gfs-zürich | MARKT- & SOZIALFORSCHUNG

Schlussbericht 2023:

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 & Mara Huber (Projektleitung)

Zürich, 24. Juli 2023

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

SWISS INSIGHTS
Swiss Data Insights Association

Inhaltsverzeichnis

1 Management Summary

Im Frühling 2022 wurden die letzten Covid-Massnahmen aufgehoben und die Schweiz kehrte langsam in die Normalität zurück. Nach einem Lockdown, zwei Homeoffice-Pflicht- und -Empfehlungsphasen hat sich die Arbeitswelt verändert. Aber noch während bezüglich Covid endlich Entspannung eintrat, überfiel Russland die Ukraine. Der Krieg brachte eine drohende Energiemangellage mit sich, weshalb man plötzlich über Homeoffice aufgrund ungeheizter Bürogebäude nachdachte. Nötig wurde eine weitere Homeoffice-Phase aber nicht. Jedoch bekam das Thema «Cybercrime» eine neue Dimension durch den Krieg: Angriffe von russischen Hackern auf westliche Infrastrukturen machten Schlagzeilen und nach der Video-Ansprache Selenskis im Bundeshaus am 15. Juni 2023 betraf es auch die Schweiz. Zu diesem Zeitpunkt war die Feldzeit dieser Studie allerdings gerade beendet (Feldende am 13. Juni 2023), und auch der grosse Databreach bei einer Berner Software-Firma, bei dem der Bund sensible Daten verlor, hatte keinen Einfluss mehr auf die hier vorliegenden Resultate.

Vor diesem Hintergrund wurde die vierte Welle zu den Auswirkungen der Corona-Krise auf die Digitalisierung und Cybersicherheit in Schweizer KMU durchgeführt. Es wurden 502 Geschäftsführende von KMU mit 4 bis 49 Mitarbeitenden in der Deutsch-, Französisch- und Italienischsprachigen Schweiz telefonisch befragt.

1.1 Homeoffice: Angebot und Nachfrage

Die Anzahl der Arbeitsstellen, welche von den Geschäftsführenden als homeoffice-tauglich bezeichnet werden ist das vierte Jahr in Folge rückläufig: von durchschnittlich 3.8 Homeofficestellen pro Unternehmen im Jahr 2020 ging es 2021 zurück auf 3.4, auf 2.9 im Jahr 2022 und nun auf 2.5 im Jahr 2023. Wahrscheinlich verändern sich aber nicht die Arbeitsstellen an sich, sondern die Einschätzung der Arbeitgebenden, welche Ihre Mitarbeitenden gerne wieder vor Ort hätten.

Nachdem in den letztjährigen Studien der Fokus auf dem Homeoffice-Anteil vor, während und nach den Pflichtphasen lag, wurde die Frage nach effektiv im Homeoffice tätigen Arbeitnehmenden angepasst: Neu wurde 2023 gefragt, wie viele Personen *hauptsächlich* und wie viele *teilweise* im Homeoffice tätig sind (bisher: nur *hauptsächlich*). Über alle Befragte gesehen, ist je rund ein Fünftel der Mitarbeitenden *hauptsächlich* (21 %) und *teilweise* (21 %) im Homeoffice, insgesamt also rund zwei Fünftel (42 %). Besonders viele Homeoffice-Mitarbeitende haben Firmen mit 4 bis 9 Mitarbeitenden (49 %), die Branchen Finanz-Dienstleistungen, Information und Kommunikation (89 %) sowie Dienstleistungen (50 %) und Firmen in den Grossregionen Zürich (53 %) und Genfersee (55 %). Ein Vergleich zu den Vorjahresstudien ist aufgrund der veränderten Fragestellung nicht möglich; tendenziell scheint es aber eher eine Steigerung als ein Rückgang zu sein. Dies steht im Widerspruch zu den sinkenden Zahlen bei den Homeoffice-tauglichen Stellen (siehe vorheriger Absatz), und zeigt somit die wahrscheinlich vorhandenen Differenzen zwischen Arbeitge-

benden und Arbeitnehmenden: Erstere möchten ihre Mitarbeitenden gerne zurück am Arbeitsplatz, zweitere möchten im Homeoffice arbeiten. Aufgrund des Fachkräftemangels können Arbeitnehmende dabei wahrscheinlich ihre Ansprüche eher durchsetzen.

Mit Blick auf die Zukunft gehen die Geschäftsführenden davon aus, dass sich bezüglich Homeoffice nicht mehr viel verändern wird: Rund drei Viertel (73 %) erwarten einen gleichbleibenden Anteil Mitarbeitender im Homeoffice, nur rund jede/-r zehnte (9 %) einen sinkenden Anteil und rund jede-/r siebte (15 %) einen steigenden Anteil. Nachdem diese Zahlen sich in den letzten Jahren stark verändert hatten – erst wurde eine Steigerung erwartet, dann ein Rückgang – scheint sich die Lage nun einzupendeln.

Ein «Einpendeln» zeigt sich auch bei der Anzahl verwendeter Kommunikationsmittel. Diese hat während der Pandemie gewisse Höhenflüge erlebt und ist nun rückläufig. Dies ist insbesondere der Fall bei Online Konferenztools wie Skype, Teams, Zoom oder Google Meet (von 62 % im Jahr 2022 auf 45 % im aktuellen Jahr) sowie Online Beratungen oder -Schulungen (von 39 % in den Jahren 2021 und 2022 auf 23 % im aktuellen Jahr).

1.2 Wichtigkeit der IT-Dienstleister

Rund vier Fünftel der befragten Unternehmen (79 %) lassen sich von einem (44 %) oder mehreren (35 %) IT-Dienstleistern unterstützen. KMU, die über mindestens einen IT-Dienstleister verfügen, vergeben rund einen Drittel (36 %) der IT-Arbeiten auswärts, und rund 8 von 10 lassen sich auch von ihnen bezüglich Cybersicherheit beraten (84 %). Die Hälfte (53 %) dieser Befragten bestätigen, dass ihr IT-Dienstleister über eine IT-Sicherheitszertifizierung (z.B. ISO 27001 oder CyberSeal der Allianz Digitale Sicherheit Schweiz) verfügt. Auffallend viele Befragte – rund ein Drittel (34 %) – weiss nicht, ob ein entsprechendes Zertifikat vorliegt. Das könnte an noch mangelnder Bekanntheit der Zertifikate liegen oder daran, dass vielen Befragten die Zertifizierung nicht wichtig ist. Es besteht ein gewisser Verdacht, dass IT-Dienstleister per Definition als kompetent im Bereich Cybersicherheit wahrgenommen werden, ohne dass diese Kompetenz überprüft wird. Dies birgt Gefahren und die Autorenschaft erwartet, dass die Nachfrage nach Zertifizierungen zukünftig steigen wird.

Rund jede/-r siebte Geschäftsführende (14 %) hat in den letzten ein bis zwei Jahren einen bestehenden IT-Dienstleister durch einen neuen ersetzt. Die genannten Gründe dafür sind in erster Linie die interne Optimierung und Kompatibilität sowie die Kommunikation und Service-Qualität. Rund zwei Drittel (64 %) der Befragten sagt, der Wechsel sei eher oder sehr einfach gewesen.

Die Befragten, die ihren IT-Dienstleister nicht in den letzten ein bis zwei Jahren ersetzt haben, sind grundsätzlich sehr zufrieden mit ihnen: Rund neun von zehn (90 %) geben an, eher oder sehr zufrieden zu sein. Der Hauptgrund für die Zufriedenheit ist die Erreichbarkeit bzw. Reaktionszeit.

1.3 Cybersicherheitsmassnahmen: Wenig Veränderung

Der gefühlte Informationsstand der Befragten bezüglich Cyberrisk-Thematik hat sich seit der ersten Befragung 2020 ein wenig verbessert: Etwas mehr als die Hälfte (56 %) fühlt sich eher oder sehr gut informiert (2020:47 %), der Mittelwert liegt bei 3.6 (2020: 3.4). Dabei gibt es einige deutliche Unterschiede zwischen den Subgruppen; so fühlen sich Pioniere (4.2) signifikant besser informiert als Early Follower (3.6) und Late Follower (3.3). Zudem fühlen sich Befragte, die schon viele technische (3.9) und/oder organisatorische Massnahmen (4.2) umgesetzt haben, signifikant besser informiert als Befragte mit tiefem Umsetzungsgrad (2.7 bzw. 3.1).

Trotz häufiger Berichterstattung in den Medien und auch trotz des neuen Datenschutzgesetzes, welches im September 2023 gültig wird, hat sich die Wahrnehmung der Wichtigkeit des Themas Cybersicherheit nicht verändert. Knapp zwei Drittel (65 %) der Befragten schätzen das Thema als eher oder sehr wichtig ein; der Mittelwert liegt bei 3.8 (2022: 3.8, 2021: 3.9, 2020: 3.9). Je mehr Mitarbeitende ein Unternehmen beschäftigt, desto höher wird die Cybersicherheit priorisiert (4–9 Mitarbeitende: 3.7, 10–19 Mitarbeitende: 3.9, 20–49 Mitarbeitende: 4.2). Besonders hoch ist die Priorisierung in den Grossregionen Tessin (4.1) und Zürich (4.0), in den Branchen Finanz-Dienstleistungen, Information und Kommunikation (4.4), bei den Pionieren (4.4) sowie bei den Befragten mit hohen technischen (4.2) und organisatorischen (4.6) Massnahmenumsetzungsgraden.

Zur Eruierung der technischen Massnahmenumsetzung wurden – wie schon in den Vorjahren – sieben verschiedene Massnahmen nach ihrem Umsetzungsgrad abgefragt. Die Umsetzungsgrade liegen zwischen 3.9 und 4.5 auf der Fünferskala, alle fast unverändert zu den Vorjahren. Unternehmen mit 20 bis 49 Mitarbeitenden heben sich dabei deutlich ab von den kleineren Unternehmen; sie haben bei allen Massnahmen einen höheren Umsetzungsgrad. Das gleiche gilt für die Pioniere und die (eher) gut Informierten, die bei allen Massnahmen mit einen höheren Umsetzungsgrad angeben als die Early und Late Follower bzw. die (eher) schlecht Informierten.

Gleiches gilt für die organisatorischen Massnahmen: Bei den sieben abgefragten Massnahmen liegen die Umsetzungsgrade zwischen 2.8 und 4.2 auf der Fünferskala, ebenfalls alle praktisch unverändert zu den Vorjahren. Am ehesten fand eine Entwicklung statt bei der Massnahme *vorsichtiges Verhalten beim Teilen von persönlichen Informationen* (Steigerung von 4.0 auf 4.2), allenfalls hat hier das neue Datenschutzgesetz einen gewissen Einfluss. Weiterhin gilt: Organisatorische Massnahmen werden seltener umgesetzt als technische. Regelmässige Mitarbeiterschulungen (2.9) und die Durchführung eines Sicherheitsaudits (2.8) sind die am seltensten umgesetzten Massnahmen.

Es besteht ein deutlicher Zusammenhang zwischen der technischen bzw. organisatorischen Massnahmenumsetzung und dem Informationsgrad, der Priorisierung des Themas Cyberrisk und der Einstellung zu technischen Innovationen.

Zwei Fünftel der Befragten (40 %) geben an, eine Cyberversicherung zu haben, was eine ausgeprägte Steigerung zur Vorjahreszahl (30 %) bedeutet. Eventuell ist das ein Hinweis darauf, dass die Wichtigkeit des Themas doch ein bisschen gestiegen ist, obwohl die Befragten dies nicht so

angeben (siehe Kapitel 3.5.2, Wichtigkeit des Themas Cybersicherheit). Die Autorenschaft schätzt diese Zahl als zu hoch ein und geht davon aus, dass viele Befragte von ihrer normalen Versicherung einen Schutz bei Cyberangriffen erwarten.

Die Frage nach erfolgten Cyberangriffen wurde 2023 modifiziert. Bisher wurde direkt nach der Angriffstechnik gefragt, was verschiedene Nachteile hatte: Die Befragten wussten nicht immer, über welche Technik sie angegriffen wurden und häufig traf eine Kombination verschiedener Techniken zu. Zudem wurde durch das Vorlesen der verschiedenen Angriffstechniken die Erinnerung an einzelne Vorfälle eher geweckt und somit wurden zu viele leichte Angriffe angegeben. Dies zeigte sich durch die vielen Befragten, die dann in der der Folgefrage «keine Schäden» angaben. Die neue Fragestellung sollte sich ohne Ablenkung durch die Angriffstechnik auf die schwereren Fälle fokussieren. Ein Vergleich zu den Vorwellen ist daher nicht mehr möglich. 2023 gab rund jede/-r zehnte Befragte (11 %) an, dass sein bzw. ihr Unternehmen schon einmal erfolgreich von Cyberkriminellen angegriffen wurde, so dass ein erheblicher Aufwand nötig war, um die Schäden zu beheben. Erlaubt man sich eine Hochrechnung auf die Grundgesamtheit, ergibt das rund 16'830 (Sicherheitsbereich: 16'360 bis 17'300) betroffene Schweizer KMU. Unternehmen mit 10 bis 19 Mitarbeitern (17 %) heben sich dabei als einzige Subgruppe mit einem höheren Wert von den anderen ab; zwischen den Branchen gibt es keine Unterschiede. Das heisst, es gibt keine gefährdeten oder ungefährdeten Branchen; es kann also jeden gleichermassen treffen. Etwas mehr als die Hälfte der von Cyberangriffen Betroffenen (55 %) gab an, einen finanziellen Schaden erlitten zu haben; einen Reputationsschaden (13 %) oder einen Kundendatenverlust (13 %) beklagt rund jede/-r Achte. Somit darf angenommen werden, dass 6 Prozent der Schweizer KMU mit 4 bis 49 Mitarbeitenden schon einmal einen finanziellen Schaden durch einen Cyberangriff erlitten haben (Vertrauensintervall: +/- 2.1 Prozentpunkte).

Jede/-r zehnte Befragte (10 %) gibt an, schon einmal von Cyberkriminellen erpresst worden zu sein. Die Schwere des Falles wurde nicht definiert, d.h. es kann sich auch um leichte Fälle gehandelt haben. Auch hier gibt es keine Unterschiede zwischen den Subgruppen. Ein Prozent der gesamten Stichprobe sagt, dass sein/ihr Unternehmen schon einmal Lösegeld an Cyberkriminelle bezahlt hat. Somit bezahlte jede/-r zehnte Erpresste Lösegeld; zusätzlich muss wahrscheinlich noch von einer Dunkelziffer ausgegangen werden. – Für Hochrechnungen auf die Grundgesamtheit ist diese Zahl aber zu tief.

Über die Hälfte der Befragten (56 %) schätzt das Risiko, durch einen Cyberangriff für mindestens einen Tag lang ausser Kraft gesetzt zu werden, als eher oder sehr tief ein. Somit ist die Risikoeinschätzung wieder leicht gesunken, nachdem sie in den letzten drei Wellen stetig ganz leicht gestiegen ist. Ein Zusammenhang besteht zwischen der Einstellung zu technischen Innovationen (Pioniere schätzen das Risiko höher ein) und zum Informationsgrad ((eher) gut Informierte schätzen das Risiko höher ein). Zu bedenken ist dabei, dass Pioniere und (eher) gut Informierte nicht häufiger angegriffen wurden als Early bzw. Late Follower oder (eher) schlecht Informierte); das Risiko ist also für alle gleich.

Wie schon in den Vorwellen zeigt auch die 2023er Studie: Cyberkriminalität wird als ernstzunehmendes Problem eingeschätzt; die Gefahr wird grundsätzlich erkannt. Massnahmen dagegen

werden aber nur von einer Minderheit der Befragten geplant. Gründe gegen die Massnahmen können in deren Umsetzungsschwierigkeit liegen oder darin, dass die Befragten keinen sozialen Druck dazu spüren.

2 Ausgangslage und Ziele

2.1 Mandat und Fragestellung

Nach rund drei Jahren immer wiederkehrender Pandemiemassnahmen wie Masken- und Isolationspflicht oder Homeoffice-Pflicht bzw. -Empfehlung wurde die vierte Welle dieser Studie erstmals in einer von Covid zur Ruhe gekommenen Gesellschaft geführt. Allerdings hatte der Überfall Russlands auf die Ukraine und der darauffolgende Krieg die Schlagzeilen der Schweizer Medien im Griff, somit kann auch bei der 2023er Studie nicht von «Normalität» die Rede sein.

Vor diesem Hintergrund wurde die vierte 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 18. April bis 13. Juni 2023 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 bezüglich den Firmengrössen und Sprachregionen 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=502
4–9 Beschäftigte	66 %	326 (65 %)
10–19 Beschäftigte	22 %	110 (22 %)
20–49 Beschäftigte	12 %	66 (13 %)
	Effektiver Anteil (BFS / STATENT 2017)	Stichprobe nach vorgeschichteten Adressen:
Espace Mittelland	20 %	104 (21 %)
Genferseeregion	19 %	122 (24 %)
Nordwestschweiz	12 %	51 (10 %)
Ostschweiz	14 %	61 (12 %)
Tessin	6 %	47 (9 %)
Zentralschweiz	12 %	52 (10 %)
Zürich	16 %	65 (13 %)

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

Die Ausschöpfung liegt bei eher tiefen 3.2 %:

Realisiert Interviews	502
Verweigerung	15’238
Termine	420
Keine Antwort	10’117
Besetzt	412
Anrufbeantworter	4’786
Quote Komplet/Nicht Zielgruppe	945
Fax/Geschäft/Nicht existent	4739
nicht erreichbar während der Feldzeit	141
Sprachprobleme	76
Total	37’376

Berechnung Ausschöpfung:
37'376 - Summe aller nicht-erreichten Adressen (21'636) = 15’740
502 / 15’740 = 3.2 %

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 Massnahmenumsetzung, 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:

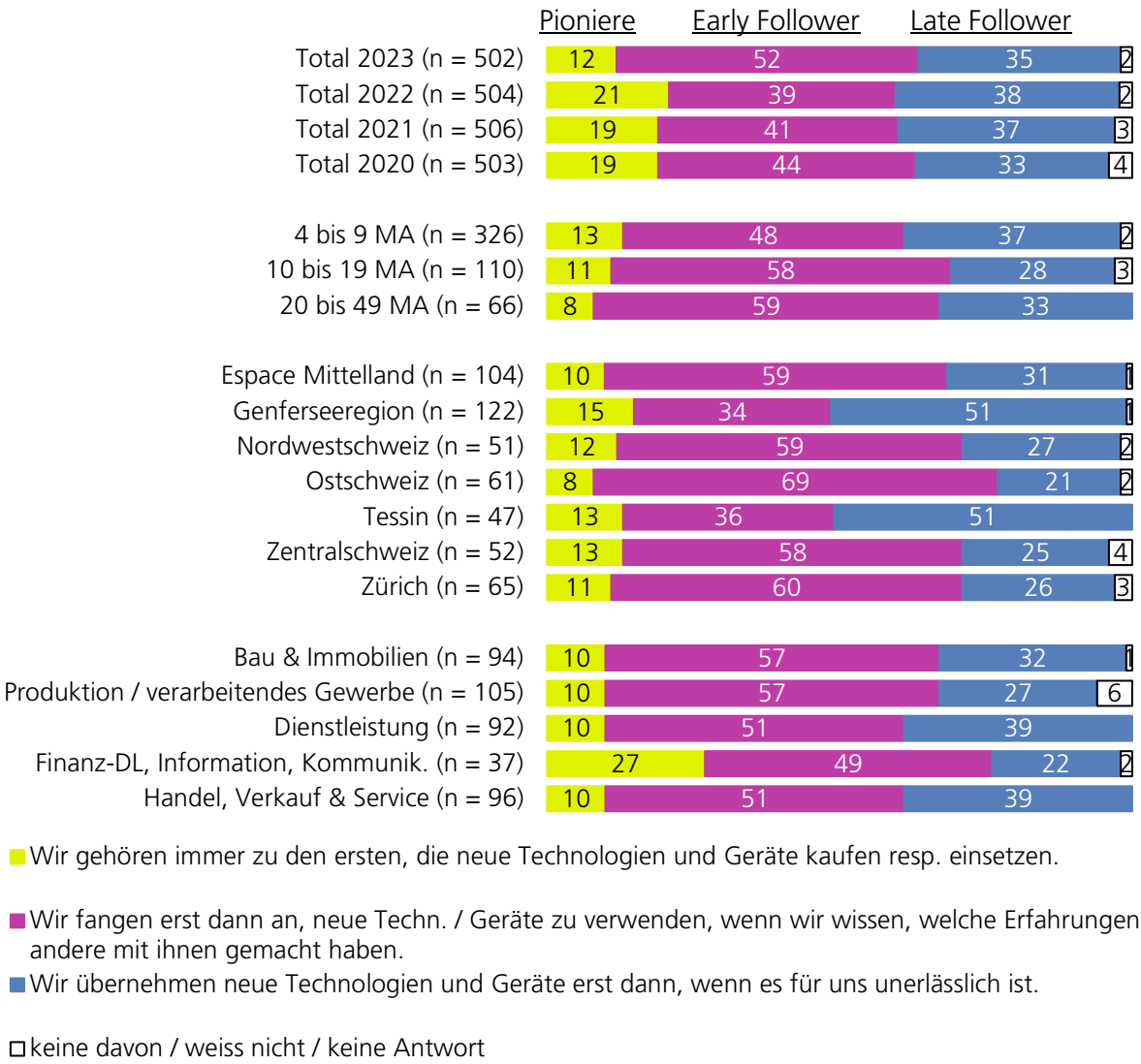
- Wir gehören immer zu den ersten, die neue Technologien und Geräte kaufen resp. einsetzen.
- Wir fangen erst dann an, neue Technologien / Geräte zu verwenden, wenn wir wissen, welche Erfahrungen andere mit ihnen gemacht haben.
- Wir übernehmen neue Technologien und Geräte erst dann, wenn es für uns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

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

Die Resultate von 2023 unterscheiden sich leicht von denjenigen von 2020 bis 2022, so sind dieses Jahr weniger Pioniere in der Stichprobe: Rund ein Zehntel (12 %) der Befragten zählt sich zur Gruppe der Pioniere, während es bisher rund ein Fünftel war (2022: 21 %, 2021: 19 %, 2020: 19 %). Dafür zählen sich 2023 mehr Befragte zu den Early Followern, nämlich rund die Hälfte (52 %) der Befragten (2022: 39 %, 2021: 41 %, 2020: 44 %). Bei den Late Followern ist es wie in den Vorwellen: Rund ein Drittel (35 %), zählt sich dazu (2022: 38 %, 2021: 37 %, 2020: 33 %). Über den Grund dieser Verschiebung kann nur vermutet werden: So könnte das plötzliche Aufkommen von Artificial Intelligence oder Plattformen wie ChatGPT dazu geführt haben, dass sich Personen und Unternehmen weniger als «Pioniere» fühlen als vorher. Auch die Umsetzung der Massnahmen für das neue Datenschutzgesetz, das ab September 2023 gilt, könnte die Befragten

etwas einschüchtern und das Gefühl verleihen, dass man noch nicht soweit ist, wie man eigentlich sollte.

Pioniere finden sich am ehesten in den Branchen Finanzdienstleistungen, Information & Kommunikation (27 %). Die anderen Branchen verfügen mit einem Zehntel (10 %) über weniger Pioniere. Die Genferseeregion und das Tessin weisen deutlich mehr Late Follower (je 51 %) auf als die anderen Regionen (Werte siehe Grafik).



Grafik 1

3.1.2 Massnahmenumsetzung

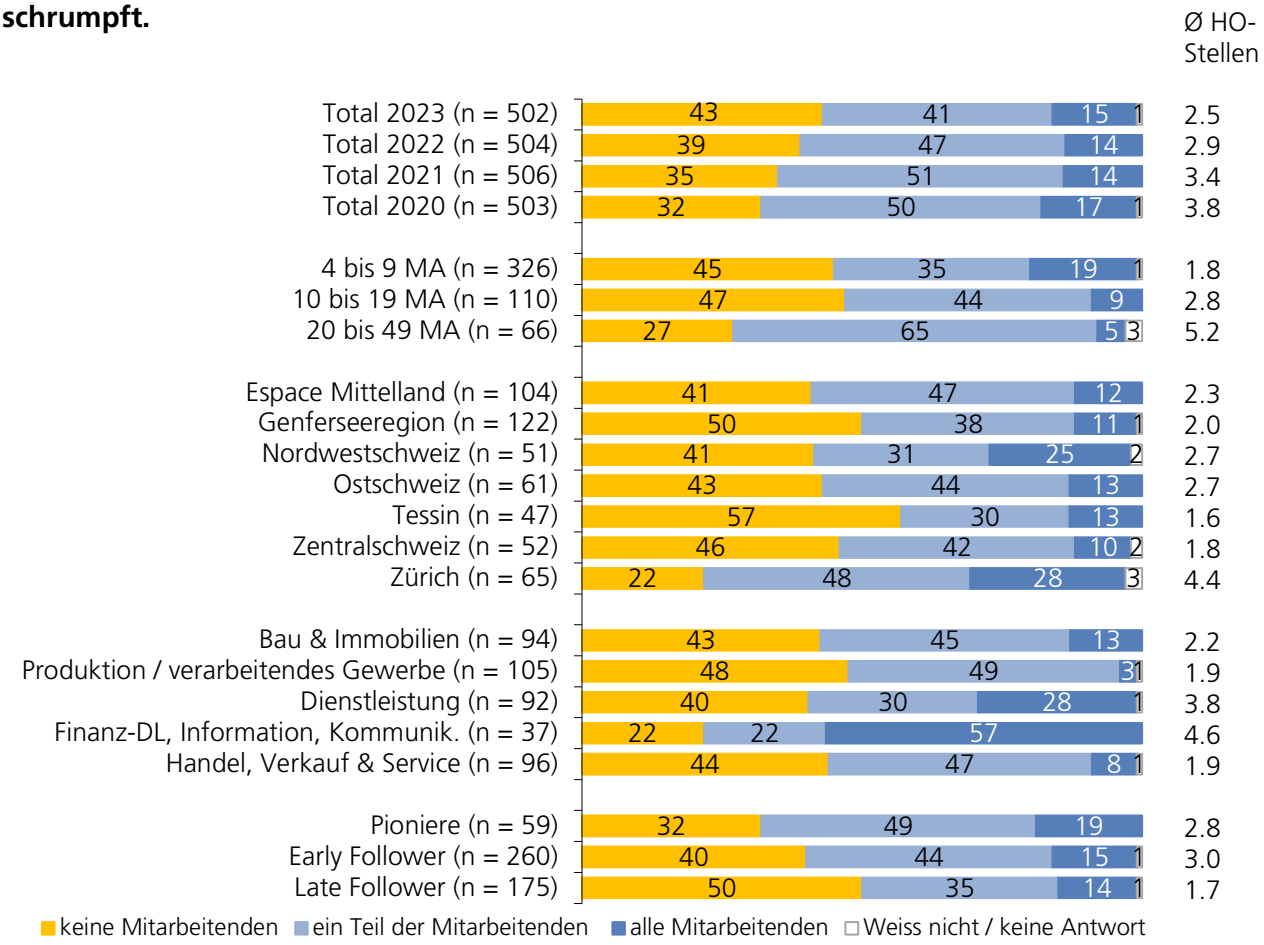
Im Fragenblock zur Cybersicherheit wurden verschiedene technische und organisatorische Sicherheitsmassnahmen nach deren Umsetzungsgrad auf einer Fünferskala abgefragt (siehe Kapitel 3.5.3 und 3.5.4). Für die Bildung der Subgruppe wurde der Durchschnitt aller technischen bzw. organisatorischen Massnahmen 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

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 = 502

Als diese Studie 2020 erstmals durchgeführt wurde, war gerade die erste Homeoffice-Pflichtphase vorüber. Damals sagte rund ein Drittel (32 %) der befragten KMU-Geschäftsführenden, dass *keine* ihrer Mitarbeitenden theoretisch im Homeoffice arbeiten könnten, die Hälfte (50 %) meinte, *ein Teil* ihrer Mitarbeitenden könne im Homeoffice arbeiten und rund ein Sechstel (17 %) sagte, *alle* ihre Mitarbeitenden können theoretisch im Homeoffice arbeiten. Die durchschnittliche Anzahl an Homeoffice-tauglichen Stellen lag bei 3.8. **Seit 2020 ist die Anzahl Homeoffice-tauglicher Stellen von Jahr zu Jahr stetig geschrumpft.**



Grafik 2

2023 bestehen gemäss den befragten KMU-Geschäftsführenden durchschnittlich nur noch 2.5 Stellen, bei denen theoretisch aus dem Homeoffice gearbeitet werden kann. Mehr als zwei Fünftel (43 %) der Befragten sagen, bei ihnen gäbe es *keine* einzige Homeoffice-taugliche Stelle, weitere rund zwei Fünftel (41 %) nennen *einen Teil* ihrer Arbeitsstellen als Homeoffice-tauglich. Rund ein Siebtel (15 %) der Befragten sagt, *alle* Mitarbeitenden können theoretisch aus dem Home-

office arbeiten. Der Rückgang ist signifikant. Die Studienautor:innen nehmen an, dass die Arbeitgebenden über die letzten Jahre stetig weniger überzeugt wurden vom Homeoffice und deshalb immer weniger ihrer Arbeitsstellen als «theoretisch Homeoffice-tauglich» bezeichnen. Das bedeutet aber nicht, dass die effektive Menge von Homeoffice-Tätigkeit in der Schweiz gesunken ist, denn in der Realität werden Arbeitgebende sich zumindest teilweise den Ansprüchen der Mitarbeitenden fügen müssen.

Die Branchen Dienstleistung (3.8) und Finanz-Dienstleistungen, Information & Kommunikation (4.6) sind signifikant Homeoffice-freundlicher als die beiden Branchen Produktion & verarbeitendes Gewerbe (1.9) und Handel, Verkauf & Service (1.9). Dies hat sich schon über die vergangenen Wellen so gezeigt. Auch dass der Grossraum Zürich signifikant aufgeschlossener ist gegenüber Homeoffice (4.4) als die Grossräume Espace Mittelland (2.3), Genferseeregion (2.0), Tessin (1.6) und Zentralschweiz (1.8), hat sich schon in vorherigen Wellen gezeigt.

3.2.2 Veränderung Homeoffice-Gewohnheiten während Homeoffice-Pflicht

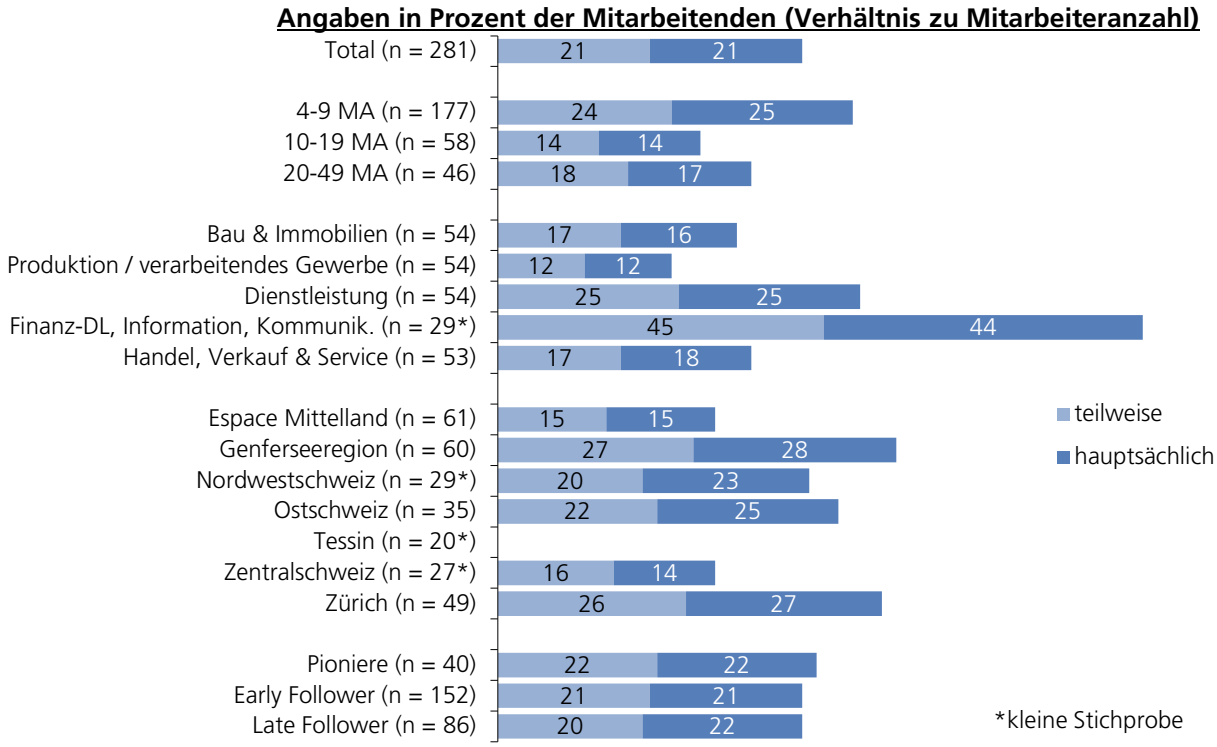
Frage 2:
Wie viele von Ihren Mitarbeitenden arbeiten teilweise und wie viele hauptsächlich von zuhause aus?
Filter: Mindestens ein/e Mitarbeiter/in kann theor. im Homeoffice arbeiten, n = 281

Diejenigen Arbeitgebenden, die mindestens eine ihrer Arbeitsstellen als Homeoffice-tauglich bezeichnet hatten, wurden gefragt, wie viele Ihrer Mitarbeitenden teilweise bzw. hauptsächlich von zuhause aus arbeiten: Es sind je rund ein Fünftel (je 21 %) der Mitarbeitenden. Wie schon in den Vorwellen gilt: Bei den kleinsten Unternehmen ist der Anteil an Mitarbeitenden im Homeoffice am grössten: Unternehmen mit 4 bis 9 Mitarbeitenden haben je rund einen Viertel (24 % bzw. 25 %) der Mitarbeitenden *teilweise* bzw. *hauptsächlich* im Homeoffice, insgesamt arbeitet also fast die Hälfte (49 %) der Mitarbeitenden in dieser Grössenkategorie zumindest teilweise im Homeoffice. In der nächstgrösseren Kategorie, 10 bis 19 Mitarbeitenden, arbeitet je rund ein Siebtel (14 %) *teilweise* oder *hauptsächlich* im Homeoffice. Bei Unternehmen mit 20 bis 49 Mitarbeitenden ist es je rund ein Sechstel (18 % bzw. 17 %) der Mitarbeitenden, die *teilweise* bzw. *hauptsächlich* im Homeoffice arbeiten.

Besonders hoch ist der Anteil an Mitarbeitenden im Homeoffice in den Branchen Finanzdienstleistungen, Information und Kommunikation: Insgesamt arbeiten fast 9 von 10 Mitarbeitenden (89 %) dieser Branchen zumindest teilweise von zuhause aus: Rund die Hälfte (45 %) *teilweise* und rund zwei Fünftel (44 %) *hauptsächlich*. Auch in der Branche Dienstleistungen liegt der Anteil hoch: Die Hälfte der Mitarbeitenden (50 %) arbeitet zumindest teilweise im Homeoffice, hälftig aufgeteilt auf *teilweise* oder *hauptsächlich* (je 25 %). Ebenfalls hoch ist der Anteil im Grossraum Zürich, wo je rund ein Viertel (26 % bzw. 27 %) *teilweise* bzw. *hauptsächlich* im Homeoffice arbeitet. Die Branchen der (Finanz-)Dienstleister, Information und Kommunikation sowie der Grossraum Zürich fielen schon in den Vorwellen als besonders Homeoffice-freundlich auf.

Tief hingegen ist der Anteil in der Branche Produktion und verarbeitendes Gewerbe, wo je rund jede/-r achte (12 %) Mitarbeitende *teilweise* bzw. *hauptsächlich* von zuhause aus arbeitet.

Zwischen Pionieren, Early Followern und Late Followern gibt es 2023 kaum Unterschiede, obwohl sich in den Vorwellen jeweils zeigte, dass Pioniere mehr Mitarbeitende im Homeoffice hatten als Early Follower und diese wiederum mehr als die Late Follower. Das könnte bedeuten, dass die technischen Anpassungen, die Remote Work benötigt, mittlerweile auch bei den Late Followern angekommen sind.



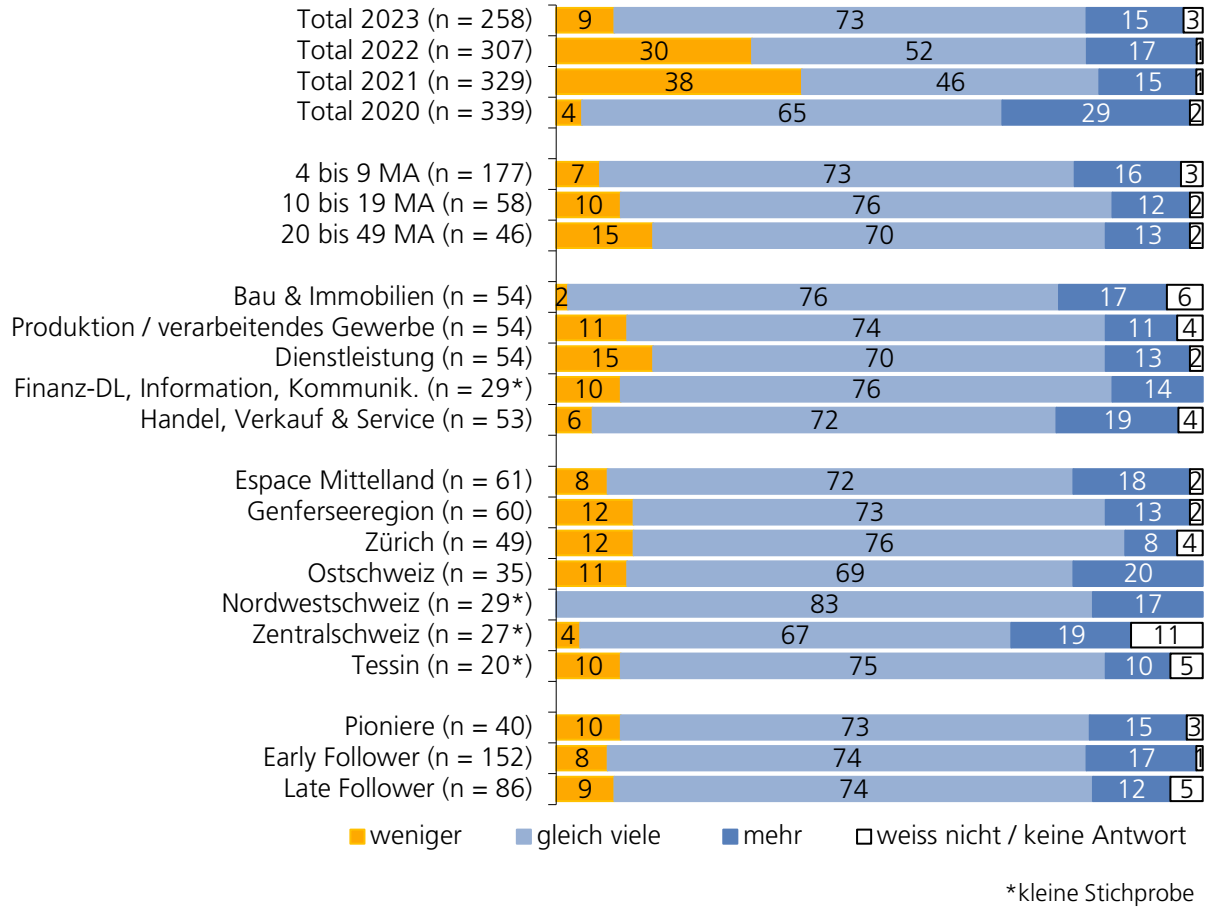
Grafik 3

Aufgrund der veränderten Fragestellung lässt sich nicht eindeutig sagen, ob der Anteil tatsächlich im Homeoffice arbeitender Mitarbeitenden gestiegen ist oder nicht: Bis und mit 2022 konzentrierte sich die Fragestellung darauf, wie viele Mitarbeitende vor, während und nach der jeweiligen Pandemiemassnahmen *hauptsächlich* im Homeoffice arbeiteten. 2023 wurden die Antwortmöglichkeiten unterteilt in *teilweise* und *hauptsächlich*, was eine andere Einschätzung und somit ein anderes Antwortverhalten der Befragten zur Folge haben kann. Erlaubt man sich den Vergleich trotzdem, zeigt sich: Nach dem Lockdown 2020 arbeiteten noch 16 Prozent der Mitarbeitenden der befragten Geschäftsführenden *hauptsächlich* im Homeoffice, nach der Homeoffice-Pflicht 2021 noch 20 Prozent, aber nach der Homeoffice-Pflicht 2022 nur noch 12 Prozent. 2023 sind es 21 Prozent der Mitarbeitenden, die hauptsächlich im Homeoffice arbeiten, und somit fast doppelt so viele wie nach dem «Taucher» 2022 bzw. fast gleich viele wie 2021. Die Autorenschaft vermutet, dass sich über diese drei Jahre eine andere Interpretation des Begriffst *hauptsächlich* eingestellt hat. Eine weitere mögliche Interpretation ist, dass 2022, nach zwei Jahren Pandemie und wiederkehrenden sozialen Abschottungen, viele Geschäftsführende ihre Mitarbeitenden wieder am Arbeitsplatz haben wollten. Bis ins Jahr 2023, also der aktuellen Befragungswelle, wird sich das Spannungsfeld zwischen Angebot (Geschäftsführende möchten Mitarbeitende vor Ort haben) und Nachfrage (Mitarbeitende möchten im Homeoffice arbeiten) etwas eingependelt haben. Dazu ist zu anzufügen, dass ein Fachkräftemangel herrscht und Mitarbeitende somit Ihre Wünsche eher durchsetzen können.

3.2.3 Einschätzung der Entwicklung der Homeoffice-Arbeitsplätze

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?
Filter: Wenn mindestens ein/-e Mitarbeitende theoretisch im Homeoffice arbeiten kann, n = 281

Die Einschätzung, wie sich der Anteil an Mitarbeitenden im Homeoffice langfristig verändern wird, hat sich seit 2020 stetig verändert. Kurz nach der ersten Homeoffice-Pflichtphase, welche mit dem generellen Lockdown einherging, erwartete fast ein Drittel (29 %) der befragten Geschäftsführenden eine langfristige Steigerung des Homeoffice-Anteils. Nach der zweiten Homeoffice-Pflichtphase 2021 änderte sich dies; mehr als ein Drittel (38 %) der Befragten gingen nun davon aus, dass es langfristig weniger Mitarbeitende im Homeoffice geben würde und nur noch rund jede/r siebte Befragte (15 %) erwartete eine Steigerung. Auch 2022 erwartete noch knapp ein Drittel (30 %) eine Reduktion des Homeoffice-Anteils und knapp ein Sechstel (17 %) eine Steigerung. 2023 jedoch, nach dem Ende sämtlicher Pandemiemassnahmen, erwarten fast drei Viertel der Befragten (73 %), dass der Homeoffice-Anteil langfristig gleichbleiben wird. Nur noch rund jede/-r Zehnte (9 %) erwartet eine Reduktion und weiterhin rund jede/-r Siebte eine Steigerung. Es scheint somit, als habe sich die Situation etwas eingependelt, und dies in sämtlichen Subgruppen in ähnlichem Mass.



*kleine Stichprobe

Grafik 4

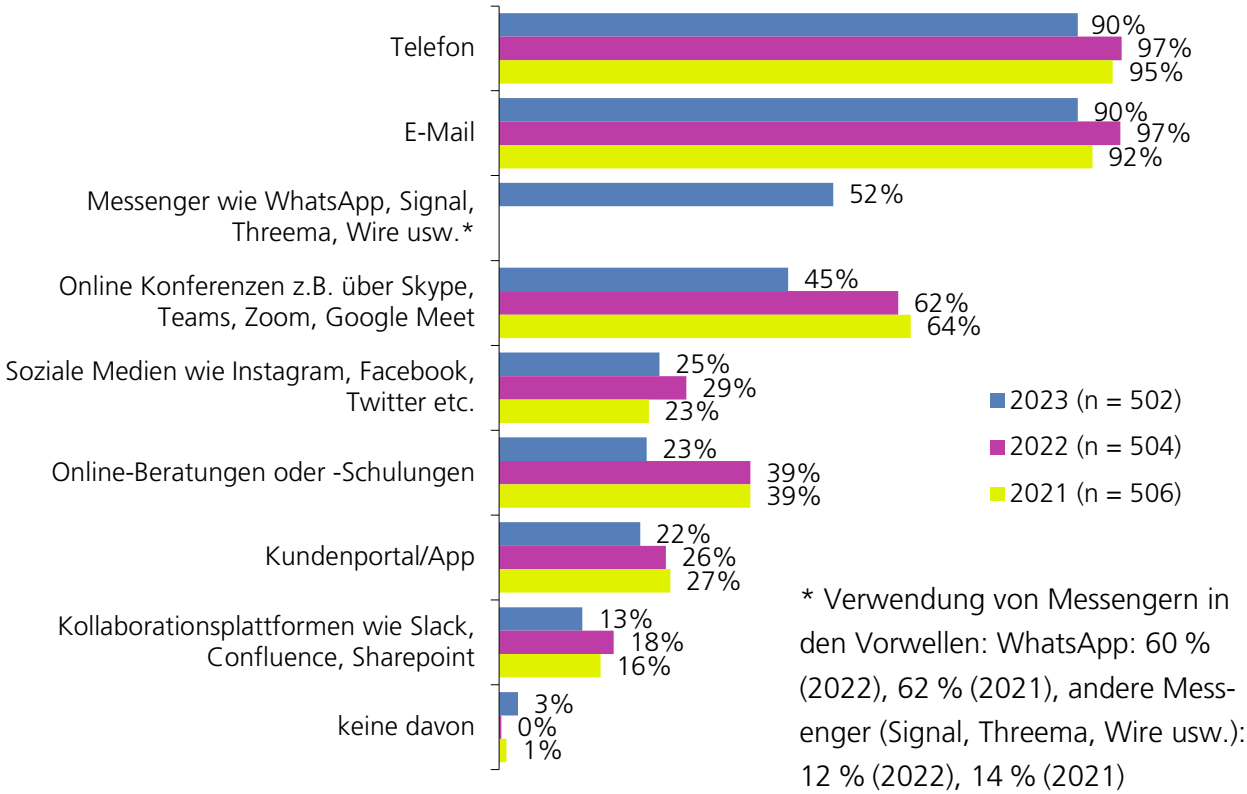
3.3 Kommunikation

3.3.1 Nutzung digitaler Kommunikationsmittel

Telefon und E-Mail (je 90 %) sind, wie schon in den Vorwellen, auch 2023 die am häufigsten verwendeten Kommunikationsmittel der befragten Unternehmen. Gegenüber den Vorwellen gibt es nur marginale Veränderungen.

Frage 4:
Ich lese Ihnen jetzt einige digitale Kommunikationsmittel vor. Welche davon nutzen Ihre Mitarbeitenden aktuell für Partner, Kundschaft und anderen Mitarbeitende?
Basis: Total, n = 502, Mehrfachnennungen möglich

Die Verwendung sämtlicher Kommunikationstools wurde 2023 tiefer eingeschätzt als noch 2022. Auffallend ist dies beispielsweise bei den Messengern wie WhatsApp, Signal, Threema, Wire usw. (in den Vorwellen noch separat abgefragt): WhatsApp erreichte in den Vorwellen alleine noch fast zwei Drittel (60 % in 2022 und 62 % in 2021). Jetzt, zusammen mit Signal, Threema, Wire usw., wird es von rund der Hälfte (52 %) der Befragten genannt.
Auch Online Konferenztools werden gemäss den befragten Geschäftsführenden seltener (45 %) verwendet als 2022 (62 %) und 2021 (64 %), ebenfalls stark zurückgegangen ist die Anwendungen von Online-Beratungen oder -Schulungen (2023: 23 %, 2022: 39 %, 2021: 39 %).



* Verwendung von Messengern in den Vorwellen: WhatsApp: 60 % (2022), 62 % (2021), andere Messenger (Signal, Threema, Wire usw.): 12 % (2022), 14 % (2021)

Grafik 5

Im Durchschnitt werden 3.6 verschiedene Kommunikationsmittel angegeben. Je mehr Mitarbeitende theoretisch im Homeoffice arbeiten können, desto mehr Kommunikationsmittel werden

verwendet. So verwenden Unternehmen *ohne* homeoffice-taugliche Arbeitsstellen durchschnittlich 3.3 verschiedene Kommunikationsmittel, Unternehmen *mit einem Teil* homeoffice-tauglichen Arbeitsplätzen 3.7 und Unternehmen mit *ausschliesslich* homeoffice-tauglichen Stellen 4.4.

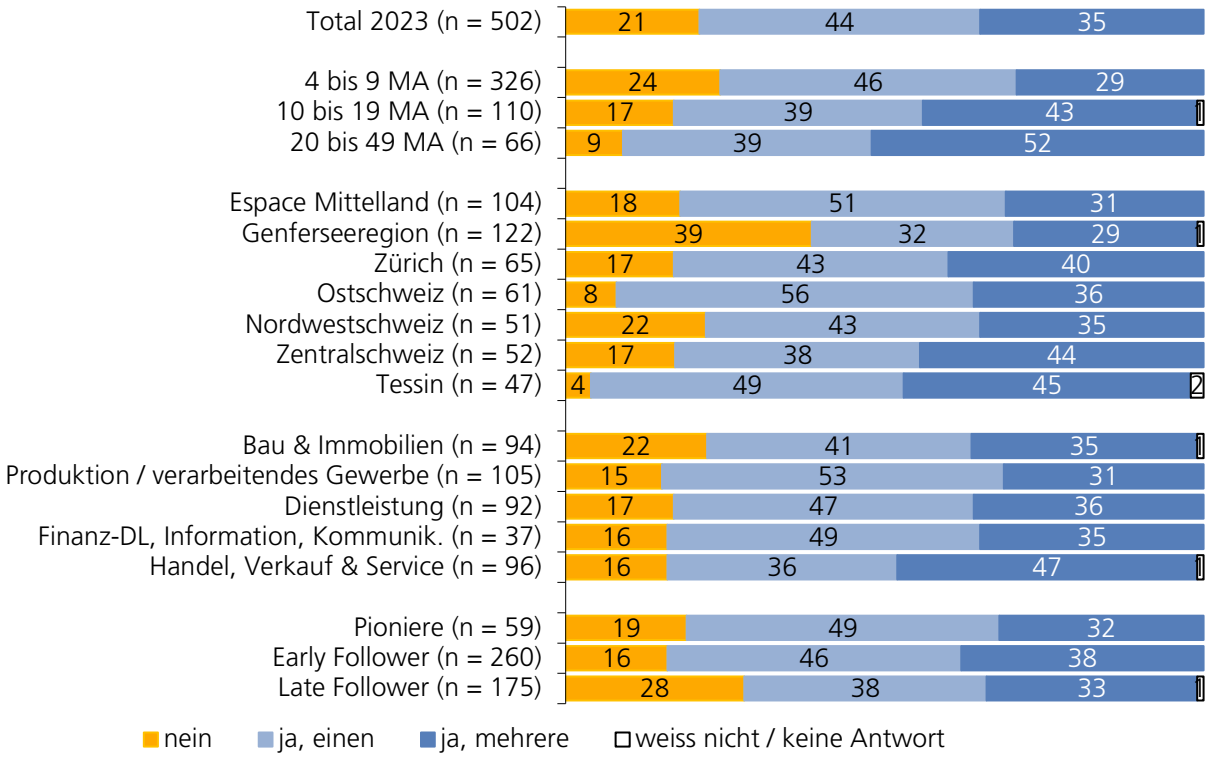
Besonders viele verschieden Kommunikationsmittel werden in den Branchen Finanz-Dienstleistungen, Information & Kommunikation verwendet (4.7). Diese Branchen verwendet Online Konferenztools wie Skype, Teams, Zoom oder Google Meet signifikant häufiger (78 %) als die Branchen Bau & Immobilien (38 %), Produktion und verarbeitendes Gewerbe (43 %) sowie Handel, Verkauf und Service (47 %). Auch die Kollaborationsplattformen werden hauptsächlich in den Branchen Finanz-Dienstleistungen, Information & Kommunikation verwendet (35 %). Dieser Wert liegt ebenfalls signifikant höher als derjenige der drei Branchen Bau & Immobilien (9 %), Produktion und verarbeitendes Gewerbe (9 %) sowie Handel, Verkauf und Service (13 %).

3.4 IT-Dienstleister

3.4.1 Anzahl IT-Dienstleister

Die meisten Geschäftsführenden haben einen einzelnen IT-Dienstleister (44 %), rund ein Drittel hat mehrere IT-Dienstleister (35 %) und immerhin rund jeder fünfte Geschäftsführende hat gar keinen IT-Dienstleister (21 %).

Frage 5:
Haben Sie einen oder mehrere IT-Dienstleister, d.h. externe Partner für Informatik, Telefonie, Software- oder Hardware-Arbeiten?
Basis: Total, n = 502



Grafik 6

Je grösser das Unternehmen, desto eher und desto mehr IT-Dienstleister hat das Unternehmen: Unternehmen mit 10 bis 49 Mitarbeitenden (10–19 Mitarbeitende: 43 %; 20–49 Mitarbeitende: 52 %) haben signifikant häufiger *mehrere* IT-Dienstleister als Unternehmen mit 4 bis 9 Mitarbeitenden (29 %). Kleinere Unternehmen haben hingegen signifikant häufiger *keinen* IT-Dienstleister (4–9 Mitarbeitenden: 24 %; 10–19 Mitarbeitenden: 17 %; 20–49 Mitarbeitenden: 9 %).
Des Weiteren scheint es in der Genferseeregion weniger verbreitet zu sein, einen IT-Dienstleister zu haben: Knapp zwei Fünftel der Geschäftsführenden in der Genferseeregion (39 %) haben keinen IT-Dienstleister. Diese Zahl ist signifikant höher als im Espace Mittelland (18 %), in der Ost-Schweiz (8 %), im Tessin (4 %) und in Zürich (17 %). Zwischen den Branchen bestehen keine signifikanten Unterschiede: In der Bau- & Immobilien-Branche ist der Anteil derjenigen Unternehmen, die *keinen* IT-Dienstleister haben mit 22 % aber am höchsten (übrige Branchenwerte: siehe Grafik).
Auch bei der Einstellung zu neuen Technologien bestehen kaum signifikante Unterschiede: Hier ist der Anteil derjenigen Unternehmen, die *keinen* IT-Dienstleister haben, bei den Late Followern (28 %) signifikant höher als bei den Early Followern (16 %) und den Pionieren (19 %).

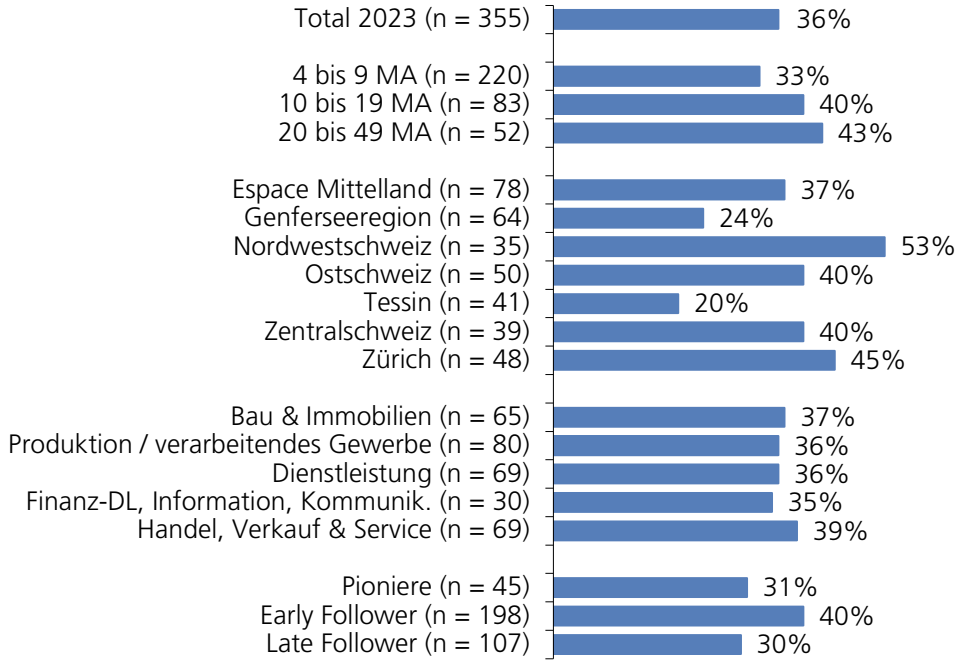
3.4.2 Outsourcen von IT-Arbeiten

Geschäftsführende, die mindestens einen externen IT-Dienstleister haben, vergeben rund einen Drittel (36 %) der IT-Arbeiten auswärts. Dieser Wert liegt leicht höher als in den Vorjahren (2022: 29 %, 2021: 30 %), was sich aber durch die unterschiedliche Fragestellung erklären lässt: In den Vorjahren wurde alle Interviewten befragt, 2023 nur diejenigen, die mindestens einen externen Dienstleister haben.

Frage 6:
Wieviel Prozent der IT-Arbeiten werden bei Ihnen ungefähr von externen Dienstleistern wahrgenommen?
Basis: Wenn mind. 1 externer IT-Dienstleister, n = 396

Je grösser die Unternehmen sind, desto eher vergeben sie IT-Arbeiten auswärts. Bei den kleinsten Unternehmen (4–9 Mitarbeitende) ist es 2023 ein Drittel (33 %) und bei der mittleren Kategorie (10–19 Mitarbeitende) sowie der grössten Kategorie (20–49 Mitarbeitende) rund zwei Fünftel (40 % bzw. 43 %). Diese Unterschiede sind jedoch nicht signifikant!
Wie in den Vorjahren ist die Outsourcing-Rate in der Nordwest-Schweiz am höchsten (53 %), am tiefsten ist sie im Tessin (20 %).

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 rund einen Viertel (27 %) ihrer IT-Arbeiten auswärts gegeben, Unternehmen mit hoher Massnahmenumsetzung knapp zwei Fünftel (38 %). Ein ähnliches Bild zeigt sich bei den organisatorischen Massnahmen: Unternehmen mit tiefer organisatorischer Massnahmenumsetzung haben weniger als einen Drittel (29 %) der IT-Arbeiten einem externen Dienstleister gegeben, Unternehmen mit hoher organisatorischer Massnahmenumsetzung mehr als zwei einen Drittel (36 %). Diese Verhältnisse waren in der Vorwellen 2021 und 2022 sehr ähnlich, sind aber nicht signifikant.

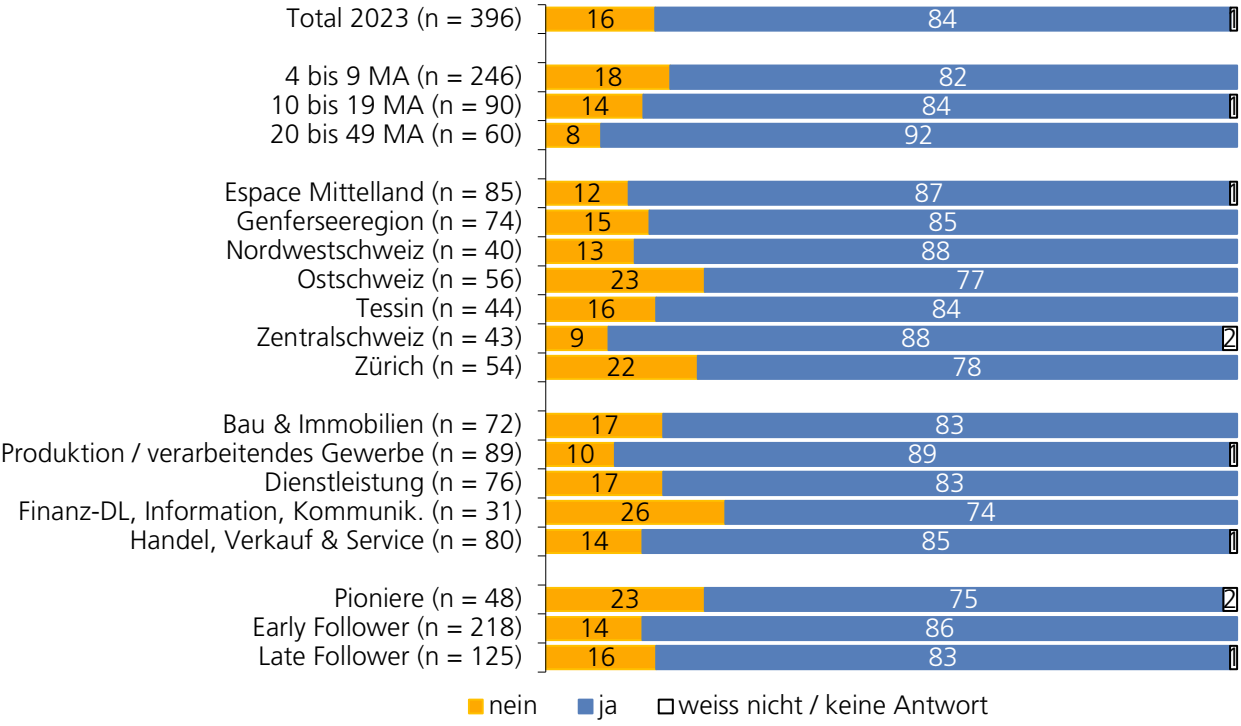


Grafik 7

3.4.3 IT-Dienstleister für Cybersicherheit

Bei der Mehrheit (84 %) der Unternehmen, die mindestens einen externen IT-Dienstleister haben, berät und unterstützt dieser externe IT-Dienstleister die Unternehmen auch bezüglich Cybersicherheit.

Frage 7:
Berät und unterstützt Sie Ihr externer IT-Dienstleister auch bezüglich Cybersicherheit?
Basis: Wenn mind. 1 externer IT-Dienstleister, n = 396



Grafik 8

Je grösser das Unternehmen, desto eher berät und unterstützt der externe IT-Dienstleister auch bezüglich Cybersicherheit, allerdings liegt der Anteil bei den kleinsten Unternehmen (4–9 Mitarbeitende) mit rund vier Fünfteln (82 %) bereits sehr hoch.

Sowohl zwischen den Regionen als auch zwischen den Branchen bestehen keine bedeutenden/signifikanten Unterschiede. In der Nordwestschweiz und der Zentralschweiz ist der Anteil der Unternehmen, bei denen der externe IT-Dienstleister auch bezüglich Cybersicherheit berät und unterstützt, am höchsten (je 88 %). In der Ostschweiz ist dieser Anteil am geringsten (77 %). Bei den Branchen ist er in der Produktion / verarbeitendes Gewerbe (89 %) am höchsten, in der Finanz-Dienstleistung, Information und Kommunikations-Branche hingegen am tiefsten (74 %). Da letztere ansonsten eher durch ihre hohe Digitalisierung und Massnahmenumsetzung auffallen, ist anzunehmen, dass zumindest ein Teil von ihnen zusätzlich zum IT-Dienstleister auch einen Cybersicherheits-Dienstleister hat oder über einen höheren Anteil interner Lösungen verfügt.

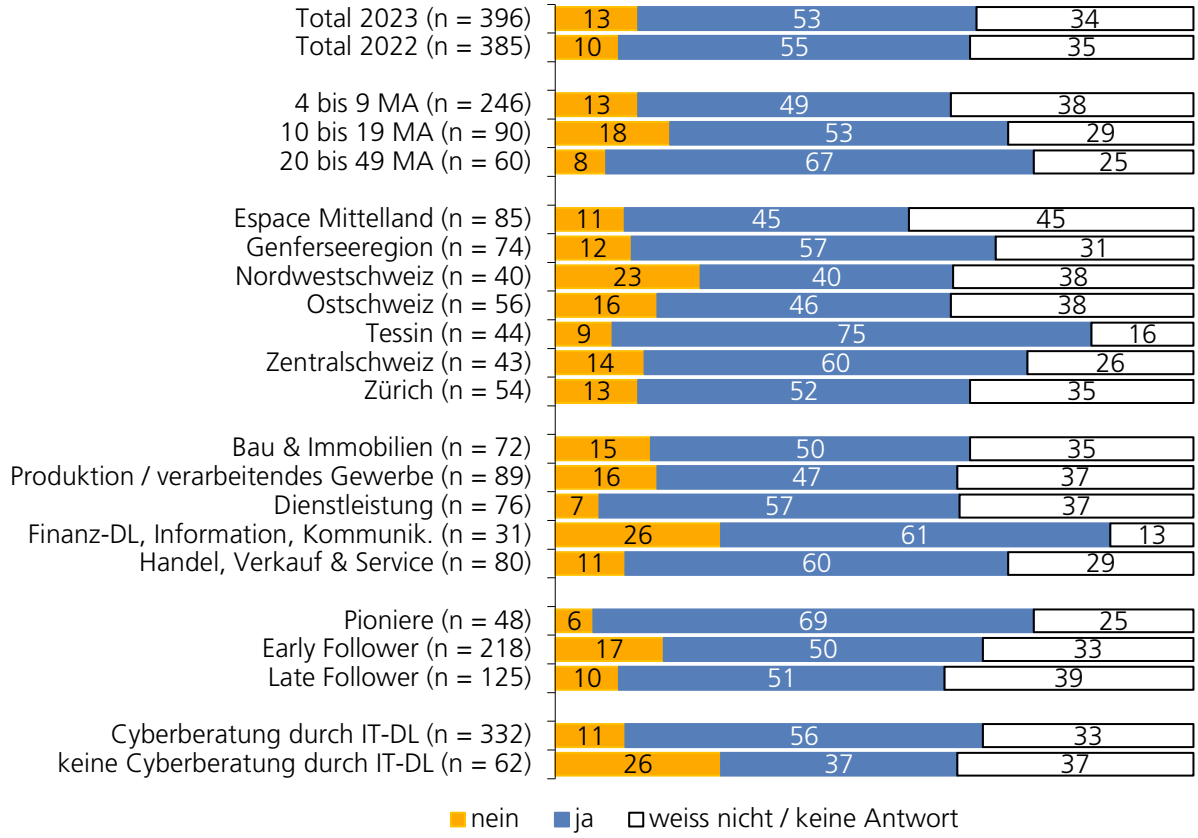
Signifikante Unterschiede bestehen bezüglich des Informationsgrades zur Cyberrisk-Thematik: Geschäftsführende, die sich (eher) uninformiert fühlen, geben mit knapp einem Drittel (32 %) signifikant häufiger an, dass der externe IT-Dienstleister sie NICHT bezüglich Cybersicherheit berät und unterstützt als dies bei Geschäftsführenden der Fall ist, welche sich (eher) informiert fühlen (16 %). Die Beratung durch den externen IT-Dienstleister könnte also zum (eher) hohen Informationsgrad zur Cyberrisk-Thematik beitragen, oder die Befragten mit hohem Informationsgrad fühlen eher die Notwendigkeit eines externen Beraters.
Auch bezüglich der technischen sowie organisatorischen Massnahmenumsetzung zeigen sich signifikante Unterschiede: je mehr technische oder organisatorische Massnahmen umgesetzt sind, desto eher berät und unterstützt der externe IT-Dienstleister die Unternehmen auch bezüglich Cybersicherheit.

3.4.4 IT-Sicherheitszertifizierung des externen Dienstleisters

Frage 8:
Verfügt ihr externer IT-Dienstleister über eine IT-Sicherheitszertifizierung (z.B. ISO 27001 oder CyberSeal der Allianz Digitale Sicherheit Schweiz)?
Basis: Wenn mind. 1 externer IT-Dienstleister, n = 396

Auch 2023 verfügt über die Hälfte (53 %) der eingesetzten IT- Dienstleister über eine IT-Sicherheitszertifizierung wie z.B. ISO 27001. Damit hat sich dieser Anteil gegenüber 2022 kaum verändert (55 %).
Je nach Grossregion variiert dieser Anteil teilweise deutlich: Mit drei Vierteln (75 %) ist der Anteil an Unternehmen mit zertifizierten externen IT-Dienstleistern im Tessin signifikant höher als im Espace Mittelland (45 %) und der Nordwestschweiz (40 %). Auch nach Firmengrösse bestehen signifikante Unterschiede: Bei grossen Unternehmen (20–49 Mitarbeitende) ist der externe IT-Dienstleister signifikant häufiger zertifiziert (67 %) als bei kleinen Unternehmen (4–9 Mitarbeitende: 49 %). Bezüglich den Branchen bestehen keine signifikanten Unterschiede. Hingegen haben besser über Cyberrisiken informierte Befragte signifikant häufiger zertifizierte IT-Dienstleister (62 %) als schlechter informierte (29 %). Zudem ist der Umsetzungsgrad der technischen und organisatorischen Massnahmen höher bei Unternehmen, die einen zertifizierten IT-Dienstleister engagieren –

vielleicht ist die IT-Sicherheitszertifizierung des externen Dienstleisters ebenfalls als Sicherheitsmassnahmenumsetzung zu betrachten.



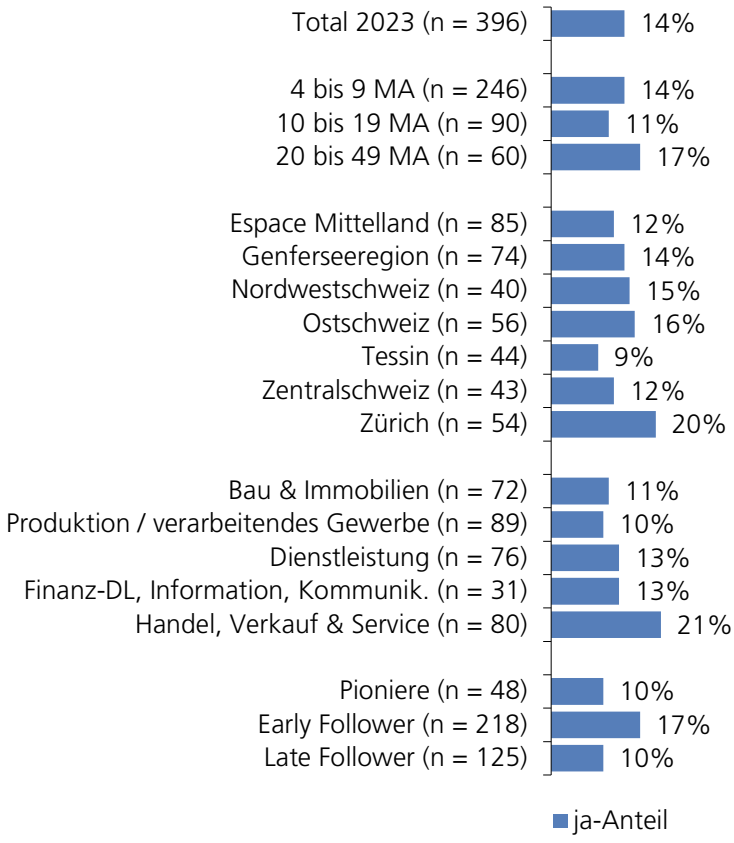
Grafik 9

Auffallend ist bei dieser Frage der hohe Anteil an Befragten, welche sie nicht beantworten wollten oder konnten: Er liegt, je nach Subgruppe, zwischen 16 und 45 Prozent (siehe Grafik). Ebenfalls auffallend ist der hohe Anteil an Befragten aus den Branchen Finanz-Dienstleistungen, Information & Kommunikation, die keinen zertifizierten IT-Dienstleister haben (26 %): Dies passt nicht zu den sonst hohen Werten bezüglich Massnahmenumsetzung bzw. Wichtigkeit des Themas. Es drängt sich erneut (wie zuvor bei Frage 7) der Verdacht auf, dass in diesen Branchen zumindest teilweise neben dem IT-Dienstleister auch ein Cybersicherheits-Dienstleister existiert, weshalb der IT-Dienstleister kein entsprechendes Zertifikat benötigt.

3.4.5 Ersatz des IT-Dienstleisters in den letzten 1 bis 2 Jahren

Rund jeder siebte Geschäftsführende (14 %) hat in den letzten 1 bis 2 Jahren einen bestehenden IT-Dienstleister durch einen neuen ersetzt.
Nach Grossregion, Branche und Firmengrösse bestehen keine signifikanten Unterschiede. Am häufigsten haben Firmen in Zürich (20 %), Firmen, die im Handel/Verkauf & Service (21 %) tätig sind und grosse Firmen (20–49 Mitarbeitende. 17 %) einen bestehenden IT-Dienstleister durch einen neuen ersetzt.
Ein signifikanter Unterschied besteht allerdings zwischen Firmen, welche schon einmal erfolgreich von Cyberkriminellen angegriffen wurden und Firmen, die noch nie einen erfolgreichen Cyberangriff erlitten haben. So haben Firmen, welche einen erfolgreichen Cyberangriff erlitten haben, in den letzten 1 bis 2 Jahren doppelt so häufig und damit signifikant häufiger einen bestehenden IT-Dienstleister durch einen neuen ersetzt (26 %) als Firmen, die keinen solchen Cyberangriff erlitten haben (13 %). Aus den Umfragedaten geht jedoch nicht hervor, ob diese IT-Dienstleister wegen dieses Cyberangriffs ersetzt wurden oder nicht (Gründe fürs Ersetzen des IT-Dienstleisters sind nachfolgend aufgeführt).

Frage 9:
Haben Sie in den letzten 1 bis 2 Jahren einen bestehenden IT-Dienstleister durch einen neuen ersetzt?
Basis: Wenn mind. 1 externer IT-Dienstleister, n = 396
Frage 10:
Aus welchen Gründen haben Sie in den letzten 1 bis 2 Jahren einen bestehenden IT-Dienstleister durch einen neuen ersetzt?
Frage 11:
Wie schwierig war es für Sie, einen geeigneten IT-Dienstleister zu finden?
Basis: Basis: Wenn bestehender IT-Dienstleister ersetzt, n = 55



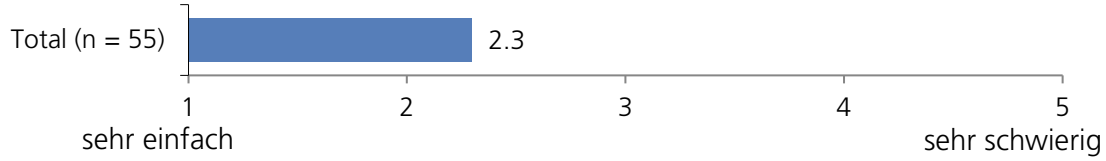
Grafik 10

Unternehmen, die in den letzten 1 bis 2 Jahren einen bestehenden IT-Dienstleister durch einen neuen ersetzt haben, haben dies vor allem aus internen Optimierungs- und Kompatibilitätsgründen (z.B. neue Software oder Server gekauft, n = 18) sowie aufgrund der Kommunikation und Service-Qualität (n = 17) getan. Darauf folgen personelle oder Kapazitätsgründe sowie Kostengründe (n = 8).

Gründe (kategorisiert)	Anzahl Nennungen (n = 55)
Interne Optimierung und Kompatibilität	18
Kommunikation und Service-Qualität	17
Personelle oder Kapazitätsgründe	8
Kostengründe	8
Pensionierung oder Geschäftsaufgabe	7
Externe oder vertragliche Gründe	3
Sonstiges	3
Weiss nicht/keine Antwort	2

Tabelle 1

Für die meisten Unternehmen scheint dieser Wechsel (sehr) einfach gewesen zu sein: Gut zwei Drittel geben an, es sei (sehr) einfach (64 %) gewesen, einen geeigneten IT-Dienstleister zu finden, ein Fünftel empfand es als (sehr) schwierig (18 %) und ein weiterer Fünftel als weder schwierig noch einfach (18 %). Der Mittelwert liegt damit bei 2.3 auf einer Skala von 1=sehr einfach bis 5=sehr schwierig.
Aufgrund der tiefen Fallzahl können hier keine statistisch verlässlichen Subgruppen-Unterschiede untersucht werden.

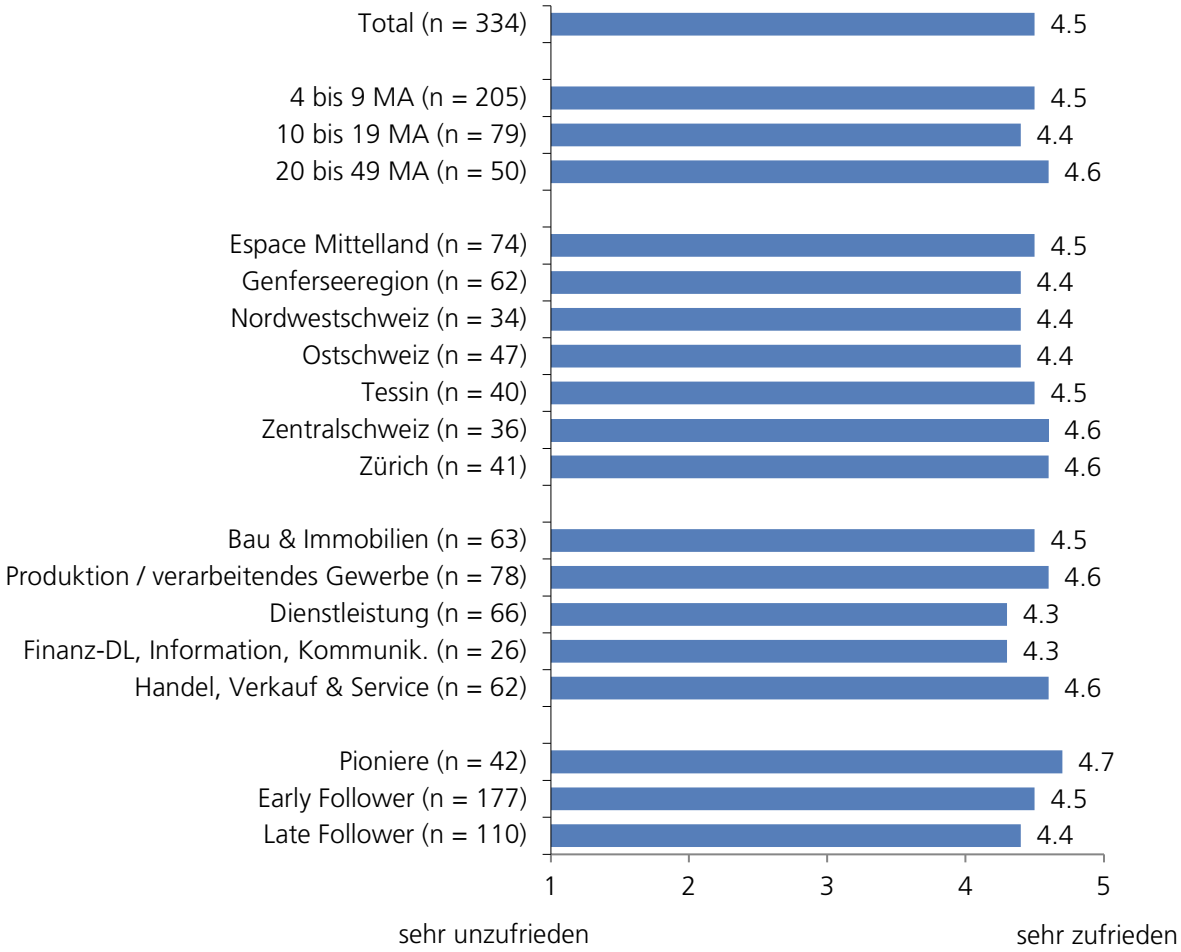


Grafik 11

3.4.6 Zufriedenheit mit IT-Dienstleister

Frage 12:
Wie zufrieden sind Sie mit Ihrem IT-Dienstleister?
Basis: Wenn IT-DL nicht ersetzt, n = 334
Frage 13:
Aus welchen Gründen sind Sie (eher) zufrieden?
Basis: Wenn mit IT-DL (eher) zufrieden, n = 305
Frage 14:
Aus welchen Gründen sind Sie (eher) unzufrieden?
Basis: Wenn mit IT-DL (eher) unzufrieden, n = 8

Bei Unternehmen, welchen ihren IT-Dienstleister nicht ersetzt haben, ist die Zufriedenheit mit dem IT-Dienstleister sehr hoch: 9 von 10 Unternehmen (91 %) geben an, damit (sehr) zufrieden zu sein. Der Mittelwert liegt somit bei 4.5 auf einer Skala von 1 = sehr unzufrieden bis 5 = sehr zufrieden. Nach Grossregion, Branche und Firmengrösse bestehen keine signifikanten Unterschiede. Je höher der Informationsgrad über Cyberrisk, desto höher ist die Zufriedenheit mit dem IT-Dienstleister: Geschäftsführende, die sich (eher) informiert fühlen (4.5) sind signifikant zufriedener als Geschäftsführende, die sich (eher) uninformiert fühlen (4.1). Zudem sind Unternehmen mit einem hohen Umsetzungsgrad an technischen und organisatorischen Massnahmen signifikant häufiger zufrieden mit ihrem IT-Dienstleister als Unternehmen mit einem tieferen Umsetzungsgrad.



Grafik 12

Der häufigste Grund, weshalb Unternehmen mit ihrem IT-Dienstleister zufrieden sind, ist die Erreichbarkeit und Reaktionszeit (n = 127). An zweiter Stelle folgt die Begründung, dass die Unternehmen allgemein eine gute Meinung des IT-Dienstleisters hätten (n = 85). Die Kompetenz und das Fachwissen werden erst als Drittes (n = 67) genannt. Es bestehen keine signifikanten Unterschiede nach Grossregion, Branche oder Firmengrösse.

Gründe (kategorisiert)	Anzahl Nennungen
Erreichbarkeit und Reaktionszeit	127
Allgemein gute Meinung	85
Kompetenz und Fachwissen	67
Kundenservice und Kommunikation	48
Funktionalität und Zuverlässigkeit	41
Sicherheit	20
Preis-/Leistungsverhältnis	18
Flexibilität und Anpassungsfähigkeit	15
Vertrauen und langfristige Beziehung	10

Tabelle 2

Zu einer Unzufriedenheit mit dem IT-Dienstleister kommt es hingegen am häufigsten wegen einer allgemein schlechten Meinung, einem schlechten Preis-/Leistungsverhältnis und einem Mangel an Kompetenz und Fachwissen (je n = 2). Aufgrund der tiefen Fallzahl können hier keine statistisch verlässlichen Subgruppen-Unterschiede untersucht werden.

Gründe (kategorisiert)	Anzahl Nennungen
Allgemein schlechte Meinung	2
Preis-/Leistungsverhältnis	2
Kompetenz und Fachwissen	2
Sicherheit	1
Flexibilität und Anpassungsfähigkeit	1
Kundenservice und Kommunikation	1
Erreichbarkeit, Reaktionszeit	1

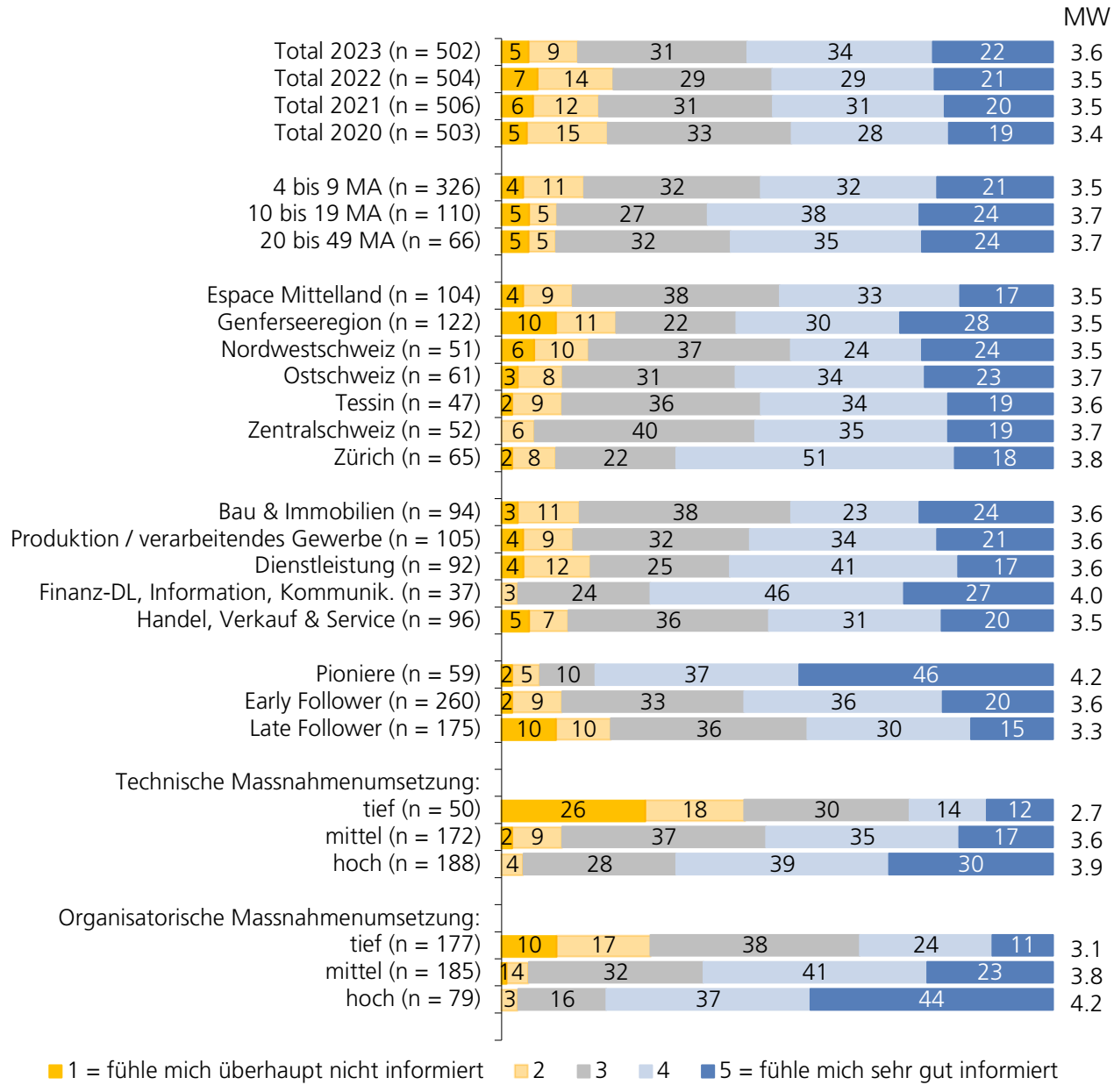
Tabelle 3

3.5 Cybersicherheit

3.5.1 Gefühlter Informationsgrad zur Cyberrisk-Thematik

Etwas mehr als die Hälfte (56 %) der befragten Geschäftsführenden fühlt sich eher oder sehr gut informiert (Skalenwerte 4–5) bezüglich der Cyberrisk-Thematik. Dieser Wert hat sich gegenüber den Vorwellen minimal, aber stetig verbessert (2020: 47 %). Der Mittelwert liegt 2023 bei 3.6.

Frage 15:
Ganz allgemein: wie gut fühlen Sie sich persönlich in der Cyberrisk-Thematik informiert?
Basis: Total, n = 502



Grafik 13

Zwischen den drei Unternehmensgrössen gibt es keine signifikanten Unterschiede. Die kleinsten befragten Unternehmen (4–9 Mitarbeitende) erreichen mit ihrem gefühlten Informationsgrad einen Mittelwert von 3.5, die beiden grösseren Kategorien (10–19 und 20–49 Mitarbeitende) je 3.7. Pioniere (4.2) fühlen sich jedoch signifikant besser informiert als Early Follower (3.6) und diese wiederum fühlen sich signifikant besser informiert als Late Follower (3.3).

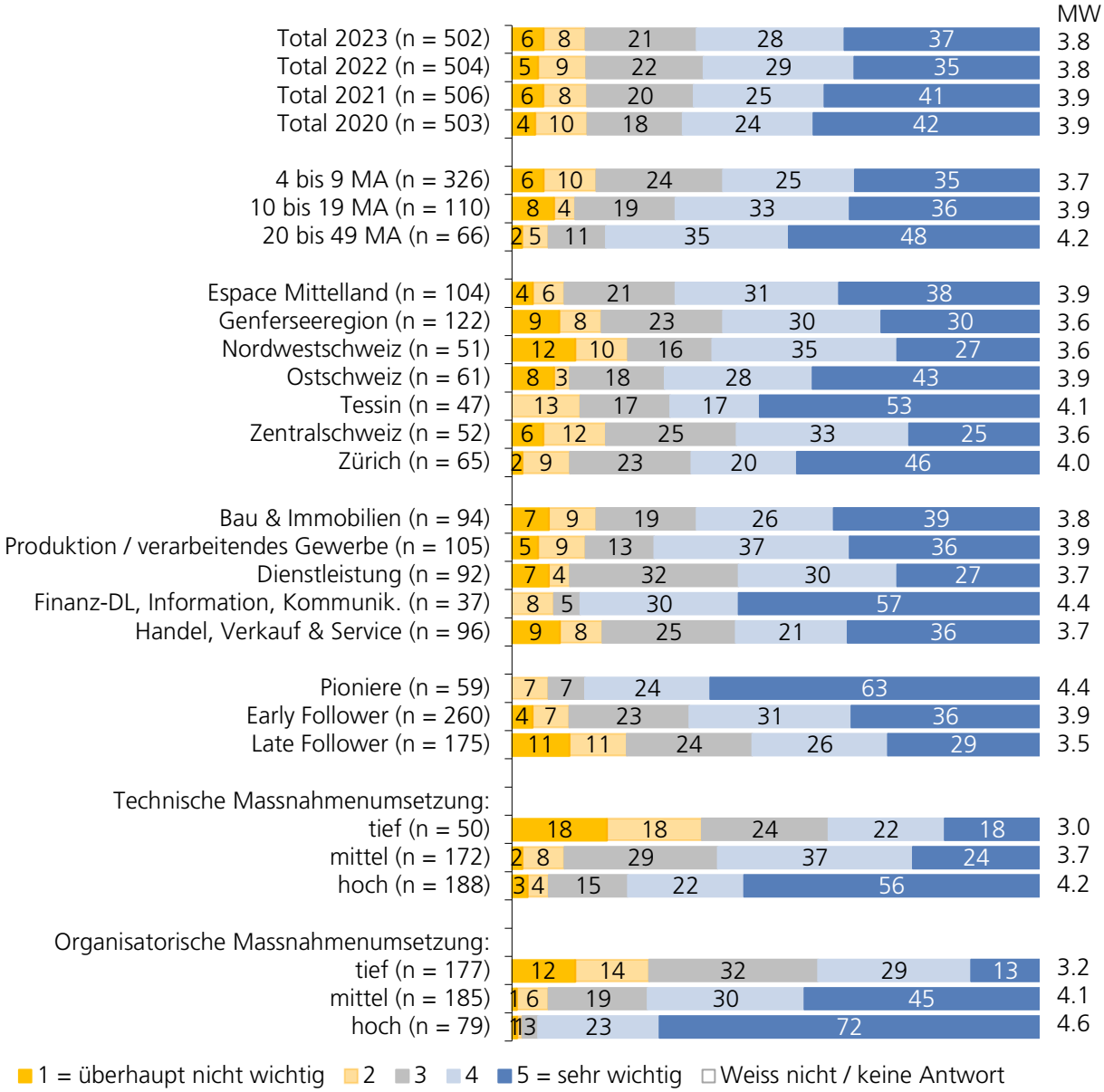
Besonders hoch und ebenfalls signifikant sind die Unterschiede zwischen den Unternehmen, die erst wenige bzw. schon viele technische und organisatorische Sicherheitsmassnahmen umgesetzt haben. Eher oder sehr gut informiert fühlt sich nur rund ein Viertel (26 %) der Befragten mit einer *tiefen technischen* Massnahmenumsetzung, aber mehr als zwei Drittel (69 %) der Befragten mit einer *hohen technischen* Massnahmenumsetzung. Rund ein Drittel (35 %) der Befragten mit einer *tiefen organisatorischen* Massnahmenumsetzung fühlt sich eher oder sehr gut informiert, aber mehr als vier Fünftel (81 %) der Befragten mit einer *hohen organisatorischen* Massnahmenumsetzung.

3.5.2 Wichtigkeit des Themas Cybersicherheit

Frage 16:
Welche Wichtigkeit hat in Ihrer Firma das Thema Cybersicherheit?
Basis: Total, n = 502

Die Wichtigkeit der Cybersicherheit wird seit 2020 praktisch unverändert eingeschätzt. Knapp zwei Drittel (65 %) der Befragten schätzen das Thema Cybersicherheit als eher oder sehr wichtig ein und rund ein Siebtel (14 %) eher oder sehr unwichtig. Der Mittelwert liegt 2023 bei 3.8 (2022: 3.8, 2021: 3.9, 2020: 3.9).

Wie schon im Jahr zuvor gilt: Je mehr Mitarbeitende ein Unternehmen beschäftigt, desto höher wird die Cybersicherheit priorisiert, der Unterschied zwischen den kleinsten befragten Unternehmen (4–9 Mitarbeitende: 3.7) und den grössten (20–49 Mitarbeitende: 4.2) ist signifikant. Ein Zusammenhang besteht auch zwischen der Einstellung zu technischen Neuerungen und der Einschätzung der Wichtigkeit des Themas Cybersicherheit: Fast 9 von 10 Pionieren (87 %) schätzen das Thema Cybersicherheit als eher oder sehr wichtig ein, aber nur etwas mehr als die Hälfte (55 %) der Late Follower. Wer viele technische Massnahmen umgesetzt hat, empfindet das Thema Cybersicherheit signifikant wichtiger (4.2) als wer wenige Massnahmen umgesetzt hat (3.0). Gleiches gilt bei den organisatorischen Massnahmen: Befragte mit einer tiefen organisatorischen Massnahmenumsetzung empfinden das Thema Cybersicherheit signifikant weniger wichtig (3.2) als Befragte mit einer hohen Umsetzung (4.6). Diese Unterschiede sind nicht neu; sie wurden schon in der Studie 2021 und 2022 festgestellt.

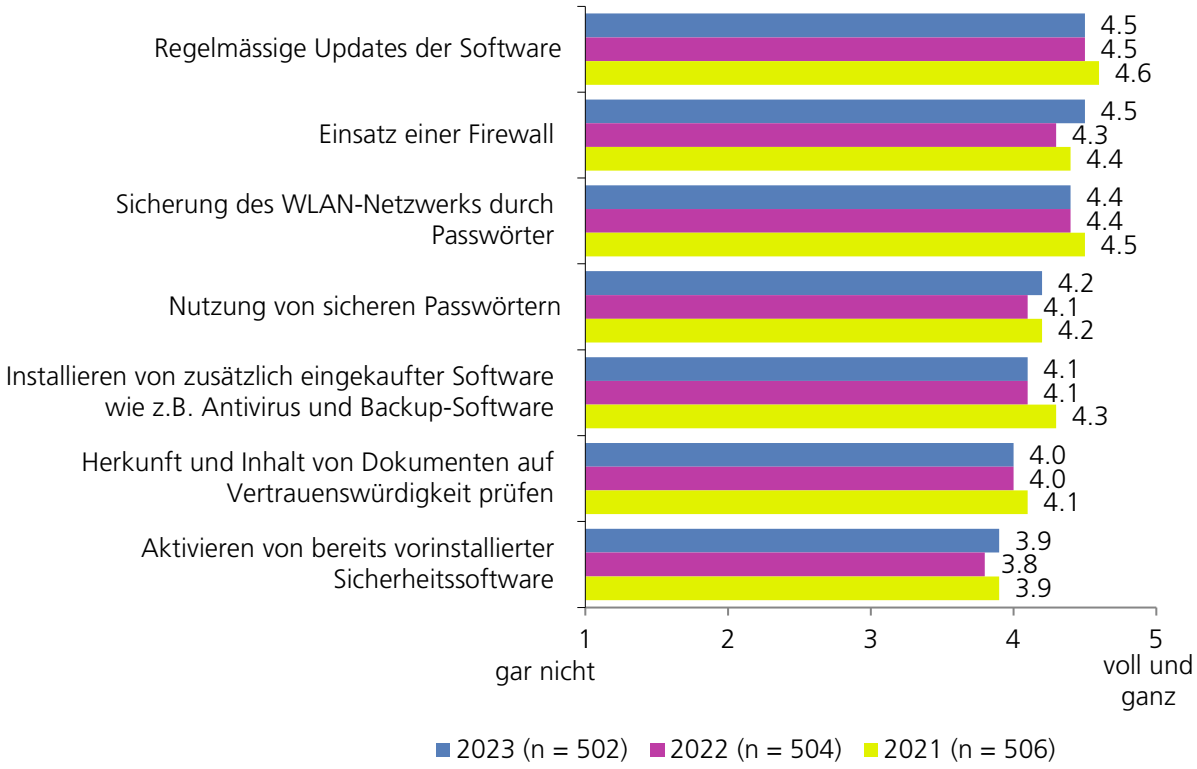


Grafik 14

3.5.3 Technische Massnahmen zur Erhöhung der Cybersicherheit

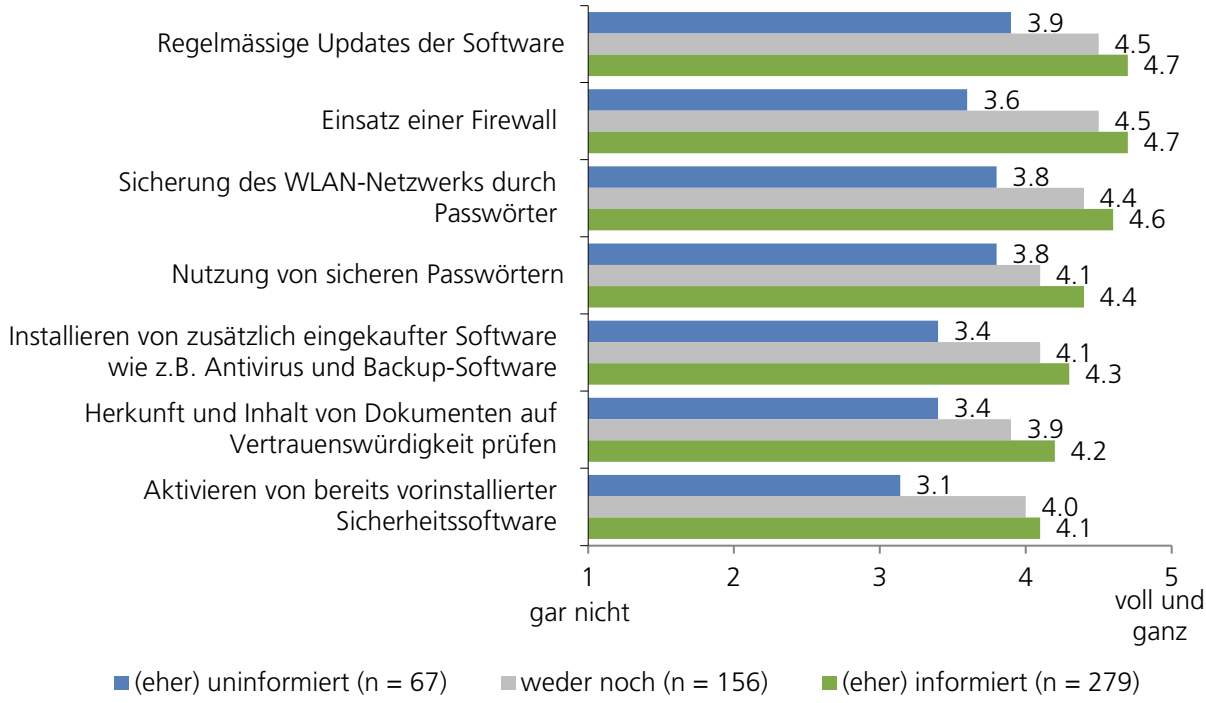
Frage 17:
Inwieweit sind die folgenden **technischen** Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?
Basis: Total, n = 502

Die Umsetzungsgrade der verschiedenen abgefragten Massnahmen liegen zwischen 3.9 und 4.5, allesamt auf praktisch unverändertem Niveau zu 2022 und 2011. Den höchsten Umsetzungsgrad erzielen die beiden Massnahme *Regelmässige Softwareupdates* (4.5) und *Einsatz einer Firewall* (4.5), gefolgt von der Massnahme *Sicherung des WLAN-Netzwerks durch Passwörter* (Mittelwert 4.4). Den tiefsten Umsetzungsgrad und einen Mittelwert unter 4.0 erreicht die Massnahme *Aktivieren von bereits vorinstallierter Sicherheitssoftware* (Mittelwert 3.8).



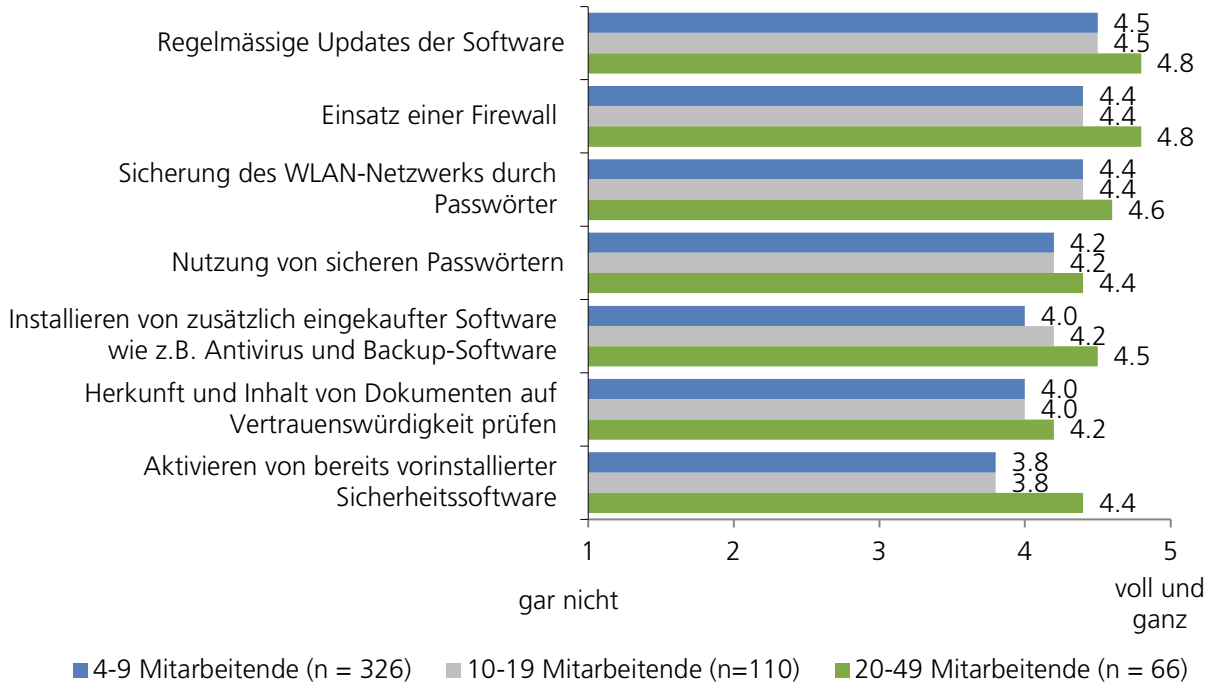
Grafik 15

Bei allen Massnahmen gilt in signifikanter Weise (wie schon in den Vorwellen): Je höher der selbst eingeschätzte Informationsgrad ist, desto höher ist auch die Massnahmenumsetzung (Werte siehe Grafik 15).



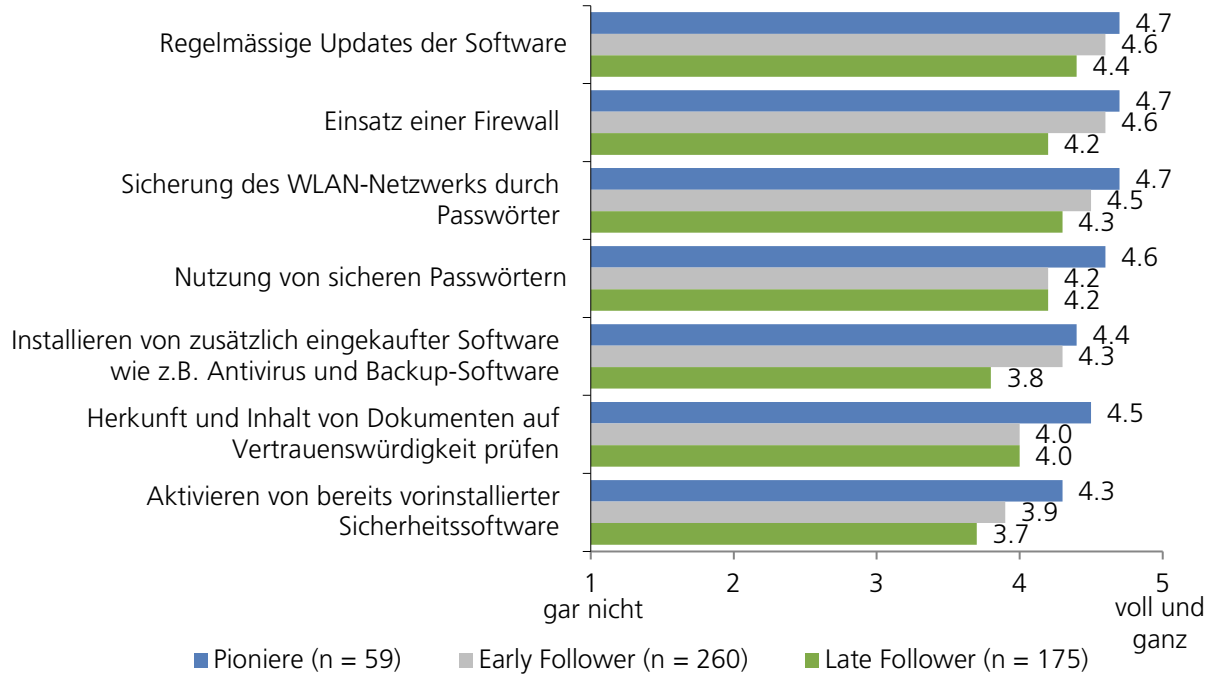
Grafik 16

Sämtliche Massnahmen wurden von den Firmen mit 20 bis 49 Mitarbeitenden häufiger umgesetzt als von Firmen mit 4 bis 9 bzw. 10 bis 19 Mitarbeitenden (Werte siehe Grafik 16). Bei den Massnahmen *Installieren von zusätzlich eingekaufter Software* sowie *Aktivieren von bereits vorinstallierter Sicherheitssoftware* ist der Unterschied signifikant.



Grafik 17

Unterschiede gibt es auch bezüglich der Einstellung zu neuen Technologien. Grundsätzlich haben Pioniere mehr Massnahmen umgesetzt als Early Follower und diese mehr als Late Follower. Diesbezüglich signifikante Unterschiede gibt es bei allen Massnahmen ausser dem *Aktivieren von bereits vorinstallierter Sicherheitssoftware*.

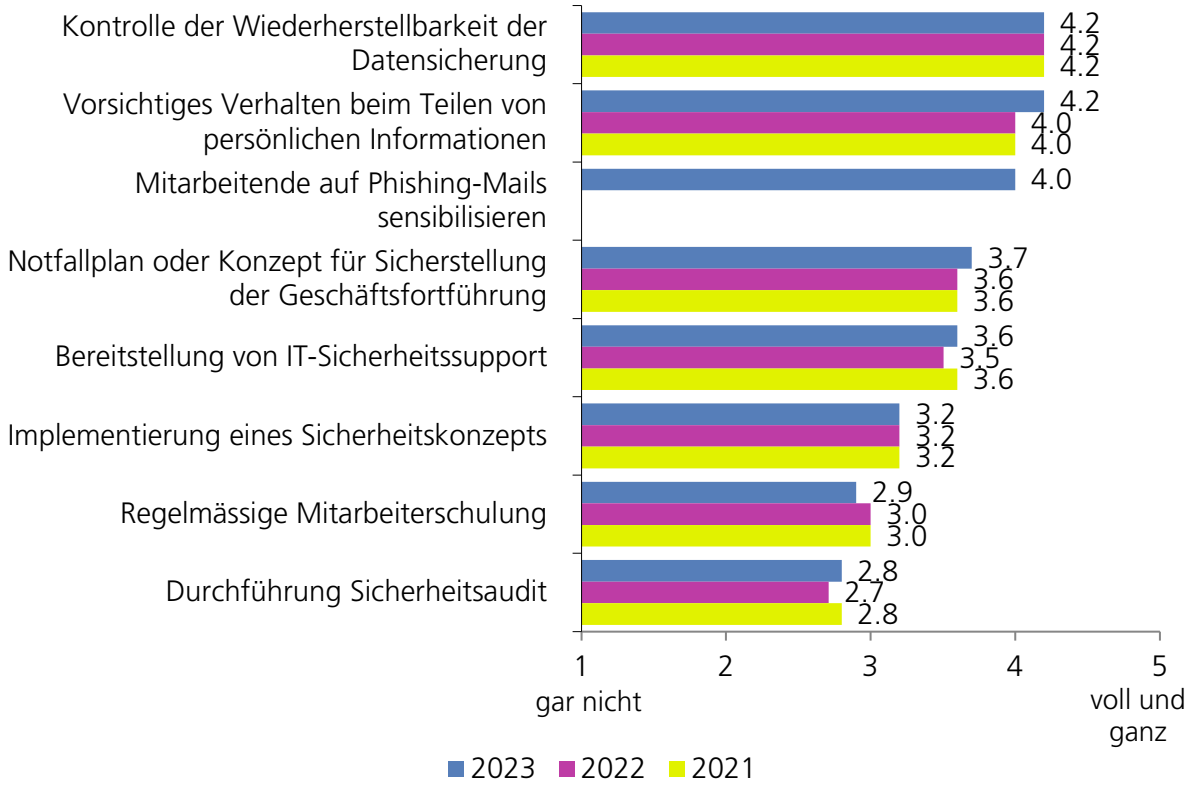


Grafik 18

3.5.4 Organisatorische Massnahmen zur Erhöhung der Cybersicherheit

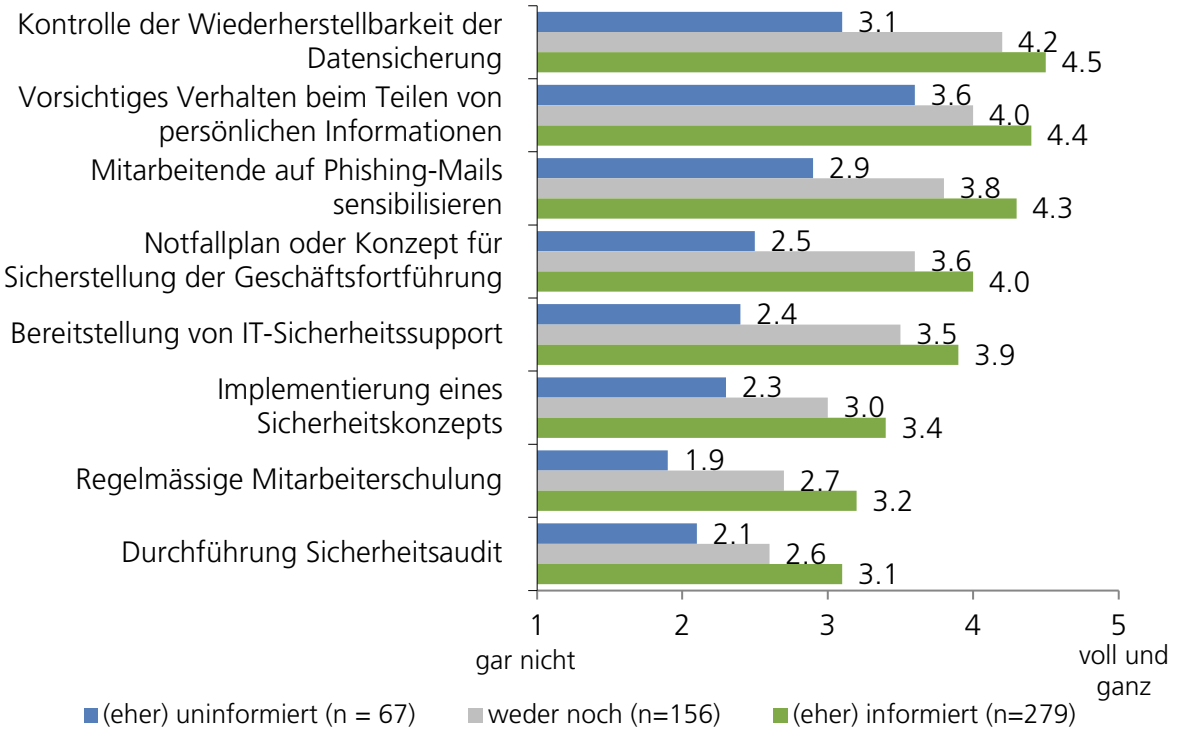
Frage 18:
Inwieweit sind die folgenden **organisatorischen** Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?
Basis: Total, n = 502

Analog zu der Frage nach technischen Sicherheitsmassnahmen (siehe 3.5.3) wurde auch eine Frage nach organisatorischen Sicherheitsmassnahmen gestellt. Wie schon in den Vorwellen 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). Zum Vergleich: Die am häufigsten vollständig umgesetzte *technische* Massnahme, regelmässige Softwareupdates, erreicht den höheren Mittelwert von 4.5. Deutlicher ist der Unterschied, wenn am anderen Ende der Rangfolge verglichen wird: Die beiden am seltensten umgesetzten *organisatorischen* Massnahmen sind die regelmässige Mitarbeiterschulung (2.9) und die Durchführung eines Sicherheitsaudits (2.8); bei den technischen Massnahmen liegt der tiefste Mittelwert bei 3.9 (Aktivieren von bereits vorinstallierter Sicherheitssoftware). Die Veränderungen gegenüber den Vorwellen sind minimal bzw. nicht signifikant.



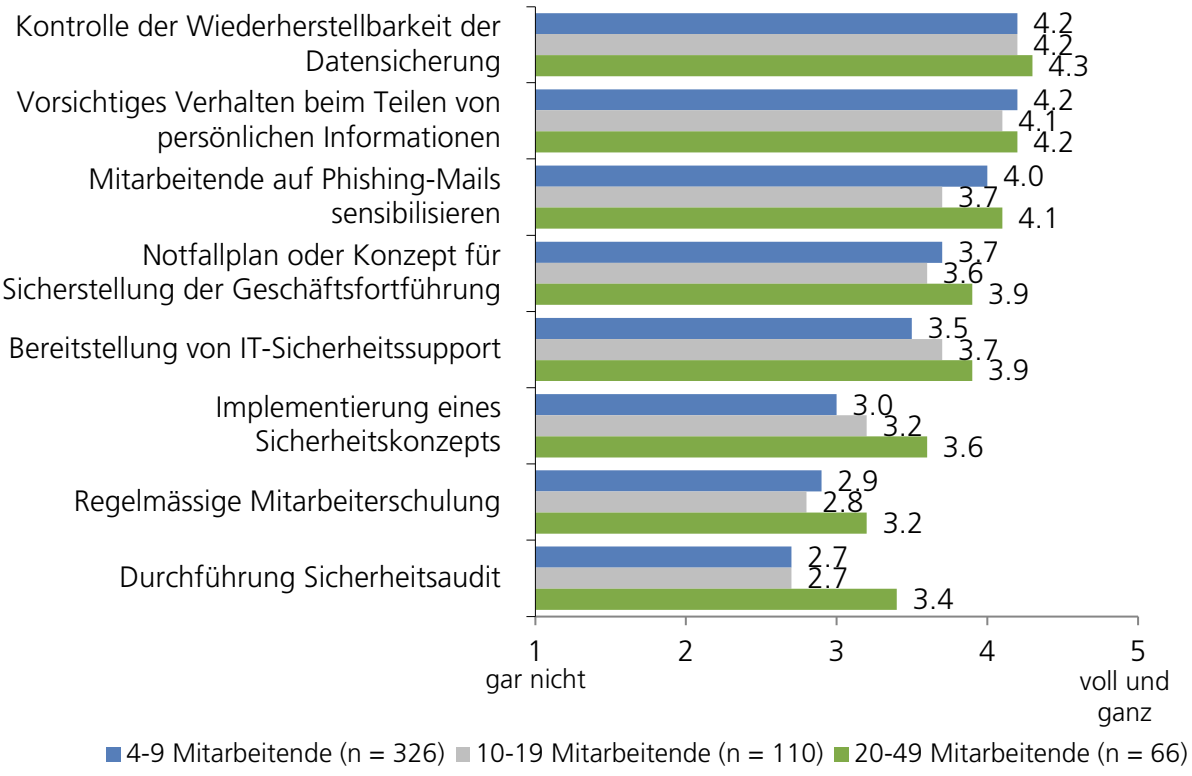
Grafik 19

Je besser sich die Befragten bezüglich dem Thema Cyberrisk informiert fühlen, desto höher ist ihre organisatorische Massnahmenumsetzung. Besonders tief ist der Umsetzungsgrad der regelmässigen Mitarbeiterschulung bei den (eher) uninformierten (1.9). Die Unterschiede sind bei allen Massnahmen signifikant.



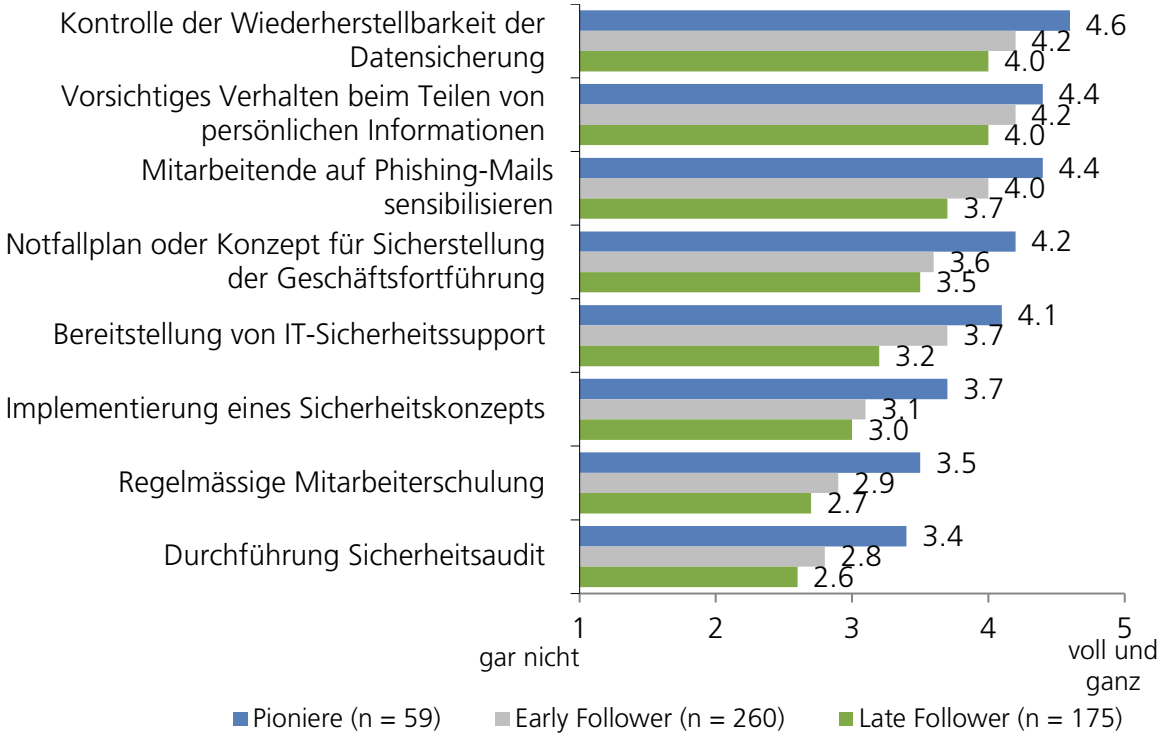
Grafik 20

Bei der grossen Mehrheit der organisatorischen Massnahmen verhält es sich so, dass die grössten abgefragten Unternehmen sie eher umgesetzt haben als die kleineren. Im Falle der *Massnahmen Implementierung eines Sicherheitskonzepts* und *Durchführung eines Sicherheitsaudits* sind die Unterschiede signifikant (Werte siehe Grafik).



Grafik 21

Pioniere haben die meisten Massnahmen umgesetzt, Late Follower die wenigsten. Die Unterschiede sind alle signifikant (Werte siehe Grafik).



Grafik 22

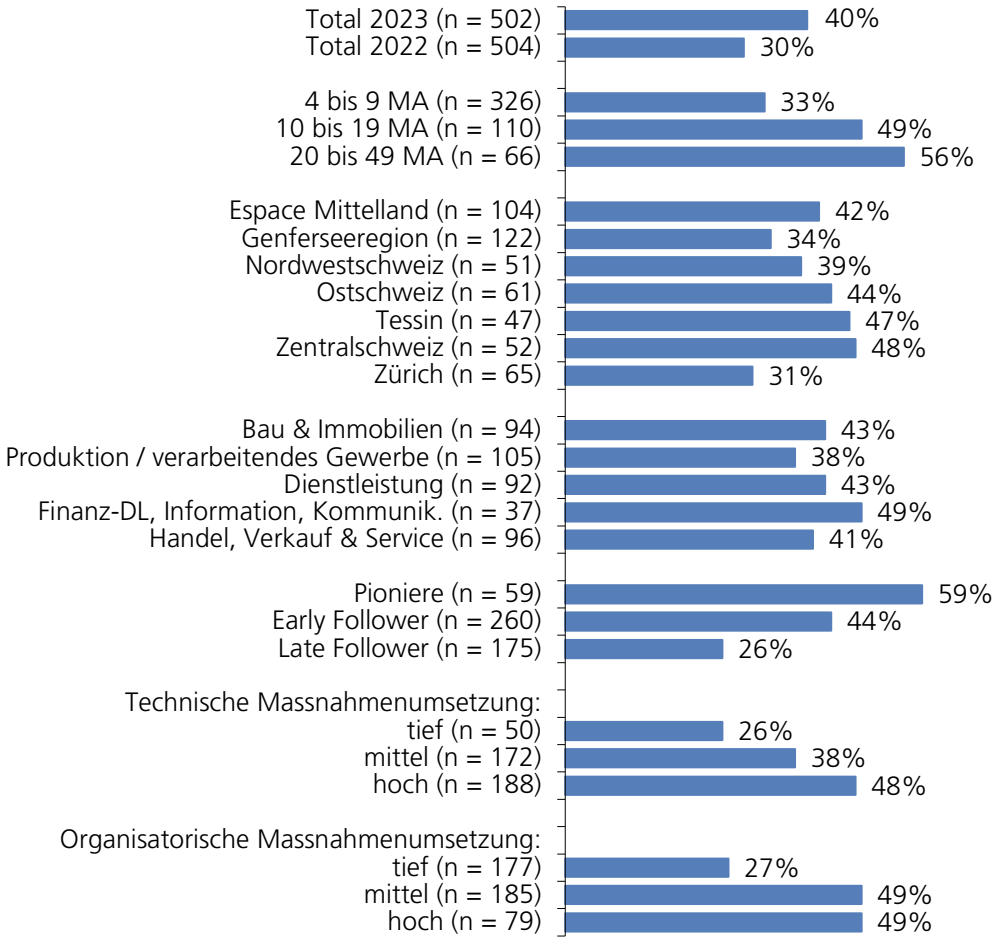
3.5.5 Cyberversicherung

Frage 19:
Verfügt Ihr Unternehmen über eine Cyberversicherung?
Basis: Total, n = 502

Zwei Fünftel (40 %) der befragten Geschäftsführenden verfügen über eine Cyberversicherung für das Unternehmen. Gegenüber dem Vorjahr (30 %) ist das eine eindrückliche Steigerung um 10 Prozentpunkte. Wie schon im Vorjahr ist die grösste befragte Unternehmenskategorie (20–49 Mitarbeitende) am häufigsten versichert: Über die Hälfte von ihnen (56 %) verfügt über eine Cyberversicherung, 2022 war es noch etwas mehr als ein Drittel (36 %). Die kleinste Kategorie (4–9 Mitarbeitende) hat sich von rund einem Viertel (26 %) im letzten Jahr auf einen Drittel (33 %) in diesem Jahr gesteigert, die mittlere Kategorie (10–19 Mitarbeitende) von rund einem Drittel (35 %) auf fast die Hälfte (49 %) der Befragten. Somit haben sich alle drei Unternehmensgrössen-Kategorien in ähnlichem Ausmass – um rund einem Drittel – gesteigert.

Die Pioniere verfügen über den höchsten Versicherungsgrad aller geprüften Subgruppen: Fast 6 von 10 Pionieren (59 %) sind cyberversichert. Gegenüber dem Vorjahr (31 %) hat sich ihr Versicherungsgrad somit fast verdoppelt. Die Early Follower haben sich von etwas mehr als einem Drittel (36 %) auf über zwei Fünftel (44 %) gesteigert und die Late Follower von knapp einem Fünftel (23 %) auf rund einen Viertel (26 %).

Es gilt auch: Je höher die technische und organisatorische Massnahmenumsetzung fortgeschritten ist, desto eher besteht auch eine Cyberversicherung (Werte siehe Grafik 23).



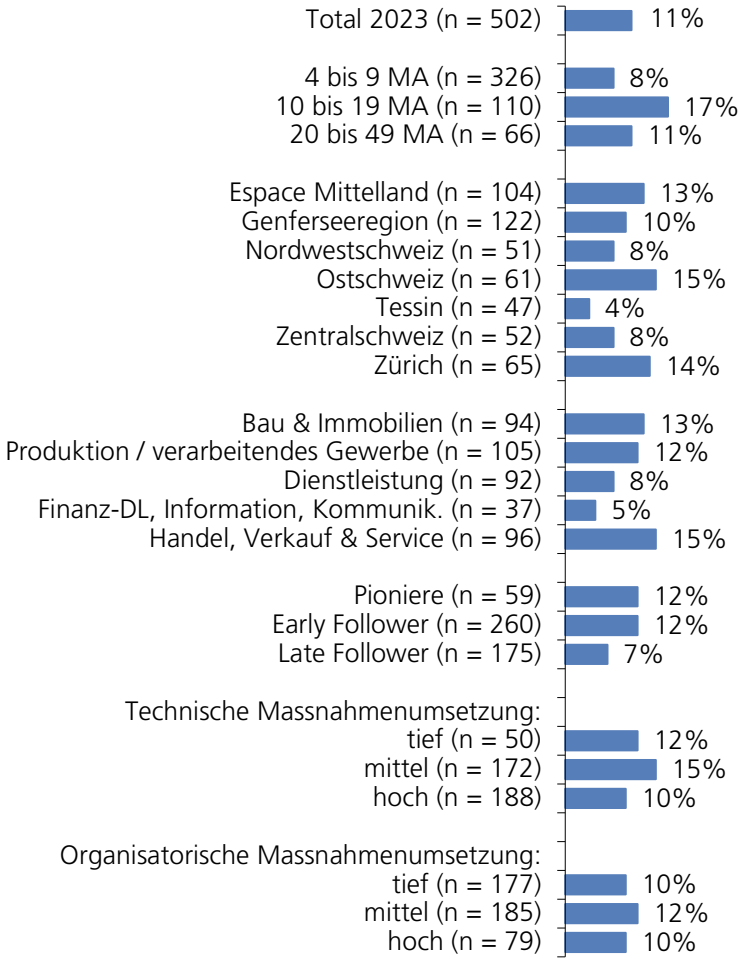
Grafik 23

3.5.6 Erfolgreiche Cyberangriffe

Frage 20:
Wurde Ihre Firma schon einmal erfolgreich von Cyberkriminellen angegriffen, so dass ein erheblicher Aufwand nötig war, um Schäden zu beheben?
Basis: Total, n = 502

Rund jede/-r zehnte Befragte (11 %) sagt, dass sein bzw. ihr Unternehmen schon einmal erfolgreich von Cyberkriminellen angegriffen wurde, so dass ein erheblicher Aufwand nötig war, um die Schäden zu beheben. Unternehmen mit 10 bis 19 Mitarbeitenden (17 %) heben sich dabei signifikant von Unternehmen mit 4 bis 9 Mitarbeitenden (8 %) ab; ansonsten gibt es aber keine signifikanten Unterschiede zwischen den untersuchten Subgruppen, insbesondere nicht zwischen den verschiedenen Branchen: Es gibt also keine besonders gefährdeten oder ungefährdeten Branchen und es gilt der Grundsatz: Es kann jeden treffen.

Aufgrund einer wesentlichen Veränderung (Vereinfachung) der Fragestellung ist ein Vergleich zu den Vorwellen nicht möglich.

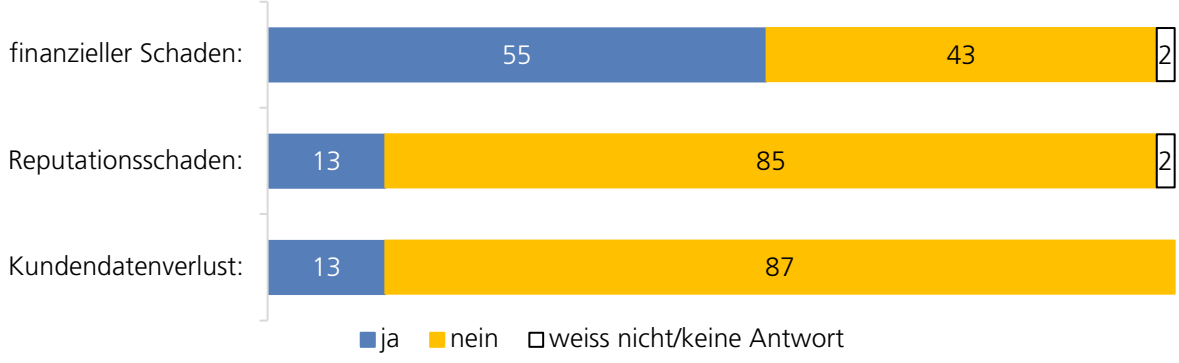


Grafik 24

3.5.7 Schaden durch Cyberangriffe

Frage 21:
Entstand durch diesen Angriff / Entstanden durch diese Angriffe ein …
Basis: wurde schon angegriffen, n = 53

Über die Hälfte (55 %) der Befragten, die schon angegriffen wurden, beklagt einen finanziellen Schaden. Das entspricht rund 6 Prozent der Gesamtstichprobe (n = 502). Somit darf angenommen werden, dass 6 Prozent der Schweizer KMU mit 4 bis 49 Mitarbeitenden schon einmal einen finanziellen Schaden durch einen Cyberangriff erlitten haben (Vertrauensintervall: +/- 2.1 Prozent). Einen Reputationsschaden bzw. einen Kundendatenverlust beklagt je rund ein Achtel (13 %) der Befragten, die schon einmal angegriffen wurden.

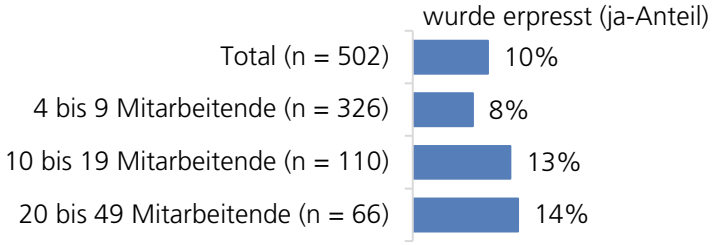


Grafik 25

3.5.8 Erpressung und Lösegeld

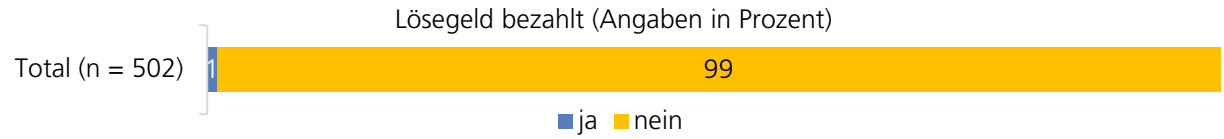
Jede/-r zehnte Befragte (10 %) sagt, dass sein/ihr Unternehmen schon einmal von Cyberkriminellen erpresst wurde. Dabei kann es sich um einfachere Fälle (z.B. reine Drohung per Mail), aber auch um schwere Fälle (z.B. Denial-of-Service-Attacke oder Datendiebstahl) handeln. Auch hier zeigt sich im Vergleich der Subgruppen: Es gibt keine signifikanten Unterschiede und somit keine besonders gefährdeten oder ungefährdeten Gruppen.

Frage 22:
Wurde Ihr Unternehmen schon einmal von Cyberkriminellen erpresst?
Frage 23:
Hat Ihr Unternehmen schon einmal Lösegeld an Cyberkriminelle bezahlt?
Basis: Total, n = 502



Grafik 26

Ein Prozent der Befragten sagt, dass sein/ihr Unternehmen schon einmal Lösegeld an Cyberkriminelle bezahlte. Somit bezahlte jede/-r zehnte Erpresste Lösegeld; zusätzlich muss wahrscheinlich noch von einer gewissen Dunkelziffer ausgegangen werden. Die fünf befragten Unternehmen in der hier vorliegenden Stichprobe verfügen alle über eine Cyberversicherung, allerdings kann diese Studie nichts darüber aussagen, ob die Versicherung vor oder nach dem Erpressungsfall in Kraft trat. Für Hochrechnungen auf die gesamte Stichprobe bzw. Grundgesamtheit ist der Wert zu tief.



Grafik 27

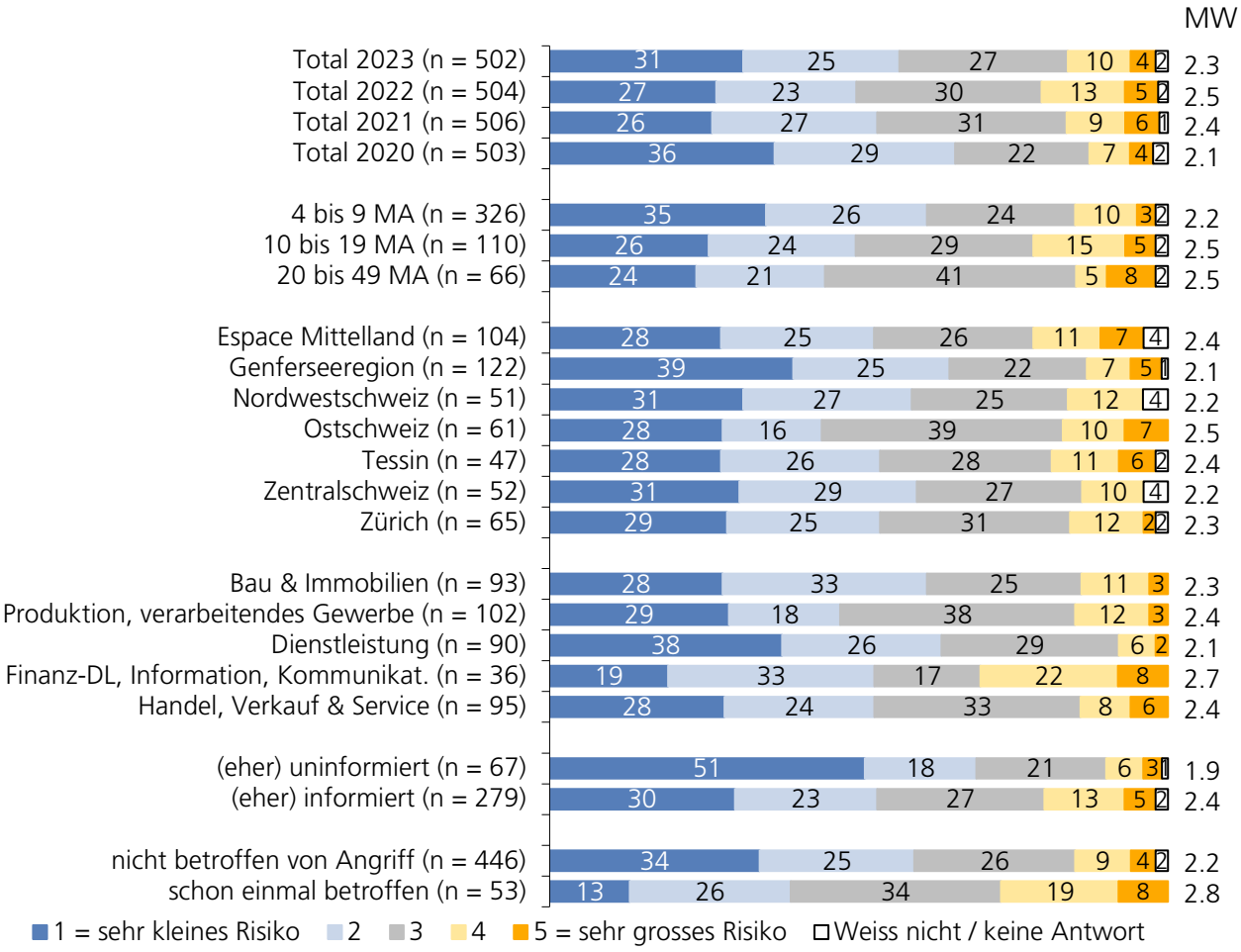
3.5.9 Risiko-Einschätzung eines Cyberangriffs

Über die Hälfte der Befragten (56 %) schätzt das Risiko, für mindestens einen Tag lang ausser Kraft gesetzt zu werden durch einen Cyberangriff, als eher oder sehr tief ein. Nur rund jede/-r Siebte (14 %) schätzt das Risiko als eher oder sehr hoch ein. Somit ist die Risikoeinschätzung wieder leicht gesunken, nachdem sie in den letzten drei Wellen stetig ganz leicht gestiegen ist.

Frage 24:
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 = 502

Die kleinste abgefragte Unternehmensgrössen-Kategorie (4–9 Mitarbeitende) schätzt das Risiko tendenziell etwas tiefer ein (2.2) als die grösseren beiden Kategorien (je 2.5). Auch die Unterschiede zwischen den Grossregionen und Branchen sind nicht signifikant (Werte siehe Grafik).
Bei der Einstellung zu technischen Neuerungen gilt wie schon in den Vorwellen: Je innovativer die befragten Unternehmen sind, desto höher schätzen sie das Risiko eines Cyberangriffs ein (Late Follower: 2.0, Early Follower: 2.4, Pioniere: 2.5). Der Unterschied zwischen den Pionieren und den Late Followern ist signifikant. Zur Erinnerung: Die Late Follower sind nicht in statistisch signifikantem Masse weniger von Angriffen betroffen als Pioniere (siehe Kapitel xxx). Auch zwischen dem Informationsgrad und der Risikoeinschätzung gibt es einen Zusammenhang: Wer sich (eher) gut informiert fühlt bezüglich dem Thema Cyberrisk, schätzt das Risiko eines Angriffs signifikant höher ein (2.4) als Personen, die sich (eher) uninformiert fühlen (1.9).

Angesichts der hohen Anzahl Betroffener und der weitverbreitenden Berichterstattung über Cyberkriminalität ist es auch 2023 wieder erstaunlich, wie tief das Risiko eingeschätzt wird.



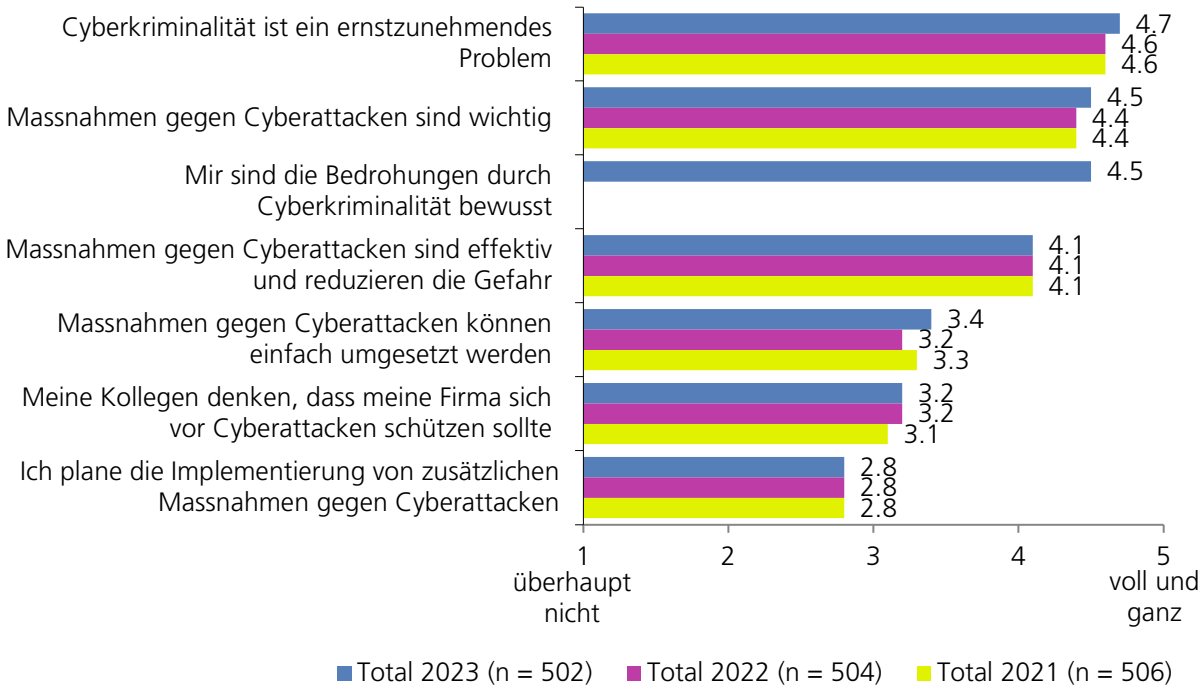
Grafik 28

3.5.10 Einstellung zu Cyberkriminalität

Frage 25:
Inwiefern stimmen Sie den folgenden Aussagen zu Cyberkriminalität wie Malware, Online-Betrug und Hacking zu?
Basis: Total, n = 502

Die sieben abgefragten Einstellungsmerkmale zu Cyberkriminalität werden 2023 fast gleich beantwortet wir in den beiden Vorwellen. Hohe Zustimmung erhalten die Aussagen *Cyberkriminalität ist ein ernstzunehmendes Problem* (4.7), *Massnahmen gegen Cyberattacken sind wichtig* (4.5), *Mir sind die Bedrohungen durch Cyberkriminalität bewusst* (4.5) und *Massnahmen gegen Cyberattacken sind effektiv und reduzieren die Gefahr* (4.1). Weniger einverstanden sind die Befragten mit der Aussage *Massnahmen gegen Cyberattacken können einfach umgesetzt werden* (3.4). Noch tiefer ist die Zustimmung zur Aussage, welche den sozialen Druck abzubilden versucht: *Meine Kollegen denken, dass meine Firma sich vor Cyberattacken schützen sollte* (3.2). Auffallend ist hier die hohe Zustimmung der Befragten aus den Branchen Finanz-Dienstleistungen, Information und Kommunikation: Mit einem Mittelwert von 4.1 liegen sie signifikant höher als die Branchen Bau & Immobilien (3.2), Dienstleistungen (3.2) und Handel, Verkauf & Service (3.1). Die tiefste Zustimmung erhält die Aussage *Ich plane die Implementierung von zusätzlichen Massnahmen gegen Cyberattacken* (2.8). Dieser Mittelwert hat sich in den drei Wellen nicht verändert. Befragte in der grössten Unternehmenskategorie (20–49 Mitarbeitende) stimmen dieser Aussage signifikant stärker zu (3.4) als Befragte der kleineren Kategorien (4–9 Mitarbeitende: 2.7, 10–19 Mitarbeitende: 2.8).

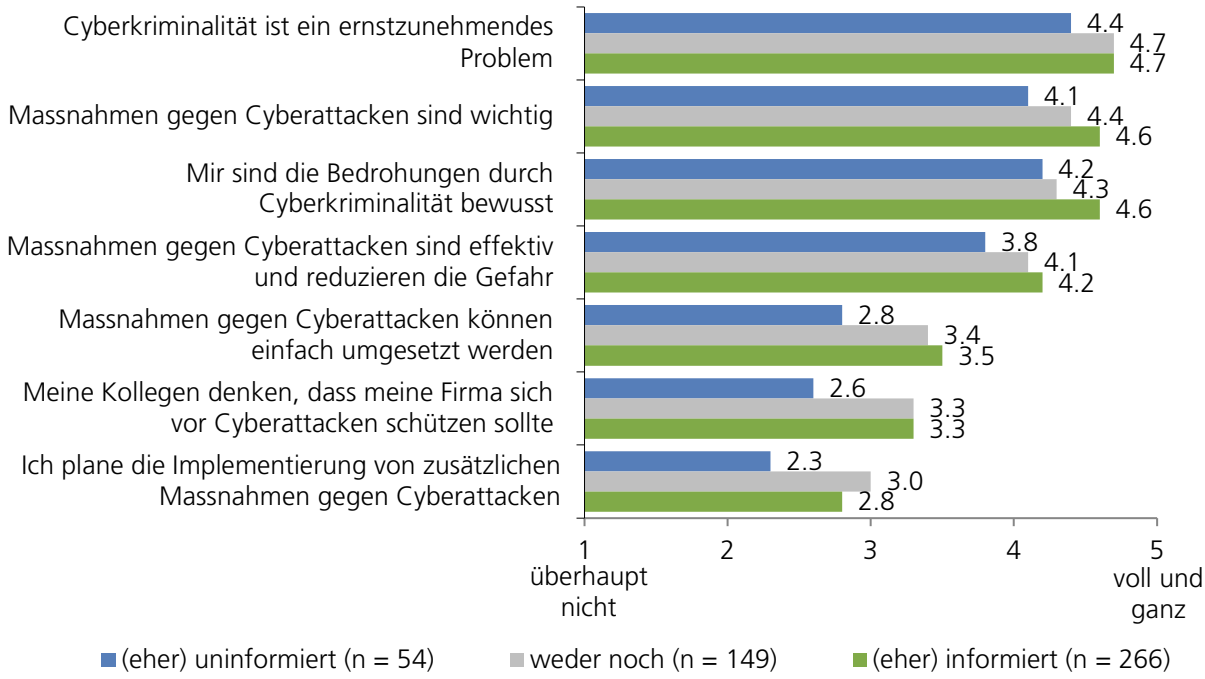
Unverändert gegenüber den beiden Vorwellen kann gesagt werden: Die Gefahr wird grundsätzlich erkannt, Massnahmen dagegen werden aber nur von einer Minderheit der Befragten geplant. Gründe gegen die Massnahmen können in deren Umsetzungsschwierigkeit liegen oder darin, dass die Befragten keinen sozialen Druck dazu spüren.



Grafik 29

Zwischen Unternehmensgrössen-Kategorien, Branchen und Regionen gibt es keine nennenswerten Unterschiede, mit Ausnahme der weiter oben erwähnten Differenz bei der Aussage *Meine Kollegen denken, dass meine Firma sich vor Cyberattacken schützen sollte*.

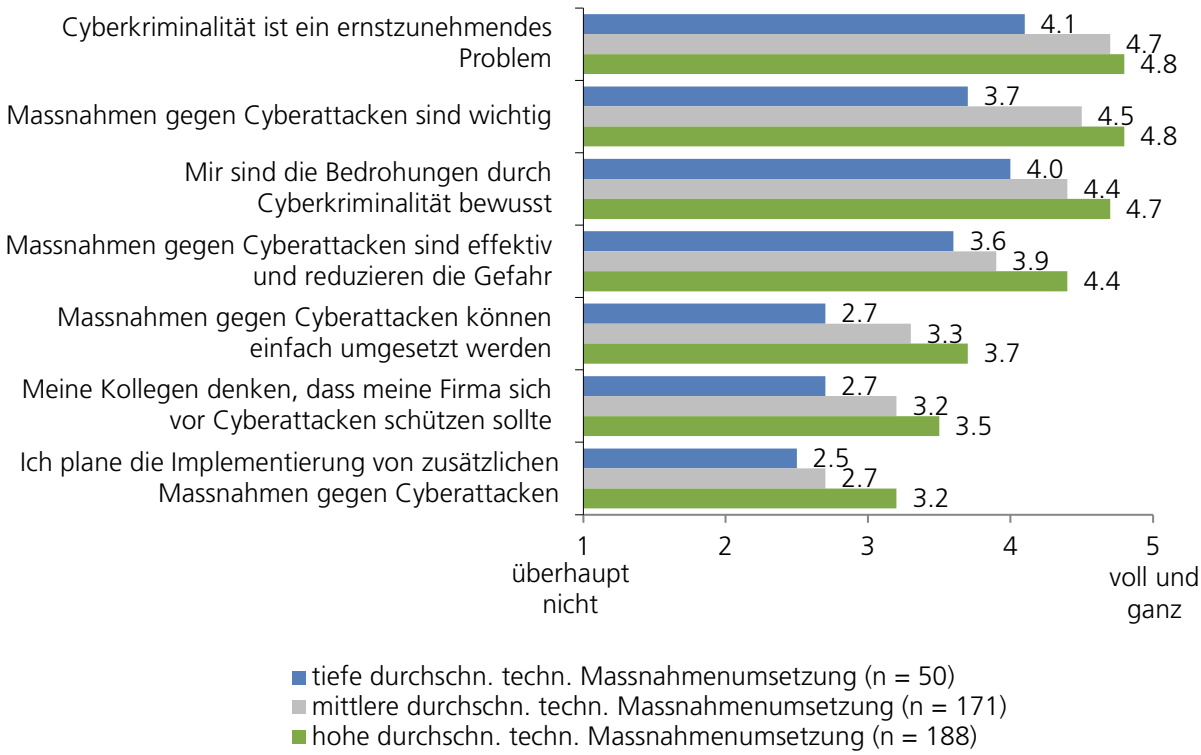
Bei fast allen Aussagen steigt die Zustimmung mit dem gefühlten Informationsgrad zum Thema Cyberrisiken (Werte siehe Grafik 30). Die Unterschiede zwischen den (eher) Informierten und den (eher) Uninformierten sind alle signifikant.



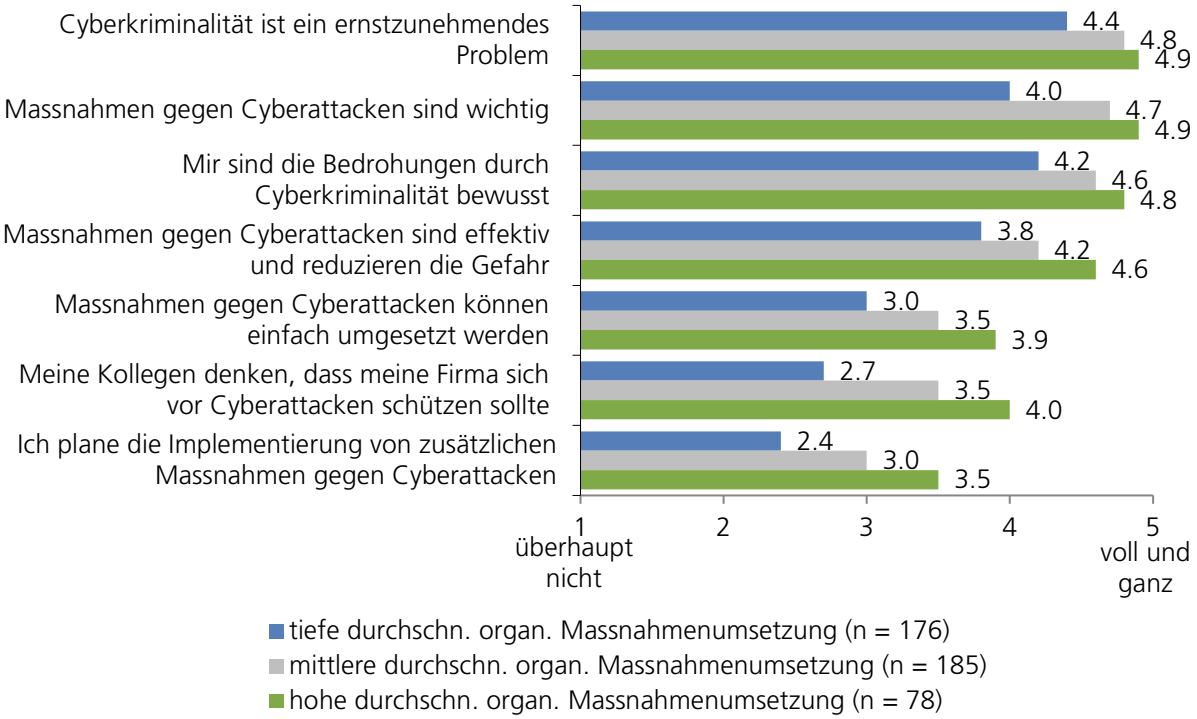
Grafik 30

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 31 und 32). Die Unterschiede vom höchsten zum tiefsten Umsetzungsgrad sind bei allen Aussagen signifikant.

Es sind also vor allem die Befragten mit tiefem Umsetzungsgrad der technischen und organisatorischen Sicherheitsmassnahmen, die den Aussagen widersprechen: Sie empfinden Massnahmen als weniger wichtig, als weniger effektiv, als weniger einfach umsetzbar, fühlen weniger sozialen Druck ausgesetzt und planen auch weniger, Massnahmen umzusetzen. Es ist möglich, dass zumindest ein Teil dieser Gruppe aufgrund tiefer Digitalisierung tatsächlich etwas weniger gefährdet ist; aber die Resultate aus Frage 20 (Betroffenheit von Cyberangriffen) zeigt, dass alle Gruppen gleichermassen betroffen und somit gefährdet sind.

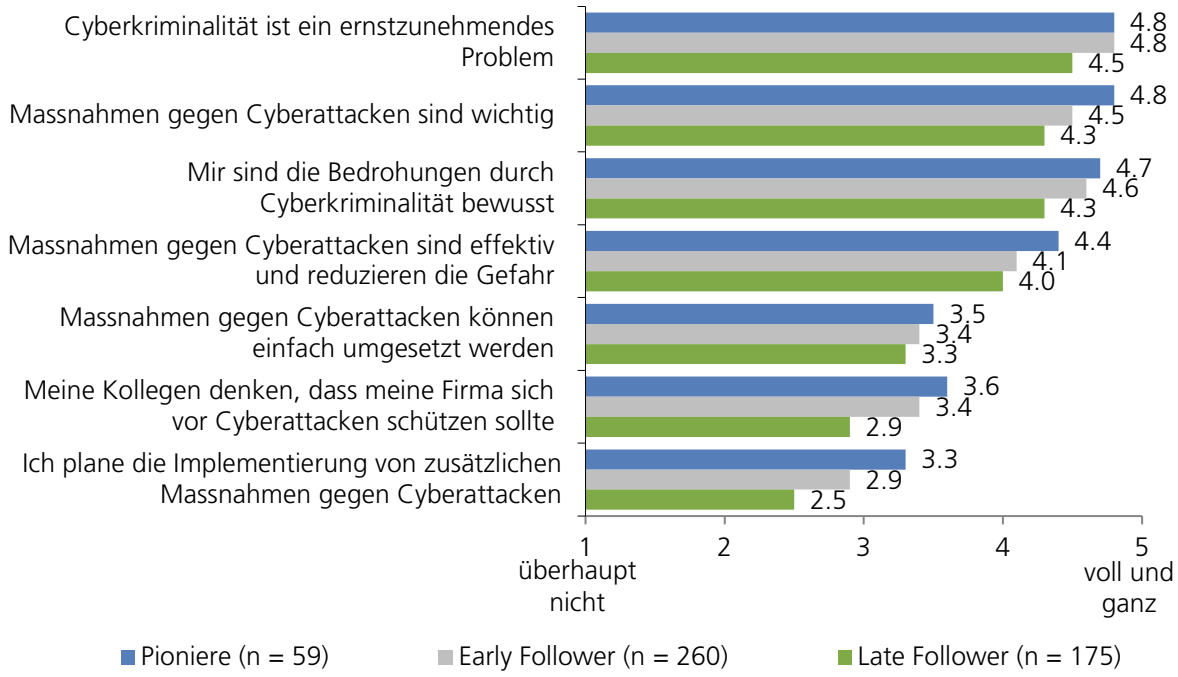


Grafik 31



Grafik 32

Grundsätzlich gilt: Je innovativer die Unternehmen eingestellt sind, desto höher ist ihre Zustimmung zu den verschiedenen Aussagen. Late Follower geben allen Aussagen signifikant tiefere Zustimmungswerte als Pioniere, einzig bei der Aussage *Massnahmen gegen Cyberattacken können einfach umgesetzt werden* gibt es keine signifikanten Unterschiede.



Grafik 33

3.5.11 Passwort-Sicherheitsvorkehrungen

Frage 26:
Welche der folgenden Passwort-Sicherheitsvorkehrungen haben Sie in Ihrem Unternehmen umgesetzt?
Basis: Total, n = 502

2023 wurden fünf Passwort-Sicherheitsvorkehrungen abgefragt (2022: 3), die Befragten haben im Durchschnitt 2.7 davon in ihrem Unternehmen umgesetzt. Fast neun von zehn Befragten (89 %) haben mindestens eine Passwort-Sicherheitsvorkehrung getroffen; das heisst aber auch, dass rund jede/-r zehnte (11 %) gar keine entsprechenden Vorkehrungen traf. Je grösser das befragte Unternehmen ist und je aufgeschlossener die Befragten gegenüber technischen Innovationen sind, desto mehr Passwort-Sicherheitsvorkehrungen werden umgesetzt (4–9 Mitarbeitende: 2.6, 10–19 Mitarbeitende: 2.7, 20–49 Mitarbeitende: 2.9 / Late Follower: 2.4, Early Follower: 2.8, Pioniere: 3.4). Bei den (eher) gut bezüglich Cyberrisk informierten Befragten liegt die durchschnittliche Anzahl umgesetzter Passwort-Sicherheitsvorkehrungen bei 3.0, bei den (eher) schlecht informierten bei 2.1. Und es gilt auch: Je mehr technische und organisatorische Massnahmen generell umgesetzt sind, desto eher werden auch Passwort-Sicherheitsvorkehrungen getroffen (technische Massnahmenumsetzung tief: 2.3, mittel: 2.6, hoch: 3.0 / organisatorische Massnahmenumsetzung tief: 2.1, mittel: 3.0, hoch: 3.3).

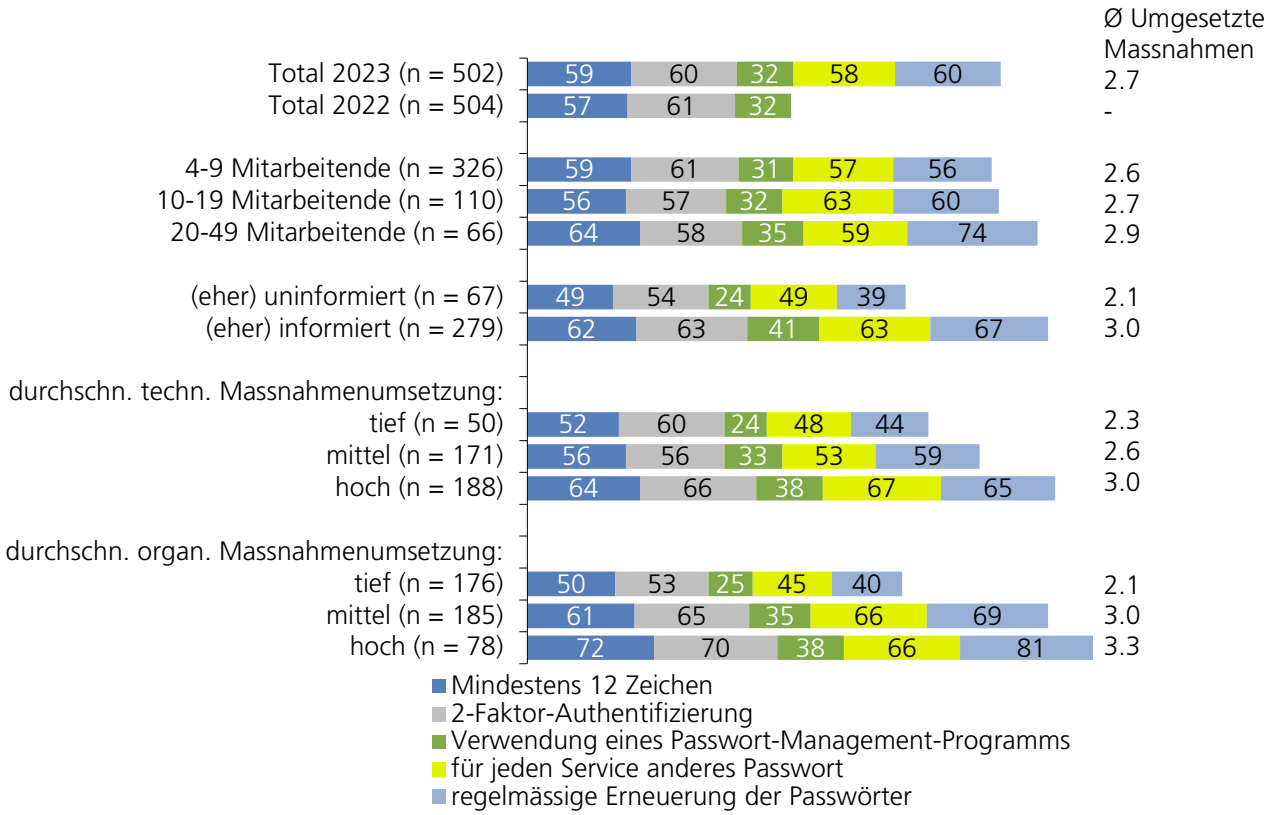
Vier der fünf Massnahmen wurden von jeweils rund 6 von 10 Befragten umgesetzt: Die Mindestlänge von 12 Zeichen (59 %), die 2-Faktor-Authentifizierung (60 %), ein unterschiedliches Passwort für jeden Service (58 %) und die regelmässige Erneuerung der Passwörter (60 %). Über eine Passwort-Management-Programm verfügt rund ein Drittel (32 %) der befragten Unternehmen. Die drei Massnahmen, die schon im Vorjahr abgefragt wurden, erreichten damals die fast genau gleichen Werte (siehe Grafik).
Die Unternehmensgrössen-Kategorien unterschieden sich hauptsächlich durch die Massnahme *regelmässige Erneuerung der Passwörter*. In der grössten Kategorie (20–49 Mitarbeitende) haben

fast drei Viertel (74 %) diese Massnahme umgesetzt, in den beiden kleineren Kategorien nur rund 6 von 10 Unternehmen (4–9 Mitarbeitende: 56 %, 10–19 Mitarbeitende: 60 %).

Die (eher) gut Informierten haben sämtliche Massnahmen deutlich häufiger umgesetzt als die (eher) schlecht Informierten. Bei den beiden Massnahmen *Verwendung eines Passwort-Management Systems* und *Regelmässige Erneuerung der Passwörter* sind die Unterschiede signifikant (Werte siehe Grafik).

Unternehmen mit hoher technischer Massnahmenumsetzung haben signifikant häufiger eine 2-Faktor-Authentifizierung (66 %) und verlangen signifikant häufiger ein anderes Passwort für jeden Service (67 %) bzw. die regelmässige Erneuerung der Passwörter (65 %) als Unternehmen mit mittlerer oder tiefer technischer Massnahmenumsetzung.

Unternehmen mit hoher organisatorischer Massnahmenumsetzung haben sämtliche abgefragten Passwort-Sicherheitsvorkehrungen signifikant häufiger umgesetzt als Unternehmen mit mittlerer oder tiefer organisatorischer Massnahmenumsetzung.



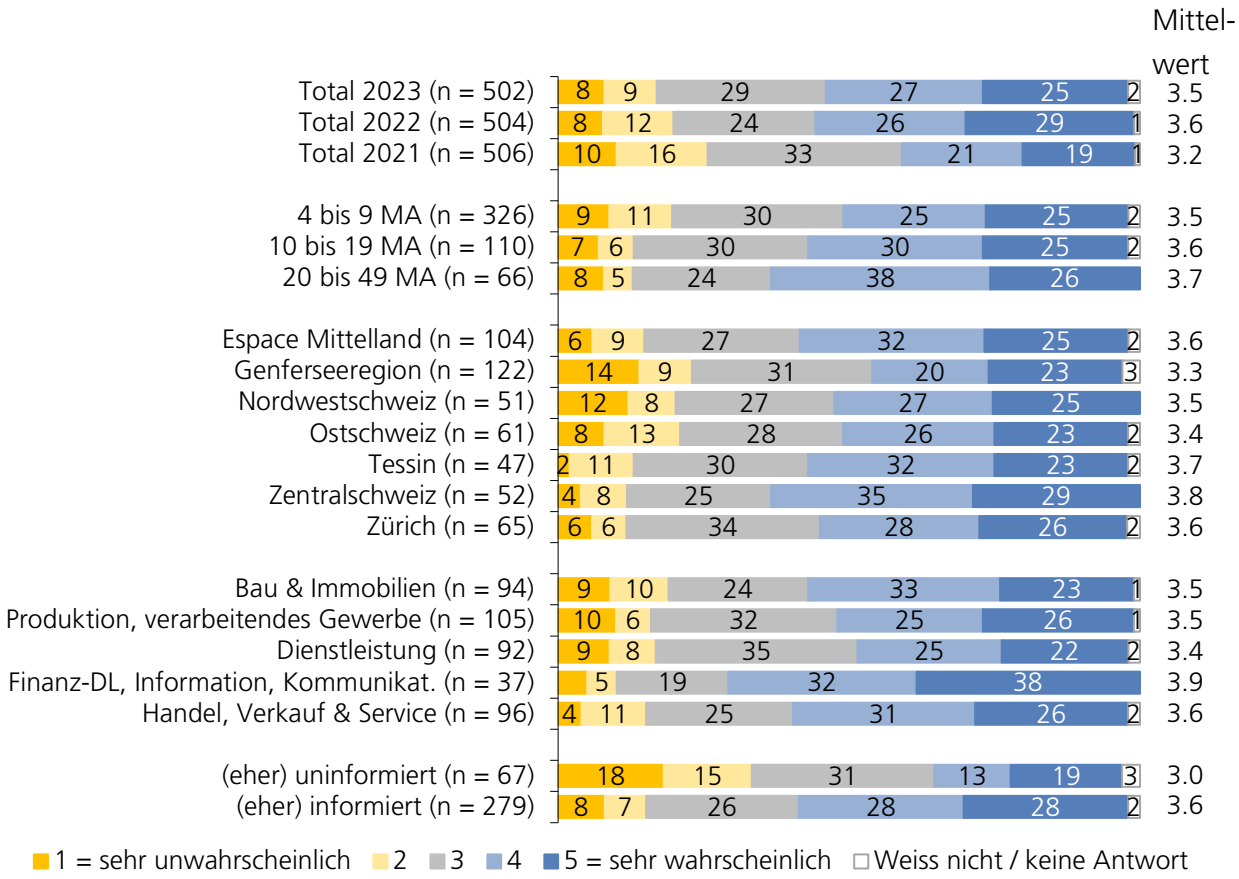
Grafik 34

3.5.12 Geplante Erhöhung der Sicherheitsmassnahmen

Rund die Hälfte (52 %) der Befragten hält es für eher oder sehr wahrscheinlich, dass sie in den nächsten 1 bis 3 Jahren ihre Sicherheitsmassnahmen gegen Cyberkriminalität erhöht. Das sind fast genau gleich viele wie im Vorjahr (55 %) und deutlich mehr als noch 2021 (40 %).

Frage 27:
Wie wahrscheinlich ist es, dass Sie in den kommenden 1 bis 3 Jahren die Sicherheitsmassnahmen gegen Cyberkriminalität erhöhen werden?
Basis: Total, n=502

Je grösser das Unternehmen ist, desto eher sind zukünftige Massnahmen geplant: Der Mittelwert der kleinsten befragten Unternehmen (4–9 Mitarbeitende) liegt bei 3.5, bei den mittleren Unternehmen (10–19 Mitarbeitende) bei 3.6 und bei den grössten Unternehmen (20–49 Mitarbeitende) bei 3.7. Zwischen den Grossregionen und Branchen gibt es keine signifikanten Unterschiede, wenn auch die Wahrscheinlichkeit, Sicherheitsmassnahmen zu erhöhen, bei den Branchen Finanz-Dienstleistungen, Information und Kommunikation tendenziell etwas höher liegt (3.9) als bei den anderen (3.4 bis 3.6).
Signifikant ist der Unterschied zwischen den (eher) uninformierten Befragten (3.0) und den (eher informierten (3.6), und auch Pioniere (4.0) und Early Follower (3.7) planen signifikant häufiger eine Erhöhung der Sicherheitsmassnahmen als Late Follower (3.2).



Grafik 35

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, IT-Dienstleister, Cybersicherheit
Grundgesamtheit:	Geschäftsführende von kleinen Unternehmen (4-49 Mitarbeitende) in der Deutsch-, Westschweiz und im Tessin
Methode:	Telefonische Befragung (CATI)
Stichprobe:	502 durchgeführte Interviews
Gewichtung:	Keine
Quoten	proportional nach Unternehmensgrössen (4–9, 10–19, 20–49)
Interviewdauer:	13 Minuten
Sprachen:	Deutsch, Französisch, Italienisch
Auswertung:	Tabellenband Grafiken Schriftlicher Bericht
Feldphase:	18. April bis 13. Juni 2023
Projektleiterin gfs-zürich:	Karin Mändli Lerch & Mara Huber
Projektmitarbeiter:	Joël Grosjean