ALARM
Awareness Labor KMU Informationssicherheit

IT-Sicherheit
IN DER WIRTSCHAFT

2021

Report zur Informationssicherheit in KMU – Sicherheitsrelevante Tätigkeitsprofile

Mittelstand-Digital

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

Bibliographische Informationen der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliographische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Impressum

Herausgeberin und Kontakt

Prof. Dr. Margit Scholl
Technische Hochschule Wildau
Hochschulring 1
15745 Wildau

alarm@th-wildau.de

Der vorliegende **Report zur Informationssicherheit in KMU – Sicherheitsrelevante Tätigkeitsprofile** ist der erste von insgesamt drei geplanten Reporten, die im dreijährigen Projekt „Awareness Labor KMU (ALARM) Informationssicherheit“ verfasst werden.

Das Projekt wird vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) gefördert.

Projektlaufzeit

01.10.2020 – 30.09.2023

Der Report basiert auf Ergebnissen einer Umfrage in Unternehmen zur Lage und zum aktuellen Stand der Informationssicherheit, die online durchgeführt wurde.

Das diesem Bericht zugrundeliegende Vorhaben wird mit Mitteln des Bundesministeriums für Wirtschaft und Klimaschutz unter dem Förderkennzeichen 01MS19002A gefördert.

Das Mittelstand-Digital Netzwerk bietet mit den *Mittelstand-Digital Zentren*, der Initiative *IT-Sicherheit in der Wirtschaft* und *Digital Jetzt* umfassende Unterstützung bei der Digitalisierung. Kleine und mittlere Unternehmen profitieren von konkreten Praxisbeispielen und passgenauen, anbieterneutralen Angeboten zur Qualifikation und IT-Sicherheit. Das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) ermöglicht die kostenfreie Nutzung und stellt finanzielle Zuschüsse bereit. Weitere Informationen finden Sie unter www.it-sicherheit-in-der-wirtschaft.de.

Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autorinnen und Autoren.

Bilder

Alle Abbildungen sind entsprechend mit Quellen vermerkt.
Titelgrafik: Forschungsgruppe Scholl
Illustrationen und Design: Olesja Mujkic und Forschungsgruppe Scholl

Juni 2022

ISBN 978-3-949639-01-2

Report zur Informationssicherheit in KMU – Sicherheitsrelevante Tätigkeitsprofile

Ergebnisse einer Umfrage im Rahmen des Projektes
Awareness Labor KMU (ALARM) Informationssicherheit

von Tippelskirch, Hubertus
Schuktomow, Regina
Scholl, Margit
Walch, Marie Christin

Forschungsgruppe
Frau Prof. Dr. rer. nat. Margit C. Scholl

Inhaltsverzeichnis

Abkürzungsverzeichnis

ALARM	Awareness Labor KMU
BMWi	Bundesministerium für Wirtschaft und Energie
BMWK	Bundesministerium für Wirtschaft und Klimaschutz
BSI	Bundesamt für Sicherheit in der Informationstechnik
DLR	Deutsches Zentrum für Luft- und Raumfahrt
DSGVO	Datenschutz-Grundverordnung
ERP	Enterprise Resource Planning (mittels Prozess-Planungssoftware)
ggf.	gegebenenfalls
gr.	groß
HR	Human Resources (Personalwesen)
i. d. R.	in der Regel
IHK	Industrie- und Handelskammer
inkl.	inklusive
IS	Informationssicherheit
ISMS	Informationssicherheitsmanagementsystem
IT	Informationstechnologie
kl.	klein
KMU	kleines und mittleres Unternehmen; kleine und mittlere Unternehmen
m. E.	meines Erachtens
PDA	persönlicher digitaler Assistent (Synonym: „handheld (computer)“)
RFID	Radio-Frequency Identification
s.	siehe
sog.	sogenannt
TH	Technische Hochschule
TN	Teilnehmende
u. a.	unter anderem
VPN	Virtual Private Network (Netzwerktunnel)
WIK	Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste
WLAN	Wireless Local Area Network (Drahtlosnetzwerk)
WSI	Wirtschafts- und Sozialwissenschaftliches Institut
z. B.	zum Beispiel
z. T.	zum Teil

Abbildungsverzeichnis

Tabellenverzeichnis

1 Vorwort und Ergebnisreflexion

Hintergrund

Mit zunehmend allgegenwärtiger Digitalisierung wird die Bedeutung von Informationssicherheit für jede Institution von Jahr zu Jahr deutlicher. Der Begriff Informationssicherheit ist nach dem Bundesamt für Sicherheit in der Informationstechnik (BSI) umfassender als die Begriffe IT-Sicherheit oder Cyber-Sicherheit, da es sich um den Schutz der Vertraulichkeit, der Verfügbarkeit und der Integrität aller Informationen einer Institution handelt. Mehr noch: alle digital agierenden Menschen sind den Bedrohungen aus dem Cyber-Space ausgesetzt, ob dienstlich oder privat, ob bewusst reflektiert oder nicht. Treffen die vielfältigen Bedrohungen auf Schwachstellen, so werden sie zu realen Gefährdungen und können zu großen Schäden führen. Sicherheitsschwachstellen können infrastrukturelle Ursachen haben und mit technischem Systemversagen verbunden sein, sie können aber auch organisatorische Gründe und menschliche Fehlhandlungen als Ausgangspunkt vereinen. Im Unternehmenskontext muss Informationssicherheit daher *Chefsache* sein und *ganzheitlich* beachtet werden, können doch die möglichen Schäden mit einer Nichterfüllung der Aufgaben, Nichtbeachtung von Gesetzen und Verträgen, mit negativen finanziellen Auswirkungen und Imageverlusten verbunden sein.

Ohne angemessene Informationssicherheit ist die Existenz eines Unternehmens gefährdet. Das Top-Management sollte sich daher bewusst sein, gerade für die Initiierung und Etablierung eines Informationssicherheitsmanagementsystems (ISMS) inklusive seiner strategischen Ausrichtung, seiner Ressourcen (Zeit, Geld, Personen) und abgeleiteten Maßnahmen die Verantwortung zu tragen und zudem eine Vorbildfunktion inne zu haben. Auch die Initiierung von zielgerichteten Sensibilisierungs- und Schulungsmaßnahmen für alle Mitarbeitenden gehört dazu und ist von großer Bedeutung, um das Sicherheitsbewusstsein der Menschen und das Sicherheitsniveau einer Institution zu erhöhen. Darüber hinaus sind alle Mitarbeitenden selbst innerhalb ihrer konkreten Tätigkeiten und Kontexte verantwortlich, aufmerksam zu agieren und sicherheitsrelevante Risiken zu minimieren. Der Begriff Sicherheitsbewusstsein (Information Security Awareness) wird in der NIST Special Publication 800-16 [1] wie folgt definiert:

> *„Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly.“, übersetzt: „Der Zweck von Awareness-Präsentationen besteht einfach darin, die Aufmerksamkeit auf die Sicherheit zu lenken. Awareness-Präsentationen sollen es Einzelpersonen ermöglichen, IT-Sicherheitsprobleme zu erkennen und entsprechend zu reagieren.“*

Dies macht für Bada u. a. deutlich, wo der Schwerpunkt der Sensibilisierungsmaßnahmen liegen sollte: Die einzelnen Menschen müssen sich nicht nur möglicher Cyber-Risiken bewusst sein, sondern sich auch entsprechend verhalten [2].

Als das komplexe Projekt „Awareness Labor KMU (ALARM) Informationssicherheit“ mit dem Ziel des Aufbaus eines innovativen Gesamtszenarios zur Erhöhung der Informationssicherheit in kleinen und mittleren Unternehmen (KMU) von mir 2019 final entwickelt und zur Förderung ab 2020 beim Bundesministerium für Wirtschaft und Energie (BMWi) eingereicht wurde, bestand ein Teilziel darin, aus Tätigkeitsprofilen der betrieblichen Praxis entsprechende Sicherheitsprofile und letztlich Kompetenzprofile abzuleiten, um durch zielgruppenorientierte Sensibilisierungsmaßnahmen bundesweit eine Verbesserung der Information Security Awareness in KMU zu erzielen. Dazu sollten die Defizitbereiche wichtiger Geschäftsprozesse [3] systematisch und gemeinsam mit Pilot-KMU erschlossen und konkrete Tätigkeitsprofile abgeleitet werden, da dies für die Digitalisierung in KMU von zentraler Bedeutung ist, wie der Digital Office Index [4:7] zeigt. Mit Projektstart im Oktober 2020 wurde diese Ist-Analyse gemeinsam mit Unterauftragnehmern, Pilotunternehmen und assoziierten Partnern vorbereitet und im Februar 2021 durchgeführt.

Die Ist-Analyse, aus der die Profile für KMU abgeleitet werden, bestand aus psychologischen Tiefeninterviews und einer Online-Umfrage. Die Ist-Analyse im Allgemeinen und die Profildefinitionen im Speziellen sind die Basis des anvisierten innovativen Prozessszenarios für die Sensibilisierung in KMU. Als innovative Sensibilisierungsmaßnahmen werden im Projekt sieben erlebnisorientierte analoge und digitale Lernszenarien sowie „Vor-Ort-Angriffe“ und Awareness-Messungen mit und für KMU entwickelt. Die Corona-Pandemie hat jedoch die Kommunikation, den persönlichen Austausch und die konzeptionelle Erarbeitung deutlich erschwert sowie die Entwicklung und den Einsatz der Lernszenarien verzögert. Nichtsdestotrotz konnten inzwischen die Ergebnisse der tiefenpsychologischen Interviews in der ersten Studie des Projekts namens „Qualitative Wirkungsanalyse Security Awareness in KMU“ veröffentlicht werden [5]. Mit einer leichten Verzögerung folgen nun mit diesem Report 1 des Projekts die Ergebnisse der ersten Online-Umfrage von drei geplanten Online-Umfragen.

Die erste Studie [5] zu den Tiefeninterviews in KMU offenbarte, dass der Begriff Informationssicherheit für viele noch diffus ist und nicht selten Expertinnen und Experten und Dienstleistern zugeordnet wird, weshalb zukünftig die persönliche Wahrnehmung auf die eigene Verantwortung für Informationssicherheit am Arbeitsplatz geschärft werden sollte. Darüber hinaus fehlt in KMU bislang für eine nachhaltige Sensibilisierung oft die Etablierung einer Strategie zur Erhöhung von Informationssicherheitsbewusstsein in allen Tätigkeitsbereichen [5]. Eine solche Strategie muss auch Fundament der notwendigen Sicherheitskultur in KMU sein. Es ist daher zwingend, die Tätigkeitsprofile wichtiger Geschäftsprozesse des betrieblichen Alltags in KMU zu untersuchen, die Ausgangspunkt für die Ableitung der notwendigen Sicherheits- und Kompetenzprofile sind. Dazu werden u. a. auch der modernisierte IT-Grundschutz und die Standards des BSI [6] herangezogen. Die abgeleiteten Sicherheits- und Kompetenzprofile werden für alle KMU übertragbar ausgerichtet und verdeutlichen die Sicherheitsmaßnahmen der Basis-Absicherung entsprechend dem modernisierten IT-Grundschutz, so dass die praktische Umsetzung von Sicherheitsmaßnahmen für die KMU möglich wird und ihre Wettbewerbs- und Innovationsfähigkeit gestärkt werden.

Um Nachhaltigkeit zu erreichen, werden mit und für die Menschen hinter den Profildefinitionen der realitätsbezogenen betrieblichen Alltagsszenarien beispielhaft aktivierende Sensibilisierungsmaßnahmen entwickelt, erprobt und evaluiert, die mit Projektende im September 2023 als Best-Practice-Anleitungen den KMU kostenlos zur Verfügung gestellt werden. Unsere Projektstudie [5] ergab, dass die folgenden Awareness-Themen für KMU von zentraler Bedeutung sind:

1. **Passwort**
2. **Phishing, CEO Fraud & Co.**
3. **Social Engineering, Manipulation & Co.**
4. **Apps, Software & Co.**
5. **Sicher im Homeoffice**
6. **Datenschutz in der Cloud sowie Datenschutz im Kontext Kunden und Lieferanten**
7. **Messenger, sichere Übertragung, Storage (Speicherplatz), Verschlüsselung & Co.**
8. **Informationsklassifizierung (nur dort von Bedeutung, wo sie als Prozess bereits in den KMU eingeführt ist)**

Zusammenfassung der Ergebnisse

Die Ergebnisse unserer ersten Online-Umfrage innerhalb des Projekts „Awareness Labor KMU (ALARM) Informationssicherheit“ lassen vermuten, dass Informationssicherheit nicht in allen KMU tatsächlich ganzheitlich wahrgenommen wird. Ganzheitlich bedeutet nach BSI-Standard 200-1 [7:6], dass „Sicherheit […] ein integraler Bestandteil von Planung, Konzeption und Betrieb von Geschäftsprozessen und der Informationsverarbeitung sein [muss]“. Dies bedeutet, dass das Informationssicherheitsmanagement auf der Basis von IT-Grundschutz neben technischen auch infrastrukturelle, organisatorische und personelle Aspekte enthält und nur in einem solchen ganzheitlichen Ansatz die Erhöhung der Informationssicherheit nachhaltig erzielen kann [7:6]. Dabei handelt es sich um einen kontinuierlichen Prozess, dessen Strategien und Konzepte ständig auf ihre Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf fortzuschreiben sind [8:11]. Ein kontinuierlicher Verbesserungsprozess ist daher im Unternehmen zu etablieren. Die IT-Grundschutz-Methodik des BSI schlägt viele kleine Schritte im langfristigen Verbesserungsprozess ohne hohe Investitionen zu Beginn vor: Beginnend mit der *Basis*-Absicherung für die dringend erforderlichen Sicherheitsvorkehrungen [8:14] über die eng begrenzte *Kern*-Absicherung für die besonders schutzbedürftigen Werte und Ressourcen einer Institution [8:69] bis hin zur ganzheitlich umfassenden *Standard*-Absicherung [8:169].

Die hier im Report 1 getroffenen Aussagen dürfen nicht als repräsentativ, sondern nur unter Berücksichtigung der Limitierung einer kleinen Stichprobe bewertet werden. Zudem kann ein teilweise verzerrender Selektionsprozess bei der Auswahl der Probanden innerhalb der KMU für die Umfrage nicht ausgeschlossen werden. Trotzdem gibt der Report einen konkreten und aktuellen Einblick in die Ist-Situation von KMU unter Pandemie-Bedingungen. Einige Beispiele sind:

- *Die meisten Mitarbeitenden verüben ihre Tätigkeit an einem festen Arbeitsplatz.*
- *Homeoffice wird besonders häufig von Mitarbeitenden in Forschung und Entwicklung genutzt.*

- *In Zeiten der Reisebeschränkungen aufgrund der pandemischen Lage spielen Reisen in den untersuchten Gruppen kaum eine Rolle.*
- *Mobiles Arbeiten kommt in traditionellen Kerntätigkeiten kaum vor – es gehört eher in die Tätigkeitsfelder IT/Administration, Vertrieb/Außendienst, Kundenmanagement/Kundenservice.*
- *Das allgegenwärtige Kommunikationsmittel ist E-Mail, wobei E-Mail-Verschlüsselung noch keine Sicherheitsroutine in KMU darstellt.*
- *Zugangskontrollen per Biometrie werden bislang nicht verwendet – durchgängig werden Passwörter genutzt.*
- *Die überwiegende Mehrheit der Befragten sieht für sich einen Schulungsbedarf im KMU zum Thema Informationssicherheit, wobei die Mitarbeitenden in den verschiedenen Tätigkeitsfeldern unterschiedlich oft an Schulungs- und Sensibilisierungsmaßnahmen teilnehmen.*

Im vorliegenden Report 1 werden die folgenden Tätigkeitsfelder untersucht:

- Fertigung/Produktion
- Materialwirtschaft/Logistik/Lager
- Einkauf/Beschaffung
- Vertrieb/Außendienst
- Kundenmanagement/Kundenservice
- Prozessmanagement/Qualitätssicherung/Controlling
- Forschung/Entwicklung
- IT/Administration
- Sekretariat/Empfang/Pförtnerei/Poststelle
- Finanzen/Buchhaltung/Rechnungswesen
- Personal(-wesen/-verwaltung)/HR
- Marketing/Kommunikation

Außerdem werden folgende Personengruppen näher beleuchtet:

- Geschäftsleitung/Top-Management
- Mittleres Management
- Mitarbeitende
- Auszubildende/Praktikant/innen

Die Geschäftsleitung in KMU kann i. d. R. Fremdsprachen und nutzt soziale (Karriere-) Netzwerke, benötigt Online-Buchungen, nutzt Datenverschlüsselung sowie digitale Signaturen, Freeware und Backup-Software. Für die Geschäftsleitung sind mobiles Arbeiten und Reisen sowie eine häufige Nutzung u. a. von USB-Sticks, externen Festplatten, Kreditkarten, WLAN, Clouddiensten, Video-Konferenzen und Datenbanken charakteristisch. Damit ist die KMU-Personengruppe Geschäftsleitung/Top-Management extrem gefährdet und benötigt m. E. ein spezifisches Sensibilisierungs-Coaching.

Auch das Mittlere Management nutzt häufig Datenbanken, ERP-Programme und Video-Konferenzen zu ihrer Aufgabenerledigung und immer Drucker bzw. Scanner. Diese Personengruppe benötigt vermutlich sowohl eine spezifisch angepasste wie auch allgemeine Sensibilisierungsmaßnahme.

Die befragten Mitarbeitenden nutzen hingegen so gut wie nie soziale Netzwerke, Tablets, Smartphones, Payware und USB-Sticks/externe Festplatten und sind auch nicht mit vertraulichen Daten, Downloads, E-Mail-Verschlüsselung, Datenlöschung oder -verschlüsselung betraut. Drucken und Scannen sind bei ihnen allerdings ebenfalls tägliche Routine. Diese Personengruppe benötigt m. E. eine allgemeine Sensibilisierung für Informationssicherheit.

Auszubildende begeben sich in der Regel nicht auf Geschäftsreisen, folglich stehen auch keine Übernachtungen an. Ihr Arbeitsplatz wird nicht von Kunden und Geschäftspartnern aufgesucht. Auch mobiles Arbeiten, die Nutzung von Freeware, Messenger oder ERP-Programmen tritt nicht auf. Mobile Telefon- oder Video-Konferenzen, VPN/Remote, Kontakte mit Geschäftspartnern/Behörden oder Kunden sowie die Nutzung der digitalen Signatur kommen eher selten vor. Allerdings erhalten sie häufig einen Firmenschlüssel, kümmern sich um Dokumentenvernichtung, nutzen Festnetztelefone und führen durchaus externe Telefonate. Da Auszubildende unterschiedliche Abteilungen durchlaufen, arbeiten sie an wechselnden Arbeitsplätzen. Meine Empfehlung für diese Personengruppe ist, eine allgemeine Sensibilisierung für Informationssicherheit mit der Einführung in die Sicherheitsrichtlinien des KMUs zu verknüpfen. Dabei sollte beachtet werden, dass einer der Hauptgründe, warum Nutzerinnen und Nutzer sich nicht optimal verhalten, ist, dass Sicherheitssysteme und -richtlinien schlecht konzipiert sind und ungenügend kommuniziert werden [9].

Wie in der ebenfalls im „Awareness Labor KMU (ALARM) Informationssicherheit“ erstellten psychologisch gestützten Studie [5] stellte sich auch in der Online-Umfrage dieses Reports 1 heraus, dass viele Sicherheitsthemen durch die Teilnehmenden so allgemein gehalten werden, dass sie schwer auf nur ein Profil begrenzt werden können. Daher werden in diesem Report 1 die definierten Tätigkeitsfelder neu strukturiert und als Profilgruppen wie folgt zusammengefasst:

- Allgemeine Grundkompetenzen
- Produktion, Entwicklung und Vertrieb
- Informationsverarbeitung und IT-Infrastruktur
- Instandhaltung und Vermittlung
- Organisations- und Assistenztätigkeiten
- Verwaltung und Personal
- Strategie und Führung

Fokus in der Profilgruppe Allgemeine Grundkompetenzen sollten die Basis-Anforderung nach der IT-Grundschutz-Methodik des BSI [8] und allgemeine Grundkenntnisse der Informationssicherheit sein. Es ist eine Sensibilisierungsmaßnahme zu konzipieren, die grundlegend für alle Tätigkeitsfelder wichtig ist und zu deren Lernszenarien auch die Sensibilisierung für E-Mails (Phishing), Passwort-Konstruktion und CEO-Fraud (Betrug unter Verwendung von falscher Identität, um Geldüberweisungen durchsetzen zu können; i. d. R. geben sich die Kriminellen als Führungskraft aus) gehören sollte.

Ergänzend zu diesen Grundkenntnissen sollten in der Profilgruppe Produktion, Entwicklung und Vertrieb spezifische Informationssicherheitsaspekte für entwicklungs- und prozessintensive Aufgaben behandelt werden. Hinsichtlich der Lernszenarien sind m. E. gezielt die Themen Verschlüsselung, Wirtschaftsspionage und Reiseaktivitäten (Travel-Security) angebracht.

Die Profilgruppe Informationsverarbeitung und IT-Infrastruktur ist entscheidend für die Einrichtung und Wartung der technischen Infrastruktur. Daher gilt sie im Report 1 als eine von vier „Gatekeepers“ (Torwächter) und kontrolliert die digitalen und technischen Zugänge. Sie entwickelt die technischen Richtlinien und steuert entsprechende Sicherheitstrainings, weswegen diese Gruppe auch den Schulungsbedarf am höchsten einschätzt. Neben einem besonderen Augenmerk auf die Vermittlung der neuesten für das KMU relevanten Richtlinien sollte diese Gruppe auch technische Schulungen z. B. zu den Themen Ransomware (Erpressungssoftware) und Datenverfügbarkeit erhalten. Diejenigen in der Gruppe, die die Sicherheitstrainings steuern, sollten m. E. zudem in effizienten Sensibilisierungsmethoden geschult und als Moderatorinnen und Moderatoren der analogen Lernszenarien ausgebildet werden.

Mitarbeitende der Profilgruppe Instandhaltung und Vermittlung sind für die haustechnische Infrastruktur zuständig. Zudem nehmen sie Organisationsaufgaben bei der Steuerung von Kontakten, Personenflüssen und analogen Kommunikationskanälen wahr. Sie gelten im Report 1 somit als physischer „Gatekeeper“. Hierarchisch ist diese Profilgruppe zwar auf einer eher unteren Ebene angesiedelt, muss aber als kritisch bei der Durchführung von Sicherheitsmaßnahmen gelten, so dass hier auch zu Themen wie Desinformation und Social Engineering sensibilisiert werden sollte. Konkret zählen im Report 1 hierzu Tätigkeiten in der Hausverwaltung, dem Facility Management, im Empfang, in der Pförtnerei oder Poststelle.

Die Profilgruppe Organisations- und Assistenztätigkeiten bildet im Report 1 den kommunikativen KMU-„Gatekeeper“, der alle Kommunikationsflüsse beispielsweise zur Unternehmensleitung oder zu einer Abteilung kontrolliert und Verwaltungsaufgaben ausübt sowie Zugriffe auf finanzielle Bereiche wie Online-Buchungen, Online-Bestellungen und Kreditkarten hat. Die Mitarbeitenden dieser Profilgruppe sollten neben spezifischen Sicherheitsaspekten entsprechend ihrer konkreten Aufgabenstellung m. E. ebenfalls für die Themen Desinformation, Social Engineering und CEO-Fraud sensibilisiert werden.

Mitarbeitende der Profilgruppe Verwaltung und Personal sind i. d. R. mit sehr sensiblen Daten in der Finanz- und Personalverwaltung befasst. Dabei sind die Zugriffsmöglichkeiten zwar eng beschnitten, aber tiefer als beispielsweise bei der Profilgruppe Organisation und Assistenz. Diese Gruppe wird im Report 1 als personeller und finanzieller „Gatekeeper“ bezeichnet, da sie die Finanzströme und Personalzugänge kontrolliert. Generalfirmenschlüssel, Zutritt zum Tresor, Zugriff auch auf sensibelste Personendaten, dienstliche Smartphones und auch Verantwortlichkeiten zur Dokumentenvernichtung und Datenlöschung sind hier am ausgeprägtesten. Zudem existieren viele Kontakte nach außen und innen. In dieser Profilgruppe sind vor allem die Tätigkeiten im Personalwesen und der Buchhaltung zusammengefasst. Je nach konkreter Unternehmenssituation sind m. E. speziell rechtliche Themen wie Datenschutz in die Sensibilisierung für Informationssicherheit einzubeziehen.

In der Profilgruppe Strategie und Führung werden Entscheidungen getroffen und Richtlinien veröffentlicht. Zu allen Unternehmensbereichen, einschließlich sensibler Daten, Tresore und sicherheitsrelevanter Mechanismen, besitzt diese Gruppe teilweise oder ganz Zutritt, Zugang und Zugriff. Außerdem ist sie sehr mobil und durch ihren ständigen Kontakt mit allen Stakeholdern (Anspruchsberechtigten) extrem exponiert. Neben dem (Top-)Management können Tätigkeitsfelder wie Marketing/Kommunikation und Öffentlichkeitsarbeit integriert werden. Diese Profilgruppe sollte über alle Sicherheitsbereiche auf dem neuesten Stand gehalten und selbst abgesichert werden. Das Top-Management muss zur strategischen Ausrichtung eines ISMS, zur spezifischen Gefährdungslage und zum Risikomanagement sensibilisiert werden. Auf den nächsten Seiten werden die prägnantesten Ergebnisse des Reports zusammenfassend dargestellt.

Ausblick

Die Ergebnisse unserer ersten Studie [5] und dieses Reports 1 bilden im Projekt „Awareness Labor KMU (ALARM) Informationssicherheit“ die Ausgangsbasis für die Entwicklung von neuen, an die KMU angepassten und die Menschen aktivierenden Sensibilisierungsmaßnahmen. Ihr Ziel und damit der Mehrwert für KMU ist die Bereitstellung integrativ verzahnter Maßnahmen für eine systematische Sensibilisierung, die eine Sicherheitskultur tatsächlich zu entwickeln hilft und sich von klassischen Schulungen unterscheidet. Die Befragungen und die zusammenfassende Darstellung der Ist-Situation sollen zu Empfehlungen für modulare Sensibilisierungsmaßnahmen und niederschwellige Sicherheitskonzepte für die deutschen KMU führen.

Mit aktivierende Lernszenarien sind insbesondere interaktive, kurzweilige, teambasierende, diskursive und emotionalisierende Lernerfahrungen gemeint. Informationssicherheit muss erlebt werden. Darüber muss gesprochen werden! Des Weiteren sind neuartige betriebliche *Awareness-Messungen* geplant, die zu Reifegradaussagen, niederschwelligen Sicherheitskonzepten und konkreten Handlungsempfehlungen für KMU führen sollen. Awareness-Messungen sind dabei kein einfaches Unterfangen, da die Maßnahmen keinen wirklichen Einblick in ihren Erfolg bei der Verhaltensänderung geben und bislang weder Fortschritt noch Wert gemessen werden [2]. Zudem sind unrealistische Erwartungen an Menschen und ihre Motivationen zu vermeiden. Bada u. a. betonen, dass Verhaltensänderungen im Kontext der Cybersicherheit möglicherweise durch Risikominderung gemessen werden könnten, aber nicht durch das, was die Menschen wissen, ignorieren oder nicht wissen [2]. Wir werden mit weiteren wissenschaftlichen Veröffentlichungen auf dieses Problem zurückkommen.

Für die zukünftige Weiterentwicklung der Ergebnisse [der Studie 1 und des Reports 1] im Projekt *„Awareness Labor KMU (ALARM) Informationssicherheit“* bleibt es wichtig, einen Fokus auf die notwendigen sicherheitsrelevanten Verhaltensänderungen von Menschen zu legen. Eine Verhaltensänderung zu bewirken, erfordert dabei mehr als nur die Bereitstellung von Informationen über Risiken und reaktive Verhaltensweisen – zum einen müssen die Menschen die Ratschläge verstehen und anwenden können, zum anderen müssen sie dazu motiviert und gewillt sein und gerade Letzteres erfordert eine Änderung der eigenen Einstellungen und Absichten [2]. Die Untersuchung internationaler Literatur von Bada u. a. mit der Fragestellung, warum Sicherheitsbewusstseinskampagnen oft scheitern, kommt u. a. zu dem Ergebnis, dass Wissen und Bewusstsein zwar Voraussetzung für eine Verhaltensänderung, aber nicht unbedingt ausreichend sind [2]. Für Bada u. a. ist das Verständnis der Risikowahrnehmung von Menschen entscheidend für die Erstellung effektiver Sensibilisierungskampagnen [2].

Auch nach der Literaturrecherche von Ertan u. a. besteht zukünftig Forschungsbedarf an einem besseren Verständnis, wie Verhaltensänderungen im Kontext der alltäglichen Cybersicherheit gefördert werden können [10]. Insbesondere sollte zu Verhaltensunterschieden zwischen Mitarbeitendentypen oder innerhalb verschiedener Unternehmensumgebungen geforscht werden, da diese auch unterschiedliche Verhaltensweisen in Bezug auf Cybersicherheitsprobleme aufweisen können [10]. Unser Report 1 bietet hierzu eine interessante Datenbasis zur deutschen Ist-Situation. Ertan u. a. identifizieren vier Verhaltensmuster, die maßgeblich beeinflussen, wie Menschen Cybersicherheit praktizieren: Einhaltung der Sicherheitsrichtlinien, Koordination und Kommunikation zwischen den Gruppen, Phishing-/E-Mail-Verhalten und Passwortverhalten [10]. Darüber hinaus ist die *Sicherheitskultur* als übergreifendes Thema bedeutend, das die vier Verhaltensweisen überlappt und umrahmt [10]. Diese internationalen Ergebnisse decken sich mit unseren Erkenntnissen aus der Studie [5] und aus diesem Report 1. Darüber hinaus bildet die Datenbasis des Reports 1 mit seinen sieben Profilgruppen eine interessante Möglichkeit, solche internationalen Forschungsfragen auch für deutsche KMU zu eruieren.

Prof. Dr. rer. nat. Margit C. Scholl

Dezember 2021

Abb. 1: *Für Teilnehmende wichtige Begriffe der Informationssicherheit*

Grafische Zusammenfassung

Die Wortwolke (siehe Abbildung 1) stellt die Relevanz der Begriffe dar, die die Teilnehmenden mit Informationssicherheit verbinden. Dem Datenschutz wird mit 34 Prozent die größte Bedeutung zugeschrieben. Es folgen Datensicherheit (21%), Awareness (11%), Passwort (10%) und Vertraulichkeit (9%). Dies zeigt aber auch auf, dass Informationssicherheit nicht ganzheitlich, also nicht vollständig und nur in Einzelteilen betrachtet und wahrgenommen wird. Es ist daher wichtig, den Unternehmen das breite und umfassende Feld der Informationssicherheit zu demonstrieren und Mitarbeitende ebenso wie Führungskräfte dafür zu sensibilisieren und dabei die Komplexität von Security-Maßnahmen zu minimieren [11:9].

In den folgenden drei ausgewählten Betrachtungen wurden alle Antworten, die selten, häufiger und immer angaben, zusammengezählt und als Nutzung gewertet. Dem wurden die Antworten gegenübergestellt, die bei Nutzung nie angaben. Nummer eins der Kommunikationsmittel in den befragten Unternehmen ist die E-Mail, gefolgt von externen und internen Telefonaten. Dies bedeutet, dass alle Unternehmen per E-Mail angreifbar sind, und nur zwei bis drei Prozent nicht Gefahr laufen, Opfer eines Telefonbetrugs zu werden (siehe Abbildung 2).

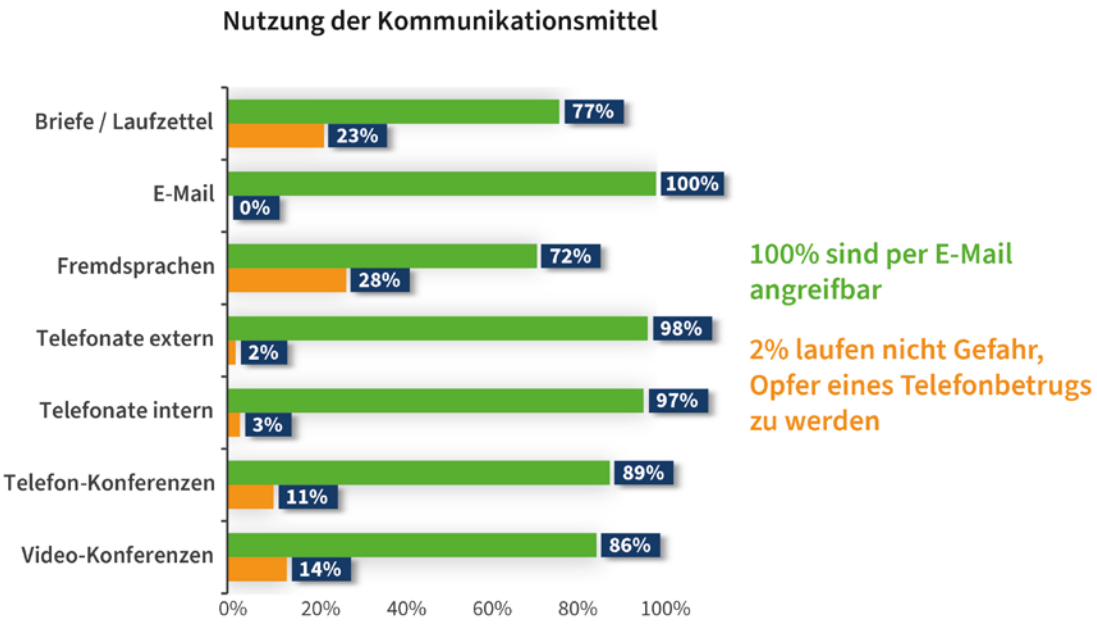


Abb. 2: *Nutzung der Kommunikationsmittel*

Trotz der Pandemie-Situation bleibt der feste Arbeitsplatz in Unternehmen die Priorität. Da 82 Prozent der Befragten im Homeoffice arbeiten, ist anzunehmen, dass diese Gruppe einem erhöhten Sicherheitsrisiko ausgesetzt ist (siehe Abbildung 3). Denn im Homeoffice entziehen sich viele Sicherheitsaspekte der Kontrolle des Unternehmens, einheitliche Standards sind schwerer durchsetzbar und beruflicher und privater Raum gehen meist schwer trennbar ineinander über.

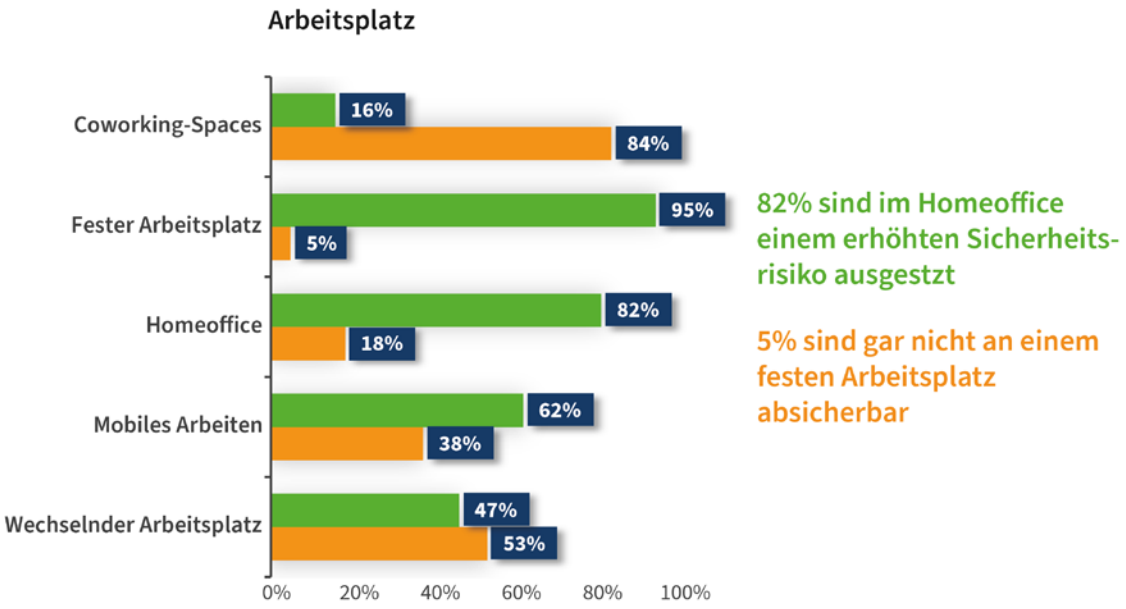


Abb. 3: *Art des Arbeitsplatzes*

Mehr als die Hälfte der befragten Personen (53%) nutzten nie die Datensicherheitsmaßnahme E-Mail-Verschlüsselung (siehe Abbildung 4). Etwas im Widerspruch steht dagegen die Aussage, dass Verschlüsselungsmöglichkeiten den Befragten zu 48 Prozent bewusst sind. Da Verschlüsselung unterschiedliche Bereiche betrifft, können hier keine Aussagen über den nicht erfolgten Einsatz der Verschlüsselung z. B. von E-Mails getroffen werden. Sinnvoll wäre hier, eine Sensibilisierungsmaßnahme zur Verschlüsselung in Unternehmen anzugehen, aber vorher den Bedarf der Verschlüsselung in den einzelnen Bereichen zu konkretisieren.

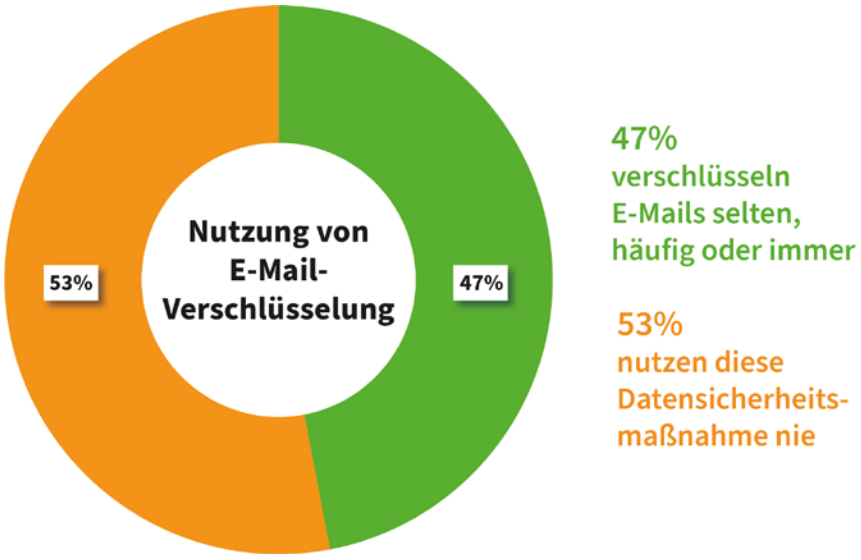


Abb. 4: *Nutzung von E-Mail-Verschlüsselung*

99% der Befragten sehen einen Schulungsbedarf in Informationssicherheit für sich oder für das eigene Unternehmen (siehe Abbildung 5). Dies bedeutet, dass Mitarbeitende offen gegenüber dem Thema Informationssicherheit (IS) und den Sensibilisierungsmaßnahmen sind.

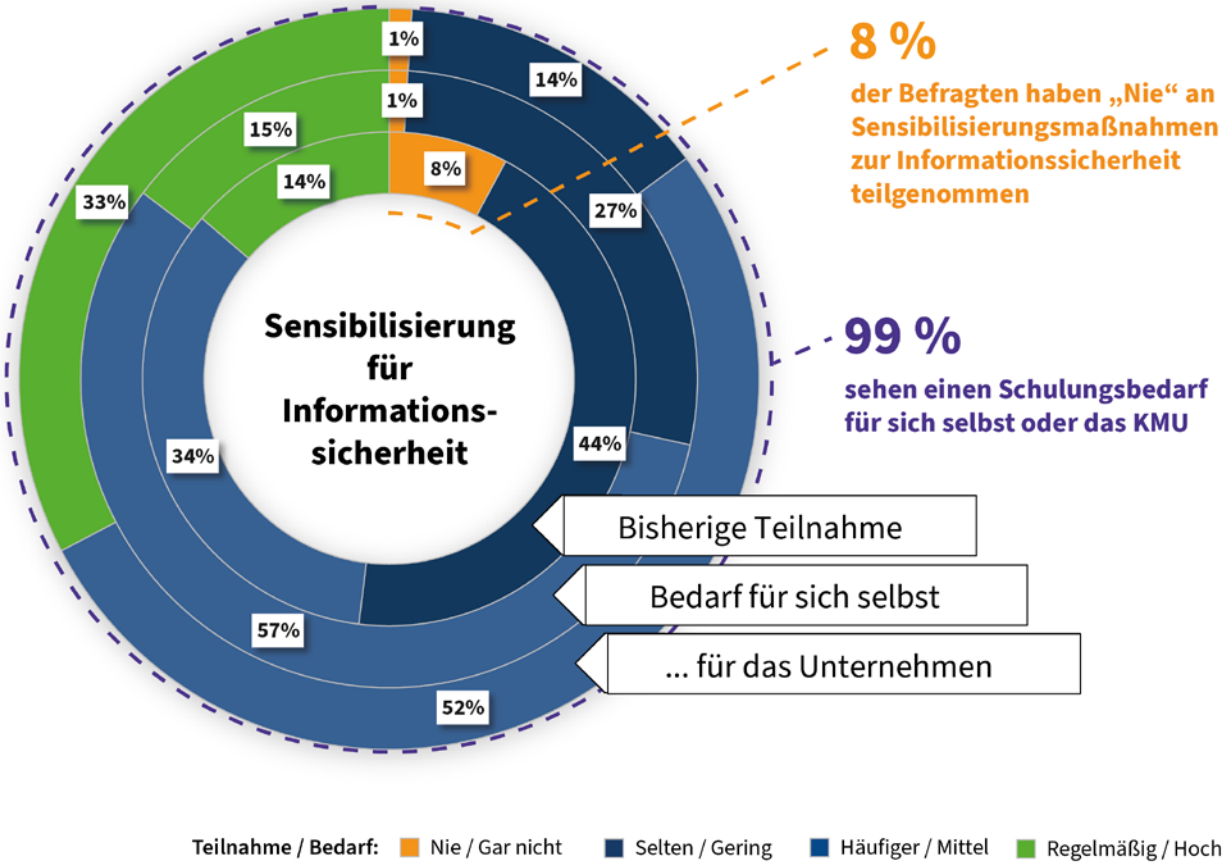


Abb. 5: *Sensibilisierung für Informationssicherheit*

Auf Basis der Umfrage wurden sieben Tätigkeitsprofile definiert (siehe Abbildung 6), die es ermöglichen, die Kompetenzprofile abzuleiten. Das erste und allgemeine Tätigkeitsprofil setzt allgegenwärtige Informationssicherheitskompetenzen voraus, um überhaupt einer Tätigkeit nachgehen zu können. Dazu gehören z. B. Aspekte wie Einhaltung der Schweigepflicht über unternehmensinterne wichtige Daten oder Umgang mit arbeitstechnischen Geräten. Die anderen sechs Profile greifen in- und übereinander und sind in ihren Kompetenzprofilen spezifisch ausgerichtet. Die einzelnen Kompetenzprofile ermöglichen eine konkrete Konzepterarbeitung für die Sensibilisierungsmaßnahmen, die spezifisch auf die Tätigkeiten ausgerichtet werden und somit zur Erhöhung der Sicherheitskultur im Unternehmen führen können.

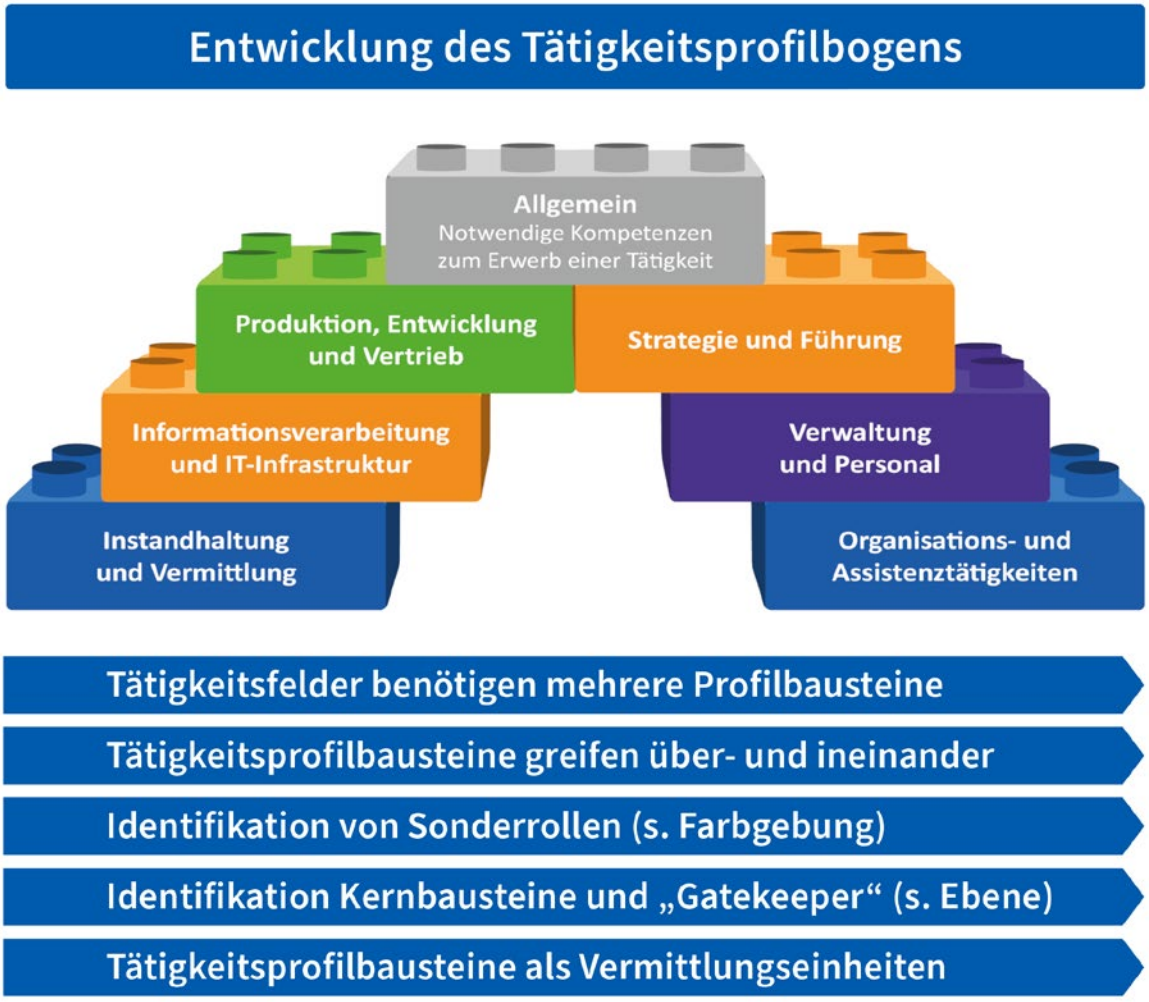


Abb. 6: *Tätigkeitsprofile der Befragten unter Einbeziehung des IT-Grundschutzes*

2 Einleitung

Das vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) geförderte interdisziplinäre Forschungsprojekt „Awareness Labor KMU (ALARM) Informationssicherheit“ baut innerhalb von drei Jahren ein Gesamtszenario zur Sensibilisierung und Unterstützung von kleinen und mittleren Unternehmen (KMU) für Informationssicherheit bis hin zu deren Selbsthilfe auf. Das Gesamtszenario soll zu der dringend notwendigen Sensibilisierung von Führungskräften und Mitarbeitenden sowie zu einer gezielten Personalentwicklung in KMU führen. Die Informationssicherheit (IS) soll konkret (be-)greifbar gemacht werden, indem die Menschen emotional berührt und sensibilisiert werden. Dies erfolgt durch analoge (siehe Abbildung 7) und digitale erlebnisorientierte Lernszenarien sowie „Vor-Ort-Angriffe“ und weitere Überprüfungen wie Awareness-Messungen und Tests. Damit verbunden ist der Aufbau eines mobilen Awareness-Vorort-Übungslaboratoriums mit flexiblen, interaktiven, erlebnisorientierten Lernszenarien zu aktuellen Sicherheitsthemen, die für KMU relevant sind. Diese Lernszenarien werden mit Übungsanleitungen, Handlungsempfehlungen und Schrittfolgen für die Praxis von KMU kombiniert.

Im Projekt werden diese Lernszenarien iterativ in drei Phasen, agil und partizipatorisch mit allen Beteiligten als Gesamtszenario entwickelt. Als Grundlage dienen dazu im Projekt „Awareness Labor KMU (ALARM) Informationssicherheit“ sowohl die Interviews und Umfragen mit Pilotunternehmen und Austausche zwischen allen Projektpartnerinnen und -partnern als auch der IT-Grundschutz des BSI. Ziel ist es, eine nachhaltige und verbesserte Sicherheitskultur in KMU herzustellen. Das Projekt wird von Unterauftragnehmern mit entsprechender Expertise unterstützt und zeichnet sich darüber hinaus durch die Interdisziplinarität des Forschungsteams der Technische Hochschule Wildau (TH Wildau) aus. Insgesamt sollen im Projektverlauf drei Studien und drei Reporte erstellt werden, um den Ist-Zustand und den Bedarf der Sensibilisierungsthemen zu ermitteln, die Konzeption der Lernszenarien zu überprüfen und die entwickelten Produkte zu evaluieren.

Die erste tiefenpsychologische Grundlagenstudie zur Informationssicherheit im Projekt wurde von dem Unterauftragnehmer known_sense im Auftrag der TH Wildau vorgelegt [5]. Sie offenbart, dass der Begriff Informationssicherheit für viele noch diffus ist und nicht selten Expertinnen, Experten und Dienstleistern zugeordnet wird. Damit wird auch deutlich, dass in KMU für alle Mitarbeitenden und Führungskräfte eine Bewusstseinsbildung (Englisch: awareness raising) für Informationssicherheit notwendig ist.

Der hier vorliegende erste Report der Forschungsgruppe Information Security & Awareness um Professorin Dr. Margit Scholl basiert auf einer Online-Umfrage, die Tätigkeitsprofile und deren Relevanz zur Informationssicherheit in Unternehmen definiert, um unter Einbeziehung des IT-Grundschutzes des BSI aus sieben akkumulierten Tätigkeitsprofilen Sicherheitsprofile abzuleiten, die wiederum die Grundlage für Kompetenzprofile bilden sollen. Die Kompetenzprofile sollen die wichtigsten Fähigkeiten und Fertigkeiten der Mitarbeitenden in deren Tätigkeiten umfassen, so dass Schulungs- und Sensibilisierungsmaßnahmen in Form von Lernszenarien, die auch als „Serious Games“ bezeichnet werden, darauf zugeschnitten werden können. Der

Sensibilisierung mit „Serious Games“ folgen als Test Vor-Ort-Angriffe. Diese bedienen sich sowohl physischer als auch digitaler Angriffsvektoren. Dieses geschieht nach Abstimmung mit eingeweihten Verantwortlichen aus den Unternehmen, aber meist unter Unwissenheit der Probandinnen und Probanden.

Die voranschreitende Digitalisierung birgt zahlreiche Chancen, gleichzeitig gehen damit aber neue Herausforderungen für die Cybersicherheit einher. Dies betrifft vor allem KMU, die nicht die notwendigen Ressourcen für IS aufbringen können. So sind 75% aller Unternehmen in Deutschland laut einer Umfrage des Bitkom e. V. in den vergangenen zwei Jahren Opfer von digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl geworden [12]. Privatpersonen und Haushalte sind genauso von Cyberangriffen und Social Engineering betroffen wie die Unternehmen. Es ist also davon auszugehen, dass Informationssicherheit jede und jeden betrifft. Die Angreifenden bedienen sich einer Vielfalt von Methoden und setzen vor allem am Menschen an. Daher sind Bewusstseinsbildung für mehr IS und die Umsetzung von technischen und organisatorischen Maßnahmen wichtige Elemente institutioneller Präventions- und Lernprozesse: die Menschen müssen zur „Human Firewall“ ausgebildet werden. Wie wichtig dies ist, zeigt auch die aktuelle Situation während der COVID-19-Pandemie, durch die die Nutzung des Homeoffices rasant angestiegen ist und dabei oft Sicherheitsmaßnahmen vernachlässigt worden sind. Die meisten Unternehmen waren nicht auf den Umstieg ins Homeoffice vorbereitet und mussten ad hoc reagieren und Lösungen finden, um den Betrieb möglichst aufrechtzuerhalten. Nach Angaben von Forrester Research kostet der durchschnittliche Datenverstoß bis zu 7 Millionen Dollar pro Vorfall – von der Reaktion und Benachrichtigung, über Produktivitätsverluste, potenzielle Klagen, Bußgelder, bis hin zu Geldstrafen und anderen Verbindlichkeiten. Im Allgemeinen nehmen auch die Verstöße gegen die Datenschutzrichtlinien zu [13]. Um das Risiko einer nicht korrekten menschlichen Reaktion auf z. B. externe Angriffe zu minimieren, müssen KMU verstärkt in Präventionsmaßnahmen wie Sensibilisierung und Schulung investieren. Das Projekt ALARM Informationssicherheit stellt dazu bundesweit kostenfrei die entwickelten Lernszenarien inkl. Moderationsanleitungen, Anleitungen für die „Vor-Ort-Angriffe“ und darauf aufbauende Sicherheitskonzepte und weitere sicherheitsrelevante Handlungsempfehlungen sukzessive bis zum Projektende als Download zur Verfügung.

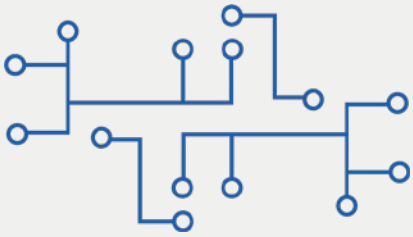


Abb. 7: *Awareness-Training anhand im Projekt ALARM Informationssicherheit entwickelter analoger Lernszenarien (Quelle: Forschungsgruppe Scholl)*

3 Methodik

3.1 Konzeption der Umfrage

Ziel dieser Umfrage war es, eine Orientierungshilfe bei der Erstellung von allgemeingültigen und branchenübergreifenden Tätigkeitsprofilen zu schaffen, aus denen wiederum Sicherheits- und Kompetenzprofile abgeleitet werden können. Die Umfrage sollte darüber hinaus zusammen mit den tiefenpsychologischen Interviews [5] relevante Informationssicherheitsthemen für die analogen und digitalen erlebnisorientierten Lernszenarien liefern.

Die Umfrage selbst wurde als Online-Umfrage konzipiert und mit „QUAMP Survey Sociolutions“ erstellt. Sie sollte eine Dauer von 15 Minuten Bearbeitungszeit durch die Teilnehmenden nicht überschreiten. Eingeleitet wurde die Umfrage durch einen Begrüßungstext, in dem das Projekt und die Unterauftragnehmer vorgestellt und auf die gemäß Datenschutz-Grundverordnung (DSGVO) erstellte Datenschutzerklärung verwiesen wurde. Bei der ersten Frage sollten sich die Teilnehmenden einem von insgesamt 15 Tätigkeitsfeldern zuordnen, das am ehesten zu ihren Tätigkeiten passt. Diese sind nach klassischen Funktionen wie z. B. Einkauf, Produktion, Vertrieb und Personal in einem Unternehmen aufgeteilt und teilweise bereits zusammengefasst. In der zweiten Frage ging es darum, auf welcher Ebene (Auszubildende / Trainee / Praktikant / in, Mitarbeiter / in, Mittleres Management, Geschäftsleitung / Top-Management) das in der ersten Frage ausgewählte Tätigkeitsfeld ausgeübt wird.

Die Fragen 3 bis 15 mit den jeweiligen Antwortmöglichkeiten waren nach dem gleichen Schema aufgebaut und enthielten insgesamt 70 Unterfragen, die nach Bereichen wie z. B. Arbeitsplatz, Hardware, Software und Datenschutz unterteilt waren. Die Fragestruktur folgte überwiegend dem Aufbau: *„Wie häufig haben Sie in bzw. für Ihren Job mit Folgendem zu tun?“*. Es wurde eine 4-Punkte-Likert-Skala zur Häufigkeit mit einem ordinalen Skalenniveau und den Antwortmöglichkeiten *„Immer“*, *„Häufiger“*, *„Selten“* und *„Nie“* gewählt. Hiermit sollte eine klare Entscheidung der Teilnehmenden „erzwungen“ werden, da bei ungerader Skala die Tendenz zur Wahl der Mitte besteht [14].

Für die Beantwortung der Online-Umfrage wurde den Teilnehmenden eine Zeitspanne von zwei Wochen eingeräumt. Nach Ilieva et al. beträgt die Antwortzeit bei E-Mail-Umfragen etwa 5,6 Tage [15], weshalb nach einer Woche eine Erinnerung erfolgte. Von den etwa 364 Mitarbeitenden der Pilotunternehmen nahmen 85 Personen an der Online-Umfrage teil. Dies entspricht etwas weniger als einem Viertel. Die Einladungen zur Umfrage wurden an die jeweiligen Kontaktpersonen in den Pilotunternehmen per E-Mail versendet, in der um die Weiterleitung an die weiteren Mitarbeitenden gebeten wurde.

3.2 Untersuchungsgruppe

Mit Beginn des Forschungsprojekts wurden vier Pilotunternehmen gesucht, die zum einen der Definition von KMU entsprechen [16] und zum anderen bereit waren, für die Gesamtdauer von drei Jahren an den geplanten Vorhaben (z. B. Umfragen und Interviews) teilzunehmen und die entwickelten erlebnisorientierten Lernszenarien zu testen. Die Pilotunternehmen wurden vom assoziierten Partner der Industrie- und Handelskammer (IHK) Ostbrandenburg sowie dem Unterauftragnehmer Thinking Objects akquiriert. Ihre Unternehmenssitze befinden sich in Brandenburg und Baden-Württemberg. Sie sind in den Branchen Personalberatung, Industrieanlagenbau, Hard- und Softwareentwicklung sowie Elektrogroßhandel tätig. Die Unternehmensgröße reicht von 30 bis 250 Mitarbeitende. Insgesamt nehmen an dem Projekt ca. 364 Mitarbeitende der vier Pilotunternehmen teil.

Bei dieser Auswahl der Unternehmen lag der Fokus in erster Linie weniger auf der Repräsentativität, die bei der Größe der Zielgruppe quantitativ kaum erreicht werden kann, sondern auf der Erstellung einer realistischen Zustandsanalyse von geeigneten Vertretern, deren Genauigkeit stark von der Bereitschaft und Offenheit dieser abhängt. In der Konsequenz verbleibt die Stichprobenlage disproportional zur Grundgesamtheit der KMU in Deutschland (vgl. einen Überblick aus dem Jahr 2017 [17:14–18] und 2012 [18:11–12]) nach Betriebsgröße, Branche und Region geschichtet und wird auch nachträglich nicht durch eine Gewichtung ausgeglichen. Es wurden drei Teilstichproben gezogen. Die größte mit n=85 kommt aus den Pilotunternehmen (Umfrage 101). Über den Projektträger, das Deutsche Zentrum für Luft- und Raumfahrt (DLR), (Umfrage 102, N=17) und die assoziierten Partner IHK Cottbus, Potsdam und Ostbrandenburg (Umfrage 103, N=6) wurden zwei weitere Teilstichproben hinzugenommen und unter dem Begriff weitere Unternehmen zusammengefasst. Die Auswahl dieser weiteren Unternehmen erfolgte durch die genannten Projektpartner. Wie deren Zusammensetzung in Bezug auf Branche und Region und deren Mitarbeitenden innerhalb dieser Teilstichprobe ausfiel, war bei der Auswertung nicht bekannt. Das zugrundeliegende Untersuchungsdesign folgte üblichen methodischen Grundlagen (siehe [19]) und findet sich zusammengefasst in Tabelle 1.

Tabelle 1: *Untersuchungsdesign*

Untersuchungsdesign	
Definition KMU	EU-Empfehlung 2003 / 361 KMU: unter 250 Mitarbeitende, bis zu 50 Mio. Umsatz / Jahr
Grundgesamtheit	Kleine und mittlere Unternehmen in Deutschland entsprechend der Definition
Stichprobe	Vier Pilotunternehmen Region: Brandenburg und Baden-Württemberg Branchen: Personalberatung, Industrieanlagen, Hardware und Software, Elektrogroßhandel Mitarbeitende: je 30–250 / Gesamt ca. 364 Stichprobenziehung: über assoziierten Partner IHK-Ostbrandenburg und den Unterauftragnehmer Thinking Objects Weitere Unternehmen: über die assoziierten Partner IHK Cottbus, Potsdam und Ostbrandenburg und den Projektträger DLR
Stichprobenanlage	disproportional geschichtet nach Betriebsgröße, Branche und Region
Gewichtung	keine Gewichtung
Befragungsmethode	Online-Fragebogen durch QUAMP Survey Sociolutions
Ziel	Zustandsanalyse als Orientierungshilfe bei der Formierung zusammenfassender Profile aus mehreren Tätigkeitsfeldern

Dabei basiert die folgende Auswertung auf einer Gesamtgruppe von 108 Personen. Beteiligte Gruppen stellen sich wie folgt zusammen:

Tabelle 2: *Teilstichproben*

Umfragegruppe	Kurzbezeichnung	Anzahl TN
Pilotunternehmen	(Umfrage 101 — „Pilotunternehmen“)	85
Partner des Deutschen Zentrums für Luft- und Raumfahrt (DLR)	(Umfrage 102 — „PT-Partner“)	17
Partner der Industrie- und Handelskammern (IHK)	(Umfrage 103 — „IHK-Partner“)	6

Es kann daher von einer Grundgesamtheit von 108 Teilnehmenden (TN) ausgegangen werden. Da nicht alle Teilnehmenden alle Fragen beantwortet haben, schwankt die Gesamtstichprobengröße (N) zwischen 102 und 108. Für die weitere Analyse im Rahmen der ursprünglichen Anlage der Umfrage gilt die Form einer Zustandsanalyse mit dem Ziel, zusammenfassende Profile aus mehreren Tätigkeitsfeldern zu erfassen. Der Fokus liegt im Erkenntnisgewinn aus einer Versuchsumgebung, um Stützstellungen für den Zuschnitt von Maßnahmen zur Personalentwicklung zu erhalten. Es wurde daher bereits zuvor auf eine Gewichtung und den Ansatz einer repräsentativen Umfrage verzichtet. Eine Gewichtung hätte nur weitere Schritte erschwert und ist im stückweisen fokussierten Blick auf die einzelnen Tätigkeitsfelder zudem vernachlässigbar. Getroffene Aussagen dürfen nicht als repräsentativ, sondern nur unter Berücksichtigung dieser Limitierung bewertet werden. Durch den verhältnismäßig kleinen Umfang der Stichprobe und einen vermutlich verzerrenden Selektionsprozess bei der Auswahl der Teilnehmenden innerhalb der Unternehmen ist von der möglichen Unterrepräsentation einzelner Tätigkeitsfelder auszugehen. Drei Tätigkeitsfelder erhielten keinen Rücklauf. Es bleibt daher offen, inwieweit manche Tätigkeitsfelder bei vielen KMU nicht vorhanden (z. B. PR/Öffentlichkeitsarbeit) oder durch Subunternehmen (z. B. Facility Management) bzw. Einzelauftragsnehmende (z. B. Rechtsvertretung) abgedeckt werden. Es besteht auf der anderen Seite auch der Verdacht, dass beispielsweise Tätigkeitsfelder wie Facility Management (keine Rückmeldung) oder Sekretariat/Empfang/Pförtnerei/Poststelle (nur eine Rückmeldung) in ihrer Relevanz bezüglich der Informationssicherheit unterschätzt und nicht angeschrieben worden sein könnten. Als in einer Diskussionsrunde mündlich nachgefragt wurde, stellte sich heraus, dass in KMU vermutlich viele Posten universell gehandhabt würden und daher mehrere Tätigkeitsfelder abdeckten. Bei der Zuordnung beispielsweise in einer Umfrage zum Thema „Informationssicherheit“ habe sich daher jemand, der sich sowohl um Themen wie „Informatik“ als auch teilweise um „Legal/Rechtsabteilung“ kümmern würde, vermutlich eher der „IT/Administration“ zugeordnet [20]. Es sollte daher bei der Konzeption einer Umfrage in diesem spezifischen Umfeld diskutiert werden, ob die

Abfrage von weiteren Tätigkeitsfeldern, in denen Aufgaben in erheblichem Umfang anfallen, sinnvoll wäre (z. B. „Übernehmen Sie zusätzlich zu Ihrer Haupttätigkeit in einem der folgenden Tätigkeitsfelder ebenfalls Aufgaben?“). Zudem wäre von Interesse, welche Tätigkeitsfelder ggf. bei KMU „outgesourct“ (ausgegliedert) werden. Eine Protokollierung des Auswahlprozesses durch Daten zur allgemeinen Personalstärke innerhalb der Tätigkeitsfelder in den Unternehmen und zur Zugehörigkeit der Angeschriebenen könnte mehr Aufschluss geben. Dieses erfordert aber einen Mehraufwand für die teilnehmenden Pilotunternehmen. Im Gegensatz zur vermuteten und bereits angesprochenen Unterrepräsentation einzelner Tätigkeitsfelder war die stärkste Prägung der Gesamtgruppe durch die Teilstichprobe „Pilotunternehmen“ im Tätigkeitsfeld Vertrieb / Außendienst zu beobachten. Diese bezifferte sich auf 47 Prozent der Teilnehmenden aus der Teilstichprobe „Pilotunternehmen“ (siehe Abbildung 9) bzw. 37 Prozent der formierten Gesamtgruppe (siehe Abbildung 8).

Die vorliegenden Daten wurden jedoch trotz aller benannten Einschränkungen für die Erstellung von Profilgruppen im Rahmen des zu erarbeitenden Zuschnitts auf Schulung und zielgruppengerechte Personalentwicklung als ausreichend befunden. Die ableitbaren Erkenntnisse sind bereits selbst als Orientierungshilfe zweckmäßig, da sie als erste Bestandsaufnahme für die zukünftige Forschung genügend Ansatzpunkte liefern.

4 Ergebnisse

4.1 Tätigkeitsfelder und Personengruppen

Die erste Frage bezieht sich auf die eindeutige Zuordnung der Teilnehmenden zu 15 verschiedenen Tätigkeitsfeldern, von denen nur zwölf Tätigkeitsfelder vorkamen und untersucht werden konnten. Den größten Anteil in der Gesamtstichprobe nimmt mit 37 Prozent die Gruppe Vertrieb / Außendienst ein, gefolgt von Forschung / Entwicklung (11%) und Einkauf / Beschaffung (10%) sowie IT / Administration und Personal mit jeweils acht Prozent (siehe Abbildung 8).

Wird nur die Teilstichprobe der vier Pilotunternehmen betrachtet (siehe Abbildung 9), wird deutlich, dass sich darin fast die Hälfte der Teilnehmenden dem Tätigkeitsfeld Vertrieb / Außendienst zuordneten. Etwa ein Viertel der Teilneh-

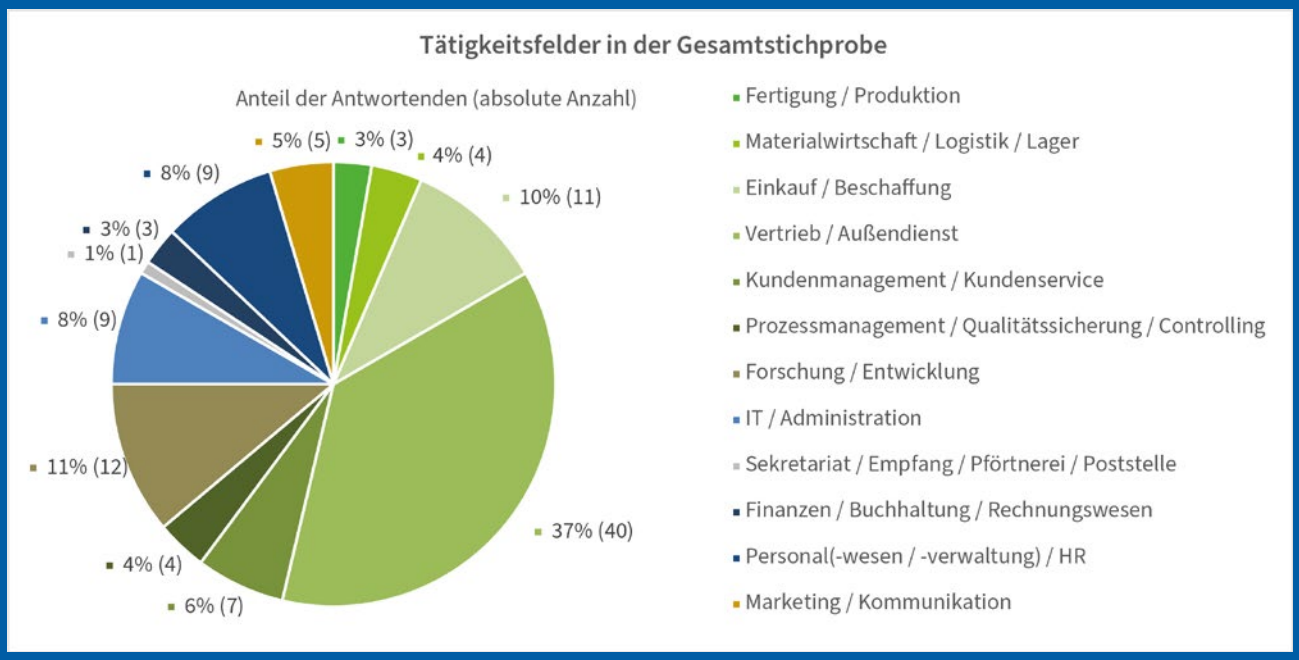


Abb. 8: *Tätigkeitsfelder in der Gesamtstichprobe*

menden verteilen sich dort auf die Tätigkeitsfelder Einkauf/Beschaffung (13%) und Personal (11%). Ebenso haben auch die Teilstichproben 102-PT und 103-IHK einen nicht unwesentlichen Einfluss auf die Verteilung der Tätigkeitsfelder in der Gesamtstrichprobe. Auffällig war dort eine geringe Anzahl von beantworteten Tätigkeitsfeldern. Mit zehn Antworten bestand eine große Häufung im Tätigkeitsfeld Forschung und Entwicklung und somit 59 Prozent innerhalb der „PT-Partner“ (siehe Abbildung 10) sowie mit drei Antworten zu Marketing/Kommunikation und somit 50 Prozent innerhalb der „IHK-Partner“ (s. ebendort). Des Weiteren schien die sehr begrenzte Auswahl an Teilnehmenden dieser Teilstichprobe thematisch zum Thema „Informationssicherheit“ ausgewählt worden zu sein. Die Auswertung lässt diese Vermutung zu, da sich Antworten in beiden Teilstichproben in den Feldern IT/Administration und Prozessmanagement/Qualitätssicherung/Controlling verstärkt wiederfinden. Ähnlich könnte bei den „PT-Partnern“ die Ballung im Kundenmanagement/Kundenservice erklärt werden.

Die „IHK-Partner“ bestanden zudem nur aus Teilnehmenden der Personengruppen Geschäftsleitung/Top-Management (67% dieser Teilstichprobe, siehe Abbildung 12) und Mittleres Management (33%). Infolgedessen können die dort vertretenen Tätigkeitsfelder (z. B. Marketing) durch die Unterrepräsentation von Mitarbeitenden verzerrt sein.

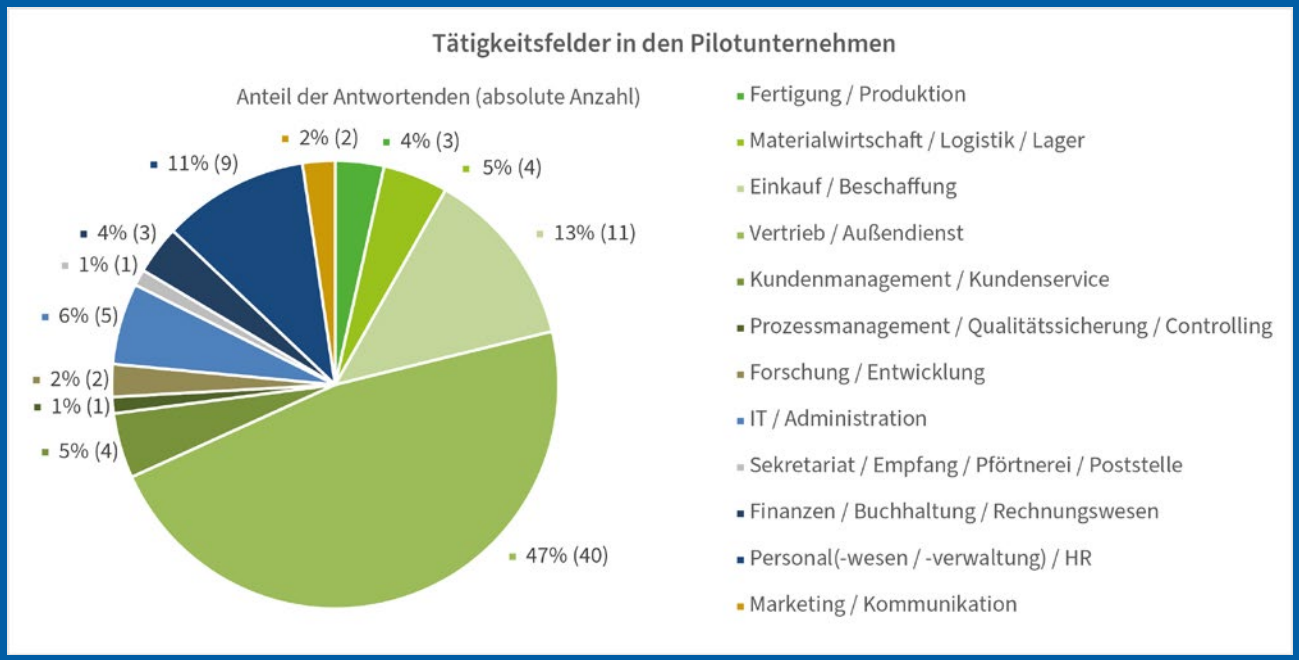


Abb. 9: *Tätigkeitsfelder in den Pilotunternehmen*

Die Personengruppe Mitarbeitende macht mit knapp 60 Prozent sowohl in der Gesamtstichprobe als auch in der Teilstichprobe „Pilotunternehmen“ den größten Anteil der Teilnehmenden aus (siehe Abbildung 11). Etwa ein Viertel ordnet sich der Personengruppe Mittleres Management zu. Die absolute Zahl der Gruppe Geschäftsleitung liegt bei vier in den Pilotunternehmen, was einer Teilnahmequote von fünf Prozent entspricht. Die höhere Quote in der Gesamtstichprobe ist der überdurchschnittlichen Teilnahme von Top-Führungskräften in der Teilstichprobe 103-IHK geschuldet (siehe Abbildung 12). Auszubildende, Trainees und Praktikantinnen und Praktikanten machten mit acht Prozent einen relativ kleinen Anteil aus.

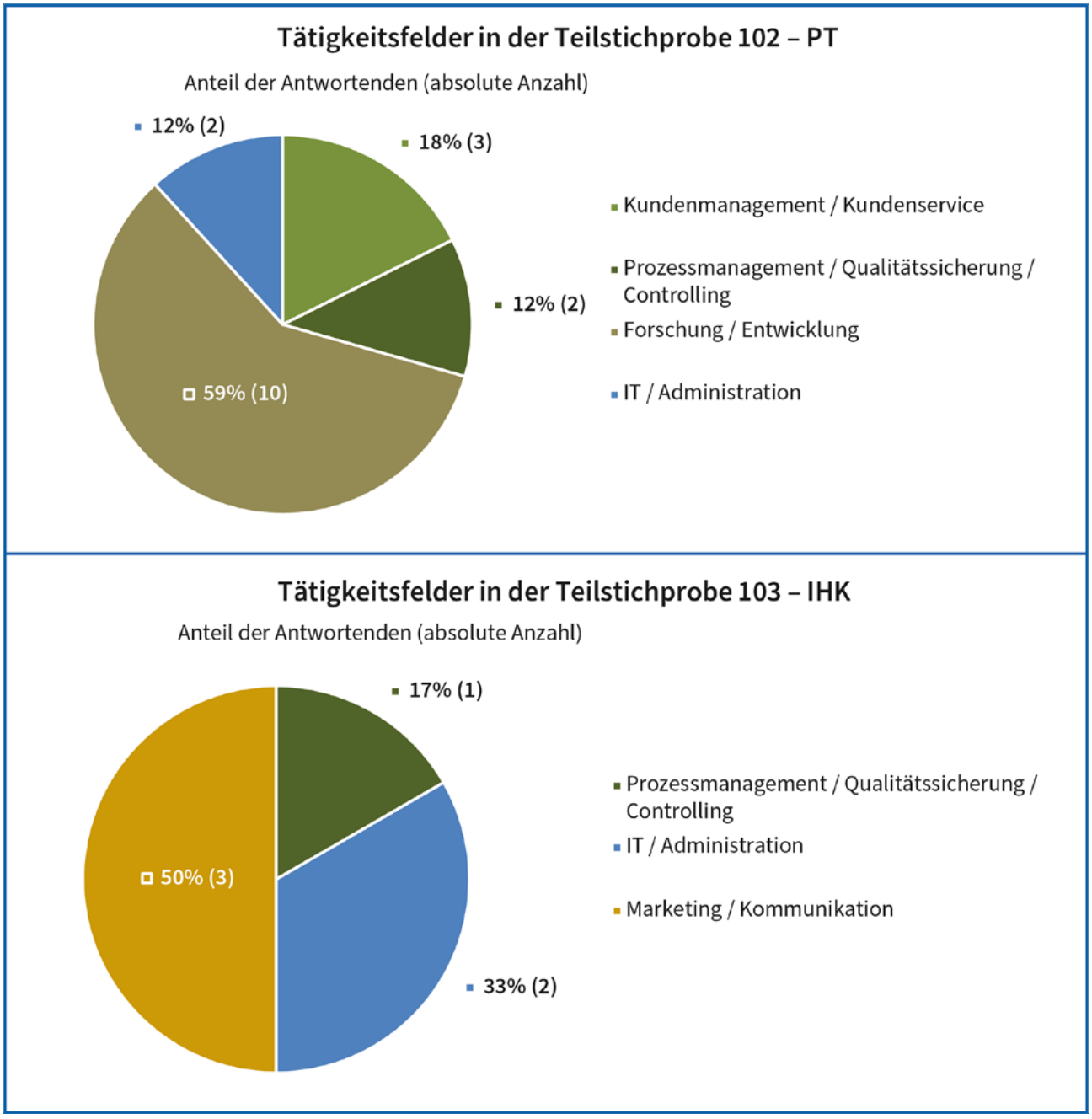


Abb. 10: *Tätigkeitsfelder in den weiteren Unternehmen*

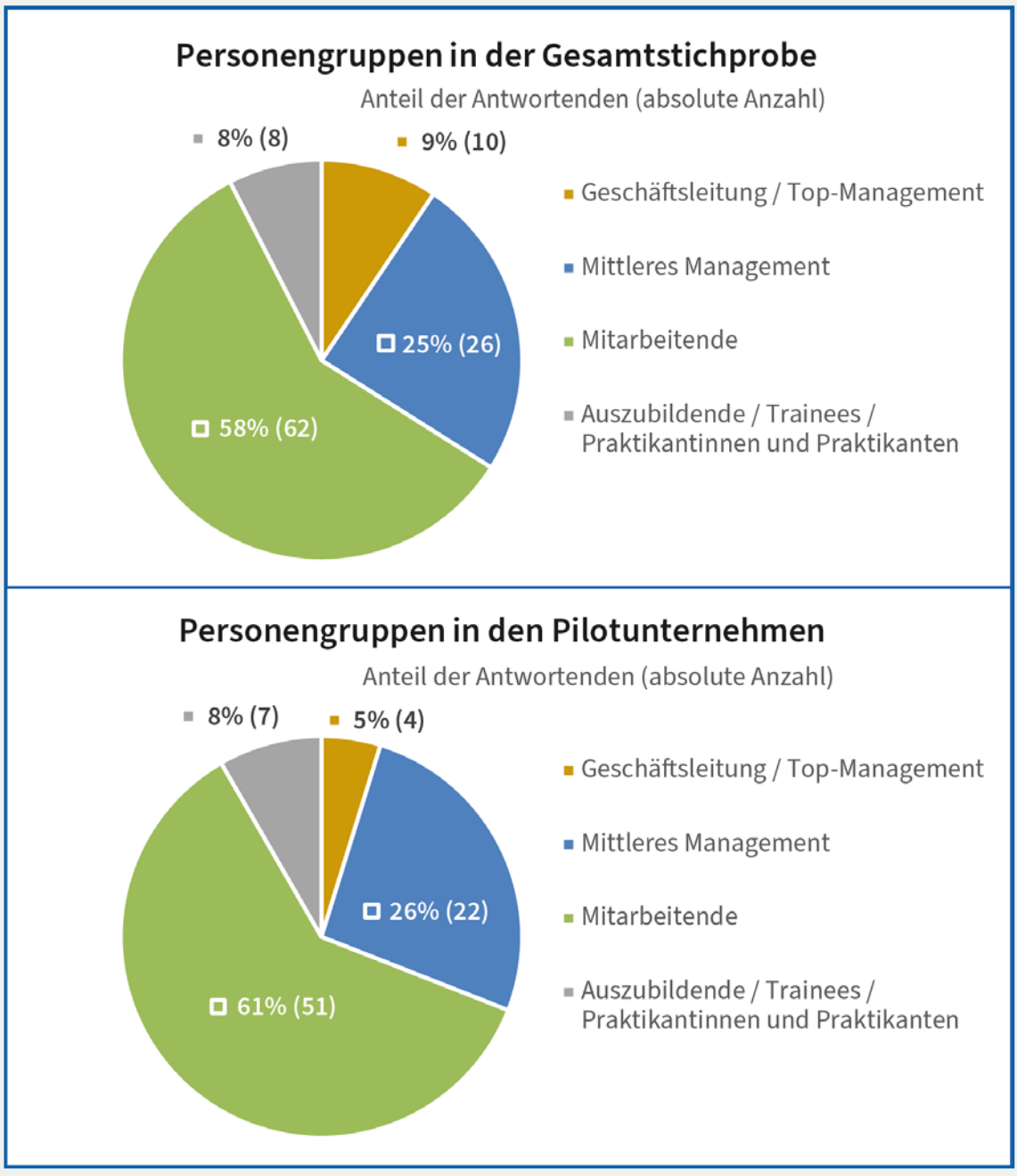


Abb. 11: *Personengruppen in der Gesamtstichprobe und in den Pilotunternehmen*

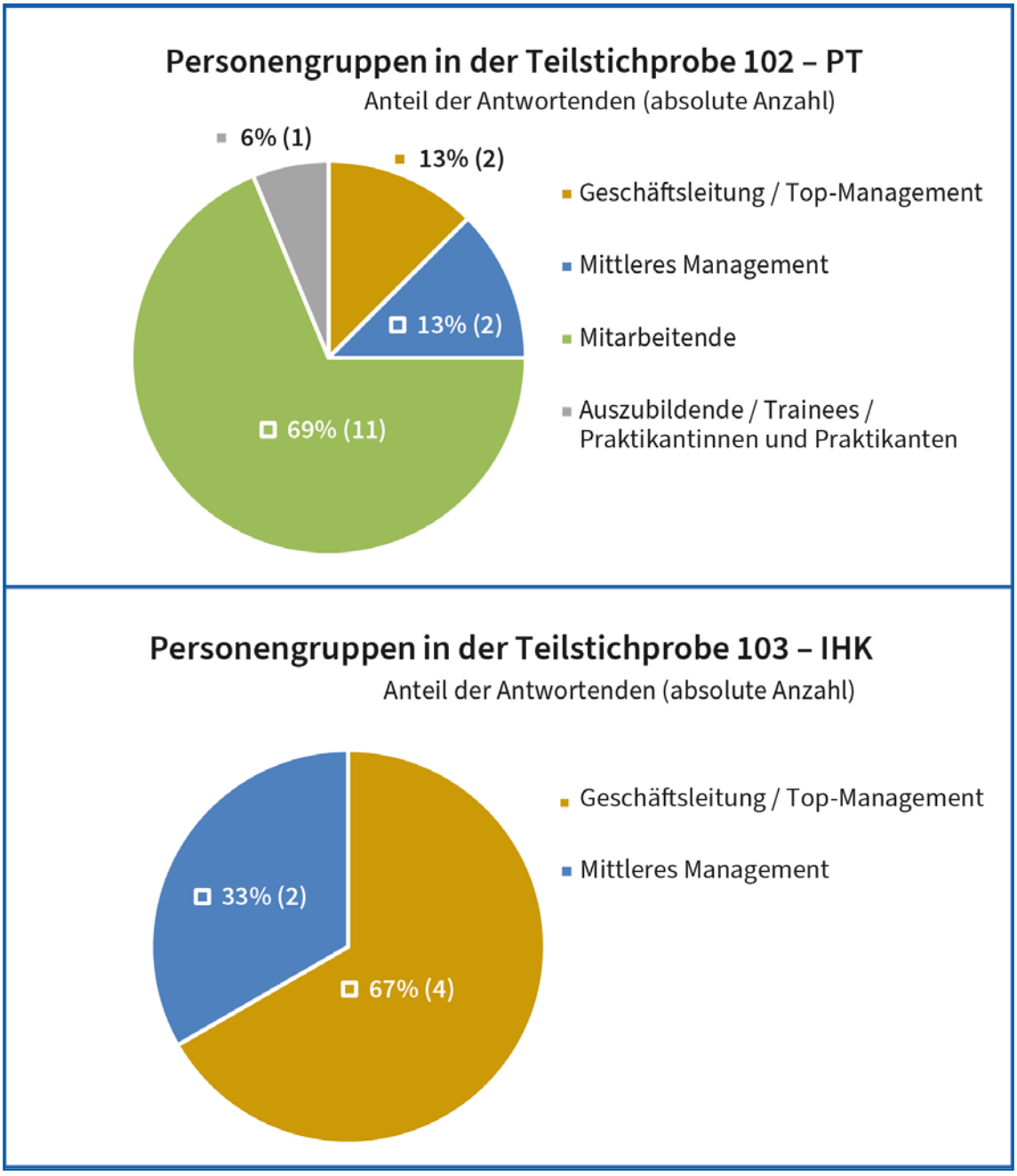


Abb. 12: *Personengruppen in den weiteren Unternehmen*

4.2 Die fünf Fragerubriken

Im Vorfeld der Konzeption der Umfrage wurden im Rahmen der Forschung und Lehre Grundlagen zu Tätigkeitsbereichen aus den sich fortlaufend weiterentwickelnden IT-Grundschutz-Katalogen des BSI [12] abgeleitet. Diese Vorarbeit bildete den Rahmen für die 18 entwickelten Fragekomplexe (in der Umfrage nummeriert), die aus mehreren Einzelfragen bezüglich eines Schlagworts bzw. Umfrage-Labels (ggf. inkl. einer näheren Definition) bestanden. Die Standardfrage hierbei lautete: „Wie häufig haben Sie in bzw. für Ihren Job mit Folgendem zu tun?“. Die Schlagwörter finden sich in Kurzform der Labels als Bezeichnung in den abgebildeten Grafiken. Es konnte meist aus vier Stufen eine Antwort gewählt werden. Dabei gibt die Summe aller bejahenden Antworten der Stufen „Selten“, „Häufiger“ und „Immer“ Auskunft darüber, ob etwas verwendet wird bzw. vorkommt, und die verneinende Stufe „Nie“, ob nicht. Bei der Auswertung wurden die Stufen auch aggregiert als Mittelwerte und Mediane betrachtet, wobei letzterer aufgrund der geringen Stichprobe bevorzugt wurde. Im Zuge der Auswertung wurden in Hinblick auf die Formierung von Gruppen aus den Tätigkeitsfeldern und der parallelen Entwicklung eines auf Tätigkeitsprofile abgestimmten Leitfadens diese Fragen in folgenden Fragerubriken zusammengefasst, die nicht durchgängig der ursprünglichen Reihenfolge der Befragung folgen und mit römischen Zahlen bezeichnet sind.

I. **Technische Infrastruktur**
II. **Externe Interaktion / [Risiken]**
III. **Arbeitsumgebung**
IV. **Sicherheitsmaßnahmen**
V. **Sensibilisierung**

Entsprechend dieser Einteilung werden im Weiteren die thematischen Umfrageergebnisse in Rang gebracht und Besonderheiten herausgestellt.

4.2.1 Nutzung technischer Infrastruktur

Im Fokus der umfassendsten Frage-Rubrik „I. Nutzung technischer Infrastruktur“ stehen Geräte, Software und Netzwerke im sozialen und technischen Sinne (siehe Abbildung 13). Die Grafik verdeutlicht die Tendenz der Antworten. Zentriert zeigt sie die Verteilung der Basisaussagen „Häufiger“ (hellblau) und „Selten“ (dunkelblau) und ist je nach Tendenz in Richtung der Spitzen „Immer“ (grün) oder „Nie“ (orange) ausgerichtet.

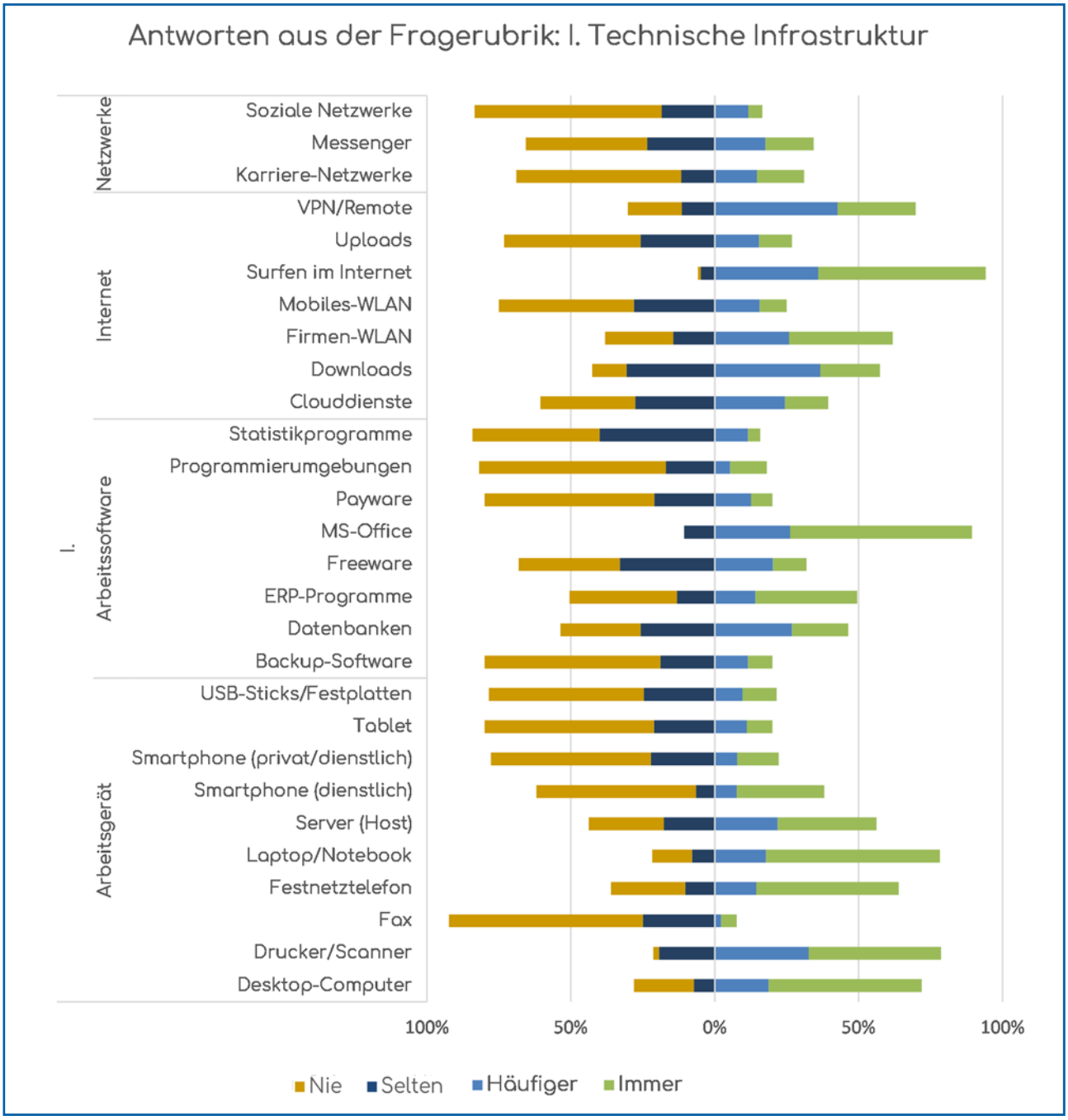


Abb. 13: *Antworten aus der Fragerubrik „I. Technische Infrastruktur“*

So gut wie gar nicht wird das Kommunikationsmittel Fax genutzt („Nie“ 68%, „Selten“ 25%). Ebenso gehören Programmierumgebungen, Backup-Software, Payware, Tablets und USB-Speichermedien zur kaum genutzten technischen Infrastruktur. Im beruflichen Kontext scheinen Karrierenetzwerke (57% „Nie“, 12% „Selten“) und noch weniger Soziale Netzwerke (65% „Nie“, 18% „Selten“) bei den ausgewählten Pilotunternehmen und Partnern eine Rolle zu spielen. Auffällig ist ebenfalls, dass angeblich gemischt genutzte (56% „Nie“) oder rein dienstliche Smartphones (55% „Nie“) oft gar nicht zum Einsatz kommen, während auf Messenger nicht in dem Maße verzichtet wird (42% „Nie“), obwohl sie meist auf Smartphones laufen. Eine Erklärung für beide Phänomene könnte der Einsatz firmeninterner Chatsysteme und Messenger als Teil von allgemeinen Softwarelösungen liefern, die auf Desktoprechnern genutzt werden. Messenger scheinen vor allem bei Tätigkeitsfeldern beliebt, die naturgemäß mit Kunden, Forschung, Personal, Finanzen (beispielsweise bei Finanzen/Buchhaltung/Rechnungswesen 100 Prozent „Häufiger“), Personal und der strategischen Kommunikation befasst sind (siehe Abbildung 14, es ist zu beachten, dass in allen Detailgraphiken aufgrund der Ausreißertendenz mit nur einer einzigen Antwort das Tätigkeitsfeld Sekretariat/Empfang/Pförtnerei/Poststelle schraffiert dargestellt wird). Die dargestellte Nutzung zieht gerade in diesen schutzbedürftigen Feldern die Frage nach der Sicherheit der Kommunikation über Messenger nach sich. Die Nutzung des dienstlichen Smartphones ist darüber hinaus stark vom Tätigkeitsfeld abhängig. Tätigkeitsfelder wie Kundenmanagement/-service (z. T. auch Vertrieb/Außendienst), Prozessmanagement/Qualitätssicherung/Controlling sind die einzigen Tätigkeiten im grob gefassten Feld der Kerntätigkeiten, die dieses nutzen, während es im Overhead, wie z. B. Verwaltung, Sekretariat und Marketing, sehr viel stärker verbreitet ist (siehe Abbildung 15).

Mit dem zuvor verwendeten Begriff „Overhead“ sind nicht direkt einzelnen Kostenträgern zurechenbare, allgemeine Tätigkeiten gemeint, während Kerntätigkeiten, die eine Haupttätigkeit eines Unternehmens darstellen und dieses untrennbar prägen, wie z. B. Materialwirtschaft/Logistik/Lager, Einkauf/Beschaffung, meist Kostenträgern leichter zurechenbar sind. Im Zuge der späteren Analyse der Korrelationen und Profilgruppen fiel früh ein Zusammenhang zwischen Zuordnung einer Tätigkeit zu Kerntätigkeiten und Zuordnung einer Tätigkeit zum Overhead im Hinblick auf ähnliches Nutzungsverhalten auf. Diese Beobachtung hatte letztlich auch einen Einfluss auf die Anordnung der Tätigkeitsfelder in den Detail-Grafiken und führte dort zu einheitlicheren Verläufen (vgl. Abbildung 14).

Statistikprogramme, Mobiles-WLAN, Uploads, Freeware und Clouddienste (beispielsweise 15% „Immer“, 24% „Häufiger“, 28% „Selten“) gehören im Median ebenfalls zu den eher selten genutzten technischen Mitteln. Datenbanken, ERP-Programme zur Prozessplanung (beispielsweise bei 63% der Teilnehmeden selten bis immer in Verwendung) und Server gehören zu den häufig genutzten Mitteln, so wie erwartet auch Downloads, VPN-/Remote-Zugänge, das Festnetztelefon und Drucker/Scanner. Laptops/Notebooks („Häufiger“ 18%, „Immer“ 60%) werden durchgängiger genutzt als Desktop-Computer („Häufiger“ 19%, „Immer“ 53%). Nur eine Person (knapp 1%) gab an, anstelle eines Laptops oder Desktoprechners auf ein Tablet zurückzugreifen. Personen ohne digitalen Arbeitsplatz gab es unter den Befragten nicht. Im Median sind das Surfen im Internet (nur knapp unter 1% surfen „Nie“, 58% „Immer“) und die Nutzung von Office-Software-Produkten des Marktführers (63% „Immer“, 0% „Nie“) fester Bestandteil der meisten Tätigkeiten.

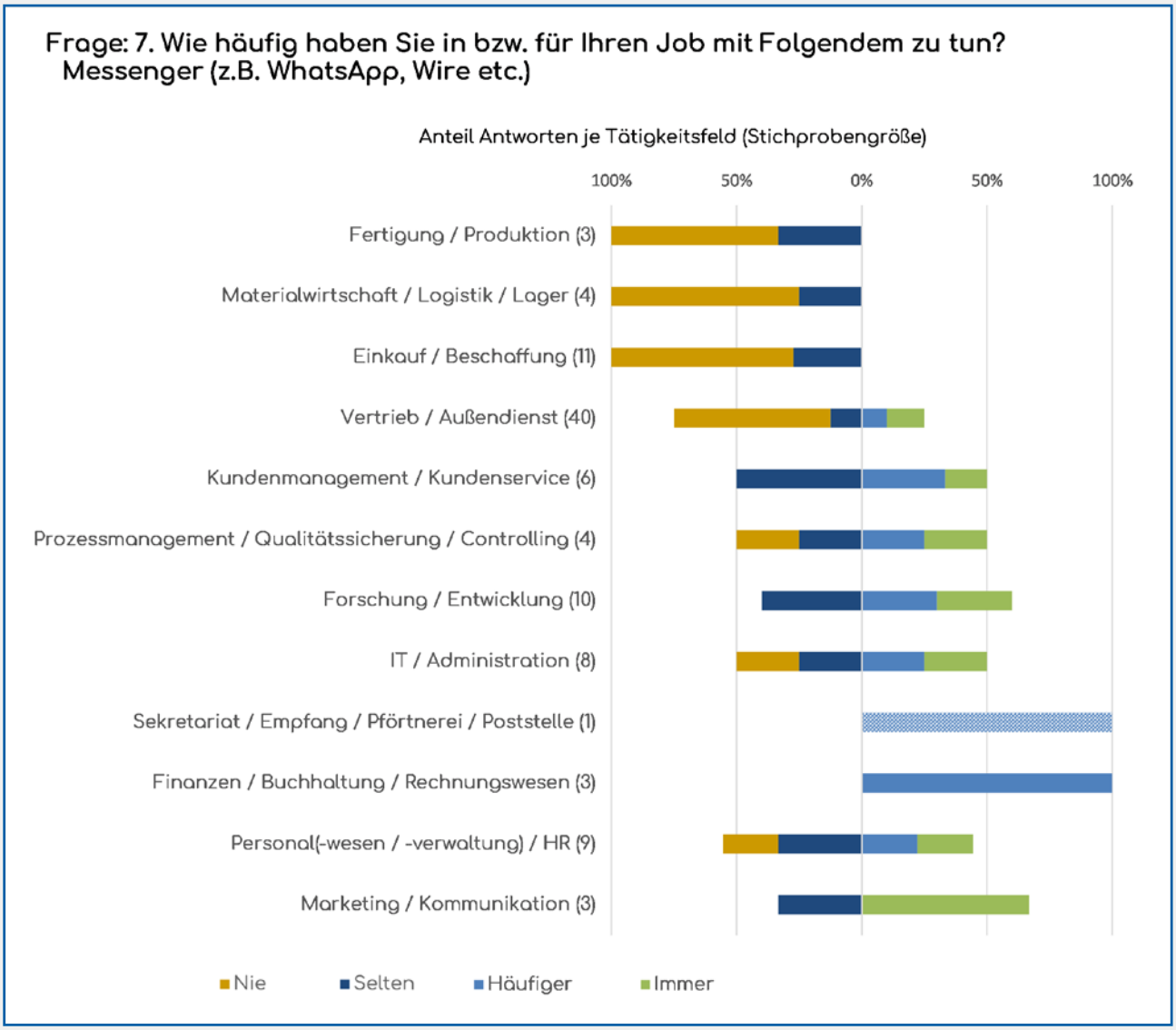


Abb. 14: *Frage „Messenger“ aus Fragekomplex 7 mit Ergebnissen zu den Tätigkeitsfeldern*

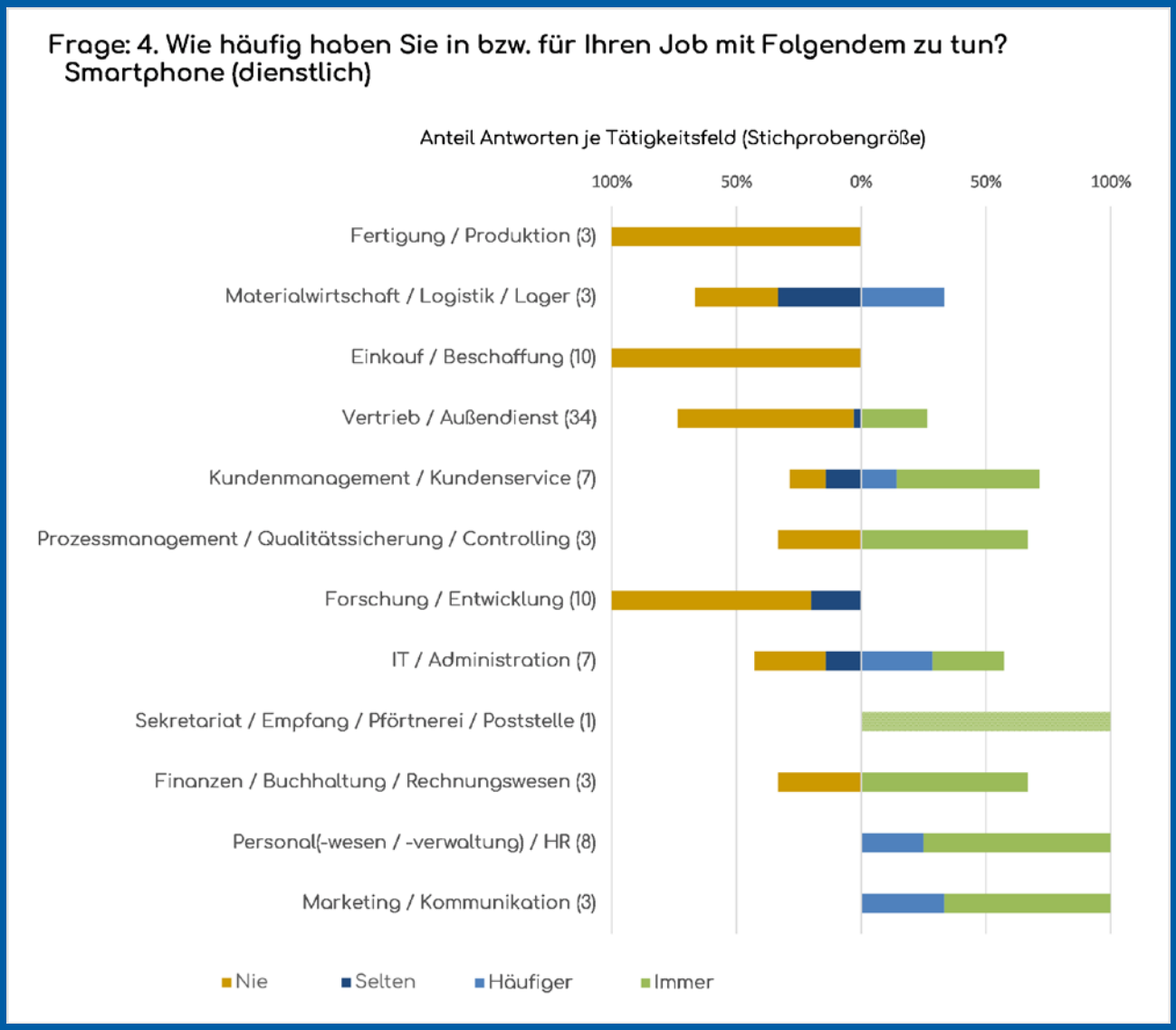


Abb. 15: *Frage „Smartphone (dienstlich)“ aus Fragekomplex 4 mit Ergebnissen zu den Tätigkeitsfeldern*

4.2.2 Externe Interaktion

Die Fragerubrik „II. Externe Interaktion“ (siehe Abbildung 16) beschreibt am ehesten die Bedrohungen und Risiken, welche meist im Austausch mit firmenexternen Akteurinnen und Akteuren bestehen. Selbst wenn keine interne Gefahr besteht, z. B. durch Geheimnisverrat oder Sabotage, sind Außenkontakte nach wie vor relevant, da an diese meist Informationen weitergegeben werden oder Anreize gekoppelt sind.

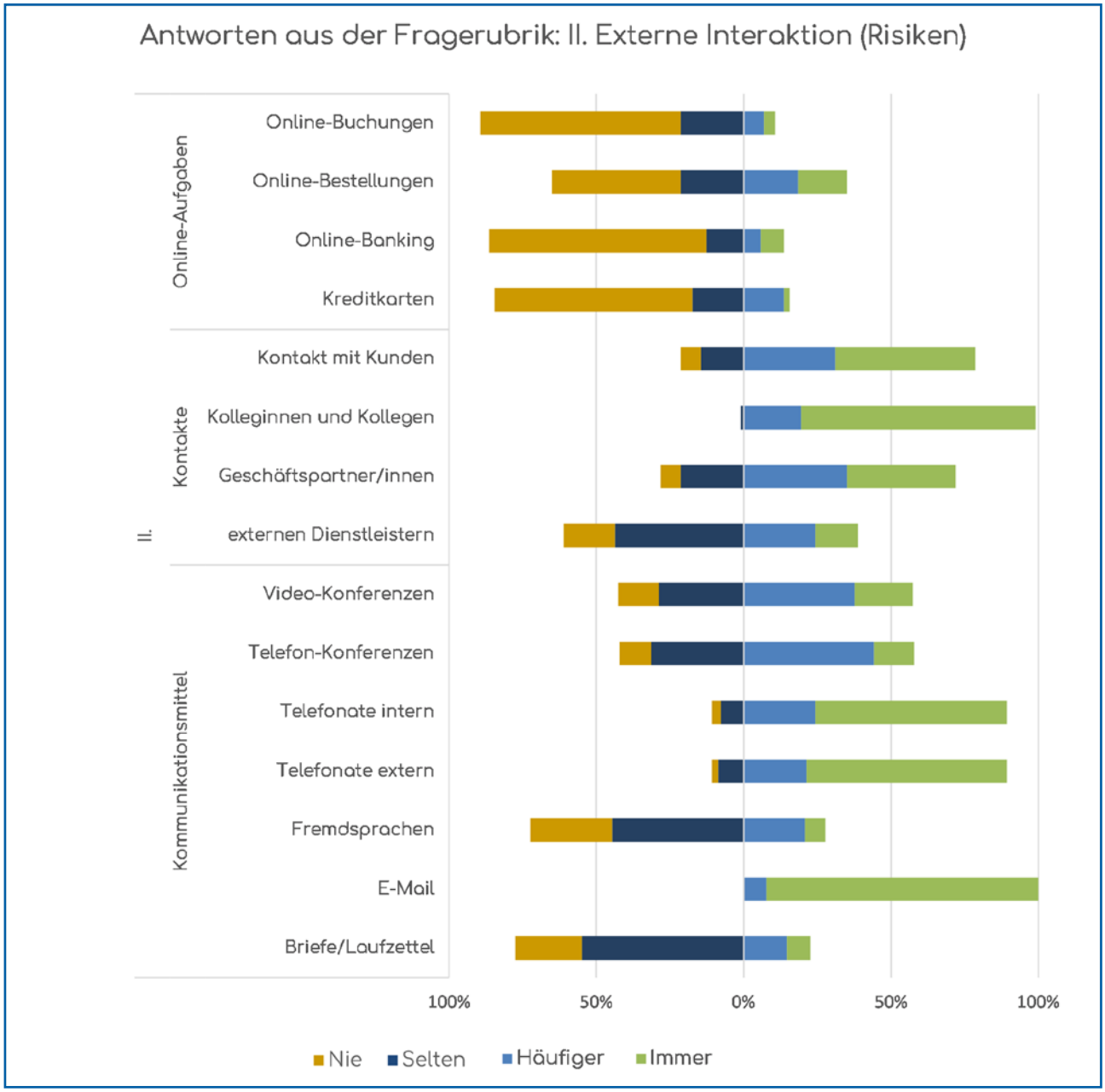


Abb. 16: *Antworten aus der Fragerubrik „II. Externe Interaktion“*

Online-Buchungen (4% „Immer“, 7% „Häufiger“, 21% „Selten“) und Online-Banking (8% „Immer“, 6% „Häufiger“, 13% „Selten“) sowie die Verwendung von Kreditkarten (2% „Immer“, 14% „Häufiger“, 17% „Selten“) bleiben hierbei meist nur spezifischen Tätigkeitsfeldern wie Sekretariat, Marketing und Finanzen/Buchhaltung/Rechnungswesen vorbehalten (siehe Abbildung 17).

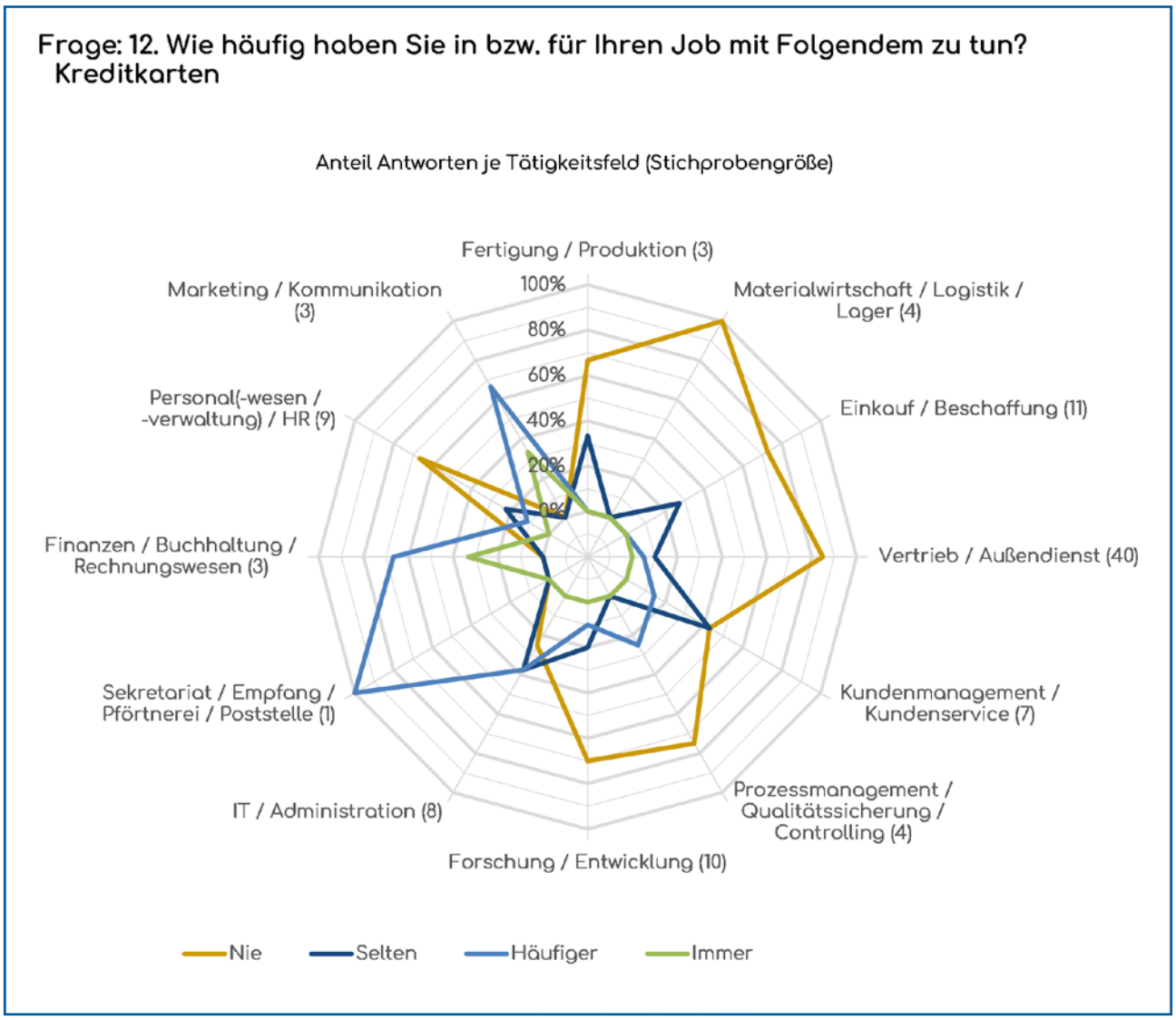


Abb. 17: *Frage „Kreditkarten“ aus Fragekomplex 12 mit Ergebnissen zu den Tätigkeitsfeldern*

Ähnlich verhält es sich bei der insgesamt relativ seltenen Nutzung von Fremdsprachen oder Online-Bestellungen (17% „Immer“, 18% „Häufiger“, 21% „Selten“). Der Kontakt mit externen Dienstleistern findet wesentlich seltener statt als der häufige oder permanente Kontakt mit Geschäftspartnern und Kunden (zusammengefasst 70% bzw. 80%). Briefe und Laufzettel werden erwartungsgemäß seltener genutzt (wenn auch häufiger auf Ebene der Geschäftsleitung) als das Telefon und das allgegenwärtige Kommunikationsmittel E-Mail (92% „Immer“, 8% „Häufiger“). Konferenzen, sowohl per Telefon als auch Video (siehe Abbildung 18), sind unterschiedlich über die Tätigkeitsfelder verteilt. Kerntätigkeiten wie Fertigung/Produktion, Materialwirtschaft/Logistik/Lager, auch überraschend selten Einkauf/Beschaffung nehmen diese trotz Pandemie kaum wahr. Der an die Kerntätigkeiten direkt angegliederte Overhead wie Vertrieb und Kundenmanagement, aber auch der klassische Overhead aus Verwaltung und Führung greifen hier häufiger oder fast immer zu dieser Kommunikationsform. Die aufgrund nur einer Antwort immer kritisch zu betrachtende Tätigkeit Sekretariats/Empfang/Pförtnerei/Poststelle scheint in dieser durch Planung geprägten Gruppe in diesem Einzelfall nicht vertreten. Der Kontakt mit Kolleginnen und Kollegen ist in allen Tätigkeitsfeldern selbstverständlich und liegt bei einer Bejahung von 100 Prozent, wovon nur ein Prozent selten Kontakt hat.

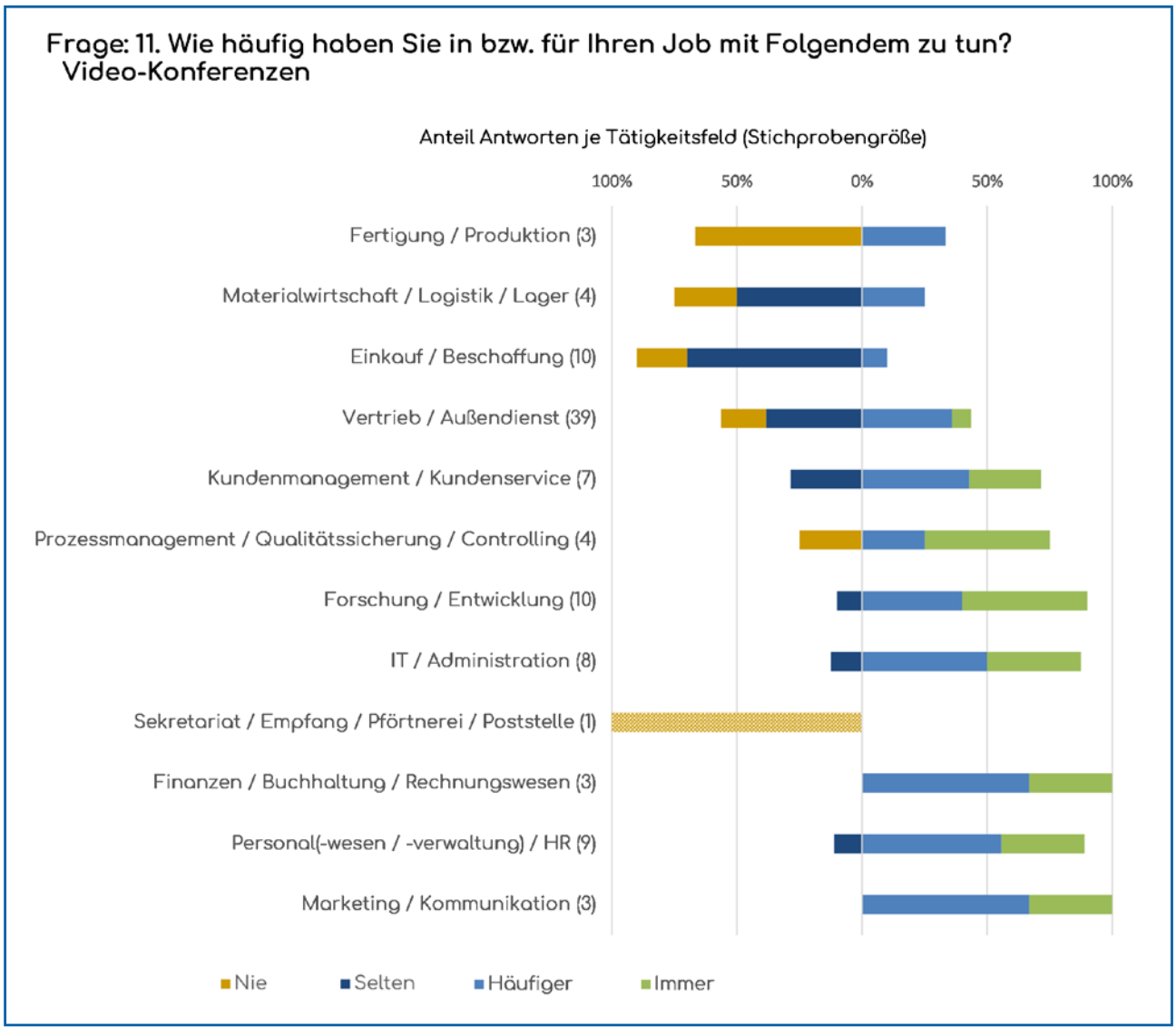


Abb. 18: *Frage „Video-Konferenzen“ aus Fragekomplex 11 mit Ergebnissen zu den Tätigkeitsfeldern*

4.2.3 Arbeitsumgebung

Die Fragerubrik „III. Arbeitsumgebung“ (siehe Abbildung 19) beschreibt am besten die physische Exposition, der Mitarbeitende ausgesetzt sind, und ist durch Ort, dessen Beständigkeit und Bewegung durch ungesicherte Räume im weiten Sinne gekennzeichnet. Daher ist die Arbeitsumgebung durch das Pandemiegeschehen am stärksten geprägt. Im Vergleich zu der Zeit vor der Covid-19-Pandemie verdoppelte sich grob die Anzahl der Mitarbeitenden, die ihre Tätigkeit im Homeoffice ausüben. Außerdem wurde ein Zusammenhang zwischen einer höheren Nutzung von Homeoffice und Personen mit einem höheren Bildungsabschluss nachgewiesen. Es kann zudem davon ausgegangen werden, dass vieles von diesem Wandel bleiben und neue Sicherheitslagen prägen wird [22].

Vor diesem Hintergrund sollen folgende Ergebnisse betrachtet werden. Co-Working-Spaces werden so gut wie nie genutzt (95% „Selten“ bzw. „Nie“), während erwartungsgemäß die meisten Mitarbeitenden häufiger oder immer an einem festen Arbeitsplatz ihrer Tätigkeit nachkommen (60% „Immer“, 30% „Häufiger“, 5% „Selten“). Dieser wird gefolgt vom Homeoffice, dessen Häufigkeit sicherlich von der Pandemiesituation im Untersuchungszeitraum Februar 2021 geprägt ist und das von der Forschung/Entwicklung besonders häufig genutzt wird. Es ist festzustellen, dass in Zeiten der Reisebeschränkungen die Nutzung von wechselnden Arbeitsplätzen in der untersuchten Gruppe kaum eine Rolle gespielt hat. Bemerkenswert ist ein verhältnismäßig häufig wechselnder Arbeitsplatz in Personalwesen/-verwaltung. Selten wurden Übernachtungen eingelegt, mobil gearbeitet (beispielsweise nur 3% „Immer“, 25% „Häufiger“, 34% „Selten“) oder Reisen mit einem KFZ durchgeführt. Auch die seltene Teilnahme an betrieblichen Feierlichkeiten könnte auf die Pandemie zurückgeführt werden.

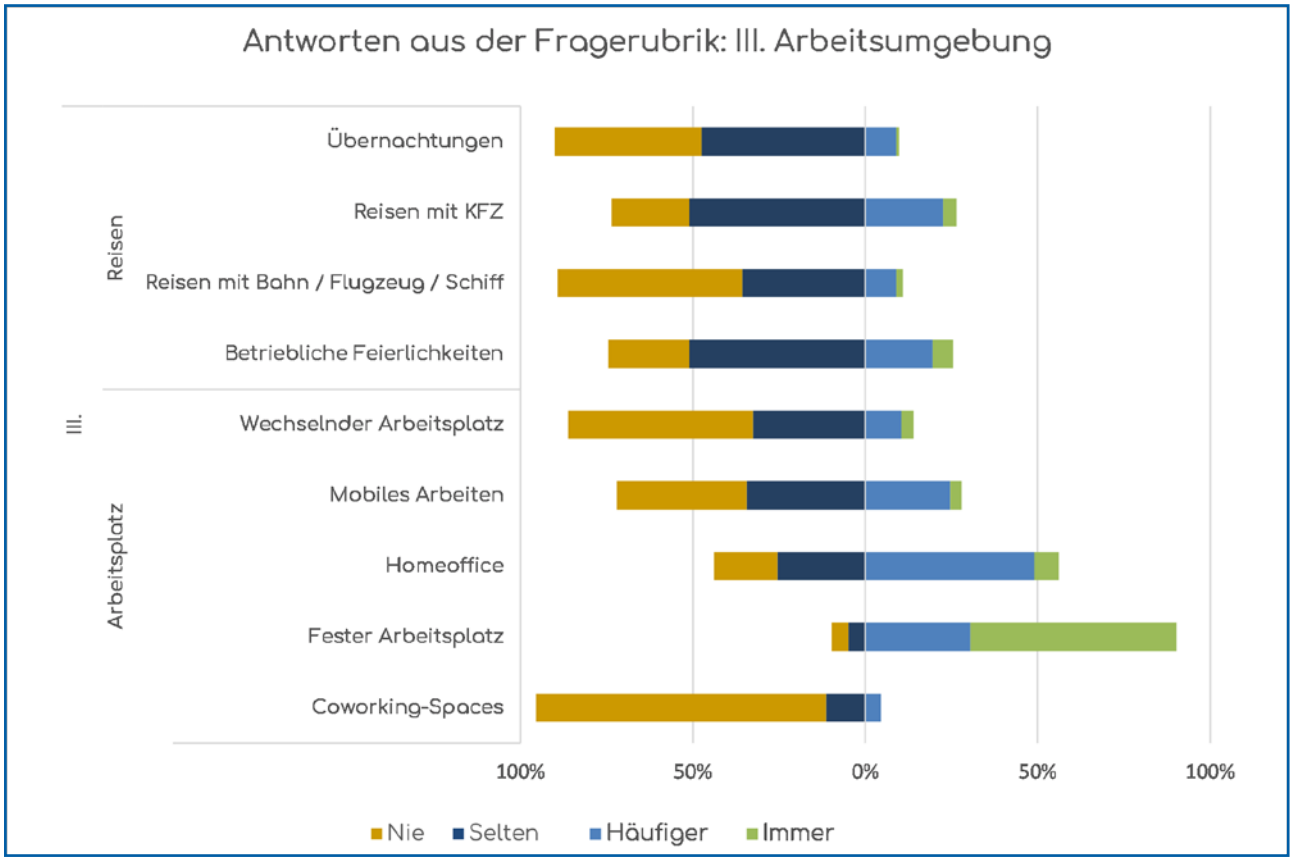


Abb. 19: *Antworten aus der Fragerubrik „III. Arbeitsumgebung“*

Beim genaueren Hinschauen gehört mobiles Arbeiten (siehe Abbildung 20) eher in Tätigkeitsfeldern wie IT/Administration, Vertrieb/Außendienst, Kundenmanagement/Kundenservice und Marketing und vereinzelt in den Verwaltungstätigkeiten zu den häufigen Arbeitsformen. In traditionellen Kerntätigkeiten kommt dieses eher selten oder nie vor.

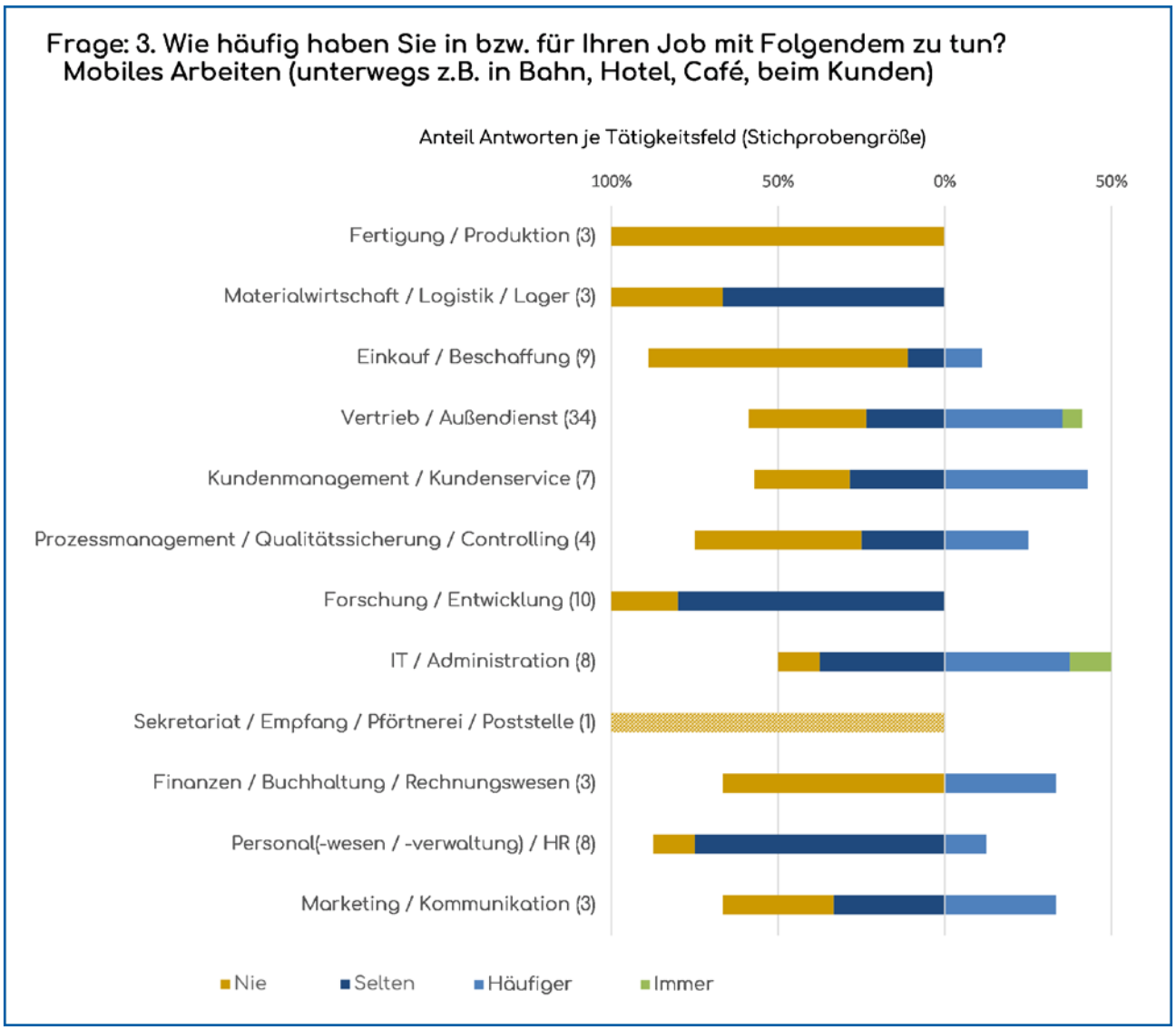


Abb. 20: *Frage „Mobiles Arbeiten" aus Fragekomplex 3 mit Ergebnissen zu den Tätigkeitsfeldern*

4.2.4 Sicherheitsmaßnahmen

Die Fragerubrik „IV. Sicherheitsmaßnahmen“ spiegelt den jeweiligen Stand zu Maßnahmen, Zutrittskontrolle, Zugriffskontrolle und Zugangskontrolle wider (siehe Abbildung 21). Sie geht eng mit der Fragerubrik „V. Sensibilisierung“ einher, die im Ganzen ebenfalls als Sicherheitsmaßnahme betrachtet werden kann, deren Schulungskonzepte aber alle vorigen Fragerubriken überspannen und daher gesondert betrachtet werden sollen. Zugangskontrollen per Biometrie werden so gut wie nie verwendet, dort ist immer und durchgängig das Passwort das Mittel der Wahl (18% „Häufiger“, 66% „Immer“). Lediglich im Tätigkeitsfeld Einkauf / Beschaffung (9%) und im stark vertretenen Vertrieb / Außendienst (7,5%) wurde ausgesagt, nie ein Passwort zu nutzen. Wenig erstaunlich, wenn auch sicherheitstechnisch bedenklich, ist zudem, dass fast immer Kolleginnen und Kollegen Zutritt zum Arbeitsplatz (65% „Immer“, 20% „Häufiger“, 13% „Selten“) haben und dieser meist über einen Firmenschlüssel bzw. Chip erhalten wird. Zutritt wiederum zum Tresor / Safe, zu sensiblen Bereichen oder mit Generalfirmenschlüssel ist so wie auch Zugriff auf sensible personenbezogene Daten nur einzelnen Tätigkeitsfeldern vorbehalten. Hierbei ist anzumerken, dass der Generalfirmenschlüssel keinen Zutritt zu sensiblen Bereichen ermöglichen muss, sondern meist für alle Räumlichkeiten bis zu einer gewissen Sicherheitsstufe gilt. Daher wird dieser etwas häufiger vergeben als der Zutritt zu sensiblen Bereichen.

Erstaunlich häufig und weit verbreitet scheint im Median nach Selbstaussage der Probanden und Probandinnen jedoch der Zugriff auf vertrauliche (z. T. interne / geheime) Unternehmensdaten und allgemeine personenbezogene Daten zu sein (siehe Abbildung 21). Zugriff auf sensible personenbezogene Daten hat erwartungsgemäß „Selten“ bis „Immer“ Personal (-wesen / -verwaltung) / HR, aber überraschenderweise „Nie“ alle zehn Befragten aus Einkauf / Beschaffung (siehe Abbildung 22).

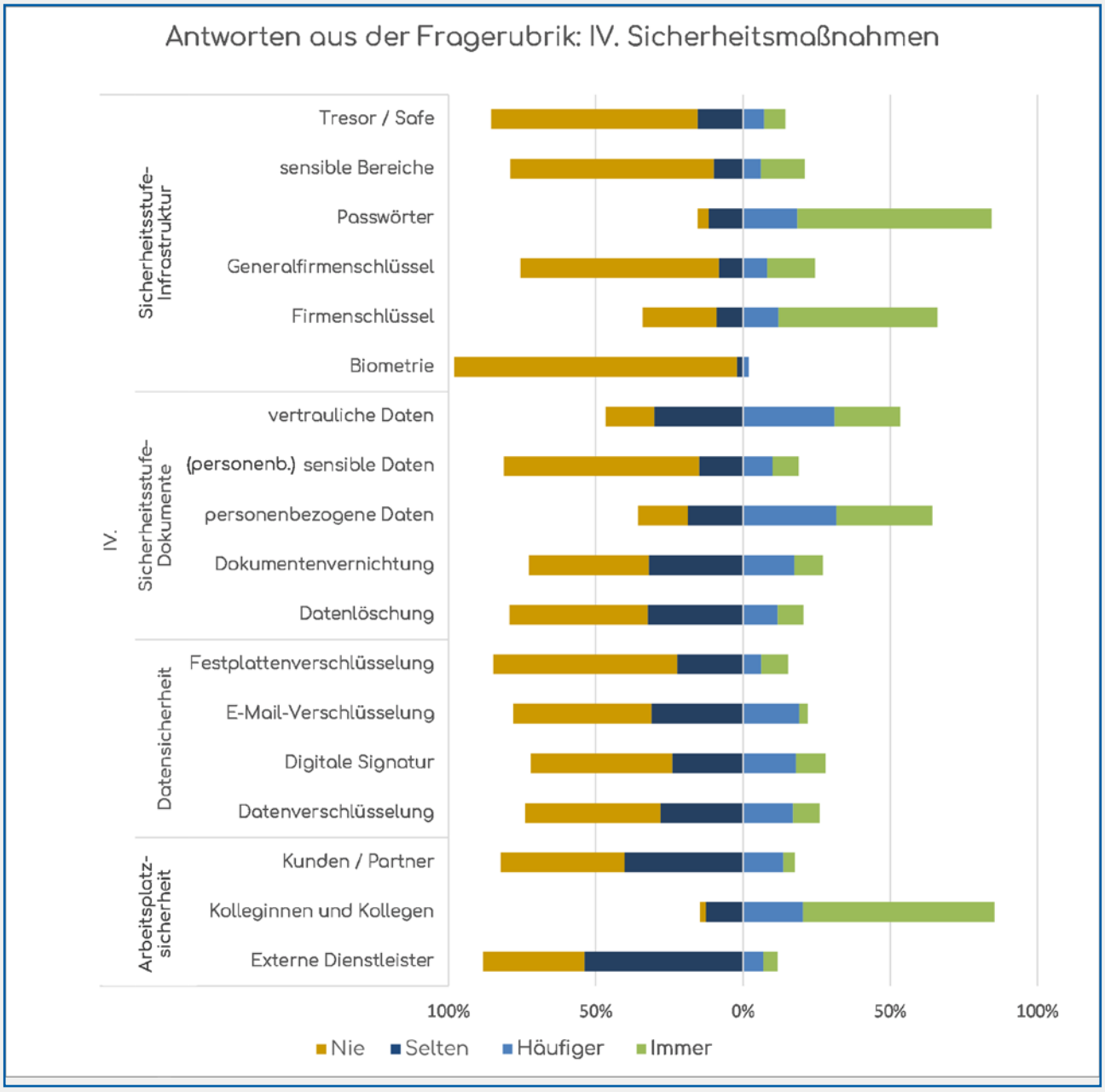


Abb. 21: *Antworten aus der Fragerubrik „IV. Sicherheitsmaßnahmen“*

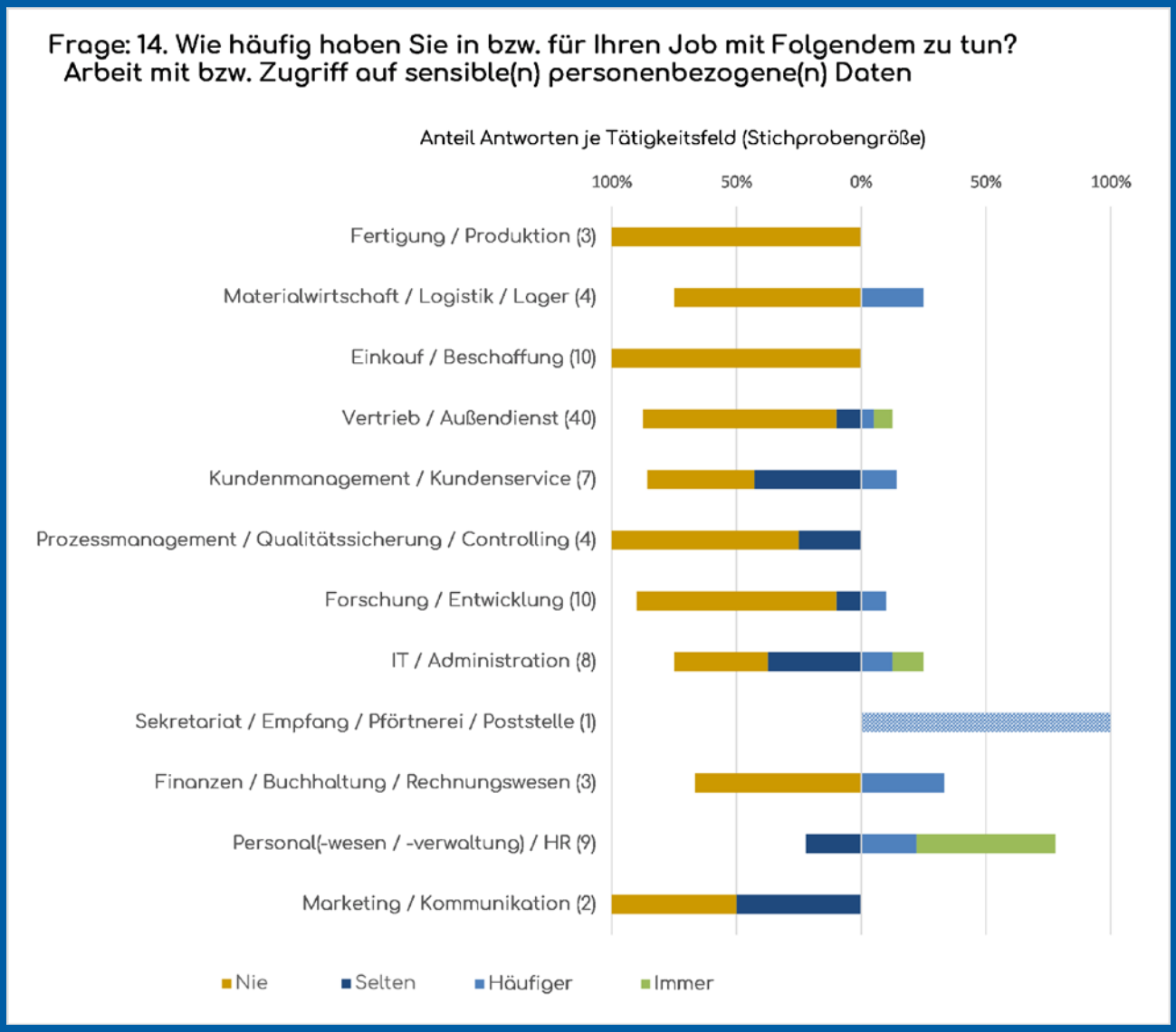


Abb. 22: *Frage „sensible personenbezogene Daten“ aus Fragekomplex 14 mit Ergebnissen zu den Tätigkeitsfeldern*

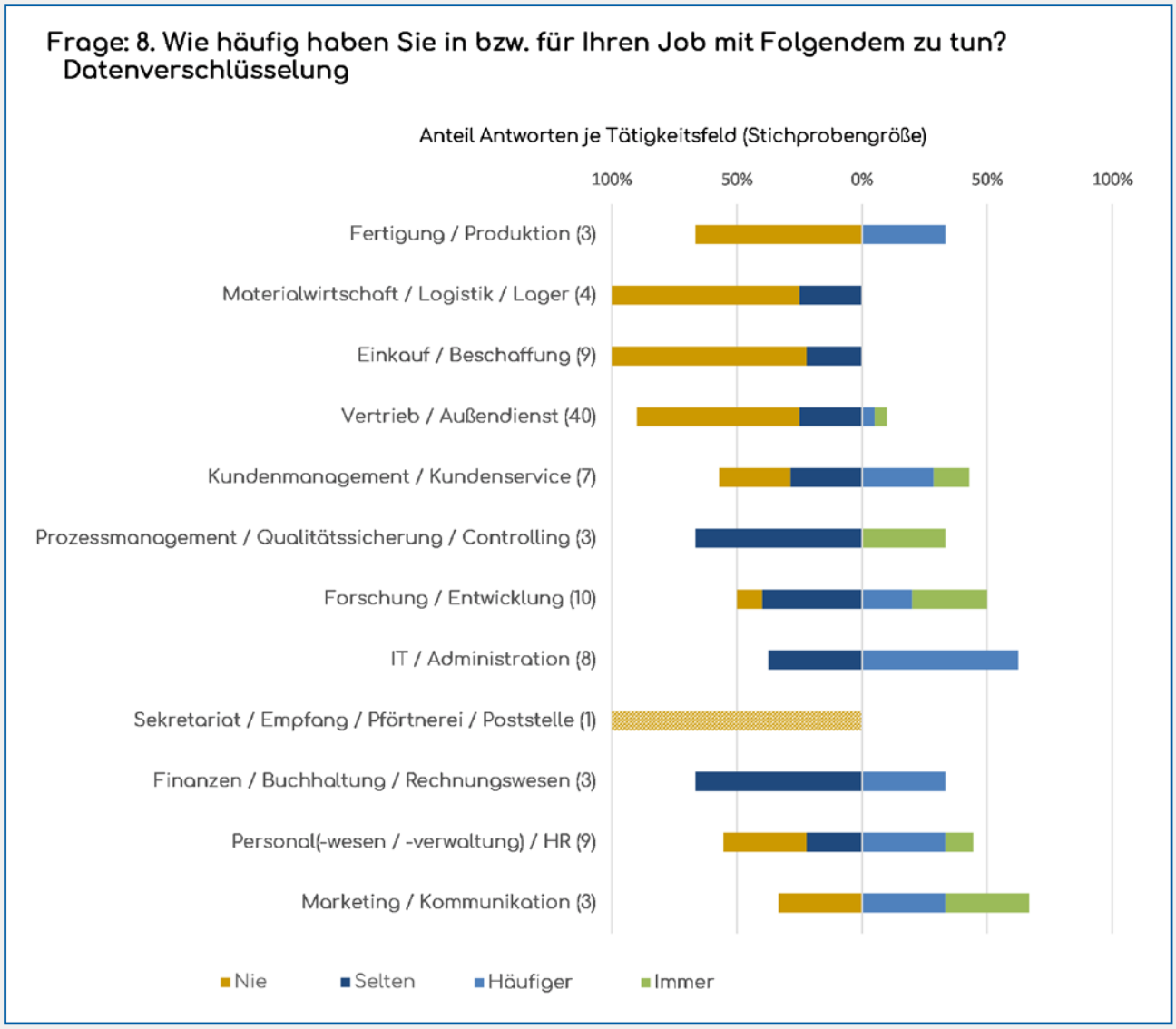


Abb. 23: *Frage „Datenverschlüsselung" aus Fragekomplex 8 mit Ergebnissen zu den Tätigkeitsfeldern*

Zugriffskontrollen durch E-Mail-Verschlüsselung, Datenlöschung, Datenverschlüsselung und Digitale Signatur, aber auch Zutritt von Kunden/Partnern oder externen Dienstleistern sind eher selten (siehe Abbildung 21). Wird die Sicherheitsmaßnahme Datenverschlüsselung (siehe Abbildung 23) betrachtet, so ist festzustellen, dass diese bereits überall verwendet wird, sofern die einzelne Antwort im Sekretariat vernachlässigt wird. Tätigkeitsfelder im Zusammenhang mit Finanz- und Technologiedaten (Forschung/Entwicklung, IT/Administration) sichern ihre Daten relativ betrachtet häufiger durch Verschlüsselung. Insbesondere mit Blick auf die Datenverschlüsselung und E-Mail-Verschlüsselung fällt das Fehlen der Angabe „Nie“ im Bereich Finanzen bzw. Controlling auf, ebenso in der IT, sowie die starke Nutzung bei der Forschung und bei Marketing/Kommunikation, welches bei letzterem durch die strategischen Daten und der Nähe zur Unternehmensführung begründet sein könnte (siehe Abbildung 24). Weniger schlüssig und homogen ist der Einsatz einer Digitalen Signatur (siehe Abbildung 25), die zwar ähnlichen Mustern folgt, aber allgemein kaum verbreitet ist, am wenigsten in den traditionellen Kernbereichen und beim Personal oder im Marketing. Unter anderem wird auch dort nochmal unterstrichen, dass IT/Administration von Natur aus sich stark affin zu fast allen digitalen Sicherheitsmaßnahmen verhält.

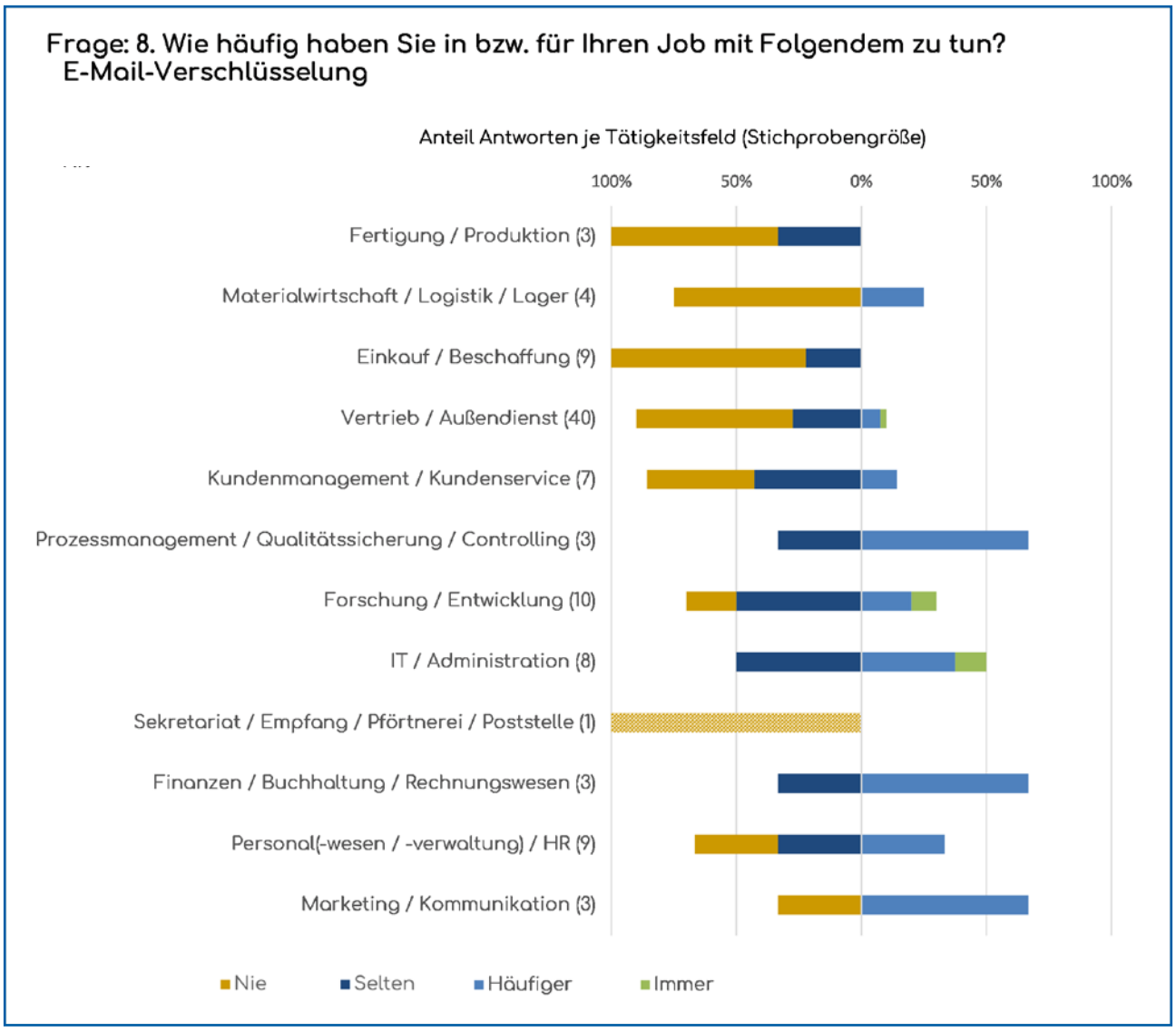


Abb. 24: *Frage „E-Mail-Verschlüsselung“ aus Fragekomplex 8 mit Ergebnissen zu den Tätigkeitsfeldern*

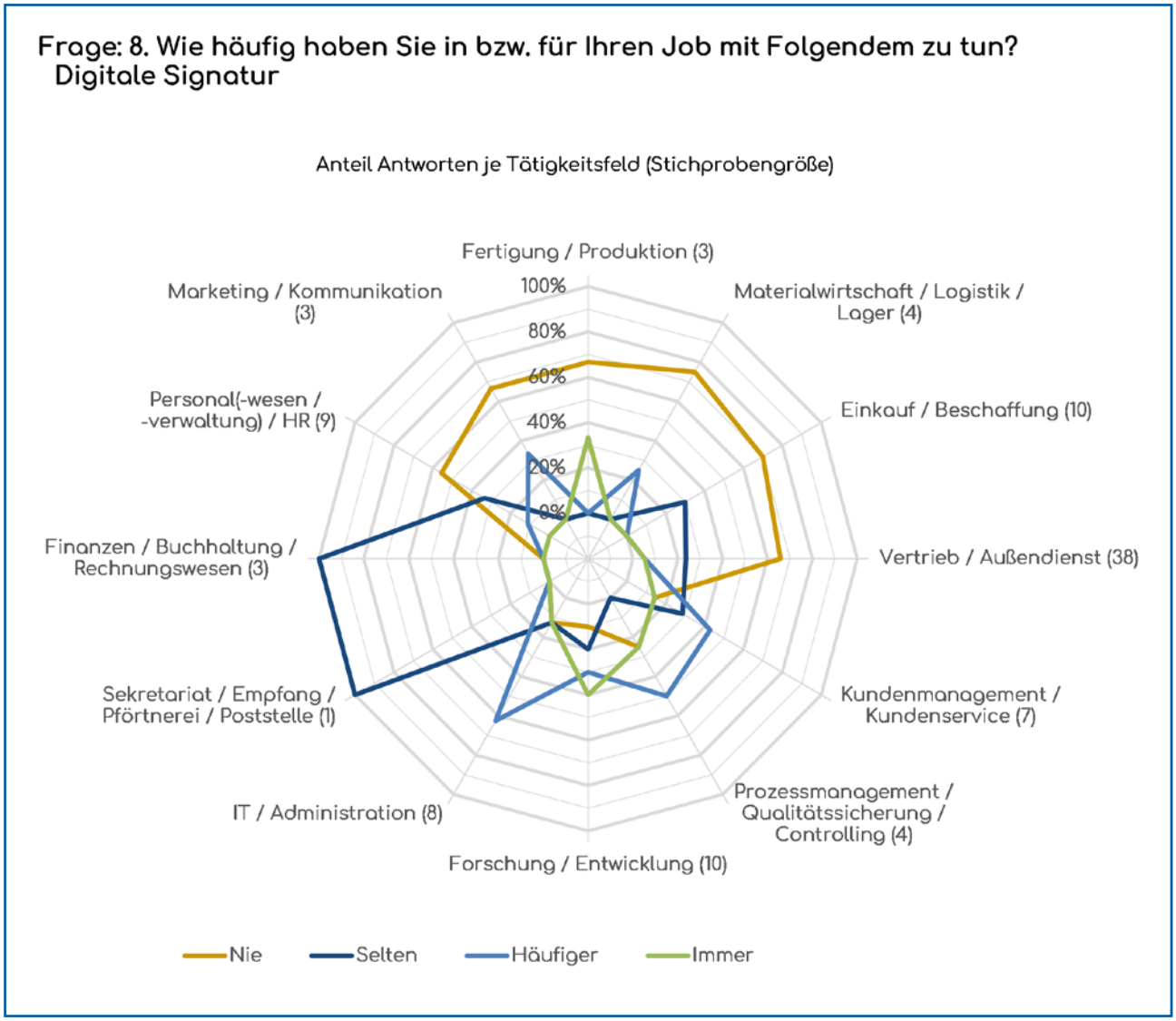


Abb. 25: *Frage „Digitale Signatur“ aus Fragekomplex 8 mit Ergebnissen zu den Tätigkeitsfeldern*

4.2.5 Sensibilisierung

Sensibilisierung ist grundsätzlich für alle wichtig, sowohl für einen selbst als auch für das ganze Unternehmen. Sich den möglichen Gefahren in Informationssicherheit bewusst zu sein, ist nicht selbstverständlich und erfordert kontinuierlichen Input.

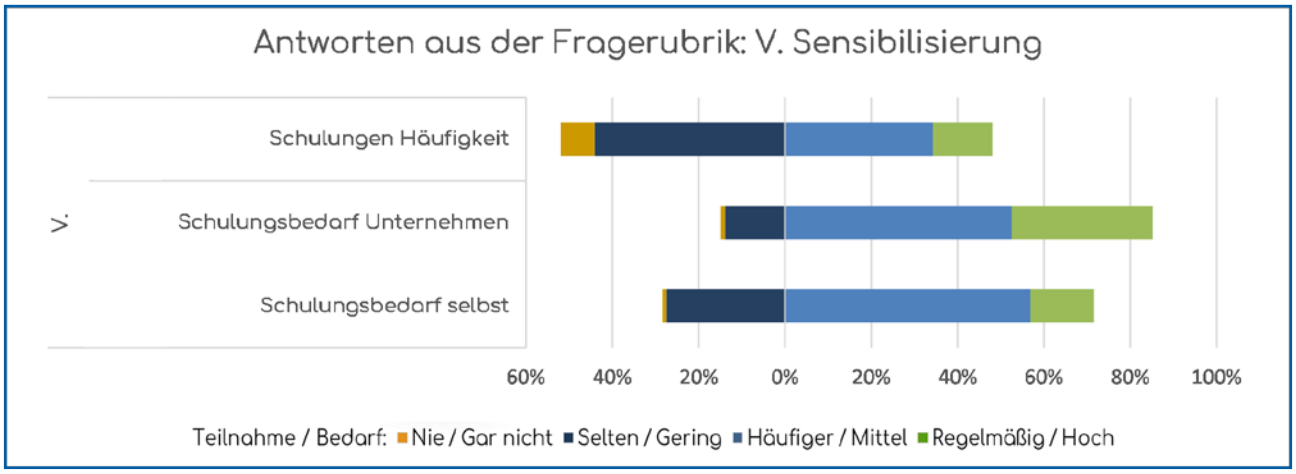


Abb. 26: *Antworten aus der Fragerubrik „V. Sensibilisierung“*

Aus der Umfrage geht hervor, dass verschiedene Tätigkeitsfelder unterschiedlich oft an Schulungen oder Sensibilisierungsmaßnahmen zum Thema Informationssicherheit teilgenommen haben (siehe Abbildung 27). So ist zu vermerken, dass ca. 20 Prozent der Beschäftigten in den Bereichen Personalwesen, Vertrieb, Einkauf, IT / Administration, Forschung / Entwicklung und Kundenmanagement regelmäßig an solchen Schulungen teilnehmen. Fertigung / Produktion gaben besonders auffällig mit über 30 Prozent an, nie eine Schulung zur Informationssicherheit besucht zu haben. Die Tätigkeitsbereiche Sekretariat / Empfang, Buchhaltung / Finanzen und Marketing / Kommunikation gaben meistens an, häufiger solche Sensibilisierungsmaßnahmen genießen zu dürfen.

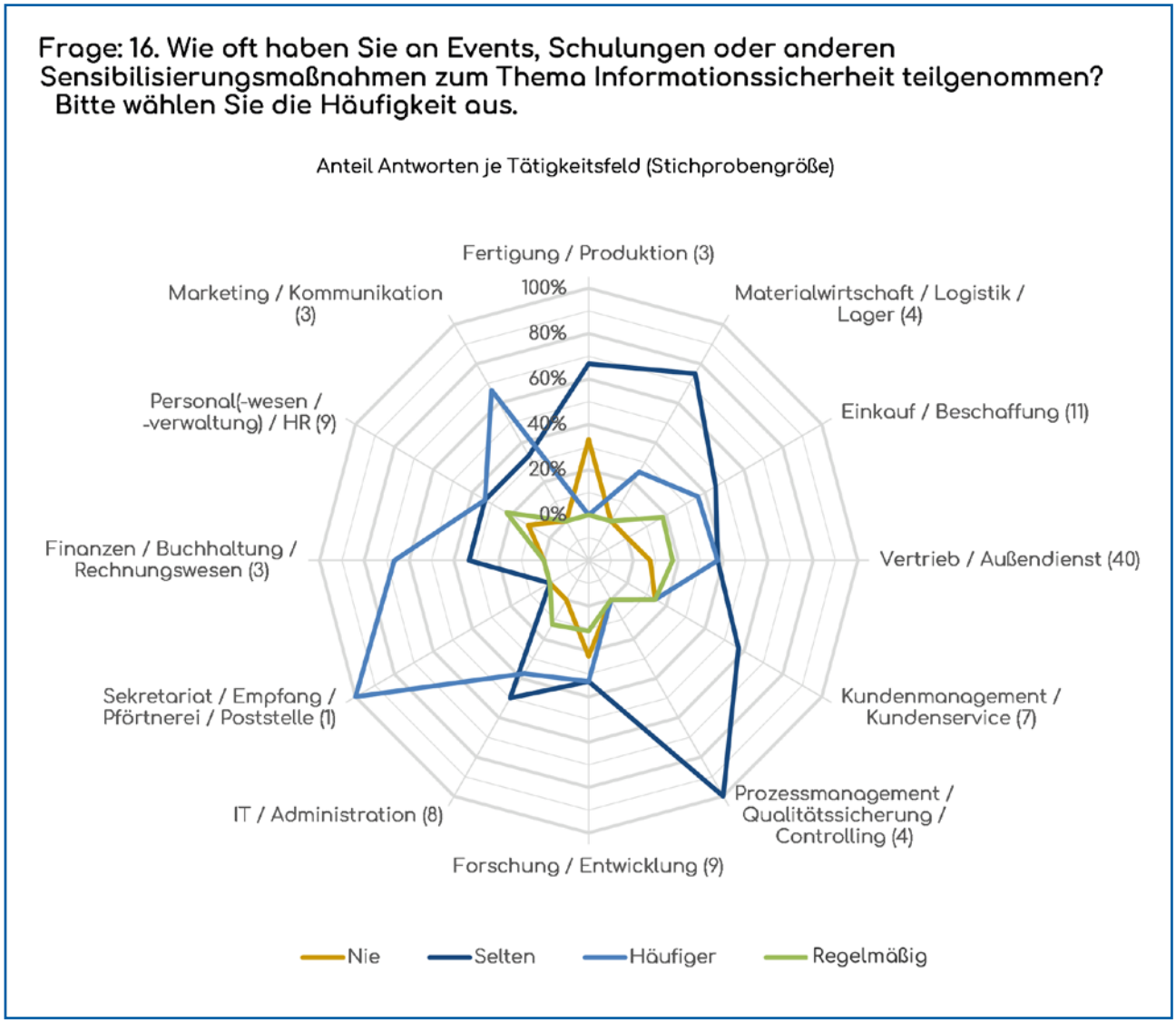


Abb. 27: *Häufigkeit der Schulungsmaßnahmen nach Tätigkeit (Fragekomplex 16)*

Zur Frage nach dem Bedarf an Schulungen zur Informationssicherheit in den jeweiligen Tätigkeitsfeldern wurde deutlich, dass alle befragten Bereiche den Bedarf mit stärkerer Tendenz „Hoch“ für das Unternehmen (siehe Abbildung 26 und 29), als für sich selbst einschätzen (siehe Abbildung 26 und 28). Es besteht mit über einem Dreiviertel der Antwortenden besonders bei Azubis und Geschäftsleitung ein mittlerer Bedarf sich selbst weiterzubilden (siehe Abbildung 30). Diese Tendenz dominiert bei allen Personengruppen, während niemand die Maßnahme für ganz unnötig hält. Bei Mitarbeitenden und Mittlerem Management verteilen sich die Antworten aber etwas stärker zu „Gering“. Im Mittleren Management besteht bei rund 20 Prozent ein hoher Weiterbildungswunsch für sich selbst, welches den stärksten Ausschlag dieser Antwortstufe im Vergleich zu anderen Personengruppen bedeutet.

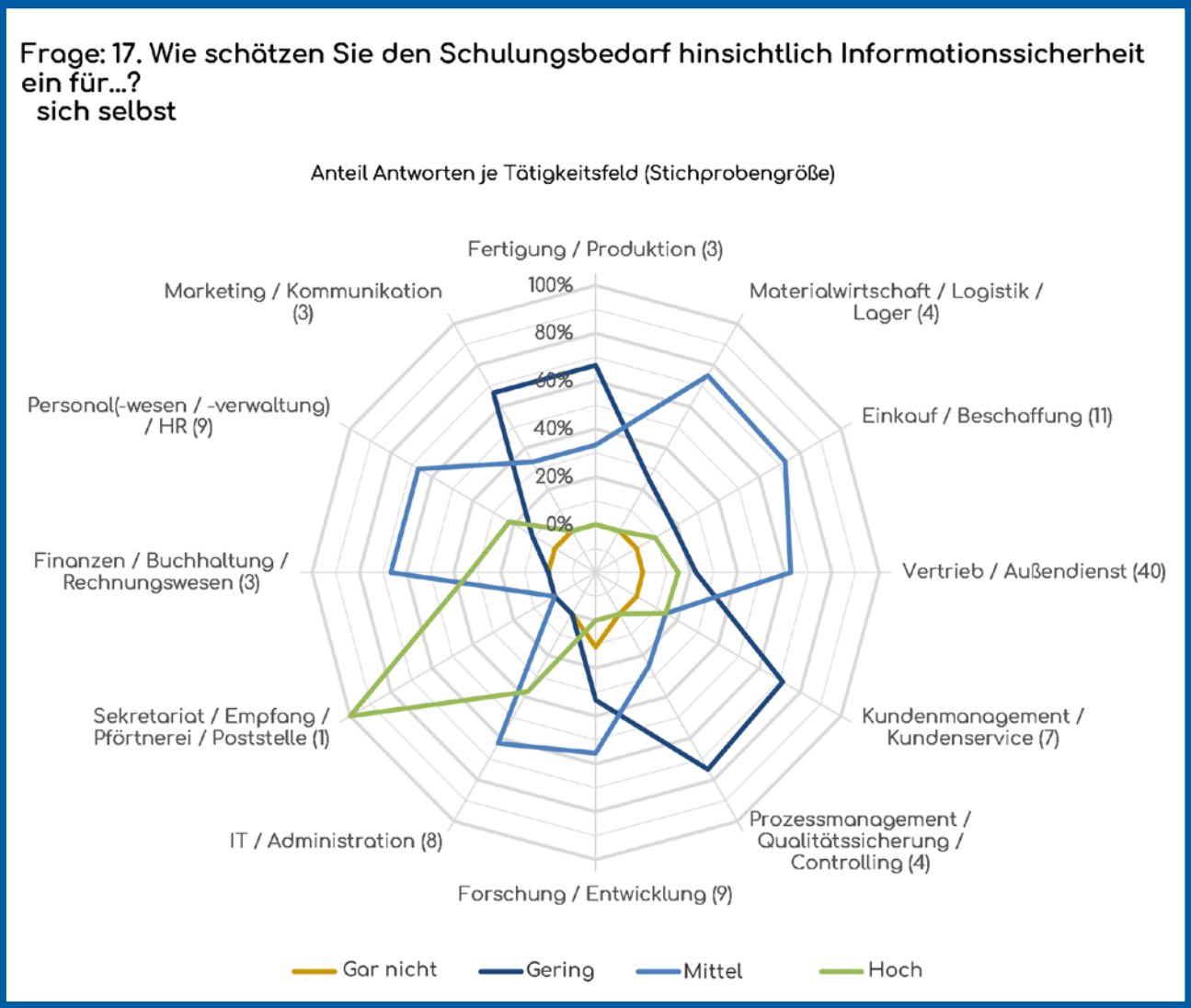


Abb. 28: *Schulungsbedarf für „sich selbst“ nach Tätigkeitsfeldern (Fragekomplex 17)*

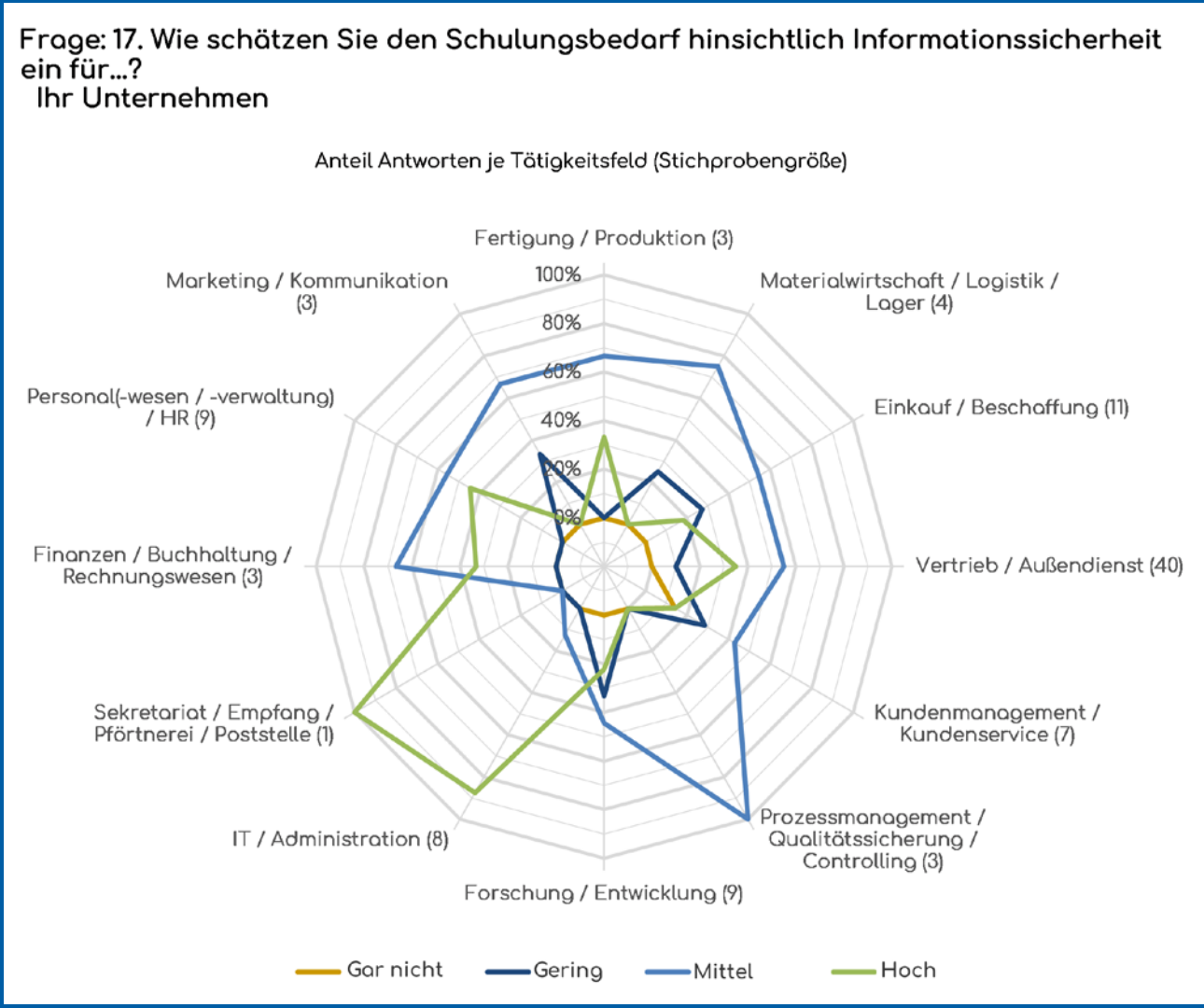


Abb. 29: *Schulungsbedarf für „Ihr Unternehmen" nach Tätigkeitsfeldern (Fragekomplex 17)*

Für das Unternehmen wird der Schulungsbedarf durch die Tätigkeitsbereiche meist als „Mittel“ eingeschätzt, zwischen 50% und 100% (siehe Abbildung 29) und bestätigt sich auch aus Perspektive der Personengruppen (siehe Abbildung 31). Diese Erkenntnis ist als Motivation zum Handeln und Verändern zu verstehen, um die Kompetenz der Mitarbeitenden im Bereich IS in den Unternehmen zu erhöhen und die Mitarbeitenden zu sensibilisieren.

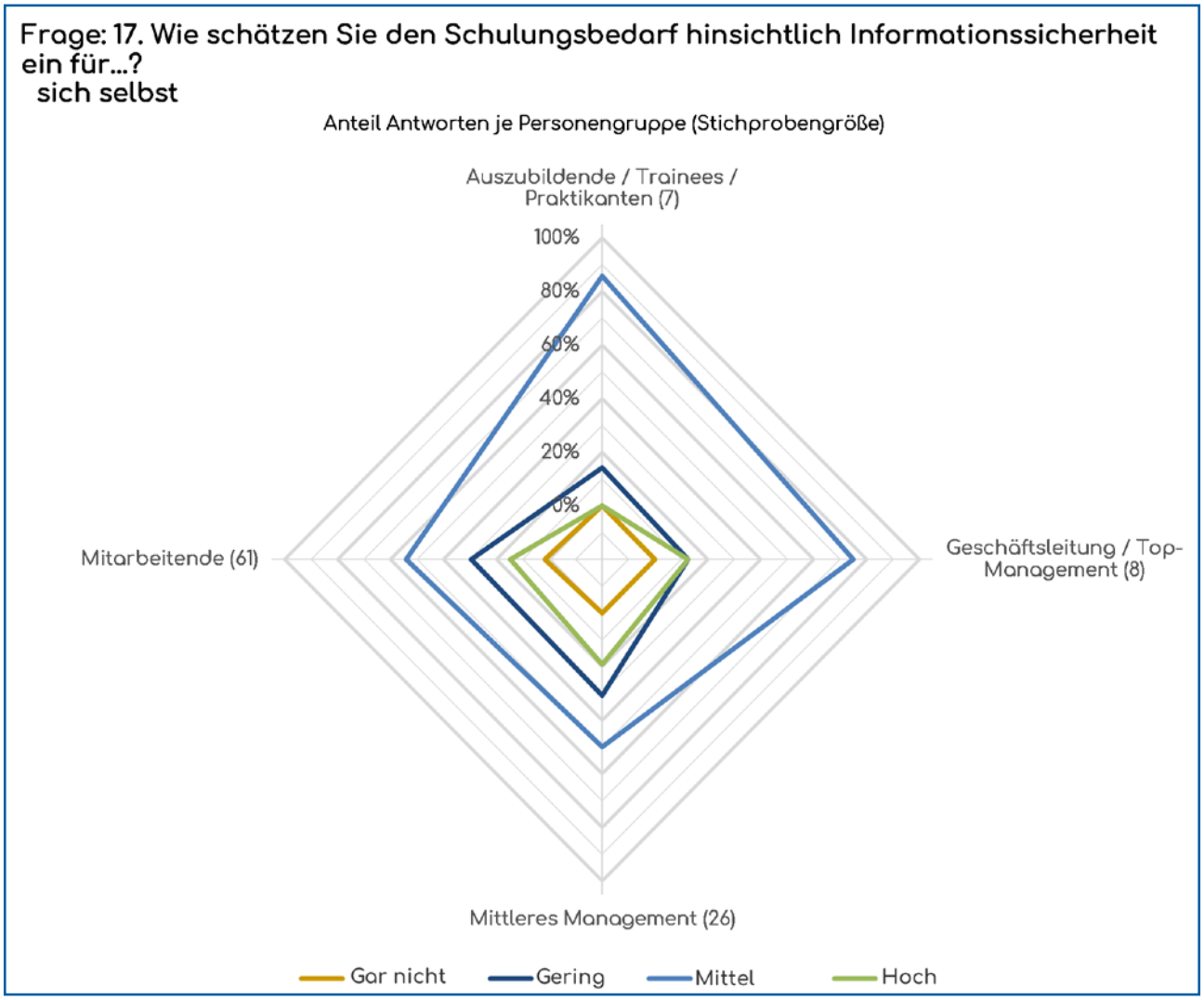


Abb. 30: *Schulungsbedarf für „sich selbst“ nach Personengruppen (Fragekomplex 17)*

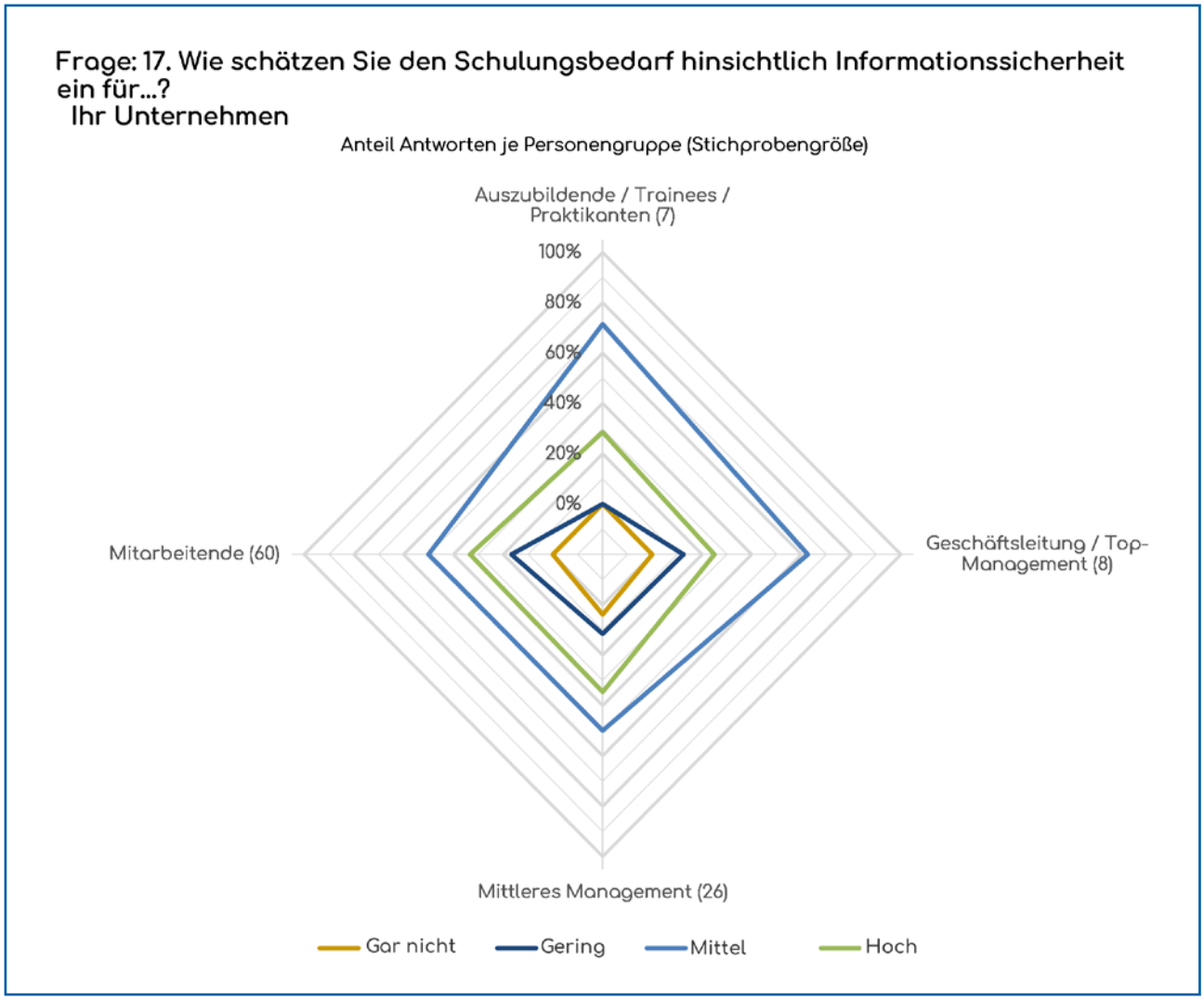


Abb. 31*: Schulungsbedarf für „Ihr Unternehmen“ nach Personengruppen (Fragekomplex 17)*

4.3 Informationssicherheitsrelevante Tätigkeitsfelder in KMU – Bildung gemeinsamer Tätigkeitsprofile

Während in den vorherigen Abschnitten ausgiebig Datenmaterial hervorgebracht wurde, das die Wichtigkeit der Informationssicherheit in KMU stützt, sollen im Folgenden die ersten Versuche skizziert werden, anhand einer Analyse von Streudiagrammen auf hochaggregierter Datenbasis, der Identifikation einzelner Korrelationspaare und qualitativer Überlegungen in den daraus formierten Gruppen Gemeinsamkeiten zu finden und erste Charakteristika einzelner Profilgruppen zu definieren. Lassen sich diese formieren, so böten sie für angepasste Maßnahmen eine adäquate Einstiegsstufe zur effizienten Personalentwicklung. Für die Analyse wurden die Variablen und Parameter wie folgt definiert (siehe Abbildung 32):

DEFINITION DER BASIS-INFO

- T(i) Tätigkeitsfeld (alternativ hierarchische Personengruppe G(i))
- N(i) Probanden und Probandinnen (Grundgesamtheit), die aus T(i) geantwortet haben, durch Filter bereinigt (ohne Testaufrufe, Abbrüche etc.)
- F(j): j.te Frage, j=1,...74 (bei T(i) ist F(1)=Personengruppe, bei G(i) ist F(1) = Tätigkeitsfeld)
- NF(j): Anzahl der auswählbaren Antworten der Frage j, je eine Auswahlmöglichkeit
- SF(j): = {Stufen für die Frage F(j)}. Beispiel: nie, selten, häufiger, immer
- s(k,j) εSF(j): z.B. „nie“, Stufe k. k = 1,..., NF(j)
- P(i,k,j) Prozentzahl (Gesamt: N(i)) der Probanden aus Tätigkeitsfeld i, die die k.te Antwort zur Frage j angekreuzt haben
- N(i,k,j) Anzahl der Ankreuzungen aus dem i.ten Tätigkeitsfeld, auf Stufe k, der j.ten Frage
- Ch(N(i,j)) = f(N(i,k,j)), Charakteristika: Mittelwert, Median, Streumaße u.s.w anhand von N(i,k,j) genommen über alle k

Abb. 32: *Definition der Basis-Info*

4.3.1 Erstellung einer Korrelationsmatrix zur Identifikation von Tätigkeitsfelder-Paaren

Im ersten Schritt wurde der Frage nachgegangen, welche Beziehung unter den Tätigkeitsfeldern besteht, in diesem Fall welche Paare mit extrem starker oder schwacher Korrelation gebildet werden können. Es wird die Korrelation nach Pearson (siehe [23]) beschrieben. Eine Rangkorrelation nach Spearman wurde ebenfalls untersucht, wich aber in den Erkenntnissen im Gesamtbild nicht entscheidend ab. Die Pearson-Korrelation (z. B. Korr(W(i1)), W(i2) zweier Tätigkeitsfelder wurde über 74 Fragen (ein 74-Tupel W(i) = [Ch(N(i,1), N(i,2), …)]) berechnet. Über die zwölf beantworteten Tätigkeitsfelder (drei blieben unbeantwortet) wurde eine Matrix mit je elf Pärchen gebildet (siehe Abbildung 33 für die Gesamtstichprobe, unten links, und zum Vergleich dessen Teilmenge der Pilotunternehmen (Umfrage 101), oben rechts).

Die Berechnung der Korrelation ist aber schwierig zur Gruppenbildung verwendbar (siehe [24]), daher soll sie hier nur zur Paarbildung in den Fokus gerückt werden. Nutzen war dennoch über die direkte Beziehung hinaus die Erstellung einer „affinen Folge“, die in den Tätigkeitsfeld-Detailgrafiken der Fragen meist durch stark korrelierende „Nachbarpärchen“ homogenere Bildverläufe erzeugte und Zusammenhänge in den Grafiken leichter ablesbar und Gemeinsamkeiten leichter sichtbar machte.

Wird nun für ein bestimmtes Tätigkeitsfeld ein Streudiagramm erstellt, in dem die zwei stärksten und ein schwacher Korrelationspartner eingefügt werden, zeigt sich eine zusätzliche Information: wie nah bzw. fern die verglichenen Tätigkeitsfelder mit den gleichmäßigen Stufen des ausgerichteten Tätigkeitsfeldes gleichlaufen oder abweichen (siehe Abbildung 34). Auf die Streudiagramme wird im folgenden Kapitel näher eingegangen.

SIGNIFIKANZNIVEAU:

Es wurden Signifikanzniveaus bei $\alpha < 0{,}05$ für ein signifikantes, und bei $\alpha < 0{,}01$ für ein sehr signifikantes Ergebnis herangezogen [25]. Die kritischen Werte lagen bei Schwellwert $r>=0{,}30$ für sehr signifikante Korrelationswerte (rote Färbung in der Matrix) und bei Schwellwert $r>=0{,}23$ für signifikante Korrelationswerte (schwarze Färbung, nicht signifikante Werte in grauer Färbung). Da aber die herangezogenen Fragen zum einen mit hoher Wahrscheinlichkeit nicht unabhängig voneinander sind und es sich zum anderen um hochaggregierte Daten handelt, deren Wertebasis zudem aufgrund der geringen Zahl der Teilnehmenden nicht durchgängig als besonders groß angesehen werden kann, muss dieser Bewertung kritisch gegenüber gestanden werden. Es handelt sich daher vermutlich nicht um statistische Korrelation und Signifikanz im engeren Sinne.

Korrelationsmatrix Mittelwert Korrelation r=0,55 (Gesamtstichprobe) Signifikanzniveaus und Schwellwerte für r über n=74 Mediane bei α < 0,01 sehr signifikant r>=0,30 (rote Färbung) bei α < 0,05 signifikant r>=0,23 (schwarze Färbung) niedrigere Werte (graue Färbung)	Sekretariat / Empfang / Pförtnerei / Poststelle	Einkauf / Beschaffung	Materialwirtschaft / Logistik / Lager	Fertigung / Produktion	Forschung / Entwicklung	Marketing / Kommunikation	Vertrieb / Außendienst	Kundenmanagement / Kundenservice	Personal(-wesen / -verwaltung) / HR	Finanzen / Buchhaltung / Rechnungswesen	IT / Administration	Prozessmanagement / Qualitätssicherung / Controlling
Sekretariat / Empfang / Pförtnerei / Poststelle		0,35	0,38	0,29	0,20	0,39	0,34	0,25	0,37	0,56	0,28	0,21
Einkauf / Beschaffung	0,35		0,82	0,70	0,60	0,46	0,91	0,65	0,62	0,54	0,73	0,59
Materialwirtschaft / Logistik / Lager	0,38	0,82		0,75	0,62	0,47	0,81	0,63	0,63	0,51	0,72	0,56
Fertigung / Produktion	0,29	0,70	0,75		0,70	0,40	0,71	0,59	0,53	0,44	0,65	0,64
Forschung / Entwicklung	0,11	0,57	0,57	0,54		0,30	0,64	0,64	0,40	0,49	0,67	0,47
Marketing / Kommunikation	0,20	0,31	0,36	0,28	0,34		0,45	0,53	0,68	0,58	0,46	0,26
Vertrieb / Außendienst	0,34	0,91	0,81	0,71	0,60	0,31		0,71	0,63	0,53	0,76	0,63
Kundenmanagement / Kundenservice	0,41	0,67	0,68	0,64	0,60	0,54	0,72		0,68	0,53	0,74	0,52
Personal(-wesen / -verwaltung) / HR	0,37	0,62	0,63	0,53	0,43	0,51	0,63	0,72		0,58	0,59	0,42
Finanzen / Buchhaltung / Rechnungswesen	0,56	0,54	0,51	0,44	0,42	0,45	0,53	0,64	0,58		0,59	0,38
IT / Administration	0,28	0,71	0,65	0,60	0,65	0,48	0,73	0,78	0,60	0,62		0,58
Prozessmanagement / Qualitätssicherung / Controlling	0,29	0,67	0,65	0,60	0,58	0,48	0,68	0,80	0,56	0,61	0,69	

Gesamtstichprobe

Teilstichprobe Pilotunternehmen

Abb. 33: *Korrelationspaare zwischen den Tätigkeitsfeldern (basierend auf Aggregatdaten: Mediane)*

4.3.2 Charakteristika der Tätigkeitsfelder und Personengruppen

Die bisher erbrachte Darstellung der Umfrageergebnisse folgte bereits einem Schema, in dem von „Nie“, dann „Selten“ über „Häufiger“ zu „Immer“ die Antworten aller Teilnehmenden in Rangfolge gebracht und deskriptiv vorgestellt wurden. Diese Idee folgte aus dem Versuch heraus, die Korrelation zu visualisieren — ein grafischer Ansatz mit Hilfe von Streudiagrammen, die eigens hierfür entwickelt und in denen zuerst nur die Antworten (N(i)) aus einem einzigen Tätigkeitsfeld (T(i)) betrachtet wurden (siehe grüne Punkte in Abbildung 34). Unmittelbar auf der Ordinate (Y-Achse) wurde das Ergebnis aus dem Median (Ch(N(i,1))) der zweiten Frage der Umfrage zur Personengruppe (F(1)) in den vier aufsteigenden, in diesem besonderen Fall alternativen Antwort-Stufen (SF(1)) Auszubildende / Trainees / Praktikantinnen / Praktikanten, Mitarbeitende, Mittleres Management und Geschäftsleitung / Topmanagement als großer Punkt dargestellt.

In der Haupt-Y-Achsenbeschriftung wurden aufsteigend von „Nie“ nach „Immer“ die vier bereits genannten Häufigkeits-Stufen (SF(j>1)) verzeichnet. Abweichende Stufenbezeichnungen bei der Häufigkeit von Schulungen von „Nie“ nach „Regelmäßig“ und bei Schulungsbedarf von „Gar nicht“ nach „Hoch“ wurden in der Achsenbenennung vernachlässigt. Auf der Abszisse (X-Achse) wurden die Schlagwörter der restlichen 73 Fragen (F(j>1)) und folglich ein 73-Tupel (W(i) = [Ch(N(i,2), N(i,3), …)]) in Rangfolge gebracht. Dieses Ranking (Sk(W(i))) basiert auf den Werten der Antwort-Mediane (CH(N(i,j>1))) und nachrangig der zugehörigen Mittelwerte. Nutzt man nur die Mittelwerte ergibt sich ein leicht verändertes, aber feinstufigeres Bild (siehe Abbildung 35 mit Medianen und Abbildung 36 nur mit Mittelwerten). Im Folgenden wurden die Antwort-Mediane (CH(N(i,j>1))) als große, grüne Punkte in das beschriebene Koordinatensystem eingetragen. Da nun sowohl auf Ordinate als auch auf Abszisse vom Ursprung nach oben, bzw. nach rechts, eine Folge mit zunehmender Häufigkeit entstand, steigen die in Rangfolge gebrachten Mittelwerte über vier Stufen monoton an (siehe grüne Punkte in Abbildung 34). Es lässt sich auf der X-Achse zum Ursprung hin nun ablesen, womit die Teilnehmenden selten oder nie im Job zu tun haben und in die andere Richtung, was sie häufiger oder immer nutzen. Dieses auf ein Tätigkeitsfeld (T(i)) bezogene Koordinatensystem gibt zusammengefasst über Folgendes Aufschluss: den Median der Personengruppenzugehörigkeit, die spezifische Rangfolge der Fragethemen, welche durch die Häufigkeit der Nutzung / des Vorkommens aus den Antworten bestimmt ist, und die zugehörigen Stufenwerte der Antwort-Median / -Mittelwerte.

Entsprechend des ursprünglichen Ziels, die Korrelation zu anderen Tätigkeitsfeldern zu visualisieren, wurden neben dem untersuchten Tätigkeitsfeld (Vergleichsobjekt) auch noch die anderen Tätigkeitsfelder eingetragen (schwarze Punkte) und besonders starke oder schwache Korrelation durch Kästchen hervorgehoben (siehe Abbildung 36 das Beispiel Marketing: stark korrelierende Tätigkeitsfelder Kundenmanagement und Personalwesen werden durch blaue und dunkelblaue Kästchen gekennzeichnet, das gering korrelierende Tätigkeitsfeld Sekretariat durch orangene Kästchen).

Solche Streudiagramme wurden für zwölf beantwortete Tätigkeitsfelder und die vier hierarchischen Personengruppen erstellt. Die Streudiagramme nutzen zum einen hochaggregierte Lagemaße, zum anderen visualisieren sie die einzelnen Frageergebnisse. Aufgrund der Anzahl und Komplexität sprengt deren Darstellung den Rahmen dieses Berichts. Daher sollen im Folgenden nur Besonderheiten der vergleichenden Auswertung der Streudiagramme (als Beispiel siehe Markierung durch blaue Rahmen in Abbildung 36) als Beschreibung ergänzt werden. Fiel beispielsweise ein Mittelwert eines Tätigkeitsfelds im Vergleichsfeld durch eine extreme Randposition auf, also einem vergleichsweise niedrigen oder hohen Wert (vgl. blaue Rahmen in den Streudiagrammen), wird dieser besonders angesprochen.

Diese Streudiagramme geben zwar genauso wenig wie die Korrelationsanalyse quantitativ fundierte Rückschlüsse auf eine Gruppenzusammengehörigkeit, liefern aber zum einen eine Art „DNA“ (einzigartig zusammengesetzter, genetischer Bauplan), anhand der man ein Tätigkeitsfeld im Blick auf die Vielzahl der Fragen charakterisieren kann, und zum anderen lassen sich doch Verwandtschaften schnell erkennen oder verwerfen. Starke Korrelationen können veranschaulicht werden und deuten darauf hin, dass eine Clusteranalyse [26] oder eine Hinzunahme von Modellen wie partieller Ordnungen (z.B. Hasse-Diagramme) [27] größere Gruppenzusammenhänge nachweisen könnten. Mögliche mathematische Modelle werden als passende Messmethode dieser Zusammenhänge von sudile, einem Unterauftragnehmer des Projektes, derzeit getestet und auf ihre Eignung untersucht.

Die folgenden Ergebnisse (Kapitel 4.3.3–4.3.5) beschreiben die Mediane der Antworten zu den 73 Fragen. Bei den zwölf Tätigkeitsfeldern werden aufgrund des größeren Vergleichsfelds Besonderheiten unter Zuhilfenahme des Mittelwerts bestimmt. Bei den vier hierarchischen Personengruppen ist es hingegen einfacher, bereits am Median Alleinstellungsmerkmale hervorzuheben. Zudem werden das niedrigste Ergebnis und höchste Ergebnis im Ranking zwischen „Nie“ und „Immer“ speziell herausgestellt. Da Biometrie fast immer den niedrigsten Rang einnimmt, wird diese durch die Nennung des nächsten Rangs ergänzt, ebenso falls es Abweichungen zwischen dem Ranking basierend auf Median und Mittelwert gab.

VERWENDUNG VON MEDIANEN UND MITTELWERTEN IN DEN STREUDIAGRAMMEN:

Der Median wurde als bevorzugtes Lagemaß gewählt, da in der Umfrage einzelne Tätigkeitsfelder nur wenige Antworten erhielten und auch die Grundgesamtheit relativ klein war. Es war also eine Robustheit gegen Ausreißer vorrangig. Für ein einheitliches Bild war dieser von Vorteil, wenn man einen klaren Überblick über die Verteilung bzw. Charakteristik des Antwortverhaltens des Tätigkeitsfelds geben wollte. Jedoch war das Ergebnis im großen Vergleichsfeld schlechter differenzierbar, da sich seltener Bruchteilswerte ergaben und Werte übereinander lagen. Daher wurde in der vergleichenden Analyse mit Blick auf markante Züge zu Lasten der Robustheit wiederum der Mittelwert bevorzugt. Die jeweiligen Streudiagramme wiesen daher je nach Lagemaß geringfügig abweichende Fragen-Rankings und Verteilungen auf die vier Antwortstufen auf.

Lag ein Median im Streudiagramm zwischen zwei Kategorien, so wurde dieser in der folgenden Beschreibung der Vereinfachung halber abgerundet zugeordnet, dabei gilt:

Immer > Häufiger > Selten > Nie

AGGREGATDATEN UND ANTWORTVERTEILUNG:

Sofern Daten in dieser Form der Lagemaße hoch aggregiert analysiert werden, bleibt unberücksichtigt, ob die Ergebnisse innerhalb der Antwortstufen sich normal, gleichmäßig, auf gewissen Werten gehäuft oder gar polarisierend verteilen. Hierfür geben die bereits vorgestellten Detail-Balkengrafiken einen abermals höher aufgelösten Einblick oder ein Streumaß, wie die Standardabweichung oder Schärfe, das hinzugezogen werden könnte. Für einen strukturellen Überblick reichen die im Folgenden genutzten Streudiagramme jedoch aus.

ANMERKUNG ZUR DARSTELLUNG DER KORRELATION IN DEN STREUDIAGRAMMEN:

Die Datenpunkte sind hierbei zum einen farblich abweichend dargestellt, zum anderen nehmen sie mit der Korrelation in ihrer Größe ab, so dass bei übereinander liegenden Datenpunkten Kreise bzw. Randflächen entstehen.

Grüner Punkt = ausgerichtetes Tätigkeitsfeld

(Dunkel-)blaues Kästchen = starke Korrelation

Oranges Kästchen = schwache Korrelation

Schwarze Punkte = weiteres Vergleichsfeld

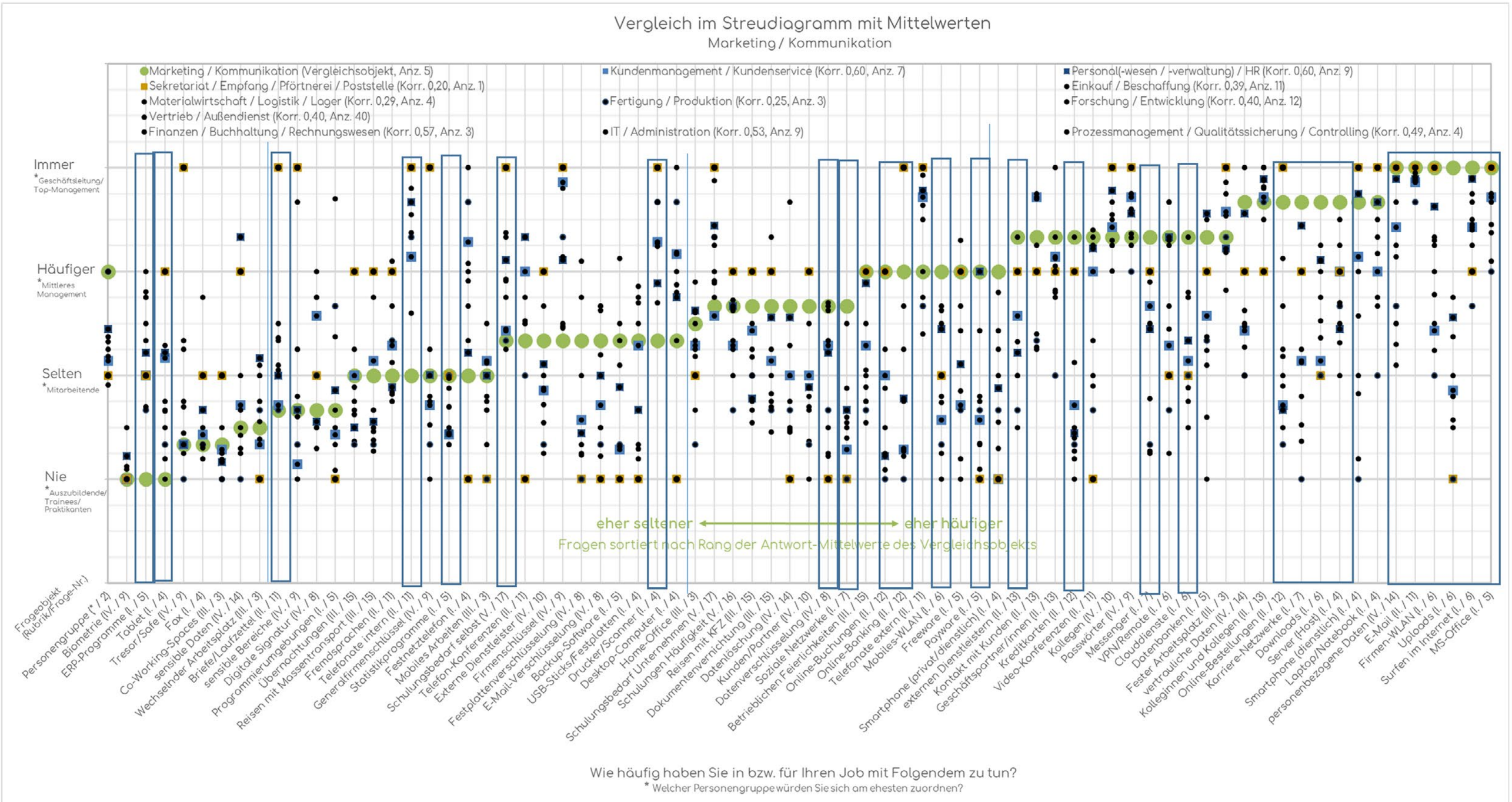


Abb. 34: *Volldarstellung Streudiagramm zum Tätigkeitsfeld „Marketing/Kommunikation". Unmittelbar auf der Ordinate (Y-Achse) finden sich die Ergebnisse der Gruppenzugehörigkeit. Die Ordinatenbeschriftung zeigt die vier Antwortstufen zur Nutzungshäufigkeit. Die Abszissenbeschriftung (X-Achse) ordnet zum Ursprung eher seltene und in die andere Richtung eher häufigere Nutzung entsprechend der Ergebnisse, wodurch die grünen Punkte monoton aufsteigen. Darstellung der Mittelwerte als Punkte und Kästchen: Große grüne Punkte zeigen das in Rang gebrachte Tätigkeitsfeld (Vergleichsobjekt), blaue/dunkelblaue Kästchen je ein damit stark korreliertes, orange Kästchen ein damit schwach korreliertes Tätigkeitsfeld, schwarze Punkte das restliche Vergleichsfeld. Markante Randpositionen des Vergleichsobjekts wurden mit blauen Rahmen gekennzeichnet.*

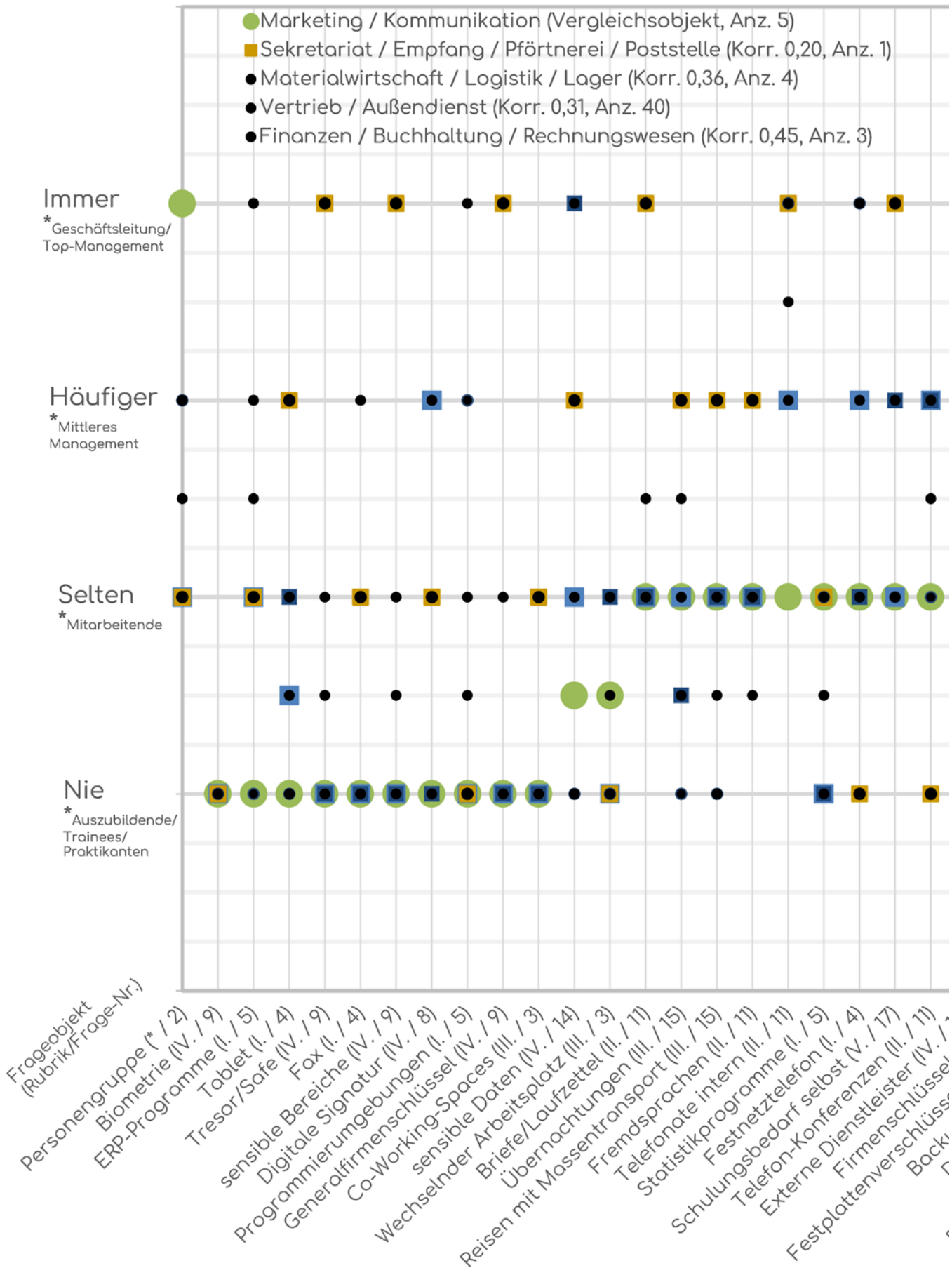


Abb. 35: *Ausschnitt aus dem Streudiagramm zum Tätigkeitsfeld „Marketing/Kommunikation“, klarere Stufen durch Darstellung der Mediane*

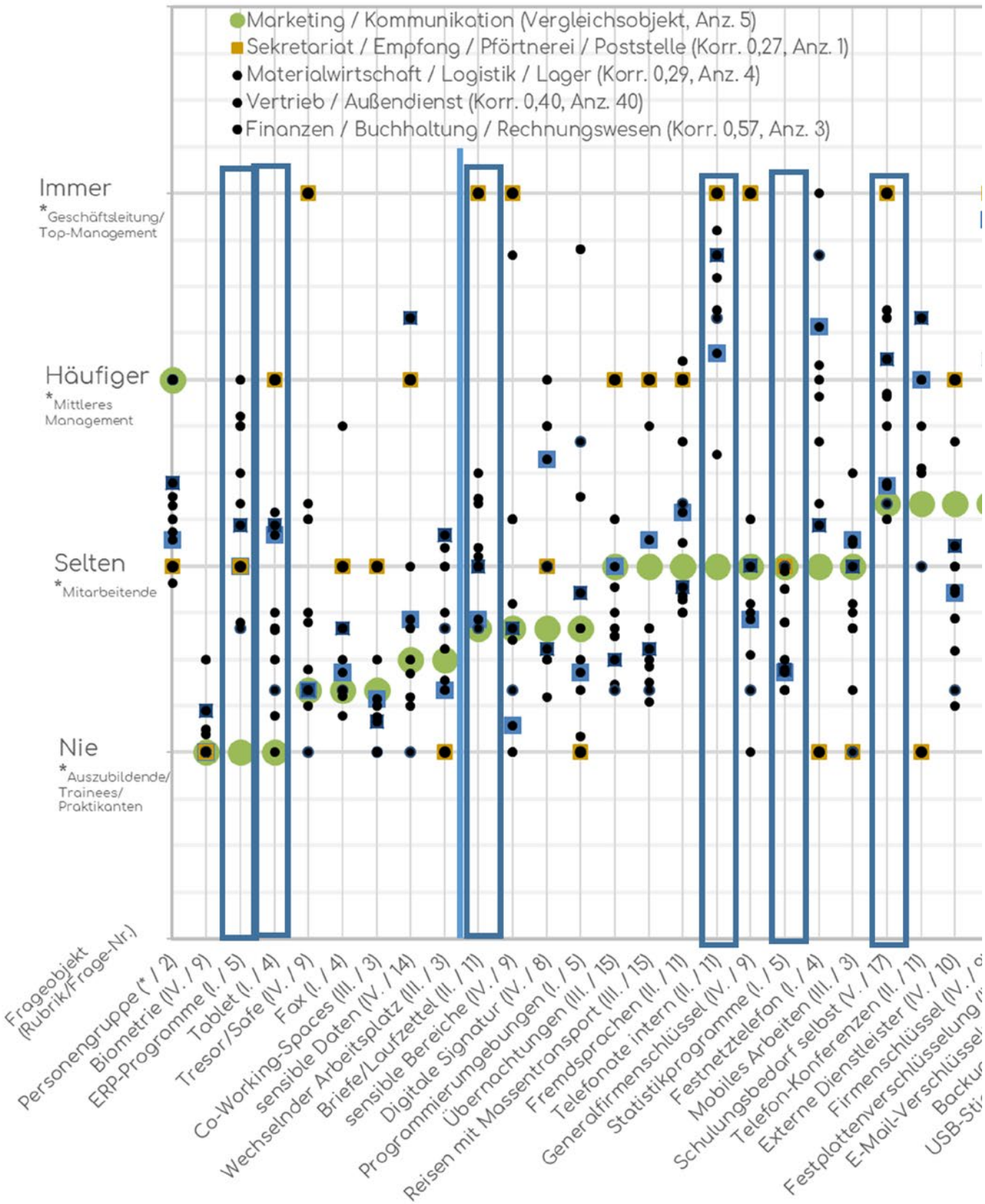
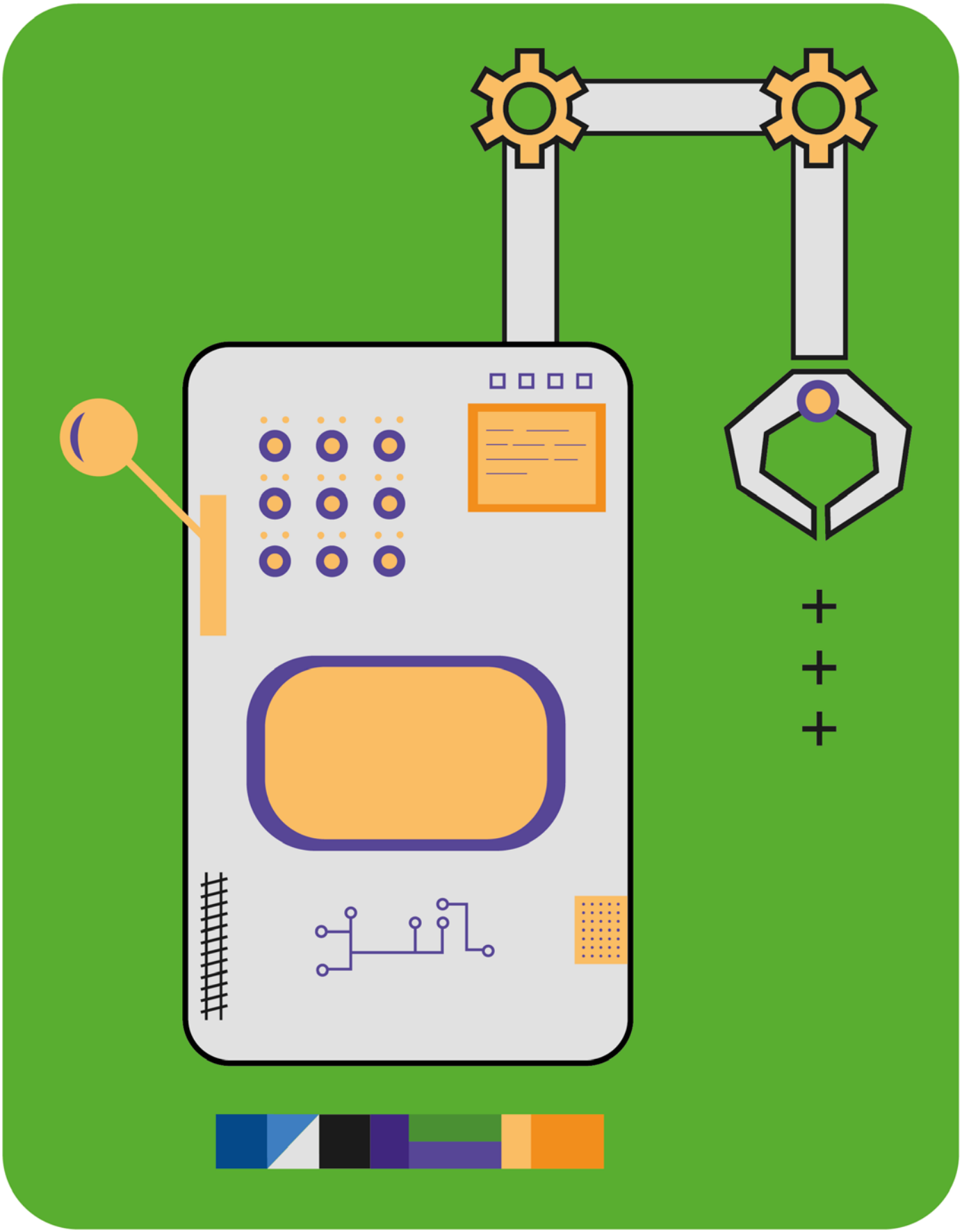


Abb. 36: *Ausschnitt aus dem Streudiagramm zum Tätigkeitsfeld „Marketing/Kommunikation“, dieses Mal Darstellung der Mittelwerte und Markierungen (blaue Rahmen) markanter Randpositionen zur Auswertung*

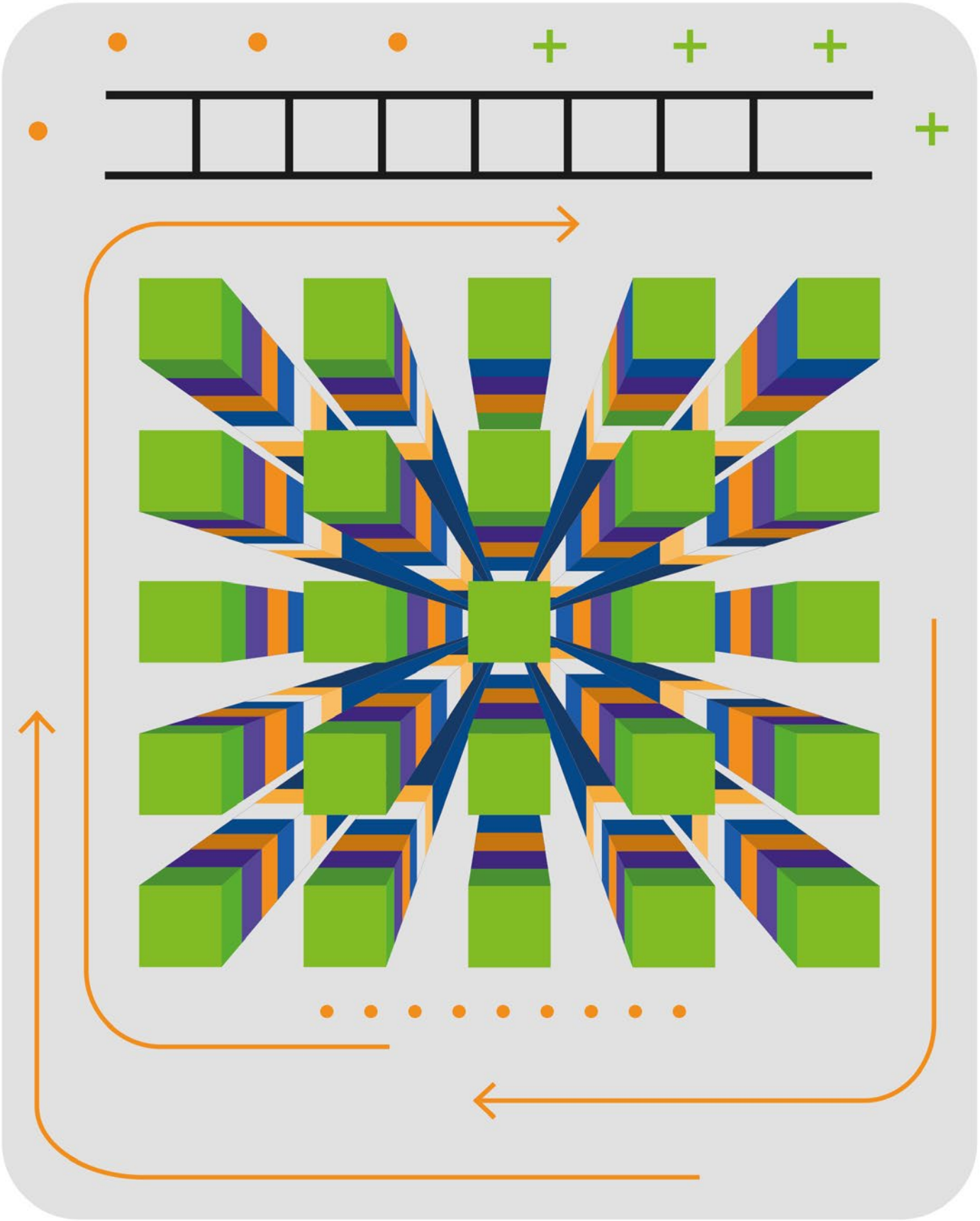


4.3.3 Vergleichsanalyse der Tätigkeitsfelder

Fertigung / Produktion
(kurz „Fertigung“)

Gruppengröße:	**3 Antwortende**
Personengruppe:	**Mittleres Management (Median)** (unerwartet, lässt vermuten, dass Personen unterhalb dieser Stufe möglicherweise nicht befragt wurden)
Antwortcharakteristik:	**36x „Nie“, 19x „Selten“, 10x „Häufiger“, 8x „Immer“**
Hohe Korrelation:	**Materialwirtschaft (0,75), Vertrieb (0,71)**
Niedrige Korrelation:	**Marketing (0,28)**

Insgesamt zeichnen die Antworten des Tätigkeitsfeldes ein sehr passendes Bild. Fertigung lieferte bei **„Nie“** im Vergleichsfeld die niedrigsten Antwortwerte bezüglich der Nutzung von sensiblen Daten, Online-Buchungen, Online-Banking, Biometrie, Tresor / Safe, Festplattenverschlüsselung, Sozialen Netzwerken, Karriere-Netzwerken, Uploads, Smartphones (dienstlich), Coworking-Spaces und mobilem Arbeiten. Ebenfalls auffällig war die extrem seltene Nutzung von Übernachtungen, Online-Bestellungen und Arbeit im Homeoffice. **„Seltener“** im Vergleich zu anderen Feldern wurde angegeben: die Teilnahme an Schulungen und Sensibilisierungsmaßnahmen zur Informationssicherheit, an betrieblichen Feierlichkeiten, Telefonkonferenzen, Nutzung des Firmen-WLANs oder eines Notebooks. Der Schulungsbedarf an sich selbst wurde ebenfalls relativ niedrig eingeschätzt. Zudem war der Umgang mit vertraulichen Daten verhältnismäßig selten im Vergleich zu den anderen Tätigkeitsfeldern. Mitarbeitende der Fertigung surfen weniger **„Häufig“** als Tätige anderer Felder im Internet. Zu **„Immer“** ist Folgendes bemerkenswert: sowohl die Nutzung von Festnetztelefonen als auch von Desktop-Computern. Auf dem niedrigsten Rang auf Stufe „Nie“ findet sich die Nutzung von sensiblen Daten. Auf der Stufe „Immer“ erscheint auf dem höchsten im Mittelwert der Desktop-Computer (verbunden damit: fester Arbeitsplatz im Median).



Materialwirtschaft / Logistik / Lager
(kurz „Materialwirtschaft“)

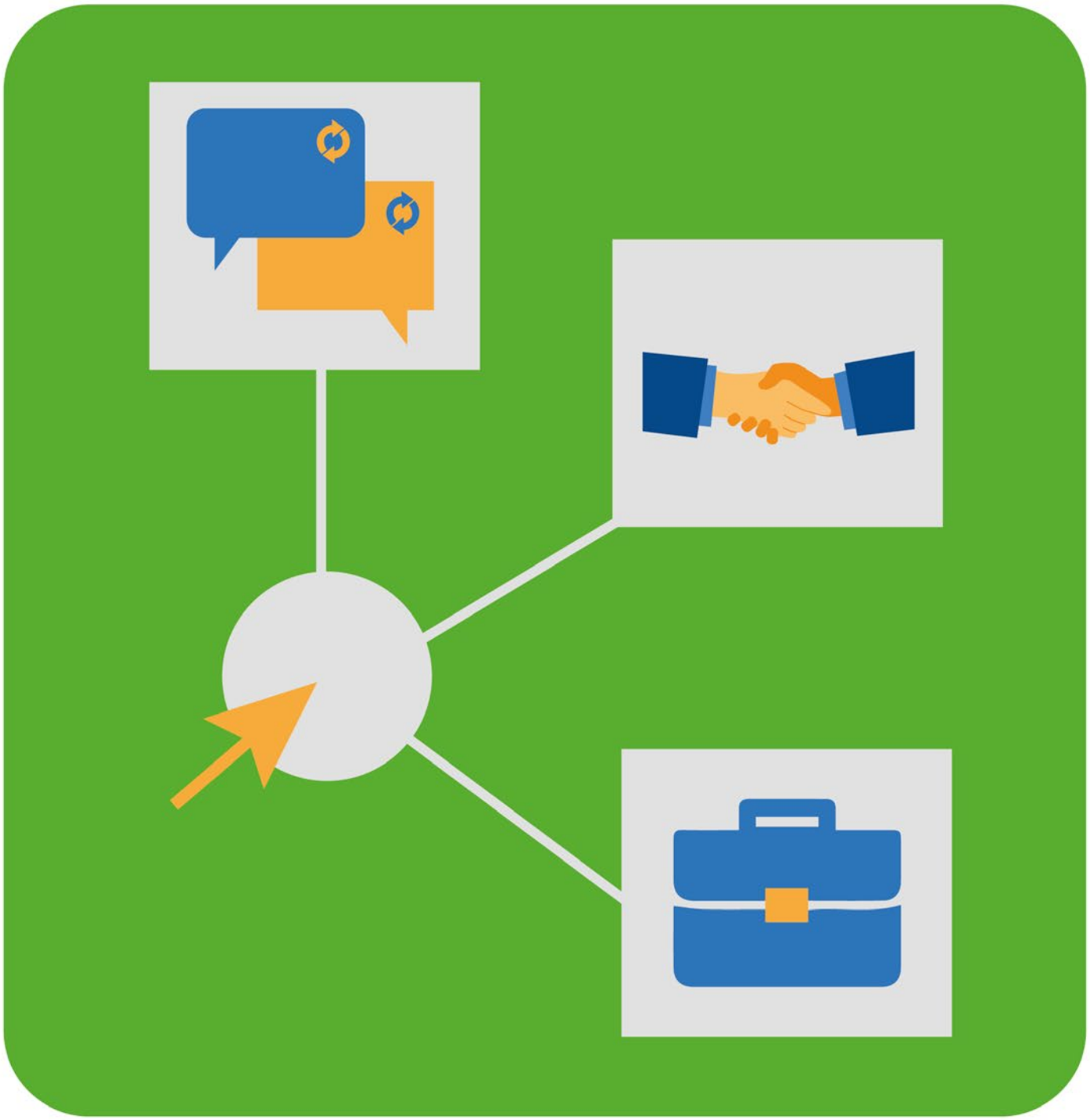
Gruppengröße:	**4 Antwortende**
Personengruppe:	**Mitarbeitende / Mittleres Management (Median)**
Antwortcharakteristik:	**40x „Nie“, 18x „Selten“, 8x „Häufiger“, 7x „Immer“**
Hohe Korrelation:	**Einkauf (0,82), Vertrieb (0,81)**
Niedrige Korrelation:	**Marketing (0,31)**

Materialwirtschaft gab bei **„Nie“** im Schnitt die meisten Antworten im Vergleichsfeld an und lieferte zudem die niedrigsten Antwortwerte bei Fragen zur Nutzung von Kreditkarten, Freeware, Datenbanken und VPN / Remote-Netzwerken. Ebenso gaben sie den geringsten Kontakt mit externen Dienstleistern an, die wie auch Kunden und Partner nie Zutritt zum Arbeitsplatz dieses Tätigkeitsfeldes haben. Bei folgenden Fragen wurde im Schnitt „Nie“ angegeben, während die meisten anderen Tätigkeitsfelder darüber lagen: Nutzung von Payware, Messenger, Statistikprogrammen, Uploads, Homeoffice oder Fremdsprachen. **„Seltener“** als in allen oder in den meisten anderen Feldern wird Folgendes genutzt: vertrauliche Daten, Downloads, Server und der Kontakt mit Kunden. Beinahe alle anderen Tätigkeitsfelder nutzen außerdem noch **häufiger** Laptops und Passwörter. Zu **„Immer“** ist bemerkenswert, dass sich der oberste Rang zu folgenden Themen geteilt wird: Kontakt zu Kolleginnen und Kollegen und Nutzung von internen Telefonaten sowie Druckern / Scannern. „Immer“ und somit im Schnitt an der Spitze des Vergleichsfelds und des spezifischen Rankings der Materialwirtschaft war die Nutzung von Desktop-Computern. Im Median lag, wie beim Tätigkeitsfeld Fertigung, der feste Arbeitsplatz auf dem höchsten Rang. Den niedrigsten Rang auf Stufe „Nie“ bekleidete die Nutzung der Kreditkarten.

Einkauf / Beschaffung
(kurz „Einkauf“)

Gruppengröße:	**11 Antwortende**
Personengruppe:	**Mittleres Management (Median)**
Antwortcharakteristik:	**38x „Nie“, 14x„Selten“, 10x „Häufiger“, 11x „Immer“**
Hohe Korrelation:	**Vertrieb (0,91), Materialwirtschaft (0,82)**
Niedrige Korrelation:	**Marketing (0,31)**

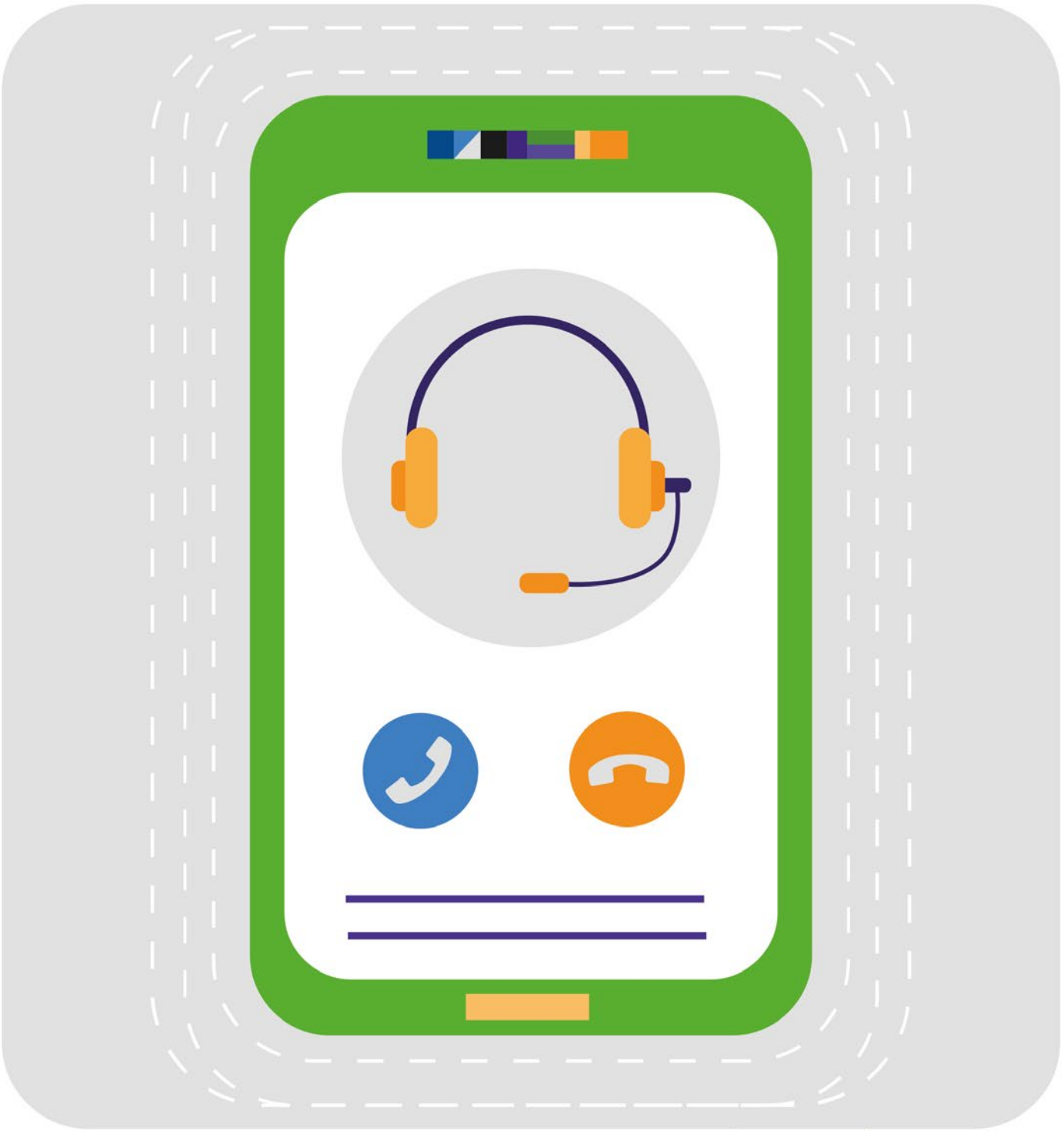
Die zum Tätigkeitsfeld Einkauf gehörende Gruppe gab **„Nie“** bei Folgendem an: Zutritt mit einem Generalfirmenschlüssel zu erhalten, mobiles WLAN, digitale Signatur, Clouddienste zu nutzen, betrieblichen Feierlichkeiten beizuwohnen, mit Bahn / Flugzeug / Schiff oder KFZ zu reisen oder an der Dokumentenvernichtung beteiligt zu sein. Bei **„Selten“** stach Folgendes heraus: die Nutzung von Datenbanken (andere meist häufiger), Telefonkonferenzen (andere meist häufiger), Kontakt mit Kundinnen und Kunden (andere häufiger). Bei **„Häufiger“** war besonders die im Vergleichsfeld häufigste Nutzung von ERP-Programmen auffällig. Zu Stufe **„Immer“** ist kaum etwas bemerkenswert. Den niedrigsten Rang auf Stufe „Nie“ bekleidet der Zugang zu sensiblen Personendaten und auf Stufe „Immer“ erreichte die Arbeit am Desktop-PC den höchsten Rang.



Vertrieb / Außendienst
(kurz „Vertrieb“)

Gruppengröße:	**40 Antwortende**
Personengruppe:	**Mitarbeitende (Median)**
Antwortcharakteristik:	**30x „Nie“, 19x „Selten“, 11x „Häufiger“, 13x „Immer“**
Hohe Korrelation:	**Einkauf (0,91), Materialwirtschaft (0,81)**
Niedrige Korrelation:	**Marketing (0,31)** (dieses überrascht, da die Felder meist eng zusammenarbeiten, ein Grund könnte in der unterschiedlichen Personengruppenzusammensetzung in der Stichprobe liegen)

Relativ niedrig mit **„Nie“** wurden bewertet: die Nutzung von Biometrie, Programmierumgebungen, Coworking-Spaces, Kreditkarten, Fax, Online-Banking und -Buchung. Bei **„Selten“** stach Folgendes heraus: der Einsatz von Fremdsprachen (andere meist häufiger) und Nutzung des Firmen-WLANs sowie der Server (fast alle anderen häufiger). Weniger **häufig** als andere erhält diese Tätigkeit den Zutritt mit Firmenschlüsseln. Das Homeoffice und ERP-Programme werden wiederum häufiger genutzt. Bei **„Immer“** ist der Kontakt zu Kundinnen und Kunden vergleichsweise sehr hoch ausgeprägt, was bei dieser Tätigkeit zu erwarten war. Auf dem niedrigsten Rang der Stufe „Nie“ steht Biometrie gefolgt von Programmierumgebungen und auf Stufe „Immer“ als höchster Rang im Mittelwert die Nutzung von E-Mail bzw. im Median der feste Arbeitsplatz.



Kundenmanagement / Kundenservice
(kurz „Kundenmanagement“)

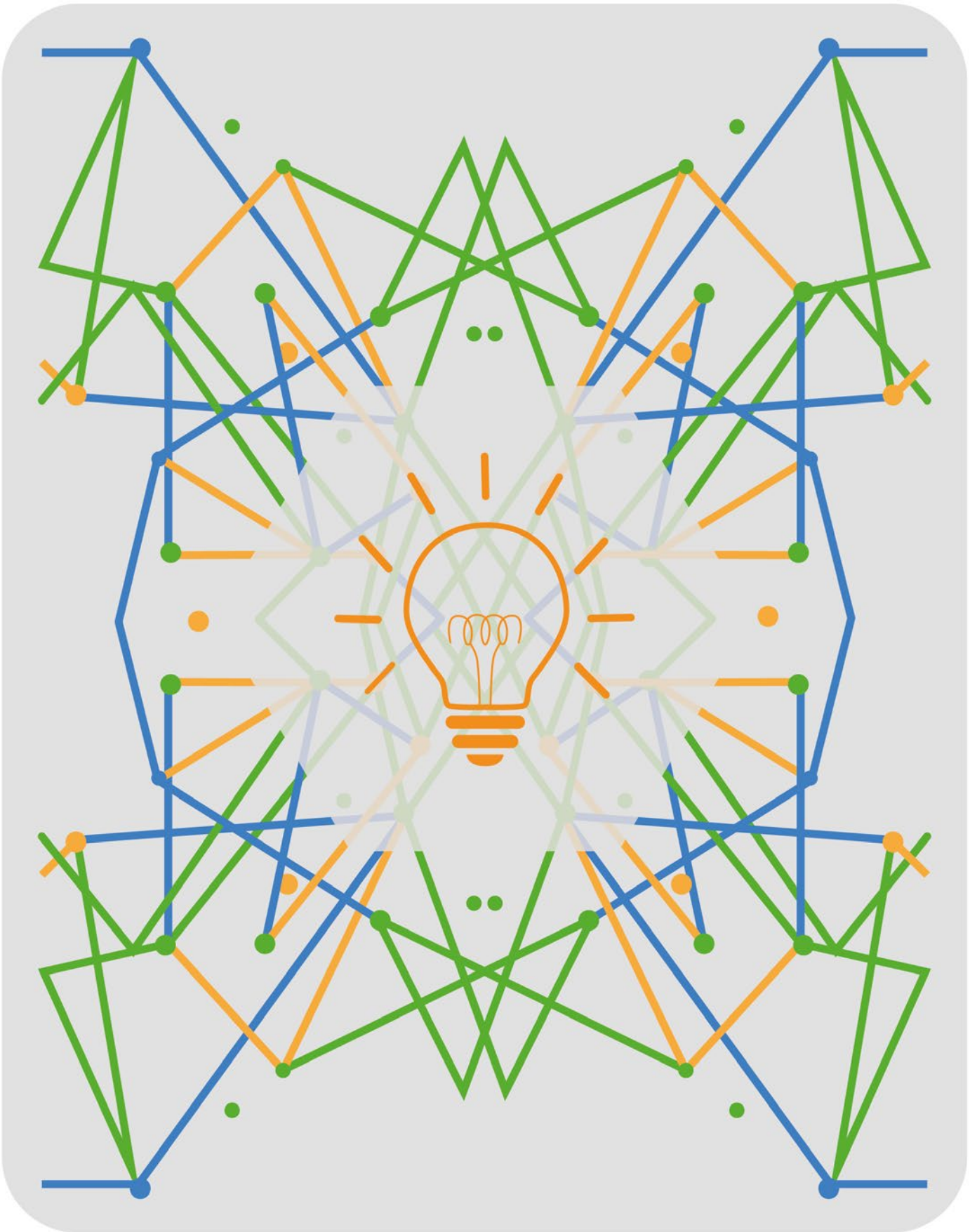
Gruppengröße:	**7 Antwortende**
Personengruppe:	**Mitarbeitende (Median)**
Antwortcharakteristik:	**16x „Nie“, 29x „Selten“, 14x „Häufiger“, 14x „Immer“**
Hohe Korrelation:	**Prozessmanagement (0,80), IT (0,78)**
Niedrige Korrelation:	**Sekretariat (0,41)**

Beim Kundenmanagement gab es auffällig geringe Mittelwerte im Bereich **„Nie“** bei der Nutzung von Folgendem: Biometrie, Smartphones (privat/dienstlich) und Statistikprogramme. Fast alle anderen Tätigkeitsfelder wiesen diesbezüglich einen höheren Mittelwert auf. **„Seltener“** als beinahe alle anderen Tätigkeitsfelder stach die Nutzung von Laufzetteln und Downloads heraus. Das Kundenmanagement schätzte den Schulungsbedarf im Unternehmen als **mittel** ein. Zu **„Immer“** sticht das Kundenmanagement naheliegenderweise durch seinen hohen Kundenkontakt heraus, wird aber überraschenderweise noch vom stark korrelierten „Prozessmanagement / Qualitätssicherung / Controlling“ übertroffen. Den niedrigsten Rang auf Stufe „Nie“ bekleidet, wie so oft, die Biometrie, aber eng gefolgt von Smartphone-Nutzung (privat / dienstlich). Auf der Stufe „Immer“ nimmt den höchsten Rang die Nutzung von Firmenschlüsseln ein (im Median ist der feste Arbeitsplatz knapp höher bewertet).

Prozessmanagement / Qualitätssicherung / Controlling (kurz „Prozessmanagement“)

Gruppengröße:	**4 Antwortende**
Personengruppe:	**Mittleres Management (Median)**
Antwortcharakteristik:	**12x „Nie“, 24x „Selten“, 19x „Häufiger“, 18x „Immer“**
Hohe Korrelation:	**Kundenmanagement (0,80), IT (0,69)**
Niedrige Korrelation:	**Sekretariat (0,29)**

Es fällt auf, dass das Prozessmanagement mit etwas Abstand bei den Fragen im Vergleichsfeld oft den zweithöchsten Mittelwert der Nutzung erreicht. Diese Personengruppe nutzt **„Nie“** Coworking-Spaces und Fremdsprachen, fast alle anderen Tätigkeitsfelder erzielten hier höhere Mittelwerte. Zudem liegt der Durchschnitt zur Nutzung von Biometrie auch bei „Nie“. **„Seltener“** als fast alle anderen Tätigkeitsfelder erfolgt die Nutzung von vertraulichen Daten. Trotz des seltenen Gebrauchs von Übernachtungen, Online-Buchungen, einem Generalsschlüssel, Briefen / Laufzetteln, Sozialen Netzwerken und Backup-Software ist dieser dennoch höher als bei den meisten anderen Feldern. Interessant ist, dass Prozessmanagement den Schulungsbedarf bei sich selbst am geringsten sah. **„Häufiger“** als alle anderen Gruppen wird Folgendes genutzt: E-Mail-Verschlüsselung, Datenverschlüsselung, Fax und Uploads sowie Reisen mit Bahn / Flugzeug / Schiff. Angaben zu **„Immer“** sind bemerkenswert dahingehend, dass viele Spitzenwerte erreicht wurden, wenn auch oft nur knapp oder auf geteiltem Platz. Im Kontakt zu Kundinnen und Kunden und auch zu Geschäftspartnerinnen und -partnern erreichte Prozessmanagement sogar den Höchstwert. Mit „Immer“ und gleichzeitig am häufigsten wurde die Nutzung des Festnetztelefons angegeben. Den niedrigsten Rang auf Stufe „Nie“ bekleidet im Mittelwert die Arbeit in Coworking-Spaces bzw. im Median die Nutzung sensibler Personendaten. Auf der Stufe „Immer“ erreicht der zum Untersuchungszeitraum noch in vielen Tätigkeitsfeldern weit verbreitete feste Arbeitsplatz den höchsten Rang.



Forschung / Entwicklung
(kurz „Forschung“)

Gruppengröße:	**12 Antwortende**
Personengruppe:	**Mitarbeitende (Median)**
Antwortcharakteristik:	**18x „Nie“, 28x „Selten“, 19x „Häufiger“, 8x „Immer“**
Hohe Korrelation:	**IT (0,65), Vertrieb (0,60), Kundenmanagement (0,60)**
Niedrige Korrelation:	**Sekretariat (0,11)**

Forschung gab bei **„Nie“** im Schnitt am seltensten an, ein Fax zu nutzen. Während andere Tätigkeitsfelder eine eher seltene Nutzung angaben, wurde in der Forschung im Schnitt fast nie ein dienstliches Smartphone genutzt. Obwohl die Inanspruchnahme eines Coworking-Spaces eher selten erfolgt, hat Forschung hier den höchsten Wert. Bei **„Selten“** stach Folgendes heraus: die seltenste Nutzung von personenbezogenen Daten und ebenso von externen Telefonaten. Interne Telefonate, feste Arbeitsplätze und die Nutzung von Druckern / Scannern und MS-Office Produkten kommen zwar **häufiger** vor, die meisten anderen Tätigkeitsfelder zeigen hier dennoch stärkere Tendenzen. Am häufigsten nutzt Forschung allerdings private / dienstliche Smartphones, das Homeoffice, digitale Signatur, Fremdsprachen, Festplattenverschlüsselungen und Downloads. Zu **„Immer“** ist Folgendes bemerkenswert: Die häufigste Nutzung von Freeware, Video-Konferenzen und Programmierumgebungen. Zwar immer, aber dennoch relativ gering ist der Kontakt zu Kolleginnen und Kollegen (fast alle anderen noch häufiger). Den niedrigsten Rang auf Stufe „Nie“ bekleidet abermals die Nutzung der Biometrie, dieses Mal gefolgt vom Fax. Auf Stufe „Immer“ bekleidet das Surfen im Internet den höchsten Rang. Forschung scheint mit Blick auf die Ergebnisse in vielerlei Hinsicht einen vom Rest losgelösten Eindruck zu machen, obwohl es z. B. im Vergleich zum Sekretariat (n=1) über eine größere Anzahl von Antwortenden (n=12) verfügt. Diese Einzelstellung wird durch das Fehlen eines starken Korrelationspartners bestätigt.

IT / Administration
(kurz „IT“)

Gruppengröße:	**9 Antwortende**
Personengruppe:	**Mitarbeitende (Median)**
Antwortcharakteristik:	**10x „Nie“, 29x „Selten“, 24x „Häufiger“, 10x „Immer“**
Hohe Korrelation:	**IT (0,65), Vertrieb (0,60), Kundenmanagement (0,60)**
Niedrige Korrelation:	**Sekretariat (0,11)**

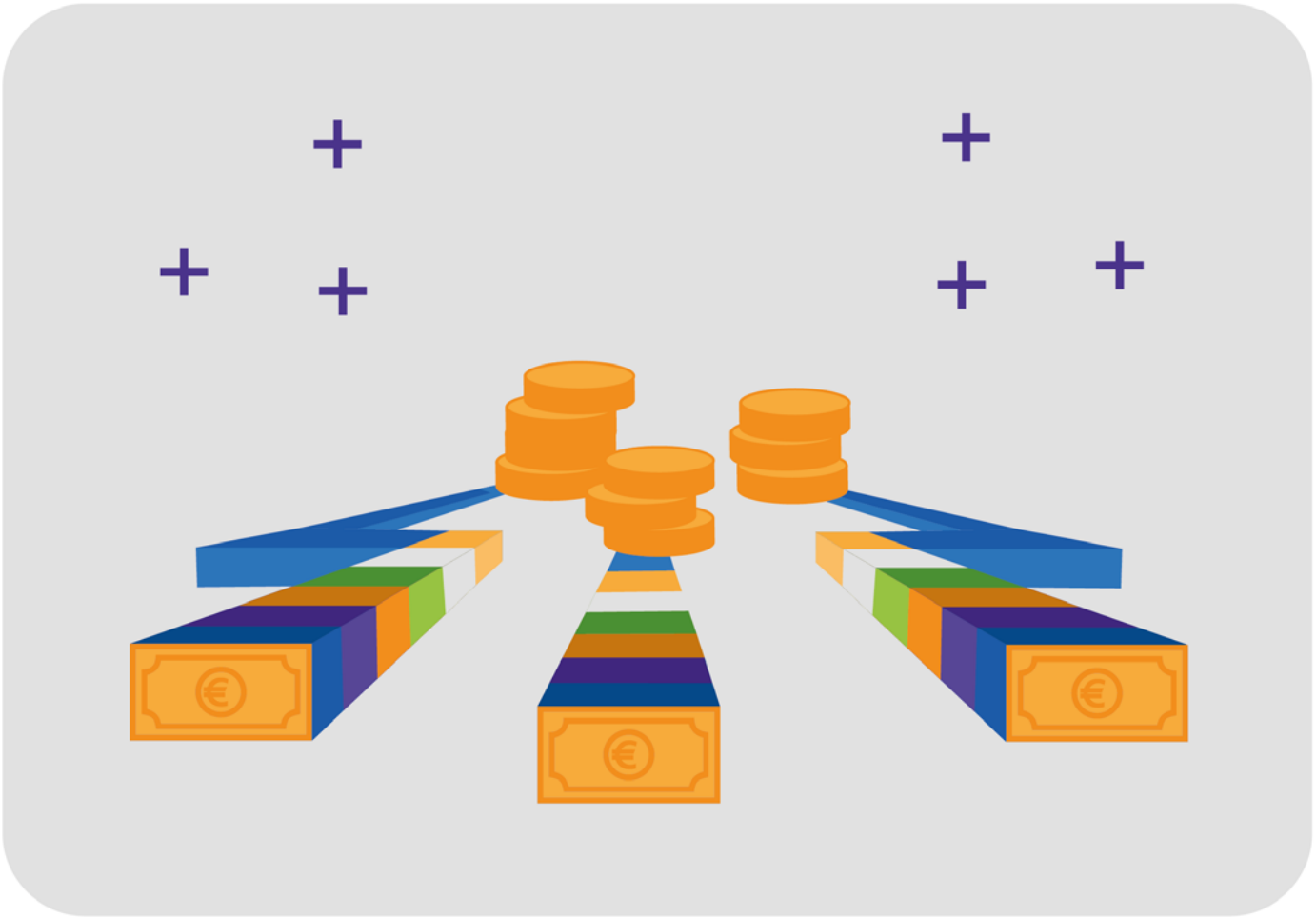
IT fällt durch sehr wenige Randpositionen auf allen Antwortstufen und ein hohes Nutzungsniveau auf. So ist bei **„Nie“** nichts Bemerkenswertes festzustellen. Gleichwohl IT **selten** Tablets oder Payware nutzt, geschieht dies in diesem Tätigkeitsfeld häufiger als in den anderen. Ebenfalls selten, aber im Vergleichsfeld am häufigsten, wird das mobile Arbeiten angegeben. **„Häufiger“** als beinahe alle anderen werden E-Mail-Verschlüsselung, Festplattenverschlüsselung und Downloads genutzt. Am häufigsten werden USB-Sticks und Backup-Software von der IT verwendet. Als Spitzenwert ist die Bereitstellung eines Servers (**„Immer“**) bemerkenswert. Die Angabe, immer am festen Arbeitsplatz zu arbeiten (fast alle anderen weniger häufig), zeigt im Vergleich zum hohen Wert bei mobilem Arbeiten den hybriden Charakter der IT, die sich um die Infrastruktur zu kümmern hat. Es ist keine Überraschung, dass der Schulungsbedarf bezüglich Informationssicherheit bei der IT mit „Hoch“ und fast am höchsten angegeben wurde. Den niedrigsten Rang auf Stufe „Nie“ nimmt die Biometrie, gefolgt von Arbeit in Coworking-Spaces ein und auf Stufe „Immer“ nimmt den höchsten die Nutzung von Laptop / Notebook ein.

Sekretariat / Empfang / Pförtnerei / Poststelle (kurz „Sekretariat“)

Gruppengröße:	**1 Antwort**
Personengruppe:	**Mitarbeitende**
Antwortcharakteristik:	**18x „Nie“, 10x „Selten“, 24x „Häufiger“, 21x „Immer“**
Hohe Korrelation:	**Finanzen (0,56), Kundenmanagement (0,41)**
Niedrige Korrelation:	**Forschung (0,11)**

Da nur eine Person aus dem Tätigkeitsfeld an der Umfrage teilgenommen hat, sind die Daten mit Vorsicht zu betrachten. Das Sekretariat gab bei **„Nie“** am seltensten Folgendes an: Beteiligung an der Datenlöschung, Video-Konferenzen oder Telefonkonferenzen, zudem Nutzung von E-Mail-Verschlüsselung, Datenverschlüsselung, USB-Sticks, privatem / dienstlichem Smartphone, Desktop-Computern oder wechselndem Arbeitsplatz. Die Person scheint **„Selten“** Coworking-Spaces zu nutzen, während alle anderen dieses aber noch seltener tun. Bei **„Häufiger“** nahm die eine Antwort in Folgendem die Spitzenposition im Vergleichsfeld ein: Schulungshäufigkeit, Übernachtungen, Reisen mit Bahn / Flugzeug / Schiff oder KFZ, Kontakt zu externen Dienstleistern, Zutritt zum Arbeitsplatz durch Kunden / Partner und Nutzung eines Tablets. Mit Kollegen und Kolleginnen kommt es zwar häufig, aber im Vergleich am seltensten zum Kontakt. Die Person sah sowohl für sich selbst als auch das Unternehmen im Vergleich den höchsten Schulungsbedarf mit „Hoch“. Zudem nahm die Angabe **„Immer“** in diesem einen Fall im Vergleichsfeld bei Folgendem den höchsten Wert an: Online-Bestellungen, Online-Banking, Briefe / Laufzettel, Zutritt zu sensiblen Bereichen oder dem Tresor / Safe. Wie aus den vorigen Antworten zu vermuten, arbeitet diese Person mit einem rein dienstlichen Smartphone und einem Laptop / Notebook. Den niedrigsten Rang auf Stufe „Nie“ bekleidet die Datenlöschung. Auf Stufe „Immer“ hat der feste Arbeitsplatz den höchsten Rang.

In diesem Einzelfall wurde vermutlich eine Assistenzstelle mit Zugriff auf sensible Bereiche, Reisetätigkeiten und gehobener technischer Ausstattung erfasst. Dieses wird nicht gleichsam auf alle Stellen in einem gemeinsamen Tätigkeitsfeld Sekretariat / Empfang / Pförtnerei / Poststelle zutreffen. Daher sollte dieses Tätigkeitsfeld überdacht werden und bei der Erstellung der Profile eine Trennung von abteilungsspezifischen und den stark kommunikativen Assistenztätigkeiten eines Sekretariats und den eher räumlich, physischen Aufgaben der Gruppe Empfang / Pförtnerei / Poststelle erfolgen. Eine neues Tätigkeitsfeld könnte mit Sekretariat / Assistenz umschrieben werden.



Finanzen / Buchhaltung / Rechnungswesen (kurz „Finanzen“)

Gruppengröße:	**3 Antwortende**
Personengruppe:	**Mittleres Management (Median)**
Antwortcharakteristik:	**10x „Nie“, 18x „Selten“, 26x „Häufiger“, 19x „Immer“**
Hohe Korrelation:	**Kundenmanagement (0,72), Vertrieb (0,63)**
Niedrige Korrelation:	**Forschung (0,42)**

Finanzen gab bei **„Nie“** die Nutzung von Statistikprogrammen mit am seltensten an (fast alle anderen weniger selten). Als besonders **selten** stach Folgendes heraus: die zweitseltenste Tätigung von Reisen mit dem KFZ und der relativ gesehen zweithäufigste Zutritt zum Tresor / Safe. **„Häufiger“** als bei den meisten anderen Feldern fand der Kontakt mit externen Dienstleistern sowie Zutritt durch externe Dienstleister zum Arbeitsplatz und durch Geschäftspartnerinnen und -partner bzw. Behörden, die Nutzung von E-Mail-Verschlüsselung, mobilem WLAN, Akten- und / oder Dokumentenvernichtung und Kreditkarten statt. Bei **„Immer“** erreicht das Tätigkeitsfeld im Vergleich besonders hohe Werte bei der Nutzung von Telefon-Konferenzen, Clouddiensten, Datenbanken, Datenlöschung (Höchstwert), Zutritt zu sensiblen Bereichen, Zugriff auf vertrauliche Daten (Höchstwert), Kontakt mit Kolleginnen und Kollegen, Nutzung von E-Mail, Zutritt per Generalfirmenschlüssel, Zutritt per Firmenschlüssel, Zugang per Passwort und Tätigkeit am festen Arbeitsplatz. Den niedrigsten Rang auf Stufe „Nie“ bekleidet Biometrie gefolgt von Coworking-Spaces und auf Stufe „Immer“ hat den höchsten Wert der „Feste Arbeitsplatz“.

Personal(-wesen / -verwaltung) / HR (kurz „Personal“)

Gruppengröße:	**9 Antwortende**
Personengruppe:	**Mitarbeitende (Median)**
Antwortcharakteristik:	**18x „Nie“, 19x „Selten“, 19x „Häufiger“, 17x „Immer“**
Hohe Korrelation:	**Kundenmanagement (0,72), Vertrieb (0,63)**
Niedrige Korrelation:	**Forschung (0,37)**

Personal bildet ein recht unauffälliges Profil im Mittelfeld, wobei im Bereich „Immer“ oft der Höchstwert hinter Sekretariat erreicht wird. Personal gab bei **„Nie“** aber im Schnitt trotzdem an zweithöchster Position im Testfeld die Nutzung von Biometrie an. Bei **„Selten“** stach der höchste Antwortwert im Vergleichsfeld bezüglich eines wechselnden Arbeitsplatzes heraus. Auffällig ist, dass dieses Profil **„Häufiger“** als bei anderen mit Payware in Kontakt kommt. Besonders hohe Werte von **„Immer“** wurden von den Teilnehmenden angegeben bei: Zugriff auf sensible Daten (Höchstwert), Nutzung von Telefon-Konferenzen, Karriere-Netzwerken, Datenbanken (Höchstwert), Firmen-WLAN, Laptops, dienstlichem Smartphone, Zutritt von Kolleginnen und Kollegen zum Arbeitsplatz sowie Zugriff auf personenbezogene Daten und die Nutzung von MS-Office. Den niedrigsten Rang auf Stufe „Nie“ bekleidet die Nutzung von Coworking-Spaces und auf Stufe „Immer“ den höchsten die Verwendung von Office-Software.

Marketing / Kommunikation
(kurz „Marketing“)

Gruppengröße:	**5 Antwortende**
Personengruppe:	**Geschäftsleitung / Top-Management (Median)**
Antwortcharakteristik:	**12x „Nie“, 20x „Selten“, 20x „Häufiger“, 20x „Immer“**
Hohe Korrelation:	**Kundenmanagement (0,54), Personal (0,51)**
Niedrige Korrelation:	**Sekretariat (0,20)**

Marketing gab bei **„Nie“** im Schnitt am seltensten die Nutzung von ERP-Programmen und Tablets an. Als **„Selten“** stachen heraus die Nutzung von Statistikprogrammen, Druckern / Scannern und eine relativ niedrige Einschätzung des Schulungsbedarfs bei sich selbst. Zwar „Selten“ aber noch immer häufiger im Schnitt wurde die Nutzung von Briefen/Laufzetteln und das Führen interner Telefonate angegeben. Bei besonders **„Häufig“** erscheint zudem die Nutzung von Datenverschlüsselung, Sozialen Netzwerken, Online-Buchungen, Online-Banking, mobilem WLAN (Höchstwert) und Payware. Zu **„Immer“** sind folgende im Vergleich hohe Werte bemerkenswert: der Kontakt zu externen Dienstleistern und die Nutzung von Kreditkarten, Messengern (Höchstwert), Clouddiensten, Online-Bestellungen, Karriere-Netzwerken, Downloads, Servern / Hosts, Uploads, Surfen im Internet, personenbezogenen Daten, E-Mail, Firmen-WLAN und Office-Software. Den niedrigsten Rang auf Stufe „Nie“ bekleidet Biometrie gefolgt von ERP-Programmen und auf Stufe „Immer“ den höchsten Rang die Verwendung von Office-Software.

Zwischenfazit Tätigkeitsfelder

Die Analyse der Antworten nach Tätigkeitsfeldern bestätigt in vielen Fällen Grundannahmen zu typischem Nutzungsverhalten, wie etwa die starke Nutzung von sensiblen personenbezogenen Daten durch die Gruppe Personal, zeigt jedoch auch einige Auffälligkeiten. Die Gruppengröße in der Stichprobe weicht zum Teil zwischen den Feldern stark voneinander ab und reicht von einer Person (Sekretariat) bis zu 40 Personen (Vertrieb). Die Anzahl der Teilnehmenden je Tätigkeitsfeld beträgt neun im Mittelwert bzw. sechs im Median. Marketing ist als einziges Tätigkeitsfeld im Median der Personengruppe Geschäftsleitung/Top-Management zuzuordnen. Allerdings ist diese Gruppe im Schnitt weniger stark vertreten als andere. Die Verteilung der Antworten zeigt, dass die Tätigkeitsfelder Einkauf und Materialwirtschaft „Nie“ mit einigem Abstand am häufigsten auswählten.

Zwischen den Tätigkeitsfeldern Einkauf und Vertrieb tritt die höchste Korrelation auf. Dies entspricht der zu erahnenden Nähe beider Bereiche. Die geringen Korrelationen mit Marketing hingegen könnten mit den höherrangigen Mitarbeitenden dieser Gruppe zusammenhängen.

Überraschend waren auch einige Antwortverteilungen spezifischer Tätigkeitsfelder. Prozessmanagement schätzte den Schulungsbedarf bei sich selbst am geringsten ein. Dieses scheint bei den vergleichsweisen hohen Werten bezüglich der Sicherheitsmaßnahmen zumindest in dieser Versuchsumgebung nicht unbegründet. Dennoch kann hier eine Selbstüberschätzung für die Unternehmen gefährlich werden. Aus den Angaben von Einkauf lässt sich schlussfolgern, dass dieses Tätigkeitsfeld wenige bis gar keine Dienstreisen antreten muss. Allerdings fand die Erhebung im Zeitraum der COVID-19-Pandemie statt und es bleibt unklar, wie hoch dieser Wert in der Zeit davor ausgefallen wäre. Zur Personengruppe des Tätigkeitsfeldes Fertigung fällt auf, dass lediglich das mittlere Management an der Befragung teilgenommen hat und die Gruppengröße gering ausfällt. Möglicherweise erhielten Mitarbeitende unter dieser Stufe keinen Zugang zu der Umfrage. Dies könnte auch bei anderen Tätigkeitsfeldern der Fall gewesen sein. Der Vertrieb nutzt erstaunlicherweise nie bzw. selten Online-Banking und -Buchung, Fremdsprachen und Firmen-WLAN. Mitarbeitende des Bereichs Forschung haben den seltensten Zugriff auf personenbezogene Daten und tätigen kaum externe Telefonate laut den Ergebnissen.

4.3.4 Vergleichsanalyse der Personengruppen

Die **hierarchischen Personengruppen** können ebenfalls in gleicher Weise und in diesem Fall ausschließlich anhand des Medians verglichen werden.

Geschäftsleitung / Top-Management (kurz „Geschäftsleitung“)

Gruppengröße: 10 Antwortende
Antwortcharakteristik: 5x „Nie“, 25x „Selten“, 25x „Häufiger“, 18x „Immer“

Die Geschäftsleitung gab als einzige Personengruppe bei **„Nie“** die Nutzung von Desktop-Computern an. Bei **„Selten“** stach Folgendes heraus: Zutritt zum Tresor / Safe (andere nie), Nutzung von Programmierumgebungen (andere noch seltener oder nie), von einem Festnetztelefon (andere häufiger oder immer), Erhalt eines Firmenschlüssels für sensible Bereiche (andere nie), Zugriff auf sensible Personendaten (andere seltener oder nie) und Arbeit an wechselndem Arbeitsplatz. Zwar immer noch tendenziell **„Selten“**, aber häufiger als alle anderen, nutzt die Geschäftsleitung Fremdsprachen, digitale Signaturen, Soziale Netzwerke, Online-Buchungen, Datenverschlüsselung, Freeware und Backup-Software. Die Geschäftsleitung ragt im Vergleich zu anderen Personengruppen hervor durch die **häufigste / n** mobile Arbeit, Reisen mit KFZ, Teilnahme an betrieblichen Feierlichkeiten und Nutzung von USB-Sticks / externen Festplatten, Kreditkarten, mobilem WLAN, Uploads, Karrierenetzwerken, Clouddiensten, Online-Bestellungen, Online-Banking, Downloads, Video-Konferenzen und Datenbanken. Häufig, aber im Gegensatz zu anderen Personengruppen nicht immer, wird in der Geschäftsleitung von internen Telefonaten Gebrauch gemacht. Als Einzige gaben die 10 Personen aus der Geschäftsleitung an, **„Immer“** Smartphones (privat / dienstlich), Generalfirmenschlüssel, Firmen-WLAN zu nutzen sowie Zugriff auf personenbezogene Daten (ebenso vertrauliche) zu besitzen und Kontakt zu externen Dienstleistern, Kundinnen und Kunden sowie Geschäftspartnerinnen und -partnern zu haben. Sie sind damit extrem exponiert und tragen zugleich das höchste Gefahrenpotential.

Mittleres Management

Gruppengröße: 26 Antwortende
Antwortcharakteristik: 13x „Nie“, 31x „Selten“, 16x „Häufiger“, 13x „Immer“

Personen aus dem mittleren Management gaben als Einzige bei **„Nie“** die Nutzung einer digitalen Signatur an. Bei **„Selten“** stach Folgendes heraus: Arbeit im Homeoffice, Tätigung von Online-Buchungen oder -Bestellungen, die Nutzung Sozialer Netzwerke, von Payware (andere noch seltener oder nie), von USB-Sticks / externen Festplatten, von Uploads, von Karriere-Netzwerken, von Smartphones (privat / dienstlich), von Generalfirmenschlüsseln und von mobilem WLAN. Es ist anzumerken, dass sich das „Mittlere Management“ trotz der genannten Eigenarten vergleichsweise oft im Mittelfeld der Antworten befindet. Bei **„Häufiger“** war besonders auffällig: die Nutzung von Datenbanken, von ERP-Programmen (andere seltener oder nie) oder von Video-Konferenzen. Zudem hatten Kolleginnen und Kollegen zwar häufig, aber nicht immer wie in den anderen Personengruppen Zutritt zum Arbeitsplatz. Als Einzige gaben die 26 Probandinnen und Probanden aus dem mittleren Management an, **„Immer“** Drucker / Scanner zu nutzen.

Mitarbeitende

Gruppengröße: 62 Antwortende

Antwortcharakteristik: 32x „Nie“, 17x „Selten“, 11x „Häufiger“, 13x „Immer“

Mitarbeitende gaben als Einzige bei **„Nie“** Folgendes an: Soziale Netzwerke, Tablets, Smartphones, Payware, USB-Sticks / externe Festplatten und E-Mail-Verschlüsselung zu nutzen oder mit Datenlöschung oder -verschlüsselung betraut zu werden. Bei **„Selten“** stach Folgendes heraus: Zugriff auf vertrauliche Daten (andere häufiger oder immer) oder Nutzung von Downloads (andere häufiger). Bei **„Häufiger“** war besonders die Nutzung von Druckern / Scannern auffällig (andere noch häufiger oder immer). Die 62 Mitarbeitenden fielen in Bezug auf die Antwort **„Immer“** kaum auf.

Auszubildende / Trainees / Praktikantinnen und Praktikanten

Gruppengröße: 8 Antwortende

Antwortcharakteristik: 31x „Nie“, 19x „Selten“, 13x „Häufiger“, 10x „Immer“

Auszubildende gaben als Einzige bei **„Nie“** Folgendes an: Übernachtungen, Zutritt zum Arbeitsplatz durch Kundinnen und Kunden und Geschäftspartnerinnen und -partner, Reisen mit KFZ, mobiles Arbeiten, Nutzung von Freeware, Messenger oder ERP-Programmen. Bei **„Selten“** stach Folgendes heraus: Nutzung von Telefon- oder Video-Konferenzen (andere häufiger oder immer), digitaler Signatur, VPN / Remote Netzwerken (andere häufiger), Kontakt mit Geschäftspartnerinnen und -partnern und Behörden oder Kundinnen und Kunden (andere häufiger oder immer). Bei **„Häufiger“** war besonders auffällig: Erhalt eines Firmenschlüssels (andere „Immer“), Dokumentenvernichtung (andere seltener), Nutzung von Festnetztelefonen, Führen externer Telefonate (andere immer), Arbeit an wechselnden Arbeitsplätzen (andere seltener oder nie). Als Einzige gaben die 8 Auszubildenden an, **„Immer“** einen Server / Host zu nutzen.

4.3.5 Profilgruppen

Bedarf und Verwendung von Sicherheitsmaßnahmen in KMU scheinen bereits klar. Es müssen im Weiteren Ansatzpunkte für gemeinsame Maßnahmen aus der Auswertung der Umfrage ebenfalls abgeleitet werden. Grundlage soll eine Zuordnung der 15 Tätigkeitsfelder zu sieben Profilgruppen sein. Ein Hindernis stellte sich durch den fehlenden Rücklauf zu drei Tätigkeitsfeldern (Rechtsabteilung, Hausverwaltung / Facility Management, Öffentlichkeitsarbeit / Public Relations). Ohne präzisere Ergebnisse aus aufwendigeren, stärker aufbereiteten quantitativen Analysetechniken (Clusteranalyse und Hasse-Diagramme) blieb vorerst zudem nur ein qualitativer Ansatz auf Basis der Umfragedaten. Dazu zählten die Einbeziehung erster Auffälligkeiten aus den durch Hilfe von Korrelationswerten affin geordneten Detail-Grafiken (Darstellung durch Balken und Netze / Amöben), der Rankings aus den Streudiagrammen, der Korrelationsanalyse und die Hinzunahme des BSI IT-Grundschutzes [21]. Es wurde dahingehend im Team iterativ eine Matrix aus den fünf Fragerubriken („I. Technische Infrastruktur", „II. Externe Interaktion / [Risiken]", „III. Arbeitsumgebung", „IV. Sicherheitsmaßnahmen" und „V. Sensibilisierung") erstellt. Diese bestand aus den 15 Fragekomplexen, in denen die 73 auf die Stufen „Nie", „Selten", „Häufiger" und „Immer" basierten Fragen in der Umfrage abgefragt wurden. Aus dieser Matrix wurden die sieben Zielprofile zur Organisation der Personalentwicklung herausgearbeitet. Wie in der ebenfalls im Projekt erstellten psychologisch gestützten Studie [5] stellte sich bald heraus, dass viele Themen so allgemein sind, dass sie schwer auf ein Profil begrenzt werden können. Diese Beobachtung wurde auch durch einen ersten Versuch einer Clusteranalyse und einer Erstellung von Hasse-Diagrammen zu den Tätigkeitsfeldern über die sämtlichen 73 Fragen dahingehend gestützt, dass eine klare Zuordnung ohne weitere Verfeinerung durch kleinere Fragegruppen schwerfiel.

Allgemeine Grundkompetenzen

Daher wurde ausgehend eine Profilgruppe Allgemeine Grundkompetenzen erstellt, die allgemein Anforderungen und Grundlagen für den Erwerb einer Tätigkeit in KMU beschreibt und für alle Tätigkeitsfelder gilt. Fokus ist hier, einen Basis-Schutz und Grundkenntnisse zu vermitteln. Dieser Bereich muss daher besonders breit, aber auf einer für alle Tätigkeitsfelder vermittelbaren Ebene entwickelt werden. Als Lernszenario könnte hierbei allgemein eine Schulung zu E-Mails (Phishing) / CEO Fraud angeboten werden.

Produktion, Entwicklung und Vertrieb

Als nächstes ist festzustellen, dass sich gerade die Kerntätigkeiten, also die Tätigkeiten, die unmittelbar mit der Herstellung des Produkts oder der Erstellung der Dienstleistung zu tun haben, durch gewisse Gemeinsamkeiten auszeichnen. Diese waren zum Beispiel ein geringes Niveau an Verschlüsselungsmaßnahmen, seltener Zugriff auf sensible Personendaten, kaum Zutritt zu sensiblen Bereichen, keine Verwendung von Kreditkarten oder Online-Banking. Ebenso wird vorwiegend an festen Arbeitsplätzen und Desktop-Computern gearbeitet. Oft wurde auch der Schulungsbedarf für sich selbst und das Unternehmen als gering eingeschätzt. Grundlegend überschneidet sich der Schulungsumfang für diese Teilgruppe mit dem der allgemeinen Profilgruppe Grundkompetenzen. Zum Profil gehören überdurchschnittlich starke Korrelationspaare mit besonderer Nähe zur Produktion: Einkauf / Beschaffung, Materialwirtschaft / Logistik / Lager und Fertigung / Produktion. Diese Teilgruppe Produktion wurde mit einer weiteren aus starken Korrelationspaaren bestehenden

Teilgruppe Vertrieb zusammengelegt, die zum einen operativ sehr nah mit den Kerntätigkeiten agiert, zum anderen aber ein agileres Profil durch Reisen, stärkere externe Kontakte zu Kundinnen und Kunden und prozessuale Datenverarbeitung aufweist. Dazu zählen Vertrieb/Außendienst, Kundenmanagement/Kundenservice, Prozessmanagement/Qualitätssicherung/Controlling. Auf einer Sonderposition zwischen diesen beiden Teilgruppen befindet sich das Tätigkeitsfeld Forschung/Entwicklung, das etwas losgelöst vom normalen Betrieb erscheint und einen höheren Anspruch an Sicherheitsmaßnahmen besitzt. Sie hat eine besonders hohe Korrelation mit Vertrieb/Außendienst und kann durch ihren substanziellen Beitrag zum Produkt oder zur Dienstleistung ebenfalls zu den Kerntätigkeiten gezählt werden. Diese gesamte Profilgruppe Produktion, Entwicklung, Vertrieb machte in der Befragung zusammen rund 75 Prozent aus (siehe grüne Tönungen in Abbildung 8) und es finden sich dort die stärksten Korrelationspaare von Tätigkeitsfeldern. Ergänzend zu den Grundkenntnissen könnten hier Schulungen für entwicklungs- und prozesslastige Aufgaben im Bereich Verschlüsselung und Wirtschaftsspionage und für die mobilere Teilgruppe im Bereich Travel-Security angeboten werden.

Nachdem in den ersten beiden Profilgruppen entweder allgemeine Grundkenntnisse vermittelt werden oder ein Sammelbecken für Kerntätigkeiten und mit ihnen eng verbundene, anspruchsvollere Tätigkeitsfelder entstanden ist, sind die weiteren fünf Profilgruppen etwas spezieller gefasst worden.

Informationsverarbeitung und IT-Infrastruktur

Die Profilgruppe Informationsverarbeitung und IT-Infrastruktur ist entscheidend für die Einrichtung und Wartung der technischen Infrastruktur. Sie ist der digitale der vier „Gatekeeper“ (Torwächter, die als besondere Instanz bei der Zugangskontrolle fungieren) und kontrolliert die technischen Zugänge. Sie machte in der Befragung acht Prozent aus (siehe Abbildung 8). Zudem entwickelt sie die technischen Richtlinien und steuert das dahingehende Sicherheitstraining, weswegen sie auch den Schulungsbedarf am höchsten einschätzt. Sie ist zum einen an einen festen Arbeitsplatz gebunden, muss aber gleichzeitig überall im Unternehmen mobil tätig sein und ist in allen technischen Geräten und Netzwerken versiert. Neben einem besonderen Augenmerk auf die Vermittlung von neuesten Richtlinien und „Trainingskonzepten“ könnte dieser Gruppe beispielsweise eine Schulung in Ransomware zum Schutz und Erhalt der Datenverfügbarkeit angeboten werden.

Instandhaltung und Vermittlung

Die Profilgruppe Instandhaltung und Vermittlung ist durch keine Probanden oder Probandinnen in der Umfrage repräsentiert worden, aber ebenfalls für die Einrichtung und Wartung der Infrastruktur zuständig, jedoch mehr im haustechnischen Sinne. Zudem nimmt sie Organisationsaufgaben bei der Steuerung von Kontakten, Personenflüssen und analogen Kommunikationskanälen war. Sie ist also der physische „Gatekeeper“ und kontrolliert räumliche, postalische und als allgemeine Anlaufstelle telefonische Zugänge. Hierarchisch ist sie auf einer unteren Ebene angesiedelt, aber nicht unkritisch bei der Durchführung von Sicherheitsmaßnahmen. Es zählen hierzu die Tätigkeitsfelder Hausverwaltung/Facility Management und Empfang/Pförtnerei/Poststelle, dem das Sekretariat in seiner besonderen Stellung einer eigenen Gruppe ausgegliedert wurde. Eine Schulung würde sich beispielsweise hier zum Thema Desinformation und Social Engineering anbieten.

Organisations- und Assistenztätigkeiten

Die Profilgruppe Organisations- und Assistenztätigkeiten umfasst grundlegend die Aufgaben des Sekretariats. Sie machte in der Befragung mit nur einer Antwort ein Prozent aus (siehe Abbildung 8). Das Sekretariat übernimmt eine Hybridstellung zwischen seiner Vermittlungs- und Organisationstätigkeit und dem jeweiligen Tätigkeitsfeld, dem es konkret zuarbeitet. Es ist also der kommunikative „Gatekeeper", der alle Kommunikationsflüsse beispielsweise zur Unternehmensleitung oder einem Ressort kontrolliert. Ebenfalls übernimmt diese Profilgruppe im Gegensatz zur „Vermittlung" bereits Verwaltungsaufgaben und hat auch Zugriff auf finanzielle Bereiche wie Online-Buchungen, Online-Bestellungen, Kreditkarten. Diese Profilgruppe kann daher im Zuge der Schulung entweder der Vermittlung zugeordnet werden und ebenfalls dessen Themen Desinformation und Social Engineering übernehmen oder je nach Aufgabenteilung im Unternehmen quasi als „Libero" Expertisen aus allen andern Profilbereichen übernehmen.

Verwaltung und Personal

Die Profilgruppe Verwaltung und Personal befasst sich, wie der Name schon signalisiert, mit sehr empfindlichen Bereichen in der Finanz- und Personalverwaltung. Dabei sind die Zugriffsmöglichkeiten zwar eng beschnitten, aber tiefer als beispielsweise bei der Profilgruppe Organisation und Assistenz. Die Gruppe machte in der Befragung zusammen elf Prozent aus (siehe dunkelblaue Tönungen in Abbildung 8). Die Gruppe ist der finanzielle und personelle „Gatekeeper", der Finanzströme und Personalzugänge kontrolliert. Generalfirmenschlüssel, Zutritt zum Tresor, Zugriff auch auf sensibelste Personendaten, dienstliche Smartphones und auch Verantwortlichkeiten zur Dokumentenvernichtung und Datenlöschung sind hier am ausgeprägtesten. Es ist zu bemerken, dass in diesem Profil zum einen viele Kontakte nach außen bestehen, aber zum anderen sowohl Kollegen und Kolleginnen als auch Partnern / Kunden / Behörden Zutritt zum Arbeitsplatz möglich scheint. Das Profil umfasst die Tätigkeitsfelder Personal(-wesen / -verwaltung) / HR, Finanzen / Buchhaltung / Rechnungswesen und, auch wenn es keine Rückmeldung in der Umfrage dazu gab, die Rechtsabteilung, da diese zwar weniger ausführt, aber doch tiefe Einblicke in alle Unternehmensbereiche besitzt. Diese Profilgruppe könnte beispielsweise speziell im Thema Datenschutz geschult werden.

Strategie und Führung

Die Profilgruppe Strategie und Führung wird aus der Unternehmensleitung selbst, d.h. aus leitenden Führungspositionen und strategisch operierenden Unternehmensbereichen gebildet. Sie machte in der Befragung fünf Prozent in den Pilotunternehmen und neun Prozent in der Gesamtstichprobe aus (siehe Abbildung 11), sofern man nur die Personengruppe Geschäftsleitung / Top-Management betrachtet. Hier werden Entscheidungen getroffen und Richtlinien vorgegeben. Zu allen Unternehmensbereichen, einschließlich sensibler Daten, Tresore und sicherheitsrelevanter Mechanismen besitzt diese Gruppe teilweise oder ganz Zutritt, Zugang und Zugriff. Außerdem ist sie sehr mobil und durch ihren ständigen Kontakt mit allen Stakeholdern extrem exponiert. Sie muss über alle Sicherheitsbereiche als erstes auf dem neuesten Stand gehalten und abgesichert werden. Zu dieser Gruppe können Tätigkeitsfelder wie Marketing / Kommunikation und das zwar in der Umfrage unbeantwortete, aber eng mit Marketing / Kommunikation verbundene Feld „Öffentlichkeitsarbeit" gezählt werden. Dieses Profil kann beispielsweise in dem Thema Travel-Security geschult werden.

4.3.6 Konstruktion eines Profilbogens

Es soll noch einmal klar unterstrichen werden, dass die genannten Schulungsbeispiele für die meisten Profilgruppen ebenfalls von Wert sind, insbesondere weil Profile in der Praxis nicht klar abzugrenzen sind und alle Bereiche von verschiedenen Angriffsvektoren betroffen sein können. Daher sollen die thematischen Zuordnungen eher als „Leuchtturm-Themen“ des Profils verstanden werden, die beispielsweise über „Train the Trainer“-Ansätze zwar dort eingebracht, aber dann von dort auf das ganze Unternehmen abstrahlen und eigenständig verbreitet werden können.

Aus diesen Profilgruppen lässt sich modular ein „Profilbogen“ konstruieren (siehe Abbildung 37). Es lassen sich zudem gemeinsame Sonderrollen identifizieren, die farblich hervorgehoben wurden. Die „Allgemeinen Grundkompetenzen“ bilden an der Spitze die Grundvoraussetzung für alle Tätigkeiten (grauer Baustein). Zusammen mit dem stark auf Grundkompetenzen aufbauenden, und daher mit der Ampelfarbe Grün eingefärbten, Baustein „Produktion, Entwicklung und Vertrieb“ und dem Baustein „Strategie und Führung“ bildet sich über drei Steine auf zwei Ebenen die Spitze des Bogens, die in jedem KMU vorhanden ist. Ist ein KMU diversifizierter in seinen Aufgabenbereichen, können die nächsten beiden Bausteine „Informationsverarbeitung und IT-Infrastruktur“ und „Verwaltung und Personal“ explizit als organisatorische Einheiten vorhanden sein. Jedoch ist auch diese Ebene in jedem Unternehmen essenziell, selbst wenn sie aufgrund der geringen Unternehmensgröße nur als Rolle in anderen Abteilungen übernommen werden kann. Die orange Einfärbung weist auf die Richtlinienkompetenzen jener Bausteine bezüglich IT und grundlegender Entscheidungen der Führung hin. Die violette Einfärbung signalisiert die besonders sensible Natur des Bausteins „Verwaltung und Personal“. Der Bogen fußt auf zwei blauen Bausteinen, die greifbar hinzukommen, falls das Unternehmen auch hierfür eigene Beschäftigte hat. Die Bausteine „Instandhaltung und Vermittlung“ und „Organisations- und Assistenztätigkeiten“ mögen zwar hierarchisch niedrig angesiedelt sein, sind aber in ihrer Sicherheitsfunktion nicht zu unterschätzen, denn sie bilden zusammen mit der zweiten Ebene die vier „Gatekeeper“ (Torwächter), die den Kernteil (die oberen zwei Ebenen) des Unternehmens vor Angreifenden bereits weitestgehend abschirmen können. Doch ganz an der Spitze ist klar ersichtlich: die ständige Aufmerksamkeit auf Basis von „Allgemeinen Grundkompetenzen“ steht über allem. Unabhängig davon, ob ein KMU jeden Profilbaustein explizit besetzt oder nicht, müssen spätestens die aus diesen Tätigkeitsprofilen abgeleiteten Kompetenzprofile in jedem Unternehmen vollständig vorhanden sein, sonst bricht der Bogen zusammen. Die Wichtigkeit der Informationssicherheit in den KMU ist durch die Umfrageergebnisse in den Tätigkeitsfeldern klar aufgezeigt worden. Die Entwicklung und Notwendigkeit angepasster Maßnahmen zur Personalentwicklung leitet sich aus dem Konstrukt des Profilbogens deutlich ab, auch dann, wenn dessen Funktionen in kleinsten Unternehmen mehrfach verteilt werden müssen. Denn obwohl sich meist nicht zu jedem Baustein ein klar abgrenzbares Pendant in der Unternehmensstruktur wiederfindet, müssen die Rollen dennoch verteilt werden und in offenem Dialog miteinander stehen.

Abb. 37: *Profilbogen*

5 Schlussfolgerung

Der BSI-Lagebericht 2021 der Bundesregierung ist bezüglich der nach EU-Klassifikation 2,6 Millionen deutschen Unternehmen im Bereich KMU und damit 99,4 Prozent aller deutschen Unternehmen recht deutlich:

> *„Anders als typische Großunternehmen beschäftigen KMU in der Regel keine dedizierten IT-Sicherheitsteams. Oftmals verfügen sie nicht einmal über einen eigenen IT-Betrieb. Daraus folgt vielfach eine mangelnde Beurteilungskompetenz für IT-Sicherheitsgefährdungen. Zudem fehlt auf Managementebene häufig das grundsätzliche Bewusstsein für die Risiken und Abhängigkeiten, die der Einsatz von Informationstechnik mit sich bringt. Dadurch sind KMU gegenüber Bedrohungen aus dem Cyber-Raum besonders anfällig. Durch den stetig zunehmenden Grad an Digitalisierung verschärft sich die Gefährdungslage kontinuierlich.“ [27:63]*

Dieses unterstreicht die in „Cybersicherheitsstrategie für Deutschland 2021“ festgestellte Ausgangslage: „Insbesondere KMU sind den Herausforderungen aufgrund von Mängeln an Ressourcen und Wissen nicht ausreichend gewachsen.“ [28]. Auch die Interessensvertretung der Wirtschaft in Bezug auf Cybersicherheit, bitkom e. V., empfiehlt „... in Übereinstimmung mit dem BSI […] 20 % des IT-Budgets in Cybersicherheit zu investieren“ [29]. Somit wird die Tendenz sichtbar, dass innerhalb der KMU die kritische Lage immer mehr erkannt wird (siehe [30]). Die durchgeführte Umfrage, gerade da die untersuchten Unternehmen einen bereits aktiven Eindruck hinterlassen haben, bestätigt jenes ebenfalls: Nutzungsverhalten ist exponiert, Informationssicherheit wichtig und Schulungsbedarf allgegenwärtig.

Vergleicht man die Ergebnisse der Anfang 2021 durchgeführten Umfrage mit den Studien des Wissenschaftlichen Instituts für Infrastruktur und Kommunikationsdienste (WIK) aus dem Zeitraum 2011/2012 (im Auftrag des Bundesministeriums für Wirtschaft und Technologie) [18] und 2017 [17] (siehe Tabellen 3 bis 7), so lassen sich keine großen Widersprüche erkennen, im Gegenteil, es werden Entwicklungen und Tendenzen durch diesen Report bestätigt. Auch wenn der Vergleich sehr vorsichtig ausgeführt werden muss, da dort KMU als Ganzes befragt wurden, 2017 zudem ausschließlich zwischen kleinen und großen KMU differenziert wurde, während in der erörterten Umfrage bei grob vier Pilotunternehmen der Fokus auf die Gesamtheit der Mitarbeitenden gelegt war, so lassen sich wichtige Schlüsse bestätigen. KMU werden digitaler, mobiler und schulungsbedürftiger.

Tabelle 3: *Ergebnisse verschiedener Studien zum Thema Arbeitsgerät*

Arbeitsgerät		
ALARM Report 1 (2021) (Anteil Mitarbeitende)	**WIK (2017)** (Anteil Firmen, z. T. kl./gr. KMU)	**BMWi (2012)** Quelle: WIK (2011/12) (Anteil Firmen)
Surfen im Internet 99%	PC-Arbeitsplatz 94% (mit Internet)	PC-Arbeitsplatz 96% (mit Internet)
Laptop/Notebook 86%	Notebooks/Netbooks 53%/88%	Notebooks/Netbooks 71%
Smartphone (privat/dienstlich) 44% (inkl. 14% „Immer“) Smartphone (privat/dienstlich) 44% (inkl. 30% „Immer“)	Smartphones 71%/90% Herkömmliche Handys 12%/39%	Smartphones 48% Herkömmliche Handys 66%
Tablets 41%	Tablet-PCs 37%/68% PDAs 3%/9%	Tablet-PCs 14% PDAs 13%
Server (Host) 74%		Client-Server-Architektur 40%

Tabelle 4: *Ergebnisse verschiedener Studien zu den Themen Arbeitssoftware und Onlineaufgaben*

Arbeitssoftware und Onlineaufgaben		
ALARM Report (2021) (Anteil Mitarbeitende)	**WIK (2017)** (Anteil Firmen, z. T. kl./gr. KMU)	**BMWi (2012)** Quelle: WIK (2011/12) (Anteil Firmen)
ERP-Software 63%		kaufm./Rechnungswesen 75%
Backup-Software 39%	Sicherungskopien Daten 89%/99%	Regelmäßige Backups 94%
Online-Banking 26%	Online-Banking 80%/82%	Online-Banking 80%

Tabelle 5: *Ergebnisse verschiedener Studien zu den Themen Internet, Netzwerke und Kommunikation*

Internet, Netzwerke und Kommunikation		
ALARM Report (2021) (Anteil Mitarbeitende)	**WIK (2017)** (Anteil Firmen, z. T. kl./gr. KMU)	**BMWi (2012)** Quelle: WIK (2011/12) (Anteil Firmen)
mobiles Arbeiten 62% Mobiles-WLAN 53%	mobiler Zugriff 42%/73%	mobiler Zugriff 44%
VPN - Remote 81%	VPN 31%/88%	VPN 45%
Clouddienste 67%	Cloud Computing 23%	Cloud Computing 10%
Soziale Netzwerke 35%	Soziale Netzwerke 36%/46%	Soziale Netzwerke 16%
Messenger 58%	WhatsApp 47%/36%	SMS/MMS 58%
E-Mail 100%	E-Mail 96%/99%	E-Mail 98%

Tabelle 6: *Ergebnisse verschiedener Studien zu den Themen Sicherheitsstufen und Datensicherheit*

Sicherheitsstufen und Datensicherheit		
ALARM Report (2021) (Anteil Mitarbeitende)	WIK (2017) (Anteil Firmen, z. T. kl./gr. KMU)	**BMWi (2012)** Quelle: WIK (2011/12) (Anteil Firmen)
Passwörter 96%	Passwörter 96%/98%	Passwörter (Authentisierung) 94%
Datenverschlüsselung 54%	Verschlüsseln von Dateien 41%/58%	Verschlüsseln von Dateien 39%
Festplattenverschlüsselung 38%	Festplattenverschlüsselung 24%/39%	Festplattenverschlüsselung 20%
E-Mail-Verschlüsselung 53 %	E-Mail-Verschlüsselung 35 % / 44 %	E-Mail-Verschlüsselung 18 %

Tabelle 7: *Ergebnisse verschiedener Studien zum Thema Sensibilisierung*

Sensibilisierung		
ALARM Report (2021) (Anteil Mitarbeitende)	**WIK (2017)** (Anteil Firmen, z.T. kl./gr. KMU)	**BMWi (2012)** Quelle: WIK (2011/12) (Anteil Firmen)
Schulungen und Sensibilisierung 92%	Teilnahme an Schulungen 29%/60% (kostenlos) 22%/61% (kostenpflichtig) Regelmäßige IS-Schulungen 15%/29% (für Mitarbeitende) 22%/58% (für IT-Personal) Regelmäßige Sensibilisierung 47%/73%	Teilnahme an Schulungen 31% (kostenlos) 31% (kostenpflichtig) davon regelmäßig 14 %
Schulungsbedarf 99%	Unterstützungsbedarf Teilnahme an Schulungen 12%/15%	mehr Schulungen 18% (für Mitarbeitende) 11% (für IT-Mitarbeitende) Allg. Verbesserungswürdig 35%

Das BSI rät, langfristig die Realisierung eines Schulungs- und Sensibilisierungskonzepts anzustreben, und bietet mit dem IT-Grundschutz folgende Kernthemen [31]:

- Sensibilisierung für Informationssicherheit
- Mitarbeiterbezogene Informationssicherheitsmaßnahmen
- Produktbezogene Sicherheitsmaßnahmen
- Verhalten bei Auftreten von Schadsoftware
- Bedeutung der Datensicherung und deren Durchführung
- Umgang mit personenbezogenen Daten
- Einweisung in Notfallmaßnahmen
- Vorbeugung gegen Social Engineering

Jedoch beschreiben Schulung und Sensibilisierung nur das Ziel und nicht das Mittel.

Die Ergebnisse der ersten Grundlagenstudie im Projekt „Awareness Labor KMU (ALARM) Informationssicherheit“ (siehe [5]) greifen diese Frage auf und bilden die Ausgangsbasis für die Entwicklung von neuen, an die KMU angepassten Sensibilisierungsmaßnahmen. Ihr Ziel und damit der Mehrwert für KMU ist, die Bereitstellung integrativ verzahnter Maßnahmen für eine systematische Sensibilisierung, die eine Sicherheitskultur tatsächlich zu entwickeln hilft.

Um eine nachhaltige und fest verankerte Sicherheitskultur in Unternehmen zu etablieren, müssen zielgerichtete sowie an die Menschen, die Tätigkeitsfelder, das vorhandene Wissen und die Gegebenheiten des Unternehmens angepasste Maßnahmen ergriffen werden. Dazu gehören Sensibilisierungskonzepte wie Trainings oder Schulungen in einer begreifbaren und greifbaren Form wie den erlebbaren und interaktiven analogen und digitalen Lernszenarien. Um einzelne Zielgruppen der Tätigkeitsprofile zu erreichen und deren Kompetenzen für Informationssicherheit zu steigern, bedarf es integrierter Maßnahmen in Unternehmen. Der Report stützt die Notwendigkeit angepasster Maßnahmen, zeigt aber nach Hinzunahme quantitativer Analysetechniken und Betrachtungen in den Streudiagrammen gleichermaßen die Grenzen eines Zuschnitts auf einzelne Tätigkeitsfelder.

Die Entwicklung des Profilbogens wird diesem Spannungsfeld wiederum gerecht. Die Bogenkonstruktion unterstreicht, dass Tätigkeitsprofilbausteine über- und ineinandergreifen. Das Ganze bedeutet für KMU, fehlt ein Baustein, dann brechen der Bogen und der Schutz zusammen. Die Identifikation von Sonderrollen, Kernbausteinen und „Gatekeepern“ im eigenen Unternehmen unterstützt dessen Statik. Durch die mögliche Zuweisung der Tätigkeitsfelder an mehrere Tätigkeitsprofilbausteine, und nicht nur an eine einzelne Tätigkeitsprofilgruppe, bleiben die Maßnahmen bedarfsgerecht anpassbar. Dieses kommt den fließenden Grenzen zwischen den Tätigkeitsfeldern zugute, die in KMU zu beobachten sind. Tätigkeitsprofilbausteine dienen zudem als Transmissionsriemen. Auch wenn Tätigkeitsfelder nicht aus einzelnen Bausteinen eins zu eins bestehen, so können sie um einen Baustein gruppiert und im „Train-the-Trainer“ Prinzip organisatorische Vermittlungseinheiten mit „Leuchtturmfunktion“ bilden und im Gegenzug von anderen Tätigkeitsfeldern trainiert werden. Letztlich lassen sich so die Bausteine mit den aus der Studie entwickelten Awareness-Themen füllen (siehe Kasten und [5]).

AWARENESS-THEMEN (ALARM-STUDIE)

1. **Passwort**
2. **Phishing, CEO Fraud & Co.**
3. **Social Engineering, Manipulation & Co.**
4. **Apps, Software & Co.**
5. **Sicher im Homeoffice**
6. **Datenschutz in der Cloud sowie Datenschutz im Kontext Kunden und Lieferanten**
7. **Messenger, sichere Übertragung, Storage, Verschlüsselung & Co.**
8. **Informationsklassifizierung (nur dort, wo sie als Prozess eingeführt ist)**

6 Ausblick und Empfehlungen

6.1 Ausblick

Offen bleibt eine weitere Auseinandersetzung und Bestätigung der Profilgruppen durch eine Clusteranalyse, partielle Ordnungen (Hasse-Diagramme) oder Ähnlichem. Aufgrund der Komplexität der Themen und Umfrage (über 70 Fragen) und des nicht repräsentativen Designs als Zustandsanalyse wurde dieses für den vorliegenden Bericht nicht realisiert. Ebenso bietet sich an, die Analyserichtung umzukehren und Spielszenarien / IS-Themen anhand der 70 Nutzungsfragen und vier Stufen zu bewerten und mittels Korrelationen oder Clusteranalysen Tätigkeitsfeldern bzw. Profilgruppen zuzuordnen. Ein besonderes Augenmerk muss zukünftig darauf gelegt werden nachzuverfolgen, welche temporären Erscheinungen durch die COVID-19-Pandemie im Umfragezeitraum begründet sind, welche Themen sich in der Zukunft relativieren und was bleibt oder sich daraus weiterentwickelt. Aus der ersten Umfrage haben sich zudem gewisse Lerneffekte für die nächste Umfrage ergeben. So bietet es sich an, mit den für die Durchführung der Umfrage in den Pilotunternehmen und weiteren Unternehmen Verantwortlichen ein kurzes Briefing und nach der Umfrage Debriefing durchzuführen, um offene Fragen zu klären, und auch auf dieser Ebene Feedback einzusammeln. Die Sicherheitskultur muss zudem eigenständig unter die Lupe genommen werden.

6.2 Sieben Empfehlungen

Zur Hilfe bei der Personalentwicklung werden den Mitarbeitenden sieben Empfehlungen an die Hand gegeben, die in jedem Unternehmen vollständig umgesetzt werden sollten. Haben alle Mitarbeitenden diese Empfehlungen verinnerlicht und ein Grundverständnis vom Profilbogen und dessen Tragweite und Tragkraft, so ist der Grundstein bereits gelegt.

1.

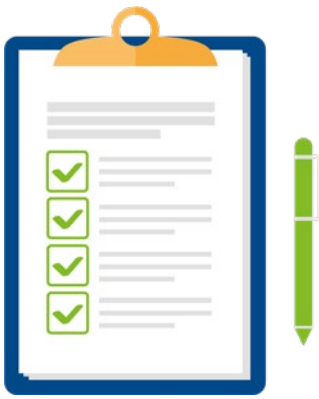
Grundlage muss sein, den Ist-Zustand im eigenen Unternehmen festzustellen (Bedrohungen, Sicherheitslücken, Schutzmaßnahmen, Eigenarten des Personals, Schulungsstand/Awareness und Trainingsbedarf) (vgl. [32]). Vorzugsweise sollte dabei nach dem modernisierten IT-Grundschutz des BSI vorgegangen werden. Dessen Module lauten: Informationssicherheitsmanagementsysteme (ISMS), Organisation und Personal, Konzeption und Vorgehensweise, Betrieb, Detektion und Reaktion, Anwendungen (Software), IT-Systeme, Industrieller IT, Netze und Kommunikation sowie Infrastruktur (siehe Webangebot des BSI [21]). Kein Ersatz, aber ein ergänzendes Hilfsmittel stellt der vorgestellte Tätigkeitsprofilbogen dar, mit dessen Hilfe Tätigkeitsbereiche schnell erfasst und mit der realen Aufgabenteilung im eigenen Unternehmen abgeglichen, dort zugeordnet und effizient trainiert werden können.

Abgeleitet aus der ausschließlich gemeinsamen Tragfähigkeit aller Profilbausteine gehört dazu die Schaffung des Bewusstseins, dass alle Mitarbeitenden eines Unternehmens eine wichtige Rolle spielen und eine gemeinsame Sicherheitsstruktur bilden, die „Human-Firewall". Alle tragen dazu bei. Jede Tätigkeit kommt mit Informationen und Bedrohungen in Kontakt und spielt eine essenzielle Rolle. Wird es auf die Individuen heruntergebrochen, so helfen bei der Charakterisierung aus der ersten tiefenpsychologischen Grundlagenstudie im Projekt ALARM die darin entwickelten Akteurstypologien (IT-Kapitän/in, Vorfall-Experte/in, Verständnisvolle/r Tröster/in, IT-Notfallsirene und Volldeligierer/in [5]).

Es muss stets bewusst sein, dass es keine klaren Abgrenzungen bezüglich der Informationssicherheit gibt und die folgenden zugeordneten Empfehlungen für alle passenden Stellen gelten bzw. im Einzelnen mitgedacht werden müssen (über Gefahren z. B. per E-Mail, in Arten des Phishings oder CEO-Frauds, hinaus). Grundkompetenzen müssen überall vorhanden sein, reichen aber im Einzelfall so gut wie nie aus.

2.

Strategie und Führung: Erstellung, Kommunikation (innen wie außen) und Prüfung von allgemeinen Richtlinien und Vorgaben der Sicherheitskonzepte. Je mehr Befugnisse eine Führungskraft hat, desto höher muss diese selbst geschult sein und darüber hinaus immer als positives Vorbild fungieren. Im Detail sollte auch Travel-Security besonders in dieser Gruppe thematisiert werden.



3.

Produktion, Entwicklung und Vertrieb, wie in allen Profilen: Schaffung eines Bewusstseins im Umgang mit Internet, für Informationssicherheit im Allgemeinen und Anwendung der Zugangskontrollen (Passwörter generieren, mehrfache Authentisierung, Radio-Frequency Identification (RFID), Biometrie, automatische Computersperrung) im Besonderen. Speziell in der Entwicklung und Forschung stellt die Nutzung von Verschlüsselung, VPN, Storage, Sicherheit im Homeoffice und Schutz gegen Wirtschaftsspionage eine wichtige Basis dar. Im Vertrieb/Kundenservice findet sich das Thema Travel-Security und Datenschutz im Umgang mit Kunden und Lieferanten etwas häufiger wieder.

4.

Informationsverarbeitung und IT-Infrastruktur: Umsetzung von Zugangs-, (digital gestützten) Zutritts- und Zugriffskontrollkonzepten (digitales Gatekeeping). Erarbeitung, Vermittlung und Prüfung von IT-Sicherheits-Richtlinien sowie Apps und Software. Etablierung von „Remindern“ (dem sog. Erinnerungsmanagementsystem), Aktualisierung sowie Wartung der IT-Infrastruktur und Sicherheitsmechanismen. Der Schutz vor Ransomware, bzw. besonders den daraus entstehenden Gefahren, bildet ein präsentes Einzelthema.

5.

Verwaltung und Personal: Personalzugänge überwachen (personelles Gatekeeping) und Finanzströme kontrollieren (finanzielles Gatekeeping). Je nach spezieller Befugnis muss ein darauf abgestimmtes Training gewährleistet werden. Datenschutz muss hier besonders bei sensiblen Daten thematisiert werden und ist auch im Kontext der Cloudspeicherung mitzudenken.

6.

Instandhaltung und Vermittlung: Zutritt überwachen (physisches Gatekeeping), Arbeitssicherheits- und Evakuierungspläne bereithalten. Bewusstsein ist hier besonders gegenüber Vor-Ort-Angriffen durch Social Engineers und Desinformation aufzubauen.

7.

Organisations- und Assistenztätigkeiten: Kommunikation überwachen und legitimieren (kommunikativer Gatekeeper), je nach zugeordnetem Fachbereich bzw. der erteilten Sonderbefugnisse spezielles Training erhalten. Social Engineering und Manipulation will auch an dieser Stelle ein wohl vorbereitetes Thema sein.

Abschließend ist zu betonen: Das Sicherheitstraining zum einen speziell auf eine Tätigkeit zuzuschneiden und Aufgaben aufzuteilen, liegt auf der Hand, benötigt dafür passendes Trainingsmaterial und lässt die Abläufe und die Sicherheitsausbildung effizient im Alltag gestalten. Das engmaschig verflochtene Sicherheitsnetz einer bestmöglich aufgestellten „Human-Firewall“ bildet sich aber erst, wenn Rollenprofile, wo es möglich ist, zu Trainingszwecken getauscht und ebenfalls verinnerlicht werden. So besteht der im Projekt „Awareness Labor KMU (ALARM) Informationssicherheit“ gewählte Ansatz darin, Sensibilisierungsmaßnahmen in Form von dafür hervorragend anpass- und vermittelbaren Lernszenarien auf Tätigkeits-, Kompetenz- und Sicherheitsprofile zuzuschneiden. Hierdurch wird ein effizienter Transmissionsriemen zum Antrieb eines spezialisierten und durch Informationsaustausch umfassend wirksamen Schutzmechanismus in einem komplexen Gesamtszenario gespannt.

Danksagungen

Wir bedanken uns für die tatkräftige Unterstützung und produktive Zusammenarbeit bei allen Beteiligten des Projektes „Awareness Labor KMU (ALARM) Informationssicherheit“: der gesamten Forschungsgruppe um Frau Prof. Dr. Scholl (Frauke Prott, Peter Koppatz, Stefanie Gube, Olesja Mujkic), Pilotunternehmen, Unterauftragnehmern, assoziierten Partnern (IHK Ostbrandenburg, IHK Cottbus, IHK Potsdam und DIZ Digitales Innovationszentrum), bei Kolleginnen und Kollegen sowie ehemaligen Mitarbeitenden. Ebenso danken wir für die Förderung des Projektes dem Bundesministerium für Wirtschaft und Klimaschutz sowie dem Projektträger Deutsches Zentrum für Luft- und Raumfahrt.

Literatur

[1] Wilson, Mark und Joan Hash. Building an Information Technology Security Awareness and Training Program. NIST special publication 800-50 (October). Washington D.C.: U.S. Governement Printing Office, 2003. Zuletzt geprüft am 29.12.2021. http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.

[2] Bada, Maria, Angela M. Sasse und Jason R. C. Nurse. „Cyber Security Awareness Campaigns: Why do they fail to change behaviour?," 2019. Zuletzt geprüft am 29.12.2021. https://arxiv.org/ftp/arxiv/papers/1901/1901.02672.pdf.

[3] WIK Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste. „Digitales Handwerk unterschätzt IT-Risiken." Infoblatt (2017). Zuletzt geprüft am 30.01.2019. https://www.wik.org/fileadmin/Sonstige_Dateien/IT-Sicherheit_in_KMU/Infoblatt_Handwerk_-_Aktuelle_Lage_der_IT-Sicherheit_in_KMU_-_WIK_2017.pdf.

[4] Bitkom e. V.. „Bitkom Digital Office Index 2018: Eine Studie zur Digitalisierung von Büro- und Verwaltungsprozessen in deutschen Unternehmen." Berlin, 28. Juni 2018. Zuletzt geprüft am 04.03.2022. https://www.bitkom.org/sites/default/files/file/import/180813-Studienbericht-Bitkom-Digital-Office-Index-2018.pdf.

[5] Pokoyski, Dietmar, Ivona Matas und Ankha Haucke. „Qualitative Wirkungsanalyse Security Awareness in KMU: Tiefenpsychologische Grundlagenstudie im Projekt Awareness Labor KMU (ALARM) Informationssicherheit." Technische Hochschule Wildau, 2021. Zuletzt geprüft am 16.03.2022. https://alarm.wildau.biz/static/d6490e49f8d31adfa35259134b8d1b9d/220316-alarm-studie-final.pdf.

[6] Bundesamt für Sicherheit in der Informationstechnik, Hrsg. „BSI-Standards." Zuletzt geprüft am 29.12.2021. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards_node.html.

[7] Bundesamt für Sicherheit in der Informationstechnik, Hrsg. „BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS)." Version 1.0, 2017. Zuletzt geprüft am 29.12.2021. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-1-Managementsysteme-fuer-Informationssicherheit/bsi-standard-200-1-managementsysteme-fuer-informationssicherheit_node.html.

[8] Bundesamt für Sicherheit in der Informationstechnik, Hrsg. „BSI-Standard 200-2: IT-Grundschutz-Methodik." Version 1.0, 2017. Zuletzt geprüft am 29.12.2021. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-2-IT-Grundschutz-Methodik/bsi-standard-200-2-it-grundschutz-methodik_node.html.

[9] Nurse, Jason R. C., Sadie Creese, Michael Goldsmith und Koen Lamberts. „Guidelines for usable cybersecurity: Past and present." In 2011 Third International Workshop on Cyberspace Safety and Security (CSS 2011): Milan, Italy, 8 September 2011; [held in conjunction with the 5th International Conference on Network and System Security (NSS 2011), in Milan, Italy, September 6 - 8, 2011. Hrsg. von Cliff C. Zou, 21–6. Piscataway, NJ: IEEE, 2011. doi:10.1109/CSS.2011.6058566.

[10] Ertan, Amy, Georgia Crossland, Claude Heath, David Denny und Rikke Bjerg Jensen. „Everyday Cyber Security in Organisations: Literature review." Reviewentwurf übermittelt an das Cabinet Office am 24. April 2018. Zuletzt geprüft am 29.12.2021. https://arxiv.org/ftp/arxiv/papers/2004/2004.11768.pdf.

[11] Schonschek, Oliver. „Security muss an Komplexität verlieren." In Security Insider. Die neue Cybersecurity. 2021.

[12] Bitkom e. V.. „Spionage, Sabotage und Datendiebstahl: Wirtschaftsschutz in der vernetzten Welt. Studienbericht 2020.“ Zuletzt geprüft am 11.11.2021. https://www.bitkom.org/sites/default/files/2020-02/200211_bitkom_studie_wirtschaftsschutz_2020_final.pdf.

[13] Forrester, Hrsg. „The 2020 State Of Security Operations.“ Zuletzt geprüft am 11.11.2021. https://www.paloguard.com/datasheets/forrester-the-2020-state-of-security.pdf.

[14] Porst, Ralf. Fragebogen: Ein Arbeitsbuch. SpringerLink Bücher. Wiesbaden: VS Verlag für Sozialwissenschaften, 2008. Lehrbuch zur Praxis der Fragebogenerstellung. Zuletzt geprüft am 20.08.2021. doi:10.1007/978-3-531-90897-7. http://swbplus.bsz-bw.de/bsz283371803cov.htm.

[15] Ilieva, Janet, Steve Baron und Nigel M. Healey. „Online Surveys in Marketing Research.“ International Journal of Market Research 44, Nr. 3 (2002): 361–376. doi:10.1177/147078530204400303.

[16] Europäische Kommission. „Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen: Aktenzeichen K(2003) 1422.“ In Amtsblatt der Europäischen Union. L 124 (20.05.2003), 36–41. Zuletzt geprüft am 02.06.2021. https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32003H0361&from=DE.

[17] WIK Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste, Hrsg. „Aktuelle Lage der IT-Sicherheit in KMU [2017].“ Zuletzt geprüft am 03.11.2021. https://www.it-sicherheit-in-der-wirtschaft.de/ITS/Redaktion/DE/PDF-Anlagen/Studien/aktuelle-lage-der-it-sicherheit-in-kmu-langfassung.pdf?__blob=publicationFile&v=3.

[18] Bundesministerium für Wirtschaft und Technologie, Hrsg. „IT-Sicherheitsniveau in kleinen und mittleren Unternehmen: Studie im Auftrag des Bundesministeriums fur Wirtschaft und Technologie [2011/2012].“ Deutschland. Zuletzt gepruft am 06.07.2021.

[19] Faulbaum, Frank. Methodische Grundlagen der Umfrageforschung. Lehrbuch. Wiesbaden: VS Verl. Sozialwissenschaften, 2019. Zuletzt geprüft am 30.09.2021. doi:10.1007/978-3-531-93278-1. https://link.springer.com/content/pdf/10.1007%2F978-3-531-93278-1.pdf.

[20] Aussage einer leitenden Person aus den Pilotunternehmen. 16.06.2021. Video-Meeting.

[21] Bundesamt für Sicherheit in der Informationstechnik, Hrsg. „IT-Grundschutz.“ Zuletzt geprüft am 23.04.2021. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html.

[22] Wirtschafts- und Sozialwissenschaftliches Institut (WSI), Hans-Böckler-Stiftung, Hrsg. „Homeoffice: Was wir aus der Zeit der Pandemie für die zukünftige Gestaltung von Homeoffice lernen können.“ WSI Report Nr. 65, April 2021. Zuletzt geprüft am 06.07.2021. https://www.boeckler.de/pdf/p_wsi_report_65_2021.pdf.

[23] Brückler, Franka M. Geschichte der Mathematik kompakt: Das Wichtigste aus Analysis, Wahrscheinlichkeitstheorie, angewandter Mathematik, Topologie und Mengenlehre. Springer eBook Collection. Berlin, Heidelberg: Springer Spektrum, 2018. doi:10.1007/978-3-662-55574-3.

[24] Kuckartz, Udo. Statistik: Eine verständliche Einführung. 2., überarb. Aufl. 2013. Springer eBook Collection. Wiesbaden: VS Verlag für Sozialwissenschaften, 2013. doi:10.1007/978-3-531-19890-3. https://link.springer.com/chapter/10.1007/978-3-531-19890-3_9.

[25] Bortz, Jürgen und Nicola Döring. Forschungsmethoden und Evaluation: Für Human- und Sozialwissenschaftler. 5. Aufl. Berlin: Springer, 2016.

[26] Bock, Hans H. Automatische Klassifikation: Theoretische und praktische Methoden zur Gruppierung und Strukturierung von Daten; (Cluster-Analyse). Studia mathematica 24. Göttingen: Vandenhoeck & Ruprecht, 1974.

[27] Brüggemann, Rainer, Lars Carlsen und Jochen Wittmann, Hrsg. Multi-indicator Systems and Modelling in Partial Order. New York, NY, s.l.: Springer New York, 2014.

[28] Bundesamt für Sicherheit in der Informationstechnik, Hrsg. „Die Lage der IT-Sicherheit in Deutschland 2021." Zuletzt geprüft am 17.12.2021. https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-cybersicherheit-2021.pdf?__blob=publicationFile&v=3.

[29] Bundesministerium des Innern, für Bau und Heimat, Hrsg. „Cybersicherheitsstrategie für Deutschland 2021." Zuletzt geprüft am 12.11.2021. https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf.

[30] Bitkom e. V., Hrsg. „Cybersicherheit & Sicherheitstechnologien: Bitkom-Position zur Bundestagswahl 2021." Zuletzt geprüft am 11.11.2021. https://www.bitkom.org/sites/default/files/2021-08/bitkom_wahlpapier2021_cybersicherheit-sicherheitstechnologien.pdf.

[31] Ruge, Frank und Peter Schmitz. „Die richtige Security-Lösung finden: So klappt es mit der IT-Sicherheit im Mittelstand." Vogel Business Media, 2017. Zuletzt geprüft am 10.06.2021. https://www.security-insider.de/so-klappt-es-mit-der-it-sicherheit-im-mittelstand-a-630567/.

[32] Bundesamt für Sicherheit in der Informationstechnik. „Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen (KMU): Grad der Sensibilisierung des Mittelstandes in Deutschland." 2011; in Zusammenarbeit mit secunet Security Networks. Zuletzt geprüft am 25.03.2021. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/KMU/Studie_IT-Sicherheit_KMU.pdf?__blob=publicationFile.

[33] Beißel, Stefan. Security Awareness: Grundlagen, Maßnahmen und Programme für die Informationssicherheit. De Gruyter STEM. Berlin, Boston: De Gruyter, 2019. doi:10.1515/9783110668261.

Technische Hochschule Wildau
Technical University of Applied Sciences

Ergebnisse einer Umfrage in Pilotunternehemen zur Lage und zum Stand der Informationssicherheit sowie zu sicherheitsrelevanten Tätigkeitsprofilen im Rahmen des Projektes **Awareness Labor KMU (ALARM) Informationssicherheit.**

Projektlaufzeit: 01.10.2020 – 30.09.2023

https://alarm.wildau.biz

ISBN 978-3-949639-01-2