IT Finanzmagazin
Das Fachmagazin für IT und Organisation bei Banken, Sparkassen und Versicherungen

STRATEGIE

21. Januar 2019

MaGo, VAIT & BAIT? Was Versicherer von Banken lernen können – von der Regulierung zur IT

Das ist neu für Versicherer: Zukünftig wird die BaFin jeden Versicherer prüfen. Ohne Ausnahme. Auch neu sind die „Versicherungsaufsichtlichen Anforderungen an die IT" (VAIT). Sie bilden die Grundlage für künftige Prüfungen. Wie die Umsetzung gelingen kann, zeigt der Blick in die Bankenbranche.

von Dr. Christian Thiel und Hans Schätzle, Finanz Informatik Technologie Service

Dr. Christian Thiel, Generalbevollmächtigter und Produkt- und Innovationsmanagement, FI-TS Quelle: FI-TS

Mit der VAIT hat die BaFin eine Zeitenwende eingeläutet und die bisherige Praxis der sporadischen Prüfungen beendet. Außerdem sind die Vorgaben sofort zu erfüllen. Da mag es tröstlich erscheinen, dass diese der Branche immerhin bekannt sind. Denn die VAIT konkretisieren lediglich bestehende Regularien wie etwa die MaGo .

> *„Das Ziel sind Standards für den verlässlichen Betrieb von IT-Systemen. Die Prüfer setzen voraus, dass Assekuranzen diese Themen durchgängig, vollständig und nachhaltig behandeln."*

Ein Blick zur Seite

Hans Schätzle,, Vertrieb & Kundenbetreuung FI-TS

Quelle: FI-TS

Angesichts der VAIT hilft es nicht, wenn Versicherungen der Vogel-Strauß-Taktik folgend den Kopf in den Sand stecken. Wie also das Thema angehen? Ein Blick in die Welt der Banken ist hilfreich. Denn Kreditinstitute und ihre IT-Dienstleister verfügen bereits über Erfahrungen mit aufsichtsrechtlichen Vorgaben wie etwa den „Bankenaufsichtlichen Anforderungen an die IT" (BAIT). Beide Regelwerke sind gleich aufgebaut und verfolgen dasselbe Ziel. Versicherungen können also die Erfahrungen der Banken für sich nutzen. Es sind acht Themenfelder erkennbar:

1. **IT-Strategie:**
Wichtig ist der Aufsicht, dass die IT der Gesamtstrategie des Versicherungsunternehmens folgt und dabei konsistent ist. Im Einzelnen hinterfragen die Prüfer die Aufbau- und Ablauforganisation, die Weiterentwicklung der IT-Architektur sowie Zuständigkeiten der Informationssicherheit.

2. **IT-Governance:**
Hier stehen die Steuerung und Überwachung des IT-Betriebs sowie die Weiterentwicklung von IT-Systemen unter Einbeziehung der entsprechenden IT-Prozesse im Mittelpunkt.

3. **Informationsrisiko-Management:**
„Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität" (VIVA): Das sind die vier Schutzbedarfsziele, die Versicherungen laut BaFin beim Umgang mit IT-Risiken beachten müssen.

4. **Informationssicherheits-Management:**
Hier erwartet die BaFin, dass Versicherungen die Position des Informationssicherheitsbeauftragten mit einem Experten besetzen. Er ist frühzeitig bei allen relevanten Vorfällen einzubinden und direkt der Geschäftsführung oder dem Vorstand unterstellt. Zu seinem Verantwortungsbereich gehört es, Sicherheitsrichtlinien zu definieren und diese aktuell zu halten.

5. **Benutzerberechtigungs-Management:**
Die Prüfungserfahrungen im Bankensektor zeigen, dass die Zuweisung von Rollen und Nutzerrechten und deren regelmäßige Überprüfung häufig lückenhaft sind. Daher erwartet die Behörde Vollständigkeit, Durchgängigkeit und Konsistenz etwa beim Umgang mit hochprivilegierten Nutzern.

Versicherungen müssen Funktionen sauber zwischen Anwendungsentwicklung und Produktion trennen. Programmierer aus der Anwendungsentwicklung haben dann keinen direkten Zugriff auf Daten aus der Produktion.

6. **IT-Projekte und Anwendungsentwicklung:**
Die BaFin hinterfragt, ob Änderungen, Tests und die Produktivsetzung von Anwendungen nachvollziehbar und durchgehend dokumentiert sind. Sie erwartet zudem eine eindeutige Trennung zwischen Entwicklungs-, Test- und Produktionssystemen.

7. **IT-Betrieb:**
Verfahren zur Datensicherung und Wiederherstellbarkeit im Sinne eines durchgängigen Business Continuity Management garantieren aus Sicht der Aufsicht einen unterbrechungsfreien IT-Betrieb. (Anmerkung: Die Wirklichkeit ist eine andere. Noch setzen viele Versicherungen auf einen einzigen Rechenzentrums-Standort und kommen dem Postulat der Aufsicht nach georedundanten Standorten nicht nach.)

8. **Ausgliederungen:**
Nicht nur Versicherungen, sondern auch deren IT-Dienstleister sowie Subdienstleister müssen sich mit der VAIT auseinandersetzen und die Vorgaben zeitnah erfüllen.

Quo Vadis Versicherungen?

> *„Assekuranzen müssen sich intensiv mit der VAIT auseinandersetzen und die Vorgaben kurzfristig erfüllen – daran führt kein Weg vorbei.“*

In diesem Zusammenhang sind sie gut beraten, ihre gewachsenen IT-Strukturen zu hinterfragen. Angesichts des aktuell hohen Kostendrucks in der anhaltenden Niedrigzinsphase sowie dem IT-Fachkräftemangel überdenken Versicherungen ihre IT-Strategie. Dabei ziehen immer mehr Verantwortliche die Auslagerung der IT-Infrastruktur in Betracht. Somit setzen sich Versicherungen mit der Frage auseinander, welche IT-Dienstleister ihre Anforderungen erfüllen können. Denn der Kreis potenzieller Provider ist klein. Er beschränkt sich auf Spezialisten, die bereits in der Finanzwirtschaft tätig sind. Diese haben bereits Erfahrungen mit der BAIT sammeln können. Deshalb sind ihre großen Pluspunkte die Erfahrung mit Prüfungen und das Know-how bei der Umsetzung aufsichtsrechtlicher Vorgaben. Daher können sie auf dieser Basis Versicherungen bei der Umsetzung der VAIT unterstützen.

Ein Beispiel sind etwa Services, mit denen Versicherungen die Vorgaben der Aufsicht beim Benutzerberechtigungs-Management erfüllen können. Ein Identity-and-Access-Management - System (IAM) sorgt für eine zentrale Verwaltung von Identitäten und Zugriffsrechten auf unterschiedlichen Systemen und Applikationen. Das IAM erteilt und entzieht Zugriffsrechte in Echtzeit. Auch beim Thema Ausfallsicherheit haben IT-Provider zeitgemäße Lösungen im Portfolio. Denn für versierte IT-Dienstleister gehört der Rechenzentrums-Betrieb an räumlich getrennten Standorten zum Selbstverständnis. Gleichzeitig nutzen sie Verfahren wie etwa Schwenktests oder Schwachstellen-Scans, um die Sicherheit der Daten dauerhaft zu gewährleisten.

VAIT: Zukunftssicher IT betreiben

Wenn sich Versicherungen für die Auslagerung ihres IT-Betriebs entscheiden, profitieren sie auf mehreren Ebenen. Denn IT-Provider setzen nicht nur State-of-the-Art-Technologien ein und unterstützen Versicherungen auf dem Weg in die Cloud. Sie richten diese Infrastrukturen gleichzeitig regulationskonform aus und sorgen für die Umsetzung der aktuellen Vorgaben wie etwa der VAIT. Gleichzeitig müssen Versicherungen, die sich für eine Zusammenarbeit mit dem richtigen IT-Partner entscheiden, den Besuch der BaFin nicht fürchten. ▪

Autoren Dr. Christian Thiel und Hans Schätzle, FI-TS

Dr. Christian Thiel ist Generalbevollmächtigter bei Finanz Informatik Technologie Service (FI-TS). Er verantwortet seit 2015 das Produkt- und Innovationsmanagement sowie die Beratung und das technische Lösungsdesign. Sein Fachgebiet sind aufsichtsrechtliche Anforderungen in der Finanz- und Versicherungsbranche an die IT. Von 2011 bis 2015 war er verantwortlich für die Unternehmensentwicklung bei FI-TS. Vor seinem Eintritt in FI-TS war er von 2004 bis 2011 in einer internationalen Strategieberatung tätig. Dort lag sein Fokus auf IT-Dienstleistern für Banken und Versicherungen mit dem fachlichen Schwerpunkt auf IT Strategie, IT-Transformation, IT-Konsolidierung (Pre-Merger, Post-Merger) und Organisationsdesign. Er studierte Wirtschaftsinformatik an der Technischen Universität Darmstadt und promovierte in Organisations- und Entscheidungstheorie am Karlsruher Institut für Technologie (KIT).

Hans Schätzle ist bei der Finanz Informatik Technologie Service GmbH& Co. KG (FI-TS) für

den Vertrieb und die Kundenbetreuung des kompletten Versicherungsmarktes und das Marketing der FI-TS (Bank und Versicherung) verantwortlich. Nach Abschluss des Studiums als Diplom-Betriebswirt (FH) beschäftigt er sich seit fast 20 Jahren mit Prozessen und IT im Finanzumfeld bei Banken und Versicherungen. Im speziellen war er bei verschiedenen Banken, Outsouring- und IT Dienstleistern wie z.B. der Coface Deutschland AG, Arvato Financial Solutions oder aktuell bei FI-TS tätig.

Sie finden diesen Artikel im Internet auf der Website:
https://itfm.link/83839