# Wirtschaftsschutz 2025

Lagebild der deutschen Wirtschaft

bitkom

# Wirtschaftsschutz 2025

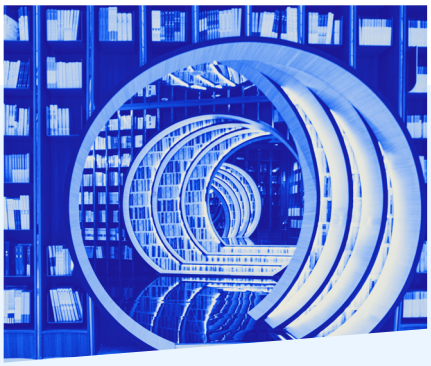
Lagebild der deutschen Wirtschaft

## Bitkom-Dataverse

Diese und weitere Bitkom-Studien finden Sie in unserem Datenportal.

Zum Bitkom-Dataverse

Zu den Studienberichten



DOI
10.64022/2025-wirtschaftsschutz

# Wichtigste Erkenntnisse

Die Frage nach den Wirtschaftsschutzmaßnahmen in Deutschland ist im Kontext zunehmender Bedrohungen durch Cyberkriminalität, Industriespionage und Sabotage von zentraler Bedeutung. Der Digitalverband Bitkom untersucht mit der vorliegenden Studie seit 2015 jährlich, wie es um die Sicherheit der deutschen Wirtschaft steht: Welche Branchen sind betroffen? Wer steckt dahinter? Und welche wirtschaftlichen Schäden entstehen?

Grundlage der aktuellen Erhebung ist eine repräsentative Befragung von 1.002 Unternehmen in Deutschland mit mindestens zehn Beschäftigten und einem Jahresumsatz ab einer Million Euro. Der Befragungszeitraum lag zwischen den Kalenderwochen 16 und 24 des Jahres 2025.

## Die Schlaglichter der Studie:

- Im Jahr 2025 beläuft sich der Gesamtschaden, den Unternehmen in Deutschland durch Diebstahl, Sabotage oder Industriespionage erlitten haben, auf rund **289,2 Milliarden Euro**. 70 Prozent dieses Schadens gehen direkt auf Cyberattacken zurück.
- Fast drei Viertel (**72 Prozent**) der Unternehmen bewerten die Bedrohungslage als hoch. 87 Prozent waren im vergangenen Jahr von Angriffen betroffen oder vermuten dies. Besonders häufig sind digitale Attacken: **73 Prozent** der betroffenen Unternehmen berichten von Angriffen auf Informations- und Produktionssysteme.
- Die Täter stammen häufig aus dem Ausland: **China und Russland** bleiben laut Einschätzung der Unternehmen die größten Bedrohungsquellen.
- Ransomware bleibt eine der gefährlichsten Bedrohungen: **Jedes siebte Unternehmen** zahlt bei Daten-Erpressungen Lösegeld, in Einzelfällen bis zu einer Million Euro und mehr.
- Immer mehr Unternehmen investieren in Cybersicherheit: Der Anteil des IT-Sicherheitsbudgets am gesamten IT-Budget liegt im Durchschnitt bei **18 Prozent**, Tendenz steigend. 59 Prozent verfügen über ein Notfallmanagement, und die Hälfte der Unternehmen schult regelmäßig ihre Beschäftigten im Umgang mit Sicherheitsrisiken.
- Politisch wächst der Handlungsdruck: **78 Prozent** der Unternehmen fordern, dass sich Deutschland besser gegen digitale Angriffe verteidigen kann, 44 Prozent plädieren für eine deutliche Erhöhung der Ausgaben für Cybersicherheit, und 74 Prozent wünschen sich stärkere Unterstützung für deutsche Anbieter von Sicherheitslösungen.

# Inhalt

# Abbildungen

# 1 Bedrohungslage

# 1 Bedrohungslage

Immer häufiger werden deutsche Unternehmen Ziel von Angriffen, digital wie analog: Daten werden gestohlen, Produktionsprozesse sabotiert, oder vertrauliche Informationen ausgespäht. Wirtschaftsschutz ist längst eine gesamtunternehmerische Herausforderung: Fast drei Viertel der Unternehmen fühlen sich durch analoge und digitale Angriffe stark bedroht. Eine Bedrohung, die real und messbar ist: Hinter ihr stehen Schäden in dreistelliger Milliardenhöhe, zunehmende Angriffe aus dem Ausland und neue Angriffsrisiken durch Künstliche Intelligenz. Wie also schätzen die befragten Unternehmen die aktuelle Lage ein? Wie stark empfinden sie die Bedrohung durch Datendiebstahl, Industriespionage und Sabotage?

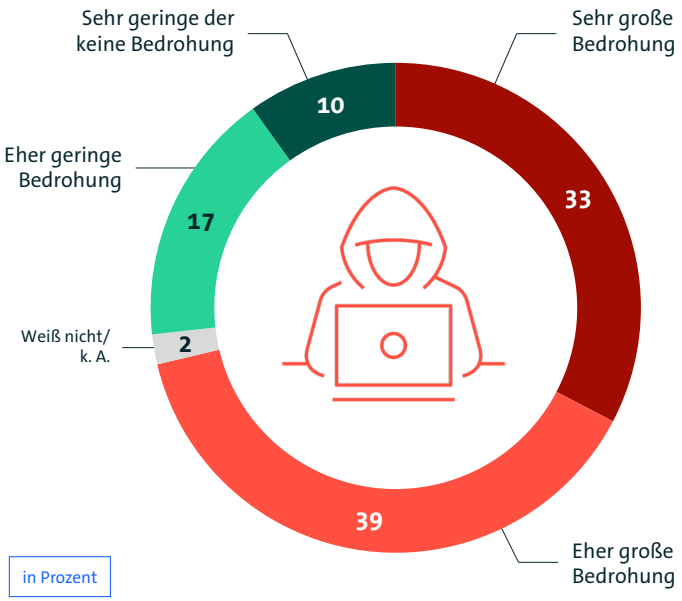
## 1.1 Allgemeine Einschätzung

Die große Mehrheit der Unternehmen sieht sich durch analoge und digitale Angriffe wie Datendiebstahl, Industriespionage und Sabotage stark bedroht: Insgesamt 72 Prozent der Befragten schätzen die Bedrohungslage als hoch ein. Davon bewerten 33 Prozent die Bedrohungslage als »sehr groß« und weitere 39 Prozent als »eher groß«. Nur ein kleinerer Anteil der Unternehmen stuft die Gefahr als weniger relevant ein: 17 Prozent sehen eine »eher geringe« und 10 Prozent »sehr geringe oder keine« Bedrohung.

Die Ergebnisse zeigen, dass Sicherheitsrisiken im analogen und digitalen Raum in der Risikoeinschätzung vieler Unternehmen eine bedeutende Rolle spielen.

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

**72%**
der Befragten schätzen die Bedrohungslage als **hoch** ein.




Basis: Alle Unternehmen (n=1.002) | Abweichungen von 100 Prozent sind rundungsbedingt | Quelle: Bitkom Research 2025

Abbildung 1: Einschätzung deutscher Unternehmen zur Bedrohung durch analoge und digitale Angriffe

# 2 Betroffenheit

# 2 Betroffenheit

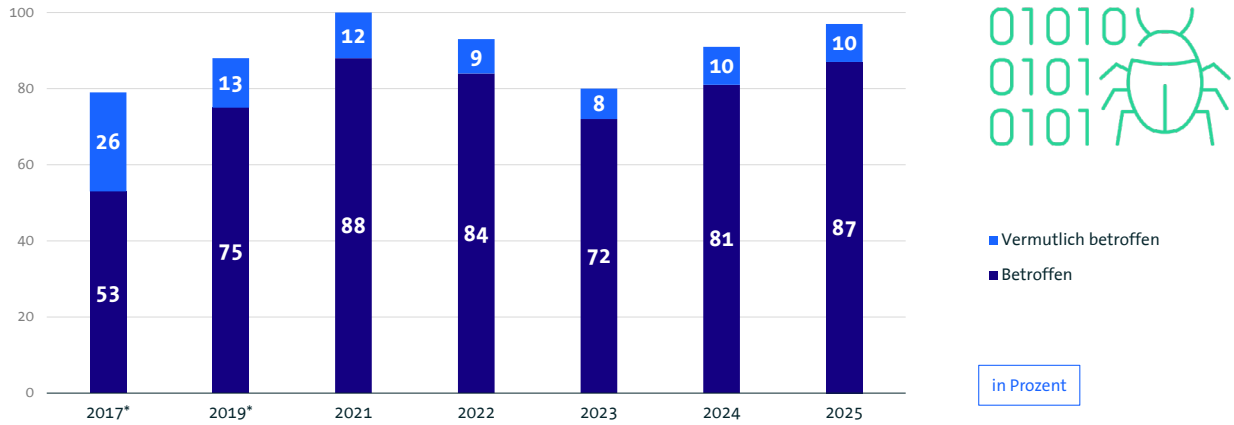
## 2.1 Anteil betroffener Unternehmen

Im Jahr 2025 gaben insgesamt 97 Prozent der befragten Unternehmen an, innerhalb der letzten zwölf Monate von Diebstahl, Industriespionage oder Sabotage betroffen oder vermutlich betroffen gewesen zu sein. Davon berichten 87 Prozent, dass ihr Unternehmen konkret betroffen war.

Der Anteil der tatsächlich betroffenen Unternehmen bewegt sich seit mehreren Jahren auf einem hohen Niveau:
Im Jahr 2021 wurde mit 88 Prozent der höchste Wert gemessen. Damit nähert sich der aktuelle Wert mit 87 Prozent wieder diesem bisherigen Höchststand an.

**Nahezu alle befragten Unternehmen** (97 Prozent) waren innerhalb der letzten zwölf Monate **von Diebstahl, Spionage oder Sabotage betroffen** oder vermuten betroffen zu sein.

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




Basis: Alle Unternehmen (n=1.002) | * 2017 und 2019 »innerhalb der letzten zwei Jahre« | Quelle: Bitkom Research 2025

Abbildung 2: Anteil betroffener Unternehmen in den Jahren 2017 bis 2025 (innerhalb der letzten 12 Monate)

## 2.2 Angriffsformen

### Digitale vs. analoge Angriffstypen

- **Digitale Angriffe** richten sich gegen IT-Systeme, Netzwerke und Daten, häufig in Form von Phishing, Schadsoftware oder Ransomware.
- **Analoge Angriffe** betreffen physische Werte, etwa durch Einbruch, Diebstahl oder Sabotage von Anlagen oder Geräten.
- **Hybride Angriffsmuster** verbinden beide Dimensionen, etwa wenn physischer Zugang zur Vorbereitung digitaler Angriffe genutzt wird.

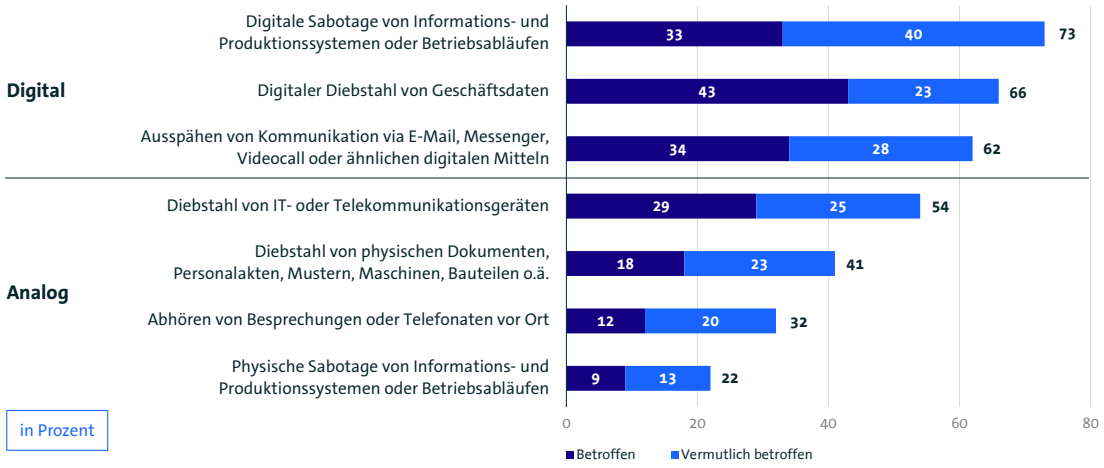
Digitale Angriffe dominieren, analoge Angriffe treten seltener auf, bleiben aber relevant – und Hybridformen nehmen weiter zu.

Digitale Angriffsformen betreffen Unternehmen deutlich häufiger als analoge. Am häufigsten genannt wird digitale Sabotage von Informations- und Produktionssystemen oder Betriebsabläufen: Insgesamt 73 Prozent der Unternehmen waren davon betroffen oder vermuten eine Betroffenheit. Auch der digitale Diebstahl von Geschäftsdaten (66 Prozent) sowie das Ausspähen digitaler Kommunikation wie E-Mails oder Messenger-Nachrichten (62 Prozent) wurden häufig berichtet.

Im analogen Bereich liegen die Werte deutlich darunter: So gaben 54 Prozent an, vom Diebstahl von IT- oder Telekommunikationsgeräten betroffen oder vermutlich betroffen gewesen zu sein. Der Diebstahl physischer Dokumente oder Muster (41 Prozent) sowie das Abhören von Besprechungen (32 Prozent) wurden seltener genannt. Am wenigsten betroffen sehen sich Unternehmen bei physischer Sabotage von Informations- oder Produktionssystemen (22 Prozent).

## Unternehmen werden vor allem digital angegriffen

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




Basis: Alle Unternehmen (n=1.002) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2025

Abbildung 3: Betroffene Unternehmen nach Art des Angriffs (digital vs. analog)

## 2.3 Arten gestohlener digitaler Geschäftsdaten

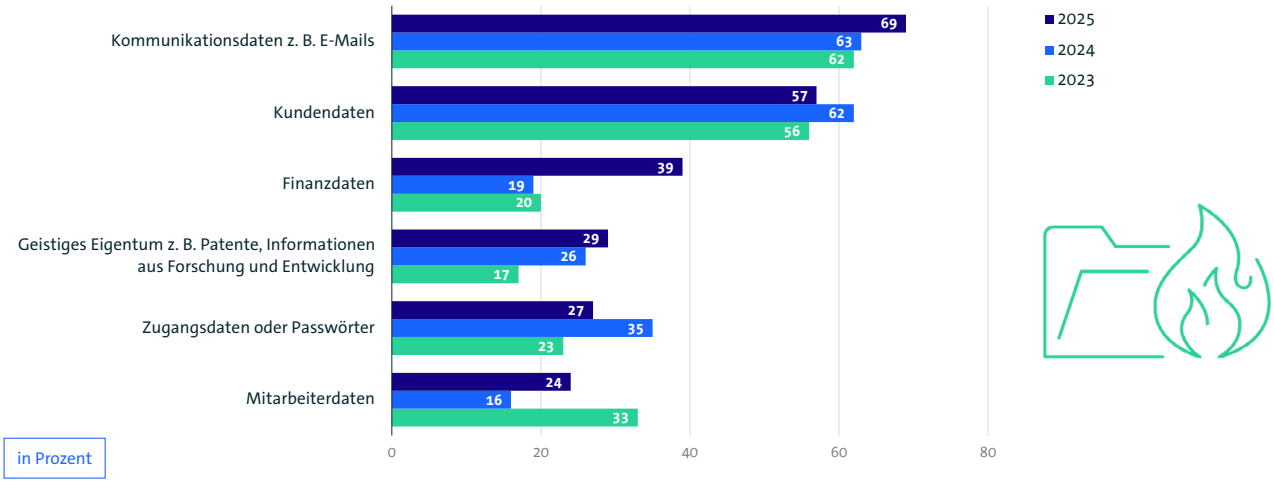
Im Jahr 2025 wurden besonders häufig Kommunikationsdaten wie E-Mails gestohlen: 69 Prozent der betroffenen Unternehmen meldeten entsprechende Vorfälle. Auch Kundendaten waren mit 57 Prozent häufig Ziel digitaler Angriffe, gefolgt von Finanzdaten mit 39 Prozent.
Alle drei Kategorien waren bereits in den Vorjahren regelmäßig betroffen.

Der Diebstahl geistigen Eigentums – etwa von Patenten oder Forschungsdaten – wurde von 29 Prozent der betroffenen Unternehmen angegeben. Zugangsdaten oder Passwörter waren bei 35 Prozent betroffen, Mitarbeiterdaten bei 24 Prozent.

> **Datendiebstahl bleibt der häufigste Angriffstyp (69 Prozent):** Er zeigt, dass wirtschaftliche Informationen längst genauso wertvoll sind wie physische Güter. Insbesondere Kommunikationsdaten und Daten von Kundinnen und Kunden sind für Angreifende attraktiv, da sie Einblicke in interne Abläufe, Geschäftsbeziehungen und digitale Identitäten ermöglichen.

### Datendiebstahl: Kommunikation, Kunden & Finanzen

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




Basis: Unternehmen, die in den letzten 12 Monaten vom Diebstahl digitaler Daten betroffen waren (n=432) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2025

Abbildung 4: Arten gestohlener digitaler Daten im Zeitvergleich

## 2.4 Täterakteure

Angriffe auf Unternehmen werden am häufigsten der organisierten Kriminalität zugeschrieben. 68 Prozent der betroffenen Unternehmen nannten Banden oder kriminelle Gruppen als Täterkreis. Knapp dahinter folgen Privatpersonen mit 42 Prozent. Beide Gruppen werden über die Jahre hinweg konstant häufig genannt.

Auffällig ist der Anstieg bei Angriffen, die ausländischen Nachrichtendiensten zugeschrieben werden: Während 2023 noch 7 Prozent der Unternehmen diese Quelle angaben, stieg der Wert 2024 auf 20 Prozent und erreicht dieses Jahr mit 28 Prozent einen neuen Höchststand.

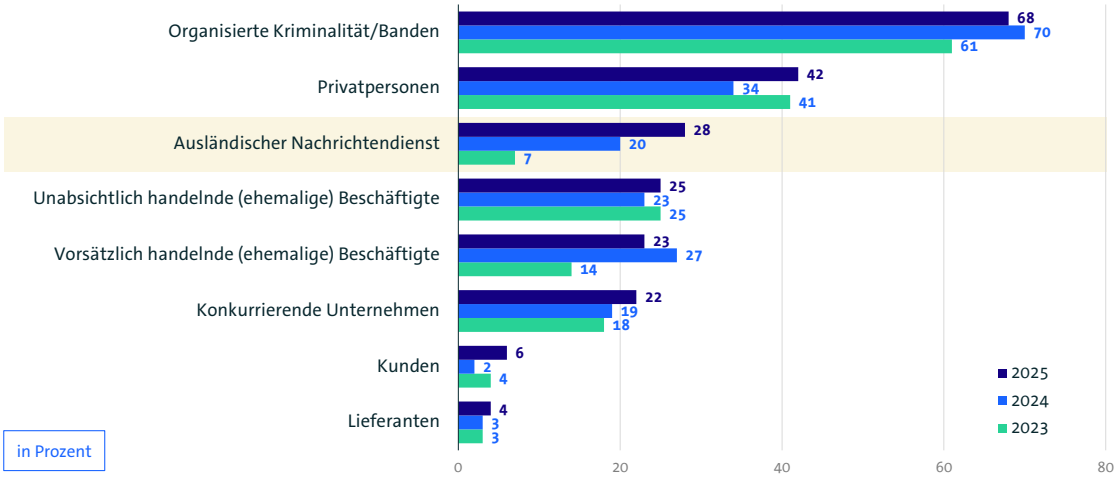
Auch ehemalige Beschäftigte spielen weiterhin eine Rolle: 25 Prozent der Unternehmen berichten von unabsichtlichem Fehlverhalten, 23 Prozent von vorsätzlichem Handeln. Konkurrierende Unternehmen wurden 2025 von 22 Prozent genannt. Kundinnen und Kunden und Akteure der Lieferkette spielen bei der Angabe von Täterkreisen hingegen eine untergeordnete Rolle.

**28 %**

Angriffe durch **ausländische Nachrichtendienste.** Und sie nehmen deutlich zu: Ihr Anteil stieg von 7 Prozent im Jahr 2023 auf nun 28 Prozent im Jahr 2025.

## Geheimdienste nehmen die Wirtschaft ins Visier

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




Basis: Unternehmen, die in den letzten 12 Monaten von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=868) | Mehrfachnennungen möglich |
Quelle: Bitkom Research 2025

Abbildung 5: Täterkreise bei Angriffen auf Unternehmen

## 2.5 Informationsgewinn über Täterkreise

Bei der Aufklärung von Angriffen auf Unternehmen spielen technische Auswertungen weiterhin die größte Rolle. 75 Prozent der betroffenen Unternehmen nannten die Analyse von Log-Dateien als Grundlage ihrer Erkenntnisse – ein deutlicher Anstieg gegenüber dem Vorjahr (66 Prozent). Auf Platz zwei folgen Informationen von Behörden, deren Bedeutung ebenfalls deutlich zugenommen hat: 35 Prozent der Unternehmen nannten diese Quelle im Jahr 2025, im Vorjahr waren es noch 24 Prozent.

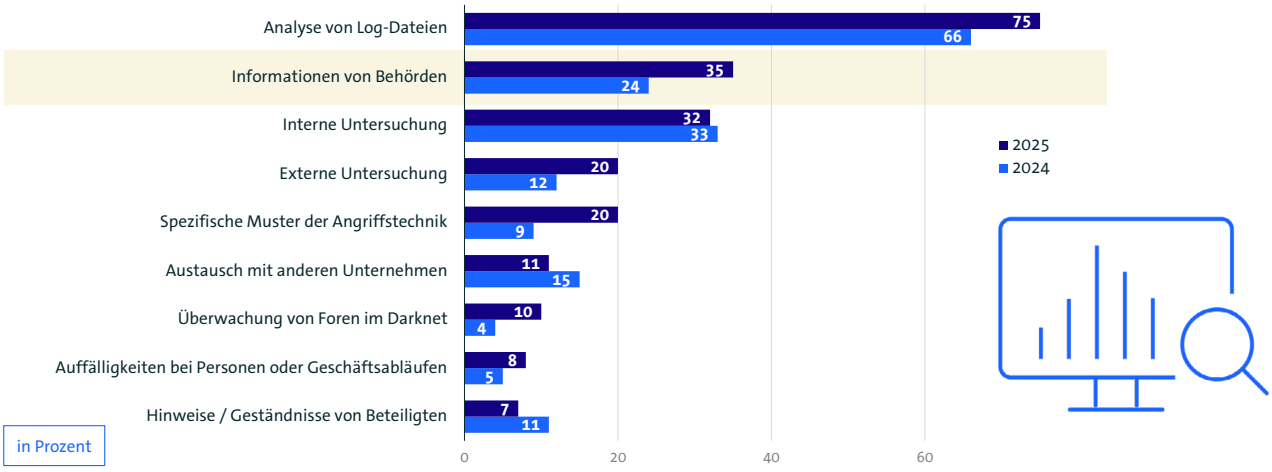
Darüber hinaus kamen Erkenntnisse häufig durch interne Untersuchungen zustande (32 Prozent), während externe Untersuchungen bei 20 Prozent der Unternehmen eine Rolle spielten. Andere Quellen wie spezifische Angriffsmuster (20 Prozent), der Austausch mit anderen Unternehmen (15 Prozent) oder die Überwachung von Foren im Darknet (10 Prozent) wurden seltener genannt. Hinweise durch Beteiligte oder Auffälligkeiten im Unternehmen spielten nur in wenigen Fällen eine Rolle.

**35 %**

**Mehr als ein Drittel** der Unternehmen erhielt Hinweise auf Täterkreise über Behörden.

### Ermittlung der Täter: Behörden helfen verstärkt mit

Auf welcher Grundlage haben Sie die Erkenntnisse erlangt?




Basis: Unternehmen, die in den letzten 12 Monaten von Datendiebstahl, Industriespionage oder Sabotage betroffen waren und Erkenntnisse über Herkunft oder Täterkreis (n=823) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2025

Abbildung 6: Quellen der Kenntnis über Täterkreise bei Angriffen auf Unternehmen

## 2.6 Zulieferer

Rund jedes vierte Unternehmen berichtet, dass innerhalb der letzten zwölf Monate ein Zulieferer entweder »sicher« (9 Prozent) oder »vermutlich« (19 Prozent) von Datendiebstahl, Sabotage oder Industriespionage betroffen war. 53 Prozent der befragten Unternehmen verneinen dies, 15 Prozent können keine Angabe machen.

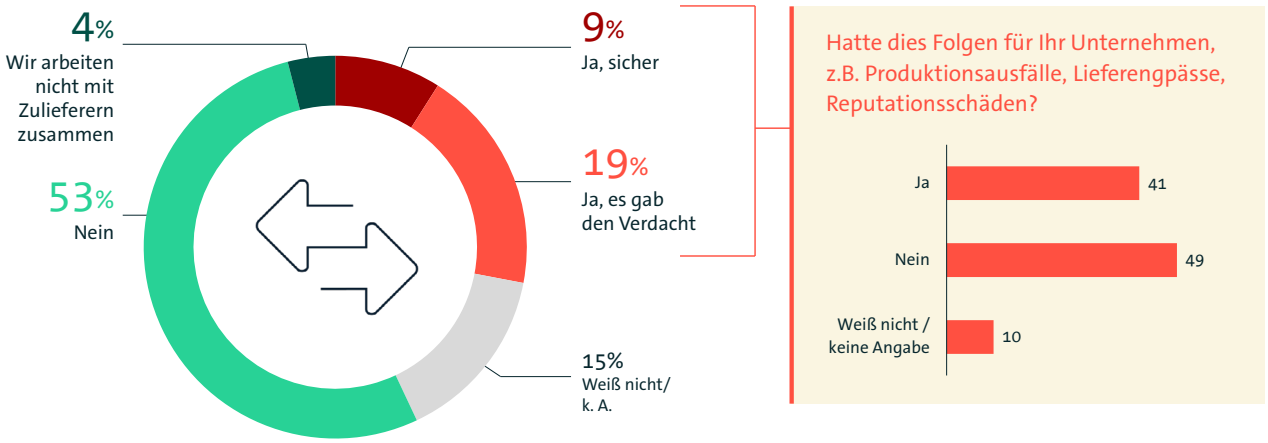
Wenn Zulieferer betroffen waren oder ein Verdacht bestand, hatte das in 41 Prozent der Fälle direkte Auswirkungen auf das eigene Unternehmen, zum Beispiel durch Produktionsausfälle, Lieferengpässe oder Reputationsschäden. In 49 Prozent der Fälle waren keine Folgewirkungen spürbar. Und zehn Prozent machten hierzu keine Angabe.

Die Ergebnisse zeigen: Angriffe auf Partnerunternehmen können sich spürbar auf die eigene Geschäftstätigkeit auswirken, insbesondere in eng vernetzten Lieferketten.

**41 %**

Der betroffenen Unternehmen berichten von spürbaren Folgen durch Angriffe auf Zulieferer, etwa **Lieferausfälle** oder **Reputationsschäden**.

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




Basis links: Unternehmen (n=1.002) | Basis rechts: Unternehmen, bei denen Zulieferer betroffen oder vermutlich betroffen waren (n=284) | Quelle: Bitkom Research 2025

Abbildung 7: Betroffenheit von Zulieferern durch Angriffe sowie Folgewirkungen auf das eigene Unternehmen

## 2.7 Herkunft der Angriffe

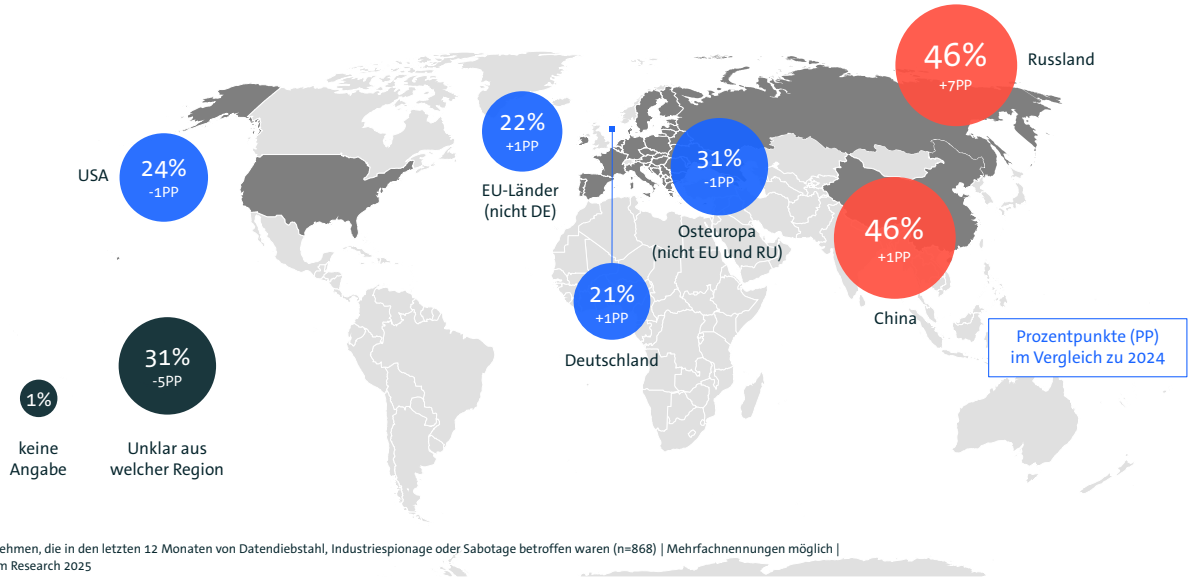
Die meisten Angriffe auf Unternehmen werden weiterhin mit China und Russland in Verbindung gebracht. Jeweils 46 Prozent der betroffenen Unternehmen geben an, mindestens einen Angriff aus Russland oder China festgestellt zu haben. Im Vergleich zum Vorjahr bedeutet dies einen deutlichen Anstieg bei Russland (2024: 39 Prozent) und eine leichte Zunahme bei China (2024: 45 Prozent).

Mit deutlichem Abstand folgen weitere Herkunftsregionen: 31 Prozent der Unternehmen berichten von Angriffen aus Osteuropa (außerhalb der EU) (2024: 32 Prozent), 24 Prozent aus den USA (2024: 25 Prozent), 22 Prozent aus anderen EU-Ländern (2024: 21 Prozent) und 21 Prozent aus Deutschland (2024: 20 Prozent).

Rund jedes dritte Unternehmen (31 Prozent, 2024: 36 Prozent) konnte die Angriffe keinem bestimmten Herkunftsland zuordnen.

### China und Russland bleiben die größte Bedrohung

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




Basis: Unternehmen, die in den letzten 12 Monaten von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=868) | Mehrfachnennungen möglich |
Quelle: Bitkom Research 2025

Abbildung 8: Herkunftsregionen von Cyberangriffen

« Die Grenzen zwischen Cyberspionage und Cybercrime verschwimmen zunehmend. Wir sehen, dass staatliche Akteure kriminelle Aktivitäten privater Gruppierungen dulden oder aktiv einsetzen. Deshalb kommt es entscheidend darauf an, dass wir als Cyber- und Spionageabwehr die enge und gute Zusammenarbeit der nationalen und internationalen Sicherheitsbehörden weiter ausbauen, gleichzeitig aber auch die deutschen Wirtschaftsunternehmen enger und intensiver einbinden.»[1]

1 Sinan Selen, Vizepräsident des Bundesamtes für Verfassungsschutz ↗Bitkom-Presseinformation

# 3 Schäden und Angriffsformen

# 3 Schäden und Angriffsformen

## 3.1 Schadenshöhe

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

| Schaden durch... | Schadenssummen in Mrd. Euro (**2025**) | Schadenssummen in Mrd. Euro (2024) | Schadenssummen in Mrd. Euro (2023) |
|---|---|---|---|
| **Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen** | 73,3 | 54,5 | 35,0 |
| **Kosten für Rechtsstreitigkeiten** | 53,0 | 53,1 | 29,8 |
| **Kosten für Ermittlungen und Ersatzmaßnahmen** | 37,0 | 32,2 | 25,2 |
| **Umsatzeinbußen durch nachgemachte Produkte bzw. Plagiate** | 30,6 | 39,2 | 15,3 |
| **Datenschutzrechtliche Maßnahmen, z.B. durch Behörden** | 23,8 | 27,2 | 12,4 |
| **Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen** | 23,1 | 11,2 | 21,5 |
| **Patentrechtsverletzungen, auch vor Anmeldung** | 16,0 | 14,8 | 10,4 |
| **Imageschaden bei Kunden oder Lieferanten, Negative Medienberichterstattung** | 15,9 | 20,2 | 35,3 |
| **Erpressung mit gestohlenen Daten** | 15,6 | 13,4 | 16,1 |
| **Geldabfluss durch Betrugsversuche** | 0,9 | 0,8 | 3,9 |
| **Sonstige Schäden** | 0 | 0 | 1,1 |
| **Gesamtschaden pro Jahr** | **289,2** | **266,6** | **205,9** |

Basis: Alle Unternehmen (n=1.002) | Mehrfachnennungen möglich | rundungsbedingt kann die Summe der Einzelschäden vom Gesamtschaden abweichen. | Quelle: Bitkom Research 2025

Abbildung 9: Wirtschaftliche Schäden durch Angriffe auf Unternehmen in Milliarden Euro

Der Gesamtschaden durch Angriffe auf Unternehmen ist seit 2023 **um über 83 Milliarden Euro gestiegen**: Dabei entfallen 70 Prozent allein auf Cyberattacken.

Im Jahr 2025 beläuft sich der Gesamtschaden, den Unternehmen in Deutschland durch Diebstahl, Sabotage oder Industriespionage erlitten haben, auf rund **289,2 Milliarden Euro**. Damit setzt sich der negative Trend der Vorjahre fort: 2024 lag der Schaden noch bei 266,6 Milliarden Euro, 2023 bei 205,9 Milliarden Euro.

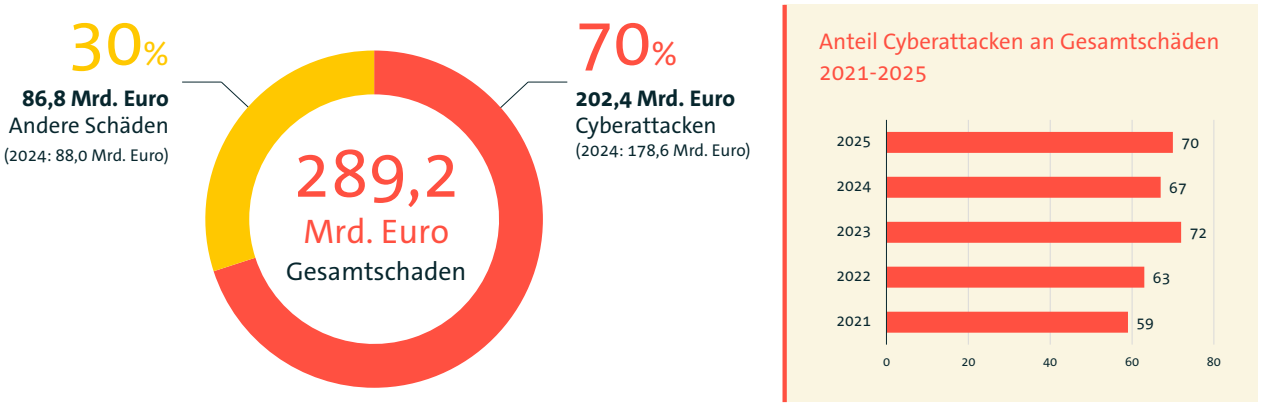
Besonders gravierend sind die Auswirkungen durch den **Ausfall, Diebstahl oder die Schädigung von Informations- und Produktionssystemen**. Allein dieser Bereich verursacht 2025 Schäden in Höhe von **73,3 Milliarden Euro**.

Auch die Kosten für Rechtsstreitigkeiten (53,0 Mrd. Euro) sowie für Ermittlungen und Ersatzmaßnahmen (37,0 Mrd. Euro) sind erheblich. Weitere Schadenstreiber sind nachgemachte Produkte, Datenschutzauflagen und der Verlust von Wettbewerbsvorteilen. Auch Erpressung, Reputationsverluste und Patentverletzungen tragen spürbar zum Gesamtschaden bei.

Die wirtschaftlichen Folgen krimineller Angriffe auf Unternehmen nehmen also weiter zu, sowohl in der Breite der Schadensarten als auch im Gesamtumfang.

# Der Großteil der Schäden entsteht durch Cyberattacken

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




Basis: Unternehmen, die in den letzten 12 Monaten von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=868) | Quelle: Bitkom Research 2025

Abbildung 10: Prozentualer Anteil des entstandenen Gesamtschadens, der auf Cyberattacken zurückgeführt werden kann

Rund 70 Prozent des gesamten Schadens entfallen inzwischen auf Cyberattacken. Damit übersteigen die digitalen Angriffe erstmals die Marke von 200 Milliarden Euro. Während andere Schadensarten nahezu konstant bleiben, wächst der Anteil der Cyberkriminalität Jahr für Jahr weiter.

Die Zahlen zeigen: Wirtschaftliche Verluste entstehen heute in erster Linie im digitalen Raum – durch gehackte Systeme, gestohlene Daten und erpresste Unternehmen.

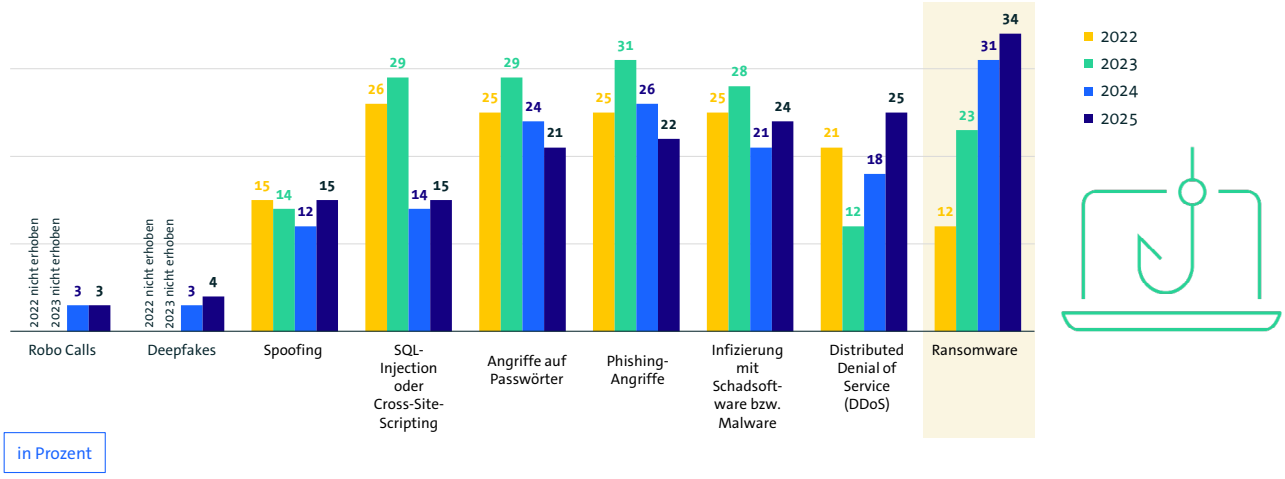
## 3.2 Arten von Cyberangriffen

Unternehmen berichten am häufigsten von Schäden durch Ransomware: 34 Prozent der Befragten gaben an, in den letzten 12 Monaten betroffen gewesen zu sein. Auf dem zweiten Platz liegen Distributed Denial of Service (DDoS)-Angriffe mit 25 Prozent, gefolgt von Infektionen mit Schadsoftware bzw. Malware mit 24 Prozent. Phishing-Angriffe verursachten bei 22 Prozent der Unternehmen Schäden, Angriffe auf Passwörter bei 21 Prozent.

Technisch anspruchsvollere Angriffe wie SQL-Injection oder Cross-Site-Scripting wurden 2025 von 15 Prozent der Unternehmen als schadensverursachend genannt. Spoofing liegt ebenfalls bei 15 Prozent. Vergleichsweise selten berichten Unternehmen von Schäden durch Robocalls (3 Prozent) und Deepfakes (4 Prozent).

> **DDoS-Angriffe** sind Überlastungen, bei denen Server mit Anfragen geflutet werden, bis sie lahmgelegt sind. So stehen Webseiten und Prozesse stundenlang still.

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




Basis: Alle Unternehmen (n=1.002) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2025

Abbildung 11: Schäden durch verschiedene Arten von Cyberangriffen

> **Ransomware** zählt zu den gefährlichsten Arten von Schadsoftware. Dabei werden Daten verschlüsselt und erst gegen Zahlung eines Lösegelds wieder freigegeben (engl. »ransom«). Neben dem direkten Datenverlust kann es zu Produktionsausfällen, Reputationsschäden und hohen Wiederherstellungskosten kommen. In vielen Fällen wird mit der Veröffentlichung sensibler Daten zusätzlich Druck auf die Opfer ausgeübt.[1]

1 Bundesamt für Sicherheit der Informationstechnik (BSI)

## Haben Sie bei Ransomware-Angriffen Lösegeld gezahlt?

Unternehmen, die von Ransomware betroffen waren, reagieren bisher überwiegend zurückhaltend auf Lösegeldforderungen. 70 Prozent der befragten Unternehmen geben an, kein Lösegeld gezahlt zu haben. 15 Prozent zahlten dagegen einmalig. Kein Unternehmen gab an, mehrfach gezahlt zu haben. Weitere 15 Prozent machten keine Angabe dazu.

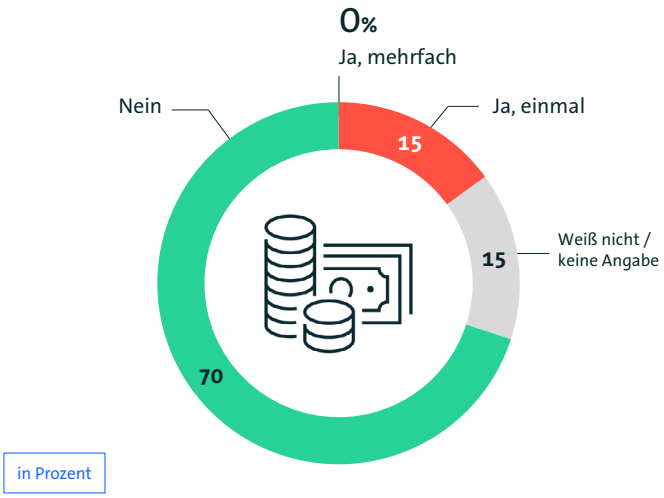
Bei denjenigen, die Lösegeld zahlten, liegen die Summen überwiegend im Bereich von 100.000 bis 500.000 Euro (34 Prozent) oder zwischen 10.000 und 100.000 Euro (19 Prozent). 12 Prozent zahlten zwischen 500.000 und 1 Million Euro, 4 Prozent sogar über 1 Million Euro.

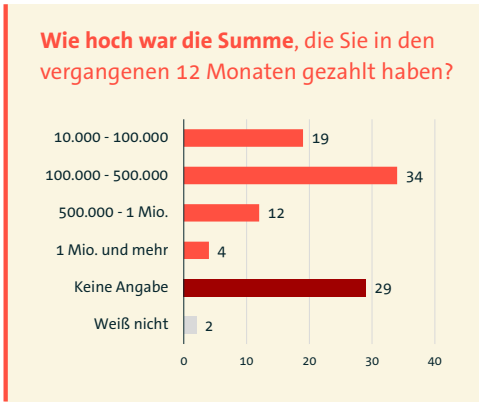
Knapp ein Drittel (29 Prozent) der Unternehmen machte keine Angaben zur Summe.

Die Ergebnisse zeigen: Zwar ist die Bereitschaft zur Zahlung gering, doch wenn bezahlt wird, fallen die Beträge in vielen Fällen erheblich aus.

> **Wer zahlt, zahlt oft viel:** 50 Prozent der Befragten haben nach Angriffen mehr als 100.000 Euro Lösegeld gezahlt.

## Jedes siebte Unternehmen zahlt an Daten-Erpresser




Basis links: Unternehmen, die von Ransomware-Angriffen betroffen waren (n=588) | Basis rechts: Unternehmen, die Lösegeld bezahlt haben (n=86) | Quelle: Bitkom Research 2025

Abbildung 12: Lösegeldzahlungen an Erpresser

## 3.3 Entwicklung von Cyberangriffen

Die Mehrheit der Unternehmen in Deutschland berichtet von einer Zunahme der Cyberangriffe innerhalb der letzten zwölf Monate. 37 Prozent der befragten Unternehmen geben an, dass die Anzahl der Attacken »stark zugenommen« hat. Weitere 36 Prozent berichten von einem »eher« gestiegenen Angriffsniveau. Nur 26 Prozent sehen keine Veränderung, während Rückgänge bei Cyberangriffen kaum genannt werden.

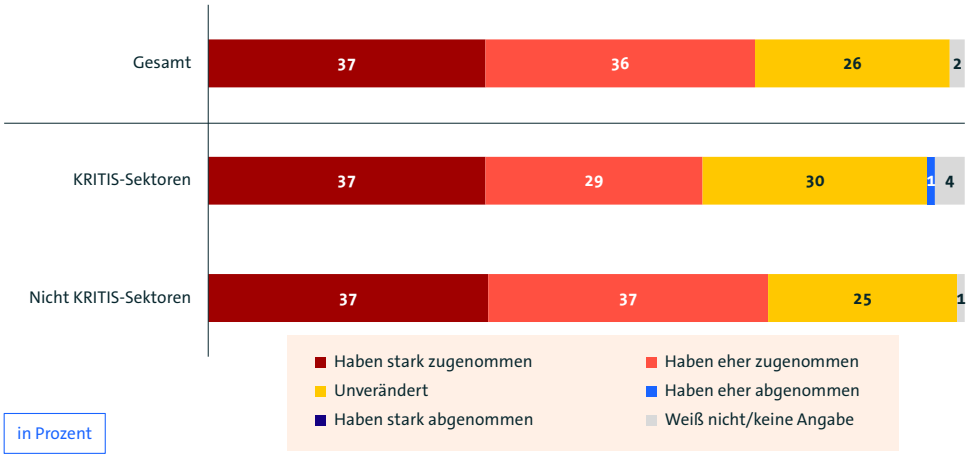
Der Vergleich zwischen KRITIS- und Nicht-KRITIS-Sektoren zeigt interessante Unterschiede: Auch hier berichten jeweils 37 Prozent von einer starken Zunahme. In den KRITIS-Sektoren fällt die Gruppe mit eher zunehmenden Angriffen jedoch kleiner aus (29 Prozent) als in den Nicht-KRITIS-Sektoren (37 Prozent). Gleichzeitig geben in den KRITIS-Bereichen 30 Prozent an, dass sich die Angriffslage nicht verändert hat.

Rückgänge sind die Ausnahme: Nur 1 Prozent der KRITIS-Unternehmen und 1 Prozent der Nicht-KRITIS-Unternehmen berichten von leicht abnehmenden Angriffen. Werte für eine starke Abnahme liegen bei null oder ein Prozent.

Insgesamt zeigt sich damit ein klarer Trend: Die Zahl der Cyberattacken nimmt weiter zu, und das quer durch alle Unternehmensbereiche.

> **Mehr als jedes dritte Unternehmen** (37 Prozent) verzeichnet stark gestiegene Cyberangriffe – unabhängig vom Sektor.

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




Basis: Alle Unternehmen (n=1.002) | Abweichungen von 100 Prozent sind rundungsbedingt | Quelle: Bitkom Research 2025

Abbildung 13: Entwicklung der Anzahl von Cyberattacken in den vergangenen 12 Monaten

## 3.4 Erwartete Entwicklung

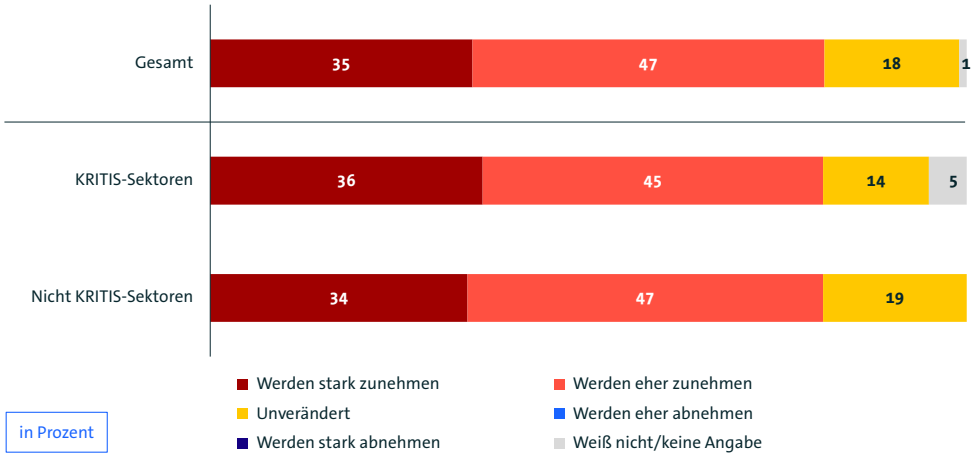
Die große Mehrheit der Unternehmen in Deutschland erwartet in den kommenden zwölf Monaten eine Zunahme der Cyberattacken. 35 Prozent gehen davon aus, dass die Anzahl der Angriffe »stark zunehmen« wird, weitere 47 Prozent rechnen mit einer »eher zunehmenden« Bedrohungslage. Zusammengenommen erwarten damit 82 Prozent der Befragten eine Zunahme der Cyberangriffe.

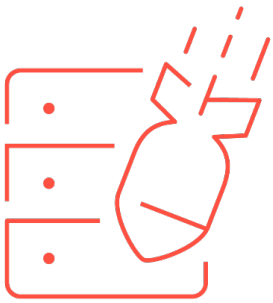
Im Detail zeigt sich: In den KRITIS-Sektoren rechnen 36 Prozent mit einer »stark zunehmenden« Anzahl an Cyberattacken, weitere 45 Prozent erwarten eine »eher zunehmende« Entwicklung. 14 Prozent der befragten KRITIS-Unternehmen gehen von einer unveränderten Lage aus, während niemand mit einer Abnahme rechnet.

Auch in den Nicht-KRITIS-Sektoren ist das Bild ähnlich: 34 Prozent prognostizieren stark steigende, 47 Prozent eher steigende Angriffe. 19 Prozent rechnen mit einer gleichbleibenden Bedrohungslage. Rückgänge werden auch hier praktisch nicht erwartet.

> Über alle Unternehmensbereiche hinweg herrscht eine klare Erwartung, dass die Bedrohungslage weiter zunimmt.

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



Basis: Alle Unternehmen (n=1.002) | Abweichungen von 100 Prozent sind rundungsbedingt | Quelle: Bitkom Research 2025

Abbildung 14: Erwartete Entwicklung der Anzahl von Cyberattacken in den nächsten 12 Monaten

## 3.5 «Social Engineering»

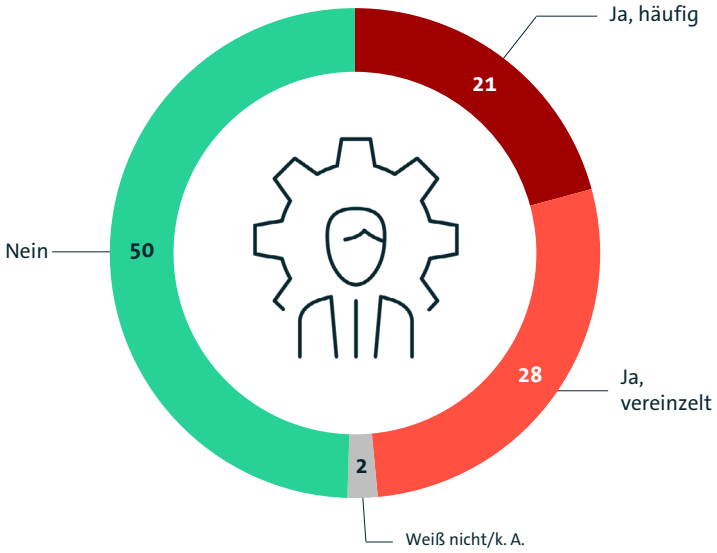
Knapp jedes zweite Unternehmen berichtet von Versuchen, mit Hilfe von »Social Engineering« Angriffe wie Datendiebstahl, Industriespionage oder Sabotage vorzubereiten.

28 Prozent der befragten Unternehmen geben an, dass solche Versuche in den letzten zwölf Monaten »vereinzelt« stattgefunden haben, 21 Prozent berichten von »häufigen« Fällen. Die übrige Hälfte (50 Prozent) hat keine entsprechenden Versuche festgestellt.

Die Daten zeigen: Social Engineering ist ein relevantes Angriffsmuster, das zwar nicht alle Unternehmen betrifft, aber bei rund jedem fünften Betrieb häufig auftritt. Die Mehrheit berichtet von »vereinzelt« auftretenden Vorfällen, meist in Form gefälschter E-Mails oder täuschender Anrufe.

### Jedes zweite Unternehmen im Visier

Gab es in den vergangenen 12 Monaten Versuche, mit Hilfe von **Social Engineering** Datendiebstahl, Industrie-spionage oder Sabotage vorzubereiten?




in Prozent

Basis: Alle Unternehmen (n=1.002) | Abweichungen von 100 Prozent sind rundungsbedingt | Quelle: Bitkom Research 2025

Abbildung 15: Anteil der Unternehmen mit beobachteten Social-Engineering-Versuchen

**»Social Engineering«** bezeichnet Techniken, bei denen Angreifende menschliches Verhalten ausnutzen, um Zugang zu Informationen, Systemen oder Einrichtungen zu erlangen. Typische Mittel sind z. B.**gefälschte E-Mails**, **Anrufe** oder **manipulierte Webseiten**, die Mitarbeitende zur Herausgabe von Zugangsdaten oder zur Ausführung schädlicher Aktionen bringen.[1]

1 Bundesamt für Sicherheit der Informationstechnik (BSI)

# 4 Künstliche Intelligenz & IT-Sicherheit

# 4 Künstliche Intelligenz & IT-Sicherheit

Künstliche Intelligenz verändert auch die Spielregeln der Cybersicherheit: Sie kann Angriffe schneller erkennen, Datenströme analysieren und Systeme in Echtzeit schützen. Dieselben Technologien stehen jedoch auch den Angreifern zur Verfügung. Damit entwickelt sich KI zu einem Schlüsselfaktor im digitalen Ringen zwischen Schutz und Angriff. Wie gehen Unternehmen heute also mit dieser neuen Dynamik um, welche Rolle spielt KI bereits in der IT-Sicherheit?

## 4.1 KI-Einsatz in der IT-Sicherheit

Aktuell setzen sechs Prozent der befragten Unternehmen bereits Künstliche Intelligenz (KI) zur Verbesserung der IT-Sicherheit ein. Weitere 32 Prozent geben an, dies fest geplant zu haben. Somit befürworten 38 Prozent der Unternehmen den Einsatz von KI im Bereich der Cybersicherheit.

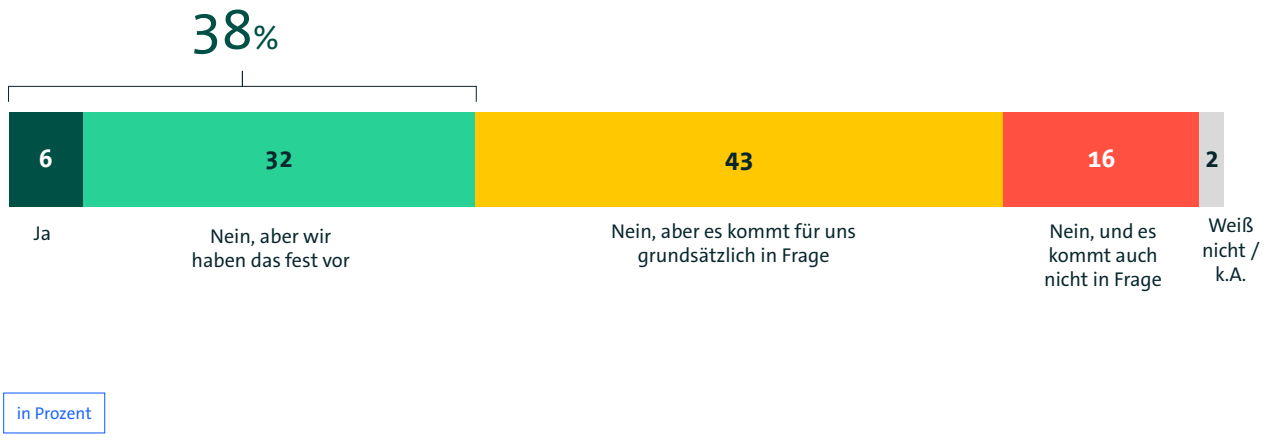
Ein größerer Anteil von 43 Prozent der Unternehmen nutzt derzeit keine KI, kann sich deren Einsatz aber grundsätzlich vorstellen. 16 Prozent schließen den Einsatz von KI im Kontext der IT-Sicherheit hingegen aus.

Insgesamt zeigt sich also, dass sich eine Mehrheit der Unternehmen (insgesamt 81 Prozent) zumindest offen gegenüber KI-Lösungen in der IT-Sicherheit zeigt.

> Die Mehrheit der Unternehmen zeigt sich offen für den Einsatz von Künstlicher Intelligenz in der IT-Sicherheit – **tatsächlich umgesetzt wird das bislang jedoch nur von wenigen.**

**4 von 10 Unternehmen setzen auf KI**

Setzen Sie KI zur Verbesserung der IT-Sicherheit ein?




Basis: Alle Unternehmen (n=1.002) | Abweichungen von 100 Prozent sind rundungsbedingt | Quelle: Bitkom Research 2025

Abbildung 16: Anteil der Unternehmen, die KI zur Verbesserung der IT-Sicherheit einsetzen

## 4.2 KI-Einsatz von Angreifern

Mehr als jedes zweite Unternehmen (insgesamt 66 Prozent) hat den Eindruck, dass bei Cyberangriffen auf ihr Unternehmen verstärkt Künstliche Intelligenz zum Einsatz kommt. 16 Prozent bestätigen dies eindeutig mit »Ja, auf jeden Fall«, während 50 Prozent »eher ja« angeben.

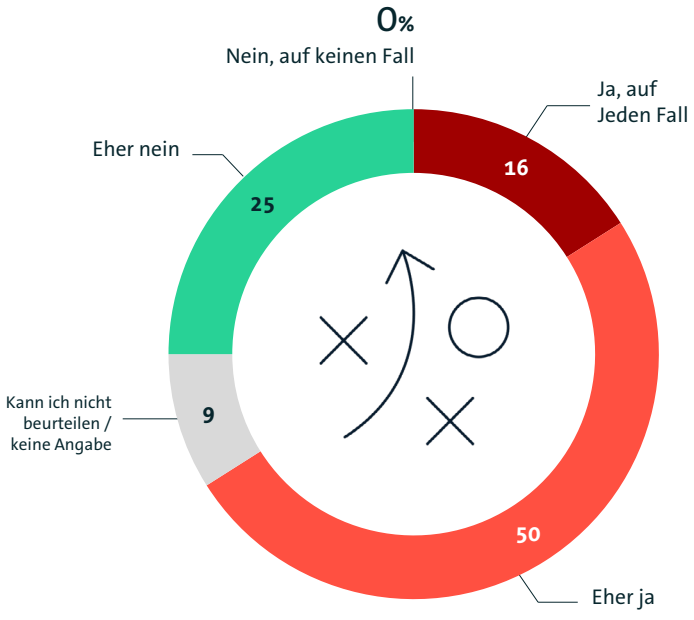
Ein Viertel der Befragten (25 Prozent) sieht hingegen keine eindeutigen Hinweise auf KI-Einsatz bei Angriffen und gibt »eher nein« an. Keines der befragten Unternehmen verneint den KI-Einsatz vollständig. Weitere neun Prozent können die Frage nicht beurteilen oder machten keine Angabe.

Die Ergebnisse verdeutlichen, dass der Eindruck eines zunehmenden KI-Einsatzes durch Angreifende in der Unternehmensrealität angekommen ist.

Gleichzeitig herrscht bei einem Teil der Befragten noch Unsicherheit über die genaue Vorgehensweise der Angreifer.

> **Angreifer setzen zunehmend auf Künstliche Intelligenz:** Zwei von drei Unternehmen (66 Prozent) beobachten entsprechende Hinweise bei Cyberattacken.

Haben Sie den Eindruck, dass bei Angriffen auf Ihr Unternehmen verstärkt KI eingesetzt wird?




in Prozent

Basis: Alle Unternehmen (n=1.002) | Quelle: Bitkom Research 2025

Abbildung 17: Einschätzung von Unternehmen zum KI-Einsatz bei Cyberangriffen auf das eigene Unternehmen

# 5 Sicherheitsmaßnahmen im Unternehmen

# 5 Sicherheitsmaßnahmen im Unternehmen

Cybersicherheit ist längst keine reine IT-Frage mehr, sondern ein entscheidender Faktor für die Widerstandsfähigkeit der gesamten Wirtschaft. Wie gut Unternehmen auf Angriffe vorbereitet sind, zeigt sich in Strukturen, Prozessen und Prioritäten, vom Notfallmanagement über Mitarbeiterschulungen bis zu Investitionen in Sicherheitstechnologien.
Doch investieren Unternehmen ausreichend in Prävention und Abwehr, sind sie auf den Ernstfall vorbereitet?

## 5.1 Notfallmanagement

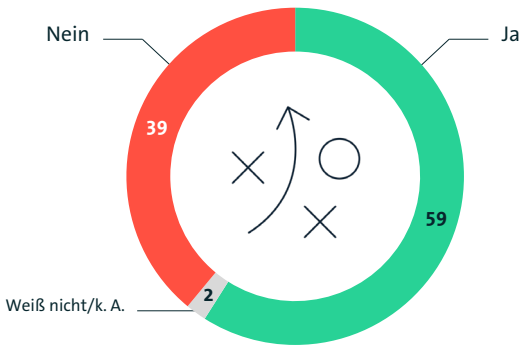
59 Prozent der Unternehmen verfügen über ein Notfallmanagement für den Fall von Datendiebstahl, Sabotage oder Industriespionage. 39 Prozent geben an, keinen entsprechenden Plan zu haben.

Der Blick auf die Entwicklung seit 2017 zeigt zudem einen langfristigen Anstieg: Während 2017 nur 43 Prozent ein Notfallmanagement eingeführt hatten, stieg der Anteil bis 2023 auf 59 Prozent. Im Jahr 2024 sank der Wert kurzzeitig auf 54 Prozent, erreichte 2025 aber erneut den Höchststand von 59 Prozent.

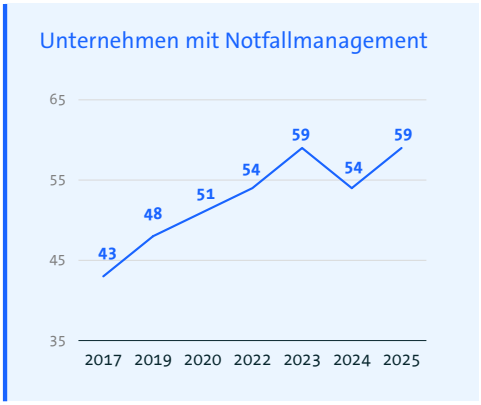
Trotz dieser positiven Entwicklung verfügt weiterhin mehr als ein Drittel der Unternehmen über keine strukturierte Vorbereitung auf sicherheitsrelevante Vorfälle.

**Sechs von zehn Unternehmen haben einen Notfallplan für Sicherheitsvorfälle –** 39 Prozent sind hingegen weiterhin unvorbereitet.

Verfügt Ihr Unternehmen über ein **Notfallmanagement**, für den Fall des Auftretens von Datendiebstahl, Industriespionage oder Sabotage?




in Prozent




Basis: Alle Unternehmen (n=1.002) | Quelle: Bitkom Research 2025

Abbildung 18: Anteil der Unternehmen mit Notfallmanagement bei Datendiebstahl, Spionage oder Sabotage

## 5.2 Anteil des Budgets für IT-Sicherheit

Der durchschnittliche Anteil des IT-Sicherheitsbudgets am gesamten IT-Budget beträgt im Jahr 2025 18 Prozent. Damit setzt sich der kontinuierliche Anstieg der letzten Jahre fort: 2022 lag der Durchschnitt noch bei 9 Prozent, 2023 bei 14 Prozent und 2024 bereits bei 17 Prozent.

Im Detail zeigt sich: 43 Prozent der Unternehmen investieren zwischen 10 und unter 20 Prozent ihres IT-Budgets in Sicherheit. Weitere 41 Prozent geben sogar an, 20 Prozent oder mehr dafür aufzuwenden. Nur ein kleiner Teil der Unternehmen liegt deutlich darunter: 8 Prozent investieren zwischen 5 und unter 10 Prozent, lediglich 2 Prozent weniger als 5 Prozent. 6 Prozent machten hierzu keine Angabe.

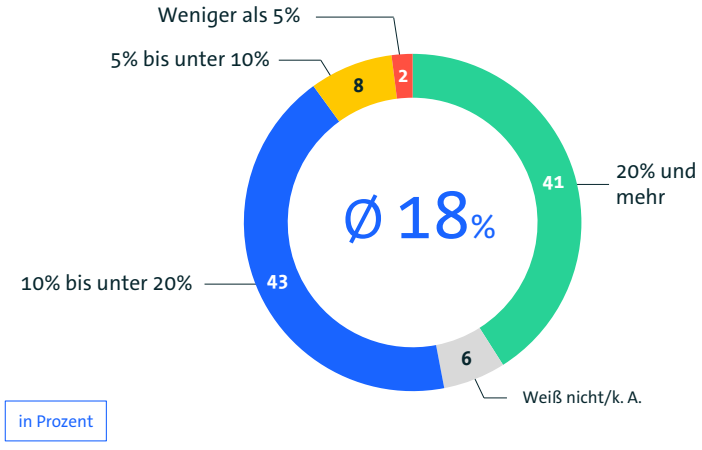
Die Daten zeigen, dass Cybersicherheit mittlerweile einen erheblichen Teil der IT-Ausgaben ausmacht und die Bereitschaft zu investieren stark ausgeprägt ist.

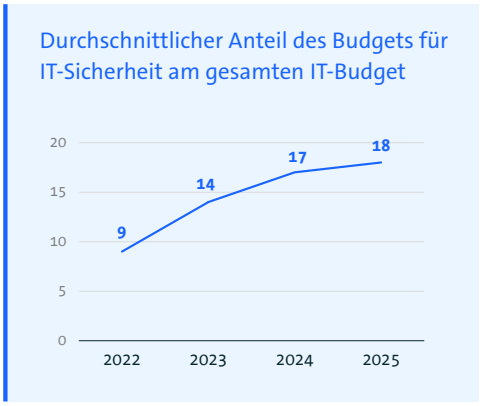
**IT-Sicherheit ist für viele Unternehmen ein relevanter Investitionsbereich:**

**84 Prozent** investieren nach eigener Angabe mindestens zehn Prozent ihres IT-Budgets in Sicherheitsmaßnahmen, davon über 40 Prozent sogar 20 Prozent oder mehr.

# Investitionsbereitschaft in Cybersicherheit steigt

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




Basis: Alle Unternehmen (n=1.002) | Quelle: Bitkom Research 2025

Abbildung 19: Verteilung des geschätzten Anteils des IT-Sicherheitsbudgets am Gesamt-IT-Budget

## 5.3 IT-Sicherheitsschulungen

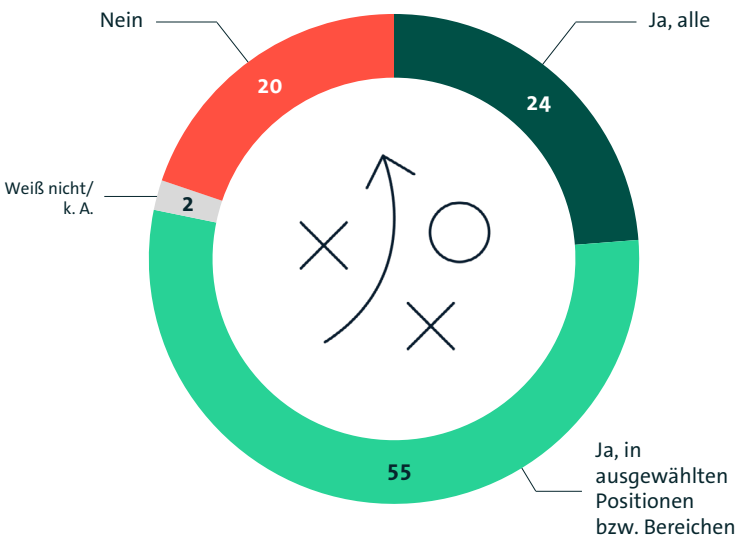
Die Mehrheit der Unternehmen führt regelmäßige Schulungen zu IT-Sicherheitsthemen wie Phishing oder Social Engineering durch, allerdings nicht flächendeckend: 55 Prozent schulen Mitarbeitende nur in ausgewählten Bereichen oder Positionen. Weitere 24 Prozent bieten solche Schulungen für alle Beschäftigten an.

20 Prozent der Unternehmen verzichten komplett auf IT-Sicherheitsschulungen.

Es zeigt sich also, dass zwar ein großer Teil der Unternehmen Sensibilisierungsmaßnahmen umsetzt, der vollständige Einbezug aller Mitarbeitenden jedoch eher die Ausnahme bleibt.

Die Umsetzung von Schulungen zu IT-Sicherheitsrisiken hängt oft von Funktionen und Zuständigkeiten im Unternehmen ab, **eine flächendeckende Schulung aller Beschäftigten ist eher die Ausnahme.**

**Schulen** Sie Ihre Mitarbeiterinnen und Mitarbeiter regelmäßig zu IT-Sicherheitsfragen, also etwa zum Erkennen von mit Phishing-Mails oder Social Engineering?




in Prozent

Basis: Alle Unternehmen (n=1.002) | Abweichungen von 100 Prozent sind rundungsbedingt | Quelle: Bitkom Research 2025

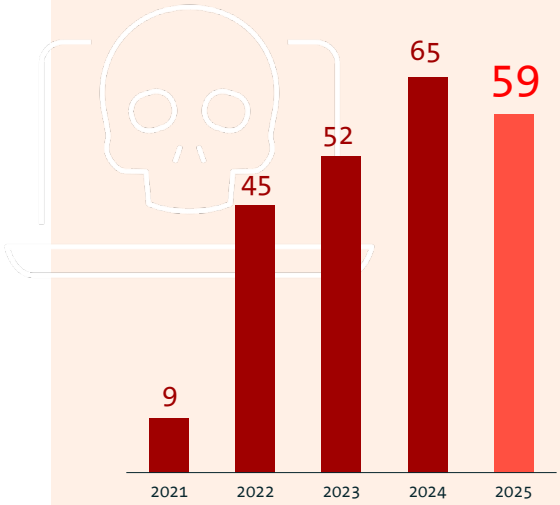
Abbildung 20: Anteil der Unternehmen mit regelmäßigen Schulungen zu IT-Sicherheitsfragen

## 5.4 Wahrnehmung von Risiken durch Cyberattacken

Inwieweit treffen die folgenden Aussagen zu?

**50%** (2024: 53%)

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




in Prozent

Basis: Alle Unternehmen (n=1.003) | Prozentwerte für »Trifft voll und ganz zu« und »Trifft eher zu« | Quelle: Bitkom Research 2025

Abbildung 21: Anteil der Unternehmen, die sich sehr gut auf Cyberangriffe vorbereitet sehen bzw. diese als existenzielle Bedrohung einstufen

Der Anteil der Unternehmen, die Cyberangriffe als existenzielle Bedrohung einstufen, ist in den vergangenen Jahren deutlich gestiegen: Während 2021 nur 9 Prozent diese Aussage teilten, liegt der Wert im Jahr 2025 bei 59 Prozent. Den bisherigen Höchststand erreichte er im Jahr 2024 mit 65 Prozent.

Gleichzeitig sehen sich aktuell 50 Prozent der Unternehmen sehr gut auf Cyberangriffe vorbereitet.

Damit zeigt sich eine zunehmende Diskrepanz zwischen dem eigenen Sicherheitsgefühl und der als hoch eingeschätzten Bedrohungslage. Trotz vergleichsweise stabiler Vorbereitung wächst in vielen Unternehmen die Sorge vor den möglichen Auswirkungen von Cyberattacken.

59 Prozent der befragten Unternehmen halten Cyberattacken derzeit für **existenzbedrohend**.

# 6 Weltlage & Digitale Souveränität

# 6 Weltlage & Digitale Souveränität

Cybersicherheit ist längst geopolitisch geworden: In einer zunehmend angespannten Weltlage wird digitale Souveränität zur Voraussetzung dafür, technologische Abhängigkeiten zu verringern und die eigene Handlungsfähigkeit zu bewahren. Unternehmen fordern mehr Eigenständigkeit bei Sicherheitslösungen, während zugleich das Vertrauen in internationale Partner schwindet. Wie gut ist Deutschland aus Sicht der Unternehmen vorbereitet?

## 6.1 Positionen zu Cybersicherheit

Die Mehrheit der befragten Unternehmen sieht einen deutlichen Handlungsbedarf beim Schutz vor Cyberangriffen: So sind 78 Prozent der Meinung, dass Deutschland in der Lage sein muss, sich im digitalen Raum verteidigen zu können. Etwas mehr als die Hälfte (53 Prozent) fordert zudem eine deutliche Erhöhung der Ausgaben für Cybersicherheit. 44 Prozent betonen, dass Deutschland selbst in der Lage sein sollte, Cyberangriffe durchzuführen. Demgegenüber halten nur 40 Prozent das Land für gut vorbereitet auf großflächige Cyberangriffe.

Die Ergebnisse zeigen, dass insbesondere die Fähigkeit zur digitalen Selbstverteidigung als vorrangig angesehen wird und vergleichsweise weniger Unternehmen Deutschland bereits jetzt als ausreichend geschützt betrachten.

> **»Deutschland muss sich im digitalen Raum verteidigen können«** – darin sind sich die meisten der befragten Unternehmen einig.

### Cyberkrieg: Deutschland muss sich besser vorbereiten

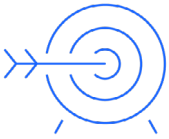
Welche der Aussagen treffen Ihrer Meinung nach zu?

78%

Deutschland muss sich im digitalen Raum **verteidigen können**.

53%

Deutschland muss die **Ausgaben** für Cybersicherheit massiv **erhöhen**.



44%

Deutschland muss in der Lage sein, selbst **Cyberangriffe durchführen** zu können.

40%

Deutschland ist auf **großflächige Cyberangriffe** gut vorbereitet.

Basis: Alle Unternehmen (n=1.002) | Quelle: Bitkom Research 2025

Abbildung 22: Positionen von Unternehmen zur Vorbereitung Deutschlands auf Cyberangriffe

## 6.2 Digitale Souveränität

Digitale Souveränität gewinnt für Unternehmen sichtbar an Bedeutung. Zwei Drittel (67 Prozent) der befragten Unternehmen geben an, bei Sicherheitslösungen von Anbietern aus den USA abhängig zu sein.

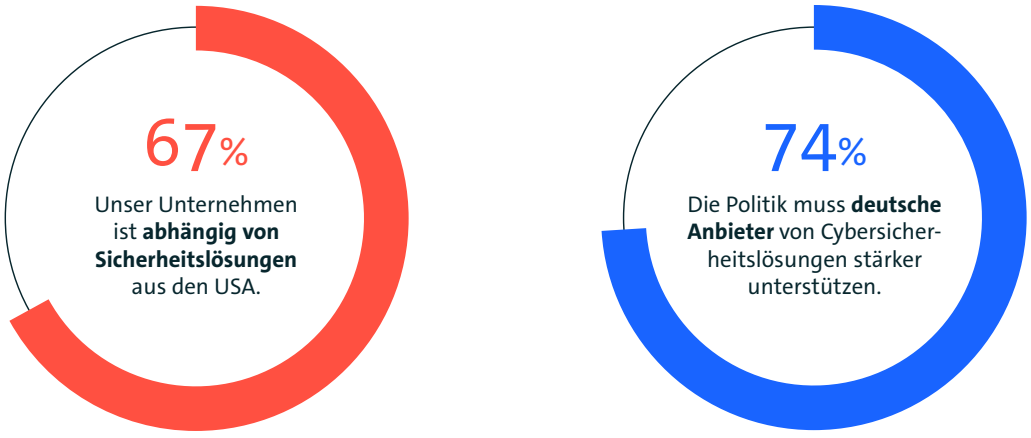
Gleichzeitig fordern 74 Prozent, dass die Politik deutsche Anbieter von Cybersicherheitslösungen stärker unterstützt.

Die Ergebnisse zeigen eine Spannung zwischen aktueller Abhängigkeit und dem Wunsch nach mehr Unabhängigkeit im Bereich der digitalen Sicherheit.

**Wirtschaftsschutz und digitale Souveränität gehören zusammen, das zeigt der Blick auf die Realität vieler Unternehmen:** Zwei von drei Unternehmen sehen sich bei Sicherheitslösungen in Abhängigkeit von Anbietern aus den USA.

### Digitale Souveränität rückt in den Fokus

Welche der Aussagen treffen Ihrer Meinung nach bzw. auf Ihr Unternehmen zu?




Basis: Alle Unternehmen (n=1.002) | Quelle: Bitkom Research 2025

Abbildung 23: Unternehmen zu Deutschlands Abhängigkeit von Cybersicherheitslösungen

## 6.3 Einschätzung zur US-Sicherheitspolitik

Eine wachsende Zahl von deutschen Unternehmen betrachtet die USA nicht mehr uneingeschränkt als vertrauenswürdigen Partner im Bereich der Cybersicherheit: So geben 66 Prozent an, dass sich Deutschland verstärkt vor Cyberangriffen aus den USA schützen müsse. 54 Prozent vermuten, dass die USA ihre wirtschaftlichen Interessen auch mithilfe von Cyberangriffen oder Cyberspionage durchsetzen würden. Zudem sagen 53 Prozent der Unternehmen, die USA entwickelten sich von einem Partner zu einer Bedrohung für die deutsche Sicherheit.

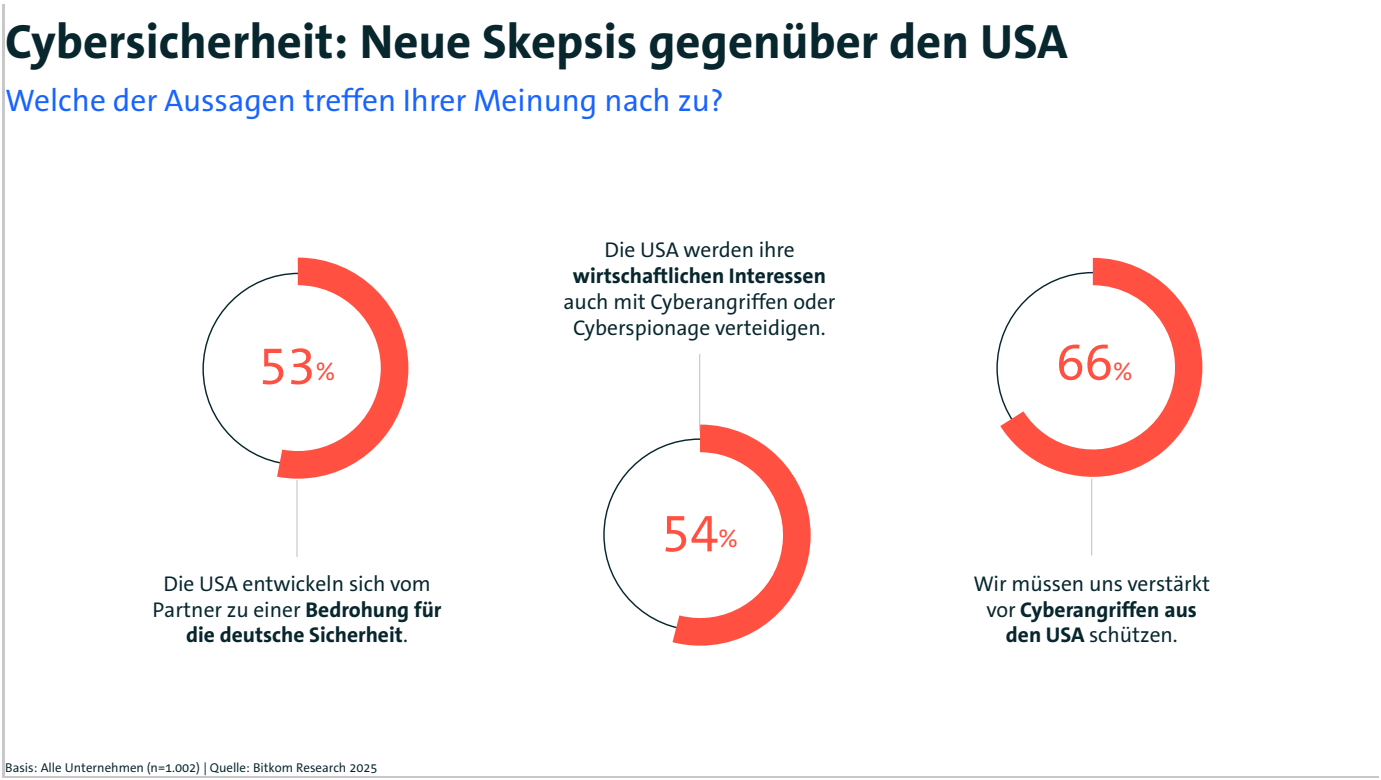



Abbildung 24: Einschätzungen deutscher Unternehmen zur Cybersicherheitsbedrohung durch die USA

»IT-Sicherheit ist kein Zustand, IT-Sicherheit ist ein Prozess und ihn müssen wir aktiv betreiben. Der Schutz gegen Cyberangriffe gehört mit ins Zentrum einer Strategie für ein sicheres und digital souveränes Deutschland«, so Bitkom-Präsident Ralf Wintergerst.

# 7 Fazit

Die Studie Wirtschaftsschutz 2025 zeigt eindrücklich, wie stark die deutsche Wirtschaft unter dem wachsenden Druck von Spionage, Sabotage und Datendiebstahl steht: **87 Prozent** der Unternehmen waren in den vergangenen zwölf Monaten betroffen oder vermuten Angriffe. Der entstandene Schaden erreicht mit **289,2 Milliarden Euro** einen neuen Höchststand, davon entfallen **70 Prozent** auf Cyberattacken.

Die Bedrohung ist internationaler und professioneller geworden: **Russland und China** gelten mit jeweils **46 Prozent** als Hauptquellen von Angriffen, und **28 Prozent** der Unternehmen berichten von Attacken ausländischer Nachrichtendienste – viermal so viele wie noch 2023. Zugleich verbessert sich die Zusammenarbeit zwischen Wirtschaft und Behörden und immer mehr Unternehmen erhalten Hinweise von Sicherheitsbehörden.

Trotz gestiegener Investitionen in IT-Sicherheit, Notfallmanagement und Schulungen – das Sicherheitsbudget liegt im Schnitt bei **18 Prozent** – sind die Sorgen groß. **59 Prozent** der Unternehmen sehen Cyberangriffe weiterhin als existenzielle Bedrohung. Unternehmen reagieren zwar, doch das Bedrohungsniveau wächst schneller als ihre Schutzmaßnahmen.

**Bitkom-Präsident Dr. Ralf Wintergerst** betont:

«Ein umfassender Schutz muss essenzieller Bestandteil der Digitalisierung von Unternehmen sein. Die Frage ist nicht, ob Unternehmen angegriffen werden, sondern wann – und ob sie diese Angriffe erfolgreich abwehren können.»
↗ Bundesamt für Verfassungsschutz

Zugleich wird auch deutlich, dass Digitale Souveränität immer stärker zur sicherheitspolitischen Aufgabe wird. **Zwei Drittel der Unternehmen** sehen sich zu abhängig von US-Anbietern, drei Viertel fordern politische Unterstützung für deutsche Sicherheitslösungen. Cybersicherheit gehört ins Zentrum der Politik für ein digital souveränes Deutschland, als gemeinsame Verantwortung von Unternehmen, Staat und Sicherheitsbehörden.

↗ Mehr hierzu in der Presseinformation «Angriffe auf die deutsche Wirtschaft nehmen zu»

# 8 Methodik

## Befragung 2025

| Auftraggeber | Bitkom |
|---|---|
| **Methodik** | Computergestützte telefonische Befragung/ Computer Assisted Telephone Interview (CATI) |
| **Grundgesamtheit** | Unternehmen in Deutschland mit mindestens 10 Beschäftigten und einem Jahresumsatz von 1 Mio. Euro oder mehr |
| **Zielpersonen** | Führungskräfte, die für das Thema Wirtschaftsschutz verantwortlich sind. Dazu zählen Geschäftsführer und vor allem Führungskräfte aus den Bereich IT |
| **Stichprobengröße** | n=1.002 |
| **Befragungszeitraum** | KW 16 bis KW 24 2025 |
| **Statistische Fehlertoleranz** | +/- 3 Prozent in der Gesamtstichprobe |

Herausgeber
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Fachliche Leitung
Felix Kuhlenkamp

Wissenschaftliche Leitung
Bettina Lange

Redaktion
Alissa Geffert



DOI
10.64022/2025-wirtschaftsschutz

Seit 2015 untersucht der Digitalverband Bitkom jährlich, wie es um den Wirtschaftsschutz in Deutschland steht. Die Wirtschaftsschutzstudie 2025 zeigt erneut eine alarmierende Entwicklung: 87 Prozent der Unternehmen waren in den vergangenen zwölf Monaten von Datendiebstahl, Spionage oder Sabotage betroffen. Der dabei entstandene Schaden beläuft sich auf 289,2 Milliarden Euro. Besonders häufig werden Angriffe Russland und China zugeordnet – jeweils 46 Prozent der betroffenen Unternehmen berichten von Vorfällen aus diesen Ländern. Zugleich rücken ausländische Geheimdienste stärker in den Fokus, und immer mehr Unternehmen kooperieren mit Behörden bei der Aufklärung.

DOI
10.64022/2025-wirtschaftsschutz

bitkom