Cybersicherheit als Führungsaufgabe in Schweizer KMU

5

Herausforderungen und Chancen im Zuge der Digitalisierung

Dominique Adrian Meier und Daniel Burda

Cybersicherheit gewinnt im Kontext der Digitalisierung auch in KMU zunehmend an Wichtigkeit und verdient die Aufmerksamkeit von Führungskräften und Entscheidungsträgern

Zusammenfassung

Durch die digitale Transformation gewinnt Cybersicherheit für kleine und mittlere Unternehmen (KMU) zunehmend an Bedeutung und rückt damit auch auf die Tagesordnung der Unternehmensleitung. Diverse Studien zeigen, dass KMU Cybersicherheit als relevantes Handlungsfeld identifizieren, gleichzeitig aber nicht genügend adressieren. Bestehende Forschung liefert für dieses Verhalten keine Erklärung. Dieser Beitrag widmet sich der Untersuchung dieses Phänomens, welches im Beitrag als „Security Paradox" definiert wird. Dabei werden dessen Ursachen aufgezeigt und praxisrelevante Empfehlungen für Führungskräfte und Entscheidungsträger im Umgang mit der Herausforderung „Cybersicherheit im Zuge der Digitalisierung" abgegeben.

D. A. Meier (✉)
Bülach, Schweiz
E-Mail: me@dominiquemeier.ch

D. Burda
Berner Fachhochschule Wirtschaft, Bern, Schweiz
E-Mail: daniel.burda@bfh.ch

J. Schellinger et al. (Hrsg.), *Digitale Transformation und Unternehmensführung*,
https://doi.org/10.1007/978-3-658-26960-9_5

5.1 Einleitung

Die digitale Transformation stellt kleine und mittlere Unternehmen (KMU) sowie deren IT vor neue große Herausforderungen. Ein zentrales Thema in diesem Zusammenhang stellt die Cybersicherheit[1] dar, die auch in KMU zunehmend an Bedeutung gewinnt und auf die Tagesordnung der Unternehmensleitung rückt. Gemäß EY (2018) rechnen 41 % der im Rahmen des Unternehmensbarometers 2018 befragten Schweizer Unternehmen mit Schwierigkeiten bei der Sicherung ihrer IT-Infrastruktur. Ferner zeigen Studien wie die der KPMG (2017, S. 38) sowie andererseits Berichterstattungen zu Cybersicherheitsvorfällen bei Schweizer KMU (Inside-IT 2018), dass Cybersicherheit ein aktuelles Kernthema für Schweizer Unternehmen darstellt. Rund 88 % der im Rahmen der Studie befragten Schweizer Unternehmen wurden im vergangenen Jahr Ziel von Cyberangriffen. Auch eine Studie der Zürich Versicherungs-Gesellschaft (2016, S. 1) identifiziert Cyberkriminalität als relevantes Schlüsselrisiko für Schweizer KMU. Untermauert werden diese Aussagen durch Entwicklungen am Sicherheitsdienstleistermarkt in der Schweiz. So hat 2017 ein Zusammenschluss von verschiedenen IT- und Security-Dienstleistern stattgefunden, die sich drauf spezialisieren, Security-Dienstleistungen für Schweizer KMU zu erbringen (Inside-Channels 2017).

Andererseits zeigen Studien, wie die der Zürich Versicherungs-Gesellschaft (2016) auf, dass trotz des Bewusstseins für Cyberkriminalität in KMU lediglich 2,5 % der befragten Unternehmen über einen ausreichenden Schutz verfügen. Aufgrund der erheblichen Differenz zwischen Risikobewusstsein und Ergreifen von konkreten Maßnahmen leiten die Autoren der Studie ab, dass die Mehrheit der KMU mit der Thematik Informationssicherheit überfordert ist. Dass es Schweizer KMU im Umgang mit dem Thema Informationssicherheit an Wissen fehlt, bestätigen auch Hirschi und Portmann (2017, S. 8–10). Sie zeigen auf, dass lediglich 46 % der befragten KMU Standards bei der Umsetzung von Informationssicherheit berücksichtigen. In derselben Studie gaben 74 % der befragten KMU an, kein Informationssicherheitsmanagementsystem (ISMS) einzusetzen, wodurch Informationssicherheit nicht systematisch adressiert wird. Dass Cybersicherheit durch KMU zwar als relevantes Handlungsfeld identifiziert, gleichzeitig aber nicht genügend adressiert wird, zeigen auch die Studien von Renaud (2016) und

[1]In Anlehnung an den allgemeinen Sprachgebrauch und wissenschaftliche Veröffentlichungen (vgl. Eckert 2017; Klipper 2015) werden die Begriffe „IT-Sicherheit“ und „Informationssicherheit“ in der vorliegenden Arbeit unter dem Begriff „Cybersicherheit“ zusammengefasst, wobei Cybersicherheit eine inhaltliche Erweiterung des Begriffs Informationssicherheit und dieser wiederum eine inhaltliche Erweiterung des Begriffs IT-Sicherheit darstellt. Diese eingeführte Terminologie wird bestärkt durch Erkenntnisse aus bestehenden Studien wie beispielsweise der von gfs-zürich (2017) oder der von Hirschi und Portmann (2017). Aus den Studien geht hervor, dass KMU in der Regel keine Unterscheidung zwischen den Begriffen vornehmen. So wird in der vorliegenden Analyse ausschließlich der übergeordnete Begriff „Cybersicherheit“ verwendet, der Informationssicherheit und IT-Sicherheit mit einschließt.

gfs-zürich (2017). Dieses Phänomen wurde ansatzweise von Straub (1990) bereits zu Beginn der 1990er-Jahre beschrieben:

> Over the last several decades, managers have become aware that information and information systems are critical organizational resources. It is reasonable to expect therefore, that they would consider the security of information to be a crucial activity. Curiously, this is not the case (Straub 1990, S. 255).

Auch eine Studie des Bundesamts für Sicherheit in der Informationstechnik (BSI 2011, S. 99) hinsichtlich des IT-Sicherheitsniveaus von KMU in Deutschland kommt zu einem ähnlichen Schluss – das Bewusstsein für das Thema ist sehr ausgeprägt, der Umsetzungsgrad von Maßnahmen sowie die Etablierung eines systematischen IT-Sicherheitsmanagement lassen jedoch zu wünschen übrig.

Bestehende Forschung liefert aktuell keine Erklärung bezüglich dieser Intentionsverhaltenslücke. Die vorliegende Untersuchung setzt an dieser Forschungslücke an und untersucht mithilfe eines qualitativen Forschungsansatzes die Ursachen für dieses Phänomen bei Schweizer KMU im Bereich Cybersicherheit. Vor diesem Hintergrund lassen sich folgende Forschungsfragen als Ausgangspunkt der Analyse formulieren:

- Forschungsfrage 1: Kann eine Intentionsverhaltenslücke (IVL) hinsichtlich der Cybersicherheit bei Schweizer KMU nachgewiesen werden?
- Forschungsfrage 2: Welche Ursachen sind ausschlaggebend für das Vorhandensein der IVL hinsichtlich Cybersicherheit in Schweizer KMU?

Durch die Beantwortung obiger Forschungsfragen soll die vorliegende Analyse eine Hilfestellung für Führungskräfte von Schweizer KMU bei der Adressierung von Cybersicherheit bieten und einen bedeutenden Meilenstein in dem noch jungen Themengebiet Cybersicherheit bei Schweizer KMU darstellen.

5.2 Forschungsmodell

Für die vorliegende Analyse wurde ein Forschungsmodell (siehe Abb. 5.1) auf Basis einer umfassenden Literaturrecherche erarbeitet, das gemäß vorhergehender Untersuchungen Determinanten umfasst, die entscheidend dafür sind, ob eine Organisation adäquate Cybersicherheitsmaßnahmen ergreift. Im Rahmen der vorliegenden Analyse werden diese Determinanten basierend auf empirischen Daten aus den durchgeführten Fallstudien analysiert. So sollen das Vorhandensein und die Ursache der Intentionsverhaltenslücke, hinsichtlich Cybersicherheit bei Schweizer KMU, nachgewiesen werden.

Das für die vorliegende Analyse erarbeitete Forschungsmodell orientiert sich dabei primär an den Forschungsmodellen von Browne et al. (2015), Liang und Xue (2009) sowie Renaud (2016). Zur Erarbeitung des Forschungsmodell wurden zudem die folgenden Theorien und Modelle analysiert und als Determinanten im Forschungsmodell verankert:

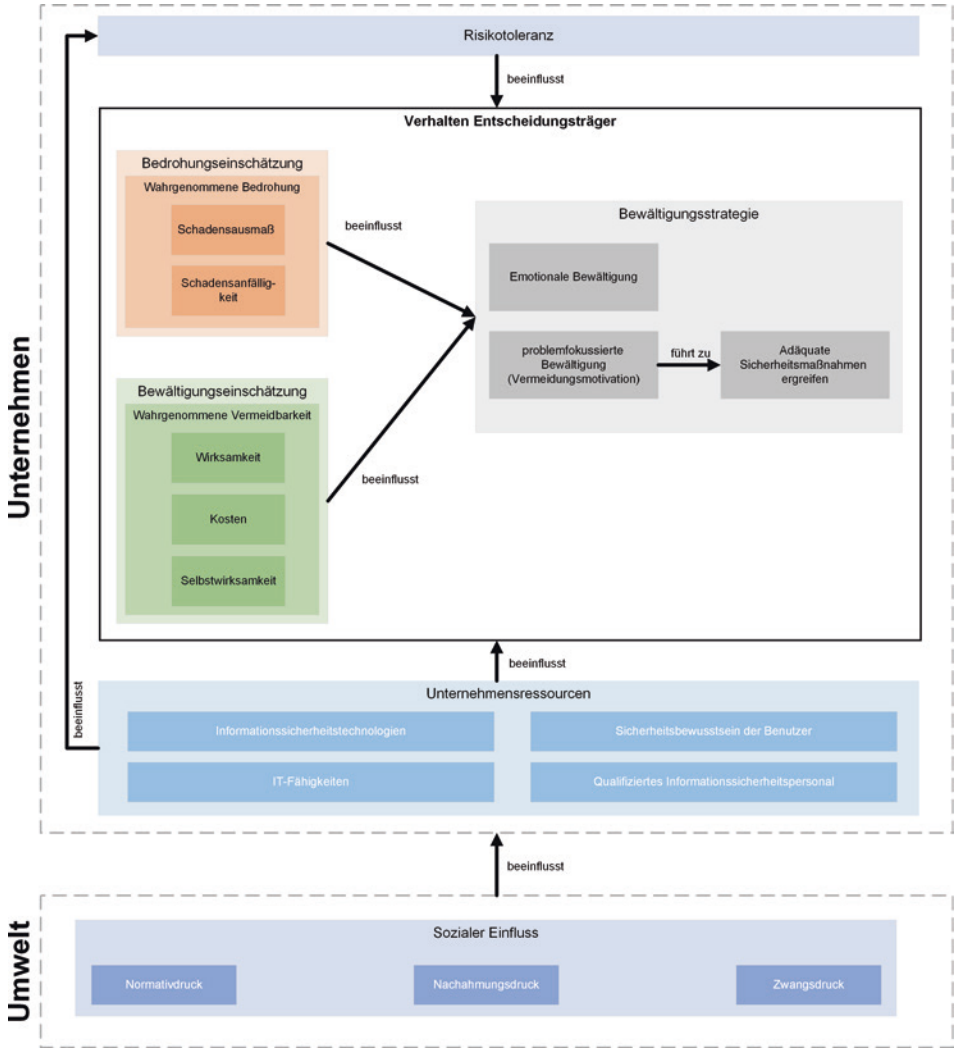

Abb. 5.1 Forschungsmodell. (Eigene Darstellung)

A. Cybersicherheit Ressourcen

Damit ein KMU in der Lage ist, Cybersicherheit adäquat zu adressieren, benötigt es bestimmte Unternehmensressourcen (Cavusoglu et al. 2015, S. 385). Cavusoglu et al. identifizierten basierend auf dem Unternehmensressourcenmodell von Grant (2010, S. 127) vier unterschiedliche aber zusammenhängende Dimensionen von Informationssicherheitskontrollressourcen, die für das Umsetzen von Informationssicherheitskontrollen essenziell sind:

a) Informationssicherheitstechnologien (präventive und detektivische technische Lösungen zur Behebung von Schwachstellen innerhalb der IT-Infrastruktur),
b) qualifiziertes Informationssicherheitspersonal (Ausmaß an professionellen Mitarbeitenden zur Definition, Ausführung und Pflegen des ISMS),
c) Sicherheitsbewusstsein der Benutzer (Ausmaß des Sensibilisierungsgrads hinsichtlich Cybersicherheit der Mitarbeitenden),
d) IT-Fähigkeiten (Ausmaß an professionellen IT-Mitarbeitenden und vorhandenes IT Wissen).

B. Risikotoleranz

Browne et al. (2015, S. 35) argumentieren, dass die Risikotoleranz eines KMU einen Einfluss auf den Umgang mit wahrgenommenen Cybersicherheit-Bedrohungen hat. Sie gehen davon aus, dass die Risikotoleranz die Vermeidungsmotivation mindert und gleichzeitig eine emotionale Bewältigung von Bedrohungen fördert. Zudem folgern sie aus der von ihnen untersuchten Fachliteratur, dass die Risikotoleranz eines Unternehmens in starker Abhängigkeit zu dessen Herkunft, Größe und Reifegrad steht. Dies ist ihrer Ansicht nach ein Indikator dafür, dass sich die Risikotoleranz von KMU zu KMU stark unterscheidet und deshalb als Determinante für das Umsetzen von adäquaten Sicherheitsmaßnahmen infrage kommt. Im Forschungsmodell zur vorliegenden Analyse wird die Risikotoleranz deshalb ebenfalls als potenzielle Determinante eingeführt.

C. Verhaltensmodelle (Verhalten von Führungskräften)

Die für die Erarbeitung des Forschungsmodells analysierten sozialpsychologischen Verhaltensmodelle beziehen sich jeweils auf das Verhalten von Individuen (vgl. Ajzen 1985; Rogers 1975; Kelman 2006; Liang und Xue 2009). Wie Browne et al. (2015, S. 34) in ihrer Forschungsarbeit aufzeigen, besteht im Kontext von KMU jedoch eine gewisse Legitimität, Organisationsverhalten zu anthropomorphisieren. Grund dafür ist die bei KMU bestehende Abhängigkeit zu dominanten Einzelpersonen. In der vorliegenden Analyse werden deshalb die nachfolgend beschriebenen Verhaltensmodelle auf das Organisationsverhalten in Bezug auf die Vermeidung von Cybersicherheitsbedrohungen und das Umsetzen von Cybersicherheitsmaßnahmen übertragen.

a) Protection Motivation Theory

Um Cybersicherheitsbedrohungen zu vermeiden, müssen Unternehmen eine Reihe von Beurteilungs- und Bewältigungsschritten hinsichtlich einer spezifischen Bedrohungslage vornehmen (Browne et al. 2015, S. 34). Die von Rogers (1975) entwickelte Theorie der Schutzmotivation (engl. Protection Motivation Theory) beschreibt, wie von einem Individuum erlebte Bedrohungen dazu führen, dass es sein Verhalten ändern will. Gemäß der Theorie führt der Erhalt von überzeugenden Informationen über die unerwünschten Folgen eines bestimmten Ereignisses zu zwei Beurteilungsprozessen, von denen die Verhaltensintention des Individuums abhängt:

1. Bedrohungseinschätzung – Dabei wird beurteilt, welchen Schweregrad eine Bedrohung aufweist und wie die eigene Verwundbarkeit wahrgenommen wird.
2. Bewältigungseinschätzung – Dabei wird beurteilt, ob ein Individuum selbst in der Lage ist, Maßnahmen gegen eine Bedrohung zu ergreifen (Selbstwirksamkeitserwartung[2]), ob das Umsetzen von Maßnahmen tatsächlich gegen die Bedrohung schützt (Handlungsergebniserwartung) und wie viel die Umsetzung der Maßnahmen kostet.

   Wird eine Bedrohung von einem Individuum als hoch eingeschätzt und die Bewältigungseinschätzung fällt positiv aus, kommt es beim Individuum zu einer Verhaltensintention, die der Bedrohung entgegenwirkt (Rogers, 1975). Dass die Wahrnehmung einer Cybersicherheitsbedrohung ausschlaggebend dafür ist, wie stark Individuen motiviert sind, diese zu verhindern, zeigte eine Studie von Workman, Bommer und Straub (2008, S. 2813–2814). Sie stellten fest, dass Sicherheitsmaßnahmen mit größerer Konsequenz umgesetzt werden, wenn eine Bedrohung als schwerer empfunden wird, als wenn eine Bedrohung als harmlos angesehen wird. Eine weitere Erkenntnis der Studie war, dass bei Individuen ein gegensätzliches Verhalten eintritt, wenn der Grad an Bedrohungsmeldungen ein chronisches Ausmaß annimmt und diese in der Folge keine Maßnahmen umsetzen. Dies ist vermutlich auf eine reduzierte Selbstwirksamkeitserwartung und reduzierte Handlungsergebniserwartung, bedingt durch eine Überhäufung mit Bedrohungsmeldungen, zurückzuführen.

b. Model of Social Influence

   Der soziale Einfluss stellt eine bedeutende Variable in jedem Verhaltensmodell dar (vgl. Burnkrant und Cousineau 1975; Deutsch und Gerard 1955). So wurde die Bedeutung von sozialem Einfluss auf das Verhalten von Individuen im Kontext von IT- und Informationssystemen bereits breit erforscht und bewiesen (vgl. Pavlou und Fygenson 2006; Taylor und Todd 1995; Venkatesh und Davis 2000; Venkatesh et al. 2003). Wie in den Forschungsmodellen von Browne et al. (2015) und Liang und Xue (2009) wird der soziale Einfluss auch im Forschungsmodell der vorliegenden Analyse als Determinante eingeführt. Basierend auf Erkenntnissen bestehender Forschung (vgl. Cavusoglu et al. 2015; Kelman 2006; Liang und Xue 2009) werden im vorliegenden Forschungsmodell die folgenden Arten von sozialem Einfluss unterschieden:

[2]Es wird davon ausgegangen, dass die Ausführung eines Verhaltens umso wahrscheinlicher ist, je größer die subjektive Überzeugung ist, das Verhalten zu bestimmen, das heißt je mehr ein Individuum der Ansicht ist, über genügend Fähigkeiten, Fertigkeiten oder Ressourcen zu verfügen, um das Verhalten zu realisieren (Ajzen 1985). Diese subjektive Überzeugung wird auch als Selbstwirksamkeitserwartung (engl. Perceived Self Efficacy) bezeichnet. Hohmann und Schwarzer (2009, S. 67) weisen in ihrem Werk darauf hin, dass Selbstwirksamkeitserwartung von den Fähigkeiten eines Individuums unterschieden werden muss, da geringe Fähigkeiten durchaus mit hoher Selbstwirksamkeitserwartung einhergehen können oder umgekehrt.

1. Normativdruck (Normativer Einfluss)
   Das soziale Umfeld eines Individuums generiert gemäß Kelman (2006) normativen Einfluss auf den drei Ebenen Compliance (das Bedürfnis eines Individuums nach Akzeptanz und Belohnung oder Angst vor Bestrafung), Internalisierung (das Entwickeln einer Übereinstimmung zwischen den Werten und Zielen eines Individuums und denen einer Gruppe) und Identifikation (die selbstbestimmte Beziehung eines Individuums zu einem anderen Individuum oder einer Gruppe. Als Konsequenz aus dieser Beziehung verhält sich ein Individuum entsprechend den Werten und Zielen seines sozialen Umfelds).
2. Nachahmungsdruck
   Unter Nachahmungsdruck verstehen Cavusoglu et al. (2015, S. 387–388) den Druck, den Organisationen spüren, wenn erfolgreiche Praktiken bei Konkurrenten beobachtet werden. Diese Beobachtung führt zu einem Nachahmungsdruck, die als erfolgreich beobachteten Maßnahmen in der eigenen Organisation umzusetzen.
3. Zwangsdruck
   Nach Cavusoglu et al. (2015, S. 388) entspricht Zwangsdruck dem Einfluss, den Regulierungsbehörden direkt auf bestimmte Organisationen und Branchen ausüben. Durch diesen Einfluss entsteht ein Zwangsdruck für Organisationen, gesellschaftliche und politische Erwartungen zu erfüllen.
   Basierend auf den empirischen Daten aus ihrer Forschung konnten Cavusoglu et al. (2015, S. 396) beweisen, dass normativer und zwanghafter Druck einen starken direkten Einfluss auf das Sicherheitsbedürfnis und die Informationssicherheitskontrollressourcen einer Organisation haben. Ein starker Einfluss durch Nachahmungsdruck konnte jedoch nicht nachgewiesen werden. Cavusoglu et al. schlussfolgern daraus, dass Organisationen nicht dazu neigen, zu glauben, dass erfolgreiche Sicherheitsmaßnahmen ihrer Konkurrenten auch ihre Sicherheitsprobleme lösen können.

c. Technology Threat Avoidance Theory
   Liang und Xue (2009) entwickelten durch die Zusammenführung von verschiedenen Theorien aus den Forschungsgebieten Psychologie, Gesundheitspsychologie, Informationssysteme, Management, Marketing und Finanzen eine Technologie-Bedrohungs-Vermeidungstheorie (engl. Technology Threat Avoidance Theory = TTAT). Die von Liang und Xue beschriebene Theorie erklärt das Verhalten eines einzelnen IT-Anwenders bei der Vermeidung von Bedrohungen durch Informationstechnologien. Die Theorie zeigt auf, dass das Bedrohungsvermeidungsverhalten eines Benutzers in Abhängigkeit von den zwei kognitiven Prozessen Bedrohungseinschätzung (engl. Threat-Appraisal) und Bewältigungseinschätzung (engl. Coping-Appraisal) steht. Dabei beziehen sie sich auf die Protection Motivation Theory. Im Kontext der Bewältigungsstrategie (engl. Coping) unterscheiden Liang & Xue (2009, S. 77) zwischen problemorientierter Bewältigung (engl. Problem-Focused Coping) und emotionaler Bewältigung (engl. Emotion-Focused Coping). Abhängig von der Bedrohungs- und Bewältigungseinschätzung eines

Benutzers tendiert dieser zu einer der obigen Bewältigungsstrategien. Die problemorientierte Bewältigung führt gemäß Liang und Xue zur Umsetzung von Sicherheitsmaßnahmen und emotionale Bewältigung führt beispielsweise zu Verneinung im Sinne von Ablehnung der Situation oder Wunschdenken, d. h. beispielsweise, nicht interessant für einen Angreifer zu sein.

5.3 Methode und Sample

Die für die vorliegende Analyse gewählte Forschungsmethode basiert auf einem holistischen Multiple-Case-Design nach Yin (2014, S. 50) und durchläuft die drei Phasen „Define and Design", „Prepare, Collect and Analyze" und „Analyze and Conclude". In der Phase Define and Design wurden die theoretischen Grundlagen zur vorliegenden Analyse erarbeitet, die Forschungsfragen präzisiert, mögliche Wirtschaftspartner (Fälle) kontaktiert und selektiert. Im Rahmen der vorliegenden Analyse wurden insgesamt drei Fallstudien durchgeführt. Jede Fallstudie bezieht sich dabei auf den realen Kontext eines Schweizer KMU. Um potenzielle Fallstudienpartner zu finden, wurden Schweizer KMU mit mindestens 10 Mitarbeitenden sowie einem Tätigkeitsfeld im tertiären Sektor im Internet, auf sozialen Netzwerken und im privaten Umfeld gesucht. Insgesamt konnten so drei Fallstudienpartner für die vorliegende Forschungsarbeit gewonnen werden. Da davon ausgegangen wird, dass es sich bei der zu untersuchenden Intentionsverhaltenslücke um ein grundsätzliches Phänomen bei Schweizer KMU handelt, wurden als Auswahlkriterien lediglich Unternehmensgröße und Wirtschaftssektor definiert und eine Kombination von gezieltem und Convenience-Stichprobenziehungsverfahren angewandt. Die Fallstudienanzahl ($n = 3$) wurde dabei aufgrund der im Rahmen der vorliegenden Analyse zur Verfügung stehenden Ressourcen festgelegt.

In der Phase Prepare, Collect and Analyze werden die einzelnen Fälle betrachtet. Dabei wird jeder Fall isoliert untersucht und aufbereitet. Die Erhebung der empirischen Daten für die vorliegende Analyse basierte auf Interviews und Dokumenten, die im Kontext der drei Fallstudien erhoben wurden. Alle Interviews wurden nach Zustimmung durch die Teilnehmenden aufgenommen und im Anschluss transkribiert. Die Transkription und Codierung (Kategorienzuweisung) der Interviews erfolgte mit der Software MAXQDA[3]. Eisenhardt (1989, S. 540) folgend wurden in einem ersten Analyseschritt fallinterne Muster identifiziert, bevor generalisierte fallübergreifende Muster im Rahmen der abschließenden Phase Analyse and Conclude abgeleitet wurden. Die Musterbildung orientierte sich an der qualitativen Inhaltsanalyse nach Gläser und Laudel (2010, S. 46). Dazu wurde ein Kategoriensystem einerseits deduktiv aus der analysierten Literatur (Theorie) sowie andererseits induktiv aus den Erkenntnissen der empirischen Daten gebildet. Die definierten Kategorien bilden bewusst sämtliche Determinanten aus dem Forschungsmodell (siehe Abschn. 5.2) ab. Das finale Kategoriensystem wird in der Tab. 5.1 dargestellt.

[3]Software zur qualitativen Datenanalyse – https://www.maxqda.de/.

Tab. 5.1 Kategoriensystem. (Eigene Darstellung)

ID	Kategorie	Beschreibung
A	Intentionsverhaltenslücke	A1: Wichtigkeit der IT-Landschaft A2: Umgesetzte Sicherheitsmaßnahmen (Technologie, Prozess, Mensch) A3: Angestrebtes Cybersicherheitsniveau
B	Unternehmensressourcen	B1: Informationssicherheitstechnologien B2: Qualifiziertes Informationssicherheits-personal B3: Sicherheitsbewusstsein der Benutzer B4: IT-Fähigkeiten
C	Bewältigungsmanagement (Bewältigungs-einschätzung)	C1: Selbstwirksamkeit C2: Wirksamkeit C3: Kosten
D	Bedrohungsmanagement (Bedrohungsein-schätzung)	D1: Schadensausmaß D2: Schadensanfälligkeit
E	Sozialer Einfluss	E1: Normativdruck E2: Nachahmungsdruck E3: Zwangsdruck
F	IT-Risikomanagement	Keine Subkategorie
G	Selbsteinschätzung	Keine Subkategorie
H	Motivation	Keine Subkategorie
I	Subjektive Wahrnehmung	Keine Subkategorie
J	Hilfsmittel	Keine Subkategorie
K	Erfolgsfaktoren	Keine Subkategorie

Der gewählte Forschungsprozess nach Yin (2014) erlaubt dabei, die Datenerhebungsmethoden während des Forschungsprozesses basierend auf ermittelten Erkenntnissen anzupassen. So wurde sichergestellt, dass eine bedeutende Entdeckung innerhalb einer Fallstudie bereits während des laufenden Forschungsprozesses in die noch bevorstehende Forschung einfließen konnte (Yin 2014, S. 59 ff.).

5.3.1 Sample

Die Fallstudienpartner der vorliegenden Forschungsarbeit werden in der Tab. 5.2 kurz vorgestellt. Auf Wunsch der Fallstudienpartner werden diese anonymisiert und nicht namentlich vorgestellt.

Tab. 5.2 Fallstudienpartner. (Eigene Darstellung)

Fallstudienpartner 1	Beim Fallstudienpartner 1 handelt es sich um ein Schweizer KMU mit Sitz im Zürcher Oberland. Das Kerngeschäft des Fallstudienpartners 1 ist die Erbringung von Hauswartungs- und Reinigungsdienstleistungen. Aktuell beschäftigt das Unternehmen etwas mehr als 200 Mitarbeitende. Rund 50 Mitarbeitende arbeiten regelmäßig mit IT-Mitteln der Unternehmung. Als Interviewpartner stellte sich der Geschäftsführer zur Verfügung. Er entscheidet in seiner Rolle als Geschäftsführer über sämtliche IT-Fragen innerhalb der Unternehmung
Fallstudienpartner 2	Der Fallstudienpartner 2 ist ein Schweizer KMU mit Hauptsitz in der Zentralschweiz. Das Unternehmen besitzt zwei Zweigstellen, die sich ebenfalls in der Zentralschweiz befinden. Das Kerngeschäft des Fallstudienpartners 2 sind Unternehmens-, Steuer- und Rechtsberatungen sowie weitere Treuhand- und Revisionsdienstleistungen. Das Unternehmen beschäftigt zurzeit 50 Mitarbeitende. Als Interviewpartner stellte sich der ICT-Verantwortliche des Fallstudienpartners zur Verfügung
Fallstudienpartner 3	Beim Fallstudienpartner 3 handelt es sich um ein im Bereich Tourismusmarketing tätiges Schweizer KMU mit Hauptsitz in Zürich sowie 33 Außenstandorten weltweit. Aktuell beschäftigt das Unternehmen rund 245 Mitarbeitende. Die gesamte IT-Landschaft wird dabei vom Hauptsitz in Zürich bewirtschaftet. Als Interviewpartner stellten sich der IT-Leiter sowie ein Senior-System-Engineer zur Verfügung

5.4 Ergebnisse

In diesem Abschnitt werden die aus den empirischen Daten gewonnenen Erkenntnisse anonymisiert aufgezeigt und die definierten Forschungsfragen beantwortet. Die vorliegende Veröffentlichung fokussiert sich auf die Erkenntnisse aus der Cross-Case-Analyse und verzichtet bewusst auf die Ausführung der Erkenntnisse der einzelnen Within-Case-Analysen (siehe Abschn. 5.2).

5.4.1 Intentionsverhaltenslücke

Die Analyse der empirischen Daten zeigt, dass bei allen Entscheidungsträgern der Fallstudienpartner die Verhaltensintention „ein adäquates Cybersicherheitsniveau zu erreichen“ besteht. Dies äußerte sich in Interviewaussagen der Entscheidungsträger sowie in firmeninternen Dokumenten, welche zusammengefasst festhalten, dass die Informationstechnologie für die Kontinuität der Unternehmen eine entscheidende Rolle spielt und deshalb der Schutz der Daten und IT-System besonders wichtig ist. Die Wichtigkeit der IT-Landschaft wird dabei von den Entscheidungsträgern mit dessen Verfügbarkeits- oder Vertraulichkeitsanforderungen argumentiert. Die bestehende

Verhaltensintention lässt vermuten, dass somit durch die Unternehmen oder deren Entscheidungsträger als für sie relevant wahrgenommene Cybersicherheitsbedrohungen durch adäquate Maßnahmen adressiert werden (Ausführung des Zielverhaltens vgl. Abschn. 5.2). Die Analyse der empirischen Daten zeigt jedoch, dass häufig das Gegenteil der Fall ist. Als relevant wahrgenommene Bedrohungen werden nicht oder lediglich teilweise durch adäquate Maßnahmen adressiert. So werden beispielsweise Phishing-Angriffe[4] von allen Entscheidungsträgern als relevante Bedrohung wahrgenommen, möglich Abwehrmaßnahmen, bspw. zur Stärkung der Mitarbeitersensibilisierung, werden jedoch nicht umgesetzt. Ein Interviewpartner des Fallstudienpartner 1 unterstreicht sein Verhalten sinnbildlich mit folgender Aussage:

> Man sagt ja bekanntlich der Deckel kommt erst dann auf den Brunnen, wenn das Kind hineingefallen ist. Wenn etwas passieren würde, wäre das Thema natürlich von einer Sekunde auf die andere extrem wichtig für mich.

Das dabei gezeigte Verhalten entspricht der Form einer emotionalen Bewältigungsstrategie. Diese Form von Bewältigung führt zu Verleugnung „diese Bedrohung wird bei mir nicht eintreten“ oder Wunschdenken „niemand will meiner IT-Landschaft Schaden zufügen“ (Liang und Xue 2009, S. 86). Das bereits in mehreren Studien (vgl. BSI 2011; Hirschi und Portmann 2017; Renaud 2016; Zürich Versicherungs-Gesellschaft 2016; gfs-zürich 2017) sowie von Straub (1990, S. 255) aufgezeigte Phänomen der Intentionsverhaltenslücke hinsichtlich Cybersicherheit konnte auf Basis der erhobenen empirischen Daten der vorliegenden Analyse somit auch bei Entscheidungsträgern in Schweizer KMU beobachtet werden. Basierend auf den erhobenen empirischen Daten sowie der bestehenden Literatur kann zudem davon ausgegangen werden, dass es sich dabei um ein großflächig vorhandenes Phänomen bei KMU handelt, das unabhängig von der Größe, Branche und Herkunft der KMU vorkommt.

Das Phänomen der Intentionsverhaltenslücke hinsichtlich Cybersicherheit hat in der bestehenden Forschung keine einheitliche Bezeichnung und wird in der vorliegenden Forschungsarbeit als Security-Paradox[5] bezeichnet. Nachfolgend wird der Versuch einer Definition des Begriffs Security-Paradox vorgenommen.

▶ Als **Security-Paradox** wird bei einer Organisation eine beobachtbare Intentionsverhaltenslücke hinsichtlich der Bestrebung[6] eines gewünschten Cybersicherheitsniveaus

[4]Die betrügerische Praxis, E-Mails zu versenden, die angeblich von seriösen Absendern stammen, um Einzelpersonen dazu zu bringen, persönliche Daten wie Passwörter und Kreditkartennummern preiszugeben.

[5]Der Begriff IT-Sicherheits-Paradox wurde erstmalig von Buxmann (2017) in einem Blogeintrag erwähnt.

[6]Die Bestrebung ergibt sich dabei aus der Wichtigkeit der IT-Landschaft der Unternehmung.

(Verhaltensintention) und der fehlenden Umsetzung von hierfür notwendigen Maßnahmen (Ausführung des Zielverhaltens) bezeichnet.

Das Security-Paradox darf dabei nicht mit den Begriffen Privacy-Paradox oder Datenschutzparadox verwechselt werden, die sich auf das Phänomen beziehen, dass Privatsphäre und Datenschutz für die Menschen im digitalen Zeitalter ein Hauptanliegen sind, während auf der anderen Seite Einzelpersonen persönliche Informationen für relativ kleine oder gar keine Belohnungen preisgeben (Kokolakis 2017, S. 122). Buxmann (2017), der den Begriff IT-Sicherheits-Paradox erstmalig 2017 in einem Blogbeitrag erwähnt, führt aus, dass unrealistischer Optimismus eine der Hauptursachen für das Vorhandensein des Security-Paradox sein könnte. Dies gründet auf seiner Feststellung, dass Entscheidungsträger dazu tendieren, ihr eigenes Cybersicherheitsniveau im Vergleich mit jenem zu konkurrierenden Unternehmen als deutlich besser einschätzen. Gemäß Buxmann wird dieses Verhalten in der Psychologie als unrealistischer Optimismus beschrieben, bei welchem Menschen dazu tendieren, ihr eigenes Risiko im Vergleich mit anderen verzerrt wahrzunehmen und zu unterschätzen. Dasselbe Verhalten von Entscheidungsträgern konnte auch in den im Rahmen der vorliegenden Analyse durchgeführten Fallstudien beobachtet werden. So schätzen zwei der drei Entscheidungsträger ihr eigenes Cybersicherheitsniveau als deutlich besser ein, als jenes von konkurrierenden Unternehmen. Im folgenden Kapitel werden die potenziellen Ursachen für das Vorhandensein des Security-Paradoxes diskutiert.

5.4.2 Ursachenanalyse

Die dieser Analyse zugrunde liegende Forschungsarbeit fokussierte sich auf die Ursachenanalyse für das Vorhandensein des Security-Paradoxes. Die folgenden Analyseergebnisse wurden von den Autoren bewusst für die Führungskräfte und Entscheidungsträger aufbereitet. So werden Determinanten, für welche kein oder lediglich ein geringer Einfluss auf das Vorhandensein des Security-Paradoxes festgestellt werden konnte, nicht berücksichtigt. Gleiches gilt für Determinanten, die von Führungskräften und Entscheidungsträgern nicht beeinflusst werden können. Das Lesen der Analyseergebnisse soll Führungskräfte und Entscheidungsträger somit befähigen, bessere Entscheidungen betreffend Cybersicherheit im Rahmen der zu bewältigenden Digitalisierung treffen zu können.

5.4.2.1 Unternehmensressourcen

Cavusoglu et al. (2015, S. 396) stellten fest, dass die IT-Fähigkeiten einer Organisation einen maßgeblichen Einfluss auf ihr Cybersicherheitsniveau besitzen. Dieser Sachverhalt konnte auch in den empirischen Daten der vorliegenden Forschungsarbeit nachgewiesen werden und wird in der Abb. 5.2 illustriert.

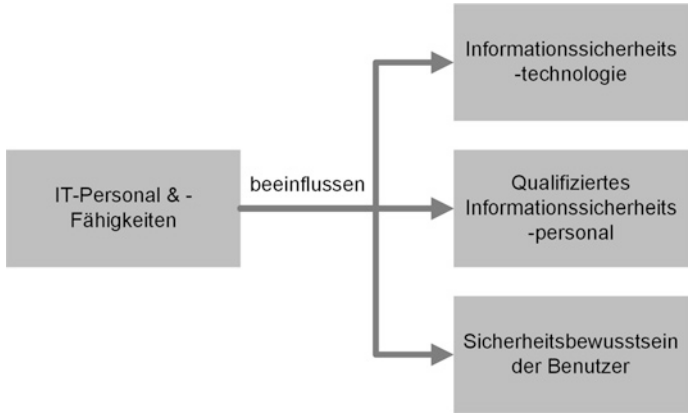

Abb. 5.2 Einfluss IT-Fähigkeiten. (Eigene Darstellung)

So haben die Fallstudienpartner, die über eine interne IT-Abteilung verfügen, ein merklich höheres Cybersicherheitsniveau als jene ohne interne IT-Abteilung. Zudem wurde festgestellt, dass dieselben Fallstudienpartner ihre eigene Selbstwirksamkeit deutlich höher einschätzen. Die Literaturrecherche zeigt, dass die Ausführung eines Verhaltens umso wahrscheinlicher ist, je höher die Selbstwirksamkeitserwartung ausfällt (siehe Abschn. 5.2). Im heutigen digitalen Wandel ist es deshalb umso wichtiger, dass Führungskräfte und Entscheidungsträger sicherstellen, dass eine Unternehmung über ausreichend IT-Fähigkeiten verfügt. Gleichwohl reicht das lediglich Vorhandensein von IT-Fähigkeiten jedoch für die meisten Schweizer KMU nicht aus, um ein für sie angemessenes Cybersicherheitsniveau zu erreichen. Ferner ist es wichtig, dass Führungskräfte und Entscheidungsträger Cybersicherheit als Führungsaufgabe wahrnehmen und eine Cybersicherheitskultur etablieren. Dazu müssen notwendige Verantwortlichkeiten definiert, das Sicherheitsbewusstsein der Mitarbeiter gestärkt, Topmanagement-Unterstützung für das Thema gezeigt und notwendiges Fachwissen beschafft werden. Kurzfristig ist nicht davon auszugehen, dass in Zukunft jedes Schweizer KMU einen Cybersicherheitsverantwortlichen benennt und diesen mit Unmengen an Unternehmensressourcen ausrüstet – dies soll auch keinesfalls die Quintessenz der vorliegenden Analyse sein – jedoch müssen sich Führungskräfte der Verantwortung, ein für ihre Unternehmung angemessenes Cybersicherheitsniveau zu erreichen, stellen. Dies kann beispielsweise bereits mit dem Durchführen institutionalisierter Sensibilisierungsmaßnahmen für Mitarbeitende, dem Umsetzen von technologischen Grundschutzmaßnahmen und der Definition grundlegender Prozesskontrollen, wie bspw. dem Vieraugenprinzip erreicht werden.

5.4.2.2 Bedrohungs- und Bewältigungsmanagement

Die Erkenntnisse aus den empirischen Daten der vorliegenden Analyse zeigen, dass bei keinem der untersuchten Fallstudienpartner ein systematischer Ansatz zum Bedrohungs- oder Bewältigungsmanagement vorhanden ist. Die kognitiven Prozesse der Bedrohungs- und Bewältigungseinschätzung sind jedoch ausschlaggebend dafür, ob eine Verhaltensintention, welche einer Bedrohung entgegenwirkt, entsteht oder nicht und wie mit dieser Verhaltensintention umgegangen wird (siehe Abschn. 5.2). Die dabei fehlende Systematik zur Behandlung des Themas führt dazu, dass die Adressierung stark von den persönlichen Erfahrungen, Fähigkeiten und dem Wissen der jeweiligen Entscheidungsträger abhängt. Dies birgt hohes Potenzial für das Auftreten einer emotionalen Bewältigungsstrategie und damit einhergehenden Fehleinschätzungen (vgl. Buxmann 2017) und unvollständigen Ansätzen bei der Behandlung des Themas Cybersicherheit. Beispielsweise wenn der Entscheidungsträger nicht über genügend Wissen über die Materie verfügt oder nicht genügend stark sensibilisiert ist. So wurde bei der Analyse der empirischen Daten festgestellt, dass die Entscheidungsträger aller Fallstudienpartnern eine klare Präferenz für technologische Maßnahmen gegenüber organisatorischen oder prozessualen Maßnahmen zur Stärkung ihrer Cybersicherheit besitzen, die von den Entscheidungsträgern erkannten Bedrohungen jedoch häufiger organisatorische oder prozessuale Maßnahmen nahelegen würden (bspw. menschliches Fehlverhalten). Um dieser Herausforderung erfolgreich zu begegnen, sollten sich Entscheidungsträger und Führungskräfte deshalb bei der Analyse von Cybersicherheitsbedrohungen und bei der Festlegung von Cybersicherheitsmaßnahmen an etablierten Standards (z. B. ISO 2700x[7], NIST Cybersecurity Framework[8], IT-Grundschutz des BSI[9] oder den IKT-Minimalstandard des Bundesamt für wirtschaftliche Landesversorgung[10]) orientieren und sofern sinnvoll, externe Fachspezialisten beiziehen.

Die Literaturrecherche und die empirischen Daten zeigen, dass ein ganzheitlicher Ansatz zur adäquaten Adressierung von Cybersicherheit notwendig ist. Dies bedeutet, dass gerade sich im digitalen Wandel befindliche Schweizer KMU Maßnahmen auf organisatorischer, prozessualer sowie technologischer Ebene ergreifen müssen, um ein angemessenes Cybersicherheitsniveaus zu erreichen. Dabei ist die Aufklärung und Schulung der Mitarbeitenden in Bezug auf Cybersicherheit ein zentraler Aspekt. Eine angemessene Aufklärung fördert das allgemeine Bewusstsein und das Verständnis bei den Mitarbeitenden und ermöglicht die Etablierung einer Cybersicherheitskultur. In dieser Kultur teilen die Mitarbeitenden gemeinsame Werte, Normen und Überzeugungen bezüglich Cybersicherheits-Praktiken (Woodhouse 2008, S. 247; Tu und Yuan 2014, S. 1878–1879). Dieses gemeinsame Verständnis erzeugt einen sich bei den Mitarbeitenden auf Cybersicherheit positiv auswirkenden sozialen

[7] https://www.iso.org/news/ref2266.html.

[8] https://www.nist.gov/cyberframework.

[9] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html.

[10] https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html.

Einfluss in Form von Normativdruck (siehe Abschn. 5.2). Um das für ein KMU passende Cybersicherheitsniveau identifizieren zu können, sollte zudem ein unternehmensweites Risikomanagement etabliert werden. Dies hilft bei der Auswahl passender Sicherheitsmaßnahmen sowie bei der realistischen Einschätzung von Bedrohungs- und Bewältigungsmöglichkeiten (Tu und Yuan 2014, S. 1878–1879).

5.4.2.3 Verhalten Entscheidungsträger

Die Analyse der empirischen Daten zeigt, dass bei allen drei Fallstudienpartnern eine klare Definition hinsichtlich der Verantwortlichkeiten und Aufgaben zur Cybersicherheit nicht oder nur teilweise vorhanden sind. Auch fehlt bei sämtlichen Fallstudienpartnern ein systematisches Bewältigungs-, Bedrohungs- und/oder Risikomanagement (siehe Abschn. 5.4.2.2). Diese beiden Tatsachen führen dazu, dass das Cybersicherheitsniveau einer Organisation stark dem Einfluss des jeweiligen IT-Verantwortlichen unterliegt. So zeigte sich bei den Fallstudienpartnern 2 und 3, dass der Vorgänger des jeweiligen IT-Verantwortlichen dem Cybersicherheitsniveau der jeweiligen IT-Landschaft lediglich geringe Beachtung schenkte. Durch den Wechsel zu den heutigen IT-Verantwortlichen konnte das Cybersicherheitsniveau der IT-Landschaften merklich gesteigert werden. Der IT-Leiter des Fallstudienpartners 3 hält diesbezüglich fest:

> Wenn IT- und Informationssicherheit nicht systematisch in einer Unternehmung ausgeübt wird, entscheiden die Erfahrungen, die Interessen und die Fokusse des IT-Verantwortlichen, ob *Security* adäquat adressiert wird oder nicht.

Fehlendes Wissen oder Erfahrung beim IT-Verantwortlichen führen so zu einer nicht realistischen Bedrohungs- und Bewältigungseinschätzung. Diese Fehleinschätzung[11] führt wiederum zur Nichtergreifung von adäquaten Sicherheitsmaßnahmen. Führungskräfte und Entscheidungsträger von Schweizer KMU müssen sich diesem Entscheidungsbias bewusst werden. Um diesem entgegen zu wirken, sollten sich Führungskräfte und Entscheidungsträger stärker auf Sicherheitsstandards zur Adressierung von Cybersicherheit berufen. Bestehende Studien (vgl. Hirschi und Portmann 2017; gfs-zürich 2017) zeigen jedoch, dass lediglich zirka 30 % der Schweizer KMU Sicherheitsstandards zur Adressierung von Cybersicherheit verwenden. Von den untersuchten Fallstudienpartnern verwendet keines der Unternehmen Sicherheitsstandards. Die Verwendung von Sicherheitsstandards hätte für KMU jedoch den Vorteil, eine durch den Standard geführte, ganzheitliche Betrachtung von Cybersicherheit sicherzustellen. Dabei gilt es jedoch anzumerken, dass eine Vielzahl verfügbarer Sicherheitsstandards (z. B. ISO 2700x, NIST Cybersecurity Framework, IT-Grundschutz des BSI usw.) sich für KMU zwar grundsätzlich eignen, diese aber in der Praxis Mangels an Erfahrung mit solchen Werken für KMU schwer umsetzbar sind. Gemäß Kardel (2011, S. 44–48) müssen Sicherheitsstandards

[11] Siehe Abschn. 5.4.1 – Fehleinschätzung betreffend „Cybersicherheitsniveau im Vergleich mit konkurrierenden Unternehmen“.

deshalb an den KMU-Kontext angepasst werden. Eine Möglichkeit für KMU, diese Kontextanpassung zu umgehen, ist die direkte Verwendung von KMU-spezifischen Hilfsmitteln, wie beispielsweise:

- Merkblatt IT-Sicherheit für KMU von der Melde- und Analysestelle Informationssicherung und dem Swiss Government Computer Emergency Response Team (MELANI & GovCert 2018)
- 10-Punkte-Regel zur Stärkung der Cybersicherheit des Schweizer KMU Portal (KMU Portal, 2018)
- Mehr Informationssicherheit für Klein- und Mittelbetriebe (KMU) (KMU Portal, 2016)
- Informationssicherheits- und Datenschutzstandard für KMU der ENISA (Manso et al. 2015)

5.5 Diskussion

Die vorliegende Forschungsarbeit identifizierte erstmalig[12] mittels empirischer Forschung Ursachen, die zum Vorhandensein des Security-Paradoxes führen. Es ist allerdings zu beachten, dass die kleine Anzahl beobachteter Fälle in dieser Forschungsarbeit eine wesentliche Einschränkung bei der Interpretation der Ergebnisse bedeutet und damit Vorsicht geboten ist, die vorliegenden Ergebnisse für sämtliche Schweizer KMU oder grundsätzlich für KMU zu verallgemeinern. Stattdessen gilt es durch den Leser zu prüfen, ob die Ergebnisse im relevanten KMU-Kontext wiedererkannt werden und wie die beschriebenen Empfehlungen situationsgerecht adaptiert werden können.

Bezugnehmend auf die Forschungsfragen dieser Arbeit lassen sich folgende Beobachtungen zusammenfassend festhalten. 1) Eine Intentionsverhaltenslücke (Security-Paradox) hinsichtlich Cybersicherheit konnte bei allen drei Fallstudienpartnern beobachtet werden (siehe Abschn. 5.4.1). Bestehende Studien und die empirischen Ergebnisse lassen somit die Vermutung zu, dass es sich beim Security-Paradox um ein verbreitetes Phänomen handelt, das auch bei Schweizer KMU zu beobachten ist. Die vorliegende Analyse liefert dazu jedoch keinen stichhaltigen Nachweis. 2) Basierend auf dem entwickelten Forschungsmodell und den erhobenen empirischen Daten wurde für folgende, von Führungskräften und Entscheidungsträgern beeinflussbaren, Determinanten ein starker Einfluss auf das Vorhandensein des Security-Paradox beobachtet[13]:

[12]Gemäß dem durch die Autoren dieser Veröffentlichung erhobenen aktuellen Forschungsstand.

[13]Nebst den drei genannten Determinanten wurde für die Determinante „Sozialer Einfluss“ ebenfalls ein starker Einfluss auf das Vorhandensein des Security-Paradoxes beobachtet. Da Zwangsdruck beispielsweise durch Regulatorien einen starken Einfluss auf das Verhalten von Entscheidungsträgern besitzt. Dies wurde in der vorliegenden Veröffentlich jedoch nicht detaillierter behandelt, da Entscheidungsträger nicht verantworten ob ein Zwangsdruck besteht oder nicht.

- Unternehmensressourcen (siehe Abschn. 5.4.2.1)
- Bewältigungs- und Bedrohungsmanagement (siehe Abschn. 5.4.2.2)
- Verhalten Entscheidungsträger (siehe Abschn. 5.4.2.3)

Im Rahmen der Ursachenanalyse zeigte sich jedoch, dass die Zusammenhänge und Wechselwirkungen der Determinanten vielschichtig sind und so nicht eine einzelne Determinante für das Vorhandensein des Security-Paradoxes identifiziert werden konnte. Kritisch merken die Autoren der vorliegenden Analyse an, dass aufgrund der eingeschränkten Datenbasis möglicherweise relevante Ursachen nicht identifiziert wurden. Zukünftige Forschungsarbeiten könnten an diesen Punkt anknüpfen und die in dieser Forschungsarbeit identifizierten Ursachen validieren und allfällig erweitern.

Zusammenfassend stellen die Autoren der vorliegenden Forschungsarbeit fest: Cybersicherheit ist generell sowie spezifisch für KMU ein Thema, das im Kontext der Digitalisierung an Wichtigkeit gewinnt und somit auch in Zukunft die Aufmerksamkeit von Führungskräften und Entscheidungsträger verdient.

5.6 Zusammenfassung und Empfehlungen für die Praxis

In dem Versuch das Vorhandensein des Security-Paradoxes zu vermeiden, ist es für Führungskräfte und Entscheidungsträger von Schweizer KMU unerlässlich, zu verstehen, welche Faktoren einen erheblichen Einfluss auf dieses Phänomen besitzen. Dazu wurden in der vorliegenden Forschungsarbeit, die für Führungskräfte und Entscheidungsträger relevanten Determinanten aufbereitet (siehe Abschn. 5.4.2) und nachfolgende Empfehlungen zusammengestellt:

Cybersicherheit als Führungsaufgabe wahrnehmen
Um die Herausforderung der Cybersicherheit, im Zuge der Digitalisierung zu meistern, müssen Entscheidungsträger und Führungskräfte von Schweizer KMU sich ihrer Verantwortung hinsichtlich Cybersicherheit bewusst werden und sie wahrnehmen. Unterstützung durch Entscheidungsträger (Management Support) wird in der bestehenden Forschung als einer der wichtigsten Erfolgsfaktoren zur erfolgreichen Adressierung von Cybersicherheit genannt (vgl. Chew et al. 2008; Dirks et al. 2016; Schwyter und Wisler 2013; Tu und Yuan 2014; Woodhouse 2008; Manso et al. 2015). Diese Tatsache wird in den empirischen Daten der vorliegenden Forschungsarbeit klar bestätigt. Es konnte eine starke Abhängigkeit zwischen der Möglichkeit einer Organisation, Sicherheitsmaßnahmen zu ergreifen und der Unterstützung für die Maßnahmenumsetzung durch die Geschäftsleitung (in der Regel der Entscheidungsträger) erkannt werden. So entscheidet bei allen drei Fallstudienpartnern die Geschäftsleitung über die Umsetzung von Maßnahmen zur Stärkung der Cybersicherheit. Es ist aus diesem Grund wichtig, dass Entscheidungsträger einer Organisation ein Bewusstsein für Cybersicherheit besitzen. Fehlt dieses Bewusstsein bei den Entscheidungsträgern, bleiben Investitionen in die Stärkung der Cybersicherheit mit

hoher Wahrscheinlichkeit aus. Die Sensibilisierung der Entscheidungsträger von Schweizer KMU wird aktuell einerseits durch den Staat und andererseits durch die Privatwirtschaft (Gewerbeverbände) bewusst gefördert. Um die Unterstützung von Schweizer KMU im Bereich Cybersicherheit zu stärken, wurde 2015 von der damaligen Bundesrätin Eveline Widmer-Schlumpf die Expertengruppe Zukunft der Datenbearbeitung und Datensicherheit eingesetzt.[14] In einem Interview mit der Neuen Zürcher Zeitung gibt Brigitta M. Gadient als Präsidentin der Expertengruppe an (Mäder 2017):

> Wir wollen bei den kleinen und mittleren Unternehmen eine Sensibilisierung für die IT-Sicherheit erreichen.

Im September 2018 wurde von der Expertengruppe gemeinsam mit den wichtigsten Verbänden und Gruppierungen aus dem IT-Bereich sowie dem Bundesamt für wirtschaftliche Landesversorgung in einer gemeinsamen Initiative ein Schnelltest[15] zur Cyberresilienz von KMU lanciert. Der Schnelltest liefert Erkenntnisse, in welchen Bereichen eines KMU hinsichtlich Cybersicherheit Lücken und allfälliger Handlungsbedarf bestehen (ICTswitzerland 2018).

Etablierte Standards verwenden

Bestehende Studien (vgl. Hirschi und Portmann 2017; gfs-zürich 2017) zeigen, dass lediglich ein geringer Teil (zirka 30 %) der Schweizer KMU Sicherheitsstandards zur Adressierung von Cybersicherheit verwenden. In den empirischen Daten der vorliegenden Forschungsarbeit zeigte sich ein noch deutlicheres Bild – keiner der Fallstudienpartner verwendet Sicherheitsstandards zur Adressierung von Cybersicherheit. Die Verwendung von Sicherheitsstandards hätte für KMU jedoch den Vorteil, eine durch den Standard geführte, ganzheitliche und auf etablierten Praktiken basierende Betrachtung von Cybersicherheit sicherzustellen. So können die relevanten organisatorischen, technologischen und prozessualen Sicherheitsmaßnahmen zur Erreichung eines adäquaten Sicherheitsniveaus bestmöglich definiert werden, was für einige Entscheidungsträger und Führungskräfte aufgrund fehlender Erfahrungswerte zunehmend eine Herausforderung darstellt (Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit 2018, S. 64). Das systematische Vorgehen anhand eines Sicherheitsstandards zur Einführung sowie zur Unterhaltung eines Cybersicherheit-Managementsystems ist ein relevanter Erfolgsfaktor für die erfolgreiche Adressierung von Cybersicherheit (Woodhouse 2008, S. 247). Es empfiehlt sich somit für Entscheidungsträger und Führungskräfte von Schweizer KMU, sich mit bestehenden Sicherheitsstandards (z. B. ISO 2700x, NIST Cybersecurity Framework, IT-Grundschutz des BSI usw.) auseinanderzusetzen und diese bei der Bearbeitung des Themas zu berück-

[14]Motion 13.3841 – https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20133841.

[15]https://www.cybersecurity-check.ch/.

sichtigen. Nach Ansicht der Autoren stellt der Schnelltest zur Cyberresilienz von KMU einen guten Ausgangspunkt zur erstmaligen systematischen Adressierung des Themas dar.

Cybersicherheitskultur etablieren

Um Cybersicherheit nachhaltig in einem Unternehmen zu verankern und das Verhalten der Mitarbeitenden langfristig positiv zu verändern, bedarf es der Definition notwendiger Verantwortlichkeiten und einer flächendeckenden Sensibilisierung aller Mitarbeitenden. Eine angemessene Aufklärung fördert das allgemeine Bewusstsein und das Verständnis bei den Mitarbeitenden und ermöglicht die Etablierung einer Cybersicherheitskultur. Dabei teilen die Mitarbeitenden gemeinsame Werte, Normen und Überzeugungen bezüglich Cybersicherheitspraktiken. Durch dieses gemeinsame Verständnis entsteht eine sich positiv auswirkende Form von Normativdruck (siehe Abschn. 5.2). Diese verankert einen sicheren Umgang mit IT-Mitteln im Unternehmen und fördert so eine nachhaltige Stärkung des Cybersicherheitsniveaus. Entscheidungsträger und Führungskräfte müssen dazu ihre Verantwortung hinsichtlich Cybersicherheit wahrnehmen, mit gutem Beispiel vorangehen und die entsprechenden Werte, Normen und Überzeugungen vorleben, um diese als Unternehmenskulturwerte zu verankern.

Abschließend halten die Autoren der vorliegenden Forschungsarbeit fest: Die Digitalisierung kann für ein KMU nur dann nachhaltig sein, wenn sie auf Vertrauen in eine organisatorische, prozessuale und technologische sichere IT beruht und Cybersicherheit dabei als Führungsaufgabe wahrgenommen wird.

Literatur

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In: J. Kuhl & J. Beckman (Hrsg.), *Action-control: From cognition to behavior* (S. 11–39). Heidelberg: Springer.

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2011). Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/KMU/Studie_IT-Sicherheit_KMU.pdf. Zugegriffen: 9. Apr. 2018.

Burnkrant, R. E., & Cousineau, A. (1975). Informational and normative social influence in buyer behavior. *Journal of Consumer Research, 2*(3), 206–215. https://doi.org/10.1086/208633.

Buxmann, P. (2017). Das IT-Sicherheits-Paradox: Warum Unternehmen zu wenig in IT-Sicherheit investieren. http://www.peterbuxmann.de/2017/08/03/das-it-sicherheits-paradox-warum-unternehmen-zu-wenig-in-it-sicherheit-investieren/. Zugegriffen: 19. März 2018.

Browne, S., Lang, M., & Golden, D. W. (2015). Linking threat avoidance and security adoption: A theoretical model for SMEs. BLED 2015 Proceedings. https://aisel.aisnet.org/bled2015/35. Zugegriffen: 11. März 2018.

Cavusoglu, H., Cavusoglu, H., Son, J.-Y., & Benbasat, I. (2015). Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information & Management, 52*(4), 385–400. https://doi.org/10.1016/j.im.2014.12.004.

Chew, E., Swanson, M., Stine, K. M., Bartol, N., Brown, A., & Robinson, W. (2008). *Performance measurement guide for information security*. Gaithersburg: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-55r1.

Deutsch, M., & Gerard, H. B. (1955). A study of normative and informational social influences upon individual judgement. *Journal of Abnormal Psychology, 51*(3), 629–636. https://doi.org/10.1037/h0046408.

Dirks, N., Schemmer, S., & Schumann, R. (2016). Etablierung effektiver Informationssicherheit. In: S. Helmke & M. Uebel (Hrsg.), *Managementorientiertes IT-Controlling und IT-Governance* (S. 239–251). Wiesbaden: Springer. https://doi.org/10.1007/978-3-658-07990-1_15.

Eckert, C. (2017). Cybersicherheit beyond 2020! *Informatik-Spektrum, 40*(2), 141–146. https://doi.org/10.1007/s00287-017-1025-6.

Eisenhardt, M. K. (1989). Building theories from case study research. *The Academy of Management Review, 14*(4), 532–550. https://doi.org/10.2307/258557.

Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit. (2018). Bericht der Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit. https://www.newsd.admin.ch/newsd/message/attachments/53591.pdf. Zugegriffen: 10. Jan. 2019.

EY. (2018). Schweizer Unternehmen so optimistisch wie lange nicht mehr. http://www.ey.com/ch/de/newsroom/news-releases/medienmitteilung-ey-schweizer-unternehmen-so-optimistisch-wie-lange-nicht-mehr. Zugegriffen: 11. März 2018.

gfs-zürich. (2017). Cyberrisiken in Schweizer KMU. Zürich: gfs-zürich. https://ictswitzerland.ch/media/dateien/Studien/Schlussbericht_Cyberrisk_KMU_2017.pdf. Zugegriffen: 25. März 2018.

Gläser, J., & Laudel, G. (2010). *Experteninterviews und qualitative Inhaltsanalyse* (4. Aufl.). Wiesbaden: VS Verlag.

Grant, R. M. (2010). *Contemporary strategy analysis: Text only* (7. Aufl.). Hoboken: Wiley.

Hirschi, O., & Portmann, A. (2017). Nationale Studie zur Informationssicherheit in Schweizer KMU. Zustand der Informationssicherheit in Schweizer KMU (Veröffentlichte Studie). Luzern: Hochschule Luzern.

Hohmann, C., & Schwarzer, R. (2009). Selbstwirksamkeitserwartung. In J. Bengel & M. Jerusalem (Hrsg.), *Handbuch der Gesundheitspsychologie und Medizinischen Psychologie* (S. 61–67). Göttingen: Hogrefe.

ICTswitzerland. (2018). Medienmappe. Cybersecurity-Schnelltest für KMU. https://ictswitzerland.ch/media/dateien/Cyber_Security/Minimalstandards/Medienmappe_Cybersecurity-Schnelltest_KMU_2018_09_03_de.pdf. Zugegriffen: 18. Jan. 2019.

Inside-Channels. (2017). Initiative soll Schweizer KMU-Security verbessern. http://www.inside-channels.ch/articles/49147. Zugegriffen: 26. Okt. 2017.

Inside-it. (2018). Hacker stehlen Kundendaten von Waadtländer IT-Unternehmen. https://www.inside-it.ch/articles/50941. Zugegriffen: 30. Apr. 2018.

Kardel, D. (2011). IT-Sicherheitsmanagement in KMU. *HMD Praxis der Wirtschaftsinformatik, 48*(5), 44–51. https://doi.org/10.1007/BF03340623.

Kelman, H. C. (2006). Interests, relationships, identities: Three central issues for individuals and groups in negotiating their social environment. *Annual Review of Psychology, 57*(1), 1–26. https://doi.org/10.1146/annurev.psych.57.102904.190156.

Klipper, S. (2015). *Cybersicherheit*. Wiesbaden: Springer. https://doi.org/10.1007/978-3-658-11577-7.

KMU Portal für kleine und mittlere Unternehmen (KMU Portal). (2016). Mehr Informationssicherheit für Klein- und Mittelbetriebe (KMU). https://www.kmu.admin.ch/dam/kmu/de/dokumente/savoir-pratique/Informatique-et-IT/InfoSurance_10_Points_Programme_FR.pdf. Zugegriffen: 16. Mai 2018.

KMU Portal für kleine und mittlere Unternehmen (KMU Portal). (2018). Zehn Regeln für die Informationssicherheit im KMU. https://www.kmu.admin.ch/kmu/de/home/aktuell/monatsthema/2018/zehn-regeln-fuer-die-informationssicherheit-im-kmu.html. Zugegriffen: 17. Mai 2018.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64,* 122–134. https://doi.org/10.1016/j.cose.2015.07.002.

KPMG. (2017). Clarity on Cybersicherheit. https://assets.kpmg.com/content/dam/kpmg/ch/pdf/clarity-on-Cybersicherheit-2017-en.pdf. Zugegriffen: 4. Juni 2018.

Mäder, L. (11. Dez. 2017). KMU sollen eine Grundhygiene für IT-Sicherheit beachten. *Neue Zürcher Zeitung*. https://www.nzz.ch/schweiz/kmu-sollen-eine-grundhygiene-fuer-it-sicherheit-beachten-ld.1337191. Zugegriffen: 17. Mai 2018.

Manso, C. G., Rekleitis, E., Papazafeiropoulos, F., & Maritsas, V. (2015). Information security and privacy standards for SMEs. https://www.enisa.europa.eu/publications/standardisation-for-smes. Zugegriffen: 11. Mai 2018.

Melde- und Analysestelle Informationssicherung (MELANI), & Swiss Government Computer Emergency Response Team (GovCERT). (2016) Merkblatt IT-Sicherheit für KMU. https://www.melani.admin.ch/dam/melani/de/dokumente/2015/01/merkblatt_it-sicherheitfuerKMU.pdf.download.pdf/merkblatt_it-sicherheitfuerKMU.pdf. Zugegriffen: 10. Apr. 2018.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly, 33*(1), 71–90. https://doi.org/10.2307/20650279.

Pavlou, P. A., & Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *MIS Quarterly, 30*(1), 115–143. https://doi.org/10.2307/25148720.

Renaud, K. (2016). How smaller businesses struggle with security advice. *Computer Fraud & Security, 2016*(8), 10–18. https://doi.org/10.1016/S1361-3723(16)30062-8.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology, 91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803.

Schwyter, F., & Wisler, A. (2013). *Informationssicherheit für KMU. Sicherheitskonzepte & praktische Umsetzung* (2. Aufl.). Rheinfelden: BPX-Edition.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255–276. https://doi.org/10.1287/isre.1.3.255.

Taylor, S., & Todd, P. A. (1995). Understanding information technology usage – A test of competing models. *Information Systems Research, 6*(2), 144–176. https://doi.org/10.1287/isre.6.2.144.

Tu, Z., & Yuan, Y. (2014). Critical success factors analysis on effective information security management: A literature review. In: Association for Information Systems (Hrsg.), *20th Americas Conference on Information Systems (AMCIS 2014): Smart sustainability: The information systems opportunity* (S. 1874–1886). Red Hook: Curran.

Woodhouse, S. (2008). Critical success factors for an information security management system. In: Fifth international conference on information technology & applications 2008: ICITA2008, D. Tien, & M. Kavakli (Hrsg.), (S. 244–249). Bathurst: Macquarie Scientific Publishing.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science, 46*(2), 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425–478. https://doi.org/10.2307/30036540.

Yin, R. K. (2014). *Case study research. Design and methods* (5. Aufl.). Los Angeles: Sage.

Zürich Versicherungs-Gesellschaft. (2016). Schweizer KMU sind nicht vor Cybercrime geschützt. Abgerufen von https://www.zurich.ch/de/ueber-uns/medien/medienmitteilungen/2016/20161123-medienmitteilung. Zugegriffen 4. Nov. 2017.

Meier, Dominique Adrian (M.Sc. WI/me@dominiquemeier.ch) Konsekutives Masterstudium in Wirtschaftsinformatik an der Zürcher Fachhochschule für Angewandte Wissenschaften. Langjährige Tätigkeit als Berater im Bereich IT- und Informationssicherheit. Aktuell als Partner & Head of Operations in der Geschäftsleitung bei einem auf Informationssicherheit spezialisierten Schweizer Beratungsunternehmen (https://www.redguard.ch).

Burda, Daniel (Prof. Dr./daniel.burda@h-da.de) ist Professor für Wirtschaftsinformatik am Fachbereich Informatik der Hochschule Darmstadt. Zuvor war er an der Berner Fachhochschule als Professor für Wirtschaftsinformatik tätig. Vor seiner Berufung zum Professor war Herr Burda mehrere Jahre als SAP und Business Process Consultant u.a. bei SAP in Deutschland und der Schweiz tätig.