STUDIE STATUS IT-SICHERHEIT KMU ÖSTERREICH 2020

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, Jänner 2020

Inhalt

Einleitung

- Eckdaten der Studie
- Beschreibung der Stichprobe

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

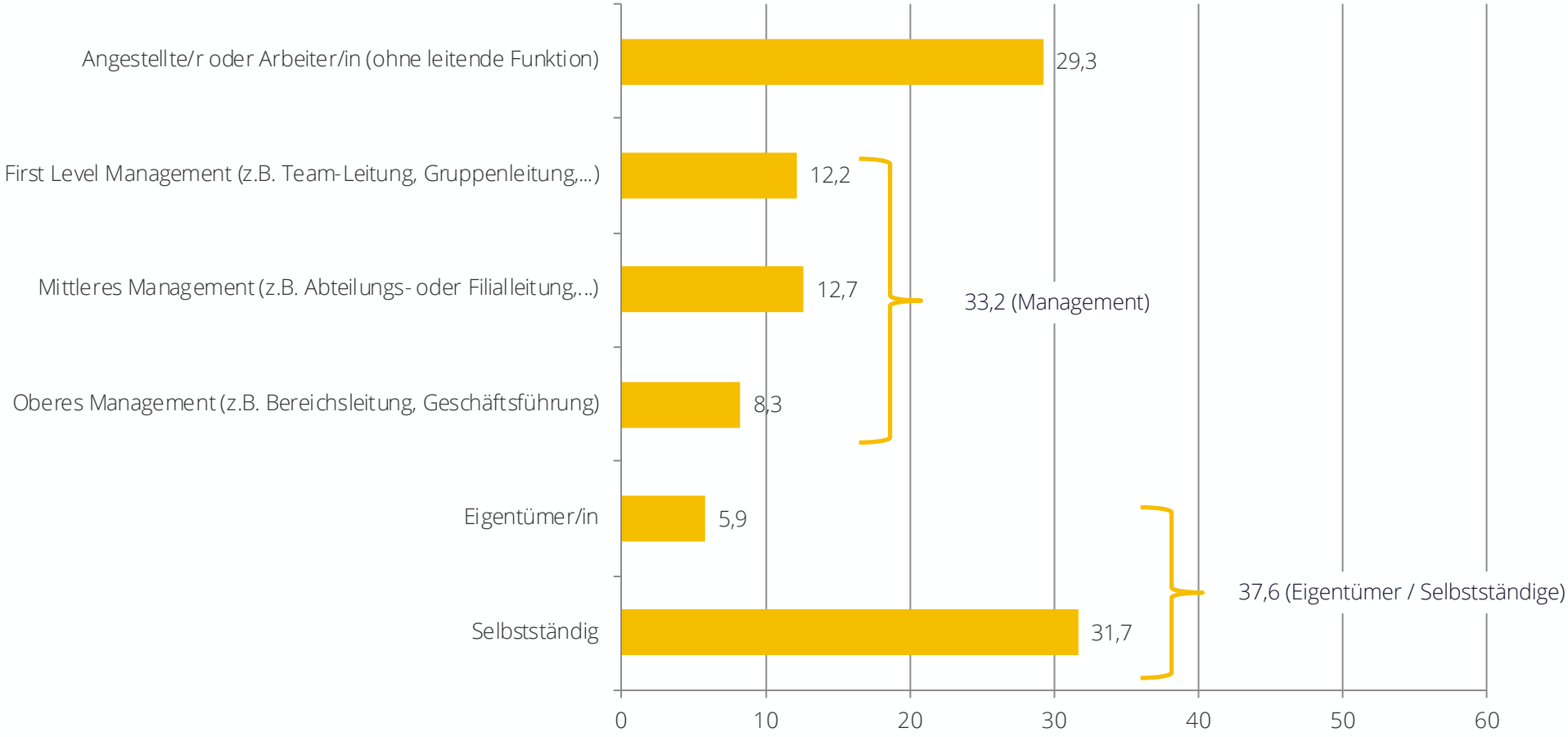
- Erhebungsmethode:

  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=205
- **Erhebungszeitraum:** 7.1.2020 – 12.1.2020
- **Befragungsdauer:** 4,07 Minuten (Median)

Beschreibung der Stichprobe (1/4)

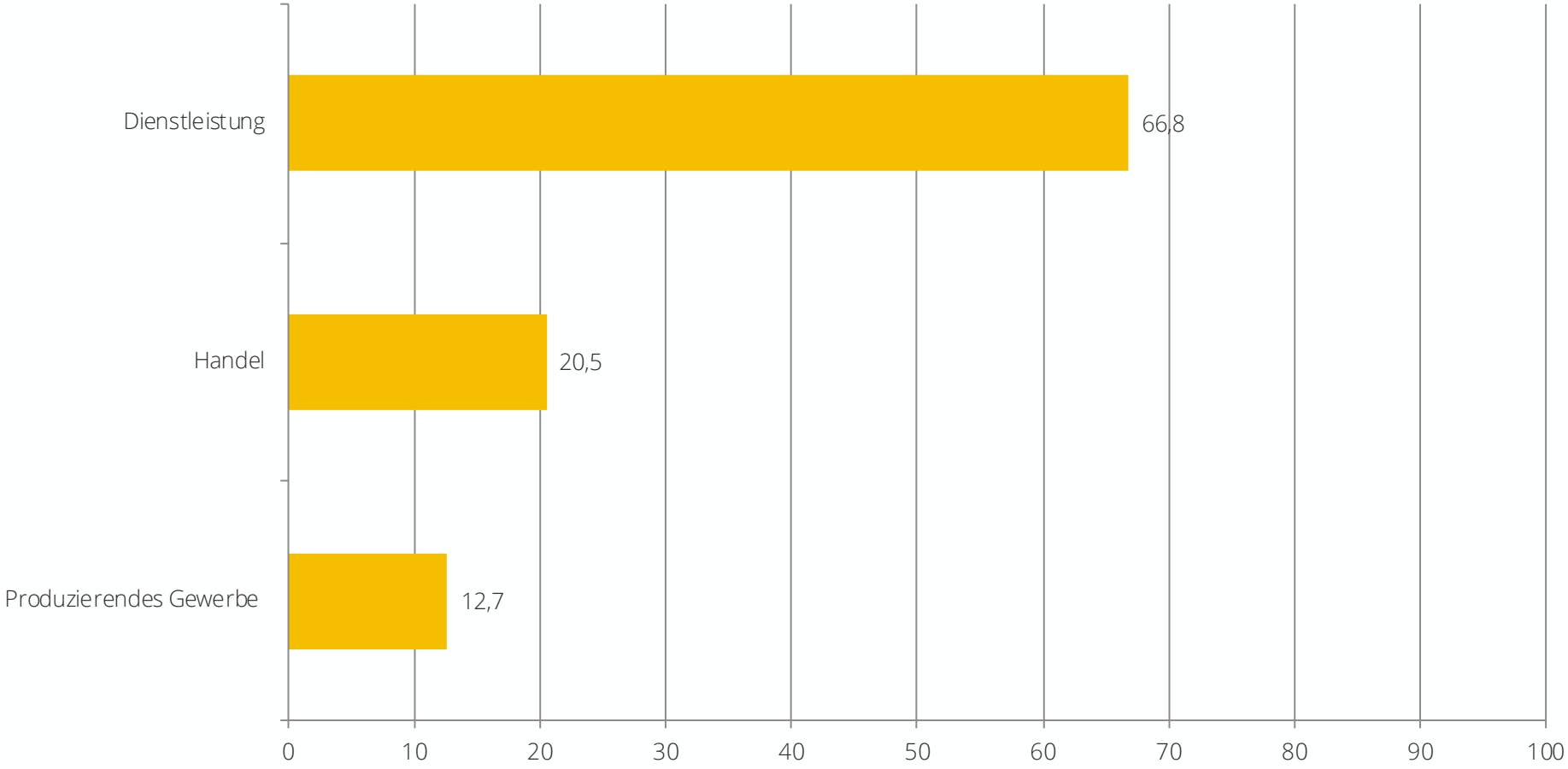
„In welcher Position sind Sie tätig?“



In %, Einfachantwort, n=205

Beschreibung der Stichprobe (2/4)

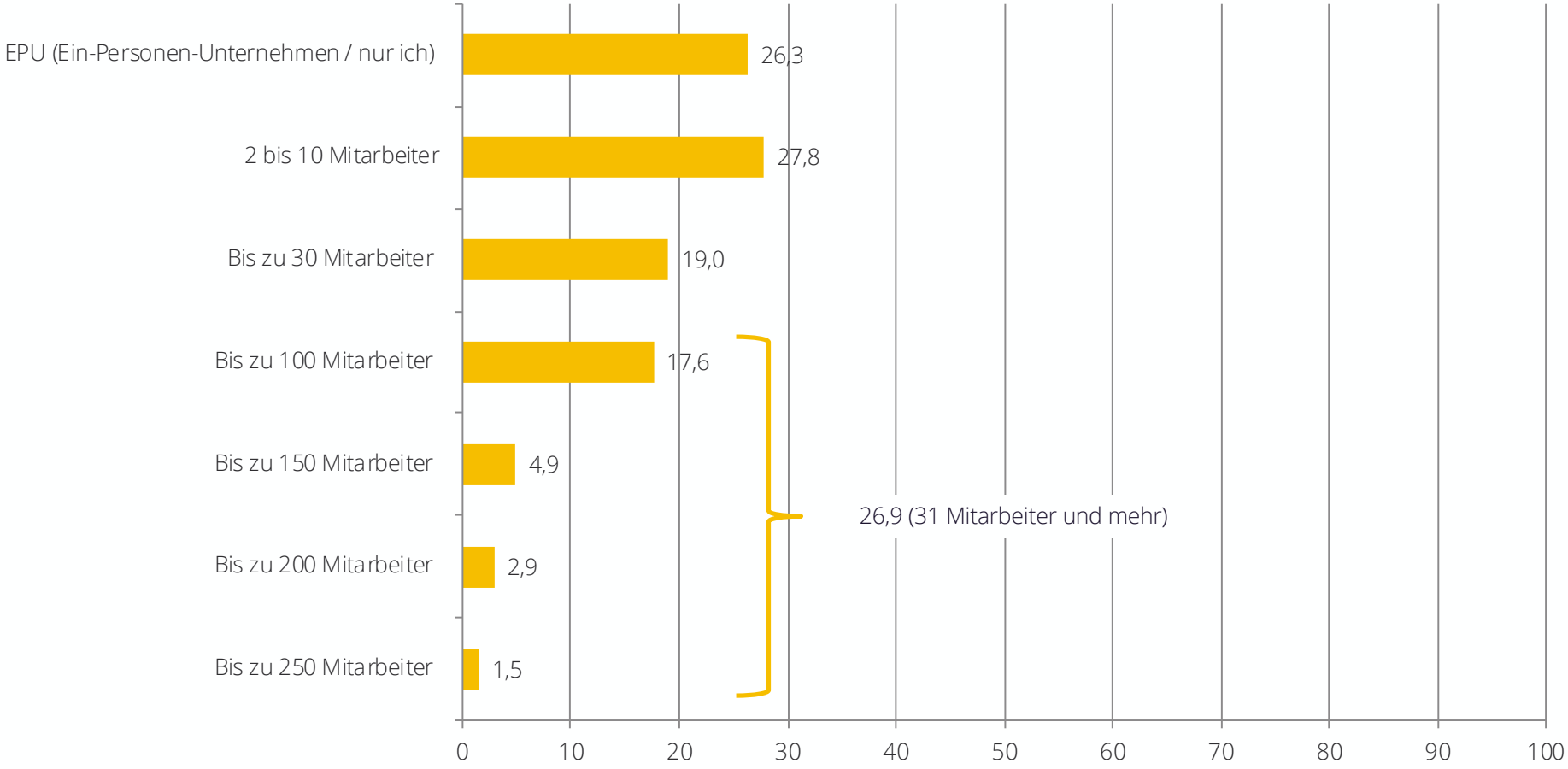
„In welcher Branche ist Ihr Unternehmen bzw. Arbeitgeber hauptsächlich tätig?“



In %, Einfachantwort, n=205

Beschreibung der Stichprobe (3/4)

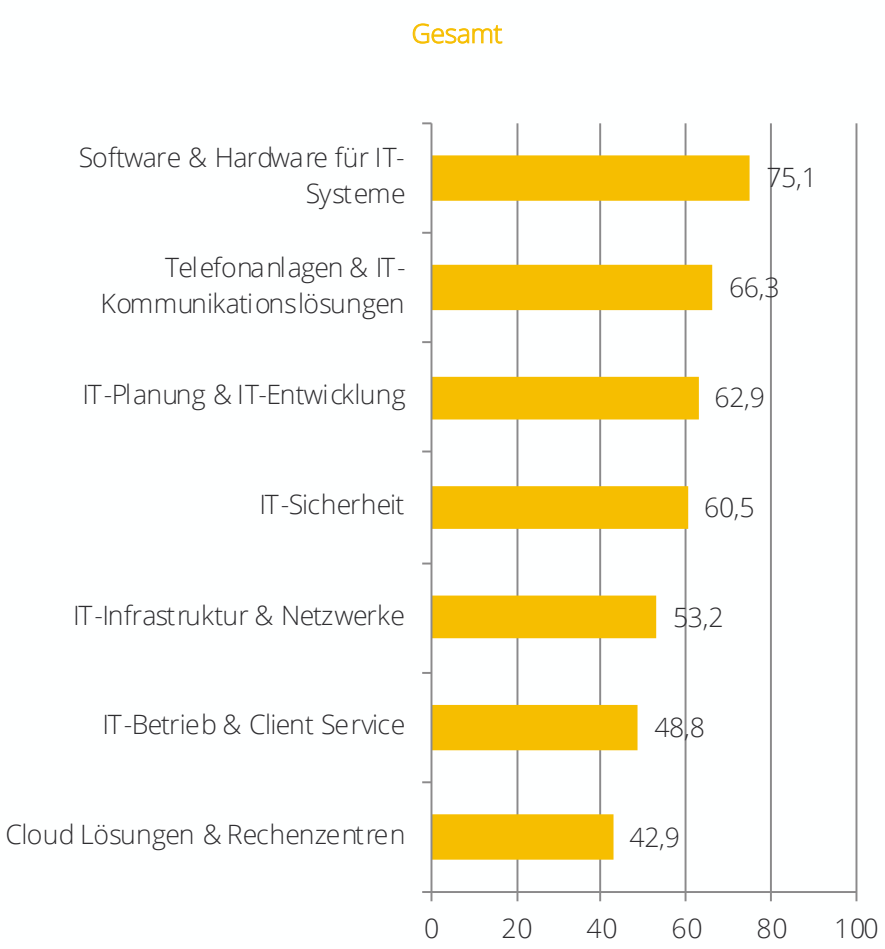
„Wie viele fixe Mitarbeiter sind ungefähr in Ihrem Unternehmen beschäftigt?“



In %, Einfachantwort, n=205

Beschreibung der Stichprobe (4/4)

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



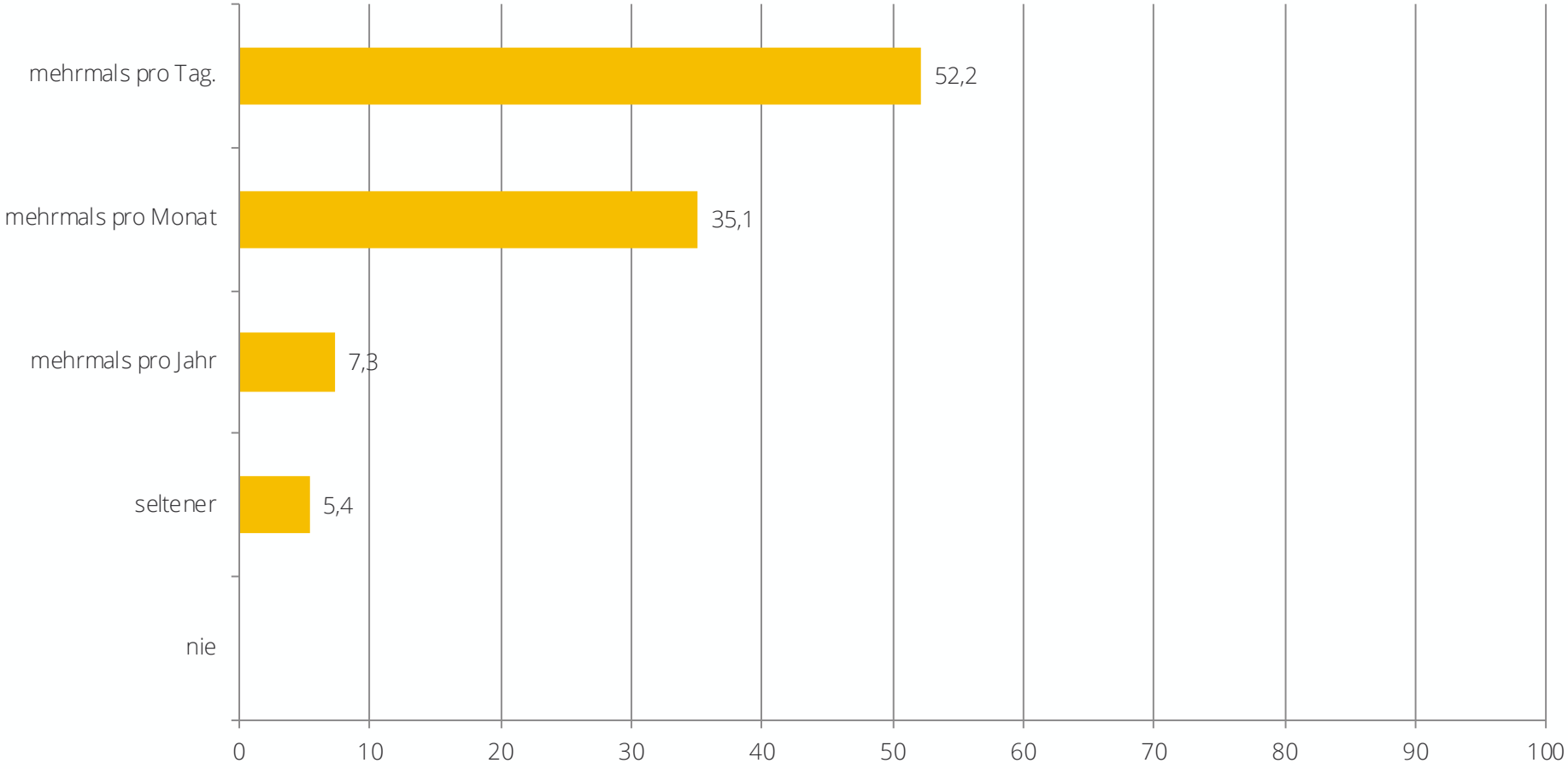
Position			Unternehmensgröße			
Angestellte /Arbeiter	Manage-ment	Eigentümer / Selbst-ständige	EPU	2 bis 10 MA	11 bis 30 MA	31 MA und mehr
56,7	76,5	88,3	90,7	71,9	69,2	67,3
55,0	63,2	77,9	72,2	82,5	53,8	52,7
40,0	63,2	80,5	81,5	63,2	59,0	47,3
36,7	57,4	81,8	87,0	57,9	51,3	43,6
35,0	44,1	75,3	72,2	56,1	53,8	30,9
33,3	44,1	64,9	68,5	43,9	38,5	41,8
21,7	35,3	66,2	68,5	42,1	30,8	27,3

In %, Mehrfachantworten, n=205

Ergebnisse der Studie

Einschätzung der Bedrohungslage

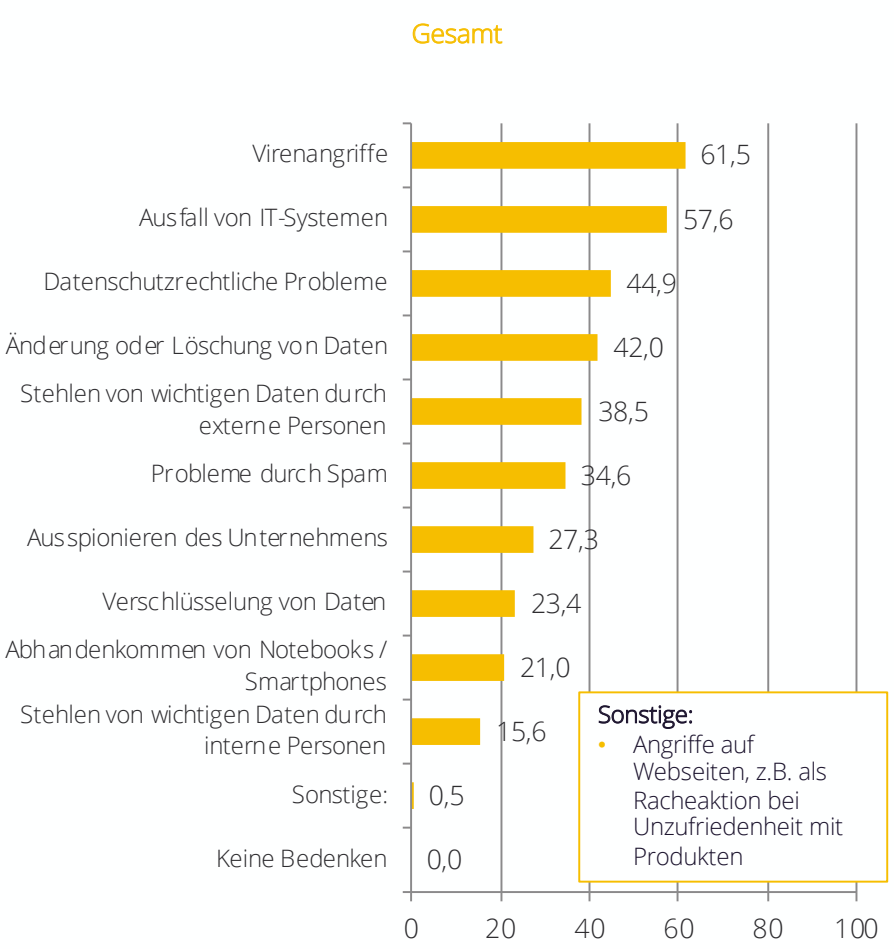
„Was schätzen Sie, wie oft werden österreichische Unternehmen im Durchschnitt (durch z.B. Hacker, Malware, Phishing, usw.) angegriffen?“



In %, Einfachantwort, n=205

Bedenken im Bereich IT-Security

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

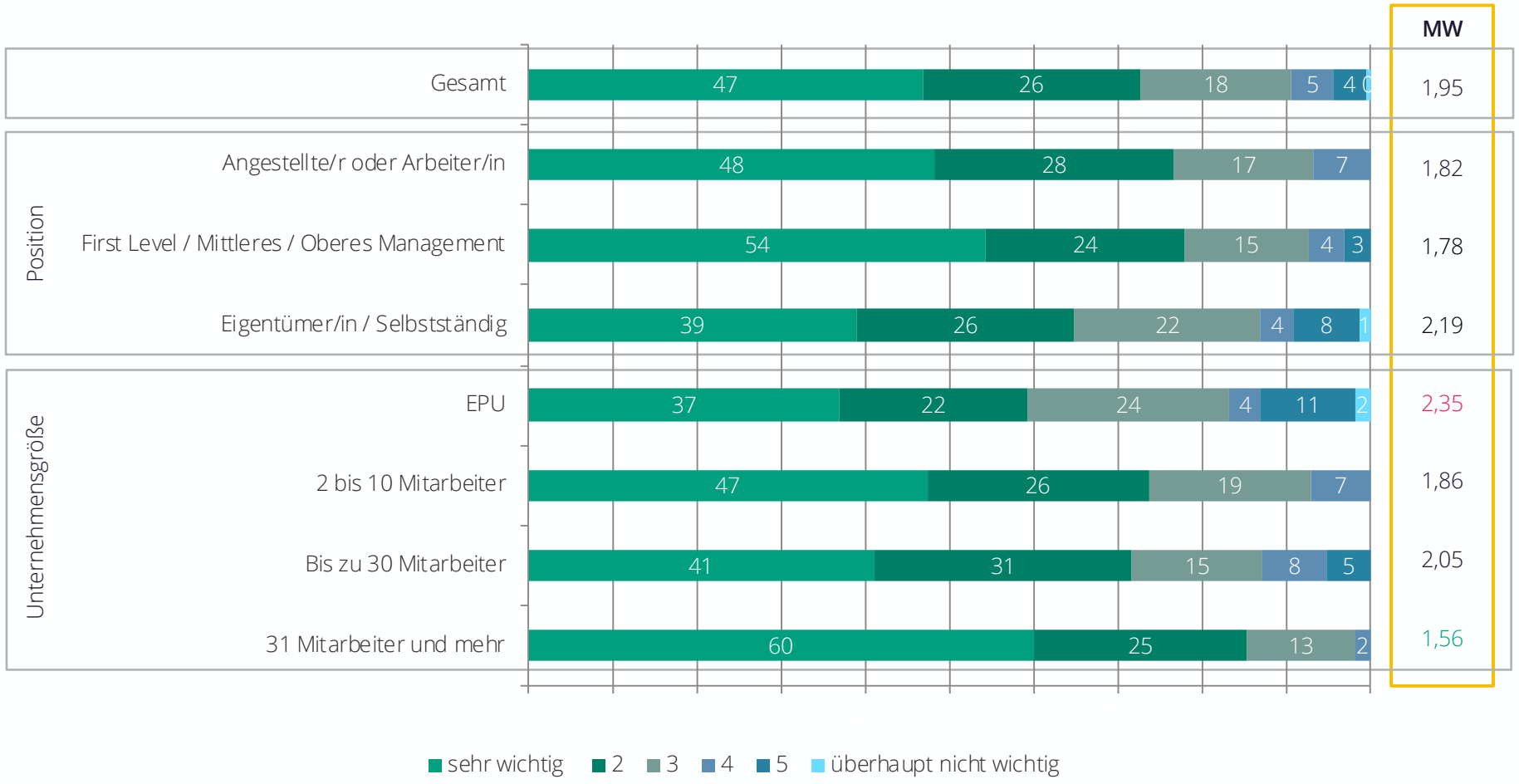


Position			Unternehmensgröße			
Angestellte /Arbeiter	Manage-ment	Eigentümer / Selbst-ständige	EPU	2 bis 10 MA	11 bis 30 MA	31 MA und mehr
56,7	63,2	63,6	64,8	68,4	53,8	56,4
48,3	60,3	62,3	59,3	59,6	64,1	49,1
33,3	55,9	44,2	40,7	54,4	35,9	45,5
35,0	42,6	46,8	38,9	50,9	41,0	36,4
45,0	38,2	33,8	31,5	42,1	38,5	41,8
31,7	36,8	35,1	35,2	35,1	43,6	27,3
31,7	30,9	20,8	18,5	26,3	28,2	36,4
21,7	30,9	18,2	11,1	29,8	23,1	29,1
20,0	16,2	26,0	31,5	15,8	15,4	20,0
20,0	19,1	9,1	7,4	14,0	17,9	23,6
1,7	0,0	0,0	0,0	0,0	2,6	0,0
0,0	0,0	0,0	0,0	0,0	0,0	0,0

In %, Mehrfachantworten, n=205

Wichtigkeit von IT-Security im Unternehmen

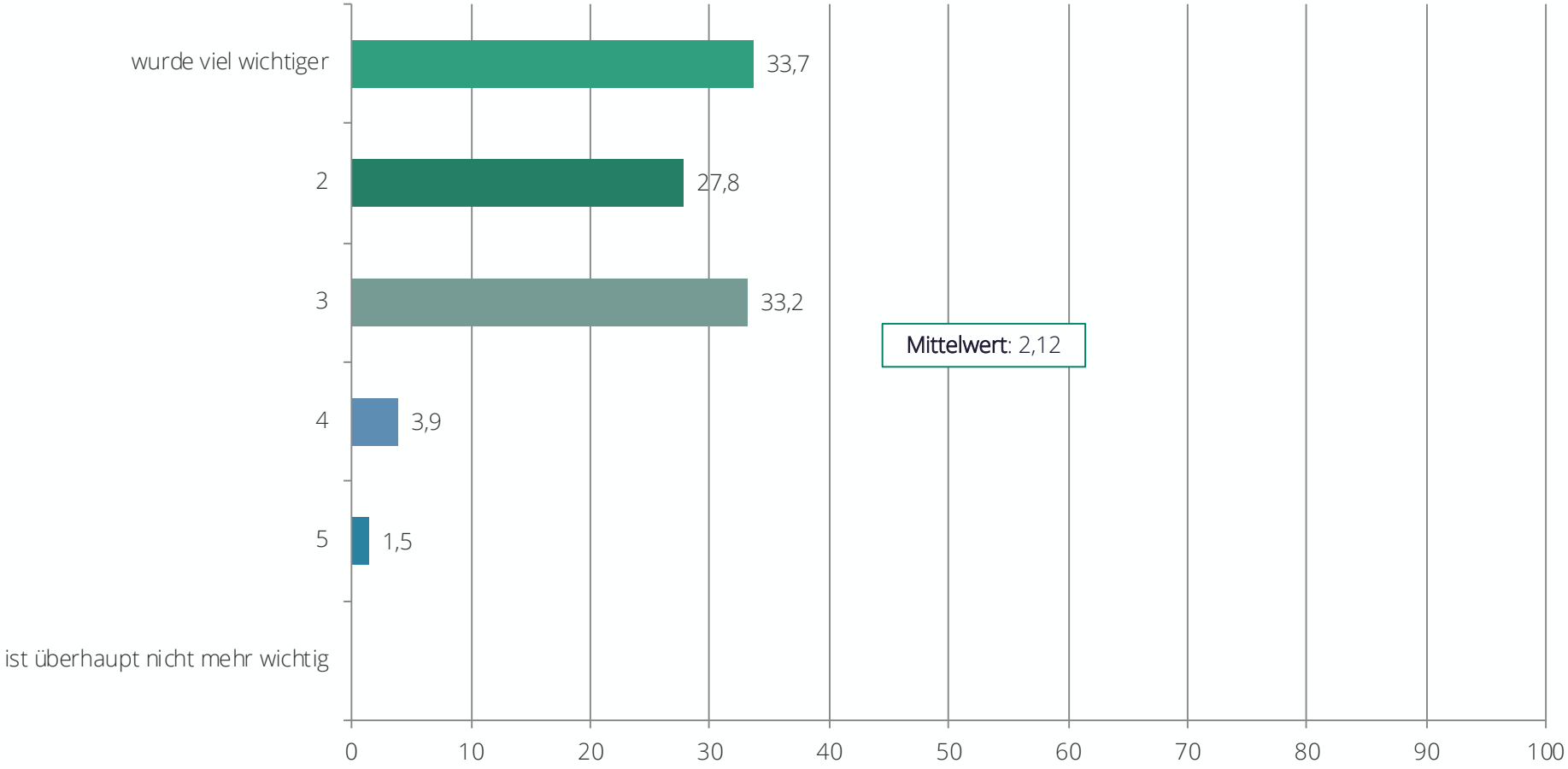
„Wie wichtig ist das Thema IT-Security innerhalb Ihres Unternehmens?“



In % und Mittelwerte, Einfachantwort, n=205

Veränderung der Wichtigkeit von IT-Security in Unternehmen

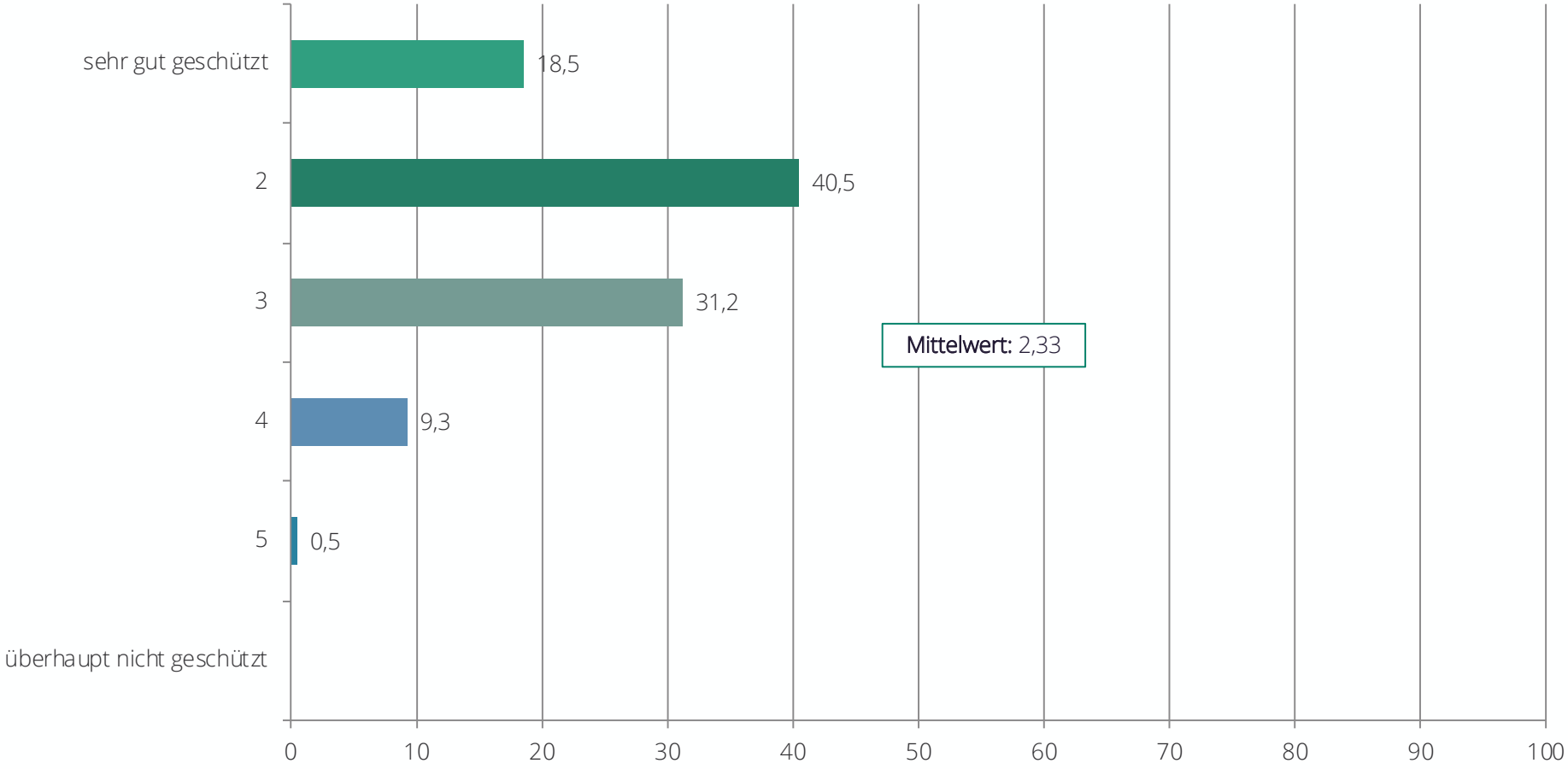
„Wie hat sich der Stellenwert der IT-Security in Ihrem Unternehmen in den letzten zwei Jahren verändert?“



In % und Mittelwert, Einfachantwort, n=205

Einschätzung des bestehenden Schutzes

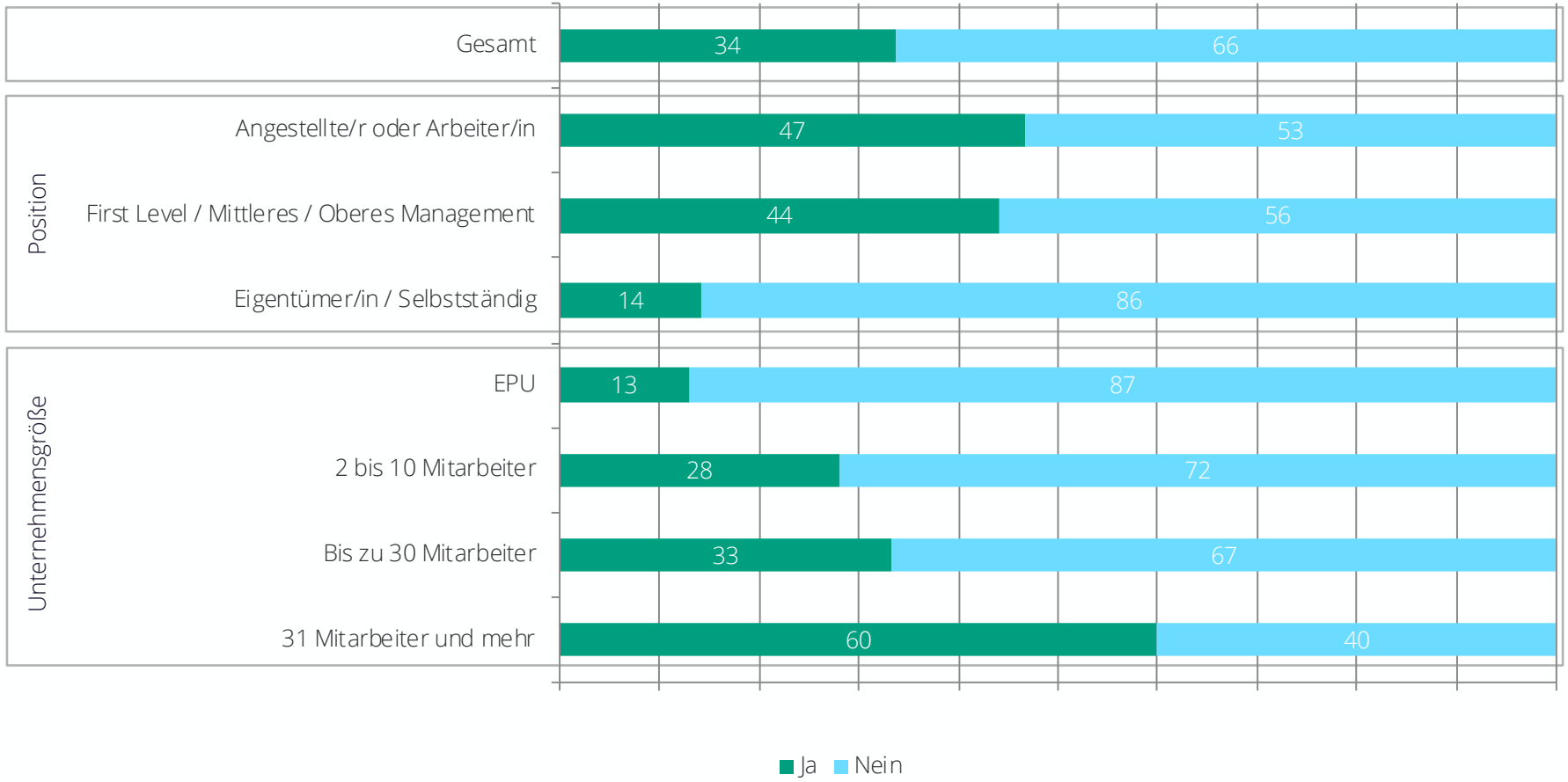
„Was denken Sie, wie gut ist Ihr Unternehmen vor internen und externen Angriffen und Datenverlust geschützt?“



In % und Mittelwert, Einfachantwort, n=205

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, Datenmanipulation, usw.) gegeben?“

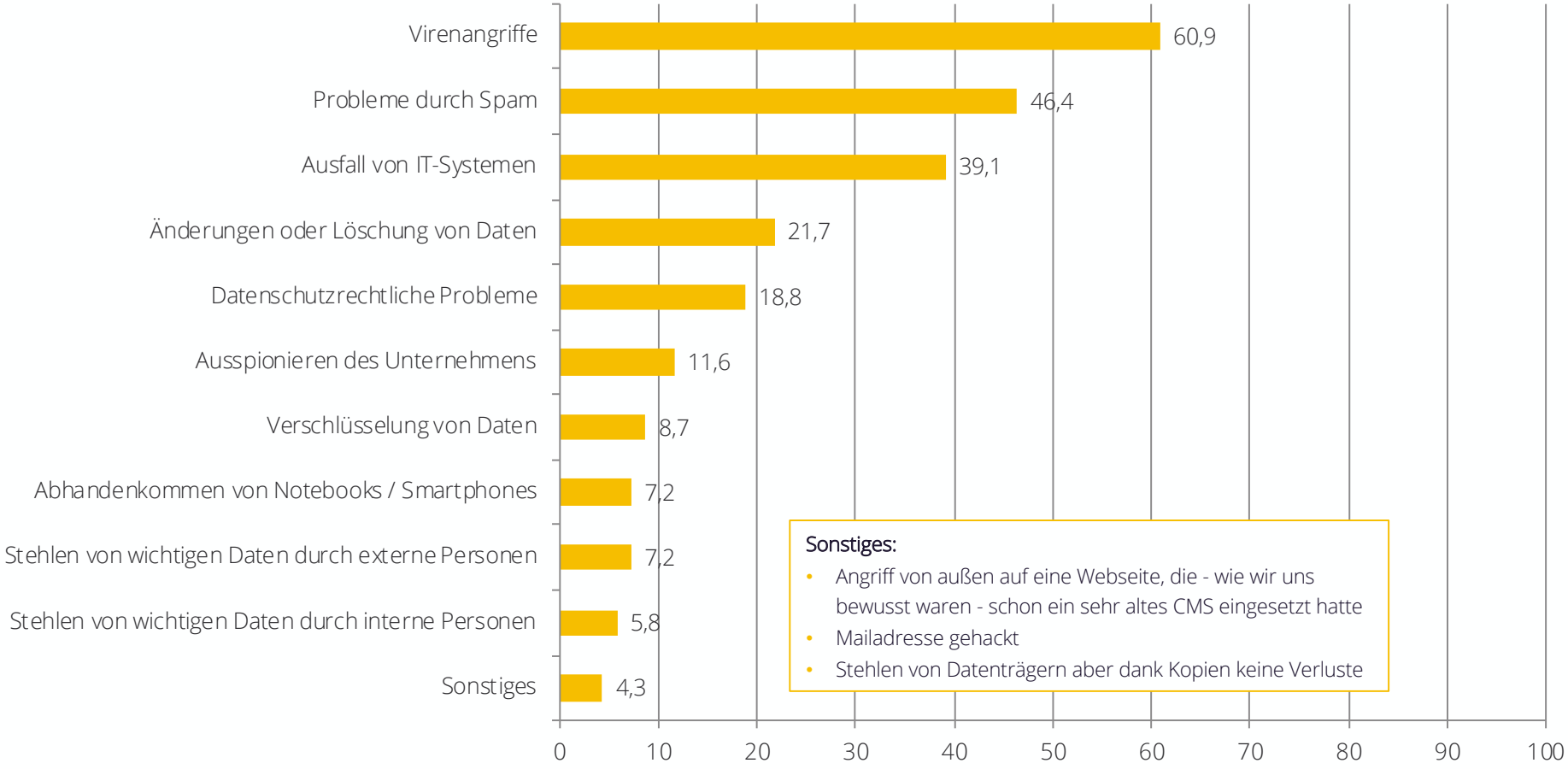


In %, Einfachantwort, n=205

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.

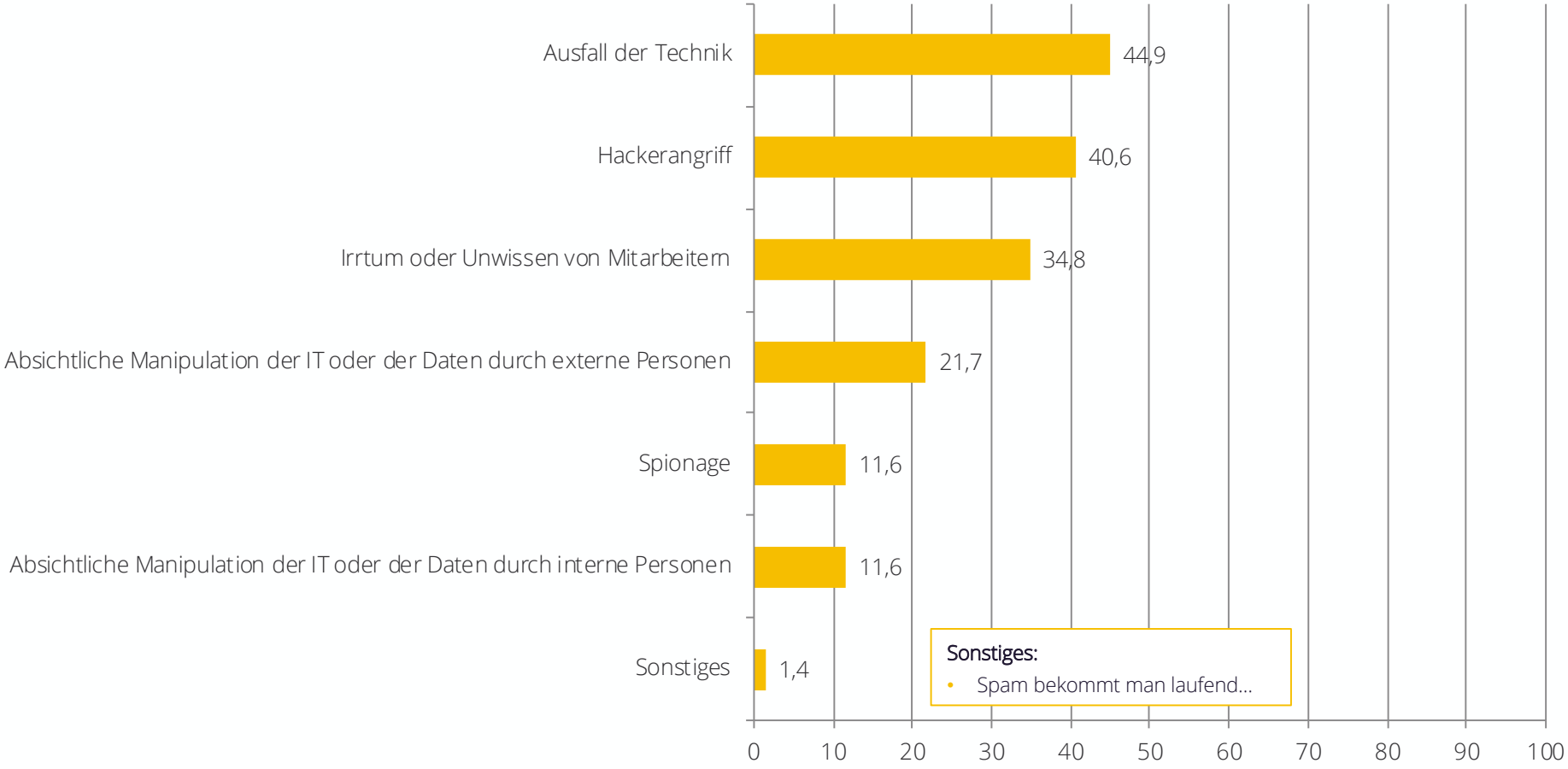


In %, Mehrfachantworten, n=69

Ursachen für IT-Security-Vorfälle

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

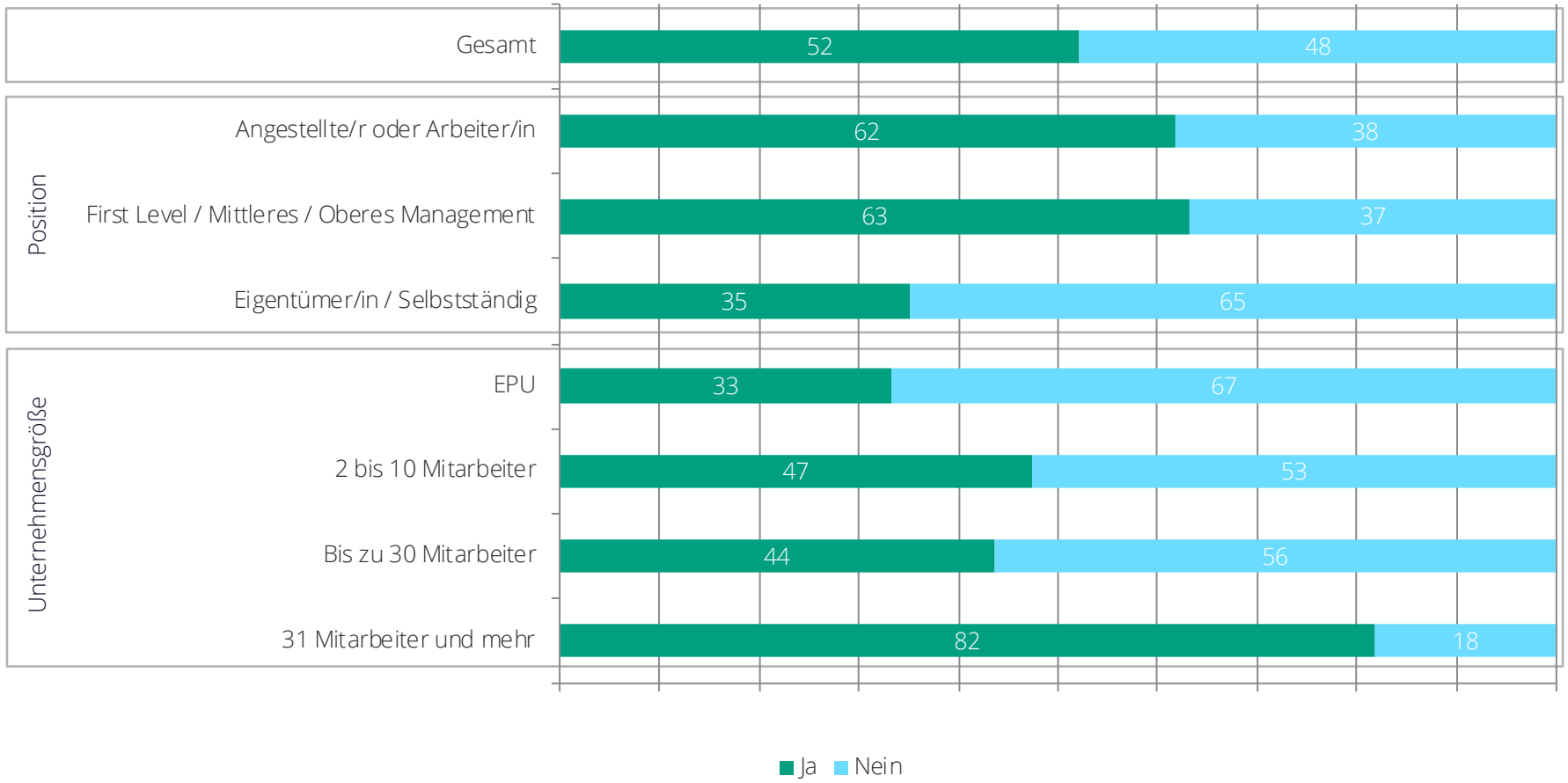
Frage wurde nur jenen gestellt, in deren Unternehmen es in den letzten 2 Jahren einen IT-Vorfall gab.



In %, Mehrfachantworten, n=69

Regelmäßigkeit von IT-Security Audits

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

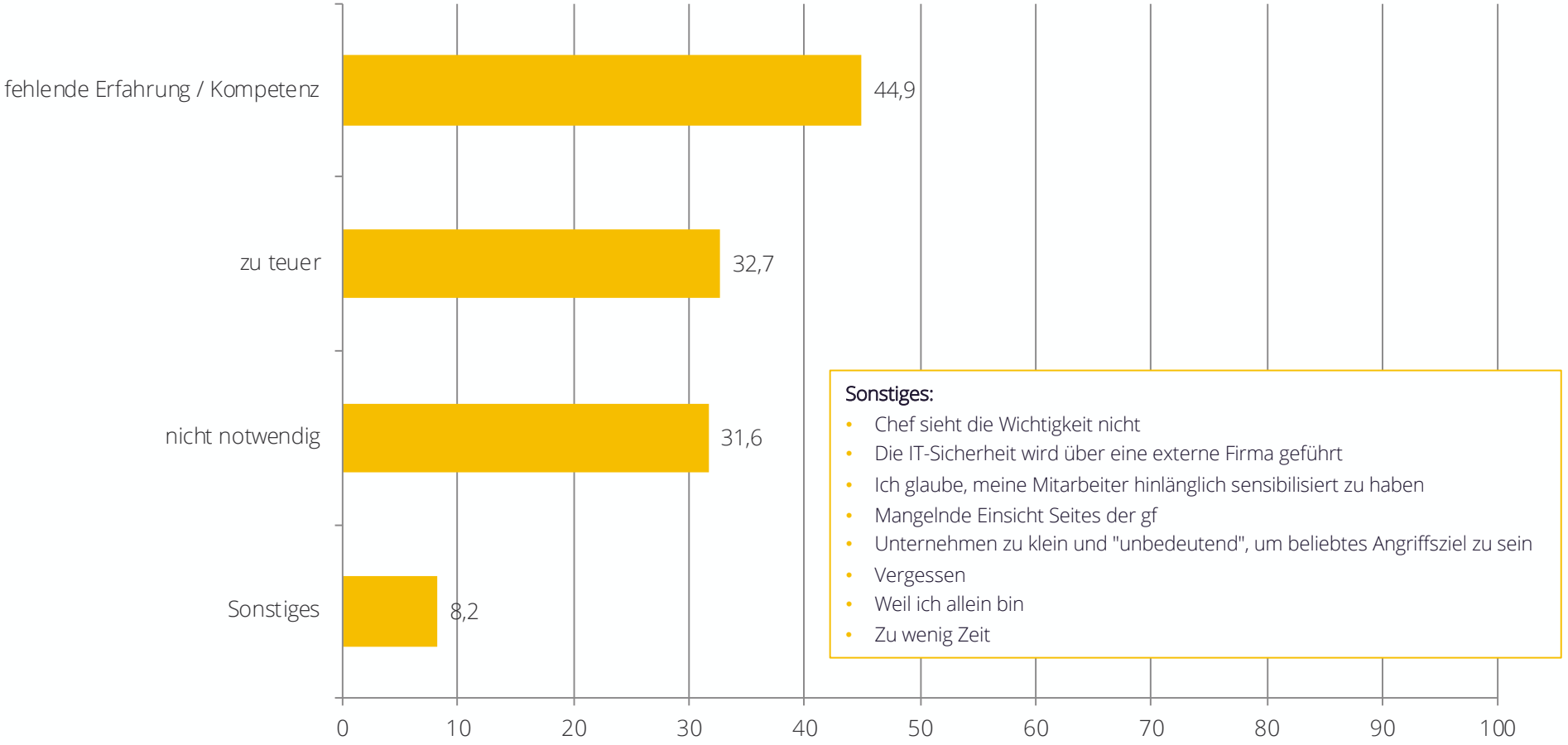


In %, Einfachantwort, n=205

Gründe für keine regelmäßigen IT-Security Audits

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

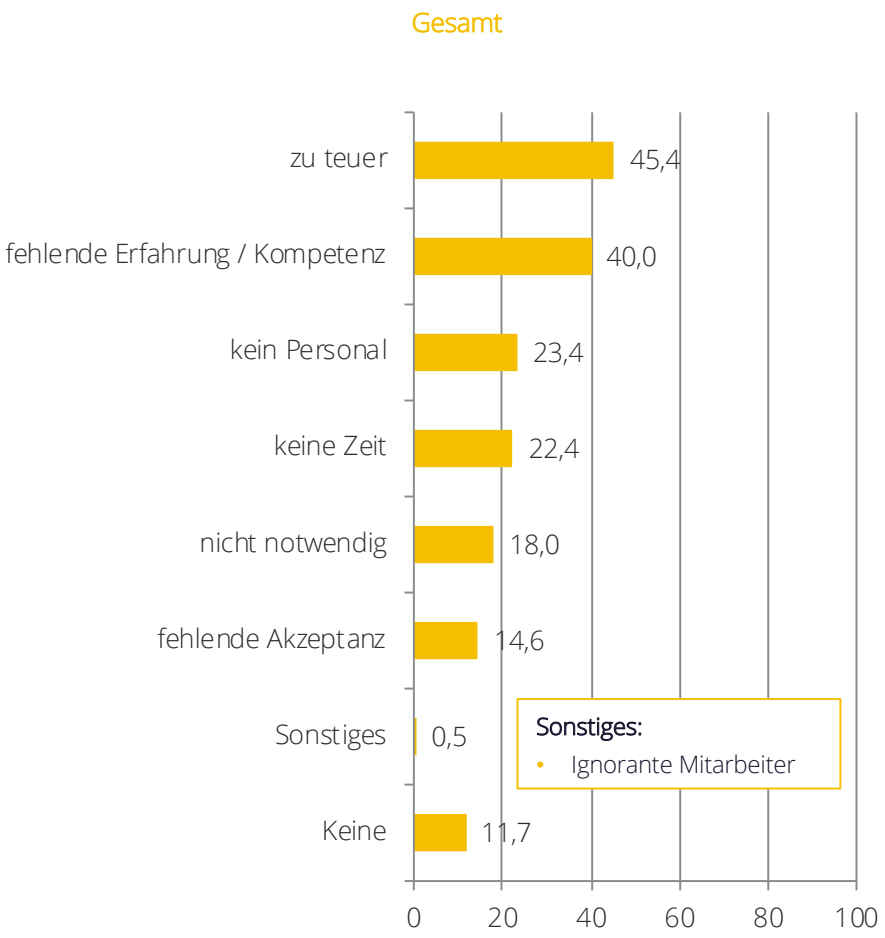
Frage wurde nur jenen gestellt, die keine regelmäßigen IT-Security Audits durchführen.



In %, Mehrfachantworten, n=98

Hemmnisse bei der Verbesserung der IT-Security (1/2)

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

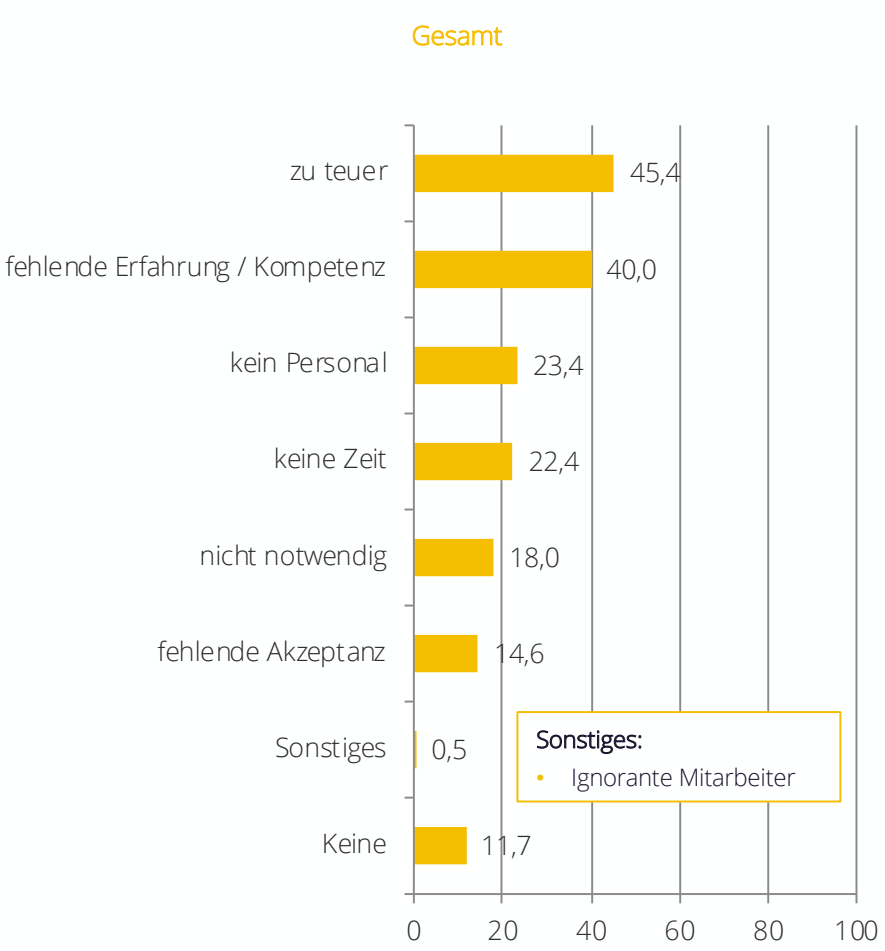


Position			Branche		
Angestellte/Arbeiter	Manage-ment	Eigentümer / Selbst-ständige	Prod. Gewerbe	Handel	Dienst-leistung
51,7	41,2	44,2	53,8	59,5	39,4
36,7	45,6	37,7	34,6	42,9	40,1
18,3	29,4	22,1	30,8	21,4	22,6
26,7	14,7	26,0	19,2	19,0	24,1
6,7	20,6	24,7	11,5	14,3	20,4
21,7	23,5	1,3	3,8	14,3	16,8
0,0	1,5	0,0	3,8	0,0	0,0
5,0	14,7	14,3	3,8	4,8	15,3

In %, Mehrfachantworten, n=205

Hemmnisse bei der Verbesserung der IT-Security (2/2)

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

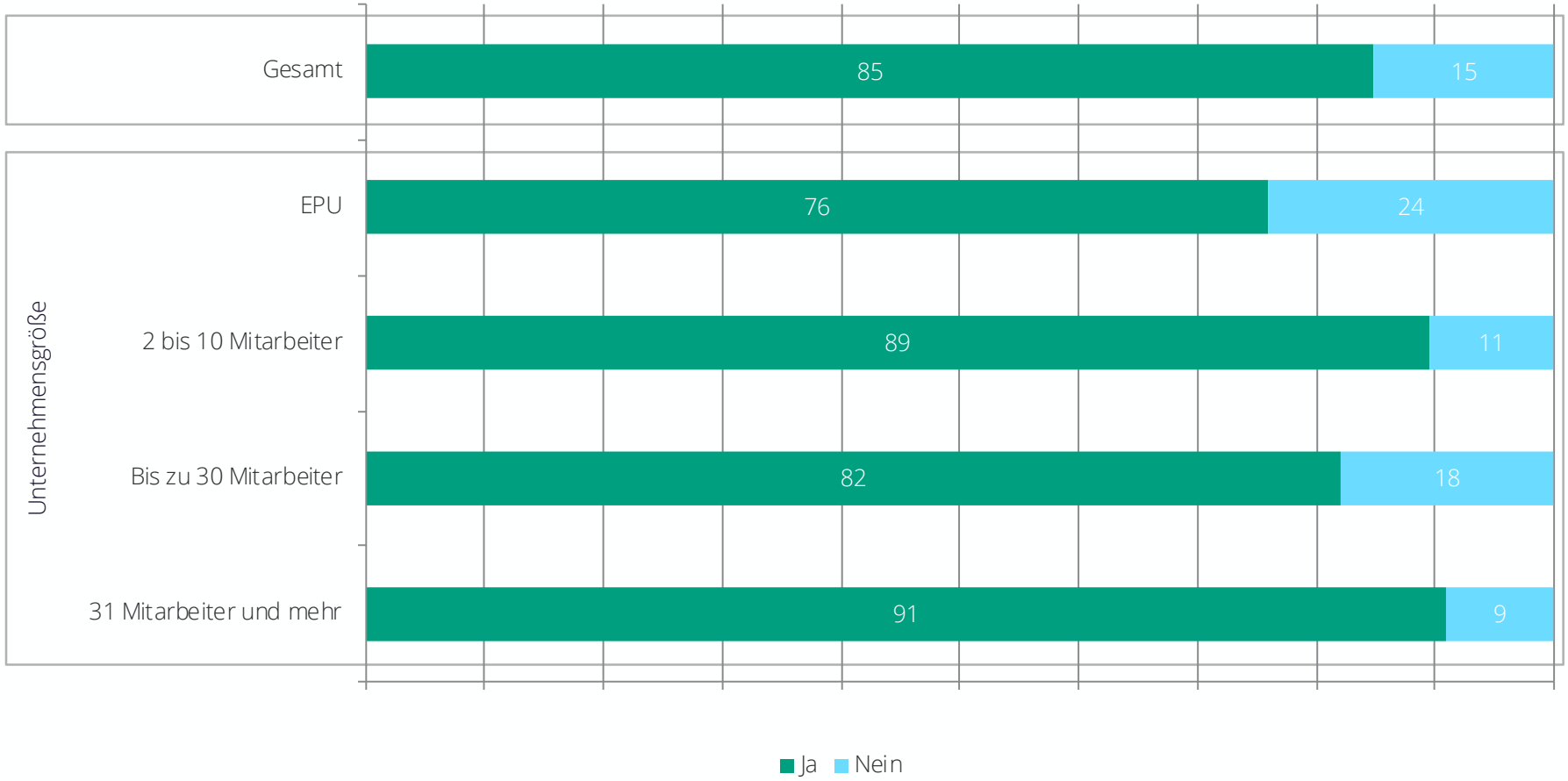


Unternehmensgröße			
EPU	2 bis 10 MA	11 bis 30 MA	31 MA und mehr
46,3	38,6	53,8	45,5
33,3	47,4	46,2	34,5
16,7	17,5	33,3	29,1
24,1	26,3	17,9	20,0
33,3	14,0	7,7	14,5
0,0	12,3	33,3	18,2
0,0	0,0	0,0	1,8
14,8	12,3	10,3	9,1

In %, Mehrfachantworten, n=205

Vertrauen auf externe Fachkompetenz

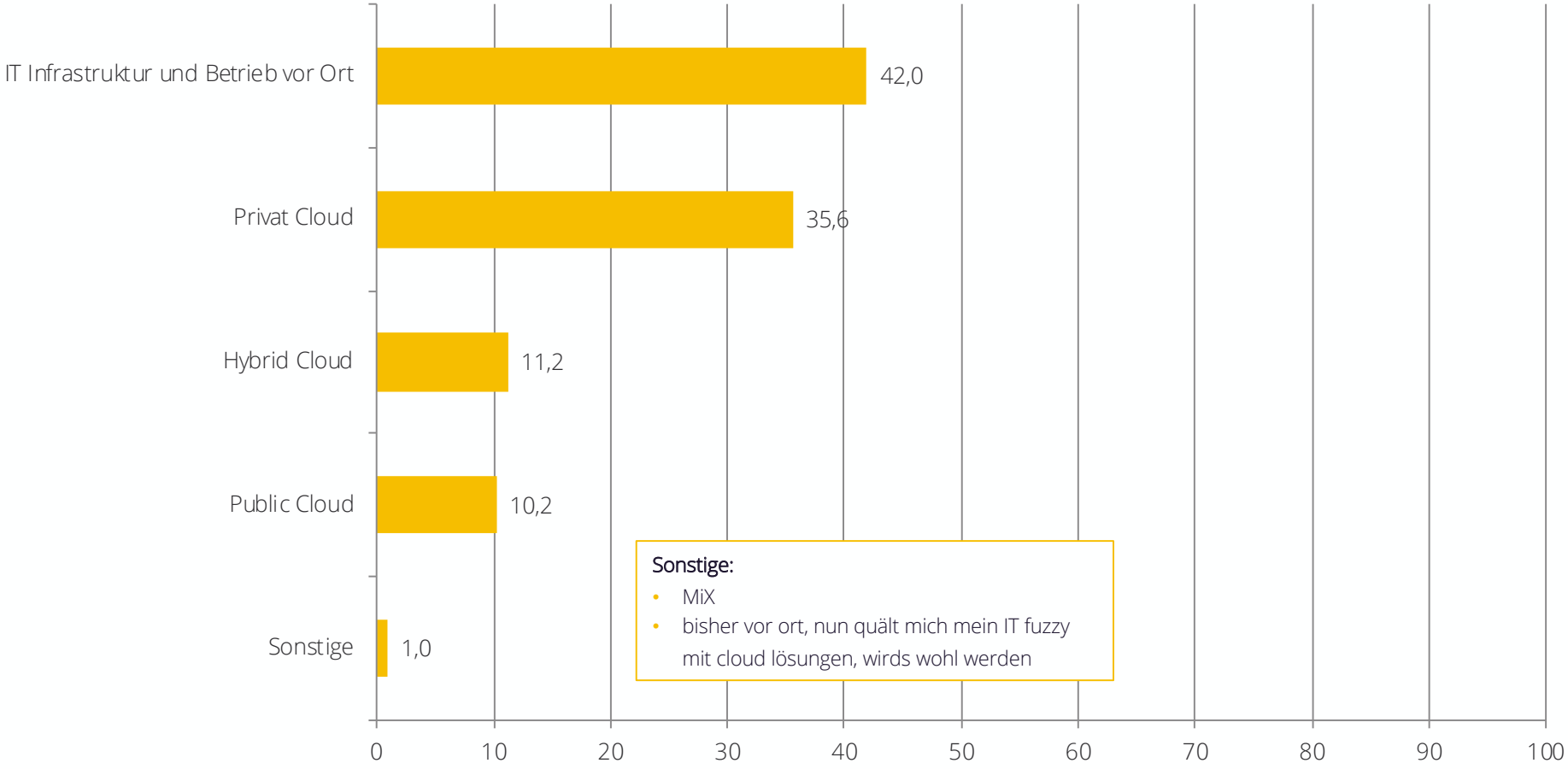
„Würden Sie auf externe(s) Fachkompetenz / Wissen vertrauen, um in Ihrem Unternehmen Sicherheitslücken im IT-Bereich aufzudecken und/oder beheben zu lassen?“



In %, Einfachantwort, n=205

Bevorzugte Settings für IT-Infrastruktur

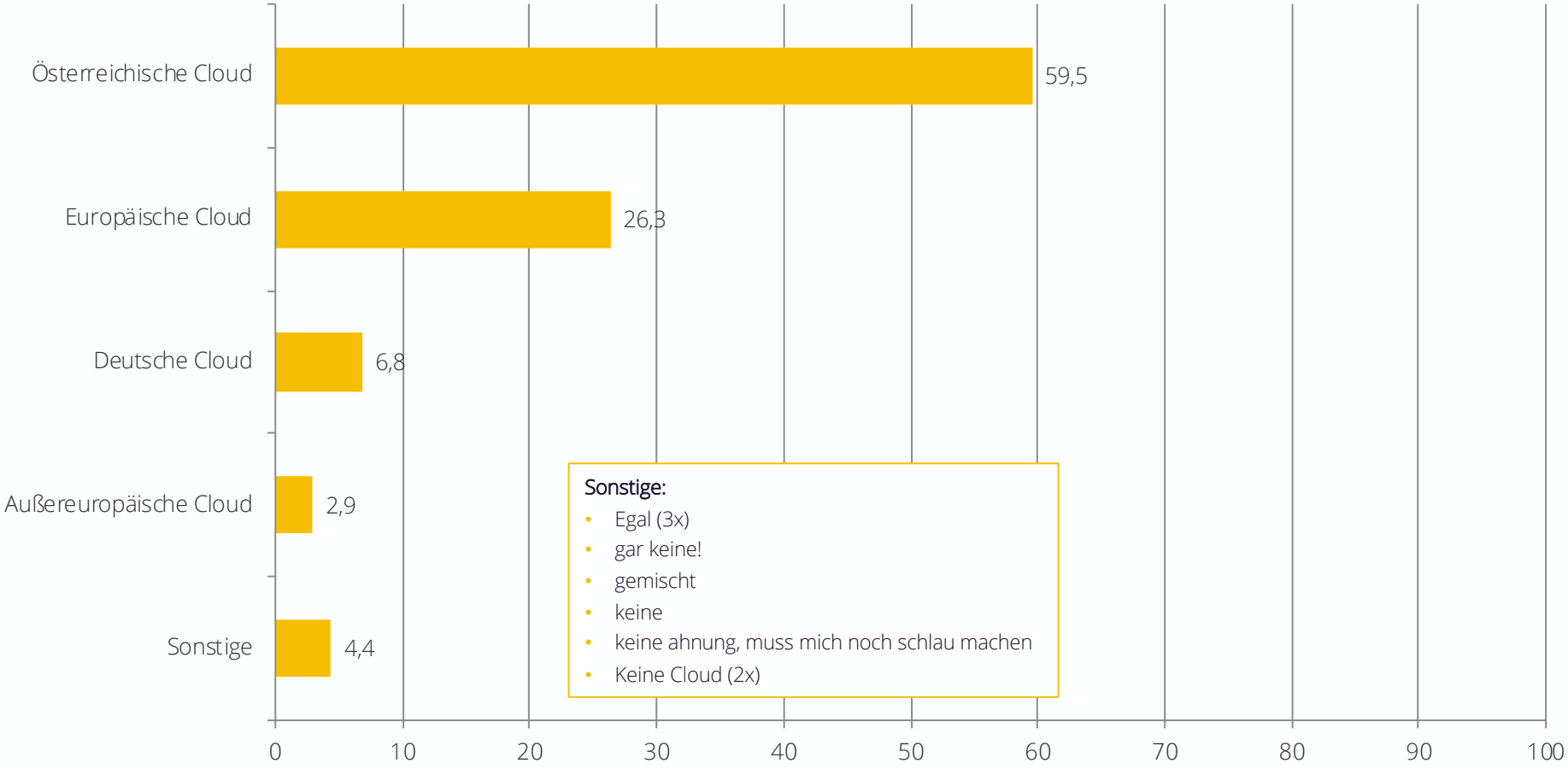
„Welche der folgenden Settings für eine IT-Infrastruktur bevorzugen Sie?“



In %, Einfachantwort, n=205

Bevorzugte Standorte für die Cloud

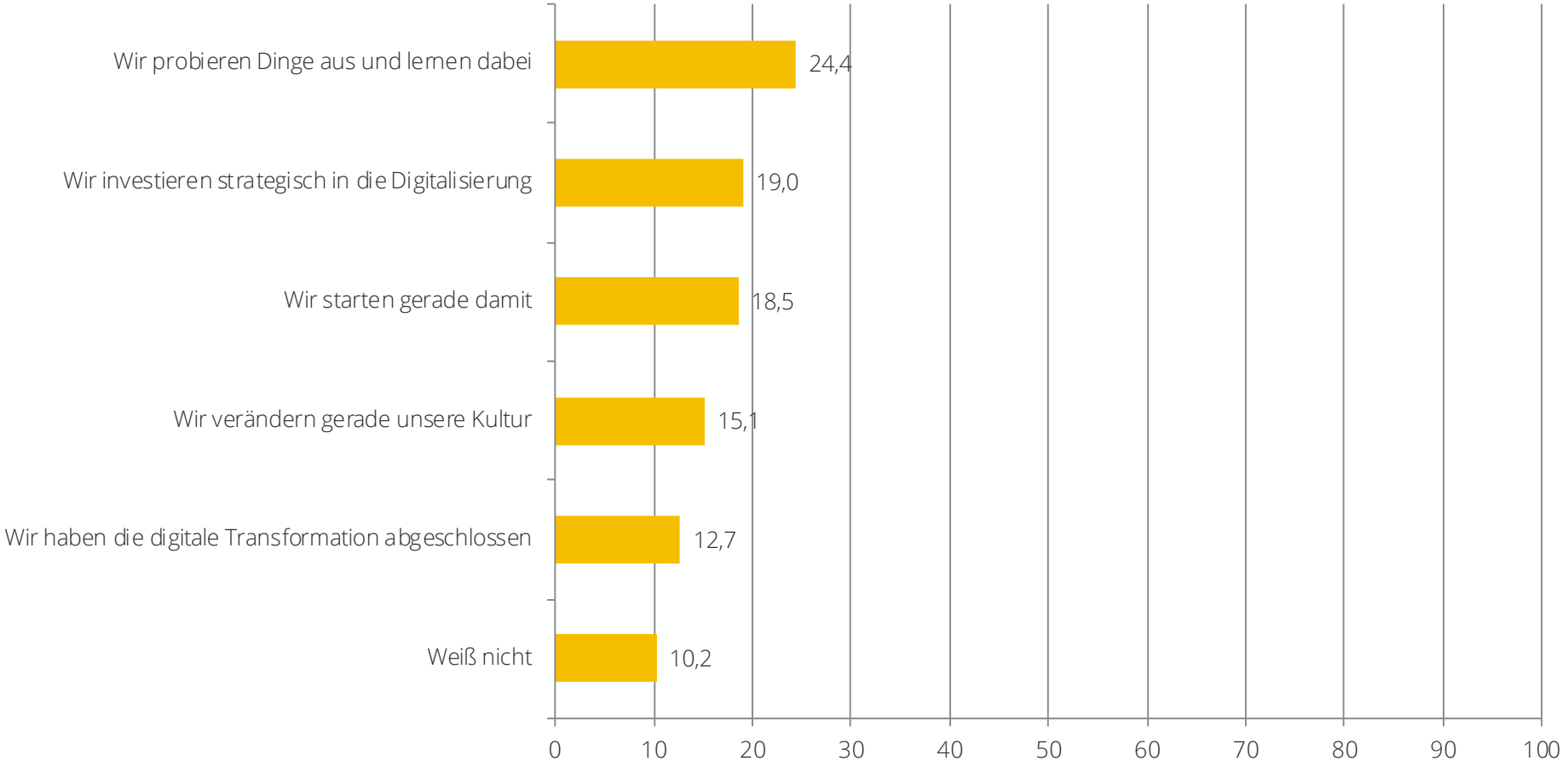
„Welchen Standort für die Cloud bevorzugen Sie? “



In %, Einfachantwort, n=205

Status der Digitalisierung im Unternehmen

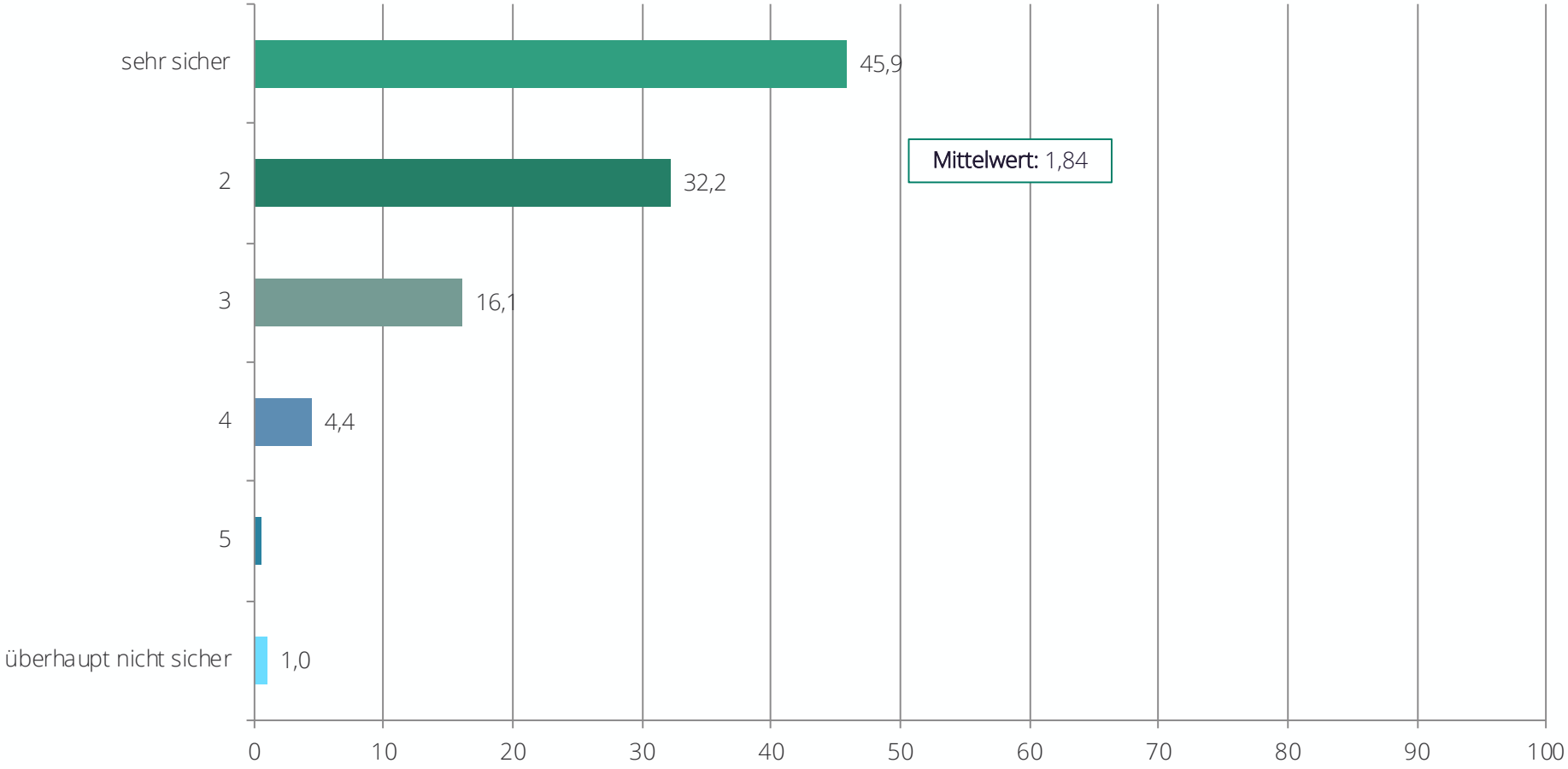
„Wie würden Sie den aktuellen Status der Digitalisierung (oder der digitalen Transformation) in Ihrem Unternehmen bezeichnen? “



In %, Einfachantwort, n=205

Ordnungsgemäße Backups im Unternehmen

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

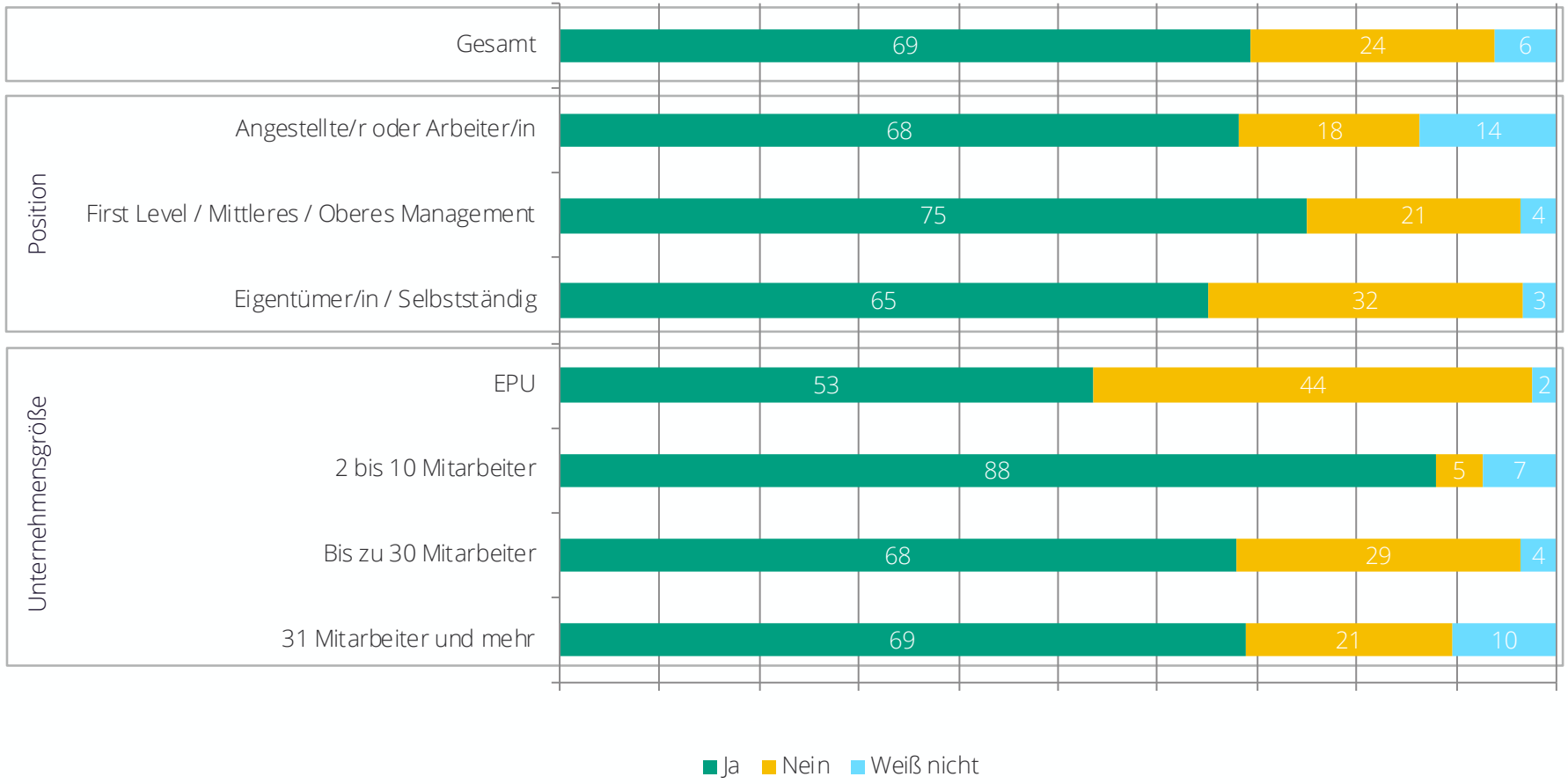


In %, Einfachantwort, n=205

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.

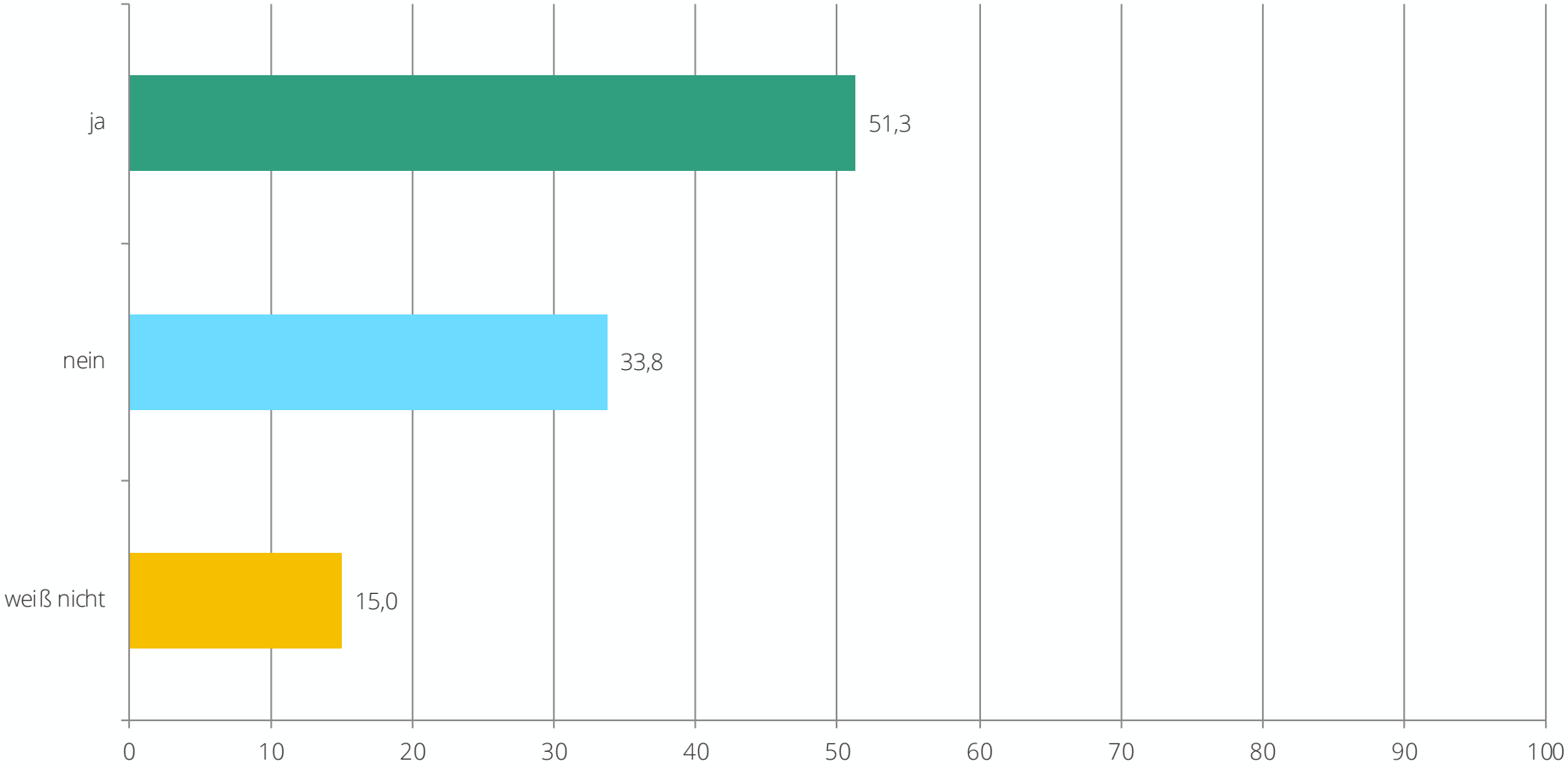


In %, Einfachantwort, n=160

Testweise Wiederherstellung von Backups

„Und werden die Backups regelmäßig testweise wiederhergestellt?“

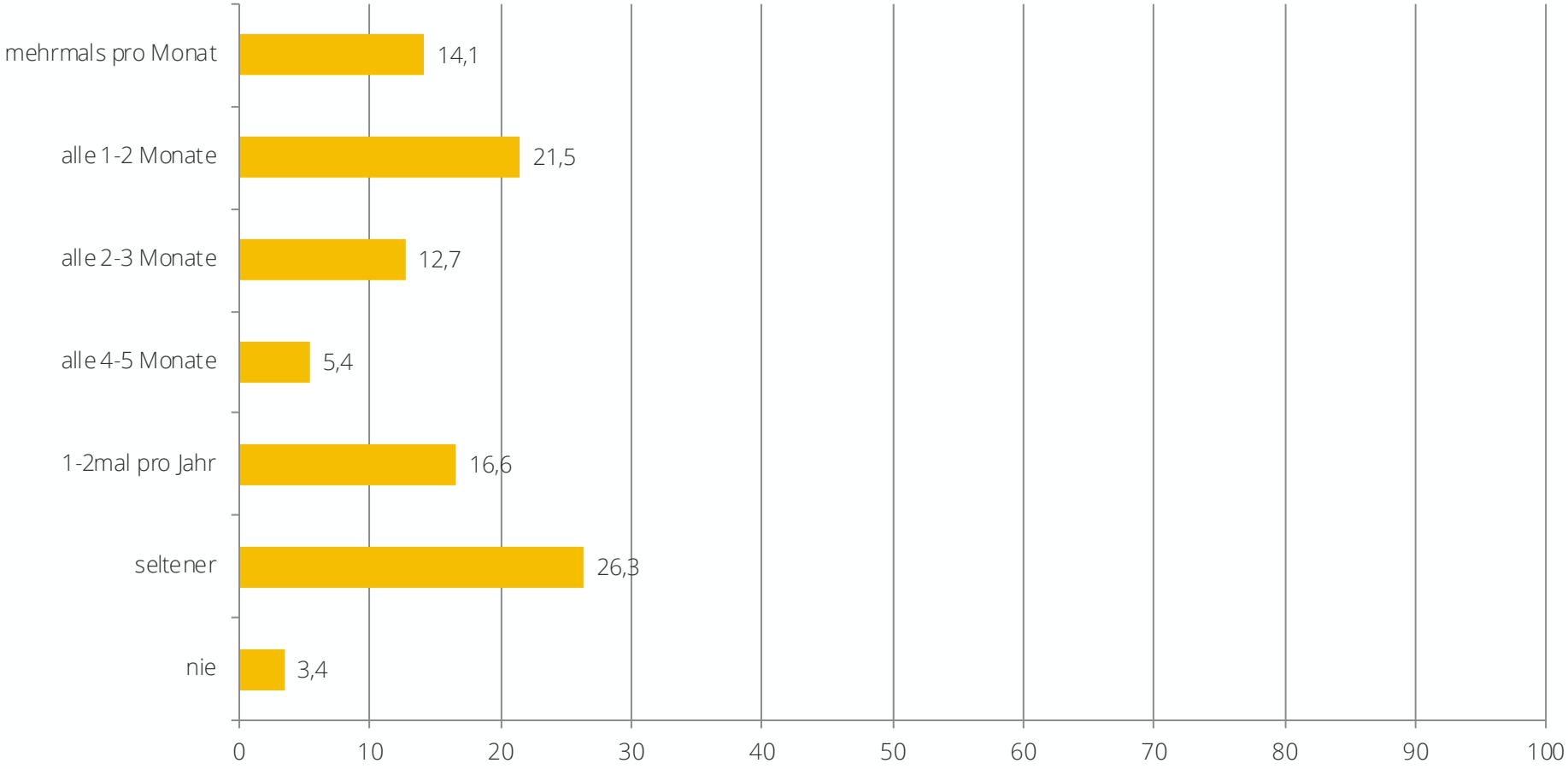
Frage wurde nur jenen gestellt, die (sehr) sicher sind, dass Backups im Unternehmen durchgeführt werden.



In %, Einfachantwort, n=160

Änderung von Passwörtern

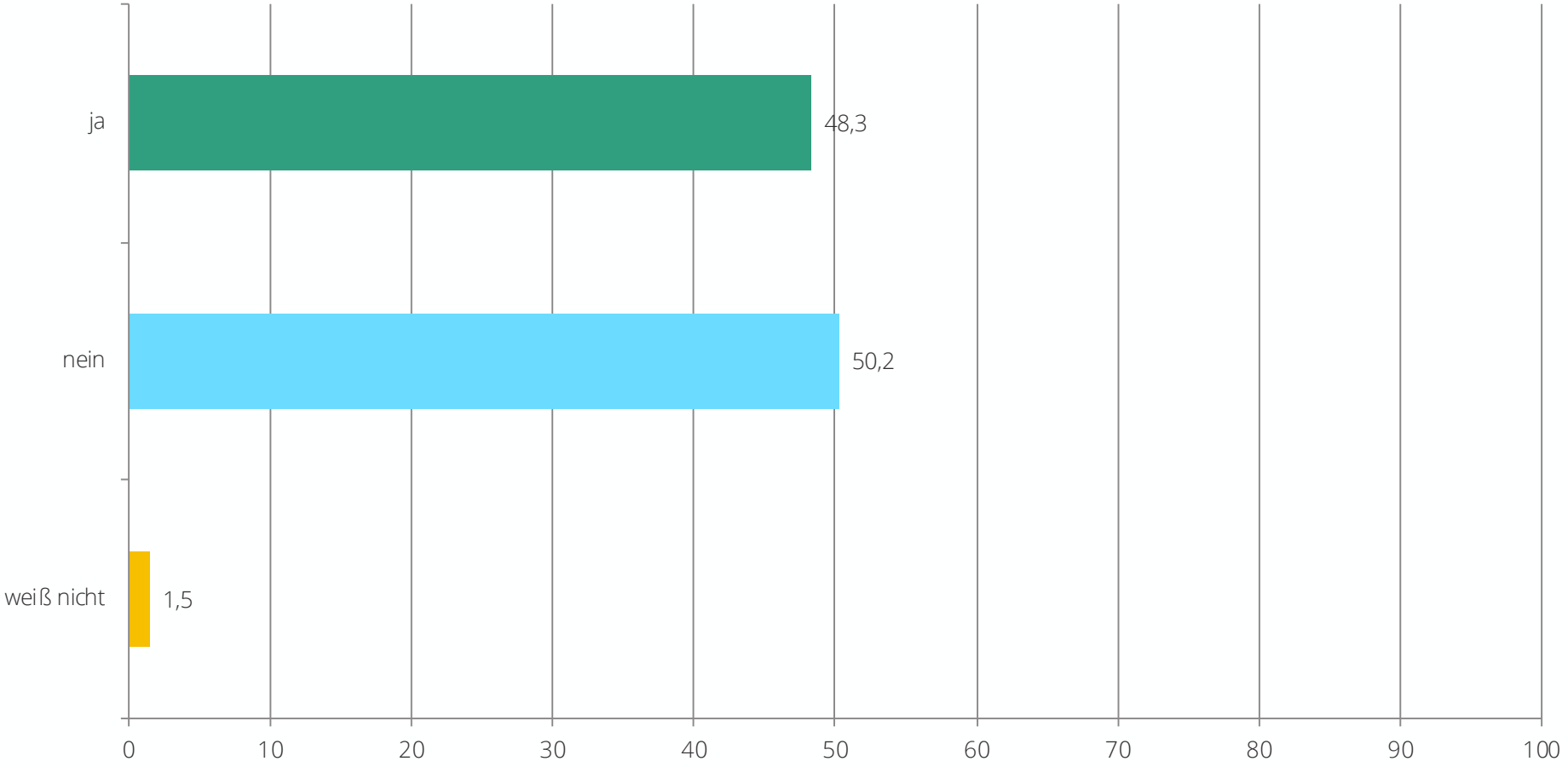
„Wie oft werden Passwörter in Ihrem Unternehmen geändert?“



In %, Einfachantwort, n=205

SPAM Problematik

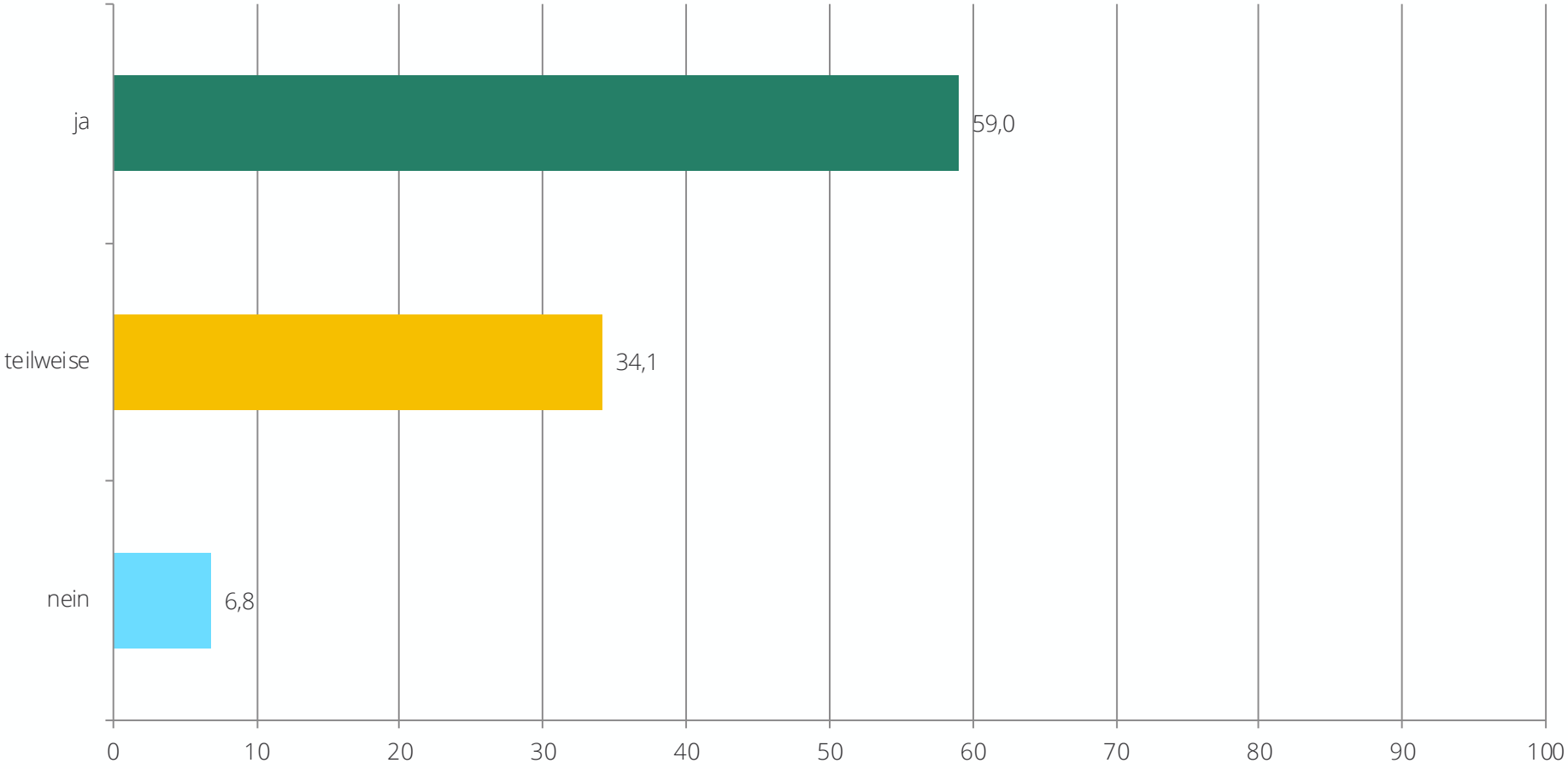
„Leiden Sie bzw. Ihre Mitarbeiter unter SPAM-E-Mail Nachrichten?“



In %, Einfachantwort, n=205

Umsetzung von Maßnahmen der DSGVO (1/5)

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

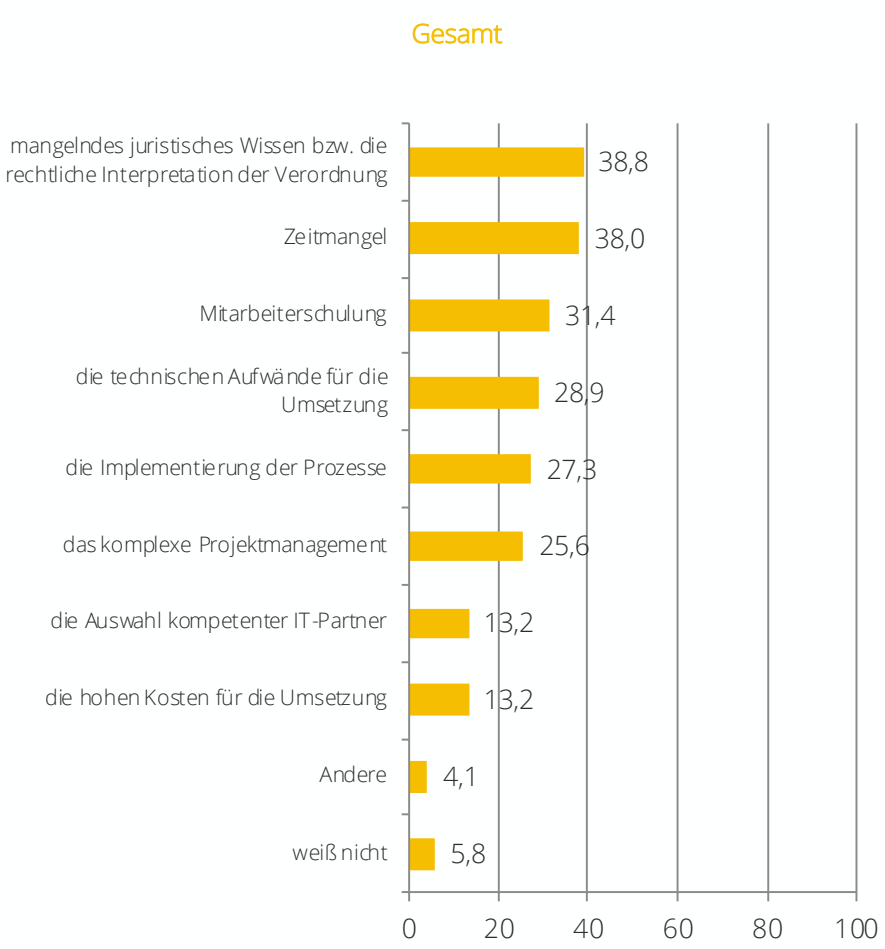


In %, Einfachantwort, n=205

Umsetzung von Maßnahmen der DSGVO (2/5)

„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
26,7	42,0	43,9	30,8	51,4	53,8	20,6
36,7	38,0	39,0	30,8	42,9	50,0	29,4
33,3	48,0	9,8	3,8	20,0	50,0	50,0
26,7	40,0	17,1	11,5	31,4	34,6	35,3
23,3	42,0	12,2	15,4	20,0	46,2	29,4
16,7	36,0	19,5	15,4	28,6	30,8	26,5
13,3	20,0	4,9	0,0	11,4	15,4	23,5
6,7	18,0	12,2	7,7	8,6	19,2	17,6
0,0	2,0	9,8	15,4	2,9	0,0	0,0
10,0	0,0	9,8	11,5	5,7	0,0	5,9

In %, Mehrfachantworten, n=121

Umsetzung von Maßnahmen der DSGVO (3/5)

„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:

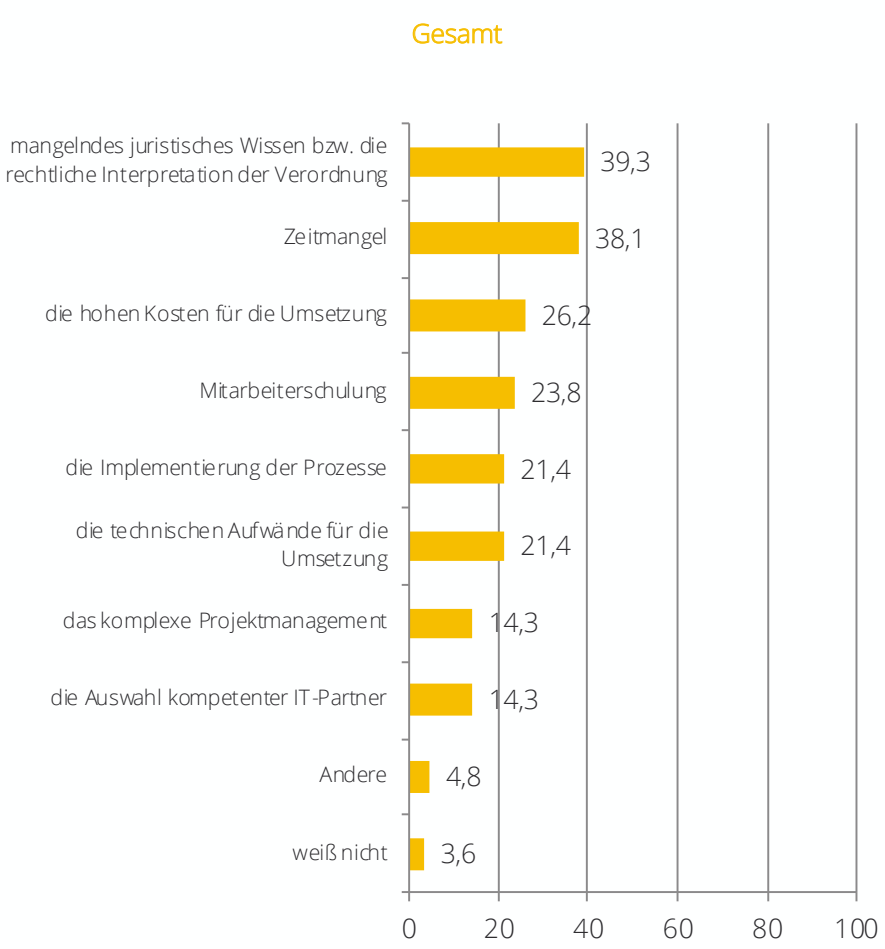
- Die hysterische Bewerbung durch profitgierige Rechtsanwälte
- Fehlinformationen von allen Seiten sogar von der WK
- Hab das meinen web Administrator machen lassen
- Ich speichere keinerlei Daten mehr
- Keine

Originalnennungen, n=121

Umsetzung von Maßnahmen der DSGVO (4/5)

„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
33,3	16,7	55,6	53,6	40,9	30,8	23,8
26,7	44,4	44,4	46,4	50,0	23,1	23,8
33,3	33,3	16,7	10,7	36,4	30,8	33,3
36,7	44,4	2,8	0,0	31,8	38,5	38,1
20,0	11,1	27,8	25,0	18,2	7,7	28,6
6,7	33,3	27,8	28,6	22,7	15,4	14,3
20,0	22,2	5,6	0,0	13,6	30,8	23,8
20,0	5,6	13,9	10,7	18,2	15,4	14,3
0,0	0,0	11,1	10,7	4,5	0,0	0,0
0,0	5,6	5,6	7,1	0,0	7,7	0,0

In %, Mehrfachantworten, n=84

Umsetzung von Maßnahmen der DSGVO (5/5)

„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.

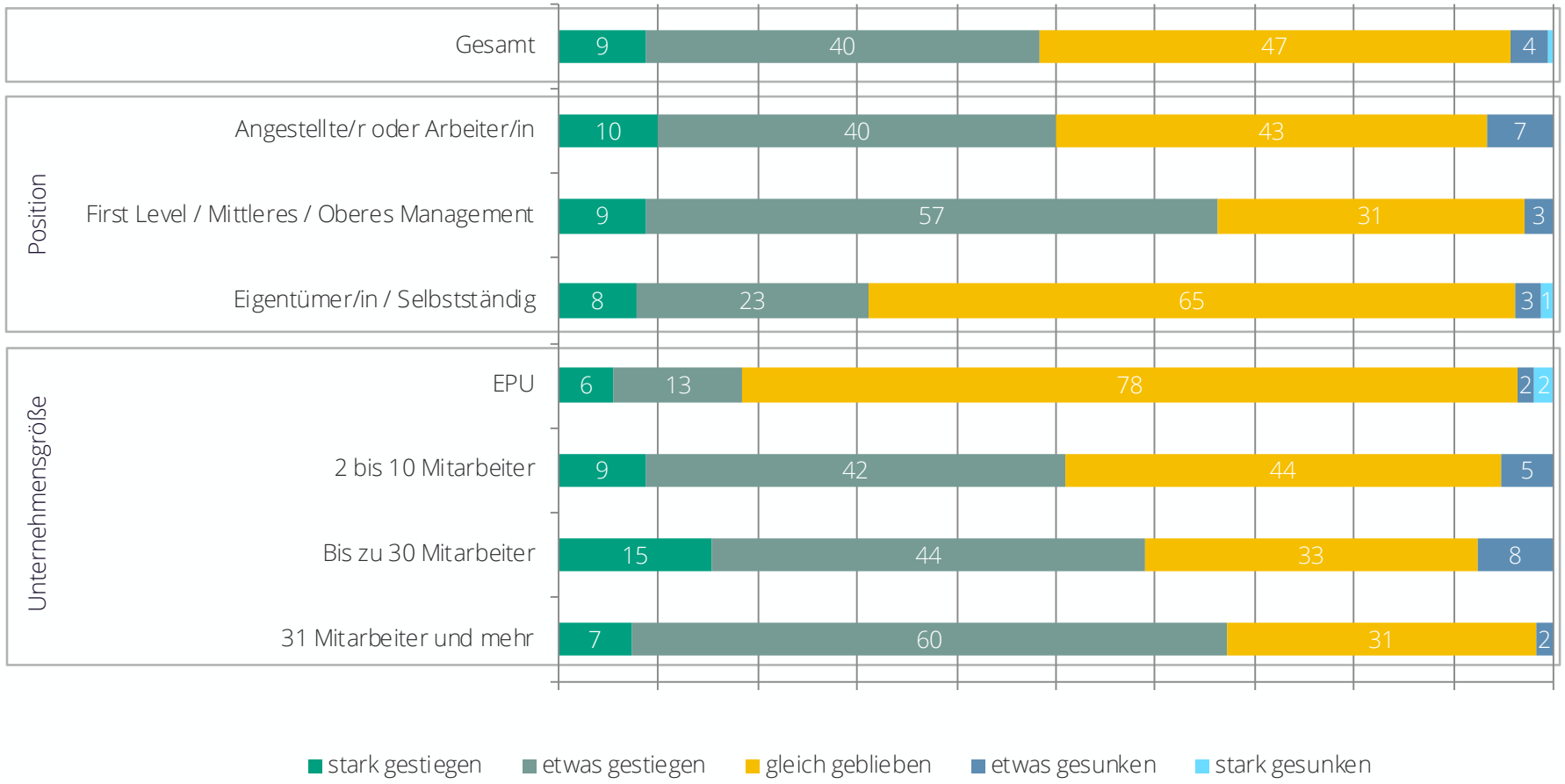
Sonstiges:

- Einiges davon ist echt unnütz
- Habe keine Mitarbeiter
- Ich stehe lediglich mit Selbständigen und Unternehmen in Kontakt
- Nicht notwendig

Originalnennungen, n=84

Veränderung des IT-Budgets im letzten Jahr

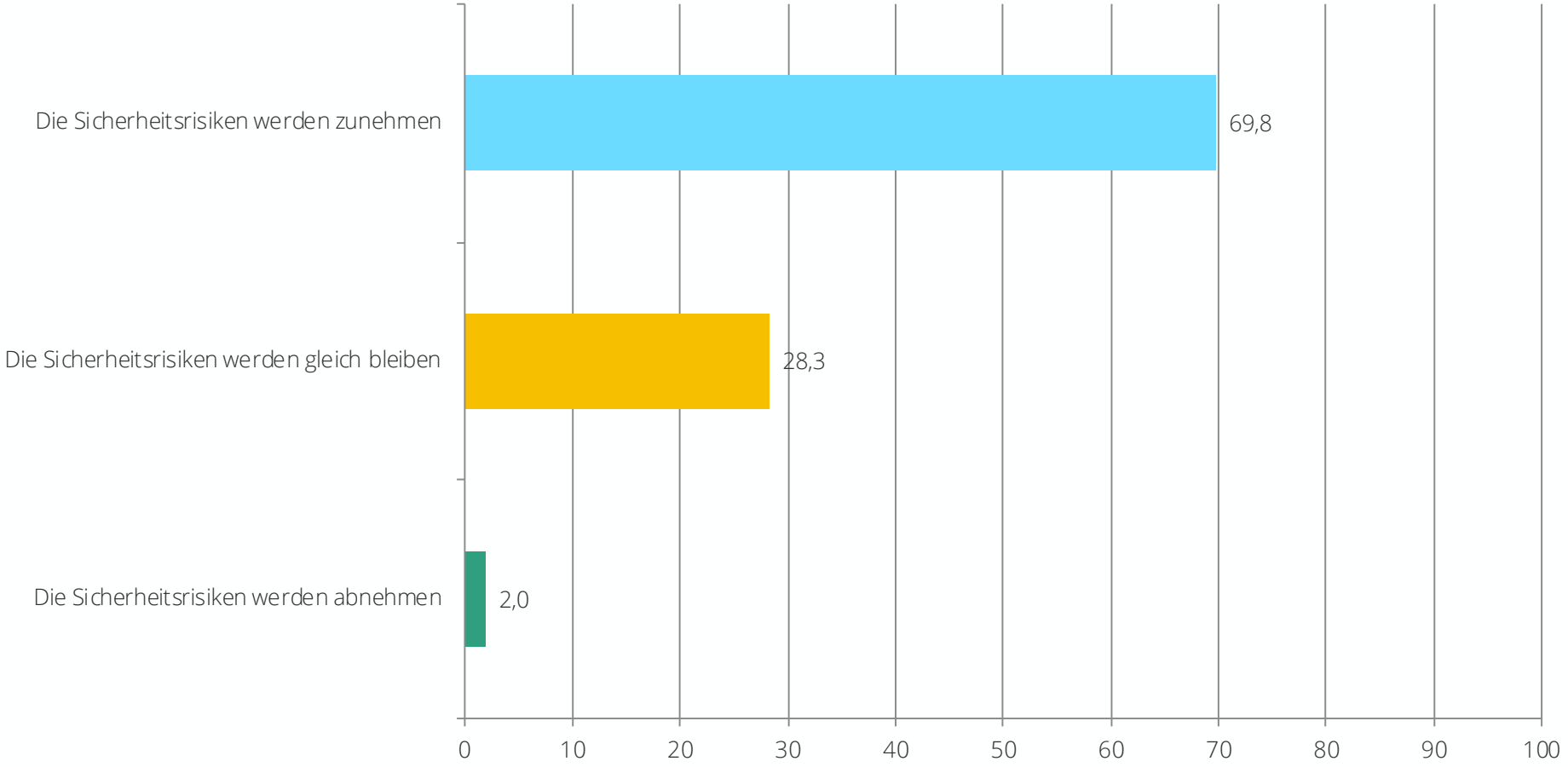
„Wie hat sich das IT-Budget in Ihrem Unternehmen im Vergleich zum Vorjahr verändert?“



In %, Einfachantwort, n=205

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?“



In %, Einfachantwort, n=205

Zusammenfassung

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 52% für „mehrmals pro Tag“ relativ hoch ein. Weitere 35% nehmen an, dass diese Angriffe „mehrmals pro Monat“ passieren.
- Mit 62% bzw. 58% sind „Virenangriffe“ und „Ausfälle von IT-Systemen“ die größten Bedenken der Befragten im Bereich IT-Security, gefolgt von „Datenschutzrechtlichen Problemen“ mit 45%, „Änderung oder Löschung von Daten“ mit 42% und das „ Stehlen von wichtigen Daten durch externe Personen“ mit 39%.

Status und Veränderung der Wichtigkeit von IT-Security in Unternehmen

- Mit einem Mittelwert von 1,95 (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 1,56) ist dieser Stellenwert höher als in EPUs (MW 2,35).
- In den letzten zwei Jahren ist das Thema IT-Security auch immer wichtiger geworden. 62% 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.

Einschätzung des bestehenden Schutzes

- 59% der Befragten sind der Annahme, dass ihr Unternehmen „(sehr) gut“ (Top2Box) vor internen und externen Angriffen und Datenverlusten geschützt ist.

Zusammenfassung (2/5)

IT-Security Vorfälle in den letzten 2 Jahren

- In den letzten 2 Jahren gab es in 34% der befragten Unternehmen IT-Security Vorfälle. Unter „Eigentümern/Selbstständigen" gab es mit 14% vergleichsweise weniger Vorfälle als unter „Angestellten/Arbeitern" mit 47%. Auch bei den EPUs gab es weniger Vorfälle mit 13% als in größeren Unternehmen mit mehr als 30 Mitarbeitern (60%).
- Bei den Vorfällen kam es meist mit 61% zu „Virenangriffen", „Problemen durch Spam" (46%) und zu „Ausfällen von IT-Systemen" (39%) oder zur „Änderung oder Löschung von Daten" (22%).

Ursachen für IT-Security Vorfälle in den letzten 2 Jahren

- Als Ursachen für IT-Security Vorfälle werden mit 45% vor allem ein „Ausfall der Technik" und mit 41% „Hackerangriffe" genannt. „Irrtum oder Unwissen von Mitarbeitern" wird von 35% der Befragten als Ursache genannt.

IT-Security Audits

- In gut der Hälfte aller befragten Unternehmen (52%) werden regelmäßig, wiederkehrende IT-Security Audits durchgeführt, um interne Schwachstellen, Konzeptions- und Konfigurationsfehler aufzuzeigen. Unter den Eigentümern/Selbständigen geben nur 35% an, dass IT-Security Audits regelmäßig durchgeführt werden. Der Anteil ist bei größeren Unternehmen mit mehr als 30 Mitarbeitern höher (82%).

Zusammenfassung (3/5)

- In jenen Unternehmen, wo nicht regelmäßig IT-Security Audits durchgeführt werden, wird mit 45% als häufigster Grund die „fehlende Erfahrung / Kompetenz“ angeführt, gefolgt vom „Kostenfaktor “ mit 33%. Als weiterer Grund für das Ausbleiben von regelmäßigen IT-Security Audits wird mit 32% die „Nicht-Notwendigkeit “ genannt.

Hemmnisse bei der Verbesserung der IT-Security

- Der „Kostenfaktor“ (45%) und die „fehlende Erfahrung / Kompetenz“ (40%) sehen die Befragten als Hauptgründe, die einer Verbesserung der IT-Security entgegenwirken. Weiters werden „Personalmangel“ (23%) und „Zeitmangel“ (22%) als Hemmnisse genannt. Die „fehlende Akzeptanz“ wird von 15% der Befragten angegeben, wobei dieser Faktor von Eigentümern/Selbständigen (1%) sehr selten genannt wird.

Vertrauen auf externe Fachkompetenz

- 85% der Befragten würden auf „externe(s) Fachkompetenz / Wissen“ vertrauen, um Sicherheitslücken im IT-Bereich aufzudecken bzw. beheben zu lassen.

Bevorzugte Settings für IT-Infrastruktur und Standorte für die Cloud

- 42% der Befragten bevorzugen eine „IT Infrastruktur und Betrieb vor Ort“ und 36% nutzen lieber eine „Privat Cloud“. „Hybrid Clouds“ und „Public Clouds“ werden vergleichsweise eher ungern genutzt (je 10-11%).
- In Bezug auf den Standort für die Cloud wird eine österreichische Cloud mit 60% bevorzugt. 26% würden eine europäische Cloud bevorzugen und nur 7% eine deutsche Cloud.

Zusammenfassung (4/5)

Status der Digitalisierung im Unternehmen

- 24% der Befragten würden den aktuellen Status der Digitalisierung in Ihrem Unternehmen mit folgenden Worten beschreiben „Wir probieren Dinge aus und lernen dabei“. Jeweils 19% würden eher sagen, dass sie „strategisch in die Digitalisierung investieren“ bzw. „gerade erst damit starten“.

Backups und Änderung von Passwörtern

- 78% 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 69% an, dass sie Backups auch außerhalb der Räumlichkeiten ihres Unternehmens aufbewahren und 51% 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.
- Bei mehr als der Hälfte der befragten Unternehmen (54%) werden Passwörter zumindest „alle 4-5 Monate“ geändert. 36% davon ändern ihre Passwörter im Unternehmen sogar „alle 1-2 Monate“ oder öfters.

SPAM Problematik

- Zum Thema SPAM Problematik geben 48% 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 (59%) haben die technischen und organisatorischen Maßnahmen der DSGVO bereits umgesetzt und weitere 34% zumindest teilweise.
- Für jene Unternehmen, die diese Maßnahmen bereits umgesetzt haben, waren die größten Herausforderungen dabei „ das mangelnde juristische Wissen bzw. die rechtliche Interpretation der Verordnung“ (36%), „Zeitmangel“ (38%) sowie “Mitarbeiterschulungen“ (31%) und die „technischen Aufwände für die Umsetzung“ (29%). Personen in Management-Positionen nennen “Mitarbeiterschulungen“ noch häufiger als größte Herausforderung (48%), für EPUs war dies natürlich weniger relevant (4%) als für größere Unternehmen.
- Jene Unternehmen, die die Maßnahmen der DSGVO erst teilweise oder noch nicht umgesetzt haben, sehen dabei die größten Hindernisse wiederum im „ mangelnden juristischen Wissen bzw. der rechtlichen Interpretation der Verordnung“ (39%) und im „ Zeitmangel “ (38%).

Veränderung des IT-Budgets im letzten Jahr

- In den meisten der befragten Unternehmen (47%) ist das IT-Budget im Vergleich zum Vorjahr „gleich geblieben“, bei 40% 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 2% sprechen von einer Abnahme der Sicherheitsrisiken.

KONTAKT

techbold technology group AG
Dresdner Str. 89
1200 Wien

FBNr.: 436735 h
UID: ATU69951457

Tel: +43 59 555
Fax: +43 59 555 – 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