# Hybride Angriffe: Wie gut ist Deutschland vorbereitet?

Perspektiven aus Bevölkerung und Unternehmen

bitkom

# Hybride Angriffe: Wie gut ist Deutschland vorbereitet?

Perspektiven aus Bevölkerung und Unternehmen

## Bitkom-Dataverse

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

Zum Bitkom-Dataverse

Zu den Studienberichten

DOI
10.64022/2026-hybride-angriffe

# Executive Summary

Hybride Angriffe – also die Kombination aus Cyberangriffen, Desinformationskampagnen, Sabotage, Spionage sowie wirtschaftlichem oder militärischem Druck – zielen darauf ab, Staaten zu destabilisieren und wirtschaftlichen Schaden zu verursachen. Mit der Verschärfung der geopolitischen Lage in Europa und den anhaltenden Spannungen zwischen Russland und der NATO rückt die Frage nach der Resilienz von Staat, Wirtschaft und Gesellschaft zunehmend in den Mittelpunkt.

Dieser Studienbericht untersucht, wie Unternehmen und Bevölkerung in Deutschland die Gefahr hybrider Angriffe einschätzen, welche konkreten Risiken sie sehen und wie sie ihren eigenen Vorbereitungsstand bewerten. Er zeigt außerdem, welche kritischen Infrastrukturen als besonders gefährdet gelten, welche Vorsorgemaßnahmen bereits getroffen wurden und welche Erwartungen an Politik und Sicherheitsbehörden bestehen.

Die Ergebnisse basieren auf zwei repräsentativen, computergestützten telefonischen Befragungen (CATI), die Bitkom Research im Auftrag des Digitalverbands Bitkom durchgeführt hat: Befragt wurden 604 Unternehmen in Deutschland sowie 1.263 Personen ab 16 Jahren in Deutschland.

## Zentrale Ergebnisse der Studie:

- **Hybride Angriffe gelten als reale und wachsende Bedrohung**
  83 Prozent der Unternehmen und 82 Prozent der Bevölkerung halten eine ernsthafte Krise infolge hybrider Angriffe für wahrscheinlich.
- **Deutschland wird als unzureichend vorbereitet wahrgenommen**
  73 Prozent der Unternehmen halten Deutschland im internationalen Vergleich für nicht ausreichend vorbereitet. Nur 39 Prozent sehen die Wirtschaft insgesamt gut gerüstet.
- **Unternehmen sind nur begrenzt krisenfest**
  Im Schnitt können Betriebe ohne Internet nur 20 Stunden weiterarbeiten; 21 Prozent müssten sofort einstellen, nur 8 Prozent kämen länger als 48 Stunden aus.
- **Kritische Infrastrukturen im Fokus der Sorge**
  Als besonders gefährdet gelten Energieversorgung (90 Prozent) und Finanzwesen (89 Prozent). 97 Prozent der Unternehmen erwarten gravierende Auswirkungen bei einem Ausfall der Energieversorgung. Auch in der Bevölkerung dominiert die Angst vor Energieausfällen (77 Prozent) und Störungen bei Banken (69 Prozent).
- **Informationsdefizite bei gleichzeitig hohem Staatsvertrauen**
  Nur 22 Prozent der Unternehmen fühlen sich ausreichend durch Behörden informiert. 64 Prozent der Bevölkerung sehen sich selbst nicht ausreichend informiert. Gleichzeitig erwarten 80 Prozent der Unternehmen im Ernstfall verlässliche Informationen von staatlichen Stellen.
- **Politik soll Prävention, Information und Abschreckung stärken**
  79 Prozent der Unternehmen fordern verpflichtende Sicherheitsstandards, 71 Prozent eine staatliche Informationskampagne. 60 Prozent befürworten Cyber-Gegenangriffe der Bundeswehr, 58 Prozent eine Ausweitung digitaler Überwachungsbefugnisse.

# Inhalt

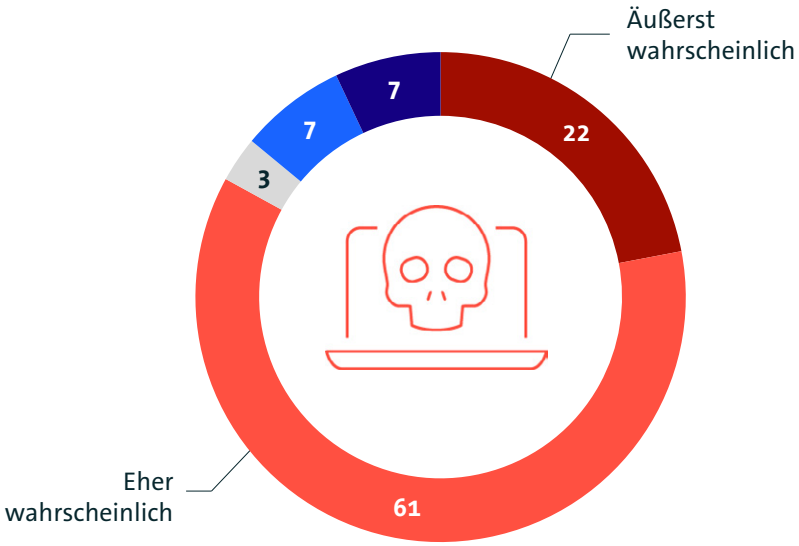
# Abbildungen

# 1 Risikoeinschätzung

# 1 Risikoeinschätzung

## 1.1 Wahrnehmung hybrider Bedrohungen

Für wie wahrscheinlich halten Sie es, dass es in Deutschland zu einer ernsthaften Krise infolge hybrider Angriffe kommt?




- Äußerst unwahrscheinlich
- Eher unwahrscheinlich
- Weiß nicht/k. A

in Prozent

Basis: Alle befragten Unternehmen (n=604) | Quelle: Bitkom Research 2026

Abbildung 1: Erwartung einer ernsthaften Krise in Deutschland durch hybride Angriffe (Unternehmen)

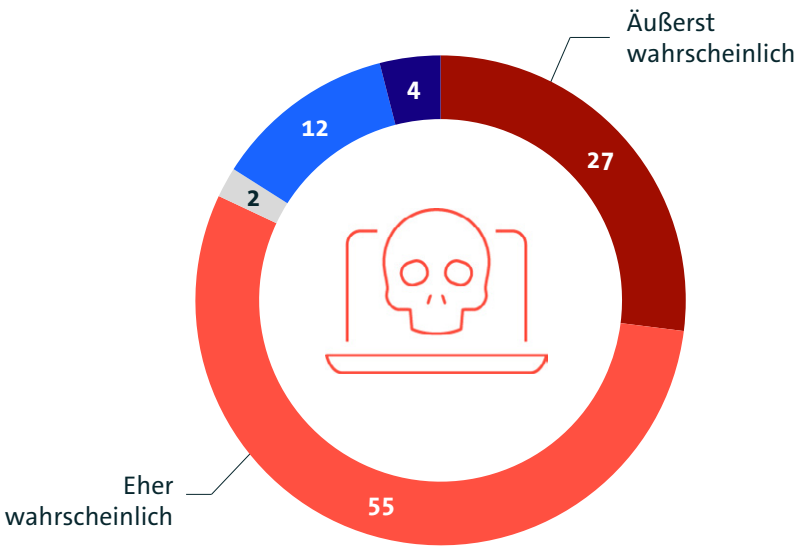
### Wirtschaft erwartet folgenschwere hybride Angriffe

Acht von zehn Unternehmen rechnen mit einer ernsthaften Krise in Deutschland infolge hybrider Angriffe, 61 Prozent halten sie für eher wahrscheinlich, 22 Prozent für äußerst wahrscheinlich. Nur 14 Prozent sehen das Risiko als eher oder äußerst unwahrscheinlich.

Damit wird deutlich: Das Thema ist nicht abstrakt und Unternehmen rechnen aktiv mit Bedrohungen.

**8 von 10 Unternehmen** rechnen mit einer ernsthaften Krise in Deutschland infolge hybrider Angriffe.

Für wie wahrscheinlich halten Sie es, dass es in Deutschland zu einer ernsthaften Krise infolge hybrider Angriffe kommt?




- Äußerst unwahrscheinlich
- Eher unwahrscheinlich
- Weiß nicht/k. A

in Prozent

Basis: Alle befragten Personen ab 16 Jahren (n=1.263) | Quelle: Bitkom Research 2026

Abbildung 2: Erwartung einer ernsthaften Krise in Deutschland durch hybride Angriffe (Bevölkerung)

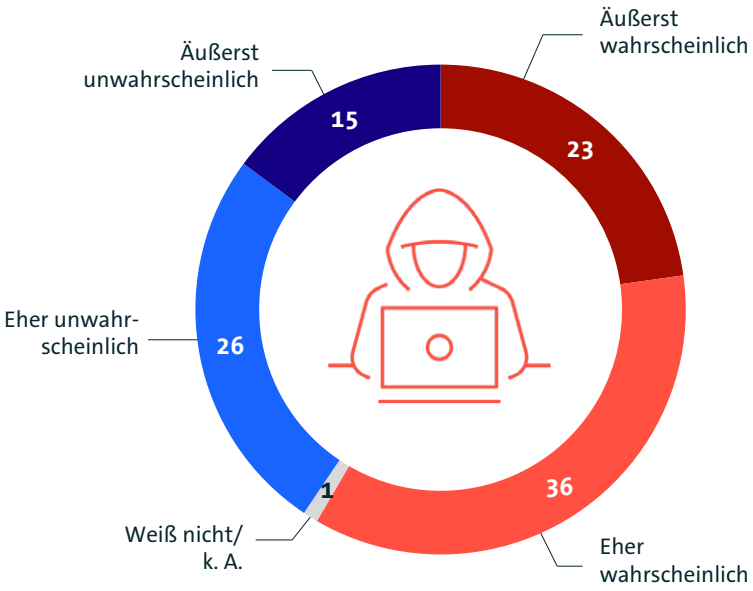
Die Mehrheit der Deutschen (82 Prozent) rechnet mit ernsten Konsequenzen durch hybride Angriffe: 55 Prozent halten eine solche Krise für eher wahrscheinlich, 27 Prozent für äußerst wahrscheinlich. Nur 16 Prozent schätzen die Gefahr als eher oder äußerst unwahrscheinlich ein.

Dieses Bild zeigt: Hybride Bedrohungen werden auch von der Bevölkerung als Gefahrenpotenzial wahrgenommen.

Gefahrenbewusstsein fast identisch: **82 Prozent** der Bevölkerung und **83 Prozent** der Unternehmen erwarten eine ernsthafte Krise in Deutschland durch hybride Angriffe.

## 1.2 Wahrscheinlichkeit eigener Betroffenheit

Für wie wahrscheinlich halten Sie es, dass Ihr Unternehmen Ziel hybrider Angriffe wird?




**61%** Sicherheit bzw. der Schutz vor hybriden Angriffen **ist bei uns Chefsache**.

in Prozent

Basis: Alle befragten Unternehmen (n=604) | Abweichungen von 100 Prozent sind rundungsbedingt | Quelle: Bitkom Research 2026

Abbildung 3: Erwartung der Unternehmen, selbst das Ziel hybrider Angriffe zu werden

Die Mehrheit der Unternehmen hält es für wahrscheinlich, selbst Ziel hybrider Angriffe zu werden: 36 Prozent schätzen dies als eher wahrscheinlich und 23 Prozent als äußerst wahrscheinlich ein. 41 Prozent sehen die Gefahr als eher oder äußerst unwahrscheinlich.

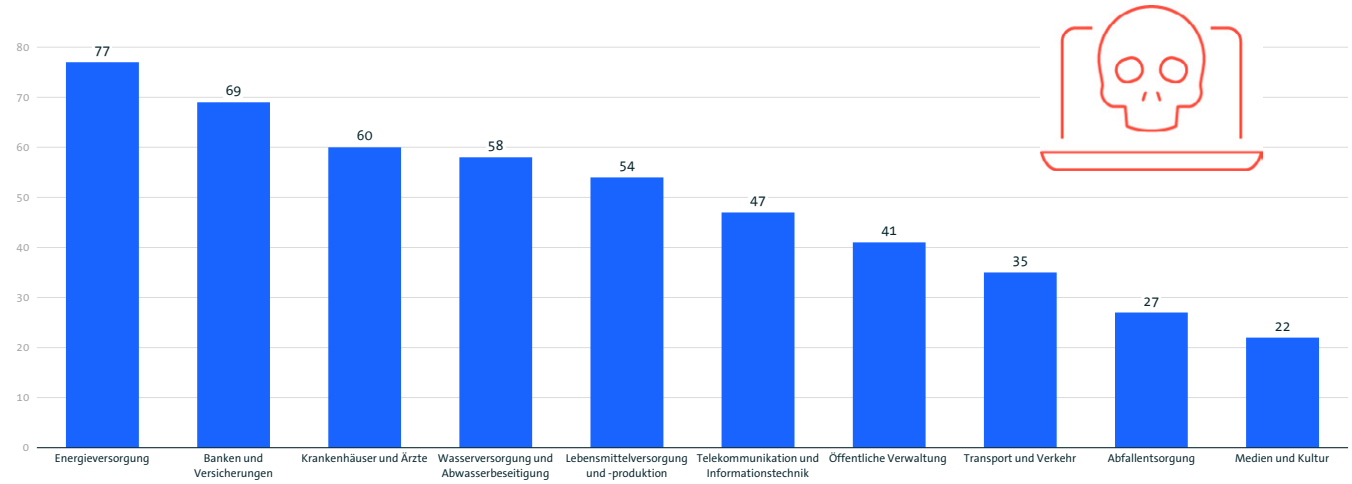
Diese Einschätzung unterstreicht, dass die Wirtschaft nicht nur indirekt, sondern auch unmittelbar von hybriden Angriffen betroffen ist.

61 Prozent der Unternehmen geben außerdem an, dass der Schutz vor solchen Attacken Chefsache ist.

> **Sechs von zehn Unternehmen** sehen sich als direktes Angriffsziel.

## 1.3 Gefährdung kritischer Infrastrukturen

### Wie viel Angst haben Sie, dass die folgenden Branchen oder Sektoren durch hybride Angriffe geschädigt oder sogar lahmgelegt werden?




in Prozent

Basis: Alle befragten Personen ab 16 Jahren (n=1.263) | Angaben für »Große Angst«| Quelle: Bitkom Research 2026

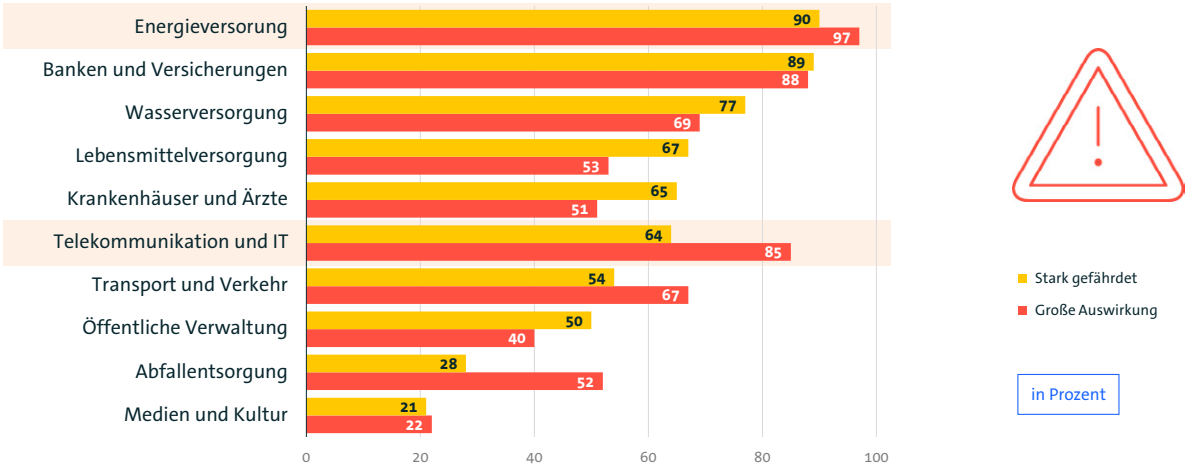
Abbildung 4: Angst der Bevölkerung vor Schäden durch hybride Angriffe nach Branchen

### Kein Strom, Geld oder Arzt – was der Bevölkerung Angst macht

Die Bevölkerung zeigt große Sorge, dass hybride Angriffe zentrale Bereiche lahmlegen könnten. Am stärksten ist die Angst vor Schäden in der Energieversorgung (77 Prozent), gefolgt von Banken und Versicherungen (69 Prozent). Weitere wichtige Bereiche sind Krankenhäuser und Ärzte (60 Prozent), Wasserversorgung und Abwasserentsorgung (58 Prozent) sowie Lebensmittelversorgung und -produktion (54 Prozent).

Weniger als die Hälfte der Befragten äußert große Angst vor Ausfällen bei Telekommunikation und IT (47 Prozent), der öffentlichen Verwaltung (41 Prozent) oder beim Transport und Verkehr (35 Prozent). Am wenigsten besorgt sind die Menschen über Abfallentsorgung (27 Prozent) und Medien und Kultur (22 Prozent).

## Welche dieser Branchen/Sektoren sind besonders stark gefährdet, durch hybride Angriffe lahmgelegt zu werden? Welche Ausfälle hätten große Auswirkungen auf Ihr Unternehmen?




Basis: Alle befragten Unternehmen (n=604) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2026

Abbildung 5: Gefährdung und Auswirkungen hybrider Angriffe auf Branchen aus Unternehmenssicht

Unternehmen sehen die Energieversorgung (90 Prozent stark gefährdet) sowie Banken und Versicherungen (89 Prozent) als besonders stark gefährdet. Auch die Wasser- und Abwasserversorgung (77 Prozent), Lebensmittelversorgung (67 Prozent), Krankenhäuser und Ärzte (65 Prozent) sowie Telekommunikation und IT (64 Prozent) gelten als gefährdet.

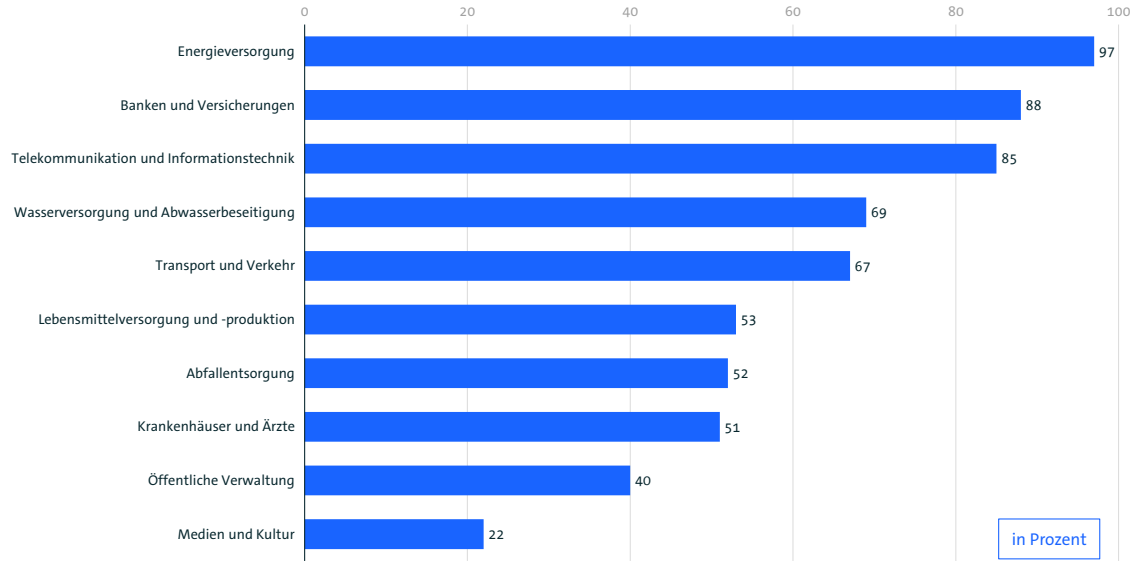
Weniger stark gefährdet erscheinen Transport und Verkehr (54 Prozent) und die öffentliche Verwaltung (50 Prozent), während Abfallentsorgung (28 Prozent) und Medien und Kultur (21 Prozent) am wenigsten gefährdet bewertet werden.

Betrachtet man die potenziellen Auswirkungen auf das eigene Unternehmen, hätten Angriffe auf die Energieversorgung (97 Prozent), Telekommunikation und IT (85 Prozent) sowie Banken und Versicherungen (88 Prozent) die größten Folgen. Auch Ausfälle in der Wasserversorgung (69 Prozent) und im Transport- und Verkehrssektor (67 Prozent) würden demnach stark spürbare Effekte haben.

> »Neben der Energieversorgung sind das Finanzwesen und die Kommunikation die neuralgischen Punkte der deutschen Wirtschaft«, so Bitkom-Präsident Ralf Wintergerst. »Zum notwendigen Schutz gehört zuallererst, es potenziellen Angreifern nicht unnötig leicht zu machen. Wir sollten darauf verzichten, Datenleitungen im Gigabit-Grundbuch öffentlich zugänglich zu verzeichnen, denn das bedeutet ein zusätzliches Risiko für Sabotageakte. Wir brauchen im Bereich kritischer Infrastrukturen Datensparsamkeit und ein strenges Sicherheits- und Zugangskonzept.«
>
> ↗Presseinformation

## 1.4 Erwartete Auswirkungen auf das eigene Unternehmen

Wenn es zu einem erfolgreichen hybriden Angriff auf die folgenden Branchen und Sektoren käme, welche Auswirkungen hätte dies auf Ihr Unternehmen?




Basis: Alle befragten Unternehmen (n=604) | Quelle: Bitkom Research 2026

Abbildung 6: Auswirkungen erfolgreicher hybrider Angriffe auf Unternehmen nach Branchen

Unternehmen erwarten bei einem erfolgreichen hybriden Angriff deutliche Auswirkungen auf ihr Geschäft, wobei die Einschätzungen je nach Branche variieren. Besonders gravierend wären Angriffe auf die Energieversorgung, auf die 97 Prozent der Unternehmen große Auswirkungen erwarten. Auch Banken und Versicherungen mit 88 Prozent sowie Telekommunikation und IT mit 85 Prozent würden erheblich betroffen sein.

Betrachtet man weitere Bereiche, zeigen sich Unterschiede: Bei der Wasserversorgung und Abwasserbeseitigung erwarten 69 Prozent der Unternehmen große Auswirkungen, bei Transport und Verkehr 67 Prozent, bei der Lebensmittelversorgung und -produktion 53 Prozent, bei Abfallentsorgung 52 Prozent und bei Krankenhäusern und Ärzten 51 Prozent. Am wenigsten betroffen würden laut Befragung öffentliche Verwaltung mit 40 Prozent und Medien und Kultur mit 22 Prozent sein.

Die Auffächerung nach Unternehmensgruppen verdeutlicht die Unterschiede zwischen Industrie, Dienstleistungen und Handel: In der Industrie sehen 100 Prozent der Befragten die Energieversorgung, 94 Prozent Banken und Versicherungen und 91 Prozent Telekommunikation und IT als besonders kritisch. Bei den Dienstleistern sind es 98 Prozent, 92 Prozent und 87 Prozent, im Handel 92 Prozent, 74 Prozent und 74 Prozent ↗Bitkom-Dataverse.

Diese Differenzen zeigen, dass kritische Infrastrukturen wie Energie, Finanzwesen und IT aus Sicht der Unternehmen besonders stark ins Gewicht fallen.

# 2 Informationsstand, Vertrauen & gesellschaftliche Resilienz

# 2 Informationsstand, Vertrauen & gesellschaftliche Resilienz

## 2.1 Informiertheit & staatliche Schutzfähigkeit

Inwieweit treffen die folgenden Aussagen zu?


Basis: Alle Befragten Unternehmen (l., n=604) bzw. alle befragten Personen ab 16 Jahren (r., n=1.263) | Quelle: Bitkom Research 2026

Abbildung 7: Informationsstand zu hybriden Angriffen bei Unternehmen und Bevölkerung

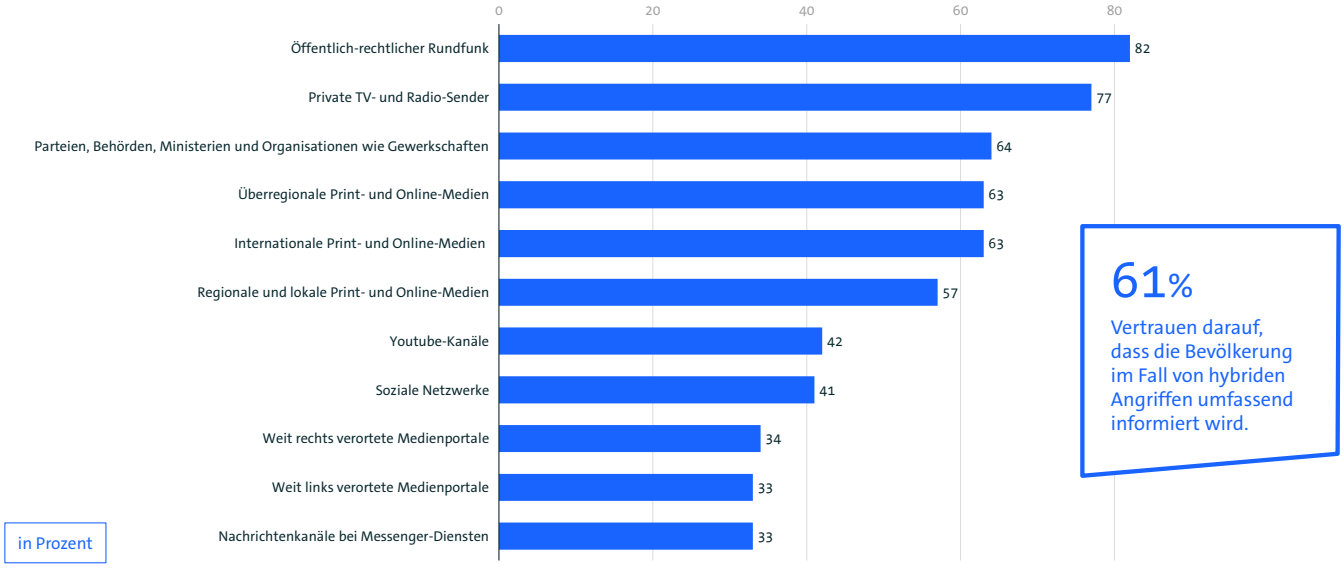
22 Prozent der Unternehmen geben an, sich ausreichend durch Sicherheitsbehörden über mögliche hybride Angriffe informiert zu fühlen.

Bei der Bevölkerung geben 64 Prozent an, über Bedrohungen durch hybride Angriffe nicht informiert zu sein. Gleichzeitig vertrauen jedoch 61 Prozent der Bevölkerung darauf, im Falle hybrider Bedrohungen umfassend informiert zu werden (siehe S. 16).

Niedriger Informationsstand: Nur **22 Prozent** der Unternehmen fühlen sich durch Sicherheitsbehörden ausreichend über hybride Angriffe informiert, und **64 Prozent** der Bevölkerung geben an, keine ausreichenden Informationen zu haben.

## 2.2 Vertrauen in Informationsquellen

Inwieweit vertrauen Sie den folgenden Informationsquellen, wenn sie speziell an hybride Angriffe auf Deutschland und deren Folgen denken?




Basis: Alle Befragten Unternehmen (l., n=604) bzw. alle befragten Personen ab 16 Jahren (r., n=1.263) | Quelle: Bitkom Research 2026

Abbildung 8: Vertrauen der Bevölkerung in Informationsquellen bei hybriden Angriffen

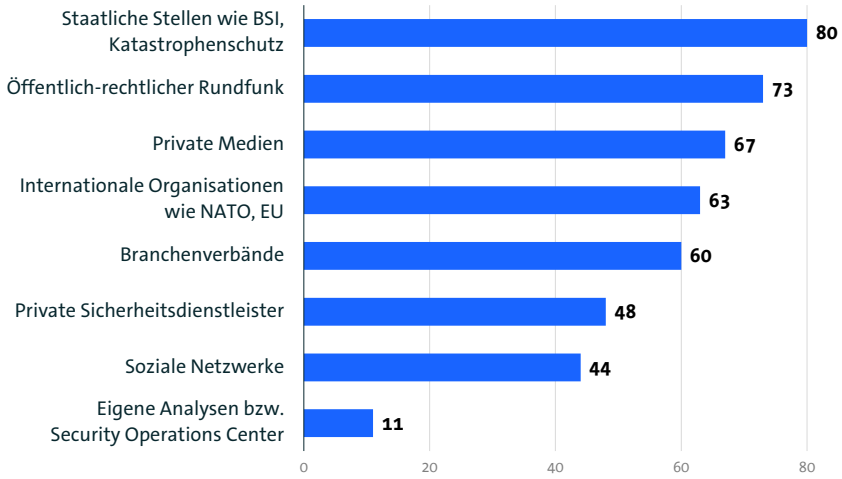
Die Bevölkerung vertraut im Krisenfall unterschiedlich stark auf Informationsquellen: Am höchsten ist das Vertrauen in den öffentlich-rechtlichen Rundfunk mit 82 Prozent, gefolgt von privaten TV- und Radiosendern mit 77 Prozent. 64 Prozent der Befragten vertrauen auf Parteien, Behörden, Ministerien und Organisationen wie Gewerkschaften. Überregionale sowie internationale Print- und Online-Medien werden jeweils von 63 Prozent als vertrauenswürdig eingestuft, regionale und lokale Print- und Online-Medien von 57 Prozent.

Deutlich geringer fällt das Vertrauen in YouTube-Kanäle (42 Prozent), soziale Netzwerke (41 Prozent) sowie in weit rechts (34 Prozent) oder weit links verortete Medienportale (33 Prozent) und Nachrichtendienste über Messenger-Kanäle (33 Prozent) aus.

> Wem vertrauen die Menschen im Krisenfall? Öffentlich-rechtlicher Rundfunk (**82 Prozent**) und private TV- und Radiosender (**77 Prozent**) genießen das höchste Vertrauen.

Insgesamt vertrauen zudem 61 Prozent der Befragten darauf, dass die Bevölkerung im Falle hybrider Angriffe umfassend informiert wird.

## Von wem erwarten Sie im Fall eines hybriden Angriffs die verlässlichsten Informationen?




**22%**

»Wir fühlen uns ausreichend durch Sicherheitsbehörden über mögliche hybride Angriffe informiert.«

in Prozent

Basis: Alle befragten Unternehmen (n=604) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2026

Abbildung 9: Erwartete verlässliche Informationsquellen bei hybriden Angriffen aus Unternehmenssicht

## Wem die Unternehmen in der Krise vertrauen

Unternehmen erwarten im Fall eines hybriden Angriffs die verlässlichsten Informationen vor allem von staatlichen Stellen wie BSI und Katastrophenschutz, denen 80 Prozent Vertrauen entgegenbringen. Auf den öffentlich-rechtlichen Rundfunk vertrauen 73 Prozent, auf private Medien 67 Prozent. Internationale Organisationen wie NATO oder EU werden von 63 Prozent als verlässliche Quellen angesehen, Branchenverbände von 60 Prozent.

Private Sicherheitsdienstleister genießen das Vertrauen von 48 Prozent, soziale Netzwerke von 44 Prozent. Eigene Analysen bzw. Security Operations Center werden nur von 11 Prozent als verlässlich betrachtet.

Daneben geben jedoch nur 22 Prozent der Unternehmen an, sich ausreichend durch Sicherheitsbehörden über mögliche hybride Angriffe informiert zu fühlen. Ein großes Problem für die Unternehmen sind daher nicht unverlässliche, sondern fehlende Informationen über mögliche hybride Angriffe.

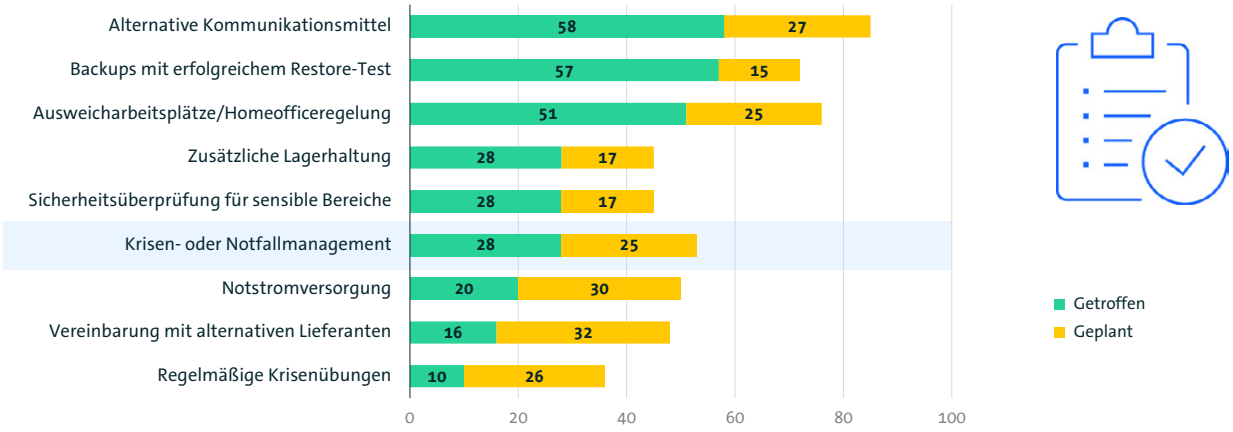
Verlässliche Informationen im Krisenfall: **80 Prozent** der Unternehmen vertrauen staatlichen Stellen wie BSI und Katastrophenschutz, **73 Prozent** dem öffentlich-rechtlichen Rundfunk und **67 Prozent** privaten Medien. Eigene Analysen oder Security Operations Center werden nur von **11 Prozent** als verlässlich eingeschätzt.

# 3 Konkrete Vorbereitung & Resilienz

# 3 Konkrete Vorbereitung & Resilienz

## 3.1 Vorsorgemaßnahmen

### Welche der folgenden Vorkehrungen haben Sie zum Umgang mit hybriden Angriffen in Ihrem Unternehmen getroffen?




in Prozent

Basis: Alle befragten Unternehmen (n=604) | Quelle: Bitkom Research 2026

Abbildung 10: Vorkehrungen von Unternehmen zum Umgang mit hybriden Angriffen

### In den meisten Unternehmen gibt es keinen Notfallplan

In den Unternehmen gibt es eine Vielzahl von Maßnahmen zum Umgang mit hybriden Angriffen, ein flächendeckender Notfallplan fehlt jedoch. 58 Prozent der Unternehmen verfügen über alternative Kommunikationsmittel, 27 Prozent planen dies. Backups mit erfolgreichen Restore-Tests sind bei 57 Prozent vorhanden. Ausweicharbeitsplätze oder Homeoffice-Regelungen existieren in 51 Prozent der Unternehmen.

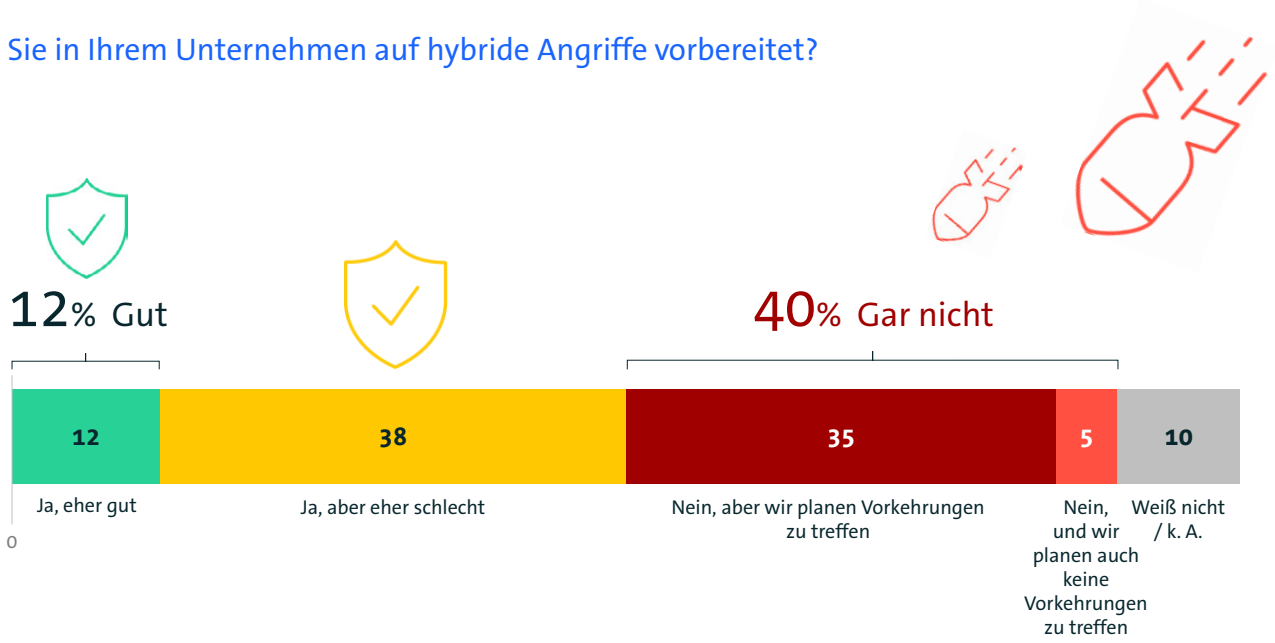
Rund ein Viertel der Unternehmen hat zusätzliche Lagerhaltung getroffen und 16 Prozent haben Vereinbarungen mit alternativen Lieferanten, 32 Prozent planen solche Vereinbarungen.

Sicherheitsüberprüfungen in sensiblen Bereichen setzen 28 Prozent um, 17 Prozent planen sie. Ein Krisen- oder Notfallmanagement existiert in 28 Prozent der Unternehmen, 25 Prozent wollen eines einführen.

Über eine Notstromversorgung verfügen 20 Prozent, 30 Prozent planen sie. Nur 10 Prozent führen regelmäßige Krisenübungen durch, 26 Prozent planen diese.

Die Befragung verdeutlicht, dass viele Unternehmen einzelne Vorkehrungen treffen, ein umfassender, flächendeckender Schutz bislang aber nicht gegeben ist.

## Sind Sie in Ihrem Unternehmen auf hybride Angriffe vorbereitet?




in Prozent

Basis: Alle befragten Unternehmen (n=604) | Quelle: Bitkom Research 2026

Abbildung 11: Vorbereitung von Unternehmen auf hybride Angriffe

Die Mehrheit der Unternehmen fühlt sich nur unzureichend auf hybride Angriffe vorbereitet. Kein Unternehmen hält sich für sehr gut vorbereitet, lediglich 12 Prozent bewerten ihren Vorbereitungsgrad als eher gut. 38 Prozent der Unternehmen geben an, eher schlecht vorbereitet zu sein.

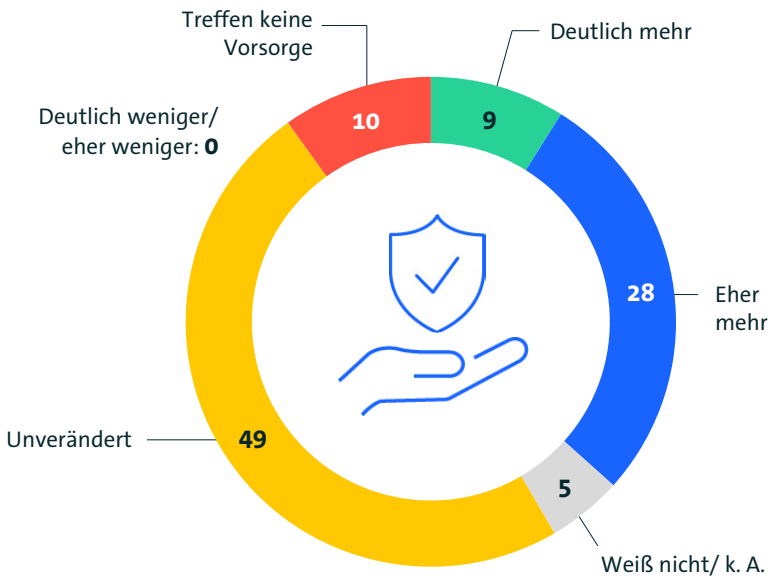
Weitere 40 Prozent sind gar nicht vorbereitet, wobei 35 Prozent davon immerhin planen, Vorkehrungen zu treffen, und 5 Prozent keine Maßnahmen planen. 10 Prozent der Unternehmen können oder wollen keine Angaben zum Stand der Vorbereitungen machen.

Die Daten verdeutlichen, dass es eine deutliche Lücke zwischen dem Gefahrenbewusstsein und dem aktuellen Schutzniveau gibt.

»Wir müssen die Lücke zwischen Gefahrenbewusstsein und Schutzniveau schnellstmöglich schließen«, so Bitkom-Präsident Ralf Wintergerst ↗Presseinformation.

Aktuell halten sich nur **12 Prozent** der Unternehmen für eher gut auf hybride Angriffe vorbereitet, **38 Prozent** für eher schlecht, weitere **40 Prozent** sind gar nicht vorbereitet – während zugleich **83 Prozent** der befragten Unternehmen eine ernsthafte Krise infolge hybrider Angriffe erwarten.

Verglichen mit Ihren aktuellen Ausgaben, werden Sie in Ihrem Unternehmen im Jahr 2026 mehr oder weniger in die Vorbereitung auf hybride Angriffe und deren Folgen investieren?




in Prozent

Basis: Alle befragten Unternehmen (n=604) | Abweichungen von 100% sind rundungsbedingt | Quelle: Bitkom Research 2026

Abbildung 12: Geplante Investitionen von Unternehmen in den Schutz vor hybriden Angriffen im Jahr 2026

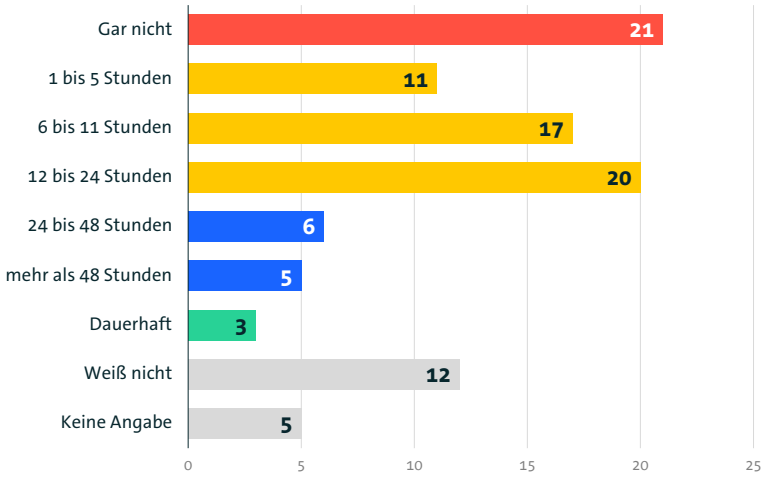
Viele Unternehmen planen, ihre Investitionen in den Schutz vor hybriden Angriffen zu erhöhen. 9 Prozent der Unternehmen wollen in diesem Jahr deutlich mehr Geld ausgeben, 28 Prozent eher mehr. Knapp die Hälfte der Unternehmen (49 Prozent) plant unveränderte Investitionen. Kein Unternehmen will die Ausgaben senken, 10 Prozent treffen jedoch aktuell keine Vorsorge.

Die Daten zeigen, dass rund 4 von 10 Unternehmen ihre Ausgaben für Prävention erhöhen wollen, während die Mehrheit zumindest ihre bestehenden Maßnahmen beibehält.

> Unternehmen wollen den Schutz vor hybriden Angriffen hochfahren: **9 Prozent** investieren deutlich mehr, **28 Prozent** eher mehr – **10 Prozent** treffen aktuell keine Vorsorge.

## 3.2 Resilienz bei Internetausfall

### Wie lange könnten Sie den Geschäftsbetrieb ohne Internet aufrechterhalten?




**20** Stunden

können Unternehmen im Schnitt ohne Internet den Geschäftsbetrieb aufrechterhalten.

in Prozent

Basis: Alle befragten Unternehmen (n=604) | Quelle: Bitkom Research 2026

Abbildung 13: Dauer, die Unternehmen den Geschäftsbetrieb ohne Internet aufrechterhalten können

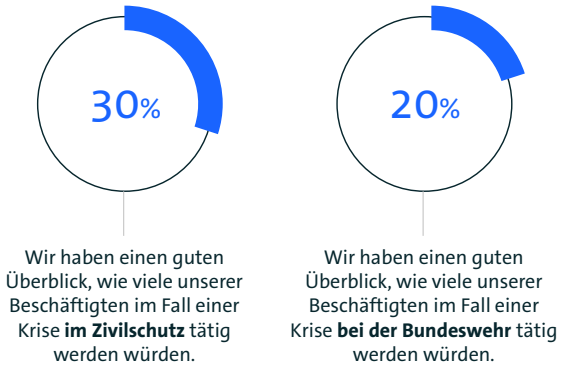
Unternehmen könnten ihren Geschäftsbetrieb ohne Internet im Durchschnitt nur 20 Stunden aufrechterhalten. 21 Prozent der Unternehmen könnten gar nicht mehr arbeiten, während 11 Prozent nur 1 bis 5 Stunden durchhalten würden. 17 Prozent könnten 6 bis 11 Stunden, 20 Prozent 12 bis 24 Stunden den Betrieb aufrechterhalten.

Länger als 48 Stunden weiterarbeiten könnten lediglich 8 Prozent der Unternehmen, dauerhaft unabhängig vom Internet wären nur 3 Prozent. 12 Prozent der Befragten machten keine Angaben.

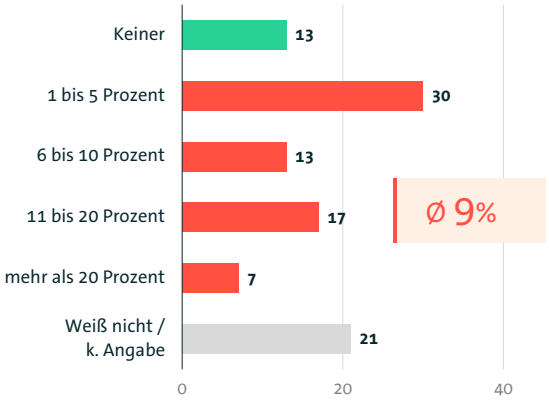
Diese Zahlen verdeutlichen, wie schnell ein Ausfall von Internetdiensten in Unternehmen zu massiven Unterbrechungen führen kann, besonders wenn zentrale Netze oder Knotenpunkte betroffen sind.

> Ohne Internet gehen nach 20 Stunden die Lichter aus: **21 Prozent** der Unternehmen müssten sofort die Arbeit einstellen, nur **8 Prozent** könnten länger als 48 Stunden weiterarbeiten.

## Welche der folgenden Aussagen treffen auf Ihr Unternehmen zu?




## Wie viel Prozent Ihrer Beschäftigten würde im Krisenfall bei Bundeswehr oder im Zivilschutz tätig werden?




in Prozent

Basis links: Alle befragten Unternehmen ( n=604) | Basis rechts: Befragte Unternehmen, die einen Überblick über Ausfälle in der Belegschaft haben ( n=218) |
Quelle: Bitkom Research 2026

Abbildung 14: Überblick der Unternehmen über Mitarbeiterausfälle im Krisenfall

Im Krisenfall könnten Unternehmen mit Personalengpässen rechnen, da Beschäftigte beim Zivilschutz oder der Bundeswehr abwesend sein könnten. Nur 30 Prozent der Unternehmen haben einen guten Überblick darüber, wie viele Mitarbeiterinnen und Mitarbeiter den Zivilschutz unterstützen, etwa bei Feuerwehren oder beim Technischen Hilfswerk. Nur 20 Prozent wissen, wie viele Beschäftigte bei der Bundeswehr im Krisenfall tätig würden.

Unternehmen, die eine Schätzung abgeben können, rechnen im Schnitt damit, dass 9 Prozent der Belegschaft ausfallen würden. Selbst bei Unternehmen mit gutem Überblick kann jedes fünfte keine genaue Zahl benennen.

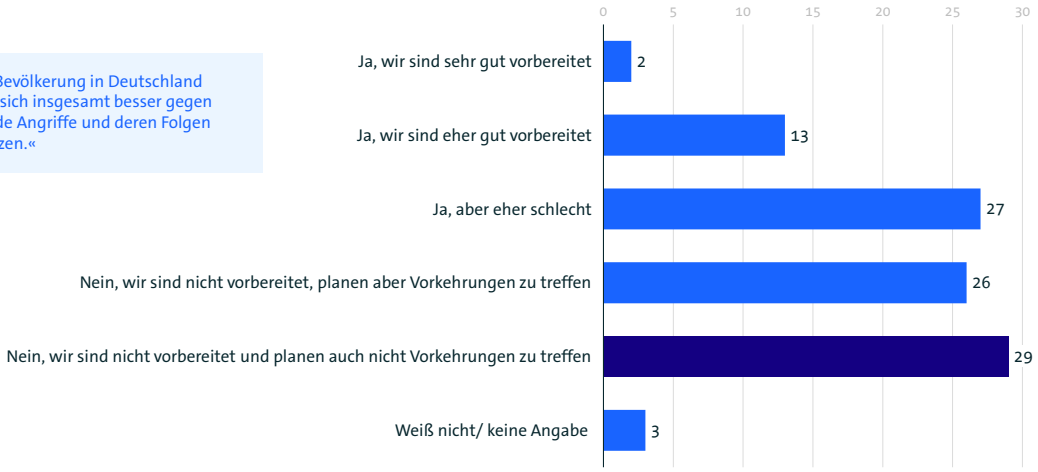
Diese Zahlen verdeutlichen, dass Personalengpässe im Krisenfall ein zusätzliches Risiko darstellen, das bei der Planung von Notfallmaßnahmen berücksichtigt werden muss.

> Im Ernstfall fehlen Beschäftigte: Unternehmen schätzen, dass im Schnitt **9 Prozent** der Belegschaft ausfallen würden, nur **20 bis 30 Prozent** haben einen genauen Überblick.

## 3.3 Private Vorsorge in Haushalten

### Sind Sie in Ihrem Haushalt auf hybride Angriffe und deren Folgen vorbereitet?

**65%** »Die Bevölkerung in Deutschland muss sich insgesamt besser gegen hybride Angriffe und deren Folgen schützen.«




Basis: Alle befragten Personen ab 16 Jahren (n=1.263) | Abweichungen von 100 Prozent sind rundungsbedingt | Quelle: Bitkom Research 2026

Abbildung 15: Vorbereitung der Bevölkerung auf hybride Angriffe und deren Folgen

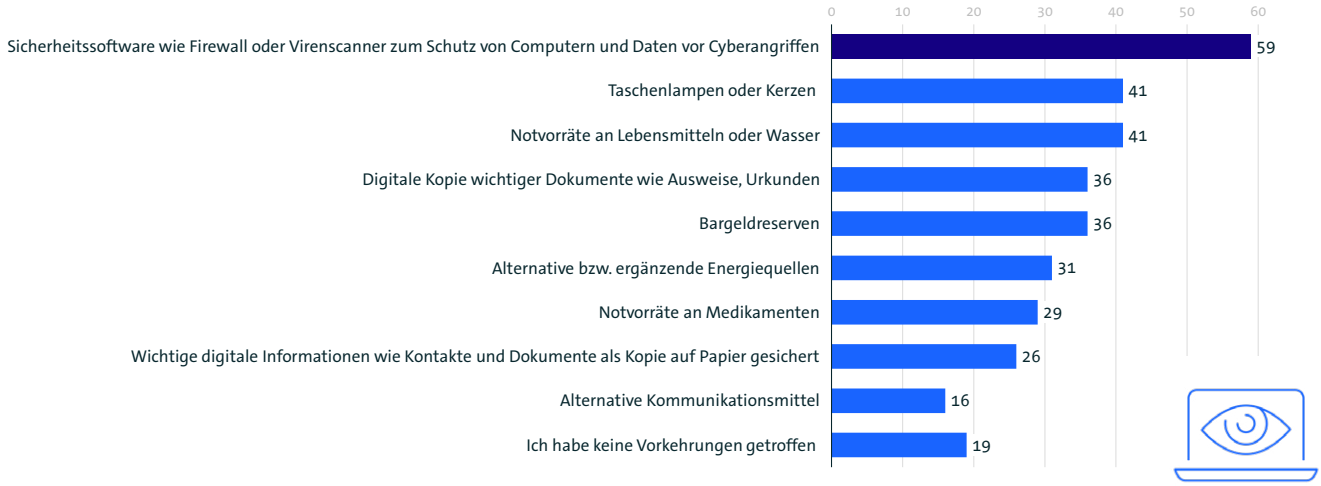
Die Mehrheit der Bevölkerung ist nur unzureichend auf hybride Angriffe vorbereitet. Nur 2 Prozent der Befragten fühlen sich sehr gut vorbereitet, 13 Prozent eher gut. 27 Prozent geben an, eher schlecht vorbereitet zu sein, und 26 Prozent planen zwar Vorkehrungen, fühlen sich aber nicht vorbereitet.

29 Prozent der Menschen sind weder vorbereitet noch planen sie, Maßnahmen zu ergreifen.

Insgesamt zeigt sich, dass 65 Prozent der Befragten der Meinung sind, dass die Bevölkerung in Deutschland sich insgesamt besser gegen hybride Angriffe und deren Folgen schützen muss, während nur 15 Prozent eher oder sehr gut privat vorgesorgt haben.

**65 Prozent** der Bevölkerung sehen Nachholbedarf: Nur **15 Prozent** fühlen sich gut vorbereitet auf hybride Angriffe, **29 Prozent** planen derzeit keinerlei Maßnahmen.

## Welche der folgenden Vorkehrungen haben Sie in Ihrem Haushalt getroffen, um im Falle eines erfolgreichen hybriden Angriffs mit Kommunikations- oder Versorgungsengpässen umzugehen?




Basis: Alle befragten Personen ab 16 Jahren (n=1.263) | Abweichungen von 100 Prozent sind rundungsbedingt | Quelle: Bitkom Research 2026

Abbildung 16: Vorkehrungen der Haushalte gegen hybride Angriffe und deren Folgen

Die Mehrheit der Bevölkerung hat sich in ihren Haushalten zumindest teilweise auf hybride Angriffe vorbereitet. 59 Prozent nutzen Sicherheitssoftware wie Firewalls oder Virenscanner, 36 Prozent haben digitale Kopien wichtiger Dokumente angelegt, und 26 Prozent haben analoge Kopien wichtiger digitaler Dateien erstellt. 31 Prozent verfügen über alternative Energiequellen wie Powerbanks oder Batterien.

Viele Haushalte haben auch klassische Vorsorgemaßnahmen getroffen: 41 Prozent besitzen Taschenlampen oder Kerzen, ebenso viele halten Notvorräte an Lebensmitteln und Wasser bereit, 36 Prozent haben Bargeldreserven, und 29 Prozent verfügen über Notvorräte an Medikamenten. 16 Prozent nutzen alternative Kommunikationsmittel wie batteriebetriebene Radios oder Funkgeräte.

Trotzdem hat fast ein Fünftel der Bevölkerung (19 Prozent) keinerlei Vorkehrungen getroffen.

Die meisten Haushalte sind nur teilweise vorbereitet: **59 Prozent** nutzen Sicherheitssoftware, **41 Prozent** haben Notvorräte, **19 Prozent** haben keinerlei Vorkehrungen getroffen.

## 3.4 Bereitschaft zum persönlichen Engagement

Inwieweit treffen folgende Aussagen auf Sie zu?

54%

»Im Fall einer Krise bin ich bereit, **im Zivilschutz tätig zu werden**, etwa beim Technischen Hilfswerk, in der Freiwilligen Feuerwehr oder einer ähnlichen Organisation.«

41%

»Ich bin bereit, im Fall einer Krise **für die Bundeswehr** tätig zu werden.«

Basis: Alle befragten Personen ab 16 Jahren (n=1.263) Quelle: Bitkom Research 2026

Abbildung 17: Bereitschaft der Bevölkerung zur Unterstützung im Zivilschutz oder bei der Bundeswehr im Krisenfall

Wie bereit ist die Bevölkerung in Deutschland, im Krisenfall aktiv zu werden? 54 Prozent der Befragten geben an, dass sie im Zivilschutz tätig werden würden, zum Beispiel beim Technischen Hilfswerk, in der Freiwilligen Feuerwehr oder ähnlichen Organisationen. 41 Prozent der Befragten wären bereit, im Krisenfall für die Bundeswehr tätig zu werden.

Die Zahlen machen deutlich, dass mehr Menschen bereit sind, in zivilen Schutzorganisationen zu helfen, während die Bereitschaft, militärisch aktiv zu werden, etwas geringer ausfällt. Ein signifikanter Teil der Bevölkerung ist grundsätzlich einsatzbereit.

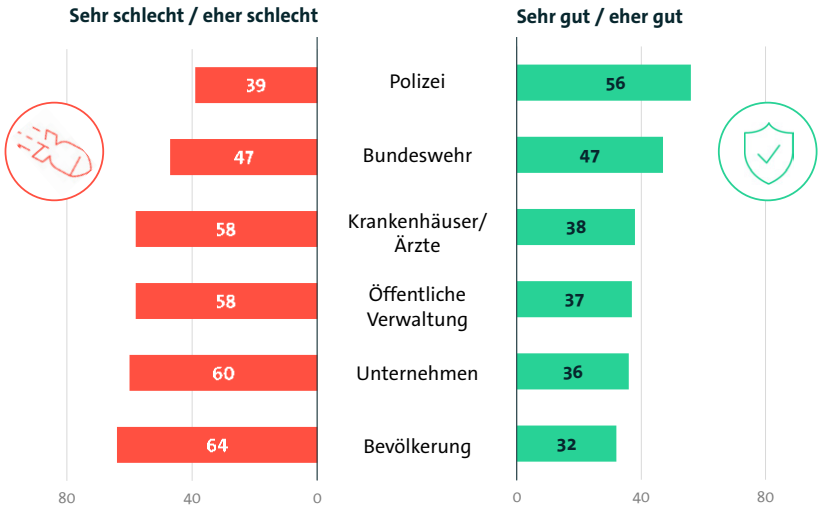
**Mehr als die Hälfte der Bevölkerung** wäre einsatzbereit – besonders im Zivilschutz

# 4 Bewertung der Vorbereitung Deutschlands

# 4 Bewertung der Vorbereitung Deutschlands

## 4.1 Einschätzung zentraler Akteure

### Wie gut sind die folgenden Akteure in Deutschland auf hybride Angriffe vorbereitet?




**49%**

der Bürgerinnen und Bürger in Deutschland sagen: »Die Bundesregierung schenkt Bedrohungen durch hybride Angriffe zu wenig Beachtung.«

in Prozent

Basis: Alle befragten Personen ab 16 Jahren (n=1.263) | nicht dargestellt: »Weiß nicht/k. A.« | Quelle: Bitkom Research 2026

Abbildung 18: Einschätzung der Vorbereitung verschiedener Akteure in Deutschland auf hybride Angriffe (Bevölkerung)

Die Einschätzungen der Bevölkerung zeigen deutliche Unterschiede darin, wie gut verschiedene Akteure auf hybride Angriffe vorbereitet sind: Mit Abstand am besten vorbereitet werden Polizei (56 Prozent) und Bundeswehr (47 Prozent) eingeschätzt. Krankenhäuser und Ärzte folgen mit 38 Prozent, die öffentliche Verwaltung mit 37 Prozent und Unternehmen mit 36 Prozent.

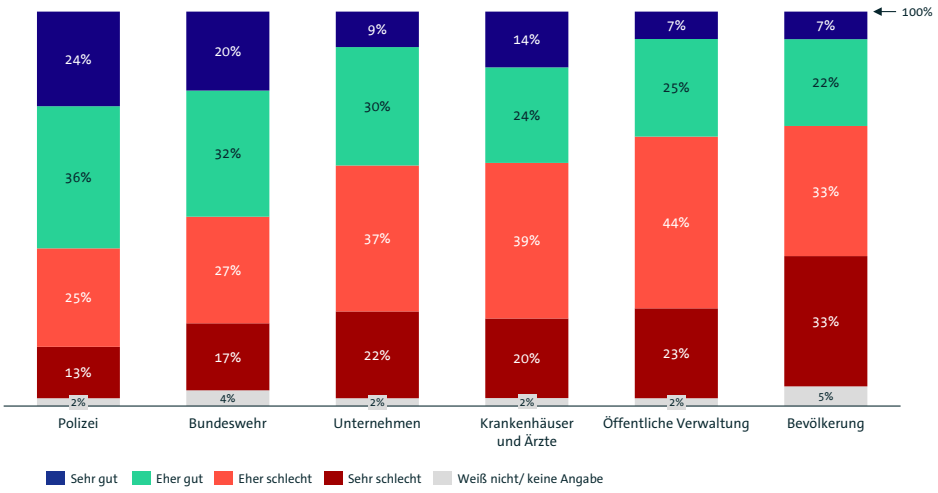
Die Bevölkerung selbst wird nur von 32 Prozent als gut vorbereitet gesehen.

Auf der anderen Seite sehen viele die Akteure kritisch vorbereitet: 39 Prozent bewerten die Polizei eher schlecht, 47 Prozent die Bundeswehr, 58 Prozent Krankenhäuser/Ärzte, 58 Prozent die öffentliche Verwaltung, 60 Prozent Unternehmen und 64 Prozent die Bevölkerung als schlecht vorbereitet.

Insgesamt sagen 49 Prozent der Befragten, dass die Bundesregierung Bedrohungen durch hybride Angriffe zu wenig Beachtung schenkt.

> Bürgerinnen und Bürger sehen Polizei und Bundeswehr als am besten auf hybride Angriffe vorbereitet.

## Wie gut sind die folgenden Akteure in Deutschland auf hybride Angriffe vorbereitet?




**57%**

»Wir vertrauen darauf, dass Sicherheitsbehörden uns im Fall eines hybriden Angriffs schützen.«

Basis: Alle befragten Unternehmen (n=604) | Abweichungen von 100% sind rundungsbedingt | Quelle: Bitkom Research 2026

Abbildung 19: Vorbereitung verschiedener Akteure in Deutschland auf hybride Angriffe aus Sicht der Unternehmen

Die Einschätzungen der Unternehmen zur Vorbereitung auf hybride Angriffe unterscheiden sich deutlich zwischen den Akteuren: Polizei (60 Prozent) und Bundeswehr (52 Prozent) gelten als am zuverlässigsten. Krankenhäuser und Ärzte liegen bei 38 Prozent, die öffentliche Verwaltung bei 32 Prozent, die Wirtschaft bei 39 Prozent und die Bevölkerung bei 29 Prozent.

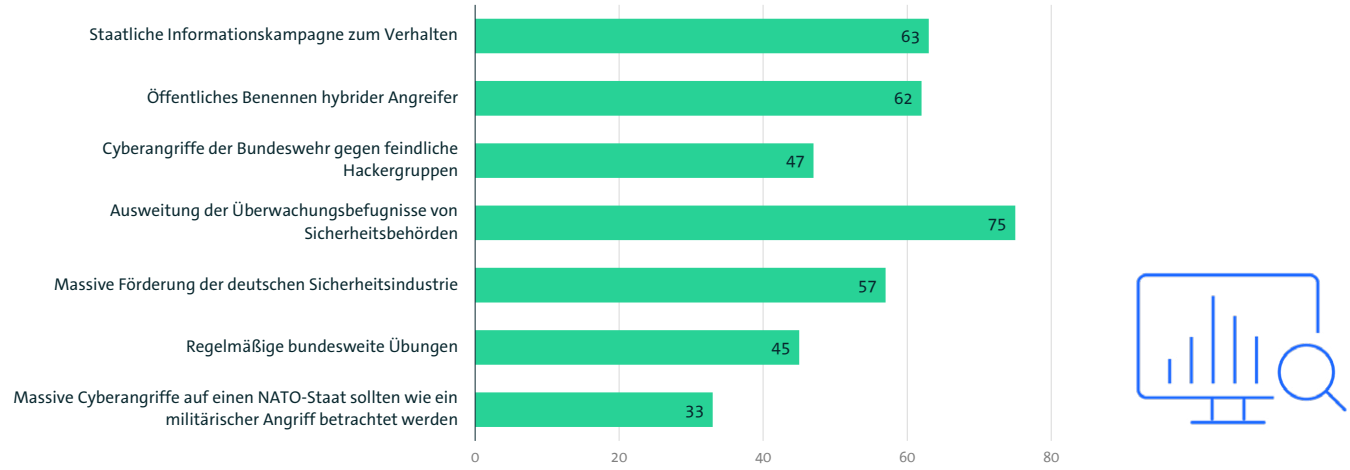
Diese Angaben verdeutlichen, dass die Unternehmen in Deutschland vor allem auf staatliche Sicherheitskräfte vertrauen, während andere Akteure als weniger gut vorbereitet wahrgenommen werden.

Insgesamt geben 57 Prozent der Unternehmen an, darauf zu vertrauen, dass Sicherheitsbehörden sie im Fall eines hybriden Angriffs schützen.

> **Nur Polizei und Bundeswehr gelten als gut vorbereitet** – allerdings auch nur mit Werten von 60 bzw. 52 Prozent.

## 4.2 Politische Maßnahmen

### Was sollte die Politik tun, damit Deutschland besser auf hybride Angriffe vorbereitet ist?




in Prozent

Basis: Alle befragten Personen ab 16 Jahren (n=1.263) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2026

Abbildung 20: Politische Maßnahmen zur besseren Vorbereitung Deutschlands auf hybride Angriffe (aus Sicht der Bevölkerung)

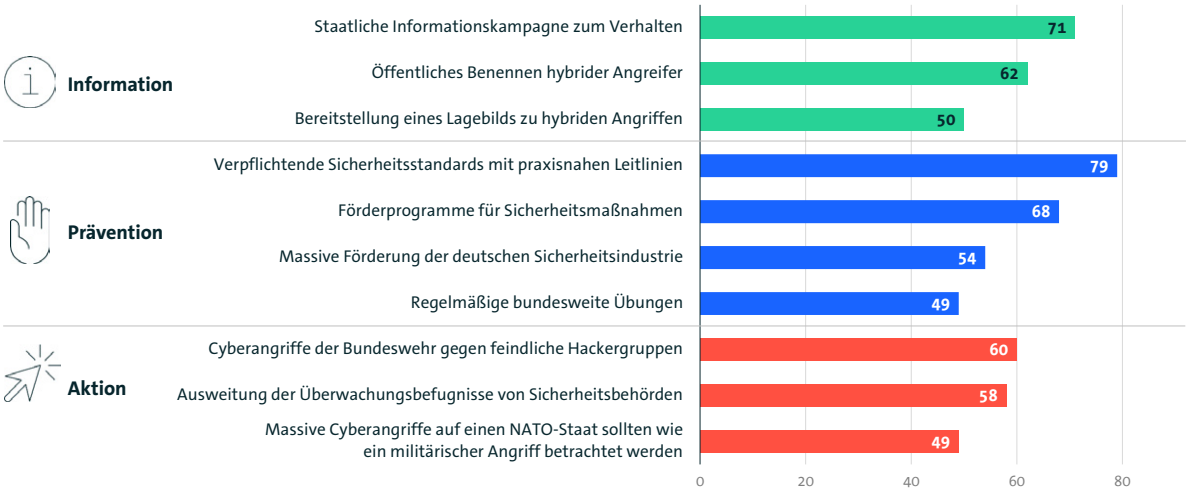
### Mehr Schutz, mehr Informationen, mehr Übungen – Bürgerinnen und Bürger fordern konsequente Maßnahmen für ein widerstandsfähiges Deutschland

Die Befragten sehen vor allem Handlungsbedarf bei staatlichen Maßnahmen, um Deutschland besser auf hybride Angriffe vorzubereiten. An erster Stelle steht die Ausweitung der Überwachungsbefugnisse von Sicherheitsbehörden, die 75 Prozent unterstützen.

Eine staatliche Informationskampagne zum Verhalten in Krisen halten 63 Prozent für wichtig, das öffentliche Benennen hybrider Angreifer 62 Prozent. 57 Prozent sprechen sich für eine stärkere Förderung der deutschen Sicherheitsindustrie aus.

Regelmäßige bundesweite Übungen zur Krisenvorsorge finden 45 Prozent wichtig, während 47 Prozent Cyberangriffe der Bundeswehr gegen feindliche Hackergruppen befürworten. Weniger Zustimmung gibt es für die Betrachtung massiver Cyberangriffe auf einen NATO-Staat wie einen militärischen Angriff, hier stimmen nur 33 Prozent zu.

## Was sollte die Politik tun, damit Deutschland besser auf hybride Angriffe vorbereitet ist?




in Prozent

Basis: Alle befragten Unternehmen (n=604) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2026

Abbildung 21: Maßnahmen, die die Politik ergreifen sollte, damit Deutschland besser auf hybride Angriffe vorbereitet ist (Unternehmen)

## Was die Politik jetzt tun muss

Die Unternehmen erwarten von der Politik ein umfassendes Maßnahmenpaket, um Deutschland gegen hybride Angriffe zu stärken. Im Bereich Information wünschen sich 71 Prozent eine staatliche Kampagne zum Verhalten in Krisensituationen, 62 Prozent ein öffentliches Benennen hybrider Angreifer und 50 Prozent ein Lagebild zu solchen Angriffen.

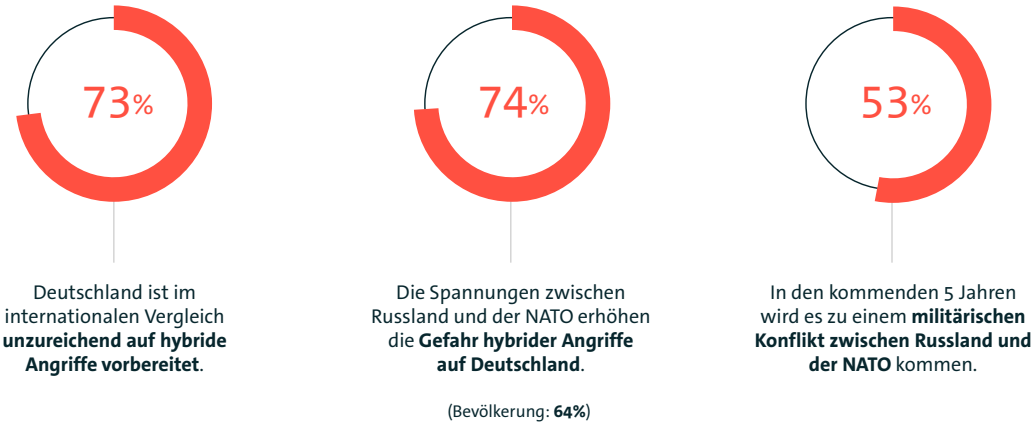
Zur Prävention sprechen sich 79 Prozent der Unternehmen für verpflichtende Sicherheitsstandards mit praxisnahen Leitlinien aus. Zudem erwarten 68 Prozent Förderprogramme für Sicherheitsmaßnahmen, 54 Prozent eine massive Förderung der deutschen Sicherheitsindustrie und 49 Prozent regelmäßige bundesweite Übungen mit Bevölkerung und Unternehmen.

Bei konkreten Maßnahmen halten 60 Prozent Cyberangriffe der Bundeswehr gegen feindliche Hackergruppen für sinnvoll, 58 Prozent die Ausweitung der Überwachungsbefugnisse von Sicherheitsbehörden und 49 Prozent vertreten die Ansicht, dass massive Cyberangriffe auf einen NATO-Staat wie ein militärischer Angriff behandelt werden sollten.

Diese Ergebnisse verdeutlichen, dass Unternehmen sowohl präventive als auch reaktive Maßnahmen erwarten, um die Resilienz von Verwaltung, Wirtschaft, Bevölkerung und kritischer Infrastruktur deutlich zu erhöhen.

## 4.3 Sicherheitspolitische Grundüberzeugungen

### Inwieweit treffen die folgenden Aussagen Ihrer Meinung nach zu?




Basis: Alle befragten Unternehmen (n=604) bzw. alle befragten Personen ab 16 Jahren (n=1.263) | Prozentwerte für »Trifft voll und ganz zu« und »Trifft eher zu« | Quelle: Bitkom Research 2026

Abbildung 22: Einschätzungen zur Bedrohungslage (Unternehmen und Bevölkerung)

### Sicherheitslage verschärft sich weiter

Die Einschätzungen der Unternehmen und der Bevölkerung zeichnen ein deutliches Bild einer angespannten und sich weiter zuspitzenden Sicherheitslage. 73 Prozent der Unternehmen halten Deutschland im internationalen Vergleich für unzureichend auf hybride Angriffe vorbereitet. In der Bevölkerung teilt mit 64 Prozent ebenfalls eine klare Mehrheit diese Einschätzung.

Auch mit Blick auf die geopolitische Lage ist die Wahrnehmung eindeutig: 74 Prozent der Unternehmen sehen durch die Spannungen zwischen Russland und der NATO eine erhöhte Gefahr hybrider Angriffe auf Deutschland. In der Bevölkerung ist dieser Wert mit 77 Prozent sogar noch etwas höher.

Besonders bemerkenswert ist zudem die Einschätzung eines möglichen militärischen Konflikts zwischen Russland und der NATO in den kommenden fünf Jahren. 53 Prozent der Unternehmen halten ein solches Szenario für wahrscheinlich, in der Bevölkerung sind es 49 Prozent.

Insgesamt zeigt sich damit ein breiter gesellschaftlicher Konsens über die Verschärfung der Sicherheitslage. Hybride Bedrohungen werden nicht als Randphänomen wahrgenommen, sondern als Teil einer realen geopolitischen Zuspitzung.

# 5 Fazit

Die Ergebnisse des Studienberichts zeigen: Hybride Angriffe werden von Wirtschaft und Bevölkerung als reale und wachsende Bedrohung wahrgenommen.
Über 80 Prozent erwarten eine ernsthafte Krise infolge hybrider Angriffe. Gleichzeitig besteht eine deutliche Lücke zwischen Risikobewusstsein und tatsächlicher Vorbereitung, die es zu schließen gilt.

Unternehmen sehen insbesondere Energieversorgung, Finanzwesen und Telekommunikation als empfindliche Schwachstellen. Ein Ausfall digitaler Infrastruktur hätte unmittelbare wirtschaftliche Folgen. Denn ohne Internet könnten Betriebe im Schnitt nur 20 Stunden weiterarbeiten und jedes fünfte Unternehmen gar nicht. Trotz dieser Abhängigkeit und trotz der Erwartung schwerer Krisen geben nur 12 Prozent an, »eher gut vorbereitet« zu sein.

Auch in der Bevölkerung ist das Problembewusstsein hoch, die Vorsorge jedoch begrenzt: Nur 15 Prozent halten ihren Haushalt für gut vorbereitet, fast ein Fünftel hat keinerlei Maßnahmen getroffen. Besonders gefürchtet werden Ausfälle bei Energie und Banken.

Zugleich zeigt sich ein Informationsdefizit. Während 80 Prozent der Unternehmen im Ernstfall auf staatliche Stellen vertrauen, fühlt sich nur knapp jedes fünfte ausreichend informiert. Auch zwei Drittel der Bevölkerung sehen sich nicht ausreichend informiert.

Hinzu kommt eine deutlich verschärfte sicherheitspolitische Grundwahrnehmung:
73 Prozent der Unternehmen und 64 Prozent der Bevölkerung halten Deutschland im internationalen Vergleich für unzureichend vorbereitet. Rund drei Viertel sehen durch die Spannungen zwischen Russland und der NATO eine erhöhte Gefahr hybrider Angriffe auf Deutschland. Mehr als die Hälfte der Unternehmen und knapp die Hälfte der Bevölkerung halten in den kommenden fünf Jahren sogar einen militärischen Konflikt zwischen Russland und der NATO für möglich.

Insgesamt zeigt sich damit eine sicherheitspolitische Spannungslage, wie sie es so in Deutschland noch nie gab: eine akute Bedrohungswahrnehmung, sogar die Erwartung eines potenziellen Konflikts bei der gleichzeitigen Selbsteinschätzung von Bevölkerung und Unternehmen, dass die Vorbereitungen auf ein Krisenszenario stark verbessert werden könnten. Eine klare Erwartungshaltung sowie Vertrauen, Vorsorge zu treffen und in der Krise handlungsfähig zu sein, zeigt sich vor allem gegenüber staatlichen Akteuren.

Die Ergebnisse der Studie sind damit auch ein Spiegel des Zustands der gesamtgesellschaftlichen Resilienz in Deutschland insgesamt. Sie zeigen eine deutlich gestiegene Bedrohungswahrnehmung in Wirtschaft und Bevölkerung, bei gleichzeitig erkennbaren Mängeln bei der Vorbereitung, Information und struktureller Krisenvorsorge. Unabhängig von unterschiedlichen Bewertungen im Detail verdeutlichen die Ergebnisse aus Sicht des Bitkom damit den dringenden Handlungsbedarf, die Widerstandsfähigkeit Deutschlands gegenüber hybriden Bedrohungen deutlich zu stärken. Besonders die Vorbereitung auf den Ausfall kritischer digitaler Infrastrukturen wird dabei zu einer zentralen Herausforderung für alle Akteure. Prävention, verbindliche Standards, bessere Informationsstrukturen sowie koordinierte Übungen zwischen staatlichen Stellen und Wirtschaft sind entscheidende Hebel, um die Resilienz nachhaltig zu erhöhen. Zugleich unterstreichen die Ergebnisse, dass Krisenvorsorge eine gesamtgesellschaftliche Aufgabe ist. Staat, Wirtschaft und Bevölkerung tragen gemeinsam Verantwortung für Vorbereitung und Krisenfähigkeit.

Der Bitkom wird diese Debatte weiterhin aktiv begleiten und mit Studien, Dialogformaten und Handlungsempfehlungen zur Stärkung der Resilienz beitragen. Eine Wiederholung der Studie in den kommenden Jahren soll zudem ermöglichen, Entwicklungen sichtbar zu machen, Fortschritte zu messen und die Wirksamkeit ergriffener Maßnahmen besser zu bewerten.

# 6 Methodik

## Befragung 2025/2026 | Unternehmen

| 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 |
| **Zielpersonen** | Geschäftsführung und Vorstand sowie Führungskräfte im Bereich Unternehmenssicherheit und Informationsschutz |
| **Stichprobengröße** | n=604 |
| **Befragungszeitraum** | KW 47 2025 bis KW 3 2026 |
| **Gewichtung** | Repräsentative Gewichtung des Datensatzes auf Grundlage des aktuellen Unternehmensregisters des Statistischen Bundesamtes |
| **Statistische Fehlertoleranz** | +/- 4 Prozent in der Gesamtstichprobe |

## Befragung 2025/2026 | Bevölkerung

| Auftraggeber | Bitkom |
|---|---|
| **Methodik** | Computergestützte telefonische Befragung/ Computer Assisted Telephone Interview (CATI) |
| **Grundgesamtheit** | Personen in Deutschland ab 16 Jahren |
| **Stichprobengröße** | n=1.263 |
| **Befragungszeitraum** | KW 51 2025 bis KW 2 2026 |
| **Gewichtung** | Repräsentative Gewichtung des Datensatzes auf Grundlage auf Grundlage amtlicher Bevölkerungsstatistik |
| **Statistische Fehlertoleranz** | +/- 3 Prozent in der Gesamtstichprobe |

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

Wissenschaftliche Leitung
Bettina Lange

Ansprechpartner
Nemo Buschmann
Felix Kuhlenkamp

Redaktion
Alissa Geffert



DOI
10.64022/2026-hybride-angriffe

Stromausfälle durch zerstörte Leitungen, gezielte Sabotage von Internetkabeln, oder Ransomware in Fabriken: Hybride Angriffe sind Realität – und sie treffen auf eine Wirtschaft und Gesellschaft, die darauf bislang nur unzureichend vorbereitet sind. Unternehmen sind stark von stabilen Infrastrukturen abhängig; fällt das Internet aus, können sie ihren Betrieb im Schnitt nur 20 Stunden aufrechterhalten, jedes fünfte müsste sofort schließen. Ein ähnliches Bild zeigt sich in der Bevölkerung: 82 Prozent erwarten eine ernsthafte Krise infolge hybrider Angriffe, doch nur 15 Prozent halten ihren Haushalt für vorbereitet. Besonders gefürchtet werden Ausfälle bei Energieversorgung und Finanzwesen. Der Studienbericht basiert auf zwei repräsentativen CATI-Befragungen im Auftrag des Bitkom unter 604 Unternehmen sowie 1.263 Personen ab 16 Jahren in Deutschland.

DOI
10.64022/2026-hybride-angriffe

bitkom