gfs-zürich | MARKT- & SOZIALFORSCHUNG

Schlussbericht 2022:

Auswirkungen der Corona-Krise auf die Digitalisierung und Cybersicherheit in Schweizer KMU

Befragung von Geschäftsführenden kleiner Unternehmen in der Schweiz

Studie im Auftrag von bzw. in Zusammenarbeit mit:

Schweizerische Mobiliar Versicherungsgesellschaft AG
Digitalswitzerland
Allianz Digitale Sicherheit Schweiz
Fachhochschule Nordwestschweiz FHNW, Kompetenzzentrum Digitale Transformation
Schweizerische Akademie der Technischen Wissenschaften SATW

gfs-zürich, Markt- und Sozialforschung

Karin Mändli Lerch (Projektleitung)
Mara Tanner (Projektmitarbeit)

Zürich, 28. Juni 2022

gfs-zürich
Riedtlistrasse 9, 8006 Zürich
Tel. +41 44 360 40 20
Tel. dir. +41 44 360 40 25
E-mail: gfs@gfs-zh.ch
Internet: www.gfs-zh.ch

Inhaltsverzeichnis

1 Management Summary

Im Winter 2021/2022 wurden die Schweizer Arbeitnehmenden ein weiteres Mal aufgrund eines bundesrätlichen Beschlusses zur Eindämmung der Covid-Pandemie ins Homeoffice geschickt. Die Gesundheitskrise förderte grosse Meinungsdifferenzen bezüglich des Umgangs mit Gefahren, Eigenverantwortung und der Rolle des Bundes bzw. der Kantone zutage. So war die Homeoffice-Pflicht für die einen eine Erleichterung, weil sie sich weniger ansteckungsgefährdet fühlten, andere empfanden es als übertriebener Eingriff in ihre persönliche oder unternehmerische Freiheit. Unabhängig von der Pandemie konnte das erzwungene Homeoffice einerseits als organisatorische und/oder emotionale Belastung, oder andererseits als Chance für neue Arbeitsformen und Digitalisierung empfunden werden. Die teilweise sehr schnell eingeführten Lösungen für Homeoffice förderten zudem die Cyberkriminalität, die Gesundheitskrise führte besonders zu ihrer Anfangszeit zu massiv mehr Angriffen.

Vor diesem Hintergrund wurde die dritte Welle zu den Auswirkungen der Corona-Krise auf die Digitalisierung und Cybersicherheit in Schweizer KMU durchgeführt. Es wurden 504 Geschäftsführende von KMU mit 4 bis 49 Mitarbeitenden in der Deutsch-, Französisch- und Italienischsprachigen Schweiz telefonisch befragt.

1.1 Homeoffice-Erschöpfung?

Sowohl die Anzahl der Arbeitsstellen, welche von den Geschäftsführenden als homeoffice-tauglich bezeichnet werden, als auch der Anteil an Mitarbeitenden, die hauptsächlich von zuhause aus arbeiten, sind rückgängig:

- 2020 bezeichneten die Geschäftsführenden durchschnittlich 3.8 Stellen als homeoffice-tauglich, 2021 waren es 3.4 und 2022 noch 2.9. Der Rückgang von 2020 auf 2022 ist signifikant.
- Während den jeweiligen Homeoffice-Pflichtphasen blieben 2020 fast zwei Fünftel der Mitarbeitenden hauptsächlich im Homeoffice (38 %), 2021 ein bisschen weniger (36 %) und 2022 war es noch knapp ein Drittel (32 %). Dieser Rückgang ist nicht signifikant, könnte aber eine Tendenz aufzeigen. Dazu muss aber auch bemerkt werden, dass die Angst vor einer Ansteckung wahrscheinlich von Jahr zu Jahr kleiner wurde und auch dies möglicherweise einen Einfluss hatte auf die Entscheidung, im Homeoffice oder vor Ort zu arbeiten.
- Vor der Pandemie arbeitete ein Zehntel (10 %) der Mitarbeitenden der befragten KMU hauptsächlich im Homeoffice. Zwischen den jeweiligen Homeoffice-Pflichtphasen stieg dieser Anteil auf rund einen Sechstel (2020: 16 %), dann sogar auf einen Fünftel (2021: 20 %) und sank nun im Jahr 2022, als die Pandemie umgangssprachlich für «beendet» erklärt wurde, fast wieder auf ihren Ausgangswert zurück (2022: 12 %).

Diese Ergebnisse lassen auf eine gewisse Homeoffice-Erschöpfung seitens der Arbeitgebenden schliessen und/oder dass sich die Einschätzung darüber, welche Stellen in welchem Masse homeoffice-tauglich sind, verändert hat. Gleichzeitig ist davon auszugehen, dass sich viele Arbeitnehmende an die Vorzüge des Homeoffice gewöhnt haben und diese nun – auch aufgrund des Fachkräftemangels in einigen Branchen – einfordern wollen und können.

Die Pandemie gab den KMU die Möglichkeit, Homeoffice zu testen, aber zum heutigen Zeitpunkt ist ein gewisser Rückzug in alte Muster feststellbar. Das heisst aber nicht, dass das Homeoffice grundsätzlich gescheitert ist. Diese Studie enthält keine Informationen über Arbeitnehmende, die nicht hauptsächlich, sondern «nur» teilzeitlich im Homeoffice arbeiten (hybrides Arbeiten). Dieser Anteil könnte durchaus gewachsen sein und müsste in weiteren Studien untersucht werden.

1.2 Keine Fortschritte bezüglich Cybersicherheitsmassnahmen

Sowohl in der medialen Berichterstattung als auch in der Werbung wurde das Thema Cybersicherheit in den letzten zwei Jahren viel sichtbarer. Trotzdem kann in der dritten Welle dieser Studie keine Entwicklung bezüglich der technischen und organisatorischen Sicherheitsmassnahmen festgestellt werden.

- Technische Massnahmen wurden nach wie vor besser umgesetzt als organisatorische. Die durchschnittlichen Umsetzungsgrade der abgefragten technischen Massnahmen lagen zwischen 3.8 und 4.5 auf einer Fünferskala, auf der 1 «gar nicht umgesetzt» und 5 «voll und ganz umgesetzt» bedeutet. Bei den organisatorischen Massnahmen lagen sie zwischen 2.7 und 4.2.
- Besonders tief waren die Umsetzungsgrade bei den Massnahmen «regelmässige Mitarbeiterschulung» (3.0) und «Durchführung eines Sicherheitsaudits» (2.7).
- Im Vergleich zur Vorwelle 2021 gab es keine Veränderung, tendenziell gingen die Umsetzungsgrade sogar eher zurück.

Erstaunlich ist diese fehlende Entwicklung angesichts der Tatsache, dass das Risiko, von einem Cyberangriff betroffen zu werden und dadurch einen Tag ausser Kraft gesetzt zu werden, stetig höher beurteilt wurde. In der ersten Welle 2020 wurde dieses Risiko auf der Fünferskala mit einer 2.1 bewertet, wobei 1 «sehr kleines Risiko» und 5 «sehr grosses Risiko» bedeutet. 2021 stieg diese Einschätzung auf 2.4 und 2022 auf 2.5. Auch die Risikoeinschätzung, durch einen Cyberangriff in der Existenz bedroht zu werden, stieg auf sehr tiefem Niveau stetig an (2020: 1.5, 2021: 1.7, 2022: 1.9). Die wachsende Risikoeinschätzung scheint aber keinen Einfluss auf die Massnahmenumsetzung zu haben.

Ein starker Zusammenhang konnte mit dem Informationsgrad festgestellt werden: Je informierter sich die Befragten bezüglich Cyberrisiken fühlen, desto höher ist die organisatorische und technische Massnahmenumsetzung. Diese Selbsteinschätzung bezüglich dem Informationsgrad veränderte sich über die drei Wellen aber nicht (2020: 3.4, 2021: 3.5, 2022: 3.5).

Die Wichtigkeitseinschätzung des Themas bewegte sich ebenfalls nicht bzw. ist sogar leicht rückläufig: Der Mittelwert lag 2020 und 2021 bei 3.9 und 2022 bei 3.8; auffälliger ist aber der Rückgang des Skalenwertes 5 («sehr wichtig»), dieser sank von 42 Prozent im Jahr 2020 auf 41 Prozent 2021 und dann auf 35 Prozent im Jahr 2022. Auch dies ist ein eher überraschendes Ergebnis in Anbetracht der häufigen medialen Berichterstattung zum Thema Cyberkriminalität.

Es zeigt sich also eine gewisse Trägheit in der Bearbeitung dieses wichtigen Themas und es fragt sich, wie eine Verhaltensänderung gefördert werden kann, wenn nicht durch die mediale Berichterstattung.

1.3 Bedeutung des IT-Dienstleisters

Bei der Frage nach der Verantwortlichkeit für die Cybersicherheit bezeichneten sich über die Hälfte (55 %) der befragten Geschäftsführenden als selbst verantwortlich. Ein Drittel der Befragten (33 %) nannte einen externen IT-Dienstleister, rund ein Zehntel (11 %) meinte, dass «jede/-r Mitarbeitende» verantwortlich ist, bei rund jedem vierzehnten Unternehmen war «niemand» verantwortlich.

Sowohl die technischen als auch die organisatorischen Massnahmen erreichten höhere Umsetzungsgrade, wenn der/die Geschäftsführende oder ein IT-Dienstleister als verantwortlich bezeichnet wurde. Der grösste Zusammenhang konnte dabei beim IT-Dienstleister festgestellt werden.

Eine entsprechende Zusammenarbeit ist also im Sinne einer höheren Cyberresilienz empfehlenswert; allerdings dürfen die organisatorischen Massnahmen dabei nicht vergessen gehen, da anzunehmen ist, dass der Fokus von IT-Dienstleistern oftmals eher auf den technischen Massnahmen liegt. Die Geschäftsführenden von KMU werden also – trotz scheinbar eher tiefer Begeisterung – nicht um das Thema Cybersicherheit herumkommen.

2 Ausgangslage und Ziele

2.1 Mandat und Fragestellung

Im Winter 2021/2022 wurden die Schweizer Arbeitgeberinnen und Arbeitgeber ein weiteres Mal durch einen bundesrätlichen Beschluss verpflichtet, ihre Mitarbeitenden ins Homeoffice zu schicken «…wo dies aufgrund der Art der Aktivität möglich und mit verhältnismässigem Aufwand umsetzbar ist». (Verordnung über Massnahmen in der besonderen Lage zur Bekämpfung der Covid-19-Epidemie, 17.12.2021, Art. 25, Abs. 5). Die Homeoffice-Pflicht galt vom 20. Dezember 2021 bis zum 3. Februar 2022 und wurde dann in eine Empfehlung umgewandelt, wobei der Schutz vor einer Ansteckung am Arbeitsplatz immer noch gewährt werden musste, beispielsweise mit einer Maskenpflicht am Arbeitsplatz. Die Kontaktquarantäne wurde zum gleichen Zeitpunkt aufgehoben bzw. auf die Mitglieder desselben Haushalts beschränkt.

Unter diesen Voraussetzungen wurde die dritte Welle der hier vorliegenden Befragung durchgeführt, um die Einstellung der KMU-Geschäftsführenden zu Homeoffice und Cyberrisiken und deren Entwicklung zu messen.

Die Projektgruppe besteht aus Mitarbeitenden von Die Mobiliar (Patric Vifian), digitalswitzerland (Andreas Kaelin), der Fachhochschule Nordwestschweiz FHNW (Marc K. Peter), der Schweizerischen Akademie der Technischen Wissenschaften SATW (Nicole Wettstein) und gfs-zürich (Karin Mändli Lerch).

2.2 Befragung und Stichprobe

Die telefonische Befragung wurde vom 28. Februar bis 30. März 2022 mit Geschäftsführenden von kleinen Unternehmen (4 bis 49 Mitarbeitende) in der deutsch-, französisch- und italienischsprachigen Schweiz durchgeführt.

Die durch die Stichprobe abgebildete Grundgesamtheit umfasst **rund 153'000 Firmen** mit 4 bis 49 Mitarbeitenden in allen Landesteilen. Das Vertrauensintervall der Gesamtstichprobe liegt bei +/- 4.4 Prozent bei einer Sicherheit von 95 Prozent (50/50 Verteilung). Die Erhebung zeigt ein strukturgleiches Abbild der Grundgesamtheit, die Ergebnisse sind somit unter Berücksichtigung des Vertrauensintervalls auf die Grundgesamtheit extrapolierbar.

Die Stichprobe wurde proportional zu den Firmengrössen erhoben. Dabei wurde die Verteilung der drei Grössenkategorien (nach Anzahl Mitarbeitenden) mittels Quotensteuerung sichergestellt; die Verteilung nach Grossregion wurde mittels Adress-Vorschichtung erzielt. Die nachfolgende Tabelle zeigt die Verteilung der Interviews im Vergleich zur Verteilung der untersuchten Unternehmensgrössen in der Schweiz.

	Effektiver Anteil (BFS / STATENT 2017)	Stichprobe nach Quotierung: n=504
4-9 Beschäftigte	66 %	327 (65 %)
10-19 Beschäftigte	22 %	111 (22 %)
20-49 Beschäftigte	12 %	66 (13 %)
	Effektiver Anteil (BFS / STATENT 2017)	Stichprobe nach vorgeschichteten Adressen:
Espace Mittelland	20 %	110 (22 %)
Genferseeregion	19 %	146 (29 %)
Zürich	16 %	48 (10 %)
Ostschweiz	14 %	63 (13 %)
Nordwestschweiz	12 %	42 (8 %)
Zentralschweiz	12 %	50 (10 %)
Tessin	6 %	45 (9 %)

Die Adressen stammen von einem Schweizer Adressbroker aus einem Potenzial von über 100'000 Adressen.

Die Ausschöpfung liegt bei eher tiefen 3.6 %:

Realisiert Interviews	504
Verweigerung	13'554
Termine	521
Keine Antwort	2'907
Besetzt	201
Anrufbeantworter	1'024
Quote Komplet/Nicht Zielgruppe	700
Fax/Geschäft/Nicht existent	3281
nicht erreichbar während der Feldzeit	172
Sprachprobleme	45
Total	22'909

Berechnung Ausschöpfung:
22'909 - Summe aller nicht-kontaktierten Adressen (8'851) = 14'058
504 / 14'058 = 3.6 %

3 Ergebnisse

Im folgenden Kapitel werden die Ergebnisse der telefonischen Befragung erläutert.

Allgemeiner Lesehinweis zu den Grafiken: Subgruppen, die weniger als 30 Interviews enthalten, werden als Warnhinweis mit * gekennzeichnet, um einer Überinterpretation vorzubeugen. Subgruppen mit n ≥ 20 werden noch abgebildet, Subgruppen <20 nicht mehr.

Die Prozentzahlen sind auf ganze Zahlen gerundet, es können deshalb kleine Rundungsdifferenzen entstehen.

3.1 Erklärung der Subgruppen

Die Resultate sind nach verschiedenen Subgruppen aufgeschlüsselt. Beispielsweise die Unternehmensgrössenkategorie nach Anzahl Mitarbeitenden oder die geografische Region. Bei zwei Subgruppen, nämlich der Einstellung zu technischen Innovationen und der Sicherheitsmassnahmenumsetzung, sind weitere Erläuterungen notwendig:

3.1.1 Einstellung zu technischer Innovation (Pioniere, Early- und Late Follower)

Um die Resultate nach der persönlichen Aufgeschlossenheit gegenüber technischen Innovationen aufschlüsseln zu können, teilten die Befragten ihr Unternehmen gemäss einer Typologie ein, die ihnen vorgelesen wurde:

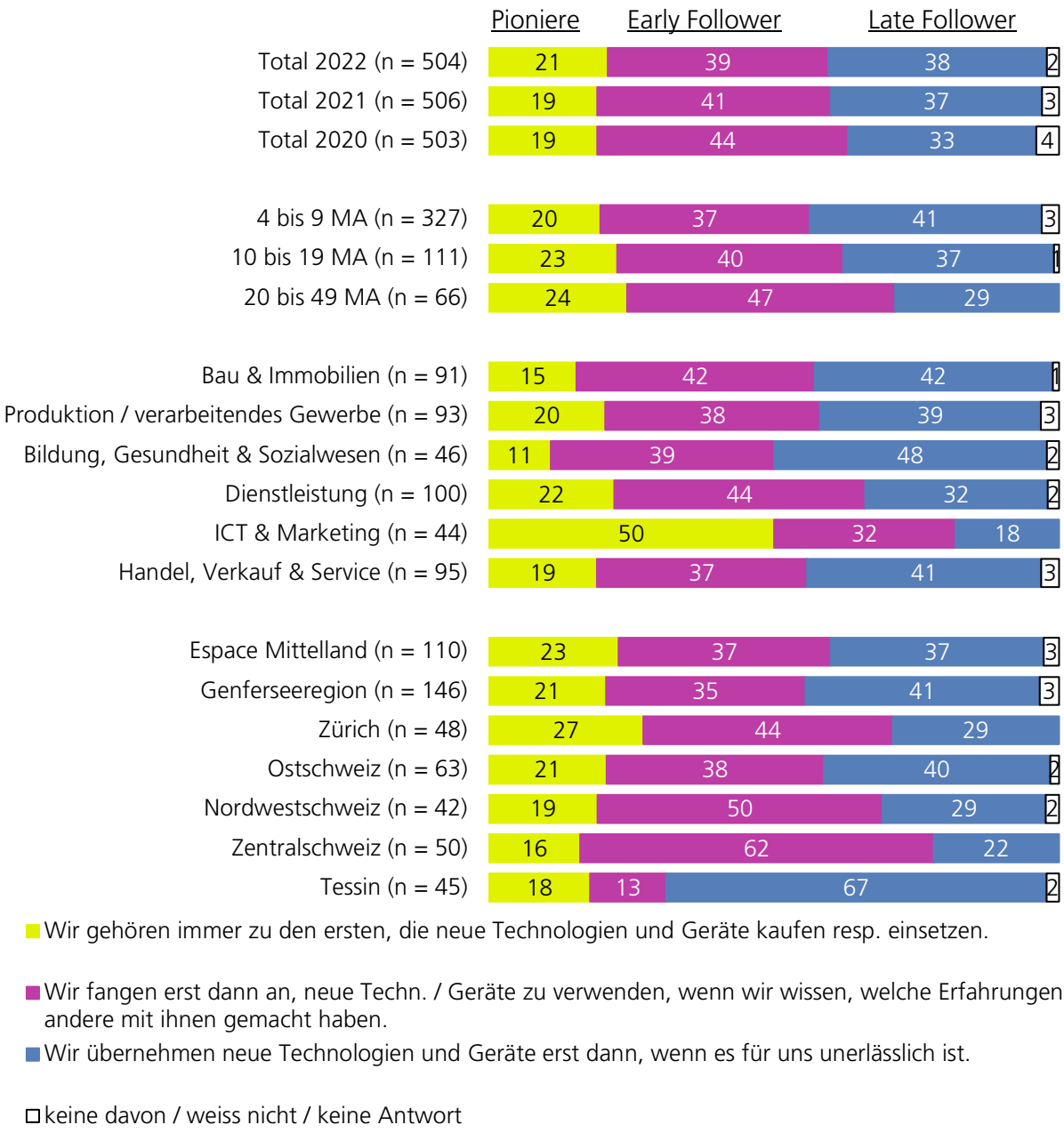
- Wir gehören immer zu den ersten, die neue Technologien und Geräte kaufen resp. einsetzen.
- Wir fangen erst dann an, neue Technologien / Geräte zu verwenden, wenn wir wissen, welche Erfahrungen andere mit ihnen gemacht haben.
- Wir übernehmen neue Technologien und Geräte erst dann, wenn es für uns unerlässlich ist.

Je nach Antwort wurden die Befragten in die drei Subgruppen «Pioniere», «Early Follower» und «Late Follower» eingeteilt.

Die Resultate von 2022 sind denjenigen von 2021 und 2020 sehr ähnlich: Rund ein Fünftel der Befragten zählt sich zur Gruppe der Pioniere (2022: 21 %, 2021: 19 %, 2020: 19 %), rund zwei Fünftel zur Gruppe der Early Follower (2022: 39 %, 2021: 41 %, 2020: 44 %), und rund ein Drittel zu den Late Followern (2022: 38 %, 2021: 37 %, 2020: 33 %).

Pioniere finden sich am ehesten, wie schon 2021 und 2020, in der Branche ICT & Marketing (50 %). Die anderen Branchen verfügen mit rund einem Zehntel bis einem Fünftel über signifikant weniger Pioniere (Werte siehe Grafik 1). Der höchste Anteil an Late Followern findet sich in der Branche Bildung, Gesundheit & Sozialwesen (48 %).

Im Tessin bezeichnen sich besonders viele Befragte als Late Follower (67 %, gleicher Wert wie 2021), dafür besonders wenige als Early Follower (13 %). Am häufigsten findet man die Gruppe der Pioniere in Zürich (2022: 27 %, 2021: 24 %).



Grafik 1

3.1.2 Sicherheitsmassnahmenumsetzung

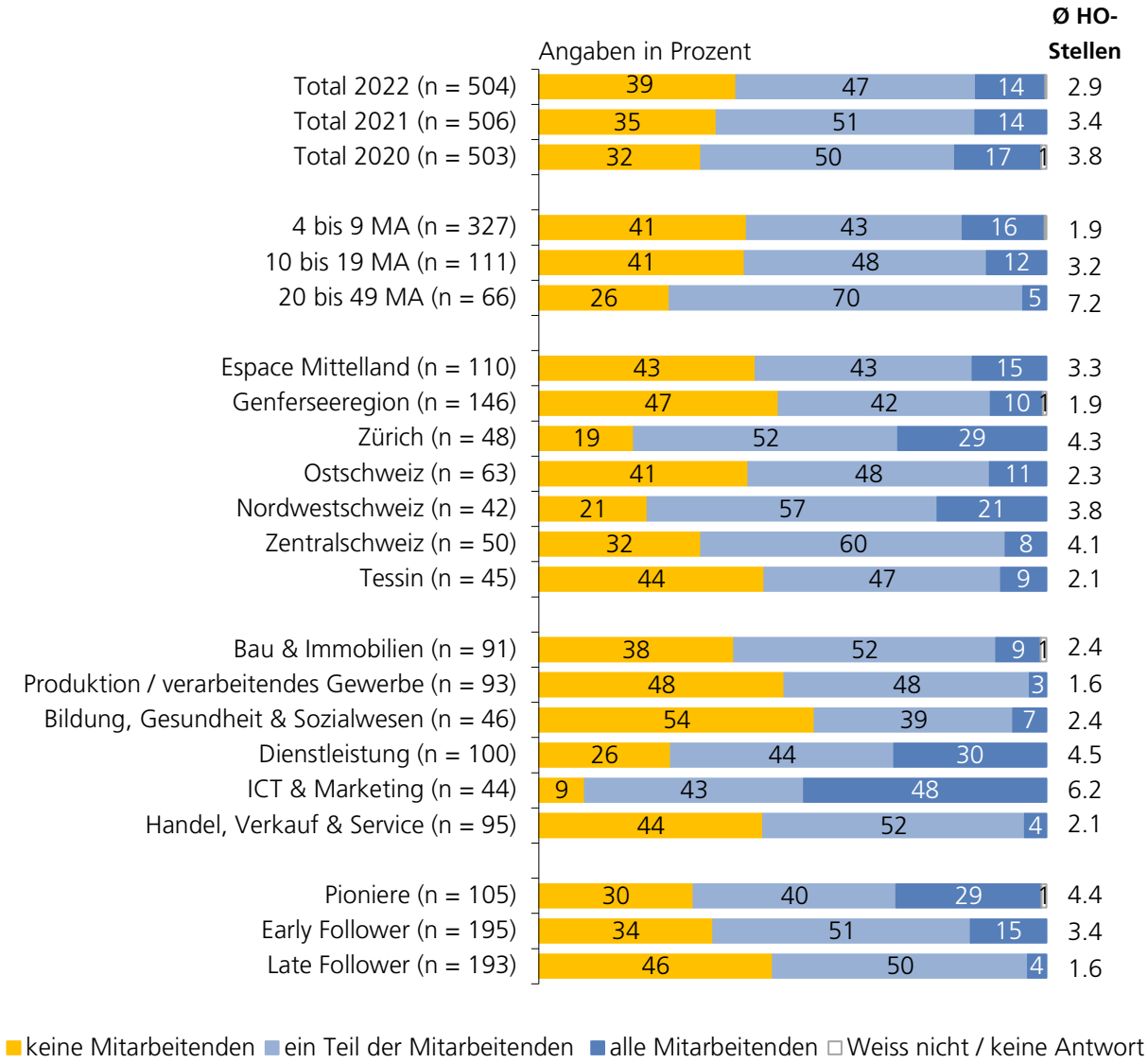
Im Fragenblock zur Cybersicherheit wurden verschiedene technische und organisatorische Sicherheitsmassnahmen nach deren Umsetzungsgrad auf einer Fünferskala abgefragt (siehe Kapitel 3.4.6 und 3.4.8). Für die Bildung der Subgruppe wurde der Durchschnitt aller technischen bzw. organisatorischen Massnahmen berechnet: Durchschnittswerte von 1 bis 3 gelten als tiefe Massnahmenumsetzung, der Durchschnittswert 4 als mittlere Massnahmenumsetzung, der Durchschnittswert 5 als hohe Massnahmenumsetzung.

3.2 Stellenwert und Nutzung des Homeoffice

3.2.1 Potenzial an Homeoffice-Stellen

Die Homeoffice-Pflicht galt für Arbeitsstellen, bei denen Homeoffice «…aufgrund der Art der Aktivität möglich und mit verhältnismässigem Aufwand umsetzbar» war. In dieser Studie zeigen sich seit 2020 stetig weniger homeoffice-taugliche Stellen: 2020 waren es durchschnittlich 3.8, 2021 3.4 und 2022 noch 2.9. Der Rückgang von 2020 auf 2022 ist signifikant und könnte entweder eine gewisse Homeoffice-Erschöpfung seitens der Arbeitgebenden, oder eine veränderte Einschätzung über die Homeoffice-Tauglichkeit der Arbeitsstellen aufgrund vergangener Erfahrungen zeigen. Die Branchen Dienstleistung (4.5) und ICT & Marketing (6.2) verfügen über überdurchschnittlich viele Arbeitsstellen, die vom Homeoffice aus erledigt werden können, während die Branchen Produktion & verarbeitendes Gewerbe (1.6) und Handel, Verkauf und Service (2.1) nur wenige solche Arbeitsstellen anbieten können.

Frage 1:
Wie viele von Ihren Mitarbeitenden können theoretisch von zuhause aus arbeiten, müssen also z.B. keine Kunden vor Ort bedienen, ein Fahrzeug lenken oder auf einer Baustelle arbeiten?
Basis: Total, n = 504



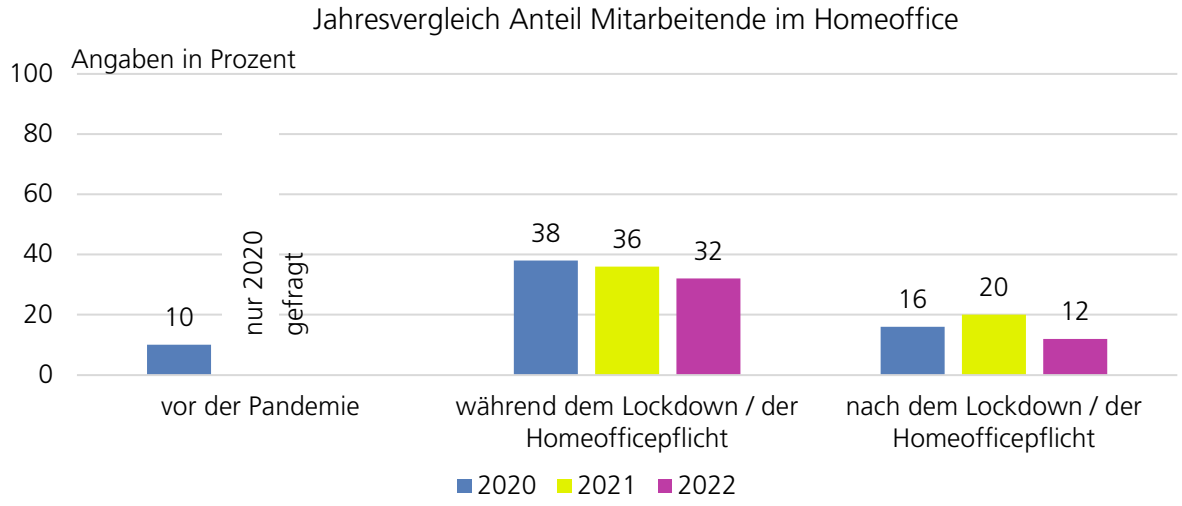
Grafik 2

3.2.2 Veränderung Homeoffice-Gewohnheiten während Homeoffice-Pflicht

Frage 2:
Wie viele Ihrer Mitarbeiter haben zwischen dem 20. Dezember 2021 und dem 2. Februar 2022 **hauptsächlich** von zuhause aus gearbeitet, also währenddem die Homeoffice-Pflicht galt?
Und wie viele arbeiten jetzt, nach der Homeoffice Pflicht, hauptsächlich von zuhause aus?
Filter: Mindestens ein/e Mitarbeiter/in kann theor. im Homeoffice arbeiten, n = 307

Die Frageformulierung nach der Anzahl Mitarbeitenden im Homeoffice während und nach der Homeoffice-Pflicht hat sich im Laufe der drei Studien den jeweiligen Tatsachen angepasst. So wurde bei der ersten Welle 2020 noch von einem «Lockdown» gesprochen, der deutlich weiter ging als die Massnahmen während den späteren beiden Phasen der Homeoffice-Pflicht (Studien 2021 und 2022).
Die folgende Grafik zeigt den prozentualen Anteil von Mitarbeitenden, die vor der Pandemie, während den Homeoffice-Pflichtphasen in allen drei Jahren und nach diesen jeweiligen Pflichtphasen. Während vor der Pandemie 2020 noch jede/-r zehnte Mitarbeitende (10 %) hauptsächlich im Homeoffice gearbeitet hatte, war es nach der ersten Welle bereits rund jede/r sechste (16 %). Nach der zweiten Welle 2021 blieb sogar jede/-r fünfte Mitarbeitende (20 %) im Homeoffice. 2022, nach der dritten Welle, gibt es allerdings einen signifikanten Rückgang auf nur noch jede/-n achte/-n Mitarbeitende/-n (12 %), der/die nach der Homeoffice-Pflicht trotzdem noch hauptsächlich vom Homeoffice arbeitet. Während den jeweiligen Pflichtphasen ist der Anteil an Mitarbeitenden im Homeoffice ebenfalls leicht (nicht-signifikant) zurückgegangen (2020: 38 %, 2021: 36 %, 2022: 32 %).

Dieser Rückgang kann an den unterschiedlichen Realitäten liegen, die während den Befragungsphasen galten. So verlor die Pandemie mit der Zeit ihren Schrecken, die Todeszahlen waren 2022 aufgrund der Omikron-Variante deutlich tiefer und es wurde absehbar, dass die Intensivstationen leerer würden. Gleichzeitig ist es auch möglich, dass eine gewisse Homeoffice-Erschöpfung sowohl seitens Vorgesetzter als auch seitens Mitarbeitenden entstand. Zudem ist zu beachten, dass die Fragestellung auf «hauptsächlich» von zuhause aus arbeitenden Mitarbeitenden ausgerichtet ist. Es ist anzunehmen, dass es einen – evt. gewachsenen – Anteil an Mitarbeitenden gibt, der «teilweise», aber eben nicht «hauptsächlich» von zuhause aus arbeitet.

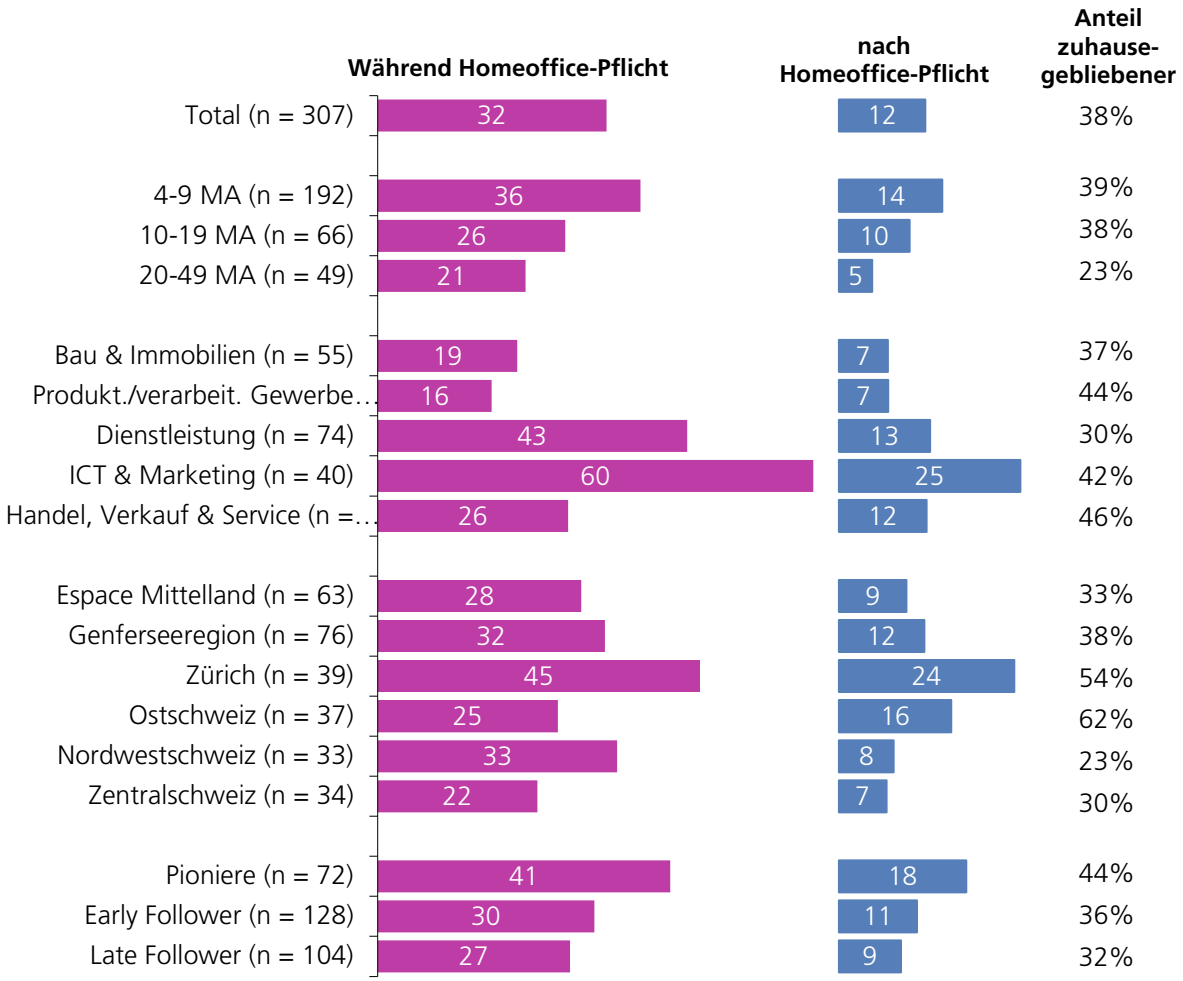


Grafik 3

Von allen befragten Unternehmen, die über mindestens eine homeoffice-taugliche Stelle verfügen, sind während der Homeoffice-Pflicht rund ein Drittel (32 %) der Mitarbeitenden daheim geblieben. In Unternehmen mit 4 bis 9 Mitarbeitenden war der Anteil höher (36 %) als in Unternehmen mit 10 bis 19 Mitarbeitenden (26 %) bzw. mit 20 bis 49 Mitarbeitenden (21 %). Auch nach der Homeoffice-Pflicht blieb der Anteil in den kleinen Unternehmen am höchsten (4–9 Mitarbeitende: 14 %), gefolgt von den mittleren Unternehmen (10–19 Mitarbeitende: 10 %) und den grössten abgefragten Unternehmen (20–49 Mitarbeitende: 5 %).

Besonders hoch war der Anteil an Mitarbeitenden im Homeoffice während der Homeoffice-Pflicht in der Branche ICT & Marketing (60 %), wo auch danach noch ein Viertel der Mitarbeitenden (25 %) weiterhin zuhause arbeitete. Auch die Branche Dienstleistungen verzeichnet einen hohen Anteil Homeoffice: Rund zwei Fünftel (43 %) der Mitarbeitenden blieben während der Homeoffice-Pflicht daheim, und auch danach blieb gut ein Achtel (13 %) hauptsächlich im Homeoffice.

Angaben in Prozent der Mitarbeitenden (Verhältnis zu Mitarbeiteranzahl)



Grafik 4

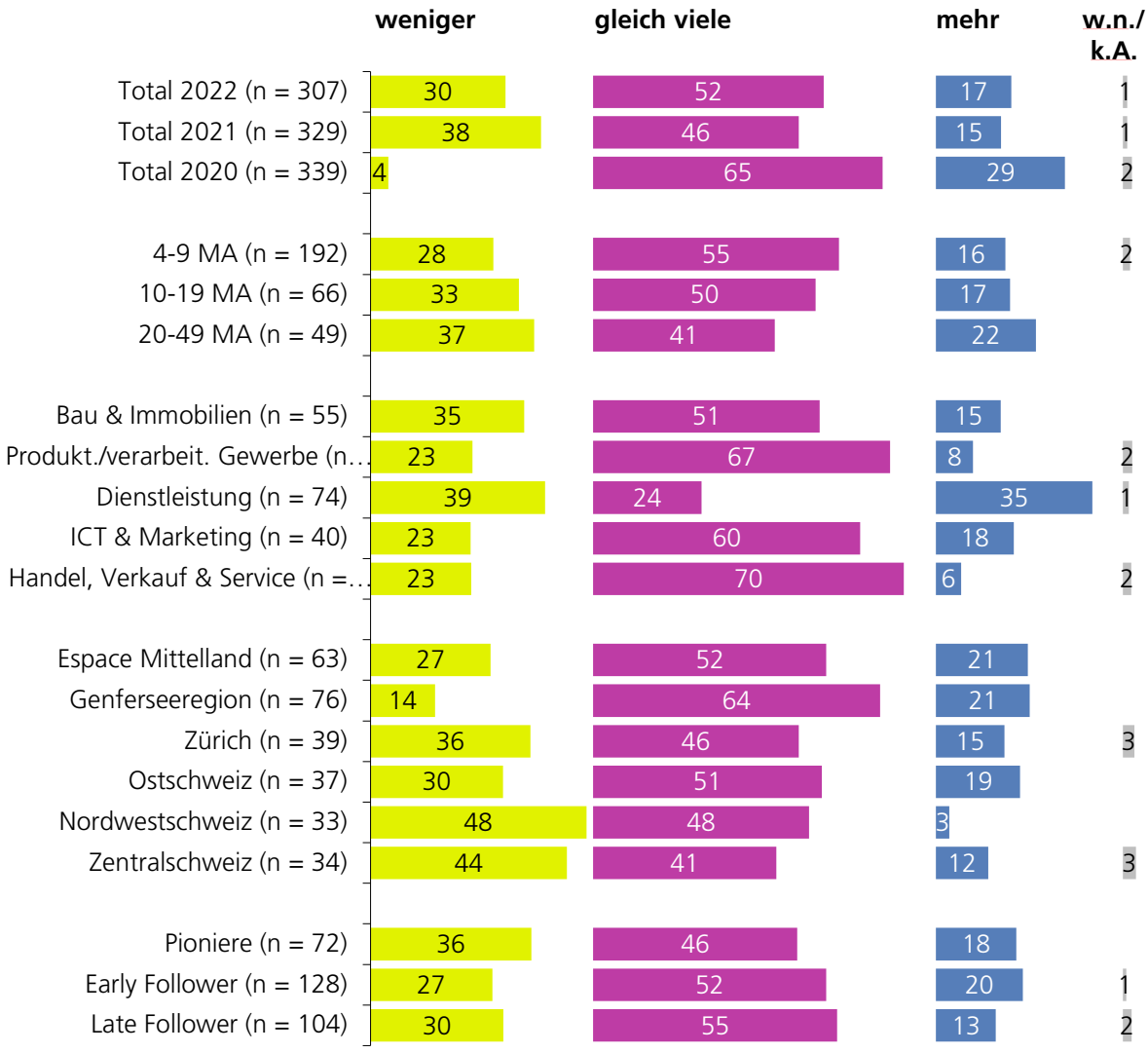
Je aufgeschlossener die befragten Geschäftsführenden ihr Unternehmen bezüglich technischer Innovationen bezeichnen, desto eher haben die Mitarbeitenden im Homeoffice gearbeitet. Bei den Pionieren war es während der Homeoffice-Pflicht rund zwei Fünftel (41 %), bei den Early-Followern rund ein Drittel (30 %) und bei den Late Followern rund ein Viertel (27 %). Nach der

Pflicht verblieb bei den Pionieren rund ein Fünftel (18 %), bei den Early und Late Followern rund ein Zehntel (11 bzw. 9 %) im Homeoffice.

3.2.3 Einschätzung der Entwicklung der Homeoffice-Arbeitsplätze

Während nach der ersten Homeoffice-Pflichtphase noch fast jede/r dritte Geschäftsführende (29 %) der Meinung war, dass zukünftig mehr Mitarbeitende im Homeoffice arbeiten würden, waren es 2021 nur noch halb so viele (15 %). 2022 verbleibt dieser Anteil auf gleichem Niveau (17 %). Rund jede/-r dritte Geschäftsführende (30 %) erwartet zukünftig weniger Mitarbeitende im Homeoffice. Etwas mehr als die Hälfte (52 %) der Befragten geht davon aus, dass sich der Anteil an Homeoffice-Mitarbeitenden eingependelt hat, es also zukünftig gleich viele bleiben werden.

Frage 3:
Wie schätzen Sie die langfristige Entwicklung ein: Werden in Ihrer Firma in Zukunft mehr, gleich viele oder weniger Mitarbeitende von zuhause aus arbeiten als während der Pandemie?
Filter: Wenn mindestens ein/e Mitarbeiter/in theoretisch im Homeoffice arbeiten kann, n = 307



Grafik 5

Je mehr Mitarbeitende in einem Unternehmen arbeiten, desto weniger gehen die Geschäftsführenden von einem gleichbleibendem Homeoffice-Anteil aus: Nur rund zwei Fünftel (41 %) der Unternehmen mit 20 bis 49 Mitarbeitenden erwarten zukünftig gleich viele Mitarbeitende im Homeoffice, knapp zwei Fünftel (37 %) gehen von einem sinkenden Anteil und rund ein Fünftel (22 %) von einem steigenden Anteil aus. Bei den kleinsten Unternehmen (4–9 Mitarbeitende) erwartet mehr als die Hälfte der Geschäftsführenden (55 %) einen gleichbleibenden Homeoffice-Anteil, bei den mittleren (10–19 Mitarbeitende) genau die Hälfte (50 %).

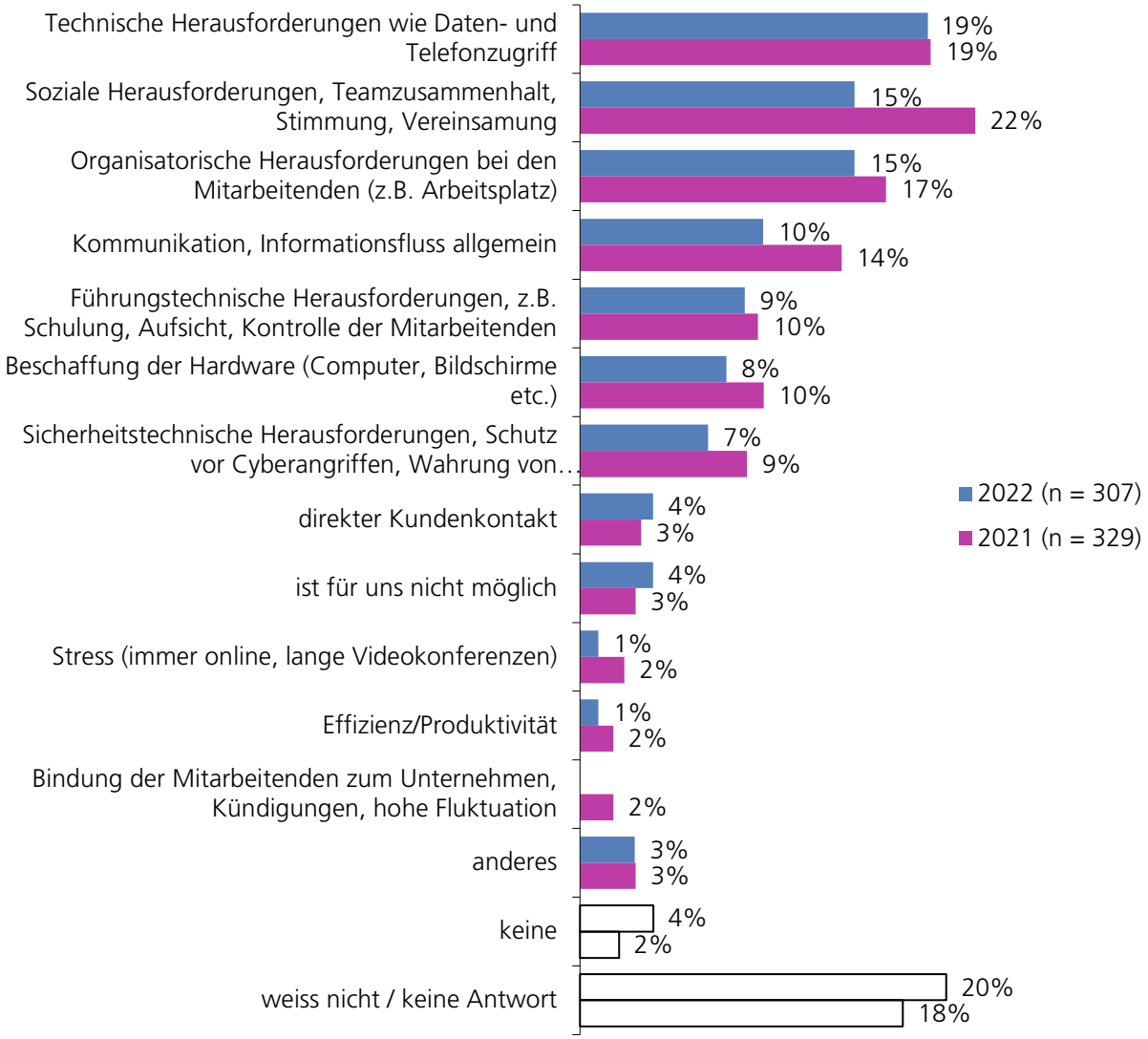
Beim Branchenvergleich zeigt sich die Branche Dienstleistungen als Ausreisser. Nur rund ein Viertel (24 %) und damit signifikant weniger als bei den anderen Branchen geht von gleich vielen Homeoffice-Mitarbeitenden in der Zukunft aus. Fast zwei Fünftel (39 %) erwarten weniger, rund ein Drittel (35 %) erwartet mehr Homeoffice-Mitarbeitende.

3.2.4 Grösste Herausforderungen bei der Umstellung auf Homeoffice

Gegenüber 2021 ist die Beurteilung fast aller Herausforderungen gesunken, was ein Zeichen der mittlerweile entschärften Situation sein dürfte. Wurden 2021 durchschnittlich noch 1.4 Herausforderungen genannt, waren es 2022 derer noch 1.2.

Frage 4:
Was sind aus unternehmerischer Sicht die grössten Herausforderungen bei der Umsetzung des Homeoffice?
Filter: Mindestens ein/e Mitarbeiter/in kann theoretisch im Homeoffice arbeiten, offene/vorcodierte Frage, n = 307

Am deutlichsten zurück ging die Beurteilung der sozialen Herausforderungen, Teamzusammenhalt, Stimmung, Vereinsamung (2021: 22 %, 2022: 15 %). Dieser Aspekt fällt damit von Rang 1 auf Rang 2 zurück, wo er gemeinsam mit den organisatorischen Herausforderungen (ebenfalls 15 %) liegt. Die «technischen Herausforderungen wie Daten- und Telefonzugriff» rücken damit neu auf Rang 1 vor mit einem gegenüber 2021 unveränderten Wert (2021 und 2022: 19 %).


Technische Herausforderungen wie Daten- und Telefonzugriff
19%
19%
Soziale Herausforderungen, Teamzusammenhalt, Stimmung, Vereinsamung
15%
22%
Organisatorische Herausforderungen bei den Mitarbeitenden (z.B. Arbeitsplatz)
15%
17%
Kommunikation, Informationsfluss allgemein
10%
14%
Führungstechnische Herausforderungen, z.B. Schulung, Aufsicht, Kontrolle der Mitarbeitenden
9%
10%
Beschaffung der Hardware (Computer, Bildschirme etc.)
8%
10%
Sicherheitstechnische Herausforderungen, Schutz vor Cyberangriffen, Wahrung von…
7%
9%
direkter Kundenkontakt
4%
3%
ist für uns nicht möglich
4%
3%
Stress (immer online, lange Videokonferenzen)
1%
2%
Effizienz/Produktivität
1%
2%
Bindung der Mitarbeitenden zum Unternehmen, Kündigungen, hohe Fluktuation
2%
anderes
3%
3%
keine
4%
2%
weiss nicht / keine Antwort
20%
18%
2022 (n = 307)
2021 (n = 329)

Grafik 6

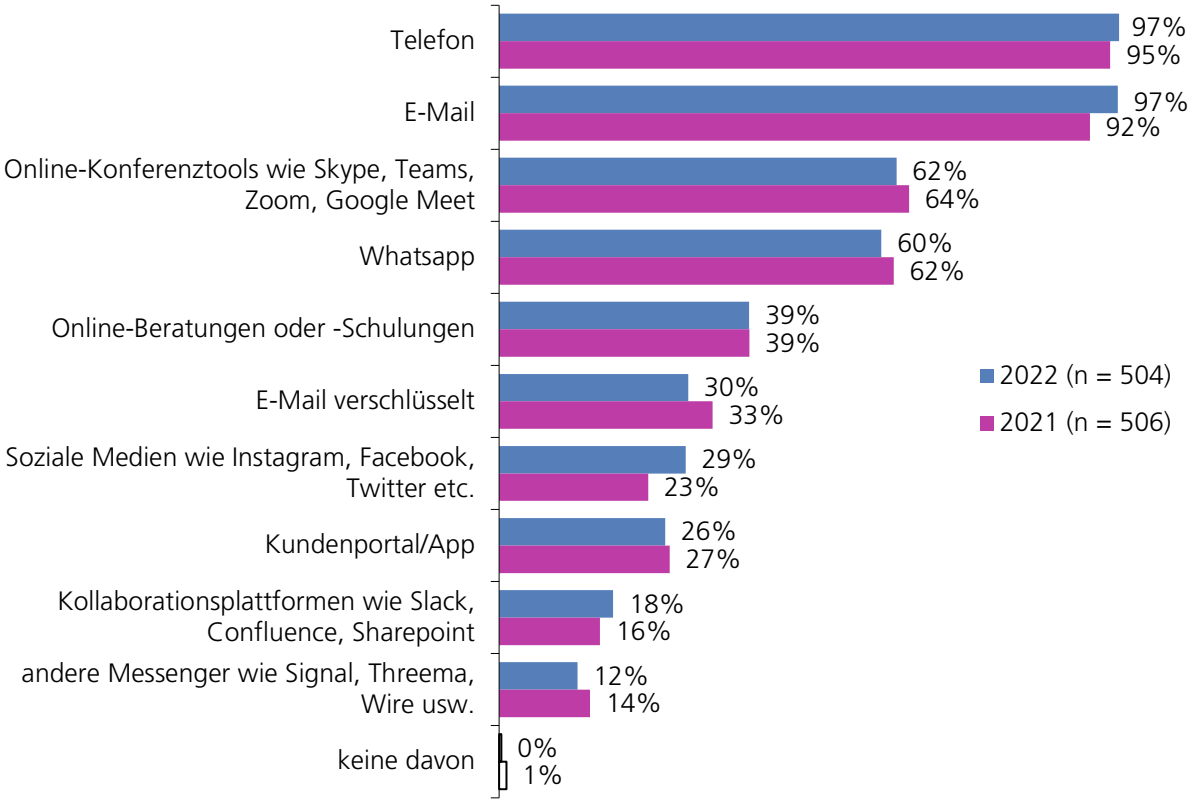
3.3 Kommunikation

3.3.1 Nutzung digitaler Kommunikationsmittel

Telefon (97 %) und E-Mail (97 %) sind auch 2022 die am häufigsten verwendeten Kommunikationsmittel der befragten Unternehmen. Gegenüber dem Jahr 2021 gibt es nur marginale Veränderungen. Ein Vergleich zu 2020 ist nur mit Vorbehalt möglich, da damals teilweise andere Antwortkategorien vorgelesen wurden.

Frage 5:
Ich lese Ihnen jetzt einige digitale Kommunikationsmittel vor. Welche davon nutzen Ihre Mitarbeitenden aktuell für Partner, Kundschaft und anderen Mitarbeitende?
Basis: Total, n = 504, geschlossene Frage, Mehrfachnennungen möglich

Die Verwendung von Online-Konferenztools stieg damals von knapp der Hälfte (46 %) Prozent auf knapp zwei Drittel (64 %) und stagniert jetzt (62 %). Auch Online-Beratungen oder -Schulungen stiegen von 2020 auf 2021 auf knapp zwei Fünftel (2020: 20 %, 2021: 39 %) und bleiben nun auf diesem Wert (2022: 39 %).



Grafik 7

Online Konferenztools (91 %), Online-Beratungen bzw. -Schulungen (64 %) und Kollaborationsplattformen (64 %) werden in der ICT & Marketingbranche deutlich häufiger verwendet als in allen anderen Branchen. Diese Branche nutzt generell mehr Kommunikationsmittel als die anderen; durchschnittlich sind es 6.0, während es bei den anderen Branchen 4.3 bis 4.9 sind. Es gilt auch: Je mehr Mitarbeitende ein Unternehmen hat und je mehr Mitarbeitende im Homeoffice arbeiten können, desto mehr Kommunikationsmittel werden verwendet. So verwenden Unternehmen mit 4 bis 9 Mitarbeitenden durchschnittlich 4.5 Kommunikationsmittel, Unternehmen mit 10 bis 19

Mitarbeitenden 4.8 und Unternehmen mit 20 bis 49 Mitarbeitenden 5.2. Unternehmen **ohne** homeoffice-taugliche Arbeitsstellen nutzen durchschnittlich 4 verschiedene Kommunikationsmittel, Unternehmen **mit einem Teil** homeoffice-tauglichen Arbeitsplätzen nutzen derer 4.9 und Unternehmen mit **ausschliesslich** homeoffice-tauglichen Stellen 5.7. Auch die Einstellung zu technischen Innovationen zeigt sich in der Anzahl genutzter Kommunikationsmittel: Pioniere nutzen durchschnittlich 5.7 verschiedene Kommunikationsmittel, Early Follower 5.0 und Late Follower 3.9.

3.4 Cybersicherheit

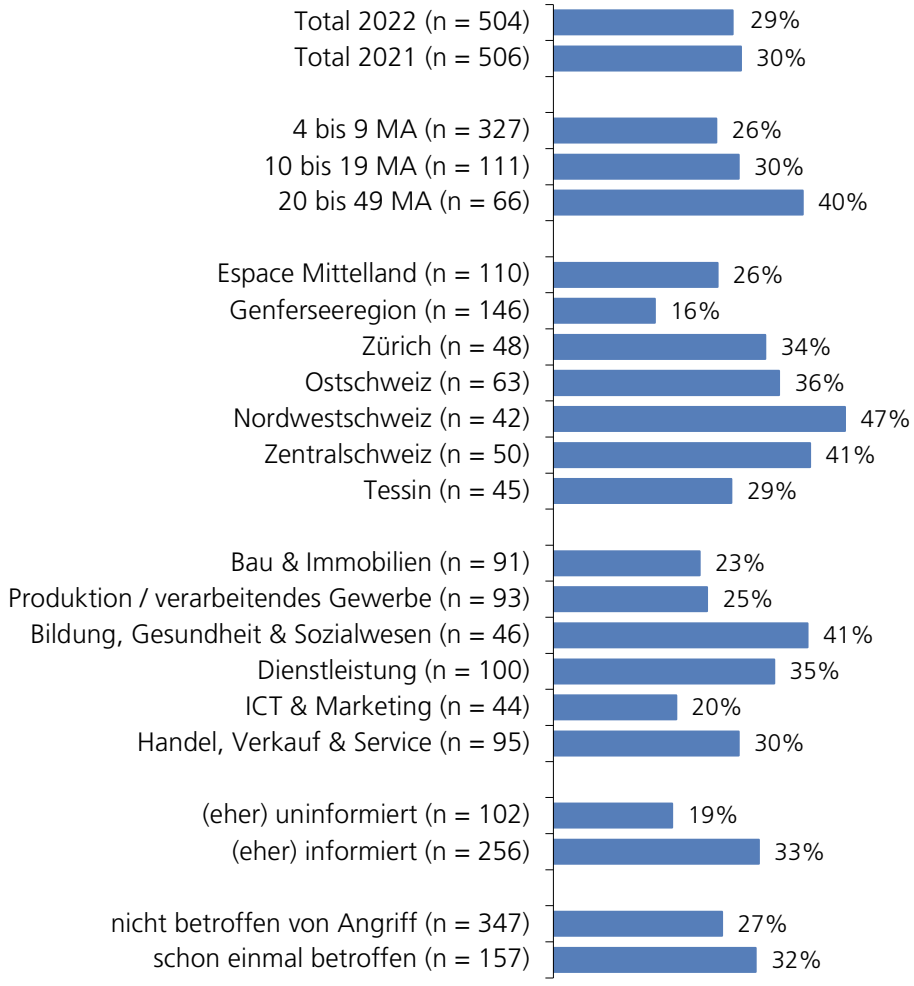
3.4.1 Outsourcen von IT-Arbeiten

Durchschnittlich wird knapp ein Drittel bzw. etwas mehr als ein Viertel (29 %) der IT-Arbeiten von den befragten Unternehmen an externe Dienstleister vergeben, dieser Wert hat sich seit der letzten Welle nicht verändert (2021: 30 %).

Frage 6:
Wieviel Prozent der IT-Arbeiten werden bei Ihnen ungefähr von externen Dienstleistern wahrgenommen?
Basis: Total, n = 504

Auch im Subgruppenvergleich gibt es keine nennenswerten Veränderungen gegenüber der Vorwelle. Je grösser die Unternehmen sind, desto eher vergeben sie IT-Aufgaben auswärts: Bei den kleinsten Unternehmen (4–9 Mitarbeitende) sind es etwas mehr als ein Viertel (2022: 26 %, 2021: 27 %) der IT-Arbeiten, bei den mittleren Kategorie (10–19 Mitarbeitende) rund ein Drittel (2022: 30 %, 2021: 33 %) und bei der grössten Kategorie (20–49 Mitarbeitende) zwei Fünftel (2022: 40 %, 2021: 38 %). Der Unterschied zwischen den grössten und kleinsten Unternehmen ist 2022 signifikant.

Die Outsourcing-Rate ist in der Nordwest- (47 %) und Zentral-Schweiz (41 %) am höchsten, in der Genferseeregion (16 %) am tiefsten.



Grafik 8

Je mehr Mitarbeitende ein Unternehmen beschäftigt und je mehr Homeoffice-taugliche Stellen vorhanden sind, desto eher werden IT-Arbeiten nach extern verlegt: Unternehmen mit 4 bis 9 Mitarbeitenden geben durchschnittlich rund einen Viertel (26 %) ihrer IT-Arbeiten auswärts, Unternehmen mit 10 bis 19 Mitarbeitenden rund einen Drittel (30 %) und Unternehmen mit 20 bis 49 Mitarbeitenden zwei Fünftel (40 %) (Unterschiede von den grössten zu den kleinsten Unternehmen signifikant). Unternehmen ohne homeoffice-taugliche Stellen geben durchschnittlich rund einen Fünftel (21 %) IT-Arbeiten auswärts, Unternehmen mit einem Teil homeoffice-tauglicher Stellen rund einen Drittel (32 %) und Unternehmen mit ausschliesslich homeoffice-tauglichen Stellen knapp zwei Fünftel (37 %) (die Werte der mittleren und oberen Kategorie unterscheiden sich signifikant von der untersten Kategorie).

Je höher der Anteil an auswärts gegebenen IT-Arbeiten ist, desto höher ist auch die durchschnittliche Umsetzung von technischen und organisatorischen Cyber-Sicherheitsmassnahmen. Unternehmen mit tiefer technischer Massnahmenumsetzung haben durchschnittlich knapp einen Fünftel (19 %) ihrer IT-Arbeiten auswärts gegeben, Unternehmen mit hoher Massnahmenumsetzung knapp zwei Fünftel (38 %). Ein ähnliches Bild ergibt sich bei den organisatorischen Massnahmen: Unternehmen mit tiefer organisatorischer Massnahmenumsetzung haben knapp einen Viertel (23 %) der IT-Arbeiten einem externen Dienstleister gegeben, Unternehmen mit hoher organisatorischer Massnahmenumsetzung knapp zwei Fünftel (37 %). Diese Verhältnisse waren in der Vorwelle 2021 sehr ähnlich.

3.4.2 Gefühlter Informationsgrad zur Cyberrisk-Thematik

Die Hälfte (50 %) der befragten Geschäftsführenden fühlt sich eher oder sehr gut informiert (Skalenwerte 4–5) bezüglich der Cyberrisk-Thematik, rund ein Fünftel (21 %) eher oder sehr schlecht (Skalenwerte 1–2). Der Mittelwert liegt somit bei 3.5 und ist unverändert gegenüber dem Vorjahr und nur minimal verändert gegenüber 2020 (3.4).

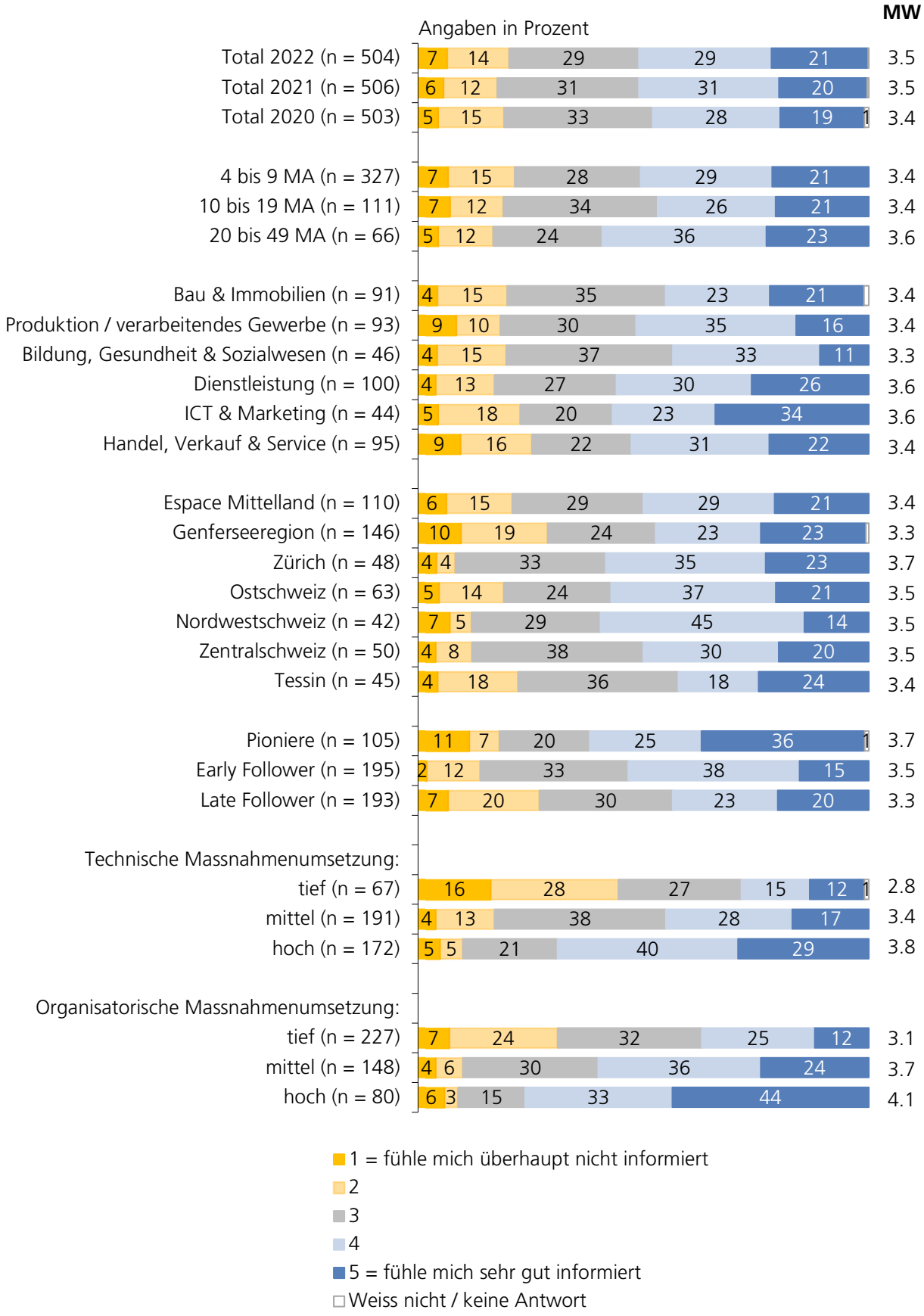
Frage 7:
Ganz allgemein: wie gut fühlen Sie sich persönlich in der Cyberrisk-Thematik informiert?
Basis: Total, n = 504

Die grössten Unternehmen (20–49 Mitarbeitende) fühlen sich am besten informiert (Mittelwert 3.6), die beiden kleineren Kategorien (4–9 bzw. 10–19 Mitarbeitende) liegen mit einem Mittelwert von 3.4 leicht tiefer (Unterschied nicht signifikant).

Die Branchen ICT & Marketing sowie Dienstleistungen schätzen ihren Informationsgrad am höchsten (je 3.6) ein, aber nicht signifikant höher als die anderen Branchen (3.3 bis 3.4). In den Vorjahren 2020 und 2021 lag die ICT & Marketingbranche noch signifikant höher als die anderen Branchen (2021: 4.0, 2020: 4.1), hat also ihre Selbsteinschätzung als einzige Branche stark nach unten korrigiert, während die anderen auf ähnlichem Niveau blieben.

Je aufgeschlossener die Unternehmen gegenüber technischen Innovationen sind und je höher die technischen und organisatorischen Sicherheitsmassnahmen umgesetzt sind, desto besser fühlen

sich die Geschäftsführenden auch über Cyberrisiken informiert (Werte siehe Grafik 9, Unterschiede sind signifikant).

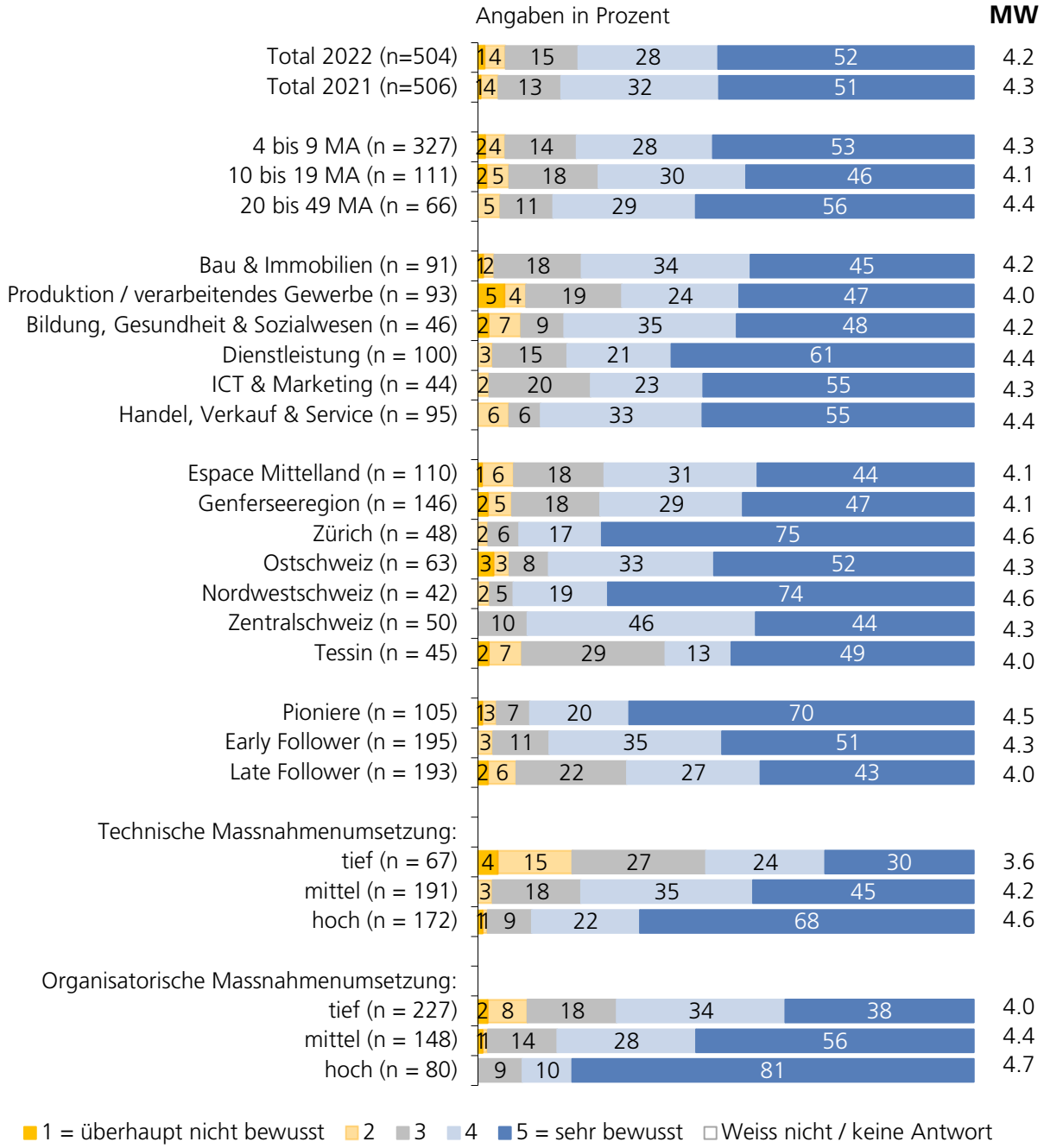


Grafik 9

3.4.3 Bedrohungsbewusstsein

Acht von zehn Befragten (80 %) geben an, sich der Cyberrisk-Bedrohungen eher bis sehr bewusst zu sein (Skalenwerte 4–5). Nur jeder Zwanzigste (5 %) gibt an, sich der Bedrohungen überhaupt nicht oder eher nicht bewusst zu sein (Skalenwerte 1–2). Diese Werte unterscheiden sich kaum vom Vorjahr; der Mittelwert sinkt von 4.3 im Jahr 2021 auf 4.2 im Jahr 2022. Die beiden Werte aus Frage 7 (Informationsgrad) und Frage 8 (Bedrohungsbewusstsein) steigen gemeinsam: Je höher der Informationsgrad, desto höher ist auch das Bedrohungsbewusstsein: Eher uninformierte Befragte schätzen ihr Bedrohungsbewusstsein auf 3.6, eher informierte Befragte auf 4.6.

Frage 8:
Wie bewusst sind Ihnen die Bedrohungen durch Cyberkriminalität wie Malware, Online-Betrug und Hacking?
Basis: Total, n = 504



Grafik 10

Das Bedrohungsbewusstsein (Mittelwert 4.2) ist also, wie schon 2021, deutlich höher als der Informationsgrad (Frage 7: Mittelwert 3.5). Das könnte daran liegen, dass ein hoher Informationsgrad eine ständige Beschäftigung mit dem Thema erfordert, während die Bedrohungslage – das Risiko von Verlusten irgendwelcher Art durch Cyberangriffe – mit scheinbar weniger Aufwand eingeschätzt werden kann. Kurz: Die Befragten glauben um die Bedrohungslage zu wissen, haben aber nicht die Kapazität oder fühlen sich persönlich nicht dafür verantwortlich, sich auf einem hohen Informationsgrad zu halten.

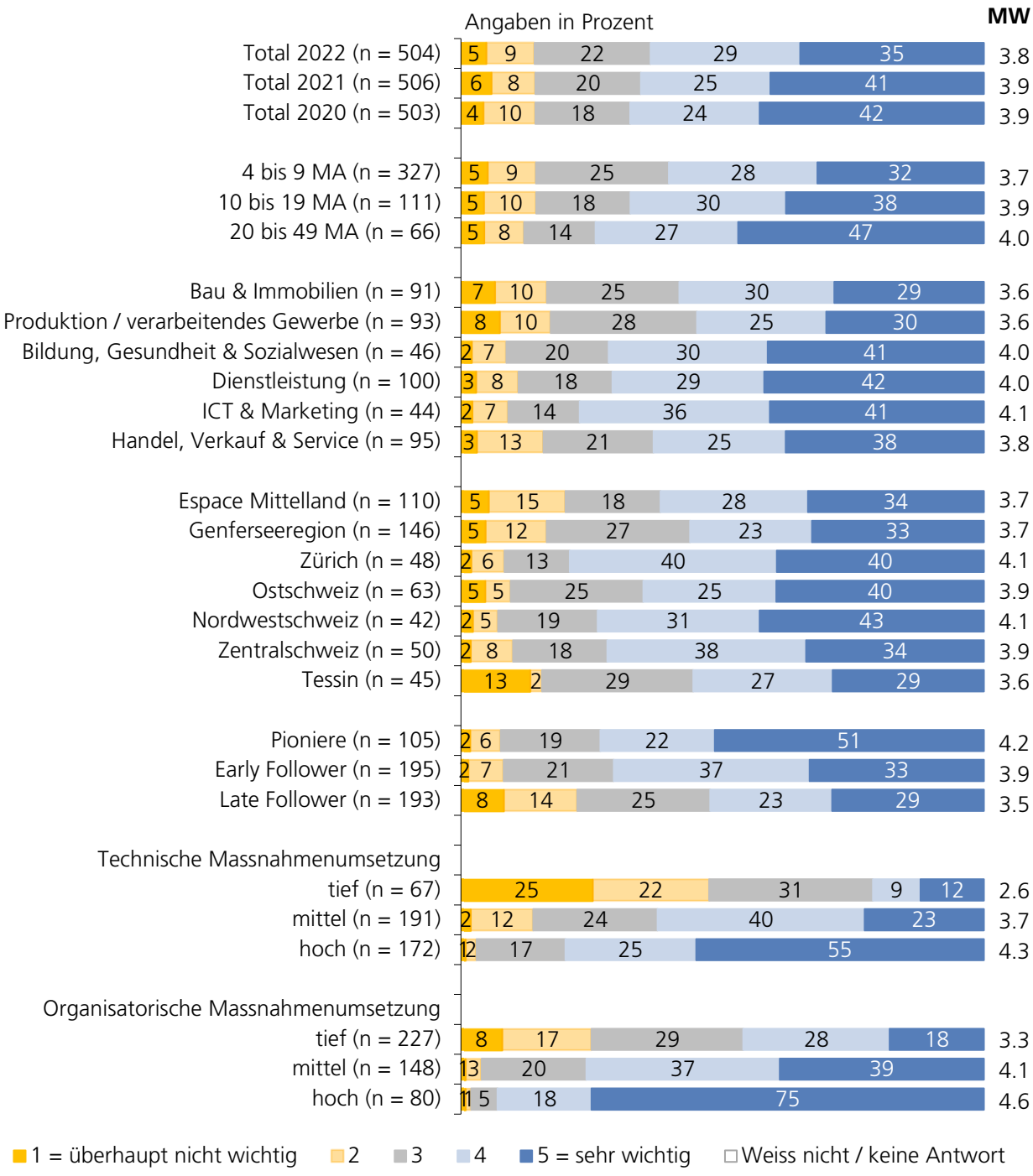
Die Antworten der verschieden Unternehmensgrössen und Branchen unterscheiden sich nicht signifikant. Doch es gilt wieder die Regel: Je aufgeschlossener die Befragten gegenüber technischen Innovationen sind und je weiter ihre technischen und organisatorische Massnahmen umgesetzt sind, desto höher ist ihr Bedrohungsbewusstsein (Werte siehe Grafik 10, Unterschiede sind signifikant).

3.4.4 Wichtigkeit des Themas Cybersicherheit

Frage 9:
Welche Wichtigkeit hat in Ihrer Firma das Thema Cybersicherheit?
Basis: Total, n = 504

Die Wichtigkeit der Cybersicherheit wird 2022 ähnlich wie 2021 und 2020 beurteilt: Rund zwei Drittel der Befragten (64 %) beurteilen das Thema Cybersicherheit als eher bis sehr wichtig (Skalenwerte 4–5), rund ein Siebtel (14 %) beurteilt es als eher bis sehr unwichtig (Skalenwerte 1–2). Der Mittelwert liegt somit im Jahr 2022 mit 3.8 minimal tiefer als 2021 und 2020 (je 3.9).

Je mehr Mitarbeitende ein Unternehmen beschäftigt, desto höher wird die Cybersicherheit priorisiert (Werte siehe Grafik 11), die Unterschiede sind allerdings nicht signifikant. Auch zwischen den Branchen und Grossregionen ergeben sich keine signifikanten Unterschiede. Hingegen finden sich Zusammenhänge bei der Einstellung zu technischen Innovationen und der Massnahmenumsetzung: Je aufgeschlossener die befragten gegenüber technischen Innovationen sind und je mehr technische bzw. organisatorische Massnahmen sie umgesetzt haben, desto höher ist ihre Priorisierung des Themas Cyberrisiken (Unterschiede signifikant, Werte siehe Grafik 11). Diese Unterschiede sind nicht neu; sie wurden schon in der Studie 2021 festgestellt.



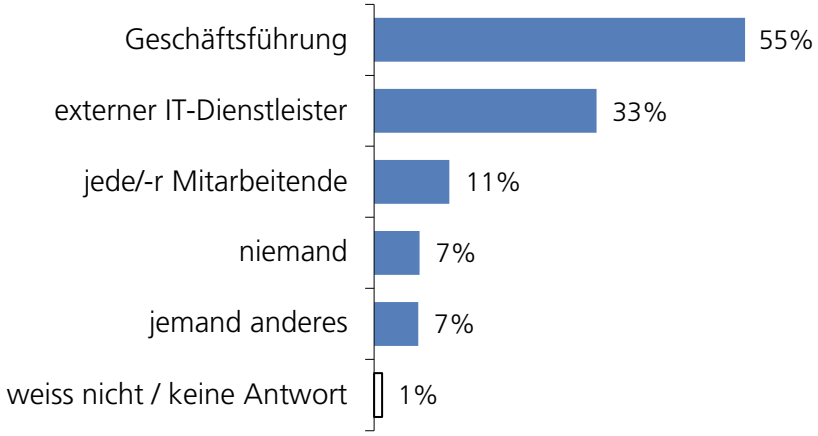
Grafik 11

3.4.5 Verantwortlichkeit Cybersicherheit

Frage 10:
Wer ist in Ihrer Firma verantwortlich für die Cybersicherheit?
Basis: Total, n = 504

In über der Hälfte der befragten Unternehmen (55 %) zeichnet sich der/die Geschäftsführende verantwortlich für die Cybersicherheit. Ein Drittel der Befragten (33 %) nennt einen externen Dienstleister, rund ein Zehntel (11 %) meint, dass «jede/-r Mitarbeitende» verantwortlich ist. Da Mehrfachantworten möglich waren, ergibt die Summe aller Antworten mehr als 100 Prozent; die durchschnittliche Anzahl Nennungen liegt bei 1.1.

Spannend sind die Antworten der Branche ICT & Marketing, die deutlich aus den anderen Branchen heraussticht: Jede/-r dritte Befragte (34 %) dieser Branche sieht *sämtliche* Mitarbeitende in der Verantwortung; bei den anderen Branchen liegt dieser Wert unter einem Zehntel (zwischen 6 und 9 %), mit Ausnahme der Branche Bildung, Gesundheits- und Sozialwesen, welche mit rund einem Siebtel (15 %) dazwischen, aber auch deutlich tiefer liegen. Der Anteil an externen IT-Dienstleistern, welche die Verantwortung tragen, liegt dafür bei der ICT & Marketingbranche deutlich (aber nicht signifikant) tiefer, nämlich bei knapp einem Fünftel (18 %) (andere Branchen: 28 % bis 46 %).



Grafik 12

Ein spezielles Augenmerk sollte auch auf die Antwortkategorie «niemand» gerichtet werden. Sieben von hundert befragten Unternehmen (7 %) bezeichnen «niemanden» als verantwortlich für die Cybersicherheit. In den folgenden Subgruppen ist der Anteil dieser Unternehmen besonders hoch (Unterschiede signifikant):

- Westschweizer (10 %) und Tessiner (13 %) Unternehmen (D-CH: 3 %)
- Verfügen über keine homeoffice-tauglichen Stellen (14 %)
- Late Follower (10 %)
- Sind sehr oder eher uninformiert bezüglich Cyberrisiken (19 %)
- Haben eine tiefe technische Massnahmenumsetzung (30 %)
- Haben eine tiefe organisatorische Massnahmenumsetzung (11 %)

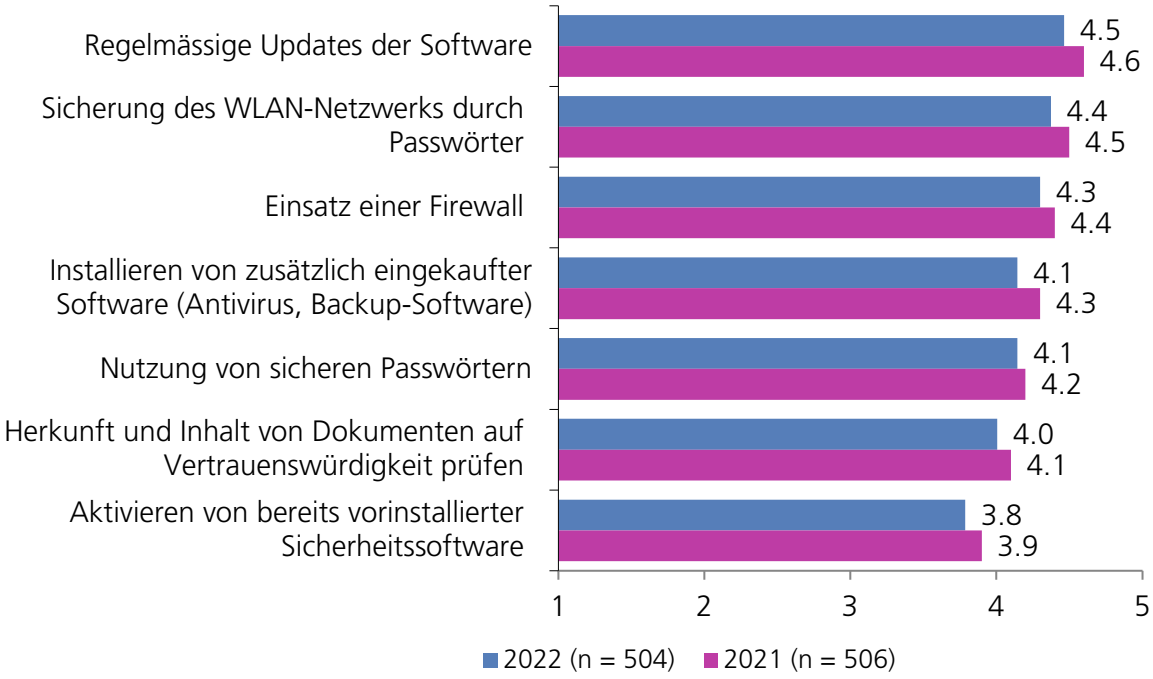
(Lesebeispiel: Von allen befragen Westschweizer Unternehmen haben 10 % geantwortet, dass bei ihnen «niemand» für die Cybersicherheit verantwortlich ist.)

Unternehmen mit hoher technischer und organisatorischer Massnahmenumsetzung haben zudem signifikant häufiger einen externen Dienstleister in der Verantwortung (technisch: 40 %, organisatorisch: 44 %) als Unternehmen mit jeweils tiefer Massnahmenumsetzung (technisch: 21 %, organisatorisch: 27 %).

3.4.6 Technische Massnahmen zur Erhöhung der Cybersicherheit

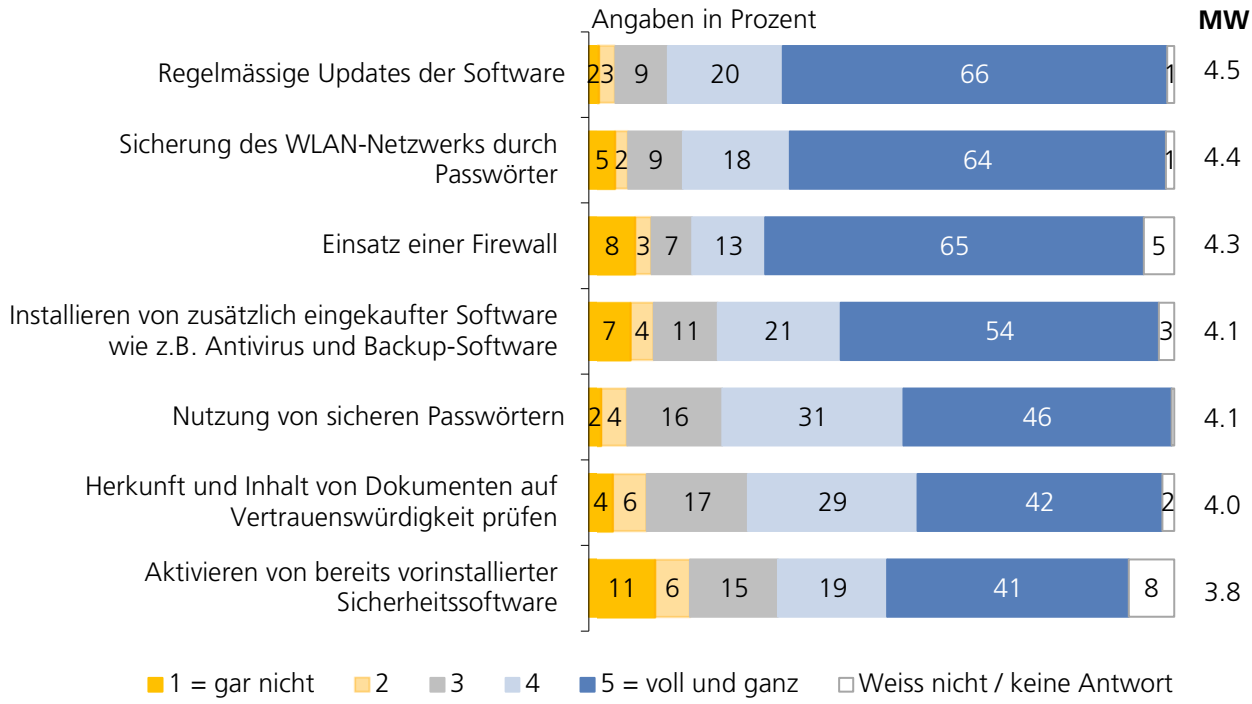
Frage 11:
Inwieweit sind die folgenden **technischen** Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?
Basis: Total, n = 504

Die Umsetzungsgrade der verschiedenen abgefragten Massnahmen liegen zwischen 3.8 und 4.5, allesamt minimal tiefer als 2021. Den höchsten Umsetzungsgrad erzielt die Massnahme «Regelmässige Softwareupdates» (86 % fast/voll umgesetzt, Mittelwert 4.5), gefolgt von der Massnahme «Sicherung des WLAN-Netzwerks durch Passwörter» (82 % fast/voll umgesetzt, Mittelwert 4.5). Den tiefsten Umsetzungsgrad und einen Mittelwert unter 4.0 erreicht die Massnahme «Aktivieren von bereits vorinstallierter Sicherheitssoftware (60 % fast/voll umgesetzt, Mittelwert 3.8).



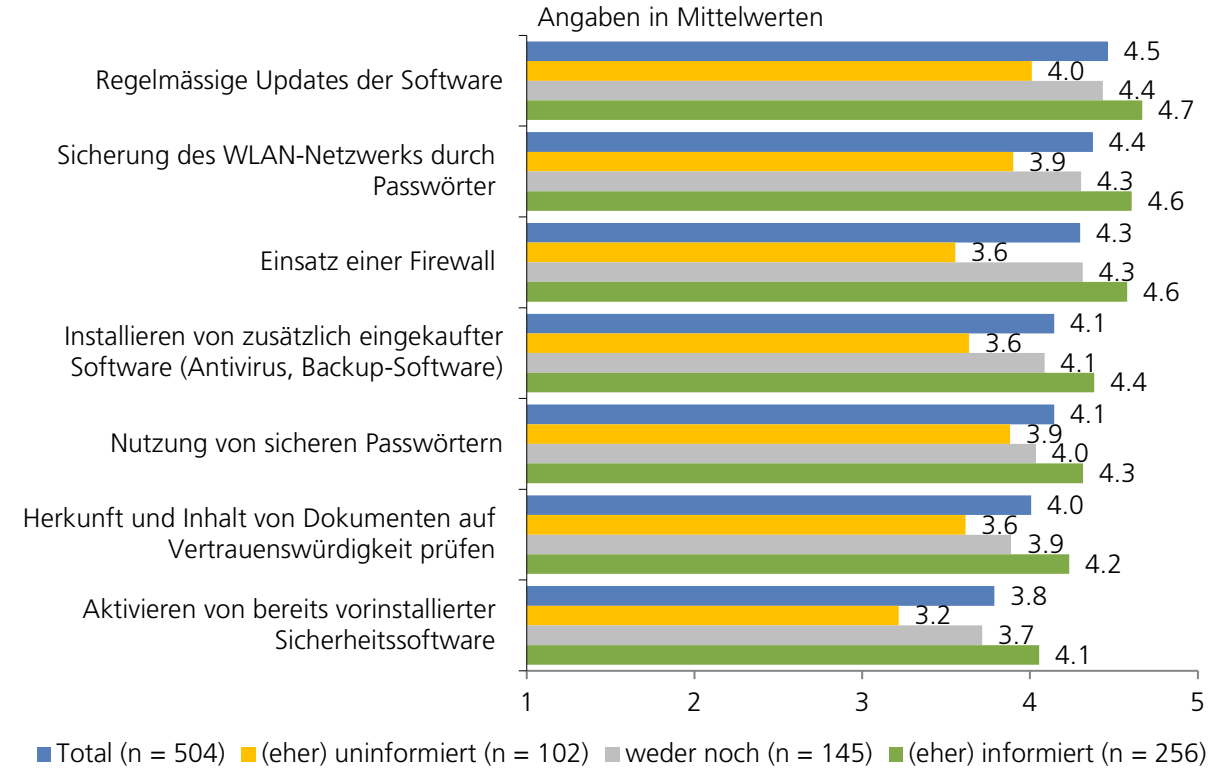
Grafik 13

Nicht oder nur minimal umgesetzte Massnahmen können unter Umständen ein massgebliches Sicherheitsrisiko bedeuten: Einerseits für die Unternehmen selbst, andererseits für die Besitzer der Daten, die dort entwendet werden können (z.B. Kundendaten, Passwörter). Diesen Gedanken berücksichtigend, sollte auch auf tiefe Skalenwerte geachtet werden: So haben zum Beispiel 8 von 100 befragten Unternehmen keine Firewall (8 %) oder 7 von 100 Unternehmen keine zusätzlich eingekaufte Sicherheitssoftware (7 %), mehr als jedes zehnte Unternehmen (11 %) aktiviert nicht die bereits vorinstallierte Sicherheitssoftware (jeweils Skalenwert 1 von 5). Eine gewisse Ungenauigkeit aufgrund zu tiefen Wissensstands der Befragten ist dabei aber mitzuberücksichtigen.



Grafik 14

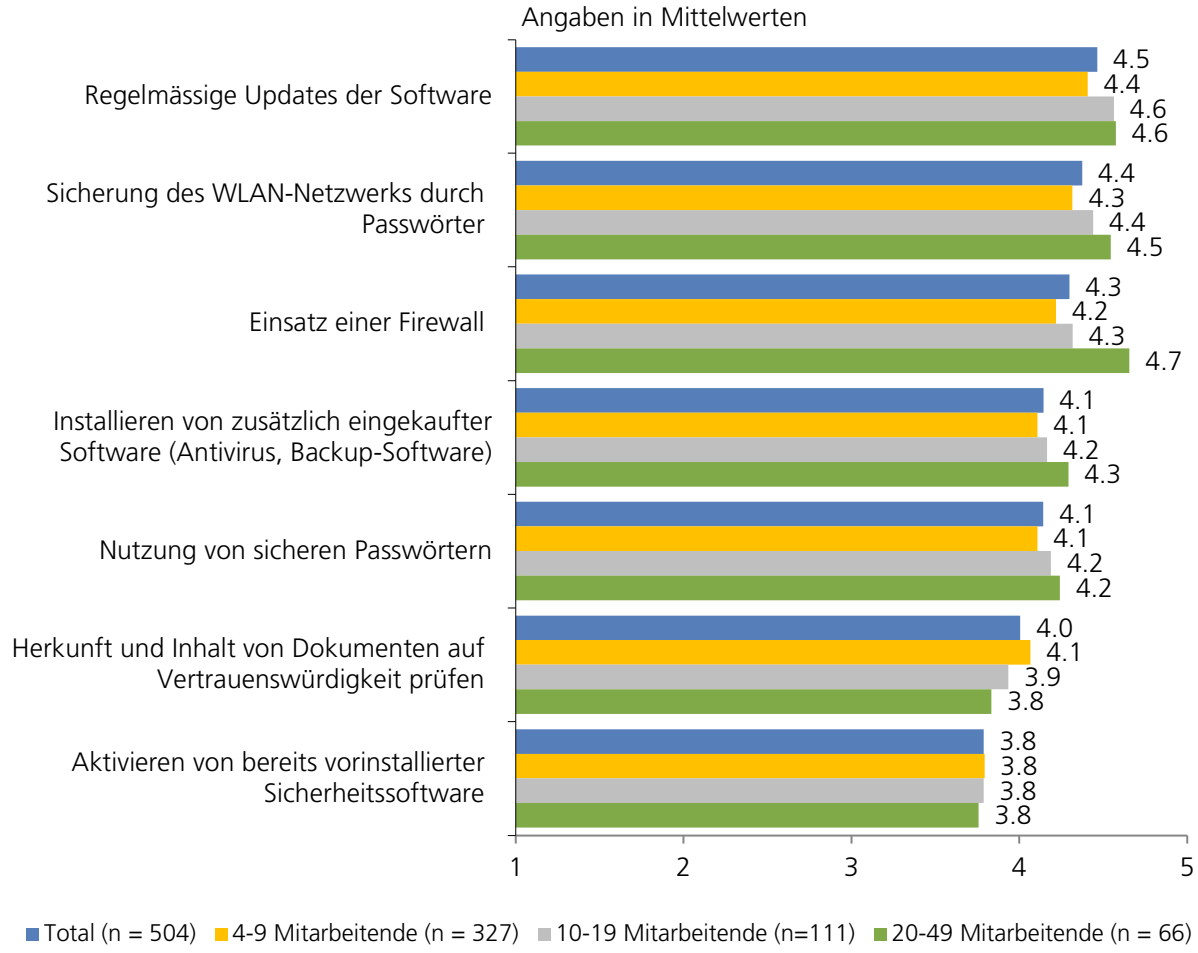
Nachdem die Branche ICT & Marketing einen hohen Homeoffice-Anteil (Kapitel 3.2.2) hat und ihren Informationsgrad (Kapitel 3.4.2) sowie die Wichtigkeit des Themas Cybersicherheit (Kapitel 3.4.4) leicht höher als die anderen Branchen beurteilt, wäre bei der Massnahmenumsetzung zu erwarten gewesen, dass sie ebenfalls höher ausfällt. Dies ist allerdings nur bei den Massnahmen «Sicherung des WLAN-Netzwerk durch Passwörter» (Mittelwert 4.8, andere Branchen 4.2 bis 4.5) und «Nutzung von sicheren Passwörtern» (Mittelwert 4.5, andere Branchen 4.0 bis 4.2) so.



Grafik 15

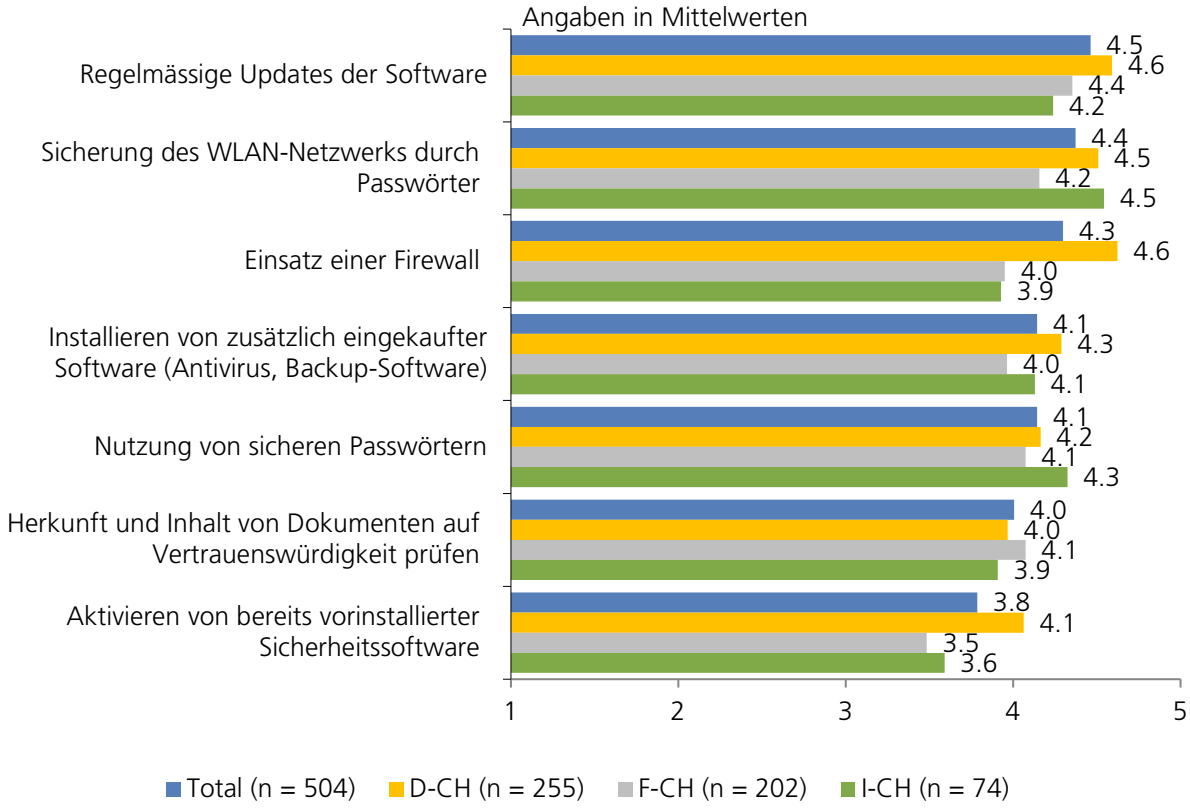
Bei allen Massnahmen gilt: Je höher der selbst eingeschätzte Informationsgrad ist, desto höher ist auch die Massnahmenumsetzung (Werte siehe Grafik 15).

Firmengrösse und Massnahmenumsetzungsgrad hängen nicht zwingend zusammen. Nur bei den vier Massnahmen «Sicherung des WLAN-Netzwerks durch Passwörter», «Einsatz einer Firewall», «Installieren von zusätzlich eingekaufter Software» und «Nutzung von sicheren Passwörtern» gilt: Je grösser das Unternehmen, desto höher ist der technische Massnahmenumsetzungsgrad (Werte siehe Grafik 16).

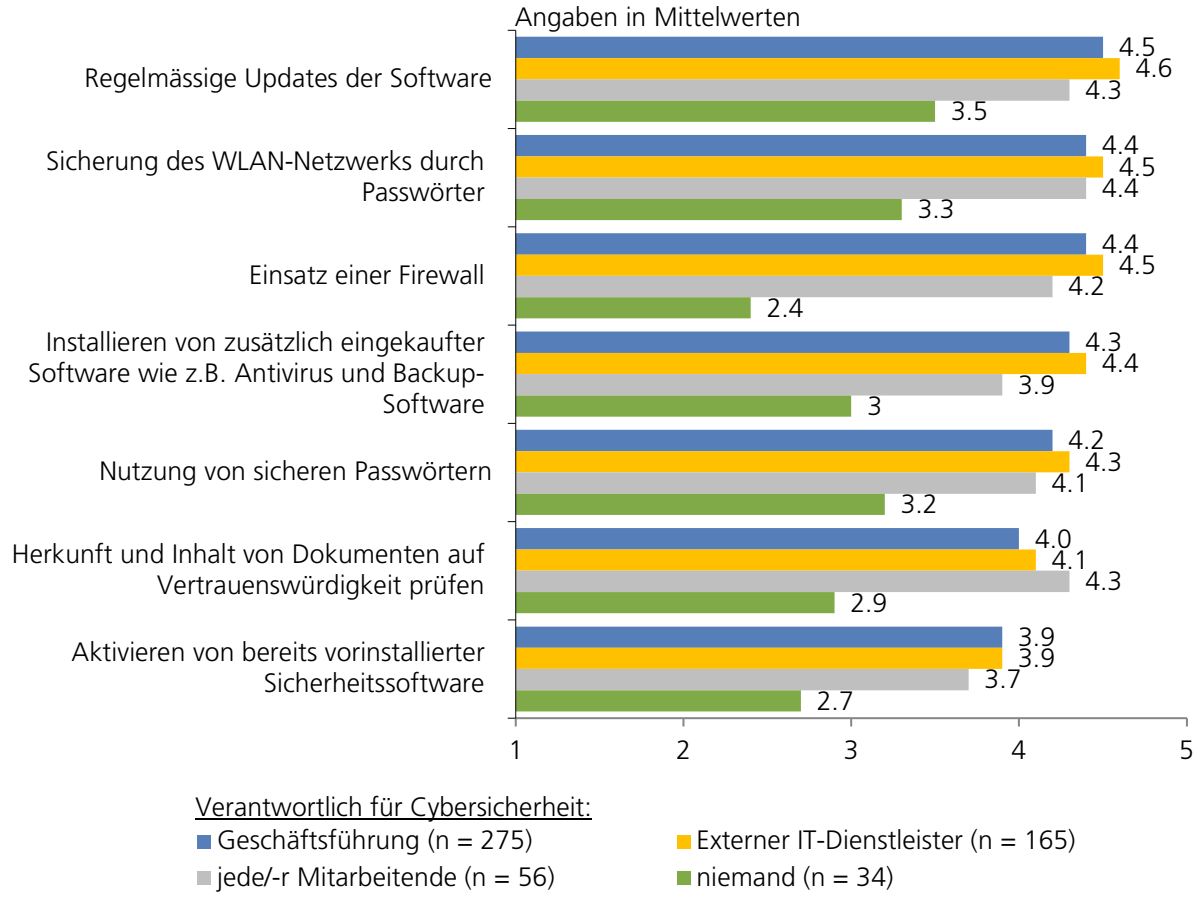


Grafik 16

Wie schon 2021 festgestellt werden konnte, sind in der Westschweiz und im Tessin viele Massnahmen tendenziell bis signifikant weniger umgesetzt als in den Regionen der Deutschschweiz. Signifikant sind die in der folgenden Grafik abgebildeten Unterschiede bei den Massnahmen «Regelmässige Softwareupdates» (D-CH / W-CH / TI), «Sicherung des WLAN-Netzwerks durch Passwörter» (D-CH / W-CH), «Einsatz einer Firewall» (D-CH / W-CH / TI), «Installation von zusätzlich eingekaufter Sicherheitssoftware» (D-CH / W-CH) und «Aktivieren bereits vorinstallierter Software» (D-CH / W-CH) (Werte siehe Grafik 17).



Grafik 17



Grafik 18

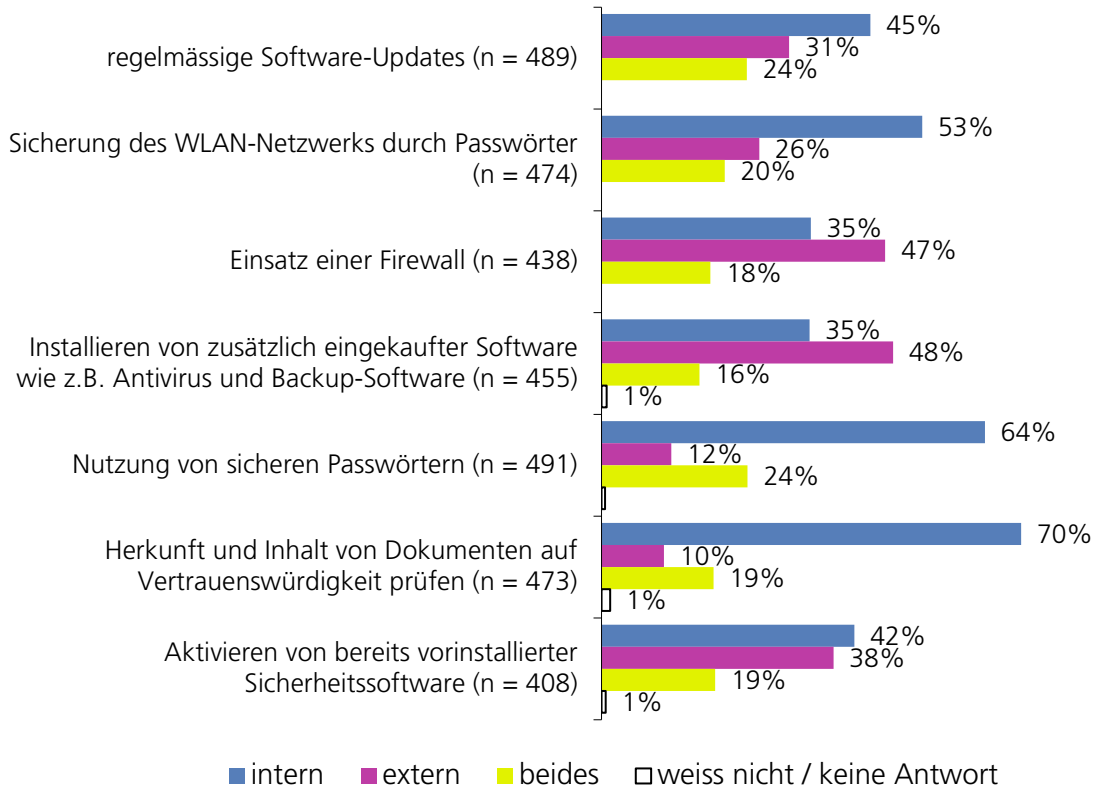
Ist der/die Geschäftsführende, ein externer IT-Dienstleister oder «jede/-r Mitarbeitende» für die Cybersicherheit verantwortlich, werden die Massnahmen signifikant besser umgesetzt als wenn «niemand» verantwortlich ist. Am besten werden die Massnahmen umgesetzt, wenn ein IT-Dienstleister verantwortlich ist (siehe Grafik 18).

3.4.7 Outsourcen von Aufgaben der IT-Sicherheit

3.4.7.1 Interne oder externe Bearbeitung

Die Firewall und die Installation von zusätzlich eingekaufter Sicherheitssoftware sind Massnahmen, die mehrheitlich von externen Dienstleistern (47 % und 48 %) umgesetzt werden, alle anderen Massnahmen werden von einer Mehrheit der Befragten intern bearbeitet (Werte siehe Grafik 19). Rund ein Sechstel bis ein Viertel der Befragten teilen die jeweiligen Massnahmen auf interne und externe Mitarbeitende auf.

Frage 12:
Werden die folgenden Aufgaben intern bearbeitet oder haben Sie einen externen Dienstleister dafür?
Basis: Nur wenn jeweilige Massnahme umgesetzt wird, n = siehe Grafik 19



Grafik 19

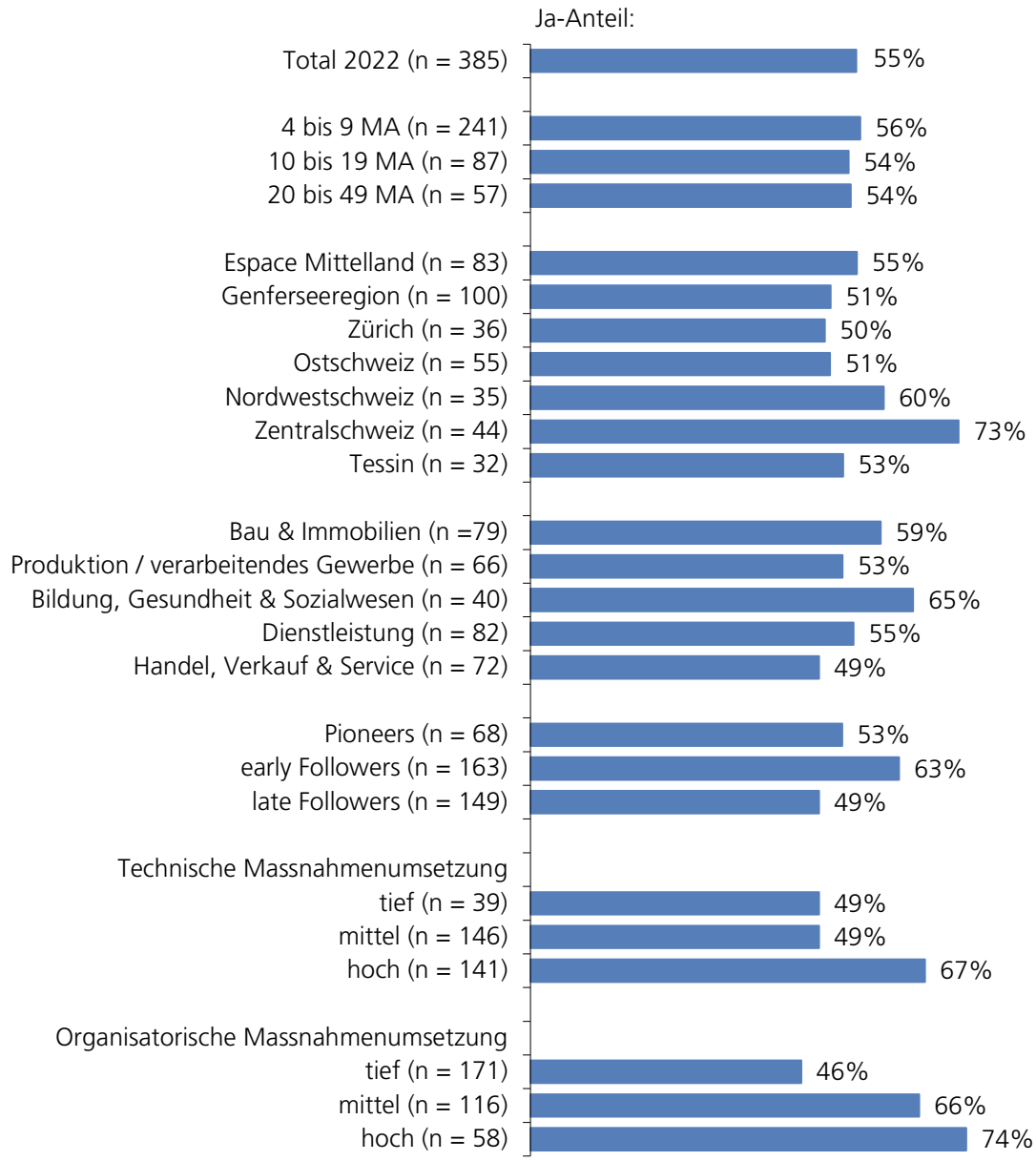
Grundsätzlich bearbeiten Pioniere und die Branche ICT & Marketing mehr Sicherheitsmassnahmen intern als Early und Late Follower bzw. als die anderen Branchen. Auch haben kleine Unternehmen seltener einen externen Dienstleister für die Sicherheitsmassnahmen als grössere Unternehmen: Die nachfolgende Tabelle zeigt diejenigen Massnahmen, bei denen zwischen den Unternehmensgrössenkategorien mindestens ein signifikanter Unterschied besteht:

		4–9 Mitarbeitende (A)	10–19 Mitarbeitende (B)	20–49 Mitarbeitende (C)
Regelmässige Software-Updates	Intern	50 % (sign. zu C)	40 %	25 %
	Extern	27 %	35 %	45 % (sign. zu A)
	Beides	23 %	24 %	31 %
Sicherung des WLAN-Netzwerks durch Passwörter	Intern	56 % (sign. zu C)	59 % (sign. zu C)	28 %
	Extern	22 %	29 %	44 % (sign. zu A)
	Beides	22 %	12 %	28 % (sign. zu B)
Einsatz einer Firewall	Intern	41 % (sign. zu B, C)	26 %	21 %
	Extern	40 %	55 % (sign. zu A)	65 % (sign. zu A)
	Beides	19 %	18 %	15 %
Aktivieren von bereits vorinstallierter Sicherheitssoftware	Intern	47 % (sign. zu C)	40 %	22 %
	Extern	31 %	47 % (sign. zu A)	60 % (sign. zu A)
	Beides	21 %	13 %	18 %

3.4.7.2 IT-Sicherheitszertifizierung des externen Dienstleisters

Frage 13:
Verfügt ihr externer IT-Dienstleister über eine IT-Sicherheitszertifizierung (z.B. ISO 27001 oder CyberSeal der Allianz Digitale Sicherheit Schweiz)?
Basis: Setzt externen IT-Dienstleister ein, n = 385

Über die Hälfte (55 %) der eingesetzten IT-Dienstleister verfügt über eine IT-Sicherheitszertifizierung wie z.B. ISO 27001. Die Unterschiede zwischen Firmengrössen, Grossregionen und Branchen sind nicht signifikant, aber besser über Cyberrisiken informierte Befragte haben signifikant häufiger zertifizierte IT-Dienstleister (58 %) als schlechter informierte (39 %). Zudem ist der Umsetzungsgrad der technischen und organisatorischen Massnahmen höher bei den Unternehmen, die einen zertifizierten IT-Dienstleister engagieren – vielleicht ist die IT-Sicherheitszertifizierung des externen Dienstleisters ebenfalls als Sicherheitsmassnahmenumsetzung zu betrachten.

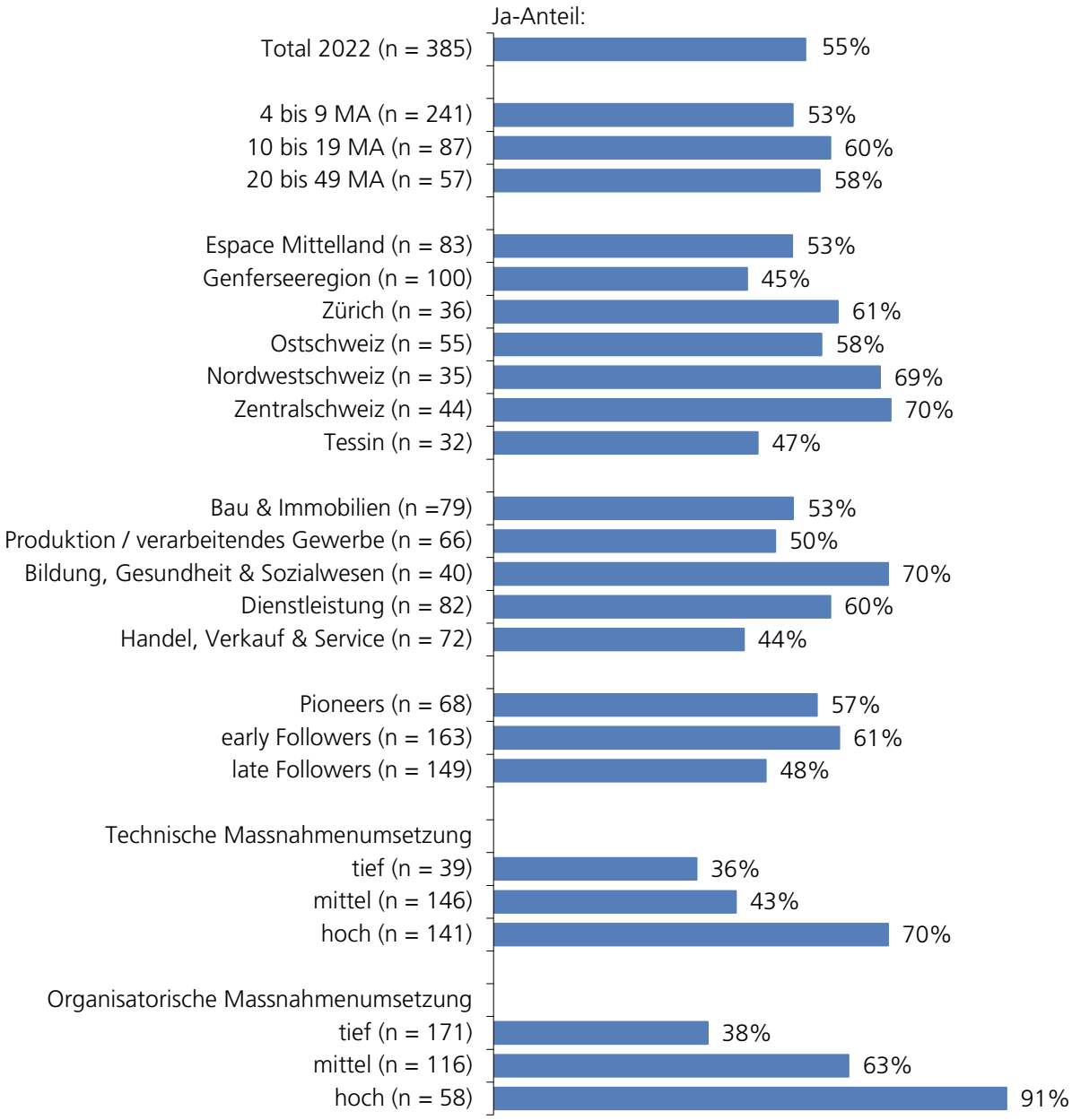


Grafik 20

3.4.7.3 Schriftliche Vereinbarungen mit externem IT-Dienstleister

Frage 14:
Bestehen schriftliche Vereinbarungen mit dem IT-Dienstleister hinsichtlich Aufgaben und Verantwortungen oder nicht?
Basis: Setzt externen IT-Dienstleister ein, n = 385

Auch der Anteil an Unternehmen, die eine schriftliche Vereinbarung mit dem IT-Dienstleister hinsichtlich Aufgaben und Verantwortung haben, liegt leicht über der Hälfte (55 %, gleicher Wert wie IT-Sicherheitszertifizierung). Wie schon bei der vorangehenden Frage sind auch hier die Unterschiede zwischen den Unternehmensgrössenkategorien, Grossregionen und Branchen nicht signifikant. Über Cyberrisiken informierte Befragte haben aber eher schriftliche Vereinbarungen mit ihrem IT-Dienstleister (63 %) als uninformierte (42 %), und Befragte mit höheren organisatorischen und technischen Massnahmenumsetzungen ebenfalls (Werte siehe Grafik 21).

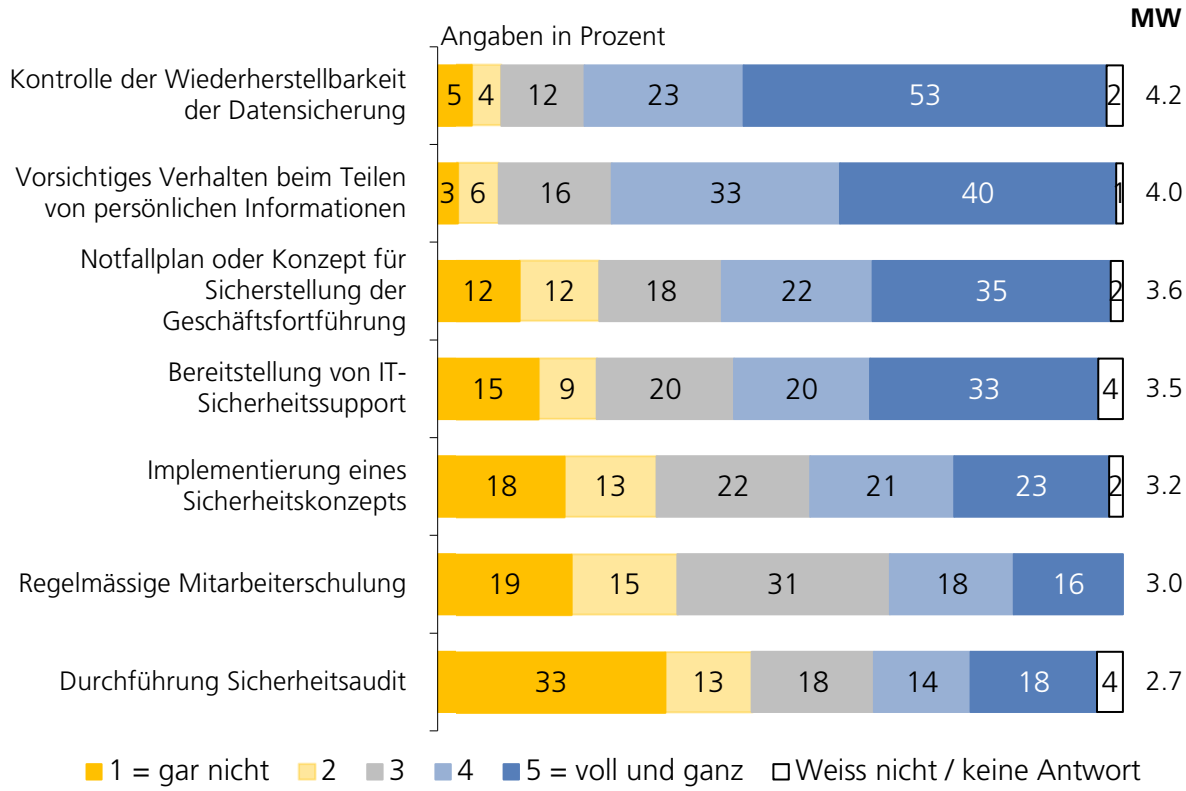


Grafik 21

3.4.8 Organisatorische Massnahmen zur Erhöhung der Cybersicherheit

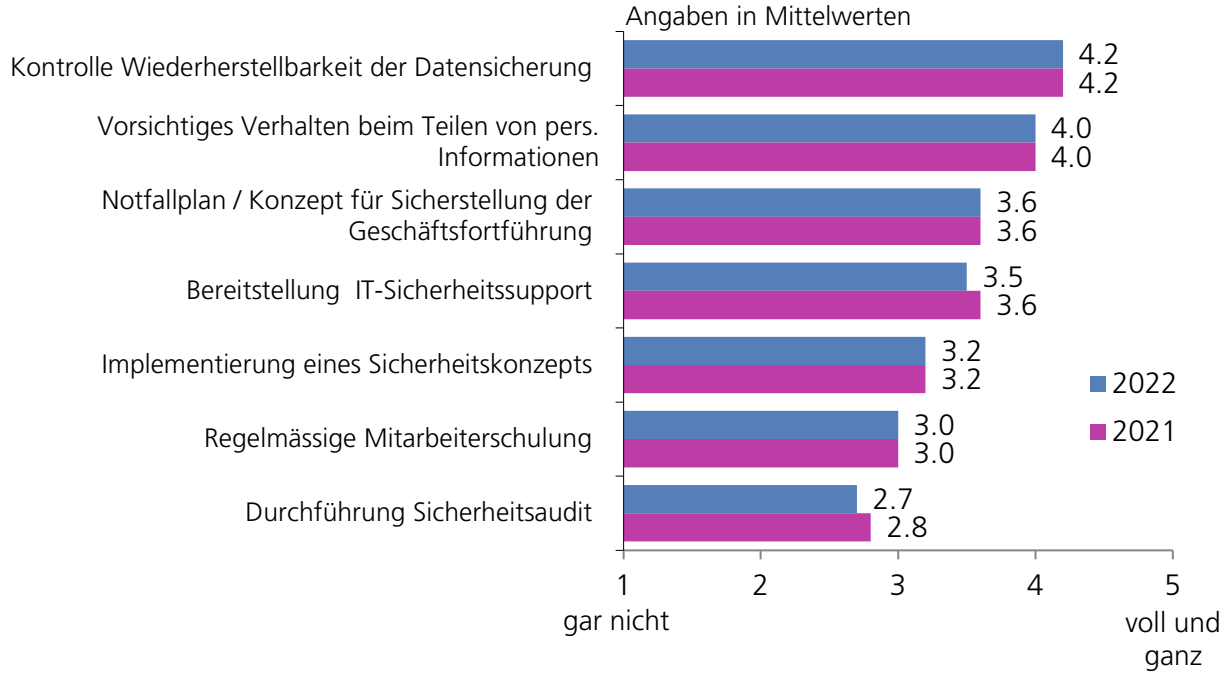
Frage 15:
Inwieweit sind die folgenden **organisatorischen** Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?
Basis: Total, n = 504

Analog zu der Frage nach technischen Sicherheitsmassnahmen (siehe 3.4.6) wurde auch eine Frage nach organisatorischen Sicherheitsmassnahmen gestellt. Wie schon in der Vorjahresstudie festgestellt wurde, werden organisatorische Massnahmen immer noch deutlich weniger umgesetzt als technische. Die am häufigsten umgesetzte organisatorische Massnahme ist die Kontrolle der Wiederherstellbarkeit der Datensicherung (4.2). Rund drei Viertel (76 %) der Befragten haben sie fast oder voll und ganz umgesetzt (2021: 77 %). Zum Vergleich: Die am häufigsten vollständig umgesetzte technische Massnahme, regelmässige Softwareupdates, wurden von über vier Fünfteln (86 %) fast oder voll und ganz umgesetzt.



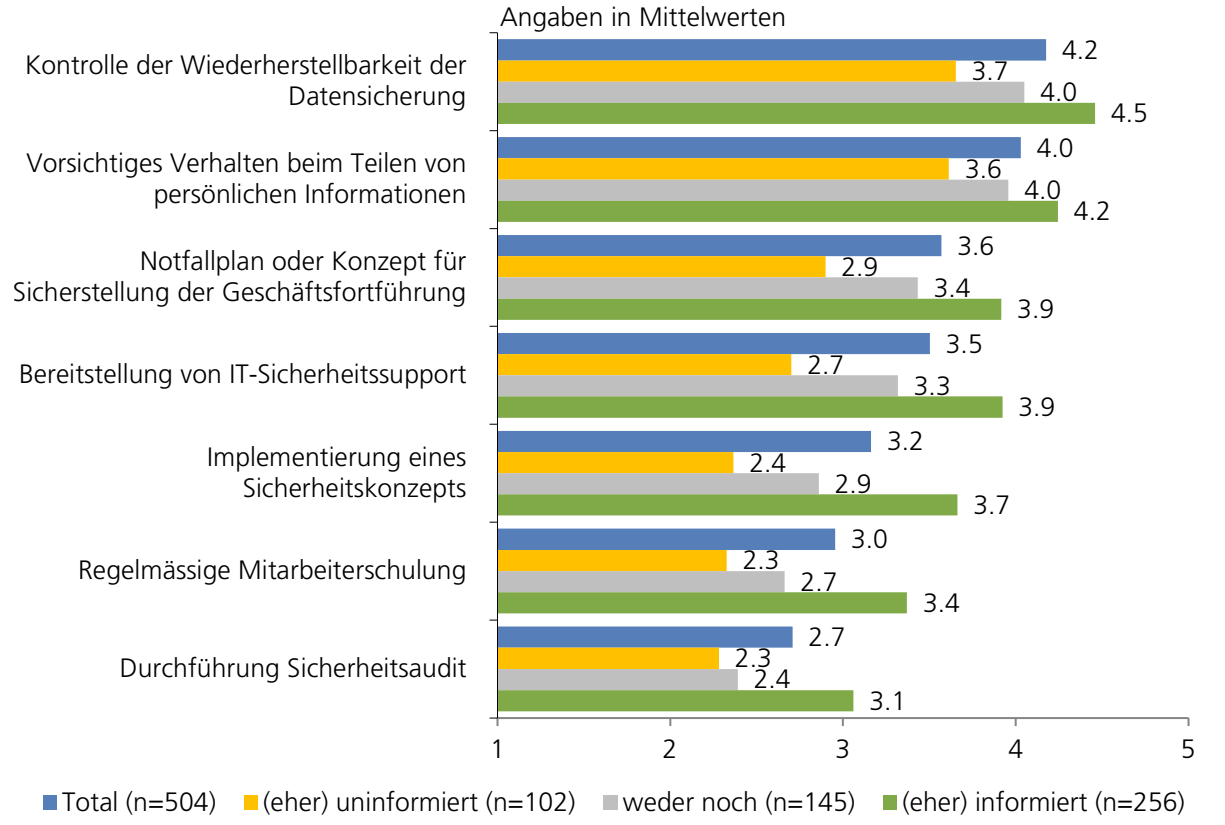
Grafik 22

An zweiter Stelle in der Reihenfolge der umgesetzten organisatorischen Massnahmen steht das «Vorsichtige Verhalten beim Teilen von persönlichen Informationen»: Fast drei Viertel der Befragten (73 %) haben sie fast oder voll und ganz umgesetzt (2021: 74 %). An dritter Stelle und damit neu einen Platz weiter vorne liegt der «Notfallplan oder Konzept für die Sicherstellung der Geschäftsfortführung» mit etwas mehr als der Hälfte (57 %) der Befragten, die diese Massnahme fast oder voll umgesetzt haben (2021: 58 %). Es folgt die Bereitstellung von Sicherheitssupport mit rund der Hälfte (53 %) der Befragten, die sie fast oder voll und ganz umgesetzt haben (2021: 61 %). Die drei am wenigsten umgesetzten Massnahmen sind die «Implementierung eines Sicherheitskonzepts» (von 44 % fast oder voll umgesetzt), «Regelmässige Mitarbeiterschulung» (von 34 % fast oder voll umgesetzt) und «Durchführung eines Sicherheitsaudits» (von 32 % fast oder voll umgesetzt). Die Unterschiede gegenüber dem Vorjahr sind minimal bzw. nicht signifikant.
Bei der grossen Mehrheit der organisatorischen Massnahmen verhält es sich so, dass Deutschschweizer Unternehmen sie eher als Westschweizer Unternehmen umgesetzt haben, Pioniere eher als Early und Late Follower und bereits von Cyberangriffen betroffene eher als nicht-betroffene.



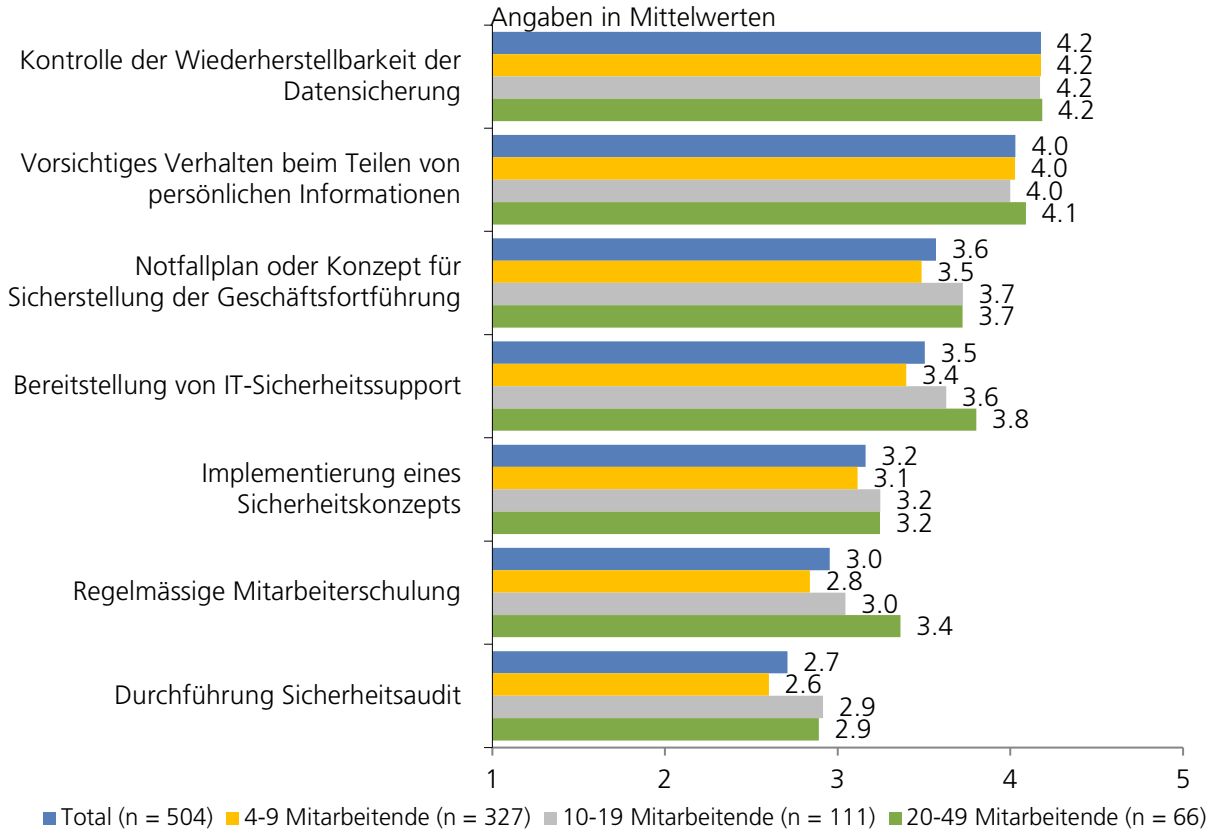
Grafik 23

Je besser sich die Befragten über die Cyberrisk-Thematik informiert fühlen, desto mehr organisatorische Massnahmen treffen sie zur Verbesserung der Cybersicherheit (bei allen Massnahmen signifikant). Diese Erkenntnis wurde auch schon aus der 2020er und 2021er Studie gewonnen.



Grafik 24

Die kleinste Unternehmensgrössenkategorie (4–9 Mitarbeitende) hat bei allen Massnahmen ausser der «Kontrolle der Wiederherstellbarkeit der Datensicherung» und dem «vorsichtigen Verhalten beim Teilen von persönlichen Informationen» den tiefsten Umsetzungsgrad. Signifikant ist aber nur der Unterschied zwischen der grössten und kleinsten Grössenkategorie bei der «regelmässigen Mitarbeiterschulung» (Werte siehe Grafik 25).

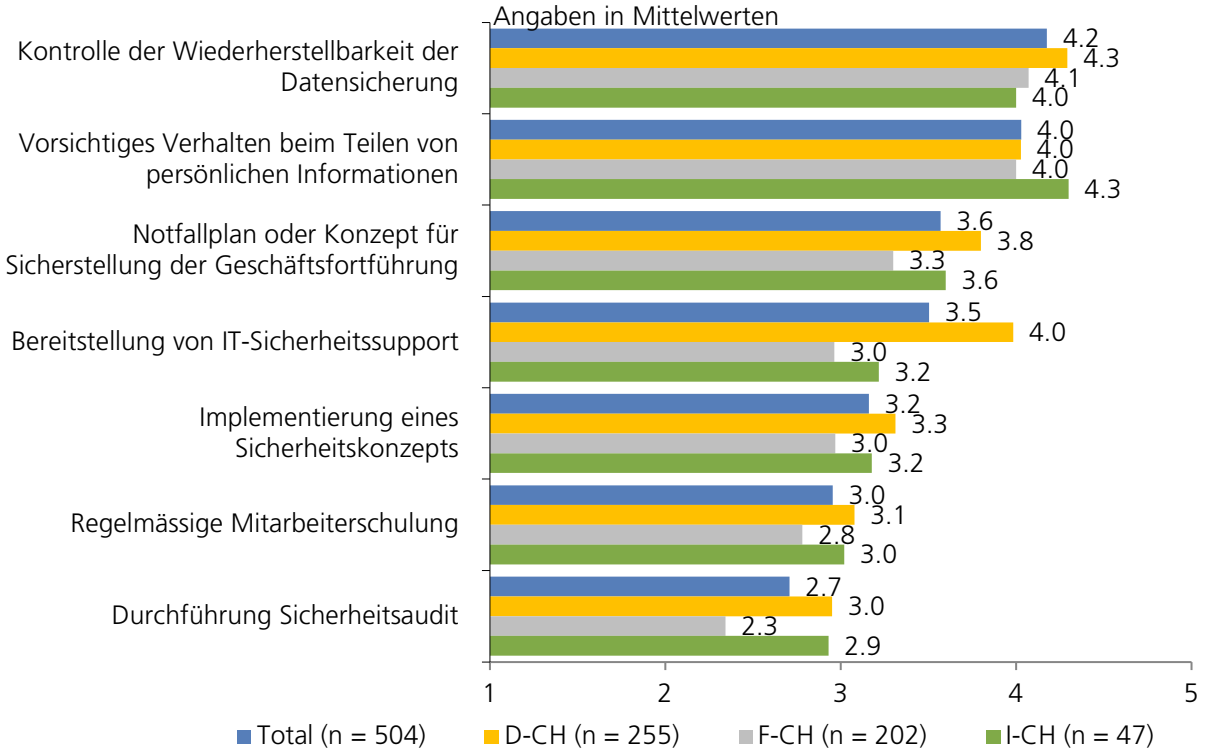


Grafik 25

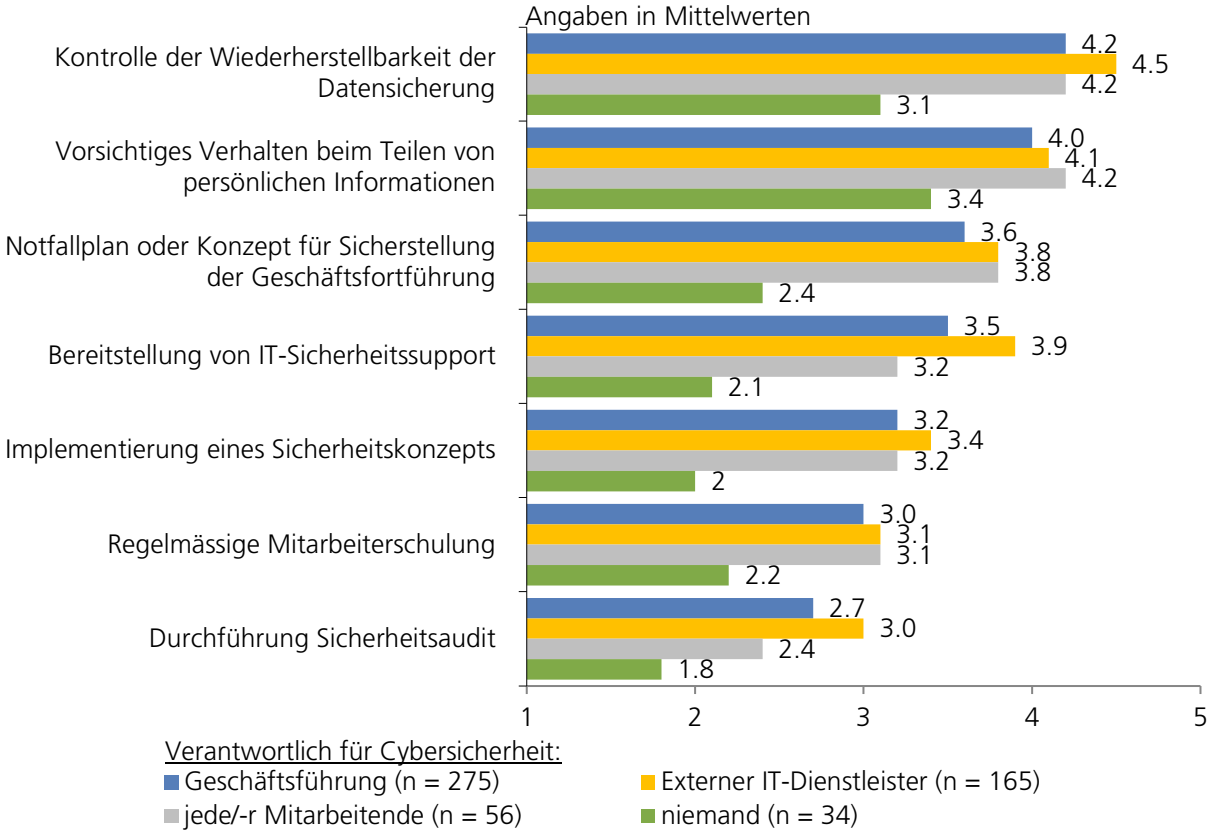
Die Massnahmenumsetzung ist in der Deutschschweiz bei allen Massnahmen mit Ausnahme des «vorsichtigen Verhaltens beim Teilen von persönlichen Informationen» weiter fortgeschritten als in der Westschweiz und im Tessin. Signifikant sind die Unterschiede bei den folgenden Massnahmen:

- Bereitstellung von IT-Sicherheitssupport (ggü. W-CH und TI),
- Notfallplan für Sicherstellung der Geschäftsfortführung (ggü. W-CH),
- Implementierung eines Sicherheitskonzepts (ggü. W-CH) sowie
- Durchführung eines Sicherheitsaudits (ggü. W-CH).

Bei den Massnahmen «Kontrolle der Wiederherstellbarkeit der Datensicherung» und «Regelmässige Mitarbeiterschulung» sind die Sprachregionen-Unterschiede nicht signifikant.



Grafik 26



Grafik 27

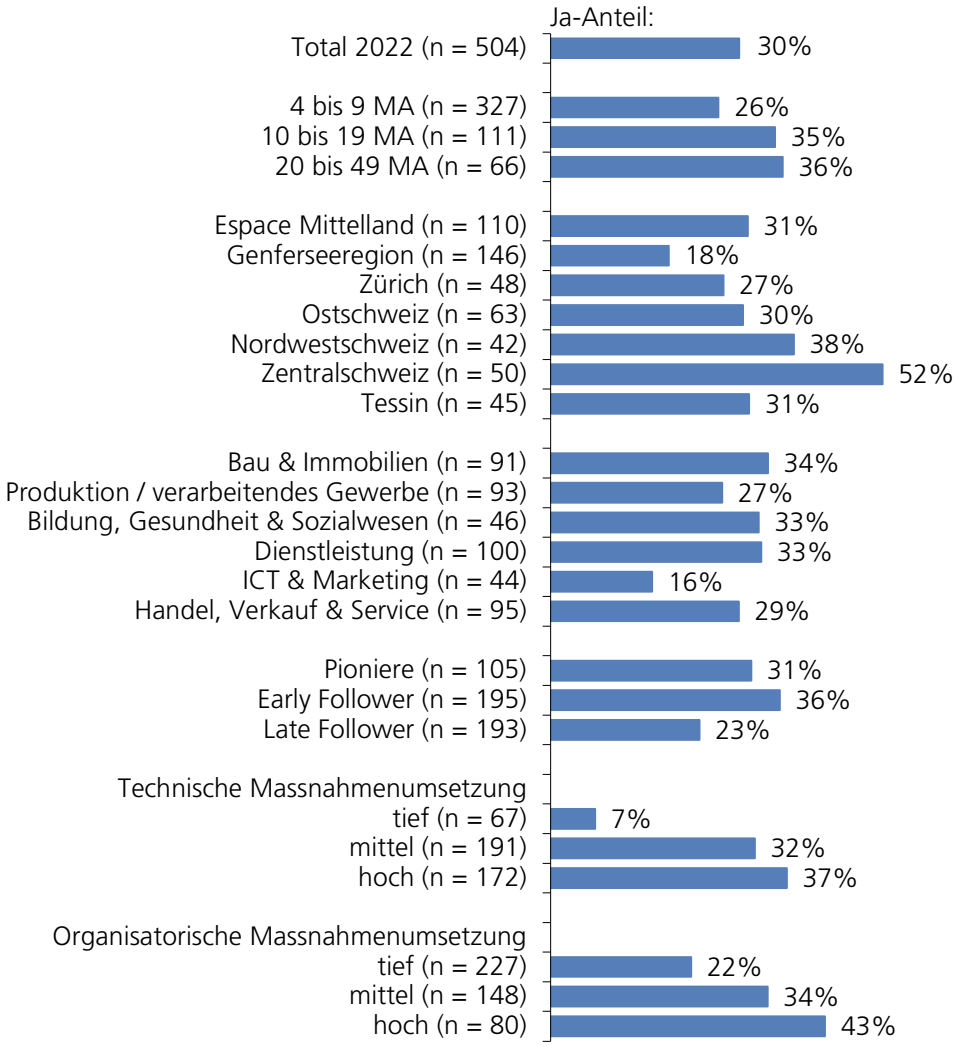
Wie schon bei den technischen Massnahmen, zeigt sich auch bei den organisatorischen Massnahmen ein höherer Umsetzungsgrad, wenn entweder die Geschäftsführung, ein externer IT-Dienstleister oder «jede/-r Mitarbeitende» verantwortlich ist. Vier von sieben Massnahmen werden am

besten umgesetzt, wenn der/die Befragte einen IT-Dienstleister als verantwortlich bezeichnet: Kontrolle der Wiederherstellbarkeit der Daten (4.5), Bereitstellung von IT-Sicherheitssupport (3.9), Implementierung eines Sicherheitskonzepts (3.4) und Durchführung eines Sicherheitsaudits (3.0).

3.4.9 Cyberversicherung

Frage 16:
Verfügt Ihr Unternehmen über eine Cyberversicherung?
Basis: Total, n = 504

Knapp ein Drittel (30 %) der befragten Geschäftsführenden verfügt über eine Cyberversicherung für das Unternehmen. Es handelt sich dabei eher um die oberen beiden Unternehmensgrössenkategorien (10–19 Mitarbeitende: 35 %, 20–49 Mitarbeitende: 36 %) als um die tiefere (4–9 Mitarbeitende: 26 %) und eher um Pioniere (31 %) und Early Follower (36 %) als um Late Follower (23 %). Besser informierte Befragte haben signifikant häufiger eine Cyberversicherung (38 %) als schlechter informierte (12 %). Auch die Sprachregionen unterscheiden sich: In der Deutschschweiz (36 %) und im Tessin (32 %) sind die Cyberversicherungen verbreiteter als in der Westschweiz (21 %). Und: Je höher die technische und organisatorische Massnahmenumsetzung fortgeschritten ist, desto eher besteht auch eine Cyberversicherung (Werte siehe Grafik 28).



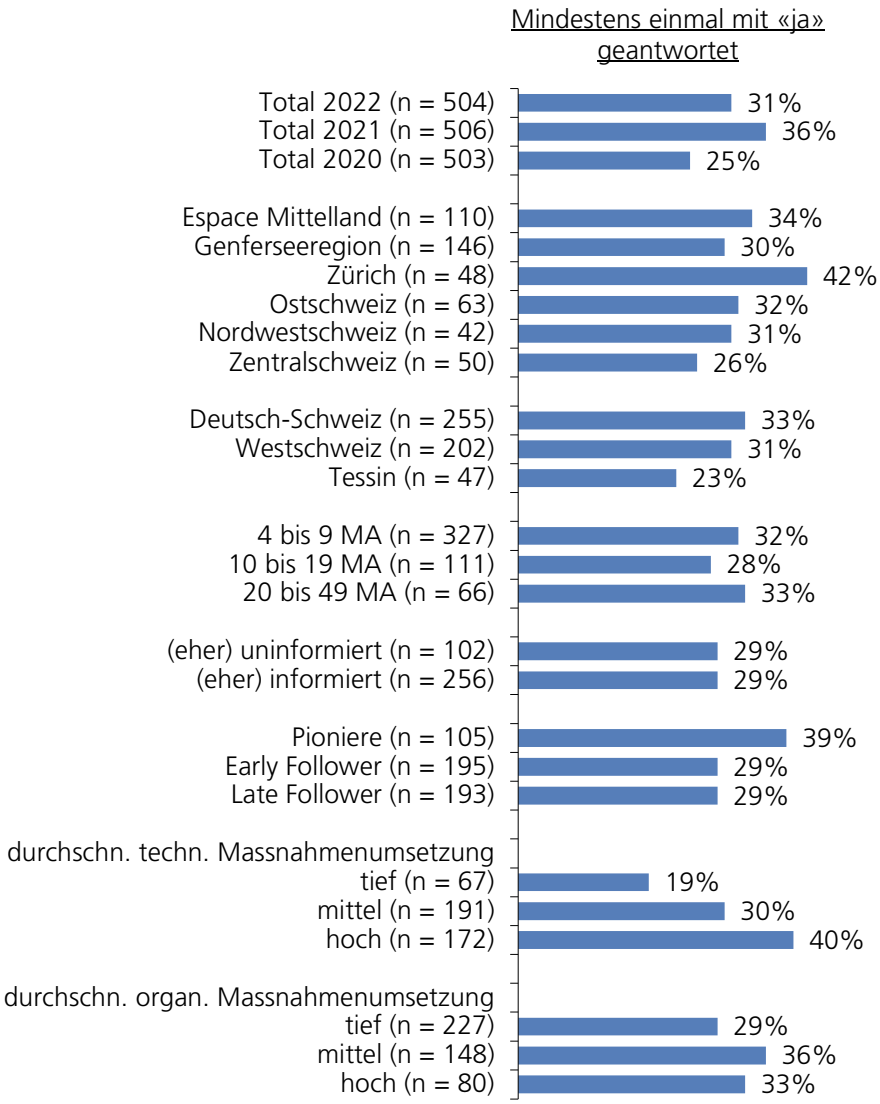
Grafik 28

3.4.10 Cyberangriffe und entstandener Schaden

Frage 17:
Wurde Ihre Firma schon einmal erfolgreich durch eine der folgenden Techniken angegriffen, so dass ein erheblicher Aufwand nötig war, um Schäden zu beheben?
Basis: Total, n = 504

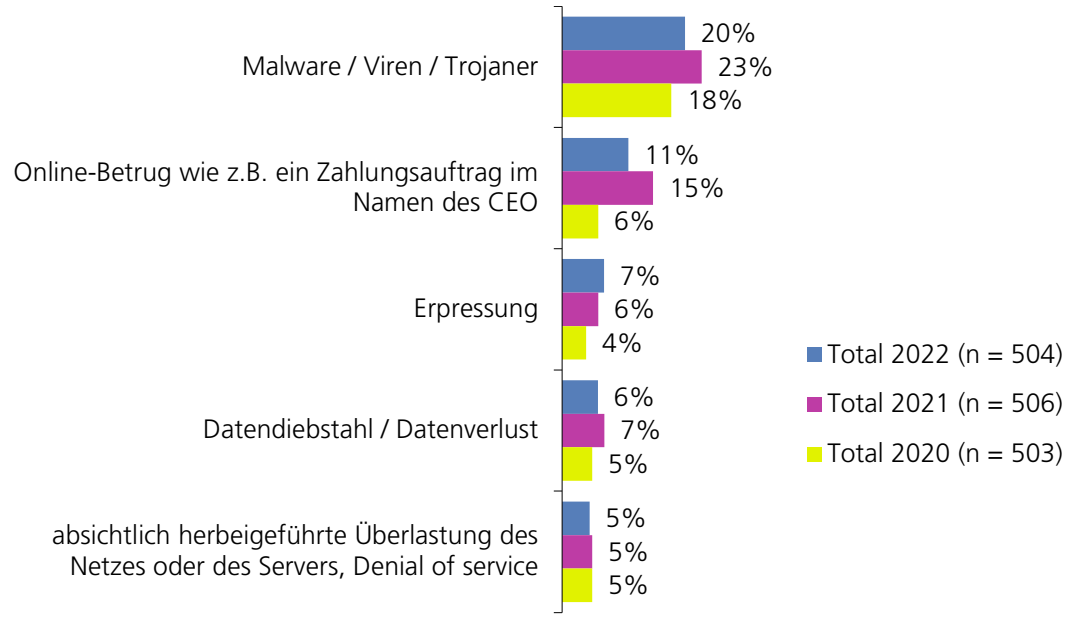
Nachdem der Anteil angegriffener Unternehmen von 2020 auf 2021 signifikant von 25 auf 36 Prozent stieg, sank er 2022 nur um wenige Prozentpunkte von 36 auf 31 Prozent.

Wie schon 2021 gibt es keine signifikanten Unterschiede zwischen den Subgruppen; selbst nicht zwischen denjenigen, welche sich ansonsten in dieser Studie konsequent unterschieden, wie zum Beispiel der hohe und tiefe Informationsgrad oder die Einstellung zu technischen Innovationen. Interessanterweise gilt aber: Je höher die technischen Sicherheitsmassnahmen umgesetzt sind, desto eher sind die Unternehmen schon einmal angegriffen worden (Werte siehe Grafik 29). Dieses Verhältnis galt schon bei den Ergebnissen 2021. Eine mögliche Erklärung ist, dass die betroffenen Unternehmen die entsprechenden Massnahmen *nach* dem Angriff umgesetzt haben und nun deshalb auf gutem Stand sind. Ausserdem ist davon auszugehen, dass höhere Massnahmen eher dazu führen, dass ein Angriff überhaupt festgestellt und somit in dieser Studie erwähnt wird.
Bei den organisatorischen Massnahmen ergibt sich ein ähnliches, wenn auch nicht so deutliches (nicht signifikantes) Bild: Unternehmen mit mittlerer und hoher Massnamenumsetzung verzeichnen tendenziell häufiger einen erfolgreichen Cyberangriff in der Vergangenheit als Unternehmen mit tiefer Massnahmenumsetzung (Werte siehe Grafik 29). Auch dieses Verhältnis galt schon 2021. Falls obenstehende Annahme stimmt, dass Angriffe zu höheren technischen Massnahmen führen, dann gilt dies offenbar weniger oder nicht für organisatorische Massnahmen.



Grafik 29

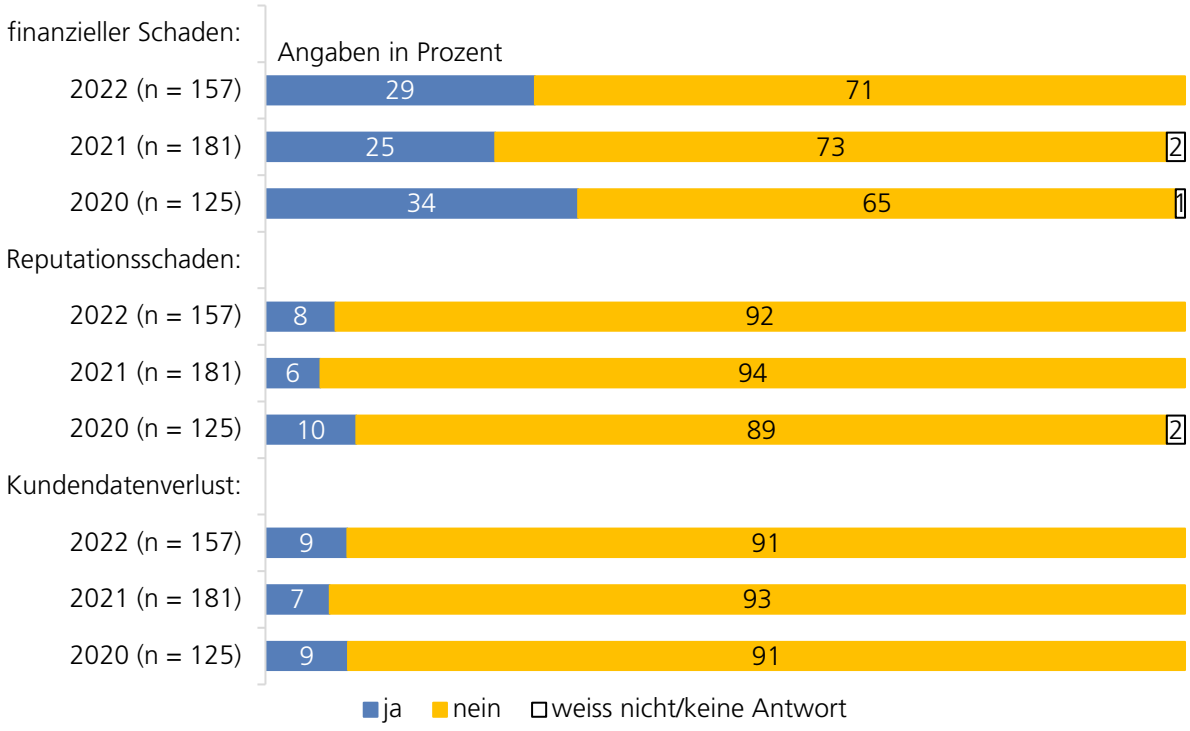
Die am häufigsten genannten Angriffe erfolgten, wie schon 2021, via Malware, Viren bzw. Trojaner: Ein Fünftel der Befragten (20 %) wurde so angegriffen. Dieser Wert liegt zwischen dem Ergebnis von 2020 (18 %) und 2021 (23 %). Die zweithäufigste genannte Angriffsform ist Onlinebetrug (11 %). Auch dieser Wert stieg 2021 sehr stark an (von 6 auf 15 %) und sank jetzt wieder leicht. Erpressungsfälle sind seit 2020 stetig angestiegen, die Unterschiede sind aber sehr klein und könnten auch durch Zufall entstanden sein (Werte siehe Grafik 30). Datendiebstahl und absichtlich herbeigeführte Überlastungen des Netztes oder Servers (DoS) liegen konstant bei einem zwanzigstel der Unternehmen (5 %).



Grafik 30

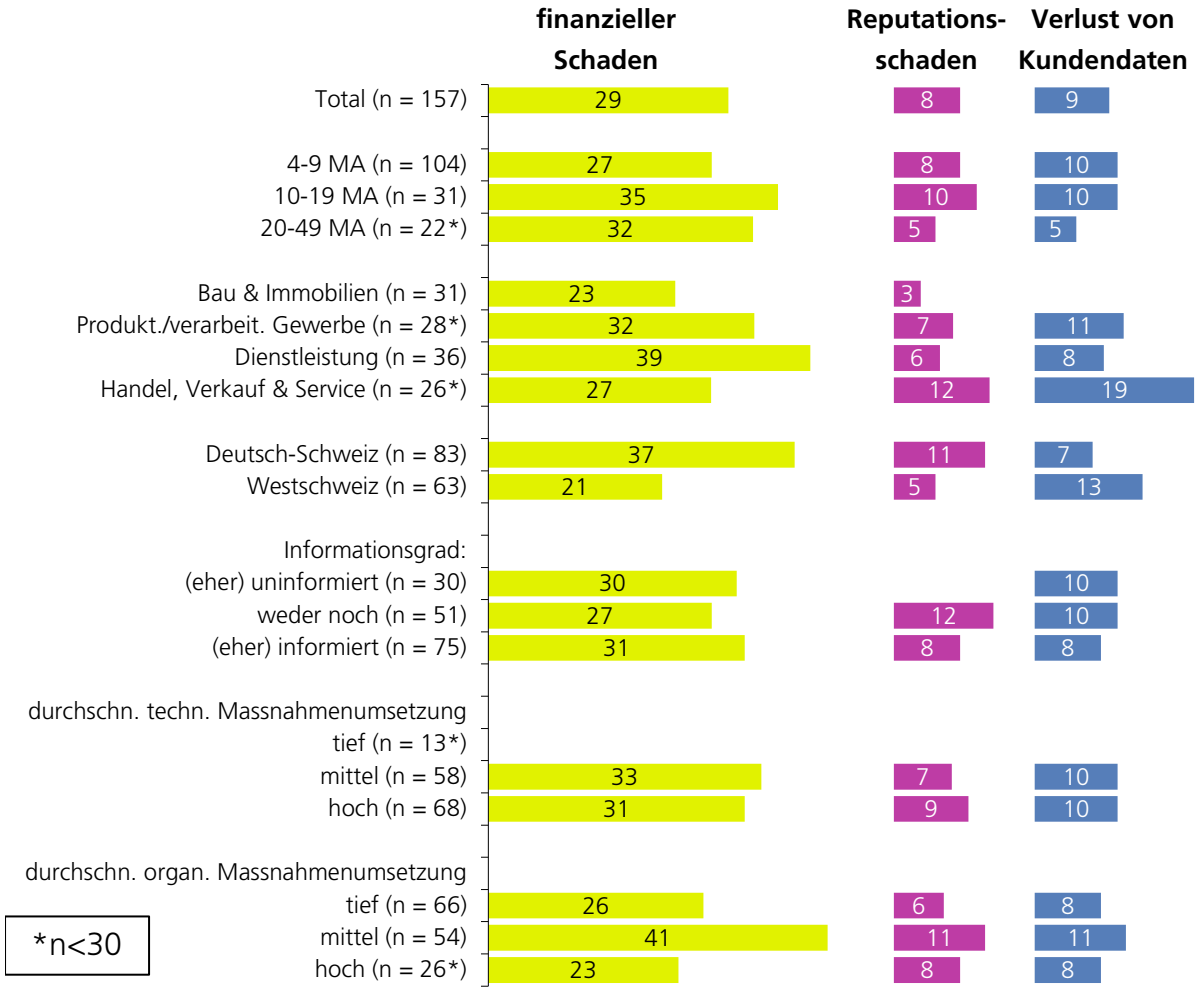
Der aus den Angriffen resultierende Schaden ist prozentual gegenüber dem letzten Jahr leicht gestiegen. Fast ein Drittel (29 %) beklagt einen finanziellen Schaden (2021: 25 %), je knapp ein Zehntel einen Reputationsschaden (8 %) oder einen Kundendatenverlust (9 %).

Frage 18:
Entstand durch diesen Angriff / Entstanden durch diese Angriffe …
Filter: Wurden Opfer von mindestens einem Angriff gemäss Frage 17, n = 157



Grafik 31

Zwischen den Subgruppen ergeben sich keine Unterschiede. Die verschiedenen Branchen, Regionen und Unternehmensgrössenkategorien sind in ähnlichem Masse von den Schäden betroffen.



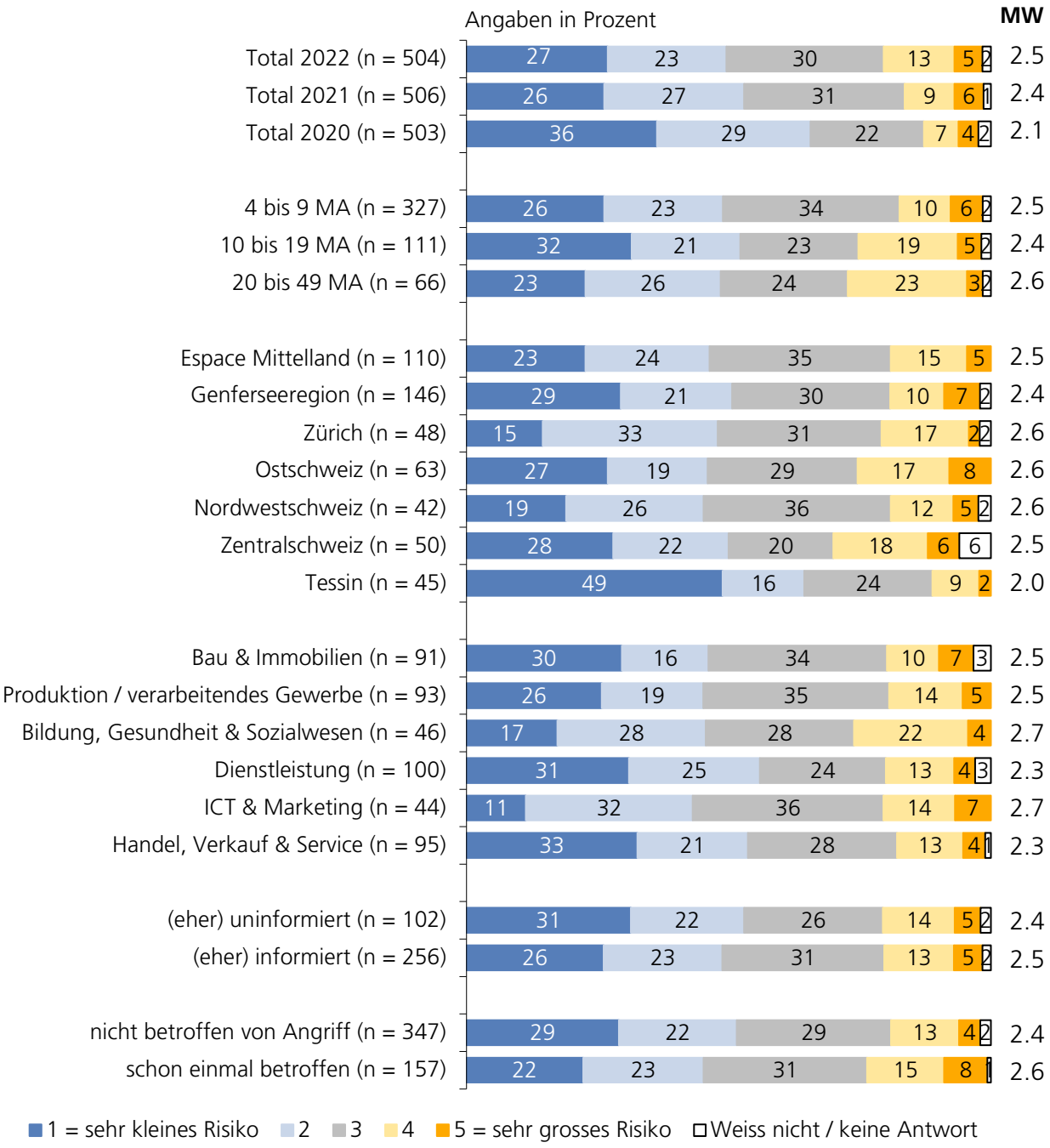
Grafik 32

3.4.11 Risiko-Einschätzung eines Cyberangriffs

Die Einschätzung des Risikos, durch einen Cyberangriff einen Tag lang ausser Kraft gesetzt zu werden, steigt 2022 zum zweiten Mal leicht an: 2020 lag der Mittelwert auf der Fünferskala noch bei einer 2.1, stieg dann 2021 auf 2.4 und liegt nun im Jahr 2022 bei 2.5. Der Anteil an Befragten, die das Risiko für sehr oder eher hoch einschätzen, einen Tag lang ausser Kraft gesetzt zu werden wegen eines Cyberangriffs, liegt mittlerweile bei knapp einem Fünftel (18 %). Die Hälfte der Befragten (50 %) hält dieses Risiko für eher oder sehr tief.

Frage 19:
Als wie hoch schätzen Sie das Risiko ein, dass Ihr Unternehmen innerhalb der nächsten zwei bis drei Jahre von einem Cyberangriff betroffen sein wird, der Ihr Geschäft für **mindestens einen Tag lang ausser Kraft** setzt?
Basis: Total, n = 504

Dieses Sicherheitsgefühl ist zwischen den Subgruppen gleichmässig bzw. innerhalb des Vertrauensbereichs verteilt; es ergeben sich nur wenige signifikante Unterschiede: Late Follower (Mittelwert 2.2) schätzen das Risiko signifikant tiefer ein als Pioniere (2.8) und Early Follower (2.6). Die Einschätzung der Late Follower hat sich gegenüber dem Vorjahr nicht verändert, während die Early Follower und Pioniere das Risiko 2022 etwas höher einschätzen als 2021 (Pioniere: 2.7, Early Follower: 2.5). Ausserdem gilt: Wer schon einmal von einem Cyberangriff betroffen war, schätzt das Risiko ebenfalls signifikant höher ein (2.6) als (noch) nicht Betroffene (2.4).

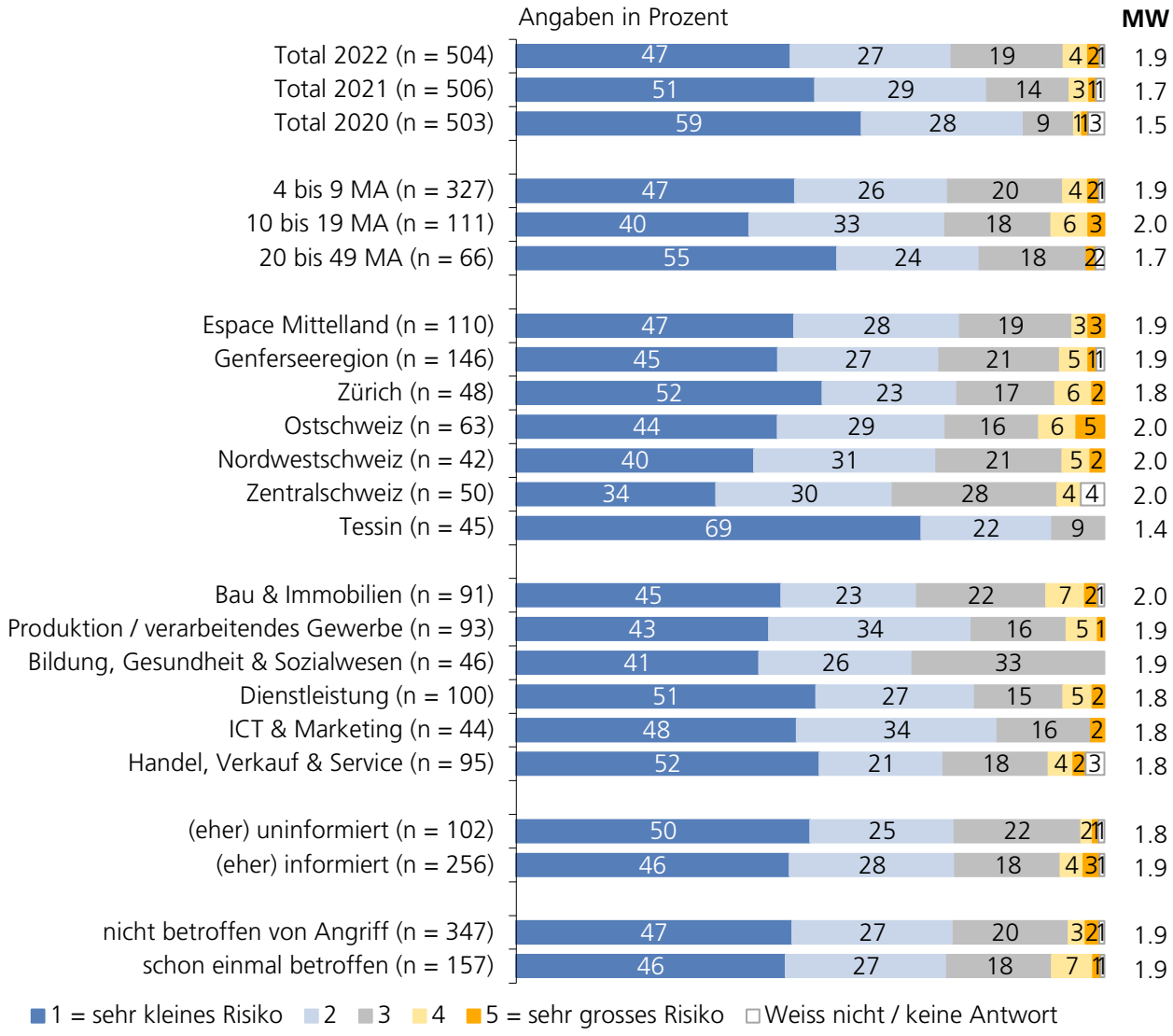


Grafik 33

Ein Cyberangriff als existenzgefährdendes Vorkommnis ist für nur sehr wenige Geschäftsführende ein realistisches Szenario, aber auch diese Einschätzung steigt seit 2020 kontinuierlich. Damals lag der Mittelwert auf der Fünferskala noch bei 1.5, 2021 bei 1.7 und jetzt bei 1.9. Der Anteil an Befragten, welche das Risiko eines existenzgefährdenden Cyberangriffs als eher oder sehr hoch einschätzen, liegt bei rund einem Zwanzigstel (6 %). Als eher oder sehr tiefes Risiko beurteilen es knapp drei Viertel der Befragten (74 %).

Frage 20:
Als wie hoch schätzen Sie das Risiko ein, dass Ihr Unternehmen innerhalb der nächsten 2–3 Jahre von einem Cyberangriff betroffen sein wird, der für Ihr Geschäft **existenzgefährdend** ist?
Basis: Total, n = 504

Nur bei einer einzigen Subgruppe gibt es einen signifikanten Unterschied: Deutsch- und Westschweizer Unternehmen (2.0 bzw. 1.8) schätzen das Risiko signifikant höher ein als Tessiner Unternehmen (1.4). Anders als bei der vorangegangenen Frage besteht hier kein Unterschied zwischen von Cyberangriffen betroffenen und nicht betroffenen (je 1.9); Betroffene erkennen also ein höheres Risiko von Cyberangriffen, die ein Unternehmen einen Tag ausser Kraft setzen können, nicht aber eines, das existenzgefährdend ist.



Grafik 34

3.4.12 Einstellung zu Cyberkriminalität

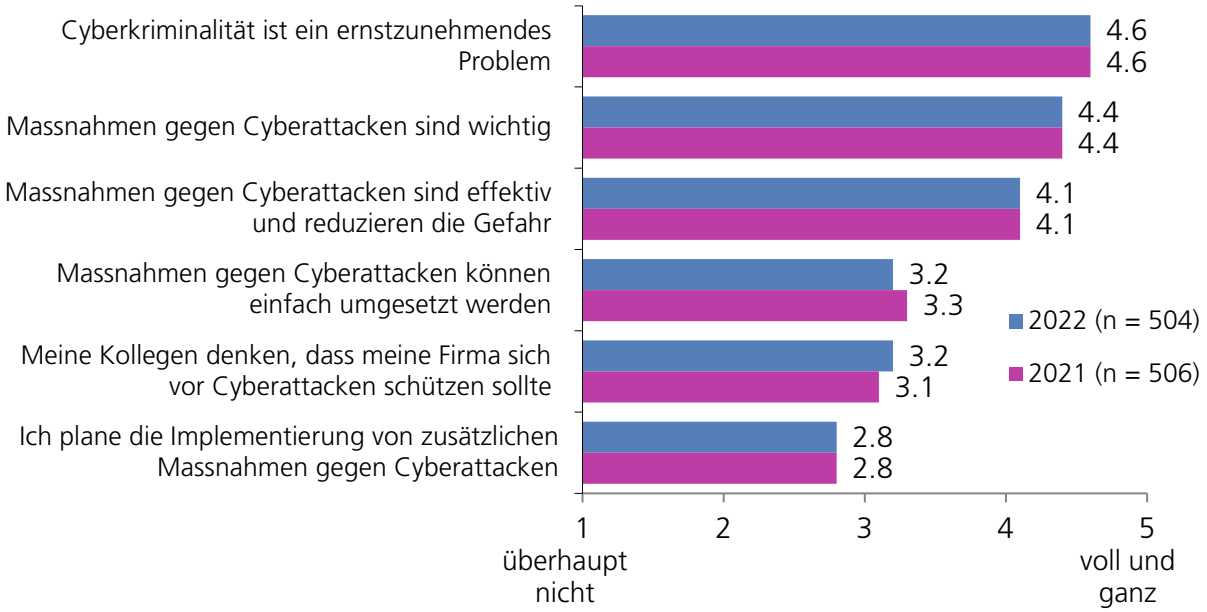
Die sechs abgefragten Aussagen zu Cyberkriminalität teilen sich in zwei Gruppen auf, von denen der einen deutlich häufiger zugestimmt wurde als der anderen. Unterschiede gegenüber 2021 gibt es kaum und wenn, dann sind sie marginal.

Frage 21:
Inwiefern stimmen Sie den folgenden Aussagen zu Cyberkriminalität wie Malware, Online-Betrug und Hacking zu?
Basis: Total, n = 504

Eine hohe Zustimmung mit Mittelwerten über 4 auf der Fünferskala erhielten: Cyberkriminalität ist ein ernstzunehmendes Problem (4.6), Massnahmen gegen Cyberattacken sind wichtig (4.4) und Massnahmen gegen Cyberattacken sind effektiv und reduzieren die Gefahr (4.1). Diejenigen Einstellungen, welche auf konkrete Handlungen bezogen sind, erhalten deutlich weniger Zustimmung: Massnahmen gegen Cyberattacken können einfach umgesetzt werden (3.2), meine Kollegen denken, dass meine Firma sich vor Cyberattacken schützen sollte (3.2) und ich plane die Implementierung von zusätzlichen Massnahmen gegen Cyberattacken (2.8). Die Gefahr wird also grundsätzlich erkannt, Massnahmen dagegen scheinen aber eher als zu schwierig, als unnötig oder als zu aufwändig betrachtet zu werden. Die beiden Aussagen mit eher tiefer Zustimmung:

- Massnahmen gegen Cyberattacken können einfach umgesetzt werden
- Meine Kollegen denken, dass meine Firma sich vor Cyberattacken schützen sollte

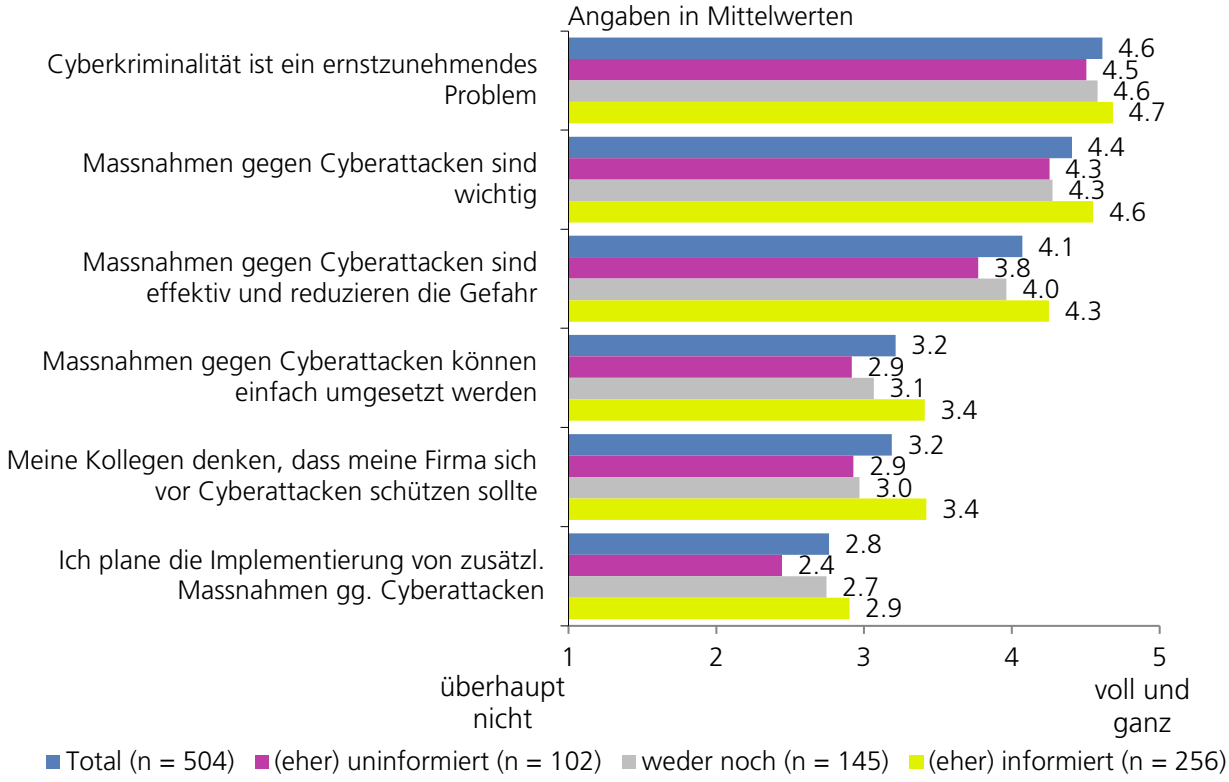
… können sich als Verhaltenshemmnisse zeigen. Wenn die Befragten sich die Massnahmen nicht zutrauen bzw. keinen sozialen Druck verspüren, Massnahmen zu ergreifen, wirkt sich dies negativ auf ihre Handlungen aus.



Grafik 35

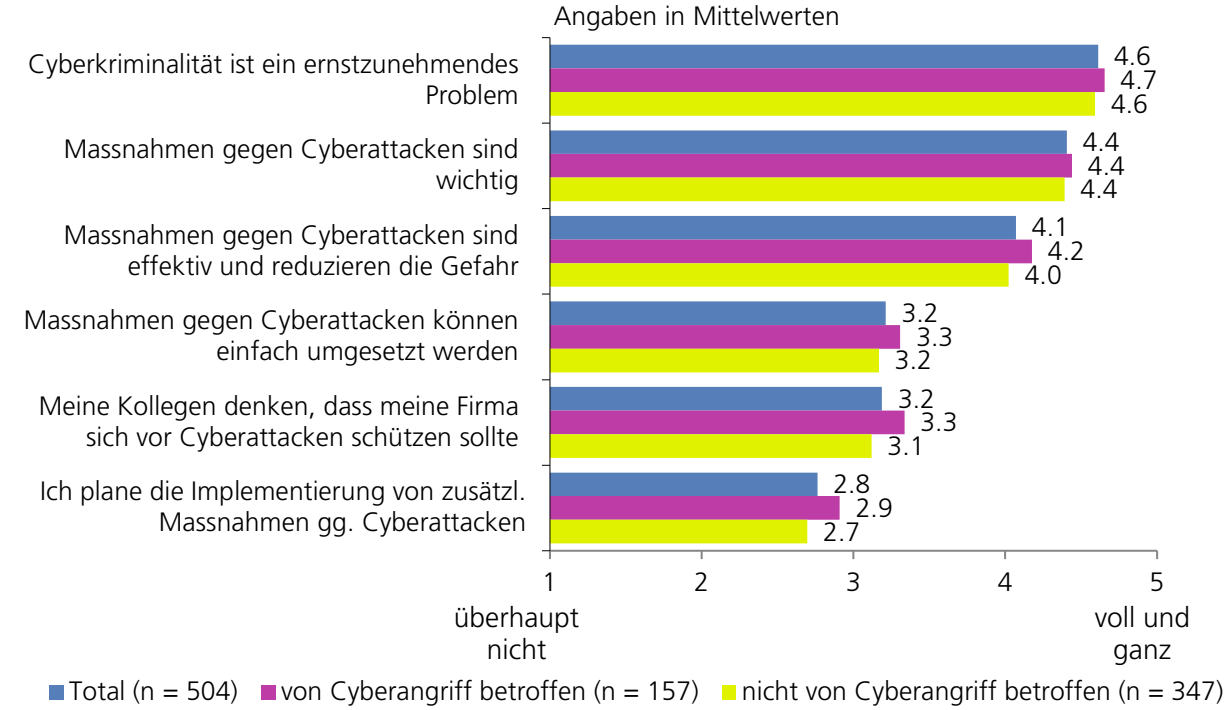
Zwischen Branchen und Regionen gibt es keine auffälligen Unterschiede, mit Ausnahme der ICT & Marketingbranche, welche der Aussage «Meine Kollegen denken, dass meine Firma sich vor Cyberattacken schützen sollte» stärker zustimmt (Mittelwert 4.0) als die anderen Branchen (Mittelwerte 2.9 bis 3.3).

Bei allen Aussagen steigt die Zustimmung mit dem gefühlten Informationsgrad zum Thema Cyberrisiken. Die Unterschiede sind alle signifikant ausser bei der Aussage «Cyberkriminalität ist ein ernstzunehmendes Problem» (Werte siehe Grafik 36).



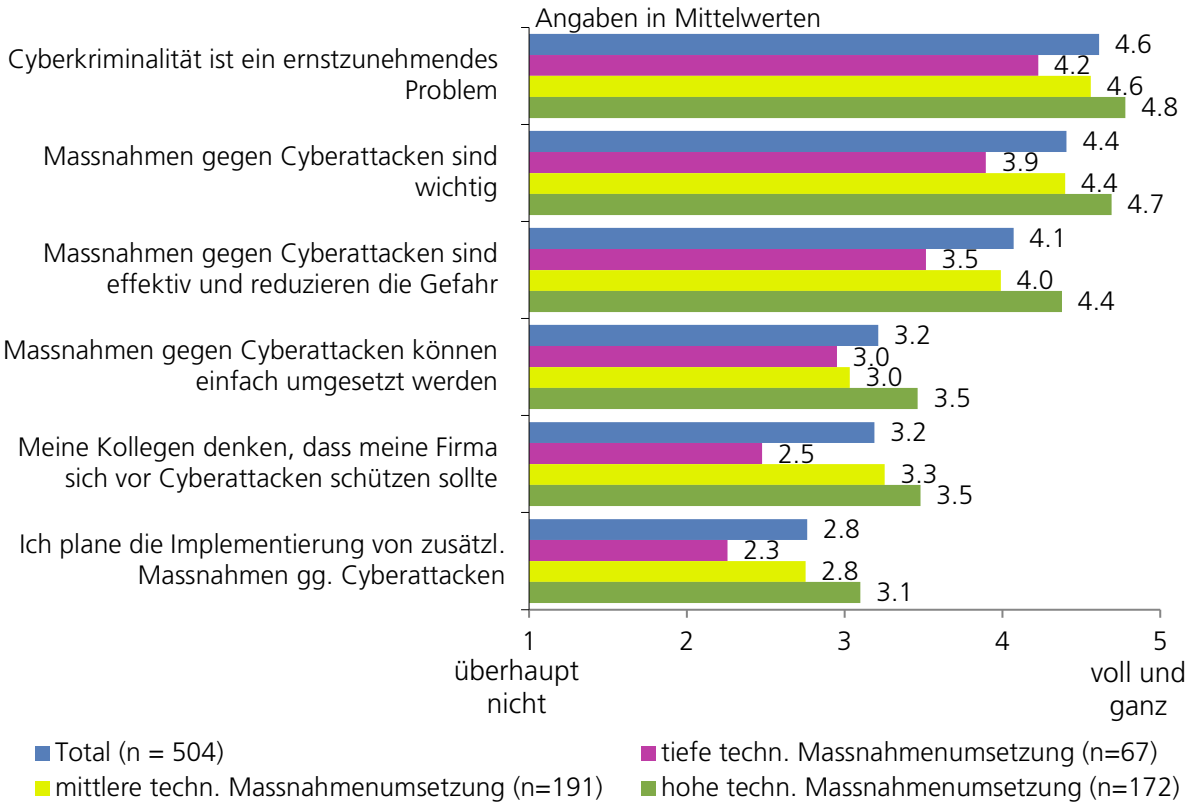
Grafik 36

Auch bereits einmal von einem Cyberangriff betroffene Befragte stimmen den Aussagen eher zu (Werte siehe Grafik 37), der Unterschied ist allerdings nicht signifikant.

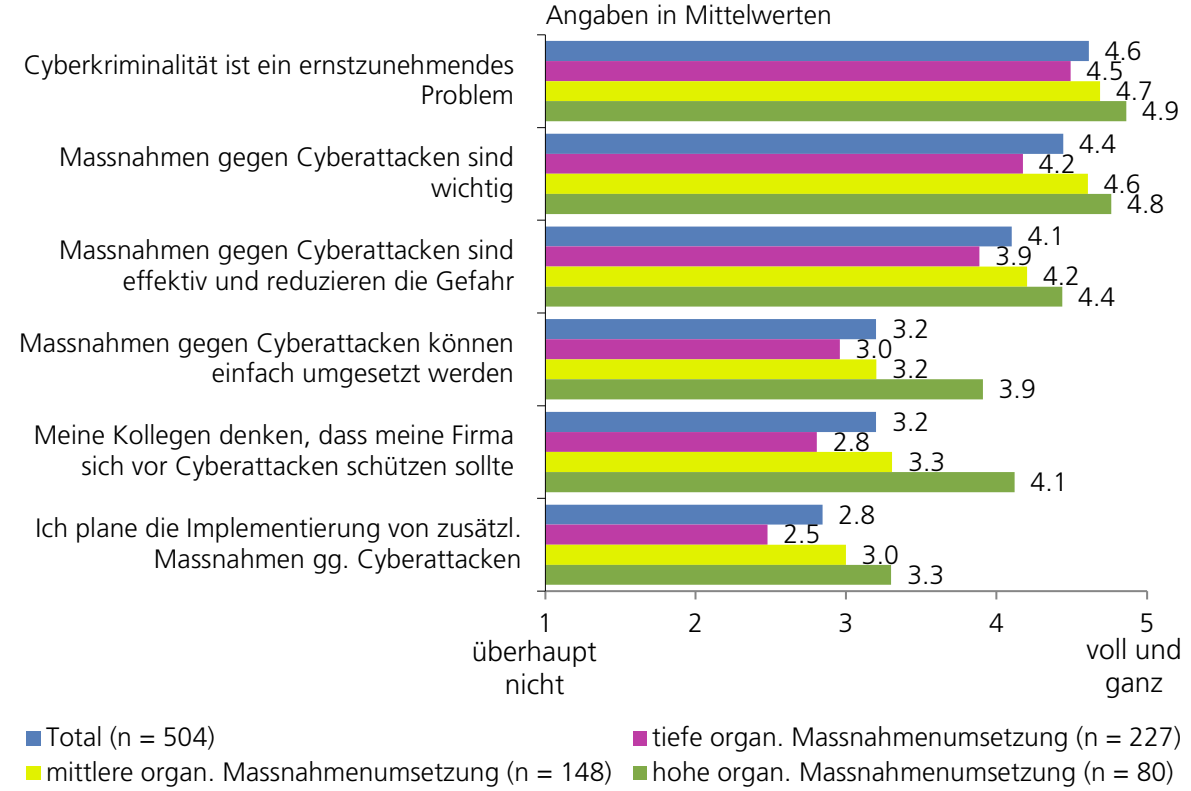


Grafik 37

Ausserdem gilt bei sämtlichen Aussagen: Je höher die technische oder organisatorische Sicherheitsmassnahmenumsetzung ist, desto höher ist auch die Zustimmung zu den Aussagen (Werte siehe Grafiken 38 und 39), Unterschiede sind signifikant).



Grafik 38



Grafik 39

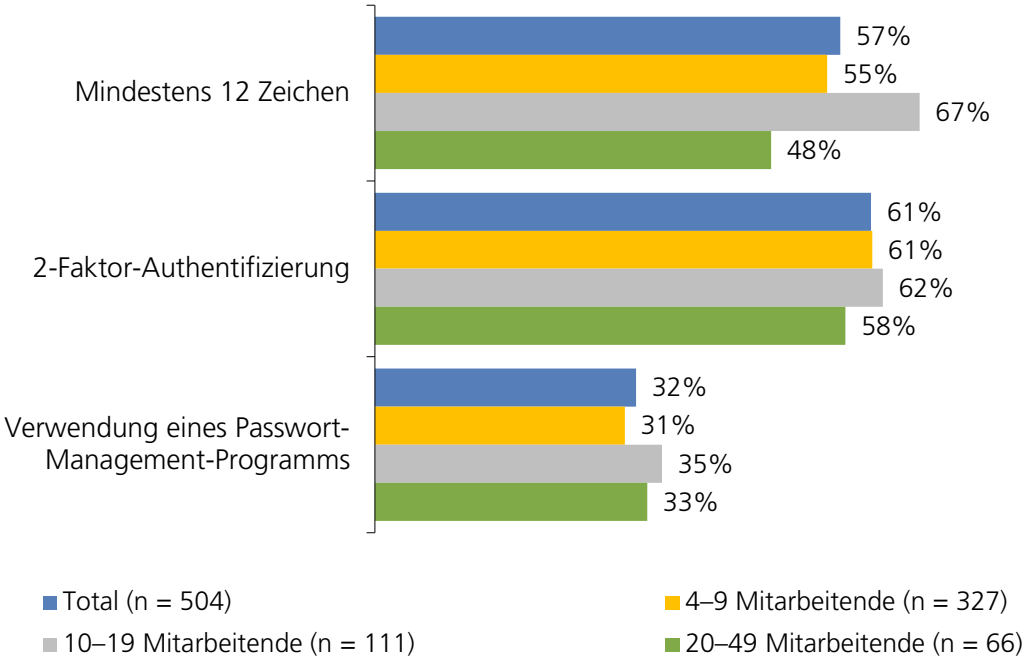
3.4.11 Passwort-Sicherheitsvorkehrungen

Über vier Fünftel (83 %) der Befragten haben mindestens eine Passwort-Sicherheitsvorkehrung getroffen. Die gegenüber digitalen Innovationen aufgeschlossenen Befragten (Pioniere) haben mehr Passwort-Sicherheitsvorkehrungen getroffen (90 % mindestens eine Massnahme) als Early Follower (83 %) und Late Follower (79 %).

Frage 22:
Welche der folgenden Passwort-Sicherheitsvorkehrungen haben Sie in Ihrem Unternehmen umgesetzt?
Basis: Total, n = 504

Bei den (eher) gut bezüglich Cyberrisk informierten Befragten ist der Anteil derjenigen, welche *alle* vorgelesenen Massnahmen umgesetzt haben, signifikant höher als bei den (eher) schlecht informierten (20 % vs. 9 %).
Firmen mit 10 bis 19 Mitarbeitenden setzen etwas (nicht signifikant) häufiger Passwort-Sicherheitsmassnahmen um (90 % mindestens eine Massnahme) als die kleineren Firmen mit 4 bis 9 Mitarbeitenden (81 %) und die grösseren mit 20 bis 49 Mitarbeitenden (79 %).
Und es gilt: Je mehr technische und organisatorische Massnahmen generell umgesetzt sind, desto eher werden auch Passwort-Sicherheitsvorkehrungen getroffen.

Die am häufigsten umgesetzte Passwort-Massnahme ist die Zwei-Faktor-Authentifizierung: Mehr als sechs von zehn Befragten (61 %) setzen darauf. Mehr als die Hälfte (57 %) verlangt mindestens 12 Zeichen. Rund ein Drittel (32 %) verwendet einen Passwort-Manager.



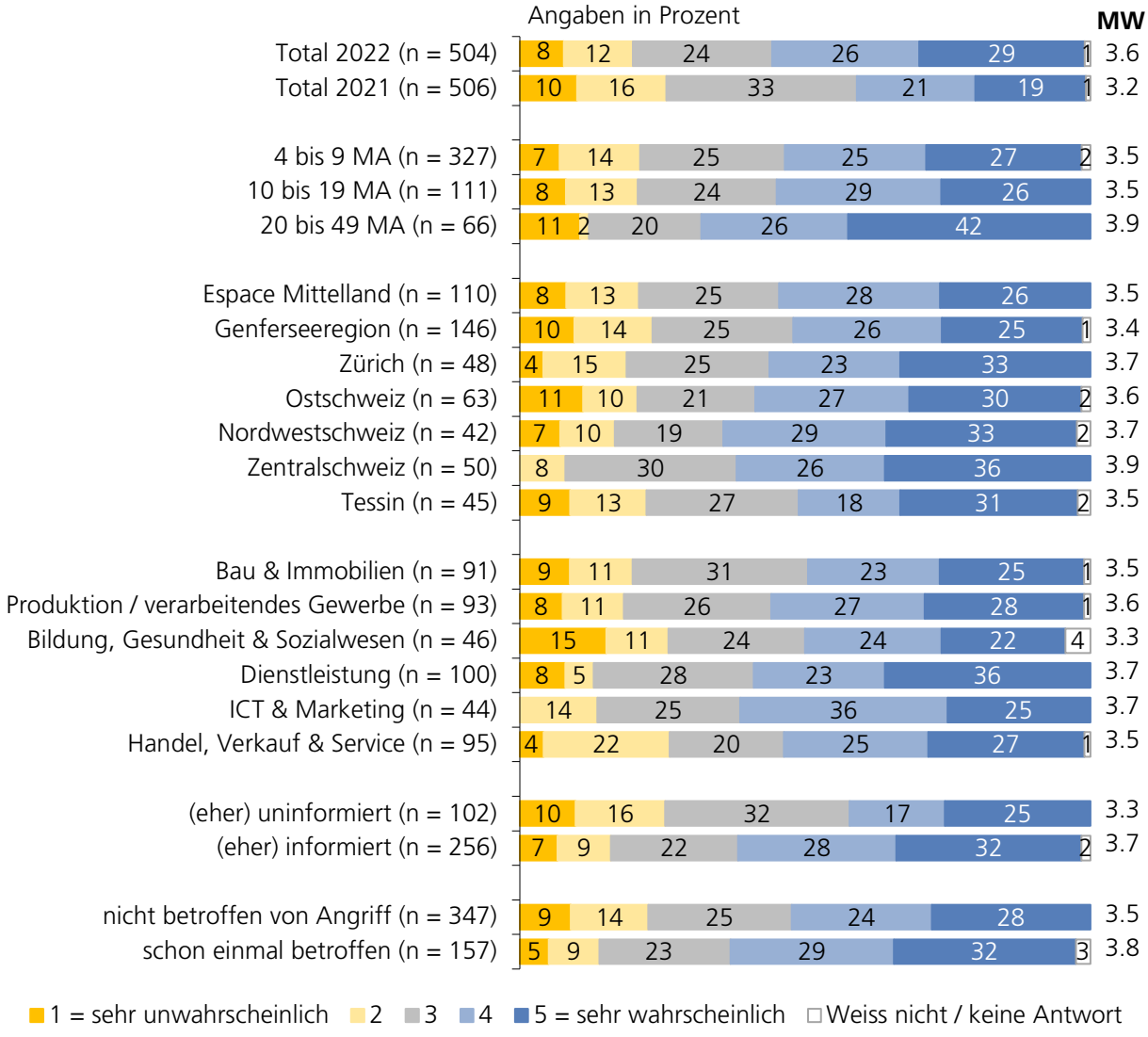
Grafik 40

3.4.12 Geplante Erhöhung der Sicherheitsmassnahmen

Fast ein Drittel (29 %) der Befragten halten es für sehr wahrscheinlich (Skalenwert 5), dass sie in den nächsten 1 bis 3 Jahren ihre Sicherheitsmassnahmen gegen Cyberkriminalität erhöhen. Seit dem letzten Jahr (19 %) hat sich dieser Anteil somit um rund die Hälfte erhöht. Rund ein weiterer Viertel (26 %) hält eine Sicherheitserhöhung für eher wahrscheinlich (Skalenwert 4). Der Mittelwert stieg seit dem Vorjahr von 3.2 auf 3.6.

Frage 23:
Wie wahrscheinlich ist es, dass Sie in den kommenden 1 bis 3 Jahren die Sicherheitsmassnahmen gegen Cyberkriminalität erhöhen werden?
Basis: Total, n=504

Pioniere (3.9) und Early Follower (3.7) gehen signifikant häufiger von einer Erhöhung der Sicherheitsmassnahmen aus als Late Follower (3.3), und auch die bezüglich Cyberrisiken eher bis sehr gut informierten Befragten wollen ihre Sicherheitsmassnahmen eher erhöhen (3.7) als die eher bis sehr uninformierten (3.3). Wer schon einmal von einem Angriff betroffen war, will die Massnahmen eher erhöhen (3.8) als wer noch nie betroffen war (3.5). Die Unterschiede zwischen den Regionen, Branchen und Firmengrössen (Werte siehe Grafik 41) sind nicht signifikant.



Grafik 41

3.5 Datenschutz

Im Hinblick auf das neue Datenschutzgesetz wurde auch eine Frage zu den Massnahmen zum Schutz von personenbezogenen Daten gestellt. Die Antworten auf diese Frage sind jedoch – wahrscheinlich aufgrund hoher sozialer Erwünschtheit – nicht interpretierbar. Die Projektpartner verzichten deshalb auf die Dokumentation der Ergebnisse und werden sie evt. zu einem späteren Zeitpunkt kommunizieren.

4 Studiendesign in Kürze

Projektpartner:	Schweizerische Mobiliar Versicherungsgesellschaft AG Digitalswitzerland Allianz Digitale Sicherheit Schweiz Fachhochschule Nordwestschweiz FHNW Schweizerische Akademie der Technischen Wissenschaften SATW
Inhalt:	Stellenwert und Nutzung Homeoffice, Cybersicherheit, Datenschutz
Grundgesamtheit:	Geschäftsführende von kleinen Unternehmen (4-49 Mitarbeitende) in der Deutsch-, Westschweiz und im Tessin
Methode:	Telefonische Befragung (CATI)
Stichprobe:	504 durchgeführte Interviews
Gewichtung:	Keine
Quoten	proportional nach Unternehmensgrössen (4-9, 10-19, 20-49)
Interviewdauer:	17.4 Minuten
Sprachen:	Deutsch, Französisch, Italienisch.
Auswertung:	Tabellenband Grafiken Schriftlicher Bericht
Feldphase:	28. Februar bis 30. März 2022
Projektleiterin gfs-zürich:	Karin Mändli Lerch
Projektmitarbeiterin:	Mara Tanner