STUDIE STATUS IT-SICHERHEIT KMU ÖSTERREICH 2018

techbold

mindtake

mindtake
360° ANALYTICS AND INSIGHTS

Der vorliegende Bericht wurde im Auftrag
von techbold technology Group AG erstellt.
Er ist alleiniges Eigentum des Auftraggebers.

MindTake Research GmbH
Wien, Juni 2018

INHALT

ECKDATEN DER STUDIE

- Ziel der Studie:

  Im Zeitalter elektronischer Geschäftsprozesse ist eine funktionierende und sichere IT-Infrastruktur eine Voraussetzung für die Leistungsfähigkeit der Österreichischen Unternehmen. Ziel der Studie ist es:

  - Ermittlung des IST Zustandes des IT-Sicherheitsmanagements, sowie der Sicherheit der IT-Infrastruktur
  - Identifikation von kritischen Bereichen mit der Zielsetzung der Sensibilisierung der betroffenen Unternehmen

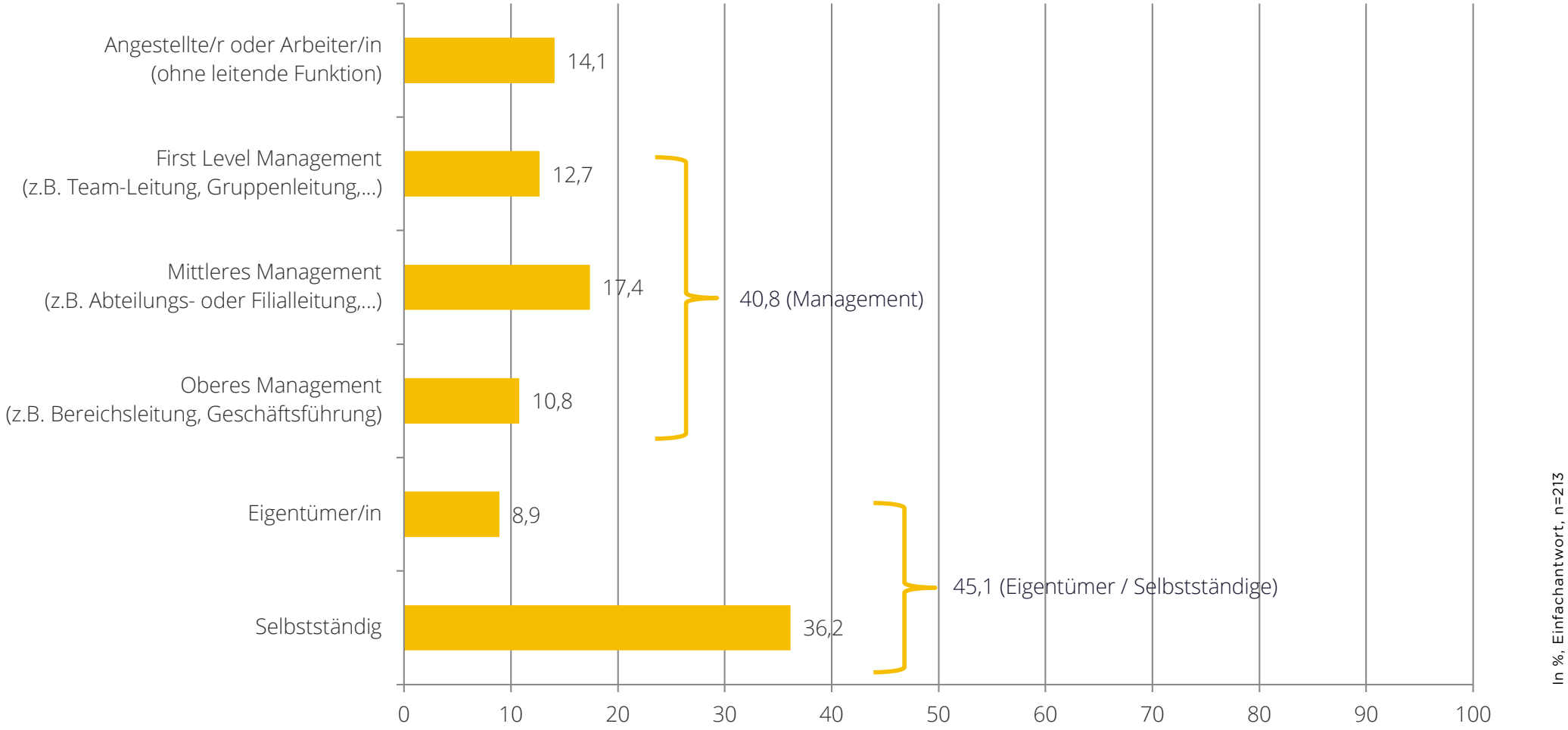
- Erhebungsmethode:

  Computer Assisted Web Interviews (CAWI) im Talk Online-Panel

- Zielgruppe: IT-Entscheider in KMUs (bis 250 Mitarbeiter) in den Branchen produzierendes Gewerbe, Handel und Dienstleistung
- Stichprobengröße: n=213
- Erhebungszeitraum: 7.6.2018 – 19.6.2018
- Befragungsdauer: 4,18 Minuten (Median)

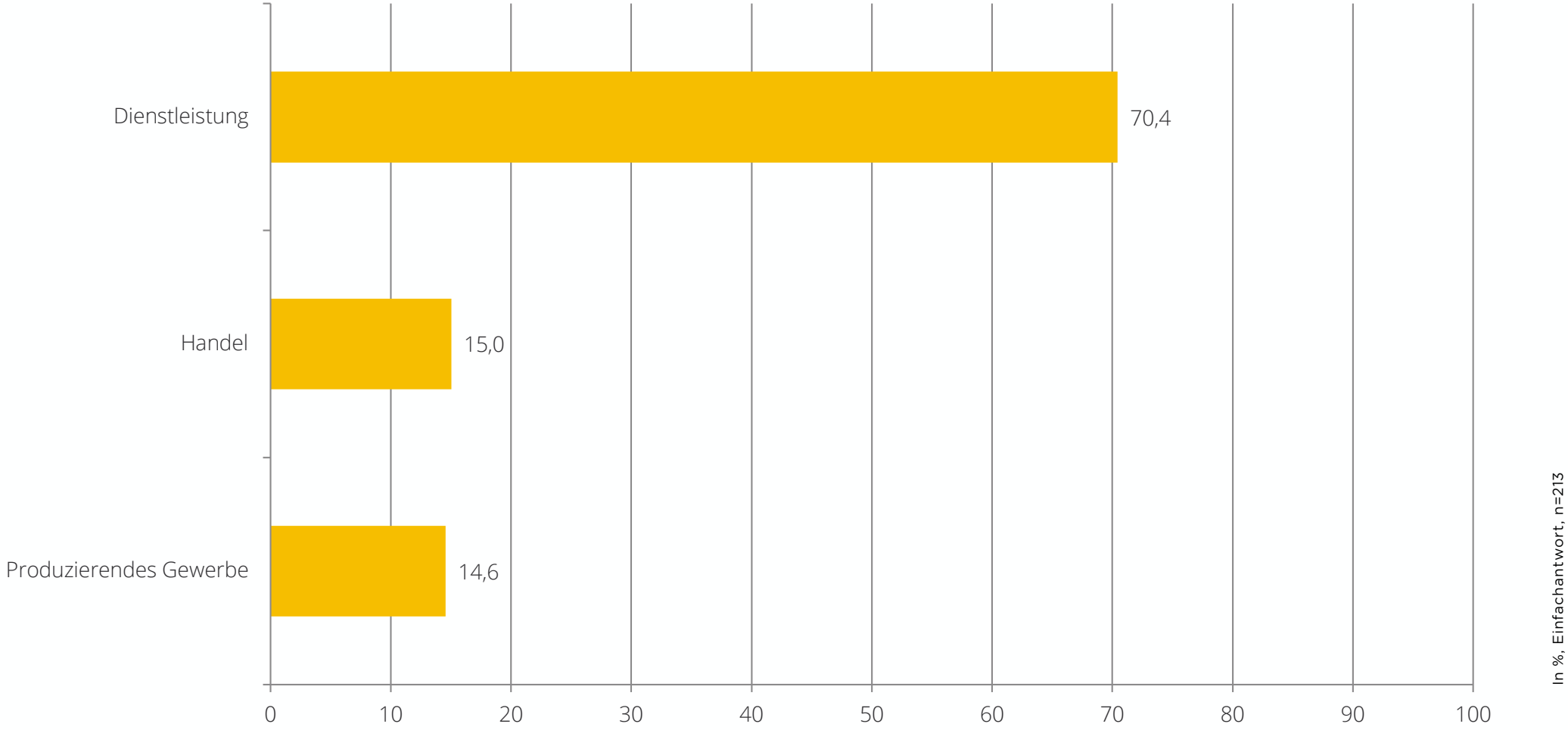
BESCHREIBUNG DER STICHPROBE (1/4)

„In welcher Position sind Sie tätig?“



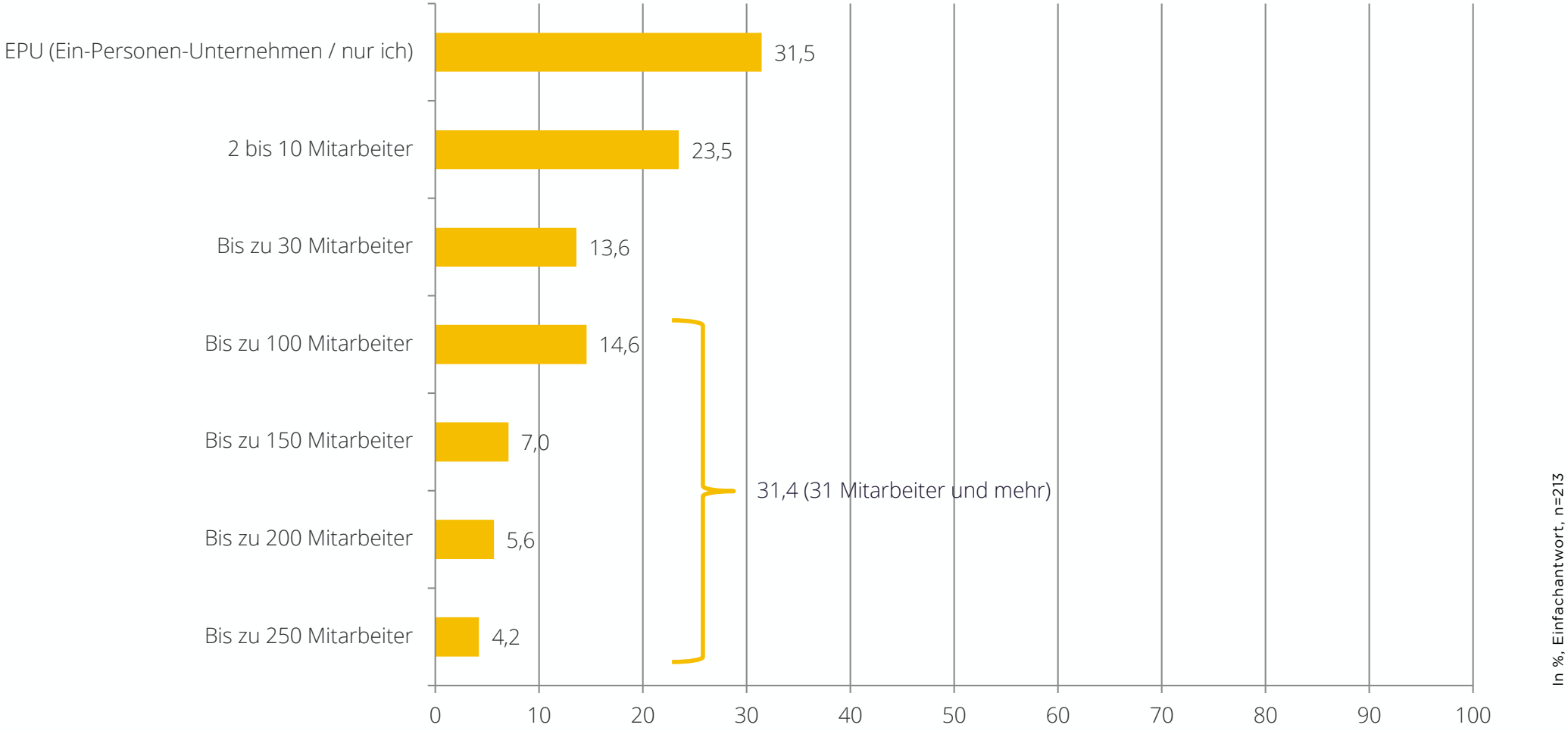
BESCHREIBUNG DER STICHPROBE (2/4)

„In welcher Branche ist Ihr Unternehmen bzw. Arbeitgeber hauptsächlich tätig?“



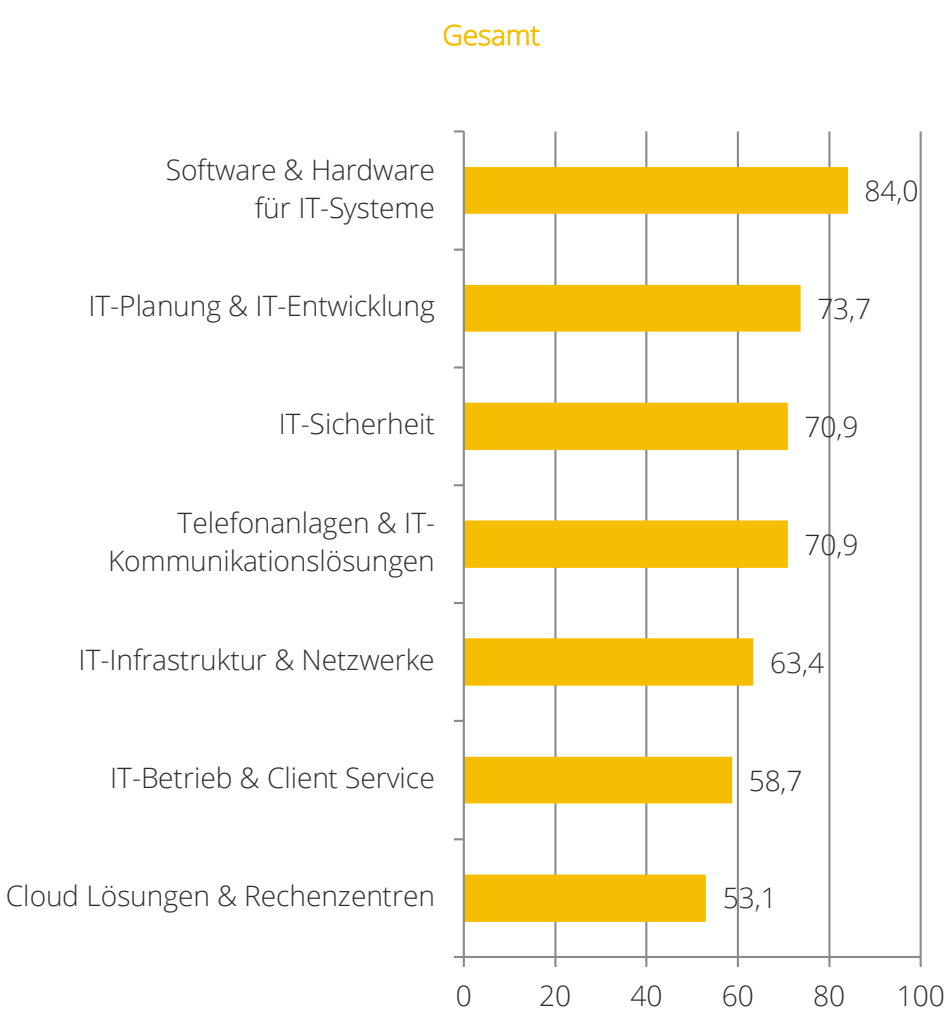
BESCHREIBUNG DER STICHPROBE (3/4)

„Wie viele fixe Mitarbeiter sind ungefähr in Ihrem Unternehmen beschäftigt?“



BESCHREIBUNG DER STICHPROBE (4/4)

„Haben Sie in Ihrem Unternehmen Einfluss auf die folgenden Bereiche?“



Position			Unternehmensgröße			
Angestellte /Arbeiter	Manage-ment	Eigentümer / Selbst-ständige	EPU	2 bis 10 MA	11 bis 30 MA	31 MA und mehr
66,7 ↓	80,5	92,7 ↑	91,0	88,0	86,2	73,1 ↓
60,0	67,8	83,3 ↑	80,6	70,0	58,6	76,1
43,3 ↓	64,4	85,4 ↑	88,1 ↑	66,0	65,5	59,7
36,7 ↓	67,8	84,4 ↑	80,6	80,0	55,2	61,2
36,7 ↓	57,5	77,1 ↑	74,6	76,0	41,4 ↓	52,2
33,3 ↓	54,0	70,8 ↑	68,7	60,0	48,3	52,2
23,3 ↓	50,6	64,6 ↑	64,2	58,0	37,9	44,8

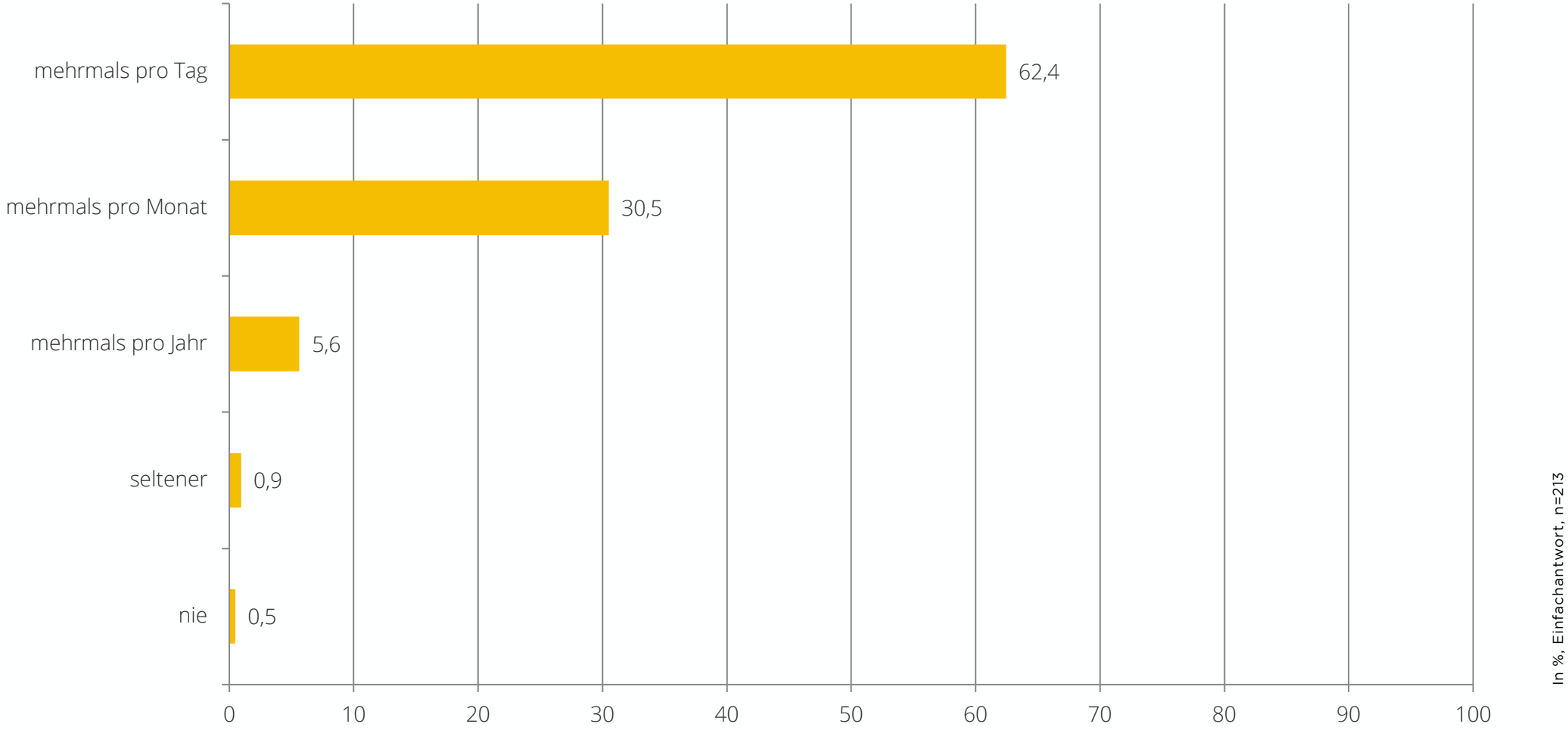
In %, Mehrfachantworten, n=213

ERGEBNISSE DER STUDIE

- Einschätzung der Bedrohungslage und Bedenken im Bereich IT-Security
- Status und Veränderung der Wichtigkeit von IT-Security in Unternehmen
- Einschätzung des bestehenden Schutzes
- IT-Security -Vorfälle und Ursachen in den letzten 2 Jahren
- IT-Security Audits
- Hemmnisse bei der Verbesserung von IT-Security
- Vertrauen auf externe Fachkompetenz
- Backups und Änderung von Passwörtern
- SPAM Problematik
- Umsetzung von Maßnahmen der DSGVO
- Veränderung des IT -Budgets im letzten Jahr
- Veränderung der Sicherheitsrisiken in den nächsten 2 Jahren

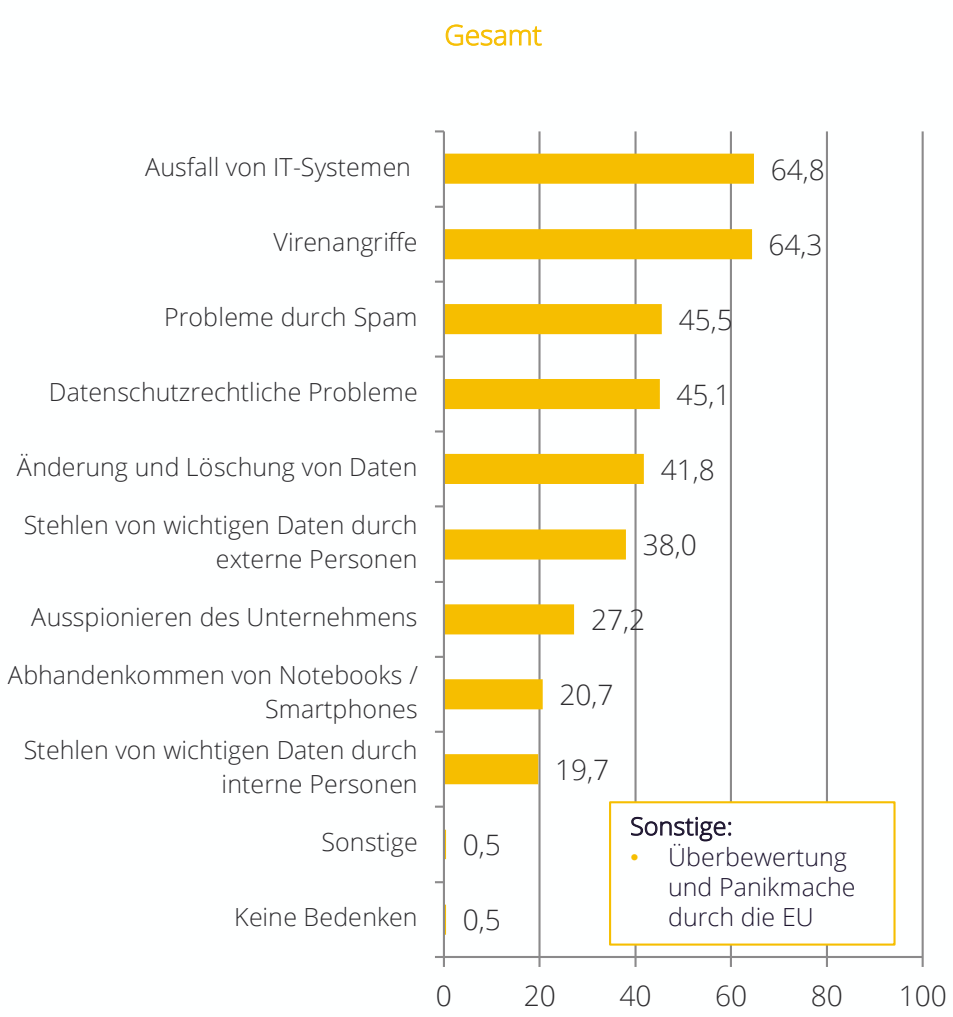
EINSCHÄTZUNG DER BEDROHUNGSLAGE

„Was schätzen Sie, wie oft werden österreichische Unternehmen im Durchschnitt (durch z.B. Hacker, Malware, Phishing, usw.) angegriffen?“



BEDENKEN IM BEREICH IT-SECURITY

„Was sind Ihr größten IT-Security Bedenken in Ihrem Unternehmen?“

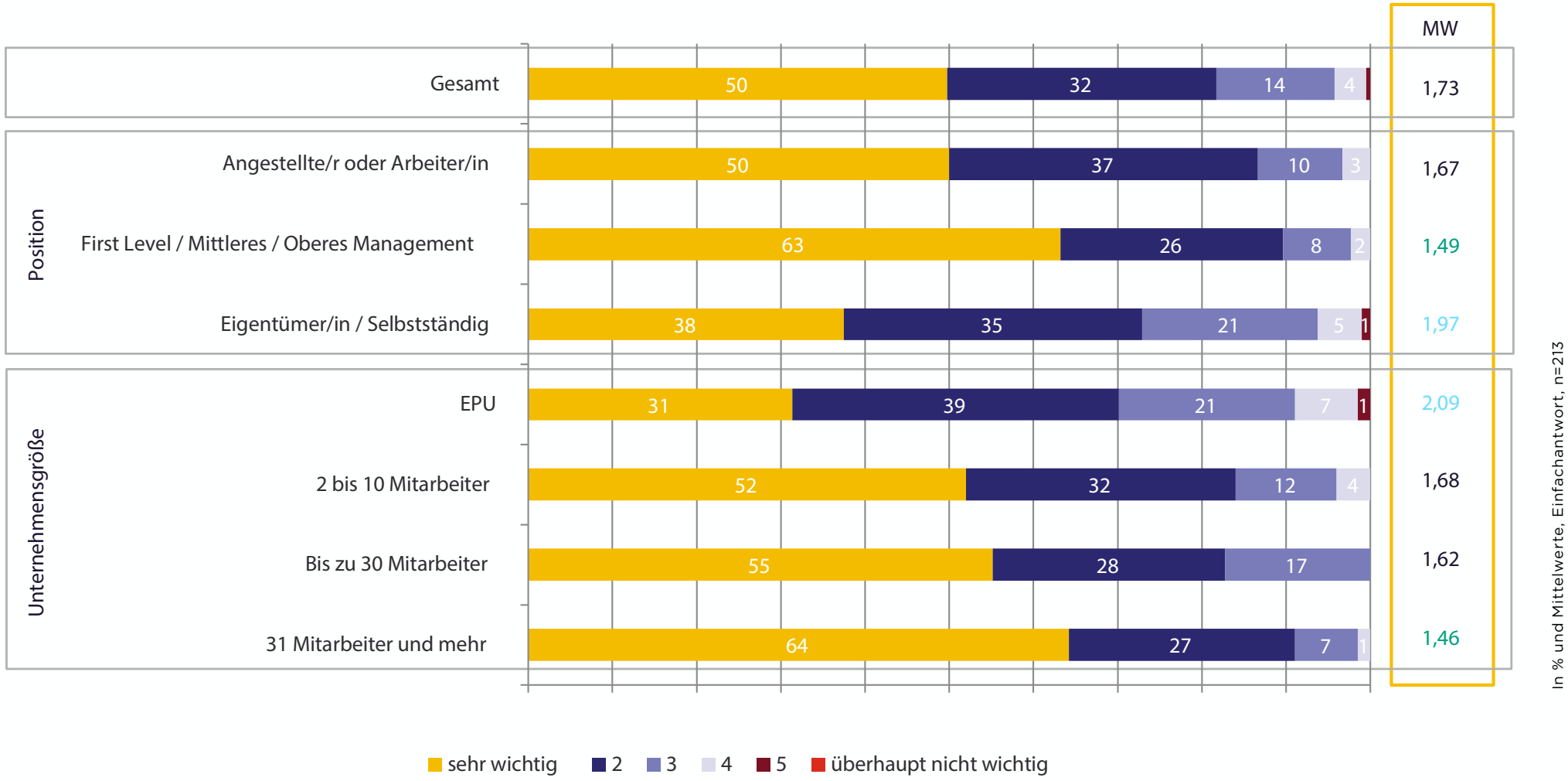


Position			Unternehmensgröße			
Angestellte /Arbeiter	Manage-ment	Eigentümer / Selbst-ständige	EPU	2 bis 10 MA	11 bis 30 MA	31 MA und mehr
66,7	67,8	61,5	53,7	68,0	65,5	73,1
63,3	60,9	67,7	62,7	70,0	62,1	62,7
40,0	40,2	52,1	55,2	38,0	44,8	41,8
50,0	46,0	42,7	41,8	42,0	48,3	49,3
26,7	42,5	45,8	44,8	36,0	51,7	38,8
36,7	40,2	36,5	31,3	36,0	37,9	46,3
23,3	35,6	20,8	20,9	20,0	31,0	37,3
40,0	12,6	21,9	22,4	26,0	6,9	20,9
23,3	29,9	9,4 ↓	7,5	14,0	20,7	35,8 ↑
0,0	0,0	1,0	0,0	0,0	0,0	1,5
3,3	0,0	0,0	0,0	0,0	0,0	1,5

In %, Mehrfachantworten, n=213

WICHTIGKEIT VON IT-SECURITY IN UNTERNEHMEN

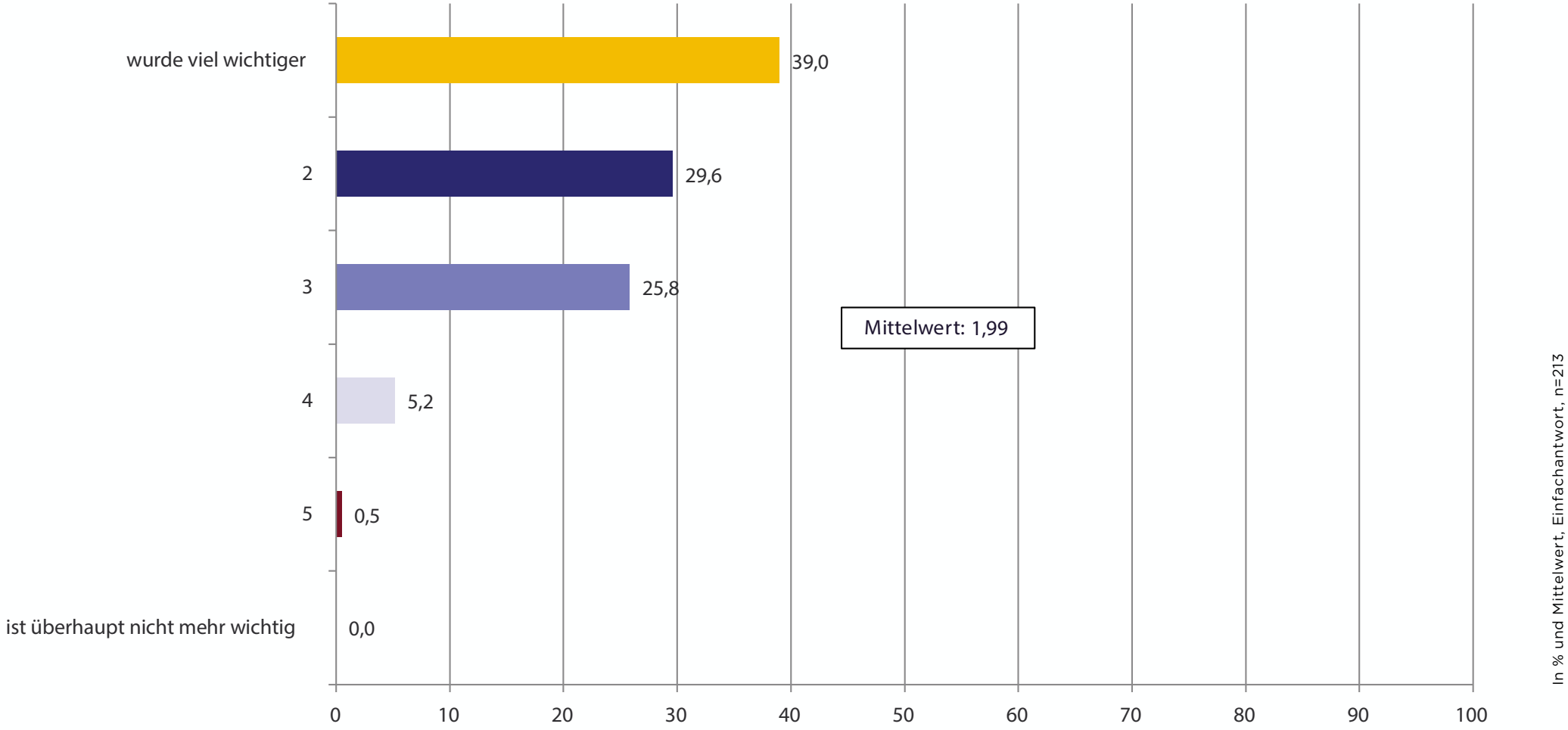
„Wie wichtig ist das Thema IT-Security innerhalb Ihres Unternehmens?“



In % und Mittelwerte, Einfachantwort, n=213

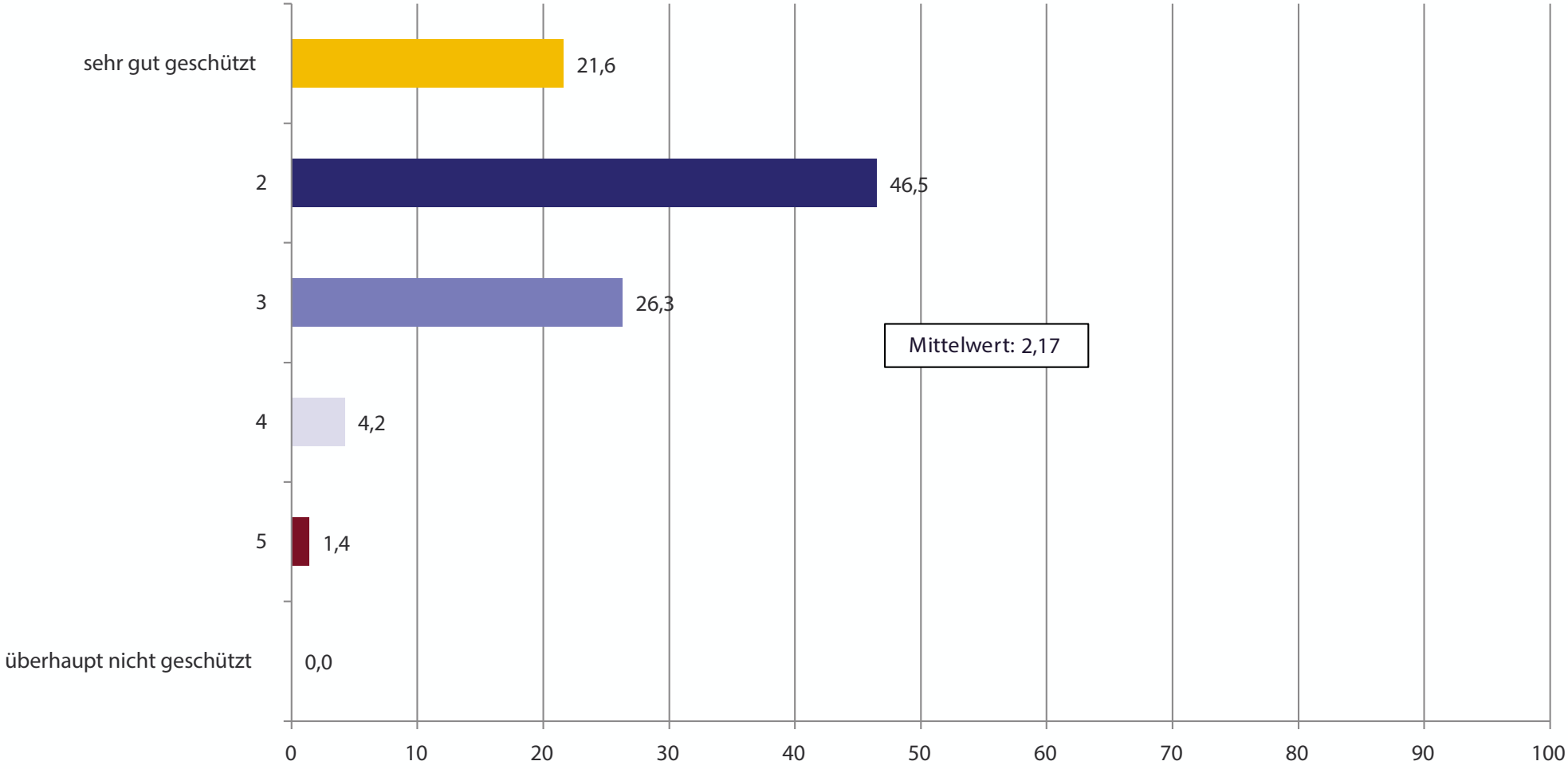
VERÄNDERUNG DER WICHTIGKEIT VON IT-SECURITY IN UNTERNEHMEN

„Wie hat sich der Stellenwert der IT-Security in Ihrem Unternehmen in den letzten zwei Jahren verändert?“



EINSCHÄTZUNG DES BESTEHENDEN SCHUTZES

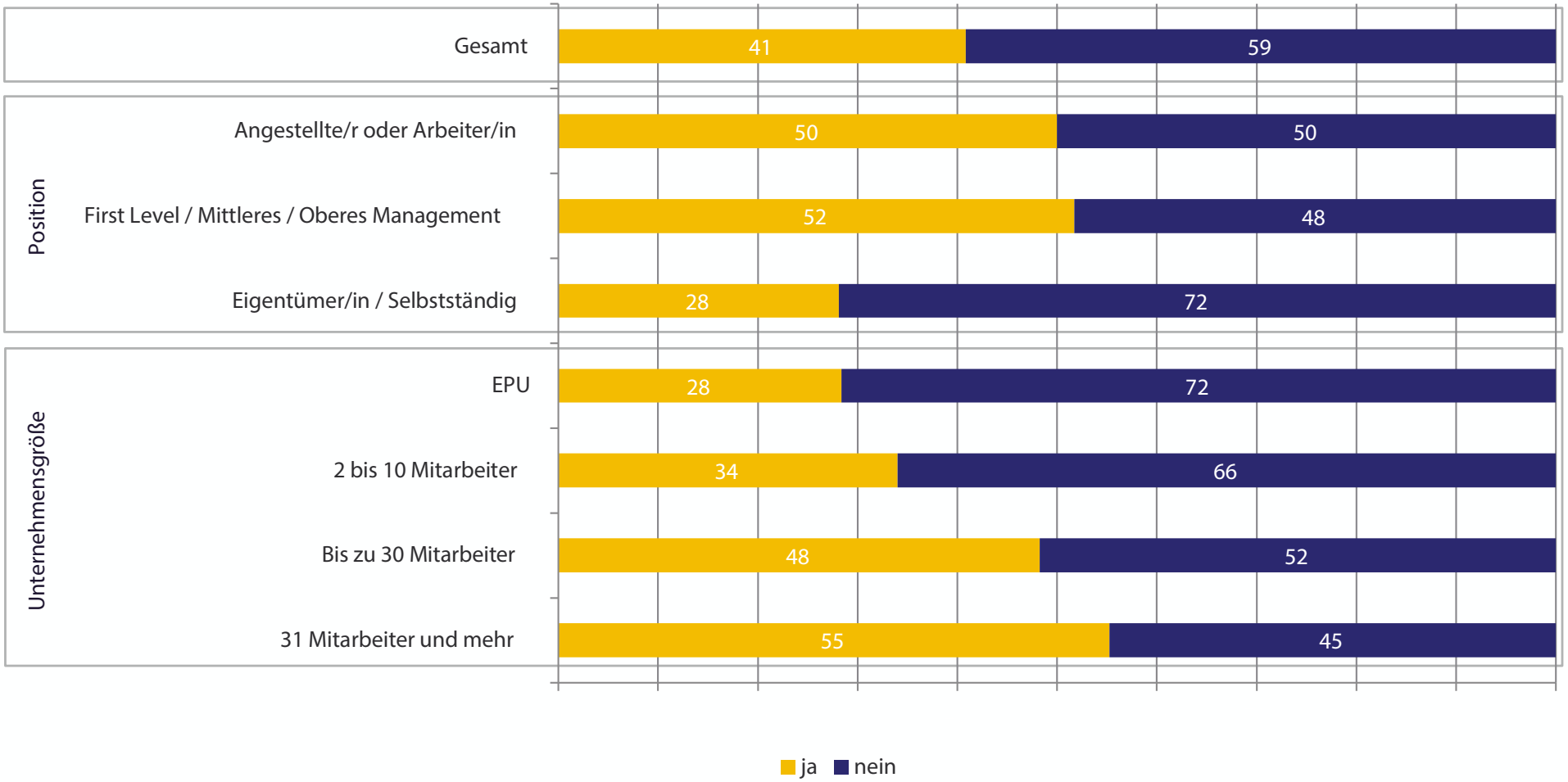
„Was denken Sie, wie gut ist Ihr Unternehmen vor internen und externen Angriffen und Datenverlust geschützt?“



In % und Mittelwert, Einfachantwort, n=213

IT-SECURITY-VORFÄLLE IN DEN LETZTEN 2 JAHREN

„Hat es in Ihrem Unternehmen in den letzten 2 Jahren einen IT-Security-Vorfall (wie z.B. Spamprobleme, Virenangriffe, Ausfall von IT-Systemen, Datenverlust, Datenänderung, usw.) gegeben?“



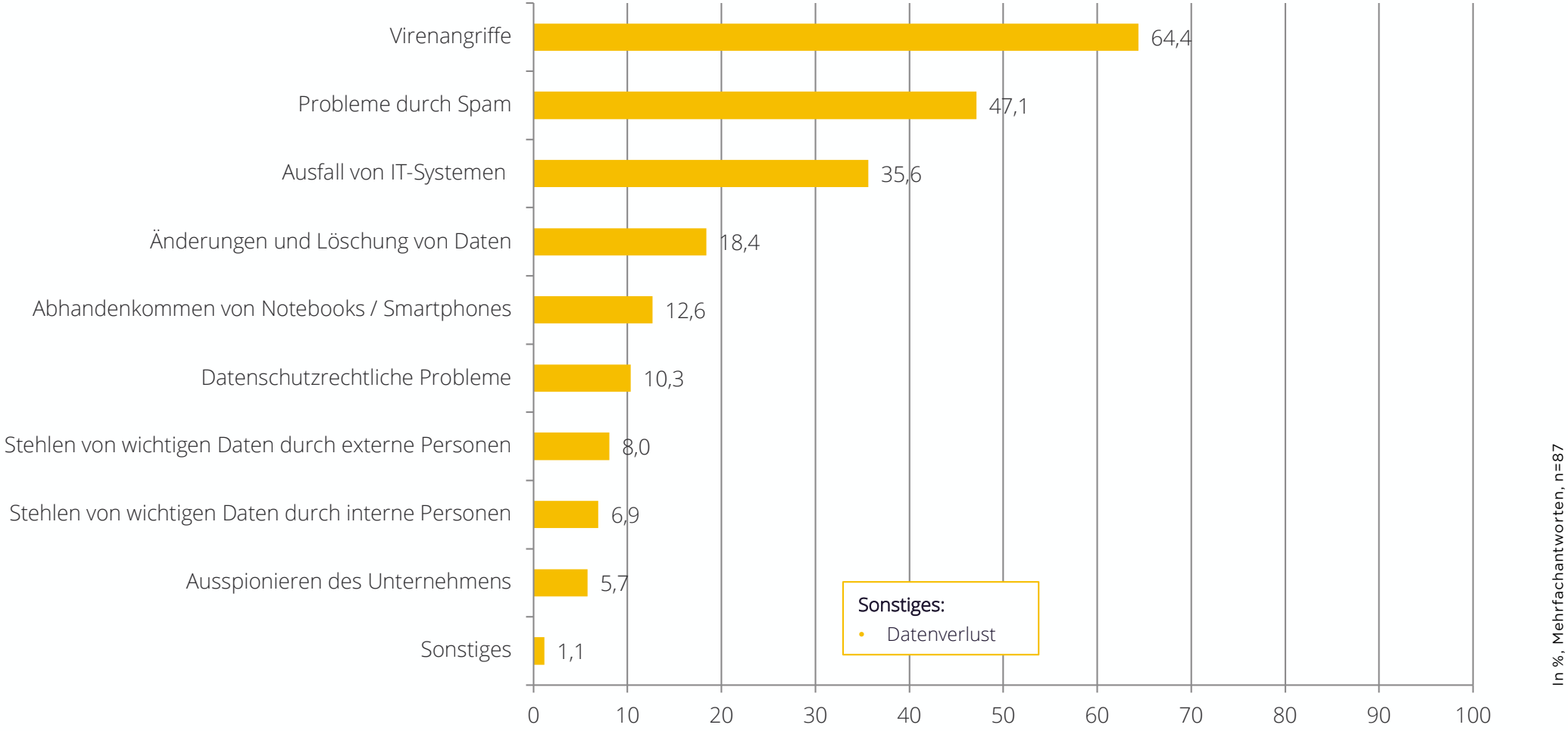
In %, Einfachantwort, n=213

In %, Einfachantwort, n=213

ART DER IT-SECURITY VORFÄLLE IN DEN LETZTEN 2 JAHREN

„Welche IT-Security-Vorfälle waren das?“

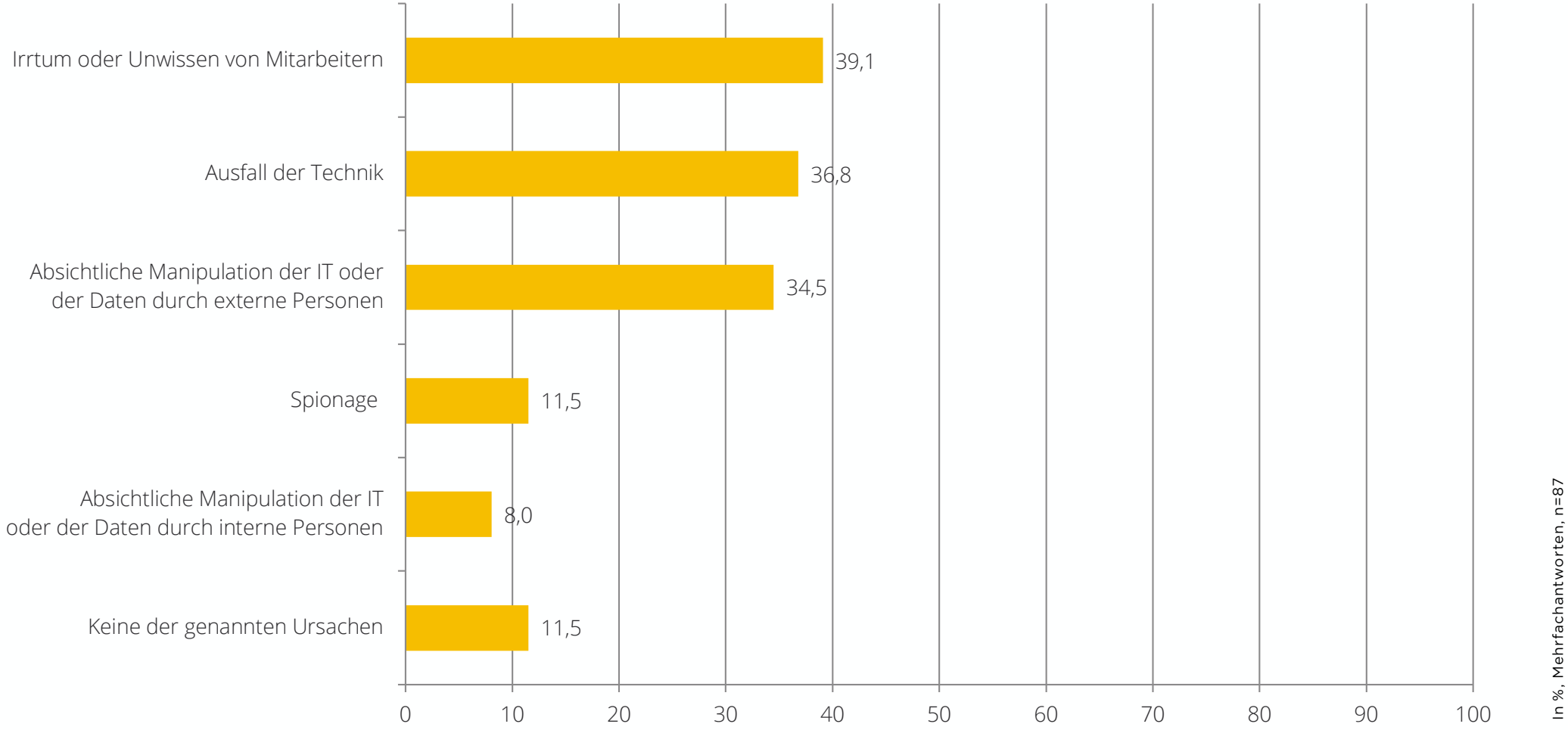
Frage wurde nur jenen gestellt, in deren Unternehmen es in den letzten 2 Jahren einen IT-Vorfall gab.



URSACHEN FÜR IT-SECURITY-VORFÄLLE

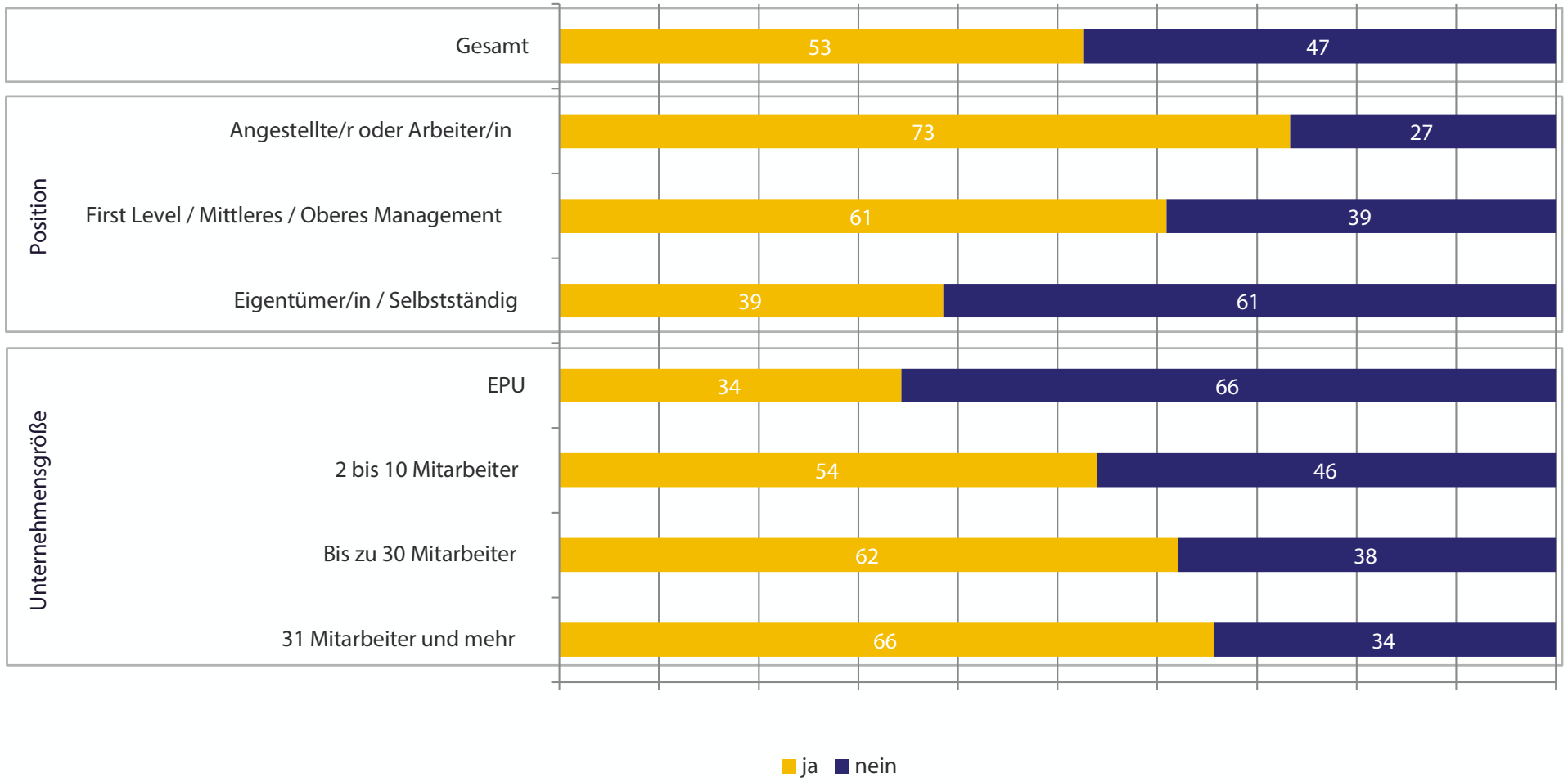
„Und was waren die Ursachen für diese IT-Security-Vorfälle?“

Frage wurde nur jenen gestellt, in deren Unternehmen es in den letzten 2 Jahren einen IT-Vorfall gab.



REGELMÄSSIGKEIT VON IT-SECURITY AUDITS

„Führen Sie regelmäßig, wiederkehrende IT-Security Audits durch, um interne und externe Schwachstellen, Konzeptionsund Konfigurationsfehler aufzuzeigen?“

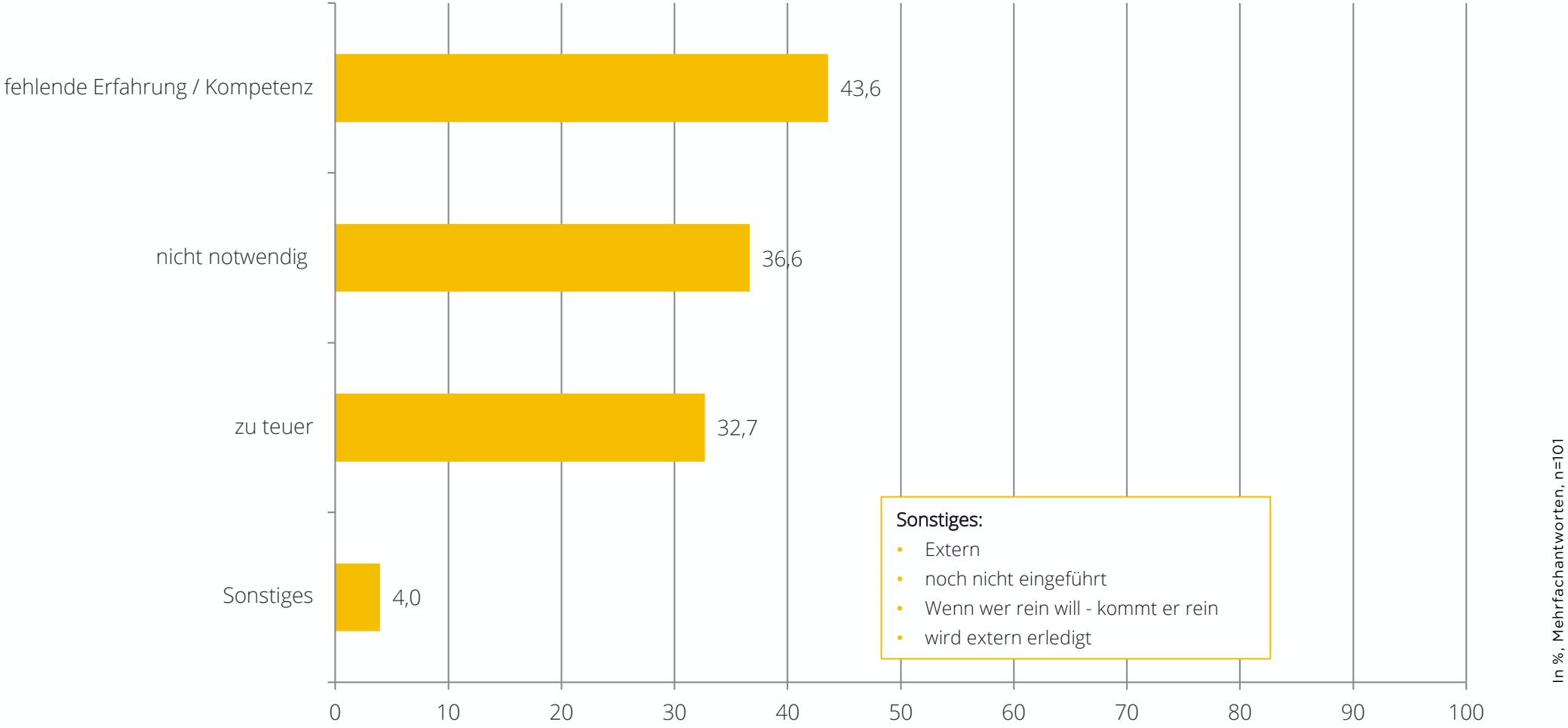


In %, Einfachantwort, n=213

GRUND FÜR KEINE REGELMÄSSIGEN IT-SECURITY AUDITS

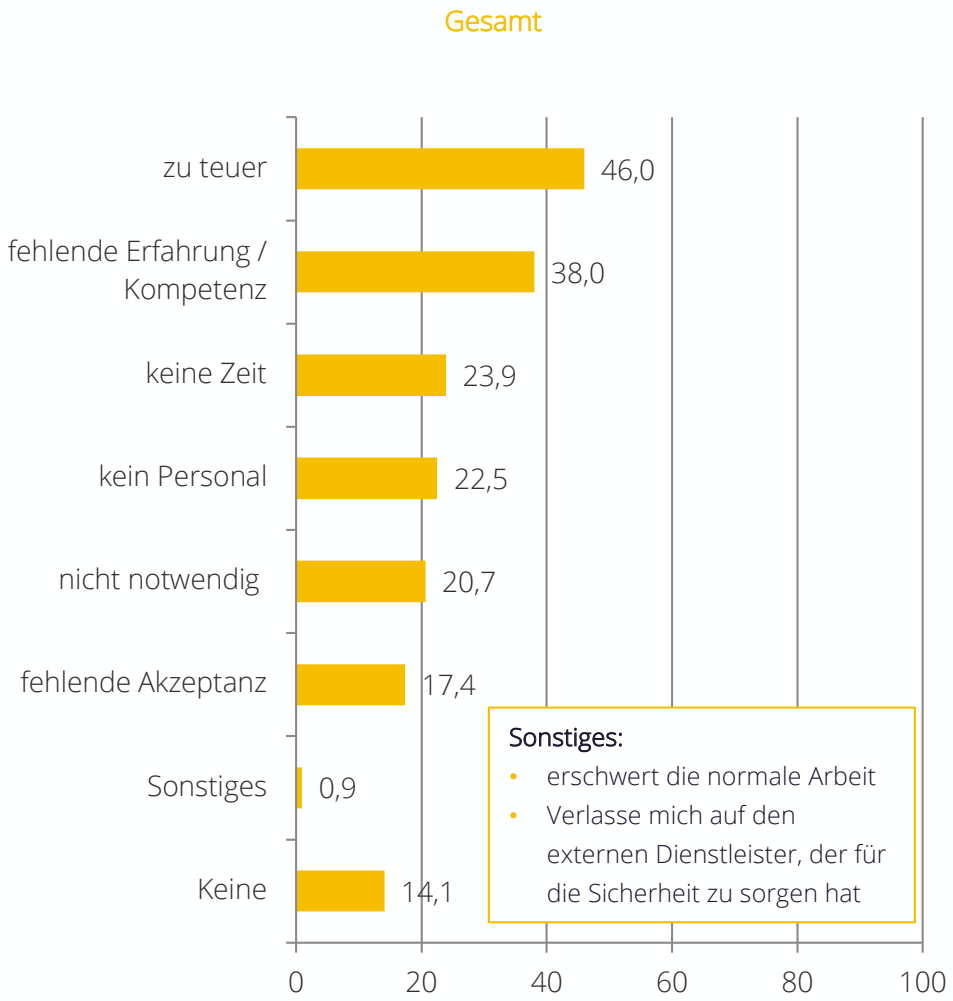
„Warum werden in Ihrem Unternehmen nicht regelmäßig IT-Security Audits durchgeführt?

Frage wurde nur jenen gestellt, die keine regelmäßigen IT-Security Audits durchführen.



HEMMNISSE BEI DER VERBESSERUNG DER IT-SECURITY (1/2)

„Welche Hemmnisse sehen Sie in Ihrem Unternehmen, die einer Verbesserung der IT-Security entgegenwirken?“

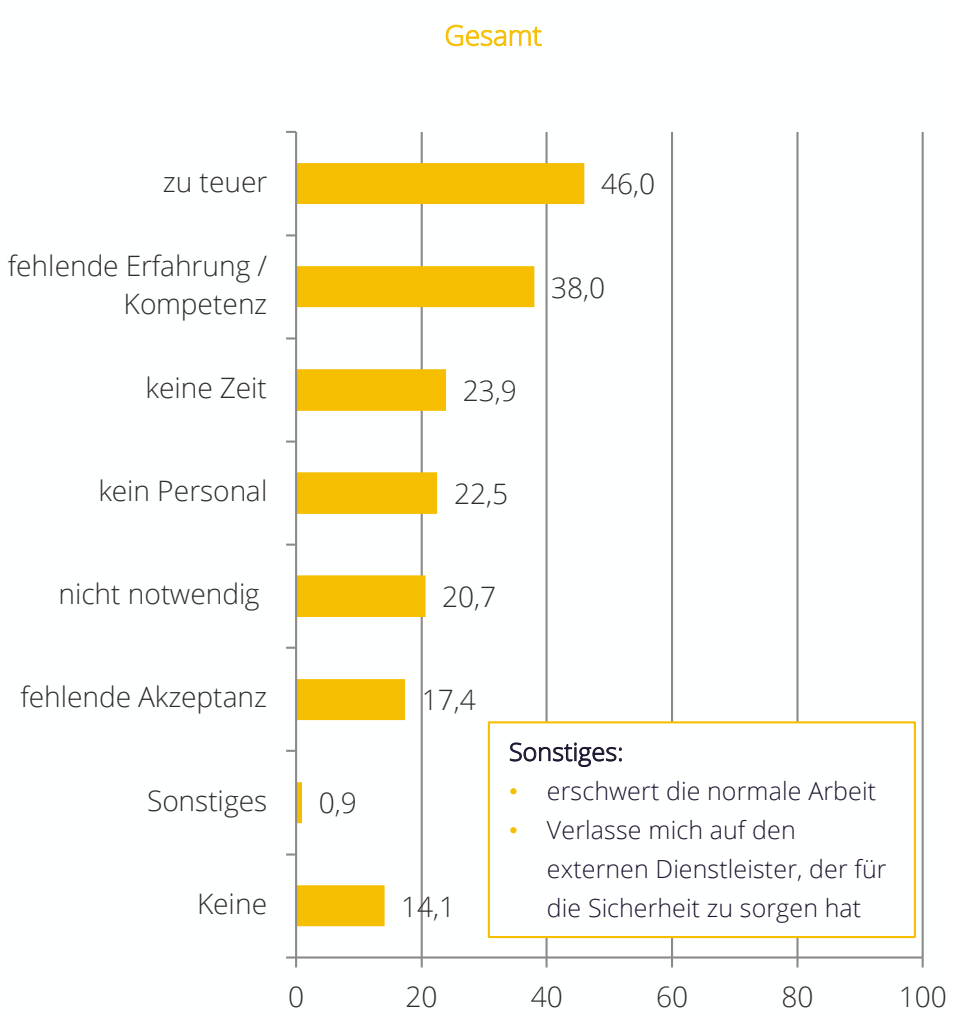


Position			Branche		
Angestellte/Arbeiter	Manage-ment	Eigentümer / Selbst-ständige	Prod. Gewerbe	Handel	Dienst-leistung
40,0	42,5	51,0	54,8	40,6	45,3
50,0	36,8	35,4	45,2	50,0	34,0
40,0	19,5	22,9	22,6	25,0	24,0
30,0	26,4	16,7	29,0	31,3	19,3
20,0	13,8	27,1	16,1	12,5	23,3
20,0	31,0 ↑	4,2 ↓	38,7 ↑	9,4	14,7
0,0	1,1	1,0	0,0	0,0	1,3
6,7	13,8	16,7	0,0	15,6	16,7

In %, Mehrfachantworten, n=213

HEMMNISSE BEI DER VERBESSERUNG DER IT-SECURITY (2/2)

„Welche Hemmnisse sehen Sie in Ihrem Unternehmen, die einer Verbesserung der IT-Security entgegenwirken?“

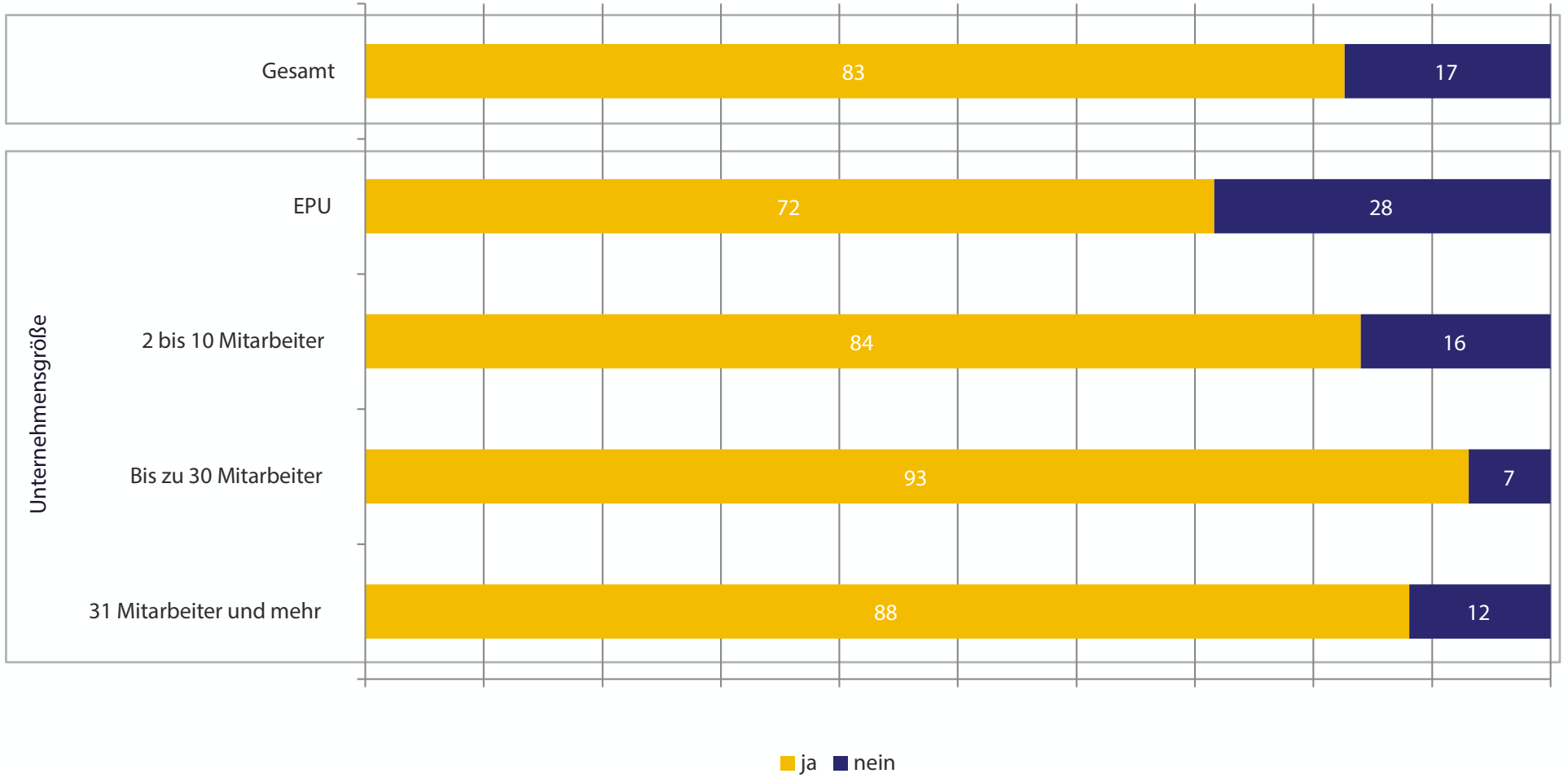


Unternehmensgröße			
EPU	2 bis 10 MA	11 bis 30 MA	31 MA und mehr
49,3	48,0	27,6	49,3
35,8	40,0	48,3	34,3
17,9	24,0	27,6	28,4
13,4	24,0	37,9	23,9
29,9	20,0	24,1	10,4
3,0 ↓	12,0	31,0	29,9 ↑
1,5	0,0	0,0	1,5
16,4	10,0	13,8	14,9

In %, Mehrfachantworten, n=213

VERTRAUEN AUF EXTERNE FACHKOMPETENZ

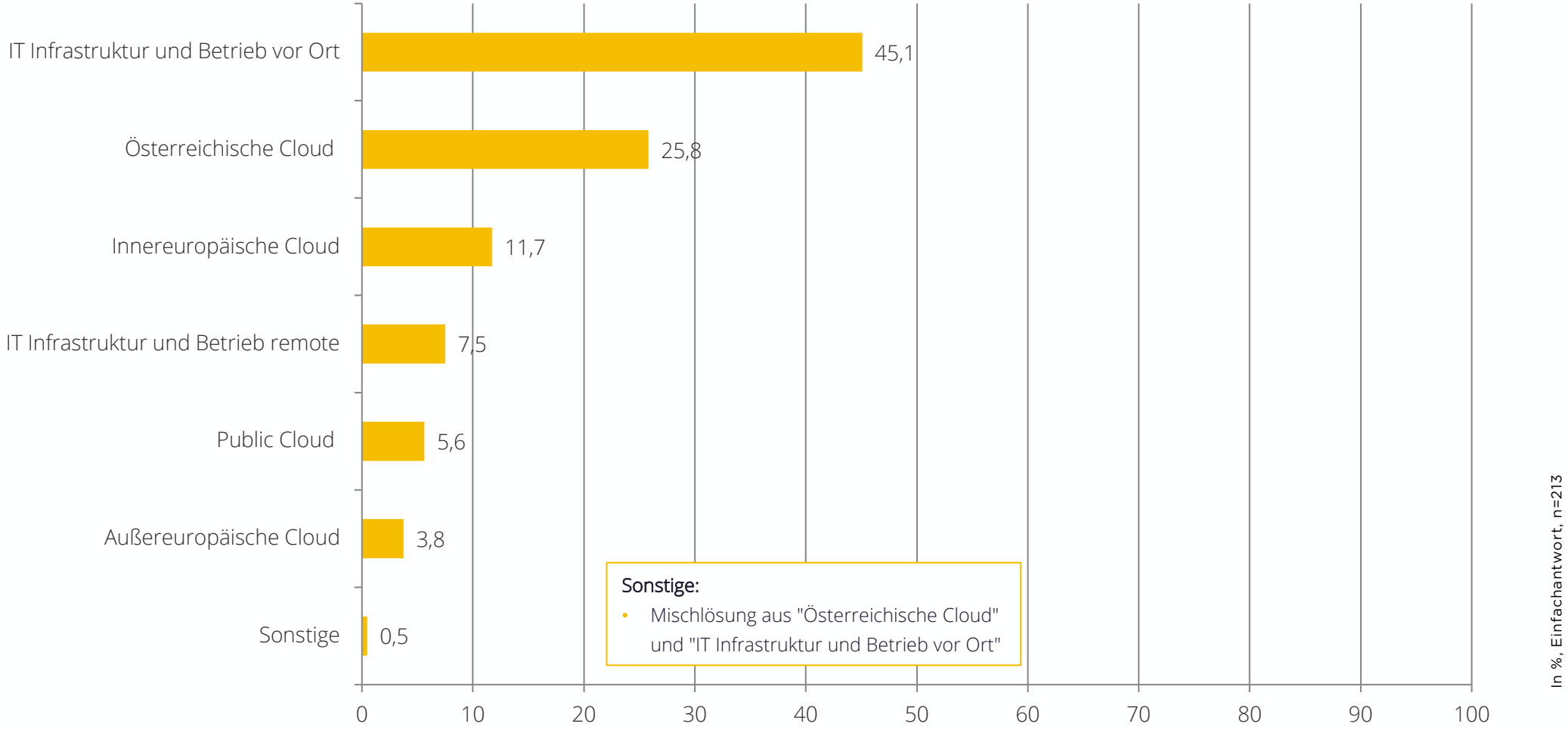
„Würden Sie auf externe(s) Fachkompetenz / Wissen vertrauen, um in Ihrem Unternehmen Sicherheitslücken im ITBereich aufzudecken und/oder beheben zu lassen?“



In %, Einfachantwort, n=213

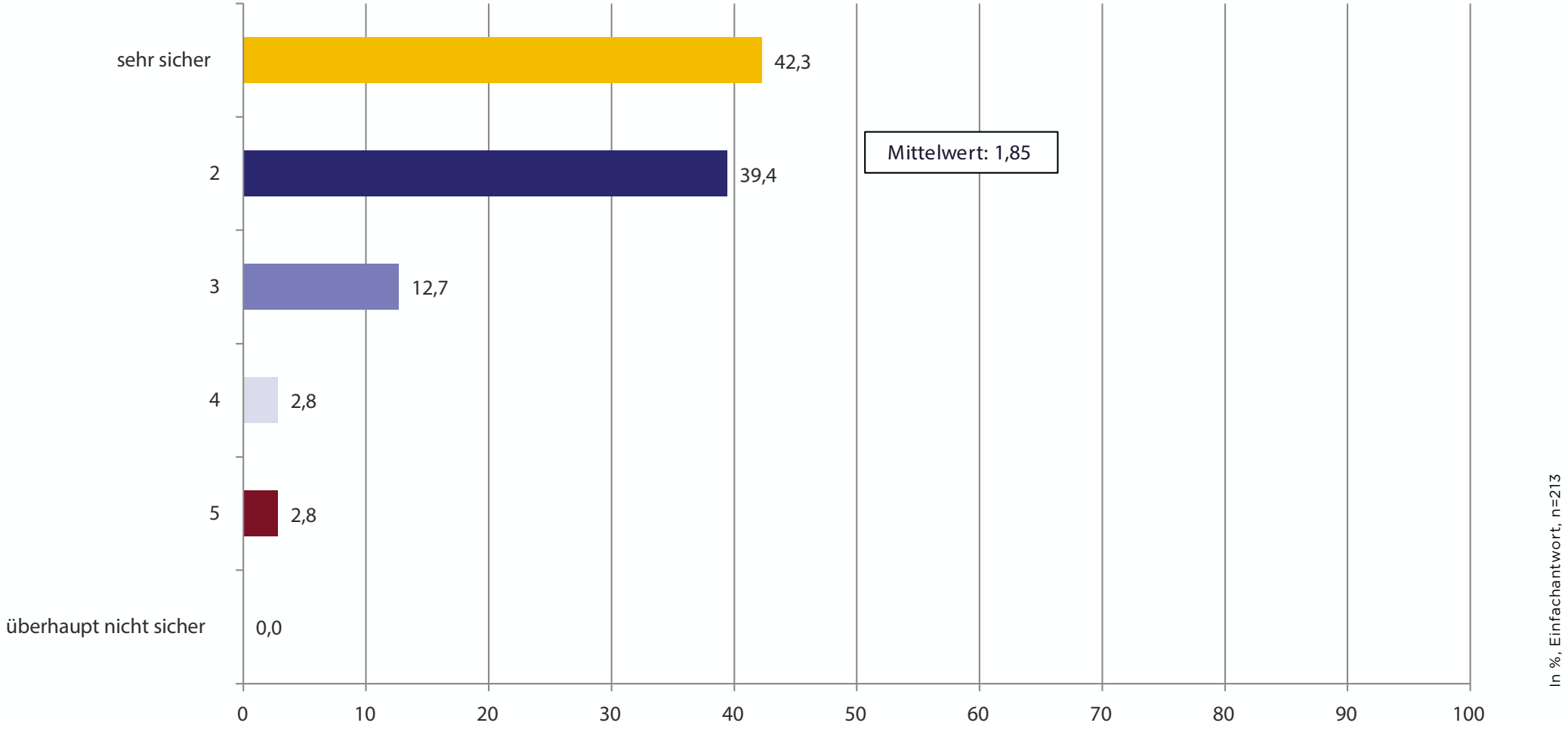
BEVORZUGTE SETTINGS FÜR IT-INFRASTRUKTUR

„Welche der folgenden Settings für eine IT-Infrastruktur bevorzugen Sie?“



ORDNUNGSGEMÄSSE BACKUPS IM UNTERNEHMEN

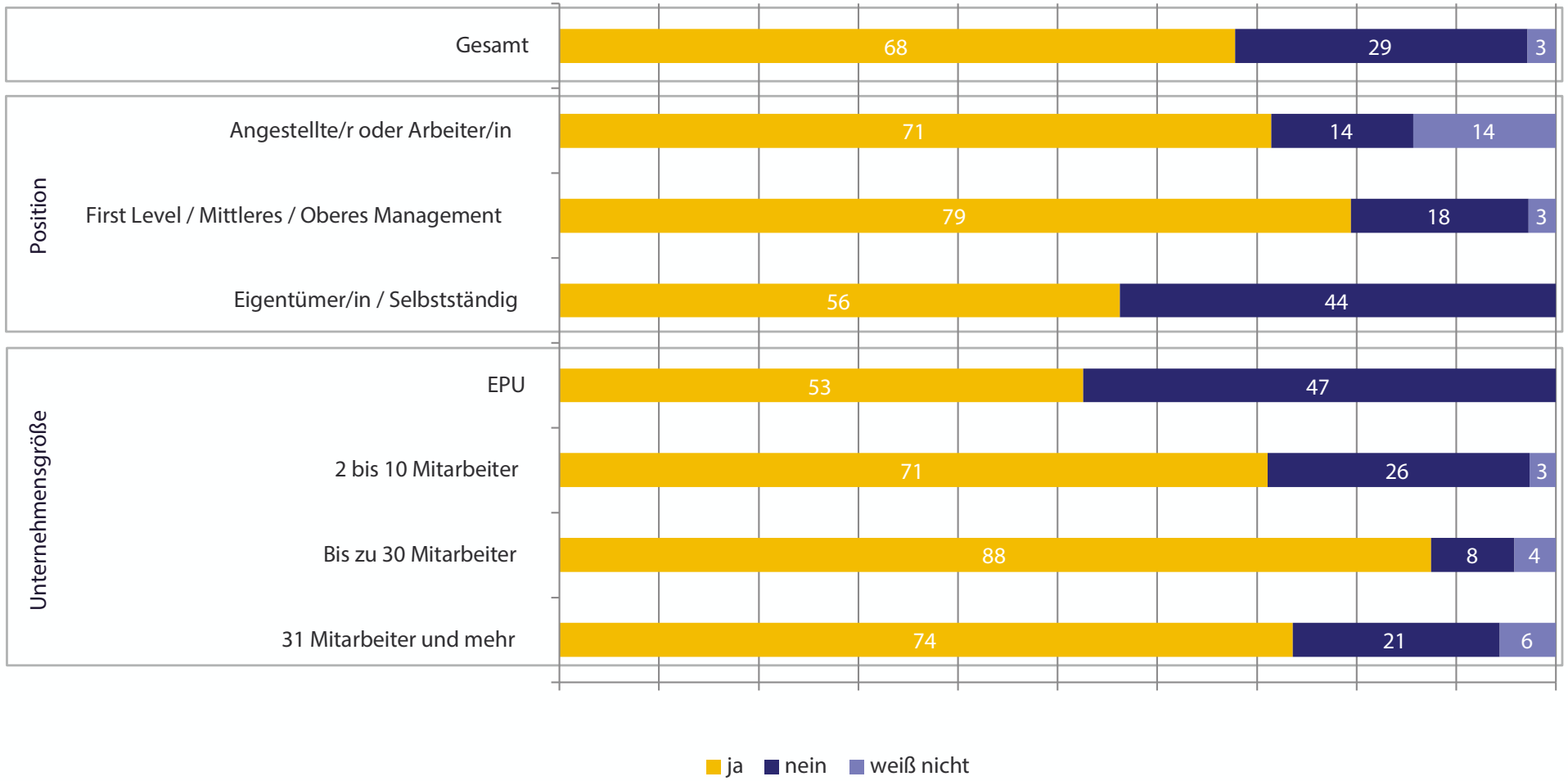
„Sind Sie sicher, dass die Daten in Ihrem Unternehmen ordnungsgemäß gesichert werden (Backup)?“



BACKUPS AUSSERHALB DES UNTERNEHMENS

„Werden die Backups auch außerhalb der Räumlichkeiten Ihres Unternehmens aufbewahrt?“

Frage wurde nur jenen gestellt, die (sehr) sicher sind, dass Backups im Unternehmen durchgeführt werden.

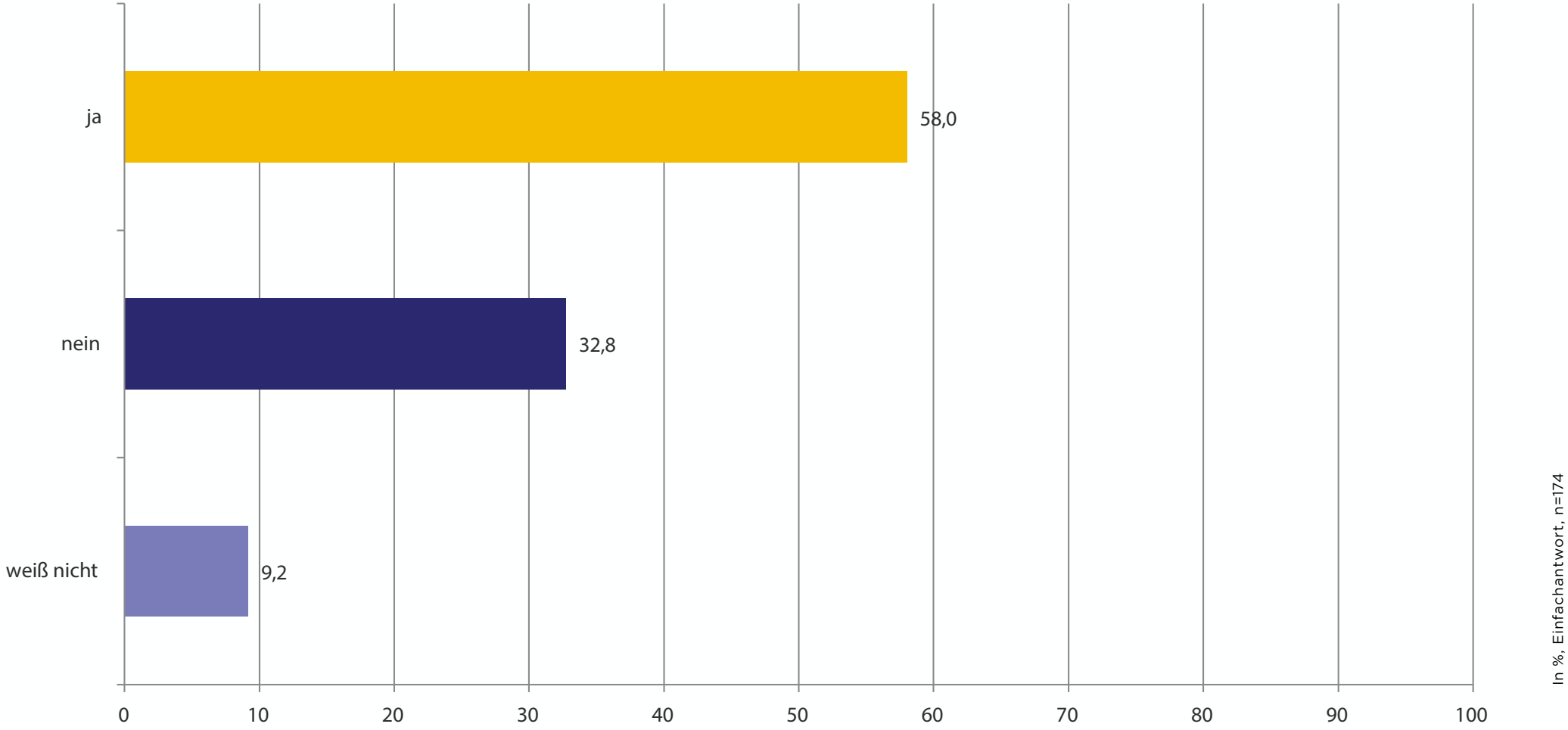


In %, Einfachantwort, n=174

TESTWEISE WIEDERHERSTELLUNG VON BACKUPS

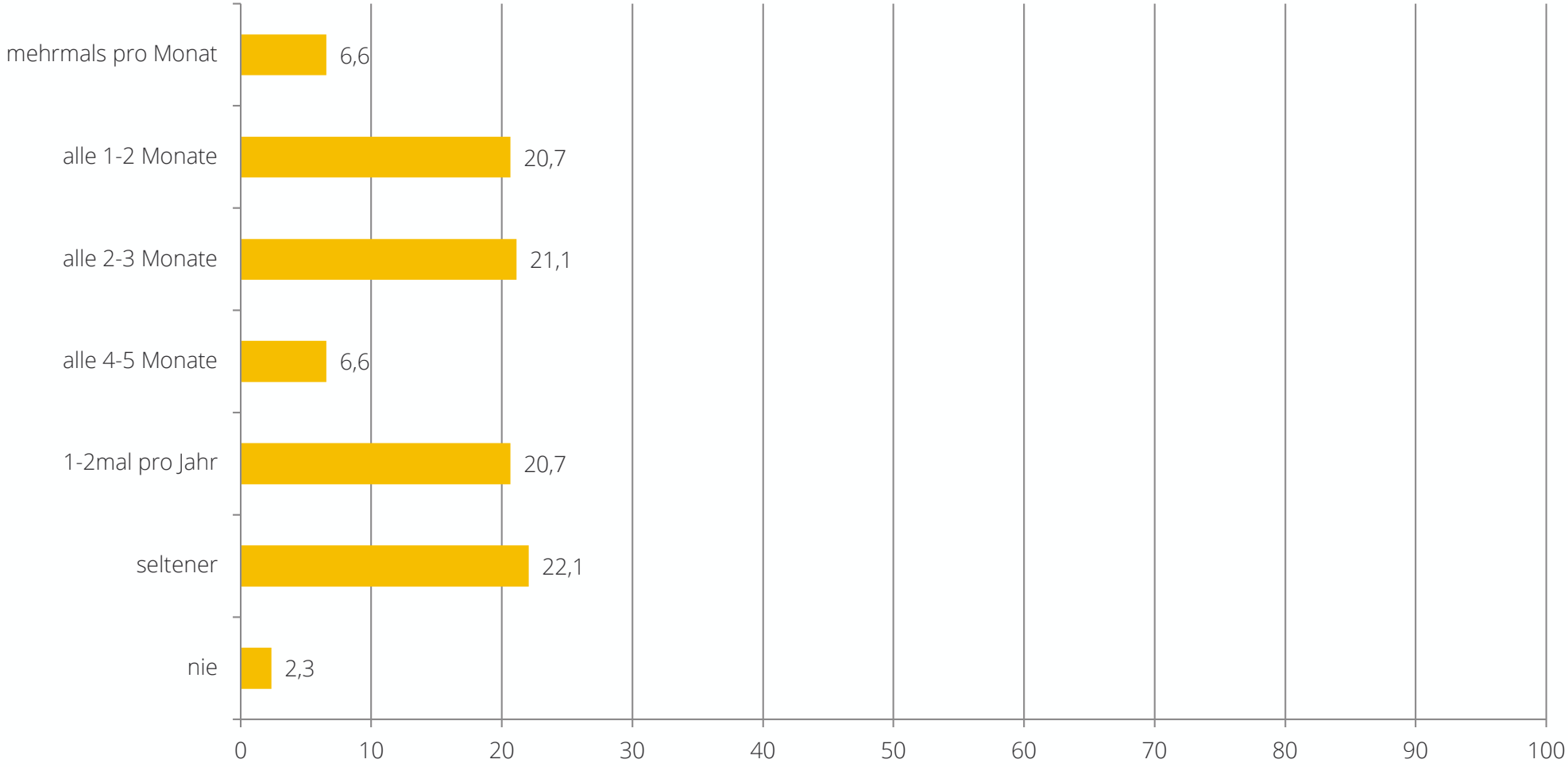
„Und werden die Backups regelmäßig testweise wiederhergestellt?“

Frage wurde nur jenen gestellt, die (sehr) sicher sind, dass Backups im Unternehmen durchgeführt werden.



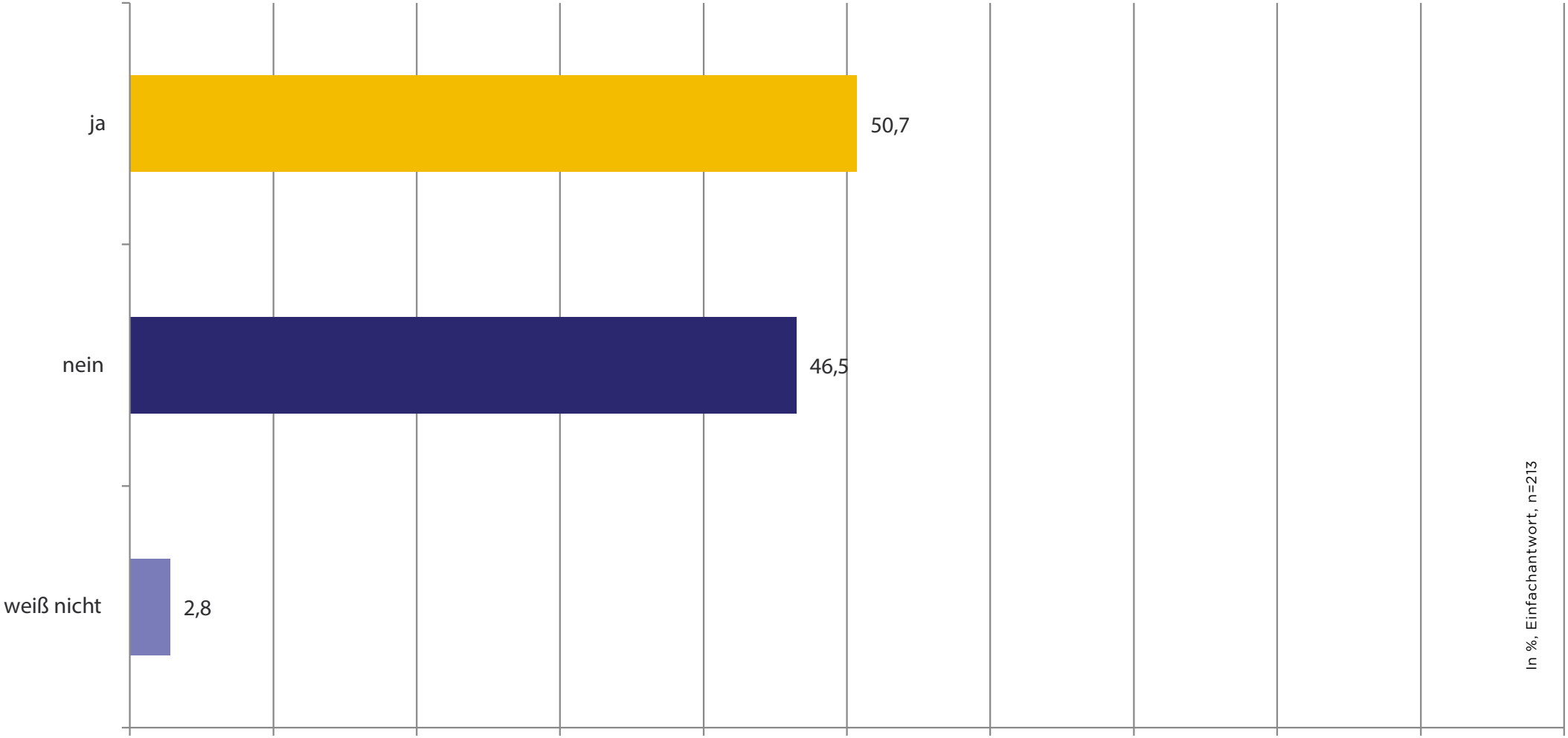
ÄNDERUNG VON PASSWÖRTERN

„Wie oft werden Passwörter in Ihrem Unternehmen geändert?“



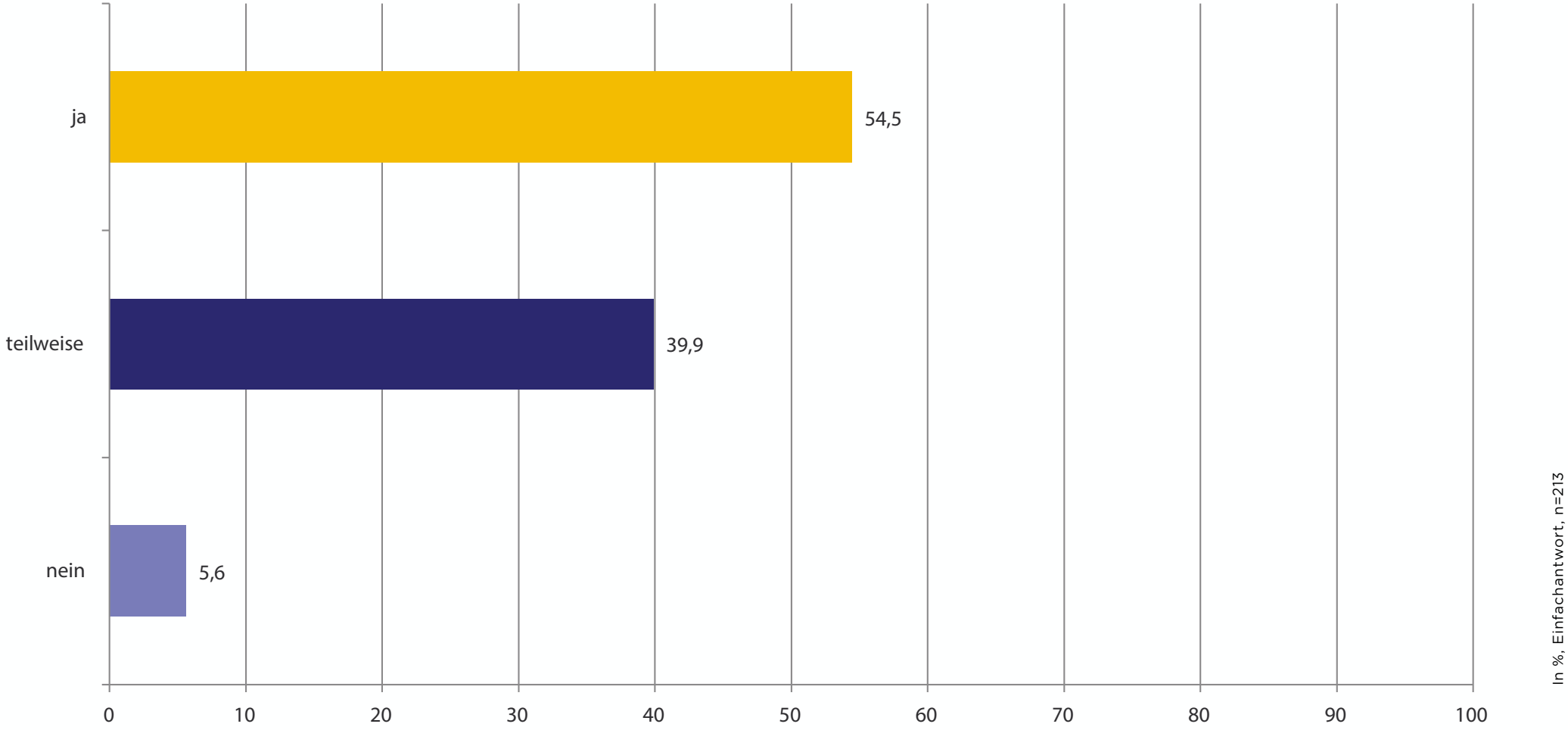
SPAM PROBLEMATIK

„Leiden Sie bzw. Ihre Mitarbeiter unter SPAM-E-Mail Nachrichten?“



UMSETZUNG VON MASSNAHMEN DER DSGVO (1/4)

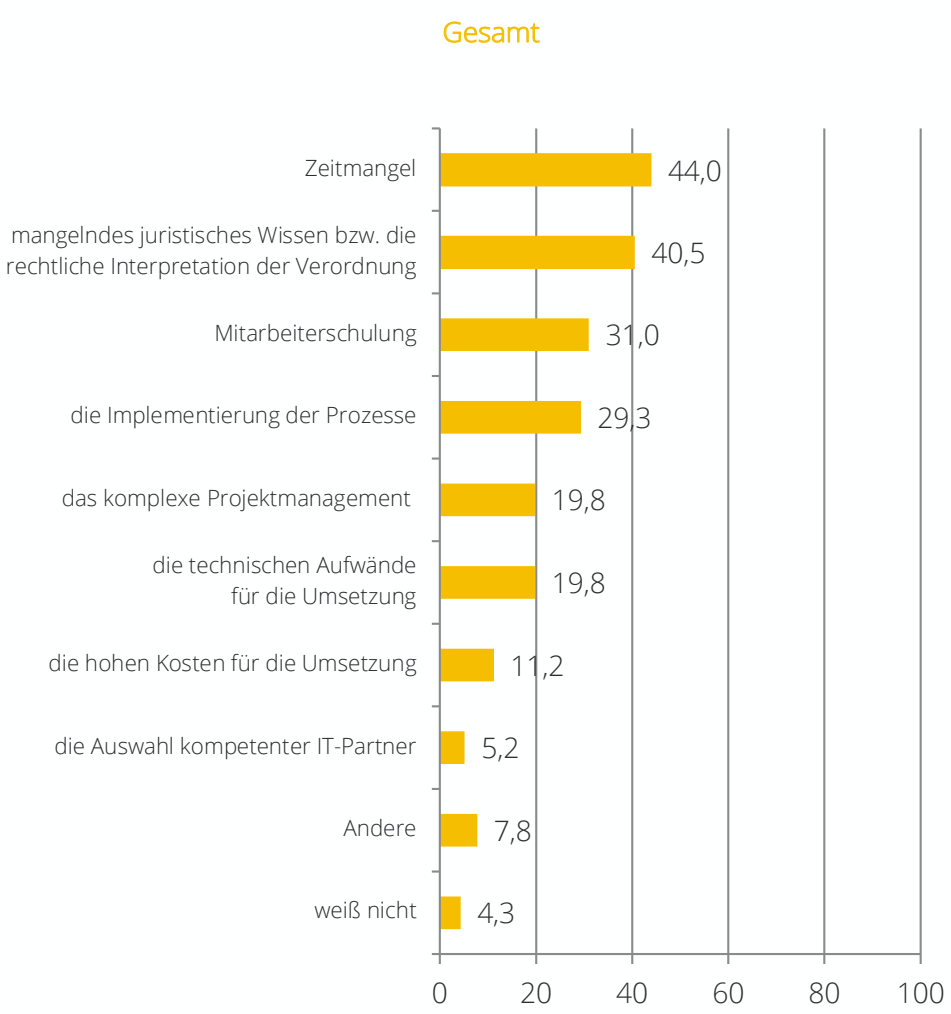
„Haben Sie schon die technischen und organisatorischen Maßnahmen der DSGVO umgesetzt?“



UMSETZUNG VON MASSNAHMEN DER DSGVO (2/4)

„Was waren die größten Herausforderungen für die Umsetzung der Maßnahmen für die DSGVO?“

Frage wurde nur jenen gestellt, deren Unternehmen bereits die technischen und organisatorischen Maßnahmen der DSGVO umgesetzt haben.



Position			Unternehmensgröße			
Angestellte /Arbeiter	Manage-ment	Eigentümer / Selbst-ständige	EPU	2 bis 10 MA	11 bis 30 MA	31 MA und mehr
50,0	42,3	43,2	43,8	55,0	26,3	46,7
40,0	46,2	34,1	31,3	45,0	42,1	44,4
25,0	50,0 ↑	11,4 ↓	6,3 ↓	20,0	47,4	46,7
25,0	34,6	25,0	21,9	30,0	47,4	26,7
15,0	30,8	9,1	6,3	5,0	26,3	33,3
25,0	23,1	13,6	12,5	15,0	21,1	26,7
10,0	13,5	9,1	12,5	15,0	0,0	13,3
10,0	5,8	2,3	3,1	0,0	5,3	8,9
5,0	3,8	13,6	15,6	0,0	5,3	6,7
0,0	1,9	9,1	9,4	5,0	0,0	2,2

In %, Mehrfachantworten, n=116

UMSETZUNG VON MASSNAHMEN DER DSGVO (3/4)

„Was waren die größten Herausforderungen für die Umsetzung der Maßnahmen für die DSGVO?“

Frage wurde nur jenen gestellt, deren Unternehmen bereits die technischen und organisatorischen Maßnahmen der DSGVO umgesetzt haben.

Sonstiges:

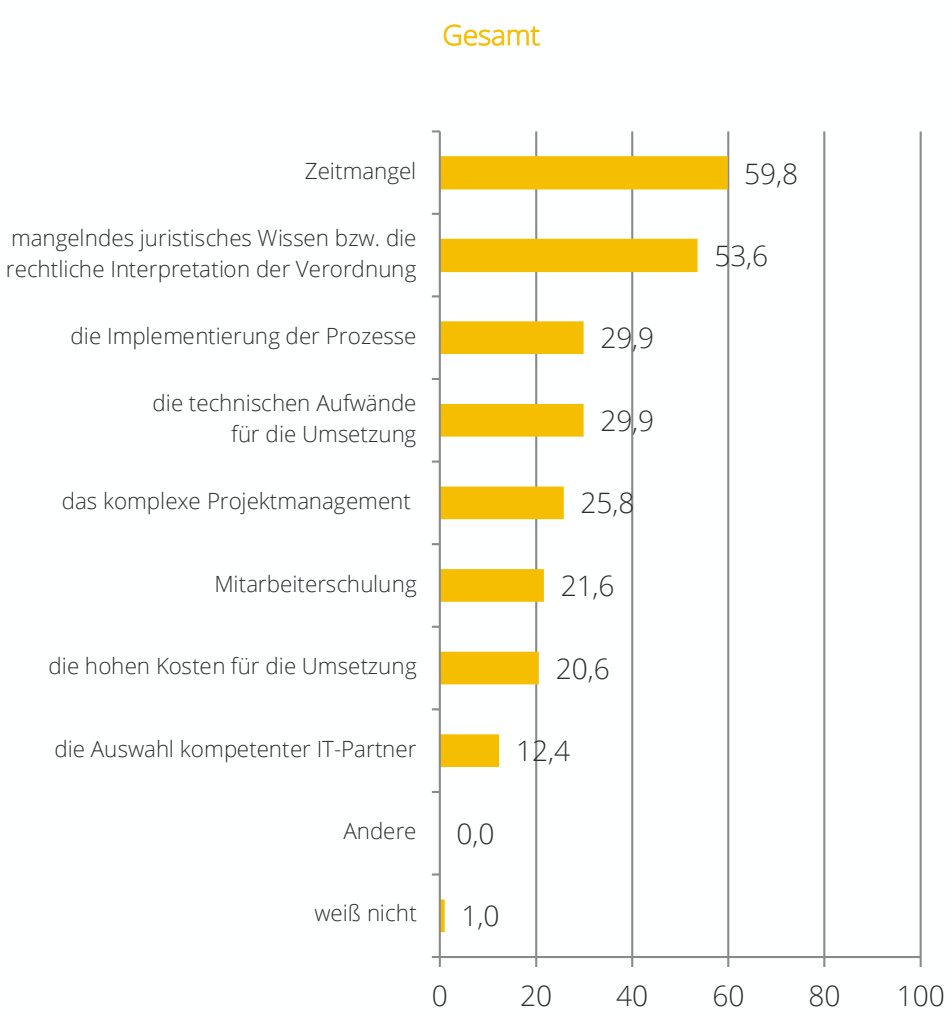
- Bei frühzeitiger und guter Vorbereitung, waren das keine Herausforderungen.
- bürokratischer Aufwand (Auftragsverarbeitungsverträge und Verrarbeitungsverzeichnisse)
- die überzogene Aufbauschung des Themas durch Berater und Medien; unkonkrete Anforderungen
- Dokumentationsaufwand und mangelnde interne Akzeptanz
- DSGVO ist noch nicht fertig... zuviel Interpretationsspielraum,
- eine klare Richtilinie zu finden
- Es gab in dieser Thematik keine Herausforderung.
- unklare Gesetzeslage
- widersprüchliche Informationen

Originalnennungen, n=116

UMSETZUNG VON MASSNAHMEN DER DSGVO (4/4)

„Was sind die größten Hindernisse für die Umsetzung der Maßnahmen für die DSGVO?“

Frage wurde nur jenen gestellt, deren Unternehmen die technischen und organisatorischen Maßnahmen der DSGVO erst teilweise oder noch nicht umgesetzt haben.

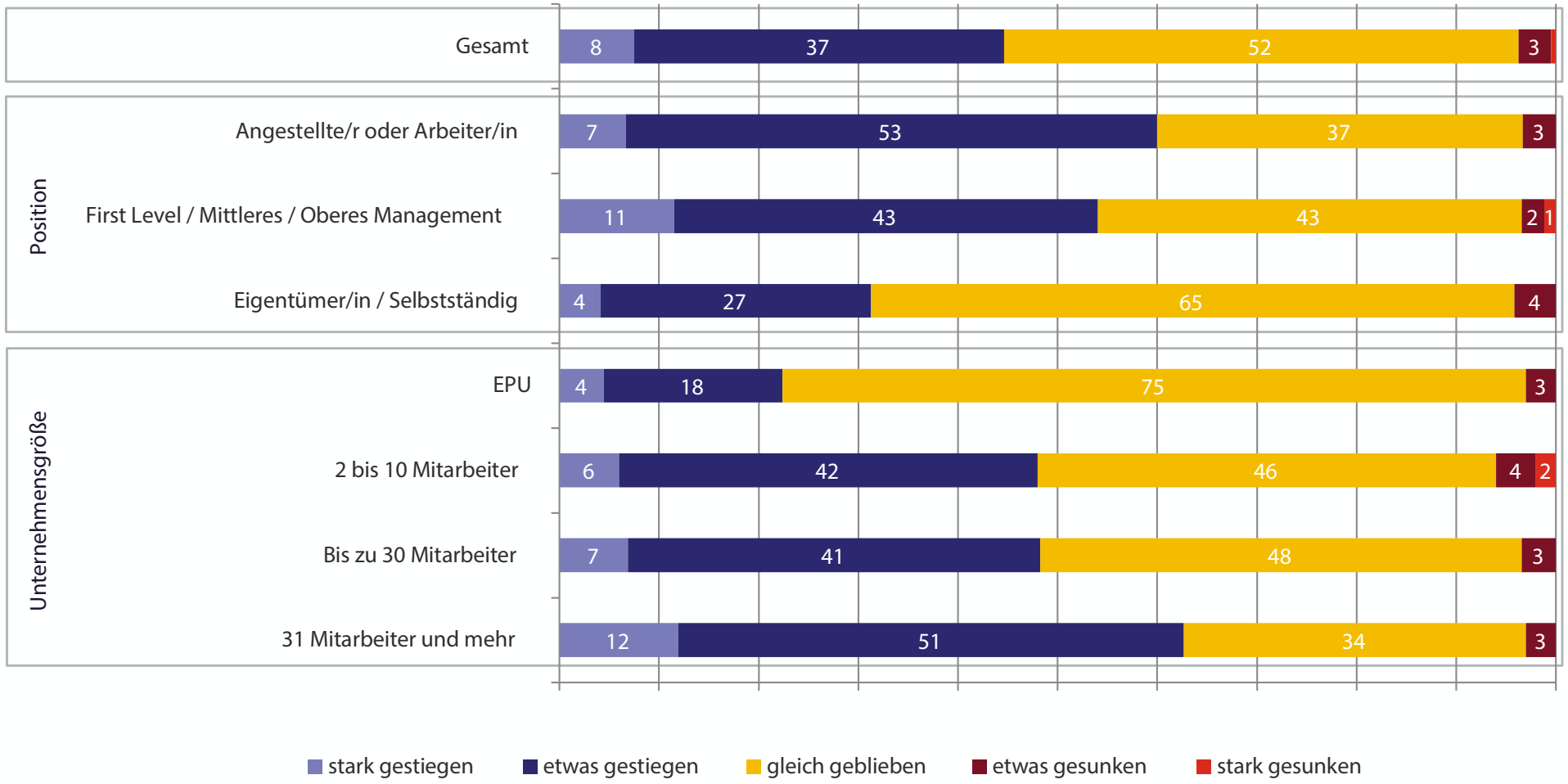


Position			Unternehmensgröße			
Angestellte /Arbeiter	Manage-ment	Eigentümer / Selbst-ständige	EPU	2 bis 10 MA	11 bis 30 MA	31 MA und mehr
40,0	60,0	63,5	60,0	70,0	70,0	40,9
60,0	42,9	59,6	68,6	40,0	60,0	45,5
30,0	31,4	28,8	28,6	33,3	30,0	27,3
10,0	37,1	28,8	22,9	26,7	50,0	36,4
20,0	25,7	26,9	17,1	20,0	40,0	40,9
30,0	45,7 ↑	3,8 ↓	0,0 ↓	16,7	40,0	54,5 ↑
10,0	20,0	23,1	22,9	16,7	10,0	27,3
10,0	25,7 ↑	3,8	2,9	10,0	10,0	31,8 ↑
0,0	0,0	0,0	0,0	0,0	0,0	0,0
0,0	2,9	0,0	0,0	0,0	10,0 ↑	0,0

In %, Mehrfachantworten, n=97

VERÄNDERUNG DES IT-BUDGETS IM LETZTEN JAHR

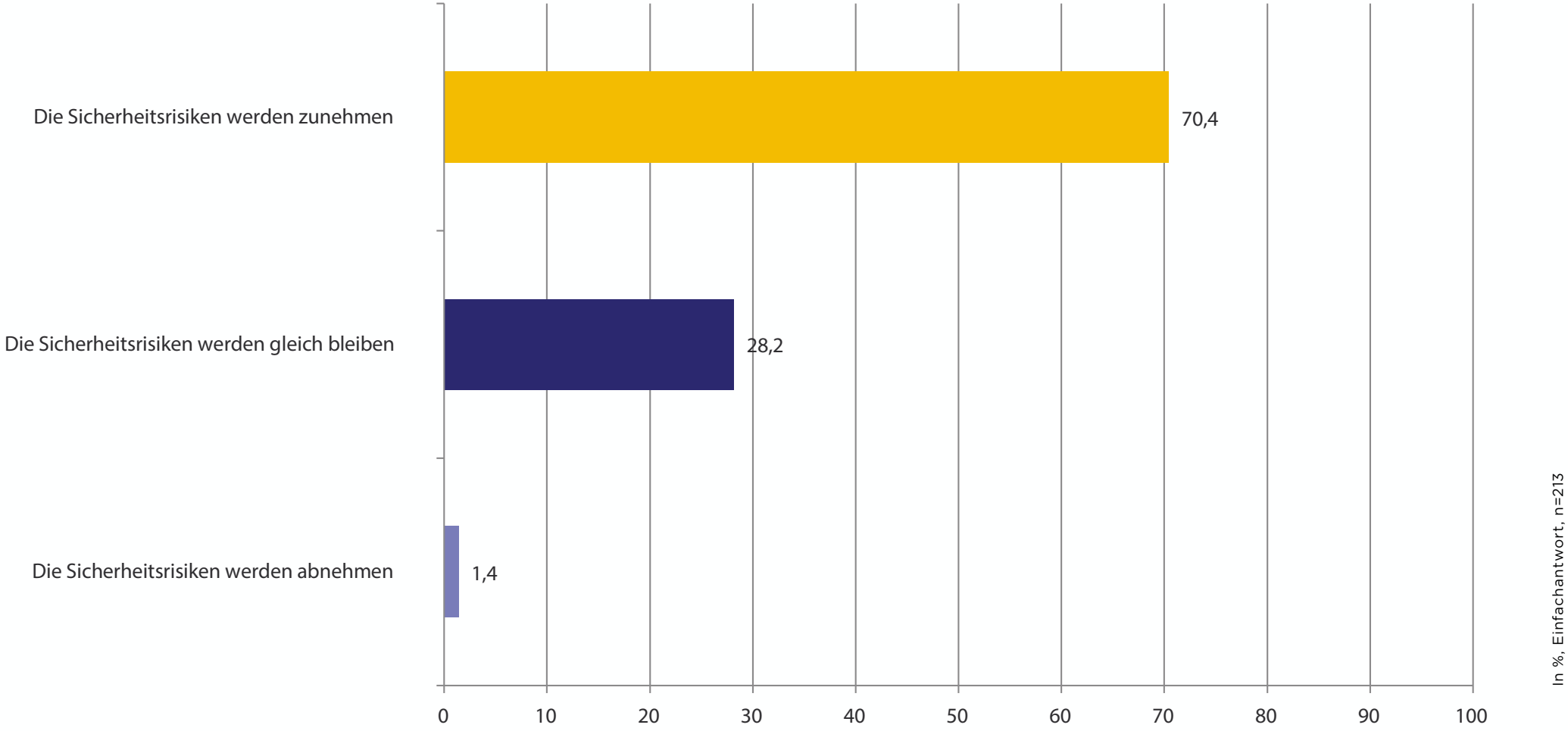
„Wie hat sich das IT-Budget in Ihrem Unternehmen im Vergleich zum Vorjahr verändert?“



In %, Einfachantwort, n=213

VERÄNDERUNG DER SICHERHEITSRISIKEN IN DEN NÄCHSTEN ZWEI JAHREN

„Wie werden sich Ihrer Meinung nach die Sicherheitsrisiken im IT-Bereich in den nächsten zwei Jahren verändern?“



ZUSAMMENFASSUNG (1/5)

Einschätzung der Bedrohungslage und Bedenken im Bereich IT-Security

- Die Bedrohungslage österreichischer Unternehmen durch zB. Hacker, Malware, Phishing usw. angegriffen zu werden, schätzen die Befragten mit 62% für „mehrmals pro Tag“ relativ hoch ein. Weitere 31% nehmen an, dass diese Angriffe „mehrmals pro Monat“ passieren.
- Mit 65% bzw. 64% sind „Ausfälle von IT -Systemen“ und „Virenangriffe“ die größten Bedenken der Befragten im Bereich IT-Security, gefolgt von „Problemen durch Spam“ mit 46%, „Datenschutzrechtlichen Problemen“ mit 45% und die „Änderung und Löschung von Daten“ mit 42%. Hinsichtlich der Unternehmensgröße gibt es mit zunehmender Mitarbeiteranzahl größere Bedenken, dass „wichtige Daten, durch interne Personen gestohlen werden“, hier liegt der Anteil in EPUs bei 8% während er in Unternehmen mit 31 oder mehr Mitarbeitern bei 36% liegt.

Status und Veränderung der Wichtigkeit von IT-Security in Unternehmen

- Mit einem Mittelwert von 1,7 (bewertet auf einer 6 -stufigen Skala von 1=„sehr wichtig“ bis 6=„überhaupt nicht wichtig“) wird dem Thema „IT -Security“ ein relativ hoher Stellenwert zugeschrieben. In Unternehmen mit 31 oder mehr Mitarbeitern (MW 1,5) ist dieser Stellenwert höher als in EPUs (MW 2,1). Personen in Management -Positionen (MW 1,5) ist “IT -Security“ noch wichtiger als Eigentümern bzw. Selbstständigen (MW 2,0).
- In den letzten zwei Jahren ist das Thema IT -Security auch immer wichtiger geworden. 69% der Befragten geben an, dass der Stellenwert der IT -Security im Unternehmen „(viel) wichtiger“ (Top2Box auf einer 6 -stufigen Skala von 1=„wurde viel wichtiger“ bis 6=„ist überhaupt nicht mehr wichtig“) geworden ist.

ZUSAMMENFASSUNG (2/5)

Einschätzung des bestehenden Schutzes

- 68% der Befragten sind der Annahme, dass ihr Unternehmen „(sehr) gut“ (Top2Box) vor internen und externen Angriffen und Datenverlusten geschützt ist.

IT-Security Vorfälle in den letzten 2 Jahren

- In den letzten 2 Jahren gab es in 41% der befragten Unternehmen IT-Security Vorfälle. Unter „Eigentümern/Selbstständigen“ gab es mit 28% vergleichsweise weniger Vorfälle als unter „Angestellten/Arbeitern“ bzw. „Personen in Management Positionen“ (50% bzw. 52%). Auch bei den EPUs und kleinen Unternehmen (2 bis 10 Mitarbeiter) gab es weniger Vorfälle mit 28% bzw. 34%.
- Bei den Vorfällen kam es meist mit 64% zu „Virenangriffen“, „Problemen durch Spam“ (47%) und zu „Ausfällen von IT-Systemen“ (36%) oder zur „Änderung oder Löschung von Daten“ (18%).

Ursachen für IT-Security Vorfälle in den letzten 2 Jahren

- Als Ursachen für IT-Security Vorfälle werden mit 39% vor allem „Irrtum oder Unwissen von Mitarbeitern“ und mit 37% der „Ausfall der Technik“ genannt. Die „absichtliche Manipulation der IT oder der Daten durch externe Personen“ wird von 35% der Befragten als Ursache genannt.

ZUSAMMENFASSUNG (3/5)

IT-Security Audits

- In gut der Hälfte aller befragten Unternehmen (53%) werden regelmäßig, wiederkehrende IT-Security Audits durchgeführt, um interne Schwachstellen, Konzeptions- und Konfigurationsfehler aufzuzeigen. Unter den Angestellten/Arbeitern geben sogar 73% an, dass IT-Security Audits regelmäßig durchgeführt werden. Der Anteil nimmt auch mit der Unternehmensgröße zu.
- In jenen Unternehmen, wo nicht regelmäßig IT-Security Audits durchgeführt werden, wird mit 44% als häufigster Grund die „fehlende Erfahrung / Kompetenz" angeführt, gefolgt von der „Nicht-Notwendigkeit" mit 37%. Als weiterer Grund für das Ausbleiben von regelmäßigen IT-Security Audits wird mit 33% der „Kostenfaktor" genannt.

Hemmnisse bei der Verbesserung der IT-Security

- Der „Kostenfaktor" (46%) und die „fehlende Erfahrung / Kompetenz" (38%) sehen die Befragten als Hauptgründe, die einer Verbesserung der IT-Security entgegenwirken. Weiters werden „Zeitmangel" (24%) und „Personalmangel" (23%) als Hemmnisse genannt. Die „fehlende Akzeptanz" wird von 17% der Befragten angegeben, wobei dieser Faktor mit der Unternehmensgröße zunimmt und von Personen in der Management-Ebene (31%) öfters genannt wird sowie in der Branche des „produzierenden Gewerbes" (39%) eine größere Rolle spielt.

Vertrauen auf externe Fachkompetenz

- 83% der Befragten würden auf „externe(s) Fachkompetenz / Wissen" vertrauen, um Sicherheitslücken im IT-Bereich aufzudecken bzw. beheben zu lassen. Dieses Vertrauen ist in EPUs geringer (72%) als in größeren Unternehmen.

ZUSAMMENFASSUNG (4/5)

Bevorzugte Settings für IT-Infrastruktur

- 45% der Befragten bevorzugen eine „IT Infrastruktur und Betrieb vor Ort“ und 26% nutzen lieber eine „österreichische Cloud“. „Außereuropäische Clouds“ und „Public Clouds“ werden vergleichsweise eher ungern genutzt (je 4-6%).

Backups und Änderung von Passwörtern

- 82% der Befragten sind sich „(sehr) sicher“, dass Daten in ihrem Unternehmen ordnungsgemäß gesichert werden. (Top2Box auf einer 6 -stufigen Skala von 1=„sehr sicher“ bis 6=„überhaupt nicht sicher).
- Unter jenen Befragten, die sich bezüglich der ordnungsgemäßen Datensicherung in ihrem Unternehmen „(sehr) sicher“ sind, geben 68% an, dass sie Backups auch außerhalb der Räumlichkeiten ihres Unternehmens aufbewahren und 58% geben an, dass die Backups regelmäßig testweise wiederhergestellt werden. Bei den EPUs werden mit 53% Backups vergleichsweise weniger oft außerhalb der Räumlichkeiten ihres Unternehmens aufbewahrt, auch unter den Eigentümern/Selbstständigen geben dies nur 56% an.
- Bei mehr als der Hälfte der befragten Unternehmen (55%) werden Passwörter zumindest „alle 4-5 Monate“ geändert. 27% davon ändern ihre Passwörter im Unternehmen sogar „alle 1-2 Monate“ oder öfters.

SPAM Problematik

- Zum Thema SPAM Problematik geben 51% der Befragten an, dass Mitarbeiter in ihrem Unternehmen unter SPAM E-Mail Nachrichten leiden.

ZUSAMMENFASSUNG (5/5)

Umsetzung von Maßnahmen der DSGVO

- Mehr als die Hälfte der befragten Unternehmen (55%) haben die technischen und organisatorischen Maßnahmen der DSGVO bereits umgesetzt und weitere 40% zumindest teilweise.
- Für jene Unternehmen, die diese Maßnahmen bereits umgesetzt haben, waren die größten Herausforderungen dabei der „Zeitmangel“ (44%), „das mangelnde juristische Wissen bzw. die rechtliche Interpretation der Verordnung“ (41%) sowie “Mitarbeiterschulungen“ (31%) und die „Implementierung der Prozesse“ (29%). Personen in Management -Positionen nennen “Mitarbeiterschulungen“ noch häufiger als größte Herausforderung (50%), für EPUs war dies natürlich weniger relevant (6%) als für größere Unternehmen.
- Für jene Unternehmen, die die Maßnahmen der DSGVO erst teilweise oder noch nicht umgesetzt haben, sehen dabei die größten Hindernisse wiederum im „Zeitmangel“ (60%) und im „mangelnden juristischen Wissen bzw. der rechtlichen Interpretation der Verordnung“ (54%).

Veränderung des IT-Budgets im letzten Jahr

- In den meisten der befragten Unternehmen (52%) ist das IT -Budget im Vergleich zum Vorjahr „gleich geblieben“, bei 37% ist es „etwas gestiegen“. Mit der Unternehmensgröße hat auch der Anstieg des IT -Budgets zugenommen.

Veränderung der Sicherheitsrisiken in den nächsten 2 Jahren

- Der Großteil der Befragen geht mit 70% davon aus, dass die Sicherheitsrisiken in den nächsten 2 Jahren „noch weiter zunehmen“ werden. 28% meinen, dass die Risiken „gleich bleiben“ und nur 1% spricht von einer Abnahme der Sicherheitsrisiken.

KONTAKT

techbold technology group AG
Dresdner Str. 89
1200 Wien

FBNr.: 436735 h
UID: ATU69951457

Tel: +43 1 34 34 333
Fax: +43 1 34 34 333 – 499

Mail: office@techbold.at
Web: www.techbold.at

MindTake Research GmbH
Karlsgasse 7/5
1040 Wien

FBNr.: 257512w
UID: ATU61393566
DVRNr.: DVR3000686

Tel.: +43 228 88 10
Fax: +43 228 98 01

Mail: office@mindtake.com
Web: www.mindtake.com