Cyberversicherungen: Analyse und Marktentwicklungen

Masterarbeit

zur Erlangung des akademischen Grades „Master of Science (M. Sc.)“ im Studiengang Wirtschaftswissenschaft der Wirtschaftswissenschaftlichen Fakultät der Leibniz Universität

vorgelegt von

Name: Porsch Vorname: Kristina

[redacted]

Prüfer: Prof. Dr. Michael H. Breitner

Hannover, den 30.09.2019

Inhaltsverzeichnis

Seite

1 Einleitung

„Es gibt zwei Arten von Unternehmen: Diejenigen die gehackt wurden und solche, die nicht wissen, dass sie gehackt worden sind."
- John Chambers, CEO von Cisco (2015) -

In heutiger Zeit ist es ersichtlich, dass IT-Sicherheit zur größten Sorge eines Unternehmens wird (Münch, 2015). Dies hat zur Folge, dass Cyberversicherungen auch in Deutschland zunehmend an Bedeutung gewinnen. Diesbezüglich wird in diesem Kapitel die Motivation und Relevanz des Themas dargelegt. Dabei wird eine Zielsetzung für die Arbeit erarbeitet, sowie eine Abgrenzung getroffen. Daraus werden Forschungsfragen abgeleitet, welche im Verlauf der Arbeit beantwortet werden. Der Aufbau der Arbeit beschließt das Kapitel.

1.1 Motivation und Relevanz der Thematik

Aufgrund der zunehmenden Komplexität der Systeme und der zunehmenden Vernetzung, steigt auch die Gefahr von Cyberangriffen. Dabei sind lange nicht mehr nur große Unternehmen betroffen. Infolge dessen, dass die Hacker in vielen Fällen kein konkretes Angriffsziel haben, sondern vielmehr zufällige Opfer, aufgrund von IT-Schwachstellen angreifen, geraten auch niedergelassene Ärzte[1] in das Visier von Hackern. Die Digitalisierung im Gesundheitswesen ist bereits fortgeschritten, sodass nur noch wenige bis keine Ärzte mit Papierakten arbeiten. Doch diese Zielgruppe arbeitet mit besonders sensiblen Daten: Gesundheitsdaten der Patienten. Nach § 3 Abs. 9 Bundesdatenschutzgesetz (BDSG) handelt es sich dabei um besondere personenbezogene Daten (dejure.org (Hrsg.), 2019). Im Gegensatz zu anderen Branchen steigt in Arztpraxen die Gefahr von lebensbedrohlichen Cyberangriffen, aufgrund von zunehmender Vernetzung und mangelnder Sicherheit. In Israel haben IT-Experten bereits eine Methode entwickelt, mit der Computertomografie (CT) Scans verfälscht werden können. Dies hat zur Folge, dass mit Hilfe einer Schadsoftware Krebsdiagnosen manipuliert werden können. Ärzte nutzen diese Bilder als Basis für die Feststellung der Diagnose. Hacker können aber mit einer Schadsoftware diese Bilder manipulieren, dies würde zu Fehldiagnosen führen. Entweder wird ein gesunder Patient dadurch Therapien durchlaufen, die für ihn nicht notwendig sind oder ein Patient mit Krebs wird nicht behandelt, weil er als gesund eingestuft wird. Solche Cyberangriffe

[1] Aus Gründen der einfacheren und besseren Lesbarkeit fallen im Rahmen der vorliegenden Arbeit die Psychotherapeuten und Zahnärzte auch unter den Begriff niedergelassener Ärzte. Zusätzlich wird nur die männliche Form verwendet, trotzdem beziehen sich die Angaben im Text auf beide Geschlechter.

sind lebensbedrohlich, denn sogar Fachärzte können in nahezu 100 Prozent nicht erkennen, dass die Bilder manipuliert wurden (spiegel.de (Hrsg.), 2019), (focus.de (Hrsg.), 2015).

Darüber hinaus kann es bei der Arztpraxis[2] auch zu Reputationsschäden kommen, wenn die Gesundheitsdaten der Patienten geklaut werden. Bei einem Cyberangriff entstehen grds. für die Arztpraxis hohe Kosten, die sich sogar als existenzbedrohend auswirken können.
Um sich gegen die Folgen von Cyberangriffen abzusichern, besteht die Möglichkeit eine Cyberversicherung abzuschließen. Die Nachfrage nach speziellem Versicherungsschutz steigt langsam bei niedergelassenen Ärzten. Allerdings handelt es sich dabei um einen sehr jungen Markt, bei welchem das Prämienvolumen im Jahr 2016 bei 80 Mio. Euro in Deutschland lag.
Erst 2011 kam der erste Anbieter auf den deutschen Versicherungsmarkt. Da es sich im Vergleich zu anderen Sparten um eine junge Sparte handelt, besteht das Hauptproblem der Versicherer bei der Festlegung von angemessenen Preisen. Im Vergleich bspw. zu der Haftpflichtversicherung in der viele Daten vorhanden sind, fehlt es hier den Versicherern an Daten zur Schadenerfahrung. Zusätzlich sind die Risiken schwer abschätzbar (Frommes & Hagen, 2017, S. 6-8), (Gesamtverband der Deutschen Versicherungswirtschaft (Hrsg.), 2015).
Auf dem deutschen Markt sind laut dem Gesamtverband der Deutschen Versicherungswirtschaft (GDV) aktuell 38 Versicherer vorhanden, die eine Cyberversicherung anbieten. Dabei ist dieser Markt noch sehr heterogen. Einige Policen unterscheiden sich sehr stark voneinander und auch der Aufbau der Bedingungen und die Ausschlüsse sind unterschiedlich (Krieger, 2017, S. 10-11), (Gesamtverband der Deutschen Versicherungswirtschaft (Hrsg.), o. J).
Die Meinungen von Experten zu dieser Sparte teilen sich. Einigen bereitet die Gefahr vor einem Mega-Kumul Sorgen, so sagte Ulrich-Bernd Wolff (ehemaliger Präsident des Verbands öffentlicher Versicherer): „Cyberversicherung ist wie Dynamithandel.“ (Gentrup & Hagen, 2017, S. 15). Andere Experten sind wiederum der Meinung, dass es sich dabei um einen Boommarkt handelt und die Cyberversicherung prämienmäßig mittelfristig die Kraftfahrtzeug (Kfz)-Versicherung überholen wird (Wichert, 2018).

[2] Im weiteren Verlauf der Arbeit werden Arztpraxis und Praxis synonym verwendet.

1.2 Zielsetzung und Abgrenzung der Arbeit

Der Fokus dieser Arbeit liegt nur auf der Zielgruppe der niedergelassenen Ärzte. Weitere Zielgruppen können nicht untersucht werden, dies würde den Rahmen der vorliegenden Arbeit überschreiten, weil der Aufbau der IT und die Daten sich je nach Zielgruppe unterscheiden. Des Weiteren liegt eine geografische Eingrenzung vor, es werden lediglich Arztpraxen in Deutschland betrachtet. Bei Betrachtung weiterer Länder oder Zielgruppen besteht die Gefahr, dass der Rahmen der Arbeit zu weit gefasst sein könnte.

Basierend auf der Motivation und Relevanz dieser Thematik, ist das Ziel zunächst den deutschen Cyberversicherungsmarkt zu untersuchen. In Anknüpfung daran sollen folgende Forschungsfragen geklärt werden:

1. Wie ist der aktuelle Stand der IT-Sicherheit in Arztpraxen? Treffen diese bereits ausreichend Schutzmaßnahmen im Hinblick auf die IT-Sicherheit?

2. Wie sollte eine branchenspezifische Cyberversicherung für Ärzte gestaltet werden, damit im Falle eines Cyberangriffes eine notwendige Absicherung gewährleistet werden kann? Und handelt es sich dabei um eine besondere Risikoklasse für die Versicherer?

Dazu soll zunächst der Aufbau und die Ausstattung der IT untersucht werden, um daraus Rückschlüsse ziehen zu können. Durch die empirische Studie soll der aktuelle Umsetzungsstand der IT-Sicherheit in Arztpraxen in Deutschland ermittelt werden und ein Bild zur Schadenerfahrung geschaffen werden. Schließlich ist es aus Sicht der Versicherer wichtig, gleich bei Abschluss des Versicherungsvertrages die Risiken des Versicherungsnehmers richtig einzuschätzen, um so auch einen angepassten Versicherungsschutz zu gewährleisten. Zusätzlich werden Hypothesen im Rahmen der empirischen Studie aufgestellt, die im
Anschluss geprüft werden.

1.3 Aufbau der Arbeit

Die vorliegende Arbeit ist in neun Kapitel gegliedert. Nachdem das erste Kapitel zunächst eine Einleitung in die Thematik liefert, wird in Kapitel 2 der theoretische Rahmen der Arbeit dargelegt und betrachtet. Dazu gehören zwei große Themenkomplexe: IT-Sicherheit und Cyberrisiken. Dieses Kapitel widmet sich vielmehr der terminologischen Klärung.

Die Überführung zum Hauptteil findet durch die Literaturanalyse nach Webster und Watson statt. Wobei im ersten Abschnitt das methodische Vorgehen der Untersuchung zunächst geschildert wird und im Anschluss die relevante Literatur vorgestellt wird.

Im Fokus des vierten Kapitels steht der deutsche Cyberversicherungsmarkt, dazu werden zunächst einige seiner Facetten präsentiert. Danach wird ein Marktüberblick über die derzeit bestehenden Cyberversicherungen in Deutschland gegeben.
Aufbauend auf den vorangegangenen Kapiteln, wird zunächst im Hauptteil der Arbeit die ITSicherheit in Arztpraxen betrachtet (Kapitel 5). Zudem werden neben der IT-Ausstattung von Arztpraxen, die Maßnahmen vorgestellt, die die IT-Sicherheit in einer Arztpraxis gewähren sollen. Darüber hinaus sollen unter anderem die IT-Branchenlösungen für Arztpraxen sowie ausgewählte Cyberangriffe auf Arztpraxen vorgestellt werden.

Im Mittelpunkt des sechsten Kapitels steht die empirische Studie. Dabei wird im ersten Abschnitt das methodische Vorgehen geschildert und im Anschluss die Forschungsergebnisse präsentiert, sowie dort definierte Hypothesen überprüft.

Im siebten Kapitel werden Handlungsempfehlungen gegeben, wie eine mögliche Cyberversicherung für Ärzte aufgebaut werden sollte bzw. gestaltet sein könnte.
In Bezug darauf werden im achten Kapitel die bereits zuvor ausgearbeiteten Ergebnisse nochmals detailliert erörtert und kritisch hinterfragt. Dabei werden unter anderem auch Empfehlungen für weitere Forschungen gegeben. Zusätzlich werden die Limitationen der Arbeit aufgezeigt.
Im letzten Kapitel (Kapitel 9) werden alle wesentlichen Erkenntnisse dieser Arbeit zusammengefasst. Und im Anschluss daran gibt ein Ausblick, Informationen über die vermutlich weitere Entwicklung des Cyberversicherungsmarktes in Deutschland.

2 Zusammenfassung und Ausblick

Ziel dieser Arbeit war es einerseits den Aufbau und die Sicherheit der IT in Arztpraxen zu untersuchen, um Erkenntnisse zu gewinnen, inwiefern die vorhandenen sensiblen Daten ausreichend geschützt werden und andererseits daraus Rückschlüsse zu ziehen, wie eine Cyberversicherung für Arztpraxen gestaltet werden sollte.

Dazu wurde zunächst ein fundamentales Verständnis für das Thema geschaffen, indem zum einen die IT-Sicherheit beleuchtet wurde und zum anderen die Cyberrisiken aufgezeigt wurden. Hierbei wurde festgestellt, dass zahlreiche rechtliche Regelungen vorliegen, die die ITSicherheit beeinflussen bzw. regeln. Darüber hinaus unterlag die Definition von Cyberrisiken im Zeitverlauf einem Verständniswandel. Die wesentlichen Aspekte von Cyberrisiken sind, dass diese heterogen sind und das Umfeld der Cyberrisiken sich in einer ständigen Veränderung befindet. Dies hat zur Folge, dass Cyberrisiken wenig erforscht sind und deshalb nur ein geringer Bestand an historischen Daten zur Schadenerfahrung vorliegt. Aufgrund dessen ist das Schadenpotential schlecht bzw. kaum quantifizierbar.
Cyberangriffe nehmen von Jahr zu Jahr zu und die Schadprogramme entwickeln sich immer weiter, sodass im Jahr 2015 59,1 Mio. Cyberangriffe weltweit stattgefunden haben. Aufgrund von Sorgen um die Reputation, werden viele Cyberangriffe nicht gemeldet bzw. öffentlich gemacht, sodass die Dunkelziffer dennoch höher liegt.

Anhand der Literaturanalyse nach Webster und Watson konnte bestätigt werden, dass es sich hierbei um ein sehr junges Forschungsfeld handelt. Schließlich wurden die meisten Artikel in den letzten drei Jahren veröffentlicht.

Im Fokus der Arbeit stand neben der IT-Sicherheit in Arztpraxen, die Cyberversicherung für niedergelassene Ärzte. Aus diesem Grund wurde dafür der Cyberversicherungsmarkt in Deutschland untersucht. Genau wie die Cyberrisiken selbst, ist auch der Versicherungsmarkt für Cyberrisiken recht heterogen. Während einige Versicherer lediglich unterschiedliche Pakete mit unterschiedlichem Versicherungsumfang anbieten, bieten andere Versicherer eine individuelle Zusammenstellung des Versicherungsumfangs, indem aus vielen optionalen Bausteinen eine individuelle Cyber-Police erstellt werden kann. Hingegen bieten andere Versicherer auch einen Grundbaustein an, zu dem weitere optionale Bausteine hinzu gewählt werden können. Dies wurde vor allem aus der Marktübersicht deutlich. Um die Versicherer etwas zu unterstützen, hat der GDV unverbindliche Musterbedingungen für Cyber-Policen entwickelt. Abgesehen davon, dass es sich um eine junge Sparte handelt, wird ein umfangreicher Versicherungsschutz angeboten. Aber aufgrund der Vielzahl von optionalen

Bausteinen, muss für jeden Kunden meist eine individuelle Zusammenstellung erfolgen, dies führt wiederum zu Herausforderungen im Vertrieb.
In Deutschland sind Cyber-Policen seit 2011 auf dem Versicherungsmarkt, wobei aktuell laut dem GDV 38 Versicherer auf dem deutschen Markt Cyberversicherungen anbieten. Dieser Markt bringt für die Versicherungen allerdings Risiken, schließlich haben diese kaum bzw. keine Erfahrung bei der Preisfindung. Sodass davon auszugehen ist, dass nicht alle Versicherungsunternehmen diesem Wachstumsmarkt Stand halten werden können.

In einem weiteren Kapitel wurde die IT-Ausstattung in den Arztpraxen untersucht. Dabei wurde zunächst festgestellt, dass keine einheitliche IT-Ausstattung vorhanden ist. Die KBV gibt Empfehlungen, wie die IT am besten aufgebaut werden sollte. So sollte bspw. der Patientenserver nicht mit dem Netzwerk verbunden sein. In der Arbeit wurden einige mögliche IT-Ausstattungen beleuchtet, aber diese stellen keine Pflicht für die Praxen dar. Für die Dokumentation und Organisation stehen den Praxen zahlreiche PVS zur Verfügung, wobei Vertragsärzten empfohlen wird, diejenigen mit einem KBV-Zertifikat zu nutzen.
Für einen sicheren digitalen Datenaustausch hat das KBV das SNK eingerichtet. Hierdurch können vertragsärztliche Praxen sicher Daten elektronisch untereinander austauschen. Dabei liegen drei Varianten vor, wie eine Praxis das SNK nutzen kann. Grundsätzlich werden die Daten hierbei über VPN übertragen und je nachdem welche Variante des SNK gewählt wurde stehen mehr oder weniger Anwendungen zur Verfügung. Bei den medizinischen Geräten wird der Stand-alone-Betrieb empfohlen. Dieser stellt die sicherste Variante gegen Cyberangriffe dar, weil bei diesem Betrieb die medizinischen Geräte mit keinem Netzwerk verbunden sind.

Die TI stellt ein vielumstrittenes und kontrovers diskutiertes Thema dar. Für Privatpraxen ist die TI nicht verpflichtend, während vertragsärztliche Praxen bei nicht Anbindung an die TI bis zum 30. Juni 2019, mit Honorarkürzungen i. H. v. einem Prozent rechnen müssen. Zu Beginn ist lediglich die Anwendung VSDM vorhanden. Weitere Anwendungen werden in den kommenden Jahren folgen.
Ein wesentlicher Kritikpunkt bei der Anbindung der Arztpraxen an die TI besteht darin, dass Ärzte das Gefühl haben, keine Kontrolle über die Patientendaten zu haben. Dabei wird die ärztliche Schweigepflicht und das vertrauliche Arzt-Patienten-Verhältnis in Frage gestellt. Trotz dessen, liegen auch Vorteile vor, schließlich kommt es zur Vermeidung von Doppeluntersuchungen.

Eine Vielzahl der Praxen hat einen externen IT-Dienstleister, der sich um die IT in der Praxis kümmert. Im Rahmen des Marktüberblicks wurde ersichtlich, dass zwei Marktführer für PVS vorhanden sind. Dazu gehört die CompuGroup Medical Deutschland AG und medatixx GmbH & Co. KG.

Da keine Daten dazu vorliegen, wie viele Arztpraxen jährlich von Cyberangriffen betroffen sind, wurden im Rahmen der Arbeit einige Institutionen angeschrieben. Demzufolge wurden im Jahr 2018 in Bayern lediglich drei Cyberangriffen auf Arztpraxen zur Anzeige gebracht. Im Jahr 2019 (Stand 23.07.2019) wurden in Bayern vier Cyberangriffe auf Arztpraxen zur Anzeige gebracht. Aufgrund der Sorge um Reputationsschäden, melden viele niedergelassene Ärzte die Cyberangriffe nicht, sodass die Dunkelziffer deutlich höher ist.

Durch die Durchführung der empirischen Studie hat sich diese Masterarbeit im Wesentlichen mit der IT-Sicherheit der Arztpraxen auseinandergesetzt. Ziel der vorliegenden empirischen Studie war es, durch die Umfrage niedergelassener Ärzte den Umgang mit der IT-Sicherheit in den Praxen genauer zu beleuchten, da keine einheitliche IT-Ausstattung in den Praxen vorliegt. Durch die Standardisierung des Fragebogens ist sowohl die Reliabilität als auch die Validität dieser Forschung gewährleistet. Durch die geschlossenen Fragen blieb jedoch wenig Raum für Teilnehmende, sich über die vorgegebenen Antworten hinweg zu äußern.
Die Ergebnisse der vorliegenden Forschung haben gezeigt, dass die Betroffenheit durch Cyberangriffe keinen wesentlichen Einfluss auf die Nachfrage nach Cyberversicherungen hat. Zusätzlich konnte auch nicht festgestellt werden, dass bereits von einem Cyberangriff betroffene Praxen besser gegen Cyberangriffe geschützt sind als Praxen, die noch nie von einem Cyberangriff betroffen waren. Wohingegen nicht gesagt werden kann, dass Arztpraxen grds. zu wenig ihre IT schützen.
Nach Prüfung, ob einzelne Fachgruppen von Ärzten mehr oder weniger von Cyberangriffen betroffen sind, konnte festgestellt werden, dass die Radiologen in der Stichprobe noch nie von Cyberangriffen betroffen waren. Um die Ursache dafür herauszustellen, wurde weiterhin untersucht wie viele Schutzmaßnahmen die Fachgruppen durchschnittlich treffen. Dabei wurde ersichtlich, dass die Radiologen im Schnitt mehr Schutzmaßnahmen treffen.
Des Weiteren konnte im Rahmen der Untersuchung gezeigt werden, dass mit zunehmender Praxisgröße durchschnittlich mehr Schutzmaßnahmen getroffen werden, jedoch sind auch mit zunehmender Praxisgröße mehr Praxen von Cyberangriffen betroffen. Dies wurde darauf zurückgeführt, dass aufgrund dessen, dass größere Praxen mehr von Cyberangriffen betroffen waren, diese sich nun mehr schützen.
Zuletzt konnte ermittelt werden, dass mit zunehmendem Grad der Digitalisierung in den Praxen, die Nachfrage nach einer Cyberversicherung nicht signifikant zunimmt.
Zusammenfassend haben die Ergebnisse gezeigt, dass bei den niedergelassenen Ärzten ein mangelndes Bewusstsein für Cyberrisiken vorliegt. Deshalb sollte eine Cyberversicherung für niedergelassene Ärzte Schulungen zu dieser Thematik beinhalten.
Dazu konnte festgestellt werden, dass die untersuchte Thematik bislang wenig akademische Aufmerksamkeit erlangt hat. Aufgrund dessen kann diese Masterarbeit als erster Grundstein für weiterführende Forschung in diesem Bereich angesehen werden.

Offen bleibt also, wie sich die Situation zukünftig entwickelt. Grundsätzlich ist eine Einschätzung in Bezug auf Cyberrisiken schwierig, weil diese sich ständig in einer Weiterentwicklung befinden.

Einerseits werden die Cyberangriffe auf Arztpraxen womöglich weiter zunehmen, weil diese ganz klar aufgrund ihrer Daten, mit denen sie arbeiten, ein begehrtes Ziel und eine leicht erpressbare Zielgruppe sind. Dabei sind auch neue Geschäftsmodell der Hacker denkbar, wohingegen die Folgen schwerwiegender werden und die niedergelassenen Ärzte sich noch mehr dazu gezwungen sehen das Lösegeld zu zahlen, anstatt eine Anzeige zu erstatten und den Cyberangriff an die Öffentlichkeit zu tragen. Unter dieser Annahme wird auch die Nachfrage nach Cyberversicherungen steigen, sodass es in den kommenden Jahren zu einem Wachstum des Cyberversicherungsmarktes in Deutschland kommt. Andererseits soll die TI viel Sicherheit geben, sodass viele Cyberangriffe ohne Erfolg stattfinden. Wobei die TI für Hacker ein begehrtes Ziel werden kann, weil alle Patientendaten auf einem zentralen Server gespeichert sind. Das wichtigste für Versicherer von Cyberrisiken ist es, dass die Cyberversicherung sich ständig den neuen Risiken anpassen muss, damit die Arztpraxen umfassend abgesichert sind.