IT-Sicherheit
IN DER WIRTSCHAFT

DPT25
Kongress 2020 · Kassel

DEUTSCHER PRÄVENTIONSTAG | PRÄVENTION IN DER DIGITALEN WELT

28./29. SEPTEMBER 2020

SMART PREVENTION

Cyberangriffe gegen Unternehmen

Ergebnisse einer repräsentativen Unternehmensbefragung in Deutschland

Arne Dreißigacker • Bennet von Skarczinski • Prof. Dr. Gina Rosa Wollinger

KFN KRIMINOLOGISCHES FORSCHUNGSINSTITUT NIEDERSACHSEN E.V.

HSPVNRW

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Zusatzförderung durch:

pwc

VHV STIFTUNG

Gliederung

1) Forschungsprojekt
2) Befragungsmethode
3) Stichprobe
4) Ergebnisse
   - Betroffenheit
   - Risikofaktoren
   - Schutzmaßnahmen
   - Folgen von Cyberangriffen
   - Anzeige
5) Fazit

CYBERANGRIFFE GEGEN UNTERNEHMEN

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheit IN DER WIRTSCHAFT

Förderkennzeichen: BMWi-VID5-090168623-01-1/2017
Projektlaufzeit: Dezember 2017 bis November 2020

Projektbeirat

Ausschreibungsverfahren

GEORG-AUGUST-UNIVERSITÄT GÖTTINGEN

Umfrageinstitut

KANTAR EMNID

Teilprojekt I

KFN

Teilprojekt II

Leibniz Universität Hannover

Forschungszentrum L3S Research Center

Projektträger

DLR Projektträger

Zusatzförderung

VHV STIFTUNG

pwc

Regionaler Unternehmens-stammtisch

Assoziierte Partnerorganisationen

Mittelstand-Digital

IHK Industrie- und Handelskammer Hannover

Verfassungsschutz Niedersachsen

pwc

LANDESKRIMINALAMT NIEDERSACHSEN

BVMW Bundesverband mittelständische Wirtschaft Unternehmerverband Deutschlands e.V.

HSPVNRW

IT-Sicherheit IN DER WIRTSCHAFT

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

CYBERANGRIFFE GEGEN UNTERNEHMEN
ARBEITSPAKETE

Förderkennzeichen: BMWi-VID5-090168623-01-1/2017
Projektlaufzeit: Dezember 2017 bis November 2020

insb. kleine und mittlere Unternehmen in Deutschland

AP 6 Ergebnistransfer

Projektbeirat und assoziierte Partner-organisationen

Teilprojekt I

KFN

Teilprojekt II

Leibniz Universität Hannover

Forschungszentrum L3S

AP 10 Plattform Vorhersage

Regionaler Unternehmens-stammtisch

Forschungsstand AP 1

Expertenbefragung AP 2

Unternehmensbefragung I AP 3

Feldstudie Evaluation v. Doku. AP 4

AP 5 Feldstudie IT-Sicherheitsregeln

AP 7 Feldstudie Strategien zur Bekämpfung

AP 8 Feldstudie Benutzbarkeit SIEMs

AP 9 Unternehmensbefragung II

Zusatzförderung durch: VHV STIFTUNG / pwc

- **Computer Assisted Telephone Interview**
  - Durchgeführt von Kantar EMNID, August 2018 bis Januar 2019
  - Zielpersonen: Verantwortliche für den Bereich IT- und Informationssicherheit

- **Standardisierter Fragebogen** mit 40 Fragen zu den Bereichen:
  - Unternehmen und Unternehmensvertreter*innen & Risikoeinschätzungen
  - Erlebte Cyberangriffe (in den letzten zwölf Monaten),
  - Schwerwiegendsten Cyberangriff (Art, Ausmaß, Folgen, Anzeigeverhalten u.a.)
  - Technische und Organisatorische IT-Sicherheitsmaßnahmen (vor und nach dem schwerwiegendsten Cyberangriff)

B01 Immer bezogen auf die **letzten 12 Monate**: Wie oft war Ihr Unternehmen von folgenden Angriffsarten **betroffen und musste reagieren**?

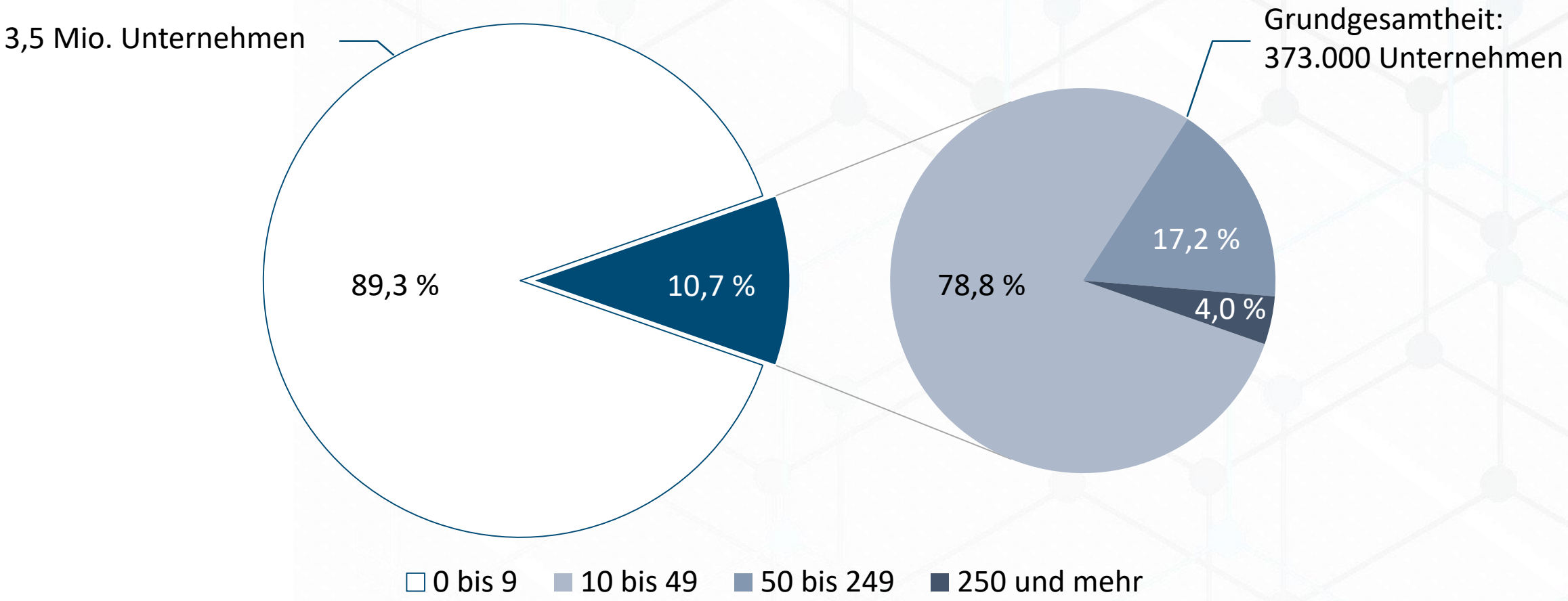
	Anzahl	Keine Angabe	Weiß nicht
☐ **Ransomware**, die das Ziel hatte, Unternehmensdaten zu verschlüsseln	☐☐☐☐	☐	☐

Befragung ●●○

- **Ransomware**: Verschlüsselung v. Unternehmensdaten 
- **Spyware**: Ausspähung v. Nutzeraktivitäten und sonst. Daten 
- **Sonst. Malware**: Schadsoftware wie Viren, Würmer, Trojaner 
- **Manuelles Hacking**: Manipulation von Soft- und Hardware ohne spez. Malware 
- **(D)DoS**: Überlastung von Web- und E-Mail-Servern 
- **Defacing**: Unbefugte Veränderung von Webinhalten 
- **CEO-Fraud**: Manipulation v. Besch. durch Vortäuschung einer Führungsperson 

- **Phishing**: Erlangung sensi. Daten durch Täuschung mit falschen E-Mails o. Webseiten 

Anteile der Unternehmen nach Beschäftigtengrößenklassen (URS, Statistisches Bundesamt, 2017)



3 Stichprobe ●○

- Unternehmen mit Sitz in Deutschland ab 10 Beschäftigten in den Firmendatenbanken von Bisnode (ehemals Hoppenstedt) und Heins & Partner

gem. URS des Statistischen Bundesamtes (2017): 373.000 Unternehmen

ca. 294.000 Unternehmen (10-49 Besch.)	ca. 64.000 Unternehmen (50-249 Besch.)	ca. 15.000 Unternehmen ab 250 Besch.

Disproportional geschichtete Zufallsstichprobe (43.219 kontaktierte Unternehmen)

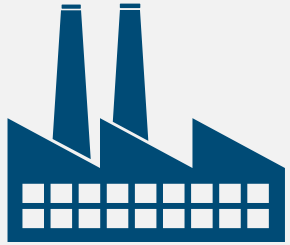
Nettostichprobe: N=5.000

1.000 Unternehmen (10-49 Besch.)

1.000 Unternehmen (50-99 Besch.)

1.000 Unternehmen (100-249 Besch.)

1.000 Unternehmen (250-499 Besch.)

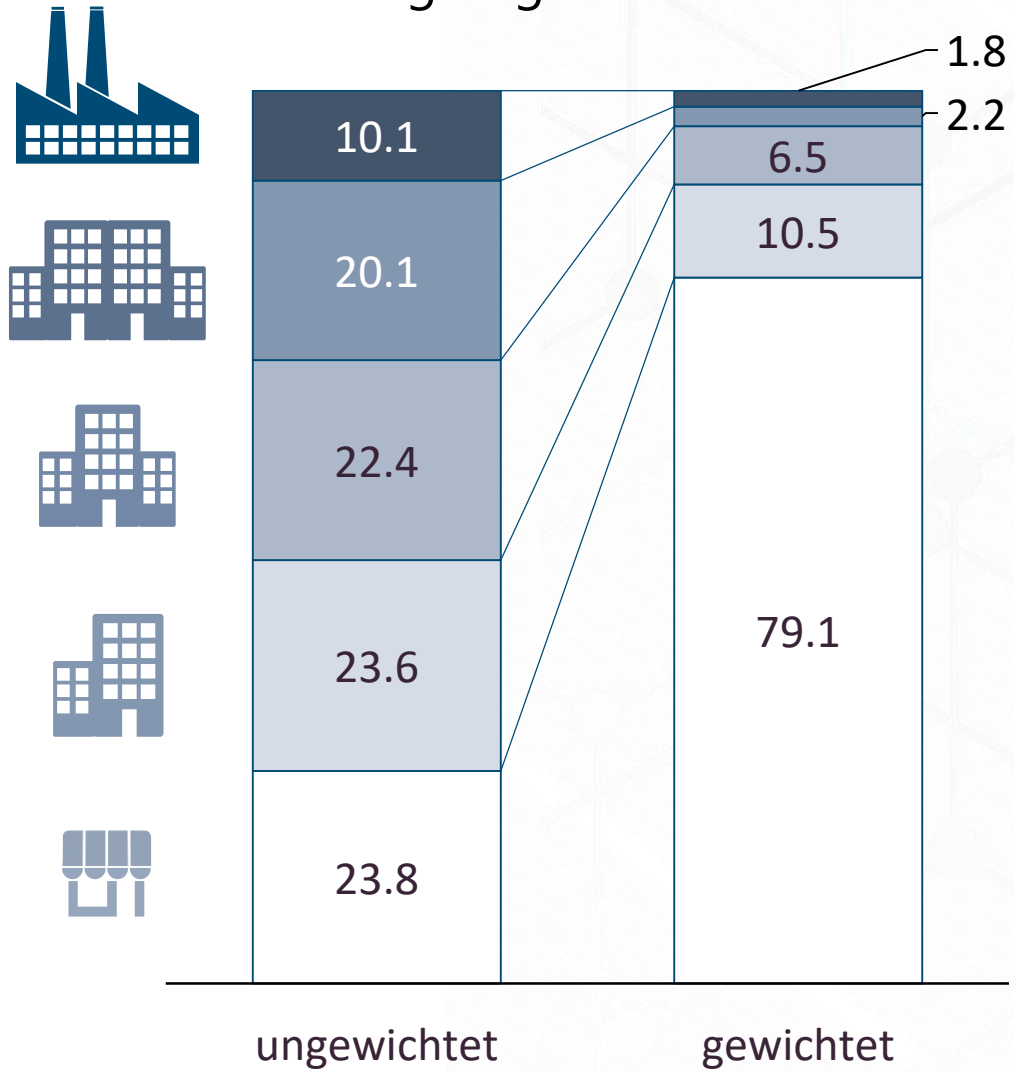


500 Unternehmen (ab 500 Besch.)

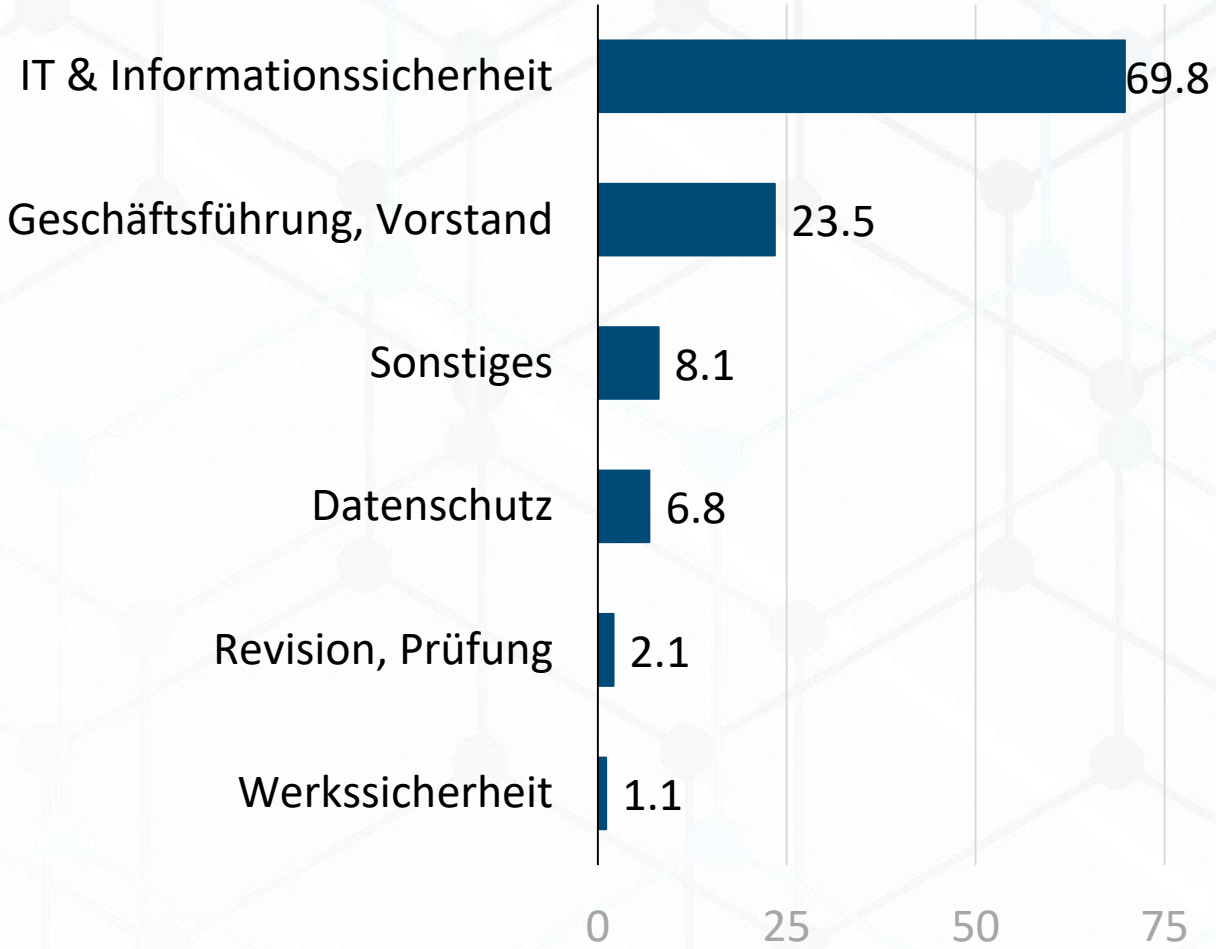
500 Unternehmen der Daseinsvorsorge

3 Stichprobe ●●

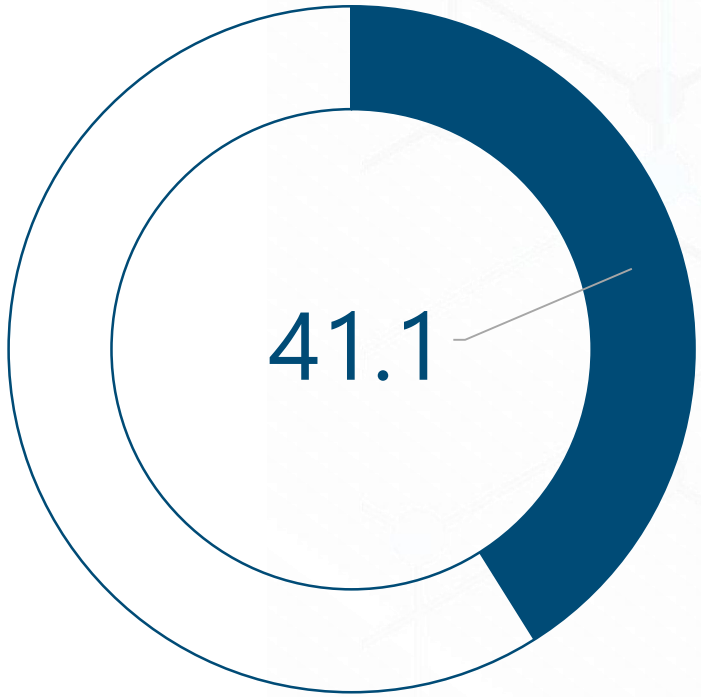
Beschäftigtengrößenklasse in Prozent



Position der Befragten in Prozent



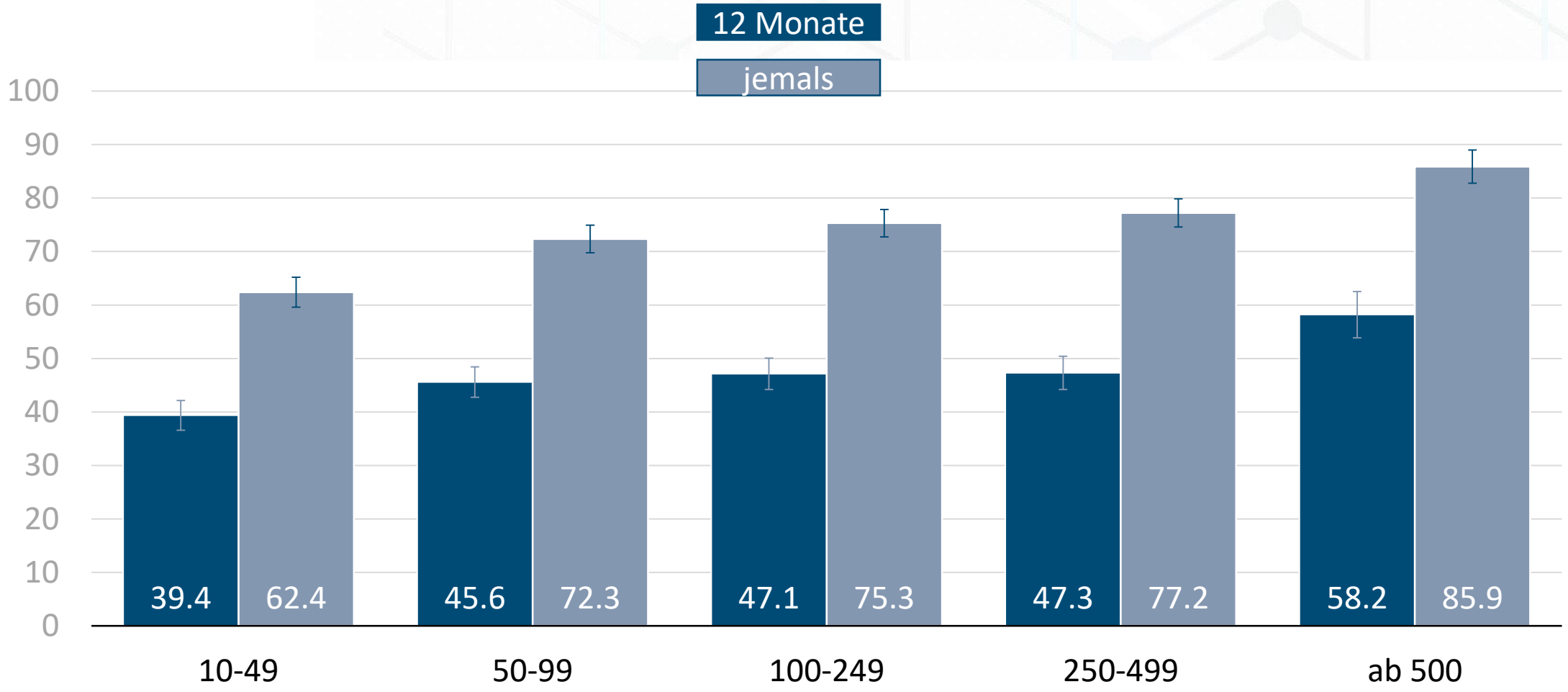
…in den letzten 12 Monaten
(in Prozent; N=4.981)



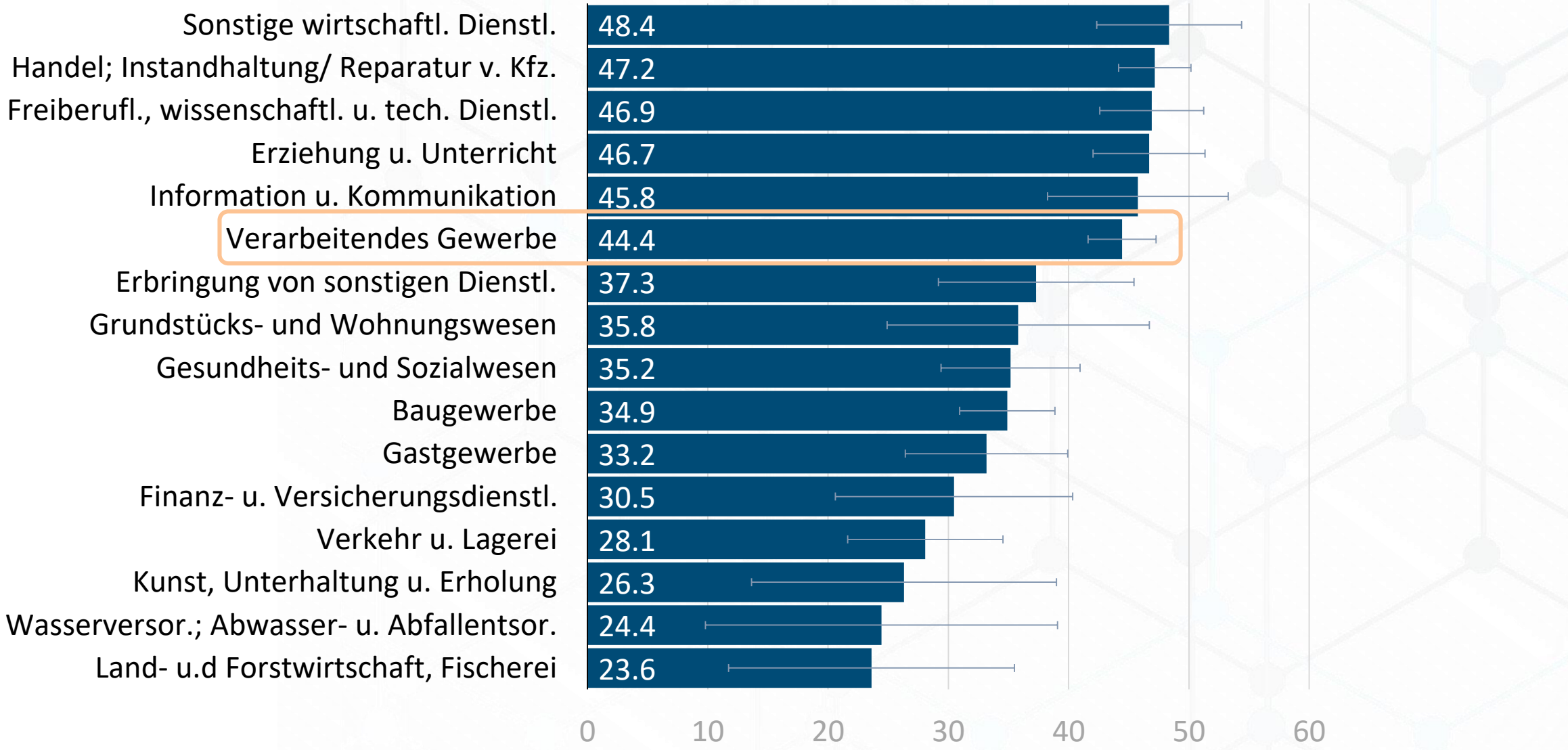
jemals
(in Prozent; N=4.844)

Anteile der Unternehmen, die in den letzten zwölf Monaten bzw. jemals von mindestens einer der erfragten Angriffsarten betroffen waren und auf diese aktiv reagieren mussten

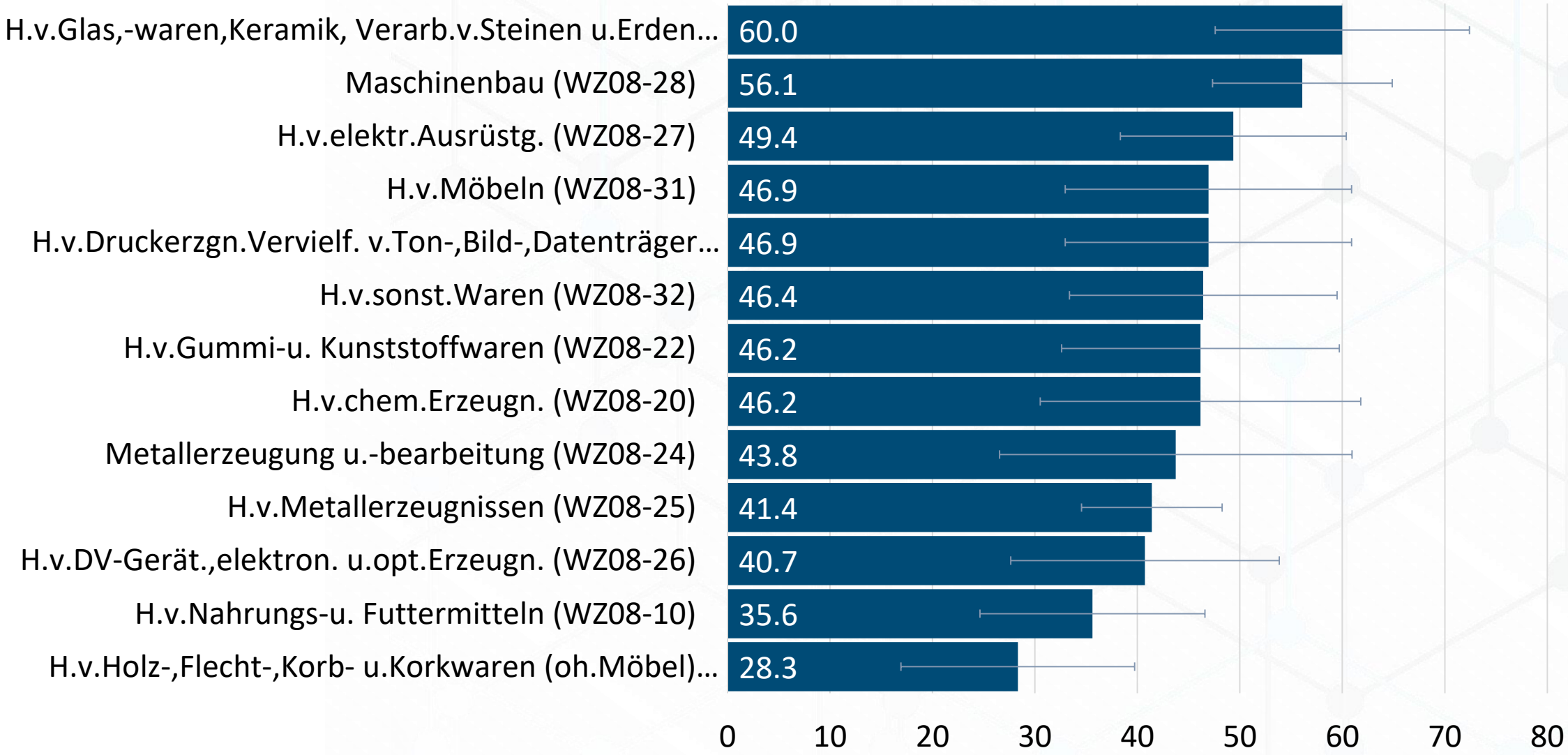
Anteile der (in den letzten 12 Monaten) betroffenen Unternehmen nach Größe



Anteile der (in den letzten 12 Monaten) betroffenen Unternehmen nach Branche (WZ08 Ebene 1)

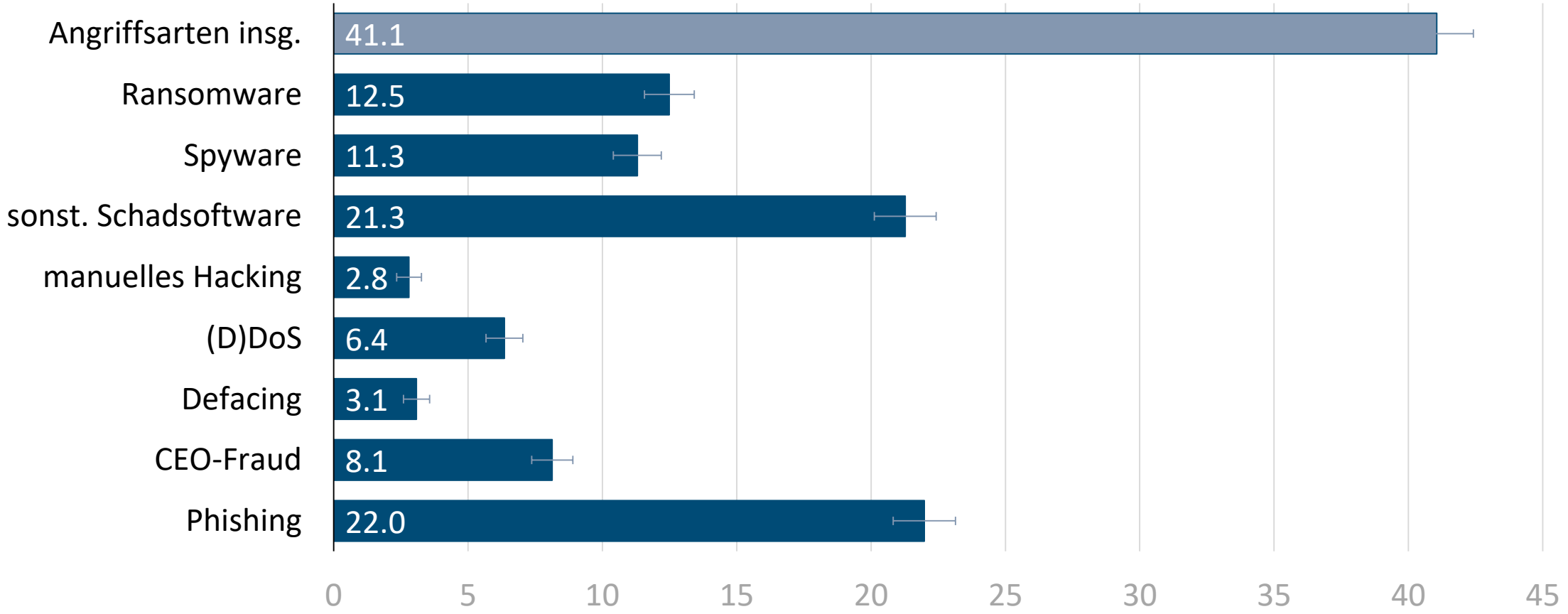


Anteile der (in den letzten 12 Monaten) betroffenen Unternehmen des verarbeitenden Gewerbes



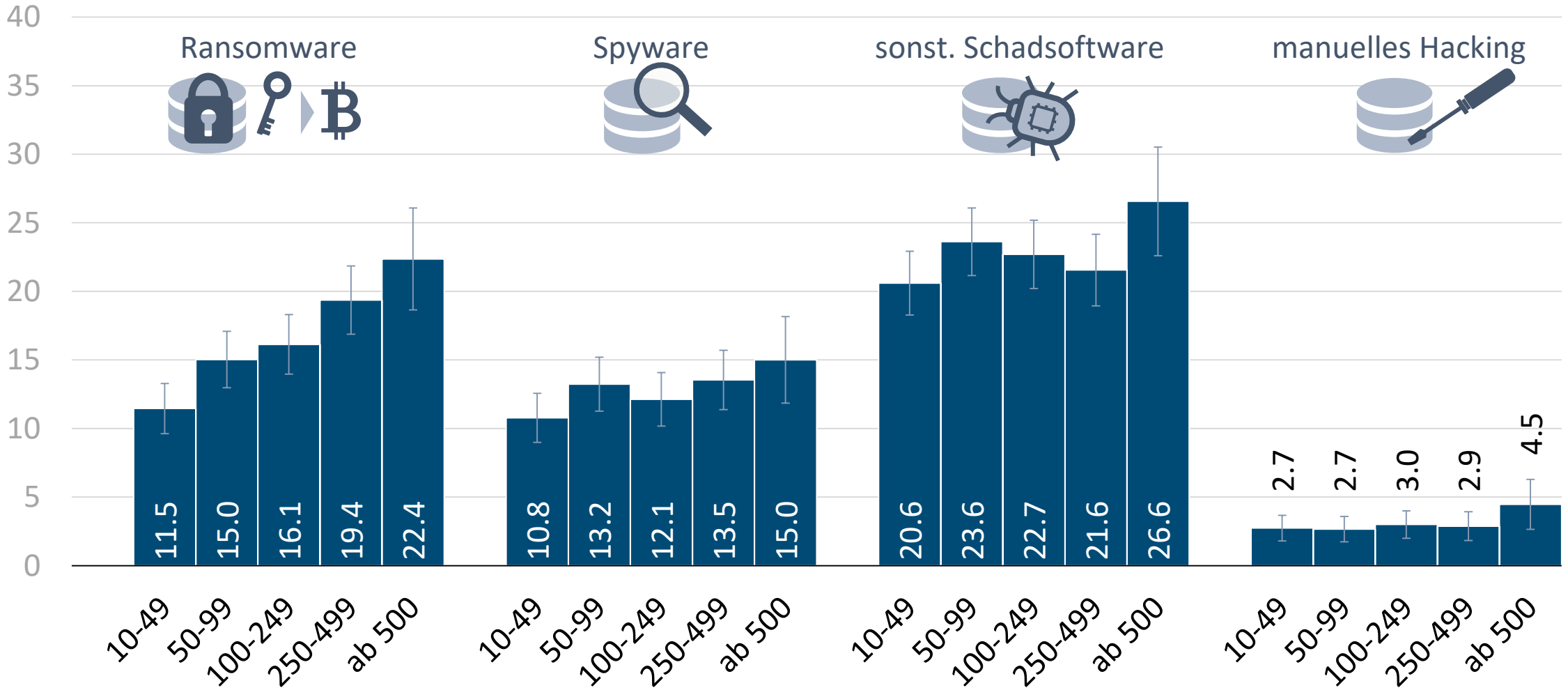
4.1 Betroffenheit ●●●●●○○

Anteile der in den letzten 12 Monaten betroffenen Unternehmen nach Angriffsart



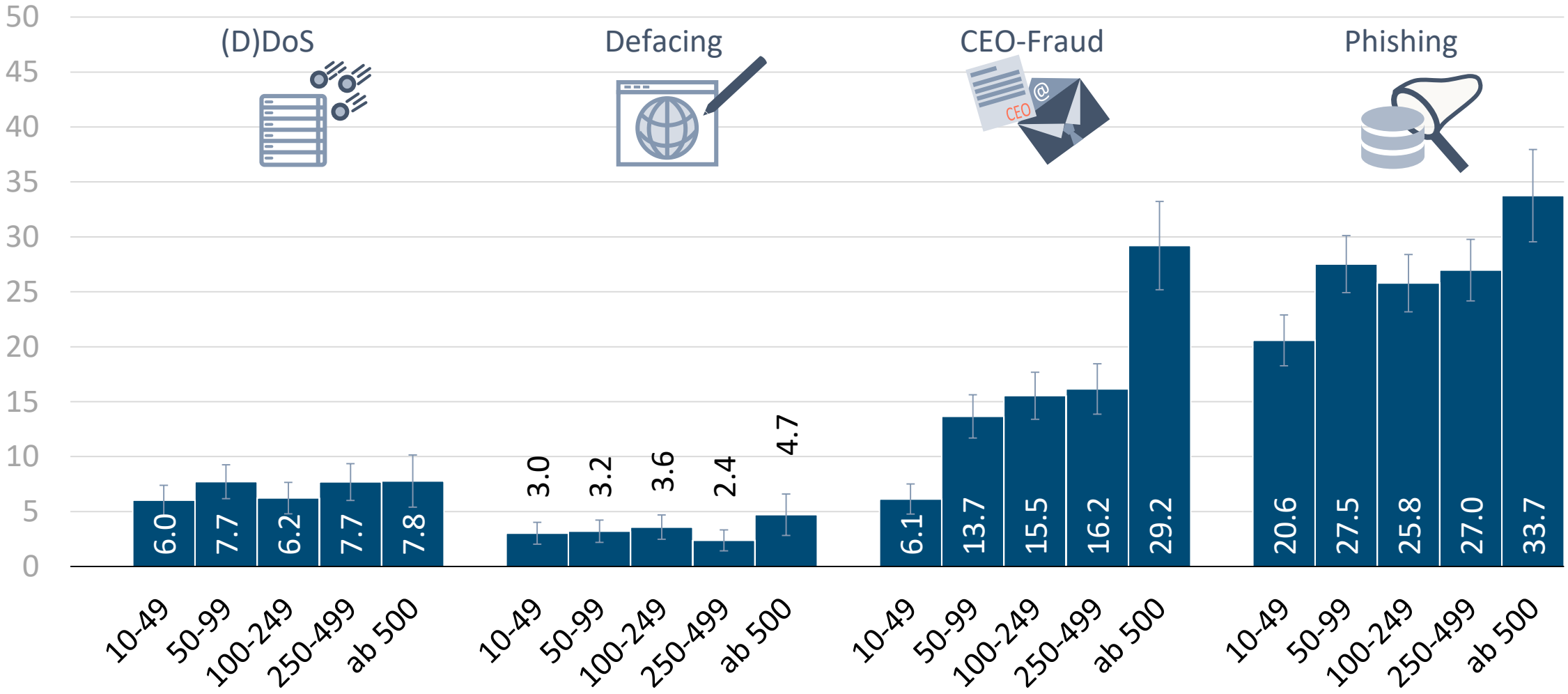
4.1 Betroffenheit

Anteile der in den letzten 12 Monaten betroffenen Unternehmen nach Angriffsart u. Größe



4.1 Betroffenheit

Anteile der in den letzten 12 Monaten betroffenen Unternehmen nach Angriffsart u. Größe



4.2 Risikofaktoren

Anteile der betroffenen Unternehmen nach Risikofaktoren

Mehrere Standorte in Dtl.?

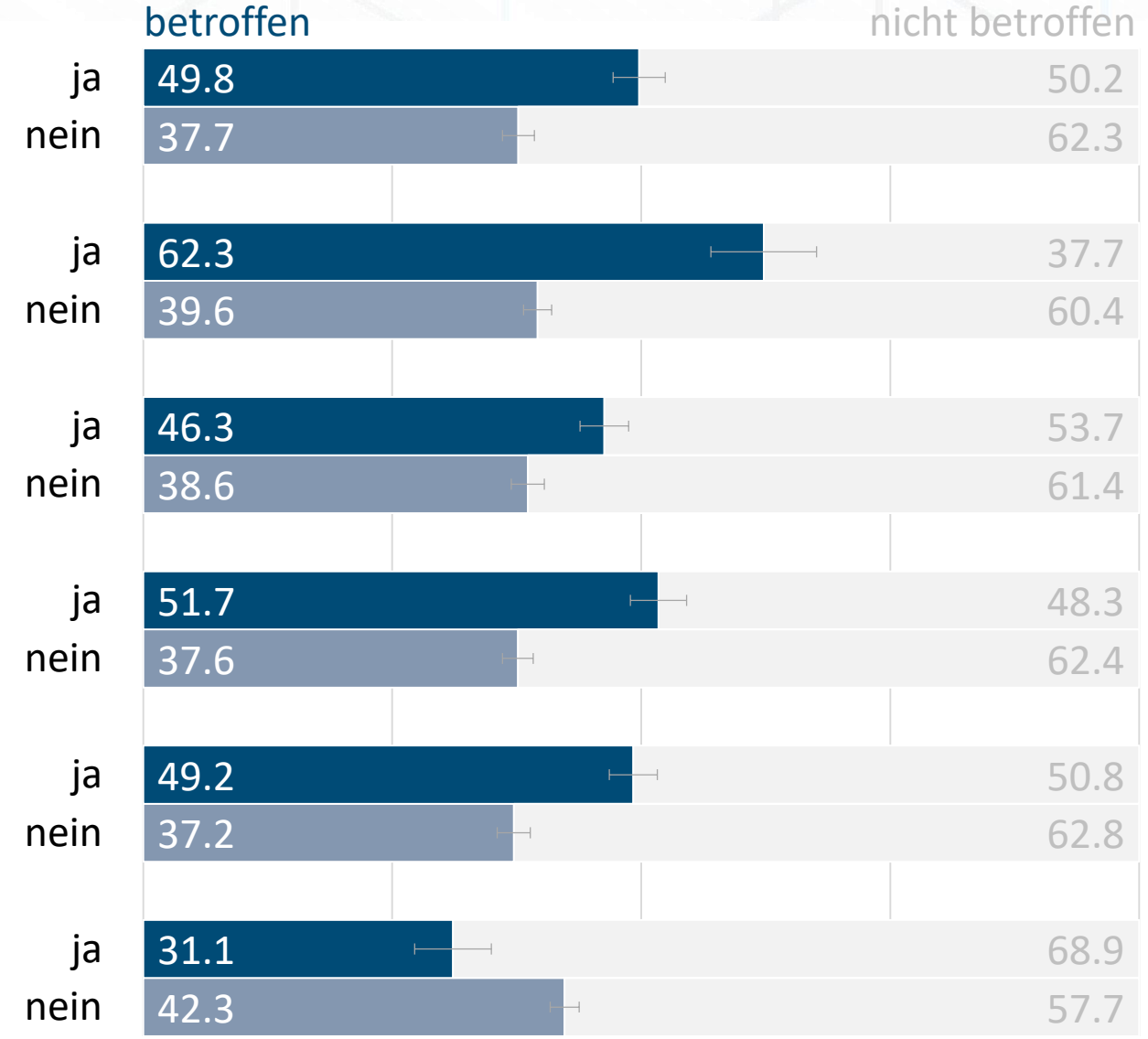
Standort(e) im Ausland?

Exporttätigkeit?

Besondere Produkte, Herstellungsverf. etc.?

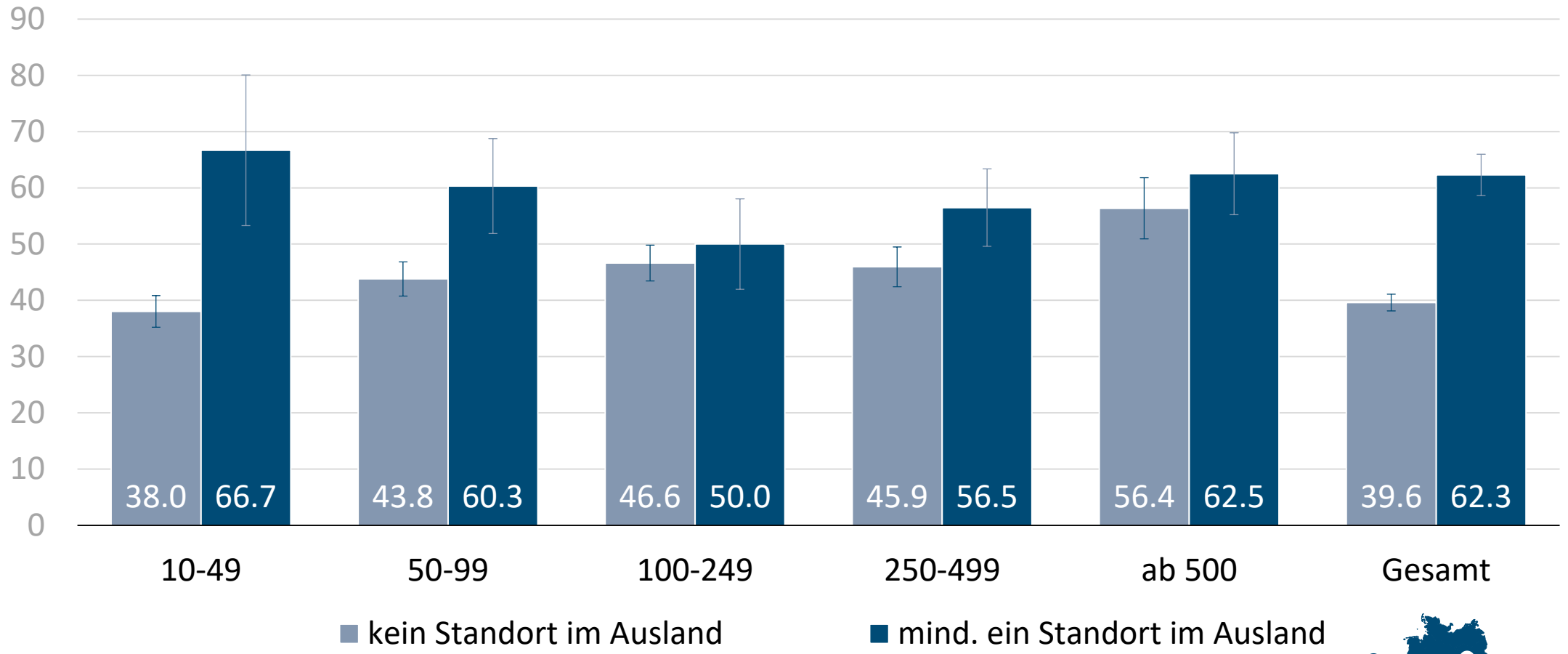
Besondere Reputation/ Kundenkreis?

Unternehmen der Daseinsvorsorge?

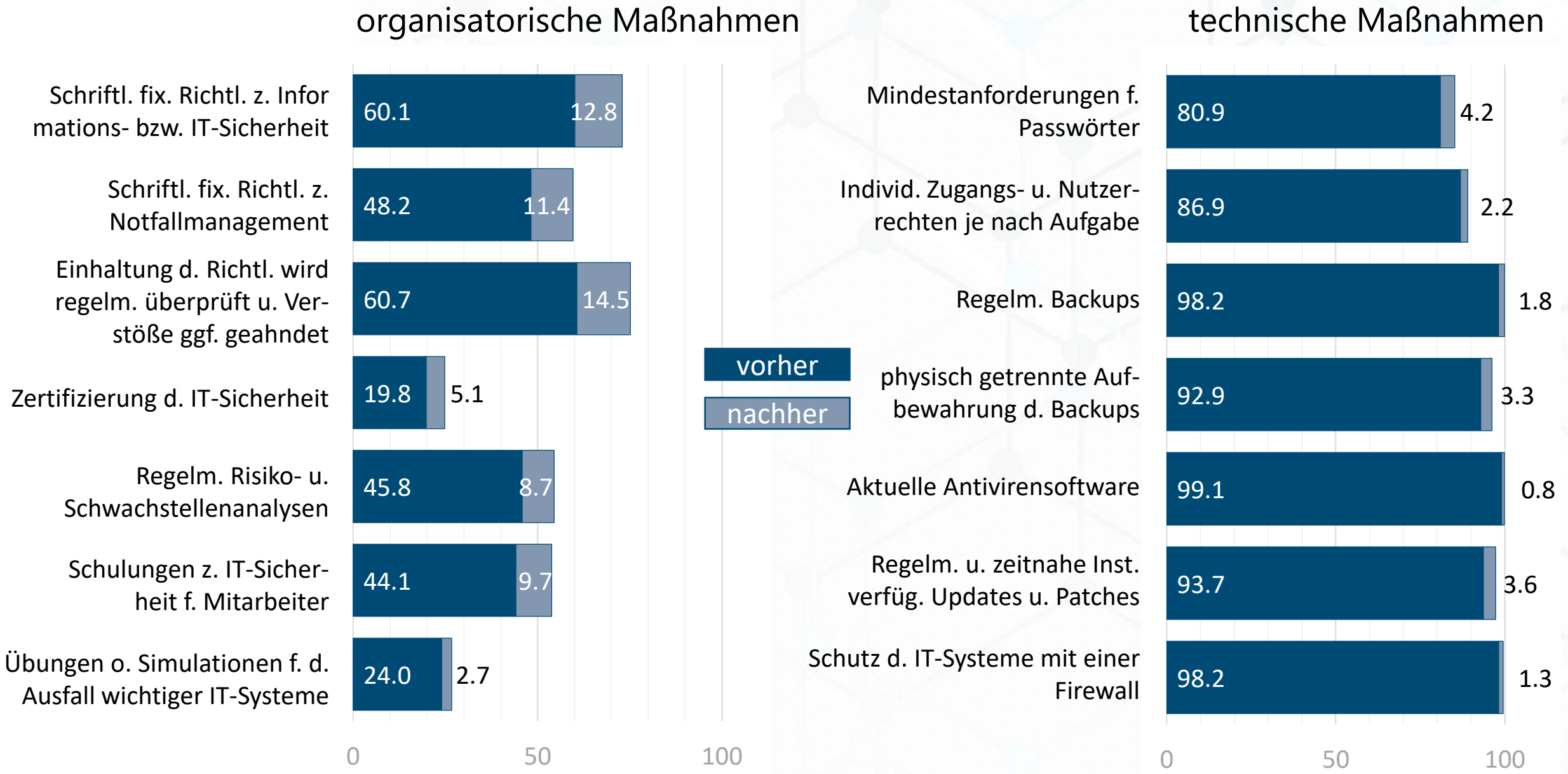


4.2 Risikofaktoren ●●

Anteile der betroffenen Unternehmen nach Auslandsstandort

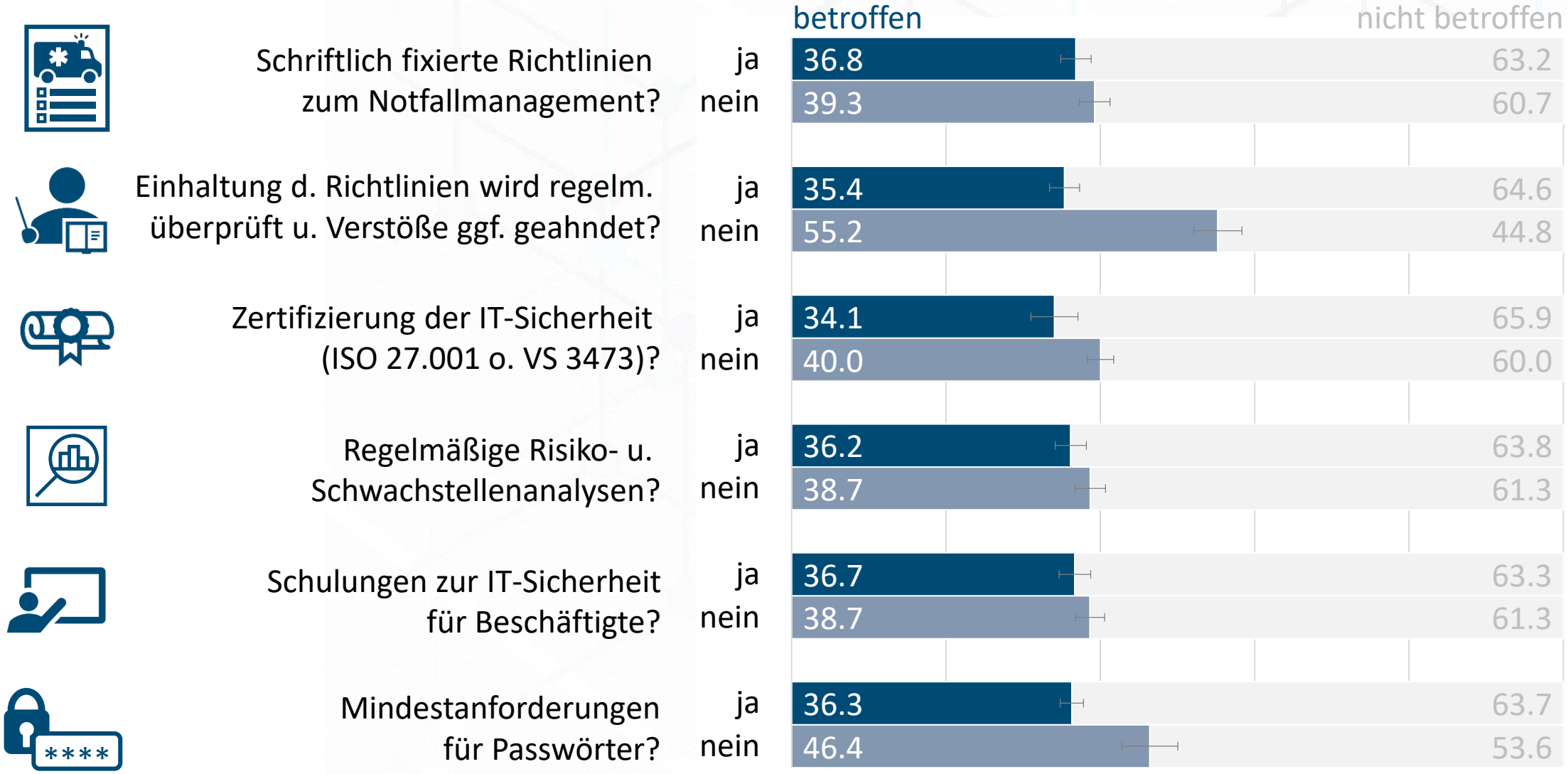


4.3 Schutzmaßnahmen



4.3 Schutzmaßnahmen ●●○

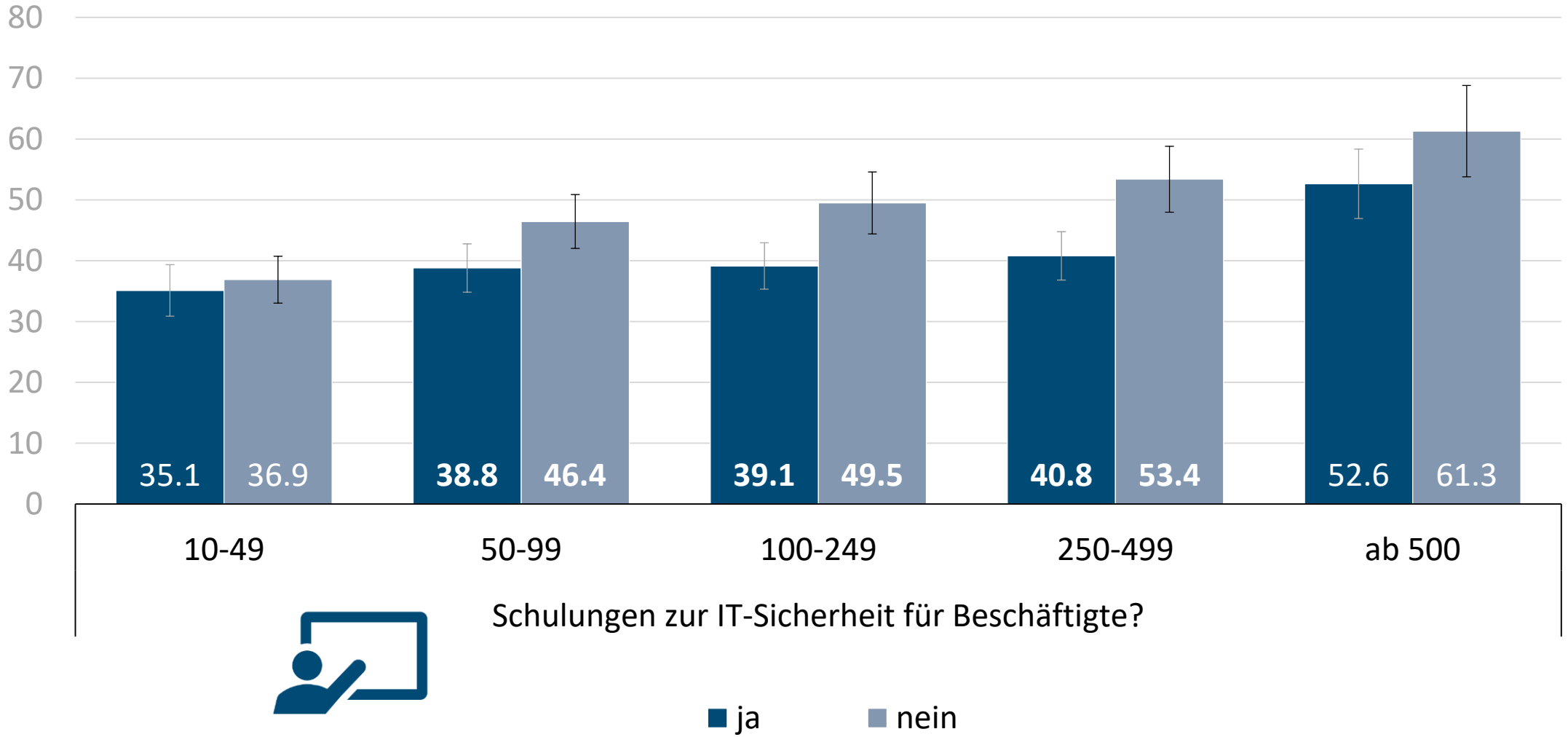
Anteile der betroffenen Unternehmen nach vorhandenen IT-Sicherheitsmaßnahmen*



*) nur Unternehmen mit Angaben zum schwerwiegendsten Angriff

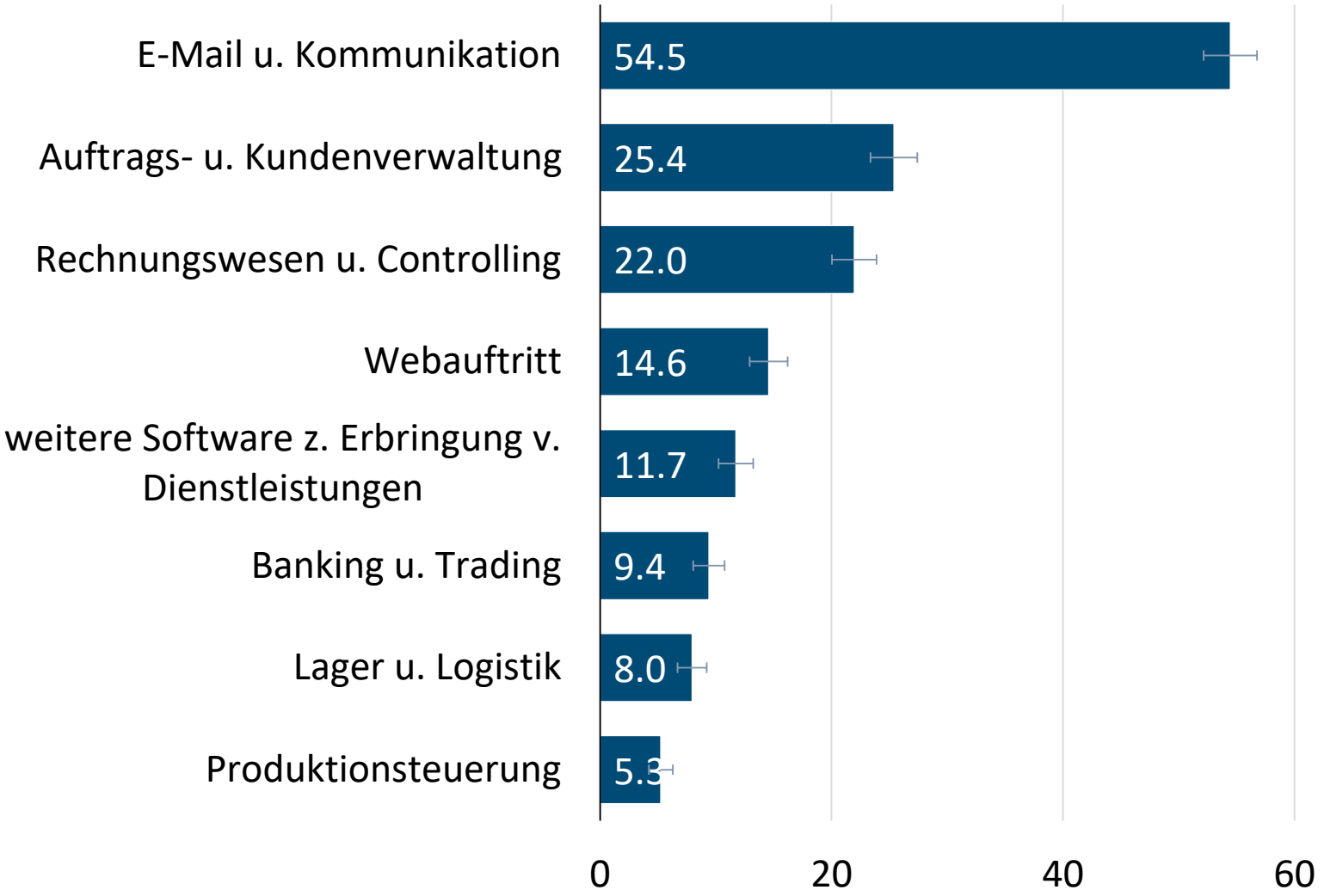
4.3 Schutzmaßnahmen

Anteile der betroffenen Unternehmen mit o. ohne Mitarbeiterschulung nach Beschäftigtengröße



4.4 Folgen von Cyberangriffen

Anteile der von schwerwiegendsten Angriffen betroffener Systeme

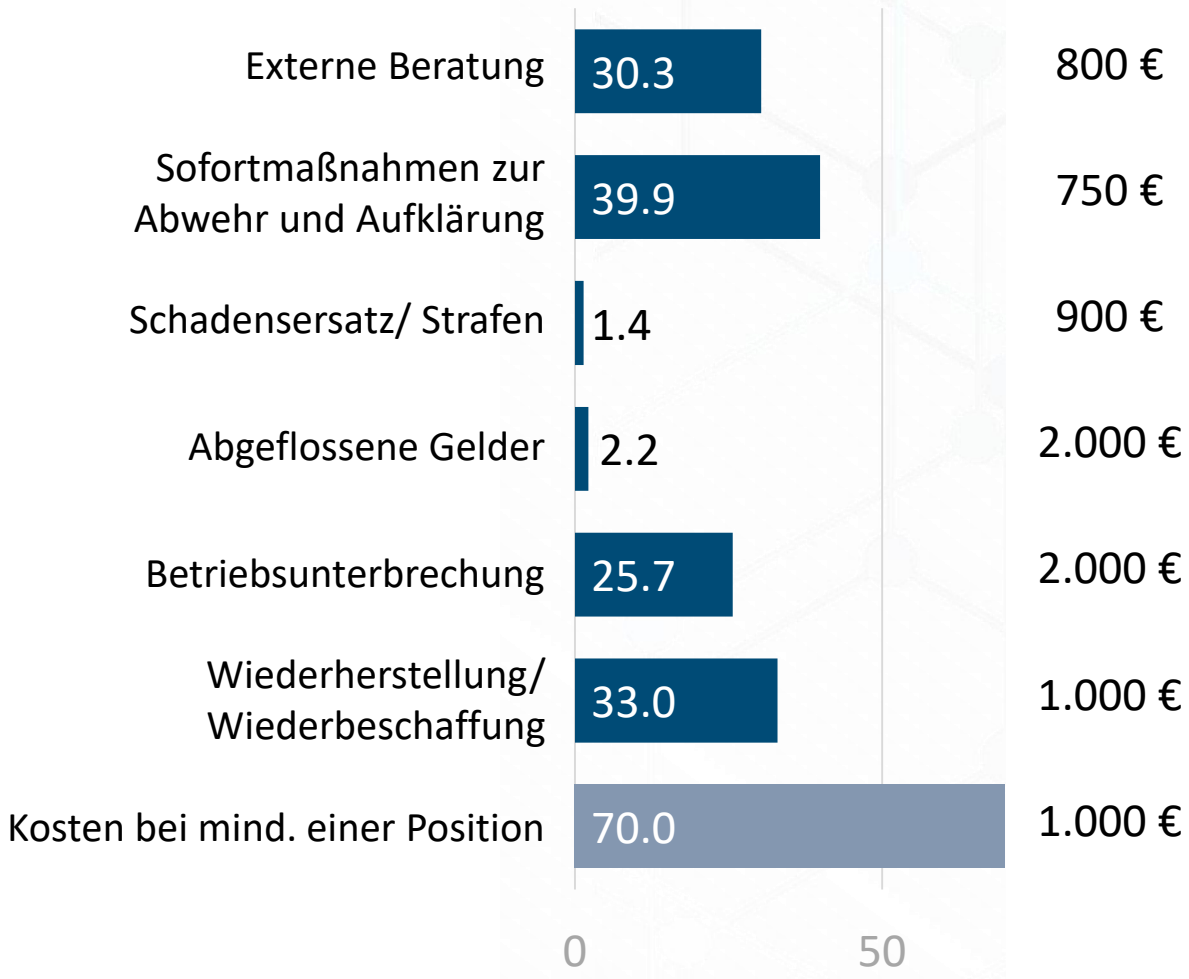


Dauer des Ausfalls (h)*	Ø	Median	SD	N
E-Mail u. Kommunikation	65	24	201,0	705
Auftrags- u. Kundenverwaltung	76	24	172,1	393
Rechnungswesen u. Controlling	73	24	169,4	310
Webauftritt	337	12	1463,2	161
weitere Software z. Erbringung v. Dienstleistungen	89	24	166,6	172
Banking u. Trading	44	24	110,2	117
Lager u. Logistik	73	24	151,7	103
Produktionsteuerung	65	48	63,4	82

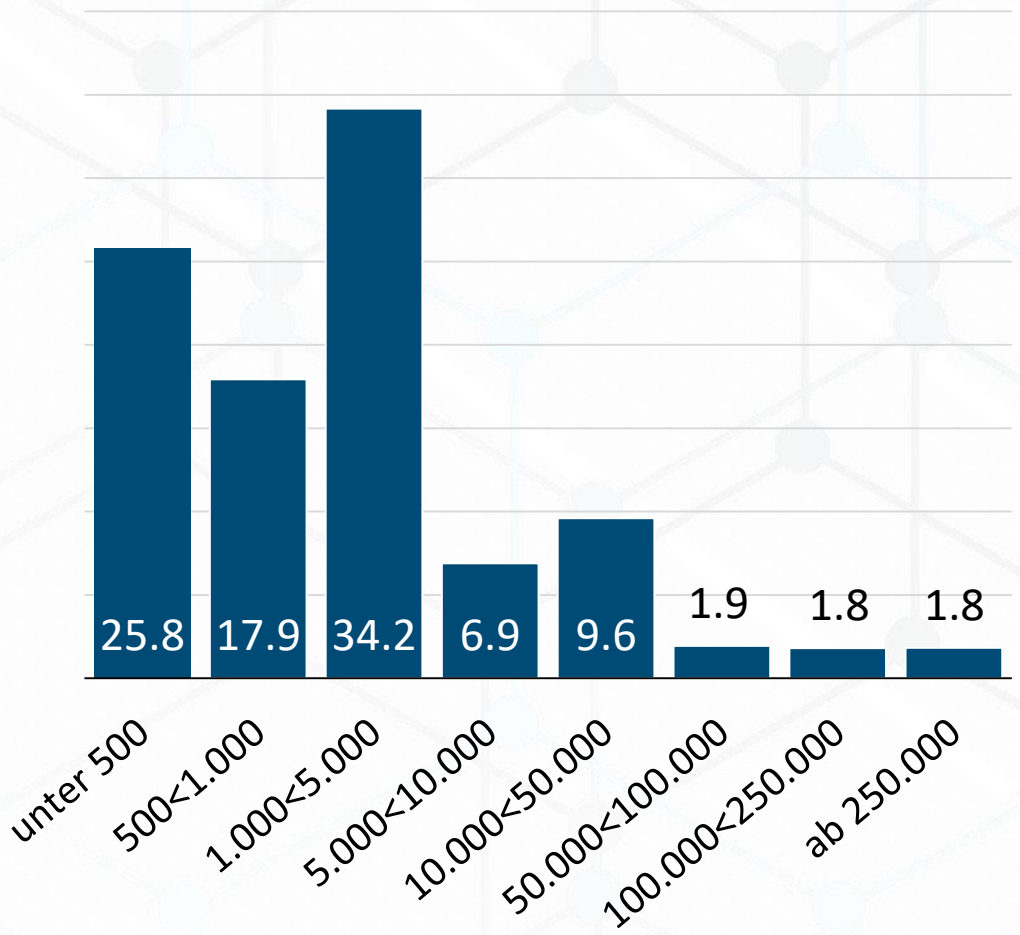
*) nur als „(eher) wichtig“ eingestufte Systeme

4.4 Folgen von Cyberangriffen

Anteile der Unternehmen mit Kosten nach Kostenpositionen

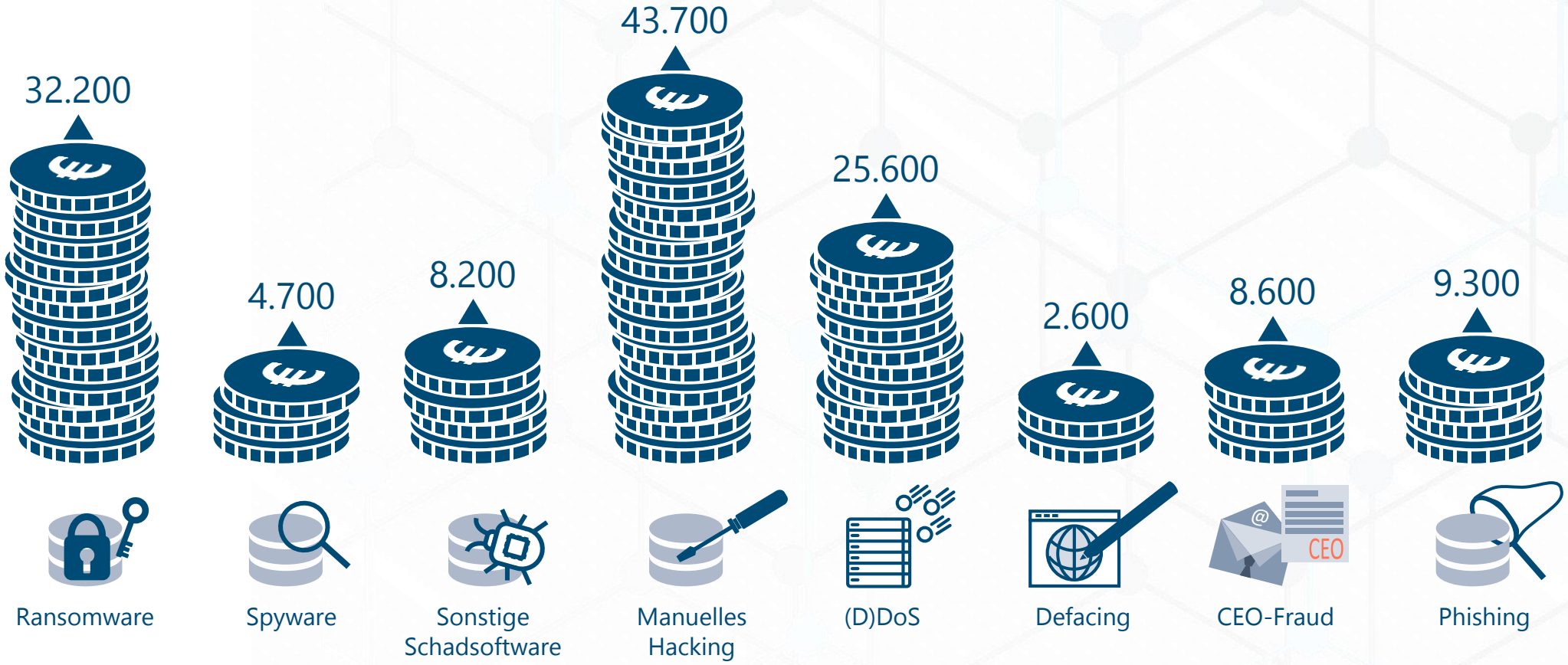


Kosten insg. klassiert in €



4.4 Folgen von Cyberangriffen

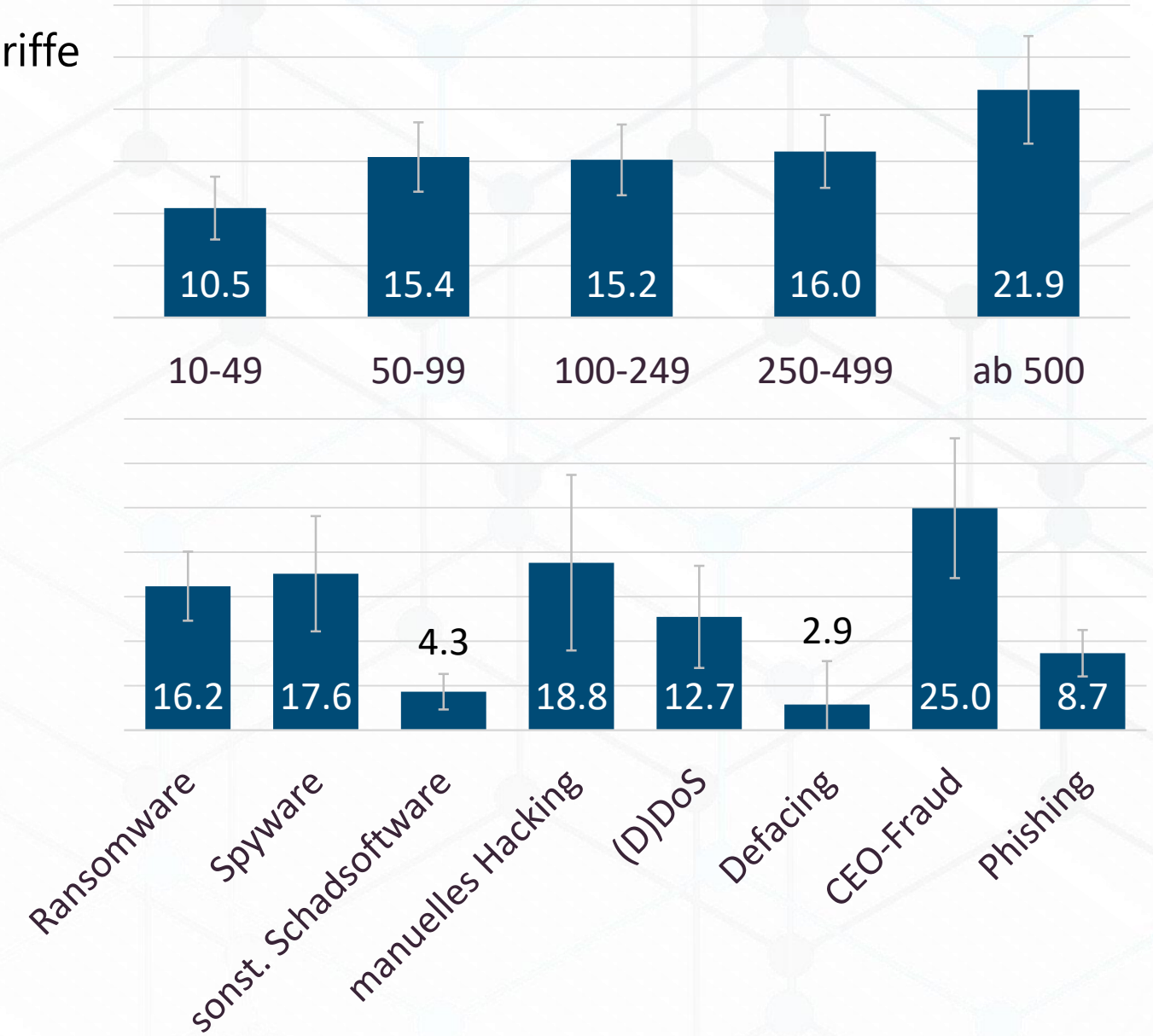
Durchschnittliche Kosten des schwerwiegendsten Cyberangriffs in EUR nach Angriffsart



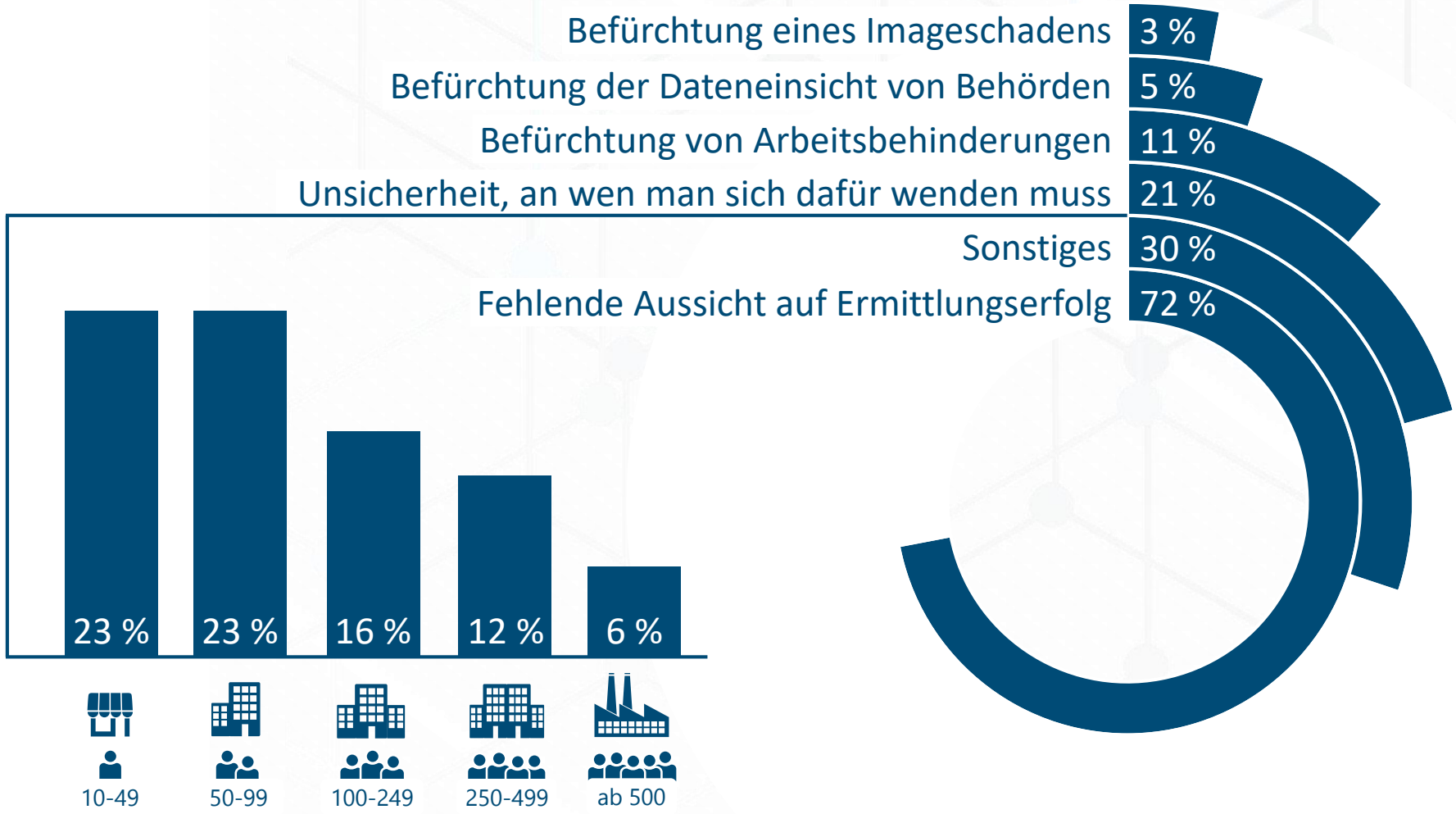
4.5 Anzeige ●○○

Anzeigequote der schwersten Cyberangriffe

(in Prozent; N=1.726)

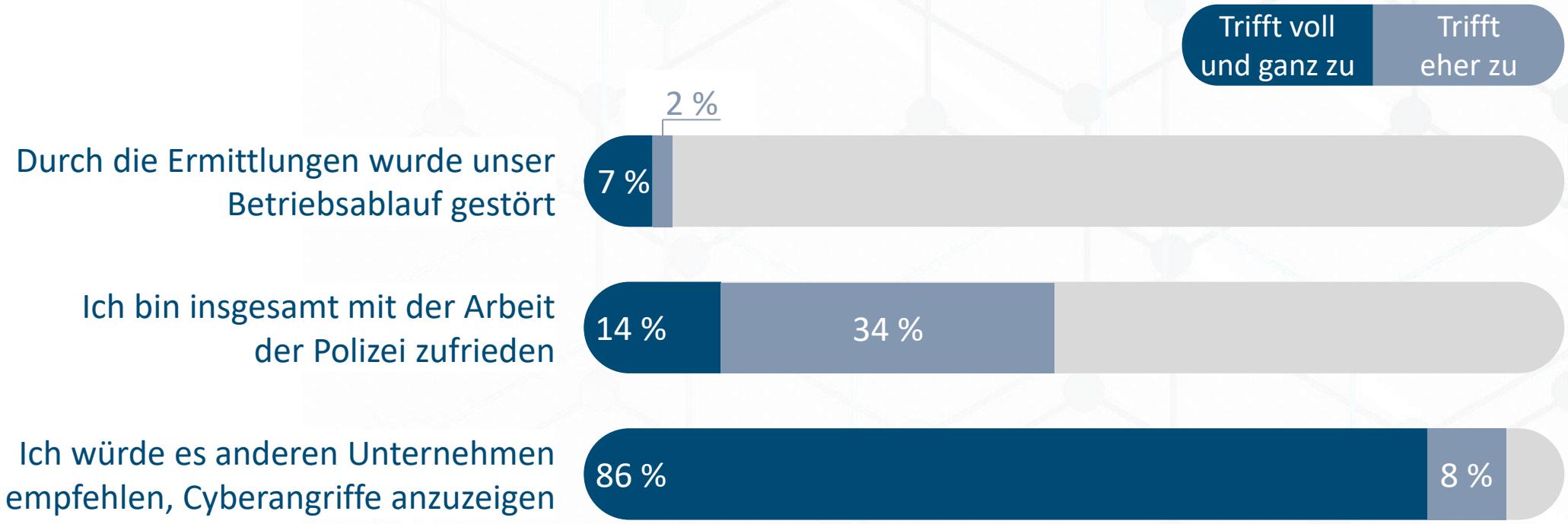


Nichtanzeigegründe (N=686)

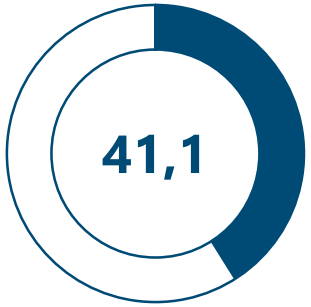


4.5 Anzeige •••

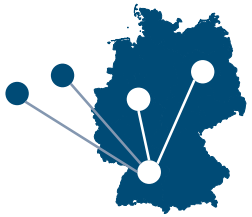
Einschätzung nach Anzeige des schwerwiegendsten Cyberangriffs



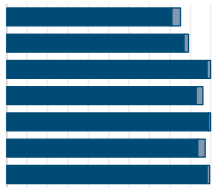
5 Resümee



- Deutsche Unternehmen sind relativ häufig von **unterschiedlichen Cyberangriffen** betroffen
  - Aber, Unternehmen sind in Prävalenzen und Auswirkungen **nicht gleichermaßen** von Cyberangriffen betroffen
    - z.B. sind große Unternehmen insgesamt häufiger betroffen als KMU (insb. von CEO-Fraud und Phishing)

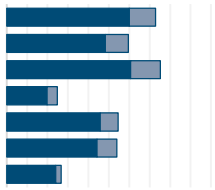


- Zu den **Risikofaktoren insb. für KMU** zählen neben der Unternehmensgröße die **Zahl der Standorte**, **Auslandsstandorte**, **Exporttätigkeit**, **besondere Produkte, Herstellungsverfahren** u.ä. sowie **besondere Reputation/ Kundenkreis**

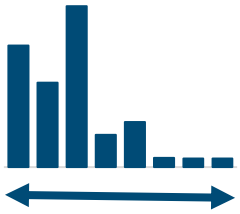


- **Technische IT-Sicherheitsmaßnahmen** sind inzwischen auch bei KMU weit verbreitet, aber deren Effektivität und mögl. qualitative Unterschiede und sind kaum erforscht
  - **Reifegrad, fachgerechte Implementierung, Anwendung und Wartung dürften eine wichtige Rolle spielen**

5 Resümee



- **Organisatorischer IT-Sicherheitsmaßnahmen** sind insbesondere bei KMU geringer verbreitet, stehen aber z.T. in Zusammenhang mit einer niedrigeren Betroffenheitsrate (insbs. Richtlinien und deren Überprüfung, Zertifizierung, Schwachstellenanalysen, Mindestanforderungen an Passwörter)
  - Der **Faktor Mensch** scheint insofern eine vergleichsweise **große Bedeutung** bei der IT- und Informationssicherheit zu spielen



- **Spannweite** entstehender direkter **finanzieller Kosten** für die Unternehmen **war sehr groß**; Gesamtkosten **in der Mehrheit aber relativ gering** (Durchschnitt: 16.900 €; Median: 1.000 €)

- Die **Anzeigequote** von Cyberangriffen ist **sehr gering** und das Dunkelfeld sehr groß
  - KMU zeigen seltener an als große Unternehmen
    - KMU wissen häufiger nicht, an wen man sich dafür wenden muss
  - Die Anzeigebereitschaft ist daneben abhängig von der Schadenshöhe und der Angriffsart

Veröffentlichungen

- https://cybercrime-forschung.de/forschung/Cyberangriffe_gegen_Unternehmen_FB.pdf

- https://cybercrime-forschung.de/forschung/Cyberangriffe_gegen_Unternehmen_kurz.pdf

Vielen Dank!

Kontakt: www.cybercrime-forschung.de
info@cybercrime-forschung.de

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

IT-Sicherheit IN DER WIRTSCHAFT

aufgrund eines Beschlusses des Deutschen Bundestages

Die Initiative „IT-Sicherheit in der Wirtschaft“ des Bundesministeriums für Wirtschaft und Energie will vor allem kleine und mittelständische Unternehmen beim sicheren Einsatz von IKT-Systemen unterstützen. Gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung soll eine Grundlage dafür geschaffen werden, um die Bewusstseinsbildung in der digitalen Wirtschaft beim Thema IT-Sicherheit im Mittelstand zu stärken. Unternehmen sollen durch konkrete Unterstützungsmaßnahmen dazu befähigt werden, ihre IT-Sicherheit zu verbessern. Weitere Informationen zur Initiative und ihren Angeboten sind unter www.it-sicherheit-in-der-wirtschaft.de abrufbar.

Zusatzförderung durch: VHV STIFTUNG pwc