2026/2027

CYBERSICHERHEIT IN ZAHLEN

Lernen. Wissen. Handeln.

Liebe Leserinnen und Leser,

digitale Abhängigkeit ist kein abstraktes Risiko mehr. Wenn ein Sicherheitsupdate ausbleibt, ein Cloud-Dienst nicht verfügbar ist oder ein Anbieter plötzlich anderen Regeln folgt, wird digitale Abhängigkeit schlagartig konkret. Dann steht nicht mehr nur eine IT-Abteilung unter Druck: Kommunen können keine Leistungen mehr anbieten, Unternehmen keine Prozesse absichern und Verantwortliche keine souveränen Entscheidungen treffen. Digitale Souveränität beginnt dort, wo wir Abhängigkeiten konsequent abbauen. Nicht irgendwann, nicht nur politisch, sondern operativ: in Strategien, Infrastrukturen und Sicherheitsarchitekturen. Digitale Souveränität bedeutet deshalb weit mehr als technologische Unabhängigkeit. Sie ist die Voraussetzung für Vertrauen – in digitale Infrastrukturen, staatliches Handeln und unternehmerische Entscheidungen.

Gerade in der Cybersicherheit wird dabei sichtbar, wie kritisch diese strukturelle Abhängigkeit ist. Ohne eigene Kernkompetenzen bleibt Europa anfällig für Sicherheitslücken, geopolitische Einflussnahmen und extern gesetzte Prioritäten. Es ist also an der Zeit, dass jedes Unternehmen eine tragfähige Strategie entwickelt, um digital eigenständig zu werden. Dabei ist der Weg dorthin ein Marathon – und sein entscheidender Engpass sind die Menschen. Denn ohne qualifizierte Fachkräfte in der IT und Informationssicherheit bleibt jede strategische Vision bloße Theorie.

Hinzu kommt die rasante Geschwindigkeit der technologischen Entwicklung. Gerade KI entwickelt sich in atemberaubendem Tempo – und mit ihr wachsen auch die Risiken. Cyberkriminelle setzen KI längst ein, um Angriffe schneller, gezielter und glaubwürdiger zu machen. Wer digitale Souveränität ernst nimmt, muss deshalb nicht nur Technologie, sondern auch Kompetenzen aufbauen. Beides schafft nicht nur mehr Sicherheit, sondern stärkt zugleich Innovationsfähigkeit, Wettbewerbsfähigkeit und Vertrauen. Digitale Souveränität schafft die Voraussetzung dafür, auch unter unsicheren geopolitischen Rahmenbedingungen handlungsfähig zu bleiben und den technologischen Wandel aktiv mitzugestalten, statt ihn nur zu verwalten.

Genau hier setzt die sechste Ausgabe unseres Magazins an, die wir mit brand eins und Statista erstellt haben. „Cybersicherheit in Zahlen“ liefert Daten, Einordnungen und Perspektiven zur Sicherheit in der digitalen Welt – und fragt, welche Konsequenzen sich daraus ergeben. Den Auftakt bildet unsere exklusive Umfrage mit mehr als 5.000 Teilnehmenden in Deutschland. Sie zeigt unter anderem, wie es um die digitale Sicherheit in Kommunen und öffentlichen Verwaltungen steht.

Darüber hinaus beleuchten wir, wo der Fachkräftemangel in IT und IT-Sicherheit besonders spürbar ist, welche Folgen er für Unternehmen und öffentliche Institutionen hat. Außerdem spricht Karsten Wildberger, seit Mitte 2025 Bundesdigitalminister, über künstliche Intelligenz, digitale Souveränität und die Frage, wie Deutschland seine digitale Handlungsfähigkeit stärken kann.

Ich lade Sie herzlich zu einer spannenden Lektüre ein und freue mich auf den Austausch mit Ihnen.

Mit herzlichem Gruß

Ihr Andreas Lüning
Vorstand und Mitgründer G DATA CyberDefense AG

Nicht delegierbar

Cybersicherheit war einmal ein Thema für Spezialisten. Heute betrifft sie praktisch alle. Unternehmen schützen nicht nur ihre Systeme, ihre Lieferketten und ihr Know-how. Verwaltungen müssen auch im Krisenfall handlungsfähig bleiben. Und wir alle treffen täglich Entscheidungen, die über unsere digitale Sicherheit mitentscheiden – oft, ohne es zu merken. Die Verantwortung dafür lässt sich schon lange nicht mehr einfach an IT-Abteilungen oder Sicherheitsbeauftragte delegieren.

Gleichzeitig hat sich auch die Bedrohung verändert. Cyberangriffe richten sich nicht mehr nur gegen einzelne Unternehmen oder Behörden. Sie treffen öffentliche Einrichtungen, kritische Infrastrukturen und das Vertrauen in digitale Systeme. Künstliche Intelligenz beschleunigt diese Entwicklung zusätzlich. Sicherheit ist deshalb heute weniger ein technisches Detail als eine Voraussetzung dafür, dass Wirtschaft, Verwaltung und Gesellschaft überhaupt funktionieren können.

Von diesem Wandel erzählen die Geschichten in unserem Heft. Wir gehen der Frage nach, was digitale Souveränität eigentlich bedeutet – und warum sich darüber so schwer Einigkeit erzielen lässt. Wir zeigen, weshalb der größte Engpass der Cybersicherheit ausgerechnet der Mensch ist und was geschehen muss, damit genügend Fachkräfte nachkommen. Und wir sprechen mit Bundesdigitalminister Karsten Wildberger darüber, wie Deutschland digital handlungsfähiger werden kann, welche Rolle KI dabei spielt und warum Sicherheit künftig immer stärker auch von autonomen Systemen abhängen wird.

Den Auftakt bildet wie immer unsere gemeinsame Umfrage mit Statista. Mehr als 5.000 Menschen in Deutschland haben uns Auskunft über ihren digitalen Alltag, ihr Sicherheitsgefühl und ihre Erfahrungen mit IT-Sicherheit gegeben. In diesem Jahr richtet sie den Blick besonders auf die öffentliche Verwaltung – einen Bereich, der für das Funktionieren unseres Gemeinwesens unverzichtbar ist und zugleich vor großen digitalen Herausforderungen steht.

Sicherheit entsteht nicht allein durch bessere Technologien. Sie lebt vom Austausch, vom gemeinsamen Lernen und von Menschen, die Verantwortung übernehmen. Denn Cybersicherheit beginnt nicht erst im Serverraum – sondern überall dort, wo Entscheidungen getroffen werden.

Ich wünsche Ihnen eine anregende Lektüre.

Susanne Risch
Chefredakteurin

Inhalt

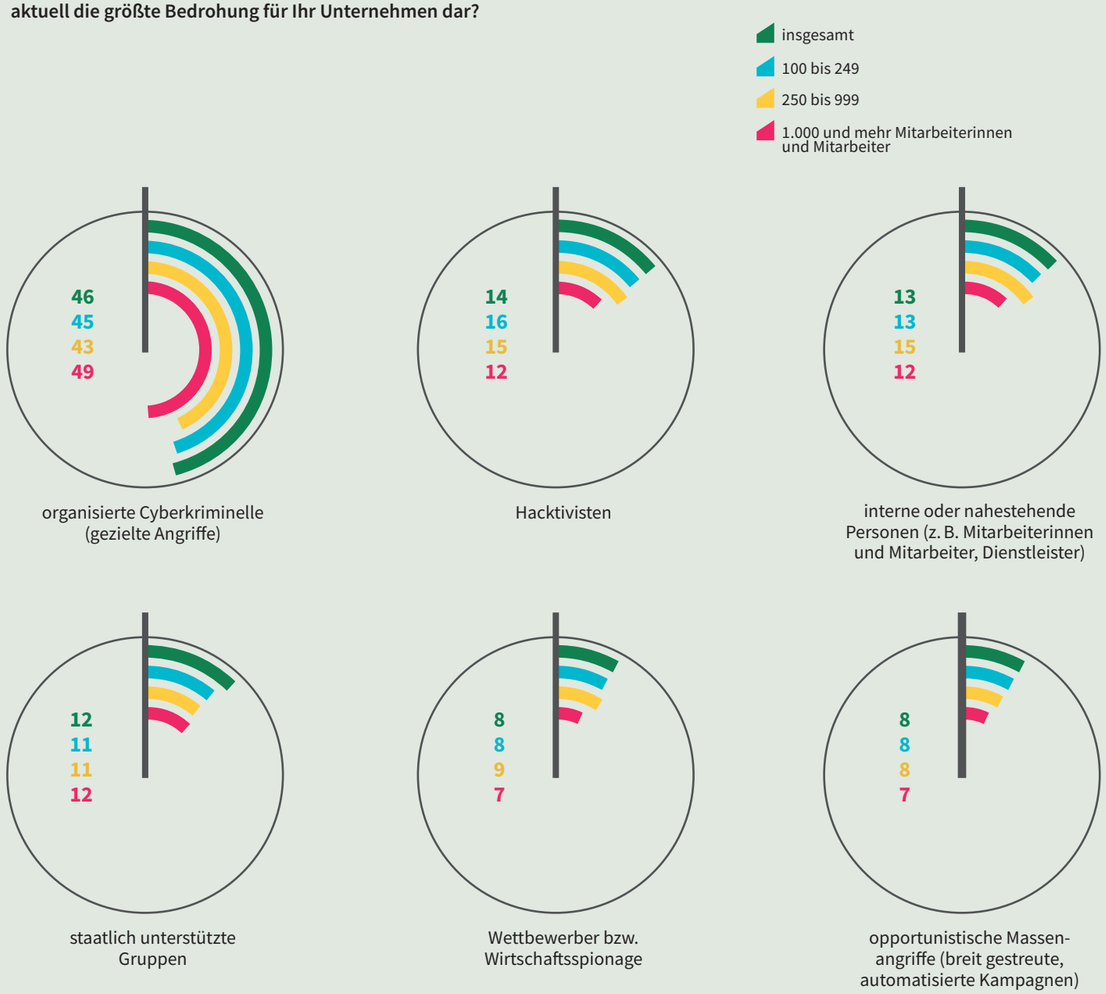
Zwischen Routine und Risiko

Cyberangriffe treffen längst nicht mehr nur Unternehmen. Mehr als 5.000 Beschäftigte zwischen 16 und 70 Jahren wurden im Frühjahr 2026 zu ihrem Wissen, ihren Erfahrungen und ihren Einschätzungen rund um IT-Sicherheit befragt. Die repräsentative Umfrage zeigt das aktuelle Stimmungsbild – mit einem besonderen Blick auf die öffentliche Verwaltung.

Die größten Bedrohungen

Cyberangriffsakteure; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2026; in Prozent

Welche der folgenden Gruppen stellt aus Ihrer Wahrnehmung aktuell die größte Bedrohung für Ihr Unternehmen dar?

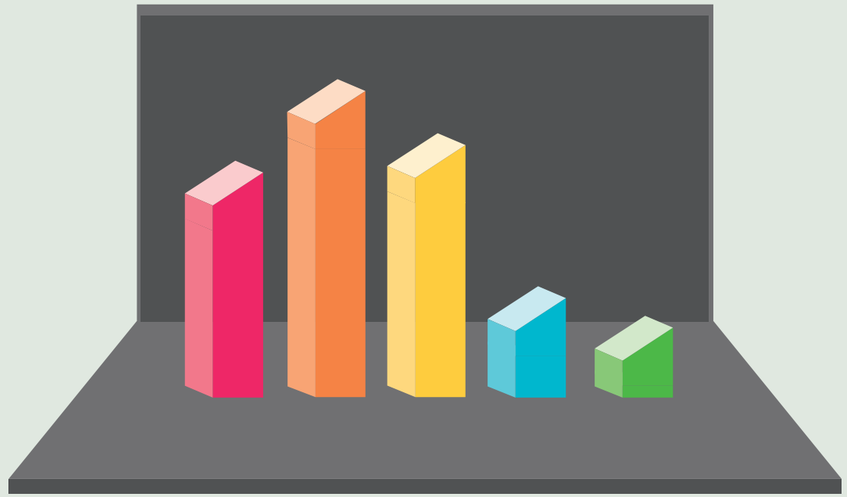


Quelle: Statista im Auftrag von G DATA

Die häufigsten Angriffe

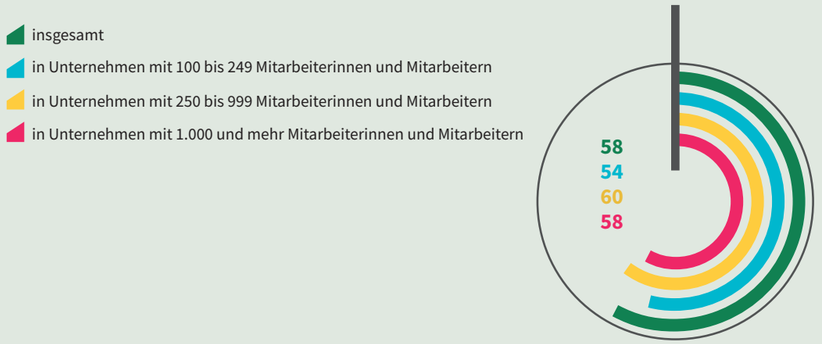
Häufigkeit von Cyberangriffen; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die in IT-Security bzw. IT/EDV (inkl. Leitung) sowie Geschäftsführung, Vorstand oder Behörden-/Amtsleitung tätig sind; 2026; in Prozent

Wie hat sich die Häufigkeit von Cyberangriffen (inkl. Angriffsversuchen, z. B. Phishing, Ransomware, DDoS) auf Ihr Unternehmen in den vergangenen zwei Jahren entwickelt?



17	42	33	7	2
deutlich zugenommen	eher zugenommen	gleich geblieben	eher abgenommen	deutlich abgenommen

Anteil der Befragten, in deren Unternehmen die Häufigkeit deutlich oder eher zugenommen hat:



Quelle: Statista im Auftrag von G DATA

Zwischen Anspruch und Alltag

Die öffentliche Verwaltung ist ein zentrales Rückgrat des Staates – und damit ein attraktives Ziel für Cyberangriffe. Wie sicher arbeitet die öffentliche Verwaltung? Wo wurden in den vergangenen Monaten Fortschritte erzielt? Und wo bremsen komplizierte Verfahren, fehlende Ressourcen oder technologische Abhängigkeiten? Unsere Befragung unter 690 Beschäftigten zeichnet ein differenziertes Bild: mehr Sicherheitsbewusstsein und mehr Maßnahmen als oft vermutet – aber auch strukturelle Hürden, die den Weg zu einer resilienten Verwaltung erschweren.

Nötig

Zustand der IT-Systeme; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die im öffentlichen Dienst tätig sind; 2026; in Prozent*

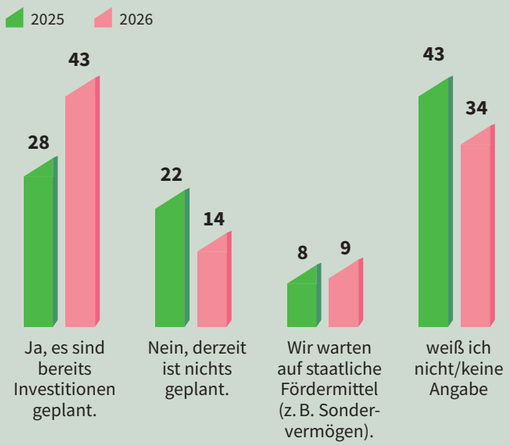
Wie würden Sie den aktuellen Zustand der IT-Systeme in Ihrer Verwaltung einschätzen?

*Mehrfachnennung möglich. Quelle: Statista im Auftrag von G DATA

Künftig

Künftige Investitionen in IT-Sicherheit; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die im öffentlichen Dienst tätig sind; in Prozent

Wissen Sie, ob Ihre Verwaltung in nächster Zeit mehr in IT-Sicherheit investieren wird?

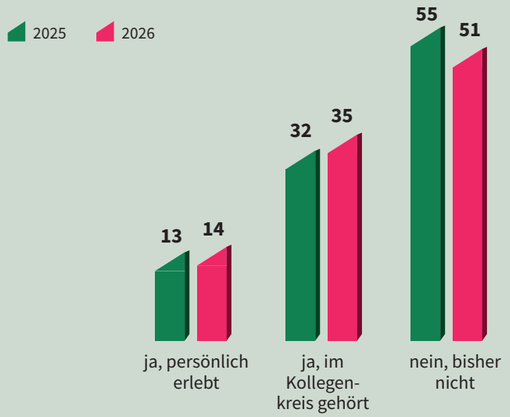


Quelle: Statista im Auftrag von G DATA

Brüchig

Persönliche Erfahrungen mit Cyberangriffen; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die im öffentlichen Dienst tätig sind; in Prozent

Haben Sie selbst schon einmal einen Cyberangriff in Ihrer Verwaltung miterlebt – oder davon bei Ihnen gehört?

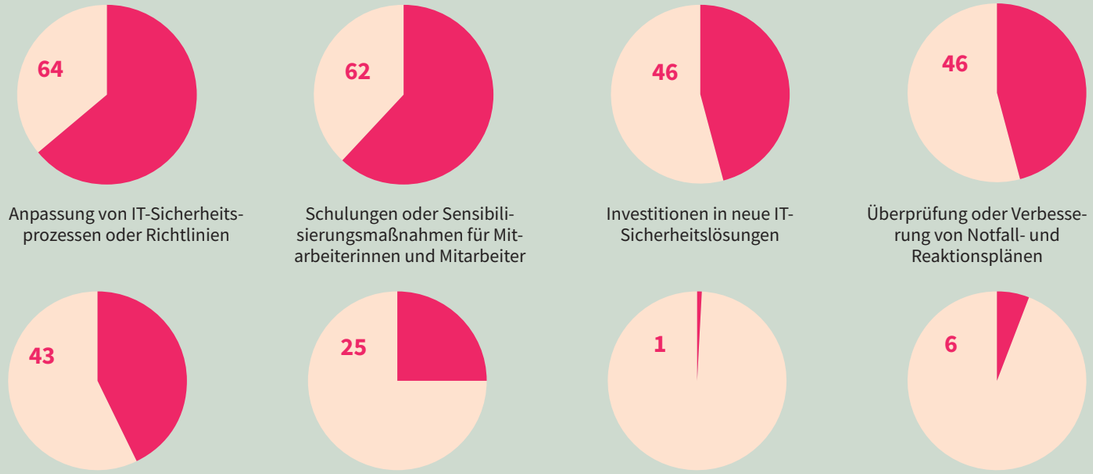


Quelle: Statista im Auftrag von G DATA

Wichtig

Maßnahmen infolge von IT-Angriffen; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die im öffentlichen Dienst in IT-Security, IT/EDV (inkl. Leitung) sowie Behörden- bzw. Amtsleitungen arbeiten; 2026; in Prozent*

Welche Maßnahmen wurden in Ihrer Organisation infolge von Berichten über IT-Angriffe auf andere Kommunen oder kommunale IT-Dienstleister angestoßen oder umgesetzt?

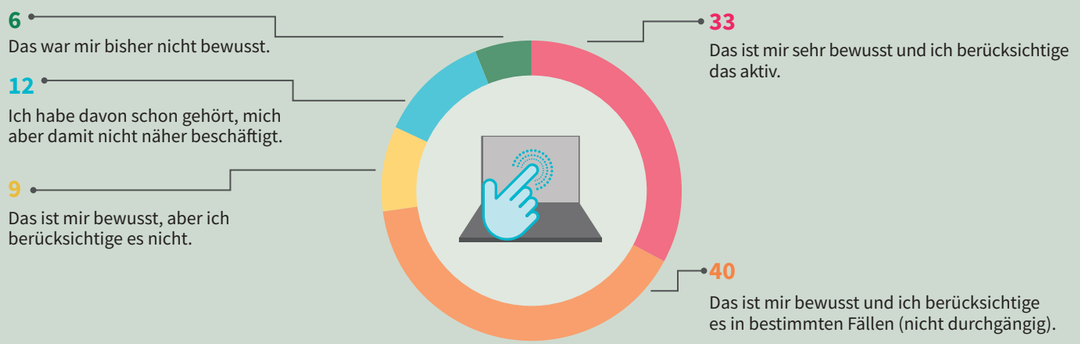


*Mehrfachnennung möglich. Quelle: Statista im Auftrag von G DATA

Mulmig

Sicherheitsbewusstsein; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die im öffentlichen Dienst tätig sind; 2026; in Prozent

Inwieweit ist Ihnen bewusst, dass internationale Anbieter auch Zugriff auf Ihre Daten haben können – selbst wenn diese in Deutschland gespeichert werden?



Quelle: Statista im Auftrag von G DATA

Vorsichtig

Schutzmaßnahmen für IT-Systeme; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die im öffentlichen Dienst tätig sind; 2026; in Prozent*

Wissen Sie, ob Ihre Verwaltung auch außerhalb der regulären Arbeitszeiten Schutzmaßnahmen für IT-Systeme ergreift?

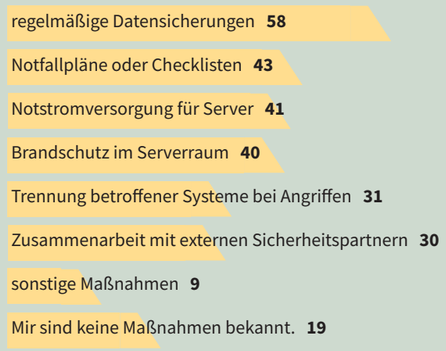
33	30	17	24
ja, z. B. durch Bereitschaft oder Schichtdienste	ja, durch externe Dienstleister	nein, meines Wissens nicht	weiß ich nicht/keine Angabe

*Mehrfachnennung möglich. Quelle: Statista im Auftrag von G DATA

Regelmäßig

Bekannte Notfallmaßnahmen; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die im öffentlichen Dienst tätig sind; 2026; in Prozent*

Welche Notfallmaßnahmen zur IT-Sicherheit sind Ihnen in Ihrer Verwaltung bekannt (z. B. im Kontext aktueller Anforderungen an Resilienz und KRITIS)?



*Mehrfachnennung möglich. Quelle: Statista im Auftrag von G DATA

Vielschichtig

Informationsquellen zum Thema IT-Sicherheit; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die im öffentlichen Dienst tätig sind; 2026; in Prozent*

Von welchen Quellen erhalten Sie Empfehlungen zur IT-Sicherheit, die Sie auch umsetzen?

32	30	29	17	12
vom Bund (z. B. BSI)	vom Land	von Kolleginnen und Kollegen aus anderen Kommunen oder Einrichtungen	von Veranstaltungen, Konferenzen oder Fach-Events	aus Fachzeitschriften

11	11	6	9	18
aus sozialen Medien	von Vereinen oder Organisationen (z. B. Städtetag)	von Vergleichsportalen	Sonstige	Ich folge keinen Empfehlungen zur IT-Sicherheit.

*Mehrfachnennung möglich. Quelle: Statista im Auftrag von G DATA

Verständlich

Wichtige Aspekte für die Nutzbarkeit von IT-Sicherheitsinformationen; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die im öffentlichen Dienst tätig sind; 2026; in Prozent*

Welche Aspekte sind Ihnen besonders wichtig, damit Informationen oder Empfehlungen zur IT-Sicherheit für Sie im Arbeitsalltag gut nutzbar sind?

38	37	32	30	23
verständliche, nicht zu technische Sprache	schnelle und unkomplizierte Verfügbarkeit von Informationen	klare und übersichtliche Aufbereitung der Inhalte	Austausch oder Zusammenarbeit mit anderen Behörden oder Einrichtungen	kurze und kompakte Formate

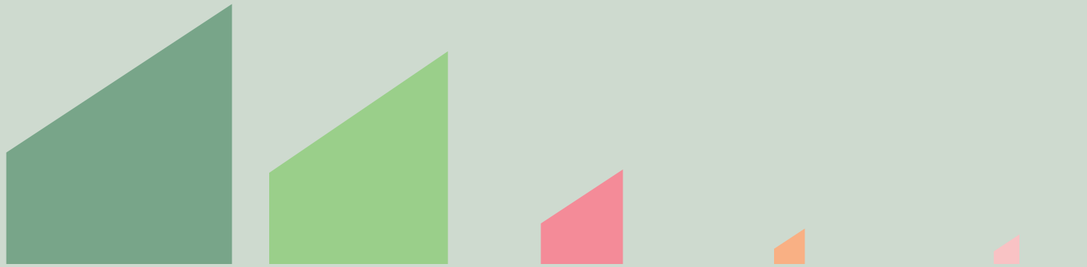
22	21	19	3	7
klare zentrale Anlaufstellen oder Plattformen für Informationen	Praxisbeispiele aus vergleichbaren Behörden oder Einrichtungen	digitale Kommunikationswege (z. B. Newsletter, Online-Portale)	Sonstiges	Nichts davon ist für mich besonders relevant.

*Mehrfachnennung möglich. Quelle: Statista im Auftrag von G DATA

Öffentlich

Rolle des öffentlichen Sektors bei digitaler Souveränität; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die im öffentlichen Dienst tätig sind; 2026; in Prozent*

Welche Rolle sollte der öffentliche Sektor Ihrer Meinung nach bei der Stärkung der digitalen Souveränität in Deutschland spielen (z. B. in Bezug auf Daten, IT-Infrastruktur und technologische Abhängigkeiten)?



44	30	16	6	5
wichtige Rolle, da der öffentliche Sektor Anforderungen an Technologien, Anbieter und Datennutzung vorgeben kann	zentrale Vorreiterrolle, da hier besonders sensible Daten und kritische Infrastrukturen geschützt werden müssen	Impulsgeber, da digitale Souveränität nur gemeinsam mit Wirtschaft und Technologieanbietern erreicht werden kann	keine besondere Rolle, da digitale Abhängigkeiten primär durch Markt und technologische Entwicklungen bestimmt werden	eher geringe Rolle, da Unternehmen und Anbieter näher an Innovation und Umsetzung sind

*Abweichung zu 100 Prozent durch Rundung. Quelle: Statista im Auftrag von G DATA

Mehr Sicherheit

Vorteile durch Unterstützung von externen Fachleuten; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die im öffentlichen Dienst tätig sind; in Prozent*

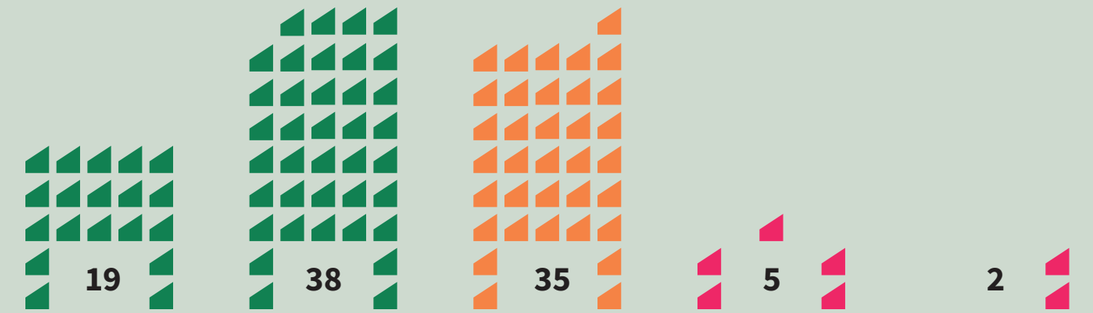
Was würden Sie als Vorteile sehen, wenn IT-Sicherheit teilweise durch externe Fachleute unterstützt wird?

*Mehrfachnennung möglich. Quelle: Statista im Auftrag von G DATA

Weniger Abhängigkeit

Bewertung des Einsatzes von Open-Source-Software; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die im öffentlichen Dienst tätig sind; 2026; in Prozent

Wie bewerten Sie Bestrebungen, im öffentlichen Sektor verstärkt auf Open-Source-Software zu setzen, um digitale Abhängigkeiten zu reduzieren?



Sehr positiv: Open Source stärkt die Unabhängigkeit, weil man nicht an einzelne Anbieter gebunden ist.

Eher positiv: Open Source ist sinnvoll, sollte aber gezielt eingesetzt werden.

Teils, teils: Es gibt sowohl Vorteile als auch Herausforderungen.

Eher kritisch: Der Aufwand und die Umstellung sind oft zu hoch.

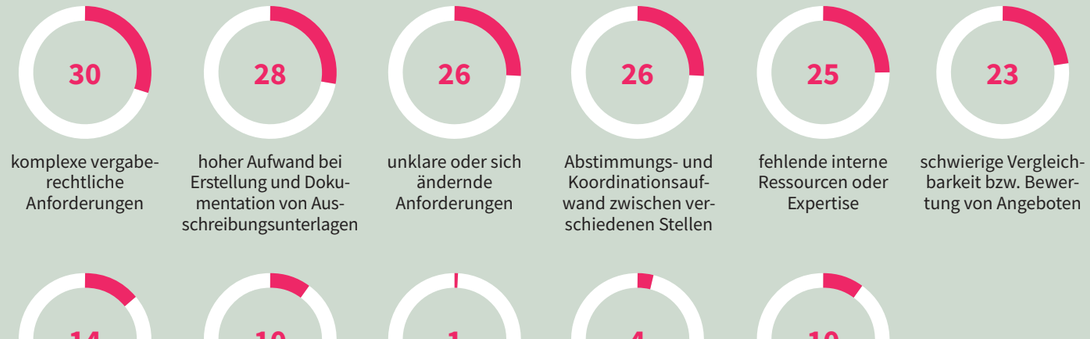
Sehr kritisch: Open Source ist keine geeignete Lösung, da hoher Aufwand und neue Abhängigkeiten entstehen können.

Quelle: Statista im Auftrag von G DATA

Sehr komplex

Hürden bei Ausschreibungsprozessen; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die im öffentlichen Dienst in IT-Security, IT/EDV (inkl. Leitung) sowie Behörden- bzw. Amtsleitungen tätig sind; 2026; in Prozent*

Welche Hürden erschweren Ihnen aktuell den Ausschreibungsprozess bei IT-Sicherheitsprojekten?

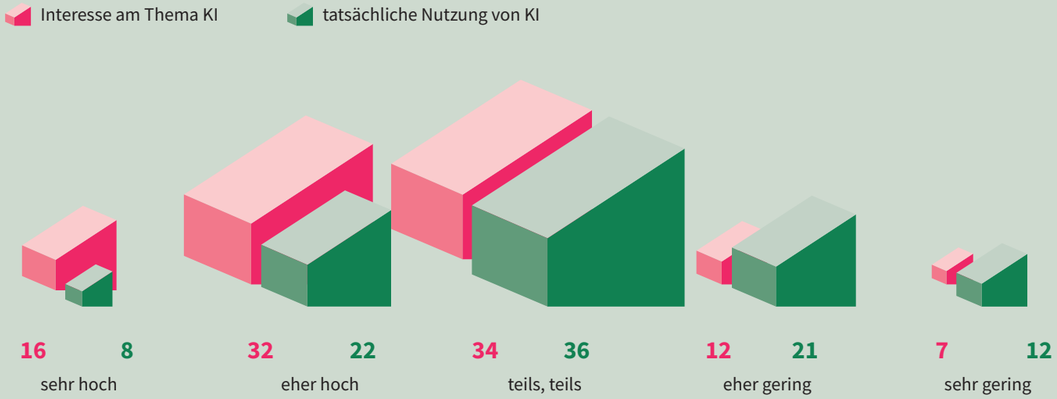


*Mehrfachnennung möglich. Quelle: Statista im Auftrag von G DATA

Mäßig interessant

KI-Nutzung; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die im öffentlichen Dienst tätig sind; 2026; in Prozent*

Wie würden Sie das Interesse und die tatsächliche Nutzung von KI in Ihrer Verwaltung aktuell einschätzen?

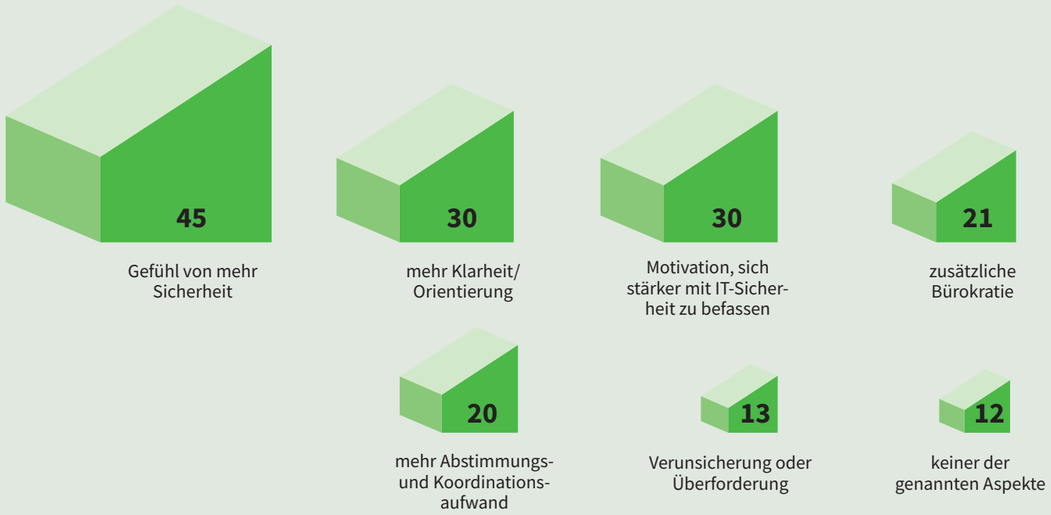


*Abweichung zu 100 Prozent durch Rundung. Quelle: Statista im Auftrag von G DATA

Gute Gefühle

Aspekte im Zusammenhang mit neuen IT-Sicherheitsvorgaben; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2026; in Prozent*

Welche der folgenden Aspekte verbinden Sie mit der Einführung neuer IT-Sicherheitsvorgaben (z. B. NIS-2)?

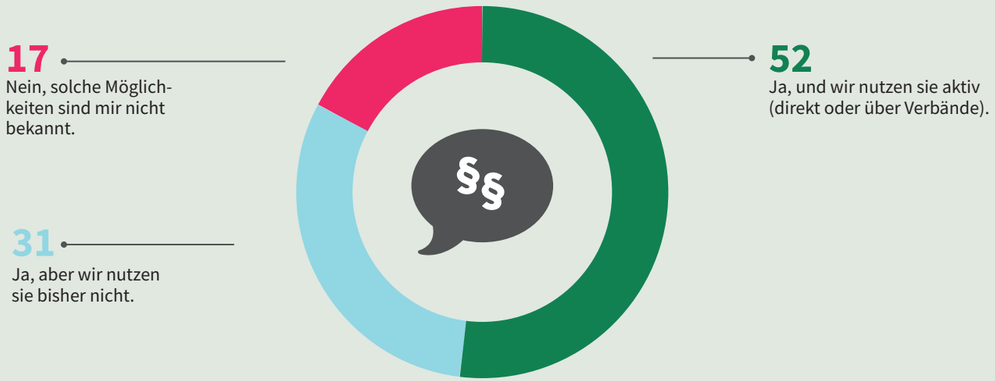


*Mehrfachnennung möglich. Quelle: Statista im Auftrag von G DATA

Aktive Beteiligung

Beteiligung an Gesetzgebungsverfahren im Bereich IT; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die in IT-Security bzw. IT/EDV (inkl. Leitung) sowie Geschäftsführung, Vorstand oder Behörden-/Amtsleitung tätig sind; 2026; in Prozent

Sind Ihnen Möglichkeiten bekannt, sich als Unternehmen an Gesetzgebungsverfahren im Bereich IT-Sicherheit zu beteiligen (z. B. über Verbände oder Konsultationen)?

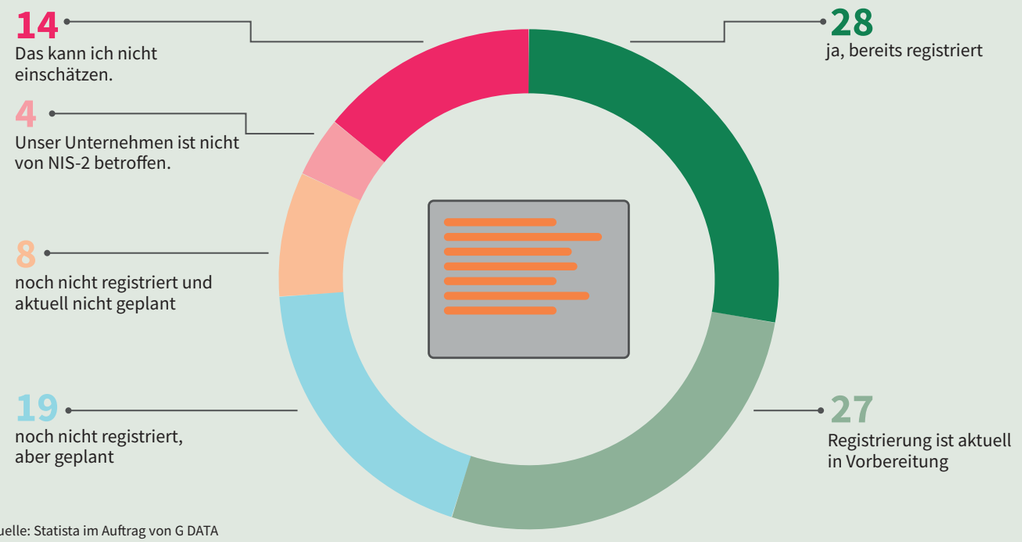


Quelle: Statista im Auftrag von G DATA

Gute Absichten

Registrierung für NIS-2; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die in IT-Security bzw. IT/EDV (inkl. Leitung) sowie Geschäftsführung, Vorstand oder Behörden-/Amtsleitung tätig sind; 2026; in Prozent

Ist Ihr Unternehmen im Rahmen von NIS-2 bereits bei der zuständigen Stelle registriert bzw. in Vorbereitung darauf?



Quelle: Statista im Auftrag von G DATA

Konkrete Maßnahmen

Konkrete Maßnahmen im Zusammenhang mit NIS-2; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die in IT-Security bzw. IT/EDV (inkl. Leitung) sowie Geschäftsführung, Vorstand oder Behörden-/Amtsleitung tätig sind; 2026; in Prozent*

Welche der folgenden Punkte im Zusammenhang mit NIS-2 treffen auf Ihr Unternehmen zu?

Interne Prozesse und Richtlinien wurden angepasst.	31
Schulungen oder Sensibilisierungsmaßnahmen wurden durchgeführt.	30
Zertifizierungen werden aktuell angestrebt (z. B. ISMS).	27
Meldeprozesse für Sicherheitsvorfälle wurden eingerichtet bzw. angepasst.	27
Zertifizierungen wurden umgesetzt (z. B. ISMS).	23
Anforderungen von Kunden mit NIS-2-Vorgaben wurden umgesetzt.	22
Geschäftsaktivitäten wurden im Zuge von NIS-2-Anforderungen angepasst oder eingeschränkt (z. B. Rückzug aus bestimmten Bereichen).	21
Mindestens ein Sicherheitsvorfall wurde bereits gemeldet.	19
Anforderungen von Kunden im Zusammenhang mit NIS-2 haben zur Beendigung von Geschäftsbeziehungen geführt.	17
Wir haben uns mit den Anforderungen beschäftigt, aber noch keine konkreten Maßnahmen umgesetzt.	6
weiß nicht	1

*Mehrfachnennung möglich. Quelle: Statista im Auftrag von G DATA

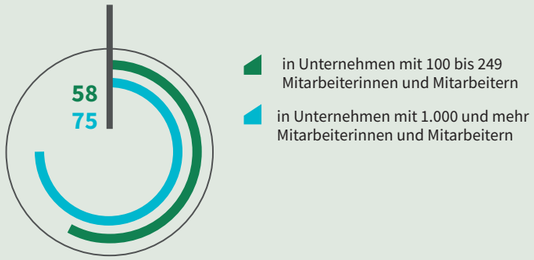
Sehr überzeugt

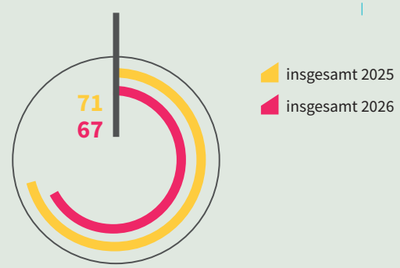
IT-Reifegrad; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2026; in Prozent

Wie schätzen Sie den Reifegrad der IT-Sicherheit in Ihrem Unternehmen ein?

26	41	25	5	3
Sehr hoch: Wir haben umfassende Sicherheitsmaßnahmen, regelmäßige Audits und ein starkes Sicherheitsbewusstsein.	**Hoch:** Unsere IT-Sicherheit ist gut aufgestellt, es gibt aber noch Optimierungsmöglichkeiten.	**Mittel:** Grundlegende Sicherheitsmaßnahmen sind implementiert, aber einige Lücken bestehen noch.	**Niedrig:** IT-Sicherheit wird berücksichtigt, aber es fehlen klare Prozesse oder Ressourcen.	**Sehr niedrig:** IT-Sicherheit spielt eine untergeordnete Rolle oder ist kaum etabliert.

Anteil der Befragten, die den Reifegrad als (sehr) hoch einschätzen:



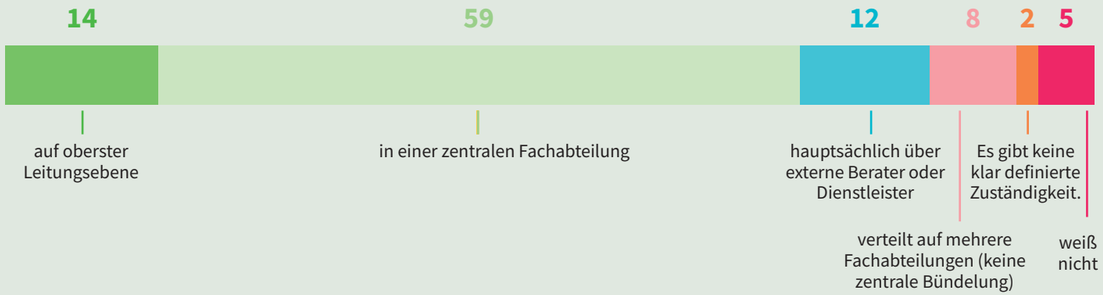


Quelle: Statista im Auftrag von G DATA

Zentral gesteuert

Umsetzung regulatorischer IT-Sicherheitsanforderungen; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die in IT-Security bzw. IT/EDV (inkl. Leitung) sowie Geschäftsführung, Vorstand oder Behörden-/Amtsleitung tätig sind; 2026; in Prozent

Auf welcher Ebene wird die Umsetzung regulatorischer IT-Sicherheitsanforderungen in Ihrem Unternehmen hauptsächlich gesteuert?

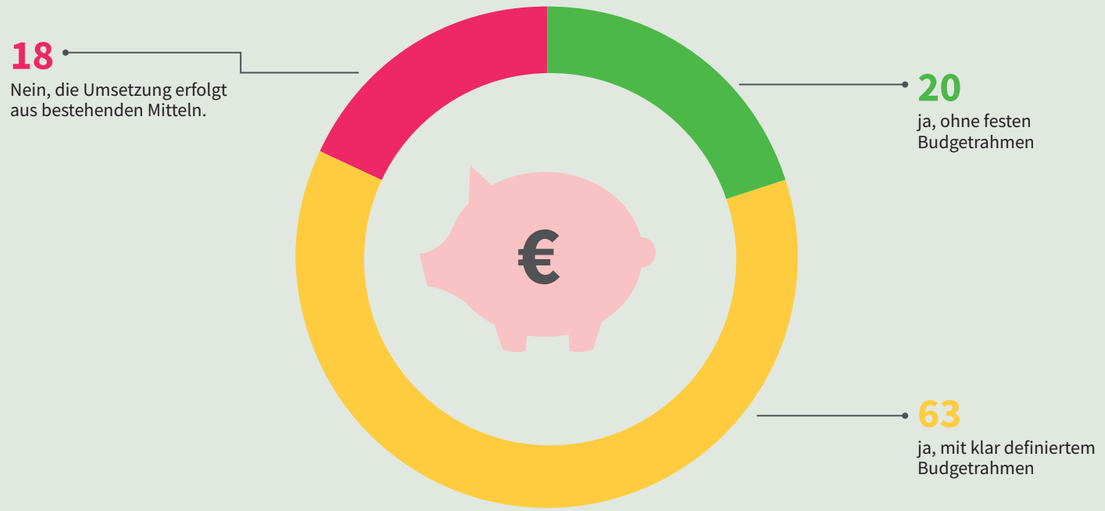


Quelle: Statista im Auftrag von G DATA

Klar definiert

Budgets für die Umsetzung regulatorischer IT-Sicherheitsanforderungen; Arbeitnehmerinnen und Arbeitnehmer, die in Bereichs-, Abteilungs- oder Teamleitung sowie Geschäftsführung, Vorstand oder Behörden-/Amtsleitung tätig sind; 2026; in Prozent*

Werden für die Umsetzung regulatorischer Anforderungen zusätzliche Budgets bereitgestellt?



*Abweichung zu 100 Prozent durch Rundung. Quelle: Statista im Auftrag von G DATA

Stark gebunden

Ressourcen für regulatorische Anforderungen; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die in IT-Security bzw. IT/EDV (inkl. Leitung) sowie Geschäftsführung, Vorstand oder Behörden-/Amtsleitung tätig sind; 2026; in Prozent

Wie stark binden regulatorische Anforderungen Ressourcen, die sonst unmittelbar in Schutzmaßnahmen gegen Cyberangriffe fließen würden (z. B. Monitoring, Patch-Management oder Reaktion auf Sicherheitsvorfälle)?

Quelle: Statista im Auftrag von G DATA

Teuer, aufwendig, komplex

Größte Herausforderungen bei regulatorischen IT-Sicherheitsvorgaben; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die in IT-Security bzw. IT/EDV sowie Geschäftsführung, Vorstand oder Behörden-/Amtsleitung tätig sind; 2026; in Prozent*

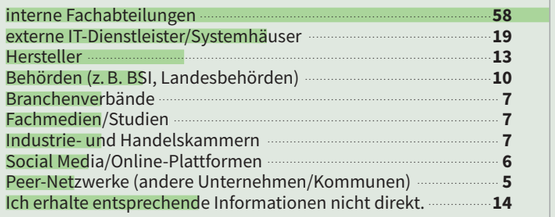
Welche der folgenden Aspekte regulatorischer IT-Sicherheitsvorgaben stellen für Ihr Unternehmen derzeit die größten Herausforderungen bei der praktischen Umsetzung dar?

*Mehrfachnennung möglich, max. 3 Antworten. Quelle: Statista im Auftrag von G DATA

Intern

Ansprechpartner bei neuen regulatorischen Anforderungen; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2026; in Prozent*

Wenn neue regulatorische Anforderungen angekündigt werden (z. B. NIS-2): An wen wenden Sie sich typischerweise am ehesten, um zu verstehen, welche konkreten Auswirkungen das für Sie persönlich oder Ihr Unternehmen hat?

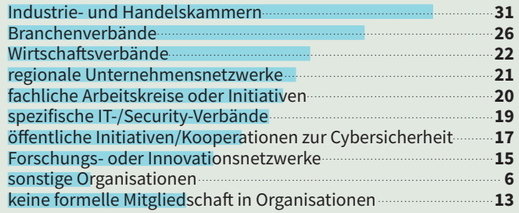


*Mehrfachnennung möglich, max. 3 Antworten. Quelle: Statista im Auftrag von G DATA

Extern

Ansprechpartner bei neuen regulatorischen Anforderungen; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die in Bereichs-, Abteilungs- oder Teamleitung sowie Geschäftsführung, Vorstand oder Behörden-/Amtsleitung tätig sind; 2026; in Prozent*

Soweit Ihnen bekannt: In welchen Organisationen ist Ihr Unternehmen aktiv Mitglied (z. B. zur Interessenvertretung oder zum fachlichen Austausch)?



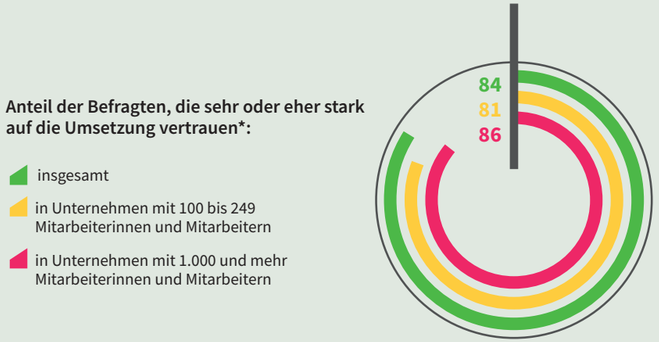
*Mehrfachnennung möglich. Quelle: Statista im Auftrag von G DATA

Vertrauensvoll

Vertrauen in die Umsetzung gesetzlicher IT-Sicherheitsanforderungen; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2026; in Prozent*

Wie stark vertrauen Sie darauf, dass Ihr Unternehmen gesetzliche IT-Sicherheitsanforderungen vollständig und fristgerecht umsetzt?

Anteil der Befragten, die sehr oder eher stark auf die Umsetzung vertrauen*:



*Abweichung zu 100 Prozent durch Rundung. Quelle: Statista im Auftrag von G DATA

Hilfreich

Hilfreiche Unterstützung bei neuen IT-Sicherheitsregeln; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2026; in Prozent

Welche Form der Unterstützung würde Ihnen am meisten helfen, wenn neue IT-Sicherheitsregeln/-anforderungen (z. B. NIS-2) kommen?

Quelle: Statista im Auftrag von G DATA

Technologisch

Wichtige Aspekte bei der Auswahl von IT-Sicherheitslösungen; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2026; in Prozent

Welcher der folgenden Aspekte ist aus Ihrer Sicht am wichtigsten bei der Auswahl von IT-Sicherheitslösungen?

24 hohe technologische Sicherheitsstandards – unabhängig vom Herkunftsland

18 Zuverlässigkeit und reibungsloser Betrieb der IT-Sicherheitslösung

15 Benutzerfreundlichkeit

12 digitale Unabhängigkeit – auch wenn Lösungen evtl. weniger komfortabel sind

10 regulatorische Konformität/ Rechtssicherheit

9 persönlicher Support/ Ansprechpartner in deutscher Sprache

7 geringe Kosten

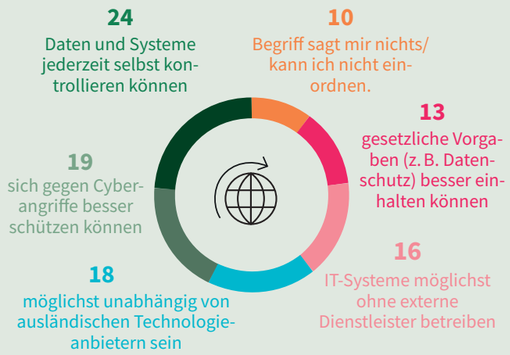
4 Integration in bestehende Systeme

Quelle: Statista im Auftrag von G DATA

Eigenverantwortlich

Assoziationen zu digitaler Souveränität; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2026; in Prozent

Woran denken Sie spontan am ehesten, wenn Sie den Begriff „digitale Souveränität“ hören?

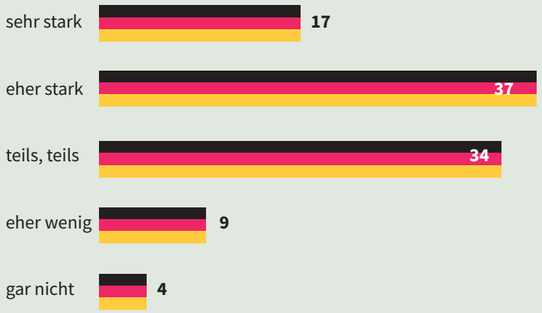


Quelle: Statista im Auftrag von G DATA

Heimisch

Einschätzung der Vertrauenswürdigkeit des Labels „Made in Germany“; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2026; in Prozent*

Wie sehr verbinden Sie mit dem Label „Made in Germany“ bei IT-Sicherheitslösungen eine höhere Vertrauenswürdigkeit?

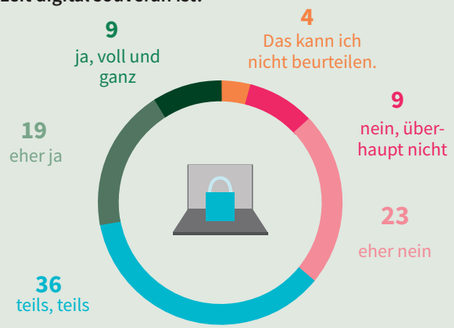


*Abweichung zu 100 Prozent durch Rundung. Quelle: Statista im Auftrag von G DATA

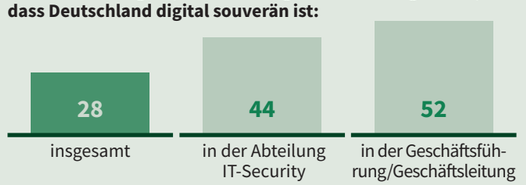
Unschlüssig

Einschätzung zum Stand digitaler Souveränität; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2026; in Prozent

Glauben Sie, dass Deutschland im Bereich IT-Sicherheit derzeit digital souverän ist?



Anteil der Befragten, die voll und ganz oder eher glauben, dass Deutschland digital souverän ist:

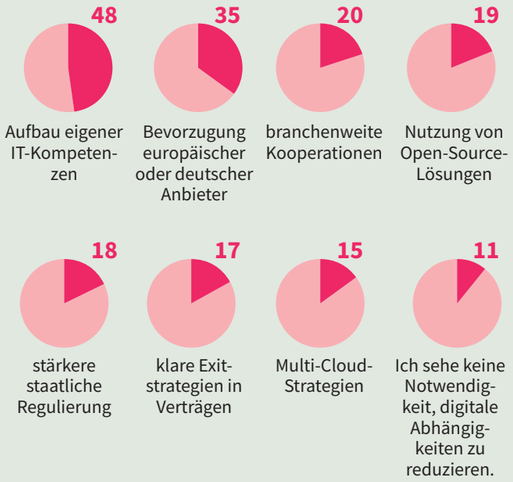


Quelle: Statista im Auftrag von G DATA

Unabhängig

Maßnahmen zur Reduzierung von digitalen Abhängigkeiten; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2026; in Prozent*

Welche der folgenden Maßnahmen halten Sie für die wirksamsten, um digitale Abhängigkeiten Ihres Unternehmens zu reduzieren?



*Mehrfachnennung möglich, max. 3 Antworten. Quelle: Statista im Auftrag von G DATA

Widrig

Hindernisse für digitale Souveränität; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die in IT-Security bzw. IT/EDV (inkl. Leitung) sowie Geschäftsführung, Vorstand oder Behörden-/Amtsleitung tätig sind; 2026; in Prozent

Welcher der folgenden Aspekte stellt aus Ihrer Sicht aktuell das größte Hindernis auf dem Weg zu mehr digitaler Souveränität in Ihrem Unternehmen dar?

15 Fachkräftemangel

15 bestehende technische Abhängigkeiten (z. B. proprietäre Systeme, Vendor-Lock-in)

14 fehlende technisch oder wirtschaftlich gleichwertige Alternativen

13 hohe Wechselkosten (z. B. für Migration, neue Systeme oder Schulungen)

10 fehlende strategische Priorisierung durch das Management

9 Budgetrestriktionen

8 fehlendes Vertrauen in alternative Anbieter oder Technologien

8 rechtliche Unsicherheiten

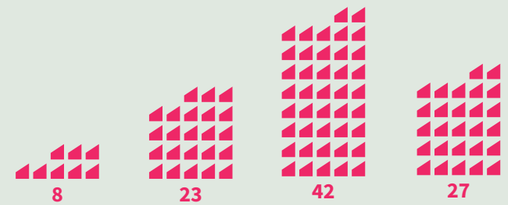
7 Ich sehe derzeit keine Hindernisse.

Quelle: Statista im Auftrag von G DATA

Bekannt

Bekanntheit von Security Operations Centern; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2026; in Prozent

Wie gut sind Sie mit dem Begriff Security Operations Center (SOC) vertraut?



Quelle: Statista im Auftrag von G DATA

Relevant

Relevanz von Security Operations Centern; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die mit dem Begriff SOC eher/sehr vertraut sind; 2026; in Prozent*

Glauben Sie, dass ein Security Operations Center (SOC) einen relevanten Beitrag zur IT-Sicherheit eines Unternehmens leisten kann?

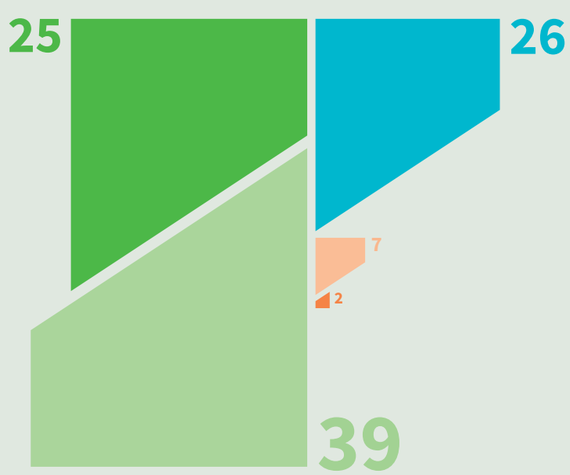
*Abweichung zu 100 Prozent durch Rundung. Quelle: Statista im Auftrag von G DATA

Signifikant

Bedeutung von externen Fachleuten; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die in IT-Security bzw. IT/EDV (inkl. Leitung) sowie Geschäftsführung, Vorstand oder Behörden-/Amtsleitung tätig sind; 2026; in Prozent*

Wie wichtig sind externe IT-Dienstleisterinnen und -Dienstleister (z. B. Systemhäuser, MSPs, MSSPs) für die Cyberresilienz Ihres Unternehmens?

- **Sehr wichtig:** Sie sind ein zentraler Bestandteil unserer IT-Sicherheit.
- **Eher wichtig:** Sie leisten einen wesentlichen Beitrag.
- **Teils, teils:** Sie unterstützen uns, sind aber nicht entscheidend.
- **Eher unwichtig:** Wir könnten weitgehend ohne sie auskommen.
- **Gar nicht wichtig:** Unsere IT-Sicherheit funktioniert vollständig ohne externe Dienstleister.

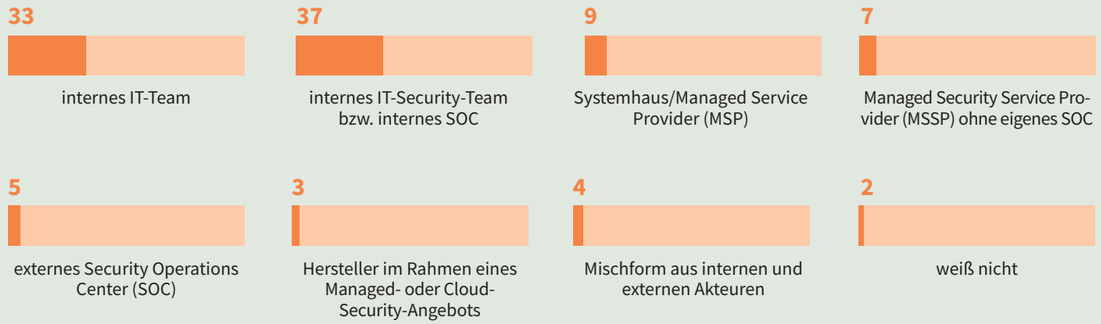


*Abweichung zu 100 Prozent durch Rundung. Quelle: Statista im Auftrag von G DATA

Ignorant

Interne und externe Akteure im operativen Betrieb der IT-Sicherheitsinfrastruktur; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die in IT-Security bzw. IT/EDV (inkl. Leitung) sowie Geschäftsführung, Vorstand oder Behörden-/Amtsleitung tätig sind; 2026; in Prozent

Wer übernimmt in Ihrem Unternehmen überwiegend den operativen Betrieb der IT-Sicherheitsinfrastruktur (z. B. Monitoring, Updates, Reaktion auf Vorfälle)?

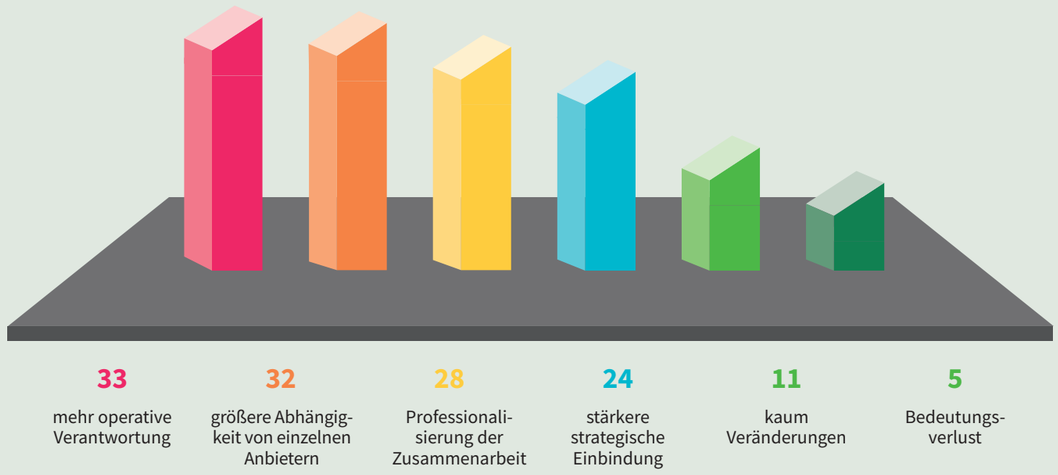


Quelle: Statista im Auftrag von G DATA

Rasant

Veränderung der Rolle externer IT-Fachleute; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die in IT-Security bzw. IT/EDV (inkl. Leitung) sowie Geschäftsführung, Vorstand oder Behörden-/Amtsleitung tätig sind; 2026; in Prozent*

Welche Veränderungen haben Sie in den vergangenen zwei Jahren bei der Rolle externer IT-Dienstleisterinnen und -Dienstleister (z. B. Systemhäuser, MSPs, MSSPs) in Ihrem Unternehmen beobachtet?

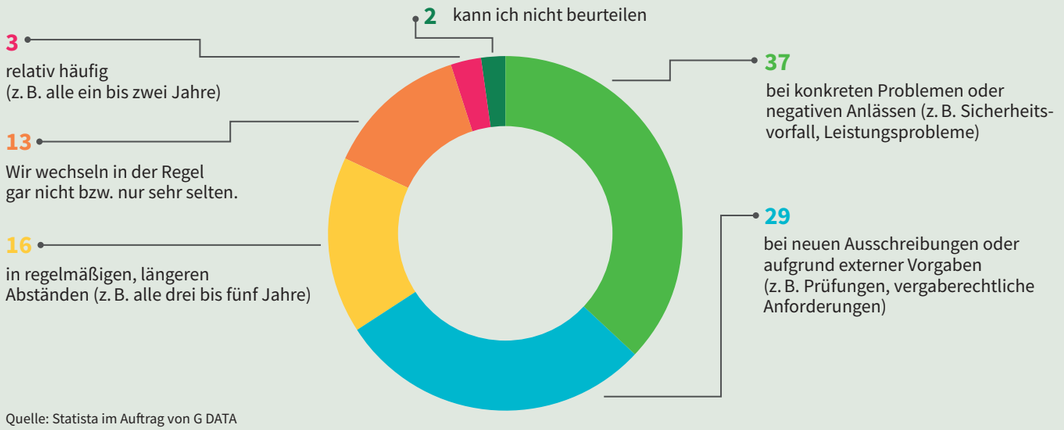


*Mehrfachnennung möglich. Quelle: Statista im Auftrag von G DATA

Wechselfälle

Anlässe für den Wechsel externer Sicherheitsfachleute; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die mit externen IT-Dienstleistern zusammenarbeiten und in IT-Security bzw. IT/EDV (Bereichs-, Abteilungs-, Teamleitung oder IT-Administration) sowie Geschäftsführung, Vorstand oder Behörden-/Amtsleitung tätig sind; 2026; in Prozent

Wann wechselt Ihr Unternehmen typischerweise den bzw. die externen IT-Sicherheitsfachleute (z. B. Systemhaus, MSSP)?

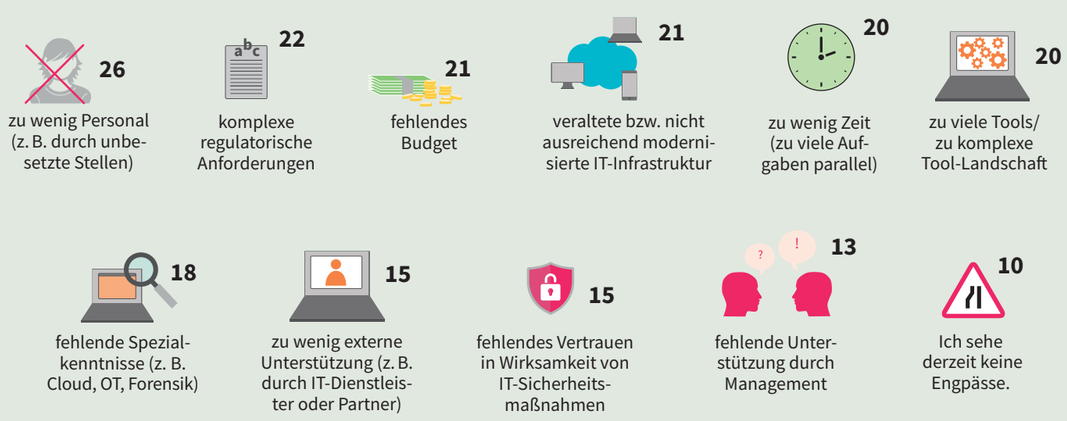


Quelle: Statista im Auftrag von G DATA

Engpässe

Größte Engpässe im Bereich IT-Sicherheit; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die in IT-Security bzw. IT/EDV (inkl. Leitung) sowie Geschäftsführung, Vorstand oder Behörden-/Amtsleitung tätig sind; 2026; in Prozent*

Welche dieser Aspekte stellen aktuell die größten Engpässe im Bereich IT-Sicherheit in Ihrem Unternehmen dar?

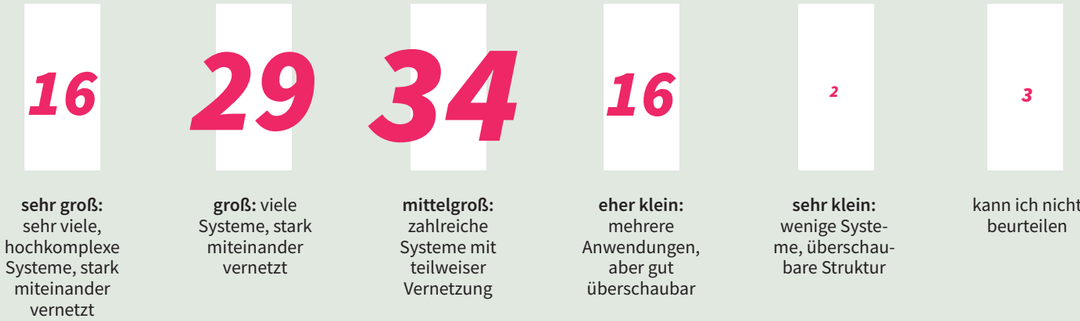


*Mehrfachnennung möglich, max. 3 Antworten. Quelle: Statista im Auftrag von G DATA

Größeneinschätzung

Einschätzung zur Komplexität der IT-Infrastruktur; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die in IT-Security bzw. IT/EDV (inkl. Leitung) sowie Geschäftsführung, Vorstand oder Behörden-/Amtsleitung tätig sind; 2026; in Prozent

Wie würden Sie die Größe und Komplexität der IT-Infrastruktur in Ihrem Unternehmen einschätzen?

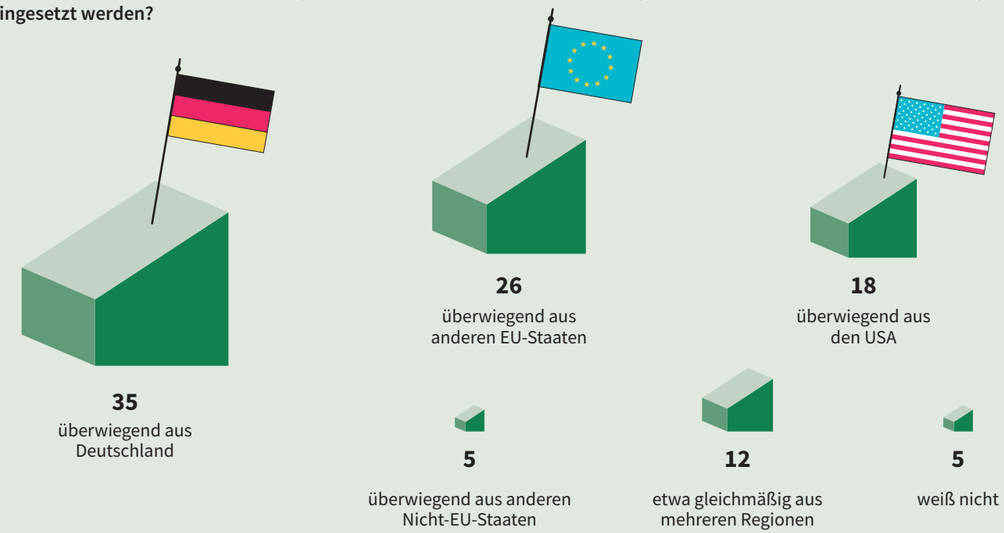


Quelle: Statista im Auftrag von G DATA

Standortentscheidung

IT-Sicherheitslösungen nach Standort; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die in IT-Security bzw. IT/EDV (inkl. Leitung) sowie Geschäftsführung, Vorstand oder Behörden-/Amtsleitung tätig sind; 2026; in Prozent*

Aus welcher Region bzw. welchen Regionen stammen die IT-Sicherheitslösungen, die in Ihrem Unternehmen überwiegend eingesetzt werden?

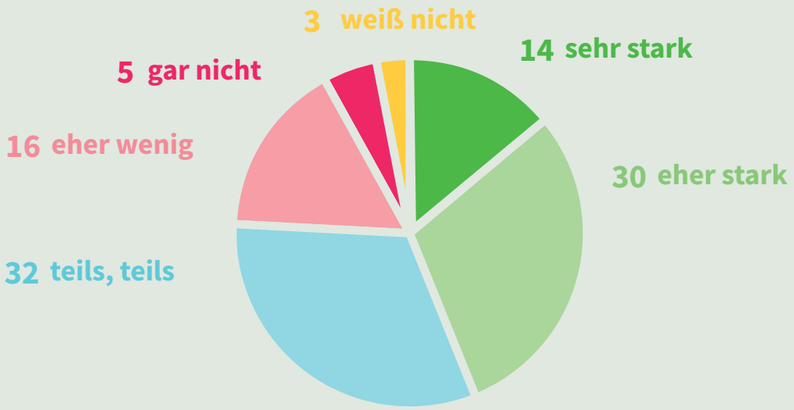


*Abweichung zu 100 Prozent durch Rundung. Quelle: Statista im Auftrag von G DATA

Beeinträchtigt

Beeinträchtigung durch Fachkräftemangel; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die in IT-Security bzw. IT/EDV (inkl. Leitung) sowie Geschäftsführung, Vorstand oder Behörden-/Amtsleitung tätig sind; 2026; in Prozent

Wie stark beeinträchtigt der Fachkräftemangel die IT-Sicherheit Ihrer Organisation?

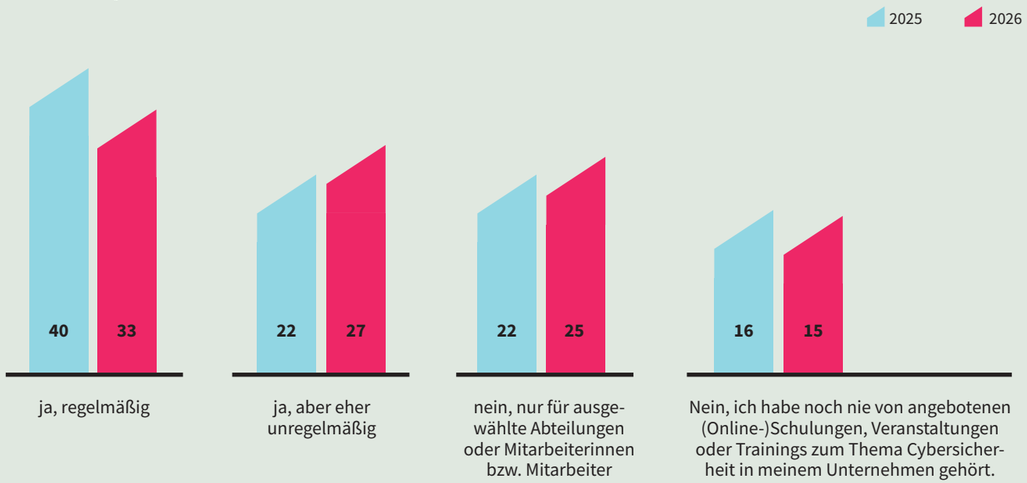


Quelle: Statista im Auftrag von G DATA

Vernachlässigt

Schulungen zum Thema Cybersicherheit; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; in Prozent

Bietet Ihr Unternehmen für alle Mitarbeiterinnen und Mitarbeiter (Online-)Schulungen/Veranstaltungen/Trainings rund um das Thema Cybersicherheit an?

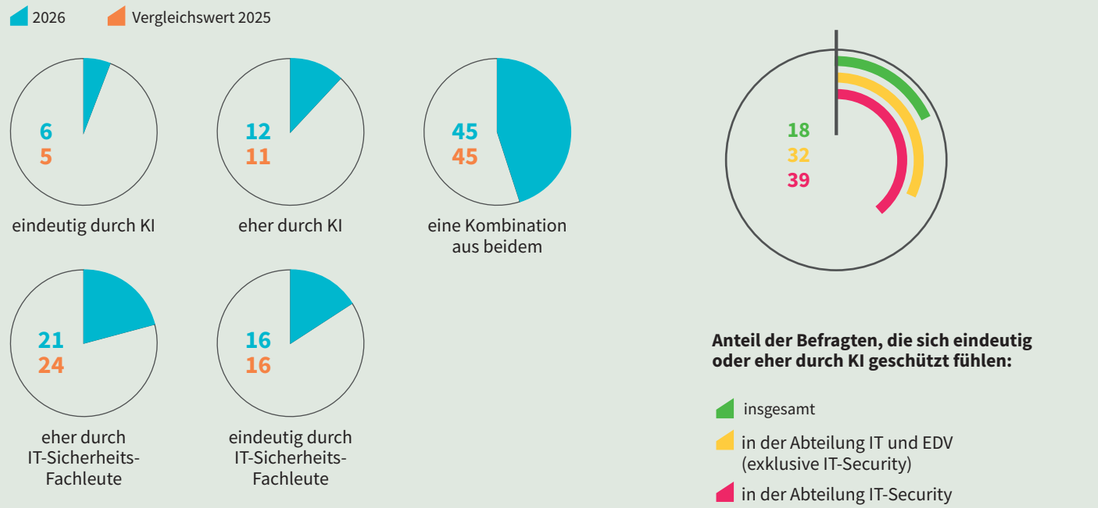


Quelle: Statista im Auftrag von G DATA

Geschützt

Schutz durch künstliche Intelligenz oder Sicherheitsfachleute; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; in Prozent

Würden Sie sich durch eine KI besser geschützt fühlen oder durch ein Team aus IT-Sicherheitsfachleuten?

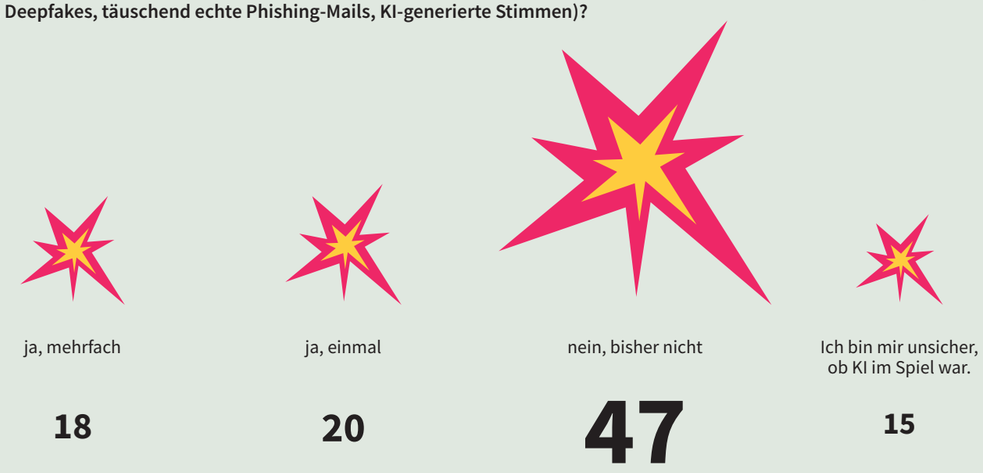


Quelle: Statista im Auftrag von G DATA

Geschätzt

Cyberangriffe mit KI; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2026; in Prozent

Haben Sie bereits Cyberangriffe oder Cyberangriffsversuche wahrgenommen, bei denen Sie vermuten, dass KI eingesetzt wurde (z. B. Deepfakes, täuschend echte Phishing-Mails, KI-generierte Stimmen)?

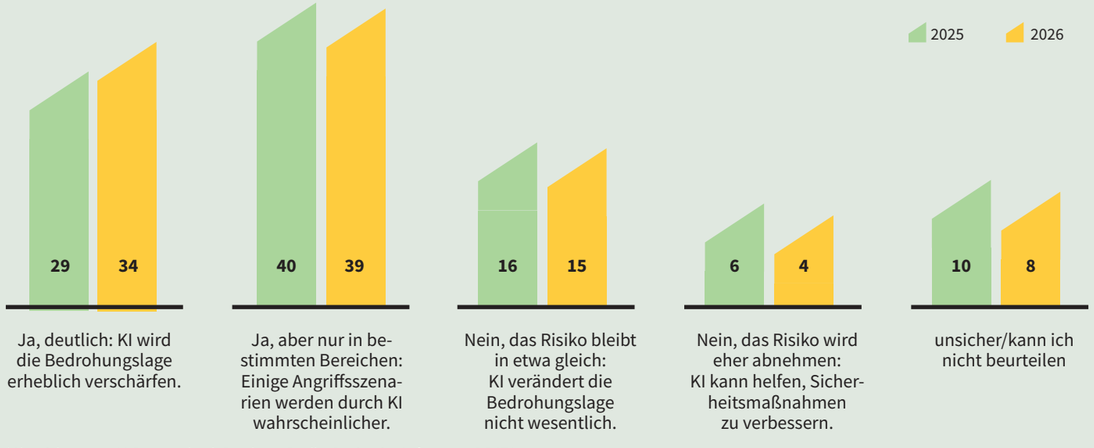


Quelle: Statista im Auftrag von G DATA

KI bedroht

Bedrohungen durch KI; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; in Prozent*

Erwarten Sie, dass Bedrohungen für die IT-Sicherheit durch den verstärkten Einsatz von KI zunehmen?



*Abweichung zu 100 Prozent durch Rundung. Quelle: Statista im Auftrag von G DATA

KI sichert

Verbesserung der IT-Sicherheit durch KI; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2026; in Prozent

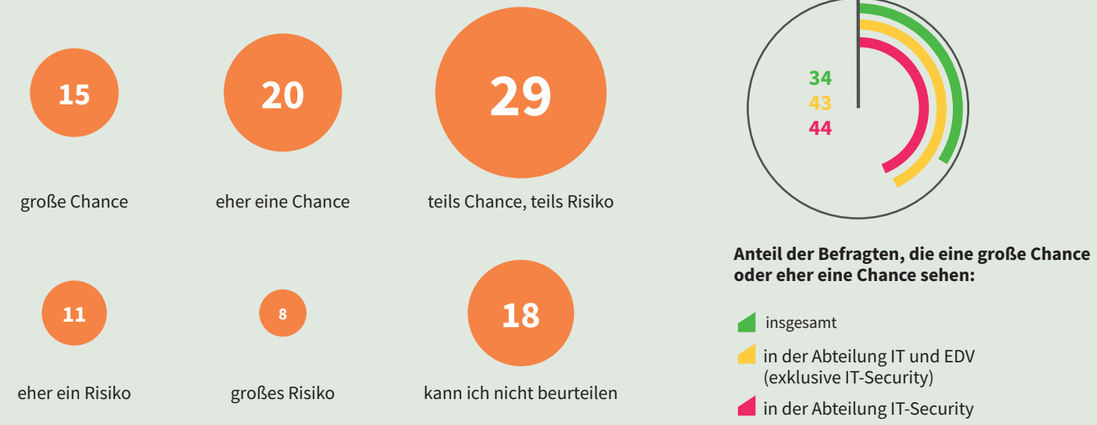
In welchen Bereichen kann KI aus Ihrer Sicht besonders zur Verbesserung der IT-Sicherheit beitragen?

*Mehrfachnennung möglich. Quelle: Statista im Auftrag von G DATA

Mehr Chancen

KI als Chance oder Risiko; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2026; in Prozent*

Wie bewerten Sie den Einsatz von KI im Bereich IT-Sicherheit derzeit insgesamt?

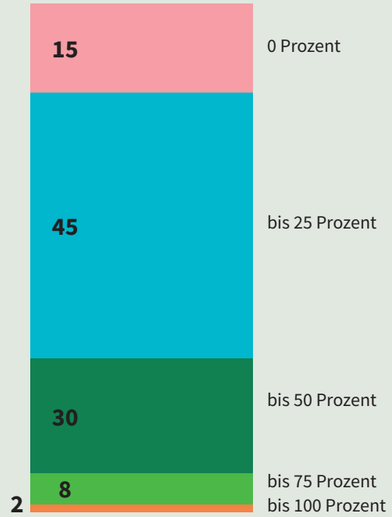


*Abweichung zu 100 Prozent durch Rundung. Quelle: Statista im Auftrag von G DATA

Mehr KI

KI als Arbeitsplatz-Bedrohung; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2026; in Prozent

Wie viel Prozent Ihrer täglichen Arbeit kann in den nächsten fünf Jahren von einer KI übernommen werden?



Quelle: Statista im Auftrag von G DATA

Mehr Mensch

KI und menschliche Expertise; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2026; in Prozent*

Welche Rolle wird menschliche Expertise künftig im Zusammenspiel mit KI in der IT-Sicherheit spielen?

*Abweichung zu 100 Prozent durch Rundung. Quelle: Statista im Auftrag von G DATA

Der Minister
Karsten Wildberger, Jahrgang 1969, ist seit Mai 2025 Bundesminister für Digitales und Staatsmodernisierung im Kabinett Merz. Zuvor war er CEO von Ceconomy, dem Mutterkonzern von Media-Markt und Saturn. Er hat Physik studiert.

„Wollen wir Kunden sein? Oder wollen wir gestalten?“

Karsten Wildberger will als Bundesdigitalminister das Land technologisch modernisieren. Schafft das neue Gefahren? Ein Gespräch über KI als Cyberwaffe, digitale Souveränität und die Frage, was man gegen Quantencomputer tun kann, die fast jede Verschlüsselung überflüssig machen.

Interview: Markus Albers

Foto: © BMDS/Woithe

Herr Wildberger, fast alle Verwaltungsangestellten in Deutschland – 96 Prozent – arbeiten täglich mit Microsoft-Produkten. Allein für diesen einen US-amerikanischen Softwareanbieter zahlte der Bund 2025 mehr als 481 Millionen Euro Lizenzgebühren. Bundesländer wie Schleswig-Holstein oder Bayern setzen zunehmend auf Open-Source-Lösungen. Das scheint konsequent, aber ist es auch sicher?
Dabei geht es ja um klassische Office-Anwendungen – Textverarbeitung, Tabellenkalkulation, E-Mail. Produkte, die wir seit Jahrzehnten in der Microsoft-Welt genutzt haben. Wir erleben gerade eine Situation, in der aus Souveränitätsgründen die Frage anders gestellt wird. Ich schaue auf dieses Thema aber nicht nur defensiv, sondern auch offensiv: Wie kann es sein, dass wir in einem so wichtigen Feld so lange keine eigenen Produkte gebaut haben, die sicher sind und Wachstum generieren?

Wie gehen Sie selbst im Ministerium damit um?
Wir testen Open-Source-Lösungen – Open Desk – bereits im Haus und in anderen Behörden auf mehreren Hundert Arbeitsplätzen. Und wir lernen viel von Schleswig-Holstein. Aber man muss ehrlich sein: Es gibt Bereiche, da ist die Open-Source-Software noch nicht so leistungsfähig wie das kommerzielle Äquivalent.

Wir wollen unabhängig werden, schaffen es aber nicht?
Souveränität bedeutet für mich keine Abschottung. Wir im Digitalministerium führen sehr klare Gespräche mit den großen Technologieunternehmen, auch darüber, dass sie sich auf unsere Anforderungen einstellen müssen. Und gleichzeitig müssen wir viel mehr Kraft aufbringen, eigene Lösungen zu entwickeln – und nicht, in dem wir nachbauen, was es schon gibt, dann kämen wir wieder zu spät. Die Office-Anwendungen von morgen werden KI-getrieben sein, KI-Agenten werden einen Großteil der repetitiven Arbeit übernehmen. Deshalb müssen Bund und Länder in agentische KI-Lösungen investieren. In Anbieter wie Aleph Alpha, Mistral und andere.

Manche Experten sagen, die Modelle selbst werden bald eine Commodity sein – der Wettbewerb entscheidet sich auf der Anwendungsebene.
Da wäre ich sehr vorsichtig. Wenn Sprachmodelle eine Commodity wären: Warum ist der Zugang zu den leistungsfähigsten Modellen derzeit noch eingeschränkt? Wenn sich Modelle aus sich heraus permanent verbessern, erreichen diese Systeme asymptotisch die maximale Leistungsfähigkeit, die die zugrundeliegende Hardware erlaubt. Das soll Commodity sein? Ich halte dieses Argument für eine gefährliche Beruhigungspille. Die Unternehmen, die heute führend sind, werden dadurch einen Vorsprung halten, der sehr schwer aufzuholen ist. Der Zug ist schon fast abgefahren. Trotzdem sage ich: Wir müssen aufspringen. Es gibt noch genug Innovationen, die man leisten kann.

Vor einer Weile warnte Anthropic-Chef Dario Amodei, sein neues Modell „Mythos Preview“ sei so gut darin, Sicherheitslücken in Software aufzuspüren, dass man es nicht einfach für alle Nutzer bereitstellen könne. Den Zugang zum öffentlich zugänglichen Nachfolger Fable 5, und zu Mythos 5, der wegen der Dual-Use-Gefahr zunächst nur ausgewählten Partnern zur Verfügung stand, musste Anthropic kurz nach der Einführung aufgrund einer Verordnung der US-Regierung deaktivieren. Wie schauen Sie als Digitalminister auf die Entwicklungen?
Es geht nicht allein um Mythos. Alle Modelle gefährden die Cybersicherheit, seitdem sie leistungsfähig genug sind, um Software zu erstellen. Wenn sie programmieren können, können sie auch Schwachstellen finden – oder Code härten. Was sich mit Mythos verändert hat, ist die Qualität dieses Sprungs.

Inwiefern?
Die Leistungsfähigkeit der Modelle steigt nicht linear, sondern in Sprüngen. Und irgendwann erreicht ein Sprung ein Niveau, auf dem es nicht mehr darum geht, ob die Technologie theoretisch gefährlich sein könnte. Dann ist sie es. Vergleichbare Benchmarks sehen wir auch bei anderen Modellen – Systeme, die Sicherheitslücken in Code mit einer Geschwindigkeit und Präzision finden, die kein menschlicher Analyst erreichen würde. Das wird sicherlich nicht der letzte Sprung dieser Art gewesen sein.

Überwiegt für Sie bei KI Chance oder Risiko?
Das hängt davon ab, wer die Technologie zu welchem Zweck einsetzt. Die Chancen sind riesig: Krebsforschung, nachhaltige Energie, vielleicht sogar Kernfusion. Wir reden davon, Menschenleben zu retten und endlich Probleme zu lösen, die wir seit Jahrzehnten nicht in den Griff bekommen haben.

Und die Risiken?
Meine persönliche Einschätzung: Solange die Regeln – im Sinne eines ethischen Kompasses – global nicht klar sind, muss man die Risiken mit sehr viel Ernsthaftigkeit betrachten. Das Problem in Europa war allerdings nicht, dass wir zu wenig auf Risiken geschaut haben. Wir haben uns bei der Innovation vielmehr zu stark auf das mögliche Risiko fokussiert. Das ist einer der Gründe, warum wir bei diesen Technologien heute nicht führend sind. Beides ist gefährlich, auf unterschiedliche Weise.

Sie haben gefordert, Europa brauche ein eigenes Modell auf dem Niveau von Mythos. Können wir das überhaupt?
Die Grundfrage ist: Wollen wir Kunden sein oder wollen wir mitgestalten? Wenn ein Modell bestimmte Fähigkeiten hat – Programmierung, Cybersicherheit, strategische Analyse – dann macht es Sinn, in diesen Bereichen auch selbst Fähigkeiten aufzubauen. Nicht weil man glaubt, morgen OpenAI zu überholen. Sondern weil Abhängigkeit in Schlüsseltechnologien immer ein Risiko ist – und weil Wertschöpfung dort entsteht, wo man mitbaut. Diese Antwort hätte ich mir für die vergangenen zwanzig Jahre in viel kraftvollerer Form gewünscht.

Und was tun Sie jetzt?
Wir haben uns als Bundesregierung gemeinsam mit Kanada dafür eingesetzt, dass sich Aleph Alpha und das kanadische ›

Unternehmen Cohere zusammenschließen. Eine neue Firma mit zwei Pässen – kanadisch und deutsch – mit Entwicklungskapazitäten auf beiden Seiten, auch unterstützt von der Schwarz Gruppe als Investor. Das ist ein erster Schritt. Wir arbeiten parallel auch sehr gut mit Mistral und SAP zusammen, die gemeinsam eine souveräne KI für die Verwaltung entwickeln. Ich glaube, bei der Schnelllebigkeit dieses Feldes braucht man mehrere vielversprechende Optionen. Der Staat kann dabei eine Rolle spielen – als Ankerkunde, indem er Produkte aktiv einsetzt, und durch gezielte Investitionen, wo diese sinnvoll sind. So konnten wir kürzlich den Auftrag für eine KI-Cloud für die Verwaltung an ein heimisches Konsortium vergeben, auch weil wir in der Ausschreibung Souveränitätskriterien aufgenommen haben.

Aleph Alpha hatte den Ansatz des eigenständigen Frontier-Modells ja aufgegeben …

Was jetzt durch die Fusion mit Cohere entsteht, ist etwas anderes: größere Kapazitäten, Zusammenspiel von deutsch-kanadischen Talenten, ein breiteres Investitions-Ökosystem. Das ist keine Garantie für Erfolg, aber es sind ganz andere Voraussetzungen, um zu skalieren, und es besteht die Chance, dass hier ein global wettbewerbsfähiger KI-Champion entsteht – und das sollte der Staat unterstützen.

Sie treiben mit Macht die Digitalisierung der Verwaltung voran, gleichzeitig sprechen Sie über KI-basierte Cyberrisiken. Ist das nicht ein Widerspruch – je digitaler der Staat, desto größer die Angriffsfläche?

Das ist eine echte Spannung, die man ernst nehmen muss. Absolute Sicherheit gibt es nie. Aber der Maßstab muss sein, alle möglichen Vorkehrungen zu treffen und dem jeweils besten Standard zu genügen. Dazu gehört auch die Frage: Wenn etwas schiefgeht, sind wir in der Lage zu reagieren?

Aber diese Reaktionen müssen immer schneller erfolgen.

Ja, was KI grundlegend verändert, ist die Geschwindigkeit. Angriffe passieren heute auf einer Zeitskala, auf der menschliche Reaktion allein nicht mehr ausreicht. Das heißt, wir müssen von einer Welt, in der Cybersicherheit von Mensch zu Mensch organisiert wird, in eine Welt autonomer Systeme und Agenten kommen. Das BSI arbeitet daran, wir arbeiten daran, gemeinsam mit europäischen und wo möglich amerikanischen Partnern.

Haben Sie ein konkretes Beispiel aus der Praxis?

Wenn wir im Ministerium eine Software entwickeln, setzen wir KI ein, um den Code automatisch auf Schwachstellen zu prüfen – ein automatisierter Sicherheitsaudit in der Entwicklungsphase. Die Fragen sind dann immer: Welches Modell steht uns zur Verfügung? Wie groß ist der Unterschied zwischen dem stärksten verfügbaren Modell und dem zweitbesten? Und welche Vulnerabilität entsteht dadurch?

Sie haben auf der re:publica gesagt, die Hacker-Community solle gern helfen, die digitale Brieftasche – die EUDI-Wallet – sicher zu machen, die im Januar 2027 in Betrieb gehen wird. Das klang ein bisschen nach einer Einladung zum Angriff.

Es war kein Witz und keine spontane Äußerung. Wir entwickeln in wichtigen Bereichen der öffentlichen Verwaltung mit Open Source. Der Code ist einsehbar. Das ist eine bewusste Entscheidung. Und ja, wir laden ein, uns zu testen – der Chaos Computer Club gehört beispielsweise zu den Akteuren, die das nutzen sollen. Wir haben das formalisiert, ein Bug-Bounty-Programm mit dem wir Hacker aufrufen, die Systeme zu testen, wird vor dem regulären Launch starten.

Wie läuft das ab?

Der zugrunde liegende Gedanke lautet: Schwachstellen in Software gibt es immer. Wichtiger als die Frage, ob jemand etwas findet, ist die Frage, wie schnell wir es schließen können. Und je mehr Talente mitdenken, desto besser. Das ist weniger Ausdruck von Misstrauen in die eigene Arbeit, vielmehr vernünftige Sicherheitspraxis.

Trotzdem gibt es Bürger, die sagen: Ich will meine Ausweisdaten nicht auf dem Handy haben.

Diese Sorgen nehme ich sehr ernst. Gleichzeitig ist es wichtig zu erklären, wie die Technologie tatsächlich funktioniert. Die Wallet ist kein einfaches Abbild des Ausweises auf dem Telefon. Der Datensatz liegt nicht vollständig auf dem Gerät. Er wird erst zusammengebaut, indem ein externer Schlüssel mit dem Gerät zusammengebracht wird. Das ist deutlich sicherer. Wenn das Gerät verloren geht, sind die Daten trotzdem sicher.

So sicher wie das eigene Portemonnaie?

Das analoge Portemonnaie ist auch nicht sicher. Man kann es verlieren, es kann gestohlen werden. Wir tun häufig so, als sei die physische Welt das Sicherheitsideal – und zugleich hinterlassen wir im Internet und auf Social Media täglich massenhaft Daten, ohne nachzudenken. Da ist eine erhebliche Diskrepanz im Anspruch.

Was ist Ihre positive Antwort auf die Sorge – jenseits des technischen Arguments?

Transparenz! Wir können viel von den Esten lernen, die diesen Weg seit den 1990er-Jahren gehen. Das Prinzip ist eine Art Beweislastumkehr: Nicht ich werde vom Staat kontrolliert – ich kontrolliere, was der Staat mit meinen Daten macht. Konkret heißt das: In der Wallet werden wir ein Nutzungsregister für den Nutzer führen. Ich kann nachverfolgen, wo ich meine Daten wann verwendet habe – zum Beispiel für die Kfz-Zulassungsstelle oder eine Altersverifikation für einen Kauf im Onlineshop. Es wird keine Transaktion möglich sein, von der ich nichts weiß. Das ist ein ganz wichtiges Versprechen.

Schauen wir auf die Sicherheit in deutschen Unternehmen. Man liest, dass im vergangenen Jahr mehr als 70 Prozent von Cyberangriffen betroffen waren oder dies vermuten. Wie schätzen Sie die Gefährdung ein?

Die überwiegende Zahl dieser Versuche wird abgewehrt. Aber es gibt Fälle, in denen jemand tatsächlich ins System kommt. Das klassische Beispiel: Ransomware. Jemand verschlüsselt Ihre Systeme, Sie kommen nicht mehr ran. Das passiert. Die häufigsten Ursachen sind fehlende Updates, keine Multifaktor-Authentifizierung und menschliche Fehler. Das Risiko wächst mit der Menge an Legacy-Systemen. Und da haben wir in Deutschland ein ernstes Problem.

Welches?

Nehmen Sie den Gesundheitssektor. Wir erlauben uns im Jahr 2026, kritische Gesundheitsinfrastruktur auf On-Premise-Servern zu betreiben, die irgendwo in einem Serverraum stehen. Das geht so nicht, das ist aus der Zeit gefallen. Eine Cloud-Lösung souveräner Bauart wäre sicherer, skalierbarer, besser wartbar. Aber unser Datenschutzrahmen macht das extrem schwierig.

Viele argumentieren, dass On-Premise-Hosting sicherer sei als die Nutzung einer cloudbasierten Infrastruktur.

Aber doch nicht mehr im Jahr 2026! Eine zerklüftete Systemlandschaft, in der jemand vergessen hat, irgendwo ein Sicherheitsupdate einzuspielen, ist keine Alternative zur modernen Cloud-Infrastruktur. Wir verfolgen beim Bund mit dem Deutschland-Stack genau diesen Weg: eine souveräne, sichere Cloud-Infrastruktur für Bund, Länder und Kommunen. Das wünsche ich mir auch für kritische Sektoren wie das Gesundheitswesen.

Wo sehen Sie positive Entwicklungen in der Digitalwirtschaft?

Wir haben im Bereich Cybersicherheit sehr starke Unternehmen und eine starke Forschung: das CISPA Helmholtz-Zentrum für Informationssicherheit, das Max-Planck-Institut für Sicherheit und Privatsphäre in Bochum. Unternehmen, die in Verschlüsselung und quantensicherer Kryptografie tätig sind. Wir haben ein starkes Ökosystem – wir müssen es nur besser aktivieren, koordinieren und als Wachstumsfeld begreifen.

Regulierung wie die EU-Richtlinie NIS-2 verpflichtet Unternehmen zu mehr Sicherheit – Mittelständler klagen, der Aufwand sei zu hoch. Können sich das nur die Großen leisten?

Ich bin vorsichtig mit dem Reflex, jeden Aufwand sofort als Bürokratie zu bezeichnen. Es gibt Dinge, die ich tun muss, weil sie Sicherheit erfordern. Das Aber: Man muss sehr genau hinschauen, ob die Regulierung in ihrer konkreten Umsetzung tatsächlich mehr Sicherheit erzeugt – oder ob sie hauptsächlich Berichte produziert. Ein Unternehmen, das jeden Monat einen Sicherheitsbericht schreibt, ist dadurch nicht zwangsläufig sicherer. Das ist ein Unterschied, den man in der Regulierungspraxis zu oft aus den Augen verliert.

Anderes Thema: In Deutschland fehlen Cybersecurity-Experten. Nimmt das Problem zu, weil junge Menschen nicht mehr Informatik studieren, wenn die KI eh alles programmiert?

Es ist sinnvoll, Informatik zu studieren. Aber das Studium wird anders aussehen. Was wir brauchen, sind Menschen, die lernen, in Koproduktion mit KI zu arbeiten – in jedem Beruf. Wer das nicht tut, wird unter Druck kommen. Wer es tut, wird leistungsfähiger sein als zuvor.

Wird die künstliche Intelligenz lediglich Rollen verändern oder wird sie bestimmte Berufe gänzlich überflüssig machen?

Ich kann mir einen Endzustand vorstellen, in dem wir wieder viele gute Arbeitsplätze haben – nur anders gewichtet. Mehr zwischenmenschliche Arbeit, neue Berufsbilder, neue Möglichkeiten. Aber der Weg dahin wird fordernd. Und er kostet auch etwas. Die Unternehmen, die mit KI enorme Wertschöpfung generieren, schaffen die Mittel, diesen Übergang zu gestalten. Wenn wir an dieser Wertschöpfung nicht teilhaben, weil sie woanders passiert, fehlen uns genau dann die Mittel, wenn wir sie am dringendsten bräuchten. Deshalb kämpfe ich so sehr für Wirtschaftswachstum im Technologiesektor.

Zum Schluss: Was fehlt Ihnen persönlich in der Sicherheitsdebatte?

Zwei Dinge! Das erste ist die Infrastruktur, die wir zu wenig mitdenken: Sicherheit fängt bei den Netzen an. Die 6G-Netze werden de facto KI in Echtzeit integrieren – auf dem Netz selbst, nicht nur auf Endgeräten. Das muss man sich so vorstellen, dass dann live in einem Telefonat zwischen zwei Sprachen übersetzt wird oder dass das Netz auf Wunsch direkt ein Transkript anfertigt. Das bedeutet, wer die Standards schreibt und die Infrastruktur baut, bestimmt auch, was möglich ist und was nicht. Heute werden diese Standards vor allem in China und den USA geschrieben. Europa droht zurückzufallen. Das ist auch eine Frage von Satelliten und Mobilfunk – wer hat diese Technologie? Wir müssen das viel stärker mit strategischer Industriepolitik betreiben, europäisch und mit der notwendigen Geschwindigkeit.

Und das zweite?

Das ist die Frage, wie wir mit deutschen und europäischen Champions umgehen. Wir reden viel über Abhängigkeit – aber wir feiern zu selten die Unternehmen, die in diesen Feldern tatsächlich etwas aufbauen.

Haben Sie ein Beispiel?

Ich war kürzlich bei einem Unternehmen, das Rechenzentren mit quantensicherer Lichtkommunikation verbindet – das ist heute schon Realität. Da haben wir in Deutschland führende Unternehmen und führende Forschung.

Das müssen Sie genauer erklären.

Quantencomputer stellen klassische Verschlüsselungsverfahren vor ein fundamentales Problem: Viele dieser Verfahren basieren auf der Schwierigkeit, große Zahlen in Primfaktoren zu zerlegen – ein Problem, das der Shor-Algorithmus auf einem hinreichend leistungsfähigen Quantencomputer lösen kann. Das ist kein theoretisches Szenario, sondern eine absehbare Bedrohung. Aber – und das ist die gute Nachricht – es gibt bereits heute Verschlüsselungsverfahren, die auch quantensicher sind. Und es gibt eben Quantenkommunikation: Signale, die mit Licht übertragen werden und durch die Gesetze der Quantenmechanik inhärent abhörsicher sind. Wenn jemand versucht, das Signal abzugreifen, bricht es zusammen.

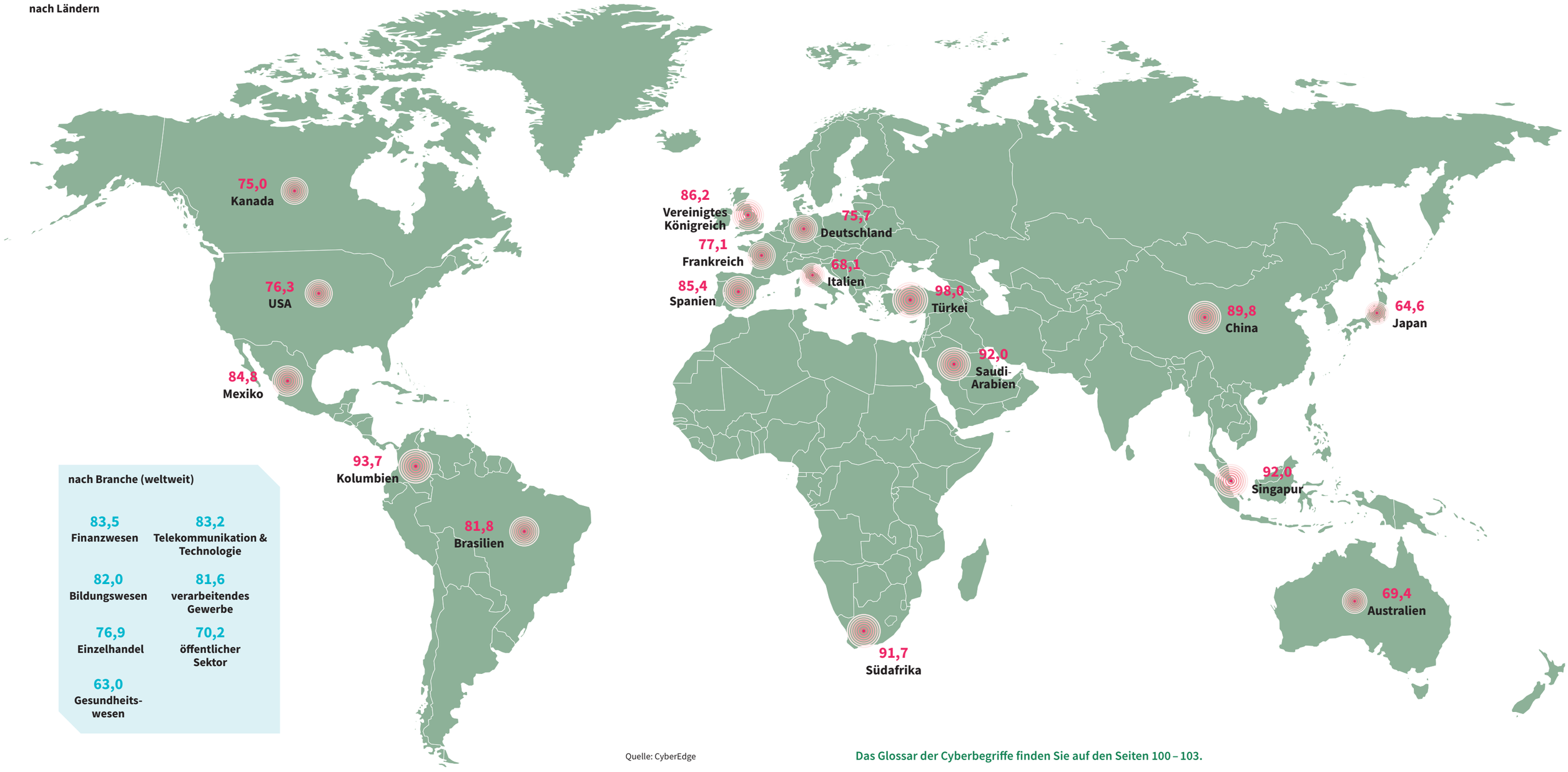
WELT

Mit Digitalisierung und künstlicher Intelligenz wachsen Möglichkeiten – und Risiken. Cyberangriffe treffen Unternehmen, öffentliche Verwaltung und Gesellschaft gleichermaßen. Sie verursachen hohe Schäden und gefährden kritische Prozesse. Cybersecurity ist zu einer wirtschaftlichen und gesellschaftlichen Herausforderung geworden.

Global verwundbar

Unternehmen, die in den vergangenen zwölf Monaten mindestens einem erfolgreichen Cyberangriff zum Opfer gefallen sind; IT-Sicherheits-Fachkräfte in einer privatwirtschaftlichen oder staatlichen Organisation, die mindestens 500 Mitarbeitende beschäftigt (n=1.200); weltweit; 2026; in Prozent

nach Ländern



nach Branche (weltweit)

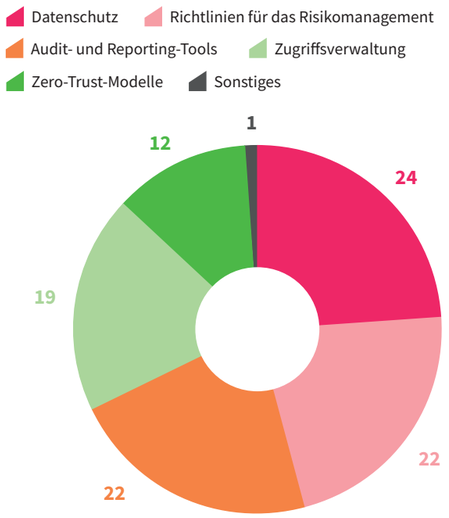
83,5 Finanzwesen	83,2 Telekommunikation & Technologie
82,0 Bildungswesen	81,6 verarbeitendes Gewerbe
76,9 Einzelhandel	70,2 öffentlicher Sektor
63,0 Gesundheitswesen	

Quelle: CyberEdge

Das Glossar der Cyberbegriffe finden Sie auf den Seiten 100 – 103.

Fokussiert

Fokusfelder der IT-Sicherheit; Sicherheitsexperten; weltweit; 2026; in Prozent



Quelle: Gallagher Security

Konzentriert

Künftige Entwicklung des Cyberbudgets; Sicherheitsverantwortliche (n=1.740); weltweit; 2025; in Prozent

Welche Investitionen haben für Sie bei der Zuweisung des Cyberbudgets Ihrer Organisation in den nächsten zwölf Monaten Priorität?

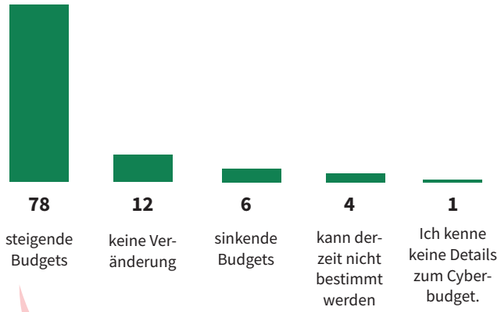
künstliche Intelligenz (KI)	36
Cloud-Sicherheit	34
Netzwerksicherheit und Zero Trust	28
Datenschutz	26
Bedrohungsmanagement	24
Cyber-Managed-Services	21
Sicherheitsbewusstseinstraining	19
Identitäts- und Zugriffsmanagement	18
Lieferketten- und Drittanbieterrisikomanagement	16
Endpunktsicherheit	15
Anwendungssicherheit	15
Sicherheit für Betriebstechnologie	10
vernetzte Produkte	10
Quantencomputing	8
API-Sicherheit	7
Mobilsicherheit	7

Quelle: PwC

Budgetiert

Künftige Entwicklung des Cyberbudgets; Sicherheitsverantwortliche, CFOs und Finanzdirektoren (n=2.027); weltweit; 2025; in Prozent

Wie wird sich das Cyberbudget Ihrer Organisation im nächsten Jahr verändern?

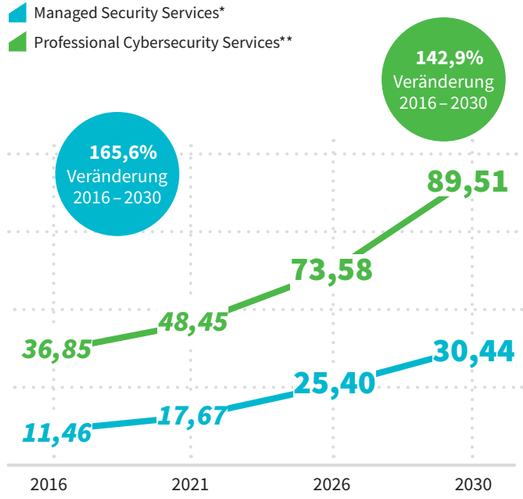


Anstieg um 15% oder mehr	7
Anstieg um 11 – 14%	10
Anstieg um 6 – 10%	32
Anstieg um 5% oder weniger	29

Quelle: PwC

Expandiert

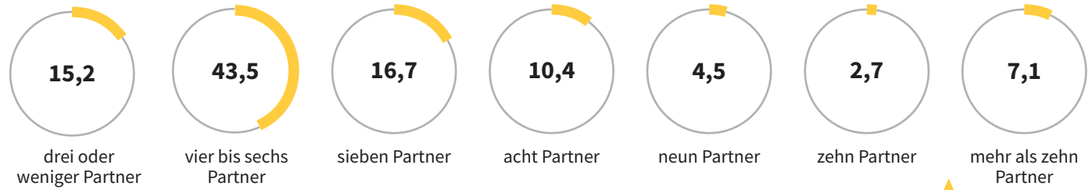
Umsatz mit Security-Services mit Prognose; weltweit; in Milliarden Euro



*Kontinuierliche, rund um die Uhr laufende Überwachungs- und Verwaltungsdienste. **Spezialisierte, zeitlich begrenzte Dienstleistungen, die auf spezifische Sicherheitsprojekte oder -initiativen fokussiert sind. Quelle: Statista Market Insights

Diversifiziert

Zahl unterschiedlicher Partner zur Erfüllung der IT-Anforderungen; Omdia-Kunden (n=5.280); weltweit; 2025; in Prozent



durchschnittliche Anzahl genutzter Partner pro Kunde: **6,3**

Quelle: Omdia

Reagiert

Auswirkung geopolitischer Volatilität auf Cybersicherheitsstrategien; Führungskräfte auf C-Level, Wissenschaftlerinnen und Wissenschaftler, Vertreterinnen und Vertreter der Zivilgesellschaft sowie Verantwortliche für Cybersicherheit im öffentlichen Sektor (n=804); weltweit; 2026; in Prozent*

Hat sich die Cybersicherheitsstrategie Ihrer Organisation aufgrund geopolitischer Unsicherheiten verändert?

*Mehrfachnennung möglich. Quelle: World Economic Forum

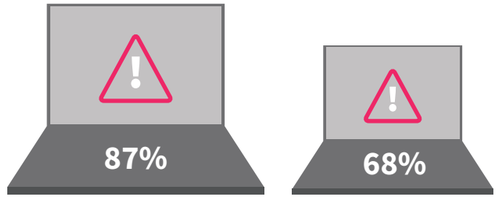
Limitiert

Größte Herausforderungen im Management der Cybersicherheit; kleinere Unternehmen unter 500 Mitarbeitende (n=2.210); Kanada, USA, Frankreich, Deutschland, Spanien, Portugal, Vereinigtes Königreich, Südafrika; 2026; in Prozent

Quellen: Sage, IDC

Irritiert

Zusammenhang zwischen Cyberangriffen und Investitionen in Schulungen; Mitarbeitende, die für die Cybersicherheitsstrategie verantwortlich sind (n=5.750); Vereinigtes Königreich, USA, Frankreich, Deutschland, Spanien, Irland, Portugal; 2025



Anteil der Unternehmen, die in den vergangenen zwölf Monaten **einen Cyberangriff erlebt haben** und in Schulungen investieren

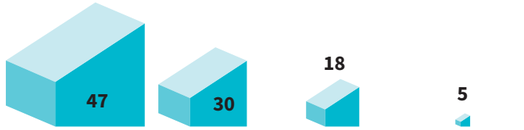
Anteil der Unternehmen, die in den vergangenen zwölf Monaten **keinen Cyberangriff erlebt haben** und in Schulungen investieren

Quelle: Hiscox

Priorisiert

Bedeutung digitaler Souveränität und lokaler Cloudspeicherung; Fach- und Führungskräfte aus der globalen Mobilfunk-, Telekommunikations- und Technologiebranche (n= rund 200); weltweit; 2026; in Prozent

Wie wichtig sind Datensouveränität und die Speicherung von Daten in lokalen Cloud-Infrastrukturen für Ihre Kundinnen und Kunden?



kritisch: ein wesentlicher Faktor für Vertrauen und Compliance

wichtig: relevant, hat aber nicht die höchste Priorität

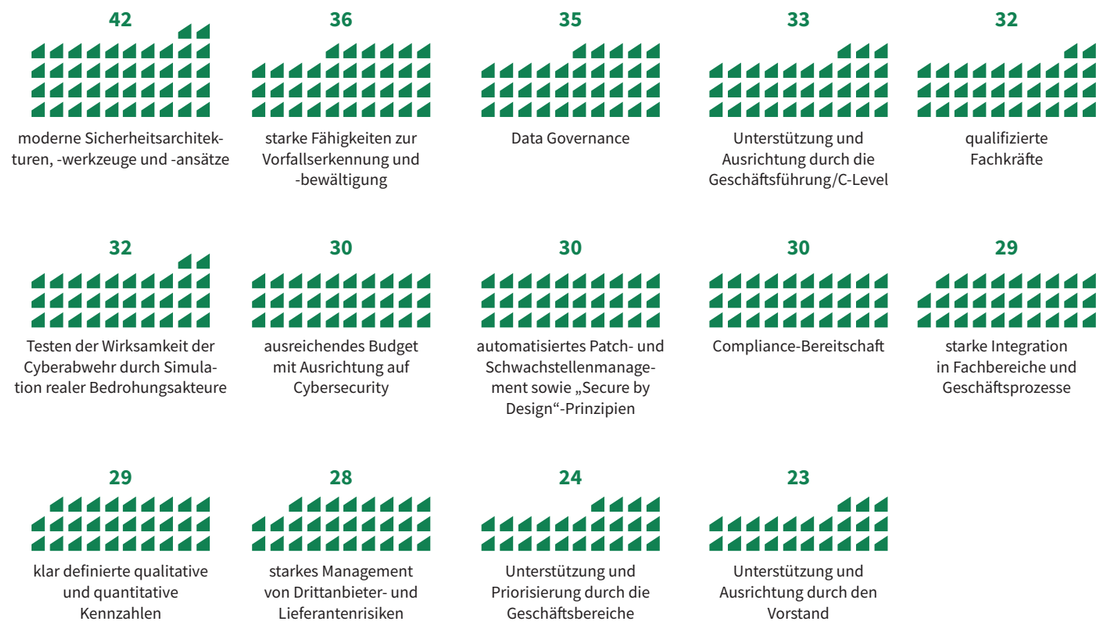
neutral: nur für bestimmte Kundensegmente relevant

gering: hat nur wenig Einfluss auf Kundenentscheidungen

Quellen: Mobile World Live, Globalstar, bmc helix, ANS

Orchestriert

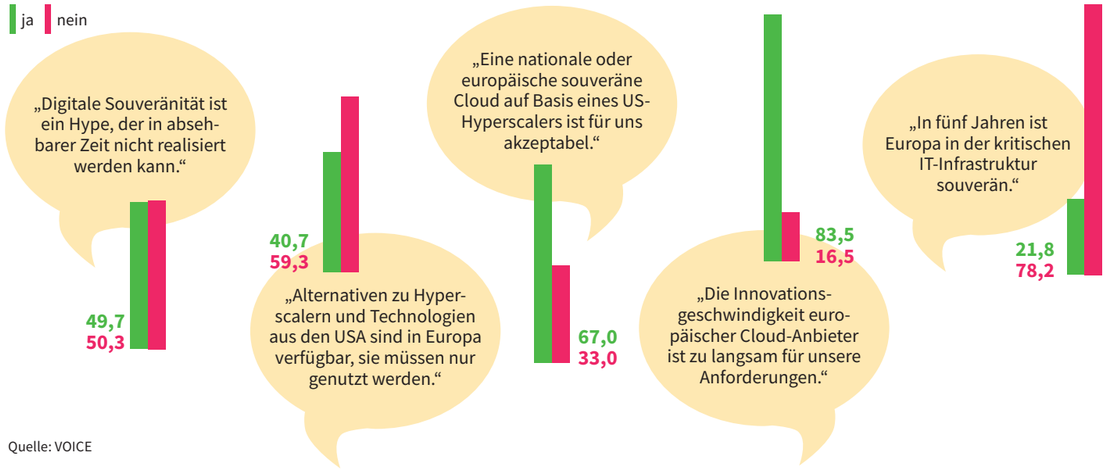
Wichtigste Treiber des Cybervertrauens in Organisationen; Geschäfts- und Technologieführungskräfte (n=1.058); weltweit; 2026; in Prozent



Quelle: Deloitte

Polarisiert

Thesen zur digitalen Souveränität in Europa; IT-Verantwortliche (n=268); Europa; 2026; in Prozent

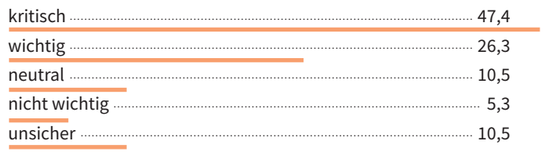


Quelle: VOICE

Favorisiert

Bedeutung von Open-Source-Software für digitale Souveränität; Technologie- und Politikführer (n=mehr als 270); Europa; 2025; in Prozent

Wie wichtig ist Open-Source-Software für die Strategie Ihrer Organisation zur digitalen Souveränität?



Quelle: Wire

mehr als **75%**

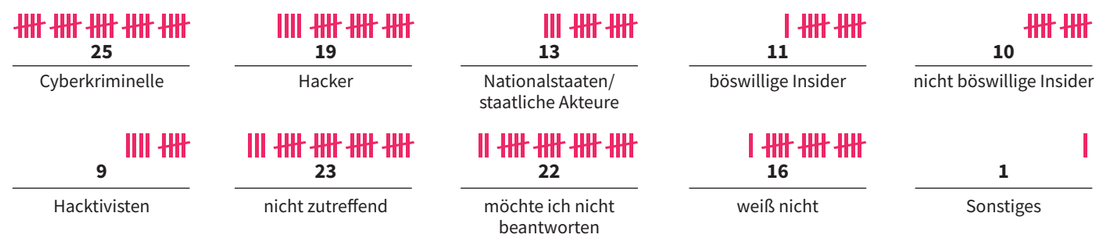
Anteil der Unternehmen außerhalb der USA, die bis 2030 eine Strategie zur digitalen Souveränität haben, die durch eine souveräne Cloud-Strategie unterstützt wird

Quelle: Gartner

Identifiziert

Bedrohungsakteure; Cybersicherheits-Fachkräfte (n=3.812); weltweit; 2025; in Prozent*

Wenn Ihre Organisation in diesem Jahr Opfer eines Cyberangriffs wurde: Welche Bedrohungsakteure waren dafür verantwortlich?

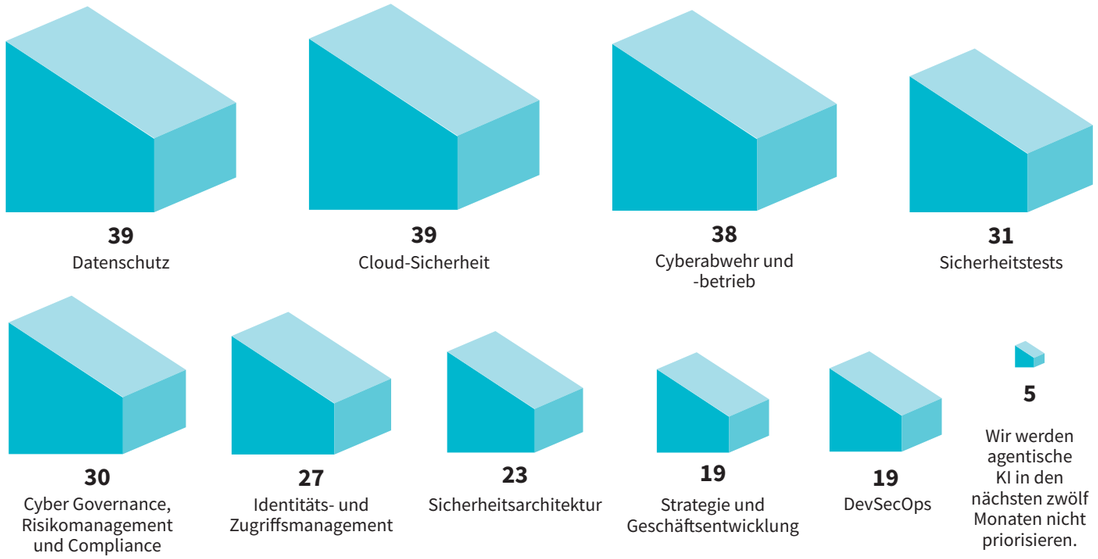


*Mehrfachnennung möglich. Quelle: ISACA

Eigenständige Unterstützung

Künftig priorisierte Bereiche für agentische KI*; Sicherheitsverantwortliche (n=1.740); weltweit; 2025; in Prozent

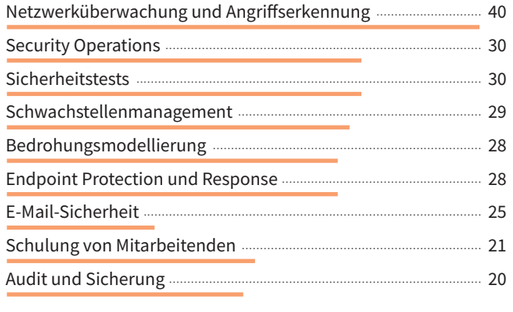
In welchen Cyberbereichen wird Ihre Organisation im nächsten Jahr agentische KI priorisieren, um effizienter und produktiver zu werden?



*KI-Systeme, die nicht nur auf Befehle reagieren, sondern selbstständig komplexe Ziele planen, Aktionen ausführen und Werkzeuge bedienen. Quelle: PwC

Schnelle Effizienzen

Schnellste Effizienzgewinne durch KI-Sicherheistools; Personen, die in Unternehmen und Organisationen für Cybersicherheit verantwortlich sind (n=16.029); weltweit; 2025; in Prozent

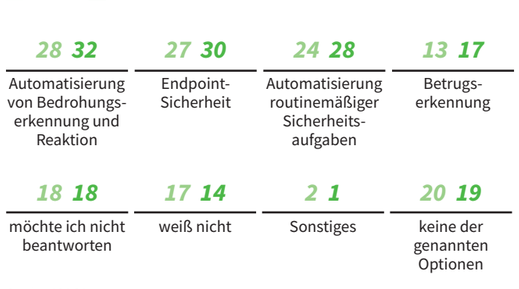


Quelle: (ISC)²

Gezielte Automatisierung

Einsatz von KI in Sicherheitsoperationen; Cybersicherheits-Fachkräfte (n=3.812); weltweit; in Prozent

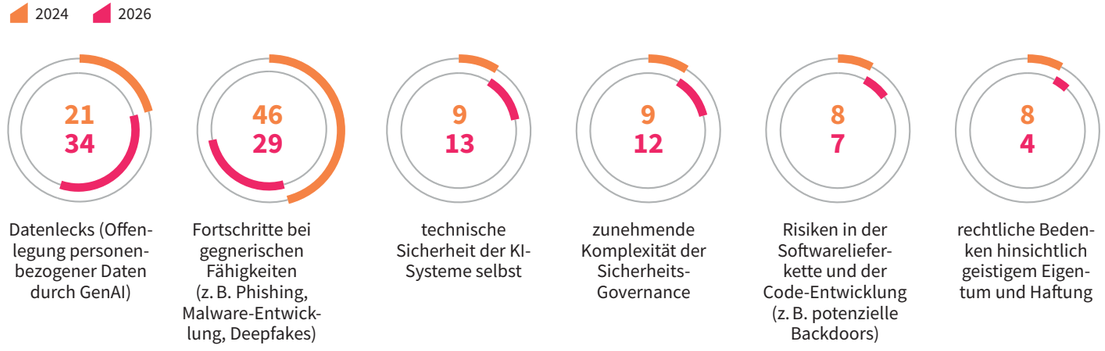
Nutzt Ihre Organisation KI in einem der folgenden Bereiche der Sicherheitsoperationen?



Quelle: ISACA

Wachsende Bedenken

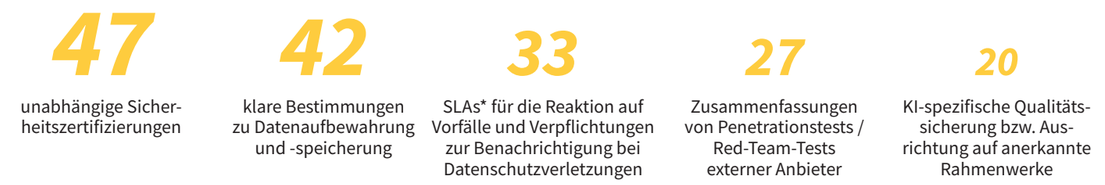
Größte Sorgen zu generativer KI in der Cybersicherheit; Führungskräfte auf C-Level, Wissenschaftlerinnen und Wissenschaftler, Vertreterinnen und Vertreter der Zivilgesellschaft sowie Verantwortliche für Cybersicherheit im öffentlichen Sektor (n=804); weltweit; in Prozent



Quelle: World Economic Forum

Klare Nachweise

Nachweise, die Vertrauen in die KI-Sicherheit eines Drittanbieters schaffen; kleinere Unternehmen unter 500 Mitarbeitende (n=2.210); Kanada, USA, Frankreich, Deutschland, Spanien, Portugal, Vereinigtes Königreich, Südafrika; 2026; in Prozent



*Ein Service Level Agreement (SLA) ist ein Vertrag zwischen einem Dienstleister und einem Kunden, der den zu erbringenden Service und das zu erwartende Leistungsniveau festlegt. Quellen: Sage, IDC

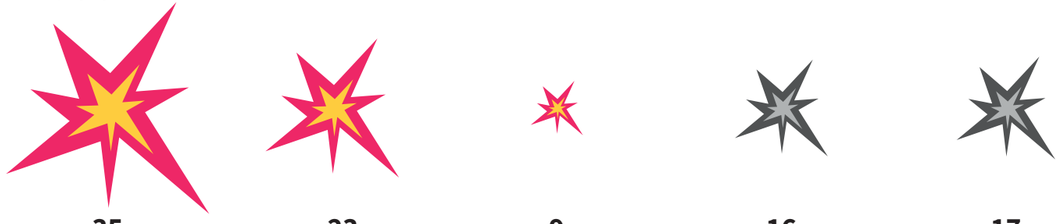
Breite Vorbereitung

Vorbereitung auf KI-Bedrohungen; Mitarbeitende, die für die Cybersicherheitsstrategie verantwortlich sind (n=5.750); Vereinigtes Königreich, USA, Frankreich, Deutschland, Spanien, Irland, Portugal; 2025; in Prozent

Quelle: Hiscox

Steigende Angriffe

Entwicklung der Cyberangriffe im Vergleich zum Vorjahr; Cybersicherheits-Fachkräfte, (n=3.812); weltweit; 2025; in Prozent



35 mehr Angriffe

23 gleich viele Angriffe

9 weniger Angriffe

16 möchte ich nicht beantworten

17 weiß nicht

Quelle: ISACA

Wachsende Risiken

Einschätzung der Veränderung von Cyberrisiken im vergangenen Jahr; Führungskräfte auf C-Level, Wissenschaftlerinnen und Wissenschaftler, Vertreterinnen und Vertreter der Zivilgesellschaft sowie Verantwortliche für Cybersicherheit im öffentlichen Sektor (n=804); weltweit; 2026; in Prozent

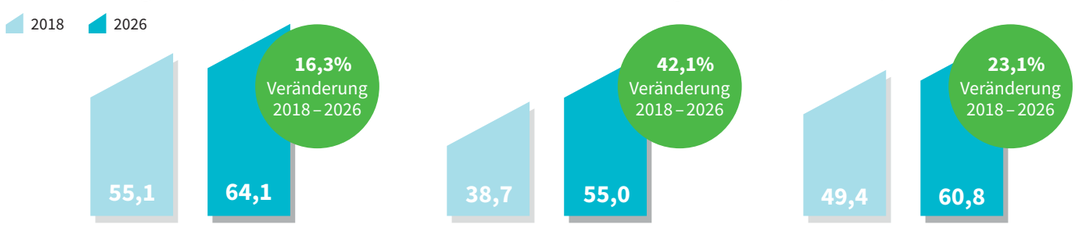
Cyberrisiko — zugenommen | gleich geblieben | abgenommen

zugenommen	gleich geblieben	abgenommen	
87	13	0	Schwachstellen durch KI
77	21	2	Cyberbetrug und Phishing
65	32	3	Störungen der Lieferkette
58	39	3	Ausnutzung von Softwareschwachstellen
54	39	7	Ransomware-Angriffe
32	61	7	Bedrohungen durch Insider
28	54	18	Denial-of-Service-Angriffe

Quelle: World Economic Forum

Hohe Schäden

Ransomware: Angriffe, Bezahlung, Datenrettung; IT-Sicherheits-Fachkräfte in einer privatwirtschaftlichen oder staatlichen Organisation, die mindestens 500 Mitarbeitende beschäftigt (n=1.200); weltweit; in Prozent



Anteil der Organisationen, die Opfer von Ransomware geworden sind

Anteil der betroffenen Organisationen, die Lösegeld zahlen

Anteil der Lösegeldzahler, die Daten wiederhergestellt haben

Quelle: CyberEdge

Regelmäßige Prüfungen

Häufigkeit von Cyberrisikobeurteilungen; Cybersicherheits-Fachkräfte (n=3.812); weltweit; 2025; in Prozent

Wie häufig wird in Ihrem Unternehmen eine Cyberrisikobewertung durchgeführt?

2 nie

11 monatlich

20 alle ein bis sechs Monate

9 alle sieben bis zwölf Monate

40 jährlich

4 alle ein bis zwei Jahre

3 alle zwei Jahre oder seltener

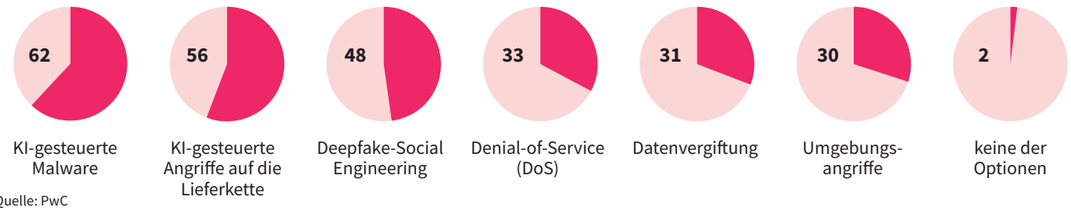
12 weiß nicht

Quelle: ISACA

Konkrete Sorgen

Größte Sorgen bei KI-Angriffsszenarien; Sicherheitsverantwortliche (n=1.740); weltweit; 2025; in Prozent

Welches der folgenden KI-Angriffsszenarien bereitet Ihrer Organisation die größten Sorgen?



62 KI-gesteuerte Malware

56 KI-gesteuerte Angriffe auf die Lieferkette

48 Deepfake-Social Engineering

33 Denial-of-Service (DoS)

31 Datenvergiftung

30 Umgebungsangriffe

2 keine der Optionen

Quelle: PwC

Größte Lücken

Größte Sorgen bei KI-Angriffsszenarien; Sicherheitsverantwortliche (n=1.740); weltweit; 2025; in Prozent

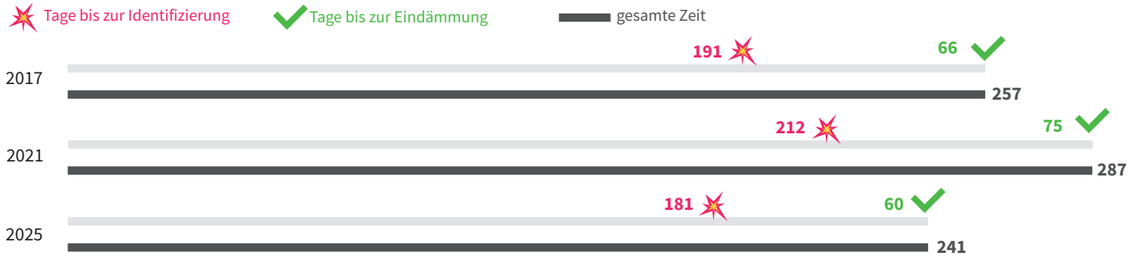
Auf welche dieser Cyberbedrohungen ist Ihre Organisation in den nächsten zwölf Monaten am wenigsten vorbereitet?

Cloud-bezogene Bedrohungen	33
Angriffe auf vernetzte Produkte	28
Bedrohungen durch Quantencomputer	26
Verstöße durch Dritte (Third Party Breaches)	27
Social Engineering	25
Hack-and-Leak-Operationen	21
Ransomware	20
Infiltration durch Mitarbeitende	20
Kompromittierung der Softwarelieferkette	20
Ausnutzung von Zero-Day-Schwachstellen	19
Kompromittierung von Geschäftsmails/Übernahme von Accounts	17
Distributed-Denial-of-Service-Attacken (DDoS)	15

Quelle: PwC

Spät entdeckt

Zeit bis zur Identifizierung und Behebung von Datenlecks; Unternehmen unterschiedlicher Größe aus 16 Ländern und geografischen Regionen und 17 Branchen (n=604); weltweit; in Tagen



Quellen: IBM, Ponemon Institute

Heftig diskutiert

Gründe für und gegen eine Offenlegung von Lösegeldzahlungen bei Ransomware-Angriffen; Mitarbeitende, die für die Cybersicherheitsstrategie verantwortlich sind (n=5.750); Vereinigtes Königreich, USA, Frankreich, Deutschland, Spanien, Irland, Portugal; 2025; in Prozent

Gründe für eine Offenlegung von Lösegeldzahlungen bei Ransomware-Angriffen

54 Offenlegungen geben Kundinnen, Kunden und Stakeholdern ein klareres Bild der finanziellen Lage eines Unternehmens.

52 Mehr Transparenz könnte Behörden dabei helfen, auf weitere Ransomware-Vorfälle zu reagieren.

Gründe gegen eine Offenlegung von Lösegeldzahlungen bei Ransomware-Angriffen

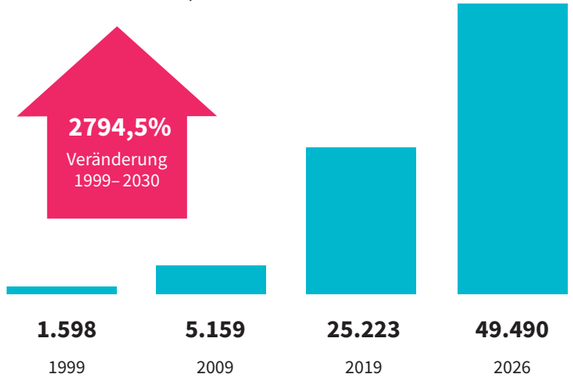
53 Private Unternehmen sollten nicht verpflichtet werden, finanzielle Details offenzulegen.

49 Offenlegungen könnten Anreize für kriminelle Akteure schaffen, sich an Ransomware-Angriffen zu beteiligen.

Quelle: Hiscox

Rasant gewachsen

Zahl der von CVE dokumentierten Schwachstellen in der IT-Sicherheit; weltweit*



*Stand 01.06.2026. Quelle: CVE

Zum Verständnis:
Aufgabe des CVE®-Programms ist es, öffentlich bekannt gemachte Sicherheitslücken in der Cybersicherheit zu identifizieren, zu definieren und zu katalogisieren. Für jede Schwachstelle im Katalog gibt es einen CVE-Eintrag. Die Schwachstellen werden von Organisationen aus der ganzen Welt, die eine Partnerschaft mit dem CVE-Programm eingegangen sind, entdeckt, zugewiesen und veröffentlicht. Die Partner veröffentlichen CVE-Datensätze, um konsistente Beschreibungen von Sicherheitslücken zu kommunizieren.

Hart bestraft

Top-10-Bußgelder für Datenschutzverstöße 2019 – 2026*; weltweit; in Euro

1 **4.536.999.350**
USA
Facebook Inc.
24.7.2019
*Verstoß gegen frühere FTC**-Datenschutzanordnungen und das Gesetz der Federal Trade Commission*

2 **1.200.000.000**
Irland
Meta Platforms Ireland Ltd.
22.5.2023
rechtswidrige Übermittlung personenbezogener Facebook-Daten an die USA

3 **1.165.011.903**
China
DiDi
21.7.2022
Verstöße gegen Gesetze zur Netzwerksicherheit, Datensicherheit und zum Schutz persönlicher Informationen

4 **746.000.000**
Luxemburg
Amazon Europe Core S.à r.l
30.7.2021
Verstöße im Zusammenhang mit der Anzeige von Werbung und der Weitergabe von Daten an Dritte

5 **530.000.000**
Irland
TikTok Technology Limited
2.5.2025
Unzureichender Datenschutz bei Übermittlung nach China, mangelnde Transparenz während der Untersuchungen

6 **508.130.081**
USA
Equifax Inc.
22.7.2019
Unzureichende Schutzmaßnahmen ermöglichten Diebstahl von Bonitätsdaten von 147 Mio. Betroffenen.

7 **405.000.000**
Irland
Instagram
5.9.2022
Rekordbußgeld für Instagram nach Bruch von Datenschutzrechten Minderjähriger

8 **405.000.000**
Irland
Meta Platforms Ireland Ltd.
2.9.2022
unzureichender Schutz von personenbezogenen Daten von Minderjährigen-Accounts

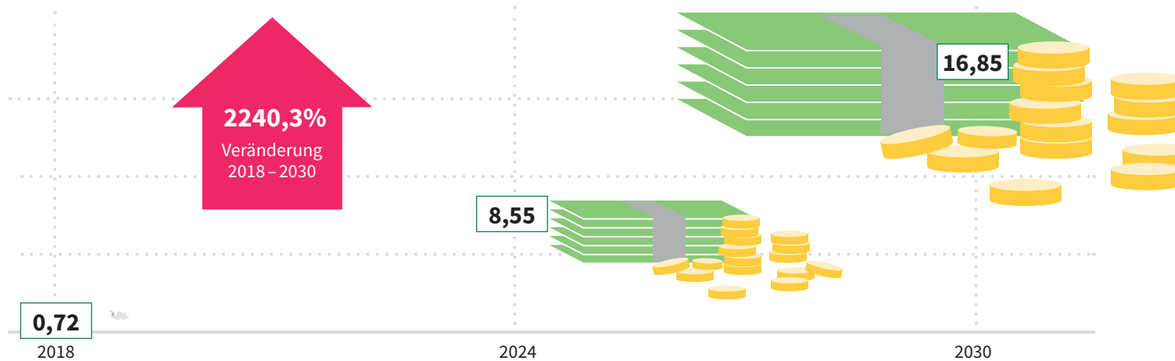
9 **390.000.000**
Irland
Meta Platforms Ireland Ltd.
4.1.2023
Vertragserfüllung, keine Rechtsgrundlage für personalisierte Werbung

10 **379.397.228**
USA
Google
15.11.2022
Rekordvergleich nach irreführenden Informationen zum Standort-Tracking

*Datenabruf am 23.2.2026. **FTC: Federal Trade Commission (Bundesbehörde der USA). Quelle: DSGVO-Portal

Teuer bezahlt

Zukünftige Entwicklung der Kosten durch Cyberkriminalität; weltweit; in Billionen Euro



Quellen: Statista Market Insights, National Cyber Security Organizations, FBI, IMF

Starke Netzwerke

Umgang mit Cyberrisiken in der Lieferkette; Führungskräfte auf C-Level, Wissenschaftlerinnen und Wissenschaftler, Vertreterinnen und Vertreter der Zivilgesellschaft sowie Verantwortliche für Cybersicherheit im öffentlichen Sektor (n=804); weltweit; 2026; in Prozent*

Wie geht Ihre Organisation mit Cyberrisiken in der Lieferkette um?

CEOs hoch resilienzfähiger Organisationen | CEOs unzureichend resilienzfähiger Organisationen

- 70 / 31 — Einbindung der Sicherheitsfunktion in den Beschaffungsprozess
- 59 / 31 — Bewertung des Sicherheitsreifegrads von Lieferanten
- 48 / 31 — Abstimmung der Cyber-Resilienzstrategie mit Partnern im Ökosystem
- 48 / 31 — Detaillierte Analyse des Ökosystems zur Identifikation von Cyberrisiken bei Partnern
- 44 / 6 — Simulation von Cybervorfällen und/oder Planung gemeinsamer Wiederherstellungsübungen mit Ökosystempartnern
- 30 / 38 — Austausch von Informationen über Bedrohungen mit Partnern im Ökosystem (Kunden, Lieferanten, Partner)

*Mehrfachnennung möglich. Quelle: World Economic Forum (WEF)

Die Resilienz wird im WEF-Report anhand eines Kriterienkatalogs gemessen, der Führungsengagement, Governance, Skills, Prozesse, Technik, Krisenmanagement und Ökosystemintegration umfasst. Die Messung erfolgt durch quantitative Kennzahlen und qualitative Bewertungen. Organisationen mit hoher Resilienz erfüllen in allen sieben Kategorien deutlich mehr Kriterien als weniger resiliente Unternehmen und sind dadurch besser auf Cyberbedrohungen vorbereitet.
Details: reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf

Deutliche Hürden

Größte Herausforderungen bei Cyberresilienz; Führungskräfte auf C-Level, Wissenschaftlerinnen und Wissenschaftler, Vertreterinnen und Vertreter der Zivilgesellschaft sowie Verantwortliche für Cybersicherheit im öffentlichen Sektor (n=804); weltweit; 2026; in Prozent*

Was ist die größte Herausforderung Ihrer Organisation auf dem Weg zu mehr Cyberresilienz?

CEOs hoch resilienzfähiger Organisationen | CEOs unzureichend resilienzfähiger Organisationen

- 78 / 31 — Schwachstellen bei Drittanbietern und in der Lieferkette
- 56 / 13 — sich schnell wandelnde Bedrohungslage und neue Technologien
- 41 / 25 — Komplexität regulatorischer Anforderungen und Governance
- 19 / 56 — fehlende Transparenz über IT-, OT- und IoT-Umgebungen
- 19 / 56 — Mangel an Cybersicherheitskompetenzen und Fachwissen
- 15 / 19 — unzureichende Planung für Reaktion und Wiederherstellung nach Vorfällen
- 15 / 25 — Altsysteme
- 15 / 63 — fehlende finanzielle Mittel

*Mehrfachnennung möglich. Quelle: World Economic Forum (WEF)

Hohe Resilienz

Bewertung der Cyberresilienz nach Organisationstyp; Führungskräfte auf C-Level, Wissenschaftlerinnen und Wissenschaftler, Vertreterinnen und Vertreter der Zivilgesellschaft sowie Verantwortliche für Cybersicherheit im öffentlichen Sektor (n=804); weltweit; 2026; in Prozent

Wie würden Sie die Cyberresilienz Ihrer Organisation einschätzen?

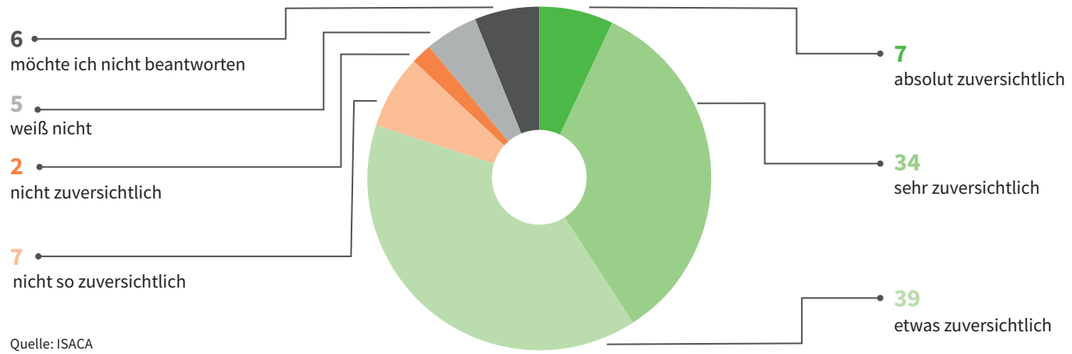
Unsere Cyberresilienz übertrifft die Anforderungen. | Unsere Cyberresilienz ist unzureichend. | Unsere Cyberresilienz erfüllt die Mindestanforderungen.

	übertrifft die Anforderungen	ist unzureichend	erfüllt die Mindestanforderungen
öffentlicher Sektor und internationale Organisationen	24	23	54
Privatwirtschaft	22	11	67
Nichtregierungsorganisationen (NGOs)	8	37	55

Quelle: World Economic Forum (WEF)

Großes Vertrauen

Vertrauen in Cybersicherheitsteams in Unternehmen; Cybersicherheits-Fachkräfte (n=3.812); weltweit; 2025; in Prozent



Quelle: ISACA

Zentrale Kompetenzen

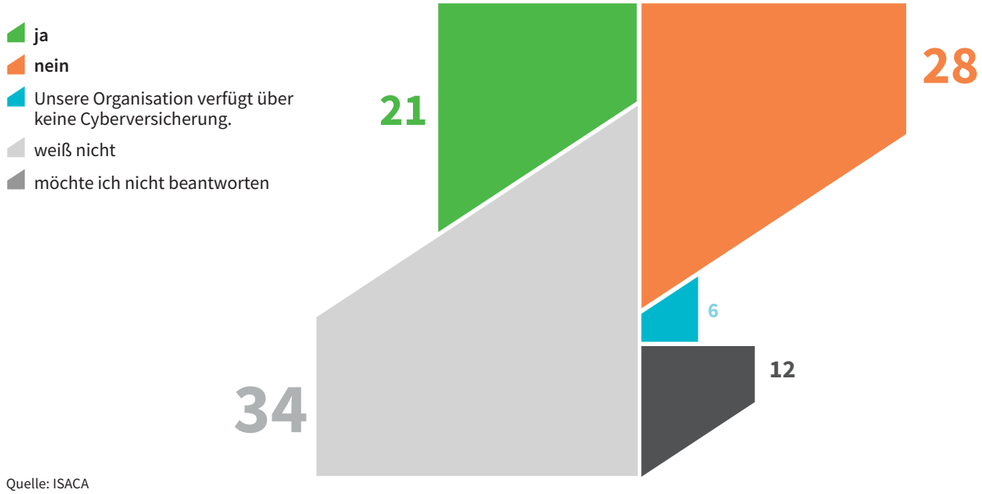
Die fünf wichtigsten Sicherheitskompetenzen, die in Unternehmen heute benötigt werden; Cybersicherheits-Fachkräfte (n=3.812); weltweit; 2025; in Prozent*

- 54 — Datenschutz
- 50 — Schwachstellenmanagement
- 49 — Technologien zur Bedrohungserkennung und -abwehr
- 47 — Cloud Computing
- 47 — Identity and Access Management (IAM)

*Mehrfachnennung möglich. Quelle: ISACA

Noch zögerlich

Inanspruchnahme einer Cyberversicherung; Cybersicherheits-Fachkräfte (n=3.812); weltweit; 2025; in Prozent



Quelle: ISACA

Drei Wege

Strategien zur Bewältigung von Cyberrisiko-Herausforderungen; Verantwortliche für Cyberrisiken (n= mehr als 2.200); weltweit; 2025; in Prozent

73

Aufbauen:
Einstellung und/oder Weiterbildung von Fachkräften zum Aufbau interner Cyberrisikoteams oder Kompetenzzentren – von technischen Expertinnen und Experten bis hin zu Führungskräften auf C-Level

66

Kaufen:
Erwerb von Fähigkeiten, Talenten oder Lösungen zur Bewältigung von Cyberrisiken (z. B. durch die Übernahme eines Unternehmens)

42

Ausleihen:
Zusammenarbeit mit Drittanbietern, um bestehende Cybersecurity-Fähigkeiten zu erweitern und/oder bei Bedarf zu skalieren

Quelle: Marsh

Technik reicht nicht

Top 5 technische und nicht-technische Fähigkeiten, die Fachkräfte als besonders gefragt ansehen; Cybersicherheitsexperten und -entscheidungsträger (n=16.029); weltweit; 2025; in Prozent

technische Fähigkeiten

künstliche Intelligenz/maschinelles Lernen	44
Cloud-Sicherheit	40
Governance Risk Compliance	30
Zero-Trust-Implementierung	27
Beurteilung, Analyse und Steuerung von Risiken	26

nicht-technische Fähigkeiten

starke Kommunikationsfähigkeiten	59
starke Problemlösefähigkeiten	55
Teamwork und Kooperationsfähigkeit	50
Neugierde/Lernbereitschaft	44
starkes strategisches Denken	39

Quelle: (ISC)²

Menschen zählen

Umgang mit Fachkräften und Personalbindung im SOC*-Umfeld; Arbeitnehmerinnen und Arbeitnehmer aus verschiedenen Branchen; weltweit; 2025; Zahl der Nennungen

Wie wird Humankapital in Ihrem Umfeld berücksichtigt?

120

Das Management hört auf die Anforderungen von SOC-Leitungen hinsichtlich der Einstellung qualifizierter und erfahrener Fachkräfte, erkennt jedoch nicht die Dringlichkeit, diese langfristig zu halten.

108

Das Management berücksichtigt die Bedürfnisse von SOC-Leitungen sowohl bei der Einstellung als auch bei der Bindung qualifizierter und erfahrener Fachkräfte.

59

Das Management berücksichtigt die besonderen Personalanforderungen eines SOCs nicht ausreichend und unternimmt wenig, um qualifizierte Fachkräfte zu gewinnen oder zu halten.

25

Das Management hält es für eine akzeptable Strategie, mehrere weniger qualifizierte Mitarbeitende einzustellen, um Cybersecurity-Warnmeldungen zu bearbeiten.

17

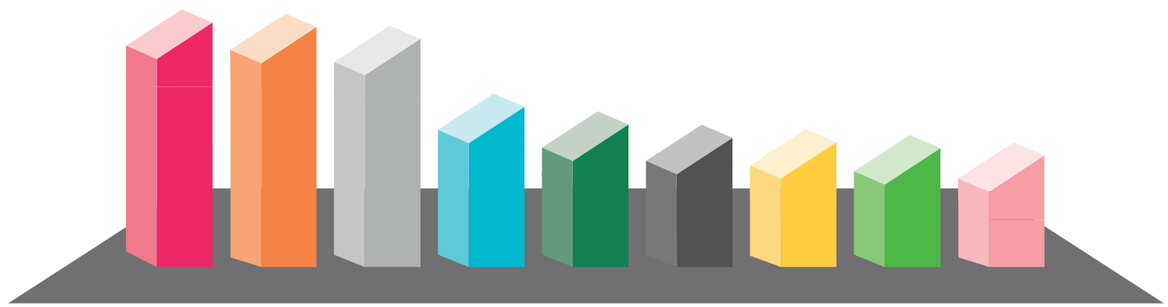
Sonstiges

*Security Operations Center. Quelle: SANS Institute

Haltung zählt

Wichtigste Qualifikationen von Cybersicherheitskandidaten; Fachleute für Cybersicherheit (n=3.812); weltweit; 2025; in Prozent

Wie wichtig sind die folgenden Faktoren bei der Beurteilung, ob ein Cybersicherheitskandidat qualifiziert ist?
Anteil der Befragten, die „sehr wichtig“ angaben:



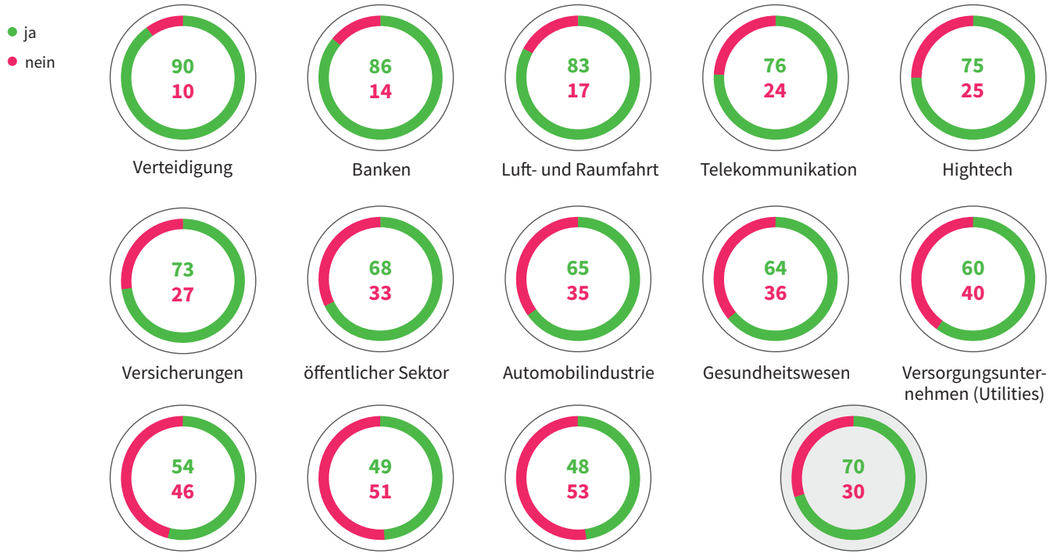
61	60	56	33	27	22	21	19	16
Anpassungsfähigkeit	vorherige Berufserfahrung im Bereich Cybersicherheit	Passung zur Organisation (z. B. Unternehmenskultur)	vorhandene Zertifikate/ Qualifikationsnachweise	praxisorientierte Trainingsprogramme	Cyber-Übungsumgebungen	Hochschulabschluss	berufliches Netzwerken	Empfehlung des vorherigen Arbeitgebers

Quelle: ISACA

Umsetzung im Gange

Status der Einführung quantensicherer Technologien nach Branchen; Unternehmen mit einem Jahresumsatz von mindestens 1 Milliarde US-Dollar (n=1.000); weltweit; 2025; in Prozent

Arbeiten Sie derzeit an der Einführung quantensicherer Lösungen oder planen Sie deren Einsatz innerhalb der nächsten fünf Jahre?



*Fast-Moving Consumer Goods. Quelle: Capgemini Research Institute

Quanten im Aufbau

Status der Einführung quantenresistenter Sicherheitsmaßnahmen; Geschäfts- und Technologieführungskräfte (n=3.887); weltweit; 2025; in Prozent

Wie weit ist Ihr Unternehmen bei der Umsetzung quantenresistenter Sicherheitsmaßnahmen?

Bereits gestartet: **51**
Wir setzen quantenresistente Sicherheitsmaßnahmen um. 22
Wir haben mit der Implementierung begonnen und befinden uns in der Pilot- und Testphase. 29

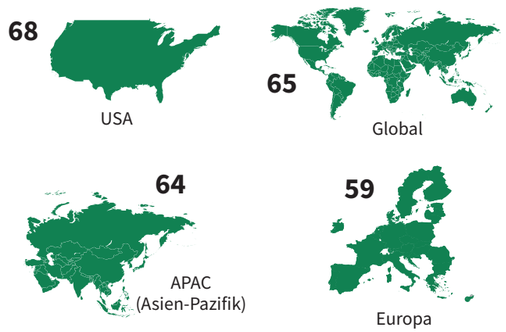
Noch nicht gestartet: **42**
Unsere Organisation hat begonnen, sich mit quantenresistentenSicherheitsmaßnahmen zu befassen, aber noch keine Schritte zur Umsetzung unternommen. 33
Unsere Organisation hat quantenresistente Sicherheitsmaßnahmen noch nicht in Betracht gezogen und hat keine Pläne, dies zu tun. 9

derzeit nicht zu bestätigen **7**

Quelle: PwC

Passkeys im Kommen

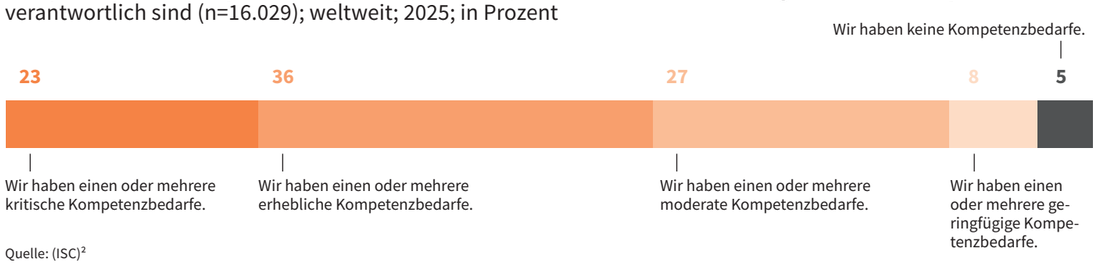
Anteil der Unternehmen, in denen Passkeys eingeführt wurden oder demnächst eingeführt werden oder deren Einsatz diskutiert wird; erwerbstätige Befragte, die sich regelmäßig bei Websites, Apps oder Onlinediensten anmelden (n=6.481); weltweit; 2026; in Prozent



Quelle: Fido Alliance

Kompetenzen gefragt

Kompetenzbedarfe in Cybersecurity-Teams; Personen, die in Unternehmen und Organisationen für Cybersicherheit verantwortlich sind (n=16.029); weltweit; 2025; in Prozent



Quelle: (ISC)²

Maßnahmen im Einsatz

Maßnahmen zur Deckung des Kompetenzbedarfs; Personen, die in Unternehmen und Organisationen für Cybersicherheit verantwortlich sind (n=16.029); weltweit; 2025; in Prozent

28 Zeit für berufliche Weiterbildung während der Arbeitszeit ermöglichen

25 kostenlose Trainings- und Bildungsinhalte von Security-Anbietern fördern

25 Investitionen in zusätzliche/neue Technologien

25 Integration von KI-Technologien zur Automatisierung von Aufgaben

24 Budget für interne Schulungen bereitstellen

22 Mitarbeitende außerhalb der Cybersecurity in Cybersecurity-Kompetenzen schulen

21 Mitarbeitende dazu ermutigen, interne Schulungen selbst durchzuführen

20 Outsourcing

20 Investitionen in die Teilnahme von Securityteams an Branchenkonferenzen

19 Online-Trainingsplattformen implementieren/verbessern

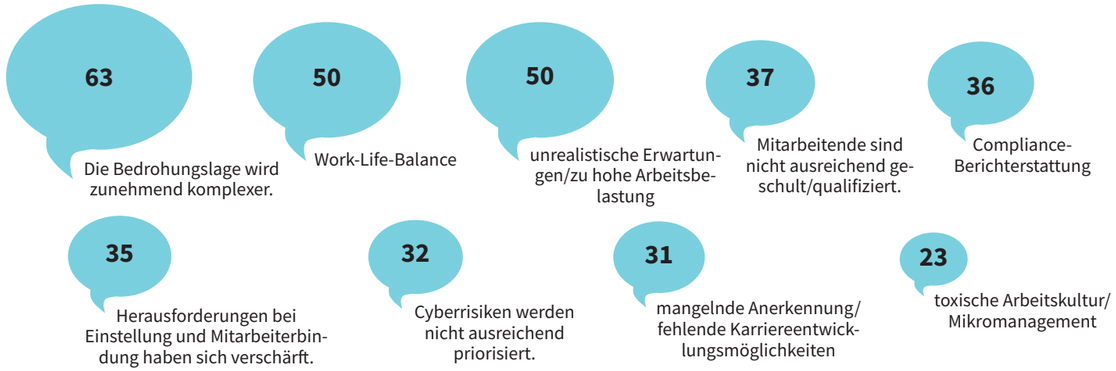
19 externe Dienstleister mit den benötigten Fähigkeiten beauftragen

19 Budget für externe Schulungen bereitstellen

Quelle: (ISC)²

Teams unter Druck

Stressquellen von Cybersecurity-Angestellten; Fachleute für Cybersicherheit (n=3.812); weltweit; 2025; in Prozent*

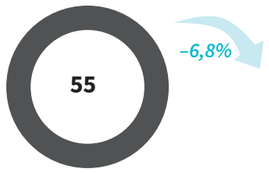


*Mehrfachnennung möglich. Quelle: ISACA

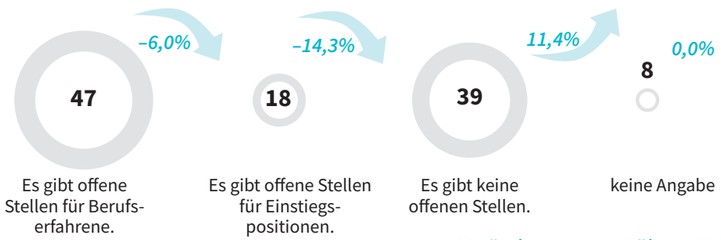
Personal gesucht

Fachkräftemangel und offene Stellen im Bereich Cybersicherheit (n=3.812); weltweit; 2025; in Prozent*

Das Cybersicherheitsteam ist unterbesetzt.



unbesetzte (offene) Stellen im Bereich Cybersicherheit:



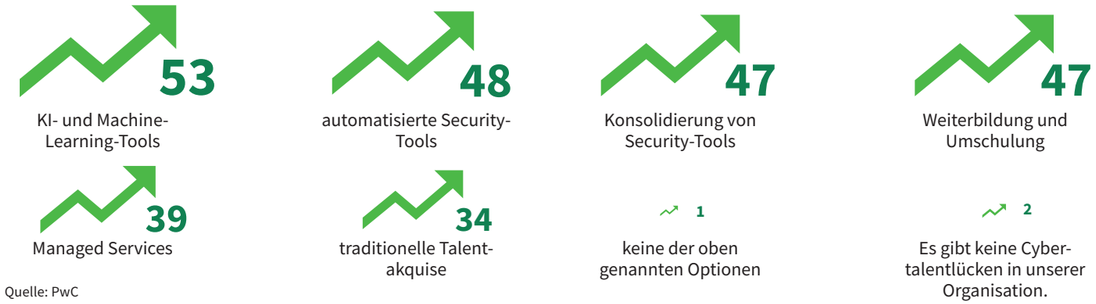
Veränderung gegenüber 2023

Quelle: ISACA

Weiterbildung priorisiert

Priorisierte Maßnahmen gegen Fachkräftemangel; Geschäfts- und Technologieführungskräfte (n=3.887); weltweit; 2025; in Prozent

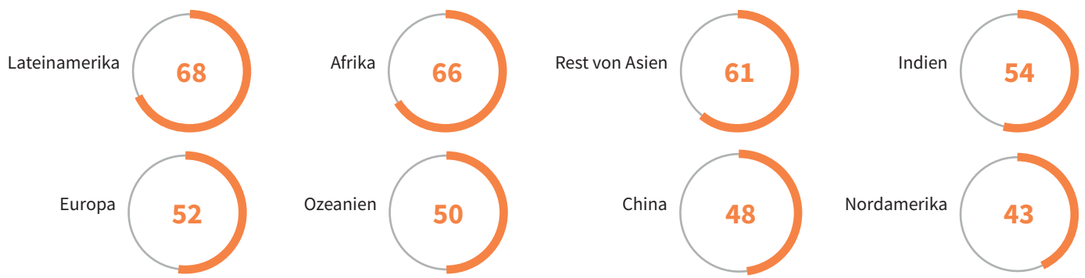
Welche Maßnahmen wird Ihr Unternehmen im nächsten Jahr priorisieren, um den Mangel an Cyberfachkräften zu beheben?



Quelle: PwC

Bindung erschwert

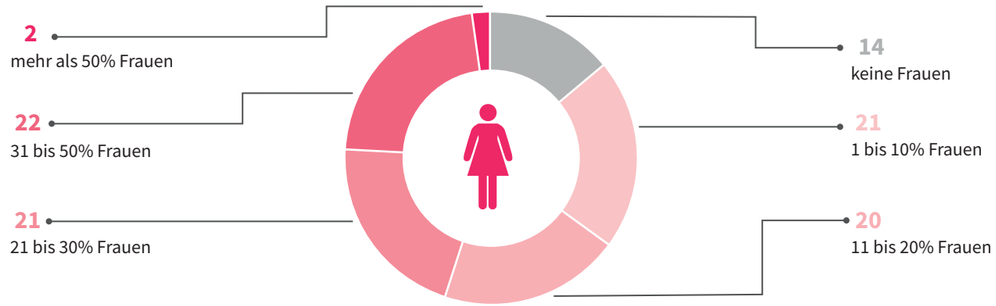
Anteil der Unternehmen, die im Bereich Cybersicherheit Schwierigkeiten hatten, Mitarbeitende zu halten; Fachleute für Cybersicherheit (n=3.812); weltweit; 2025; in Prozent*



Quelle: ISACA

Frauen unterrepräsentiert

Frauenanteil im Cybersecurity-Team; Personen, die in Unternehmen und Organisationen für Cybersicherheit verantwortlich sind (n=16.029, darunter Frauen: n=2.603); weltweit; 2025; in Prozent

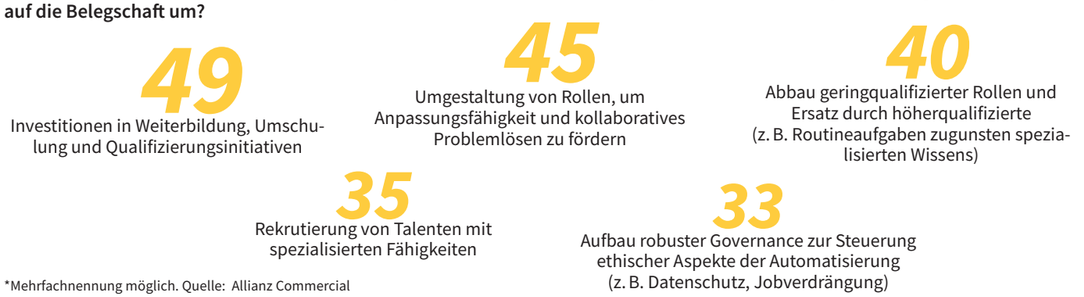


Quelle: (ISC)²

Arbeitswelt verändert

Umgang von Unternehmen mit den Auswirkungen zunehmender Automatisierung auf die Belegschaft; Allianz-Kunden (Unternehmen weltweit), Makler, Branchenverbände, Risikoberater, Underwriter, leitende Angestellte, Schadenexperten sowie weitere Fachkräfte aus dem Risikomanagement (n=1.084); weltweit; 2026; in Prozent*

Wie geht Ihr Unternehmen mit den Auswirkungen der zunehmenden Nutzung von Automatisierungstechnologien auf die Belegschaft um?



*Mehrfachnennung möglich. Quelle: Allianz Commercial

KI-Kompetenzen gefragt

KI-bezogene Fähigkeiten, die bei neuen IT-Sicherheits-Fachkräften besonders gefragt sind; IT-Sicherheits-Fachkräfte in einer privatwirtschaftlichen oder staatlichen Organisation, die mindestens 500 Mitarbeitende beschäftigt (n=1.200); weltweit; 2026; in Prozent*

Erfahrung im Einsatz von KI zur Verbesserung und Automatisierung von Incident Response und Behebungsmaßnahmen	43,8
Fähigkeit, Sicherheitsrisiken in KI-Modellen und -Tools zu bewerten	42,5
Erfahrung im Einsatz von KI zur Verbesserung von Überwachung und Angriffserkennung	39,9
Fähigkeit, Halluzinationen und Fehlinformationen in KI-Ausgaben zu erkennen und zu vermeiden	38,7
Erfahrung im Einsatz von KI für fortgeschrittene Analysen und Forensik	38,6
Fähigkeit, mithilfe von KI präzise Zusammenfassungen und Berichte zu erstellen	34,8
Erfahrung bei der Implementierung von agentischer KI	33,7
Fähigkeit zur Erstellung von KI-Prompts	30,2

*Mehrfachnennung möglich. Quelle: CyberEdge

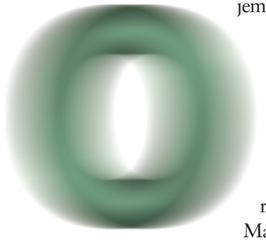
SOUVERÄNITÄT

Alles unklar

„Digitale Souveränität“ ist der meistgebrauchte Begriff der europäischen Technologiepolitik. Und der unschärfste. Ein Versuch zu erklären, warum das so ist – und wie jeder dennoch ins Handeln kommen kann.

Text: Meike Kirsch

Ich weiß schon: Nach diesem Text werden sowieso alle nicken. Ist doch heute so, dass man sofort zustimmt, wenn es um digitale Souveränität geht. Dass man reflexhaft an amerikanische Konzerne denkt, an Abhängigkeit, an geopolitische Risiken – kurz besorgt schaut, um danach weiterzumachen wie bisher. Dass man sich auf das Wort geeinigt hat, ohne sich je auf eine Bedeutung geeinigt zu haben. Dass „digitale Souveränität“ inzwischen das ist, was „Nachhaltigkeit“ vor ein paar Jahren war: ein Begriff, den alle gut finden und kaum jemand einlöst.



„Digitale Souveränität“ ist das Schweizer Taschenmesser der vernetzten Welt. Der Begriff lässt sich in alle Richtungen aufklappen. Er gefällt dem Sicherheitsexperten, der kritische Infrastrukturen schützen will. Dem Trump-Hasser, der generell für weniger Amerika ist. Dem Manager von Amazon Web Services, der seinen Kunden versichert, dass seine European Sovereign Cloud selbstverständlich souverän ist, auch wenn sie dem CLOUD Act der USA unterliegt.

Braucht man ein Argument gegen die Plattform-Riesen? Digitale Souveränität. Braucht man ein Argument für europäische KI-Förderung? Digitale Souveränität. Braucht man ein Argument gegen chinesische Hardware-Lieferanten? Auch das: digitale Souveränität.

Digitale Souveränität spaltet nicht

Alle verstehen etwas anderes. Das ist die eigentliche Stärke des Begriffs. Ein Wort, das so unscharf ist, ist unbezahlbar.

Politikern erlaubt es, zu handeln, ohne entscheiden zu müssen. Man kann Milliarden ankündigen, Gipfel einberufen, Strategiepapiere veröffentlichen – und trotzdem nie die eigentliche Frage beantworten: Sind wir bereit, dafür ungewohnte Produkte zu akzeptieren? Hohe Umstiegsinvestitionen? Konflikte mit den USA? Diese Fragen sind politisch toxisch. Der unscharfe Begriff schützt davor, sie stellen zu müssen.

Unternehmen nutzen ihn als Marketingargument ohne Verfallsdatum. Wer „digitale Souveränität“ ins Produktversprechen schreibt, signalisiert Europatauglichkeit – ohne irgendetwas Konkretes zu versprechen. Auf diese Weise wirken selbst die europäischen Dienste von amerikanischen Hyperscalern digital souverän. Ob das stimmt, hängt davon ab, welche Definition man anlegt – aber genau das bleibt eben offen. Die Unschärfe ist ein Freifahrtschein.

Lobbyisten kämpfen um die Deutungshoheit. Denn: Wer definiert, was Souveränität bedeutet, definiert auch, wer die Lösungen verkauft. Heißt Souveränität: Open Source? Dann gewinnen die Open-Source-Anbieter die Ausschreibungen. Heißt sie: Daten in Europa? Dann gewinnen die Rechenzentrumsanbieter. Heißt sie: europäische KI? Dann fließen die Fördergelder in eine ganz andere Richtung. Der Begriff umspannt einen Milliardenmarkt.

Ein Begriff, der alles bedeuten kann

An diesem Punkt meiner Recherche habe ich noch auf jemanden gehofft, der ihn sortieren kann. Dann telefonierte ich mit Julia Pohle. Sie ist die wohl profundeste Erforscherin des Begriffs in Deutschland, leitet die wissenschaftliche Expertengruppe für die Europäische Kommission zu diesem Thema und hat mehr als eineinhalb Jahrzehnte lang analysiert, wie „digitale Souveränität“ im Diskurs funktioniert. Ihr Urteil: Eine Definition ist schlicht unmöglich. Digitale Souveränität ist das, was Politikwissenschaftler ein „politisches Hochwertwort“ nennen: eine Vokabel, die so positiv besetzt ist, dass niemand dagegen sein kann, und so vage, dass jeder etwas anderes darunter versteht.

Deshalb würde Pohle den Begriff am liebsten gar nicht nutzen. Einen kleinsten gemeinsamen Nenner lässt sie sich abringen: „Digitale Souveränität ist die kollektive und individuelle Fähigkeit zur Selbstbestimmung darüber, wie digitale Technologien entwickelt, gesteuert und genutzt werden.“ Das klingt vernünftig. Aber sobald man genauer nachfragt, fächert sie Souveränität wieder in so viele Dimensionen auf, dass einem schwindlig wird.

Sehr vereinfacht kommt sie auf drei abgeleitete Konzepte, die unterschiedlicher kaum sein könnten.

Das erste und radikalste heißt Autarkie. Eigene Chips, eigene Software, eigene Cloud, eigene KI. Kein amerikanischer Code auf europäischen Rechnern. Die Vertreter dieser Maximalposition meinen es ernst. Sie kostet nach konservativen Schätzungen mehrere hundert Milliarden Euro, dauert Jahrzehnte und führt wahrscheinlich zu einer digitalen Infrastruktur, die hinter dem globalen Standard zurückbleibt. Hinzu kommt: Die Rohstoffe, die moderne Chips und Batterien brauchen – Lithium, Kobalt, seltene Erden – sind in Europa oft eher wenig vorrätig. Vollständige Autarkie ist also unmöglich. Das sagt jedoch kaum jemand.

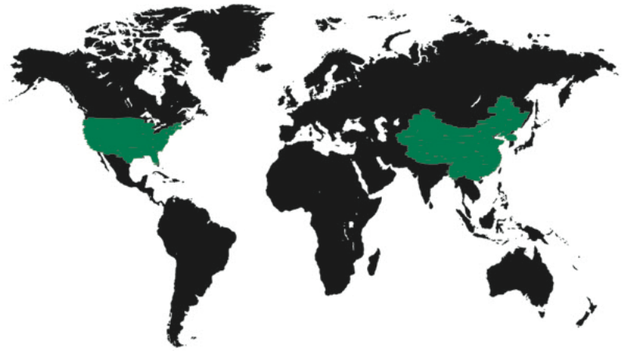
Das zweite heißt Resilienz. Man akzeptiert, dass Microsoft und Co. nicht morgen von allen Computern verschwinden können, dass OpenAI, Google und Anthropic in Sachen KI führend sind und es vorerst bleiben werden. Aber man baut Exitstrategien, diversifiziert Anbieter, setzt dort, wo möglich, auf Open-Source-Lösungen und schreibt Ausstiegsklauseln in Verträge. Das ist pragmatisch, aber nicht heroisch. Kaum ein Politiker gewinnt eine Wahl mit dem Versprechen von mehr LibreOffice.

Das dritte Konzept heißt Gestaltungsmacht: Europa soll nicht die Technologien der anderen nachbauen. Europa soll die Regeln schreiben, nach denen alle anderen ihre Technologien betreiben müssen. Die DSGVO war so ein Versuch und ist durchaus wirksam: Kein amerikanisches Unternehmen, das in Europa Geschäfte machen will, kommt an ihr vorbei. Der Haken: Gestaltungsmacht ist etwas völlig anderes als Unabhängigkeit.

Als Julia Pohle vor Jahren ihren ersten Artikel über digitale Souveränität schrieb, riet ihr eine Kollegin ab. Ernsthaft? Mit digitaler Souveränität beschäftigen? Ein absolutes Nischenthema sei das, musste Pohle sich anhören.

Heute ist das einstige Nischenthema zu einem Top-Topic avanciert. Auch jüngst auf der re:publica in Berlin, Europas größter Digitalkonferenz. Ständig fiel der Begriff. Alle wollten digitale Souveränität. Niemand meinte dasselbe. Babylon in Berlin. Pohle hat daraus die einzig logische Konsequenz gezogen: Ihren eigenen Talk auf der Konferenz nannte sie „Digitale Souveränität: Das Bullshit-Bingo“. Der Saal war voll. Und wahrscheinlich gingen danach nicht wenige mit Google Maps ins Hotel. Irgendwie scheint „digitale Souveränität“ ein Begriff zu sein wie „Biodiversität“ oder „Lieferkettensorgfaltspflichtengesetz“. Wichtig, aber nicht zwingend etwas, das das eigene Verhalten berühren muss.

Es ist bequem. Es funktioniert. Bis die Abhängigkeit plötzlich kein abstraktes Risiko mehr ist.



Die drei Souveränen

Aktuell können nur drei Länder umfassende digitale Souveränität über Infrastruktur, Dienste und Daten beanspruchen.

Die **USA** haben Souveränität durch Geschichte und Marktmacht. Das Internet wurde dort erfunden, die dominanten Plattformen sind dort beheimatet. Die USA müssen den digitalen Raum nicht zurückerobern. Sie befinden sich in seinem Zentrum. Jedenfalls noch.

China hat Souveränität durch Jahrzehnte der Planung. Ausländische Technologien wurden genutzt, beherrschbar gemacht, dann durch eigene Alternativen ersetzt. Das Ergebnis: ein vollständiges digitales Ökosystem, das vom Rest der Welt abgeschnitten werden kann, ohne zu kollabieren.

Und dann ist da **Nordkorea**. Das ungewöhnlichste Mitglied dieses Trios. Minimale Wirtschaft, minimale Vernetzung, maximale Kontrolle. Nordkorea verdeutlicht, was die Maximaldefinition von digitaler Souveränität bedeutet: auch nichts Gutes.
Für die verbleibenden 190 UN-Mitgliedsstaaten – darunter alle EU-Staaten – gilt: Vollständige digitale Souveränität ist realistisch wohl nie erreichbar.

Zwei Männer, aus dem digitalen Leben ausgesperrt

So wie bei Karim Khan. Der mittlerweile aufgrund des Verdachts auf sexuelle Übergriffe von seinem Dienst suspendierte Chefankläger des Internationalen Strafgerichtshofs in Den Haag wollte in seinem Büro Mails abrufen. Aber da waren keine mehr. Der Grund war kein Hackerangriff und auch kein technisches Problem, sondern eine Anweisung aus Washington. US-Präsident Donald Trump hatte Sanktionen gegen Khan verhängt. Und Microsoft, ein amerikanisches Unternehmen, das amerikanischem Recht unterliegt, stellte daraufhin die Dienste ein.

Der Richter Nicolas Guillou, ebenfalls vom IStGH, ebenfalls auf der Sanktionsliste wie sein Kollege, beschrieb in einem Interview, was das konkret bedeutet: kein Microsoft, kein Amazon, kein PayPal. Vom Bankgeschäft auf einem guten Teil des Planeten ausgeschlossen. Keine Kreditkarte, weil auch Visa, Mastercard und American Express US-Unternehmen sind.

Zwei Männer, mitten in Europa, aus dem digitalen Leben ausgesperrt – weil Washington das so wollte. Das war das erste Mal, dass ich wirklich verstanden habe, um was es geht.

Dennis-Kenji Kipker, Professor für IT-Sicherheitsrecht und Forschungsdirektor am Cyberintelligence Institute in Frankfurt und eine der profiliertesten Stimmen in der Debatte um digitale Souveränität, hat dafür einen drastischen Begriff parat: „Das ist der Kill Switch.“ Der Knopf, der aus abstrakter Abhängigkeit plötzlich ganz reale Ohnmacht macht. Kipker sagt, wenn dieser Knopf gedrückt wird, „dann sind wir in der Europäischen Union sehr schnell in der digitalen Steinzeit“.

Er weiß, wovon er spricht. Wer sich in eine Videokonferenz mit ihm einwählt, landet bei BigBlueButton, einem Open-Source-System. Kipker nutzt OpenOffice, Signal, Threema, privat kein Facebook, kein WhatsApp. Server hostet sein Institut selbst. Aber beispielsweise an Instagram und Linkedin kommt auch Kipker nicht vorbei.

Die Abhängigkeiten, sagt Kipker, ziehen sich durch alle drei Ebenen. Wirtschaft: Die meisten deutschen Unternehmen importieren ihre digitale Infrastruktur aus den USA oder China – und wären nur kurzzeitig überlebensfähig, sollten diese Importe ausbleiben. Staat: Hier sieht es nicht grundsätzlich anders aus. Individuum: Ich schreibe diesen Text auf einem amerikanischen Laptop, in Word. Die Redaktion arbeitet mit Google Drive. Drei amerikanische Dienste. Ein Text über Unabhängigkeit.

Hier liegt wahrscheinlich eines der Probleme: Wir haben uns daran gewöhnt, digitale Entscheidungen nicht als ›

Entscheidungen zu verstehen. Wir sind in Systeme eingebettet, die wir als so selbstverständlich ansehen wie Straßen und Leitungswasser – nur dass Straßen und Leitungswasser tatsächlich uns gehören, während die digitale Infrastruktur, auf der wir unser Leben aufgebaut haben, Unternehmen gehört, die anderen Gesetzen folgen als wir.

Kipker formuliert das so: „Jede Beschaffungsentscheidung, also jeder IT-Einkauf, egal ob Software oder Hardware, ist eine Entscheidung für oder gegen digitale Souveränität." Das klingt einleuchtend. Es klingt so, als wäre das Problem durchaus zu lösen. Aber dann folgt die eigentliche Aussage, mit der Kipker seltener zitiert wird: „Seit 20 Jahren verschlafen wir es, endlich zu handeln. Jetzt sind wir gezwungen, innerhalb kürzester Zeit digitale Souveränität herzustellen. Das ist natürlich unmöglich."

Die Lähmung, die sich als Aktivismus tarnt

Irgendwann während dieser Recherche wurde mir klar: Die Schwierigkeit ist längst nicht nur, dass uns Definitionen fehlen. Deshalb bat ich Petra Bock um ein Gespräch. Die Transformationsforscherin und Gründerin des Dr. Bock Institute wird seit 25 Jahren gerufen, wenn Führungspersönlichkeiten aus Wirtschaft und Politik unter Druck sind. Was Bock dabei immer wieder beobachtet, nennt sie den Knowledge-Action-Gap: Das Wissen ist da. Die Handlung bleibt aus.

Bei digitaler Souveränität, sagt Bock, sei dieser Gap besonders groß. Und besonders gefährlich. „Es kann das Aus bedeuten, wenn man hier nicht die richtigen Entscheidungen trifft." Eine Elite, die über Jahrzehnte auf Effizienz, Skalierung und globale Vernetzung optimiert wurde, soll nun kontraintuitiv handeln: unbequemere Lösungen wählen, Redundanzen aufbauen, erst mal weniger Produktivität in Kauf nehmen. „Das ist eine verdammt große Zumutung", sagt Bock.

Das Ergebnis ist eine kollektive Lähmung, die sich als Aktivität tarnt. Konferenzen, Strategiepapiere, Gipfel – das erzeugt das Gefühl, dass etwas passiert. Ein gefährlicher Eindruck, weil er den Druck nimmt – den Druck, den es bräuchte, um wirklich zu handeln. Das zeigt sich nirgendwo deutlicher als in der Politik, die weiterhin Hunderte Millionen für Microsoft-Lizenzen ausgibt und das gelegentlich mit dem Wort „Souveränität" garniert, ohne auch nur kurz innezuhalten bei der Frage, ob das nicht ein Widerspruch ist. Allein der Bund zahlte im vergangenen Jahr 481,4 Millionen Euro für Microsoft-Lizenzen. Nach 347,7 Millionen und 274,1 Millionen in 2024 und 2023.

Und doch: „Etwas hat sich verändert. Donald Trump und die Unsicherheiten unserer Zeit haben mehr für digitale Souveränität getan als zwanzig Jahre Strategiepapiere", sagt Bock. Seit seiner zweiten Amtszeit, seit den Sanktionsdrohungen, seit dem ersten Kill-Switch-Moment, wächst die Zahl derer, die wirklich handeln wollen. Unternehmen, die jahrelang zögerten, fragen plötzlich nach Alternativen. Verwaltungen, die Microsoft nie in Frage stellten, beginnen Gespräche über Open Source. Endlich, so der Eindruck, meinen es mehr und mehr wirklich ernst.

Dieses Opportunitätsfenster hat die Wirtschaft längst entdeckt. Kaum ein Technologieanbieter, der seinen Dienst nicht

inzwischen als „souverän" bewirbt. Souveräne Cloud. Souveräne KI. Souveräne Plattform. ZenDiS, das vom Bund eingerichtete Zentrum Digitale Souveränität, hat dafür einen Begriff geprägt: „Souveränitäts-Washing" – in Anlehnung an Greenwashing. Produkte, die Unabhängigkeit versprechen, aber gar nicht unabhängig sind. Kipker bringt es auf den Punkt: „Jeder kann zurzeit auf sein Angebot digitale Souveränität draufdrucken. Es ist nicht geschützt." Und dann fügt er hinzu, was selten so offen gesagt wird: „Es gibt genügend Akteure, die unter dem Deckmantel der digitalen Souveränität handeln, die aber gar keine wollen."

Das Paradebeispiel ist Amazon Web Services. Amazon hat Rechenzentren in Frankfurt eröffnet, europäische Ingenieure eingestellt, europäische Steuern gezahlt – und das Ganze als „European Sovereign Cloud" vermarktet. Technisch liegen die Daten in Europa. Juristisch aber ist AWS ein amerikanisches Unternehmen, das weiterhin amerikanischem Recht unterliegt.

Der Norden geht voran

Dirk Schrödter, Digitalisierungsminister von Schleswig-Holstein, betrachtet Souveränitäts-Washing ebenfalls mit Sorge. „Es nützt nichts, amerikanische proprietäre Lösungen mit so etwas zu ersetzen", sagt er. Gemeint sind Angebote, die europäisch klingen, aber im Kern dieselben Abhängigkeiten fortschreiben. Auch das Buy-European-Prinzip, das manche unter digitale Souveränität einsortieren, reiche nicht aus. Nur weil eine Lösung aus Europa kommt, muss sie noch lange nicht souverän sein. Entscheidend ist, bei wem die Gestaltungsmacht liegt. Bei proprietären Lösungen liegt sie beim Hersteller. Das ist das Problem. Auch ein europäisches Unternehmen kann ein Monopolist sein und so handeln, dass es von seinen proprietären Lösungen einseitig profitiert und Abhängigkeiten schafft. Entscheidend ist, wer den Code kontrolliert, den Durchgriff hat.

Schrödter ist ein konsequenter Open-Source-Verfechter. Für eine Videokonferenz lädt er zu OpenTalk ein, einer quelloffenen Alternative aus Deutschland. Und er spricht das Kürzel „IT" deutsch aus: „Itee". Nicht englisch: „Eiti". Aus Prinzip.

Schleswig-Holstein ist bisher das einzige deutsche Bundesland, das aus digitaler Souveränität wesentlich mehr als ein Leitbild gemacht hat. Dort gilt verpflichtend: LibreOffice statt Microsoft Office. Nextcloud statt SharePoint. OpenTalk statt Teams. Die Zahlen sind beeindruckend: Über 40.000 Mailpostfächer mit mehr als 110 Millionen Mails und Kalendereinträgen wurden erfolgreich migriert. Auf 100 Prozent der Arbeitsplätze ist LibreOffice die Standard-Office-Lösung, nur auf lediglich circa 20 Prozent sind noch einzelne andere Lizenzen verblieben, etwa für Excel oder Word. Das Land sparte zuletzt mehr als 15 Millionen Euro an Microsoft-Lizenzgebühren. Schrödters Kernlogik: „Es macht keinen Sinn, mit unseren Lizenzgebühren länger den technologischen Fortschritt anderswo in der Welt zu finanzieren, wenn wir gleichzeitig mit unseren öffentlichen Budgets unseren Digitalstandort stärken können."

Es muss gesagt werden: Schleswig-Holstein ist nicht erst seit Trumps jüngsten Eskapaden unterwegs. Die Entscheidung fiel viel früher, die Umsetzung läuft länger. Aber die aktuell gefühlt höhere Dringlichkeit hat etwas verändert. Plötzlich schaut man auf den Norden Deutschlands. Delegationen aus dem In- und Ausland melden sich an. Sie wollen von denen in Kiel wissen, wie man das macht: souveräner werden.

Alexander Rosenthal leitet den DigitalHub.SH, den zentralen Knotenpunkt, der alle bei der Transformation vernetzt. Er ist auch derjenige, der oft die Delegationen empfängt. „Wenn wir ein paar der Schmerzen nehmen können, die andere noch vor sich haben – dann geben wir das gerne weiter", sagt er. Nächste Woche kommen Kollegen aus Lettland. Die Niederländer haben sich angekündigt. Die Dänen stehen vor der Tür. „Man kann schon fast sagen, wir werden überrannt."

Rosenthal sagt das ohne Größenpathos. Natürlich wolle man, dass andere mit auf die Reise kommen. Natürlich sei Schleswig-Holstein selbstbewusst genug, voranzugehen. „Aber die Welt werden wir nicht allein retten", sagt er. „Dafür sind wir dann doch ein bisschen zu klein."

Digitales Souveränerwerden muss ganz offenbar nicht mit einer großen europäischen Erfolgsgeschichte beginnen, sondern zum Beispiel in einem überschaubaren Bundesland, das sich durch Migrationslisten arbeitet. In Verwaltungen, in denen Menschen plötzlich andere Menüleisten sehen und trotzdem weitermachen. Genau daran scheitern Transformationen ja oft: an nervigen Computerproblemchen am Montagmorgen.

„Durch die gröbsten Schmerzen sind wir durch", sagt Rosenthal. Aber es wäre falsch zu behaupten, jetzt sei alles nur noch „Juptidupti und Einhörner". Schleswig-Holstein verkauft den Umstieg nicht als Zaubertrick. Es tut nicht so, als sei digitale Souveränität eine App, die man einfach herunterlädt und fertig. Schrödter und Rosenthal machen deutlich, dass Unabhängigkeit Reibung erzeugt. Dass sie Geduld verlangt. Und dass sie trotzdem möglich ist.

Wie ernst sie es in Kiel meinen, zeigt sich auch im Kleinen. Auf einem Event verteilte Rosenthals Team gebrandete Socken an alle, die sich vor Ort die WhatsApp-Alternative Signal heruntergeladen hatten. „Auch das rettet nicht die Welt", sagt Rosenthal. Dann lächelt er. „Aber meine Mutter hat jetzt Signal."

Einfach tun. Das ist auch Schrödters Tipp an alle, die zögern. Der Minister hält wenig davon, noch jahrelang nach dem perfekten Migrationsplan zu suchen. Sein Rat in Großbuchstaben und mit drei Ausrufezeichen: ANFANGEN!!! Mit der nächsten Abhängigkeit, die sich verringern lässt.

Schrödter weiß, dass Umstellung ordentlich Ärger bringen kann. Wenn etwas nicht funktioniert, steht derjenige in der Kritik, der den Wechsel wollte. Die Herausforderungen kämen „wie das Amen in der Kirche", sagt er. Aber das dürfe kein Grund sein, nicht anzufangen. „Digitale Souveränität zu schaffen, ist so viel wichtiger als die ein oder andere schlaflose Nacht weniger."

Es gibt sie, die Alternativen

Und dann sind da noch Menschen wie Daniel Niesler, der die nerdige Softwareschmiede FTAPI mitgegründet und zu einem der ambitioniertesten Cybersecurity-Unternehmen Europas geformt hat. Schon seit 2010 baut er an Alternativen zu WeTransfer und SharePoint, bietet sichere Datenübertragung für Behörden, Versicherungen, Krankenhäuser – Ende-zu-Ende-verschlüsselt, konform mit Compliance-Vorgaben wie DSGVO, NIS-2 und TISAX. Inzwischen hat FTAPI mehr als 2.000 Kunden, nach eigenen Angaben 150 Mitarbeitende und ein Jahreswachstum von rund 50 Prozent. 2025 gelang eine Investmentrunde über 65 Millionen Euro, bewusst europäisch aufgestellt. „Lange haben wir gedacht: Was wir da machen, versteht ja keiner. Schön, dass sich das nun geändert hat."

Niesler ist der Praktiker in diesem Text – einer von vielen, die täglich daran arbeiten, digitale Souveränität Wirklichkeit werden zu lassen. Wie andere kleine und mittelgroße europäische Technologieunternehmen, die echte Alternativen zu den amerikanischen Platzhirschen bauen – für Kommunikation, Datenspeicherung, Verschlüsselung. Wie Softwareentwickler, die Open-Source-Projekte pflegen. Wie IT-Abteilungen in Behörden, die Migrationsprojekte durchfechten. Wie Aktivisten, die Wechselanleitungen schreiben. Wie Netzpolitiker, die für offene Standards kämpfen. Eine Community, die immer größer wird.

Und die trotzdem noch gegen Wände läuft. Niesler weiß das. Kürzlich hat er die Vorstände der größten deutschen Banken angeschrieben. Er macht sich Sorgen, dass besonders Bankensysteme in absehbarer Zeit angegriffen werden könnten, dass Abhängigkeiten hier besonders große Auswirkungen haben. Er lud zum Gespräch ein. Niemand antwortete.

„Es liegt vor uns, was passieren wird", sagt Niesler, „und die kommen nicht in Action." Er klingt ungläubig. Gleichzeitig warnt er vor der naheliegenden Überreaktion: raus aus Amerika, Grenzen dicht. „Auch wenn es politisch gerade schwierig ist mit den USA … Wir müssen es zusammen schaffen. Es ist eine Welt."

Doch bleibt die Frage, die über allem schwebt: Wird das alles gut ausgehen? Niesler atmet durch: „Ich habe aufgehört, so zu tun, als wüsste ich es." Dann, nach einer Pause: „Am Ende bleibt nur der Optimismus. Wir haben bisher immer einen Weg gefunden."

WIRTSCHAFT

Künstliche Intelligenz verändert die Wirtschaft – und die Cyberkriminalität. Angriffe werden raffinierter und professioneller, Unternehmen, Organisationen und öffentliche Verwaltung geraten zunehmend unter Druck. Doch vielerorts fehlen Fachkräfte, Ressourcen, Strategien – und ein ausreichendes Bewusstsein für die Risiken.

Digital bedroht

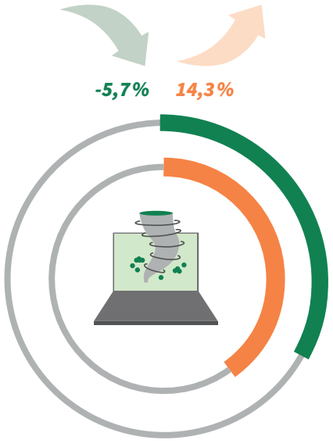
IT-Angriffe auf Unternehmen nach Art des Angriffs; Führungskräfte, die für das Thema Wirtschaftsschutz verantwortlich sind in Unternehmen mit mindestens zehn Beschäftigten und einem Jahresumsatz von 1 Mio. Euro oder mehr (n=1.002); Deutschland; 2025; in Prozent*

betroffen

Veränderung gegenüber 2024

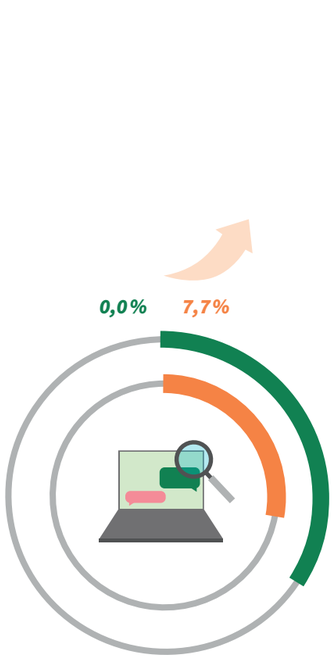
vermutlich betroffen

Veränderung gegenüber 2024



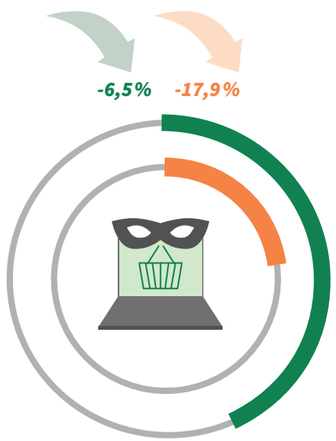
33 **40**

digitale Sabotage von Informations- und Produktionssystemen oder Betriebsabläufen



34 **28**

Ausspähen von Kommunikation via E-Mail, Messenger, Videocall oder ähnlichen digitalen Mitteln

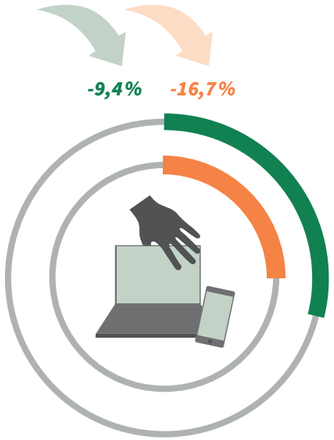


43 **23**

digitaler Diebstahl von Geschäftsdaten

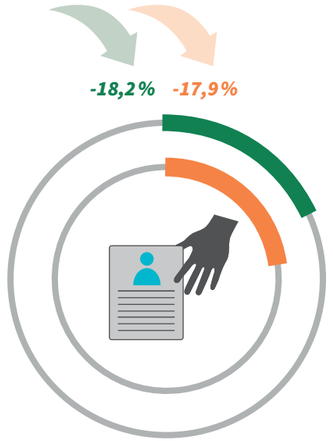
digital

*Mehrfachnennung möglich. Quelle: Bitkom



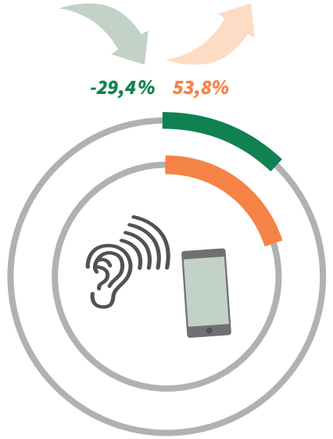
29 **25**

Diebstahl von IT- oder Telekommunikationsgeräten



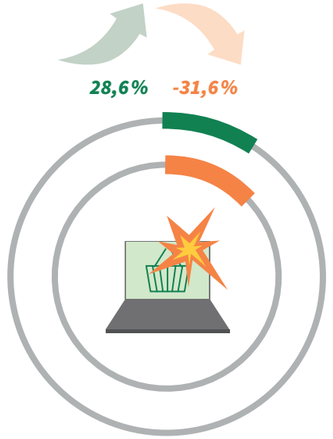
18 **23**

Diebstahl von physischen Dokumenten, Personalakten, Mustern, Maschinen, Bauteilen o. Ä.



12 **20**

Abhören von Besprechungen oder Telefonaten vor Ort



9 **13**

physische Sabotage von Informations- und Produktionssystemen oder Betriebsabläufen

analog

Das Glossar der Cyberbegriffe finden Sie auf den Seiten 100 – 103.

Risiko erkannt?

Relevanteste IT-Sicherheitsrisiken; Unternehmensentscheiderinnen und -entscheider (n=533); Deutschland; 2026; in Prozent*

Welche der folgenden IT-Sicherheitsrisiken halten Sie für Ihr Unternehmen für relevant?

47 gezielte Hacker-/Cyber-/DDoS-Angriffe

44 technische Ausfälle

35 menschliches/organisatorisches Versagen

34 Phishing

31 Downloads von Malware (z. B. Ransomware)

25 unzureichende Kenntnis technischer Entwicklungen

20 Social Engineering

20 Diebstahl

18 fehlende Redundanz/Back-up-Kapazität

17 höhere Gewalt (Naturkatastrophen, Brände)

16 Inside Jobs

10 Vandalismus

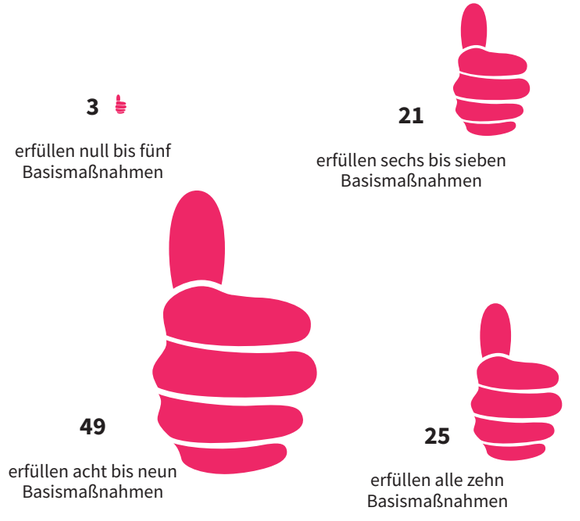
8 keines der genannten Risiken

3 weiß nicht/keine Angabe

*Mehrfachnennung möglich. Quelle: 1&1 Versatel

Pflicht erfüllt?

Erfüllung der Basisschutzmaßnahmen in mittelständischen Unternehmen; Entscheiderinnen und Entscheider sowie IT-Verantwortliche von kleinen und mittleren Unternehmen (n=300); Deutschland; 2025; in Prozent



Die **zehn Basisschutzmaßnahmen** entsprechen grundlegenden Obliegenheiten der GDV-Musterbedingungen für eine Cyberversicherung. Hier geht es unter anderem um Passwörter und Zugänge, Schutz vor Schadsoftware, Datensicherungen und Sicherheitsupdates.

Basisschutzmaßnahmen: www.gdv.de/cybercheck

Quelle: GdV

Richtig investiert?

Investitionsschwerpunkte von Anwenderunternehmen aus dem gehobenen Mittelstand und Konzernen (n=138-144); Deutschland; 2025; in Prozent (Skala von 1 =„gar nicht“ bis 4 = „sehr stark“; die dargestellten Antworten beziehen sich auf „stark“ und „sehr stark“)

In welche Themen investiert Ihr Unternehmen in den kommenden zwei Jahren?

91 Cybersecurity/Informationssicherheit

80 IT-Modernisierung

77 Prozessautomatisierung und Aufbau von End-to-End-Prozessketten

69 Data Analytics

69 Mitarbeiterweiterqualifikationen zu Digital- und Technologiethemen

64 ESG/Nachhaltigkeit

59 künstliche Intelligenz

57 Umsetzung von Regulatorik

55 Softwareentwicklung und -einführung

53 Digital Workplace

47 Cloud-Transformation

46 Digital Experience & Nutzerzentrierung

31 Digital Commerce

Quelle: Lünendonk

Klug verteilt?

Verteilung des IT-Budgets; Anwenderunternehmen aus dem gehobenen Mittelstand und Konzerne (n=131); Deutschland; 2025; in Prozent

Erhalt der Bestands-IT	37
Erneuerung der Bestands-IT	36
Innovation	28

Quelle: Lünendonk

Womit verdient?

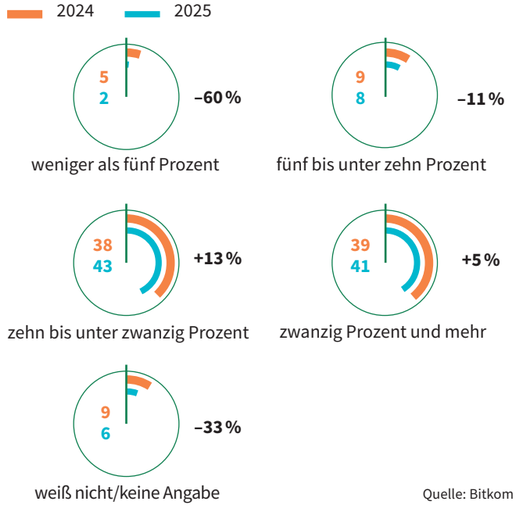
Umsatzanteile verschiedener Leistungsbereiche bei IT-Dienstleistern; IT-Dienstleister (n=41-64); Deutschland; 2025; in Prozent

Managed Services	20,8
Cloud-Transformation und -Migration	14,4
Data & AI	13,7
Digital Experience Services	9,6
Cybersecurity	5,7

Quelle: Lünendonk

Budget gesichert?

Geschätzter Anteil des Budgets für IT-Sicherheit am gesamten IT-Budget; Unternehmen mit mind. zehn Beschäftigten und einem Jahresumsatz von 1 Mio. Euro oder mehr (n=1.002); Deutschland; in Prozent



Quelle: Bitkom

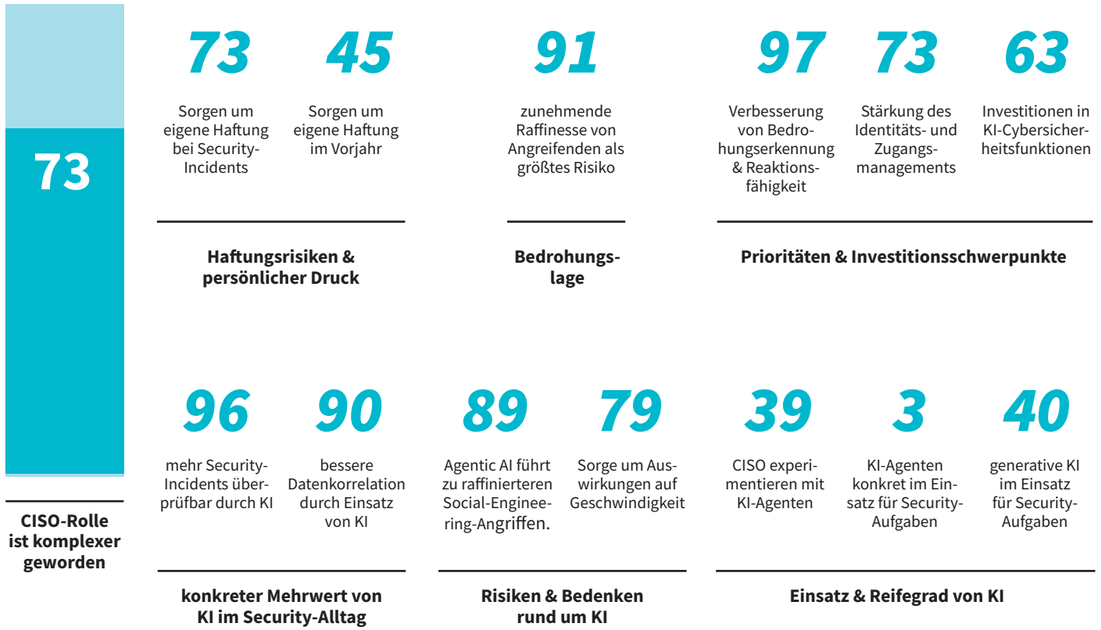
Teuer und komplex

Kosten und Komplexität von Cybersicherheitsstandards; IT-Leitung/CIO, Chief Information Security Officer (CISO), Verantwortliche/r für IT-Sicherheit, Geschäftsführung oder Vorstand in Unternehmen ab zehn Mitarbeiterinnen und Mitarbeitern (n=506); Deutschland; 2025; in Prozent

Quelle: TÜV-Verband

Raffiniert und gefährlich

CISOs in Deutschland (n=60): Rolle, Risiken und Einsatz von künstlicher Intelligenz; Deutschland; 2026; in Prozent

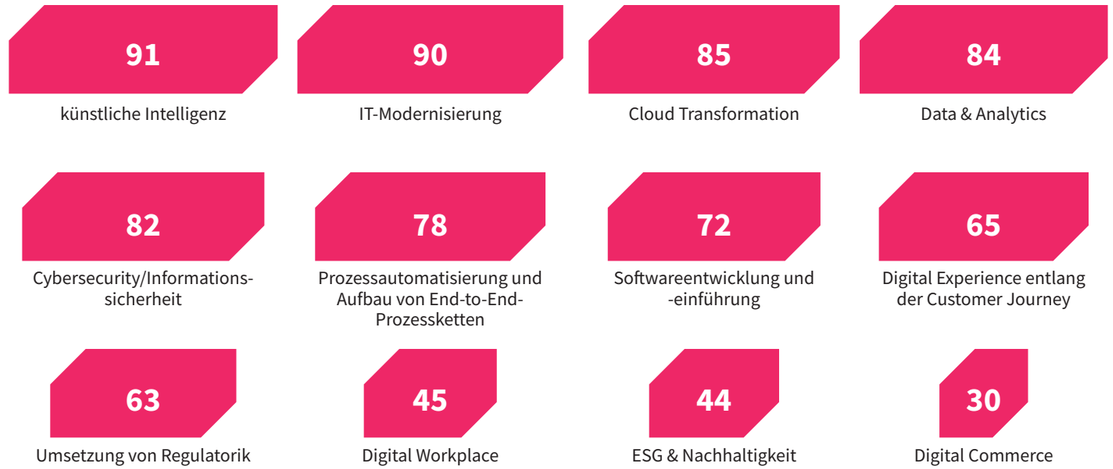


Quelle: Splunk

KI und Modernisierung

Die größten Trendthemen aus Sicht von IT-Dienstleistern (n=83); Deutschland; 2025; in Prozent (Skala von 1 =„gar nicht“ bis 4 = „sehr stark“; die dargestellten Antworten beziehen sich auf „stark“ und „sehr stark“)

Wonach richten Sie Ihr Portfolio 2025/2026 aus?



Quelle: Lünendonk

Anforderungen und Experten

Themen, die in Zukunft einen erhöhten Bedarf an Managed Services auslösen; Führungskräfte in Großunternehmen und Konzerne mit einem Umsatz von mindestens 500 Millionen (n=95); Deutschland; 2025; in Prozent (Skala von 1 =„gar nicht“ bis 4 = „sehr stark“; die dargestellten Antworten beziehen sich auf „eher stark“ und „sehr stark“)

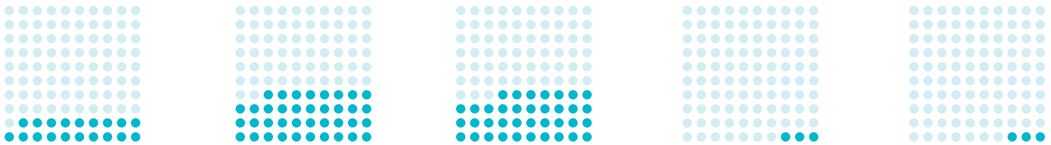
Welche Themen werden in Zukunft in Ihrem Unternehmen für einen erhöhten Bedarf an Managed Services sorgen?

Quelle: Lünendonk

Wolkig

Cloud-Strategien von Unternehmen; IT-Verantwortliche mit Fokus IT Operations, IT Service Management (ITSM), IT Sourcing und CIOs in mittelständischen und großen Anwenderunternehmen und Konzerne (n=121); Deutschland; 2025; in Prozent

Welche Cloud-Strategie verfolgt Ihr Unternehmen?



19 Wir verfolgen eine Cloud-only-Strategie, sodass on-premise für uns keine Rolle spielt.

38 Wir verfolgen eine Cloud-first-Strategie und setzen nur in Ausnahmen auf on-premise.

37 Wir verfolgen eine Cloud-too-Strategie und verlagern einzelne Anwendungen in die Cloud bzw. beziehen Cloud-Ressourcen, wägen es aber individuell mit On-premise-Lösungen ab.

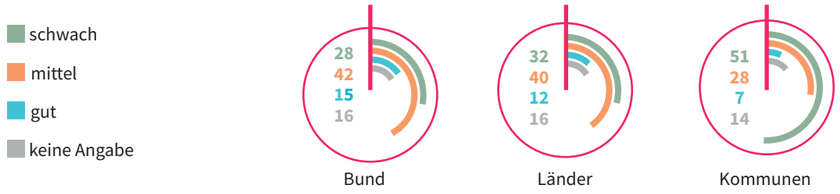
3 Wir haben noch keine Cloud-Strategie definiert, planen aber die Entwicklung und Operationalisierung innerhalb der nächsten zwei Jahre.

3 Wir verfolgen sowohl aktuell als auch zukünftig keine explizite Cloud-Strategie. Einzelne Cloud-Services können aber genutzt werden.

Quelle: Lünendonk

Dürftig

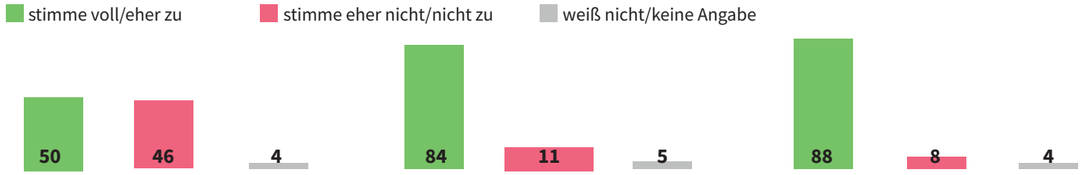
Aufstellung von Bund, Ländern und Kommunen gegen Cyberangriffe; Expertinnen und Experten in verantwortlichen IT-Funktionen, die über Einblicke in die Sicherheitsstrukturen ihrer Organisation verfügen (n=1.001); Deutschland; 2025; in Prozent



Quelle: Schwarz Digits

Behäbig

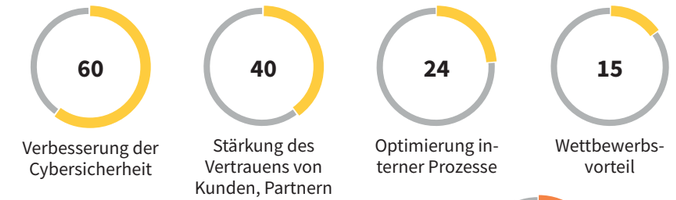
Aussagen zur politischen Regulierung von Cybersecurity; IT-Leitung/CIO, Chief Information Security Officer (CISO), Verantwortliche/r für IT-Sicherheit, Geschäftsführung oder Vorstand in Unternehmen ab zehn Mitarbeiterinnen und Mitarbeitern (n=506); Deutschland; 2025; in Prozent



Quelle: TÜV-Verband

Nachlässig

Vorteile durch Umsetzung der NIS-2-Richtlinie; IT-Leitung/CIO, Chief Information Security Officer (CISO), Verantwortliche/r für IT-Sicherheit, Geschäftsführung oder Vorstand in Unternehmen ab zehn Mitarbeiterinnen und Mitarbeitern, die von den NIS-2-Richtlinien wissen (n=281); Deutschland; 2025; in Prozent*

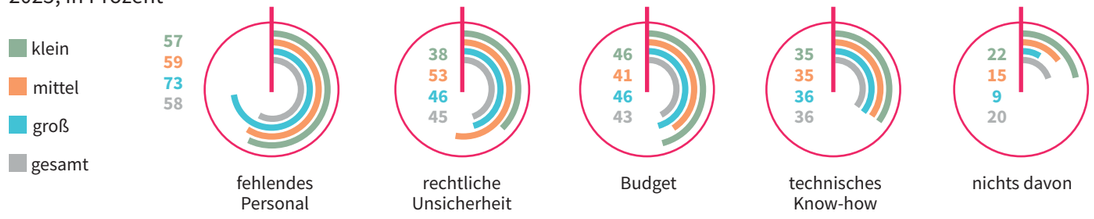


*Mehrfachnennung möglich. Quelle: TÜV-Verband

Ziel der von der EU geschaffenen **NIS-2-Regulierung** ist es, Unternehmen dazu zu verpflichten, ihre IT-Systeme und digitalen Infrastrukturen besser gegen Angriffe zu schützen. Seit dem 6. Dezember 2025 gelten diese Vorgaben auch in deutschem Recht. Viele der rund 30.000 betroffenen Unternehmen haben die Regelungen bislang nicht oder nur teilweise umgesetzt.

Vielschichtig

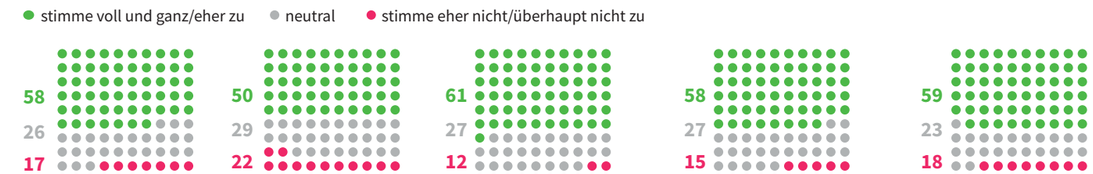
Größte Herausforderungen bei der Umsetzung der NIS-2-Richtlinie; Expertinnen und Experten in verantwortlichen IT-Funktionen, die über Einblicke in die Sicherheitsstrukturen ihrer Organisation verfügen und sich als betroffen von der NIS-2-Richtlinie einstufen (gesamt: n=105, klein: n=37, mittel: n=81, groß: n=44); Deutschland; 2025; in Prozent



* Unternehmensgröße: klein (10-49 MA), mittel (50-249 MA), groß (250 und mehr MA). Quelle: Schwarz Digits

Mäßig

Wahrnehmung zu Vorgaben, Nutzen und Belastung durch die NIS-2-Richtlinie; Unternehmen aus dem verarbeitenden Gewerbe und der Informationswirtschaft, die sich aus IKT-Branche, Mediendienstleistern und wissensintensiven Dienstleistern zusammensetzt und die voraussichtlich von der NIS-2-Richtlinie betroffen sind (n=200); Deutschland; 2026; in Prozent



Quelle: ZEW

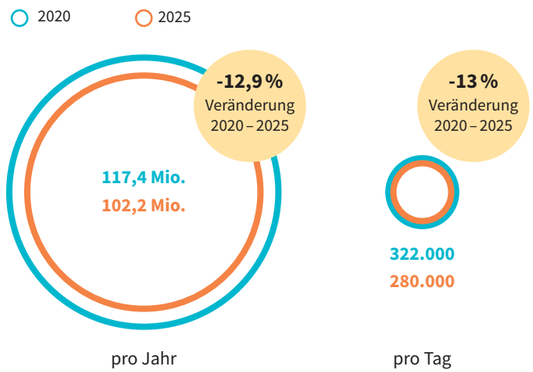
Bürokratisch

Größte Herausforderungen in der deutschen Digitalpolitik; IT-Entscheiderinnen und -Entscheider (n=500); Deutschland; 2026; in Prozent*

*Mehrfachnennung möglich. Quelle: eco – Verband der Internetwirtschaft

Dramatisch

Zahl neuer Schadprogrammvarianten; Deutschland

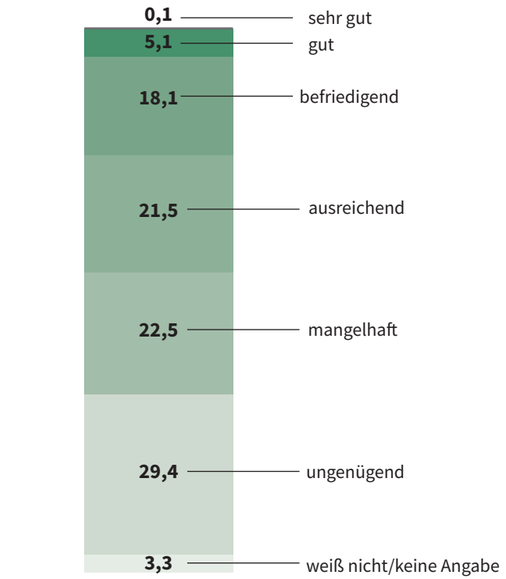


Quelle: BSI

Dilettantisch

Bewertung der Digitalpolitik der Bundesregierung; IT-Entscheiderinnen und -Entscheider (n=500); Deutschland; 2026; in Prozent

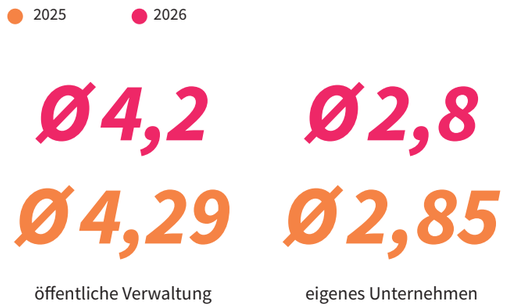
Welche Schulnote von 1 bis 6 würden Sie der Digitalpolitik der Bundesregierung nach einem Jahr insgesamt geben?



Quelle: eco – Verband der Internetwirtschaft

Kritisch

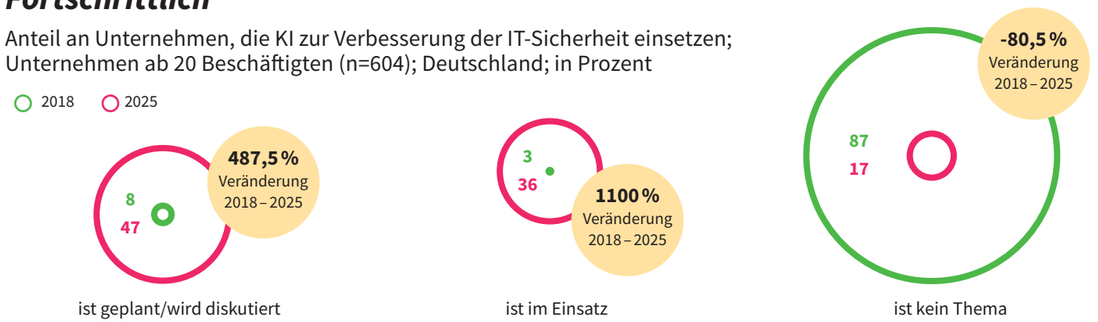
Stand der Digitalisierung in Unternehmen und öffentlicher Verwaltung; Unternehmen (2025: n=5.381, 2026: n=4.686); Deutschland; Bewertung von 1 = sehr gut bis 6 = ungenügend



Quelle: DIHK

Fortschrittlich

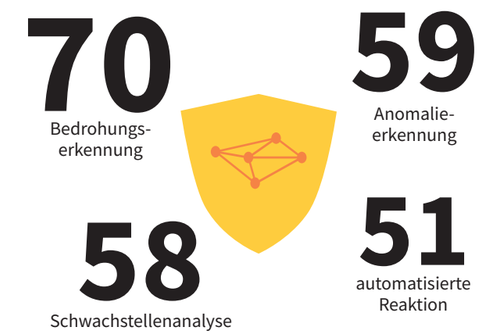
Anteil an Unternehmen, die KI zur Verbesserung der IT-Sicherheit einsetzen; Unternehmen ab 20 Beschäftigten (n=604); Deutschland; in Prozent



Quelle: Bitkom

Dynamisch

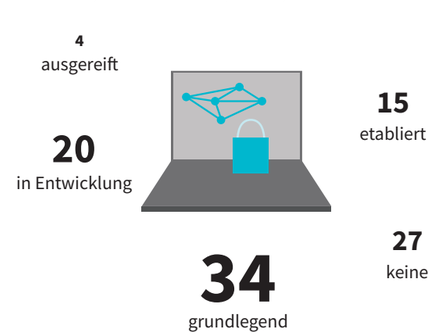
KI-Einsatz bei der Cyberabwehr; Unternehmen ab zehn Mitarbeiterinnen und Mitarbeitern, die KI im Einsatz oder dessen Einsatz in Planung haben (n= 126); Deutschland; 2025; in Prozent



Quelle: TÜV-Verband

Problematisch

Aktuelles Sicherheitsniveau für KI-gestützte Anwendungen; Unternehmen bis 499 Mitarbeiterinnen und Mitarbeiter; Deutschland; 2026; in Prozent



Quellen: Sage, IDC

Strategisch

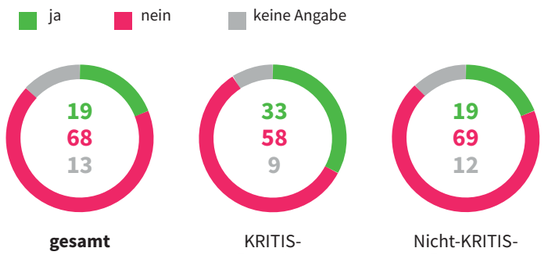
Beurteilung vom KI-Einsatz bei Cyberangriffen; Unternehmen ab zehn Mitarbeiterinnen und Mitarbeitern (n=506); Deutschland; 2025; stimme voll/eher zu in Prozent

Quelle: TÜV-Verband

Kaum Strategie

Vorhandensein einer digitalen Souveränitätsstrategie; Expertinnen und Experten in verantwortlichen IT-Funktionen, die über Einblicke in die Sicherheitsstrukturen ihrer Organisation verfügen (gesamt: n=1.001, KRITIS: n=162, Nicht-KRITIS: n=839); Deutschland; 2025; in Prozent

Hat Ihr Unternehmen eine digitale Souveränitätsstrategie?



Quelle: Schwarz Digits

Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.
Alle Organisationen aus den folgenden Sektoren zählen unabhängig von ihrer Größe zu den KRITIS: Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Medien und Kultur, Wasser, Ernährung, Finanz- und Versicherungswesen, Siedlungsabfallentsorgung, Staat und Verwaltung.

Deutlicher Konsens

Aussagen zur digitalen Souveränität; Führungskräfte, die für das Thema Wirtschaftsschutz verantwortlich sind in Unternehmen mit mindestens zehn Beschäftigten und einem Jahresumsatz von 1 Mio. Euro oder mehr (n=1.002); Deutschland; 2025; in Prozent

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

67

Unser Unternehmen ist abhängig von Sicherheitslösungen aus den USA.

74

Die Politik muss deutsche Anbieter von Cybersicherheitslösungen stärker unterstützen.

Quelle: Bitkom

Wenig Zahlungsbereitschaft

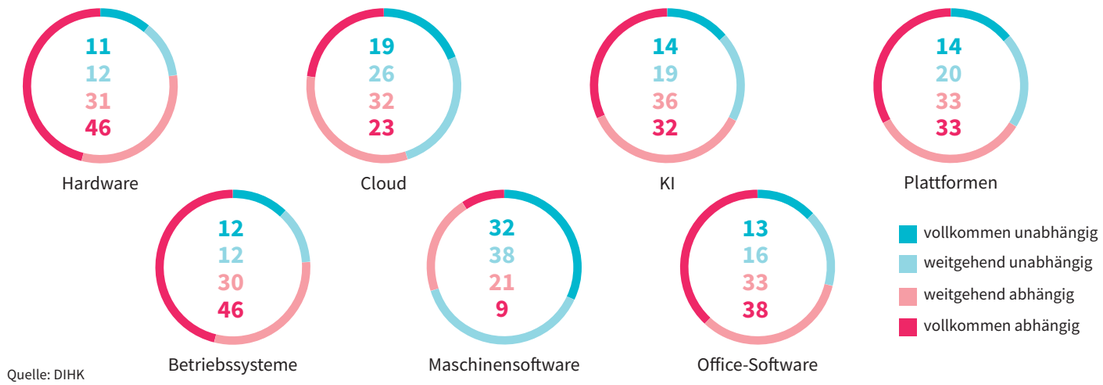
Zahlungsbereitschaft für souveräne IT-Produkte; Expertinnen und Experten in verantwortlichen IT-Funktionen, die über Einblicke in die Sicherheitsstrukturen ihrer Organisation verfügen (n=1.001); Deutschland; 2025; in Prozent

Wäre Ihr Unternehmen bereit, für souveräne IT-Produkte mehr zu bezahlen?

Quelle: Schwarz Digits

Hohe Abhängigkeit

Einschätzung der Abhängigkeit des eigenen Unternehmens von Nicht-EU-Ländern; Unternehmen (n=4.686); Deutschland; 2026; in Prozent



Quelle: DIHK

Konkrete Hebel

Prioritäten der Wirtschaft bei politischen Maßnahmen zur Verbesserung der digitalen und technologischen Souveränität; Unternehmen (n=4.686); Deutschland; 2026; in Prozent

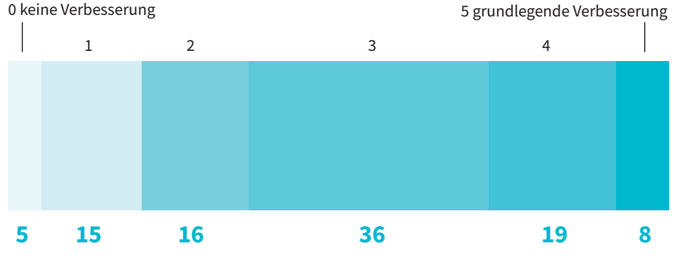
Unterstützung gemeinsamer offener Schnittstellen & Standards	48
mehr Angebote zur Kompetenzvermittlung an Schulen, Universitäten und staatlichen Bildungseinrichtungen	43
Förderung von Open-Source-Lösungen	41
Förderung von Schlüsseltechnologien und Sprunginnovationen	39
Forcierung des Ausbaus von Rechenzentrumskapazitäten und notwendiger Infrastruktur	37
Verbesserung von Technologietransfer, Forschungseinrichtungen und Unternehmen	30
öffentliche Hand als Ankerkunde (Deutschland-Stack, Vergaberecht)	16

Quelle: DIHK

Verhaltene Erwartungen

Erwartete Verbesserungen der digitalen Souveränität durch den Deutschland-Stack; öffentliche Verwaltung (n=341); Deutschland; 2026; in Prozent

Welche Erwartungen verbinden Sie mit dem Deutschland-Stack?



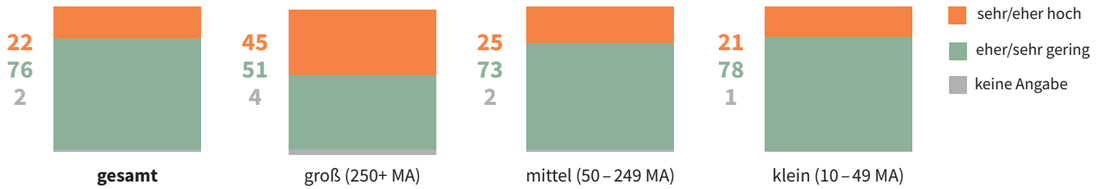
Quellen: ÖFIT, Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS, Behörden Spiegel

Der Deutschland-Stack (auch D-Stack) ist ein zentrales digitalpolitisches Projekt des Bundesministeriums für Digitales und Staatsmodernisierung (BMDS), um die IT-Infrastruktur der deutschen öffentlichen Verwaltung zu modernisieren und zu vereinen. Ziel ist es, eine sichere, einheitliche und europäisch souveräne Technologieplattform für Bund, Länder und Kommunen zu schaffen.

Beziehungsstrukturen

Risiko von Cyberangriffen über Zulieferer oder Kunden nach Unternehmensgröße; Unternehmen ab zehn Mitarbeiterinnen und Mitarbeitern (n=506); Deutschland; 2025; in Prozent

Wie hoch schätzen Sie das Risiko eines Cyberangriffs über einen Ihrer Zulieferer oder Kunden ein?



Quelle: TÜV-Verband

Einfallstore

Einfallstore für Cyberangriffe; Entscheiderinnen und Entscheider und IT-Verantwortliche von kleinen und mittleren Unternehmen, die bereits Opfer erfolgreicher Cyberangriffe waren (n=300); Deutschland; 2025; in Prozent

Der Cyberangriff erfolgte durch …

68 … eine E-Mail mit Schadsoftware.

17 … Hacker, die von außen ins System eingedrungen sind.

5 … Mitarbeitende, die das System manipuliert haben.

5 … eine DDoS-Attacke, die das System lahmgelegt hat.

Quelle: GDV

Angriffsarten

Arten der Cyberangriffe mit Schäden in den vergangenen zwölf Monaten; Führungskräfte, die für das Thema Wirtschaftsschutz verantwortlich sind in Unternehmen mit mindestens zehn Beschäftigten und einem Jahresumsatz von 1 Mio. Euro oder mehr (n=1.002); Deutschland; 2025; in Prozent*

Ransomware	34
Distributed Denial of Service (DDoS)	25
Infizierung mit Schadsoftware	24
Phishing-Angriffe	22
Angriffe auf Passwörter	21
Spoofing	15
SQL-Injection oder Cross-Site-Scripting	15
Deepfakes	4
Robo Calls	3

*Mehrfachnennung möglich. Quelle: Bitkom

Täterkreise

IT-Angriffe auf Unternehmen nach Täterkreis; Führungskräfte, die für das Thema Wirtschaftsschutz verantwortlich sind in Unternehmen mit mindestens zehn Beschäftigten und einem Jahresumsatz von 1 Mio. Euro oder mehr, die in den vergangenen zwölf Monaten von Diebstahl, Datendiebstahl, Industriespionage oder Sabotage betroffen waren (2025: n=868; 2019: n=801); Deutschland; in Prozent*

2019 | 2025 | Veränderung 2019 – 2025

2019	2025	Veränderung	
21	68	223,8 %	Organisierte Kriminalität/ Banden
38	42	10,5 %	Privatpersonen
12	28	133,3 %	ausländischer Nachrichtendienst
37	25	-32,4 %	unabsichtlich handelnde (ehemalige) Beschäftigte
33	23	-30,3 %	vorsätzlich handelnde (ehemalige) Beschäftigte
20	22	10,0 %	konkurrierende Unternehmen
8	6	-25,0 %	Kunden
16	4	-75,0 %	Lieferanten

*Mehrfachnennung möglich. Quelle: Bitkom

Datenarten

Art der gestohlenen Daten; Führungskräfte, die für das Thema Wirtschaftsschutz verantwortlich sind in Unternehmen mit mindestens zehn Beschäftigten und einem Jahresumsatz von 1 Mio. Euro oder mehr, die in den vergangenen zwölf Monaten vom Diebstahl digitaler Daten betroffen waren (n=432); Deutschland; 2025; in Prozent*

*Mehrfachnennung möglich. Quelle: Bitkom

Angriffszahlen

Entwicklung der Zahl von Cyberattacken im vergangenen Jahr; Führungskräfte, die für das Thema Wirtschaftsschutz verantwortlich sind in Unternehmen mit mindestens zehn Beschäftigten und einem Jahresumsatz von 1 Mio. Euro oder mehr (n=1.002); Deutschland; 2025; in Prozent

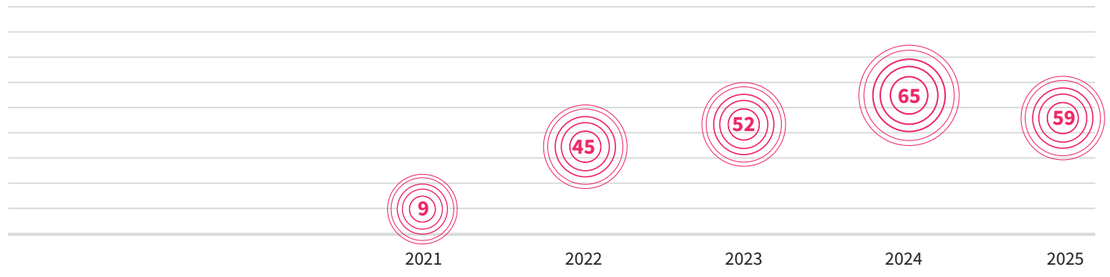
haben eher/stark zugenommen | unverändert | haben eher/stark abgenommen | weiß nicht/keine Angabe

Quelle: Bitkom

Bedrohungslagen

Bedrohung der Existenz durch Cyberattacken; Führungskräfte, die für das Thema Wirtschaftsschutz verantwortlich sind in Unternehmen mit mindestens zehn Beschäftigten und einem Jahresumsatz von 1 Mio. Euro oder mehr (n=1.002); Deutschland; in Prozent

Zustimmung der Aussage: „Cyberangriffe bedrohen unsere geschäftliche Existenz“ (trifft voll und ganz zu/trifft eher zu)



Quelle: Bitkom

Weitgehend ignoriert

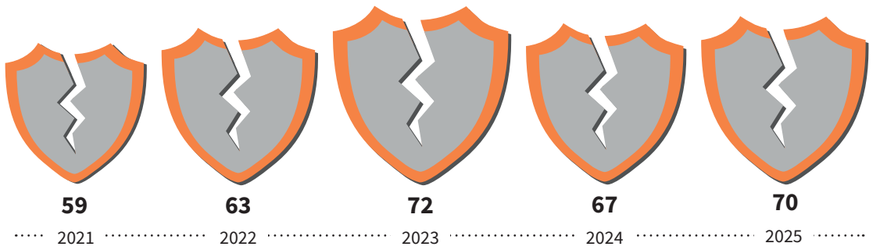
Bedrohung durch Quantencomputing; Unternehmen (n=300); DACH; 2026

14%	38%	40%	52%	44%	28%	22%	14%
… sehen quantencomputing-basierte Angriffe als ernsthafte Bedrohung.	… sehen ein moderates Bedrohungspotenzial.	… halten das Risiko durch Quantencomputing für vernachlässigbar.	… haben bislang keinerlei Vorkehrungen getroffen, um ihre Datenbestände quantensicher zu verschlüsseln.	… wollen daran auch künftig nichts ändern.	…planen zumindest teilweise den Umstieg oder haben erste Schritte bzgl. Vorkehrungen eingeleitet.	… arbeiten mit einem festen Zeitplan zur Umstellung bzgl. der Vorkehrungen.	… sehen sich bereits vollständig auf Quantenbedrohungen vorbereitet.

Quelle: Horizon3.ai

Deutlich verteilt

Anteil des entstandenen Gesamtschadens, der auf Cyberattacken zurückgeführt werden kann; Unternehmen mit mindestens zehn Beschäftigten und einem Jahresumsatz von 1 Mio. Euro oder mehr, die in den vergangenen zwölf Monaten von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (2025: n=868; 2024: n=812); Deutschland; in Prozent



Quelle: Bitkom

Klar erkannt

Grundlagen, auf denen Cyberattacken aufgedeckt wurden; Unternehmen mit mindestens zehn Beschäftigten und einem Jahresumsatz von 1 Mio. Euro oder mehr, die in den vergangenen zwölf Monaten von Datendiebstahl, Industriespionage oder Sabotage betroffen waren und Erkenntnisse über Herkunft, Täterkreis oder Motive hatten; Führungskräfte, die für das Thema Wirtschaftsschutz verantwortlich sind (n=823); Deutschland; 2025; in Prozent

Quelle: Bitkom

Teuer bezahlt

Schadenssummen, die im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage entstanden sind; Unternehmen mit mindestens zehn Beschäftigten und einem Jahresumsatz von 1 Mio. Euro oder mehr (n=1.002); Deutschland; 2025; in Milliarden Euro*

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

73,3	53,0	37,0	30,6	23,8	23,1
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	Kosten für Rechtsstreitigkeiten	Kosten für Ermittlungen und Ersatzmaßnahmen	Umsatzeinbußen durch nachgemachte Produkte bzw. Plagiate	datenschutzrechtliche Maßnahmen, z. B. durch Behörden	Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen

16,0	15,9	15,6	0,9
Patentrechtsverletzungen, auch vor Anmeldung	Imageschaden bei Kunden oder Lieferanten, negative Medienberichterstattung	Erpressung mit gestohlenen Daten	Geldabfluss durch Betrugsversuche

289,2
Gesamtschaden pro Jahr

*Mehrfachnennung möglich. Quelle: Bitkom

Ungleich betroffen

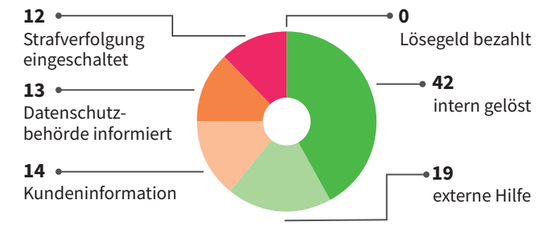
Zahl der von Betreibern kritischer Infrastrukturen gemeldeten Störungen nach Sektor; Deutschland; Q3/2024 bis Q2/2025

Gesundheit	155
Energie	153
Transport und Verkehr	150
IT und TK	123
Finanz- und Versicherungswesen	68
Ernährung	27
Wasser	24
Siedlungsabfallentsorgung	24

Quelle: BSI KRM

Selten gemeldet

Unternehmensreaktionen auf Angriffe; Expertinnen und Experten für IT-Sicherheit (n=175); Deutschland; 2025; in Prozent



Quelle: eco – Verband der Internetwirtschaft

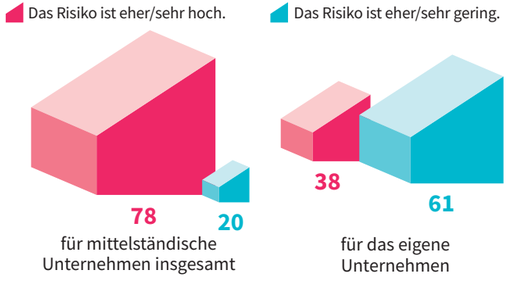
20 Stunden

… können Unternehmen in Deutschland im Schnitt den Geschäftsbetrieb ohne Internet aufrechterhalten.

Quelle: Bitkom, 2026

Irrtümer

Einschätzung des Risikos, Opfer von Cyberkriminalität zu werden; Entscheiderinnen und Entscheider und IT-Verantwortliche von kleinen und mittleren Unternehmen (n=300); Deutschland; 2025; in Prozent



Quelle: GDV

Trugschlüsse

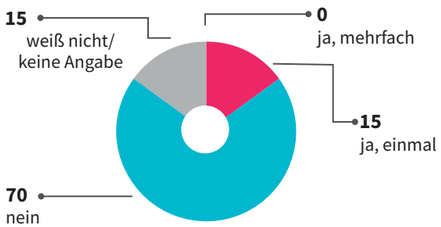
Gründe für die Annahme eines geringen Risikos in mittelständischen Unternehmen; Entscheiderinnen und Entscheider und IT-Verantwortliche von kleinen und mittleren Unternehmen, die ein eher oder sehr geringes Risiko eines Cyberangriffs auf das eigene Unternehmen sehen (n=183); Deutschland; 2025; in Prozent

Quelle: GDV

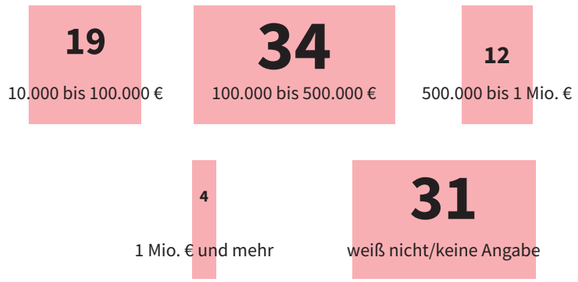
Lehrgelder

Lösegeldzahlungen nach Ransomware-Angriffen; Führungskräfte, die für das Thema Wirtschaftsschutz verantwortlich sind in Unternehmen mit mindestens zehn Beschäftigten und einem Jahresumsatz von 1 Mio. Euro oder mehr, die von Ransomware-Angriffen betroffen waren (n=588) und die Lösegeld bezahlt haben (n=86); Deutschland; 2025; in Prozent

Haben Sie bei Ransomware-Angriffen Lösegeld bezahlt?



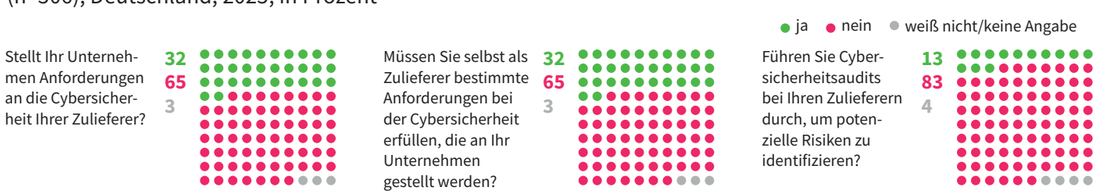
Wie hoch war die Summe, die Sie in den vergangenen zwölf Monaten gezahlt haben?



Quelle: Bitkom

Prüfsteine

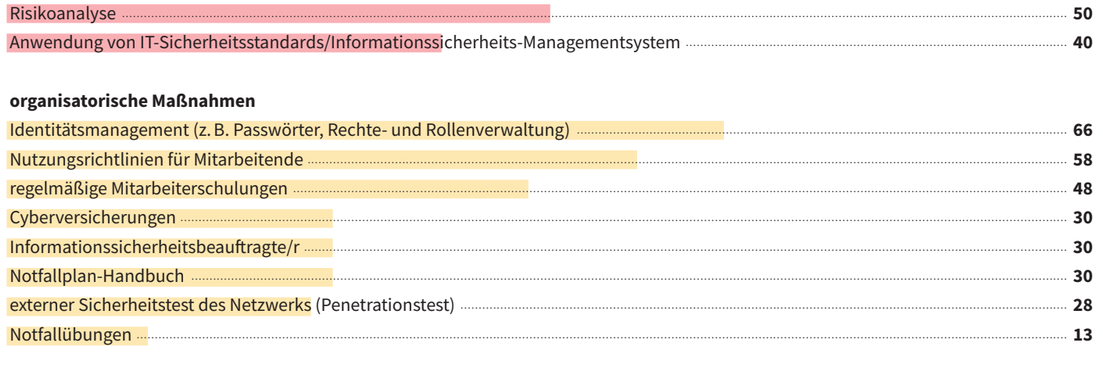
Sicherheitsanforderungen an Zulieferer; IT-Leitung/CIO, Chief Information Security Officer (CISO), Verantwortliche für IT-Sicherheit, Geschäftsführung oder Vorstand in Unternehmen ab zehn Mitarbeiterinnen und Mitarbeitern (n=506); Deutschland; 2025; in Prozent



Quelle: TÜV-Verband

Sicherheitsmaßnahmen

Strategische, organisatorische und technische Maßnahmen für mehr Cybersicherheit, die in Unternehmen umgesetzt werden (n=4.686); Deutschland; 2025; in Prozent*

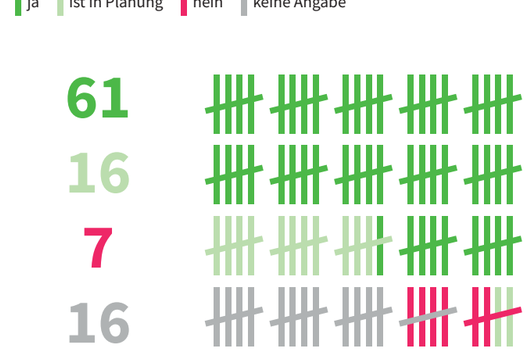


*Mehrfachnennung möglich. Quelle: DIHK

Notfallpläne

Interne Prozesse und Notfallplan für IT-Sicherheitsvorfälle; Expertinnen und Experten für IT-Sicherheit (n=175); Deutschland; 2025; in Prozent

Hat Ihr Unternehmen für den Fall eines IT-Sicherheitsvorfalls interne Prozesse bzw. einen Notfallplan festgelegt?



Quelle: eco – Verband der Internetwirtschaft

Normen und Standards

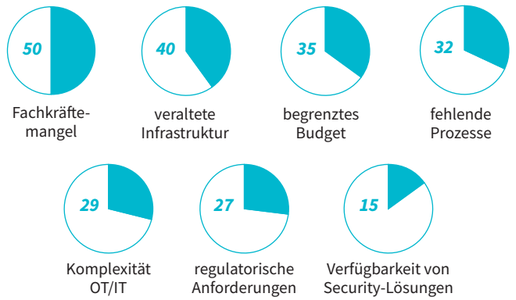
Normen und Standards für Cybersicherheit; Unternehmen ab zehn Mitarbeiterinnen und Mitarbeitern (n=506); Deutschland; 2025; in Prozent

Quelle: TÜV-Verband

Hindernisse

Hindernisse bei der Umsetzung von Cybersecurity-Maßnahmen; IT-Verantwortliche sowie Geschäftsführerinnen und Geschäftsführer aus Unternehmen der deutschen Industrie unterschiedlicher Größenklassen (n=200); Deutschland; 2026; in Prozent*

Welche aktuellen Schwierigkeiten oder Hindernisse erschweren die Umsetzung von Cybersecurity-Maßnahmen in Ihrem Unternehmen?

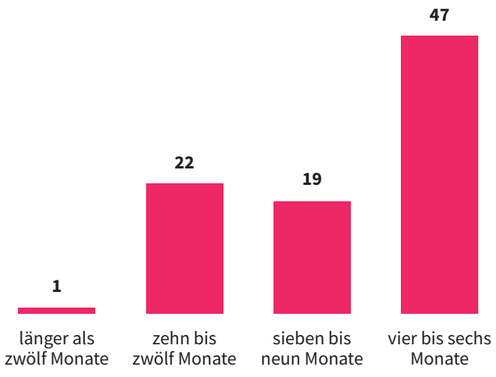


*Mehrfachnennung möglich. Quelle: Diconium

Wartezeiten

Vakanzdauer von IT-Stellen in Unternehmen; Unternehmen mit mindestens drei Beschäftigten; Personalverantwortliche und Geschäftsführung/Vorstand mit Verantwortung für Personalentscheidungen (n=855); Deutschland; 2025; in Prozent

Wie lange sind Stellen für IT-Fachkräfte in Ihrem Unternehmen in der Regel vakant?

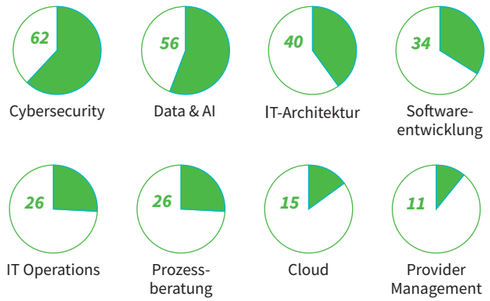


Quelle: Bitkom

Mangelbereiche

Bereiche mit dem größten IT-Fachkräftemangel; Anwenderunternehmen aus dem gehobenen Mittelstand und Konzerne (n=133); Deutschland; 2025; in Prozent*

In welchen Bereichen fehlen in den nächsten Jahren die meisten IT-Mitarbeitenden?



*Mehrfachnennung möglich. Quelle: Lünendonk

Folgeerscheinungen

Auswirkungen des Fachkräftemangels; IT-Entscheiderinnen und -Entscheider in Anwenderunternehmen (n=136); Deutschland; 2025; in Prozent

Welche Auswirkungen hat der Mangel an Fachkräften auf Ihre IT-Organisation?

Das Honorarniveau für externe Dienstleister wird steigen, um knappe Ressourcen am Markt zu sichern.	74
Wir müssen unsere Legacy-Systeme auf neue Technologieplattformen heben, um deren Wartung und Pflege zu gewährleisten.	66
Externe IT-Dienstleister gewinnen für uns an Relevanz.	65
Wir setzen stärker auf die Möglichkeiten von künstlicher Intelligenz und Automatisierung.	65
Wir bilden verstärkt aus (z. B. duale Studiengänge).	60
Geplante Projekte und Vorhaben müssen aufgrund knapper Ressourcen gestoppt oder neu priorisiert werden.	49
Wir beziehen unsere Kernanwendungen in Zukunft als Software-as-a-Service (SaaS).	46
Es entstehen Wettbewerbsnachteile, und wir verlieren den Anschluss an die digitalen Vorreiter.	31
Wir rekrutieren zukünftig deutlich mehr IT-Personal aus den Near- und Offshoring-Regionen.	23
Wir holen IT-Experten aus dem Ruhestand wieder zurück.	13

Quelle: Lünendonk

Wissensverluste

IT-Fachkräftemangel und Wissensverlust als Risikofaktor für IT-Dienstleister und IT-Organisationen; Anwenderunternehmen aus dem gehobenen Mittelstand und Konzerne (IT-Personalbedarf in drei Jahren: n=134, ausscheidende IT-Mitarbeitende (Ruhestand): n=121, Risiko des Wissensverlustes durch den demografischen Wandel n=131); Deutschland; 2025; in Prozent

Wie wird sich der Personalbedarf Ihrer internen IT in den kommenden drei Jahren entwickeln?

nimmt stark zu	3
nimmt eher zu	46
bleibt konstant	44
nimmt eher ab	6
nimmt sehr stark ab	1

Wie viel Prozent Ihrer IT-Mitarbeiterinnen und -Mitarbeiter gehen in den nächsten Jahren in etwa in Ruhestand?

2025	2,5
2026	3,2
bis 2030	9,7

Wie hoch schätzen Sie das Risiko des mit dem demografischen Wandel einhergehenden Wissensverlusts ein?

geschäftskritisch	9
signifikant	38
handhabbar	38
gering	15

Quelle: Lünendonk

Gegenmaßnahmen

Maßnahmen gegen den IT-Fachkräftemangel; Unternehmen ab drei Beschäftigten (n=855); Deutschland; 2025; in Prozent*

Was tut ihr Unternehmen, um dem IT-Fachkräftemangel entgegenzuwirken?

*Mehrfachnennung möglich. Quelle: Bitkom

Rekrutierungspläne

Maßnahmen zur Gewinnung von Frauen für IT- und Digitalberufe; Unternehmen mit mindestens 20 Beschäftigten (n=605); Deutschland; 2025; in Prozent*

Welche Maßnahmen haben Sie im Einsatz bzw. planen Sie, um Frauen speziell auf IT- und Digitalberufe in Ihrem Unternehmen aufmerksam zu machen und zu rekrutieren?

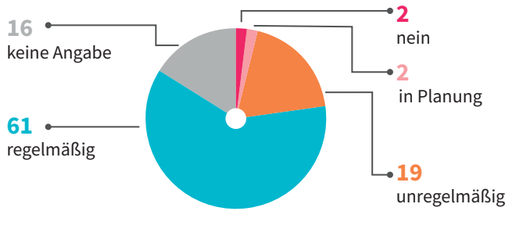
	im Einsatz	geplant
Kooperation mit Hochschulen und Schulen	24	31
Einstiegsprogramme, z. B. Traineeships	19	24
aktives Recruitment, z. B. Talentpools	13	15
Quereinstiegsprogramme	3	10
zugeschnittene Werbe-/Social-Media-Kampagnen	15	20
frauenspezifische Karriereevents/-messen	16	17
Nutzung weiblicher Rollenvorbilder in der Kommunikation	10	17
Frauen werden bei gleicher Qualifikation bevorzugt.	5	12
auf Frauen ausgerichtete Stellenausschreibungen	6	14
Kampagnen zur Ansprache weiblicher Fachkräfte aus dem Ausland	7	17

*Mehrfachnennung möglich. Quelle: Bitkom

Mitarbeitertrainings

Mitarbeiterschulungen bezüglich IT-Sicherheit; Expertinnen und Experten für IT-Sicherheit (n=175); Deutschland; 2025; in Prozent

Schulen und sensibilisieren Sie Ihre Mitarbeitenden bezüglich IT-Sicherheit?



Quelle: eco – Verband der Internetwirtschaft

Dringend gesucht: Sicherheitsexperten

Es ist eigentlich ganz einfach: Will Deutschland souverän sein, braucht es Menschen, die für diese digitale Unabhängigkeit sorgen. Bislang gibt es viel zu wenige. Wo könnten sie in Zukunft herkommen?

Text: Daniel Erk

Sicherheitslücke: Wie finden wir mehr Cybersicherheits-Fachkräfte?

Keine Ausbildungswege, kaum Studiengänge: Wer in Deutschland als Cybersicherheitsexperte arbeiten wollte, musste lange selbst sehen, wie und wo er sich Kompetenzen aneignete. Das Feld lag nahezu unbeackert da, ein Nischenthema mit überschaubarer politischer und wirtschaftlicher Relevanz. Cybersicherheit wurde als etwas angesehen, das es geben musste, das funktionieren sollte, aber mit dem sich keiner so recht befassen wollte. Fachkräfte waren oftmals Seiteneinsteiger, die auf verschlungenen Pfaden in den Beruf gelangten.

Das hat sich grundlegend geändert. Seit Cyberattacken nicht mehr nur Behörden oder Betreiber kritischer Infrastruktur treffen, hat sich die Aufmerksamkeit drastisch verschoben. Erst im Frühjahr 2026 wurde der Sportartikelhersteller Adidas zum zweiten Mal innerhalb weniger Monate Opfer eines Hackerangriffs, bei dem Datensätze eines Dienstleisters erbeutet wurden.

Der Anteil, den Cyberattacken am Gesamtschaden der deutschen Wirtschaft durch Datendiebstahl, Sabotage und Industriespionage haben, ist laut des deutschen Digitalverbands Bitkom auf 70 Prozent gestiegen – auf eine Summe in Höhe von 202,4 Milliarden Euro. Das entspricht nahezu der jährlichen Wirtschaftsleistung Berlins. Entsprechend beschreiben fast drei Viertel aller Unternehmen die derzeitige Bedrohungslage für analoge und digitale Angriffe als „hoch“. 87 Prozent der Befragten berichten von konkreten Angriffen, weitere Unternehmen vermuten Vorfälle.

Gleichzeitig stieg der Anteil der betroffenen Unternehmen, die mindestens einen Angriff ausländischen Nachrichtendiensten zurechnen, innerhalb von zwei Jahren sprunghaft von sieben auf 28 Prozent. Die Angst vor Wirtschaftsspionage und anschließendem Technologietransfer insbesondere aus China wächst in Deutschlands Wirtschaft stetig. Sie kommt nicht von ungefähr: Laut des jüngsten Berichts des Bundesamts für Sicherheit in der Informationstechnik (BSI) von 2025 wurden weltweit durchschnittlich 119 neue Schwachstellen bekannt – pro Tag! 24 Prozent mehr als im Vorjahr. Dazu registrierte das BSI 2025 in Deutschland rund 950 angezeigte Ransomware-Angriffe, 461 bekannt gewordene Datenlecks und täglich etwa 280.000 neue Schadprogrammvarianten.

Foto: istock

Leerstellen: Kann ein neues Ausbildungsangebot helfen?

All das bedeutet vor allem eins: Deutschland braucht mehr Cybersicherheitsexpertinnen und -experten.

Verschärfend kommt hinzu, dass sich der russische Angriffskrieg auf die Ukraine längst nicht mehr auf physische Auseinandersetzungen beschränkt, sondern auch im Digitalen tobt. Den Angriff auf das Satellitennetzwerk KA-SAT von Viasat kurz vor Beginn der russischen Invasion 2022 schrieb unter anderem die Bundesregierung Russland zu. In ganz Europa fielen tausende Modems aus, auch deutsche Windkraftanlagen waren betroffen. Attacken auf Infrastruktur sowie digitale Störungen sind heute ein bedeutender Teil hybrider Konflikte geworden.

Auch das bedeutet: Deutschland braucht mehr Cybersicherheitsexpertinnen und -experten.

Und dann wäre da auch noch die Regulierung: Die Europäische Union verschärfte mit der NIS-2-Richtlinie, die mit dem NIS-2-Umsetzungsgesetz im Dezember 2025 in Deutschland in Kraft getreten ist, die Anforderungen an Cybersicherheit und den Schutz kritischer Infrastruktur deutlich. Sicherheit wird nicht mehr nur empfohlen. Sie wird Pflicht.

Sie wird Pflicht für öffentliche und private Einrichtungen aus insgesamt 14 kritischen Sektoren wie Energie, Verkehr, Gesundheitswesen, digitale Infrastruktur, Verwaltung und Forschung, die mehr als 50 Mitarbeitende beschäftigen oder mindestens 10 Millionen Euro Jahresumsatz vorweisen. Sie müssen künftig digitale Risiken systematisch analysieren, Sicherheitsmaßnahmen implementieren, Lieferketten absichern und Vorfälle teilweise innerhalb weniger Stunden an die Behörden melden.

Und ja, natürlich bedeutet das: Deutschland braucht mehr Cybersicherheitsexperten.

Aber woher sollen sie kommen?

Ächzender Arbeitsmarkt

Laut Bitkom fehlen in Deutschland derzeit rund 109.000 IT-Fachkräfte. Das sind zwar deutlich weniger als noch 2023, als 149.000 Stellen als unbesetzt galten, aber wenn man sich vorstellt, dass jeder einzelne dieser freien Arbeitsplätze eine potenzielle Sicherheitslücke darstellt, wird klar: Das Problem ist riesig.

Der Markt für Cybersicherheit wächst derweil weiter: 2025 wurden in Deutschland mit Cybersicherheit 11,1 Milliarden Euro umgesetzt, schätzt Bitkom. 2026 wird sogar mit rund 12,2 Milliarden Euro gerechnet.

Gleichzeitig erwarten fast vier von fünf Unternehmen, dass sich der Fachkräftemangel noch verschärfen wird. „Cyberangriffe sind nicht mehr nur ein abstraktes IT-Problem“, sagt Michaela Geierhos, Professorin für Data Science an der Universität der Bundeswehr München.

Was lange als Spezialgebiet für Administratoren und IT-Abteilungen galt, ist heute zu einer Querschnittsaufgabe geworden. Je digitaler Unternehmen, Behörden und Infrastruktur werden, desto weniger lässt sich Sicherheit an einzelne Abteilungen delegieren. Software Engineering, künstliche Intelligenz, Cloud-Systeme, Verwaltung, kritische Infrastruktur oder militärische Systeme lassen sich ohne genaue Berücksichtigung von Sicherheitsaspekten nicht mehr entwickeln und betreiben.

Der Fachkräftemangel ist nicht mehr allein ein Arbeitsmarktproblem. Er ist zur zentralen Frage der politischen und wirtschaftlichen Souveränität eines ganzen Landes geworden.

Schneller Quereinstieg

Laut einer Bitkom-Umfrage dauert es durchschnittlich 7,7 Monate, bis eine IT-Stelle besetzt werden kann. Das Problem ist dabei keineswegs auf Deutschland beschränkt: Die internationale Branchenorganisation ISC2, die Zertifikate wie CISSP vergibt, schätzt die weltweite Lücke bei Cybersecurity-Fachkräften weiterhin auf mehrere Millionen Stellen. „Der Bedarf wächst schneller als die Ausbildungskapazität“, sagt Expertin Michaela Geierhos.

Für Felix Kuhlenkamp, Leiter des Bereichs Sicherheit bei Bitkom, ist die Lage allerdings noch komplexer. „Die Frage ist ja nicht allein, ob wir diese Stellen besetzt bekommen“, sagt er, „die größere Frage lautet: Gibt es genug Leute, die kompetent genug sind, um diese wachsenden Sicherheitsanforderungen ›

abzudecken?“ Sicherheitslücken entstehen also nicht nur zwischen Angebot und Nachfrage, sondern auch in der Qualifikation der Mitarbeitenden – und das in einem Markt, der sich immer weiter ausdifferenziert.

Die Branche reagiert pragmatisch. Nach Bitkom-Zahlen entfallen inzwischen rund 27 Prozent der Neueinstellungen in der IT auf Menschen, die nicht den klassischen Ausbildungsweg gegangen sind, also auf Quereinsteigende. Nach einer OECD-Analyse verzichten inzwischen 30 bis 35 Prozent der Stellenanzeigen auf konkrete Bildungsabschlüsse. Gesucht werden häufig weniger bestimmte Studiengänge als vielmehr Erfahrung, technische Kompetenzen und die Fähigkeit, sich in neue Bedrohungslagen einzuarbeiten. Der typische Quereinsteiger hat vor allem berufspraktische IT-Kenntnisse, Berufsausbildungen außerhalb der IT oder auch autodidaktisch erworbene IT-Kenntnisse.

Die hohe Zahl an Quereinsteigenden ist zugleich ein Hinweis darauf, dass sich der Arbeitsmarkt bereits verändert hat. Neue Cybertools, neue Angriffsmethoden und neue Regulierungen sorgen dafür, dass Wissen schneller veraltet als früher. Eine Branche, in der lebenslanges Lernen schon immer galt, muss sich jetzt darauf einstellen, dass Lernen zur täglichen Aufgabe wird.

Anspruchsvolle Ausbildung

Trotzdem gibt es in der Ausbildung weiterhin keinen eigenständigen Schwerpunkt. Das ist bemerkenswert, weil Fachinformatikerinnen und -informatiker häufig die grundlegende Arbeit in der IT-Sicherheit übernehmen.

„Hier gibt es aus unserer Sicht noch Nachholbedarf, weil es weiterhin nur die Ausbildung zum Fachinformatiker gibt und keinen Schwerpunkt Cybersicherheit“, sagt Felix Kuhlenkamp vom Bitkom.

Ein Zusammenschluss aus führenden Branchenvertretern schlug 2025 deshalb einen eigenständigen Ausbildungsberuf für Cybersicherheit vor. Die Vorstellung, Cybersicherheit sei vor allem eine akademische Disziplin, greift ganz offenbar zu kurz. Wer Sicherheitslücken schließen will, braucht nicht nur Forscherinnen, Analysten und Strateginnen. „Wir brauchen Menschen, die Infrastrukturen härten, Logfiles analysieren und Sicherheit im Alltag umsetzen, gerade im Mittelstand“, sagt Sebastian Barchnicki, einer der Initiatoren des Zusammenschlusses und Sprecher der Geschäftsführung bei „Digital.Sicher.NRW“ (siehe auch Interview S. 81). Genau auf diese praktische Arbeit zielt daher der Vorschlag für einen eigenständigen Ausbildungsberuf. Der soll nicht auf einzelne Technologien zugeschnitten sein, sondern auf die Grundlagen der Sicherheit. Barchnicki: „Cybersicherheit ist ein anspruchsvolles, operatives Handwerk.“ Und weil sie eben auch ein Handwerk ist, soll sie künftig nicht mehr nur an Hochschulen vermittelt werden.

Praxisnahe Studiengänge

Die deutschen Hochschulen haben bereits auf die veränderten Anforderungen reagiert. Was lange als Spezialisierung innerhalb der Informatik galt, wird heute zunehmend als eigenes Fach ausgebildet. Neben klassischen Informatikstudiengängen entstanden in den vergangenen Jahren zahlreiche Bachelor- und Masterprogramme, die Cybersicherheit ins Zentrum stellen. Neben klassischer Informatik mit Schwerpunkt IT-Sicherheit gibt es nun auch eigene Angebote zu digitaler Forensik.

Dahinter steht die Erkenntnis, dass digitale Sicherheit längst kein Spezialgebiet mehr ist, sondern nahezu alle Bereiche moderner Infrastruktur betrifft. Besonders weit reicht diese Entwicklung an der Universität der Bundeswehr München. Dort wird Cybersicherheit nicht nur als technische Disziplin verstanden, sondern auch als Frage staatlicher Resilienz. Neben Offiziersanwärterinnen und -anwärtern studieren dort auch Mitarbeitende von Bundesbehörden und -ministerien sowie aus einigen Unternehmen mit Bezug zur Bundeswehr. Das Studium beschäftigt sich nicht nur damit, wie digitale Systeme gebaut werden, sondern auch mit der Frage, wie sie im Krisenfall funktionsfähig bleiben.

Michaela Geierhos steht an der Bundeswehr-Universität für diese Expertise: Seit 2020 ist sie dort Professorin für Data Science, seit 2021 zudem technische Direktorin des Forschungsinstituts Cyber Defence und Smart Data (CODE), an dem Forschung zu Cybersicherheit, Datenanalyse und digitalen Bedrohungen gebündelt wird.

Verfügbarkeit, Resilienz und digitale Souveränität sind längst zu sicherheitspolitischen Kategorien geworden. Gute Cybersicherheit entsteht dort, wo Theorie, Systemkompetenz, Recht und operative Erfahrung zusammenkommen. Dafür braucht es nicht allein mehr Studienplätze, sondern auch mehr Lehrende, Labore und realistische Übungsumgebungen. Die größte Lücke liegt für Michaela Geierhos nicht in der Zahl derer, die ihr Studium abschließen – „sondern in der Kombination aus Spezialisierung und Praxiserfahrung“.

Harte Konkurrenz

Hochschulabsolventen, hervorragend ausgebildet in Cybersicherheit – und nun? Bleiben sie in Deutschland? Qualifizierte Absolventinnen und Absolventen sind längst Teil eines internationalen Arbeitsmarkts. Sie konkurrieren nicht nur um Stellen in Deutschland, sondern auch um Angebote aus aller Welt, vor allem aus den USA und Großbritannien.

„Unternehmen an attraktiven internationalen Standorten, große bekannte Arbeitgeber, aber auch Beratungsunternehmen und dedizierte Security-Dienstleister können häufig mit Gehältern, Budgets und Geschwindigkeit punkten“, sagt Geierhos.

Die Konkurrenz um die besten Fachkräfte ist auch eine Frage des Gehalts. Nach Daten des Stellenmarkts „Jobs-beim-Staat“ beginnen IT- und Cybersecurity-Karrieren im öffentlichen Dienst für Hochschulabsolventinnen und -absolventen bei rund 47.000 Euro im Jahr, selbst in höheren Laufbahnen liegen die Gehälter häufig unter 85.000 Euro. Der Personaldienstleister Hays verortet IT-Fachkräfte mit Studium zwischen 56.000 und 85.000 Euro, in der Industrie können es in Führungspositionen auch über 150.000 Euro werden. Generell gilt: In der Privatwirtschaft verdient man aufgrund variabler Gehaltsanteile im Mittel fast 20 Prozent mehr als im öffentlichen Dienst. In den USA wiederum verdienen Cybersecurity Engineers laut der Job-Plattform Indeed bereits in Positionen ohne Leitungsfunktion oft mehr als 120.000 Dollar jährlich.

Können Behörden, Bundeswehr und öffentliche Einrichtungen mit anderen Vorteilen im Vergleich zur Privatwirtschaft punkten? „Sinn, Verantwortung, langfristige Perspektiven, spannende Aufgaben und Zugang zu sicherheitskritischen Problemstellungen“, zählt Michaela Geierhos auf. Dauerhaft dürfte das allerdings nur dann reichen, wenn Karrierewege flexibler werden, technische Fachlaufbahnen attraktiver und Einstellungsverfahren schneller.

Gefährliche Verlagerung

In Zeiten der Globalisierung lässt sich Cybersicherheit grundsätzlich ebenso auslagern wie viele andere Teile der Wertschöpfung. Sicherheitsdienstleistungen können dort eingekauft werden, wo Löhne niedriger und Arbeitszeiten länger sind. Mit der Kostenersparnis kaufen Unternehmen allerdings unbewusst oft auch Risiken ein: andere Rechtsnormen, andere Sicherheitsstandards und zusätzliche Abhängigkeiten.

Das eigentliche Risiko liegt jedoch nicht in den Gehaltsunterschieden selbst. Problematisch wird es dann, wenn aus Gehaltsunterschieden Verfügbarkeitsprobleme werden. Wenn Unternehmen, Behörden und Forschungseinrichtungen um dieselben Menschen konkurrieren, aber mit sehr unterschiedlichen Möglichkeiten antreten, wird aus Wettbewerb schnell Knappheit.

Während große Unternehmen eigene Sicherheitsabteilungen aufbauen und um Fachkräfte konkurrieren können, fehlen vielen Städten und Verwaltungen dafür die personellen und finanziellen Möglichkeiten.

Gleichzeitig schreitet die Digitalisierung auch in den Kommunen weiter voran. Bürgerämter, Register, Schulen, Verkehrssysteme und kommunale Versorger werden digitalisiert – und selbst zu potenziellen Angriffszielen. Das Problem: Ein neu entwickelter Prozess, der ohne den Gedanken an Sicherheit entwickelt wurde, ist unmöglich im Nachhinein abzusichern. Die Systeme, die heute aufgebaut werden, bestimmen später, wie widerstandsfähig Staat und Verwaltung tatsächlich sind.

Verlässliches Prinzip

Kurzfristig wird sich der Fachkräftemangel kaum vollständig beheben lassen. Dafür wachsen die Anforderungen durch neue Bedrohungen, Regulierung und Digitalisierung schlicht zu schnell. Die eigentliche Frage lautet deshalb nicht nur, wie Deutschland möglichst viele zusätzliche Expertinnen und Experten für Cybersicherheit hervorbringen kann. Sondern wie die vorhandenen Aufgaben zielgerichteter verteilt werden können. Dabei könnte ausgerechnet ein altes deutsches Prinzip helfen: die Aufgabenteilung zwischen Hochschulen und beruflicher Ausbildung. Nicht jede Sicherheitsaufgabe braucht einen Hochschulabschluss, aber jedes Problem seinen Spezialisten.

„Eigene Fachkräfte sind ein Stück Souveränität“

Branchenvertreter sagen: Es braucht eine neue Ausbildung in Sachen Cybersicherheit. Sebastian Barchnicki, Mitinitiator dieser Forderung und Sprecher der Geschäftsführung bei „Digital.Sicher. NRW“, erklärt, warum.

Woher kam der Impuls, neben dem akademischen Weg auch eine Berufsausbildung im Bereich Cybersicherheit zu etablieren?

Alle sprechen vom Fachkräftemangel, gerade in der Cybersicherheit. Für uns war das der Anstoß, die Frage anders zu stellen: Was kann die Branche selbst tun, um Nachwuchs zu gewinnen? Bislang stützte sich die Cybersicherheit fast ausschließlich auf die akademische Ausbildung, aber das greift zu kurz. Wir brauchen Menschen, die Infrastrukturen härten, Logfiles analysieren und Sicherheit im Alltag umsetzen, gerade im Mittelstand. Viele Unternehmen können sich hoch bezahlte akademische Fachkräfte gar nicht leisten und brauchen deshalb praxisnah ausgebildete Spezialistinnen und Spezialisten.

Hat bei der Etablierung des Ausbildungsberufs die nationale Souveränität eine Rolle gespielt?

Absolut, ja. Nationale und europäische Souveränität beginnt in unseren Köpfen. Sie entsteht nur, wenn Technologien und Sicherheitsprozesse verstanden und verantwortungsvoll umgesetzt werden können. Das stärkt die Unabhängigkeit von Drittstaaten und schützt zugleich die Wirtschaft. Jede unbesetzte Stelle erhöht Risiken. Gleichzeitig verpflichten Vorgaben wie NIS-2 immer mehr Unternehmen zu nachweisbarer Cybersicherheit. Auch das ist ein Stück Souveränität: die Fähigkeit, eigene gesetzliche Standards mit eigenen Fachkräften umzusetzen.

Wie definiert man die Inhalte eines solchen Ausbildungsberufs, gerade in einem so dynamischen Feld wie der Cybersicherheit?

Auch wenn sich die Bedrohungslandschaft ständig verändert: Die Prinzipien der Sicherheit bleiben grundsätzlich gleich. Basissicherheit wie Patch- und Updatemanagement, Netzwerkprotokolle, Kryptografie, Berechtigungskonzepte oder Security by Design lassen sich nur mit Fachkräften flächendeckend und qualitativ hochwertig umsetzen und aufrechterhalten. Im neuen Beruf sollen Cybersicherheitsaspekte deshalb den Schwerpunkt bilden, praxisnah, technologieneutral, risikoorientiert und mit einem tiefgehenden methodischen Fundament.

Die Initiative, einen eigenständigen Ausbildungsberuf vorzuschlagen, geht zurück auf Christine Skropke (Secunet), Ralf Kleinfeld (Vorstand der CISO Alliance), Andreas Lüning (Mitgründer und Vorstand von G DATA CyberDefense), Sebastian Barchnicki (Digital.Sicher.NRW) und den Branchenverband Eurobits.

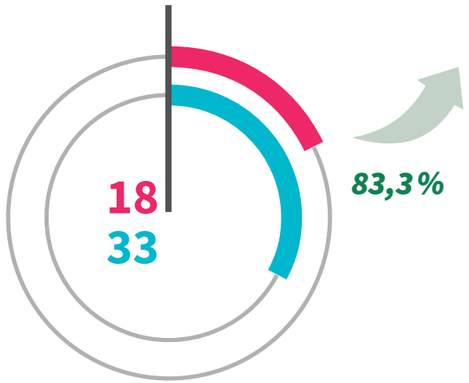
WIR

Digital ist Alltag. Wir arbeiten, lernen, kommunizieren, kaufen ein, reisen und bezahlen online. Mit jedem Klick entstehen neue Möglichkeiten – und neue Angriffsflächen. Cybersecurity wird damit zur Alltagsfrage. Wie gut schützen wir unsere Daten, Geräte und Identitäten? Und was passiert, wenn Cyberkriminelle erfolgreich sind?

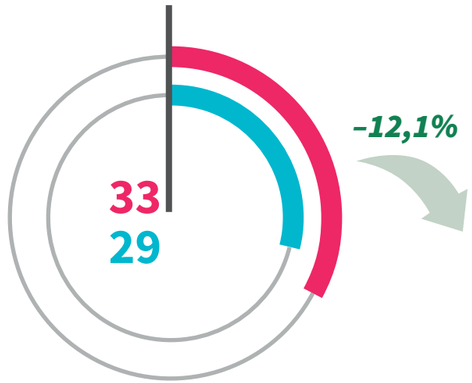
Licht und Schatten

Schäden bei Opfern von Cyberkriminalität; deutschsprachige Bevölkerung ab 16 Jahren, die in einem Privathaushalt lebt, über einen Internetzugang verfügt und in den vergangenen zwölf Monaten Opfer von Internetkriminalität geworden ist (2026: n=273; 2023: n=305); in Prozent*

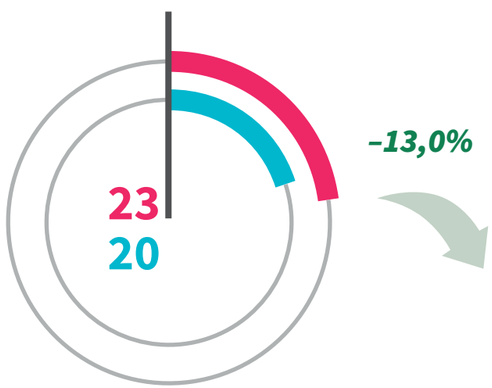
2023 2026 Veränderung 2023 – 2026



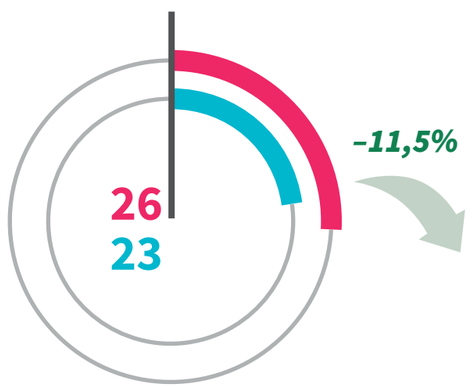
finanzieller Schaden



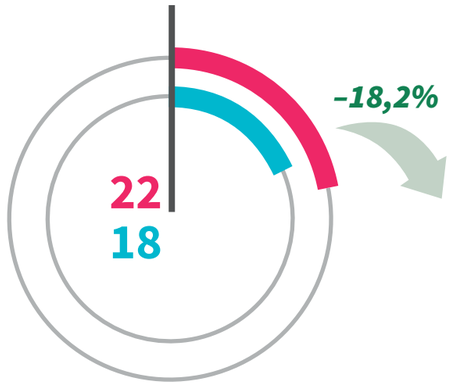
Vertrauensverlust in entsprechende Onlinedienste



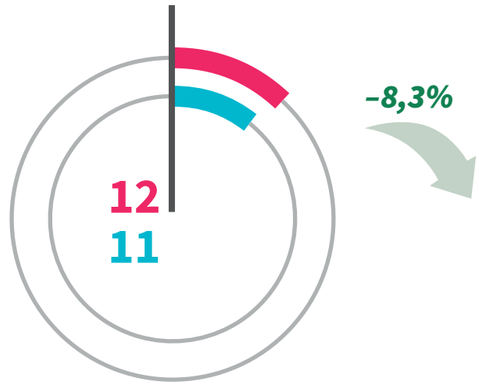
emotionaler Schaden



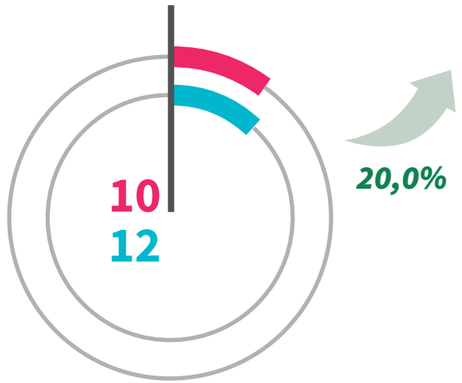
zeitlicher Schaden



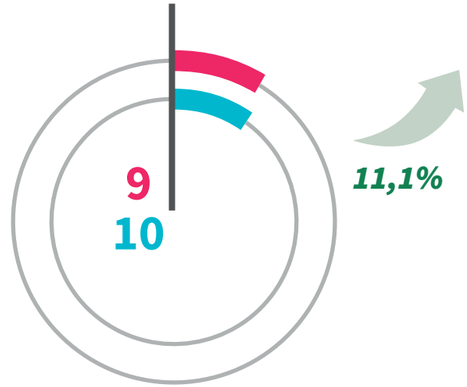
Verlust von Daten



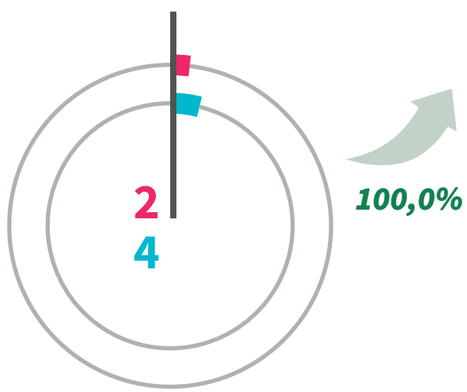
theoretischer finanzieller Schaden (Versicherungsfall)



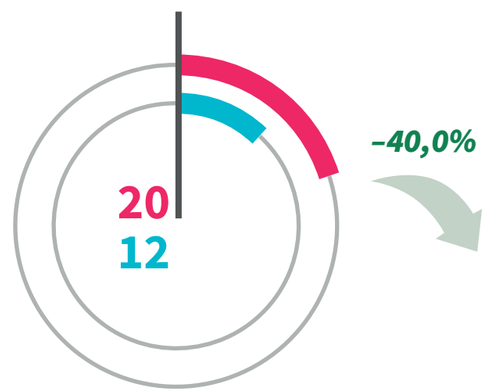
Rufschädigung



Verlust eines Gerätes



Sonstiges



kein nennenswerter Schaden

*Mehrfachnennung möglich. Quelle: BSI

Das Glossar der Cyberbegriffe finden Sie auf den Seiten 100 – 103.

Informiert

Aktive Suche nach Informationen zu Cybersicherheit; deutschsprachige Bevölkerung im Alter ab 16 Jahren, die in einem Privathaushalt lebt und über einen Internetzugang verfügt (n=3.060); Deutschland; 2026; in Prozent

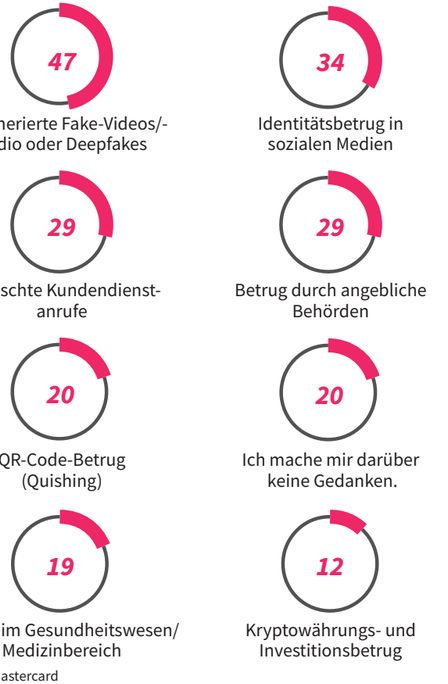
Informieren Sie sich gezielt über Cybersicherheit?

14	40	19	24	2
ja, regelmäßig	ja, hin und wieder	ja, aber nur im Problemfall	nein, eigentlich nie	weiß nicht/ keine Angabe

Quelle: BSI

Beunruhigt

Betrugsmaschen, die die Deutschen am meisten beunruhigen; Verbraucherinnen und Verbraucher (n=1.002); Deutschland; 2025; in Prozent

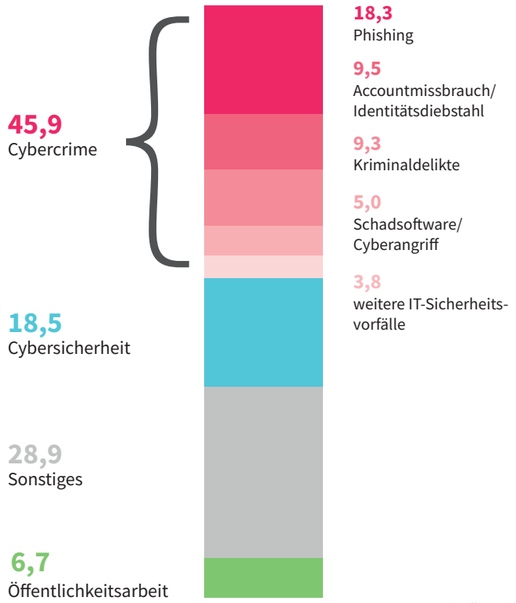


47 KI-generierte Fake-Videos/-Audio oder Deepfakes	34 Identitätsbetrug in sozialen Medien
29 gefälschte Kundendienstanrufe	29 Betrug durch angebliche Behörden
20 QR-Code-Betrug (Quishing)	20 Ich mache mir darüber keine Gedanken.
19 Betrug im Gesundheitswesen/ Medizinbereich	12 Kryptowährungs- und Investitionsbetrug

Quelle: Mastercard

Nachgefragt

Anfragen an das Servicecenter des BSI nach Thema; knapp 10.500 Anfragen von Verbraucherinnen und Verbrauchern zum Thema Cybersicherheit; Deutschland; 2025; in Prozent



45,9 Cybercrime	18,3	Phishing
	9,5	Accountmissbrauch/ Identitätsdiebstahl
	9,3	Kriminaldelikte
	5,0	Schadsoftware/ Cyberangriff
	3,8	weitere IT-Sicherheitsvorfälle
18,5 Cybersicherheit		
28,9 Sonstiges		
6,7 Öffentlichkeitsarbeit		

Quelle: BSI

Verunsichert

Verunsicherungsgefühl im Internet; Internetnutzerinnen und -nutzer ab 16 Jahren (n=1.000); Deutschland; 2025; in Prozent

Dabei fühlen sich Nutzerinnen und Nutzer am unsichersten:

Öffnen von Anhängen in E-Mails	41,0
Austausch vertraulicher Inhalte via Webseiten oder Apps	30,6
Bankgeschäfte im Internet	27,4
Dating-Anwendungen	27,3
soziale Netzwerke	26,7

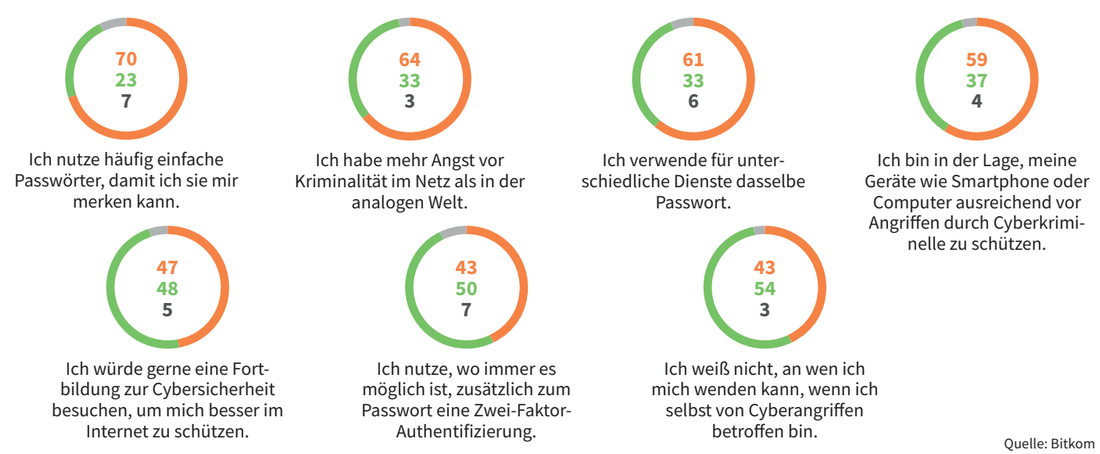
Dabei fühlen sich Nutzerinnen und Nutzer am wenigsten unsicher:

Onlineeinkauf/Reisebuchungen	12,2
Streamen von Filmen/Sendungen/Musik	9,8
Recherchieren in Suchmaschinen und Nachschlagewerken	9,0
Nutzung von (Weiter-) Bildungsangeboten (z. B. Webinare)	8,3

Quelle: DsiN

Überschätzt

Einstellungen und Verhaltensweisen im Umgang mit Cyberkriminalität; Internetnutzerinnen und -nutzer ab 16 Jahren (n=1.115); Deutschland; 2025; in Prozent

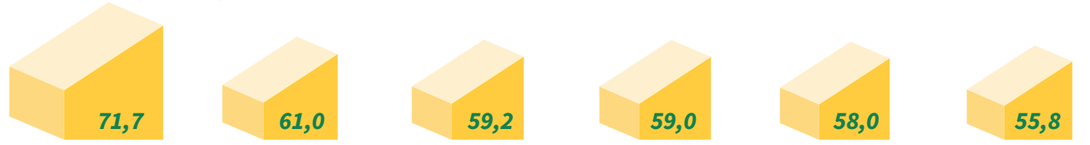


70 / 23 / 7 Ich nutze häufig einfache Passwörter, damit ich sie mir merken kann.	64 / 33 / 3 Ich habe mehr Angst vor Kriminalität im Netz als in der analogen Welt.	61 / 33 / 6 Ich verwende für unterschiedliche Dienste dasselbe Passwort.	59 / 37 / 4 Ich bin in der Lage, meine Geräte wie Smartphone oder Computer ausreichend vor Angriffen durch Cyberkriminelle zu schützen.
47 / 48 / 5 Ich würde gerne eine Fortbildung zur Cybersicherheit besuchen, um mich besser im Internet zu schützen.	43 / 50 / 7 Ich nutze, wo immer es möglich ist, zusätzlich zum Passwort eine Zwei-Faktor-Authentifizierung.	43 / 54 / 3 Ich weiß nicht, an wen ich mich wenden kann, wenn ich selbst von Cyberangriffen betroffen bin.	

Quelle: Bitkom

Gewünscht

Bevorzugte Formen der Informationsvermittlung zu digitaler Sicherheit; Internetnutzerinnen und -nutzer ab 16 Jahren (n=1.000); Deutschland; 2025; in Prozent *



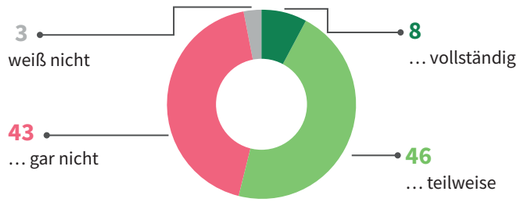
71,7	61,0	59,2	59,0	58,0	55,8
Der bewusste Umgang mit dem Internet sollte bereits in der Schule mehr vermittelt werden.	Anbieter von Diensten und Programmen müssten mehr über Risiken aufklären.	Ich wünsche mir im Internet mehr Informationen zu möglichen Risiken.	Risiken müssten in der öffentlichen Diskussion stärker aufgegriffen werden.	Es sollte Ansprechpartner geben, die ich zu Risiken persönlich fragen kann.	Ich möchte außerhalb des Internets (z. B. Fernsehen, Radio, Zeitung) über Risiken aufgeklärt werden.

*Mehrfachnennung möglich. Quelle: DsiN

Weggeklickt

Umgang mit Datenschutzerklärungen; Wohnbevölkerung ab 18 Jahren (n=2.234); Deutschland; 2026; in Prozent

Ich lese Datenschutzerklärungen in der Regel …



Quelle: eco – Verband der Internetwirtschaft e. V.

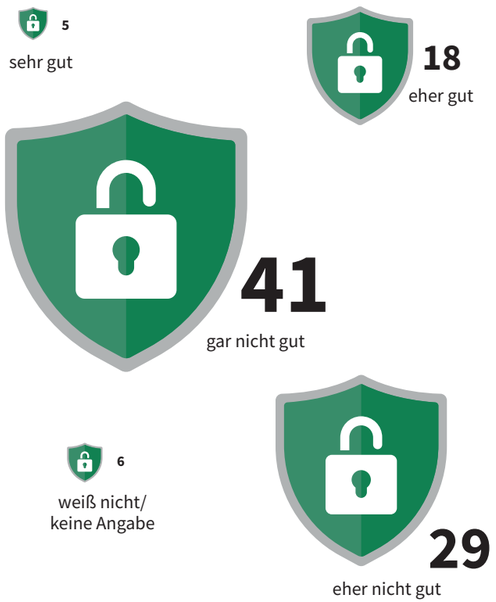
Aus welchen Gründen lesen Sie Datenschutzerklärungen nicht immer vollständig?

Sie sind mir zu lang.	66
Ich gehe davon aus, ohnehin zustimmen zu müssen, um den Dienst nutzen zu können.	55
Sie sind mir zu kompliziert oder schwer verständlich.	34
Ich habe dafür im Alltag keine Zeit.	26
Ich vertraue dem Anbieter.	12
Das Thema Datenschutz interessiert mich nicht besonders.	9
Sonstiges/weiß nicht	4

Überfordert

Einschätzung der Fähigkeit Deutschlands, Cyberangriffe abzuwehren; Personen ab 16 Jahren (n=1.115); Deutschland; 2025; in Prozent

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



Quelle: Bitkom

Gefordert

Einstellungen zu staatlichen Maßnahmen bei Cyberangriffen; Personen in Privathaushalten ab 16 Jahren, die das Internet privat nutzen (n=8.058); Deutschland; 2025; in Prozent

stimme voll und ganz/eher zu

81
Ich erwarte, dass der Staat genauso stark gegen Cyberkriminalität vorgeht wie gegen analoge.

70
Ich finde, der Staat muss viel mehr Geld in moderne und effektive Cybersicherheitsmaßnahmen investieren.

25
Ich vertraue in die Fähigkeit staatlicher Institutionen, sich gegen Cyberangriffe zu schützen.

Quelle: Initiative D21

Geglaubt

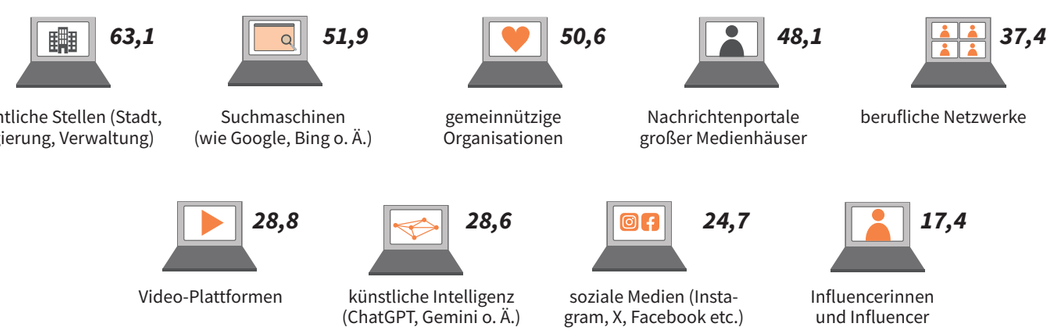
Vertrauen der Bevölkerung in Informationsquellen bei hybriden Angriffen; Personen ab 16 Jahren (n=1.263); Deutschland; 2026; in Prozent

öffentlich-rechtlicher Rundfunk	82
private TV- und Radio-Sender	77
Parteien, Behörden, Ministerien und Organisationen wie Gewerkschaften	64
überregionale Print- und Onlinemedien	63
internationale Print- und Onlinemedien	63
regionale und lokale Print- und Onlinemedien	57
Youtube-Kanäle	42
soziale Netzwerke	41

Quelle: Bitkom

Vertraut

Vertrauen in verschiedene digitale Informationsquellen; Internetnutzerinnen und -nutzer ab 16 Jahren (n=1.000); Deutschland; 2025; in Prozent



Quelle: DsiN

Vernetzt

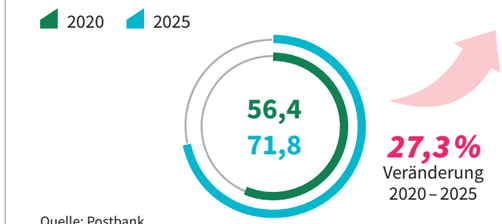
Nutzung von Onlinekommunikationsdiensten; Internetnutzerinnen und -nutzer zwischen 18 und 64 Jahren (n=35.991); Deutschland; 2025; in Prozent*

WhatsApp	77
Facebook Messenger	25
FaceTime	16
Telegram	15
Discord	13
Microsoft Teams	10
iMessage	7
Signal	7
Google Chat/Google Meet	6
Skype	6
Zoom	6
Viber	2
Threema	2
Kik	2
WeChat	2
KakaoTalk	2
Slack	1
andere	2
Ich nutze keine Messenger- oder Videocall-Dienste.	9

*Mehrfachnennung möglich. Quelle: Statista Global Consumer Survey

Verbunden

Durchschnittliche Internetnutzung pro Woche; Internetnutzerinnen und -nutzer ab 16 Jahren (n=3.050); Deutschland; in Stunden



Quelle: Postbank

Konsumiert

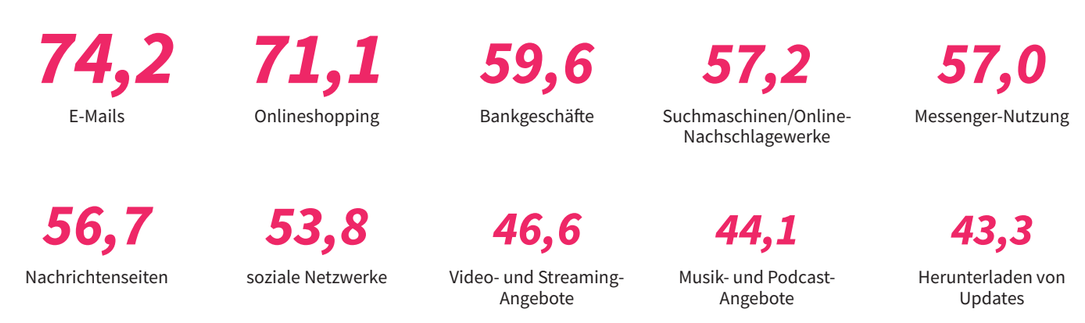
Genutzte Informationskanäle für sicherheitspolitische Themen; Bürgerinnen und Bürger ab 18 Jahren (n=5.000); Deutschland; 2026; in Prozent

Zeitungen/Nachrichtenportale (online/print)	65,9
öffentlich-rechtliches Fernsehen (z. B. ARD)	59,5
private Fernsehsender	20,3
Podcasts/YouTube-Kanäle	16,6
soziale Netzwerke (z. B. Instagram, Tiktok)	11,2
Familie, Freundinnen und Freunde, Bekannte	10,0
Messenger-Dienste (z. B. Telegram, WhatsApp)	5,2
andere	11,8
keinen/weiß nicht	3,8

Quelle: Deloitte

Genutzt

Top-10-Internetnutzungszwecke; Internetnutzerinnen und -nutzer ab 16 Jahren (n=1.000); Deutschland; 2025; in Prozent



Quelle: DsiN

Bezahlen

Nutzung digitaler Wallets; Personen in Privathaushalten ab 16 Jahren, die das Internet privat nutzen (Deutschland: n=8.058, Österreich: n=1.000, Schweiz: n=1.000); DACH; 2025; in Prozent

43 Österreich

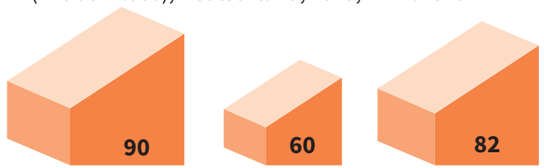
44 Deutschland

52 Schweiz

Quelle: Initiative D21

Melden

Betroffenheit und Anzeige von Zahlungsbetrug; Onlineverbraucherinnen und -verbraucher ab 18 Jahren (n=über 1.000); Deutschland; 2025; in Prozent



90 würden einen Zahlungsbetrug anzeigen (bisher nicht Betroffene)

60 haben bei einem Zahlungsbetrug tatsächlich Anzeige erstattet (Betroffene)

82 waren einer Zahl von Betrugsversuchen über das Internet ausgesetzt

Quelle: Visa

Einkaufen

Einschätzung zu Gefahren beim Einkaufen im Internet; Internetnutzerinnen und -nutzer ab 16 Jahren (n=1.000); Deutschland; in Prozent

nutzen sichere Zahlungssysteme

kaufen online ein

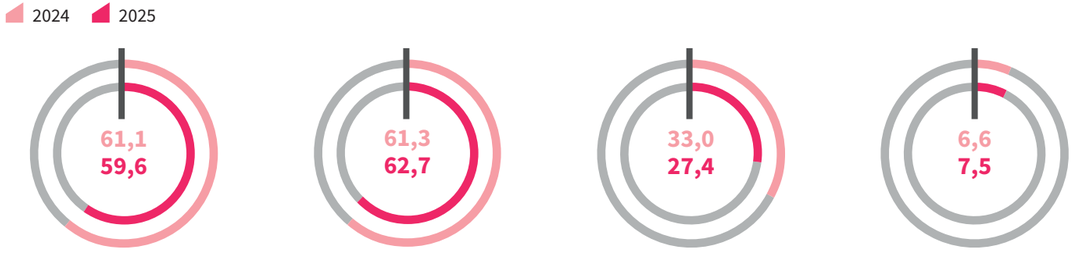
sind in den vergangenen zwölf Monaten Opfer eines Betrugs beim Onlineshopping geworden

empfinden Einkaufen im Internet als gefährlich

Quelle: DsiN

Absichern

Einschätzung zu Gefahren beim Onlinebanking; Internetnutzerinnen und -nutzer ab 16 Jahren (n=1.000); Deutschland; in Prozent



nutzen Onlinebanking

achten auf verschlüsselte Datenverbindung beim Austausch sensibler Daten

empfinden Bankgeschäfte im Netz als gefährlich

stellen fest, dass ihre Zugangsdaten zum Onlinebanking ausgespäht wurden

Quelle: DsiN

Ausprobieren

Nutzung von generativer KI; Bürgerinnen und Bürger (n=1.005); Deutschland; 2025; in Prozent*

Haben Sie eine Anwendung von generativer künstlicher Intelligenz schon einmal ausprobiert bzw. genutzt?

61 ja, für private Zwecke

32 ja, für berufliche Zwecke (inkl. Schule/Ausbildung)

34 nein

*Mehrfachnennung möglich. Quelle: TÜV-Verband

Nachdenken

Sorgen bezüglich KI; Jugendliche (13 bis 17 Jahre) und Erwachsene (18 bis 64 Jahre) (n=1.000); Deutschland; 2025; „sehr besorgt“ und „eher besorgt“ in Prozent*

Wie besorgt sind Sie über die potenziellen Probleme, die durch den Einsatz generativer KI entstehen könnten?

sexueller oder Onlinemissbrauch	74
Betrugsmaschen mit KI erstellen	74
KI-Halluzinationen	67
Deepfakes	67
Datenschutz	63
Verstärkung von Vorurteilen	61
Aufbau von Beziehungen durch KI	57

*Mehrfachnennung möglich. Quelle: Microsoft

Erkennen

Erfahrungen mit KI; Bürgerinnen und Bürger (n=1.005); Deutschland; 2025; in Prozent*

Welche Erfahrungen haben Sie im Zusammenhang mit dem Einsatz von KI bereits gemacht?

51 Ich bin online auf manipulierte KI-Videos gestoßen, die reale Personen zeigten (sog. Deepfakes).

31 Ich habe KI-generierte Phishing-Mails mit täuschend echt formulierten Texten erhalten.

26 Ich wurde von automatisierten KI-Stimmen angerufen, die menschliche Gespräche nachahmten.

22 Ich habe den Eindruck, dass ich durch den häufigen Einsatz von KI-Anwendungen weniger selbst nachdenke oder hinterfrage.

*Mehrfachnennung möglich. Quelle: TÜV-Verband

Einsetzen

Nutzungszwecke von generativer KI; Bürgerinnen und Bürger, die generative KI nutzen (n=655); Deutschland; 2025; in Prozent

Für welche Zwecke nutzen Sie generative KI?

72 Ich suche mit der KI nach Informationen.

43 Ich lasse die KI Texte erstellen oder verbessern.

38 Ich nutze KI zur Ideenfindung oder -entwicklung.

34 Ich lasse die KI Übersetzungen anfertigen.

16 Ich erstelle mit der KI Bilder, Videos oder Audiodateien.

11 Ich lasse von der KI Berechnungen durchführen.

8 Ich erstelle mit der KI Websites oder Code.

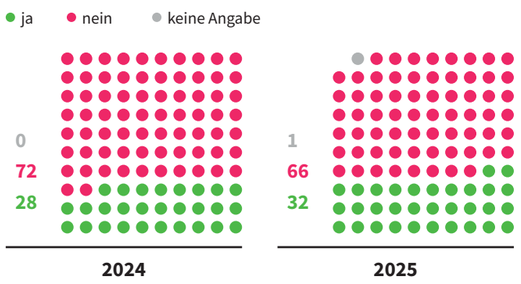
8 Ich lasse von der KI Datensätze analysieren.

Quelle: TÜV-Verband

Wahrnehmen

Bekanntheit der europäischen KI-Verordnung (EU AI Act); Bürgerinnen und Bürger (n=1.005); Deutschland; 2025; in Prozent

Haben Sie schon einmal vom EU AI Act gehört?



Quelle: TÜV-Verband

Fordern

Zustimmung zu Aussagen zu digitaler Souveränität; Personen ab 16 Jahren (n=1.156); Deutschland; 2025; in Prozent

97 Die Bundesregierung muss mehr tun, um ganz grundsätzlich die deutsche Unabhängigkeit zu sichern.

96 Ich habe Sorge, dass Deutschland bei der Digitalisierung zu abhängig vom Ausland ist.

69 Ich wünsche mir mehr digitale Geräte, Technologien und Dienstleistungen aus Deutschland und Europa.

65 Ich halte die digitale Abhängigkeit für ähnlich bedrohlich wie militärische Gefahren.

63 Ich habe bereits von „digitaler Souveränität“ gehört und weiß genau oder ungefähr, was das bedeutet.

15 Ich kenne zwar den Begriff, weiß aber nicht, was sich dahinter verbirgt.

18 Ich habe davon noch nicht gehört.

Quelle: Bitkom

Bewerten

Bewertung der digitalen Verwaltung; Personen in Privathaushalten ab 16 Jahren, die das Internet privat nutzen (Deutschland: n=8.058, Österreich: n=1.000, Schweiz: n=1.000); DACH; 2025; in Prozent

Wenn Sie an Ämter und Behörden denken: Haben Sie das Gefühl, dass Ihre Erwartungen an eine moderne digitale Verwaltung aktuell erfüllt werden?

Ja:

15 Deutschland

36 Österreich

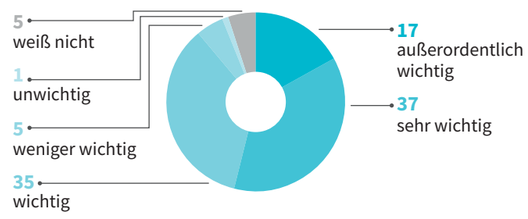
46 Schweiz

Quelle: Initiative D21

Gewichten

Relevanz von digitaler Souveränität; Mobilfunknutzerinnen und -nutzer zwischen 18 und 75 Jahren (n=1.000); Deutschland; 2026; in Prozent

Wie wichtig ist Ihnen persönlich digitale Souveränität?



Wählen Sie digitale Dienste z. B. E-Mail, Apps, Cloud-Speicher nach der Herkunft des Anbieters aus?

Ich bevorzuge überwiegend Daten-Services von europäischen Anbietern und habe das bewusst so umgesetzt. **33**
Ich plane konkret, innerhalb der nächsten zwölf Monate stärker auf deutsche oder europäische Anbieter umzustellen. **14**
Ich beabsichtige es grundsätzlich, habe aber noch keinen festen Zeitplan. **18**
Der Standort des Anbieters ist für mich zweitrangig – andere Kriterien wie Preis oder Leistung sind wichtiger. **14**
Ich bevorzuge auch Anbieter außerhalb der EU, wenn die Leistung oder der Preis besser sind. **4**
weiß nicht/keine Angabe **17**

Quelle: O2 Telefónica

Erleben

Die häufigsten und seltensten IT-Sicherheitsvorfälle; Internetnutzerinnen und -nutzer über 16 Jahren (n=1.000); Deutschland; 2025; in Prozent

am häufigsten

31,6 Phishing-Versuch

33,5 Phishing-Versuch per SMS/ Messenger (Smishing)

27,8 Erhalt infizierter E-Mails/ Anhänge/Weblinks

15,2 Scam (Betrug durch Kontaktaufnahme mit falschen Versprechungen)

15,5 Betrug bei Onlineeinkäufen/ bei Onlinebuchungen

am seltensten

7,5 Ausspähen von Zugangsdaten für das Onlinebanking

6,2 manipulierte oder gefälschte Audioaufnahmen*

4,9 unbefugter Zugriff auf privates WLAN-Netzwerk*

5,9 Manipulation von Hausvernetzung im Smart Home

7,7 Betrug mit virtuellen Währungen

7,5 unbefugte Ortung mobiler Geräte

*2024. Quelle: DsiN

Entdecken und schützen

Zahl der über Shodan via Internet auffindbaren „verletzlichen“ Systeme; Deutschland und weltweit; 2026

auffindbare verletzliche Systeme nach Betriebssystem

weltweit / Deutschland

Windows 11	Windows 10	Windows 8.1
232.516	902.029	274.183
22.546	65.822	8.343

Windows 8	Windows 7	Windows XP
12.050	92.260	1.936
453	1.636	13

Quelle: Shodan

auffindbare Systeme mit „default password“

34.821 weltweit

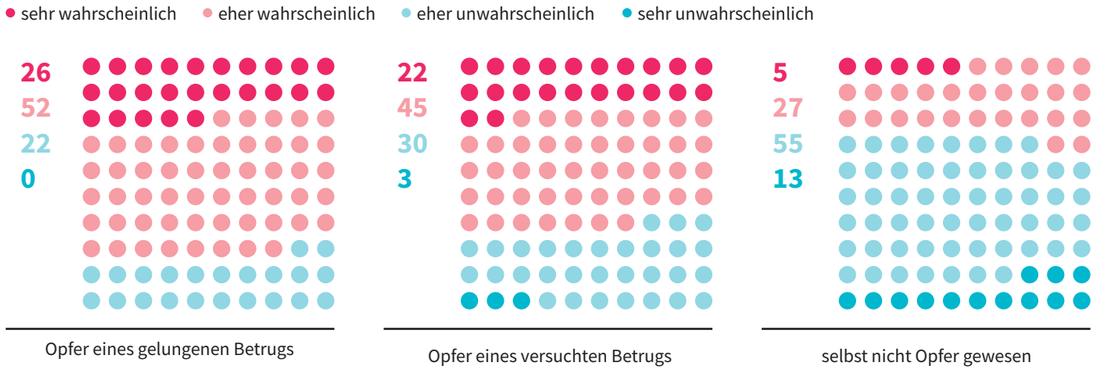
1.463 Deutschland

Shodan.io ist eine Suchmaschine, die ungeschützte Anwendungen oder Systeme mit nur geringen Sicherheitsvorkehrungen im Internet findet. Geräte, Anwendungen und Systeme, die dort gefunden werden, bieten leichte Ziele für Cyberkriminelle.

Wer rechnet mit einem Angriff?

Risiko eines Onlineangriffs nach Betroffenheit; Personen ab 18 Jahren (Opfer eines Onlinebetrugs: n=237, davon gelungen: n=70, versucht: n=167; keine Opfer eines Onlinebetrugs: n=820); Deutschland; 2025; in Prozent

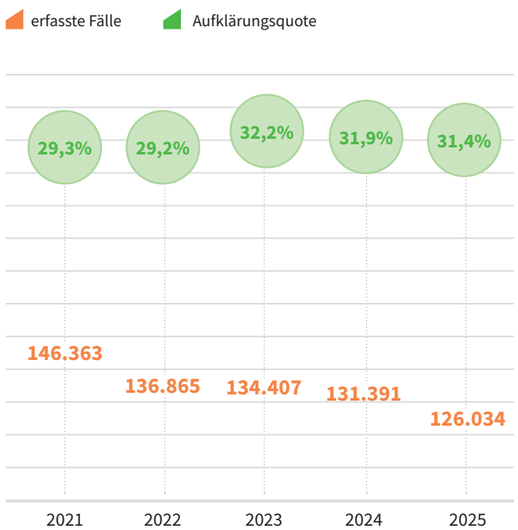
Für wie wahrscheinlich halten Sie es, selbst Opfer eines Onlineangriffs, also eines Betrugs oder Betrugsversuchs über das Internet, zu werden?



Quelle: Bundesverband deutscher Banken

Wie viele Täter werden gefasst?

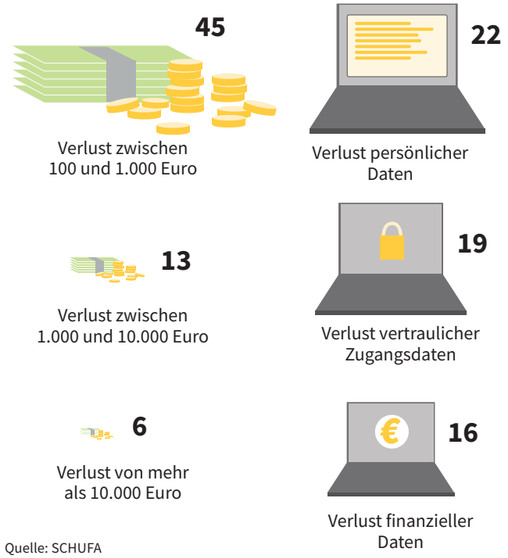
Kriminalitätsstatistik zu Cybercrime: erfasste Fälle und Aufklärungsquote; Deutschland; in Prozent



Quelle: BKA

Was kostet ein Betrug?

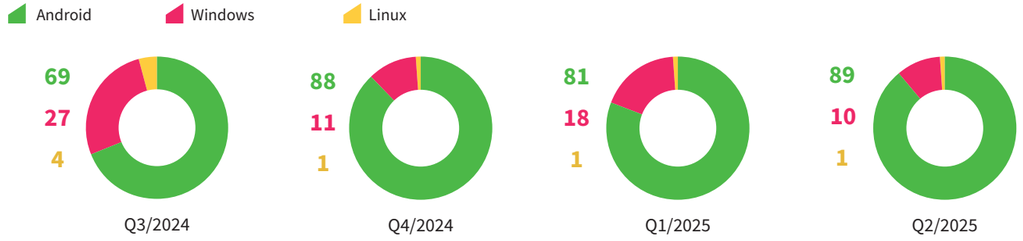
Folgen und Schadensausmaß von Internetbetrug; Verbraucherinnen und Verbraucher (n=1.000); Deutschland; 2026; in Prozent



Quelle: SCHUFA

Welche Systeme setzen sich durch?

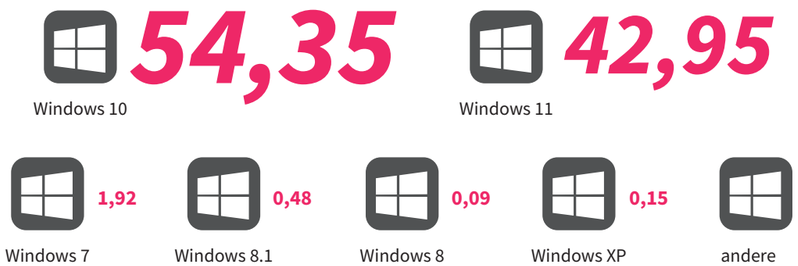
Infizierte Systeme nach Betriebssystem; Deutschland; in Prozent



Quelle: BSI

Windows-Versionen

Marktanteile der verschiedenen Windows-Versionen; Deutschland; 2025; in Prozent



Support-Ende:

Windows XP: 08. April 2014;
Windows Vista*: 10. April 2012;
Windows 7: 14. Januar 2020;
Windows 8: 12. Januar 2016;
Windows 8.1: 10. Januar 2023

Damit gibt es (unter der Annahme, dass die „anderen Versionen" als veraltete Windows-Versionen zu zählen sind) für rund 3,6 Prozent der Computer keinen Support und somit auch keine Sicherheitsupdates mehr.

*Gelistet unter „andere". Quelle: Statcounter

macOS-Versionen

Marktanteile der verschiedenen macOS-Versionen; Deutschland; 2025; in Prozent

macOS Catalina	63,19
macOS Sequoia	12,90
macOS Sonoma	7,59
macOS Ventura	2,38
macOS Cheetah	2,13
macOS Monterey	1,72
andere	10,10

Quelle: Statcounter

Android-Versionen

Marktanteile der verschiedenen Android-Versionen (Mobile & Tablet); Deutschland; 2026; in Prozent

16.0	28,24
14.0	12,19
13.0	12,67
12.0	6,90
11.0	5,31
10.0	4,17
15.0	13,60
8.0 Oreo	4,67
6.0 Marshmallow	4,28
andere	7,97

Quelle: Statcounter

iOS-Versionen

Marktanteile der verschiedenen iOS-Versionen (Mobile & Tablet); Deutschland; 2026; in Prozent

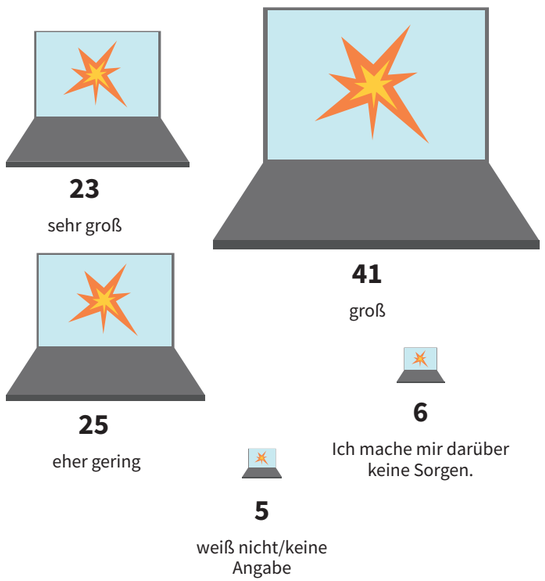
iOS 18.7	30,47
iOS 26.2	21,70
iOS 18.6	18,29
iOS 26.1	7,47
iOS 11.0	5,45
iOS 18.5	4,30
iOS 16.7	1,31
andere	11,03

Quelle: Statcounter

Wie verändert KI das Risiko?

Einschätzung zur Gefahr von Passworthacks durch KI; Internetnutzerinnen und -nutzer ab 18 Jahren (n=1.121); Deutschland; 2025; in Prozent

Wie groß ist Ihre Sorge, dass das Knacken von Passwörtern und Accounts durch KI deutlich einfacher wird und Online-kriminelle so leichter an Ihre persönlichen Daten gelangen?



23
sehr groß

41
groß

25
eher gering

6
Ich mache mir darüber keine Sorgen.

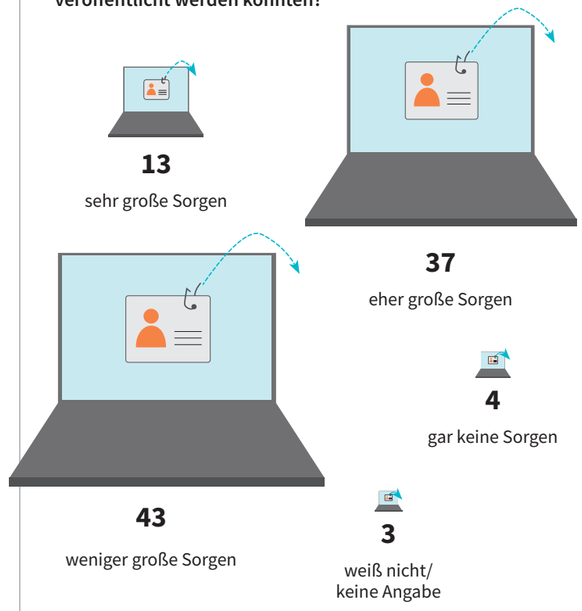
5
weiß nicht/keine Angabe

Quellen: Web.de, GMX

Wie vorsichtig sind wir?

Sorgen über Datenmissbrauch bei der Nutzung von KI-Anwendungen; Bürgerinnen und Bürger, die generative KI nutzen (n=655); Deutschland; 2025; in Prozent

Wie groß ist Ihre Sorge, dass Ihre Eingaben in den KI-Anwendungen gehackt, missbraucht oder ohne Ihr Einverständnis veröffentlicht werden könnten?



13
sehr große Sorgen

37
eher große Sorgen

4
gar keine Sorgen

43
weniger große Sorgen

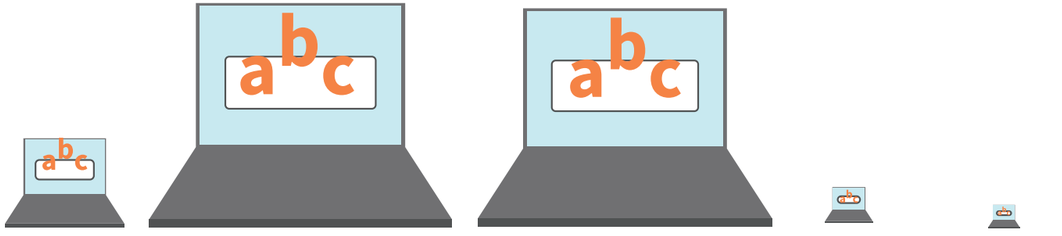
3
weiß nicht/
keine Angabe

Quellen: TÜV-Verband

Wie verwundbar fühlen wir uns?

Sorge vor Passwortdiebstahl und Kontoübernahme; Internetnutzerinnen und -nutzer ab 18 Jahren (n=1.121); Deutschland; 2025; in Prozent

Wie groß ist Ihre Sorge, dass Onlinekriminelle eines Ihrer Passwörter stehlen und in Ihre Onlineaccounts eindringen?



15
groß

38
eher groß

37
gering

6
Ich mache mir darüber keine Sorgen.

4
weiß nicht/
keine Angabe

Quellen: Web.de, GMX

Wie gut schützen wir uns?

Bekannteste und unbekannteste Sicherheitsmaßnahmen; Internetnutzerinnen und -nutzer über 16 Jahren (n=1.000); Deutschland; 2025; in Prozent

am bekanntesten →

98,5 Sicherung von WLAN durch ein starkes Passwort

98,4 Schutz des Geräts mit einer PIN

98,3 regelmäßige Installation von Updates bei Programmen

98,3 Virenschutz-Software

98,2 Verwendung starker Passwörter

98,1 regelmäßige Aktualisierung des Betriebs-systems des Computers

am unbekanntesten →

88,6 Einsatz eigener elektronischer Signaturen

88,1 Überprüfung fremder elektronischer Signaturen

86,7 Plug-ins zur Erhöhung der Daten-sicherheit

86,4 Auslesen der E-Mail-Header

Quelle: DsiN

Wie konsequent handeln wir?

Meistgenutzte und am wenigsten genutzte Sicherheitsmaßnahmen; Internetnutzerinnen und -nutzer über 16 Jahren (n=1.000); Deutschland; 2025; in Prozent

am meisten genutzt →

77,8 Verwendung starker Passwörter

76,7 Sicherung von WLAN durch ein starkes Passwort

76,6 regelmäßige Updates von Apps

75,3 Nutzung sicherer Zahlungs-systeme

75,2 regelmäßiges Update des Betriebs-systems

73,6 Verwendung unterschiedlicher Pass-wörter für unterschiedliche Zwecke

am wenigsten genutzt →

29,7 Auslesen der E-Mail-Header

29,2 Überprüfung fremder elektronischer Signaturen

28,6 Verschlüsselung der Festplatte

22,0 Einsatz eigener elektronischer Signaturen

Quelle: DsiN

Schutz bleibt lückenhaft

Genutzte Maßnahmen für weniger Gefahren im Internet; deutschsprachige Bevölkerung im Alter ab 16 Jahren, die in einem Privathaushalt lebt, über einen Internetzugang verfügt und denen die Schutzmaßnahme bekannt ist (n=3.060); Deutschland; 2026; in Prozent*

- 46 sichere Passwörter
- 40 aktuelles Antivirenprogramm
- 40 Zwei-Faktor-Authentifizierung (2FA)
- 28 aktuelle Firewall
- 26 automatische Installation von verfügbaren Updates
- 24 regelmäßige manuelle Installation von Updates
- 21 regelmäßiges Anlegen von Sicherheitskopien
- 21 passwortloses Anmelden
- 20 Verzicht auf das Anschließen fremder Geräte
- 18 Verzicht auf das Anschließen an fremde Schnittstellen
- 16 Verzicht auf die Nutzung öffentlicher Netzwerke
- 15 Passwortmanager im Browser
- 14 verschlüsselte E-Mail-Kommunikation
- 13 verschlüsselte Kommunikation im Messenger
- 12 Nutzung eines Virtual Private Network (VPN)
- 10 eigenständiger Passwortmanager
- 8 Verzicht auf soziale Netzwerke
- 7 Verzicht auf Onlinebanking
- 3 Verzicht auf Onlineshopping
- 8 Ich nutze keine der Schutzmaßnahmen.

*Mehrfachnennung möglich. Quelle: BSI

Erwartungen sind hoch

Einstellungen zu staatlichen Maßnahmen im Bereich Cybersicherheit; Internetnutzerinnen und -nutzer ab 16 Jahren (n=1.021); Deutschland; 2025; in Prozent

trifft voll und ganz/eher zu | trifft eher nicht/überhaupt nicht zu | weiß nicht/keine Angabe

- 91 / 7 / 2 — Die Polizei muss mehr Präsenz im digitalen Raum zeigen, z. B. aktiv soziale Netzwerke oder Onlineforen nach Straftaten überwachen.
- 81 / 14 / 5 — Für Cyberkriminalität sollte es höhere Strafen geben.
- 76 / 20 / 4 — Die Polizei sollte zusätzliche Befugnisse erhalten, um gegen Cyberkriminalität vorzugehen, z. B. durch das Ausspähen von digitaler Kommunikation.
- 70 / 27 / 3 — Die Regierung sollte mehr Angebote zur Aufklärung und Bildung zum Thema Cyberkriminalität finanziell fördern.
- 5 / 91 / 4 — Das Thema Cyberkriminalität wird in der öffentlichen Debatte übertrieben dargestellt.

Quelle: Bitkom

Sicherheit täuscht

Gründe für Nichtnutzung von Schutzmaßnahmen; deutschsprachige Bevölkerung im Alter ab 16 Jahren, die in einem Privathaushalt lebt, über einen Internetzugang verfügt und nicht alle Schutzmaßnahmen verwendet (n=3.055); Deutschland; 2026; in Prozent*

Was sind die Gründe dafür, dass Sie nicht alle Schutzmaßnahmen nutzen?

- 27 Ich fühle mich sicher.
- 23 Es ist zu kompliziert.
- 23 Ich fühle mich überfordert.
- 20 Ich weiß nicht, was ich tun soll, weil überall etwas anderes empfohlen wird.
- 19 Es ist zu viel Aufwand.
- 14 Ich weiß nicht, wo ich seriöse Empfehlungen bekomme.
- 12 Jemand anderes kümmert sich für mich darum.
- 8 Ich verstehe nicht, wie ich mich schützen kann.
- 7 Es interessiert mich nicht/ ich möchte mich nicht damit beschäftigen.
- 6 Es ist mir nicht wichtig.
- 6 Ich gehe das Risiko ein, betroffen zu werden.
- 7 weiß nicht/ keine Angabe

*Mehrfachnennung möglich. Quelle: BSI

Hilfe kommt zuerst

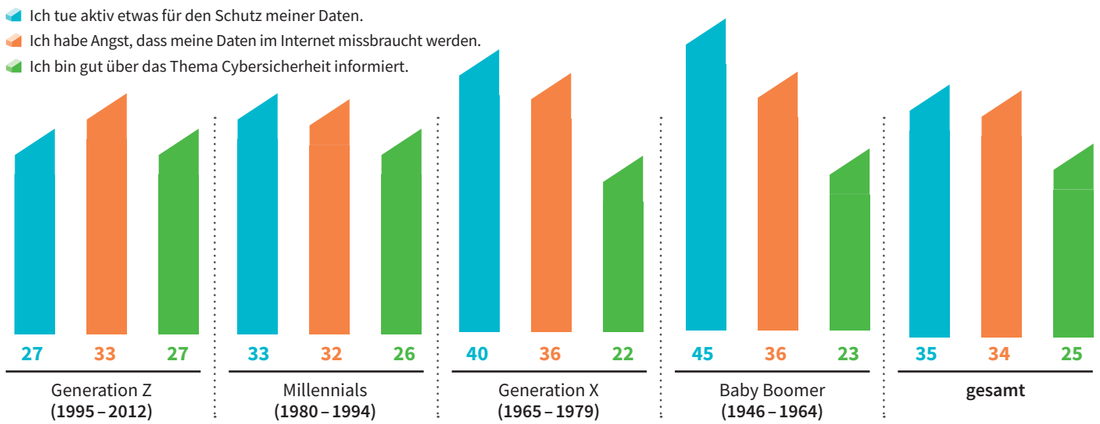
Reaktionen auf Sicherheitsvorfälle; deutschsprachige Bevölkerung im Alter ab 16 Jahren, die in einem Privathaushalt lebt, über einen Internetzugang verfügt und in den letzten zwölf Monaten Opfer von Internetkriminalität geworden ist (n=287); Deutschland; 2026; in Prozent*

- 35 an Betreiber des betroffenen Dienstes gewendet
- 32 Anzeige bei der Polizei erstattet
- 28 Ich habe mir selbst geholfen.
- 26 Ich habe im Internet recherchiert, was zu tun ist, und bin den Handlungsempfehlungen gefolgt.
- 19 Account gelöscht/ Anwendung deinstalliert
- 17 Familie/Freunde/ Bekannte um Hilfe gebeten
- 11 an Netzwerkbetreiber/Provider/ Internetanbieter gewendet
- 12 Internetbeschwerdestelle kontaktiert
- 8 an eine Beratungs-/ Verbraucher-/ Dienststelle gewendet
- 5 Sonstiges
- 2 weiß nicht/keine Angabe

*Mehrfachnennung möglich. Quelle: BSI

Wir lernen

Einstellungen zum Datenschutz im Internet nach Generationen; Personen zwischen 18 und 64 Jahren (n=35.978); Deutschland; 2025; in Prozent*



*Mehrfachnennung möglich. Quelle: Statista Consumer Insights

Wir suchen

Genutzte Informationskanäle zum Thema Cybersicherheit; deutschsprachige Bevölkerung im Alter ab 16 Jahren, die in einem Privathaushalt lebt, über einen Internetzugang verfügt, das Internet nutzt und gezielt nach Informationen sucht (n=2.277); Deutschland; 2026; in Prozent*

Über welche Kanäle suchen Sie Informationen über Cybersicherheit?

*Mehrfachnennung möglich. Quelle: BSI

Wir schützen

Passwortsicherheit und Passwortverhalten; Wohnbevölkerung ab 18 Jahren (n=2.134); Deutschland; 2026; in Prozent

Einschätzung der eigenen Passwortsicherheit als eher oder sehr hoch	74
Einschätzung der eigenen Passwörter als unsicher	19
Nutzung von Zwei-Faktor-Authentifizierung	39
Nutzung passwortloser Verfahren wie Passkeys oder biometrischer Log-ins	32
Nutzung von Passwortmanagern	24
Nutzerinnen und Nutzer, die ihre Passwörter teilweise noch aufschreiben	37
Nutzerinnen und Nutzer, die ihre Passwörter teilweise im Browser speichern	21
Nutzung identischer Passwörter für mehrere Onlinedienste	18

Quelle: eco – Verband der Internetwirtschaft e. V.

Wir sichern ab

Wunsch nach Multi-Faktor-Authentifizierung (MFA) bei verschiedenen Onlinediensten; Internetnutzerinnen und -nutzer ab 18 Jahren (n=1.121); Deutschland; 2025; in Prozent

Bei welchen Diensten würden Sie sich wünschen, dass eine zusätzliche Sicherheitsmaßnahme wie ein Code per SMS, eine Authentifizierungs-App o. Ä. angeboten oder verpflichtend wird?

E-Mail-Postfach	30
Onlineshops	28
Onlinespeicher/Cloud	21
Social Media	20
Messenger-Dienste	14
Streaming-Dienste	13
KI-Dienste	10
Dating-Apps	8
Ich wünsche mir keine weiteren MFA-Angebote.	27
weiß nicht/keine Angabe	17

Quellen: Web.de; GMX

Wir wechseln

Bekanntheit und Nutzung von Passkey; Internetnutzerinnen und -nutzer ab 18 Jahren (n=1.121); Deutschland; 2025; in Prozent

Haben Sie schon einmal von der Log-in-Technologie „Passkey“ gehört, bei der kein Passwort mehr nötig ist?

Ja, ich habe davon gehört und Passkeys bereits verwendet.	32
Ja, ich habe davon gehört, aber noch nicht genutzt.	38
Nein, ich habe noch nie davon gehört.	27
weiß nicht/keine Angabe	4

Wären Sie bereit, klassische Passwörter durch Passkeys zu ersetzen, wenn viele Anbieter diese Möglichkeit anbieten würden?

Ja, aber nur für besonders wichtige Accounts.	34
Nein, ich bleibe lieber beim Passwort.	29
Ja, ich würde Passkeys gerne für alle Accounts nutzen.	27
weiß nicht/keine Angabe	10

Quellen: Web.de; GMX

Wir teilen

Eingabe persönlicher oder vertraulicher Daten in generative KI nach Alter; Bürgerinnen und Bürger, die generative KI nutzen (n=655); 2025; in Prozent

Quellen: TÜV-Verband

GLOSSAR

Advanced Persistent Threats (APT): Im Unterschied zu rein wirtschaftlich motivierten Tätern zeichnen sich APT durch eine auf Langfristigkeit ausgelegte Strategie aus, bei der es nicht auf kurzfristige Gewinne ankommt. Dabei führen sie sehr zielgerichtete Angriffe aus, die sich zuweilen auch nur gegen eine Einzelperson richten. Sie nutzen dafür fortgeschrittene (advanced) Angriffstechniken, um eine dauerhafte (persistent) Präsenz im Netzwerk einzurichten.

Backdoor (Deutsch: Hintertür): Eine Backdoor ist ein üblicherweise durch Viren, Würmer oder Trojaner installiertes Programm, das Dritten unbefugten Zugang zum Computer verschafft, jedoch versteckt und unter Umgehung der üblichen Sicherheitseinrichtungen.

Brute-Force-Angriff: Wählen Nutzerinnen und Nutzer ein schwaches Passwort und ist der Benutzername bekannt, kann sich eine Angreifergruppe unter Umständen auch durch wiederholtes automatisiertes Ausprobieren von Passwörtern (Brute-Force-Angriff) Zugang zu einem Benutzerkonto verschaffen. Mittels Brute-Force-Techniken können Cyberkriminelle auch versuchen, kryptografisch geschützte Daten, z. B. eine verschlüsselte Passwortdatei, zu entschlüsseln.

Business E-Mail Compromise (BEC): Bei einem BEC versuchen Cyberkriminelle, andere Personen durch betrügerische E-Mails dazu zu bringen, Geld zu überweisen oder vertrauliche Unternehmensdaten preiszugeben. Die Akteure geben sich als vertrauenswürdige Personen aus und verlangen die Bezahlung einer gefälschten Rechnung oder die Herausgabe vertraulicher Daten, die sie für weitere betrügerische Aktivitäten missbrauchen können.

Computervirus: Ein Computervirus ist eine nicht selbstständige Programmroutine, die sich selbst reproduziert und dadurch von den Anwenderinnen und Anwendern nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt. Der Begriff hat sich als Sammelbezeichnung für alle Arten von Schadsoftware durchgesetzt – auch für Schadprogramme, die in ihrer eigentlichen Definition keine Viren mehr sind.

Cookie: Zeichenfolge, die mit einer Webseite vom Server geladen werden kann und bei einer erneuten Anfrage an den Server mitgesendet wird. Sinn ist unter anderem, Besucherinnen und Besucher wiederzuerkennen, sodass es beispielsweise nicht erforderlich ist, Nutzerdaten neu einzugeben.

Cyberabwehr: Cyberabwehr umfasst alle Maßnahmen mit dem Ziel der Wahrung oder Erhöhung der Cybersicherheit.

Cyberangriff: Ein Cyberangriff ist eine Einwirkung auf ein oder mehrere andere informationstechnische Systeme im oder durch den Cyberraum, die zum Ziel hat, deren IT-Sicherheit durch informationstechnische Mittel zu beeinträchtigen.

Cybermobbing: Cybermobbing steht für verschiedene Formen der Diffamierung, Belästigung, Bedrängung und Nötigung anderer Menschen oder Firmen über das Internet. Das Opfer wird durch aggressive oder beleidigende Texte, kompromittierende Fotos oder Videos angegriffen oder der Lächerlichkeit ausgesetzt.

Cyberstalking: Cyberstalking (auch Digital Stalking oder Onlinestalking) bezeichnet das Nachstellen, Verfolgen und auch Überwachen einer Person mit digitalen Hilfsmitteln.

Data Breach: Ein Data Breach ist das Ergebnis eines Angriffs von außen, in dessen Zuge ein Angreifer entweder Einsicht in vertrauliche Daten genommen hat, Daten abgegriffen oder diese für Dritte zugänglich gemacht hat. Ein Data Breach liegt auch dann vor, wenn zunächst keine Daten veröffentlicht wurden. Sobald die Vertraulichkeit von Daten nicht mehr gegeben ist, sprechen wir von einem Data Breach.

Data Leak: Data Leaks sind nicht autorisierte Übertragungen von Informationen innerhalb eines Unternehmens nach außen. Dabei wird nicht zwischen der physischen (USB-Stick) und der digitalen (E-Mail) Übertragung unterschieden. Das kann beispielsweise eine Kollegin oder ein Kollege sein, die oder der Kundendaten an andere Unternehmen oder Hackerinnen und Hacker verkauft. Hauptmerkmal eines Data Leaks ist, dass es von innen nach außen passiert. Deshalb ist diese Art des Datendiebstahls für Unternehmen schwer zu verhindern.

Defacement / Defacing: Ein Defacement bezeichnet die – meist plakative – Veränderung von Webseiteninhalten durch Dritte.

Denial-of-Service-Angriffe (DoS / DDoS): DoS-Angriffe richten sich gegen die Verfügbarkeit von Diensten, Webseiten, einzelnen Systemen oder ganzen Netzen. Wird ein solcher Angriff mittels mehrerer Systeme parallel ausgeführt, spricht man von einem verteilten DoS- oder DDoS-Angriff (DDoS = Distributed Denial of Service). DDoS-Angriffe erfolgen häufig durch eine sehr große Zahl von Computern oder Servern. Ziel eines DDoS-Angriff ist es, ein System oder einen Dienst gezielt durch automatisiert durchgeführte massenhafte Anfragen zu überlasten und so zum Zusammenbruch zu bringen.

DevSecOps: Das Kunstwort setzt sich aus den Einzelbegriffen Entwicklung (Development), Sicherheit (Security) und Betrieb (Operations) zusammen. Es handelt sich um einen ganzheitlichen Ansatz, der die Sicherheit in allen Phasen des Lebenszyklus einer Software berücksichtigt und in die Prozesse integriert.

Distributed-Ledger-Technologie (DLT): Bei DLT handelt es sich um ein digitales System zur Aufzeichnung von Transaktionen, bei dem die Transaktionen und ihre Details an mehreren Stellen gleichzeitig aufgezeichnet werden. Im Gegensatz zu herkömmlichen Datenbanken gibt es bei einem Distributed Ledger (verteiltes Hauptbuch oder Kassenbuch) keine zentrale Datenhaltung oder Verwaltungsfunktion. Blockchain ist der bekannteste Anwendungsfall für DLT.

Doxing: Doxing oder Doxxing („Dox" als Abkürzung für „Documents") bezeichnet das internetbasierte Zusammentragen und Veröffentlichen von personenbezogenen Daten an einem zentralen Ort wie einer Datenbank. Hierzu gehören Kontaktdaten und -adressen, Informationen zu Kontakten, Beziehungen oder Gruppenzugehörigkeit, aber auch freizügige Fotos oder intime Aussagen. Doxing kommt oft auch als Druckmittel zum Einsatz, um Personen zu einer bestimmten Handlung zu zwingen (z. B. Drohung mit der Veröffentlichung anzüglicher Bilder, falls bestimmte Daten nicht übergeben oder Zahlungen nicht geleistet werden). Insofern ist das Doxing auch den Erpressungstechniken zuzurechnen.

Ende-zu-Ende-Verschlüsselung (E2EE): E2EE ist eine durchgängige Verschlüsselung zwischen Absenderinnen und Absendern und Empfängerinnen und Empfängern. Den Begriff trifft man vor allem bei der E-Mail-Kommunikation an. Um Ende-zu-Ende-Verschlüsselung verwenden zu können, benötigen beide Parteien entsprechende Verschlüsselungssoftware und müssen den jeweils öffentlichen Schlüssel des Kommunikationspartners besitzen. Die bekanntesten Verfahren sind S/MIME und PGP. Auch viele Messenger-Plattformen (z. B. Signal) nutzen E2EE.

Endpoint Security: Endpoint Security schützt die verschiedenen Endgeräte in einem Netzwerk vor diversen Bedrohungen. Technische und organisatorische Maßnahmen verhindern den unbefugten Zugriff auf Geräte oder die Ausführung schädlicher Software. Der Endpunktschutz stellt sicher, dass die Endgeräte das gewünschte Sicherheitsniveau erreichen.

Exploit: Als Exploit bezeichnet man eine Methode oder einen Programmcode, mit dem über eine Schwachstelle in Hardware- oder Softwarekomponenten nicht vorgesehene Befehle oder Funktionen ausgeführt werden können. Je nach Art der Schwachstelle kann mithilfe eines Exploits z. B. ein Programm zum Absturz gebracht oder ein beliebiger Programmcode ausgeführt werden.

Firewall: Die Firewall besteht aus Hard- und Software, die den Datenfluss zwischen dem internen Netzwerk und dem externen Netzwerk kontrolliert. Alle Daten, die das Netz verlassen, können ebenso überprüft werden wie die, die hineinwollen.

Hack-and-Leak-Angriffe: Bei Hack-and-Leak-Operationen versuchen Bedrohungsakteure mittels cybergestützter Angriffstechniken, in private oder berufliche Computersysteme vorzudringen („Hack"), um diskreditierendes oder belastendes Material über das Opfer zu erlangen. Dieses wird anschließend im Original oder in verfälschender Form beispielsweise in Onlineforen oder über Social-Media-Kanäle veröffentlicht („Leak").

Hacker: Im Kontext von IT-Sicherheit bezeichnet der Begriff Hacker Computernutzerinnen und -nutzer mit überdurchschnittlichem Fachwissen rund um das Verändern von Software sowie den Aufbau, die Struktur und Funktionsweise von Computernetzwerken. Es gelingt ihnen oft, Sicherheitslücken aufzuspüren und sie helfen dabei, diese zu schließen. Man spricht hier vom „White Hat Hacker". Im Unterschied dazu nutzen „Black Hat Hacker" ihr Wissen dazu, um illegalen Zugriff auf fremde Systeme zu erlangen und dort eventuell Schaden anzurichten.

Identity and Access Management (IAM): Unter IAM versteht man in der IT alle Aufgaben rund um die Verwaltung von digitalen Identitäten (Identity) und den damit verknüpften Zugriffsrechten (Access). IT-Berechtigungen legen fest, welche Dateien ein Benutzer öffnen kann, welche Applikationen er verwenden kann und welche Bereiche des Netzwerks ihm zugänglich sind.

Information Stealer: Ein Info Stealer (Information Stealer) ist ein Schadprogramm, das darauf spezialisiert ist, bestimmte Arten von persönlichen Daten, beispielsweise Log-in-Daten, zu erkennen, zu sammeln und an eine fremde Quelle zu senden. Dies geschieht in der Regel unbemerkt und über einen langen Zeitraum.

Intrusion Detection & Prevention System (IDS / IPS): Ein IDS ist ein System, das ein Netzwerk oder eine Netzwerkkomponente überwacht und verdächtige Aktivitäten wie Angriffe oder schadhafte Datenübertragung anhand von Mustern und Heuristik erkennen kann. Über die reine Erkennung hinaus kann ein Intrusion Prevention System (IPS) auch aktiv abwehrende Maßnahmen einleiten.

Keylogger: Als Keylogger wird Hard- oder Software zum Mitschneiden von Tastatureingaben bezeichnet. Sie zeichnen alle Tastatureingaben auf, um sie möglichst unbemerkt an Angreiferinnen und Angreifer zu übermitteln. Diese können dann aus diesen Informationen für sie wichtige Daten wie etwa Anmeldeinformationen oder Kreditkartennummern filtern.

Malware: Ähnlich wie „Virus" ist Malware ein Sammelbegriff für alle Arten von Schadsoftware. Das Kunstwort leitet sich aus „malicious" und „Software" ab und bezeichnet die Gesamtheit aller Programme, die mit dem Ziel entwickelt wurden, Schaden anzurichten.

Managed Detection & Response (MDR) Services: Bei MDR lagern Unternehmen ihre IT-Sicherheit in Bezug auf Erkennung und Reaktion auf Bedrohungen an Dienstleister aus. Je nach MDR-Angebot wird die Technologie lokal beim Kunden installiert und bietet zusätzliche externe und automatisierte Dienste über Software an.

Multi-Faktor-Authentifizierung (MFA): Bei der MFA werden zwei oder mehr unabhängige Berechtigungsnachweise kombiniert: etwas, das die Nutzerinnen und Nutzer wissen (z. B. ein Kennwort), was sie besitzen (z. B. ein Sicherheitstoken) oder was sie sind (z. B. durch die Verwendung biometrischer Verifizierungsverfahren).

Network Access Control: Die Netzwerkzugangskontrolle ist eine Methode, mit der die Sicherheit eines Netzwerks verbessert werden kann. Man schränkt dabei die Verfügbarkeit der Netzwerkressourcen auf entsprechende Endgeräte ein, die definierte Sicherheitsrichtlinien erfüllen.

Paketfilter- / Proxy-Firewall: Eine Proxy-Firewall (auch Application Firewall oder Gateway Firewall) ist ein Security-System für das Netzwerk. Es schützt die Ressourcen im Netzwerk, indem Kommunikation auf der Anwendungsschicht gefiltert wird.

Patch (Deutsch: Flicken): Kleines Programm, das Fehler in Anwendungsprogrammen oder Betriebssystemen behebt.

Penetrationstest: Ein Unternehmen kann einen Penetrationstest in Auftrag geben, um Schwachstellen in exponierten oder kritischen Systemen zu finden, die auf den ersten Blick nicht augenfällig sind. Es handelt sich nicht um eine Angriffssimulation, sondern um eine gezielte Suche nach angreifbaren Systemen und Anwendungen. Hierbei kommen sowohl automatisierte als auch manuelle ›

Methoden zum Einsatz. Bei einem Penetrationstest sind die IT-Verantwortlichen in der Regel eingeweiht. Der Test findet innerhalb eines genau definierten Umfangs und Umfelds („Scope“) statt. Die Erkenntnisse aus einem Penetrationstest werden genutzt, um Schwachstellen gezielt zu schließen.

Personal Firewall: Programm, das auf einem Heimrechner installiert wird. Genau wie eine „große“ Hardware-Firewall in einem Unternehmensnetz soll diese den Rechner vor Angriffen aus dem Netzwerk schützen.

Pharming: Wie beim Phishing sind auch beim Pharming meist Zugangsdaten das Ziel eines Angriffs. Der Unterschied zum Phishing besteht darin, dass beim Pharming die Infrastruktur so manipuliert wird, dass das Opfer auch dann auf einer gefälschten Webseite landet, wenn es die korrekte Adresse des Dienstes eingegeben hat. Technisch geschieht das in der Regel durch eine Manipulation der DNS-Einträge in der lokalen Hosts-Datei, an einem Zwischenspeicher oder an der zentralen DNS-Infrastruktur.

Phishing: Das Wort setzt sich aus „Password“ und „Fishing“ zusammen, zu Deutsch „nach Passwörtern angeln“. Beim Phishing wird z. B. mittels gefälschter E-Mails und/oder Webseiten versucht, Zugangsdaten für einen Dienst oder eine Webseite zu erlangen. Wird diese Manipulation vom Opfer nicht erkannt und die Authentizität einer Nachricht oder Webseite nicht hinterfragt, gibt das Opfer seine Zugangsdaten unter Umständen selbst unwissentlich in unberechtigte Hände. Bekannte Beispiele sind Phishing-Angriffe gegen Bankkunden, die in einer E-Mail aufgefordert werden, ihre Zugangsdaten auf der Webseite der Bank einzugeben und validieren zu lassen. Mit dem gleichen Verfahren werden aber auch Nutzerinnen und Nutzer von E-Commerce-Anwendungen angegriffen, z. B. Onlineshops oder Onlinedienstleister.

Ransomware: Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (englisch: „ransom“) wieder freigeben. Es handelt sich dabei um eine digitale Form der Erpressung.

Remote Access Trojaner (RAT): Ein RAT ist ein Fernzugriffs-Trojaner, ein Malware-Programm, das eine Hintertür für die administrative Kontrolle über den Zielcomputer enthält. RATs werden in der Regel unsichtbar mit einem von Benutzerinnen und Benutzern angeforderten Programm – z. B. einem Tool – heruntergeladen oder als E-Mail-Anhang versandt.

Remote Desktop Protocol (RDP): RDP ist ein Netzwerk-Kommunikationsprotokoll, das von Microsoft entwickelt wurde. Es ermöglicht Administratoren, aus der Ferne auf Computer von Benutzern zuzugreifen, um Probleme zu identifizieren und zu lösen. Sicherheitsfachleute raten dringend von der Verwendung zu Wartungszwecken ab – vor allem, wenn Systeme über RDP aus dem öffentlichen Internet erreichbar sind.

Rootkit: Als Rootkit wird eine Sammlung von Softwarewerkzeugen bezeichnet, die die Präsenz schädlicher oder unerwünschter Software auf einem Rechner verschleiert und verdächtige Aktivitäten versteckt. Sie greift tief in das Betriebssystem des betroffenen Rechners ein, verschafft Angreifern erweiterte Rechte und bietet Remote-Zugriffsmöglichkeiten.

Scam (Deutsch: Betrug, Schwindel): Beispiel für eine Scam-Mail ist eine E-Mail, die Empfängerinnen und Empfängern einen Gewinn vorgaukelt, für die Überweisung desselben aber eine Gebühr verlangt. Natürlich existiert der Gewinn nicht wirklich.

Schwachstelle: Eine Schwachstelle oder Sicherheitslücke ist ein sicherheitsrelevanter Fehler in einem IT-System oder einer Anwendung. Ursachen können in der Konzeption, den verwendeten Algorithmen (wie z. B. veraltete und unsichere Verschlüsselungs- oder Hashing-Algorithmen), der Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und eine Institution oder ein System geschädigt wird.

Security Information and Event Management (SIEM): Es handelt sich um ein softwarebasiertes Technologiekonzept, mit dem ein ganzheitlicher Blick auf die IT-Sicherheit möglich wird. SIEM stellt eine Kombination aus Security Information Management (SIM) und Security Event Management (SEM) dar. Durch das Sammeln, Korrelieren und Auswerten von Meldungen, Alarmen und Logfiles verschiedener Geräte, Netzkomponenten, Anwendungen und Security-Systemen in Echtzeit werden Angriffe, außergewöhnliche Muster oder gefährliche Trends sichtbar.

Sinkhole: Als Sinkhole wird ein Computersystem bezeichnet, auf das Anfragen von botnetzinfizierten Systemen umgeleitet werden. Sinkhole-Systeme werden typischerweise von Sicherheitsforschern betrieben, um Botnetzinfektionen aufzuspüren und betroffene Anwender zu informieren.

Skimming (Deutsch: abschöpfen): Skimming bezeichnet das unbemerkte Auslesen von Zahlungskarten durch physische Manipulation von Zahlungsterminals. Mit den ausgelesenen Daten werden Kopien der Karten erstellt. Um auf das Konto des Opfers zugreifen zu können, wird meist auch die Eingabe der zugehörigen PIN aufgezeichnet, mithilfe einer unauffälligen Kamera oder einer manipulierten Tastatur.

Smishing: Smishing ist eine Form des Phishings, bei dem überzeugende Phishing-SMS/-Textnachrichten verwendet werden, um ein potenzielles Opfer dazu zu verleiten, auf einen Link zu klicken und private Informationen zur Angreiferin oder zum Angreifer zu senden oder Malware auf das Handy zu laden.

Social Engineering: Bei Cyberangriffen durch Social Engineering versuchen Kriminelle ihre Opfer dazu zu verleiten, eigenständig Daten preiszugeben, Schutzmaßnahmen zu umgehen oder selbstständig Schadprogramme auf ihren Systemen zu installieren. Sowohl im Bereich der Cyberkriminalität als auch bei der Spionage gehen die Täter geschickt vor, um vermeintliche menschliche Schwächen wie Neugier oder Angst auszunutzen und so Zugriff auf sensible Daten und Informationen zu erhalten.

Software Bundler: Ein Software Bundler ist ein Programm, das unerwünschte Software auf einem PC installiert, und zwar gleichzeitig mit der Software, die man zu installieren versucht.

Spam: Unter Spam versteht man unerwünschte Nachrichten, die massenhaft und ungezielt per E-Mail oder über andere Kommunikationsdienste versendet werden. In der harmlosen Variante enthalten Spam-Nachrichten meist unerwünschte Werbung. Häufig enthält Spam jedoch auch Schadprogramme im Anhang, Links zu verseuchten Webseiten oder wird für Phishing-Angriffe genutzt.

Spear-Phishing: Beim Spear-Phishing wird nicht breitflächig attackiert, sondern nur ein kleiner Empfängerkreis (häufig Führungskräfte oder Wissensträgerinnen und Wissensträger auf Leitungsebene). Voraussetzung für einen erfolgreichen Angriff ist die Einbettung in einen für das Opfer glaubwürdigen Kontext. Spear-Phishing richtet sich in der Regel nicht gegen allgemein nutzbare Dienste wie Onlinebanking, sondern gegen Dienste oder Informationen, die für Angreifergruppen einen besonderen Wert haben.

Spoofing (Deutsch: manipulieren, vortäuschen): Spoofing nennt man in der Informationstechnik verschiedene Täuschungsversuche zur Verschleierung der eigenen Identität und zum Fälschen übertragener Daten. Das Ziel besteht darin, die Integrität und Authentizität der Informationsverarbeitung zu untergraben.

Spyware: Als Spyware werden Programme bezeichnet, die heimlich Informationen über eine Benutzerin oder einen Benutzer bzw. die Nutzung eines Rechners sammeln und an die Person oder Personen, die die Spyware kontrollieren, weiterleiten. Dabei können auch sicherheitsrelevante Informationen wie Passwörter ausgeforscht werden.

SQL Injection: SQL Injection ist eine Sicherheitslücke, bei der die Angreiferin oder der Angreifer eine Anfrage über ein Web-Formular per Structured Query Language (SQL) erweitert, um auf Ressourcen zuzugreifen oder um Daten zu verändern. Eine SQL-Abfrage ist eine Anforderung, die eine Aufgabe in einer Datenbank ausführt. Lücken, die auf SQL Injections basieren, gehören zu den „Klassikern“ unter den Sicherheitslücken, da sie trotz ihres Alters noch immer verbreitet sind.

Telephone-Oriented Attack Delivery (TOAD): TOAD ist eine Spielart des Social Engineering. Hier kontaktieren Kriminelle eine Zielperson und geben dabei vor, im Namen eines Unternehmens oder einer Behörde aufzutreten (z. B. Hausbank, Polizei oder andere Behörden oder Organisationen). Dabei versuchen sie, ihre Opfer zur Preisgabe vertraulicher Informationen zu verleiten. Im Laufe dieses Angriffs versenden die Angreifer dann eine E-Mail, die einen Phishing-Link oder einen manipulierten Anhang enthält. Dadurch, dass die Mail (aus Sicht des Opfers) von einer legitimen Quelle stammt und auch im Gespräch angekündigt wurde, ist die Wahrscheinlichkeit wesentlich höher, dass Daten preisgegeben werden.

Threat Monitoring: Threat Monitoring ist die gezielte und kontinuierliche Analyse und Bewertung von Onlinedaten, um Cyberbedrohungen oder Datenschutzverletzungen zu erkennen. Die Überwachung umfasst in der Regel einen hochgradigen Zugriff auf Netzwerke und Benutzeraktionen, um unerwünschte Eindringlinge leicht zu identifizieren, zu stoppen oder die Bedrohung zu verhindern.

Trojaner: Ein Trojaner ist ein Programm mit einer verdeckten, nicht dokumentierten Funktion oder Wirkung. Es verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogrammes für seine Installation durch Nutzerinnen und Nutzer.

Virenschutzprogramm: Ein Virenschutzprogramm überprüft neue Dateien (z. B. E-Mail-Anhänge) und den gesamten Computer auf Schadsoftware. Dazu vergleicht es in erster Linie die Daten auf dem Rechner mit den „Fingerabdrücken“ bekannter Schadprogramme. Ebenso wie der Begriff „Computervirus“ zur Sammelbezeichnung für alle Arten von Schadprogrammen geworden ist, bezeichnet auch der Begriff „Virenschutzprogramm“ inzwischen alle Schutzfunktionen eines Sicherheitsprogramms – auch wenn sie mit „echten“ Viren nicht mehr viel zu tun haben.

Virensignatur: Eine Virensignatur ist der Fingerabdruck eines Virus. Technisch gesehen ist es eine kurze Byte-Folge, die aus dem betreffenden Virus extrahiert wird und ihn eindeutig identifiziert. Virenschutzprogramme, die mit Signatur-Scanning arbeiten, besitzen eine Datenbank mit den Fingerabdrücken aller bekannten Viren.

Virtual Private Network (VPN): VPNs verschlüsseln die Datenkommunikation zwischen zwei Endpunkten – z. B. zwischen einem Endgerät und einem VPN-Server. Auf diese Weise kann die Kommunikation nicht ohne Weiteres mitgelesen oder verändert werden. Unternehmen nutzen VPNs, um zum Beispiel Mitarbeitenden aus dem Homeoffice den sicheren Zugriff auf Daten und Systeme innerhalb des Firmennetzes zu ermöglichen.

Vishing: Betrugsmasche von Datendieben (Kombination aus der englischen Bezeichnung für Internettelefonie „Voice over Internet Protocol“ (VoIP) und dem Namen der Betrugstechnik „Phishing“). Die geringen Kosten der Internettelefonie werden dazu genutzt, um automatisch eine große Zahl von Telefongesprächen zu führen. In diesen wird beispielsweise behauptet, eine Kreditkarte sei verloren gegangen. Die Opfer sollen dann persönliche Daten wie PIN- oder TAN-Codes über die Telefontastatur eingeben.

Zero-Day-Exploit: Die Ausnutzung einer Schwachstelle, die nur der Entdeckerin oder dem Entdecker bekannt ist, charakterisiert man mit dem Begriff Zero-Day-Exploit. Die Öffentlichkeit und insbesondere die Herstellerin oder der Hersteller des betroffenen Produktes erlangen in der Regel erst dann Kenntnis von der Schwachstelle, wenn Angriffe entdeckt werden, die auf dieser Schwachstelle basieren. Die Bezeichnung „zero day“ leitet sich also davon ab, dass ein entsprechender Exploit bereits vor dem ersten Tag der Kenntnis der Schwachstelle durch die Herstellerin oder den Hersteller existierte – also an einem fiktiven „Tag null“. Die Herstellerin oder der Hersteller haben somit keine Zeit, die Nutzerinnen und Nutzer vor den ersten Angriffen zu schützen.

Zero-Trust-Modell: Das Zero-Trust-Sicherheitskonzept geht davon aus, dass nichts sicher ist – auch nicht hinter der Firmen-Firewall. Deshalb prüft das Modell jede Anforderung so, als käme sie aus einem offen zugänglichen Netzwerk. Bevor der Zugriff gewährt wird, muss eine Anforderung vollständig authentifiziert, autorisiert und verschlüsselt sein.

Quellen: Bundesamt für Sicherheit in der Informationstechnik (BSI), Cloudflare, ComputerWeekly, Dataversity, Externetworks, Gabler Wirtschaftslexikon, G DATA CyberDefense AG, Google, IT-Service.Network, LSI Bayern, Microsoft, NIST, Proofpoint, Rapid7, RiskXchange, Security Insider, TechTarget, Wiener Börse

QUELLENVERZEICHNIS

(ISC)²
1&1 Versatel
Allianz Commercial
ANS
Behörden Spiegel
Bitkom e. V.
bmc helix
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Bundeskriminalamt (BKA)
Bundesverband deutscher Banken
Capgemini Research Institute
CVE
CyberEdge
Deutschland sicher im Netz (DsiN)
Deloitte
Diconium
DIHK
DSGVO-Portal
eco – Verband der Internetwirtschaft e. V.
FBI
Fido Alliance
Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
Gallagher Security
Gartner
Globalstar
GMX
Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GdV)
Hiscox
Horizon3.ai
IBM
IDC
IMF
Initiative D21
ISACA
Lünendonk
Marsh
Mastercard
Microsoft
Mobile World Live
National Cyber Security Organizations
O2 Telefónica
ÖFIT
Omdia
Ponemon Institute
PwC
Sage
SANS Institute
SCHUFA
Schwarz Digits
Shodan.io
Splunk
Statcounter
Statista
TÜV-Verband
Visa
VOICE
Web.de
Wire
World Economic Forum
ZEW

IMPRESSUM

Herausgeber: G DATA CyberDefense AG • G DATA Campus • Königsallee 178 a • 44799 Bochum,
vertreten durch die Vorstände Kai Figge, Frank Heisler, Andreas Lüning
G DATA-Projektteam: Verantwortlich: Vera Haake & Dr. Daniela Kalkühler
Kathrin Beckert-Plewka, Tim Berghoff, Marita Bierhoff, Stefan Karpenstein
Konzept: brand eins Medien AG / Redaktion Corporate Services, statista.com
Chefredaktion: Susanne Risch
Artdirektion & Infografik: Britta Max
Chefin vom Dienst: Michaela Streimelweger
Redaktion: Lydia Gless, Kathrin Lilienthal (freie Mitarbeit),
Daniel Ramm, Margitta Schulze Lohoff
Autoren (fM): Markus Albers, Daniel Erk, Meike Kirsch
Marktforschung, Recherche, Daten und Quellen:
Cindy Karwowski, Robin Rehfeldt, Johannes Seedorff, Linda Lämke, Malte Hildebrandt

brand eins

G DATA CyberDefense

statista