Wirtschaftsschutz 2026

Lagebild der deutschen Wirtschaft

bitkom

Wirtschaftsschutz 2026

Lagebild der deutschen Wirtschaft

Bitkom-Dataverse

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

Zum Bitkom-Dataverse

Zu den Studienberichten

DOI
10.64022/2026-wirtschaftsschutz

Executive Summary

Seit 2015 untersucht der Digitalverband Bitkom jährlich, wie es um den Wirtschaftsschutz in Deutschland steht. Die jüngsten mutmaßlichen Sabotageversuche auf Umspannwerke und andere Teile der Strominfrastruktur zeigen, wie verwundbar zentrale Strukturen gegenüber physischen – und digitalen – Angriffen sein können. Für Unternehmen stellt sich damit dringlich die Frage: Wie sicher ist die deutsche Wirtschaft im Jahr 2026?

Dieser Studienbericht untersucht die Bedrohung durch Datendiebstahl, Industriespionage, Sabotage und Cyberangriffe. Wie viele Unternehmen sind betroffen? Welche Täter und Herkunftsregionen spielen eine Rolle? Welche Schäden entstehen und wie verändern sich die Angriffsmuster durch Künstliche Intelligenz? Auch geht es um die Frage, wie gut Unternehmen vorbereitet sind und wie viel sie in IT-Sicherheit investieren. Grundlage des Studienberichts ist eine repräsentative Befragung von 1.003 Unternehmen in Deutschland mit mindestens 10 Beschäftigten und einem Jahresumsatz von mindestens 1 Million Euro, die Bitkom Research im Auftrag des Bitkom durchgeführt hat.

Zentrale Ergebnisse:

- **Fast alle Unternehmen sind von Diebstahl, Industriespionage oder Sabotage betroffen oder vermuten entsprechende Vorfälle**
  96 Prozent waren in den vergangenen zwölf Monaten von Diebstahl, Industriespionage oder Sabotage betroffen oder vermuten entsprechende Vorfälle. Auffällig ist das wachsende Dunkelfeld: 67 Prozent geben an, sicher betroffen gewesen zu sein; weitere 29 Prozent vermuten eine Betroffenheit.
- **Die Schäden bleiben im dreistelligen Milliardenbereich**
  Für 2026 ergibt sich ein Schadenskorridor von 211 bis 270,8 Milliarden Euro. Die Obergrenze basiert dabei auf der Annahme von 10 Prozent vermutlich betroffenen Unternehmen.
- **Cyberattacken verursachen drei Viertel der Schäden**
  76 Prozent des Gesamtschadens entfallen inzwischen auf Cyberangriffe. Das entspricht 160,4 bis 205,8 Milliarden Euro. 2021 lag der Cyberanteil noch bei 59 Prozent.
- **Ausländische Nachrichtendienste gewinnen als Tätergruppe an Bedeutung**
  37 Prozent der betroffenen Unternehmen konnten mindestens einen Vorfall einem ausländischen Nachrichtendienst zuordnen. 2023 waren es erst 7 Prozent. Organisierte Kriminalität und Banden bleiben mit 62 Prozent die am häufigsten genannte Tätergruppe.
- **China und Russland werden besonders häufig als Herkunft genannt**
  52 Prozent der betroffenen Unternehmen konnten mindestens einen Angriff China zuordnen, 49 Prozent Russland.
- **Künstliche Intelligenz verändert das Angriffsgeschehen**
  82 Prozent der Unternehmen gehen sicher oder vermutlich davon aus, dass Cyberangreifer verstärkt KI einsetzen.
- **Investitionen stagnieren, Wunsch nach digitaler Souveränität ist groß**
  Im Durchschnitt fließen 18 Prozent des IT-Budgets in IT-Sicherheit. Zugleich sehen sich 59 Prozent der Unternehmen von Sicherheitslösungen aus den USA abhängig, 70 Prozent plädieren dafür, stärker auf deutsche und europäische Lösungen zu setzen.

Inhalt

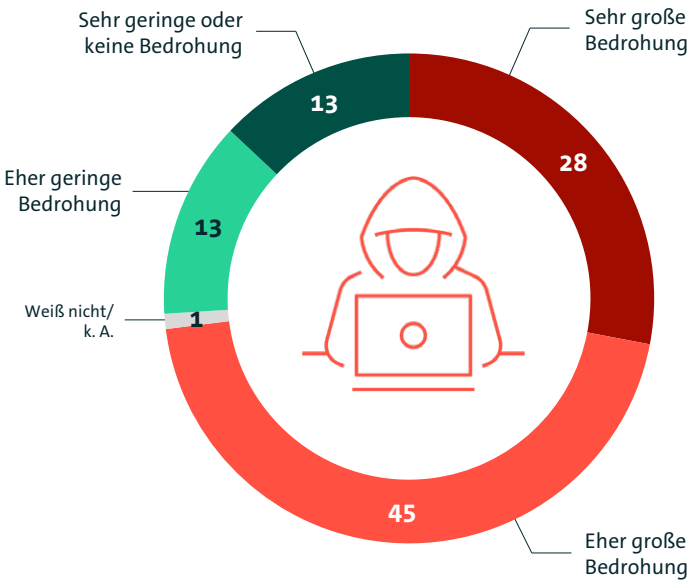
Abbildungen

1 Bedrohungslage und Betroffenheit

1 Bedrohungslage und Betroffenheit

1.1 Wahrgenommene Bedrohung durch analoge und digitale Angriffe

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



in Prozent

Basis: Alle befragten Unternehmen ab 10 Beschäftigten (n=1.003) | Quelle: Bitkom Research 2026

Abbildung 1: Bedrohungswahrnehmung der Unternehmen durch analoge und digitale Angriffe wie Datendiebstahl, Industriespionage und Sabotage

Analoge und digitale Angriffe: Drei Viertel der Unternehmen fühlen sich stark bedroht

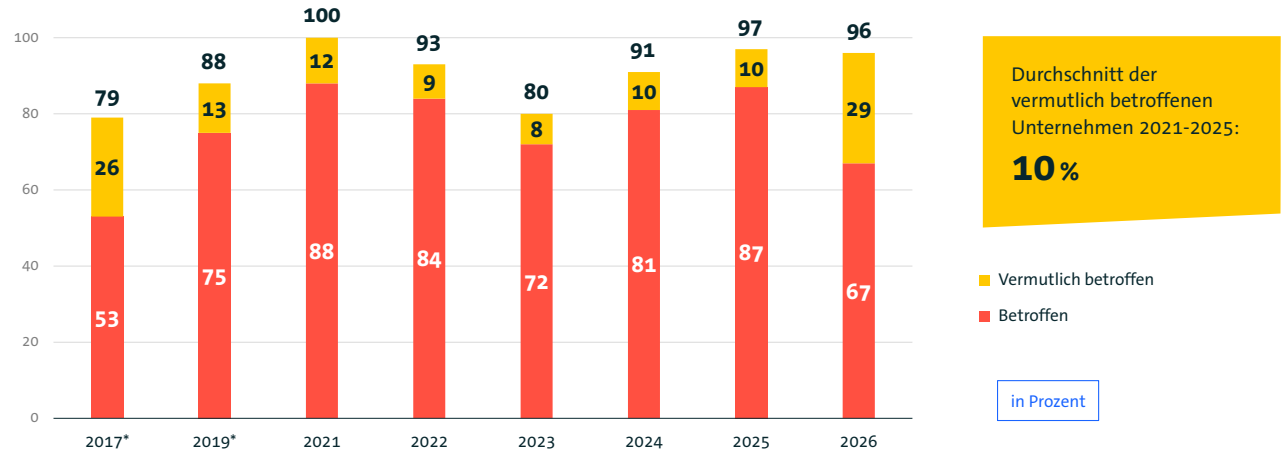
Die Bedrohung durch analoge und digitale Angriffe wird von der großen Mehrheit der Unternehmen weiterhin als hoch eingeschätzt. 2026 sehen **73 Prozent** in Datendiebstahl, Industriespionage und Sabotage eine große Bedrohung für ihr Unternehmen, davon 28 Prozent eine sehr große und 45 Prozent eine eher große.

Im Vorjahr lag dieser Anteil mit 72 Prozent auf einem ähnlich hohen Niveau: 33 Prozent sahen eine sehr große und 39 Prozent eine eher große Bedrohung ↗Dataverse.

Damit bleibt die Bedrohungswahrnehmung hoch und nur eine Minderheit stuft die Risiken als gering oder nicht vorhanden ein.

1.2 Betroffenheit durch Diebstahl, Industriespionage und Sabotage

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



Basis: Alle befragten Unternehmen ab 10 Beschäftigten (n=1.003) | * 2017 und 2019 »innerhalb der letzten zwei Jahre« | Quelle: Bitkom Research 2026

Abbildung 2: Betroffenheit der Unternehmen durch Diebstahl, Industriespionage und Sabotage im Zeitvergleich

Fast jedes Unternehmen ist (vermutlich) betroffen

Fast alle Unternehmen in Deutschland waren 2026 von Diebstahl, Industriespionage oder Sabotage betroffen oder vermuten zumindest einen entsprechenden Vorfall. Insgesamt liegt dieser Anteil bei **96 Prozent**.

Dabei geben 67 Prozent an, tatsächlich betroffen gewesen zu sein, weitere 29 Prozent vermuten eine Betroffenheit. Auffällig ist hier vor allem die Verschiebung gegenüber dem Vorjahr: 2025 waren 87 Prozent sicher betroffen und nur 10 Prozent vermutlich betroffen. Der Anteil der lediglich vermuteten Fälle liegt 2026 somit deutlich über dem Durchschnitt der Jahre 2021 bis 2025 von 10 Prozent.

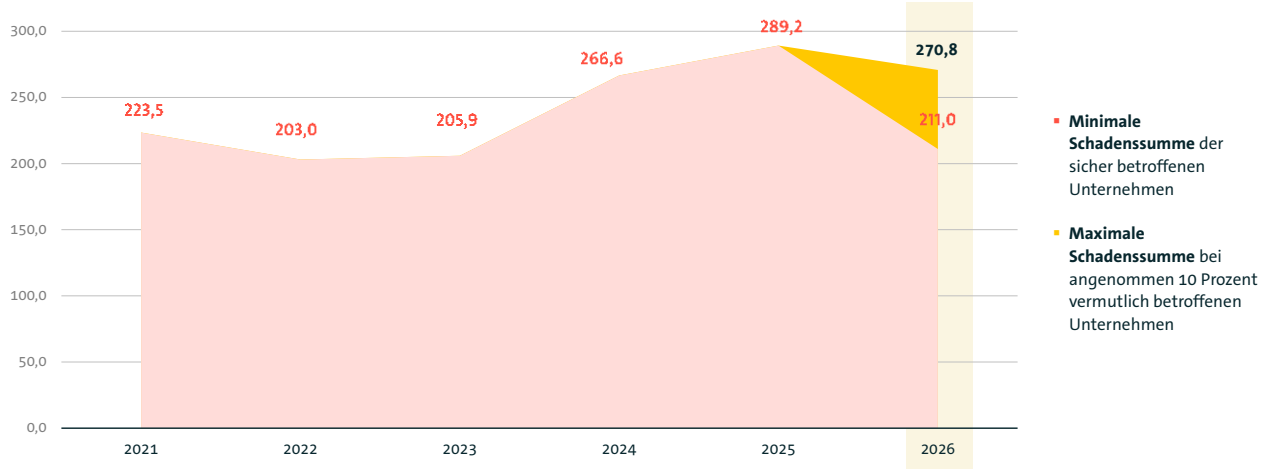
Damit bleibt die Betroffenheit insgesamt auf sehr hohem Niveau und gleichzeitig ist die Unsicherheit über konkrete Vorfälle deutlich gestiegen.

2 Schäden durch Diebstahl, Industriespionage und Sabotage

2 Schäden durch Diebstahl, Industriespionage und Sabotage

2.1 Entwicklung der Schadenssumme

Schadenssumme 2021 bis 2026



Basis: Alle befragten Unternehmen ab 10 Beschäftigten (n=1.003) | Quelle: Bitkom Research 2026

Abbildung 3: Entwicklung der Schadenssumme durch Diebstahl, Industriespionage und Sabotage von 2021 bis 2026

Für 2026 ergibt sich ein Korridor zwischen 211 und 270,8 Milliarden Euro

Die Schäden durch Diebstahl, Industriespionage und Sabotage bleiben auch 2026 auf einem hohen Niveau. Allein bei den Unternehmen, die sicher von einem Vorfall betroffen waren, summieren sich die Schäden auf **211 Milliarden Euro.**

Die Obergrenze von 270,8 Milliarden Euro basiert auf der Annahme eines Anteils von 10 Prozent vermutlich betroffener Unternehmen. Aufgrund des ungewöhnlich hohen Anteils vermutlich betroffener Unternehmen wird für 2026 erstmals ein Schadenskorridor ausgewiesen.

Im Vorjahr hatte die Schadenssumme mit 289,2 Milliarden Euro einen Höchststand erreicht, 2024 waren es 266,6 Milliarden Euro. Damit bewegt sich die Schadenssumme im Jahr 2026 weiterhin in einer Größenordnung von mehreren hundert Milliarden Euro.

2.2 Zusammensetzung der wirtschaftlichen Schäden

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

	Schadenssummen in Mrd. Euro		
Schaden durch...	2026	2025	2024
Umsatzeinbußen durch nachgemachte Produkte bzw. Plagiate	38,9	30,6	39,2
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	36,5	73,3	54,5
Kosten für Ermittlungen und Ersatzmaßnahmen	35,6	37,0	32,2
Kosten für Rechtsstreitigkeiten	34,9	53,0	53,1
Imageschaden bei Kunden oder Lieferanten, Negative Medienberichterstattung	21,1	15,9	20,2
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	18,2	23,1	11,2
Datenschutzrechtliche Maßnahmen, z. B. durch Behörden	11,5	23,8	27,2
Geldabfluss durch Betrugsversuche	8,4	0,9	0,8
Erpressung mit gestohlenen Daten	5,0	15,6	13,4
Patentrechtsverletzungen, auch vor Anmeldung	0,9	16,0	14,8
Sonstige Schäden	0	0	0
Gesamtschaden pro Jahr	211,0	289,2	266,6

Basis: Alle befragten Unternehmen ab 10 Beschäftigten (n=1.003) | Mehrfachnennungen möglich | Rundungsbedingt kann die Summe der Einzelschäden vom Gesamtschaden abweichen |
Quelle: Bitkom Research 2026

Abbildung 4: Zusammensetzung der Schäden durch Diebstahl, Industriespionage und Sabotage im Jahresvergleich

Mindestens 211 Milliarden Euro Schaden in Deutschland

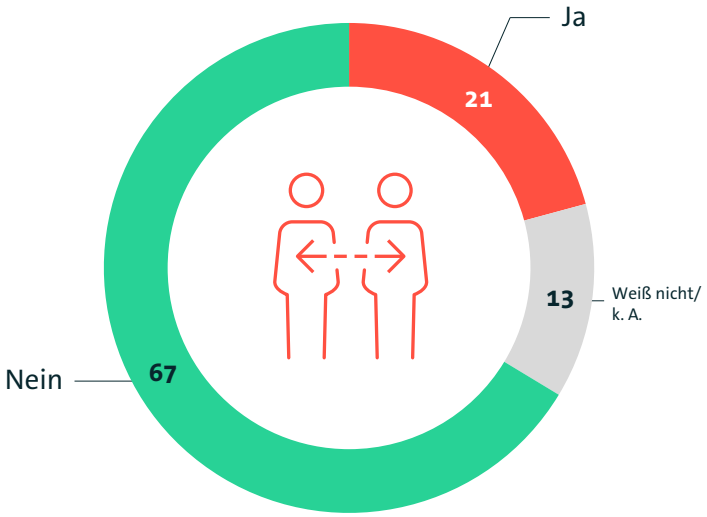
Die wirtschaftlichen Folgen von Diebstahl, Industriespionage und Sabotage verteilen sich auf sehr unterschiedliche Schadensarten. 2026 entstehen die größten Einbußen durch nachgemachte Produkte und Plagiate mit **38,9 Milliarden Euro**. Dahinter folgen Schäden durch den Ausfall, Diebstahl oder die Schädigung von Informations- und Produktionssystemen beziehungsweise Betriebsabläufen mit 36,5 Milliarden Euro sowie Kosten für Ermittlungen und Ersatzmaßnahmen mit 35,6 Milliarden Euro.

Im Vergleich zum Vorjahr haben sich einzelne Schadenspositionen verschoben: So sind die Schäden durch beeinträchtigte Informations- und Produktionssysteme von 73,3 auf 36,5 Milliarden Euro und die Kosten für Rechtsstreitigkeiten von 53 auf 34,9 Milliarden Euro zurückgegangen.

Gleichzeitig stiegen die Umsatzeinbußen durch Plagiate von 30,6 auf 38,9 Milliarden Euro sowie der Geldabfluss durch Betrugsversuche von 0,9 auf 8,4 Milliarden Euro. Insgesamt summieren sich die Schäden der sicher betroffenen Unternehmen 2026 auf mindestens **211 Milliarden Euro**.

2.3 Auswirkungen auf andere Unternehmen

Hatte Ihr Schaden Auswirkungen auf andere Unternehmen, etwa Produktionsausfälle bei Geschäftspartnern oder Reputationsschäden für Auftraggeber?



in Prozent

Basis: Befragte Unternehmen ab 10 Beschäftigten, die in den letzten 12 Monaten von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=671) | Abweichungen von 100 Prozent sind rundungsbedingt | Quelle: Bitkom Research 2026

Abbildung 5: Auswirkungen von Schäden auf Geschäftspartner und andere Unternehmen

Bei jedem fünften betroffenen Unternehmen hat der Schaden Folgen für Dritte

Ein Angriff bleibt häufig nicht auf das unmittelbar betroffene Unternehmen beschränkt: **21 Prozent** der Unternehmen, die von Datendiebstahl, Industriespionage oder Sabotage betroffen waren, berichten von Auswirkungen auf andere Unternehmen – etwa durch Produktionsausfälle bei Geschäftspartnern oder Reputationsschäden bei Auftraggebern.

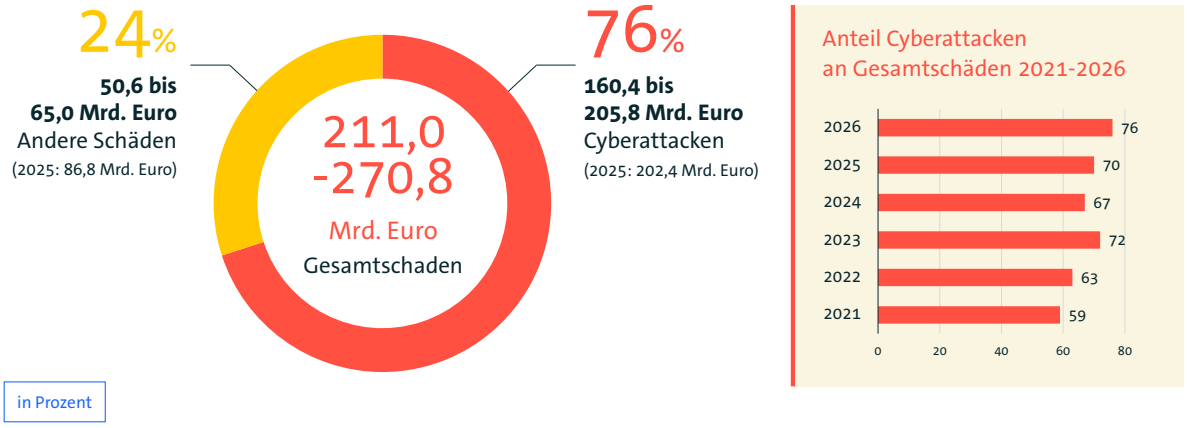
67 Prozent geben an, dass der Vorfall keine Folgen für Dritte hatte, 13 Prozent können oder wollen dazu keine Angabe machen.

»Wer die eigenen Schutzmaßnahmen vernachlässigt, gefährdet andere. Wer sein Unternehmen schützen will, muss physische und digitale Sicherheit gemeinsam angehen und sollte auch seine Partner in die Pflicht nehmen.«

Bitkom-Präsident Dr. Ralf Wintergerst ↗Presseinformation

2.4 Schäden durch Cyberangriffe

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



Basis: Befragte Unternehmen ab 10 Beschäftigten, die in den letzten 12 Monaten von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=671) | Quelle: Bitkom Research 2026

Abbildung 6: Anteil der Cyberattacken am Gesamtschaden im Zeitvergleich

Cyberattacken verursachen drei Viertel der Schäden

Cyberattacken verursachen inzwischen den größten Teil der wirtschaftlichen Schäden durch Datendiebstahl, Industriespionage und Sabotage. 2026 entfallen **76 Prozent** des Gesamtschadens auf Cyberattacken – das entspricht 160,4 bis 205,8 Milliarden Euro. Im Vorjahr lag der Anteil noch bei 70 Prozent, 2021 bei 59 Prozent. Damit ist der Anteil der Cyberattacken am Gesamtschaden über die vergangenen Jahre deutlich gestiegen.

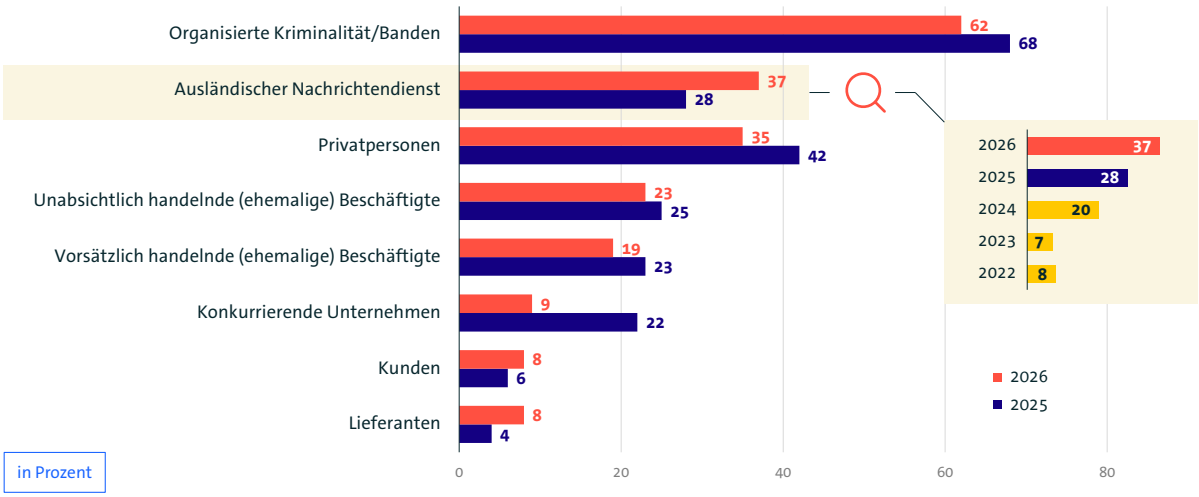
Auf andere Schadensursachen entfallen 2026 noch 24 Prozent beziehungsweise 50,6 bis 65 Milliarden Euro. Im Vorjahr waren es 86,8 Milliarden Euro.

3 Täterkreise und Herkunft der Angriffe

3 Täterkreise und Herkunft der Angriffe

3.1 Täterkreise

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



Basis: Befragte Unternehmen ab 10 Beschäftigten, die in den letzten 12 Monaten von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=671) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2026

Abbildung 7: Täterkreise bei Diebstahl, Industriespionage und Sabotage im Jahresvergleich

Hinter Angriffen stecken immer öfter Geheimdienste

Die Organisierte Kriminalität bleibt der am häufigsten genannte Täterkreis: **62 Prozent** der betroffenen Unternehmen konnten 2026 mindestens einen Angriff organisierten kriminellen Strukturen oder Banden zuordnen. Gegenüber dem Vorjahr mit 68 Prozent ist der Anteil allerdings leicht gesunken. Deutlich häufiger führen die Spuren dagegen zu ausländischen Nachrichtendiensten. Ihr Anteil steigt binnen eines Jahres von 28 auf **37 Prozent** – 2023 waren es erst 7 Prozent. Damit haben sich die Nennungen innerhalb von drei Jahren mehr als verfünffacht.

Rückläufig sind die Nennungen bei Privatpersonen (35 Prozent nach 42 Prozent) und insbesondere bei konkurrierenden Unternehmen (9 Prozent nach 22 Prozent).

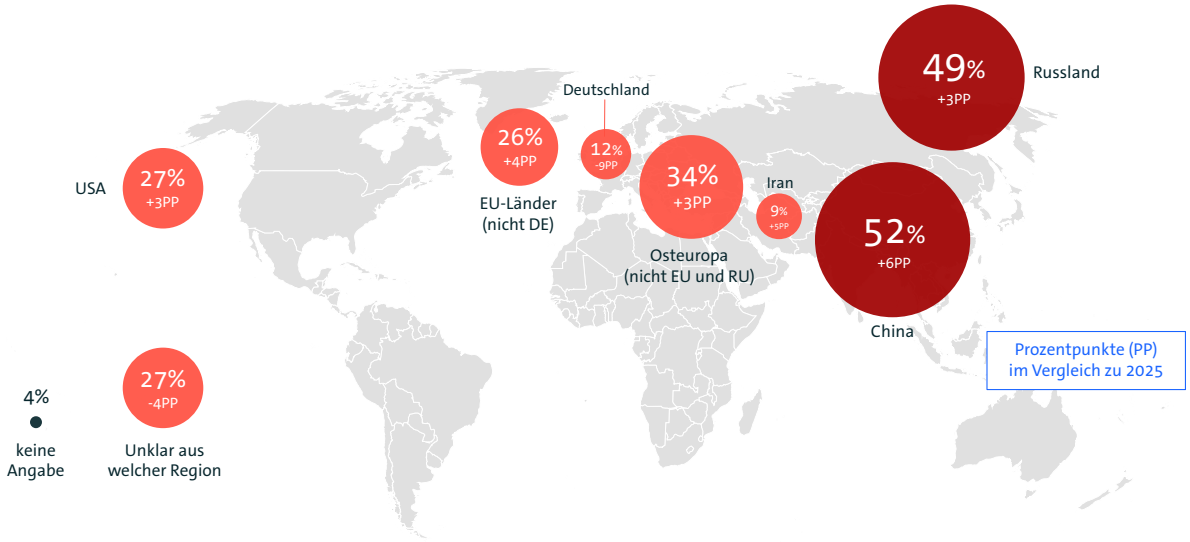
Aktuelle oder ehemalige Beschäftigte werden ebenfalls seltener als Täter genannt: 23 Prozent der Unternehmen berichten von unabsichtlichem und 19 Prozent von vorsätzlichem Handeln.

»Die Grenzen zwischen Organisierter Kriminalität und den Geheimdiensten sind in vielen Ländern fließend. Nachrichtendienste bedienen sich krimineller Strukturen, umgekehrt wird Kriminellen freie Hand gelassen, solange sie ihre Ziele den politischen Vorgaben entsprechend wählen.«

Bitkom-Präsident Dr. Ralf Wintergerst ↗Presseinformation

3.2 Herkunftsregionen der Angriffe

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



Basis: Befragte Unternehmen ab 10 Beschäftigten, die in den letzten 12 Monaten von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=671) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2026

Abbildung 8: Herkunftsregionen von Angriffen durch Diebstahl, Industriespionage und Sabotage

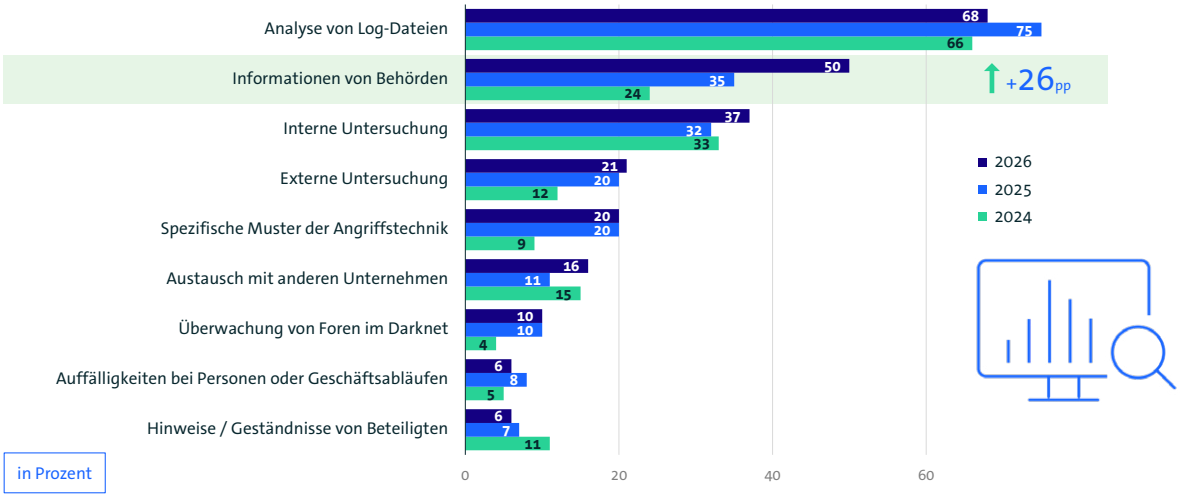
Bedrohung aus China und Russland wächst weiter

Die Spuren von Angriffen auf deutsche Unternehmen führen besonders häufig nach China und Russland – und bei beiden Ländern nimmt die Bedeutung weiter zu. **52 Prozent** der betroffenen Unternehmen konnten 2026 mindestens einen Angriff nach China zurückverfolgen, 6 Prozentpunkte mehr als im Vorjahr. Russland folgt mit **49 Prozent** und einem Plus von 3 Prozentpunkten. An dritter Stelle steht Osteuropa außerhalb von EU und Russland mit 34 Prozent.

Auch die USA werden mit 27 Prozent häufiger als Herkunftsregion genannt als im Vorjahr. Besonders deutlich fällt der Anstieg beim Iran aus: Der Anteil hat sich von 4 auf 9 Prozent mehr als verdoppelt. Gleichzeitig können 27 Prozent der Unternehmen Angriffe keiner bestimmten Region zuordnen.

3.3 Grundlage der Erkenntnisse zu Tätern und Herkunft

Auf welcher Grundlage haben Sie die Erkenntnisse erlangt?



Basis: Befragte Unternehmen ab 10 Beschäftigten, die in den letzten 12 Monaten von Datendiebstahl, Industriespionage oder Sabotage betroffen waren und Erkenntnisse über Herkunft oder Täterkreis hatten (n=667) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2026

Abbildung 9: Informationsquellen zur Zuordnung von Herkunft und Täterkreis von Angriffen

Behörden liefern wichtige Hinweise auf Täter

Bei der Aufklärung von Angriffen gewinnen Informationen von Behörden deutlich an Bedeutung. Jedes zweite Unternehmen (**50 Prozent**), das Erkenntnisse über Herkunft oder Täterkreis eines Angriffs gewinnen konnte, erhielt 2026 entsprechende Hinweise von Behörden. 2025 waren es erst 35 Prozent, 2024 sogar nur 24 Prozent – ein Anstieg um 26 Prozentpunkte innerhalb von zwei Jahren.

Wichtigste technische Erkenntnisquelle bleibt die Analyse von Log-Dateien mit **68 Prozent**. Daneben stützen sich Unternehmen auf interne Untersuchungen (37 Prozent), externe Untersuchungen (21 Prozent) und spezifische Muster der Angriffstechnik (20 Prozent).

»Der Austausch zwischen Wirtschaft und staatlichen Stellen funktioniert heute besser als noch vor einigen Jahren. Jetzt müssen wir auf ein gemeinsames Lagebild hinarbeiten, von dem beide Seiten profitieren würden.«

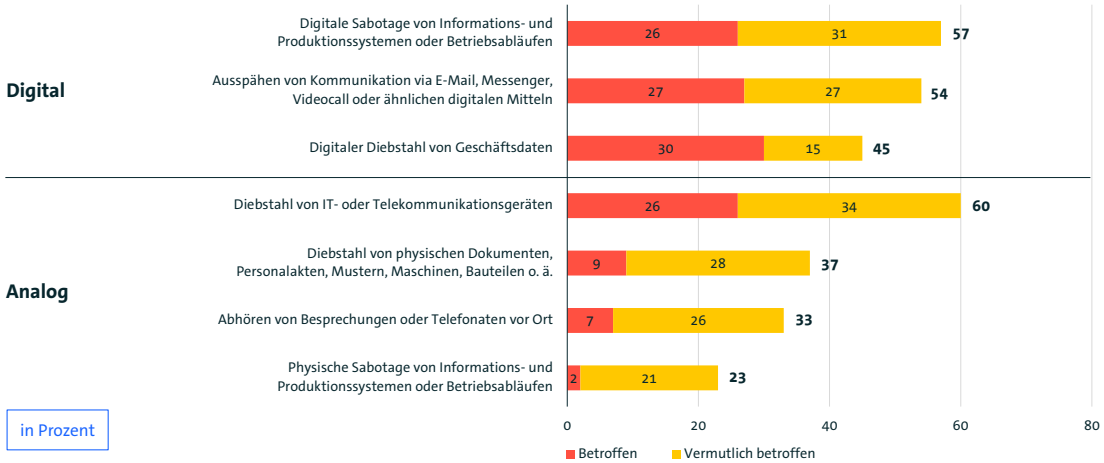
Bitkom-Präsident Dr. Ralf Wintergerst ↗Presseinformation

4 Angriffsformen und Entwicklung von Cyberangriffen

4 Angriffsformen und Entwicklung von Cyberangriffen

4.1 Analoge und digitale Angriffsformen

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



Basis: Alle befragten Unternehmen ab 10 Beschäftigten (n=1.003) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2026

Abbildung 10: Betroffenheit der Unternehmen durch analoge und digitale Angriffsformen

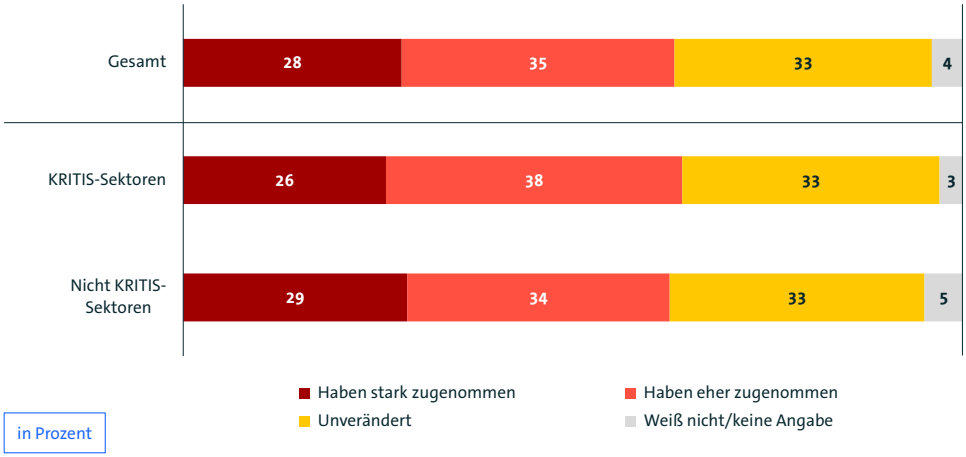
Angriffe auf Unternehmen erfolgen überwiegend digital

Angriffe auf Unternehmen finden auf unterschiedlichen Wegen statt – digitale Angriffsformen sind dabei besonders verbreitet. **57 Prozent** der Unternehmen waren in den vergangenen zwölf Monaten sicher oder vermutlich von digitaler Sabotage ihrer Informations- und Produktionssysteme oder Betriebsabläufe betroffen. **54 Prozent** berichten vom Ausspähen ihrer digitalen Kommunikation, **45 Prozent** vom digitalen Diebstahl von Geschäftsdaten.

Aber auch analoge Angriffswege spielen weiterhin eine Rolle. 60 Prozent der Unternehmen waren sicher oder vermutlich vom Diebstahl von IT- oder Telekommunikationsgeräten betroffen. Beim Diebstahl physischer Dokumente, Personalakten, Muster oder Bauteile sind es 37 Prozent, beim Abhören von Besprechungen oder Telefonaten vor Ort 33 Prozent. Physische Sabotage von Informations- und Produktionssystemen oder Betriebsabläufen wird von 23 Prozent sicher festgestellt oder vermutet.

4.2 Entwicklung der Cyberangriffe

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



Basis: Alle befragten Unternehmen ab 10 Beschäftigten (n=1.003) | Abweichungen von 100 Prozent sind rundungsbedingt | Quelle: Bitkom Research 2026

Abbildung 11: Entwicklung der Anzahl von Cyberattacken auf Unternehmen nach KRITIS-Zugehörigkeit

Cyberangriffe auf Unternehmen nehmen weiter zu

Für die Mehrheit der Unternehmen hat sich der Druck durch Cyberangriffe weiter erhöht. **63 Prozent** berichten, dass die Zahl der Cyberattacken in den vergangenen zwölf Monaten zugenommen hat – bei 28 Prozent stark, bei weiteren 35 Prozent eher. Nur ein Drittel der Unternehmen beobachtet eine unveränderte Zahl von Angriffen.

Dabei zeigen sich kaum Unterschiede zwischen KRITIS-Unternehmen und der übrigen Wirtschaft: In den KRITIS-Sektoren berichten **64 Prozent** von einer Zunahme der Cyberattacken, außerhalb der KRITIS-Sektoren sind es **63 Prozent**. Eine wachsende Zahl von Cyberangriffen betrifft damit Unternehmen unabhängig davon, ob sie zur Kritischen Infrastruktur zählen.

Wie relevant der Schutz Kritischer Infrastrukturen ist, zeigen auch die jüngsten mutmaßlichen Sabotageversuche auf die Strominfrastruktur. Hier treffen physische und digitale Bedrohungen unmittelbar aufeinander: »Dabei geht es nicht nur um physische Angriffe und Sabotage, sondern ebenso um Cyberangriffe.«

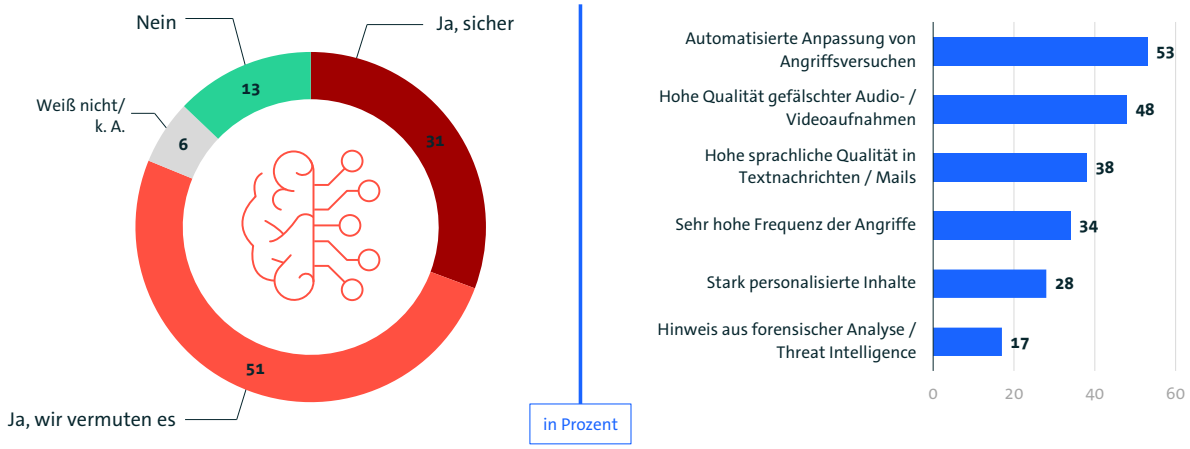
– Bitkom-Hauptgeschäftsführer Dr. Bernhard Rohleder

↗Presseinformation

Digitale Überwachung und robuste Cybersicherheitsmaßnahmen sind daher für den Schutz und stabilen Betrieb der Energieinfrastruktur von zentraler Bedeutung.

4.3 Einsatz Künstlicher Intelligenz bei Cyberangriffen

Stellen Sie fest, dass bei Angriffen auf Ihr Unternehmen verstärkt KI eingesetzt wird? Und woran machen Sie das fest?



Basis (links): Alle befragten Unternehmen ab 10 Beschäftigten (n=1.003) | Abweichungen von 100 Prozent sind rundungsbedingt | Basis (rechts): Befragte Unternehmen ab 10 Beschäftigten, die den verstärkten Einsatz von KI wahrnehmen (n=820) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2026

Abbildung 12: Wahrnehmung und Merkmale des verstärkten KI-Einsatzes bei Cyberangriffen

Cyberangreifer setzen zunehmend auf KI

Der Einsatz Künstlicher Intelligenz wird im Angriffsgeschehen zunehmend sichtbar: **82 Prozent** der Unternehmen gehen davon aus, dass Angreifer verstärkt KI einsetzen. Allerdings sind sich nur 31 Prozent dessen sicher, weitere 51 Prozent vermuten den KI-Einsatz. Lediglich 13 Prozent stellen keinen verstärkten Einsatz von KI fest.

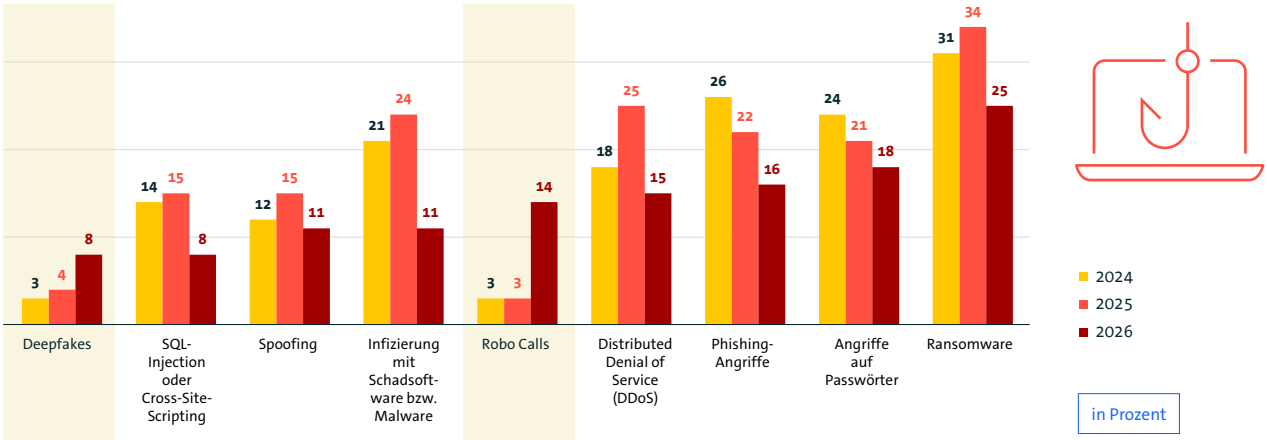
Die Unternehmen machen den KI-Einsatz vor allem an der automatisierten Anpassung von Angriffsversuchen fest, die **53 Prozent** als Hinweis nennen. 48 Prozent beobachten eine hohe Qualität gefälschter Audio- und Videoaufnahmen, 38 Prozent eine hohe sprachliche Qualität von Textnachrichten und Mails. Eine sehr hohe Frequenz der Angriffe nennen 34 Prozent, stark personalisierte Inhalte 28 Prozent. Bei 17 Prozent ergeben sich entsprechende Hinweise aus forensischen Analysen oder Threat Intelligence.

»Künstliche Intelligenz verändert das Angriffsgeschehen grundlegend. Leistungsfähige Modelle können Schadcode generieren und werden künftig auch für autonome Angriffsarten verwendet werden. Deepfakes oder täuschend echte Anrufe und Mails mit sehr persönlichem Bezug machen Betrug einfacher und Angriffe schwerer erkennbar. Künstliche Intelligenz kann aber auch eingesetzt werden, um Angriffe schneller aufzudecken und zu verhindern – diese Chance müssen Unternehmen nutzen.«

Bitkom-Präsident Dr. Ralf Wintergerst ↗Presseinformation

4.4 Arten schadensverursachender Cyberangriffe

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



Basis: Alle befragten Unternehmen ab 10 Beschäftigten (n=1.003) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2026

Abbildung 13: Schadensverursachende Cyberangriffsarten im Zeitvergleich

KI-gestützte Angriffe verursachen häufiger Schäden

Ransomware richtet unter den abgefragten Cyberangriffsarten weiterhin am häufigsten Schaden an (bei Ransomware verschlüsseln oder stehlen Angreifer Daten und fordern für deren Freigabe beziehungsweise Nichtveröffentlichung ein Lösegeld). Bei **25 Prozent** der Unternehmen haben solche Angriffe in den vergangenen zwölf Monaten einen Schaden verursacht. Gegenüber dem Vorjahr ist das allerdings ein Rückgang: 2025 waren es noch 34 Prozent, 2024 31 Prozent.

Passwortangriffe führten 2026 bei 18 Prozent der Unternehmen zu einem Schaden, Phishing-Angriffe bei 16 Prozent und DDoS-Attacken bei 15 Prozent. Eine Infizierung mit sonstiger Schadsoftware beziehungsweise Malware sowie Spoofing verursachten bei jeweils 11 Prozent der Unternehmen Schäden.

Während klassische Angriffsarten seltener Schaden anrichten, nehmen KI-gestützte Methoden zu. Besonders deutlich zeigt sich das bei Robo Calls: Ihr Anteil steigt von 3 Prozent im Vorjahr auf 14 Prozent. Deepfakes verursachten bei 8 Prozent der Unternehmen einen Schaden, doppelt so häufig wie 2025 mit 4 Prozent.

»Viele Unternehmen haben sich auf Ransomware-Angriffe vorbereitet und können so Schäden verhindern oder minimieren. Das Ziel muss sein, aus diesem bislang einmaligen Rückgang eine echte Trendwende zu machen.«

Bitkom-Präsident Dr. Ralf Wintergerst ↗Presseinformation

↗Presseinformation

Was ist Ransomware?

Bei Ransomware-Angriffen versuchen Cyberkriminelle, Unternehmen zu erpressen. Häufig werden IT-Systeme und Daten verschlüsselt, sodass Beschäftigte nicht mehr darauf zugreifen können und im Extremfall der gesamte Geschäftsbetrieb stillsteht.

Zunehmend werden zudem sensible oder personenbezogene Daten gestohlen. Die Angreifer drohen anschließend damit, diese zu veröffentlichen oder weiterzuverkaufen, falls kein Lösegeld gezahlt wird.

Ransomware: Jedes fünfte Ransomware-Opfer hat schon einmal Lösegeld gezahlt

Fast jedes zweite Unternehmen betroffen

Ransomware zählt zu den relevantesten Cyberbedrohungen für Unternehmen in Deutschland. 45 Prozent der Unternehmen waren innerhalb der vergangenen zwölf Monate von einem Ransomware-Angriff betroffen.

Die Mehrheit der betroffenen Unternehmen entscheidet sich gegen eine Zahlung. 66 Prozent haben kein Lösegeld an die Angreifer überwiesen. Dennoch hat bereits jedes fünfte betroffene Unternehmen, also 20 Prozent, Lösegeld gezahlt. Weitere 14 Prozent wollten oder konnten hierzu keine Angabe machen.

Fünf Maßnahmen gegen Ransomware

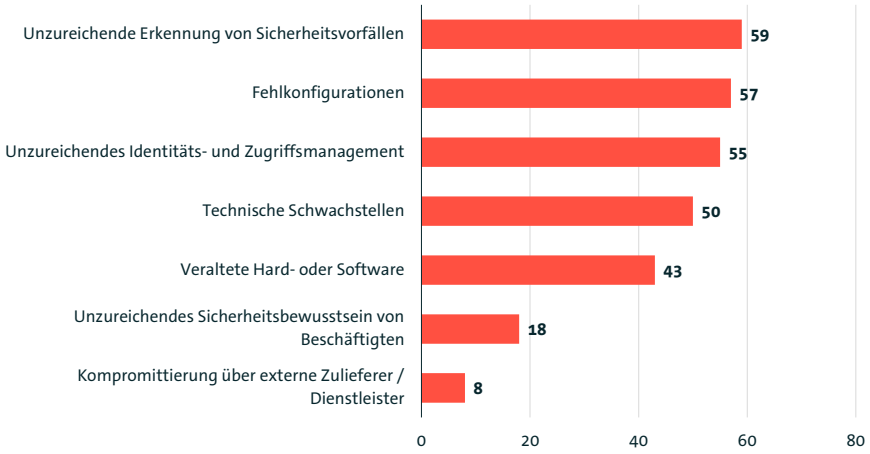
- **IT-Landschaft kennen**
  Unternehmen sollten jederzeit wissen, welche Systeme, Datenbestände, Schnittstellen und Zugänge vorhanden sind.
- **Backups erstellen und offline sichern**
  Datensicherungen sollten vom Unternehmensnetz getrennt aufbewahrt und ihre Wiederherstellung regelmäßig getestet werden.
- **Zugänge absichern**
  Mehr-Faktor-Authentifizierung, konsequentes Rechtemanagement und das Löschen nicht mehr benötigter Konten reduzieren mögliche Einfallstore.
- **Angriffe frühzeitig erkennen**
  Protokolldaten und Sicherheitssysteme sollten kontinuierlich überwacht werden, damit verdächtige Aktivitäten möglichst früh erkannt werden.
- **Den Ernstfall üben**
  Notfallpläne sollten Verantwortlichkeiten, Meldewege und Krisenkommunikation klar festlegen und auch bei einem Ausfall der IT verfügbar sein.

5 Faktoren, Vorbereitung und erwartete Entwicklung

5 Faktoren, Vorbereitung und erwartete Entwicklung

5.1 Faktoren erfolgreicher Cyberangriffe

Welche Faktoren haben maßgeblich dazu beigetragen, dass Ihr Unternehmen erfolgreich angegriffen werden konnte?



58%

der Unternehmen haben in den vergangenen zwölf Monaten einen Schaden durch Cyberangriffe erlitten.

Basis: Befragte Unternehmen ab 10 Beschäftigten, denen in den letzten 12 Monaten ein Schaden durch Cyberangriffe entstanden ist (n=580) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2026

Abbildung 14: Faktoren, die erfolgreiche Cyberangriffe begünstigen

Womit es Unternehmen Cyberkriminellen leicht machen

58 Prozent der Unternehmen haben in den vergangenen zwölf Monaten einen Schaden durch Cyberangriffe erlitten. Als wichtigsten Grund dafür, dass ein Angriff auch tatsächlich zu einem Schaden führte, nennen die betroffenen Unternehmen die unzureichende Erkennung von Sicherheitsvorfällen mit **59 Prozent**. Es folgen Fehlkonfigurationen von IT-Systemen mit 57 Prozent und ein unzureichendes Identitäts- und Zugriffsmanagement mit 55 Prozent.

Danach folgen technische Schwachstellen mit 50 Prozent und veraltete Hard- oder Software mit 43 Prozent. Deutlich seltener wird ein unzureichendes Sicherheitsbewusstsein der Beschäftigten genannt: 18 Prozent führen erfolgreiche Cyberangriffe darauf zurück. Eine Kompromittierung über externe Zulieferer oder Dienstleister nennen 8 Prozent.

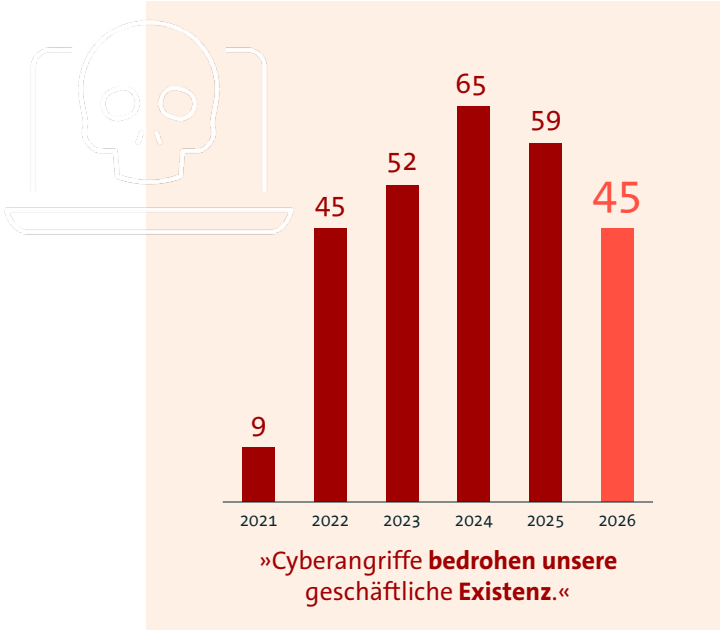
»Die häufigsten Schadensursachen sind keine besonders ausgefeilten oder exotischen Angriffe, sondern blinde Flecken im eigenen System. Wer Vorfälle nicht zuverlässig erkennt, kann auch nicht rechtzeitig handeln und wird am Ende womöglich nicht einmal sicher sagen können, was überhaupt passiert ist. Wer in Angriffserkennung, saubere Konfigurationen und ein striktes Identitätsmanagement investiert, schließt die wichtigsten Lücken, die Angreifer heute nutzen.«

Bitkom-Präsident Dr. Ralf Wintergerst ↗Presseinformation

5.2 Vorbereitung auf Cyberangriffe

Welche der folgenden Aussagen treffen auf Ihr Unternehmen zu?

43% (2025: 50%)
»Unser Unternehmen ist auf Cyberangriffe **sehr gut vorbereitet**.«



in Prozent

Basis: Alle befragten Unternehmen ab 10 Beschäftigten (n=1.003) | Prozentwerte für »Trifft zu« | Quelle: Bitkom Research 2026

Abbildung 15: Vorbereitung der Unternehmen auf Cyberangriffe und wahrgenommene Existenzbedrohung im Zeitvergleich

Unternehmen sind weniger gut vorbereitet, dennoch nimmt Existenzbedrohung ab

Die Unternehmen schätzen ihre eigene Vorbereitung auf Cyberangriffe zurückhaltender ein als noch vor einem Jahr. 2026 geben **43 Prozent** an, sehr gut auf Cyberangriffe vorbereitet zu sein. Im Vorjahr waren es noch 50 Prozent.

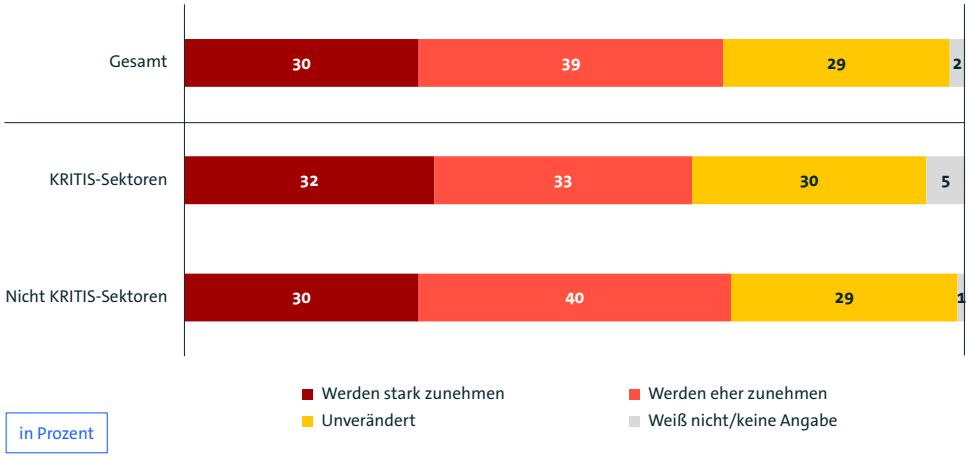
Gleichzeitig geht die wahrgenommene Bedrohung für die geschäftliche Existenz zurück. **45 Prozent** der Unternehmen sehen ihre geschäftliche Existenz durch Cyberangriffe bedroht – nach 59 Prozent im Jahr 2025 und dem bisherigen Höchstwert von 65 Prozent im Jahr 2024. Damit liegt die wahrgenommene Existenzbedrohung wieder auf dem Niveau von 2022.

Zum Vergleich: 2021 hatten lediglich 9 Prozent Cyberangriffe als Bedrohung für ihre geschäftliche Existenz eingestuft.

Weniger Unternehmen als im Vorjahr sehen sich damit sehr gut auf Cyberangriffe vorbereitet, zugleich nimmt aber auch der Anteil derjenigen ab, die Cyberangriffe als existenzbedrohend für ihr Unternehmen einschätzen.

5.3 Cyberangriffe: Erwartete Entwicklung

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 befragten Unternehmen ab 10 Beschäftigten (n=1.003) | Abweichungen von 100 Prozent sind rundungsbedingt | Quelle: Bitkom Research 2026

Abbildung 16: Erwartete Entwicklung der Anzahl von Cyberattacken nach KRITIS-Zugehörigkeit

Zwei Drittel rechnen mit Zunahme von Cyberangriffen

Die Unternehmen rechnen auch für die kommenden zwölf Monate mit weiter zunehmenden Cyberangriffen. Insgesamt erwarten **69 Prozent**, dass die Zahl der Cyberattacken steigen wird. 30 Prozent gehen von einer starken Zunahme aus, weitere 39 Prozent von einer eher zunehmenden Zahl an Angriffen. Nur 29 Prozent rechnen mit einer unveränderten Entwicklung.

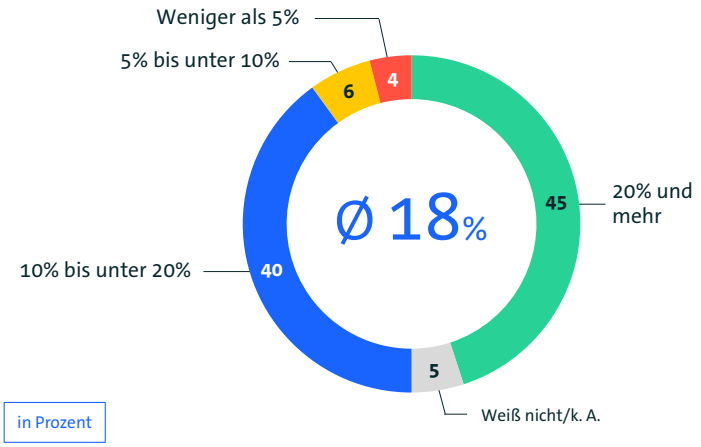
Die Einschätzung fällt in KRITIS- und Nicht-KRITIS-Sektoren ähnlich aus: Unter den KRITIS-Unternehmen erwarten 65 Prozent eine Zunahme der Cyberattacken, darunter 32 Prozent eine starke. In den Nicht-KRITIS-Sektoren rechnen 70 Prozent mit steigenden Angriffszahlen. Damit erwartet eine deutliche Mehrheit der Unternehmen, dass der bereits hohe Angriffsdruck in den kommenden zwölf Monaten weiter zunehmen wird.

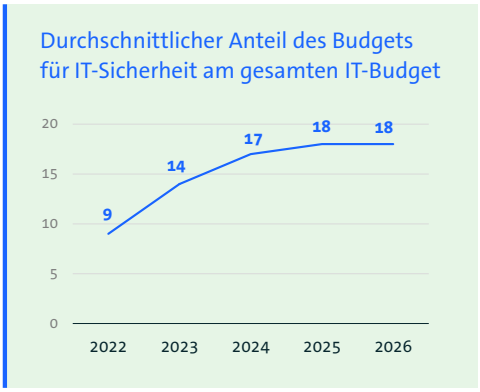
6 Investitionen und Digitale Souveränität

6 Investitionen und Digitale Souveränität

6.1 Investitionen in Cybersicherheit

Wie hoch schätzen Sie den Anteil des Budgets für IT-Sicherheit am gesamten IT-Budget Ihres Unternehmens?





Basis: Alle befragten Unternehmen ab 10 Beschäftigten (n=1.003) | Quelle: Bitkom Research 2026

Abbildung 17: Anteil der IT-Sicherheit am gesamten IT-Budget im Zeitvergleich

Investitionsbereitschaft in Cybersicherheit stagniert

Die Investitionen in IT-Sicherheit treten auf der Stelle: Im Durchschnitt fließen 2026 wie bereits im Vorjahr **18 Prozent** des gesamten IT-Budgets in die IT-Sicherheit. Zuvor war dieser Anteil deutlich gestiegen: von 9 Prozent im Jahr 2022 über 14 Prozent 2023 auf 17 Prozent 2024.

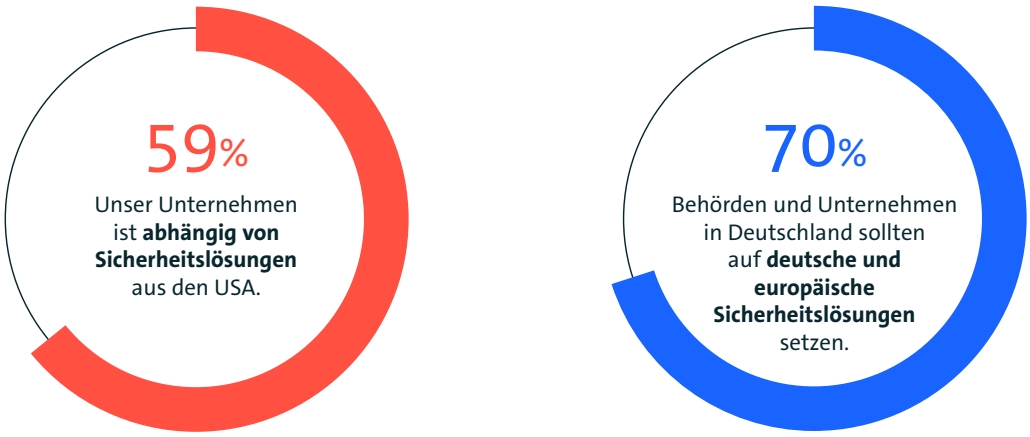
45 Prozent der Unternehmen investieren 20 Prozent oder mehr ihres IT-Budgets in IT-Sicherheit, im Vorjahr waren es 41 Prozent. Weitere 40 Prozent wenden zwischen 10 und unter 20 Prozent auf. Bei 6 Prozent liegt der Anteil zwischen 5 und unter 10 Prozent, 4 Prozent investieren weniger als 5 Prozent ihres IT-Budgets in IT-Sicherheit.

Das BSI und Bitkom empfehlen, 20 Prozent des IT-Budgets für Sicherheit aufzuwenden: »IT-Sicherheit betrifft jedes Unternehmen, ausreichende Investitionen sind unerlässlich. Unternehmen dürfen es nicht darauf ankommen lassen, dass ihnen nichts passieren wird«, so Bitkom-Präsident Ralf Wintergerst.

↗Presseinformation

6.2 Digitale Souveränität bei Sicherheitslösungen

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



Basis: Alle befragten Unternehmen ab 10 Beschäftigten (n=1.003) | Prozentwerte für »Trifft zu« | Quelle: Bitkom Research 2026

Abbildung 18: Abhängigkeit von US-Sicherheitslösungen und Präferenz für deutsche und europäische Anbieter

Digitale Souveränität ist für die Mehrheit ein Thema

Fragen der Digitalen Souveränität spielen auch bei der Cybersicherheit eine wichtige Rolle. **59 Prozent** der Unternehmen geben an, von Sicherheitslösungen aus den USA abhängig zu sein. Gleichzeitig sprechen sich **70 Prozent** dafür aus, dass Behörden und Unternehmen in Deutschland auf deutsche und europäische Sicherheitslösungen setzen sollten.

Damit zeigt sich ein Spannungsfeld zwischen bestehender Abhängigkeit und dem Wunsch nach stärkerer technologischer Eigenständigkeit. Besonders deutlich wird dies daran, dass eine Mehrheit der Unternehmen zwar auf US-Lösungen angewiesen ist, zugleich aber mehr Gewicht auf deutsche und europäische Angebote legen möchte.

»Zur Souveränität gehört, die zentralen Fragen der Sicherheit in die eigene Hand nehmen zu können – das gilt insbesondere auch im Cyberraum«, so Wintergerst ↗Presseinformation.

Die Bundesregierung muss bei ihren Programmen für ein digital souveränes Deutschland einen Schwerpunkt im Bereich der Cybersicherheit setzen.

7 Fazit

Die Ergebnisse des Wirtschaftsschutzes 2026 zeigen eine dauerhaft hohe und zunehmend schwerer durchschaubare Bedrohungslage. 96 Prozent der Unternehmen waren von Diebstahl, Industriespionage oder Sabotage betroffen oder vermuten entsprechende Vorfälle. Besonders auffällig ist das wachsende Dunkelfeld: 29 Prozent vermuten eine Betroffenheit, ohne einen Vorfall sicher feststellen zu können. Diese zunehmende Unsicherheit erschwert nicht nur die Bewertung der tatsächlichen Bedrohungslage, sondern auch die Bezifferung ihrer wirtschaftlichen Folgen. Deshalb weist die Studie 2026 erstmals einen Schadenskorridor zwischen 211 und 270,8 Milliarden Euro aus. BfV-Präsident Sinan Selen ordnet die Ergebnisse entsprechend ein: »Die Ergebnisse der Bitkom-Studie fügen sich nahtlos in das Bild der aktuell hohen Bedrohungslage ein.«

Gleichzeitig verändert sich der Charakter der Bedrohung. Ausländische Nachrichtendienste gewinnen als Tätergruppe stark an Bedeutung: Ihr Anteil ist seit 2023 von 7 auf 37 Prozent gestiegen. Hinzu kommt der zunehmende Einsatz Künstlicher Intelligenz, der Angriffe automatisierter, personalisierter und schwerer erkennbar macht. Die Grenzen zwischen Cyberkriminalität, Spionage und geopolitisch motivierten Operationen verschwimmen dabei zunehmend. Bitkom-Präsident Dr. Ralf Wintergerst warnt: »Die Grenzen zwischen Organisierter Kriminalität und den Geheimdiensten sind in vielen Ländern fließend.«

Umso wichtiger wird die eigene Widerstandsfähigkeit. Unzureichende Angriffserkennung, Fehlkonfigurationen sowie Schwächen beim Identitäts- und Zugriffsmanagement gehören zu den häufigsten Ursachen erfolgreicher Cyberangriffe. Gleichzeitig sehen sich nur 43 Prozent der Unternehmen sehr gut vorbereitet, während die Investitionen in IT-Sicherheit bei durchschnittlich 18 Prozent des IT-Budgets stagnieren. Wie Dr. Ralf Wintergerst betont: »Cybersicherheit muss integraler Teil jeder Digitalstrategie sein. Es geht darum, Angriffe abzuwehren und im Ernstfall schnell wieder arbeitsfähig zu werden.«

Wirtschaftsschutz muss deshalb als strategische Resilienzaufgabe verstanden werden, die Prävention, Erkennung, Reaktion und Wiederanlauf zusammendenkt. Entscheidend ist dabei nicht allein die Höhe der Investitionen, sondern dass Unternehmen bestehende Schwachstellen konsequent schließen und ihre Handlungsfähigkeit auch im Krisenfall sichern. Resilienz wird damit zu einer zentralen Voraussetzung für Wettbewerbsfähigkeit und wirtschaftliche Sicherheit.

8 Methodik

Befragung 2026

Auftraggeber	Bitkom
Methodik	Computergestützte telefonische Befragung/ Computer Assisted Telephone Interview (CATI), Dual Frame
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 dem Bereich IT.
Stichprobengröße	n=1.003
Befragungszeitraum	KW 16 bis KW 23 2026
Statistische Fehlertoleranz	+/- 3 Prozent in der Gesamtstichprobe

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

Wissenschaftliche Leitung
Anja Weber

Ansprechpartner
Felix Kuhlenkamp

Redaktion
Alissa Geffert

DOI
10.64022/2026-wirtschaftsschutz

Ansprechpartner

Felix Kuhlenkamp
Leiter Sicherheit
Bitkom e. V.

Die Frage nach dem Wirtschaftsschutz in Deutschland ist angesichts 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: Wie viele Unternehmen sind 2026 betroffen? Wer steckt hinter den Angriffen? Welche Rolle spielen Cyberattacken und Künstliche Intelligenz? Und wie hoch ist der wirtschaftliche Schaden? Grundlage des Studienberichts ist eine repräsentative Befragung von 1.003 Unternehmen in Deutschland.

DOI
10.64022/2026-wirtschaftsschutz

bitkom