YouGov

Switzerland

Cyberstudie 2024

Report erstellt durch YouGov für digitalswitzerland

August 2024

Living consumer intelligence | business.yougov.com

digitalswitzerland

Inhalt

01 Studiendesign

Projektteam

Kristof A. Hertig
Senior Project Manager
digitalswitzerland, Zürich
kristof@digitalswitzerland.com

Patric Vifian
Marketing Manager
Die Mobiliar, Bern
patric.vifian@mobi.ch

Andreas W. Kaelin
Senior Advisor digitalswitzerland, Zürich
Mitgründer und Geschäftsführer Allianz Digitale Sicherheit Schweiz ADSS, Zug
andreas.kaelin@digitalsecurity switzerland.ch

Prof. Dr. Marc K. Peter
Leiter Kompetenzzentrum Digitale Transformation
FHNW Hochschule für Wirtschaft, Olten
marc.peter@fhnw.ch

Katja Dörlemann
Präsidentin
Swiss Internet Security Alliance (SISA), Zürich
katja.doerlemann@swiss-internet-security-alliance.ch

Nicole Wettstein
Leiterin Schwerpunktprogramm Cybersecurity
Schweizerische Akademie der Technischen Wissenschaften SATW, Zürich
nicole.wettstein@satw.ch

Studiendesign

Kunde: Die Mobiliar (Patric Vifian)
digitalswitzerland (Kristof Hertig)
Allianz digitale Sicherheit Schweiz (Andreas W. Kaelin)
Fachhochschule Nordwestschweiz FHNW (Marc K. Peter)
Schweizerischen Akademie der Technischen Wissenschaften SATW (Nicole Wettstein)
Swiss Internet Security Alliance SISA (Katja Dörlemann)

YouGov: Karin Mändli Lerch | Senior Consultant
Susanne Vontobel | Head of Financial Market Research

Studienziel: Erhebung der Einstellung von Schweizer KMU, IT-Dienstleistungsunternehmen und der Bevölkerung zum Thema Cyberkriminalität

Erhebungsphase: 4. Juli bis 5. August 2024

Zielgruppe: KMU mit 1 bis 49 Mitarbeitenden (Personen, die in ihrem Unternehmen alleine oder gemeinsam mit anderen Personen Entscheidungen in Bezug auf die Unternehmensstrategie treffen.)

IT-Dienstleister (NOGA Codes: 620200: Erbringung von Beratungsleistungen auf dem Gebiet der Informationstechnologie, 620300: Betrieb von Datenverarbeitungsanlagen für Dritte, 620900: Erbringung von sonstigen Dienstleistungen der Informationstechnologie, 631100: Datenverarbeitung, Hosting und damit verbundene Tätigkeiten)

Bevölkerung 18 bis 79 Jahre

Studiendesign

Anzahl Interviews: KMU: n = 526 Interviews
IT-Dienstleister: n = 401 Interviews
Bevölkerung: n = 1‘247 Interviews

Befragungsmethode: Online-Fragebogen

Einladungsverfahren: KMU: postalischer Versand mit eingekauften Adressen und YouGov Internet-Panel*
IT-Dienstleister: postalischer Versand mit eingekauften Adressen
Bevölkerung: YouGov Internet-Panel*

Gewichtung:

Die **KMU-Stichprobe** wurde mittels Adressvorschichtung (Sektoren II und III) und Quoten nach Firmengrösse (Mitarbeitende: 1 – 3, 4 – 9, 10 – 19, 20 – 49) und Sprachregion disproportional erhoben und anschliessend proportional gewichtet. Die Tabelle auf der folgenden Seite zeigt die Verteilung der Interviews im Vergleich zur Verteilung der untersuchten Unternehmensgrössen in der Schweiz, nach der die Daten gewichtet wurden.

IT-Dienstleister: Keine Gewichtung

Die **Bevölkerungsstichprobe** wurde nach vier Altersgruppen (18 – 29, 30 – 39, 40 – 64, 65 – 79), Geschlecht und Sprachregion quotiert, wobei das Tessin überproportional befragt und anschliessend gewichtet wurde. Die Gewichtungstabelle befindet sich auf der nächsten Seite.

* mit 115'000 validierten, aktiven Mitgliedern

Studiendesign

Gewichtung KMU-Stichprobe

	Erhobene Stichprobe (disproportional)		Repräsentative Gewichtung gem. STATENT 2021 (proportional)	
1 – 3 MA	165	31%	392	74%
4 – 9 MA	174	33%	86	16%
10 – 19 MA	96	18%	30	6%
20 – 49 MA	91	17%	17	3%
D-CH	363	69%	363	69%
W-CH	116	22%	132	25%
Tessin	47	9%	32	6%
Total (gerundet)	526	100%	526	100%

Die durch die Stichprobe abgebildete Grundgesamtheit umfasst **rund 613‘600 Firmen** mit 1 bis 49 Mitarbeitenden (bfs STATENT; 2021) in allen Landesteilen. Das Vertrauensintervall der Gesamtstichprobe liegt bei +/- 4.4 Prozentpunkte bei einer Sicherheit von 95 Prozent (50/50 Verteilung). Die Erhebung zeigt ein bezüglich den Firmengrössen und Sprachregionen strukturgleiches Abbild der Grundgesamtheit, die Ergebnisse sind somit unter Berücksichtigung des Vertrauensintervalls auf die Grundgesamtheit extrapolierbar.

Gewichtung Bevölkerungsstichprobe

	Erhobene Stichprobe (disproportional)		Repräsentative Gewichtung (proportional)	
Männer	612	49%	636	51%
Frauen	635	51%	611	49%
18-29	201	16%	200	16%
30-39	222	18%	212	17%
40-64	524	42%	536	43%
65-79	300	24%	299	24%
D-CH	761	61%	889	71%
W-CH	272	22%	306	24%
Tessin	214	17%	52	4%
Total (gerundet)	1247	100%	1247	100%

Die Erhebung zeigt ein bezüglich Alter, Geschlecht und Sprachregionen strukturgleiches Abbild der Grundgesamtheit, die Ergebnisse sind somit unter Berücksichtigung des Vertrauensintervalls (+/- 2.8 Prozentpunkte bei 50/50 Verteilung und einer Sicherheit von 95%) auf die Grundgesamtheit extrapolierbar.

02 Stichproben-struktur

Stichprobenstruktur (gewichtet)

Zielgruppe 1: KMU

Total	**526**
Entscheider	
Ja, alleine	292
Ja, gemeinsam mit anderen Personen	234
Nein	0
Funktion	
Firmeninhaber	275
Freie Berufe	54
Selbständige	115
Leitende Angestellte / Beamte	82
Übrige Angestellte / Beamte / Vertreter	0
Facharbeiter mit Lehre	0
Ungelernte / angelernte Arbeiter	0
In Ausbildung	0
Hausfrau/Hausmann	0
Nicht berufstätig	0
Arbeitslos	0
Pensioniert	0
Mitarbeitende	
1-3 Mitarbeiter	392
4-9 Mitarbeiter	86
10-19 Mitarbeiter	30
20-49 Mitarbeiter	17
Sprachregion	
D-CH	363
W-CH	132
TI	32
lat CH	163

Total	**526**
Branche	
Land-, Forstwirtschaft, Gartenbau, Fischerei	0
Industrie / Verarbeitung & Herstellung von Waren	48
Baugewerbe	79
Chemie / Pharma / Biotechnologie	6
Energie	5
Grosshandel	18
Detailhandel	26
Handel / Reparatur	35
Bank-, Kredit-, Finanzwesen	36
Versicherungen	9
Verkehr, Lagerei, Logistik	2
Kommunikation	15
Informatik	26
Gastgewerbe / Tourismus	13
Unterhaltung, Kultur, Kunst, Erholung, Sport	7
Immobilien	34
Wirtschaftliche, technische oder wissensch. DL	31
Bildungswesen	3
Gesundheitswesen	38
Sozialwesen	10
Architektur- und Ingenieurbüro	60
Öffentliche Verwaltung, öffentliche Hand	0
Andere Dienstleistungen	19
Einstellung	
Pioniere	24
Early Follower	216
Late Follower	236

Stichprobenstruktur (gewichtet)

Zielgruppe 2: IT-Dienstleister

Total	**401**
Mitarbeitende	
1-9 Mitarbeiter	288
10+ Mitarbeiter	113
Sprachregion	
D-CH	320
W-CH	58
TI	23
Funktion	
Firmeninhaber/in	311
Geschäftsführer/in	253
Entwicklung, Anpassung, Testen / Pflege Software	143
Planung und Entwurf von Computersystemen	147
Verwaltung und Betrieb der Computersysteme	137
Sonstige fachliche und technische Tätigkeiten	113
Anderes	31
Kundenstamm	
Privatpersonen	118
KMU mit 1-9 Mitarbeitenden	217
KMU mit 10-49 Mitarbeitenden	226
KMU mit 50-250 Mitarbeitenden	192
Firmen mit über 250 Mitarbeitenden	199

Total	**401**
Regionalität	
Lokal	170
Regional	225
National	245
International	152
Einstellung	
Pioniere	121
Early Follower	205
Late Follower	43
IT-Sicherheitszertifikat	
Ja	39

Stichprobenstruktur (gewichtet)

Zielgruppe 3: Bevölkerung

Total	**1'247**
Geschlecht	
Männer	**636**
Frauen	**611**
Alter	
18-29 Jahre	**200**
30-39 Jahre	**212**
40-64 Jahre	**536**
65-79 Jahre	**299**
Sprachregion	
D-CH	**889**
W-CH	**306**
TI	**52**
Einstellung	
Pioniere	**101**
Early Follower	**582**
Late Follower	**524**

03 KMU-Befragung

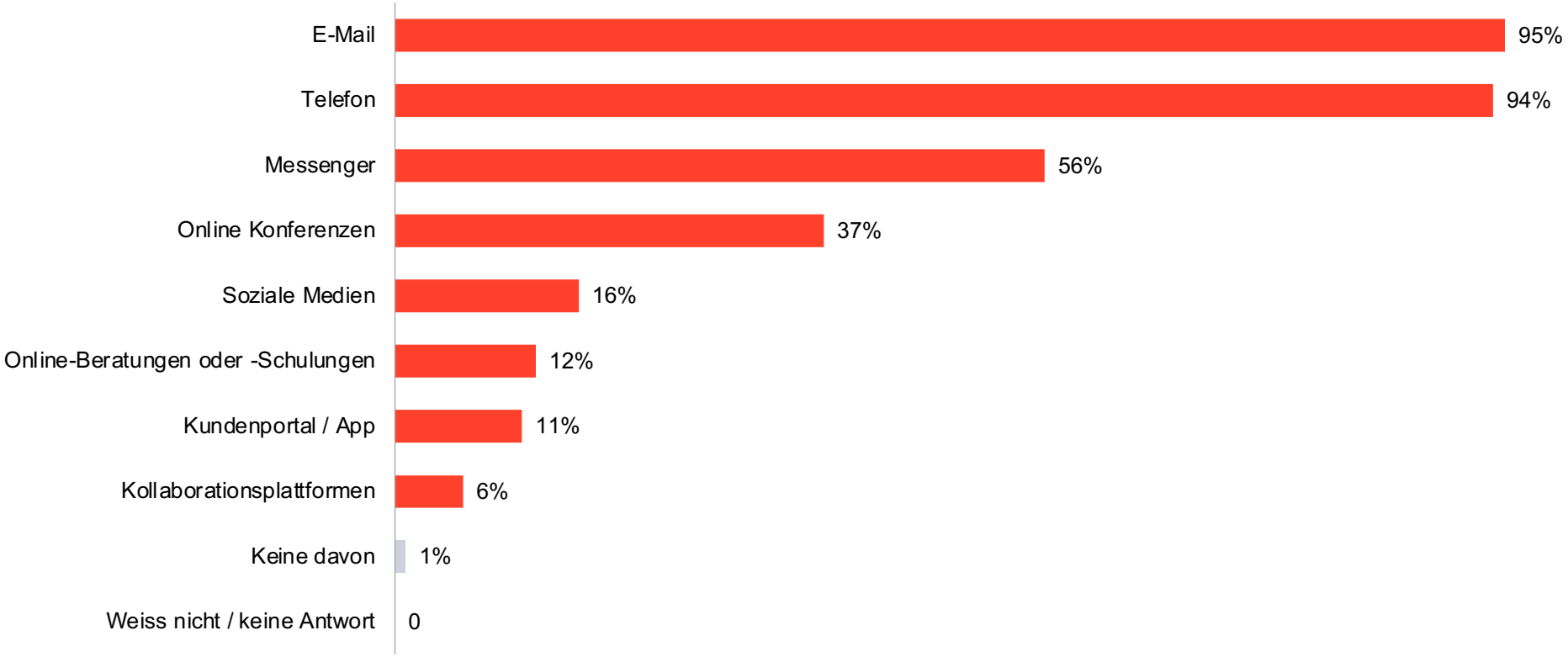
Branche und Firmengrösse

	Gesamt	1-3	4-9	10-19	20-49
Ungewichtete Basis Netto	526	165	174	96	91
Basis Netto	526	392	86	30	17
Baugewerbe (Hoch-, Tiefbau, Baunebengewerbe	15%	14%	19%	19%	11%
Architektur- und Ingenieurbüro	11%	11%	12%	10%	10%
Industrie / Verarbeitung und Herstellung von Waren	9%	9%	9%	13%	15%
Gesundheitswesen	7%	7%	7%	6%	6%
Bank-, Kredit-, Finanzwesen	7%	7%	7%	4%	5%
Handel / Reparatur (Motorfahrzeuge, Maschinen, …)	7%	6%	12%	8%	5%
Immobilien	6%	7%	5%	2%	2%
Wirtschaftliche, technische oder wissenschaftliche DL	6%	7%	4%	4%	3%
Detailhandel	5%	4%	8%	7%	4%
Informatik	5%	6%	2%	2%	8%
Andere Dienstleistungen (Friseursalon, Entsorgung, …)	4%	4%	1%	2%	3%
Grosshandel	3%	2%	5%	10%	5%
Kommunikation (Medien, Telekommunikation, Agentur, Marketing, ...)	3%	3%	2%	3%	-
Gastgewerbe / Tourismus	2%	3%	-	1%	1%
Sozialwesen	2%	2%	1%	3%	5%
	2%	2%	1%	-	3%
Unterhaltung, Kultur, Kunst, Erholung, Sport	1%	1%	2%	-	1%
Chemie / Pharma / Biotechnologie	1%	1%	2%	1%	2%
Energie	1%	1%	2%	-	7%
Bildungswesen	1%	1%	-	1%	-
Verkehr, Lagerei, Logistik	0%	-	1%	2%	2%
Öffentliche Verwaltung, öff. Hand (Sicherheit, Sozialversicherung, …)	0%	-	-	-	2%
Weiss nicht / keine Antwort	1%	2%	1%		

S05: In welcher Branche ist Ihr Betrieb tätig? / S03 Anzahl Mitarbeitende
Basis: n=526 | Filter: KMU | Geschlossene Frage

Kommunikationsmittel

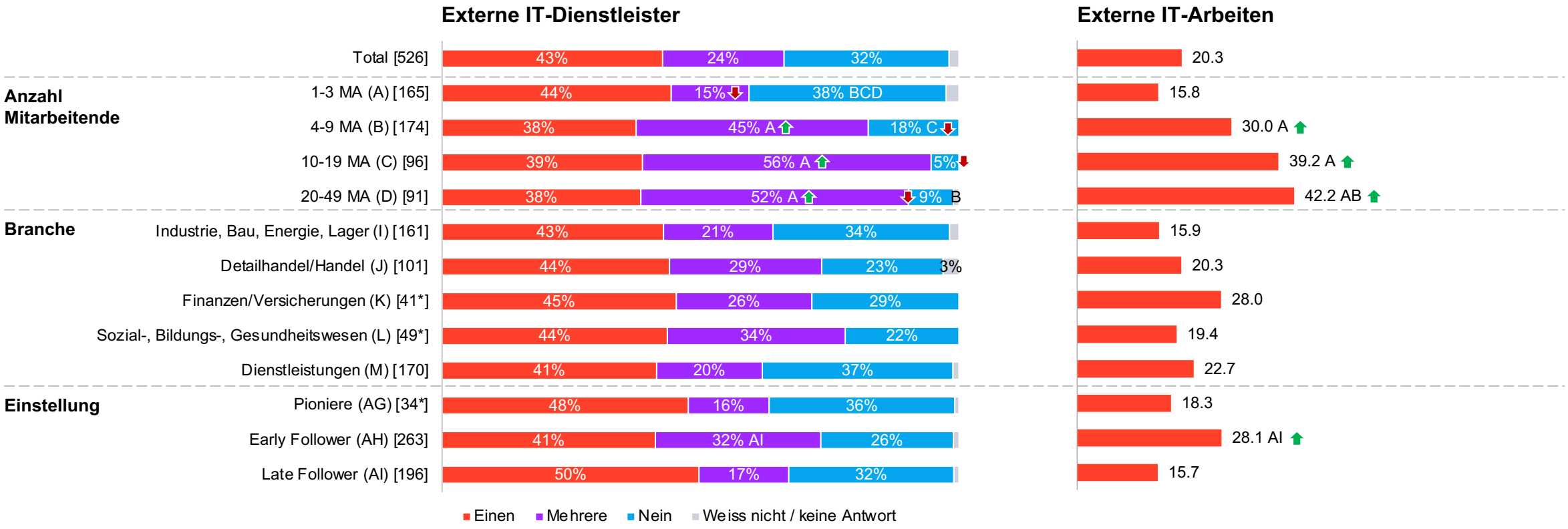
Neben den Haupt-Kommunikationsmitteln Telefon und E-Mail nutzen etwas mehr als die Hälfte der Befragten Messenger-dienste (56%). Unternehmen mit 20 – 49 Mitarbeitenden nutzen Online Konferenzen (73%), Kundenportale (31%) soziale Medien (27%), Online-Beratungen (24%) und Kollaborationsplattformen (23%) signifikant häufiger (nicht abgebildet).



F001: Welche der folgenden Kommunikationsmittel nutzen Ihre Mitarbeitenden aktuell für die Kommunikation mit Partnern, Kundschaft und anderen Mitarbeitenden?
Basis: n=526 | Filter: KMU | Geschlossene Frage

IT-Dienstleister

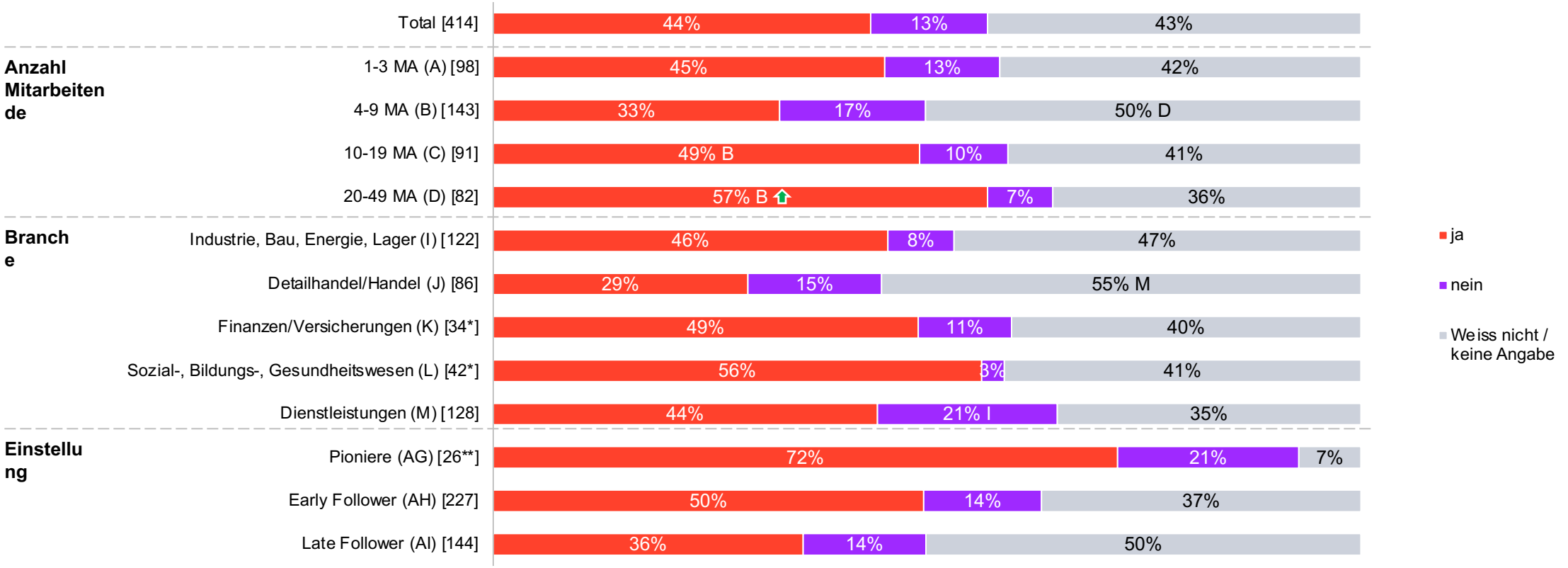
Rund zwei Drittel (67%) der KMU haben einen oder mehrere externe IT-Dienstleister für Informatik, Telefonie, Software- oder Hardware-Arbeiten. Je mehr Mitarbeitende die Unternehmen haben, desto mehr Arbeiten geben sie extern. Im Schnitt werden 20 Prozent der IT-Arbeiten extern gegeben.



F002: Haben Sie einen oder mehrere IT-Dienstleister, d.h. externe Partner für Informatik, Telefonie, Software- oder Hardware-Arbeiten? | F003: Wieviel Prozent der IT-Arbeiten werden bei Ihnen ungefähr von externen Dienstleistern wahrgenommen? | Basis: n=[ ] | Filter: KMU | Geschlossene Frage (F002) & Zahlenfeld (F003) | ↑signifikant höher als Total; ↓ signifkant tiefer als Total | *Kleine Basis <50 | Datenbeschriftung ab 3%
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Zertifikat

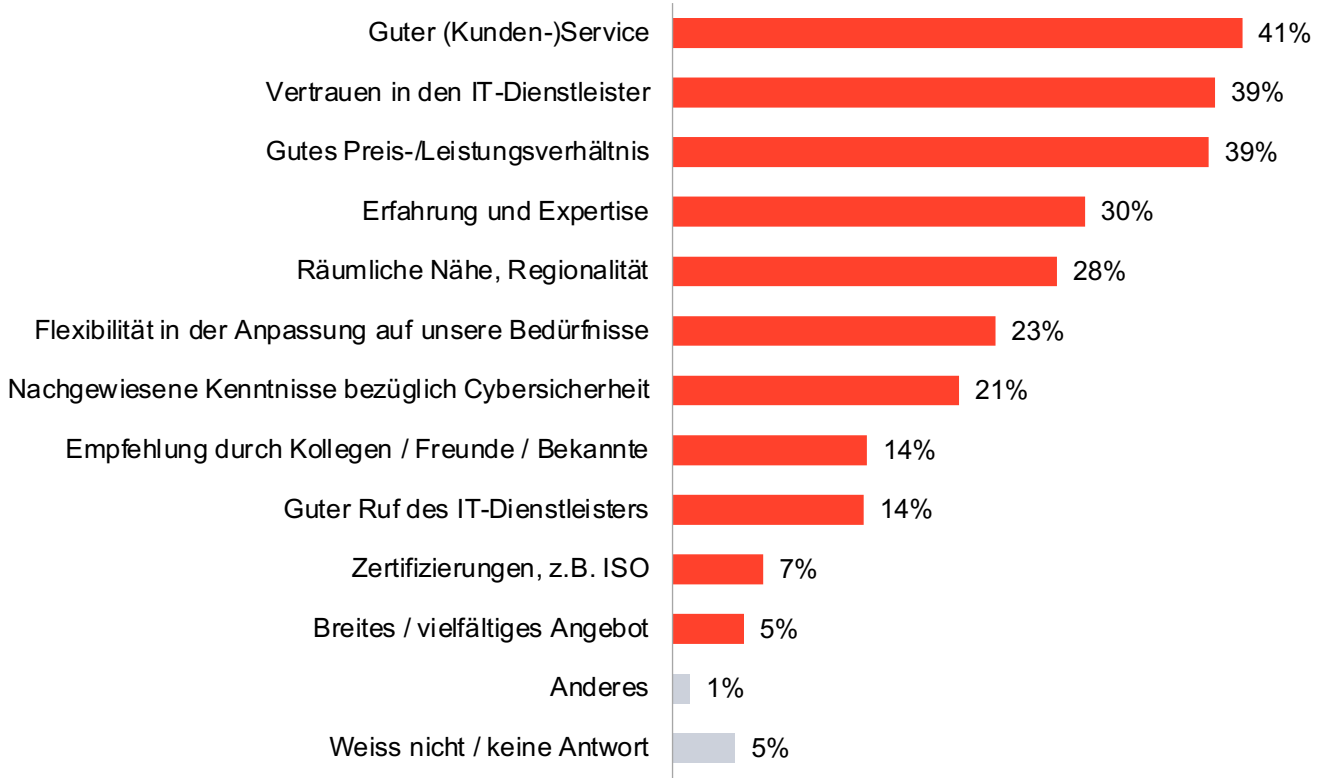
Rund zwei Fünftel (44%) der befragten KMU mit externen IT-Dienstleistern wissen, dass diese über eine IT-Sicherheitszertifizierung wie z.B. ISO 27001 verfügen. Fast genau gleich viele (43%) können diese Frage nicht beantworten.



F004: Verfügt ihr externer IT-Dienstleister über eine IT-Sicherheitszertifizierung (z.B. ISO 27001 oder CyberSeal der Allianz Digitale Sicherheit Schweiz)?
Basis: n=[ ] | Filter: KMU | ⬆ signifikant höher als Total; ⬇ signifkant tiefer als Total | *Kleine Basis <50
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Auswahlkriterien IT-Dienstleister

Wie wichtig die Kriterien für die Auswahl eines IT-Dienstleisters sind, unterscheidet sich nach Region. So ist in der Deutschschweiz das Vertrauen (44%); in der Westschweiz ein gutes Preis-/Leistungsverhältnis (46%) und im Tessin der gute (Kunden-)Service (40%) am wichtigsten (Regionenunterschiede nicht abgebildet).

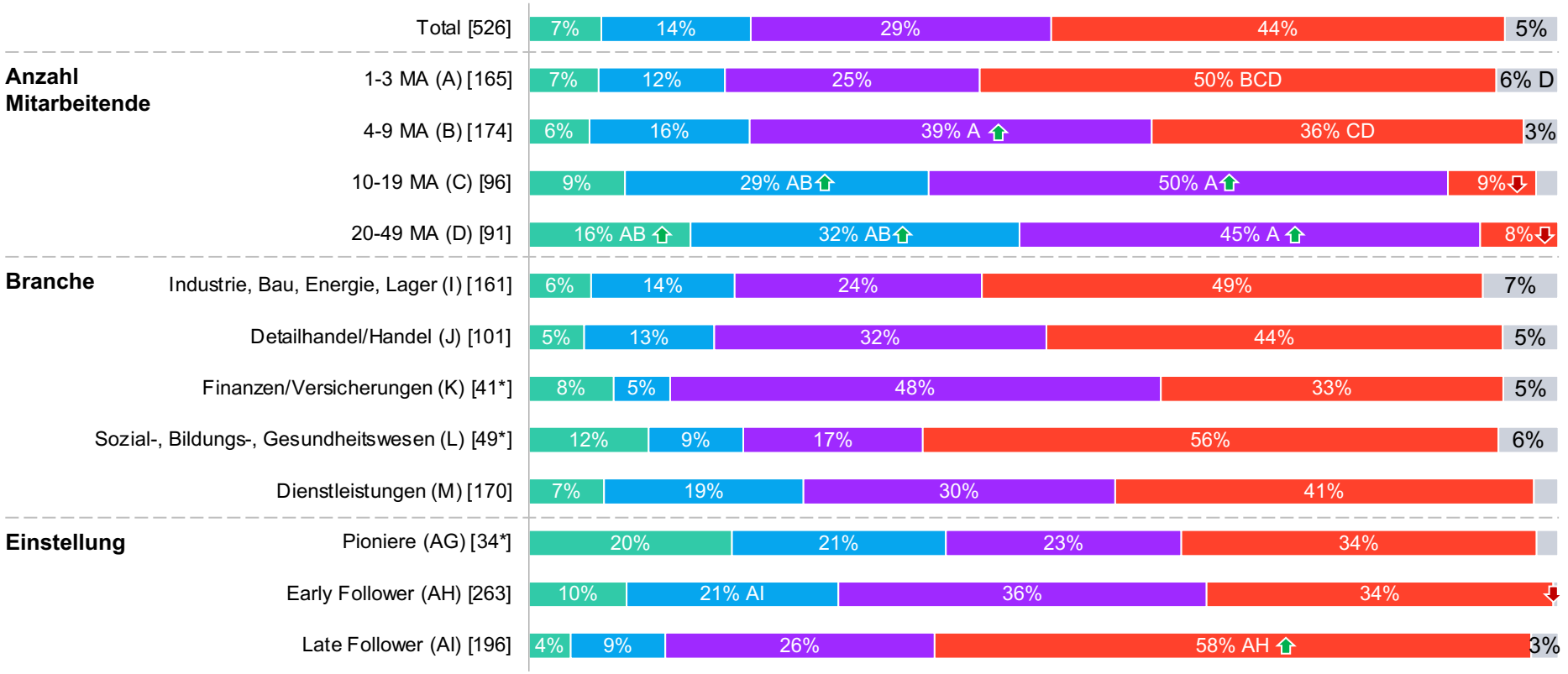


F005: Welche der folgenden Kriterien sind aus Ihrer Sicht für die Auswahl eines IT-Dienstleisters am wichtigsten? Bitte wählen Sie max. 3 Antworten aus.
Basis: n=526 | Filter: KMU | Geschlossene Frage

Aus Sicht der IT-DL…
ist Erfahrung/Expertise am wichtigsten und räumliche Nähe deutlich weniger wichtig (siehe Seite 51).

Cyberrisk-Verantwortung

Die eine Hälfte der befragten KMU haben eine interne oder externe (Teil-)Funktion für Cybersicherheit, die andere Hälfte hat keine solche Funktion oder weiss darüber nicht Bescheid. Je grösser die Unternehmen sind, desto eher haben sie eine Funktion für Cybersicherheit.

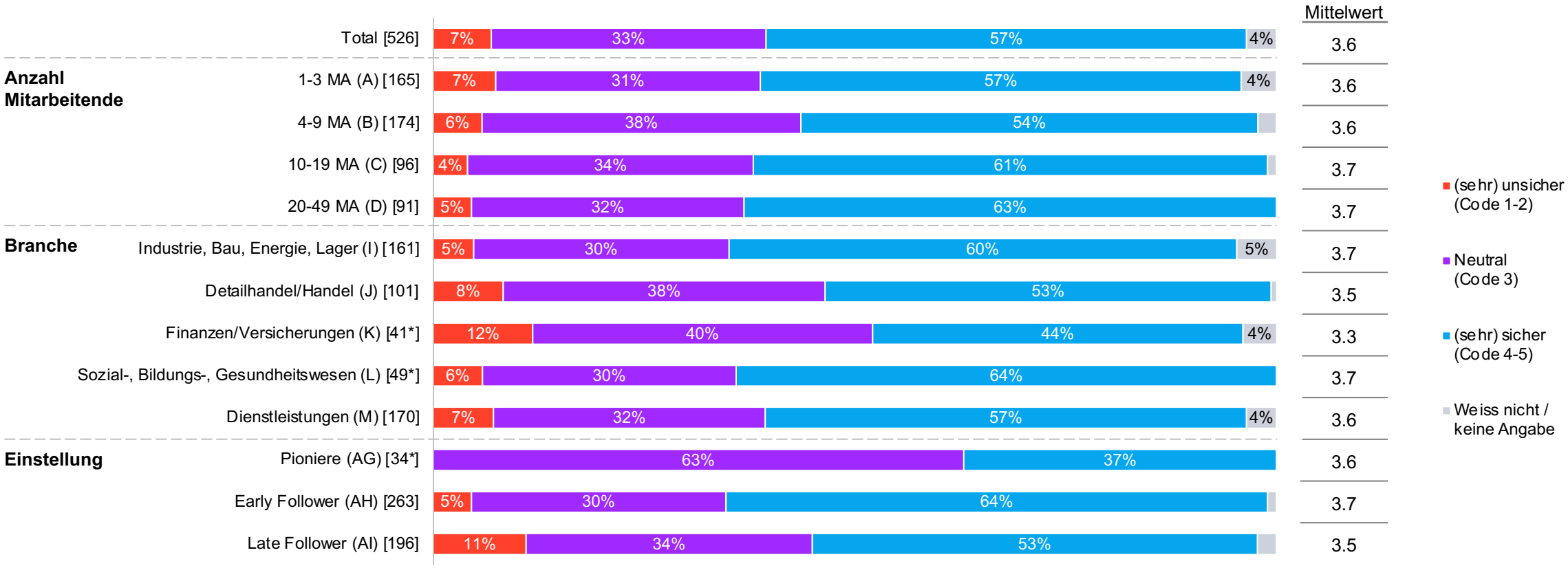


F006: Gibt es in Ihrem Unternehmen eine oder mehrere Personen, die für Cybersicherheit zuständig ist?
Basis: n=[ ] | Filter: KMU | Geschlossene Frage | ⬆ signifikant höher als Total; ⬇ signifkant tiefer als Total | *Kleine Basis <50 | Datenbeschriftung ab 3%
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Aus Sicht der IT-DL…
Die befragten IT-DL sind bei durchschnittlich 36% ihrer Kunden für technische, bei 27% für organisatorische Cybersicherheits-Massnahmen zuständig (siehe S. 71).

Sicherheitsgefühl

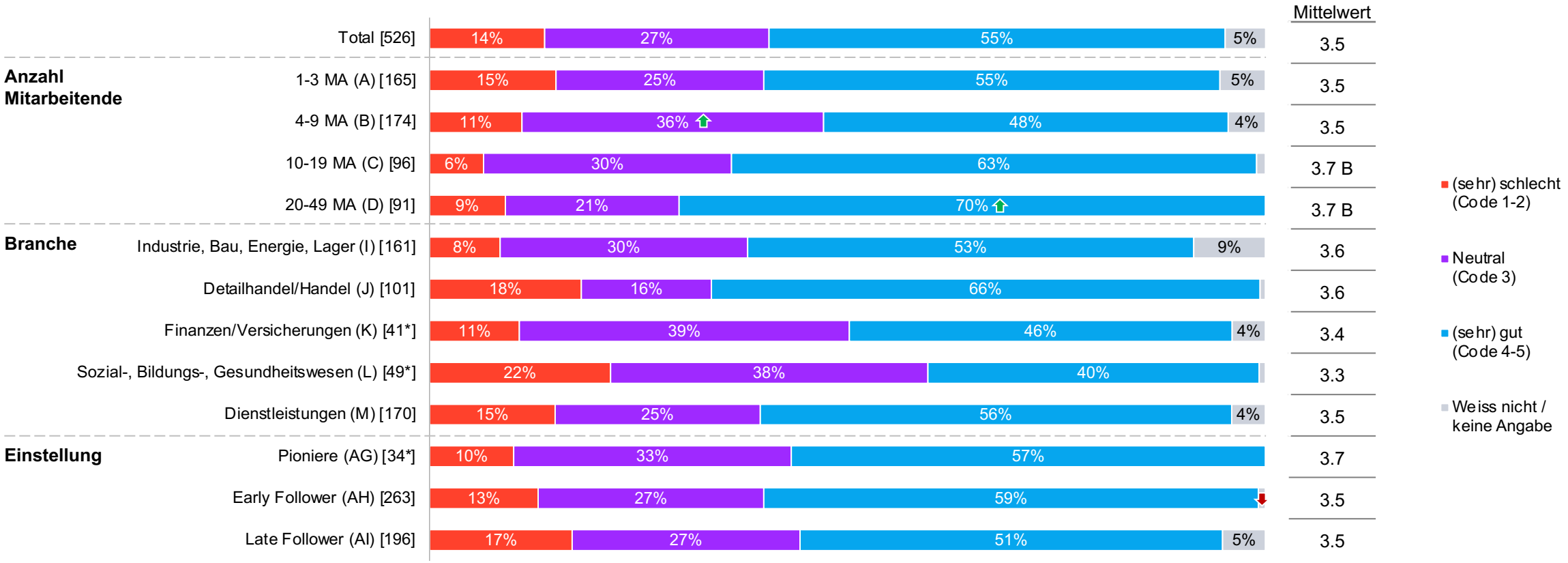
Über die Hälfte der befragten KMU (57%) fühlen sich eher oder sehr sicher vor Cyberkriminalität, nur eine kleine Minderheit (7%) fühlt sich eher oder sehr unsicher.



F007: Wie sicher fühlen Sie sich in Ihrem Unternehmen vor Cyberkriminalität?
Basis: n=[ ] | Filter: KMU | Skalierte Frage: 1= sehr unsicher bis 5= sehr sicher | ▲ signifikant höher als Total; ▼ signifkant tiefer als Total | *Kleine Basis <50 | Datenbeschriftung ab 3%
Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Resilienz

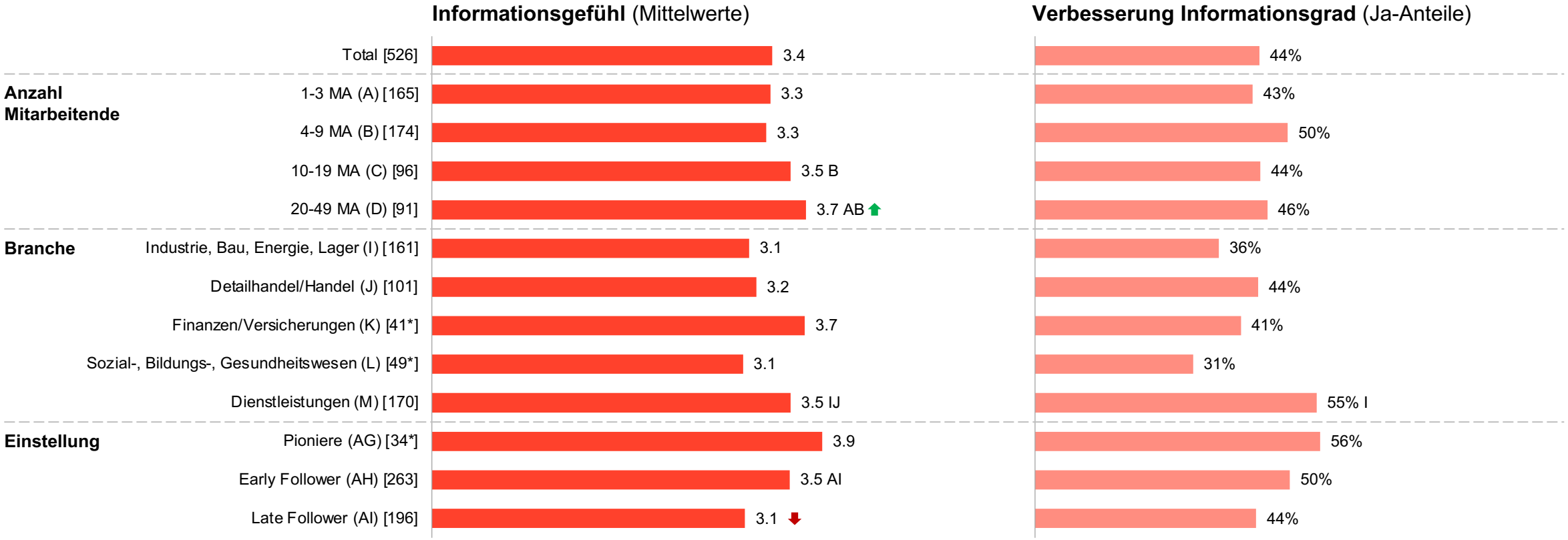
Rund jedes siebte befragte KMU fühlt sich (sehr) schlecht, über die Hälfte (55%) (sehr) gut geschützt bzw. vorbereitet gegen Cyberangriffe. Es fühlen sich somit doppelt so viele Unternehmen (sehr) schlecht geschützt (14%) als (sehr) unsicher (7%, s. vorherige Folie); schlechter Schutz führt also nicht immer zu einem tiefen Sicherheitsgefühl.



F008: Was schätzen Sie: Wie gut sind Sie vor Cyberangriffen geschützt und auf einen Angriff vorbereitet?
Basis: n=[ ] | Filter: KMU | Skalierte Frage: 1= sehr schlecht bis 5= sehr gut | ⬆ signifikant höher als Total; ⬇ signifkant tiefer als Total | *Kleine Basis <50 | Datenbeschriftung ab 3%
Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Informationsgrad

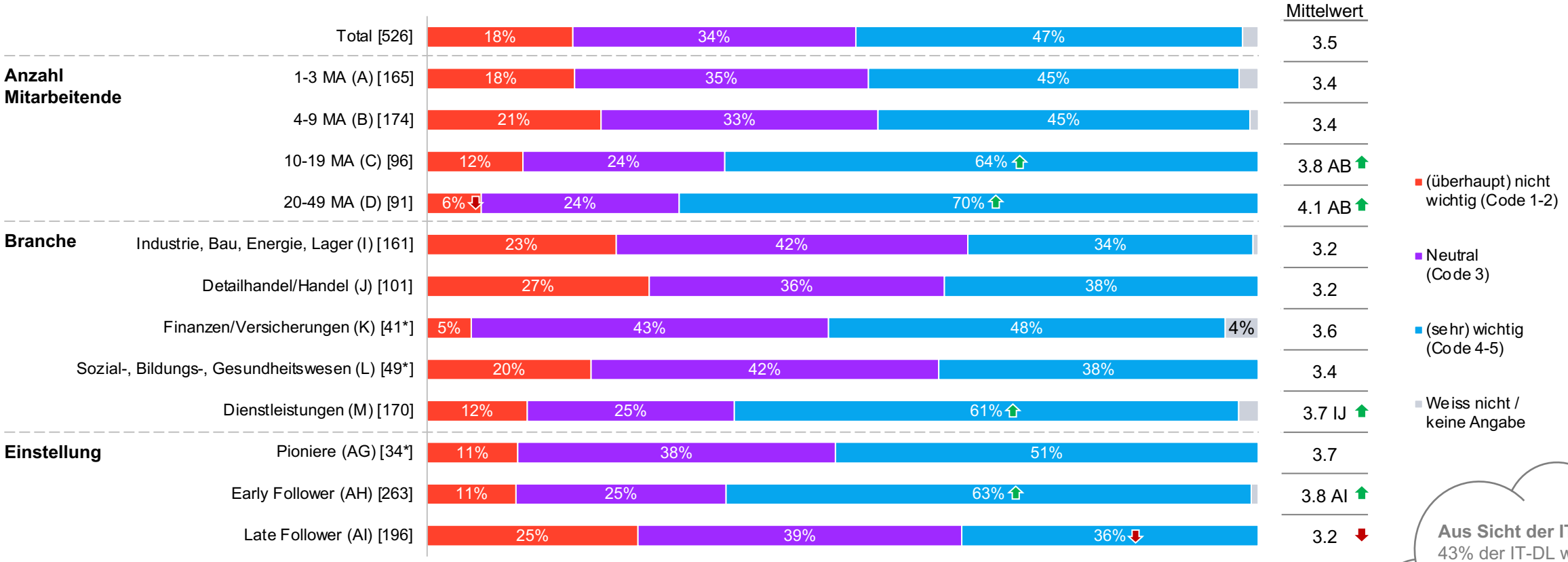
Der gefühlte Informationsgrad liegt bei 3.4 auf der Fünferskala. KMU mit 20 – 49 Mitarbeitenden, aus der Finanzbranche sowie Pioniere fühlen sich besser informiert als die anderen Subgruppen. Etwas mehr als zwei Fünftel der Befragten wünschen sich, besser informiert zu sein, am häufigsten besteht dieser Wunsch bei den gut informierten Pionieren (56%).



F009: Wie gut fühlen Sie sich persönlich in der Cyberrisk-Thematik informiert? | F010: Wären Sie gerne besser informiert über das Thema Cybersicherheit?
Basis: n=[ ] | Filter: KMU | Skalierte Frage: 1= sehr schlecht bis 5= sehr gut (F009) & geschlossene Frage (F010) | ▲ signifikant höher als Total; ▼ signifkant tiefer als Total | *Kleine Basis <50
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Priorität Cybersicherheit

Knapp die Hälfte der befragten KMU gibt dem Thema Cybersicherheit eine eher oder sehr hohe Priorität, knapp ein Fünftel eine eher oder sehr tiefe. KMU mit 10 – 49 Mitarbeitenden geben der Cybersicherheit eine höhere Priorität als die kleineren Unternehmen, und auch die Finanz- und Dienstleistungsbranche fallen mit hohen Werten auf.



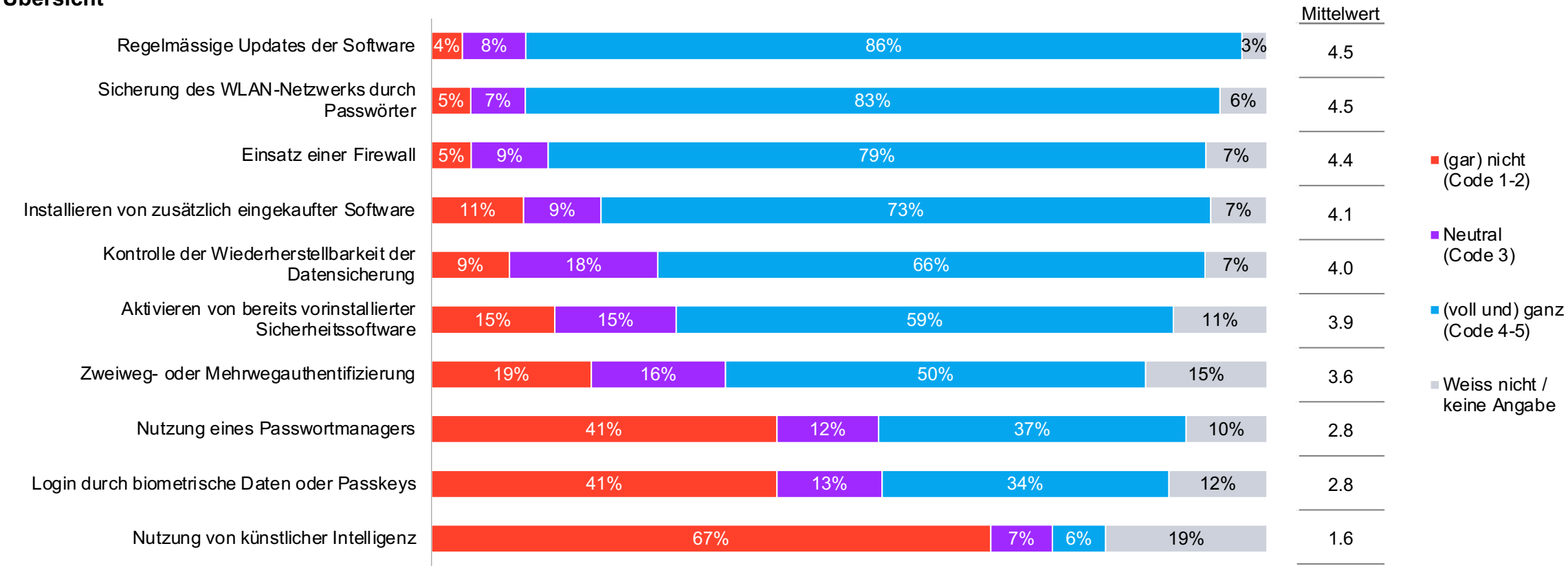
F011: Welche Priorität hat in Ihrer Firma das Thema Cybersicherheit?
Basis: n=[ ] | Filter: KMU | Skalierte Frage: 1= überhaupt nicht wichtig bis 5= sehr wichtig | ▲ signifikant höher als Total; ▼ signifkant tiefer als Total | *Kleine Basis <50 | Datenbeschriftung ab 3%
Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Aus Sicht der IT-DL…
43% der IT-DL würden ihren Kunden empfehlen, das Thema Cyber-sicherheit ernster zu nehmen (siehe S. 73).

Technische Massnahmenumsetzung (1/4)

7 von 10 Massnahmen zur Erhöhung der Cybersicherheit wurden von über der Hälfte der befragten KMU eher oder voll und ganz umgesetzt. Einen tieferen Umsetzungsgrad erhalten „Passwortmanager“ (2.8) und „Login durch biometrische Daten/Passkeys“ (2.8). KI wird nur von ganz wenigen (6%) eingesetzt.

Übersicht

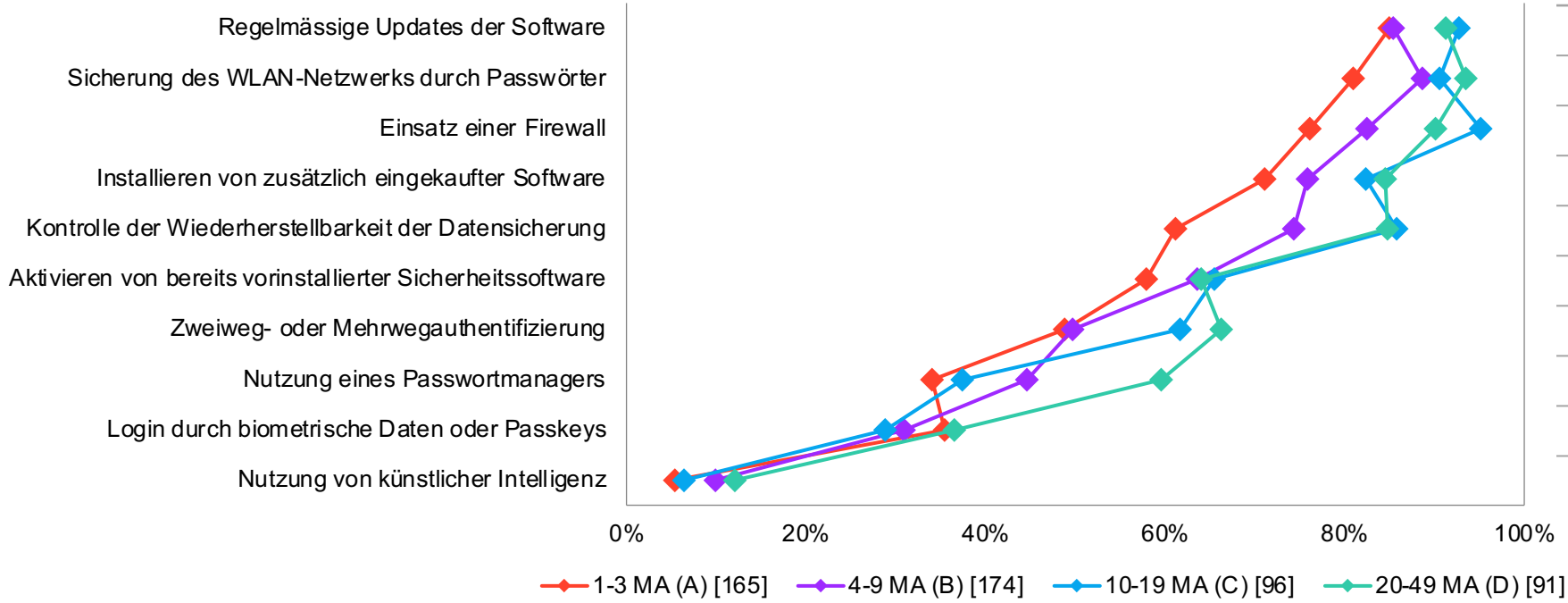


F012: Inwieweit sind die folgenden technischen Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?
Basis: n=526 | Filter: KMU | Skalierte Frage: 1= gar nicht bis 5= voll und ganz

Technische Massnahmenumsetzung (2/4)

Die ganz kleinen Unternehmen (1-3 Mitarbeitende) haben bei fast allen Massnahmen die tiefsten Umsetzungsgrade, etwas höher sind diejenigen der Unternehmen mit 4-9 Mitarbeitenden. Unternehmen mit 10-19 bzw. 20-49 Mitarbeitenden unterscheiden sich nur wenig voneinander (Ausnahme: Passwortmanager).

Nach Anzahl Mitarbeitenden



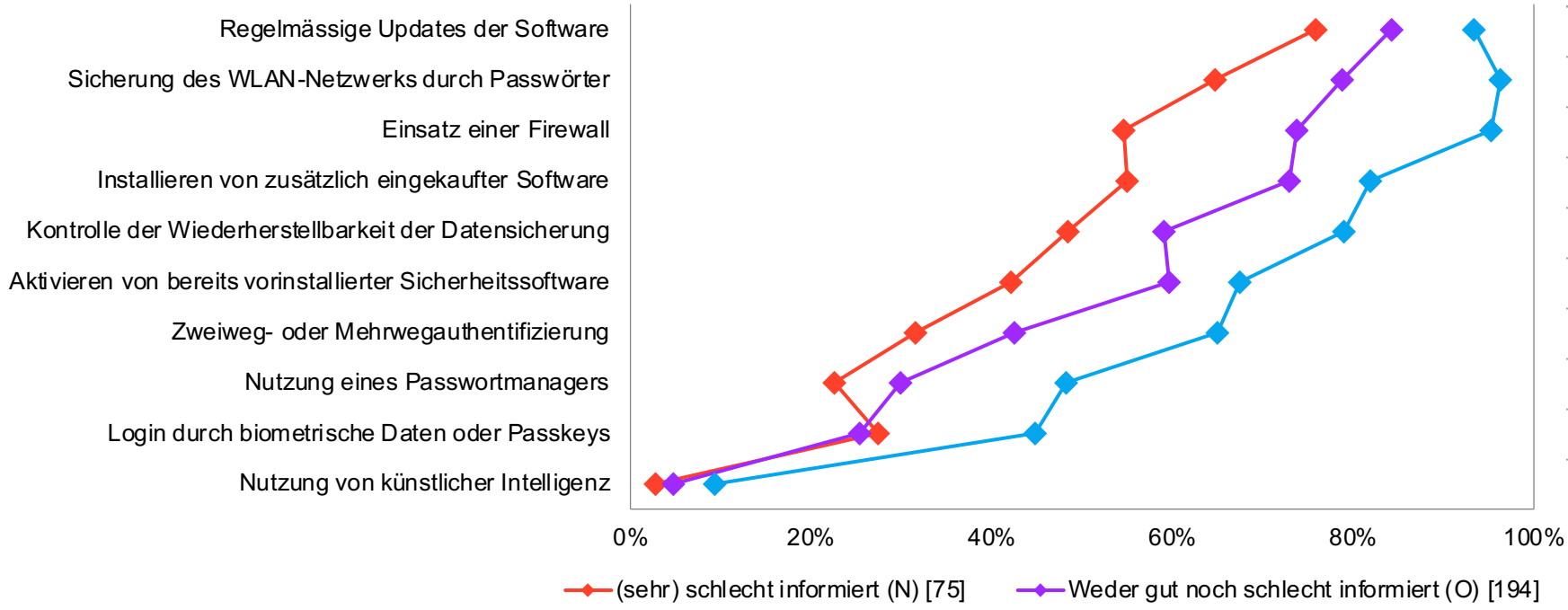
	Mittelwert			
	1-3 MA	4-9 MA	10-19 MA	20-49 MA
Regelmässige Updates der Software	4.5	4.5	4.7	4.7
Sicherung des WLAN-Netzwerks durch Passwörter	4.4	4.6	4.8 A	4.7 A
Einsatz einer Firewall	4.4	4.4	4.8 AB	4.7 AB
Installieren von zusätzlich eingekaufter Software	4.1	4.3	4.5 A	4.4 A
Kontrolle der Wiederherstellbarkeit der Datensicherung	3.9	4.2 A	4.5 AB	4.5 A
Aktivieren von bereits vorinstallierter Sicherheitssoftware	3.8	3.9	4.1	4.1
Zweiweg- oder Mehrwegauthentifizierung	3.6	3.4	3.8	3.9 B
Nutzung eines Passwortmanagers	2.7	3.1 A	3.0	3.7 ABC
Login durch biometrische Daten oder Passkeys	2.8	2.6	2.6	2.8
Nutzung von künstlicher Intelligenz	1.5	1.7	1.6	1.9 A

F012: Inwieweit sind die folgenden technischen Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?
Basis: n=[ ] | Filter: KMU | Skalierte Frage: 1= gar nicht bis 5= voll und ganz | Top2 und Mittelwerte ausgewiesen
signifikant höher als Total; signifikant tiefer als Total | Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Technische Massnahmenumsetzung (3/4)

Je besser die KMU zum Thema Cybersicherheit informiert sind, desto höher ist der technische Massnahmen-Umsetzungsgrad.

Nach Informationsgrad



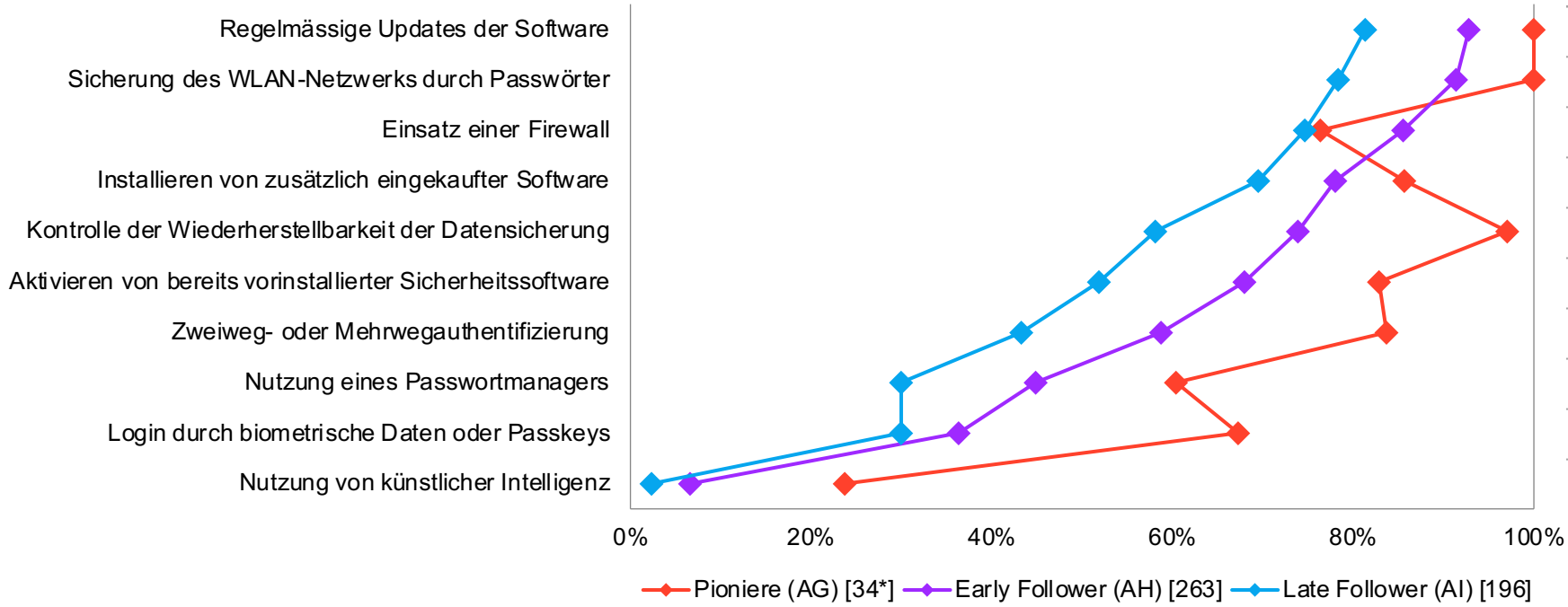
Mittelwert Informationsgrad		
Eher/sehr schlecht	Weder gut noch schlecht	Eher/ sehr gut
4.2	4.4	4.7 NO
4.1	4.2	4.8 NO
3.8	4.2	4.8 NO
3.6	4.0	4.4 NO
3.5	3.7	4.4 NO
3.5	3.8	4.1 N
2.9	3.3	4.0 NO
2.1	2.7	3.2 NO
2.6	2.4	3.1 O
1.3	1.5	1.7 N

F012: Inwieweit sind die folgenden technischen Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?
Basis: n=[ ] | Filter: KMU | Skalierte Frage: 1= gar nicht bis 5= voll und ganz | Top2 und Mittelwerte ausgewiesen
signifikant höher als Total; signifikant tiefer als Total | Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Technische Massnahmenumsetzung (4/4)

Je offener die Befragten gegenüber technischen Innovationen sind, desto höher ist der Massnahmen-Umsetzungsgrad.

Nach Einstellung



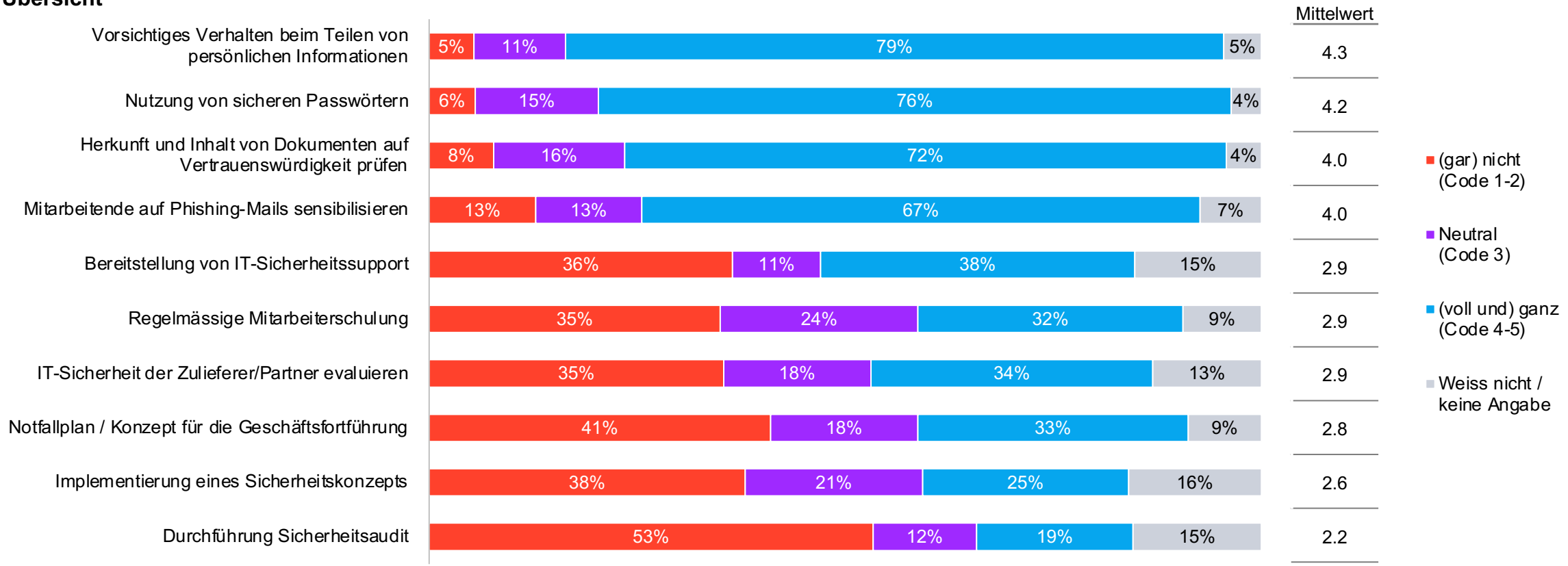
	Mittelwert	
Pioniere	Early Follower	Late Follower
4.9	4.7 AI	4.3
4.7	4.7 AI	4.3
4.7	4.6 AI	4.2
4.5	4.3 AI	3.9
4.7	4.2 AI	3.7
4.3	4.1 AI	3.7
4.5	3.7 AI	3.3
3.3	3.1 AI	2.5
3.7	2.9	2.6
2.4	1.6 AI	1.3

F012: Inwieweit sind die folgenden technischen Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?
Basis: n=[ ] | Filter: KMU | Skalierte Frage: 1= gar nicht bis 5= voll und ganz | Top2 und Mittelwerte ausgewiesen | *Kleine Basis <50
signifikant höher als Total; signifikant tiefer als Total | Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Organisatorische Massnahmenumsetzung (1/4)

Organisatorische Massnahmen sind grundsätzlich weniger umgesetzt als technische Massnahmen. 4 von 10 Massnahmen wurden von über der Hälfte der Befragten eher oder voll und ganz umgesetzt, Sicherheitsaudits und Sicherheitskonzepte werden am seltensten umgesetzt.

Übersicht

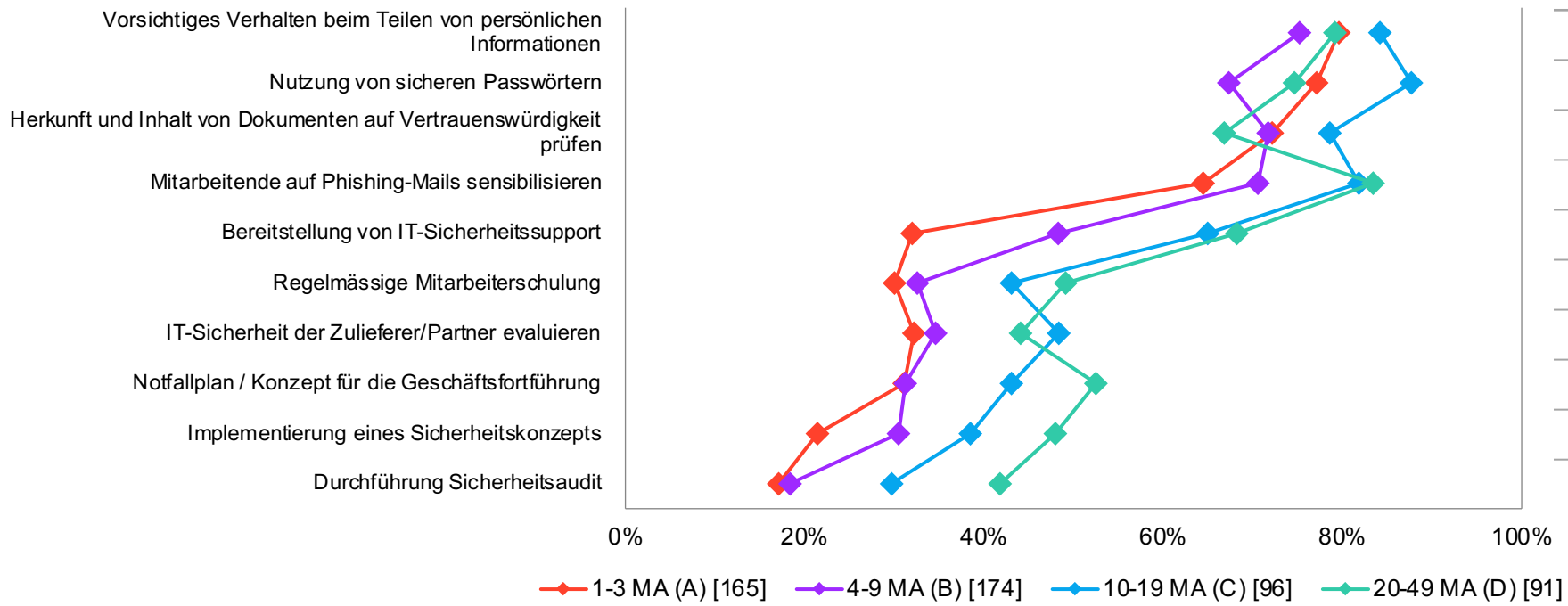


F013: Inwieweit sind die folgenden organisatorischen Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?
Basis: n=526 | Filter: KMU | Skalierte Frage: 1= gar nicht bis 5= voll und ganz

Organisatorische Massnahmenumsetzung (2/4)

Bei den 3 Massnahmen mit den höchsten Umsetzungsgraden unterscheiden sich die verschieden grossen Unternehmen nur wenig. Massnahmen mit tieferem Umsetzungsgrad hingegen werden von den grösseren Unternehmen (10+ Mitarbeitende) signifikant häufiger bzw. stärker umgesetzt als von den kleineren.

Nach Anzahl Mitarbeitenden



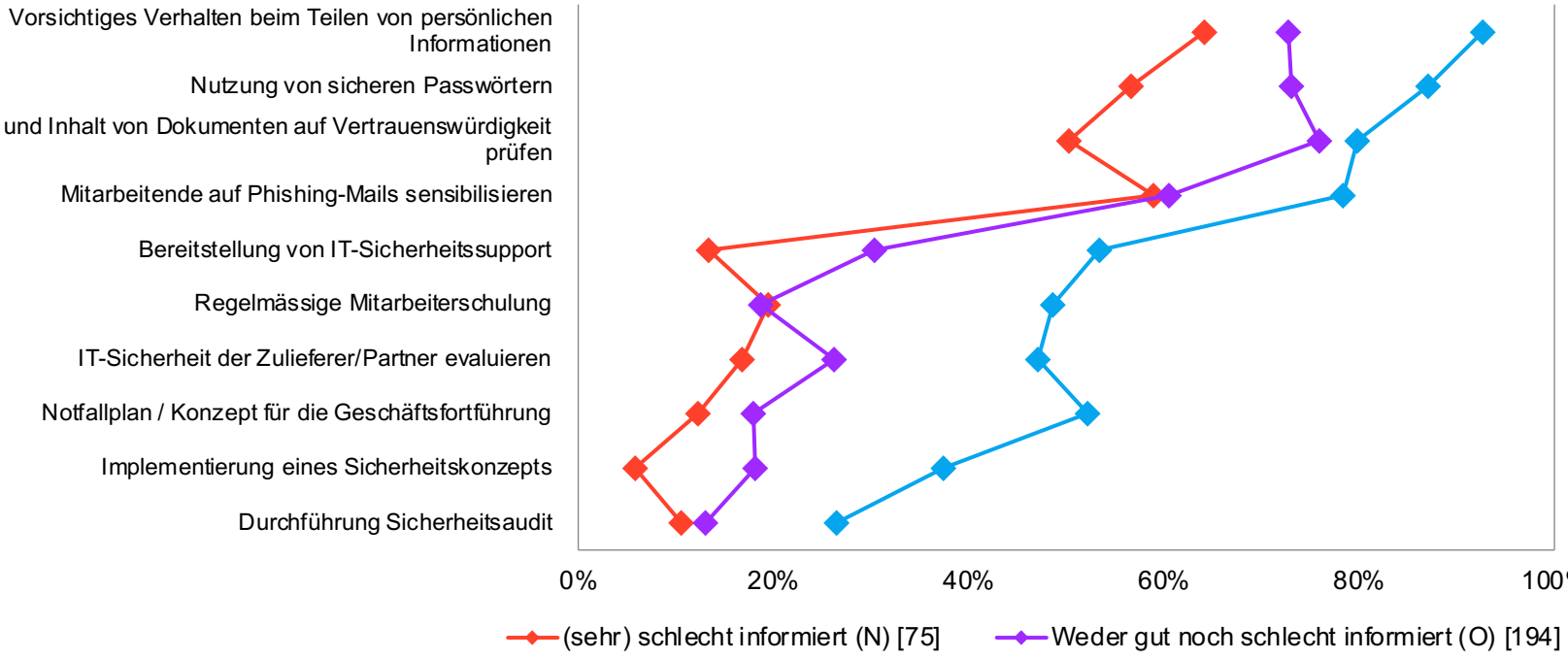
	Mittelwert			
	1-3 MA	4-9 MA	10-19 MA	20-49 MA
Vorsichtiges Verhalten beim Teilen von persönlichen Informationen	4.3 B	4.1	4.2	4.1
Nutzung von sicheren Passwörtern	4.2	4.0	4.4 B	4.2
Herkunft und Inhalt von Dokumenten auf Vertrauenswürdigkeit prüfen	4.0	4.0	4.1	3.9
Mitarbeitende auf Phishing-Mails sensibilisieren	4.0	4.0	4.3 B	4.4 AB
Bereitstellung von IT-Sicherheitssupport	2.7	3.3 A	3.9 AB	4.0 AB
Regelmässige Mitarbeiterschulung	2.9	2.9	3.2 AB	3.6 AB
IT-Sicherheit der Zulieferer/Partner evaluieren	2.8	2.9	3.5 AB	3.3 AB
Notfallplan / Konzept für die Geschäftsfortführung	2.7	2.9	3.2 AB	3.4 AB
Implementierung eines Sicherheitskonzepts	2.5	2.9 A	3.1 A	3.3 AB
Durchführung Sicherheitsaudit	2.1	2.3	2.8 AB	3.1 AB

F013: Inwieweit sind die folgenden organisatorischen Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?
Basis: n=[ ] | Filter: KMU | Skalierte Frage: 1= gar nicht bis 5= voll und ganz | Top2 und Mittelwerte ausgewiesen
signifikant höher als Total; signifikant tiefer als Total | Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Organisatorische Massnahmenumsetzung (3/4)

Je besser die befragten Unternehmen in Bezug auf Cyberrisiken informiert sind, desto höher sind die Umsetzungsgrade der verschiedenen organisatorischen Massnahmen.

Nach Informationsgrad



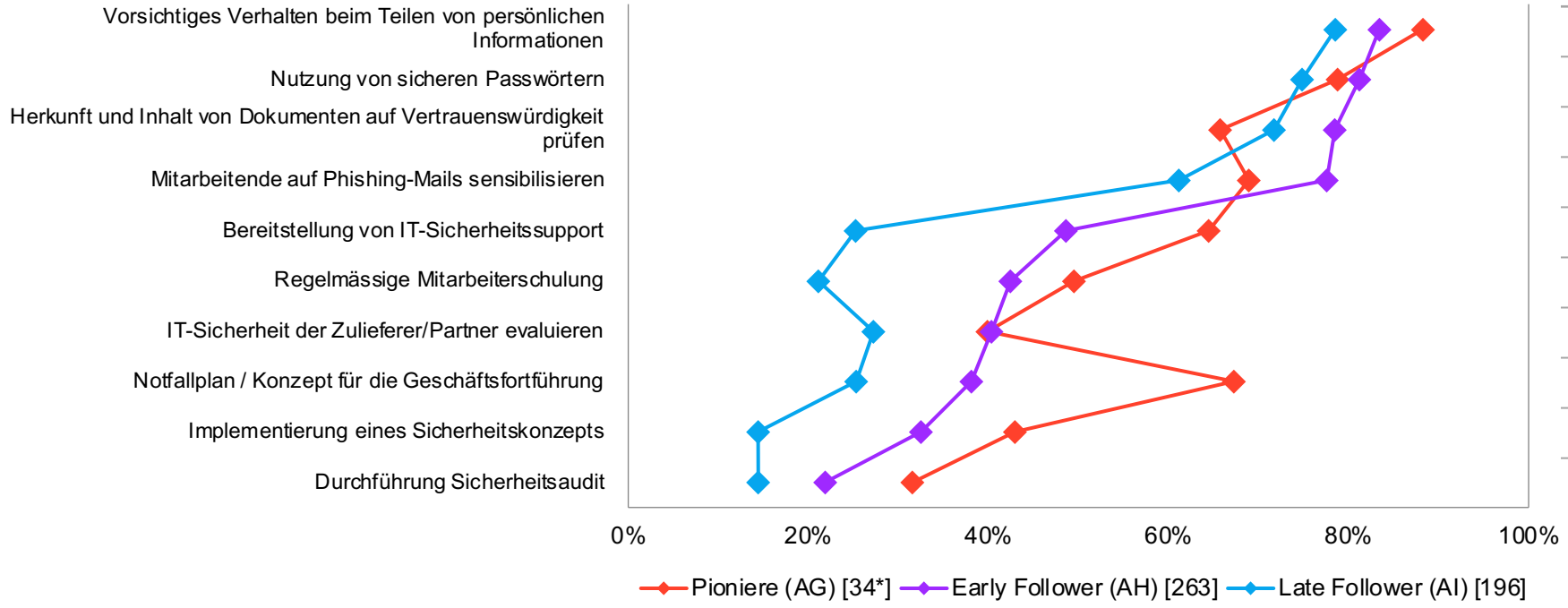
Mittelwert Informationsgrad		
Eher/sehr schlecht	Weder gut noch schlecht	Eher/ sehr gut
3.8	4.1	4.6 NO
3.7	4.0	4.5 NO
3.5	4.0 N	4.2 N
3.6	3.8	4.3 NO
1.9	2.8 N	3.4 NO
2.3	2.6	3.4 NO
2.1	2.7 N	3.3 NO
2.0	2.3	3.5 NO
1.9	2.4	3.1 NO
1.6	2.0	2.5 NO

F013: Inwieweit sind die folgenden organisatorischen Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?
Basis: n=[ ] | Filter: KMU | Skalierte Frage: 1= gar nicht bis 5= voll und ganz | Top2 und Mittelwerte ausgewiesen
signifikant höher als Total; signifikant tiefer als Total | Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Organisatorische Massnahmenumsetzung (4/4)

Bei den meisten organisatorischen Massnahmen gilt: Je offener die Befragten gegenüber neuen Technologien sind, desto eher sind die organisatorischen Massnahmen umgesetzt.

Nach Einstellung

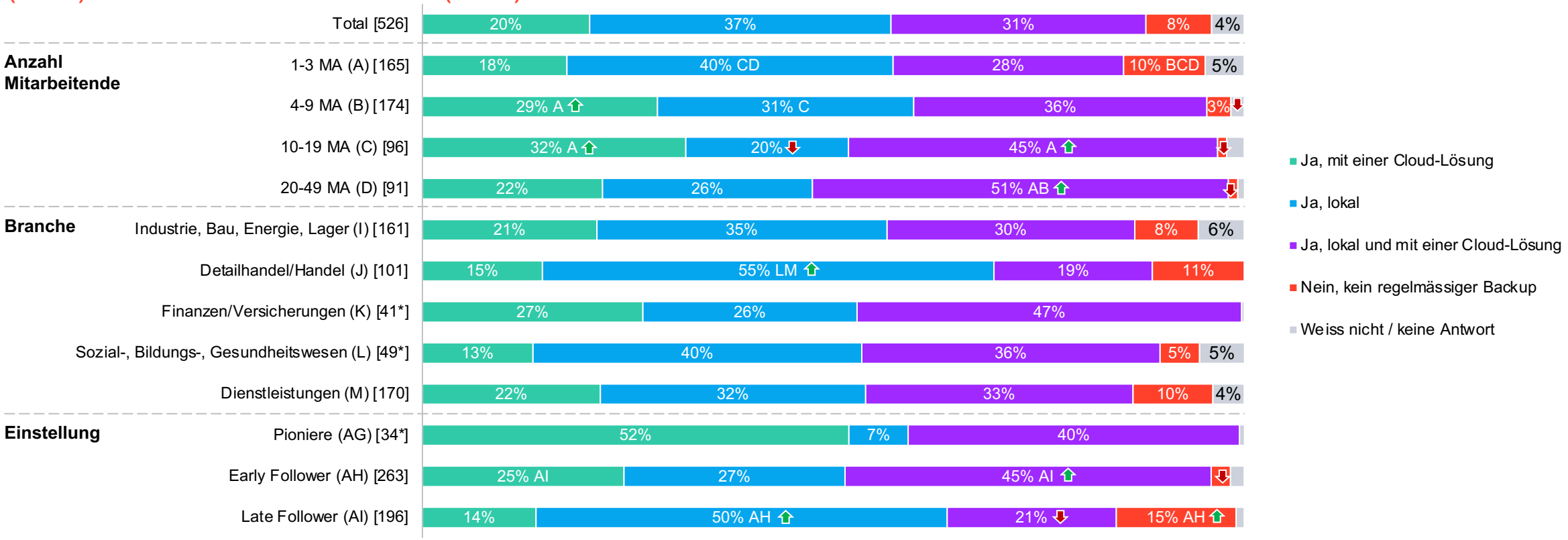


	Mittelwert		
	Pioniere	Early Follower	Late Follower
Vorsichtiges Verhalten beim Teilen von persönlichen Informationen	4.3	4.3	4.2
Nutzung von sicheren Passwörtern	4.4	4.3 AI	4.0
Herkunft und Inhalt von Dokumenten auf Vertrauenswürdigkeit prüfen	3.7	4.1	3.9
Mitarbeitende auf Phishing-Mails sensibilisieren	3.7	4.2 AI	3.7
Bereitstellung von IT-Sicherheitssupport	3.6	3.2 AI	2.5
Regelmässige Mitarbeiterschulung	3.3	3.2 AI	2.5
IT-Sicherheit der Zulieferer/Partner evaluieren	2.9	3.1 AI	2.6
Notfallplan / Konzept für die Geschäftsfortführung	3.7	3.0 AI	2.5
Implementierung eines Sicherheitskonzepts	3.2	2.9 AI	2.1
Durchführung Sicherheitsaudit	2.6	2.4 AI	1.9

F013: Inwieweit sind die folgenden organisatorischen Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?
Basis: n=[ ] | Filter: KMU | Skalierte Frage: 1= gar nicht bis 5= voll und ganz | Top2 und Mittelwerte ausgewiesen | *Kleine Basis <50
signifikant höher als Total; signifikant tiefer als Total | Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Backup mit/ohne Cloud

Die meisten Unternehmen führen regelmässige Daten-Backups durch (88%). Am ehesten verzichten die kleinsten Unternehmen (1-3 Mitarbeitende: 10%), Firmen aus dem Detailhandel/Handel (11%), der Dienstleistungsbranche (10%) und Late Follower darauf (15%).

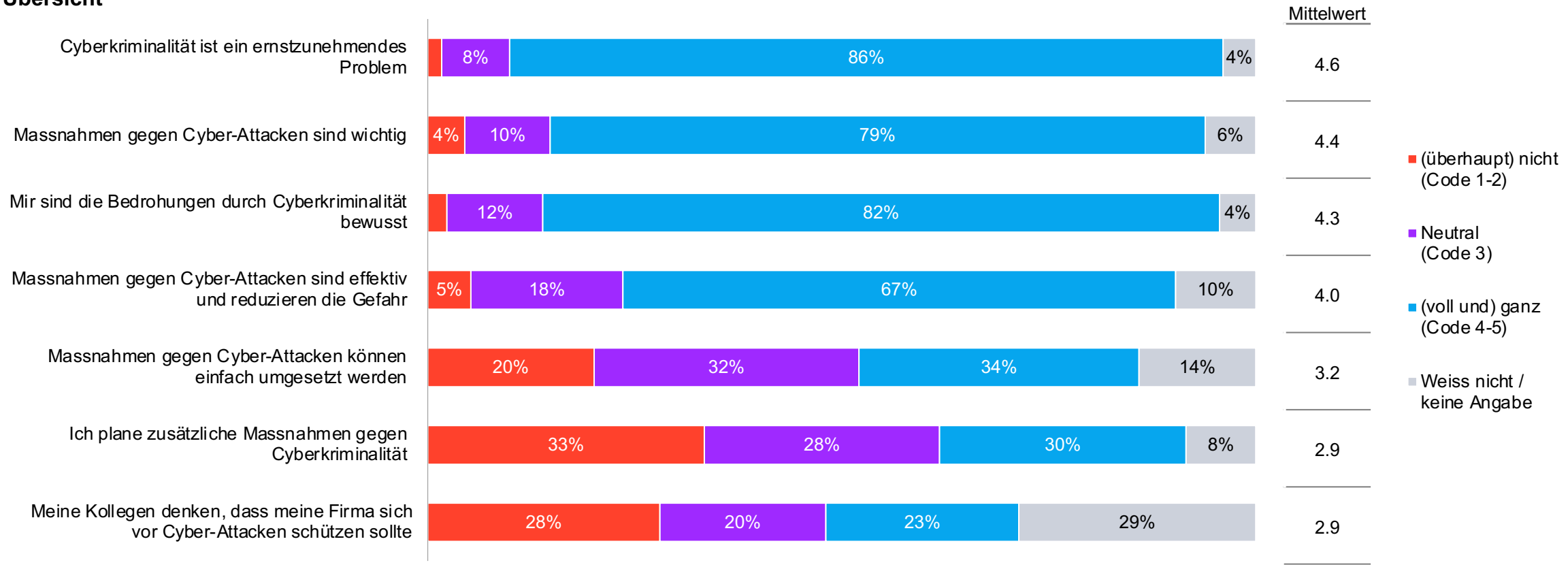


F014: Wird in Ihrem Unternehmen regelmässig ein Backup der Daten durchgeführt?
Basis: n=[ ] | Filter: KMU | Geschlossene Frage | ⬆ signifikant höher als Total; ⬇ signifkant tiefer als Total | *Kleine Basis <50 | Datenbeschriftung ab 3%
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Einstellung zu Cyberkriminalität (1/6)

Einen sehr hohen Zustimmungswert erhält die Aussage, dass Cyberkriminalität ein ernstzunehmendes Problem ist (86%). Hingegen spürt nur knapp ein Viertel einen sozialen Druck für Schutzmassnahmen (23%) und nur knapp ein Drittel (30%) plant zusätzliche Massnahmen bzw. findet deren Umsetzung einfach (34%).

Übersicht

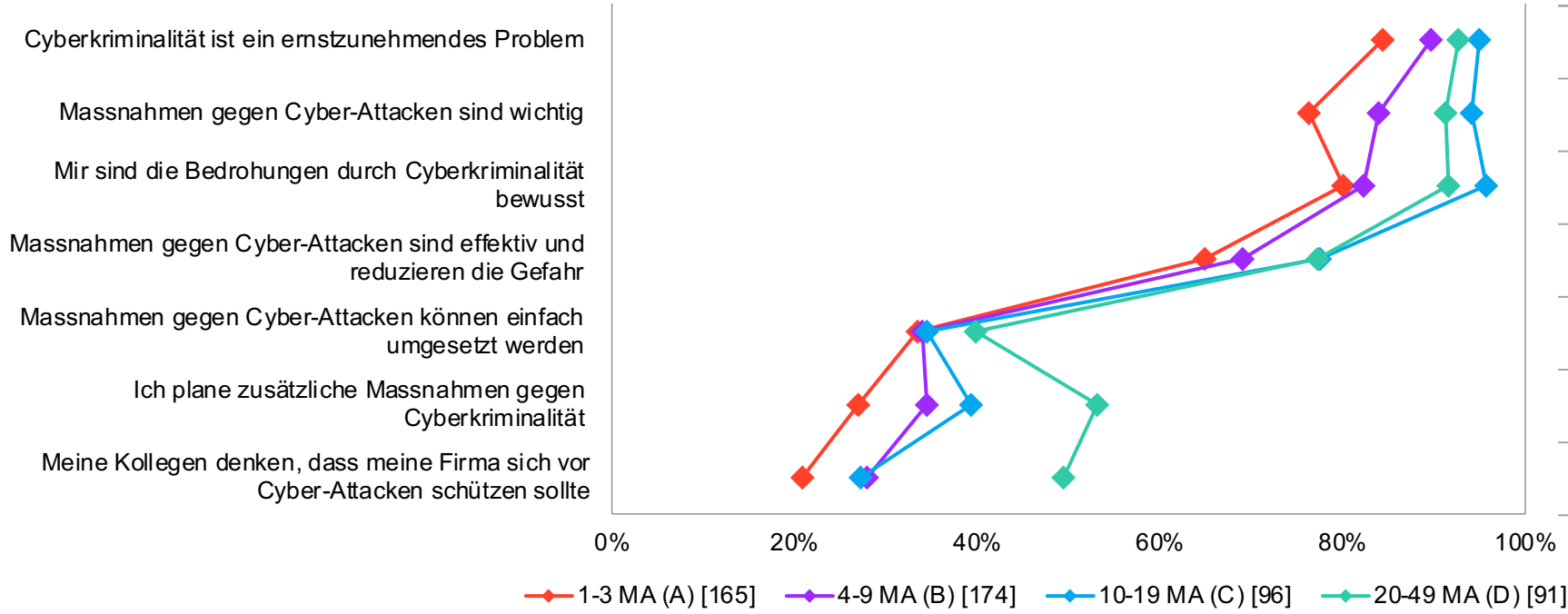


F015: Inwiefern stimmen Sie den folgenden Aussagen zu Cyberkriminalität wie Malware, Online-Betrug und Hacking zu?
Basis: n=526 | Filter: KMU | Skalierte Frage: 1= überhaupt nicht bis 5= voll und ganz | Datenbeschriftung ab 3%

Einstellung zu Cyberkriminalität (2/6)

Je grösser die Unternehmen sind, desto eher stimmen sie den Aussagen zu. Die ansonsten eher weniger befürworteten Aussagen zur Planung zusätzlicher Massnahmen sowie zum sozialen Druck für mehr Massnahmen erhalten von den grössten befragten Unternehmen (20-49 Mitarbeitende) eine signifikant höhere Zustimmung.

Nach Anzahl Mitarbeitenden



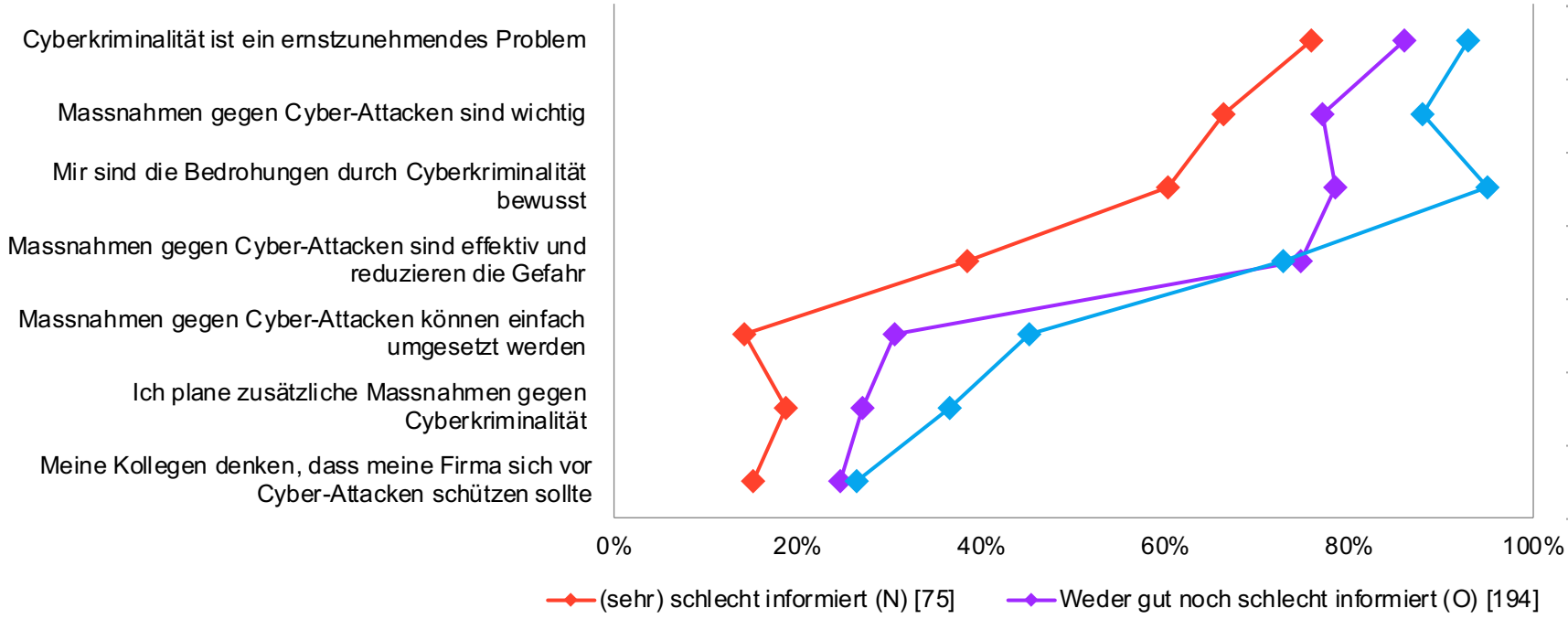
	Mittelwert			
	1-3 MA	4-9 MA	10-19 MA	20-49 MA
Cyberkriminalität ist ein ernstzunehmendes Problem	4.5	4.6	4.8 AB	4.7
Massnahmen gegen Cyber-Attacken sind wichtig	4.3	4.4	4.7 AB	4.6 AB
Mir sind die Bedrohungen durch Cyberkriminalität bewusst	4.3	4.3	4.7 AB	4.5
Massnahmen gegen Cyber-Attacken sind effektiv und reduzieren die Gefahr	4.0	4.0	4.3 AB	4.2
Massnahmen gegen Cyber-Attacken können einfach umgesetzt werden	3.2	3.3	3.2	3.3
Ich plane zusätzliche Massnahmen gegen Cyberkriminalität	2.8	3.1	3.1	3.5 ABC
Meine Kollegen denken, dass meine Firma sich vor Cyber-Attacken schützen sollte	2.8	3.0	2.8	3.4 ABC

F015: Inwiefern stimmen Sie den folgenden Aussagen zu Cyberkriminalität wie Malware, Online-Betrug und Hacking zu?
Basis: n=[ ] | Filter: KMU | Skalierte Frage: 1= überhaupt nicht bis 5= voll und ganz | Top2 und Mittelwerte ausgewiesen
signifikant höher als Total; signifikant tiefer als Total | Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Einstellung zu Cyberkriminalität (3/6)

Je besser sich die befragten Unternehmensleitenden bezüglich Cyberkriminalität informiert fühlen, desto eher stimmen sie den Aussagen zu.

Nach Informationsgrad



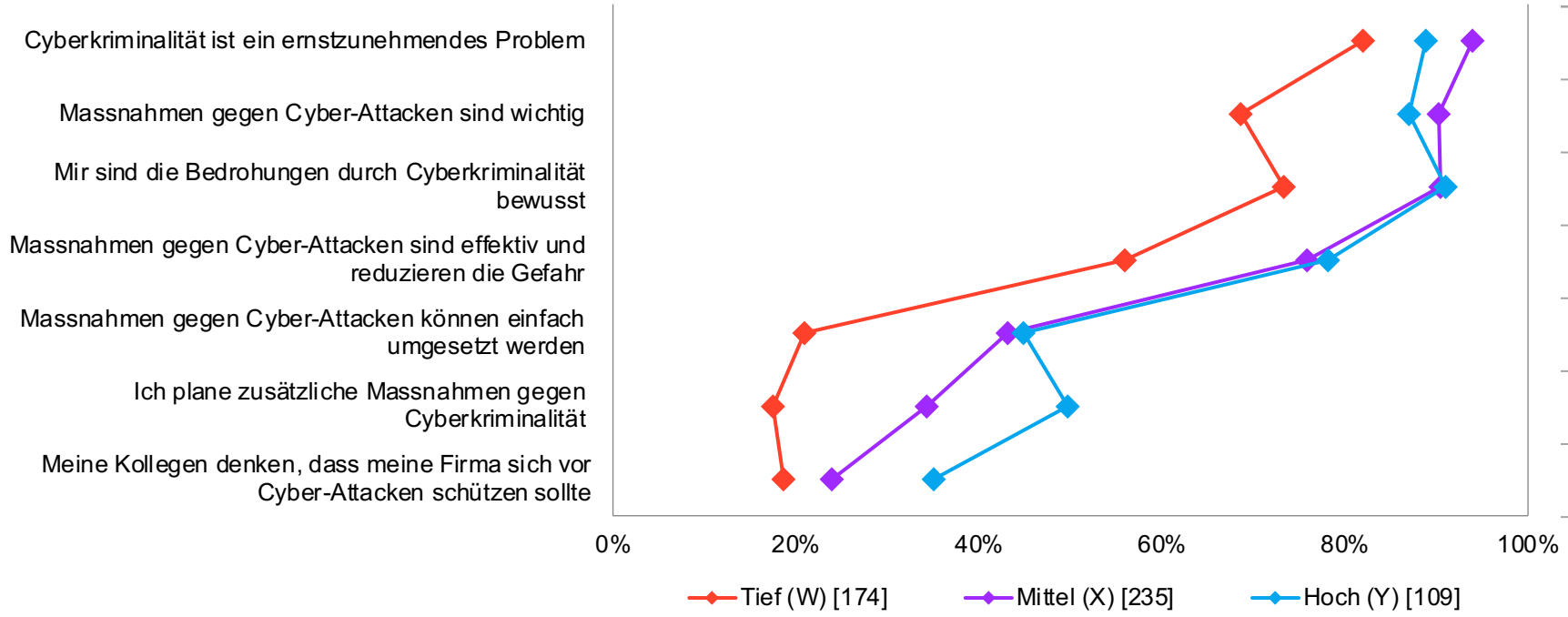
	Mittelwert		
	Eher/sehr schlecht	Weder gut noch schlecht	Eher/ sehr gut
Cyberkriminalität ist ein ernstzunehmendes Problem	4.3	4.4	4.7 NO
Massnahmen gegen Cyber-Attacken sind wichtig	4.0	4.2	4.7 NO
Mir sind die Bedrohungen durch Cyberkriminalität bewusst	3.9	4.1	4.7 NO
Massnahmen gegen Cyber-Attacken sind effektiv und reduzieren die Gefahr	3.6	4.1 N	4.1 N
Massnahmen gegen Cyber-Attacken können einfach umgesetzt werden	2.7	3.2 N	3.4 N
Ich plane zusätzliche Massnahmen gegen Cyberkriminalität	2.5	2.8	3.1 N
Meine Kollegen denken, dass meine Firma sich vor Cyber-Attacken schützen sollte	2.7	2.9	3.0

F015: Inwiefern stimmen Sie den folgenden Aussagen zu Cyberkriminalität wie Malware, Online-Betrug und Hacking zu?
Basis: n=[ ] | Filter: KMU | Skalierte Frage: 1= überhaupt nicht bis 5= voll und ganz | Top2 und Mittelwerte ausgewiesen
signifikant höher als Total; signifikant tiefer als Total | Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Einstellung zu Cyberkriminalität (4/6)

Befragte mit einer tiefen technischen Massnahmenumsetzung stimmen den Aussagen zu Cyberkiminalität signifikant weniger zu als Befragte mit einer mittleren oder hohen technischen Massnahmenumsetzung.

Nach technischer Massnahmenumsetzung



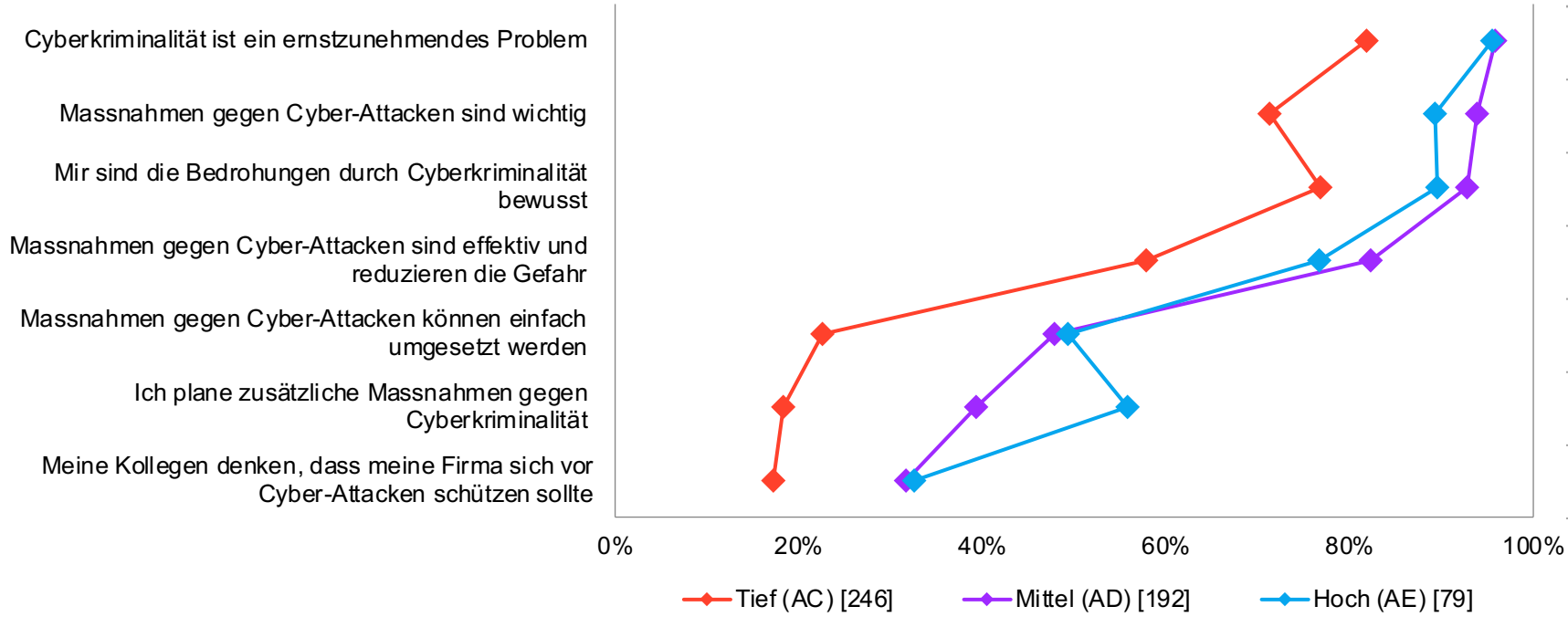
	Mittelwert	
Tief	**Mittel**	**Hoch**
4.3	4.7 W	4.8 W
4.0	4.7 W	4.7 W
4.0	4.5 W	4.7 W
3.7	4.2 W	4.3 W
2.9	3.3 W	3.6 W
2.5	3.0 W	3.6 WX
2.7	2.9	3.1

F015: Inwiefern stimmen Sie den folgenden Aussagen zu Cyberkriminalität wie Malware, Online-Betrug und Hacking zu?
Basis: n=[ ] | Filter: KMU | Skalierte Frage: 1= überhaupt nicht bis 5= voll und ganz | Top2 und Mittelwerte ausgewiesen
signifikant höher als Total; signifikant tiefer als Total | Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Einstellung zu Cyberkriminalität (5/6)

Bei den organisatorischen Massnahmen gilt dasselbe wie bei den technischen: Befragte mit mittlerer und hoher Massnahmenumsetzung stimmen den Aussagen zu Cyberkriminalität eher zu als Befragte mit tiefer Massnahmenumsetzung.

Nach organisatorischer Massnahmenumsetzung



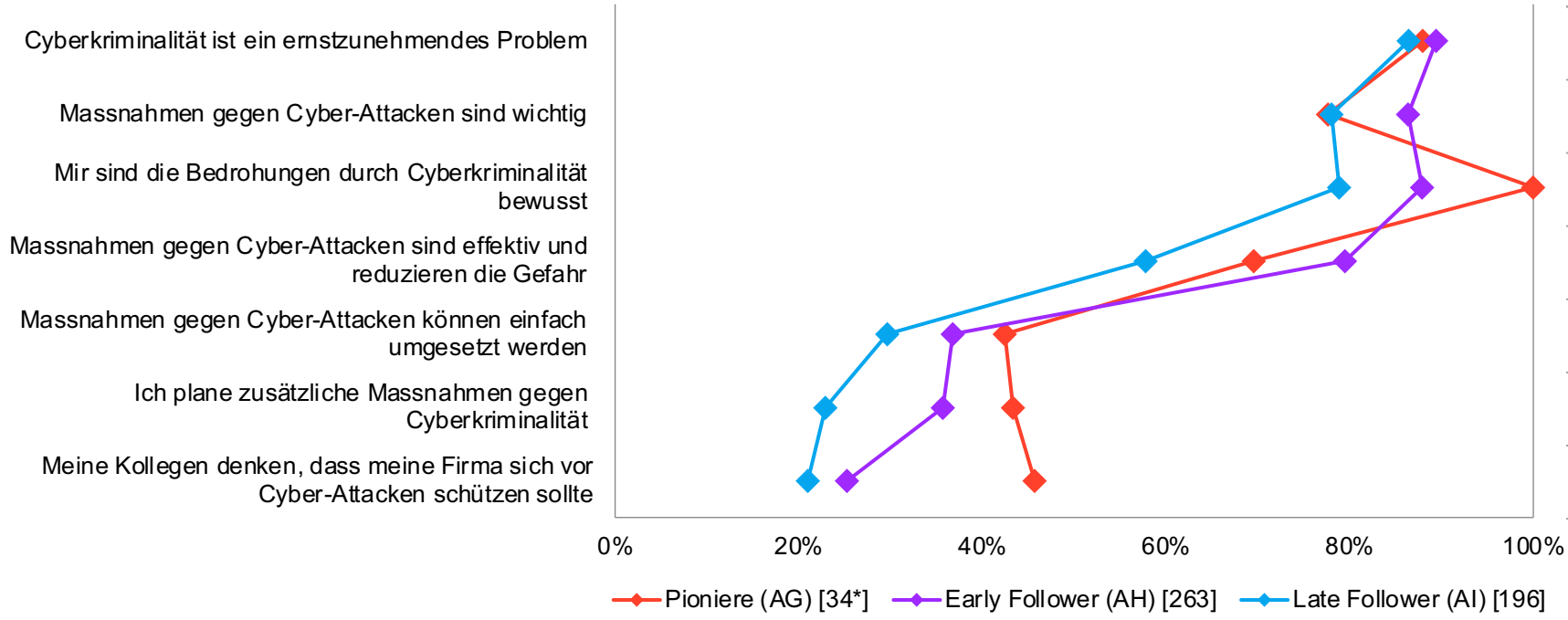
	Mittelwert	
Tief	Mittel	Hoch
4.3	4.8 AC	4.9 AC
4.0	4.8 AC	4.9 AC
4.1	4.6 AC	4.9 AC AD
3.8	4.2 AC	4.4 AC
2.9	3.5 AC	3.8
2.5	3.2 AC	3.7 AC
2.7	3.1 AC	3.1

F015: Inwiefern stimmen Sie den folgenden Aussagen zu Cyberkriminalität wie Malware, Online-Betrug und Hacking zu?
Basis: n=[ ] | Filter: KMU | Skalierte Frage: 1= überhaupt nicht bis 5= voll und ganz | Top2 und Mittelwerte ausgewiesen
signifikant höher als Total; signifikant tiefer als Total | Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Einstellung zu Cyberkriminalität (6/6)

Befragte, die technische Innovationen nur einführen, wenn es unabdingbar ist (Late Follower), stimmen den Aussagen zu Cyberkriminalität weniger zu als Early Follower und Pioniere.

Nach Einstellung



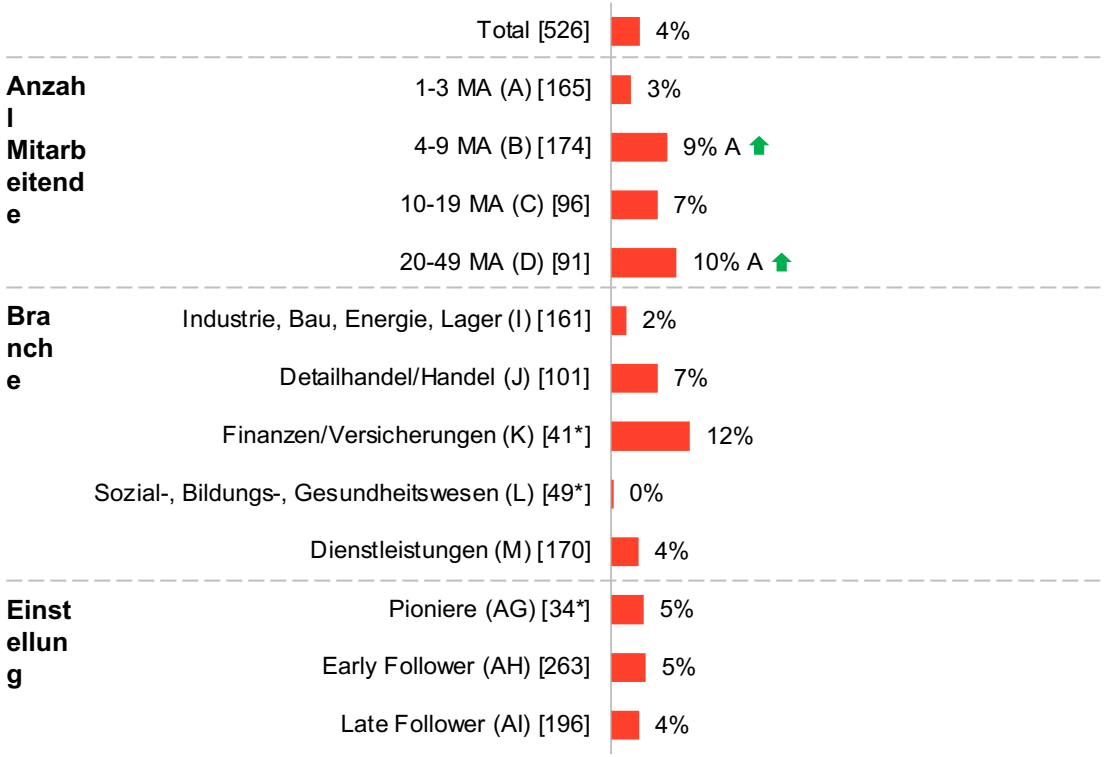
	Mittelwert	
Pioniere	Early Follower	Late Follower
4.3	4.6	4.5
4.2	4.5 AI	4.2
4.6	4.5 AI	4.2
4.1	4.2 AI	3.8
3.3	3.3	3.0
3.1	3.1 AI	2.6
3.3	2.9	2.8

F015: Inwiefern stimmen Sie den folgenden Aussagen zu Cyberkriminalität wie Malware, Online-Betrug und Hacking zu?
Basis: n=[ ] | Filter: KMU | Skalierte Frage: 1= überhaupt nicht bis 5= voll und ganz | Top2 und Mittelwerte ausgewiesen | *Kleine Basis <50
signifikant höher als Total; signifikant tiefer als Total | Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Erfahrung Cyberkriminalität

Vier Prozent der befragten Unternehmen haben innerhalb der letzten 3 Jahre einen Cyberangriff erlitten. Bei fast drei Vierteln davon erfolgte daraus ein finanzieller Schaden, bei der Hälfte ein grosser Arbeitsaufwand; über zwei Fünftel berichten von emotionaler Belastung durch den Angriff oder dessen Folgen.

Erlittene Angriffe (Ja-Anteile)
Basis: [ ] | Filter: KMU



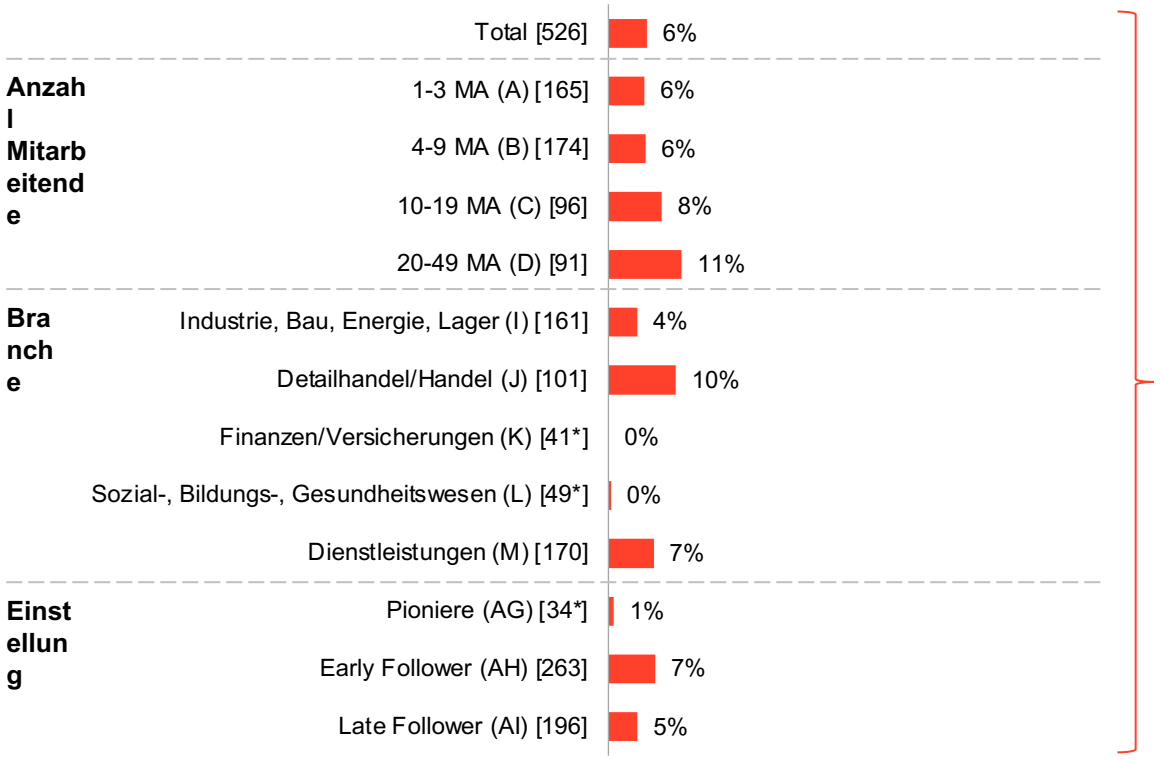
Erlittene Schäden
Basis: n=36* | Filter: KMU – wenn Cyberangriff erlitten

F016: Hat Ihr Unternehmen innerhalb der letzten 3 Jahre einen Cyberangriff erlitten, der einen finanziellen Schaden oder einen Reputationsschaden verursachte, viel Mühe für die Schadensbereinigung bereitete oder Ihnen emotional sehr zu schaffen gemacht hat? | F017: Entstand durch diesen Angriff… | Basis: n=[ ] | Filter: siehe oben | Geschlossene Fragen | ⬆ signifikant höher als Total; ⬇ signifikant tiefer als Total | *Kleine Basis <50
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

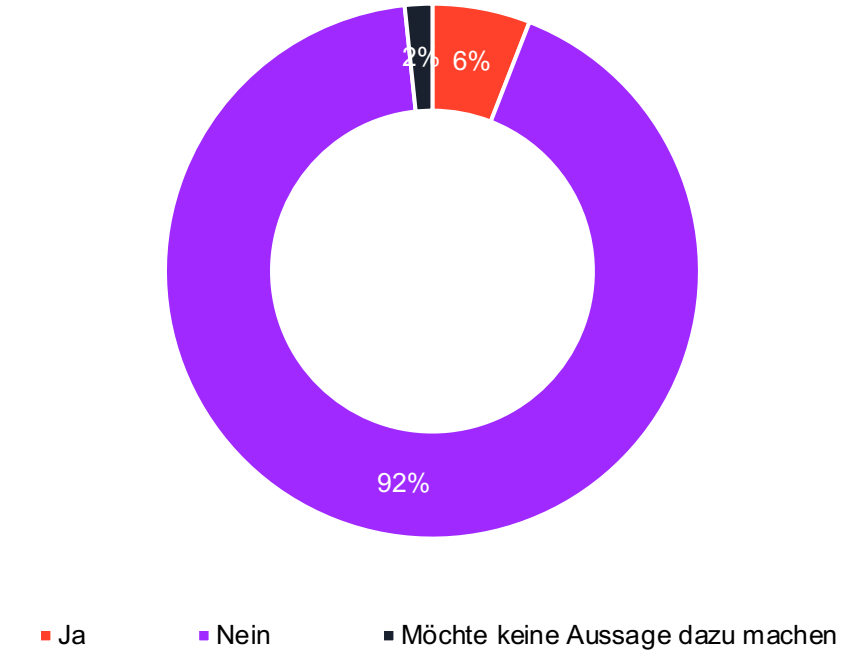
Erpressung

Sechs Prozent der befragten Unternehmen wurden schon einmal durch Cyberkriminelle erpresst; je grösser sie sind, desto eher wurden sie schon erpresst. Zwei von 31 erpressten Unternehmen haben schon einmal Lösegeld an Cyberkriminelle bezahlt.

Erpressung durch Cyberkriminelle (Ja-Anteile)
Basis: [ ] | Filter: KMU



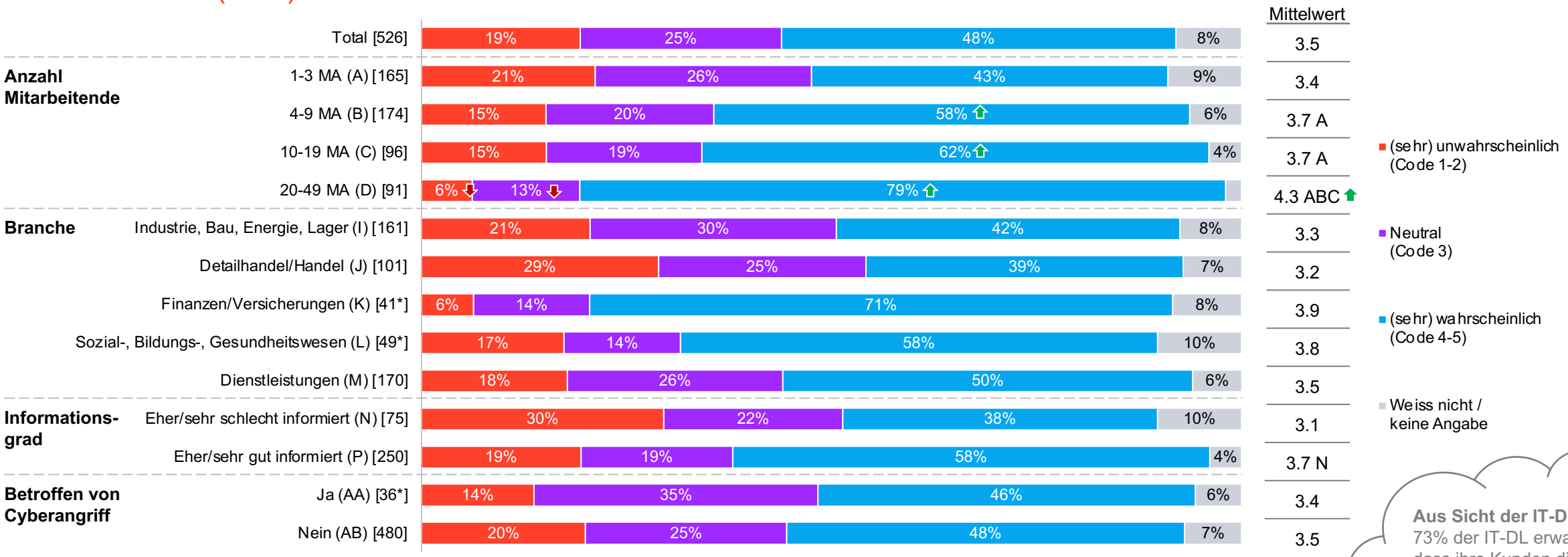
Lösegeld an Cyberkriminelle
Basis: n=31 | Filter: durch Cyberkriminelle erpresste Befragte



F019: Wurde Ihr Unternehmen schon einmal von Cyberkriminellen erpresst? | F020: Hat Ihr Unternehmen schon einmal Lösegeld an Cyberkriminelle bezahlt?
Basis: n=[ ] | Filter: siehe oben | Geschlossene Fragen | ⬆ signifikant höher als Total; ⬇ signifkant tiefer als Total | Datenbeschriftung ab 3%
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Erhöhung Sicherheitsmassnahmen

Knapp die Hälfte der Befragten (48%) möchte in den kommenden 1 bis 3 Jahren ihre Cybersicherheits-Massnahmen erhöhen. Besonders hoch ist dieser Anteil bei den Unternehmen mit 20 bis 49 Mitarbeitenden (79%) und in der Finanzbranche (71%).

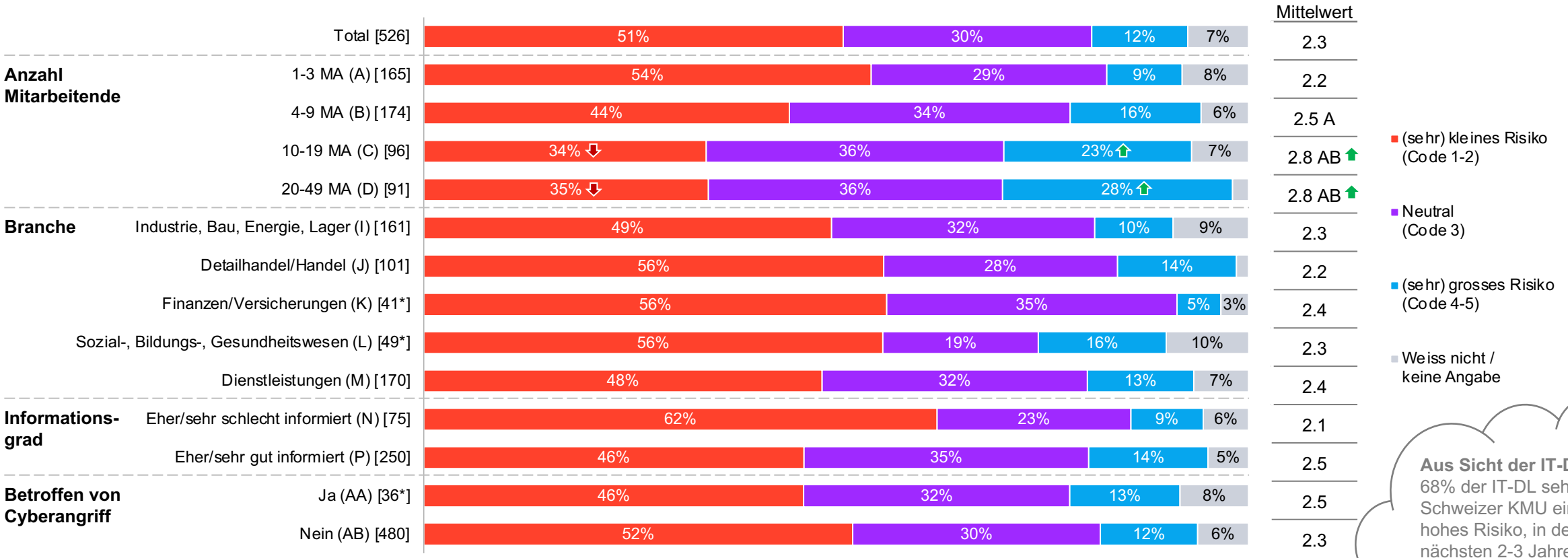


F018: Wie wahrscheinlich ist es, dass Sie in den kommenden 1 bis 3 Jahren die Sicherheitsmassnahmen gegen Cyberkriminalität erhöhen werden?
Basis: n=[ ] | Filter: KMU | Skalierte Frage: 1= sehr unwahrscheinlich bis 5= sehr wahrscheinlich | ↑ signifikant höher als Total; ↓ signifkant tiefer als Total
Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Aus Sicht der IT-DL…
73% der IT-DL erwarten, dass ihre Kunden die Sicherheitsmassnahmen erhöhen werden (siehe S. 73).

Risikoeinschätzung

Rund die Hälfte der befragten Unternehmen (51%) schätzt das Risiko eines Cyberangriffes, der ihren Betrieb mindestens einen Tag ausser Kraft setzen wird, als eher oder sehr klein ein. Je grösser die Unternehmen sind, desto höher schätzen sie das Risiko ein.

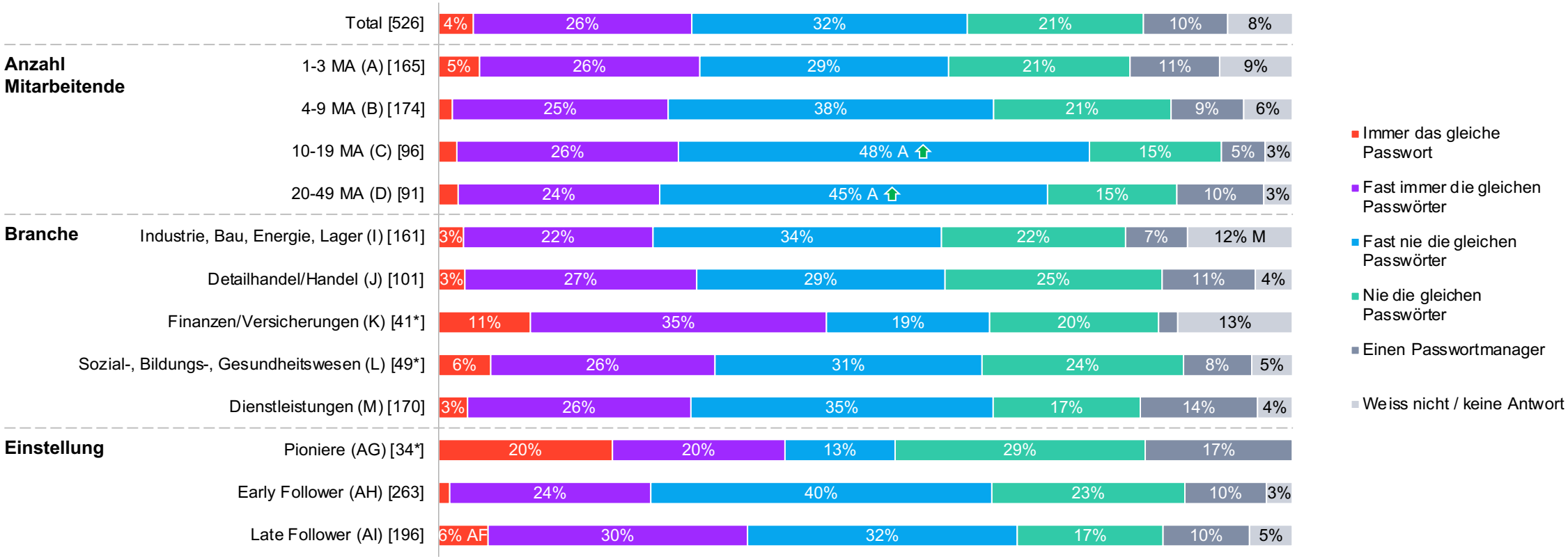


F021: Wie hoch schätzen Sie das Risiko ein, dass Ihr Unternehmen innerhalb der nächsten 2-3 Jahre durch einen Cyberangriff mindestens einen Tag lang ausser Kraft gesetzt wird?
Basis: n=[ ] | Filter: KMU | Skalierte Frage: 1= sehr kleines Risiko bis 5= sehr grosses Risiko | ⬆ signifikant höher als Total; ⬇ signifkant tiefer als Total | *Kleine Basis <50 | Datenbeschriftung ab 3%
Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Aus Sicht der IT-DL…
68% der IT-DL sehen für Schweizer KMU ein (sehr) hohes Risiko, in den nächsten 2-3 Jahren durch einen Cyberangriff für mind. einen Tag ausser Kraft gesetzt zu werden (siehe S. 66).

Umgang mit Passwörtern

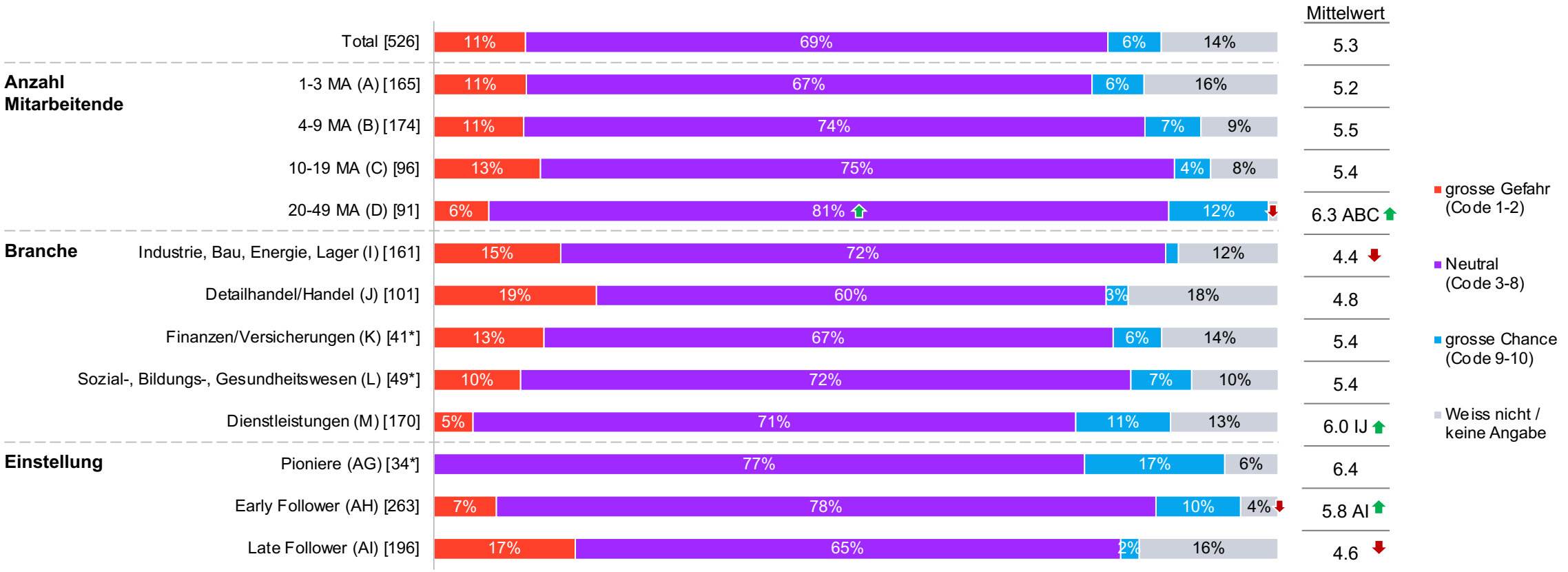
Nur ganz wenige Geschäftsführende nutzen immer dasselbe Passwort, aber rund ein Viertel (26%) nutzt „fast immer“ das gleiche Passwort und geht damit ein Risiko ein. Passwortmanager haben sich noch nicht durchgesetzt, nur rund jedes zehnte befragte Unternehmen nutzen die entsprechende Technologie.



F022: Benutzen Sie für verschiedene Programme oder Plattformen das gleiche Passwort mehrfach? Ich benutze…
Basis: n=[ ] | Filter: KMU | Geschlossene Frage | ⬆ signifikant höher als Total; ⬇ signifkant tiefer als Total | *Kleine Basis <50 | Datenbeschriftung ab 3%
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Einstellung zu KI

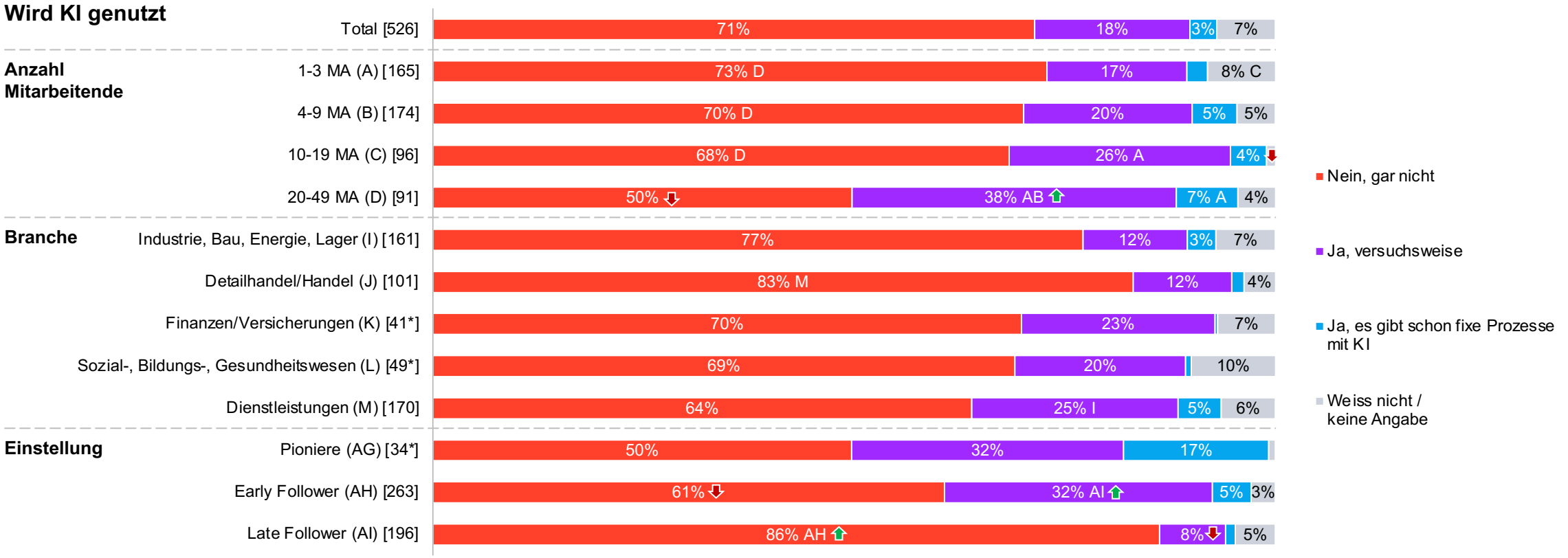
Die grosse Mehrheit (69%) hat eine neutrale Haltung zu KI, während rund jedes zehnte Unternehmen (11%) eine grosse Gefahr darin sieht und rund jedes siebzehnte (6%) eine grosse Chance. Unternehmen mit über 20 Mitarbeitenden, aus der Dienstleistungsbranche, Pioniere und Early Follower sind KI gegenüber offener eingestellt.



F023: Sehen Sie in den technischen Fortschritten künstlicher Intelligenz eher eine Gefahr oder eine Chance für die Zukunft Ihres Unternehmens?
Basis: n=[ ] | Filter: KMU | Skalierte Frage: 1= sehr grosse Gefahr bis 10= sehr grosse Chance | ⬆ signifikant höher als Total; ⬇ signifkant tiefer als Total | *Kleine Basis <50 | Datenbeschriftung ab 3%
Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Nutzung KI

Fast drei Viertel der Befragten nutzen KI noch gar nicht in ihrem Unternehmen, rund ein Fünftel hat schon Versuche durchgeführt und nur ganz wenige befragte Unternehmen (3%) haben schon fixe Prozesse mit KI. Unternehmen mit über 20 Mitarbeitenden, aus der Dienstleistungsbranche, Pioniere und Early Follower setzen KI schon häufiger ein.



F024: Wird in Ihrem Unternehmen schon aktiv künstliche Intelligenz eingesetzt?
Basis: n=[ ] | Filter: KMU | Geschlossene Frage | ⬆ signifikant höher als Total; ⬇ signifkant tiefer als Total | *Kleine Basis <50 | Datenbeschriftung ab 3%
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Nutzung KI

Am ehesten wird KI für das Schreiben von Texten genutzt, aber auch als Ersatz der klassischen Suchmaschinen zur Informationsbeschaffung.

Wofür wird KI genutzt

Formulierungen, Briefe überarbeiten. grosse Datensätze analysieren

Texte und Analysen von Bildern. Nur sehr sporadisch.

Code Beispiele, Texte verfassen, Fragen analog Google

Génération de textes pour du marketing ou offres de services

Analyses détaillées des données

Automatische Offerterstellung aufgrund eingehender Emails

Creazione di testi per pubblicità, social media, articoli promozionali.

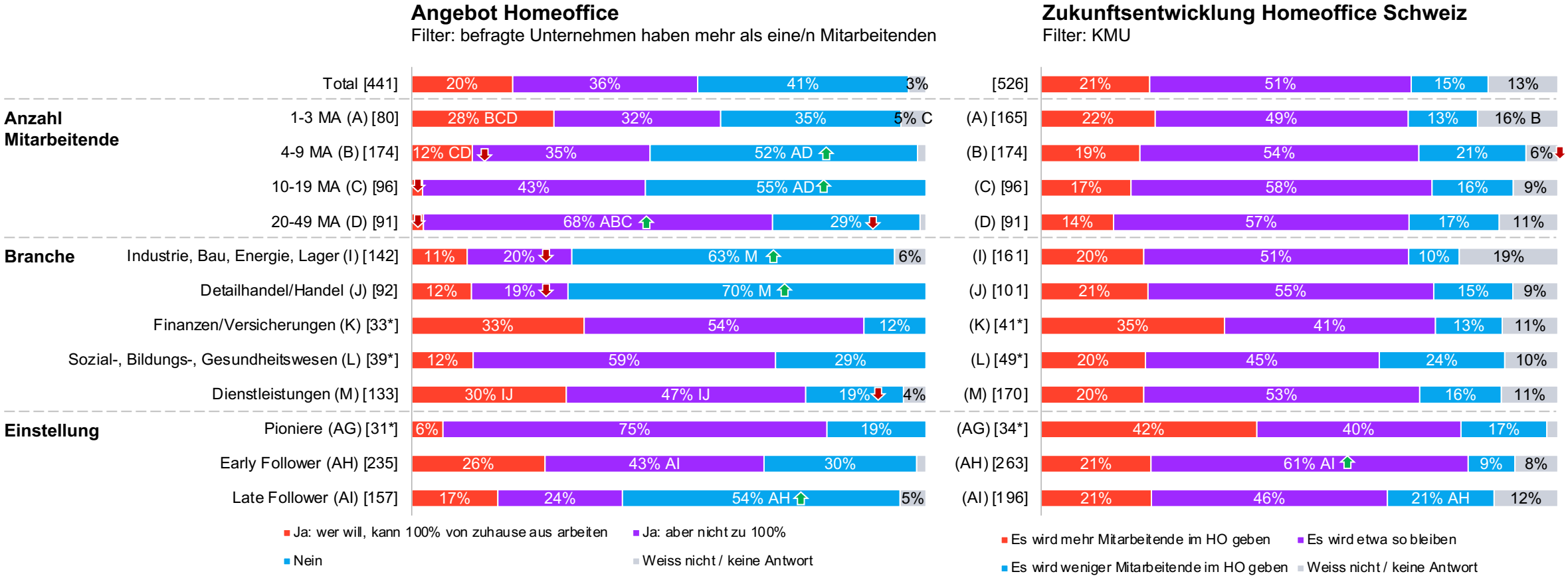
Für Recherchearbeiten und Übersetzungen

Generierung von juristischen Texten, PDF-Zusammenfassungen, einfache Code-Generatoren, Suspicious Login Detection, Verknüpfungen der Cloud-Lösungen für Kunden mit llm2 Servern

F025: Wofür wird KI in Ihrem Unternehmen eingesetzt? Bitte erläutern Sie.
Basis: n=142 | Filter: KMU - Wenn KI genutzt wird | Offene Frage

Homeoffice

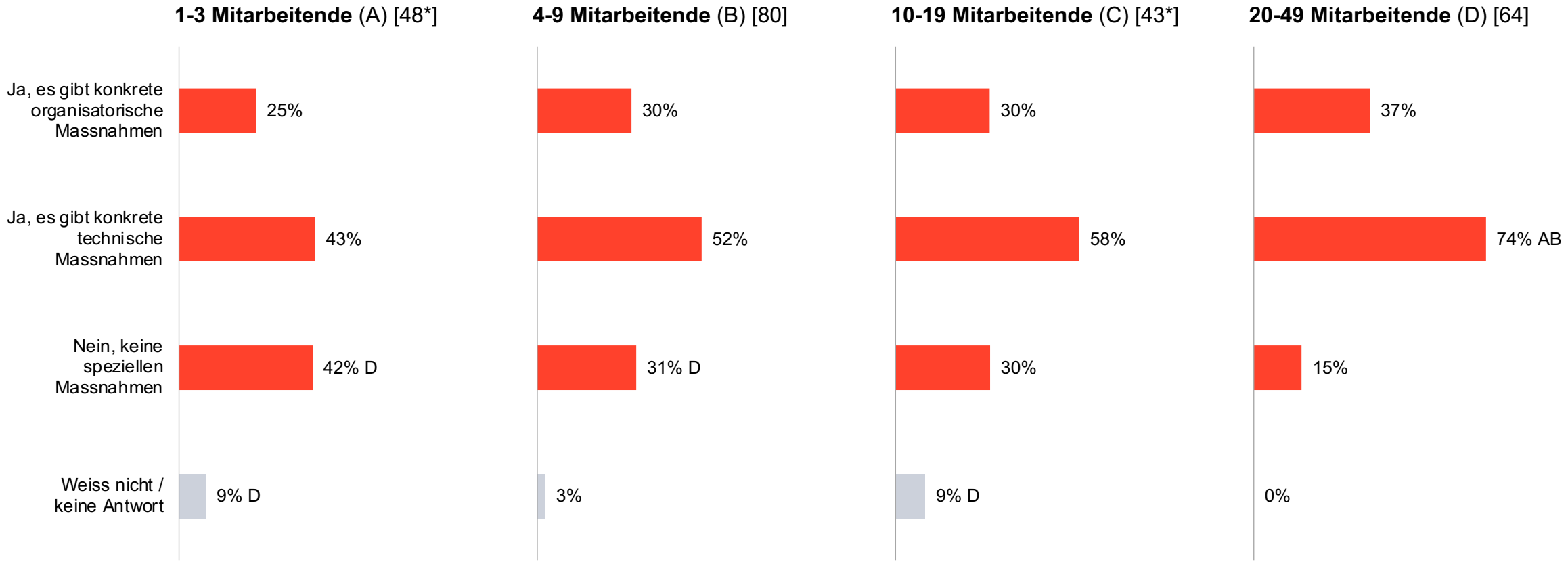
Etwas mehr als die Hälfte der befragten Unternehmen bietet Homeoffice zumindest für einen Teil der Arbeitszeit an, etwas weniger als die Hälfte bietet gar kein Homeoffice an. Eine Mehrheit der Befragten geht davon aus, dass das Homeoffice-Angebot in der Schweiz in Zukunft etwa so bleiben wird, wie es jetzt ist.



F026: Bieten Sie Ihren Mitarbeitenden die Möglichkeit, im Homeoffice zu arbeiten? | F027: Wie schätzen Sie die zukünftige Entwicklung von Homeoffice in der Schweiz ein?
Basis: n=[ ] | Filter: siehe oben | Geschlossene Fragen | ⬆ signifikant höher als Total; ⬇ signifkant tiefer als Total | *Kleine Basis <50 | Datenbeschriftung ab 3%
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Massnahmen für Homeoffice

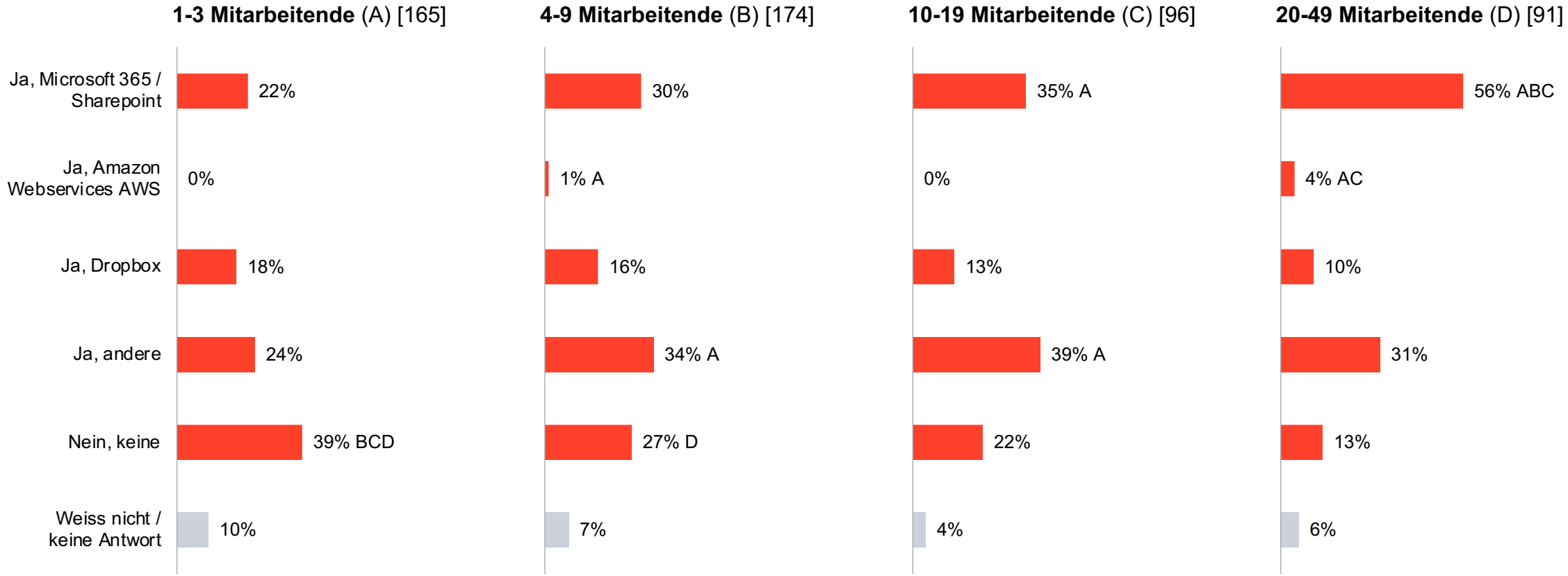
Drei Viertel aller Befragten (75%) trafen konkrete organisatorische und/oder technische Massnahmen zum Schutz vor Cyberangriffen im Homeoffice (Total-Werte nicht abgebildet). Je grösser die Unternehmen sind, desto eher haben sie technische Massnahmen ergriffen. Organisatorische Massnahmen werden im Vergleich dazu eher vernachlässigt.



F028: Treffen Sie konkrete Vorkehrungen zum Schutz vor Cyberangriffen im Homeoffice?
Basis: n=[ ] | Filter: KMU – Homeoffice wird angeboten | Geschlossene Frage | Kleine Basis <50
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Cloudnutzung

Mehr als zwei Drittel der befragten Unternehmen nutzen Cloud-Dienstleistungen zur Datenablage (70%, Total-Werte nicht abgebildet). Je grösser die Unternehmen sind, desto eher nutzen sie Cloud-Dienstleistungen, insbesondere Microsoft 365/Sharepoint.



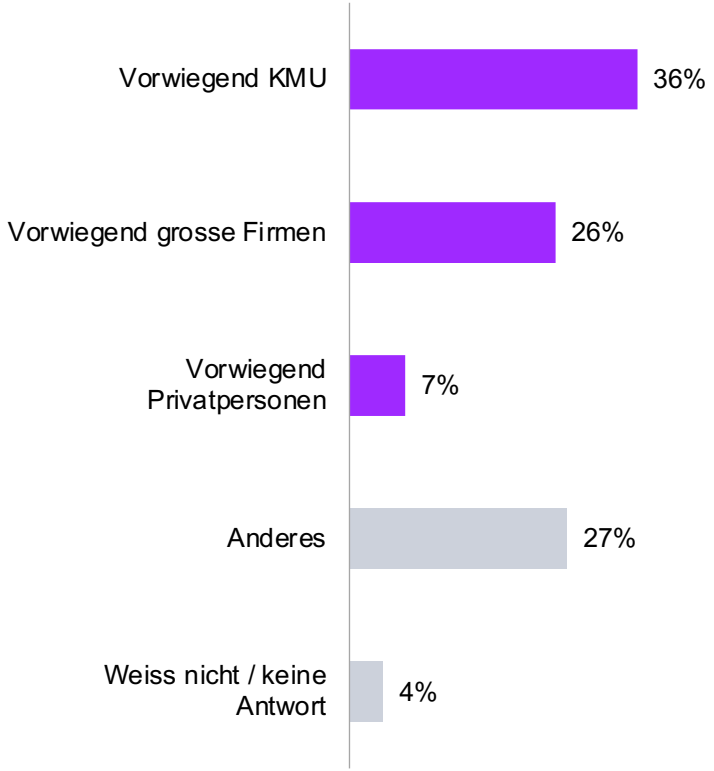
F029: Nutzen Sie für Ihre Datenablage Cloud-Dienstleistungen?
Basis: n=[ ] | Filter: KMU | Geschlossene Frage
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

04 IT-Dienstleister

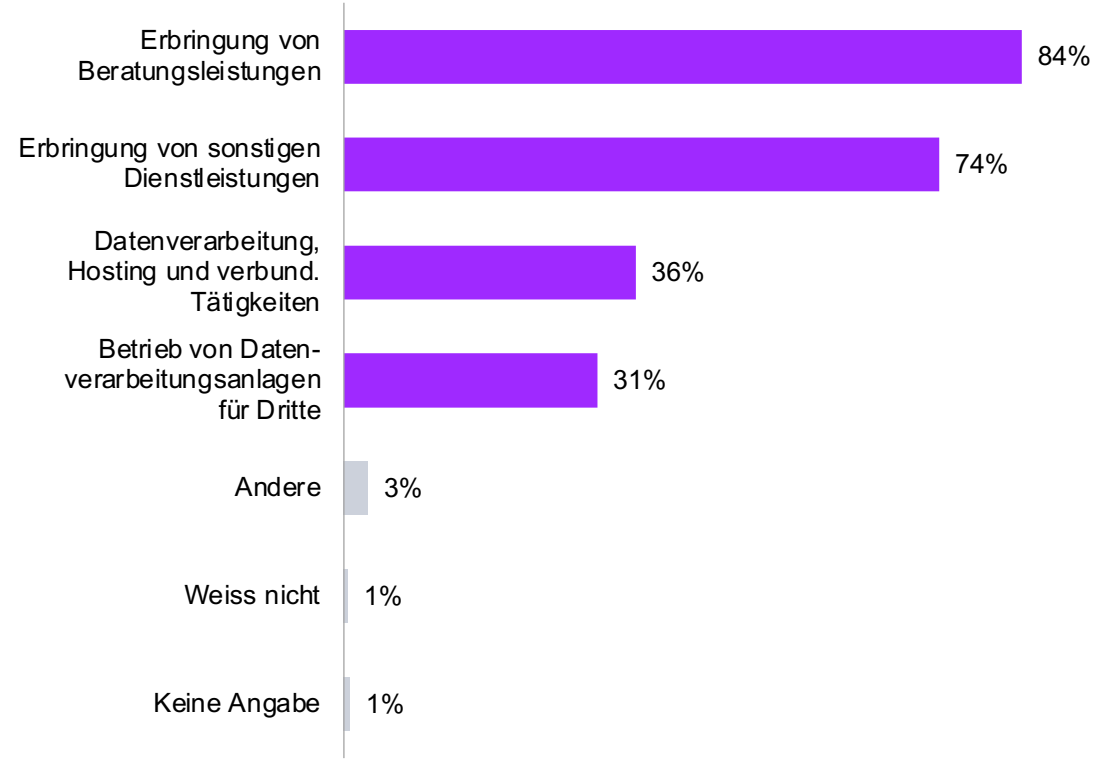
Kunden & Angebot

Die befragten IT-Dienstleister bedienen zu rund einem Drittel vorwiegend KMU und zu rund einem Viertel grosse Firmen. Ihre Haupttätigkeiten sind die Erbringung von Beratungs- und anderen Dienstleistungen.

Verteilung Kundenstamm



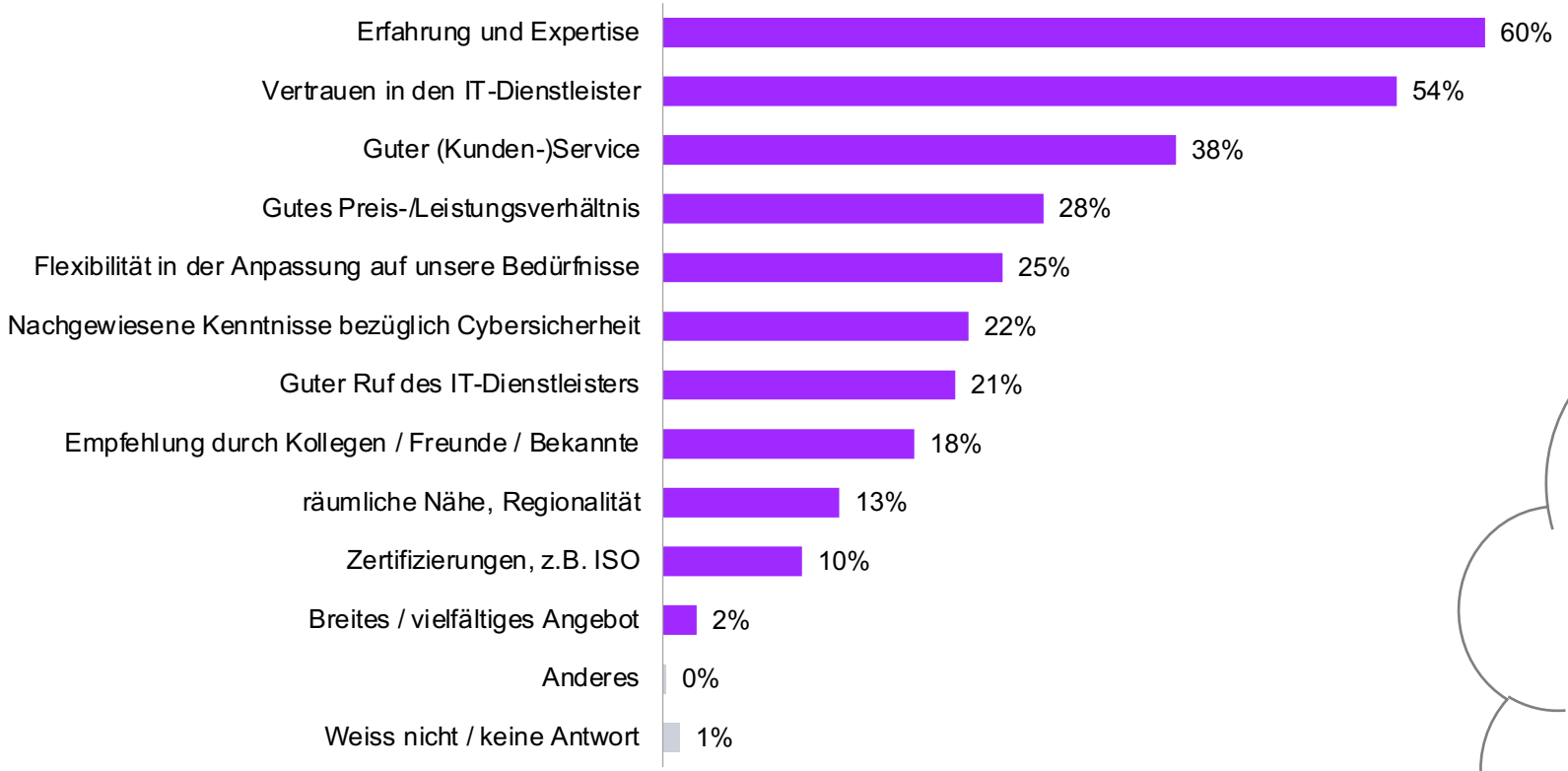
Dienstleistungen



S08: Wie setzt sich der Kundenstamm Ihres Unternehmens ungefähr zusammen? (Eine grobe Schätzung reicht als Antwort) | S10: Welches ist Ihr Angebot?
Basis: n=401 | Filter: IT-Dienstleister | Geschlossene Fragen

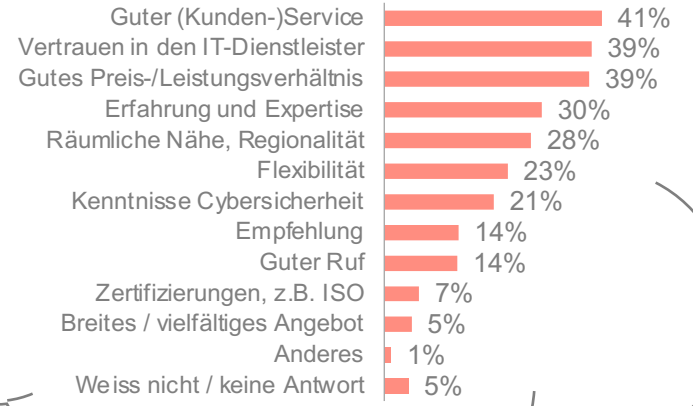
Auswahlkriterien IT-Dienstleister

Aus Sicht der IT-Dienstleister sind Erfahrung und Expertise die wichtigsten Kriterien für die Auswahl eines IT-Dienstleisters, gefolgt von hohem Vertrauen und gutem (Kunden-)Service.



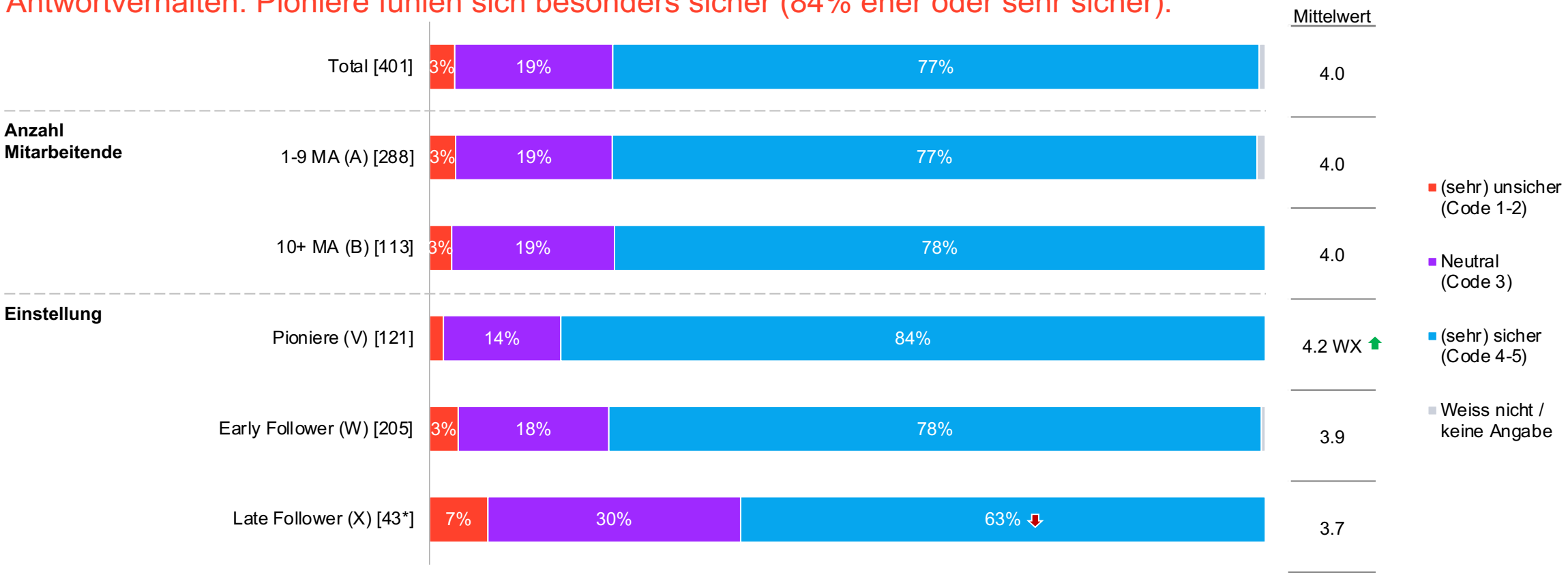
F050: Welche der folgenden Kriterien sind aus Ihrer Sicht für die Auswahl eines IT-Dienstleisters am wichtigsten? Bitte wählen Sie max. 3 Antworten aus.
Basis: n=401 | Filter: IT-Dienstleister | Geschlossene Frage

Aus Sicht der KMU…
ist räumliche Nähe wichtiger als die IT-DL vermuten, guter Service ist am wichtigsten (siehe Seite 17).



Sicherheitsgefühl

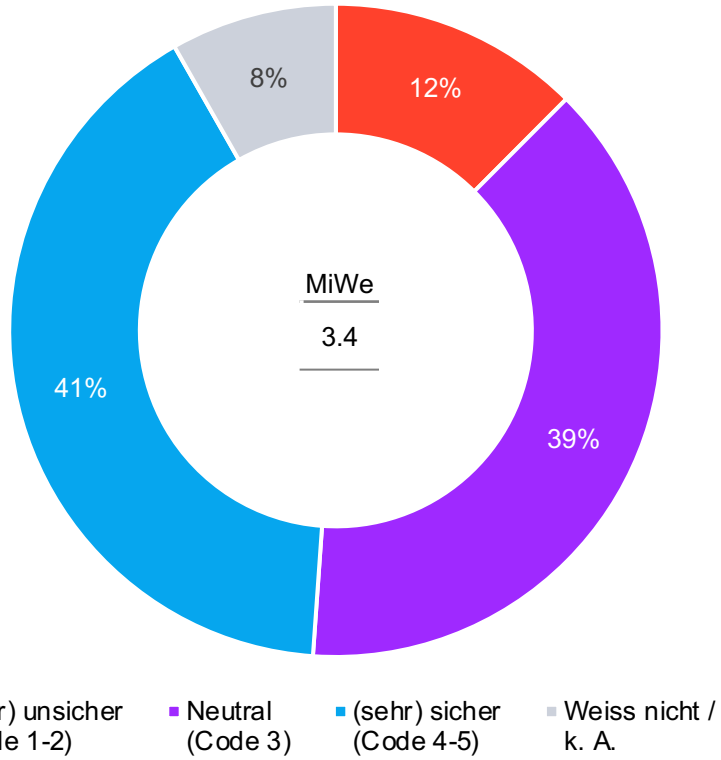
Mehr als drei Viertel der befragten IT-Dienstleister fühlen sich in ihrem Unternehmen (sehr) sicher vor Cyberkriminalität. Zwischen Unternehmen mit unter und über 10 Mitarbeitenden gibt es keinen Unterschied im Antwortverhalten. Pioniere fühlen sich besonders sicher (84% eher oder sehr sicher).



F007: Wie sicher fühlen Sie sich in Ihrem Unternehmen vor Cyberkriminalität?
Basis: n=[ ] | Filter: IT-Dienstleister | Skalierte Frage: 1= sehr unsicher bis 5= sehr sicher | ⬆ signifikant höher als Total; ⬇ signifkant tiefer als Total | *Kleine Basis <50 | Datenbeschriftung ab 3%
Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Sicherheit der Kunden

Die Sicherheit der Kunden wird von den IT-Unternehmen tiefer eingeschätzt als die eigene: Nur rund zwei Fünftel (41%) gehen davon aus, dass ihre Kunden eher oder sehr sicher sind, der Mittelwert liegt bei 3.4 auf der Fünferskala (Eigeneinschätzung: 4.0).

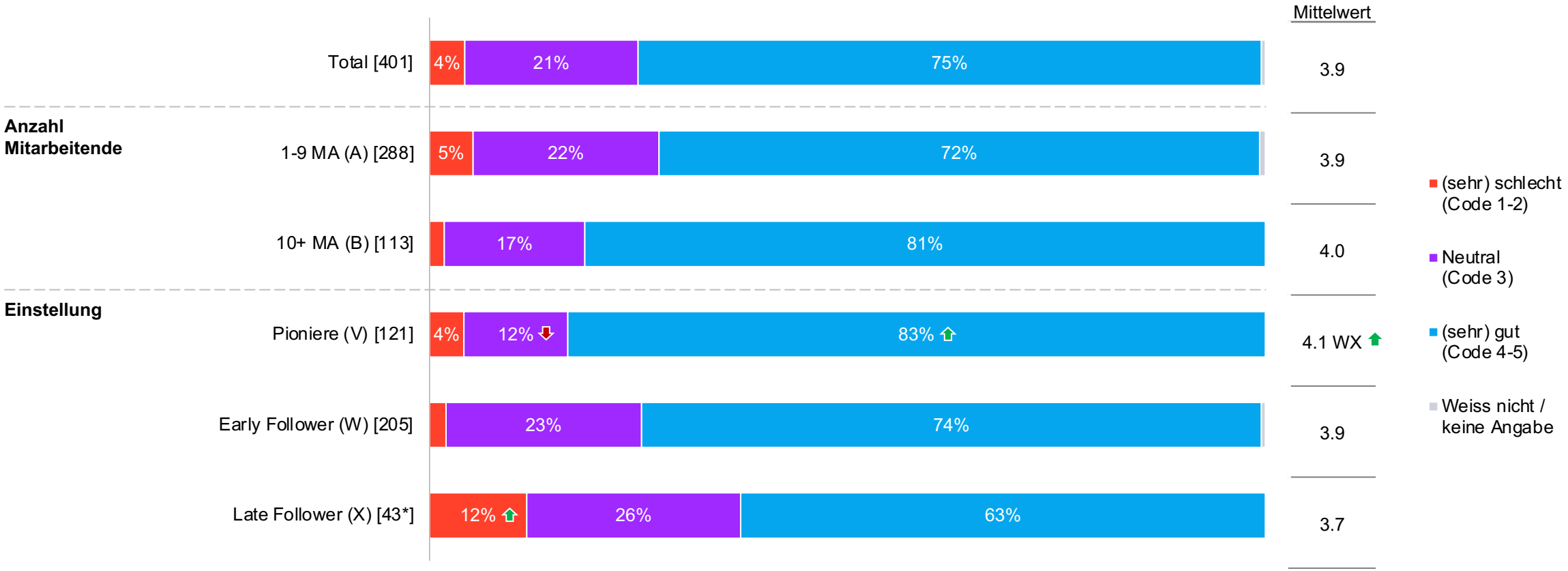


F052. Wie schätzen Sie die Cybersicherheit Ihrer Kunden alles in allem ungefähr ein?
Basis: n=401 | Filter: IT-Dienstleister | Skalierte Fragen (siehe oben)

Aus Sicht der KMU…
57% der befragten KMU fühlen sich eher oder sehr sicher vor Cyberkriminalität (siehe S. 19).

Resilienz

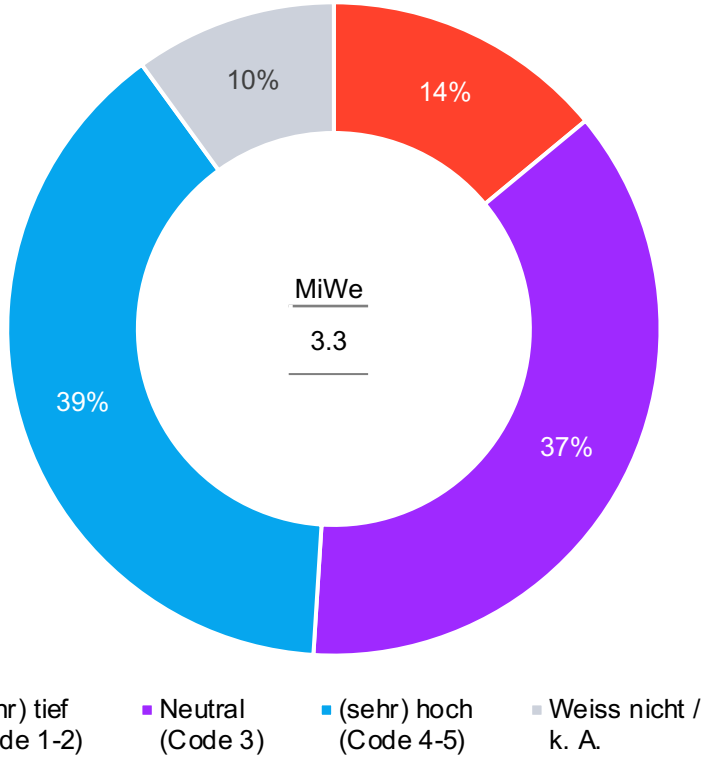
Drei Viertel der befragten IT-Dienstleister fühlen sich eher oder sehr gut vor Cyberangriffen geschützt und auf einen Angriff vorbereitet. Pioniere fühlen sich signifikant besser geschützt als Late Follower.



F008: Was schätzen Sie: Wie gut sind Sie vor Cyberangriffen geschützt und auf einen Angriff vorbereitet?
Basis: n=[ ] | Filter: IT-Dienstleister | Skalierte Frage: 1= sehr schlecht bis 5= sehr gut | ⬆ signifikant höher als Total; ⬇ signifkant tiefer als Total | *Kleine Basis <50 | Datenbeschriftung ab 3%
Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Resilienz der Kunden

Auch die Resilienz der Kunden wird von den IT-Unternehmen tiefer eingeschätzt als die eigene: Nur rund zwei Fünftel (39%) der Befragten schätzen die Resilienz ihrer Kunden eher oder sehr hoch ein, der Mittelwert liegt bei 3.3 auf der Fünferskala (Eigeneinschätzung: 3.9).

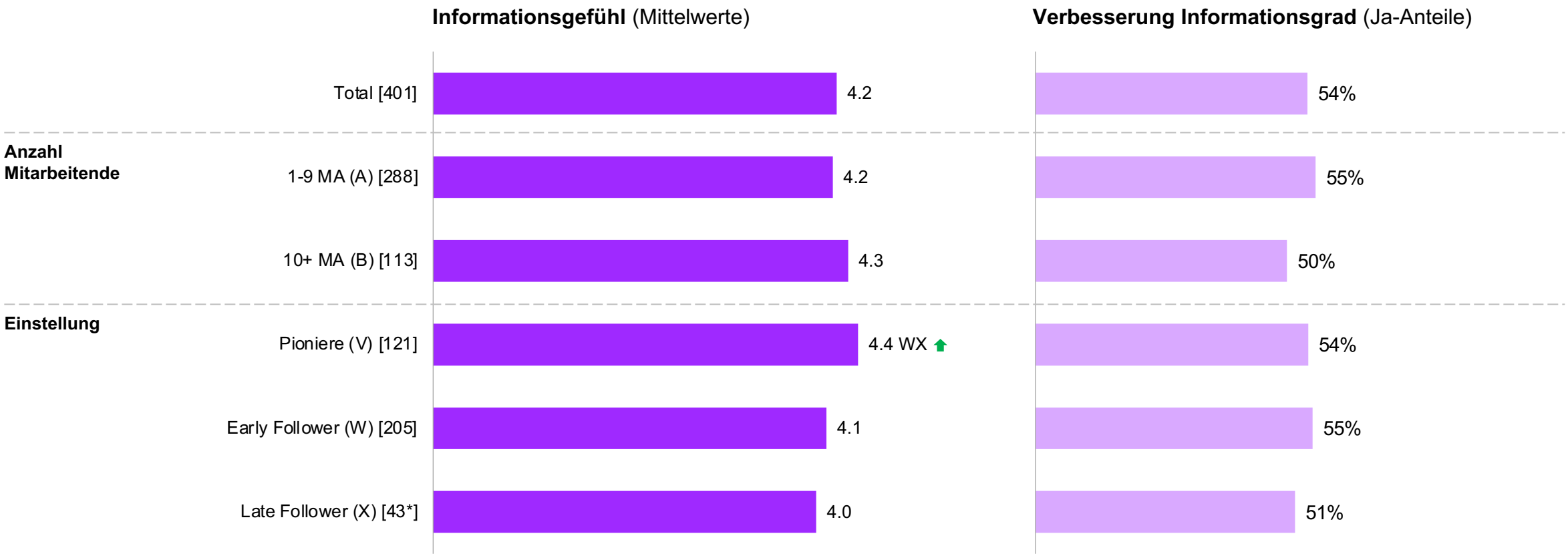


F053. Wie schätzen Sie die Widerstandsfähigkeit Ihrer Kunden gegen Cyberangriffe alles in allem ungefähr ein?
Basis: n=401 | Filter: IT-Dienstleister | Skalierte Fragen (siehe oben)

Aus Sicht der KMU…
55% der befragten KMU fühlen sich eher oder sehr gut geschützt und auf einen Angriff vorbereitet (siehe S. 20).

Informationsgrad

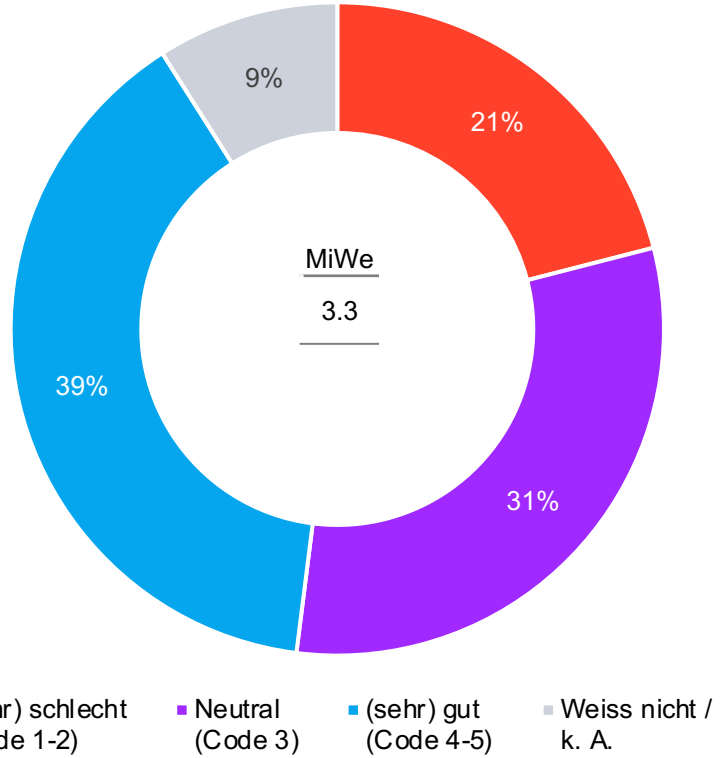
IT-Dienstleister fühlen sich sehr gut informiert bezüglich Cyberrisk-Thematik; auf der Fünferskala geben sie im Durchschnitt eine 4.2 an. Rund die Hälfte der Befragten wäre gerne besser informiert zum Thema Cybersicherheit.



F009: Wie gut fühlen Sie sich persönlich in der Cyberrisk-Thematik informiert? | F010: Wären Sie gerne besser informiert über das Thema Cybersicherheit?
Basis: n=[ ] | Filter: IT-Dienstleister | Skalierte Frage: 1= sehr schlecht bis 5= sehr gut (F009) & geschlossene Frage (F010) | ⬆ signifikant höher als Total; ⬇ signifkant tiefer als Total | *Kleine Basis <50
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Informationsgrad der Kunden

Die befragten IT-Dienstleistungsunternehmen sind der Meinung, dass ihre Kunden deutlich schlechter informiert sind als sie selber: Knapp zwei Fünftel gehen von einem eher oder sehr guten, rund ein Fünftel von einem eher oder sehr schlechten Informationsgrad der Kunden aus. Der Mittelwert liegt bei 3.3 (Eigeneinschätzung: 4.2)

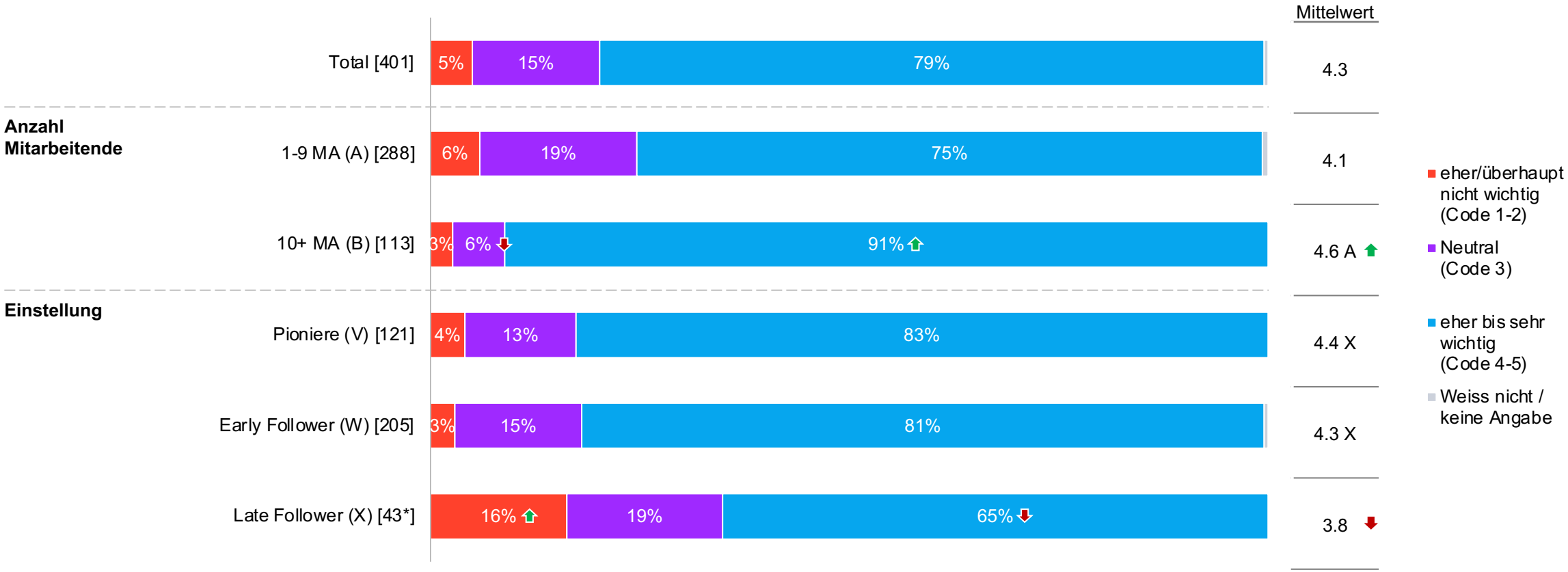


F054. Wie gut sind - Ihrer Meinung nach - Ihre Kunden zur Cyberrisk-Thematik informiert?
Basis: n=401 | Filter: IT-Dienstleister | Skalierte Fragen (siehe oben)

Aus Sicht der KMU…
Der gefühlte Informationsgrad der befragten KMU liegt bei 3.4 auf der Fünferskala (siehe S. 21).

Priorität Cybersicherheit

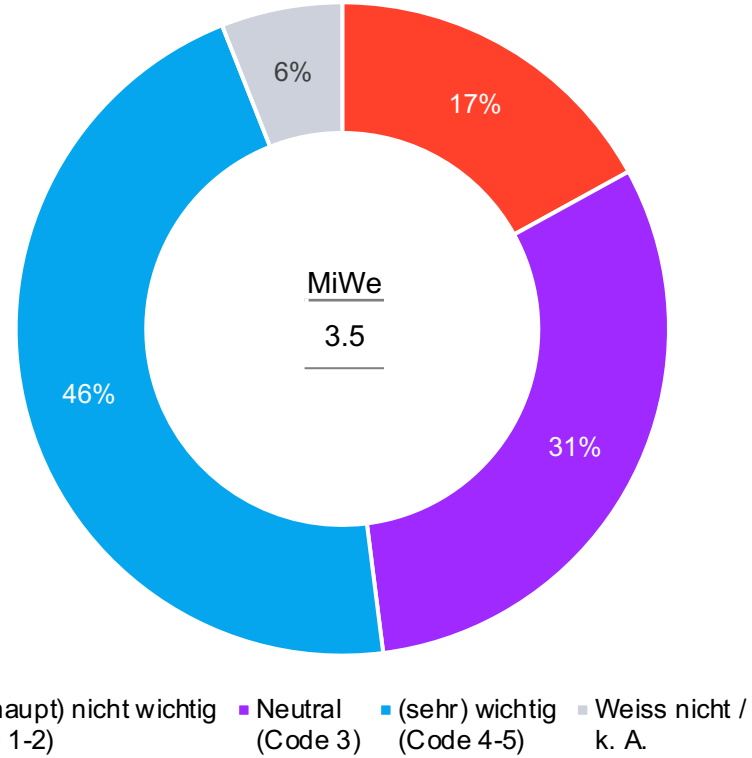
Fast acht von zehn der befragten IT-Dienstleistern geben dem Thema Cybersicherheit in ihrer Firma eine eher bis sehr hohe Priorität (Mittelwert 4.3). Bei Firmen mit über 10 Mitarbeitenden sind es sogar 9 von 10.



F011: Welche Priorität hat in Ihrer Firma das Thema Cybersicherheit?
Basis: n=[ ] | Filter: IT-Dienstleister | Skalierte Frage: 1= überhaupt nicht wichtig bis 5= sehr wichtig | ⬆ signifikant höher als Total; ⬇ signifkant tiefer als Total | *Kleine Basis <50 | Datenbeschriftung ab 3%
Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Priorität Cybersicherheit bei den Kunden

Gemäss den IT-Unternehmen nehmen ihre Kunden das Thema Cybersicherheit deutlich weniger wichtig als sie selber: Nur knapp die Hälfte (46%) geht von einer eher oder sehr hohen Priorität bei den Kunden aus, der Mittelwert liegt bei 3.5 auf der Fünferskala (Eigeneinschätzung: 4.3).



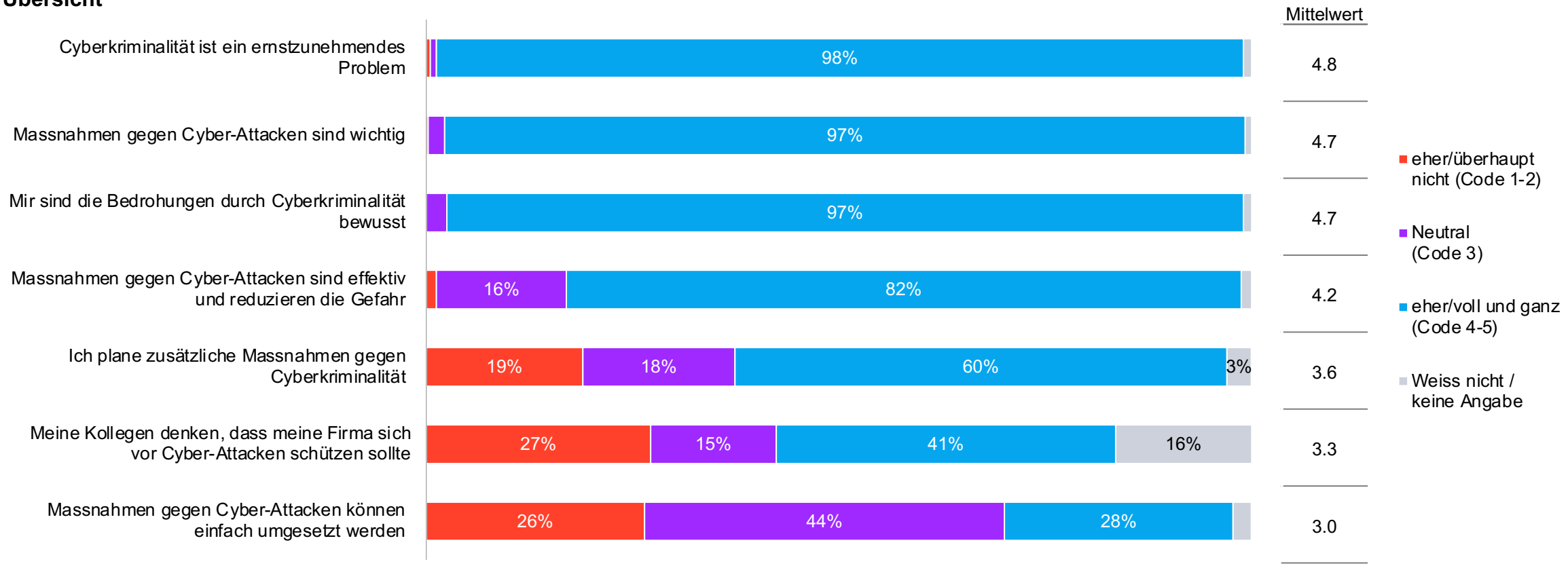
F055. Was schätzen Sie, alles in allem: Welche Priorität hat das Thema Cybersicherheit bei Ihren Kunden?
Basis: n=401 | Filter: IT-Dienstleister | Skalierte Fragen (siehe oben)

Aus Sicht der KMU…
47% der befragten KMU geben der Cybersicherheit in ihrem Unternehmen eine (sehr) hohe Priorität (siehe S. 22).

Einstellung zu Cyberkriminalität (1/3)

Fast alle befragten IT-Unternehmer stimmen den Aussagen zu, dass Cyberkriminalität ein ernstes Problem ist und Massnahmen dagegen wichtig. Es sind auch fast alle der Meinung, dass ihnen die Bedrohungen bewusst sind. Sie finden aber die Massnahmenumsetzung nicht so einfach: Rund ein Viertel widerspricht dieser Aussage.

Übersicht

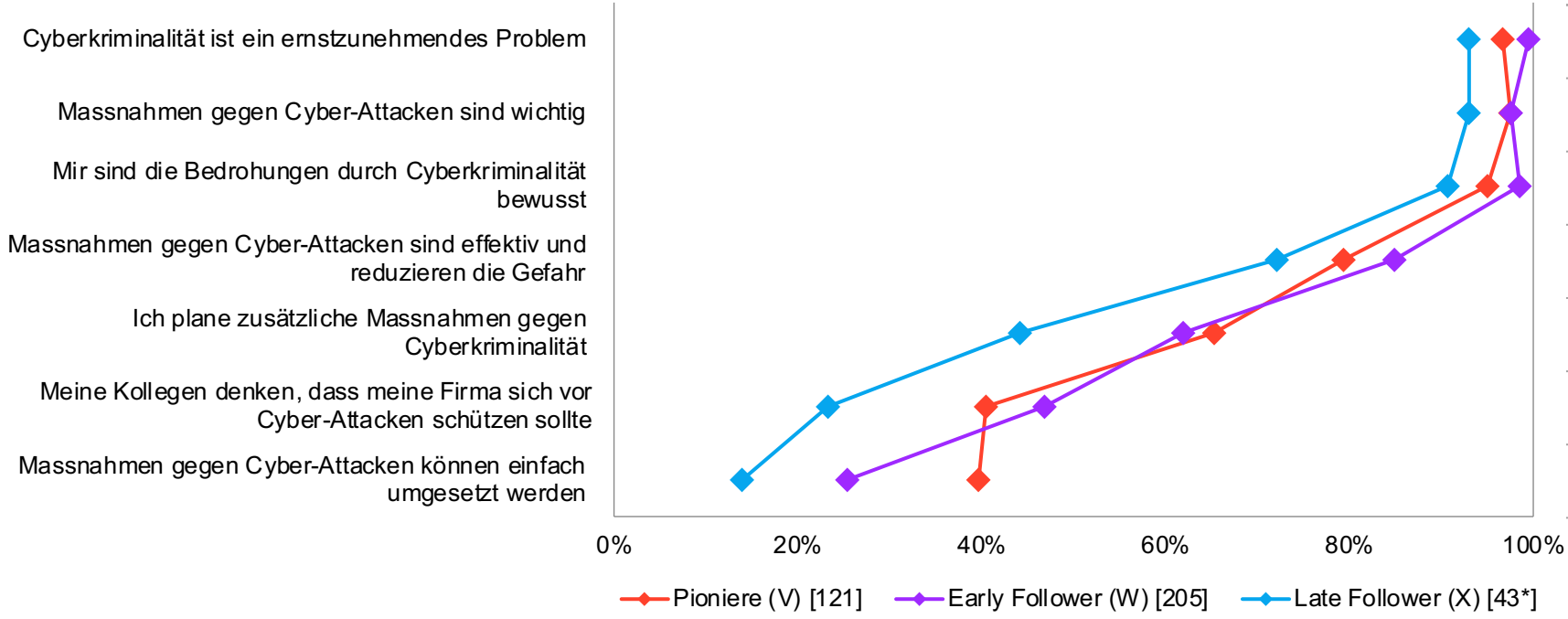


F015: Inwiefern stimmen Sie den folgenden Aussagen zu Cyberkriminalität wie Malware, Online-Betrug und Hacking zu?
Basis: n=401 | Filter: IT-Dienstleister | Skalierte Frage: 1= überhaupt nicht bis 5= voll und ganz | Datenbeschriftung ab 3%

Einstellung zu Cyberkriminalität (2/3)

Pioniere, Early und Late Follower unter den IT-Dienstleistern sind weitgehend gleicher Meinung, wenn es um das Thema Cyberkriminalität geht. Pioniere und Early Follower finden die Massnahmen gegen Cyberkriminalität allerdings einfacher umsetzbar als Late Follower.

Nach Einstellung



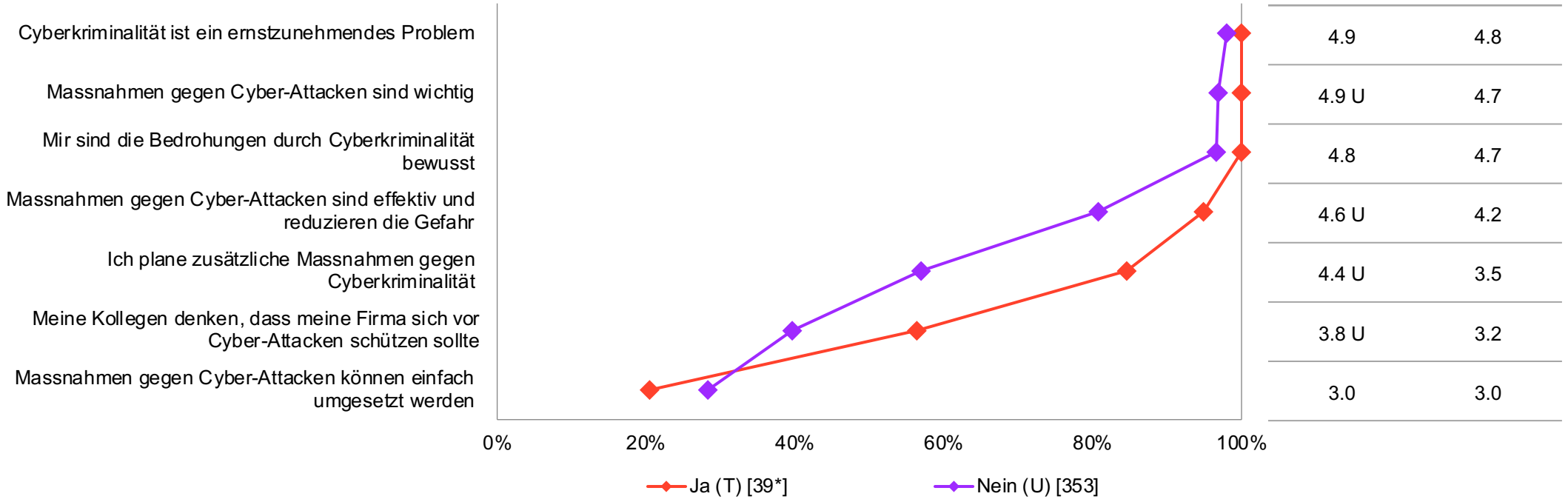
	Mittelwert		
	Pioniere	Early Follower	Late Follower
Cyberkriminalität ist ein ernstzunehmendes Problem	4.9	4.8	4.7
Massnahmen gegen Cyber-Attacken sind wichtig	4.8	4.7	4.7
Mir sind die Bedrohungen durch Cyberkriminalität bewusst	4.7	4.7	4.7
Massnahmen gegen Cyber-Attacken sind effektiv und reduzieren die Gefahr	4.3	4.2	4.1
Ich plane zusätzliche Massnahmen gegen Cyberkriminalität	3.8	3.6	3.3
Meine Kollegen denken, dass meine Firma sich vor Cyber-Attacken schützen sollte	3.2	3.4 X	2.8
Massnahmen gegen Cyber-Attacken können einfach umgesetzt werden	3.3 WX	3.0 X	2.7

F015: Inwiefern stimmen Sie den folgenden Aussagen zu Cyberkriminalität wie Malware, Online-Betrug und Hacking zu?
Basis: n=[ ] | Filter: IT-Dienstleister | Skalierte Frage: 1= überhaupt nicht bis 5= voll und ganz | Top2 und Mittelwerte ausgewiesen | *Kleine Basis <50
signifikant höher als Total; signifikant tiefer als Total | Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Einstellung zu Cyberkriminalität (3/3)

IT-Dienstleister mit IT-Sicherheitszertifikat stimmen vier von sieben Aussagen zu Cyberkriminalität signifikant stärker zu als diejenigen ohne Zertifikat.

Nach IT-Sicherheitszertifikat



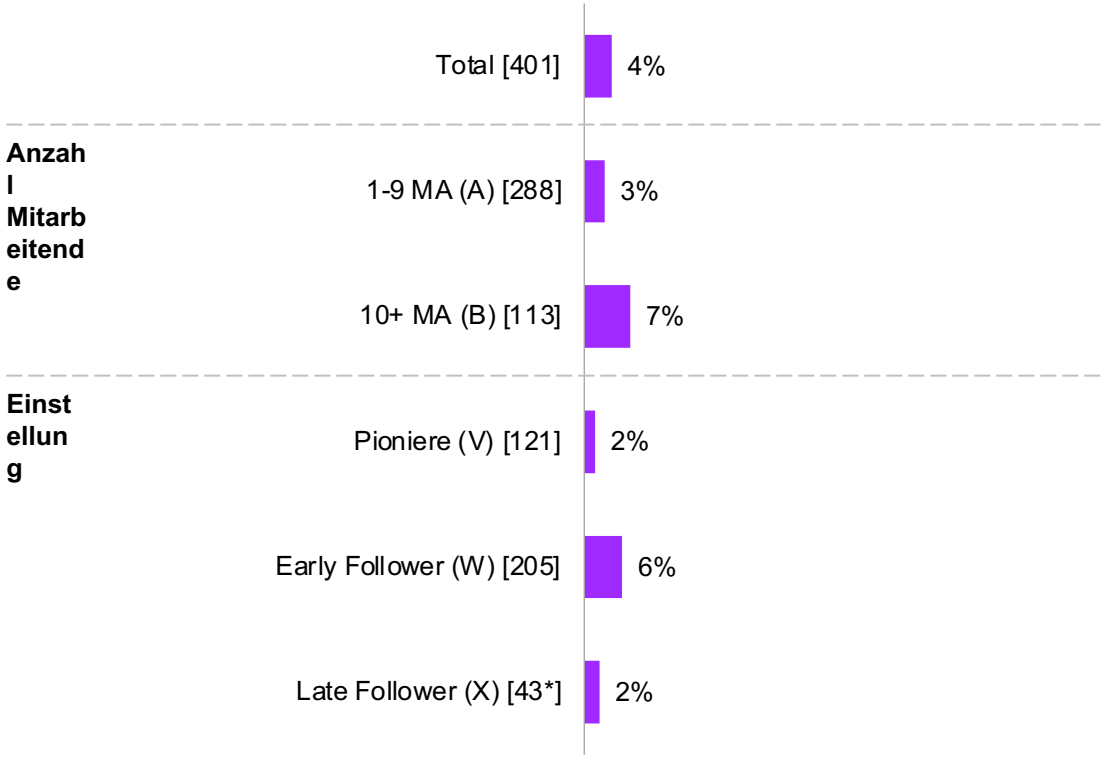
	Mittelwert	
	Zertifikat ja	Zertifikat nein
Cyberkriminalität ist ein ernstzunehmendes Problem	4.9	4.8
Massnahmen gegen Cyber-Attacken sind wichtig	4.9 U	4.7
Mir sind die Bedrohungen durch Cyberkriminalität bewusst	4.8	4.7
Massnahmen gegen Cyber-Attacken sind effektiv und reduzieren die Gefahr	4.6 U	4.2
Ich plane zusätzliche Massnahmen gegen Cyberkriminalität	4.4 U	3.5
Meine Kollegen denken, dass meine Firma sich vor Cyber-Attacken schützen sollte	3.8 U	3.2
Massnahmen gegen Cyber-Attacken können einfach umgesetzt werden	3.0	3.0

F015: Inwiefern stimmen Sie den folgenden Aussagen zu Cyberkriminalität wie Malware, Online-Betrug und Hacking zu?
Basis: n=[ ] | Filter: IT-Dienstleister | Skalierte Frage: 1= überhaupt nicht bis 5= voll und ganz | Top2 und Mittelwerte ausgewiesen | *Kleine Basis <50
signifikant höher als Total; signifikant tiefer als Total | Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Erfahrung Cyberkriminalität

Jedes 25. IT-Unternehmen hat in den letzten 3 Jahren einen erfolgreichen Cyberangriff erlebt. In 15 Fällen entstand daraus ein grosser Aufwand zur Behebung und 9 bzw. 8 Betroffene erwähnen auch emotionale Belastung und einen finanziellen Schaden.

Erlittene Angriffe (Ja-Anteile)
Filter: IT-Dienstleister



Erlittene Schäden
Basis: 17** | Filter: IT-Dienstleister – wenn Cyberangriff erlitten

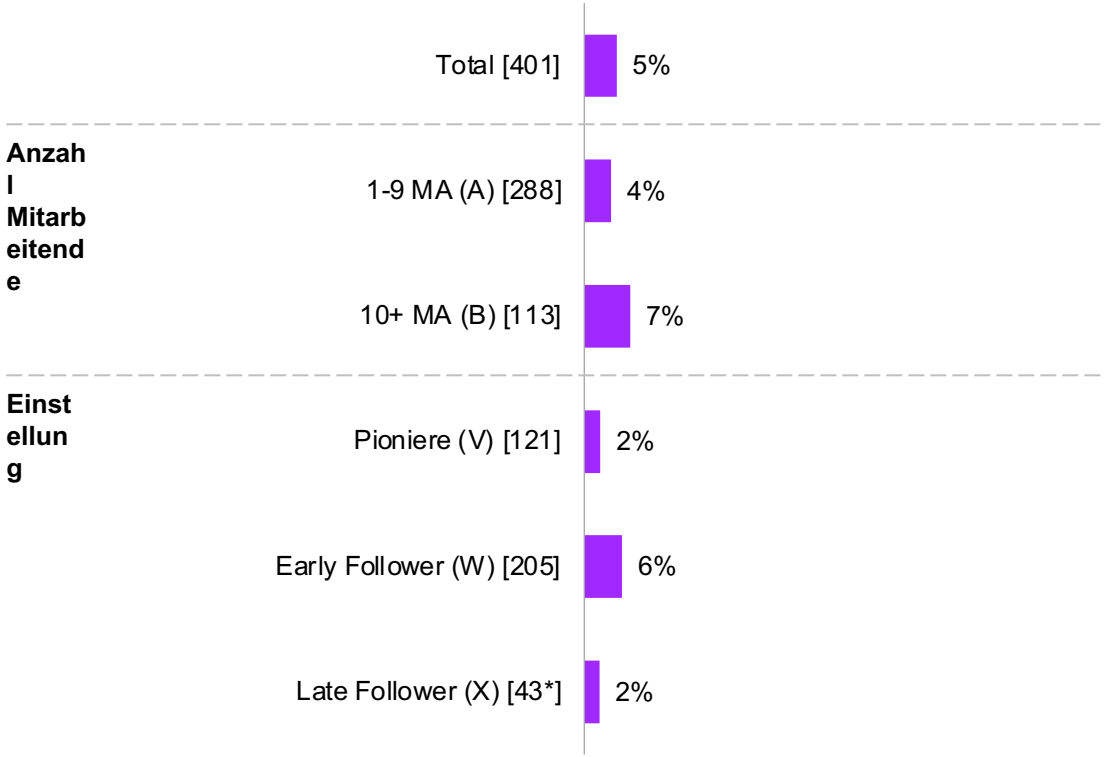
Schäden	Anzahl Fälle
Ein grosser Arbeitsaufwand zur Behebung	15
Emotionale Belastung	9
Ein finanzieller Schaden	8
Ein Reputationsschaden	3
Ein Kundendatenverlust	3
Nichts davon	1
Weiss nicht / keine Antwort	0

F016: Hat Ihr Unternehmen innerhalb der letzten 3 Jahre einen Cyberangriff erlitten, der einen finanziellen Schaden oder einen Reputationsschaden verursachte, viel Mühe für die Schadensbereinigung bereitete oder Ihnen emotional sehr zu schaffen gemacht hat? | F017: Entstand durch diesen Angriff… | Basis: n=[ ] | Filter: siehe oben | Geschlossene Fragen | ⬆ signifikant höher als Total; ⬇ signifkant tiefer als Total | *Kleine Basis <50; **Sehr kleine Basis <30
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

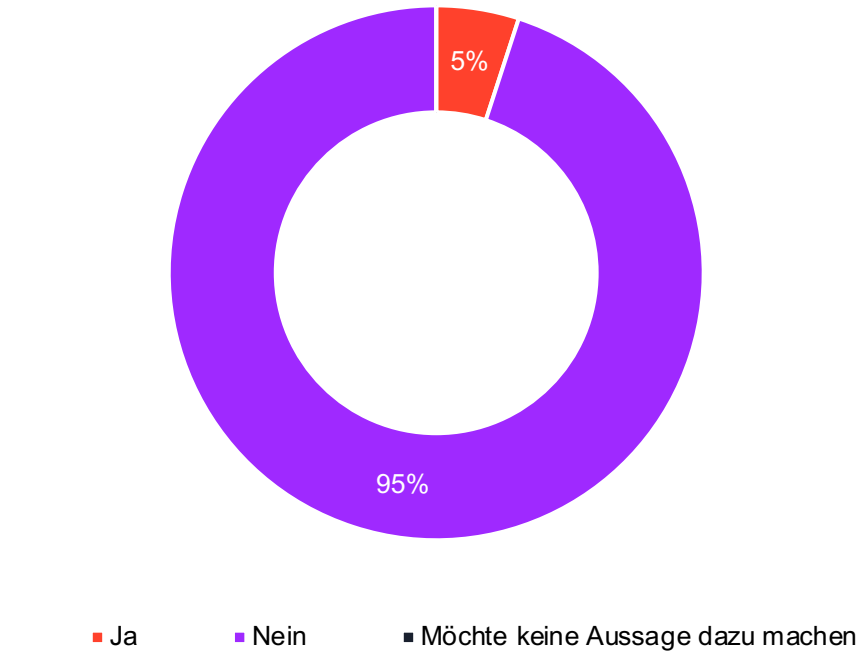
Erpressung

Jedes zwanzigste befragte IT-Unternehmen wurde schon einmal von Cyberkriminellen erpresst; von den 20 betroffenen Unternehmen gibt eines an, Lösegeld bezahlt zu haben.

Erpressung durch Cyberkriminelle (Ja-Anteile)
Filter: IT-Dienstleister



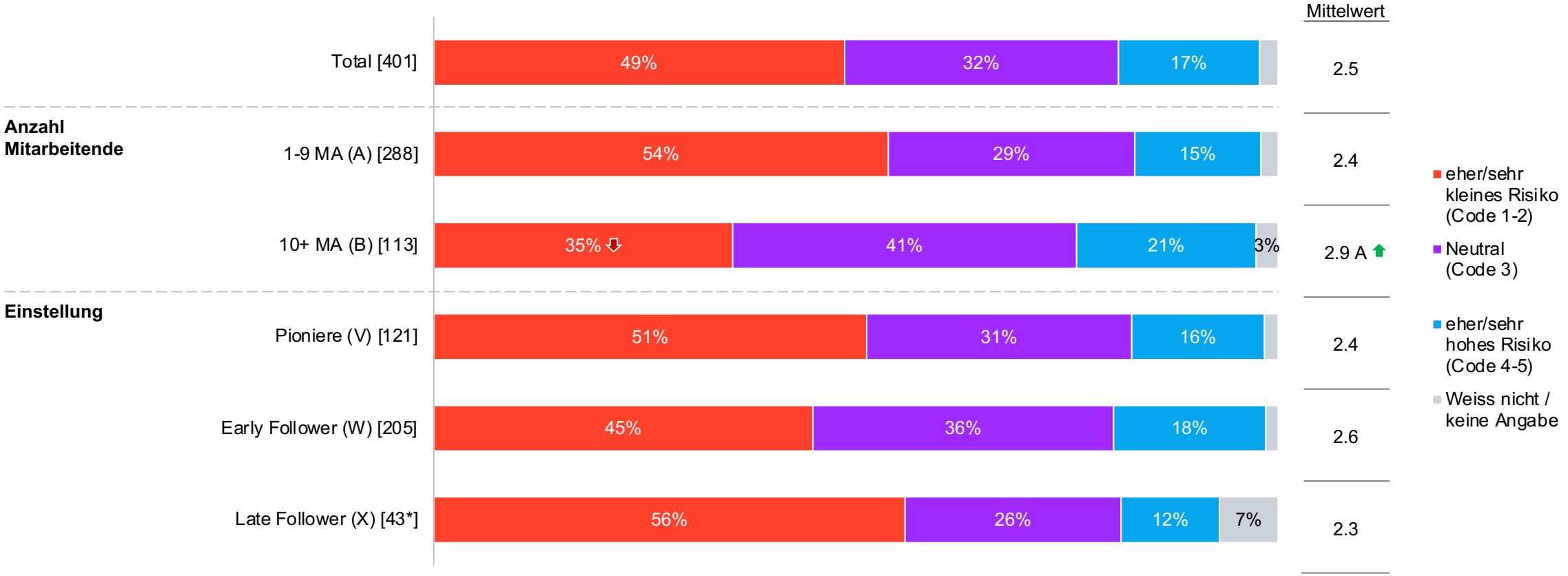
Lösegeld an Cyberkriminelle
Basis: 20 | Filter: IT-Dienstleister – wenn erpresst durch Cyberkriminelle



F019: Wurde Ihr Unternehmen schon einmal von Cyberkriminellen erpresst? | F020: Hat Ihr Unternehmen schon einmal Lösegeld an Cyberkriminelle bezahlt?
Basis: n=[ ] | Filter: siehe oben | Geschlossene Fragen | ⬆ signifikant höher als Total; ⬇ signifkant tiefer als Total | *Kleine Basis <50
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Risikoeinschätzung

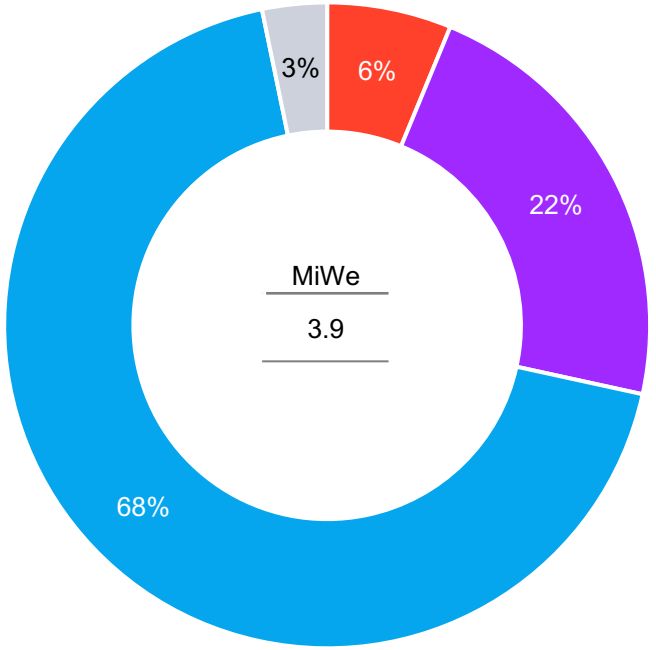
Knapp ein Fünftel (17%) der befragten IT-Unternehmen schätzt das Risiko, innerhalb der nächsten 2-3 Jahre durch einen Cyberangriff für mindestens einen Tag ausser Kraft gesetzt zu werden, eher oder sehr hoch ein. Unternehmen mit mehr als 10 Mitarbeitenden gehen signifikant häufiger von einem eher/sehr hohen Risiko aus.



F021: Wie hoch schätzen Sie das Risiko ein, dass Ihr Unternehmen innerhalb der nächsten 2-3 Jahre durch einen Cyberangriff mindestens einen Tag lang ausser Kraft gesetzt wird?
Basis: n=[ ] | Filter: IT-Dienstleister | Skalierte Frage: 1= sehr kleines Risiko bis 5= sehr grosses Risiko | ⬆ signifikant höher als Total; ⬇ signifkant tiefer als Total | *Kleine Basis <50 | Datenbeschriftung ab 3%
Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Risikoeinschätzung Schweizer KMU

Seitens Schweizer KMU sehen bedeutend mehr IT-Dienstleistungs-Unternehmen ein eher oder sehr hohes Risiko als bei sich selbst, durch einen Cyberangriff ausser Kraft gesetzt zu werden: Mehr als zwei Drittel (68%) schätzen das Risiko eher oder sehr hoch ein, nur rund jeder zwanzigste (6%) eher oder sehr tief.

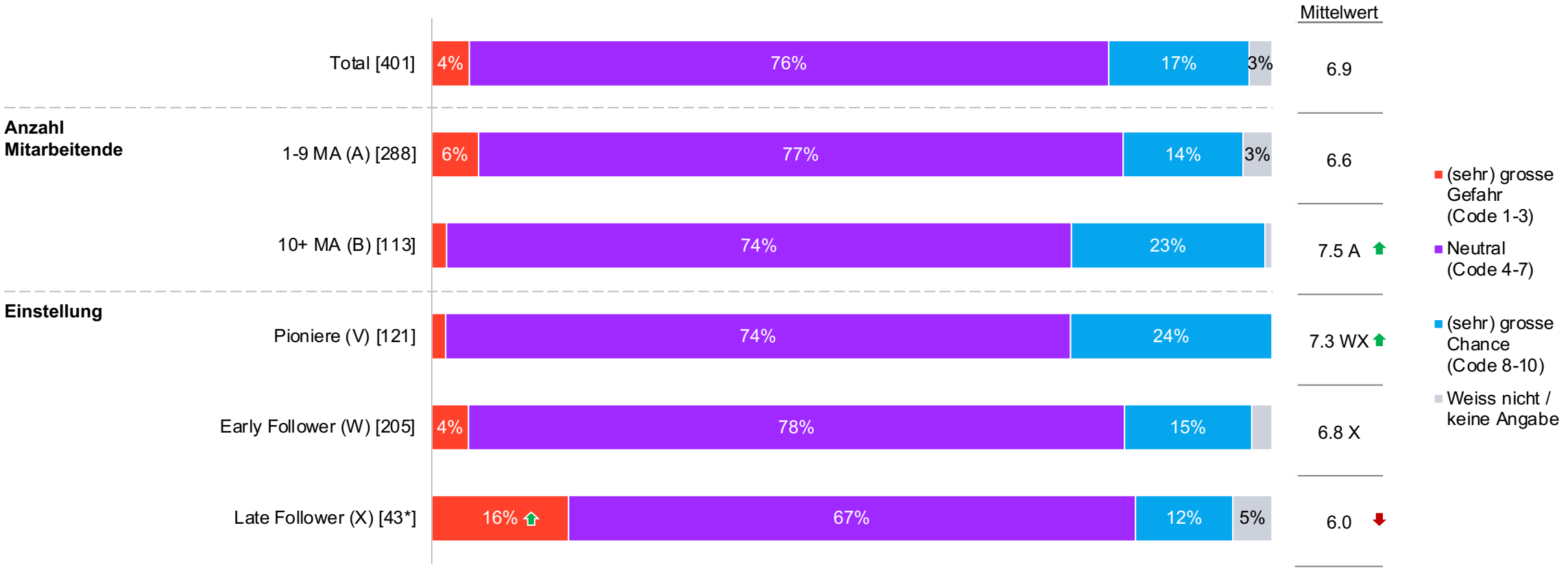


Aus Sicht der KMU…
Die befragten KMU empfinden dieses Risiko als deutlich geringer: Nur 12% schätzen es als (sehr) hoch ein, der Mittelwert liegt bei 2.3 (siehe S. 41).

F057: Wie hoch schätzen Sie das Risiko für ein durchschnittliches Schweizer KMU ein, innerhalb der nächsten 2-3 Jahre durch einen Cyberangriff für mindestens einen Tag ausser Kraft gesetzt zu werden?
Basis: n=401 | Filter: IT-Dienstleister | Skalierte Frage: 1= sehr kleines Risiko bis 5= sehr grosses Risiko

Einstellung zu KI

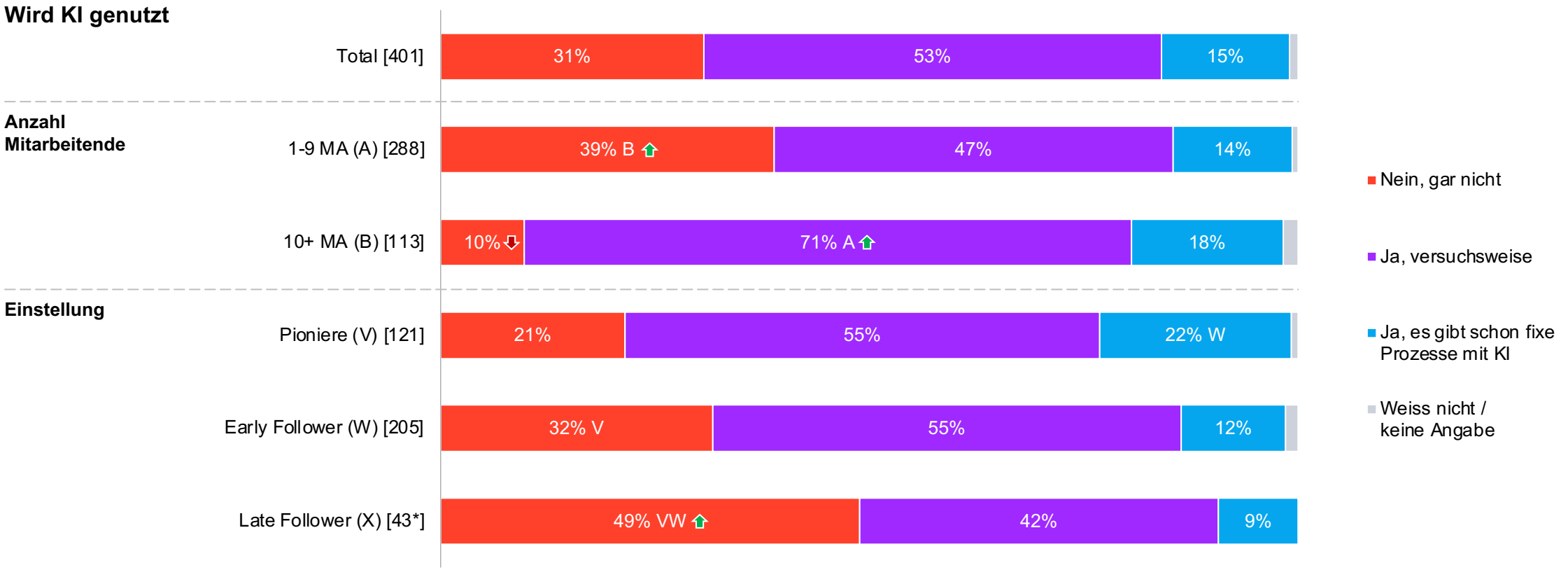
Etwas weniger als jedes fünfte IT-Unternehmen (17%) sieht in KI eine (sehr) grosse Chance für die Zukunft des Unternehmens, nur ganz wenige (4%) eine (sehr) grosse Gefahr. Die grosse Mehrheit (76%) hat eine neutrale Haltung dazu, Unternehmen ab 10 Mitarbeitenden und Pioniere sind aufgeschlossener gegenüber KI.



F023: Sehen Sie in den technischen Fortschritten künstlicher Intelligenz eher eine Gefahr oder eine Chance für die Zukunft Ihres Unternehmens?
Basis: n=[ ] | Filter: IT-Dienstleister | Skalierte Frage: 1= sehr grosse Gefahr bis 10= sehr grosse Chance | ⬆ signifikant höher als Total; ⬇ signifkant tiefer als Total | *Kleine Basis <50 | Datenbeschriftung ab 3%
Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Nutzung KI

Etwas mehr zwei Drittel der befragten IT-Unternehmen setzen KI schon versuchsweise (53%) oder in fixen Prozessen (15%) ein. In Unternehmen mit über 10 Mitarbeitenden gibt es signifikant häufiger versuchsweise Einsätze und je aufgeschlossener die Befragten ggü. neuen Technologien sind, desto häufiger setzen sie KI ein.

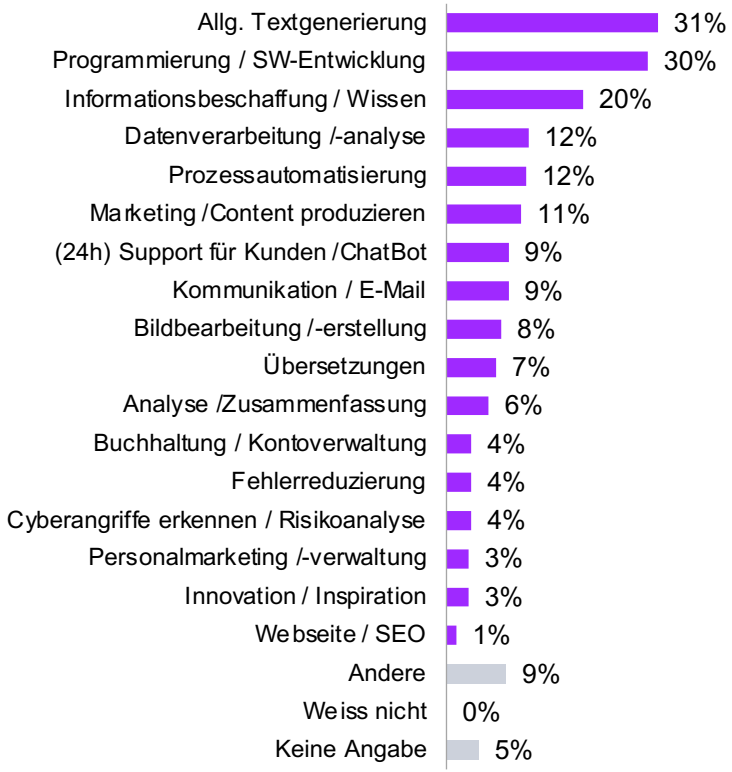


F024: Wird in Ihrem Unternehmen schon aktiv künstliche Intelligenz eingesetzt?
Basis: n=[ ] | Filter: IT-Dienstleister | Geschlossene Frage | ⬆ signifikant höher als Total; ⬇ signifkant tiefer als Total | *Kleine Basis <50 | Datenbeschriftung ab 3%
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Nutzung KI

KI wird von knapp einem Drittel ihrer Nutzer in IT-Unternehmen für Textgenerierung und Programmierungen bzw. Software-Entwicklungen verwendet. Ein Fünftel verwendet KI für die Informations- und Wissensbeschaffung.

Wofür wird KI genutzt



Création de contenu visuel et écrit.

Zur Optimierung von Kollaborationen, um Use-Cases für Kunden zu erproben.

Bildbearbeitung, Untertitelung

Améliorer la vitesse de développement de certaines parties du code informatique

Datenverarbeitung und Automationen. Hilfe bei Programmierung, Textverarbeitung etc.

Arbeitszeugnisse, GIS (geoportal.ch): Abfragen und Dialoge

div. Mustererkennungen

Prototypage, aide au développement, premier jets de documentation, traductions.

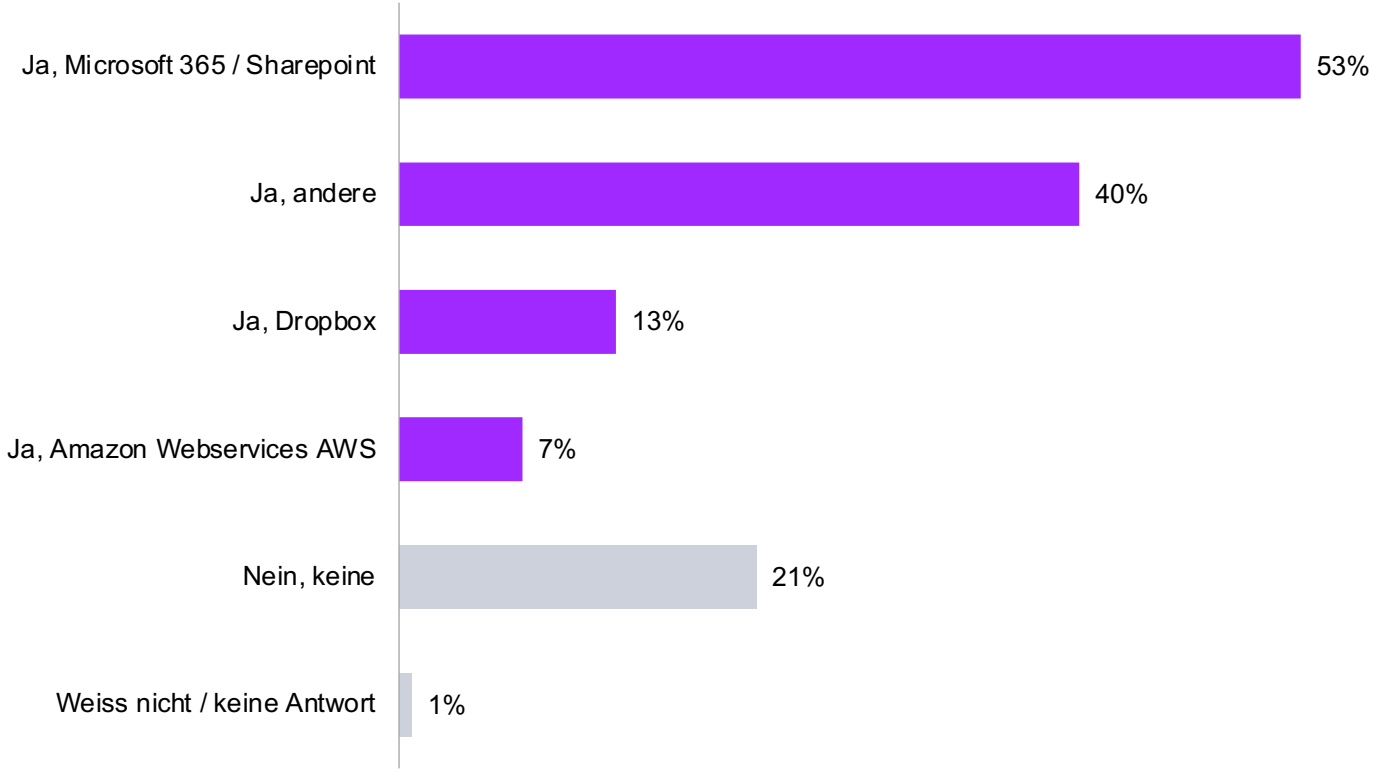
Erkennen von Cyber Security Mustern, Angriffen, Vorkommnissen

Regeln für Behaviour Analytics

F025: Wofür wird KI in Ihrem Unternehmen eingesetzt? Bitte erläutern Sie.
Basis: n=274 | Filter: IT-Dienstleister - Wenn KI genutzt wird | Offene Frage

Cloudnutzung

Über die Hälfte der befragten IT-Dienstleister nutzt mit Microsoft 365 bzw. Sharepoint Cloud-Dienstleistungen; bei den Unternehmen mit über 10 Mitarbeitenden liegt der Anteil deutlich höher (81%, nicht abgebildet). Viele Unternehmen nutzen mehr als eine Cloud-Lösung; nur rund ein Fünftel nutzt gar keine.

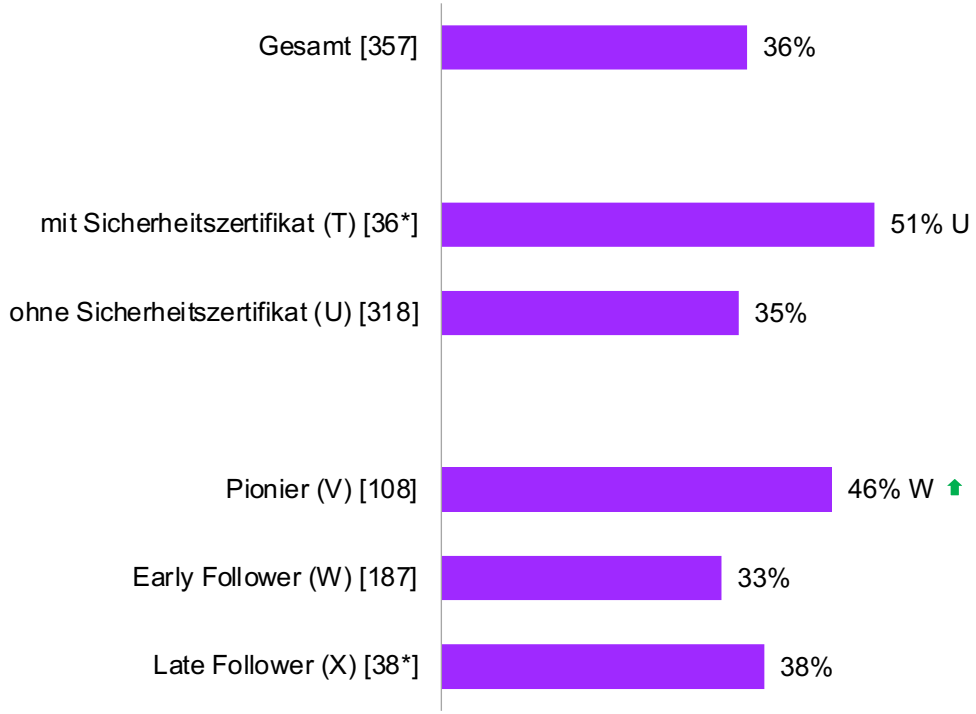


F029: Nutzen Sie für Ihre Datenablage Cloud-Dienstleistungen?
Basis: n=401 | Filter: IT-Dienstleister | Geschlossene Frage

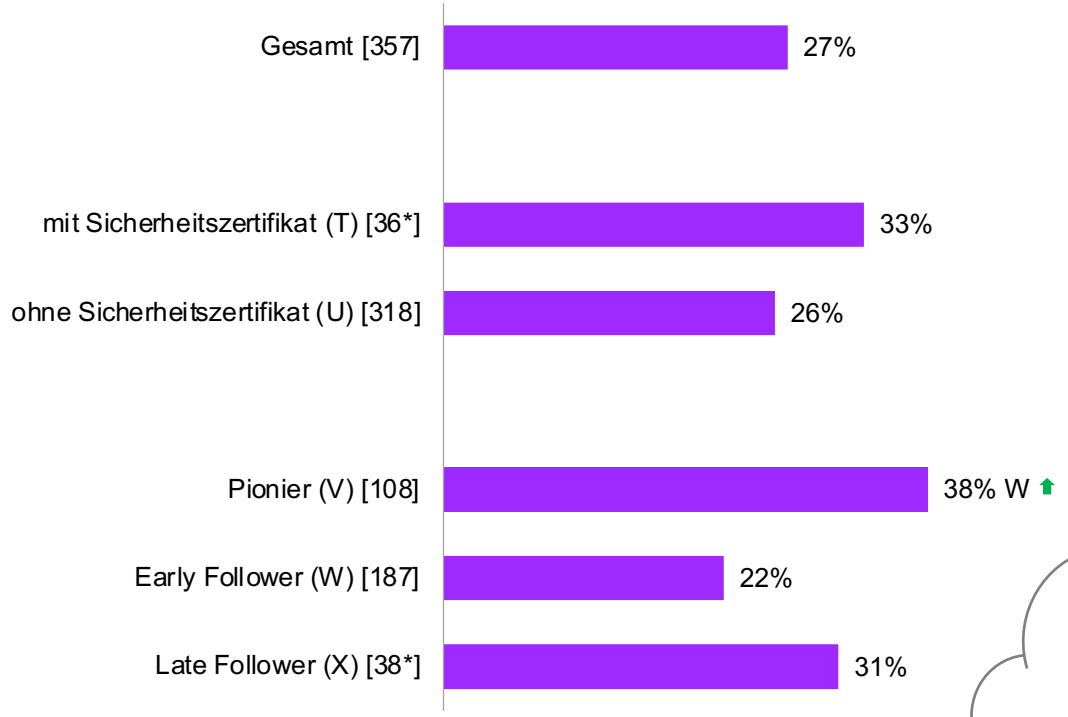
Prozentualer Anteil outgesourcter IT-Arbeiten

Die befragten IT-Dienstleistungunternehmen sind bei durchschnittlich rund einem Drittel ihrer Kunden für technische, und bei rund einem Viertel für organisatorische Cybersicherheits-Massnahmen zuständig.

Zuständig für technische Cybersicherheits-Massnahmen bei durchschnittlich…:



Zuständig für organisatorische Cybersicherheits-Massnahmen bei durchschnittlich…:

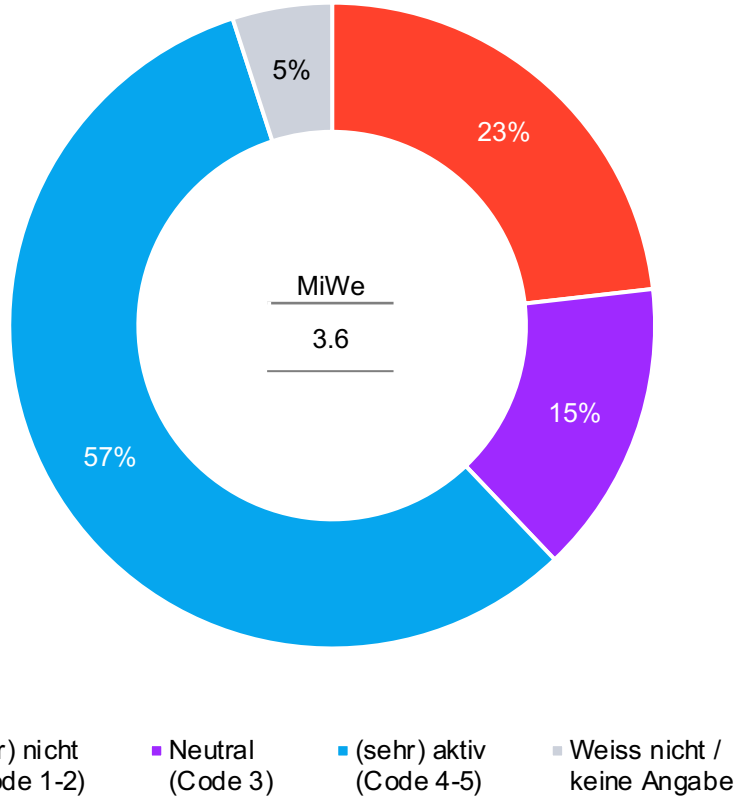


F051: Bei wie vielen Ihrer Kunden sind Sie zumindest teilweise zuständig für…
Basis: n=[ ] | Filter: IT-Dienstleister | Geschlossene Frage ⬆ signifikant höher als Total; ⬇ signifkant tiefer als Total | | *Kleine Basis <50

Aus Sicht der KMU…
29% der befragten KMU werden beim Thema Cybersicherheit durch einen externen IT-DL unterstützt (siehe S. 18).

Cybersicherheit in Beratungs-/Verkaufsgesprächen

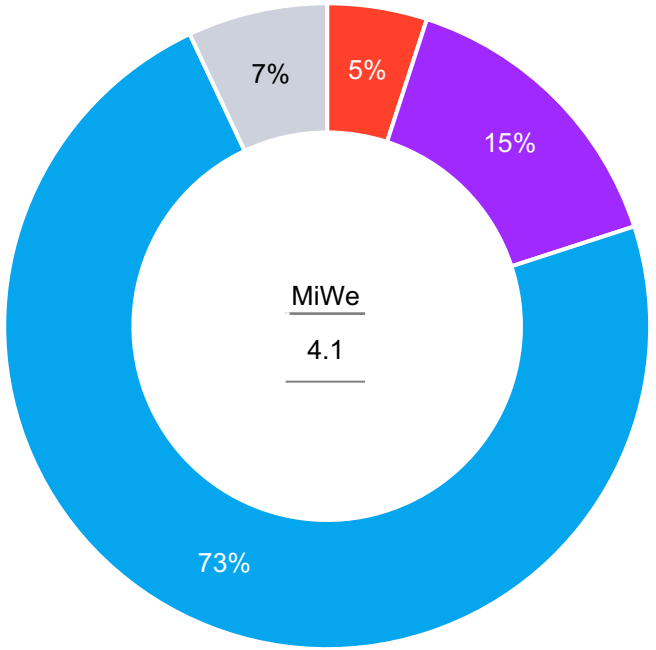
Mehr als die Hälfte der befragten IT-Unternehmen bearbeiten das Thema Cybersicherheit (sehr) aktiv in ihren Beratungs-/Verkaufsgesprächen, rund ein Viertel hingegen (gar) nicht.



F058: Wie aktiv bearbeiten Sie das Thema Cybersicherheit in Beratungs-/Verkaufsgesprächen?
Basis: n=401 | Filter: IT-Dienstleister | Skalierte Frage: 1= gar nicht bis 5= sehr aktiv

Geplante Verbesserung Sicherheitsmassnahmen

Fast drei Viertel der befragten IT-Unternehmen gehen davon aus, dass ihre Kunden in den kommenden 1 bis 3 Jahren ihre Sicherheitsmassnahmen gegen Cyber-Kriminalität erhöhen werden.



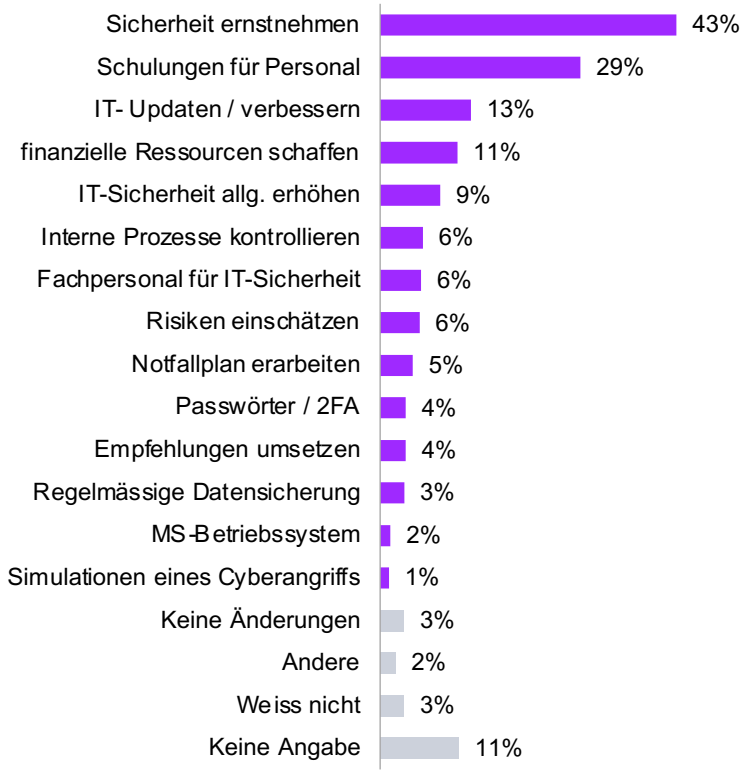
F056. Gehen Sie davon aus, dass Ihre Kunden in den kommenden 1-3 Jahren ihre Sicherheitsmassnahmen gegen Cyber-Kriminalität erhöhen werden?
Basis: n=401 | Filter: IT-Dienstleister | Skalierte Fragen (siehe oben)

Aus Sicht der KMU…
48% der befragten KMU planen, in den nächsten 1-3 Jahren ihre Cyber-Sicherheitsmassnahmen zu erhöhen (siehe S. 40).

Empfehlungen für höhere Cybersicherheit

IT-Dienstleister empfehlen ihren Kunden vor allem, Cybersicherheit ernster zu nehmen (43%). An zweiter Stelle, mit deutlichem Abstand, folgt mit Personalschulungen (29%) eine wichtige organisatorische Massnahme, und an dritter Stelle, nochmals mit deutlichem Abstand, das Updaten der IT als wichtige technische Massnahme (13%).

Verbesserungspotential



F059: Was müssten Ihre Kunden bezüglich Cybersicherheit besser machen?
Basis: n=401 | Filter: IT-Dienstleister | Offene Frage

Massnahmen bzw. Schutz wird nicht allumfassend umgesetzt bzw. es bestehen meist gute Bestrebungen und auch aktive Massnahmen, aber gleichzeitig an manchen Stellen grosse und bekannte Lücken, welche auch durchaus ignoriert werden. Insbesondere das Risiko Mensch (Mitarbeitende) wird zu wenig adressiert und neue Risiken wie Voice-Phising (Vishing).

Die Abhängigkeit von externen Dienstleistern und die Überführung vieler Applikationen in die Cloud erhöht m.A. das Risiko stark. Durch das fehlende Wissen und die Kompetenz in Sachen Cyberrisiko, Cyberabwehr schwindet die Resilienz stark. Unsere Kunden verlassen sich u.E. zu stark auf die grossen DL wie Microsoft, Amazon, Google und andere Cloudanbieter - das macht anfällig auf "Erpressbarkeit" in Sachen Service, Preis. Die Einflussnahme ist dann eingeschränkt.

Sich besser und genauer informieren und dies nicht aus Unwissenheit oder Angst vor Kosten hinausschieben, bzw. denken, sie wären nie betroffen sein davon.

Sich dafür interessieren und das Thema als geschäftsrelevant erkennen. Diese Einsicht ist an vielen Orten noch nicht vorhanden.

Ganzheitliche Sichtweise, nicht nur technische Lösungen, auch organisatorische Massnahmen

Das Erhalten einer permanenten Cybersicherheitskultur nach deren Einführung wird innerhalb der Firmen oft vernachlässigt. Dabei wird die lange Liste von Schutzmassnahmen und Verhaltensweisen nicht regelmässig kontrolliert und auf dem neusten Stand gehalten.

- Sich weniger auf das Prinzip Hoffnung verlassen.
- Personal schulen (Organisatorische Massnahmen)

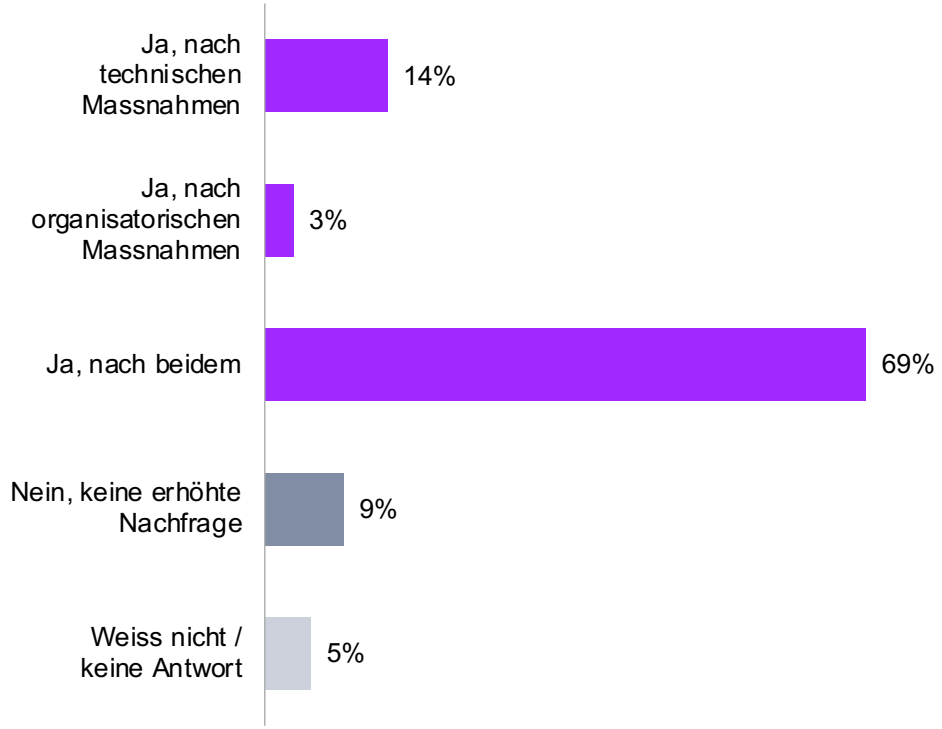
Côté informatique : investir plus dans la cybersécurité et notamment les pentest

Coté organisationnel : Mieux considérer la protection des données et le rôle des DPO. Ce nouveau métier et ses atouts sont délaissés en Suisse en comparaison de nos voisins européens

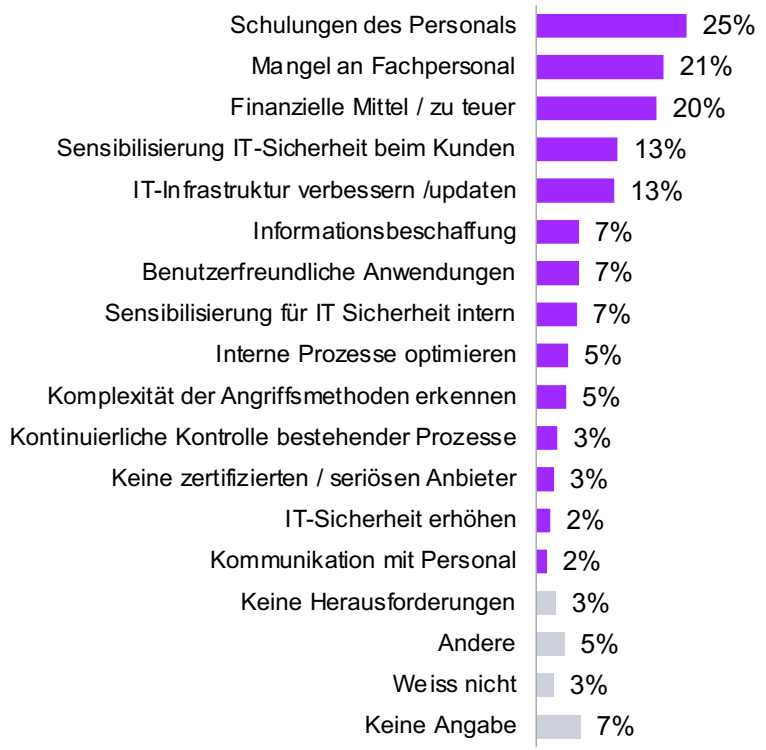
Cybersicherheits-Nachfrage in Zukunft

Fast 9 von 10 befragten IT-Unternehmen erwarten eine höhere Nachfrage nach Sicherheitsmassnahmen. Die grössten Herausforderungen für ihre Branche, um dieser Nachfrage nachzukommen, sind aus ihrer Sicht Personalschulungen bzw. der Mangel an Fachpersonal sowie die erforderlichen finanziellen Mittel.

Erhöhung der Nachfrage
Basis: n=401 | Filter: IT-Dienstleister



Herausforderungen für die Branche
Basis: n=344 | Filter: IT-Dienstleister – erhöhte Nachfrage erwartet



Aus Sicht der KMU…
48% der befragten KMU möchten in den kommenden 1-3 Jahren ihre Cybersicherheits-Massnahmen erhöhen (siehe Folie 40).

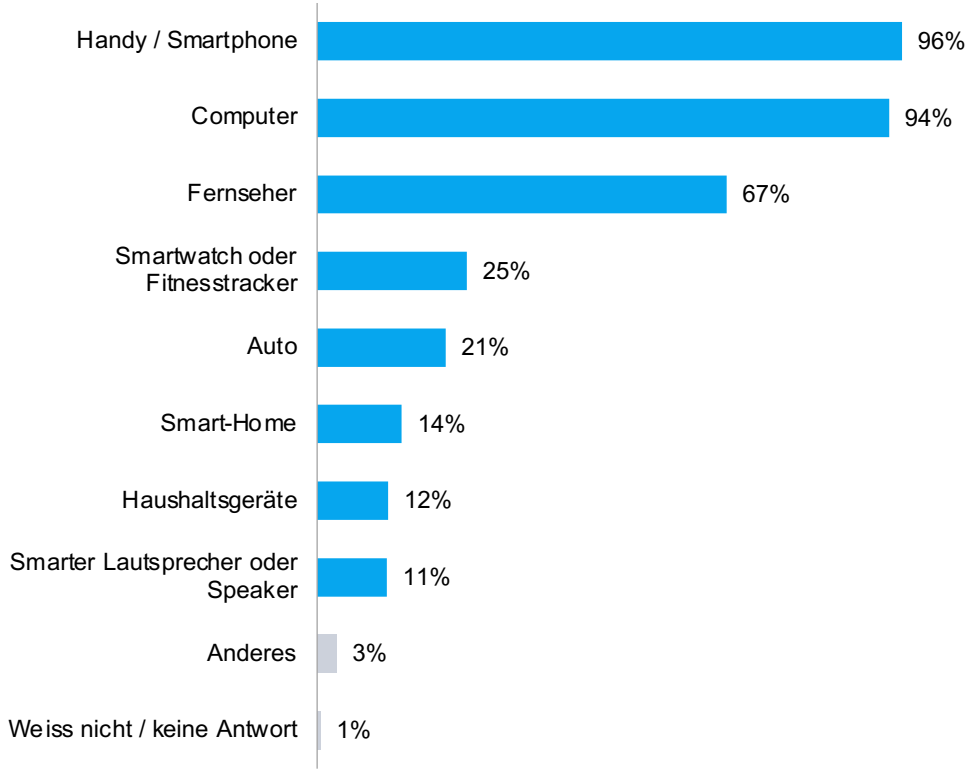
F060: Erwarten Sie in naher Zukunft eine erhöhte Nachfrage durch KMU nach Cybersicherheit? | F061: Was sind die Herausforderungen für Ihre Branche, um dieser erhöhten Nachfrage nachzukommen?
Basis: n=[ ] | Filter: siehe oben | Geschlossene Frage (F060) & offene Frage (F061)

05 Bevölkerung

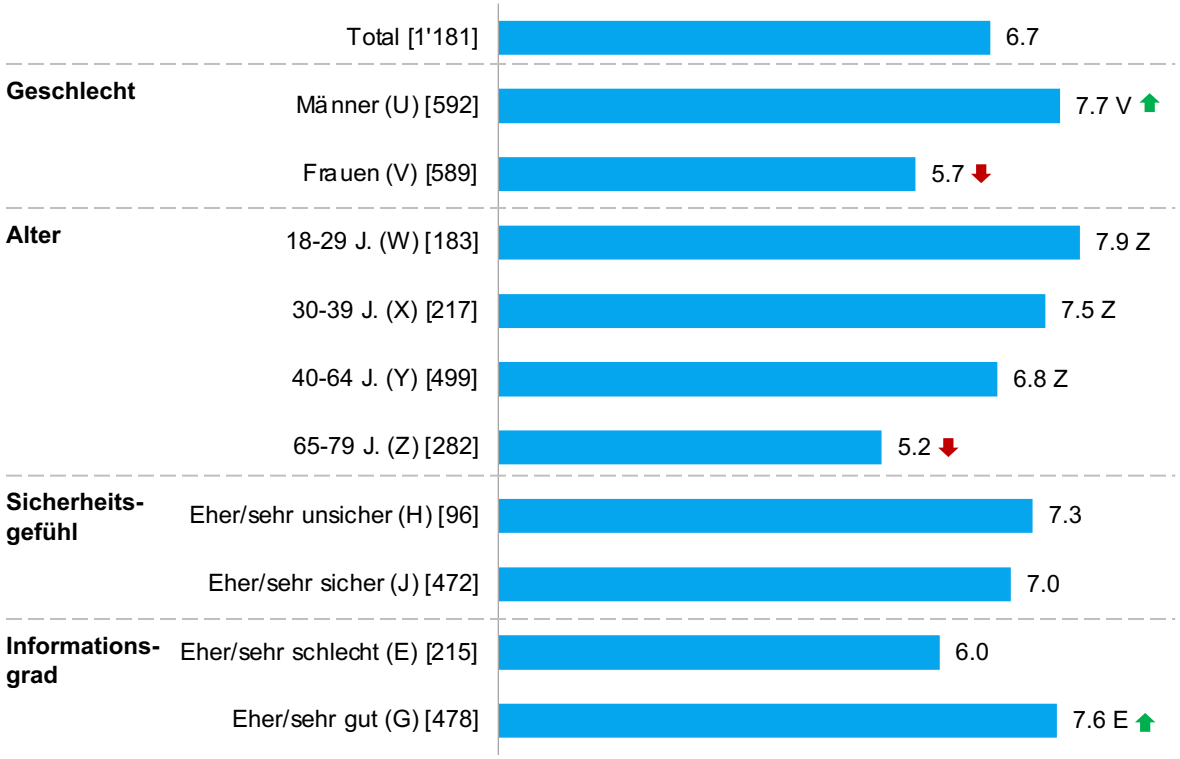
Anzahl Onlinegeräte

Fast alle Befragten verfügen über ein Smartphone und/oder einen Computer, rund zwei Drittel über einen mit dem Internet verbundenen Fernseher. Durchschnittlich verfügen die Befragten über 6.7 mit dem Internet verbundene Geräte, wobei Männer und jüngere Befragte signifikant mehr Geräte haben als Frauen und ältere Befragte.

Art der Onlinegeräte [1‘247]



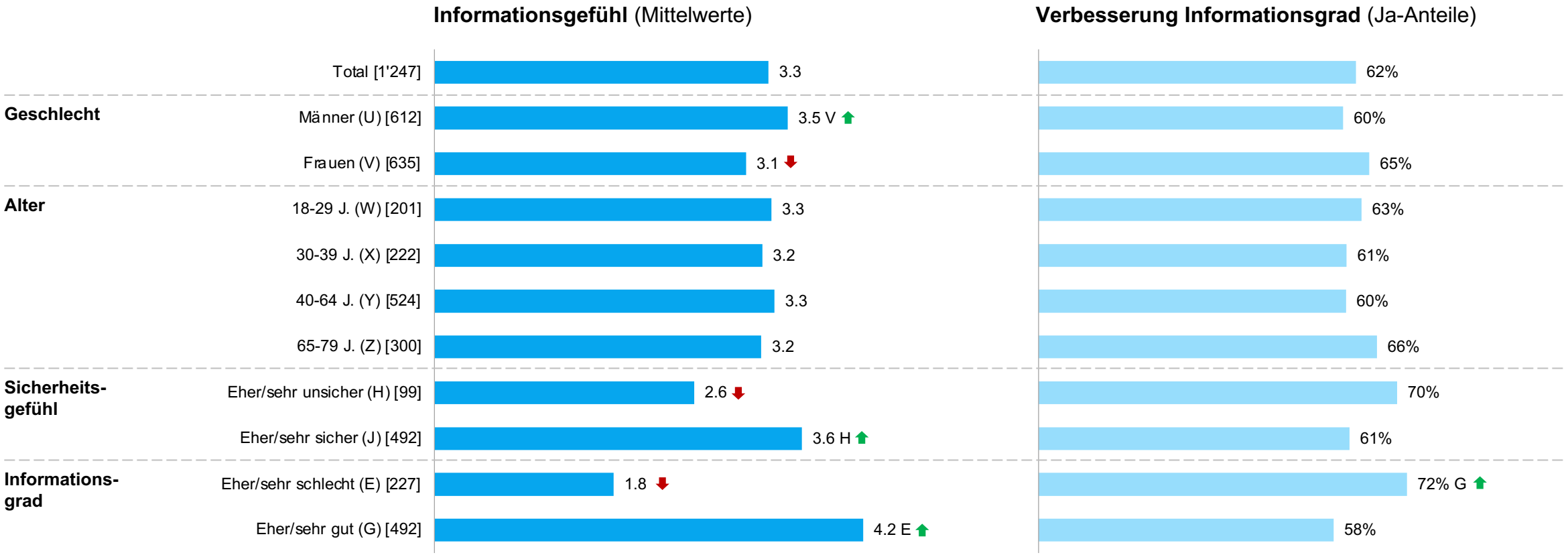
Anzahl Onlinegeräte (Mittelwert)



F101: Welche Geräte besitzen Sie, die mit dem Internet verbunden sind? | F102: Was schätzen Sie: Wie viele Geräte besitzen Sie zuhause, die mit dem Internet verbunden sind?
Basis: n=[ ] | Filter: Bevölkerung | Geschlossene Frage (F101) & Zahlenfeld (F102) | ⬆ signifikant höher als Total; ⬇ signifkant tiefer als Total
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Informationsgrad

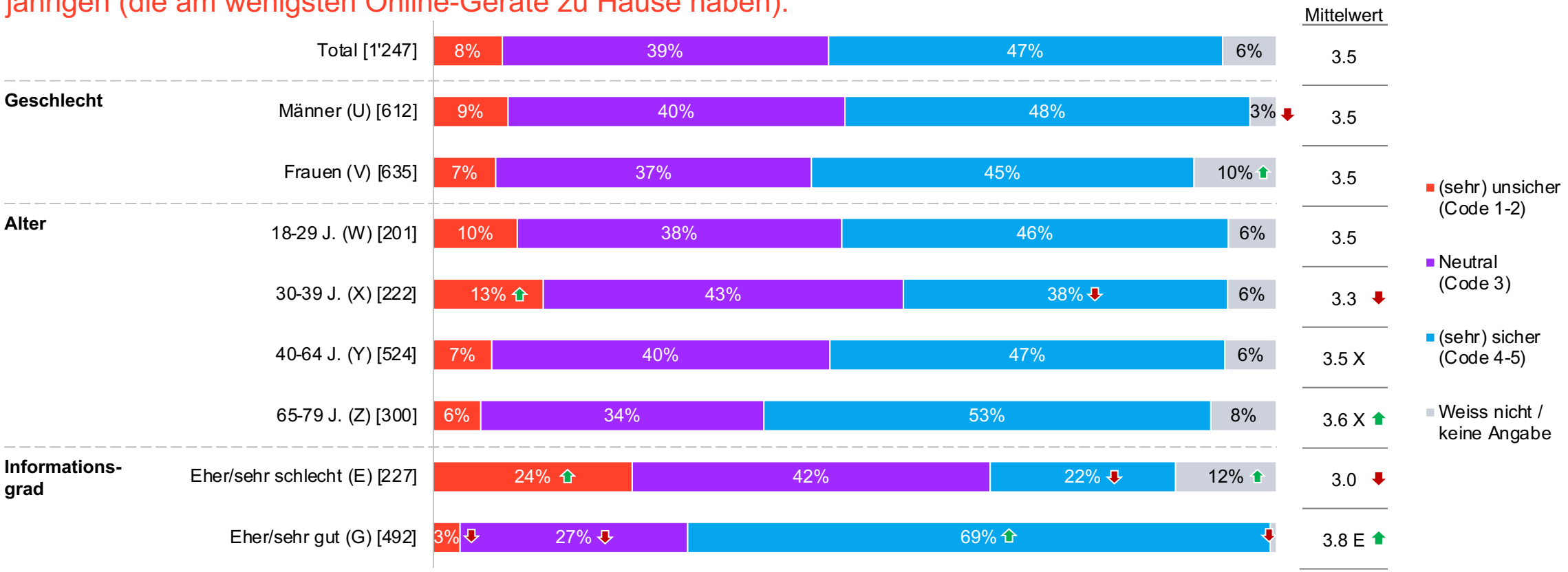
Die Befragten sind mehrheitlich der Meinung, eher bis sehr gut Bescheid zu wissen, wie sie sich vor Cyberangriffen schützen können. Auf der 5er-Skala schätzen sie ihren Informationsgrad durchschnittlich auf 3.3. Fast zwei Drittel wären gerne besser informiert, besonders diejenigen, die ihren Informationsgrad tief einschätzen.



F009: Wie gut wissen Sie im Vergleich zu ihren Kolleginnen und Kollegen Bescheid, wie Sie sich vor Cyberangriffen schützen können? | F010: Wären Sie gerne besser informiert über das Thema Cybersicherheit?
Basis: n=[ ] | Filter: Bevölkerung | Skalierte Frage: 1= sehr schlecht bis 5= sehr gut (F009) & geschlossene Frage (F010) | ⬆ signifikant höher als Total; ⬇ signifkant tiefer als Total
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Sicherheitsgefühl bezüglich Cybergefahren

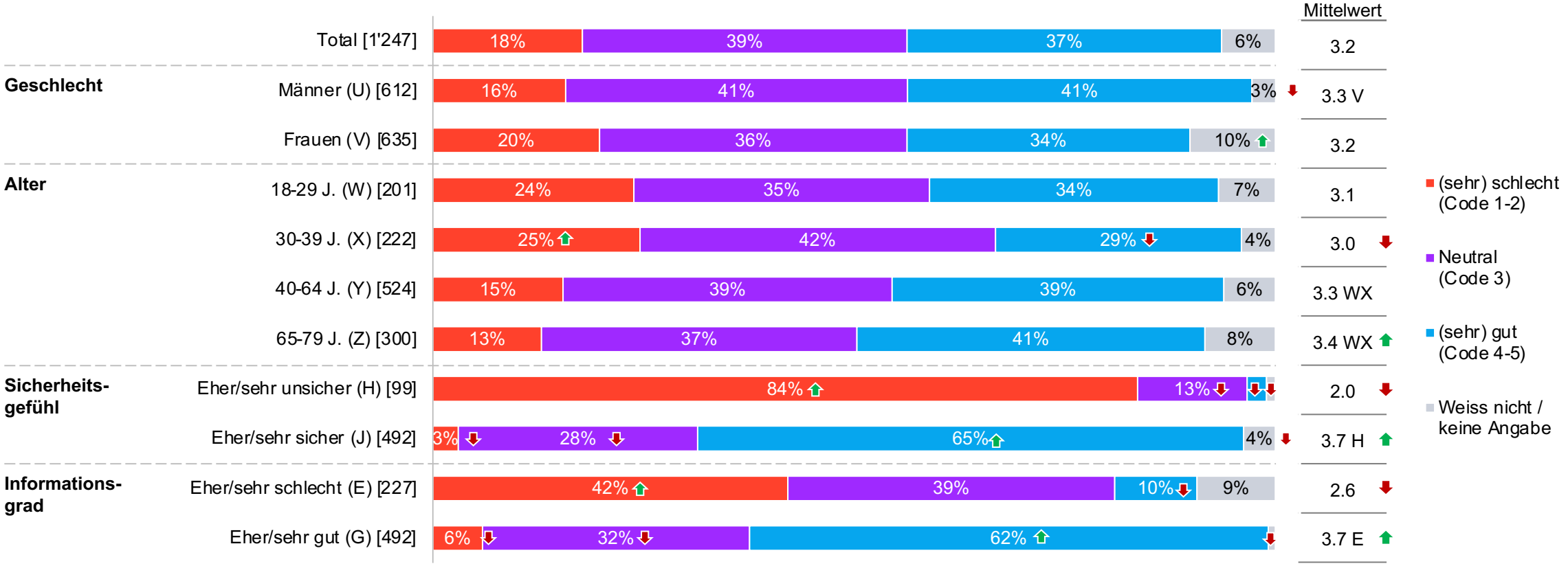
Fast die Hälfte der Befragten beurteilt die Cybersicherheit des eigenen Haushalts als (sehr) sicher. (Eher) schlecht Informierte bezüglich Cybersicherheit empfinden ihren Haushalt als signifikant unsicherer als (eher) gut Informierte. Auffallend ist die hohe Unsicherheit der 30- bis 39-Jährigen, besonders im Vergleich zu den besonders sicheren über 65-jährigen (die am wenigsten Online-Geräte zu Hause haben).



F007: Wie bewerten Sie die Cybersicherheit Ihres Haushalts?
Basis: n=[ ] | Filter: Bevölkerung | Skalierte Frage: 1= sehr unsicher bis 5= sehr sicher | ▲ signifikant höher als Total; ▼ signifkant tiefer als Total | Datenbeschriftung ab 3%
Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Resilienz

Etwas tiefer als das Sicherheitsgefühl liegt das Gefühl, gut geschützt und auf einen Angriff vorbereitet zu sein. Fast ein Drittel (31%) derjenigen, die sich (sehr) sicher fühlen, tun dies, ohne sich gleichzeitig auch (sehr) gut geschützt zu fühlen. Evt. ist das so, weil sie nur wenige Onlinegeräte besitzen oder von einem kleinen Angriffsrisiko ausgehen.

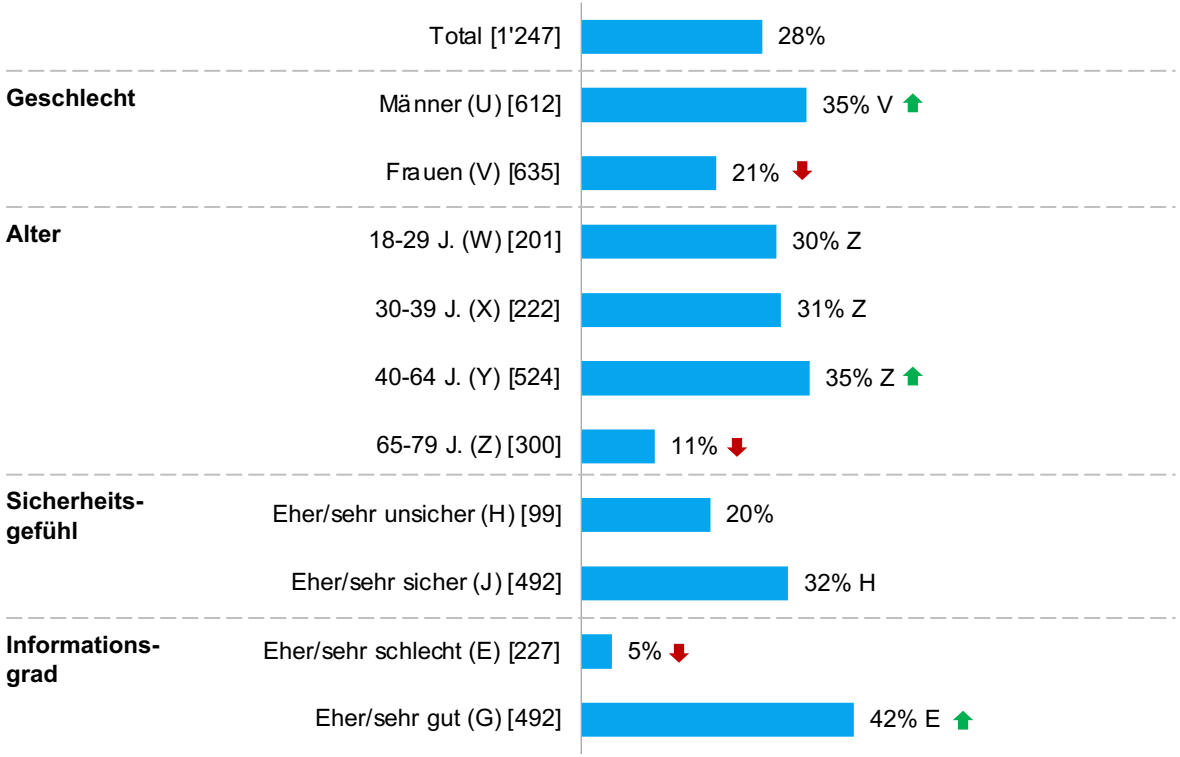


F008: Was schätzen Sie: Wie gut sind Sie vor Cyberangriffen geschützt und auf einen Angriff vorbereitet?
Basis: n=[ ] | Filter: Bevölkerung | Skalierte Frage: 1= sehr schlecht bis 5= sehr gut | ▲ signifikant höher als Total; ▼ signifkant tiefer als Total | Datenbeschriftung ab 3%
Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

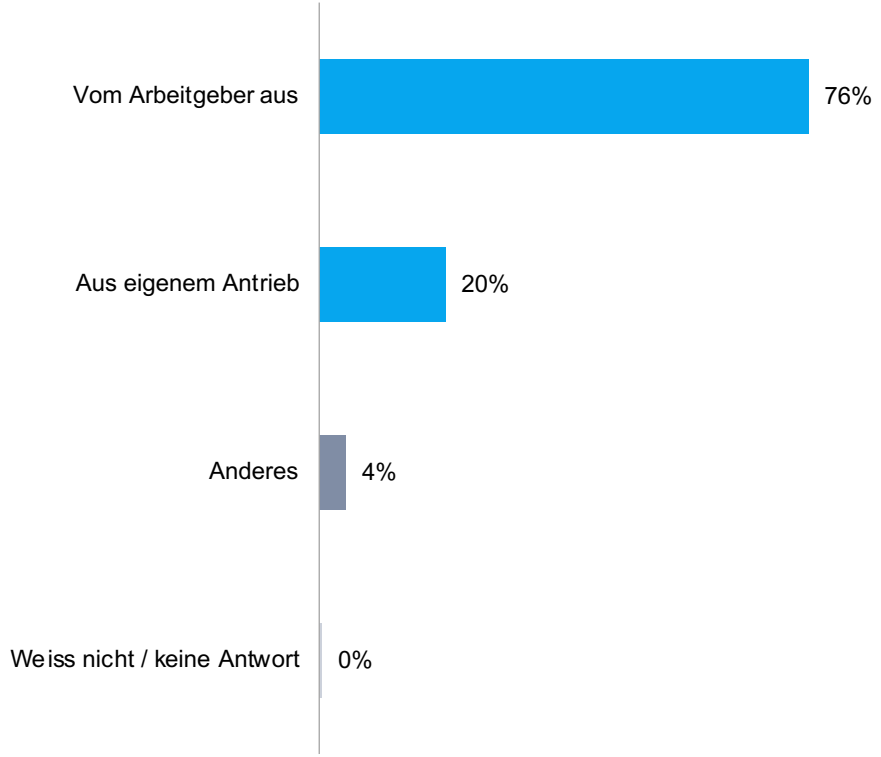
Schulung

Rund ein Viertel der Befragten hat schon Cybersicherheits-Schulung(en) besucht; dabei handelt es sich eher um Männer (35%) als um Frauen (21%) und nur selten um über 65-Jährige (11%); rund drei Viertel der Schulungen wurden denn auch von Arbeitgebern initiiert. Sicherheits- und Informationsgefühl stehen in einem positiven Zusammenhang mit Schulungen.

Schulung besucht (Ja-Anteile)
Filter: Bevölkerung



Motivation für Schulung
Basis: 338 | Filter: Bevölkerung – Schulung besucht

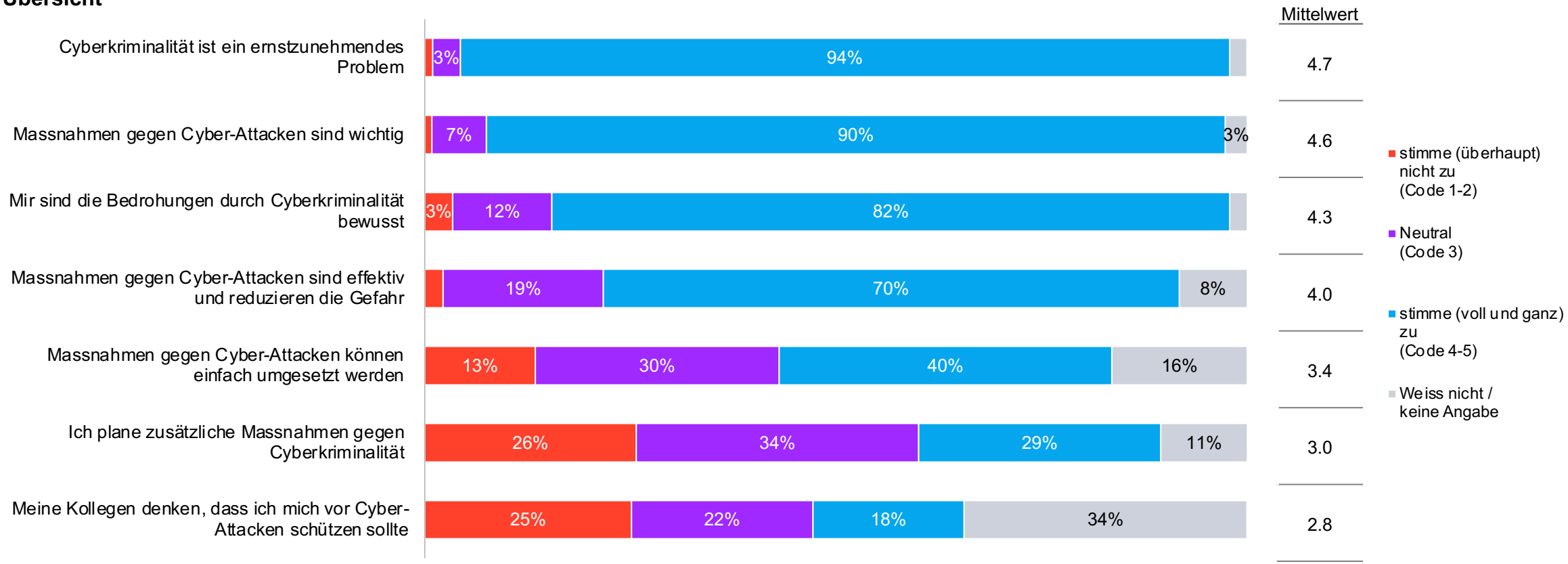


F106: Haben Sie schon einmal eine Schulung zum Thema Cybersicherheit besucht? | F107: Haben Sie diese Schulung aus eigenem Antrieb heraus besucht oder mussten Sie sie von Ihrem Arbeitgeber aus besuchen, oder trifft etwas anderes zu?
Basis: n=[ ] | Filter: siehe oben | Geschlossene Fragen | ⬆ signifikant höher als Total; ⬇ signifkant tiefer als Total
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Einstellung zu Cyberkriminalität (1/2)

Fast alle Befragten sind sich einig, dass Cyberkriminalität ein ernstzunehmendes Problem ist und Massnahmen dagegen wichtig sind. Dass die Massnahmen einfach umsetzbar sind, finden nur zwei Fünftel, und weniger als ein Drittel plant zusätzliche Massnahmen. Knapp ein Fünftel findet, dass Kollegen denken, sie müssten sich vor Cyberattacken schützen.

Übersicht

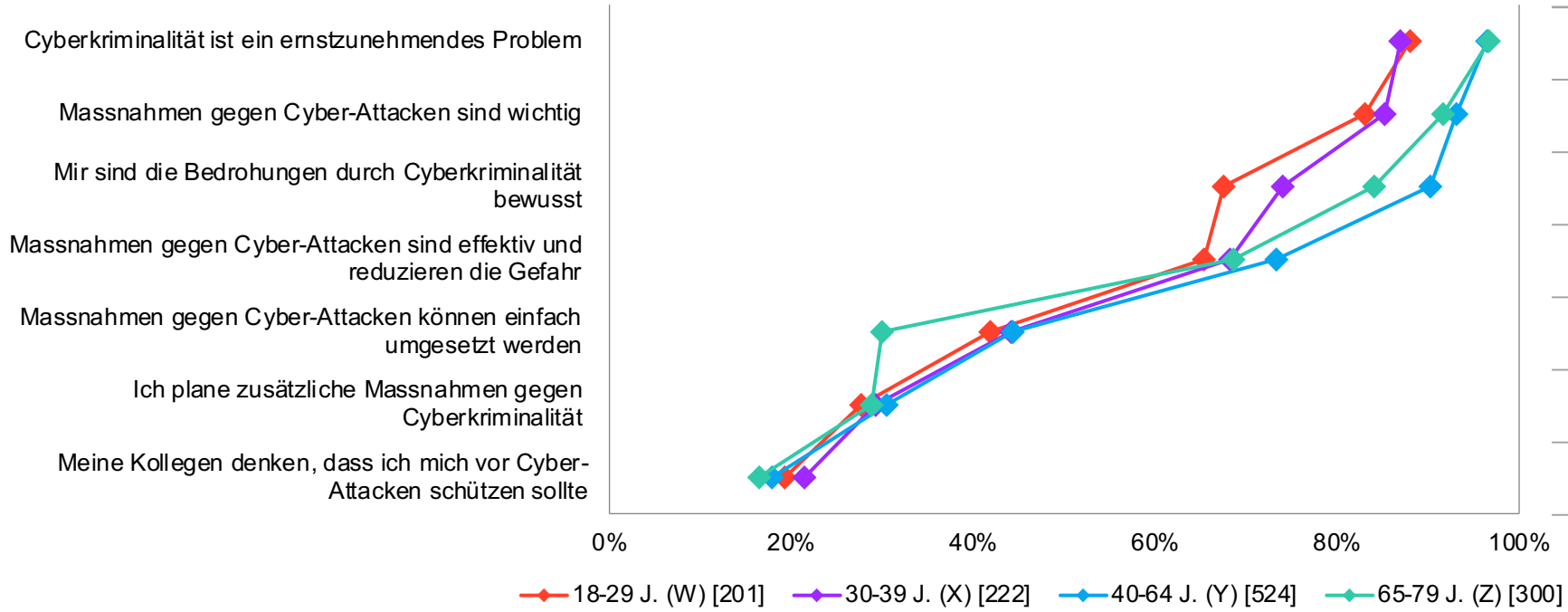


F015: Inwiefern stimmen Sie den folgenden Aussagen zu Cyberkriminalität wie Malware, Online-Betrug und Hacking zu?
Basis: n=1‘247 | Filter: Bevölkerung | Skalierte Frage: 1= überhaupt nicht bis 5= voll und ganz | Datenbeschriftung ab 3%

Einstellung zu Cyberkriminalität (2/2)

Auch die unter 40-Jährigen beurteilen Cyberkriminalität als ernstzunehmend, Massnahmen dagegen wichtig und sie sind sich der Bedrohungen bewusst; die Mittelwerte ihrer Beurteilungen liegen aber signifikant tiefer als diejenigen der über 40-Jährigen. Es gibt also, wenn auch auf hohem Niveau, einen gewissen Altersgraben.

Nach Alter



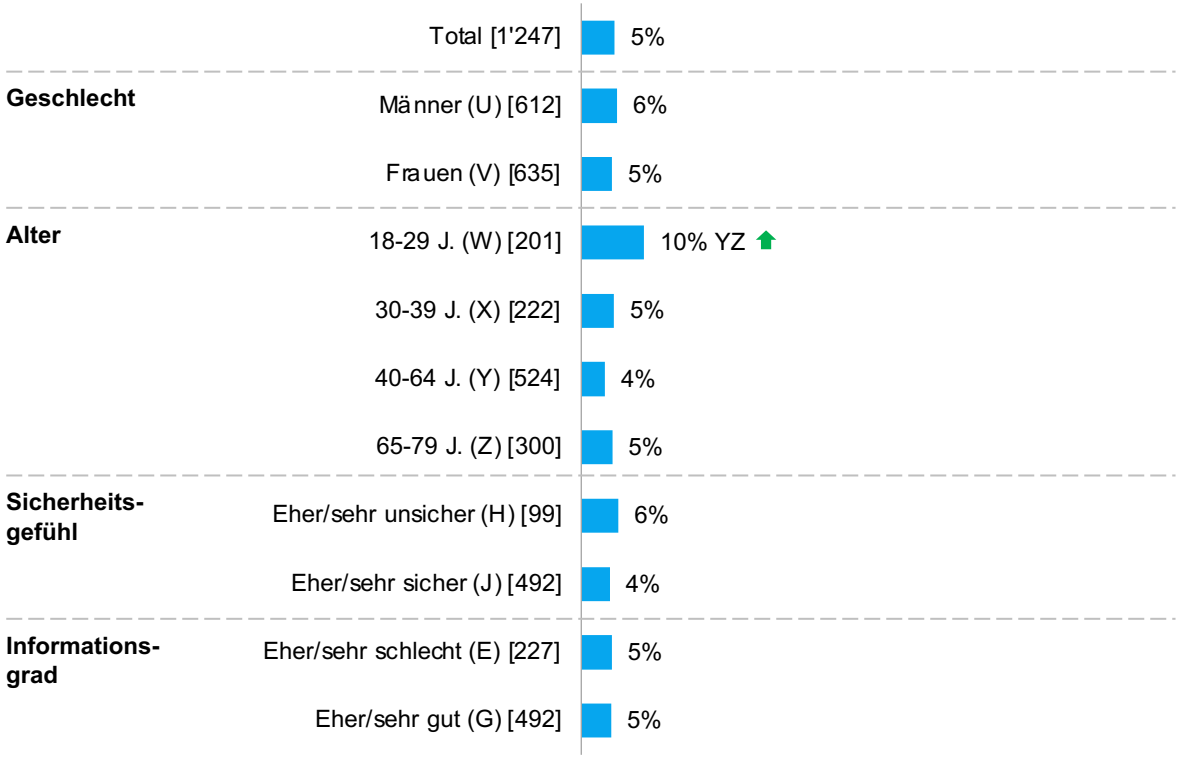
	Mittelwert			
	18-29 Jahre	30-39 Jahre	40-64 Jahre	65-79 Jahre
Cyberkriminalität ist ein ernstzunehmendes Problem	4.4	4.5	4.8 WX	4.8 WX
Massnahmen gegen Cyber-Attacken sind wichtig	4.2	4.4 W	4.7 WX	4.7 WX
Mir sind die Bedrohungen durch Cyberkriminalität bewusst	3.9	4.0	4.4 WX	4.4 WX
Massnahmen gegen Cyber-Attacken sind effektiv und reduzieren die Gefahr	3.9	4.0	4.1 W	4.1 W
Massnahmen gegen Cyber-Attacken können einfach umgesetzt werden	3.5 Z	3.5 Z	3.4 Z	3.2
Ich plane zusätzliche Massnahmen gegen Cyberkriminalität	3.0	3.0	3.1	3.0
Meine Kollegen denken, dass ich mich vor Cyber-Attacken schützen sollte	2.8	2.8	2.8	3.0

F015: Inwiefern stimmen Sie den folgenden Aussagen zu Cyberkriminalität wie Malware, Online-Betrug und Hacking zu?
Basis: n=[ ] | Filter: Bevölkerung | Skalierte Frage: 1= überhaupt nicht bis 5= voll und ganz | Top2 und Mittelwerte ausgewiesen
signifikant höher als Total; signifikant tiefer als Total | Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

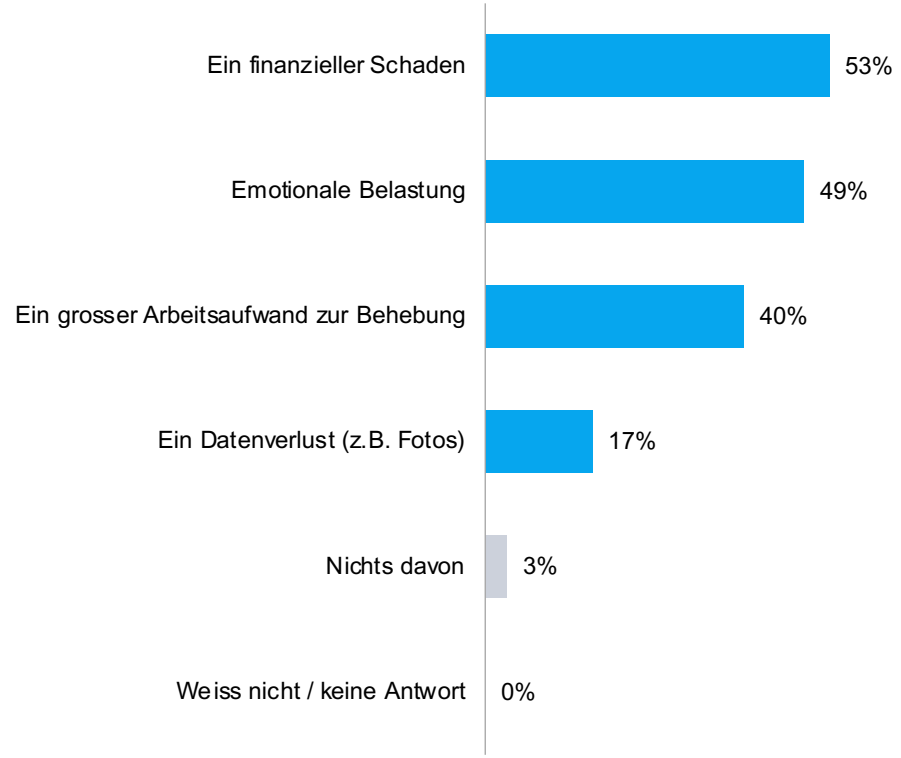
Erfahrung Cyberkriminalität

Jede/-r zwanzigste Befragte hat in den letzten 3 Jahren einen Cyberangriff erlebt; in rund der Hälfte der Fälle entstand dadurch ein finanzieller Schaden und emotionale Belastung, zwei Fünftel der Betroffenen nennen hohen Arbeitsaufwand und rund jede/-r sechste erlitt einen Datenverlust. 18- bis 29-jährige sind rund doppelt so häufig betroffen wie ältere.

Erlittene Angriffe (Ja-Anteile)
Filter: Bevölkerung



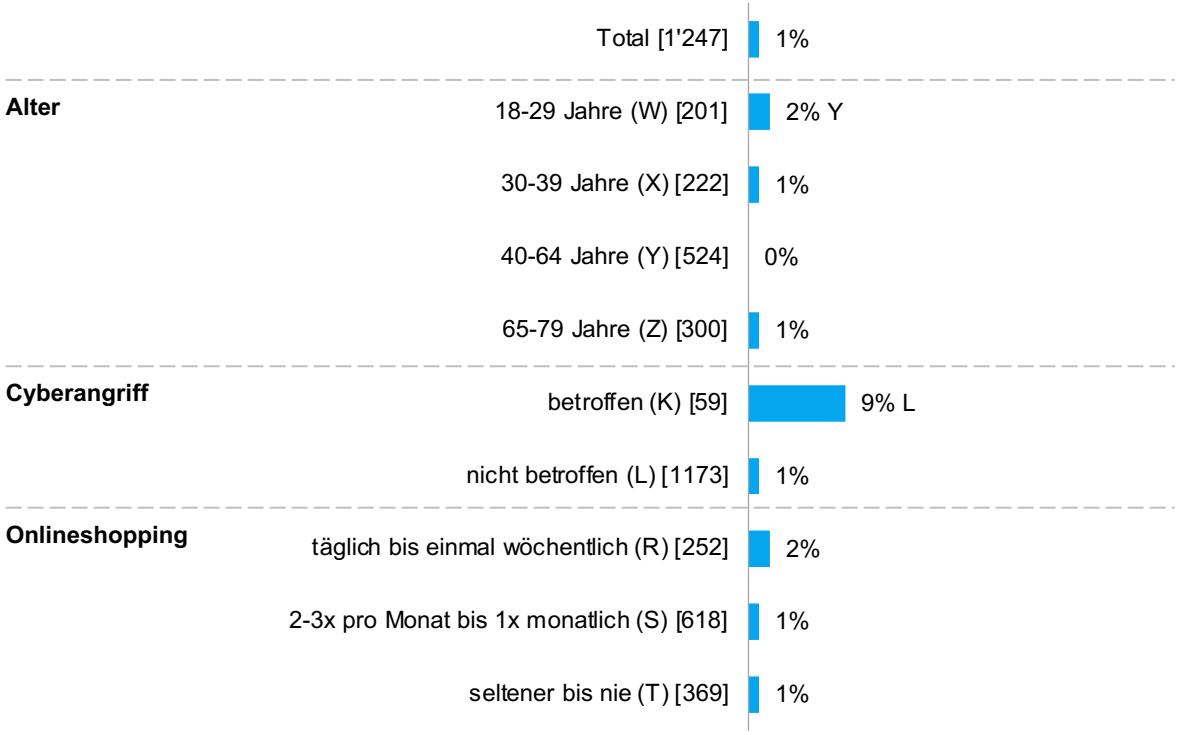
Erlittene Schäden
Basis: 59 | Filter: Bevölkerung – wenn Cyberangriff erlitten



F016: Haben Sie als Privatperson innerhalb der letzten 3 Jahre durch einen Cyberangriff einen finanziellen Schaden erlitten, viel Mühe für die Schadensbereinigung gehabt oder emotional gelitten? | F017: Entstand durch diesen Angriff…
Basis: n=[ ] | Filter: siehe oben | Geschlossene Fragen | ▲ signifikant höher als Total; ▼ signifkant tiefer als Total
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Lösegeld an Cyberkriminelle

Einer von hundert Befragten hat schon einmal Lösegeld an Cyberkriminelle bezahlt; bei der jüngsten Befragungsgruppe sind es zwei von hundert. Fast jede/-r zehnte Befragte, der/die von einem Cyberangriff betroffenen war, zahlte schon Lösegeld.



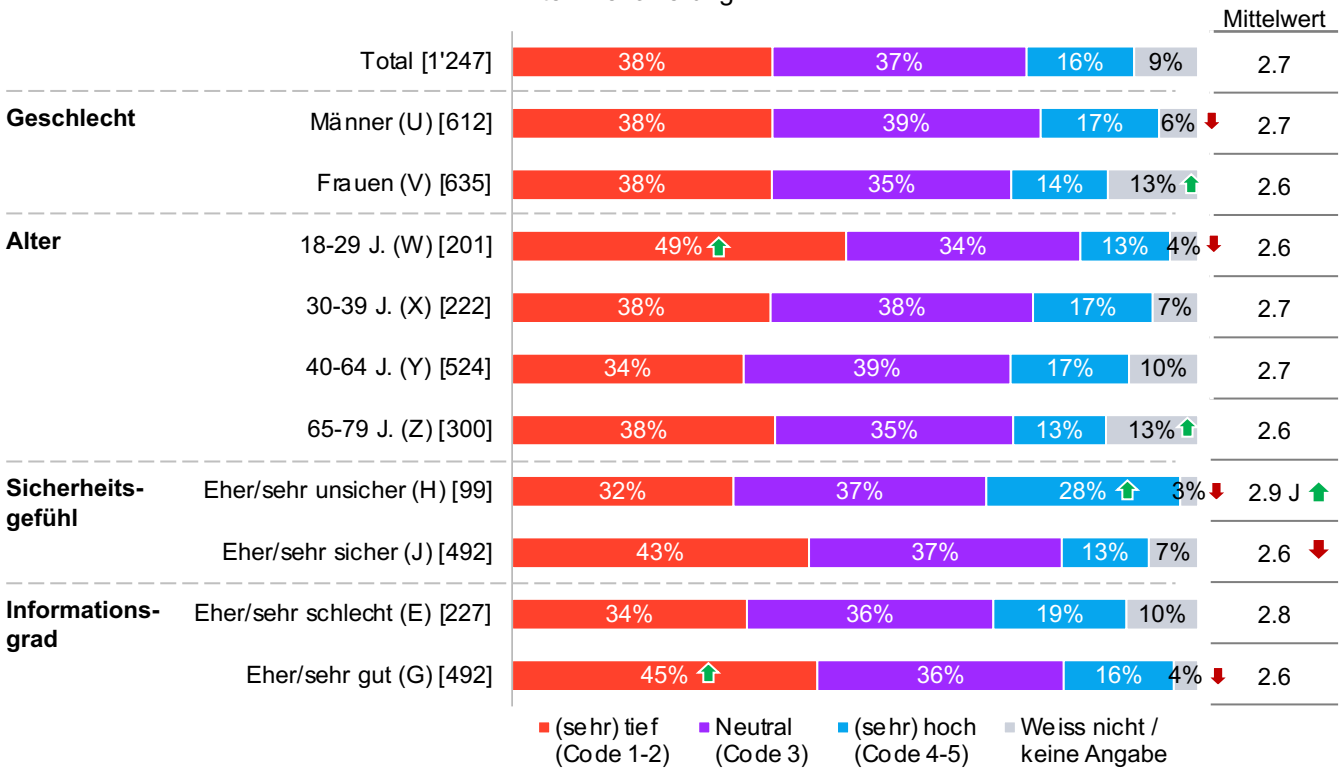
F020: Haben Sie schon einmal Lösegeld an Cyberkriminelle bezahlt?
Basis: n=[] | Filter: Bevölkerung | Geschlossene Frage
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen

Risiko eines Angriffs

Rund jede/-r sechste Befragte (16%) schätzt das Risiko, innerhalb 2-3 Jahren durch einen Cyberangriff Geld oder Daten zu verlieren, als (sehr) hoch ein, knapp zwei Fünftel (38%) als (sehr) klein. 18- bis 29-jährige taxieren das Risiko häufiger als (sehr) klein als die älteren Befragten. Hauptgrund für eine tiefe Risikoeinschätzung ist vorsichtiges Verhalten (42%).

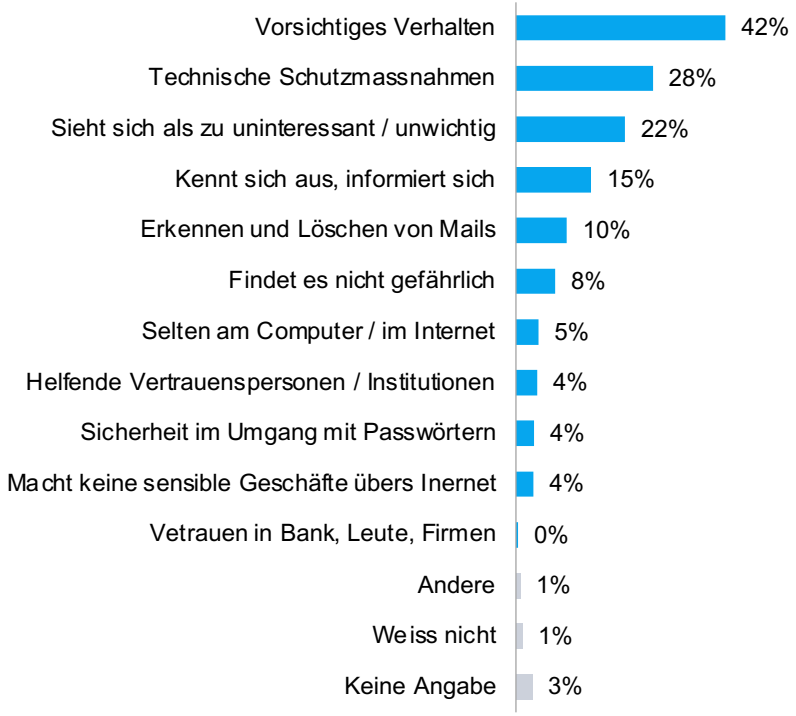
Einschätzung

Filter: Bevölkerung



Begründung

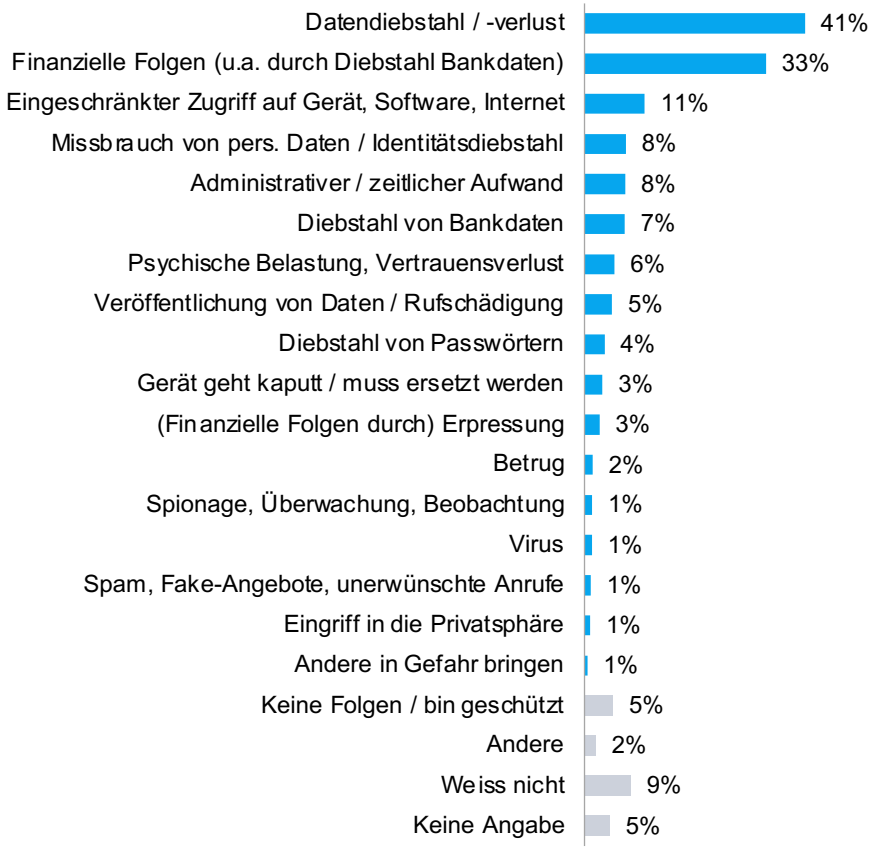
Basis: 459 | Filter: Bevölkerung, die das Risiko eher tief einschätzen



F021: Wie hoch schätzen Sie das Risiko ein, innerhalb der nächsten 2-3 Jahre durch einen Cyberangriff Geld oder Daten zu verlieren? | F113: Was sind die Gründe dafür, dass Sie dieses Risiko eher tief einschätzen?
Basis: n=[ ] | Filter: siehe oben | Skalierte Frage: 1= sehr kleines Risiko bis 5= sehr grosses Risiko (F021) & offene Frage (F113) | ⬆ signifikant höher als Total; ⬇ signifkant tiefer als Total
Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Nachteile eines Angriffs

Die Befragten fürchten in erster Linie den Diebstahl bzw. Verlust von Daten (41%) und finanzielle Folgen (33%). Ältere Befragte (65-79 Jahre) und solche, die sich (sehr) schlecht informiert fühlen und/oder noch nie eine Schulung besuchten, können diese Frage schlechter beantworten (höherer Anteil weiss nicht/keine Antwort).



Il materiale scolastico con dati senisibili e la perdita di documenti a me cari e/o importanti.

Perte de mes connections sécurisée...impossibilité d'utiliser internet

Diffusion (vente) de données personnelles

Finanzielles und emotionales Desaster

Finanzielle. Datenverlust. Ausspionieren. Überwachung.

Zugriff auf Bankkonto, Internetkäufe über meine Karten oder Paypal Konto.

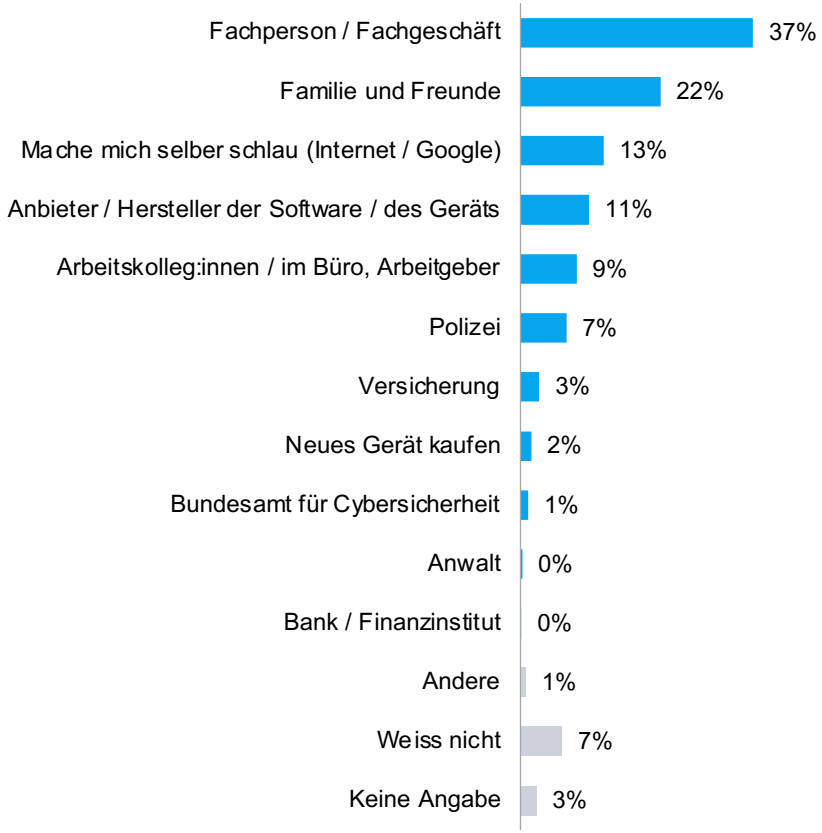
Datenverlust, Geldverlust, Umtriebe

Non possiedo nulla e sono una cittadina tranquilla per cui la condidererei una violazione della privacy ma nessuno si interesserebbe a me per trarre profitto.

F114: Welche Nachteile für Sie persönlich könnten, Ihrer Meinung nach, bei einem Angriff aus dem Internet eintreten?
Basis: n=1‘225 | Filter: Bevölkerung | Offene Frage

Hilfe bei Angriffen

Die Befragten würden sich, wenn ihr Computer aufgrund eines Cyberangriffs nicht mehr funktioniert, am ehesten an Fachpersonen bzw. /-geschäfte wenden (37%), etwas mehr als jede/-r fünfte würde sich bei Familie und Freunden informieren.



In einem Computergeschäft oder wenn jemand aus meinem Bekanntenkreis privat jemanden empfehlen kann, der sich auskennt. Oder meine Versicherung kontaktieren und anfragen.

Via Handy im Internet.

Im Fachhandel oder beim Sohn, der Softwareentwickler ist.

Bin einerseits selbst in der Lage dazu. Allenfalls beim Support der Symantec Internet Security (Norton).

Ich habe einen Freund, der sehr gut in IT ist, also melde ich mich bei ihm.

Ehemann, Vater, Polizei

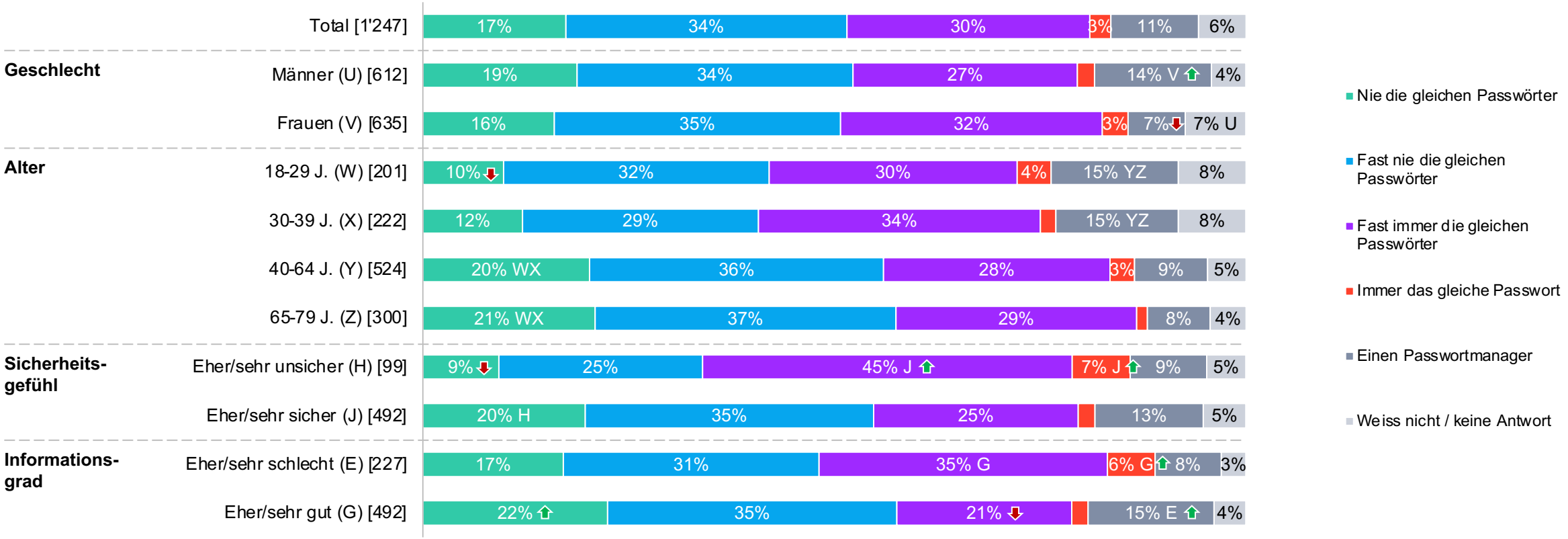
Niemand, ich würde das Problem persönlich durch Nachfragen im Internet und mit meinem Wissen lösen.

Gute Frage! Keine Ahnung! Bei niemandem. Ich versuche, mich zu schützen. Wenn's schief geht, habe ich den Nachteil. Niemand fühlt sich zuständig.

F115: Angenommen Ihr Computer zuhause funktioniert wegen einem Cyberangriff nicht mehr: Wo holen Sie sich Hilfe?
Basis: n=1‘225 | Filter: Bevölkerung | Offene Frage

Umgang mit Passwörtern

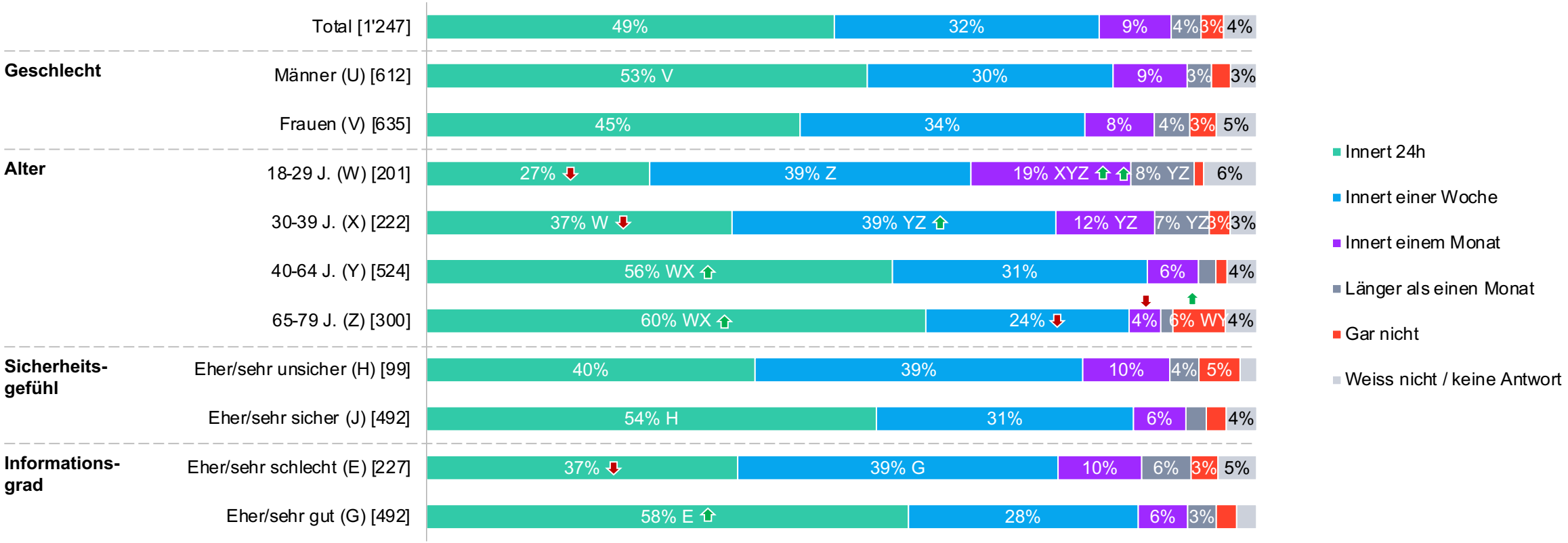
Ein Drittel der Befragten nutzt (fast) immer das gleiche Passwort für mehrere Anwendungen und geht somit das Risiko ein, an mehreren Orten gleichzeitig bestohlen zu werden. Bei den (sehr) unsicheren Befragten und den (sehr) schlecht informierten Befragten ist der Anteil signifikant höher. Passwortmanager werden von rund jeder/jedem zehnten Befragten verwendet, häufiger jedoch von den unter 40-jährigen (15%).



F022: Benutzen Sie an verschiedenen solchen Orten das gleiche Passwort mehrfach? Ich benutze…
Basis: n=[ ] | Filter: Bevölkerung | Geschlossene Frage | ⬆ signifikant höher als Total; ⬇ signifkant tiefer als Total | Datenbeschriftung ab 3%
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Umgang mit Updates

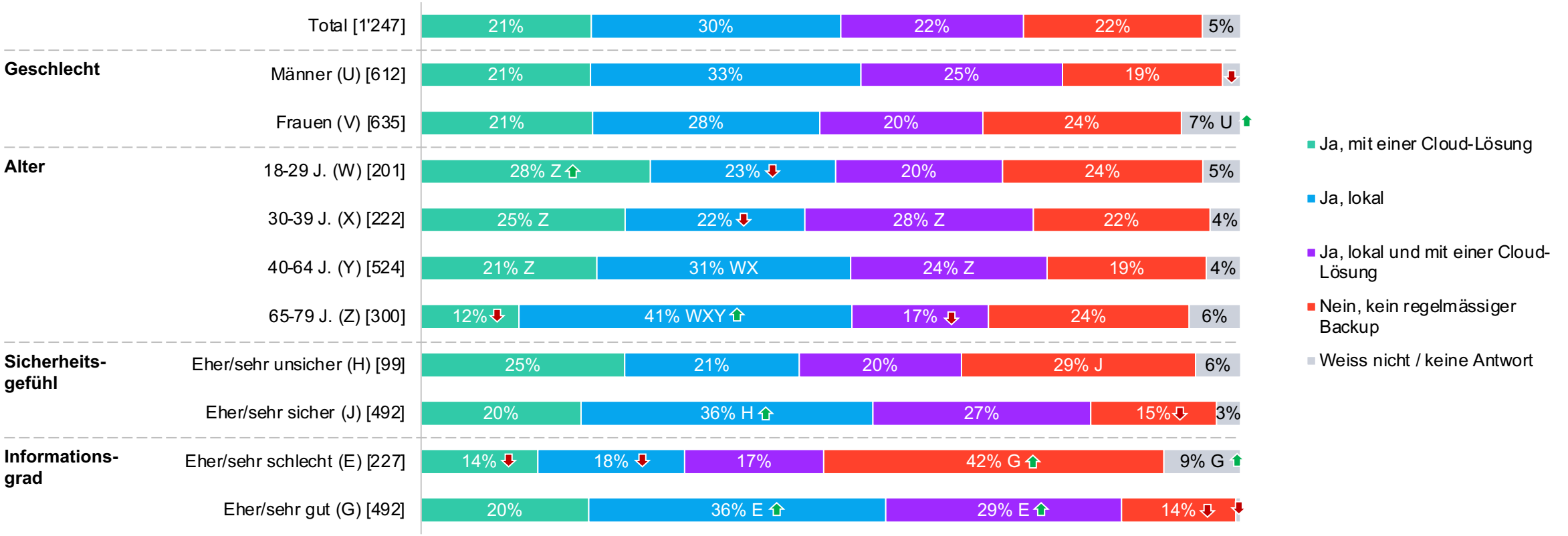
Fast die Hälfte der Befragten führt Software-Updates innerhalb von 24 Stunden durch, ein weiterer knapper Drittel immerhin innert einer Woche. Die 18- bis 29-jährigen lassen sich am meisten Zeit für die Updates, bei den über 65-jährigen hingegen ist der Anteil derjenigen am höchsten, welche die Updates gar nicht durchführen (6%).



F117: Wenn Ihr Computer oder Ihr Handy Sie auffordert, ein Software-Update durchzuführen, tun Sie das:
Basis: n=[ ] | Filter: Bevölkerung | Geschlossene Frage | ⬆ signifikant höher als Total; ⬇ signifkant tiefer als Total | Datenbeschriftung ab 3%
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Backup mit/ohne Cloud

Rund drei Viertel der Befragten führen regelmässig lokal und/oder mit einer Cloud-Lösung Backups durch, rund ein Viertel macht keine regelmässigen Backups oder kann die Frage nicht beantworten. (Sehr) unsichere und (sehr) schlecht informierte Befragte führen seltener Backups durch.

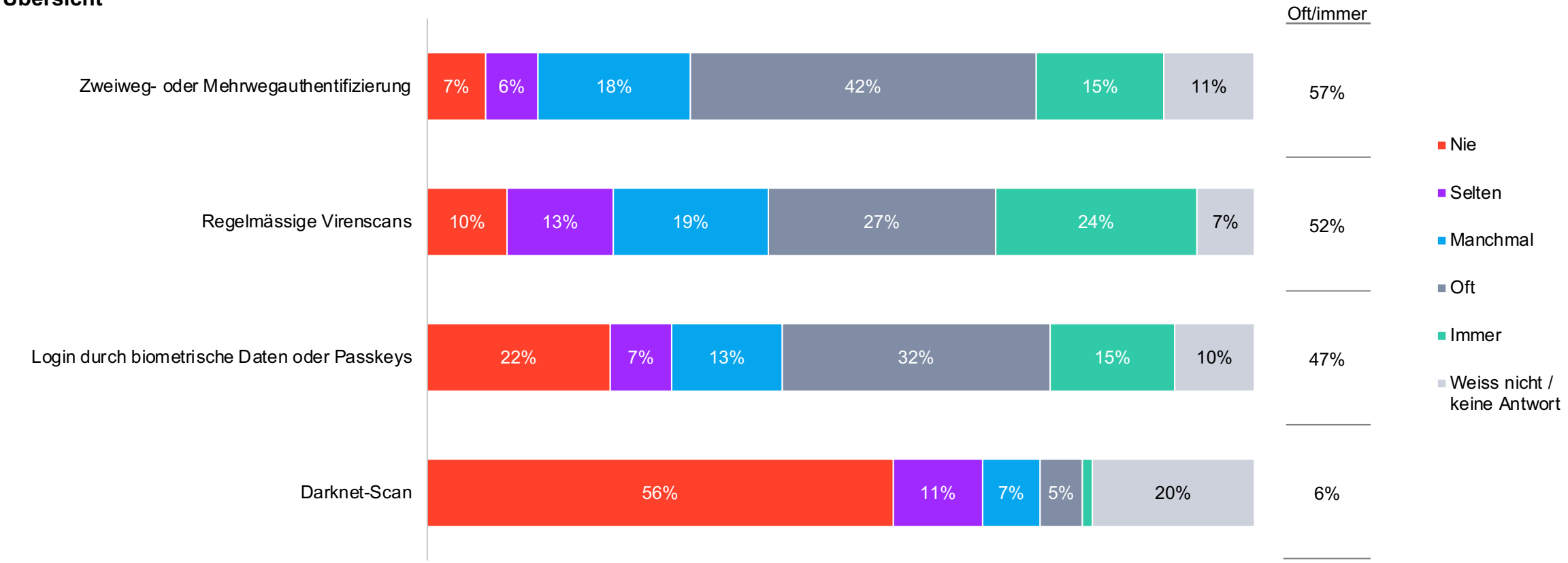


F118: Führen Sie regelmässig ein Backup Ihrer Daten durch?
Basis: n=[ ] | Filter: Bevölkerung | Geschlossene Frage | ⬆ signifikant höher als Total; ⬇ signifkant tiefer als Total | Datenbeschriftung ab 3%
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Technische Massnahmenumsetzung (1/2)

Die Zwei- bzw. Mehrwegauthentifizierung hat sich schon recht weit durchgesetzt; mehr als die Hälfte der Befragten (57%) nutzen sie oft oder immer. Biometrische Daten und Passkeys werden seltener, aber immerhin von knapp der Hälfte (47%) oft oder immer verwendet. Darknet-Scans hingegen sind weitgehend unbekannt.

Übersicht

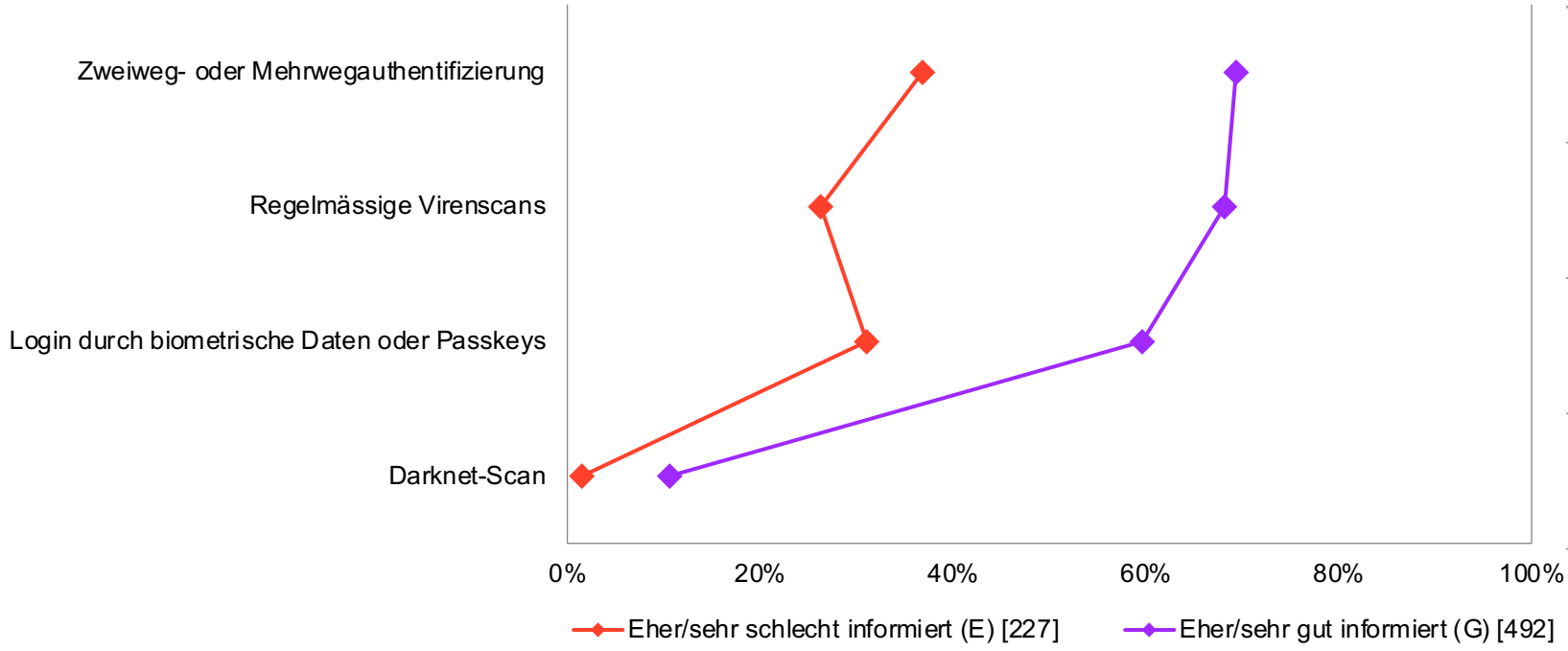


F119: Wie häufig führen Sie die folgenden technischen Sicherheitsmassnahmen durch?
Basis: n=1‘247 | Filter: Bevölkerung | Geschlossene Frage | Datenbeschriftung ab 3%

Technische Massnahmenumsetzung (2/2)

Eher bzw. sehr gut informierte Befragte führen alle abgefragten technischen Massnahmen signifikant häufiger durch als eher/sehr schlecht informierte.

Nach Informationsgrad

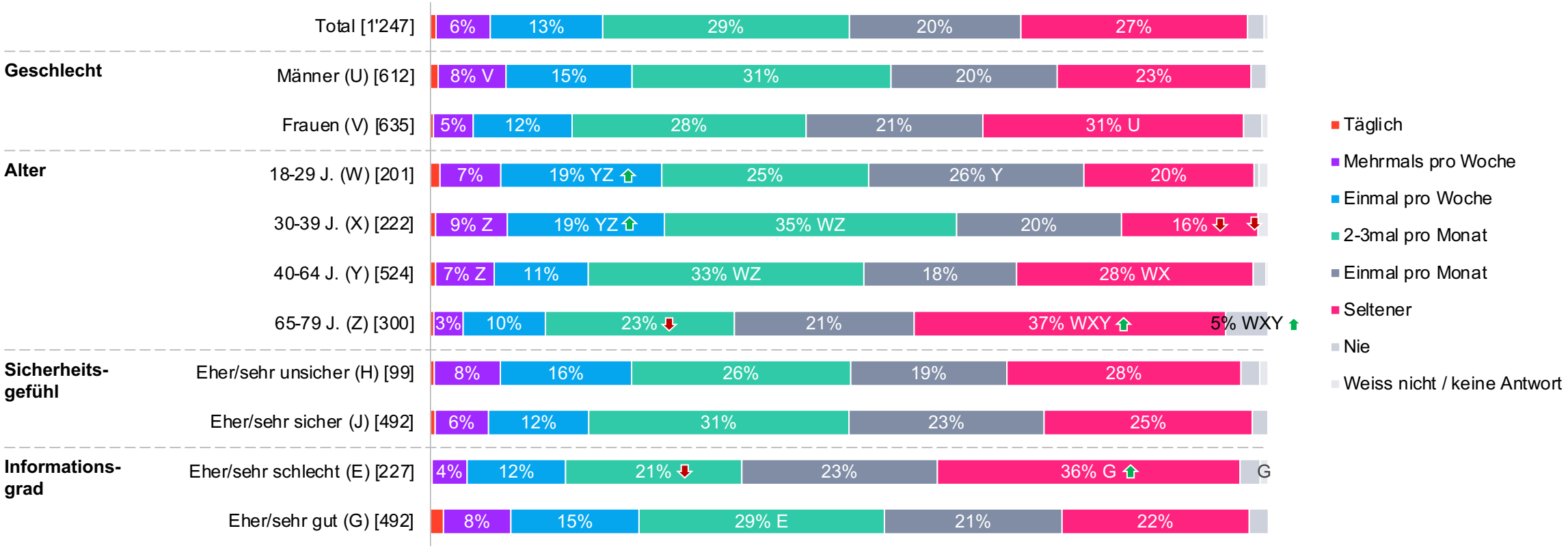


	Oft/immer	
	Eher/sehr schlecht	Eher/sehr gut
Zweiweg- oder Mehrwegauthentifizierung	37%	69% E
Regelmässige Virenscans	26%	68% E
Login durch biometrische Daten oder Passkeys	31%	60% E
Darknet-Scan	2%	11% E

F119: Wie häufig führen Sie die folgenden technischen Sicherheitsmassnahmen durch?
Basis: n=[ ] | Filter: Bevölkerung | Geschlossene Frage
signifikant höher als Total; signifikant tiefer als Total | Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Häufigkeit Onlineshopping

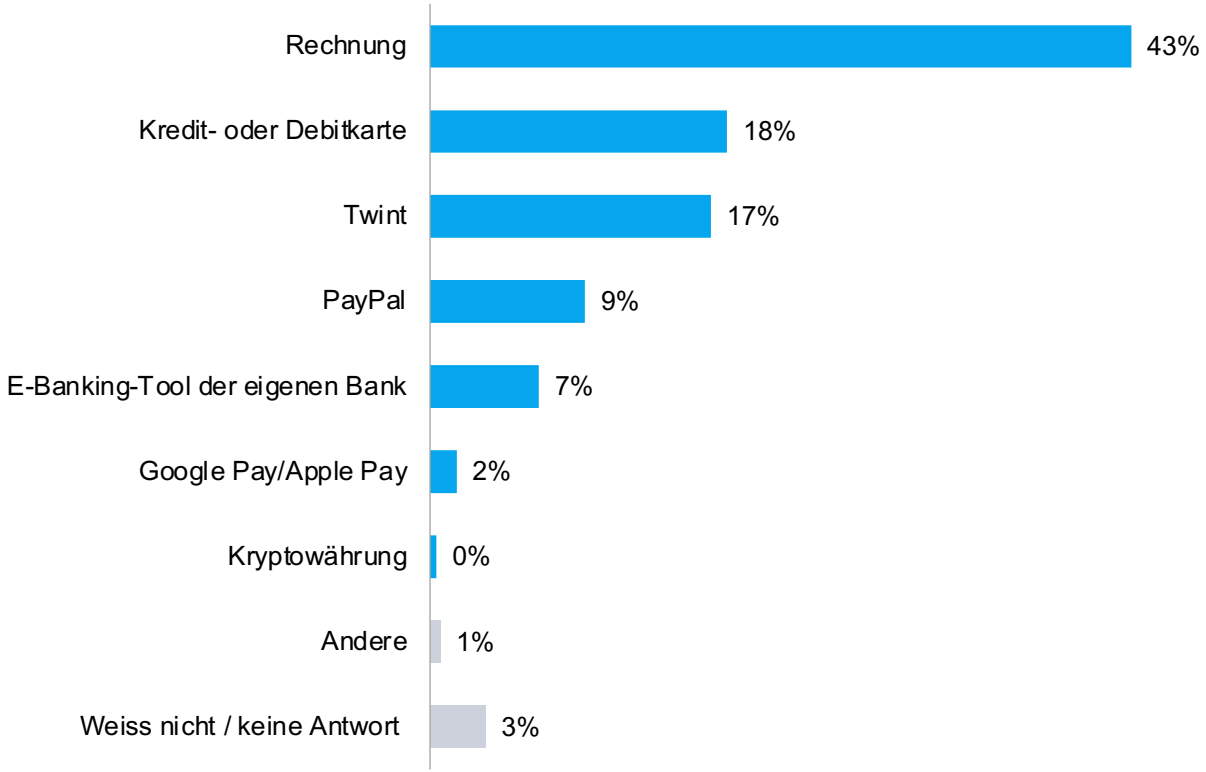
Fast die Hälfte der Befragten (49%) kauft mindestens zwei- bis dreimal pro Monat online ein, weitere 20% monatlich und gut ein Viertel (27%) seltener. Frauen, über 65-jährige und (sehr) schlecht informierte Befragte shoppen signifikant seltener online.



F120: Wie oft kaufen Sie im Internet ein?
Basis: n=[ ] | Filter: Bevölkerung | Geschlossene Frage | ▲ signifikant höher als Total; ▼ signifkant tiefer als Total | Datenbeschriftung ab 3%
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Sicherstes Zahlungsmittel

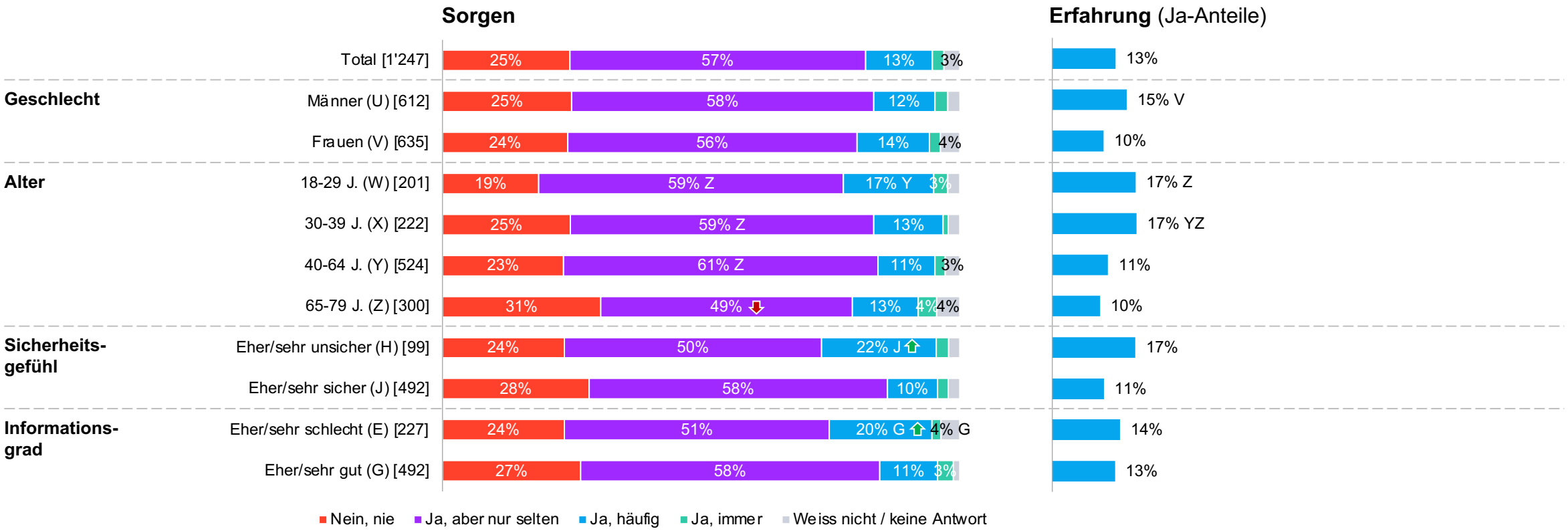
Etwas mehr als zwei Fünftel der Befragten beurteilen die Rechnung als sicherste online Bezahlmethode. Auf Platz zwei und drei liegen, dicht beieinander, die Kredit-/Debitkarte und Twint. Bei den 18- bis 29-jährigen liegt Twint an erster Stelle (30%), dicht gefolgt von der Rechnung (29%), mit der Debit-/Kreditkarte (12%) deutlich abgeschlagen auf dem 3. Platz.



F121: Welche der folgenden Zahlungsmethoden finden Sie am sichersten, wenn Sie online einkaufen?
Basis: n=1‘221 | Filter: Bevölkerung | Geschlossene Frage

Betrug beim Onlineshopping

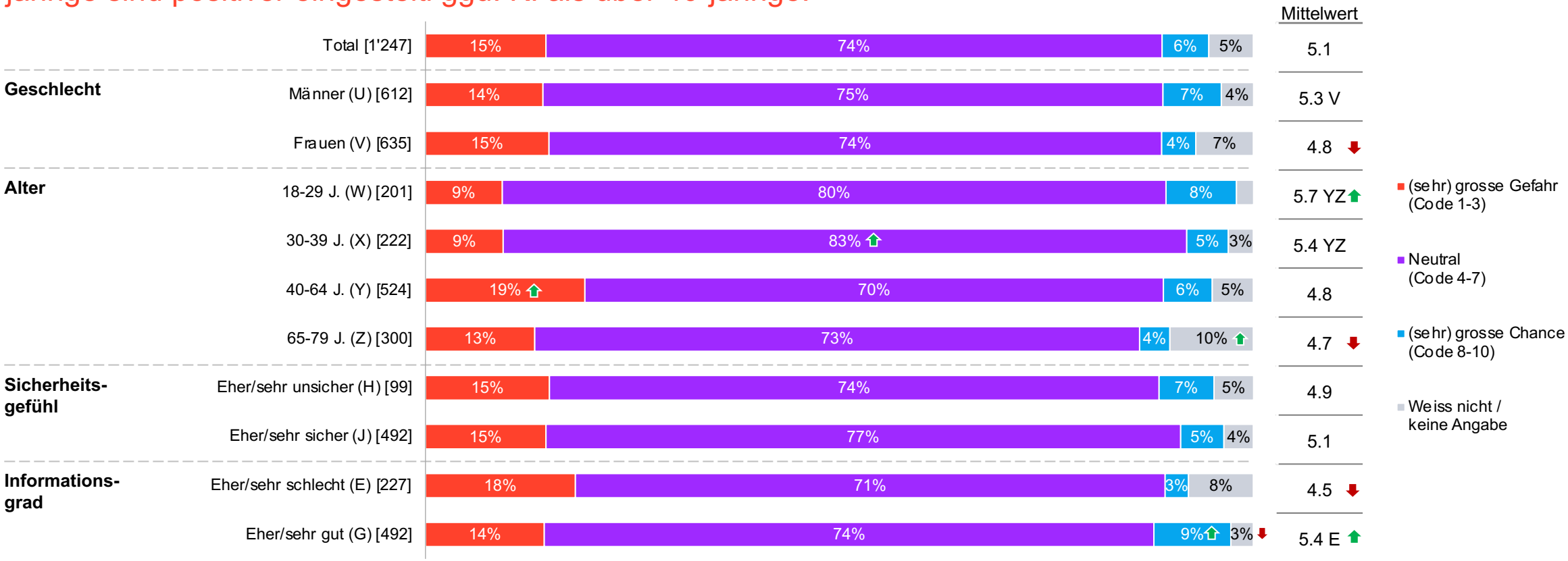
Knapp drei Viertel (72%) der Befragten machen sich (zumindest selten) Sorgen, auf Onlineshops oder Buchungsplattformen betrogen zu werden. (Sehr) unsichere und (sehr) schlecht informierte sorgen sich häufiger. Tatsächlich von Betrug betroffen waren 13% der Befragten, Männer (15%) und unter 40-jährige (17%) signifikant häufiger.



F122: Haben Sie sich schon Sorgen gemacht, dass Sie auf Onlineshops oder Buchungsplattformen betrogen werden, dass also die Webseite oder das Angebot nicht echt ist?
F123: Wurden Sie in den letzten fünf Jahren in einem Onlineshop oder auf einer Buchungsplattform betrogen in dem Sinne, dass Sie für etwas bezahlten, dies dann aber nicht bekamen?
Basis: n=[ ] | Filter: Bevölkerung | Geschlossene Fragen | ⇧ signifikant höher als Total; ⇩ signifkant tiefer als Total | Datenbeschriftung ab 3%
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Einstellung zu KI

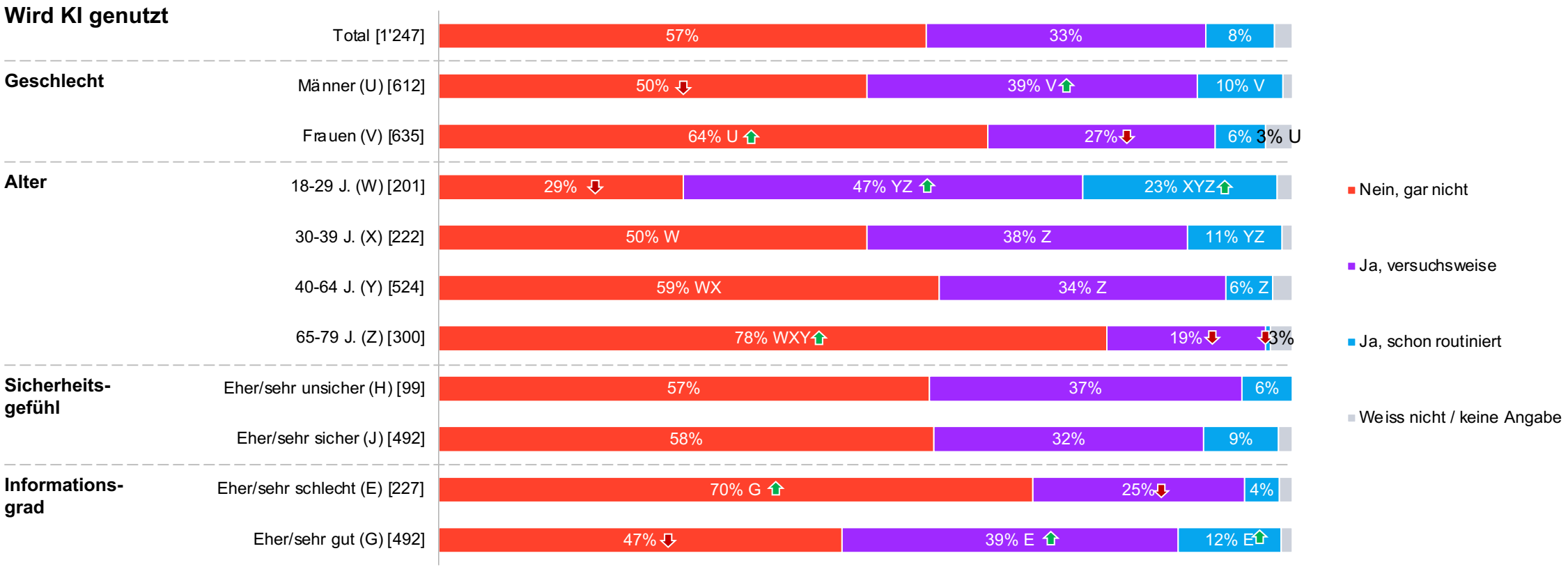
Fast drei Viertel der Befragten haben eine indifferente Meinung zu Gefahren und Chancen von KI. Knapp jede/-r siebte sieht eine (sehr) grosse Gefahr darin (15%), knapp jede/-r siebzehnte eine (sehr) grosse Chance. Unter 40-jährige sind positiver eingesteltl ggü. KI als über 40-jährige.



F023: Sehen Sie in den technischen Fortschritten künstlicher Intelligenz eher eine Gefahr oder eine Chance für Sie persönlich?
Basis: n=[ ] | Filter: Bevölkerung | Skalierte Frage: 1= sehr grosse Gefahr bis 10= sehr grosse Chance | ⬆ signifikant höher als Total; ⬇ signifkant tiefer als Total | Datenbeschriftung ab 3%
Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Nutzung KI

Ein Drittel der Befragten hat schon Versuche mit KI durchgeführt, knapp jede/-r zehnte (8%) setzt KI schon routiniert ein. Die Altersunterschiede sind beträchtlich; je jünger die Befragten sind, desto eher haben sie KI schon ausprobiert bzw. arbeiten routiniert damit.

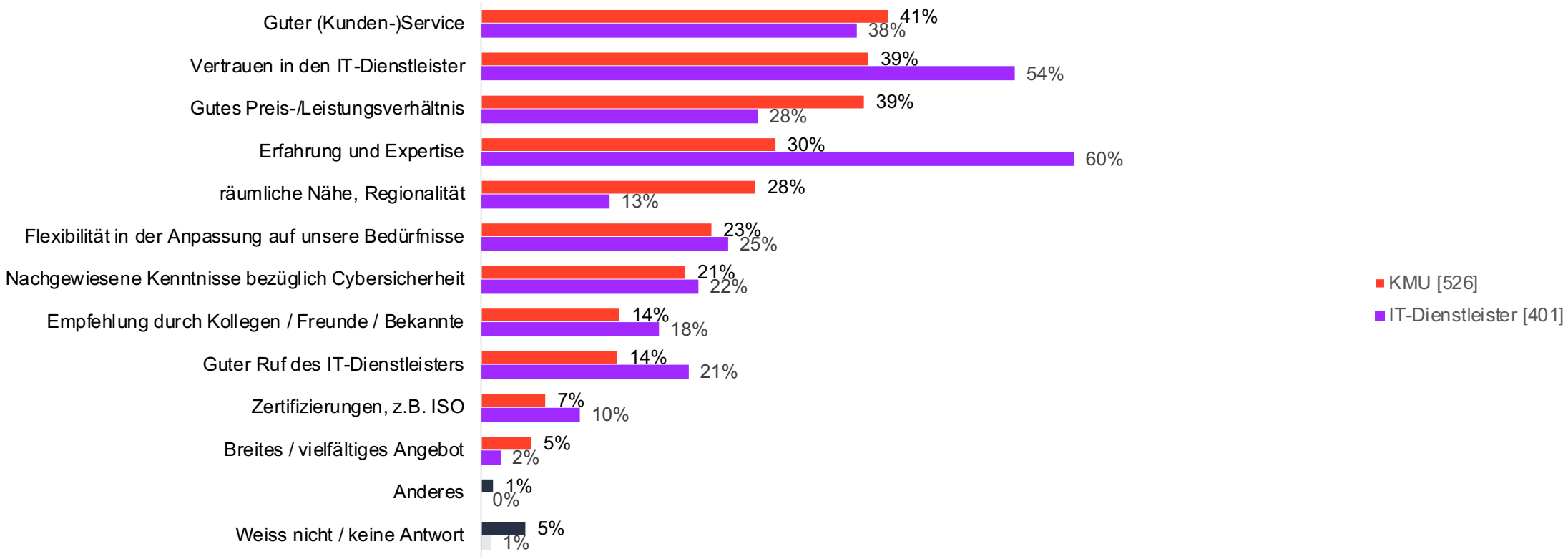


F024: Setzen Sie persönlich schon aktiv künstliche Intelligenz ein?
Basis: n=[ ] | Filter: Bevölkerung | Geschlossene Frage | ⬆ signifikant höher als Total; ⬇ signifkant tiefer als Total | Datenbeschriftung ab 3%
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

06 Zielgruppen-vergleiche

Auswahlkriterien IT-Dienstleister

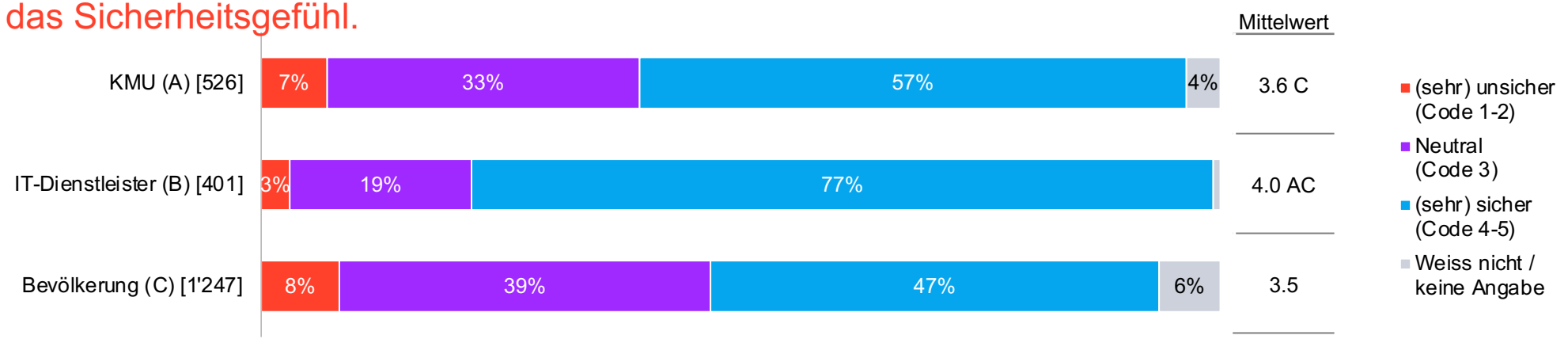
IT-Dienstleister und KMU sind sich mit der Priorisierung der meisten Aspekte einig. Vertrauen und Erfahrung/ Expertise wird allerdings von den IT-Dienstleistern viel höher bewertet als von den KMU, während die KMU ein gutes Preis-/Leistungsverhältnis und Regionalität höher gewichten als IT-Dienstleister.



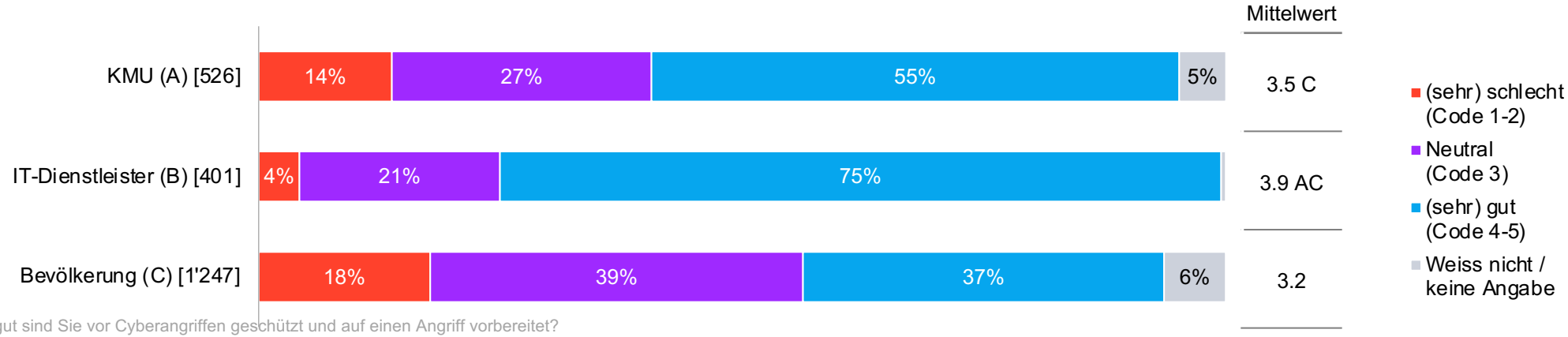
F005: Welche der folgenden Kriterien sind aus Ihrer Sicht für die Auswahl eines IT-Dienstleisters am wichtigsten? Bitte wählen Sie max. 3 Antworten aus.
Basis: n=526 | Filter: Alle Befragten | Geschlossene Frage
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Sicherheitsgefühl und Resilienz

IT-Dienstleister fühlen sich am sichersten (MW 4.0); das Sicherheitsgefühl der KMU liegt signifikant tiefer (3.6) und dasjenige der Bevölkerung noch etwas tiefer (3.5). Das Gefühl der Resilienz liegt bei allen drei Zielgruppen je leicht tiefer als das Sicherheitsgefühl.



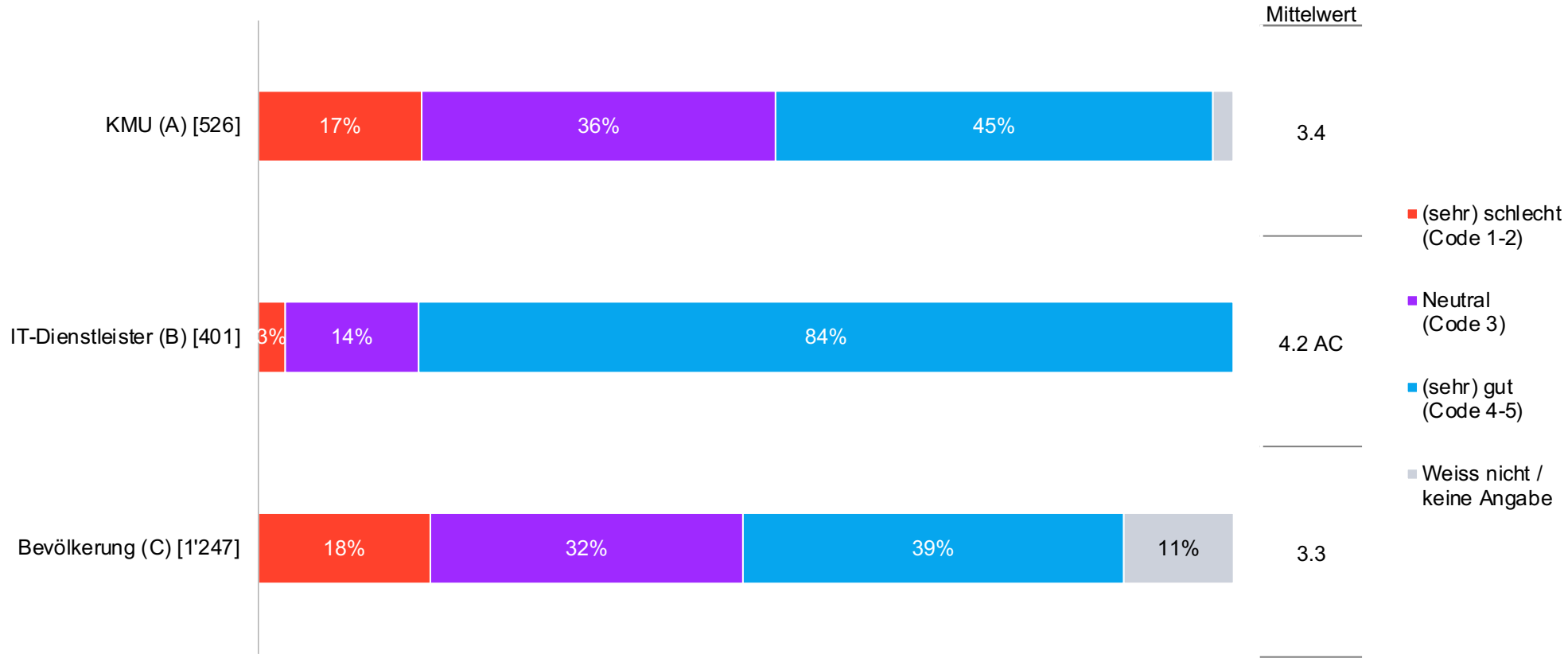
F007: Wie sicher fühlen Sie sich in Ihrem Unternehmen vor Cyberkriminalität? / Wie bewerten Sie die Cybersicherheit Ihres Haushalts?
Basis: n=[ ] | Filter: Alle Befragten | Skalierte Frage: 1= sehr unsicher bis 5= sehr sicher | Datenbeschriftung ab 3%
Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.



F008: Was schätzen Sie: Wie gut sind Sie vor Cyberangriffen geschützt und auf einen Angriff vorbereitet?
Basis: n=[ ] | Filter: Alle Befragten | Skalierte Frage: 1= sehr schlecht bis 5= sehr gut | Datenbeschriftung ab 3%
Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Informationsgefühl

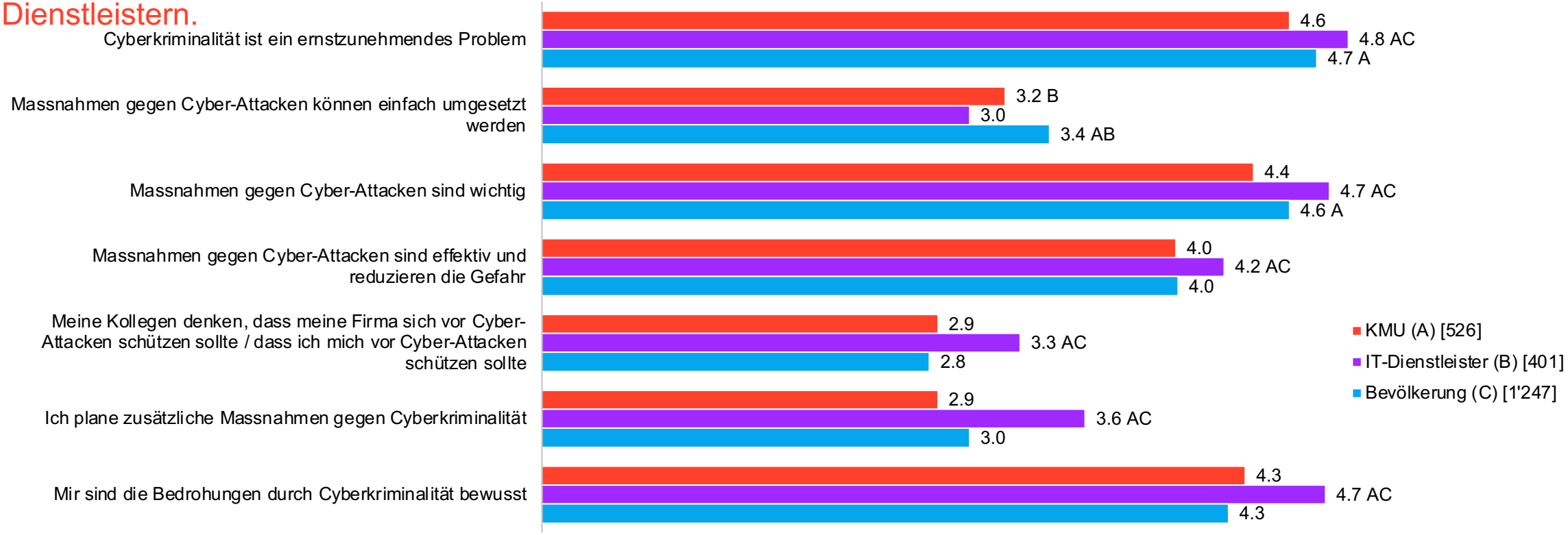
IT-Dienstleister fühlen sich am besten informiert, wie Sie sich vor Cyberangriffen schützen können. KMU und die Bevölkerung antworten ähnlich.



F009: Wie gut fühlen Sie sich persönlich in der Cyberrisk-Thematik informiert? / Wie gut wissen Sie im Vergleich zu ihren Kolleginnen und Kollegen Bescheid, wie Sie sich vor Cyberangriffen schützen können?
Basis: n=[ ] | Filter: Alle Befragten | Skalierte Frage: 1= sehr schlecht bis 5= sehr gut | Datenbeschriftung ab 3%
Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Einstellung zu Cyberkriminalität

KMU und die Bevölkerung antworten auf fast alle Einstellungs-Aspekte nahezu identisch, während die IT-Dienstleister stärker zustimmen. Grosse Ausnahme ist die Aussage, dass Massnahmen einfach umgesetzt werden können. Die Bevölkerung stimmt am ehesten zu, gefolgt von den KMU und – signifikant tiefer – den IT-Dienstleistern.

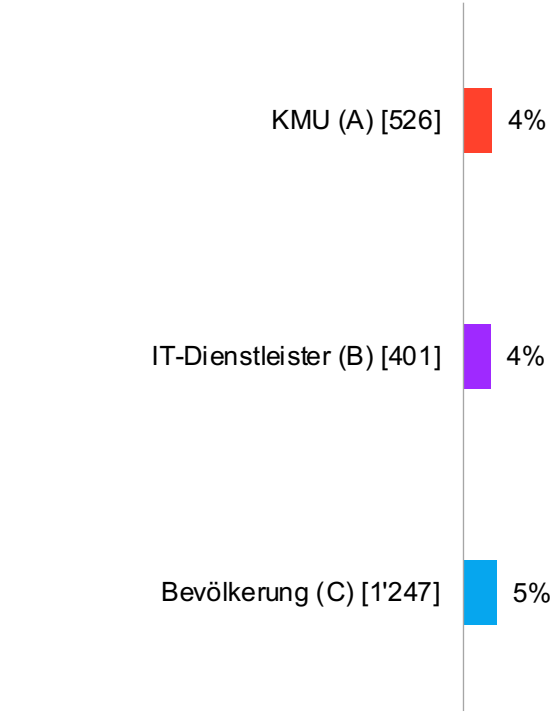


F015: Inwiefern stimmen Sie den folgenden Aussagen zu Cyberkriminalität wie Malware, Online-Betrug und Hacking zu?
Basis: n=[ ] | Filter: Alle Befragten | Skalierte Frage: 1= überhaupt nicht bis 5= voll und ganz | Mittelwerte ausgewiesen
Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

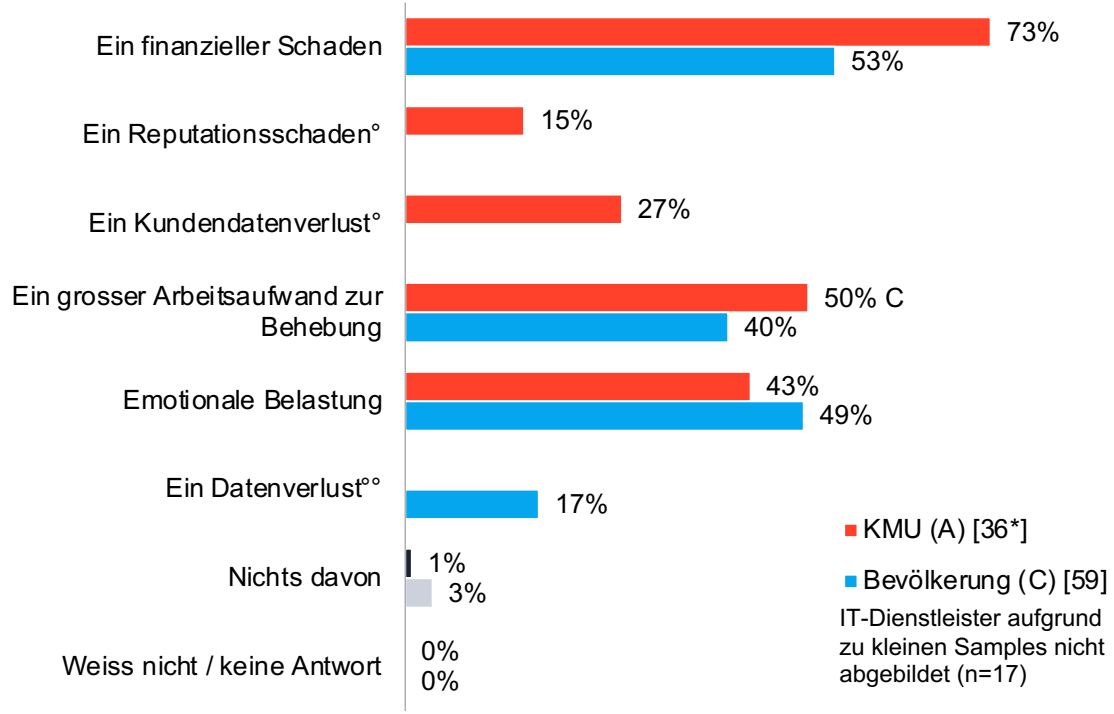
Erfahrung Cyberkriminalität

Alle drei Zielgruppen haben im selben Ausmass (4%) Angriffe erlitten, die Folgen nach sich zogen. Die häufigste Folge war sowohl bei den KMU als auch bei der Bevölkerung ein finanzieller Schaden, aber auch über grossen Arbeitsaufwand und emotionale Belastung wird bei beiden Gruppen berichtet.

Erlittene Angriffe (Ja-Anteile)
Filter: Alle Befragten



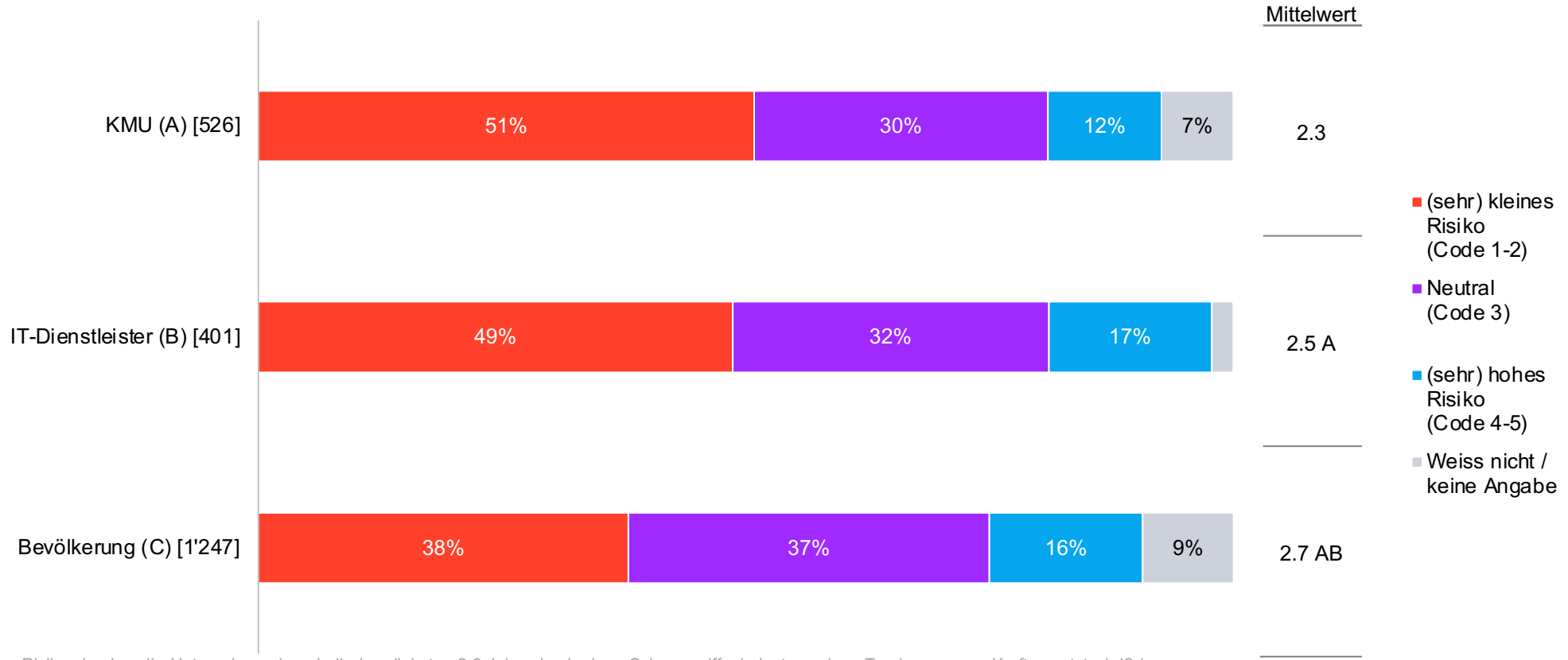
Erlittene Schäden
Filter: Alle Befragten – wenn Cyberangriff erlitten



F016: Hat Ihr Unternehmen innerhalb der letzten 3 Jahre einen Cyberangriff erlitten, der einen finanziellen Schaden oder einen Reputationsschaden verursachte, viel Mühe für die Schadensbereinigung bereitete oder Ihnen emotional sehr zu schaffen gemacht hat? / Haben Sie als Privatperson innerhalb der letzten 3 Jahre durch einen Cyberangriff einen finanziellen Schaden erlitten, viel Mühe für die Schadensbereinigung gehabt oder emotional gelitten?
F017: Entstand durch diesen Angriff… | Basis: n=[ ] | Filter: siehe oben | Geschlossene Fragen | °Nur KMU und IT-Dienstleister | °°Nur Bevölkerung | *Kleine Basis <50; **Sehr kleine Basis <30
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Risikoeinschätzung

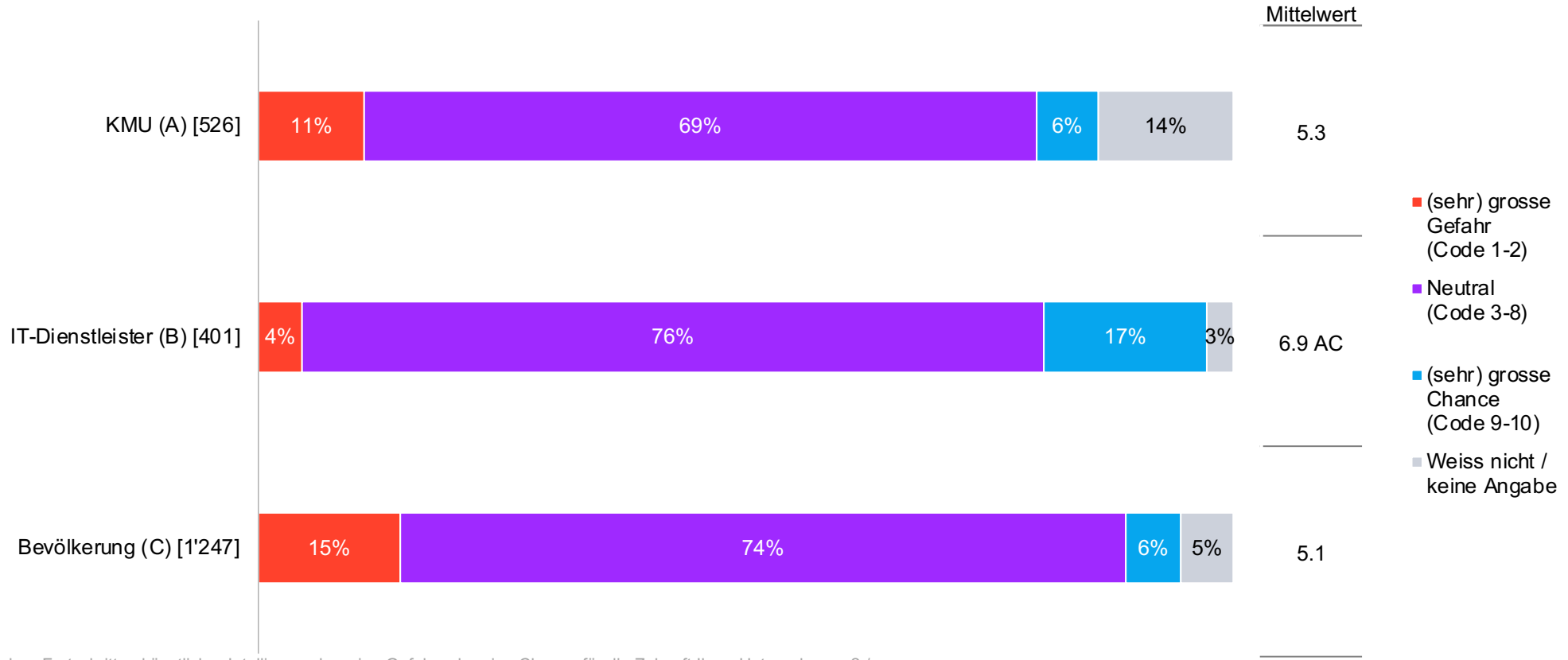
Die Bevölkerung schätzt das Risiko eines folgenschweren Cyberangriffs am höchsten ein, KMU am niedrigsten. Rund jede/-r sechste bis jede/-r achte Befrage beurteilt das Risiko als eher oder sehr hoch.



F021: Wie hoch schätzen Sie das Risiko ein, dass Ihr Unternehmen innerhalb der nächsten 2-3 Jahre durch einen Cyberangriff mindestens einen Tag lang ausser Kraft gesetzt wird? / Wie hoch schätzen Sie das Risiko ein, innerhalb der nächsten 2-3 Jahre durch einen Cyberangriff Geld oder Daten zu verlieren?
Basis: n=[ ] | Filter: Alle Befragten | Skalierte Frage: 1= sehr kleines Risiko bis 5= sehr grosses Risiko | Datenbeschriftung ab 3%
Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Einstellung zu KI

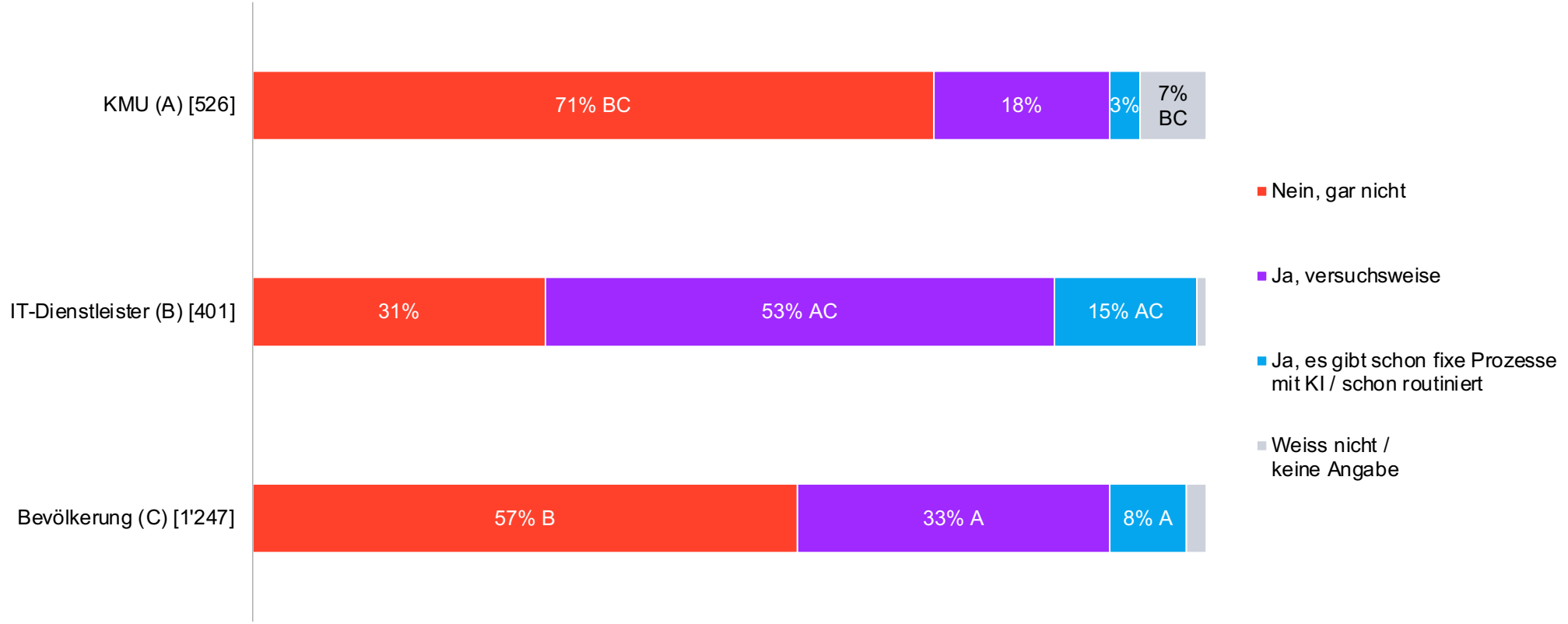
IT-Dienstleister sind am positivsten eingestellt gegenüber KI, die grosse Mehrheit aller Zielgruppen (zwei Drittel bis drei Viertel) haben eine neutrale Meinung.



F023: Sehen Sie in den technischen Fortschritten künstlicher Intelligenz eher eine Gefahr oder eine Chance für die Zukunft Ihres Unternehmens? / Sehen Sie in den technischen Fortschritten künstlicher Intelligenz eher eine Gefahr oder eine Chance für Sie persönlich?
Basis: n=[ ] | Filter: Alle Befragten | Skalierte Frage: 1= sehr grosse Gefahr bis 10= sehr grosse Chance | Datenbeschriftung ab 3%
Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Nutzung KI

Rund zwei Drittel der IT-Dienstleister und rund zwei Fünftel der Bevölkerung haben zumindest schon Versuche mit KI durchgeführt, bei den KMU liegt dieser Anteil mit rund einem Fünftel deutlich tiefer.



F024: Wird in Ihrem Unternehmen schon aktiv künstliche Intelligenz eingesetzt? / Setzen Sie persönlich schon aktiv künstliche Intelligenz ein?
Basis: n=[ ] | Filter: Alle Befragten | Geschlossene Frage | Datenbeschriftung ab 3%
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

YouGov

Thank you

Living consumer intelligence | yougov.com/business