BANKING HUB by zeb

STEUERUNG

VAIT für Versicherungen? Von Banken lernen

Kreditinstitute und ihre IT-Dienstleister haben einen Erfahrungsvorsprung

16. Juli 2019

Die BaFin zieht bei Versicherungen die regulatorischen Zügel fester an. Insbesondere das sofortige Inkrafttreten der „Versicherungsaufsichtlichen Anforderungen an die IT“ (VAIT) zwingt Assekuranzen zum Handeln. Ein Blick in die Bankenbranche zeigt, wie der Umgang mit vergleichbarer Regulatorik gelingen kann.

Die Veröffentlichung der VAIT markiert eine Zeitenwende. Zwei deutliche Signale sendet die Aufsicht damit an Versicherungen.

Erstens: Künftig prüft die BaFin jeden Versicherer – ohne Ausnahme. Zweitens: Die VAIT gelten ab sofort – ohne Übergangsfrist, da die Inhalte der Branche schon bekannt sind. Die VAIT erläutern die „Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen“ (MaGo) durch konkrete Ziele für die IT in Assekuranzen.

Mit den Vorgaben trägt die Aufsicht der wachsenden Bedeutung der IT und den damit verbundenen steigenden IT-Risiken Rechnung. Sie will Standards für den verlässlichen IT-Betrieb etablieren. Außerdem soll das IT-Risikobewusstsein der Verantwortlichen innerhalb des Unternehmens und gegenüber deren IT-Dienstleistern erhöht werden.

Banken als Vorbild

Vor dieser neuen Realität können Versicherer die Augen nicht verschließen. Statt wegschauen lohnt ein Seitenblick auf die Bankbranche. Denn im Umgang mit regulatorischen Vorgaben verfügen Kreditinstitute und ihre IT-Dienstleister über einen Erfahrungsvorsprung. Die „Bankenaufsichtlichen Anforderungen an die IT“ (BAIT) sind mit der VAIT durchaus vergleichbar. Sie sind gleich aufgebaut und verfolgen dasselbe Ziel. Versicherungen können also die Kenntnisse der Banken zum eigenen Vorteil nutzen und sich so besser auf Prüfungssituationen vorbereiten. Das gelingt, wenn Assekuranzen die Prüfungsthemen durchgängig, vollständig und nachhaltig behandeln. Wichtig ist, dass sie auch eingeführte Standards stets hinterfragen.

VAIT – was Prüfer wollen

Im Bereich *„IT-Strategie“* erwarten die Prüfer, dass Versicherer eine aktuelle IT-Strategie haben, die sich aus der Geschäftsstrategie ableitet. Wichtig dabei sind etablierte

Standards, die Fortschreibung der IT-Architektur und Aussagen zur IT-Sicherheit sowie zum Notfallmanagement.

Die *„IT-Governance“* beschreibt Mechanismen, um den IT-Betrieb zu steuern, zu überwachen und weiterzuentwickeln. Die BaFin legt dabei besonderen Wert auf Prozesse, die sich an gängigen Standards orientieren sowie auf eine sowohl qualitativ als auch quantitativ ausreichende Personalausstattung.

„Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität“ (VIVA): Diese vier Schutzziele müssen Versicherungen im Rahmen des *„Informationsrisikomanagement“* bei der Ermittlung des Schutzbedarfs und etwaiger Abweichungen beachten. Erkannte Risiken sind angemessen zu bewerten, zu überwachen, zu steuern und zu berichten.

Beim Prüfungsthema *„Informationssicherheitsmanagement“* setzt die Aufsicht voraus, dass Versicherer Maßnahmen stets an den aktuellen Stand der Technik und der jeweiligen Bedrohungslage anpassen. Dabei ist die Position des Informationssicherheitsbeauftragten professionell zu besetzen. Zu seinem Verantwortungsbereich gehört es, Sicherheitsrichtlinien zu definieren und aktuell zu halten.

Die Prüfungen im Bankensektor haben im Bereich *„Benutzerberechtigungsmanagement“* Lücken offenbart. Der Fokus der Prüfer liegt auf Vollständigkeit, Durchgängigkeit und Konsistenz etwa beim Umgang mit Nutzern. Ihnen stehen nur die Rechte zu, die den fachlichen und organisatorischen Vorgaben des Unternehmens entsprechen. Alle erteilten Berechtigungen sind regelmäßig zu überprüfen und anzupassen.

Die BaFin hinterfragt im Prüfungsfeld *„IT-Projekte und Anwendungsentwicklung“*, ob Versicherer bei wesentlichen

Veränderungen an Anwendungen etwaige Auswirkungen auf Prozesse und Strukturen der IT bewerten. Dabei setzt sie eine nachvollziehbare und durchgehende Dokumentation voraus. Die VAIT schließen auch individuell entwickelte Anwendungen ein. Außerdem müssen IT-Projekte angemessen gesteuert und eine Transparenz über das Gesamtportfolio von IT-Projekten und deren Risiken hergestellt werden.

Aus Sicht der Aufsicht sind der Überblick über IT-Komponenten und deren Beziehungen zueinander (Configuration Management System) sowie das Business Continuity Management wesentlicher Bestandteil des *IT-Betriebs*. Zu Letzterem zählen durchgängige Verfahren zur Datensicherung und Wiederherstellbarkeit, um einen unterbrechungsfreien Betrieb zu garantieren. Dafür bedarf es auch eines redundanten Rechenzentrumsstandorts. Gerade diese Vorgaben setzen Versicherungen oftmals noch nicht um. Sie vertrauen auf einen einzigen Standort. Versicherungen dürfen dabei eines nicht vergessen: Bei *Ausgliederungen* der IT, gilt die Einhaltung der Vorgaben aus den VAIT auch für die IT-Dienstleister sowie Subdienstleister.

Umsetzung VAIT – zukunftssichere IT?

Eine intensive Auseinandersetzung mit der VAIT ist zwingend erforderlich. Auch deren Umsetzung sollte kurzfristig erfolgen. Herausfordernd sind dabei die Risiken aus veralteten IT-Systemen. Daher ist es wichtig, dass Versicherer ihre

IT-Landschaft eingehend analysieren. Sie kommen dabei zu der Erkenntnis, dass die Auslagerung des IT-Betriebs folgerichtig ist. Nicht nur die Regulatorik, sondern auch der Kostendruck sowie der Fachkräftemangel von IT-Mitarbeitern beeinflussen die Entscheidungsfindung.

Somit tritt die Frage nach der künftigen IT-Landschaft in den Hintergrund. Vielmehr fragen sie sich, welcher IT-Dienstleister der richtige ist. Denn die Auswahl an möglichen Partnern ist überschaubar. Nicht zuletzt, weil sich zahlreiche IT-Dienstleister aufgrund der regulatorischen Hürden aus dem Markt für Banken und Versicherungen zurückgezogen haben. Hier schlägt die Stunde der Spezialisten, die bereits für Banken tätig sind. Ihr Vorteil: Erfahrungen mit aufsichtlichen Vorgaben wie BAIT und grundlegendes Wissen aus Prüfungssituationen. Daher können sie Versicherungen unterstützen, die VAIT umzusetzen.

Lösungen für Versicherungen

Die Anforderungen an Banken haben an zahlreichen Stellen Handlungsbedarf offenbart. Welchen Beitrag können IT-Partner leisten? Sie bieten etwa Services für das Benutzerberechtigungsmanagement. Mit einem Identity-and-Access-Management-System lassen sich etwa Zugriffsrechte zentral steuern. Ein weiteres Tool ist eine Security-Information-and-Event-Management-Plattform (SIEM). Hier lassen sich die Log-Daten aller IT-Systeme revisionssicher sowie zentral speichern und archivieren. Auch beim Thema unterbrechungsfreier IT-Betrieb sind IT-Provider gut aufgestellt. Denn redundante Standorte sind für sie selbstverständlich. Und mit Schwenktests oder Schwachstellen-Scans sorgen sie permanent für einen weitreichenden Schutz der IT.

Wenn der Prüfer vor der Tür steht

Wenn Versicherungen mit versierten IT-Dienstleistern zusammenarbeiten, können sie beruhigter auf den Besuch der Prüfer blicken. Denn IT-Partner setzen die aktuellen Vorgaben wie VAIT vollständig um und richten den IT-Betrieb entsprechend aus. Gleichzeitig begleiten sie die Versicherer auf den technologischen Weg in die Zukunft. Dieser führt in die Cloud. Aber nur in eine aufsichtskonforme.

IT, Regulatorik, VAIT, Versicherungen

Kommentieren

Dr. Christian Thiel
Generalbevollmächtigter
Finanz Informatik Technologie Service GmbH& Co. KG
(FI-TS)

PROFIL ANSEHEN