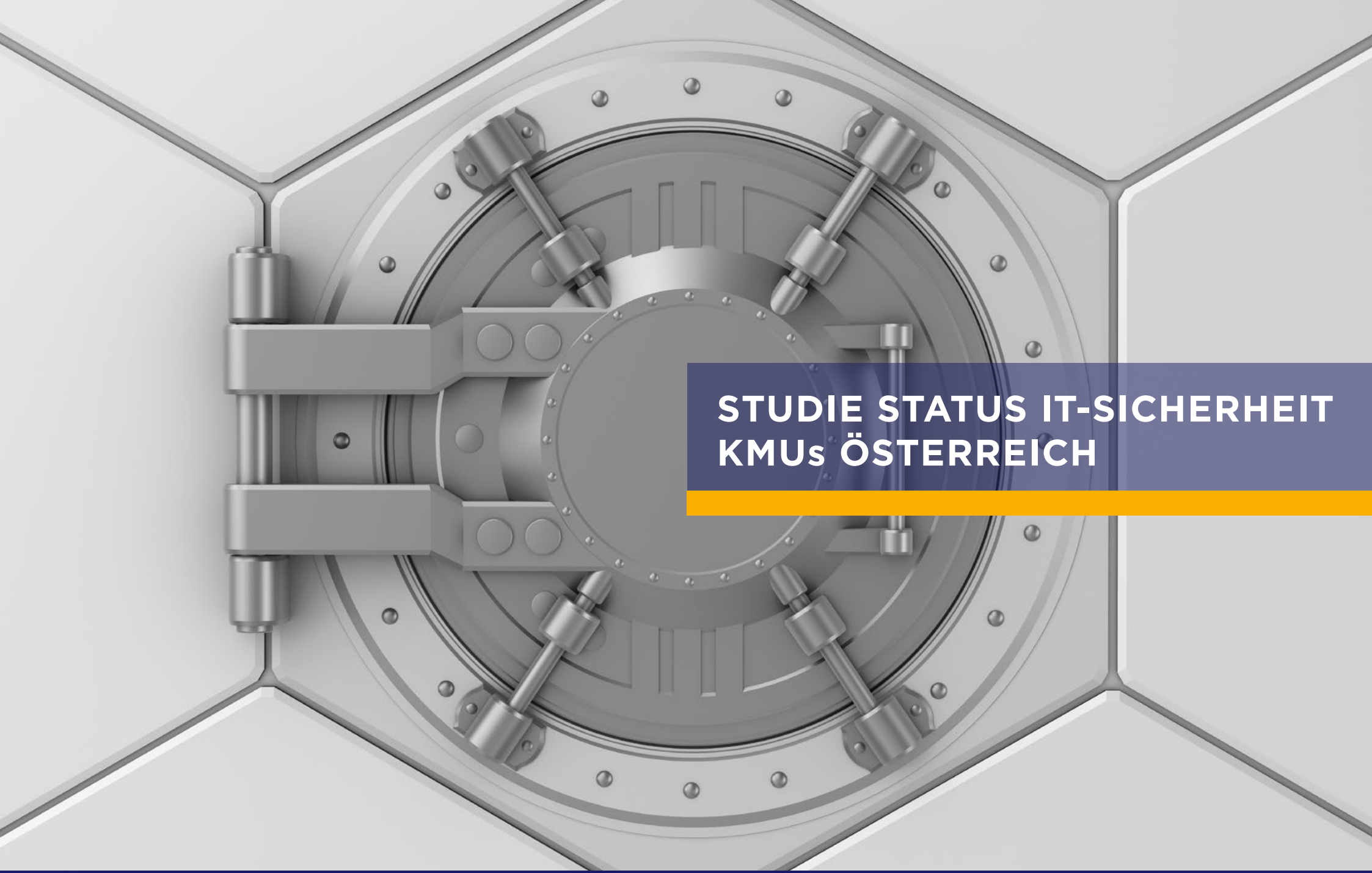


STUDIE STATUS IT-SICHERHEIT KMUs ÖSTERREICH

techbold

mindtake RESEARCH

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

MindTake Research GmbH
Wien, 3. August 2016

EINLEITUNG

- Eckdaten der Befragung
- Beschreibung der Stichprobe

ECKDATEN DER BEFRAGUNG

- **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:

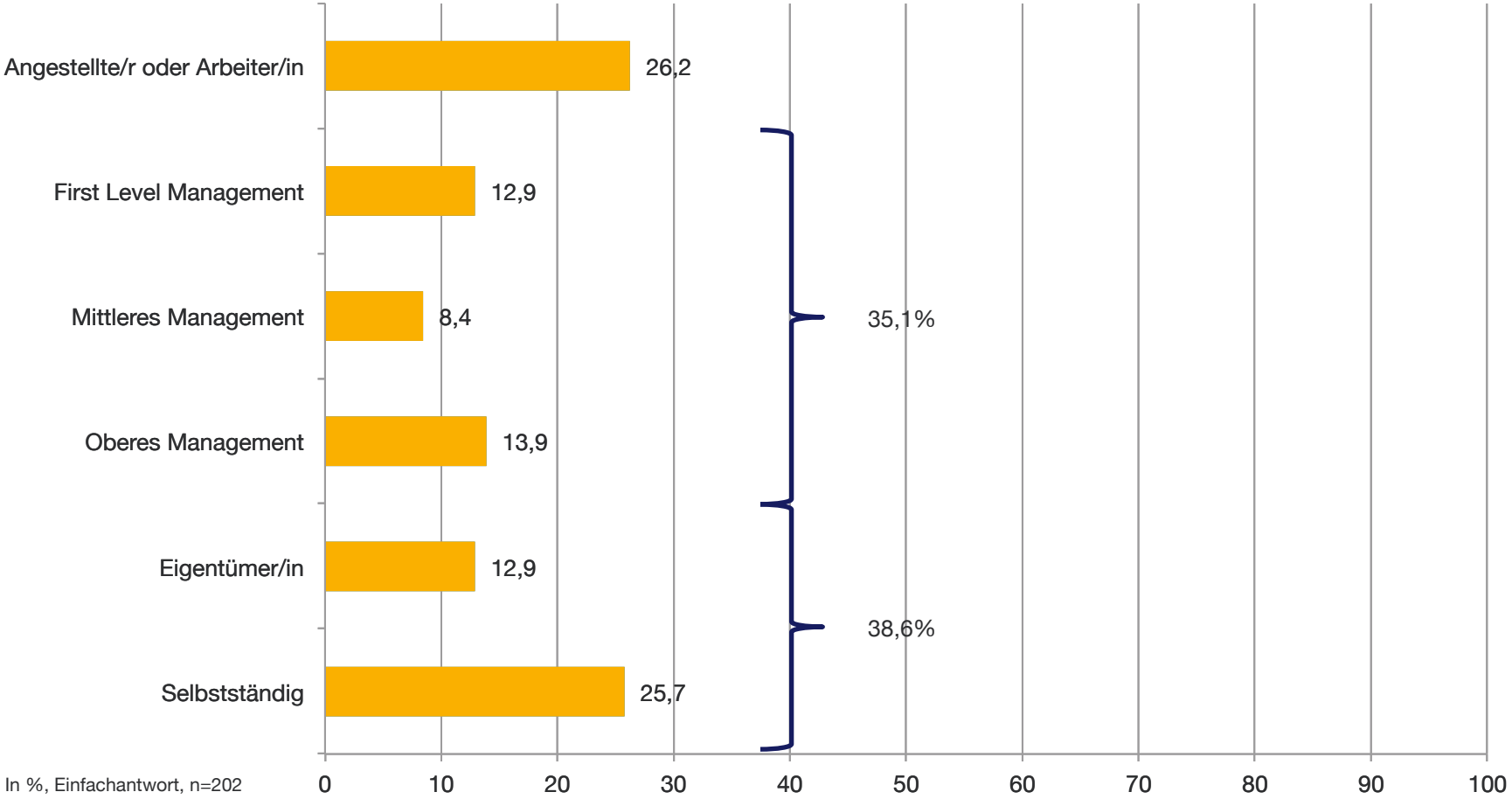
  - Ermittlung des IST Zustandes des IT-Sicherheitsmanagements, sowie der Sicherheit der IT-Infrastruktur
  - Identifikation von kritischen Bereichen mit der Zielsetzung der Sensibilisierung der betroffenen Unternehmen

- **Eckdaten der Studie**

  - **Erhebungsmethode:** Computer Assisted Web Interviews (CAWI) im Talk Online-Panel und Computer Assisted Telephone Interviews (CATI) von telemark Marketing
  - **Zielgruppe:** IT-Entscheider in KMUs (bis 250 Mitarbeiter) in den Branchen produzierendes Gewerbe, Handel und Dienstleistung
  - **Stichprobengröße:** n=202
  - **Erhebungszeitraum:** 12.07.2016 – 29.07.2016
  - **Durchschnittliche Befragungsdauer (Median):** 5,16 Minuten

BESCHREIBUNG DER STICHPROBE

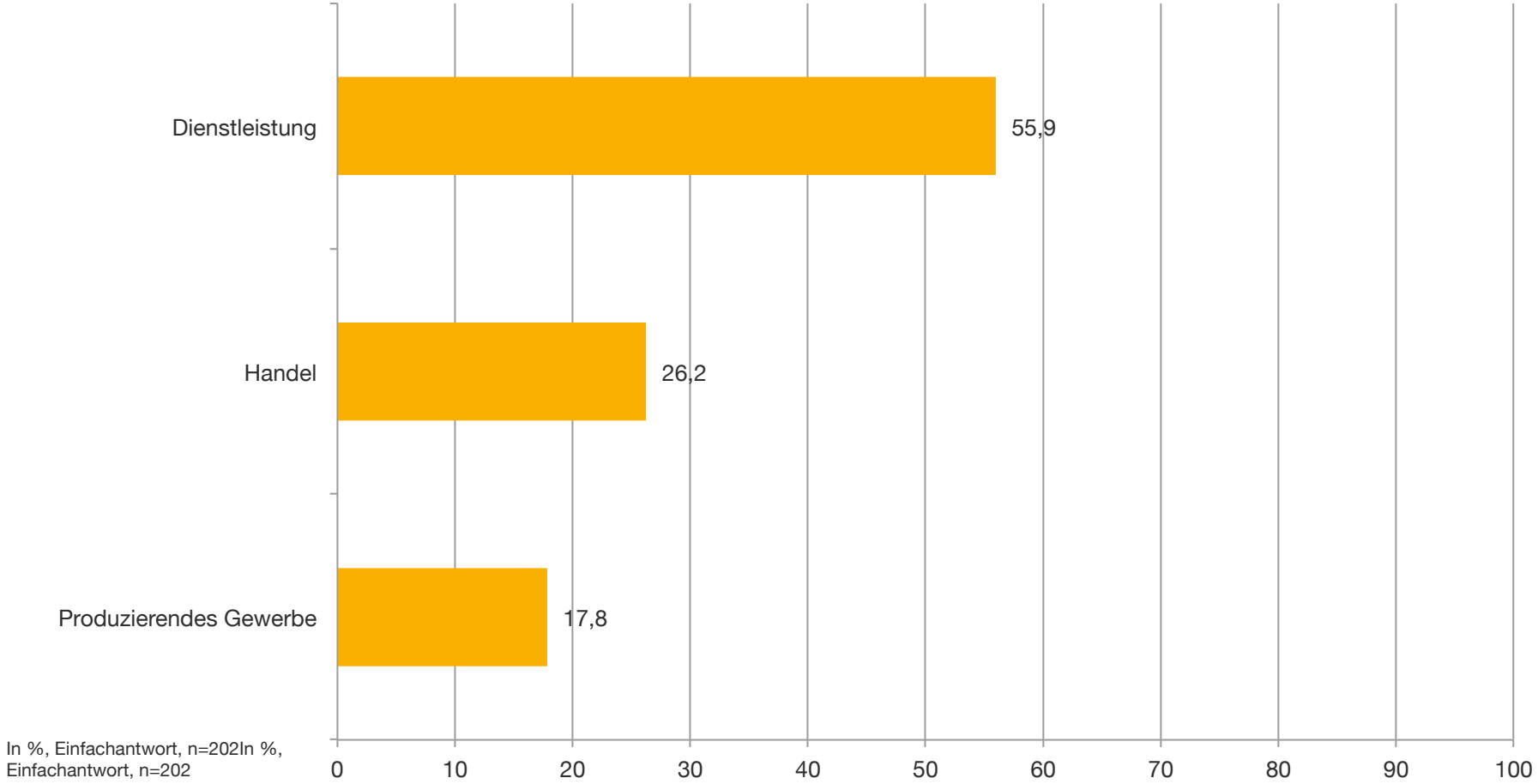
„In welcher Position sind Sie tätig?“



In %, Einfachantwort, n=202

BESCHREIBUNG DER STICHPROBE

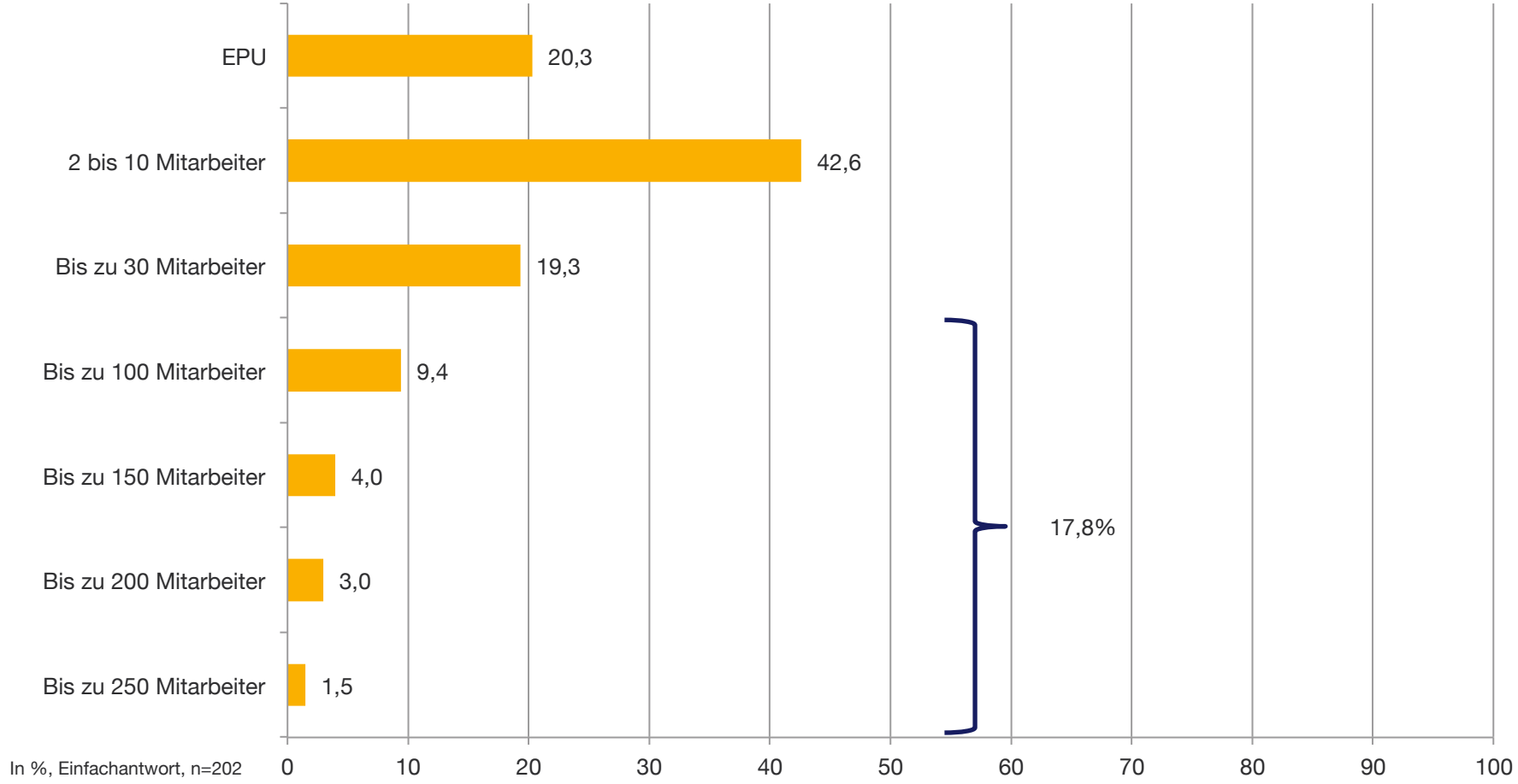
„In welcher Branche ist Ihr Unternehmen bzw. Arbeitgeber hauptsächlich tätig?“



In %, Einfachantwort, n=202In %, Einfachantwort, n=202

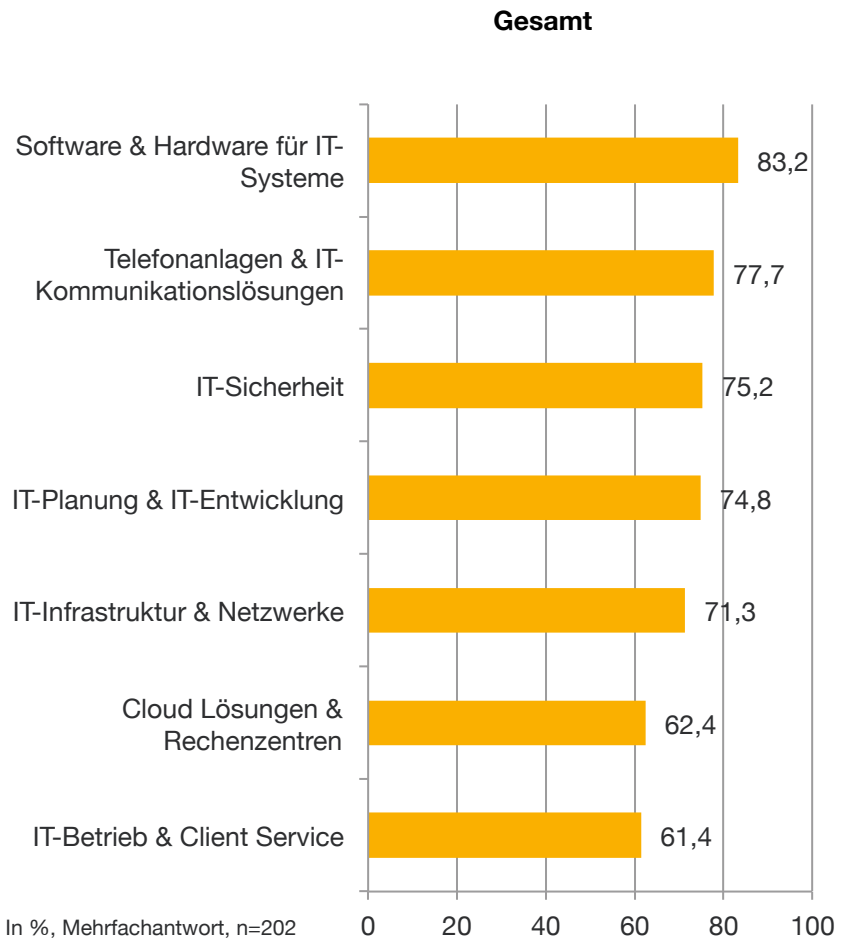
BESCHREIBUNG DER STICHPROBE

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



BESCHREIBUNG DER STICHPROBE

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



In %, Mehrfachantwort, n=202

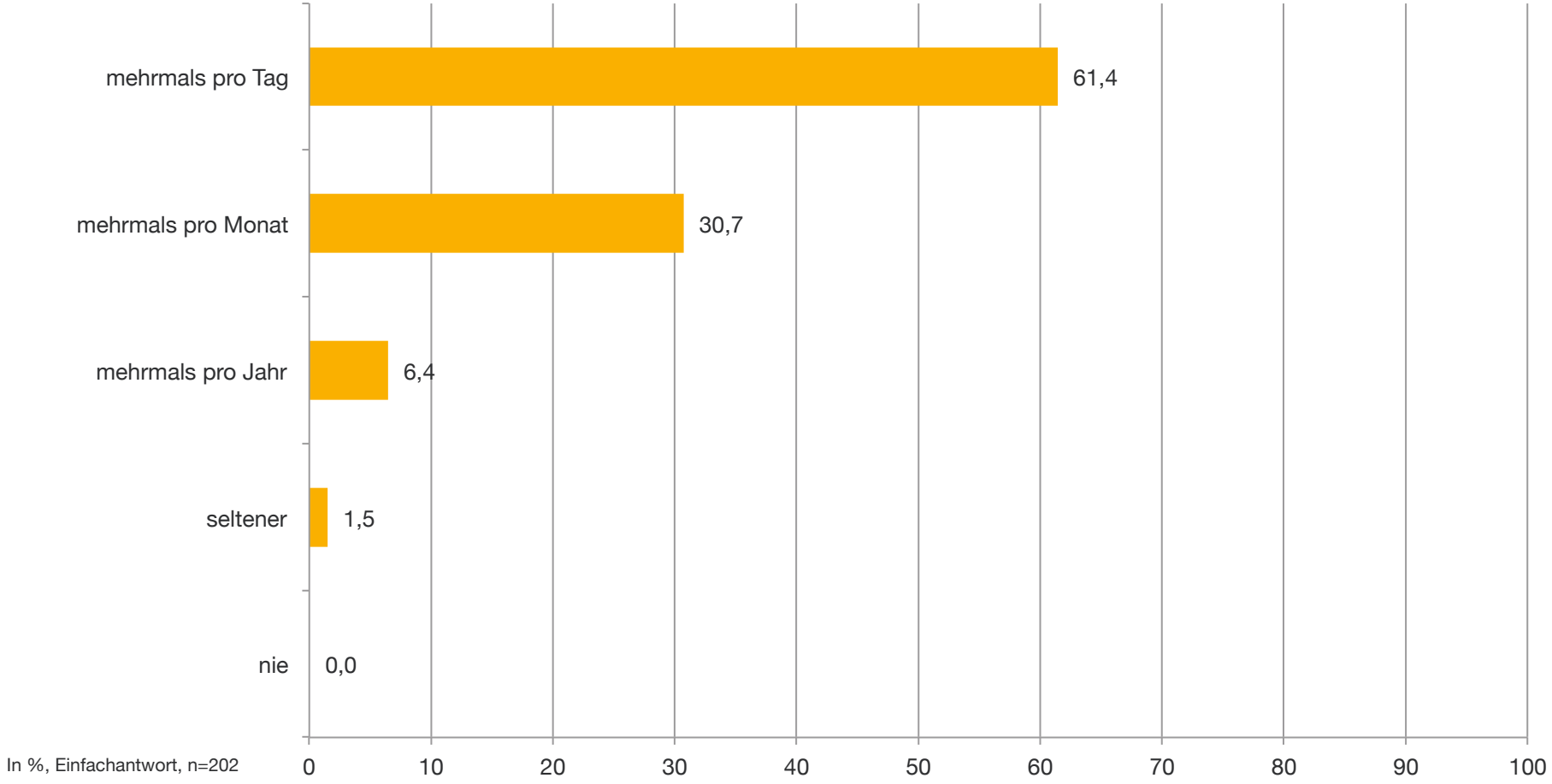
Position			Unternehmensgröße			
Angestellte/ Arbeiter	Manage-ment	Eigentümer/ Selbst-ständige	EPU	2 bis 10	11 bis 30	31 und mehr
66,0	87,3	91,0	92,7	81,4	82,1	77,8
64,2	76,1	88,5	80,5	80,2	84,6	61,1
64,2	74,6	83,3	80,5	77,9	76,9	61,1
67,9	76,1	78,2	80,5	77,9	79,5	55,6
54,7	70,4	83,3	80,5	75,6	64,1	58,3
45,3	64,8	71,8	73,2	67,4	51,3	50,0
50,9	59,2	70,5	75,6	64,0	51,3	50,0

= signifikant (p≤0,05)

ERGEBNISSE DER STUDIE

EINSCHÄTZUNG DER BEDROHUNGSLAGE

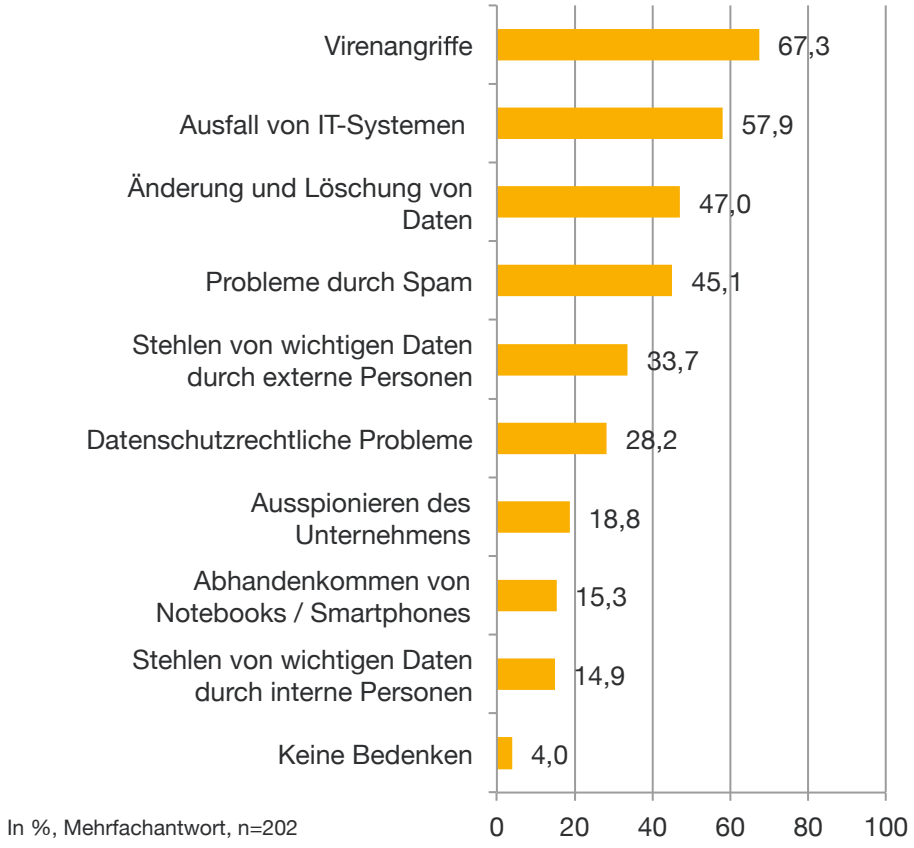
„Was schätzen Sie, wie oft werden österreichische Unternehmen im Durchschnitt (durch z.B. Hacker, Malware, Phishing, usw.) angegriffen?“



In %, Einfachantwort, n=202

BEDENKEN IM BEREICH IT-SECURITY

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



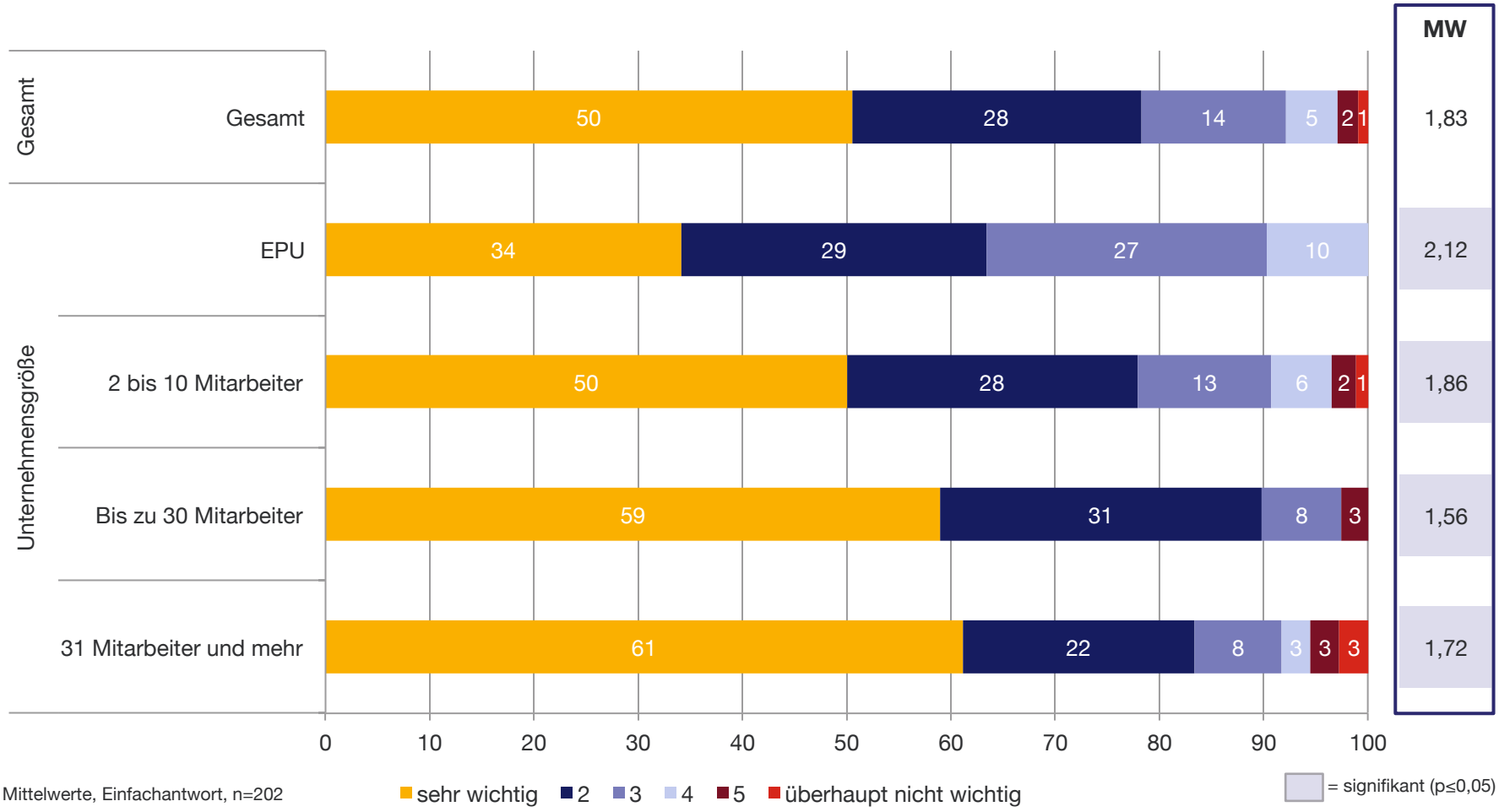
	Unternehmensgröße			
	EPU	2 bis 10	11 bis 30	31 und mehr
Virenangriffe	75,6	61,6	76,9	61,1
Ausfall von IT-Systemen	51,2	51,2	71,8	66,7
Änderung und Löschung von Daten	43,9	46,5	53,8	44,4
Probleme durch Spam	43,9	45,3	51,3	38,9
Stehlen von wichtigen Daten durch externe Personen	19,5	33,7	38,5	44,4
Datenschutzrechtliche Probleme	24,4	22,1	43,6	30,6
Ausspionieren des Unternehmens	9,8	18,6	20,5	27,8
Abhandenkommen von Notebooks / Smartphones	14,6	9,3	25,6	19,4
Stehlen von wichtigen Daten durch interne Personen	4,9	7,0	20,5	38,9
Keine Bedenken	4,9	7,0	0,0	0,0

In %, Mehrfachantwort, n=202

= signifikant (p≤0,05)

WICHTIGKEIT VON IT-SECURITY IN UNTERNEHMEN

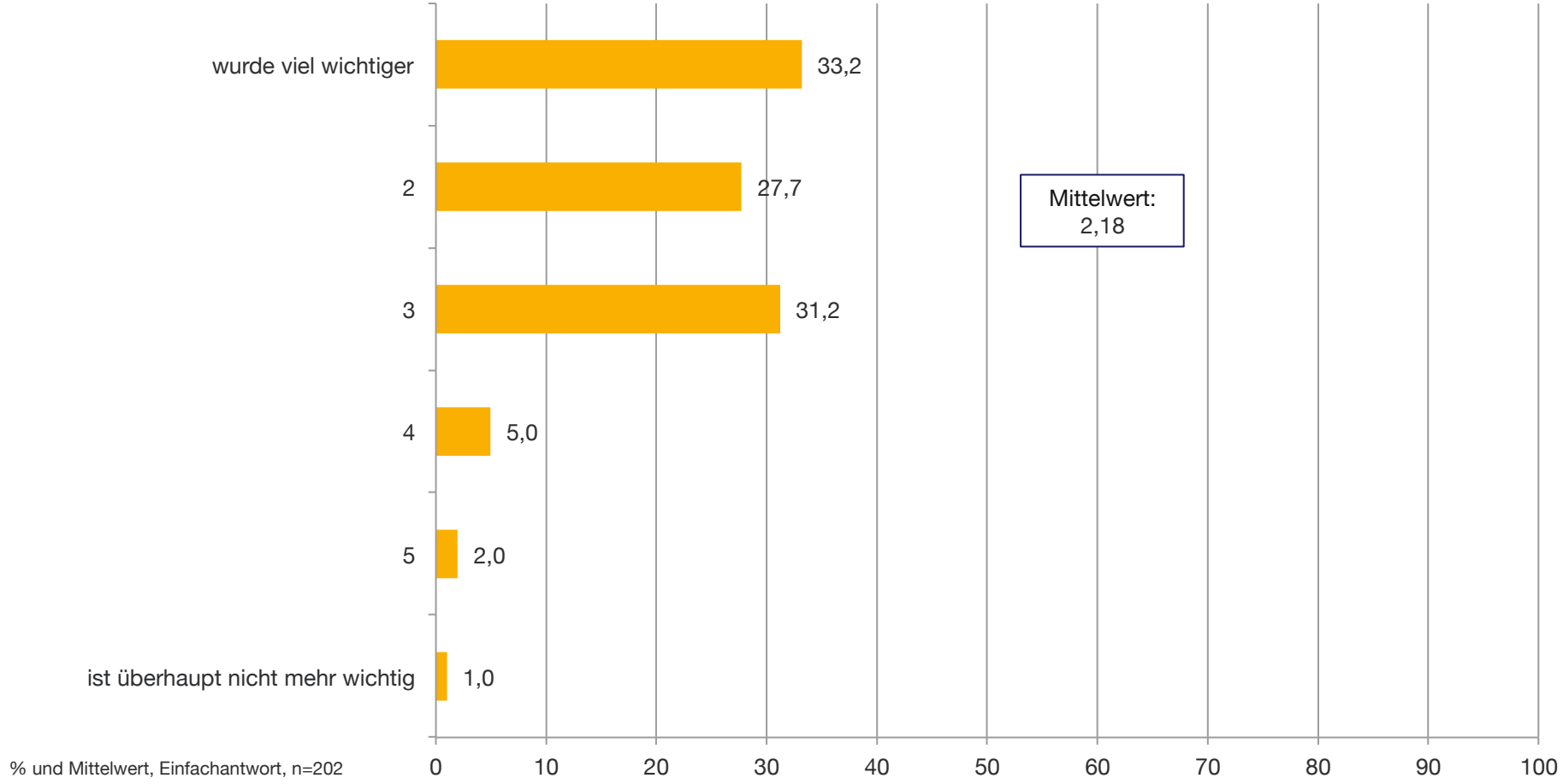
„Wie wichtig ist das Thema IT-Security innerhalb Ihres Unternehmens?"



In % und Mittelwerte, Einfachantwort, n=202

VERÄNDERUNG DER WICHTIGKEIT VON IT-SECURITY IN UNTERNEHMEN

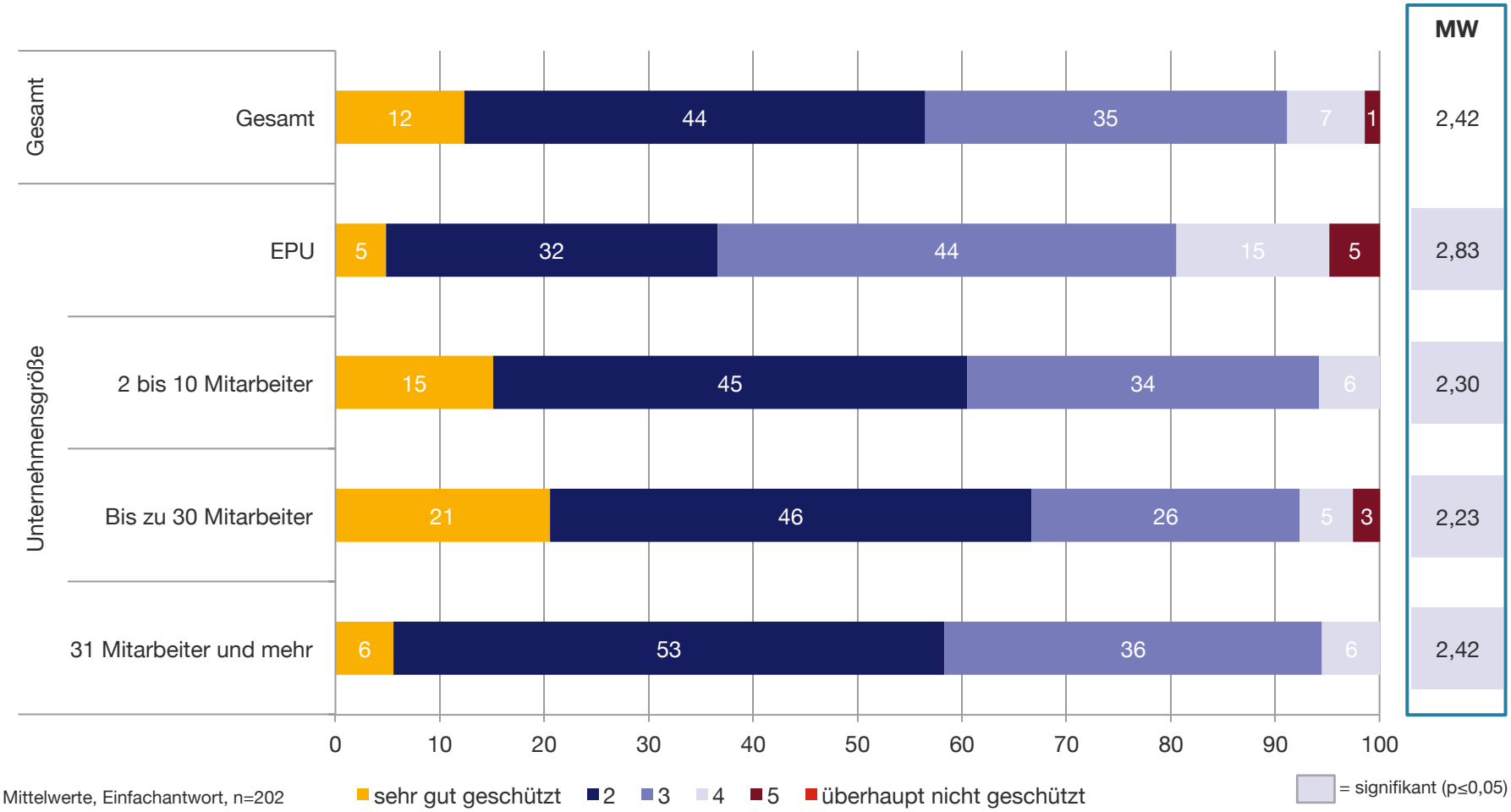
„Wie hat sich der Stellenwert der IT-Security in Ihrem Unternehmen in den letzten zwei Jahren verändert?“



% und Mittelwert, Einfachantwort, n=202

EINSCHÄTZUNG DES BESTEHENDEN SCHUTZES

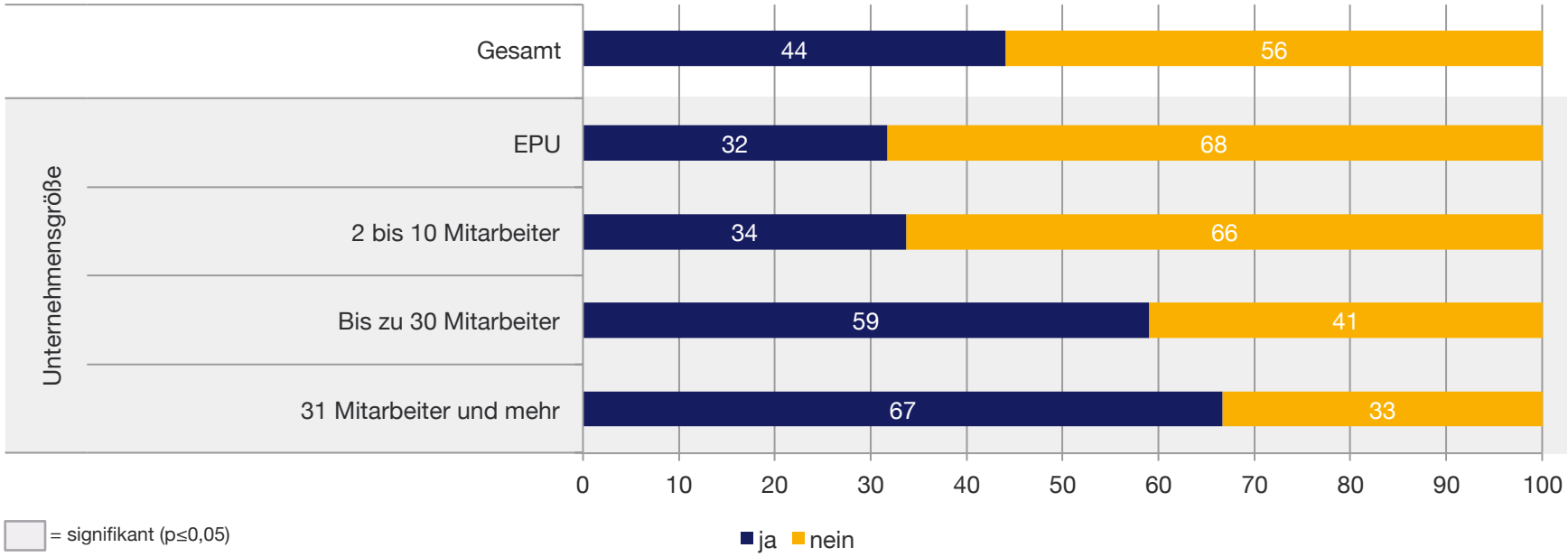
„Was denken Sie, wie gut ist Ihr Unternehmen vor internen und externen Angriffen und Datenverlust geschützt?“



% und Mittelwerte, Einfachantwort, n=202

IT-SECURITY-VORFÄLLE IN DEN LETZTEN 2 JAHREN

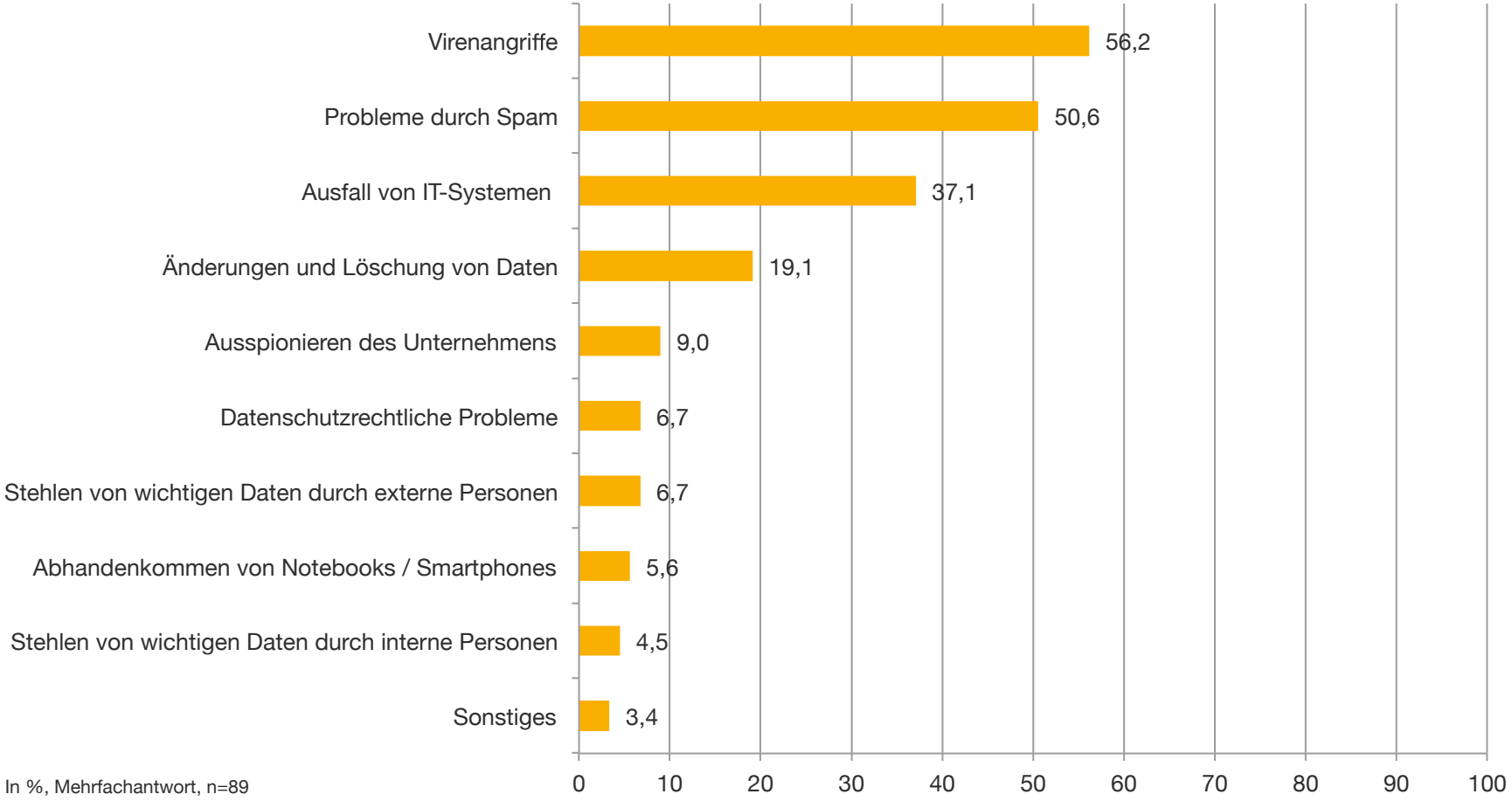
„Hat es in Ihrem Unternehmen in den letzten 2 Jahren einen IT-Security-Vorfall (wie z.B. Spamprobleme, Virenangriffe, Ausfall von IT-Systemen, Datenverlust, Datenänderung, usw.) gegeben?“



In %, Einfachantwort, n=202

ART DER IT-SECURITY VORFÄLLE IN DEN LETZTEN 2 JAHREN

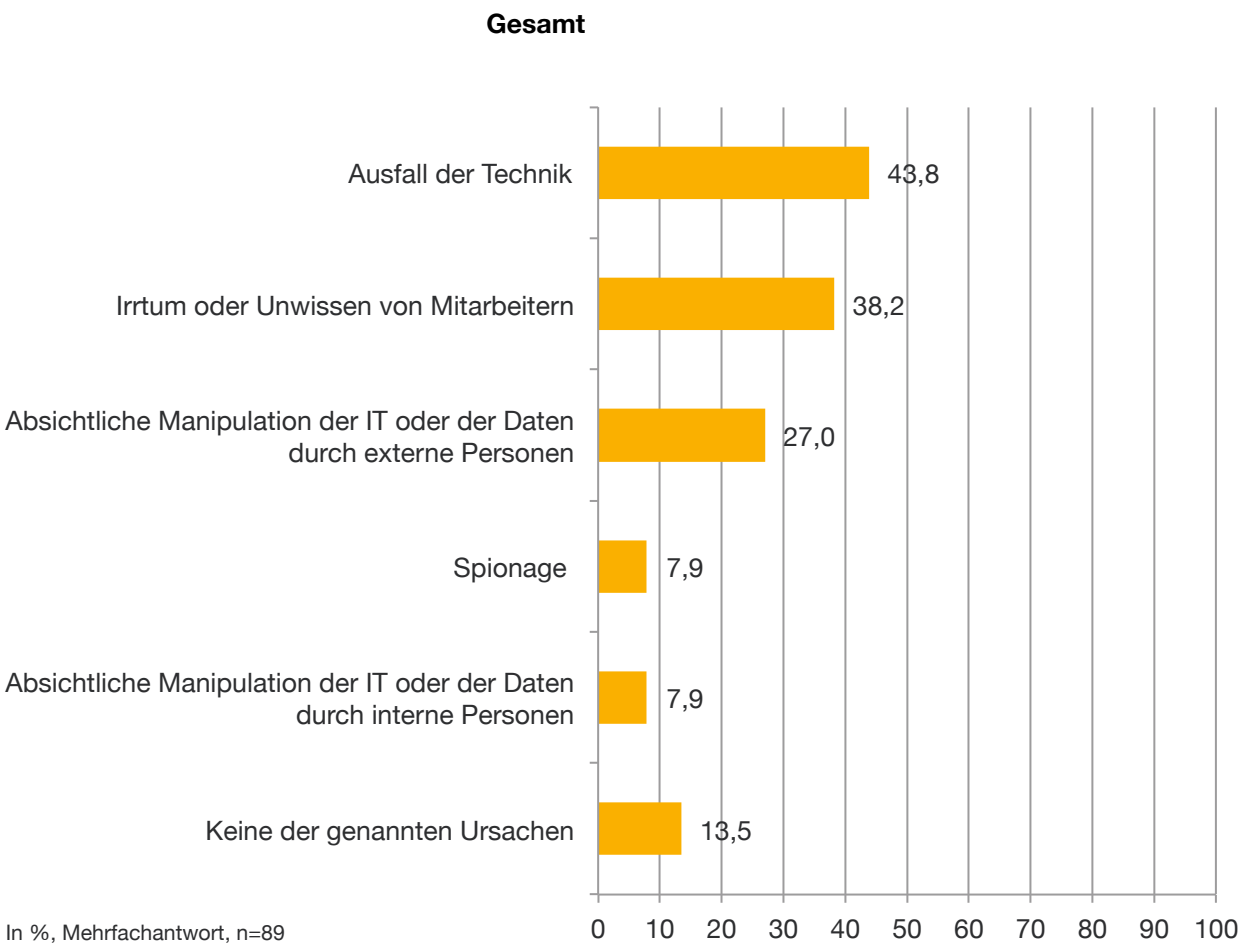
„Welche IT-Security-Vorfälle waren das?“
(Frage wurde nur jenen gestellt, in deren Unternehmen es einen IT-Security Vorfall in den letzten 2 Jahren gab.)



In %, Mehrfachantwort, n=89

URSACHEN FÜR IT-SECURITY-VORFÄLLE

„Und was waren die Ursachen für diese IT-Security-Vorfälle?“
(Frage wurde nur jenen gestellt, in deren Unternehmen es einen IT-Security Vorfall in den letzten 2 Jahren gab.)



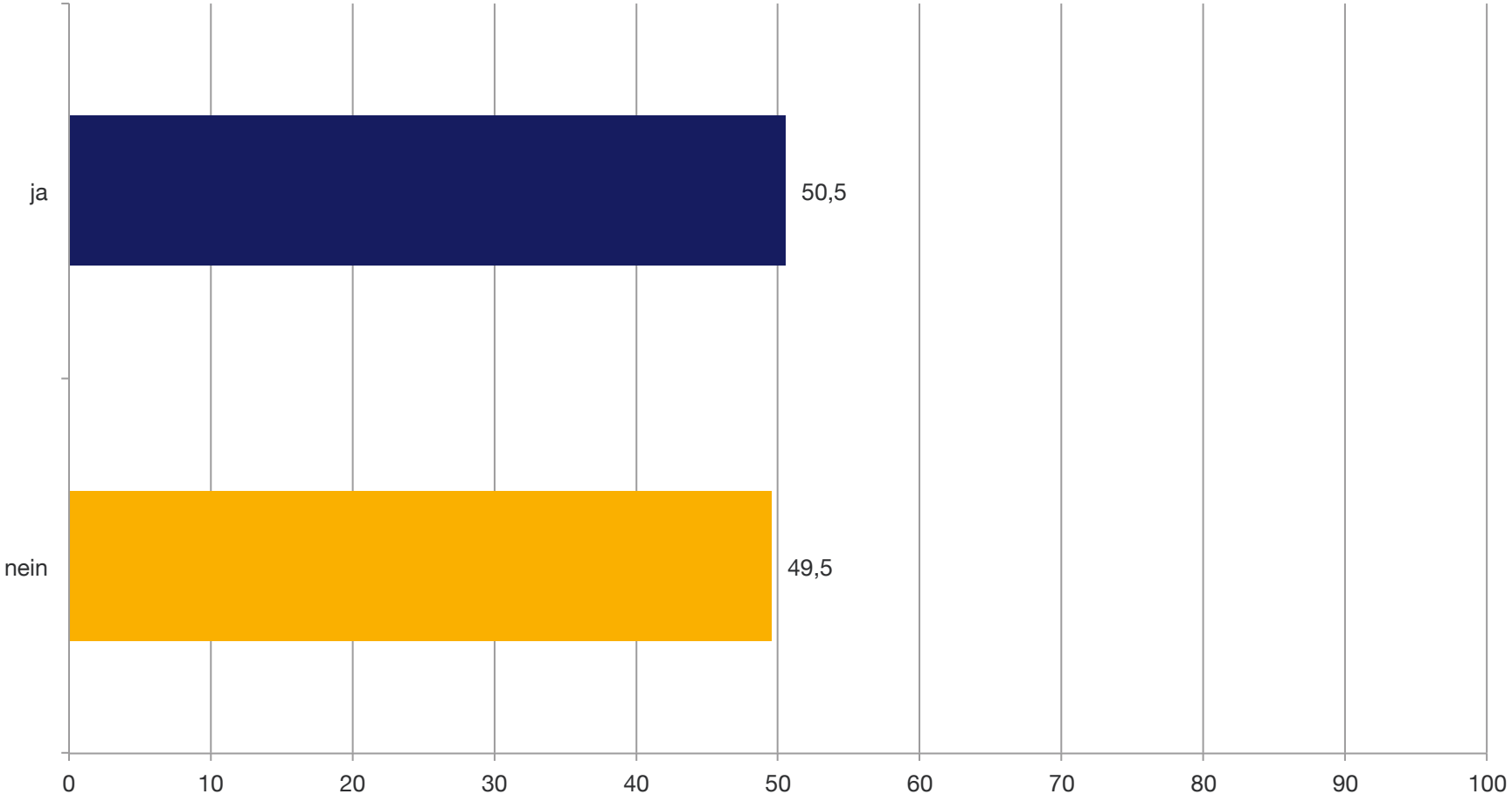
Unternehmensgröße		
Produzierendes Gewerbe	Handel	Dienstleistung
50,0	38,5	44,4
50,0	34,6	35,6
5,6	23,1	37,8
11,1	7,7	6,7
16,7	7,7	4,4
16,7	15,4	11,1

In %, Mehrfachantwort, n=89

= signifikant (p≤0,05)

REGELMÄSSIGKEIT VON IT-SECURITY AUDITS

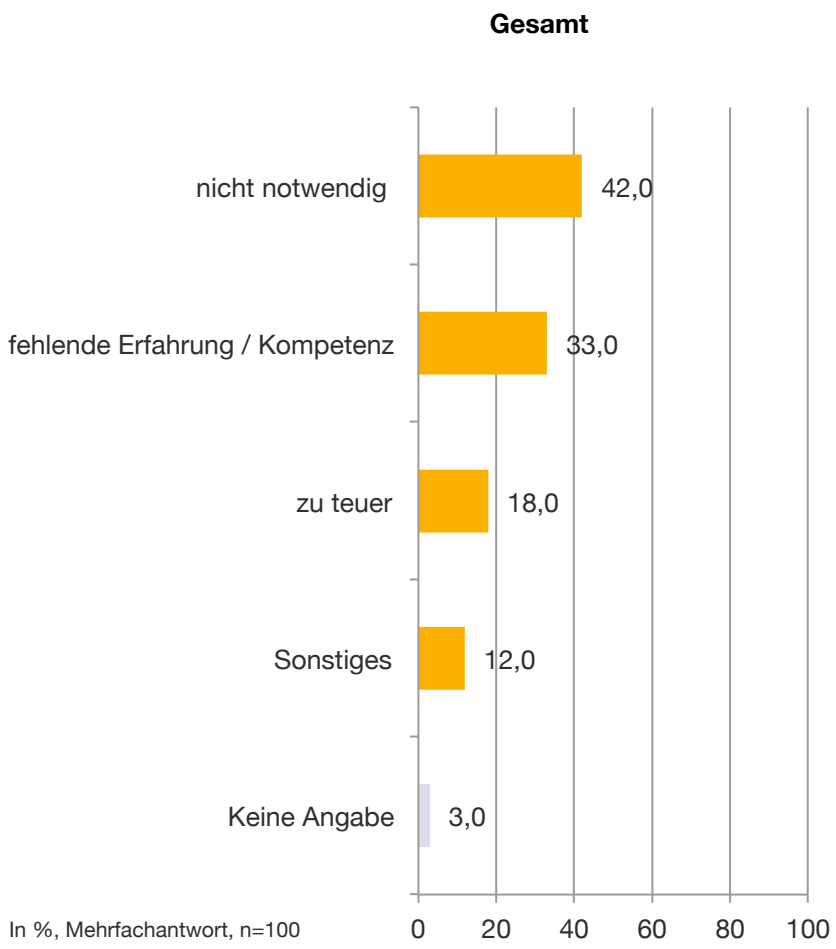
„Führen Sie regelmäßig, wiederkehrende IT-Security Audits durch, um interne und externe Schwachstellen, Konzeptions- und Konfigurationsfehler aufzuzeigen?“



In %, Einfachantwort, n=202

GRUND FÜR KEINE REGELMÄSSIGEN IT-SECURITY AUDITS (1/2)

„Warum werden in Ihrem Unternehmen nicht regelmäßig IT-Security Audits durchgeführt?“
(Frage wurde nur jenen gestellt, die keine regelmäßigen IT-Security Audits durchführen.)



Unternehmensgröße		
Produzierendes Gewerbe	Handel	Dienstleistung
18,2	51,9	47,1
45,5	29,6	29,4
27,3	7,4	19,6
18,2	7,4	11,8
4,5	7,4	0,0

In %, Mehrfachantwort, n=100

= signifikant (p≤0,05)

GRUND FÜR KEINE REGELMÄSSIGEN IT-SECURITY AUDITS (2/2)

„Warum werden in Ihrem Unternehmen nicht regelmäßig IT-Security Audits durchgeführt?“
(Frage wurde nur jenen gestellt, die keine regelmäßigen IT-Security Audits durchführen.)

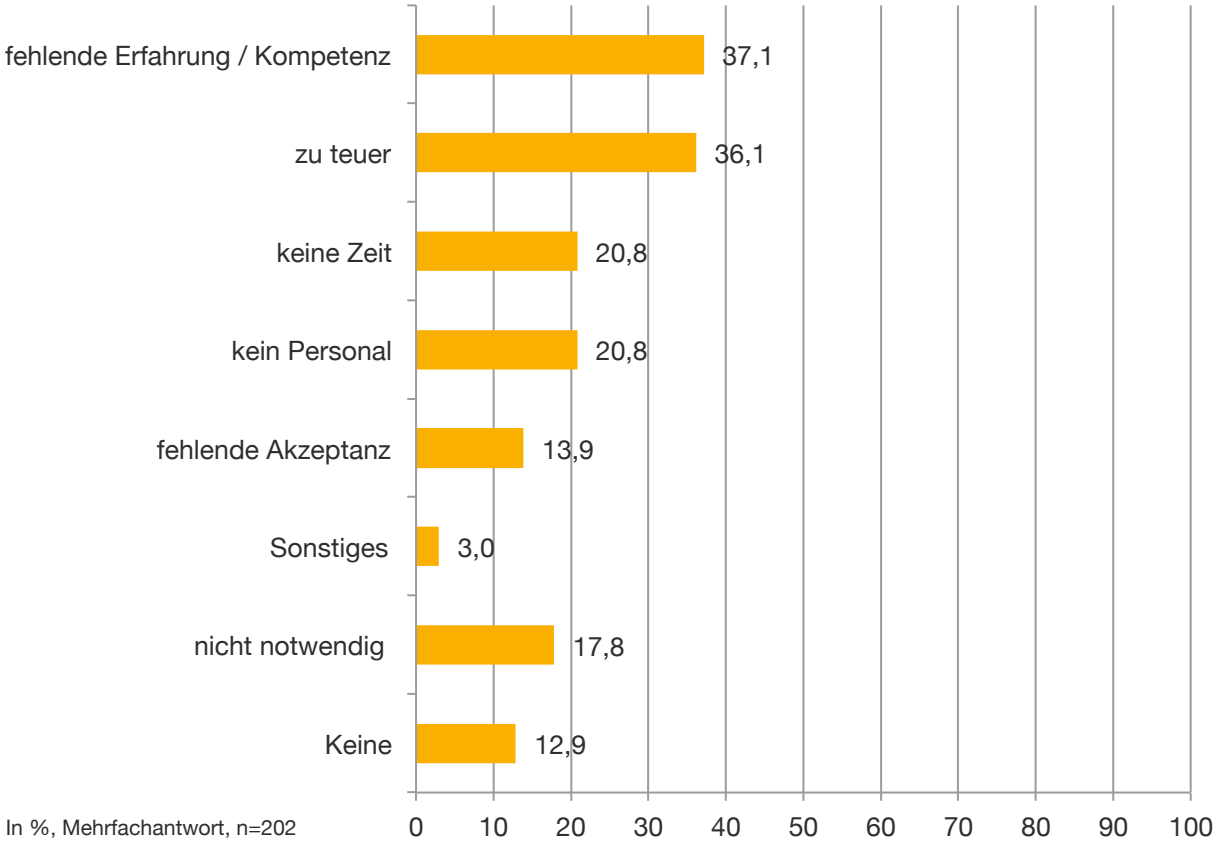
Sonstiges:

- anderes ist wichtiger
- extern durchgeführt
- haben nie daran gedacht
- keine Kosenbewilligung aus der ,,oberen,, Abteilung
- keine Zeit
- keine Zeit,
- keine Zeit, haben Standard
- keine Zeit,kl Unternehmen
- nicht gewusst, dass es so etwas gibt
- Solange nichts passiert, unternimmt man nichts.
- Wird auf Konzernebene erledigt
- zu klein

Originalnennungen

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

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



In %, Mehrfachantwort, n=202

Unternehmensgröße			
EPU	2 bis 10	11 bis 30	31 und mehr
39,0	36,0	43,6	30,6
39,0	36,0	43,6	25,0
22,0	20,9	23,1	16,7
17,1	15,1	30,8	27,8
7,3	7,0	23,1	27,8
4,9	1,2	2,6	5,6
24,4	18,6	10,3	16,7
4,9	15,1	17,9	11,1

= signifikant (p≤0,05)

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

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

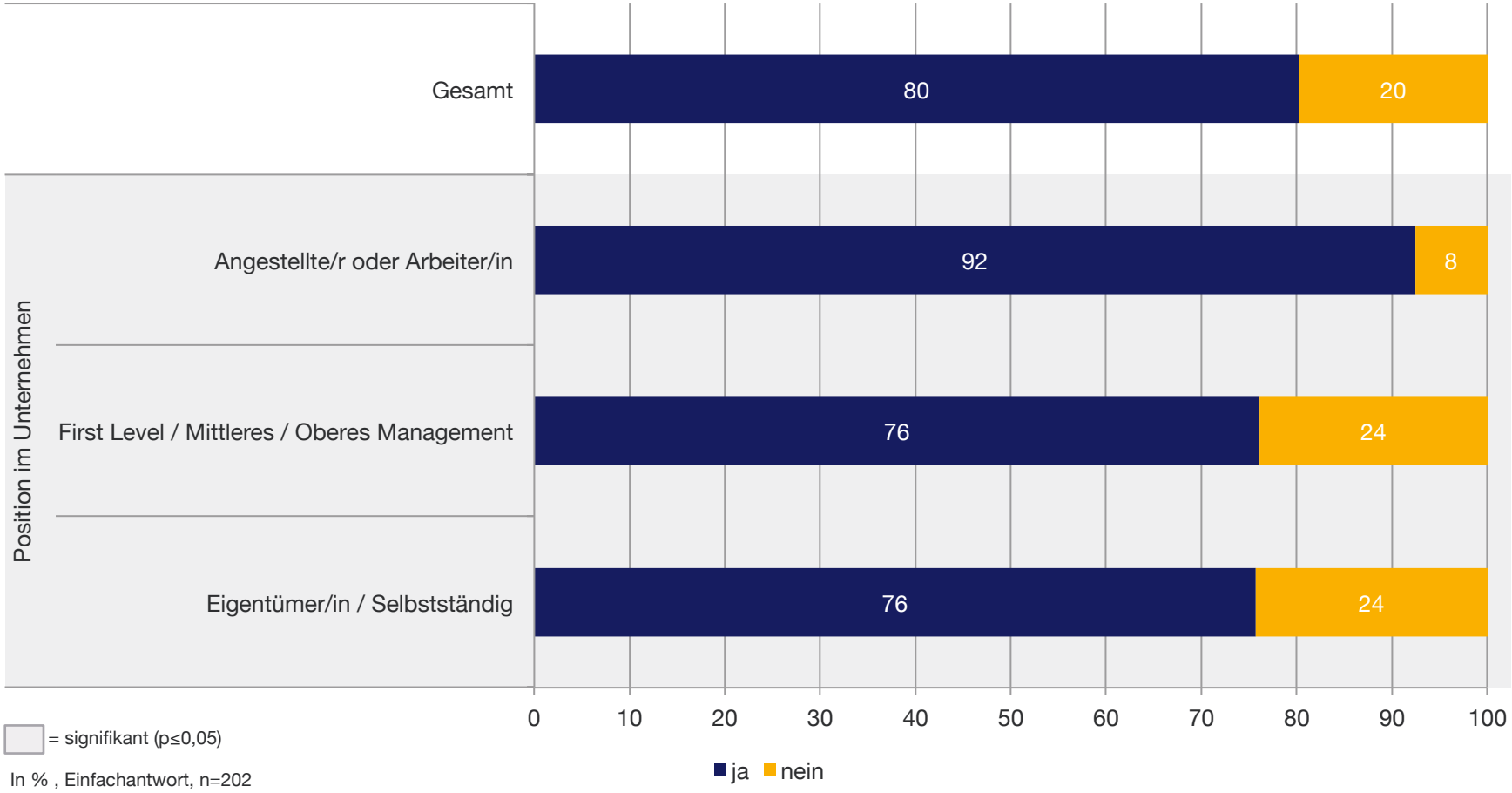
Sonstiges:

- Das Preis-Leistungsverhältnis der Security sollte insgesamt ausgewogen sein. Überperfektionismus ist nicht gut.
- Händler & Wartung ist eher inkompetent
- manche Prozesse nicht leicht umsetzbar
- möchte keine Experten,will es selber machen
- Muttergesellschaft zuständig
- Outgesourct

Offene Nennungen

VERTRAUEN AUF EXTERNE FACHKOMPETENZ

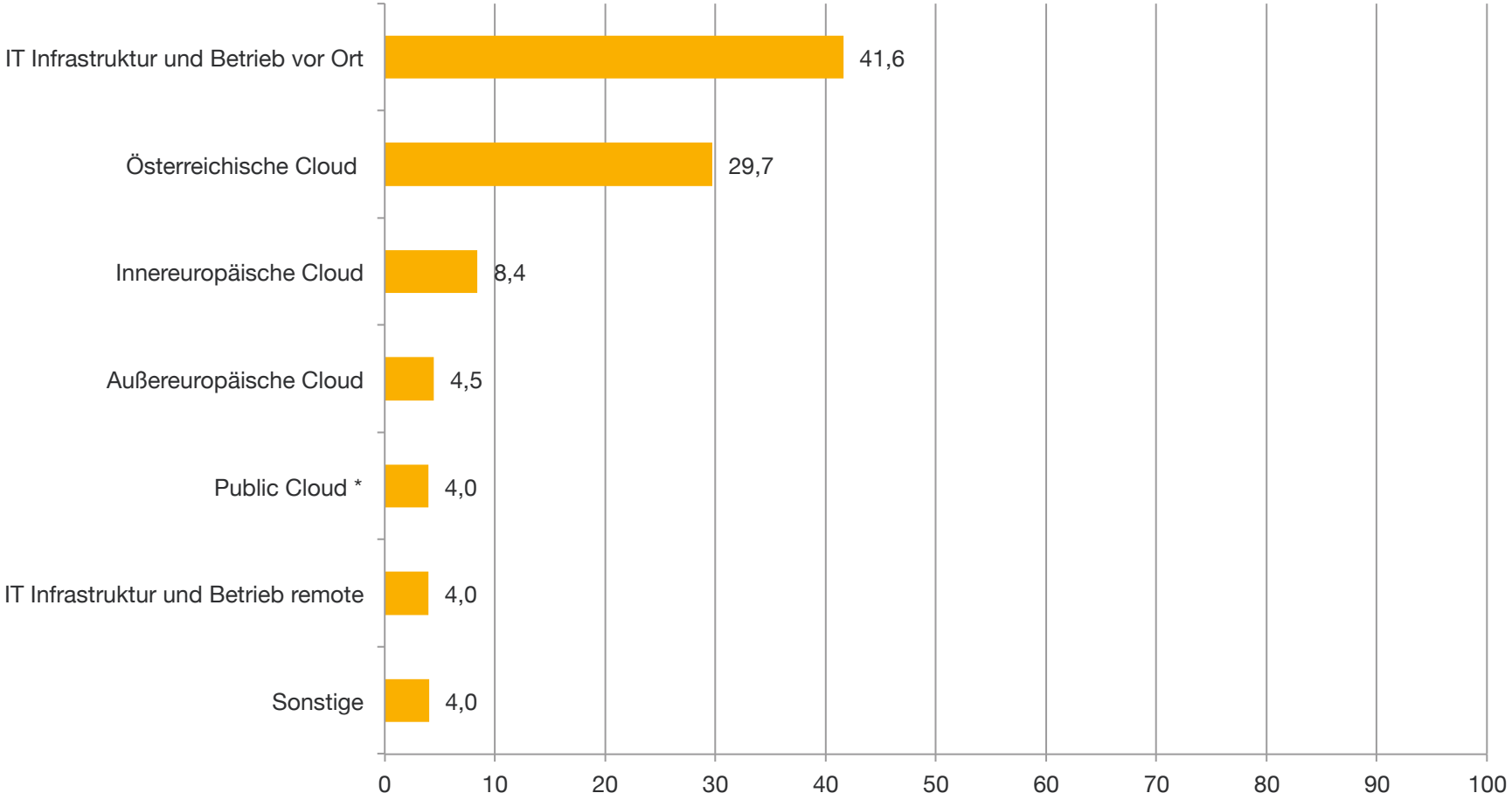
„Würden Sie auf externe(s) Fachkompetenz / Wissen vertrauen, um in Ihrem Unternehmen Sicherheitslücken im IT-Bereich aufzudecken und/oder beheben zu lassen?“



In % , Einfachantwort, n=202

BEVORZUGTE SETTINGS FÜR IT-INFRASTRUKTUR

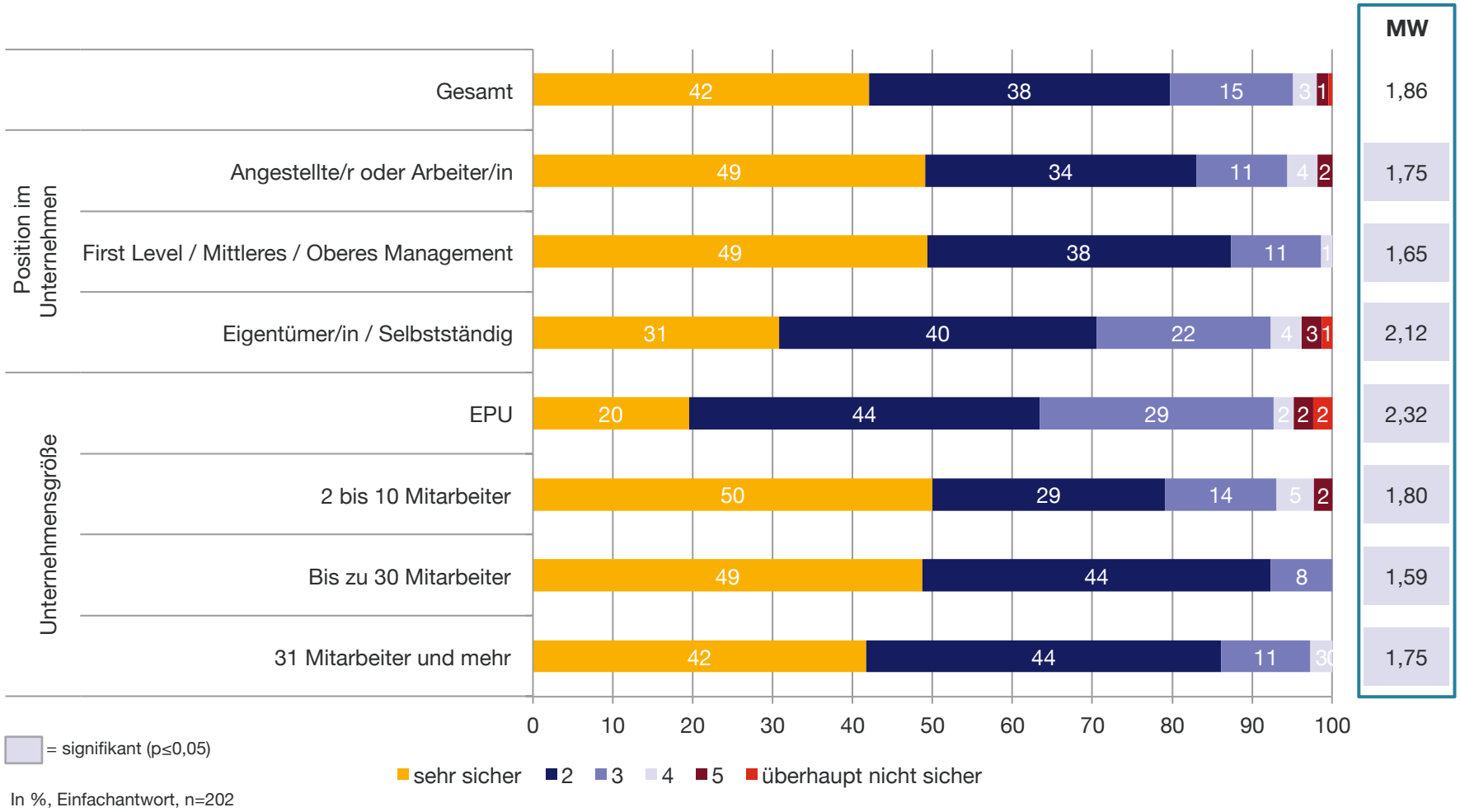
„Welche der folgenden Settings für eine IT-Infrastruktur bevorzugen Sie?“



In %, Mehrfachantwort, n=202; * Public Cloud oder öffentliche Cloud ist ein Angebot eines frei zugänglichen Providers, der seine Dienste offen über das Internet für jedermann zugänglich macht.

ORDNUNGSGEMÄSSE BACKUPS IM UNTERNEHMEN

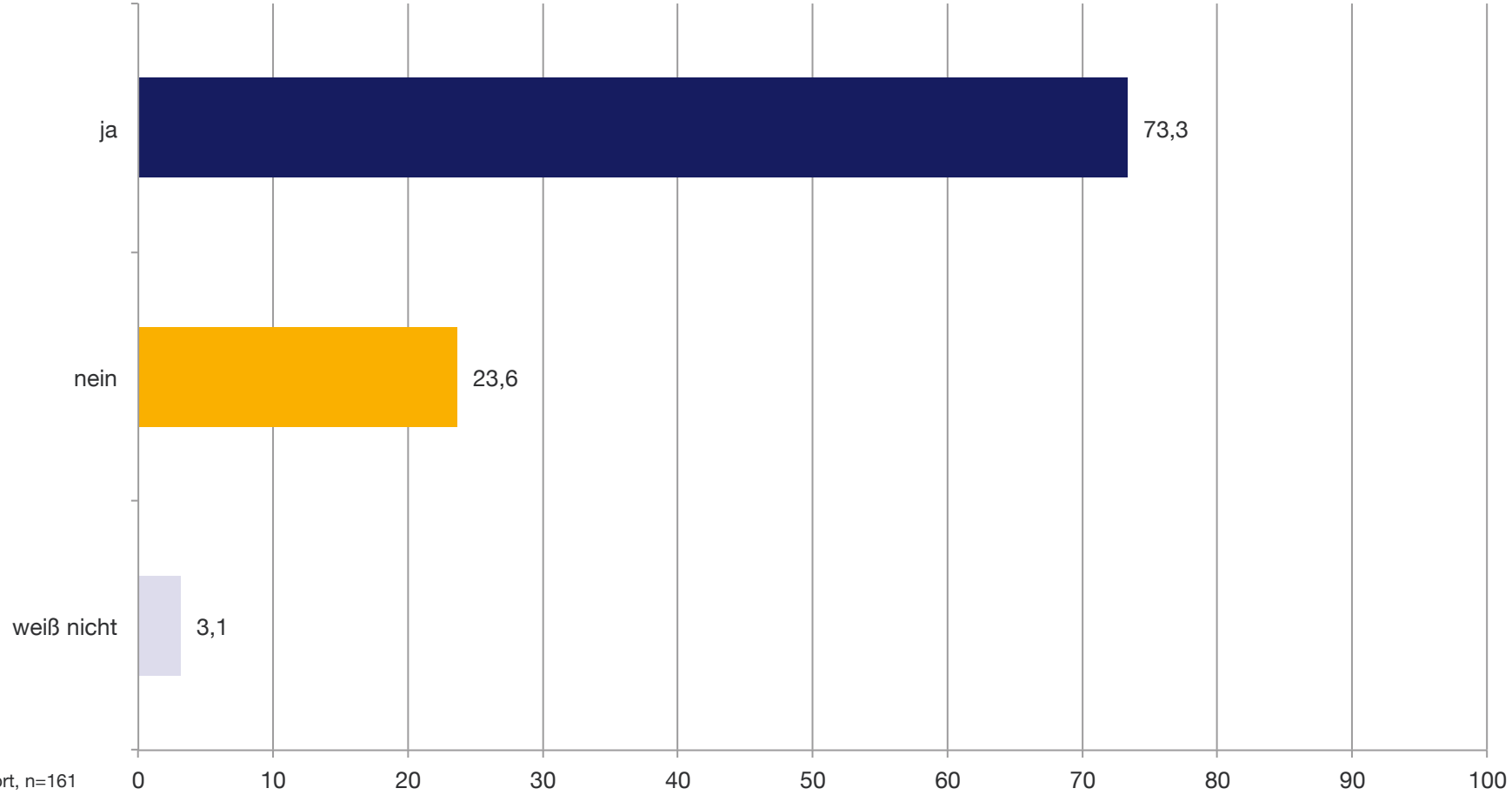
„Sind Sie sicher, dass die Daten in Ihrem Unternehmen ordnungsgemäß gesichert werden (Backup)?“



In %, Einfachantwort, n=202

BACKUPS AUSSERHALB DES UNTERNEHMENS

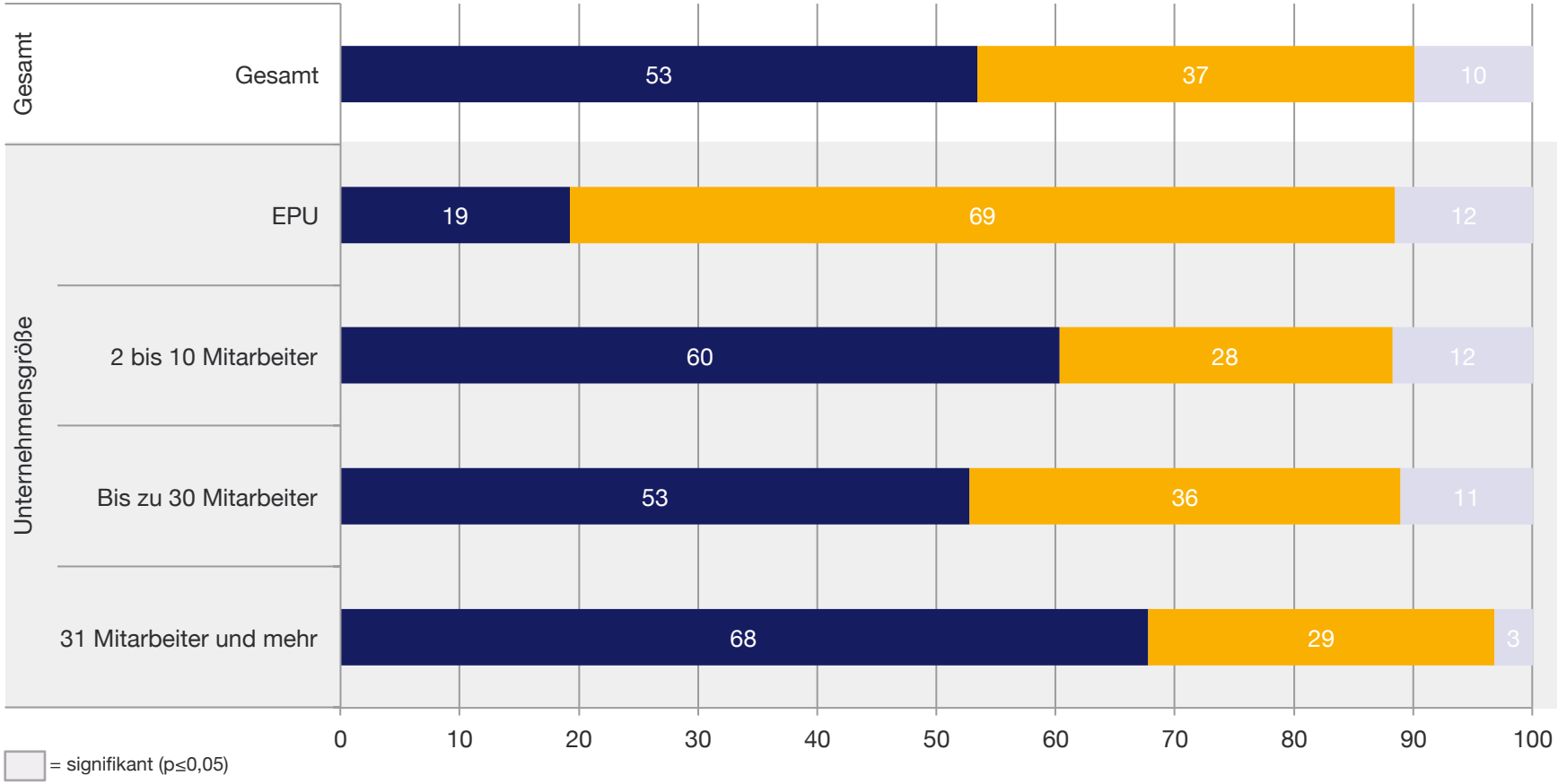
„Werden die Backups auch außerhalb der Räumlichkeiten Ihres Unternehmens aufbewahrt?“
(Frage wurde nur jenen gestellt, die (sehr) sicher sind, dass Backups im Unternehmen durchgeführt werden.)



In %, Einfachantwort, n=161

TESTWEISE WIEDERHERSTELLUNG VON BACKUPS

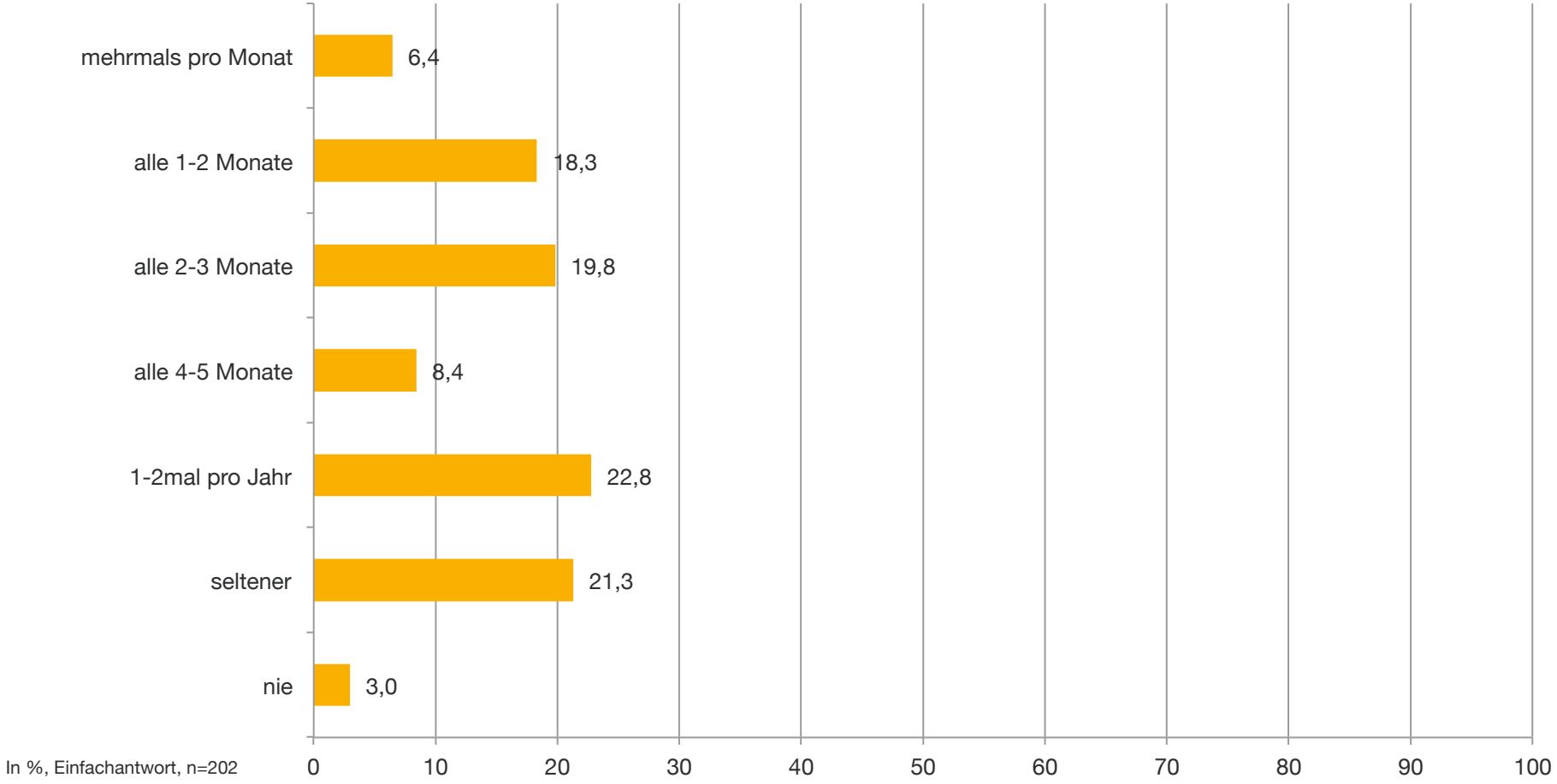
„Und werden die Backups regelmäßig testweise wiederhergestellt?“
(Frage wurde nur jenen gestellt, die (sehr) sicher sind, dass Backups im Unternehmen durchgeführt werden.)



In %, Einfachantwort, n=161

ÄNDERUNG VON PASSWÖRTERN

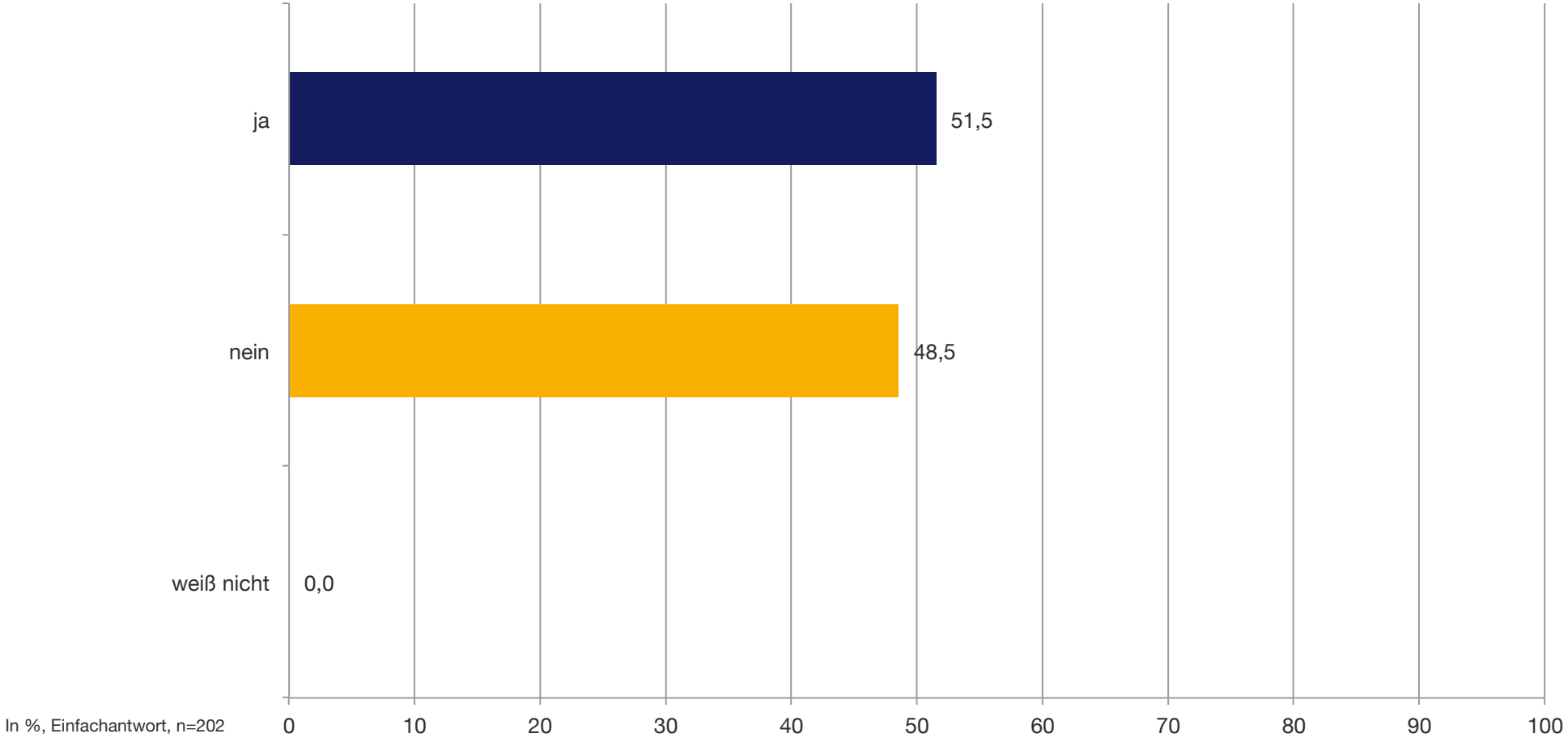
„Wie oft werden Passwörter in Ihrem Unternehmen geändert?“



In %, Einfachantwort, n=202

SPAM PROBLEMATIK

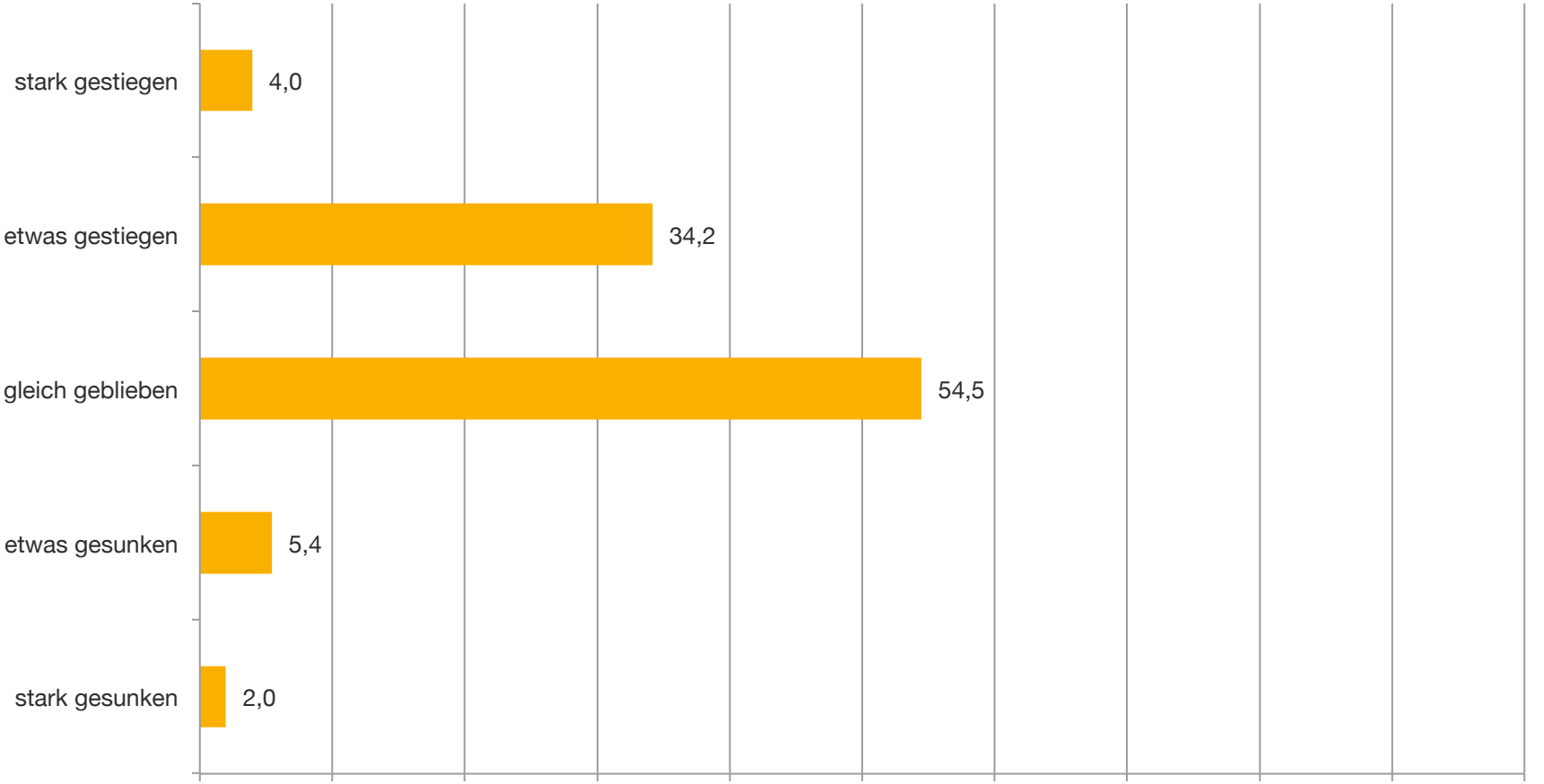
„Leiden Sie bzw. Ihre Mitarbeiter unter SPAM-E-Mail Nachrichten?“



In %, Einfachantwort, n=202

VERÄNDERUNG DES IT-BUDGETS IM LETZTEN JAHR

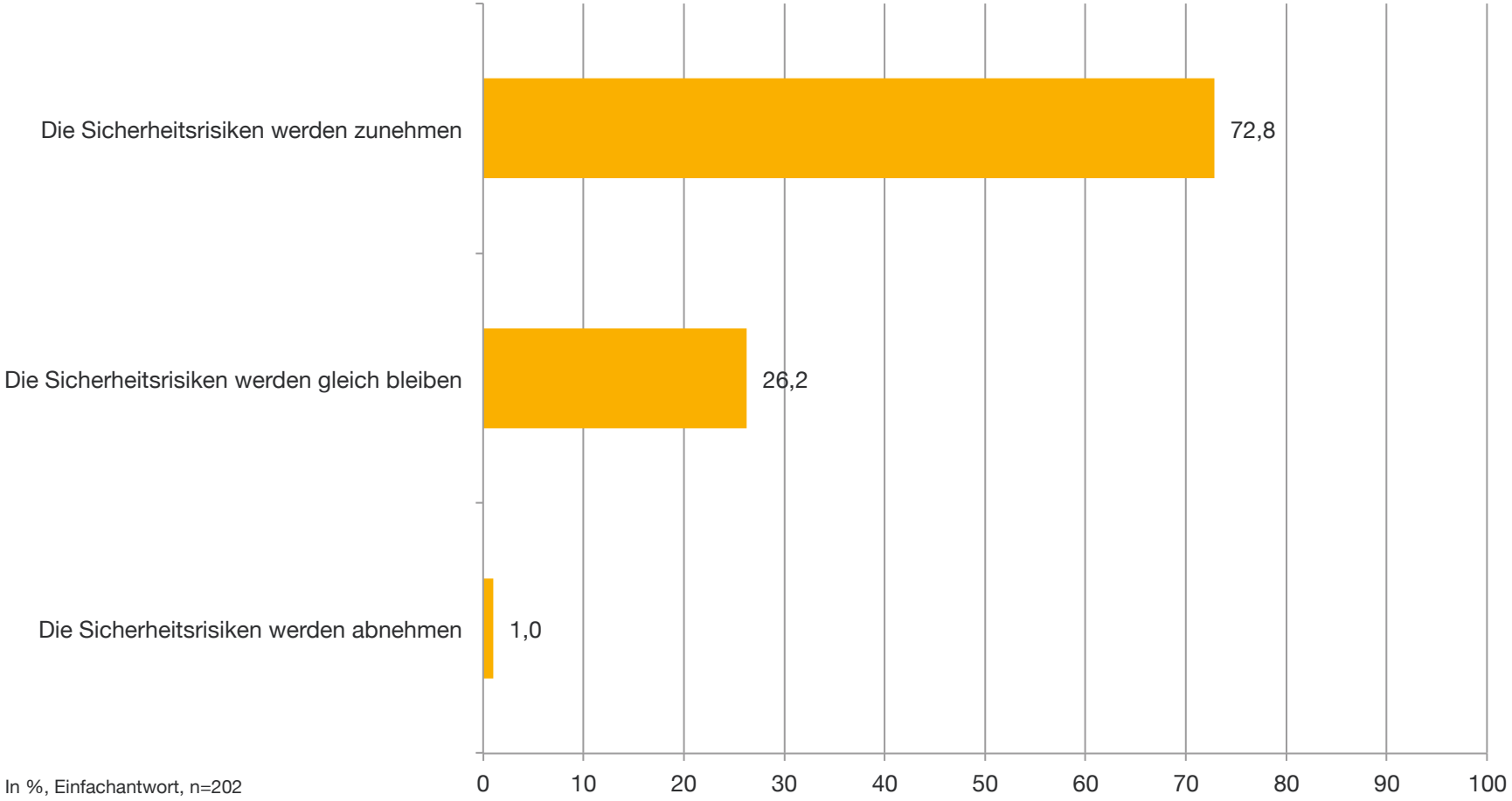
„Wie hat sich das IT-Budget in Ihrem Unternehmen im Vergleich zum Vorjahr verändert?“



In %, Einfachantwort, n=202

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=202

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