Cyber-Risk: Risikomanagement und Versicherungen für Freiberufler, KMU´s und Großunternehmen

Bachelorarbeit

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

vorgelegt von

Name: [redacted] Thesing Vorname: [redacted] Margiritte [redacted]

Prüfer: Prof. Dr. Michael H. Breitner

Hannover, den 22.06.2020

Inhaltsverzeichnis

1. Einleitung

1.1 Relevanz der Arbeit und Motivation

Es gibt zwei unterschiedliche Arten von Unternehmen: Einmal die, die gehacked wurden und dann diejenigen, die es noch gar nicht wissen (Chambers 2015).

Cyberrisiken sind heutzutage keine Seltenheit mehr und können jeden betreffen, unabhängig davon, ob es sich um einen Freiberufler, Klein-, Mittel-, (KMU´s) oder Großunternehmen handelt (Hiscox 2019). Häufig sind sich Unternehmen auch nicht darüber bewusst bereits Opfer eines Cyber-Angriffs zu sein, weshalb grundlegende Sicherheitsvorkehrungen unabdingbar sind.

Da wir uns im digitalen Zeitalter befinden und somit ein ständiger digitaler Wandel innerhalb der Informations- und Kommunikations-Technologie (IuK) stattfindet und Unternehmen zunehmend von ihnen abhängig werden, erlebt unsere Gesellschaft eine stetig wachsende Anzahl an Internetnutzern (Statista 2019). Neben den Chancen, welche das Internet für den Alltag und das Berufsleben mit sich bringt, ergeben sich auch einige Risiken. Ein weit ausgebautes World Wide Web (WWW) bietet gleichzeitig auch eine potenzielle Angriffsfläche für Cyberkriminalität, welches weitreichende Folgen für Unternehmen und die Gesellschaft mit sich bringt. Diese Art von Folgen erstrecken sich von Datenmissbrauch, über Erpressung bis hin zum Identitätsdiebstahl und können weitreichende wirtschaftliche Nachteile für die Betroffenen mit sich ziehen.

Problemtisch ist hierbei vor allem folgender Gedanke: *Um Cyberkriminalität zu umgehen, sollte unsere Gesellschaft auf das Internet weitestgehend verzichten.*

Da das Internet allerdings im Privat- sowie im Berufsleben einen wichtigen Bestandteil darstellt und auch Cloud Computing für unternehmerische Aktivitäten essenziell ist, ist ein Verzicht auf das Internet undenkbar. Besonders im 21. Jahrhundert stellt das Internet sowie die Digitalisierung einen essenziellen Baustein dar. Digitalisierung von Unternehmensbeziehungen sowie der Einfluss auf die Lieferkette und Wertschöpfung bilden einen zentralen Kern. Auch die ökonomischen Transaktionen unternehmerischer Tätigkeiten erfolgen elektronisch, weshalb das WWW unverzichtbar ist (Wrede et al. 2019).

Um den unternehmerischen Erfolg zu sichern, müssen Freiberufler und Unternehmen ihre informationstechnischen (IT) Systeme mit ausreichenden Sicherheitsvorkehrungen versehen. Dennoch wird deutlich, dass Cyber-Versicherungen nicht stark in Unternehmen etabliert sind, obwohl das Risikobewusstsein vorhanden ist (Gothaer 2019). Deshalb behandelt diese Arbeit unter anderem folgende Forschungsfrage (F1):

Wieso verzichten Freiberufler und Unternehmen trotz des Gefahrenbewusstseins weiterhin auf Cyber-Versicherungen und wieso ist es sinnvoll eine abzuschließen?

Auffällig ist, dass Hacker keine außergewöhnlichen Wege benötigen, um sich Zugriff zu fremden Dateien zu verschaffen oder ein IT-System mit Schädlingen zu infizieren. Authentische und glaubwürdige E-Mails reichen aus, um Mitarbeiter dazu zu bringen, Schädlingen durch Downloads Zugriff zum IT-System zu gewähren. Vor allem in Großunternehmen spielt Cloud Computing, wo hochsensible Informationen gespeichert werden, eine wichtige Rolle (Kwasniewski 2017), weshalb die dafür verantwortlichen Mitarbeiter äußerst achtsam sein müssen. Da wie schon erwähnt ein Gefahrenbewusstsein vorhanden ist und eine Infizierung der IT-Systeme vor allem in KMU´s meistens über eine E-Mail erfolgt (GDV 2018), beschäftigt sich diese Arbeit mit der zweiten Forschungsfrage (F2):

Welche Maßnahmen sind für eine optimale IT-Sicherheit notwendig sowie Mitarbeiter bezüglich Cyberrisiken weitestgehend zu sensibilisieren?

Hierbei darf auch nicht vernachlässigt werden, dass neben mangelnden pflichtbewussten Mitarbeitern auch technische Aspekte ein Gefahrenpotenzial darstellen, welches häufig auf die Software zurückzuführen ist. Vor allem besitzen Großunternehmen eine Software mit einer hohen Anzahl an Zeilen-Codes, welches mit einer steigenden Fehleranzahl einhergeht (Pohlmann 2019: 3-9).

Cyberrisiken werden noch in Zukunft ein enormes Gefahrenpotenzial für Freiberufler und Unternehmen darstellen. Im Gegensatz zu Großunternehmen verfügen Freiberufler und KMU´s nicht über ein gut ausgebautes IT-System sowie über ausreichend viele IT-Spezialisten (Newton et al. 2019: 9f.), weshalb sie höheren Sicherheitsvorkehrungen nachgehen müssen und grundlegende Sicherheitsmaßnahmen besonders essenziell sind. Aufgrund dessen beschäftigt sich diese Ausarbeitung zusätzlich noch mit dieser Forschungsfrage (F3):

Wie können Cyber-Versicherungen in Zukunft gestaltet werden, sodass sich diese auch bei Freiberuflern und KMU´s mehr etablieren?

Es darf hierbei nicht vernachlässigt werden, dass Cyberrisiken ohnehin schon in den letzten Jahren in allen Unternehmensgrößen stark angestiegen sind (Hiscox 2019) und es deswegen notwendig ist, sich künftig gegenüber derartigen Risiken abzusichern. Es ist also wichtig Maßnahmen zu entwickeln, um gewisse Sicherheitsvorkehrungen attraktiver zu gestalten, um somit das Ausmaß solcher Risiken auf Freiberufler und Unternehmen möglichst gering zu halten.

1.2 Gliederung der Arbeit

Diese Arbeit umfasst das Risikomanagement und Versicherungen von Freiberuflern, KMU´s und Großunternehmen bezüglich Cyberrisiken. In Kapitel zwei werden die wesentlichen Aspekte des Risikobegriffs, des Risikomanagements, der Versicherungen sowie wichtige Gesetze der Datenschutzgrundverordnung (DSGVO) vorgestellt. Auch wird hier auf die Ausgangssituation eingegangen, wieso es Cyberrisiken überhaupt gibt und welche Rolle sie in unserer Gesellschaft spielen.

Weiter wird in Kapitel drei eine Stand der Forschung- sowie eine Marktanalyse durchgeführt. Hierfür wird eine Literaturrecherche nach Templie und Paré (2015) herangezogen und die Marktanalyse bezieht sich auf Cyber-Versicherungen und ihr Angebot, welches sich auf dem deutschen Markt erstreckt. Das darauffolgende Kapitel umfasst eine Diskussion bezüglich der bisherigen Forschungsergebnisse und der aktuellen Marktsituation unter Anbetracht, wie sich die Cyberrisiken über die letzten Jahre hinweg bis heute entwickelt haben. Auch werden hier die Hauptursachen sowie die Auswirkungen von Cyberrisiken genauer erklärt und welchen Kosten Freiberufler und Unternehmen gegenüberstehen. Darauf folgt eine Übersicht des Leistungsangebotes von Cyberversicherungen in Deutschland. Anschließend werden Implikationen und Handlungsempfehlungen vorgestellt, um solche Risiken und die Auswirkungen zu minimieren, worauf die Limitationen folgen, welche dieser Arbeit unterliegen. Abgeschlossen wird diese Thematik mit einem Fazit, welches die wesentlichsten Ergebnisse übersichtlich darstellt sowie einem Ausblick für weitere Untersuchungen, welche die Erkenntnisse dieser Ausarbeitung erweitern würden.

2. Theoretische Grundlagen

2.1 Ausgangssituation

Besonders das 21. Jahrhundert ist von der Digitalisierung betroffen, welches vor allem auf Social, Mobile, Analytics sowie Cloud Computing (SMAC-Technologien) zurückzuführen ist. SMAC-Technologien ermöglichen eine steigende Anzahl an Innovationen, aber auch die Weiterentwicklung der Wirtschaft und Gesellschaft wird dadurch beeinflusst, da diese sich auf das Privat- und Berufsleben erstrecken. Digitalisierung stellt einen technischen Prozess dar, bei welchem analoge Signale in eine digitale Form umgewandelt werden und anschließend in Binärziffern. Somit werden Technologien für eine höhere Automatisierung von Arbeitsabläufen entwickelt, das Internet als Kommunkationsinfrastruktur dargestellt, welches vor allem für E-Commerce eine wichtige Rolle spielt. Durch die Digitalisierung werden aber auch steigende Rechenleistungen ermöglicht und eine Zunahme der Speicherkapazitäten und Kommunikationsmöglichkeiten.

Die Digitalisierung bringt also eine große Anzahl an Chancen mit in die Gesellschaft, weshalb Initiativen gefördert werden, welche die digitale Transformation von Wissenschaft, Industrie und der Gesellschaft fördert (Lenger et al. 2017: 302). Zudem können auch Unternehmen ihre Kundenbeziehungen stärken, indem sie mit Hilfe von Informationstechnologien ihre Produkte gestalten, wodurch gleichzeitig eine große Datenmenge entsteht, welches für Big Data-Anwendungen eine wichtige Rolle spielt (Knoll 2017: 5). Diese große Datenmenge beinhaltet vor allem auch diejenigen sensiblen und vertraulichen Kundendaten, welche durch Debit- sowie Kreditkartentransaktionen entstehen (Romanosky et al. 2019: 17).

Neben den Chancen bringt die Digitalisierung allerdings auch Risiken mit sich. In der Informationstechnologie entstehen vor allem Cyberrisiken durch die stetige

Schnittstelle zwischen der Unternehmens-IT, den Mitarbeitern sowie dem Datenschutz zu ermöglichen.

7. Fazit und Ausblick

Diese Arbeit hat sich mit den wesentlichen Grundzügen des Risikomanagements sowie mit den Versicherungen für Freiberufler, KMU´s und Großunternehmen auseinandergesetzt. Es wurden Auswirkungen durch Cyberrisiken erörtert und wieso es wichtig ist, in Sicherheitsmaßnahmen und Cyberversicherungen zu investieren.

Es geht hervor, dass die Anzahl der Cyberangriffe über die letzten Jahre hinweg stetig zugenommen haben und jeden betreffen, unabhängig davon, ob es sich um einen Freiberufler, KMU oder Großunternehmen handelt. Anzunehmen, dass kleine Unternehmen aufgrund ihrer Größe weniger attraktiv für Cyberkriminelle sind und deswegen weniger in Sicherheitsvorkehrungen investieren, zeugt von deutlichem Fehlverhalten. Somit werden KMU´s anfälliger gegenüber Cyberrisiken und Freiberufler werden unter anderem als Mittelsmann benutzt. Dies ist vor allem im Gesundheitswesen problematisch, da es sich dort ohnehin schon um hochsensible Kundendaten handelt.

Auch wenn viele Unternehmen nicht ausreichend in Sicherheitsvorkehrungen investieren, erkennen Mitarbeiter dennoch die Risiken, welche Cyberangriffe mit sich bringen. Die meisten Unternehmen erkennen, dass Vorkehrungen in IT-Sicherheiten drastisch gestiegen sind. Aufgrund dessen lässt sich die erste Forschungsfrage, wieso Freiberufler und Unternehmen trotz des Gefahrenbewusstseins weiterhin auf Cyber-Versicherungen verzichten und wieso es sinnvoll ist eine abzuschließen, damit beantworten, dass der Abschluss einer Cyberversicherung mit hohen Kosten einhergeht. Vor allem, wenn das Unternehmen ohnehin nicht über ausreichende Sicherheitsrichtlinien verfügt. Vor allem KMU´s sehen in Cyberversicherung weniger den Marktvorteil, sondern eher Zusatzkosten, welche diese mit sich bringen. Besonders mit dem Abschluss zusätzlichen Policen steigen die Prämien unterschiedlich stark an. Dennoch bietet eine Cyberversicherung den Vorteil, dass der Schaden, welcher einen Cyberangriff mit sich bringt, ja nach Vertrag und dem Erfüllen bestimmter Pflichten gedeckt wird. Somit schützen Freiberufler, KMU´s und Großunternehmen sich gegenüber Eigen- sowie Fremdschäden. Dies ist vor allem auch bei Unternehmen wichtig, die Teil einer Lieferkette sind, da ein schwaches IT-System eines anderen Glieds sich negativ auf das eigene Unternehmen auswirken kann.

Trotz des Gefahrenbewusstseins handeln Mitarbeiter oft fahrlässig, da Viren, Trojaner etc. meistens über E-Mails den IT-Server infizieren, oder sensible Informationen unverschlüsselt per E-Mail versendet werden. Auch Großunternehmen sind stark vom Outsourcing und Cloud Computing betroffen, worin häufig viele sensible Kundendaten und Betriebsgeheimnisse gespeichert werden. Aufgrund dessen ist eine Sensibilisierung von Mitarbeitern und Außendienstleistern besonders wichtig. Im Zuge dessen lässt sich die zweite Forschungsfrage, welche Maßnahmen für eine optimale IT-Sicherheit notwendig und wie Mitarbeiter bezüglich der Cyberrisiken weitestgehend

zu sensibilisieren sind, damit beantworten, dass vor allem Mitarbeiterschulungen sowie Hacker-Simulationen bei KMU´s und Großunternehmen zu einem pflichtbewussten Handeln beitragen können. Auch Außendienstleister müssen sensibilisiert werden, damit auch die Daten in der Cloud einen größtmöglichen Schutz genießen. Zudem können auch Cyberversicherungen dazu anregen, höheren Sicherheitsvorkehrungen nachzukommen. Zudem ist es notwendig, dass sich Freiberufler und Mitarbeiter im ausreichenden Umfang mit der neuen DSGVO auseinandersetzen, um auf dem neusten Stand zu sein und bezüglich allgemeinen Sicherheitsgesetzen weitestgehend informiert bleiben. Auch sollten Mitarbeiter von den Zuständigen über die Sicherheitsinformationen in ihrem Unternehmen stets in Kenntnis gesetzt werden, um die Risikosituation selbst bewerten zu können. Zudem müssen Freiberufler und Unternehmen bei einer Risikobewertung auch immer die latenten Schwachstellen einer Software berücksichtigen und sich diesbezüglich auch gegebenfalls mit dem Softwareanbieter in Verbindung setzen, um nicht noch weitere Schwachstellen bei einer Aktualisierung hervorzurufen.

Cyberversicherungen sind vor allem bei Freiberuflern und KMU´s nicht allzu sehr etabliert, da die Policen und Prämien mit hohen Kosten einhergehen und deshalb weniger ein Marktvorteil erkannt wird. Auch ist der Cyberversicherungsmarkt sehr individuell ausgelegt, weshalb sich die Kosten unter bestimmten Voraussetzungen stets unterscheiden sowie die Anforderungen unter Unternehmensgrößen und Branchen. Deswegen lässt sich die dritte Forschungsfrage, wie Cyberversicherungen attraktiver gestaltet werden können, damit sie sich bei Freiberuflern und KMU´s mehr etablieren, damit beantworten, dass Spezialisierungen bei Cyberversicherungen dazu beitragen können, sich in bestimmten Branchen und Unternehmensgrößen zu etablieren. Häufig werden bei Versicherungen Standardpakete angeboten, welches nicht für jede Unternehmensgröße oder Branche gleich optimal geeignet ist. Wenn beispielsweise eine Cyberversicherung auf Freiberufler und KMU´s ausgerichtet ist und somit das Standardpaket auch auf beide ausgelegt ist, kann es sein, dass bestimmte Vertragsvereinbarungen für den Freiberufler unnötig sind, aber für die KMU´s nicht, welches zu unnötigen Kosten führt. Beispielsweise werden bei Versicherungen häufig Netzwerkausfälle nicht abgedeckt, welches beispielsweise im Gesundheitswesen weitreichende Folgen mit sich ziehen würde, da viele wichtige Geräte für eine Patientenbehandlung digital vernetzt sind. Faire, individuelle und transparente Vertragsvereinbarungen, ausgelegt auf den Kunden und die Branche würden dazu beitragen, den Cyberversicherungsmarkt attraktiver zu gestalten und unnötig hohe Kosten zu vermeiden.

Um die Ergebnisse dieser Arbeit weiterzuführen, sind vor allem Experteninterviews unter Versicherungsanbietern, Freiberuflern, KMU´s und Großunternehmen nützlich, da somit eine qualitative Inhaltsanalyse einen differenzierten Überblick dieser Thematik verschafft. Dies würde Informationen liefern, auf welche Sicherheitsrichtlinien Versicherungsanbieter vor allem bei Freiberufler, KMU´s und Großunternehmen achten und welche Sicherheitsvorkehrungen dazu beitragen, dass bestimmte Anfrager gar keinen, einen Teil- oder sogar einen Vollschutz erhalten. Eine Umfrage unter Freiberuflern und KMU´s, weshalb oder weshalb sie keine Cyber-Police nachfragen, führt vor allem die Ergebnisse von F3 weiter. Im Rahmen solch einer Umfrage sollten auferlegte Sicherheitsmaßnahmen, Gründe, die Kosten der Prämien

sowie deren Tragbarkeit ermittelt werden. Somit ist für jede Unternehmensgröße eine Kosten-Nutzen-Analyse möglich.

Aber auch eine Umfrage unter Mitarbeitern bei KMU´s und Großunternehmen liefert Informationen darüber, inwieweit sie sensibilisiert sind und inwieweit ihr Unternehmen dies unterstützt. So eine Umfrage ist vor allem dann sinnvoll, wenn diese unter verschiedenen Branchen stattfindet, um somit festzustellen, ob eine Branche sich auf bestimmte Maßnahmen mehr fokussiert als eine andere. Vor allem Interviews bei Großunternehmen geben Informationen darüber, inwieweit sie tatsächlich darauf achten, dass Außendienstleister sensibilisiert werden. Auch dies liefert hilfreiche Informationen für F2 und F3.

Aber auch eine Studie über unterschiedliche Cyberversicherungsmärkte würden diese Ergebnisse erweitern. Im Rahmen solch einer Studie können Gemeinsamkeiten und Unterschiede dieser Branche unter verschiedenen Ländern ermittelt werden. Die daraus resultierenden Ergebnisse würden wichtige Implikationen und Handlungsempfehlungen für den deutschen Cyberversicherungsmarkt liefern, welche bisher noch nicht beachtet wurden oder unentdeckt sind.