

Dem Rundschreiben zufolge müssen künftig alle Kapitalverwaltungsgesellschaften (KVG) Leitlinien zur Informationssicherheit (IT-Strategie und IT-Governance) definieren und dokumentieren. Die wichtigsten Neuerungen sind zusammengefasst:

- Auch KVG müssen nun die Informationsrisiken aktiv managen, d. h., die jeweiligen Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen und Kommunikationswege zu definieren, aufeinander abzustimmen, zu überwachen und zu steuern.
- Das Informationssicherheitsmanagement obliegt dabei einem Beauftragten für Informationssicherheit, den die KVG zu ernennen hat. Er stellt innerhalb seiner Funktion sicher, dass die in der IT-Strategie, in der Informationssicherheitsleitlinie und in den Informationssicherheitsrichtlinien der KVG niedergelegten Ziele und Maßnahmen – sowohl intern als auch gegenüber Dritten – transparent gemacht werden und deren Einhaltung überprüft und überwacht wird.
- Ein Benutzerberechtigungsmanagement soll gewährleisten, dass den Benutzern eingeräumte Berechtigungen so ausgestaltet sind und genutzt werden, wie es den organisatorischen und fachlichen Vorgaben der KVG entspricht.
- Wesentliche Veränderungen in den IT-Systemen im Rahmen von IT-Projekten, deren Auswirkung auf die IT-Aufbau- und IT-Ablauforganisation sowie die dazugehörigen IT-Prozesse sind vorab im Rahmen einer Analyse des Risikogehalts zu bewerten.
- Der IT-Betrieb inkl. Datensicherung wird geregelt, ebenso wie Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen.

Zusammenfassend zollt das Rundschreiben dem faktischen Bedeutungszuwachs der Informationstechnik in den Kapitalverwaltungsgesellschaften Rechnung. Letztlich steht dahinter die zu begrüßende Intention, die IT- und Datensensibilität, die Datenmengen und die unterschiedlichen beteiligten Systeme mithilfe von (Mindest-)Standards in den Griff zu bekommen. Wir stehen Ihnen dabei gerne mit unseren Erfahrungen beratend bzw. als ausgelagerte Funktion zur Verfügung, sprechen Sie uns an. ▬