# Cybersicherheit in deutschen Unternehmen

» Bedrohung
» Bewusstsein
» Schutz

TÜV VERBAND

**TÜV** Cybersecurity Studie 2023

# Inhalt


## Vorwort

> Dr. Johannes Bussmann

> Dr. Gerhard Schabhüser

## Zusammenfassung und Kernergebnisse

## 1 Bedeutung von Cybersecurity in der Wirtschaft

> Vor allem große Unternehmen haben die Bedeutung der IT-Sicherheit erkannt

> Starke Cybersicherheit wird zum Wettbewerbsvorteil

> Größte Sorge vor Angriffen organisierter Cyberkriminalität

> Ein Cyberangriff ist für viele realistisch

> Ukraine-Krieg verschärft das Angriffsrisiko im digitalen Raum

## 2 IT-Sicherheitsvorfälle und ihre Folgen

> Gut jedes zehnte Unternehmen von IT-Sicherheitsvorfall betroffen

> Phishing und Ransomware sind die häufigsten Angriffsmethoden

> Die meisten Angriffe werden rasch erkannt und behoben

> Die Folgen: Finanzielle Schäden, Systemausfälle, Datenklau

> Die Mehrzahl der Betroffenen investiert in besseren Schutz

> Die meisten schweigen über IT-Sicherheitsvorfälle

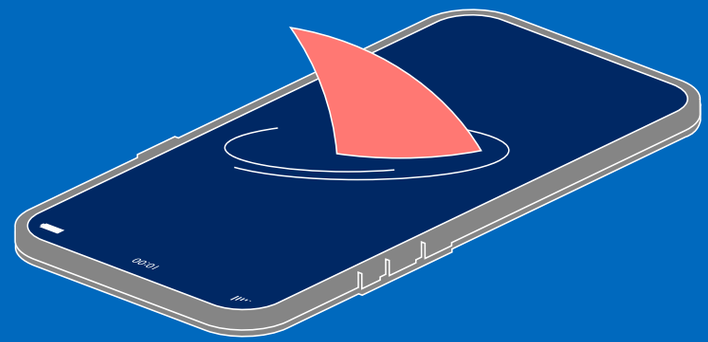
> Wunsch nach mehr Offenheit bei Cyberangriffen

## 3 Cybersecurity im Betriebsablauf

> Kunden und Partner als Motor für mehr Cybersecurity

> Mehrheit der Beschäftigten trägt IT-Sicherheitsvorgaben mit

> Fachkräftemangel: Unternehmen weichen auf Dienstleister aus



## 4 Digitale Sicherheit beim mobilen Arbeiten

> Mobiles Arbeiten hat sich etabliert

> Fast jeder dritte Arbeitgeber ermöglicht Workation

> Private Nutzung von Firmengeräten birgt Gefahren

> Mehrheit hat die Sicherheitsrisiken des mobilen Arbeitens im Griff

## 5 Maßnahmen und Investitionen für einen besseren Schutz

> Investitionen in die Hard- und Software stehen im Mittelpunkt

> Investitionen in Know-how und Praxis-Tests

> Eine Mehrheit investiert mehr in Cybersecurity

> Abwehr von Cyberangriffen hat höchste Priorität

> Unternehmen speichern Daten vorwiegend innerhalb der EU

> Bei der Auswahl von IT-Anbietern entscheidet auch die Herkunft

> Nicht immer stehen Kosten und Nutzen im Verhältnis

## 6 Gesetze, Normen und Standards als Sicherheitsfaktoren

> Unternehmen fordern strengere gesetzliche Cybersecurity-Vorgaben

> Zentrale Rolle von Normen und Standards für die IT-Sicherheit

> Öffentlicher Sektor erfüllt Normen und Standards am häufigsten

> Zuspruch für externe Prüfung von IT-Sicherheitsstandards

> Normen und Standards verursachen Aufwand

## 7 Fazit und politische Empfehlungen

## Methodik

# Verschärfte Sicherheitslage erfordert neue Antworten

Gut jedes zehnte Unternehmen ab 10 Mitarbeitenden war in Deutschland im vergangenen Jahr von einem IT-Sicherheitsvorfall betroffen. In absoluten Zahlen sind das in dieser Größenklasse rund 50.000 erfolgreiche Cyberangriffe, digitale Sabotageakte, Hardware-Diebstähle oder sonstige Vorfälle. Die Folgen sind meist gravierend. Dienste für Mitarbeitende oder Kunden sind nicht erreichbar, die Produktion fällt aus oder sensible Daten fließen ab. Häufig berichten die Unternehmen von einem Reputationsschaden. Zwar sind Cyberangriffe inzwischen alltäglich, aber trotzdem lautet die Botschaft: Das Unternehmen konnte sich nicht ausreichend schützen. Das Arsenal der Cyberkriminellen ist reichhaltig. Die betroffenen Unternehmen berichten unter anderem von Phishing-Angriffen, Erpressung mit Ransomware, Attacken auf Passwörter oder der gezielten Manipulation von Mitarbeitenden, das sogenannte Social Engineering. Technologische und politische Trends verschärfen die Situation. Kriminelle Hacker können im Darknet Cybercrime-Werkzeuge „as a Service" beauftragen oder ihre Phishing-Mails mit KI-Systemen wie ChatGPT optimieren und personalisieren. Geopolitische Krisen wie der Krieg in der Ukraine oder Handelskrieg zwischen den USA und China tun ihr Übriges. Staatlich legitimierte Gruppen greifen gezielt Rüstungsunternehmen an oder sind als digitale Freibeuter im Internet unterwegs.

Die „TÜV Cybersecurity Studie" zeigt eindrucksvoll, dass die Unternehmen diesen Gefahren keinesfalls schutzlos ausgeliefert sind. Eine große Mehrheit hat die Bedeutung der Cybersicherheit erkannt und begreift sie als essenziell für ihr Geschäft. Cybersecurity ist für die meisten Unternehmen heute ein Wettbewerbsvorteil und wird von Kunden und Partnern eingefordert. Das zeigt: IT-Sicherheit ist heute nicht nur für die IT-Abteilungen relevant, sondern auch für das Top-Management.

Die Unternehmen investieren in moderne Hard- und Software, schulen ihre Mitarbeitenden und lassen sich von externen Expert:innen beraten. Immer wichtiger werden Praxistests, um Schwachstellen aufzuspüren. Und bei Notfallübungen wird der Ernstfall durchgespielt. Es geht also heute nicht nur darum, Cyberangriffe abzuwehren. Ein weiterer Fokus liegt darauf, Angriffe zu erkennen, möglichst schnell zu reagieren und die IT-Systeme nach einem Sicherheitsvorfall wiederherzustellen. Dieser Ansatz sollte in der Wirtschaft noch stärker verfolgt werden.

Wollen Unternehmen ihre Cybersicherheit auf ein höheres Level heben, kommen sie nicht an Zertifizierungen wie ISO 27001 oder dem IT-Grundschutz des BSI vorbei. Normen und Standards helfen den Unternehmen, IT-Sicherheit umfassend in den Strukturen einer Organisation zu verankern. Mitarbeitende, Kunden und Partner können darauf vertrauen, dass die Unternehmen auf dem neuesten Stand sind. Auf diesem Feld sind die TÜV-Organisationen aktiv und unterstützen Unternehmen mit einem breiten Service-Angebot von Schulungen über Praxistests bis zur Durchführung von Zertifizierungen.

Die in der Studie befragten Sicherheitsverantwortlichen fordern aber auch die Politik zum Handeln auf. Eine Mehrheit spricht sich dafür aus, dass alle Unternehmen gesetzliche Vorgaben für die Cybersicherheit erfüllen müssen. Aus unserer Sicht gilt es jetzt, europäische Gesetzesvorhaben wie den „Cyber Resilience Act" oder den „AI Act" zügig zu verabschieden und zur Anwendung zu bringen. Mit den Verordnungen wird die digitale Produktsicherheit gestärkt und die Risiken künstlicher Intelligenz gemindert.

Unterstützung benötigen vor allem die kleineren Unternehmen, die über geringe finanzielle und personelle Ressourcen verfügen, aber ebenso gefährdet sind. Hier werden wir als Prüforganisationen weiterhin mit privaten Initiativen und Partnern wie dem Bundesamt für Sicherheit in der Informationstechnik vertrauensvoll zusammenarbeiten.

## Ich wünsche Ihnen eine anregende Lektüre!

**Herzlich Ihr**
**Dr. Johannes Bußmann**
Präsident TÜV-Verband e.V.
CEO TÜV SÜD AG

# Cybersicherheit ist eine Daueraufgabe – mit höchster Priorität

Die Digitalisierung unseres Alltags bringt uns als Gesellschaft und insbesondere Unternehmen und Organisationen zahlreiche Vorteile. Informationen fließen schneller, Prozesse werden effizienter, die Wertschöpfung steigt. All diese Vorzüge bergen aber auch Risiken, denn mit der zunehmenden Vernetzung entstehen Abhängigkeiten. Kommt es zu einem IT-Sicherheitsvorfall bei einem Unternehmen, kann dies schnell Auswirkungen auf eine ganze Lieferkette haben. Ebenso ausgeprägt ist diese Gefahr bei unzureichend abgesicherten IT-Dienstleistern, die zum Single-Point-of-Failure werden können. Fallen diese aus, sind womöglich zahlreiche Kunden ebenfalls beeinträchtigt.

Als Cyber-Sicherheitsbehörde des Bundes sieht das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Möglichkeiten und Potentiale der Digitalisierung. Gerade deshalb ist es uns so wichtig, die Digitalisierung sicher zu gestalten und sie gegen Cyber-Angriffe und IT-Sicherheitsvorfälle zu stärken und abzusichern. Wir müssen die Resilienz unserer vernetzten Gesellschaft und insbesondere unserer vernetzten Wirtschaft weiter stärken, damit die Digitalisierung auch nachhaltig erfolgreich sein kann. Um dies zu erreichen, dürfen Unternehmen und Organisationen zu keiner Zeit in ihrem Bemühen nachlassen, angemessene IT-Sicherheitsmaßnahmen umzusetzen. Da sich Cyberkriminelle und staatliche Angreifer konsequent professionalisieren und gleichzeitig die Angriffsfläche unserer digitalen Systeme immer weiterwächst, ist Cybersicherheit eine Daueraufgabe mit höchster Priorität. Und dabei stellen wir als BSI fest: Wir haben kein Maßnahmenproblem – wir haben ein Umsetzungsproblem! Gerade in kleineren Unternehmen hat Cybersicherheit noch nicht den Stellenwert, den sie einnehmen sollte.

Die vorliegende Studie zeigt: Das Bewusstsein für die Bedrohung durch Cyberangriffe ist mittlerweile in den Unternehmen vorhanden. Sie zeigt aber auch, dass Unternehmen jetzt konsequent geeignete IT-Sicherheitsmaßnahmen umsetzen müssen. Dabei ist klar: 100-prozentige Sicherheit gibt es nicht. Aber die Erfahrungen des BSI zeigen eindeutig: Wenn die richtigen IT-Sicherheitsmaßnahmen konsequent umgesetzt werden, werden die schwerwiegenden Folgen, die ein erfolgreicher Cyberangriff haben kann, drastisch gemildert.

Das BSI unterstützt Unternehmen gerne dabei, diese Maßnahmen zu identifizieren und umzusetzen. Dazu setzen wir auch auf die Kooperation mit starken Partnern wie dem TÜV-Verband.

**Dr. Gerhard Schabhüser**
Vizepräsident des Bundesamts für Sicherheit in der Informationstechnik

# Kernergebnisse

**98 %**

der Unternehmen sehen Cyberangriffe als ernste Gefahr für Wirtschaft und Gesellschaft

**11 %**

verzeichneten in den vergangenen 12 Monaten einen IT-Sicherheitsvorfall

**55 %**

der von Cyberangriffen betroffenen Unternehmen haben den Schutz verstärkt

**61 %**

schreiben Cybersecurity im Unternehmen eine große Rolle zu

**23 %**

nehmen Cyberrisiken bewusst in Kauf

**28 %**

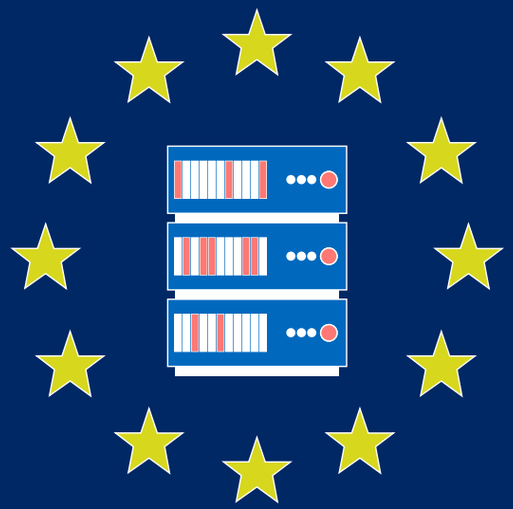
halten einen IT-Sicherheits-vorfall innerhalb des nächsten Jahres für realistisch

**83 %**

wünschen sich mehr Offenheit nach IT-Sicherheitsvorfällen, um das Bewusstsein für die Risiken zu erhöhen

**94 %**

glauben nicht, dass ein absoluter Schutz vor Cyberangriffen möglich ist



**76 %**

sind überzeugt, dass ein hohes IT-Sicherheitsniveau Vorteile im Wettbewerb bringt

**72 %**

stärken ihr Know-how mithilfe von Beratung durch externe Expert:innen

**81 %**

speichern Unternehmensdaten ausschließlich in der EU

**65 %**

ermöglichen ihren Mitarbeitenden mobiles Arbeiten

**26 %**

haben große IT-Sicherheitsprobleme durch das mobile Arbeiten

**64 %**

sprechen sich für gesetzliche Vorgaben für Cybersecurity in Unternehmen aus

**23 %**

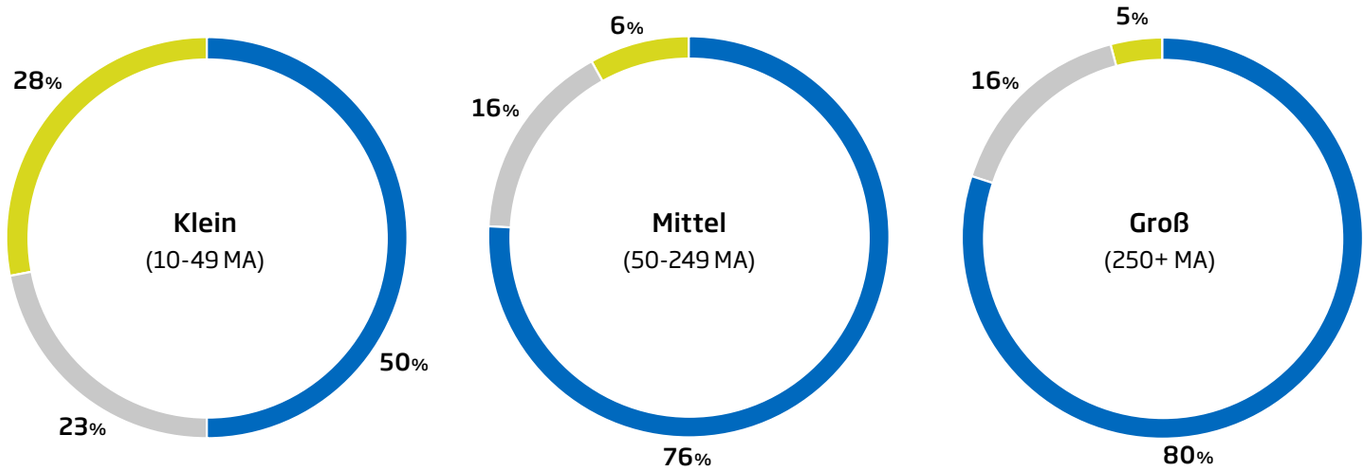
erfüllen bei der Cybersecurity bestimmte Normen und Standards

# Bedeutung von Cybersecurity in der Wirtschaft

1

# Vor allem große Unternehmen haben die Bedeutung der IT-Sicherheit erkannt

## Bedeutung von Cybersecurity in Unternehmen

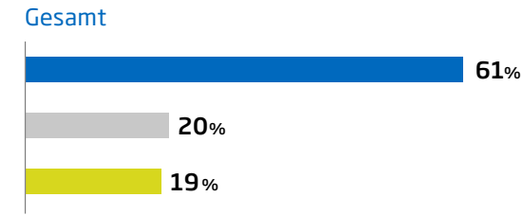



Sehr/eher große Rolle | Weder noch | Eher kleine/überhaupt keine Rolle

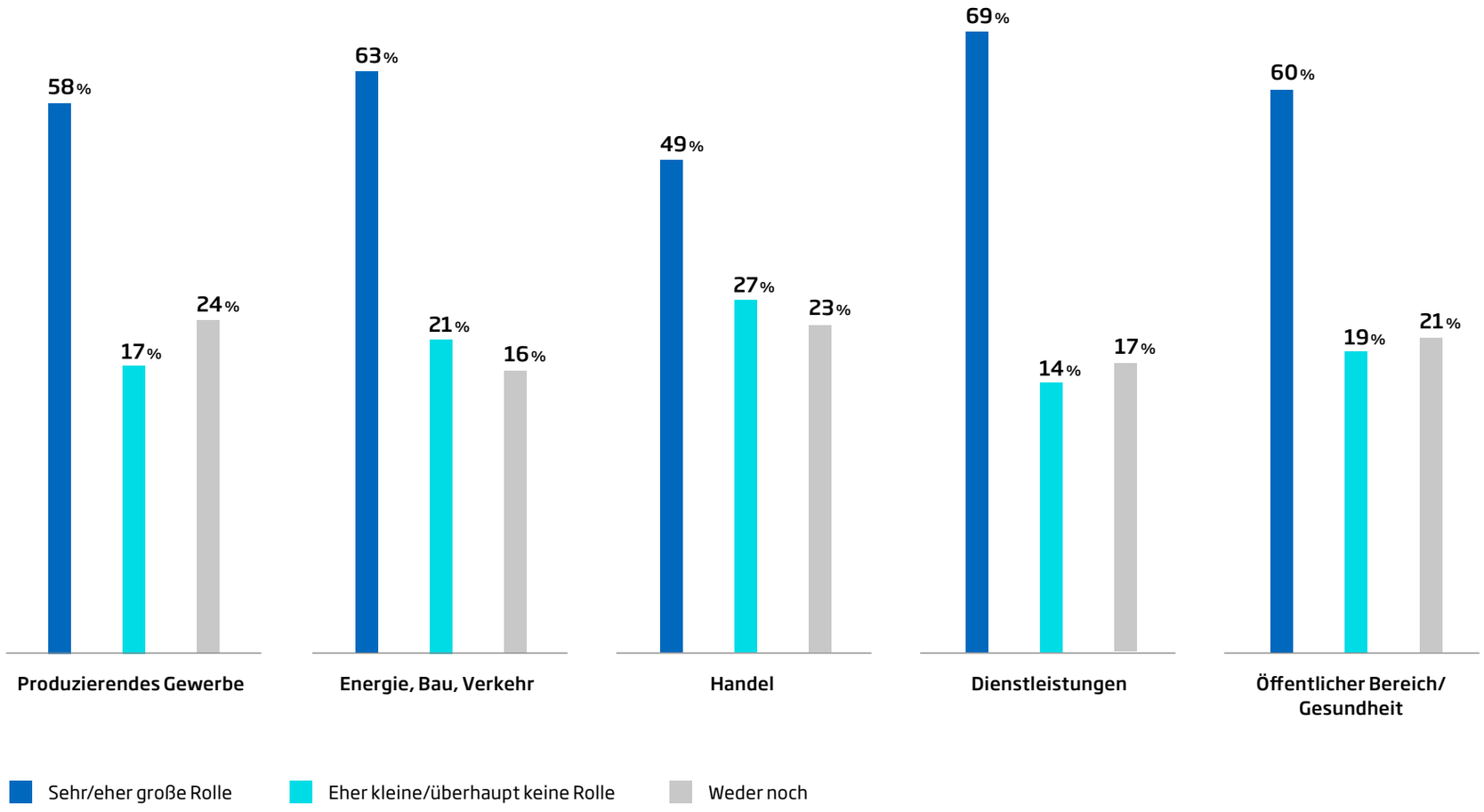
Frage: Welche Rolle spielt Cybersecurity aktuell für Ihr Unternehmen?
Unterteilung nach Unternehmensgröße (Mitarbeiter:innen) | Abweichungen von 100 Prozent sind rundungsbedingt | Basis: 501 befragte Unternehmen

**Besondere Bedeutung genießt der Schutz vor Online-Kriminellen bei großen und mittleren Unternehmen.**

Wie wichtig ist digitale Sicherheit für die Wirtschaft vor dem Hintergrund immer neuer Meldungen über Cyberangriffe auf Unternehmen? Eine große oder sehr große Rolle schreibt eine deutliche Mehrheit der Unternehmen der Cybersicherheit zu (61 Prozent). In großen und mittleren Unternehmen sind es deutlich mehr als in den kleineren. In gut jedem vierten Unternehmen mit 10 bis 49 Mitarbeitenden spielt Cybersecurity eine eher kleine oder überhaupt keine Rolle.



# Bedeutung von Cybersecurity in einzelnen Branchen



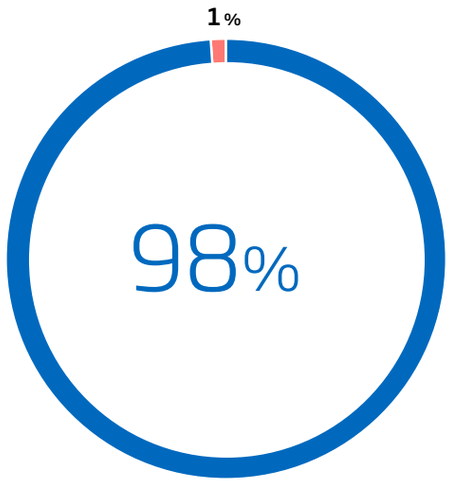

Deutliche Unterschiede bei der Bedeutung von Cybersicherheit zeigen sich beim Blick auf einzelne Branchen. Vergleichsweise gering ist das Bewusstsein dafür im Handel – nur knapp die Hälfte der Unternehmen schreiben ihr eine große Rolle zu. Besonders wichtig ist Cybersicherheit dagegen für Dienstleister (69 Prozent) und im Sektor Energie, Bau, Verkehr (63 Prozent). Im öffentlichen Bereich und im Gesundheitswesen sind es 60 Prozent und im produzierenden Gewerbe immerhin noch 58 Prozent, bei denen Cybersecurity eine große oder sehr große Rolle spielt.

Frage: Welche Rolle spielt Cybersecurity aktuell für Ihr Unternehmen? Unterteilung nach Branche | Abweichungen von 100 Prozent sind rundungsbedingt | Basis: 501 befragte Unternehmen

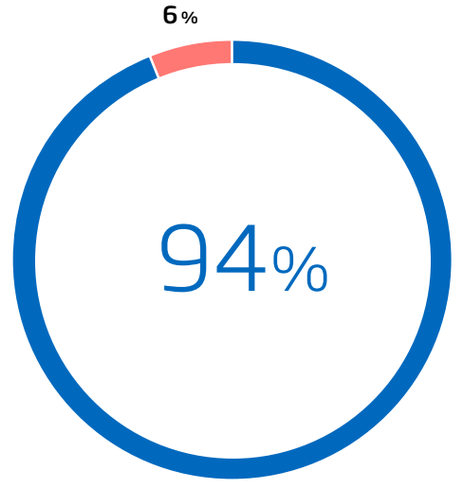
# Starke Cybersicherheit wird zum Wettbewerbsvorteil

## Gefahren durch Cyberattacken und Bedeutung von Sicherheitslösungen

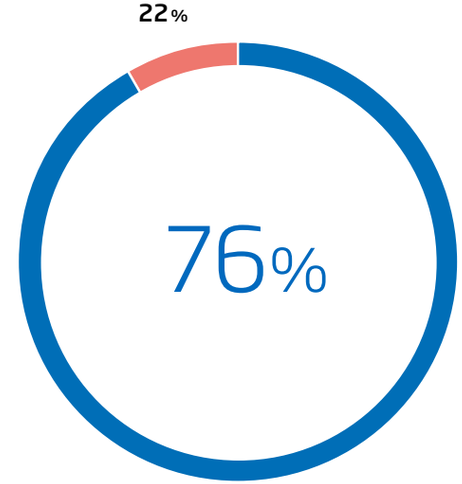
**Cyberangriffe sind eine ernste Gefahr für Wirtschaft und Gesellschaft.**




**Einen absoluten Schutz vor Cyberangriffen gibt es nicht.**




**Ein hohes Niveau an Cybersecurity ist ein Wettbewerbsvorteil.**




Stimme voll/eher zu

Stimme eher nicht/gar nicht zu

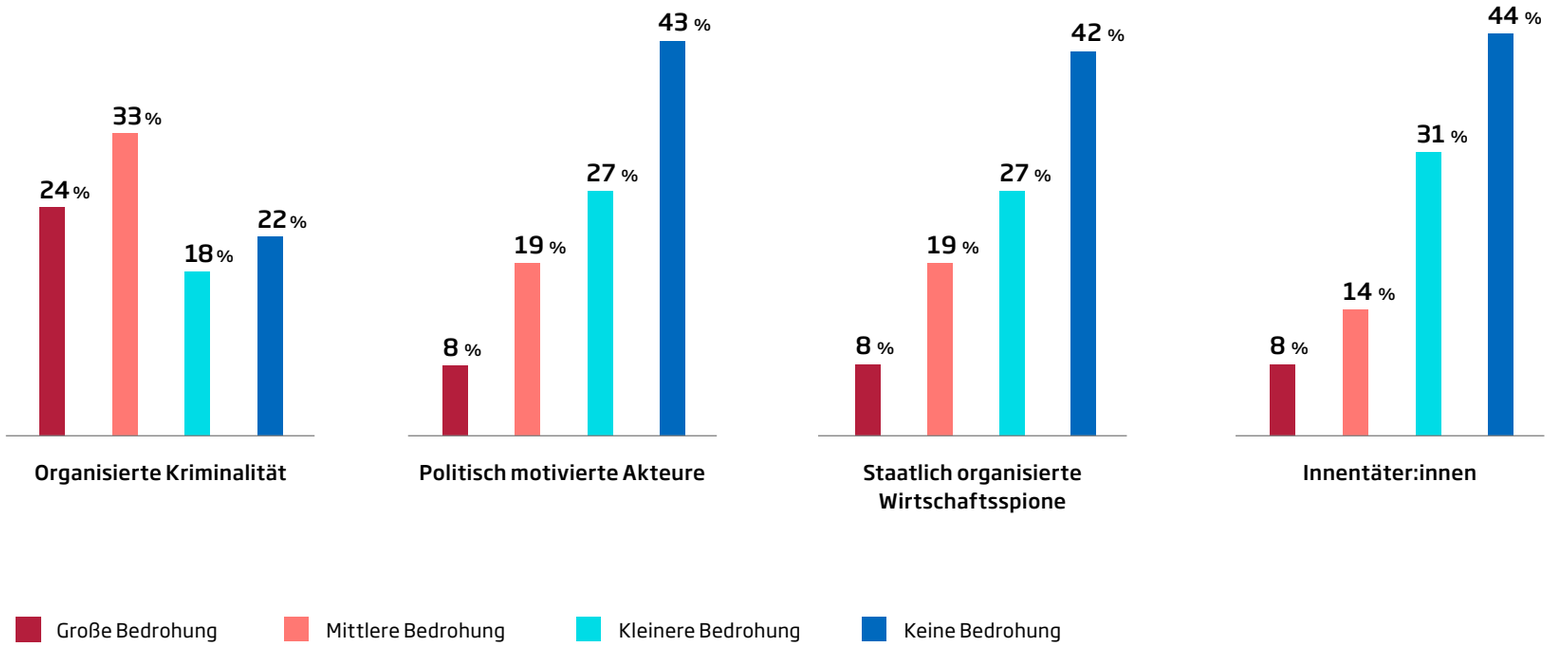
Frage: Inwiefern stimmen Sie folgenden Aussagen zu? | Abweichungen zu 100 Prozent Antworten für "Weiß nicht/Keine Angabe" | Basis: 501 befragte Unternehmen

### Hohes Bewusstsein für Cybergefahren und wirtschaftliche Chancen durch Cybersecurity

Cyberangriffe stellen eine ernste Gefahr für Wirtschaft und Gesellschaft dar – darin sind sich die Befragten einig: Fast alle stimmen dieser Aussage zu. Das Bewusstsein für die Anfälligkeit für kriminelle Cyberattacken ist dabei hoch. Die breite Mehrheit glaubt nicht an einen absoluten Schutz. Umso wichtiger wird digitale Sicherheit: Gut drei Viertel sind der Überzeugung, dass ein hohes Niveau bei der Cybersicherheit einen Vorteil im Wettbewerb darstellt (76 Prozent). Besonders ausgeprägt ist die Zustimmung in diesem Punkt bei mittleren sowie größeren Unternehmen (jeweils 86 Prozent).

# Größte Sorge vor Angriffen organisierter Cyberkriminalität

## Wahrgenommene Bedrohung durch einzelne Tätergruppen




Frage: Bitte geben Sie an, ob die jeweiligen Akteure Ihrer Meinung nach eine große, mittlere, kleine oder keine Bedrohung für die Cybersecurity Ihres Unternehmens darstellen.
Fehlende Angaben zu 100 Prozent Antworten "Weiß nicht/keine Angabe" | Basis: 501 befragte Unternehmen

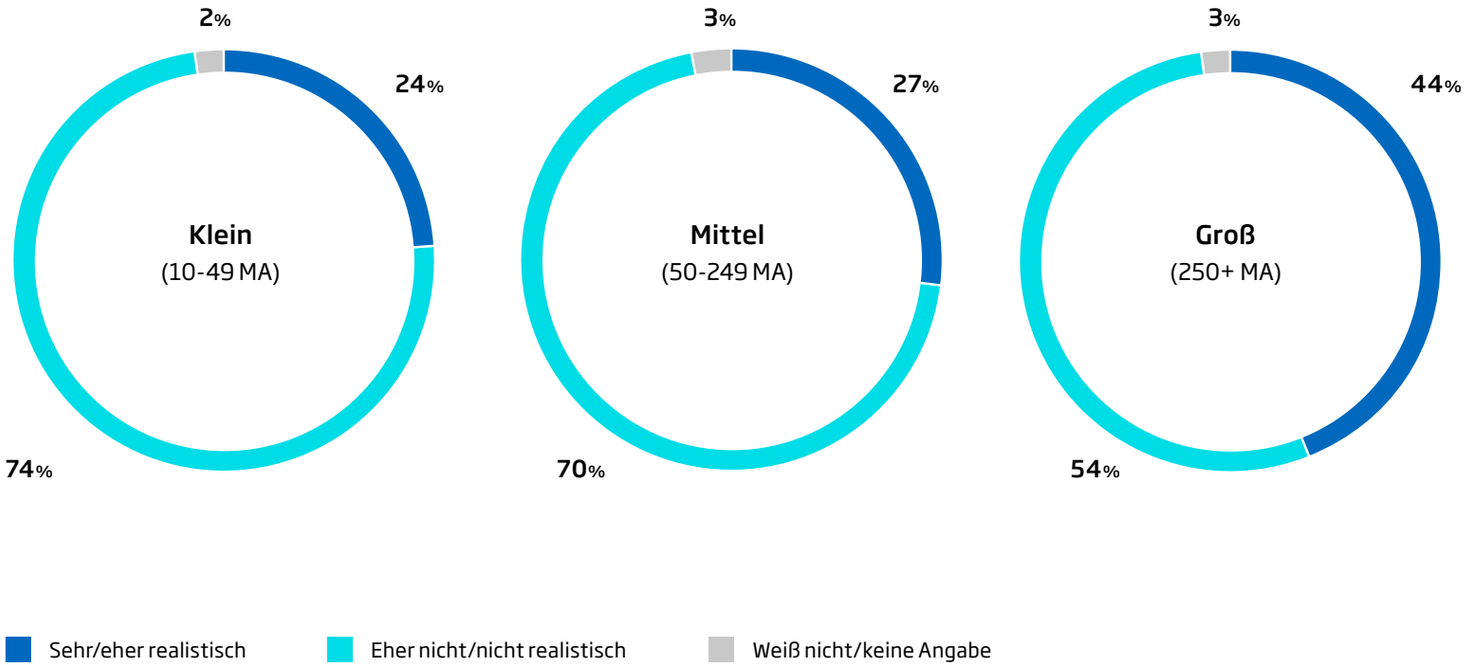
**Kriminelle Banden sind als Cyberangreifer besonders gefürchtet. Im öffentlichen Sektor ist die Angst vor politisch motivierten Täter:innen überdurchschnittlich groß.**

Eine große oder mittlere Cyberbedrohung geht nach Ansicht der Mehrheit der Unternehmen von der organisierten Kriminalität aus (57 Prozent). Politisch motivierte Akteure und staatlich organisierte Wirtschaftsspionage stellen für je 27 Prozent der Unternehmen eine Bedrohung dar. Immerhin 22 Prozent haben die Sorge, dass eigene Beschäftigte oder andere Innentäter:innen Cyberattacken verüben könnten.

Generell schätzen große und mittlere Unternehmen die Bedrohungslage durch einzelne Tätergruppen deutlich höher ein als die kleineren. Im Branchenvergleich ist im produzierenden Gewerbe die Sorge vor Cyberangriffen aus dem Bereich der organisierten Kriminalität am größten: 67 Prozent sehen hier eine mittlere oder große Bedrohung. Der öffentliche Sektor und das Gesundheitswesen fürchtet am stärksten Angriffe von politisch motivierten Akteuren (39 Prozent) und von Innentäter:innen (33 Prozent).

# Ein Cyberangriff ist für viele realistisch

## Risiko eines IT-Sicherheitsvorfalls binnen eines Jahres

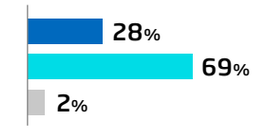



Frage: Für wie realistisch halten Sie die Gefahr, dass es in den kommenden 12 Monaten in Ihrem Unternehmen zu einem schweren IT-Sicherheitsvorfall kommt?
Unterteilung nach Unternehmensgröße (Mitarbeiter:innen) | Basis: 501 befragte Unternehmen

**Vor allem große Unternehmen fürchten, Opfer eines gravierenden IT-Sicherheitsvorfalls zu werden.**

Gut jedes vierte Unternehmen hält es für realistisch, dass es innerhalb der kommenden 12 Monate zu einem schweren IT-Sicherheitsvorfall in ihrem Unternehmen kommt. Dabei sehen sich überdurchschnittlich viele große Unternehmen dieser Gefahr ausgesetzt. Das kann ein Indikator für ein zu geringes Bewusstsein bei kleinen Unternehmen sein. Denn auch sie werden häufig angegriffen und können aufgrund ihrer Rolle in der Lieferkette als Einfallstor in große Unternehmen benutzt werden. Wenn ein Unternehmen bereits Opfer eines Cyberangriffs war, wird das Risiko höher eingeschätzt (44 Prozent), als wenn es in den vergangenen zwölf Monaten keinen Vorfall gab (26 Prozent). Grundsätzlich sollten sich alle Unternehmen der Risiken bewusst sein und sich entsprechend schützen – unabhängig von ihrer Größe und Branche.

Gesamt



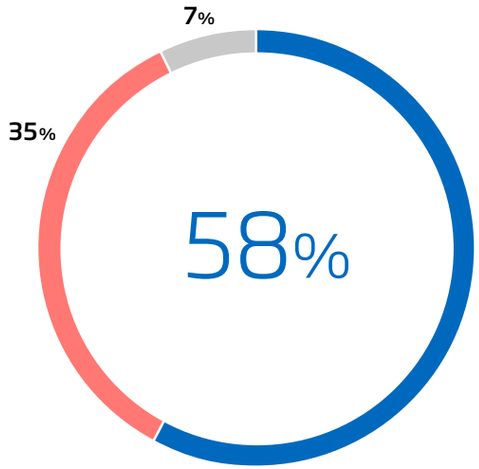

**Wie viele Unternehmen waren bereits Opfer eines Cyberangriffs?**

Anzahl von Angriffen in den letzten 12 Monaten »

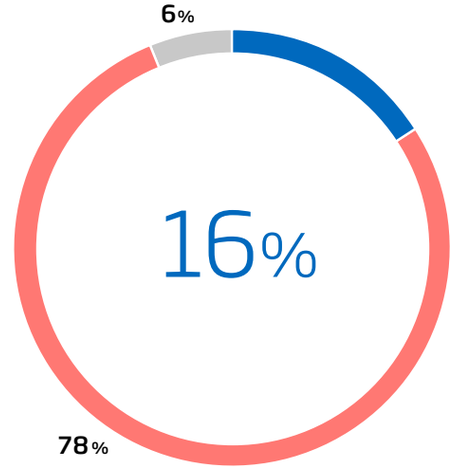
# Ukrainekrieg verschärft das Angriffsrisiko im digitalen Raum

## Cyberrisiken durch den Ukrainekrieg und Zuwachs an Cyberangriffen

**Der Krieg in der Ukraine hat das Risiko von Cyberangriffen stark erhöht**




**Seit Ausbruch des Krieges in der Ukraine verzeichnen wir mehr Cyberangriffe auf unser Unternehmen**

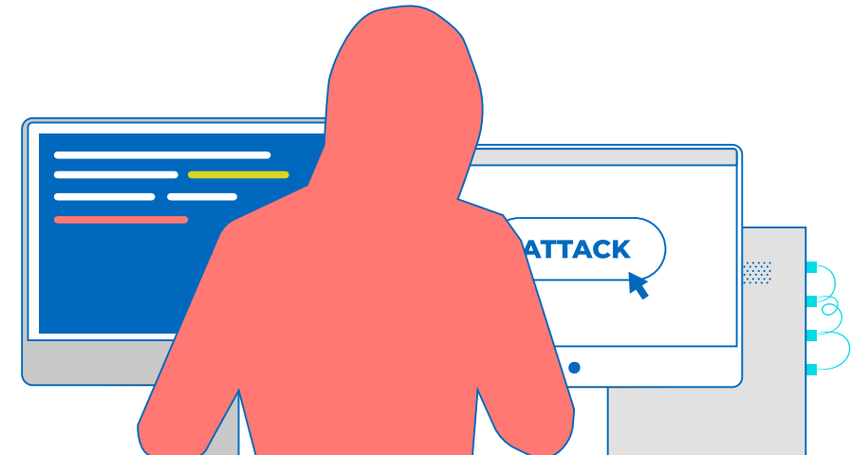



Stimme voll/eher zu | Stimme eher nicht/gar nicht zu | Weiß nicht/keine Angabe

Frage: Inwiefern stimmen Sie folgenden Aussagen zu? | Basis: 501 befragte Unternehmen

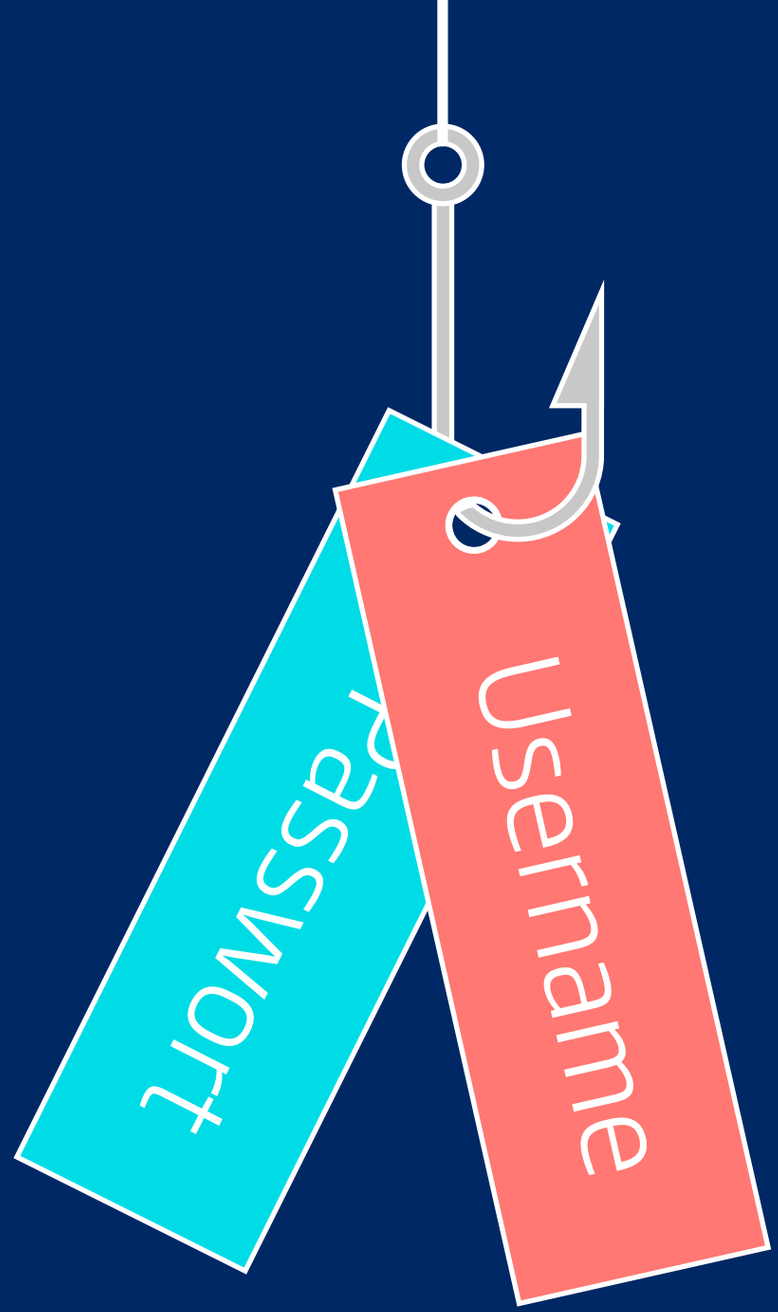
**Der Krieg in der Ukraine schürt die Angst vor Cyberattacken. Tatsächlich hat sich die Zahl der Angriffe nicht so deutlich erhöht wie befürchtet.**

Seit dem Ausbruch des Ukrainekriegs ist das Risiko von Cyberangriffen stark gewachsen – diese Einschätzung teilt mehr als die Hälfte der befragten Unternehmen (58 Prozent). Besonders groß ist die Sorge bei großen Unternehmen (71 Prozent) sowie im öffentlichen Sektor und im Gesundheitswesen (67 Prozent). Geringer wird die Gefahr im Handel bewertet (49 Prozent). Immerhin 16 Prozent der befragten Unternehmen verzeichnen seit Kriegsbeginn tatsächlich mehr Cyberattacken. Mittlere (20 Prozent) und große Unternehmen (27 Prozent) sind überdurchschnittlich häufig betroffen.



# IT-Sicherheitsvorfälle und ihre Folgen

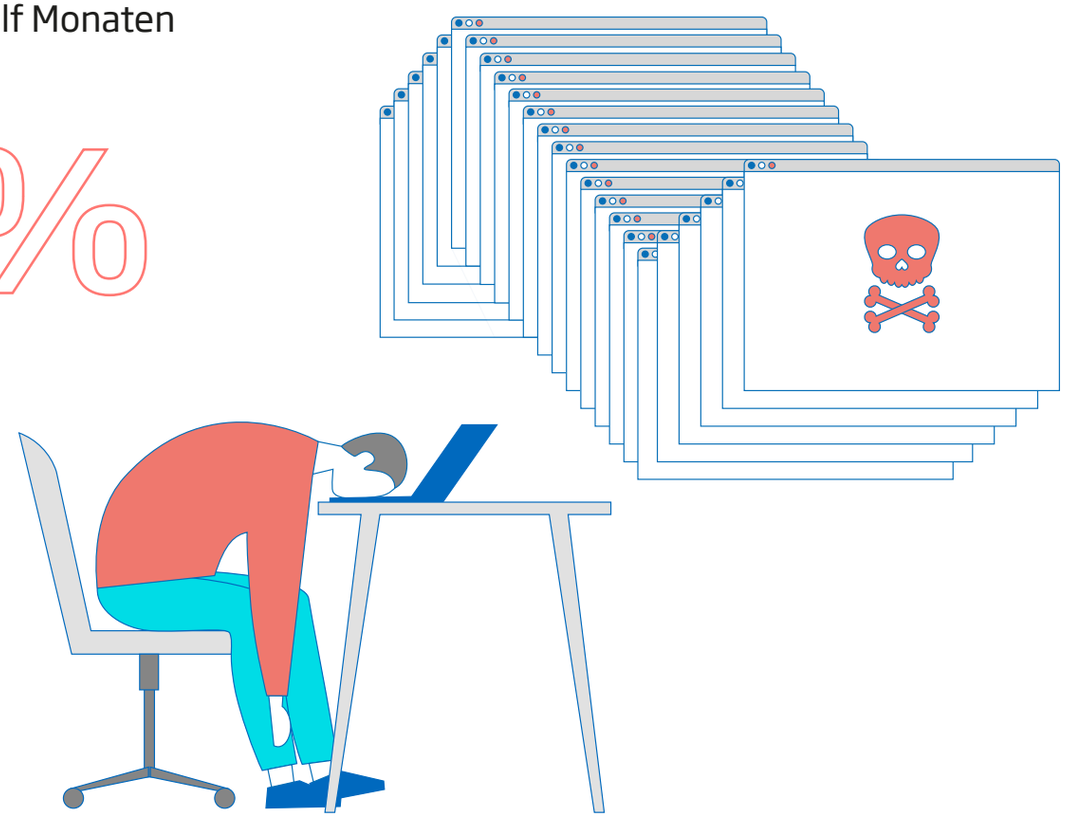
2



# Gut jedes zehnte Unternehmen von IT-Sicherheitsvorfall betroffen

Anteil der Unternehmen mit mindestens einem IT-Sicherheitsvorfall binnen zwölf Monaten

11 %



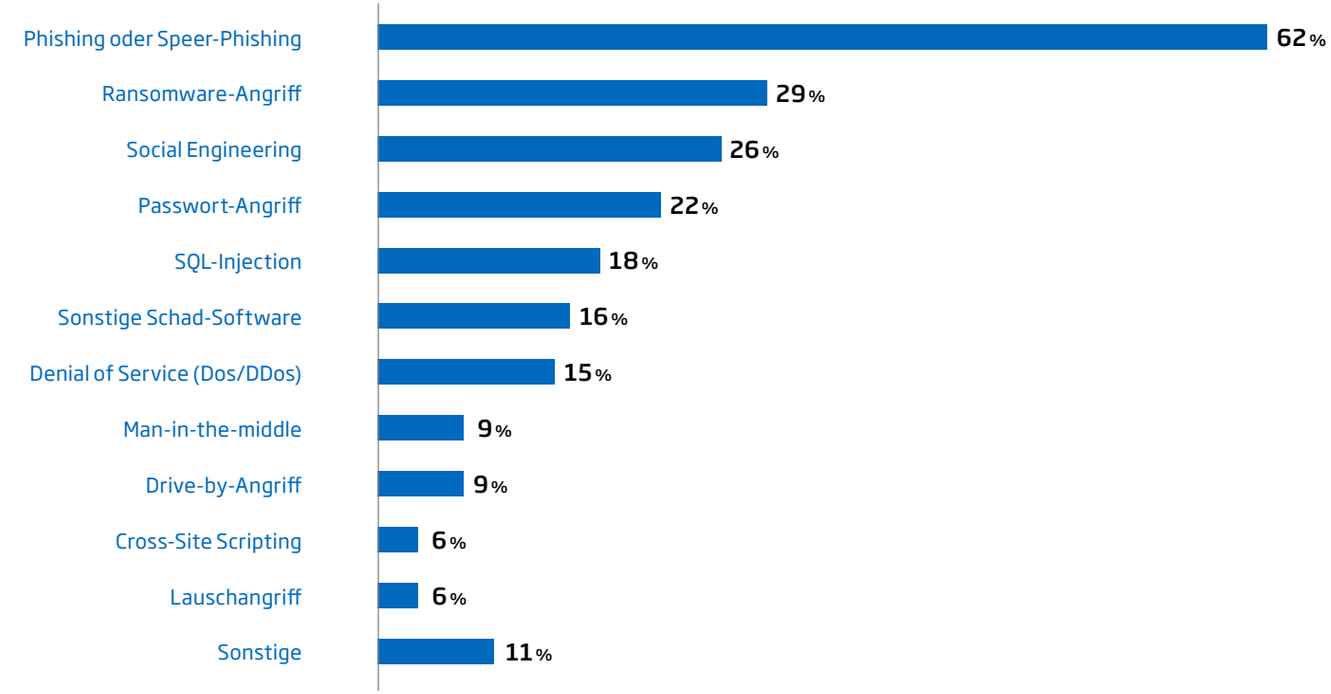
Frage: Hat Ihr Unternehmen in den letzten 12 Monaten einen IT-Sicherheitsvorfall gehabt? | Basis: 501 befragte Unternehmen

**Große Unternehmen sind überproportional häufig von IT-Sicherheitsvorfällen betroffen.**

Gut jedes zehnte Unternehmen war in den vergangenen zwölf Monaten vor der Befragung von mindestens einem IT-Sicherheitsvorfall betroffen (11 Prozent). Mehr als einen IT-Sicherheitsvorfall gab es bei 5 Prozent aller Unternehmen. Der Zeitraum umfasst im wesentlichen das Jahr 2022. Bei IT-Sicherheitsvorfällen handelt es sich um erfolgreiche Cyberangriffe oder andere sicherheitskritische Vorfälle wie Sabotageakte oder Hardware-Diebstahl. Überproportional häufig sind große Unternehmen mit mehr als 250 Mitarbeitenden Opfer eines Cyberangriffs geworden (19 Prozent). Im Dienstleistungssektor sind mit einem Anteil von 13 Prozent und in der Industrie mit 12 Prozent etwas mehr Unternehmen betroffen als im Durchschnitt. Darunter liegen der Handel mit knapp 11 Prozent sowie die Bereiche Energie, Verkehr, Bau (9 Prozent) und der öffentliche Sektor inklusive Gesundheit (9 Prozent).

# Phishing und Ransomware sind die häufigsten Angriffsmethoden

## Art der IT-Sicherheitsvorfälle bei betroffenen Unternehmen




Frage: Um welche Art von IT-Sicherheitsvorfall handelte es sich? (Mehrfachnennungen) | Basis: 55 Befragte, deren Unternehmen in den letzten zwölf Monaten mindestens einen IT-Sicherheitsvorfall hatte

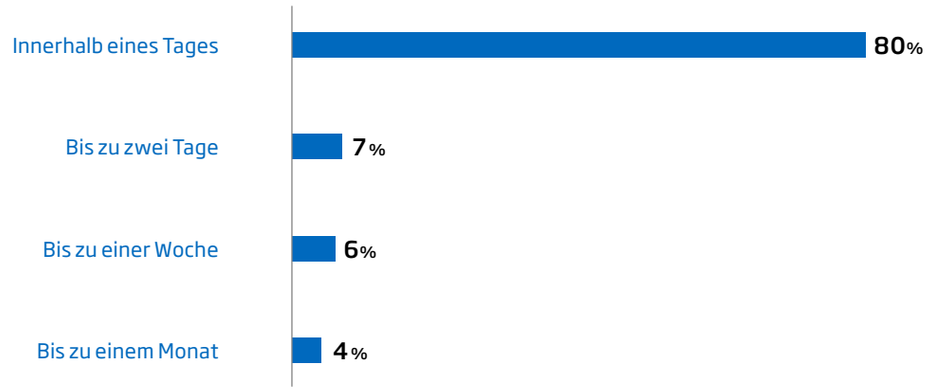
**Cyberkriminelle attackieren Unternehmen mit einer ganzen Reihe von Methoden – von Software bis zur persönlichen Manipulation.**

Am häufigsten werden die von einem IT-Sicherheitsvorfall betroffenen Unternehmen Opfer eines Phishing- oder Speer-Phishing-Angriffs. Beim Phishing versuchen Cyberkriminelle in der Regel, Zugangsdaten ihres Opfers zu erbeuten und damit Zugriff auf relevante Systeme zu erlangen. Speer-Phishing ist ein gezielter Angriff, bei dem Mitarbeitende persönlich angeschrieben werden oder die Angreifer:innen Kenntnisse der Organisation haben, um ihr Ziel zu erreichen. 29 Prozent verzeichneten einen Ransomware-Angriff, bei dem die IT-Systeme einer Organisation lahmgelegt werden und diese dann erpresst werden. An dritter Stelle liegt das so genannte Social Engineering, bei dem Beschäftigte manipuliert werden, um sich Zugang zur IT der Unternehmen zu verschaffen. Weitere erfolgreiche Angriffsmethoden sind das Überwinden des Passwortschutzes, gezielte Datenbankangriffe (SQL-Injection), Denial-of-Service-Angriffe, die zum zeitweisen Ausfall eines Dienstes führen oder Man-in-the-Middle-Angriffe, bei denen sich Cyberkriminelle in die Kommunikation innerhalb eines Netzwerks einklinken.

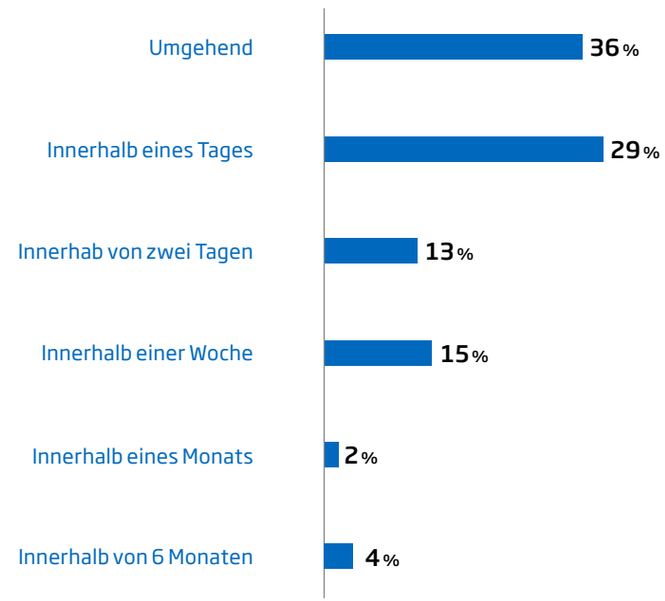
# Die meisten Angriffe werden rasch erkannt und behoben

## Wie schnell Unternehmen auf einen IT-Sicherheitsvorfall reagieren

**Dauer bis zur Erkennung**




**Dauer bis zur Behebung**




Frage: Wie lange haben Sie gebraucht um den IT-Sicherheitsvorfall zu erkennen?
Wie schnell konnte der Sicherheitsvorfall behoben werden? | Fehlende Angaben zu 100 Prozent Antworten für "Weiß nicht/Keine Angabe"
Basis: 55 Befragte, deren Unternehmen in den letzten zwölf Monaten mindestens einen IT-Sicherheitsvorfall hatte

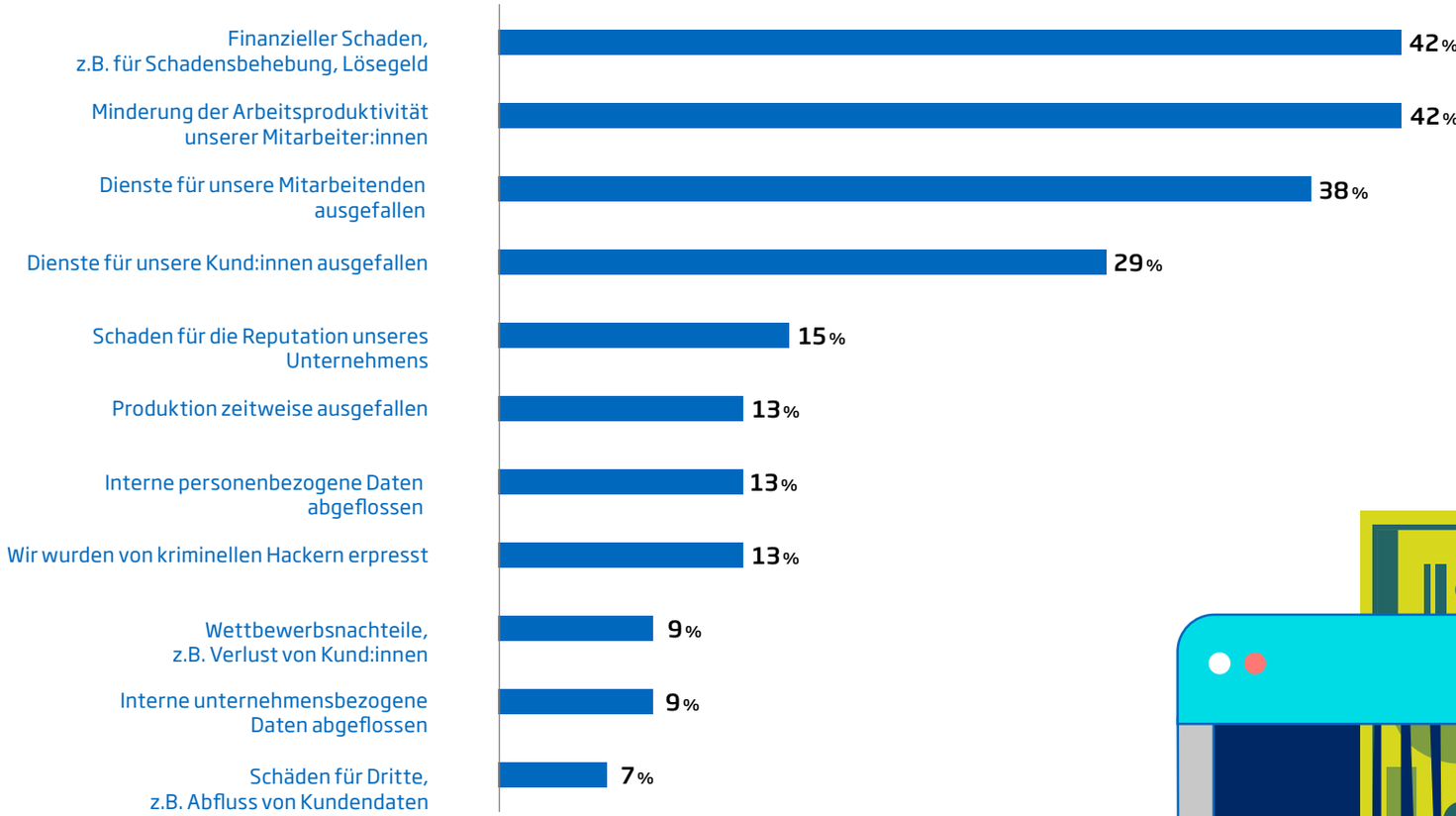
**Erfolgreiche Attacken bekommen Unternehmen in den meisten Fällen rasch in den Griff. Teils dauert die Behebung des Vorfalls auch Wochen und Monate.**

Die meisten IT-Sicherheitsvorfälle werden rasch erkannt. Vier von fünf der betroffenen Unternehmen konnten erfolgreiche Attacken innerhalb eines Tages aufdecken. Weitere 7 Prozent brauchten 2 Tage, 6 Prozent bis zu einer Woche. In gut einem Drittel der Fälle gelang es, das Problem umgehend zu beheben – bis zu einem Tag dauerte dies bei knapp einem Drittel. Ein beträchtlicher Teil der erfolgreich attackierten Unternehmen arbeitete bis zu eine Woche lang an der Behebung (15 Prozent). Immerhin 6 Prozent benötigten länger als eine Woche.

Trotz dieser insgesamt positiven Selbsteinschätzung der Befragten gehen Sicherheitsbehörden von einer hohen Dunkelziffer nicht erkannter Cyberangriffe aus. Gerade bei komplexeren Angriffen kann es mitunter Wochen dauern, bis alle Systeme wieder stabil laufen.

# Die Folgen: Finanzielle Schäden, Systemausfälle, Datenklau

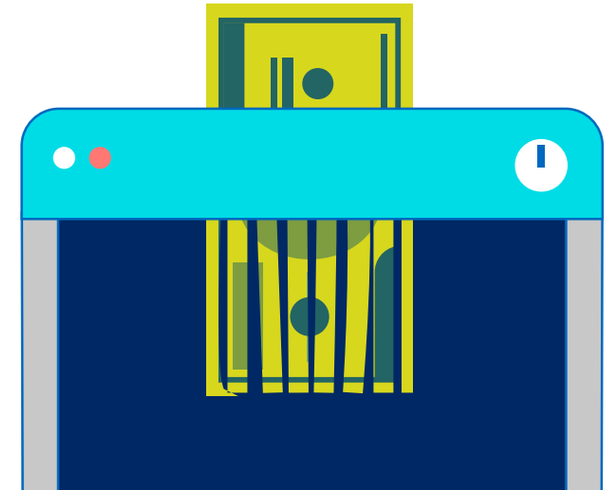
## Folgen der IT-Sicherheitsvorfälle




Frage: Sind einer oder mehrere dieser möglichen Folgen durch die letzten IT-Sicherheitsvorfälle in Ihrem Unternehmen eingetreten? (Mehrfachnennungen)
Basis: 55 Befragte, deren Unternehmen in den letzten zwölf Monaten mindestens einen IT-Sicherheitsvorfall hatte

**Erfolgreiche Cyberangriffe führen zu einer Vielzahl von Schäden – bis hin zum Verlust von Reputation und Kunden.**

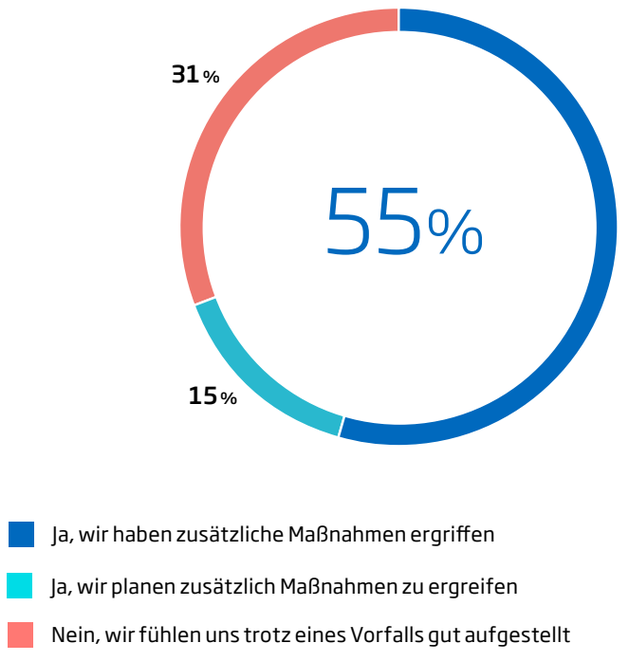
Lösegeldzahlung, entgangener Umsatz, Ausgaben für die Wiederherstellung der IT: Als Folge eines Sicherheitsvorfalls berichten jeweils gut vier von zehn Unternehmen von finanziellen Schäden sowie von einer verminderten Arbeitsproduktivität. Bei 38 Prozent der betroffenen Unternehmen fielen Dienste für Beschäftigte aus. Dienste für Kund:innen waren bei knapp drei von zehn Unternehmen nach einer IT-Attacke nicht mehr verfügbar. Von einem Reputationsschaden geht knapp jedes siebte Unternehmen aus, das Opfer eines Cyberangriffs wurde. Viele Unternehmen berichten von weiteren Schäden: Bei jeweils gut jedem achten Unternehmen ist die Produktion ausgefallen, sind personenbezogene Daten abgeflossen oder das betroffene Unternehmen wurde von kriminellen Hackern erpresst.



# Die Mehrzahl der Betroffenen investiert in besseren Schutz

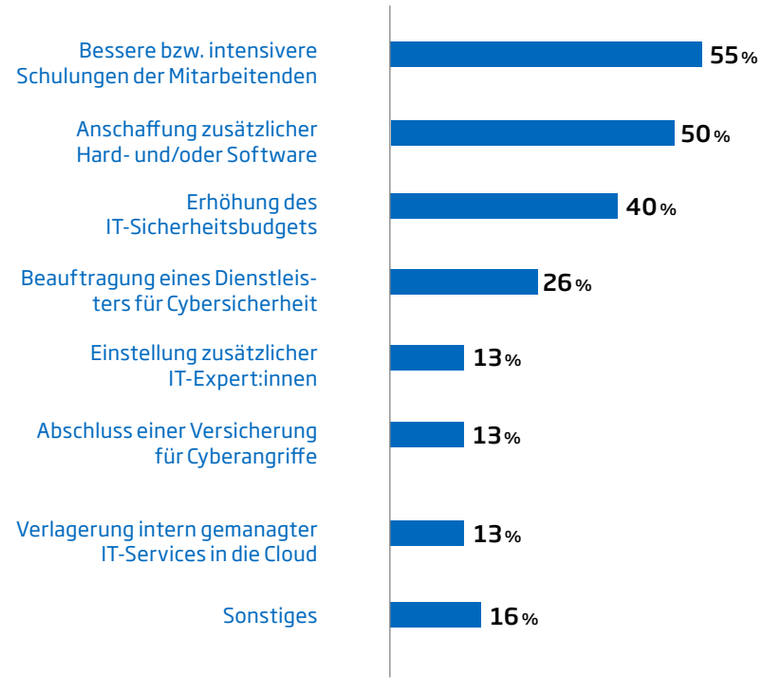
## Zusätzliche Schutzmaßnahmen nach einem IT-Sicherheitsvorfall

### Maßnahmenplanung in Folge eines Sicherheitsvorfalls




Frage: Haben Sie im Nachgang des IT-Sicherheitsvorfalls Ihre Maßnahmen zum Schutz vor Cyberangriffen verstärkt? | Abweichungen zu 100 Prozent sind rundungsbedingt | Basis: 55 Befragte, deren Unternehmen in den letzten zwölf Monaten mindestens einen IT-Sicherheitsvorfall hatte

### Art der Maßnahmen




Frage: Welche Maßnahmen haben Sie ergriffen oder planen Sie als Folge des IT-Sicherheitsvorfalls? (Mehrfachnennungen) | Basis: 38 Befragte, die aufgrund eines Sicherheitsvorfalles planen Maßnahmen zu ergreifen, bzw. Maßnahmen bereits ergriffen haben

**Schulungen für Mitarbeitende und ein erhöhtes IT-Sicherheitsbudget zählen zu den wichtigsten Maßnahmen nach einem IT-Sicherheitsvorfall.**

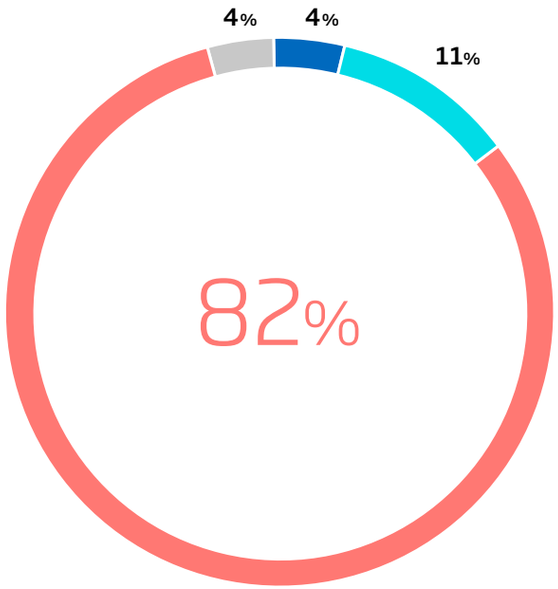
Nach einer erfolgreichen Cyberattacke erhöht die Mehrheit der Unternehmen den Einsatz für einen besseren Schutz. Mehr als die Hälfte der in den vergangenen zwölf Monaten Betroffenen hat zusätzliche Maßnahmen für die IT-Sicherheit ergriffen, weitere 15 Prozent planen das. Knapp ein Drittel sieht sich trotz des Sicherheitsvorfalls gut aufgestellt. Um künftig besser gegen Attacken gewappnet zu sein, werden vor allem Mitarbeitende geschult, neue Hard- oder Software angeschafft und das Budget für die IT-Sicherheit aufgestockt. Gut ein Viertel beauftragt für die IT-Sicherheit einen Dienstleister.

**Welche Maßnahmen ergreifen Unternehmen allgemein zur Erhöhung der Cybersicherheit?**

Maßnahmen und Investitionen für einen besseren Schutz ››

# Die meisten schweigen über IT-Sicherheitsvorfälle

## Information der Öffentlichkeit über Cyberangriffe




- Ja, wir waren dazu verpflichtet
- Ja, wir haben informiert, obwohl wir dazu nicht verpflichtet waren
- Nein
- Weiß nicht/keine Angabe

**Verpflichtung zur Veröffentlichung eines IT-Angriffs besteht nur bei einem Bruchteil der Betroffenen.**

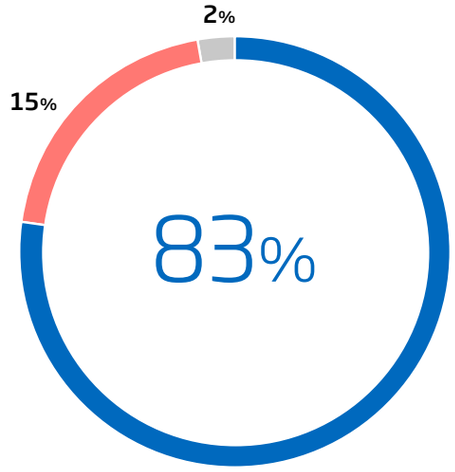
Die große Mehrheit der Unternehmen entscheidet sich für Stillschweigen, wenn sie von einem Cyberangriff betroffen sind (82 Prozent). Nur 15 Prozent haben die Öffentlichkeit informiert: 11 Prozent freiwillig und 4 Prozent, weil sie gesetzlich dazu verpflichtet waren. Letzteres ist unter anderem der Fall, wenn personenbezogene Daten als Folge eines Cyberangriffs abfließen.

Frage: Haben Sie die Öffentlichkeit über den IT-Sicherheitsvorfall informiert? | Abweichungen zu 100 % sind rundungsbedingt
Basis: 55 Befragte, deren Unternehmen in den letzten zwölf Monaten mindestens einen IT-Sicherheitsvorfall hatte

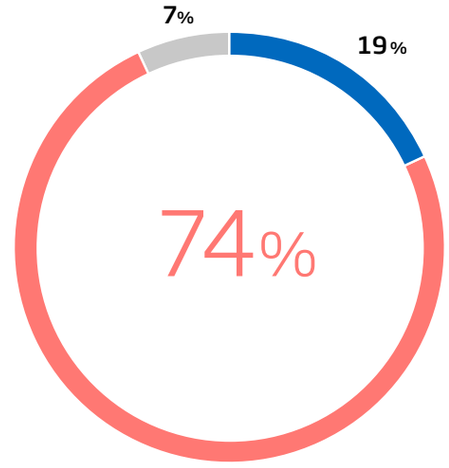
# Wunsch nach mehr Offenheit bei Cyberangriffen

## Transparenz bei Sicherheitsvorfällen

**Sollten mehr Unternehmen bei Cybersicherheitsvorfällen an die Öffentlichkeit gehen, um das Bewusstsein für die Risiken zu stärken?**




**Wir vermeiden die Veröffentlichung eines Cybersicherheitsvorfalls, weil wir einen Reputationsschaden für das Unternehmen befürchten.**




Stimme voll/eher zu | Stimme eher nicht /gar nicht zu | Weiß nicht/keine Angabe

Frage: Inwiefern stimmen Sie folgenden Aussagen zu? | Basis: 501 befragte Unternehmen

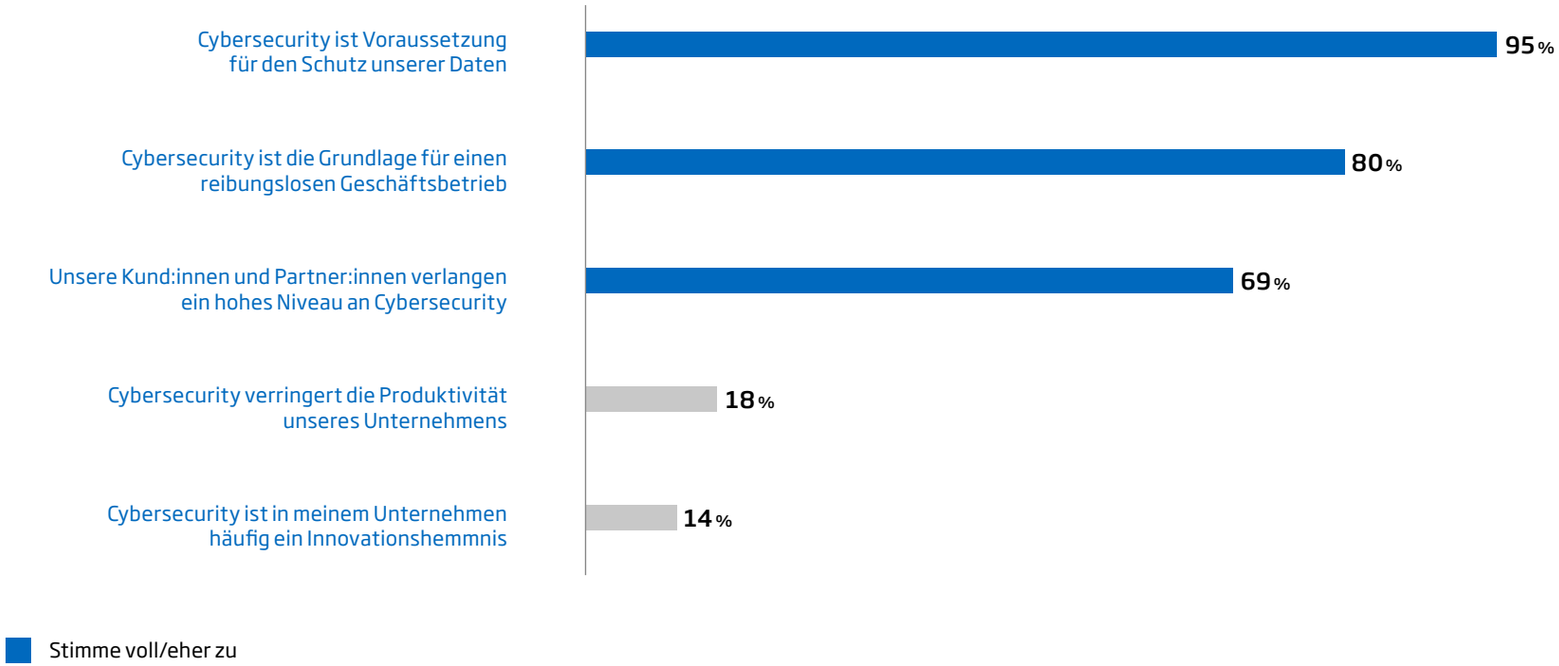
**Größere Transparenz nach erfolgreichen Cyberattacken stärkt nach Ansicht der Befragten das Bewusstsein für Gefahren.**

Eine deutliche Mehrheit der Befragten befürwortet es, dass mehr Unternehmen nach IT-Sicherheitsvorfällen an die Öffentlichkeit gehen, um das Bewusstsein für Cyberrisiken zu stärken. Nur knapp jedes fünfte Unternehmen vermeidet die Veröffentlichung eines Cyberangriffs, weil es einen Reputationsschaden befürchtet. Das steht im Widerspruch zur vorangegangenen Frage. ›› Die meisten Unternehmen handeln offenbar weniger transparent, als gedacht, wenn sie tatsächlich von einem Cyberangriff betroffen sind.

# Cybersecurity im Betriebsablauf

# Kunden und Partner als Motor für mehr Cybersecurity

## Motivation für IT-Sicherheitsmaßnahmen und mögliche Nachteile




Frage: Inwiefern stimmen Sie folgenden Aussagen zu? | Basis: 501 befragte Unternehmen

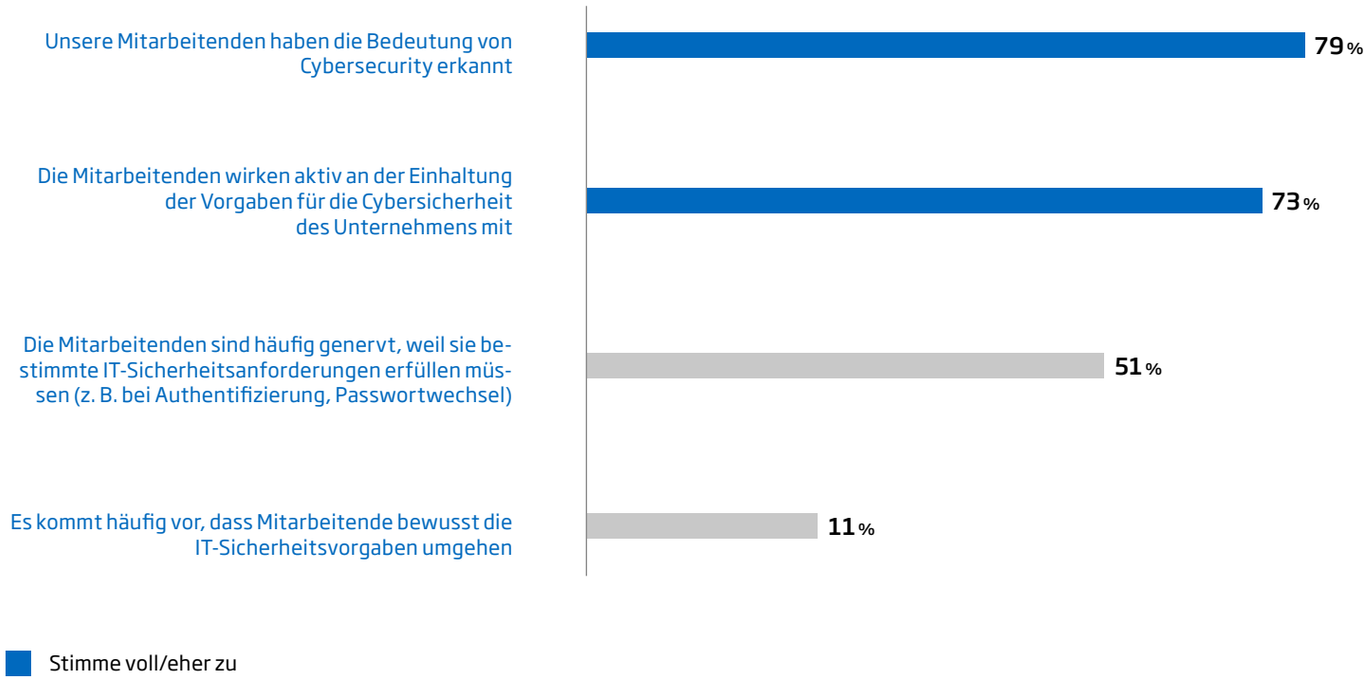
**IT-Sicherheit sichert in vielen Unternehmen den reibungslosen Geschäftsablauf. Eine Minderheit sieht auch geschäftliche Nachteile durch die Schutzmaßnahmen.**

Welche Motivation haben Unternehmen, mehr für die Sicherheit ihrer IT-Systeme zu tun? Cybersecurity ist Voraussetzung für den Schutz von Daten – fast alle Unternehmen stimmen dieser Aussage zu. Vier von fünf Befragten sehen Cybersecurity als Grundlage für einen reibungslosen Geschäftsbetrieb. Ein Motor für IT-Sicherheit sind für gut zwei Drittel der Unternehmen ihre Kund:innen und Partner:innen, die ein hohes Niveau erwarten oder sogar entsprechende Vorgaben machen (69 Prozent). Besonders gilt dies in mittleren und großen Unternehmen (je 79 Prozent).

Auf der anderen Seite ist fast jedes fünfte Unternehmen der Meinung, dass Cybersecurity die Produktivität senkt. Als Innovationshemmnis wird sie von jedem siebten Unternehmen wahrgenommen.

# Mehrheit der Beschäftigten trägt IT-Sicherheitsvorgaben mit

## Einstellung der Mitarbeitenden zu Cybersecurity-Maßnahmen




Frage: Inwiefern stimmen Sie folgenden Aussagen zu? | Basis: 501 befragte Unternehmen

**Mitarbeitende erkennen Cybersecurity-Vorgaben mehrheitlich als wichtig an und unterstützen sie – auch wenn die Regeln im Alltag oft als nervig empfunden werden.**

In den meisten Unternehmen haben die Mitarbeitenden die Bedeutung von Cybersecurity erkannt – knapp vier von fünf Befragten stimmen dieser Aussage zu. Fast drei Viertel der Beschäftigten wirken an der Einhaltung entsprechender Vorgaben mit.

Auf der anderen Seite können Maßnahmen für die IT-Sicherheit wie komplizierte Verfahren für die Authentifizierung oder häufige Passwortwechsel von den Mitarbeitenden als störend empfunden werden. Gut die Hälfte der Unternehmen gibt an, dass die Mitarbeitenden häufig davon genervt sind, Anforderungen für die IT-Sicherheit einhalten zu müssen. Das gilt besonders im öffentlichen Sektor und Gesundheitswesen (66 Prozent). Bei 11 Prozent der Unternehmen kommt es regelmäßig vor, dass Beschäftigte IT-Sicherheitsvorgaben umgehen.

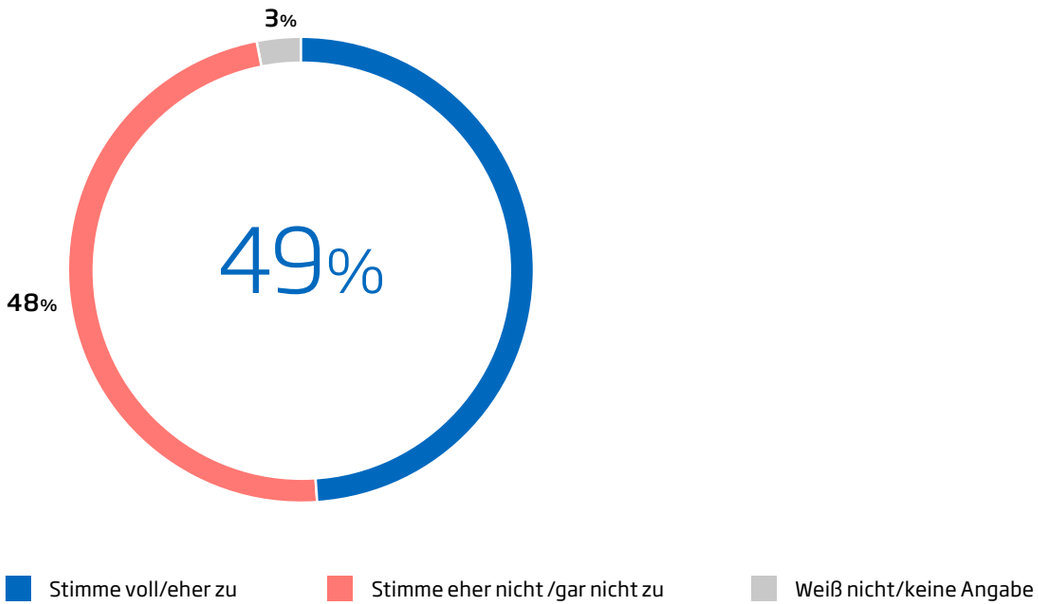
# Fachkräftemangel: Unternehmen weichen auf Dienstleister aus

## Auswirkungen des Fachkräftemangels auf die digitale Sicherheit

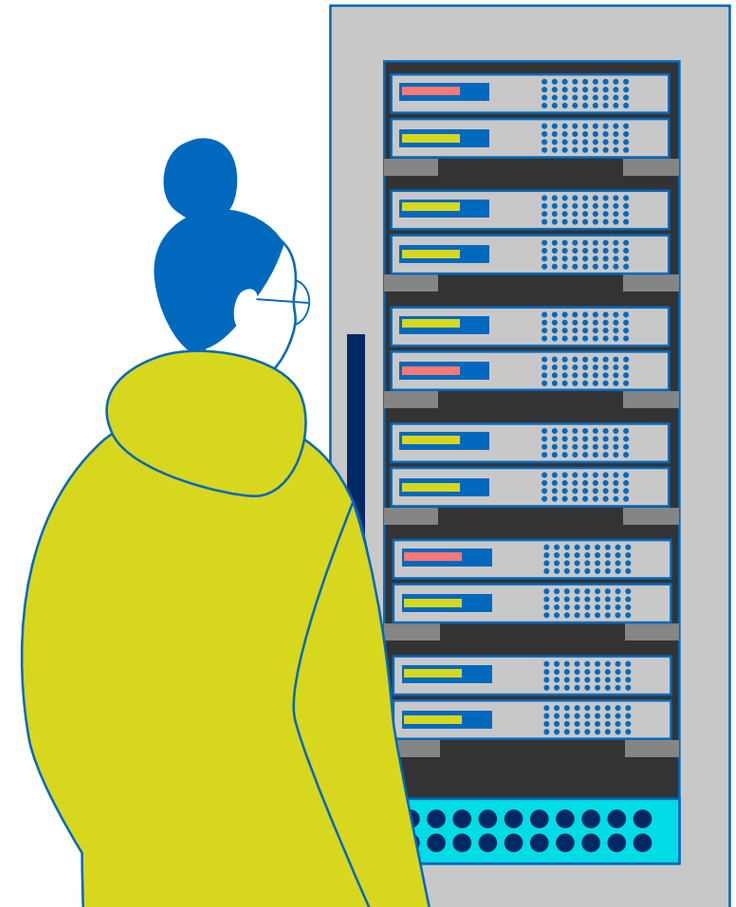
### Engpass bei IT-Expert:innen hat Folgen.

Der Fachkräftemangel im Bereich der Informationstechnologie erhöht die Abhängigkeit von externen Dienstleistern. Knapp die Hälfte der Unternehmen ist zunehmend auf externe Unterstützung angewiesen (49 Prozent).

**Aufgrund des IT-Fachkräftemangels sind wir zunehmend auf externe Dienstleister angewiesen.**




Frage: Inwiefern stimmen Sie folgenden Aussagen zu? | Basis: 501 befragte Unternehmen

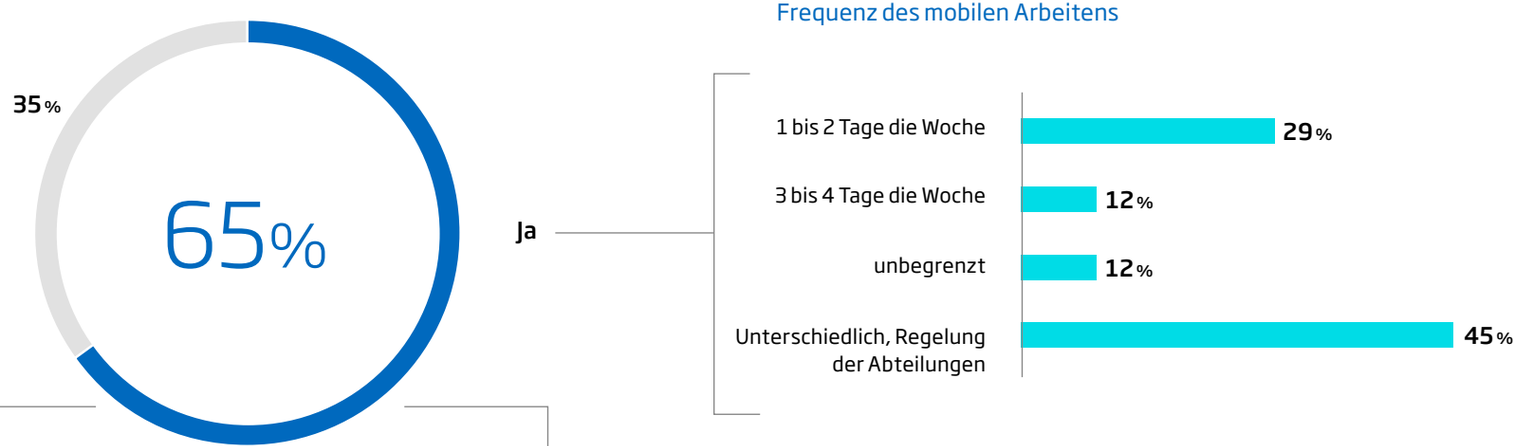


# Digitale Sicherheit beim mobilen Arbeiten

4

# Mobiles Arbeiten hat sich etabliert

## Möglichkeiten des mobilen Arbeitens in Unternehmen




### Unternehmensgröße

**53%** (10-49 MA)

**79%** (50-249 MA)

**87%** (ab 250 MA)

### Branchen

**78%** Dienstleistungen

**73%** Öffentlicher Bereich, Gesundheit

**64%** Produzierendes Gewerbe

**51%** Energie, Verkehr, Bau

**48%** Handel

Frage: Bietet Ihr Unternehmen Ihren Mitarbeitenden mobiles Arbeiten an?
Basis: 501 befragte Unternehmen

Frage: An wie vielen Tagen dürfen die Mitarbeitenden Ihres Unternehmens innerhalb einer Woche mobil arbeiten?
Abweichungen zu 100 Prozent sind rundungsbedingt | Basis: 326 Befragte, deren Unternehmen mobiles Arbeiten anbietet

**Das Homeoffice ist in der Mehrzahl der Unternehmen heute eine Selbstverständlichkeit. Unterschiede zeigen sich bei der Frage, wie viel Zeit Mitarbeitende außerhalb des Betriebs tätig sein dürfen.**

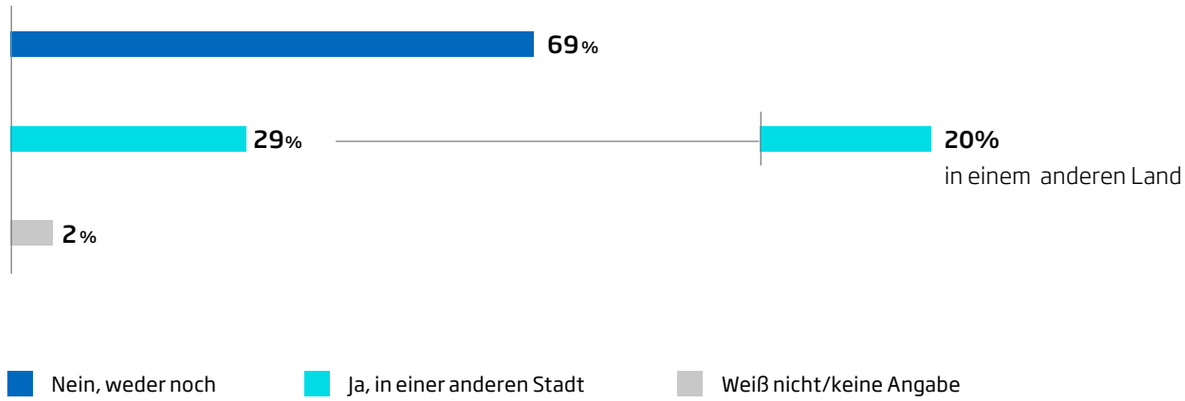
Auch nach dem Ende der Corona-Pandemie gehört mobiles Arbeiten vielerorts zum Standard. Knapp zwei Drittel der Befragten bieten ihren Beschäftigten diese Möglichkeit an. Vorreiter sind große Unternehmen mit einem Anteil von 87 Prozent und mittlere Unternehmen mit 79 Prozent. Dagegen ermöglicht nur gut jedes zweite kleinere Unternehmen mit 10 bis 49 Mitarbeitenden das mobile Arbeiten. Erlaubt sind bei knapp einem Drittel ein bis zwei Tage Homeoffice. Zeitlich unbegrenzt ist dies bei rund jedem achten Unternehmen möglich. Am häufigsten finden sich unterschiedliche Regeln einzelner Abteilungen (45 Prozent). Besonders Homeoffice-freundlich zeigt sich das Dienstleistungsgewerbe (78 Prozent), eher zurückhaltend ist der Handel (48 Prozent).

**Ist das Homeoffice gefährlich für die Cybersicherheit?**

Sicherheitsrisiken von mobilem Arbeiten ››

# Fast jeder dritte Arbeitgeber ermöglicht Workation

## Möglichkeiten der Arbeit abseits des eigentlichen Standorts für eine längere Zeit



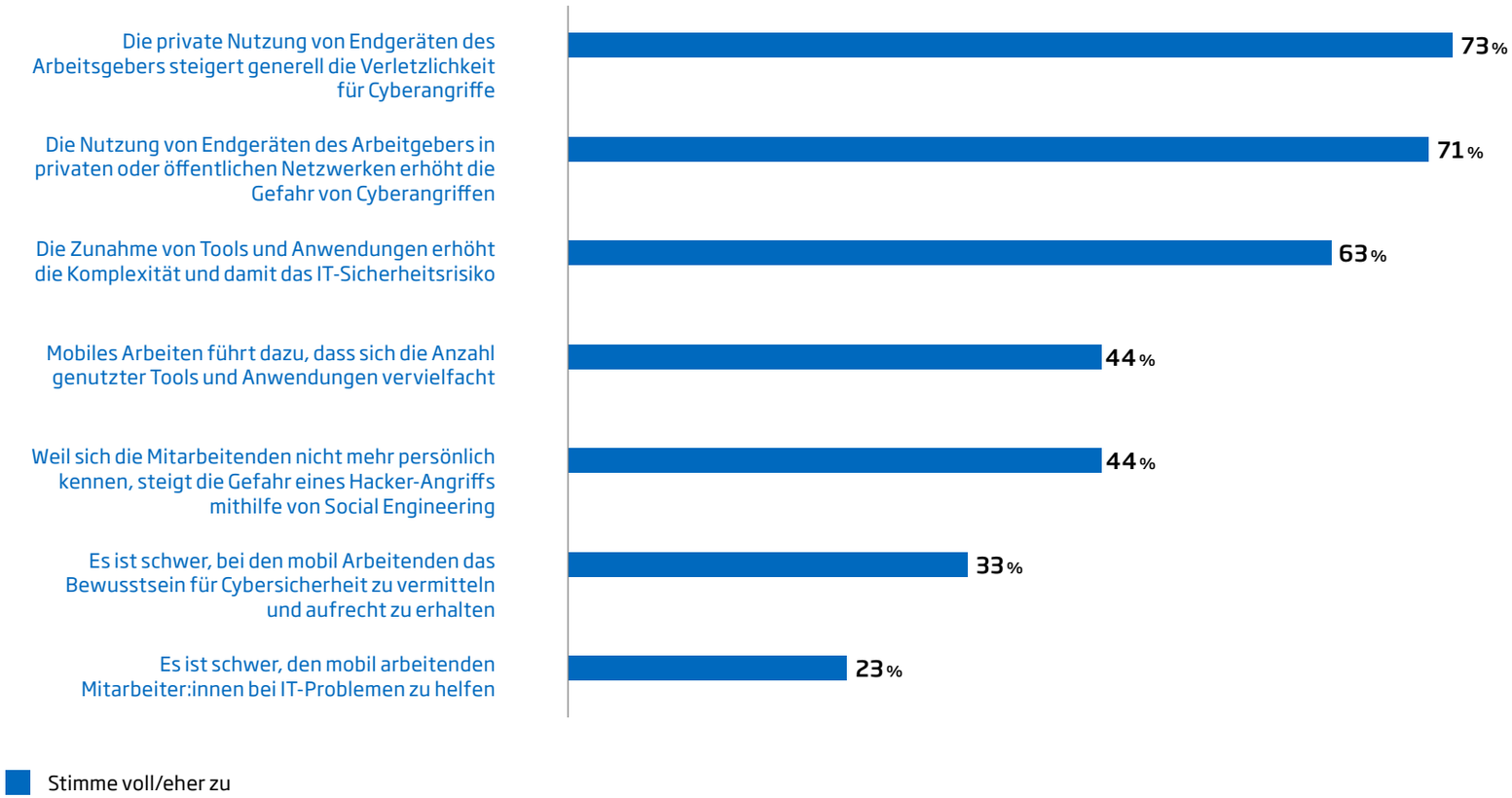

Frage: Ist es in ihrem Unternehmen möglich, dass Mitarbeitende auch abseits ihres eigentlichen Standorts für längere Zeit in einer anderen Stadt und/oder in einem anderen Land arbeiten? (Mehrfachnennungen möglich) | Basis: 501 befragte Unternehmen

**Viele Firmen sind zurückhaltend bei der Akzeptanz eines längeren Aufenthalts in einer anderen Stadt oder sogar in einem anderen Land, um von dort aus mobil zu arbeiten.**

Noch deutlich weniger Zustimmung als das Homeoffice erhält die Möglichkeit, für einen längeren Zeitraum abseits des eigentlichen Standorts in einer anderen Stadt innerhalb Deutschlands oder sogar im Ausland zu arbeiten. Workation heißt der Trend – ein Mischwort aus den englischen Begriffen Work (Arbeit) und Vacation (Urlaub). Knapp jedes dritte Unternehmen ermöglicht seinen Mitarbeitenden Workation (29 Prozent). 29 Prozent gestatten längere Ortswechsel innerhalb des Landes und ein Fünftel erlaubt auch das grenzüberschreitende Arbeiten.

# Private Nutzung von Firmengeräten birgt Gefahren

## Risiken für die Cybersicherheit durch mobiles Arbeiten



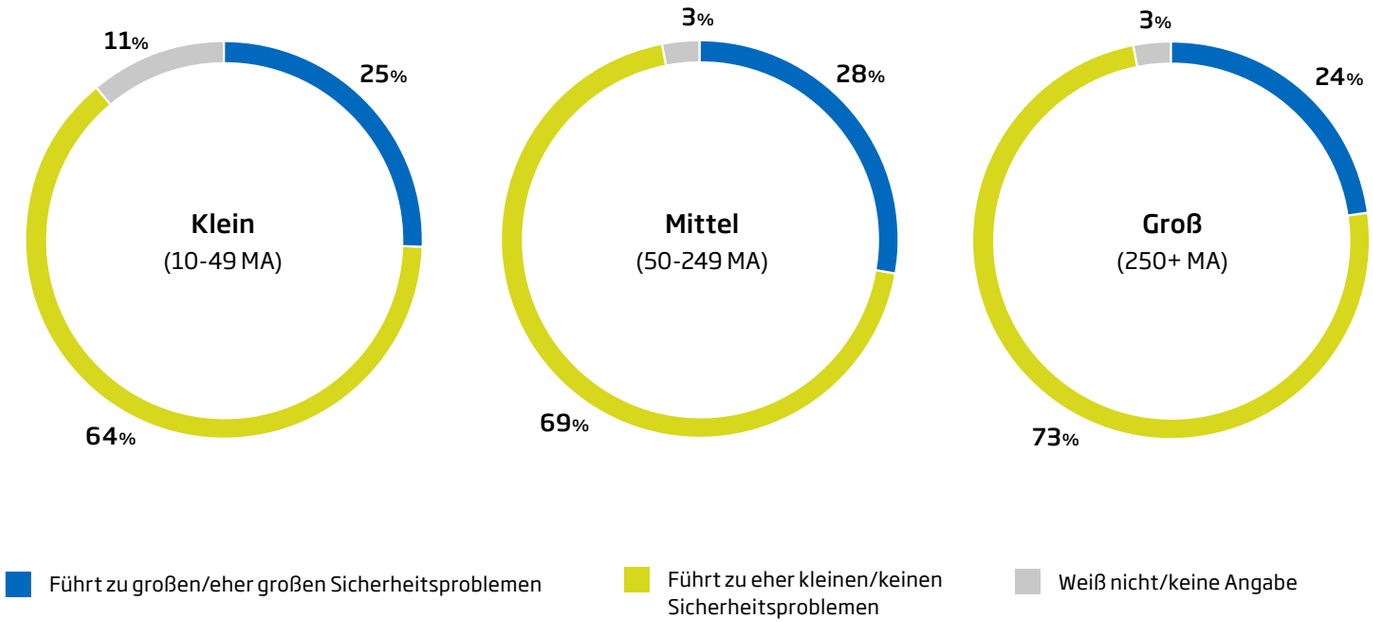

Frage: Inwiefern stimmen Sie folgenden Aussagen zu? | Basis: 501 befragte Unternehmen

### Mobiles Arbeiten schafft neue Einfallstore für Cyberkriminelle

Die Anfälligkeit für Cyberangriffe steigt, wenn Endgeräte des Arbeitgebers auch privat genutzt werden. Dieser Aussage stimmen 73 Prozent der Befragten zu. Sind die Beschäftigten mit den Geräten im heimischen WLAN oder in öffentlichen Netzwerken unterwegs, erhöht auch das die Gefahr eines Angriffs (71 Prozent). Mobiles Arbeiten führt in 44 Prozent der Unternehmen dazu, dass sich die Zahl genutzter Tools und Anwendungen vervielfacht. Fast zwei von drei Befragten geben an, dass sich folglich die Komplexität und damit das IT-Sicherheitsrisiko erhöht. Etwas weniger als die Hälfte der Unternehmen fürchtet mehr Angriffe durch Social Engineering, weil sich Mitarbeitende nicht mehr persönlich kennen.

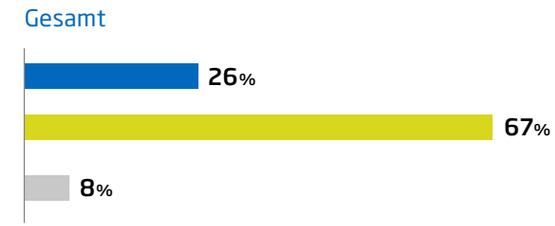
# Mehrheit hat die Sicherheitsrisiken des mobilen Arbeitens im Griff

## Sicherheitsprobleme durch mobiles Arbeiten




**Nur gut ein Viertel der Unternehmen fühlt sich durch Homeoffice beträchtlich stärker bedroht.**

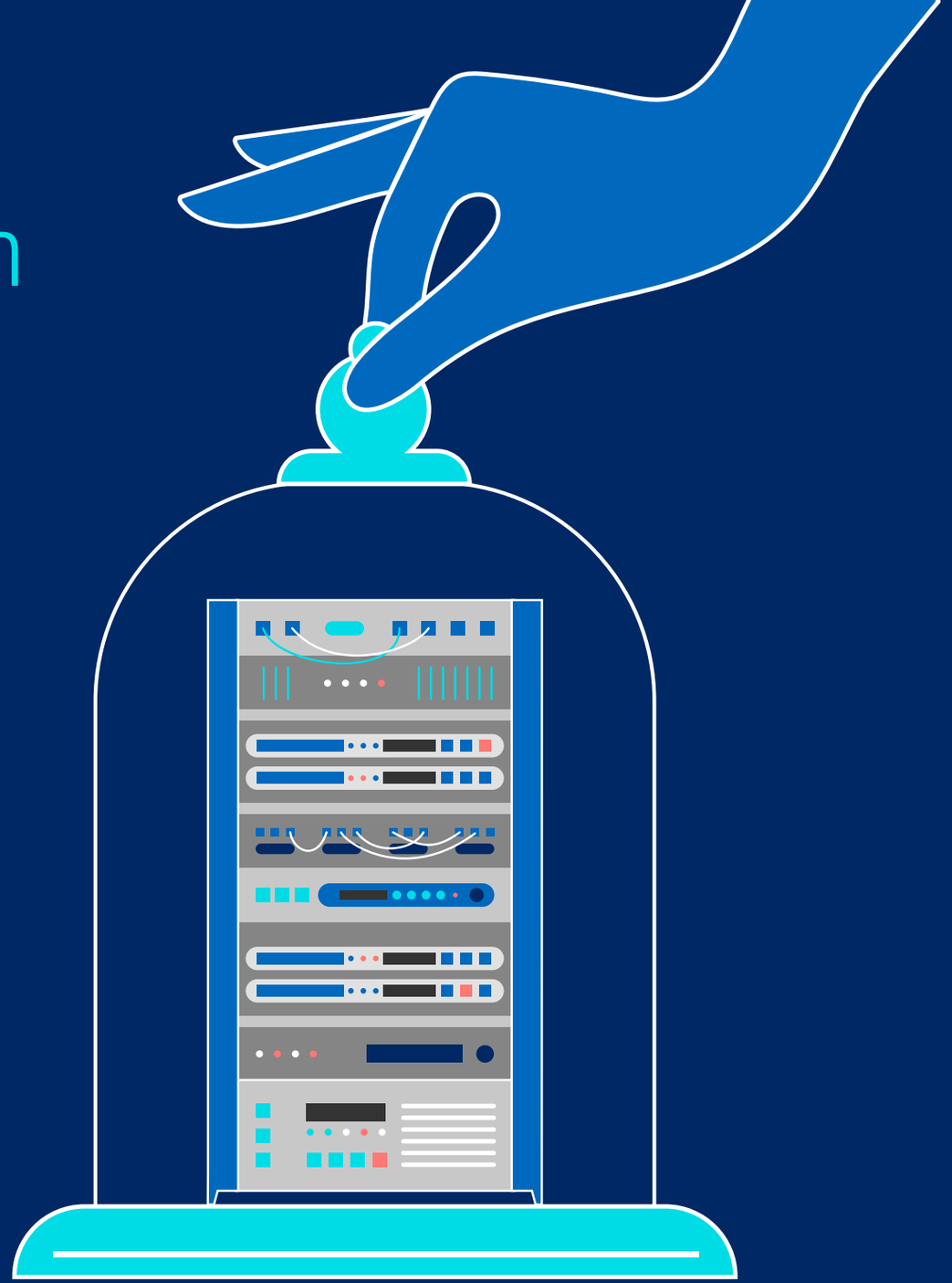
Zwar erweitert mobiles Arbeiten die Angriffsfläche für Cyberkriminelle. Aber nur gut jedes vierte Unternehmen stimmt der Aussage zu, dass Homeoffice und mobiles Arbeiten in der Praxis zu (eher) großen IT-Sicherheitsproblemen führt. Zwei Drittel sehen eher kleine oder gar keine Sicherheitsprobleme, wenn Beschäftigte im Homeoffice oder an anderen Orten abseits des Firmenstandorts tätig sind (67 Prozent). Die Einschätzungen variieren abhängig von der Größe der Unternehmen nur geringfügig.




Frage: Im Vergleich zur Arbeit im Büro bzw. in den Gebäuden des Unternehmens, führt mobiles Arbeiten Ihrer Meinung nach zu großen, eher großen IT-Sicherheitsproblemen oder eher zu kleinen, bzw. keinen Sicherheitsproblemen?
Unterteilung nach Unternehmensgröße (Mitarbeiter:innen) | Basis: 501 befragte Unternehmen

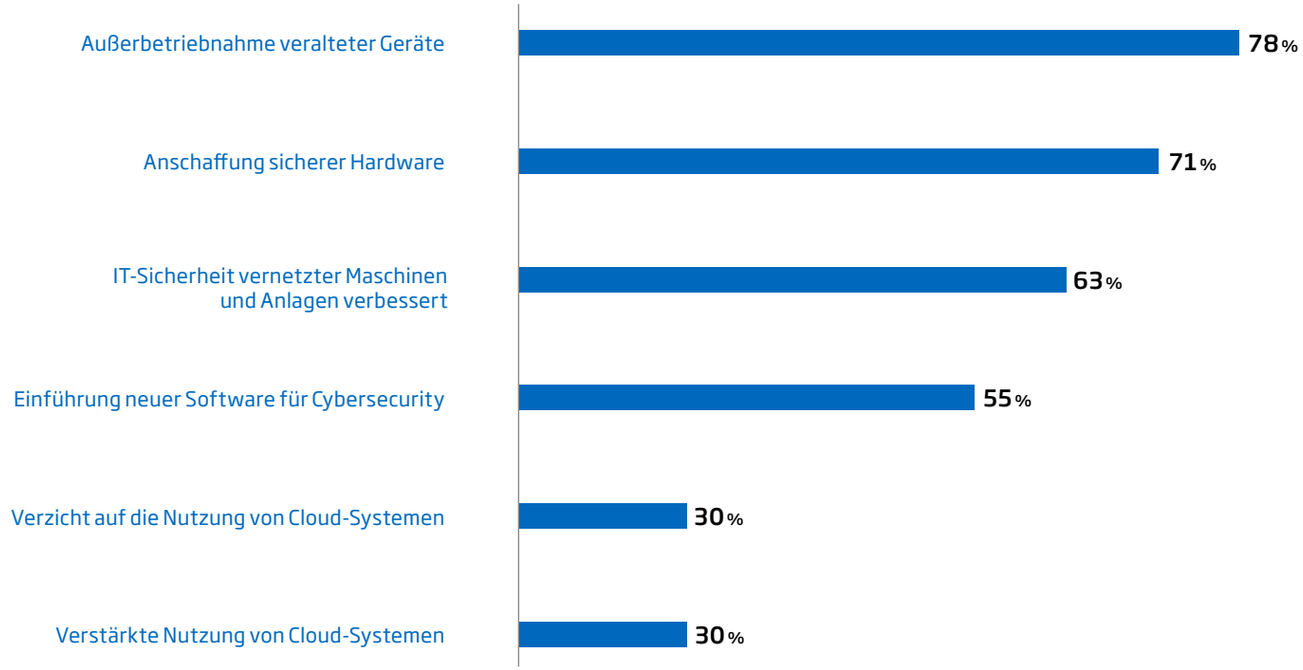
# Maßnahmen und Investitionen für einen besseren Schutz

5



# Investitionen in die Hard- und Software stehen im Mittelpunkt

## Maßnahmen bei Hard- und Software für die Verbesserung der IT-Sicherheit



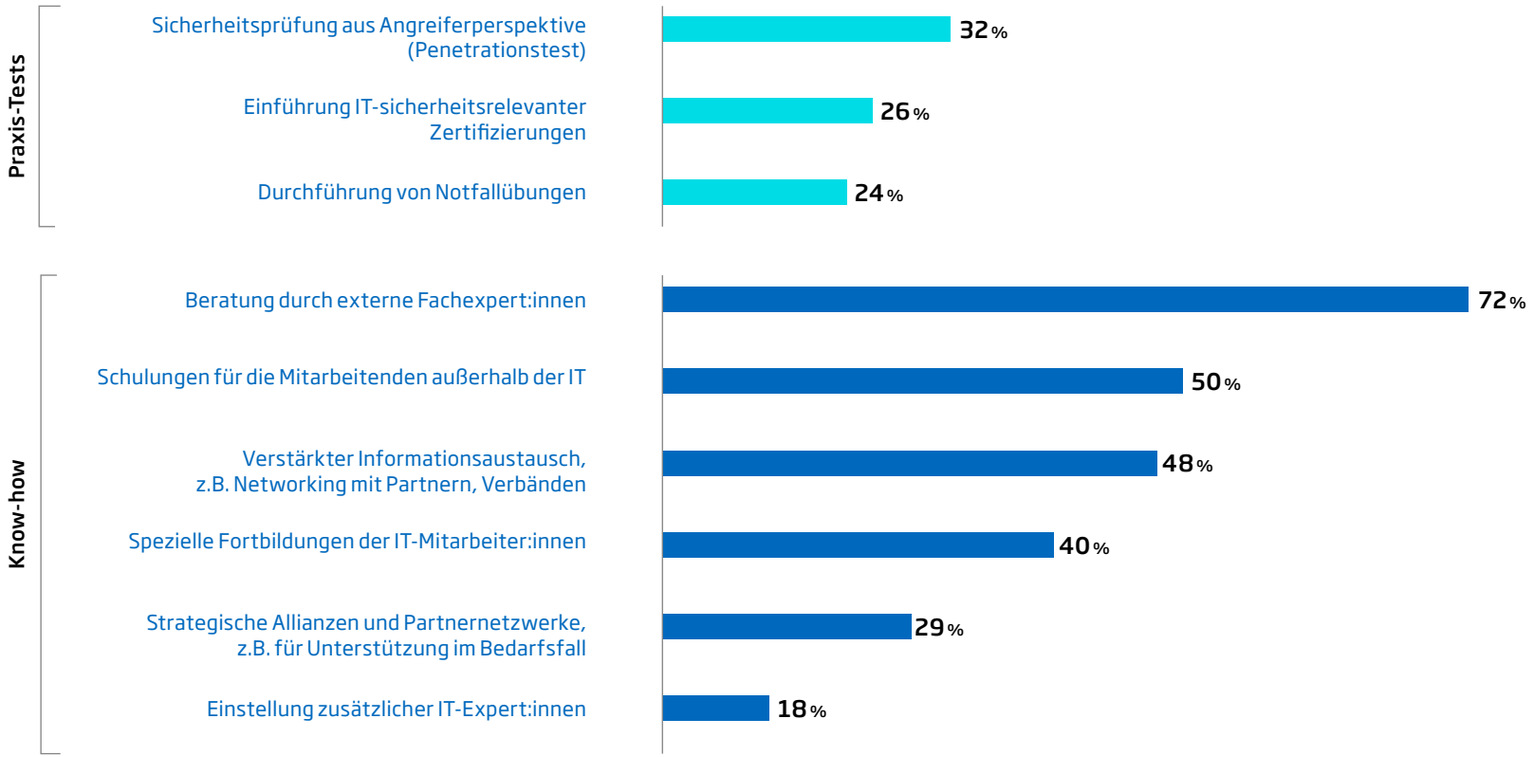

Frage: Haben Sie eine oder mehrere der folgenden Maßnahmen für die Verbesserung der IT Sicherheit ergriffen? (Mehrfachnennungen) | Basis: 501 befragte Unternehmen

**Mit der Anschaffung moderner Geräte und Anwendungen stärkt eine Mehrheit der Unternehmen die IT-Sicherheit. Uneinheitlich ist die Strategie bei Cloud-Lösungen.**

Was tun die Unternehmen konkret, um sich besser vor Cyberangriffen zu schützen? Häufig genutzte Ansatzpunkte für eine höhere IT-Sicherheit bieten eine bessere Hard- und Software. Gut drei Viertel der Unternehmen haben veraltete Geräte ausgemustert, zudem wurden häufig sichere Geräte angeschafft, vernetzte Anlagen besser geschützt und es wurde neue Cybersecurity-Software eingeführt. Uneinheitlich ist die Einschätzung von Cloud-Lösungen, wenn es um die IT-Sicherheit geht. Knapp ein Drittel verzichtet auf Cloud-Systeme, um sich besser vor Cyberattacken schützen zu können. Auf der anderen Seite setzen ebenso viele für eine erhöhte IT-Sicherheit auf die Cloud.

# Investitionen in Know-how und Praxis-Tests

## Kompetenzen für die Verbesserung der IT-Sicherheit




Frage: Haben Sie eine oder mehrere der folgenden Maßnahmen für die Verbesserung der IT Sicherheit ergriffen? (Mehrfachnennungen) | Basis: 501 befragte Unternehmen

**Vor allem die Beratung durch externe Expert:innen hat für Unternehmen eine hohe Bedeutung.**

Besonderes Augenmerk legen die Unternehmen auf Investitionen in ihr eigenes Know-how. So ließen sich knapp drei Viertel der Befragten von externen Expert:innen beraten, die Hälfte schulte Beschäftigte außerhalb der IT-Abteilung und knapp die Hälfte verstärkte den Informationsaustausch zum Beispiel mit Partnern oder Verbänden.

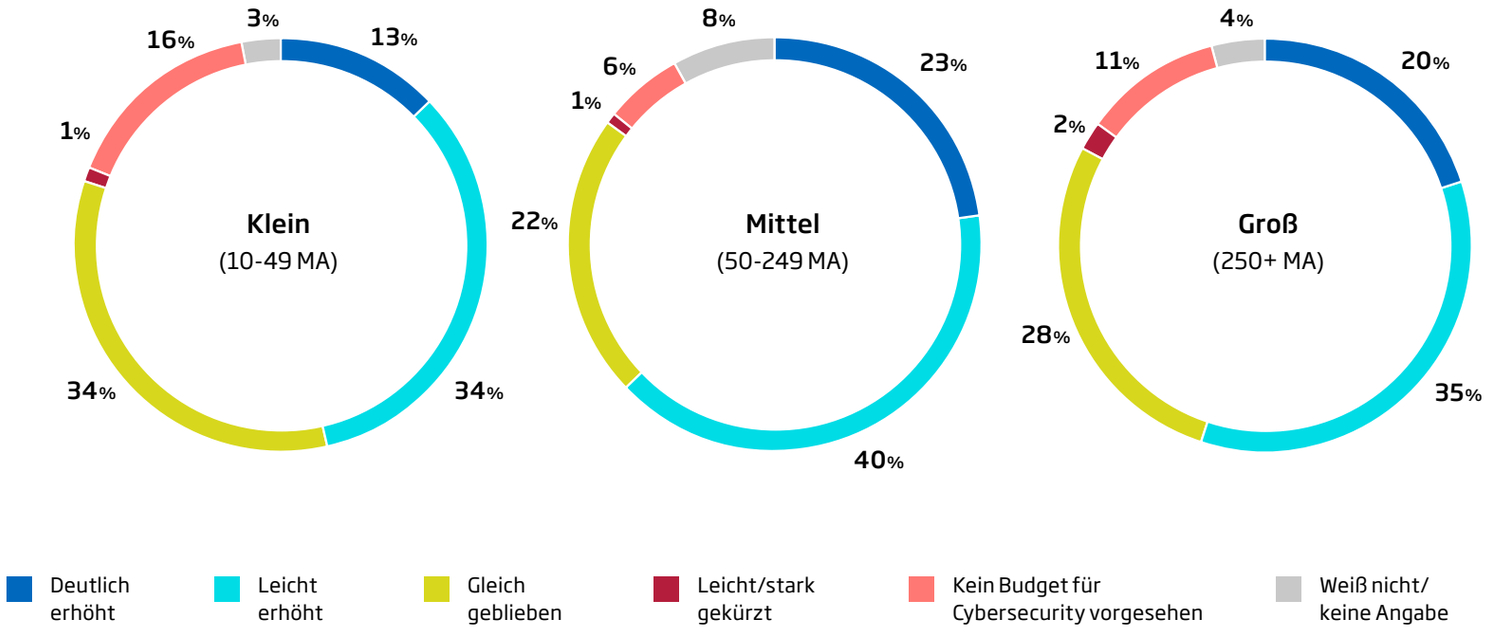
Aufwändige Praxis-Tests spielen ebenfalls eine Rolle. So setzt ein knappes Drittel auf so genannte Penetrationstests, bei denen beauftragte IT-Expert:innen auf der Suche nach potenziellen Schwachstellen die Infrastruktur der Unternehmen angreifen. Knapp jedes vierte Unternehmen führt Notfallübungen durch, bei denen die Abläufe im Fall eines IT-Angriffs durchgespielt werden. Und gut jedes vierte Unternehmen führte für die IT-Sicherheit relevante Zertifizierungen ein. Auch während einer Zertifizierung kommt es darauf an, Know-how im IT-Sicherheitsbereich aufzubauen und entsprechende Strukturen und Prozesse einzuführen oder zu verbessern.

**Was tun betroffene Unternehmen?**

Maßnahmen infolge eines Sicherheitsvorfalles »

# Eine Mehrheit investiert mehr in Cybersecurity

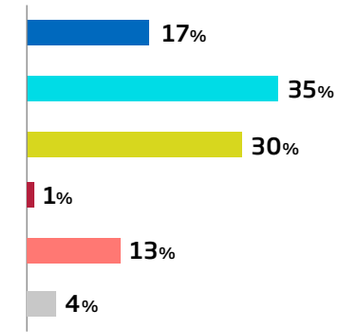
## Entwicklung der Ausgaben für Cybersecurity




**Ausgaben für IT-Sicherheit sind in den vergangenen beiden Jahren bei gut der Hälfte der Unternehmen gestiegen. 13 Prozent haben kein Budget für Cybersecurity.**

Gut jedes zweite Unternehmen hat innerhalb der vergangenen zwei Jahre das Budget für Cybersecurity erhöht. Überdurchschnittlich häufig investieren die mittelständischen Unternehmen (63 Prozent), kleinere Firmen dagegen liegen unter dem Schnitt (47 Prozent). Ein knappes Drittel hat die Ausgaben für IT-Sicherheit zuletzt nicht verändert. Bemerkenswert: Etwa jeder achte Betrieb verzichtet auf ein eigenes Budget für Cybersicherheit.

Gesamt

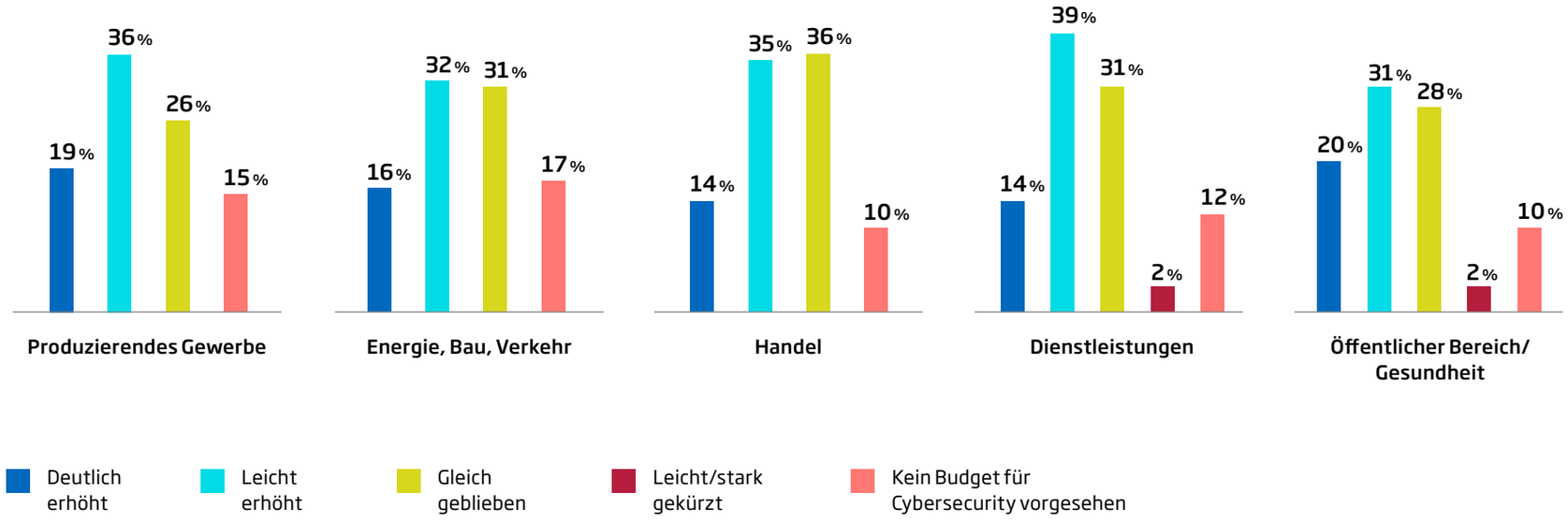



Frage: Wie hat sich das Budget Ihres Unternehmens für Ausgaben im Bereich der Cybersecurity in den vergangenen zwei Jahren entwickelt?
Unterteilung nach Unternehmensgröße (Mitarbeiter:innen) | Basis: 501 befragte Unternehmen

# Eine Mehrheit investiert mehr in Cybersecurity

## Entwicklung der Ausgaben für Cybersecurity nach Branchen

Besonders häufig haben Unternehmen des produzierenden Gewerbes in den vergangenen beiden Jahren ihre Ausgaben für IT-Sicherheit erhöht. Unterdurchschnittlich dagegen fällt die Erhöhung im Handel aus. Der höchste Anteil an Unternehmen, die auf ein eigenes Budget für Cybersecurity verzichten, findet sich im Sektor Energie, Bau, Verkehr (17 Prozent). Am seltensten geschieht dies im öffentlichen Sektor und Gesundheitswesen sowie im Handel (jeweils 10 Prozent).



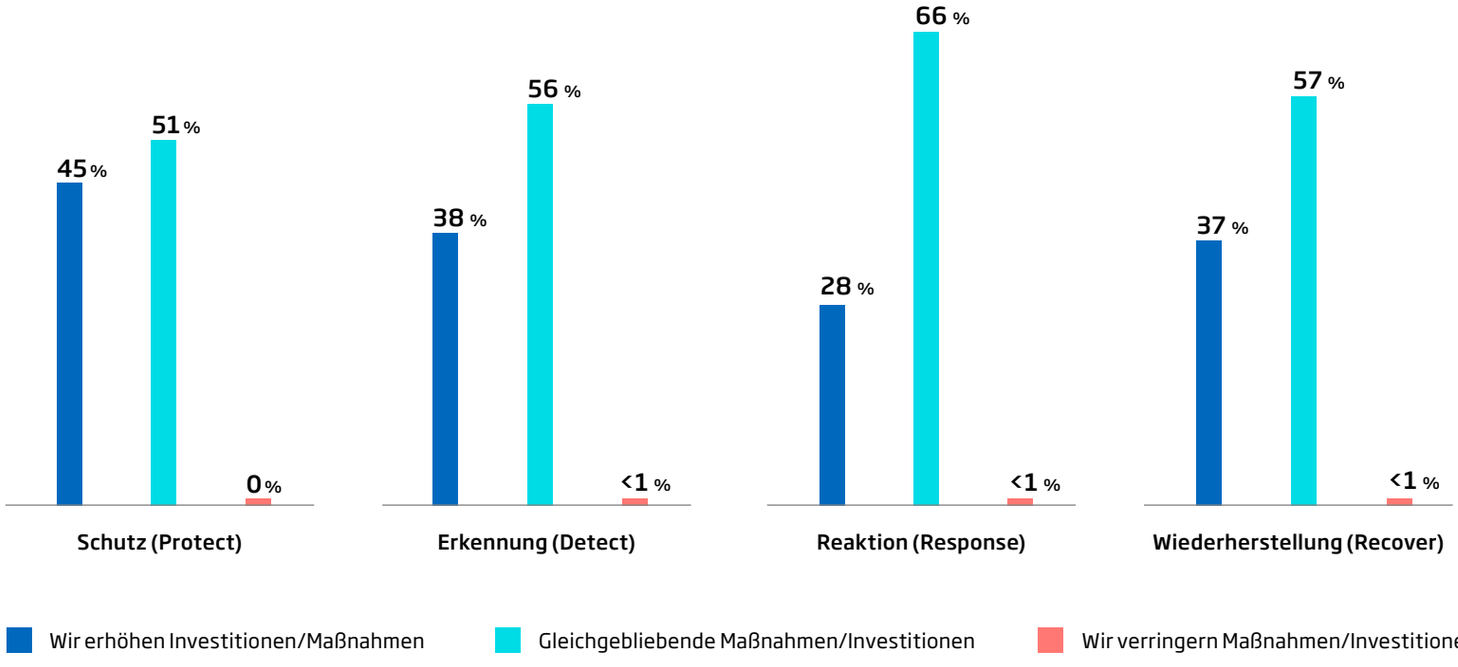

Frage: Wie hat sich das Budget Ihres Unternehmens für Ausgaben im Bereich der Cybersecurity in den vergangenen zwei Jahren entwickelt? | Fehlende Angaben zu 100% "Weiß nicht/Keine Angabe"
Unterteilung nach Unternehmensgröße (Branche) | Basis: 501 befragte Unternehmen

**Wie hoch schätzen Unternehmen das Risiko ein?**

Ein Cyberangriff für viele realistisch ››

# Abwehr von Cyberangriffen hat höchste Priorität

## Ansatzpunkte für Investitionen in Cybersicherheit




Frage: Werden die Investitionen bzw. Maßnahmen erhöht, verringert, oder bleiben sie gleich in den vier Phasen der Abwehr und im Umgang mit Cyberangriffen?
Fehlende Angaben zu 100 Prozent "Weiß nicht/Keine Angabe" | Basis: 501 befragte Unternehmen

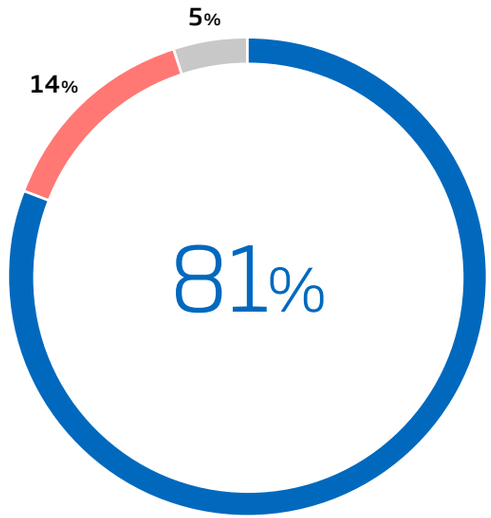
**Vor allem beim Schutz ihrer IT-Systeme planen die Unternehmen höhere Ausgaben.**

Sobald der Schutzbedarf eines Unternehmens identifiziert wurde, lässt sich der Cybersecurity als Zyklus in vier Phasen einteilen: Die präventive Abwehr von Cyberangriffen (Protect), die Erkennung von Attacken (Detect), die unmittelbare Reaktion und Abwehr des Angriffs (Response) sowie die Wiederherstellung des ursprünglichen Zustandes samt notwendiger Nachbesserungen (Recover). Den höchsten zusätzlichen Einsatz wollen die Unternehmen beim präventiven Schutz leisten, damit es erst gar nicht zu einem erfolgreichen Angriff kommt: Fast die Hälfte will hier künftig zulegen (45 Prozent). 38 Prozent wollen verstärkt in die Erkennung von Cyberattacken investieren und 28 Prozent in die Reaktionsphase. 37 Prozent planen mit höheren Investitionen im Bereich der Wiederherstellung, zum Beispiel mit Hilfe von Backup-Systemen. Einschnitte bei den Cybersecurity-Investitionen sind kaum vorgesehen.

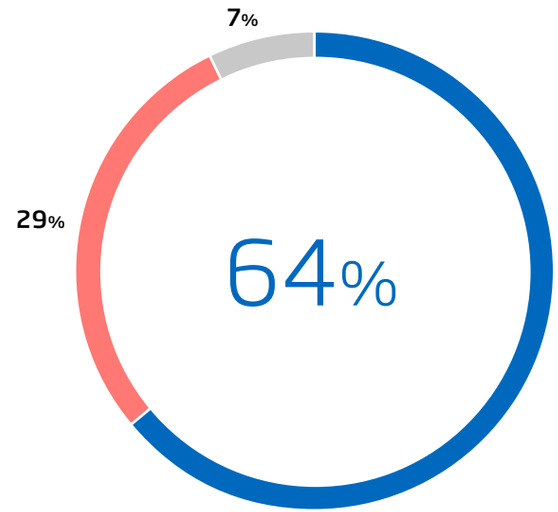
# Unternehmen speichern Daten vorwiegend innerhalb der EU

## Wo Unternehmen ihre Daten speichern

**Unsere Unternehmensdaten werden ausschließlich in Rechenzentren innerhalb der EU gespeichert und verarbeitet.**




**Es ist richtig, den Verkauf von Hard- und Software aus Ländern wie Russland oder China zu beschränken.**



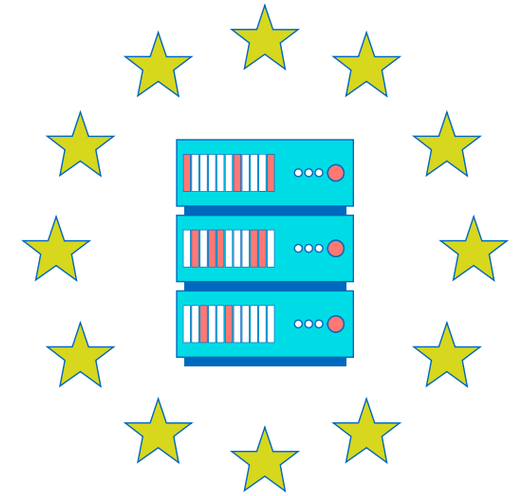

Stimme voll/eher zu | Stimme eher nicht/gar nicht zu | Weiß nicht/keine Angabe

Frage: Inwiefern stimmen Sie folgenden Aussagen zu? | Basis: 501 befragte Unternehmen

**Rechenzentren in der EU haben für eine deutliche Mehrheit der Unternehmen Priorität. Ebenfalls die Mehrzahl unterstützt Beschränkungen von Soft- und Hardware-Exporten aus China oder Russland.**

Gut vier von fünf Unternehmen speichern und verarbeiten ihre Daten ausschließlich in Rechenzentren in der Europäischen Union, in der strenge Gesetzesvorgaben für den Datenschutz und die Informationssicherheit gelten.

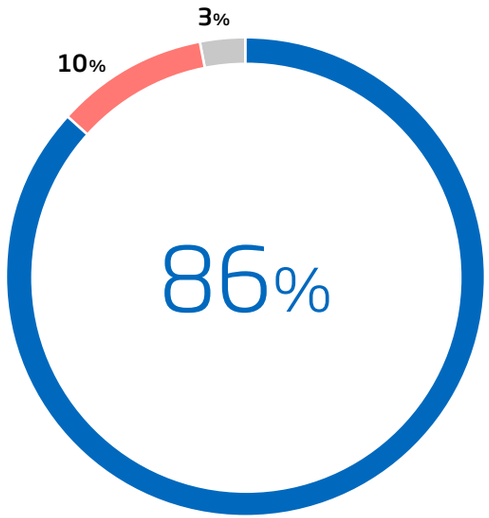
Fast zwei Drittel der befragten Unternehmen stimmen der Aussage zu, dass es richtig ist, den Verkauf von Hard- und Software aus Ländern wie Russland oder China zu beschränken. 29 Prozent sind gegenteiliger Meinung.



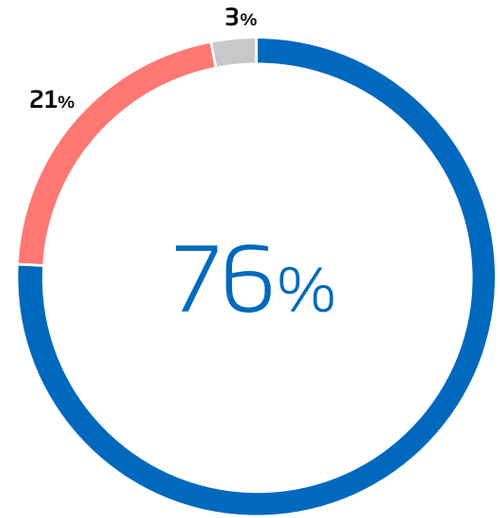
# Bei der Auswahl von IT-Anbietern entscheidet auch die Herkunft

## Bedeutung der Herkunft bei der Auswahl von IT-Anbietern

**Wir achten bei der Auswahl unserer IT-Dienstleister auf die Herkunft des Anbieters.**




**Wir achten bei der Auswahl von Hard- und Software auf die Herkunft des Anbieters.**




Stimme voll/eher zu | Stimme eher nicht/gar nicht zu | Weiß nicht/keine Angabe

Frage: Inwiefern stimmen Sie folgenden Aussagen zu? | Abweichungen zu 100 Prozent sind rundungsbedingt | Basis: 501 befragte Unternehmen

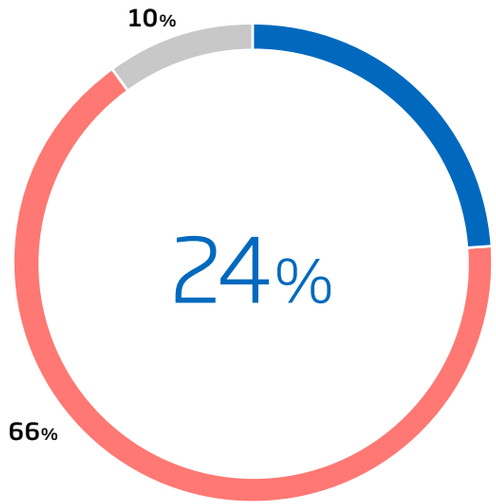
**Besonders große Unternehmen achten bei IT-Diensten sowie Hard- und Software auf das Herkunftsland.**

Die deutliche Mehrheit der Unternehmen legt bei der Auswahl ihrer IT-Dienstleister Wert auf die Herkunft (86 Prozent). Etwas niedriger liegt der Wert bei der Auswahl von Hard- und Software-Herstellern (76 Prozent). Große Unternehmen nehmen in beiden Kategorien den Spitzenrang ein – 92 Prozent von ihnen ist bei IT-Dienstleistern die Herkunft wichtig und 85 Prozent bei Hard- und Software-Herstellern.

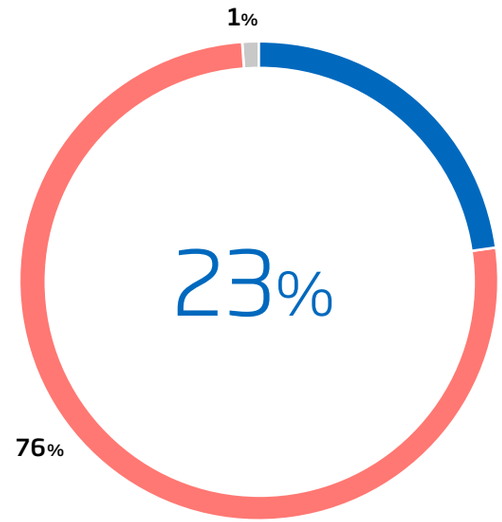
# Nicht immer stehen Kosten und Nutzen im Verhältnis

## Wie Unternehmen den Ressourceneinsatz für Cybersicherheit bewerten

**Die für Cybersecurity eingesetzten Ressourcen stehen bei uns in keinem Verhältnis zum Sicherheitsgewinn.**




**Unser Unternehmen nimmt bestimmte Risiken bei der Cybersecurity bewusst in Kauf.**




Stimme voll/eher zu | Stimme eher nicht/gar nicht zu | Weiß nicht/keine Angabe

Frage: Inwiefern stimmen Sie folgenden Aussagen zu? | Basis: 501 befragte Unternehmen

**Eingesetzte Ressourcen stehen für einige Unternehmen nicht im Verhältnis zum Sicherheitsgewinn. Risiken werden in Kauf genommen.**

Auch beim Thema Cybersecurity findet in den Unternehmen eine Abwägung von Kosten und Nutzen statt. Knapp ein Viertel der Befragten ist der Ansicht, dass die für Cybersecurity eingesetzten Ressourcen nicht im Verhältnis zum Sicherheitsgewinn stehen (24 Prozent). Besonders kritisch sieht dies die Handelsbranche (30 Prozent). Diese Einschätzung spiegelt wider, dass der konkrete Nutzen von Präventionsmaßnahmen nicht immer ersichtlich ist. Kommt es aufgrund besonders hoher IT-Sicherheitsstandards zu keinerlei Vorfällen, werden die dafür eingesetzten Ressourcen verstärkt in Frage gestellt.

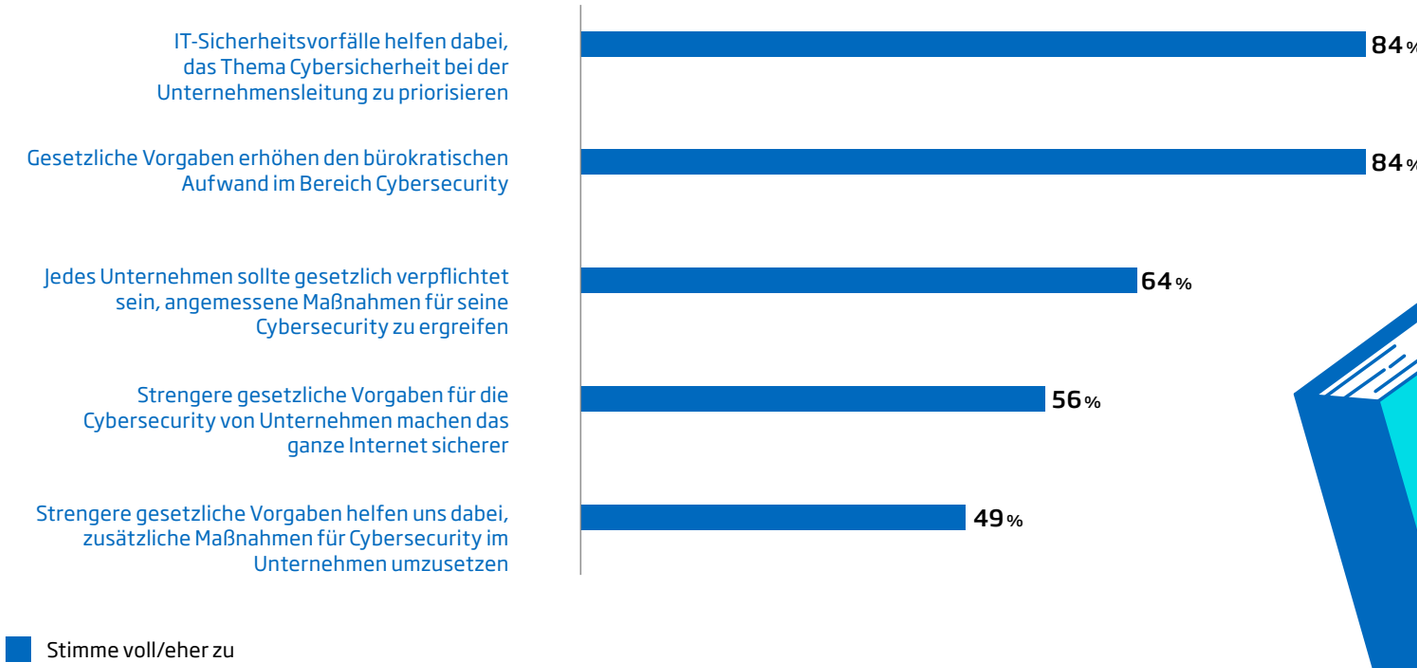
Ebenfalls ein knappes Viertel gibt an, bestimmte Cybersecurity-Gefahren bewusst in Kauf zu nehmen (23 Prozent). Große Unternehmen zeigen sich hier vorsichtiger (19 Prozent). Überdurchschnittlich hoch ist die Bereitschaft zum Risiko im öffentlichen Sektor und Gesundheitswesen (29 Prozent), am geringsten im Bereich Energie, Bau, Verkehr (15 Prozent). Die Inkaufnahme bestimmter Gefahren kann als Ausdruck von Leichtsinn verstanden werden, ist aber in der Regel Teil des Risikomanagements. Die Unternehmen müssen dabei immer wieder zwischen möglichen Gefahren und der Einführung zusätzlicher IT-Sicherheitsmaßnahmen abwägen.

# Gesetze, Normen und Standards als Sicherheitsfaktoren

6

# Unternehmen fordern strengere gesetzliche Cybersecurity-Vorgaben

## Einstellung zu gesetzlichen Maßnahmen für IT-Sicherheit



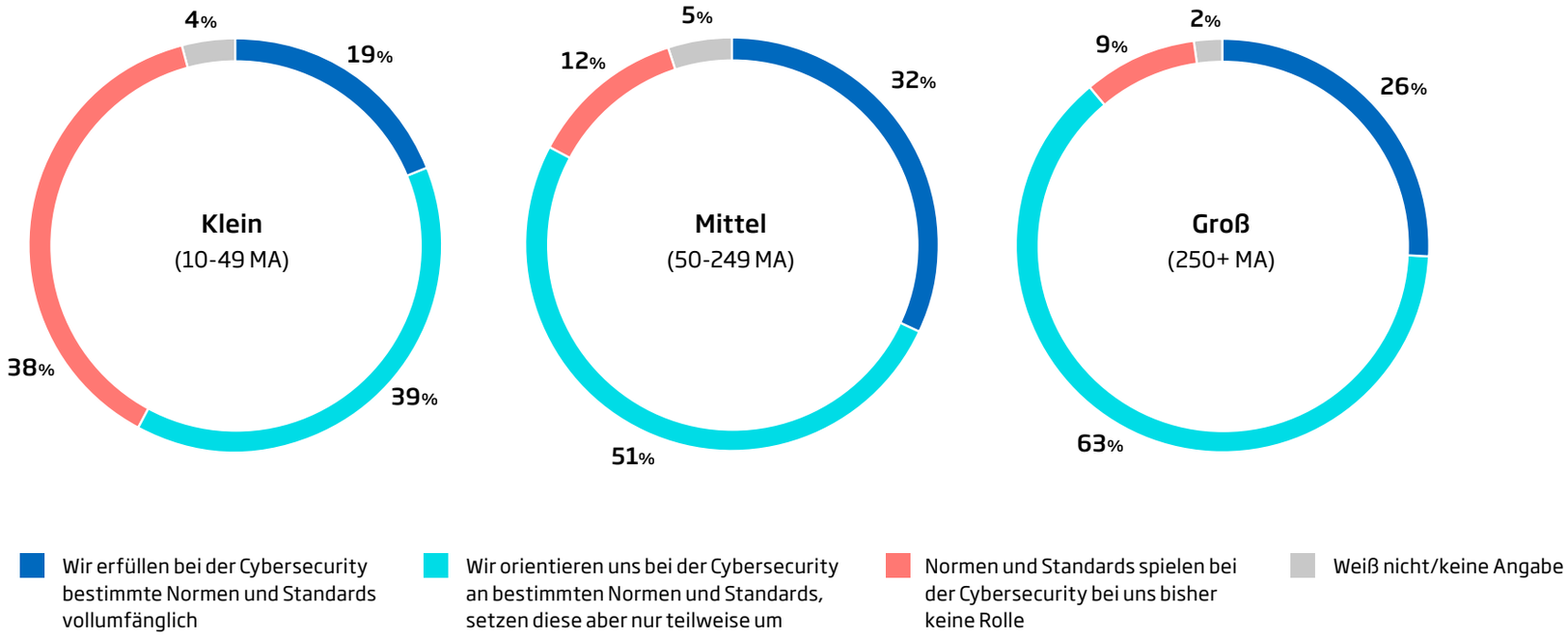

Frage: Inwiefern stimmen Sie folgenden Aussagen zu? | Basis: 501 befragte Unternehmen

**Knapp jedes zweite Unternehmen würde im Fall von strengeren Vorgaben stärker in die IT-Sicherheit investieren.**

Fast zwei Drittel der Unternehmen sehen bei der IT-Sicherheit den Gesetzgeber in der Pflicht und fordern Regelungen, die angemessene Maßnahmen für Cybersecurity in der Wirtschaft vorschreiben. Diese würden in knapp jedem zweiten Unternehmen dabei helfen, zusätzliche Maßnahmen für IT-Sicherheit umzusetzen und das Thema in der Firmenleitung zu priorisieren. Darüber hinaus ist eine Mehrheit der Meinung, dass strengere gesetzliche Vorgaben das Internet insgesamt sicherer machen. Allerdings sind sich nahezu alle Befragten darin einig, dass gesetzliche Regelungen den bürokratischen Aufwand im Bereich Cybersecurity erhöhen.

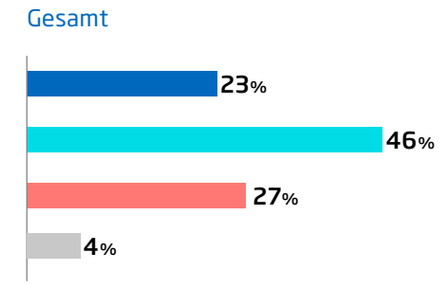
# Zentrale Rolle von Normen und Standards für die IT-Sicherheit

## Rolle von Normen und Standards für Cybersicherheit




**Besonders große und mittelgroße Unternehmen nutzen Normen und Standards für Cybersecurity-Maßnahmen.**

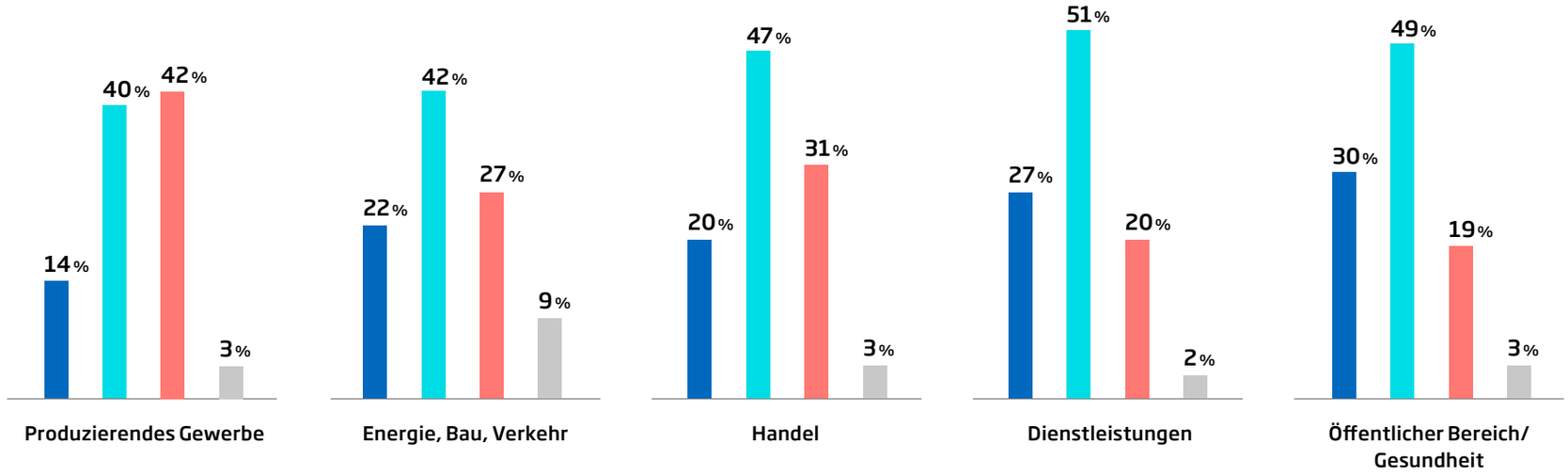
Fast jedes vierte Unternehmen erfüllt Normen und Standards der Cybersecurity in vollem Umfang – besonders aktiv sind hier mittelgroße Unternehmen, noch vor den Großunternehmen. Kleinere Unternehmen liegen unter dem Durchschnitt. Eine relative Mehrheit der Befragten orientiert sich an Normen und Standards, setzt diese jedoch nur teilweise um. Bei gut einem Viertel spielen Normen oder Standards bisher gar keine Rolle – besonders häufig ist dies bei kleinen Unternehmen der Fall.




Frage: Inwiefern stimmen Sie folgenden Aussagen zu? Unterteilung nach Unternehmensgröße (Mitarbeiter:innen) | Basis: 501 befragte Unternehmen

# Öffentlicher Sektor erfüllt Normen und Standards am häufigsten

## Rolle von Normen und Standards im Branchenvergleich




Frage: Inwiefern stimmen Sie folgenden Aussagen zu? | Unterteilung nach Branchen | Basis: 501 befragte Unternehmen

Zwischen den einzelnen Branchen zeigen sich teils deutliche Unterschiede im Umgang mit Normen und Standards. Diese werden im öffentlichen Sektor und Gesundheitswesen von fast einem Drittel der Unternehmen vollumfänglich erfüllt – im produzierenden Gewerbe sind es nicht einmal halb so viele. In der Industrie spielen Standards und Normen auch am häufigsten gar keine Rolle.

Das mag mit gesetzlichen Anforderungen in Verbindung stehen, die eine entsprechende Zertifizierung vorsehen.

# Zuspruch für externe Prüfung von IT-Sicherheitsstandards

## Prüfung und Zertifizierung von Normen und Standards für Cybersicherheit

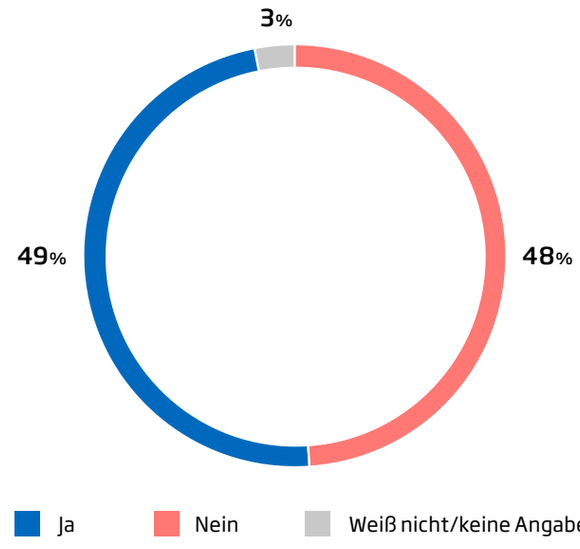
**Zertifizierungen unabhängiger, externer Prüfstellen sind besonders im Sektor Energie, Bau, Verkehr sowie dem öffentlichen Sektor und Gesundheitswesen gefragt.**

Mit dem Siegel einer unabhängigen Prüfstelle die eigenen Maßnahmen für Cybersicherheit auch nach außen dokumentieren - darauf setzt nahezu jedes zweite Unternehmen, das Normen und Standards einhält oder sich an diesen orientiert. Den stärksten Zuspruch erhält eine solche externe Zertifizierung im Sektor Energie, Bau, Verkehr (56 Prozent) und im öffentlichen Bereich und Gesundheitssektor (54 Prozent).

70%

**... der befragten Unternehmen erfüllen bei der Cybersecurity bestimmte Normen und Standards vollumfänglich, bzw. orientieren sich an bestimmten Normen und Standards.**

**Lassen Sie die Einhaltung von Normen und Standards für Cybersecurity von unabhängigen, externen Stellen überprüfen bzw. zertifizieren?**

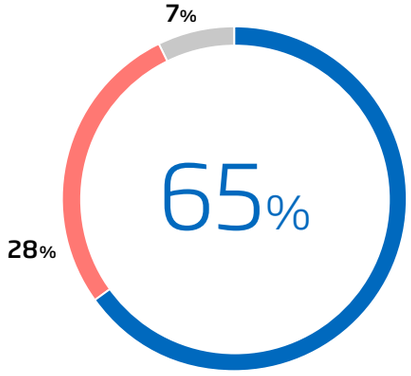



Frage: Lassen Sie die Einhaltung von Normen und Standards für Cybersecurity von unabhängigen, externen Stellen überprüfen bzw. zertifizieren?
Basis: 348 Befragte, deren Unternehmen sich an Normen und Standards bei der Cybersecurity orientieren und mindestens teilweise einhalten

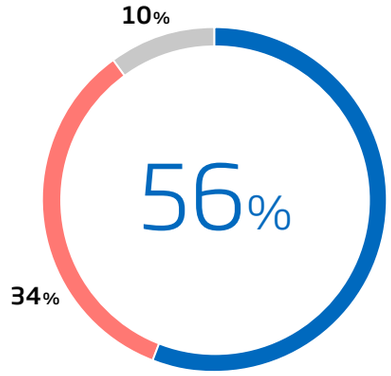
# Normen und Standards verursachen Aufwand

## Vor- und Nachteile von Normen und Standards für die Cybersicherheit

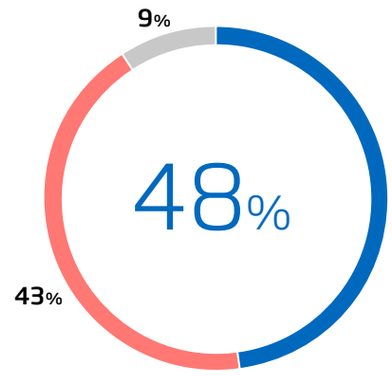
**Normen und Standards für die Cybersecurity sind für uns wichtig, um den Schutz vor Cyberangriffen stetig zu verbessern.**



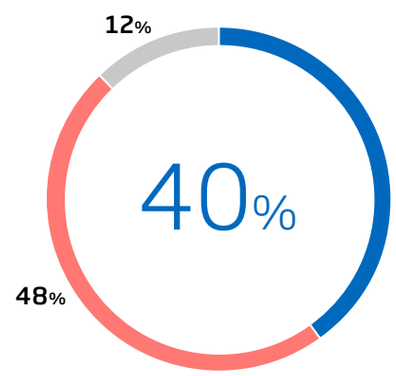

**Die Einhaltung der Normen und Standards ist mit zu viel Aufwand verbunden.**




**Es fällt schwer, zu entscheiden, welche Normen und Standards für unser Unternehmen relevant sind.**




**Die vorhandenen Normen und Standards für Cybersecurity sind zu technisch und schwer zu verstehen.**




Stimme voll/eher zu | Stimme eher nicht/gar nicht zu | Weiß nicht/keine Angabe

Frage: Inwiefern stimmen Sie folgenden Aussagen zu? | Basis: 501 befragte Unternehmen

**Der Zuspruch der Unternehmen für Normen und Standards ist hoch. Dabei entsteht häufig jedoch ein hoher Aufwand, zudem bereitet mangelnde Verständlichkeit Probleme.**

Die Bedeutung von Normen und Standards in der Praxis ist hoch. Knapp zwei Drittel der Unternehmen erachten sie als wichtig, um den Schutz vor Cyberangriffen stetig zu verbessern. Allerdings sehen die Befragten auch Nachteile. Etwas mehr als die Hälfte der Befragten stimmt der Aussagen zu, dass die Einhaltung von Normen mit zu viel Aufwand verbunden ist. Knapp der Hälfte der Unternehmen fällt es schwer zu entscheiden, welche Normen und Standards für sie relevant sind – dies gilt besonders für kleine und mittelgroße Unternehmen. Große Unternehmen tun sich hier leichter. Immerhin 40 Prozent der Befragten halten die vorhandenen Vorgaben für schwer verständlich.

# Fazit und politische Empfehlungen

7

# Fazit

Unternehmen in Deutschland zeigen ein hohes Bewusstsein für Cyberrisiken – sie werden fast ausnahmslos als ernste Gefahr für die Wirtschaft und Gesellschaft betrachtet. Und diese Gefahren sind real. Gut jedes zehnte Unternehmen, das im Rahmen dieser Studie befragt wurde, verzeichnete in den zwölf Monaten vor der Erhebung einen IT-Sicherheitsvorfall. Phishing-Attacken, Erpressung nach Ransomware-Angriffen, Aushebelung des Passwortschutzes, Social Engineering – die betroffenen Unternehmen sind mit allen möglichen Angriffsmethoden konfrontiert. Die Folgen der Vorfälle sind mitunter gravierend – finanziell und auch für die Reputation der Unternehmen. Zwar werden erfolgreiche Angriffe in der Regel rasch erkannt und innerhalb weniger Tage behoben. In vielen Fällen sind die Unternehmen jedoch deutlich länger mit den Folgen des Angriffs beschäftigt. Expert:innen gehen davon aus, dass viele erfolgreiche Cyberangriffe erst sehr spät oder gar nicht erkannt werden.

Drei von zehn Unternehmen erwarten, in den kommenden zwölf Monaten ins Visier von Cyberkriminellen zu geraten – besonders gefürchtet sind organisierte Banden. Der Ukrainekrieg schürt dabei die Angst vor mehr Cyberangriffen. Entsprechend steigt der Einsatz für die Absicherung der eigenen IT-Systeme – die Unternehmen investieren in moderne Hard- und Software und in ihr eigenes Know-how. Cloud-Dienstleistungen sehen ein Drittel als Chance für mehr IT-Sicherheit – dieselbe Anzahl der Befragten will allerdings lieber darauf verzichten, um den eigenen Schutz zu stärken. Die Unternehmen wägen hier ab, ob sie die Kontrolle für die eigene IT-Sicherheit selbst übernehmen oder in die Hände eines Cloud-Providers legen – beides kann je nach Ausgangslage Sinn ergeben.

**Bedeutung der IT-Sicherheit erkannt**

Eine große Rolle spielt Cybersecurity besonders für große und mittlere Unternehmen – in kleineren Firmen ist die Bedeutung geringer. Auch bei einzelnen Branchen sind teils deutliche Unterschiede zu erkennen – so ist die Rolle der IT-Sicherheit im Dienstleistungssektor besonders hoch, im Handel dagegen unterdurchschnittlich. Cybersecurity kann sogar das Wachstum befördern – drei Viertel der Unternehmen sehen sie als Wettbewerbsvorteil an.

Eine breite Mehrheit wünscht sich, dass Opfer von Cyberangriffen diese publik machen, um das Bewusstsein für Risiken zu stärken. Tatsächlich aber geschieht dies in der Praxis nur in Ausnahmefällen – offenbar ist die Sorge vor einem Reputationsverlust zu groß.

Nicht zuletzt haben die Unternehmen hohe Erwartungen an den Gesetzgeber – eine deutliche Mehrheit wünscht sich strengere Vorgaben für Cybersecurity in der Wirtschaft. Sie helfen den befragten Sicherheitsverantwortlichen, das Bewusstsein für das Thema in der Geschäftsleitung zu schärfen und höhere Sicherheitsstandards in ihren Unternehmen umzusetzen. Eine hohe Bedeutung wird Normen und Standards für die Cybersecurity zugeschrieben. Ein hoher Anteil der Unternehmen hält diese ein oder orientiert sich an ihnen. Zertifizierungen durch externe, unabhängige Prüforganisationen erhalten ebenfalls einen hohen Zuspruch.

# Politische Empfehlungen

Die Sicherheitslage im Cyberraum verschärft sich seit Jahren. Die Politik reagiert auf europäischer Ebene mit Gesetzesinitiativen wie dem Cybersecurity Act (CSA), dem Cyber Resilience Act (CRA) oder der NIS 2-Richtlinie. Nationale Regelungen wie das IT-Sicherheitsgesetz setzen die EU-Vorgaben um und ergänzen diese. Jetzt kommt es darauf an, diese Initiativen sinnvoll miteinander zu verzahnen und effektiv umzusetzen. Dabei wird es in Zukunft verstärkt darauf ankommen, agil auf aktuelle Trends im Cyberraum reagieren zu können. Innovative digitale Technologien wie künstliche Intelligenz (KI) und Quantencomputing stehen auch Cyberkriminellen zur Verfügung. Das führt im Bereich der Cybersicherheit zu neuen Herausforderungen.

**Für den TÜV-Verband ergeben sich daraus folgende Kernforderungen**

## ›› Cyber Resilience Act: IT-Sicherheitsvorgaben zügig beschließen und umsetzen

Bislang ist der europäische Rechtsrahmen für Cybersicherheit sehr lückenhaft, da die meisten sektoralen Rechtsvorschriften keine entsprechenden Cybersicherheitsanforderungen enthalten. Es ist daher richtig, dass der CRA hier Abhilfe schaffen will. Der darin vorgesehene risikobasierte Ansatz, der bereits heute ein Eckpfeiler der europäischen Produktregulierung ist, gewährleistet ein angemessen hohes Cybersicherheitsniveau: Je höher das Risikopotenzial des digitalen Produkts, desto höher die anzuwendenden Überprüfungsmechanismen. Bei kritischen und hochriskanten Produkten sollte eine unabhängige Drittstelle verpflichtend mit eingebunden werden. Ebenfalls ist zu beachten, die Kohärenz mit relevanten bestehenden sowie geplanten Rechtsvorschriften wie dem AI Act zu gewährleisten. Nun gilt es, den Gesetzgebungsprozess zügig abzuschließen und möglichst kurze Übergangsfristen bis zu ihrer verpflichtenden Anwendung festzulegen.

## ›› AI Act: Sicherheit von KI-Anwendungen mit hohem Risiko unabhängig prüfen

Seit der Einführung von generativen KI-Systemen wie ChatGPT werden neben dem Nutzen auch die möglichen Gefahren von künstlicher Intelligenz sehr deutlich. Der europäische AI Act soll Vertrauen und Sicherheit für KI-basierte Produkte und Anwendungen schaffen. Verbindliche Sicherheitsanforderungen werden im AI Act risikobasiert festgelegt, also entsprechend dem Gefährdungspotenzial des jeweiligen KI-Systems. Aus Sicht des TÜV-Verbands sollten alle KI-Systeme mit hohem Risiko vor ihrer Markteinführung von unabhängigen Stellen überprüft werden. Nur so kann sichergestellt werden, dass die Anwendungen nachweislich den Sicherheitsanforderungen entsprechen.

KI-Systeme müssen auch im Hinblick auf Cybersicherheit geprüft werden, da kritische Anwendungen Risiken für Leib und Leben haben können. Ein hohes Maß an Cybersicherheit ist entscheidend, um zu verhindern, dass die von KI-Systemen getroffenen Entscheidungen manipuliert werden. KI-Anwendungen müssen daher entsprechend ihrem Risikopotenzial geschützt werden und cybersicher sein.

# Politische Empfehlungen

## » Lieferketten absichern - Bewusstsein für Cybersicherheit bei KMUs fördern

Die Bedeutung eines hohen Cybersicherheitsniveaus bei kleinen und mittleren Unternehmen wird häufig unterschätzt. Die deutsche Wirtschaft ist stark mittelständisch geprägt. Diese Unternehmen sind häufig hoch spezialisiert und verfügen über einzigartiges Know-how. Cybersicherheit ist hier nicht nur unter dem Aspekt des Wirtschaftsschutzes von Bedeutung: Sie sind häufig auch als Zulieferer oder Subunternehmer für große Unternehmen tätig. Cybersicherheit entlang der Lieferkette ist hier ein zentrales Thema, das auch große Unternehmen und Betreiber kritischer Infrastrukturen betrifft. Die Allianz für Cybersicherheit, die der TÜV-Verband als Multiplikator unterstützt, bietet hier niedrigschwellige Angebote, die genutzt werden können, um Cybersicherheit in das Bewusstsein der Mitarbeiter:innen von KMU zu bringen und in der Unternehmenskultur zu verankern.

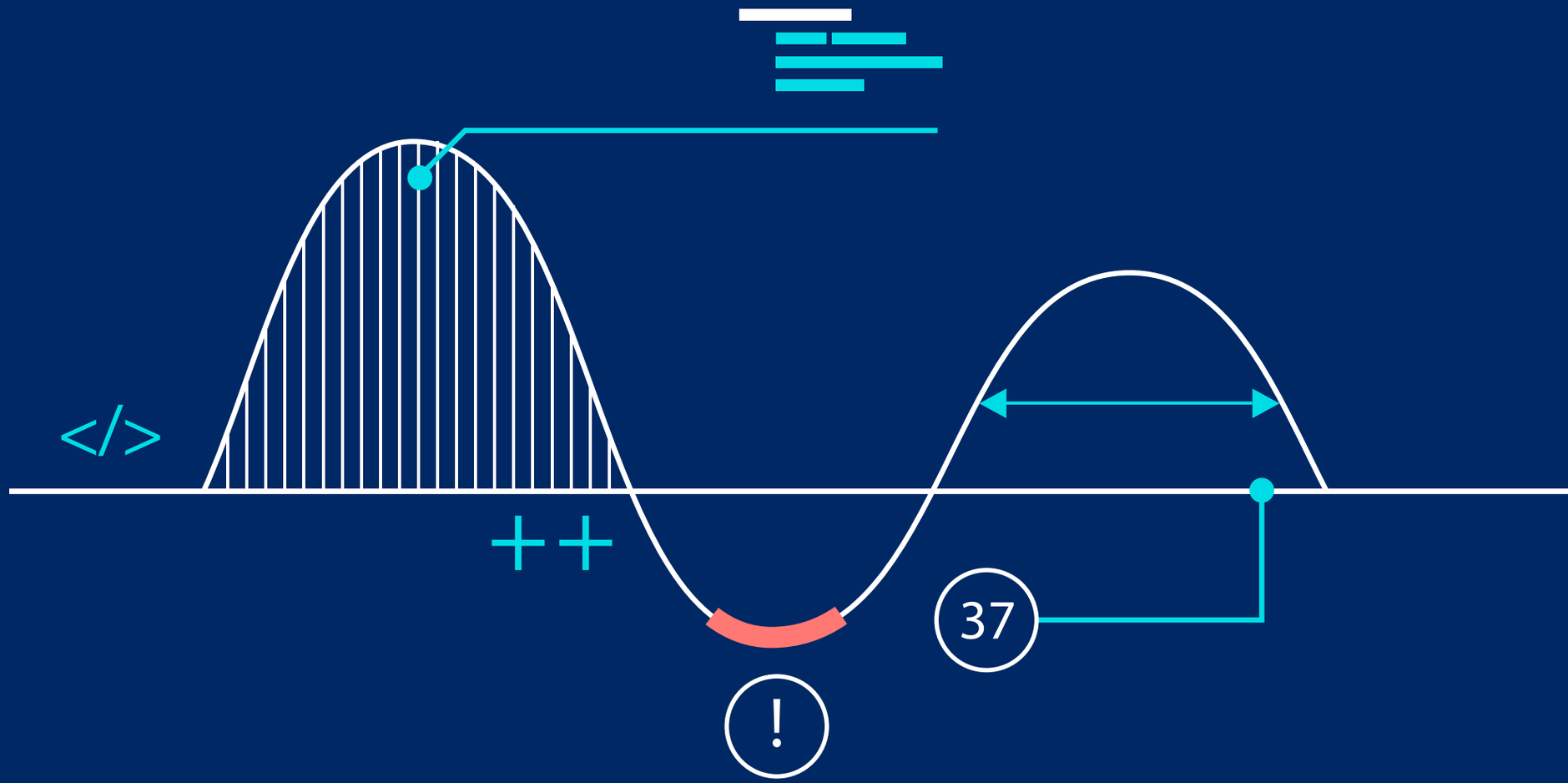
## » Kompetenzen für Cybersicherheit aufbauen - Fachkräftemangel entgegenwirken

Die internationale Cybersicherheitsorganisation ISC² schätzt, dass weltweit rund 3,4 Millionen Fachkräfte im Bereich Cybersicherheit fehlen. Die EU-Kommission hat den Mangel erkannt und versucht mit verschiedenen Maßnahmen gegenzusteuern. Auch auf nationaler Ebene ist eine schnelle und entschlossene Qualifizierungsoffensive notwendig, denn nur mit ausreichend hochqualifizierten Expert:innen für Cybersicherheit können digitale Infrastrukturen, die das Rückgrat unserer Gesellschaft bilden, sicher und zuverlässig betrieben werden. Die TÜV-Akademien stellen ihre Erfahrung und Expertise zur Verfügung, um digitale Kompetenzen und notwendige Qualifikationen zu vermitteln und so zu einer nachhaltigen digitalen Transformation beizutragen.

## » Vertrauen schaffen - Cybersicherheitszertifizierungen fördern

Vertrauen in digitale Technologien ist eine wichtige Voraussetzung für deren gesellschaftliche Akzeptanz und Nutzung. Nur wenn der sichere Betrieb digitaler Produkte, Dienste und Infrastrukturen gewährleistet ist, können die möglichen Potenziale auch genutzt werden. In diesem Sinne ist Cybersicherheit Notwendigkeit und Enabler zugleich. Cybersicherheitszertifizierungen durch unabhängige Konformitätsbewertungsstellen sind dabei ein wichtiges Mittel, um dieses Vertrauen bei Verbraucher:innen und Unternehmen zu schaffen und zu transportieren. Der TÜV-Verband hat mit „Cybersecurity Certified" (CSC) eine Zertifizierung für Geräte im Internet of Things (IoT) entwickelt. Mit vielfältigen Dienstleistungen im Bereich der Cybersecurity tragen die TÜV-Organisationen aktiv dazu bei, die Cybersicherheit von Staat, Wirtschaft, Wissenschaft und Verbraucher:innen zu erhöhen.

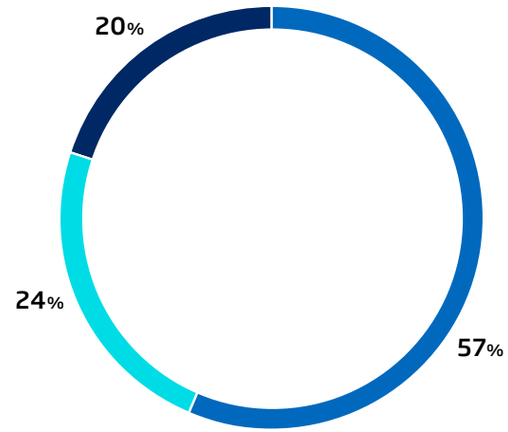
# Methodik



# Methodik

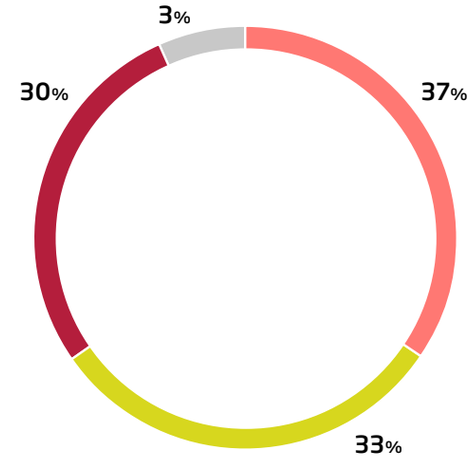
Die repräsentative Umfrage wurde von der Ipsos GmbH im Auftrag des TÜV-Verbands durchgeführt. Die Interviews erfolgten mit einer telefonischen CATI-Befragung vom 31.1. bis 3.3.2023. Basis: 501 befragte Unternehmen

**Anzahl Mitarbeitende**



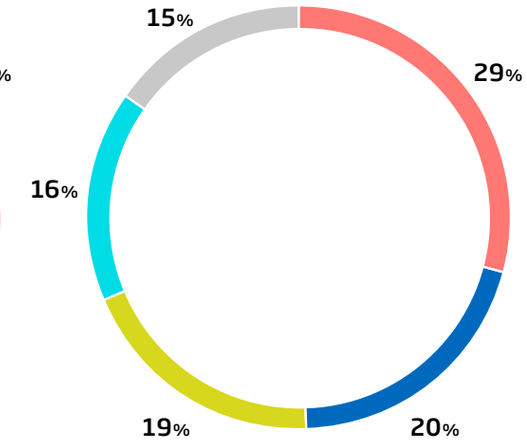

- 10-49 Mitarbeitende
- 50-249 Mitarbeitende
- ab 250 Mitarbeitende

**Funktion im Unternehmen**




- IT-Leitung / CIO
- Chief Information Security Officer (CISO)
- Verantwortliche:r für IT-Sicherheit
- Geschäftsführung oder Vorstand

**Aufteilung nach Branchen**




- Produzierendes Gewerbe
- Energie, Bau und Verkehr
- Handel
- Dienstleistungen
- Öffentlicher Bereich / Gesundheit

## Über den TÜV-Verband

Als TÜV-Verband e. V. vertreten wir die politischen Interessen der TÜV-Prüforganisationen und fördern den fachlichen Austausch unserer Mitglieder. Wir setzen uns für die technische und digitale Sicherheit sowie die Nachhaltigkeit von Fahrzeugen, Produkten, Anlagen und Dienstleistungen ein. Grundlage dafür sind allgemeingültige Standards, unabhängige Prüfungen und qualifizierte Weiterbildung. Unser Ziel ist es, das hohe Niveau der technischen Sicherheit zu wahren, Vertrauen in die digitale Welt zu schaffen und unsere Lebensgrundlagen zu erhalten. Dafür sind wir im regelmäßigen Austausch mit Politik, Behörden, Medien, Unternehmen und Verbraucher:innen.

**Mitglied der**

Allianz für Cyber-Sicherheit

TÜV VERBAND

## Ansprechpartner:innen


**Dr. Joachim Bühler**
Geschäftsführer
Tel. +49 30 760095-400
joachim.buehler@tuev-verband.de

**Marc Fliehe**
Fachbereichsleiter Digitalisierung und Bildung
+49 30 760095-460
marc.fliehe@tuev-verband.de

**Maurice Shahd**
Leiter Kommunikation
Tel. +49 30 760095-320
maurice.shahd@tuev-verband.de

**Linda Roy**
Pressereferentin
Tel. +49 30 760095-580
linda.roy@tuev-verband.de

**TÜV-Verband e. V.**
Friedrichstraße 136
10117 Berlin
Tel. +49 30 760095-400
berlin@tuev-verband.de
www.tuev-verband.de


## Grafik & Design


Nordpunkt Designagentur GmbH