Forschungsbericht

Informationssicherheitsschulung für KMU

Potenziale erschließen, Bewusstsein stärken

Funded by the
Erasmus+ Programme
of the European Union

TeBelSi

Funded by the
Erasmus+ Programme
of the European Union

Dieses Dokument entstand im Rahmen des ERASMUS+ Projektes „Teilzertifizierung im Berufsfeld Informationssicherheit – TeBeISi“, Projektnummer: 2018-1-EN02-KA202-005218.

Inhalt

1 Einführung: Teilzertifizierung in Informationssicherheit 1
2 Literaturübersicht 2
3 TeBeISi - Methode und Ansatz 6
3.1 Forschungsthema 6
3.2 Methode 8
4 Studie: Bildung und Ausbildung im Bereich der Informationssicherheit für KMU 10
4.1 Beschreibung der Daten 10
4.2 Analyse 12
4.2.1 Unternehmenskultur 12
4.2.2 Zuständigkeiten im Unternehmen 14
4.2.3 Informationssicherheit in KMU 17
4.2.4 Informationssicherheit im Unternehmen: Anforderungen an das Personal 19
4.2.5 Selbsteinschätzung der Kompetenzen 24
4.2.6 Persönlichkeit (Big Five) 24
4.2.7 Arbeitsleistung 27
4.3 Zusammenfassung 29
5 Leitfaden für KMU 30
6 Ausblick und Empfehlungen 33
7 Literatur 34

Abbildungsverzeichnis

Abbildung 1: Ein Ausweg - Die TeBeISi-Lösung zur Überwindung der Qualifikationslücke auf dem Arbeitsmarkt für Informationssicherheit. 6
Abbildung 2: Die TeBeISi-Forschungsagenda 8
Abbildung 3. Für den Erfolg entscheidende Kompetenzen 8
Abbildung 4: "Welche Unternehmen nehmen an der Umfrage teil?" 11
Abbildung 5 : "In welchem Wirtschaftszweig ist Ihr Unternehmen tätig?" 11
Abbildung 6: "Was ist Ihre Rolle im Unternehmen?" 11
Abbildung 7 : "In welchem Land ist Ihr Unternehmen hauptsächlich tätig?" 12
Abbildung 8: "Wie sieht die Geschlechterverteilung aus?" 12
Abbildung 9: Merkmale in den folgenden Kategorien "Strategie, Struktur, Führung, Zusammenarbeit" - alle Unternehmen 14
Abbildung 10: Merkmale, gruppiert in die folgenden Kategorien "Strategie, Struktur, Führung, Zusammenarbeit" - Unternehmen mit und ohne Informationssicherheitsstrategie 14
Abbildung 11 : Kompetenzen im Unternehmen - Ergebnisse 16
Abbildung 12 : Analyse der Kompetenzen in KMU 17
Abbildung 13 : "Welche Gründe haben Ihr Unternehmen bisher davon abgehalten, in die Verbesserung der Informationssicherheit zu investieren?" 18
Abbildung 14 : "Welche Art von Ausbildung oder Schulung ist Ihrer Erfahrung nach für einen Mitarbeiter, der in Ihrem Unternehmen mit der Gewährleistung der Informationssicherheit betraut ist, notwendig/hilfreich/optional?" 18
Abbildung 15 : Mögliche Optionen zur Erhöhung der Informationssicherheit 19
Abbildung 16 : "Sind Ihnen in den letzten 2 Jahren Vorfälle im Bereich der Informationssicherheit bekannt oder besteht der Verdacht auf einen Sicherheitsvorfall?" 19
Abbildung 17 : "Gibt es in Ihrem Unternehmen Mitarbeiter, die formell für die Informationssicherheit verantwortlich sind? (oben) - Wenn ja, wie viele?" (unten) in 20
Abbildung 18 : "Wie viele offene Stellen im Bereich der Informationssicherheit gibt es in Ihrem Unternehmen?" 21
Abbildung 19: Unternehmenszertifizierung für Informationssicherheit 21
Abbildung 20: "Wie gehen Sie bisher mit dem Personalbedarf im Bereich der Informationssicherheit um?" 22
Abbildung 21: "Wie gehen Sie bisher mit dem Personalbedarf im Bereich der Informationssicherheit um?" - IS und kein IS 23
Abbildung 22: "Bitte schätzen Sie sich selbst ein: Welche der folgenden Bildungs- und Ausbildungsaktivitäten können Sie durchführen?" 24
Abbildung 23: Big-Five-Histogramme für Praktiker der Informationssicherheit. 26
Abbildung 24: Big-Five, Mittelwertvergleich 26
Abbildung 25: Aufgabenerfüllung 28
Abbildung 26: Kontraproduktives Verhalten 28
Abbildung 27 : Kontextbezogene Leistung 28
Abbildung 28: IWPQ-Ergebnisse für Informationssicherheitsexpert*innen 28
Abbildung 29: Leitlinien auf der Grundlage gemeinsamer Probleme, mit denen KMU im Bereich Informationssicherheit und Datenschutz konfrontiert sind 32

Tabellenverzeichnis

Tabelle 1: "Bitte geben Sie an, inwieweit die folgenden Merkmale das Unternehmen, für das Sie arbeiten, oder die Organisation, für die Sie arbeiten, beschreiben". 13
Tabelle 2: "Aufgaben und Tätigkeiten im Bereich der Informationssicherheit" 15
Tabelle 3: Dimensionen der Big-5. 25
Tabelle 4: Aufbau des BFI-10 25
Tabelle 5: "Validitätstest: Korrelation zwischen Items und Gruppen" 27

1 Einführung: Teilzertifizierung für Informationssicherheit

Die Informationssicherheit hat in den letzten Jahren stark an Bedeutung gewonnen. Angesichts der zunehmenden Zahl von Datenschutzverletzungen, der Geiselnahme von Unternehmen durch internationale Malware-Angriffe und des strategischen Einsatzes von Cyber-Kriegsführung als Mittel zur Ausweitung der politischen Macht in fremden Sphären wird die Digitalisierung nicht mehr nur als rettende Lösung für angeschlagene Unternehmen gesehen, sondern auch als eine wesentliche Risikoquelle, die umfangreiche Schutzmaßnahmen erfordert. Risiken entstehen in vielen verschiedenen Kontexten, können aber in zwei Bereichen begründet sein: vor Ort und im Cyberspace.

Es sind ganzheitliche Ansätze erforderlich, um die bestehende und zunehmende Bedrohungslage zu bewältigen. Angesichts diffuser und nicht greifbarer Risikoszenarien neigen Einzelpersonen, sowohl im privaten als auch im unternehmerischen Bereich, dazu, die Bedeutung des Festhaltens von Informationssicherheitsrisiken als Mittel für eine nachhaltige Unternehmensführung und -verwaltung zu vernachlässigen. Um diesen weit verbreiteten Mangel an Bewusstsein, der sich von der öffentlichen Sphäre auf die Unternehmenswelt überträgt, zu überwinden, müssen Maßnahmen zur Bewusstseinsbildung, Sensibilisierung und Ausbildung ergriffen werden. Unternehmen müssen inzwischen verstehen, wie sie das Thema Informationssicherheit mit einer individuellen Strategie angehen können, die zum eigenen Bedarf und zum eigenen Budget passt. Um Unternehmen bei dieser Herausforderung zu unterstützen, wurde die Studie "Information Security Education for SMEs" durchgeführt. Die Studie setzte sich zum Ziel, den Ausbildungs- und Personalbedarf von KMU zu beleuchten, um Lösungen für den anhaltenden Fachkräftemangel zu finden.

Der Untertitel "Potenziale erschließen, Bewusstsein stärken" gibt dabei einen Hinweis auf die wichtigste Ressource: das vorhandene Personal in KMU. Viele Mitarbeiter*innen verfügen über Fähigkeiten und Kenntnisse, die sie im Laufe ihrer beruflichen Laufbahn erworben haben, ohne dass sie sich dessen oft gar nicht bewusst sind. Der Erwerb von nicht-formalem und informellem Lernen, insbesondere in technologie- und innovationsgetriebenen Branchen wie der Informationssicherheit, stellt eine reiche Ressource dar, die durch Kompetenzvalidierung und -anerkennung erschlossen werden kann. Zur Erleichterung des Anerkennungsprozesses hat das TeBeISi-Projektteam Lerneinheiten entwickelt und stellt mit Unterstützung der vorliegenden Studie Werkzeuge und Ressourcen für KMU bereit, um geeignete Mitarbeiter*innen für die Übernahme neuer Aufgaben im Bereich der Informationssicherheit zu identifizieren.

Das TeBeISi-Projekt will einen Beitrag zur Geschäftspraxis leisten und die tägliche Realität von KMU in der gesamten EU berücksichtigen. Diese Studie vertieft das Verständnis von Entscheidungsträgern, Personalverantwortlichen und interessierten Personen im Bereich der Informationssicherheit und der Entwicklung von Werten und Anforderungen der Informationssicherheit und des Informationssicherheitspersonals in KMU. Um dieses Ziel zu erreichen, ist die Studie wie folgt gegliedert: Kapitel zwei gibt einen Überblick über die bestehende Forschung zur Informationssicherheit in KMU und zu den Personalanforderungen, Kapitel drei liefert Hintergrundinformationen zur TeBeISi-Forschungsmethodik und zum Kontext, in dem diese Studie konzipiert wurde, Kapitel 4 stellt die Ergebnisse des quantitativen Fragebogens vor, Kapitel fünf leitet kurz die wichtigsten Leitlinien für KMU ab und Kapitel sechs schließt mit einem Ausblick auf zukünftige Entwicklungen.

2 Literaturübersicht

Der Einsatz von Informationssystemen und Informationstechnologie ist zu einer Voraussetzung für den Erfolg von Unternehmen in allen Wirtschaftsbereichen geworden. Ohne Informationstechnologie ist die Arbeit mit Informationen nicht nur ineffektiv, sondern auch unmöglich (Hallová et al. 2019) . Darüber hinaus nimmt unsere Abhängigkeit von diesen Systemen jeden Tag zu. Mit der rasanten Entwicklung moderner Technologien und Informationssysteme steigt jedoch auch das Missbrauchspotenzial (Smith, 2003; Leede et al., 2005; Kumar et al., 2011).

In der heutigen Welt, in der alle Menschen und Unternehmen von der Informationstechnologie abhängig sind, sind Informationssicherheit und Datenschutz wichtige Elemente, die besondere Aufmerksamkeit erfordern. In dieser Hinsicht sind die Richtlinie der Europäischen Union (EU) über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus für Netz- und Informationssysteme in der gesamten Union [1]und die allgemeine Datenschutzverordnung [2](Kogenhop, 2020) wichtige Faktoren. Die Regulierungsinitiative der Europäischen Kommission spiegelt den gestiegenen Bedarf an gesetzgeberischen Leitlinien wider, da die rasanten technologischen Entwicklungen und die Globalisierung neue Herausforderungen für den Schutz personenbezogener Daten und Informationen geschaffen haben (Wilkinson, 2018).

In den letzten Jahren haben neue Formen der Informationstechnologie (z. B. Sensoren und mobile Geräte) die Möglichkeiten der Messung und Analyse drastisch erweitert, was völlig neue Herausforderungen für Sicherheit und Datenschutz mit sich bringt (Weber, 2010; Newell & Marabelli, 2015; Sicari, Rizzardi, Grieco, & Coen-Porisini, 2015; Lee, Cho & Lim, 2018). Das Potenzial, dass Klient*innen von Sicherheits- und Datenschutzfragen im Zusammenhang mit Informationssystemen betroffen sind, macht diese Herausforderungen zu einem zentralen Thema für Geschäftspraktiker (Sicari et al., 2015; Sicari et al., 2016). Auf der anderen Seite müssen Manager von Organisationen neue Informationstechnologien nutzen, um nicht nur personenbezogene, sondern auch vertrauliche Daten zu speichern, um im 21. Jahrhundert wettbewerbsfähig zu bleiben. Die papiergestützte Datenspeicherung ist aufgrund des Potenzials der elektronischen Datenspeicherung inzwischen überholt, Organisationen übernehmen rasch neue Technologien, und die elektronische Speicherung ist in vielen Ländern alltäglich geworden (McAfee, 2010).

Der wachsende Trend zur Speicherung von Daten in elektronischer Form sowie die zunehmende Konnektivität des Internets und die daraus resultierende Gefährdung durch Cyber-Kriminelle haben zur Entwicklung spezifischer Datenschutzanforderungen geführt (McAfee, 2010). Datenspeichertechnologien müssen über Datenschutzmaßnahmen verfügen, und Nutzer*innen, die mit den Daten arbeiten, müssen so geschult werden, dass sie die Risiken des Abflusses von Unternehmensdaten an Unbefugte verstehen. Die Verantwortlichen in Unternehmen müssen sich der schwerwiegenden Folgen von elektronischen Datenlecks bewusst sein. Ebenso wie die Mitarbeiter*innen, die sich nicht an die Informationssicherheit

[1] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus für Netz- und Informationssysteme in der Union 2016.

[2]Europäische Union 2016.

halten (Siponen, Mahmood & Pahnila, 2009), setzen Manager von Organisationen, die bei der Beschaffung und Verwaltung elektronischer Daten nachlässig sind, ihre Unternehmen Risiken und Bedrohungen aus (Northhouse, 2010). Manager müssen Vorsicht und Selbstbeherrschung walten lassen, um das Unternehmen zu schützen, insbesondere im Hinblick auf die Datensicherheit (Guinote & Vescio, 2010). Eine der wichtigsten Herausforderungen im Bereich des Informationssicherheitsmanagements besteht darin, zu verstehen, wie organisatorische, individuelle und technische Faktoren zusammenwirken, um die Ergebnisse der Informationssicherheit in einer Organisation zu beeinflussen (Wilkinson, 2018).

Jüngste Untersuchungen zeigen, dass in vielen Fällen elektronische Datenverluste in kleinen Unternehmen das Ergebnis schlechter Führungs- und Managementpraktiken sind. Manager in Organisationen treffen die wichtigsten Entscheidungen, und wenn sie sich nicht richtig mit Fragen der Informationstechnologie befassen, gefährden sie das Überleben des Unternehmens (Davies & Hertig, 2008). Ein möglicher mildernder Faktor wurde von Noguerol und Branch vorgeschlagen. (2018) Sie argumentieren, dass Unternehmensleiter*innen das Verhalten der Mitarbeiter*innen im Bereich der Datensicherheit positiv beeinflussen können, indem sie ein gesundes Arbeitsumfeld fördern und zwischenmenschliche Beziehungen pflegen.

Unternehmen aller Größenordnungen auf der ganzen Welt leiden unter einem Mangel an Cybersicherheit, und viele von ihnen sind der Cyberkriminalität ausgesetzt. Elektronische Datenverluste sind jedoch vor allem für kleinere Unternehmen ein Problem. KMU sind unter anderem mit finanziellen Zwängen, manchmal ineffektiven Manager*innen und mangelnder Aufmerksamkeit für kleine Probleme konfrontiert, die nicht direkt mit dem Geschäft zusammenhängen (O'Rourke, 2003; Adamkiewicz, 2005; Goodwin, 2005; Baker & Wallace, 2007).

Trotz der zunehmenden Bedrohung durch Cybervorfälle von außen bleiben Mitarbeiter und Mitarbeiterinnen die Hauptquelle für Sicherheitsvorfälle (Richardson, 2008; PwC, 2017). Humanressourcen innerhalb des Unternehmens können gefährlicher sein als solche außerhalb des Unternehmens, da sie mit den Informationssystemen des Unternehmens vertraut sind und durch ihre normalen Arbeitstätigkeiten auf Daten zugreifen (Herath & Rao, 2009a, 2009b; Bulgurcu, Cavusoglu, & Benbasat, 2010; Johnston & Warkentin, 2010; Siponen & Vance, 2010). Informationssicherheitsrichtlinien sollen die Sicherheit von Informationen gewährleisten (Bulgurcu, Cavusoglu, & Benbasat, 2010), aber Untersuchungen zeigen, dass viele Sicherheitsvorfälle dadurch verursacht werden, dass die Mitarbeiter*innen die Sicherheitsrichtlinien ignorieren oder sich ihrer nicht bewusst sind (Willison & Warkentin 2013, Path to Cyber Resilience, 2016).

Forscher und Praktiker betrachten die organisatorische Informationssicherheit zunehmend als ein soziotechnisches Thema, das nicht nur technische, sondern auch Managementansätze erfordert (Burns, Roberts, Posey, Bennett, & Courtney, 2018). Aufgrund des weit verbreiteten Einsatzes von Informationstechnologie in Unternehmen wird den Mitarbeiter*innen häufig ein ständiger Zugang zu Unternehmensinformationen und Informationssystemen gewährt, um ihre beruflichen Aufgaben zu erfüllen. Trotz dieser erhöhten betrieblichen Flexibilität sind Organisationen weniger in der Lage, das Verhalten von Mitarbeitern und Mitarbeiterinnen mit Zugang zu vertraulichen Daten zu überwachen (Herath & Rao, 2009). Um den Schutz der wertvollen Informationsressourcen von Organisationen im Kontext der zunehmenden Verbreitung von Technologie zu verbessern, ist daher eine proaktive Schulung der Mitarbeiter*innen in Sachen Informationssicherheit von zentraler Bedeutung für die Informationssicherheit von Organisationen (von Solms & von Solms, 2009; D'Arcy, Hovav &

Galletta, 2009; Albrechtsen & Hovden, 2010; Puhakainen & Siponen, 2010; Karjalainen & Sipo-nen, 2011; Posey, Roberts, Lowry, Bennett & Courtney, 2013). Untersuchungen zeigen, dass Unternehmen Programme zur Sensibilisierung der Mitarbeiter*innen als oberste Priorität in ihren Budgets für die Informationssicherheit ansehen (PWC, 2015), und Führungskräfte im Bereich der Informationssicherheit geben an, dass Mitarbeiterschulungen zu den wichtigsten Aktivitäten gehören, die für die Umsetzung einer erfolgreichen Informations- und Datensicherheitsstrategie erforderlich sind (van Zadelhoff, Lovejoy & Jarvis, 2014).

Mitarbeiterschulungen sind das wirksamste nichttechnische Mittel, um die Informationssicherheit in Organisationen zu gewährleisten und zu verhindern, dass Mitarbeiter*innen sensible Informationen an Unbefugte weitergeben (Colwill, 2009; Peikari, Shah, & Lo, 2018). Schulungen können das Wissen und das Bewusstsein der Mitarbeiter*innen über die Bedrohungen und Folgen einer Sicherheitsverletzung erhöhen und dazu beitragen, solche Vorfälle zu verhindern (Kluge, 2007; D'Arcy Hovav & Galletta, 2009).

Die Aus- und Weiterbildung der Mitarbeiter*innen ist ein Mittel für Organisationen, um das Risiko interner Sicherheitsmängel zu verringern (Burns, Roberts, Posey, Bennett & Courtney, 2015; Barlow, Warkentin, Ormond, & Dennis, 2018). Sie ist eine wichtige Voraussetzung und wirkt sich positiv auf das Informationssicherheitsverhalten aus. Gut konzipierte Mitarbeiterschulungsprogramme können dazu beitragen, Informationssicherheitsrisiken für eine Organisation zu reduzieren (Anderson & Agarwal, 2010; Liang & Xue, 2010; Bulgurcu, Cavusoglu, & Benbasat, 2010; Johnston & Warkentin, 2010; Whitman & Mattord, 2012; Jenkins & Durcikova, 2013; Johnston, Warkentin & Siponen, 2015). Forschern zufolge (Gardner & Thomas, 2014; Posey, Roberts & Lowry, 2015) ist die kontinuierliche Aus- und Weiterbildung von Mitarbeiter*innen im Bereich der Daten- und Informationssicherheit ein wirksames Mittel, um ihr Verhalten in Bezug auf die Informationssicherheit und die Einhaltung der Informationssicherheitspolitik eines Unternehmens zu beeinflussen. Mitarbeiter*innen mit angemessenen Kenntnissen im Bereich der Informationssicherheit sind in der Lage, Bedrohungen und Angriffen vorzubeugen, was zu einer erhöhten Vertraulichkeit, Integrität und Verfügbarkeit von Informationen innerhalb der Organisation führt (Sabeeh & Lashkari, 2011). Es wird darauf hingewiesen, dass aufgrund der dynamischen Natur der Bedrohungen und Schwachstellen der Informationssicherheit die Schulung und Ausbildung der Mitarbeiter und Mitarbeiterinnen eine regelmäßige und kontinuierliche Praxis in einer Organisation sein sollte (Yoo et al., 2018; McConnell, 2020).

Obwohl die Verarbeitung personenbezogener Daten für viele KMU unvermeidlich ist, gehört sie häufig nicht zu ihrem Kerngeschäft, und es fehlt ihnen an ausreichenden personellen oder finanziellen Ressourcen, um die Einhaltung der Vorschriften zu gewährleisten. Vor allem KMU sind nicht bereit, Maßnahmen zur Informationssicherheit zu ergreifen, weil sie aufgrund ihrer geringen Größe nicht zu einer dokumentierten Informationssicherheit verpflichtet sind (Kuusisto, & Ilvonen, 2003; Doherty, & Fulford, 2005). KMU sind sich der Datenschutz-Grundverordnung meist bewusst, verfügen aber nicht über die Ressourcen, um die Anforderungen zu erfüllen; ihnen fehlt die organisatorische Kapazität, um die Anforderungen der Datenschutz-Grundverordnung und der Informationssicherheit in ihrem Unternehmen umzusetzen. Zu den häufigsten Herausforderungen für den Datenschutz und die Informationssicherheit, mit denen KMU konfrontiert sind, gehören: das Verständnis dafür, welche Änderungen vorgenommen werden müssen, um die Anforderungen zu erfüllen; die Gestaltung und Entwicklung neuer Prozesse und Verfahren im Zusammenhang mit der Verarbeitung personenbezogener Daten; und die Sensibilisierung der Mitarbeiter*innen für die Bedeutung des Datenschutzes. Trotz zahlreicher Stellungnahmen und Leitlinien zur DSGVO, die von Regulierungsbehörden und Datenschutzexpert*innen herausgegeben wurden, mangelt es an praktischen, leicht verständlichen und gezielten Anleitungen für KMU, wie die Datenschutzvorschriften in der Praxis umgesetzt werden können (Jasmontaitė-Zaniewicz, Calvi, Nagy & Barnard-Wills, 2021). Darin wird hervorgehoben, dass insbesondere KMU gezielte, sektorspezifische Schulungen und Beratung auf der Grundlage von Beispielen und Fallstudien benötigen, die die Besonderheiten dieser Organisationen widerspiegeln (Barnard-Wills, Cochrane, Matturi, & Marchetti, 2019).

3 TeBeISi - Methode und Ansatz

Die Informationssicherheit in KMU ist bisher ein wenig untersuchtes Thema, und es ist nicht viel über die Bedürfnisse und Anforderungen von KMU in der EU bekannt. Während die gesetzliche Verpflichtung zum Datenschutz (GDPR) zu einem raschen Anstieg der ergriffenen Maßnahmen und des Bewusstseins der KMU geführt hat, wurde die Informationssicherheit von vielen Unternehmen eher als "nice to have" behandelt - und nicht mit viel Aufwand oder Engagement verfolgt. Die Einführung von Informationssicherheits-Managementsystemen oder die Zertifizierung von Unternehmen und Einzelpersonen dringt nur langsam in das Bewusstsein von Mitarbeiter*innen und Firmeninhaber*innen vor. Es hat sich jedoch gezeigt, dass von den vielen Faktoren, die die Sicherheit eines Unternehmens ausmachen, der menschliche Faktor, d.h. der Mitarbeiter/die Mitarbeiterin, das Management und letztlich der Beauftragte für Informationssicherheit, den größten Unterschied ausmachen kann.

Das TeBeISi-Projekt verfolgte das Ziel, Einblicke in den Stand der Informationssicherheit in KMU zu geben und tiefere Einblicke in die Aus- und Weiterbildungsmöglichkeiten für KMU zu gewinnen, um den Fachkräftemangel zu überwinden.

3.1 Forschungsthema

Die Forschungsagenda, auf die sich das TeBeISi-Projekt stützt, beruht im Wesentlichen auf drei iterativen Schritten: erstens Benchmarking gängiger Praktiken (IO1 und IO2), zweitens Bedarfsanalyse (IO3) und Entwicklung geeigneter Instrumente und Empfehlungen für Unternehmen, Einzelpersonen und Bildungseinrichtungen (IO4 und IO5). Durch die Analyse der Marktsituation, insbesondere der Rolle bestehender Zertifizierungen und Instrumente im Kontext von Kompetenzanerkennung und Transparenz. Aus der Bedarfsanalyse wurde ein Prozess entwickelt, der in **Abbildung 1**dargestellt ist.

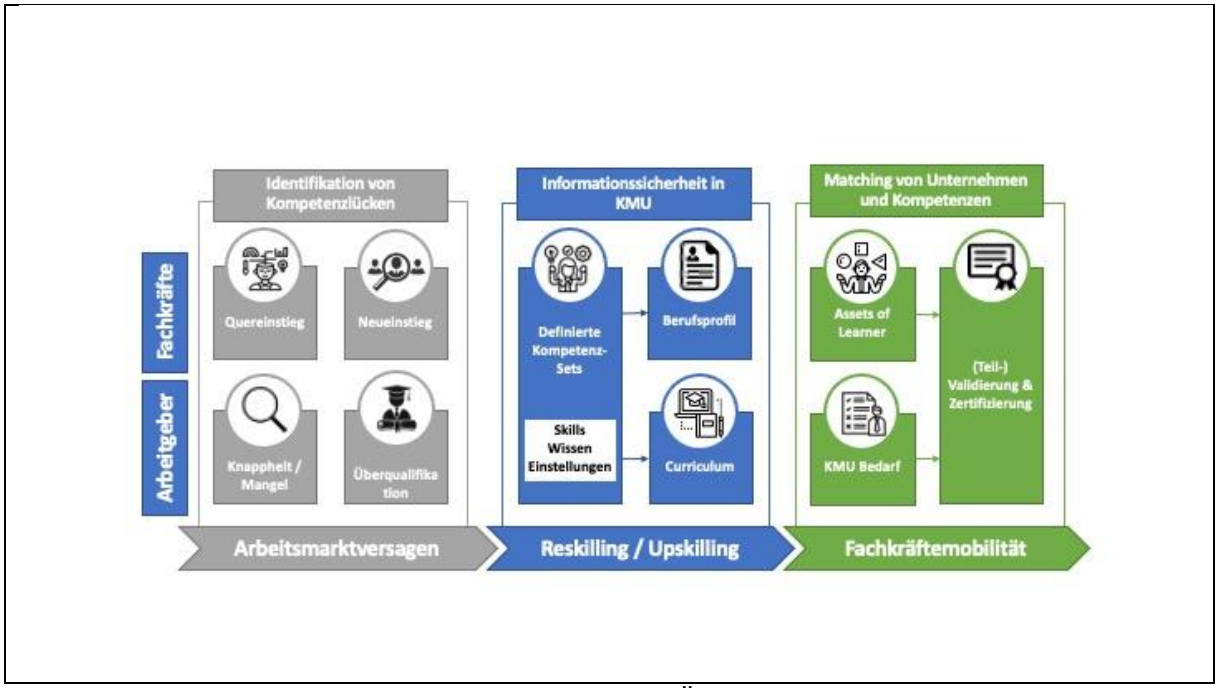


Abbildung 1: Ein Ausweg - Die TeBeISi-Lösung zur Überwindung der Qualifikationslücke auf dem Arbeitsmarkt für Informationssicherheit.

Kurz gesagt, die bestehenden Verkrustungen auf dem Arbeitsmarkt lassen sich in zweierlei Hinsicht beschreiben: Zum einen gibt es einfach nur eine geringe Anzahl von Fachkräften, die auf dem Markt verfügbar sind. Diese Knappheit wird noch dadurch verschärft, dass die meisten verfügbaren Spezialisten hoch qualifiziert sind - oft zu hoch, da sie für KMU zu teuer werden. Die derzeitige Praxis in den Unternehmen ähnelt der des gesamten IT-Sektors: Viele Quereinsteiger werden in der Branche aktiv, und völlig neue Arbeitskräfte beginnen ihre Karriere in diesem zukunftsträchtigen Bereich. Die im Rahmen des TeBeISi-Projekts entwickelte Lösung beginnt folglich mit der Analyse der in KMU erforderlichen Kenntnisse und Kompetenzen, um einen spezifischen Lehrplan zu erstellen, der auf die Bedürfnisse von KMU zugeschnitten ist. Es hat sich gezeigt, dass sich die Anforderungen in KMU nicht nur in Bezug auf die Qualifikation stark von den Anforderungen in größeren Unternehmen unterscheiden, weshalb das Projekt ein anderes Berufsprofil vorschlägt, um diese Unterschiede zu berücksichtigen. Das Berufsbild und der Lehrplan basieren auf den ermittelten Kompetenzen der KMU. Schließlich unterstützt eine Überprüfung der Bedürfnisse der Unternehmen und der Kompetenzen der Mitarbeiter*innen die Unternehmen bei der Identifizierung geeigneter Kandidat*innen, die über wertvolle Fähigkeiten für die Arbeit im Bereich der Informationssicherheit verfügen und bereit sind, sich weiterzubilden und ihre Karriere in einem neuen Bereich voranzutreiben. Die Investition in vorhandenes Personal und die Weiterbildung der eigenen Arbeitskräfte wird dabei als die wirtschaftlichste Möglichkeit für Unternehmen und Arbeitnehmer angesehen, den Qualifikationsbedarf zu überwinden.

Die vorliegende Studie unterstützt diese Agenda in mehrfacher Hinsicht: Erstens zielt sie darauf ab, die Anforderungen aus einer Managementperspektive zu ermitteln, wobei Einstellungsstrategien, offene Stellen, das Bewusstsein für Informationssicherheit und die Unternehmenskultur berücksichtigt werden. Zweitens werden die technischen Anforderungen bewertet, wobei insbesondere soziale, aber auch technische Fähigkeiten berücksichtigt werden. Für beide Bereiche wurden in einer Reihe von Experteninterviews und Fokusgruppen Items entwickelt. Daher bietet der vorliegende Fragebogen drittens eine Bestätigung und Peer-Validierung der Ergebnisse, die mit Hilfe eines Forschungsdesigns mit gemischten Methoden gewonnen wurden.

3.2 Methode

Das Mixed-Methods-Forschungsdesign, das zur Entwicklung von Kompetenzprofilen und dem TeBeISi-Lehrplan geführt hat, besteht aus vier zentralen Elementen, deren Ergebnisse während der gesamten Projektdurchführung iterativ angeregt und genutzt wurden Zunächst wurden im Rahmen einer Sekundärforschung Zertifizierungen und Berufsprofile analysiert, was Einblicke in die erlernten und die von den auf dem Markt tätigen Praktikern erwarteten Kompetenzen ermöglichte. Diese Untersuchung wurde jedoch durch die Feststellung eingeschränkt, dass der spezifische Fall der KMU kaum berücksichtigt wird und dass es unklar bleibt, was die grundlegenden Bedürfnisse eines KMU von den fortgeschritteneren Anforderungen größerer Betriebe unterscheidet. Daher wurde der Schwerpunkt auf die detaillierte Beobachtung des KMU-Kontextes gelegt, einschließlich der Einbeziehung verschiedener KMU-Akteure (Unternehmer, Handelskammern, spezifische Forscher usw.), der Berücksichtigung KMU-spezifischer Literatur und der Analyse KMU-spezifischer Zertifizierungsprozesse und verfügbarer Kurse in den Partnerländern.

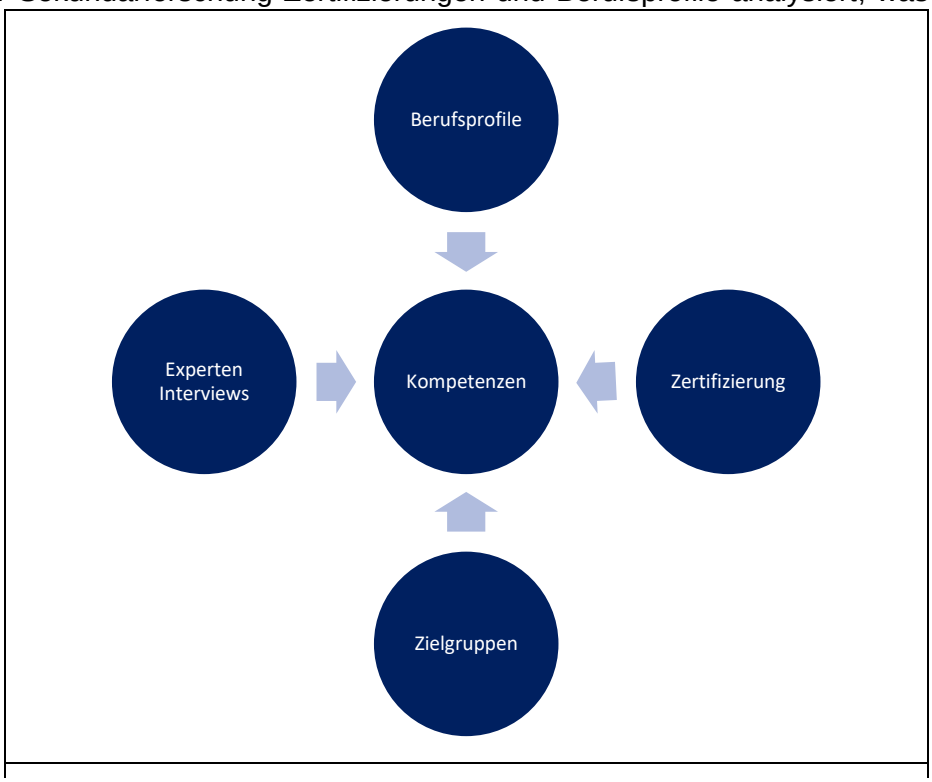


Abbildung 2: Die TeBeISi-Forschungsagenda

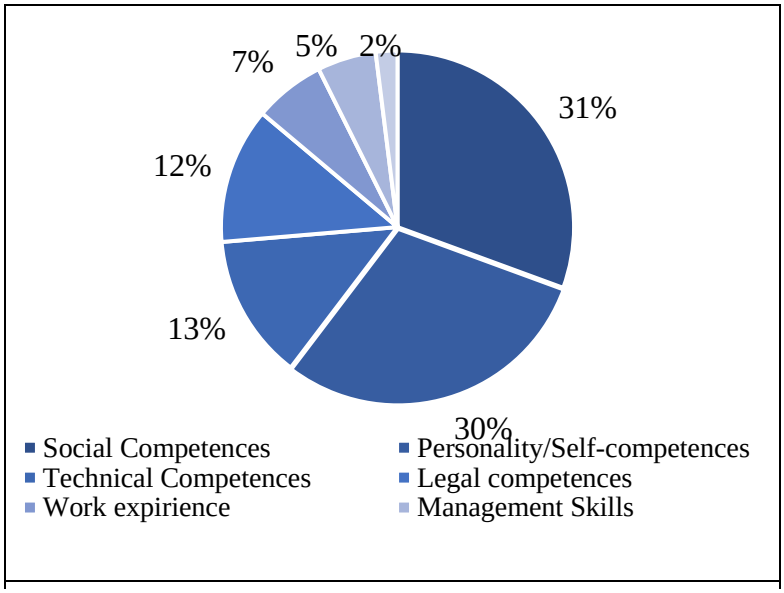


Abbildung 3. Für den Erfolg entscheidende Kompetenzen

Im Rahmen einer Reihe von Experteninterviews und Fokusgruppen, die in Litauen, Italien, Deutschland und Polen mit Arbeitgebern, Arbeitnehmern und Bildungsanbietern durchgeführt wurden, wurden die Kompetenzen von Fachleuten für Informationssicherheit analysiert. Aus der qualitativen Analyse wurden eingehende Informationen über die Bedeutung technischer, methodischer, sozialer und persönlicher Fähigkeiten gewonnen und spezifische Elemente in jeder Kategorie ermittelt. Die gesamte Analyse ist in dem Dokument "Information Security Competences - a qualitative analysis of Expert Interviews on Knowledge and Skills of Professionals in Information Security" verfügbar.

Die ermittelten Einzelpunkte wurden umformuliert und zu Lerneinheiten nach dem ECVET-Standard der Lernergebnisse (vgl. IO4) gebündelt. In der vorliegenden Erhebung wurden diese Einheiten nach Häufigkeit und Wichtigkeit in den Betrieben bewertet, so dass die Endergebnisse Aufschluss über die Prioritäten der Betriebe und die dringendsten Aufgaben geben.

4 Studie: Bildung und Ausbildung im Bereich der Informationssicherheit für KMU

Im Rahmen des Projekts führte die TeBeISi-Projektgruppe die Umfrage "Informationssicherheitsausbildung für KMU" mit dem Ziel durch, Einblicke in die aktuelle Praxis der Informationssicherheit in kleinen und mittleren Unternehmen, den Bedarf an Wissen, Fähigkeiten und Kompetenzen und die Aussichten der KMU, mit den bestehenden Herausforderungen der knappen Ressourcenverfügbarkeit umzugehen, zu gewinnen. Die Umfrage zur Informationssicherheitsausbildung für KMUs zielt darauf ab, die Kenntnisse und das Fachwissen in spezifischen Teilbereichen des Berufsfeldes der Informationssicherheit in kleinen und mittleren Unternehmen zu ermitteln. Die Befragung wurde über Limesurvey durchgeführt. In einem Zeitraum von ca. 6 Wochen haben 160 Teilnehmer*innen, Informationssicherheitsspezialist*innen, Inhaber*innen und Geschäftsführer*innen von KMUs sowie Rekrutierungs- und IT-Expert*innen auf die Online-Umfrage geantwortet, die in den Projektpartnerländern, hauptsächlich in Polen, Deutschland, Litauen, Italien und Österreich, verbreitet wurde.

Die Studie setzt sich aus zwei Hauptaspekten zusammen: Einerseits wurden die Anforderungen aus der Sicht der Personalverantwortlichen, d. h. der Personalabteilungen und der Unternehmenseigentümer, ermittelt, wobei der Schwerpunkt auf den wichtigsten Aspekten lag, die sie während des gesamten Einstellungsverfahrens berücksichtigen. Andererseits wurden IT-Abteilungen und Informationssicherheitsspezialisten gebeten, ihre Sicht der technischen Anforderungen und des Kompetenz-Benchmarkings für neue Mitarbeiter*innen in diesem Sektor darzulegen. Außerdem wurden beide Adressen gebeten, Angaben zur Unternehmenskultur und zu den Persönlichkeitsmerkmalen erfolgreicher Mitarbeiter zu machen. Zu diesem Zweck wurden validierte Items aus Ingela et al. (2005) für Unternehmenskultur und Ramos-Villagrasa et al. (2019) für Arbeitsleistung verwendet. Für den Fragebogen wurden die Skalen in 5-Punkte-Likert-Skalen rücktransformiert. Den Teilnehmer*innen wurden je nach ihrer Position Fragen vorgelegt. Der Fragebogen wurde im Rahmen von IO3 des TeBeISi-Projekts entwickelt und ist zusammen mit den übrigen Projektdokumenten verfügbar.

4.1 Beschreibung der Daten

Die Mehrheit der Unternehmen, die an der Umfrage teilgenommen haben, gehört zum Bereich der Kleinst-, Klein- und Mittelunternehmen (mehr als drei Viertel). Das verbleibende Viertel besteht unter anderem aus Großunternehmen (5 %), staatlichen (6 %) und nichtstaatlichen Organisationen (8 %). Soweit erforderlich, wurden nur die Werte für KMU berücksichtigt. **Abbildung *4*** zeigt die Verteilung der Gesamtteilnehmer nach der Unternehmensgröße. Für die Definition der Unternehmensgröße wurde die gängige europäische Definition in Bezug auf die Anzahl der Beschäftigten und den Umsatz verwendet. (Europäische Kommission 2021) .

Die Unternehmen sind in verschiedenen Wirtschaftszweigen tätig, z. B. im Gesundheits- und Sozialwesen, im Erziehungswesen oder im Bereich der freiberuflichen, wissenschaftlichen und technischen Tätigkeiten gemäß der Systematik NACE Rev. 2 (Eurostat 2008) . 10% der Unternehmen sind im Informations- und Kommunikationssektor tätig (Abbildung 5).

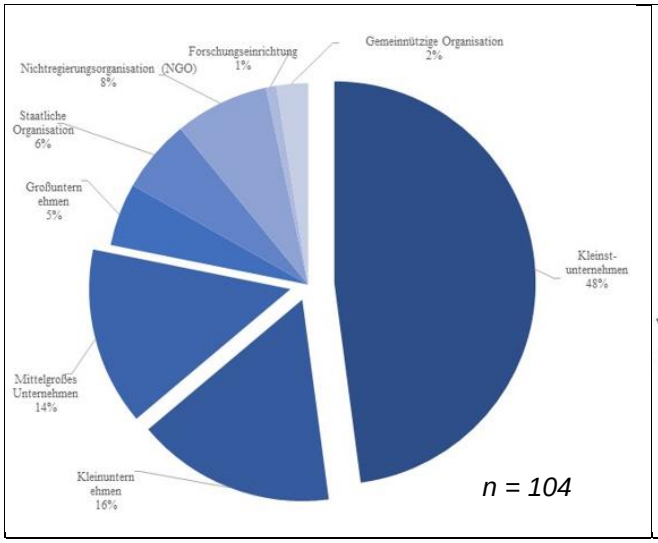


Abbildung 4: "Welche Unternehmen nehmen an der Umfrage teil?"

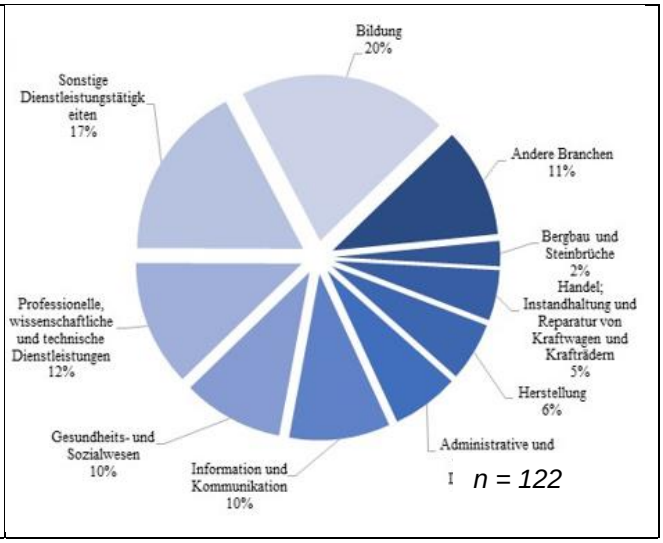


Abbildung 5 : "In welchem Wirtschaftszweig ist Ihr Unternehmen tätig?"

Für die Umfrage war es wichtig, die Art der Tätigkeit der Teilnehmer*innen im Unternehmen zu kennen, d. h. entweder IT- und Informationssicherheitsexpert*innen oder Geschäftsführer/Recruiter in einem KMU, da sich die funktionalen Arbeitsaufgaben, die die Informationssicherheit betreffen, ändern. Je nach ihren Antworten wurden den Teilnehmer*innen in der Umfrage unterschiedliche Fragen gestellt. Wie in Abbildung 4 und Abbildung 5 zu sehen ist, sind zwei Drittel der Teilnehmer*innen als Geschäftsführer*innen oder in der Personalabteilung tätig. Diese Gruppe beantwortete Fragen, die sich auf die Unternehmenskultur, die Kompetenzen im Unternehmen, die Ausbildung im Unternehmen oder die im Unternehmen verwendeten Technologien bezogen.

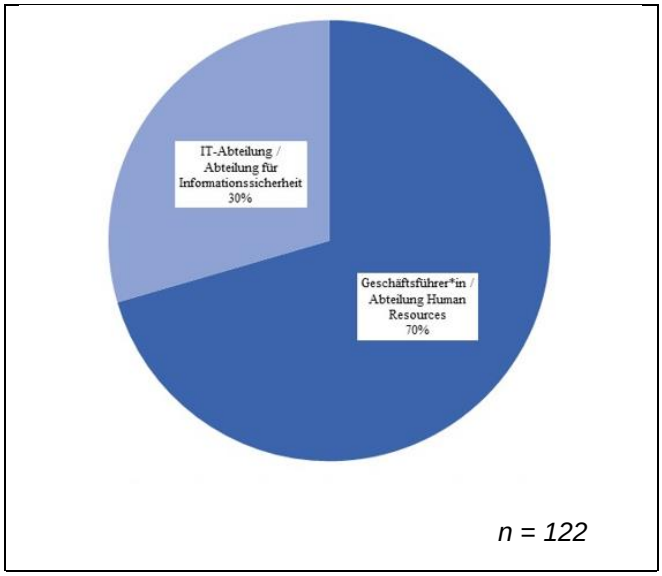


Abbildung 6: "Was ist Ihre Rolle im Unternehmen?"

Den Befragten aus der IT- oder Informationssicherheitsabteilung wurden hingegen Fragen zur eigenen Arbeitsleistung, zu Persönlichkeitsmerkmalen und Fragen zum IT-Management im Unternehmen vorgelegt. Diese Unterscheidung wurde getroffen, um den unterschiedlichen Perspektiven auf die Informationssicherheit Rechnung zu tragen, mit einem Managementfokus auf der Seite der Firmeninhaber und einem technischen Fokus auf der Seite der Informationssicherheitsexpert*innen.

Was die Herkunft der Befragten betrifft, so gab fast die Hälfte der Teilnehmer*innen an, dass ihr Unternehmen hauptsächlich in Italien tätig ist.[3] Daneben sind die Unternehmen auch in Litauen, Deutschland, Polen, Österreich und der Tschechischen Republik tätig (Abbildung 7). Abschließend noch ein kurzer

[3] Es wurde kontrolliert, ob die unausgewogene Teilnahmequote die Objektivität der Ergebnisse beeinträchtigt. Die Prüfung der Daten mit und ohne italienische Teilnehmer ergab keine signifikanten Unterschiede in den Ergebnissen der verschiedenen Fragegruppen, weshalb dieses Risiko vernachlässigt werden kann.

Ausblick auf die Geschlechterverteilung: Es gibt eine leichte Mehrheit von männlichen Teilnehmern, 38 von 102 Teilnehmern sind weiblich (Abbildung 8). Leider waren aufgrund der Größe und Verteilung der Teilnehmer*innen keine Länder- oder Geschlechtervergleiche möglich, was bei der Interpretation der Ergebnisse berücksichtigt werden muss. Alle Grafiken im Folgenden zeigen entweder einen Vergleich von KMU oder Nicht-KMU. Wenn nicht anders angegeben, wurden nur die Antworten von KMU in die Analyse aufgenommen.

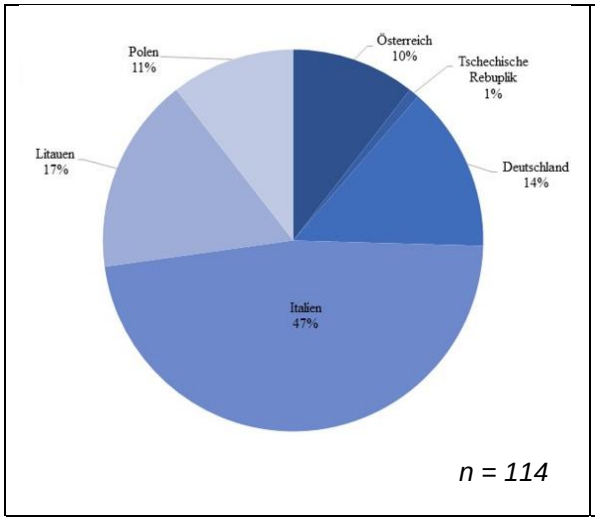


Abbildung 7 : "In welchem Land ist Ihr Unternehmen hauptsächlich tätig?"

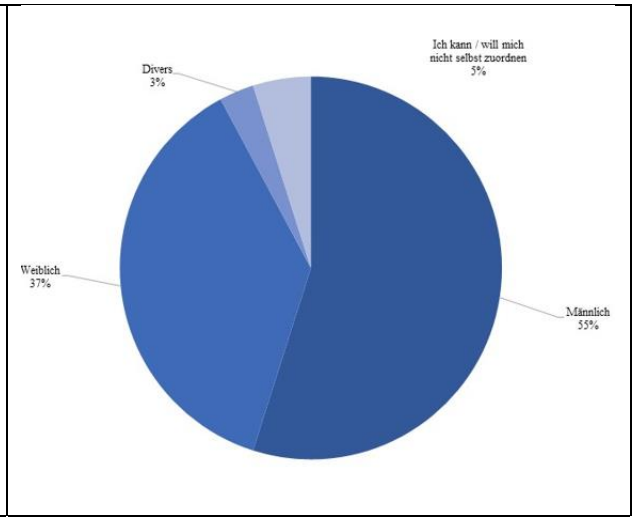


Abbildung 8: "Wie sieht die Geschlechterverteilung aus?"

4.2 Analyse

Der Hauptteil der Untersuchung kann in zwei Gruppen unterteilt werden: **Managementaspekte und technische Aspekte der Informationssicherheit in KMU**.

Während der erste Aspekt die Kapitel 4.2.1Unternehmenskultur , 0 Zuständigkeiten im Unternehmen , 4.2.3Informationssicherheit in KMU und 4.2.4Informationssicherheit im Unternehmen: Anforderungen an das Personal umfasst, beinhaltet der zweite Aspekt kompetenzspezifische Fragen in den Kapiteln 4.2.4Informationssicherheit im Unternehmen: Anforderungen an das Personal , 4.2.5Selbsteinschätzung der Kompetenzen , 4.2.6Persönlichkeit (Big Five) und 4.2.7Arbeitsleistung

4.2.1 Unternehmenskultur

Mit dem Ziel, Unterschiede zwischen Unternehmen, die Informationssicherheitsmaßnahmen implementiert haben, und solchen, die dies nicht getan haben, aufzuzeigen, wurde die Unternehmenskultur als ein entscheidender Aspekt identifiziert, der die Unternehmen voneinander unterscheidet. Folglich bestand der erste Schritt für die Teilnehmer*innen darin, die Unternehmenskultur selbst zu charakterisieren. Zur Analyse der Unternehmenskultur wurden die kurzen Skalen von Jöns et al. (2005) vorgeschlagene Kurzskala verwendet, die eine 5-Punkte-Likert-Skala mit den Extremen 1 und 5 verwendet.

In diesem Zusammenhang wurden die Befragten gebeten, ihr Unternehmen anhand der Merkmale "Strategie", "Struktur", "Führung" und "Zusammenarbeit" zu beschreiben. Für diese Merkmale entwickelten die Autoren 18 Fragen, die in

Frage	N	Mean	Std. Dev.	Var.	Kurtosis	Std. Err.
Das Unternehmen ist sehr kundenorientiert.	83	4.37	0.79	0.63	3.34	0.52
Das Unternehmen ist offen für Innovationen.	83	4.19	0.82	0.67	1.73	0.52
Das Unternehmen ist sehr qualitätsorientiert.	84	4.13	0.97	0.93	0.47	0.52
Das Unternehmen zeichnet sich durch Teamorientierung aus.	84	3.96	0.94	0.88	0.98	0.52
Das Unternehmen ist sehr leistungsorientiert.	83	3.96	0.94	0.89	1.30	0.52
Die Vorgesetzten setzen großes Vertrauen in die Mitarbeiter.	82	3.91	0.77	0.60	-0.19	0.53
Die Mitarbeiter setzen großes Vertrauen in die Führungskräfte.	84	3.87	0.89	0.79	1.32	0.52
Die Information der Mitarbeiter hat einen hohen Stellenwert.	82	3.76	0.90	0.80	-0.57	0.53
Die Mitarbeiter werden in die Entscheidungsfindung einbezogen.	82	3.67	0.99	0.99	0.29	0.53
Konflikte werden im Unternehmen offen angesprochen.	83	3.55	0.93	0.86	0.12	0.52
Das Unternehmen ist stark hierarchisch organisiert.	84	2.94	1.25	1.57	-0.98	0.52
Das Unternehmen hat einen bürokratischen Führungsstil.	84	2.64	1.09	1.20	-0.82	0.52
Die Beziehung zwischen den Arbeitnehmern ist durch Wettbewerb gekennzeichnet.	84	2.52	1.11	1.24	-0.56	0.52
Wenn Fehler und Probleme im Unternehmen auftreten, werden zunächst die Schuldigen gesucht.	84	2.26	1.03	1.06	-0.27	0.52
Der Führungsstil im Unternehmen ist autoritär.	83	2.24	1.11	1.23	-0.52	0.52

Tabelle ***1*** dargestellt sind. Wie weiter unten zu sehen ist, gibt es zwischen den 18 Fragen erhebliche Unterschiede in der Zustimmung. Es muss daher erwähnt werden, dass einige der Items positiv und einige negativ formuliert sind. Folglich liefert ein direkter Vergleich keine unmittelbaren und aussagekräftigen Ergebnisse. Noch wichtiger ist, dass in diesem Zusammenhang die Aggregation der Kategorien zu den vier oben genannten Bereichen berücksichtigt werden muss.

Frage	N	Mean	Std. Dev.	Var.	Kurtosis	Std. Err.
Das Unternehmen ist sehr kundenorientiert.	83	4.37	0.79	0.63	3.34	0.52
Das Unternehmen ist offen für Innovationen.	83	4.19	0.82	0.67	1.73	0.52
Das Unternehmen ist sehr qualitätsorientiert.	84	4.13	0.97	0.93	0.47	0.52
Das Unternehmen zeichnet sich durch Teamorientierung aus.	84	3.96	0.94	0.88	0.98	0.52
Das Unternehmen ist sehr leistungsorientiert.	83	3.96	0.94	0.89	1.30	0.52
Die Vorgesetzten setzen großes Vertrauen in die Mitarbeiter.	82	3.91	0.77	0.60	-0.19	0.53
Die Mitarbeiter setzen großes Vertrauen in die Führungskräfte.	84	3.87	0.89	0.79	1.32	0.52
Die Information der Mitarbeiter hat einen hohen Stellenwert.	82	3.76	0.90	0.80	-0.57	0.53
Die Mitarbeiter werden in die Entscheidungsfindung einbezogen.	82	3.67	0.99	0.99	0.29	0.53
Konflikte werden im Unternehmen offen angesprochen.	83	3.55	0.93	0.86	0.12	0.52
Das Unternehmen ist stark hierarchisch organisiert.	84	2.94	1.25	1.57	-0.98	0.52
Das Unternehmen hat einen bürokratischen Führungsstil.	84	2.64	1.09	1.20	-0.82	0.52
Die Beziehung zwischen den Arbeitnehmern ist durch Wettbewerb gekennzeichnet.	84	2.52	1.11	1.24	-0.56	0.52
Wenn Fehler und Probleme im Unternehmen auftreten, werden zunächst die Schuldigen gesucht.	84	2.26	1.03	1.06	-0.27	0.52
Der Führungsstil im Unternehmen ist autoritär.	83	2.24	1.11	1.23	-0.52	0.52

Tabelle 1 : "Bitte geben Sie an, inwieweit die folgenden Merkmale das Unternehmen, für das Sie arbeiten, oder die Organisation, für die Sie arbeiten, beschreiben".

Die oben genannten Merkmale lassen sich nach Strategie, Struktur, Führung und Zusammenarbeit unterscheiden. Die Autoren definieren diese Kategorien wie folgt: Kundenorientierung, Offenheit gegenüber Innovationen, eine hohe Qualitäts- und Leistungsorientierung gehören zum Bereich Strategie. Hinsichtlich der Unternehmensstruktur ist es wichtig zu wissen, ob das Unternehmen einen bürokratischen Führungsstil hat und ob es stark hierarchisch organisiert ist. Der letzte Punkt führt zur nächsten Kategorie Führung. In diesem Bereich spielen der Führungsstil, die Priorität der Mitarbeiterinformation und die

Einbeziehung der Mitarbeiter*innen in die Entscheidungsfindung eine wichtige Rolle. Außerdem werden die Teilnehmer*innen befragt, wie es sich verhält, wenn im Unternehmen Fehler und Probleme auftreten. Schließlich sind Themen wie Teamorientierung, Vertrauen der Mitarbeiter*innen gegenüber den Führungskräften, Umgang mit Konflikten im Unternehmen und die Beziehung zwischen den Mitarbeitern Teil der Kategorie Zusammenarbeit.

Wie Abbildung 9zeigt, weisen die untersuchten Unternehmen eine relativ hohe strategische Ausrichtung, einen geringen Grad an hierarchischer Struktur und einen geringen Grad an direktiver Führung auf. Auffällig ist, dass Unternehmen, die nicht dem KMU-Sektor zuzurechnen sind, einen etwas höheren Wert im Bereich Struktur aufweisen. Es kann davon ausgegangen werden, dass insbesondere große Unternehmen hierarchischer organisiert sind als kleine und mittlere Unternehmen. In Bezug auf Strategie, Führung und Kooperation sind nur marginale Unterschiede zwischen KMU und Nicht-KMU zu beobachten.

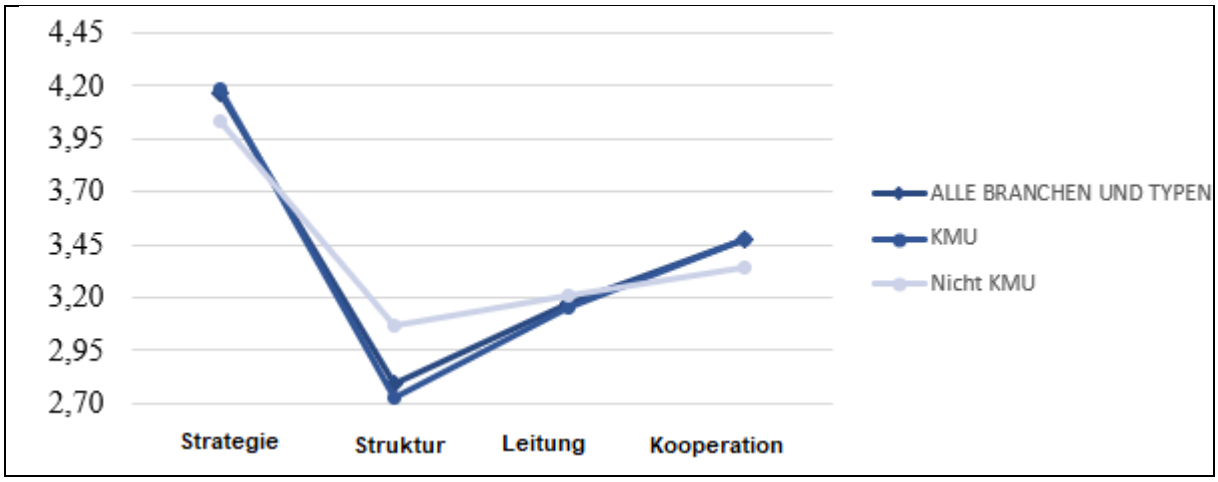


Abbildung 9: Merkmale in den folgenden Kategorien "Strategie, Struktur, Führung, Zusammenarbeit" - alle Unternehmen

In Bezug auf die Ausgangsfrage dieses Teils der Umfrage kann festgestellt werden, dass ein leichter Unterschied im Grad der Zusammenarbeit, der Strategie und der Führung besteht, der in Unternehmen, die Maßnahmen zur Informationssicherheit ergriffen haben, höher ist als in Unternehmen, die dies nicht getan haben.

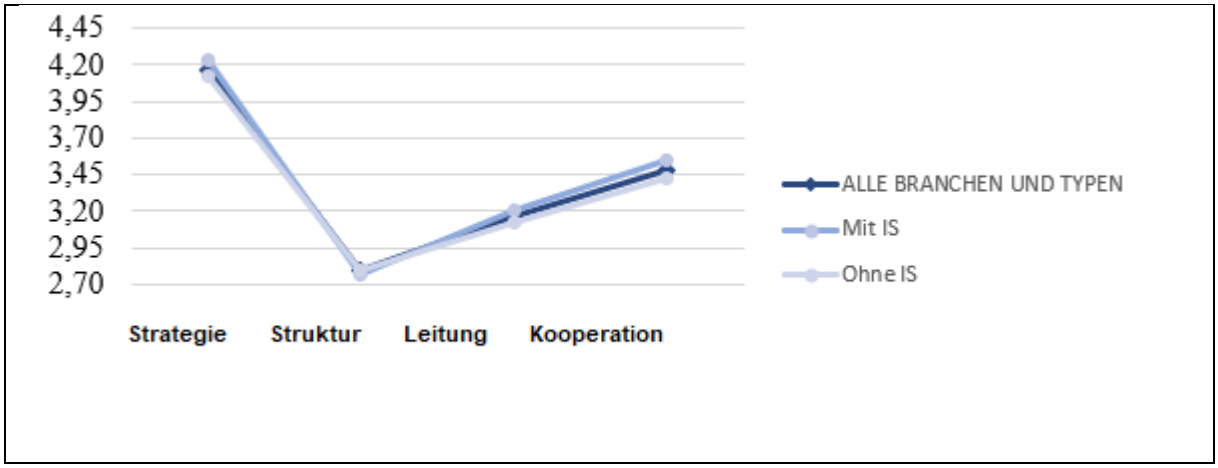


Abbildung 10: Merkmale*, gruppiert in die folgenden Kategorien "Strategie, Struktur, Führung, Zusammenarbeit" - Unternehmen mit und ohne Informationssicherheitsstrategie*

4.2.2 Zuständigkeiten im Unternehmen

Im Rahmen der Umfrage ging es vor allem darum, tiefere Einblicke in die wichtigsten Kompetenzen im Bereich der Informationssicherheit zu gewinnen, die Mitarbeiter*innen in einem KMU

mitbringen sollten. Die Befragten wurden gebeten, die Informationssicherheitsstrategie in ihrem Unternehmen und die Aufgaben, die besonders relevant sind, näher zu betrachten. Tabelle 2zeigt einen Überblick über die verschiedenen Aufgaben und Aktivitäten. Die Wichtigkeit der jeweiligen Tätigkeit wird zwischen "5 - sehr wichtig" und "1 - überhaupt nicht" gemessen, die Häufigkeit zwischen "5 - sehr oft" und "1 - nie".

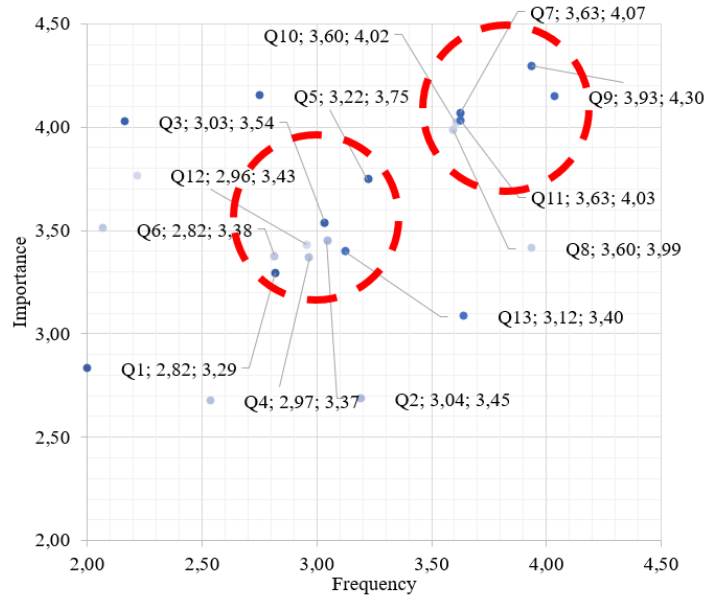
Frage	Code
Analyse von Geschäftsprozessen und Erstellung von strategischen Berichten über Datenschutz und Informationssicherheit	Q1
Verfolgung von und Berichterstattung über Veränderungen innerhalb und außerhalb der Organisation, die sich auf die Sicherheitsstrategie der Organisation auswirken	Q2
Ausarbeitung von Unternehmensrichtlinien für den systematischen Umgang mit bestimmten Informationen und Daten	Q3
Ausarbeitung von Empfehlungen für zu beschaffende Geräte unter Berücksichtigung der Anforderungen des Unternehmens an die Informationssicherheit und den Datenschutz	Q4
Durchführung von (Informations-)Maßnahmen zur Sensibilisierung der Mitarbeiter für Sicherheitsrisiken bei ihrer täglichen Arbeit und zur Verbreitung des Sicherheitsbewusstseins in der Belegschaft	Q5
Erstellung von Schulungsplänen für das Unternehmen, um die Mitarbeiter regelmäßig in Sachen Informationssicherheit und Datenschutz zu schulen	Q6
Installation von Firewall- und Antivirensoftware Durchführung von Aktualisierungen und Anwendung elementarer Methoden zur Überprüfung der Sicherheit der im Unternehmen eingesetzten Software und Erstellung entsprechender Unterlagen	Q7
Sicherung von mobilen Geräten, Kommunikationskanälen und Datenspeichern durch Passwörter oder andere Authentifizierungsmittel	Q8
Durchführung von routinemäßigen Datensicherungen und Anwendung ordnungsgemäßer Verhaltensweisen in Übereinstimmung mit der GDPR bei der Datenverarbeitung im Unternehmen	Q9
Einrichtung von Administratorkonten und Einschränkung der Zugriffsrechte für die Mitarbeiter entsprechend den festgelegten Sicherheitsstufen	Q10
Einrichtung von Passwörtern für den individuellen Zugang der Mitarbeiter sowie eines sicheren Speicher- und Wiederherstellungsprozesses	Q11
Erstellung von Richtlinien und Verfahren für das Auftreten von Ansprüchen	Q12
Koordinierung der Bedürfnisse von Führungskräften und Mitarbeitern des Unternehmens und Versorgung beider Parteien mit Informationen und Einblicken aus dem Unternehmen	Q13

Tabelle 2 : "Aufgaben und Tätigkeiten im Bereich der Informationssicherheit"

Abbildung 11zeigt die Ergebnisse in einer Kreuztabelle (die Häufigkeit wird auf der x-Achse, die Wichtigkeit auf der y-Achse dargestellt). Im Allgemeinen weist keine der genannten Aktivitäten einen niedrigen Grad an Wichtigkeit oder Häufigkeit auf. Es lassen sich jedoch deutlich zwei Gruppen von Tätigkeiten unterscheiden, von denen die eine sowohl eine hohe Häufigkeit als auch eine hohe Bedeutung aufweist, die andere eine mittlere Häufigkeit und Bedeutung. Diese Gruppen sind in der nachstehenden Abbildung rot eingekreist.

Die erste Gruppe von Kompetenzen weist sowohl bei der Häufigkeit als auch bei der Wichtigkeit hohe Werte auf. Zu dieser Gruppe gehören Kompetenzen in Bezug auf "Sicherheitstests", "Verschlüsselung", "Passwortverwaltung" und "rollenbasierte Zugriffskontrolle". Innerhalb dieser Gruppe weist das "Datenmanagement", d. h. die Durchführung routinemäßiger Datensicherungen und die Anwendung ordnungsgemäßer Verhaltensweisen gemäß der DSGVO bei der Datenverarbeitung, den höchsten Gesamtwert hinsichtlich Wichtigkeit und Häufigkeit auf (Q9: 3,93; 4,30). Andererseits können Aktivitäten im Bereich "Prozess-/Stakeholder-/Compliance-Management", "IKT-Beschaffung", "Sensibilisierung & Einflussnahme" und "Aus- und Weiterbildung" zusammengefasst werden. Alle Kompetenzen werden als eher wichtig erachtet, die Häufigkeit kann jedoch nicht als besonders häufig bezeichnet werden. Als am wenigsten wichtig und am wenigsten häufig

bezeichnen die Befragten den Bereich "Prozessmanagement". In diesem Bereich geht es um die Analyse von Geschäftsprozessen und die Erstellung von strategischen Berichten zu Datenschutz und Informationssicherheit. Dennoch zeigt der Wert von 2,82, dass das Thema in den Unternehmen durchaus Beachtung findet.



Lerneinheiten	Code
Prozess-Management	Q1
IKT-Risikomanagement	Q2
Compliance Management	Q3
IKT-Beschaffung	Q4
Sensibilisierung und Einflussnahme	Q5
Bildung und Ausbildung	Q6
Sicherheitsprüfung	Q7
Kodierung	Q8
Datenverwaltung	Q9
Rollenbasierte Zugangskontrolle	Q10
Passwortverwaltung	Q11
Management der Geschäftskontinuität	Q12
Mediation und Stakeholder-Management	Q13

Abbildung 11 : Kompetenzen im Unternehmen - Ergebnisse

Die folgende Abbildung konzentriert sich auf die Analyse der Kompetenzen in KMU (Abbildung 12). Die Daten beschreiben den Unterschied in der Bedeutung zwischen KMU und Nicht-KMU: je näher ein Wert bei Null liegt, desto geringer ist der Unterschied. Größere Werte bedeuten daher auch größere Unterschiede. Positive Werte bedeuten, dass die Kompetenzen in KMU wichtiger sind und häufiger genutzt werden, während negative Werte das Gegenteil bedeuten. Alle bereits erwähnten Kompetenzen finden sich in der Kreuztabelle wieder. Hinsichtlich der Beschreibung der Achsen ist zu beachten: In diesem Fall zeigt die x-Achse die Wichtigkeit, die y-Achse die Häufigkeit an. Es lässt sich feststellen, dass der Bereich Datenmanagement auch in KMU als wichtiger und häufiger genutzt wird. Abbildung 11zeigte bereits die hohe Bedeutung des Datenmanagements (siehe Frage 9). Im Zusammenhang mit der Teilzertifizierung in der Informationssicherheit ist der folgende Aspekt besonders interessant: Der Code Q6 beschreibt Kompetenzen und Aktivitäten in der Aus- und Weiterbildung. Wie Abbildung 12zeigt, ist Code Q6 in dem Bereich zu finden, der durch Kompetenzen gekennzeichnet ist, die

weniger wichtig und werden in KMU weniger häufig genutzt. Die Erstellung von Schulungsplänen zur regelmäßigen Schulung der Mitarbeiter*innen in Sachen Informationssicherheit und Datenschutz ist für KMU offensichtlich weniger wichtig. Es zeigt sich, dass alle Kompetenzen ziemlich wichtig sind (Mittelwert > 3,3) und häufig genutzt werden (Mittelwert > 2,8). Die wichtigsten und am häufigsten genutzten Kompetenzen sind die üblichen Aufgaben eines durchschnittlichen Systemadministrators, z. B. die Erstellung von Backups, die Installation von Antivirensoftware und Firewalls oder die Festlegung der individuellen Passwörter.

4.2.3 Informationssicherheit in KMU

In diesem Abschnitt beantworten die Befragten detailliertere Fragen im Zusammenhang mit der Informationssicherheit in ihren Unternehmen. Es geht um die Gründe, die das Unternehmen davon abgehalten haben, in die Verbesserung der Informationssicherheit zu

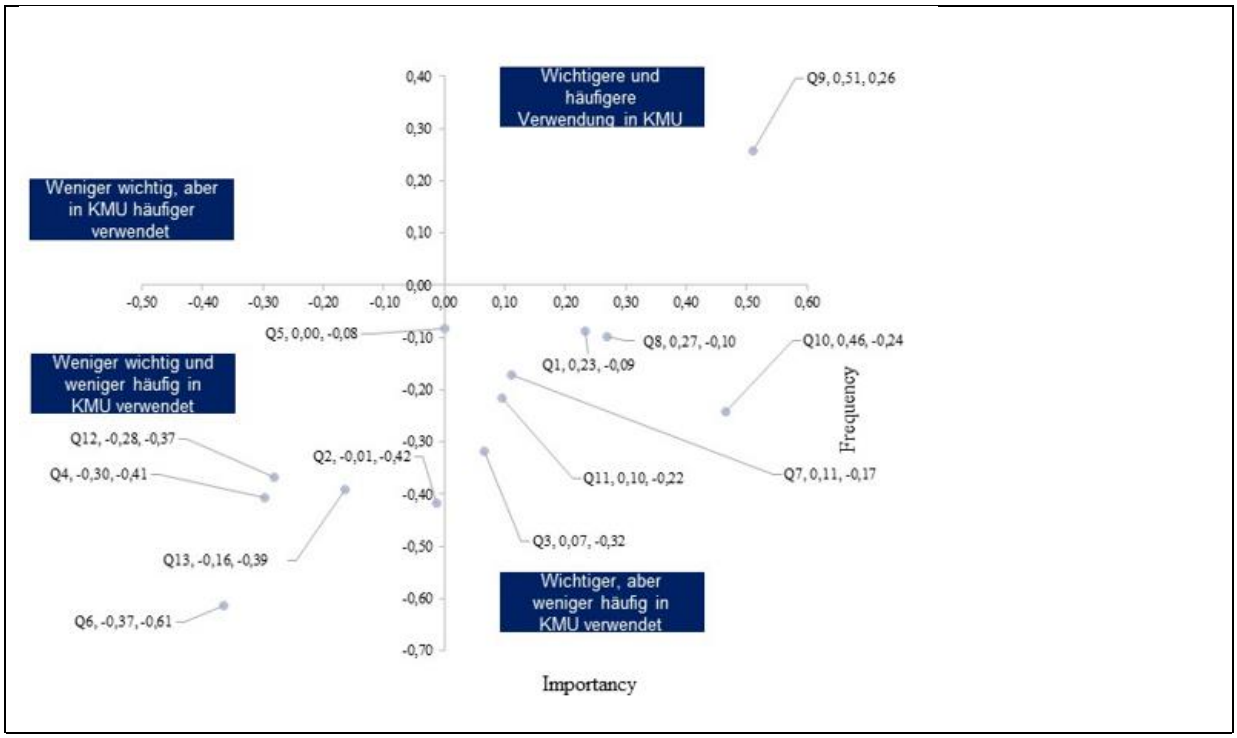


Abbildung 12 : Analyse der Kompetenzen in KMU

investieren (Abbildung 13). Die Teilnehmer*innen sind hier nur diejenigen, die KMU als Unternehmenstyp gewählt haben.

Wie aus der nachstehenden Abbildung hervorgeht, liegt der Hauptgrund darin, dass in den Unternehmen nicht genügend finanzielle Ressourcen vorhanden sind (mehr als 30 % der Befragten gaben diesen Grund an). Daneben ist auch der Mangel an Angeboten von Dienstleistern ein wichtiger Aspekt im Hinblick auf das Investitionsproblem im Bereich der Informationssicherheit. Einerseits gaben etwa 15 % der Befragten an, dass dieses Problem in ihrem Unternehmen nicht besteht bzw. dass die Firmen den Bedarf decken können: ein Aspekt, der durchaus positiv zu bewerten ist. Andererseits sieht fast ein Drittel der Teilnehmer*innen keinen Bedarf bzw. keine Priorität und gab an, dass andere Themen bisher wichtiger gewesen seien. Ein durchaus gravierender Punkt, der zeigt, dass das Thema Informationssicherheit noch nicht in allen Unternehmen zentral ist. Schließlich scheint auch der Aspekt des verfügbaren Personals eine eher untergeordnete Rolle zu spielen. Nur etwa 4 Teilnehmer*innen gaben einen Zusammenhang zwischen dem Personalmangel und dem Investitionsproblem in die Informationssicherheit an.

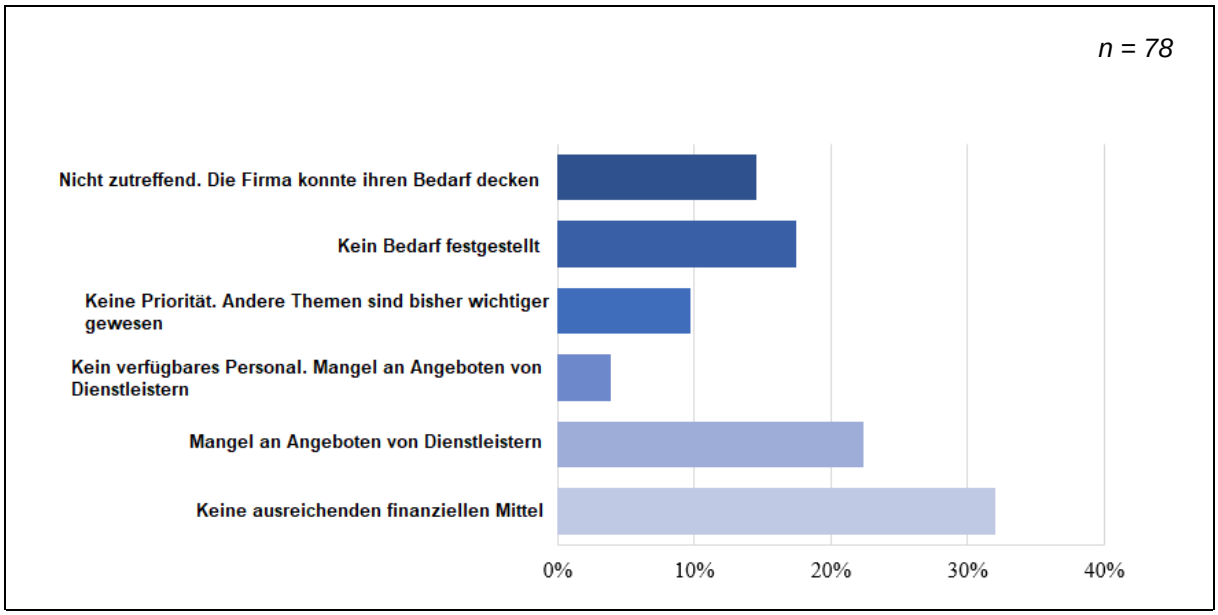


Abbildung 13 : "Welche Gründe haben Ihr Unternehmen bisher davon abgehalten, in die Verbesserung der Informationssicherheit zu investieren?"

Die Befragten betonen die Bedeutung bestimmter Arten von Ausbildung, die für die Informationssicherheit im Unternehmen erforderlich sind. In diesem Zusammenhang wurde gefragt, welche Art von Ausbildung oder Training für einen Mitarbeiter/eine Mitarbeiterin, der/die mit der Gewährleistung der Informationssicherheit in einem Unternehmen betraut ist, notwendig/ hilfreich/ etc. ist. Es muss erwähnt werden, dass es einen Unterschied gibt zwischen notwendigen Fähigkeiten oder Ausbildungen ("must-haves") und hilfreichen Fähigkeiten oder Ausbildungen ("nice-to-have"). Abbildung 14zeigt, dass der Erfahrung am Arbeitsplatz eine große Bedeutung beigemessen wird. Fast die Hälfte der Teilnehmer*innen sieht diesen Punkt als "must-have" an. Darüber hinaus sind auch innerbetriebliche Schulungen oder Weiterbildungen relevant und hilfreich. Generell zeigt sich, dass die Befragten lieber einen Mitarbeiter mit Erfahrung als einen mit Ausbildung haben wollen. Alle Formate des nicht-klassischen Studiums sind nur etwas weniger entscheidend und wichtiger als jede Art von Hochschulausbildung.

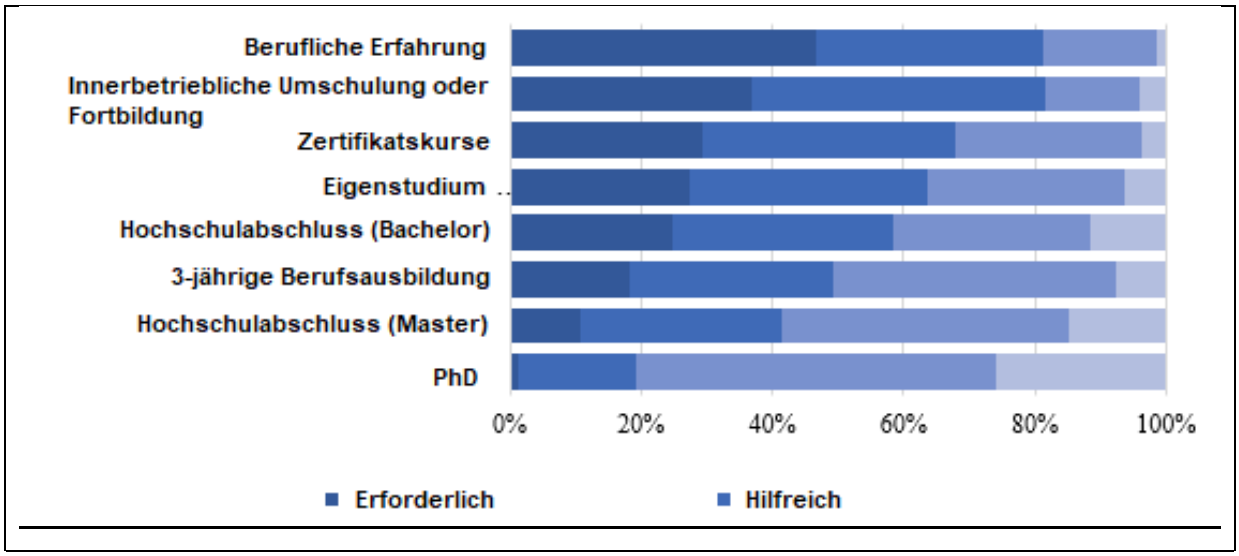


Abbildung 14 : "Welche Art von Ausbildung oder Schulung ist Ihrer Erfahrung nach für einen Mitarbeiter, der in Ihrem Unternehmen mit der Gewährleistung der Informationssicherheit betraut ist, notwendig/hilfreich/optional?"

Im Rahmen der Umfrage wurden die Befragten auch nach möglichen Optionen zur Erhöhung der Informationssicherheit gefragt (Abbildung 15). Die Möglichkeit, die Qualifikation der Mitarbeiter*innen zu erhöhen, ist am beliebtesten und wurde in fast 50 % der Fälle gewählt. Die andere Option ist der Kauf einer Dienstleistung von Dritten, die in 30 % der Fälle gewählt wurde. Die Schaffung und Besetzung einer neuen Stelle oder die Absicherung der Risiken durch eine Versicherung ist dagegen weniger beliebt.

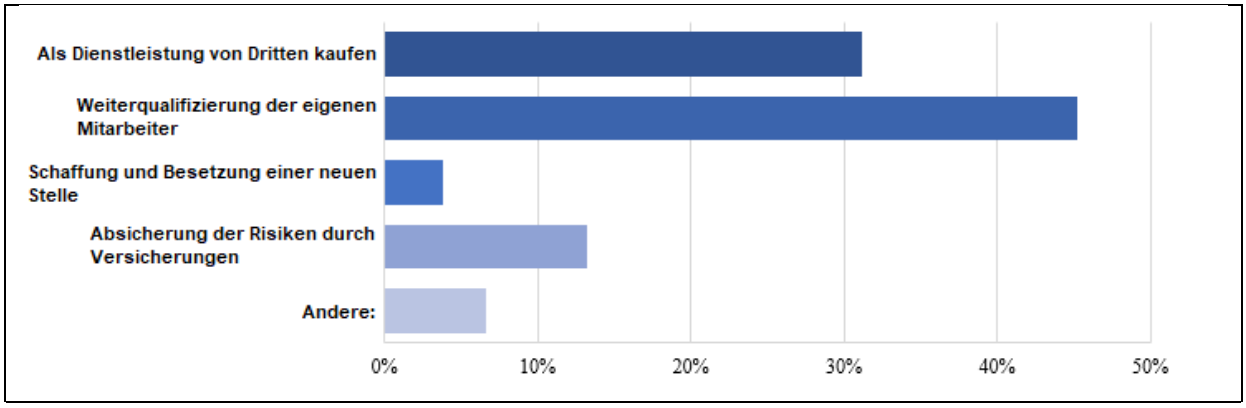


Abbildung 15 : Mögliche Optionen zur Erhöhung der Informationssicherheit

Die Studie zur Informationssicherheit in KMU zeigt, dass es an Finanzmitteln und Dienstleistungen Dritter im Bereich der Informationssicherheit mangelt - Hauptgründe für das Investitionsproblem in dem genannten Bereich. Dies ist vor allem deshalb von Bedeutung, weil die Befragten die Dienste Dritter in Anspruch nehmen wollen, um die Informationssicherheit in ihrem Unternehmen zu verbessern. Aufgrund des Mangels an Finanzmitteln und des Angebots auf dem Markt für Sicherheitsdienstleistungen scheinen unsere Befragten es vorzuziehen, die Qualifikationen ihrer Mitarbeiter*innen zu verbessern, um das unterhaltsame Niveau der Informationssicherheit aufrechtzuerhalten. Dies steht im Einklang mit den Anforderungen an die Ausbildung: Die Befragten ziehen es vor, jemanden mit Erfahrung und nicht mit Ausbildung einzustellen.

4.2.4 Informationssicherheit im Unternehmen: Anforderungen an das Personal

Ein weiterer Punkt, der im Rahmen der Befragung analysiert wurde, war der Personalbedarf an Informationssicherheit im Unternehmen. Dabei wurde nicht nur zwischen KMU und Nicht-KMU unterschieden, sondern auch die unterschiedliche Situation der Unternehmen hinsichtlich des Vorhandenseins von Informationssicherheitsvorfällen analysiert. Vor allem letzteres liefert ein klares Bild der sich ändernden Einstellung der Unternehmen zur Informationssicherheit und zu den Ausgaben für Informationssicherheit. Die Existenz von Informationssicherheitsvorfällen ist in Abbildung 16dargestellt.

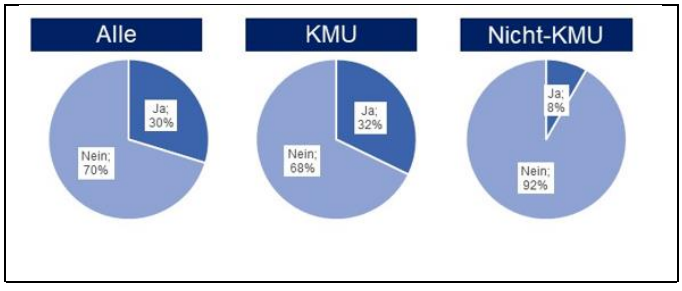


Abbildung 16: "Sind Ihnen in den letzten 2 Jahren Vorfälle im Bereich der Informationssicherheit bekannt oder besteht der Verdacht auf einen Sicherheitsvorfall?"

Um mehr über die personelle Realität in den Unternehmen zu erfahren, wurden die Befragten gefragt, wie viele Mitarbeiter*innen sie derzeit mit dem Arbeitsschwerpunkt Informationssicherheit beschäftigen und wie viele Mitarbeiter und Mitarbeiterinnen sie in den nächsten Jahren einstellen wollen. Es zeigt sich, dass es in den meisten Unternehmen in der Regel einen Mitarbeiter*innen gibt, der/die formal für die Informationssicherheit zuständig ist.

Auch in Nicht-KMUs sind in der Regel nicht mehr Mitarbeiter*innen für diesen Tätigkeitsbereich

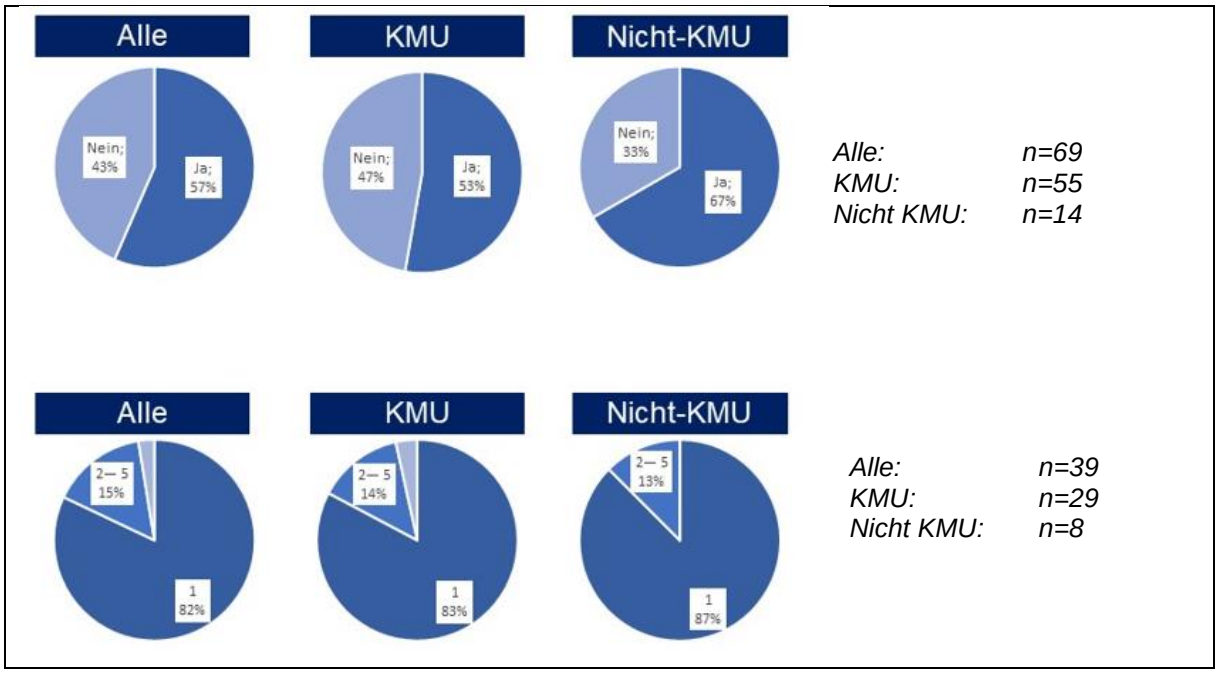


Abbildung 17 : "Gibt es in Ihrem Unternehmen Mitarbeiter, die formell für die Informationssicherheit verantwortlich sind? (oben) - Wenn ja, wie viele?" (unten)

zuständig (Abbildung 17). Oben ist dargestellt, ob Personal beschäftigt ist, unten sind die entsprechenden Zahlen der Unternehmen zu sehen, die die erste Frage bejaht haben.

Des Weiteren wurde gefragt, wie viele offene Stellen im Bereich der Informationssicherheit es im Unternehmen gibt. Wie Abbildung 18zeigt, antworteten etwa 50 % der Befragten, dass es in ihrem Unternehmen derzeit keine offenen Stellen im Bereich der Informationssicherheit gibt. Betrachtet man das Auftreten eines Informationssicherheitsvorfalls (IS), so ist ein starker Anstieg der geschaffenen Stellen zu verzeichnen. Von den Unternehmen, in denen es keinen Vorfall im Bereich der Informationssicherheit gab (NO IS), verfügen rund 90 % über keine spezifische Stelle für Informationssicherheit. Diese Zahl sinkt auf nur 20 % im Vergleich zu den Unternehmen, die einen Vorfall hatten. Vergleichbare Zahlen wurden für das Vorhandensein von mehr als einer Stelle gemeldet, was die Initiative zeigt, die Unternehmen nach einem Angriff ergreifen.

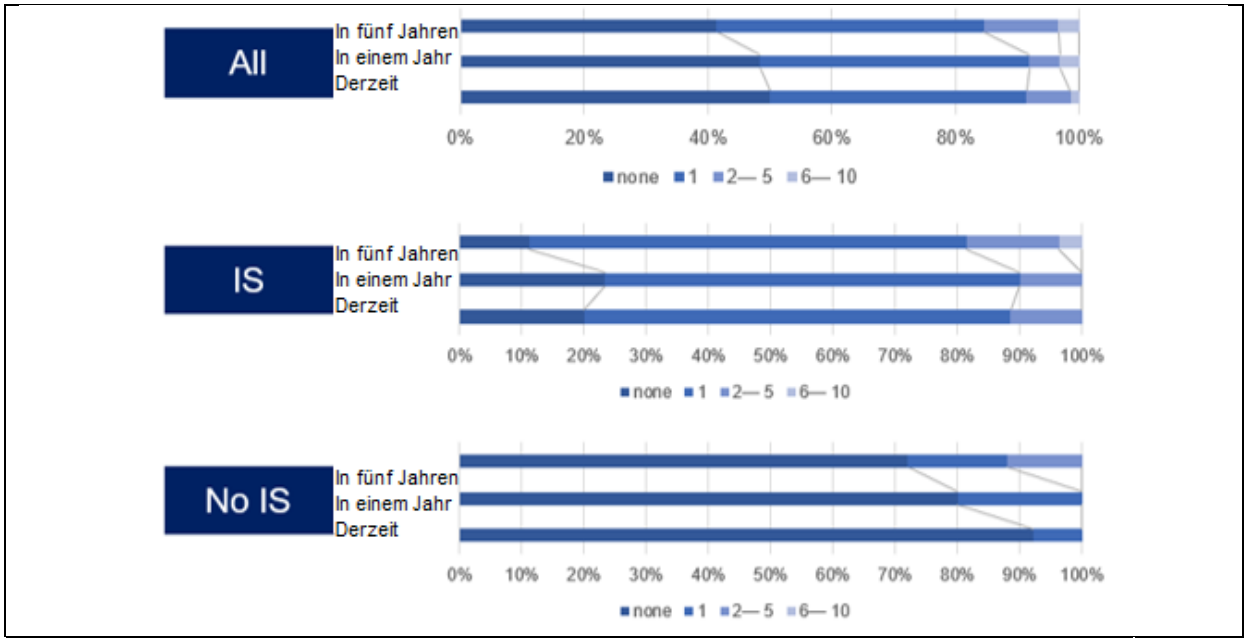


Abbildung 18 : "Wie viele offene Stellen im Bereich der Informationssicherheit gibt es in Ihrem Unternehmen?"

In diesem Zusammenhang wurden die Befragten auch gefragt, wie sie den Personalbedarf im Bereich der Informationssicherheit bisher angehen. Abbildung 20zeigt, dass vor allem Nicht-KMU der Weiterbildung der Mitarbeiter*innen große Bedeutung beimessen. Bei den KMU zeigt sich, dass der Einkauf von Dienstleistungen im Bereich "Informationssicherheit" bei Drittanbietern in etwa der Weiterbildung von Mitarbeitern entspricht. Die Einstellung neuer Mitarbeiter*innen ist dagegen für die Unternehmen von geringerer Bedeutung. Insgesamt lässt sich feststellen, dass der Aufbau interner Kapazitäten und die Weiterbildung der eigenen Mitarbeiter*innen von den meisten Unternehmen als die geeignetste Lösung angesehen wird. Nichtsdestotrotz gibt es einen Vorbehalt in Bezug auf die Gültigkeit der gemeldeten Daten, der deutlich wird, wenn man die Unternehmen, die einen Vorfall im Bereich der Informationssicherheit erlebt haben, von den Unternehmen unterscheidet, die keinen Vorfall erlebt haben. Wie in Abbildung 21sehen ist, sinkt das Item "keine Maßnahmen" von 31 % (am häufigsten genannt) bei Firmen ohne Informationssicherheitsvorfall auf nur 10 % (am wenigsten genannt) bei Firmen mit einem Informationssicherheitsvorfall.

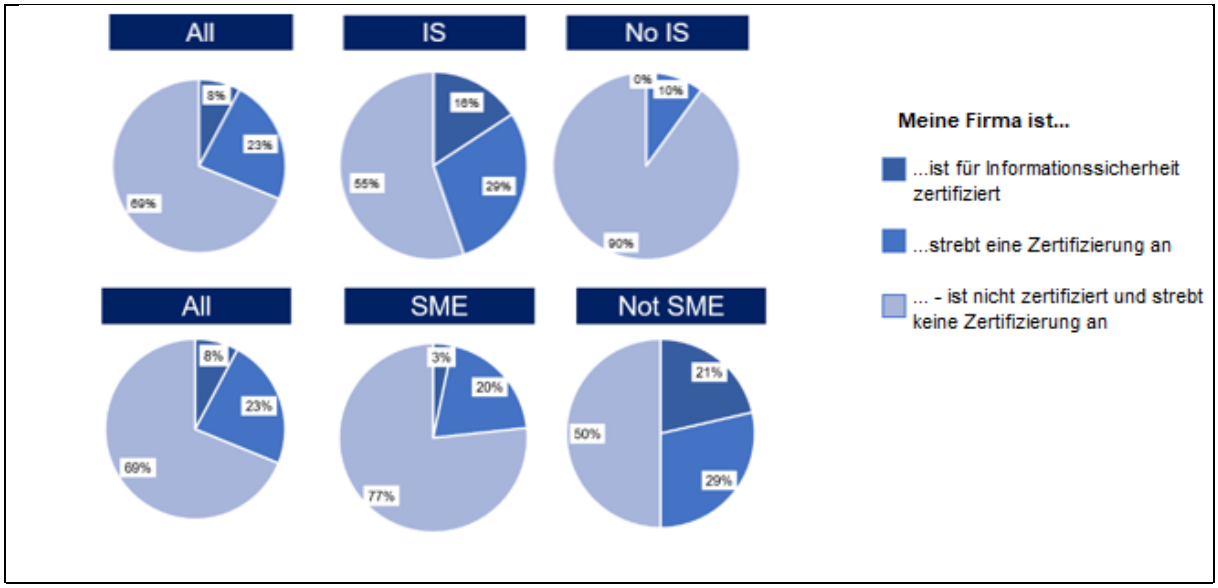


Abbildung 19: Unternehmenszertifizierung für Informationssicherheit

Analoge Zahlen lassen sich für das Vorhandensein von Zertifizierungen bei KMU und Nicht-KMU sowie bei Unternehmen mit einem Informationssicherheitsvorfall feststellen. Während Zertifizierungen bei KMU kaum vorkommen (3 %), fehlen sie bei KMU ohne Informationssicherheitsvorfall völlig. Bei Unternehmen, die einen Vorfall hatten, steigen die Zahlen sowohl für bestehende als auch für geplante Zertifizierungen deutlich an.

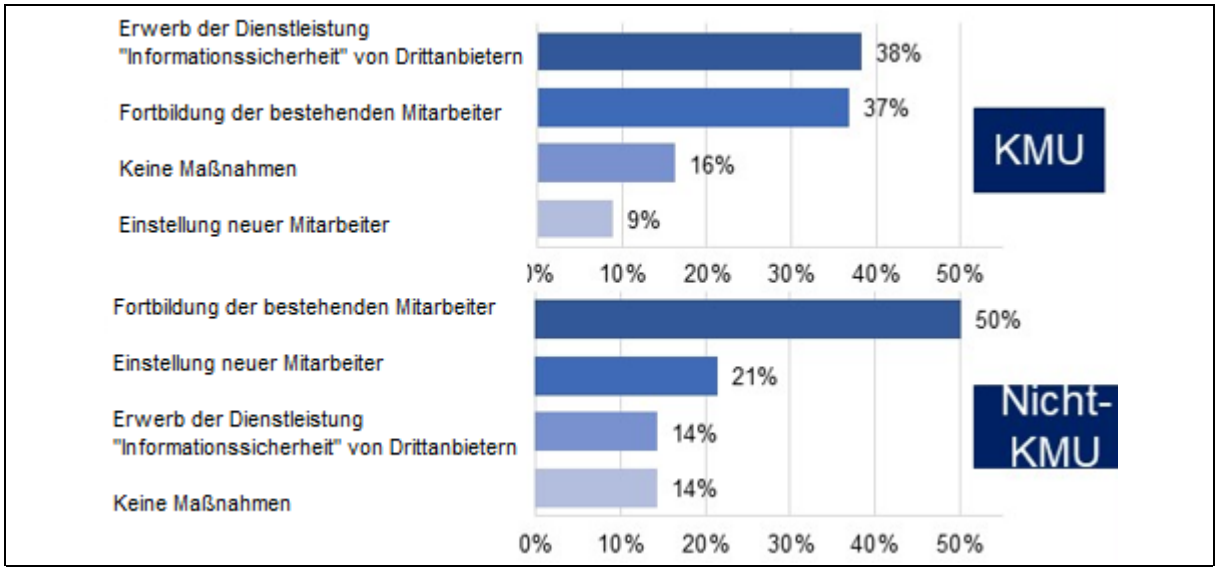


Abbildung 20: "Wie gehen Sie bisher mit dem Personalbedarf im Bereich der Informationssicherheit um?"

In Anbetracht des Umfangs dieser Umfrage ist es nicht nur wichtig, den Stand der Zertifizierung und der Investitionen zu verstehen, sondern auch die bereits ergriffenen Maßnahmen zur Bewältigung der Herausforderungen im Bereich der Informationssicherheit. Wie aus der nachstehenden Abbildung hervorgeht, haben zwei Drittel der Befragten diese Frage verneint. Dies bedeutet jedoch auch, dass etwa 30 % mit "Ja" geantwortet haben.

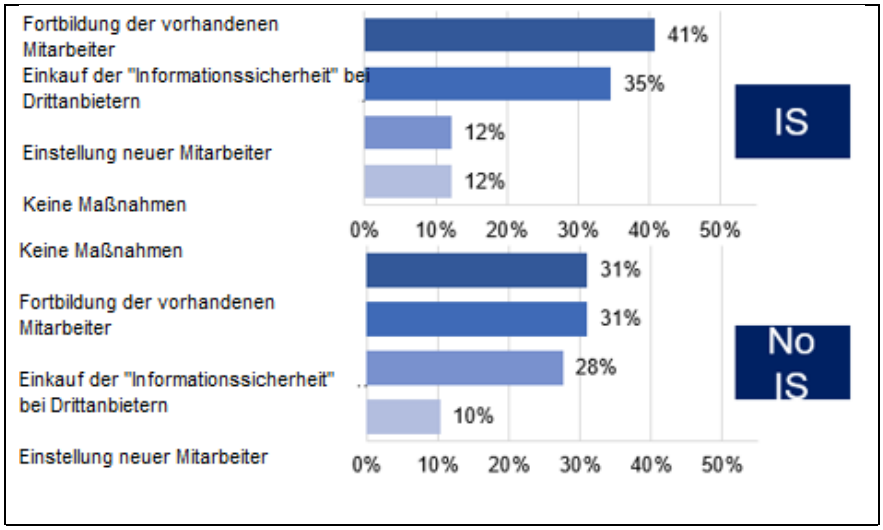


Abbildung 21: "Wie gehen Sie bisher mit dem Personalbedarf im Bereich der Informationssicherheit um?" - IS und kein IS

Betrachtet man die Ergebnisse aus Abbildung 18und Abbildung 21wird deutlich, dass die Unternehmen erst nach einem Angriff aktiv werden. Die Unternehmen sehen nicht nur die Notwendigkeit, eine entsprechende Vollzeitstelle einzurichten, sondern sie suchen auch nach Möglichkeiten, ihre Informationssicherheit mit allen Mitteln zu verbessern. Daraus lässt sich schließen, dass die unter Fachleuten für Informationssicherheit und in der Informationssicherheitsgemeinschaft vorherrschende Meinung, "Lernen durch Schmerzen", die Realität in den meisten Unternehmen zutreffend beschreibt. Die Einsicht, akute Maßnahmen zu ergreifen und Ressourcen in die Mitarbeiter*innen zu investieren, wächst meist erst nach einem Angriff - wenn der Schaden bereits angerichtet ist.

4.2.5 Selbsteinschätzung der Kompetenzen

Im Rahmen der Umfrage wurden die Befragten gebeten, sich selbst im Hinblick auf relevante Aus- und Weiterbildungsaktivitäten im Bereich der Informationssicherheit zu bewerten. Dabei stand ihnen eine Skala von "0 - Keine Erfahrung", "1 - Allgemeine Kenntnisse", "2 - Allgemeine Kenntnisse plus praktische Erfahrung", "3 - Erweiterte theoretische Kenntnisse" bis "4 - Erweiterte theoretische Kenntnisse plus praktische Erfahrung" zur Verfügung. Die Abbildung unten zeigt, dass Passwort- und Datenmanagement häufig genannt wurde. Dazu gehören zum Beispiel die Einrichtung von Passwörtern oder die Durchführung von routinemäßigen Datensicherungen. Aus den ermittelten Werten wurden Durchschnittswerte gebildet, die in der nachstehenden Abbildung aufgeführt sind. Während sich die Befragten bei der Passwortverwaltung, der Datenverwaltung und der Aus- und Weiterbildung im Durchschnitt am erfahrensten fühlten, zeigten sie sich bei der Sicherstellung der Compliance, der Verschlüsselung und der Sensibilisierung der Mitarbeiter*innen weniger zuversichtlich.

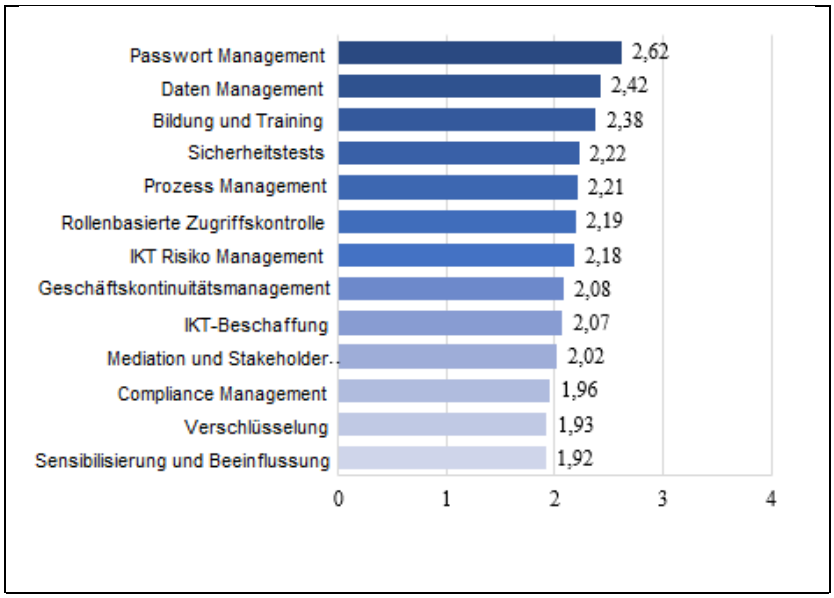


Abbildung 22: "Bitte schätzen Sie sich selbst ein: Welche der folgenden Bildungs- und Ausbildungsaktivitäten können Sie durchführen?"

4.2.6 Persönlichkeit (Big Five)

In vielen Gesprächen mit Expert*innen wurde deutlich, dass der Beruf des Informationssicherheitsbeauftragten besondere Anforderungen an die soziale Kompetenz der Praktiker stellt. Es zeigte sich aber auch, dass in den meisten Fällen implizit auch auf persönliche Eigenschaften Bezug genommen wurde. Dabei beschränkt sich das "richtige Verhalten" nicht auf den Umgang mit Mitarbeitern und im Rahmen des Arbeitsplatzes, sondern das Verhalten im Allgemeinen unter Berücksichtigung der charakterlichen Disposition wird behandelt. Es ist daher die Absicht, mit dieser Umfrage etwas Licht in die Disposition von Charaktereigenschaften und Arbeitsleistung bei Informationssicherheitsexpert*innen zu bringen. Die Ergebnisse können als Hinweis auf günstige Voraussetzungen für neue Mitarbeiter*innen am Arbeitsplatz gesehen werden. [4]Zu diesem Zweck wurden die Big-Five-Persönlichkeitseigenschaften (Rammstedt et al. 2013) eingesetzt, die ein Fünf-Faktoren-Modell zur Gruppierung von Persönlichkeitsmerkmalen liefern.

[4] Der Verweis auf die folgenden Persönlichkeitsprofile für die künftige Verwendung muss unter sorgfältiger Berücksichtigung mehrerer Einschränkungen erfolgen, die solche Messmethoden mit sich bringen. Erstens ist die Persönlichkeit kein stabiles Konstrukt und verändert sich im Laufe der Zeit. Das Ergebnis des Fragebogens kann daher bei mehreren Wiederholungen im Laufe der Zeit variieren. Zweitens kann die soziale Erwünschtheit nicht ausgeschlossen werden, da die Teilnehmer dazu neigen, das zu beantworten, was sie gerne wären, anstatt ein wahrheitsgetreues Bild zu liefern.

Diesem Modell zufolge beschreiben die folgenden fünf Grundfaktoren die meisten Persönlichkeitsmerkmale in dichotomer Form, wobei jedes Merkmal zwei Extreme beinhaltet:

Dimension	Hohe Punktzahlen	Niedrige Punktzahlen
Offenheit	erfinderisch/neugierig	konsequent/vorsichtig
Gewissenhaftigkeit	effizient/organisiert	extravagant/unvorsichtig
Extraversion	anhänglich, gesellig, gesprächig, lebenslustig, aktiv, leidenschaftlich	zurückhaltend, Einzelgänger, ruhig, nüchtern, passiv, gefühllos
Annehmlichkeit	freundlich/mitfühlend	kritisch/rational
Neurotizismus	sensibel/nervös	widerstandsfähig/zuversichtlich

Tabelle 3: Dimensionen der Big-5.

Der BFI-10 ist eine 10-teilige Skala zur Messung der oben genannten Merkmale. Diese Skala wurde speziell für Situationen entwickelt, in denen die Zeit der Befragten begrenzt ist, und ist kurz. Jede BFI-10-Skala besteht aus einem richtig bewerteten und einem falsch bewerteten Item, z. B. wird für die Messung der Offenheit der Wert aus Frage sechs vom Wert aus Frage zehn abgezogen. Je höher das Ergebnis ist, desto erfinderischer/neugieriger ist eine Person.

Nr.	Artikel	Polar-ität	Unterskala
1	Ich bin eher zurückhaltend reserviert.	-	Extraversion
2	Ich vertraue anderen leicht und glaube an das Gute im Menschen.	+	Annehmlichkeit
3	Ich bin eher bequem und neige zur Faulheit.	-	Gewissenhaftigkeit
4	Ich bin eher entspannt und kann gut mit Stress umgehen.	-	Neurotizismus
5	Ich habe wenig künstlerische Interessen.	-	Offenheit
6	Ich bin aufgeschlossen und kontaktfreudig.	+	Extraversion
7	Ich neige dazu, andere zu kritisieren.	-	Annehmlichkeit
8	Ich erledige Aufgaben gründlich.	+	Gewissenhaftigkeit
9	Ich werde leicht nervös.	+	Neurotizismus
10	Ich habe eine rege Phantasie.	+	Offenheit

Tabelle 4: Aufbau des BFI-10

Aus den nachstehenden Histogrammen lässt sich ableiten, dass die Befragten insgesamt eher effizient/organisiert als extravagant/nachlässig sind (siehe Gewissenhaftigkeit). Auch bei der Offenheit sind die Antworten positiv verteilt; wir sehen, dass sich mehr Befragte als erfinderisch/neugierig und weniger als konsequent/vorsichtig bezeichnen (siehe Offenheit). Die Befragten verteilen sich fast gleichmäßig auf die Definitionen der Extraversion, mit einer marginalen positiven Abweichung, d. h. die Befragten werden eher als kontaktfreudig/energetisch als als eigenbrötlerisch/zurückhaltend eingestuft (in einem sehr begrenzten Umfang). Die umgekehrte Situation ist bei Neurotizismus und Verträglichkeit zu beobachten. In diesem Fall sind die Befragten eher belastbar/zuversichtlich und kritisch/rational als sensibel/nervös bzw. freundlich/mitfühlend. Die allgemeine Nachsichtigkeit ist in Abbildung 24sehen.

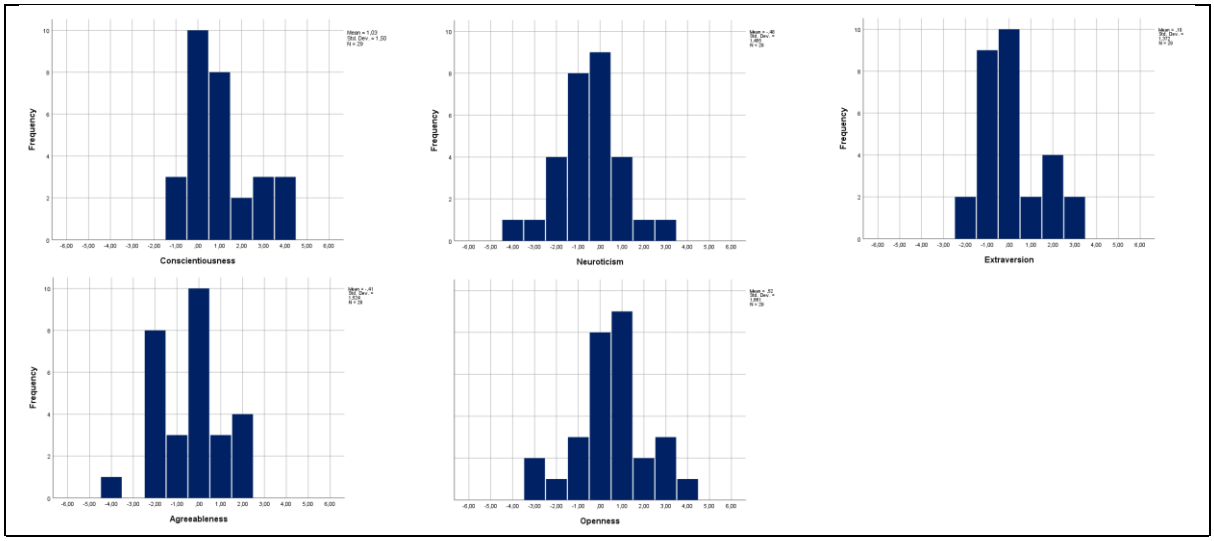


Abbildung 23: Big-Five-Histogramme für Praktiker der Informationssicherheit.

Aus der Kronzeugenregelung lassen sich mehrere entscheidende Annahmen über die Charaktereigenschaften von Informationssicherheitsexpert*innen ableiten. Der dominanteste Faktor ist der positive Wert für Gewissenhaftigkeit, der eine starke Disposition zu effizientem und organisiertem Verhalten mit sich bringt. Die negativen Werte für Neurotizismus unterstützen die Einschätzung der Expert*innen, dass Belastbarkeit und Vertrauen in die eigene Arbeit eine wichtige Rolle im Job spielen. Ferner können Expert*innen als konsequent und vorsichtig (Offenheit), kritisch und rational (Verträglichkeit) und in begrenztem Maße als zurückhaltend (Extraversion) charakterisiert werden.

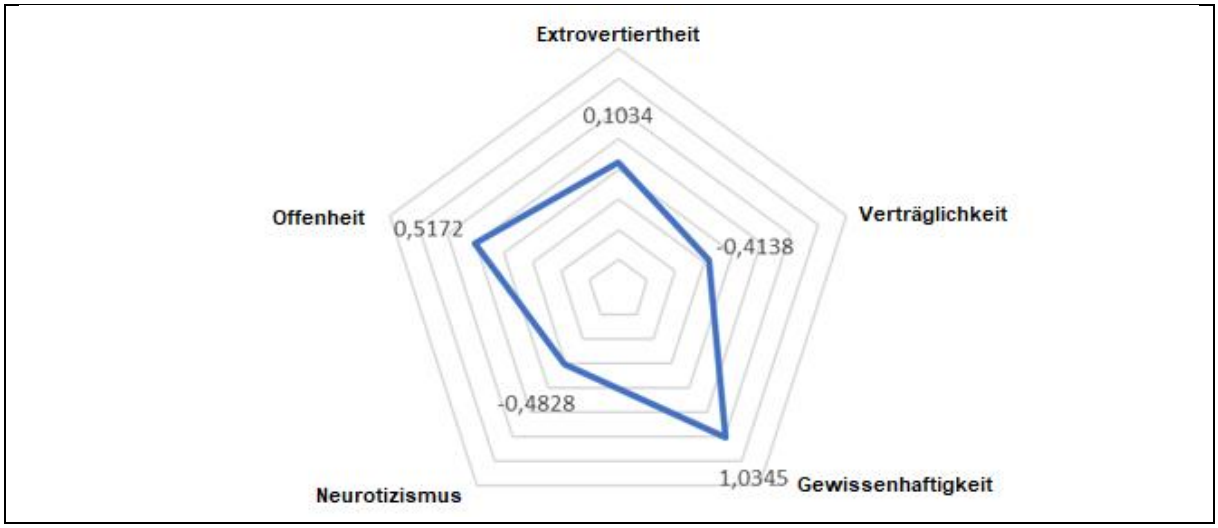


Abbildung 24: Big-Five, Mittelwertvergleich

Wie wir aus der Ladungsmatrix in Tabelle 5ersehen können, weisen im Allgemeinen alle Items ihre höchste Ladung auf dem entsprechenden Faktor auf, was den Hypothesen entspricht. Das spricht für die Gültigkeit des Ansatzes in unserem Fall.

Artikel	E	A	C	N	O
Ich sehe mich selbst als jemand, der zurückhaltend ist.	**,411***	0.067	0.212	-0.264	-0.169
Ich sehe mich selbst als jemanden, der im Allgemeinen vertrauensvoll ist.	**-,422***	**-,572****	-0.054	-0.081	0.210
Ich sehe mich selbst als jemand, der zur Faulheit neigt.	-0.163	0.138	**-,597****	0.097	0.294
Ich sehe mich als jemand, der entspannt ist und gut mit Stress umgehen kann.	0.193	0.039	0.113	**-,379***	-0.233
Ich sehe mich selbst als jemanden, der wenig künstlerische Interessen hat.	-0.101	-0.006	**-,375***	0.089	**,670****
Ich sehe mich selbst als jemand, der aufgeschlossen und gesellig ist.	**-,635****	**-,401***	-0.194	0.067	0.095
Ich sehe mich selbst als jemanden, der dazu neigt, Fehler bei anderen zu finden.	0.091	**,538****	-0.154	0.283	-0.026
Ich sehe mich selbst als jemanden, der gründliche Arbeit leistet.	0.281	0.039	**,566****	-0.335	-0.264
Ich sehe mich selbst als jemanden, der leicht nervös wird.	-0.137	0.350	-0.271	**,678****	0.000
Ich sehe mich selbst als jemanden, der eine rege Phantasie hat.	0.191	0.267	0.175	-0.137	**-,493****

Tabelle 5 : "Validitätstest: Korrelation zwischen Items und Gruppen"

Die zurückhaltenden Befragten sehen sich selbst als entspannte Menschen. Sie glauben auch, dass sie gründliche Arbeit leisten und eine rege Phantasie haben. Befragte, die sich im Allgemeinen als vertrauensvoll bezeichnen, sind auch aufgeschlossener und geselliger. Faule Befragte haben wenig künstlerische Interessen, sind aufgeschlossen und gesellig, bemängeln aber auch andere. Entspannte Befragte denken, dass sie gründliche Arbeit leisten und haben eine rege Fantasie. Diejenigen, die dazu neigen, andere zu kritisieren, werden leicht nervös und sehen sich selbst als jemanden, der eine aktive Vorstellungskraft hat. Die "gründlichen" Befragten schließlich haben eine aktive Vorstellungskraft.

4.2.7 Arbeitsleistung

Dieser Teil basiert auf dem Individual Work Performance Questionnaire (IWPQ). Der IWPQ ist eine 18-teilige Skala, die von Ramos-Villagrasa et al. (2019) entwickelt wurde, um die drei Hauptdimensionen der Arbeitsleistung zu messen:

- Aufgabenerfüllung (5 Punkte)
- kontextbezogene Leistung (8 Punkte)
- kontraproduktives Arbeitsverhalten (5).

Alle Items haben einen Erinnerungszeitraum von drei Monaten und eine 5-stufige Bewertungsskala (0 = selten bis 4 = immer für Aufgaben- und Kontextleistung; und 0 = nie bis 4 = oft für kontraproduktives Arbeitsverhalten). Bei kontraproduktivem Verhalten ist die Skala negativ gepolt, d. h. niedrigere Werte sind wünschenswerter, da dies zu weniger kontraproduktivem Verhalten im Allgemeinen führt. Die jeweiligen Werte sind in Abbildung 25bis Abbildung 27dargestellt, das endgültige Profil ist in Abbildung 28zusammengefasst.

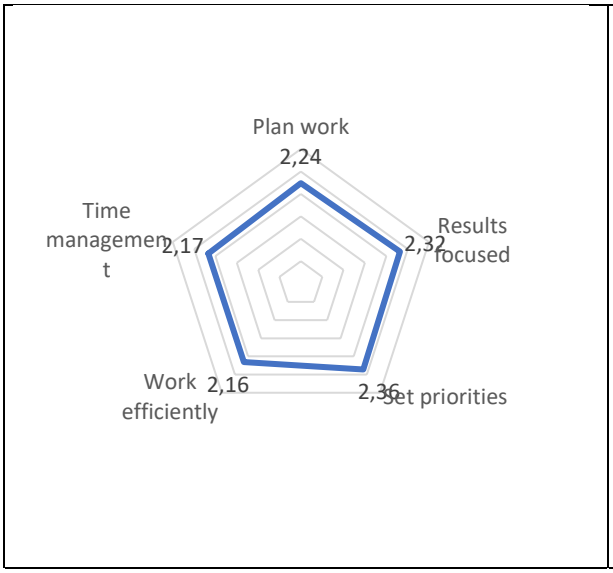


Abbildung 25: Aufgabenerfüllung

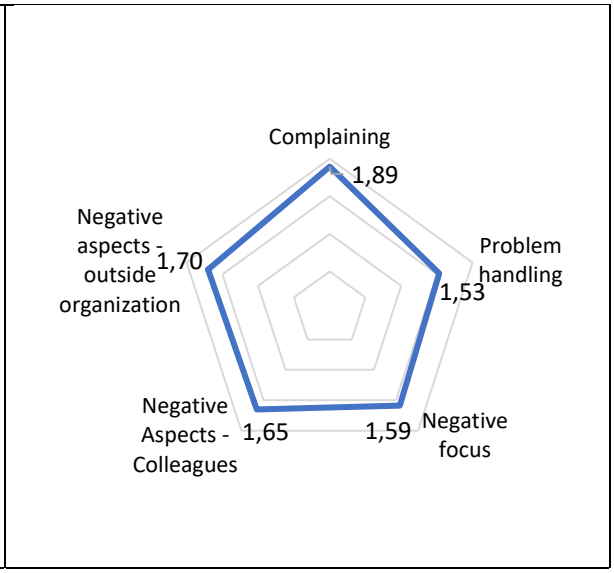


Abbildung 26: Kontraproduktives Verhalten

Es fällt auf, dass die Teilnehmer*innen über eine niedrige Punktzahl für kontraproduktive Verhaltensweisen verfügen, was das Ergebnis des BIG.5-Tests untermauert, dass Belastbarkeit und eine hohe Toleranzrate wichtige Aspekte für die Arbeit eines Informationssicherheitsexperten sind. Betrachtet man die einzelnen Kategorien, so sind die auffälligsten Faktoren die "Aktualisierung des berufsbezogenen Wissens" (2,32) und die "aktive Teilnahme" bei der kontextbezogenen Leistung, eine schwache "Konzentration auf die negativen Aspekte der Arbeit" (1,59) und eine starke "Problembewältigungs"-Orientierung (1,53) bei den kontraproduktiven Verhaltensweisen und eine hohe Konzentration auf "Prioritätensetzung" (2,36) und "Ergebnisorientierung" (2,32) bei der Aufgabenleistung.

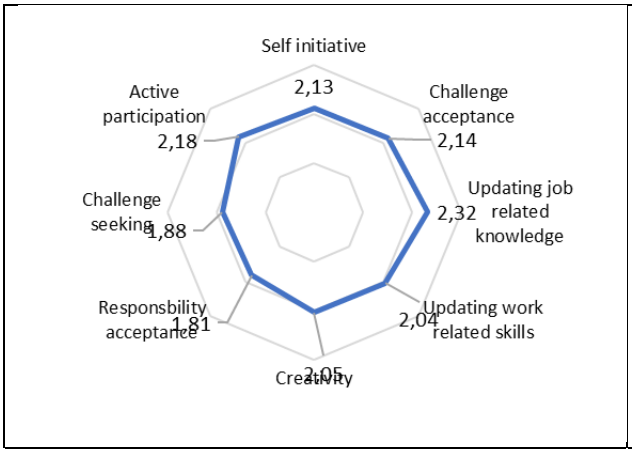


Abbildung 27 : Kontextbezogene Leistung

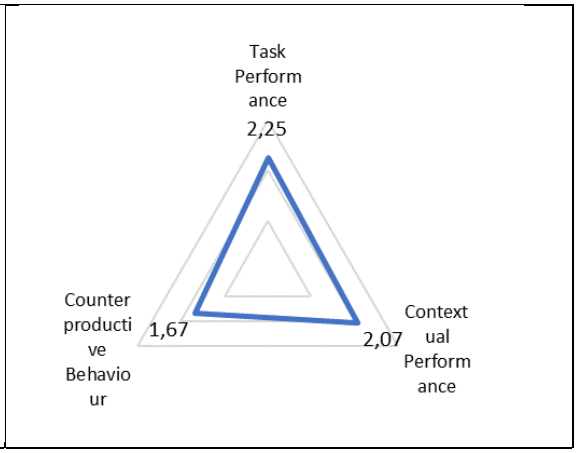


Abbildung 28: IWPQ-Ergebnisse für Informationssicherheitsexpert*innen

Wie aus Abbildung 28hervorgeht, ist die Messung der Aufgabenleistung höher als andere Messungen, und die Messung der kontextbezogenen Leistung ist höher als die Messung des kontraproduktiven Verhaltens. Diese Ergebnisse stehen im Einklang mit früheren Studien. Dennoch ist die Aufgabenleistung signifikant niedriger als die Basisergebnisse anderer Artikel, was auf Probleme in diesem Bereich hinweist - höhere Messwerte für kontraproduktives Verhalten unterstützen dieses Ergebnis. Die Messwerte für die kontextbezogene Leistung sind ebenfalls niedriger als in anderen Studien, jedoch nicht signifikant.

Zusammenfassend lässt sich sagen, dass die Teilnehmer*innen aus dem Bereich der IT- und Informationssicherheit weniger produktiv sind, als in den einschlägigen Studien üblicherweise beobachtet wird.

4.3 Zusammenfassung

Insgesamt liefert die Studie wichtige Erkenntnisse zur Informationssicherheit in KMU. Hinsichtlich der Situation auf dem Arbeitsmarkt und der Kapazitäten in den Unternehmen ist zu erwähnen, dass es in mehr als 50 % der Firmen bisher keinen Mitarbeiter und keine Mitarbeiterin gibt, der/die formal für die Informationssicherheit zuständig ist. Bejaht man die Frage, so ist in den meisten Fällen nur ein Mitarbeiter für dieses Tätigkeitsfeld zuständig. Betrachtet man die Entwicklung des Stellenangebots, so lassen sich kaum Veränderungen feststellen. Ein Teil der Unternehmen wird in den nächsten fünf Jahren etwa sechs bis zehn Stellen im Bereich der Informationssicherheit schaffen.

Die Ergebnisse untermauern das bestehende Gefühl des "Lernens durch Schmerzen", d.h., dass erst ein Vorfall eintreten muss, bevor Unternehmen Sicherheitsmaßnahmen ergreifen. Diese Aussage wird durch die übereinstimmenden Ergebnisse in Bezug auf Zertifizierungen, die Schaffung spezifischer Positionen und allgemein ergriffene Maßnahmen zur Informationssicherheit untermauert.

Hinsichtlich der geforderten Art der Aus- und Weiterbildung kann die große Bedeutung der Berufserfahrung hervorgehoben werden. Fast die Hälfte der Teilnehmer*innen gab an, dass dies besonders wichtig ist. Im Allgemeinen bevorzugen die Befragten einen Mitarbeiter/eine Mitarbeiterin mit Erfahrung gegenüber einem mit Ausbildung. Angesichts der bestehenden Knappheit an Einstellungsmöglichkeiten auf dem Arbeitsmarkt halten die Unternehmen die Weiterqualifizierung bestehender Mitarbeiter für die praktikabelste Option zur Deckung des Personalbedarfs.

Schließlich wurden durch eine Bewertung der charakteristischen Eigenschaften mittels des Big-5-Persönlichkeitstests und des IWPQ wichtige Eigenschaften von Mitarbeiter*innen identifiziert, die bei neuen Mitarbeiter*innen in diesem Bereich festgestellt werden können. Neben einer starken Disposition zur Belastbarkeit wurden in beiden Tests vor allem ein organisierter Arbeitsablauf und eine kritische und analytische Herangehensweise als charakteristische Eigenschaften bei Informationssicherheitsspezialisten festgestellt.

5 Leitfaden für KMU

Datenschutz und Informationssicherheit haben in dem Maße an Bedeutung gewonnen, in dem die IKT in den Organisations- und Managementprozessen von KMU immer intensiver eingesetzt werden. Der Druck auf KMU, Informationssicherheit und Datenschutz besser zu handhaben, kommt aus mehreren Richtungen. Erstens sind die Prozesse und das Datenmanagement in KMU in hohem Maße von der IKT-Infrastruktur abhängig geworden. Zweitens wurden die Rechtsvorschriften zum Schutz der Privatsphäre und des Datenschutzes verschärft und detaillierter kodifiziert. Drittens ist das öffentliche Bewusstsein für das Recht auf Privatsphäre und die Verantwortung für die Nutzung personenbezogener Daten gestiegen. Mehrere Vorfälle von Datenlecks auf der ganzen Welt trugen ebenfalls dazu bei, dass die Informationssicherheit bei der Nutzung digitaler Dienste als vorrangiges Thema erkannt wurde. KMU sind im Vergleich zu Großunternehmen weniger stark von der Digitalisierung betroffen. Dennoch arbeitet ein großer Teil von ihnen mit persönlichen digitalen Daten. Einige der KMUs verwalten sensible Daten. All diese Faktoren bilden die Grundlage für eine bessere Regulierung und Gewährleistung der Informationssicherheit und des Datenschutzes in KMUs. Aufgrund der aktualisierten Vorschriften der Europäischen Union haben einige KMU Schwierigkeiten, geeignetes Personal zu finden oder vorzubereiten, das die strengeren Anforderungen an die Informationssicherheit und den Datenschutz erfüllen kann.

Auf der Grundlage der Literaturrecherche und der Informationen, die während der Veranstaltungen zur Verbreitung der Projektergebnisse gesammelt wurden, kann der Schluss gezogen werden, dass es für KMU mehrere Bereiche gibt, in denen Fragen der Informationssicherheit und des Datenschutzes zusätzliche Aufmerksamkeit erfordern. Die folgenden Leitlinien heben die wichtigsten Überlegungen und möglichen Lösungen für die Probleme im Zusammenhang mit der Informationssicherheit und dem Datenschutz hervor, mit denen KMU konfrontiert sind.

1. Die Umsetzung der Datenschutz-Grundverordnung führte zu erheblichen Veränderungen in der digitalen und physischen Datenverwaltung für KMU. Einige Organisationen verfügten nicht über eine geeignete physische und digitale Infrastruktur, um die neuen Anforderungen zu erfüllen. In den meisten Fällen wurde die Übergangszeit vor der Umsetzung der DSGVO genutzt, um infrastrukturelle Defizite auszugleichen. Eine der greifbarsten Maßnahmen für KMU besteht darin, den Zustand der physischen Infrastruktur zu prüfen und die Mängel zu beheben, die den Anforderungen an eine angemessene Informationssicherheit und Datenschutzgarantie in der Organisation entgegenstehen. Erstens muss es ein internes Dokument geben, in dem die Verfahren und Vorschriften im Zusammenhang mit der Informationssicherheit und dem Datenschutz festgelegt sind (einschließlich verbindlicher Unternehmensregeln, wenn das Unternehmen Daten in Nicht-EU-Länder übermittelt). Zweitens muss es physische Zugangsbeschränkungen für physische Unterlagen geben (Schließfächer, Tresore, Bereiche mit begrenztem Zugang). Das Personal muss über die Verfahren im Zusammenhang mit der Datenverwaltung informiert werden (Beschränkungen der Weitergabe von Informationen, Verschließen der Aufzeichnungen vor öffentlichem Zugriff, Richtlinien für die Zustimmung zur Datennutzung, Passwort- und Arbeitsplatzsicherheitsrichtlinien, Verwaltung von Benutzerrechten).

2. Die betroffenen Personen (Klient*innen) müssen über die Datenverwaltungspraktiken in den Bereichen, in denen ihre Daten verwendet werden, informiert werden. Die Klient*innen müssen die Erlaubnis erhalten, auf ihre personenbezogenen Daten zuzugreifen, und sie müssen über das Recht informiert werden, die Berichtigung der

entsprechenden Daten zu verlangen, der Verarbeitung zu widersprechen, die Zustimmung zum Zugriff auf die Daten zurückzuziehen, eine Beschwerde einzureichen, die Löschung der Aufzeichnungen zu verlangen und den Datentransaktionen mit anderen Datenverwaltungssubjekten zu widersprechen.

3. Ein weiterer Bereich, in dem KMU mit Unstimmigkeiten mit den Vorschriften zur Informationssicherheit und zum Datenschutz konfrontiert sind, ist die Erhebung von Daten, die nicht erhoben oder gespeichert werden sollten. Die Daten werden in der Regel aufgrund veralteter Prozesse oder Arbeitsabläufe erhoben. In einigen Fällen werden die Daten mit Informationssystemen oder anderen digitalen Identifizierungsmaßnahmen verknüpft. Um solche Fälle zu vermeiden, sollten sich KMU darauf konzentrieren, nur so viele Daten wie nötig aufzubewahren und die Daten zu löschen, wenn ihr Verwendungszweck irrelevant ist. Vorhandene Datensätze sollten auf der Grundlage transparenter Algorithmen und Verfahren gespeichert und verwaltet werden. Sicherheitsrichtlinien wie "sauberer Schreibtisch" oder "gesperrter Bildschirm" sollten in KMU als Standard gelten.

4. Die vierte Leitlinie bezieht sich auf die Qualität von Ausbildung und Zertifizierung. Aus der Literaturanalyse und direkten Berichten von KMU-Mitarbeiter*innen geht hervor, dass die Zertifizierung für kleine und mittlere Unternehmen nicht der optimale Weg ist, um Bewerber auszuwählen, die mit privaten Informationen arbeiten könnten. Das Hauptkriterium sind Kenntnisse und Kompetenzen, die den IKT- und Rechtsbereich sowie andere interdisziplinäre soziale Fähigkeiten abdecken. KMU verfügen in der Regel nicht über die notwendigen Ressourcen, um gut ausgebildete Spezialisten für die Pflege der Informationsinfrastruktur einzustellen. Außerdem sind die Tätigkeitsbereiche der verschiedenen KMU sehr unterschiedlich. Dies führt zu dem Problem, dass universelle Ausbildungskurse oder -zertifikate die Mitarbeiter*innen nicht mit spezifischem Wissen ausstatten, das in engen Bereichen anwendbar ist. KMU benötigen praktisch anwendbare und szenariobasierte Schulungen mit Beispielen aus der Praxis. Eine Möglichkeit, diese Informationen zur Verfügung zu stellen, besteht darin, die Prozesse innerhalb des Unternehmens zu dokumentieren und die Erfahrungen später über berufliche Netzwerke oder Gemeinschaftsveranstaltungen weiterzugeben. Alternativ könnten KMU eine Zusammenarbeit mit Hochschuleinrichtungen initiieren, die die Fälle wissenschaftlich analysieren und damit das vorhandene Wissen in bestimmten Bereichen bereichern könnten.

5. Die letzte Leitlinie bezieht sich auf die Unstimmigkeiten oder Unzulänglichkeiten in den Rechtsvorschriften. Für einige Einrichtungen können die Beschränkungen des Austauschs von Informationen und personenbezogenen Daten eine ernsthafte Belastung darstellen, wenn es darum geht, die Interessen ihrer Klient*innen zu wahren. Ein Altersheim hat beispielsweise einen ständigen Bewohner, der keine Familienangehörigen mehr hat. Wenn der Bewohner in einem Notfall ins Krankenhaus gebracht wird, gibt die derzeitige Einrichtung keine privaten Informationen an Dritte weiter (auch nicht an das Altersheim). Wenn der Klient in ein anderes Krankenhaus verlegt wird, muss das Altersheim selbst nachforschen, um den Bewohner zu finden. In diesem Fall halten sich beide Einrichtungen an das Gesetz, aber die Situation schafft Rechtslücken, die geschlossen werden müssen. Die KMU sollten eine Korrektur oder die Einführung von Rechtsnormen (durch politische Vertreter) initiieren, die solche Fragen abdecken.

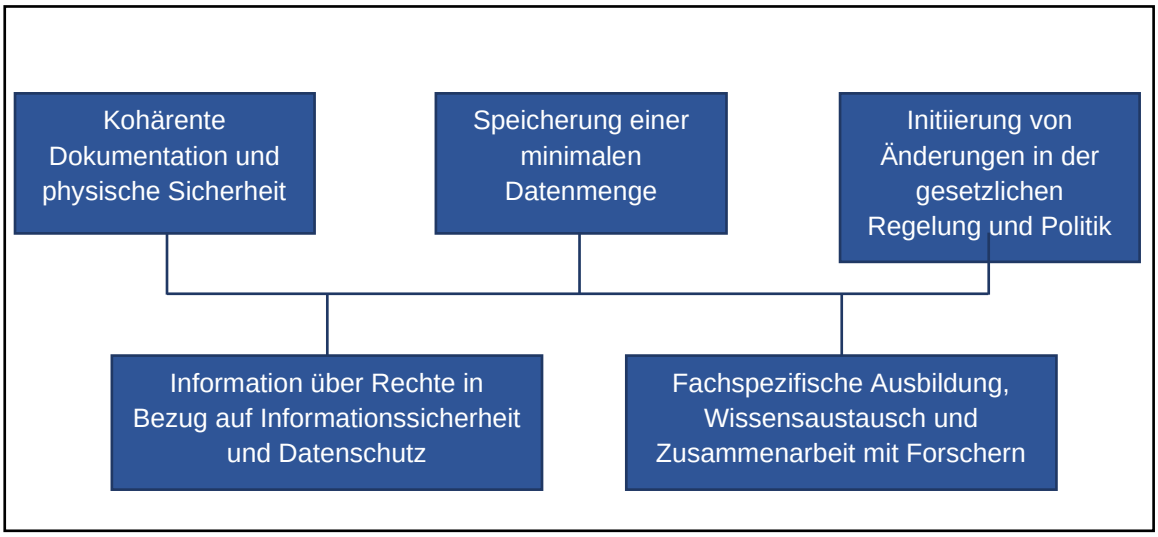


Abbildung 29: Leitlinien auf der Grundlage gemeinsamer Probleme, mit denen KMU im Bereich Informationssicherheit und Datenschutz konfrontiert sind

6 Ausblick und Empfehlungen

Während der Durchführung des TeBeISi-Projekts zeigte sich, dass der Bedarf an Schulungen zur Informationssicherheit und zum Schutz personenbezogener Daten in kleinen und mittleren Unternehmen und sozialen Einrichtungen hoch ist. Diese Organisationen haben oft finanzielle Nachteile bei der Einstellung eines professionellen Datenschutzbeauftragten, so dass diese Funktionen oft anderen Mitarbeiter*innen zugewiesen werden. Ziel ist es, die Anforderungen der Datenschutz-Grundverordnung zu erfüllen und den Schutz der personenbezogenen Daten von Klient*innen und Mitarbeiter*innen des Unternehmens zu gewährleisten. Das Projekt hat auch gezeigt, dass Schulungen zur Informationssicherheit und zum Schutz personenbezogener Daten relativ teuer sind und dass KMU sehr froh sind, wenn sie kostenlose Qualitätsschulungen zur Anwendung der DSGVO (im Rahmen des Erasmus-Plus-Projekts) erhalten und die Kompetenzen der Mitarbeiter*innen in den Bereichen Informationssicherheit und Schutz personenbezogener Daten verbessern können.

Der im Rahmen des Projekts entwickelte Fragebogen ermöglichte es den Mitarbeiter*innen kleiner und mittlerer Unternehmen, ihre vorhandenen Kompetenzen im Bereich der Informationssicherheit und des Schutzes personenbezogener Daten zu bewerten. Der im Rahmen des Projekts erstellte Lehrplan gibt den Beteiligten die Möglichkeit, eine geeignete Ausbildung zu wählen. Assoziierte Partner, KMU, Bildungseinrichtungen und Behörden bekundeten ihr Interesse, den Weg des TeBeiSi-Projekts fortzusetzen und bei künftigen Initiativen auf den Ergebnissen des Projekts aufzubauen. Daher planen die Projektpartner, die gemeinsamen Aktivitäten fortzusetzen und im Rahmen des nächsten Projekts ein Schulungspaket in allen Projektpartnerländern zu entwickeln und zu testen.

Die durchgeführten Projektaktivitäten erlauben es, den Unternehmen zu empfehlen, der internen Kommunikation und Schulung mehr Aufmerksamkeit zu schenken (sowohl durch die Organisation von Schulungen in den Unternehmen als auch durch die Entsendung von Mitarbeitern zu Schulungen). Alle Mitarbeiter*innen, insbesondere diejenigen, die im Arbeitsumfeld direkt mit personenbezogenen Daten in Berührung kommen, sollten sich der Datenschutzanforderungen bewusst sein und ständig darüber geschult werden, was personenbezogene Daten sind, wie sie zu erkennen sind und was mit personenbezogenen Daten gemacht werden kann und was nicht. Es ist auch notwendig, eine realistische Einschätzung des Bedarfs für die Sammlung personenbezogener Daten vorzunehmen, d.h. einen Überschussfonds zu unterhalten, der nur für die gesammelten personenbezogenen Daten notwendig ist. Kleine und mittlere Unternehmen sowie Einrichtungen des Sozialwesens sollten die Auswirkungen der Datenschutz-Grundverordnung bewerten und Problembereiche ermitteln, was Zeit für die Schulung und Sensibilisierung der Mitarbeiter*innen schaffen würde.

Es wird auch vorgeschlagen, dass Unternehmen zunächst ein Audit der von ihnen erhobenen und gespeicherten personenbezogenen Daten durchführen, um zu ermitteln, auf welche Datenverarbeitungsvorgänge sie sich konzentrieren sollten. Auf diese Weise ließe sich feststellen, welche Prozesse im Zusammenhang mit der Verwaltung personenbezogener Daten und der Informationssicherheit zusätzlicher Aufmerksamkeit bedürfen und welche Mitarbeiterkompetenzen verbessert werden müssen. Aus dem durchgeführten Fragebogen geht hervor, dass die KMU am ehesten bereit sind, in vorhandene Mitarbeiter*innen zu investieren, da dies den kosteneffizientesten Kompromiss in Bezug auf benötigte Ressourcen und Sicherheit darstellt.

7 Literatur

Adamkiewicz, S. L. (2005). *Die Korrelation zwischen Produktivität und der Verwendung von Informationssicherheitskontrollen in kleinen Unternehmen.* Dissertation Abstracts International, 66(03), 1541B. (UMI-Nr. 3167184).

Albrechtsen, E., & Hovden, J. (2010). Verbesserung des Informationssicherheitsbewusstseins und -verhaltens durch Dialog, Beteiligung und kollektive Reflexion. Eine Interventionsstudie. *Computer & Sicherheit, 29*(4), 432-445. doi: 10.1016/j.cose.2009.12.005

Anderson, C. L. & Agarwal, R. (2010). Sichere Computernutzung praktizieren: Eine empirische Multimethodenuntersuchung der Sicherheitsabsichten von Heimcomputernutzern. *MIS Quarterly*, *34*(3), 613-643.

Baker, W. H., & Wallace, L. (2007). Ist die Informationssicherheit unter Kontrolle? *IEEE Security & Privacy,* 5, 36-44. doi:10.1109/MSP.2007.11.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2018). Don't Even Think About It! The Effects of Antineutralization, Informational, and Normative Communication on Information Security Compliance. *Journal of the Association for Information Systems*, *19*(8), 689-715. doi: 10.17705/1jais.00506

Barnard-Wills, D., Cochrane, L., Matturi, K. & Marchetti, F. (2019). *Bericht über die Erfahrungen der KMU mit der Datenschutz-Grundverordnung.* https://www.trilateralresearch.com/wp-content/uploads/2020/01/STAR-II-D2.2-SMEs-experience-with-the-GDPR-v1.0-.pdf

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Einhaltung von Informationssicherheitsrichtlinien: Eine empirische Studie über rationalitätsbasierte Überzeugungen und Bewusstsein für Informationssicherheit. *MIS Quarterly*, *34*(3), 523-548. doi: 10.2307/25750690

Burns, A. J., Roberts, T. L., Posey, C., Bennett, R. J., & Courtney, J. F. (2018). Intentions to Comply Versus Intentions to Protect: A VIE Theory Approach to Understanding the Influence of Insiders' Awareness of Organizational SETA Efforts. *Decision Sciences*, *49*(6), 1187-1228. doi:10.1111/deci.12304

Burns, A.J., Roberts, T.L., Posey, C., Bennett, R.J., & Courtney, J.F. (2015). Bewertung der Rolle von Sicherheitsschulung, -training und -bewusstsein für das sicherheitsbezogene Verhalten von Insidern: An expectancy theory approach. *Proceedings of the IEEE 48th Hawaii International Conference on Systems Sciences, HI.* doi:10.1109/HICSS.2015.471

Colwill C. (2009). Menschliche Faktoren in der Informationssicherheit: Die Bedrohung durch Insider - wem kann man heutzutage noch trauen? Information Security Technical Report, *14*(4),186-96. doi:10.1016/j.istr.2010.04.004

D'Arcy, J., & Hovav, A. (2009). Passt eine Größe für alle? Untersuchung der unterschiedlichen Auswirkungen von Gegenmaßnahmen zur IS-Sicherheit. *Journal of Business Ethics*, *89*(1),59-71. doi:10.1007/s10551-008-9909-7

D'Arcy, J., Hovav, A, Galletta, D. (2009). Das Bewusstsein der Nutzer für Sicherheitsmaßnahmen und seine Auswirkungen auf den Missbrauch von Informationssystemen: ein Abschreckungsansatz. *Information Systems Research*, *20*(1), 79-98. doi: 10.1287/isre.1070.0160

Davies, J. S., & Hertig, A. C. (2008). *Theorie und Praxis des Vermögensschutzes. Sicherheit, Überwachung und Management*. Burlington, MA: Elsevier.

Doherty, N. F., & Fulford, H. (2005). Verringern Informationssicherheitsrichtlinien die Häufigkeit von Sicherheitsverstößen: An Exploratory Analysis. *Zeitschrift für Informationsressourcen-Management, 18*, 20-38.

Easttom, C. (2006). *Grundlagen der Computersicherheit*. Upper Saddle River, NJ: Prentice Hall.

Der Weg zur Cyber-Resilienz: Erkennen, Widerstehen, Reagieren. EY's 19th Global Information Security Survey 2016-17. https://www.ey.com/Publication/vwLUAssets/EY-giss-india/$FILE/EY-giss-india.pdf

Eurostat (2008): NACE Rev. 2. Online verfügbar unter https://ec.europa.eu/eurostat/de/web/nace-rev2, zuletzt geprüft am 08.07.2021.

Europäische Kommission (2021): KMU-Definition - Binnenmarkt, Industrie, Unternehmertum und KMU. Online verfügbar unter https://ec.europa.eu/growth/smes/sme-definition_en, zuletzt aktualisiert am 30.08.2017, zuletzt geprüft am 08.07.2021.

Gardner, B., & Thomas, V. (2014). *Aufbau eines Programms zur Sensibilisierung für Informationssicherheit: Defending against social engineering and technical threats*. New York, NY: Elsevier.

Goodwin, B. (2005, 14. Februar). *Große Geschütze gegen die Bedrohung der Lieferkette. Computer Weekly*. http://www.computerweekly.com/.

Guinote, A., & Vescio, K. T. (2010). *Die Sozialpsychologie der Macht*. New York, NY. The Gilford Press.

Hallová, M., Polakovič, P., Šilerová, E., & Slováková, I. (2019). Datenschutz und -sicherheit in KMU unter Unternehmensinfrastruktur. *Agris On-Line Papers in Economics & Informatics*, *11*(1), 27-33. doi:10.7160/aol.2019.110103

Herath, T., & Rao, H. R. (2009a). Förderung des Informationssicherheitsverhaltens in Organisationen: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165. doi: 10.1016/j.dss.2009.02.005

Herath, T., & Rao, H. R. (2009b). Schutzmotivation und Abschreckung: Ein Rahmen für die Einhaltung von Sicherheitsrichtlinien in Organisationen. *European Journal of Information Systems*, *18*(2), 106-125. doi: 10.1057/ejis.2009.6

Yoo, C.W., Sanders, G.L., & Cerveny, R.P. (2018). Explorating the influence of flow and psychological ownership on security education, training, and awareness effectiveness and security compliance. *Decision Support Systems*, *108*, 107-118. doi: https://doi.org/10.1016/j.dss.2018.02.009

Jasmontaitė-Zaniewicz, L., Calvi, A., Nagy, R. & Barnard-Wills, D. (2021). *The GDPR Made Simple(r) for SME's*. doi: 10.46944/9789461171092

Jenkins, J. L. & Durcikova, A. (2013). Was, ich hätte das nicht tun sollen? The influence of training and just-in-time reminders on secure behavior. *Proceedings of the International Conference on Information Systems*. AIS. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.661.9290&rep=rep1&type=pdf

Johnston, A. C. & Warkentin, M. (2010). Furchtappelle und Informationssicherheitsverhalten: An empirical study. *MIS Quarterly*, *34(*3), 549-566. doi: 10.2307/25750691

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). Ein erweiterter Rahmen für Angstappelle: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly, 39*(1), 113-134. doi: 10.25300/MISQ/2015/39.1.06

Jöns, Ingela; Hodapp, Markus; Weiss, Katharina (2005): Kurzskala zur Erfassung der Unternehmenskultur. Online verfügbar unter http://psydok.psycharchives.de/jspui/handle/20.500.11780/349.

Karjalainen, M., & Siponen, M. (2011). Auf dem Weg zu einer neuen Metatheorie für die Entwicklung von Schulungsansätzen für die Sicherheit von Informationssystemen (IS). *Journal of the Association for Information Systems*, *12*(8), 518-555.

Kluge, EH. (2007). Sichere elektronische Gesundheitsdienste: Umgang mit Risiken für Gesundheitsdaten von Patienten. International Journal of Medical Informatics**,** *76* **(**5-6**)**, 402-406**.** doi: 10.1016/j.ijmedinf.2006.09.003

Kogenhop, G. (2020). Werkzeuge für optimale Resilienz. *Journal of Business Continuity & Emergency Planning*, *13*(4), 352-361.

Kumar, V., Batista, L. & Maull, R. (2011). Der Einfluss der Betriebsleistung auf die Kundentreue. *Service Science*, *3*(2), 158-171. doi:10.1287/serv.3.2.158

Kuusisto, T., & Ilvonen, I. (2003). Informationssicherheitskultur in kleinen und mittleren Unternehmen. *Frontiers of e-business research*, 431-439.

Lee, J. K., Cho, D., & Lim, G. G. (2018). Design und Validierung des Bright Internet. *Journal of the Association for Information Systems*, 19(2), 63-85.

Leede, J. & Looise, J. K. (2005). Innovation und HRM: Auf dem Weg zu einem integrierten Rahmen. *Creativity and Innovation Management, 14* (2), 108-117. doi: 10.1111/j.1467-8691.2005.00331.x.

Leilanie Del Prado-Lu, J. (2005). *Geschlecht, Informationstechnologie und Gesundheit*. Quezon City, Philippinen: The University of the Philippines Press.

Liang, H. & Xue, Y. (2010). Verständnis des Sicherheitsverhaltens bei der Nutzung von Personal Computern: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394-413.

McAfee, I. (2010). *Ein gutes Jahrzehnt für Internetkriminalität.* http://www.mcafee.com/ca/resources/reports/rp-good-decade-for-cyber crime.pdf.

McConnell, J. P. (2020). *UNIX Administrator Information Security Policy Compliance: The Influence of a Focused SETA Workshop and Interactive Security Influence of a Focused SETA Workshop and Interactive Security Challenges on Heuristics and Biases Challenges on Heuristics and Biases*. https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=2127&context=gscis_etd.

Mohjel Eghdam, A., Khameneh, S., Hasankhni, H, Moghadam, S., Zamanzadeh V. (2013). Die Leistung von Krankenschwestern und Krankenpflegern in Bezug auf den iranischen Ethikkodex für die Krankenpflege aus Sicht der Patienten. *26*(84),1-11. doi: 10.5681/jcs.2013.027

Newell, S., & Marabelli, M. (2015). Strategische Chancen (und Herausforderungen) der algorithmischen Entscheidungsfindung: A call for action on the long-term societal effects of datification. *The Journal of Strategic Information Systems, 24*(1), 3-14. doi: 10.2139/ssrn.2644093

Noguerol, L. O., & Branch, R. (2018). Leadership and Electronic Data Security within Small Businesses: An Exploratory Case Study. *Journal of Economic Development, Management, IT, Finance & Marketing*, *10*(2), 7-35.

Northouse, P. G. (2010). *Leadership: Theorie und Praxis* (5. Aufl.). Thousand Oaks, CA: Sage.

O'Rourke, M. (2003). Cyber-Angriffe veranlassen zur Reaktion auf Sicherheitsbedrohungen. *Risikomanagement, 50*(1), 8.

Peikari, H. R., T., R., Shah, M. H., & Lo, M. C. (2018). Die Wahrnehmung des Informationssicherheitsmanagements in Gesundheitszentren durch die Patienten: die Rolle organisatorischer und menschlicher Faktoren. *BMC Medical Informatics & Decision Making*, *18*(1), 1-13. doi:10.1186/s12911-018-0681-z

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). Der Schutz von Informationsbeständen in Unternehmen durch Insider: Entwicklung einer auf Systematik basierenden Taxonomie und Theorie der Vielfalt für schutzmotivierte Verhaltensweisen. *MIS Quarterly, 37*(4), 1189-1210. doi: 10.25300/MISQ/2013/37.4.09

Posey, C., Roberts, T., & Lowry, P.B. (2015). Die Auswirkung des organisatorischen Engagements auf die Motivation von Insidern, Unternehmensinformationen zu schützen. *Journal of Management Information Systems, 32*(4), 179-214. Doi: 10.1080/07421222.2015.1138374

Puhakainen, P., & Siponen, M. (2010). Verbesserung der Compliance von Mitarbeitern durch Schulungen zur Sicherheit von Informationssystemen: An action research study. *MIS Quarterly*, *34*(4), 757-778. doi: 10.2307/25750704

Rammstedt, Beatrice; Kemper, Christoph J.; Klein, Mira Céline; Beierlein, Constanze; Kovaleva, Anastassiya (2013): A Short Scale for Assessing the Big Five Dimensions of Personality. 10 Item Big Five Inventory (BFI-10). In: GESIS - methoden, daten, analyse 7 (2), S. 233-249.

Ramos-Villagrasa, Pedro J.; Barrada, Juan R.; Fernández-del-Río, Elena; Koopmans, Linda (2019): Assessing Job Performance Using Brief Self-report Scales: The Case of the Individual Work Performance Questionnaire. In: Revista de Psicología del Trabajo y de las Organizaciones 35 (3), S. 195-205. DOI: 10.5093/jwop2019a21.

Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (2016). In: Amtsblatt der Europäischen Union L 119, S. 1-88.

Richardson, R. (2008). *CSI-Umfrage über Computerkriminalität und -sicherheit.* http://www.cse.msstate.edu/~cse6243/ readings/CSIsurvey2008.pdf.

Sabeeh, A., und Lashkari, A. H. (2011). *User's Perceptions on Mobile Devices Security Awareness in Malaysia.* International Conference for Internet Technology and Secured Transactions, Abu Dhabi: IEEE, 428-435.

Sicari, S., Cappiello, C., De Pellegrini, F., Miorandi, D., & Coen-Porisini, A. (2016). Eine sicherheits- und qualitätsbewusste Systemarchitektur für das Internet der Dinge*. Information Systems Frontiers*, *18*(4), 665-677.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Sicherheit, Datenschutz und Vertrauen im Internet der Dinge: The road ahead. *Computer Networks*, *76*, 146-164. doi: doi.org/10.1016/j.comnet.2014.11.008

Siponen, M., & Vance, A.O. (2010). Neutralisierung: Neue Einblicke in das Problem der Verletzung der Sicherheitsrichtlinien von Mitarbeitersystemen. *MIS Quarterly*, *34*(3), 87-502.

Siponen, M., Mahmood, M., & Pahnila, S. (2009). Setzen Mitarbeiter Ihr Unternehmen einem Risiko aus, wenn sie die Richtlinien zur Informationssicherheit nicht befolgen? *Communications of the ACM*, *52*(12), 145-147. doi: 10.1145/1610252.1610289

Smith, M. (2003). Geschäftsprozessgestaltung: Korrelate von Erfolg und Misserfolg. *The Quality Management Journal, 10* (2) 38-49. doi: 10.1080/10686967.2003.11919062.

Das Europäische Parlament und der Rat der Europäischen Union (2016). *Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus für Netz- und Informationssysteme in der Union.* https://eur-lex.europa.eu/eli/dir/2016/1148/oj (Zugriff am 31. Januar 2020).

Das Europäische Parlament und der Rat der Europäischen Union (2016). *Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.* https://eur-lex.europa.eu/eli/reg/2016/679/oj (Zugriff am 31. Januar 2020).

van Zadelhoff, M., Lovejoy, K., & Jarvis, D. (2014). *Fortifying for the future: Insights from the 2014 IBM Chief Information Security Officer Assessment*. https://www.ibm.com/smarterplanet/us/en/centerforappliedinsights/article/ciso_insights.html.

von Solms, S. H., & von Solms, R. (2009*). Information Security Governance*. NewYork, NY: Springer.

Weber, R. H. (2010). Internet der Dinge: New security and privacy challenges. *Computer Law & Security Review, 26*(1), 23-30. doi: 10.1016/j.clsr.2009.11.008

Whitman, M.E., & Mattord, H.J. (2012). *Principles of Information Security* (4thed.). Boston, MA: Course Technology.

Wilkinson, G. (2018). General Data Protection Regulation: Kein Patentrezept für kleine und mittlere Unternehmen. *Journal of Payments Strategy & Systems*, *12*(2), 139-149.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *Management Information Systems Quarterly*, *37* (1): 1-20. doi:10.25300/MISQ/2013/37.1.01

Forschungsbericht

Wir danken den Mitverfassern und Herausgebern:

Simon Rath

Prof. Irena Žemaitaitytė

Mgr. Agata Katkonienė

Assoc. Prof. Marius Kalinauskas

Prof. Odeta Merfeldaitė

Assoc. Prof. Asta Railienė

Iwan Karitonow

Teresa Rauenbusch

Teilzertifizierung im Berufsfeld Informationssicherheit - TeBeISi

Gefördert durch das Programm Erasmus+ der Europäischen Union

https://information-security-in-sme.eu/.