

Gefördert durch:



Bundesministerium
für Wirtschaft
und Energie



IT-Sicherheit
IN DER WIRTSCHAFT

aufgrund eines Beschlusses
des Deutschen Bundestages

26. Deutscher Präventionstag, 10.05.2021

Cybercrime gegen Unternehmen

Arne Dreißigacker



KRIMINOLOGISCHES
FORSCHUNGSINSTITUT
NIEDERSACHSEN E.V.

Bennet von Skarczinski



Prof. Dr. Gina Rosa Wollinger



HSPVNRW

Zusatzförderung durch:



VHV STIFTUNG /

Gliederung

1. Forschungsprojekt und Methode
2. Prävalenz
3. Anzeigeverhalten
4. Fazit



IT-Sicherheit IN DER WIRTSCHAFT

Gefördert durch:



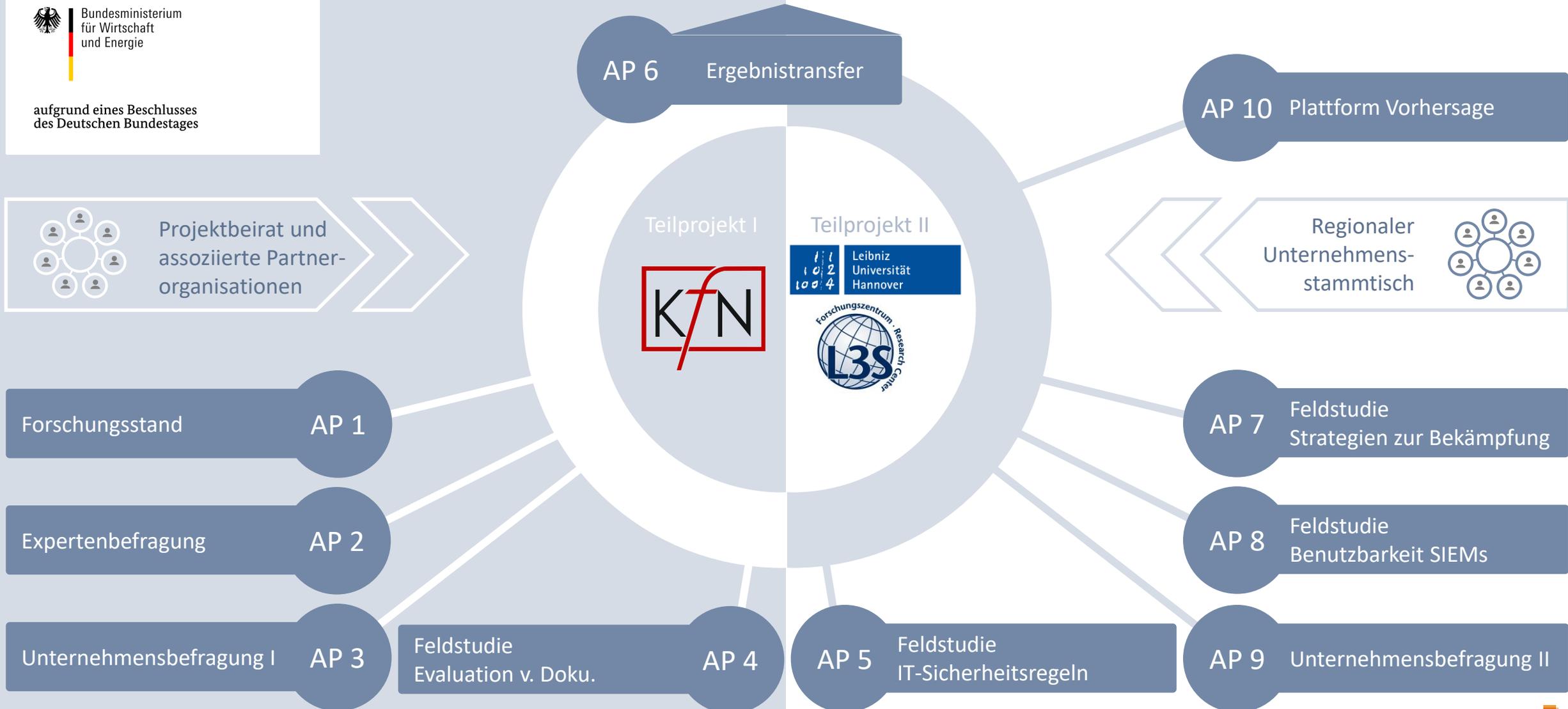
Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages



CYBERANGRIFFE GEGEN UNTERNEHMEN ARBEITSPAKETE

Förderkennzeichen: BMWi-VID5-090168623-01-1/2017
Projektlaufzeit: Dezember 2017 bis März 2021





Befragung I

- Computer Assisted Telephone Interview
 - Durchgeführt von Kantar EMNID, August 2018 bis Januar 2019



Befragung II

- Web Survey
 - Durchgeführt mit der Umfragesoftware Qualtrics, Juli 2020 bis September 2020

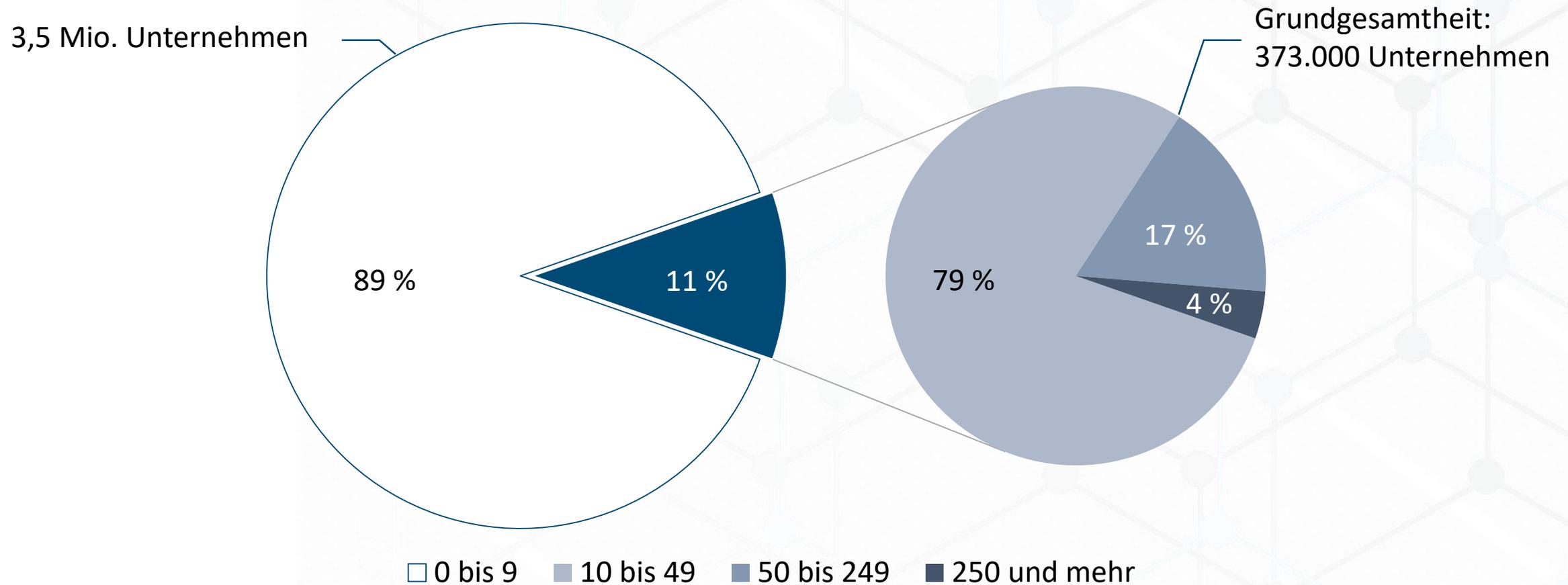


Erhebungsinstrument

- Standardisierter Fragebogen mit 40 bzw. 54 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)
 - Auswirkung der Corona-Krise auf die IT-Sicherheit

Grundgesamtheit

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



Stichprobe

Befragung I

- Disproportional geschichtete Zufallsstichprobe aus den Firmendatenbanken von Bisnode (ehemals Hoppenstedt) und Heins & Partner



Befragung II

- Folgebefragung teilnahmebereiter Unternehmen aus Befragung I

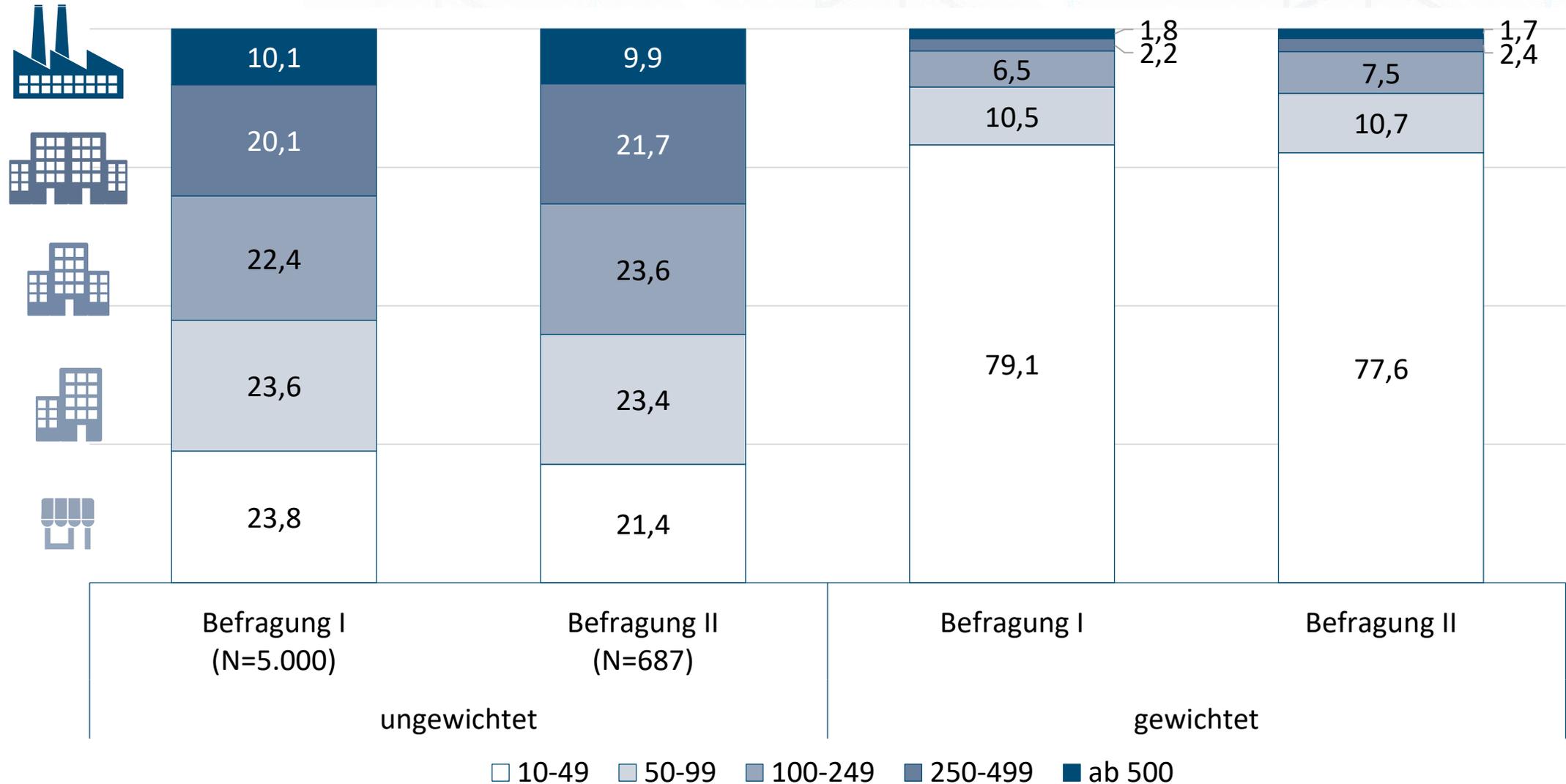
5.000 Unternehmen in Befragung I

3.431 Teilnahmebereite per E-Mail angeschrieben

759 Web Survey gestartet

687 auswertbare Fragebogen

Stichprobe



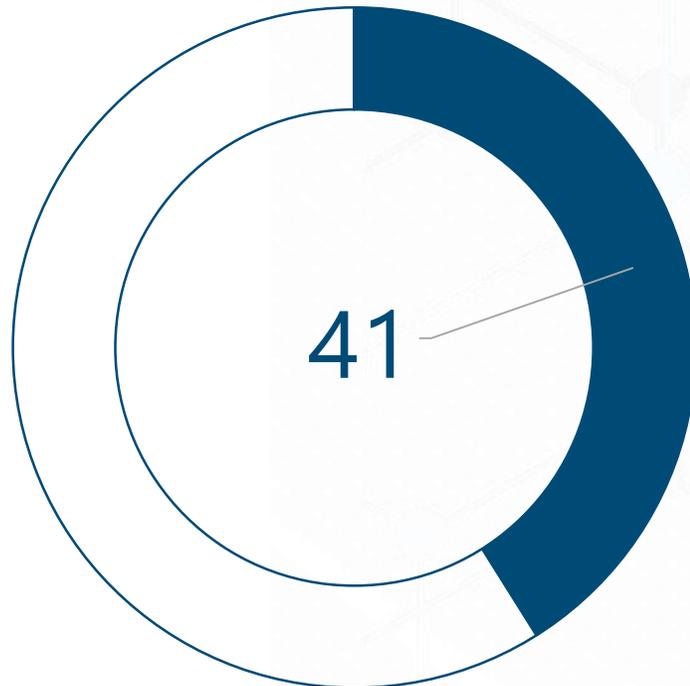
B01

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

- 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 

Befragung I: Prävalenz

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



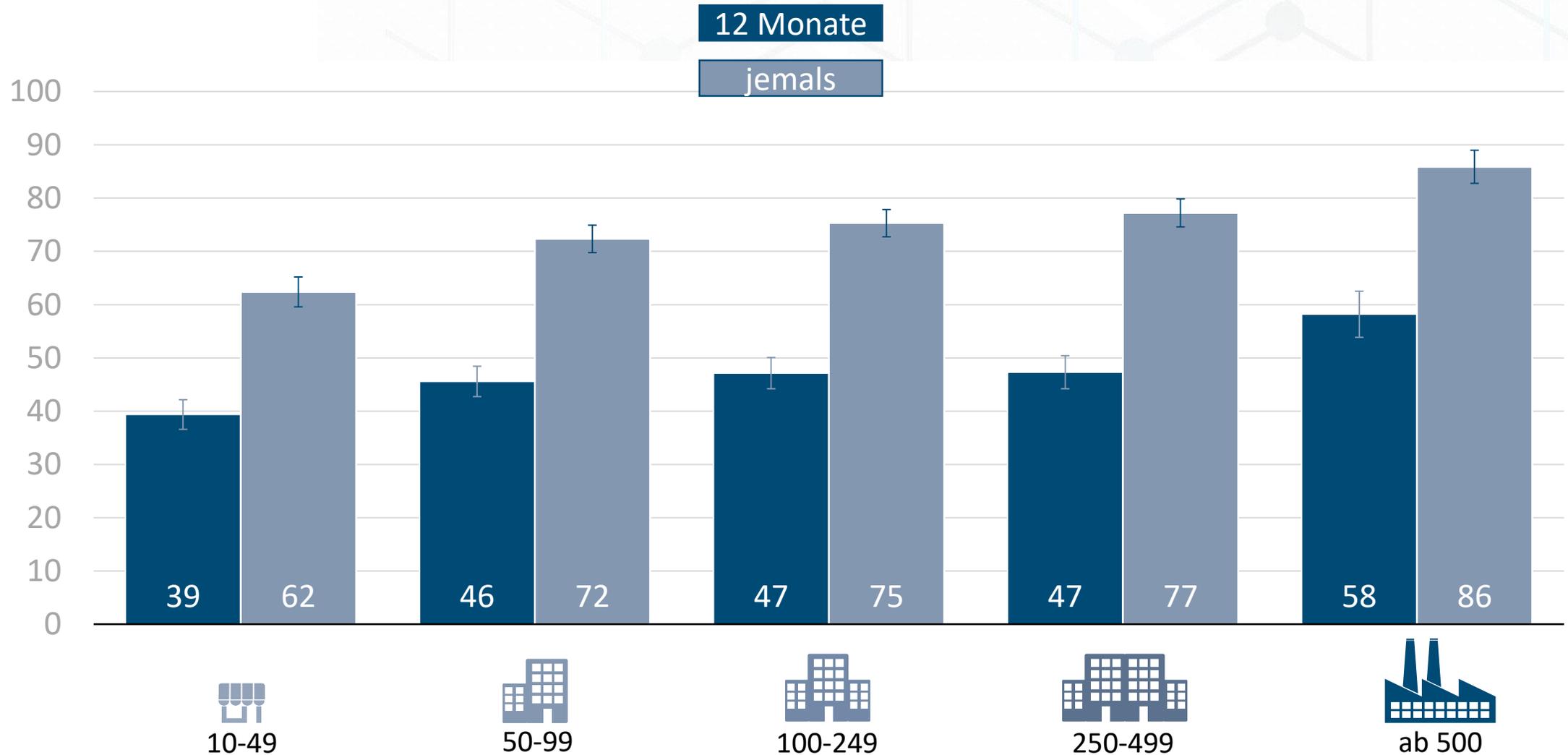
jemals
(in Prozent; N=4.844)



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

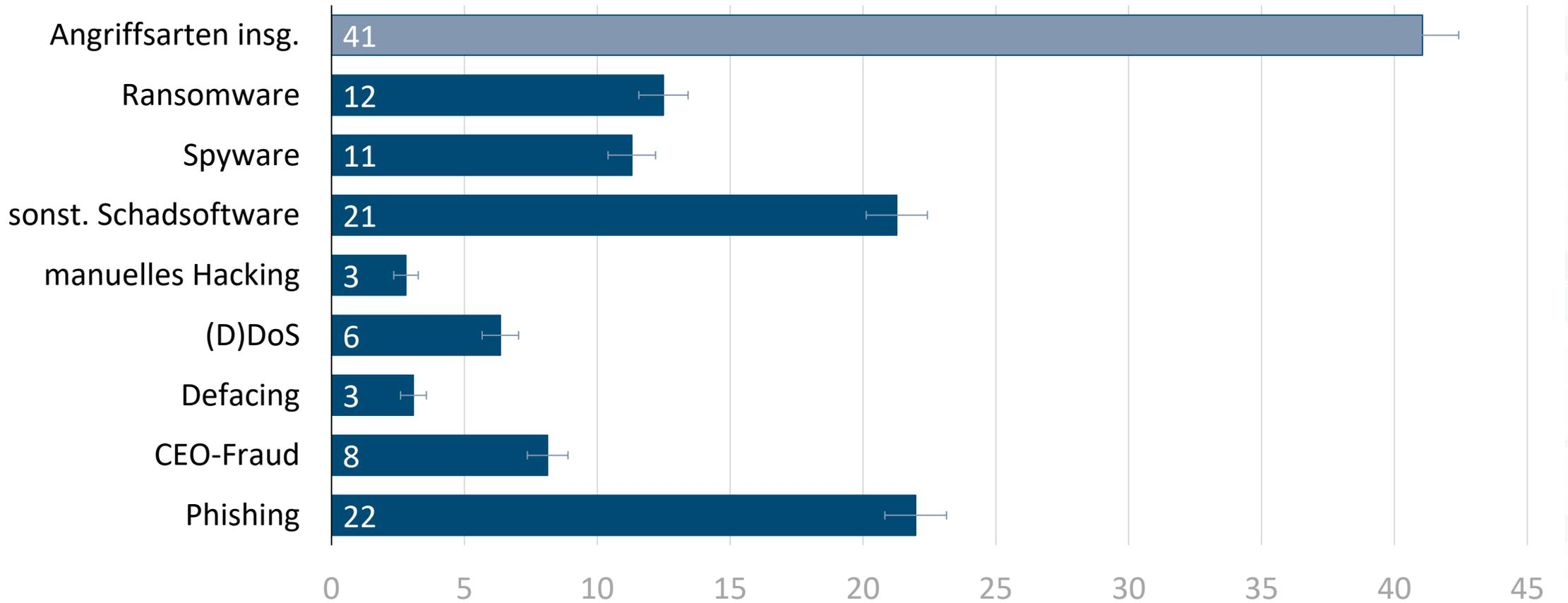
Befragung I: Jahresprävalenz nach Größe

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



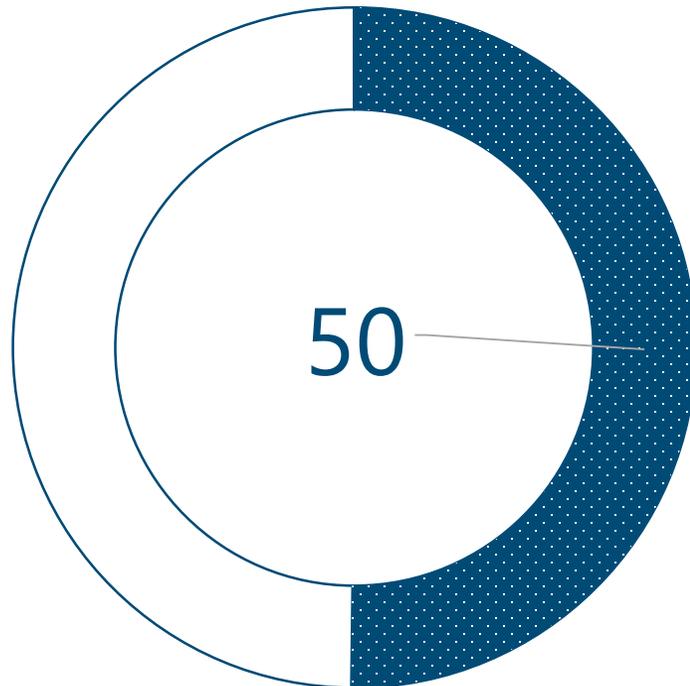
Befragung I: Jahresprävalenz nach Angriffsart

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

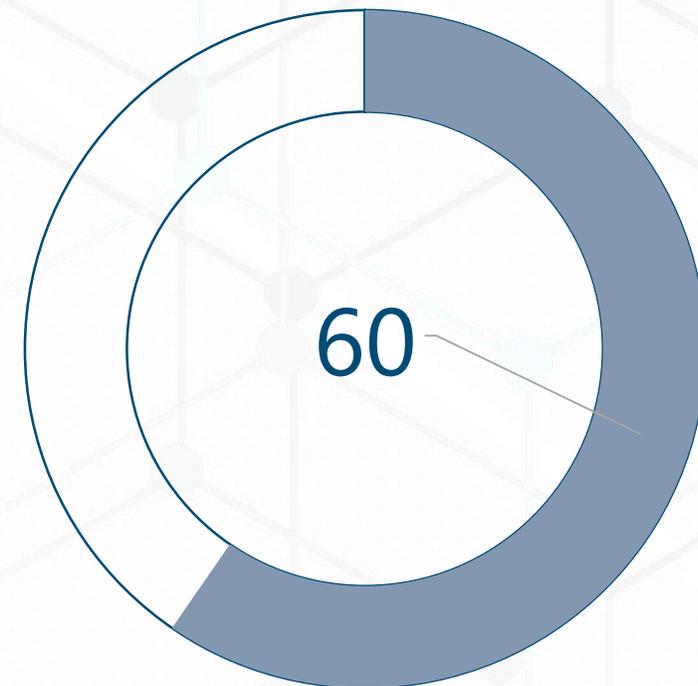


Entwicklung der Jahresprävalenz

Befragung I (2018/19)
...in den letzten 12 Monaten
(in Prozent; nur Teiln. an Befragung II; N=648)



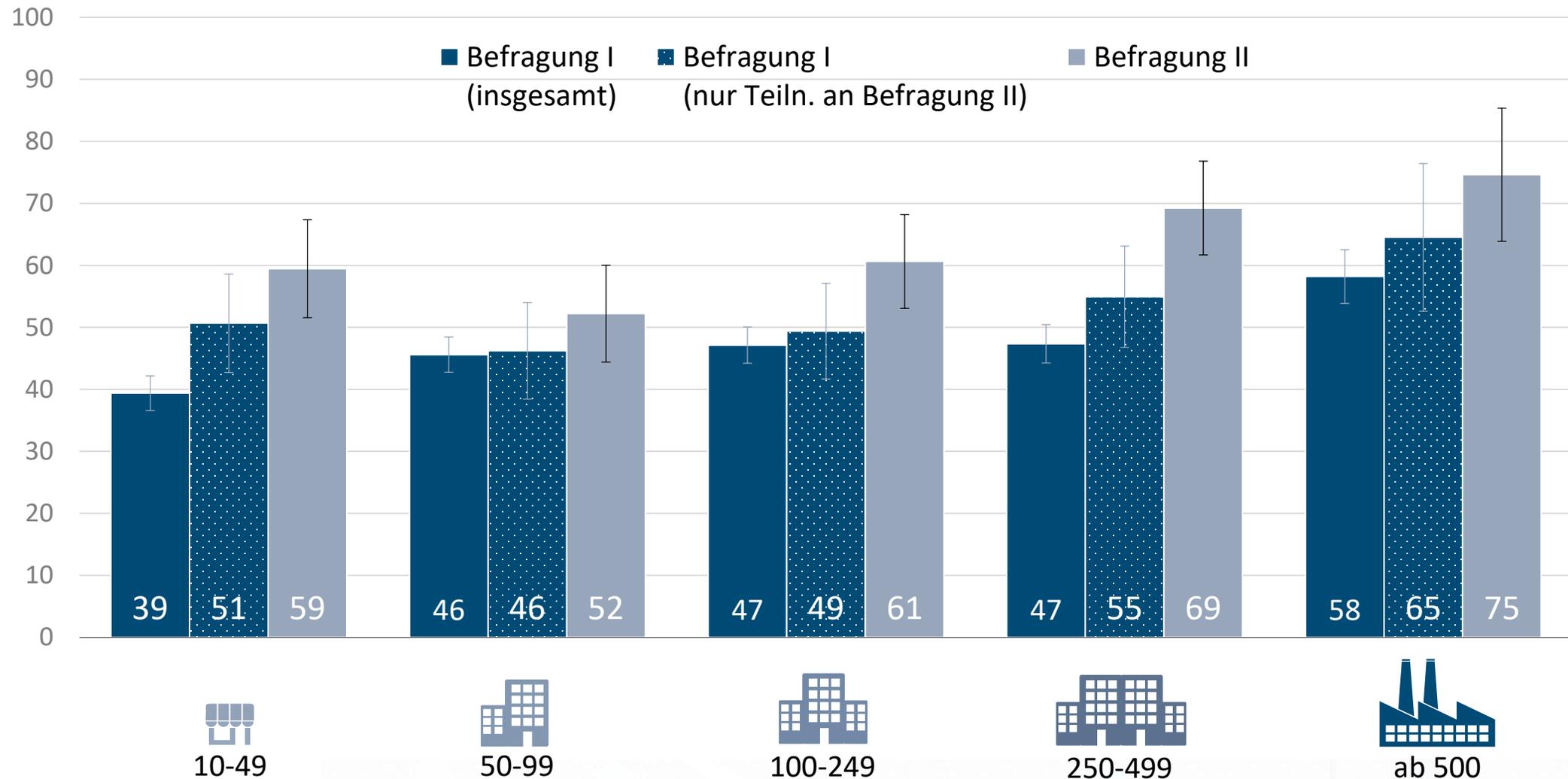
Befragung II (2020)
...in den letzten 12 Monaten
(in Prozent; N=635)



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

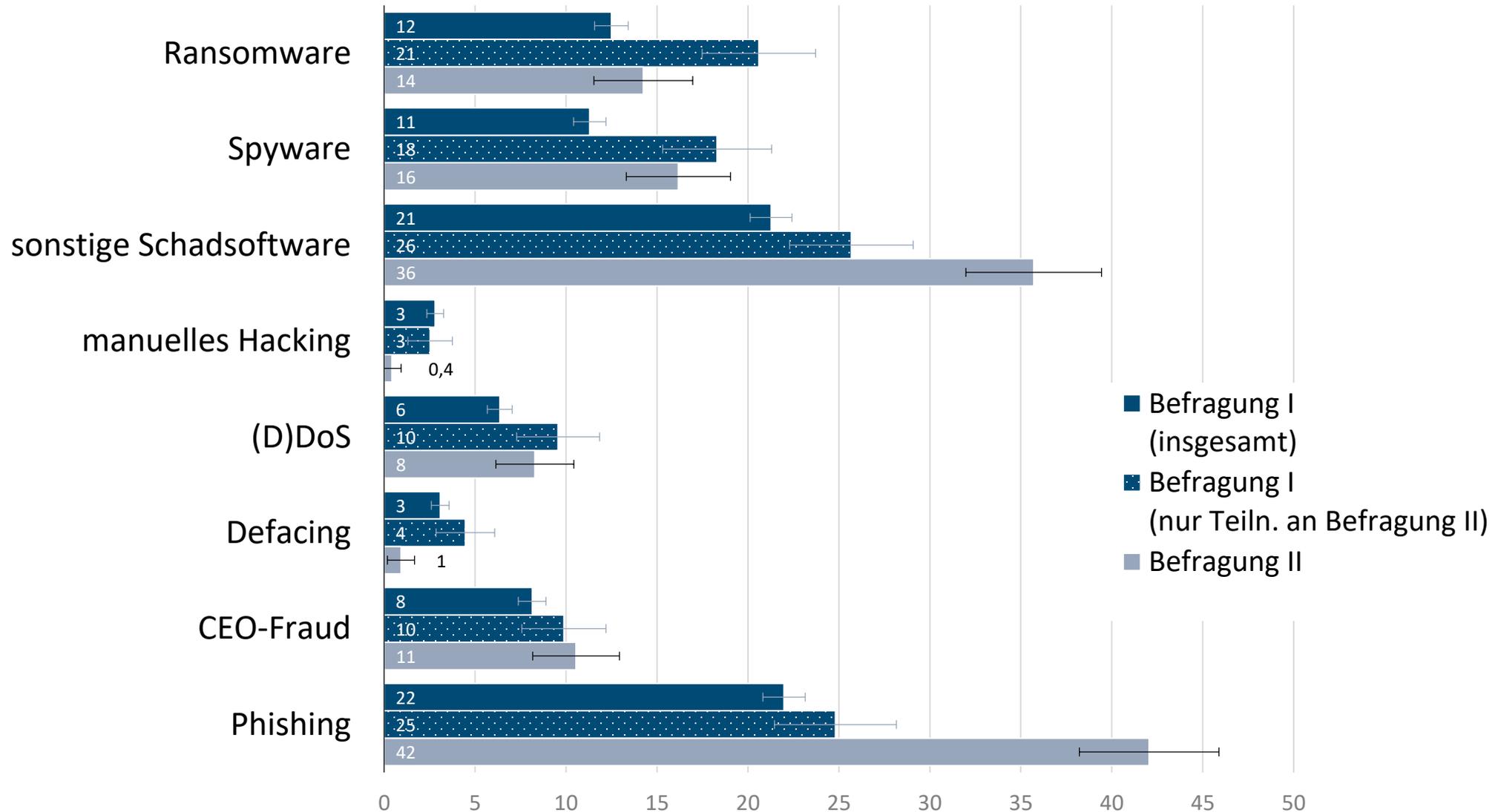
Entwicklung der Jahresprävalenz nach Größe

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



Entwicklung der Jahresprävalenz nach Angriffsart

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



Entwicklung der Anzeigequote

Befragung I (2018/19)

Anzeigequote der schwersten Cyberangriffe

(in Prozent; N=1.726)



Befragung II (2020)

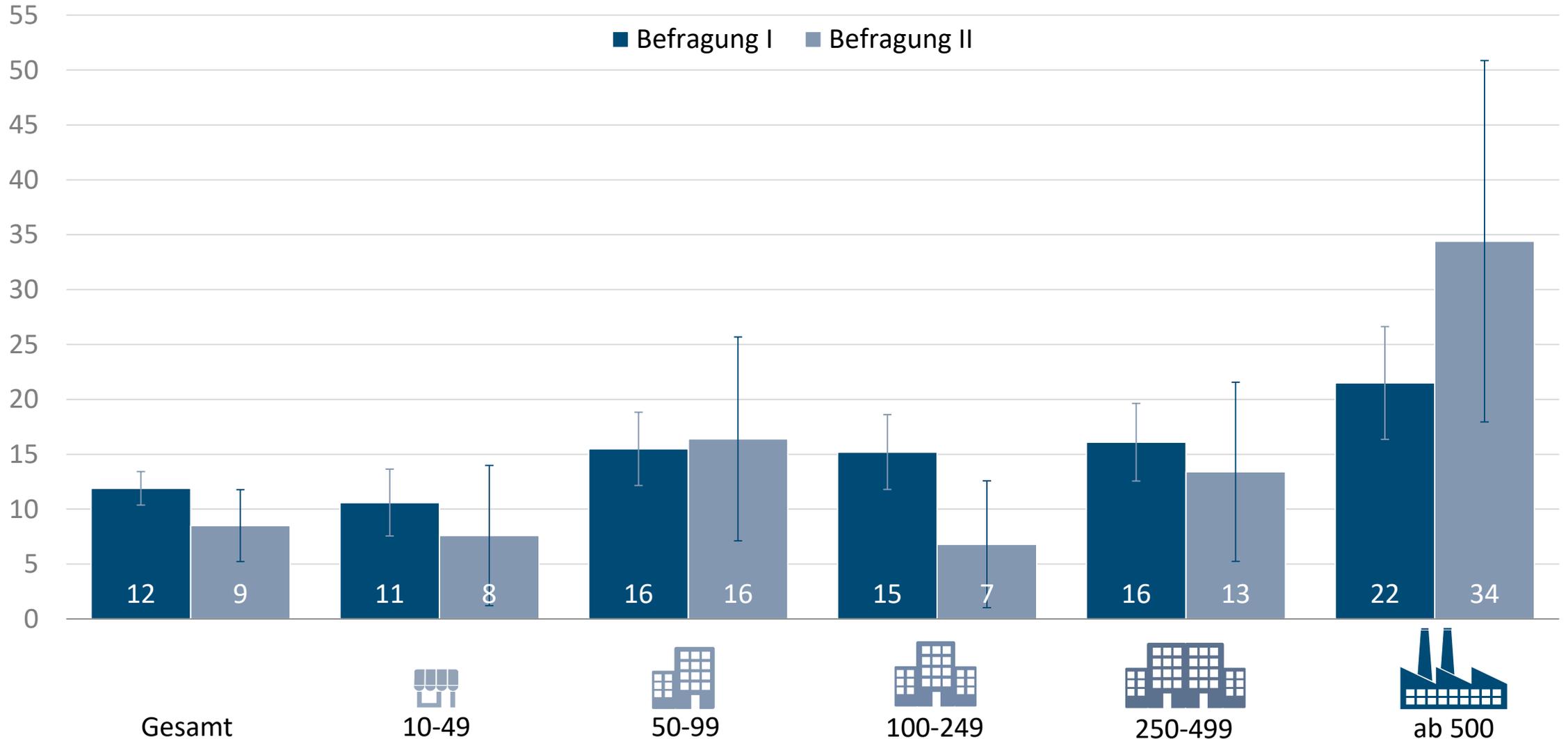
Anzeigequote der schwersten Cyberangriffe

(in Prozent; N=279)



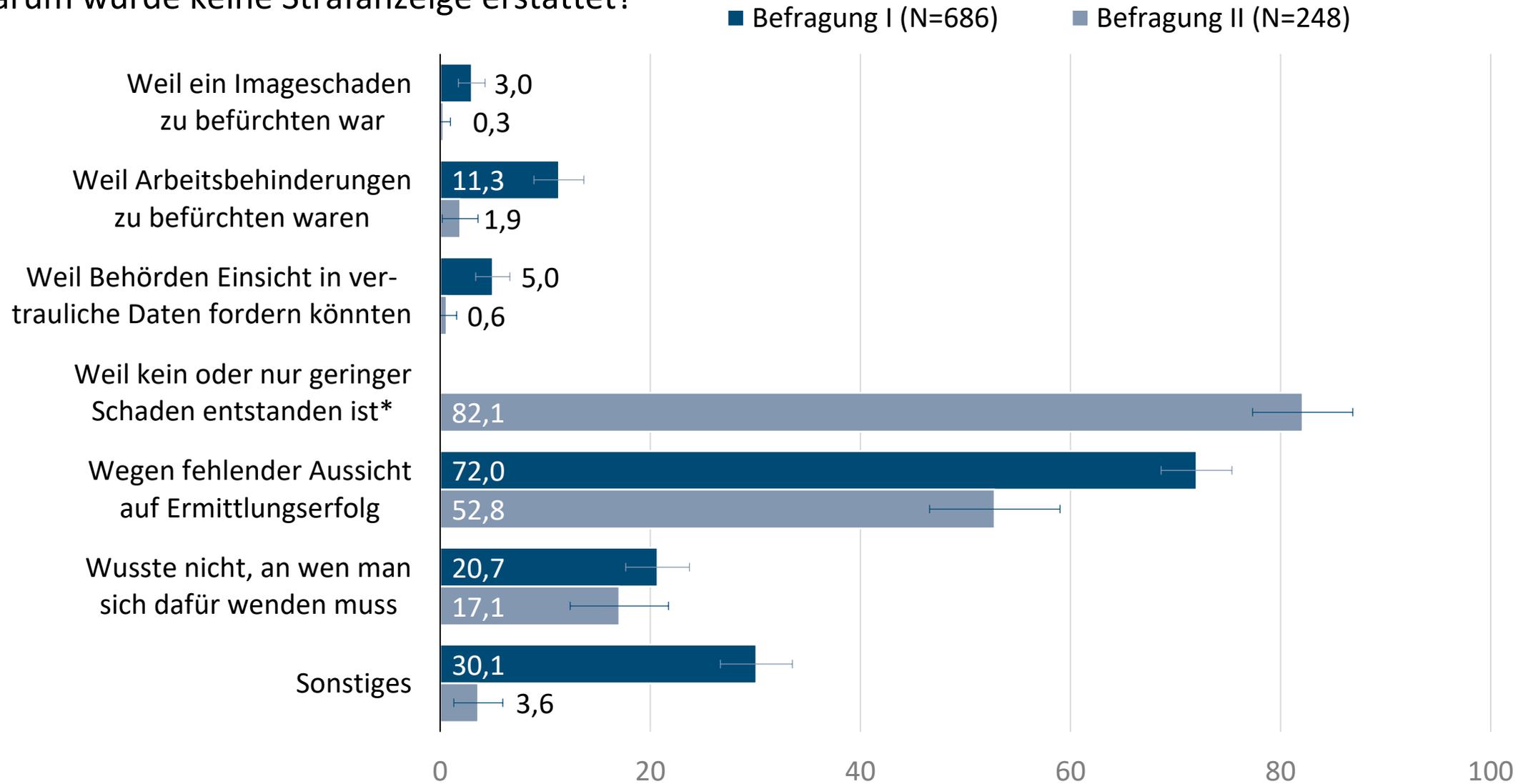
Entwicklung der Anzeigequote nach Größe

Anteile der angezeigten schwerwiegendsten Cyberangriffe (%)



Nichtanzeigegegründe

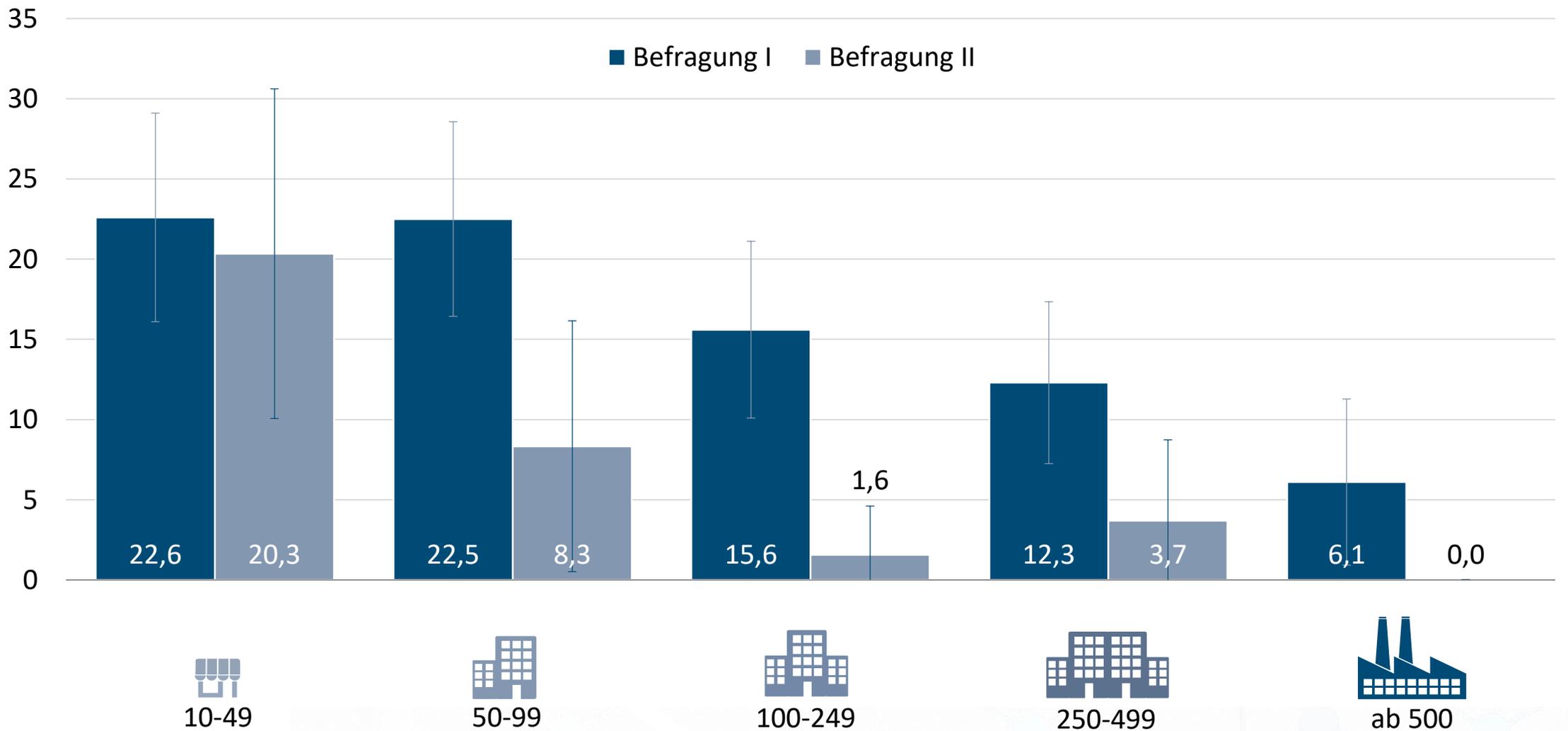
Warum wurde keine Strafanzeige erstattet?

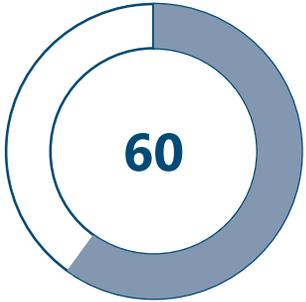


*) Antwortkategorie erst seit Befragung II

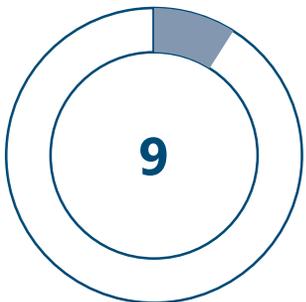
Nichtanzeigegegründe

Wusste nicht, an wen man sich dafür wenden muss (%)





- **Cyberangriffe** gegen Unternehmen (insbesondere Phishing- und Schadsoftware-Angriffe) sind **weit verbreitet und nehmen zu**
 - Thesen zu den Gründen:
 - Geringe Entdeckungswahrscheinlichkeit
 - Geringer Durchführungsaufwand
 - Hohe Lukrativität durch ungezielte und massenhafte Verbreitung von Schadsoftware
- **Technische IT-Sicherheitsmaßnahmen** sind inzwischen **weit verbreitet**, aber deren Effektivität und mögl. qualitative Unterschiede sind kaum erforscht
- **Organisatorischer IT-Sicherheitsmaßnahmen** sind insbesondere bei kleinen und mittelständischen Unternehmen **geringer verbreitet**, stehen aber z.T. in Zusammenhang mit einer niedrigeren Prävalenz
 - Der Faktor Mensch scheint insofern eine vergleichsweise große Bedeutung bei der IT- und Informationssicherheit zu spielen
- **Keine einfachen Antworten** zur Frage nach effektiven Schutzmaßnahmen
- **Anzeigequote weiterhin sehr niedrig**
 - Zu den wichtigsten Nichtanzeigegegründen zählen: die größtenteils eher geringen Schäden, die fehlende Aussicht auf Ermittlungserfolg und bei kleinen Unternehmen die Unsicherheit, an wen man sich dafür wenden muss



Ergebnisberichte

- KFN-Forschungsbericht Nr. 152
- KFN-Kurzbericht

<https://kfn.de/forschungsprojekte/cyberangriffe-gegen-unternehmen/>



Vielen Dank!

Kontakt:

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



Gefördert durch:



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/

