Informationssicherheit und Covid-19: Chancen und Herausforderungen mobilen Arbeitens

Masterarbeit

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

vorgelegt von

Name: Hempen Vorname: Marvin

[redacted] [redacted] [redacted] [redacted]

Prüfer: Prof. Dr. Michael H. Breitner

Hannover, den 18.03.2021

Inhaltsverzeichnis

1. Einleitung

Die Meldung über den Ausbruch des Coronavirus im Dezember 2019, welches folglich unter dem Synonym Covid-19 geführt wird, markiert den Beginn eines weitreichenden Einschnitts in die zuvor normale Art und Weise der Arbeit. Mit der Einstufung als Pandemie durch die World Health Organization im März 2020 betraf die Situation eine Vielzahl von Nationen auf ökonomischer und auch psychologischer Ebene (vgl. Pan et al. 2020: 1). Diese Einstufung bewegte Regierungen dazu, Maßnahmen zu ergreifen, die unter dem Begriff des Lockdowns das Ziel haben, eine weitere Ausbreitung von Covid-19 zu reduzieren. Jene Maßnahmen umfassen die vorübergehende Schließung von Geschäften und die Verlagerung des Arbeitsortes vieler Beschäftigter in das Home-Office (vgl. Richter 2020: 1).

Mobiles Arbeiten im Home-Office stellt aus Sicht von Organisationen eine effektive Maßnahme dar, unter Einhaltung der auferlegten Maßnahmen der Regierungen die Produktivität von Beschäftigten aufrechtzuerhalten. Der dabei erdachte Zeithorizont ist jedoch ein kurzfristiger. Langfristiges Arbeiten im Home-Office birgt wiederum folgenschwere Risiken (vgl. Borkovich und Skovira 2020: 239). Da auch die Pandemie, ausgelöst durch Covid-19, keinen kurzfristigen Zeithorizont aufweist, stellt die mobile Arbeit von Beschäftigten im Home-Office einen Teil der neuen Art der Arbeit dar (vgl. Carroll und Conboy 2020: 1). Die Risiken dieser neuen Art der Arbeit begründen sich aus der Schwierigkeit interne Bedrohungen der Informationssicherheit durch den Beschäftigten mithilfe bestehender Sicherheitssysteme zu adressieren. Dies meint auch den unbeabsichtigten Verlust sensibler Daten. Die Arbeit im Home-Office verbindet somit die Gefahren durch interne Beschäftigte sowie externe Bedrohungen in Form von Hacker- oder Social Engineering-Angriffen (vgl. Borkovich und Skovira 2020: 236).

Gründe für die gestiegenen Herausforderungen für Organisationen mit Bezug auf sensible Daten sind in der Schnelligkeit von Covid-19 und dem damit einhergehenden Wechsel ins Home-Office zu sehen. Diese Kurzfristigkeit stellt Organisationen vor zeitliche und finanzielle Probleme, wenn Infrastrukturen aufgesetzt, mobile Endgeräte beschafft und zudem mit Sicherheitssoftware ausgestattet werden müssen (vgl. Sarginson 2020: 10). Die Folge der Kontaktbeschränkungen kann oftmals die Nutzung privater Endgeräte der Beschäftigten sein, um die Arbeitsfähigkeit aufrecht zu erhalten. Zudem werden private Netzwerke genutzt, die parallel zu den privaten Endgeräten nicht nach industriellen Standards gesichert sind und eine Gefahr für den Abfluss sensibler Organisationsdaten darstellen. Organisationen, dessen Beschäftigte ein mobiles Dienstgerät nutzen, können ein gewisses Sicherheitsniveau gewährleisten. Mit den notwendigen Rechten, um im Home-Office essenzielle Software installieren zu können, steigen mögliche Gefahren jedoch erneut an (vgl. Pranggono und Arabo 2020: 1). Diese Herausforderungen für die Informationssicherheit sind es, die den möglichen Chancen eines Wechsels ins Home-Office in dieser Arbeit gegenübergestellt werden. Sie stellen den zentralen Gegenstand der Arbeit dar. Den Kontext bilden dazu Informationstechnologien und dessen Verarbeitung von Informationen durch verschiedene Dimensionen während der einschränkenden Covid-19 Maßnahmen.

Die Gegenüberstellung der Chancen und Herausforderungen mobiler Arbeitsformen wie die Arbeit im Home-Office und die Arbeit von unterwegs erfolgt unter der Prämisse, dass die Maßnahmen durch Covid-19 einen erheblichen Einfluss auf die Arbeitsweise von Beschäftigten und damit der Informationssicherheit ausüben. Um dieses Ziel zu erreichen, muss zunächst identifiziert werden, durch welche konkreten Faktoren sich dieser Einfluss zeigt. Dazu werden entlang der drei zentralen Dimensionen dieser Arbeit markante Faktoren hervorgehoben. Die bisher veröffentlichte Literatur zur Thematik mobiler Arbeit wird zusammen mit der aktuellen Literatur zu Covid-19 auf Chancen und Herausforderungen ebendieser Faktoren untersucht. Um anschließend die theoretischen Ergebnisse auf eine

Relevanz für die Praxis zu überprüfen, werden Experten im Rahmen einer qualitativen Inhaltsanalyse zu ihren Erfahrungen und Ansichten mithilfe eines Fragenkataloges interviewt. Jene Experten ermöglichen aufgrund ihrer diversen Positionen, Kompetenzen und Erfahrungen, unterschiedliche Blickwinkel auf die Thematik und bieten die Möglichkeit zusätzliche Ergebnisse zu gewinnen. Die gewonnenen Erkenntnisse kombinieren die bestehenden Chancen und Herausforderungen der Literatur zu mobiler Arbeit mit der Literatur, welche die generellen Herausforderungen für die Informationssicherheit untersucht, und bettet diese in den zeitlichen Kontext der weltweiten Ausnahmesituation durch Covid-19 ein. Hieraus ergeben sich praktische Implikationen für Organisationen, die es anstreben jene Chancen zu realisieren und zugleich entstehende Herausforderungen zu reduzieren.

Diese Arbeit trägt den Titel Informationssicherheit und Covid-19: Chancen und Herausforderungen mobilen Arbeitens. Der damit erforschte Gegenstand unterteilt sich in zwei grundlegende Fragestellungen die als folgende Forschungsfragen dargestellt werden:

1. *Was sind die Einflussfaktoren mobiler Arbeitsformen auf die Informationssicherheit?*

2. *Welche Chancen und Herausforderungen ergeben sich durch mobile Arbeitsformen aus Sicht von Organisationen, Beschäftigten und mobilen Endgeräten zu Covid-19?*

Die erste Forschungsfrage betrachtet den Einfluss, den mobiles Arbeiten auf die Sicherheit von Informationen darstellt und verknüpft diese zwei zentralen Aspekte. Dazu werden technische, menschliche und organisatorische Faktoren benannt. Die Aspekte Chancen und Herausforderungen sowie Covid-19 werden mithilfe der zweiten Forschungsfrage abgedeckt, welche diese Chancen und Herausforderungen mobiler Arbeitsformen zu Covid-19 untersucht.

Mobiles Arbeiten im Home-Office setzt eine Begrenzung dieser Arbeit, da aufgrund der Einschränkungen der Mobilität ein mobiles Arbeit von unterwegs zum Zeitpunkt des Verfassens nicht oder sehr eingeschränkt möglich ist. Zwar werden in der Literatur und der Expertenbefragung auch Chancen und Herausforderungen ortsunabhängiger Arbeit untersucht, der Fokus dieser Arbeit liegt jedoch auf dem Home-Office. Die dabei eingesetzten mobilen Endgeräte bilden die technische Begrenzung dieser Arbeit, sodass der Fokus auf dem für die Tätigkeit genutzten Laptop, Smartphone oder Tablet liegt, dessen Bedienung über die individuellen Beschäftigen erfolgt. Sie bilden einen weiteren zentralen Aspekt und damit gleichzeitig eine Begrenzung des Rahmens dieser Arbeit.

Die vorliegende Arbeit gliedert sich in folgende Abschnitte. Zunächst werden im zweiten Kapitel die Kerninhalte dieser Arbeit als theoretische Grundlagen verdeutlicht. Folglich werden die Schlüsselfaktoren mobiler Arbeit festgelegt. Im Weiteren werden die Definitionen der Informationssicherheit, welche die Informationstechnologie (IT)- und Cyber-Sicherheit und den Datenschutz umfasst bestimmt. Ebenfalls werden die mobilen Arbeitsformen wie die Telearbeit im Sinne des Home-Office, der mobilen Arbeit unterwegs und die Nutzung privater Endgeräte nach dem BYOD-Ansatz definiert. Kapitel 3 zielt auf die Identifikation relevanter Faktoren ab, welche die Sicherheit von Informationen während der mobilen Arbeit sowohl positiv als auch negativ beeinflussen. Hierbei werden die in Kapitel 2 benannten Schlüsseldimensionen, insbesondere deren Schnittmengen als Grundlage herangezogen. Im vierten Kapitel werden die zuvor identifizierten Faktoren anhand einer umfassenden Literaturrecherche nach Webster und Watson auf Chancen und Herausforderungen untersucht. Somit werden erste theoretische Ergebnisse gesammelt die im Anschluss in Kapitel 5 durch praktische

Erfahrungen und Sichtweisen 15 befragter Experten zur Thematik Informationssicherheit mobiler Arbeit im Home-Office untermauert, ergänzt und zum Teil wiederlegt werden. Die im Rahmen der qualitativen Inhaltsanalyse gewonnenen Erkenntnisse werden in Kapitel 6 basierend auf den identifizierten Einflussfaktoren mit den Resultaten der Literaturrecherche verglichen und diskutiert. Kapitel 7 schildert die limitierenden Aspekte dieser Arbeit und zeigt Potenzial zur Optimierung auf. Mögliche Handlungswege und Empfehlungen notwendiger Schritte, um die Chancen mobiler Arbeitsformen zu maximieren und parallel Risiken für die Informationssicherheit zu reduzieren, werden in Kapitel 8 vorgeschlagen. Das neunte und letzte Kapitel schließt diese Arbeit mit einem Fazit und einem Ausblick auf weiterführende offene Fragen für die Forschung ab.

2. Theoretische Grundlagen

Um den Kern dieser Arbeit, die informationssicherheitsbezogenen Chancen und Herausforderungen mobilen Arbeitens, betrachten zu können, bedarf es vorab festgelegter Definitionen zur Thematik. Zum einen definiert dieses Kapitel die grundlegenden Dimensionen mobilen Arbeitens, welche in dieser Arbeit betrachtet werden und die Informationssicherheit als Ganzes. Zum anderen werden die mobilen Arbeitsformen deren Ausprägung der Telearbeit, mobilen Arbeit und der Nutzung privater Endgeräte im Sinne des BYOD-Ansatzes fokussiert.

2.1 Schlüsselfaktoren mobiler Arbeit in Anlehnung an das FRAME-Model

Die Grundlage dieser Arbeit bilden drei Dimensionen, welche die unterschiedlichen Perspektiven und Schlüsselfaktoren mobiler Arbeitsformen, insbesondere des Home-Offices, abbilden sollen. Abbildung 1 zeigt diese Dimensionen in einem Venn-Diagram, welches in Anlehnung an das Framework for the Rational Analysis of Mobile Education (FRAME) Model von Koole (2009: 27) zur Thematik des mobilen Lernens ähnlich strukturiert ist. Unter den Begriffen *Device*, *Learner* und *Social*, betrachtet die Autorin die physischen und technischen Aspekte des mobilen Endgerätes in Kombination mit dem Menschen als Nutzer eines sozio-technischen Systems und kombiniert diese mit den Regeln, die es in der Kooperation miteinander zu beachten gilt. Diese Aspekte finden im Kontext der Nutzung und des Austauch von Informationen statt (vgl. Koole 2009: 26–40).

Um die Arbeit von zuhause realisieren zu können sollten Organisationen neue Technologien wie Kollaborationssoftware oder Netzwerkhardware sorgfältig prüfen und die Qualität und Leistung dieser an die bestehenden Anforderungen der Organisation anpassen. Die Nutzung der Cloud-Technologie bietet in diesem Zusammenhang einen sicheren Zugang auf die Unternehmensdaten. Wird ein VPN-Dienst für den Zugriff auf Organisationsnetzwerke genutzt, sollte dieser bereits beim Start des Dienstgerätes automatisch aktiviert werden, um das Risiko unachtsamer Handlungen des Beschäftigten präventiv zu mindern. Sichere Zugänge in Kombination mit einer intensiven Schulung der Beschäftigten gestalten mobile Arbeitsformen somit sicherer und fördern die Informationssicherheit.

9. Fazit

9.1 Zusammenfassung

Das Ziel dieser Arbeit ist es, die Chancen und Herausforderungen mobilen Arbeitens hinsichtlich der Informationssicherheit zu Covid-19 einander gegenüberzustellen und daraus Implikationen für die Praxis aufzuzeigen. Hierzu wurden in Kapitel 2 zunächst die Grundlagen der zu betrachtenden Aspekte festgelegt und definiert. Die erste Forschungsfrage untersucht die Einflussfaktoren mobilen Arbeitens auf die Informationssicherheit. Entlang der Dimensionen des mobilen Endgerätes, des Beschäftigten, der Organisation sowie deren gemeinsamer Schnittmengen werden diese benannt. In einer detailierten Betrachtung in Forschungsfrage 2 werden zu diesen Faktoren Chancen und Herausforderungen in der Literatur und anhand der Aussagen der Experten verglichen. Die zentralen Aspekte der technischen Dimension umfassen die Software und Hardware des mobilen Endgerätes. Die Schnittmenge zur Organisation stellt dabei das Netzwerk und die Verwaltung des Gerätes dar. In der Befragung der Experten wurde ein nachrangiger Stellenwert des mobilen Endgerätes im Bezug auf die Informationssicherheit deutlich. Das Endgerät stellt einen Zugangspunkt auf sensible Informationen der Organisation dar und kann durch unachtsame oder fehlerhafte Benutzung für weitreichende Folgen wie die Infektion mit Schadsoftware, die Offenlegung sensibler Dokumente oder das maliziöse Verändern von Daten sorgen. Entscheidend ist hierbei, ob und wie umfassend Sicherheitssoftware auf dem Endgerät installiert ist und verwaltet wird. In der Literatur gehen viele Risiken mit der Nutzung von privaten Endgeräten nach dem BYOD-Ansatz aufgrund der Prämisse des ungesicherten und bereits infizierten Endgerätes, welches unachtsam genutzt wird, einher. In der Praxis der Experten wurde die Nutzung privater Endgeräte in den wenigsten Fällen erlaubt. Die Herausgabe dienstlicher Endgeräte zur privaten Nutzung erhöhe die Sicherheit durch zusätzliche Sicherheitssoftware. Lediglich ein Experte nutzt nach seinen Angaben ein ungesichertes, privates Endgerät um dienstliche E-Mails zu empfangen. Die Verwendung eines Dienstgerätes in Verbindung mit einer VPN-Verbindung sowie mit cloudbasierten Anwendungen steigern die Informationssicherheit zu einem ausreichenden Level im Home-Office. In der Praxis stellen trotzdessen das Versäumen einer manuellen Aktivierung des VPN-Dienstes, die Nutzung und Offenlegung schwacher Zugangspasswörter und das Folgeleisten einer Phishing-E-Mail die größten Risiken dar. Diese Punkte sind zur Entstehung nur in Kombination mit einem Beschäftigten möglich, der diese Handlungen ausführt.

Der individuelle Beschäftigte und dessen Nutzungsverhalten bildet eine weitere zentrale Dimension und ist nach Meinung der Experten der Hauptangriffspunkt für Organisationen. Die benannten Risiken entstehen dabei dank mangelnden Know-Hows für die Nutzung jener Software im Home-Office oder durch unbewusstes und unachtsames Handeln im Laufe des Arbeitsalltages. Eine fehlende Akzeptanz für neue Technologien und Arbeitsweisen können in

Kombination mit steigender Unsicherheit in der Nutzung und Ablenkung im privaten Umfeld eine perfekte Ausgangssituation für unabsichtliche Fehler beim Verarbeiten von Informationen oder für Social Engineering-Methoden durch externe Angreifer sein. Das räumliche Umfeld des Home-Office und die eventuellen familiären Verpflichtungen können Stress und Ablenkung des Beschäftigten fördern. Die Arbeit von zuhause geht dennoch in der Literatur und aus der Sicht der Experten mit einem Zuwachs für die Produktivität und Flexibilität und somit der Zufriedenheit der Beschäftigten einher. In allen fünfzehn Fällen der Experten ist der Wechsel ins Home-Office erfolgreich durchgeführt worden, sodass neue Erfahrungen gewonnen werden können, aufgestaute Entwicklungen von Organisationen in unterschiedlichen Umfängen umgesetzt wurden und neue, digitale Arbeitsweisen und Technologien kennengelernt und in den meisten Fällen akzeptiert werden. Damit die Wahrscheinlichkeit für eine erfolgreiche Nutzung mobiler Arbeitsformen steigt, müssen vor allem Führungskräfte dazu beitragen, dass neue Leitlinien der Organisation und sich ändernde Strukturen und Prozesse intensiv und positiv an die Beschäftigten kommuniziert werden. Der transformationale Führungsstil verspricht in der Literatur und aus Sicht der Experten die größten Erfolge in der Ansprache von Konflikten während der Arbeit im Home-Office, dem Entgegennehmen von Ängsten und Wünschen und in der Vermittlung einer sich wandelnden Organisationskultur.

Organisationen selbst bilden die dritte Dimension dieser Arbeit und aufgrund der beeinflussenden Faktoren der strategischen Ausrichtung und der vorhandenen Ressourcen einen ebenso bedeutsamen Aspekt wie die Beschäftigten. Die Organisation legt fest, welches Sicherheitsniveau für mobile Endgeräte bestehen soll. Sie bestimmt, welche Regeln der Kooperation und der Sicherheit seitens der Beschäftigten eingehalten werden müssen. Zudem entscheidet sie, welche Technologien mit der Strategie in Einklang gebracht werden können und setzt diese unter Berücksichtigung der vorhandenen Ressourcen um. Anhand der Literatur und den Erfahrungen der Experten können große Unterschiede in den Organisationsstrukturen gesehen werden. So gehen mit kleinen und mittelständischen Organisationen höhere Risiken aufgrund ihrer finanziellen Mittel, der verfügbaren personellen Kapazitäten und des vorhanden Know-Hows einher. Zwar ist der Wechsel ins Home-Office aufgrund kleinerer Rollen und Prozesse schneller, die Ausgangssituation dieser Organisationen verursacht im Vergleich zu großen Organisationen jedoch zusätzliche Risiken. Jene großen Organisationen bieten das höchste Sicherheitsniveau aufgrund interner IT-Organisationseinheiten, höherer finanzieller Mittel, besseren Know-Hows und einer meist zuvor bestehenden Infrastruktur, die sicheres, mobiles Arbeiten ermöglicht. Hinzukommend stehen nicht digitale Organisationen vor größeren Umbrüchen als digitale Organisationen. Verkürzte Prozesse oder das Aufdecken ineffizienter und ineffektiver Abläufe bieten wiederum eine große Chance für alle Organisationen, bestehende Geschäftsmodelle und Strukturen innerhalb der Organisation zu optimieren. Ein erhöhtes Bewusstsein für die Informationssicherheit sollte ebenfalls im strategischen Interesse der Organisation sein, damit der unabsichtliche Verlust sensibler Daten verhindert werden kann. Intensive, regelmäßige Schulungen der Beschäftigten über die Einführung neuer Technologien, deren Nutzung und den Sinn und Zweck einzuhaltender Sicherheitsmaßnahmen sind zu Covid-19 Zeiten und darüber hinaus von höchster Priorität. Dazu bedarf es großem Engagements der Führungskräfte und einer intensiven Kommunikation mit den Beschäftigten.

9.2 Ausblick

Die Ergebnisse dieser Arbeit lassen weitere Fragen offen, deren Beantwortung über den Umfang dieser Arbeit hinausgeht. Diese Fragen sollten in zukünftigen Forschungsarbeiten aufgenommen und beantwortet werden. Ein weites Feld möglicher Risiken für die

Informationssicherheit spielen die in dieser Arbeit nur kurz erwähnten smarten Endgeräte innerhalb des Home-Office. Mögliche das Netzwerk betreffende Herausforderungen seitens des IoT sollten auf Basis der Tätigkeit in privaten Räumen genauer betrachtet werden. Dies deckt Herausforderungen der technischen Aspekte ab. Betrachtet man den Aspekt der Beschäftigten sollte der situative Faktor Covid-19 als möglicher langfristiger Einflussfaktor auf die Verhaltensbildung und auf unbeabsichtigtes Fehlverhalten der Beschäftigten untersucht werden. Die in dieser Arbeit ambivalente Beurteilung des Einflusses von Covid-19 in Form von gestiegener Unsicherheit, erhöhtem Stress und der Ablenkung im Home-Office bietet Potenzial für eine genauere und vor allem langfristige Untersuchung. Mit Blick auf die Organisation stellt sich die Frage, ob Organisation nach einer Lockerung der Covid-19 Maßnahmen weiterhin an neuen Technologien festhalten und digitale Arbeitsweisen fördern oder ob jener teilweise erzwungene Wechsel zur mobilen Arbeit wie auch Covid-19 für viele Organisationen und Beschäftigte eine Ausnahmensituation bleibt.