Waigel RECHTSANWÄLTE

Das Kreuz mit der IT

Stand: September 2019

Das Thema IT wird bei den Aufsichtsbehörden immer größer geschrieben. Offensichtlich hat es beim Thema IT bei einigen Banken größere Schwierigkeiten gegeben, bei den Großbanken liest man das immer wieder in der Zeitung, aber scheinbar auch bei Kleineren liegt vieles im Argen. Bei den größeren Instituten werden zwischenzeitlich regelmäßig IT-Sonderprüfungen durchgeführt und es ist nur eine Frage der Zeit, bis es auch die Finanzdienstleister und Vermögensverwalter erwischt. Bei einigen größeren haben bereits die Wirtschaftsprüfer die Zügel deutlich angezogen und angeblich hat es auch schon Verwarnungen an Geschäftsleiter wegen Mängeln in der IT gegeben. Ich bitte Sie daher, sich des Themas anzunehmen und eine „Groborganisation“ nach Maßgabe der sogenannten BAIT, nämlich der „bankaufsichtlichen Anforderungen an die IT“ vorzuhalten. Die BaFin hat dazu am 14.09.2018 ein Rundschreiben erlassen und geht nun langsam dazu über, dessen Einhaltung auch durchzusetzen.

Zunächst einmal verlangt die BaFin eine IT-Strategie, das heißt ein Dokument, in dem die wesentlichen Grundentscheidungen für die IT-Struktur durch die Geschäftsleitung beschlossen werden. In dieser Strategie sollte festgelegt werden, welche personelle Ausstattung und welches Budget der IT zur Verfügung gestellt wird, welche Standards eingehalten werden (z.B. der Grundschutzkatalog des Bundesamts für Sicherheit in der Informationstechnologie sowie der internationale Sicherheitsstandard ISO/IEC2700X). Entschieden werden sollte, ob das Institut eine eigenständige IT entwickelt und mit Eigenlösungen arbeitet oder IT-Komponenten zugekauft werden. Festgehalten werden sollte, dass ein Institut laufend einen Überblick über seine IT-Landschaft behält, sowie Aussagen zum Notfallmanagement, die Einrichtung eines IT-Beauftragten usw.

In diese Strategie sollte unbedingt aufgenommen werden, dass der Vermögensverwalter selbst keine Konto- und Depotführung übernimmt und die Kundenassets bei einer unabhängigen Depotbank verwahrt werden. Das reduziert schon einmal ganz wesentlich das Risiko und die entsprechenden IT-Pflichten. Zudem sollten Sie festhalten, dass der Vermögensverwalter im Prinzip von jedem Punkt der Welt aus auf die Systeme der Depotbank zugreifen kann, um seine Aufgabe als Vermögensverwalter wahrzunehmen. Selbst bei einem kompletten Ausfall der IT-Systeme des Vermögensverwalters bleibt daher das anvertraute Vermögen nicht schutzlos, sondern in der Obhut der Depotbank und zur Not kann der Vermögensverwalter von zu Hause aus durch Fernzugriff Dispositionen für das Vermögen vornehmen.

Der nächste Schritt ist das Informationsrisikomanagement. Dazu hat sich das Institut zunächst einmal über alle Bestandteile des sogenannten Informationsverbundes einen Überblick zu verschaffen, das heißt die ganzen Programme und IT-Schnittstellen zu erfassen. Dann ist zu analysieren, welche Daten durch diese Programme und Schnittstellen bearbeitet werden und welche Schutzziele für diese Programme und Daten bestehen. In der Regel werden die Schutzziele Integrität, Verfügbarkeit, Vertraulichkeit und Authentizität festgelegt. Ebenso ist

ein Soll-Maßnahmenkatalog zu erstellen. Es erfolgt eine Risikoanalyse durch einen Vergleich der Soll-Maßnahmen mit den jeweils umgesetzten Maßnahmen. Mindestens vierteljährlich muss die Geschäftsleitung über die Ergebnisse dieser Risikoanalyse (Vergleich der Soll-Maßnahmen mit den umgesetzten Maßnahmen) unterrichtet werden.

Als nächstes großes Kapitel verlangt die BaFin ein Informationssicherheitsmanagement. Dies besteht aus einer Informationssicherheitsleitlinie und verschiedenen Informationssicherheitsrichtlinien, in der Regel für die Bereiche Netzwerksicherheit, Kryptographie, Authentisierung und Protokollierung. Dazu gehört zum Beispiel eine Passwortrichtlinie, in der festgelegt wird, wie Passwörter zusammengesetzt sind, wer sie vergeben kann, wann sie zu ändern sind usw. Zu dem Thema Netzwerksicherheit gehören beispielsweise Themen wie eine Zonierung des Netzwerks oder ein Firewall-Konzept, Maßnahme zur Verhinderung des unerwünschten Abflusses von Daten durch Ports, Schnittstellen, wie zum Beispiel USB-Anschlüsse. Dabei spielen auch Sicherheitsthemen wie Brandschutz in Rechenzentren, Brandlasten, Löschvorrichtungen und Schutzmaßnahmen für die IT-Infrastruktur gegen Hochwasser oder andere Naturereignisse eine wichtige Rolle.

Es ist vor allem die Bundesbank, die bei verschiedenen Untersuchungen in Instituten sehr hohe Maßstäbe anlegt, wie zum Beispiel unabhängig voneinander laufende Rechenzentren, ausreichende Distanz der Rechenzentren, Brandschutz, einschließlich personaler Ausstattung der Rechenzentren usw. In der Praxis bemängelt die BaFin zum Beispiel, wenn bei Systemzugriffen keine Protokollierung erfolgt, zum Beispiel wenn Systemadministratoren auf die Systeme zugreifen. Notwendig ist unter anderem eine Auswertung der CERT-Bund-Meldungen des Bundesamtes für Sicherheit in der Informationstechnologie, Vorgaben für Penetrationstests sowie ein Überwachungs- und Analyseverfahren bei Vorfällen im IT-System. Die BaFin verlangt einen Informationssicherheitsbeauftragten, der die Einhaltung der Informationssicherheitsleitlinie und der Richtlinien überprüft. Der Informationssicherheitsbeauftragte soll die Geschäftsleitung mindestens vierteljährlich über den Status der Informationssicherheit im Institut berichten. Dabei reicht es der BaFin und der Bundesbank nicht aus, in der Gremiensitzung einen Tagesordnungspunkt IT festzulegen und freundlich darüber zu plaudern, notwendig ist ein schriftlicher Bericht mit klaren Aussagen.

Ein weiterer Baustein ist die Benutzerberechtigung. Nicht jeder Mitarbeiter darf auf alle Daten des Instituts zugreifen können, es gilt das „Need to know“-Prinzip. Dazu können Daten auf verschiedene Laufwerke gespeichert werden, auf die nicht jeder Mitarbeiter Zugriff hat. Bei der Personalabteilung und deren Personaldaten ist das eine Selbstverständlichkeit, es gilt aber auch für die Bereiche der unterschiedlichen Wertpapierdienstleistungen, Buchhaltung, Geschäftsleitungsaufgaben usw. Die BaFin legt großen Augenmerk darauf, dass bei ausgeschiedenen oder in andere Abteilung wechselnden Mitarbeitern die Berechtigungen gelöscht oder geändert werden, und das nicht erst nach Wochen oder Monaten, sondern unverzüglich. Augenmerk muss auch auf die sogenannten Administratoren gelegt werden, die alle Daten sehen können.

Vorgaben gibt es vor allem auch für IT-Projekte. Es darf nicht jeder Mitarbeiter und jede Abteilung eigene IT einfach entwickeln und irgendwie andocken, IT-Projekte müssen gesteuert werden, die Risiken daraus analysiert werden und vor Implementierung sind Tests durchzuführen, eine anschließende Abnahme und Freigabe will die BaFin sehen.

Augenmerk ist auch auf Auslagerungen zu legen. Dazu sind alle Verträge im IT-Bereich zu analysieren, ob sie eine Auslagerung enthalten. Das kann nach Auffassung der Bundesbank schon bei der Nutzung von Cloud-Lösungen der Fall sein, wenn das Institut nicht mehr die

vollständige Kontrolle über die in die Cloud zu speichernden Daten behält. Diese Vertragsverhältnisse sind auch entsprechend zu überwachen und zu kontrollieren, vor allem hinsichtlich des Ausfallrisikos des Dienstleisters. Dazu gehört ein Notfallwiederherstellungsplan mit Wiederherstellungszeiten.

In dem Bereich der BAIT dürfte der bankaufsichtsrechtliche Anspruch und die Realität am meisten auseinanderklaffen. Gefahr droht hier von der Bundesbank, weil diese die BAIT als Konkretisierung der MaRisk definiert und sich als Gralshüter dieser Mindestanforderungen versteht.

Nehmen Sie das Thema daher bitte nicht auf die leichte Schulter.

Mit den besten Grüßen
Ihr
Dr. Christian Waigel
Rechtsanwalt