Code of Conduct Datenschutz: Versicherer bei der Umsetzung im Verzug

Schaffen die deutschen Versicherer die Umsetzung der freiwilligen Selbstverpflichtung zum Datenschutz (Code of Conduct CoC) nicht rechtzeitig? Für 122 Versicherer wird es eng, so dass Ergebnis einer Marktbeobachtung des Software- und Beratungshauses PPI AG. Die Frist von drei Kalenderjahren läuft für sie Ende dieses Jahres aus. Bei einigen sei schon jetzt klar, dass sie die organisatorischen und IT-technischen Maßnahmen nicht rechtzeitig vollständig umsetzen können. Die Gesellschaften müssten vorrangig nach schnellen Lösungen suchen.

"Der Umfang wurde von vielen Versicherern unterschätzt. Besonders die Regelungen zum Sperren und Löschen der Kundendaten verursachen große Aufwände und beanspruchen fast drei Viertel des Zeitbudgets", sagt Ulrich Kusch, Managing Consultant und Versicherungsexperte bei PPI.

Personenbezogene Daten liegen inzwischen an vielen Orten vor. Gerade in jüngster Zeit werden für den erfolgreichen Einsatz eines Data Warehouse viele Daten über die Kunden gesammelt. Angereichert mit Informationen aus den sozialen Medien, Kundenkarteien, Internetforen und Befragungen werden diese vielfach als eine große Big-Data-Masse gespeichert. Doch dieses Datensammeln widerspricht dem CoC. Der Kodex beinhaltet den Gedanken der Datensparsamkeit im Umgang mit Kundendaten. Wenn eine Löschung nach Vertragsende aus gesetzlicher, vertraglicher oder fachlicher Pflicht nicht möglich ist, müssen die Daten zumindest gesperrt werden.

Doch es gibt keine einheitlichen Regeln über die verschiedenen Sparten und Fälle hinweg, was die Umsetzung umso schwieriger macht. Bestimmte Informationen müssen oder dürfen länger gespeichert werden als andere. Teilweise widerspricht der CoC auch gesetzlichen Aufbewahrungspflichten.

Viele Versicherer haben den Aufwand unterschätzt. Zudem gibt es kaum Konzepte, die unterschiedlichen gesetzlichen und geschäftsbedingten Aufbewahrungsfristen zu erfüllen und gleichzeitig die Arbeitsfähigkeit der Fachbereiche sicherzustellen. "Die in Zeitnot geratenen Versicherer sollten ein Zwischenfazit ziehen und nach Einsparpotenzialen suchen. Dass einige Artikel des CoC unterschiedlich ausgelegt werden können, erhöht das Risiko einer Fehlinterpretation", sagt Kusch. Eine vollständige Umsetzung in der IT ist nicht immer nötig, einzelne Anforderungen können auch organisatorisch erfüllt oder im Rahmen der Regeln weniger stringent ausgelegt werden.

Kusch empfiehlt, ein Regelwerk mit Sperr- und Löschkonzept zu erstellen, in dem die wichtigsten Grundlagen und Fristen zusammengefasst werden. Viele der nötigen Schritte lassen sich dann durch Automation beschleunigen. "Es bietet sich auch an, endlich für Ordnung in bestehenden Data Warehouses und BI-Systemen zu sorgen. Durchdachte systematisierte Löschprozesse sparen auf Dauer Zeit und Geld. Ressourcen für das Kerngeschäft werden frei."

Cyber-Crime: Nachholdbedarf beim Risk-Management

Security-Manager in deutschen Unternehmen messen Cyber-Angriffen auf IT- und Telekommunikationssysteme höchste Risikopotenziale bei. Neben der Arbeitssicherheit sind die IT-Sicherheit und der Brandschutz die wichtigsten Handlungsfelder in der Unternehmenssicherheit. So lautet ein Ergebnis der aktuellen Expertenbefragung 2014/2015, die von Sicherheitsfachzeitschrift WIK zusammen mit dem ASW Bundesverband - Allianz für Sicherheit in der Wirtschaft e.V. alle zwei Jahre durchgeführt wird.

Obwohl die Gefährdung von Unternehmensdaten durch Cyber-Kriminalität seit 2008 als drängendstes Problem von den Verantwortlichen in den Unternehmen angesehen wird, gaben mehr als 60% der Befragten an, in den letzten beiden Jahren von Cyber-Attacken betroffen gewesen zu sein, 22% sogar mehr als fünf Mal. Dies zeigt, dass die wahrgenommene Bedeutung der IT-Sicherheit und die Schadenfälle immer noch nicht zwangsläufig zur Umsetzung konkreter Maßnahmen führen.

Besonders in kleinen und mittleren Unternehmen (KMU), zu denen in Deutschland mehr als 99% der Unternehmen zählen, mangelt es an wirksamen Gesamtkonzepten für die Informationssicherheit, wie aus einer BMWi-Studie zum IT-Sicherheitsniveau in KMU aus 2012 hervorgeht. Die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) seit Jahren zur Verfügung gestellten IT-Grundschutzkataloge scheinen besonders in KMU nicht die erhoffte Wirkung zu entfalten.

Mit den neuen VdS-Richtlinien VdS 3473 steht dem Mittelstand nun ab 1. Juli eine Leitlinie zur Verfügung, um seine Informationssicherheit auf ein der Bedrohungslage angemessenes Schutzniveau zu heben, und zwar ohne die Unternehmen organisatorisch oder finanziell zu überfordern, so der VdS. Werden alle vorgeschlagenen Schutzmaßnahmen nachprüfbar umgesetzt, kann ein VdS-Zertifikat ausgestellt werden.

Dr. Rolf Meyer, Leiter Versicherungen bei BearingPoint

Wappnen gegen digitale Newcomer

„Die Chancen der Digitalisierung für die Versicherungswirtschaft sind immens – und zwar so immens, dass sie damit wieder zur größten Herausforderung werden. Wem es am besten gelingt, aus den vorhandenen Daten die geschäftsrelevanten herauszufiltern, zu verknüpfen und strukturiert nutzbar zu machen, der bereitet den Boden zur Stärkung der eigenen Positionierung im Markt. Das wird immer wichtiger, denn Newcomer aus dem IT-Bereich drängen aktuell auf den Versicherungsmarkt, die auf Schnelligkeit setzen, auch ohne auf den sicheren Business Case zu warten."