Bericht vom 42. Versicherungswissenschaftlichen Fachgespräch
„VAIT - ein Jahr versicherungsaufsichtsrechtliche Anforderungen an die IT
- Herausforderungen für Versicherer und Vermittler“

Erstmals fand am 19. Juni 2019 ein Fachgespräch im Haus der KPMG statt. Der Vorstandsvorsitzende unseres Vereins **Olaf Dilge** begrüßte die Teilnehmer und Referenten und dankte Herrn Dr. Hasenburg als Vertreter des Gastgebers KPMG. Danach führte **Prof. Dr. Hans-Peter Schwintowski** von der HU Berlin als Moderator ins Thema ein und stellte die Referenten vor. Er warf die Fragen auf: Ist Risikomanagement – besonders im IT-Bereich – nicht für alle Unternehmen wichtig? Warum braucht gerade die Versicherungswirtschaft auch hier Vorgaben, die es für andere Branchen nicht gibt?

Als erster Redner stellte **Jens Wieland**, CIO und COO der W+W sich und sein Unternehmen vor. Durch die Aufteilung in Bausparkasse und Versicherungsunternehmen mit einem konzerneigenen IT-Dienstleister habe W+W bereits Erfahrungen mit der vergleichbaren Regelung für Banken (BAIT), die sehr ähnlich aussehe. Aus seiner Sicht handelt es sich bei VAIT nicht um ein „Konjunkturprogramm für Wirtschaftsprüfer und Berater, wie zuweilen behauptet werde. Neue Vorschriften würden natürlich ständige Anpassungen der Prozesse und internen Regeln erfordern. Sein Anspruch sei aber, dass Regulatorik nicht allein im Raum stehen solle, sondern gleichzeitig Nutzen stifte. Es dürfe nicht allein bürokratischer Aufwand entstehen. Sein Unternehmen nutze die Impulse, um durch verbesserte Prozesse Synergien zu heben. Dazu müssten alle Managementsysteme miteinander verknüpft und in Beziehung gesetzt werden. Wichtig sei, nicht losgelöst ein schönes Modell zu entwickeln, sondern es auch zu „leben“, was er am Beispiel „COBIT“ verdeutlichte. Dabei sei jeweils auf Angemessenheit zu achten. Vor diesem Hintergrund sei es zu begrüßen, dass die VAIT nur einen Regelungsrahmen vorgeben, den Unternehmen aber die Entscheidung überlasse, was jeweils adäquat und risikogemäß sei. Kritisch sehe er, sagte Wieland, den Teil „Auslagerung“. Hier bestehe die Gefahr des Kontrollverlustes. Es sei wichtig, einen intensiven Dialog mit den Praktikern der IT zu führen.

Das zweite Referat trug **Silke Brüggemann,** Referentin Grundsatz IT-Aufsicht und Prüfungswesen bei der BaFin, vor. Sie beschrieb zunächst das Ziel der VAIT, Geschäftsprozesse zu unterstützen und flexibel und angemessen dafür zu sorgen, dass Risiken der Versicherungsunternehmen und deren Kunden beherrscht werden können. Orientierung biete dabei auch der Blick auf die europäische Aufsichtsbehörde EIOPA, die andererseits aber auch Anregungen und Vorschläge der nationalen Behörden für Korrekturen und Ergänzungen erwarte. Im Folgenden stellte Brüggemann die inhaltlichen Schwerpunkte vor. Sie erklärte, was mit Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität der Daten und Systeme gemeint sei und welche Bedeutung vor dem Hintergrund zunehmender Cyber-Bedrohungen diese Fragen für die Unternehmen hätten. Einen detaillierten Einblick in die neun Bereiche der Anforderungen rundeten den Vortrag ab. Die Reaktionen auf die Veröffentlichung der VAIT seien positiv ausgefallen, weil die Unternehmen nun wüssten, was die Aufsicht von ihnen erwarte. Die nationalen und internationalen Erfahrungen würden sich gegenseitig beeinflussen und werden – so die Erwartung von Brüggemann – die Regelungen weiter optimieren.

Vaike Metzger, Partner IT Consulting Insurance KPMG AG, behandelte das Thema aus der Sicht des Prüfers und Beraters. Die Abgrenzung zwischen den Sicherheitszonen der 1. bis 3. Linie (Fachbereich, Risikomanagement und Revision) sei mitunter schwierig, je nach Größe und Organisation des Unternehmens. Die Steuerung über Ziele, Maßnahmen und Erfolgsmaße müsse sich am jeweiligen Risiko orientieren und lasse den Unternehmen Entscheidungsspielräume. Alle einschlägigen Standards komplett umzusetzen sei in den meisten Fällen ein deutliches „Zuviel“, was nicht nur kostenmäßig sondern auch organisatorisch unvernünftig sei. Das BSI z. B. liste allein über 40 IT-Risiken auf. Für die Bewertung des Umsetzungsgrades habe KPMG drei Quellen genutzt: Die Erkenntnisse aus Jahresabschlussprüfungen, Die Feststellungen aus Projekten und Sonderprüfungen und eine Umfrage 2018/2019. Dabei wurde ein – nach Einschätzung

der Befragten – relativ hoher Umsetzungsgrad festgestellt, aber auch eine relativ große Spreizung zwischen den weiter und den weniger entwickelten Unternehmen. Die Reifegrade unterschieden sich auch in den Teilbereichen. Als Fazit stellte Metzger fest, dass Standardisierung und Strukturierung mit Hilfe geeigneter Tools zur Hebung der Effizienz der Systeme beitragen werde. Sie sei gespannt darauf, welche Standards sich unter dem Einfluss der BaFin und ihrer Reaktionen etablieren würden.

Moderator Schwintowski fasste die Grundaussagen der drei Vorträge zusammen und eröffnete die Diskussion mit einem Zitat aus dem VAG. Er fragte: „Warum brauchen wir solche Regelung? Und wie soll man überhaupt bewerten, wie hoch ein bestimmtes Schadenpotenzial und damit der Schutzbedarf ist?“.

Brüggemann antwortete, die VAIT sollten Geschäftsorganisation und Governance unterstützen und zur Beherrschung operationaler Risiken beitragen. Wieland ergänzte, es sei relativ einfach, aus Eintrittswahrscheinlichkeit und erwarteter Schadenhöhe das Gefahrenpotenzial zu errechnen. Auch Metzger sprang bei und erklärte, die VU sollten kritische Geschäftsprozesse identifizieren, bewerten und dann angemessenen Sicherheit anstreben.

Fragen drehten sich dann um die Angemessenheit der Vorschriften, insbesondere für kleine Unternehmen mit nur 10 oder 20 Mitarbeitern, um Vergleiche zu anderen Industrien und den Umstand, dass viele zu schützende Daten von nicht regulierten Unternehmen, z. B. Maklern und Vermittlern stammen. Für Prüfungen der BaFin seien die VAIT keine große Hilfe. Sie könnten aber als Argument für ein gutes IKS helfen. Praxisberichte zu Aspekten einer „0-Fehler-Toleranz“ bzw. „IDV“ bereicherten das Gespräch.

Angesichts der lebhaften Diskussion schloss Schwintowski die Diskussion mit 10 Minuten Verspätung und Dilge bat im Namen der KPMG mit Dank an die Referenten, den Moderator und das Publikum zum „Get together“, bei dem noch lebhaft und lange weiterdiskutiert wurde.

Das 43. Versicherungswissenschaftliche Fachgespräch wird sich im "Tieranatomischen Theater“ der HU am 26.09.19 mit dem Thema „Maklerpools - Rolle – Funktionen – offene Fragen“ befassen.

Berlin, den 21.06.19
Dietmar Neuleuf