

YouGov

Switzerland

KMU Cybersicherheit 2026

Eine Mobiliar Studie in Zusammenarbeit mit BACS,
digitalswitzerland, HES-SO, HWZ und SATW

Oktober 2026

/Research Reality | business.yougov.com

Projektteam

	Marc K. Peter Professor für Digital Business HES-SO Valais-Wallis School of Management marckurt.peter@hes-so.ch			Anna V. Rozumowski Dozentin & Studiengangleiterin HWZ Hochschule für Wirtschaft anna.rozumowski@fh-hwz.ch	
	Anu Anthamatten Senior Project Manager digitalswitzerland anu@digitalswitzerland.com			Tobias Schlegel Leiter Tech Intelligence Schweizerische Akademie der Technischen Wissenschaften SATW tobias.schlegel@satw.ch	
	Léonard Marbe Senior Marketing Manager Die Mobiliar leonard.marbe@mobiliar.ch			Romain Geiser Program Manager NCS Bundesamt für Cybersicherheit ncs@ncsc.admin.ch	

Sowie: Bettina Mavrommatis (BACS), Kenza Leclere (BACS), David Torcasso (digitalswitzerland), Karin Mändli Lerch (YouGov), Thomas Burkhardt (YouGov)

Inhalt

01 Management Summary

02 Studiendesign

03 Stichprobenstruktur

04 Resultate:
04.1 Cybersicherheit
04.2 Digitale Strategie und ESG

01 Management Summary

Die wichtigsten Entwicklungen gegenüber 2025

Deutliche Veränderungen

- Cyberrisiken werden häufiger organisatorisch verankert; insbesondere die Zuständigkeit als interne Teilaufgabe nahm von 15% auf 21% zu (Folie 21).
- Die Bedeutung von Cybersicherheit ist gegenüber 2025 wieder gestiegen; 46% stufen das Thema als (sehr) wichtig ein (2025: 33%) (Folie 25).
- Homeoffice ist weiter verbreitet: 61% der KMU bieten ihren Mitarbeitenden zumindest teilweise Homeoffice an (2025: 50%) (Folie 62).
- Der Anteil der Unternehmen ohne besondere Cybersicherheitsmassnahmen für Homeoffice sank von 44% auf 28% (Folie 63).

Kaum Veränderungen

- Das Sicherheitsgefühl gegenüber Cyberkriminalität bleibt weitgehend stabil (Folie 22).
- Die Risikoeinschätzung eines Cyberangriffs mit Betriebsausfall verändert sich kaum (Folie 53).
- Viele technische und organisatorische Schutzmassnahmen verharren auf ähnlichem Niveau wie in den Vorjahren (Folien 31, 37)

Cyberangriffe werden relevanter

- 6% der KMU berichten von einem erfolgreichen Cyberangriff innerhalb der letzten drei Jahre (Folie 48).
- Unternehmen mit 10-49 Mitarbeitenden sind deutlich häufiger betroffen (13-16%) (Folie 48).
- Die Folgen erfolgreicher Angriffe sind häufiger operativ und persönlich als unmittelbar finanziell (Folie 48).
- 7% der Unternehmen wurden bereits durch Cyberkriminelle erpresst (Folie 50).
- Rund jedes sechste von Erpressung betroffene Unternehmen hat Lösegeld bezahlt (Folie 50).

Cybersicherheit ist heute vor allem eine Frage der Umsetzung

- Cyberkriminalität wird von der grossen Mehrheit der KMU als ernstzunehmende Bedrohung wahrgenommen (Folie 41).
- Schutzmassnahmen gelten mehrheitlich als wichtig und wirksam (Folie 41).
- Gleichzeitig bleiben Sicherheitskonzepte, Notfallpläne, Mitarbeiter-Schulungen und Sicherheitsaudits vergleichsweise wenig verbreitet (Folie 33, 40).
- Viele KMU fühlen sich ausreichend über Cyberbedrohungen informiert und wissen nach eigener Einschätzung, wo sie im Ernstfall Unterstützung erhalten (Folie 54). Gleichzeitig sind organisatorische Vorkehrungen vergleichsweise wenig verbreitet (Folie 33, 40).
- Die Ergebnisse deuten auf eine Lücke zwischen wahrgenommener und organisatorisch verankerter Cyber-Resilienz hin.

Informationsgrad und Reifegrad hängen eng zusammen

- Gut informierte Unternehmen setzen technische und organisatorische Sicherheitsmassnahmen häufiger um (Folien 29, 35).
- Sie beurteilen Schutzmassnahmen häufiger als wirksam und umsetzbar (Folie 43).
- Sie planen häufiger zusätzliche Sicherheitsmassnahmen (Folie 52).
- Technologische Pioniere weisen über viele Themen hinweg höhere Reifegrade auf als Late Follower.

Digitalisierung und externe Unterstützung prägen die Praxis

- Digitale Strategiemassnahmen konzentrieren sich auf Kundenzufriedenheit, Datennutzung und Prozessoptimierung (Folie 58).
- Für die Cybersicherheit spielen externe IT-Dienstleister für viele KMU eine zentrale Rolle; bei Unternehmen mit mehr als drei Mitarbeitenden verlassen sich rund zwei Drittel auf externe Partner (Folie 20).
- Im Durchschnitt werden 38.5% der IT-Sicherheitsaufgaben an externe Dienstleister übertragen (Folie 20).

02 Studiendesign

Studiendesign

Auftraggeber_innen:	HES-SO Fachhochschule Westschweiz (Prof. Dr. Marc K. Peter) digitalswitzerland (Kristof Hertig) Die Mobiliar (Léonard Marbe) HWZ (Dr. Anna Rozumowski) Schweizerischen Akademie der Technischen Wissenschaften SATW (Tobias Schlegel)
YouGov:	Karin Mändli Lerch Senior Research Consultant Thomas Burkhardt Junior Research Consultant
Studienziel:	Erhebung der Einstellung von Schweizer KMU zu den Themen Cybersicherheit & Digitalisierung
Erhebungsphase:	24. Juni bis 10. Juli 2026
Zielgruppe:	KMU mit 1 bis 49 Mitarbeitenden Funktion: Alleinige oder gemeinsame Entscheidungen in Bezug auf Unternehmensstrategie in ihrem Unternehmen
Anzahl Interviews:	n = 507 Interviews
Befragungsmethode:	Online-Fragebogen
Einladungsverfahren:	YouGov Internet-Panel: Das YouGov Internetpanel ist ein probability based Panel und erlaubt damit eine Projektion der Studienresultate auf die befragte Grundgesamtheit. Es umfasst rund 115'000 validierte, zu 100% aktiv rekrutierte Mitglieder. Eingeladen wurden Personen die alleine oder gemeinsam mit anderen für Strategie-Entscheidungen in einem KMU (1-49 Mitarbeitende) verantwortlich sind.
Gewichtung:	Die Stichprobe wurde mittels Quoten nach Firmengrösse 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.

Studiendesign

Gewichtung KMU-Stichprobe

	Erhobene Stichprobe (disproportional)		Repräsentative Gewichtung gem. STATENT 2023 (proportional)	
1 – 3 MA	166	33%	378	75%
4 – 9 MA	156	31%	83	16%
10 – 19 MA	108	21%	29	6%
20 – 49 MA	77	15%	17	3%
D-CH	340	67%	350	69%
W-CH	96	19%	127	25%
Tessin	71	14%	30	6%
Total (gerundet)	507	100%	507	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 Prozentpunkten bei einer Sicherheit von 95 Prozent (50/50 Verteilung). Die gewichtete Stichprobe zeigt ein bezüglich Firmengrössen und Sprachregionen strukturgleiches Abbild der Grundgesamtheit, die Ergebnisse sind somit unter Berücksichtigung des Vertrauensintervalls auf die Grundgesamtheit extrapolierbar.

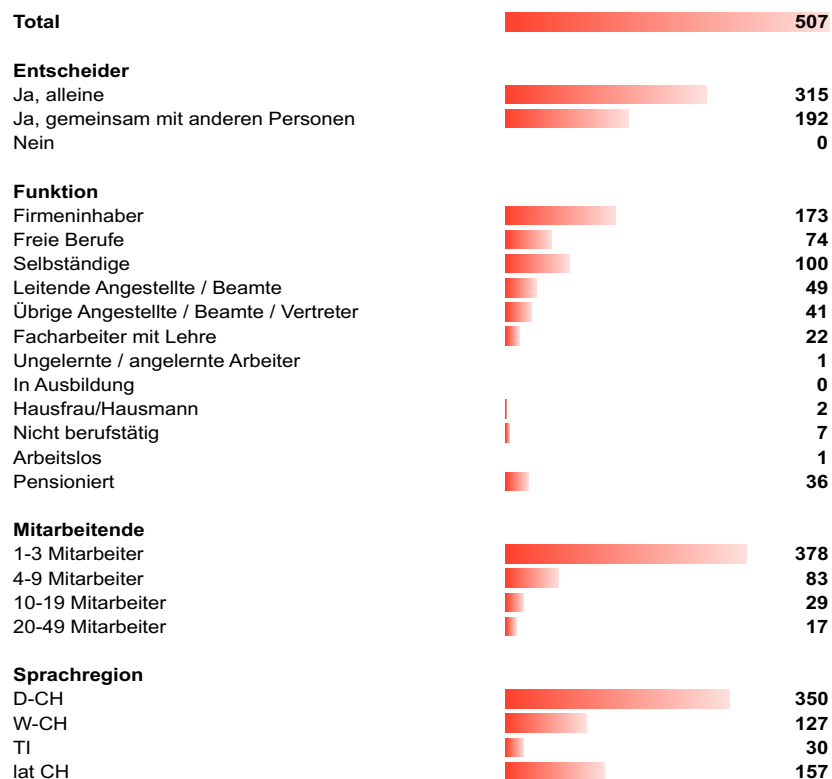
Abgebildete Grundgesamtheit

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

03 Stichproben- struktur

Stichprobenstruktur (gewichtet)



04 Resultate

04.1 Cybersicherheit

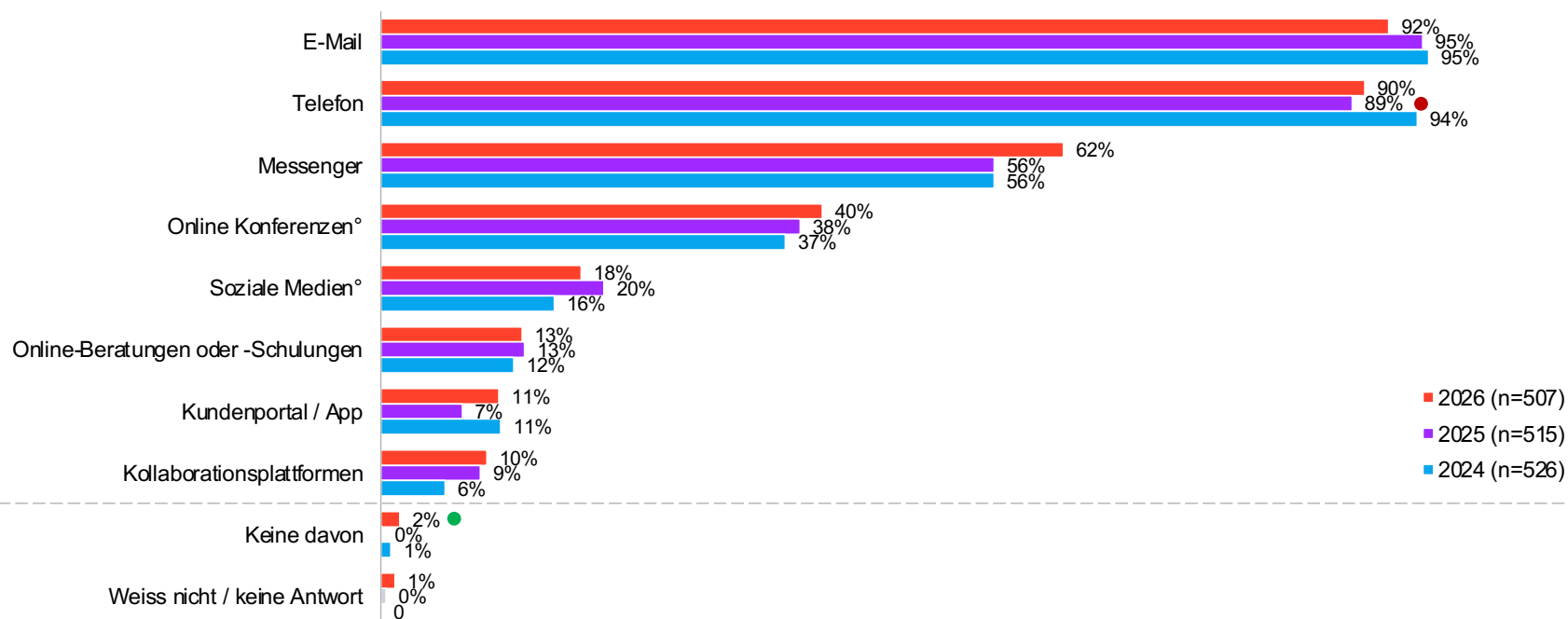
Branche und Firmengrösse

	Gesamt	1-3	4-9	10-19	20-49
Ungewichtete Basis Netto	507	166	156	108	77
Basis Netto	507	378	83	29	17
Gesundheitswesen	12%	14%	9%	4%	6%
Wirtschaftliche, technische oder wissenschaftliche DL	11%	13%	5%	6%	10%
Andere Dienstleistungen (Friseursalon, Entsorgung, ...)	10%	12%	6%	5%	2%
Informatik	8%	9%	8%	6%	6%
Baugewerbe (Hoch-, Tiefbau, Baunebengewerbe)	7%	6%	9%	7%	9%
Bildungswesen	6%	7%	3%	7%	14%
Immobilien	5%	5%	6%	3%	0%
Architektur- und Ingenieurbüro	5%	5%	6%	3%	4%
Bank-, Kredit-, Finanzwesen	4%	4%	5%	5%	0%
Industrie / Verarbeitung und Herstellung von Waren	3%	2%	8%	11%	9%
Kommunikation (Medien, Telekommunikation, Agentur, Marketing, ...)	3%	3%	4%	0%	0%
Gastgewerbe / Tourismus	3%	2%	5%	8%	4%
Unterhaltung, Kultur, Kunst, Erholung, Sport	3%	3%	3%	1%	3%
Grosshandel	3%	3%	3%	4%	0%
Handel / Reparatur (Motorfahrzeuge, Maschinen, ...)	2%	2%	5%	2%	3%
Detailhandel	2%	1%	4%	6%	3%
Öffentliche Verwaltung, öff. Hand (Sicherheit, Sozialversicherung, ...)	2%	2%	1%	5%	9%
Sozialwesen	2%	1%	2%	4%	3%
Energie	1%	1%	3%	4%	8%
Verkehr, Lagerei, Logistik	1%	1%	1%	4%	4%
Chemie / Pharma / Biotechnologie	1%	1%	1%	2%	4%
Versicherungen	1%	1%	1%	2%	1%
Weiss nicht / keine Antwort	3%	4%	1%	1%	0%

S05: In welcher Branche ist Ihr Betrieb tätig? / S03 Anzahl Mitarbeitende
 Basis: n=507 | Filter: KMU | Geschlossene Frage

Kommunikationsmittel

Die Haupt-Kommunikationsmittel sind immer noch E-Mail und Telefon, an dritter und vierter Stelle folgen Messengerdienste und Online Konferenzen mit tendenziell wachsendem Nutzeranteil (Steigerung nicht signifikant).

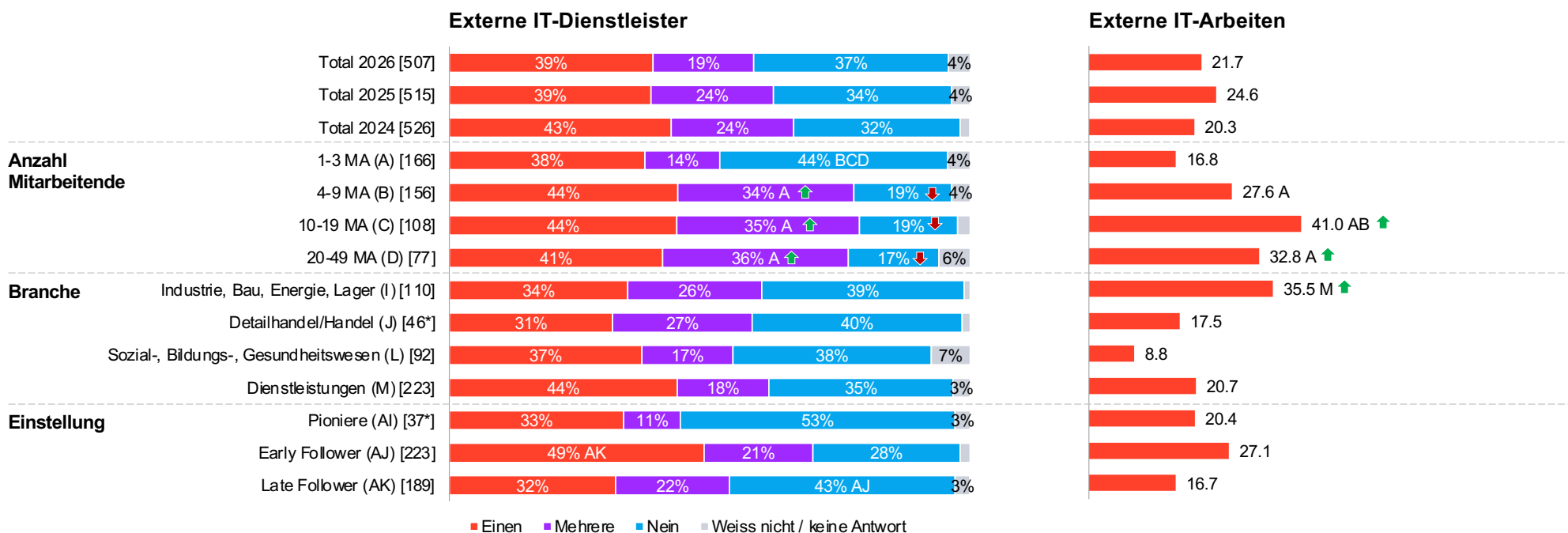


F001: Welche der folgenden Kommunikationsmittel nutzen Ihre Mitarbeitenden aktuell für die Kommunikation mit Partnern, Kundschaft und anderen Mitarbeitenden?

Basis: n=507 | Filter: KMU | Geschlossene Frage | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle | °Textanpassung in 2026

IT-Dienstleister als externe Partner

Unverändert ggü. den Vorwellen: Über die Hälfte 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 etwas mehr als ein Fünftel der IT-Arbeiten extern vergeben.

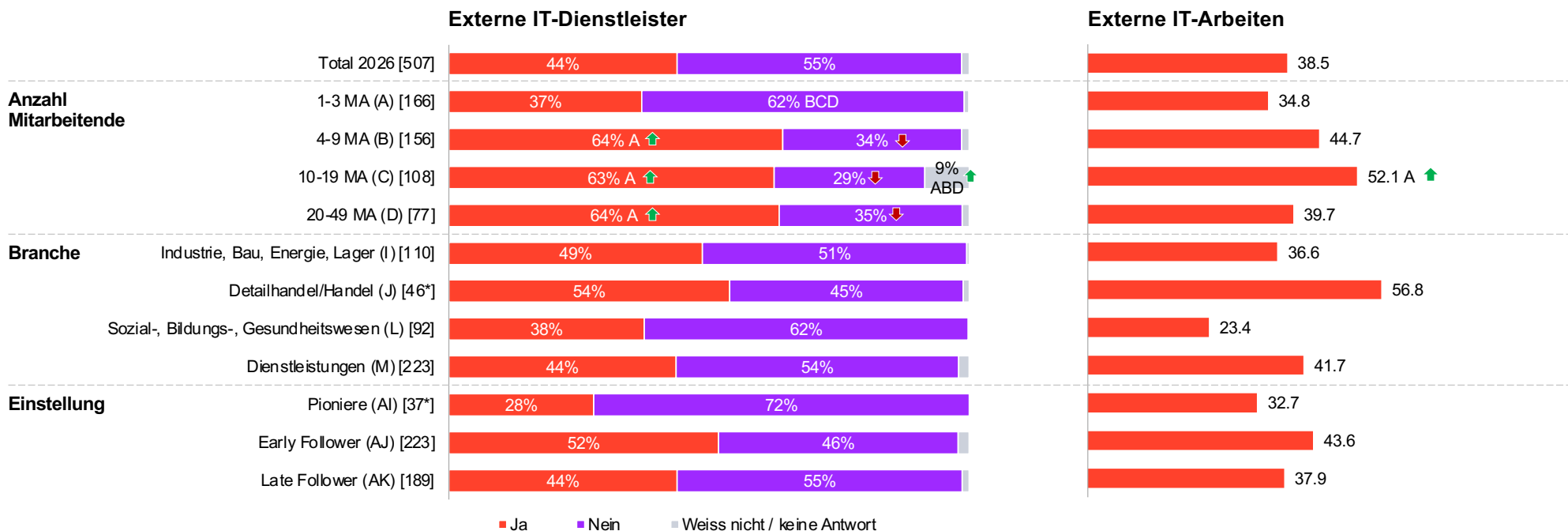


F002: Haben Sie einen oder mehrere IT-Dienstleister, d.h. externe Partner für Informatik, Telefonie, Software- oder Hardware-Arbeiten? | F003: Wieviel Prozent der IT-Arbeiten werden bei Ihnen ungefähr von externen Dienstleistern wahrgenommen? | Basis: n=[] | Filter: KMU | Geschlossene Frage (F002) & Zahlenfeld (F003) | ↑ signifikant höher als Total; ↓ signifikant tiefer als Total | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle |

*Kleine Basis <50 | Datenbeschriftung ab 3% | Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

IT-Dienstleister für Cybersicherheit

Externe IT-Dienstleister spielen für die Cybersicherheit eine zentrale Rolle. Während sich 44% aller befragten Unternehmen auf einen externen Partner verlassen, tun dies bei Unternehmen mit mehr als drei Mitarbeitenden rund zwei Drittel. Im Durchschnitt übernehmen externe Dienstleister 38.5% der IT-Sicherheitsaufgaben.



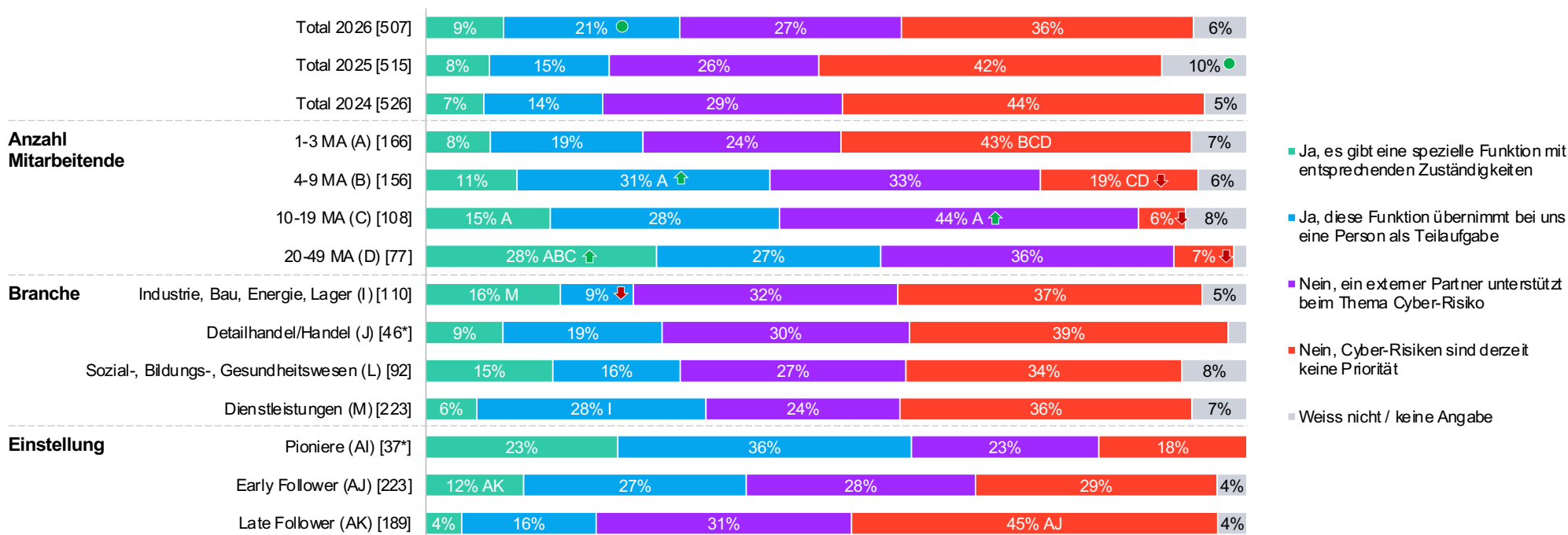
F065: Verlassen Sie sich auf Ihre(n) IT-Dienstleister, wenn es um die Cybersicherheit in Ihrem Unternehmen geht? | F066: Wieviel Prozent Ihrer Cybersicherheit übernehmen IT-Dienstleister ungefähr für Sie?

Basis: n=[] | Filter: KMU | Geschlossene Frage (F065) & Zahlenfeld (F066) | ↑ signifikant höher als Total; ↓ signifikant tiefer als Total | Neue Fragen in 2026

*Kleine Basis <50 | Datenbeschriftung ab 3% | Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Cyberisiko-Verantwortung

Cyber Risiken werden zunehmend mit Verantwortlichkeiten versehen. Der Anteil der Unternehmen, die die Cyberisiko-Verantwortung intern als Teilaufgabe vergeben, stieg von 15% auf 21%, während der Anteil der Unternehmen, für die Cyber Risiken keine Priorität haben, von 42% auf 36% sank. Dieser Trend zeigt sich auch bei Kleinunternehmen mit 1-3 Mitarbeitenden.



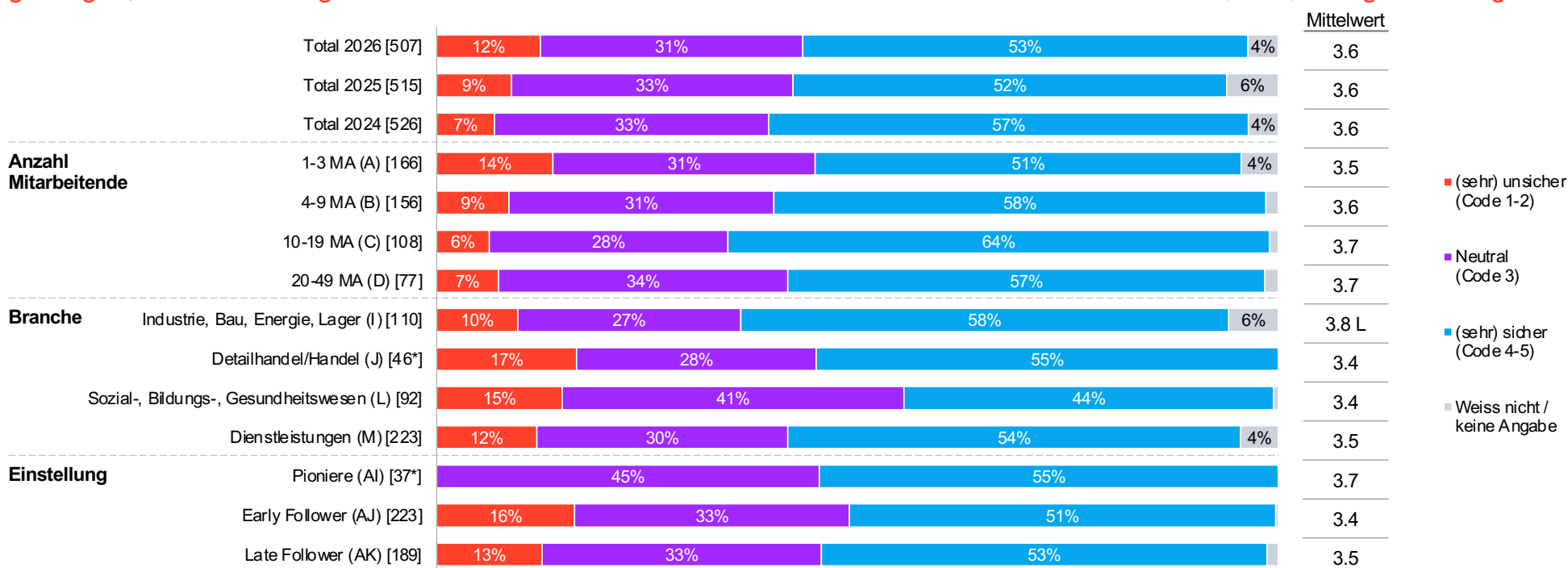
F006: Gibt es in Ihrem Unternehmen eine oder mehrere Personen, die für Cybersicherheit zuständig ist? | Basis: n=[] | Filter: KMU | Geschlossene Frage

↑ signifikant höher als Total; ↓ signifikant tiefer als Total | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle | *Kleine Basis <50 | Datenbeschriftung ab 3%

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

Sicherheitsgefühl

Das Sicherheitsgefühl gegenüber Cyberkriminalität bleibt stabil: Seit drei Jahren fühlt sich jeweils eine Mehrheit von über 50% (sehr) sicher, während der Mittelwert unverändert bei 3.6 liegt. Der Anteil der (sehr) Unsicheren ist zwar von 7% auf 12% gestiegen, bleibt aber vergleichsweise tief. Besonders sicher fühlen sich Unternehmen aus Industrie, Bau, Energie und Lager.

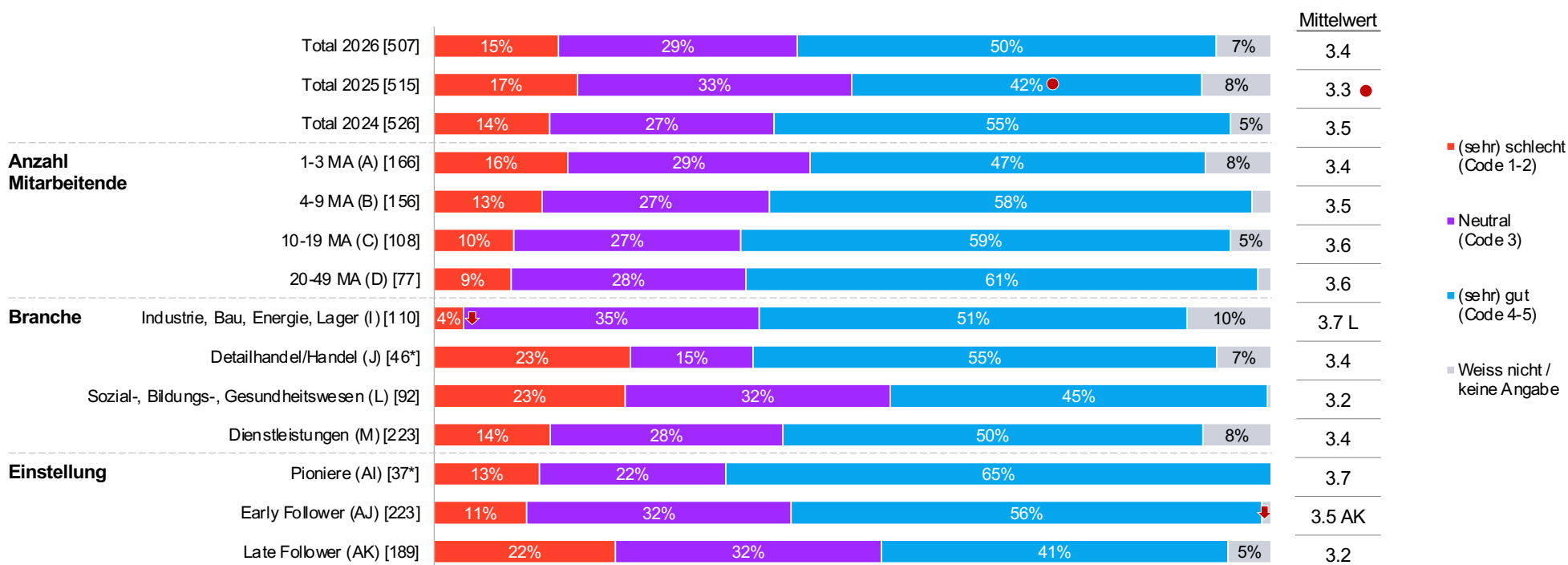


F007: Wie sicher fühlen Sie sich in Ihrem Unternehmen vor Cyberkriminalität?

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 | *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.

Cyberresilienz

Jedes zweite befragte Unternehmen fühlt sich gut gegen Cyberangriffe geschützt. Das Resilienzgefühl steigt mit der Unternehmensgrösse und ist bei technologischen Pionieren besonders ausgeprägt. Late Follower schätzen ihre Widerstandsfähigkeit gegenüber Cyberangriffen deutlich kritischer ein.

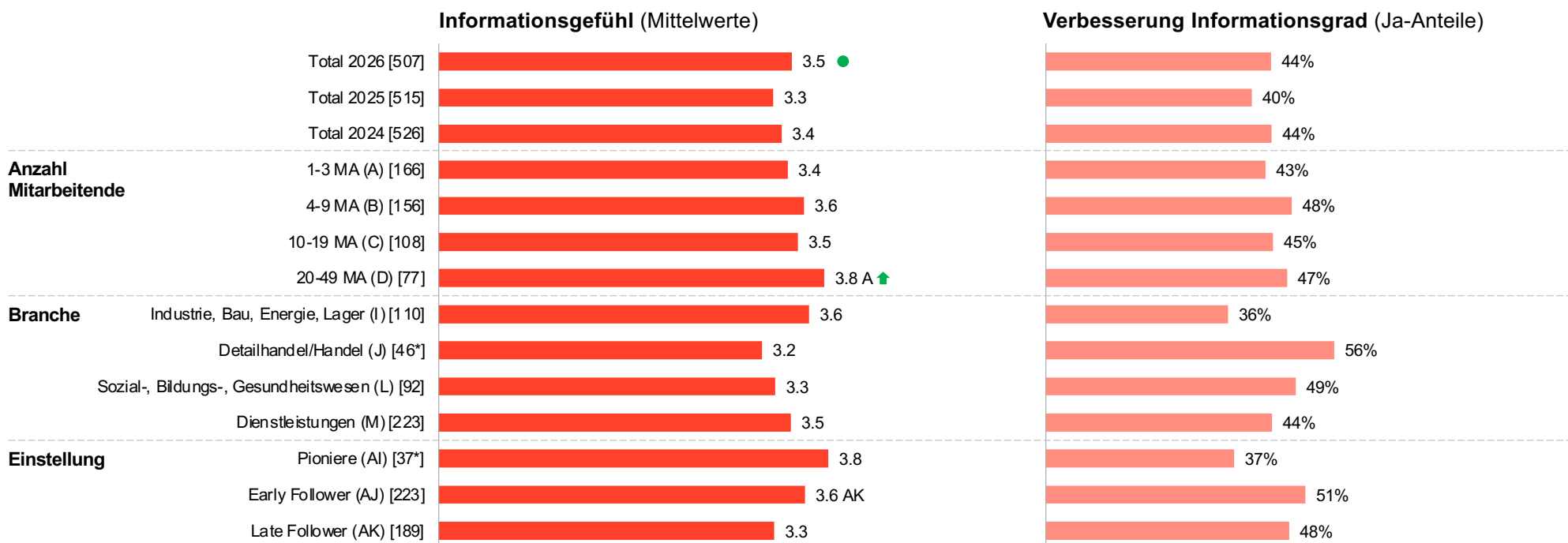


F008: Was schätzen Sie: Wie gut sind Sie vor Cyberangriffen geschützt und auf einen Angriff vorbereitet?

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 | *Kleine Basis <50
 Datenbeschriftung ab 3% | Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Informationsgrad

Das Informationsgefühl ist gegenüber 2025 signifikant gestiegen. Gleichzeitig zeigt sich ein Zusammenhang zwischen Informationsgefühl und Informationsbedarf: Besonders Unternehmen im (Detail-)Handel wünschen sich häufiger zusätzliche Informationen.



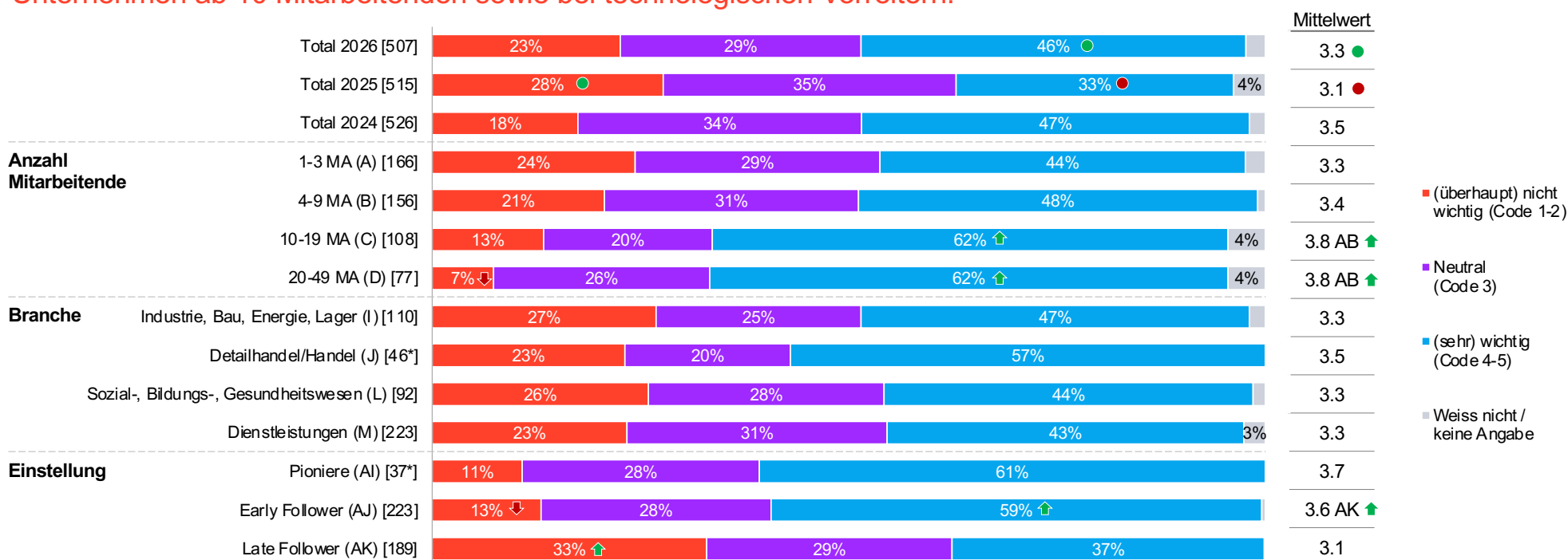
F009: Wie gut fühlen Sie sich persönlich in der Cyberrisk-Thematik informiert? | F010: Wären Sie gerne besser informiert über das Thema Cybersicherheit?

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 |

*Kleine Basis <50 | Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Priorität Cybersicherheit

Nach dem Rückgang im Vorjahr gewinnt Cybersicherheit für KMU wieder an Bedeutung: Der Anteil der Unternehmen, die das Thema als (sehr) wichtig einstufen, stieg signifikant von 33% auf 46%. Besonders hoch ist die Priorisierung bei Unternehmen ab 10 Mitarbeitenden sowie bei technologischen Vorreitern.



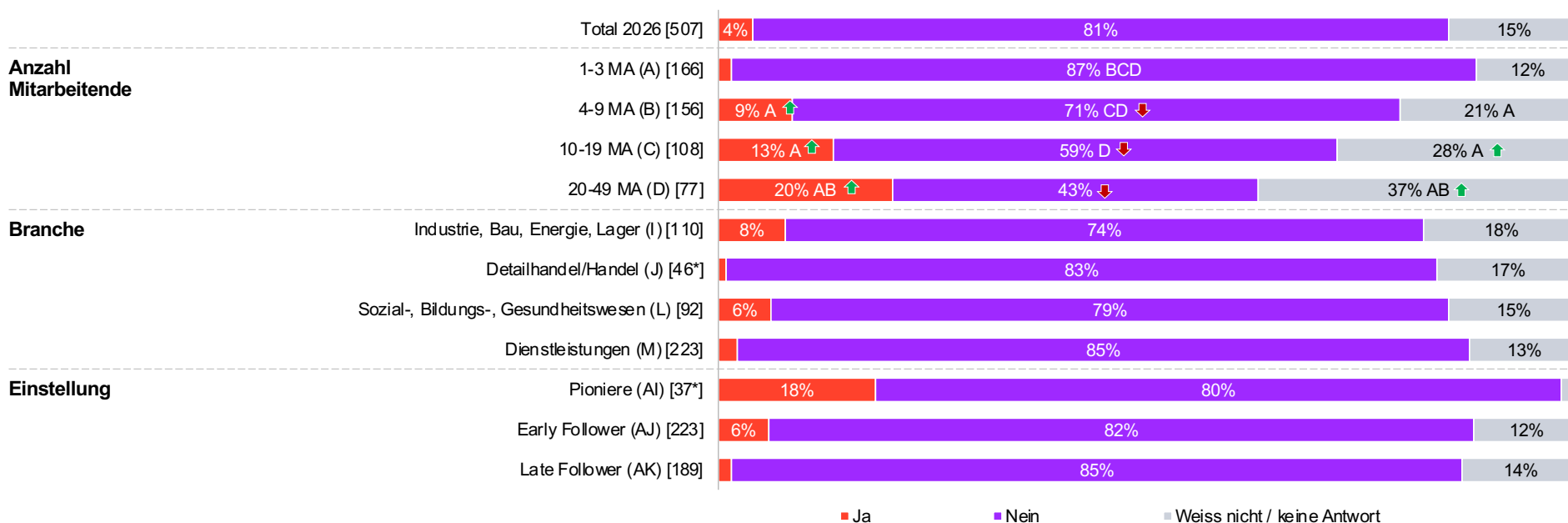
F011: Welche Priorität hat in Ihrer Firma das Thema Cybersicherheit? | Basis: n= | | Filter: KMU | Skalierte Frage: 1= überhaupt nicht wichtig bis 5= sehr wichtig |

▲ signifikant höher als Total; ▼ 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.

Zertifizierung

Vier von fünf KMU geben an, keine IT-Sicherheitszertifizierung zu besitzen, dabei handelt es sich vorwiegend um die Unternehmen mit nur 1 bis 3 Mitarbeitenden. Der Anteil an Unternehmen, die ein IT-Sicherheitszertifikat haben, steigt signifikant mit wachsender Unternehmensgrösse.



F062: Verfügt ihr Unternehmen über eine IT-Sicherheitszertifizierung (z.B. ISO 27001 oder NIST CSF 2.0)?

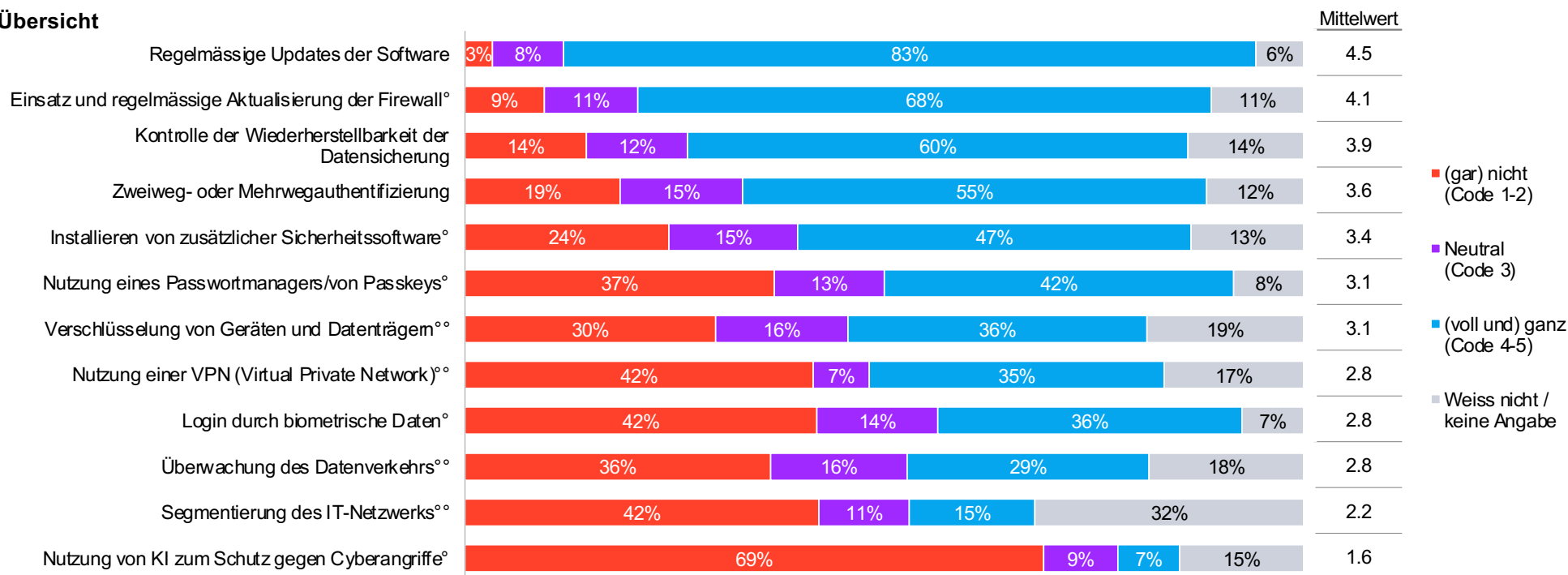
Basis: n=[] | Filter: KMU | Geschlossene Frage | ↑ signifikant höher als Total; ↓ signifikant tiefer als Total | Neue Frage in 2026

*Kleine Basis <50 | Datenbeschriftung ab 3% | Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Technische Massnahmenumsetzung (1/5)

Die Umsetzung technischer Cybersicherheitsmassnahmen konzentriert sich in KMU auf bewährte Basismassnahmen. Während Software-Updates, Firewalls, Datensicherungen und Mehrfaktorauthentifizierung bei einer Mehrheit etabliert sind, kommen fortgeschrittene Massnahmen wie Netzwerksegmentierung, Datenverkehrsüberwachung oder KI-basierte Schutzlösungen deutlich seltener zum Einsatz.

Übersicht



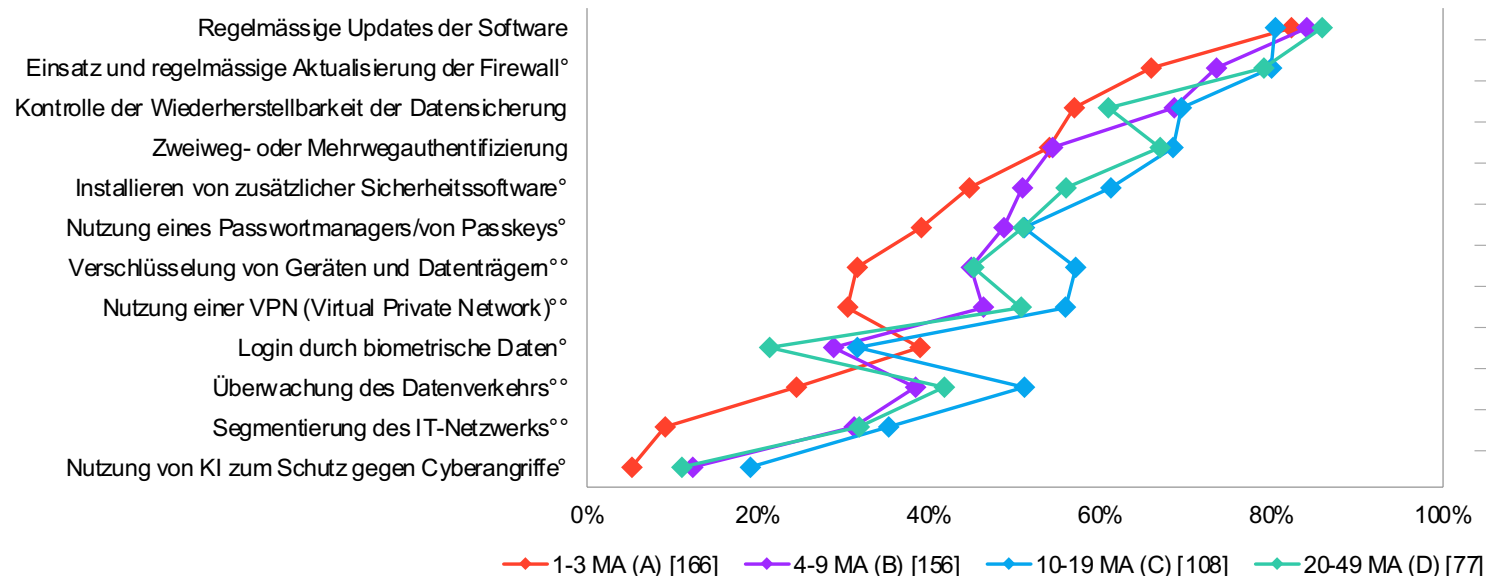
F012: Inwieweit sind die folgenden technischen Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?

Basis: n=507 | Filter: KMU | Skalierte Frage: 1= gar nicht bis 5= voll und ganz | °Textanpassung in 2026 | °°Neu in 2026

Technische Massnahmenumsetzung (2/5)

Unternehmen mit 1-3 Mitarbeitenden haben bei fast allen Massnahmen die tiefsten Umsetzungsgrade auf. Eine Ausnahme bilden biometrische Logins, die von Kleinstunternehmen häufiger genutzt werden. Unternehmen mit 4-9, 10-19 bzw. 20-49 Mitarbeitenden unterscheiden sich dagegen nur wenig voneinander.

Nach Anzahl Mitarbeitenden



Mittelwert

	1-3 MA	4-9 MA	10-19 MA	20-49 MA
Regelmässige Updates der Software	4.5	4.4	4.5	4.5
Einsatz und regelmässige Aktualisierung der Firewall°	4.1	4.2	4.5 AB	4.4
Kontrolle der Wiederherstellbarkeit der Datensicherung	3.8	4.0	4.1	4.2
Zweiweg- oder Mehrwegauthentifizierung	3.5	3.7	3.9 A	4.1 AB
Installieren von zusätzlicher Sicherheitssoftware°	3.3	3.6	4.0 A	4.0 A
Nutzung eines Passwortmanagers/von Passkeys°	3.0	3.3	3.6 A	3.6 A
Verschlüsselung von Geräten und Datenträgern°°	2.9	3.3 A	3.9 AB	3.6 A
Nutzung einer VPN (Virtual Private Network)°°	2.6	3.2 A	3.8 AB	3.8 AB
Login durch biometrische Daten°	2.9	2.5	2.6	2.5
Überwachung des Datenverkehrs°°	2.5	3.2 A	3.8 AB	3.6 AB
Segmentierung des IT-Netzwerks°°	1.9	3.1 A	3.3 A	3.4 A
Nutzung von KI zum Schutz gegen Cyberangriffe°	1.5	1.9 A	2.3 AB	2.2 A

F012: Inwieweit sind die folgenden technischen Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?

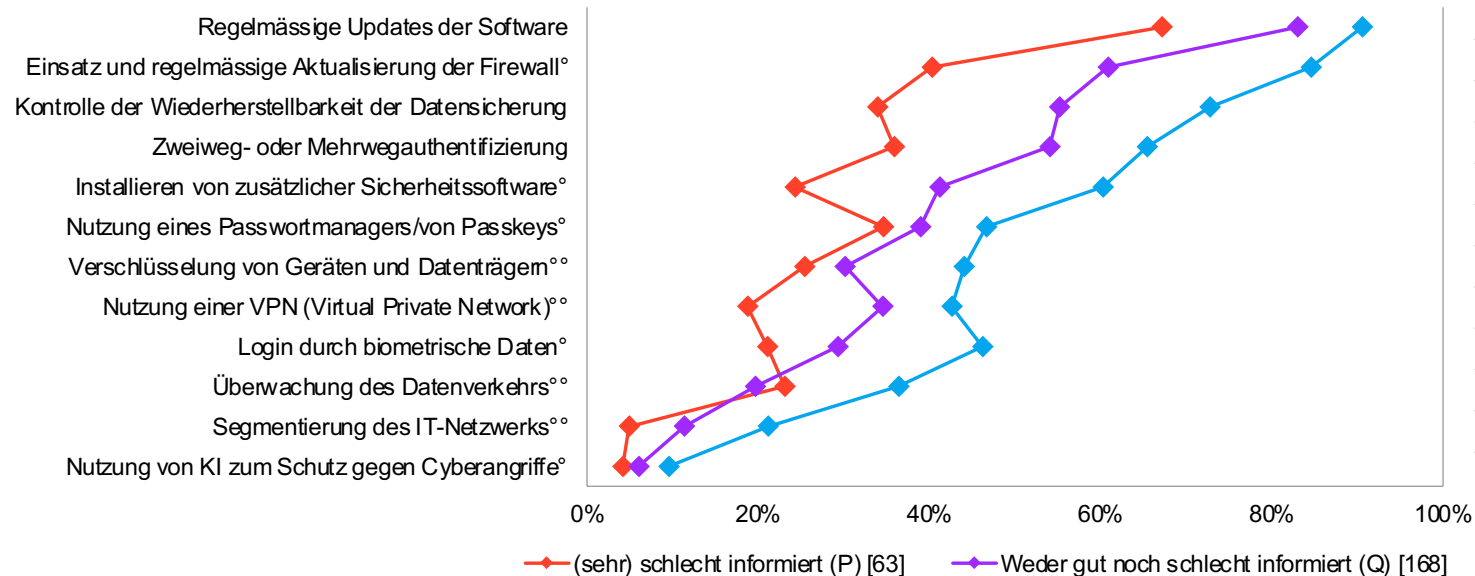
Basis: n=[] | Filter: KMU | Skalierte Frage: 1= gar nicht bis 5= voll und ganz | Top2 und Mittelwerte ausgewiesen | °Textanpassung in 2026 | °°Neu in 2026

signifikant **höher** als Total; signifikant **tief**er 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 häufiger setzen sie technische Sicherheitsmassnahmen um.

Nach Informationsgrad



Mittelwert		
Eher/sehr schlecht	Weder gut noch schlecht	Eher/sehr gut
4.0	4.3	4.8 PQ
3.4	4.0 P	4.5 PQ
3.1	3.7	4.2 Q
2.9	3.5 P	3.9 PQ
2.5	3.3 P	3.8 PQ
2.8	3.0	3.2
2.5	3.0	3.2
2.2	2.9	3.0
2.4	2.6	3.1 P
2.4	2.5	3.0 Q
1.9	2.1	2.4
1.4	1.6	1.7

F012: Inwieweit sind die folgenden technischen Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?

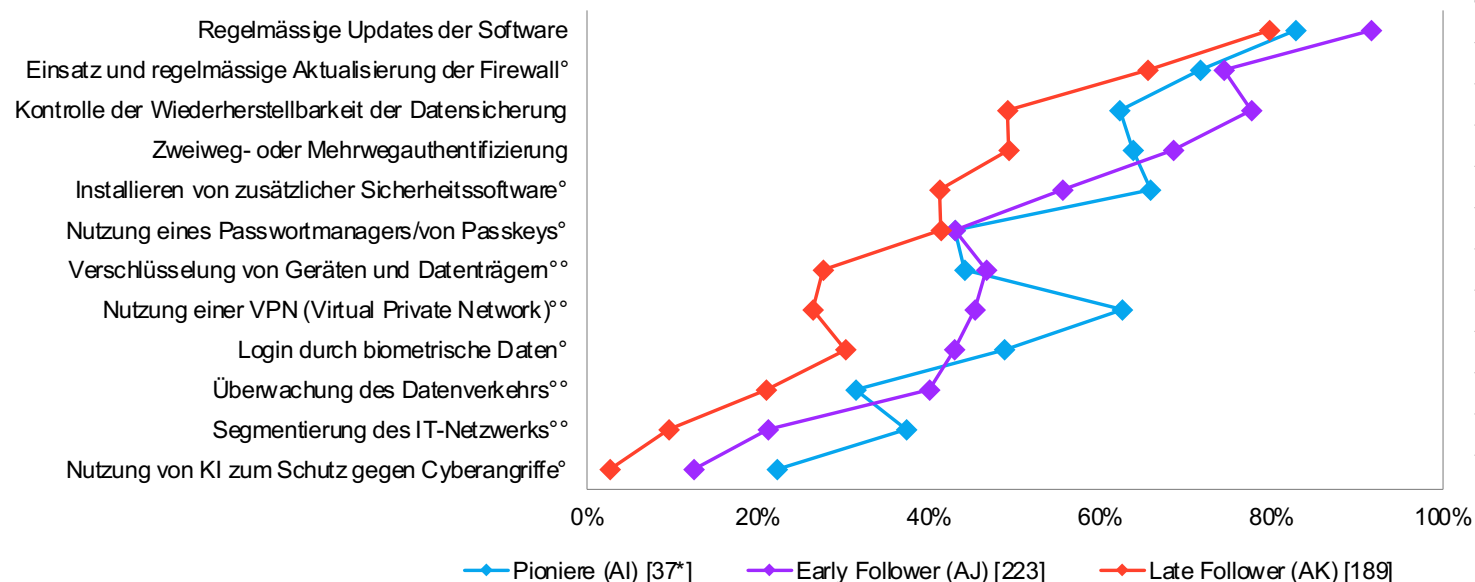
Basis: n=[] | Filter: KMU | Skalierte Frage: 1= gar nicht bis 5= voll und ganz | Top2 und Mittelwerte ausgewiesen | °Textanpassung in 2026 | °°Neu in 2026

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)

Late Follower weisen bei vielen technischen Sicherheitsmassnahmen tiefere Umsetzungsgrade auf als technologieoffenere Unternehmen. Die Unterschiede sind insbesondere bei fortgeschrittenen Massnahmen wie VPNs, Netzwerksegmentierung, Datenverkehrsüberwachung oder KI-gestütztem Schutz ausgeprägt.

Nach Einstellung



Mittelwert

Pioniere	Early Follower	Late Follower
4.5	4.6 AK	4.3
4.0	4.3 AK	4.0
3.9	4.2 AK	3.6
4.1	3.9 AK	3.3
4.0	3.7 AK	3.2
3.2	3.1	3.0
3.4	3.4 AK	2.7
3.8	3.1 AK	2.5
3.2	2.9	2.6
3.1	3.2 AK	2.3
2.8	2.6 AK	1.9
2.3	1.9 AK	1.4

F012: Inwieweit sind die folgenden technischen Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?

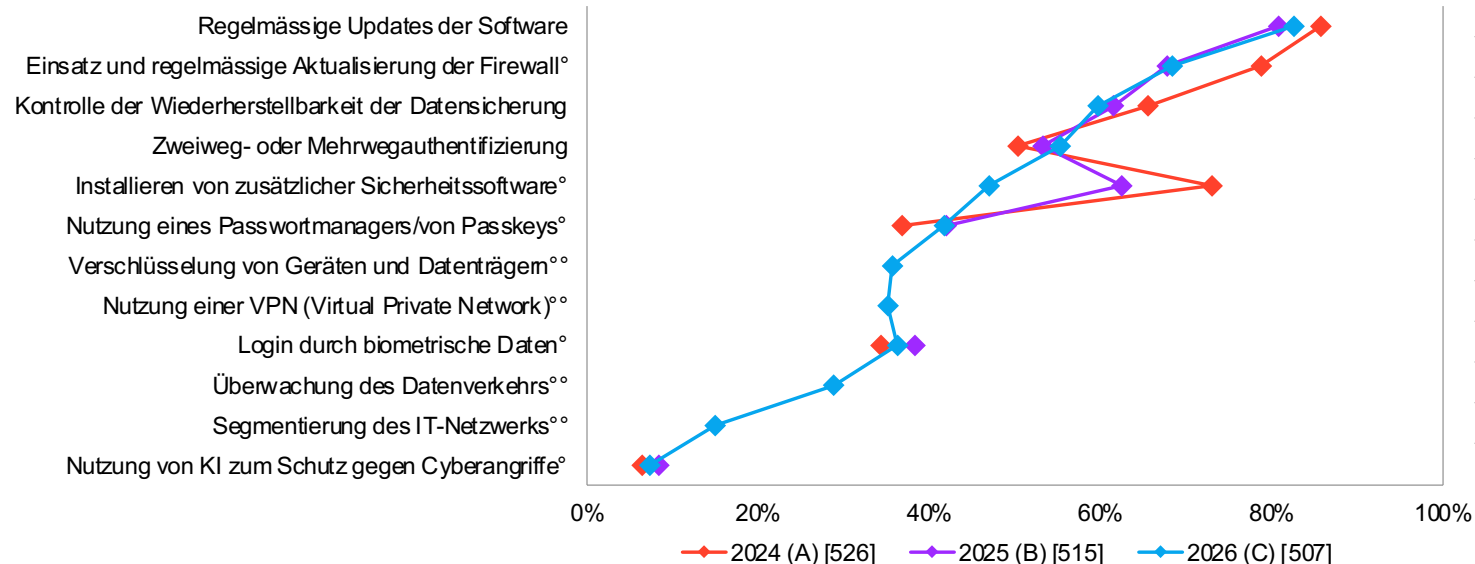
Basis: n=11 | Filter: KMU | Skalierte Frage: 1= gar nicht bis 5= voll und ganz | Top2 und Mittelwerte ausgewiesen | **Sehr kleine Basis <30 | °Textanpassung in 2026 | °°Neu in 2026

signifikant **höher** als Total; signifikant **tief** 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)

Bei den meisten technischen Cybersicherheitsmassnahmen zeigen sich gegenüber den Vorjahren nur geringe Veränderungen. Die Verbreitung von Updates, Firewalls, Datensicherungen und Multifaktorauthentifizierung stagniert auf hohem Niveau, während zusätzliche Sicherheitssoftware deutlich seltener eingesetzt wird als noch 2024.

Jahresvergleich



Mittelwert

2024	2025	2026
4.5	4.4	4.5
4.4 BC	4.1	4.1
4.0	3.9	3.9
3.6	3.5	3.6
4.1 BC	3.8 C	3.4
2.8	3.1	3.1
n/a	n/a	3.1
n/a	n/a	2.8
2.8	2.9	2.8
n/a	n/a	2.8
n/a	n/a	2.2
1.6	1.7	1.6

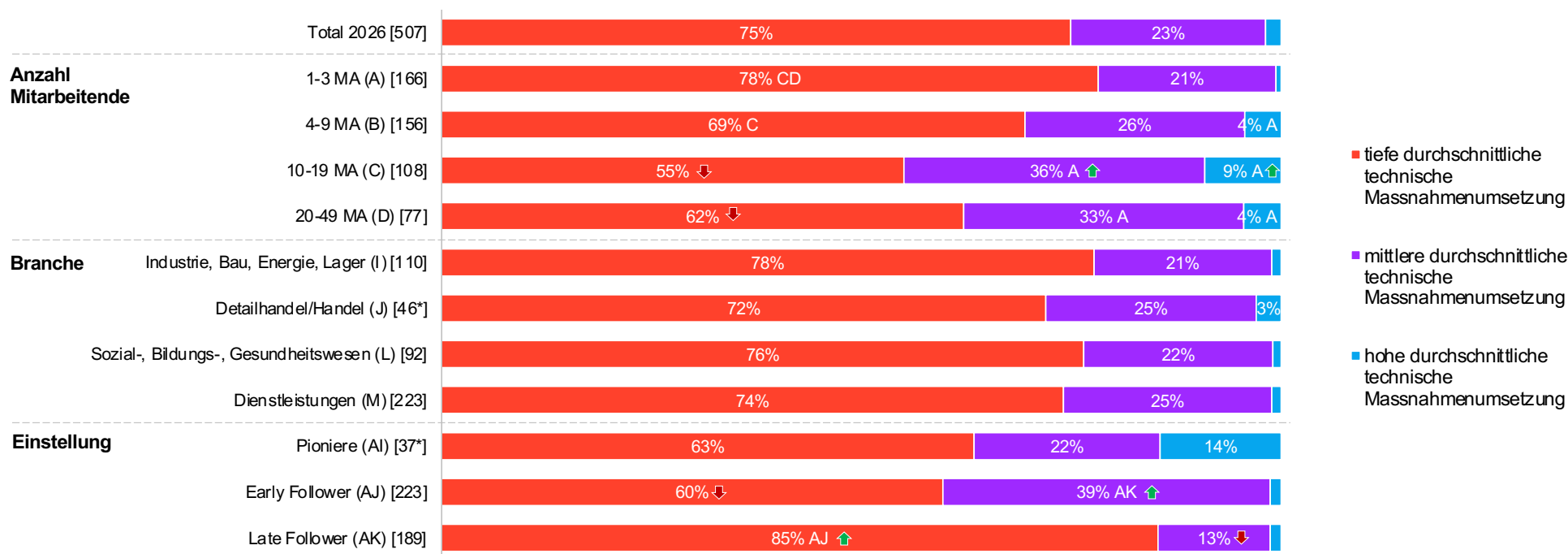
F012: Inwieweit sind die folgenden technischen Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?

Basis: n=[] | Filter: KMU | Skalierte Frage: 1= gar nicht bis 5= voll und ganz | Top2 und Mittelwerte ausgewiesen | °Textanpassung in 2026 | °°Neu in 2026

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 technische Massnahmen

Der technische Massnahmenumsetzungsgrad unterscheidet sich deutlich nach Unternehmensgrösse und Innovationsorientierung. Hohe Umsetzungsgrade werden insbesondere von Unternehmen mit 10-19 Mitarbeitenden sowie von technologischen Pionieren erreicht.



F012: Inwieweit sind die folgenden technischen Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?

Basis: n=507 | 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

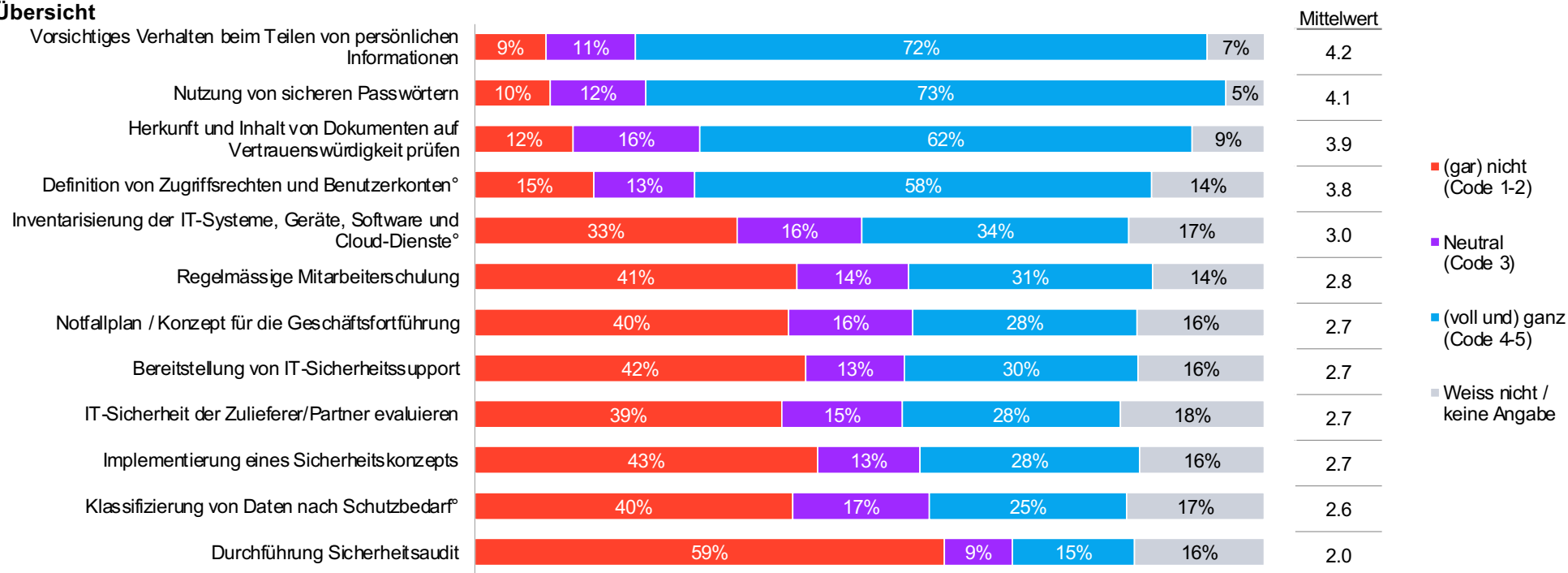
↑ signifikant höher als Total; ↓ signifikant tiefer als Total | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle | *Kleine Basis <50 | Datenbeschriftung ab 3%

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

Organisatorische Massnahmenumsetzung (1/5)

Organisatorische Massnahmen werden insgesamt seltener umgesetzt als technische. Während Verhaltensregeln und grundlegende Schutzmassnahmen bei vielen KMU etabliert sind, werden organisatorische Prozesse wie Sicherheitsaudits, Datenklassifizierung oder Notfallkonzepte deutlich seltener umgesetzt.

Übersicht

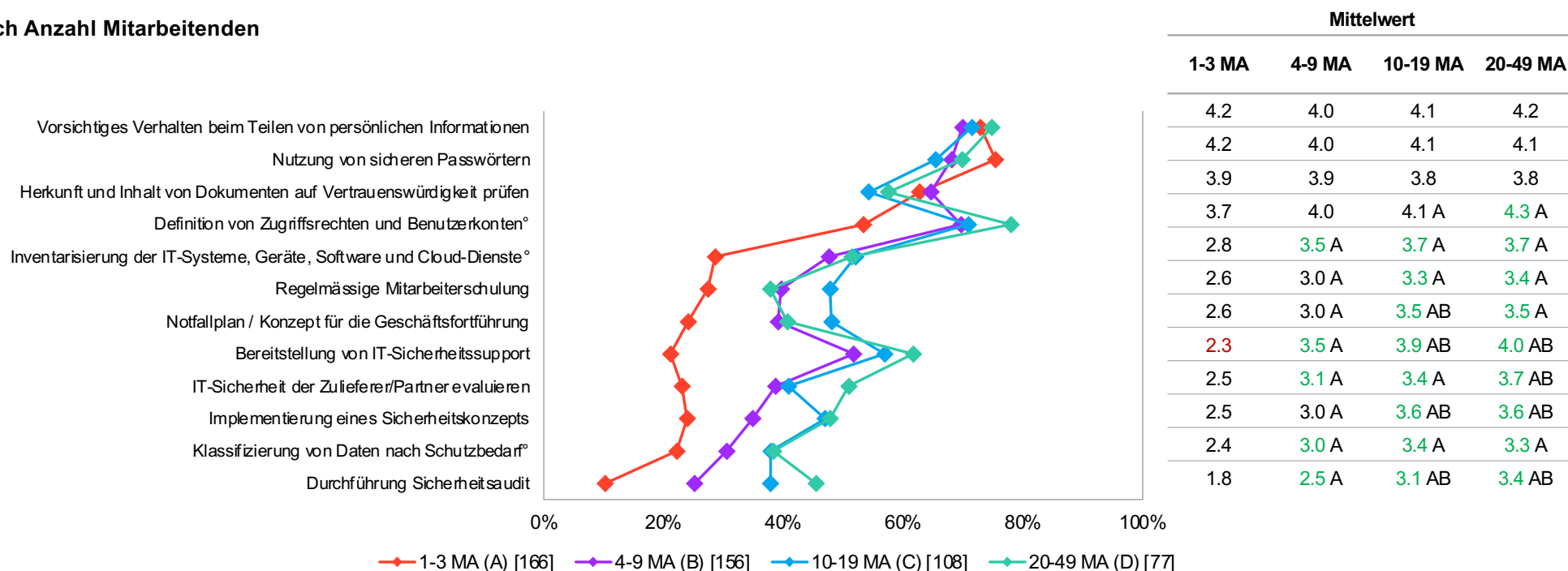


F013: Inwieweit sind die folgenden organisatorischen Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?
 Basis: n=507 | Filter: KMU | Skalierte Frage: 1= gar nicht bis 5= voll und ganz | °Neu in 2026

Organisatorische Massnahmenumsetzung (2/5)

Während grundlegende Verhaltensregeln unabhängig von der Unternehmensgrösse ähnlich häufig umgesetzt werden, steigt die Umsetzung organisatorischer Prozesse mit der Anzahl Mitarbeitender deutlich an. Besonders ausgeprägt sind die Unterschiede bei IT-Sicherheitssupport, Sicherheitskonzepten, Lieferantenbewertungen und Sicherheitsaudits.

Nach Anzahl Mitarbeitenden



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 | °Neu in 2026

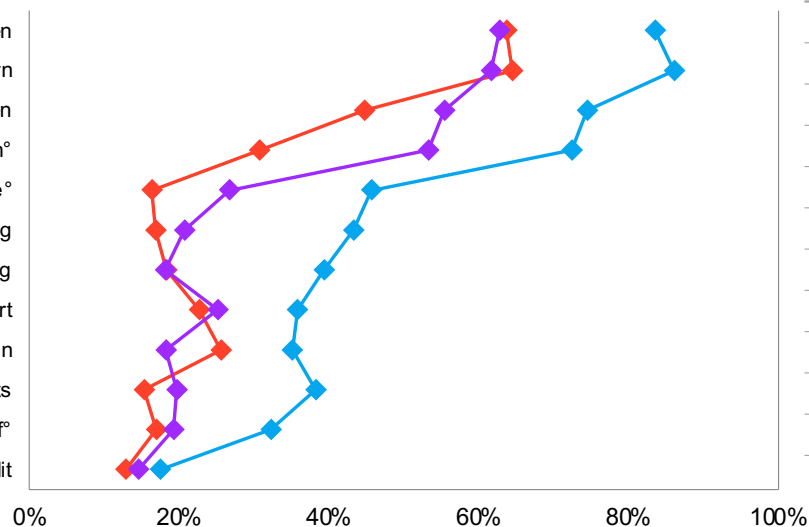
signifikant **höher** als Total; signifikant **tief** als Total | Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Organisatorische Massnahmenumsetzung (3/5)

Je besser sich KMU zu Cyberrisiken informiert fühlen, desto häufiger setzen sie organisatorische Sicherheitsmassnahmen um. Dieser Zusammenhang zeigt sich über nahezu alle untersuchten Massnahmen hinweg.

Nach Informationsgrad

Vorsichtiges Verhalten beim Teilen von persönlichen Informationen
Nutzung von sicheren Passwörtern
Herkunft und Inhalt von Dokumenten auf Vertrauenswürdigkeit prüfen
Definition von Zugriffsrechten und Benutzerkonten°
Inventarisierung der IT-Systeme, Geräte, Software und Cloud-Dienste°
Regelmässige Mitarbeiterschulung
Notfallplan / Konzept für die Geschäftsführung
Bereitstellung von IT-Sicherheitssupport
IT-Sicherheit der Zulieferer/Partner evaluieren
Implementierung eines Sicherheitskonzepts
Klassifizierung von Daten nach Schutzbedarf°
Durchführung Sicherheitsaudit



— (sehr) schlecht informiert (P) [63]

— Weder gut noch schlecht informiert (Q) [168]

— (sehr) gut informiert (R) [267]

Mittelwert		
Eher/sehr schlecht	Weder gut noch schlecht	Eher/sehr gut
3.8	3.9	4.5 PQ
3.7	3.9	4.5 PQ
3.4	3.6	4.2 PQ
3.0	3.6	4.2 PQ
2.3	2.6	3.4 PQ
1.9	2.5	3.2 PQ
2.1	2.4	3.2 PQ
2.2	2.5	3.0 PQ
2.3	2.3	3.0 PQ
2.1	2.3	3.1 PQ
2.4	2.3	2.8 Q
1.7	2.1	2.1

F013: Inwieweit sind die folgenden organisatorischen Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?

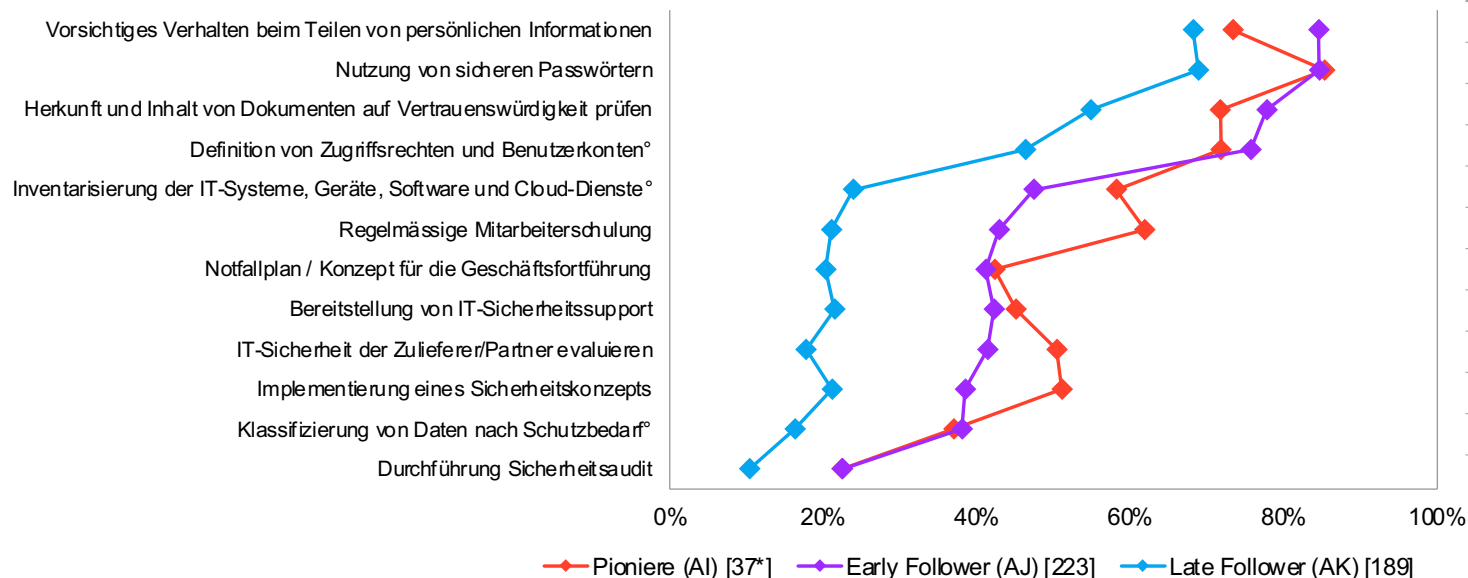
Basis: n=[] | Filter: KMU | Skalierte Frage: 1= gar nicht bis 5= voll und ganz | Top2 und Mittelwerte ausgewiesen | °Neu in 2026

signifikant **höher** als Total; signifikant **tief** 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)

Mit zunehmender Offenheit gegenüber neuen Technologien steigt auch die Umsetzung organisatorischer Sicherheitsmassnahmen. Besonders deutlich fallen die Unterschiede zwischen technologieoffenen Unternehmen und Late Followern aus.

Nach Einstellung



Mittelwert

Pioniere	Early Follower	Late Follower
4.3	4.3 AK	4.0
4.4	4.4 AK	3.9
4.1	4.1 AK	3.7
3.8	4.2 AK	3.5
3.7	3.4 AK	2.5
3.7	3.2 AK	2.3
3.2	3.2 AK	2.3
3.1	3.1 AK	2.4
3.6	3.0 AK	2.4
3.4	3.0 AK	2.3
3.2	2.9 AK	2.3
2.5	2.3 AK	1.7

F013: Inwieweit sind die folgenden organisatorischen Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?

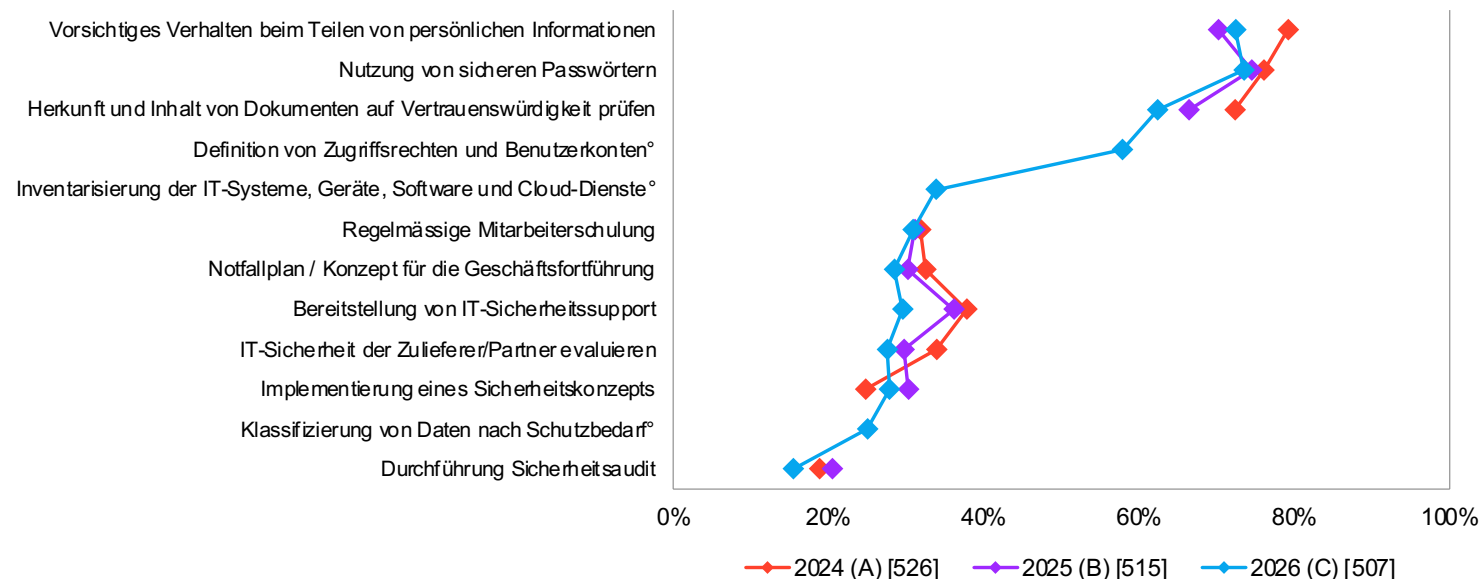
Basis: n=[] | Filter: KMU | Skalierte Frage: 1= gar nicht bis 5= voll und ganz | Top2 und Mittelwerte ausgewiesen | **Sehr kleine Basis <50 | °Neu in 2026

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 insgesamt eine hohe Stabilität bei den organisatorischen Massnahmen. Während die meisten Umsetzungsgrade nahezu unverändert bleiben, gehen Sicherheitsaudits und IT-Sicherheitssupport gegenüber 2025 signifikant zurück.

Jahresvergleich



Mittelwert

2024	2025	2026
4.3 B	4.1	4.2
4.2	4.1	4.1
4.0	4.0	3.9
n/a	n/a	3.8
n/a	n/a	3.0
2.9	2.8	2.8
2.8	2.9	2.7
2.9	3.0 C	2.7
2.9	2.8	2.7
2.6	2.8	2.7
n/a	n/a	2.6
2.2	2.3 C	2.0

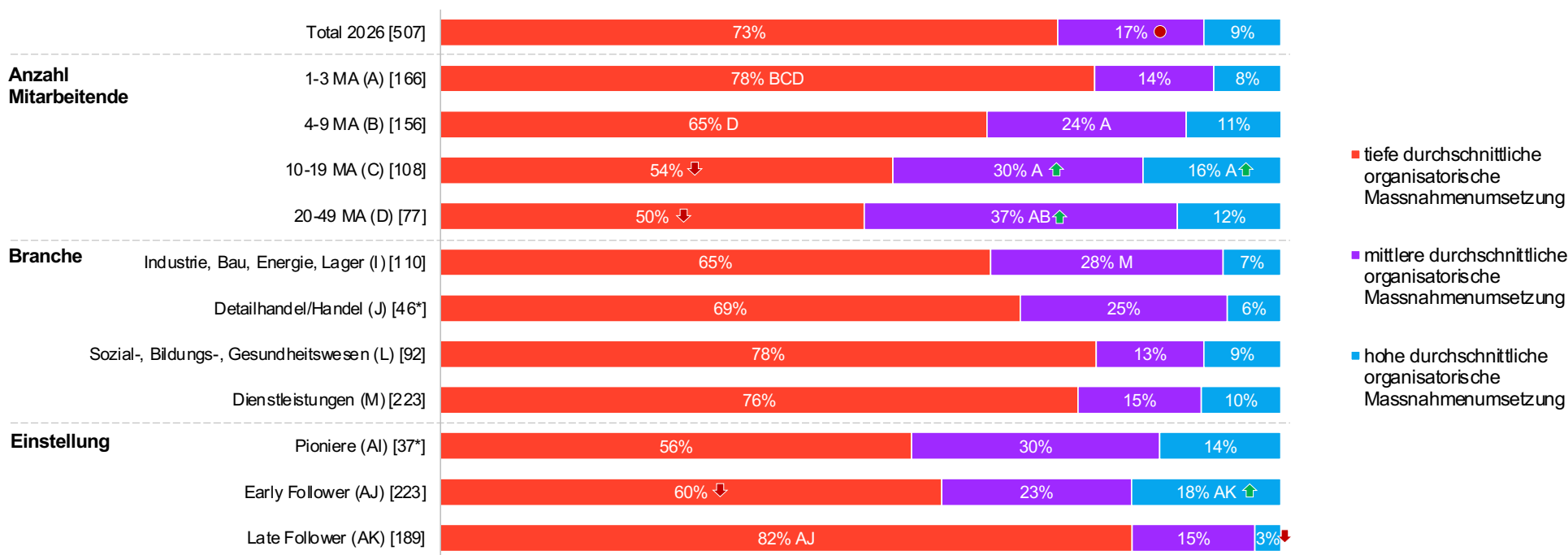
F013: Inwieweit sind die folgenden organisatorischen Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?

Basis: n=[] | Filter: KMU | Skalierte Frage: 1= gar nicht bis 5= voll und ganz | Top2 und Mittelwerte ausgewiesen | °Neu in 2026

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 organisatorische Massnahmen

Der organisatorische Massnahmenumsetzungsgrad unterscheidet sich vor allem nach Innovationsorientierung und Unternehmensgrösse. Late Follower erreichen deutlich häufiger tiefe Umsetzungsgrade, während Unternehmen mit 10 bis 19 Mitarbeitenden sowie Early Follower überdurchschnittlich oft hohe Umsetzungsgrade aufweisen.



F013: Inwieweit sind die folgenden organisatorischen Massnahmen zur Erhöhung der Cybersicherheit bei Ihnen umgesetzt?

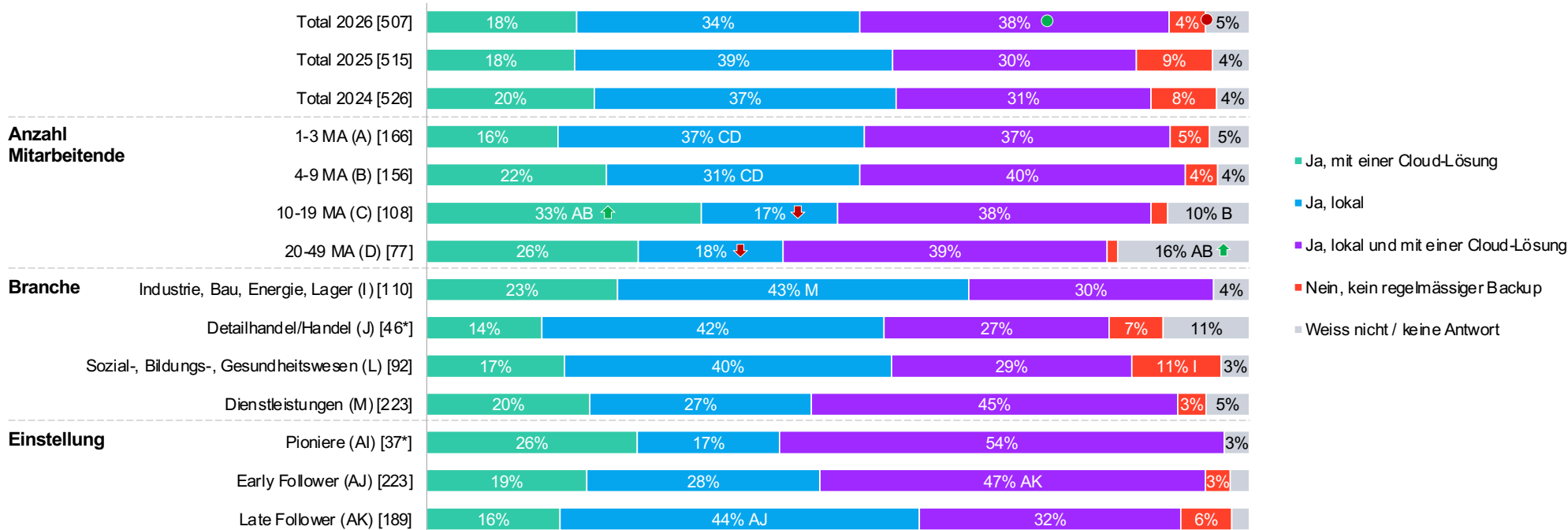
Basis: n=507 | Filter: KMU | Skalierte Frage 1-5 | „tief“ = Mittelwert aller Massnahmen ≤3.49, „mittel“ = Mittelwert aller Massnahmen ≥3.5 und ≤4.49, „hoch“ = Mittelwert aller Massnahmen ≥4.5

↑ signifikant höher als Total; ↓ signifikant tiefer als Total; ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle | *Kleine Basis <50 | Datenbeschriftung ab 3%

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

Backup mit/ohne Cloud

Regelmässige Datensicherungen sind bei KMU weit verbreitet: Neun von zehn Unternehmen führen Backups durch, während der Anteil ohne regelmässige Datensicherung auf 4% gesunken ist. Lokale und Cloud-basierte Backups werden zunehmend kombiniert, insbesondere bei Firmen mit über 10 Mitarbeitenden.

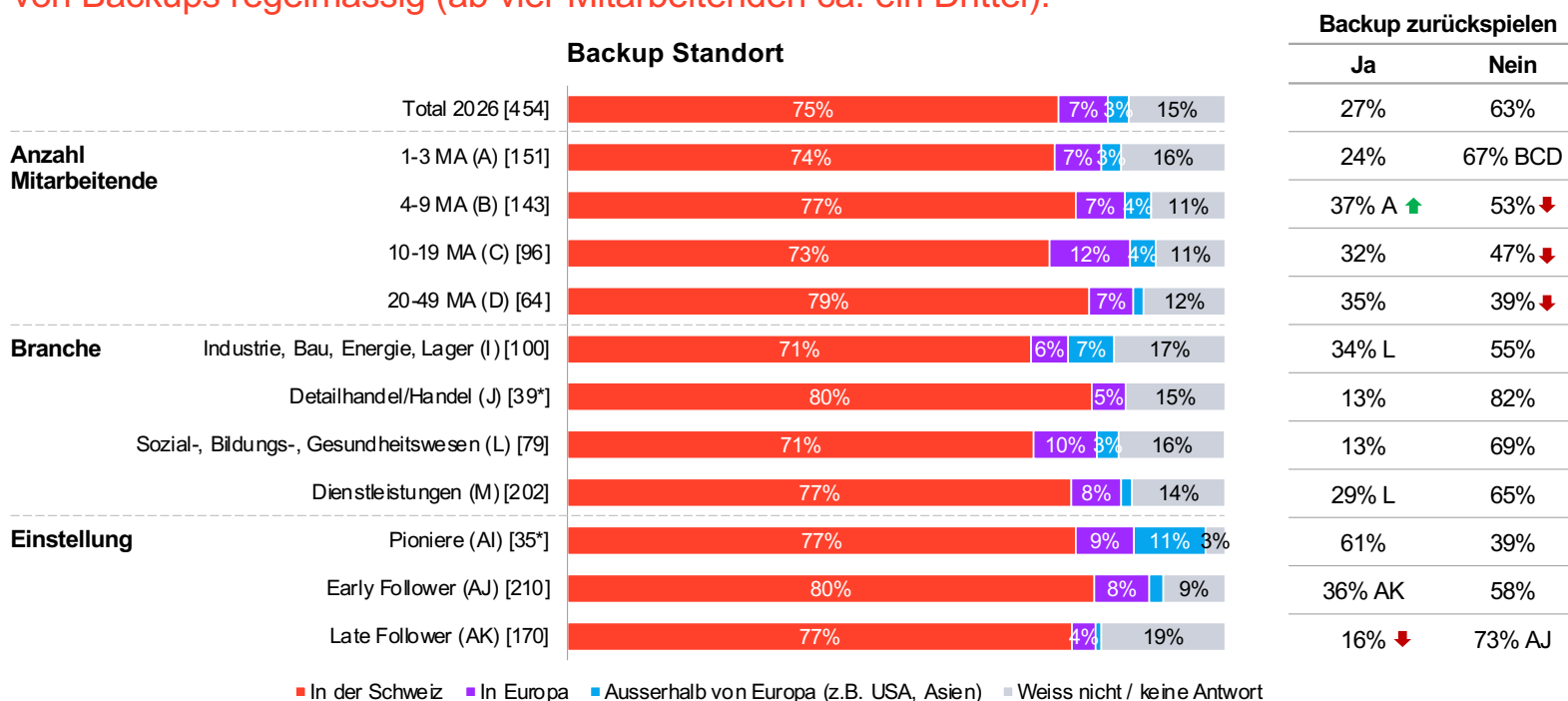


F014: Wird in Ihrem Unternehmen regelmässig ein Backup der Daten durchgeführt?

Basis: n=[] | Filter: KMU | Geschlossene Frage | ↑ signifikant höher als Total; ↓ signifikant tiefer als Total; ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle | *Kleine Basis <50 | Datenbeschriftung ab 3%
Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Backup

Backups werden überwiegend in der Schweiz gespeichert. Während regelmässige Datensicherungen zum Standard gehören, wird das Testen der Wiederherstellung noch häufig vernachlässigt: Nur 27% der KMU üben das Zurückspielen von Backups regelmässig (ab vier Mitarbeitenden ca. ein Drittel).



F014_2: Wo befindet sich Ihr Daten-Backup? | F014_3: Wird in Ihrem Unternehmen regelmässig geübt, das Backup wieder zurückzuspielen?

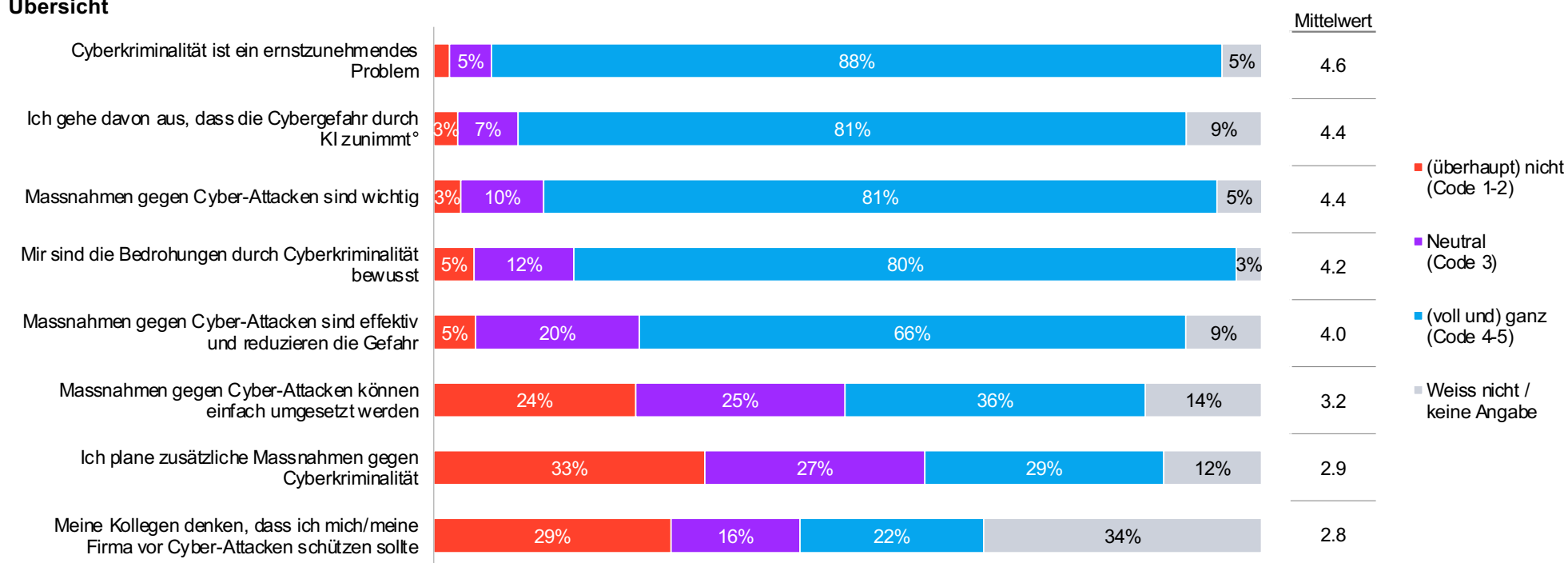
Basis: n=[] | Filter: KMU – regelmässiges Backup der Daten | Geschlossene Frage | ↑ signifikant höher als Total; ↓ signifikant tiefer als Total | Neue Fragen in 2026

*Kleine Basis <50 | Datenbeschriftung ab 3% | Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Einstellung zu Cyberkriminalität (1/7)

Das Problembewusstsein gegenüber Cyberkriminalität ist hoch und die Mehrheit der KMU glaubt an die Wirksamkeit von Schutzmassnahmen. Dennoch empfindet nur rund ein Drittel deren Umsetzung als einfach, was auf Herausforderungen bei der praktischen Umsetzung hindeutet.

Übersicht



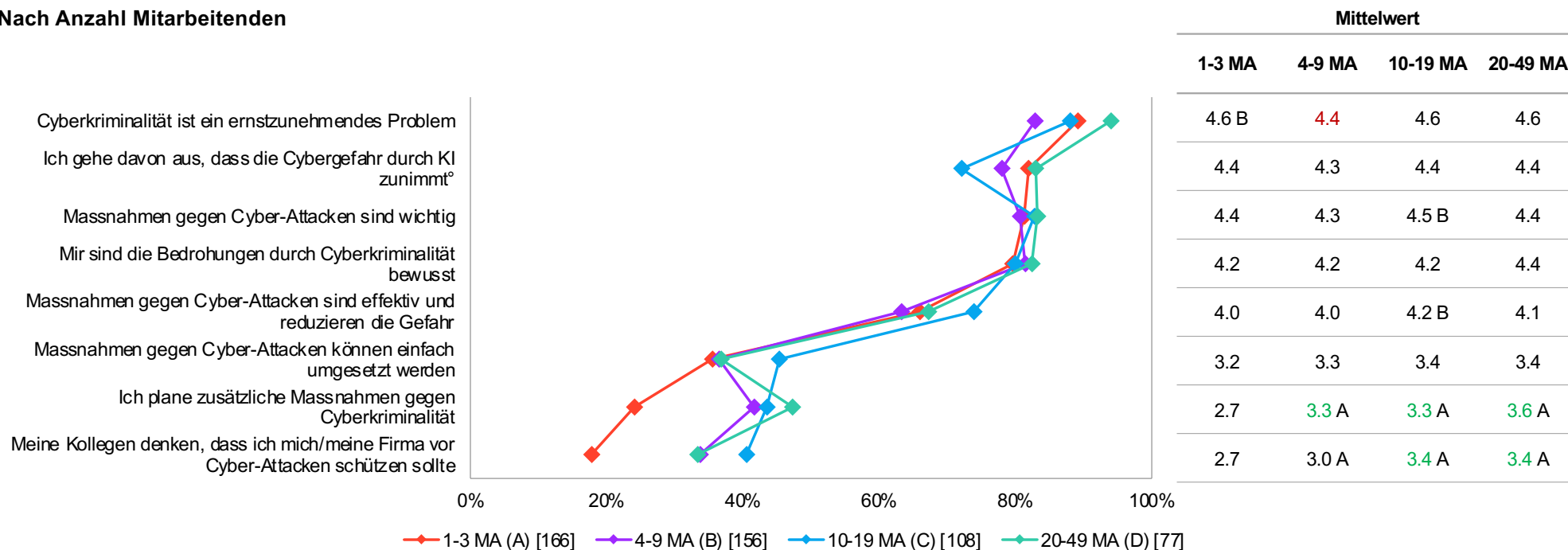
F015: Inwiefern stimmen Sie den folgenden Aussagen zu Cyberkriminalität wie Malware, Online-Betrug und Hacking zu?

Basis: n=507 | Filter: KMU | Skalierte Frage: 1= überhaupt nicht bis 5= voll und ganz | Datenbeschriftung ab 3% | *Neu in 2026

Einstellung zu Cyberkriminalität (2/7)

Die Einstellungen zur Cyberkriminalität unterscheiden sich nach Unternehmensgrösse nur gering. Am ehesten heben sich Unternehmen mit 1-3 Mitarbeitenden ab: Sie planen seltener zusätzliche Schutzmassnahmen und nehmen weniger häufig wahr, dass ihr Umfeld entsprechende Schutzmassnahmen erwartet.

Nach Anzahl Mitarbeitenden



F015: Inwiefern stimmen Sie den folgenden Aussagen zu Cyberkriminalität wie Malware, Online-Betrug und Hacking zu?

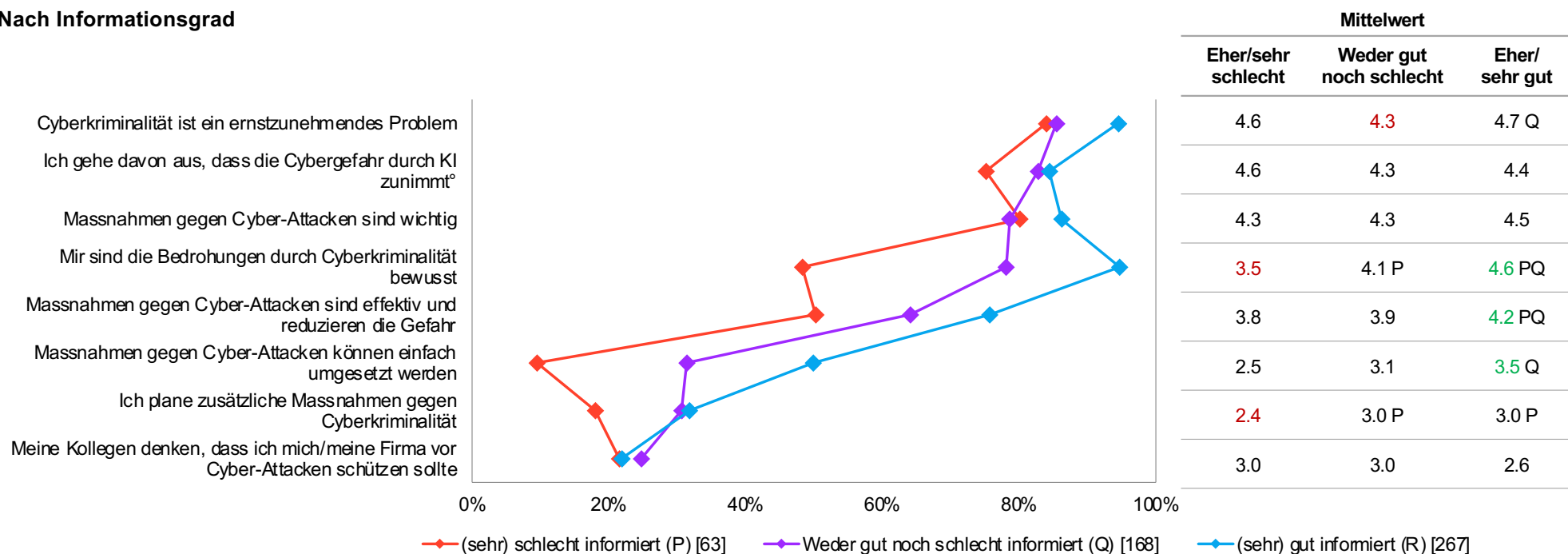
Basis: n=[] | Filter: KMU | Skalierte Frage: 1= überhaupt nicht bis 5= voll und ganz | Top2 und Mittelwerte ausgewiesen | *Neu in 2026

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 (3/7)

Je besser sich die Befragten informiert fühlen, desto eher stimmen sie den Aussagen zu. Der Informationsgrad beeinflusst weniger die Bedrohungswahrnehmung, aber viel mehr die Einschätzung der Handlungsmöglichkeiten: Gut informierte Unternehmen halten Schutzmassnahmen häufiger für wirksam und umsetzbar und planen eher zusätzliche Massnahmen.

Nach Informationsgrad



F015: Inwiefern stimmen Sie den folgenden Aussagen zu Cyberkriminalität wie Malware, Online-Betrug und Hacking zu?

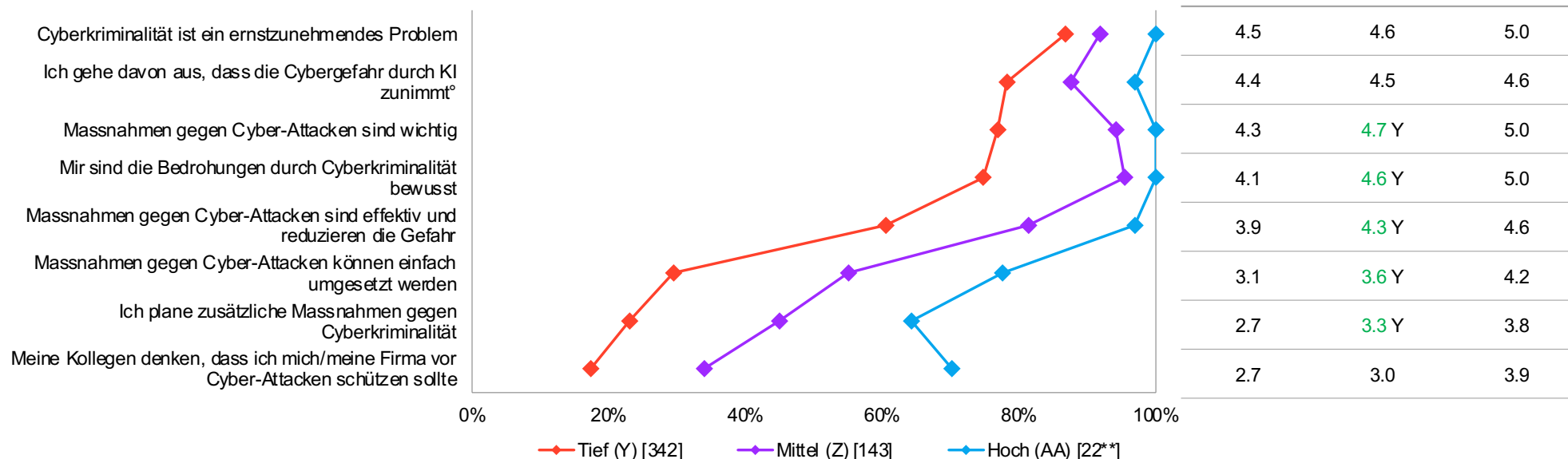
Basis: n=[] | Filter: KMU | Skalierte Frage: 1= überhaupt nicht bis 5= voll und ganz | Top2 und Mittelwerte ausgewiesen | *Neu in 2026

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)

Je höher der technische Umsetzungsgrad, desto höher die Zustimmung zu den Aussagen. Die grössten Unterschiede zeigen sich bei der Einschätzung der Wirksamkeit und Umsetzbarkeit von Schutzmassnahmen, bei der Bereitschaft, zusätzliche Massnahmen umzusetzen sowie bei der Einschätzung der Meinung der Kollegen.

Nach technischer Massnahmenumsetzung



F015: Inwiefern stimmen Sie den folgenden Aussagen zu Cyberkriminalität wie Malware, Online-Betrug und Hacking zu?

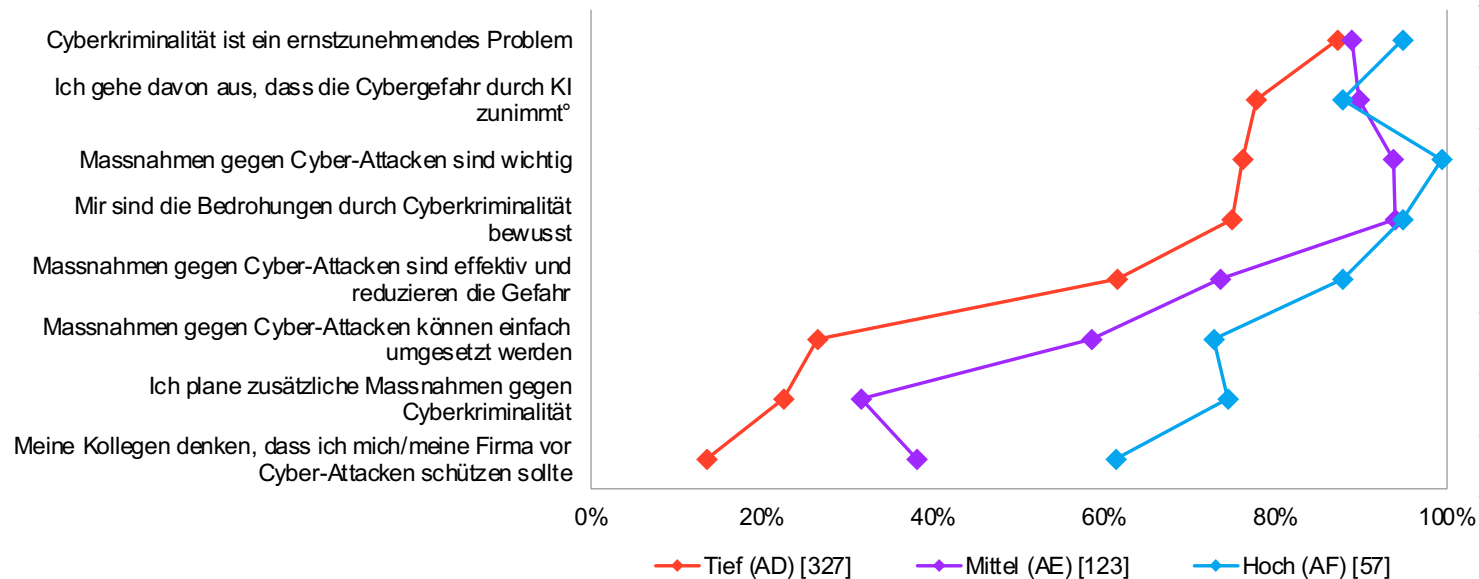
Basis: n=[] | Filter: KMU | Skalierte Frage: 1= überhaupt nicht bis 5= voll und ganz | Top2 und Mittelwerte ausgewiesen | **Sehr kleine Basis <30 | *Neu in 2026

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)

Die organisatorische Massnahmenumsetzung hängt auf dieselbe Weise mit der Einstellung zusammen: Besonders die handlungsorientierten Einstellungen werden höher bewertet, wenn die organisatorische Massnahmenumsetzung höher ist.

Nach organisatorischer Massnahmenumsetzung



Mittelwert		
Tief	Mittel	Hoch
4.5	4.6	4.7
4.4	4.5	4.6
4.2	4.7 AD	4.9
4.1	4.6 AD	4.7
3.9	4.1	4.5
3.0	3.7 AD	3.9
2.7	3.0	4.1
2.6	3.1 AD	3.6

F015: Inwiefern stimmen Sie den folgenden Aussagen zu Cyberkriminalität wie Malware, Online-Betrug und Hacking zu?

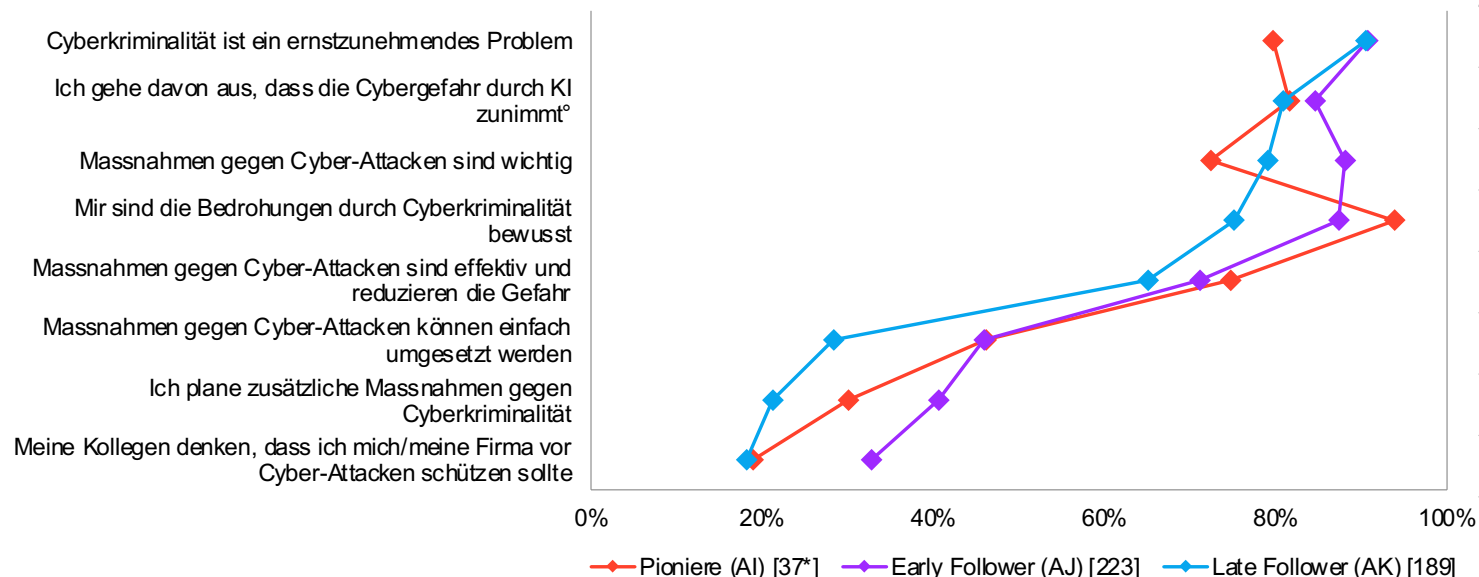
Basis: n=[] | Filter: KMU | Skalierte Frage: 1= überhaupt nicht bis 5= voll und ganz | Top2 und Mittelwerte ausgewiesen | *Neu in 2026

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)

Die Unterschiede zwischen Pionieren, Early Followern und Late Followern sind insgesamt gering. Auffällig ist jedoch, dass Early Follower Cyberkriminalität und Schutzmassnahmen tendenziell die grösste Bedeutung beimessen und am häufigsten zusätzliche Schutzmassnahmen planen.

Nach Einstellung



	Mittelwert		
	Pioniere	Early Follower	Late Follower
Cyberkriminalität ist ein ernstzunehmendes Problem	4.3	4.6	4.6
Ich gehe davon aus, dass die Cybergefahr durch KI zunimmt	4.1	4.4	4.4
Massnahmen gegen Cyber-Attacken sind wichtig	4.3	4.5	4.3
Mir sind die Bedrohungen durch Cyberkriminalität bewusst	4.6	4.4 AK	4.1
Massnahmen gegen Cyber-Attacken sind effektiv und reduzieren die Gefahr	4.0	4.0	4.0
Massnahmen gegen Cyber-Attacken können einfach umgesetzt werden	3.5	3.3	3.1
Ich plane zusätzliche Massnahmen gegen Cyberkriminalität	3.2	3.2 AK	2.7
Meine Kollegen denken, dass ich mich/meine Firma vor Cyber-Attacken schützen sollte	2.8	3.1 AK	2.7

F015: Inwiefern stimmen Sie den folgenden Aussagen zu Cyberkriminalität wie Malware, Online-Betrug und Hacking zu?

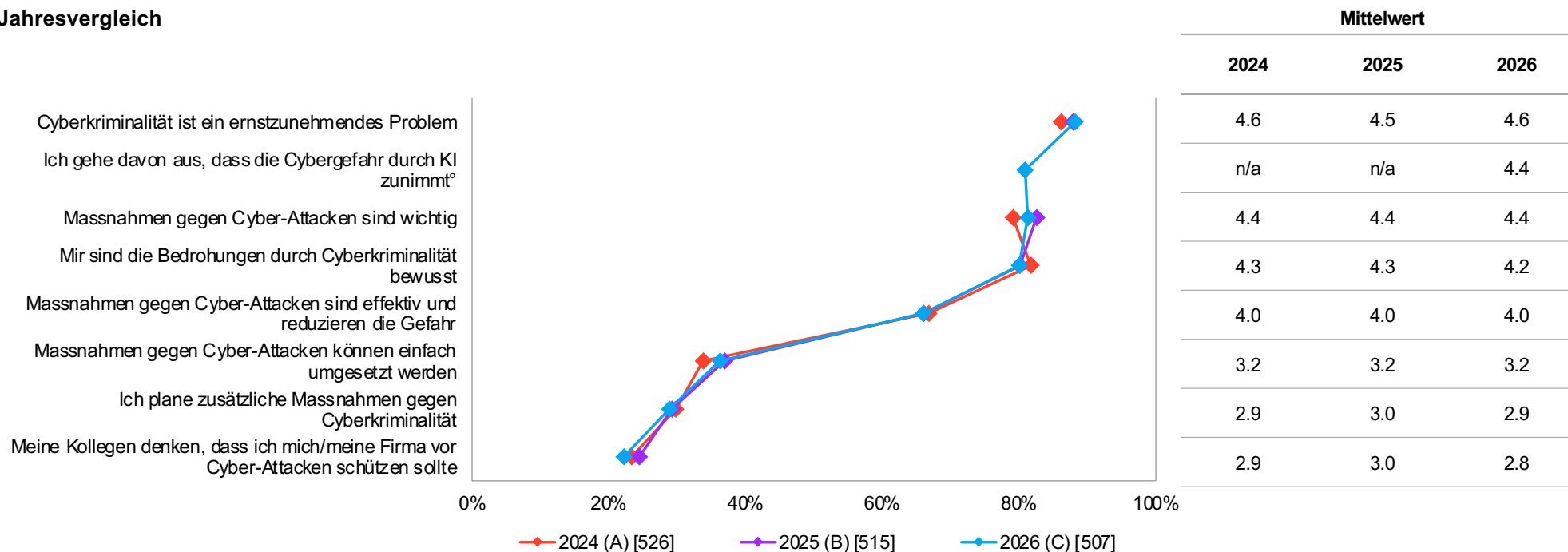
Basis: n=[] | Filter: KMU | Skalierte Frage: 1= überhaupt nicht bis 5= voll und ganz | Top2 und Mittelwerte ausgewiesen | *Kleine Basis <50 | *Neu in 2026

signifikant **höher** als Total; signifikant **tief** 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)

Die Einstellungen zu Cyberkriminalität bleiben über die Jahre weitgehend stabil. Auffallend: Die wahrgenommene Zunahme der Cybergefahr durch KI geht nicht mit einer höheren Bereitschaft zur Umsetzung zusätzlicher Schutzmassnahmen einher.

Jahresvergleich



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 | *Neu in 2026

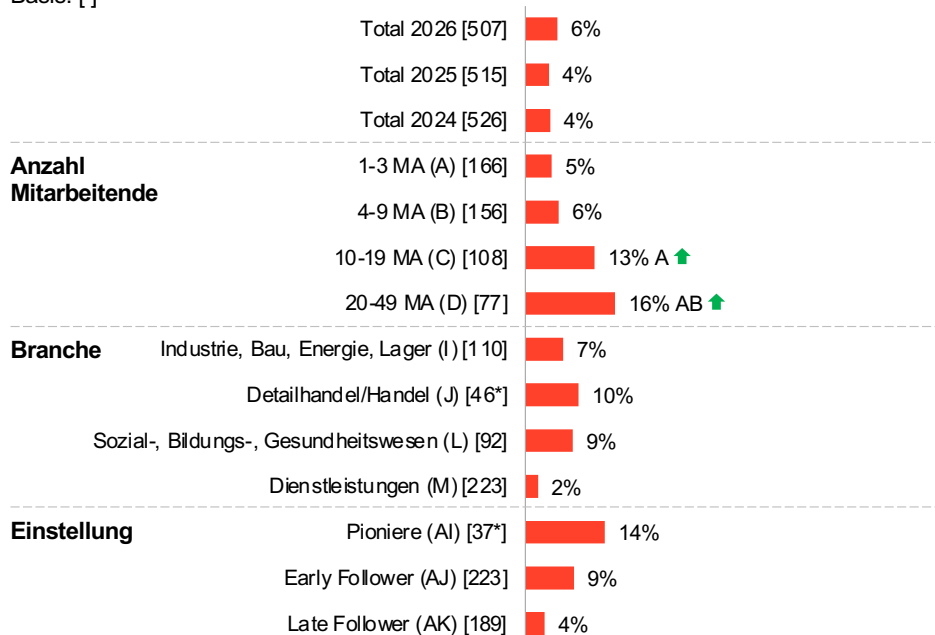
Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Erfahrung Cyberkriminalität

Sechs Prozent der befragten Unternehmen haben innerhalb der letzten 3 Jahre einen Cyberangriff erlitten. Ab 10 Mitarbeitenden ist der Anteil signifikant höher (13% resp. 16%); dieser Unterschied bestand 2025 noch nicht (4% bzw. 7%). Die Folgen der Angriffe sind häufiger operativ und persönlich als unmittelbar finanziell.

Erlittene Angriffe (Ja-Anteile)

Basis: []



Erlittene Schäden

Basis: n=44* | Filter: KMU – wenn Cyberangriff erlitten

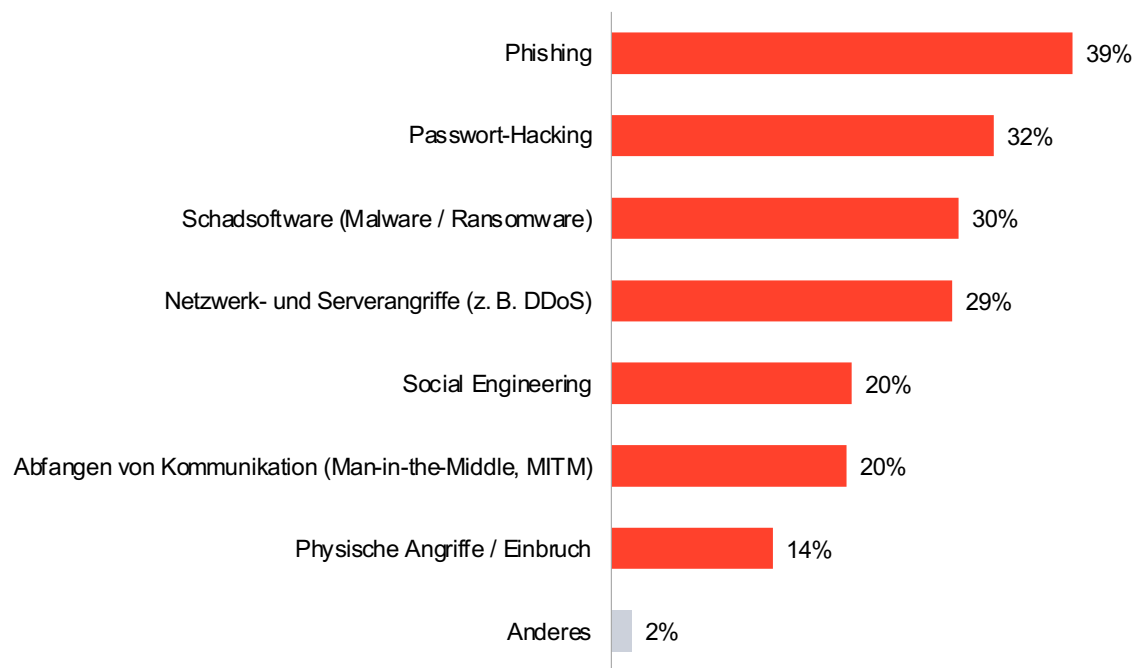
Schäden	Anzahl Fälle
Ein grosser Arbeitsaufwand zur Behebung	16
Emotionale Belastung	16
Ein finanzieller Schaden	10
Unsichere Geschäftsbeziehungen°	5
Ein Reputationsschaden	5
Ein Kundendatenverlust	4
Nichts davon	4
Weiss nicht / keine Antwort	0

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 | Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen. | °Neu in 2026

Angriffsart

Erfolgreiche Cyberangriffe erfolgen über unterschiedliche Angriffsarten. Am häufigsten werden Phishing, Passwort-Hacking, Schadsoftware sowie Netzwerk-/Serverangriffe genannt, die jeweils rund ein Drittel der Angriffe ausmachen.

(Da erfolgreiche Angriffe oft mehrere Techniken kombinieren und deren Ablauf für die Betroffenen nicht immer vollständig nachvollziehbar ist, sollten die Unterschiede zwischen den einzelnen Angriffsarten nicht überinterpretiert werden.)



F016_2: Welche Art von Angriff haben Sie erlitten?

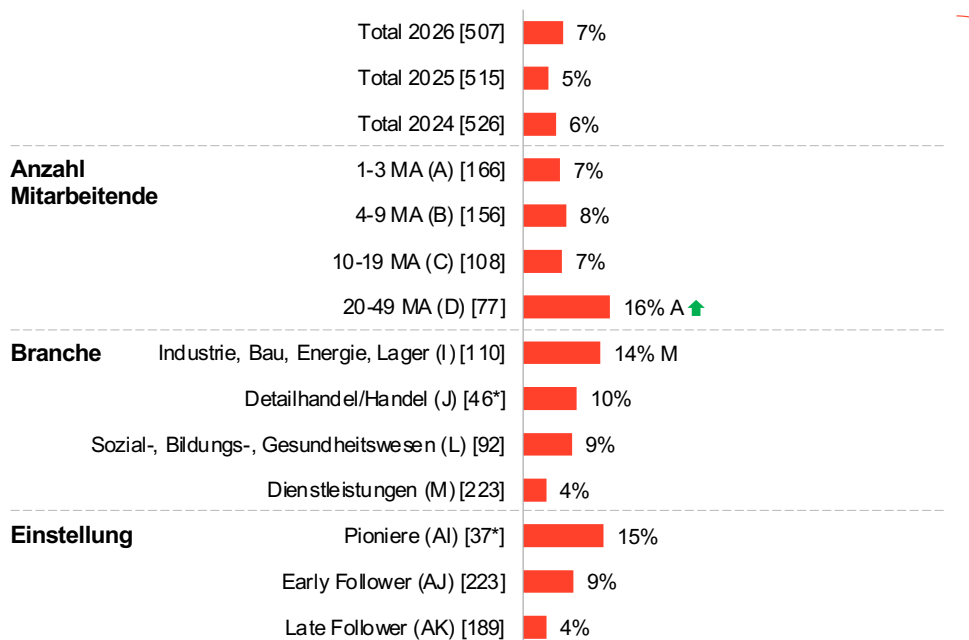
Basis: n=44* | Filter: KMU – wenn Cyberangriff erlitten | Geschlossene Frage | Neue Frage in 2026 | *Kleine Basis <50

Erpressung

Sieben Prozent der befragten Unternehmen wurden schon einmal durch Cyberkriminelle erpresst; Unternehmen mit 20+ Mitarbeitenden und Unternehmen der Industrie-/Bau-Branche sind eher betroffen. Sechs der 37 erpressten Unternehmen haben schon einmal Lösegeld an Cyberkriminelle bezahlt.

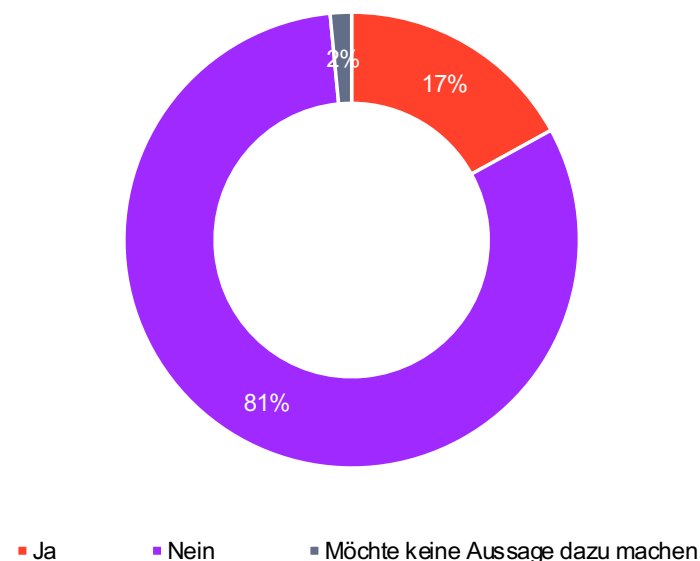
Erpressung durch Cyberkriminelle (Ja-Anteile)

Basis: n=507



Lösegeld an Cyberkriminelle

Basis: n=37 | Filter: durch Cyberkriminelle erpresste Befragte



F019: Wurde Ihr Unternehmen schon einmal von Cyberkriminellen erpresst? | F020: Hat Ihr Unternehmen schon einmal Lösegeld an Cyberkriminelle bezahlt?

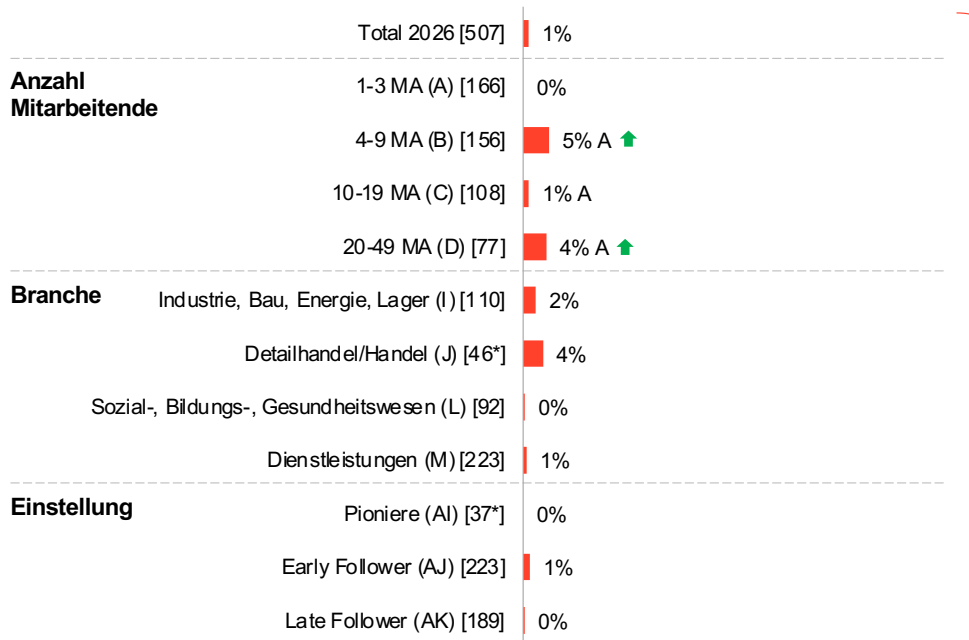
Basis: n=[] | Filter: siehe oben | Geschlossene Fragen | ↑ signifikant höher als Total; ↓ signifikant tiefer als Total | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle | Datenbeschriftung ab 3% | *Kleine Basis <50 | Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Irrtümliche Geldeinzahlungen (CEO-Betrug)

Irrtümliche Geldüberweisungen aufgrund betrügerischer E-Mails sind selten: Nur 1% der KMU berichtet von einem entsprechenden Vorfall. Ist eine Überweisung erst einmal erfolgt, kann das Geld jedoch meist nicht mehr zurückgewonnen werden.

Irrtümliche Geldeinzahlungen / CEO-Betrug (Ja-Anteile)

Basis: [] | Filter: KMU



Geldverlust bei Betrug

Basis: n=5 | Filter: schon einmal irrtümlich Geld überwiesen

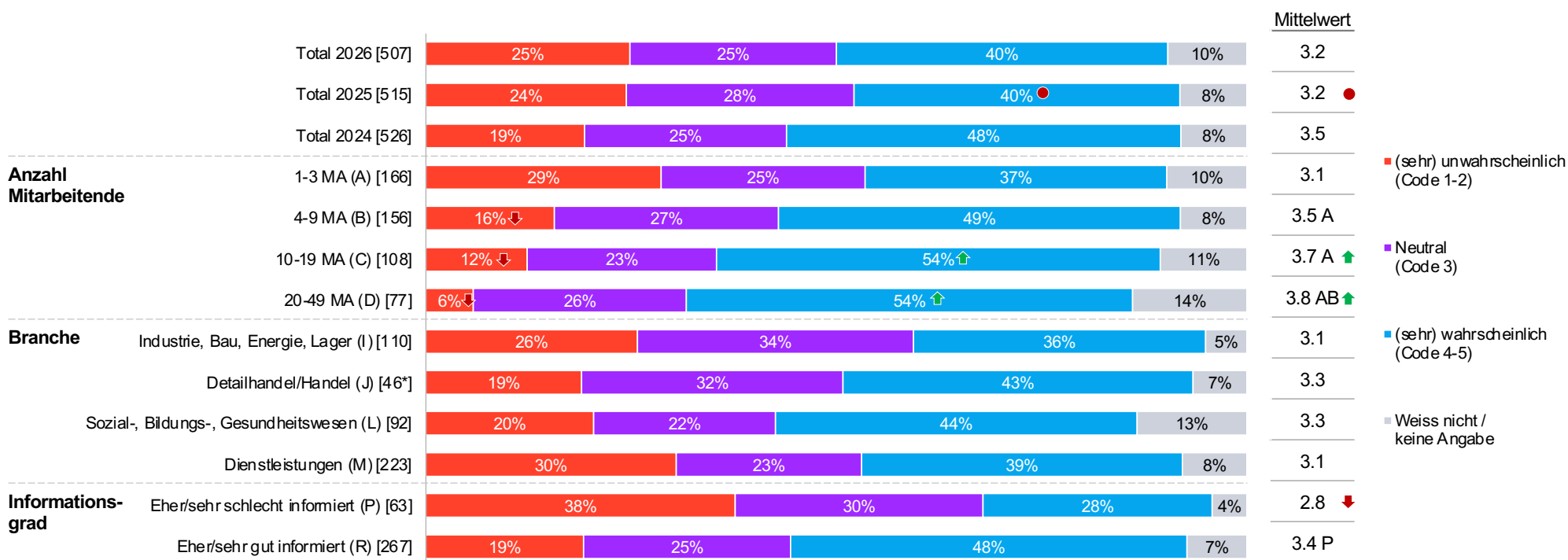
- 5 Unternehmen haben angegeben, schon einmal irrtümlich Geld überwiesen zu haben.
- 1 betroffenes Unternehmen konnte das Geld zurückgewinnen.

F068: Hat Ihr Unternehmen schon einmal irrtümlich Geld einbezahlt / überwiesen? | 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 | Fragetextanpassung in 2026 | Datenbeschriftung ab 3% | *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.

Erhöhung Sicherheitsmassnahmen

Zwei Fünftel der KMU halten zusätzliche Sicherheitsmassnahmen in den nächsten 1-3 Jahren für wahrscheinlich. Die Bereitschaft steigt mit der Unternehmensgrösse und dem Informationsgrad.



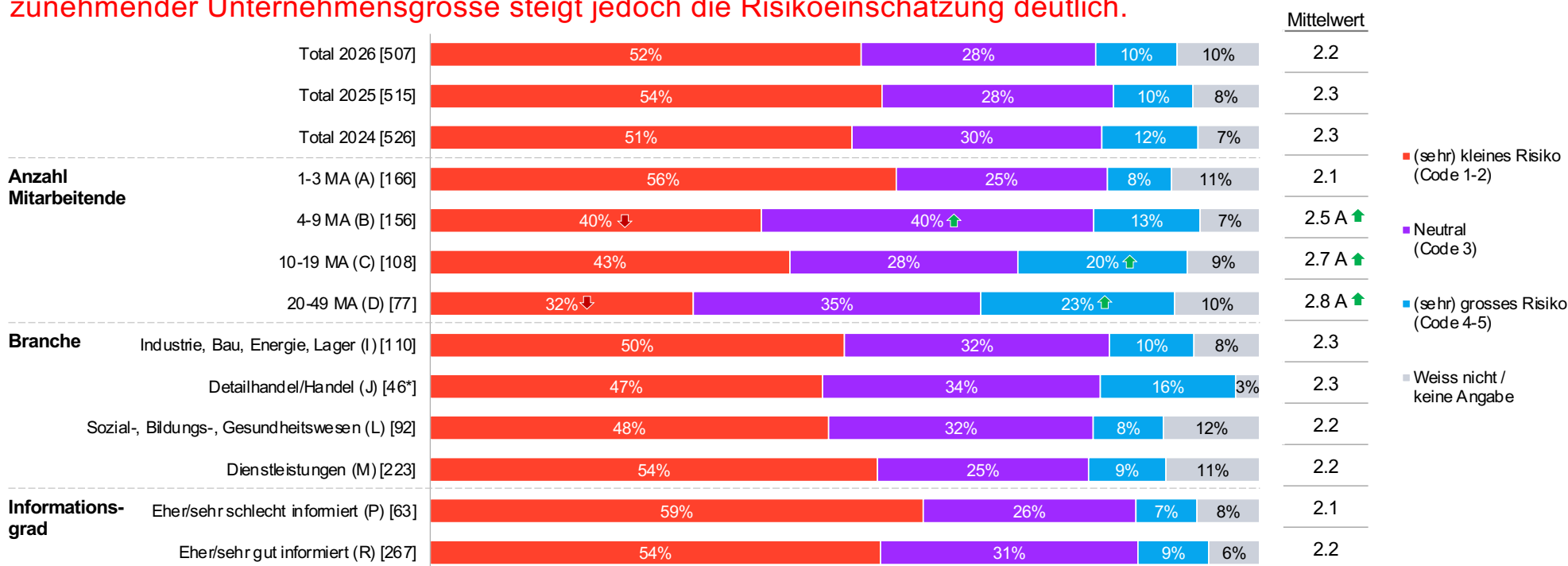
F018: Wie wahrscheinlich ist es, dass Sie in den kommenden 1 bis 3 Jahren die Sicherheitsmassnahmen gegen Cyberkriminalität erhöhen werden? | Basis: n=[] | Filter: KMU |

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%

Risikoeinschätzung

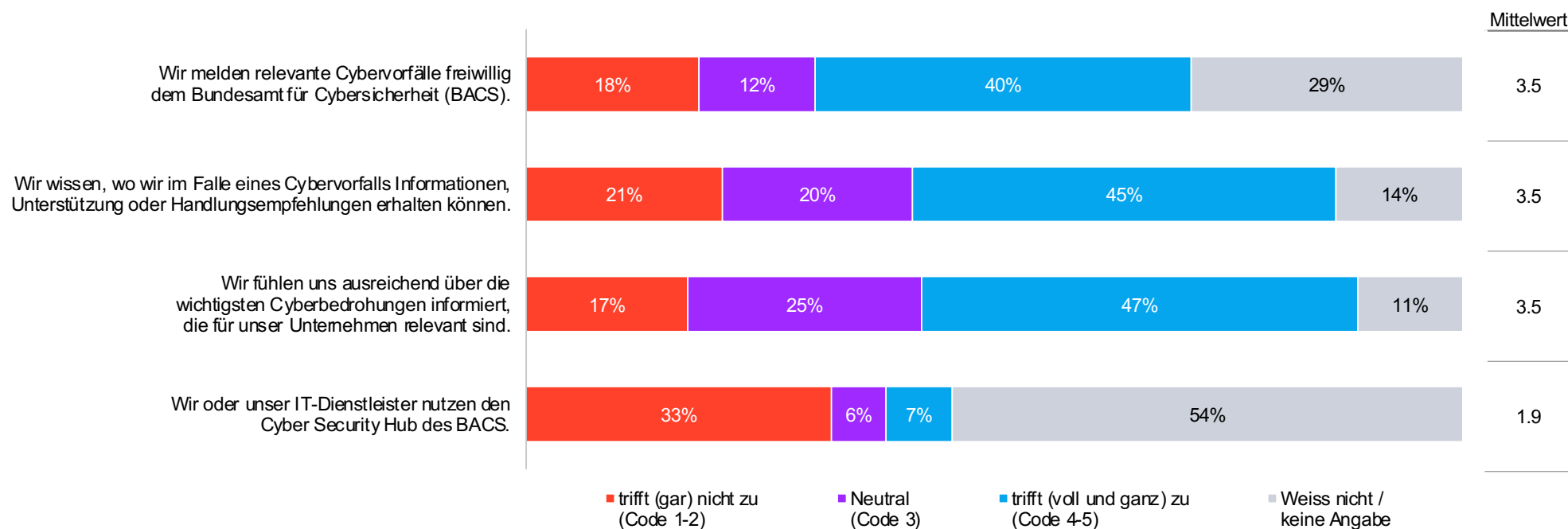
Obwohl Cyberkriminalität als ernstzunehmende Bedrohung wahrgenommen wird, schätzt eine Mehrheit der KMU das Risiko eines Angriffs mit mindestens eintägigem Betriebsausfall in den nächsten 2-3 Jahren als gering ein. Mit zunehmender Unternehmensgrösse steigt jedoch die Risikoeinschätzung deutlich.



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=507 | 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.

Kenntnis Cyberbedrohungslage und Unterstützung

Viele KMU fühlen sich grundsätzlich über Cyberbedrohungen informiert und wissen, wo sie im Ernstfall Unterstützung erhalten. Der Cyber Security Hub des BACS ist hingegen noch wenig bekannt und wird erst von 7% der Unternehmen genutzt.



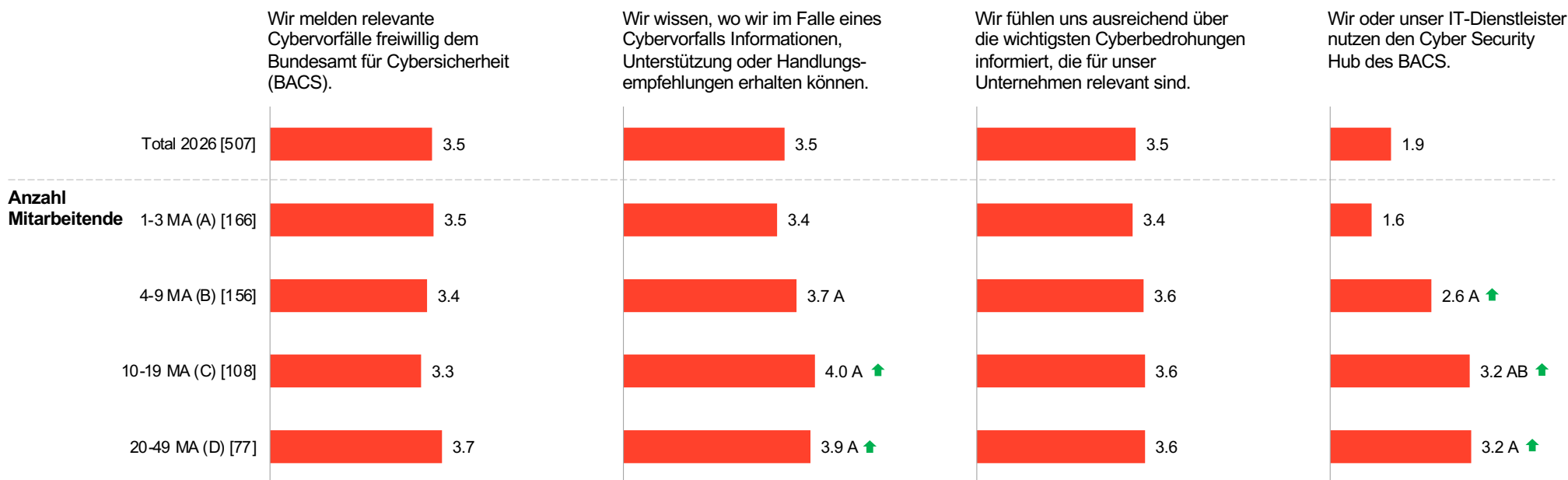
F073: Wie sehr stimmen Sie den folgenden Aussagen zu oder nicht zu?

Basis: n=507 | Filter: KMU | Skalierte Frage: 1= trifft gar nicht zu bis 5= trifft voll und ganz zu | Neue Frage in 2026

Kenntnis Cyberbedrohungslage und Unterstützung

Während sich KMU aller Grössen ausreichend über **ihre relevanten** Cyberbedrohungen informiert fühlen, verfügen grössere Unternehmen über konkretere Kenntnisse zu Unterstützungsangeboten und nutzen den Cyber Security Hub des BACS häufiger.

Nach Anzahl Mitarbeitenden



F073: Wie sehr stimmen Sie den folgenden Aussagen zu oder nicht zu?

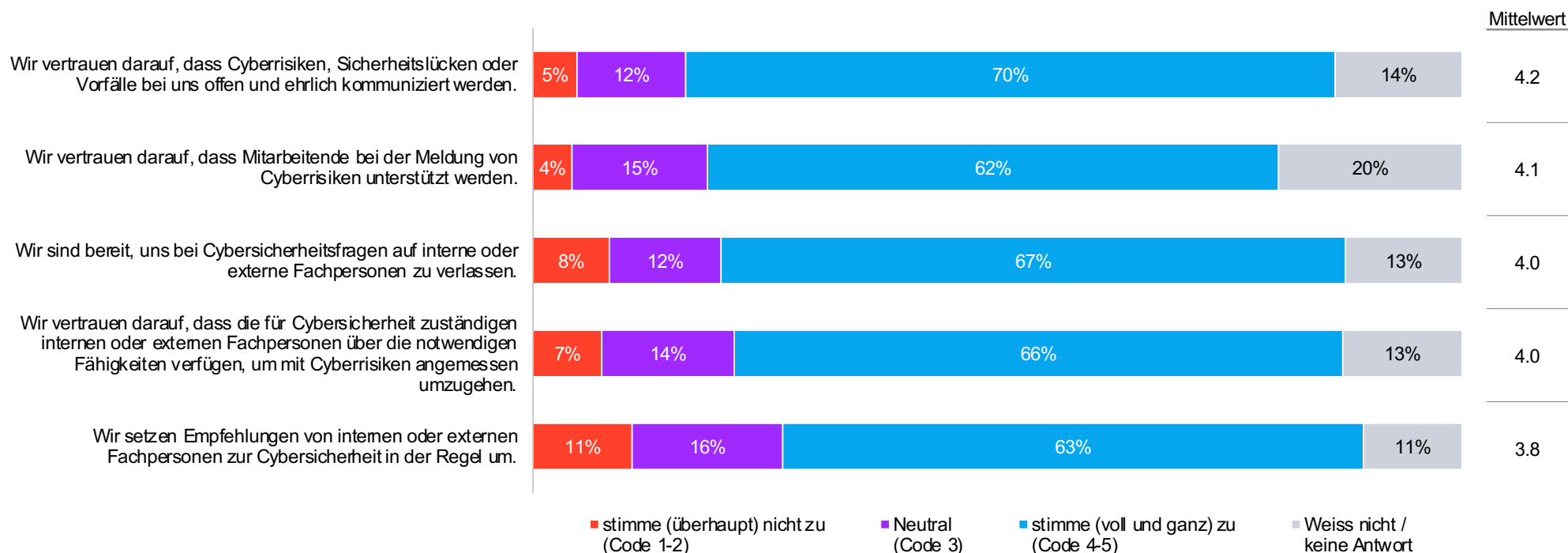
Basis: n=[] | Filter: KMU | Skalierte Frage: 1= trifft gar nicht zu bis 5= trifft voll und ganz zu | Neue Frage in 2026

↑ signifikant höher als Total; ↓ signifikant tiefer als Total | 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.

Vertrauen

Die Vertrauenswerte fallen über alle Dimensionen hinweg hoch aus. Am kritischsten wird noch die konsequente Umsetzung von Empfehlungen interner oder externer Fachpersonen beurteilt.



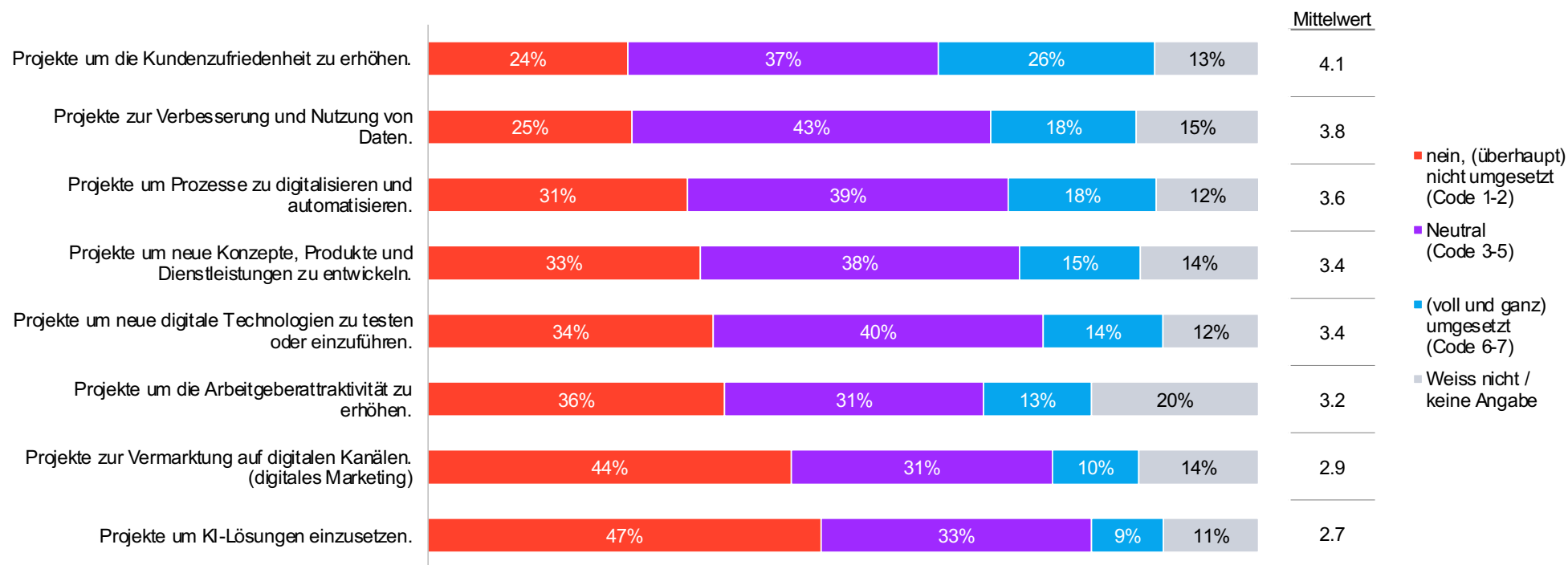
F071: Wie sehr stimmen Sie den folgenden Aussagen zu oder nicht zu? (Vertrauen nach Mayer et al., 1995)

Basis: n=507 | Filter: KMU | Skalierte Frage: 1= stimme überhaupt nicht zu bis 5= trifft stimme voll und ganz zu | Neue Frage in 2026

04.2 Digitale Strategie & ESG

Digitale Strategiemassnahmen (1/3)

Digitale Strategiemassnahmen konzentrieren sich in KMU vor allem auf Kundenzufriedenheit, Datennutzung und Prozessoptimierung. Projekte zur Entwicklung neuer Geschäftsmöglichkeiten sowie zur Einführung neuer Technologien und KI-Lösungen sind deutlich weniger verbreitet.

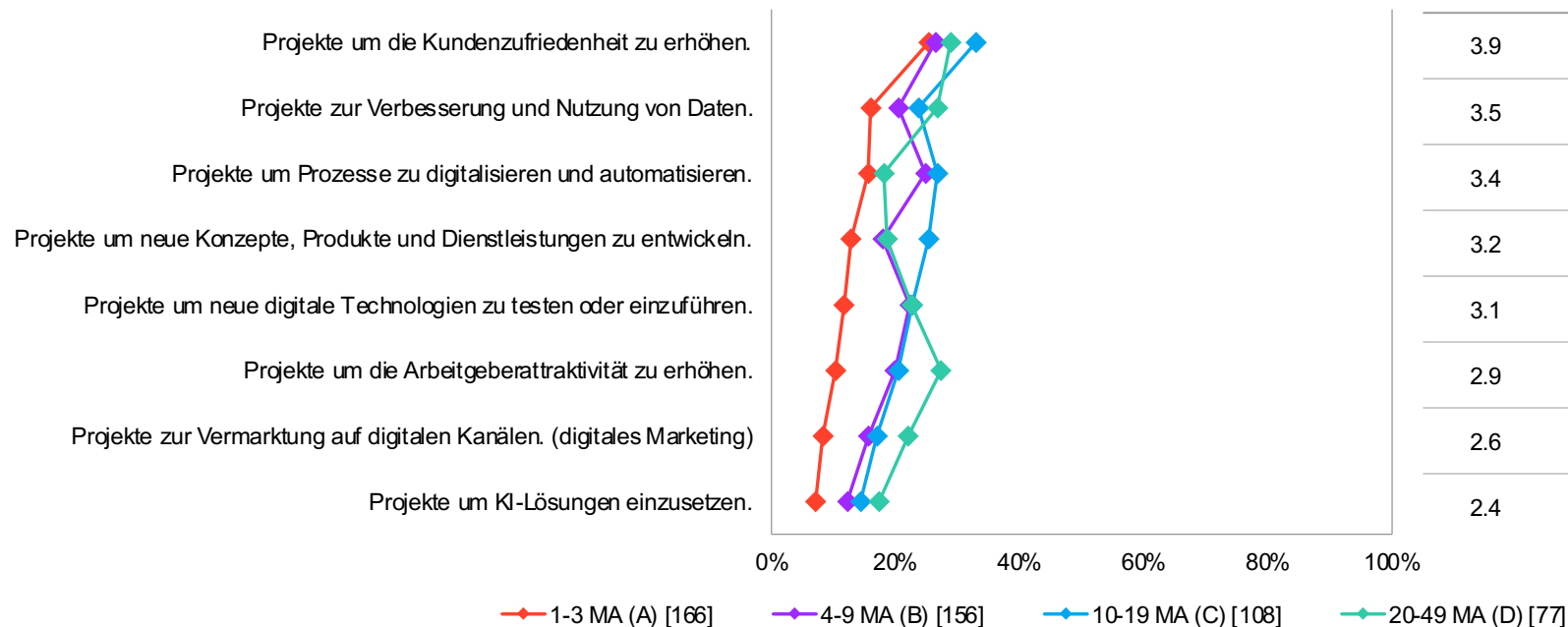


F041: Bitte geben Sie auf einer Skala von 1-7 an, inwiefern Ihr Unternehmen in den vergangenen drei Jahren die folgenden Massnahmen umgesetzt hat.
Basis: n=507 | Filter: KMU | Skalierte Frage: 1= nein, überhaupt nicht umgesetzt bis 7= voll und ganz umgesetzt | Neue Frage in 2025

Digitale Strategiemassnahmen (2/3)

Unternehmen mit 1-3 Mitarbeitenden sind bei der Umsetzung digitaler Strategiemassnahmen am wenigsten fortgeschritten, Unternehmen mit 20-49 Mitarbeitenden am weitesten.

Nach Anzahl Mitarbeitenden



Mittelwert

	1-3 MA	4-9 MA	10-19 MA	20-49 MA
Projekte um die Kundenzufriedenheit zu erhöhen.	3.9	4.4	4.8 A	4.8 A
Projekte zur Verbesserung und Nutzung von Daten.	3.5	4.2 A	4.3 A	4.8 AB
Projekte um Prozesse zu digitalisieren und automatisieren.	3.4	4.2 A	4.3 A	4.5 A
Projekte um neue Konzepte, Produkte und Dienstleistungen zu entwickeln.	3.2	3.8 A	4.0 A	4.3 A
Projekte um neue digitale Technologien zu testen oder einzuführen.	3.1	4.0 A	4.5 AB	4.7 AB
Projekte um die Arbeitgeberattraktivität zu erhöhen.	2.9	3.8 A	4.0 A	4.4 AB
Projekte zur Vermarktung auf digitalen Kanälen. (digitales Marketing)	2.6	3.7 A	3.9 A	4.2 A
Projekte um KI-Lösungen einzusetzen.	2.4	3.2 A	3.5 A	3.7 A

F041: Bitte geben Sie auf einer Skala von 1-7 an, inwiefern Ihr Unternehmen in den vergangenen drei Jahren die folgenden Massnahmen umgesetzt hat.

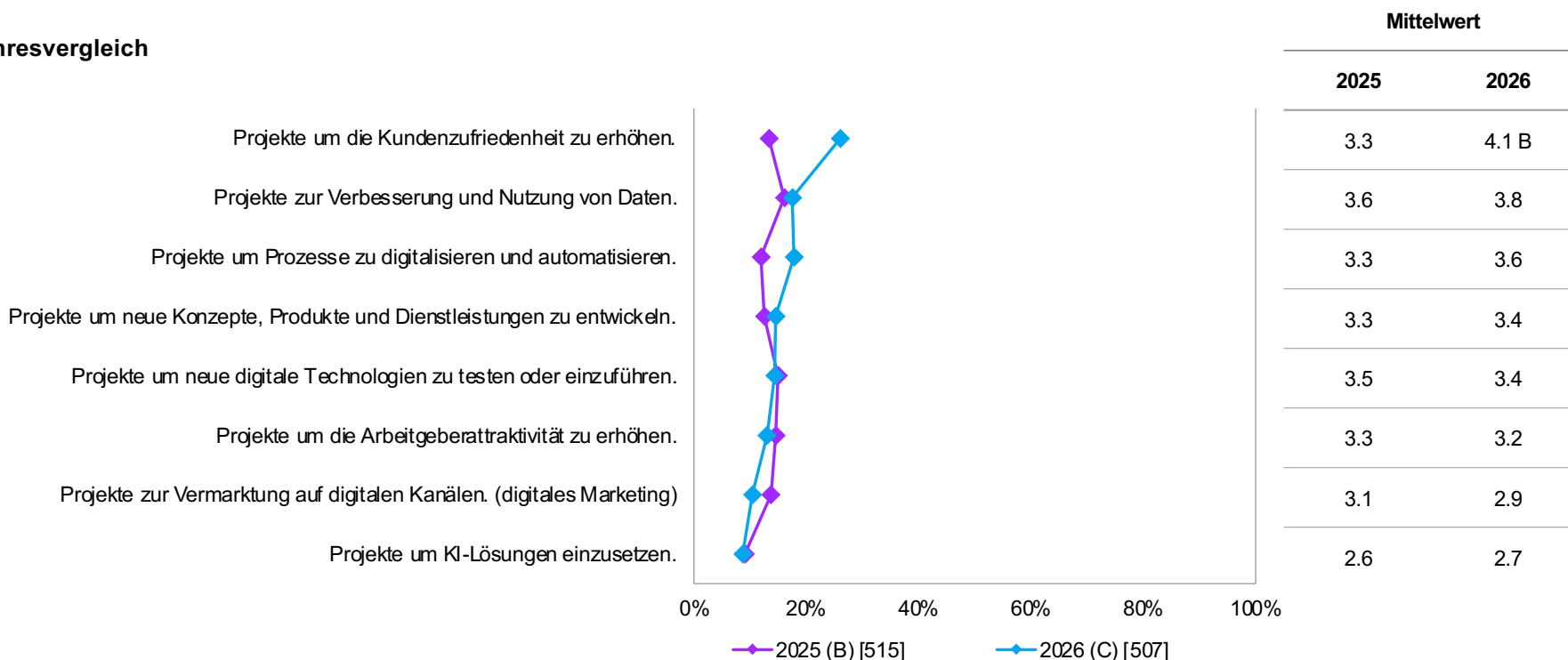
Basis: n=[] | Filter: KMU | Skalierte Frage: 1= nein, überhaupt nicht umgesetzt bis 7= voll und ganz umgesetzt | Neue Frage in 2025 | Top2 und Mittelwerte ausgewiesen

signifikant **höher** als Total; signifikant **tief**er 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 (3/3)

Digitale Strategiemassnahmen werden 2026 insgesamt ähnlich beurteilt wie im Vorjahr. Deutlich häufiger umgesetzt werden jedoch Projekte zur Steigerung der Kundenzufriedenheit.

Jahresvergleich



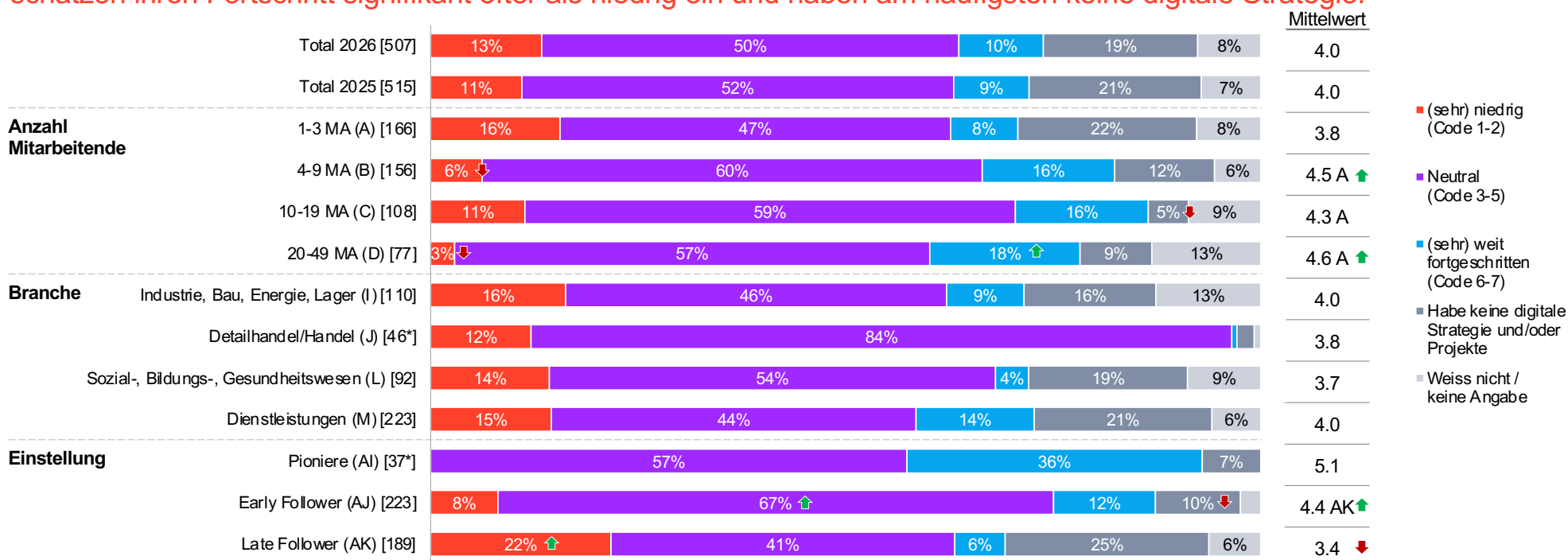
F041: Bitte geben Sie auf einer Skala von 1-7 an, inwiefern Ihr Unternehmen in den vergangenen drei Jahren die folgenden Massnahmen umgesetzt hat.

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

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

Fortschritt digitale Strategie

Fast ein Fünftel der Befragten Unternehmen hat keine digitale Strategie und/oder digitale Projekte. Rund jedes zehnte KMU hält den Fortschritt seiner digitalen Strategie für (sehr) weit fortgeschritten und 13% für (sehr) niedrig. Late Follower schätzen ihren Fortschritt signifikant öfter als niedrig ein und haben am häufigsten keine digitale Strategie.



F040: Wie schätzen Sie den Fortschritt Ihrer digitalen Strategie bzw. digitalen Transformation ein?

Basis: n=507 | Filter: KMU | Skalierte Frage: 1= sehr niedrig bis 7= sehr weit fortgeschritten | ↑ signifikant höher als Total; ↓ signifikant tiefer als Total | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle

*Kleine Basis <50 | *Kleine Basis <50 | Datenbeschriftung ab 3%

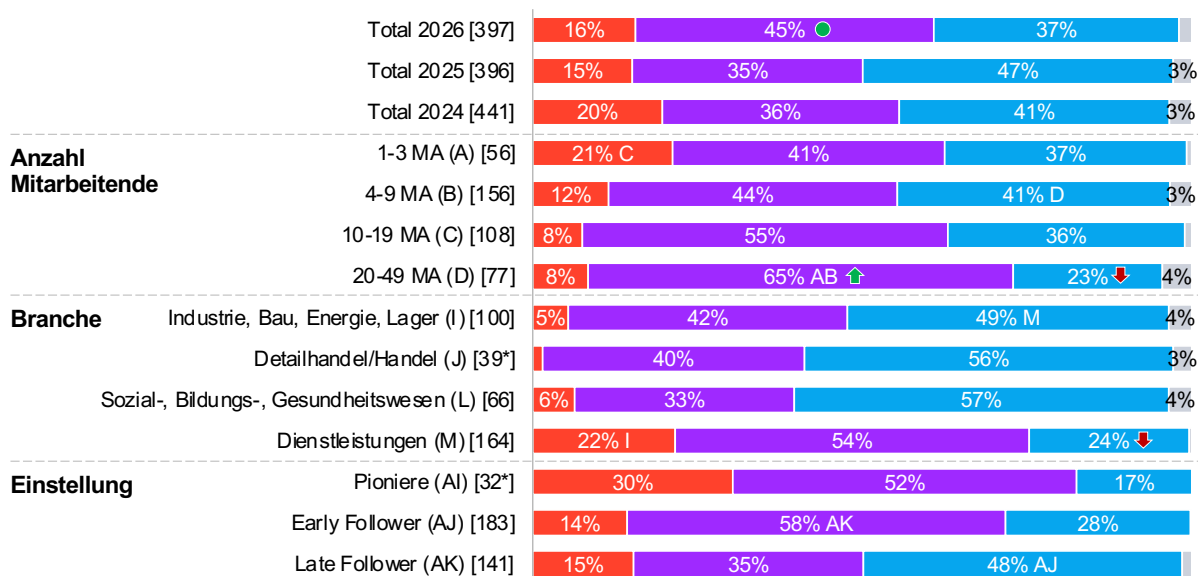
Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen. | Neue Frage in 2025

Homeoffice

Homeoffice ist bei KMU weiter verbreitet als im Vorjahr: 61% der Unternehmen bieten ihren Mitarbeitenden zumindest teilweise Homeoffice an. Gleichzeitig erwarten die meisten Unternehmen keine weitere Ausweitung, was auf eine Stabilisierung der Homeoffice-Nutzung hindeutet.

Angebot Homeoffice

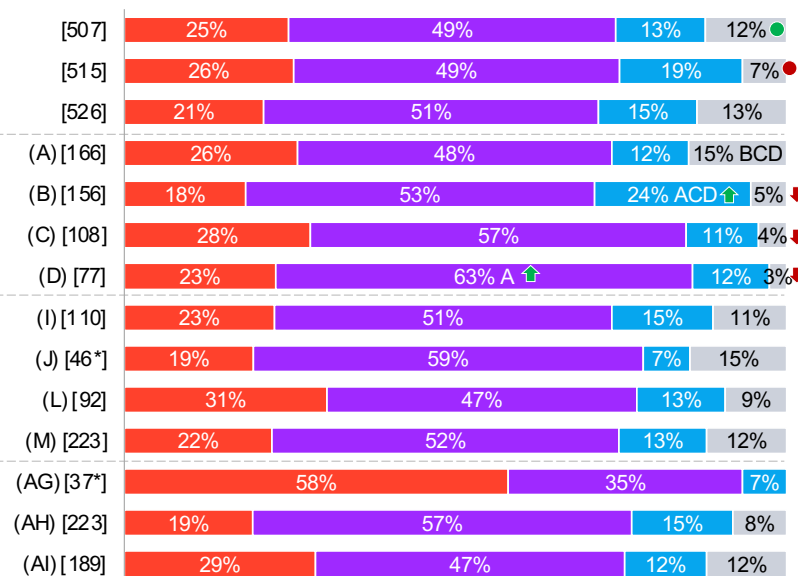
Filter: befragte Unternehmen haben mehr als eine/n Mitarbeitenden



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

Zukunftsentwicklung Homeoffice Schweiz

Filter: KMU



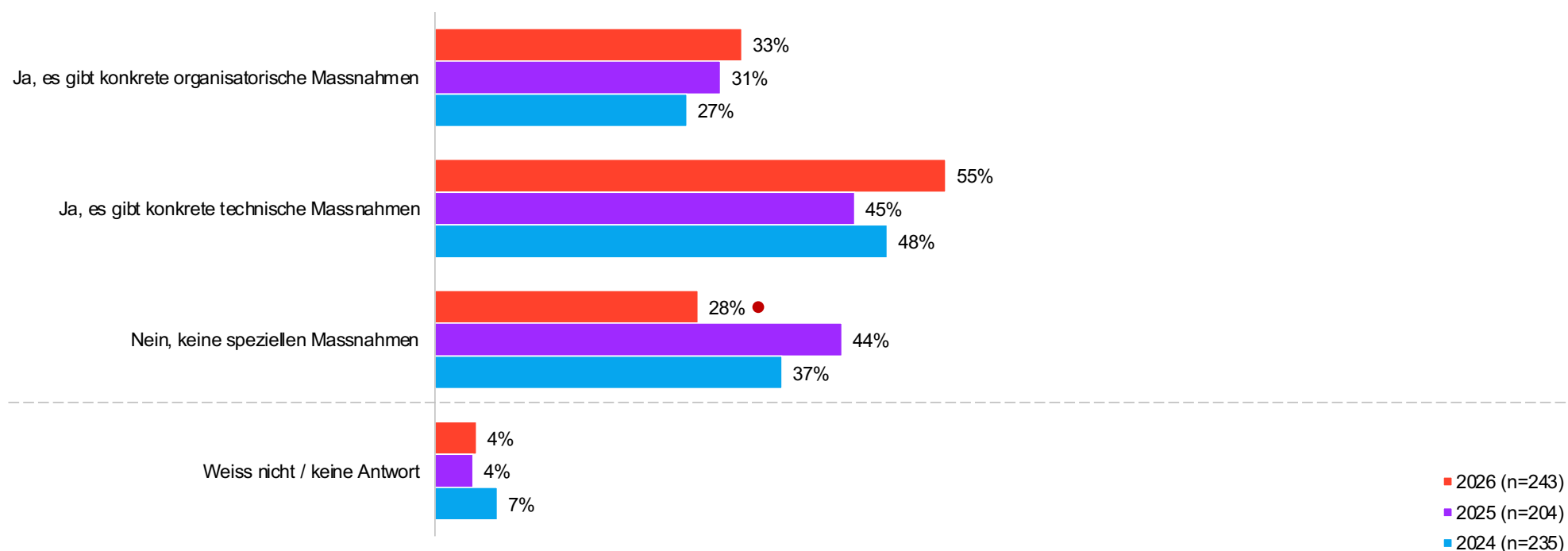
■ Es wird mehr Mitarbeitende im HO geben ■ Es wird etwa so bleiben
 ■ Es wird weniger Mitarbeitende im HO geben ■ Weiss nicht / keine Antwort

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 | *Kleine Basis <50 | Datenbeschriftung ab 3% | Die hinter den Wert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen.

Massnahmen für Homeoffice

Mit der zunehmenden Verbreitung von Homeoffice treffen immer mehr KMU spezifische Cybersicherheitsvorkehrungen. Der Anteil der Unternehmen ohne besondere Schutzmassnahmen sank gegenüber dem Vorjahr deutlich von 44% auf 28%, während insbesondere technische Sicherheitsmassnahmen häufiger eingesetzt werden.



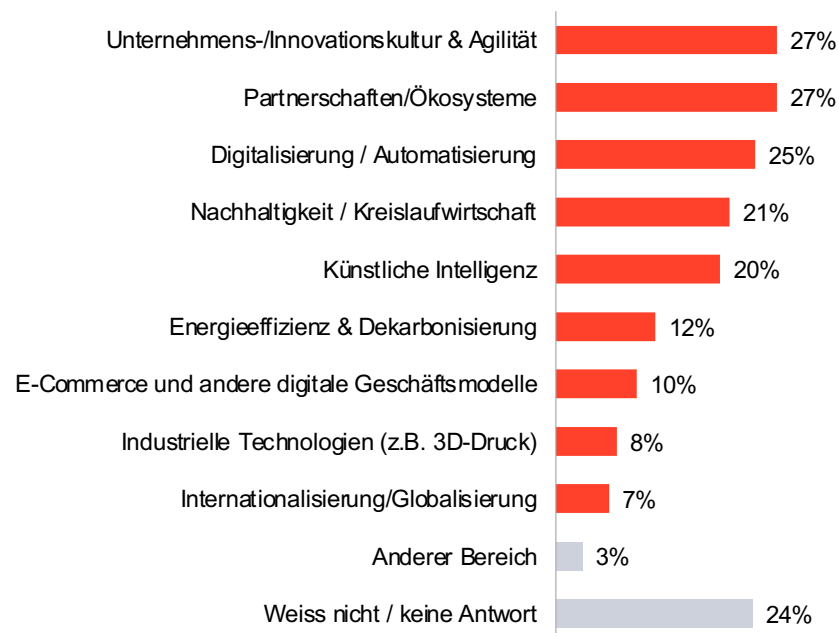
F028: Treffen Sie konkrete Vorkehrungen zum Schutz vor Cyberangriffen im Homeoffice?

Basis: n=[] | Filter: KMU – Homeoffice wird angeboten | Geschlossene Frage | ● signifikant höher als Vorwelle; ● signifikant tiefer als Vorwelle

Strategische Opportunitäten

Die grössten strategischen Chancen sehen KMU in der Unternehmens- und Innovationskultur, in Partnerschaften sowie in der Digitalisierung und Automatisierung. Mit zunehmender Unternehmensgrösse gewinnt insbesondere die Digitalisierung als strategisches Zukunftsthema an Bedeutung.

Total [507]



Anzahl Mitarbeitende

1-3 MA (A) [166]	4-9 MA (B) [156]	10-19 MA (C) [108]	20-49 MA (D) [77]
25%	33%	36%	29%
29%	20%	27%	26%
20%	33% A	47% AB	51% AB
21%	20%	33% AB	24%
18%	25%	29% A	27%
11%	13%	20% A	22% A
8%	17% A	15%	15%
6%	11%	13% A	9%
5%	11% A	14% A	7%
4%	2%	1%	1%
27% CD	19% C	8%	12%

F069_V2: Wo sehen Sie für Ihre Firma die grössten strategischen, langfristigen Chancen?

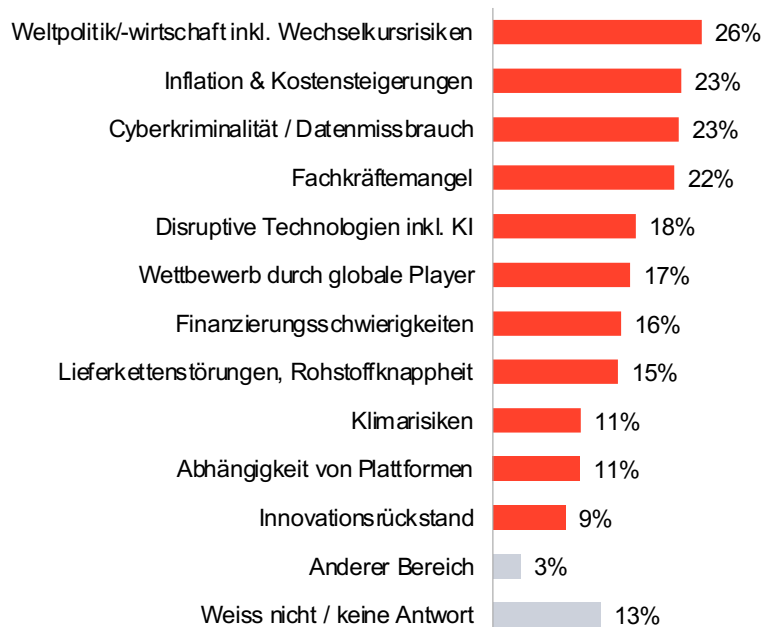
Basis: n=[] | Filter: KMU | Geschlossene Frage | signifikant **höher** als Total; signifikant **tiefer** als Total | Neue Frage in 2026

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

Strategische Risiken

Die Weltpolitik/-wirtschaft ist aus Sicht der KMU das grösste strategische Risiko. Je rund ein Fünftel bis ein Viertel sehen in Inflation, Cyberkriminalität und Fachkräftemangel strategische Risiken. Mit zunehmender Unternehmensgrösse gewinnen insbesondere Fachkräftemangel und Cyberkriminalität an Bedeutung.

Total [507]



Anzahl Mitarbeitende

1-3 MA (A) [166]	4-9 MA (B) [156]	10-19 MA (C) [108]	20-49 MA (D) [77]
25%	33% D	24%	18%
21%	32% A	24%	25%
21%	27%	25%	36% A
17%	32% A	49% AB	44% A
19%	14%	16%	15%
17%	16%	19%	17%
15%	18%	20%	22%
13%	20%	29% A	22%
11%	10%	11%	12%
11%	10%	10%	12%
8%	13%	10%	16% A
4%	4%	0%	3%
16% BC	6%	6%	9%

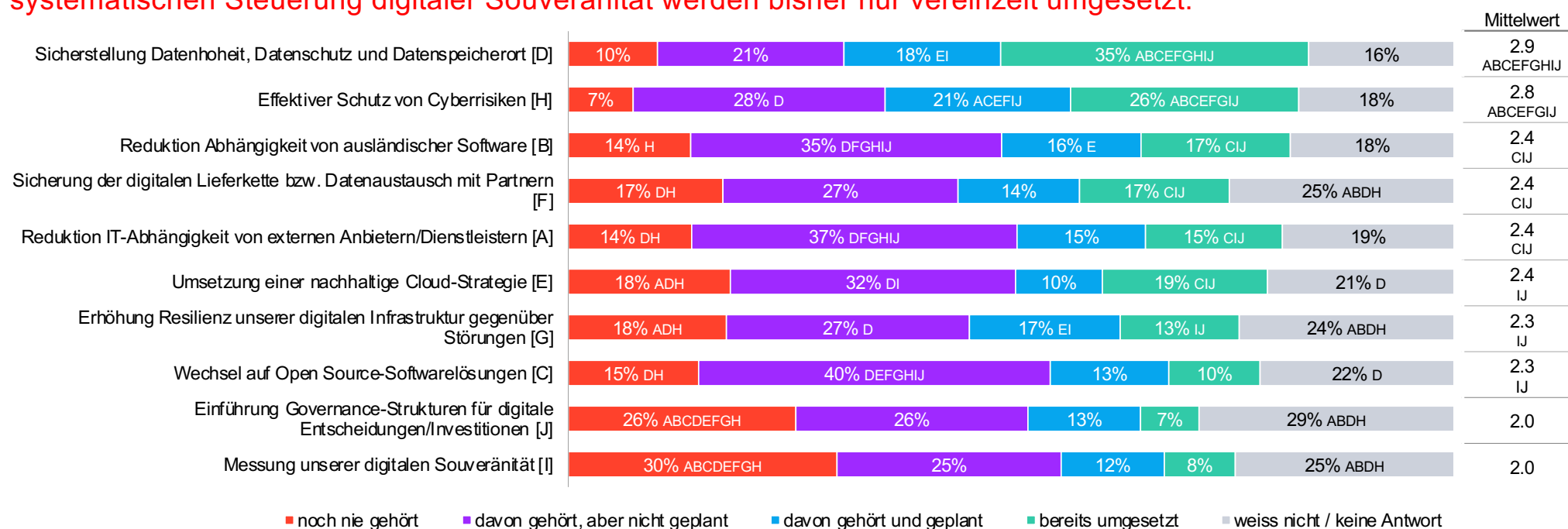
F070_V2: Wo sehen Sie für Ihre Firma die grössten strategischen, langfristigen Risiken?

Basis: n=[] | Filter: KMU | Geschlossene Frage | signifikant **höher** als Total; signifikant **tiefer** als Total | Neue Frage in 2026

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

Digitale Souveränität

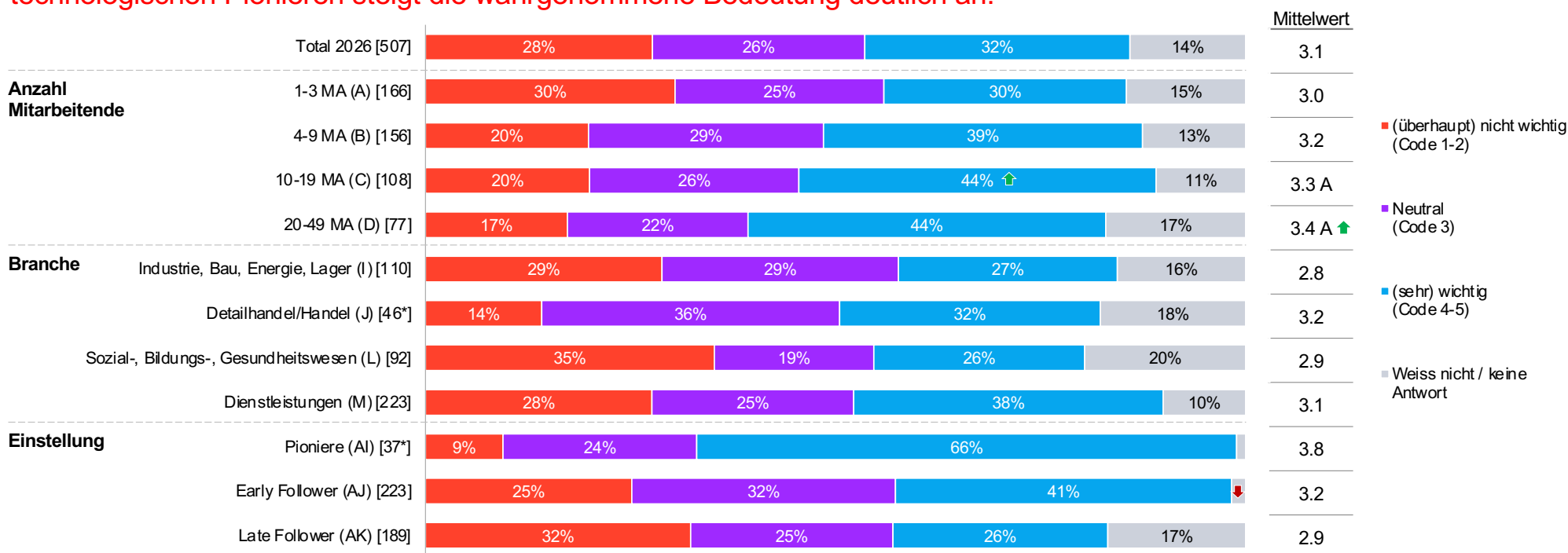
Die digitale Souveränität wird von vielen KMU bislang vor allem über Datenschutz, Datenhoheit und Cybersicherheit adressiert. Weitergehende Massnahmen zur Verringerung von Abhängigkeiten oder zur systematischen Steuerung digitaler Souveränität werden bisher nur vereinzelt umgesetzt.



F072: Haben Sie bereits Massnahmen zum Thema "digitale Souveränität" geplant oder umgesetzt?
 Basis: n=507 | Filter: KMU | Geschlossene Frage | Neue Frage in 2026

ESG-Kriterien

Rund ein Drittel der Unternehmen sehen ESG-Kriterien als (sehr) wichtig für ihr Unternehmen, während mehr als ein Viertel diese als (überhaupt) nicht wichtig ansehen. Mit zunehmender Unternehmensgrösse und insbesondere bei technologischen Pionieren steigt die wahrgenommene Bedeutung deutlich an.



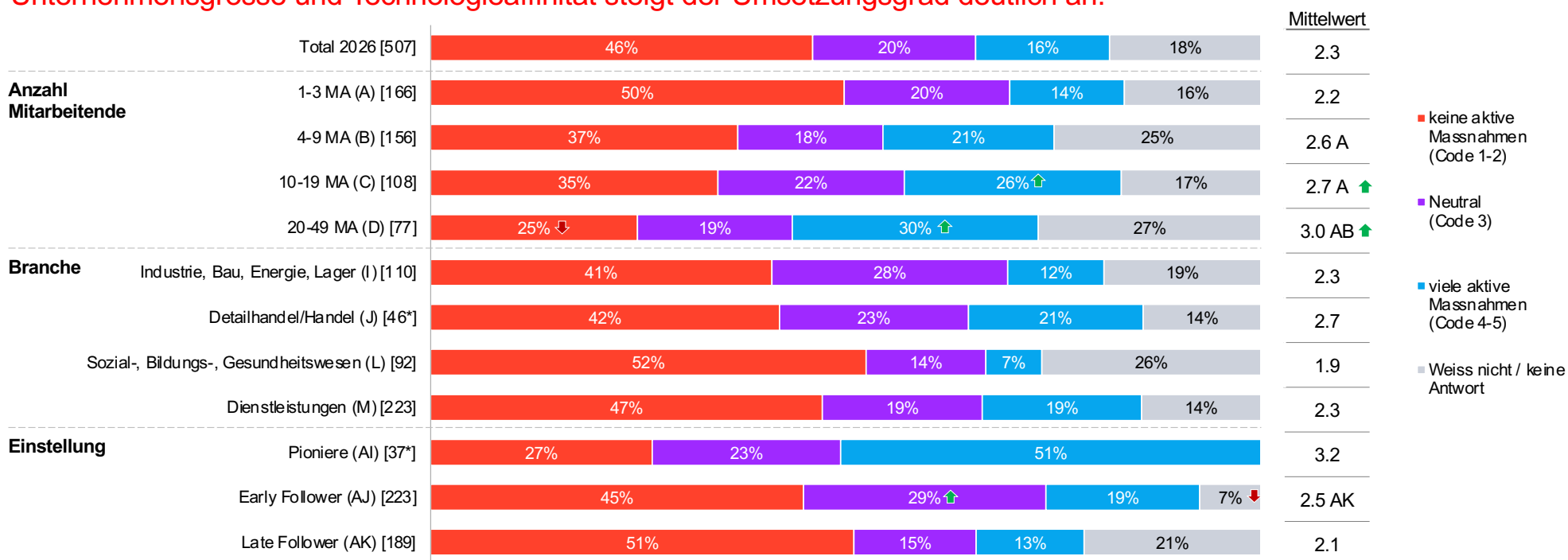
F074: Wie wichtig sind ESG-Kriterien – also Umwelt-, Sozial- und Governance-Praktiken – Ihrer Meinung nach insgesamt für den langfristigen Erfolg Ihres Unternehmens?

Basis: n=[] | Filter: KMU | Skalierte Frage: 1= überhaupt nicht wichtig bis 5= sehr wichtig | ↑ signifikant höher als Total; ↓ signifikant tiefer als Total | *Kleine Basis <50 | Datenbeschriftung ab 3%

Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen. | Neue Frage in 2026

ESG-Umsetzung

Zwischen der Bedeutung und der Umsetzung von ESG besteht eine erkennbare Lücke. Rund ein Drittel der Unternehmen stuft ESG als wichtig ein, aber nur 16% setzen entsprechende Massnahmen umfassend um. Mit zunehmender Unternehmensgrösse und Technologieaffinität steigt der Umsetzungsgrad deutlich an.



F075: Inwieweit ergreift Ihr Unternehmen aktiv ESG-Massnahmen?

Basis: n=[] | Filter: KMU | Skalierte Frage: 1= keine aktiven Massnahmen bis 5= viele aktive Massnahmen | ↑ signifikant höher als Total; ↓ signifikant tiefer als Total | *Kleine Basis <50 | Datenbeschriftung ab 3%
Die hinter den Mittelwert gesetzten Buchstaben bedeuten einen signifikanten Unterschied (95% Niveau) im Vergleich zu den jeweiligen Gruppen, für die die Buchstaben stellvertretend stehen. | Neue Frage in 2026

Thank you

/Research Reality | business.yougov.com

YouGov, 2026, all rights reserved. All materials contained herein are protected by copyright laws. Any storage, reproduction or distribution of such materials, in whole or in part, in any form without the prior written permission of YouGov is prohibited. This information (including any enclosures and attachments) is propriety and confidential and has been prepared for the exclusive use and benefit of the addressee(s) and solely for the purpose for which it is provided. We make no representations, warranties or guarantees, whether express or implied, that the information is accurate, complete or up to date. We exclude all implied conditions, warranties, representations or other terms that may apply and we will not be liable to you for any loss or damage, whether in contract, tort (including negligence), breach of statutory duty, or otherwise, even if foreseeable, arising under or in connection with use of or reliance on the information. We do not exclude or limit in any way our liability to you where it would be unlawful to do so.