Cyberkriminalität – Bevölkerungsumfrage zu Wahrnehmung, Erfahrungen und Schutzverhalten

Bitkom-Studie 2025

bitkom

Cyberkriminalität – Bevölkerungsumfrage zu Wahrnehmung, Erfahrungen und Schutzverhalten

Bitkom-Studie 2025

DOI
10.64022/2025-Cyberkriminalität

Wichtigste Erkenntnisse

Diese Studie untersucht, wie die Bevölkerung in Deutschland Cyberkriminalität wahrnimmt, welche persönlichen Erfahrungen sie damit macht und welche Erwartungen sie an Schutz- und Präventionsmaßnahmen hat. Grundlage ist eine repräsentative Befragung von 1.115 Personen ab 16 Jahren in Deutschland im Jahr 2025.

- **Bedrohungslage:** Während nur 37 % die Gefahr für sich persönlich als hoch einschätzen, sehen 70 % ein hohes Risiko für Deutschland insgesamt. Als größte Gefahrenquellen gelten ausländische Geheimdienste (78 %), organisierte Kriminalität (67 %) und Extremisten (59 %). Russland (98 %) und China (84 %) werden als wichtigste Herkunftsländer von Angriffen genannt. Zwei Drittel halten Deutschland für unzureichend auf Cyberangriffe vorbereitet.
- **Betroffenheit:** 61 % der Internetnutzenden waren in den vergangenen zwölf Monaten Opfer von Cyberkriminalität – vor allem durch Betrug beim Onlinehandel (36 %), Datendiebstahl (30 %) oder Schadsoftware (24 %). Der durchschnittliche Schaden liegt bei 219 Euro. Nur ein Viertel der Betroffenen erstattet Anzeige, die meisten reagieren im privaten Umfeld.
- **Prävention:** Mehr als die Hälfte investiert weniger als 5 Euro monatlich in Sicherheitssoftware. Nur 7 % verfügen über eine Cyberversicherung. Zwar aktualisieren 65 % ihre Geräte regelmäßig und 50 % nutzen Zwei-Faktor-Authentifizierung, dennoch verwenden viele weiterhin unsichere Passwörter oder mehrfach identische Zugangsdaten. Über die Hälfte weiß nicht, an wen man sich im Ernstfall wenden kann.
- **Gesellschaftliche Erwartungen:** 91 % fordern mehr Polizeipräsenz im digitalen Raum, 81 % härtere Strafen und 76 % zusätzliche Befugnisse für Sicherheitsbehörden. 70 % wünschen staatliche Aufklärung und Bildungsangebote.
- **Cyberkrieg:** 61 % der Bevölkerung haben Angst vor einem Cyberkrieg, 71 % erwarten, dass Kriege künftig auch digital geführt werden. Zwei Drittel sprechen sich dafür aus, Cyberangriffe wie militärische Angriffe zu behandeln. Besonders große Sorgen gibt es um die Sabotage von Unterseekabeln: 80 % wollen zusätzliche Kabel, 77 % spezielle Reparatureinheiten und 69 % die Einstufung als militärischer Angriff.

Bitkom-Bewertung

Die Ergebnisse zeigen: Cyberkriminalität betrifft große Teile der Bevölkerung unmittelbar. Mehr als jede und jeder Zweite war bereits Opfer, viele erleiden finanzielle Schäden, und das Vertrauen in die Abwehrbereitschaft staatlicher Stellen ist gering. Gleichzeitig investieren die Menschen bislang nur wenig in ihre eigene Sicherheit.
Die Forderungen nach mehr Polizeipräsenz im digitalen Raum, härteren Strafen und besserer Aufklärung zeigen, dass die Gesellschaft entschlossenes Handeln erwartet. Auch die Sorge vor Cyberkrieg und gezielten Angriffen auf kritische Infrastrukturen wie Unterseekabel unterstreicht den Handlungsdruck. Cybersicherheit muss deshalb zu einer zentralen Priorität für Staat, Wirtschaft und Gesellschaft werden – nicht nur zur Abwehr aktueller Bedrohungen, sondern auch als Grundlage für Vertrauen in die digitale Zukunft.

Inhalt

Abbildungen

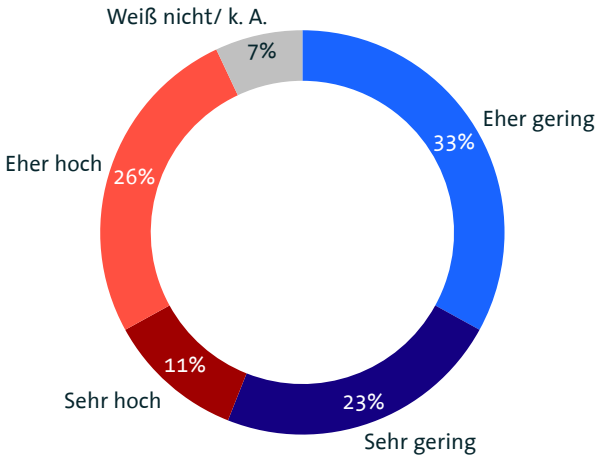
1 Wahrnehmung von Bedrohungen

1 Wahrnehmung von Bedrohungen

Wie schätzt die Bevölkerung Cyberrisiken ein – im persönlichen Umfeld und auf gesamtgesellschaftlicher Ebene? Die Ergebnisse zeigen: Die wahrgenommene Bedrohung für Deutschland insgesamt ist deutlich ausgeprägter als die für das eigene Umfeld. Besonders häufig genannt werden ausländische Geheimdienste, organisierte Kriminalität und Extremismus als zentrale Gefahrenquellen. Russland und China gelten dabei als Hauptakteure digitaler Angriffe. Zugleich wird die Vorbereitung staatlicher Institutionen mehrheitlich kritisch bewertet.

1.1 Individuelle Bedrohungseinschätzung

Wie hoch schätzen Sie die Bedrohung durch Cyberkriminalität für sich und Ihre Familie ein?



Basis: Alle Befragten (n=1.115) | Abweichungen von 100 Prozent sind rundungsbedingt | Quelle: Bitkom Research 2025

Abbildung 1: Wahrnehmung von Cyberkriminalität im privaten Umfeld

Die wahrgenommene Bedrohung durch Cyberkriminalität ist in der Bevölkerung unterschiedlich stark ausgeprägt. Insgesamt 37 Prozent der Befragten schätzen das Risiko für sich und ihre Familie als eher hoch (26 Prozent) oder sehr hoch (11 Prozent) ein. Auf der anderen Seite empfinden 33 Prozent die Bedrohung als eher gering, während 23 Prozent sogar von einer sehr geringen Gefahr ausgehen. Damit lässt sich feststellen, dass ein größerer Teil der Bevölkerung die Gefährdung durch Cyberkriminalität als gering einstuft. Gleichzeitig sieht mehr als ein Drittel ein hohes Bedrohungspotenzial. Die Ergebnisse zeigen, dass das Sicherheitsgefühl in der Bevölkerung unterschiedlich ausgeprägt ist – mit einer Mehrheit, die sich vergleichsweise wenig bedroht fühlt.

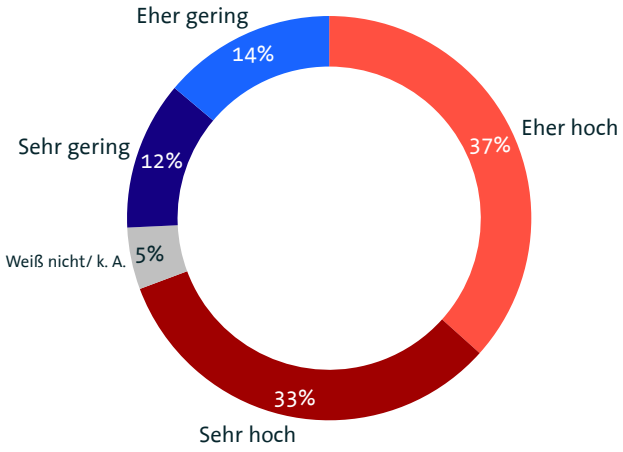
Schaut man sich zusätzlich die Altersgruppen an, zeigt sich: Vor allem Jüngere sehen persönlich Gefahren durch Cyberkriminalität. So bewerten 50 Prozent der 16- bis 29-Jährigen die Bedrohung für sich und ihre Familie als hoch oder sehr hoch. In der Altersgruppe der 30- bis 49-Jährigen sind es 41 Prozent. Unter den 50- bis 64-Jährigen liegt der Anteil bei 37 Prozent. Besonders niedrig fällt die Bedrohungseinschätzung bei den über 65-Jährigen aus: Hier sehen lediglich 26 Prozent eine hohe persönliche Gefahr durch Cyberkriminalität.

Mehr als jede dritte befragte Person

(37 Prozent) empfindet die Bedrohung durch Cybercrime für sich und ihre Familie als hoch.

1.2 Einschätzung der Cybergefahr für Deutschland

Wie hoch schätzen Sie die Bedrohung durch Cyberkriminalität **für Deutschland insgesamt** ein?



Basis: Alle Befragten (n=1.115) | Abweichungen von 100 Prozent sind rundungsbedingt | Quelle: Bitkom Research 2025

Abbildung 2: Einschätzung der Bedrohung durch Cyberkriminalität für Deutschland insgesamt

Die Bedrohung durch Cyberkriminalität wird aus Sicht der Bevölkerung für Deutschland insgesamt deutlich ernster eingeschätzt als für das eigene Umfeld. Insgesamt 70 Prozent der Befragten sehen ein hohes Risiko – 37 Prozent stufen es als »eher hoch« und weitere 33 Prozent als »sehr hoch« ein. Nur 14 Prozent empfinden die Bedrohung als »eher gering«, 12 Prozent als »sehr gering«. Diese Ergebnisse zeigen: Während sich viele Menschen persönlich relativ sicher fühlen, herrscht auf gesellschaftlicher Ebene ein starkes Bewusstsein für die Relevanz und Brisanz digitaler Gefahren.

Die hohe Zustimmung zu einer ausgeprägten Bedrohungseinschätzung unterstreicht die gesellschaftliche Wahrnehmung von Cyberkriminalität als ernst zu nehmendes Risiko für das Land insgesamt.

Cyberkriminalität als nationales Risiko

70 Prozent der Befragten sehen eine hohe Bedrohung für Deutschland insgesamt.

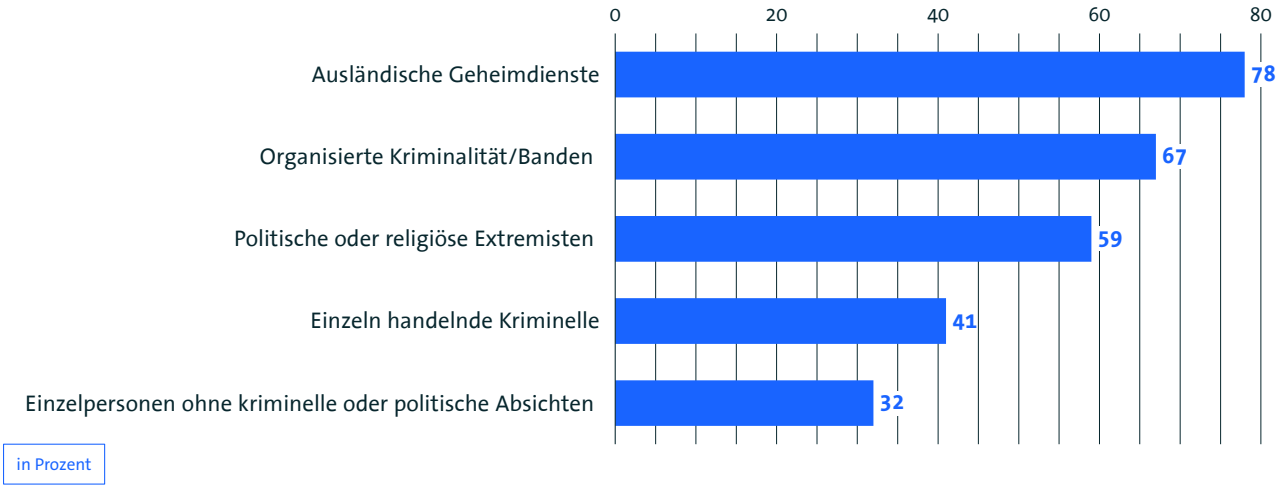
1.3 Bedrohungsquellen nach Akteuren

Von wem geht nach Einschätzung der Menschen die größte Bedrohung für die Cybersicherheit in Deutschland aus? Ganz oben stehen ausländische Geheimdienste: 78 Prozent der Befragten halten deren Einfluss für »sehr groß« oder »eher groß«. Dahinter folgt die organisierte Kriminalität bzw. Banden mit 67 Prozent sowie politische oder religiöse Extremisten mit 59 Prozent. Weniger bedrohlich werden einzelne Täter wahrgenommen. So sehen 41 Prozent eine große Gefahr durch einzeln handelnde Kriminelle. Einzelpersonen ohne kriminelle oder politische Absichten gelten nur für 32 Prozent als relevante Bedrohung.

Die Ergebnisse verdeutlichen, dass die wahrgenommene Bedrohung für die Cybersicherheit in Deutschland insbesondere staatlichen und organisierten Akteuren zugeschrieben wird. Besonders häufig werden ausländische Geheimdienste sowie kriminelle Netzwerke als Risikofaktoren genannt.

> Staatliche und organisierte Akteure gelten aus Sicht der Bevölkerung als **größte Bedrohung für die Cybersicherheit** – allen voran ausländische Geheimdienste und kriminelle Netzwerke.

Wie groß ist die Bedrohung für die Cybersicherheit in Deutschland, die von folgenden **Akteuren** ausgeht?



Basis: Alle Befragten (n=1.115) | Prozentwerte für »sehr große« oder »eher große« Bedrohung | Quelle: Bitkom Research 2025

Abbildung 3: Wahrgenommene Bedrohung für die Cybersicherheit in Deutschland durch verschiedene Akteure

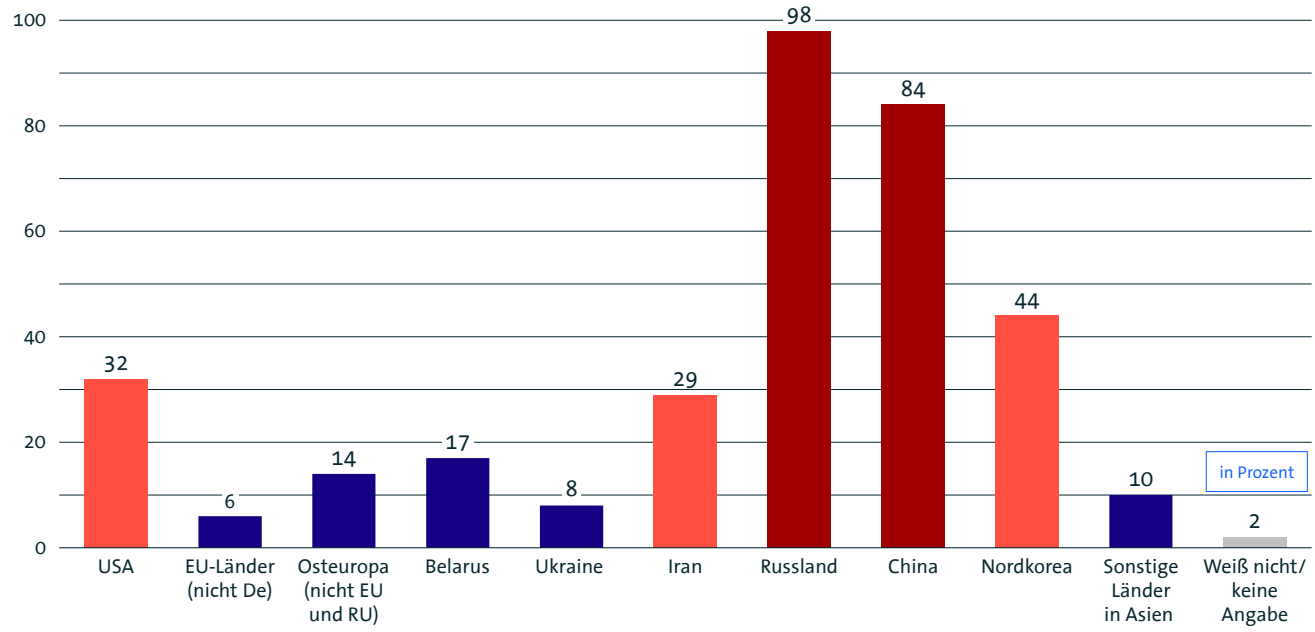
1.4 Bedrohungsquellen nach Ländern

Russland und China gelten aus Sicht der Bevölkerung als die mit Abstand größten Quellen für Cyberbedrohungen gegen Deutschland. 98 Prozent der Befragten nennen Russland, 84 Prozent China. Damit stufen nahezu alle Befragten Russland als ernsthafte Gefahr für die Cybersicherheit ein.

Mit deutlichem Abstand folgt Nordkorea, das von 44 Prozent als Bedrohung genannt wird. Auf den weiteren Plätzen liegen die USA mit 32 Prozent, Iran (29 Prozent), Belarus (17 Prozent) sowie Osteuropa außerhalb von EU und Russland (14 Prozent).

Rund ein Drittel der Befragten nennt die USA. Die Einschätzungen zeigen, dass sich das Bedrohungsbild in der digitalen Welt zunehmend differenziert.

Von welchen **Ländern** geht eine große Bedrohung für die Cybersicherheit in Deutschland aus?



Basis: Alle Befragten (n=1.115) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2025

Abbildung 4: Länder, von denen aus laut Bevölkerung eine große Bedrohung für die Cybersicherheit in Deutschland ausgeht

1.5 Bewertung der staatlichen Abwehrbereitschaft

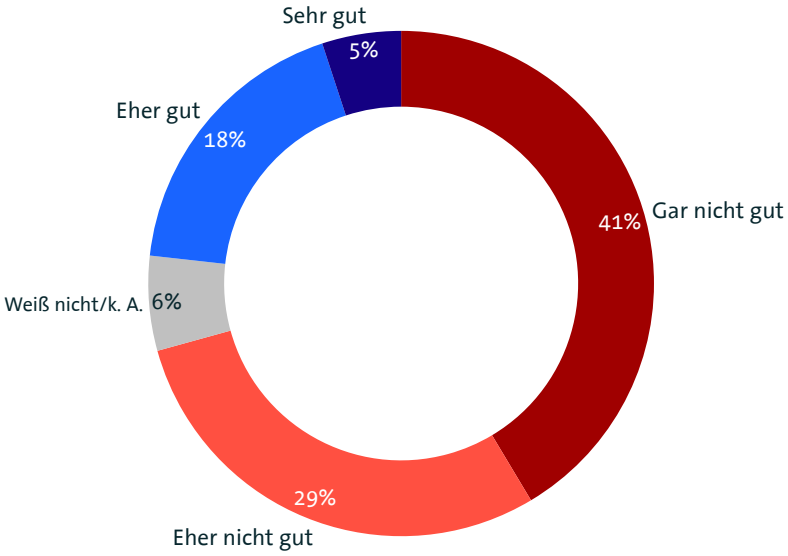
Deutschland gilt nach Meinung vieler Menschen als unzureichend auf Cyberangriffe vorbereitet. Nur 23 Prozent der Befragten halten die öffentliche Verwaltung sowie Institutionen wie Polizei, Bundeswehr oder andere Behörden für »sehr gut« (5 Prozent) oder »eher gut« (18 Prozent) vorbereitet.

Demgegenüber äußern sich deutlich mehr Befragte kritisch: 29 Prozent halten Deutschland für »eher nicht gut« und sogar 41 Prozent für »gar nicht gut« vorbereitet.

Die Zahlen zeigen ein deutliches Stimmungsbild: Die Bevölkerung traut staatlichen Institutionen im digitalen Raum offenbar nur begrenzte Widerstandsfähigkeit zu. Im Kontext zunehmender Cyberbedrohungen stellt sich die Frage, ob bestehende Strukturen und Schutzmechanismen den Anforderungen einer modernen Cybersicherheitslage gerecht werden.

> **Mehr als zwei Drittel** der Bevölkerung halten Deutschland für nicht ausreichend auf Cyberangriffe vorbereitet

Wie gut ist Deutschland – also die öffentliche Verwaltung, aber auch Behörden wie Polizei, Bundeswehr etc. – Ihrer Meinung nach **auf Cyberangriffe vorbereitet**?



in Prozent

Basis: Alle Befragten (n=1.115) | Abweichungen von 100 Prozent sind rundungsbedingt | Quelle: Bitkom Research 2025

Abbildung 5: Einschätzung der Fähigkeit Deutschlands, Cyberangriffe abzuwehren

2 Persönliche Betroffenheit

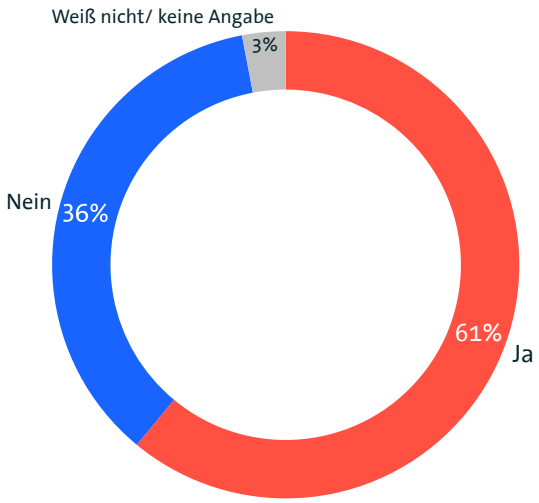
2 Persönliche Betroffenheit

2.1 Eigene Erfahrungen mit Cyberkriminalität

Ein Großteil der Internetnutzerinnen und -nutzer war in den vergangenen zwölf Monaten direkt von Cyberkriminalität betroffen. 61 Prozent berichten von eigenen Erfahrungen, während 36 Prozent keine Vorfälle angaben. Besonders häufig geht es dabei um Betrug beim Onlinehandel (36 Prozent), das Ausspähen persönlicher Informationen wie Passwörter (30 Prozent) oder die Infektion von Computern und Smartphones mit Schadsoftware (24 Prozent). Seltener genannt werden Angriffe wie das Ausspionieren von Onlinezugängen, Betrug als Verkäufer, Identitätsdiebstahl oder Bedrohungen im Netz.

Insgesamt zeigt sich: Cyberkriminalität ist für viele Menschen kein abstraktes Risiko, sondern eine direkte Alltagserfahrung – vor allem in Form von Betrug und Datenmissbrauch.

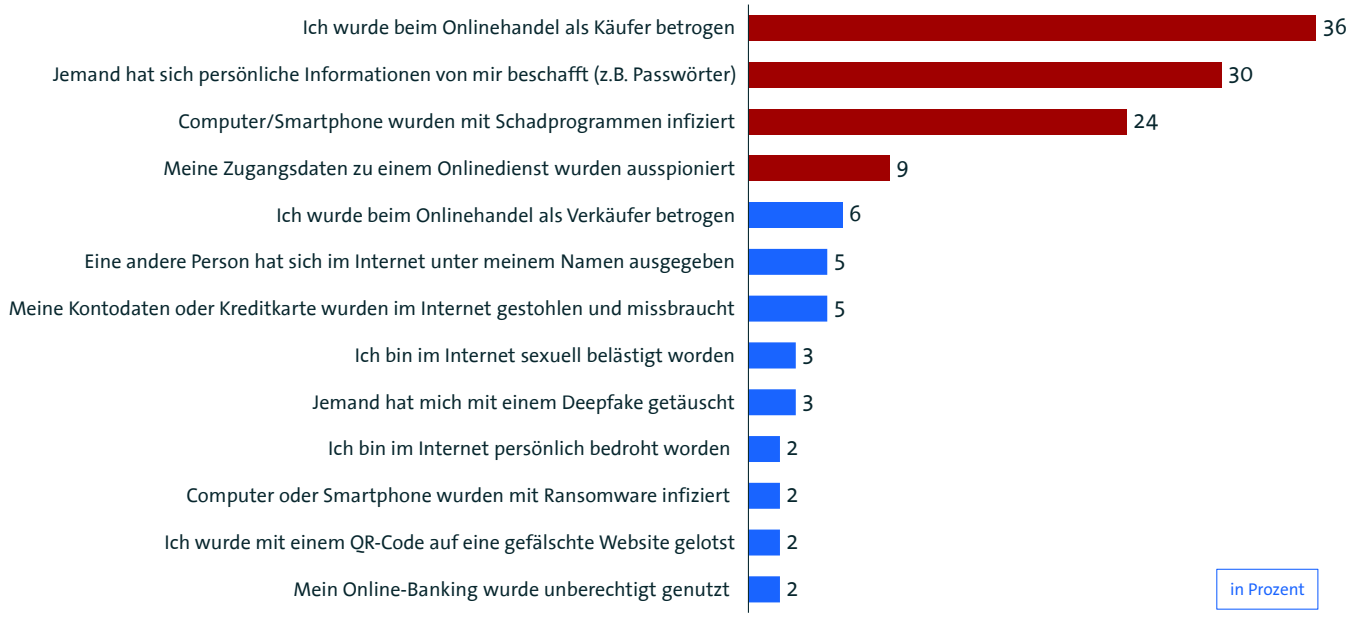
Haben Sie in den vergangenen 12 Monaten Erfahrungen mit Cyberkriminalität im Internet gemacht?



Basis: Internetnutzerinnen und -nutzer (n=1.021) | Quelle: Bitkom Research 2025

Abbildung 6: Erfahrungen mit Cyberkriminalität im Internet (letzte 12 Monate)

Welche der folgenden Erfahrungen mit Cyberkriminalität haben Sie persönlich in den letzten 12 Monaten im Internet gemacht?



Basis: Internetnutzerinnen und -nutzer (n=1.021) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2025

Abbildung 7: Arten persönlicher Erfahrungen mit Cyberkriminalität (letzte 12 Monate)

2.2 Finanzielle Auswirkungen

Cyberkriminalität verursacht für viele Betroffene nicht nur immaterielle, sondern auch finanzielle Schäden. Im Durchschnitt beläuft sich der Schaden auf 219 Euro pro Opfer innerhalb von zwölf Monaten.

Für 60 Prozent der Betroffenen entstand ein persönlicher Schaden, der im Mittel 181 Euro beträgt. In 4 Prozent der Fälle wurde der Schaden durch Dritte getragen – etwa durch Banken oder Onlinehändler. Hier liegt der durchschnittliche Betrag mit 609 Euro deutlich höher.

Nicht in allen Fällen hatte Cyberkriminalität finanzielle Folgen: 25 Prozent der Opfer gaben an, dass ihnen kein Schaden entstanden ist. 13 Prozent machten keine oder keine konkreten Angaben. Insgesamt zeigt sich, dass ein Großteil der Betroffenen durch Cyberangriffe auch finanziell belastet wird.

60 %

Der Betroffenen erleiden einen finanziellen Schaden durch Cybercrime, im Schnitt sind es **181 Euro.**

Sie haben angegeben, dass Sie Opfer von Cyberkriminalität geworden sind. Ist dabei ein **finanzieller Schaden** entstanden?

219 €

Durchschnittlicher Schaden durch **Cybercrime**

Basis: Befragte, die in den vergangenen 12 Monaten Opfer von Cyberkriminalität wurden (n=627) | Quelle: Bitkom Research 2025

Abbildung 8: Durchschnittlicher Schaden durch Cyberkriminalität

2.3 Umgangsweisen mit Cyberkriminalität

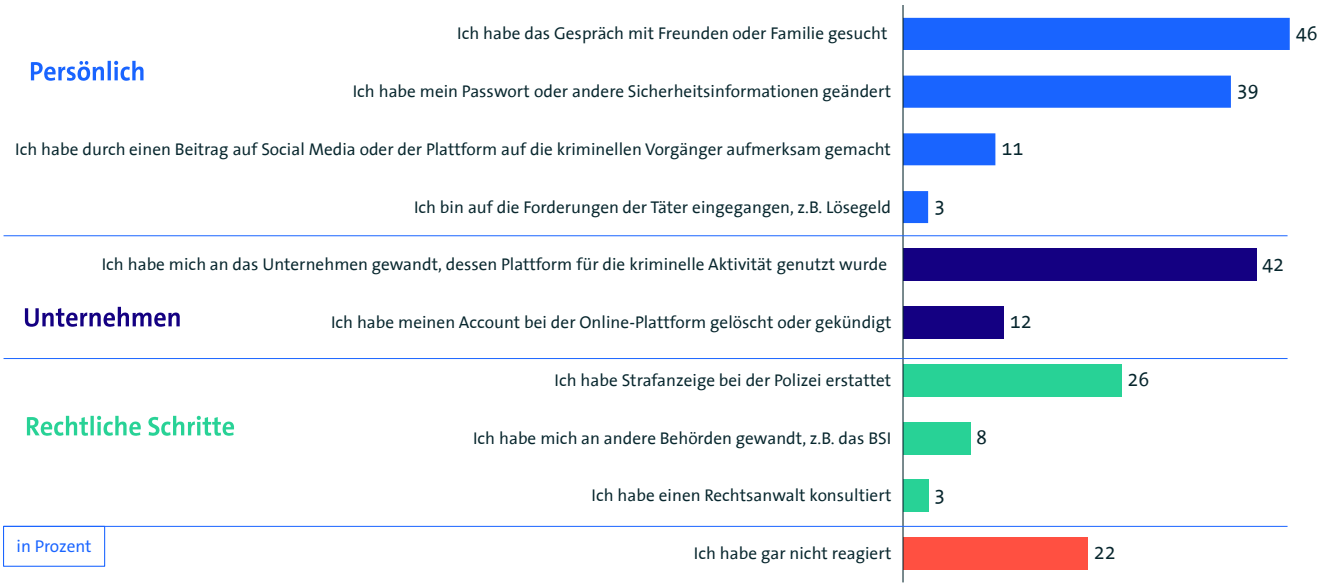
Nur eine Minderheit der von Cyberkriminalität Betroffenen wendet sich an offizielle Stellen. Rund ein Viertel (26 Prozent) hat Strafanzeige bei der Polizei erstattet, 8 Prozent suchten Hilfe bei anderen Behörden wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und lediglich 3 Prozent konsultierten einen Rechtsanwalt. Damit bleibt ein Großteil der Vorfälle außerhalb der offiziellen Statistiken, was auf eine hohe Dunkelziffer hinweist.

Häufiger reagieren Betroffene im persönlichen Umfeld oder durch eigenes Verhalten. Fast die Hälfte (46 Prozent) suchte das Gespräch mit Familie oder Freunden, 39 Prozent änderten Passwörter oder andere Sicherheitsinformationen, 11 Prozent machten über Social Media oder Plattformen auf die Vorfälle aufmerksam, und 3 Prozent gingen sogar auf Forderungen der Täter wie Lösegeldzahlungen ein. Zudem wandten sich 42 Prozent an das betroffene Unternehmen, während 12 Prozent ihren Account dort löschten oder kündigten. Etwa ein Fünftel (22 Prozent) verzichtete ganz auf eine Reaktion.

26 %

Nur rund ein Viertel erstattet Anzeige bei der Polizei. Das zeigt: **Nur eine Minderheit wendet sich bei Cybercrime an Polizei oder Behörden** – die meisten reagieren im privaten Umfeld, jeder Fünfte bleibt ganz untätig.

Wie haben Sie auf die kriminellen Vorfälle im Internet **reagiert**?



Basis: Befragte, die in den vergangenen 12 Monaten Opfer von Cyberkriminalität wurden (n=627) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2025

Abbildung 9: Reaktionen der Betroffenen auf kriminelle Vorfälle im Internet

3 Schutz- und Präventions-maßnahmen

3 Schutz- und Präventionsmaßnahmen

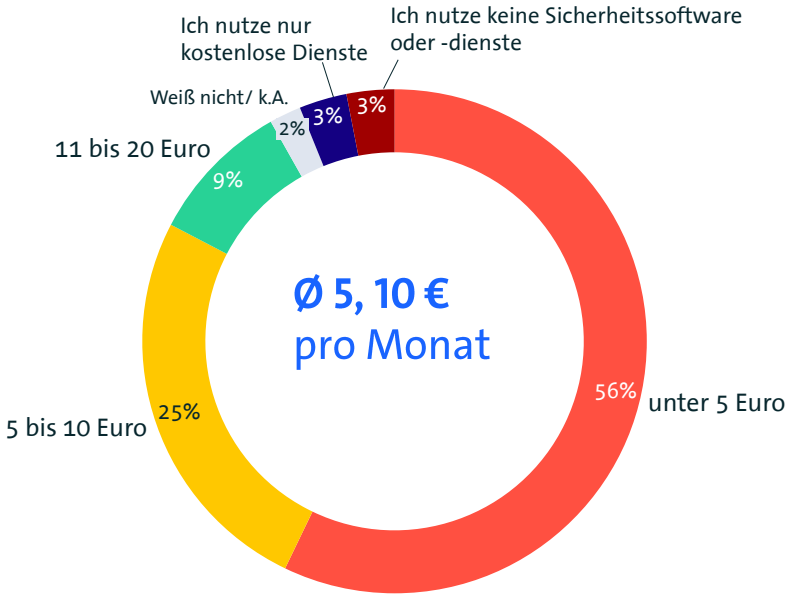
3.1 Private Investitionen in Cybersicherheit

Die meisten Internetnutzerinnen und -nutzer investieren nur geringe Beträge in Sicherheitssoftware oder -dienste. 56 Prozent geben weniger als 5 Euro pro Monat aus, weitere 25 Prozent liegen im Bereich von 5 bis 10 Euro. Nur 9 Prozent zahlen zwischen 11 und 20 Euro, während höhere Ausgaben kaum vorkommen. Ein kleiner Teil nutzt ausschließlich kostenlose Angebote (2 Prozent) oder verzichtet gänzlich auf entsprechende Software und Dienste (3 Prozent). Weitere 3 Prozent machten keine Angaben.

Insgesamt belaufen sich die durchschnittlichen Ausgaben für Sicherheitssoftware und -dienste auf 5,10 Euro pro Monat. Damit zeigt sich: Ein Großteil der Befragten setzt zwar auf Schutzmaßnahmen, ist jedoch nur in begrenztem Umfang bereit, dafür zu zahlen.

> **Mehr als die Hälfte** der Internetnutzerinnen und -nutzer gibt **weniger als 5 Euro pro Monat** für die eigene digitale Sicherheit aus.

Wie viel geben Sie im Durchschnitt für **Sicherheitssoftware oder -dienste** (z.B. Antivirus oder VPN) für private Computer und Smartphones pro Monat aus?



Basis: Internetnutzerinnen und -nutzer (n= 1.021) | Quelle: Bitkom Research 2025

Abbildung 10: Monatliche Ausgaben für Sicherheitssoftware oder -dienste privater Internetnutzer/innen

3.2 Abschluss von Cyberversicherungen

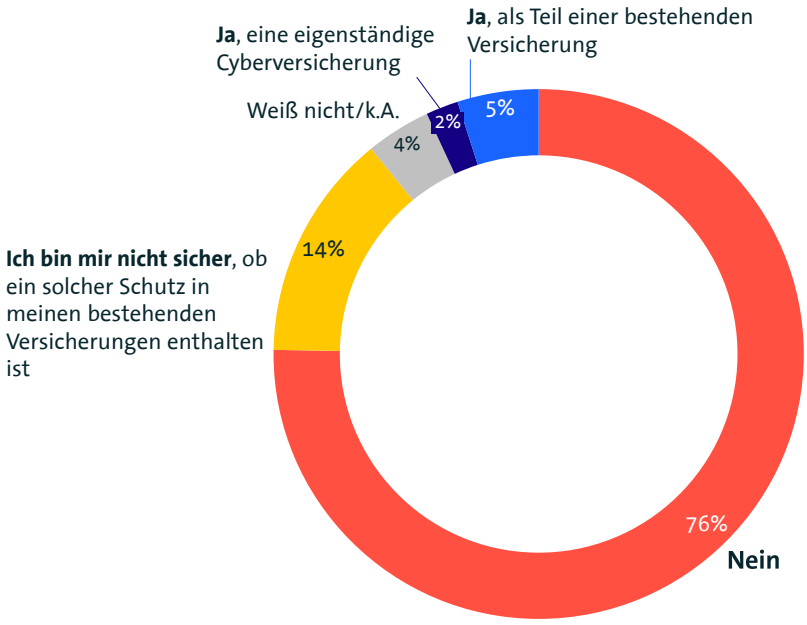
Cyberversicherungen können im Ernstfall wichtige finanzielle und organisatorische Unterstützung leisten – zum Beispiel bei Identitätsmissbrauch, Online-Betrug oder der Wiederherstellung verlorener Daten. Dennoch haben bisher nur wenige Internetnutzerinnen und -nutzer in Deutschland eine entsprechende Absicherung abgeschlossen. Lediglich 2 Prozent verfügen über eine eigenständige Cyberversicherung, weitere 5 Prozent sind über bestehende Policen – etwa Rechtsschutz- oder Haftpflichtversicherungen – abgesichert. 76 Prozent haben keinerlei Schutz, während 14 Prozent nicht wissen, ob bestehende Verträge solche Risiken abdecken.

Die Ergebnisse verdeutlichen, dass der Markt für Cyberversicherungen noch am Anfang steht. Zwar bieten entsprechende Versicherungspolicen Leistungen wie die Absicherung von Vermögensschäden, Unterstützung bei Identitätsdiebstahl oder juristische und technische Hilfe im Schadensfall. Dennoch setzen die meisten bislang eher auf Eigenverantwortung und Vorsorge durch umsichtiges Verhalten im Netz.

Drei Viertel

Der Internetnutzerinnen und -nutzer haben **keine Cyberversicherung.** Nur 7 Prozent verfügen über einen entsprechenden Schutz.

Haben Sie eine Versicherung rund um Online-Vorfälle, eine sogenannte **Cyberversicherung**?



Basis: Internetnutzerinnen und -nutzer (n=1.021) | Abweichungen von 100 Prozent rundungsbedingt | Quelle: Bitkom Research 2025

Abbildung 11: Verbreitung von Cyberversicherungen unter Internetnutzerinnen und -nutzern

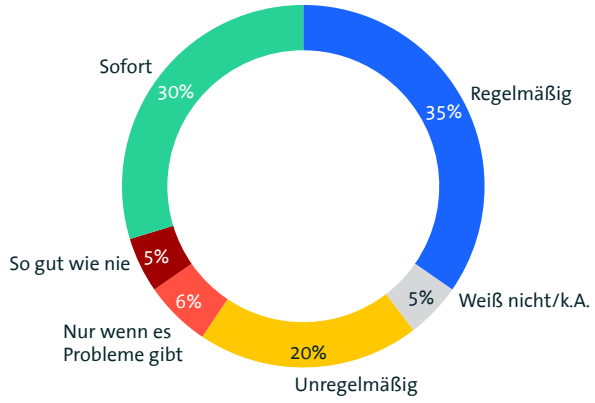
3.3 Verhalten bei Updates und Sicherheitsprüfungen

Die Mehrheit der Internetnutzerinnen und -nutzer achtet darauf, Software und Geräte regelmäßig zu aktualisieren, um Sicherheitslücken zu schließen. 35 Prozent installieren Updates in festen Abständen, 30 Prozent sogar sofort nach Verfügbarkeit. 20 Prozent handeln unregelmäßig, während 6 Prozent Updates nur dann durchführen, wenn Probleme auftreten. 5 Prozent gaben an, ihre Geräte so gut wie nie zu aktualisieren, und ebenso viele machten keine Angabe. Insgesamt zeigt sich: Viele Nutzerinnen und Nutzer verhalten sich vorsorglich, aber ein relevanter Teil verzichtet noch auf konsequente Aktualisierungen.

Beim Überprüfen von Bankkonten, E-Mail- oder Social-Media-Accounts auf verdächtige Aktivitäten sind die Nutzungsgewohnheiten vielfältig. 10 Prozent kontrollieren ihre Konten täglich, 29 Prozent mindestens einmal pro Woche und 27 Prozent mindestens einmal im Monat. Demgegenüber prüfen 24 Prozent seltener als monatlich und 7 Prozent so gut wie nie. Damit wird deutlich: Ein Teil der Nutzer zeigt ein hohes Sicherheitsbewusstsein durch häufige Kontrollen, während fast ein Drittel dies nur selten oder gar nicht tut.

> **Vier von zehn Internetnutzerinnen und -nutzer** prüfen ihre Konten mindestens wöchentlich

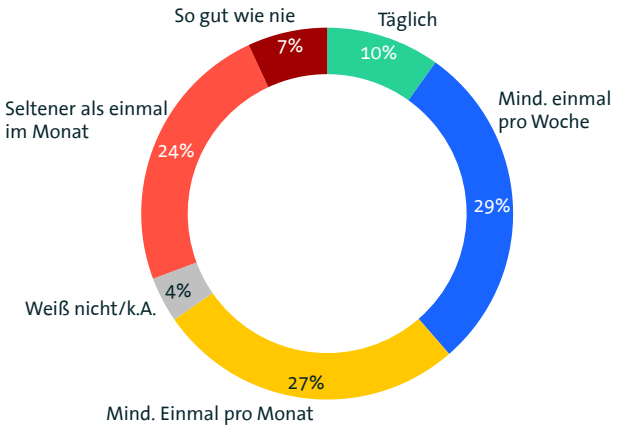
Wie oft **aktualisieren** Sie Ihre Software und Geräte, um Sicherheitslücken zu schließen?



Basis: Internetnutzerinnen und -nutzer (n=1.021) | Quelle: Bitkom Research 2025

Abbildung 12: Häufigkeit der Aktualisierung von Software und Geräten

Wie häufig **überprüfen** Sie Ihre Konten auf verdächtige Aktivitäten (z.B. Bankkonten, E-Mail, Social Media)?



Basis: Internetnutzerinnen und -nutzer (n=1.021) | Abweichungen von 100 Prozent rundungsbedingt | Quelle: Bitkom Research 2025

Abbildung 13: Häufigkeit der Überprüfung von Online-Konten auf verdächtige Aktivitäten

3.4 Fünf Bitkom-Tipps für sichere Passwörter

Ob »geheim«, »123456« oder Name und Geburtstag des Kindes – beim Umgang mit Passwörtern sind viele immer noch nachlässig, obwohl sie es damit Cyberkriminellen leicht machen, sich Zugang etwa zu Social-Media-Diensten, Online-Shopping oder Bank- und Gesundheitsdaten zu verschaffen. **Bitkom gibt fünf Tipps für sichere Zugänge**:

Keine einfachen Passwörter: Passwörter sollten nicht aus einem leicht zu erratenden persönlichen Begriff, wie dem Namen des Kindes oder des Partners, oder aus einem im Wörterbuch zu findenden einzelnen Wort bestehen. Stattdessen bietet sich eine Kombination aus verschiedenen Worten oder Silben, womöglich mit ungewöhnlicher Groß- und Kleinschreibung an. Je länger das Passwort ist, desto schwieriger ist es, es zu knacken. Sonderzeichen kann man vor allem dann nutzen, wenn man seine Passwörter ohnehin in einem Passwortmanagerspeichert.

Keine doppelten Passwörter: Für jeden Online-Dienst sollte man ein einzigartiges Passwort verwenden. Das reduziert das Risiko, dass bei einem Datenleck Cyberkriminelle Zugriff auf mehrere Konten bekommen, wenn sie gestohlene Zugangsdaten an unterschiedlichen Stellen einsetzen. Vor allem für zentrale Online-Dienste wie etwa den E-Mail-Provider, aber auch für Dienste, bei denen Kontodaten hinterlegt sind, wie etwa beim Online-Shopping, sollte man unbedingt komplexe und einzigartige Passwörter verwenden.

Keine Zettel und einfache Textdateien: Niemand kann sich Dutzende von Zugangsdaten merken. Passwörter aufzuschreiben und auf dem Büro-Schreibtisch liegenzulassen ist aber ebenso wenig eine gute Idee wie Passwortlisten in einer einfachen Textdatei auf dem Computer zu speichern. Stattdessen bieten sich Passwortmanager an. Das sind Programme für den PC oder als App für das Smartphone, in denen Zugangsdaten sicher verschlüsselt abgelegt werden können. Der Vorteil: Man muss sich nur ein – möglichst gutes – Passwort für den Passwortmanager merken oder kann diesen auf dem Smartphone zum Beispiel auch per Fingerabdruck »aufschließen«.

Doppelt hält besser: Wo immer möglich sollte die sogenannte Zwei-Faktor-Authentifizierung eingerichtet werden, denn selbst das stärkste Passwort lässt sich knacken. Bei der Zwei-Faktor-Authentifizierung reichen Nutzername und Passwort alleine nicht für den Zugang, sondern man muss aus einer speziellen App auf dem Smartphone noch einen Zahlencode ablesen und diesen zusätzlich eingeben. Das bedeutet, dass sich Angreifer nicht nur das Passwort verschaffen müssen, sondern auch Zugang zum Smartphone brauchen, wodurch die Sicherheit erhöht wird. Manchmal wird der zweite Faktor – also der Zahlencode – auch per SMS oder andere Kurznachricht verschickt oder per Mail.

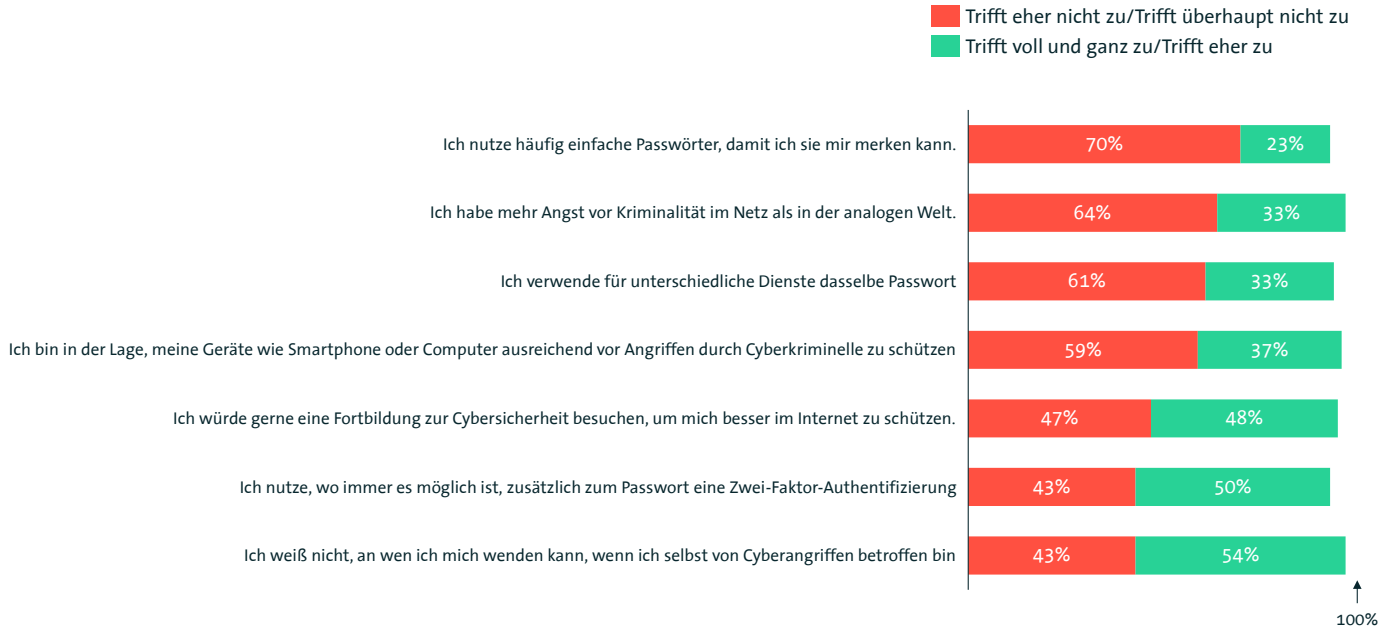
Noch mehr Sicherheit – ganz ohne Passwort: Passkeys sind eine moderne und besonders sichere Alternative zum klassischen Passwort. Anstatt wie bisher das Kennwort einzugeben, wird bei einem Passkey bei der ersten Registrierung ein Schlüsselpaar generiert, bei dem ein Teil (der private Schlüssel) sicher auf dem Gerät bleibt und der andere (der öffentliche Schlüssel) an den Online-Dienst übermittelt wird. Der Vorteil: Der private Schlüssel – der wie früher das Passwort der Ausweis für die eigene Identität ist – muss nie übertragen werden und kann so auch nicht so einfach gestohlen und missbraucht werden. Die Schlüssel selbst sind eine lange Zahlenkolonne, die der Nutzer aber gar nicht kennen muss, stattdessen wird für die Identifikation auf dem eigenen Gerät bequem der Fingerabdruck, die Gesichtserkennung oder eine PIN verwendet.

3.5 Wahrnehmung von Cyberrisiken

Die Ergebnisse verdeutlichen, wie unterschiedlich Internetnutzerinnen und -nutzer mit dem Thema Cybersicherheit umgehen. Während die Mehrheit angibt, keine einfachen Passwörter zu verwenden (70 Prozent), nutzen dennoch 23 Prozent bewusst einfache Begriffe, um sich diese besser merken zu können. Ein ähnliches Bild zeigt sich beim Umgang mit mehrfach verwendeten Passwörtern: 61 Prozent verneinen dies, 33 Prozent geben jedoch an, für verschiedene Dienste dasselbe Passwort zu verwenden.

Gleichzeitig äußern 33 Prozent mehr Angst vor Kriminalität im Netz als in der analogen Welt, während 37 Prozent überzeugt sind, ihre Geräte ausreichend schützen zu können. Besonders auffällig ist der Wunsch nach Unterstützung: 48 Prozent würden gerne eine Fortbildung zur Cybersicherheit besuchen. 50 Prozent nutzen bereits eine Zwei-Faktor-Authentifizierung, wo immer dies möglich ist. Unsicherheit besteht jedoch im Ernstfall: 54 Prozent wissen nicht, an wen sie sich wenden können, wenn sie selbst Opfer eines Cyberangriffs werden.

Aussagen zum Thema »**Cyberkriminalität**«



Basis: Internetnutzerinnen und -nutzer (n=1.021) | Rest: Weiß nicht/k.A. | Abweichungen von 100 Prozent rundungsbedingt | Quelle: Bitkom Research 2025

Abbildung 14: Einstellungen und Verhaltensweisen von Internetnutzerinnen und -nutzern im Umgang mit Cyberkriminalität

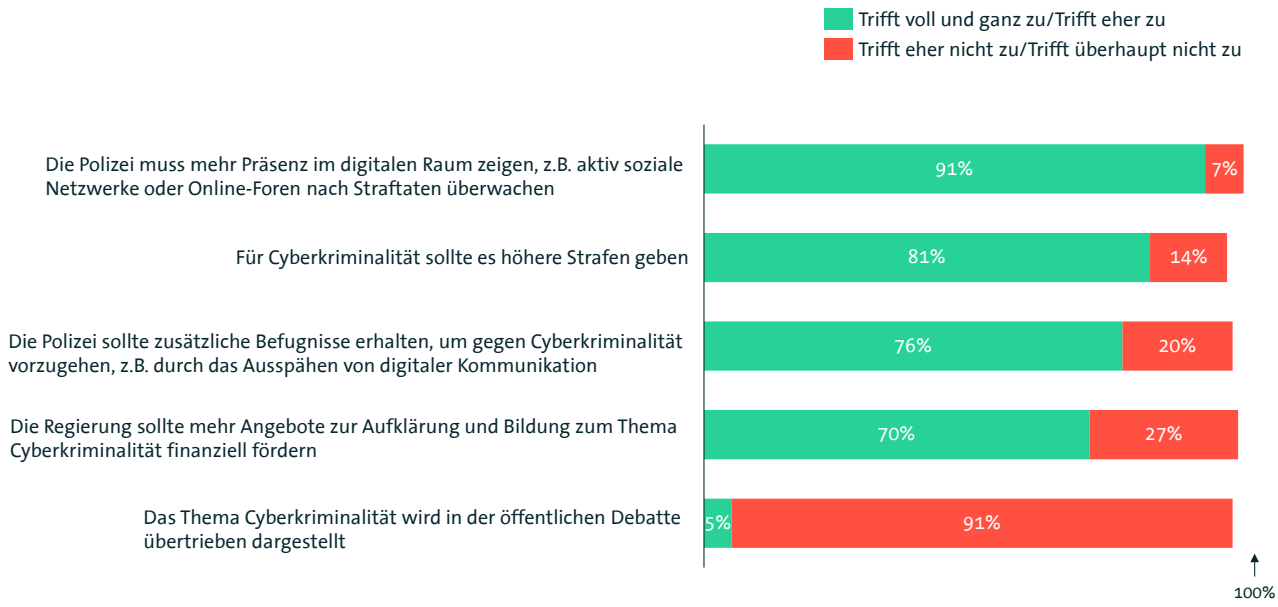
> Viele Nutzerinnen und Nutzer fühlen sich unsicher: **Über die Hälfte weiß nicht, an wen sie sich im Ernstfall bei Cyberangriffen wenden kann.**

3.6 Wahrnehmung von Schutzmaßnahmen

Die Ergebnisse verdeutlichen, dass ein breiter gesellschaftlicher Rückhalt für stärkere Maßnahmen gegen Cyberkriminalität besteht. 91 Prozent der Befragten fordern, dass die Polizei mehr Präsenz im digitalen Raum zeigt, etwa durch die Überwachung sozialer Netzwerke oder Online-Foren. Auch der Ruf nach härteren Strafen ist deutlich: 81 Prozent wünschen strengere Sanktionen. Zudem spricht sich eine Mehrheit von 76 Prozent dafür aus, der Polizei zusätzliche Befugnisse einzuräumen, um effektiver gegen Cyberkriminalität vorgehen zu können.

Darüber hinaus sehen viele die Politik in der Pflicht, mehr Aufklärung und Bildung zu fördern: 70 Prozent befürworten entsprechende staatliche Angebote. Nur bei der Einschätzung der öffentlichen Debatte zeigt sich ein anderes Bild: 91 Prozent lehnen die Aussage ab, dass Cyberkriminalität übertrieben dargestellt werde, lediglich 5 Prozent stimmen dem zu.

Aussagen zum Thema »**Cybersicherheit**«



Basis: Internetnutzerinnen und -nutzer (n=1.021) | Rest: Weiß nicht/k. A. | Abweichungen von 100 Prozent rundungsbedingt | Quelle: Bitkom Research 2025

Abbildung 15: Einstellungen von Internetnutzerinnen und -nutzern zu staatlichen Maßnahmen im Bereich Cybersicherheit

> Über 90 Prozent der Befragten fordern: **Polizei und Staat sollen stärker gegen Cyberkriminalität vorgehen**

4 Cyberkrieg und staatliche Dimension

4 Cyberkrieg und staatliche Dimension

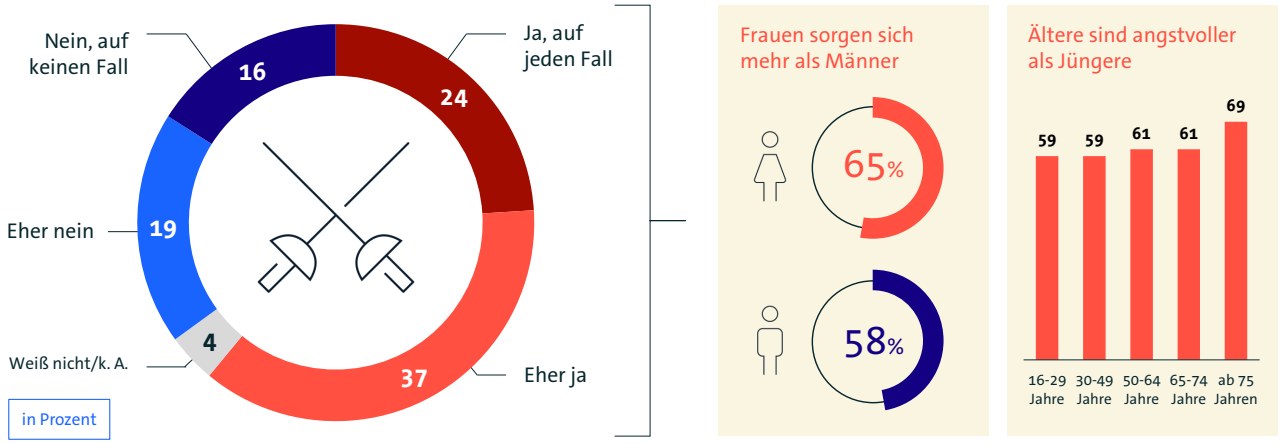
Die Angst vor einem Cyberkrieg ist weit verbreitet: 61 Prozent der Bevölkerung befürchten auf jeden Fall oder eher gezielte digitale Angriffe von Staaten auf Infrastruktur, Verwaltung oder Unternehmen. Besonders Russland (76 Prozent), die USA (75 Prozent) und China (74 Prozent) gelten als führend in ihren Cyberfähigkeiten. Zugleich erwarten 71 Prozent, dass künftige Kriege überwiegend digital geführt werden, und 63 Prozent halten Cyberangriffe auf kritische Infrastrukturen für gefährlicher als konventionelle Angriffe. Damit wird klar: Cybersicherheit ist längst Teil der Sicherheits- und Verteidigungspolitik.

4.1 Angst und Wahrnehmung eines Cyberkriegs

Die Mehrheit der Bevölkerung äußert Sorge vor einem Cyberkrieg, also vor gezielten Angriffen von Staaten auf Infrastruktur, öffentliche Einrichtungen oder Unternehmen. 24 Prozent haben »auf jeden Fall« Angst, weitere 37 Prozent »eher«. Demgegenüber geben 19 Prozent an, keine Angst zu haben, und 16 Prozent verneinen dies »auf keinen Fall«. 4 Prozent machten keine Angaben.

Dabei zeigen sich Unterschiede zwischen Bevölkerungsgruppen: 65 Prozent der Frauen befürchten einen Cyberkrieg, bei den Männern sind es 58 Prozent. Auch das Alter spielt eine Rolle: Während in der jüngsten Altersgruppe der 16- bis 29-Jährigen 59 Prozent Angst äußern, steigt der Anteil bei den Älteren deutlich an und erreicht in der Gruppe ab 75 Jahren 69 Prozent. Damit wird sichtbar, dass Cyberkriegsszenarien ein breites, aber unterschiedlich stark ausgeprägtes Bedrohungsgefühl hervorrufen.

Haben Sie **Angst vor einem Cyberkrieg**? Damit meinen wir Cyberangriffe durch Staaten, um Infrastruktur, öffentliche Einrichtungen oder Unternehmen gezielt zu stören, zu sabotieren oder zu zerstören.



Basis: Alle Befragten (n=1.115) | Quelle: Bitkom Research 2025

Abbildung 16: Angst der Bevölkerung vor einem Cyberkrieg durch staatliche Angriffe

4.2 Einschätzung technischer Fähigkeiten anderer Länder

Bei der Frage nach den technischen Fähigkeiten für einen möglichen Cyberkrieg stehen drei Länder klar an der Spitze: 76 Prozent der Befragten trauen Russland sehr gute oder eher gute Fähigkeiten zu, dicht gefolgt von den USA (75 Prozent) und China (74 Prozent). Auch Deutschland wird mit 61 Prozent vergleichsweise stark eingeschätzt.

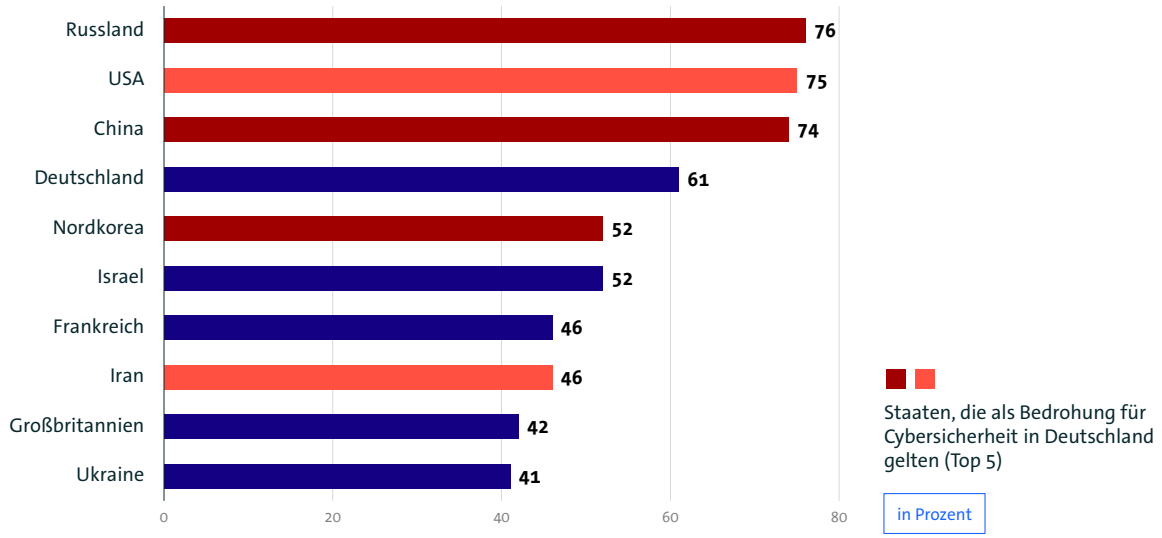
Mit deutlichem Abstand folgt eine Gruppe weiterer Länder: 52 Prozent der Befragten sehen Nordkorea und ebenso 52 Prozent Israel mit hohen technischen Kapazitäten ausgestattet. Der Iran und Frankreich liegen bei jeweils 46 Prozent, während Großbritannien (42 Prozent) und die Ukraine (41 Prozent) noch niedriger bewertet werden.

Insgesamt zeigt sich: Insbesondere die drei großen Mächte Russland, USA und China gelten in den Augen der Bevölkerung als technologisch führend im Bereich Cyberkrieg.

76 %

trauen Russland die größten Fähigkeiten für einen **Cyberkrieg** zu. Als größte Cyberbedrohung gilt auch China – ein Drittel aber sieht auch die USA als Gefahr.

Wie schätzen Sie die **technischen Fähigkeiten** dieser Länder für einen Cyberkrieg ein?



Basis: Alle Befragten (n=1.115) | Prozentwerte für »sehr gute« oder »eher gute« Fähigkeiten | Quelle: Bitkom Research 2025

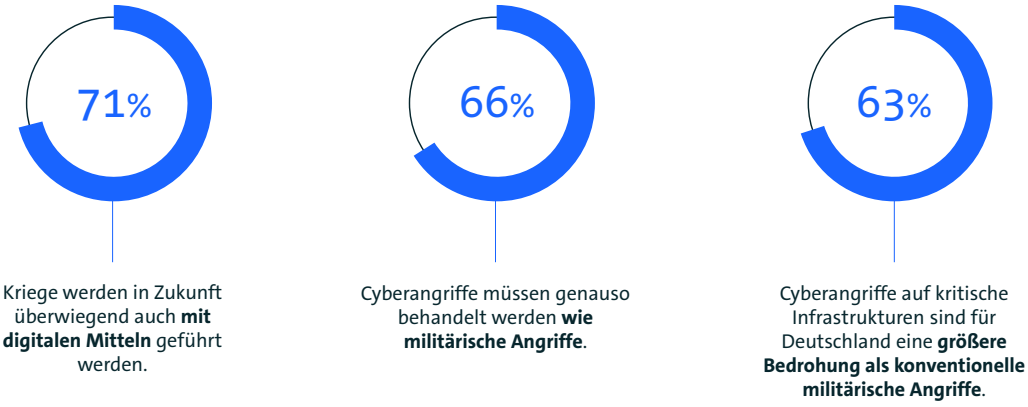
Abbildung 17: Einschätzung der technischen Fähigkeiten verschiedener Länder für einen Cyberkrieg

4.3 Sorgen und gesellschaftliche Einschätzungen

Die Befragung macht deutlich, dass Cyberangriffe weit über die Vorstellung von Datendiebstahl oder Erpressung hinausgehen und zunehmend im Kontext hybrider Kriegsführung gesehen werden. 71 Prozent der Befragten gehen davon aus, dass Kriege in Zukunft überwiegend auch mit digitalen Mitteln geführt werden. 63 Prozent halten Cyberangriffe auf kritische Infrastrukturen für eine größere Bedrohung als konventionelle militärische Angriffe.

Zugleich sehen viele die Notwendigkeit einer politischen Neubewertung: 66 Prozent sind der Meinung, dass Cyberangriffe genauso behandelt werden müssten wie militärische Angriffe. Damit wird deutlich, dass Cybersecurity aus Sicht der Bevölkerung untrennbar mit Fragen der Landes- und Verteidigungspolitik verbunden ist.

Inwieweit treffen die folgenden Aussagen Ihrer Meinung nach zu?



Basis: Alle Befragten (n=1.115) | Prozentwerte für »Trifft voll und ganz zu« und »Trifft eher zu« | Quelle: Bitkom Research 2025

Abbildung 18: Einschätzungen der Bevölkerung zu Cyberangriffen im Kontext künftiger Kriegsführung

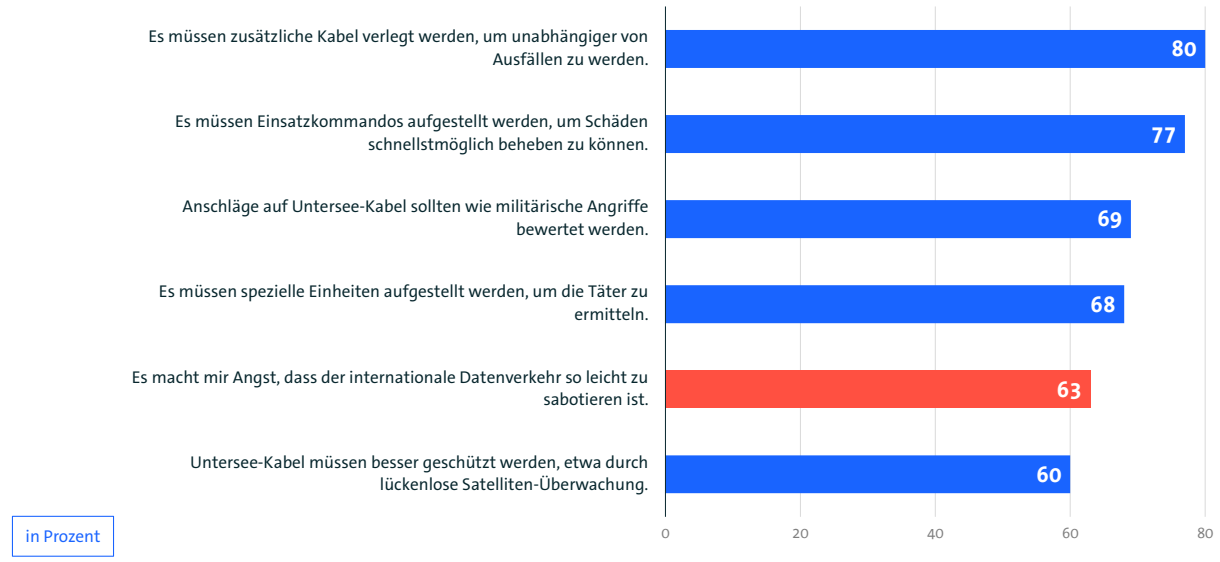
4.4 Kritische Infrastruktur: Beispiel Unterseekabel

Untersee-Kabel, die für den internationalen Datenverkehr unverzichtbar sind, werden von der Bevölkerung als besonders verwundbar wahrgenommen. Fast zwei Drittel (63 Prozent) äußern Angst davor, dass diese kritische Infrastruktur leicht sabotiert werden kann. Die große Mehrheit fordert daher stärkere Maßnahmen: 80 Prozent sprechen sich für die Verlegung zusätzlicher Kabel aus, um unabhängiger von Ausfällen zu werden. 77 Prozent halten den Einsatz spezieller Kommandos für notwendig, die Schäden schnellstmöglich beheben sollen.

Auch strafrechtliche und sicherheitspolitische Dimensionen spielen eine Rolle: 69 Prozent sind der Ansicht, dass Anschläge auf Untersee-Kabel wie militärische Angriffe bewertet werden sollten, und 68 Prozent befürworten die Aufstellung spezieller Einheiten zur Ermittlung der Täter. 60 Prozent wünschen zudem einen besseren Schutz der Kabel, beispielsweise durch eine lückenlose Satellitenüberwachung. Damit wird deutlich: Die Bedrohung durch Sabotage an Untersee-Kabeln ist ein zentrales sicherheitspolitisches Thema.

> **80 Prozent** der Befragten fordern zusätzliche Untersee-Kabel, um unabhängiger von Ausfällen zu werden.

Welche der folgenden Aussagen treffen Ihrer Meinung nach zu?



Basis: Alle Befragten (n=1.115) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2025

Abbildung 19: Einschätzungen der Bevölkerung zu Bedrohungen und Schutzmaßnahmen im Zusammenhang mit Untersee-Kabeln

5 Fazit

Cyberkriminalität ist längst ein gesamtgesellschaftliches Problem. Während nur 37 Prozent die Bedrohung für sich persönlich als hoch einschätzen, sehen 70 Prozent ein hohes Risiko für Deutschland insgesamt. Zwei Drittel halten Behörden und Verwaltung für unzureichend vorbereitet. Besonders gefährlich erscheinen ausländische Geheimdienste (78 Prozent) und organisierte Kriminalität (67 Prozent), am häufigsten werden Russland (98 Prozent) und China (84 Prozent) als Bedrohungsquellen genannt.

Die persönliche Betroffenheit ist groß: 61 Prozent der Internetnutzenden waren im letzten Jahr Opfer von Cybercrime, meist durch Betrug im Onlinehandel (36 Prozent), Datendiebstahl (30 Prozent) oder Schadsoftware (24 Prozent). Der durchschnittliche Schaden liegt bei 219 Euro, doch nur 26 Prozent der Betroffenen wenden sich an die Polizei. Zugleich investieren viele zu wenig in Vorsorge – über die Hälfte gibt weniger als 5 Euro im Monat für Sicherheit aus, nur 7 Prozent verfügen über eine Cyberversicherung.

Die Bevölkerung erwartet entschlossenes Handeln von Staat und Behörden: 91 Prozent fordern mehr Polizeipräsenz im Netz, 81 Prozent härtere Strafen, 76 Prozent zusätzliche Befugnisse und 70 Prozent mehr staatliche Aufklärung. Auch geopolitische Risiken werden zunehmend erkannt: 61 Prozent haben Angst vor einem Cyberkrieg, 71 Prozent sehen künftige Kriege vor allem digital geführt. Besonders beunruhigend sind mögliche Sabotagen an Unterseekabeln: Fast zwei Drittel fürchten solche Angriffe, die Mehrheit fordert zusätzliche Kabel, Reparatur- und Ermittlereinheiten sowie bessere Überwachung.

Um den wachsenden Bedrohungen wirksam zu begegnen, muss die Bundesregierung die richtigen Rahmenbedingungen schaffen. Dazu gehört insbesondere, europäische Cybersicherheitsregulierung praxisnah und lösungsorientiert umzusetzen, sodass Unternehmen, Verwaltung und Sicherheitsbehörden bestmöglich auf Angriffe vorbereitet sind. Auf politischer Ebene sind eine kohärente Gesamtstrategie sowie gezielte Investitionen in Sicherheits-, Investitions- und Bildungspolitik erforderlich, um langfristig Widerstandsfähigkeit aufzubauen. Ebenso entscheidend ist, die europäische Harmonisierung voranzutreiben und eine enge Zusammenarbeit zwischen den Mitgliedstaaten sicherzustellen. Dabei darf es keine Ausnahmen für die IT-Sicherheit der Verwaltung geben, denn nur wenn alle staatlichen Stellen hohe Sicherheitsstandards erfüllen, kann das Vertrauen der Bevölkerung gestärkt und die digitale Souveränität Deutschlands nachhaltig gesichert werden.

Insgesamt zeigt sich: Der Handlungsdruck ist hoch. Cybersicherheit muss zu einer zentralen Priorität werden, um Vertrauen, Resilienz und digitale Souveränität in Deutschland und Europa zu sichern.

8 Methodik

Auftraggeber	Bitkom
Methodik	Computergestützte telefonische Befragung/ Computer Assisted Telephone Interview (CATI), Dual Frame
Grundgesamtheit	Personen in Deutschland ab 16 Jahren
Stichprobengröße	n=1.115
Befragungszeitraum	KW 49 2024 bis KW 2 2025
Gewichtung	Repräsentative Gewichtung des Datensatzes auf Grundlage des aktuellen Mikrozensus des Statistischen Bundesamtes
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-Cyberkriminalität

Cyberkriminalität betrifft längst die ganze Gesellschaft: 61 Prozent der Internetnutzenden in Deutschland waren in den vergangenen zwölf Monaten direkt betroffen, der durchschnittliche finanzielle Schaden liegt bei 219 Euro. Gleichzeitig sehen 70 Prozent ein hohes Risiko für Deutschland insgesamt – besonders durch staatliche und organisierte Akteure aus dem Ausland. Das Vertrauen in die Abwehrbereitschaft staatlicher Stellen ist gering. Diese repräsentative Befragung zeigt: Viele investieren kaum in Schutzmaßnahmen, nur 7 Prozent verfügen über eine Cyberversicherung, und mehr als die Hälfte weiß im Ernstfall nicht, an wen sie sich wenden kann. Zugleich fordert die große Mehrheit mehr Polizeipräsenz im digitalen Raum, härtere Strafen und stärkere staatliche Aufklärung. Auch geopolitische Risiken stehen im Fokus: 61 Prozent der Bevölkerung fürchten einen Cyberkrieg, 80 Prozent sehen die Sabotage von Unterseekabeln als zentrale Gefahr. Die Studie macht deutlich, wie groß der Handlungsdruck ist: Cybersicherheit muss zu einer zentralen Priorität für Staat, Wirtschaft und Gesellschaft werden.

DOI
10.64022/2025-Cyberkriminalität

bitkom