YouGov

Switzerland

Cybersicherheit 2025

Report erstellt durch YouGov für ADSS, digitalswitzerland, Die Mobiliar, FHNW, ISSS, SATW und SISA

September 2025

Inhalt

01 Studiendesign

Projektteam

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

Simon Bernhard Seebeck
Leiter Kompetenzzentrum Cyber Risk
Die Mobiliar, Bern
simonbernhard.seebeck@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
Professor für Digital Business,
FHNW Hochschule für Wirtschaft
und HES-SO Valais-Wallis, School of
Management
marc.peter@fhnw.ch

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

Manuel Kugler
Data & AI Programme Manager
Schweizerische Akademie
der Technischen
Wissenschaften SATW, Zürich
manuel.kugler@satw.ch

Studienpartnerin: /SSS information security society switzerland

Studiendesign

Kunde:	Die Mobiliar (Simon Bernhard Seebeck) digitalswitzerland (Kristof Hertig) Allianz digitale Sicherheit Schweiz (Andreas W. Kaelin) Fachhochschule Nordwestschweiz FHNW (Marc K. Peter) Schweizerischen Akademie der Technischen Wissenschaften SATW (Manuel Kugler) Swiss Internet Security Alliance SISA (Katja Dörlemann)
YouGov:	Karin Mändli Lerch | Senior Consultant Michèle Kaufmann | Senior Consultant
Studienziel:	Erhebung der Einstellung von Schweizer KMU und IT-Dienstleistungsunternehmen zum Thema Cyberkriminalität
Erhebungsphase:	25. Juni bis 5. August 2025
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)

Studiendesign

Anzahl Interviews:	KMU:	n = 515 Interviews
	IT-Dienstleister:	n = 336 Interviews
Befragungsmethode:	Online-Fragebogen	
Einladungsverfahren:	KMU:	YouGov Internet-Panel: Das YouGov Internetpanel ist ein probability based Panel und erlaubt damit eine Projektion der Studienresultate auf die befragte Grundgesamtheit. Es entspricht in seiner soziodemografischen Struktur der schweizerischen Bevölkerung mit Internet-Zugang und umfasst rund 115’000 validierte, zu 100% aktiv rekrutierte Mitglieder.
	IT-Dienstleister:	postalischer Versand mit eingekauften Adressen
Gewichtung:	Die **KMU-Stichprobe** wurde mittels 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	

* mit 115'000 validierten, aktiven Mitgliedern

Studiendesign

Gewichtung KMU-Stichprobe

	Erhobene Stichprobe (disproportional)		Repräsentative Gewichtung gem. STATENT 2023 (proportional)	
1 – 3 MA	165	32%	384	75%
4 – 9 MA	162	31%	85	16%
10 – 19 MA	115	22%	29	6%
20 – 49 MA	73	14%	17	3%
D-CH	353	69%	354	69%
W-CH	129	25%	128	25%
Tessin	31	6%	31	6%
Total (gerundet)	515	100%	515	100%

Die durch die Stichprobe abgebildete Grundgesamtheit umfasst **rund 614‘400 Firmen** mit 1 bis 49 Mitarbeitenden (bfs STATENT; 2025) 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.

Abgebildete Grundgesamtheit

Bezeichnung	Anzahl Mit-arbeitende	Anzahl Unternehmen Schweiz*, gerundet	Prozentualer Anteil alle Unternehmen (626’000), gerundet	
Mikrounternehmen	1-9	561’950	90%	Abgebildet in Stichprobe
Kleine Unternehmen	10-49	52’480	8%	
Mittlere Unternehmen	50-249	9’790	2%	
Grosse Unternehmen	250+	1’800	0.3%	
Total		626’000		

*Quelle: Statistik der Unternehmensstruktur STATENT, 21.8.2025

02 Stichproben-struktur

Stichprobenstruktur (gewichtet)

Zielgruppe 1: KMU

Total	**515**
Entscheider	
Ja, alleine	329
Ja, gemeinsam mit anderen Personen	186
Nein	0
Funktion	
Firmeninhaber	187
Freie Berufe	72
Selbständige	125
Leitende Angestellte / Beamte	54
Übrige Angestellte / Beamte / Vertreter	22
Facharbeiter mit Lehre	18
Ungelernte / angelernte Arbeiter	5
In Ausbildung	0
Hausfrau/Hausmann	3
Nicht berufstätig	3
Arbeitslos	4
Pensioniert	23
Mitarbeitende	
1-3 Mitarbeiter	384
4-9 Mitarbeiter	85
10-19 Mitarbeiter	29
20-49 Mitarbeiter	17
Sprachregion	
D-CH	354
W-CH	128
TI	31
Iat CH	159

Total	**515**
Branche	
Land-, Forstwirtschaft, Gartenbau, Fischerei	0
Industrie / Verarbeitung & Herstellung von Waren	19
Baugewerbe	41
Chemie / Pharma / Biotechnologie	4
Energie	3
Grosshandel	9
Detailhandel	27
Handel / Reparatur	20
Bank-, Kredit-, Finanzwesen	23
Versicherungen	3
Verkehr, Lagerei, Logistik	5
Kommunikation	42
Informatik	31
Gastgewerbe / Tourismus	11
Unterhaltung, Kultur, Kunst, Erholung, Sport	25
Immobilien	10
Wirtschaftliche, technische oder wissensch. DL	63
Bildungswesen	30
Gesundheitswesen	49
Sozialwesen	9
Architektur- und Ingenieurbüro	22
Öffentliche Verwaltung, öffentliche Hand	3
Andere Dienstleistungen	51
Einstellung	
Pioniere	13
Early Follower	212
Late Follower	225

Stichprobenstruktur (ungewichtet)

Zielgruppe 2: IT-Dienstleister

Total	**336**
Mitarbeitende	
1-9 Mitarbeiter	**289**
10+ Mitarbeiter	**47**
Sprachregion	
D-CH	**259**
W-CH	**49**
TI	**27**
lat CH	**76**
Funktion	
Firmeninhaber/in	**250**
Geschäftsführer/in	**184**
Entwicklung, Anpassung, Testen / Pflege Software	**99**
Planung und Entwurf von Computersystemen	**112**
Verwaltung und Betrieb der Computersysteme	**108**
Sonstige fachliche und technische Tätigkeiten	**105**
Anderes	**31**
Kundenstamm	
Privatpersonen	**88**
KMU mit 1-9 Mitarbeitenden	**196**
KMU mit 10-49 Mitarbeitenden	**152**
KMU mit 50-250 Mitarbeitenden	**135**
Firmen mit über 250 Mitarbeitenden	**140**

Total	**336**
Regionalität	
Lokal	**140**
Regional	**185**
National	**202**
International	**111**
Einstellung	
Pioniere	**95**
Early Follower	**154**
Late Follower	**45**
IT-Sicherheitszertifikat	
Ja	**40**

03 KMU-Befragung

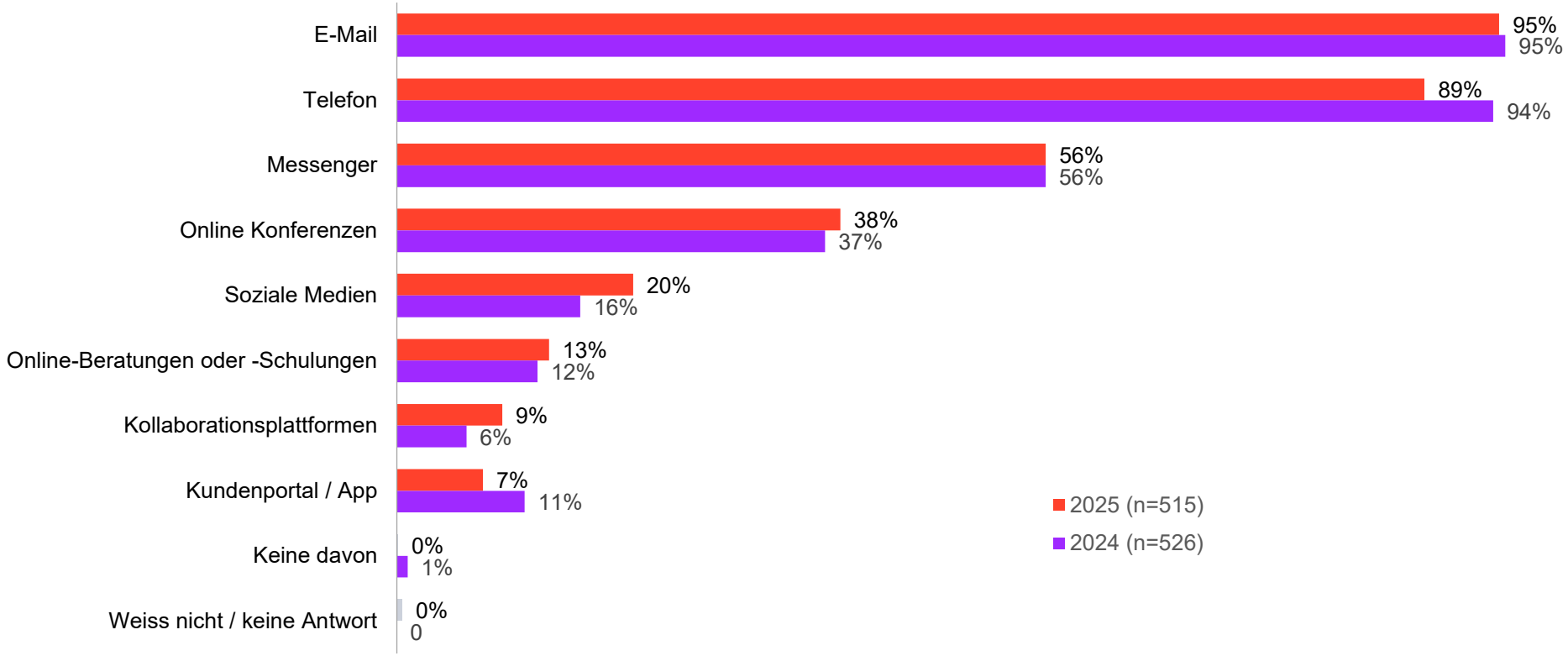
Branche und Firmengrösse

	Gesamt	1-3	4-9	10-19	20-49
Ungewichtete Basis Netto	515	165	162	115	73
Basis Netto	515	384	85	29	17
Wirtschaftliche, technische oder wissenschaftliche DL	12%	13%	10%	5%	7%
Andere Dienstleistungen (Friseursalon, Entsorgung, …)	10%	12%	6%	4%	1%
Gesundheitswesen	9%	10%	9%	6%	4%
Kommunikation (Medien, Telekommunikation, Agentur, Marketing, ...)	8%	10%	4%	1%	4%
Baugewerbe (Hoch-, Tiefbau, Baunebengewerbe)	8%	7%	10%	10%	8%
Informatik	6%	6%	6%	4%	4%
Bildungswesen	6%	6%	3%	8%	8%
Detailhandel	5%	5%	5%	12%	3%
Unterhaltung, Kultur, Kunst, Erholung, Sport	5%	5%	4%	3%	-
Bank-, Kredit-, Finanzwesen	5%	5%	4%	3%	3%
Architektur- und Ingenieurbüro	4%	4%	6%	6%	5%
Handel / Reparatur (Motorfahrzeuge, Maschinen, …)	4%	4%	6%	1%	3%
Industrie / Verarbeitung und Herstellung von Waren	4%	2%	5%	10%	16%
Gastgewerbe / Tourismus	2%	1%	5%	4%	7%
Immobilien	2%	2%	2%	3%	1%
Grosshandel	2%	1%	4%	3%	4%
Sozialwesen	2%	1%	2%	5%	4%
Verkehr, Lagerei, Logistik	1%	1%	1%	4%	4%
Chemie / Pharma / Biotechnologie	1%	-	4%	1%	3%
Öffentliche Verwaltung, öff. Hand (Sicherheit, Sozialversicherung, …)	1%	-	1%	4%	7%
Versicherungen	1%	1%	-	1%	1%
Energie	1%	1%	-	1%	-
Weiss nicht / keine Antwort	3%	4%	2%	-	1%

S05: In welcher Branche ist Ihr Betrieb tätig? / S03 Anzahl Mitarbeitende
Basis: n=515 | Filter: KMU | Geschlossene Frage

Kommunikationsmittel

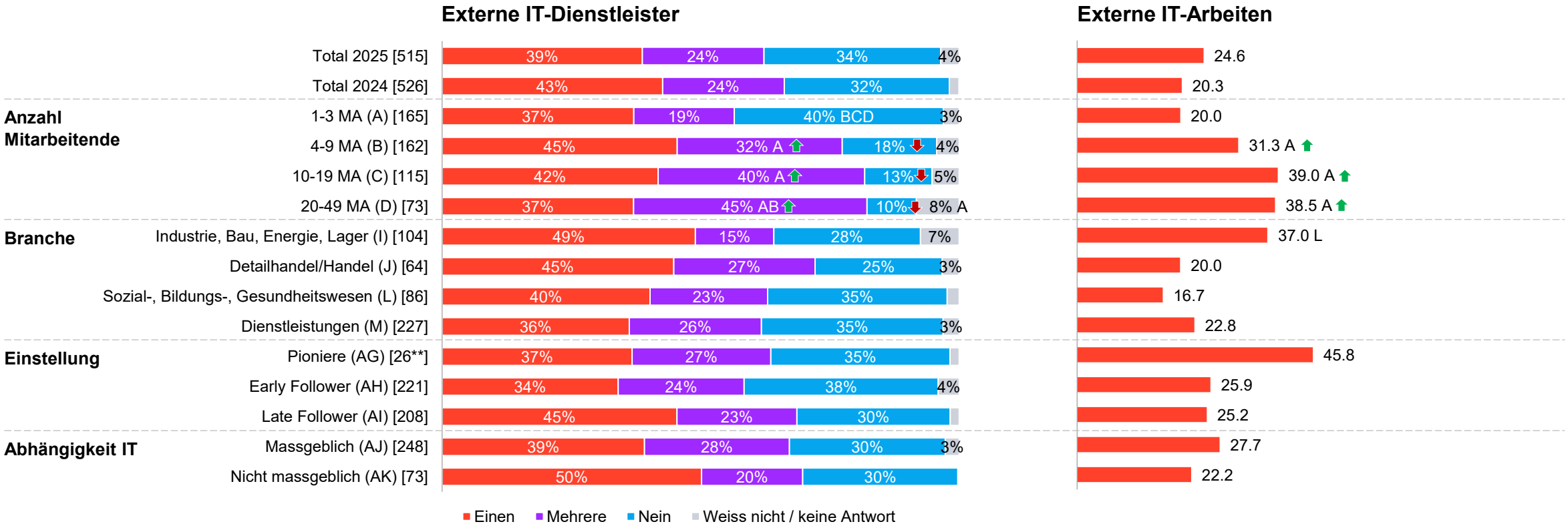
Neben den Haupt-Kommunikationsmitteln E-Mail und Telefon nutzen etwas mehr als die Hälfte der Befragten Messenger-dienste. Unternehmen mit 1-3 Mitarbeitenden nutzen Online Konferenz-Tools (34%), Online-Beratungen (12%), Kollaborationsplattformen (8%) oder ein Kundenportal (4%) deutlich weniger als grössere Unternehmen (nicht abgebildet).



F001: Welche der folgenden Kommunikationsmittel nutzen Ihre Mitarbeitenden aktuell für die Kommunikation mit Partnern, Kundschaft und anderen Mitarbeitenden?
Basis: n=515 | Filter: KMU | Geschlossene Frage

IT-Dienstleister

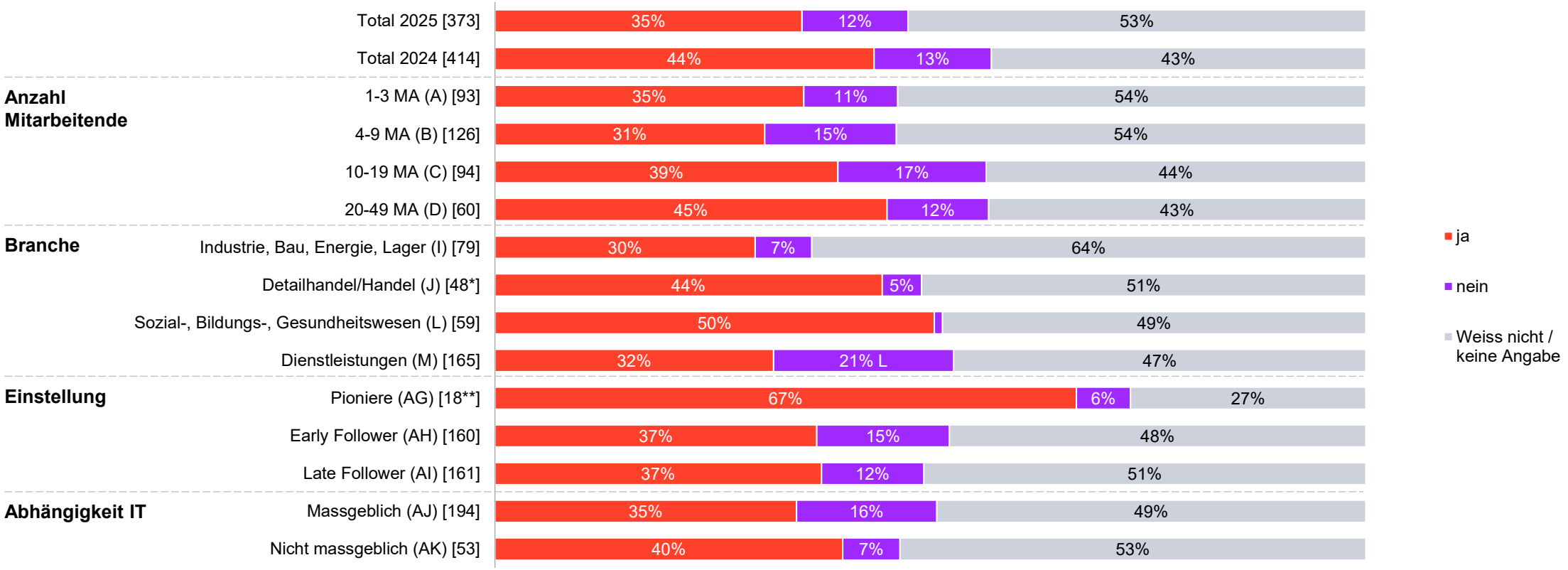
Rund zwei Drittel der KMU haben einen oder mehrere externe IT-Dienstleister für Informatik, Telefonie, Software- oder Hardware-Arbeiten. Grössere Unternehmen geben mehr Arbeiten extern ab als kleinere. Im Schnitt wird rund ein Viertel der IT-Arbeiten extern gegeben.



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; ⬇ signifikant tiefer als Total | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle | **Sehr kleine Basis <30 | 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

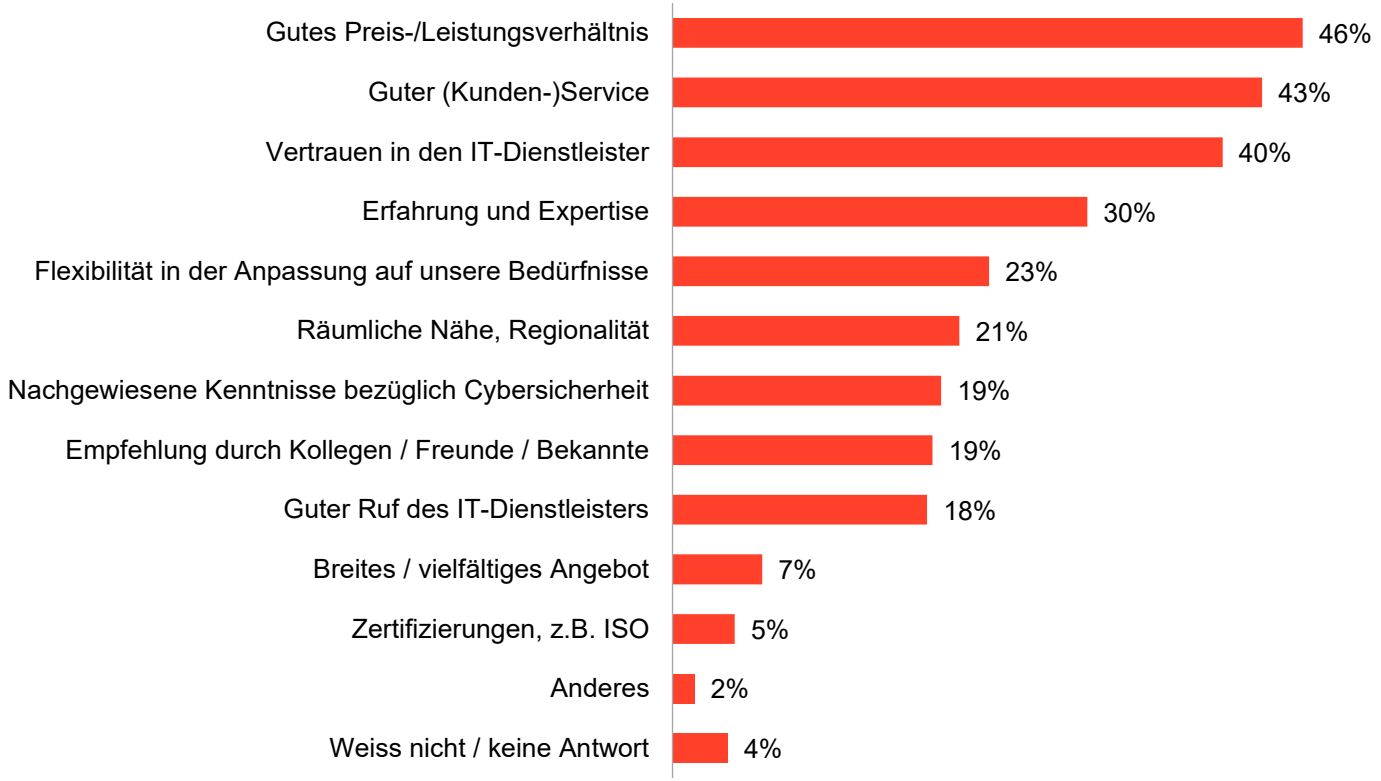
Rund ein Drittel der Befragten hat einen IT-Dienstleister mit IT-Sicherheitszertifizierung wie z.B. ISO 27001, etwas mehr als die Hälfte der Befragten weiss dazu nicht Bescheid. Dieselben Resultate gelten auch für Unternehmen, welche massgeblich von ihrer IT abhängig sind.



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; ⬇ signifikant tiefer als Total | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle | *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.

Auswahlkriterien IT-Dienstleister

Ein gutes Preis-/Leistungsverhältnis ist den Befragten am wichtigsten bei der Auswahl eines IT-Dienstleisters, am zweitwichtigsten ist guter Service und an dritter Stelle folgt ein hohes Vertrauen. Unternehmen, für welche eine funktionierende IT massgeblich ist, beurteilen Kundenservice und Vertrauen höher als das gute Preis-/Leistungsverhältnis.

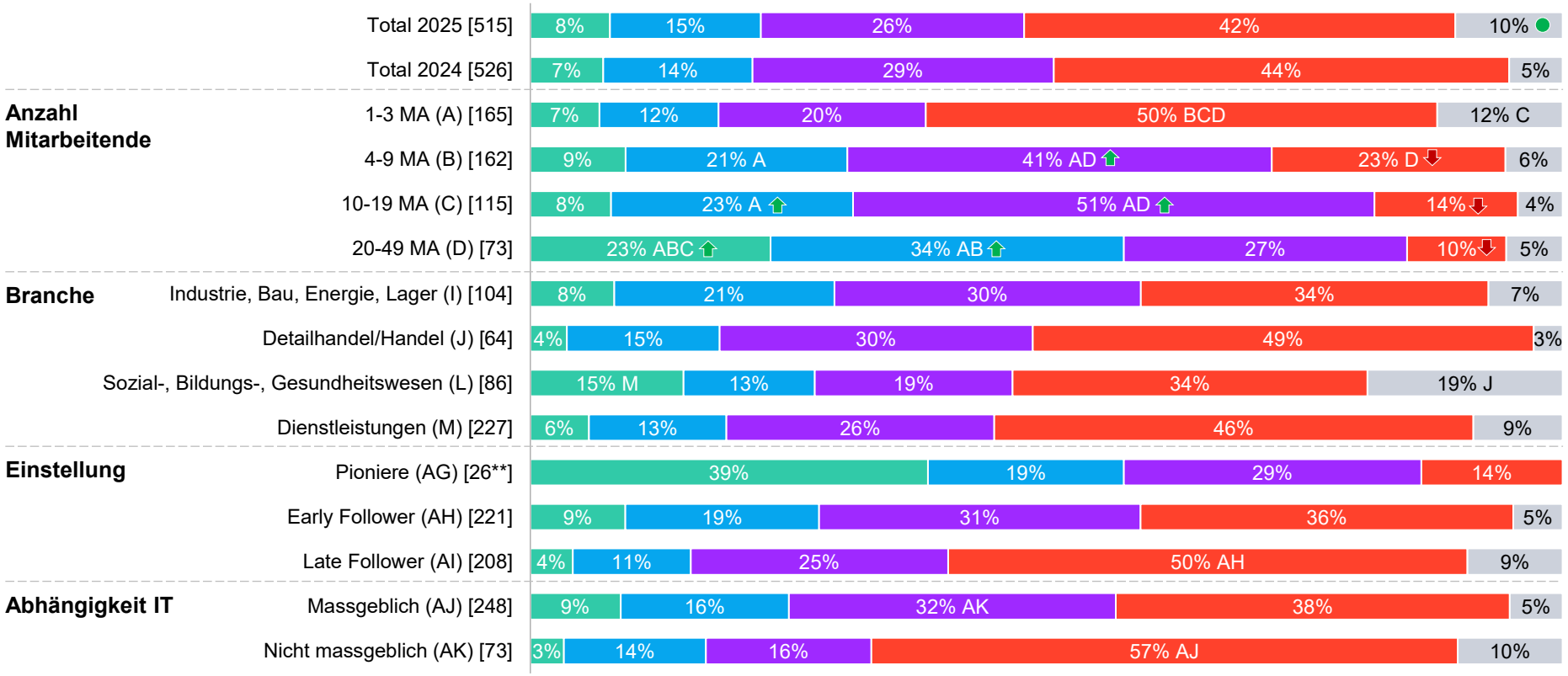


F050: Welche der folgenden Kriterien sind aus Ihrer Sicht für die Auswahl eines IT-Dienstleisters am wichtigsten? Bitte wählen Sie max. 3 Antworten aus.
Basis: n=515 | Filter: KMU | Geschlossene Frage

Aus Sicht der IT-DL…
ist Erfahrung/Expertise am wichtigsten und räumliche Nähe deutlich weniger wichtig (siehe Seite 57).

Cyberrisk-Verantwortung

In nur rund zwei Fünfteln der Unternehmen mit 1-3 Mitarbeitenden gibt es eine für Cybersicherheit zuständige Person; bei den grösseren Unternehmen ist dieser Anteil aber signifikant höher: Rund drei Viertel bis vier Fünftel haben eine zuständige Person, mehrheitlich extern oder intern als Teilaufgabe.

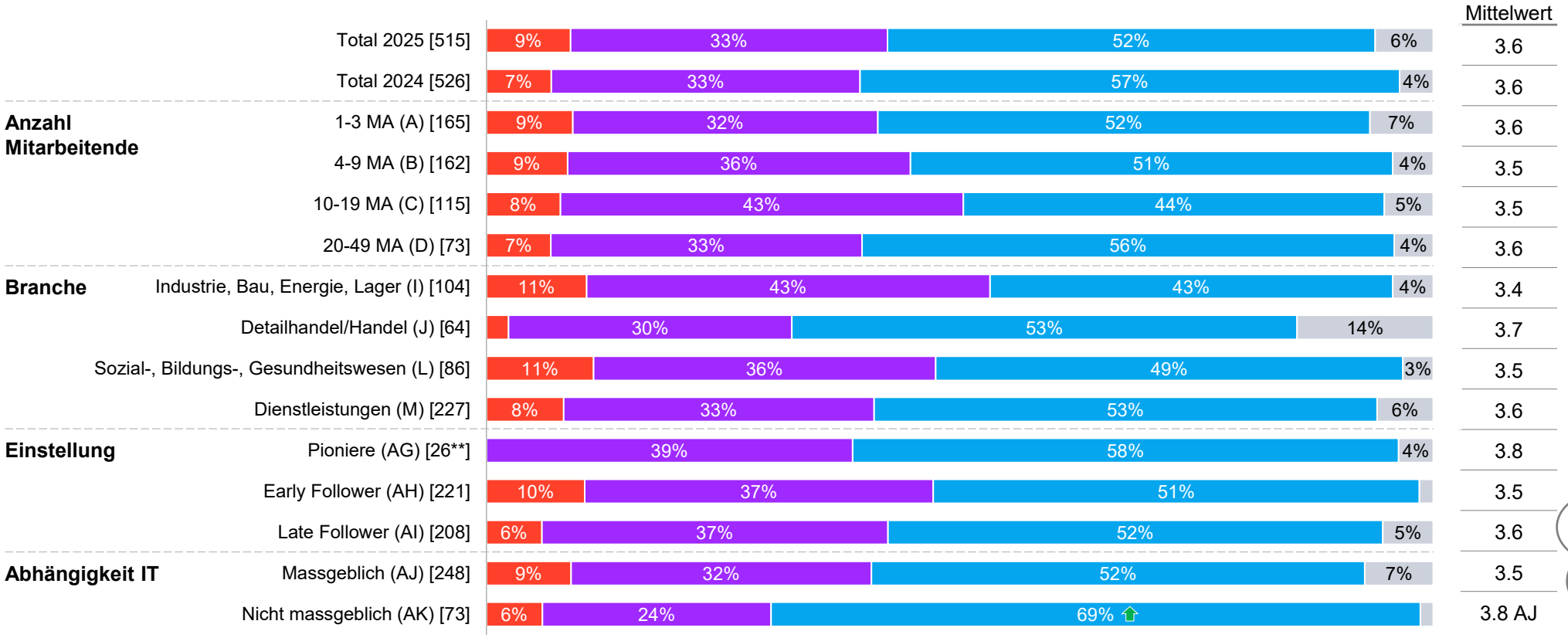


Aus Sicht der IT-DL…
Die befragten IT-DL sind bei durchschnittlich 40% ihrer Kunden für technische, bei 32% für organisatorische Cybersicherheits-Massnahmen zuständig (siehe S. 76).

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; ▼ signifikant tiefer als Total | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle | **Sehr kleine Basis <30 | 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.

Sicherheitsgefühl

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

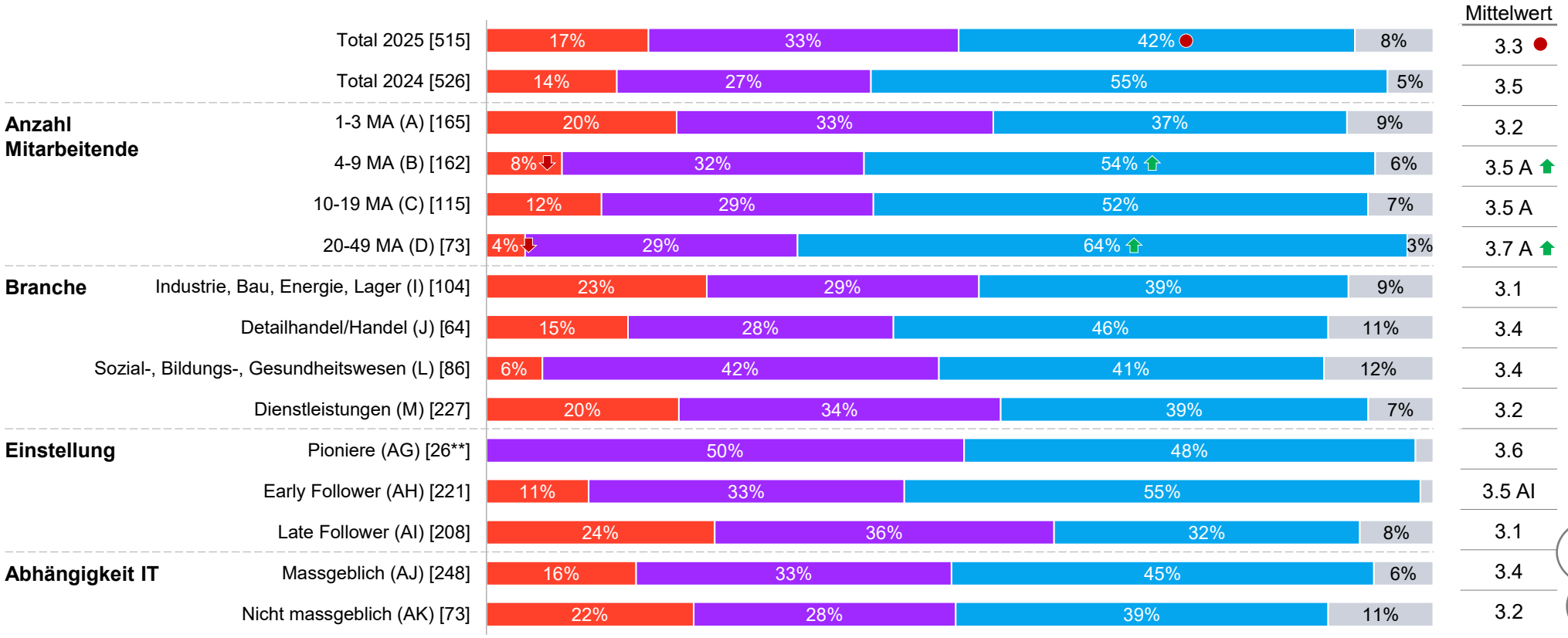


Aus Sicht der IT-DL…
Nur 39% der IT-Dienstleister gehen davon aus, dass ihre Kunden (sehr) sicher sind. (S. 59).

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; ⬇ signifikant tiefer als Total | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle | **Sehr kleine Basis <30 | 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 sechste befragte KMU fühlt sich (sehr) schlecht, rund zwei Fünftel (sehr) gut geschützt vor Cyberangriffen. Diese Zahlen haben sich verschlechtert: Signifikant weniger Befragte fühlen sich (sehr) gut geschützt als noch vor einem Jahr. Das Gefühl der Resilienz ist deutlich höher in Firmen mit 20-49 Mitarbeitenden.

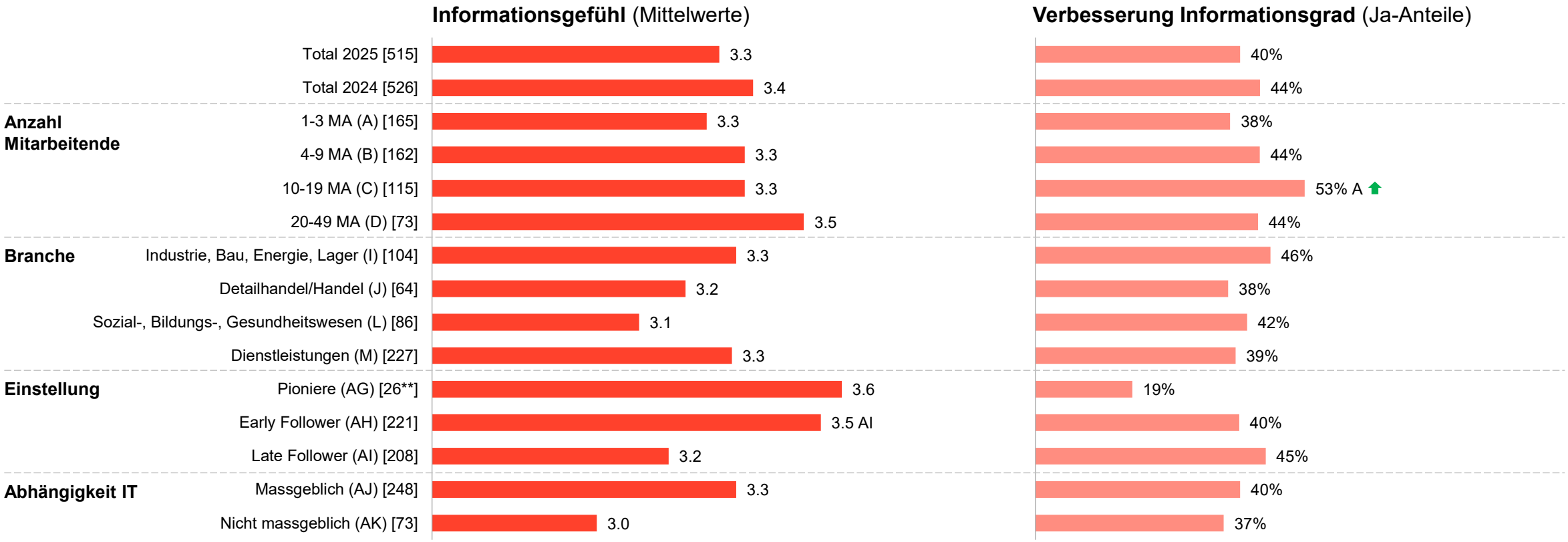


Aus Sicht der IT-DL…
Nur 33% der IT-Dienstleister gehen davon aus, dass ihre Kunden (sehr) resilient sind. (S. 61).

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; ⬇ signifikant tiefer als Total | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle | **Sehr kleine Basis <30 | 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

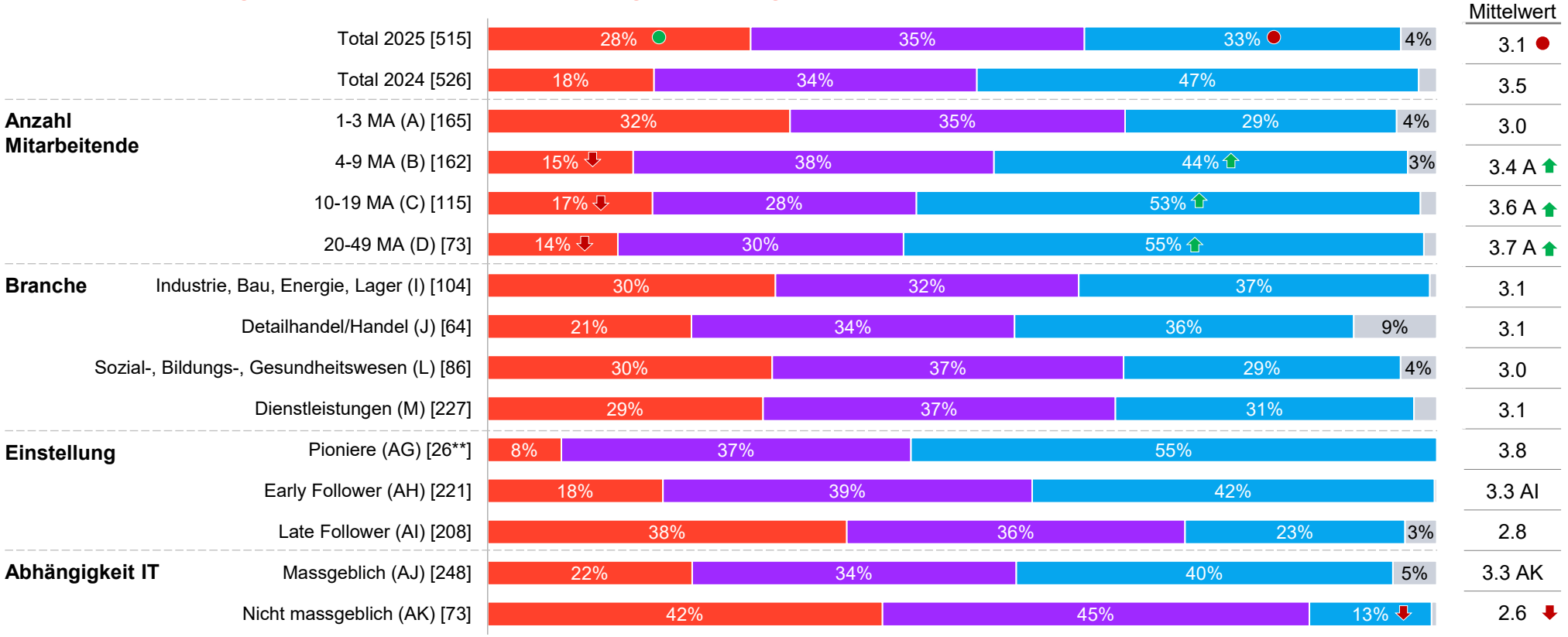
Der gefühlte Informationsgrad liegt bei 3.3 auf der Fünferskala, leicht tiefer als noch 2024 (3.4). Zwei Fünftel der Befragten wären gerne besser informiert zum Thema Cybersicherheit.



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: KMU | Skalierte Frage: 1= sehr schlecht bis 5= sehr gut (F009) & geschlossene Frage (F010) | ▲ signifikant höher als Total; ▼ signifikant tiefer als Total | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle |
**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.

Priorität Cybersicherheit

Die Wichtigkeit des Themas Cybersicherheit ist gegenüber 2024 signifikant gesunken; von einer 3.5 auf der Fünferskala auf eine 3.1. Nur noch ein Drittel der Befragten schätzt das Thema als (sehr) wichtig ein. Unternehmen mit mehr als 3 Mitarbeitenden geben dem Thema allerdings eine signifikant höhere als Unternehmen mit 1-3 Mitarbeitenden.



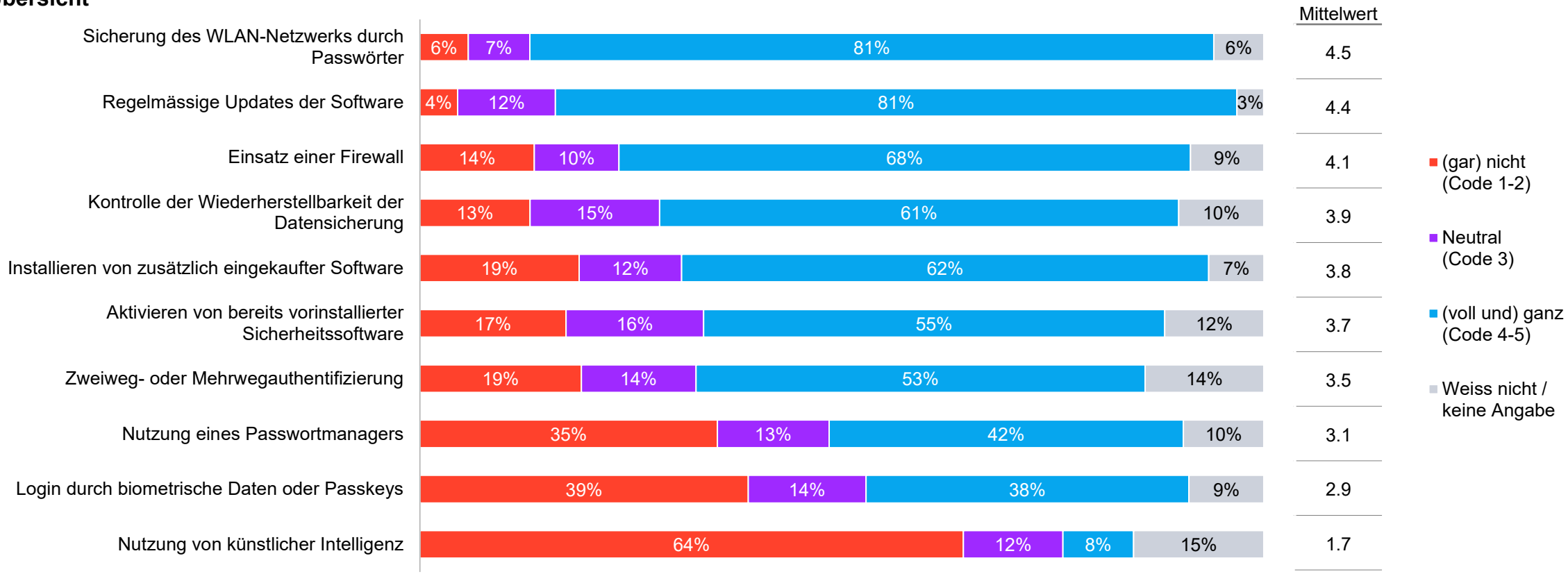
F011: Welche hat in Ihrer Firma das Thema Cybersicherheit? | Basis: n=[ ] | Filter: KMU | Skalierte Frage: 1= überhaupt nicht wichtig bis 5= sehr wichtig |
⬆ signifikant höher als Total; ⬇ signifikant tiefer als Total | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle | **Sehr kleine Basis <30 | 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…
36% der IT-DL würden ihren Kunden empfehlen, das Thema Cyber-sicherheit ernster zu nehmen (siehe S. 78).

Technische Massnahmenumsetzung (1/5)

7 von 10 Massnahmen zur Erhöhung der Cybersicherheit wurden von über der Hälfte der befragten KMU (voll und ganz) umgesetzt. Weniger als die Hälfte der Befragten haben einen Passwortmanager oder Logins durch biometrische Daten/Passkeys. KI wird nur von ganz wenigen zum Schutz gegen Cyberangriffe eingesetzt.

Übersicht

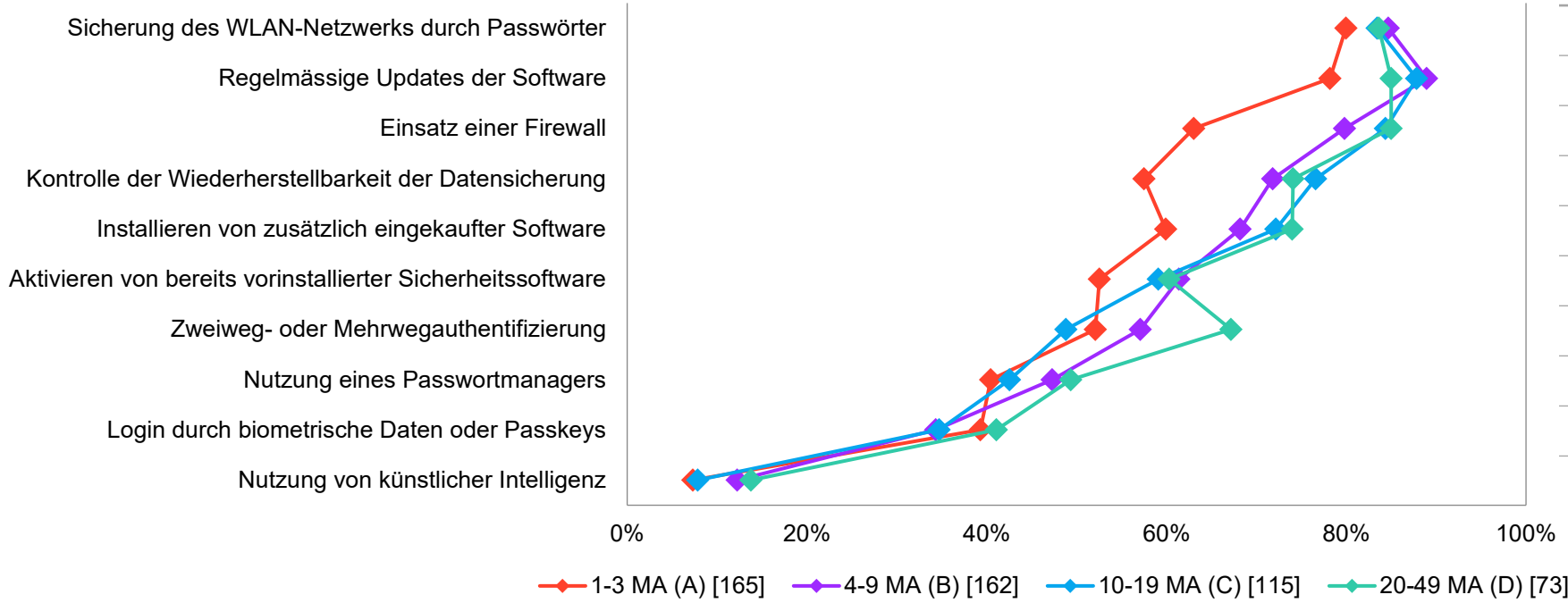


F012: Inwieweit sind die folgenden technischen Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?
Basis: n=515 | Filter: KMU | Skalierte Frage: 1= gar nicht bis 5= voll und ganz

Technische Massnahmenumsetzung (2/5)

Unternehmen mit 1-3 Mitarbeitenden haben bei fast allen Massnahmen die tiefsten Umsetzungsgrade. Unternehmen mit 4-9, 10-19 bzw. 20-49 Mitarbeitenden unterscheiden sich nur wenig voneinander. Ein „Ausreisser“ ist die Zwei-/Mehrwegauthentifizierung, die v.a. von Firmen mit 20-49 Mitarbeitenden umgesetzt ist.

Nach Anzahl Mitarbeitenden



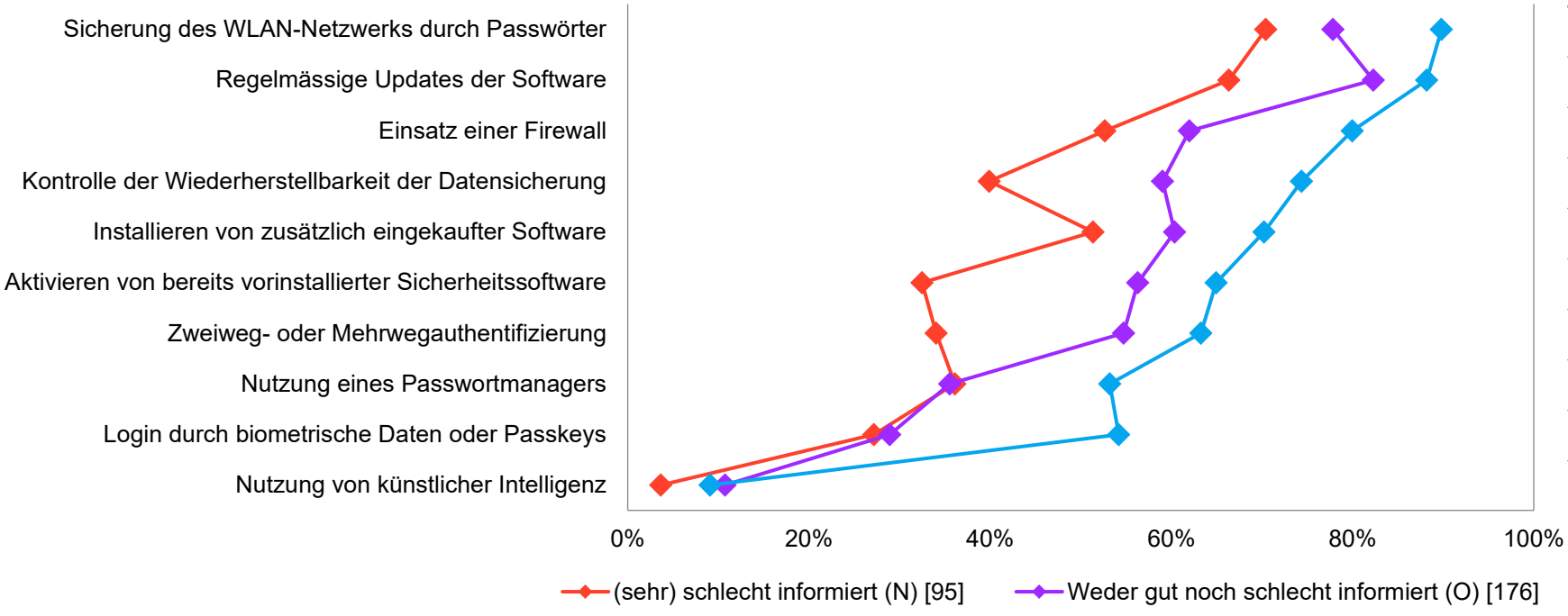
	Mittelwert			
	1-3 MA	4-9 MA	10-19 MA	20-49 MA
Sicherung des WLAN-Netzwerks durch Passwörter	4.4	4.6	4.5	4.6
Regelmässige Updates der Software	4.3	4.6 A	4.6 A	4.6
Einsatz einer Firewall	3.9	4.5 A	4.6 A	4.8 A
Kontrolle der Wiederherstellbarkeit der Datensicherung	3.8	4.2 A	4.4 A	4.4 A
Installieren von zusätzlich eingekaufter Software	3.7	4.1 A	4.3 A	4.3 A
Aktivieren von bereits vorinstallierter Sicherheitssoftware	3.5	4.0 A	4.0 A	4.2 A
Zweiweg- oder Mehrwegauthentifizierung	3.5	3.7	3.6	4.0 AC
Nutzung eines Passwortmanagers	3.0	3.3	3.2	3.6 A
Login durch biometrische Daten oder Passkeys	2.9	2.8	2.7	3.1
Nutzung von künstlicher Intelligenz	1.7	2.0 A	1.8	2.3 AC

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 (3/5)

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

Nach Informationsgrad



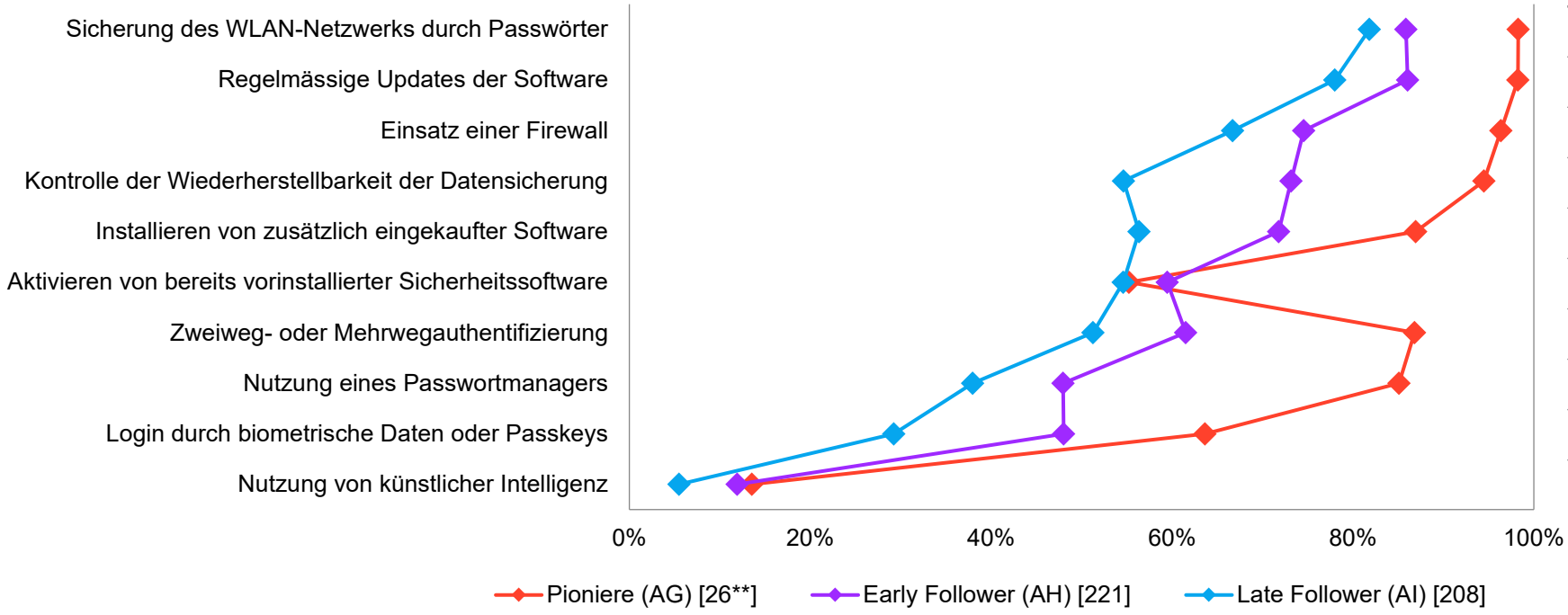
Mittelwert Informationsgrad		
Eher/sehr schlecht	Weder gut noch schlecht	Eher/ sehr gut
4.3	4.4	4.6 NO
4.1	4.3	4.6 NO
3.6	3.9	4.4 NO
3.4	3.8	4.2 NO
3.5	3.8	4.0
3.1	3.7 N	3.8 N
2.9	3.6 N	3.8 N
2.7	3.0	3.4 N
2.5	2.7	3.2 NO
1.4	1.9 N	1.8

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 (4/5)

Je offener die Befragten gegenüber technischen Innovationen sind, desto höher ist der Massnahmen-Umsetzungsgrad. Ein auffälliger Ausreisser ist das Aktivieren von bereits vorinstallierter Sicherheitssoftware, was auch von den Pionieren eher selten umgesetzt wird.

Nach Einstellung



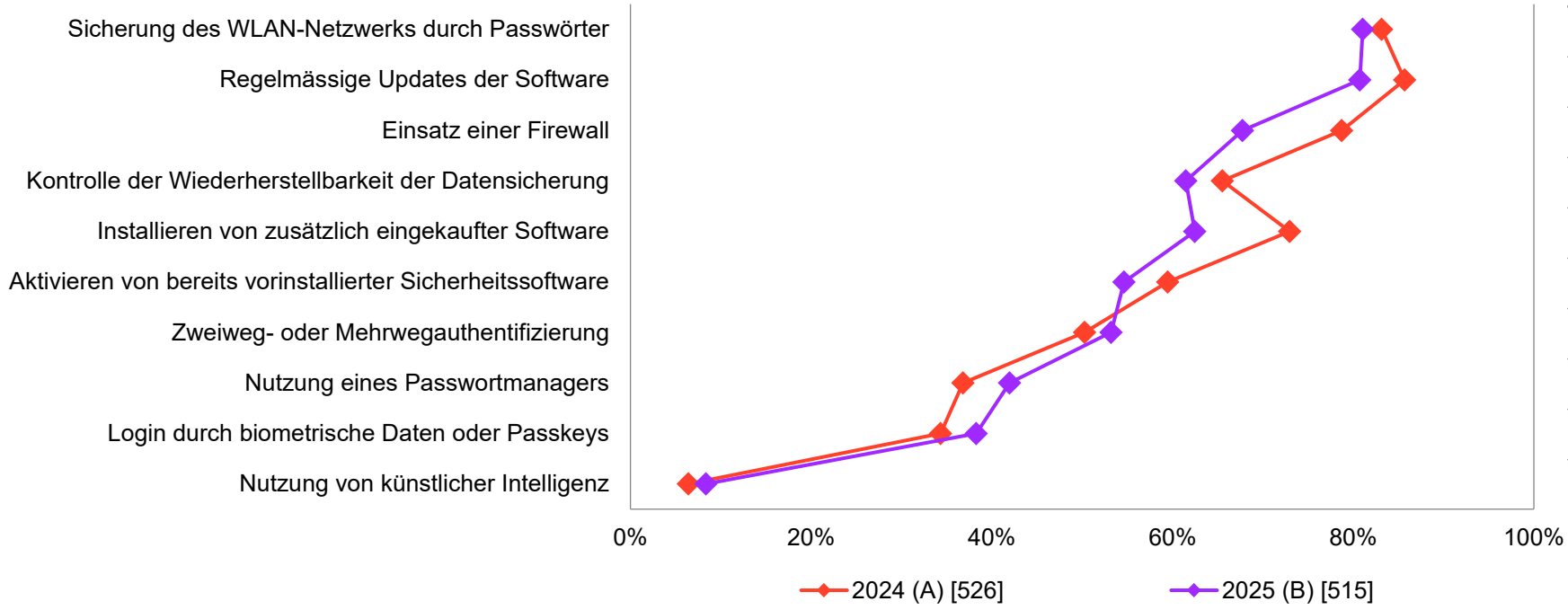
	Mittelwert	
Pioniere	Early Follower	Late Follower
4.9	4.6	4.5
4.9	4.6 AI	4.2
4.7	4.2	4.0
4.6	4.1 AI	3.7
4.4	4.1 AI	3.7
4.0	3.9	3.6
4.2	3.7	3.4
4.5	3.4 AI	2.8
3.9	3.2 AI	2.5
2.1	1.9 AI	1.6

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 | **Sehr kleine Basis <30
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 (5/5)

Die Umsetzung von sechs von zehn Massnahmen wurde 2024 höher eingeschätzt als 2025. Massnahmen mit generell tiefem Umsetzungsgrad erhalten 2025 eine etwas höhere Einschätzung als 2024, insbesondere der Passwortmanager und Logins mit biometrischen Daten/Passkeys.

Jahresvergleich

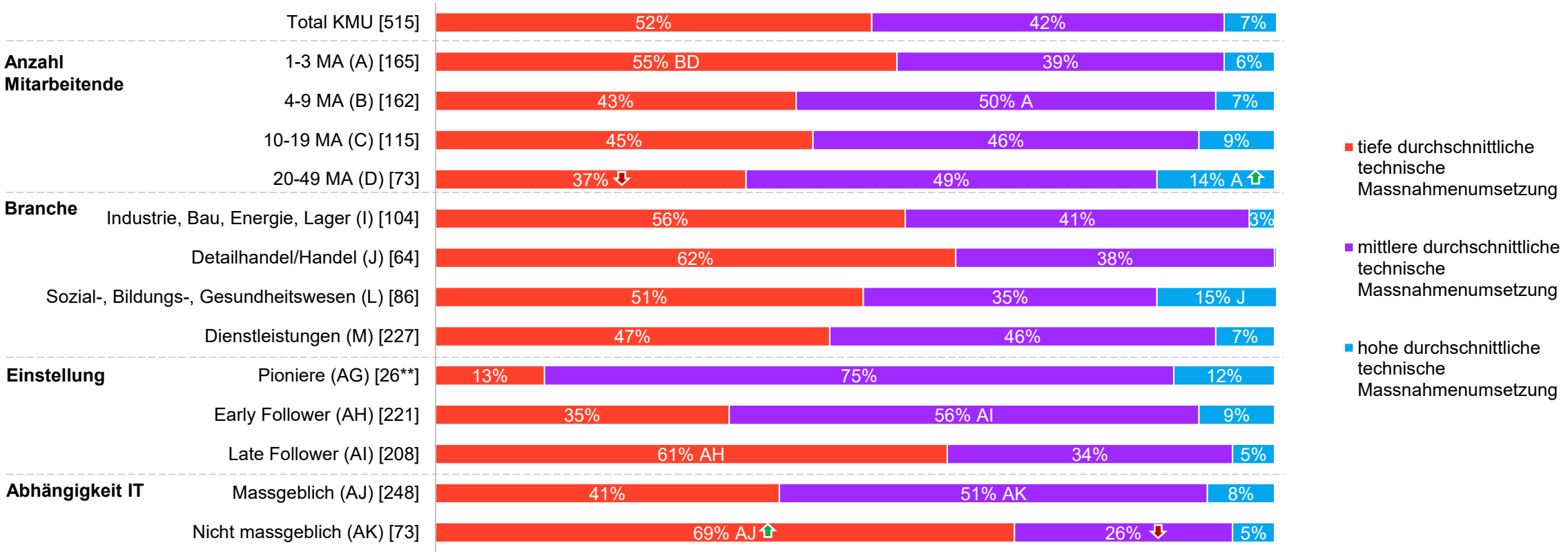


	Mittelwert	
	2024	2025
Sicherung des WLAN-Netzwerks durch Passwörter	4.5	4.5
Regelmässige Updates der Software	4.5	4.4
Einsatz einer Firewall	4.4 B	4.1
Kontrolle der Wiederherstellbarkeit der Datensicherung	4.0	3.9
Installieren von zusätzlich eingekaufter Software	4.1 B	3.8
Aktivieren von bereits vorinstallierter Sicherheitssoftware	3.9	3.7
Zweiweg- oder Mehrwegauthentifizierung	3.6	3.5
Nutzung eines Passwortmanagers	2.8	3.1
Login durch biometrische Daten oder Passkeys	2.8	2.9
Nutzung von künstlicher Intelligenz	1.6	1.7

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
Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Subgruppenvergleich zum Umsetzungsgrad technischer Massnahmen

7% der Unternehmen erreichen eine hohe technische Massnahmenumsetzung. Nur Unternehmen mit 20 bis 49 Mitarbeitenden erreichen dies signifikant häufiger (14%).

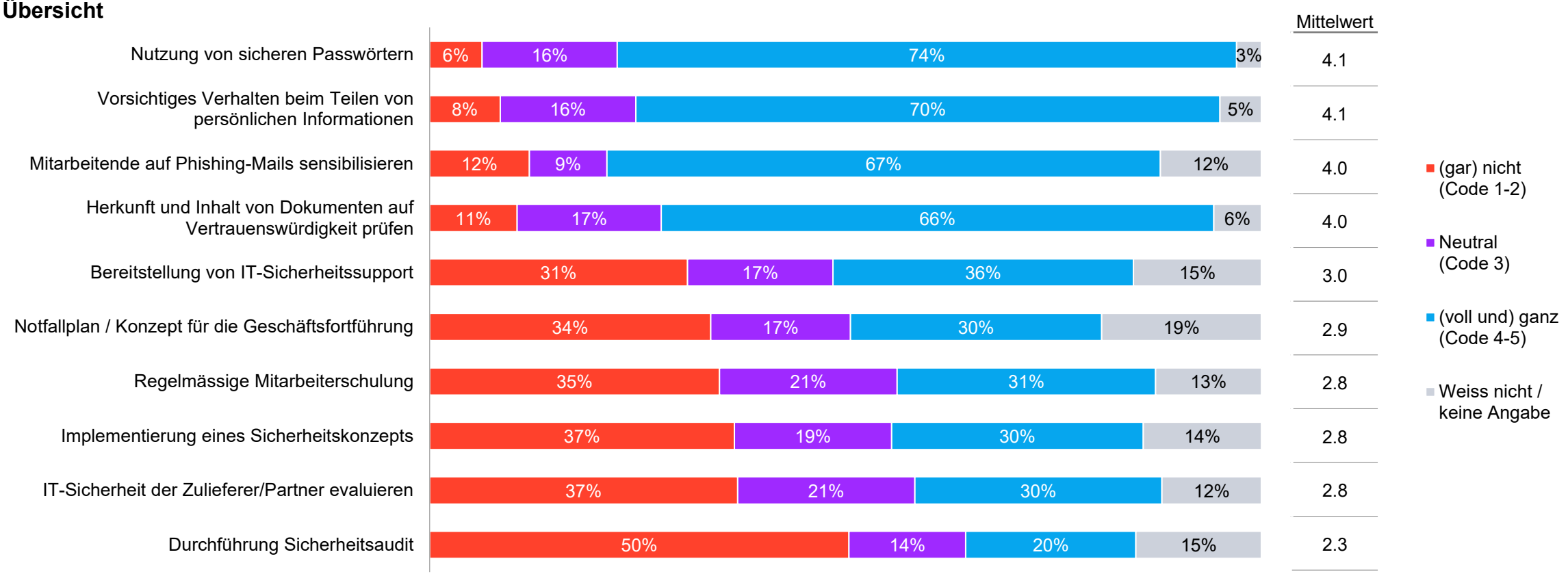


F013: Inwieweit sind die folgenden organisatorischen Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?
Basis: n=515 | Filter: KMU | Skalierte Frage 1-5 | „tief“ = Mittelwert aller Massnahmen <=3.49, „mittel“ = Mittelwert aller Massnahmen >=3.5 und <=4.49, „hoch“ = Mittelwert aller Massnahmen >= 4.5
⬆ signifikant höher als Total; ⬇ signifikant tiefer als Total | **Sehr kleine Basis <30 | 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.

Organisatorische Massnahmenumsetzung (1/5)

Organisatorische Massnahmen werden grundsätzlich weniger umgesetzt als technische. 4 von 10 Massnahmen wurden von mind. zwei Dritteln der Befragten (voll und ganz) umgesetzt, 5 von 10 Massnahmen nur von rund einem Drittel. Die Massnahme „Durchführung von Sicherheitsaudits“ wurde nur von einem Fünftel (voll und ganz) umgesetzt.

Übersicht

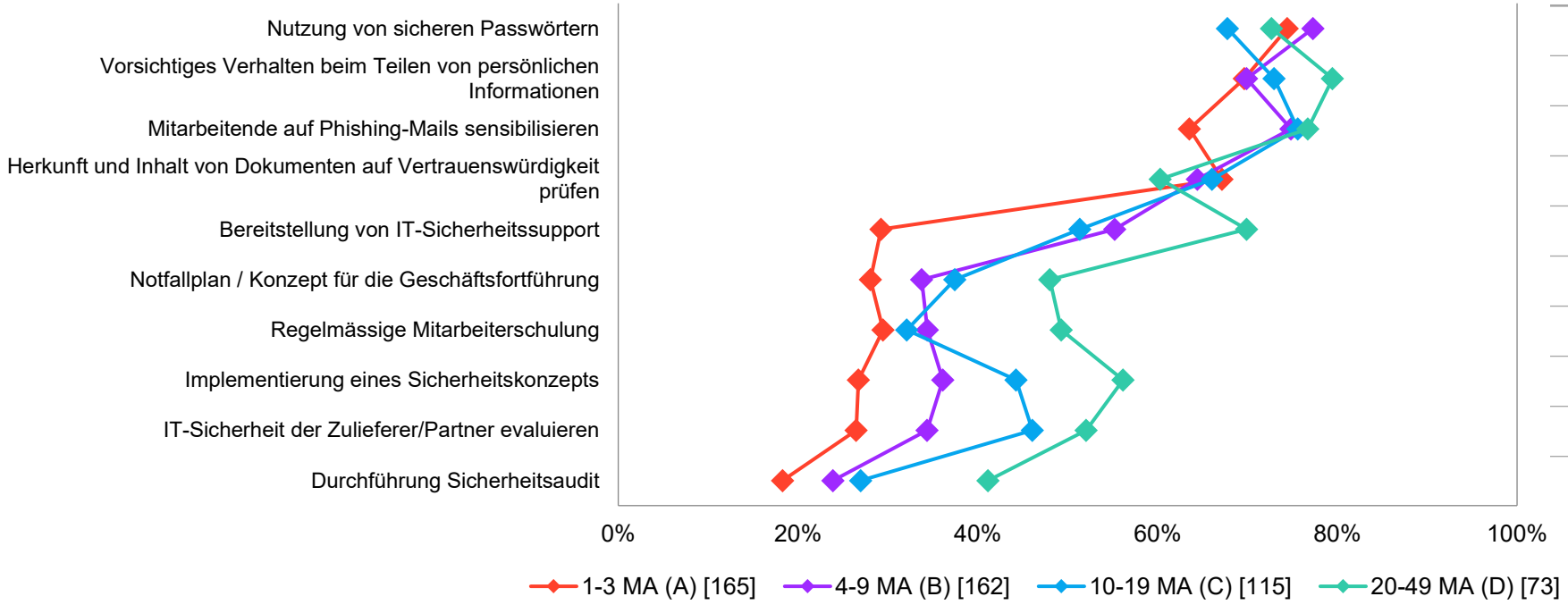


F013: Inwieweit sind die folgenden organisatorischen Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?
Basis: n=515 | Filter: KMU | Skalierte Frage: 1= gar nicht bis 5= voll und ganz

Organisatorische Massnahmenumsetzung (2/5)

Bei den 4 Massnahmen mit den höchsten Umsetzungsgraden unterscheiden sich die verschieden grossen Unternehmen nur wenig. Bei Massnahmen mit tieferem Umsetzungsgrad hingegen gilt: Je mehr Mitarbeitende, desto höher der Umsetzungsgrad, in vielen Fällen mit signifikanten Unterschieden.

Nach Anzahl Mitarbeitenden



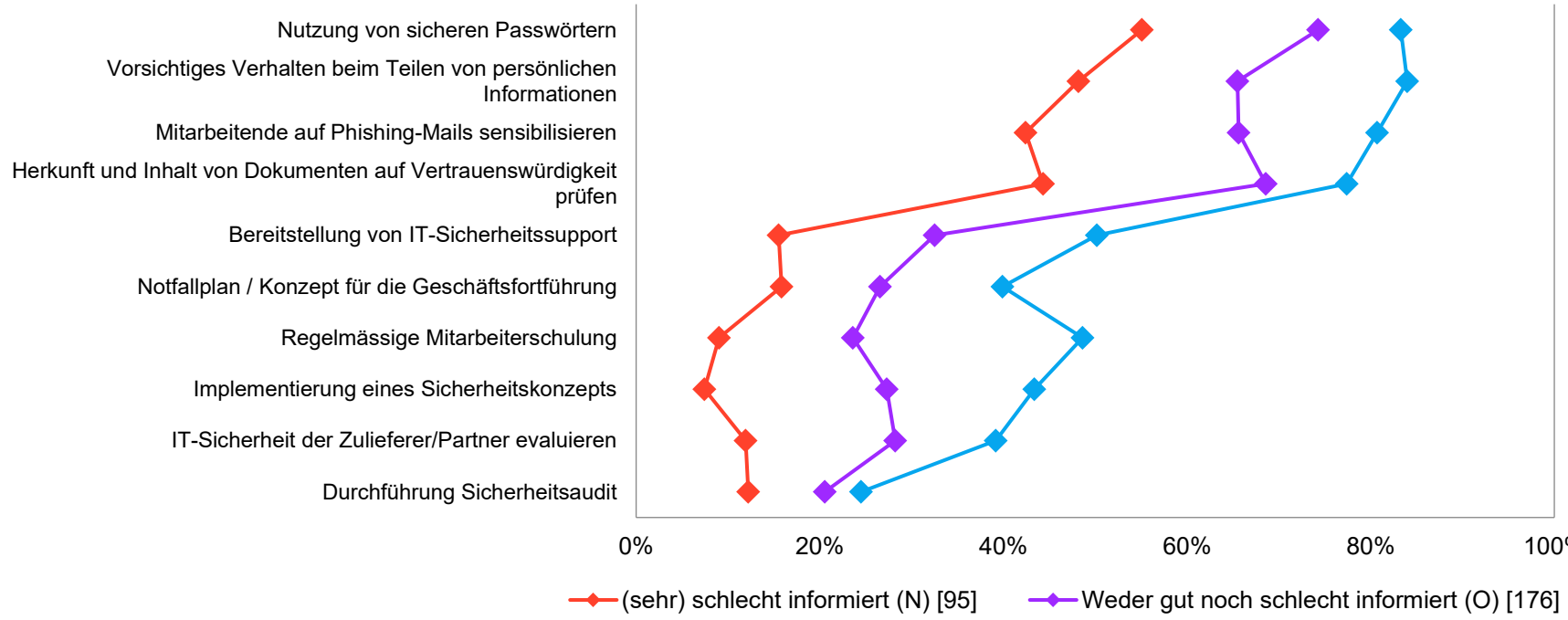
	Mittelwert			
	1-3 MA	4-9 MA	10-19 MA	20-49 MA
Nutzung von sicheren Passwörtern	4.1	4.2 C	4.0	4.1
Vorsichtiges Verhalten beim Teilen von persönlichen Informationen	4.1	4.0	4.1	4.1
Mitarbeitende auf Phishing-Mails sensibilisieren	4.0	4.1	4.2	4.3
Herkunft und Inhalt von Dokumenten auf Vertrauenswürdigkeit prüfen	4.0	3.9	4.0	3.8
Bereitstellung von IT-Sicherheitssupport	2.8	3.6 A	3.7 A	4.0 AB
Notfallplan / Konzept für die Geschäftsfortführung	2.8	3.0	3.2 A	3.7 ABC
Regelmässige Mitarbeiterschulung	2.8	2.9	3.0	3.4 ABC
Implementierung eines Sicherheitskonzepts	2.7	3.0 A	3.3 A	3.7 ABC
IT-Sicherheit der Zulieferer/Partner evaluieren	2.7	3.0	3.4 AB	3.7 AB
Durchführung Sicherheitsaudit	2.2	2.5	2.7 A	3.5 ABC

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 (3/5)

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

Nach Informationsgrad



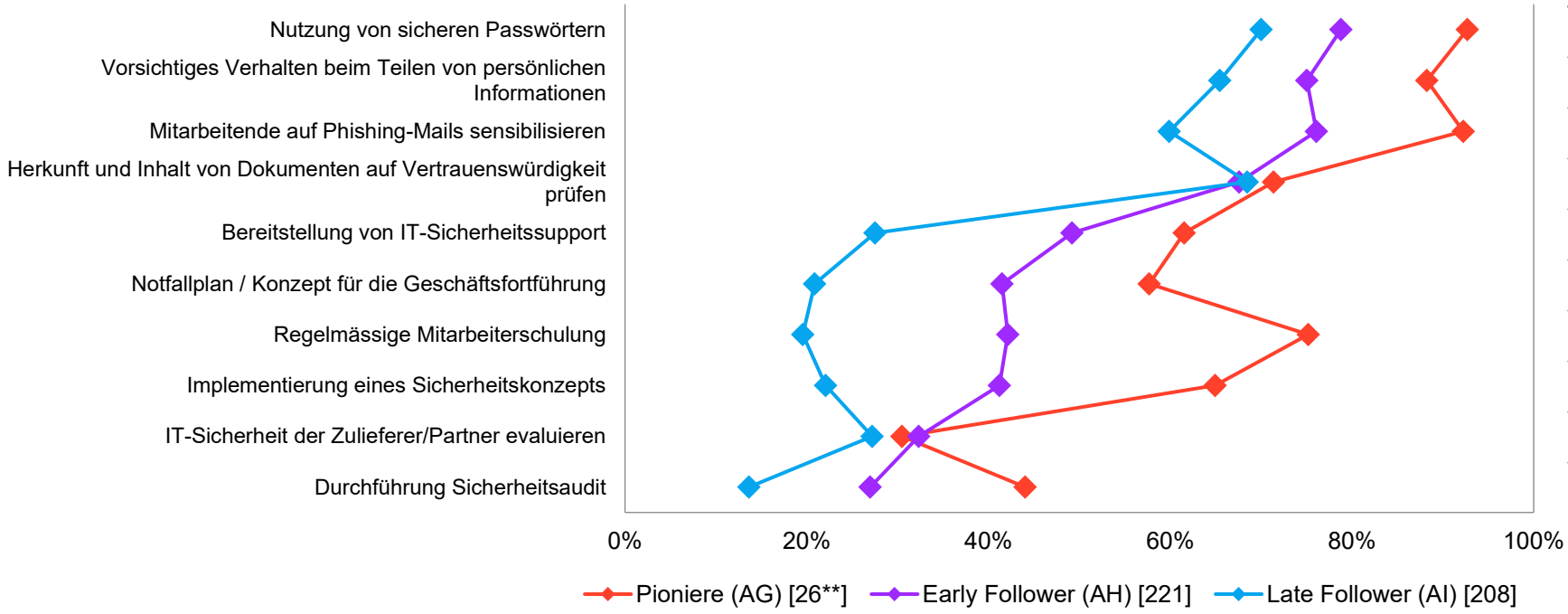
	Mittelwert Informationsgrad		
	Eher/sehr schlecht	Weder gut noch schlecht	Eher/ sehr gut
Nutzung von sicheren Passwörtern	3.7	4.0	4.4 NO
Vorsichtiges Verhalten beim Teilen von persönlichen Informationen	3.5	3.9 N	4.4 NO
Mitarbeitende auf Phishing-Mails sensibilisieren	3.3	3.9 N	4.5 NO
Herkunft und Inhalt von Dokumenten auf Vertrauenswürdigkeit prüfen	3.3	4.0 N	4.3 NO
Bereitstellung von IT-Sicherheitssupport	2.3	2.9 N	3.4 NO
Notfallplan / Konzept für die Geschäftsfortführung	2.4	2.6	3.2 NO
Regelmässige Mitarbeiterschulung	2.0	2.6 N	3.4 NO
Implementierung eines Sicherheitskonzepts	1.9	2.7 N	3.3 NO
IT-Sicherheit der Zulieferer/Partner evaluieren	2.1	2.8 N	3.1 N
Durchführung Sicherheitsaudit	1.7	2.3 N	2.5 N

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 (4/5)

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

Nach Einstellung



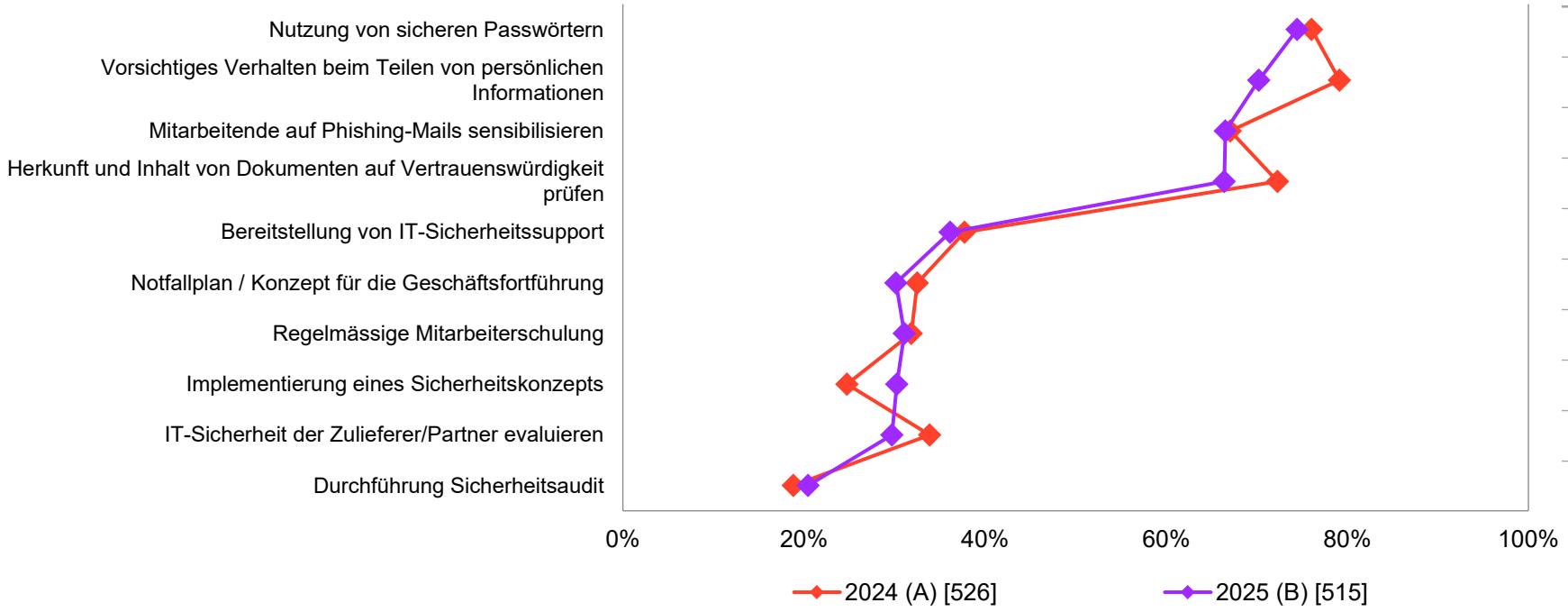
	Mittelwert		
	Pioniere	Early Follower	Late Follower
Nutzung von sicheren Passwörtern	4.5	4.2	4.0
Vorsichtiges Verhalten beim Teilen von persönlichen Informationen	4.4	4.2	3.9
Mitarbeitende auf Phishing-Mails sensibilisieren	4.6	4.3 AI	3.7
Herkunft und Inhalt von Dokumenten auf Vertrauenswürdigkeit prüfen	4.5	4.0	3.9
Bereitstellung von IT-Sicherheitssupport	4.2	3.4 AI	2.7
Notfallplan / Konzept für die Geschäftsfortführung	3.9	3.2 AI	2.4
Regelmässige Mitarbeiterschulung	3.9	3.3 AI	2.3
Implementierung eines Sicherheitskonzepts	4.0	3.2 AI	2.5
IT-Sicherheit der Zulieferer/Partner evaluieren	3.5	2.9	2.5
Durchführung Sicherheitsaudit	3.3	2.5 AI	2.0

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 | **Sehr kleine Basis <30
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 (5/5)

Der Jahresvergleich zeigt fast gar keine Unterschiede. Die Vorsicht beim Teilen von persönlichen Informationen wurde 2024 als signifikant besser umgesetzt beurteilt: Entweder wurden hier tatsächlich Massnahmen umgesetzt, oder aber die Ansprüche sind gestiegen.

Jahresvergleich

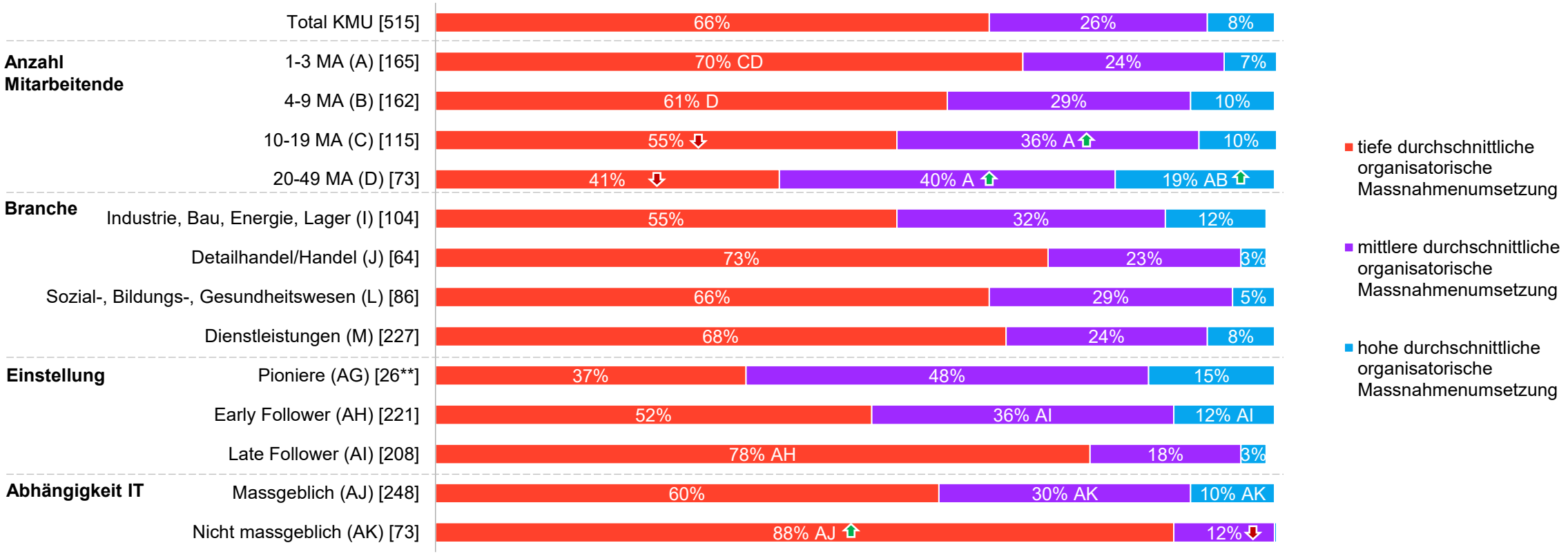


	Mittelwert	
	2024	2025
Nutzung von sicheren Passwörtern	4.2	4.1
Vorsichtiges Verhalten beim Teilen von persönlichen Informationen	4.3 B	4.1
Mitarbeitende auf Phishing-Mails sensibilisieren	4.0	4.0
Herkunft und Inhalt von Dokumenten auf Vertrauenswürdigkeit prüfen	4.0	4.0
Bereitstellung von IT-Sicherheitssupport	2.9	3.0
Notfallplan / Konzept für die Geschäftsfortführung	2.8	2.9
Regelmässige Mitarbeiterschulung	2.9	2.8
Implementierung eines Sicherheitskonzepts	2.6	2.8
IT-Sicherheit der Zulieferer/Partner evaluieren	2.9	2.8
Durchführung Sicherheitsaudit	2.2	2.3

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
Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Subgruppenvergleich zum Umsetzungsgrad organisatorischer Massnahmen

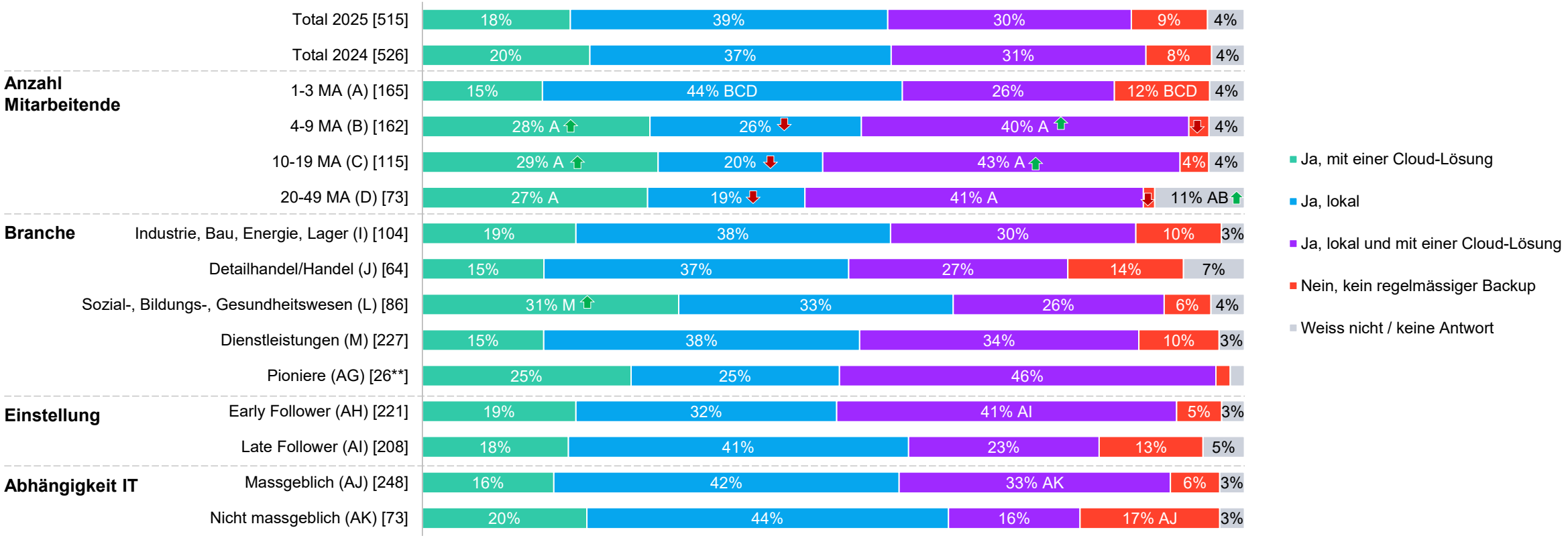
8% der Unternehmen erreichen eine hohe organisatorische Massnahmenumsetzung. Nur Unternehmen mit 20 bis 49 Mitarbeitenden erreichen dies signifikant häufiger (19%).



F013: Inwieweit sind die folgenden organisatorischen Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?
Basis: n=515 | Filter: KMU | Skalierte Frage 1-5 | „tief“ = Mittelwert aller Massnahmen <=3.49, „mittel“ = Mittelwert aller Massnahmen >=3.5 und <=4.49, „hoch“ = Mittelwert aller Massnahmen >= 4.5
⬆ signifikant höher als Total; ⬇ signifikant tiefer als Total | **Sehr kleine Basis <30 | 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.

Backup mit/ohne Cloud

Fast 9 von 10 Unternehmen führen regelmässige Daten-Backups durch, dieser Wert ist praktisch unverändert zu 2024. Am ehesten verzichten Unternehmen mit 1-3 Mitarbeitenden (12%), Firmen aus dem Detailhandel/Handel (14%), Late Follower (13%) und Unternehmen, die nicht massgeblich von der IT abhängig sind (17%) darauf.

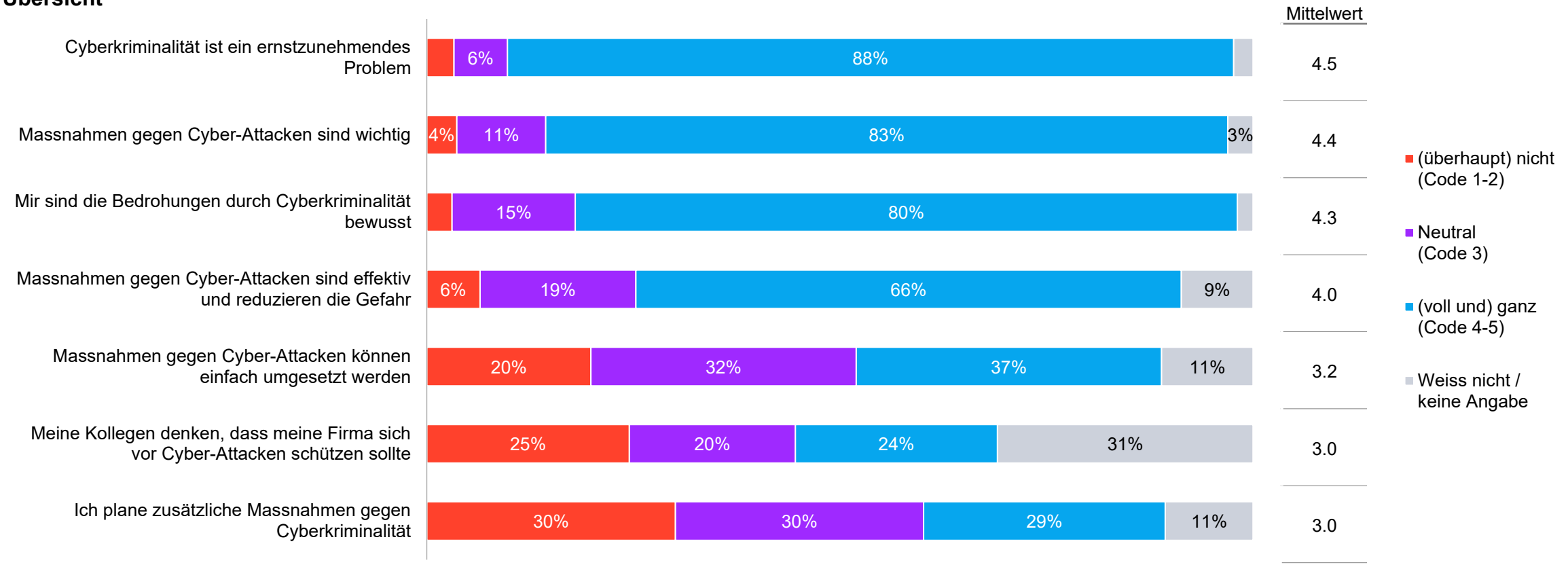


F014: Wird in Ihrem Unternehmen regelmässig ein Backup der Daten durchgeführt?
Basis: n=[ ] | Filter: KMU | Geschlossene Frage | ⬆ signifikant höher als Total; ⬇ signifikant tiefer als Total | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle | **Sehr kleine Basis <30 | Datenbeschriftung 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 (1/7)

Fast 9 von 10 Befragten stimmen (voll und ganz) zu, dass Cyberkriminalität ein ernstzunehmendes Problem ist. Hingegen spürt nur knapp ein Viertel einen sozialen Druck für Schutzmassnahmen und weniger als ein Drittel plant zusätzliche Massnahmen.

Übersicht

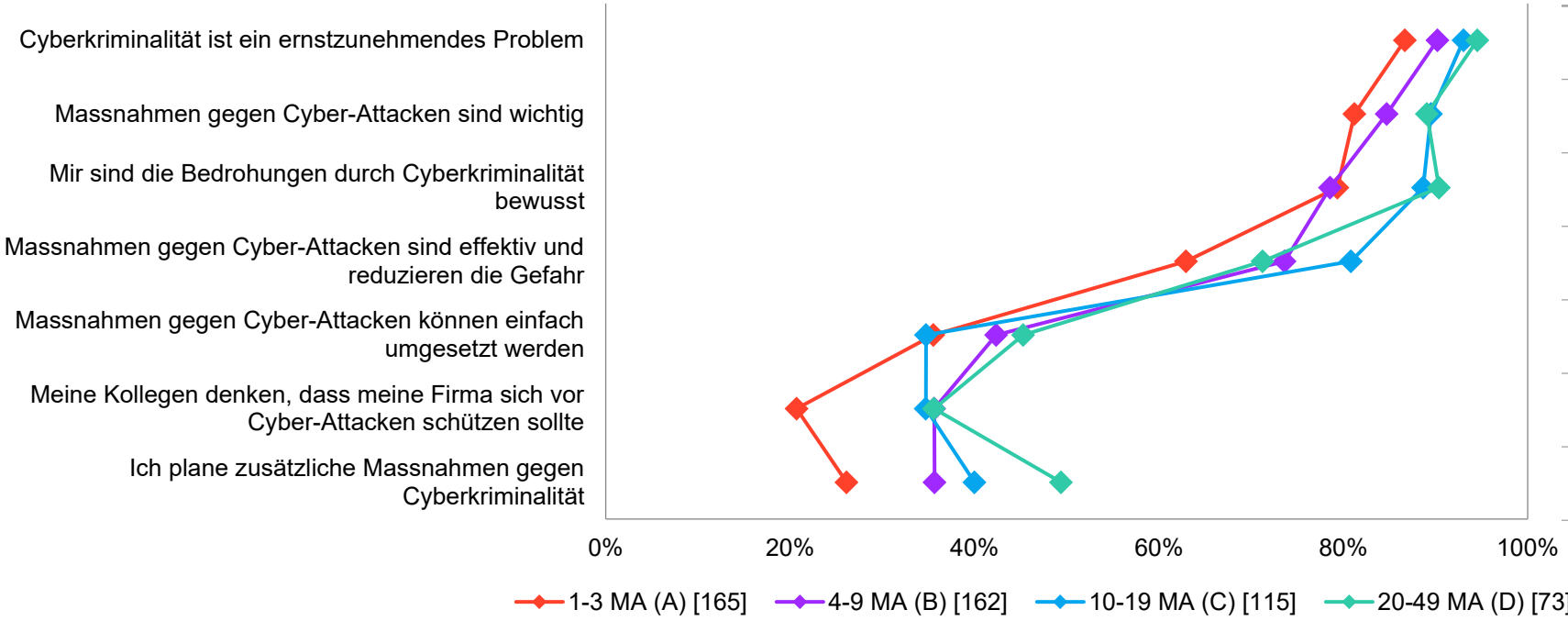


F015: Inwiefern stimmen Sie den folgenden Aussagen zu Cyberkriminalität wie Malware, Online-Betrug und Hacking zu?
Basis: n=515 | Filter: KMU | Skalierte Frage: 1= überhaupt nicht bis 5= voll und ganz | Datenbeschriftung ab 3%

Einstellung zu Cyberkriminalität (2/7)

Die verschieden grossen Unternehmen beurteilen die sieben Einstellungen sehr ähnlich. Am ehesten heben sich die kleinsten Unternehmen mit 1-3 Mitarbeitenden ab, welche am wenigsten sozialen Druck für höheren Schutz verspüren und am wenigsten zusätzliche Massnahmen planen.

Nach Anzahl Mitarbeitenden



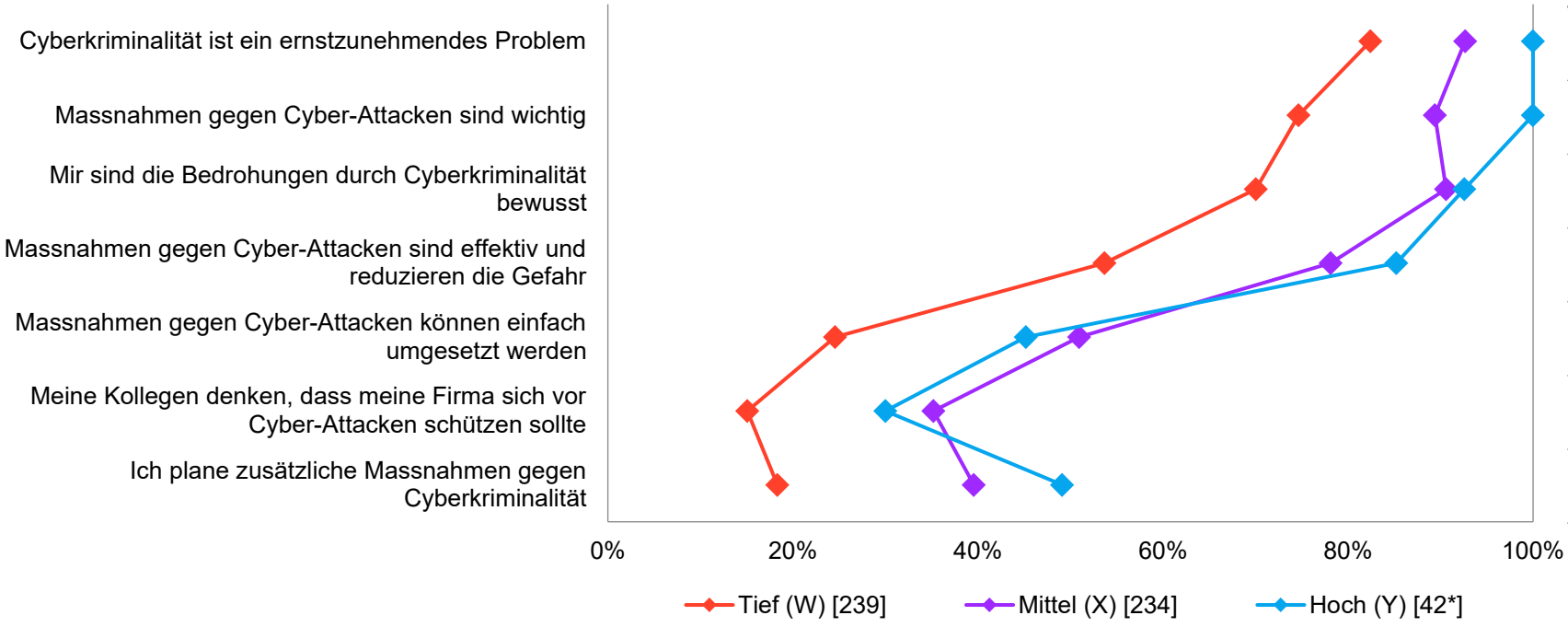
	Mittelwert			
	1-3 MA	4-9 MA	10-19 MA	20-49 MA
Cyberkriminalität ist ein ernstzunehmendes Problem	4.5	4.6	4.7 A	4.6
Massnahmen gegen Cyber-Attacken sind wichtig	4.3	4.5	4.6 A	4.6
Mir sind die Bedrohungen durch Cyberkriminalität bewusst	4.3	4.3	4.5 A	4.4
Massnahmen gegen Cyber-Attacken sind effektiv und reduzieren die Gefahr	4.0	4.1	4.1	4.1
Massnahmen gegen Cyber-Attacken können einfach umgesetzt werden	3.2	3.4 A	3.2	3.5
Meine Kollegen denken, dass meine Firma sich vor Cyber-Attacken schützen sollte	2.9	3.3 A	3.3	3.1
Ich plane zusätzliche Massnahmen gegen Cyberkriminalität	2.9	3.2 A	3.2 A	3.5 A

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 (4/7)

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



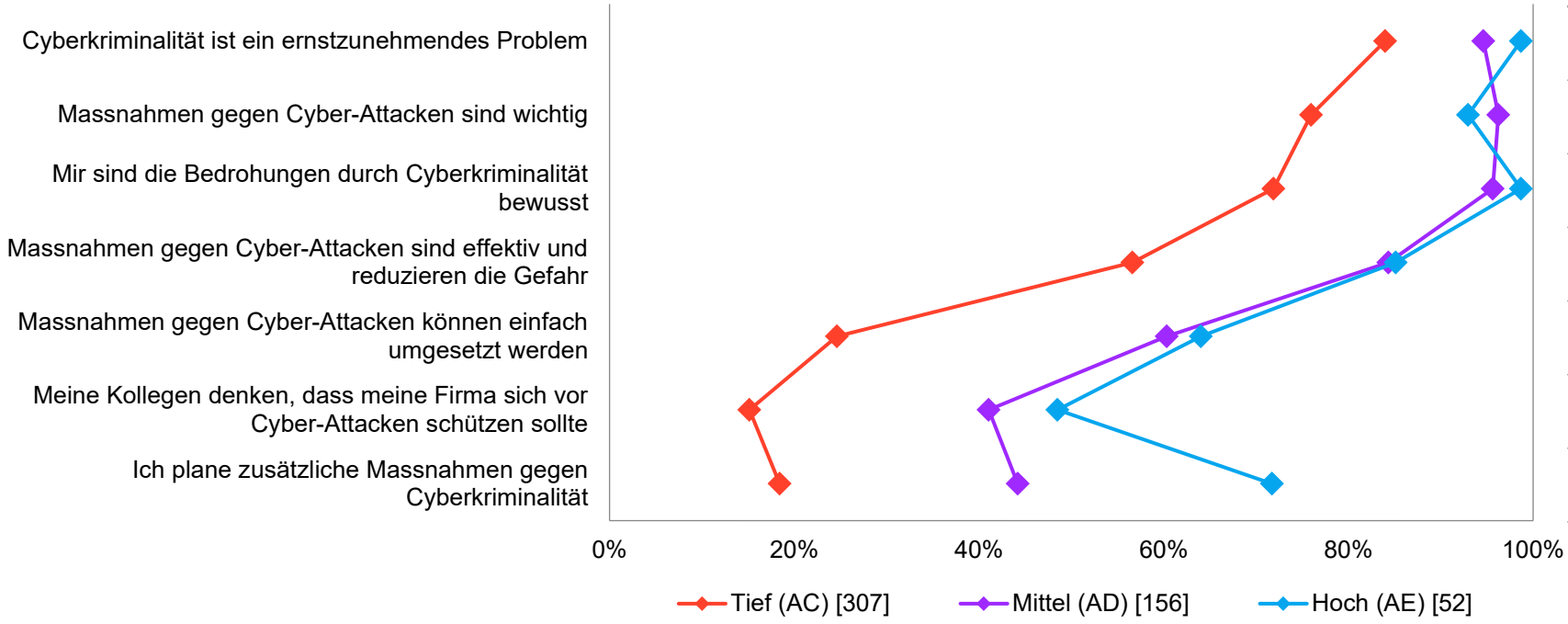
	Mittelwert		
	Tief	Mittel	Hoch
Cyberkriminalität ist ein ernstzunehmendes Problem	4.3	4.7 W	5.0
Massnahmen gegen Cyber-Attacken sind wichtig	4.2	4.5 W	4.9
Mir sind die Bedrohungen durch Cyberkriminalität bewusst	4.1	4.5 W	4.8
Massnahmen gegen Cyber-Attacken sind effektiv und reduzieren die Gefahr	3.8	4.2 W	4.6
Massnahmen gegen Cyber-Attacken können einfach umgesetzt werden	3.0	3.5 W	3.2
Meine Kollegen denken, dass meine Firma sich vor Cyber-Attacken schützen sollte	2.7	3.3 W	3.2
Ich plane zusätzliche Massnahmen gegen Cyberkriminalität	2.6	3.3 W	3.6

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.

Einstellung zu Cyberkriminalität (5/7)

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

Nach organisatorischer Massnahmenumsetzung



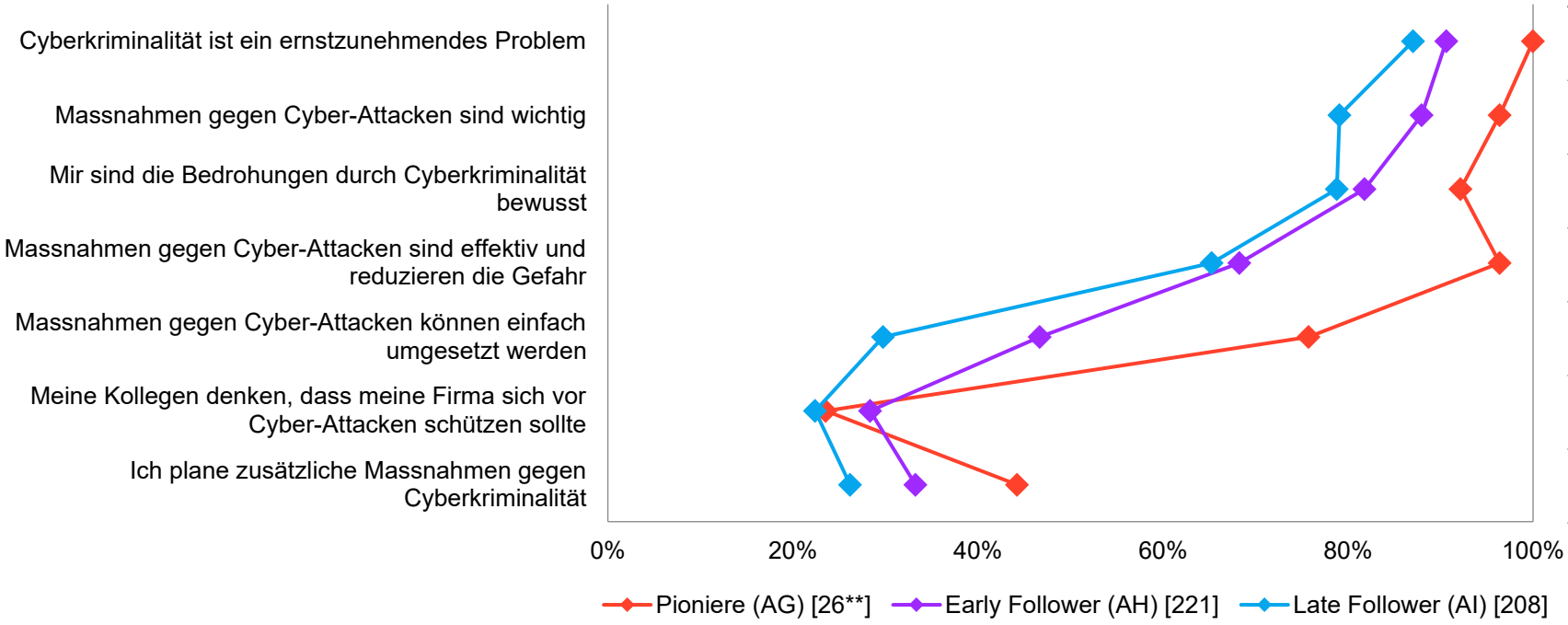
	Mittelwert	
Tief	Mittel	Hoch
4.4	4.8 AC	5.0
4.2	4.6 AC	4.9
4.1	4.7 AC	4.9
3.8	4.3 AC	4.7
3.0	3.6 AC	3.9
2.7	3.4 AC	3.7
2.6	3.5 AC	4.1

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 (6/7)

Pioniere stimmen allen Aussagen bis auf einer häufiger zu als Early und Late Follower – sozialen Druck zu mehr Schutz gegen Cyber-Attacken verspüren auch Pioniere eher selten.

Nach Einstellung



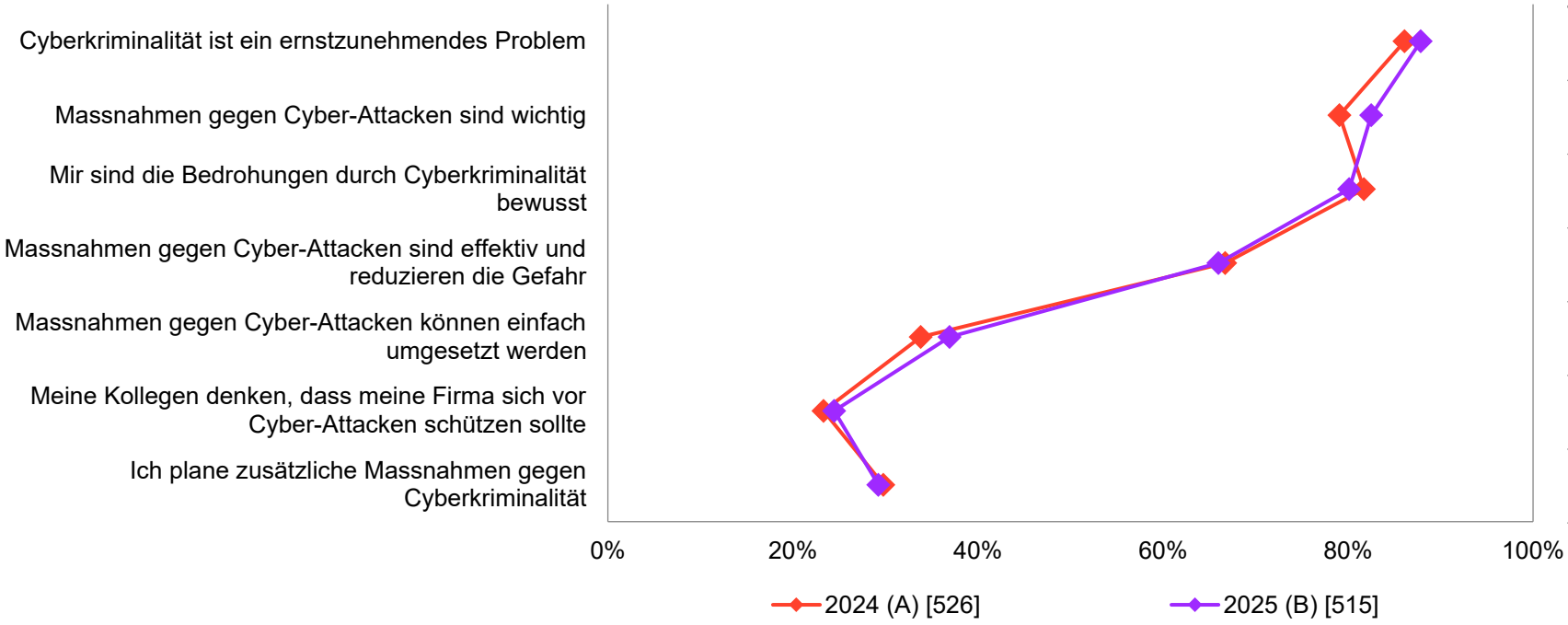
	Mittelwert		
	Pioniere	Early Follower	Late Follower
Cyberkriminalität ist ein ernstzunehmendes Problem	4.9	4.6	4.4
Massnahmen gegen Cyber-Attacken sind wichtig	4.8	4.5	4.3
Mir sind die Bedrohungen durch Cyberkriminalität bewusst	4.7	4.4	4.3
Massnahmen gegen Cyber-Attacken sind effektiv und reduzieren die Gefahr	4.5	4.0	3.9
Massnahmen gegen Cyber-Attacken können einfach umgesetzt werden	3.9	3.4 AI	3.0
Meine Kollegen denken, dass meine Firma sich vor Cyber-Attacken schützen sollte	3.0	3.1	2.9
Ich plane zusätzliche Massnahmen gegen Cyberkriminalität	3.4	3.1 AI	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 | **Sehr kleine Basis <30
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 (7/7)

Alle sieben Aussagen zu Cyberkriminalität werden 2025 nahezu identisch beurteilt wie 2024.

Jahresvergleich



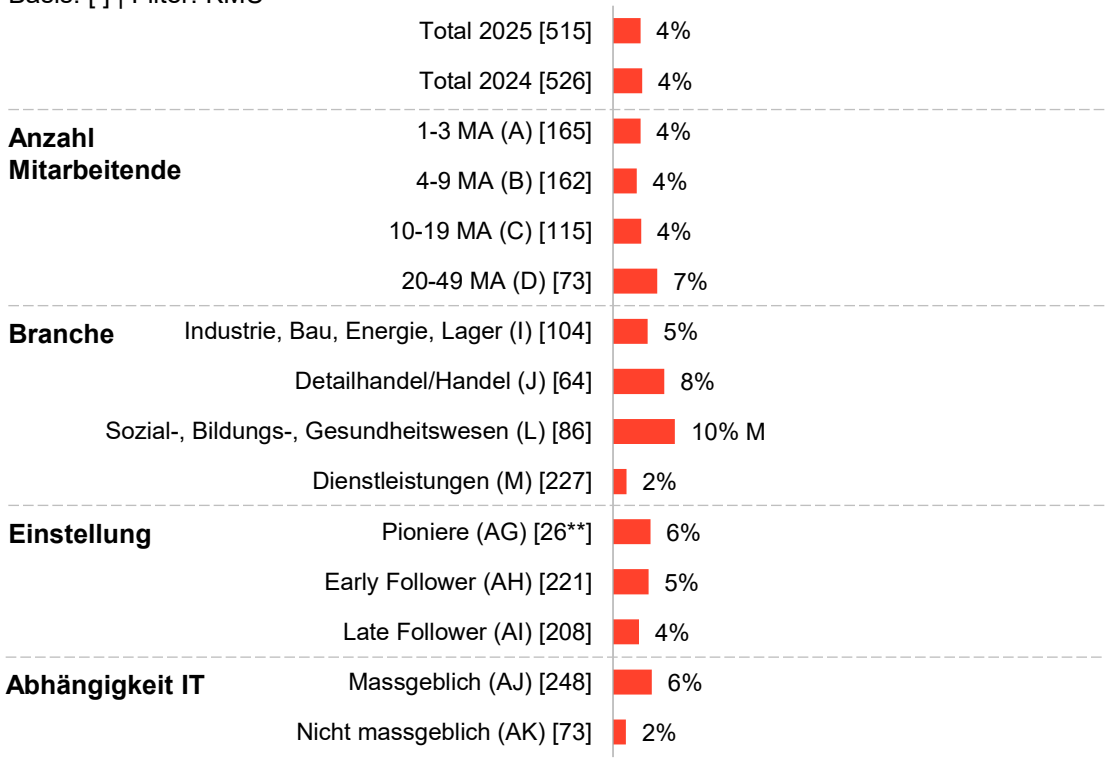
	Mittelwert	
	2024	2025
Cyberkriminalität ist ein ernstzunehmendes Problem	4.6	4.5
Massnahmen gegen Cyber-Attacken sind wichtig	4.4	4.4
Mir sind die Bedrohungen durch Cyberkriminalität bewusst	4.3	4.3
Massnahmen gegen Cyber-Attacken sind effektiv und reduzieren die Gefahr	4.0	4.0
Massnahmen gegen Cyber-Attacken können einfach umgesetzt werden	3.2	3.2
Meine Kollegen denken, dass meine Firma sich vor Cyber-Attacken schützen sollte	2.9	3.0
Ich plane zusätzliche Massnahmen gegen Cyberkriminalität	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
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 – gleich viele wie 2024. Bei fast allen davon erfolgte daraus entweder eine emotionale Belastung, ein finanzieller Schaden und/oder eine grosser Arbeitsaufwand. Kundendatenverluste oder Reputationsschäden entstanden sehr selten oder gar nicht.

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



Erlittene Schäden
Basis: n=23** | Filter: KMU – wenn Cyberangriff erlitten

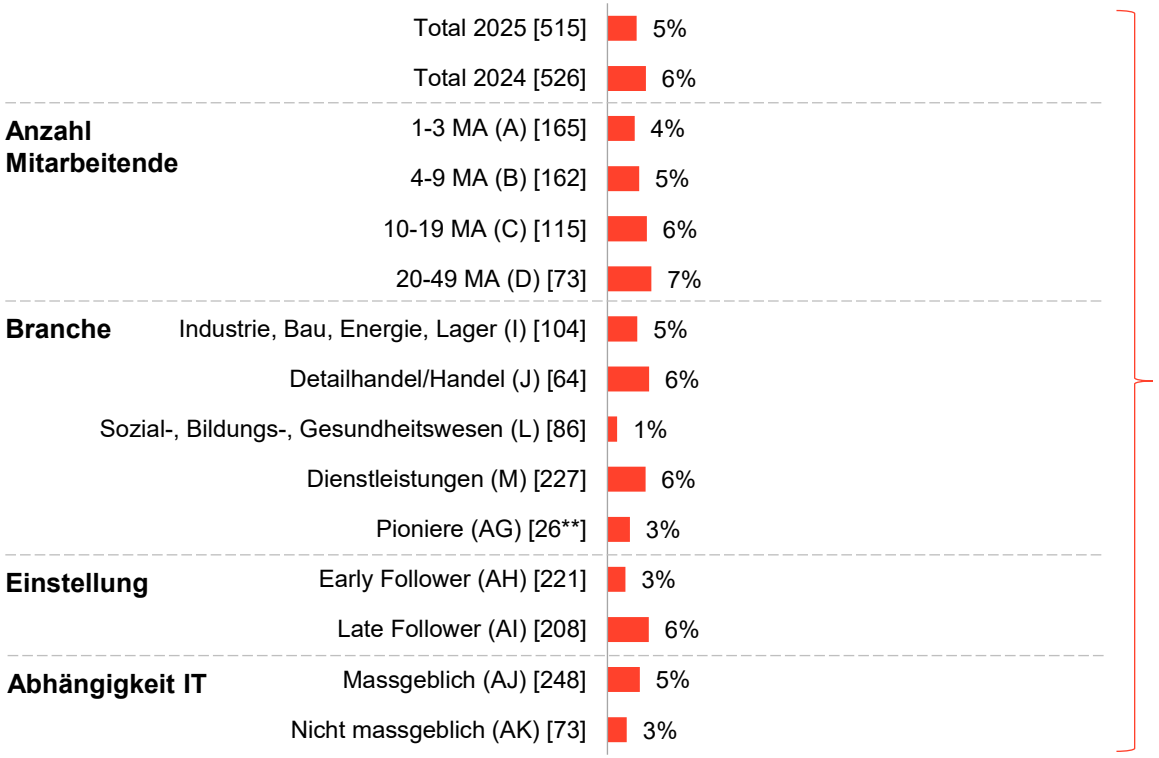
Schäden	Anzahl Fälle
Emotionale Belastung	14
Ein finanzieller Schaden	12
Ein grosser Arbeitsaufwand zur Behebung	10
Ein Kundendatenverlust	1
Ein Reputationsschaden	0
Nichts davon	1
Weiss nicht / keine Antwort	0

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; ⬇ signifikant tiefer als Total | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle
**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.

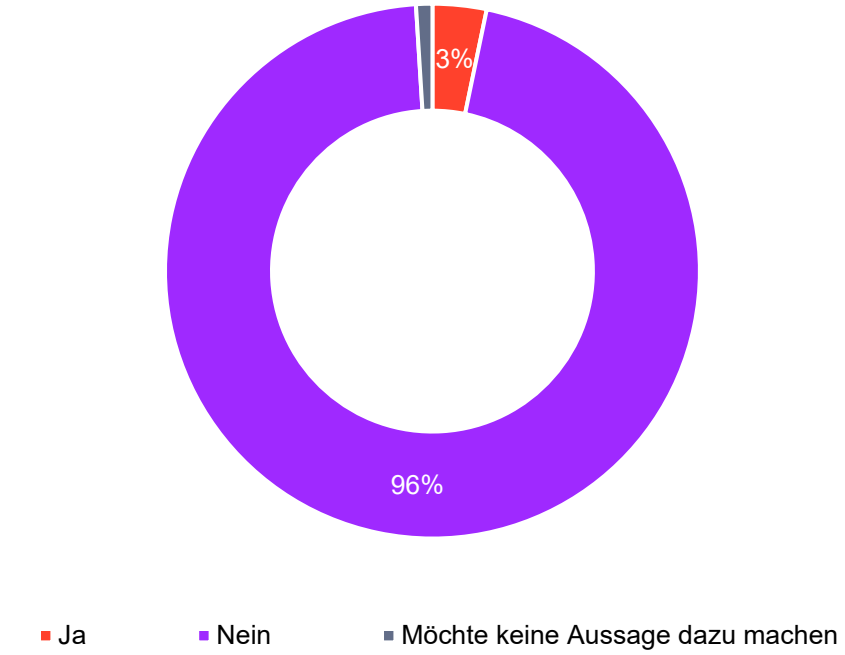
Erpressung

Fünf Prozent der befragten Unternehmen wurden schon einmal durch Cyberkriminelle erpresst; je grösser sie sind, desto eher wurden sie schon erpresst. Eines der insgesamt 23 erpressten Unternehmen hat schon einmal Lösegeld an Cyberkriminelle bezahlt.

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



Lösegeld an Cyberkriminelle
Basis: n=23** | Filter: durch Cyberkriminelle erpresste Befragte

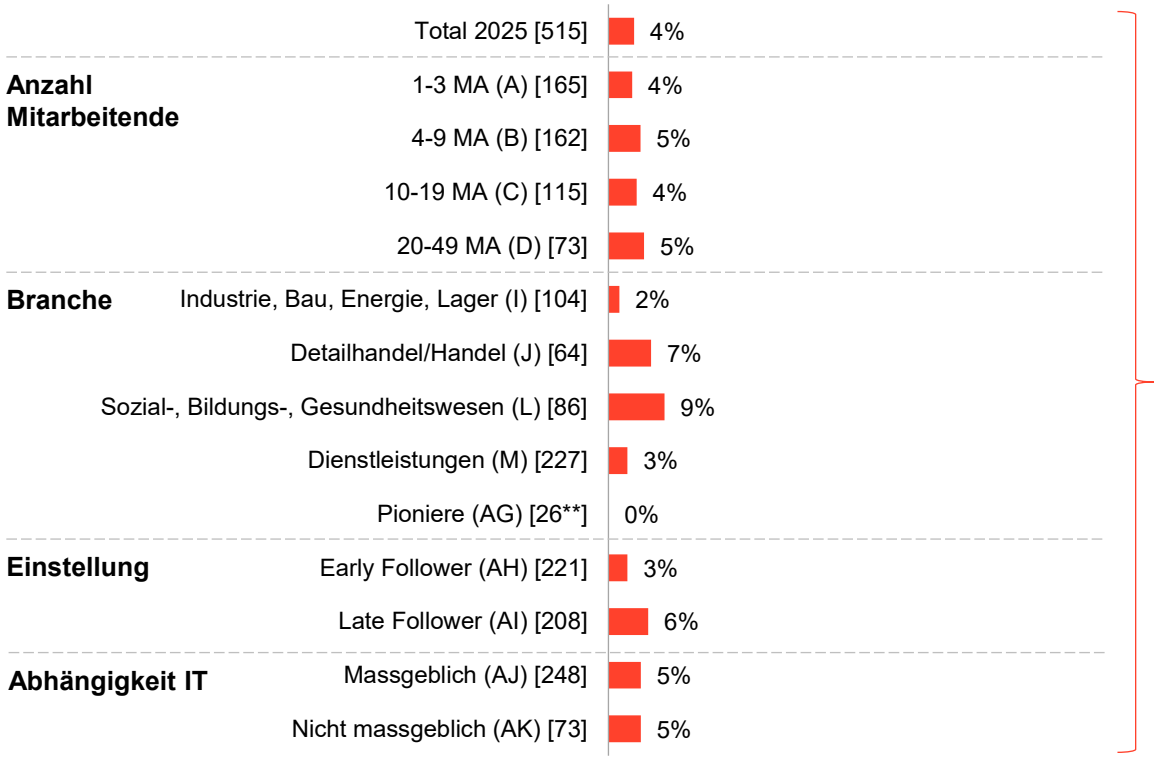


F019: Wurde Ihr Unternehmen schon einmal von Cyberkriminellen erpresst? | F020: Hat Ihr Unternehmen schon einmal Lösegeld an Cyberkriminelle bezahlt?
Basis: n=[ ] | Filter: siehe oben | Geschlossene Fragen | ⬆ signifikant höher als Total; ⬇ signifikant tiefer als Total | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle | Datenbeschriftung ab 3% | **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.

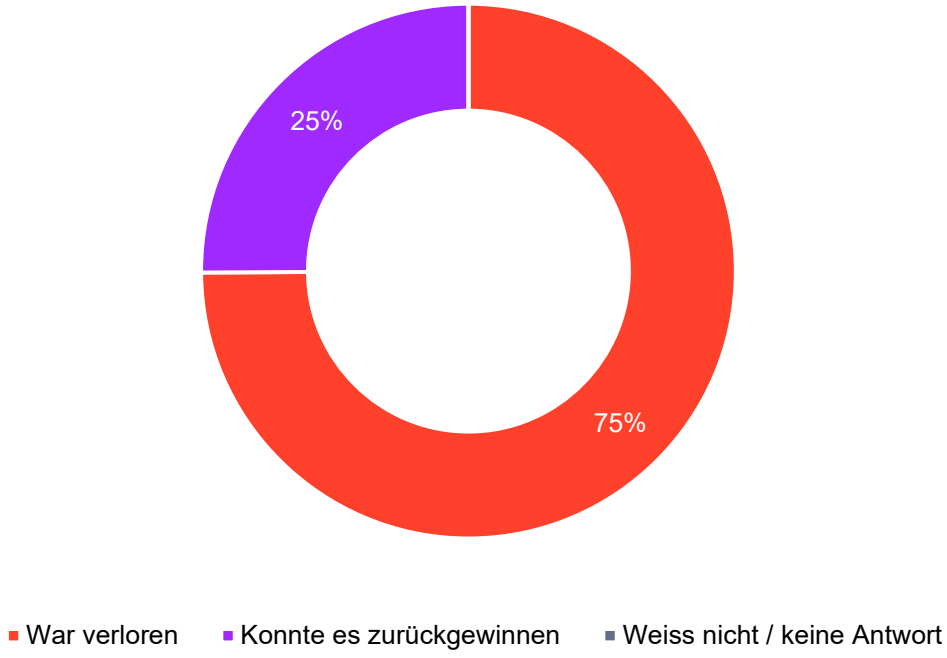
Geldeinzahlungen aufgrund betrügerischer Mails

4 Prozent der Befragten haben schon einmal irrtümlich Geld einbezahlt aufgrund betrügerischer E-Mails. Bei 15 der 20 betroffenen Unternehmen war das Geld danach verloren bzw. konnte nicht zurückgewonnen werden.

Betrügerische E-Mails (Ja-Anteile)
Basis: [ ] | Filter: KMU



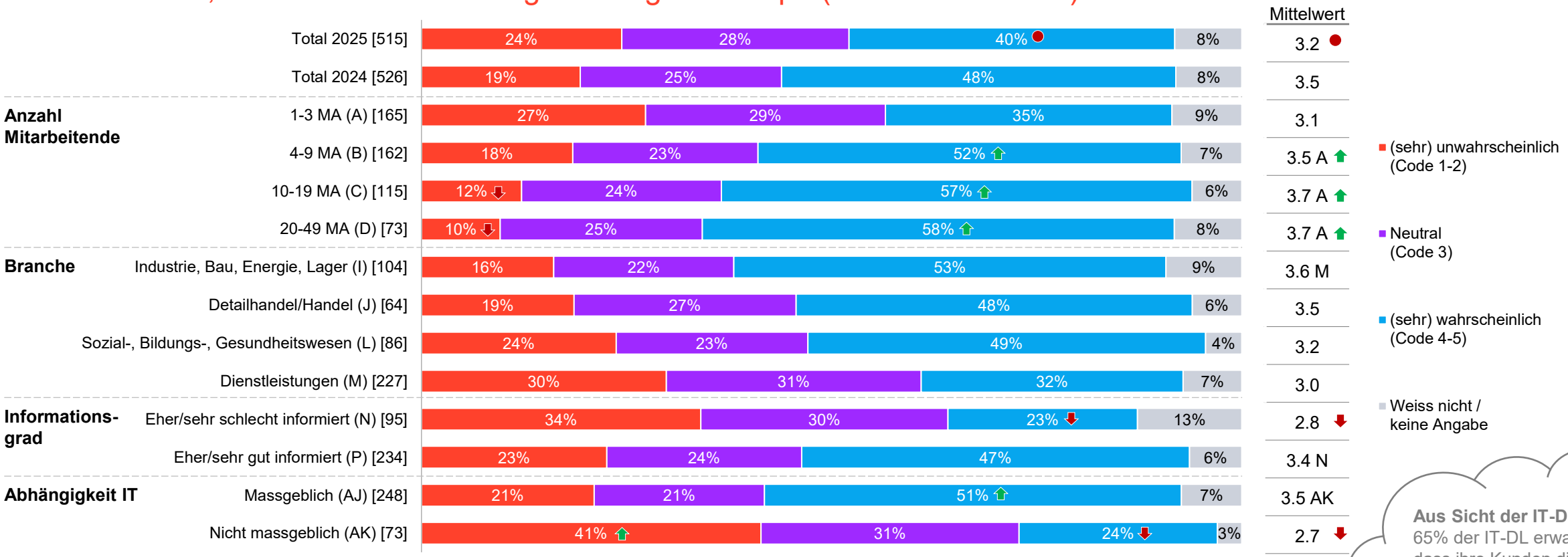
Geldverlust bei Betrug
Basis: n=20** | Filter: durch betrügerischen E-Mails irrtümlich bezahltes Geld



F035: Hat Ihr Unternehmen schon einmal irrtümlich Geld einbezahlt aufgrund eines betrügerischen E-Mails? | F036: War dieses Geld verloren, oder konnten Sie es zurückgewinnen?
Basis: n=[ ] | Filter: siehe oben | Geschlossene Fragen | ⬆ signifikant höher als Total; ⬇ signifikant tiefer als Total | Neue Frage in 2025 | Datenbeschriftung ab 3% | **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.

Erhöhung Sicherheitsmassnahmen

Nur noch zwei Fünftel der Befragten möchten in den kommenden 1 bis 3 Jahren ihre Cybersicherheits-Massnahmen erhöhen; 2024 war es noch knapp die Hälfte. Am höchsten ist der Anteil bei den Unternehmen mit 20 bis 49 Mitarbeitenden, aber auch hier ist er signifikant geschrumpft (von 79% auf 58%).

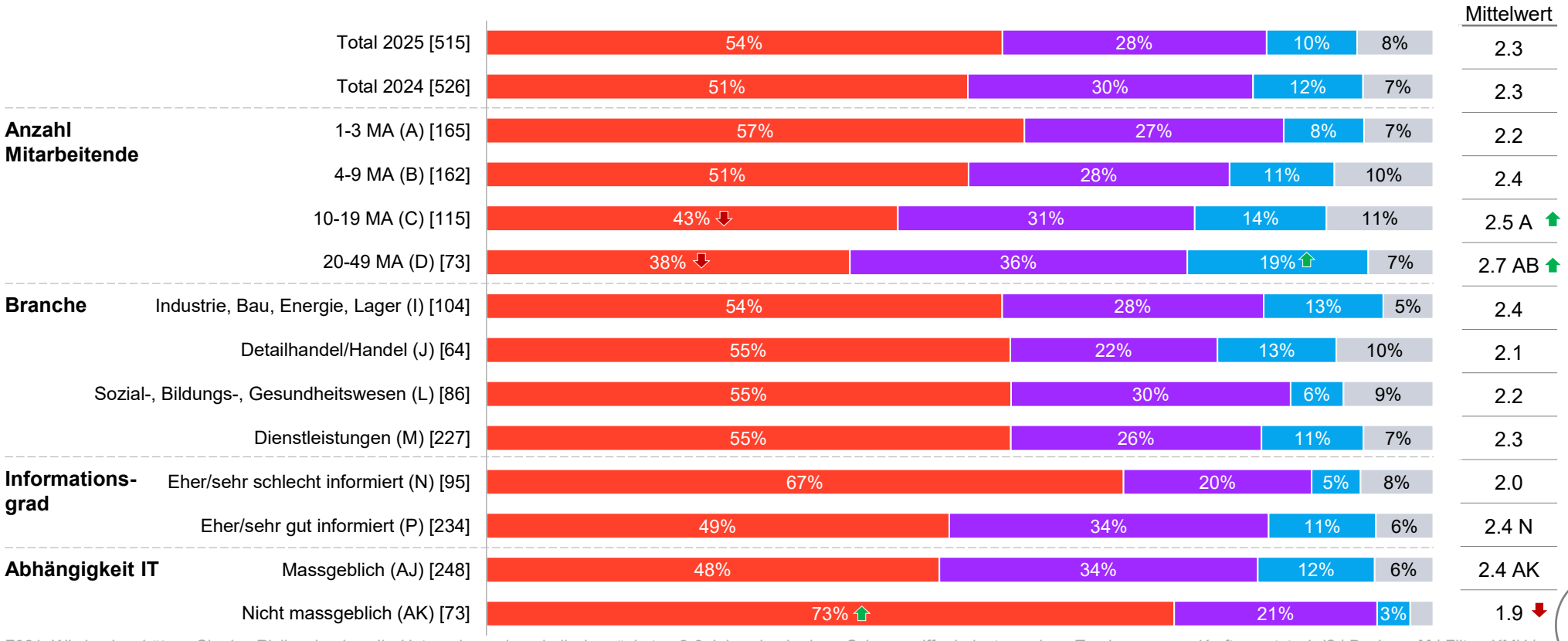


F018: Wie wahrscheinlich ist es, dass Sie in den kommenden 1 bis 3 Jahren die Sicherheitsmassnahmen gegen Cyberkriminalität erhöhen werden? | Basis: n=[ ] | Filter: KMU |
Skalierte Frage: 1= sehr unwahrscheinlich bis 5= sehr wahrscheinlich | ⬆ signifikant höher als Total; ⬇ signifikant tiefer als Total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

Aus Sicht der IT-DL…
65% der IT-DL erwarten, dass ihre Kunden die Sicherheitsmassnahmen erhöhen werden (S. 77).

Risikoeinschätzung

Etwas mehr als die Hälfte der befragten Unternehmen 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.

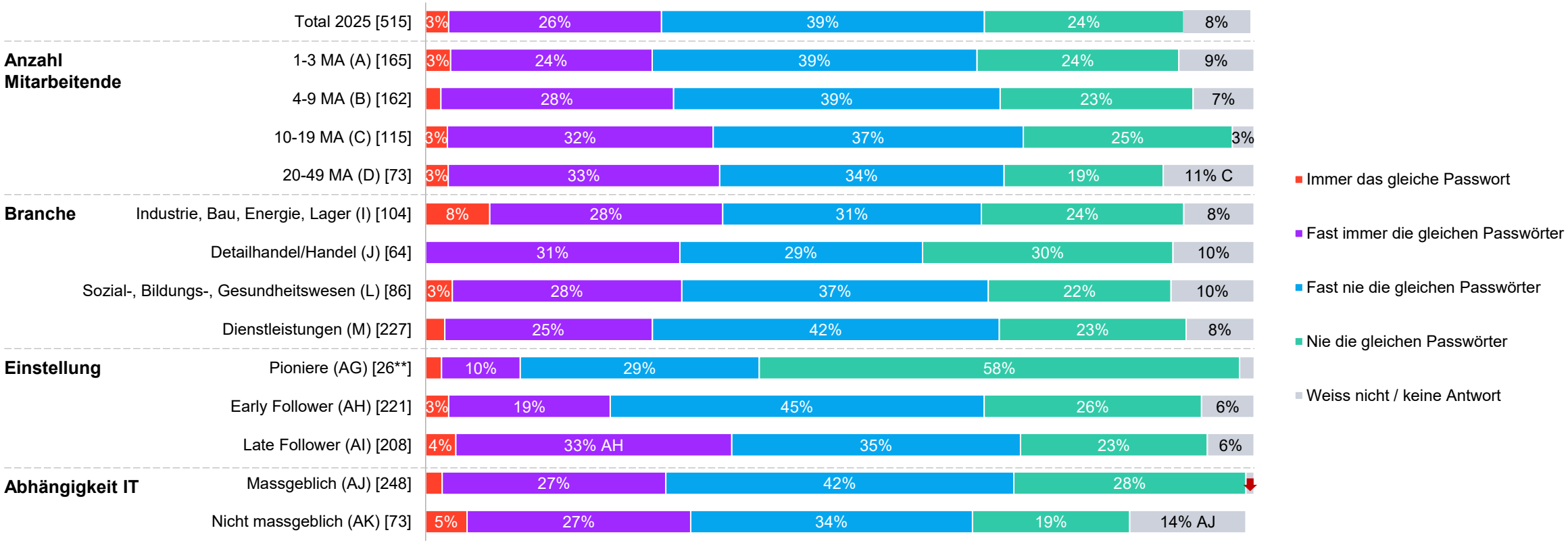


F021: Wie hoch schätzen Sie das Risiko ein, dass Ihr Unternehmen innerhalb der nächsten 2-3 Jahre durch einen Cyberangriff mindestens einen Tag lang ausser Kraft gesetzt wird? | Basis: n=[ ] | Filter: KMU | Skalierte Frage: 1= sehr kleines Risiko bis 5= sehr grosses Risiko | ▲ signifikant höher als Total;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

Aus Sicht der IT-DL…
61% 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. 74).

Umgang mit Passwörtern

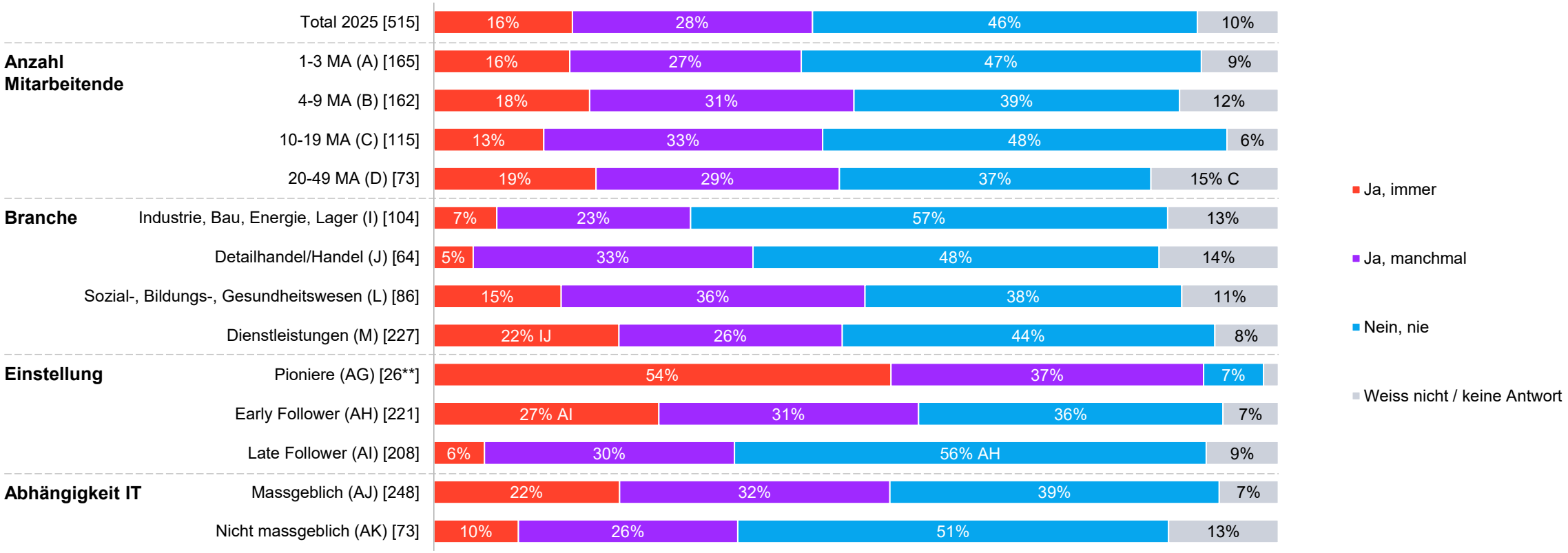
Nur ganz wenige Befragte nutzen immer dasselbe Passwort, aber rund ein Viertel nutzt „fast immer“ das gleiche Passwort und geht damit ein Risiko ein. Ebenfalls rund ein Viertel nutzt „nie“ das gleiche Passwort für verschiedene Anwendungen; in Unternehmen, deren funktionierende IT massgeblich ist, ist der Anteil etwas höher.



F022: Benutzen Sie für verschiedene Programme oder Plattformen das gleiche Passwort mehrfach? Ich benutze…
Basis: n=[ ] | Filter: KMU | Geschlossene Frage | ⬆ signifikant höher als Total; ⬇ signifikant tiefer als Total | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle | **Sehr kleine Basis <30 | 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. | °Ab 2025 nicht mehr gefragt

Passwortmanager

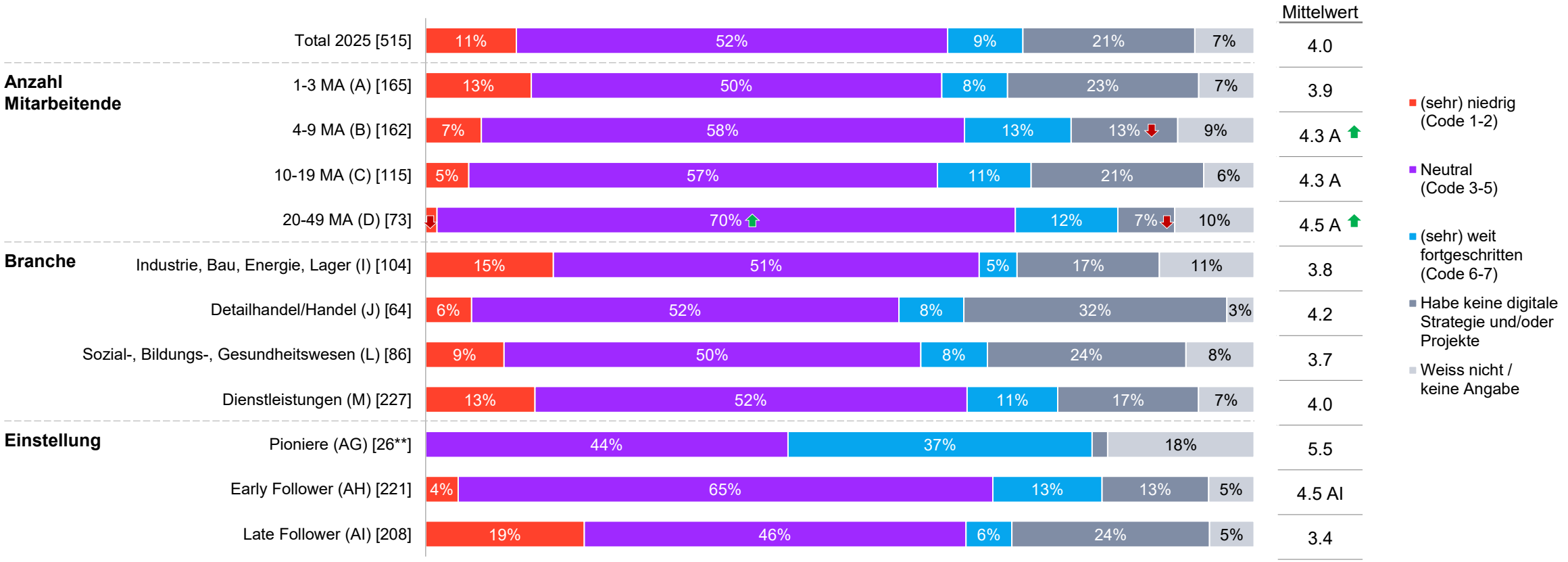
Etwas mehr als zwei Fünftel der Befragten nutzen zumindest manchmal einen Passwortmanager. Je innovationsfreudiger die Einstellung ist, desto eher wird ein Passwortmanager genutzt; und Unternehmen, die massgeblich von einer funktionierenden IT abhängig sind, nutzen ebenfalls etwas häufiger einen Passwortmanager.



F037: Benutzen Sie in Ihrem Unternehmen einen Passwortmanager?
Basis: n=[ ] | Filter: KMU | Geschlossene Frage | ⬆ signifikant höher als Total; ⬇ signifikant tiefer als Total | **Sehr kleine Basis <30 | 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. | Neue Frage in 2025

Fortschritt digitale Strategie

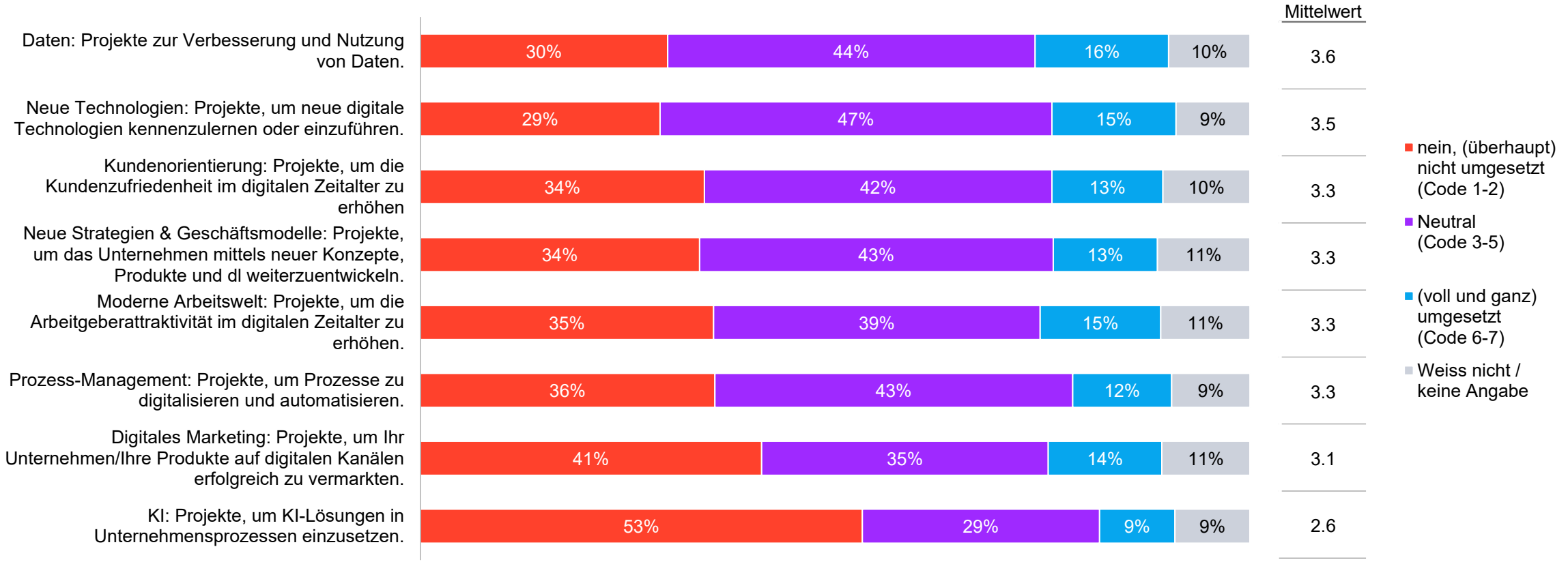
Rund ein Fünftel der Befragten hat keine digitale Strategie und/oder keine digitalen Projekte, rund jede/-r zehnte hält den Fortschritt der digitalen Strategie/Transformationen für (sehr) wenig bzw. (sehr) weit fortgeschritten. Unternehmen mit 1-3 Mitarbeitenden schätzen ihren Fortschritt am tiefsten ein bzw. haben am häufigsten keine digitale Strategie.



F040: Wie schätzen Sie den Fortschritt Ihrer digitalen Strategie bzw. digitalen Transformation ein?
Basis: n=[ ] | Filter: KMU | Skalierte Frage: 1= sehr niedrig bis 7= sehr weit fortgeschritten | ⬆signifikant höher als Total; ⬇ signifikant tiefer als Total | *Kleine Basis <50 | **Sehr kleine Basis <30 | 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. | Neue Frage in 2025

Digitale Strategiemassnahmen (1/4)

Von den acht abgefragten Massnahmen wurden „Projekte zur Verbesserung und Nutzung von Daten“ am weitesten umgesetzt; aber immerhin knapp ein Drittel der Befragten haben diesbezüglich noch (überhaupt) nichts umgesetzt. KI-Lösungen in Unternehmens-prozessen wurden von knapp jedem zehnten Unternehmen (voll und ganz) umgesetzt, von über der Hälfte (überhaupt) nicht.

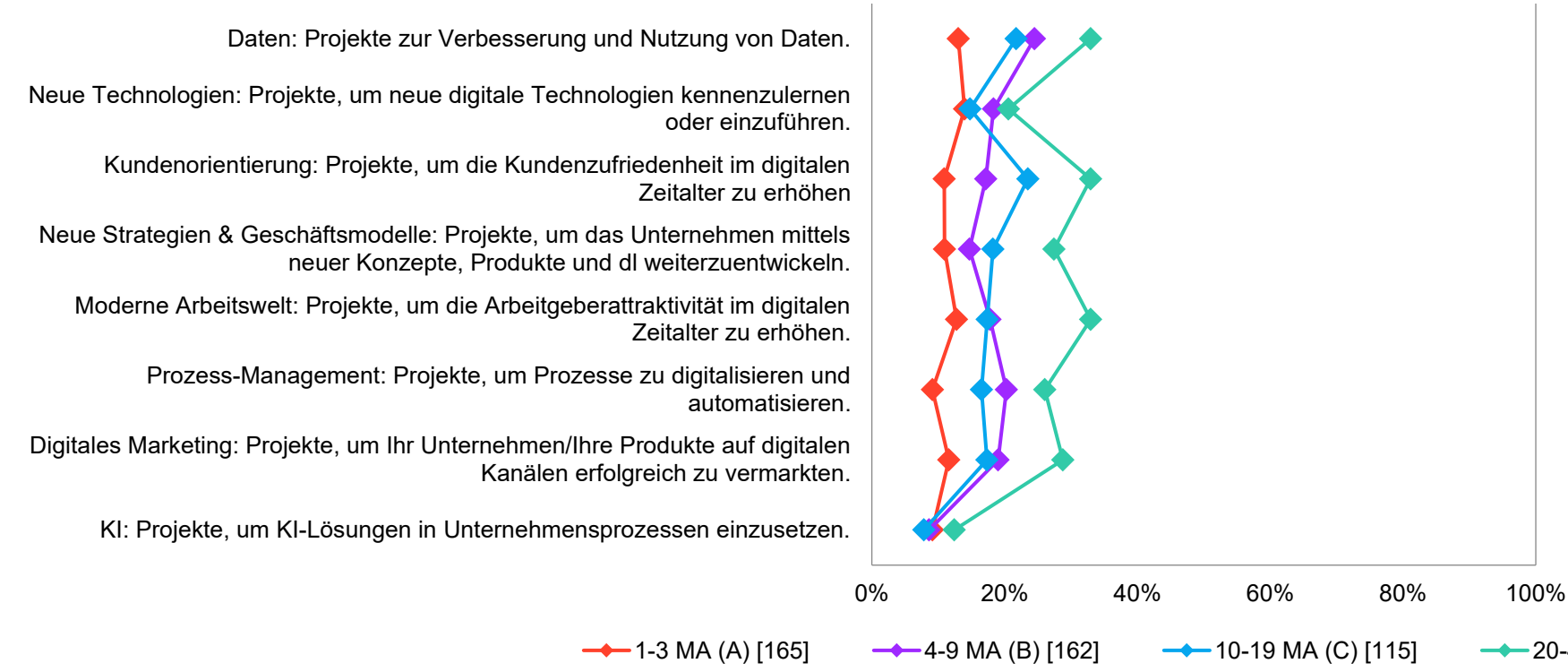


F041: Bitte geben Sie auf einer Skala von 1-7 an, inwiefern Ihr Unternehmen in den vergangenen drei Jahren die folgenden Massnahmen umgesetzt hat.
Basis: n=[ ] | Filter: KMU | Skalierte Frage: 1= nein, überhaupt nicht umgesetzt bis 7= voll und ganz umgesetzt | Neue Frage in 2025

Digitale Strategiemassnahmen (2/4)

Unternehmen mit 1-3 Mitarbeitenden sind am wenigsten weit mit der Umsetzung von digitalen Strategiemassnahmen, Unternehmen mit 20-49 Mitarbeitenden am weitesten. Die mittleren beiden Kategorien liegen sehr dicht beieinander.

Nach Anzahl Mitarbeitenden



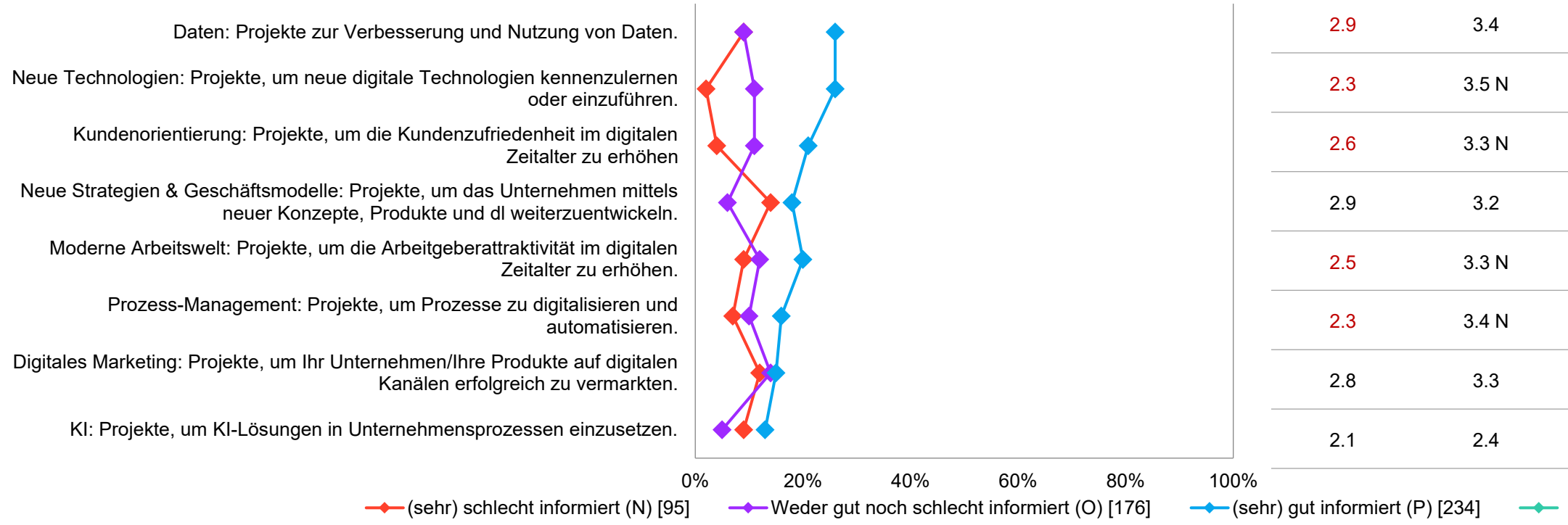
Mittelwert			
1-3 MA	4-9 MA	10-19 MA	20-49 MA
3.3	4.2 A	4.4 A	4.8 AB
3.3	3.9 A	4.0 A	4.5 AB
3.1	3.9 A	4.1 A	4.8 ABC
3.1	3.8 A	4.1 A	4.5 AB
3.1	3.9 A	4.0 A	4.6 ABC
3.0	4.0 A	4.1 A	4.7 ABC
2.9	3.7 A	3.7 A	4.4 ABC
2.5	2.8	2.8	3.4 ABC

F041: Bitte geben Sie auf einer Skala von 1-7 an, inwiefern Ihr Unternehmen in den vergangenen drei Jahren die folgenden Massnahmen umgesetzt hat.
Basis: n=[ ] | Filter: KMU | Skalierte Frage: 1= nein, überhaupt nicht umgesetzt bis 7= voll und ganz umgesetzt | Neue Frage in 2025 | 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.

Digitale Strategiemassnahmen (3/4)

Wer sich bezüglich Cybercrime eher oder sehr schlecht informiert fühlt, hat sechs von acht Massnahmen signifikant weniger weit umgesetzt als eher/sehr gut informierte Unternehmen.

Nach Informationsgrad



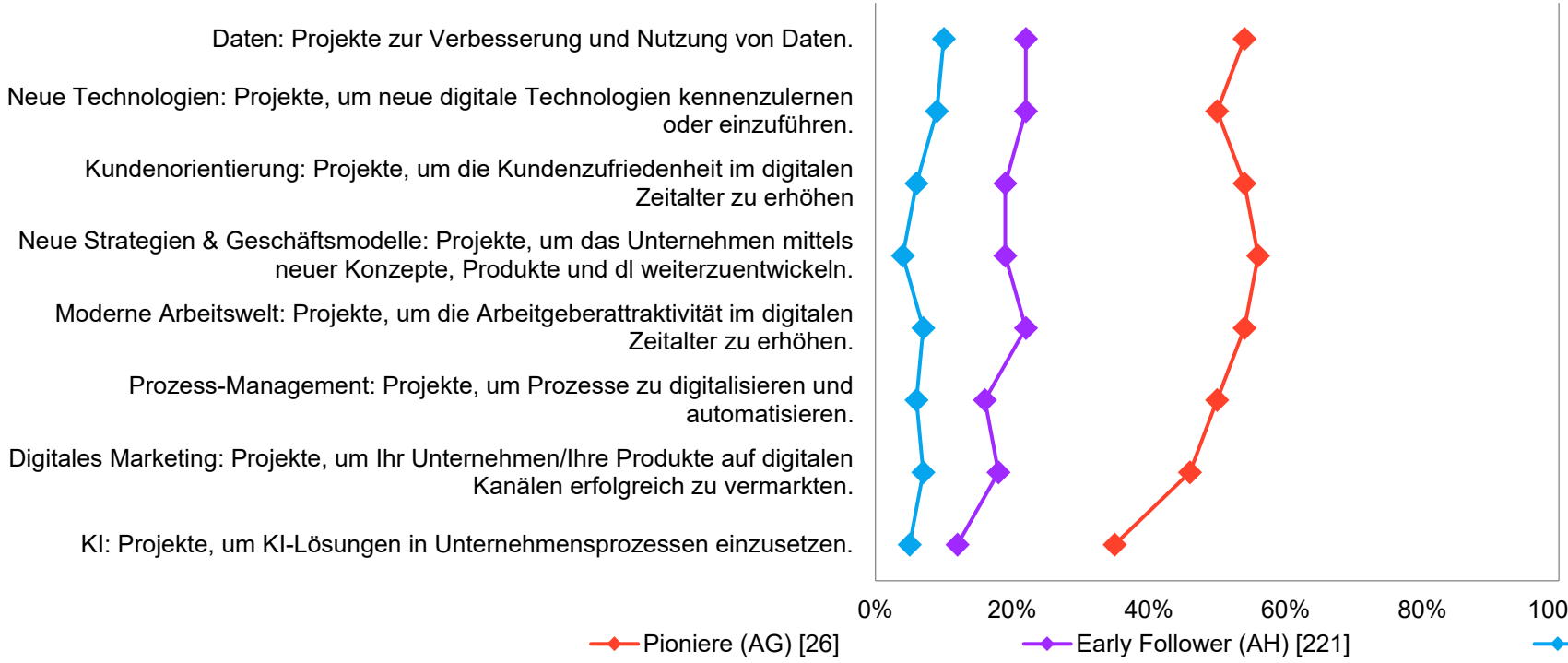
Mittelwert Informationsgrad		
Eher/sehr schlecht	Weder gut noch schlecht	Eher/ sehr gut
2.9	3.4	4.0 NO
2.3	3.5 N	4.1 NO
2.6	3.3 N	3.7 N
2.9	3.2	3.6
2.5	3.3 N	3.8 N
2.3	3.4 N	3.6 N
2.8	3.3	3.1
2.1	2.4	2.9 N

F041: Bitte geben Sie auf einer Skala von 1-7 an, inwiefern Ihr Unternehmen in den vergangenen drei Jahren die folgenden Massnahmen umgesetzt hat.
Basis: n=[ ] | Filter: KMU | Skalierte Frage: 1= nein, überhaupt nicht umgesetzt bis 7= voll und ganz umgesetzt | Neue Frage in 2025 | 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.

Digitale Strategiemassnahmen (4/4)

Pioniere sind bei der Umsetzung aller abgefragten digitalen Strategiemassnahmen deutlich weiter als Early- und Late-Follower.

Nach Einstellung



	Mittelwert		
	Pioniere	Early Follower	Late Follower
Daten: Projekte zur Verbesserung und Nutzung von Daten.	5.6	4.0 AI	3.1
Neue Technologien: Projekte, um neue digitale Technologien kennenzulernen oder einzuführen.	5.2	4.2 AI	2.9
Kundenorientierung: Projekte, um die Kundenzufriedenheit im digitalen Zeitalter zu erhöhen	5.4	4.0 AI	2.6
Neue Strategien & Geschäftsmodelle: Projekte, um das Unternehmen mittels neuer Konzepte, Produkte und dl weiterzuentwickeln.	5.3	4.0 AI	2.6
Moderne Arbeitswelt: Projekte, um die Arbeitgeberattraktivität im digitalen Zeitalter zu erhöhen.	4.8	4.1 AI	2.5
Prozess-Management: Projekte, um Prozesse zu digitalisieren und automatisieren.	5.0	3.8 AI	2.7
Digitales Marketing: Projekte, um Ihr Unternehmen/Ihre Produkte auf digitalen Kanälen erfolgreich zu vermarkten.	4.3	3.5 AI	2.6
KI: Projekte, um KI-Lösungen in Unternehmensprozessen einzusetzen.	4.1	3.0 AI	2.0

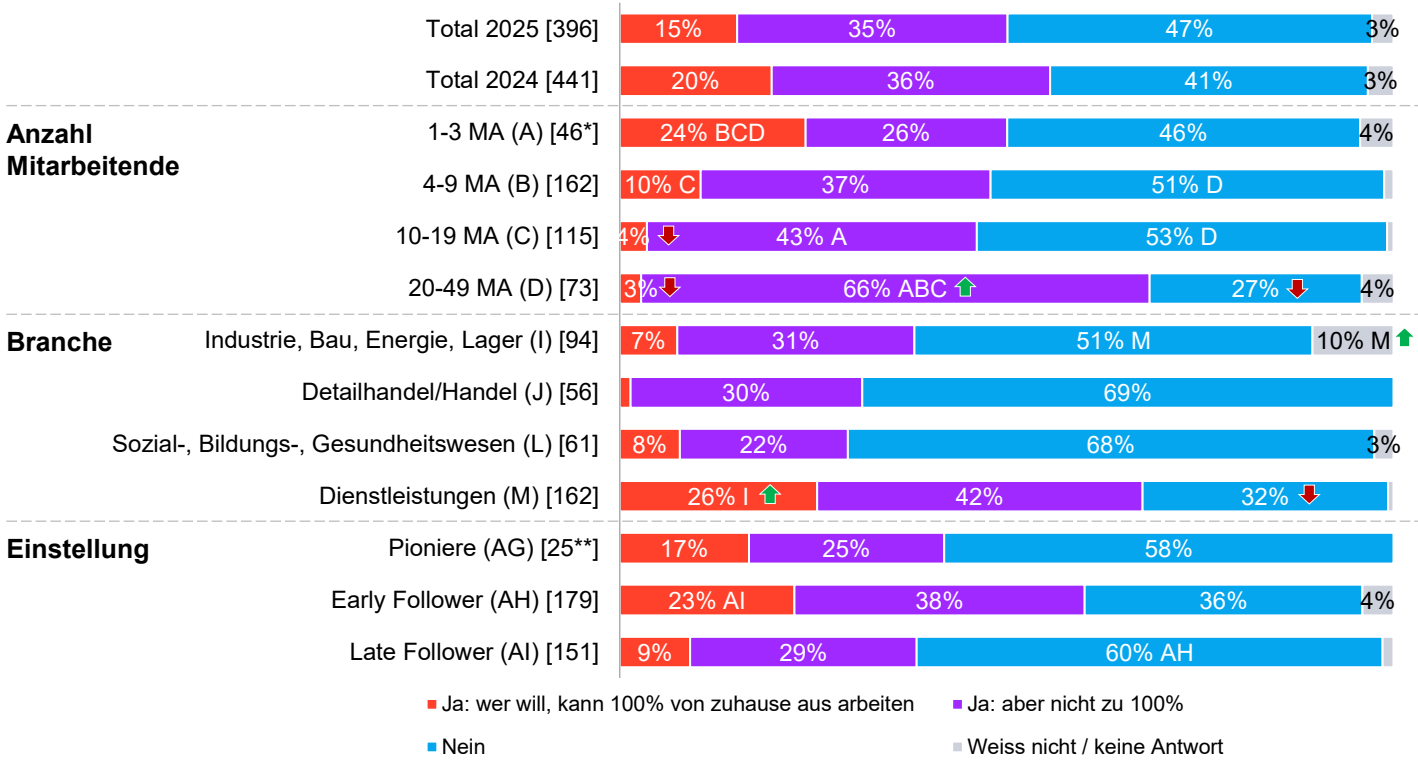
F041: Bitte geben Sie auf einer Skala von 1-7 an, inwiefern Ihr Unternehmen in den vergangenen drei Jahren die folgenden Massnahmen umgesetzt hat.
Basis: n=[ ] | Filter: KMU | Skalierte Frage: 1= nein, überhaupt nicht umgesetzt bis 7= voll und ganz umgesetzt | Neue Frage in 2025 | Top2 und Mittelwerte ausgewiesen | **Sehr kleine Basis <30
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.

Homeoffice

Das Homeoffice-Angebot sinkt tendenziell; nur noch die Hälfte der Befragten bietet (teilweise) Homeoffice an, letztes Jahr waren es noch 6 Prozentpunkte mehr. Trotzdem geht noch rund ein Viertel der Befragten davon aus, dass es in Zukunft mehr Homeoffice geben wird – es handelt sich dabei v.a. um Befragte aus kleinen Unternehmen (1-3 MA).

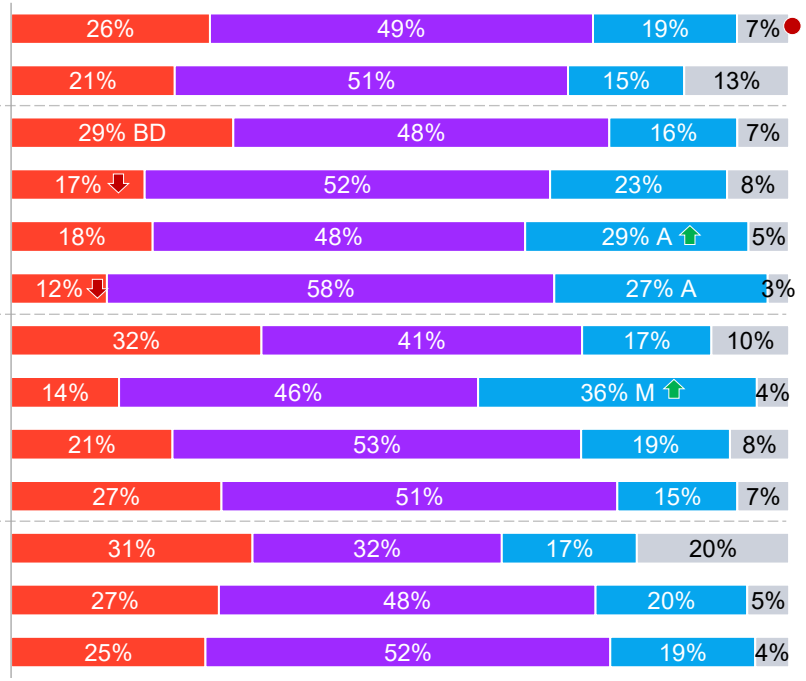
Angebot Homeoffice

Filter: befragte Unternehmen haben mehr als eine/n Mitarbeitenden



Zukunftsentwicklung Homeoffice Schweiz

Filter: KMU



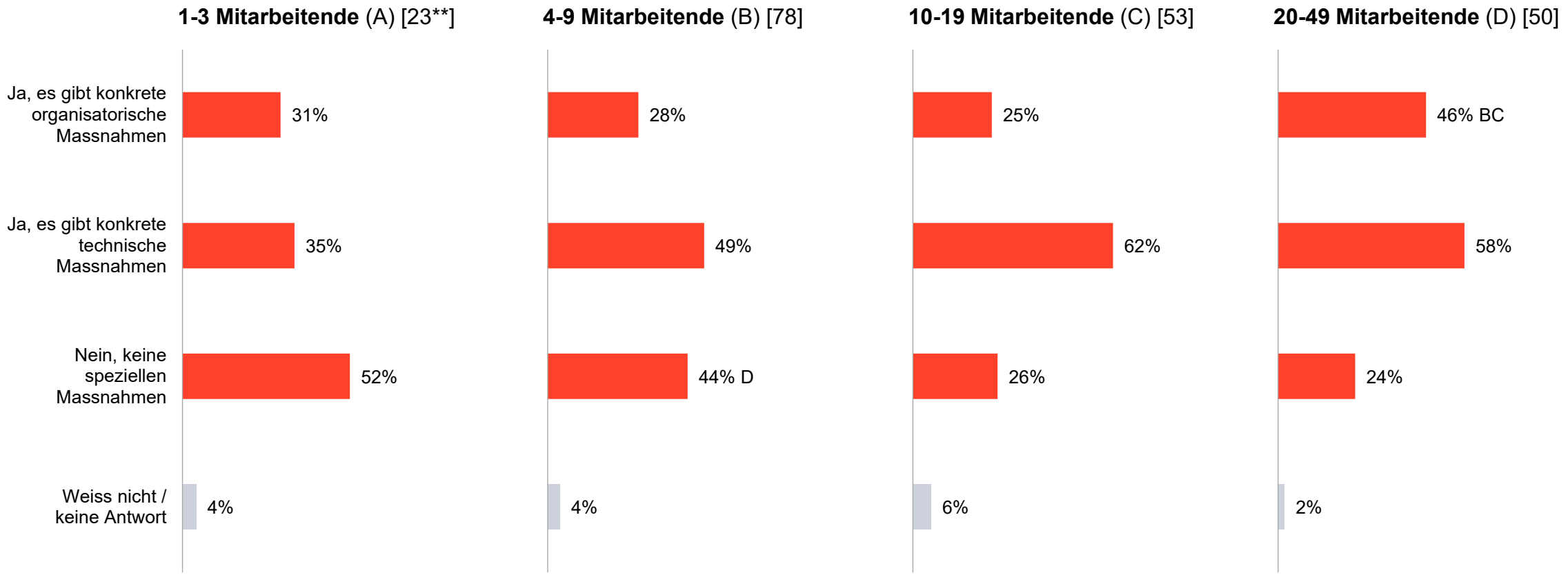
Ja: wer will, kann 100% von zuhause aus arbeiten
Ja: aber nicht zu 100%
Nein
Weiss nicht / keine Antwort

Es wird mehr Mitarbeitende im HO geben
Es wird etwa so bleiben
Es wird weniger Mitarbeitende im HO geben
Weiss nicht / keine Antwort

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; ▼ signifikant tiefer als Total | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle | **Sehr kleine Basis <30 | 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

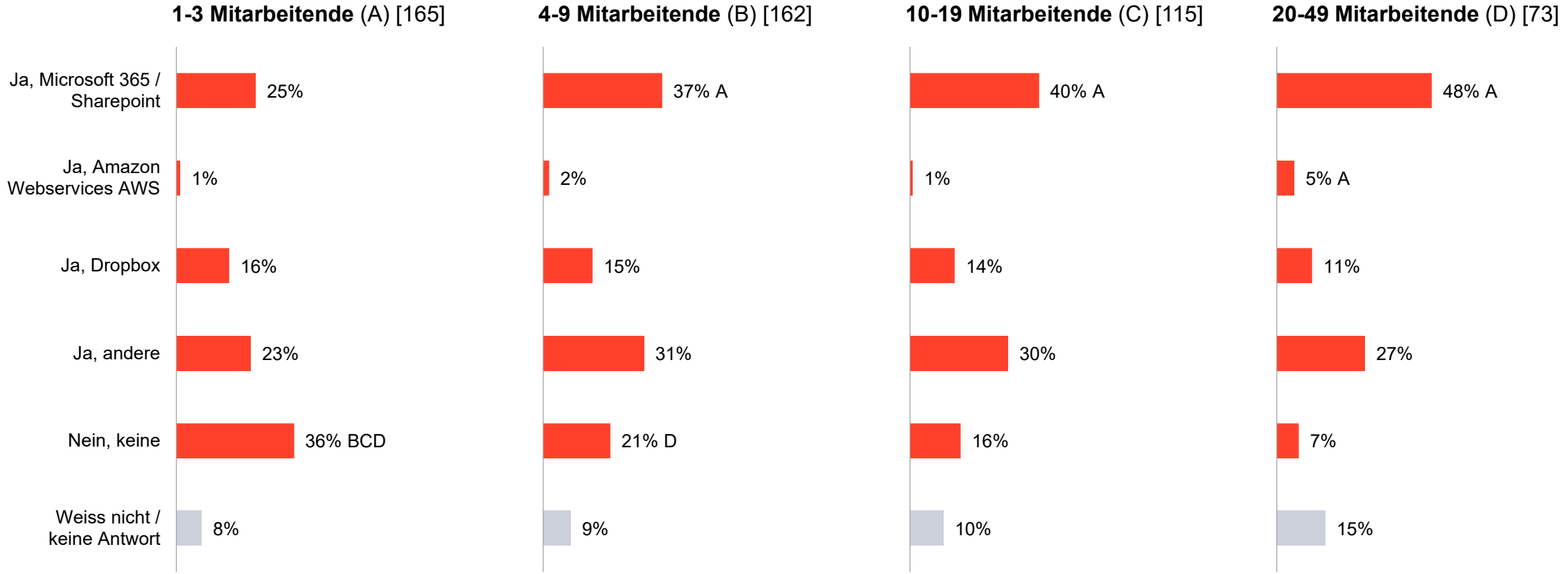
Rund die Hälfte der Befragten (52%) trafen konkrete organisatorische und/oder technische Massnahmen zum Schutz vor Cyberangriffen im Homeoffice (Total-Werte nicht abgebildet). Die grösseren Unternehmen haben eher technische Massnahmen ergriffen als die kleineren. Organisatorische Massnahmen werden von den kleineren Unternehmen eher vernachlässigt.



F028: Treffen Sie konkrete Vorkehrungen zum Schutz vor Cyberangriffen im Homeoffice?
Basis: n=[ ] | Filter: KMU – Homeoffice wird angeboten | Geschlossene Frage | **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.

Cloudnutzung

Knapp zwei Drittel der befragten Unternehmen nutzen Cloud-Dienstleistungen zur Datenablage (60%, Total-Werte nicht abgebildet). Je grösser die Unternehmen sind, desto eher nutzen sie Microsoft 365/Sharepoint. Dropbox oder andere Services werden von den verschiedenen Unternehmensgrössen im gleichen Masse verwendet.



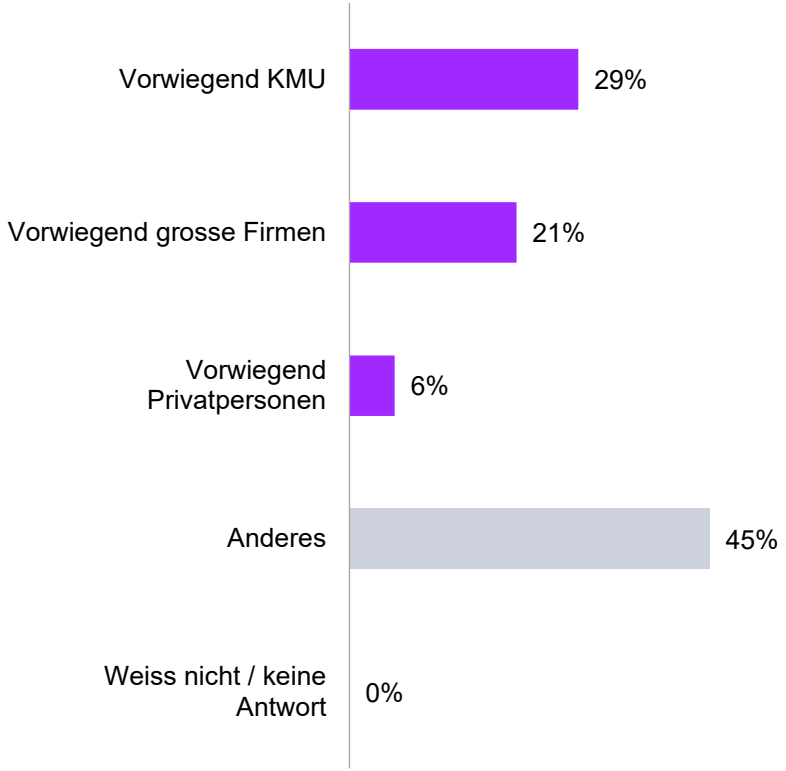
F029: Nutzen Sie für Ihre Datenablage Cloud-Dienstleistungen?
Basis: n=[ ] | Filter: KMU | Geschlossene Frage
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

04 IT-Dienstleister

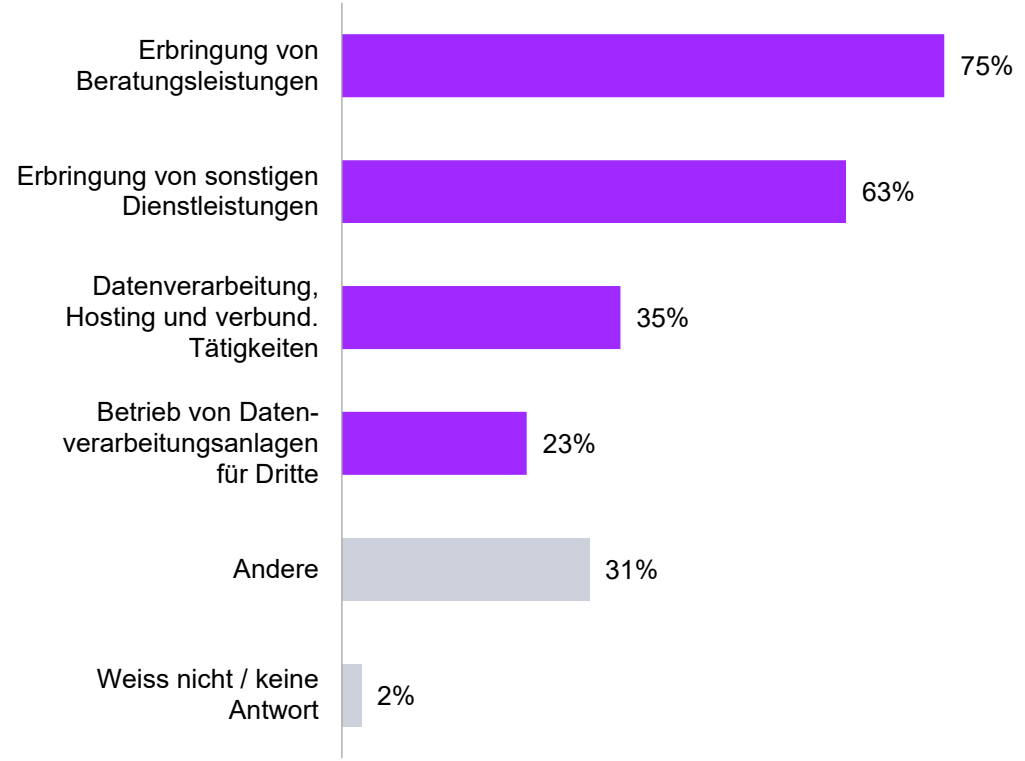
Kunden & Angebot

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

Verteilung Kundenstamm



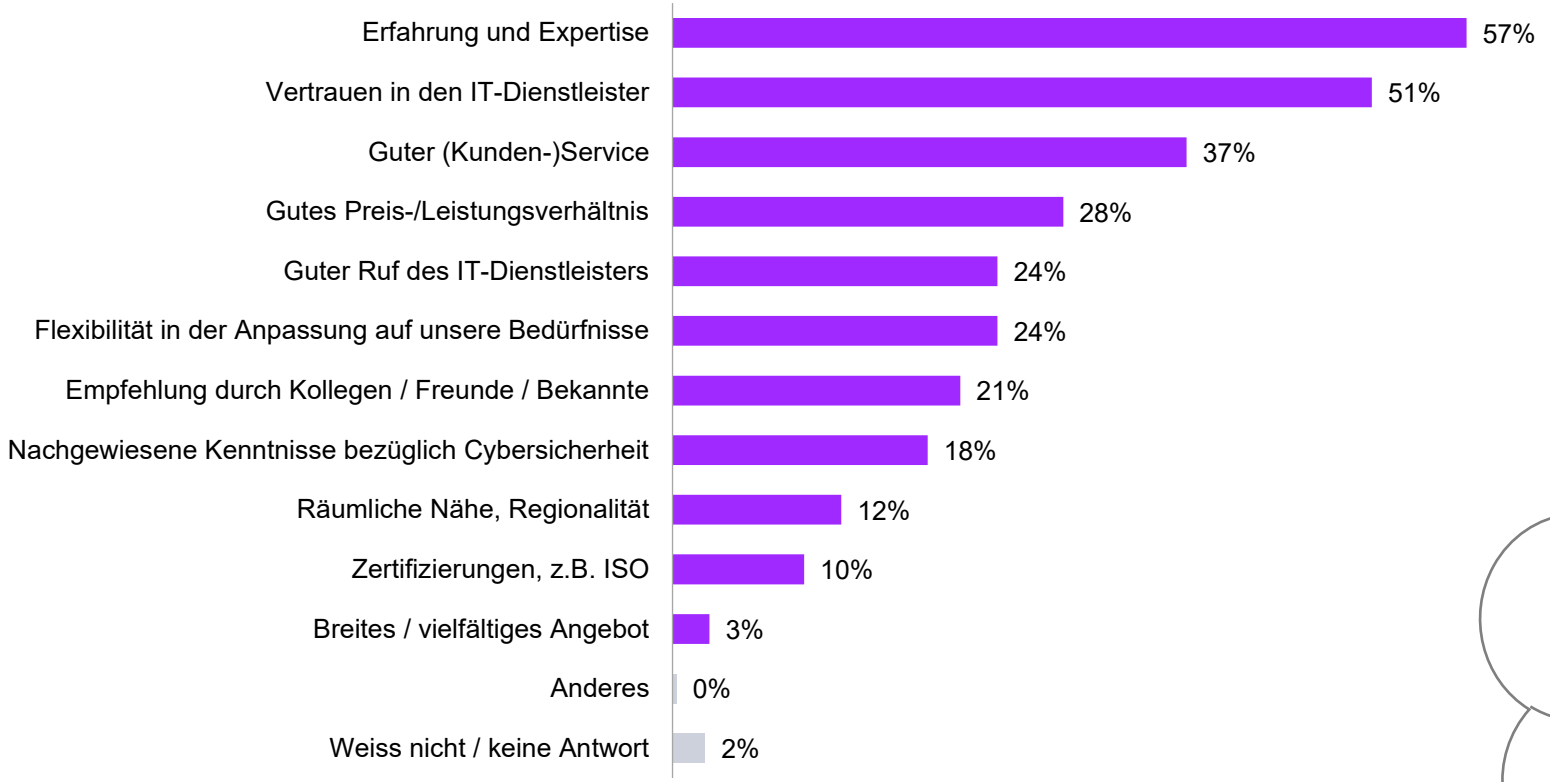
Dienstleistungen



S08: Wie setzt sich der Kundenstamm Ihres Unternehmens ungefähr zusammen? (Eine grobe Schätzung reicht als Antwort) | S10: Welches ist Ihr Angebot?
Basis: n=336 | Filter: IT-Dienstleister | Geschlossene Fragen

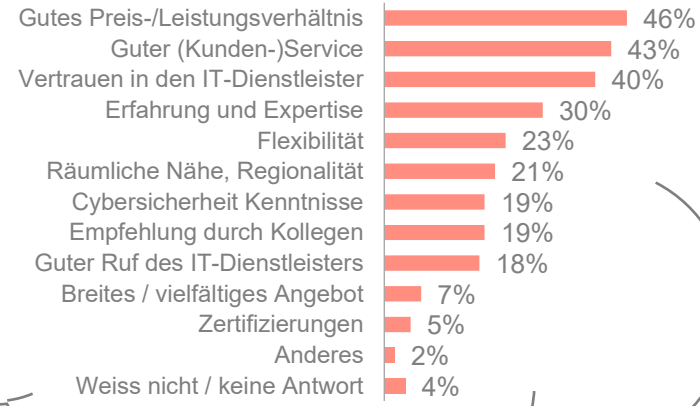
Auswahlkriterien IT-Dienstleister

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. Aus Sicht der KMU liegen Erfahrung und Expertise aber lediglich auf Platz 4, während das gute Preis-/Leistungsverhältnis auf Platz 1 liegt.



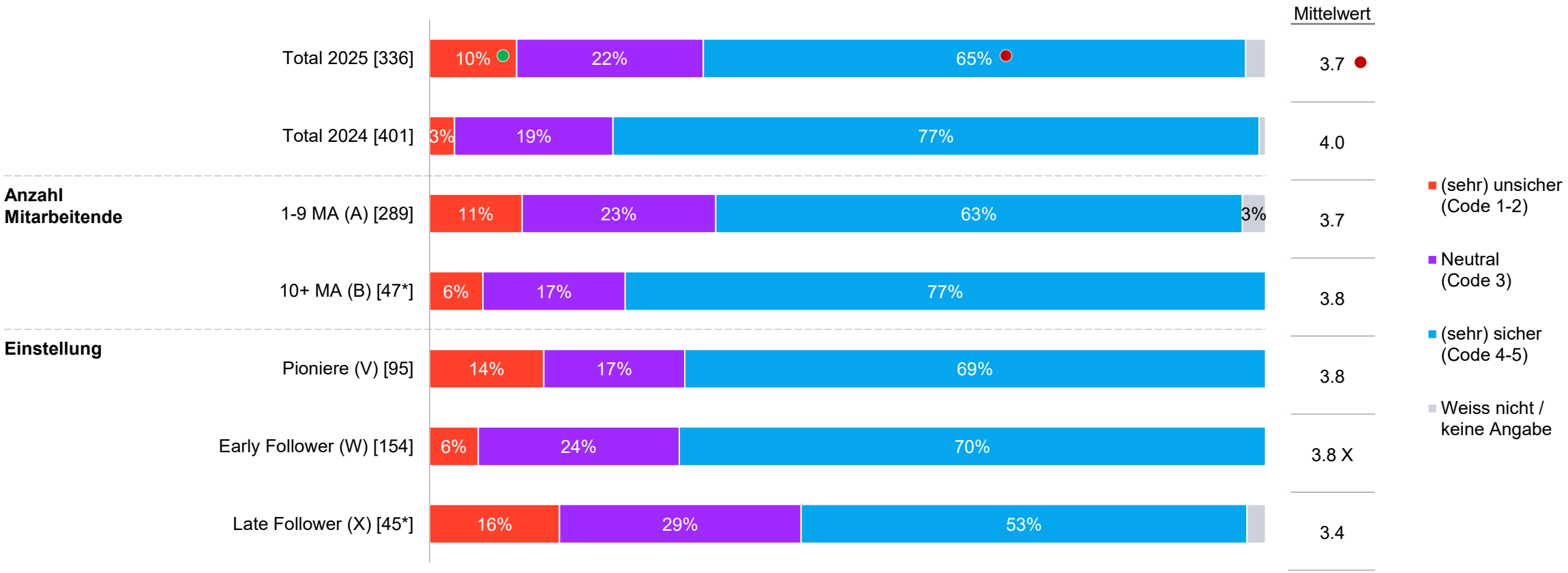
F050: Welche der folgenden Kriterien sind aus Ihrer Sicht für die Auswahl eines IT-Dienstleisters am wichtigsten? Bitte wählen Sie max. 3 Antworten aus.
Basis: n=336 | Filter: IT-Dienstleister | Geschlossene Frage

Aus Sicht der KMU…
ist räumliche Nähe wichtiger als die IT-DL vermuten, guter Service ist am wichtigsten (siehe Seite 16).



Sicherheitsgefühl

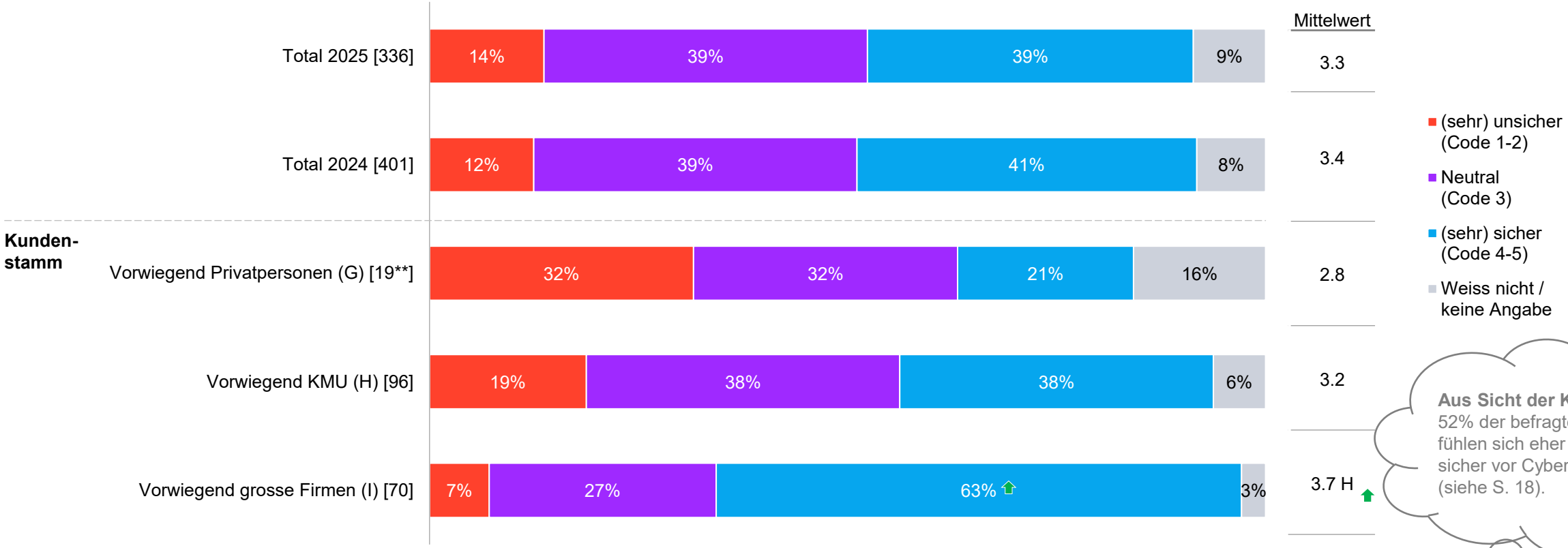
Rund zwei Drittel der IT-Dienstleister fühlen sich (sehr) sicher vor Cyberkriminalität, während sich jede/-r zehnte (sehr) unsicher fühlt. Das Sicherheitsgefühl der IT-Dienstleister ist seit der Befragung 2024 signifikant gesunken.



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; ⬇ signifikant tiefer als Total | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle | *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

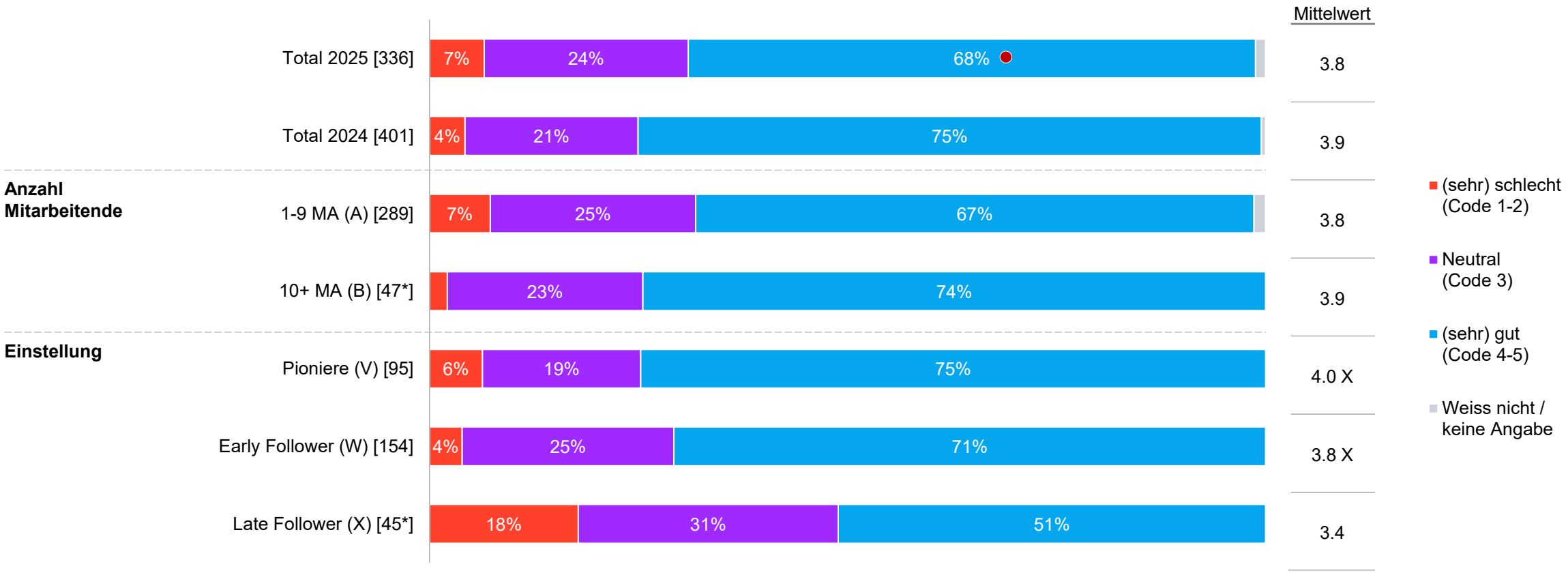
Die Sicherheit der Kunden wird von den IT-Unternehmen tiefer eingeschätzt als die eigene: Nur rund zwei Fünftel gehen davon aus, dass ihre Kunden (sehr) sicher sind, die Werte sind praktisch unverändert zum letzten Jahr. Wer vorwiegend grosse Firmen im Kundenstamm hat, geht eher von einer (sehr) hohen Sicherheit aus, als wer vorwiegend KMU bedient.



Aus Sicht der KMU…
52% der befragten KMU fühlen sich eher oder sehr sicher vor Cyberkriminalität (siehe S. 18).

F052. Wie schätzen Sie die Cybersicherheit Ihrer Kunden alles in allem ungefähr ein?
Basis: n=[ ] | Filter: IT-Dienstleister | Skalierte Fragen (siehe oben) | ▲ signifikant höher als Total; ▼ signifikant tiefer als Total | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle
**Sehr kleine Basis <30 | 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.

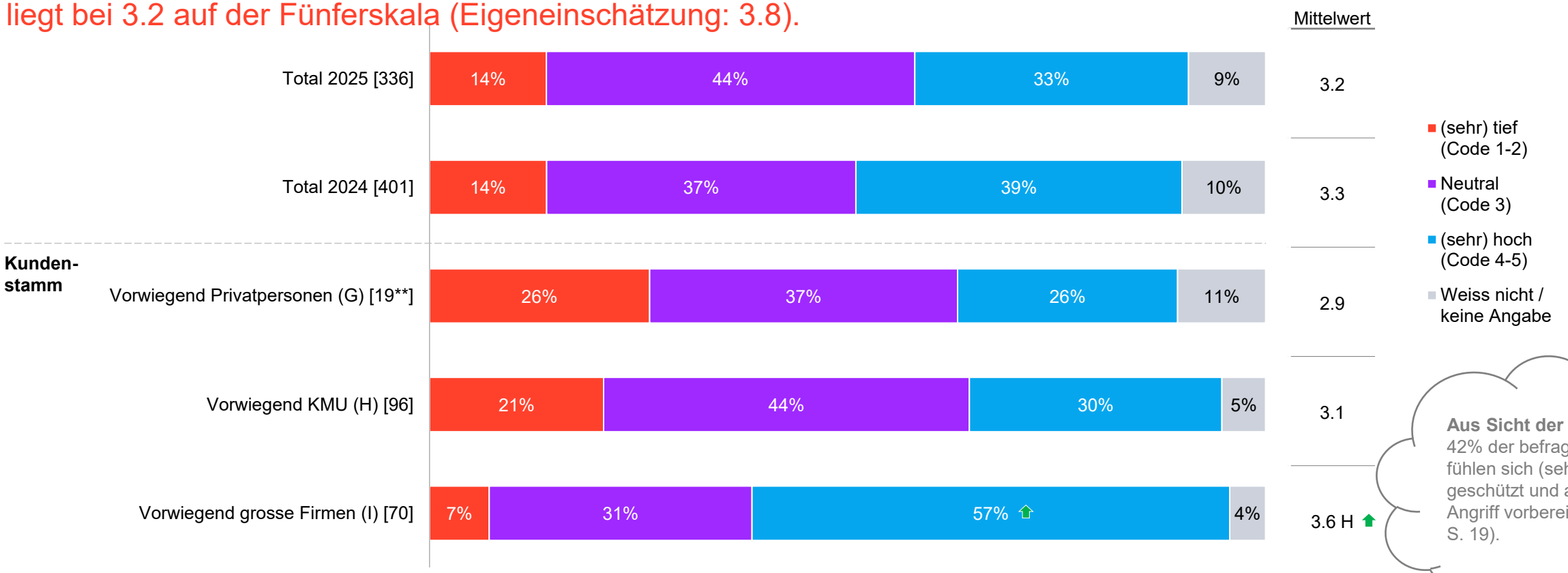
Nur noch rund zwei Drittel der befragten IT-Dienstleister fühlen sich (sehr) gut vor Cyberangriffen geschützt und auf einen Angriff vorbereitet, letztes Jahr waren es noch drei Viertel.



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; ⬇ signifikant tiefer als Total | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle | *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

Die Resilienz der Kunden wird von den IT-Unternehmen leicht tiefer eingeschätzt als letztes Jahr und auch tiefer als die eigene: Nur ein Drittel der Befragten schätzen die Resilienz ihrer Kunden (sehr) hoch ein, der Mittelwert liegt bei 3.2 auf der Fünferskala (Eigeneinschätzung: 3.8).

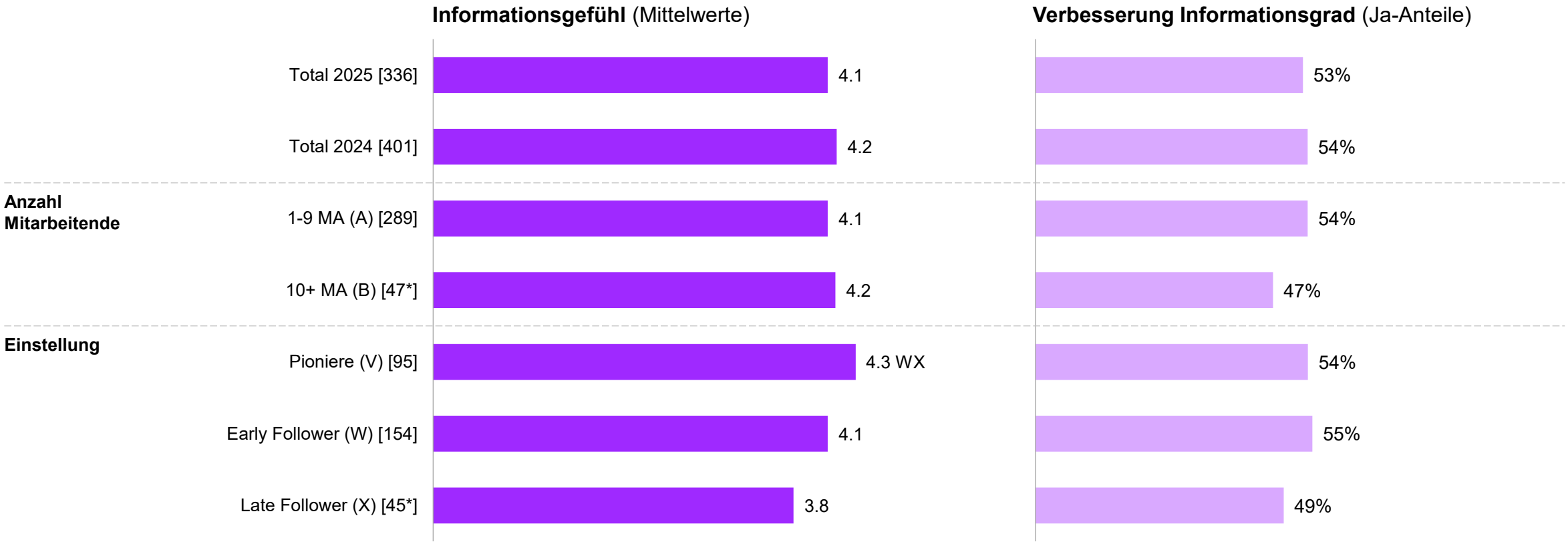


Aus Sicht der KMU…
42% der befragten KMU fühlen sich (sehr) gut geschützt und auf einen Angriff vorbereitet (siehe S. 19).

F053. Wie schätzen Sie die Widerstandsfähigkeit Ihrer Kunden gegen Cyberangriffe alles in allem ungefähr ein?
Basis: n=[ ] | Filter: IT-Dienstleister | Skalierte Fragen (siehe oben) | ▲ signifikant höher als Total; ▼ signifikant tiefer als Total | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle
**Sehr kleine Basis <30 | 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

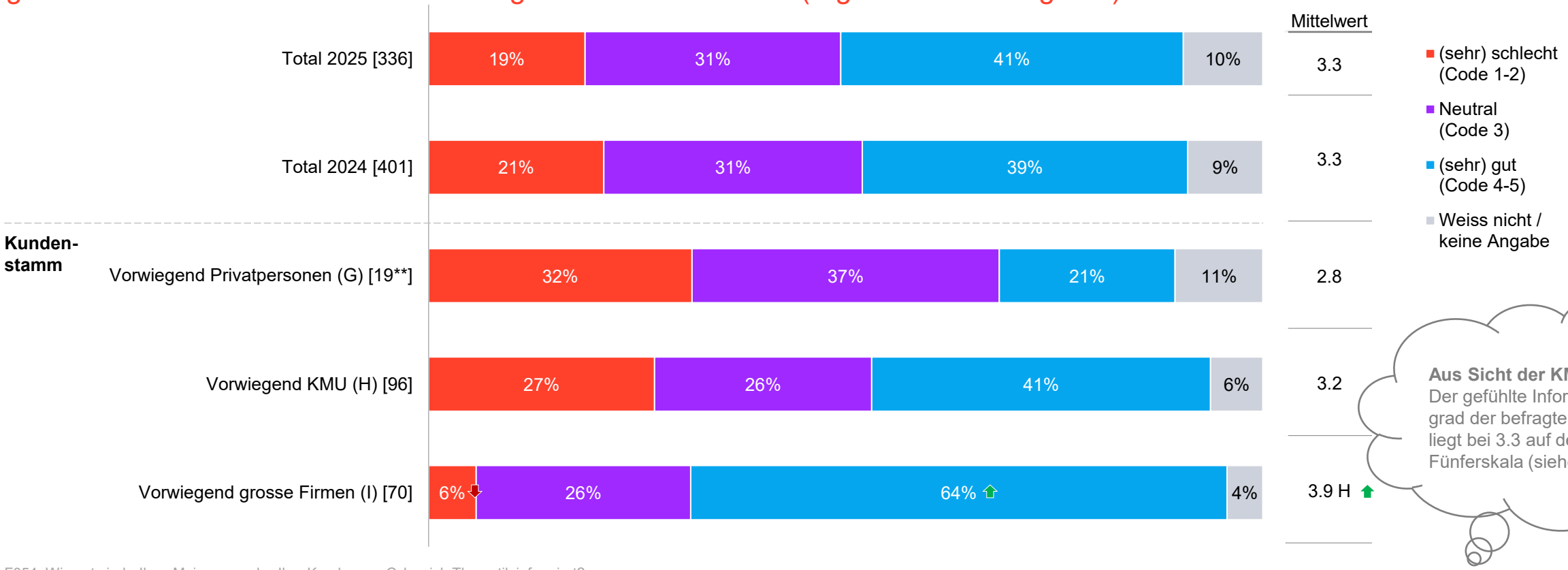
IT-Dienstleister fühlen sich sehr gut informiert bezüglich der Cyberrisk-Thematik; auf der Fünferskala geben sie im Durchschnitt eine 4.1 an. Rund die Hälfte der Befragten wäre gerne besser informiert zum Thema Cybersicherheit. Diese Werte sind gegenüber dem Vorjahr praktisch unverändert.



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; ⬇ signifikant tiefer als Total | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle | *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

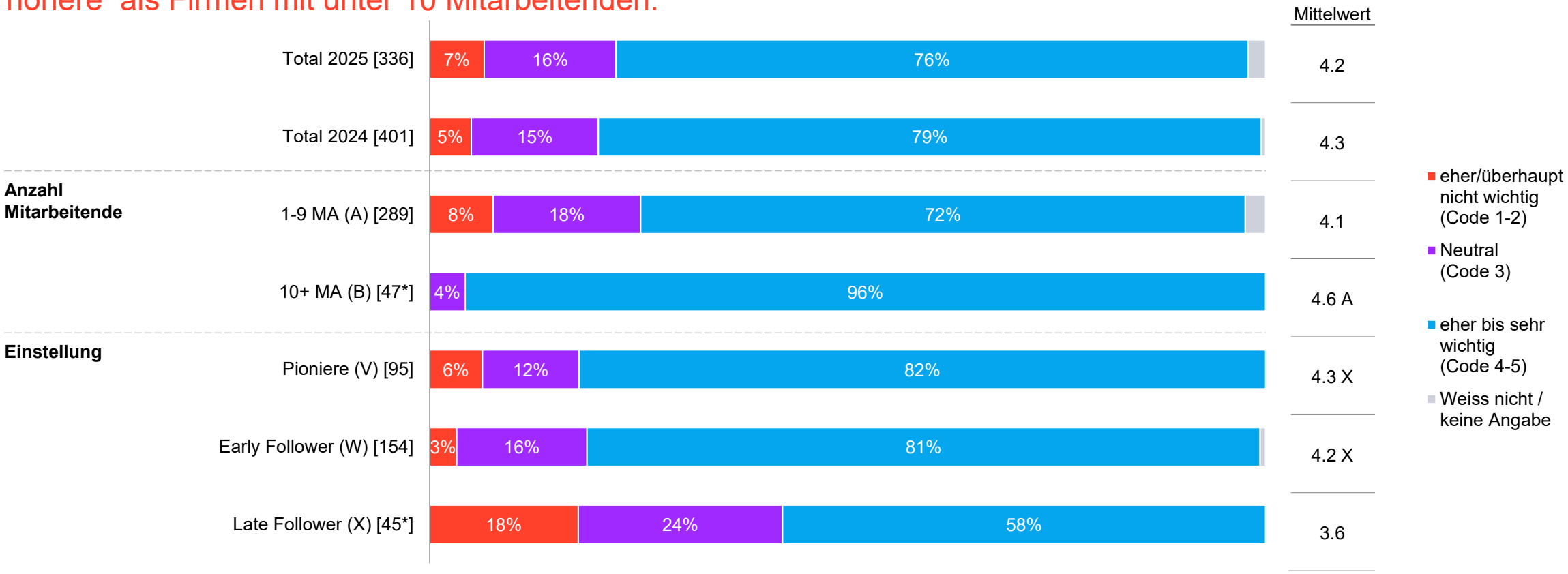
Die befragten IT-Dienstleistungsunternehmen sind der Meinung, dass ihre Kunden deutlich schlechter informiert sind als sie selber: Knapp zwei Fünftel gehen von einem (sehr) guten, rund ein Fünftel von einem (sehr) schlechten Informations-grad der Kunden aus. Der Mittelwert liegt unverändert bei 3.3 (Eigeneinschätzung: 4.1)



F054. Wie gut sind - Ihrer Meinung nach - Ihre Kunden zur Cyberrisk-Thematik informiert?
Basis: n=[ ] | Filter: IT-Dienstleister | Skalierte Fragen (siehe oben) | ▲ signifikant höher als Total; ▼ signifikant tiefer als Total | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle
**Sehr kleine Basis <30 | 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.

Cybersicherheit

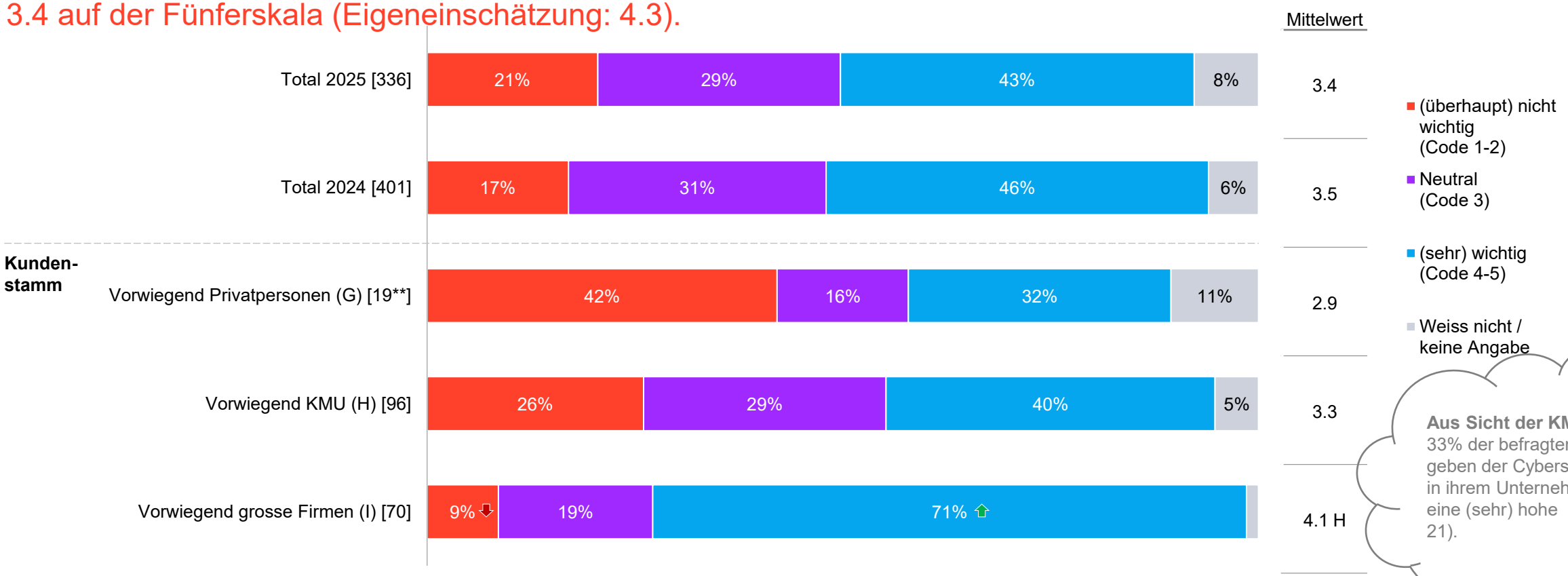
Rund drei Viertel der befragten IT-Dienstleister geben dem Thema Cybersicherheit in ihrer Firma eine (sehr) hohe (Mittelwert 4.2), unverändert zum letzten Jahr. Firmen mit 10+ Mitarbeitenden geben dem Thema eine signifikant höhere als Firmen mit unter 10 Mitarbeitenden.



F011: Welche 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; ▼ signifikant tiefer als Total | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle | *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.

Cybersicherheit bei den Kunden

Gemäss den IT-Unternehmen nehmen ihre Kunden das Thema Cybersicherheit deutlich weniger wichtig als sie selber: Nur rund zwei Fünftel gehen von einer (sehr) hohen Priorität bei den Kunden aus, der Mittelwert liegt bei 3.4 auf der Fünferskala (Eigeneinschätzung: 4.3).



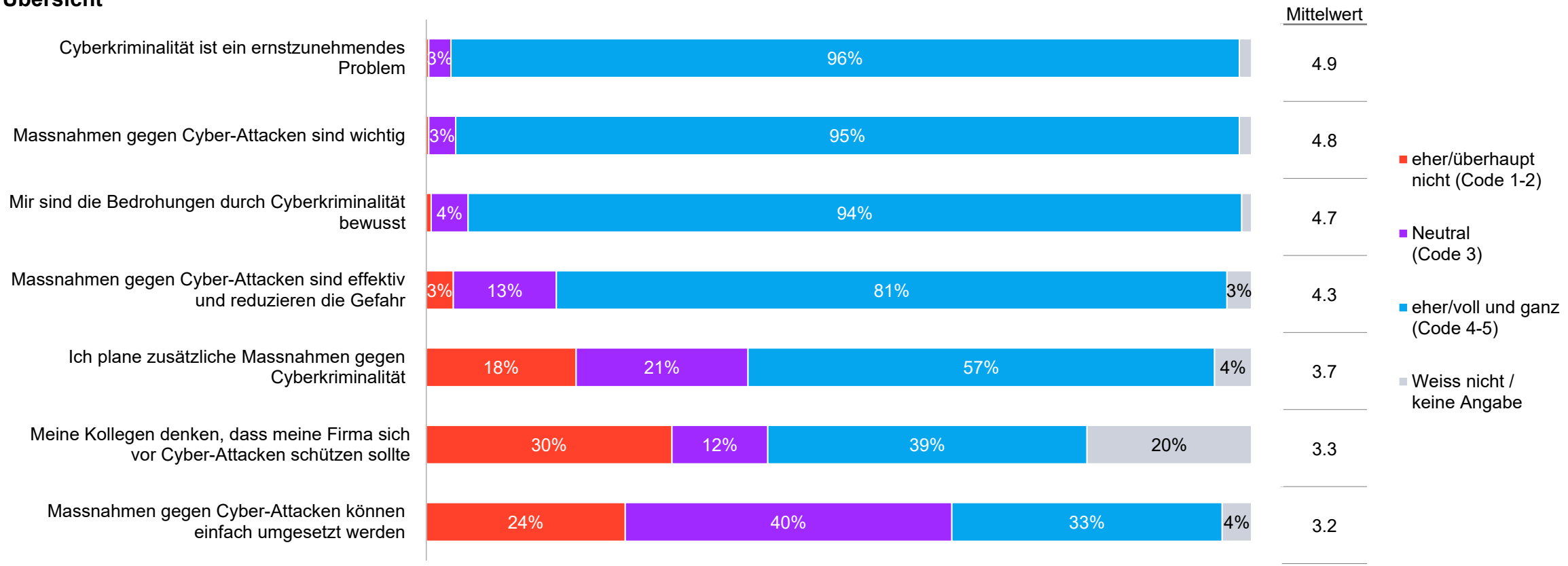
Aus Sicht der KMU…
33% der befragten KMU geben der Cybersicherheit in ihrem Unternehmen eine (sehr) hohe (siehe S. 21).

F055. Was schätzen Sie, alles in allem: Welche hat das Thema Cybersicherheit bei Ihren Kunden?
Basis: n=[ ] | Filter: IT-Dienstleister | Skalierte Fragen (siehe oben) | ▲ signifikant höher als Total; ▼ signifikant tiefer als Total | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle
**Sehr kleine Basis <30 | 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 (1/4)

Fast alle befragten IT-Unternehmer stimmen den Aussagen zu, dass Cyberkriminalität ein ernstes Problem ist, dass Massnahmen dagegen wichtig sind und dass ihnen die Bedrohungen bewusst sind. Rund ein Viertel widerspricht aber der Aussage, dass Massnahmen gegen Cyber-Attacken einfach umgesetzt werden können.

Übersicht

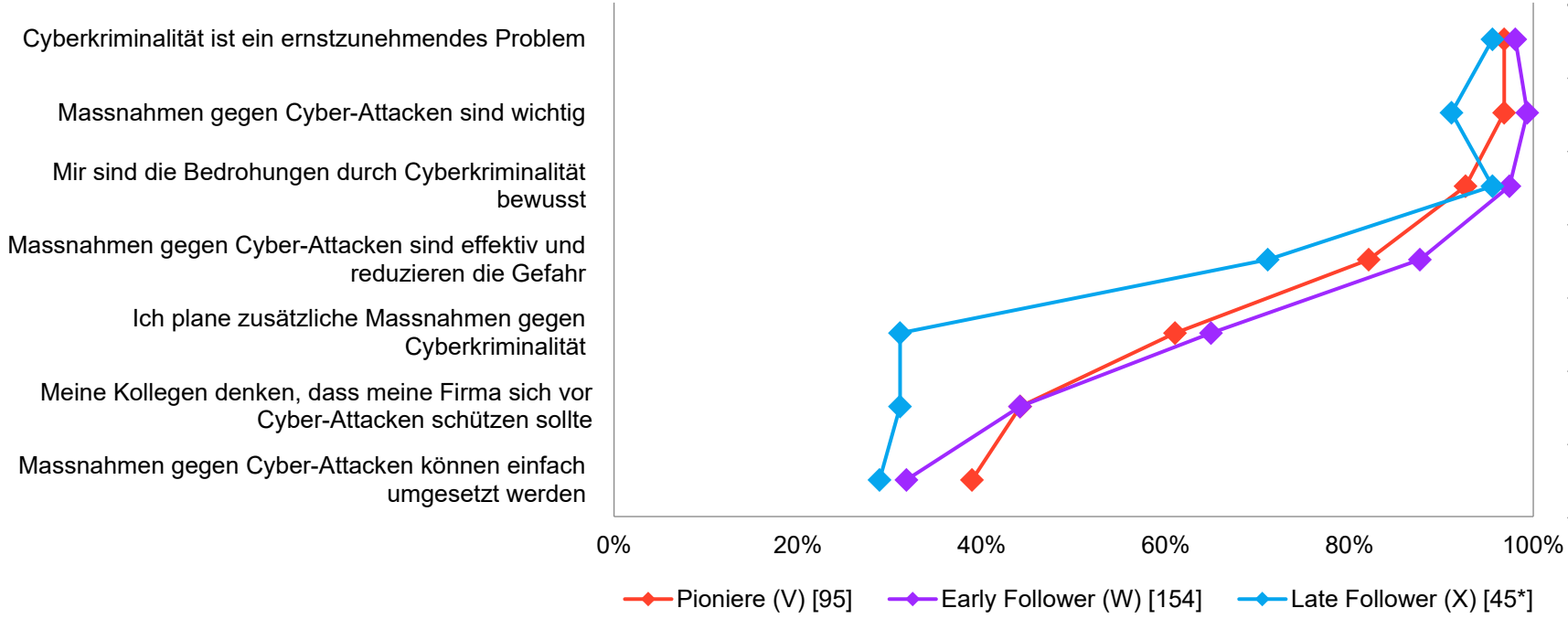


F015: Inwiefern stimmen Sie den folgenden Aussagen zu Cyberkriminalität wie Malware, Online-Betrug und Hacking zu?
Basis: n=336 | Filter: IT-Dienstleister | Skalierte Frage: 1= überhaupt nicht bis 5= voll und ganz | Datenbeschriftung ab 3%

Einstellung zu Cyberkriminalität (2/4)

Pioniere und Early Follower unter den IT-Dienstleistern sind weitgehend gleicher Meinung, wenn es um das Thema Cyberkriminalität geht. Late Follower stimmen aber mehreren Massnahmen (signifikant) weniger zu, insbesondere was die Planung zusätzlicher Massnahmen gegen Cyberkriminalität betrifft.

Nach Einstellung



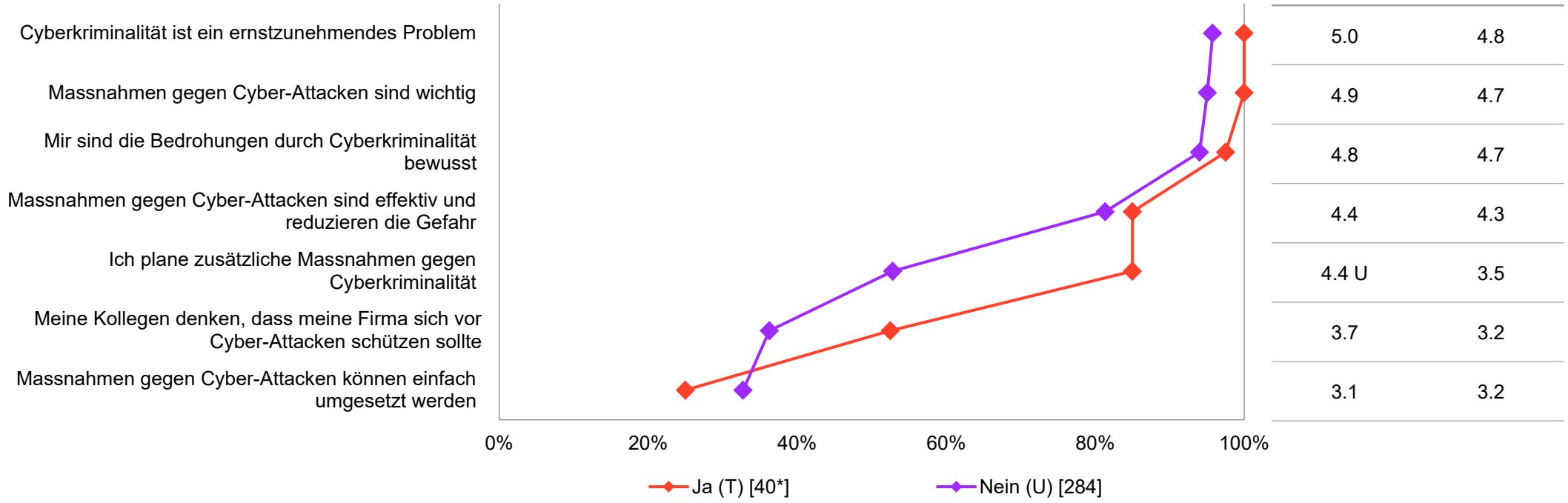
	Mittelwert		
	Pioniere	Early Follower	Late Follower
Cyberkriminalität ist ein ernstzunehmendes Problem	4.9	4.9	4.8
Massnahmen gegen Cyber-Attacken sind wichtig	4.8	4.8 X	4.7
Mir sind die Bedrohungen durch Cyberkriminalität bewusst	4.7	4.7	4.7
Massnahmen gegen Cyber-Attacken sind effektiv und reduzieren die Gefahr	4.3 X	4.3 X	4.0
Ich plane zusätzliche Massnahmen gegen Cyberkriminalität	3.8 X	3.8 X	2.9
Meine Kollegen denken, dass meine Firma sich vor Cyber-Attacken schützen sollte	3.4	3.4	2.9
Massnahmen gegen Cyber-Attacken können einfach umgesetzt werden	3.4 X	3.1	2.9

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 (3/4)

IT-Dienstleister mit IT-Sicherheitszertifikat stimmen sechs von sieben Aussagen zu Cyberkriminalität stärker zu als diejenigen ohne Zertifikat, die Unterschiede sind aber nur in einem Fall signifikant (bezüglich der Planung zusätzlicher Massnahmen gegen Cyber-Attacken).

Nach IT-Sicherheitszertifikat



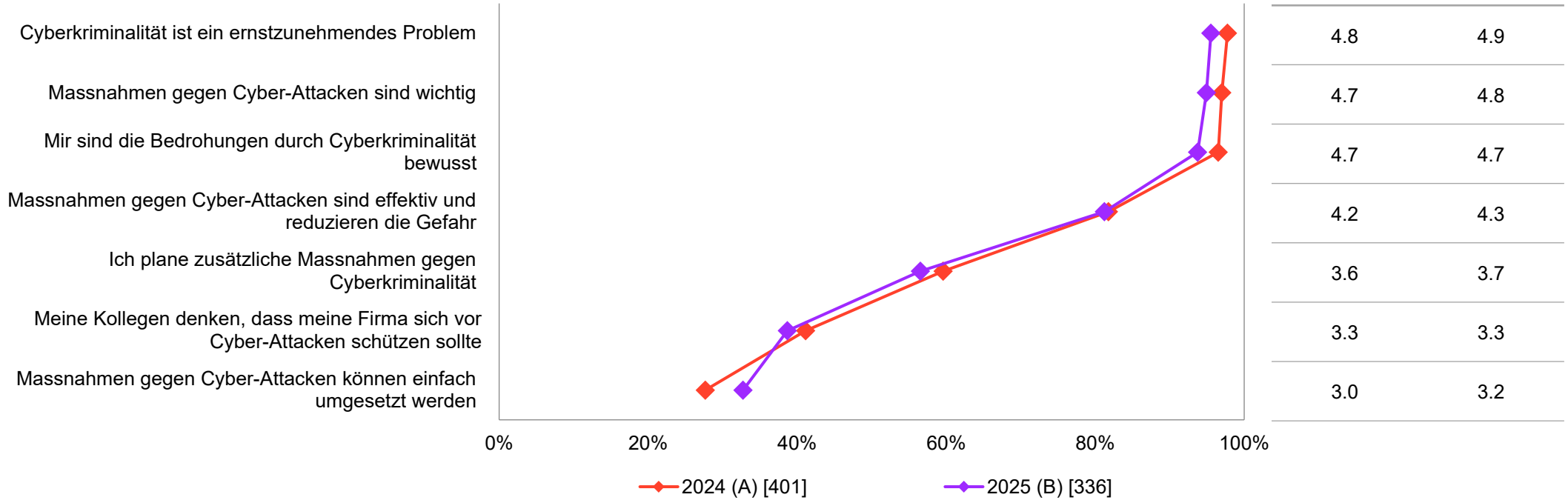
	Mittelwert	
	Zertifikat ja	Zertifikat nein
Cyberkriminalität ist ein ernstzunehmendes Problem	5.0	4.8
Massnahmen gegen Cyber-Attacken sind wichtig	4.9	4.7
Mir sind die Bedrohungen durch Cyberkriminalität bewusst	4.8	4.7
Massnahmen gegen Cyber-Attacken sind effektiv und reduzieren die Gefahr	4.4	4.3
Ich plane zusätzliche Massnahmen gegen Cyberkriminalität	4.4 U	3.5
Meine Kollegen denken, dass meine Firma sich vor Cyber-Attacken schützen sollte	3.7	3.2
Massnahmen gegen Cyber-Attacken können einfach umgesetzt werden	3.1	3.2

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 (4/4)

Das Antwortverhalten der IT-Dienstleister bezüglich der Aussagen zur Cyberkriminalität hat sich seit letztem Jahr nicht verändert.

Jahresvergleich



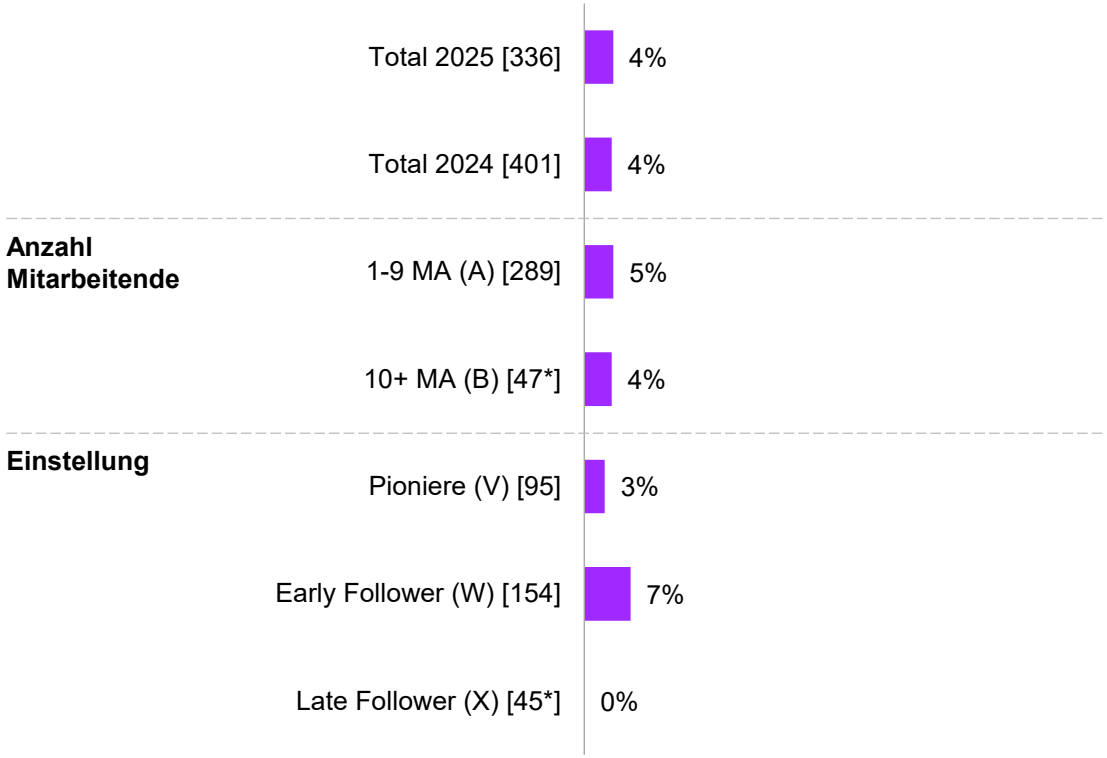
	Mittelwert	
	2024	2025
Cyberkriminalität ist ein ernstzunehmendes Problem	4.8	4.9
Massnahmen gegen Cyber-Attacken sind wichtig	4.7	4.8
Mir sind die Bedrohungen durch Cyberkriminalität bewusst	4.7	4.7
Massnahmen gegen Cyber-Attacken sind effektiv und reduzieren die Gefahr	4.2	4.3
Ich plane zusätzliche Massnahmen gegen Cyberkriminalität	3.6	3.7
Meine Kollegen denken, dass meine Firma sich vor Cyber-Attacken schützen sollte	3.3	3.3
Massnahmen gegen Cyber-Attacken können einfach umgesetzt werden	3.0	3.2

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
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 Cyberangriff erlebt, der Folgen nach sich zog. In 10 von den 15 berichteten Fällen entstand daraus ein grosser Aufwand zur Behebung, in 9 Fällen eine hohe emotionale Belastung, in 5 Fällen ein Reputationsschaden und in 4 Fällen ein finanzieller Schaden. In nur einem Fall gingen Kundendaten verloren.

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



Erlittene Schäden
Basis: 15** | Filter: IT-Dienstleister – wenn Cyberangriff erlitten

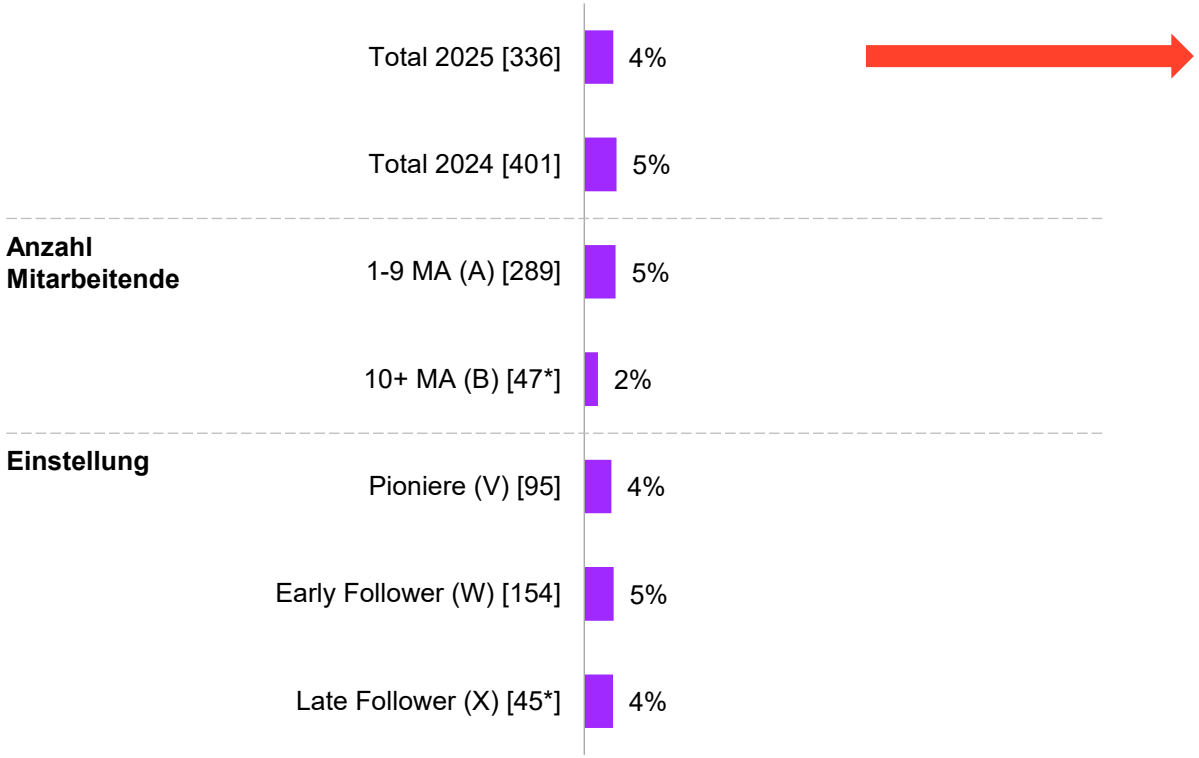
Schäden	Anzahl Fälle
Ein grosser Arbeitsaufwand zur Behebung	10
Emotionale Belastung	9
Ein Reputationsschaden	5
Ein finanzieller Schaden	4
Ein Kundendatenverlust	1
Nichts davon	0
Weiss nicht / keine Antwort	0

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; ⬇ signifikant tiefer als Total | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle | *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

Insgesamt 14 der 336 befragten IT-Unternehmen wurden schon einmal von Cyberkriminellen erpresst; jedoch hat keines von ihnen Lösegeld bezahlt.

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



Lösegeld an Cyberkriminelle
Basis: 14** | Filter: IT-Dienstleister – wenn erpresst durch Cyberkriminelle

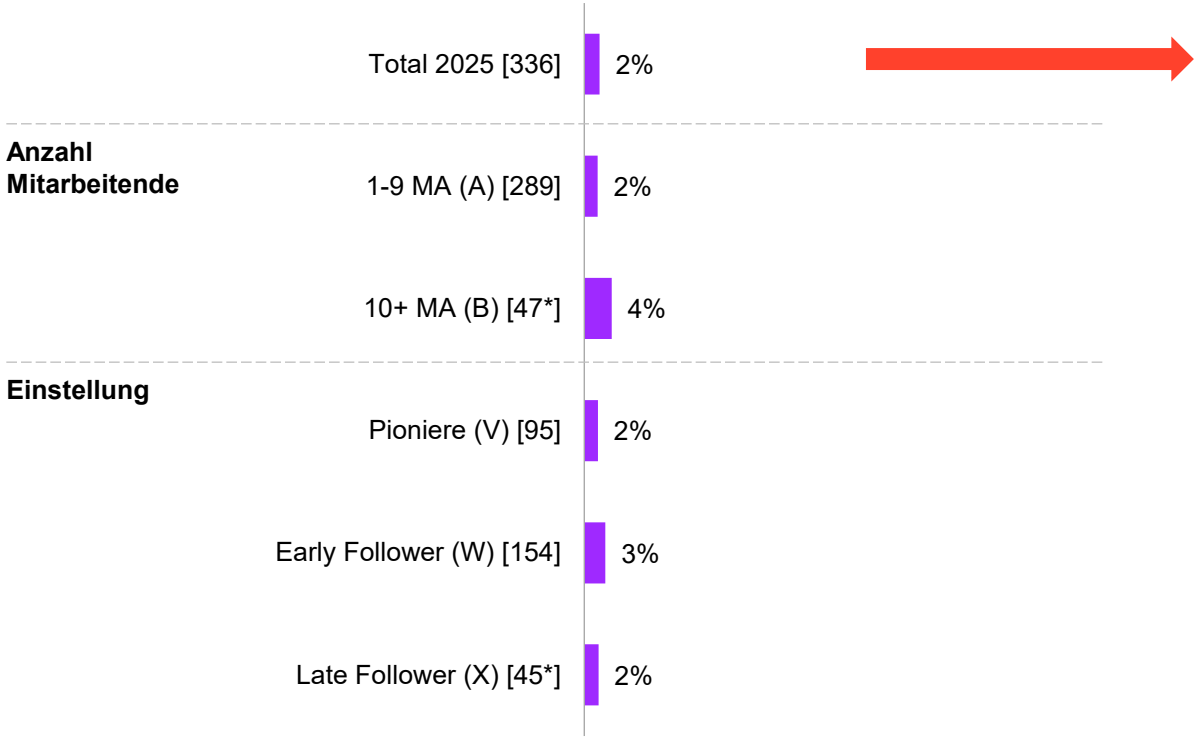
Lösegeld bezahlt	Anzahl Fälle
Ja	0
Nein	14
möchte keine Aussage dazu machen	0

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; ▼ signifikant tiefer als Total | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle | *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.

Geldeinzahlungen aufgrund betrügerischer Mails

2 Prozent der befragten IT-Unternehmen haben schon einmal irrtümlich Geld einbezahlt aufgrund eines betrügerischen E-Mails. Von den acht betroffenen Fällen haben drei ihr Geld zurückgewinnen können, für die anderen fünf war es verloren.

Betrügerische E-Mails (Ja-Anteile)
Basis: [ ] | Filter: IT-Dienstleister



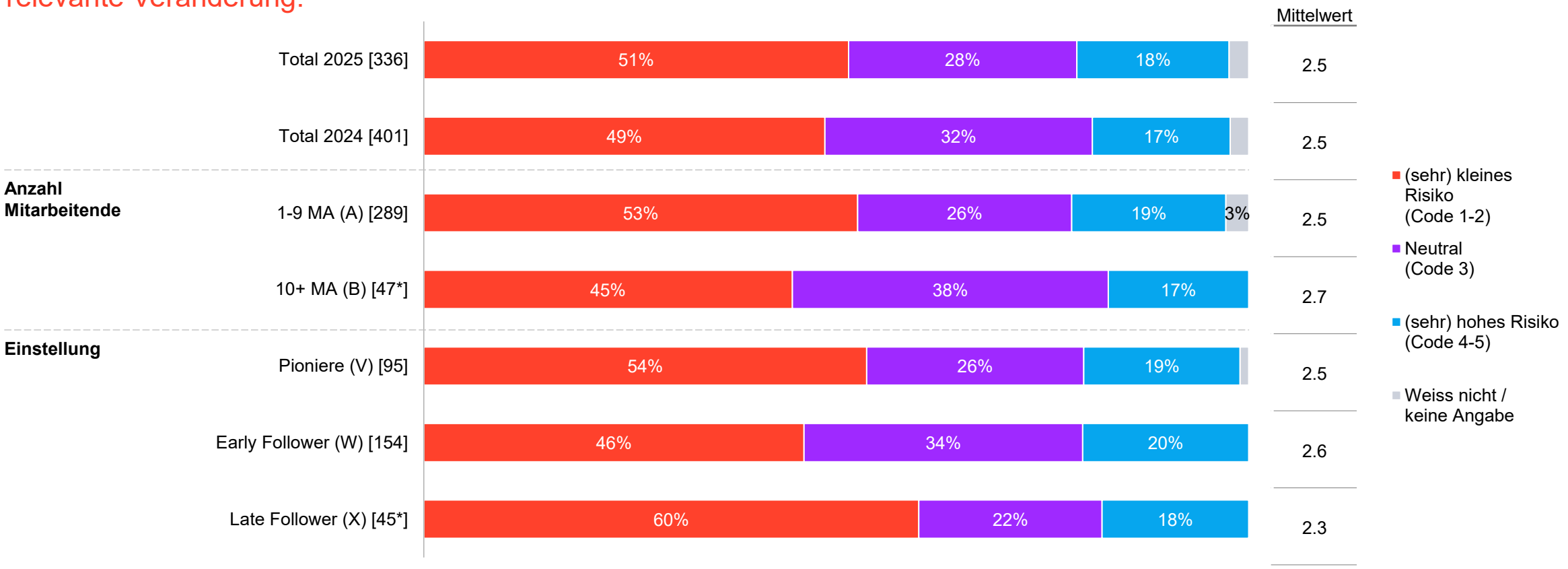
Geldverlust bei Betrug
Basis: n=8*** | Filter: durch betrügerische E-Mails irrtümlich bezahltes Geld

Geld verloren oder zurückgewonnen	Anzahl Fälle
verloren	5
zurückgewonnen	3
weiss nicht / keine Antwort	0

F035: Hat Ihr Unternehmen schon einmal irrtümlich Geld einbezahlt aufgrund eines betrügerischen E-Mails? | F036: War dieses Geld verloren, oder konnten Sie es zurückgewinnen?
Basis: n=[ ] | Filter: siehe oben | Geschlossene Fragen | ⬆ signifikant höher als Total; ⬇ signifikant tiefer als Total | *Kleine Basis <50 | ***Basis zu klein zum Charten
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen. | Neue Frage in 2025

Risikoeinschätzung für eigenes Unternehmen

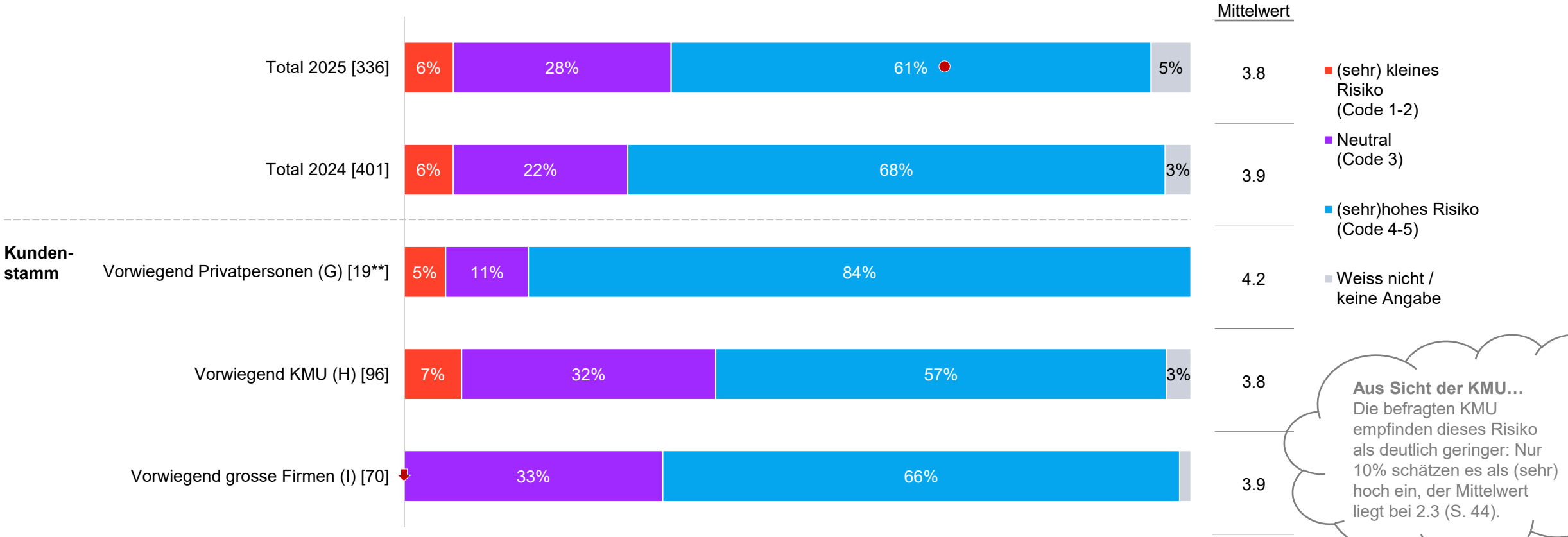
Knapp ein Fünftel der befragten IT-Unternehmen schätzt das Risiko, innerhalb der nächsten 2-3 Jahre durch einen Cyberangriff für mindestens einen Tag ausser Kraft gesetzt zu werden, (sehr) hoch ein; gegenüber 2024 gibt es keine relevante Veränderung.



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; ▼ signifikant tiefer als Total | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle | *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

Fast zwei Drittel der IT-Dienstleister schätzen das Risiko für Schweizer KMU, innerhalb der nächsten 2-3 Jahre durch einen Cyberangriff für mindestens einen Tag ausser Kraft gesetzt zu werden, (sehr) hoch ein. Das ist zwar ein hoher Wert, aber signifikant tiefer als noch 2024.

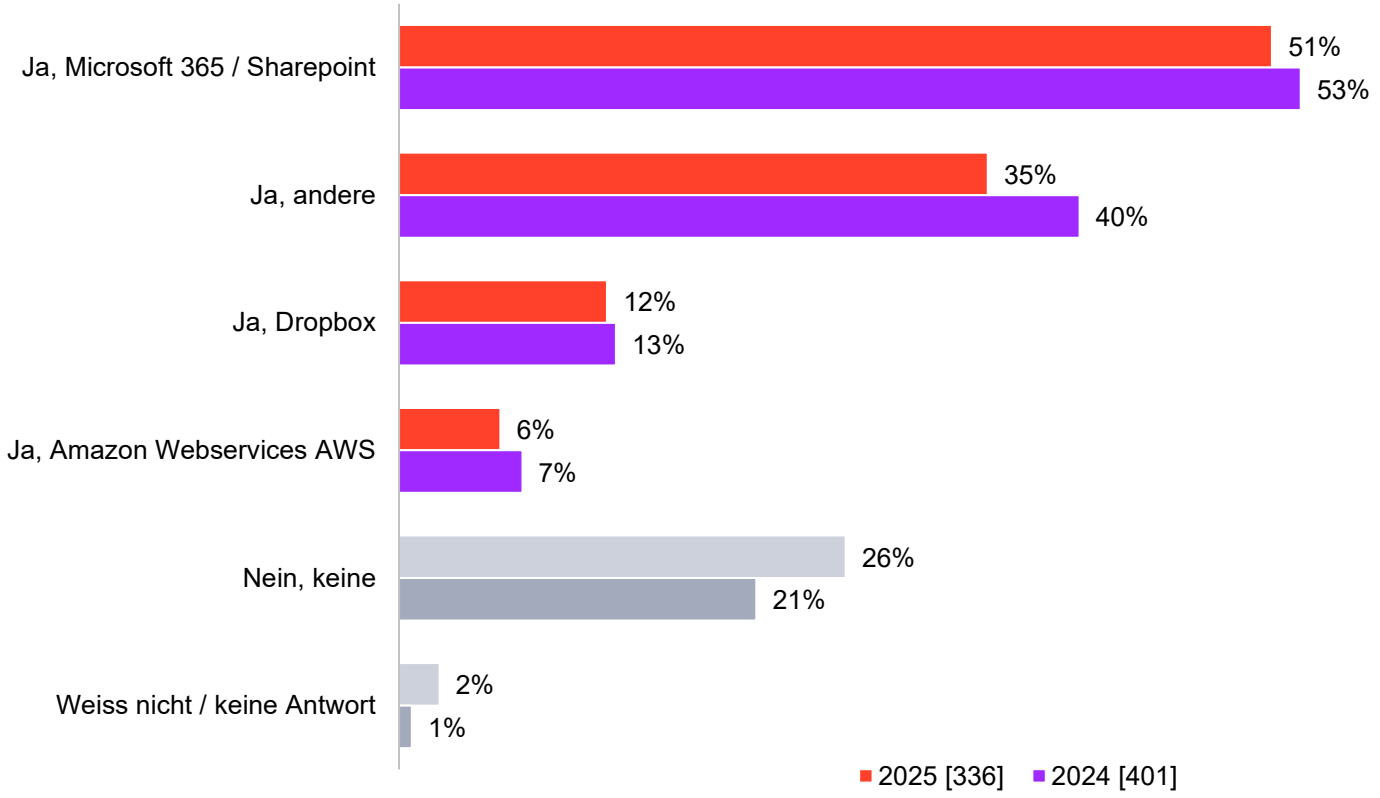


Aus Sicht der KMU…
Die befragten KMU empfinden dieses Risiko als deutlich geringer: Nur 10% schätzen es als (sehr) hoch ein, der Mittelwert liegt bei 2.3 (S. 44).

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=[ ] | Filter: IT-Dienstleister | Skalierte Frage: 1= sehr kleines Risiko bis 5= sehr grosses Risiko | ▲ signifikant höher als Total; ▼ signifikant tiefer als Total | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle
**Sehr kleine Basis <30 | 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.

Cloudnutzung

Knapp drei Viertel der der befragten IT-Dienstleister nutzen Cloud-Lösungen, am ehesten Microsoft 365 bzw. Sharepoint. Die Nutzungszahlen sind leicht (nicht signifikant) zurückgegangen seit 2024.

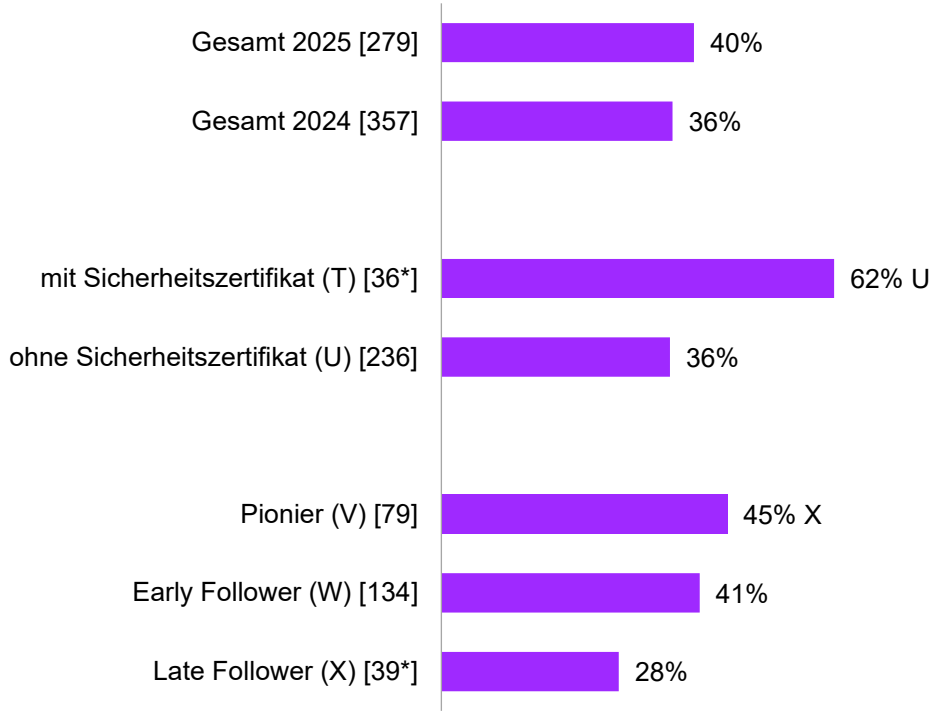


F029: Nutzen Sie für Ihre Datenablage Cloud-Dienstleistungen?
Basis: n=[ ] | Filter: IT-Dienstleister | Geschlossene Frage | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle

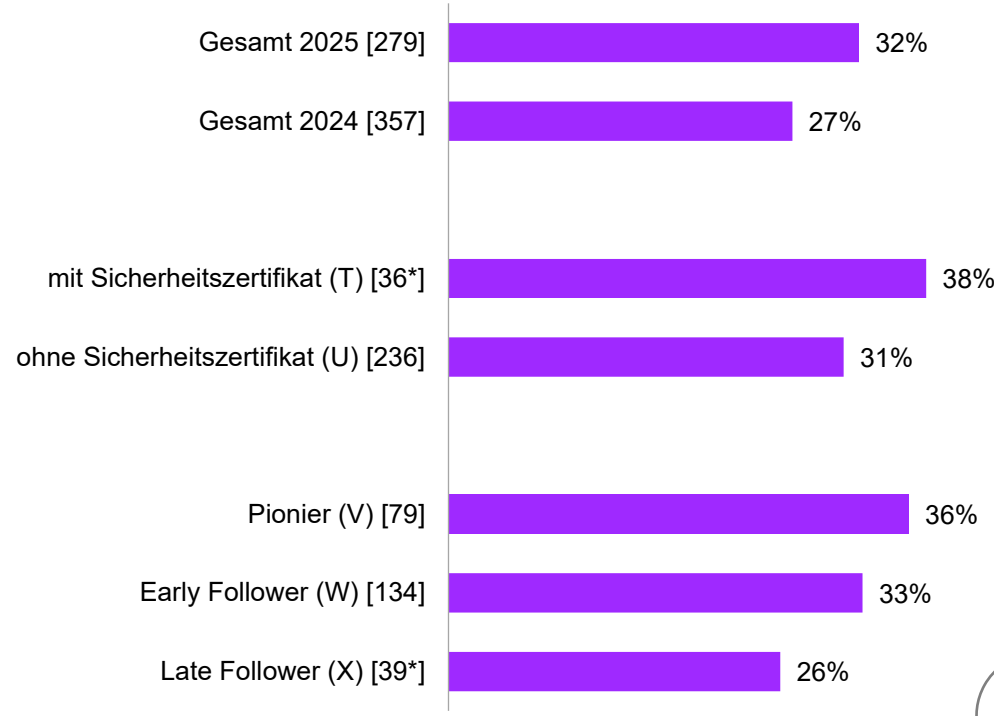
Prozentualer Anteil outgesourcter IT-Arbeiten

Die befragten IT-Dienstleistungsunternehmen sind bei durchschnittlich rund zwei Fünfteln ihrer Kunden für *technische*, bei rund einem Drittel für *organisatorische* Cybersicherheits-Massnahmen mit zuständig. Firmen mit Sicherheitszertifikat sind signifikant häufiger für technische Massnahmen und tendenziell etwas häufiger für organisatorische Massnahmen zuständig.

Zuständig für technische Cybersicherheits-Massnahmen bei durchschnittlich…:



Zuständig für organisatorische Cybersicherheits-Massnahmen bei durchschnittlich…:

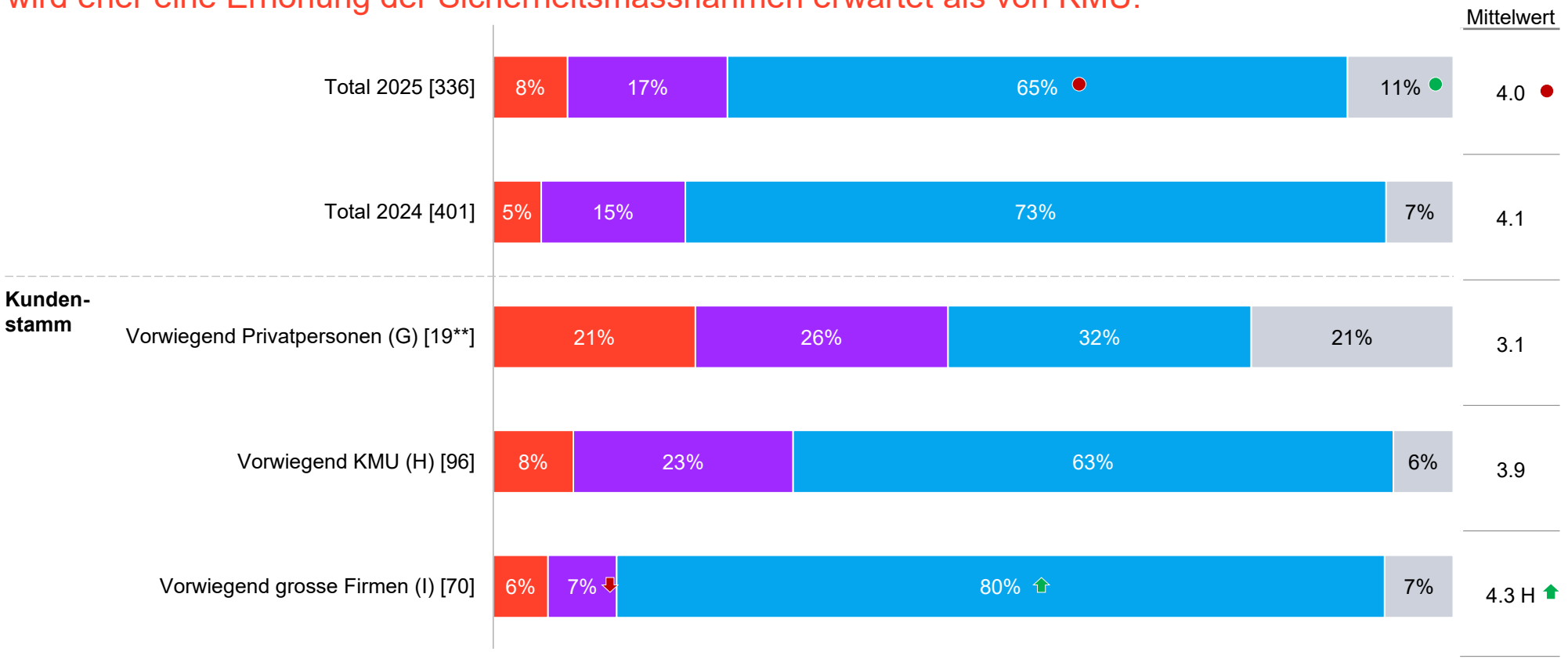


F051: Bei wie vielen Ihrer Kunden sind Sie zumindest teilweise zuständig für…
Basis: n=[ ] | Filter: IT-Dienstleister | Geschlossene Frage ⬆ signifikant höher als Total; ⬇ signifikant tiefer als Total | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle | *Kleine Basis <50

Aus Sicht der KMU…
26% der befragten KMU werden beim Thema Cybersicherheit durch einen externen IT-DL unterstützt (siehe S. 17).

Geplante Verbesserung Sicherheitsmassnahmen

Rund zwei Drittel und somit signifikant weniger der befragten IT-Unternehmen gehen davon aus, dass ihre Kunden in den kommenden 1 bis 3 Jahren ihre Sicherheitsmassnahmen gegen Cyber-Kriminalität erhöhen werden. Von grossen Firmen wird eher eine Erhöhung der Sicherheitsmassnahmen erwartet als von KMU.



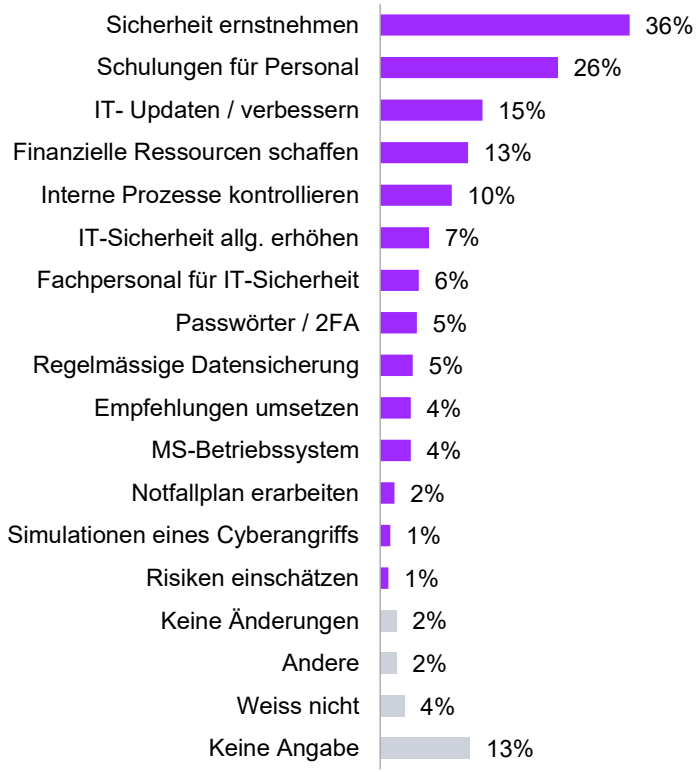
Aus Sicht der KMU…
40% der befragten KMU planen, in den nächsten 1-3 Jahren ihre Cyber-Sicherheitsmassnahmen zu erhöhen (S. 43).

F056. Gehen Sie davon aus, dass Ihre Kunden in den kommenden 1-3 Jahren ihre Sicherheitsmassnahmen gegen Cyber-Kriminalität erhöhen werden?
Basis: n=[ ] | Filter: IT-Dienstleister | Skalierte Fragen (siehe oben) | ⬆ signifikant höher als Total; ⬇ signifikant tiefer als Total | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle
**Sehr kleine Basis <30 | 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.

Empfehlungen bezüglich Cybersicherheit

IT-Dienstleister empfehlen ihren Kunden an erster Stelle, Cybersicherheit ernster zu nehmen. An zweiter Stelle folgt mit Personalschulungen eine wichtige organisatorische Massnahme, und an dritter Stelle das Updaten der IT als wichtige technische Massnahme. Diese Reihenfolge hat sich seit 2024 nicht verändert.

Verbesserungspotential



F059: Was müssten Ihre Kunden bezüglich Cybersicherheit besser machen?
Basis: n=336 | Filter: IT-Dienstleister | Offene Frage

Gesunden Menschenverstand verwenden. Nicht auf die Verkäufer hören, die ihnen ein Wunder-Produkt verkaufen wollen. Awareness für die IT-Sicherheit schaffen und periodisch wiederholen.

1) Schulung Mitarbeiter geg. Phishing (Risiko Nr 1!!!)
2) Die einfachen, billigen Massnahmen sofort umsetzen
3) Auch Validierung der Info/Daten in das Schutz-Konzept einbringen

Dranbleiben!

Backup, Backup, Backup

S'informer, s'équiper, se protéger

Sensibilisierung auf Bedrohungen wie z.B. Phishing, Impersonation, Social Engineering bei ALLEN Mitarbeitern

Bereit sein, in Cyber Sicherheit zu investieren. Die Tendenz ist zunehmend, aber noch immer gibt es gerade im KMU-Umfeld viele Unternehmen, die glauben, sie seien kein lukratives Ziel.

mehr Investitionen in die Cybersicherheit auf allen Ebenen (technisch/organisatorisch/Schulung)

Sich dem Risiko bewusst sein, Angriffsmöglichkeiten soweit wie möglich reduzieren. ABER vor allem einen Recovery Plan haben

sich besser informieren / Budgets bereit stellen

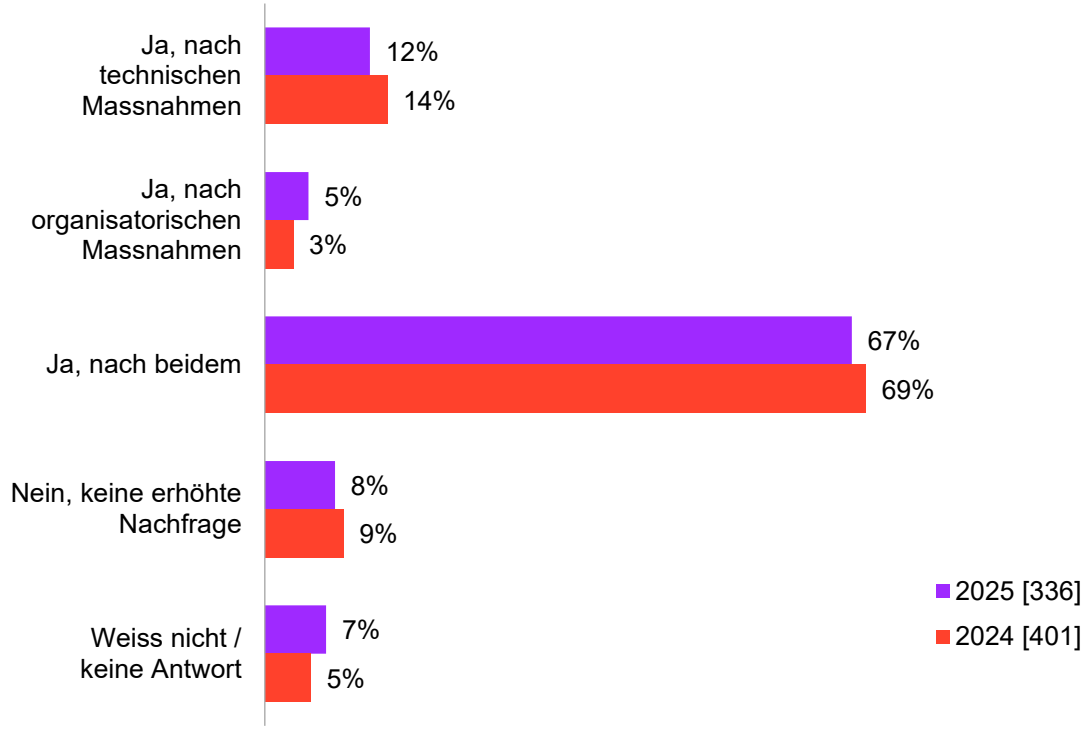
Nur wirklich bestausgebildete Profis beauftragen.

Kritischer prüfen, welche IT Services bezogen werden und was diese machen. Links zu externen Systemen und vor allem Services sind oft intransparent

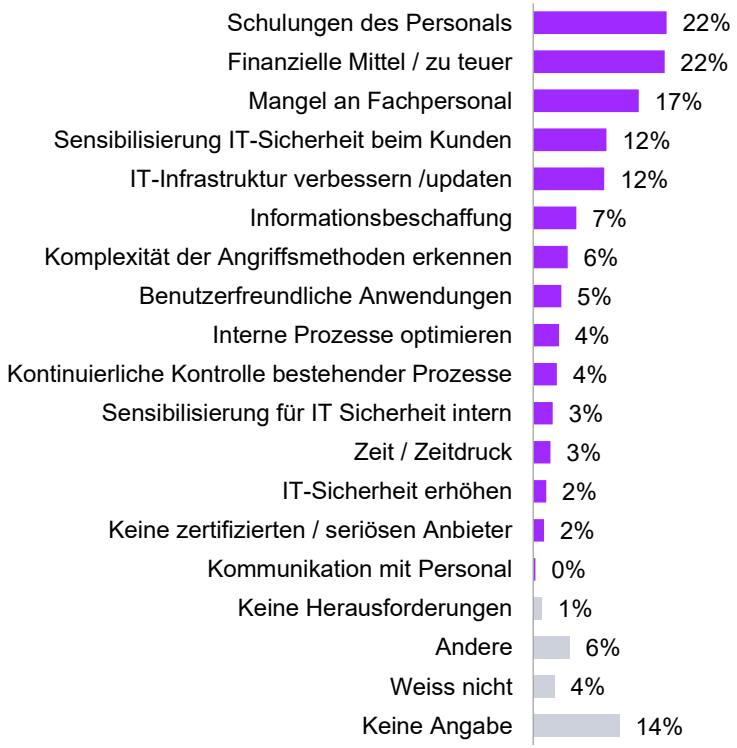
Cybersicherheits-Nachfrage in Zukunft

Wie schon 2024 erwarten rund 8 von 10 befragten IT-Unternehmen 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=283 | Filter: IT-Dienstleister – erhöhte Nachfrage erwartet



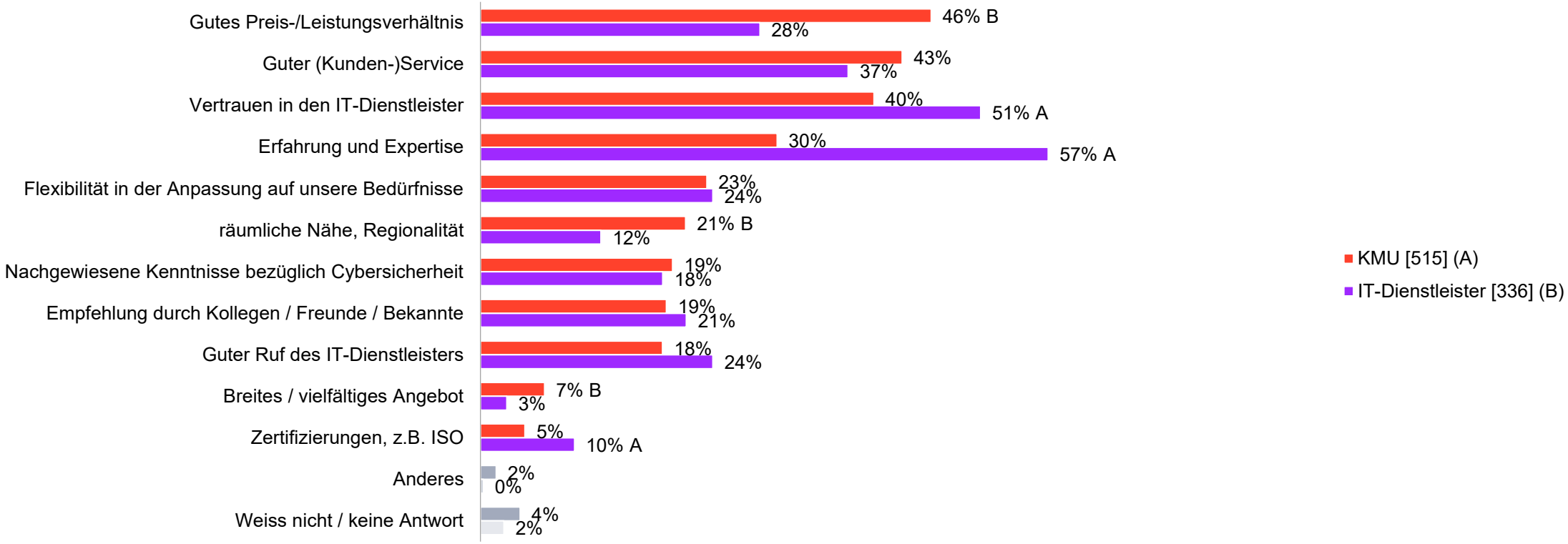
Aus Sicht der KMU…
40% der befragten KMU möchten in den kommenden 1-3 Jahren ihre Cybersicherheits-Massnahmen erhöhen (siehe Folie 43).

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 Zielgruppen-vergleiche

Auswahlkriterien IT-Dienstleister

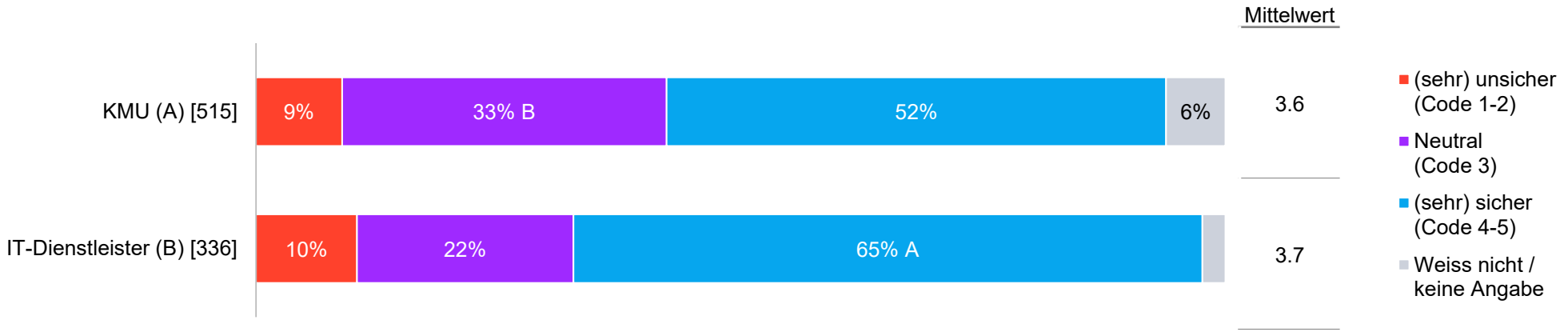
Die Wichtigkeit von Vertrauen und Erfahrung/Expertise wird von den IT-Dienstleistern viel höher bewertet als von den KMU, während die KMU ein gutes Preis-/Leistungsverhältnis und guten (Kunden-)Service höher gewichten als IT-Dienstleister. Auch die Wichtigkeit von räumlicher Nähe schätzen IT-Dienstleister auffallend tiefer ein als KMU.



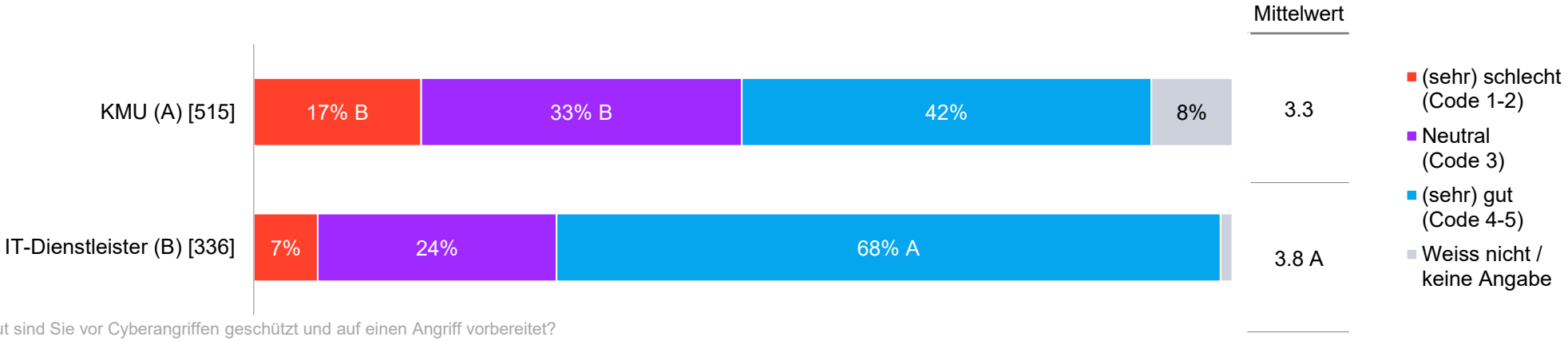
F050: Welche der folgenden Kriterien sind aus Ihrer Sicht für die Auswahl eines IT-Dienstleisters am wichtigsten? Bitte wählen Sie max. 3 Antworten aus.
Basis: n=[ ] | Filter: Alle Befragten | Geschlossene Frage | Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Sicherheitsgefühl und Resilienz

IT-Dienstleister fühlen sich signifikant sicherer als KMU. Das Resilienz-Gefühl liegt bei KMU tiefer als das Sicherheitsgefühl; sie fühlen sich also weniger gut geschützt und vorbereitet, als sie sich sicher fühlen.



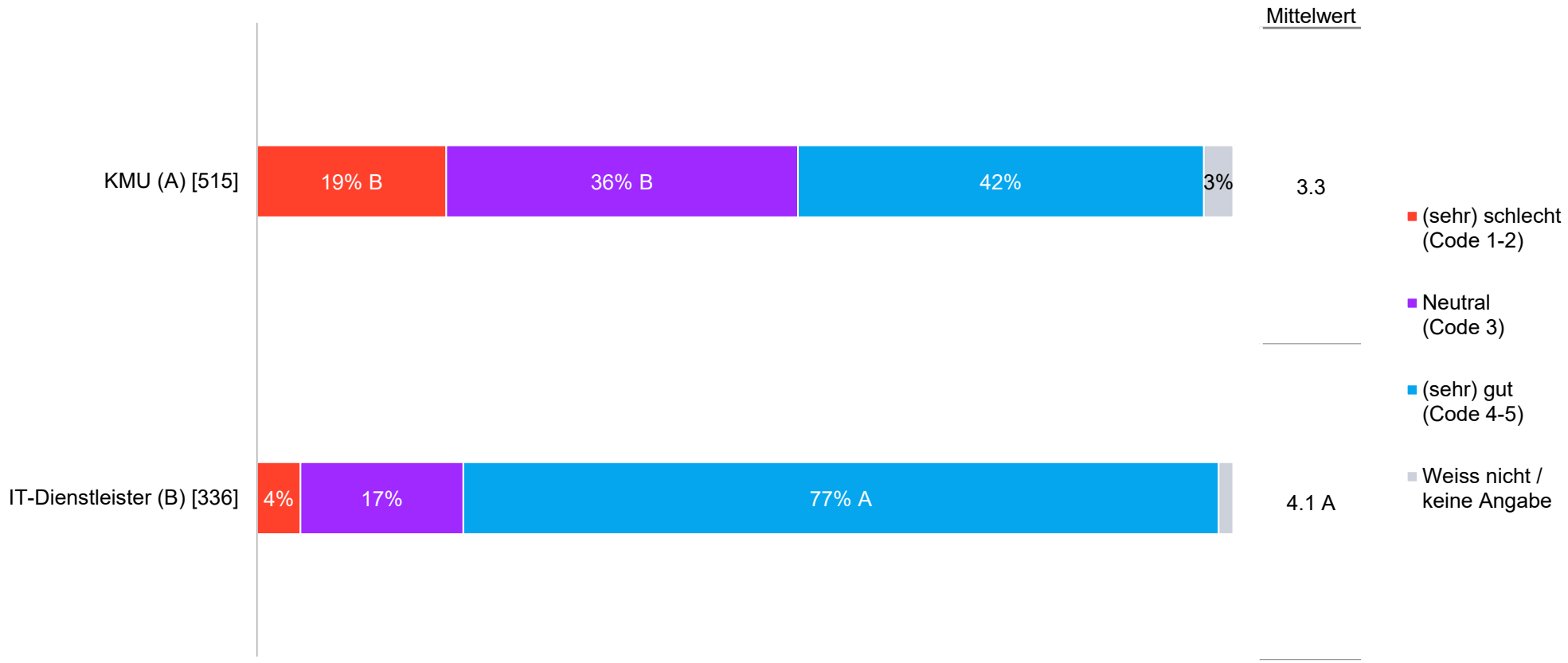
F007: Wie sicher fühlen Sie sich in Ihrem Unternehmen vor Cyberkriminalität? / Wie bewerten Sie die Cybersicherheit Ihres Haushalts?
Basis: n=[ ] | Filter: Alle Befragten | Skalierte Frage: 1= sehr unsicher bis 5= sehr sicher | Datenbeschriftung ab 3%
Die hinter den Mittelwert gesetzten Buchstaben bedeuten 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 deutlich besser informiert als KMU, wie sie sich vor Cyberangriffen schützen können.



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

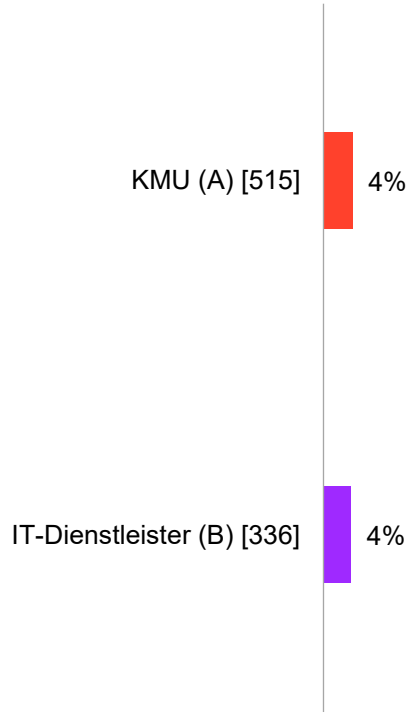
IT-Dienstleister stimmen allen Aussagen stärker zu als KMU; einzig bei den Aussagen, dass Massnahmen gegen Cyber-Attacken einfach umsetzbar sind und dass die Kollegen denken, dass sich die Firma vor Cyber-Attacken schützen sollte, sind die beiden Gruppen gleicher Meinung.

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

Beide Zielgruppen haben im selben Ausmass (4%) Angriffe erlitten, die Folgen nach sich zogen. Während KMU eher von finanziellen Schäden berichten als IT-Dienstleister, scheinen Reputationsschäden nur für IT-Dienstleister ein Thema zu sein.

Erlittene Angriffe (Ja-Anteile)
Filter: Alle Befragten



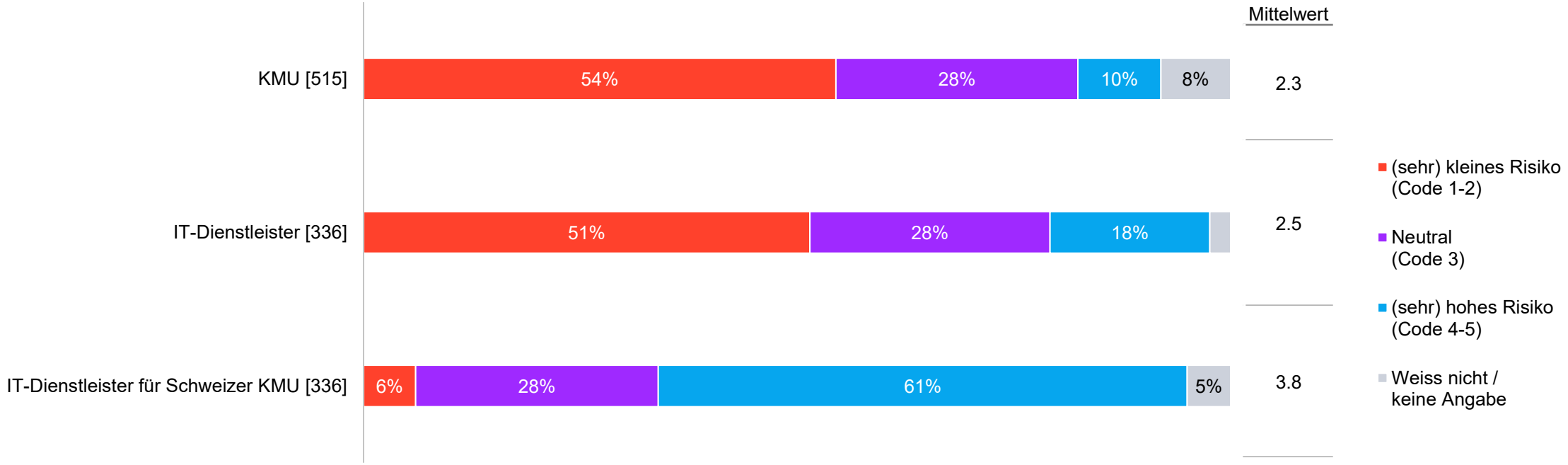
Erlittene Schäden
Filter: Alle Befragten – wenn Cyberangriff erlitten

Schäden	KMU n=23** **Anzahl Fälle**	IT-Dienstleister n=15** **Anzahl Fälle**
Ein grosser Arbeitsaufwand zur Behebung	10	10
Emotionale Belastung	14	9
Ein Reputationsschaden	0	5
Ein finanzieller Schaden	12	4
Ein Kundendatenverlust	1	1
Nichts davon	1	0
Weiss nicht / keine Antwort	0	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? / 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 | **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 für eigenes Unternehmen / Schweizer KMU

Die Einschätzung des *eigenen* Risikos, innerhalb der nächsten 2-3 Jahre durch einen Cyberangriff mindestens einen Tag lang ausser Kaft gesetzt zu werden, wird von den IT-Dienstleistern höher eingeschätzt als von KMU (obwohl sie sich sicherer und besser geschützt fühlen). Fragt man die IT-Dienstleister nach dem Risiko für Schweizer KMU, so schätzen sie dieses noch viel höher 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? / 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.

YouGov

Thank you

/Research Reality | business.yougov.com