IT-Sicherheitsmanagement: gesetzliche Vorgaben und digitale Bedrohun-gen fordern Versicherer

Nach Inkrafttreten des IT-Sicherheitsgesetzes (ITSiG) und der EU-Datenschutz-Grundverordnung (EU-DSGVO) folgen nun die Versicherungsaufsichtlichen Anforderungen an die IT (VAIT). Der Bereich IT-Sicherheit bleibt daher ein bedeutender Punkt auf den Agenden der IT-Abteilungen deutscher Versi-cherer. Bei der dritten Fachkonferenz „IT-Sicherheitsmanagement in Versicherungen“ der Versicherungsforen Leipzig am 14. und 15. Mai 2019 wurden aktuelle Entwicklungen diskutiert und Erfahrungen ausgetauscht.

Neue Gesetzgebungen bedeuten meistens Arbeit. Das gilt nicht nur für die Rechtsabteilungen, im Falle der jüngsten Gesetznovellierungen und regulatorischen Anforderungen im Bereich IT-Sicherheit und Datenschutz natürlich auch für die IT-Abteilungen. Vor dem Hintergrund vermehrter Cybervorfälle gewinnt IT-Sicherheit zudem für viele Unternehmen immer mehr an Bedeutung. Rund 60 Teilnehmer kamen auf der Fachkonferenz in Leipzig zusammen, um die aktuellen Anforderungen zu diskutieren. Fachbeiträge gab es dabei nicht nur aus Versicherungshäusern, sondern auch von Vertretern des Bundesamts für Sicherheit in der Informationstechnik (BSI), der BaFin und des Landeskriminalamtes Nordrhein-Westfalen.

Dass die Bekämpfung von Cyber-Kriminalität eine gesamtgesellschaftliche Aufgabe sei, betonte Peter Vahrenhorst, Kriminalkommissar beim Landeskriminalamt Nordrhein-Westfalen. Er zeigte auf, dass Cyber-Kriminelle heute nicht mehr im stillen Kämmerlein hacken, sondern zum Bereich organisierte Kriminalität gehören. Für Unternehmen bedeutet dies, dass sie ihre IT-Systeme dafür fit machen müssen, es vor allem aber auch gilt, die Mitarbeiter zu sensibilisieren. Nutzer hinterfragen IT heute oftmals nicht mehr, Risikobewusstsein fehle. Dr. Jens Gampe (BaFin) unterstrich, dass Mitarbeiter nur beachten könnten, was sie auch kennen. Umfangreiche Informationen über IT-Sicherheitsmaßnahmen seien daher unerlässlich. Dass sich hieraus ein großer Nutzen ergibt, zeigen Statistiken. Palo Stacho (Lucy Security) stellte vor, dass nur drei Prozent der Cyber-Angriffe heute auf technische Schwachstellen zurückzuführen sind. 97 Prozent nutzen hingegen menschliche Unkenntnis und Nachlässigkeiten aus. Dr. Hans-Joachim Popp, Präsident des Bundesverbands der IT-Anwender VOICE, betonte allerdings, dass unter den Mitarbeitern ein positives Image für Sicherheitsthemen geschaffen werden müsse. Mitarbeiter dürften bei Fehlern keine Angst vor Schuldzuweisungen haben und geschult werden, Vorfälle möglichst schnell zu melden.

Vor dem Hintergrund von DSGVO und ITSiG gab es auf der zweitägigen Konferenz natürlich auch Vorträge zur aktuellen Herausforderungen der Gesetzeslage. Karsten Bartels (HK2 Rechtsanwälte) gab ein Update über den aktuellen Stand der Gesetzgebung in den Bereichen IT-Sicherheit und Datenschutz und wies auf Stolpersteine hin, auf die Unternehmen ein genaues Augenmerk legen sollten. Im Detail stellte er auch das neue Geschäftsgeheimnisschutzgesetz (GeschGehG) und die daraus resultierenden To Dos vor.

Von Erfahrungen mit der Umsetzung der DSGVO berichtete Jens-Jürgen Vogel (Münchener Rück). - Der Rückversicherer hat ein umfassendes Projekt für die IT-Systeme umgesetzt, um in den Prozessen und Systemen DSGVO-konform zu sein. Als Ergebnis steht beispielsweise ein einheitliches Verfahren, das alle neuen IT-gestützten Geschäftsprozesse prüft, freigibt und dokumentiert. Vogel sieht die Zusammenarbeit zahlreicher Abteilungen, wie bspw. Recht, IT-Security, Datenschutz und IT-Compliance, als zentralen Erfolgsfaktor. Vogel ist zudem der Meinung, dass Datenschutz heute nicht mehr nur Pflichtfach ist, sondern auch zum Marketinginstrument geworden sei.

Einen weiteren Erfahrungsbericht lieferte Dr. Frank Simon (Zurich Deutschland). In der IT-Entwicklung war die IT-Sicherheit bei der Zurich bisher als separater Prüfschritt relativ am Ende der Entwicklung angesiedelt. Sicherheitsprobleme zu beheben war daher meist mit sehr hohem Aufwand und Kosten verbunden. Durch agilere Formen der Zusammenarbeit werden nun die Security Engineers viel früher in die Entwicklung einbezogen. In einem kollaborativen Ansatz ist ein einzelner Mitarbeiter dabei in alle Schritte eines Projekts involviert und kann kontinuierlich die IT-Sicherheit überprüfen. Auch wenn diese Änderungen organisatorisch noch nicht nominell umgesetzt sind, werden sie operativ gelebt und zeigen gute Erfolge. Simon ist sich sicher, dass es heute „kein IT-Projekt mehr ohne Security-Beteiligung“ geben darf.

Die regen Diskussionen auf der Konferenz zeigten, dass der Bereich IT-Sicherheit mehr Aufmerksamkeit bedarf als je zuvor. Vor dem Hintergrund weiterer gesetzlicher Vorgaben (Stichwort ITSiG 2.0) wird es auch zukünftig weiteren Handlungsbedarf in den Unternehmen geben.

Weitere Informationen erhalten Sie unter www.versicherungsforen.net/it-sicherheit

Pressekontakt:

Katharina Thiemann
Telefon: +49 341 98988-224
E-Mail: katharina.thiemann@versicherungsforen.net

Unternehmen

Versicherungsforen Leipzig GmbH
Hainstraße 16
04109 Leipzig

Internet: www.versicherungsforen.net

Über Versicherungsforen Leipzig GmbH

Die Versicherungsforen Leipzig verstehen sich als Dienstleister für Forschung und Entwicklung (F&E) in der Assekuranz. Als Impulsgeber für die Versicherungswirtschaft liegt ihre Kernkompetenz im Erkennen, Aufgreifen und Erforschen neuer Trends und Themen, zum Beispiel im Rahmen von Studien und Forschungsprojekten unter unmittelbarer Beteiligung von Versicherern. Basierend auf aktuellen wissenschaftlichen und fachlichen Erkenntnissen entwickeln und implementieren sie zukunftsweisende Lösungen für die Branche.
Mit dem speziellen Wissen der Versicherungsbetriebslehre, der Versicherungsinformatik, der Versicherungsmathematik und des Versicherungsrechts schaffen die Versicherungsforen Leipzig die Basis für die Lösung anspruchsvoller neuer Fragestellungen innerhalb der Assekuranz. Zudem ermöglicht die wissenschaftliche Interdisziplinarität und der hohe Praxisbezug einen aufschlussreichen »Blick über den Tellerrand«.