Dr. Christoph Schulte, Frankfurt am Main

VAIT – Versicherungsaufsichtliche Anforderungen an die IT für VU und EbAV*

Die BaFin hat im März 2018 ein neues Rundschreiben angekündigt, welches die versicherungsaufsichtlichen Anforderungen an die IT für Versicherungsunternehmen und Einrichtungen der betrieblichen Altersversorgung (EbAV) formuliert. Dieses Rundschreiben richtet sich primär an die Geschäftsleitung der Unternehmen mit dem Ziel, einen Rahmen für das Informationsrisiko- und Informationssicherheitsmanagement zu schaffen. Gleichzeitig soll das Risikobewusstsein im Unternehmen und gegenüber den Dienstleistern geschärft werden.

Stellungnahmen zum Konsultationsentwurf konnten bis zum 20.4.2018 bei der BaFin eingereicht werden, zwischenzeitlich sind auf der Internetseite der BaFin fünf Stellungnahmen veröffentlicht.

Bereits Ende 2017 hat die BaFin mit dem Rundschreiben R10/2017 (BA) die bankaufsichtlichen Anforderungen an die IT (BAIT) veröffentlicht. BAIT und VAIT sind in ihrer Gliederung sehr ähnlich, unterscheiden sich aber z.B. im Begriff des „Risikoprofils", welchen die BAIT nicht kennt und welcher in der VAIT Wesensart, Umfang und Komplexität der Tätigkeit des Unternehmens widerspiegelt. Unternehmen sollen ihr Risikoprofil bestimmen und darauf aufbauend die dafür maßgebliche Regelungstiefe der VAIT festlegen.

Ziel dieses Beitrages ist es, einen Überblick über die wesentlichen Punkte der VAIT zu geben. Die Struktur der folgenden Abschnitte orientiert sich am Aufbau des Rundschreibens, sodass die korrespondierenden Abschnitte im Rundschreiben leicht gefunden werden können.

* Vortrag gehalten auf der Tagung der Fachvereinigung Pensionskassen am 4.5.2018 in Berlin.

Vorbemerkungen

Die VAIT gilt für alle § 1 Abs. 1 VAG unterfallenden Unternehmen, dies sind im Wesentlichen alle Versicherungsunternehmen, Pensionskassen und Pensionsfonds. Sie finden keine Anwendung auf Versicherungs-Zweckgesellschaften nach § 168 VAG und auf Sicherungsfonds im Sinne von § 223 VAG.

Für Unternehmen, die den Regelungen von Solvency II unterliegen, gelten daneben auch die Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen (MaGo). Die darin enthaltenen Anforderungen gelten unabhängig von den VAIT und sind, soweit es Überschneidungen gibt, parallel zu erfüllen.

Das Rundschreiben formuliert die Themenbereiche und deren Regelungstiefe nicht abschließend, sondern verweist selber wiederum auf gängige IT-Standards, z.B. die IT-Grundschutzkataloge des BSI oder die Standards ISO 2700x. Eine tatsächliche Zertifizierung nach einem dieser Standards kann für den Nachweis, dass daraus abgeleitete Anforderungen der VAIT erfüllt sind, hilfreich sein, wird aber von der VAIT selbst nicht gefordert; das Unternehmen kann für sich auch entscheiden, dass es sich beim Aufbau seiner IT an einem dieser Standards orientiert, ohne eine tatsächliche Zertifizierung anzustreben oder durchzuführen.

Zwei wesentliche Begriffe in dem Rundschreiben sind die „Proportionalität" und „Kritikalität". Im Rahmen der Proportionalität soll jedes Unternehmen sein Risikoprofil bestimmen und anhand dieses Risikoprofils die Umsetzung der VAIT ausrichten. Für die Proportionalität ist nicht nur auf das selbst betriebene Geschäft abzustellen, sondern sind auch Tätigkeiten und Mitarbeiterkapazitäten, die im Rahmen von Ausgliederungen durch externe Dienstleister erbracht werden, einzubeziehen.

Für die Kritikalität sind alle Informationen, welche für die Prozesssicherheit notwendig und unter dem Datenschutz schützenswert sind, zu berücksichtigen. Hierunter dürften in den meisten Fällen zumindest alle diese Prozesse fallen, für die im Falle einer Ausgliederung ein Ausgliederungsvertrag nach § 32 VAG notwendig wäre. Wichtig ist in diesem Zusammenhang, alle kritischen Informationen zu betrachten, auch solche, welche beispielsweise in Office-Dokumenten enthalten sind.

IT-Strategie

Das erste Modul der VAIT befasst sich mit der IT-Strategie, welche in konsistenter und nachhaltiger Weise von jedem Unternehmen zu erstellen ist, auch von Unternehmen, die ihren gesamten IT-Betrieb ausgelagert haben.

Die Mindestinhalte der IT-Strategie beinhalten die strategische Entwicklung der IT-Aufbau- und IT-Ablauforganisation, der Ausgliederungen von IT-Dienstleistungen bzw. sonstiger IT-Dienstleistungen sowie den sonstigen Bezug von IT (Hard- und/oder Software). Weitere Aspekte der IT-Strategie sind Standards, an denen sich das Unternehmen orientiert, die Informationssicherheit, IT-Architektur, das Notfallmanagement und die von Fachbereichen selbst entwickelten IT-Systeme.

Die gesamte Geschäftsleitung ist für die IT-Strategie sowie deren regelmäßige Überprüfung und Aktualisierung verantwortlich. Die IT-Strategie ist dem Aufsichtsorgan des Unternehmens vorzulegen und ggf. zu erörtern.

IT-Governance

Im Rahmen der IT-Governance sind alle Prozesse, Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen und Kommunikationswege zu definieren. Die hierin aufgestellten Regeln sind auch auf ausgegliederte Dienstleistungen anzuwenden. Es ist sicherzustellen, dass die IT mit ausreichend Personal ausgestattet ist. Alle Mitarbeiter müssen über ausreichende Kenntnisse und Erfahrung im Bereich der IT verfügen.

Informationsrisikomanagement

Für das Informationsrisikomanagement ist der notwendige Schutzbedarf der EbAV zu definieren, auch für Risiken, die aus ausgelagerten Dienstleistungen entstehen können. Für ausgelagerte Dienstleistungen sind die identifizierten Risiken im Auslagerungsvertrag zu berücksichtigen und die vereinbarten Maßnahmen durch die EbAV zu kontrollieren.

Konkret sind die folgenden Schritte notwendig:

- Festlegung der IT-Risikokriterien,
- Identifikation von IT-Risiken,
- Schutzbedarf festlegen bzgl. Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität (niedrig, mittel, hoch, sehr hoch),
- Schutzmaßnahmen und
- Risiko der verbliebenen Restrisiken.

Die Geschäftsleitung ist mindestens vierteljährlich in einem Statusbericht über die Ergebnisse der Risikoanalyse zu informieren, wobei das Unternehmen für sich festlegen kann, dass dieser vierteljährliche Statusbericht nur an den zuständigen Geschäftsleiter geleitet wird. Der jährliche Bericht der Risikoanalyse ist an die gesamte Geschäftsleitung zu erstellen.

Informationssicherheitsbeauftragter (ISB)

Dem Informationssicherheitsbeauftragten (ISB) wird in der VAIT eine zentrale Rolle zugewiesen und grundsätzlich ist jedes Unternehmen verpflichtet, einen ISB zu benennen.

Die Aufgabe des ISB kann durch eine oder mehrere natürliche Personen wahrgenommen werden, wobei im Falle von mehreren Personen eine die Verantwortung zu übernehmen hat, dass die Aufgaben des ISB ordnungsgemäß erfüllt werden. Der ISB ist selbst nicht operativ tätig und hat eine überwachende Funktion, innerhalb der er sicherstellt, dass die IT-Strategie, die Informationssicherheitsleitlinie und die Informationssicherheitsrichtlinien im Unternehmen und – sofern relevant – beim Dienstleister transparent gemacht werden. Des Weiteren überprüft er, dass diese auch eingehalten werden.

Zentrale Aufgabe des ISB ist der Aufbau eines Informationssicherheitsmanagementsystems (ISMS). Darüber hinaus ist er an allen IT-Projekten zu beteiligen, wobei in der Praxis sich diese Beteiligung auf wesentliche Projekte beschränken wird und ansonsten eine Information stattfinden wird.

Informationssicherheitsmanagement

Das Informationssicherheitsmanagement findet in zwei Schritten statt: Übergeordnet wird von der Geschäftsleitung eine Informationssicherheits*leitlinie* erstellt. Auf deren Grundlage erstellt der ISB konkretisierende Informationssichheits*richtlinien*. Informationssicherheitsrichtlinien sollen beispielsweise für die Felder Netzwerksicherheit, Kryptografie, Authentisierung und Protokollierung erstellt werden und sich in die Teilprozesse

- Identifizierung des Bedarfs,
- Maßnahmen, mit denen der notwendige Schutz erreicht werden kann,
- Möglichkeiten, Verletzungen des Schutzbedarfs zu entdecken sowie
- Regelungen, wie auf Abweichungen vom Regelbetrieb reagiert werden soll und der Regelbetrieb wiederhegestellt werden kann,

untergliedern.

Benutzerberechtigungsmanagement

Das Benutzerberechtigungsmanagement ist entsprechend den organisatorischen und fachlichen Vorgaben des Unternehmens auszugestalten. Berechtigungen sind konsistent zum Schutzbedarf, unter Beachtung von Funktionstrennungen und dem Grundsatz der Sparsamkeit sowie unter Vermeidung von Interessenkonflikten zu vergeben.

Berechtigungen sind regelmäßig zu überprüfen, für kritische Berechtigungen wie Administratoren mindestens alle sechs Monate, für wesentliche Berechtigungen mindestens alle zwölf Monate und alle anderen mindestens alle drei Jahre.

Zu beachten ist, dass auch technische User, die in Systemen z.B. für automatisierte Änderungen vorhanden sein können, immer einer natürlichen Person zugeordnet sein müssen.

IT-Projekte, Anwendungsentwicklung

Aus IT-Projekten können erhebliche Risiken im Hinblick auf Dauer, Ressourcenverbrauch und Qualität der Geschäftsabläufe entstehen. Aufgrund der Bedeutung der IT für den Geschäftsbetrieb wird deshalb durch die VAIT auch von der Aufsicht gefordert, dass IT-Projekte angemessen gesteuert werden und der Geschäftsleitung über wesentliche IT-Projekte regelmäßig berichtet wird. Im Rahmen der Anwendungsentwicklung sind auch durch die Fachabteilungen erstellte IDV-Anwendungen zu inventarisieren, daraus entstehende Risiken zu identifizieren und ein ausreichender Schutzbedarf sicherzustellen.

Eine zunächst selbstverständliche Anforderung ist, dass IT-Systeme vor ihrer Übernahme in den produktiven Betrieb fachlich und technisch zu testen sind. Trotzdem muss jedes Unternehmen für sich festlegen, in welcher Tiefe die Tests im Einzelfall erfolgen sollen: Sicherheitspatches, die an einen großen Nutzerkreis verteilt werden und die ggf. bestehende Sicherheitslücken schließen, sollten nicht länger als unbedingt notwendig getestet werden, wohingegen eine individuell erstellte Spezialanwendung eher detailliert getestet werden sollte. Ein anderer Aspekt sind Cloudanwendungen und Software as a Service, bei denen das Unternehmen keine Vorabkontrolle neuer Softwareversionen durchführen kann und sich daher beim Dienstleister überzeugen muss, dass dieser Tests vorab in ausreichendem Maße durchführt.

IT-Betrieb

Das Portfolio der IT-Systeme ist angemessen zu steuern, auch im Hinblick auf Risiken, die aus veralteten Systemen resultieren könnten. Für sämtliche eingesetzte Hard- und Software ist ein Lebenszyklusmanagement durchzuführen.

Für die Datensicherung sind die notwendigen Verfahren festzulegen sowie das Verfahren zur Wiederherstellung von Daten. Dieses Verfahren ist regelmäßig – mindestens einmal jährlich – zu testen.

Für sämtliche eingesetzten IT-Komponenten ist ein Bestandsregister zu führen, welches den Bestand und Verwendungszweck, den Standort, den Supportzeitraum und die akzeptierte Nichtverfügbarkeit jeder Komponente beschreibt. Alle Änderungen, z.B. aufgrund von Erweiterungen, Fehlerbehebungen oder Ersatzbeschaffungen, sind zu dokumentieren.

Ausgliederungen von IT-Dienstleistungen

Für jede IT-Dienstleistung ist vorab eine Risikoanalyse durchzuführen. Diese Analyse muss nicht nur die direkt beauftragte Dienstleistung berücksichtigen, sondern auch alle Subdelegationen, die durch den beauftragten Dienstleister wiederum hinzugezogen werden. Alle Ausgliederungen sind im Einklang mit der IT-Strategie und der Risikoanalyse zu steuern und in einer vollständigen und strukturierten Vertragsübersicht vorzuhalten.

Fazit und Ausblick

Die Veröffentlichung des Rundschreibens ist für den Sommer 2018 angekündigt. Die BaFin hat in der Ausgabe 04/2018 des BaFin-Journals mitgeteilt, dass die VAIT keine neuen Anforderungen an die Unternehmen und ihre IT-Dienstleister darstellt, sondern vielmehr die bereits bestehenden Anforderungen erläutern und konkretisieren. Folglich wird es für die VAIT keine Umsetzungsfrist geben. Dies bedeutet für die betroffenen Unternehmen, dass sie sich schon jetzt mit dem vorliegenden Entwurf beschäftigen müssen, insbesondere

- ist das Risikoprofil des Unternehmens zu erstellen,
- ist eine Analyse der bereits erfüllten und entsprechend der VAIT dokumentierten Anforderungen durchzuführen,
- ist diese einem Soll-Ist-Vergleich zu unterziehen und sind Defizite und Maßnahmen – auch unter Berücksichtigung von Innovationen und Weiterentwicklungen – zu identifizieren.

Die BaFin hat ferner bereits angekündigt, dass sie prüfen wird, Teile der von den G7-Staaten identifizierten „Wesentliche[n] Elemente der Cybersicherheit" in die VAIT zu übernehmen. Als mögliche Themen wurde das Notfallmanagement sowie Test- und Wiederherstellungsverfahren genannt. Ferner ist angedacht, für Betreiber kritischer Infrastrukturen ein Modul „Kritische Infrastruktur" einzuführen.

Insbesondere für internationale Unternehmen und internationale IT-Dienstleister ist auch eine englische Übersetzung angekündigt.