Pressekonferenz
Berlin, 11. Juni 2025

Dr. Michael Fübi
Präsident TÜV-Verband e.V.

Claudia Plattner
Präsidentin Bundesamt für Sicherheit
in der Informationstechnik (BSI)

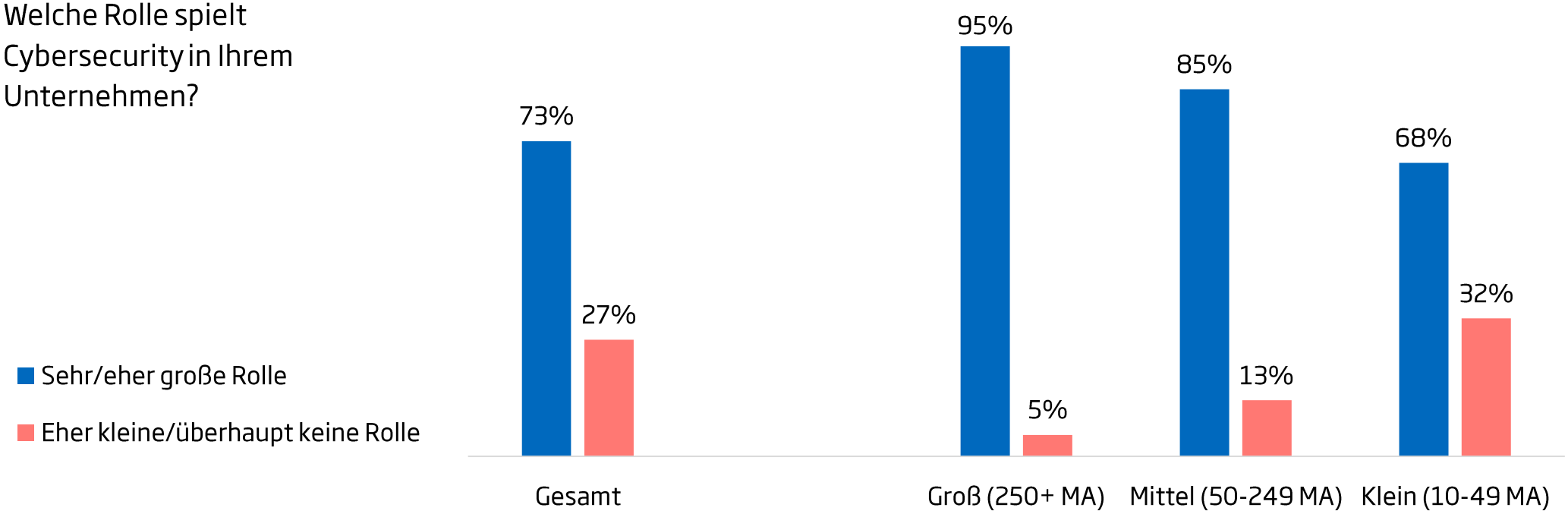
TÜV Cybersecurity Studie 2025

Cybersicherheit in deutschen Unternehmen

TÜV VERBAND

Cybersicherheit hat in drei von vier Unternehmen hohe Relevanz – in einem Viertel nicht!

Welche Rolle spielt Cybersecurity in Ihrem Unternehmen?



Frage: Welche Rolle spielt Cybersecurity aktuell für Ihr Unternehmen? | Abweichungen zu 100% „Weiß nicht“ | Basis: Alle befragten Unternehmen (n=506)

Unternehmen bewerten ihre Cybersicherheit als gut

Wie bewerten Sie die Cybersicherheit Ihres Unternehmens?

Frage: Wie bewerten Sie die Cybersicherheit Ihres Unternehmens insgesamt? | Basis: Alle befragten Unternehmen (n=506)

Fast jedes siebte Unternehmen ist in den letzten 12 Monaten Opfer eines Cyberangriffs geworden

15%

verzeichneten in den letzten 12 Monaten einen IT-Sicherheitsvorfall.

+4%-Punkte

im Vergleich zu 2023

Frage: Hat Ihr Unternehmen in den letzten 12 Monaten einen IT-Sicherheitsvorfall gehabt? | Basis: Alle befragten Unternehmen (n=506)

Was ist ein IT-Sicherheitsvorfall?

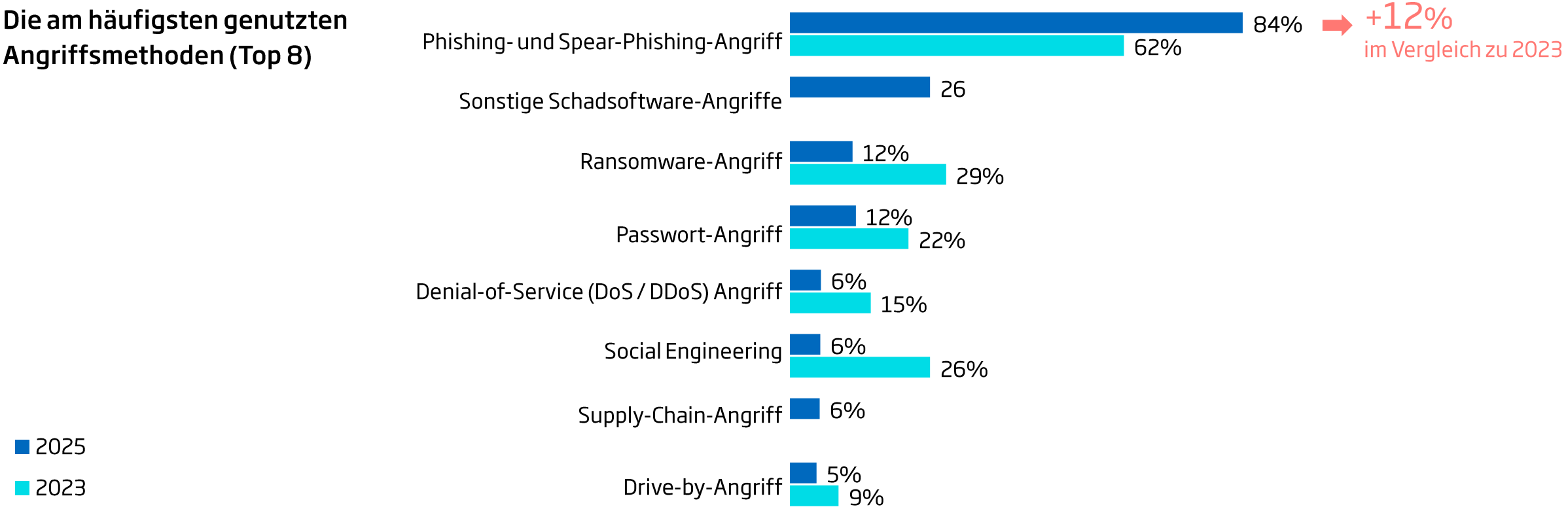
Unsere Frage: Hat Ihr Unternehmen in den letzten 12 Monaten einen IT-Sicherheitsvorfall bzw. einen Cyberangriff gehabt?
Auf Nachfrage: Ein IT-Sicherheitsvorfall bzw. Cyberangriff, auf den Ihr Unternehmen aktiv reagieren musste.

Zum Vergleich Bitkom-Frage: War Ihr Unternehmen innerhalb der letzten 12 Monate von Diebstahl, Industriespionage oder Sabotage betroffen? (81% sagen ja)

Gemeint sind erfolgreiche Angriffe	Nicht gemeint sind erfolglose Angriffsversuche
Dienste für Mitarbeitende / Kunden ausgefallen, z.B. durch Schadsoftware	Phishing-Mails, die gefiltert oder nicht „aktiviert" wurden
IT-Systeme beeinträchtigt (langsam) oder übernommen (ferngesteuert)	Portscans, manipulierte Datenpakete, ICMP-Pakete (gefiltert)
Systeme sind zeitweise ausgefallen	Erkannte Schadsoftware (von Antivirenprogrammen unschädlich gemacht)
Daten sind abgeflossen oder wurden verfälscht	Brute-Force-Attacken auf Passwörter (automatisierter Test möglicher Kombinationen) erkannt und blockiert
Erpressung durch Hacker	Angriffe auf die Webseite

Phishing die mit Abstand häufigste Angriffsmethode

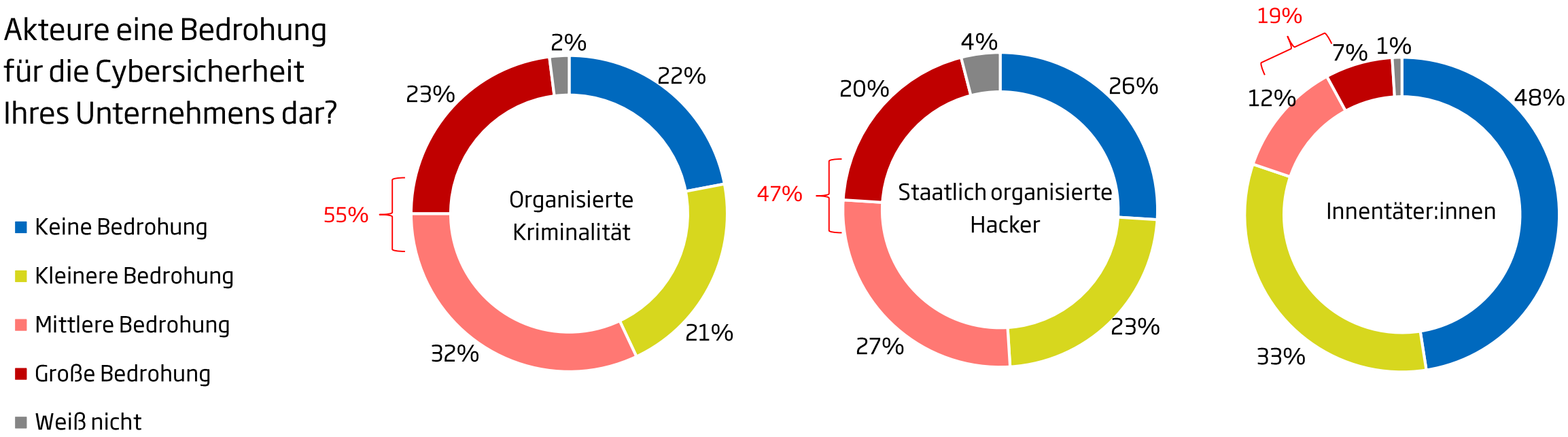
Die am häufigsten genutzten Angriffsmethoden (Top 8)



Frage: Um welche Art von IT-Sicherheitsvorfall bzw. Cyberangriffen handelte es sich? (Mehrfachnennungen) | Basis: Unternehmen, die in den letzten 12 Monaten mind. einen IT-Sicherheitsvorfall hatten (2025: n=89, 2023: n=55)

Sorge vor kriminellen und staatlichen Hackern

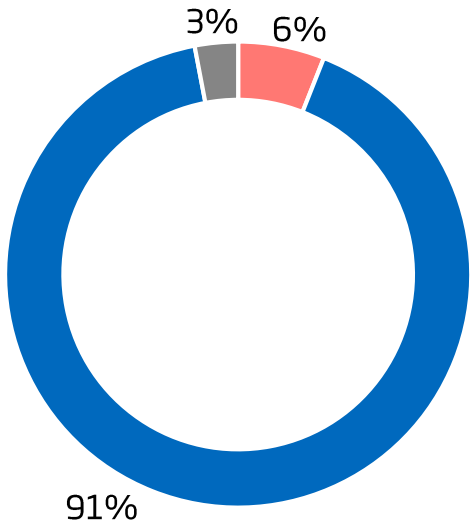
Inwiefern stellen diese Akteure eine Bedrohung für die Cybersicherheit Ihres Unternehmens dar?



Frage: Ich lese Ihnen nun einige Akteure vor, die Cyberangriffe initiieren. Inwiefern stellen diese Akteure eine große, mittlere, kleine oder keine Bedrohung für die Cybersecurity Ihres Unternehmens dar? | Basis: n= 506 Unternehmen 2025

Herkunft der Cybergangriffe meist unklar

Haben Sie in den letzten 12 Monaten Cyberangriffe aus bestimmten Regionen identifiziert?

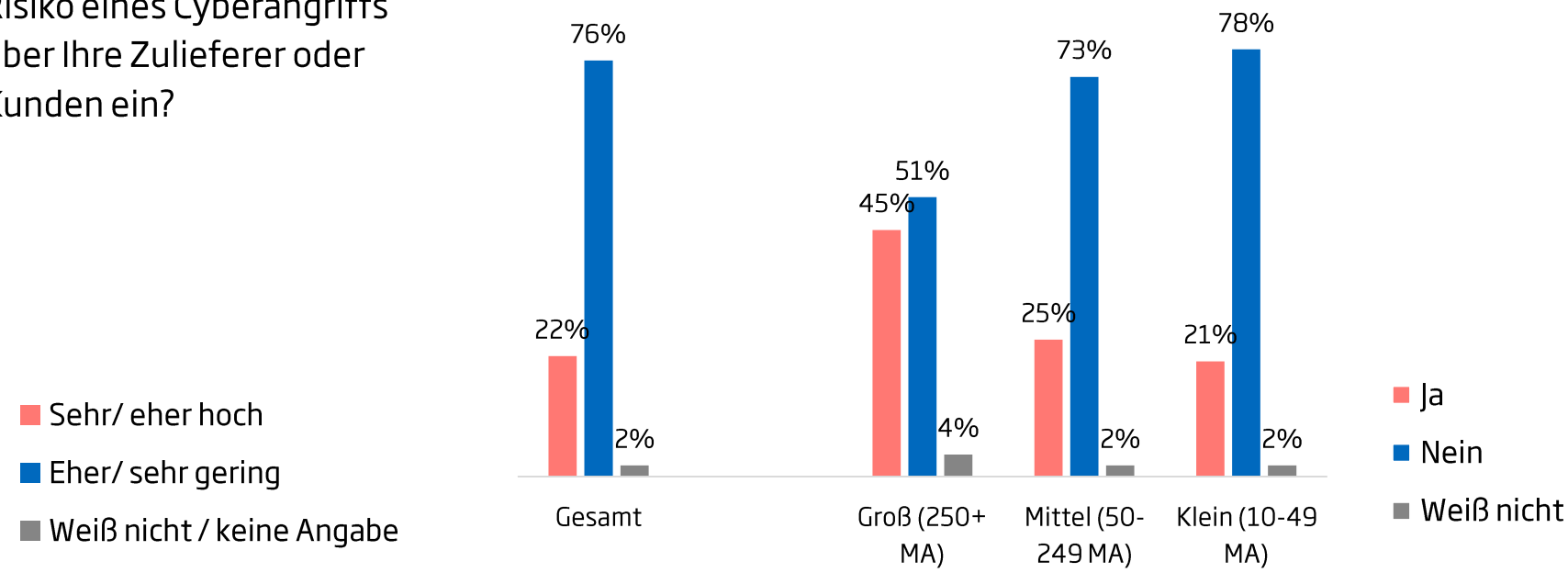


Identifikation der Regionen (offene Abfrage)

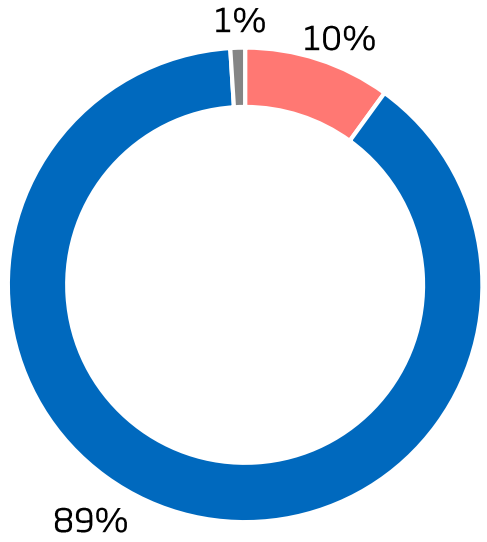
Frage: Haben Sie in den letzten 12 Monaten Angriffe aus bestimmten Regionen identifiziert? | Basis: Alle befragten Unternehmen (n= 506) und Unternehmen, die Angriffe aus bestimmten Regionen identifiziert haben (n= 37) | Die Größe der Wörter entspricht der Häufigkeit der Nennungen, d.h. je größer das der Begriff, desto mehr Teilnehmende haben dies geäußert.

Angriffe über Zulieferer und Kunden

Wie hoch schätzen Sie das Risiko eines Cyberangriffs über Ihre Zulieferer oder Kunden ein?

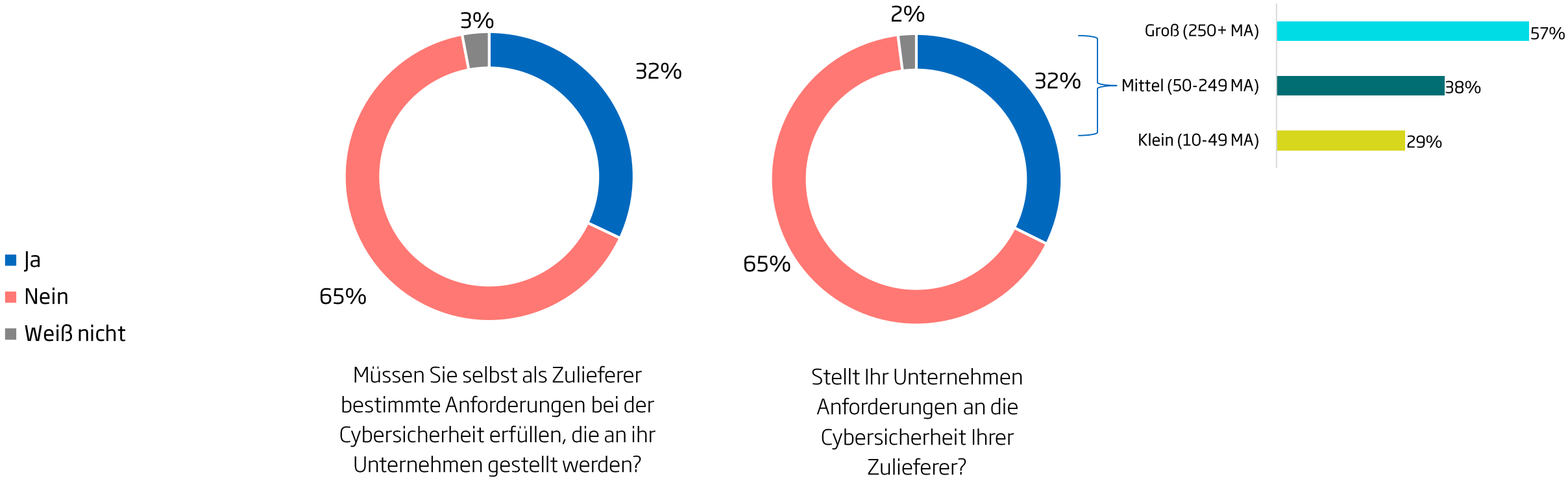


Haben Sie Cyberangriffe festgestellt, die über Zulieferer oder Kunden erfolgt sind?



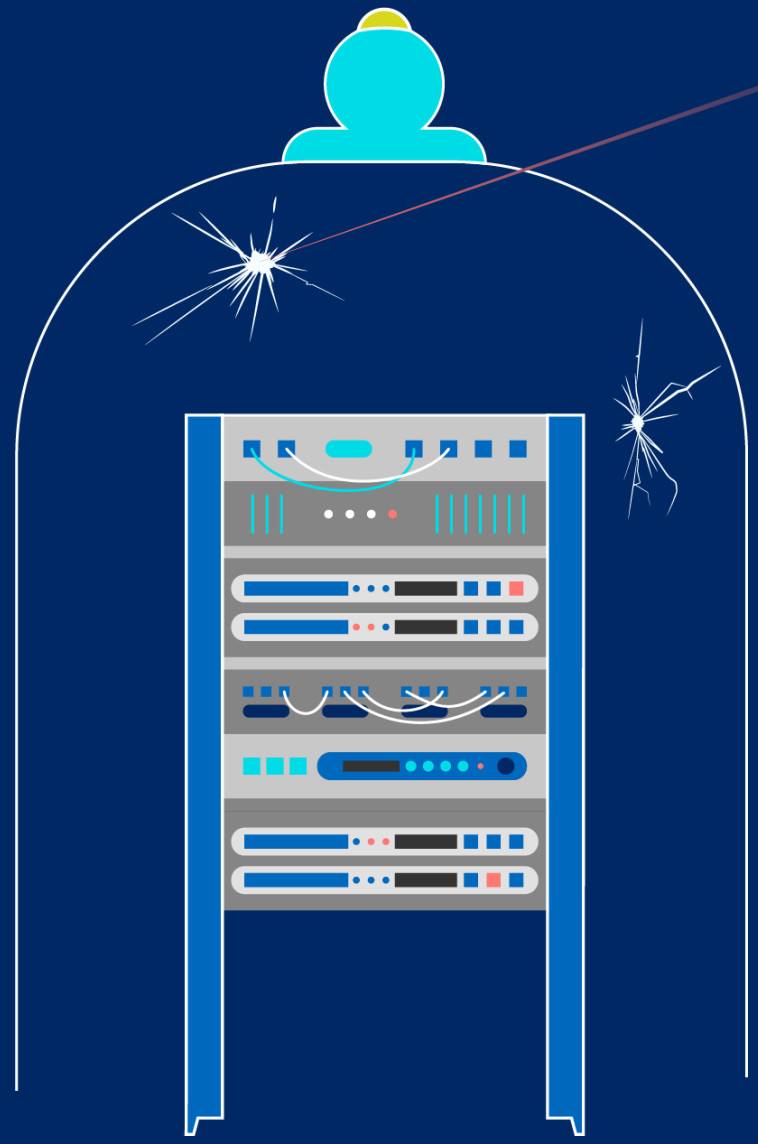
Frage: Wie hoch schätzen Sie das Risiko eines Cyberangriffs über einen Ihrer Zulieferer oder Kunden ein? Haben Sie einen oder mehrere Cyberangriffe auf Ihr Unternehmen festgestellt, die über Zulieferer oder Kunden erfolgt sind? | Basis: Alle befragten Unternehmen (n=506)

Jedes dritte Unternehmen stellt Sicherheits-anforderungen an seine Zulieferer



Basis: Alle befragten Unternehmen (n=506)

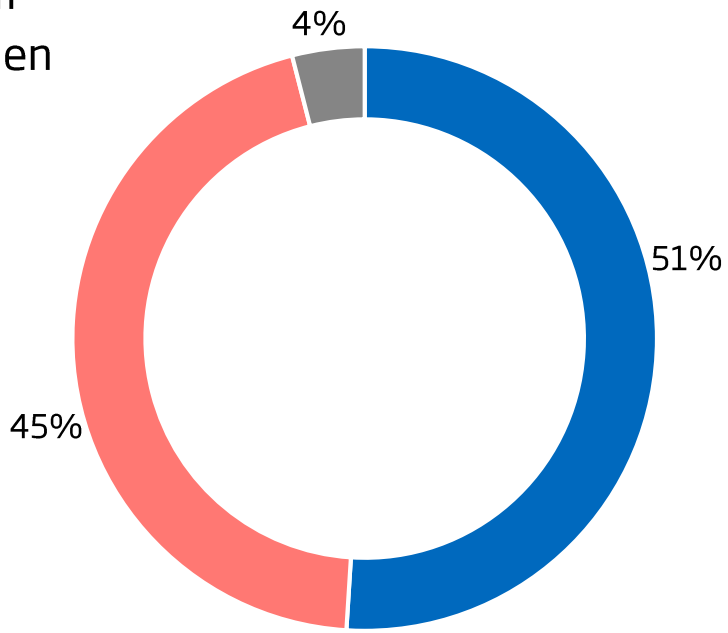
Künstliche Intelligenz: Besserer Schutz und höheres Risiko

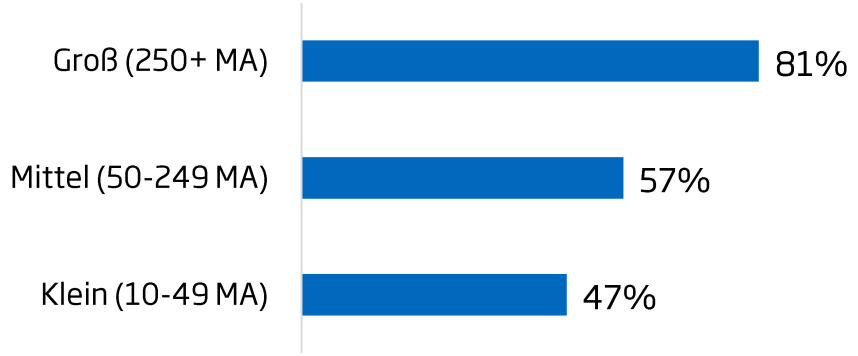


TÜV VERBAND

Die Hälfte beobachtet Cyberangriffe auf KI-Basis

Nehmen Sie wahr, dass Angreifer Künstliche Intelligenz nutzen, um Cyberangriffe auf Ihr Unternehmen durchzuführen?

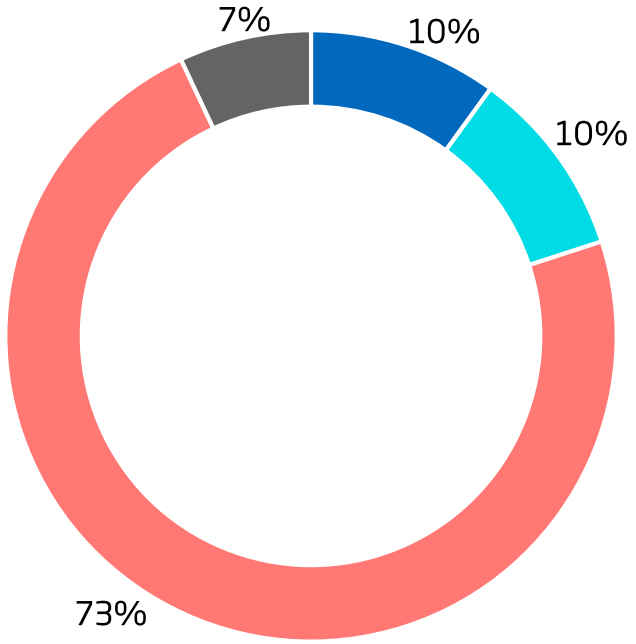




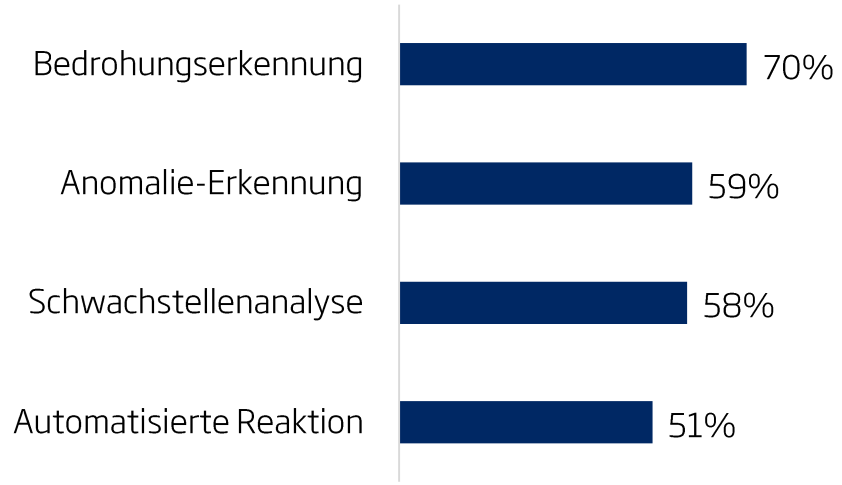
Frage: Nehmen Sie wahr, dass Angreifer Künstliche Intelligenz nutzen, um Cyberangriffe auf Ihr Unternehmen durchzuführen ? | Basis: Alle befragten Unternehmen (n=506)

Nur jedes zehnte Unternehmen nutzt schon jetzt KI für die Abwehr von Cyberangriffen

Setzt Ihr Unternehmen KI bei der Abwehr von Cyberangriffen ein?

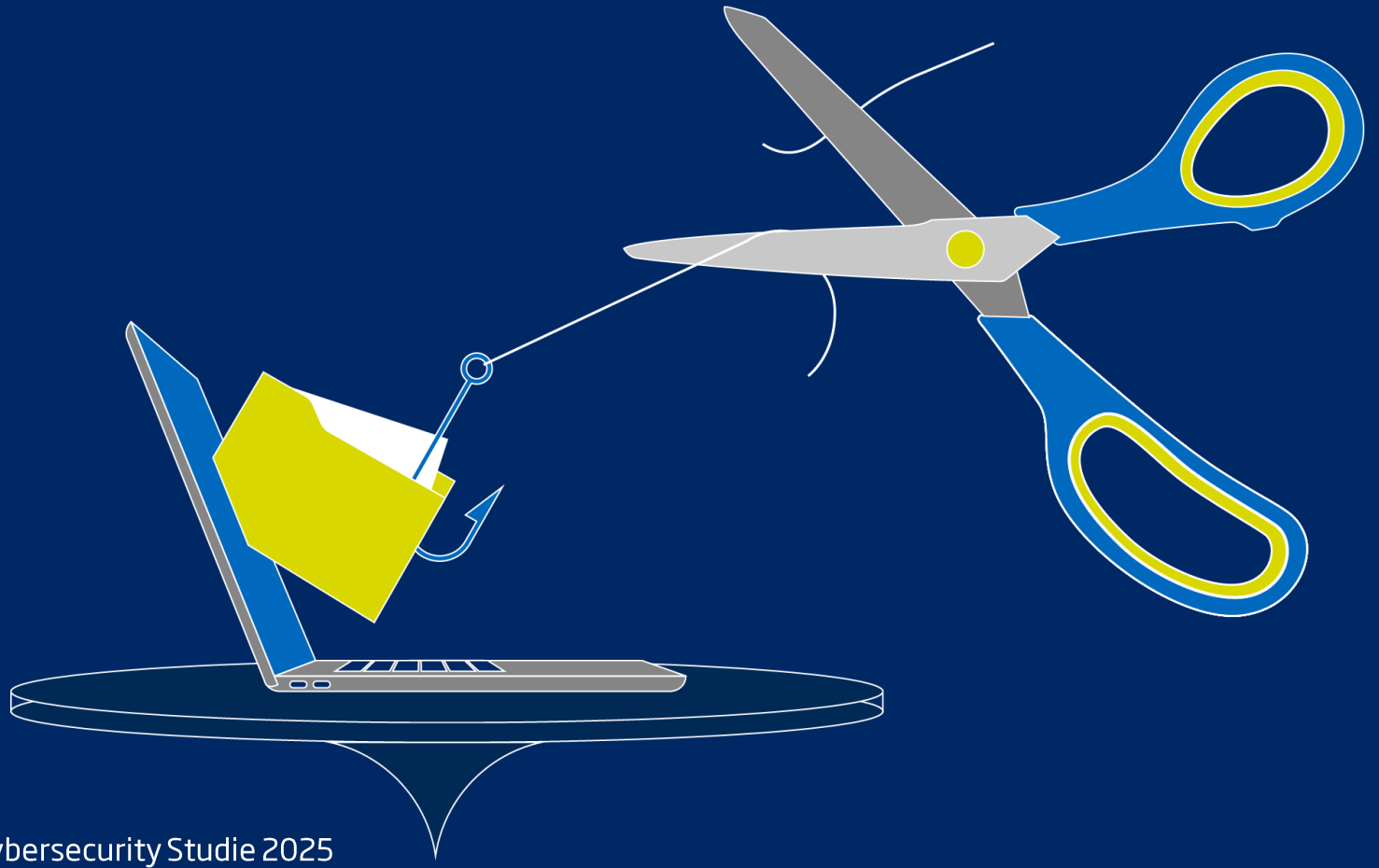


Einsatzbereiche von KI



Frage: Setzt Ihr Unternehmen Künstliche Intelligenz (KI) bei der Abwehr von Cyberangriffen ein? | Basis: Alle befragten Unternehmen (n=506)
Frage: In welchen Bereichen der Cybersicherheit setzen Sie KI-basierte Lösungen ein bzw. planen Sie diese einzusetzen? (Mehrfachnennungen) | Basis: Unternehmen, welche KI im Einsatz oder dessen Einsatz in Planung haben (n= 126)

Maßnahmen für mehr Cybersicherheit



Grundlage für Verbesserungen: Zusätzliche Ressourcen

Hat Ihr Unternehmen in den letzten 24 Monaten eine dieser Maßnahmen zur Verbesserung der IT-Sicherheit ergriffen?

27%

Erhöhung des Budget für Cybersecurity

2023: 52%

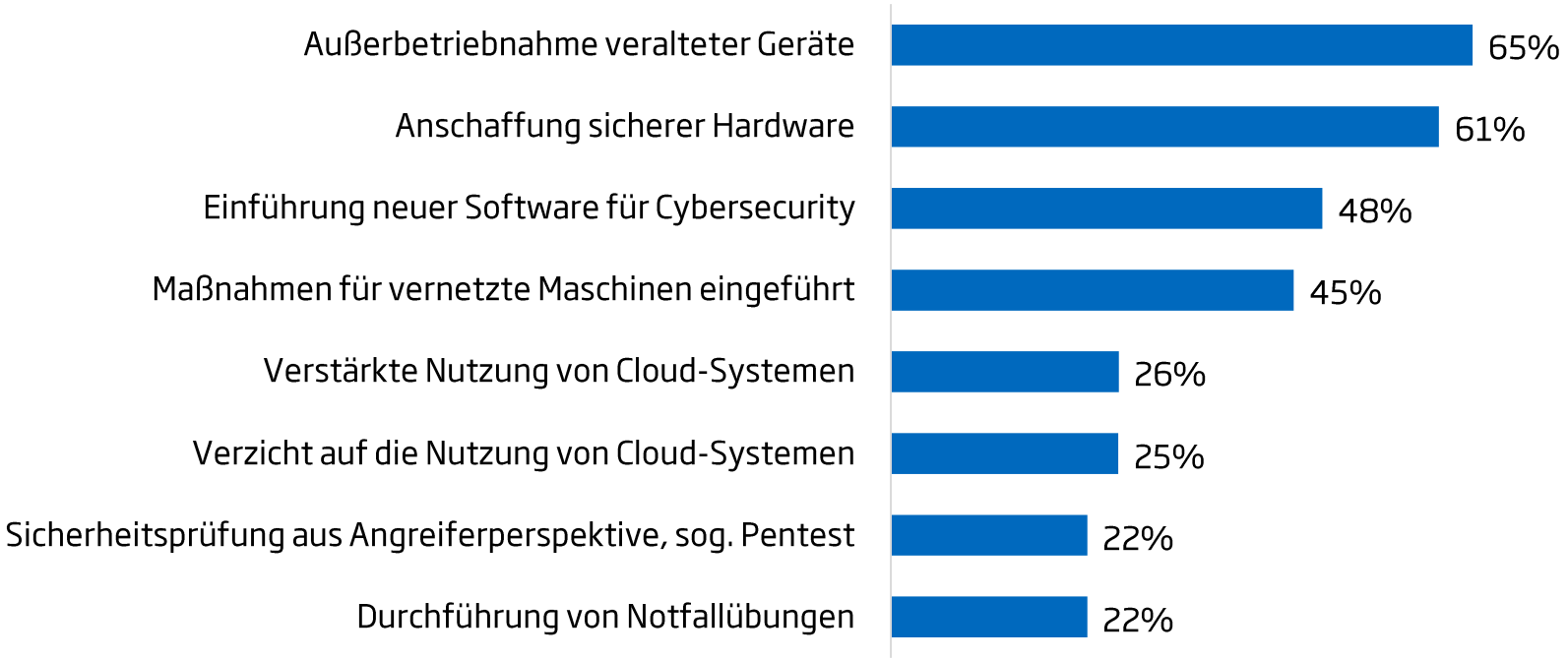
14%

Einstellung zusätzlicher IT-Experten

Frage: Nun geht es um Maßnahmen für die Verbesserung der IT-Sicherheit. Hat Ihr Unternehmen in den letzten 24 Monaten eine dieser Maßnahmen ergriffen? (Mehrfachnennungen) | Basis: Alle befragten Unternehmen (n=506)

Viele Schutzmaßnahmen betreffen Hard- und Software

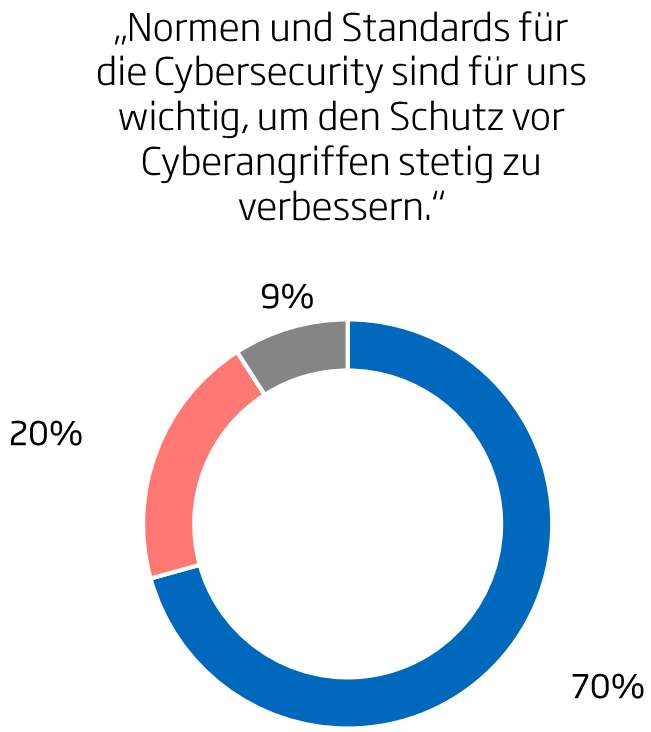
Hat Ihr Unternehmen in den letzten 24 Monaten eine dieser Maßnahmen zur Verbesserung der IT-Sicherheit ergriffen?



Frage: Nun geht es um Maßnahmen für die Verbesserung der IT-Sicherheit. Hat Ihr Unternehmen in den letzten 24 Monaten eine dieser Maßnahmen ergriffen? (Mehrfachnennungen) | Basis: Alle befragten Unternehmen (n=506)

Normen & Standards: Orientierung für besseren Schutz

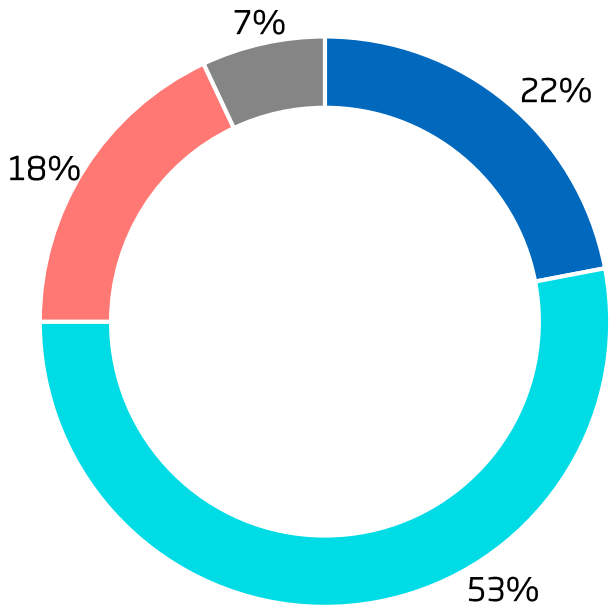
Aussagen zu Normen und Standards für die Cybersecurity



Frage: Inwiefern stimmen Sie folgenden Aussagen zu Normen und Standards für die Cybersecurity zu oder nicht zu? (Mehrfachnennungen) | Basis: Alle befragten Unternehmen (n=506)

Rund jeder Fünfte setzt Normen & Standards vollständig um

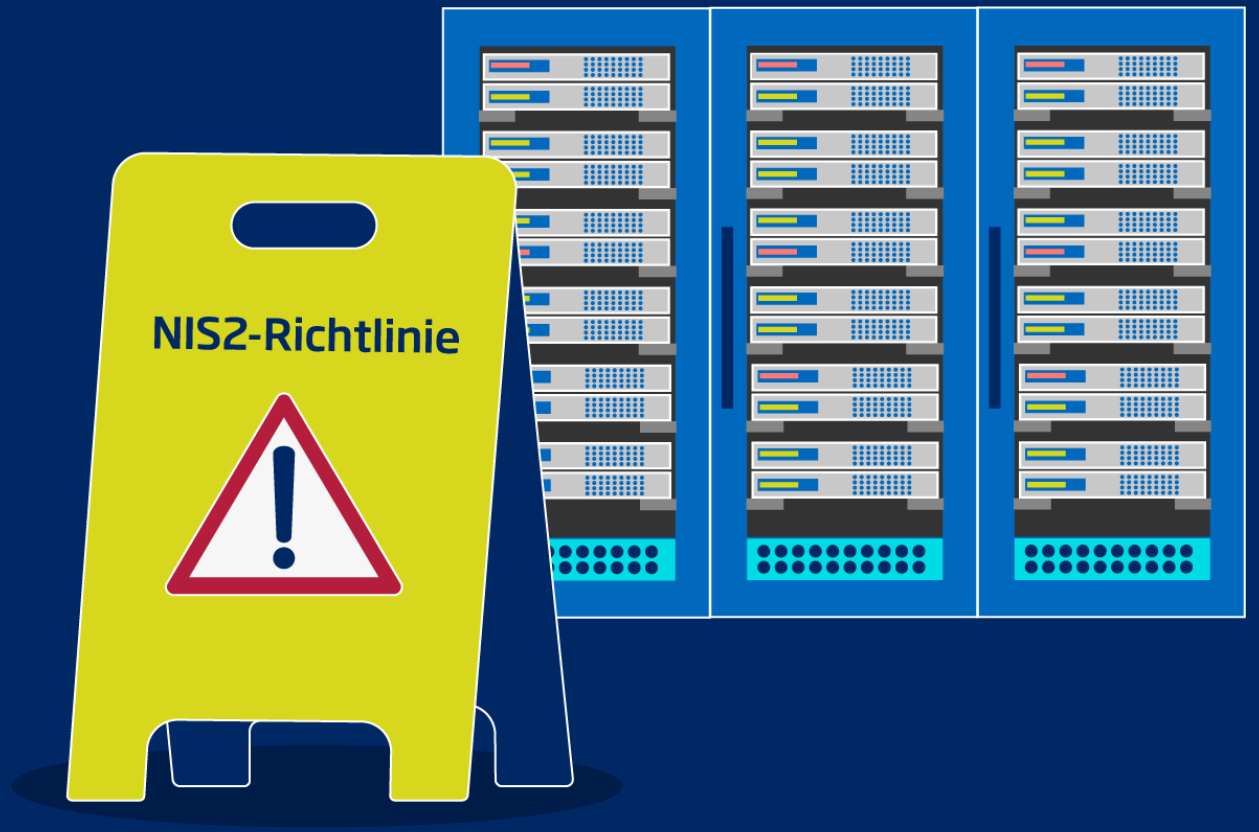
Welche Aussage zu Normen und Standards für Cybersecurity trifft am ehesten auf Ihr Unternehmen zu?



- Wir erfüllen bestimmte Normen & Standards vollumfänglich
- Wir orientieren uns an Normen & Standards, setzen diese aber nur teilweise um
- Normen und Standards spielen bisher keine Rolle
- Weiß nicht/k.A.

Frage: Nun lese ich Ihnen drei Aussagen zu Normen und Standards für Cybersecurity im Unternehmen vor. Diese werden u.a. vom Bundesamt für Sicherheit in der Informationstechnik (BSI) oder dem Deutschen Institut für Normung (DIN) ausgearbeitet. Welche der drei Aussagen, trifft am ehesten auf Ihr Unternehmen zu? | Abweichungen zu 100 Prozent „Weiß nicht“ | Basis: Alle befragten Unternehmen (n=506)

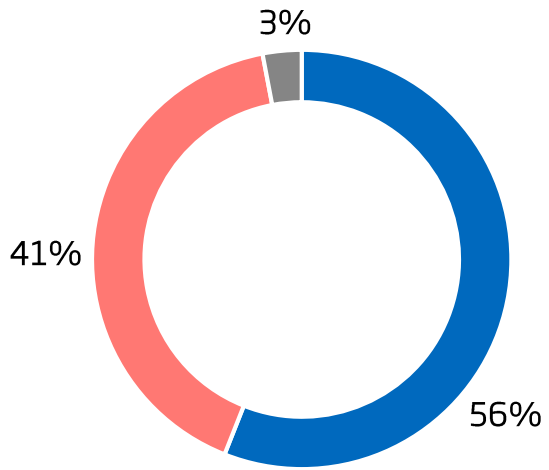
Gesetzliche Vorgaben für mehr Cybersicherheit



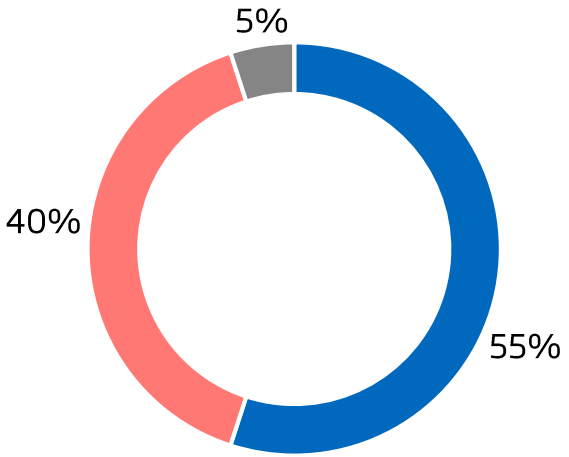
Mehrheit fordert Cybersecurity-Vorgaben für alle Unternehmen

Aussagen zur politischen Regulierung von Cybersecurity

„Jedes Unternehmen sollte gesetzlich verpflichtet sein, angemessene Maßnahmen für seine Cybersecurity zu ergreifen."



„Strengere gesetzliche Vorgaben für die Cybersecurity von Unternehmen machen das ganze Internet sicherer."

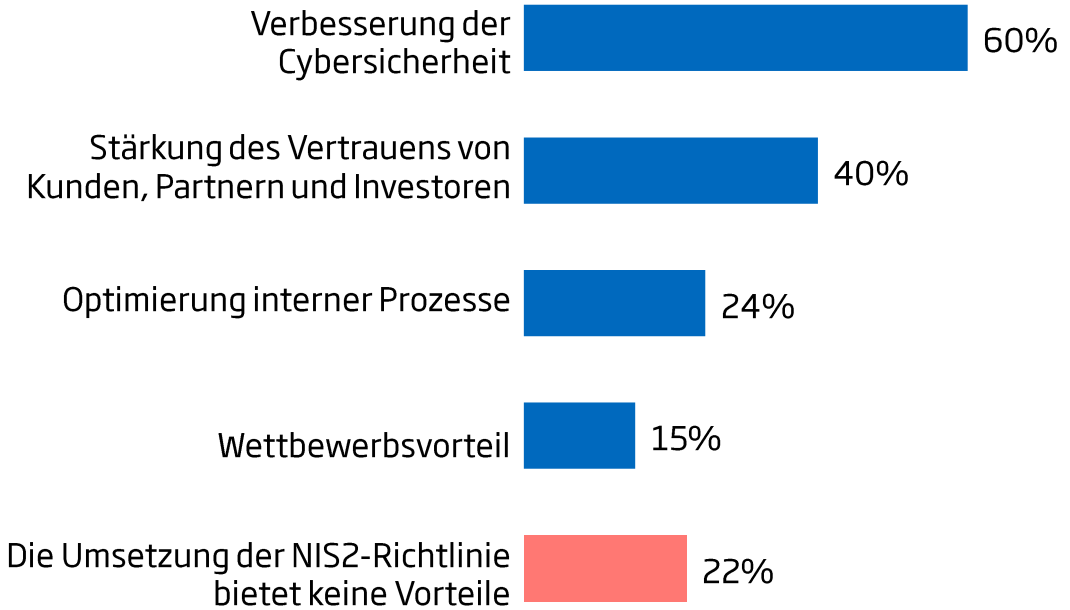


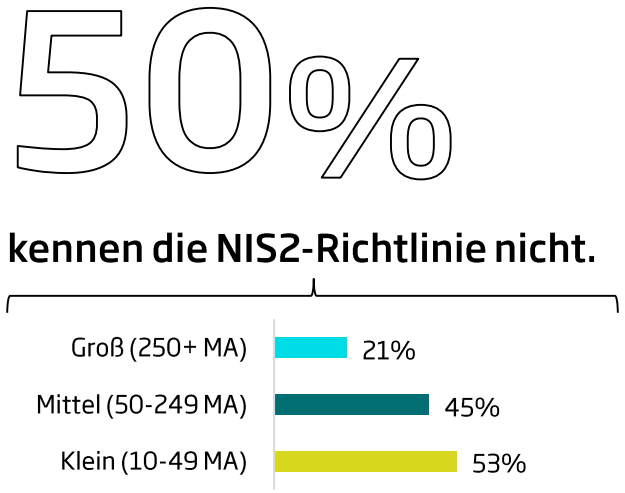
- Stimme voll/eher zu
- Stimme eher nicht/nicht zu
- Weiß nicht

Frage: Ich lese Ihnen nun einige Aussagen zum Thema politische Regulierung von Cybersecurity vor. Inwiefern stimmen Sie diesen zu oder nicht zu? | Basis: Alle befragten Unternehmen (n=506)

Network and Information Security Richtlinie (NIS2) der Hälfte nicht bekannt

Welche Vorteile bietet die Umsetzung der NIS2-Richtlinie in Ihrem Unternehmen?





Frage: Welche Vorteile bietet die Umsetzung der NIS2-Richtlinie in Ihrem Unternehmen? (Mehrfachnennungen) | Basis: Unternehmen, die die NIS2-Richtlinie kennen (n= 255)

Politische Empfehlungen TÜV-Verband

Auftrag für die neue Bundesregierung: Cybersicherheit voranbringen
Zuständigkeiten zwischen Digital- und Innenministerium klären, Cybersicherheitsagenda für die Legislaturperiode aktualisieren

Cybersecurity-Regulierung zügig umsetzen
Nationales Umsetzungsgesetz von NIS2 beschließen,
EU Cyber Resilience Act (CRA) planmäßig umsetzen

TÜV VERBAND

Empfehlungen für Unternehmen

1. **Cyberrisiken ernst nehmen!**
   Risikoanalyse durchführen

2. **Strategie entwickeln**
   Ziel: Angemessenes Sicherheitslevel erreichen

3. **Maßnahmenplan ausarbeiten**

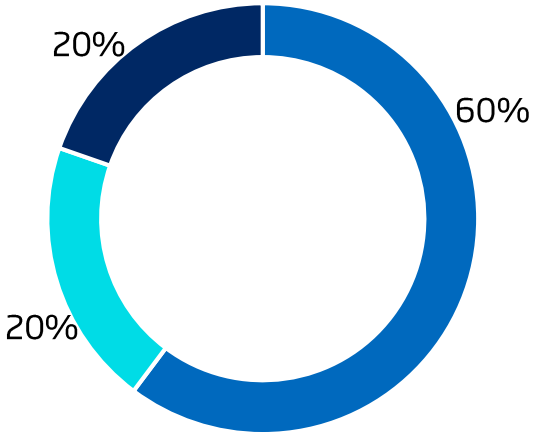
- **Vorsorge statt Nachsorge: Unternehmen krisenfest machen**
  Notfallübungen durchführen, um Prozesse einzuüben. Mit Pentests eigene Schwachstellen identifizieren.
- **Cybersicherheit mit Künstlicher Intelligenz stärken**
  Strategie für den KI-Einsatz entwickeln, entsprechende Tools testen, Mitarbeiter sensibilisieren, externe Beratungsangebote nutzen.
- **Know-how is key! Mitarbeitende qualifizieren**
  IT-Spezialisten einstellen und fortbilden, Mitarbeitende regelmäßig zu aktuellen Angriffsmethoden schulen.
- **Normen und Standards nutzen**
  Normen und Standards geben Orientierung und bringen die IT-Sicherheit auf ein höheres Level.

TÜV VERBAND

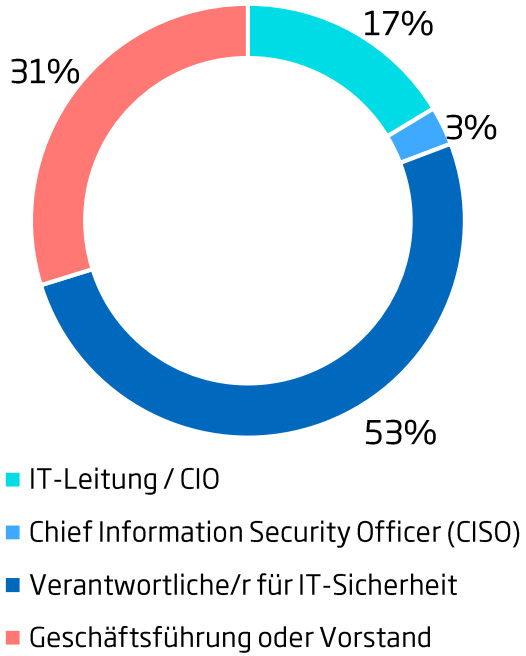
Methodik

Die repräsentative Umfrage wurde von der Ipsos GmbH im Auftrag des TÜV-Verbands durchgeführt. Die Interviews erfolgten mittels einer telefonischen CATI-Befragung zwischen 18. Februar und 14. März 2025. Grundgesamtheit: 506 Unternehmen ab 10 Mitarbeitenden.

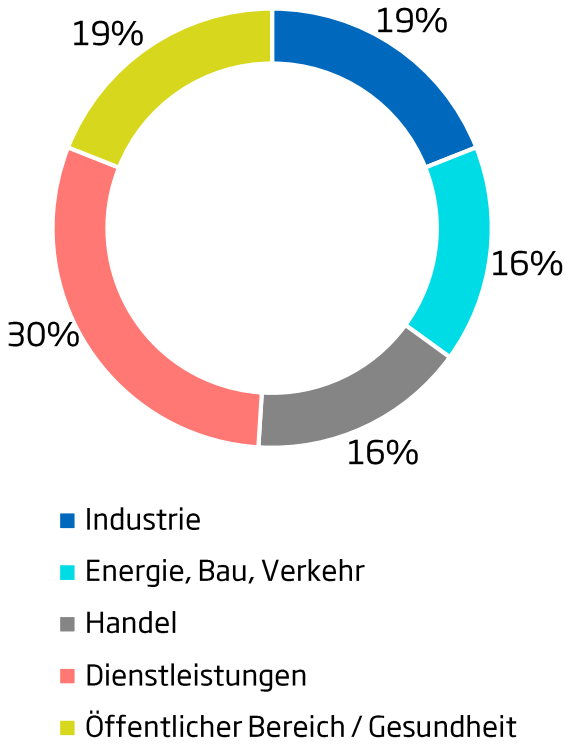
Anzahl Mitarbeitende



Funktion im Unternehmen



Aufteilung nach Branchen



Ihre Fragen bitte!

Maurice Shahd
Leiter Kommunikation und Pressesprecher

maurice.shahd@tuev-verband.de
+49 30 760095-320