IT-Sicherheit der Digitalisierung in Kleinen und Mittleren Unternehmen: Eine literaturbasierte und empirische Studie von Effekten und Barrieren

Erik Kolek[1]

[1] Universität Hildesheim, ISUM, Hildesheim, Germany
{erik_kolek}@gmx.de

Abstract. Die für kleine und mittlere Unternehmen (KMU) geeigneten IT-Sicherheitsaspekte wurden festgelegt, welche für die Digitalisierung in KMU wichtig sind. Hierzu wurde eine literaturbasierte Hypothesenbildung angewandt, welche IT-Sicherheitsaspekte für KMU wie Effekte und Barrieren hervorgebracht hat. Darauf aufbauend wurden die Hypothesen über die für KMU geeigneten IT-Sicherheitseffekte sowie -barrieren einer quantitativen Studie von KMU in Deutschland unterzogen. Diese empirische Hypothesenevaluation hat darüber Aufschluss gegeben, dass die literaturbasierten IT-Sicherheitsaspekte auch größtenteils für die Praxis der Digitalisierung in KMU in Deutschland als wichtig eingestuft werden können und daher mehr Beachtung erfahren sollten.

Keywords: IT-Sicherheit, Digitalisierung, Kleine und Mittlere Unternehmen.

1 Einführung

Die Nutzung von Informationstechnologie (IT) unabhängig von der Unternehmensgröße und Branche ist zu einem der wichtigsten Aspekte im Geschäftsumfeld von Unternehmen geworden. Vor allem kleine und mittlere Unternehmen (KMU) investieren einen entscheidenden Teil ihrer (finanziellen) Ressourcen in die IT, um ihre Fähigkeit im weltweiten Wettbewerb auszubauen. Zunehmend werden immer mehr Informationen gebildet und über eine große Anzahl von miteinander verknüpften Netzwerken übertragen. Gleichzeitig haben die Internetkriminalität und IT-Sicherheitsbedrohungen deutlich zugenommen, bspw. Schadsoftware, Spam und Phishing [1-2].

Diese Bedrohungen können zu hohen Verlusten für KMU führen und deren Wachstumschancen beeinträchtigen. Zudem bewirken Bedrohungen Kosten aufgrund von Geschäftsprozessausfällen, Schäden am Unternehmensansehen und Ausgaben, die zum Schutz der genutzten IT vor Angriffen und Missbrauch benötigt werden [2-4].

IT-Sicherheitsbedrohungen sind gekennzeichnet durch eine hohe Komplexität, da diese eine bedeutende Anzahl von Aspekten umfassen, die gemeinsam in Beziehung stehen können. Aufgrund der steigenden IT-Abhängigkeit ist die IT-Sicherheit in KMU von hohem Interesse, um entsprechenden Bedrohungen entgegen wirken zu können [2].

Da IT-Sicherheit in KMU für alle Beteiligten eine wichtige Angelegenheit darstellt, verlangt die Bekämpfung und Vorbeugung von IT-Sicherheitsbedrohungen eine

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

effektive Kooperation zum Aufbau und zur Erhaltung von IT-Sicherheit der Digitalisierung in KMU. Eine Herausforderung bei dieser Kooperation in KMU besteht daraus, dass jeder Beteiligte, wie Funktionen und Mitarbeitende, eine andere Meinung und einen anderen Ansatz vertritt, wie IT-Sicherheitsfragen beantwortet und wie potenzielle IT-Sicherheitsbedrohungen gehandhabt werden sollen. KMU verfügen über eine unterschiedliche – meist limitierte – finanzielle und personelle Ressourcenkapazität, die für die Kooperation zur Bekämpfung und Vorbeugung von IT-Sicherheitsbedrohungen zur Verfügung steht [2].

Die limitiert zur Verfügung stehende Ressourcenkapazität von KMU hinterlassen eine Lücke im Bereich der IT-Sicherheit der Digitalisierung und damit in Netzwerken von Unternehmen. Mittels des Zugangs zu wichtigen Informationssystemen werden KMU effektiver Bestandteil von Unternehmensnetzwerken, sodass in Anbetracht der potenziellen Möglichkeiten von IT-Sicherheitsbedrohungen, KMU als schwächstes Glied im Unternehmensnetzwerk auftreten können. Wie in jedem Netzwerk ist das schwächste Glied ein attraktiver Einstiegspunkt, um die in Unternehmen vorhandene IT anzugreifen. Jedes Netzwerk ist nur so sicher wie seine angreifbarste Schnittstelle, sodass für ein abgesichertes Unternehmensnetzwerk eine spezielle Aufmerksamkeit auf die IT-Sicherheit der Digitalisierung von KMU bestehen muss [2].

Vor diesem Hintergrund der fortschreitenden Digitalisierung in KMU liegt die Motivation dieser Forschungsarbeit darin, diejenigen IT-Sicherheitsaspekte zu erkennen und zu beschreiben, die für die IT-Sicherheit der Digitalisierung in KMU in Deutschland von besonderer Bedeutung sind. Die zugrundeliegende Forschungsfrage lautet daher: *Welche Aspekte hinsichtlich der IT-Sicherheit mit Wichtigkeit für KMU in Deutschland bestehen und wie lassen sich diese Aspekte inhaltlich beschreiben*?

2 Verwandte Arbeiten

Ein großer Anteil der KMU verfügt über unzureichendes IT-Personal mit genügend Wissen über die IT-Sicherheit und nicht über die Zeit und das erforderliche IT-Budget, um nötige IT-Infrastrukturen für eine Digitalisierung in KMU abzusichern [5].

Eine empirische Studie hat vor diesem Hintergrund einen Analyseschwerpunkt auf die Eignung von IT-Sicherheitsmanagement-Standards für KMU gelegt. In der Analyse waren KMU in Frankreich mit weniger als 250 Mitarbeitenden vertreten, da diese eine niedrige Akzeptanz gegenüber IT-Sicherheit innehatten. Weniger als 20% der KMU haben ein betriebliches IT-Sicherheitsmanagement oder einen Notfallplan fixiert. Dies stellt im Vergleich zu Großunternehmen einen offensichtlichen Schwachpunkt dar. In KMU bestehen eindeutige Unterschiede zwischen den tatsächlich eingeführten IT-Sicherheitsmaßnahmen und den tatsächlich vorhandenen IT-Sicherheitslücken. KMU konzentrieren sich auf IT-Sicherheitsmaßnahmen zur Vermeidung der mit niedriger Eintrittswahrscheinlichkeit existierenden Bedrohungen, anstatt häufiger auftretender und kostspieligerer Bedrohungen vorzubeugen [6].

In einer zweiten Studie wurde die Akzeptanz von IT-Sicherheitsstandards in KMU in Deutschland betrachtet. Die Forscher untersuchten deren Eignung hinsichtlich der Unternehmensgröße und diskutierten verschiedene Herausforderungen bei deren

Einführung. Der Untersuchungsgegenstand wurde begrenzt, sodass nur KMU betrachtet wurden, die mehr als 40 Mitarbeitende beschäftigten und einen Umsatz von mehr als 2 Millionen Euro pro Jahr erzielten. Da im Bereich der IT-Sicherheit der Digitalisierung viele Standards und andere Rahmenbedingungen in KMU als in Großunternehmen existieren, wurden die folgenden Rahmenwerke ausgewählt: ISO 27000-Reihe, Standard of Good Practice (SoGP), Control Objectives for Information and Related Technology (COBIT) und IT Infrastructure Library (ITIL). Die Forscher nahmen an, dass Studien hinsichtlich der Eignung von IT-Sicherheitsstandards für KMU bisher kaum im Fokus standen, da diese in KMU weitestgehend unbekannt sind. Zu diesem Phänomen gäbe es diverse Diskussionen vom Mangel an Interesse über zu wenig Akzeptanz bis hin zur geringen Eignung von IT-Sicherheitsstandards für KMU. Nichtsdestotrotz kommen die Forscher zu der Schlussfolgerung, dass im Umgang mit der IT-Sicherheit der Digitalisierung und den damit verbundenen betrieblichen Informationssystemen die Besonderheiten von KMU mehr Beachtung erfordern [7].

3 Literaturbasierte Hypothesenbildung

3.1 Für KMU entwickelte IT-Sicherheitseffekte

Die in der letzten Zeit sich rasant und schnell wandelnde wirtschaftliche Entwicklung im IT-Bereich hat auch KMU vor neuen Herausforderungen gestellt. Zu diesen neuen Herausforderungen zählen die Digitalisierung der gesamten KMU und die dazugehörigen Geschäftsprozesse. Vor allem die Umstrukturierung existierender Geschäftsmodelle, die Automatisierung einzelner oder aller Geschäftsprozesse und die weltweite digitale Vernetzung werden mit der Digitalisierung in Zusammenhang gebracht. Diese Veränderungen führen zu einer Umwandlung aller Geschäftsprozesse, die auch alle KMU beachten müssen, um ihre Wettbewerbsfähigkeit zu erhalten. Solchen Veränderungen waren lange Zeit nur große Unternehmen ausgesetzt – insbesondere im Zusammenhang mit aktuellen Themen wie Big Data, Cloud Computing oder Industrie 4.0, die in der Vergangenheit eingestuft wurden von KMU als nicht wichtig, zu kostspielig und zu kompliziert [8].

Diese digitalen Veränderungen haben zur Folge, dass KMU genauso wie die Großkonzerne allen Arten digitaler Wirtschaftskriminalität ausgesetzt sind, bspw. in Form von Datendiebstahl, Sabotage, Malware, Konkurrenzausspähung usw. Deshalb sind KMU mit schwieriger werdenden Herausforderungen konfrontiert, um relevante Informationen und ihr erworbenes Know-how vor unbefugten Dritten zu schützen und angemessene Vorkehrungen betreffs der IT-Sicherheit ihrer Digitalisierung zu treffen. Das hat zur Folge, das neben den Vorteilen der Digitalisierung insbesondere die ökonomische Bedeutung der IT-Sicherheit für KMU eine größere Rolle einnimmt und die IT-Sicherheit durch ein gutes Zusammenwirken zwischen der IT-Governance, IT-Compliance und dem IT-Risikomanagement unterstützt und gestärkt werden kann [9].

Neben der in Abstimmung mit der IT zu erreichenden Unternehmensziele sind für Unternehmen zudem gesetzliche Vorgaben bezüglich der IT-Compliance zu beachten. Inhalte dieser gesetzlichen Vorgaben sind z. B. der Datenschutz, die Ausfallsicherheit

der IT-Infrastruktur als auch die Erfüllung gesetzlicher Archivierungs- und Dokumentationspflichten. Eine etablierte IT-Compliance-Kultur ist insbesondere in KMU seltener als in Großunternehmen vorzufinden [10].

Zur Vollständigkeit gehört neben der Erreichung von Unternehmenszielen und der Einhaltung gesetzlicher Vorgaben auch ein angemessener Schutz vor Risiken zur IT-Sicherheit eines Unternehmens. Anti-Viren- und Firewall-Software bilden dabei eine solide Grundlage, genügen aber nicht annährend. Der effektivste Weg für einen umfassenden Schutz ist es ein Verständnis über die Auswirkungen der Risiken auf das Geschäftsmodell des Unternehmens zu erzeugen. Zudem sollten die Risiken in Geschäftsplanungen bedacht werden und falls möglich, sollten Investitionen in die Beseitigung oder zumindest Reduzierung der Chance des Auftretens der Risiken ausgeführt werden, um potenzielle Schäden zu verringern, die sie verursachen würden [11].

Die vorangegangenen Literaturbefunde zur Wirtschaftlichkeit, IT-Governance, IT-Compliance und zum IT-Risikomanagement wurden zu vier Hypothesen hinsichtlich der IT-Sicherheitseffekte für KMU zusammengefasst (siehe Tabelle 1).

Tabelle 1. Hypothesen hinsichtlich der IT-Sicherheitseffekte

Hypothesen H1 bis H4
H1. Die ökonomische Bedeutung der IT-Sicherheit hat für kleine und mittlere Unternehmen (KMU) deutlich zugenommen.
H2. IT-Governance (Organisation und Strategie der IT) ist ein wichtiger Aspekt zum Schutz der Vermögenswerte eines kleinen und mittleren Unternehmens.
H3. Die Einhaltung der gesetzlichen und unternehmensinternen Regelungen aus der IT-Compliance ist für KMU eine große Herausforderung im Bereich der IT-Infrastruktur.
H4. Das IT-Risikomanagement unterstützt bei der Identifizierung und Verringerung von Risiken in KMU.

3.2 Für KMU entwickelte IT-Sicherheitsbarrieren

Ein nicht vorhandenes Vertrauen zwischen der Geschäftsführung und IT und das limitierte Know-how des IT-Personals hinsichtlich der Digitalisierung in KMU sind auf eine ungenügende IT-Strategie zurückzuführen, die bei vielen KMU nur aus technologischen Maßnahmen (Virenschutz, Firewalls, Backups) besteht. Verantwortlich dafür ist der für KMU größere Stellenwert technologischer Maßnahmen anstatt der in der IT-Strategie ebenfalls einzubindenden organisatorischen Maßnahmen. Diese falsche Denkweise basiert auf einem Bewusstseins-/Awareness-Defizit der KMU und hat zur Folge, dass IT-Sicherheitsvorkehrungen mittels Schwachstellen- und Sicherheitsuntersuchungen vereinzelt oder gar nicht realisiert werden. Diese zielgerichteten Untersuchungen sind von entscheidender Bedeutung, um die Werte für KMU in ein passendes ökonomisches Verhältnis zu den IT-Sicherheitsinvestitionen zu stellen. Eine systematisierte Prozedur zur Untersuchung potenzieller Sicherheitslücken und deren Beseitigung durch organisatorische Maßnahmen gemäß der IT-Strategie stellen ein grundsolides Gerüst her, um die IT-Sicherheit im Unternehmen zu stärken [9]. Um eine planungsgemäße Umsetzung der IT-Strategie zu garantieren, sind IT-

Richtlinien erforderlich, die z. B. den Datenschutz, Rechenzentrumsbetrieb, die Informationssicherheit als auch das Aussuchen von individuell entwickelter und beschaffter computergestützter Informationssysteme beinhalten [12].

In IT-Richtlinien sind alle Geschäftsanweisungen bezüglich der Entwicklung und Nutzung von Anwendungen und IT-Systemen dokumentiert, die für alle Beteiligte in KMU gelten. IT-Richtlinien orientieren sich an den Anforderungen der in KMU genutzten IT-Applikationen und den darin modellbasiert beschriebenen Geschäftsprozessen. Die Beurteilung der Bedeutung der genutzten IT-Applikationen ist bei KMU dadurch beschränkt, dass die Entscheidungsfindung oft nur von einem Menschen, dem Geschäftsführer, vorgenommen wird. Eine richtliniengemäße Beurteilung der Bedeutung genutzter IT-Applikationen wird nur erreicht, wenn die betroffenen Abteilungen eingebunden werden, da nur diese die Wichtigkeit für das Unternehmen bewerten können. Demzufolge kann eine KMU-weite gültige IT-Richtlinie nur erstellt werden, wenn die Geschäftsführung in Kooperation mit ihren Abteilungen kooperiert und für alle Beschäftigten einzuhaltende IT-Sicherheitsmaßnahmen fixiert [12].

Um ein geplantes IT-Sicherheitsniveau mit den damit verknüpften IT-Richtlinien für die internen IT-Infrastrukturen in KMU zu erreichen, muss ferner eine Untersuchung potenzieller Schadens- und Angriffsszenarien mit einem IT-Sicherheitskonzept realisiert werden. Unzureichende IT-Sicherheitsmaßnahmen führen zu einer fehlerbehafteten IT-Infrastruktur mit verminderter Leistungsfähigkeit, Schäden am Ansehen und zu negativen ökonomischen Folgen. Um möglichst ein effektives IT-Sicherheitskonzept zu erstellen, sollte zuerst die IT-Struktur untersucht werden. Hierzu erfolgen eine Ist-Zustand-Bewertung und die Festlegung der Anwendungen und IT-Systeme, die das IT-Sicherheitskonzept betreffen [13-15].

Eine große Anzahl der KMU, im Gegensatz zu Großunternehmen, stehen vor beträchtlichen Barrieren bezüglich einer erfolgreichen Implementierung von IT-Rahmenwerken, vor allem wegen des Know-how-Mangels und den stark limitierten (finanziellen und personellen) Ressourcen. Die in KMU limitierte IT-Mitarbeiteranzahl führt oft dazu, dass die mit der Implementierung von IT-Rahmenwerken ordnungsgemäßen Aufgaben und Regeln nicht vollständig umgesetzt und eingeführt werden. Die limitierten Kapazitäten haben zur Folge, dass KMU zu vielen schwierigen Prozessen gegenüberstehen, welche für die IT-Rahmenwerkimplementierung ausgeführt werden müssen. Demnach bringen KMU (aktuellen) IT-Rahmenwerken wenig Akzeptanz entgegen und stellen sich nicht den Anforderungen. Um diesen Zustand zu optimieren, ist die Anpassung bzw. Verkleinerung existierender IT-Rahmenwerke oder die Entwicklung eines flexiblen, ökonomischen, und einfach zu nutzenden IT-Rahmenwerks notwendig, das speziell den Anforderungen von KMU entspricht [16].

Mitarbeitende neigen dazu viele Fehler zu machen, indem sie z. B. Passwörter vergessen, ihren Arbeitsplatz verlassen und dabei ihren Rechner anlassen oder Daten einfach nicht auf den neuesten Stand bringen. Solche Fehler gehören zur Arbeitsrealität in unserer heutigen IT-basierten Informationsgesellschaft und stellen auch in vielen KMU eine Barriere dar, die auf ein unzureichendes IT-Bewusstsein (IT-Awareness) zurückzuführen ist. Demnach ist nicht nur die Erkennung von technologischen Schwächen sondern zudem die Identifizierung von Sicherheitsstörungen durch den menschlichen Faktor entscheidend, um die IT-Systeme in KMU abzusichern. Dabei

wird das IT-Bewusstsein nicht nur durch die Bildung und Fortbildung von Mitarbeitenden in der Nutzung der IT erhöht, viel mehr zählt zudem eine Anpassung im Verhalten der Mitarbeitenden dazu, um einen wirkungsvollen Stimulus für die Sicherheit von sensiblen Unternehmensinformationen zu erzeugen. Dagegen weist das IT-Bewusstsein der Mitarbeitenden in KMU viel weniger an Wichtigkeit auf als Investitionen in Hard- und Software, um die IT-Sicherheit auszubauen. Die Gründe dafür sind z. B. Fahrlässigkeit, ein niedriges Verständnis und fehlende Compliance- oder Audit-Vorschriften hinsichtlich des IT-Bewusstseins. Der Ausgangspunkt des niedrigen Interesses für das IT-Bewusstsein liegt vor allem im mangelnden Verständnis der KMU für die potenziellen Risiken und deren potenziellen Auswirkungen [17-18].

Die vorgestellten Literaturbefunde zur IT-Strategie, IT-Richtlinie, IT-Awareness, zum IT-Sicherheitskonzept und IT-Rahmenwerk wurden zu fünf Hypothesen hinsichtlich von IT-Sicherheitsbarrieren für KMU zusammengefasst (siehe Tabelle 2).

Tabelle 2. Hypothesen hinsichtlich der IT-Sicherheitsbarrieren

Hypothesen H5 bis H9
H5. Eine unzureichende IT-Strategie macht den Geschäftsbetrieb eines KMUs verwundbar.
H6. Die IT-Richtlinie wird von der Geschäftsführung in KMU erstellt.
H7. Ein mangelndes IT-Sicherheitskonzept in KMU ist auf eine unvollständige IT-Richtlinie zurückzuführen.
H8. KMU benötigen ein IT-Rahmenwerk, das ihren speziellen Bedürfnissen entspricht.
H9. Die fehlende Förderung des IT-Bewusstseins (IT-Awareness) von Mitarbeitenden führt zur fehlerhaften Anwendung der IT-Richtlinien in KMU.

4 Methodische Vorgehensweise in der quantitativen Studie

Bei der Vorbereitung einer empirischen quantitativen Studie sind methodische Vorgehensweisen ein zentraler Bestandteil für eine wissenschaftliche Durchführung. Dafür wurden folgende Bestandteile einer empirischen quantitativen Studie beachtet: Hypothesenbildung, Fragebogendesign, Studiendurchführung, Datenanalyse und Datenpräsentation. Neben der Hypothesenbildung (siehe Abschnitt 3) ist die Ausgestaltung des Fragebogendesigns ein weiterer wichtiger Bestandteil in der Datenerhebung, um möglichst zahlreiche Teilnehmende gewinnen zu können. Zur Gestaltung des Fragebogens stehen viele Online-Umfragewerkzeuge zur Verfügung. Ausgewählt wurde letztendlich LimeSurvey. Dieses Umfragewerkzeug verfügt über ein Vorlagensystem, das eine benutzerdefinierte Anpassung des Layouts und Designs gestattet. Damit konnte die Studie öffentlich – durch eine vorherige Authentifizierung von Benutzern (Security-Token) – zugänglich gemacht werden. Der Beginn und die Dauer der Studie konnten nach der Ausformulierung der Frageblöcke mit den untergeordneten Fragen (Hypothesen H1-H9) individuell festgelegt werden. Nach dem Abschluss einer empirischen quantitativen Studie, kann die Analyse der erhobenen Daten erfolgen [19].

Das Fragebogendesign wurde nach erfolgreicher Validierung der Verständlichkeit mit Managern aus KMU ausgiebig getestet in LimeSurvey bezüglich der Filterfragen

(Bedingungen). Nach Beseitigung aller Unklarheiten und Fehler in LimeSurvey ging die Studie online und wurde im November 2016 durchgeführt. Die Studie wurde mit Hilfe eines motivierenden Einladungstexts samt Link zur Online-Umfrage in diversen sozialen und beruflichen Netzwerken veröffentlicht. Der Schwerpunkt lag dabei auf Gruppen, die sich z. B. mit Themen auseinandersetzten wie IT, IT-Sicherheit, IT-Rahmenwerken und KMU. Um eine denkbare Mehrfachteilnahme auszuschließen, musste sich jeder Teilnehmende für die Studie registrieren. Nach Ablauf der Frist haben sich 88 potenzielle Teilnehmende für die Studie zur IT-Sicherheit der Digitalisierung in KMU registriert. 76 Manager und Mitarbeitende haben erfolgreich teilgenommen.

Zur Datenanalyse wurde das Microsoft Excel Software-Add-In XLSTAT genutzt. Zuerst erfolgte eine Datenbereinigung unter Beachtung folgender Ausschlusskriterien: Entfernung aller leeren und unvollständigen Datensätze und aller Datensätze mit Bezug zu einem anderen Land außer Deutschland, Entfernung aller Nicht-KMU-Datensätze (bis 499 Beschäftigte UND bis 50 Millionen Euro Umsatz, KMU-Definition des IfM Bonn [20]). Von den ursprünglich 76 Teilnehmenden sind nach der Datenbereinigung 46 Teilnehmende aus KMU in Deutschland übrig geblieben. In dieser explorativen quantitativen Datenanalyse werden für die Datenpräsentation Boxplots genutzt, um die Zustimmung bzw. Ablehnung hinsichtlich einzelner Hypothesen bildlich aufzuzeigen.

Von den insgesamt 46 verbleibenden Befragten kam etwa die Hälfte der Teilnehmer aus Niedersachsen (50,00%) gefolgt von Nordrhein-Westfalen (19,57%) und Hamburg (8,70%). Die verbleibenden Bundesländer waren vereinzelt oder nicht vertreten. Daher kann von keiner statistischen Signifikanz der Datenanalyse für KMU in Deutschland gesprochen werden. Für Niedersachsen können die Daten jedoch als signifikant gelten. Hinsichtlich der Branchen, in denen die KMU positioniert waren, arbeitete ein Großteil der hierin Beschäftigten in der Beratungsbranche (34,78%) und einer anderen Branche (65,22%) als jene, die in der Studie abgefragt wurden. Bei der Frage nach der beruflichen Stellung antworteten die meisten Befragten oberste Managementebene (36,96%) und mittlere Managementebene (26,09%). Der Rest verteilte sich mit 17,39% auf die unterste Managementebene und den Mitarbeitenden, denn 19,56% hatten keine Managementfunktion. Aufgrund der Verteilung der Antworten bezüglich der Branche und des Berufsstatus ist es nicht erstaunlich, dass die meisten Befragten ihren Aufgabenbereich in der Geschäftsführung (30,43%) und im Kundenmanagement (26,09%) hatten. Andere Befragte waren im IT-Management (8,70%), Marketing und Vertrieb (8,70%), in der Revision (8,70%), im Finanzmanagement und Controlling (4,35%) oder in einem sonstigen Aufgabenbereich (13,03%) tätig.

5 Empirische Hypothesenevaluation

5.1 Für KMU in Deutschland wichtige IT-Sicherheitseffekte

Aufgrund der genutzten Likert-Skala (7 = stimme voll und ganz zu; 4 = neutral; 1 = stimme überhaupt nicht zu) ist bei allen vier Hypothesen hinsichtlich der IT-Sicherheitseffekte für KMU in Deutschland eine deutliche Tendenz zur Zustimmung gegeben (siehe Abbildung 1 und ergänzend die Tabellen 1 und 3).

Tabelle 3. Deskriptive Statistiken bezogen auf die Boxplots der IT-Sicherheitseffekte

Statistik	*Ökonomische Bedeutung für KMU*	*IT-Governance*	*IT-Compliance*	*IT-Risiko-management*
Minimum	2,000	3,000	2,000	3,000
1. Quartil	5,000	5,000	5,000	5,000
Median	6,000	6,000	6,000	6,000
3. Quartil	7,000	7,000	7,000	6,750
Maximum	7,000	7,000	7,000	7,000
Mittelwert	5,913	5,696	5,739	5,783
Varianz	1,459	1,328	1,664	1,018

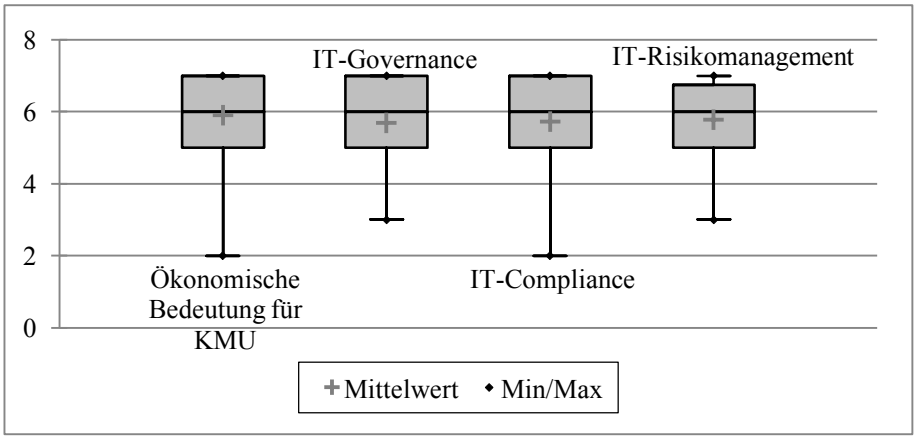

Abbildung 1. Boxplots der IT-Sicherheitseffekte

Der Hypothese H1 wird eindeutig zugestimmt. Die ökonomische Bedeutung der IT-Sicherheit scheint für kleine und mittlere Unternehmen (KMU) in Deutschland deutlich zugenommen zu haben. *Der Hypothese H2 wird eindeutig zugestimmt*. Die IT-Governance inklusive der Organisation und Strategie der IT wird als ein wichtiger Aspekt zum Schutz der Vermögenswerte eines kleinen und mittleren Unternehmens in Deutschland wahrgenommen. *Der Hypothese H3 wird eindeutig zugestimmt*. Die Einhaltung der gesetzlichen und unternehmensinternen Regelungen aus der IT-Compliance erscheint für kleine und mittlere Unternehmen in Deutschland eine große Herausforderung im Bereich der IT-Infrastruktur zu sein. *Der Hypothese H4 wird eindeutig zugestimmt*. Das IT-Risikomanagement unterstützt bei der Identifizierung und Verringerung von Risiken in kleinen und mittleren Unternehmens in Deutschland.

5.2 Für KMU in Deutschland wichtige IT-Sicherheitsbarrieren

Aufgrund der genutzten Likert-Skala ist bei allen fünf Hypothesen hinsichtlich der IT-Sicherheitsbarrieren für KMU in Deutschland eine unterschiedliche Tendenz zur Zustimmung gegeben (siehe Abbildung 2 und ergänzend die Tabellen 2 und 4).

Tabelle 4. Deskriptive Statistiken bezogen auf die Boxplots der IT-Sicherheitsbarrieren

Statistik	*IT-Strategie*	*IT-Richtlinie*	*IT-Sicherheits-konzept*	*IT-Rahmenwerk*	*IT-Bewusstsein*
Minimum	1,000	1,000	1,000	2,000	2,000
1. Quartil	5,000	3,000	4,000	5,000	5,000
Median	5,000	4,500	5,000	6,000	6,000
3. Quartil	6,000	6,000	5,000	7,000	7,000
Maximum	7,000	7,000	7,000	7,000	7,000
Mittelwert	5,261	4,087	4,435	5,848	5,826
Varianz	2,064	3,592	2,251	1,465	1,791

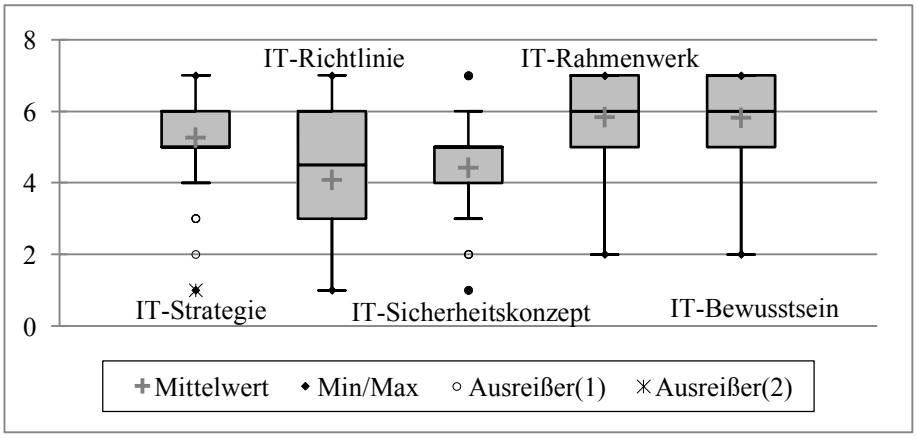

Abbildung 2. Boxplots der IT-Sicherheitsbarrieren

Der Hypothese H5 wird noch zugestimmt, obwohl Ausreißer in den Daten bestehen. Eine unzureichende IT-Strategie kann den Geschäftsbetrieb eines kleinen und mittleren Unternehmens in Deutschland verwundbar machen. *Der Hypothese H6 wird nicht eindeutig zugestimmt*. Die IT-Richtlinie kann von der Geschäftsführung in kleinen und mittleren Unternehmens in Deutschland erstellt werden, jedoch auch von anderen Funktionen und Instanzen. *Der Hypothese H7 wird nicht eindeutig zugestimmt und es bestehen Ausreißer in den Daten*. Ein mangelndes IT-Sicherheitskonzept in kleinen und mittleren Unternehmen in Deutschland kann auf eine unvollständige IT-Richtlinie zurückzuführen sein, jedoch können auch andere wichtige Ursachen vermutet werden. *Der Hypothese H8 wird eindeutig zugestimmt*. Kleine und mittlere Unternehmen in Deutschland benötigen ein (angepasstes oder zu entwickelndes) IT-Rahmenwerk, das ihren speziellen Bedürfnissen entspricht. *Der Hypothese H9 wird eindeutig zugestimmt*. Die fehlende Förderung des IT-Bewusstseins (IT-Awareness) von Mitarbeitenden führt zur fehlerhaften Anwendung der IT-Richtlinien in kleinen und mittleren Unternehmen in Deutschland. Es kann daher angenommen werden, dass in KMU in Deutschland keine gezielte Förderung des IT-Bewusstseins stattfindet und entsprechende IT-Richtlinien falsch angewandt werden.

6 Diskussion der IT-Sicherheit der Digitalisierung in KMU

Aus der empirischen Hypothesenevaluation (siehe Abschnitt 5) kann die Schlussfolgerung gezogen werden, dass KMU in Deutschland der IT-Sicherheit der Digitalisierung eine hohe ökonomische Bedeutung zuordnen und sich nicht vor Veränderungen durch die Digitalisierung hinter Großunternehmen verbergen. Zudem ist den Studienteilnehmenden klar, dass der Stellenwert einer gut implementierten IT-Governance und ein ordnungsgemäßes IT-Risikomanagement wichtige Bestandteile sind, um die eigenen angestrebten Ziele der IT-Sicherheit der Digitalisierung zu erreichen und Vermögenswerte vor digitaler Wirtschaftskriminalität abzusichern.

Die Studienteilnehmenden stimmen zu, dass Schwierigkeiten bestehen, interne Regelungen und gesetzliche Vorgaben ordnungsgemäß umzusetzen. Gründe dafür könnten hinsichtlich der gesetzlichen Vorgaben die kaum abschreckenden gesetzlichen Sanktionierungen in Verbindung mit dem niedrigen Verständnis der Geschäftsführung, große Investitionen im Gebiet der IT-Sicherheit der Digitalisierung durchzuführen, sein. Allgemein besteht ein Schwerpunkt auf den Kosten anstelle einer langfristigen Kostenverringerung aufgrund sicherer und stabiler Geschäftsprozesse, um negative geschäftliche und gesellschaftliche Reaktionen (bspw. durch sensiblen Datenverlust) aufgrund einer ungenügenden IT-Sicherheit im KMU zu verhindern. Folglich sind vom mangelnden Verständnis der Geschäftsführer zudem interne Regelungen involviert, die durch die Geschäftsführung vorgelebt werden sollten, um die Förderung der IT-Sicherheit der Digitalisierung zu bewerkstelligen.

Die Hypothesenevaluation gibt Aufschluss darüber, dass KMU in Deutschland den Standpunkt vertreten, dass ihre IT-Strategie zur Stabilität ihres Geschäftsbetriebs beitragen kann. Insbesondere sollten sich KMU in Deutschland hinsichtlich einer ordnungsgemäßen IT-Strategie mit ihren limitierten Ressourcen den zu sehr einseitigen technologischen Schwerpunkt (bspw. Virenschutz) verringern und zusätzlich verstärkt die organisatorischen Infrastrukturen involvieren. Zudem sollte die organisatorische Planung, Koordination und Kontrolle dazu beitragen, mit intelligenten Entscheidungen (bspw. Schwachstellenanalysen) und gezielten Investitionen (bspw. IT-Schulungen) das nötige Know-how und Vertrauen aufzubauen, um kontinuierlich die IT-Sicherheit der Digitalisierung zu stärken. Hinsichtlich der Erstellung von IT-Richtlinien bestand keine klare Zustimmung, da nur mit geringer Tendenz dahingehend zugestimmt wurde, dass IT-Richtlinien lediglich von der Geschäftsführung erstellt werden. Diese Tendenz kann sowohl positiv als auch negativ interpretiert werden. Auf der einen Seite wurde aufgezeigt, dass nicht alle KMU in Deutschland sich darüber bewusst sind, dass IT-Richtlinien auch durch zusätzliche Instanzen erstellt werden können, wohingegen höchstwahrscheinlich andere Studienteilnehmende es aus der Praxis nicht anders kennen oder nicht die erforderlichen Ressourcen aufbringen können, um IT-Richtlinien mit weiteren Instanzen auszuarbeiten. Daher sollten – ohne Abweichungen – alle KMU in Deutschland die Strategie verfolgen, bei der Ausgestaltung der IT-Richtlinien die betroffenen Abteilungen zu involvieren, da sich IT-Richtlinien z. B. an den Anforderungen der genutzten Applikationen und IT-Systemen sowie den damit verknüpften Geschäftsprozessen orientieren. Nur durch eine effektive Kooperation der einzelnen Fachbereiche auf Basis ihres Wissens, die im Geschäftsalltag sich mit den

Applikationen, IT-Systemen und Geschäftsprozessen auseinandersetzen, können IT-Richtlinien erstellt werden, welche die IT-Sicherheit der Digitalisierung gewährleisten.

Ein vergleichbares Bild entstand beim IT-Sicherheitskonzept, da auch bei dieser Hypothese nur mit geringer Tendenz zugestimmt wurde, dass ein mangelndes IT-Sicherheitskonzept auf eine unvollständige IT-Richtlinie zurückzuführen sei. Hier baut sich ebenso, wie bei den IT-Richtlinien, die Ansicht auf, dass die limitierten Ressourcen einen hohen Einfluss auf dieses nicht eindeutige Ergebnis haben könnten. Insbesondere wird durch das limitiert vorhandene Know-how die Beurteilung von Gefahrenbereichen aufgrund von Schwächen im IT-Betrieb oft unterbewertet und kann daher zu fehlerbehafteten IT-Sicherheitskonzepten und damit verbundenen IT-Sicherheitsmaßnahmen führen. Limitiertes Know-how im eigentlichen Sinne, dass lediglich eine Instanz entscheidungsbefugt ist, wie das IT-Sicherheitskonzept aufgebaut werden soll, ohne die Kooperation mit den betroffenen Fachbereichen zu suchen, die eine bessere Perspektive auf das haben, das diese im Geschäftsalltag bewältigen. Insbesondere die Fachbereiche sind dazu befähigt aus vielfältigen Kontexten betreffs ihres geschäftlichen Handelns auf Gefahren oder Schwächen aufmerksam zu werden, die für außenstehende Instanzen (bspw. Geschäftsführung) vorab nicht offenkundig sind. Speziell das IT-Sicherheitskonzept ist stark mit der IT-Richtlinie verknüpft, da mit IT-Richtlinien Bereiche, Anwendungen, Systeme und Prozesse fixiert werden, die für den Geschäftsbetrieb von großer Bedeutung sind. Folglich kann ein mangelndes IT-Sicherheitskonzept in KMU in Deutschland durchaus auf eine unvollständige IT-Richtlinie zurückzuführen sein.

Hinsichtlich der IT-Rahmenwerke wurde die Hypothese bestätigt, da ein Großteil der KMU in Deutschland das Bedürfnis nach einem für sie angepassten oder entwickelten IT-Rahmenwerk verspürt. Dies ist insbesondere zurückzuführen auf große Schwierigkeiten mit bereits etablierten IT-Rahmenwerken, wie bspw. der ISO 2700x, die mit ihrer extremen Anzahl an Anforderungen in keinem Verhältnis zu der Kapazität eines KMU stehen. Daher haben KMU in Deutschland nicht die nötige Akzeptanz, diese Schwierigkeiten zu meistern, sodass erleichternde Bedingungen erforderlich werden mit für KMU flexibleren, ökonomischeren und einfacheren IT-Rahmenwerken.

Auch bezüglich des IT-Bewusstseins entstand der Eindruck, dass für KMU in Deutschland mit der IT-Strategie, IT-Richtlinie, dem IT-Sicherheitskonzept und IT-Rahmenwerk nur eine erste Grundlage entsteht, wenn das IT-Bewusstsein in KMU nicht ordnungsgemäß gefördert wird. Entsprechendes IT-Bewusstsein umfasst nicht nur eine Förderung der Mitarbeitenden sondern bestenfalls eine Verhaltensanpassung, sodass jeder Mitarbeitende auf unvorhergesehene Situationen richtig reagieren kann. IT-Bewusstsein sollte deutlich weiter oben in der Geschäftsführung ansetzen, hier wird das IT-Bewusstsein für das ganze KMU vorgelebt. Insbesondere sollte die Geschäftsführung ein Verständnis entwickeln für potenzielle Risiken und potenzielle Folgen und darf die limitierten Ressourcen (bspw. IT-Budget und Zeitaufwand) nicht als Vorwand nutzen, die IT-Sicherheit der Digitalisierung zu vernachlässigen.

Referenzen

1. Householder, A., Houle, K., Dougherty, C.: Computer attack trends challenge Internet security. IEEE Computer 35(4), 5–7 (2002)

2. Tawileh, A., Hilton, J., McIntosh, S.: Managing Information Security in Small and Medium Sized Enterprises: A Holistic Approach. In: Pohlmann, N., Reimer, H., Schneider, W. (Hrsg.) ISSE/SECURE 2007 Securing Electronic Business Processes. S. 331–339. Friedr. Vieweg & Sohn Verlag, GWV Fachverlage GmbH, Wiesbaden (2007)
3. Cavusoglu, H., Mishra, B., Raghunathan, S.: The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. International Journal of Electronic Commerce, 69–104 (2002)
4. Ashish, G., Curits, J., Halper, H.: Quantifying the financial impact of IT security breaches. Information Management & Computer Security 11(2), 74–83 (2003)
5. Groner, R., Brune, P.: Towards an Empirical Examination of IT Security Infrastructures in SME, Secure IT Systems 7617, 73–88 (2012)
6. Barlette, Y., Fomin, V.V.: Exploring the suitability of IS security management standards for SMEs. In: Hawaii International Conference on System Sciences (HICSS), pp. 1-10. Waikoloa, Big Island, Hawaii (2008)
7. Kluge, D., Sambasivam, S.: Formal Information Security Standards in German Medium Enterprises. Proc CONISAR 1, 1–12 (2008)
8. Leyh, C., Bley, K.: Digitalisierung: Chance oder Risiko für den deutschen Mittelstand? – Eine Studie ausgewählter Unternehmen. HMD Praxis der Wirtschaftsinformatik 53, 29–41 (2016)
9. Sächsisches Staatsministerium für Wirtschaft, Arbeit und Verkehr, http://www.smwa.sachsen.de/download/it-sicherheit_sachsen_endbericht.pdf (Aufgerufen: 09.09.2017)
10. Schäfer, G., Strolz, G., Hertweck, D.: IT-Compliance im Mittelstand. HMD Praxis der Wirtschaftsinformatik 45(5), 69–77 (2014)
11. Rees, J.: Information security for small and medium-sized business. Computer Fraud & Security, 18–19 (2010)
12. Bartelt, J., Rieger, B.: IT-Sicherheit im Mittelstand. In: Fahrenschon, G., et al. (Hrsg.) Mittelstand – Motor und Zukunft der deutschen Wirtschaft. S. 557–569. Springer Fachmedien, Wiesbaden (2015)
13. Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/it-grundschutz_profil_klein.pdf?__blob=publicationFile (Aufgerufen: 09.09.2017)
14. Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Doku/studie_ueberblick-standards.pdf?__blob=publicationFile&v=1 (Aufgerufen: 09.09.2017)
15. Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/KMU/Studie_IT-Sicherheit_KMU.pdf;jsessionid=170B98EEDC9C3517E5079802636EE736.1_cid351?__blob=publicationFile&v=2 (Aufgerufen: 09.09.2017)
16. Ayat, M., Masrom, M., Sahibuddin, S., Sharifi, M.: Issues in Implementing IT Governance in Small and Medium Enterprises. In: International Conference on Intelligent Systems, Modelling and Simulation, S. 197–201. (2011)
17. Williams, P.: What Does Security Culture Look Like For Small Organizations? In: Security Research Institute Conferences, pp. 48-54. Edith Cowan University (2009)
18. Goucher, W.: Do SMEs have the right attitude to security?. Computer Fraud & Security, 1–3 (2011)
19. Lederer, B.: Quantitative Erhebungsmethoden. In: Hug, T., Poscheschnik, G. (Hrsg.) Empirisch Forschen. S. 100-132. UVK Verlagsgesellschaft, Konstanz (2010)
20. Institut für Mittelstandsforschung Bonn, http://www.ifm-bonn.org/definitionen/kmu-definition-des-ifm-bonn/ (Aufgerufen: 09.09.2017)