gfs-zürich | MARKT- & SOZIALFORSCHUNG

Schlussbericht 2021:

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

Befragung von Geschäftsführenden kleiner Unternehmen in der Schweiz

Studie im Auftrag von:

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, 18. November 2021

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

Vom 16. Juni bis 27. Juli 2021 führte das Markt- und Sozialforschungsinstitut gfs-zürich 506 Interviews mit Geschäftsführenden von Unternehmen mit 4 bis 49 Mitarbeitenden durch.
Ziel war eine Fortschreibung der 2020er Studie mit besonderem Fokus auf die Entwicklung der Homeoffice-Nutzung und auf die Umsetzung organisatorischer und technischer Massnahmen zur Erhöhung der Cybersicherheit.

1.1 Stellenwert und Nutzung des Homeoffice

Nicht jedes Kleinunternehmen hat die gleichen Möglichkeiten, Mitarbeitende vom Homeoffice aus arbeiten zu lassen. Rund ein Drittel der befragten Unternehmen (35 %) kann gemäss eigener Aussage gar keine Mitarbeitenden ins Homeoffice schicken. Bei rund der Hälfte (51 %) kann ein Teil der Mitarbeitenden von zuhause aus arbeiten und bei rund jedem siebten Unternehmen (14 %) können alle Mitarbeitenden vom Homeoffice aus arbeiten.

Vor der Pandemie war gemäss der 2020er-Studie jede/-r zehnte Mitarbeitende (10 %) der befragten Unternehmen hauptsächlich im Homeoffice tätig. Während dem Lockdown im Frühling 2020 blieben knapp zwei Fünftel (38%) im Homeoffice und danach noch immerhin 16 Prozent: Gegenüber den ursprünglichen 10 Prozent bedeutete dies eine Steigerung des Homeoffice-Anteils um über die Hälfte. 2021 gab es keinen weitreichenden Lockdown, aber es wurde eine Homeoffice-Pflicht erlassen (18. Januar bis 26. Juni 2021). Während dieser waren gemäss Befragung rund ein Drittel (36 %) der Mitarbeitenden hauptsächlich im Homeoffice. Dies entspricht fast exakt der Zahl aus der Lockdown-Situation in der 2020er Studie (38 %). Nach Beendigung der Homeoffice-Pflicht (es galt immer noch die Empfehlung) blieb ein Fünftel (20 %) zuhause zum Arbeiten: Gegenüber den ursprünglichen 10 Prozent bedeutet dies eine Verdoppelung des Homeoffice-Anteils.

In der Vorjahresstudie 2020 waren noch fast alle Befragten (94 %) der Meinung, dass zukünftig gleich viele oder mehr Mitarbeitende im Homeoffice arbeiten würden als während dem Lockdown im Frühling 2020. Diese Einstellung hat sich 2021 deutlich verändert: Nur noch knapp zwei Drittel (61 %) nehmen an, dass der Homeoffice-Anteil zukünftig gleichbleiben oder steigen wird. Hingegen sind 38 Prozent der Befragten der Meinung, dass zukünftig weniger Mitarbeitende im Homeoffice arbeiten werden als während der Pandemie (2020: 4 %).

1.2 Cybersicherheit

Seit der 2020er Befragung ist die Anzahl der Cyberangriffe stark angestiegen. War 2020 noch ein Viertel (25 %) der befragten Unternehmen betroffen, so ist es 2021 bereits mehr als ein Drittel (36 %). Hochgerechnet auf die Grundgesamtheit bedeutet dies, dass 2021 rund 55'000 Schweizer Unternehmen mit 4 bis 49 Mitarbeitenden von einem Cyberangriff betroffen waren (Vertrauensbereich: 52’729 bis 57’431), 2020 waren es noch rund 38'000 (Vertrauensbereich: 36’783 bis

39'717). Die Frage wurde bewusst so formuliert, dass unbedeutende oder erfolgreich abgewehrte Angriffe wie zum Beispiel unbeachtete oder ausgefilterte Phishing-Mails nicht in der Statistik erscheinen. Es handelt sich gemäss Fragestellung nur um Angriffe, die einen erheblichen Aufwand benötigten, um die Schäden zu beheben.

Prozentual sind die aus den Angriffen resultierenden Schadensfälle gegenüber dem letzten Jahr aber gesunken. Im letzten Jahr entstand in rund einem Drittel (34 %) der Angriffsfälle ein finanzieller Schaden, dieses Jahr ist das nur noch bei einem Viertel (25 %) der Fall. Bei jedem zehnten Angriff entstand letztes Jahr ein Reputationsschaden (10 %), dieses Jahr bei rund jedem 16. Angriff (6 %). Bezüglich Kundendatenverlust ist der prozentuale Rückgang kleiner: Von 9 Prozent im letzten Jahr sank er auf 7 Prozent in diesem Jahr.

Die Risikoeinschätzung ist leicht gestiegen. Das Risiko, durch einen Cyberangriff einen Tag lang ausser Kraft gesetzt zu werden, wurde 2020 noch von rund zwei Dritteln (65%) mit eins oder zwei (sehr oder eher kleines Risiko) auf der Fünferskala bewertet. In der aktuellen Studie tut dies nur noch rund die Hälfte der Befragten (53 %). Als eher hohes oder hohes Risiko (Skalenwerte 4 und 5) schätzte es 2020 noch jeder zehnte (11 %) ein, in diesem Jahr nun rund jeder siebte (15 %). Ein Cyberangriff als existenzgefährdendes Vorkommnis ist nur für sehr wenige Geschäftsführende ein realistisches Szenario, aber auch hier ist die Risikoeinschätzung gestiegen. 2020 war es jeder fünfzigste Befragte (2 %), der das Risiko als eher oder sehr hoch einschätzte (Skalenwerte 4 oder 5 auf Fünferskala). 2021 ist es nun jeder fünfundzwanzigste (4 %). Als eher oder sehr kleines Risiko (Skalenwerte 1 und 2) schätzten es 2020 87 Prozent ein, 2021 sind dies noch 80 Prozent.

Zur Beurteilung der Sicherheitsmassnahmenumsetzung wurden verschiedene technische und organisatorische Massnahmen nach ihrer Umsetzung auf einer Fünferskala abgefragt:

Bei den technischen Massnahmen erzielen die beiden Massnahmen «Regelmässige Softwareupdates» (90 % fast/voll umgesetzt) und die «Sicherung des WLAN-Netzwerks durch Passwörter» (86 % fast/voll umgesetzt) den höchsten Umsetzungsgrad. An dritter Stelle folgt der Einsatz einer Firewall (84 % fast/voll umgesetzt). Die regelmässigen Softwareupdates und die Firewall wurden schon in der Vorjahresstudie 2020 abgefragt (nur ja/nein-Antwortmöglichkeit), und erhielten dort einen fast identischen Umsetzungsgrad von 89 % (Softwareupdates) und 85 % (Firewall). Die «Installation eigens eingekaufter Sicherheitssoftware» wurde von rund vier Fünfteln (81 %) fast oder voll und ganz umgesetzt, ebenfalls vier Fünftel (80 %) der befragten Unternehmen nutzen konsequent sichere Passwörter. Die Massnahme «Prüfung der Herkunft und Inhalte von Dokumenten auf Vertrauenswürdigkeit» wurde von rund drei Vierteln (74 %) fast oder voll und ganz umgesetzt und «Aktivieren von bereits vorinstallierter Sicherheitssoftware» liegt mit 66 % Umsetzungsgrad auf dem letzten Platz.

Die am häufigsten umgesetzte organisatorische Massnahme ist die Kontrolle der Wiederherstellbarkeit der Datensicherung. Rund drei Viertel (77 %) der Befragten haben sie fast oder voll und ganz umgesetzt (2020 allg. umgesetzt: 71 %). An zweiter Stelle steht die Massnahme «Vorsichtiges Verhalten beim Teilen von persönlichen Informationen»: 74 Prozent der Befragten haben sie

fast oder voll und ganz umgesetzt. An dritter Stelle folgt die Bereitstellung von Sicherheitssupport mit rund zwei Dritteln (61 %) der Befragten, die sie fast oder voll und ganz umgesetzt haben. Einen fast gleich hohen Wert (58 %) erhält die Massnahme «Notfallplan für die Sicherstellung der Geschäftsführung» (2020: 48 %). Die restlichen Massnahmen sind von weniger als 50 Prozent der Unternehmen fast oder voll und ganz umgesetzt worden: Implementierung eines Sicherheitskonzepts (2021: 47 %, 2020: 36 %), regelmässige Mitarbeiterschulung (2021: 39 %, 2020: 37 %) und die Durchführung eines Sicherheitsaudits (2021: 37 %, 2020: 21 %). Somit scheint gleich bei mehreren organisatorischen Massnahmen der Umsetzungsgrad gegenüber der 2020er Studie gestiegen zu sein:

- Kontrolle der Wiederherstellbarkeit der Datensicherung (71 % -> 77 %)
- Notfallplan für die Sicherstellung der Geschäftsführung (48 % -> 58 %)
- Implementierung eines Sicherheitskonzepts (36 % -> 47 %)
- regelmässige Mitarbeiterschulung (37 % -> 39 %)
- Durchführung eines Sicherheitsaudits (21 % -> 37 %)

Allerdings ist die Vergleichbarkeit zur Vorstudie aufgrund der Skalenänderung (von ja/nein zu Fünferskala) mit grosser Vorsicht zu geniessen.

1.3 Datenschutz

Auch beim Thema Datenschutz wurde nach der Umsetzung mehrerer Massnahmen auf einer Fünferskala gefragt. Drei der fünf abgefragten Anforderungen des sich aktuell in der Vernehmlassung befindenden neuen Datenschutzgesetzes wurden von je rund einem Viertel der Befragten bereits umgesetzt: Der Prozess zur Herausgabe und Löschung von Daten (28 %), der Prozess zur Meldung von Datenverlust und Sicherheitsverstössen (27 %) und der Prozess zur Vornahme von Datenschutz-Folgeabschätzungen bei heiklen Datenbearbeitungen (23 %). Die weiteren zwei Anforderungen wurden von je rund einem Fünftel der Unternehmen umgesetzt: Verträge mit Auftragsbearbeitern bezüglich der Durchführung der eigenen Datenbearbeitung (21 %) und die Führung eines Dateninventars (20 %).

1.4 Fazit

Der Anteil an Arbeitnehmenden, die hauptsächlich im Homeoffice arbeiten, steigt seit Beginn der Pandemie stetig und hat sich mittlerweile verdoppelt. Vor dem Lockdown im Frühling 2020 arbeiteten 10 Prozent der Mitarbeitenden hauptsächlich von zuhause aus, nach dem Lockdown 16 Prozent und nach der Homeoffice-Pflicht vom Januar bis Juni 2021 waren es bereits 20 Prozent. Eine Mehrheit der Befragten (61 %) geht davon aus, dass diese Zahl zukünftig gleich bleiben oder noch steigen wird; das ist aber eine deutliche Reduktion gegenüber der Einschätzung im letzten Jahr, als noch fast alle (94 %) von gleich bleibenden oder steigenden Zahlen ausgingen.

Der Anteil an Unternehmen, die bereits einmal einen erheblichen Aufwand tätigen mussten, um die Schäden eines Cyberangriffs zu beheben, ist massiv gestiegen. Mehr als jedes dritte Kleinunternehmen (36 %) ist mittlerweile betroffen, 2020 war es noch jedes vierte (25 %). Die dadurch

erlittenen Schäden haben aber nicht proportional zugenommen: Finanzielle Schäden beispielsweise wurden 2020 noch bei rund jedem dritten Angriff (34 %) beklagt, 2021 nur noch bei einem Viertel (25 %). Die Risikoeinschätzung ist gegenüber dem letzten Jahr trotz der Zunahme an Angriffen nur leicht gestiegen. Durch einen Cyberangriff einen Tag ausser Kraft gesetzt zu werden, empfanden 2020 noch 11 Prozent als eher oder sehr grosses Risiko, 2021 sind es 15 Prozent. Das Risiko, in der Existenz bedroht zu werden, beurteilten 2020 noch 2 Prozent der Befragten als eher oder sehr hoch, 2021 sind es 4 Prozent.

Die Umsetzung von technischen Massnahmen gegen Cyberangriffe ist auf hohem Niveau und – so weit es diese Studie beurteilen kann – gleichgeblieben seit 2020. Organisatorische Massnahmen wurden seit 2020 verstärkt umgesetzt, es besteht aber immer noch viel Potenzial, insbesondere bezüglich Sicherheitsaudits (von 37 % der Befragten umgesetzt) und Mitarbeitenden-Schulungen (von 39 % der Befragten umgesetzt). Je besser sich die Unternehmensführenden bezüglich Cyberrisk-Thematik informiert fühlen und je offener sie gegenüber technischen Innovationen eingestellt sind, desto eher haben sie in ihren Unternehmen technische und organisatorische Massnahmen umgesetzt.

Bezüglich des neuen Datenschutzgesetzes werden die abgefragten Massnahmen von rund einem Fünftel bis einem Viertel der Befragten bereits umgesetzt. Sollte das Gesetz so umgesetzt werden, wie es sich momentan in der Vernehmlassung befindet, werden die KMU noch viel Arbeit vor sich haben.

2 Ausgangslage und Ziele

2.1 Mandat und Fragestellung

Nach dem Lockdown im Frühling 2020 führte die Projektgruppe eine Befragung zur damals sehr kurzfristig entstandenen Situation durch, in welcher die Schweizer Arbeitnehmerinnen und Arbeitnehmer gebeten wurden, möglichst zuhause zu bleiben. Die Resultate der Befragung zeigten, dass vor dem Lockdown jede/-r zehnte Mitarbeitende (10 %) hauptsächlich von zuhause aus gearbeitet hatte und sich diese Zahl während dem Lockdown auf rund zwei von fünf Mitarbeitenden (38 %) erhöhte. Nach dem ersten Lockdown ging der Anteil zurück, es blieben aber immer noch rund 16 Prozent der Mitarbeitenden im Homeoffice, was einer Steigerung an Homeoffice-Stellen von rund 60 Prozent entspricht.

Ein Jahr später und nach einer Homeoffice Pflicht vom 18. Januar bis 26. Juni 2021 (danach nur noch „Empfehlung“) stellt sich die Frage, wie sich die Einstellung zum Remote Working verändert hat und wie viele Stellen weiterhin von zuhause aus besetzt sind. Wie schon in der ersten Studie wurde ein spezieller Fokus auf Cybersicherheit gelegt, da digitales Arbeiten ausserhalb der Büro-Räumlichkeiten diesbezüglich zu zusätzlichen Herausforderungen führt. Zusätzlich wurden dieses Jahr neue Fragen zum Thema Datenschutz gestellt.

Die Projektgruppe besteht aus Mitarbeitenden von Die Mobiliar (Patric Vifian), digitalswitzerland (Andreas Kaelin), der Fachhochschule Nordweststschweiz 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 16. Juni bis 27. Juli 2021 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 repräsentatives Abbild der Grundgesamtheit, die Ergebnisse sind somit unter Berücksichtigung des Vertrauensintervalls auf die Grundgesamtheit extrapolierbar.

Die Stichprobengrösse von n=506 erlaubt eine proportionale Verteilung, d.h. die Firmengrössen wurden gemäss ihrem effektiven Anteil befragt. Die nachfolgende Tabelle zeigt die Verteilung der Interviews im Vergleich zur Verteilung der untersuchten Unternehmensgrössen in der Schweiz.

	Effektiver Anteil (BFS / STATENT 2017)	Proportionale Stichprobe: n = 506
Espace Mittelland	20%	101 (20%)
Genferseeregion	19%	98 (19%)
Zürich	16%	82 (16%)
Ostschweiz	14%	71 (14%)
Nordwestschweiz	12%	61 (12%)
Zentralschweiz	12%	60 (12%)
Tessin	6%	33 (7%)
4-9 Beschäftigte	66%	326 (64%)
10-19 Beschäftigte	22%	114 (23%)
20-49 Beschäftigte	12%	66 (13%)

Die Adressen stammen von einem Schweizer Adressbroker aus einem Potenzial von über 100'000 Adressen. Sie wurden nach Sektor, Region und Firmengrösse vorgeschichtet, die Quotierung erfolgt gemäss den am Telefon erhobenen Antworten (Firmengrösse).

Die Ausschöpfung litt unter Corona (Homeoffice, schlechte Erreichbarkeit) und liegt bei 3.7 Prozent, was für die Zielgruppe „Geschäftsführende" ein eher tiefer Wert ist.

Realisiert Interviews	**506**
Verweigerung	**13'033**
Termine	1'638
Keine Antwort	5'369
Besetzt	278
Anrufbeantworter	2'169
Quote Komplet/Nicht Zielgruppe	905
Fax/Geschäft/Nicht existent	1'740
nicht erreichbar während der Feldzeit	232
Sprachprobleme	57
Total	**25'927**

Ausschöpfung:
25'927 - Summe aller nicht-kontaktierten Adressen (12'388) = 13'539
506 / 13'539 = 3.7 %

Die Verteilung der Branchen pro Region entstand zufällig auf Basis vorgeschichteter Adressen und ist in der folgenden Tabelle abgebildet:

	Espace Mittel-land	Genfer-seere-gion	Zürich	Ost-schweiz	Nord-west-schweiz	Zentral-schweiz	Tessin	**Ge-samt**
Bau & Immobilien (n=95)	17%	24%	20%	23%	16%	18%	3%	**19%**
Produktion / verarbei-tendes Gewerbe (n=69)	14%	13%	12%	18%	10%	13%	15%	**14%**
Bildung, Gesundheit & Sozialwesen (n=28)	6%	2%	5%	11%	5%	8%	0%	**6%**
Dienstleistung (n=129)	27%	27%	27%	14%	31%	23%	33%	**25%**
ICT & Marketing (n=57)	7%	13%	15%	8%	16%	12%	6%	**11%**
Handel, Verkauf & Ser-vice (n=80)	18%	12%	13%	17%	15%	18%	21%	**16%**
Gastgewerbe (n=26)	6%	7%	2%	3%	2%	7%	12%	**5%**
Anderes (n=22)	6%	1%	6%	6%	5%	0%	9%	**4%**
Total n=506	**101**	**98**	**82**	**71**	**61**	**60**	**33**	**506**

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, welche aufgrund bestimmter Fragen gebildet wurden. 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.

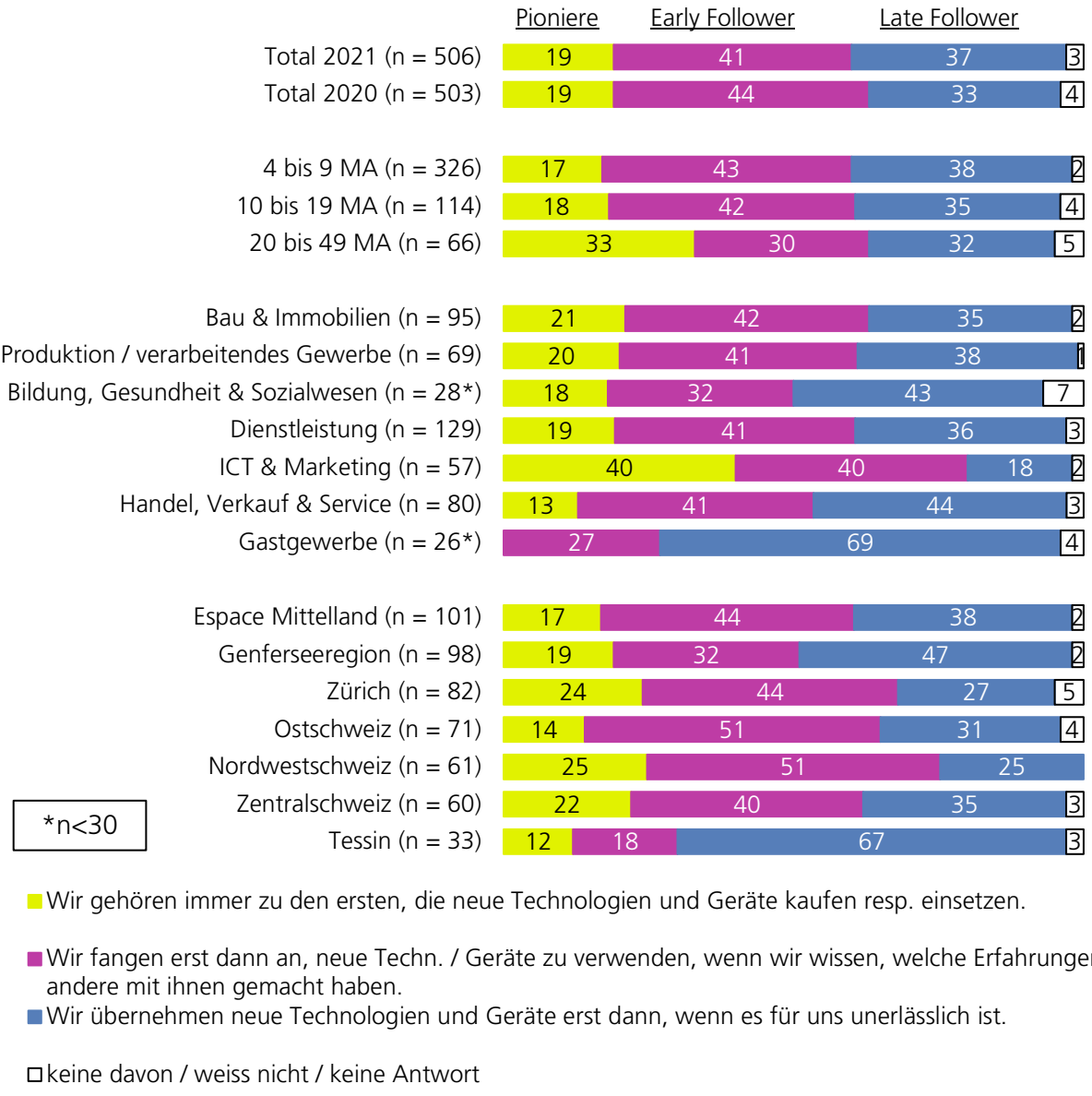
Je nach Antwort wurden die Befragten in die drei Subgruppen «Pioniere», «Early Follower» und «Late Follower» eingeteilt.

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

In die grösste Unternehmensklasse (20-49 Mitarbeitende) fallen deutlich mehr Pioniere (33 %) als in die mittlere (10-19 Mitarbeitende, 18 %) und in die kleinste Unternehmensklasse (4-9 Mitarbeitende, 17 %). Der Unterschied zwischen der grössten und kleinsten Unternehmensklasse ist signifikant.

Als besonders offen gegenüber neuen Technologien zeigt sich, wie schon 2020, die Branche ICT & Marketing mit 40 Prozent Pionieren. Am anderen Ende der Skala liegt das Gastgewerbe mit 69 Prozent Late Followern, gefolgt von den Branchen Handel, Verkauf & Service (44 %) und Bildung, Gesundheit & Sozialwesen (43 %).

Im Tessin bezeichnen sich besonders viele Befragte als Late Follower (67 %), dafür besonders wenige als Early Follower (12 %). Am häufigsten findet man die Gruppe der Pioniere in der Nordwestschweiz (25 %) und in Zürich (24 %)



3.1.2 Sicherheitsmassnahmenumsetzung

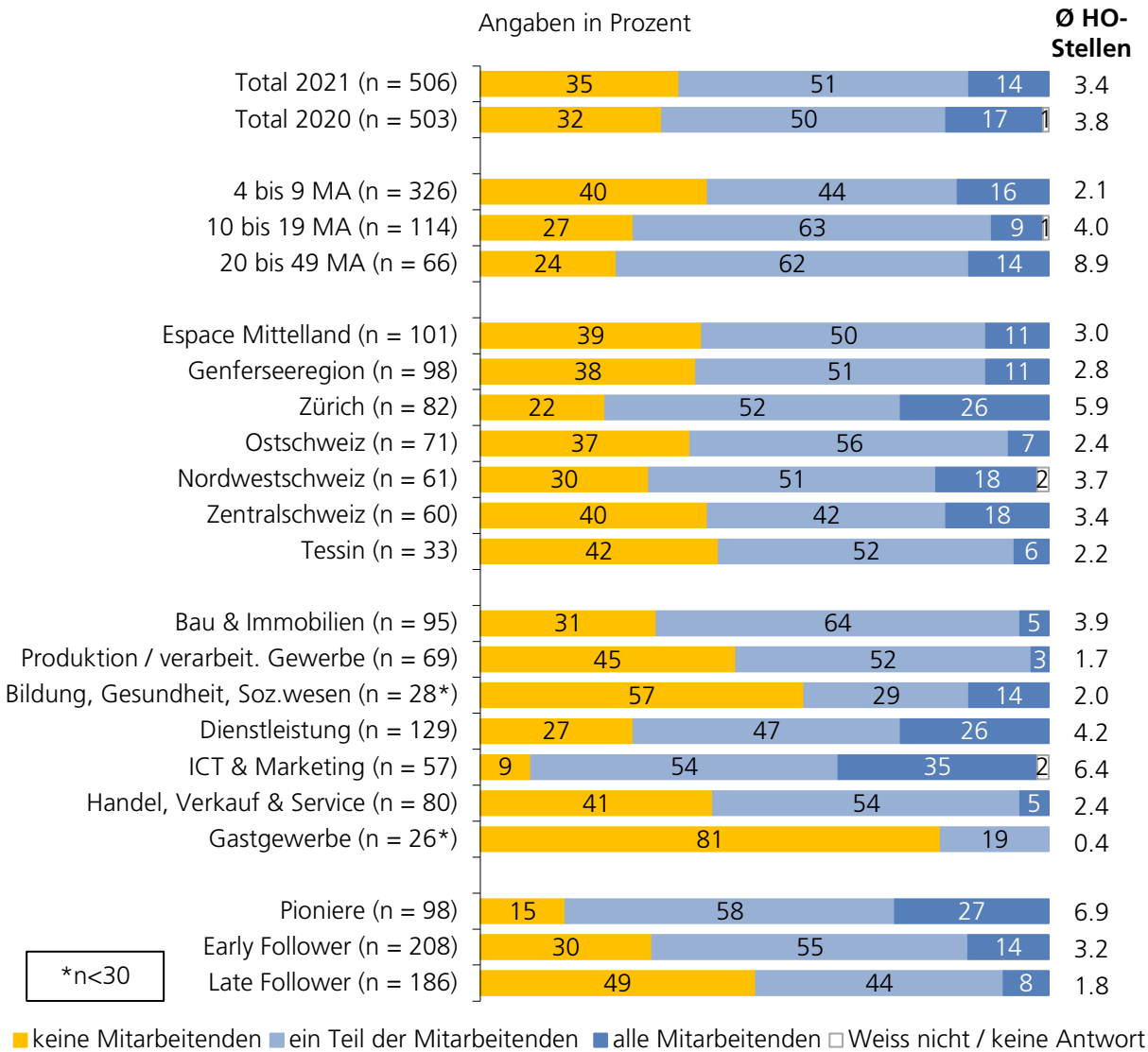
In den Fragen 12 und 13 (siehe Kapitel 3.3.5 und 3.3.6) werden verschiedene technische und organisatorische Sicherheitsmassnahmen nach deren Umsetzungsgrad auf einer Fünferskala abgefragt. Für die Bildung der Subgruppe wurde der Durchschnitt aller technischen bzw. organisatorischen Massnahmen berechnet: Durchschnittswerte von 1 bis 3 gelten als tiefe Massnahmenumsetzung, der Durchschnittswert 4 als mittlerer 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 = 506

Nicht jedes Unternehmen hat die gleichen Voraussetzungen, um den Mitarbeitenden Arbeiten im Homeoffice anzubieten. Wenn zum Beispiel persönlicher Kundenkontakt oder das Bedienen von Maschinen notwendig ist, müssen die Mitarbeitenden vor Ort sein. Das von den Firmen angegebene Potenzial an Homeoffice-Stellen hat sich seit 2020 nicht verändert: Rund ein Drittel der befragten Unternehmen (35 %) kann keine Mitarbeitenden ins Homeoffice schicken (2020: 32 %). Bei der Hälfte (51 %) kann ein Teil der Mitarbeiten von zuhause aus arbeiten (2020: 50 %) und bei rund jedem siebten kleinen Unternehmen können alle Mitarbeiter vom Homeoffice aus arbeiten (2021: 14 %, 2020: 17 %). Durchschnittlich gibt es 3.4 Homeoffice-fähige Stellen (2020: 3.8) bei den Schweizer KMU mit 4 bis 49 Mitarbeitenden.



Wie schon in der ersten Studie, ist die Branche ICT & Marketing am flexibelsten bezüglich Homeoffice: Bei 89 Prozent von ihnen kann zumindest ein Teil der Mitarbeitenden von zuhause aus arbeiten (2020: 87 %). Durchschnittlich bietet diese Branche 6.4 Homeoffice Stellen und liegt damit vor der Dienstleistungsbranche, bei welcher 73 Prozent zumindest ein Teil der Mitarbeitenden von zuhause arbeiten kann und welche durchschnittlich 4.2 Homeoffice Stellen bietet. Am wenigsten Homeoffice-Gelegenheiten bietet nachvollziehbarerweise das Gastgewerbe: 81 Prozent der Unternehmen dieser Branche bieten gar keine Homeoffice-Stellen, durchschnittlich sind es 0.4 Stellen.

Zwischen den Regionen finden sich keine signifikanten Unterschiede.

Je grösser die Firmen sind, desto eher können Homeoffice-Stellen angeboten werden. Dies lässt sich am einfachsten in der Antwortkategorie «keine Mitarbeitenden können theoretisch im Homeoffice arbeiten» ablesen: Bei Firmen mit 4 bis 9 Mitarbeitenden beträgt dieser Anteil 40 Prozent, bei Firmen mit 10 bis 19 Mitarbeitenden 27 Prozent und bei Firmen mit 20 bis 49 Mitarbeitenden 24 Prozent. In absoluten Zahlen bedeutet dies eine durchschnittliche Anzahl Homeoffice-Stellen von 2.1 bei 4 bis 9 Mitarbeitenden, von 4.0 bei 10 bis 19 Mitarbeitenden und 8.9 bei Unternehmen mit 20 bis 49 Mitarbeitenden.

Pioniere (85 % mit potenziellen Homeoffice-Stellen für zumindest einen Teil der Mitarbeitenden) und Early Follower (69 %) haben je signifikant häufiger die Möglichkeit, dass ihre Mitarbeitenden im Homeoffice arbeiten, als dies bei Late-Followern der Fall ist (52 %).

3.2.2 Technisch für das Homeoffice ausgerüstete Mitarbeitende

Frage 2:
Wie viele von Ihren Mitarbeitenden sind vollständig mit Hilfsmitteln für das Arbeiten von zuhause aus ausgerüstet, unabhängig davon, ob es sich um firmeneigene oder private Hilfsmittel handelt?
Basis: Total, n = 503

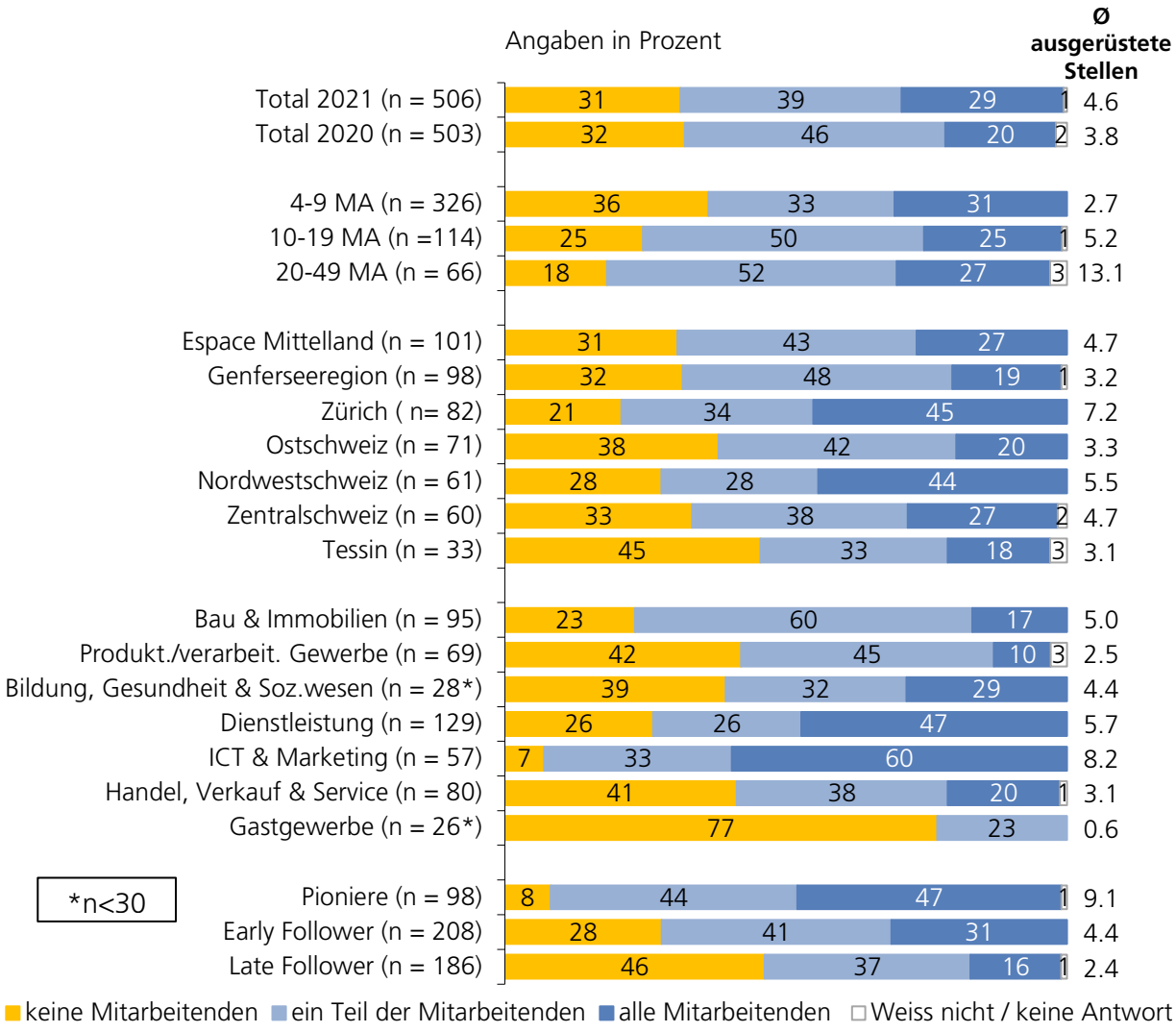
Während in der Studie von 2020 noch durchschnittlich 3.8 Arbeitnehmende technisch vollständig für das Arbeiten von zuhause aus ausgerüstet waren, sind es 2021 bereits 4.6 Arbeitnehmende. Bei mehr als einem Viertel (29 %) der befragten Unternehmen sind alle Mitarbeitenden vollständig ausgerüstet, 2020 lag dieser Anteil noch bei einem Fünftel (20 %). Bei rund zwei Fünfteln (39 %) ist ein Teil der Mitarbeitenden voll ausgerüstet (2020: 46 %) und bei rund einem Drittel (31 %) gar keine Mitarbeitenden (2020: 32 %).

Je grösser das Unternehmen ist, desto eher sind die Arbeitnehmenden für das Homeoffice ausgerüstet. Bei rund einem Drittel (36 %) der kleinsten befragten Unternehmenskategorie (4-9 Mitarbeitende) sind gar keine Mitarbeitenden für das Homeoffice ausgerüstet (10-19 Mitarbeitende: 25 %, 20-49 Mitarbeitende: 18 %).

Auch hier sind es die ICT & Marketing- sowie die Dienstleistungsbranche, die bezüglich Homeoffice am weitesten fortgeschritten sind. 60 Prozent der befragten Unternehmen aus der ICT & Marketing-Branche sowie 47 Prozent der Dienstleistungsbranche haben alle ihre Mitarbeitenden

vollständig für das Arbeiten von zuhause aus ausgerüstet. Hingegen sind bei 77 Prozent der Unternehmen aus dem Gastgewerbe gar keine Mitarbeitende für das Homeoffice ausgerüstet.

In der Nordwestschweiz (44 % «alle Mitarbeitenden») und der Region Zürich (45 %) sind signifikant mehr Mitarbeitende für das Homeoffice ausgerüstet als in der Genferseeregion (19 %) und in der Ostschweiz (20 %). Ausserdem gilt: Je innovationsfreudiger die Befragten sind, desto eher sind die Mitarbeitenden für das Homeoffice ausgerüstet (Pioniere: 47 % «alle», Early Follower: 31 %, Late Follower: 16 %). Auch diese Unterschiede sind signifikant.



3.2.3 Potenzialausschöpfung

Die Potenzialausschöpfung basiert auf einem Vergleich der Fragen 1 und 2. Dabei wird verglichen, wie gross der Anteil der Mitarbeitenden ist, die theoretisch im Homeoffice arbeiten könnten und wie gross jener der Mitarbeitenden ist, die vollständig für das Homeoffice ausgestattet sind. Bei allen Subgruppen bis auf einer zeigt sich eine Potenzialüberschreitung. Das heisst, dass mehr Personen für das Homeoffice ausgestattet sind, als tatsächlich im Homeoffice arbeiten könnten. Bei einer Potenzialunterschreitung ist der Anteil Personen, die im Homeoffice arbeiten könnten, grös-

ser, als jener der Personen, die dafür ausgestattet sind. Dies ist nur bei den befragten Unternehmen der Fall, bei denen theoretisch alle Mitarbeitenden von zuhause aus arbeiten könnten (aber «nur» 95 % dafür ausgerüstet sind).

	F1: Potenzial Homeoffice (Anteil MA, die theor. im HO arbeiten könnten) *Angaben in Prozent*	F2: Anteil für das Homeoffice ausgerüstete MA **2020** *Angaben in Prozent*	F2: Anteil für das Homeoffice ausgerüstete MA **2021** *Angaben in Prozent*	Differenz (technische Potenzialausschöpfung)	Steigerung ggü. 2020 in Prozentpunkten
Keine Mitarbeitende (n = 176)	0 %	7 %	12 %	überschritten	5 %
Teil der Mitarbeit. (n = 257)	37 %	37 %	51 %	überschritten	14 %
Alle Mitarbeitenden (n = 72)	100 %	92 %	95 %	unterschritten	3 %
Espace Mittelland (n = 101)	26 %	35 %	41 %	überschritten	6 %
Genferseeregion (n = 98)	30 %	31 %	36 %	überschritten	5 %
Zürich (n = 80)	49 %	41 %	60 %	überschritten	19 %
Ostschweiz (n = 71)	25 %	36 %	34 %	überschritten	-2 %
Nordwestschweiz (n = 61)	38 %	40 %	56 %	überschritten	16 %
Zentralschweiz (n = 60)	36 %	46 %	44 %	überschritten	-2 %
Tessin (n = 33)	23 %	30 %	32 %	überschritten	2 %
Bau & Immobilien (n = 95)	28 %	31 %	39 %	überschritten	8 %
Produktion / verarbeitendes Gewerbe (n = 69)	15 %	21 %	22 %	überschritten	1 %
Bildung, Gesundheit & Sozialwesen (n = 28*)	25 %	27 %	39 %	überschritten	12 %
Dienstleistung (n = 129)	47 %	57 %	59 %	überschritten	2 %
ICT & Marketing (n = 57)	62 %	78 %	78 %	überschritten	0 %
Handel, Verkauf & Service (n = 80)	23 %	33 %	33 %	überschritten	0 %
Gastgewerbe (n = 26*)	3 %	5 %	5 %	überschritten	0 %
Pioniere (n = 98)	51 %	48 %	68 %	überschritten	20 %
Early Follower (n = 208)	35 %	44 %	46 %	überschritten	2 %
Late Follower (n = 186)	21 %	23 %	29 %	überschritten	6 %

Offenbar wurden also auch viele Mitarbeitende für das Homeoffice ausgerüstet, obwohl sie vor Ort arbeiten. Es kann sein, dass zukünftig mehr Homeoffice-Arbeit oder eine weitere Homeoffice-Pflicht erwartet wird und deshalb vorsorglich schon mehr Mitarbeitende entsprechend ausgerüstet werden. Es ist aber auch möglich, dass aufgrund der Corona-Massnahmen mehr Mitarbeitende im Homeoffice gearbeitet haben, als dies im Normalzustand möglich oder gewünscht gewesen wäre, und diese Mitarbeitenden deshalb ausgerüstet werden mussten.

Die Gesamtzahl technisch voll ausgerüsteter Mitarbeitenden ist in fast jeder Subgruppe gestiegen. Gesunken ist die Anzahl in der Ost- und Zentralschweiz (je -2 %), unverändert blieb sie in den

Branchen ICT & Marketing, Gastgewerbe sowie Handel, Verkauf & Service (je 0 %). Besonders hoch ist die Steigerung in Zürich (+19 %) und der Nordwestschweiz (+16 %) sowie beim Innovationstyp «Pioniere» (+20 %).

3.2.3 Veränderung Homeoffice Gewohnheiten während Homeoffice-Pflicht

Gemäss der ersten Durchführung dieser Studie im Jahr 2020 war vor der Pandemie jede/-r zehnte Mitarbeitende (10 %) der kleinen Unternehmen hauptsächlich im Homeoffice tätig. Diese Anzahl hat sich aufgrund des Corona-Lockdowns im Frühling 2020 um rund die Hälfte auf 16 % nach dem Lockdown erhöht.

Frage 3:

a) Wie viele Ihrer Mitarbeiter haben seit anfangs 2021 **hauptsächlich** von zuhause aus gearbeitet, also währenddem die Homeoffice-Pflicht galt?
b) 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 = 329

2021 wurde zum Zeitpunkt der Befragung gerade die aufgrund der dritten Covid-Welle verordnete Homeoffice-*Pflicht* (18. Januar bis 26. Juni 2021) zu einer *Empfehlung* abgeschwächt. Während in der ersten Welle noch viele KMU durch die Covid-Massnahmen überrumpelt gewesen sein dürften, dürfte 2021 eine gewisse Gewöhnung an das Arbeiten von zuhause eingetreten sein. Zudem ist anzunehmen, dass während der ersten Studie 2020 noch viele von einer wenige Monate andauernden Krise ausgingen. Während der zweiten Befragung dauerte die Ausnahmesituation schon fast eineinhalb Jahre an, was ebenfalls eine Veränderung der grundsätzlichen Einstellung zur Krise und den Massnahmen zur Folge haben dürfte.

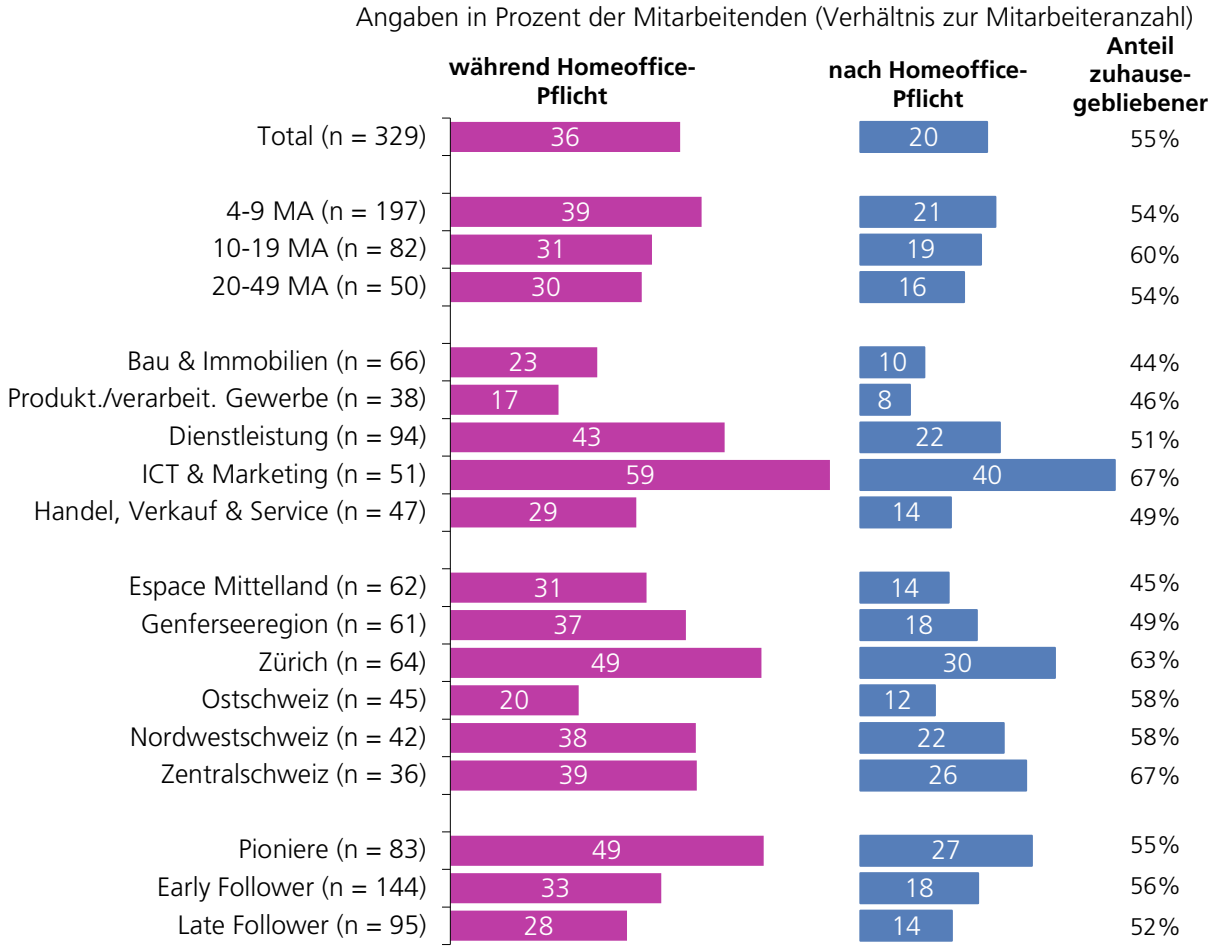
Während der Homeoffice-Pflicht waren gemäss Befragung rund ein Drittel (36 %) der Mitarbeitenden hauptsächlich im Homeoffice. Dies entspricht fast exakt der Zahl aus der Lockdown-Situation in der 2020er Studie (38 %). Nach Beendigung der Homeoffice-Pflicht (es galt immer noch die Empfehlung) blieb ein Fünftel (20 %) zuhause zum Arbeiten (2020: 16 %). Also kehrte etwas mehr als die Hälfte (55 %) der Homeoffice-Mitarbeitenden an den Arbeitsplatz zurück.

In der kleinsten und mittleren Unternehmenskategorie (4-9 bzw. 10-19 Mitarbeitende) arbeitete nach der Homeoffice-Pflicht trotzdem noch rund jeder fünfte Mitarbeitende (21 % bzw. 19 %) weiterhin von zuhause aus. In der grössten Kategorie (20-49 Mitarbeitende) sind es mit 16 % etwas weniger.

In der Branche ICT & Marketing (40 %) blieb der Homeoffice-Anteil nach der Pflicht deutlich höher als in den anderen Branchen; der Unterschied ist signifikant gegenüber Bau & Immobilien (10 %), Produktion & verarbeitendes Gewerbe (8 %), Dienstleistungen (22 %) und Handel, Verkauf & Service (14 %).

Im Raum Zürich blieb während der Homeoffice-Pflicht fast die Hälfte (49 %) der Arbeitnehmenden zuhause, danach immerhin noch 30 %. Zürich ist somit die Homeoffice-freudigste Region, gefolgt von der Zentralschweiz, wo während der Pflicht-Phase rund zwei Fünftel (39 %) zuhause blieben, danach noch rund ein Viertel (26 %). In der Ostschweiz hingegen blieben während der Homeoffice-Pflicht nur ein Fünftel der Mitarbeitenden (20 %) zuhause, danach noch rund jeder Zehnte (12 %); die Ostschweiz unterscheidet sich damit signifikant von Zürich. Auch im Espace Mittelland sind signifikant weniger Mitarbeitende im Homeoffice geblieben (14 %) als in Zürich.

Je aufgeschlossener die befragten Geschäftsführenden ihr Unternehmen bezüglich technischer Neuerungen bezeichnen, desto eher haben die Mitarbeitenden im Homeoffice gearbeitet. Bei den Pionieren war es während der Homeoffice-Pflicht fast die Hälfte (49 %), bei den Early-Followern rund ein Drittel (33 %) und bei den Late Followern rund ein Viertel (28 %). Nach der Pflicht reduzierte sich die Anzahl in allen drei Gruppen um rund die Hälfte auf 27 % bei den Pionieren, 18 % bei den Early Followern und 14 % bei den Late Followern.



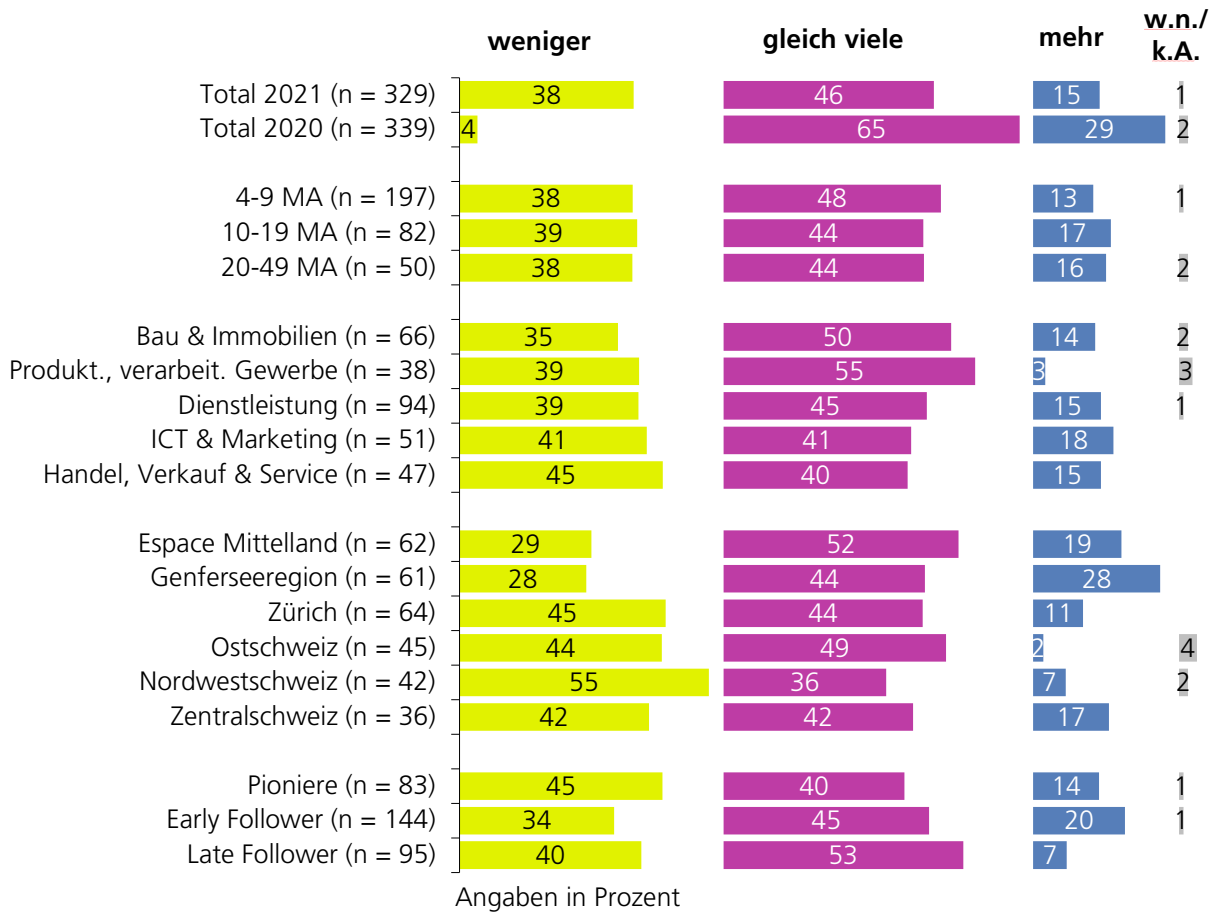
3.2.4 Einschätzung der Entwicklung der Homeoffice Arbeitsplätze

In der Vorjahresstudie 2020 war noch eine überwiegende Mehrheit der Meinung, dass zukünftig mindestens gleich viele Mitarbeitende im Homeoffice arbeiten würden wie während dem Lockdown im Frühling 2020 (65 % «gleich viele», 29 % «mehr»). Diese Einstellung hat sich 2021 deutlich geändert: Über ein Drittel der Befragten (38 %) ist der Meinung, dass zukünftig weniger Mitarbeitende im Homeoffice arbeiten werden als während der Pandemie (2020: 4 %). Knapp die Hälfte (46 %) geht davon aus, dass es etwa gleich viele sein werden, nur 15 % denken, dass es mehr sein werden.

Frage 4:
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 = 329

Die verschiedenen Unternehmensgrössenkategorien beantworten diese Frage alle fast gleich. Zwischen den Branchen und Regionen gibt es einige wenige, aber nicht signifikante Unterschiede:

Die in der vorherigen Frage am Homeoffice-freudigsten Subgruppen ICT & Marketing und Grossregion Zürich rechnen zu je rund zwei Fünfteln mit rückläufigen Homeoffice-Anteilen (ICT & Marketing: 41 %, Zürich: 45 %). Ebenfalls je rund zwei Fünftel dieser Subgruppen gehen von gleichbleibenden Homeoffice-Zahlen aus (ICT & Marketing: 41 %, Zürich: 44 %). Nur rund ein Fünftel (18 %) der ICT & Marketingbranche bzw. rund ein Zehntel (11 %) der befragten Zürcher Unternehmen erwartet steigende Homeoffice-Zahlen.



Die Branche Produktion & verarbeitendes Gewerbe erwartet besonders wenige Mitarbeitende im Homeoffice: Nur 3 Prozent geben an, dass zukünftig mehr Mitarbeitende von zuhause aus arbeiten werden als während der Pandemie. In den Branchen Bau & Immobilien, Dienstleistung, ICT & Marketing sowie Handel, Verkauf & Service liegt dieser Wert zwischen 14 und 18 Prozent.

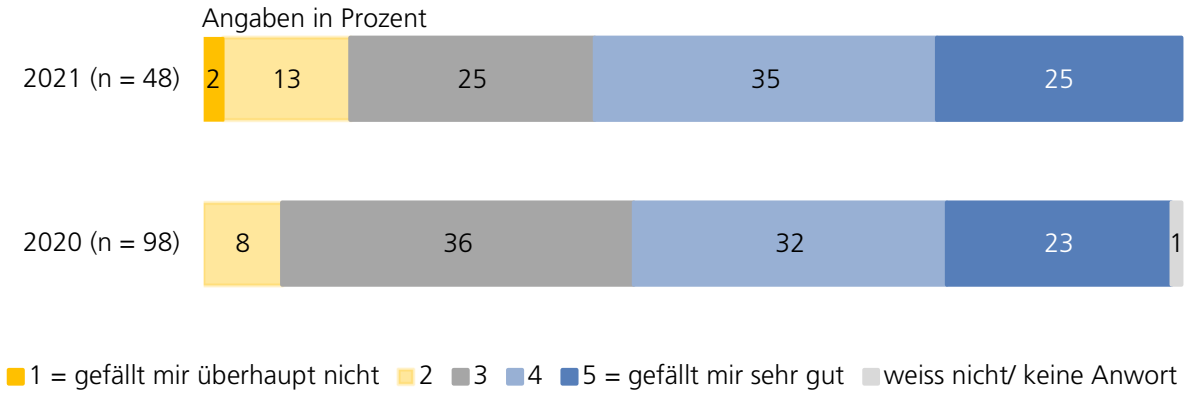
Die Genferseeregion, in der vorherigen Frage noch im Mittelfeld bezüglich des Anteils an Homeoffice-Stellen, schätzt die Zukunft Homeoffice-lastiger ein als die anderen Regionen. Mehr als ein Viertel der Befragten aus dieser Region (28 %) rechnet mit mehr Homeoffice-Stellen als während der Pandemie (Espace Mittelland: 19 %, Zentralschweiz: 17 %, Zürich: 11 %, Nordwestschweiz: 7 %, Ostschweiz: 2 %, der Unterschied zwischen der Genferseeregion und der Ostschweiz ist signifikant).

3.2.6 Einstellung zu den Veränderungen bezüglich Homeoffice

Frage 5:
Wie gefällt Ihnen persönlich diese Entwicklung?
Filter: Wenn gemäss F5 langfristig **mehr** Mitarbeitende im Homeoffice arbeiten werden, n = 98

Drei Fünftel der Befragten (60 %), welche eine Steigerung der Homeoffice Arbeitsplätze erwarten, sagen, dass ihnen dies eher oder sehr gut gefällt (Skalenwerte 4 und 5 auf einer Fünferskala). Vor einem Jahr waren das noch etwas weniger (55 %, + 5 Prozentpunkte). Aber auch am anderen Ende der Skala ergaben sich mehr Nennungen: 2 Prozent der Befragten sagen, dass ihnen die Entwicklung überhaupt nicht gefällt (Skalenwert 1) und rund jeder Achte gibt den Skalenwert 2 an (13 %). Damit ist auch die Summe der beiden negativen Bewertungen von 8 Prozent in der Vorstudie auf 15 Prozent in der aktuellen Studie leicht gestiegen (+ 7 Prozentpunkte).

Die Werte sind somit im Vergleich zur Vorstudie vom mittleren, unbestimmten Skalenwert 3 nach unten oder nach oben gerutscht (2020: 36 %, 2021: 25 %), die Meinungen scheinen sich zu akzentuieren. Der Mittelwert liegt, genau wie in der Vorstudie, bei 3.7 auf der Fünferskala.

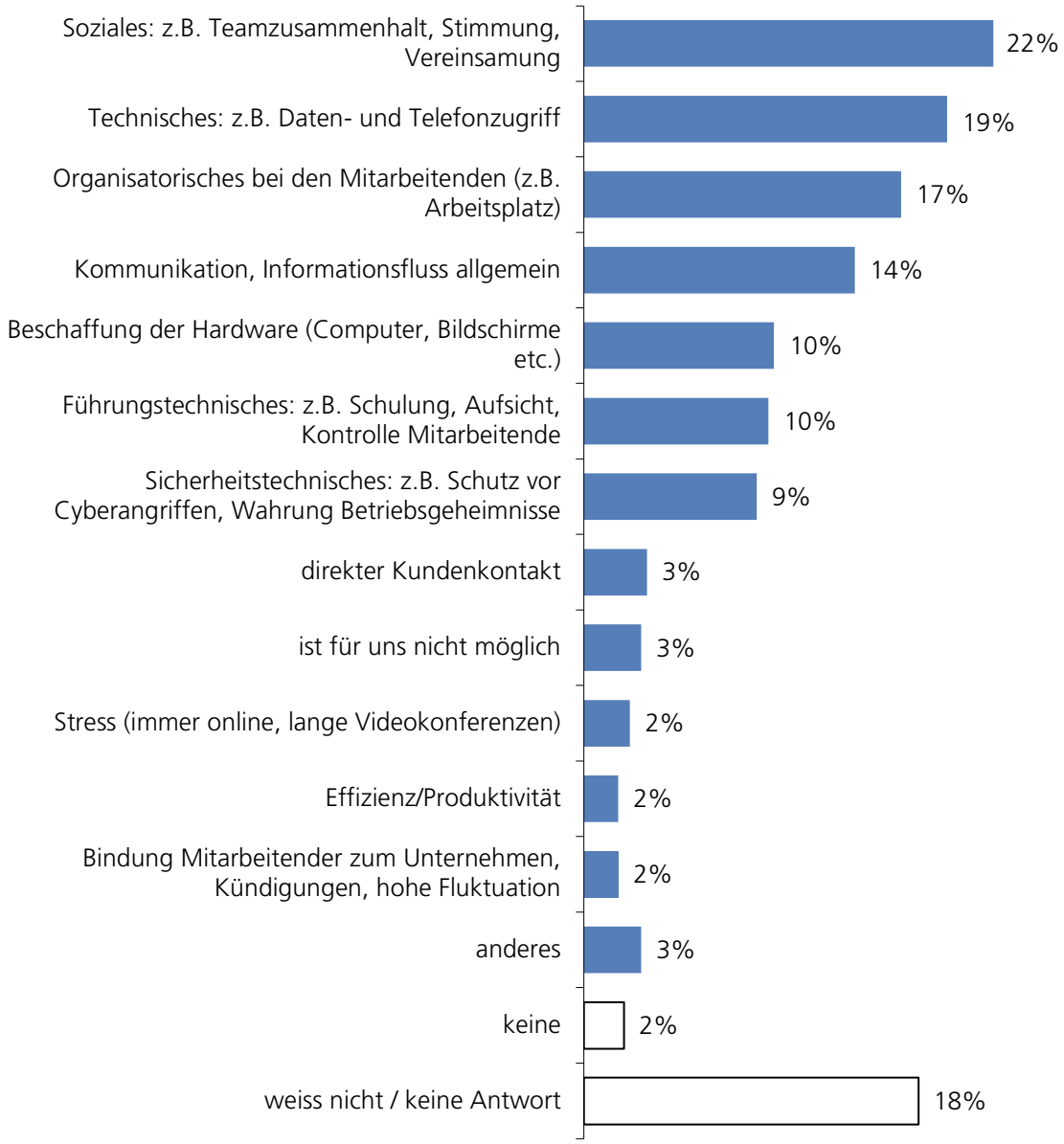


3.2.7 Grösste Herausforderungen bei der Umstellung auf Homeoffice

Soziale Faktoren wie der Teamzusammenhalt, die Stimmung unter den Mitarbeitenden oder auch die drohende Vereinsamung im Homeoffice werden am häufigsten (22 %) genannt, wenn es um die grössten Herausforderungen für ein Unternehmen bei der Umstellung auf Homeoffice geht. Am zweithäufigsten (19 %) werden die notwendigen technischen Lösungen wie Daten- und Telefonzugriff erwähnt.

Frage 6:
Was sind aus unternehmerischer Sicht die grössten Herausforderungen bei der Umsetzung des Homeoffice?
Filter: Wenn mindestens ein/e Mitarbeiter/in theoretisch im Homeoffice arbeiten kann, n = 329

Mit durchschnittlich 1.53 Antworten können Befragte aus der Bau- & Immobilienbranche die meisten Herausforderungen aufzählen. Befragte aus den Branchen Dienstleistung (1.31), Handel, Verkauf & Service (1.36) und ICT & Marketing (1.37) nennen etwas weniger Herausforderungen. Die Art der Probleme ist aber in allen Branchen sehr ähnlich, diesbezüglich gibt es kaum Unterschiede.



Die kleinsten Unternehmen (4-9 Mitarbeitende) nennen im Durchschnitt 1.33 Herausforderungen, die mittleren (10-19 Mitarbeitende) 1.35 und die grössten (20-49 Mitarbeitende) 1.48. Auch hier gibt es keine signifikanten Unterschiede zwischen den Gruppen. Die grösste Unternehmenskategorie (20-49 Mitarbeitende) erwähnt die Hardware-Beschaffung etwas seltener (6 %) als die anderen beiden Grössenkategorien (4-9 Mitarbeitende: 11 %, 10-19 Mitarbeitende: 10 %). Umgekehrt scheinen führungstechnische Herausforderungen für kleinere Unternehmen seltener ein Problem zu sein (4-9 Mitarbeitende: 8 %, 10-19 Mitarbeitende: 10 %) als für die grösste Kategorie (20-49 Mitarbeitende: 18 %).

Geschäftsführende, bei denen nach der Homeoffice-Pflicht die Mitarbeitenden mehrheitlich wieder zurück zum Arbeitsplatz gingen, erwähnen deutlich mehr Herausforderungen (durchschnittlich 1.50) als Geschäftsführende, bei denen nach der Homeoffice-Pflicht gleich viele Mitarbeitende von zuhause aus arbeiteten wie währenddessen (1.24). Signifikant ist der Unterschied bei den organisatorischen Herausforderungen seitens Mitarbeitenden: Erstere nannten diesen Punkt zu 22 Prozent, letztere nur zu 11 Prozent.

3.2.8 Nutzung digitaler Kommunikationsmittel

Telefon (95 %) und E-Mail (92 %) sind die am häufigsten verwendeten Kommunikationsmittel der befragten Unternehmen.

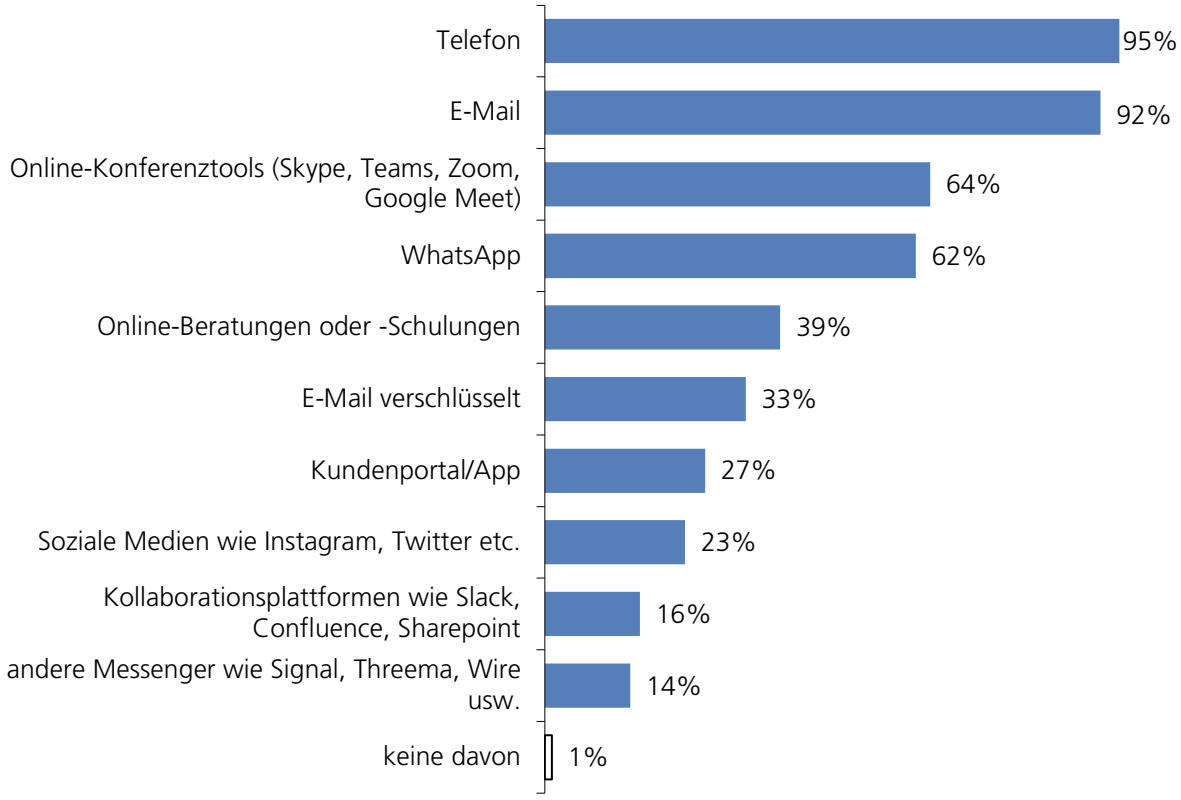
Frage 7:
Ich lese Ihnen jetzt einige digitale Kommunikationsmittel vor. Welche davon nutzen Ihre Mitarbeitenden aktuell für Partner, Kundschaft und anderen Mitarbeitende?
Basis: Total, n = 506, geschlossene Frage, Mehrfachnennungen möglich

Da die Antwortkategorien dieser Frage gegenüber 2020 leicht verändert wurden, ist der direkte Vergleich nicht in allen Kategorien möglich. Auffallend ist aber, dass die in diesem Jahr an dritter Stelle genannten Online-Konferenztools wie Skype, Teams, Zoom oder Google Meet deutlich häufiger genannt wurden (64 %) als noch 2020 (46 %). Besonders häufig werden die Online-Konferenztools in der ICT & Marketing-Branche verwendet (88 %), der Wert liegt signifikant höher als bei fast allen anderen Branchen (Bau & Immobilien: 63 %, Produktion & verarbeitendes Gewerbe: 62 %, Dienstleistungen: 65 %, Handel, Verkauf & Service: 58 %, Gastgewerbe: 15 %).

WhatsApp wurde in der aktuellen Studie bewusst einzeln abgefragt, während 2020 noch nach *WhatsApp oder andere Messenger* gefragt wurde. Diese Änderung wurde vorgenommen, weil WhatsApp zwischen den beiden Befragungen die Datenschutzrichtlinien änderte und die Nutzer zwang, diese Richtlinien anzunehmen, um die App weiter zu nutzen. Dies führte zu hohen Download-Raten bei anderen Messenger-Apps. Mit der Frage-Änderung sollten diese unterschieden werden können. In der Befragung gaben nun fast zwei Drittel (62 %) der befragten Unternehmen an, WhatsApp für die Kommunikation mit Partnern, Kundschaft und anderen Mitarbeitenden zu nutzen. Damit liegt WhatsApp auf Platz 4 der abgefragten Kommunikationsmittel. Andere Messenger wie Signal, Threema oder Wire werden von rund jedem achten Unternehmen (14 %) genannt und liegen auf dem letzten Platz der Kommunikationsmittel. In der letztjährigen Studie wurde WhatsApp oder andere Messenger von 55 Prozent der befragten Unternehmen genannt.

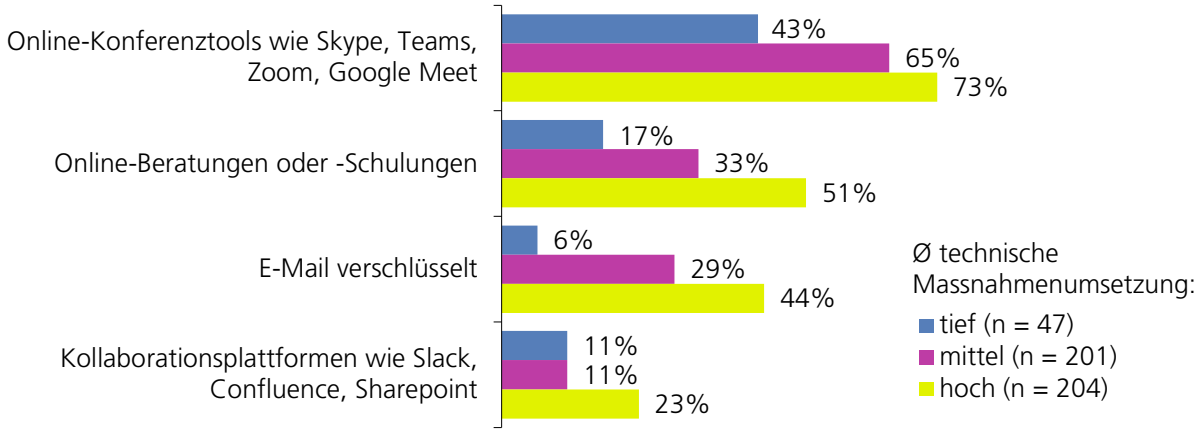
Auch Online-Beratungen oder -Schulungen nahmen in der Nutzung zu. Wurden sie 2020 noch von einem Fünftel (20 %) der Befragten genannt, so sind es 2021 bereits fast zwei Fünftel (39 %).

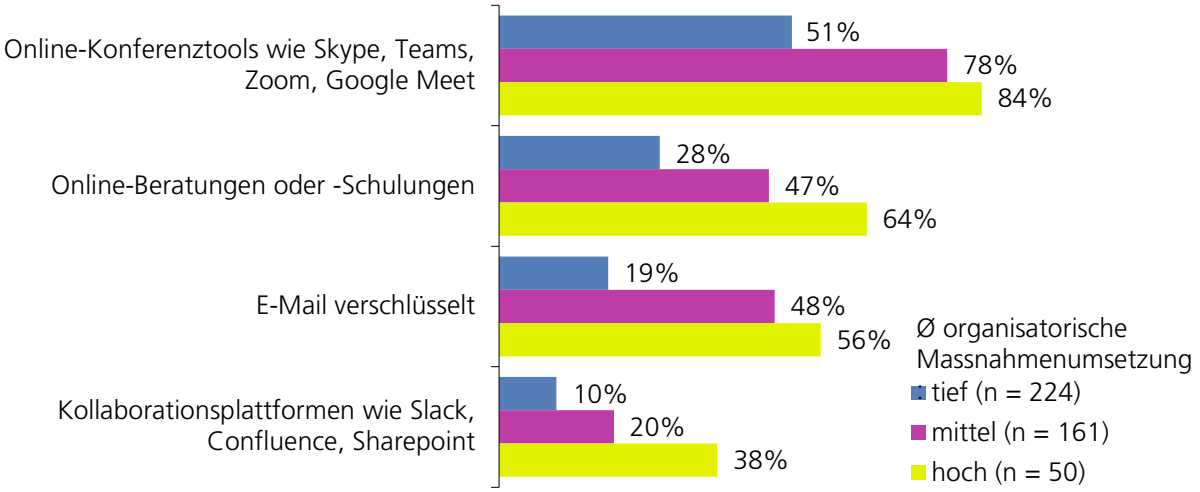
Kollaborationstools wie Slack, Confluence oder Sharepoint wurden in der 2020er Studie noch nicht abgefragt. Rund jedes sechste Unternehmen (16 %) nennt sie als Kommunikationsmittel für Kunden, Partner oder Mitarbeitende. Dabei ist – wie schon bei den Online-Konferenztools – die ICT und Marketingbranche die häufigste Verwenderin: Etwas mehr als zwei Fünftel (44 %) dieser Branche nutzen Kollaborationstools, das sind signifikant mehr als in den meisten anderen Branchen (Bau & Immobilien: 7 %, Produktion & verarbeitendes Gewerbe: 12 %, Dienstleistungen: 12 %, Handel, Verkauf & Service: 15 %, Gastgewerbe: 8 %).



Zwischen den Unternehmensgrössenkategorien ergeben sich nur wenige signifikante Unterschiede. Grundsätzlich nennt die kleinste Kategorie (4-9 Mitarbeitende) deutlich weniger Kommunikationsmittel (4.46) als die mittlere und die grösste Kategorie (10-19 Mitarbeitende: 5.04, 20-49 Mitarbeitende: 5.08). Signifikant ist der Unterschied bei den Online-Konferenztools und den Kundenportalen/Apps: Online-Konferenztools werden von 59 Prozent der kleinsten befragten Unternehmen (4-9 Mitarbeitende) genutzt, aber von 76 Prozent der grössten befragten Unternehmen (20-49 Mitarbeitende). Die mittlere Kategorie (10-19 Mitarbeitende) liegt mit 71 Prozent dazwischen. Der Wert der kleinsten und mittleren Unternehmen (4-9 und 10-19 Mitarbeitende) bei den Kundenportalen/Apps liegt bei je 25 Prozent, bei den grössten Unternehmen (20-49 Mitarbeitende) bei 39 Prozent.

Firmen mit einer durchschnittlich höheren technischen und organisatorischen Massnahmenumsetzung geben signifikant häufiger an, Online-Konferenztools, Online-Beratungen, verschlüsselte E-Mails oder Kollaborationstools zu nutzen.





3.3 Cybersicherheit

3.3.1 Outsourcen von IT-Arbeiten

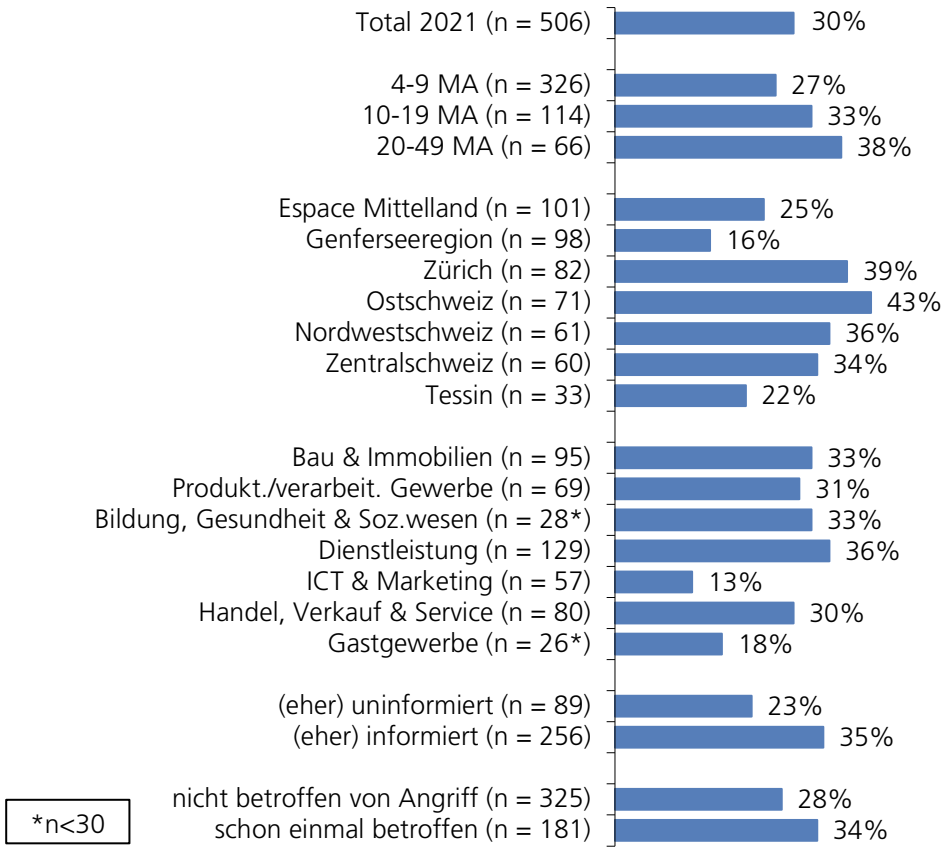
Durchschnittlich wird knapp ein Drittel (30 %) der IT-Arbeiten von den befragten Unternehmen an externe Dienstleister vergeben.

Frage 8:
Wieviel Prozent der IT-Arbeiten werden bei Ihnen ungefähr von externen Dienstleistern wahrgenommen?
Basis: Total, n = 506

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 (27 %) der IT-Arbeiten, bei den mittleren Kategorie (10-19 Mitarbeitende) rund ein Drittel (33 %) und bei der grössten Kategorie (20-49 Mitarbeitende) fast zwei Fünftel (38 %). Die Unterschiede sind nicht signifikant.

Verglichen mit der Ostschweiz (43 %), Zürich (39 %) und der Nordwestschweiz (36 %), wo am fleissigsten outgesourct wird, liegt der Outsource-Anteil in der Genferseeregion (16 %) signifikant zurück. Das Tessin (22 %), Espace Mittelland (25 %) und die Zentralschweiz (34 %) liegen mit ihren Werten dazwischen.

Unternehmen, in denen keine Arbeiten vom Homeoffice aus erledigt werden können, geben signifikant weniger IT-Arbeiten auswärts (20 %) als Unternehmen, in welchen ein Teil (35 %) oder alle Stellen (37 %) vom Homeoffice besetzt werden können. Ausserdem geben diejenigen Geschäftsführenden, die sich bezüglich Cyberrisiken eher oder sehr uninformiert fühlen, ihre IT-Arbeiten signifikant seltener auswärts (23 %) als diejenigen, die sich eher oder sehr gut informiert fühlen (35 %)



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 mehr als einen Drittel (35 %). Ein ähnliches Bild ergibt sich bei den organisatorischen Massnahmen: Unternehmen mit tiefer organisatorischer Massnahmenumsetzung haben einen Viertel (25 %) der IT-Arbeiten einem externen Dienstleister gegeben, Unternehmen mit hoher organisatorischer Massnahmenumsetzung mehr als zwei Fünftel (42 %).

3.3.2 Gefühlter Informationsgrad zur Cyberrisk-Thematik

Frage 9:
Ganz allgemein: wie gut fühlen Sie sich persönlich in der Cyberrisk-Thematik informiert?
Basis: Total, n = 506

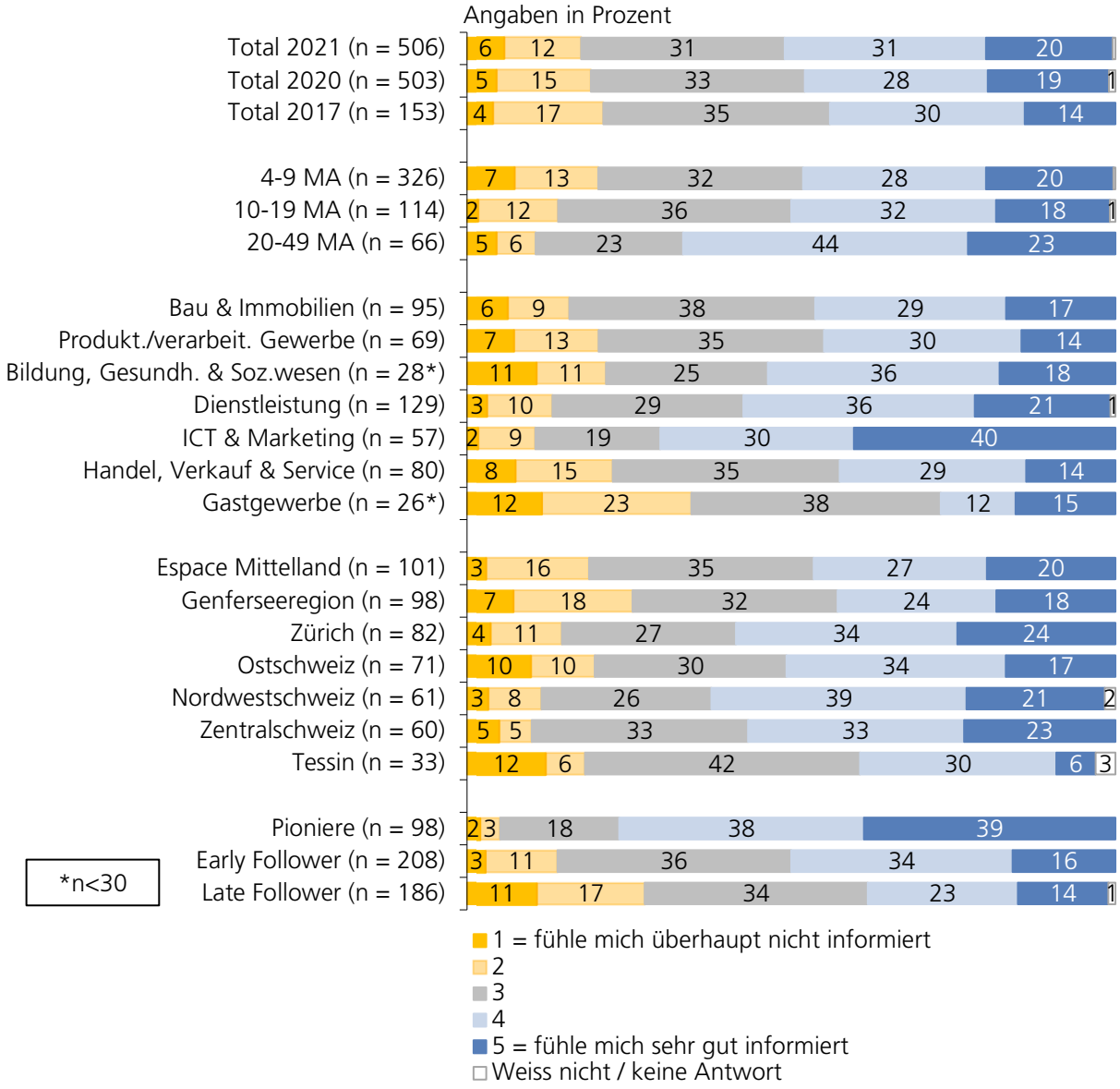
Die Einschätzung der persönlichen Informiertheit bezüglich Cyberrisiken hat sich gegenüber den Vorstudien nur minimal verändert: 2021 schätzt sich rund die Hälfte (51 %) als sehr oder eher informiert ein (Skalenwerte 4 und 5), 2020 waren dies mit 47 Prozent fast gleich viel, 2017 mit 44 Prozent noch etwas weniger. Auch seitens der sich (eher) uninformiert Fühlenden (Skalenwerte 1-2) zeigen sich kaum Unterschiede: Bezeichnen sich 2021 knapp zwei Fünftel (18 %) als eher bis sehr uninformiert, waren es 2020 genau ein Fünftel (20 %) und 2017 mit 21 Prozent ebenfalls rund ein Fünftel.

Je grösser das Unternehmen ist, desto informierter fühlen sich deren Geschäftsführenden. Die Unterschiede sind jedoch wie schon im letzten Jahr nicht signifikant: Knapp die Hälfte (48 %) der kleinsten Kategorie (4-9 Mitarbeitende), genau die Hälfte (50 %) der mittleren Kategorie (10-19 Mitarbeitende) und rund zwei Drittel (67 %) der grössten Kategorie (20-49 Mitarbeitende) fühlen sich eher bis sehr gut informiert.

Besonders hoch ist, wie schon 2020, die Einschätzung der Branche ICT & Marketing: Ihr Mittelwert von 4.0 (auf einer Fünferskala) weicht signifikant ab von den Branchen Produktion & verarbeitendes Gewerbe (3.3), Handel, Verkauf & Service (3.3) und Gastgewerbe (3.0)

Zwischen den Regionen gibt es keine signifikanten Abweichungen.

Je aufgeschlossener die Unternehmen gegenüber technischen Innovationen sind, desto besser fühlen sich die Geschäftsführenden auch zu Cyberrisiken informiert: Bei den Pionieren sind es 77 Prozent, die sich (eher) gut informiert fühlen, bei den Early Followern 50 Prozent, bei den Late Followern 37 Prozent. Die Pioniere weichen damit signifikant von den Early und Late Followern ab, auch der Unterschied zwischen den Early und Late Followern ist signifikant.



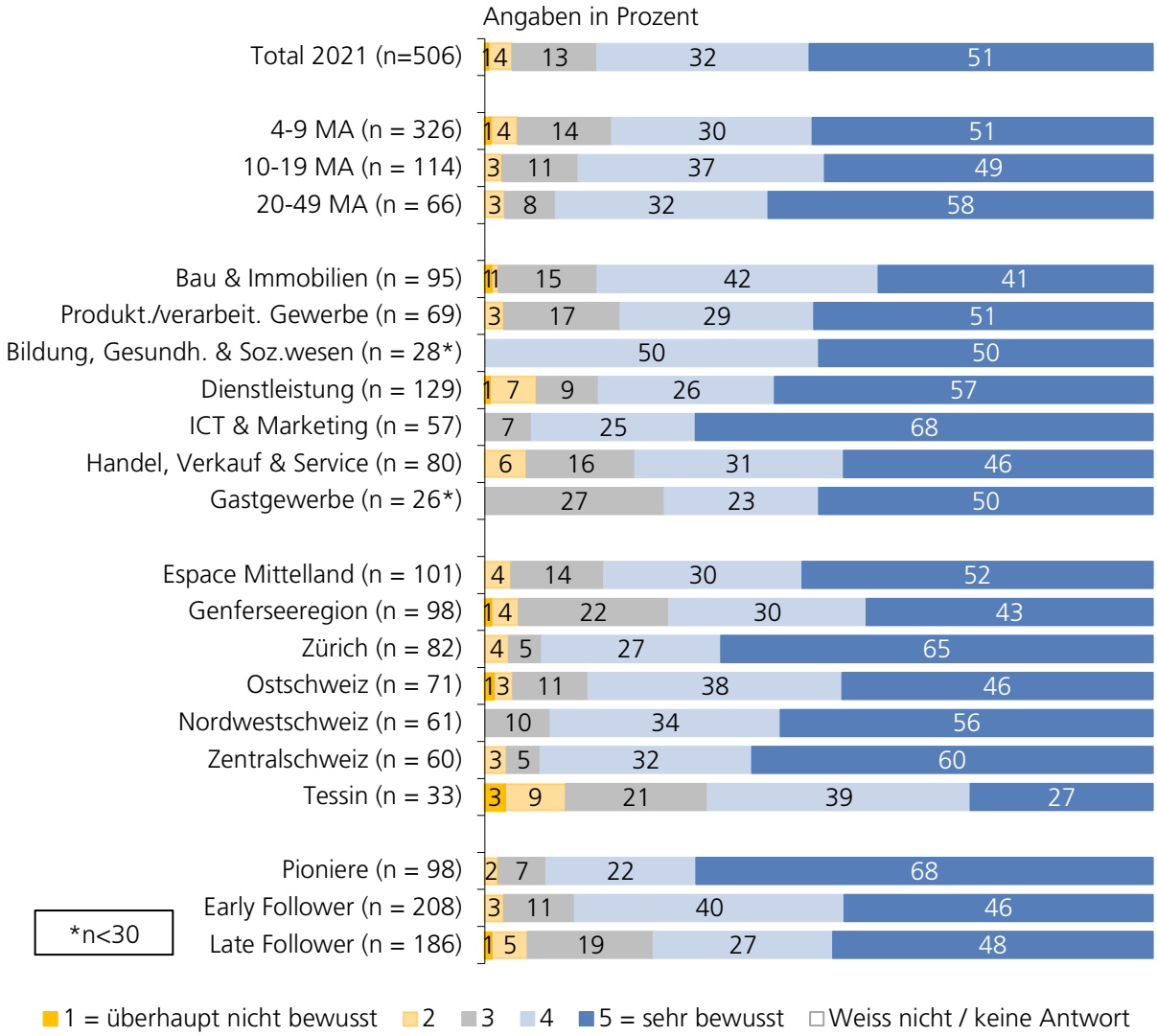
3.3.3 Bedrohungsbewusstsein

In der Studie 2021 wurde erstmals nach dem Bedrohungsbewusstsein gefragt. Über vier Fünftel (83 %) der Befragten geben an, sich der 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).

Frage 10:
Wie bewusst sind Ihnen die Bedrohungen durch Cyberkriminalität wie Malware, Online-Betrug und Hacking?
Basis: Total, n = 506

Die Befragten fühlen sich also eher «mittelgut» informiert bezüglich Cyberrisk (Mittelwert Frage 9 = 3.5), die Bedrohungen durch Cyberkriminalität sind ihnen aber eher bis sehr bewusst (Mittelwert Frage 10 = 4.3). Das Bewusstsein der Bedrohungen bedeutet nicht automatisch, dass sie auch als gross empfunden werden (dieses Thema wird später untersucht, siehe Kapitel 3.3.8). Der Vergleich der zwei Fragen lässt vermuten, dass die Befragten sich innerhalb der unbekannteren Cyberrisk-Thematik besonders bezüglich der Bedrohungen auszukennen glauben, aber weniger

bezüglich anderer Inhalte der Thematik, wie z.B. den Schutzmassnahmen. Ob dem wirklich so ist, müssten weitere Studien zeigen.



Die Antworten der verschiedenen Unternehmensgrössenkategorien unterscheiden sich kaum; es ist eine leichte Tendenz festzustellen, dass grössere Unternehmen ihr Bewusstsein bezüglich der Bedrohungen höher einschätzen (4-9 Mitarbeitende: 81 %, 10-19 Mitarbeitende: 86 %, 20-49 Mitarbeitende: 90 % bei den Skalenwerten 4-5).

Zwischen den verschiedenen Branchen gibt es keine signifikanten Unterschiede; ICT & Marketing (93 %) sowie Bildung, Gesundheit- & Sozialwesen (100 %) geben die höchsten Einschätzungen ab (Skalenwerte 4-5).

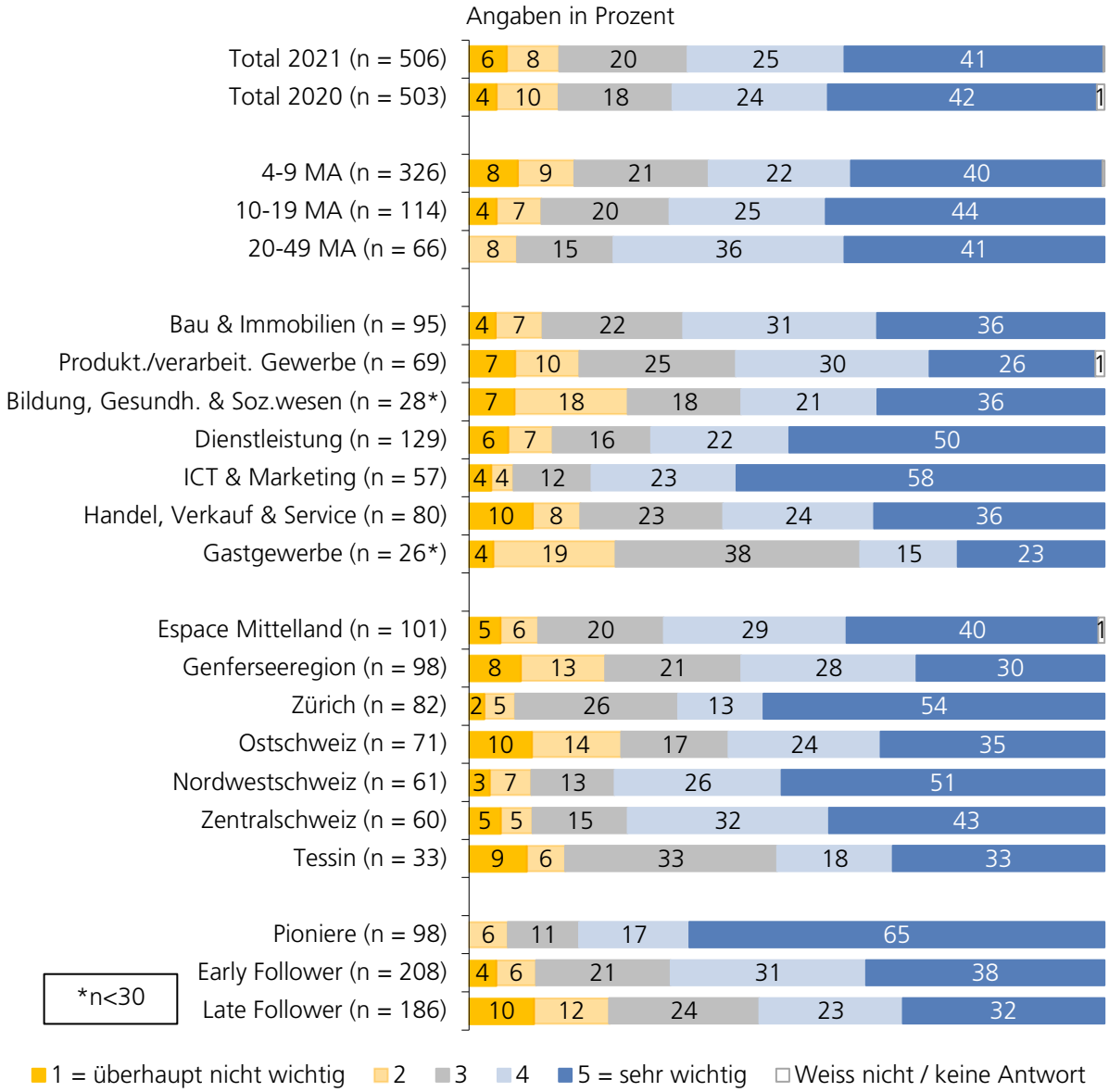
Beim Vergleich der Regionen fallen das Tessin (66 %) und die Genferseeregion (73 %) mit einer tiefen Bedrohungsbeurteilung auf: Der Tessiner Wert liegt signifikant tiefer als derjenige der Zentralschweiz (92 %), dem Grossraum Zürich (92 %), der Nordwestschweiz (90 %) und des Espace Mittelland (82 %). Zudem liegt ein signifikanter Unterschied zwischen dem Grossraum Zürich (92 %) und der Genferseeregion (73 %) vor.

3.3.4 Wichtigkeit des Themas Cybersicherheit

Die Wichtigkeit der Cybersicherheit wird 2021 ähnlich zu 2020 beurteilt: Rund zwei Drittel der Befragten (66 %) beurteilen das Thema Cybersicherheit als (eher) wichtig (Skalenwerte 4 und 5 auf einer Fünferskala).

Frage 11:
Welche Wichtigkeit hat in Ihrer Firma das Thema Cybersicherheit?
Basis: Total, n = 506

Wie schon bei der Einschätzung der eigenen Kenntnisse und des Bedrohungsbewusstseins steigen die Werte auf der Fünferskala mit der Unternehmensgrösse: Je mehr Mitarbeitende ein Unternehmen beschäftigt, desto wichtiger wird das Thema Cybersicherheit beurteilt (Skalenwerte 4-5 bei 4-9 Mitarbeitenden: 62 %, bei 10-19 Mitarbeitenden: 69 %, bei 20-49 Mitarbeitenden: 77 %)



Während im Gastgewerbe die Wichtigkeit am tiefsten bewertet wird (MW 3.3), liegt sie in der Branche ICT & Marketing am höchsten (MW 4.3); der Unterschied zwischen diesen Werten ist signifikant. Nordwestschweizer-, Zentralschweizer- und Zürcher Unternehmen geben höhere Werte

an (4.1, 4.0 und 4.1) als die übrigen Regionen (3.6 bis 3.9), es bestehen aber keine signifikanten Unterschiede.

Je aufgeschlossener die Befragten gegenüber technischen Innovationen sind, desto höher stufen sie die Wichtigkeit des Themas Cybersicherheit ein (Pioniere: 4.4, Early Follower: 3.9, Late Follower: 3.5). Der Unterschied zwischen den Pionieren und den Early sowie den Late Followern ist signifikant und auch die Early Follower unterschieden sich nochmals signifikant von den Late Followern. Geschäftsführende, die sich bezüglich dem Thema Cyberrisk (eher) gut informiert fühlen, beurteilen die Wichtigkeit signifikant höher (MW 4.3) als (eher) uninformierte Befragte (2.8).

Und: Je wichtiger das Thema Cybersicherheit eingeschätzt wird, desto höher ist die durchschnittliche Sicherheitsmassnahmenumsetzung. Bei tiefer technischer Massnahmenumsetzung liegt der Durchschnitt der Themenwichtigkeit bei 2.5, bei hoher technischer Massnahmenumsetzung bei 4.4. Der Unterschied ist signifikant. Bei den organisatorischen Massnahmen gilt dasselbe: Bei tiefer organisatorischer Massnahmenumsetzung liegt die Einschätzung der Wichtigkeit des Themas Cybersicherheit bei einem Durchschnitt von 3.3, bei hoher Massnahmenumsetzung bei 4.8 (signifikanter Unterschied).

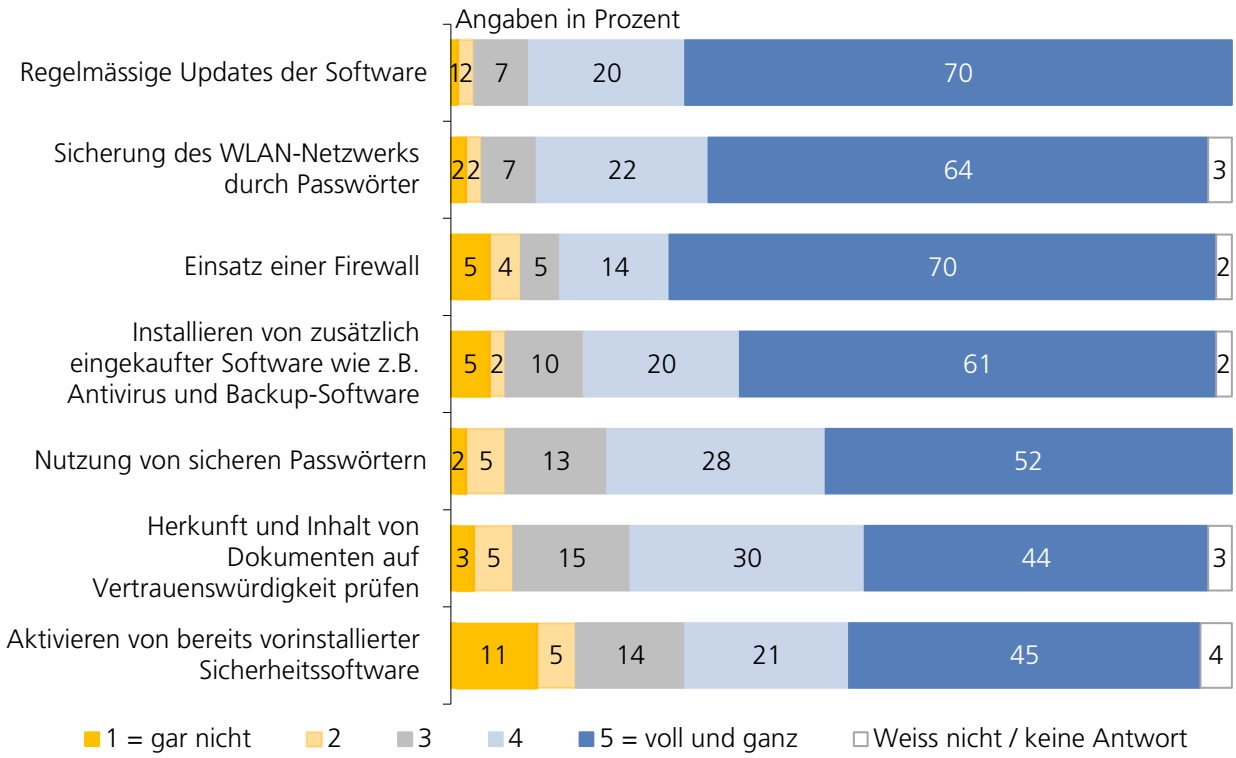
3.3.5 Technische Massnahmen zur Erhöhung der Cybersicherheit

Die Frage nach technischen Sicherheitsmassnahmen wurde 2021 ausführlicher gestellt als 2020: Es wurde nicht nur gefragt, *ob* die Massnahme umgesetzt wurde, sondern *inwieweit*. Die Vergleichbarkeit ist deshalb beschränkt. Die Befragten konnten anhand einer Fünferskala von 1 = *gar nicht* bis 5 = *voll und ganz* antworten.

Frage 12:
Inwieweit sind die folgenden **technischen** Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?
Basis: Total, n = 506

Den höchsten Umsetzungsgrad erzielen die beiden Massnahmen «Regelmässige Softwareupdates» (90 % fast/voll umgesetzt) und die «Sicherung des WLAN-Netzwerks durch Passwörter» (86 % fast/voll umgesetzt). An dritter Stelle folgt der Einsatz einer Firewall (84 % fast/voll umgesetzt). Die Softwareupdates und die Firewall wurden bereits in der Studie 2020 abgefragt (ohne Skala), und erhielten dort einen fast identischen Wert von 89 % (Softwareupdates) und 85 % (Firewall).

Die «Installation zusätzlich eingekaufter Sicherheitssoftware» wurde von rund vier Fünfteln (81 %) fast oder voll und ganz umgesetzt, ebenfalls vier Fünftel (80 %) der befragten Unternehmen nutzen konsequent sichere Passwörter. Die Massnahme «Prüfung der Herkunft und Inhalte von Dokumenten auf Vertrauenswürdigkeit» wurde von rund drei Vierteln (74 %) fast oder voll und ganz umgesetzt und «Aktivieren von bereits vorinstallierter Sicherheitssoftware» liegt mit 66 % Umsetzungsgrad auf dem letzten Platz.

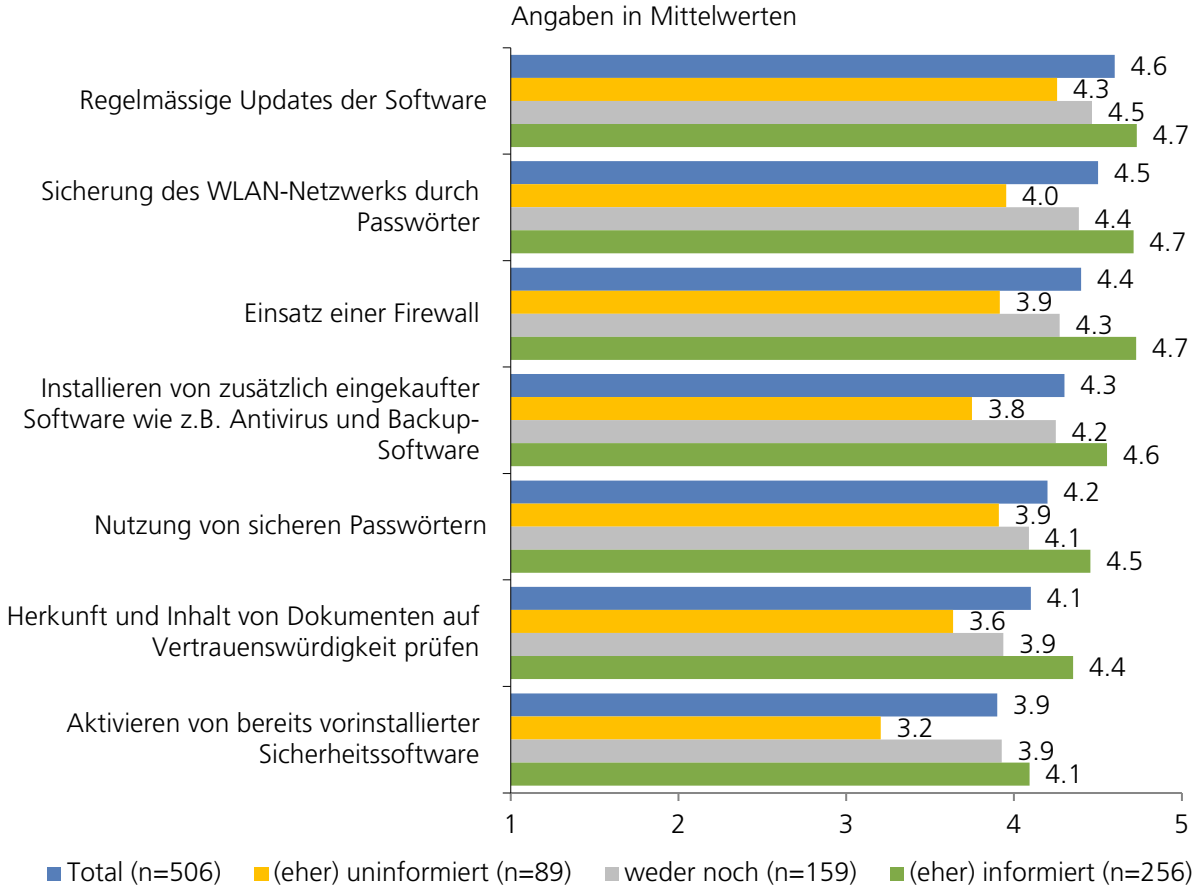


Nicht oder nur minimal umgesetzte Massnahmen können unter Umständen ein massgebliches Sicherheitsrisiko bedeuten: Einerseits für die Unternehmen selbst, andererseits für die Besitzer der Daten, die dort entwendet werden können (z.B. Kundendaten, Passwörter).

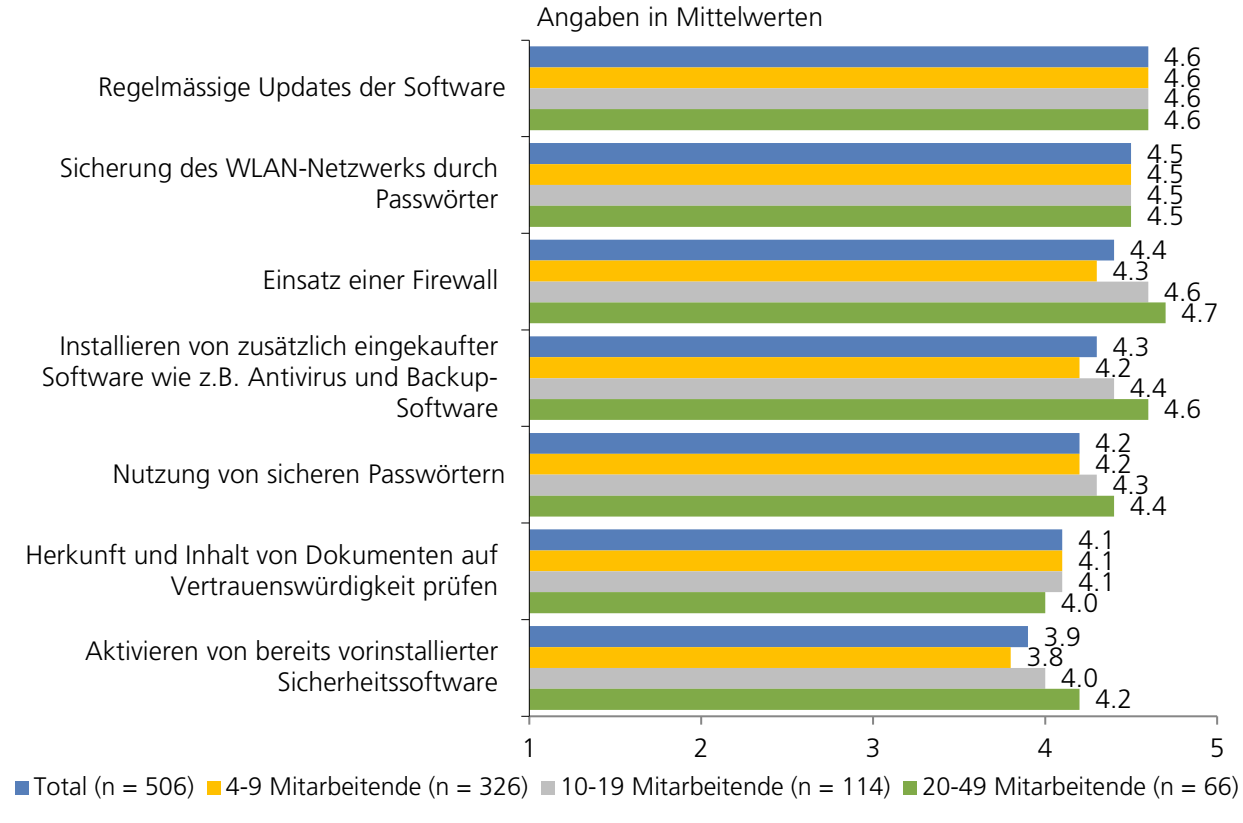
Zwischen den Branchen gibt es bezüglich Massnahmenumsetzung kaum signifikante Abweichungen. Tendenziell und über alle Branchen gesehen, sind die Massnahmen in der ICT- & Marketingbranche am weitesten umgesetzt, in der Gastgewerbebranche am wenigsten weit.

Pioniere sind mit sämtlichen Massnahmen weiter fortgeschritten als Early und Late Follower, und Early Follower sind weiter fortgeschritten als Late Follower. Die Unterschiede sind bei sämtlichen technischen Massnahmen signifikant, zumindest zwischen den Pionieren und den Late Followern.

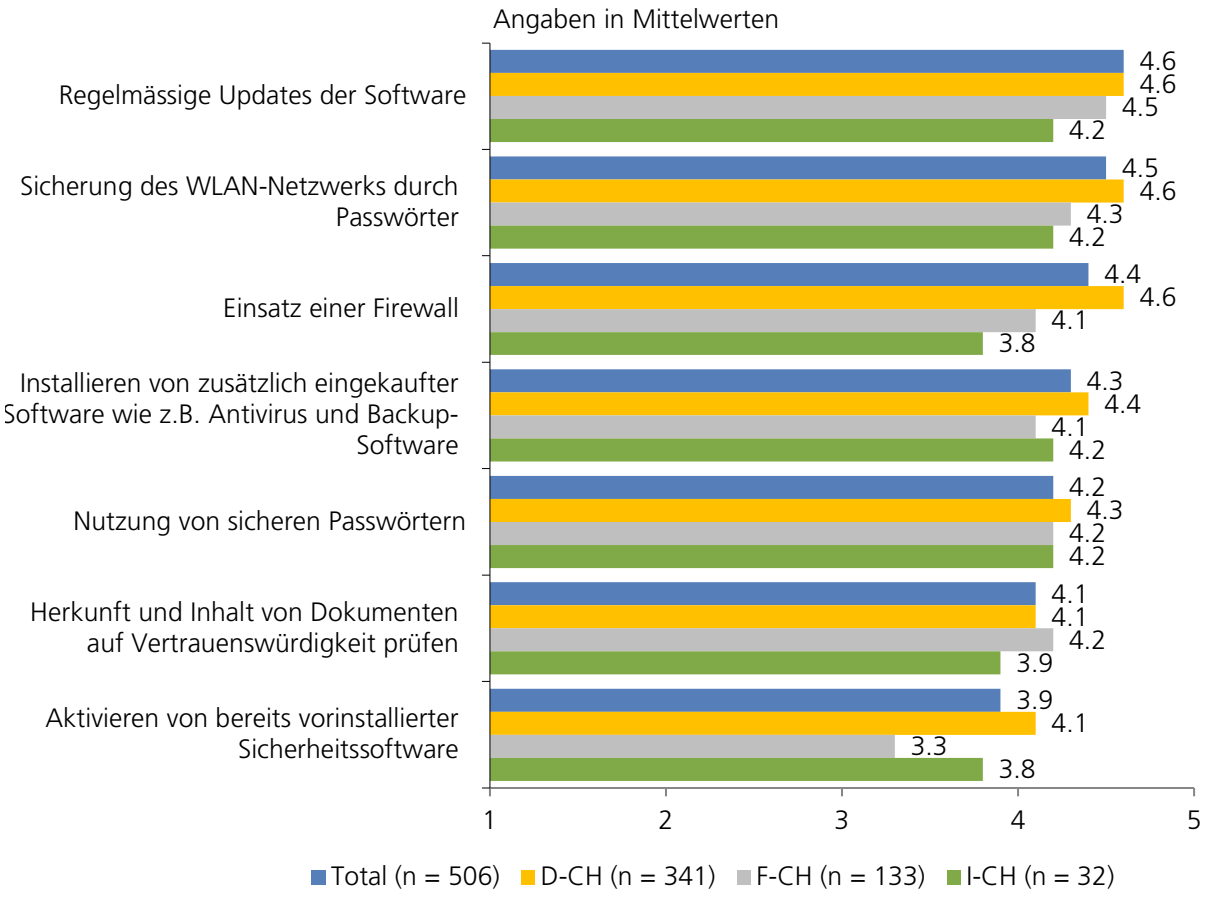
Je besser die befragten Geschäftsführenden sich bezüglich Cyberrisk informiert fühlen, desto eher haben sie Sicherheitsmassnahmen umgesetzt. Dies gilt für alle technischen Massnahmen in signifikantem Ausmass.



Bei mehreren Massnahmen gilt: Je grösser das Unternehmen, desto eher sind die Massnahmen umgesetzt (Einsatz einer Firewall, Installieren von zusätzlich eingekaufter Software, Nutzung von sicheren Passwörtern, Aktivieren von bereits vorinstallierter Sicherheitssoftware). Diese Erkenntnis liess sich bereits in der Vorjahresstudie 2020 finden.



Bei der Massnahmenumsetzung gibt es zudem einen «Röstigraben»: In der Westschweiz und im Tessin sind viele Massnahmen tendenziell bis signifikant weniger weit umgesetzt als in den Regionen der Deutschschweiz. Signifikante Unterschiede bestehen bei der Installation von zusätzlich eingekaufter Sicherheitssoftware (D-CH: 4.4, W-CH: 4.1), dem Aktivieren bereits vorinstallierter Software (D-CH: 4.1, W-CH: 3.3), dem Einsatz einer Firewall (D-CH: 4.6, W-CH: 4.1, TI: 3.8), den regelmässigen Softwareupdates (D-CH: 4.6, TI: 4.2) und der Passwortsicherung des WLANS (D-CH: 4.6, W-CH: 4.3).



Zudem gilt: Wer schon einmal von einem Cyberangriff betroffen war, hat mehr Massnahmen umgesetzt. Signifikant ist der Unterschied bei drei von sieben technischen Massnahmen: Der Installation von zusätzlich eingekaufter Sicherheitssoftware (betroffen: 4.5, nicht betroffen: 4.2), dem Einsatz einer Firewall (betroffen: 4.6, nicht betroffen: 4.3) und bei den regelmässigen Updates der Software (betroffen: 4.7, nicht betroffen: 4.5).

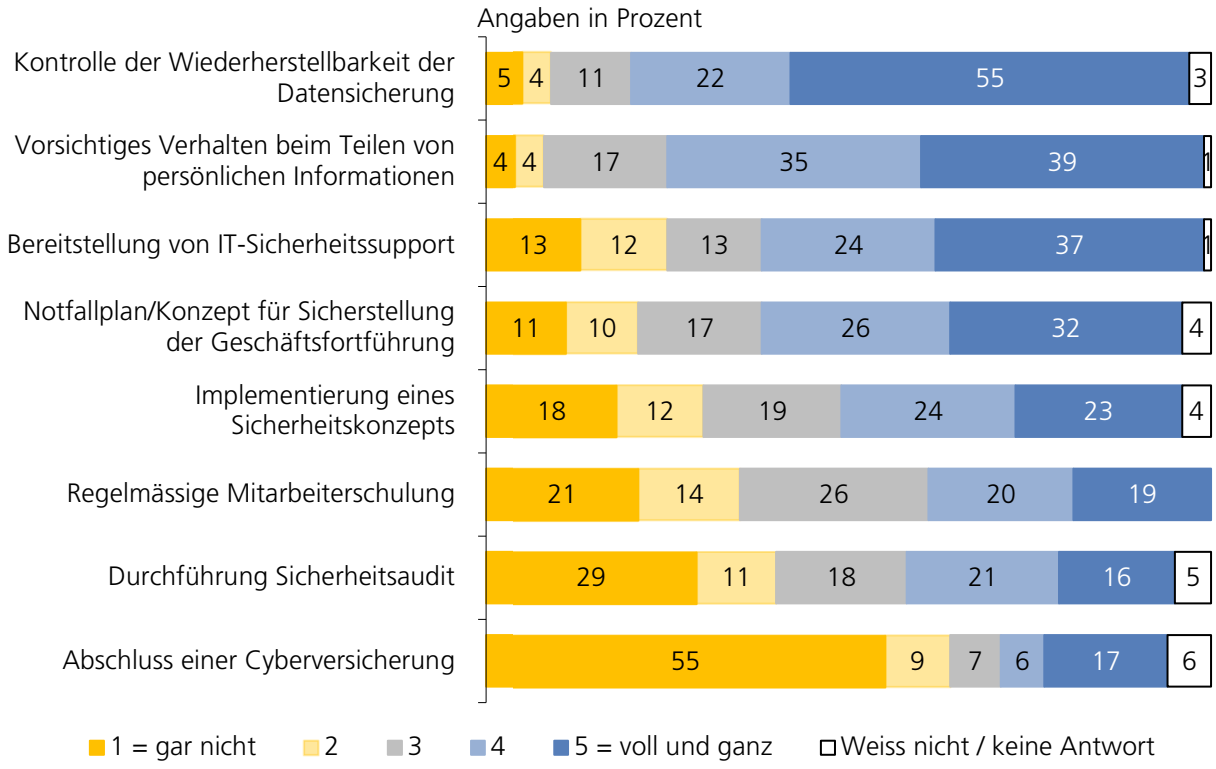
3.3.6 Organisatorische Massnahmen zur Erhöhung der Cybersicherheit

Analog zu der Frage nach technischen Sicherheitsmassnahmen wurde auch die Frage nach organisatorischen Sicherheitsmassnahmen im Jahr 2021 detaillierter gestellt als noch 2020 und Vergleiche sind deshalb nur eingeschränkt möglich.

Frage 13:
Inwieweit sind die folgenden **organisatorischen** Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?
Basis: Total, n = 506

Wie schon in der Vorjahresstudie fällt im Vergleich zur Umsetzung der *technischen* Massnahmen auf, dass *organisatorische* Massnahmen deutlich seltener umgesetzt werden. Die am häufigsten umgesetzte organisatorische Massnahme ist die Kontrolle der Wiederherstellbarkeit der Datensicherung. Rund drei Viertel (77 %) der Befragten haben sie fast oder voll und ganz umgesetzt (2020 allg. umgesetzt: 71 %). Zum Vergleich: Die am häufigsten vollständig umgesetzte technische Massnahme, regelmässige Softwareupdates, wurde von 90% der Befragten fast oder voll und ganz umgesetzt.

An zweiter Stelle in der Reihenfolge der umgesetzten organisatorischen Massnahmen steht das «Vorsichtige Verhalten beim Teilen von persönlichen Informationen»: 74 Prozent der Befragten haben sie fast oder voll und ganz umgesetzt. An dritter Stelle folgt die Bereitstellung von Sicherheitssupport mit rund zwei Dritteln (61 %) der Befragten, die sie fast oder voll und ganz umgesetzt haben. Einen beinahe gleich hohen Wert (58 %) erhält die Massnahme «Notfallplan für die Sicherstellung der Geschäftsführung» (2020: 48 %).



Die restlichen Massnahmen wurden von weniger als 50 Prozent der Unternehmen fast oder voll und ganz umgesetzt: Implementierung eines Sicherheitskonzepts (2021: 47 %, 2020: 36 %), regelmässige Mitarbeiterschulung (2021: 39 %, 2020: 37 %) und die Durchführung eines Sicherheitsaudits (2021: 37 %, 2020: 21 %). Bezüglich der Cyberversicherung dürfte sich für eine klare

Aussage und den Vergleich zur Vorjahresstudie der alleinige Skalenwert 5 besser eignen als der summierte Wert der Skalenwerte 4 und 5, weil ein Versicherungsabschluss nur ganz oder gar nicht erfolgen kann. Demzufolge haben 17 Prozent der Kleinunternehmen eine Cyberversicherung abgeschlossen, womit sich der Wert gegenüber 2020 nicht verändert hat.

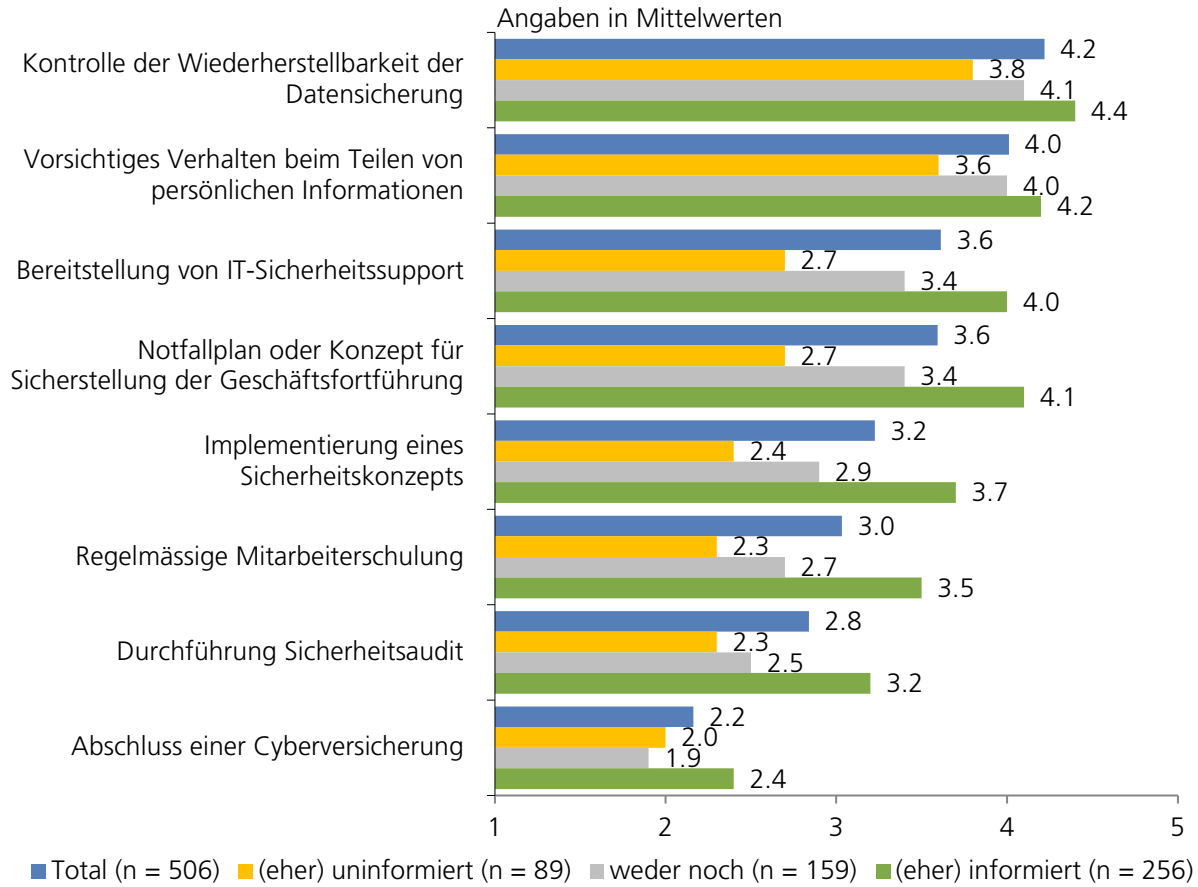
Gegenüber 2020 scheint die Umsetzung gestiegen zu sein bei den Massnahmen:

- Kontrolle der Wiederherstellbarkeit der Datensicherung (71 % -> 77 %)
- Notfallplan für die Sicherstellung der Geschäftsführung (48 % -> 58 %)
- Implementierung eines Sicherheitskonzepts (36 % -> 47 %)
- regelmässige Mitarbeiterschulung (37 % -> 39 %)
- Durchführung eines Sicherheitsaudits (21 % -> 37 %)

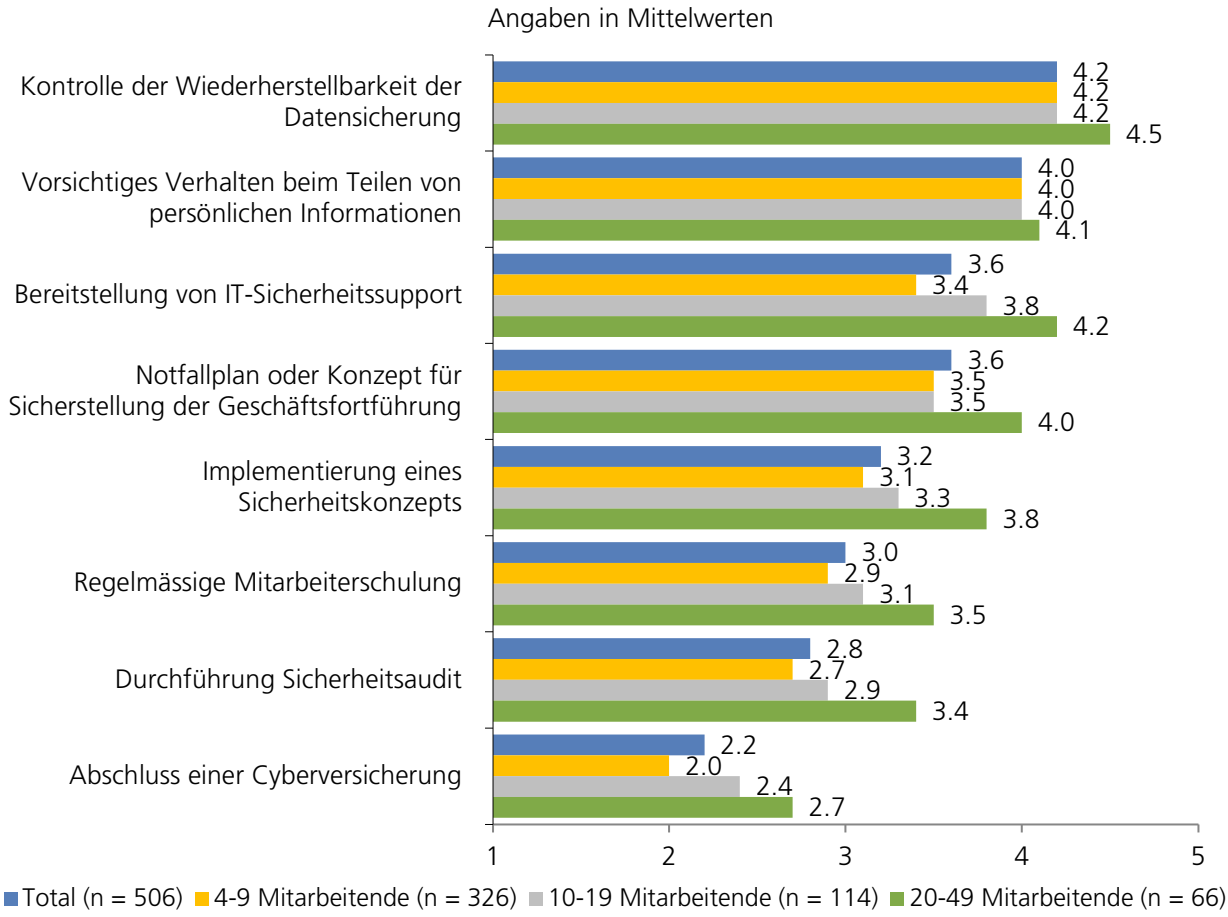
Allerdings ist hier die Vergleichbarkeit zur Vorstudie aufgrund der Skalenänderung (von ja/nein zu Fünferskala) mit grosser Vorsicht zu geniessen.

Wie schon bei den technischen Massnahmen verhält es sich bei der grossen Mehrheit der organisatorischen Massnahmen so, dass grössere Unternehmen sie eher umgesetzt haben als kleine, Deutschschweizer Unternehmen eher als Westschweizer Unternehmen, Pioniere eher als Early und Late Follower und bereits von Cyberangriffen betroffene eher als nicht-betroffene.

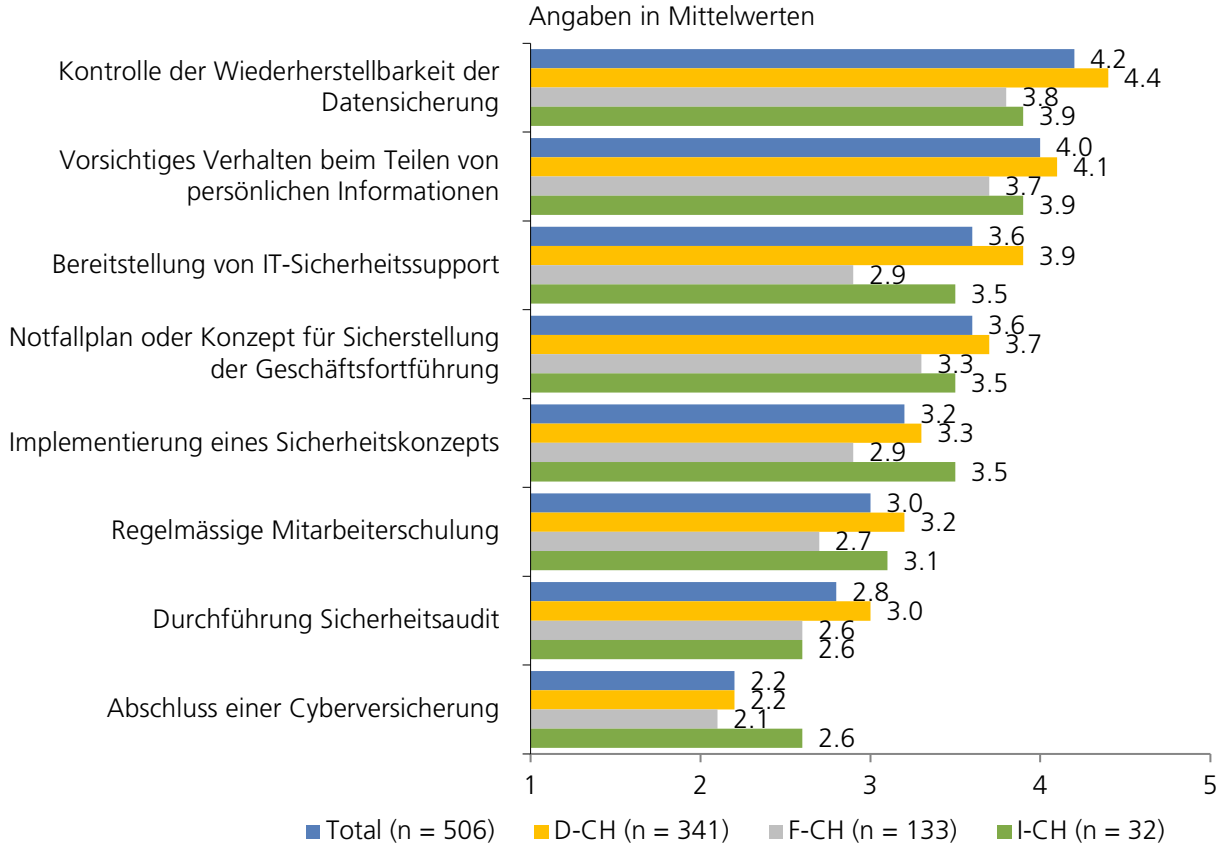
Je besser sich die Befragten über die Cyberrisk-Thematik informiert fühlen, desto mehr organisatorische Massnahmen treffen sie zur Erhöhung der Cybersicherheit (signifikant). Diese Erkenntnis wurde auch schon aus der 2020er Studie gewonnen.



Die Unterschiede zwischen den Unternehmensgrössenkategorien sind signifikant zwischen der jeweils kleinsten und grössten Kategorie bei den Massnahmen: Bereitstellung von IT-Sicherheitssupport (4-9 Mitarbeitende: 3.4, 20-49 Mitarbeitende: 4.2), regelmässige Mitarbeiterschulung (4-9 Mitarbeitende: 2.9, 20-49 Mitarbeitende: 3.5), Implementierung eines Sicherheitskonzepts (4-9 Mitarbeitende: 3.1, 20-49 Mitarbeitende: 3.8), Abschluss einer Cyberversicherung (4-9 Mitarbeitende: 2.0, 20-49 Mitarbeitende: 2.7), sowie Durchführung Sicherheitsaudit (4-9 Mitarbeitende: 2.7, 20-49 Mitarbeitende: 3.4).



Die Unterschiede zwischen den Regionen sind aufgrund der kleinen Stichprobe in der italienischsprachigen Schweiz nur zwischen der Deutsch- und Westschweiz signifikant, dies jedoch bei fast allen Massnahmen: Bereitstellung von IT-Sicherheitssupport (D-CH: 3.9, W-CH: 2.9), regelmässige Mitarbeiterschulung (D-CH: 3.2, W-CH: 2.7), Notfallplan für Sicherstellung der Geschäftsfortführung (D-CH: 3.7, W-CH: 3.3), Implementierung eines Sicherheitskonzepts (D-CH: 3.3, W-CH: 2.9), Durchführung eines Sicherheitsaudits (D-CH: 3.0, W-CH: 2.6), vorsichtiges Verhalten beim Teilen von persönlichen Informationen (D-CH: 4.1, W-CH: 3.7), Kontrolle der Wiederherstellbarkeit der Datensicherung (D-CH: 4.4, W-CH: 3.8).
Einzige Ausnahme ist der Abschluss einer Cyberversicherung, bei welcher es über alle drei Sprachregionen keine signifikanten Unterschiede gibt (D-CH: 2.2, W-CH: 2.1, TI: 2.6).



Fünf von acht organisatorischen Massnahmen wurden von Befragten, welche bereits einmal von einem Cyberangriff betroffen waren, signifikant weiter umgesetzt als von Befragten, welche nicht betroffen waren: Die Kontrolle der Wiederherstellbarkeit der Datensicherung (betroffen: 4.4, nicht betroffen: 4.1), die Bereitstellung von Sicherheitssupport (betroffen: 3.8, nicht betroffen: 3.5), der Notfallplan für die Sicherstellung der Geschäftsfortführung (betroffen: 3.8, nicht betroffen: 3.5), die Implementierung eines Sicherheitskonzepts (betroffen: 3.4, nicht betroffen: 3.1) und die Durchführung eines Sicherheitsaudits (betroffen: 3.0, nicht betroffen: 2.7).

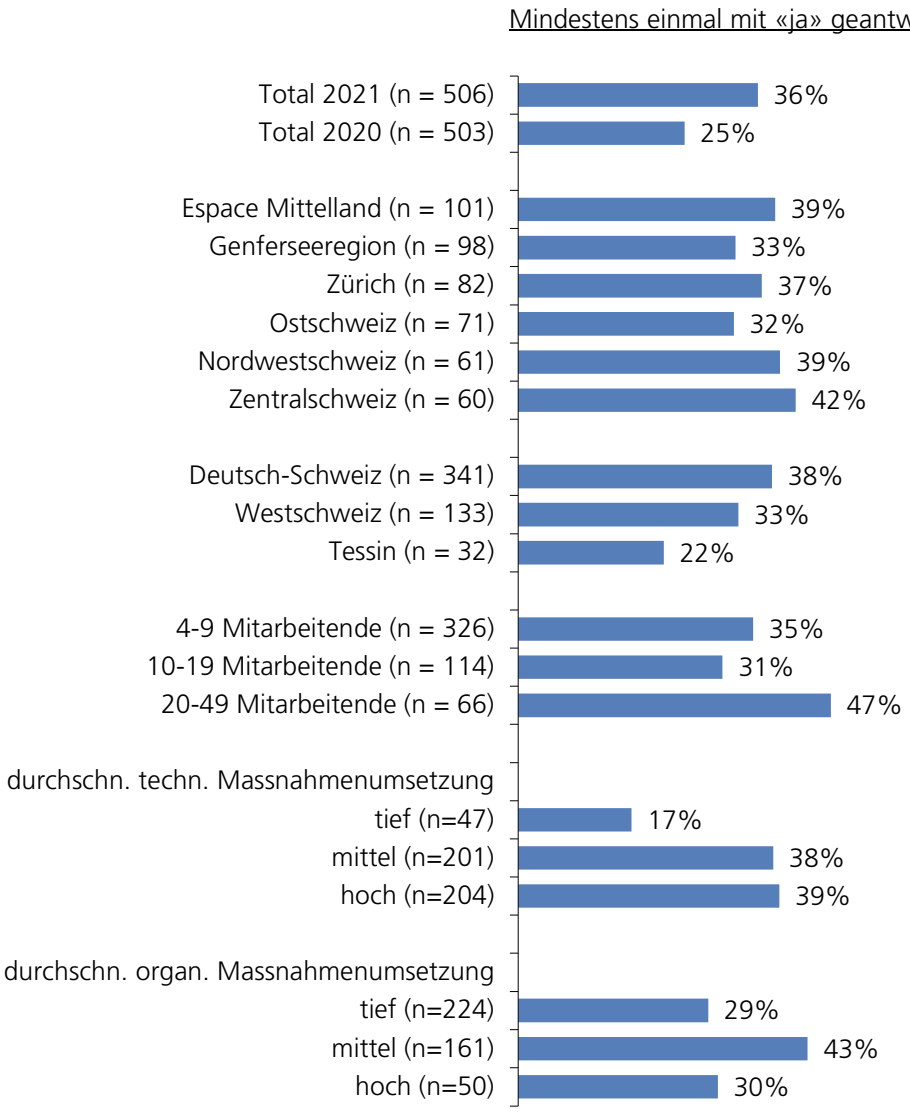
3.3.7 Cyberangriffe und entstandener Schaden

Seit der 2020er Befragung ist die Anzahl der Cyberangriffe stark angestiegen. War 2020 noch ein Viertel (25 %) der befragten Unternehmen betroffen, so ist es 2021 bereits mehr als ein Drittel (36 %). Hochgerechnet auf die Grundgesamtheit bedeutet dies, dass 2021 rund 55'000 Schweizer Unternehmen mit 4 bis 49 Mitarbeitenden von einem Cyberangriff betroffen waren (Vertrauensbereich: 52’729 bis 57’431), 2020 waren es noch rund 38'000 (Vertrauensbereich: 36’783 bis 39'717).

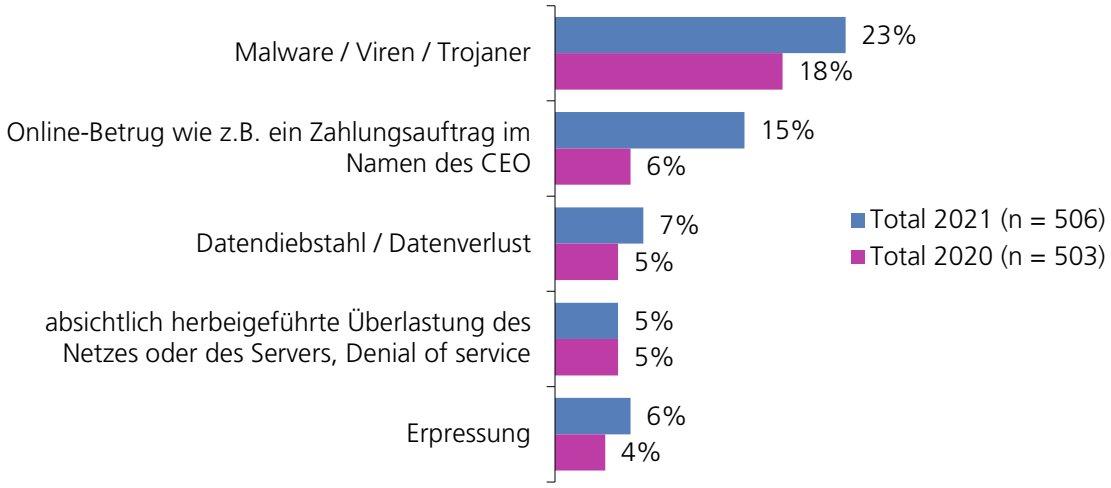
Frage 14:
Wurde Ihre Firma schon einmal erfolgreich durch eine der folgenden Techniken angegriffen, so dass ein erheblicher Aufwand nötig war, um Schäden zu beheben?
Basis: Total, n = 506

Die Frage wurde bewusst so formuliert, dass unbedeutende oder erfolgreich abgewehrte Angriffe wie zum Beispiel unbeachtete oder ausgefilterte Phishing-Mails nicht in der Statistik erscheinen. Es handelt sich gemäss Fragestellung nur um Angriffe, die einen erheblichen Aufwand benötigten, um die Schäden zu beheben.

Zwischen den Branchen, Gross- und Sprachregionen sowie zwischen Unternehmensgrössenkategorien gibt es keine signifikanten Unterschiede: Es sind alle Subgruppen in ähnlichem Ausmass von den Angriffen betroffen, trotz der unterschiedlich umfangreich umgesetzten Sicherheitsmassnahmen. Ein signifikanter Unterschied besteht zwischen Unternehmen, die eine mittlere oder hohe technische Sicherheitsmassnahmenumsetzung haben (38 % bzw. 39 % Betroffenheit) und Unternehmen mit tiefem Massnahmenumsetzungsgrad (17 %). Bei der organisatorischen Sicherheitsmassnahmenumsetzung ist es die mittlere Kategorie (43 %), die signifikant von der tiefen Umsetzungskategorie (29 %) abweicht. Eine mögliche Interpretation ist, dass die Betroffenheit von Cyberangriffen zu höheren technischen Sicherheitsmassnahmen führt, in gewissem Ausmass auch zu höheren organisatorischen Sicherheitsmassnahmen. Leider reichen die Studienergebnisse nicht für eine sichere Aussage diesbezüglich.

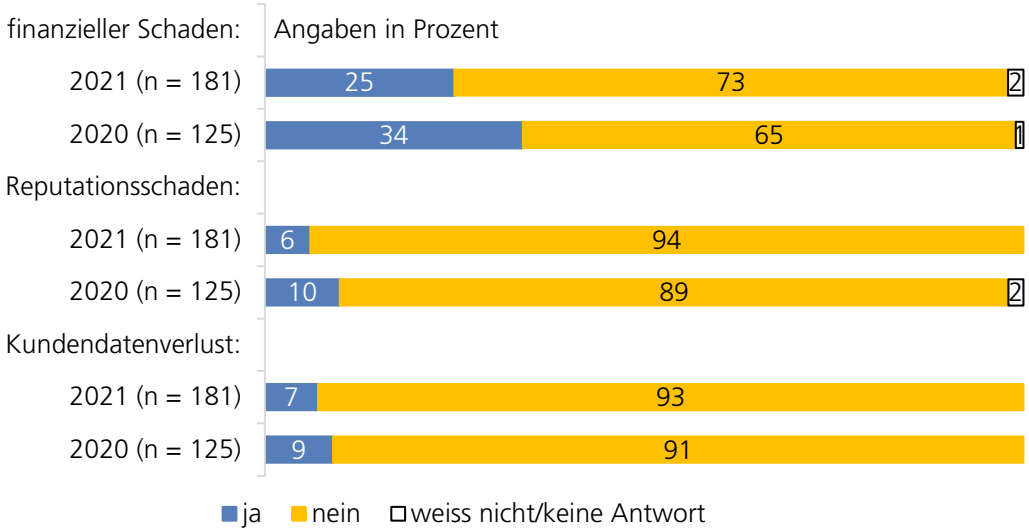


Die am häufigsten genannten Angriffe erfolgten via Malware, Viren bzw. Trojaner: Rund ein Viertel der Befragten (23 %) wurde so angegriffen. Gegenüber 2020 (18 %) bedeutet dies eine Steigerung von mehr als einem Viertel (27 %). Die zweithäufigste genannte Angriffsform ist Onlinebetrug (15 %). Hier fand gegenüber 2020 (6 %) mehr als eine Verdoppelung der erfolgreichen Angriffe statt. Auch Datendiebstahl (7 %) und Erpressung (6 %) wurde häufiger genannt als noch 2020 (5 % bzw. 4 %). Absichtlich herbeigeführte Überlastung des Netzes (DoS) wurde unverändert von 5 Prozent der Befragten genannt.



Frage 15:
Entstand durch diesen Angriff / Entstanden durch diese Angriffe …
Filter: Wurden Opfer von mindestens einem Angriff gemäss Frage 14, n = 181

Prozentual sind die aus den Angriffen resultierenden Schadensfälle gegenüber dem letzten Jahr gesunken, was vielleicht ein Hinweis auf bessere Schutzmassnahmen oder sichereres Verhalten sein könnte, wie im vorherigen Kapitel vermutet. Im letzten Jahr entstand in rund einem Drittel (34 %) der Angriffsfälle ein finanzieller Schaden, dieses Jahr ist das nur noch bei einem Viertel (25 %) der Fall. Bei jedem zehnten Angriff entstand letztes Jahr ein Reputationsschaden (10 %), dieses Jahr bei rund jedem 16. Angriff (6 %). Bezüglich Kundendatenverlust ist der anteilsmässige Rückgang kleiner: von 9 Prozent im letzten Jahr sank er auf 7 Prozent in diesem Jahr.

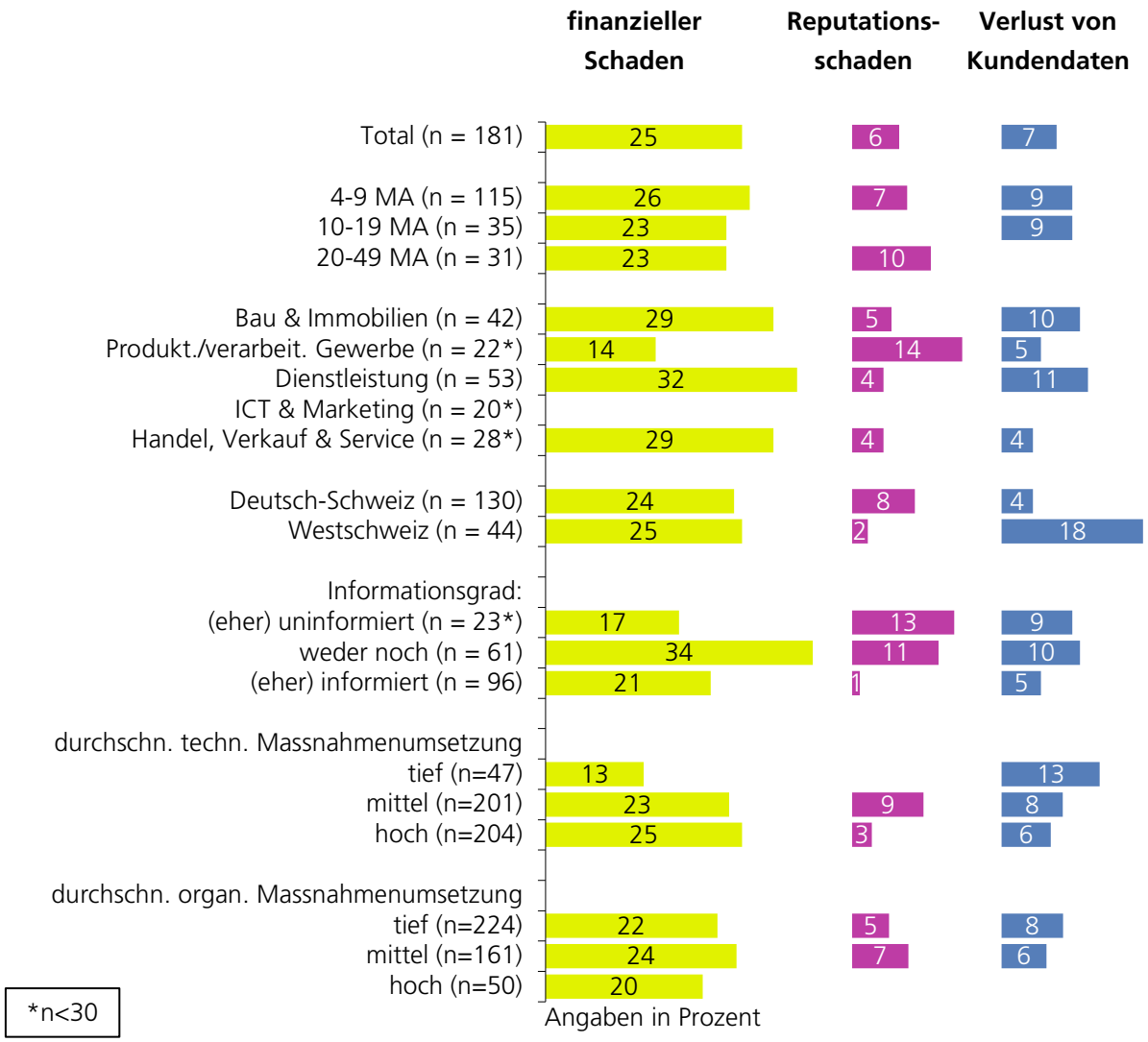


In absoluten Zahlen sind die finanziellen Schäden und die Kundendatenverluste gestiegen, die Reputationsschäden gesunken. Eine mögliche Erklärung für die gesunkenen Reputationsschäden könnte sein, dass ein Cyberangriff heute als weniger imageschädigend beurteilt wird als noch vor einem Jahr. Da in den Medien breit und oft über entsprechende Fälle berichtet wurde, hat sich diese Einstellung evt. verändert.

	%-Satz der von Angriffen betroffenen (2021: n = 181, 2020: n = 125)	%-Satz auf gesamte Stichprobe (2021: n = 506, 2020: n = 503)	In absoluten Zahlen auf die Grundgesamtheit extrapoliert (n = 153'000)
Finanzieller Schaden:			
2021 (n = 181)	25%	9%	13'770 (13'420 - 14'120)
2020 (n = 125)	34%	8.5%	13'000 (12'682 - 13'328)
Reputationsschaden:			
2021 (n = 181)	6%	2%	3'060 (3'022 - 3'098)
2020 (n = 125)	10%	2.5%	3'830 (3'772 - 3'878)
Kundendatenverlust:			
2021 (n = 181)	7%	2.5%	3'830 (3'772 - 3'878)
2020 (n = 125)	9%	2%	3'060 (3'022 - 3'098)

Zwischen den Subgruppen ergeben sich fast keine Unterschiede. Die verschiedenen Branchen und Unternehmensgrössenkategorien sind in ähnlichem Masse von den Schäden betroffen. Deutsch- und Westschweizer Unternehmen beklagen finanzielle Schäden ebenfalls in ähnlichem Ausmass (24 % bzw. 25 %). Reputationsschäden werden von Deutschschweizer Unternehmen (8 %) häufiger genannt als von den Kollegen in der Westschweiz (2 %), der Unterschied kann aber durch den Signifikanztest nicht abgesichert werden. Kundendatenverluste hingegen werden in der Westschweiz (18 %) signifikant häufiger beklagt als in der Deutschschweiz (4 %).

Geschäftsführende, welche sich in der Cyberrisk-Thematik (eher) gut informiert fühlen, nennen weniger Reputationsschäden (1 %) als (eher) schlecht informierte (13 %), dieser Unterschied ist signifikant. Kleiner und nicht signifikant ist der Unterschied bei den Kundendatenverlusten: (Eher) gut informierte (5 %) haben weniger Kundendaten verloren als (eher) schlecht informierte (9%). Bezüglich finanzieller Schäden liegen die Gruppen nahe beieinander: (Eher) gut informierte nennen zu 21 Prozent finanzielle Schäden, (eher) schlecht informierte zu 17 Prozent.



3.3.8 Risiko-Einschätzung eines Cyberangriffs

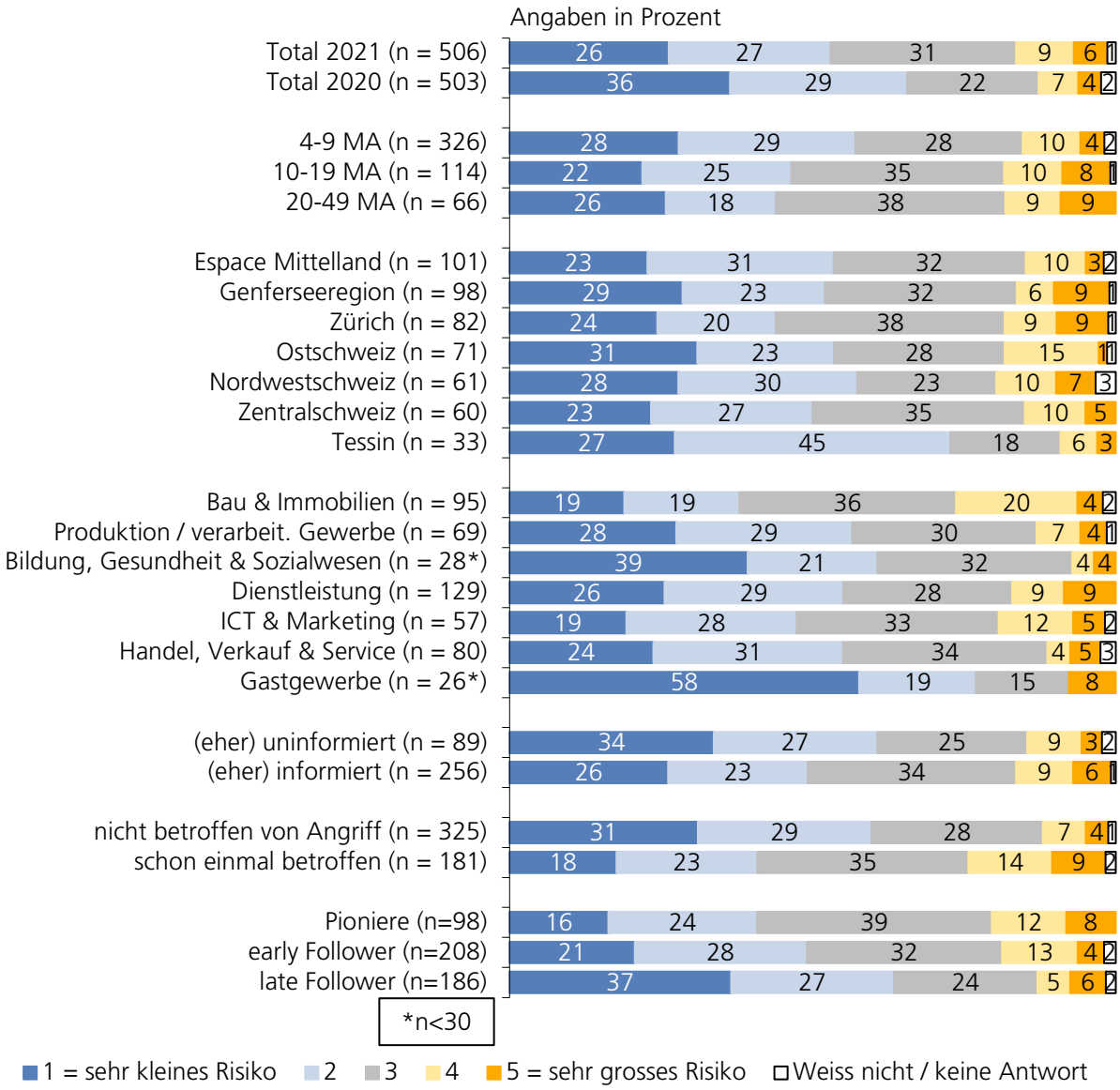
Das Risiko, durch einen Cyberangriff einen Tag lang ausser Kraft gesetzt zu werden, wird in diesem Jahr höher eingeschätzt als noch 2020: Damals bewerteten noch rund zwei Drittel der befragten Unternehmer/-innen (65 %) das Risiko mit einer eins oder zwei (sehr oder eher kleines Risiko) auf der Fünferskala. In der aktuellen Studie tut dies nur noch rund die Hälfte der Befragten (53 %). Als eher hohes oder hohes Risiko (Skalenwerte 4 und 5) schätzte es 2020 noch jeder zehnte (11 %) ein, in diesem Jahr nun rund jeder siebte (15 %).

Frage 16:
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 = 506

Diese Sorge bzw. das 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 (2.7) und Early Follower

(2.5). Ausserdem: Wer schon einmal von einem Cyberangriff betroffen war, schätzt das Risiko ebenfalls signifikant höher ein (2.7) als noch nicht Betroffene (2.2).

Der Grund für die höhere Einschätzung dürfte in den vielen Vorfällen liegen: Einerseits wurde und wird viel in den Medien darüber berichtet, andererseits sind nun deutlich mehr Unternehmen selbst betroffen oder dürften persönlich Betroffene kennen. Allerdings scheint die Einschätzung im Vergleich zu der sehr hohen Zahl an Angriffen immer noch eher zu tief auszufallen.

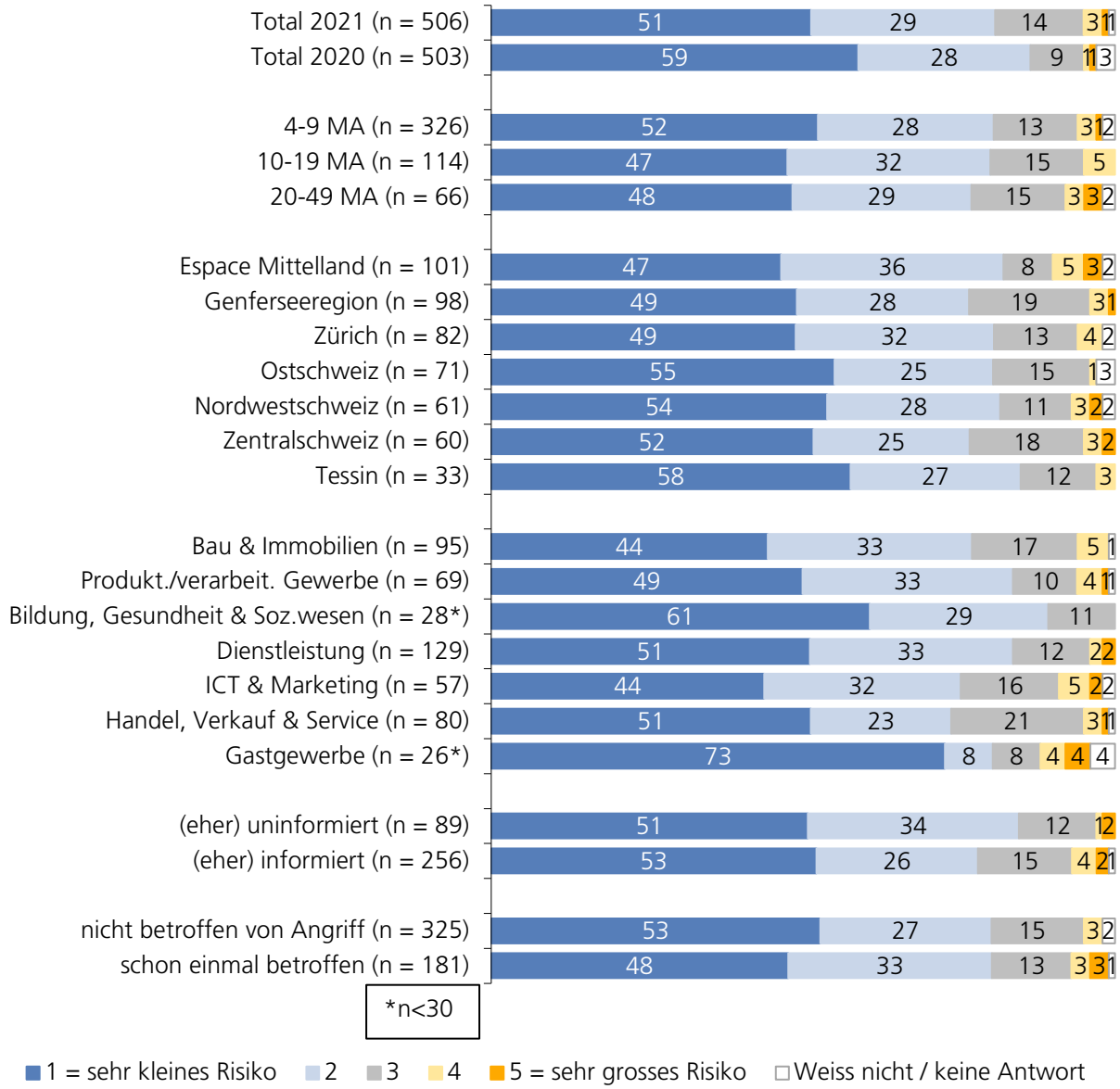


Ein Cyberangriff als existenzgefährdendes Vorkommnis ist für nur sehr wenige Geschäftsführende ein realistisches Szenario, aber auch hier ist die Risikoeinschätzung gestiegen. 2020 war es jeder fünfzigste Befragte (2 %), der das Risiko als eher oder sehr hoch einschätzte (Skalenwerte vier oder 5 auf Fünferskala). 2021 ist es nun jeder fünfundzwanzigste (4 %). Als eher kleines oder kleines Risiko (Skalenwerte 1 und 2) schätzten es 2020 noch 87 Prozent ein, 2021 sind dies noch 80 Prozent.

Frage 17:
Als wie hoch schätzen Sie das Risiko ein, dass Ihre Unternehmung innerhalb der nächsten 2-3 Jahre von einem Cyberangriff betroffen sein wird, der für Ihr Geschäft **existenzgefährdend** ist?
Basis: Total, n = 506

Zwischen den Subgruppen gibt es keine signifikanten Unterschiede: Anders als bei der vorangegangenen Frage besteht hier auch kein Unterschied zwischen von Cyberangriffen betroffenen und nicht betroffenen; Betroffene erkennen also ein höheres Risiko von Cyberangriffen, die ein Unternehmen einen Tag ausser Kraft setzen können, nicht aber eines, das existenzgefährdend ist.

Angaben in Prozent

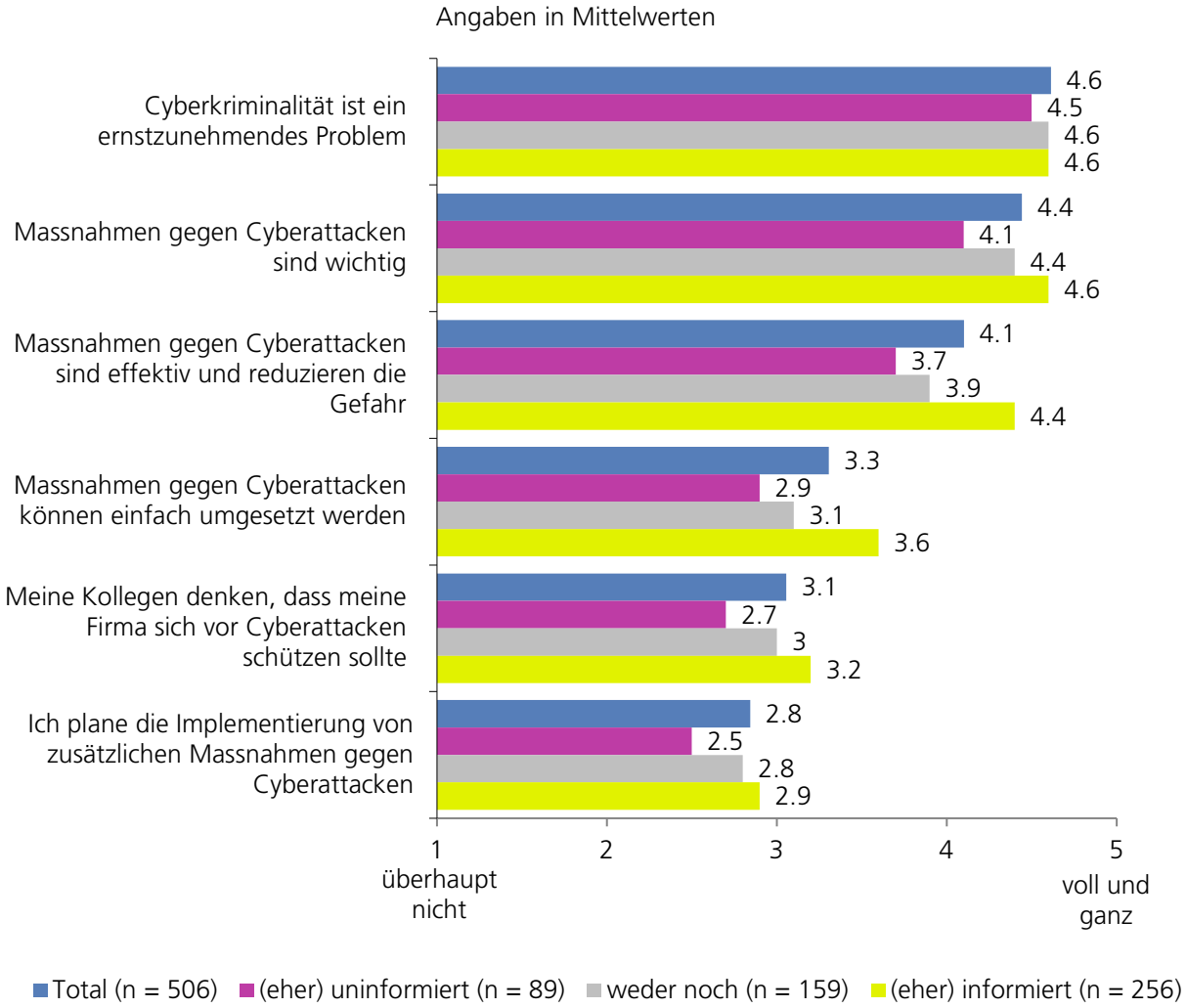


3.3.9 Einstellung zu Cyberkriminalität

Frage 18:
Inwiefern stimmen Sie den folgenden Aussagen zu Cyberkriminalität wie Malware, Online-Betrug und Hacking zu?
Basis: Total, n = 506

Von sechs abgefragten Aussagen zu Cyberkriminalität wurden drei mit einem Mittelwert über 4, auf der Fünferskala, und drei mit einem Mittelwert unter 4 bewertet. Eine Zustimmung über 4 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 (3.3), meine Kollegen denken, dass meine Firma sich vor Cyberattacken schützen sollte (3.1) 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 oder als unnötig betrachtet zu werden.

Während es zwischen Branchen und Regionen keine auffälligen Unterschiede gibt, stimmen (eher) gut informierte, Pioniere und bereits einmal von einem Cyberangriff betroffene Befragte mehreren Aussagen signifikant stärker zu als Early und Late Follower, (eher) schlecht informierte und nicht betroffene.

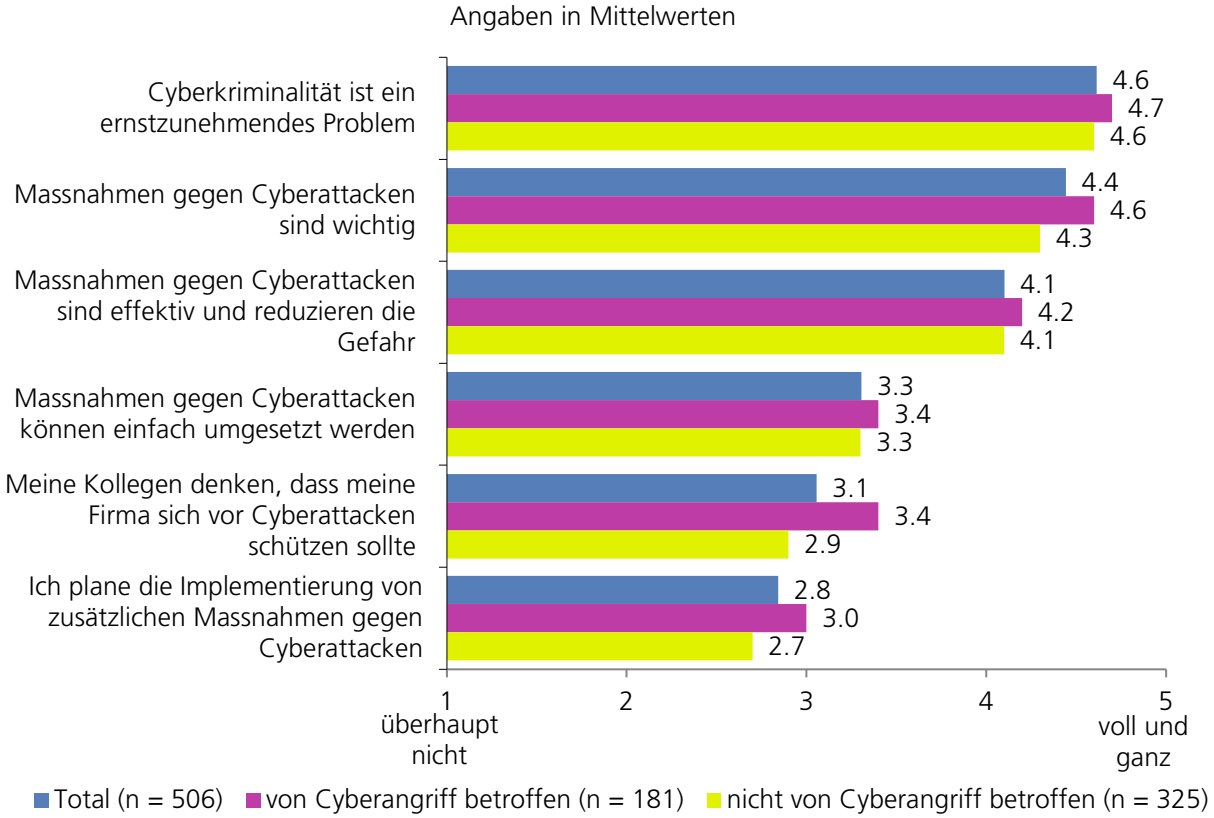


Ausserdem gilt bei sämtlichen Aussagen: Je höher die technische oder organisatorische Sicherheitsmassnahmenumsetzung ist, desto höher ist auch die Zustimmung zu den Aussagen. Die Differenz von den Unternehmen mit hohen und mittleren Massnahmenumsetzungen zu den Unternehmen mit tiefer Umsetzung ist bei allen Aussagen signifikant.

Bei fünf von sechs Aussagen stimmen die (eher) gut informierten Befragten signifikant stärker zu als diejenigen, die schlechter informiert sind als sie. Einzige Ausnahme ist die Aussage, dass «Cyberkriminalität ein ernstzunehmendes Problem» ist (eher bis gut informierte: 4.6, weder noch: 4.6, eher bis schlecht informierte: 4.5).

Pioniere stimmen vier von sechs Aussagen signifikant stärker zu als Early und Late Follower: «Massnahmen gegen Cyberattacken sind wichtig» (Pioniere: 4.7, Late Follower: 4.3), «Massnahmen gegen Cyberattacken sind effektiv und reduzieren die Gefahr» (Pioniere: 4.4, Late Follower: 3.9), «Meine Kollegen denken, dass meine Firma sich vor Cyberattacken schützen sollte» (Pioniere: 3.5, Early Follower: 3.2, Late Follower: 2.7) und «Ich plane die Implementierung von zusätzlichen Massnahmen gegen Cyberkriminalität» (Pioniere: 3.1, Late Follower: 2.6). Keine signifikanten Unterschiede gibt es bei den Aussagen «Cyberkriminalität ist ein ernstzunehmendes Problem» und «Massnahmen gegen Cyber-Attacken können einfach umgesetzt werden».

Von Cyberangriffen betroffene Unternehmen stimmen folgenden Aussagen signifikant stärker zu als nicht betroffene: «Cyberkriminalität ist ein ernstzunehmendes Problem» (betroffen: 4.7, nicht betroffen: 4.6), «Massnahmen gegen Cyberattacken sind wichtig» (betroffen: 4.6, nicht betroffen: 4.3), «Meine Kollegen denken, dass meine Firma sich vor Cyberattacken schützen sollte» (betroffen: 3.4, nicht betroffen: 2.9) und «Ich plane die Implementierung von zusätzlichen Massnahmen gegen Cyberattacken» (betroffen: 3.0, nicht betroffen: 2.7).

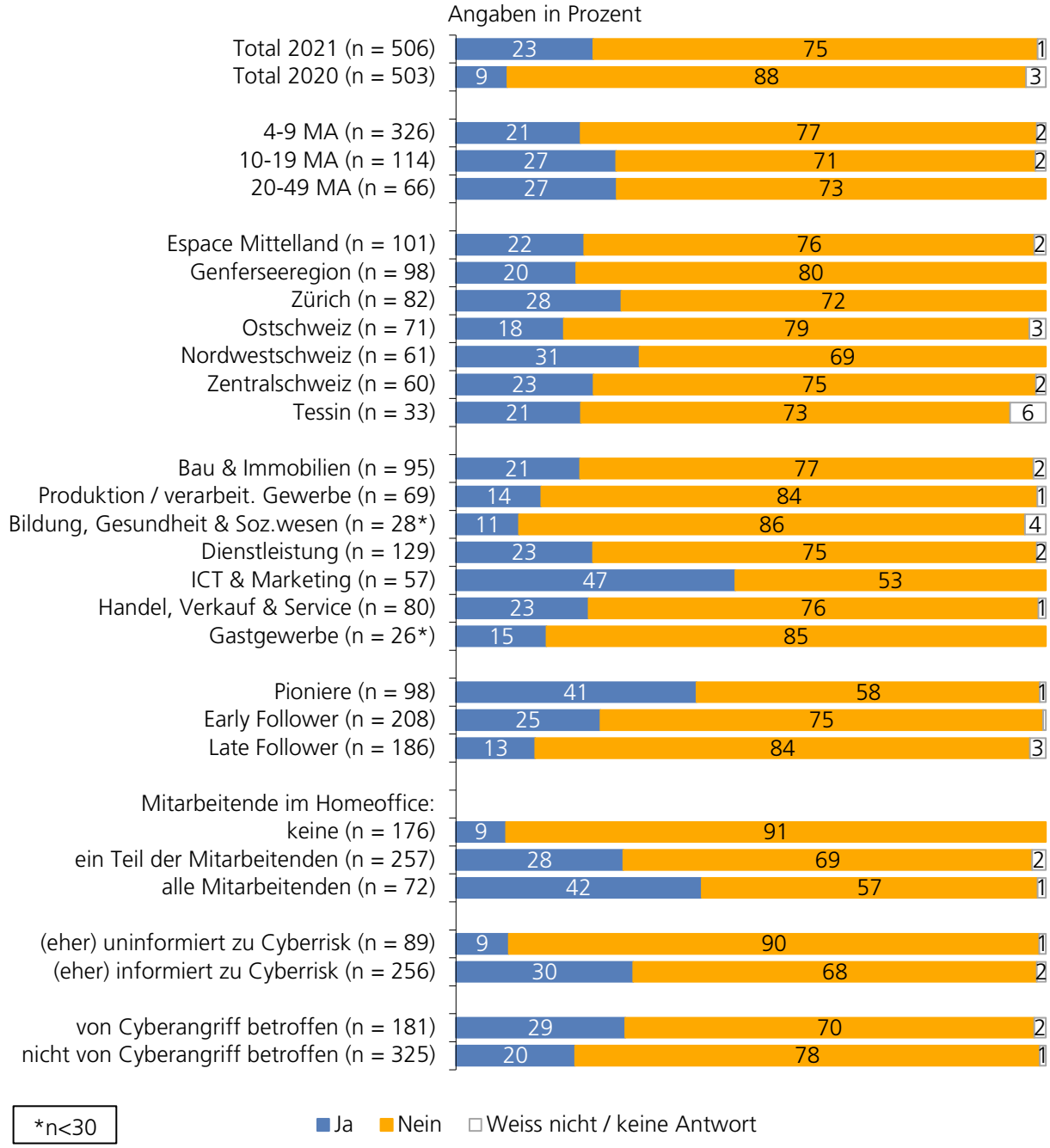


3.3.10 Cybersicherheitsmassnahmen aufgrund der Homeoffice-Pflicht

Im letzten Jahr hatte noch lediglich rund jede/-r zehnte Befragte (9 %) aufgrund des Lockdowns zusätzliche Sicherheitsmassnahmen ergriffen. Mittlerweile ist es – aufgrund der diesjährigen Homeoffice-Pflicht – fast jeder vierte (23 %).

Frage 19:
Haben Sie aufgrund der Homeoffice-Pflicht zusätzliche Sicherheitsmassnahmen gegen Cyberangriffe umgesetzt?
Basis: Total, n = 503

Wie schon 2020, wurden bei den Firmen, die potenziell alle Mitarbeitenden (42 %) oder einen Teil der Mitarbeitenden (28 %) in das Homeoffice schicken können, signifikant häufiger zusätzliche Sicherheitsmassnahmen vorgenommen als bei denjenigen, bei denen niemand (9 %) vom Homeoffice aus arbeiten kann. Ausserdem haben die Geschäftsführenden, die sich eher oder sehr gut bezüglich Cyberrisk informiert fühlen, signifikant häufiger zusätzliche Sicherheitsmassnahmen ergriffen (30 %) als diejenigen, die sich (eher) nicht gut informiert fühlen (9 %).



In besonders hohem Masse haben Geschäftsführende der Branche ICT & Marketing ihre Sicherheitsmassnahmen verschärft: Fast die Hälfte (47 %) von ihnen geben dies an. Damit weicht diese Branche signifikant ab von den Branchen Bau & Immobilien (21 %), Produktion & verarbeitendes Gewerbe (14 %), Bildung, Gesundheit & Sozialwesen (11 %) und Dienstleistung (23 %).

Je offener die Befragten gegenüber Innovationen sind, desto eher haben sie ihre Sicherheitsmassnahmen der neuen Homeoffice-Situation angepasst (Pioniere: 41 %, Early Follower: 25 %, Late Follower: 13 %). Auch diese Unterschiede sind alle signifikant.

Ein weiterer signifikanter Unterschied ergibt sich zwischen den von Cyberangriffen betroffenen Befragten, von denen fast jeder Dritte (29 %) die Sicherheitsmassnahmen aufgrund der Homeoffice-Pflicht verschärfte, und den nicht betroffenen, bei denen dies nur jeder fünfte (20 %) tat.

Befragte mit hoher technischer und organisatorischer Sicherheitsmassnahmenumsetzung geben hier signifikant höhere Werte an (techn: 34 %, organ: 40 %) als Befragte mit tiefer Massnahmenumsetzung (techn: 2 %, organ: 15 %). Allerdings geht aus der Befragung nicht heraus, ob die Massnahmenumsetzung schon vor der Homeoffice-Pflicht hoch war und durch die Homeoffice-Pflicht noch weiter erhöht wurde oder ob sie erst aufgrund der Homeoffice-Pflicht auf den hohen Stand gebracht wurde.

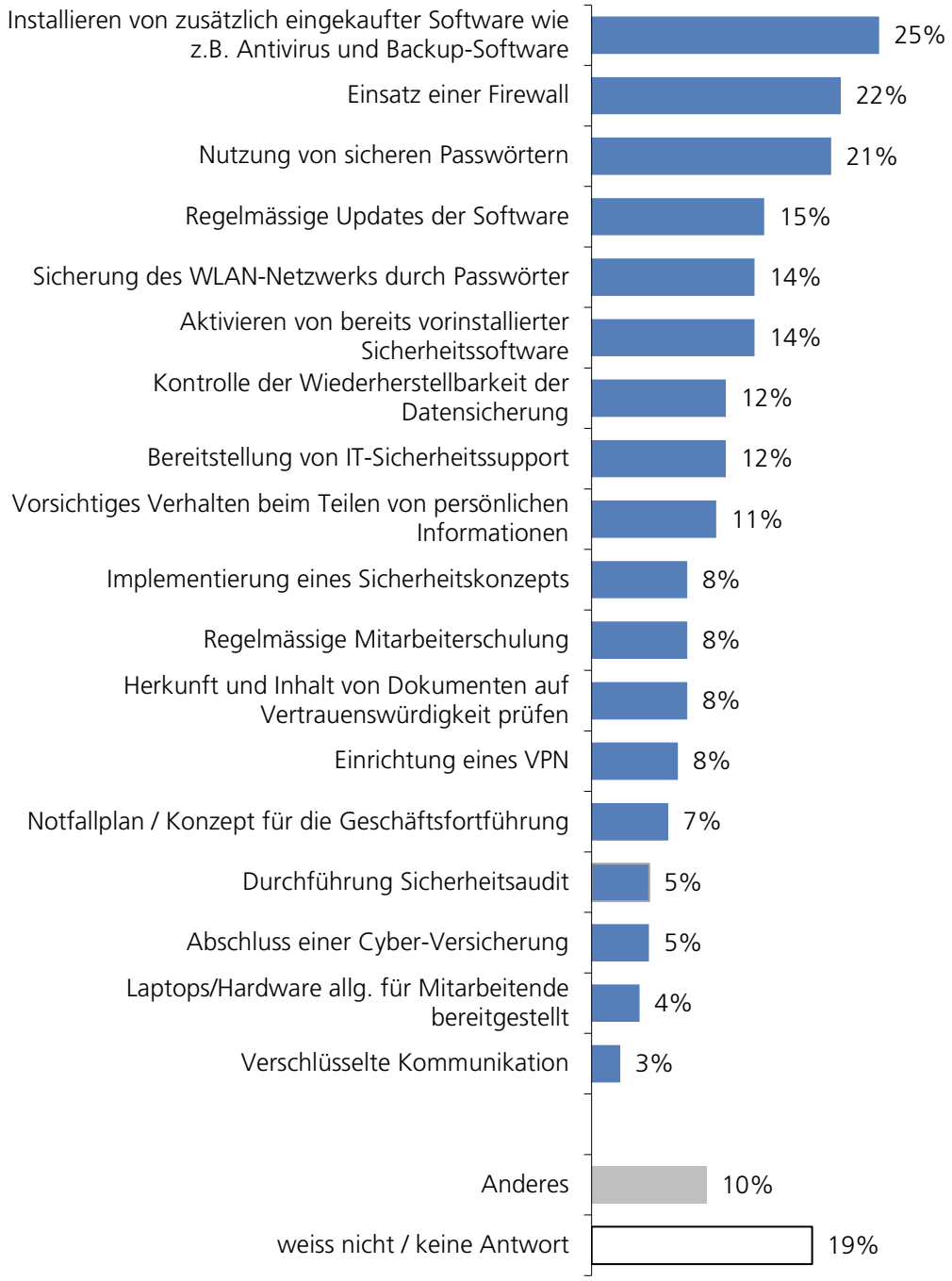
Die Antworten auf die Frage 20 wurden in der aktuellen Studie mit einer neuen, ausführlicheren Liste codiert und können deshalb nicht 1:1 mit der Vorjahresstudie verglichen werden. Dort, wo ein Vergleich möglich ist, wird es im Text erwähnt.

Frage 20:
Welche Sicherheitsmassnahmen haben Sie während der Homeoffice-Pflicht umgesetzt?
Basis: Haben während der Homeoffice-Pflicht zusätzliche Sicherheitsmassnahmen umgesetzt, n = 118
Vorcodierte, halboffene Frage: Antworten wurden nicht vorgelesen, Codierung teilweise durch Interviewer und teilweise im Nachhinein durch Codierer

Diejenigen Befragten, die zusätzliche Sicherheitsmassnahmen aufgrund der Homeoffice-Pflicht vornahmen, installierten am ehesten zusätzlich eingekaufte Sicherheitssoftware (25 %) oder setzten eine Firewall ein (22 %). In der Vorjahresstudie war der Einsatz der Firewall noch die Top-Antwort (27 %). An dritter Stelle folgt die Nutzung sicherer Passwörter (21 %) und erst an vierter Stelle folgt, mit deutlichem Abstand zu den Plätzen 1 bis 3, die erste organisatorische Massnahme, nämlich regelmässigen Softwareupdates (15 %).

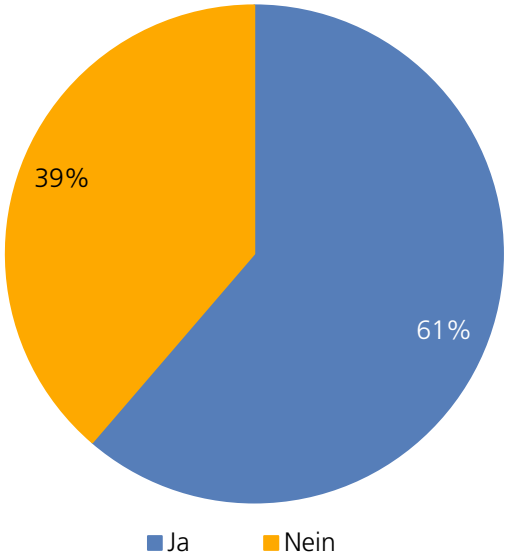
Im Durchschnitt wurden 2.3 Sicherheitsmassnahmen genannt. Je grösser ein Unternehmen ist, desto mehr Massnahmen wurden genannt (4-9 Mitarbeitende: 2.1, 10-19 Mitarbeitende: 2.6, 20-49 Mitarbeitende: 3.1). Pioniere (2.7) führten mehr Massnahmen aus als Early und Late Follower, jedoch liegen die Late Follower mit 2.3 Massnahmen bei dieser Frage vor den Early Followern (2.0).

Deutschschweizer (2.5) und Tessiner (3.1) Unternehmen nannten mehr Massnahmen als Westschweizer Unternehmen (1.6), von Cyberangriffen betroffene Unternehmen nannten mehr (2.9) als nicht betroffene (1.9).



Rund drei Fünftel (61 %) der befragten Unternehmen machen ihren Mitarbeitenden Vorgaben für die Passwörter, bei rund zwei Fünfteln gibt es keine Vorgaben (39 %). In der kleinsten Unternehmensgrössenkategorie (4-9 Mitarbeitende) werden signifikant seltener Passwortregeln verfügt (55 %) als in der mittleren (10-19 Mitarbeitende: 71 %) und der grössten Kategorie (20-49 Mitarbeitende: 74%). Pioniere verfügen signifikant häufiger über Passwortregeln (78 %) als Early Follower (63 %) und Late Follower (50 %), und (eher) gut informierte Geschäftsführende (70 %) signifikant häufiger als (eher) uninformierte (46 %). Auch zwischen den Sprachregionen ergeben sich signifikante Unterschiede: Die Deutschschweiz liegt mit 68 Prozent vor der Westschweiz (47 %) und dem Tessin (44 %).

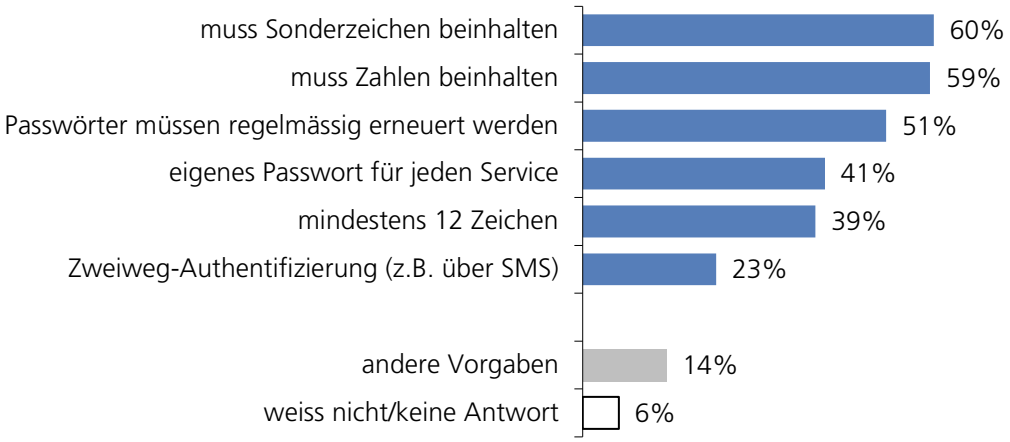
Frage 21:
Gibt es für Ihre Mitarbeitenden Vorgaben für den Umgang mit Passwörtern?
Basis: Total, n = 503



Von den Firmen, bei denen es Passwortregeln gibt, verlangen rund drei Fünftel Sonderzeichen (60 %) und/oder Zahlen (59 %) in den Passwörtern. Bei rund der Hälfte (51 %) müssen die Passwörter regelmässig erneuert werden, rund zwei Fünftel verlangen ein eigenes Passwort pro Service (41 %) und/oder Passwörter mit mindestens 12 Zeichen (39 %). Eine Zweiweg-Authentifizierung ist die seltenste Regel; es gibt sie nur bei rund einem Viertel (23 %) der Firmen, welche Passwortregeln haben.

Durchschnittlich werden 2.9 Passwortregeln genannt.

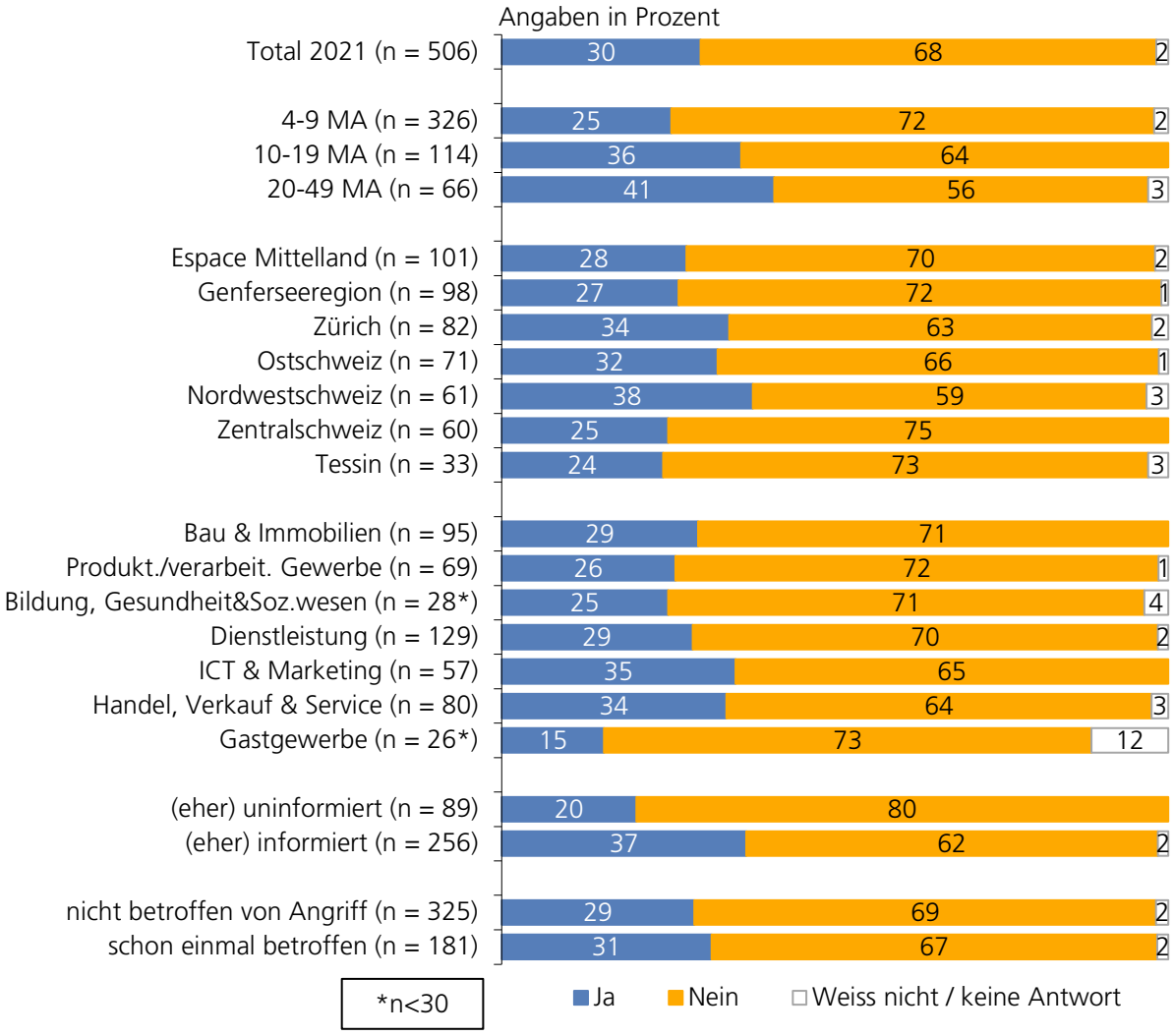
Frage 22:
Um was für Vorgaben handelt es sich dabei?
Basis: Wenn es für Mitarbeitende Vorgaben für den Umgang mit Passwörtern gibt, n = 309, geschlossene Frage mit vorgelesenen Antwortkategorien



3.3.11 Budget

Rund ein Drittel der Befragten (30 %) verfügt über ein IT-Sicherheitsbudget. Je grösser das Unternehmen, desto eher wird ein eigenes IT-Sicherheitsbudget erstellt: Bei 4 bis 9 Mitarbeitenden ist es ein Viertel (25 %), bei 10 bis 19 Mitarbeitenden rund ein Drittel (36 %) und bei 20 bis 49 Mitarbeitenden sind es rund zwei Fünftel (41 %), die ein eigenes Budget für IT-Sicherheit haben.

Frage 23:
Haben Sie ein eigenes Budget für IT-Sicherheit?
Basis: Total, n=506



Geschäftsführende, die sich im Thema Cyberrisk (eher) gut informiert fühlen, haben signifikant häufiger ein IT-Sicherheitsbudget (37 %) als solche, die sich (eher) schlecht informiert fühlen (20 %). Zwischen bereits einmal von einem Cyberangriff betroffenen (31 %) und nicht betroffenen (29 %) gibt es allerdings keinen Unterschied.

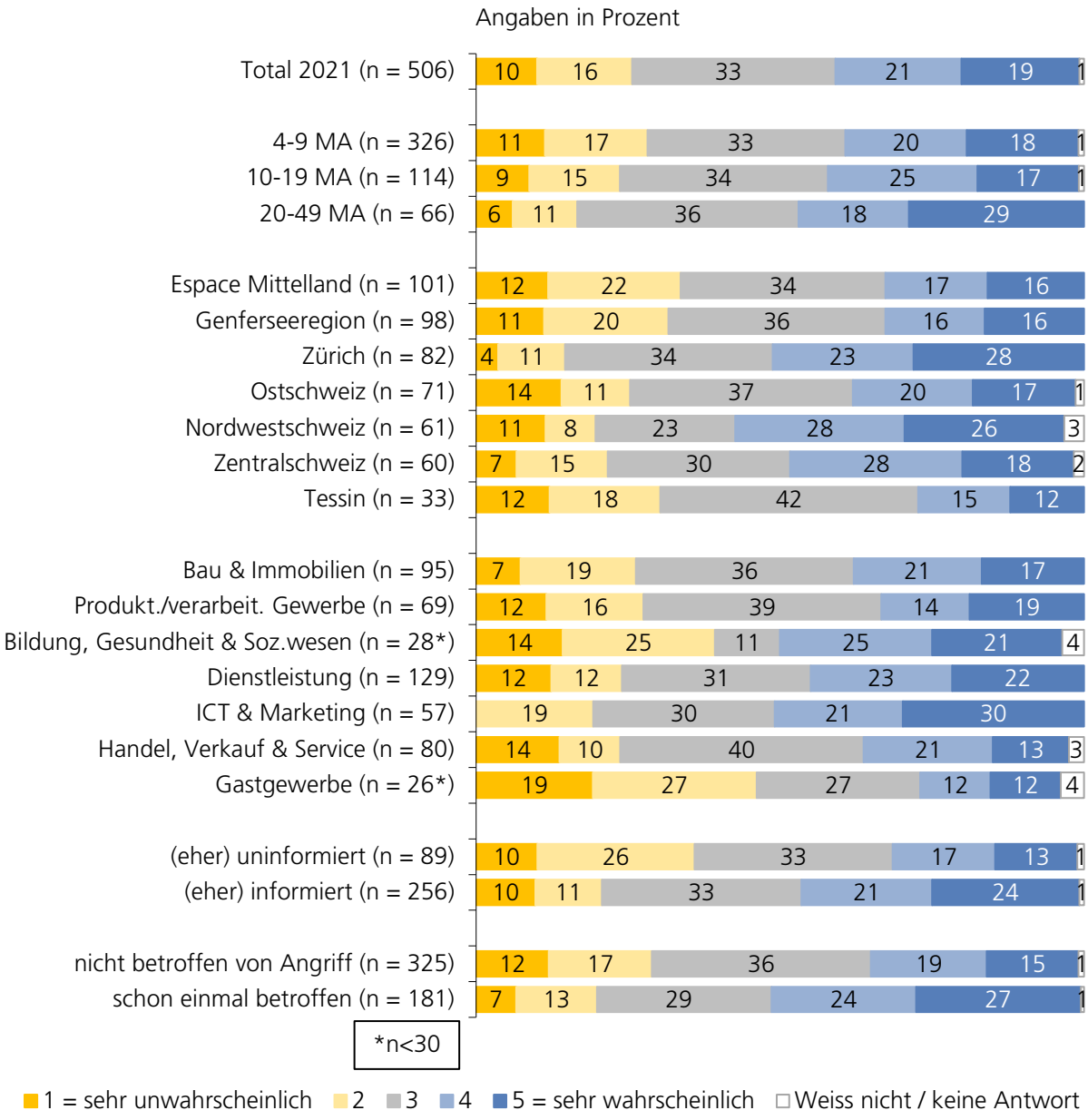
Bei den Unternehmen mit hoher Sicherheitsmassnahmenumsetzung besteht signifikant häufiger ein eigenes IT-Sicherheitsbudget (techn: 42 %, organ: 62 %) als bei Unternehmen mit tiefer Massnahmenumsetzung (techn: 9 %, organ: 15 %).

3.3.13 Geplante Erhöhung der Sicherheitsmassnahmen

Frage 24:
Wie wahrscheinlich ist es, dass Sie in den kommenden 1 bis 3 Jahren die Sicherheitsmassnahmen gegen Cyberkriminalität erhöhen werden?
Basis: Total, n=506

Rund ein Fünftel (19 %) der Befragten hält es für sehr wahrscheinlich (Skalenwert 5 von 5), dass er die Cyber-Sicherheitsmassnahmen in den kommenden ein bis drei Jahren erhöhen wird. Rund ein weiteres Fünftel (21 %) hält es für eher wahrscheinlich (Skalenwert 4). Rund ein Viertel (26 %) hält es für eher oder sehr unwahrscheinlich, ein Drittel (33 %) hat keine klare Meinung.
Je grösser das Unternehmen ist, desto eher werden Erhöhungen der Sicherheitsmassnahmen erwogen: Bei 4 bis 9 Mitarbeitenden sind es knappe zwei Fünftel (38 %), bei 10 bis 19 Mitarbeitenden etwas mehr als zwei Fünftel (42 %) und bei 20 bis 49 Mitarbeitenden knapp die Hälfte (47 %), welche eine Verbesserung der Massnahmen in ein bis drei Jahren für eher oder sehr wahrscheinlich halten (Unterschiede nicht signifikant).

(Eher) informierte (45 %), Pioniere (48 %), Early Follower (46 %) und bereits von einem Cyberangriff betroffene (51 %) gehen signifikant häufiger von einer Erhöhung der Sicherheitsmassnahmen aus als (eher) uninformierte (30 %), Late Follower (30%) und nicht von Cyberangriff betroffene Befragte (34 %).


Angaben in Prozent
Total 2021 (n = 506) 10 16 33 21 19 1
4-9 MA (n = 326) 11 17 33 20 18 1
10-19 MA (n = 114) 9 15 34 25 17 1
20-49 MA (n = 66) 6 11 36 18 29
Espace Mittelland (n = 101) 12 22 34 17 16
Genferseeregion (n = 98) 11 20 36 16 16
Zürich (n = 82) 4 11 34 23 28
Ostschweiz (n = 71) 14 11 37 20 17 1
Nordwestschweiz (n = 61) 11 8 23 28 26 3
Zentralschweiz (n = 60) 7 15 30 28 18 2
Tessin (n = 33) 12 18 42 15 12
Bau & Immobilien (n = 95) 7 19 36 21 17
Produkt./verarbeit. Gewerbe (n = 69) 12 16 39 14 19
Bildung, Gesundheit & Soz.wesen (n = 28*) 14 25 11 25 21 4
Dienstleistung (n = 129) 12 12 31 23 22
ICT & Marketing (n = 57) 19 30 21 30
Handel, Verkauf & Service (n = 80) 14 10 40 21 13 3
Gastgewerbe (n = 26*) 19 27 27 12 12 4
(eher) uninformiert (n = 89) 10 26 33 17 13 1
(eher) informiert (n = 256) 10 11 33 21 24 1
nicht betroffen von Angriff (n = 325) 12 17 36 19 15 1
schon einmal betroffen (n = 181) 7 13 29 24 27 1
*n<30
1 = sehr unwahrscheinlich
2
3
4
5 = sehr wahrscheinlich
Weiss nicht / keine Antwort

3.4 Datenschutz

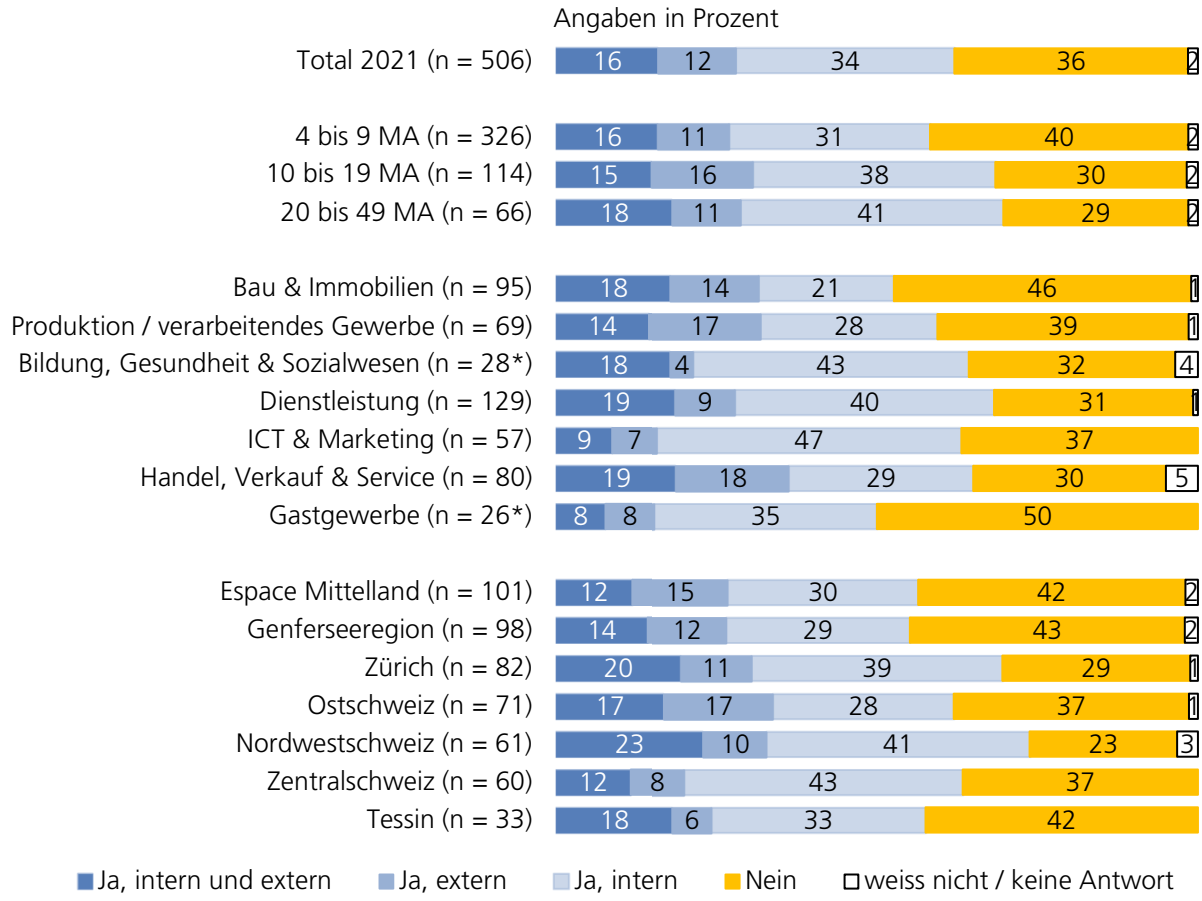
Schutz vor Cyberangriffen und Datenschutz hängen eng zusammen, wird doch bei Cyberangriffen oftmals der Datenschutz durch Diebstahl oder illegale Veröffentlichung verletzt. Vor diesem Hintergrund und auch aufgrund der anstehenden Gesetzesänderung wurden in der 2021er-Studie neue Fragen zum Thema Datenschutz gestellt.

3.4.1 Verantwortlicher für Datenschutz

Frage 25:
Haben Sie in Ihrem Unternehmen einen Datenschutzverantwortlichen bestimmt?
Basis: Total, n=506

Rund zwei Drittel (62 %) der befragten Unternehmen haben einen Datenschutzverantwortlichen bestimmt; entweder intern (34 %), extern (12 %) oder sowohl als auch (16 %). Zwischen den Unternehmensgrössenkategorien gibt es keine signifikanten Unterschiede; tendenziell hat aber die kleinste Unternehmensgrössenkategorie (4-9 Mitarbeitende) seltener einen Datenschutzverantwortlichen (40 % «nein») als die mittlere (10-19 Mitarbeitende: 30 % «nein») und die grösste Kategorie (20-49 Mitarbeitende: 29 % «nein»).

Zwischen den Branchen und den Grossregionen gibt es keine signifikanten Unterschiede.



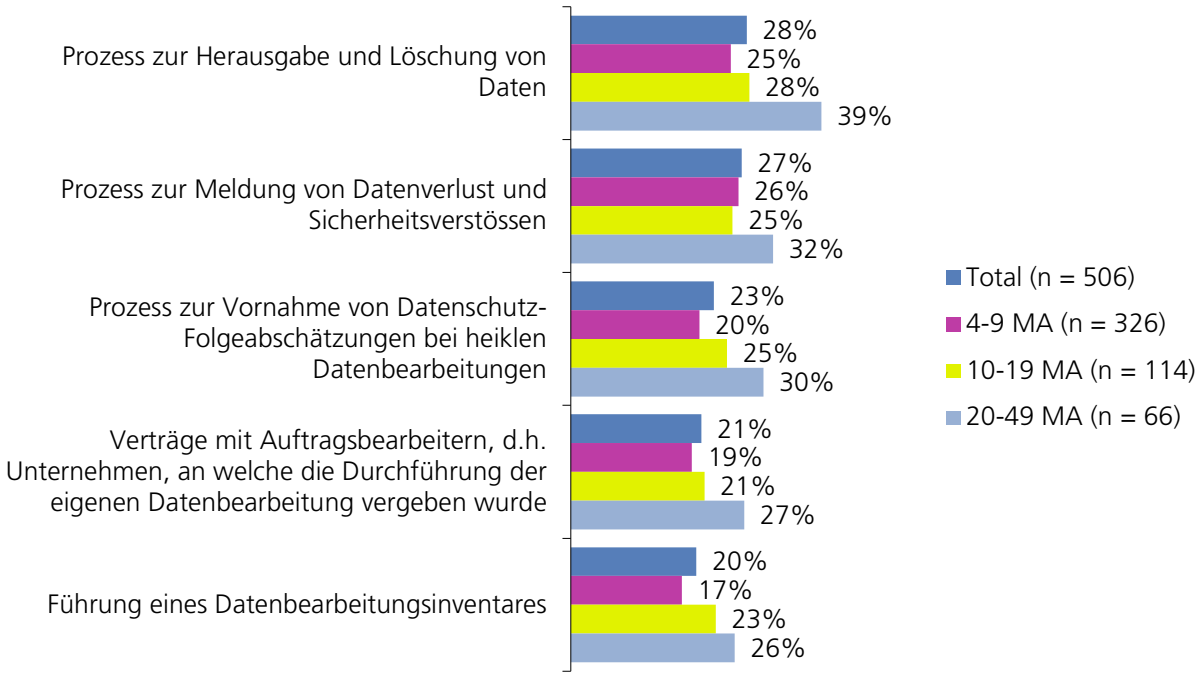
Wer sich (eher) gut informiert fühlt bezüglich dem Thema Cyberrisk, hat auch signifikant häufiger einen Datenschutzverantwortlichen (69 %) als diejenigen, die sich (eher) schlecht informiert fühlen (47 %). Es kann deshalb sein, dass hier ein Zusammenhang zwischen den Themen Cyberrisk und Datenschutz zum Vorschein kommt.

3.4.2 Neues Datenschutzgesetz

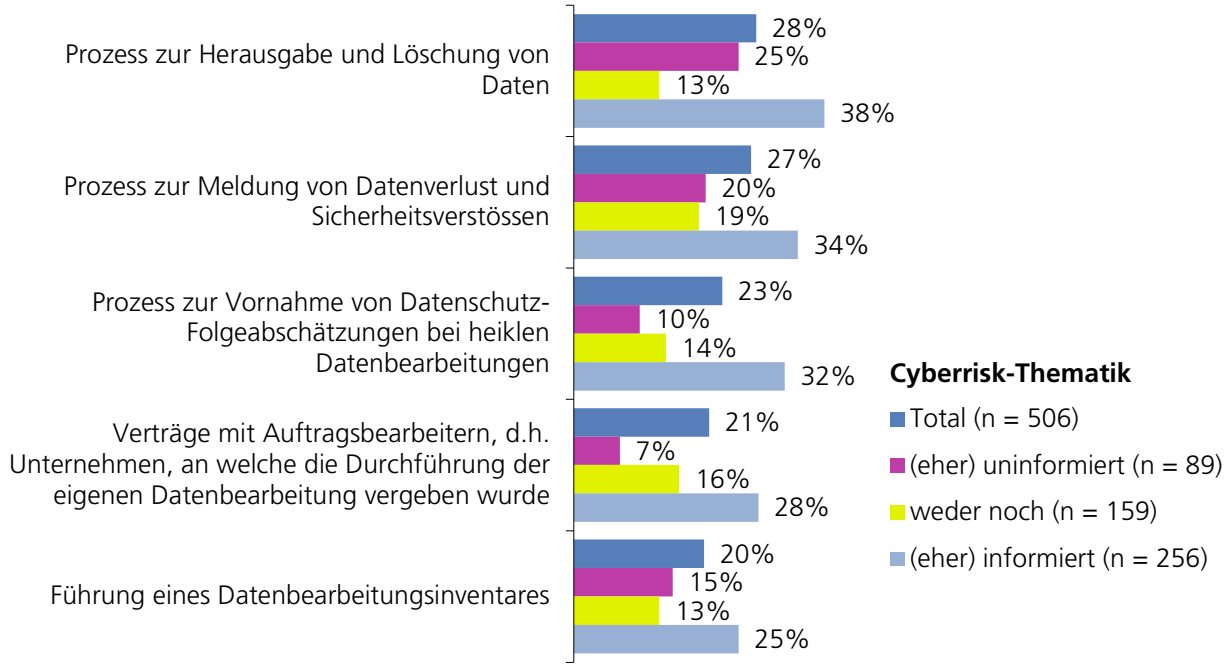
Frage 26:
In rund 1-2 Jahren tritt das neue Datenschutzgesetz in Kraft. Haben Sie die folgenden Anforderungen daraus schon umgesetzt?
Basis: Total, n=506

Drei der fünf abgefragten Anforderungen des sich aktuell in der Vernehmlassung befindenden neuen Datenschutzgesetzes wurde von rund einem Viertel der Befragten bereits umgesetzt: Der Prozess zur Herausgabe und Löschung von Daten (28 %), der Prozess zur Meldung von Datenverlust und Sicherheitsverstössen (27 %) und der Prozess zur Vornahme von Datenschutz-Folgeabschätzungen bei heiklen Datenbearbeitungen (23 %). Die weiteren zwei Anforderungen wurden von rund einem Fünftel der Unternehmen umgesetzt: Verträge mit Auftragsbearbeitern bezüglich der Durchführung der eigenen Datenbearbeitung (21 %) und die Führung eines Dateninventars (20 %).

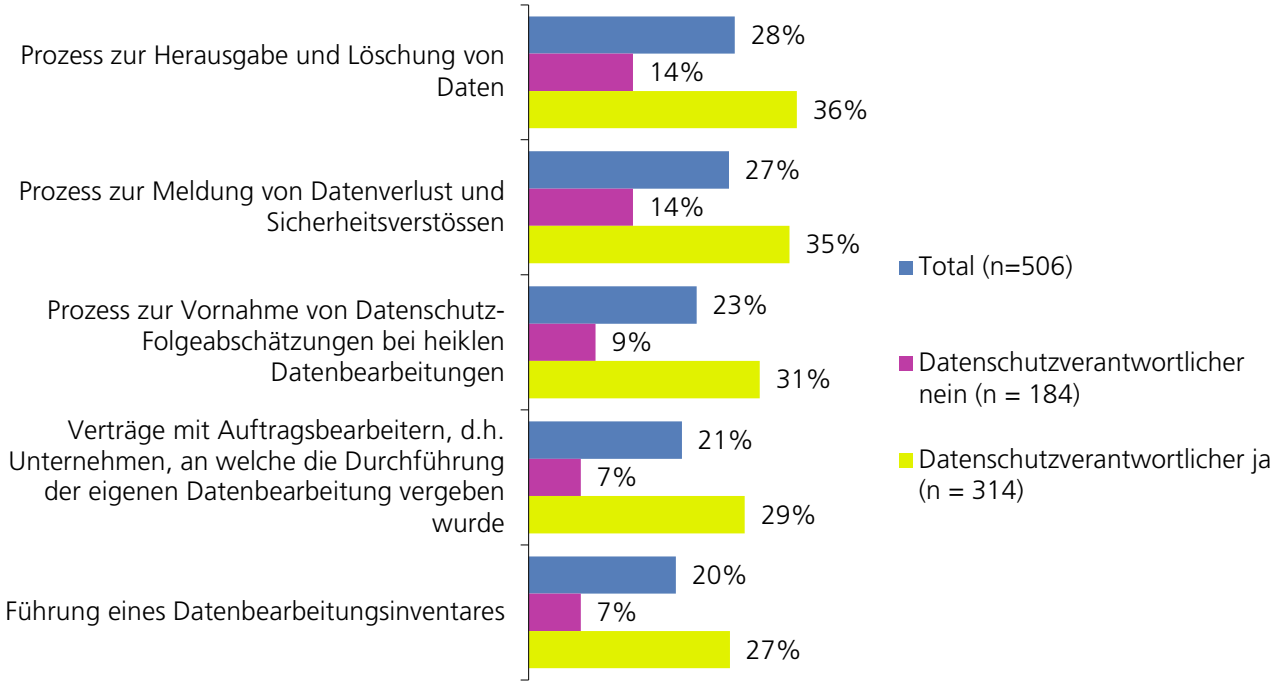
Zwischen den Branchen und Regionen fallen keine Unterschiede auf. Hinsichtlich der Unternehmensgrösse zeigt sich ebenfalls lediglich eine Tendenz: Alle Anforderungen des neuen Gesetzes wurden von der grössten Unternehmenskategorie (20-49 Mitarbeitende) am ehesten umgesetzt (nicht signifikant).



Unternehmensführende mit einem hohen Informationsgrad bezüglich der Cyberrisk-Thematik haben sämtliche Anforderungen signifikant häufiger umgesetzt als Unternehmensführende mit einem tiefen Informationsgrad. Besonders gross ist die Differenz bei den Gesetzesanforderungen «Prozess zur Datenschutz-Folgeabschätzung bei heiklen Datenbearbeitungen» (informiert: 32 %, uninformiert: 10 %) und dem Abschluss von «Verträgen mit Auftragsbearbeitern bezüglich der Durchführung der eigenen Datenbearbeitung» (informiert: 28 %, uninformiert: 7 %).



Auch die Tatsache, ob ein Unternehmen einen Datenschutzverantwortlichen hat oder nicht, führt zu signifikanten Unterschieden bei sämtlichen abgefragten Gesetzesanforderungen. Die Differenz ist bei allen Anforderungen sehr ähnlich und liegt zwischen 20 und 22 Prozentpunkten.



4 Studiendesign in Kürze

Auftraggeber:	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:	506 durchgeführte Interviews
Gewichtung:	Keine
Quoten	proportional nach Unternehmensgrössen (4-9, 10-19, 20-49) und Grossregion
Interviewdauer:	18 Minuten
Sprachen:	Deutsch, Französisch, Italienisch.
Auswertung:	Tabellenband Grafiken Berichterstattung
Feldphase:	16. Juni bis 27. Juli 2021
Projektleiterin gfs-zürich:	Karin Mändli Lerch
Projektmitarbeiterin:	Mara Tanner