

28.11.2019 Qualitätssicherung

IT-Sicherheit ist Chefsache!

Ecclesia med GmbH



Erpressersoftware, Hackerattacken oder Doxing, das „Absaugen“ von sensiblen Daten wie vor einiger Zeit von privaten Politiker-Telefonnummern, lösen viele sorgenvolle Diskussionen aus. Aber gegen solche und ähnliche Machenschaften kann man sich schützen. In Passion Chirurgie wollen wir uns in den nächsten Ausgaben mit unterschiedlichen Themenaspekten der Sicherheit elektronischer Daten beschäftigen. Am Anfang steht ein Interview mit Detlev Hrycej, Experte für Cyberversicherungen. Er weist unter anderem darauf hin, dass Hacker nicht die einzige Gefahr für Datenbestände sind.

Ecclesia med GmbH: Herr Hrycej, Anfang der 2000er-Jahre hat die Ecclesia Gruppe das Thema Cyberversicherungen in ihr Portfolio aufgenommen. Was gab damals den Ausschlag dafür?

Detlev Hrycej: Das Thema „Cyberversicherungen“ ist hierbei zu kurz gegriffen. Es geht letztlich darum, mit welchen Risiken unsere Mandanten im Zuge der fortschreitenden Digitalisierung konfrontiert werden. Deshalb haben wir früh ein Projekt aufgelegt, um zunächst zu identifizieren, in welchen Versicherungssparten Datenrisiken überhaupt abgedeckt sind und wie diese Abdeckungen aussehen. In einem zweiten Schritt haben wir daraus Rückschlüsse für die notwendige Produktentwicklung gezogen.²⁸

In den vergangenen Jahren sind sukzessive immer mehr Anbieter von Cyberpolicen auf den Markt gekommen. Die Produkte sind aber nicht oder nur schwer vergleichbar. Je nachdem aus welcher Sparte heraus die Produktentwicklung erfolgt, gibt es unterschiedliche Schwerpunkte und Definitionen des Versicherungsschutzes. Dies führt zu absoluter Intransparenz. Deshalb haben wir, auch unter dem Blickwinkel unserer umfangreichen Schadenerfahrung, nach sorgfältiger Analyse auf die Einrichtungen der Gesundheitswirtschaft und der Sozialwirtschaft zugeschnittene und sehr weitgehende, exklusive Versicherungskonzepte entwickelt, um die IT- und Cybergefahren absichern zu können.

Ecclesia med GmbH: Erst war die Datenschutz-Grundverordnung das große Thema, vor Kurzem dann gingen Hackerangriffe durch die Presse. Das Kreisklinikum Fürstenfeldbruck wurde durch eine Schadsoftware lahmgelegt und auch der Maschinenbaukonzern Krauss Maffei wurde schwer getroffen. Wie wirken diese Ereignisse bei den Kunden nach?

Detlev Hrycej: Das Thema der Ransomware-Attacken (IT-System wird gesperrt, um Lösegeld zu erpressen, d. Red.) begleitet uns schon länger. Vor Fürstentfeldbruck war 2016 das Lukaskrankenhaus Neuss in den Medien präsent. Insgesamt handelt es sich hier nach unserer Erkenntnis allerdings um ungerichtete Hackerattacken, die auch viele Unternehmen außerhalb der Gesundheitswirtschaft getroffen haben und deren Schaden wir begleitet haben.

Zwischenzeitlich hat es einen rapiden Bewusstseinswandel im Management der von uns betreuten Einrichtungen gegeben. Wurde früher das Thema IT-Sicherheit an die IT-Leitung delegiert, ist es jetzt ganz klar Chefsache! Zu diesem Bewusstseinswandel haben allerdings nicht nur die zunehmenden Attacken oder Erpressersoftwares beigetragen, sondern auch die geänderte Rechtslage. Sowohl das IT-Sicherheitsgesetz als auch die EU-Datenschutz-Grundverordnung haben die Anforderungen an das Management erhöht, einhergehend mit teils drastischen Strafen bei Nicht-Beachtung.

Ecclesia med GmbH: Welche Entwicklung lässt sich beim Thema Cyberschäden feststellen?

Detlev Hrycej: Die Nachfrage zu umfassendem Cyberversicherungsschutz hat sich deutlich erhöht. Allein in den vergangenen 13 Monaten haben wir eine Verdoppelung der Vertragsanzahl verzeichnet. Insgesamt haben wir mehr als 400 dieser Schadenfälle mit einem Gesamtaufwand von gut 4,5 Millionen Euro in Abwicklung. Schäden dieser Art nehmen zu. Der Aufwand, bezogen auf das Jahr 2018, liegt bei rund 1,35 Millionen Euro, dies entspricht rund 30 Prozent des Gesamtaufwands.

Wir sind schnell versucht, mit dem Thema Cyberrisiken Computerkriminalität, Viren, Würmer und Trojaner zu verbinden. Es gibt aber viele weitere und bekannte Gefahren durch Feuer, Wasser, Elementarschäden, Unachtsamkeiten und Bedienungsfehler etc. Diese Risiken führen täglich zu Schäden, die auch die IT-Infrastruktur unserer Mandanten betreffen. 58 Prozent der IT- und Cyberschäden in unserer Begleitung gehen auf diese Ursachen zurück; 42 Prozent beziehen sich auf Schadsoftware und Co.

Allein daraus ist abzuleiten, wie wichtig die richtige und dem Kunden nutzenbringende Versicherungstechnik ist. Die Konzepte der Ecclesia Gruppe sind modular aufgebaut, sie liefern dem Kunden Transparenz und insbesondere Wahlmöglichkeiten, damit der Versicherungsschutz individuell anhand der Gegebenheiten und des bestehenden Versicherungsschutzes des Unternehmens fachgerecht abgebildet werden kann, ohne Doppelversicherungen einzugehen.

Zur Person

Detlev Hrycej, Leiter der Arbeitsgruppe „Cyber“ in der Ecclesia Gruppe, zeigt im Interview Risiken für Manager und Unternehmen in der Gesundheits- und der Sozialwirtschaft auf. Hacker sind dabei nicht die einzige Gefahr für Datenbestände.

Die Fragen stellte:

Thorsten Engelhardt

Ecclesia med GmbH

BDC-Versicherungsservice

Ecclesiastraße 1-4



Ecclesia med GmbH: Wie ist es um die Risikoprävention bei den Kunden bestellt?

Detlev Hrycej: Prävention steht vor Risikotransfer! Denn was nützt eine Einbruchdiebstahlversicherung, wenn Tür und Tor offenstehen? Hier muss eine Standortbestimmung her. Nur durch ein systematisches Management der Cyberrisiken können die zentralen IT-Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität realisiert werden. Die gesetzlichen Anforderungen müssen ebenfalls berücksichtigt werden.

Ecclesia med GmbH: Was lässt sich in punkto Schutz überhaupt tun, die Angriffe werden ja offenbar immer perfider?

Detlev Hrycej: Den Kunden aus der Gesundheitswirtschaft bietet die Ecclesia Gruppe in Kooperation mit renommierten Beratungsunternehmen für IT-Sicherheit ein systematisches Cyber-Risk-Management an. Der Aufbau, auch dieser Exklusivkonzepte, ist modular. Basis ist immer ein Sicherheitscheck.

Um die Verwundbarkeit der IT-Infrastruktur einzugrenzen, muss das Management aber auch genau diese Prozesse und Strukturen in den Blick nehmen und überprüfen. Dafür gibt es sehr viele Möglichkeiten: von der Einführung eines Managementsystems für Informationssicherheit (ISMS) bis hin zur Zertifizierung beispielsweise von kritischen Infrastrukturen. All diese Möglichkeiten bieten wir unseren Mandanten. IT- und Datensicherheit sind Chefsache und nicht delegierbar!

Ecclesia med GmbH: Heißt das auch, dass Chefs unter Umständen selbst haften, wenn es zu Schäden kommt?

Detlev Hrycej: Datenrisiken sind erst in den vergangenen Jahren stärker zu einem haftungsrechtlichen Thema und somit auch zum neuen Haftungspotenzial für Manager geworden. Bisher ist dieses Risiko in keiner Vermögensschaden-Haftpflicht- oder D&O-Versicherung (Directors-and-Officers-Versicherung, d. Red.) umfassend abgesichert. Deshalb ist es – bei aller Komplexität – entscheidend, den Kunden so zu beraten, dass nicht nur das Cyberrisiko für das Unternehmen deutlich wird, sondern auch das zivil- und strafrechtliche Risiko der Geschäftsleitung, wenn sie ihrer Verantwortung für die Datensicherheit nicht gerecht wird.

Zur Absicherung der Unternehmen und der persönlichen Gefahren des Managements aus Datenrisiken müssen individuell zugeschnittene Versicherungskonzepte her, um umfassenden Schutz zu gewährleisten. Deshalb hat die Ecclesia Gruppe eigene und exklusive Produkte für die Gesundheits- und die Sozialwirtschaft entwickelt.

Hrycej D: IT-Sicherheit ist Chefsache! Passion Chirurgie. 2019 November, 9(11): Artikel 04_05.