

A close-up photograph of a baseball in a catcher's mitt. The baseball is white with red stitching and is positioned in the center-right of the frame. The mitt is dark brown and has a mesh pocket. The background is a blurred green field.

# Wirtschaftsschutz 2024

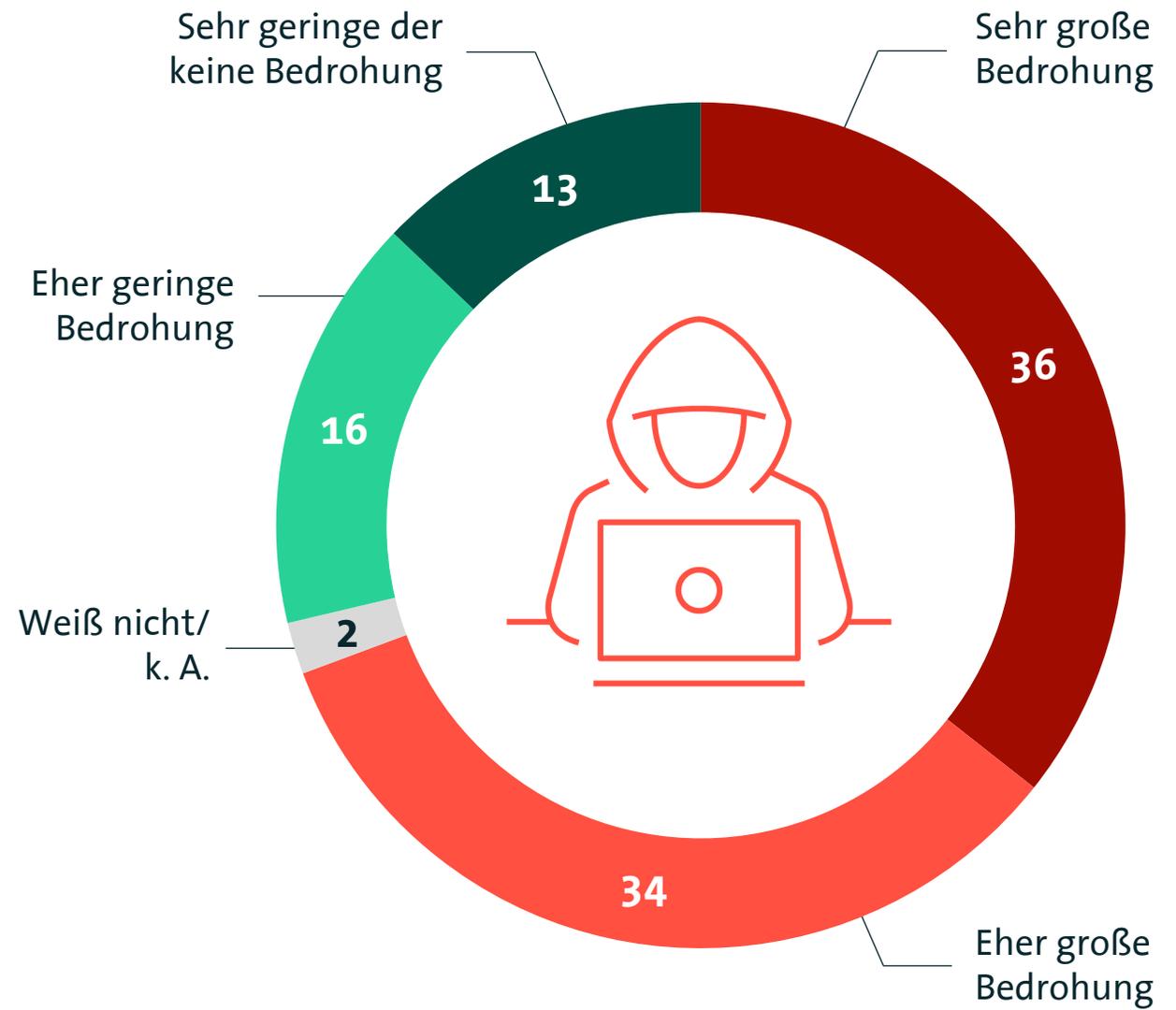
**Dr. Ralf Wintergerst**  
Bitkom-Präsident

Berlin, 28. August 2024

# 7 von 10 Unternehmen fühlen sich stark durch analoge und digitale Angriffe bedroht

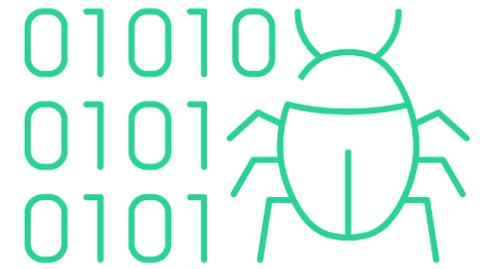
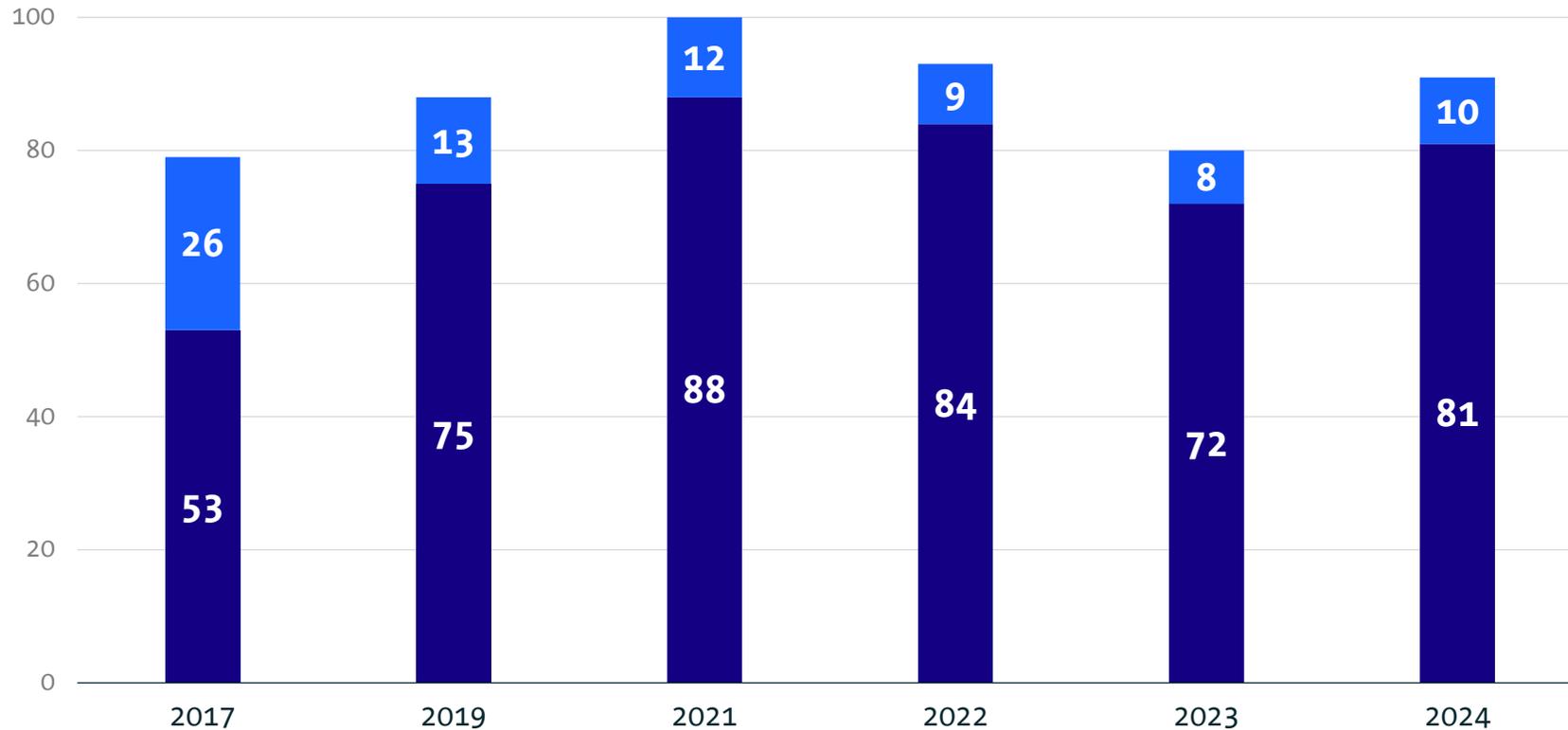
Inwieweit sehen Sie analoge und digitale Angriffe wie Datendiebstahl, Industriespionage und Sabotage als Bedrohung für Ihr Unternehmen?

in Prozent



# Wieder mehr Unternehmen von Angriffen betroffen

War Ihr Unternehmen innerhalb der letzten 12 Monate\* von Diebstahl, Industriespionage oder Sabotage betroffen?



- Vermutlich betroffen
- Betroffen

in Prozent

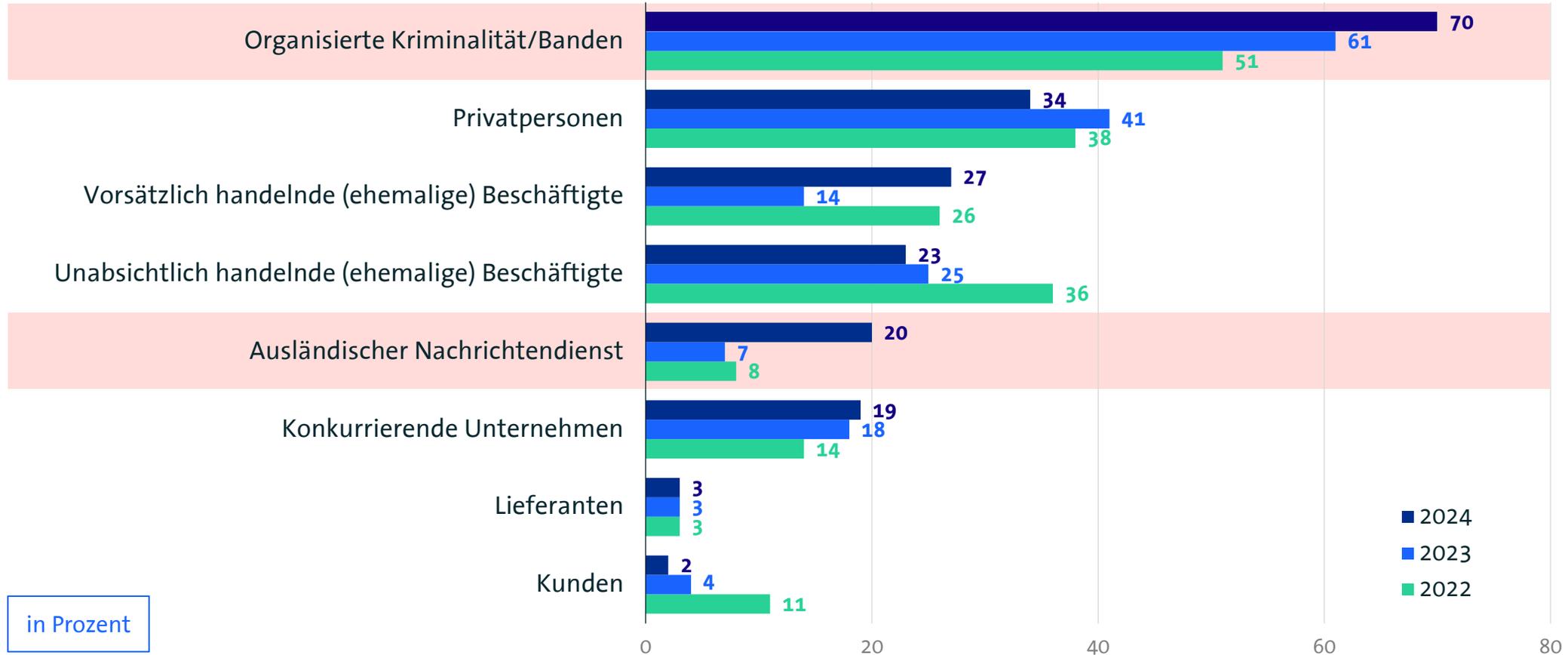
# Schaden steigt auf 266,6 Milliarden Euro

Welche Schäden sind Ihrem Unternehmen im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage entstanden?

Schaden durch...	Schadenssummen in Mrd. Euro (2024)	Schadenssummen in Mrd. Euro (2023)	Schadenssummen in Mrd. Euro (2022)
<b>Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen</b>	54,5	35,0	41,5
<b>Kosten für Rechtsstreitigkeiten</b>	53,1	29,8	16,2
<b>Umsatzeinbußen durch nachgemachte Produkte bzw. Plagiate</b>	39,2	15,3	21,1
<b>Kosten für Ermittlungen und Ersatzmaßnahmen</b>	32,2	25,2	10,1
<b>Datenschutzrechtliche Maßnahmen, z.B. durch Behörden</b>	27,2	12,4	18,3
<b>Imageschaden bei Kunden oder Lieferanten, Negative Medienberichterstattung</b>	20,2	35,3	23,6
<b>Patentrechtsverletzungen, auch vor Anmeldung</b>	14,8	10,4	18,8
<b>Erpressung mit gestohlenen Daten</b>	13,4	16,1	10,7
<b>Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen</b>	11,2	21,5	41,5
<b>Geldabfluss durch Betrugsversuche</b>	0,8	3,9	-
<b>Sonstige Schäden</b>	0	1,1	0,9
<b>Gesamtschaden pro Jahr</b>	<b>266,6</b>	<b>205,9</b>	<b>202,7</b>

# Organisierte Kriminalität und Geheimdienste greifen an

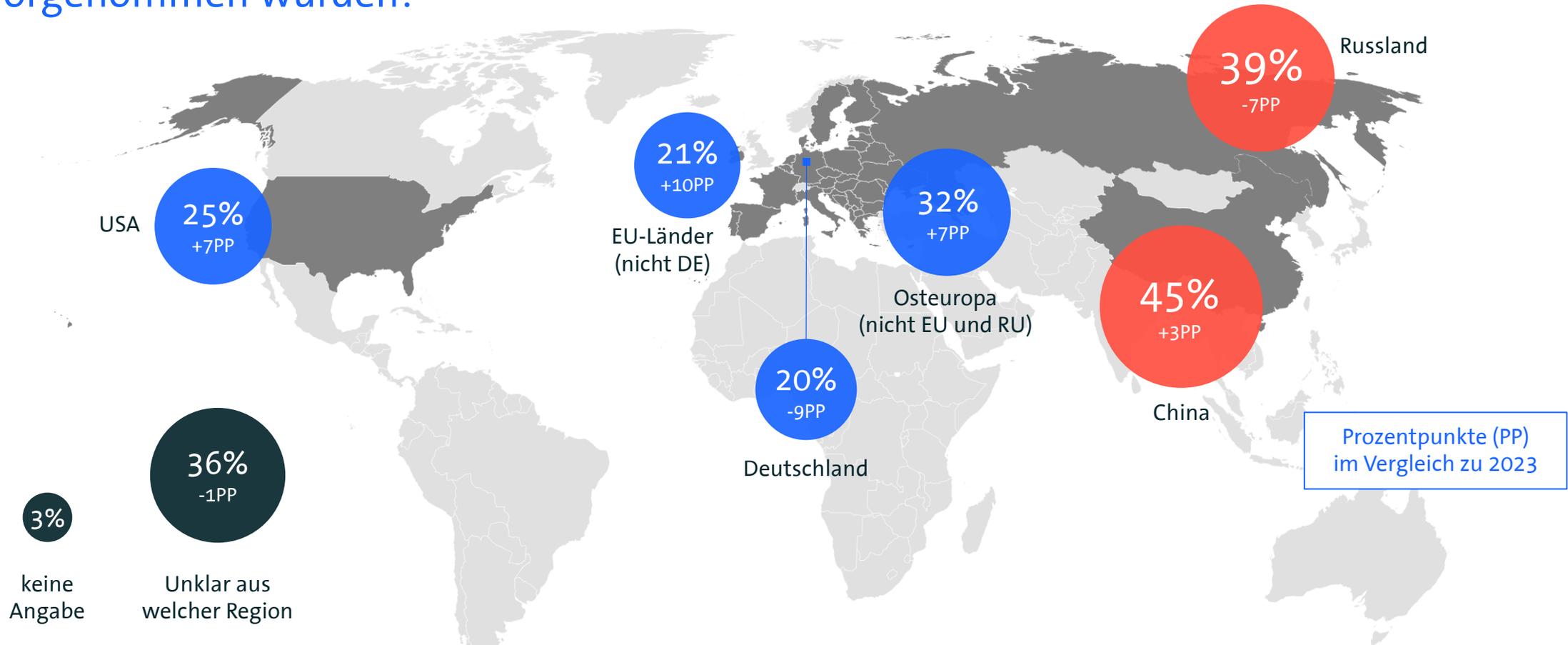
Von welchem Täterkreis gingen die Handlungen in den letzten 12 Monaten aus?



Basis: Unternehmen, die in den letzten 12 Monaten von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=812) | Mehrfachnennungen möglich |  
Quelle: Bitkom Research 2024

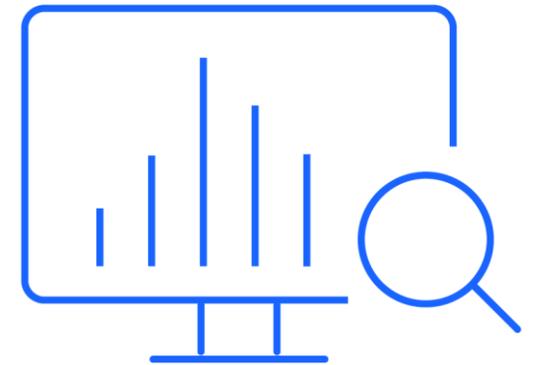
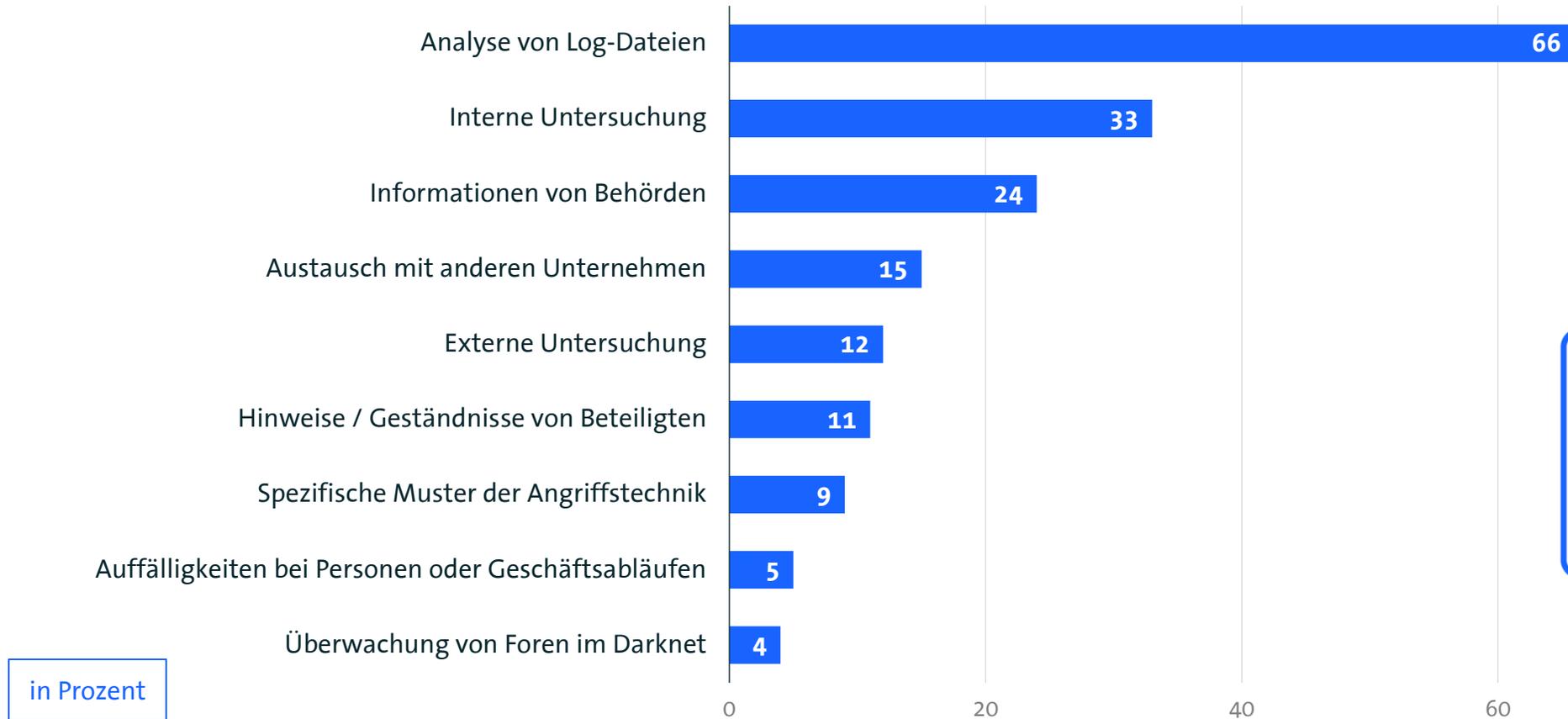
# Angriffe kommen vor allem aus China und Russland

Konnten Sie feststellen, von wo aus bzw. aus welcher Region diese Handlungen vorgenommen wurden?



# Wie Taten aufgedeckt werden

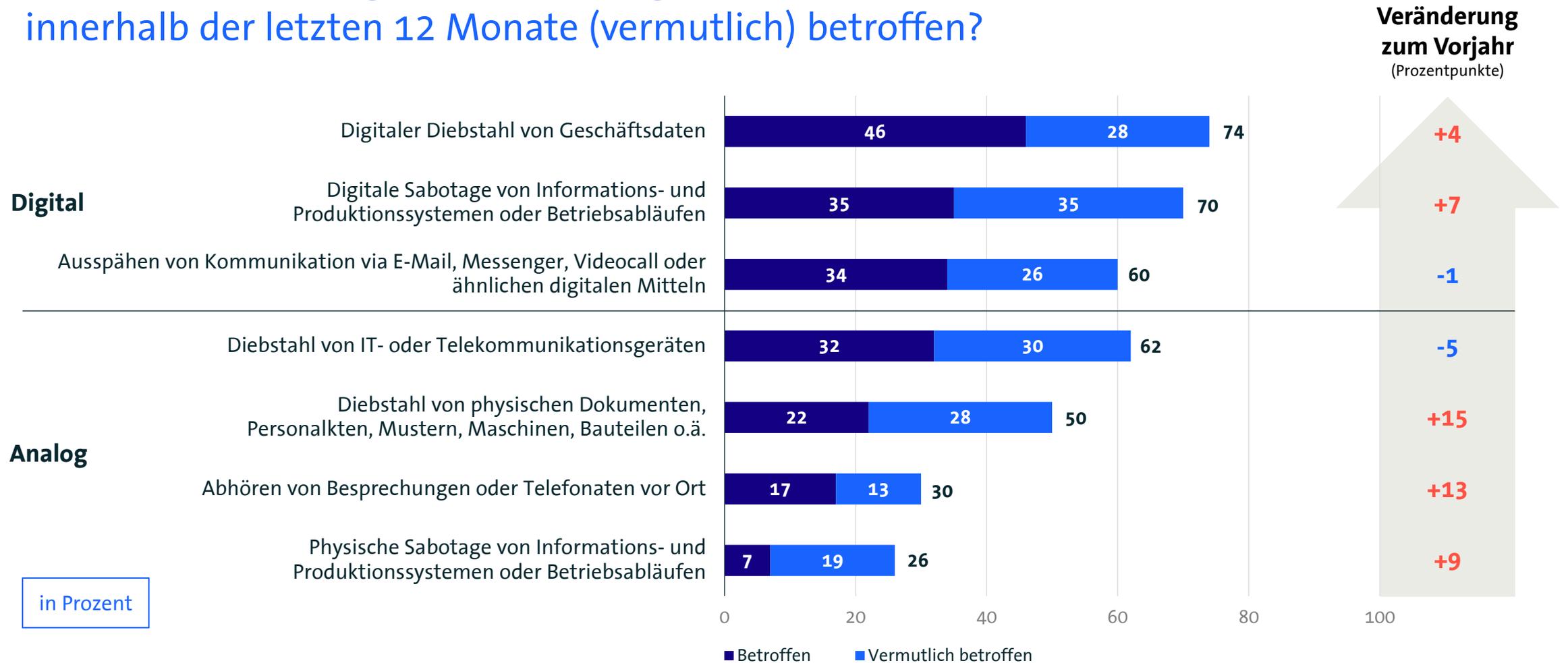
Auf welcher Grundlage haben Sie die Erkenntnisse erlangt?



Basis: Unternehmen, die in den letzten 12 Monaten von Datendiebstahl, Industriespionage oder Sabotage betroffen waren und Erkenntnisse über Herkunft, Täterkreis oder Motive hatten (n=783) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2024

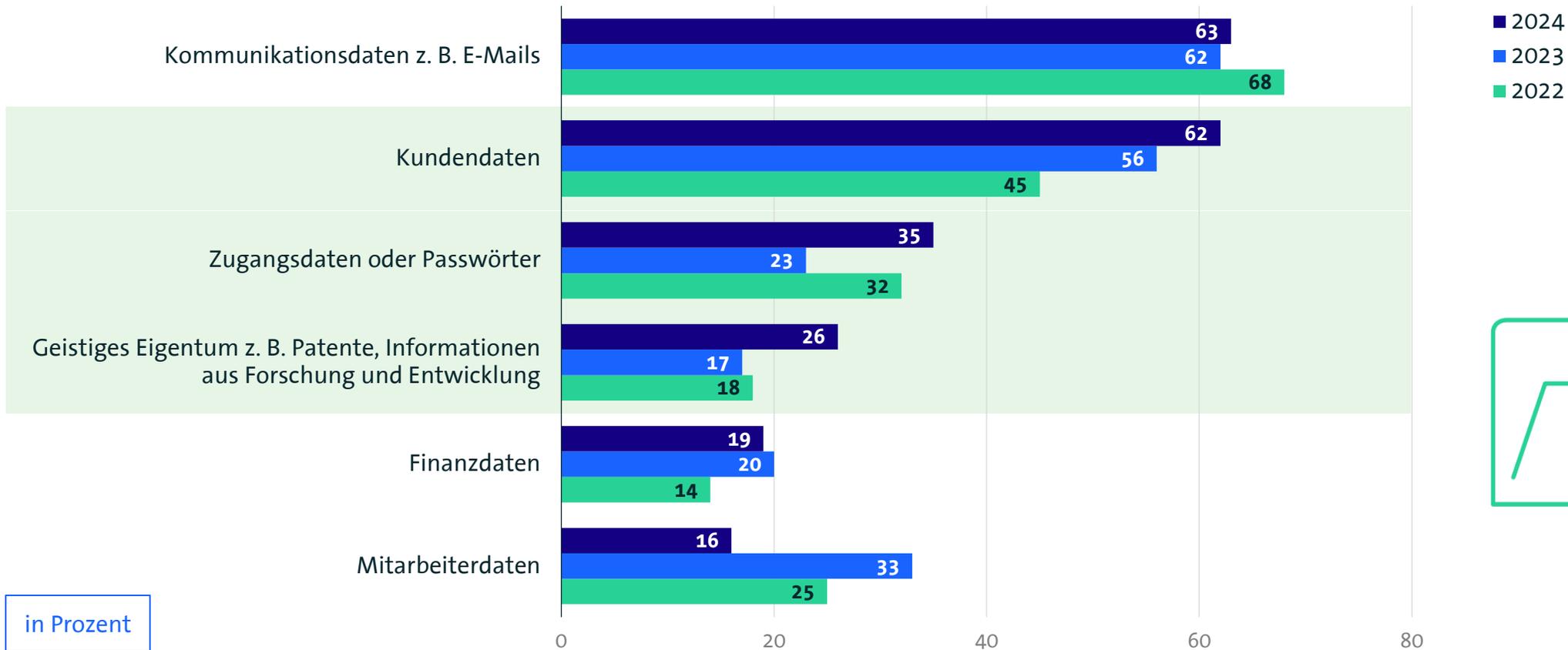
# Angriffe sind zumeist digital, nehmen aber auch analog zu

Von welchen der folgenden Handlungen war Ihr Unternehmen innerhalb der letzten 12 Monate (vermutlich) betroffen?



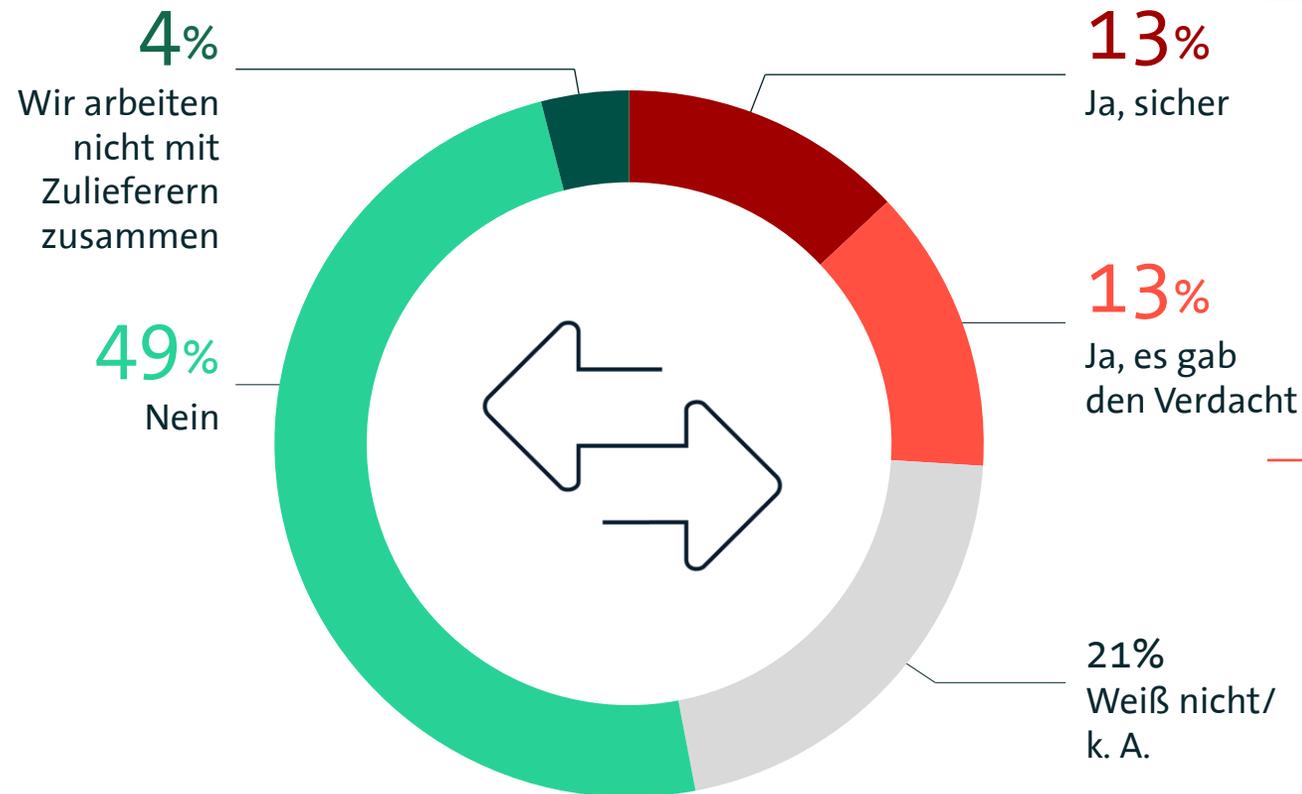
# Datendiebstahl: Kunden, Passwörter und Patente im Fokus

Welche der folgenden Arten von digitalen Daten wurden in Ihrem Unternehmen gestohlen?

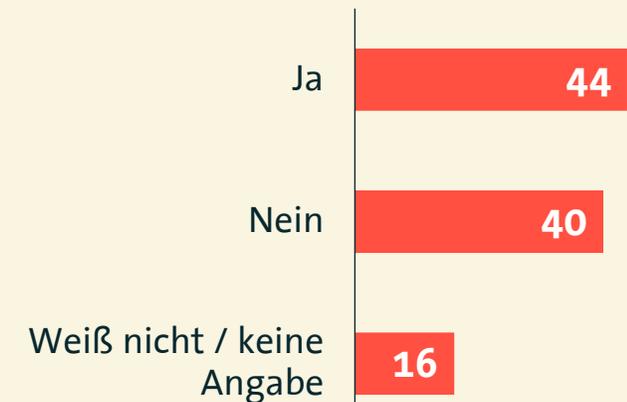


# Zulieferer als Einfallstor für Angriffe

Waren Zulieferer Ihres Unternehmens innerhalb der letzten 12 Monate von Datendiebstahl, Industriespionage oder Sabotage betroffen?

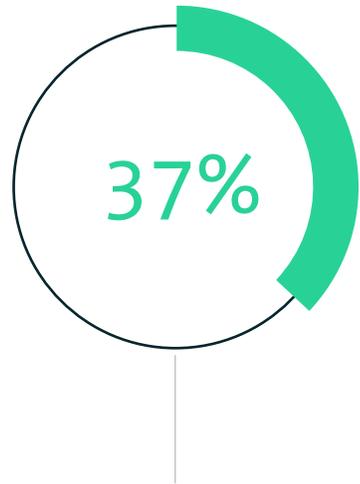


Hatte dies Folgen für Ihr Unternehmen, z.B. Produktionsausfälle, Lieferengpässe, Reputationsschäden?



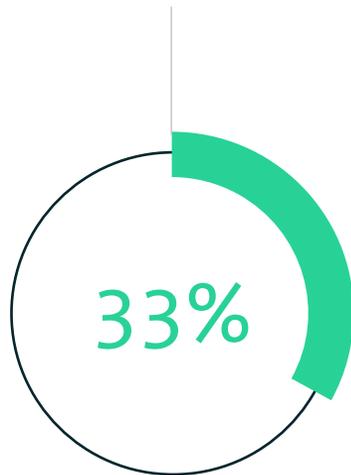
# Die Lieferkette ist nur selten im Blick

Welche Aussagen treffen auf Ihr Unternehmen im Hinblick auf die Lieferkette zu?

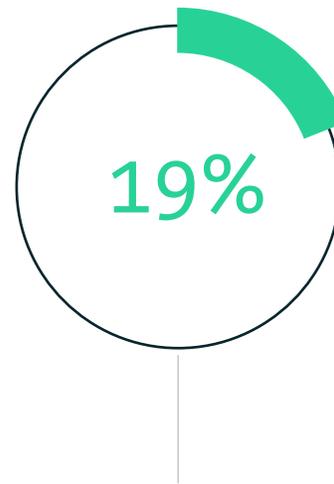


Wir haben **einen Notfallplan**, wie wir auf Sicherheitsvorfälle in unserer Lieferkette reagieren.

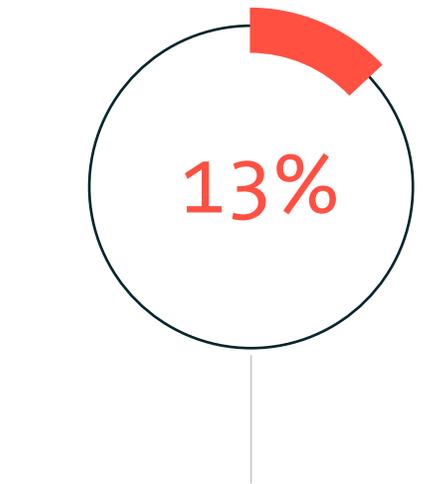
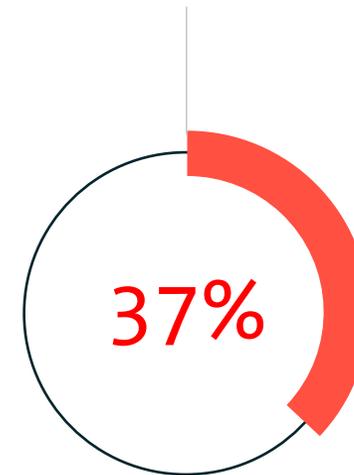
Wir stehen in **engem Austausch mit unseren Zulieferern**, um das Risiko von Angriffen innerhalb der Lieferkette zu minimieren.



Wir führen **regelmäßig Sicherheitsbewertungen** bei Zulieferern durch, um das Risiko von Angriffen zu minimieren.



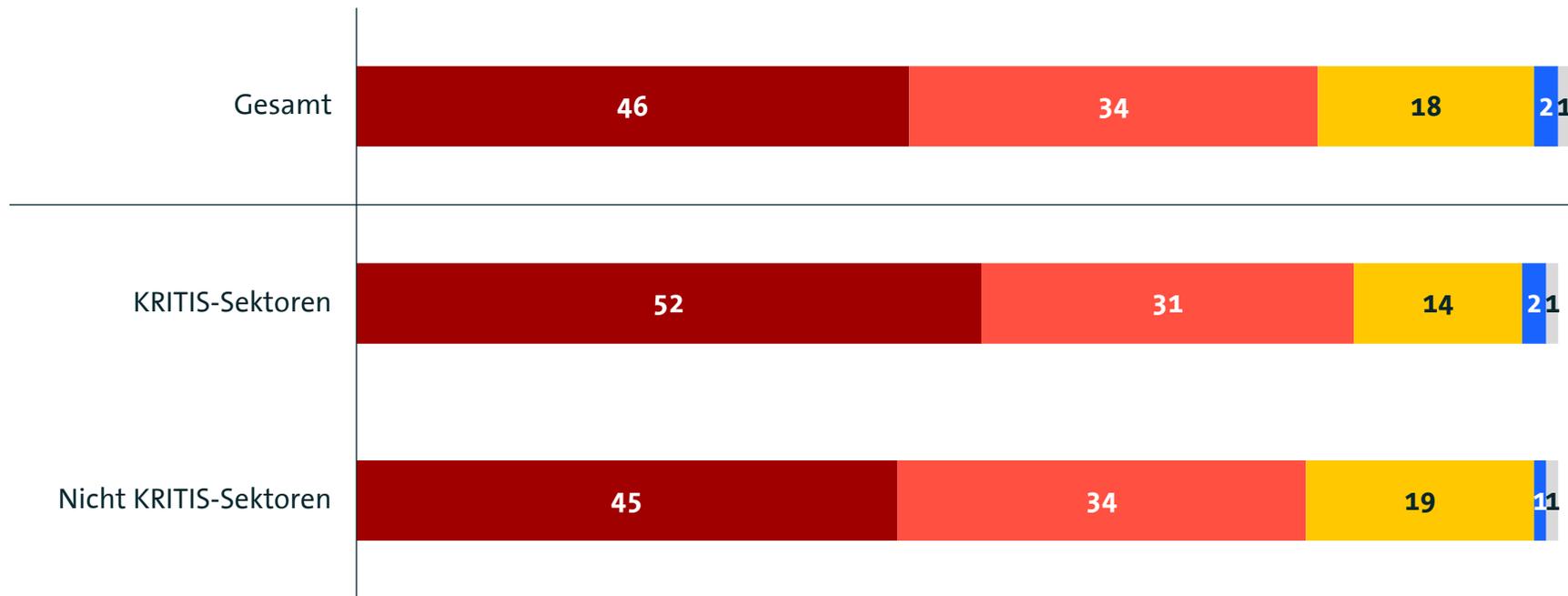
In unserem Unternehmen **fehlt das Bewusstsein** für die Risiken von Angriffen innerhalb der Lieferkette.



Uns bereitet Sorge, dass Zulieferer **nicht dieselben Sicherheitsstandards** wie wir einhalten und so zum Einfallstor für Angriffe werden.

# Cyberangriffe auf Unternehmen nehmen weiter zu

Wie hat sich die Anzahl der Cyberattacken auf Ihr Unternehmen in den vergangenen 12 Monaten entwickelt?



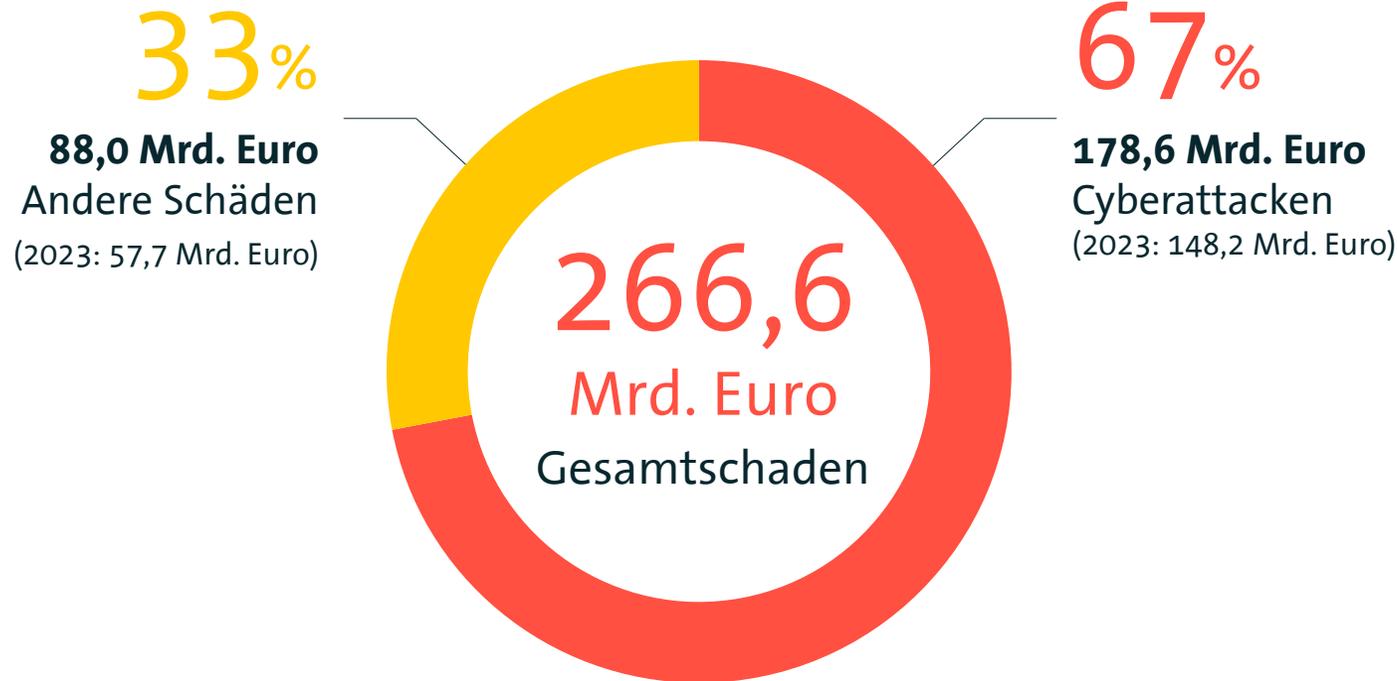
in Prozent

- Haben stark zugenommen
- Haben eher zugenommen
- Unverändert
- Haben eher abgenommen
- Haben stark abgenommen
- Weiß nicht/keine Angabe

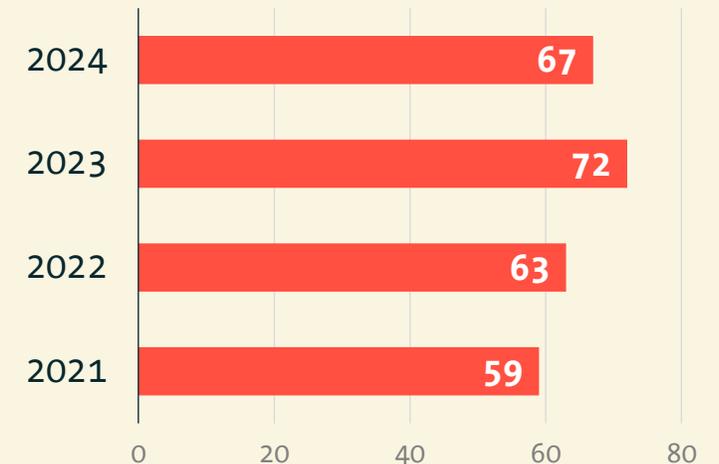


# Cyberattacken verursachen zwei Drittel der Schäden

Wie hoch ist der prozentuale Anteil des entstandenen Gesamtschadens, der auf Cyberattacken zurückgeführt werden kann?



Anteil Cyberattacken an Gesamtschäden  
2021-24



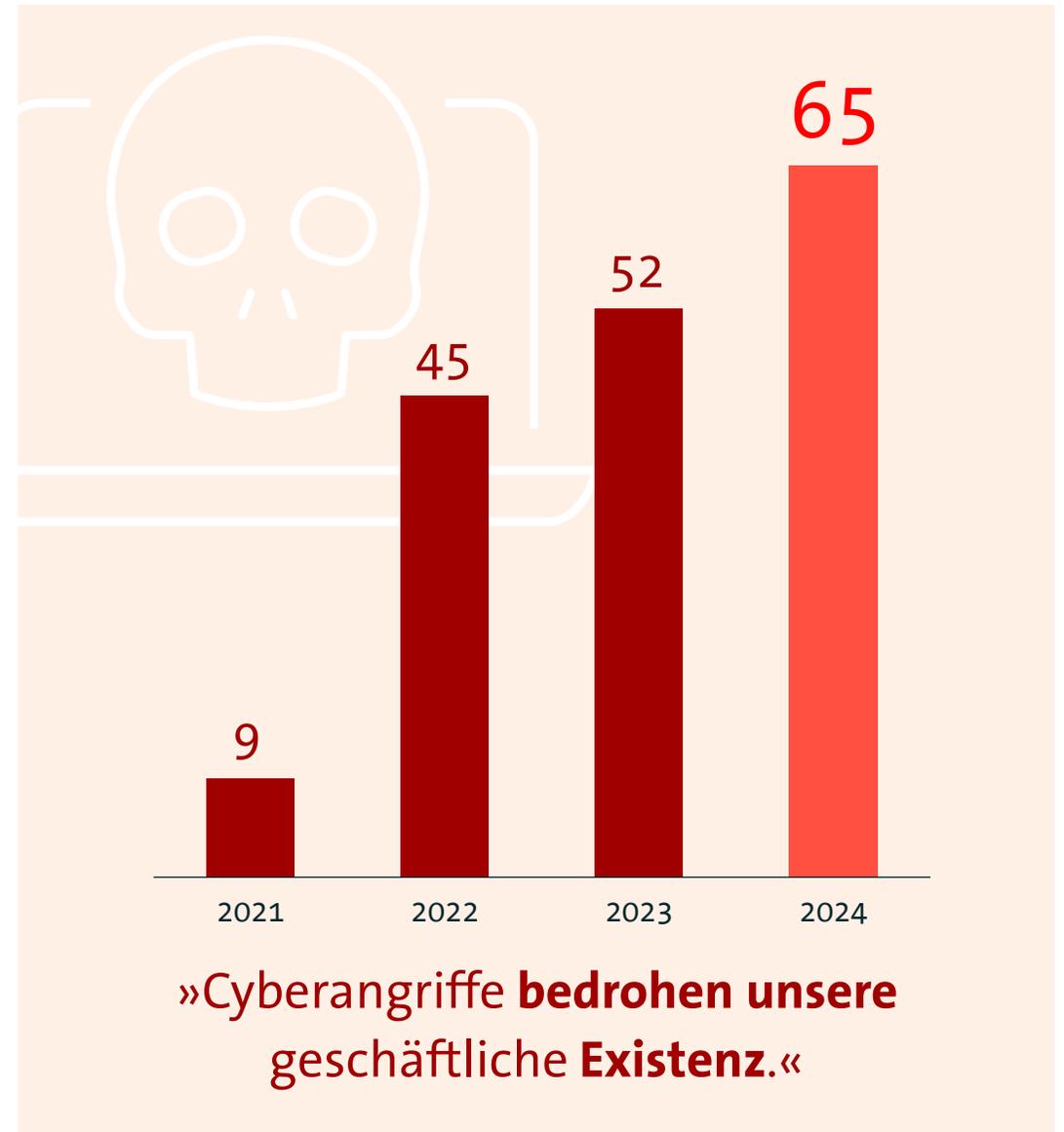
# Zwei Drittel der Unternehmen sehen sich durch Cyberattacken in ihrer Existenz bedroht

Inwieweit treffen die folgenden Aussagen zu?

53%

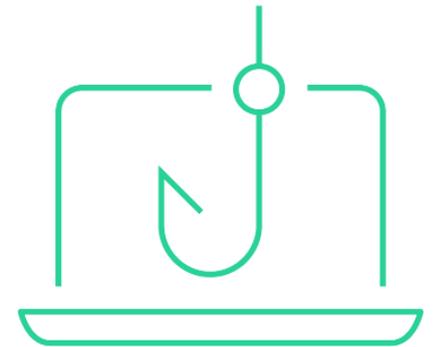
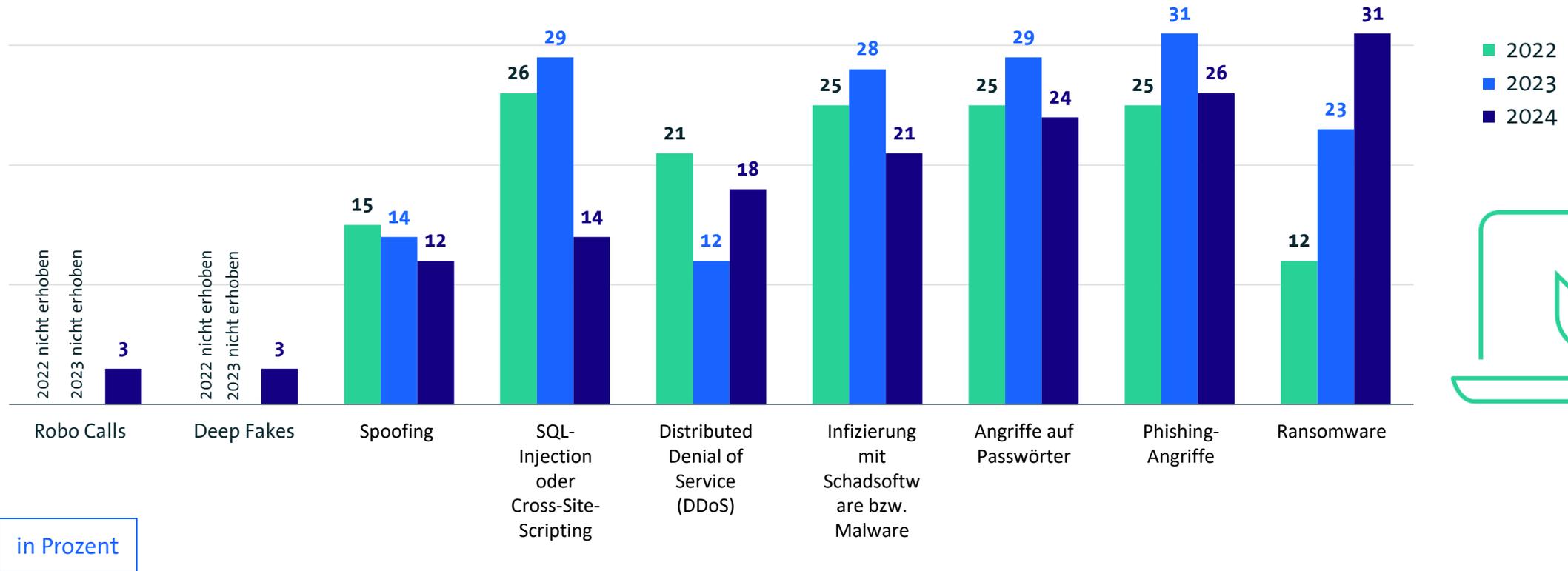
»Unser Unternehmen ist auf Cyberangriffe **sehr gut vorbereitet.**«

in Prozent



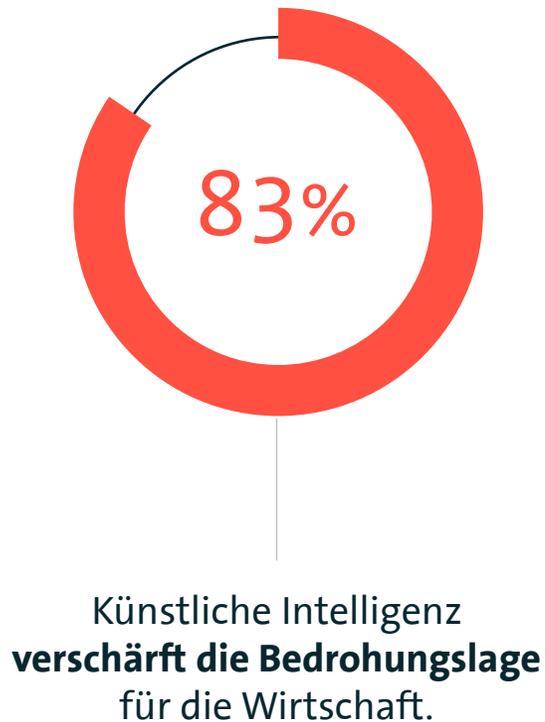
# Ransomware verursacht häufiger Schäden

Welche der folgenden Arten von Cyberangriffen haben innerhalb der letzten 12 Monate in Ihrem Unternehmen einen Schaden verursacht?

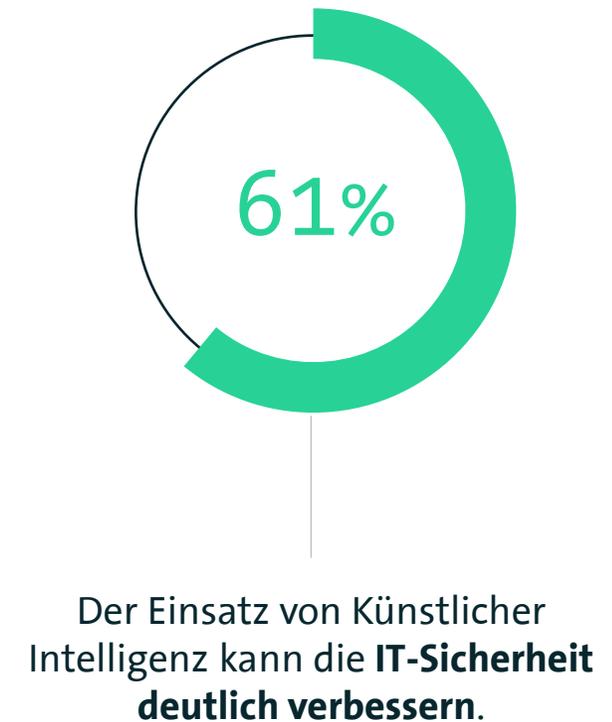
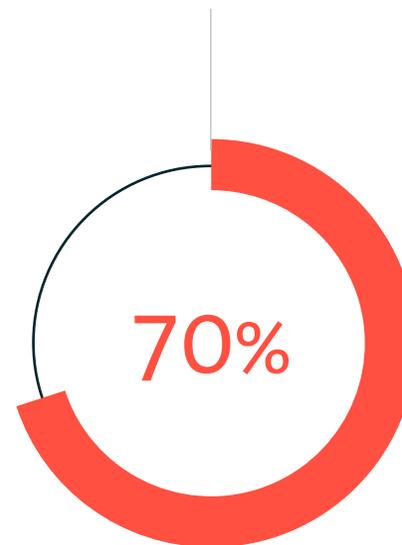


# KI gilt als Gefahr für IT-Sicherheit – aber auch als Chance

Inwieweit treffen die folgenden Aussagen zu?

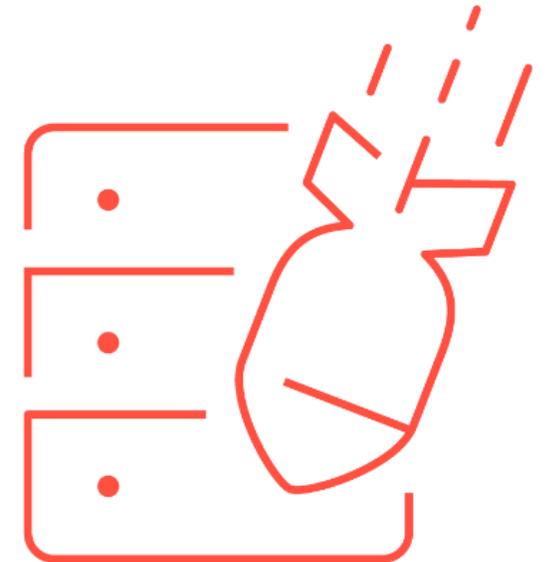
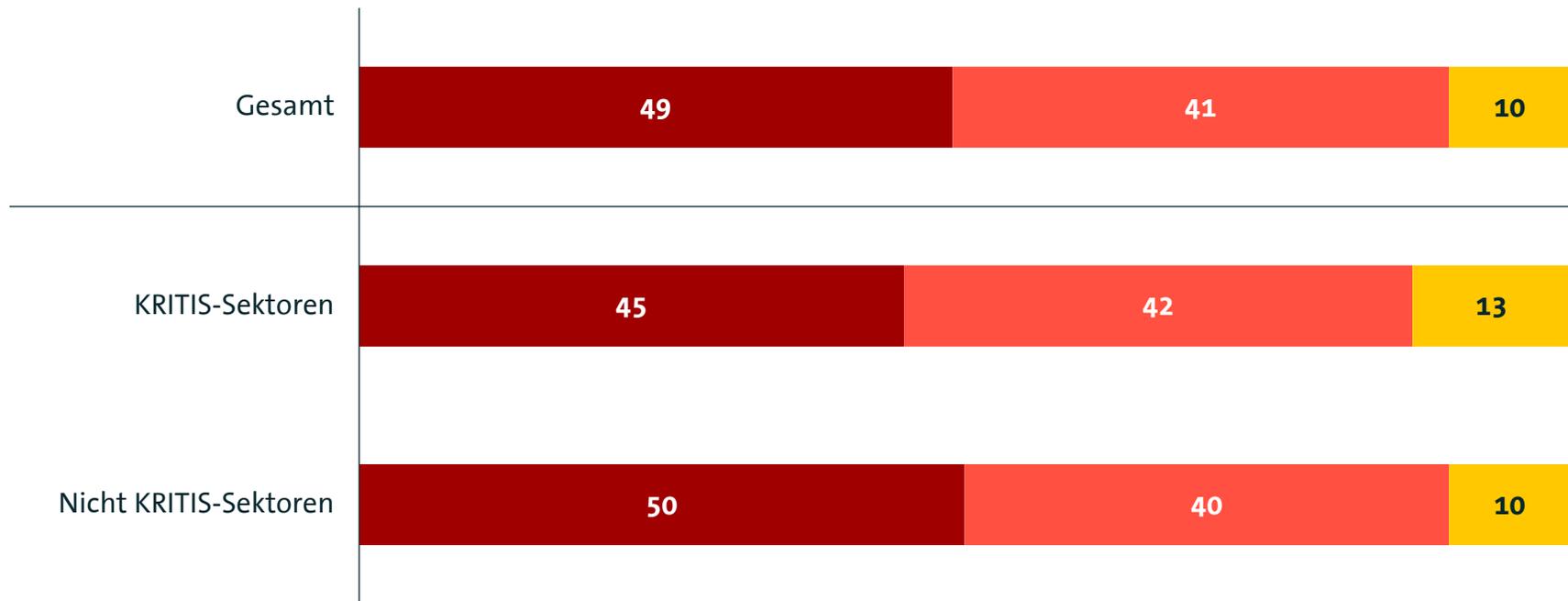


Künstliche Intelligenz **erleichtert Cyberangriffe.**



# Massive Zunahme von Cyberattacken befürchtet

Wie wird sich die Anzahl der Cyberattacken auf Ihr Unternehmen in den nächsten 12 Monaten im Vergleich zu den letzten 12 Monaten voraussichtlich entwickeln?

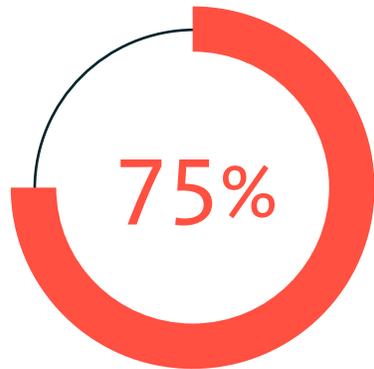


in Prozent

- Werden stark zunehmen
- Werden eher zunehmen
- Unverändert
- Werden eher abnehmen
- Werden stark abnehmen
- Weiß nicht/keine Angabe

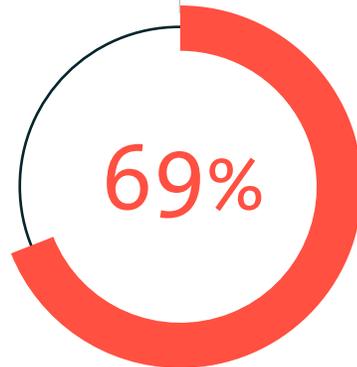
# Weltlage: Mehrheit fühlt sich bedroht – und handelt

Inwieweit treffen die folgenden Aussagen zu?



Die **Sicherheitsbehörden** sind gegenüber Cyberattacken aus dem Ausland **machtlos**.

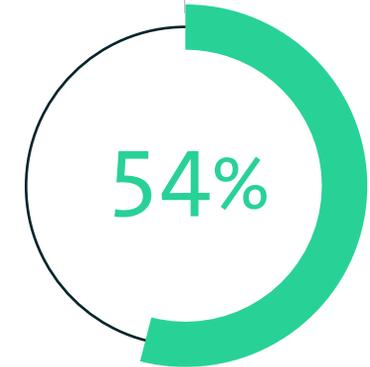
In Folge der zahlreichen **Kriege und Konflikte** hat sich die Bedrohung unseres Unternehmens durch **Cyberangriffe** verschärft.



Wir haben unsere **IT-Sicherheitsmaßnahmen** aufgrund der zahlreichen Kriege und Konflikte **verschärft**.

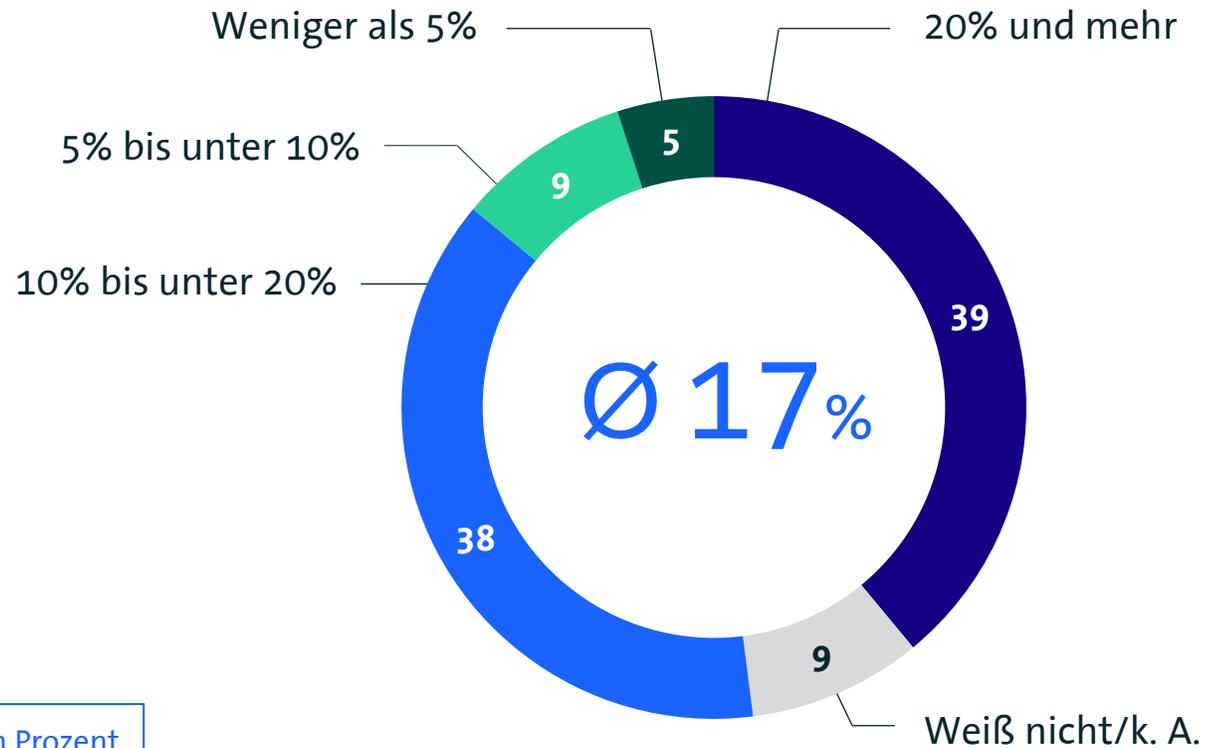


Wir haben **Maßnahmen** ergriffen, um uns vor **physischen Angriffen** auf die IT-Infrastruktur zu schützen.

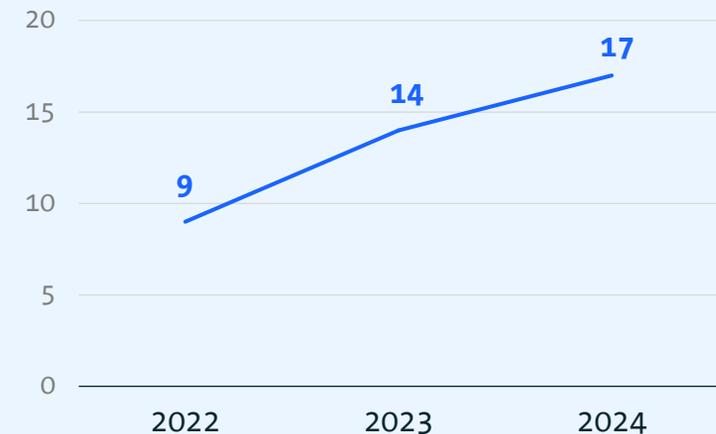


# Cybersicherheit: Investitionsbereitschaft steigt

Wie hoch ist geschätzt der Anteil des Budgets für IT-Sicherheit am gesamten IT-Budget Ihres Unternehmens?

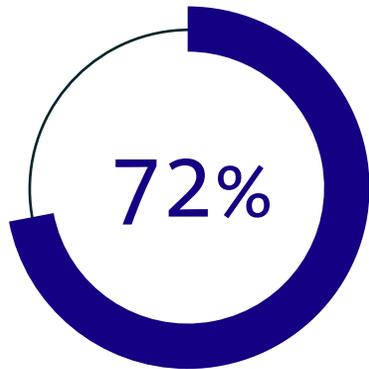


Durchschnittlicher Anteil des Budgets für IT-Sicherheit am gesamten IT-Budget



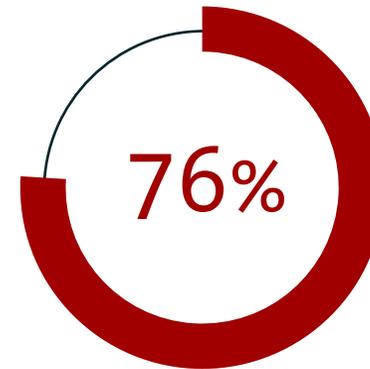
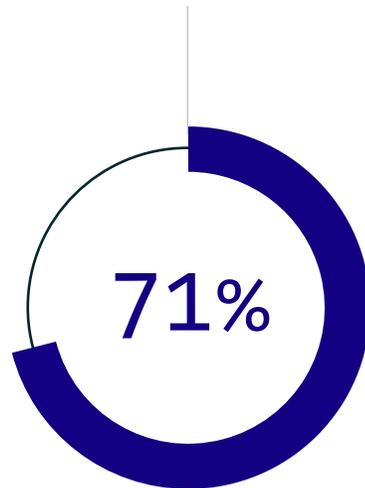
# IT-Sicherheit ist eine Frage der digitalen Souveränität

Inwieweit treffen die folgenden Aussagen zu?



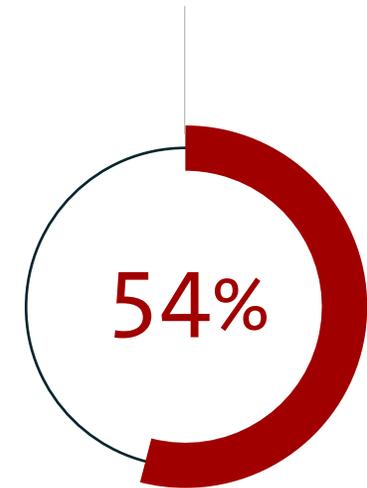
Deutsche IT-Sicherheitsunternehmen sollten von der Politik gezielt gefördert werden.

Wir achten besonders auf das **Herkunftsland des Anbieters**, wenn wir IT-Sicherheitslösungen einkaufen.



Die **öffentliche Verwaltung** ist viel schlechter auf Cyberangriffe vorbereitet als die deutsche Wirtschaft.

Im internationalen Vergleich **vernachlässigt die Politik** in Deutschland die Cybersicherheit.



A close-up photograph of a baseball in a catcher's mitt. The baseball is white with red stitching and is positioned in the center-right of the frame. The mitt is dark brown and has a mesh pocket. The background is a blurred green field.

# Wirtschaftsschutz 2024

**Dr. Ralf Wintergerst**  
Bitkom-Präsident

Berlin, 28. August 2024

# Untersuchungsdesign

Auftraggeber

Bitkom e.V.

<b>Methodik</b>	Computergestützte telefonische Befragung/ Computer Assisted Telephone Interview (CATI)
<b>Grundgesamtheit</b>	Unternehmen in Deutschland mit mindestens 10 Beschäftigten und einem Jahresumsatz von 1 Mio. Euro oder mehr
<b>Zielpersonen</b>	Führungskräfte, die für das Thema Wirtschaftsschutz verantwortlich sind. Dazu zählen Geschäftsführer sowie Führungskräfte aus den Bereichen Unternehmenssicherheit, IT-Sicherheit, Risikomanagement oder Finanzen.
<b>Stichprobengröße</b>	n=1.003
<b>Befragungszeitraum</b>	KW 16 bis KW 24 2024
<b>Statistische Fehlertoleranz</b>	+/- 3 Prozent in der Gesamtstichprobe

# Kontakt

Bitkom e. V.  
Albrechtstraße 10  
10117 Berlin

[bitkom.org](https://bitkom.org)



**Felix Kuhlenkamp**

Referent Sicherheitspolitik  
Bitkom e.V.  
[f.kuhlenkamp@bitkom.org](mailto:f.kuhlenkamp@bitkom.org)  
T 030 27576-279



**Andreas Streim**

Pressesprecher  
Bitkom e.V.  
[a.streim@bitkom.org](mailto:a.streim@bitkom.org)  
T 030 27576-112



**Bettina Lange**

Senior Research Consultant  
Bitkom Research  
[b.lange@bitkom-research.de](mailto:b.lange@bitkom-research.de)  
T 030 27576-547