Versicherungswirtschaft: **VAIT-Novelle**

BaFin-Konsultation der neuen VAIT

metafinanz
Business & IT Consulting
We. Ensure. Success.

Die BaFin hat die Versicherungsaufsichtsrechtlichen Anforderungen an die IT (VAIT) überarbeitet und hierzu am 17. August 2021 eine öffentliche Konsultation gestartet.
Die überarbeitete VAIT beinhaltet die beiden neuen Kapitel „Operative Informationssicherheit“ und „IT-Notfallmanagement“. Außerdem wurden Anforderungen in bestehenden Kapiteln angepasst oder erweitert. Unternehmen haben bis zum 24. September 2021 Zeit, Stellung zu nehmen. Die neuen Regelungen sollen noch in diesem Jahr in Kraft treten.

Wesentliche Neuerungen

- Zwei neue Kapitel: „Operative Informationssicherheit“ und „IT-Notfallmanagement“
- IT-Sicherheit von Versicherern wird ganzheitlich betrachtet
- IT-Dienstleister werden auch im Rahmen des Informationsverbundes sowie der Schutzbedarfsfeststellung enger eingebunden
- Mitarbeiter*innen müssen kontinuierlich für IT-Sicherheit sensibilisiert und geschult werden

Mit der geplanten Novelle übernimmt die BaFin die **Leitlinien der Europäischen Versicherungsaufsichtsbehörde EIOPA zu Sicherheit und Governance von Informations- und Kommunikationstechnologien (IKT)** in die VAIT und verankert damit die europäischen Anforderungen in die deutsche Aufsichtspraxis.

Schwerpunkte der VAIT-Anpassung

Gesamtheitlicher Ansatz und Fokus auf Informationssicherheit

Insgesamt legt die Aufsicht künftig mehr Wert auf einen gesamtheitlichen Ansatz bei der IT-Sicherheit von Versicherungsunternehmen. So wird das neue Regelwerk an vielen Stellen dahingehend ergänzt, dass Unternehmen neben der Formulierung von Sicherheitsstrategien und -leitlinien sowie der Definition von Schutzmaßnahmen auch entsprechende Prozesse etablieren müssen, um sowohl Maßnahmen als auch deren Anpassung regelmäßig zu überprüfen.

Mit den beiden neuen Kapiteln zur „Operativen Informationssicherheit" und zum „IT-Notfallmanagement" werden zudem weitere Anforderungen formuliert. Hiermit soll gewährleistet werden, dass Informationssicherheitsmaßnahmen adäquat umgesetzt und die Betriebsstabilität aufrecht erhalten werden.

Die Bedeutung der Informationssicherheit wird auch dahingehend untermauert, dass der IT-Sicherheitsbeauftragte zukünftig durch ein Management-Team für die Informationssicherheit in seinen Tätigkeiten unterstützt werden kann.

Stärkere Einbindung von IT-Dienstleistern

Darüber hinaus werden IT-Dienstleister stärker in die Verantwortung genommen, wenn es um die Einhaltung der regulatorischen Anforderungen an die Versicherer geht. So müssen künftig bei der Festlegung der Bestandteile des Informationsverbundes auch deren Abhängigkeiten und Schnittstellen zu Dritten berücksichtigt werden. Das hat unmittelbare Auswirkungen auf andere Anwendungsbereiche der VAIT, beispielsweise bei der Schutzbedarfsfeststellung, bei der Erstellung von IT-Notfallplänen sowie im Zusammenhang mit der Vergabe von Benutzerberechtigungen.

Qualifikation der Mitarbeiter*innen

Die Qualifikation der Mitarbeiter*innen tritt ebenfalls stärker in den Vordergrund.

Ziel ist es, das Bewusstsein für den Schutzbedarf der Informationen und für die persönliche Verantwortung für das eigene Handeln zu schärfen. Um dies sicherzustellen, verlangt die BaFin zukünftig von Versicherungen, dass sie ein kontinuierliches und angemessenes Sensibilisierungs- und Schulungsprogramm für Informationssicherheit etablieren. Darüber hinaus wird für bestimmte Tätigkeiten (u.a. Tests, interne Revision) eine „angemessene" Personenqualifikation erwartet.

Wesentliche Neuerungen im Überblick

Anforderungen	Fokus der Neuerungen	Wesentliche Neuerungen/ Konkretisierungen im Detail
1. IT-Strategie 	Stärkere Berücksichtigung von IT-Dienstleistern und Informationssicherheit als Teil der IT-Strategie	» Etablierung eines Prozesses für die Überwachung und Messung der Umsetzung der Ziele der Strategie sowie zu ihrer Beurteilung und Anpassung durch die Geschäftsführung » Berücksichtigung möglicher sonstiger wichtiger Abhängigkeiten von Dritten (wie z.B. Informations-, Telekommunikations- und Versorgungsdienstleistungen) » Schulung und Sensibilisierung zur Informationssicherheit
2. IT-Governance 	Überprüfung der IT-Governance durch regelmäßige interne Audits	» Die Vorgaben zur IT-Governance sind Bestandteil regelmäßiger Überprüfungen durch bezüglich IT hinreichend qualifizierte interne Revisoren » Konkretisierung der Ressourcenausstattung auf personelle, finanzielle und sonstige Ressourcen (nicht nur personelle Ressourcen)
3. Informationsrisikomanagement 	Regelmäßige Überprüfung des Schutzbedarfs sowie Durchführung einer Bedrohungsanalyse des Informationsverbundes, inkl. der Vernetzung mit IT-Dienstleistern	» Konkretisierung der Risikokriterien hinsichtlich der Kritikalität der Geschäftsprozesse und -aktivitäten sowie bekannter Gefährdungen und Vorfälle » Ausweitung der Anforderungen an den Informationsverbund und Schutzbedarf: » Abhängigkeiten und Schnittstellen berücksichtigen auch die Vernetzung des Informationsverbundes mit Dritten » Regelmäßige Überprüfung des Schutzbedarfs » Klarstellung der Verantwortung auf Ebene der Geschäftsprozesse » Kontrolle durch Informationsrisikomanagement » Regelmäßige Bedrohungsanalyse des Informationsverbundes (intern/extern)
4. Informationssicherheitsmanagement 	Verantwortung der Informationssicherheit wird gestärkt	» Konkretisierung der Anforderungen an den Inhalt der Informationssicherheitsleitlinie sowie das Erstellen weiterer Informationssicherheitsrichtlinien (u.a. zu Identifikations- und Rechtemanagement) » Erstellung einer Richtlinie über das Testen und Überprüfen der Maßnahmen zum Schutz der Informationssicherheit » Zugeständnis, dass die Funktion des Informationssicherheitsbeauftragten durch ein Informationssicherheitsmanagement-Team unterstützt werden kann » Festlegung eines kontinuierlichen und angemessenen Sensibilisierungs- und Schulungsprogramm für Informationssicherheit und Überprüfung dessen Wirksamkeit/Erfolg

Anforderungen	Fokus der Neuerungen	Wesentliche Neuerungen/ Konkretisierungen im Detail
5. Operative Informationssicherheit 	Implementierung der Vorgaben des IS-Managements mit dem Ziel einer stärkeren Absicherung der IT-Systeme und Informationen	» Implementierung operativer Informationssicherheitsmaßnahmen und Prozesse » Anforderungen an die Identifizierung der Gefährdungslage des Informationsverbundes » Definition eines angemessenen Portfolios an Regeln zur Identifizierung sicherheitsrelevanter Ereignisse » Anforderungen an die zeitnahe Analyse sicherheitsrelevanter Ereignisse » Regelmäßige und anlassbezogene Überprüfungen der IT-Systeme (für kritische mind. 1x jährlich)
6. Identitäts- und Rechtemanagement (vorher Benutzerberechtigungsmanagement) 	Erweiterung der Anforderungen für Zugriffs-, Zugangs- und Zutrittsrechte sowie eine regelmäßige Überprüfung der Berechtigungskonzepte	» Etablierung von standardisierten Prozessen und Kontrollen für jegliche Zugriffs-, Zugangs- und Zutrittsrechte auf Bestandteile des Informationsverbundes, d.h. auch für physische Infrastrukturen wie Zutrittsregelungen zu Räumlichkeiten » Berücksichtigung des Sparsamkeitsgrundsatzes („Need to know“ und „Least Privilege“ Prinzipien) » Regelmäßige Kontrolle und Überprüfung der Berechtigungskonzepte
7. IT-Projekte, und Anwendungsentwicklung 	Konkretisierungen hinsichtlich der Vorgaben für IT-Projekte und Anwendungsentwicklung	» Konkretisierung organisatorischer Grundlagen für IT-Projekte » Berücksichtigung des Schutzbedarfs der zum Test verwendeten Daten, ggfls. anhand von Penetrationstests
8. IT-Betrieb 	Höherer Detaillierungsgrad hinsichtlich der Ausgestaltung von IT-Systemen und IT-Komponenten	» Konkretisierung der Bestandsangaben von IT-Systemen und IT-Komponenten (u.a. Schutzbedarf) » Definition von Standardvorgehensweisen beim Auftreten von Störungen z. B. für Maßnahmen und Kommunikation sowie Zuständigkeiten » Leistungs- und Kapazitätsbedarf der IT-Systeme muss fortlaufend analysiert und geplant werden
9. Ausgliederungen 	Keine wesentlichen Änderungen	» Konkretisierung, dass bei Auswahl der IT-Dienstleister auch eine Erhebung und Bewertung von funktionalen und nicht funktionalen Anforderungen erfolgen muss

Anforderungen	Fokus der Neuerungen	Wesentliche Neuerungen/ Konkretisierungen im Detail
10. IT-Notfallmanagement 	Etablierung eines unternehmensweiten IT-Notfallmanagements mit Notfallplänen und Testszenarien zu dessen Wirksamkeit (unter Berücksichtigung der Abhängigkeiten zu IT-Dienstleistern)	» Erstellung eines IT-Notfallkonzepts » Durchführung von Auswirkungsanalysen und entsprechender Risikoanalyse identifizierter IT-Prozesse, Systeme etc. » Erstellung von Notfallplänen für alle IT-Systeme (unter Berücksichtigung der IT-Dienstleister) » Überprüfung der Wirksamkeit der IT-Notfallpläne durch regelmäßige und anlassbezogene Notfalltests
Kritische Infrastrukturen	Keine inhaltlichen Neuerungen	

Wo besteht Handlungsbedarf?

Inwieweit die neuen Anforderungen konkreten Handlungsbedarf in Unternehmen hervorrufen werden, hängt maßgeblich vom Reifegrad ihrer implementierten IT-Risiko- und IT-Sicherheitsmaßnahmen ab. Die obligatorische Berücksichtigung von IT-Dienstleistern im Informationsverbund des Unternehmens in diesem Umfang dürfte für viele neu sein. Auch die regulatorischen Anforderungen an eine regelmäßige Überprüfung und Anpassung von Prozessen und Maßnahmen sowie regelmäßige Tests und entsprechende Berichterstattung wird aus unserer Sicht dazu führen, dass viele Unternehmen ihre derzeitigen Abläufe anpassen müssen. Versicherer sollten – falls nicht bereits in weiten Bereichen etabliert – auf eine toolbasierte Unterstützung beziehungsweise Automatisierung der geforderten Maßnahmen setzen. Andernfalls sind die Anforderungen an regelbasierte Auswertungen von großen Datenmengen oder die Frequenz und Detailtiefe von Kontrollmaßnahmen schwer umsetzbar.

Die zentrale Positionierung des Prozesses eines integrierten Informationsrisikomanagements (IS und IT) in der First Line of Defense ist eine konsequente Schlussfolgerung aus den geplanten Änderungen der BaFin. Denn Risiken in der Informationssicherheit getrennt von ihren IT-Aspekten zu betrachten, führt zu einer verzerrten Sicht auf die ganzheitliche IT-Risikolandschaft. Den Fokus sehen wir in diesem Zusammenhang in der Mitigation und der Nachverfolgung der gemanagten Risiken in der First Line of Defense mittels eines automatisierten Ansatzes.
Aktuell werden IS- und IT-Prozesse oft getrennt voneinander betrachtet. Zum Beispiel wird der ausgelaufene Support einer IT-Komponente im Rahmen des IS-Risikomanagements erkannt und parallel im Rahmen der IT-Prozesse „Application Life Cycle Management“ (präventive Kontrolle) und „Release Management“ (korrektive Kontrolle) behandelt. Für eine effiziente Mitigation des erkannten Risikos ist eine Verzahnung aller Prozesse vorteilhaft. Dies stellt unter anderem eine zeitnahe Integration der beteiligten Funktionen und damit schnellere Risikominimierung sicher.

Zusätzliche Synergien aus dem integrierten Management von IS- und IT-Risiken ergeben sich ferner durch die Konzentration des Expertenwissens im Unternehmen und das Erlangen einer konsistenten Beurteilung der Risikolage. Dies muss natürlich erfolgen, ohne die organisatorische Trennung der IS- und IT-Funktionen, wie sie von der BaFin gefordert wird, aufzuweichen.

Wenn Sie Fragen zum Thema VAIT haben, freue ich mich über Ihre Kontaktaufnahme. Unser Team für IT Governance & Regulation wird die Auswirkungen der Novelle auf Versicherungen gerne in einem Gespräch mit Ihnen erörtern.

Dr. Anja Zimmer

+49 89 360531-5492
anja.zimmer@metafinanz.de

metafinanz Informationssysteme Gmbh
Leopoldstraße 146
80804 München
www.metafinanz.de

metafinanz
Business & IT Consulting
We. Ensure. Success.