IT- Sicherheitsumfrage

2025

Inhaltsverzeichnis

Einleitung

Die eco Kompetenzgruppe Sicherheit hat mit der IT-Sicherheitsumfrage 2025 eine umfassende Analyse des aktuellen Stands der IT-Sicherheit in Deutschland vorgelegt. Seit über fünfzehn Jahren widmet sich die Kompetenzgruppe der Sicherheit von (IT-) Infrastrukturen in der Internetwirtschaft. Im Fokus stehen dabei unter anderem personelle und organisatorische Aspekte der IT-Sicherheit, der Schutz von IT-Systemen wie Servern und Netzwerken, die Sicherheit mobiler Kommunikationstechnologien (zum Beispiel Tablets, Smartphones und WLAN) sowie Fragestellungen des Sicherheitsmanagements und der Sensibilisierung von Mitarbeitenden.

Die jährlich durchgeführte Umfrage greift neben wiederkehrenden Themen stets auch aktuelle Entwicklungen im Bereich der IT-Sicherheit auf. In der diesjährigen Befragung lag ein besonderer Schwerpunkt auf dem Einfluss des zunehmenden Einsatzes von künstlicher Intelligenz (KI) auf die Sicherheitslage in Unternehmen und Organisationen.

Die Datenerhebung zur IT-Sicherheitsumfrage 2025 fand im Zeitraum von September bis Dezember 2024 statt. Befragt wurden insgesamt 175 Expertinnen und Experten für IT-Sicherheit im Rahmen von Online-Formaten sowie bei Live-Veranstaltungen.

Oliver Dehning
Bereits seit 2014 begleitet Oliver Dehning als Leiter die Kompetenzgruppe Sicherheit des eco – Verbands der Internetwirtschaft e.V.

Allgemeine Lage

Für das Jahr 2025 schätzen 88 Prozent der befragten IT-Expert:innen die allgemeine Bedrohungslage als hoch oder sehr hoch ein. Etwa 11 Prozent gehen von einer gleichbleibenden Lage aus, lediglich 1 Prozent erwartet eine Abnahme der Bedrohung. Im Vergleich zu den Vorjahresergebnissen zeigt sich eine leichte Verschiebung in der Einschätzung: Der Anteil derjenigen, die von einer steigenden Bedrohungslage ausgehen, ist rückläufig, während die Bewertung „gleichbleibend" häufiger genannt wurde.

Allgemeine Bedrohungslage bei der Internetsicherheit

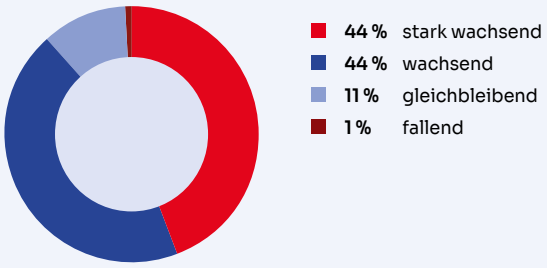


Abbildung 1: Einschätzung der Bedrohungslage 2025

Trotz dieses Rückgangs liegt das wahrgenommene Bedrohungsniveau mit einem Wert, der mit dem des Jahres 2015 vergleichbar ist, weiterhin auf einem sehr hohen Stand, fällt aber erstmals seit Jahren wieder unter die 90-Prozent-Marke. Von einer tatsächlichen Entspannung der IT-Sicherheitslage kann jedoch nicht gesprochen werden.

Einschätzung: Bedrohungslage stark wachsend / wachsend

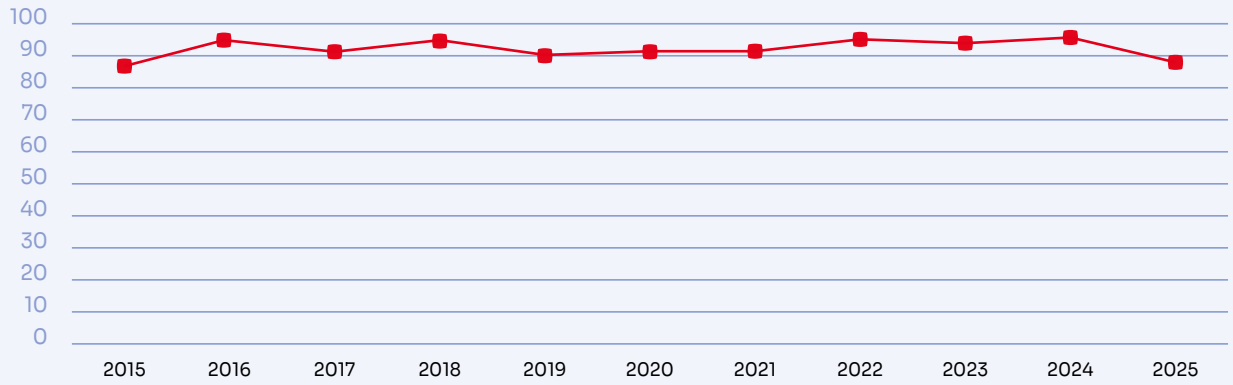


Abbildung 2: Entwicklung der Bedrohungslage 2015-25

Die Absicherung ihres eigenen Unternehmens schätzen die befragten Expert:innen überwiegend als stabil und mindestens ausreichend ein. Nur 12 Prozent der Teilnehmenden bewerten den Schutz ihres Unternehmens als unzureichend. Auffällig ist, dass die Befragten ihr eigenes Unternehmen deutlich besser gegen Cybervorfälle gewappnet sehen als die deutsche Wirtschaft insgesamt.

Mehr als die Hälfte der Befragten stuft die Sicherheitslage im eigenen Unternehmen als „gut" oder „sehr gut" ein. Im Gegensatz dazu bewerten rund drei Viertel der Teilnehmer:innen die deutsche Wirtschaft insgesamt als unzureichend auf IT-Sicherheitsvorfälle vorbereitet.

Absicherung des eigenen Unternehmens

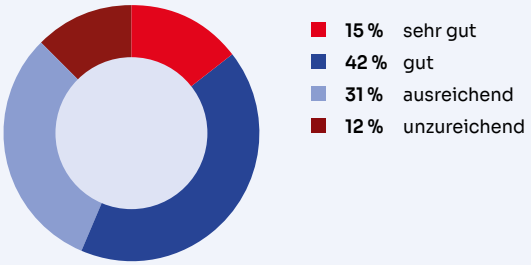


Abbildung 3: Absicherung des eigenen Unternehmens

Absicherung der deutschen Wirtschaft

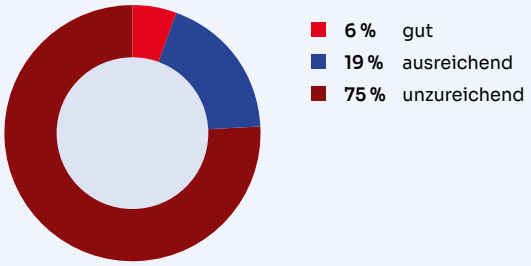
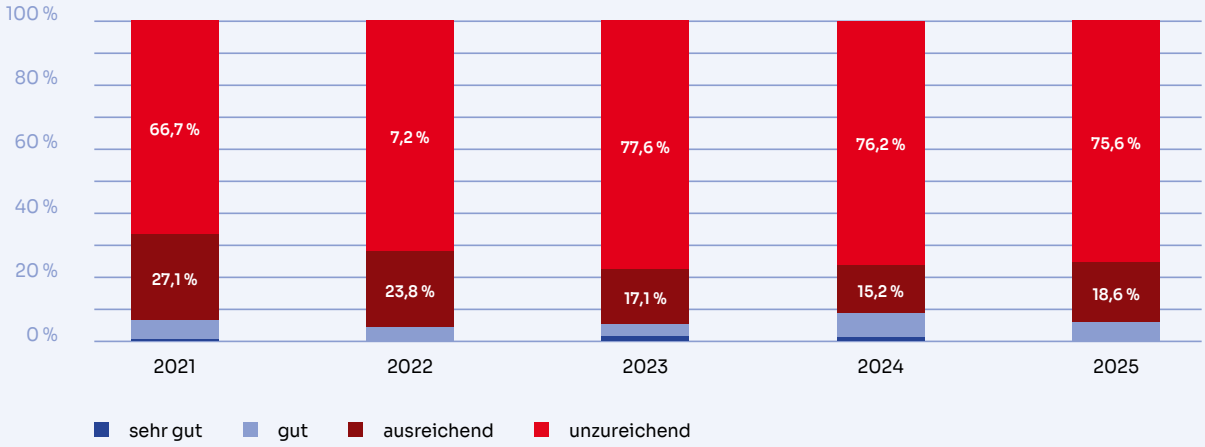


Abbildung 4: Absicherung der deutschen Wirtschaft

Diese Einschätzungen haben sich in den letzten drei Jahren kaum verändert und weisen auf eine anhaltende Diskrepanz zwischen individueller und gesamtwirtschaftlicher Risikowahrnehmung hin.

Absicherung der deutschen Wirtschaft



Absicherung des eigenen Unternehmens

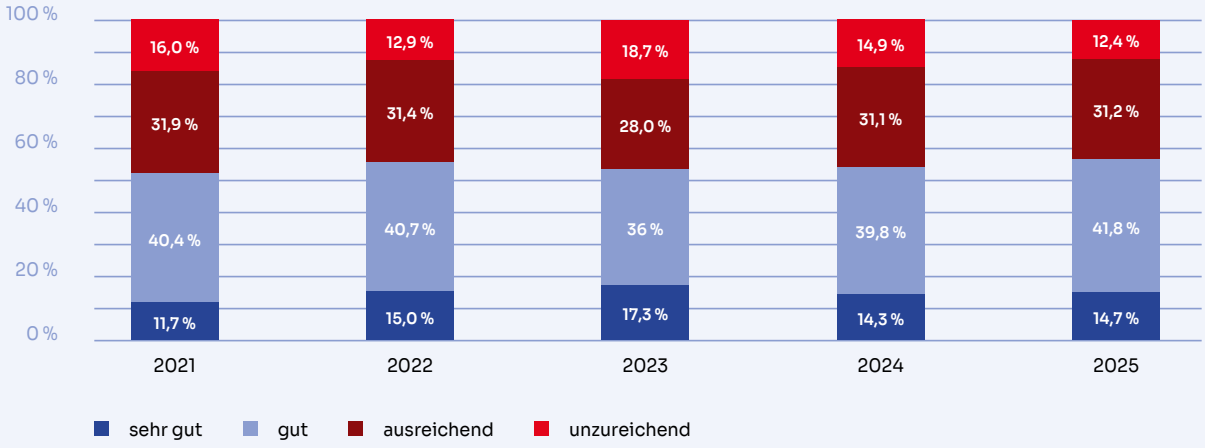


Abbildung 5: Absicherung gegen Cybercrime 2021 bis 2025

Bedrohungslage wird noch immer unterschätzt

„Die Diskrepanz bei der Beurteilung der eigenen Sicherheitslage und der Sicherheitslage in Deutschland allgemein zeigt, wie schwer es selbst Expert:innen fällt, die Bedrohung richtig einzuschätzen“, sagt Oliver Dehning, Leiter der Kompetenzgruppe Sicherheit im eco – Verband der Internetwirtschaft e. V. „Gerade viele Mittelständler stehen im Fokus international agierender Cybercrime-Netzwerke und sind sich dessen nicht bewusst.“

Jedes sechste der befragten Unternehmen war in den vergangenen zwölf Monaten von mindestens einem gravierenden Sicherheitsvorfall betroffen – 5 Prozent sogar von mehreren. Im Vergleich zum Vorjahreszeitraum zeigt sich ein leichter Anstieg: 2024 berichteten noch 7 Prozent von einem und 6 Prozent von mehreren gravierenden Vorfällen. Die aktuelle Entwicklung deutet darauf hin, dass Cyberangriffe zunehmend breiter gestreut erfolgen und damit immer mehr Unternehmen in die Zielscheibe geraten.

Gravierender Sicherheitsvorfall im Unternehmen in den letzten 12 Monaten

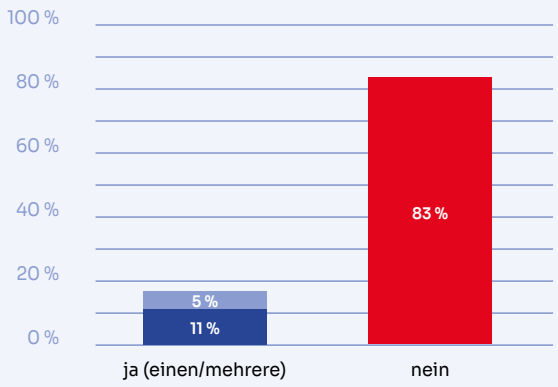


Abbildung 6: Sicherheitsvorfälle im Unternehmen

Ransomware bleibt die häufigste Angriffsform auf Unternehmen, dicht gefolgt von CEO Fraud. Datendiebstahl, Webseiten-Hacking und DDoS-Angriffe liegen im Mittelfeld. Etwa 2 Prozent der befragten Unternehmen entdeckten im vergangenen Jahr einen Fall von Industriespionage.

Art der Sicherheitsvorfälle

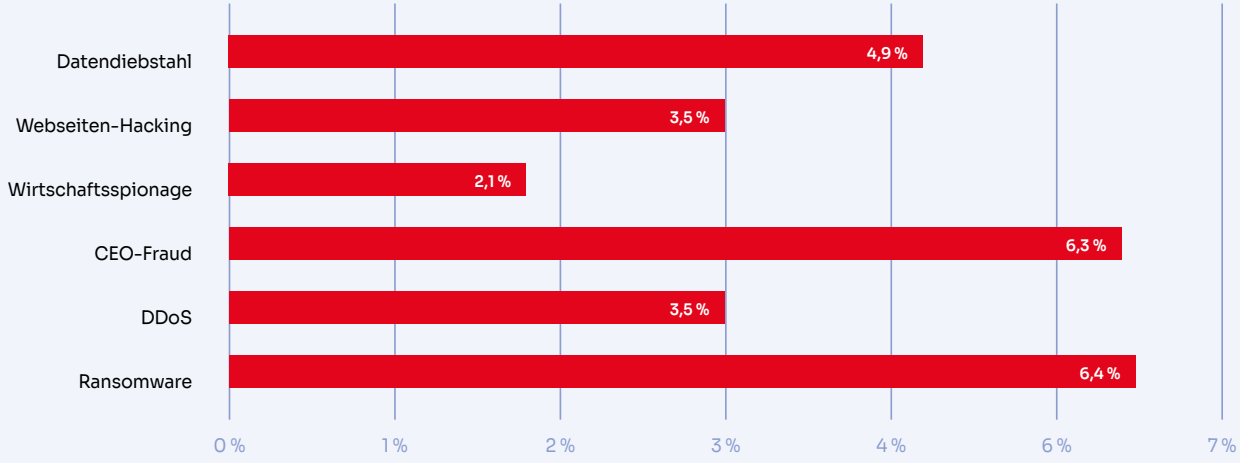


Abbildung 7: Art der Angriffe auf Unternehmen

Im Vergleich zu den Vorjahren ist ein deutlicher Anstieg bei Angriffen durch CEO Fraud zu verzeichnen. Auch bei Ransomware und Industriespionage zeigt sich eine leichte Zunahme. Zwar ist beim Datendiebstahl ein leichter Rückgang erkennbar, doch dieser muss im Kontext der zunehmenden Ransomware-Bedrohung betrachtet werden: Moderne Ransomware-Angriffe beschränken sich längst nicht mehr auf die Verschlüsselung von Systemen und Daten. Immer häufiger werden im Hintergrund zusätzlich sensible Unternehmensdaten kopiert und an die Angreifer übermittelt – mit dem Ziel, durch sogenannte Double-Extortion-Angriffe eine zweite Erpressungswelle auszulösen.

Infobox CEO Fraud

Begriffserklärung

CEO Fraud (auch „Chef-Masche“ oder „Business E-Mail Compromise“) bezeichnet eine Form des Social Engineerings, bei der sich Angreifende als Geschäftsleitung ausgeben, um Mitarbeitende zur Durchführung von betrügerischen Zahlungen zu bewegen.

Typischer Ablauf

- Informationsbeschaffung über Unternehmen (z. B. über Social Media, Website)
- Gefälschte E-Mail oder Anruf im Namen der Geschäftsleitung
- Dringlich formulierte Zahlungsaufforderung unter Hinweis auf Vertraulichkeit
- Überweisung auf ein betrügerisches Konto

Ziele

- Unbemerkte Überweisung großer Geldbeträge
- Zugriff auf vertrauliche Unternehmensdaten

Risikofaktoren

- Fehlende Sicherheitsprozesse bei Zahlungsfreigaben
- Mangelnde Awareness bei Mitarbeitenden
- Öffentliche Informationen über Unternehmensstrukturen

Schutzmaßnahmen

- Schulungen & Awareness: Mitarbeitende für Social Engineering sensibilisieren
- Vier-Augen-Prinzip: Verbindliche Freigabeprozesse etablieren
- Kommunikationsregeln: Keine Zahlungsanweisungen per E-Mail ohne Rückbestätigung
- Technische Maßnahmen: SPF, DKIM, DMARC zur E-Mail-Authentifizierung

CEO Fraud verursacht weltweit jährlich Schäden in Milliardenhöhe. Prävention ist deutlich günstiger als der potenzielle Verlust.

Sicherheitsvorfälle im Jahresvergleich

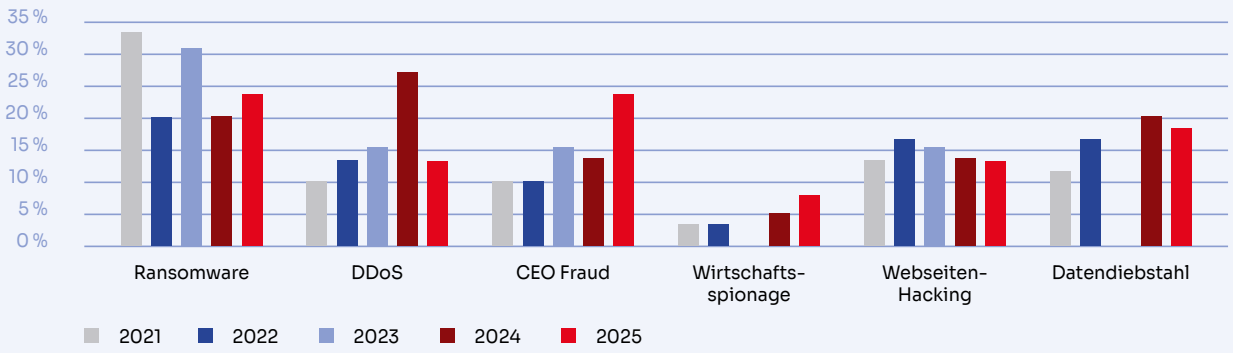


Abbildung 8: Art der Angriffe auf Unternehmen

Die wirtschaftlichen Schäden von Cyberangriffen lassen sich oft nur schwer beziffern. Für viele Unternehmen ist es eine Herausforderung, die tatsächlichen Auswirkungen vollständig zu erfassen. Zu den typischen Kostenfaktoren zählen neben der unmittelbaren Abwehr und forensischen Untersuchung des Vorfalls auch die Wiederherstellung betroffener Systeme, die Schließung der Sicherheitslücke sowie betriebliche Ausfälle und etwaige Verluste durch Datenabfluss. Diese Kosten können sowohl intern anfallen als auch durch externe Dienstleister entstehen – etwa für IT-Forensik, Rechtsberatung oder Kommunikation. In manchen Fällen kommen zusätzlich Bußgelder oder Reputationsverluste hinzu.

Erfreulicherweise gaben drei Viertel der befragten Unternehmen an, durch den Vorfall keinen direkten Schaden erlitten zu haben. Es ist jedoch davon auszugehen, dass zumindest Aufwände für die Bearbeitung und Absicherung nach dem Angriff entstanden sind. Demgegenüber verzeichnete rund jedes vierte Unternehmen einen Schaden, wobei 6 Prozent von erheblichen Auswirkungen berichteten. Im Vorjahr hatten noch 79 Prozent angegeben, keinen Schaden erlitten zu haben – lediglich 4 Prozent meldeten damals gravierende Schäden. Trotz einer grundsätzlich guten Aufstellung vieler Unternehmen im Bereich Cybersicherheit zeigen die steigenden Fallzahlen – sowohl bei allgemeinen Schadensfällen als auch bei besonders gravierenden Vorfällen – eine leichte Verschlechterung der Gesamtsituation.

Schaden auf Grund des Vorfalls

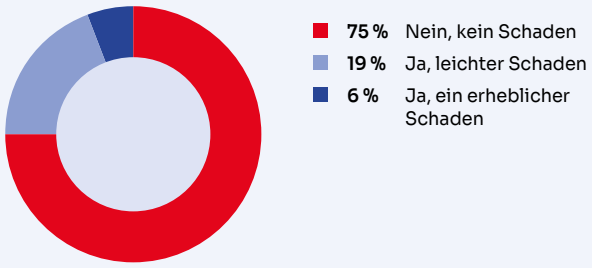
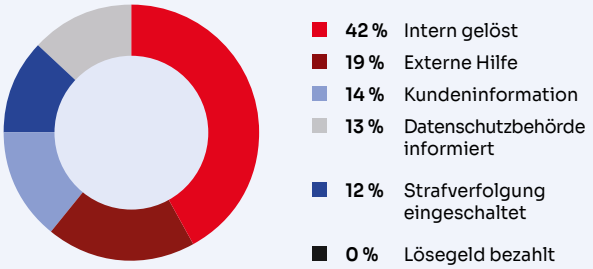


Abbildung 9: wirtschaftliche Auswirkungen eines Angriffs

Knapp die Hälfte der befragten – überwiegend IT-affinen – Unternehmen konnte Cyberangriffe mit internen Ressourcen bewältigen. In etwa jedem fünften Fall wurde externe Unterstützung hinzugezogen. Im Ernstfall ist jedoch entschlossenes und rasches Handeln gefragt: Unternehmen sollten nicht zögern, frühzeitig spezialisierte Hilfe in Anspruch zu nehmen und die zuständigen Behörden einzuschalten, die wichtige Unterstützung leisten können. So wurden im vergangenen Jahr in rund einem Viertel der Fälle Strafverfolgungs- oder Datenschutzbehörden eingebunden. Positiv hervorzuheben ist, dass bei den analysierten Vorfällen kein Lösegeld gezahlt wurde – ganz im Einklang mit den gängigen Empfehlungen von Sicherheitsbehörden und Fachleuten.

Wie hat ihr Unternehmen reagiert?



Hatte eine Cyberversicherung Ihren Schaden aufgefangen?

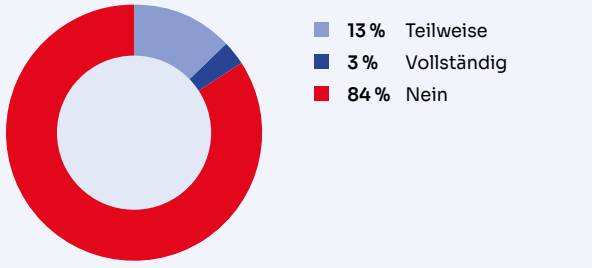


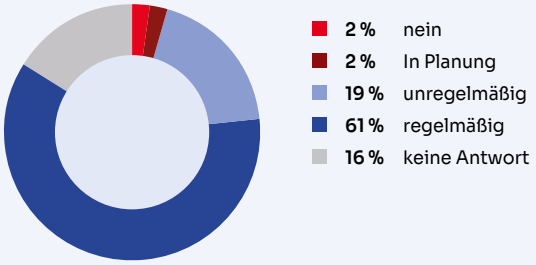
Abbildung 10: Unternehmensreaktionen auf Angriffe

Eine Möglichkeit zur Risikobehandlung besteht im Risikotransfer. Insbesondere finanzielle Risiken lassen sich durch den Abschluss von Cyberversicherungen absichern. In 16 Prozent der Fälle wurde angegeben, dass entstandene Schäden zumindest teilweise von einer Cyberversicherung übernommen wurden. Im Vergleich zu den gemeldeten Schadensfällen zeigt sich jedoch ein differenziertes Bild: Teilweise wurden Schäden, die von der Versicherung abgedeckt waren, im Nachhinein nicht mehr als solche wahrgenommen.

Cyberresilienz/Prävention

Es reicht längst nicht mehr aus, Sicherheitsvorfälle nur reaktiv zu bearbeiten. Eine ganzheitliche Sicherheitsstrategie umfasst auch präventive Maßnahmen. Ein wesentlicher Erfolgsfaktor ist dabei die Einbindung der Mitarbeitenden. Obwohl diese häufig als das „schwächste Glied" bezeichnet werden, kommt ihnen eine entscheidende Rolle im Sicherheitskonzept zu. Rund 60 Prozent der Befragten geben an, regelmäßige Schulungen für Mitarbeitende durchzuführen. Etwa 19 Prozent setzen auf unregelmäßige Schulungen, während lediglich 2 Prozent gänzlich auf diese Maßnahme verzichten.

Schulen und sensibilisieren Sie Ihre Mitarbeiter bezüglich IT-Sicherheit?



Schulen und sensibilisieren Sie Ihre Mitarbeiter bezüglich IT-Sicherheit?

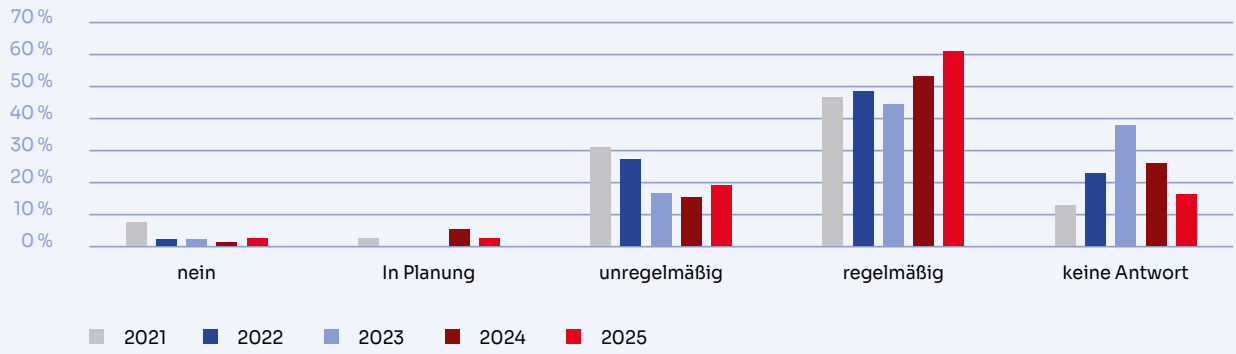


Abbildung 11: Mitarbeiterschulungen

Im Vergleich zum Vorjahr ist sowohl bei den regelmäßigen als auch bei den unregelmäßigen Schulungen eine deutliche Zunahme zu verzeichnen. Es ist anzunehmen, dass viele Unternehmen, die sich im Vorjahr noch in der Planungsphase befanden, diese Maßnahmen inzwischen umgesetzt haben. Besonders erfreulich ist, dass der Anteil der Unternehmen, die auf dieses wichtige Instrument vollständig verzichten, in den vergangenen fünf Jahren auf einen sehr niedrigen einstelligen Prozentsatz gesunken ist.

Neben Schulungen zur Sensibilisierung der Mitarbeitenden zählt auch die Notfallplanung derzeit zu den zentralen Sicherheitsthemen der befragten Unternehmen. Wer im Schadensfall auf vorbereitete Prozesse und relevante Informationen zurückgreifen kann, ist in der Lage, die Auswirkungen eines Vorfalls deutlich zu begrenzen. Notfallpläne stellen dabei einen essenziellen Baustein für mehr Cyberresilienz dar. Rund 60 Prozent der Unternehmen verfügen über definierte interne Prozesse zur Abwehr von Cyberangriffen und über bereits etablierte Notfallpläne – weitere 16 Prozent planen deren Einführung.

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

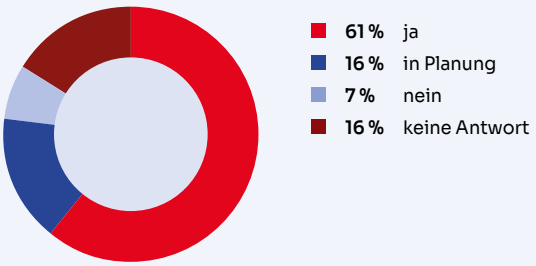


Abbildung 12: Interne Prozesse und Notfallpläne

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

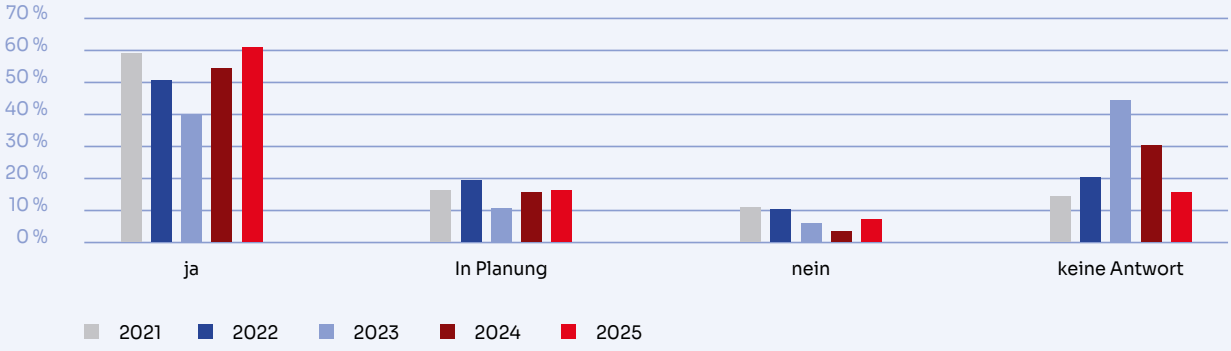


Abbildung 13: Interne Prozesse und Notfallpläne

Im Fünfjahresvergleich zeigt sich im Bereich der Notfallvorsorge ein differenziertes Bild: Nach einem deutlichen Rückgang in den Jahren 2022 und 2023 erreicht die Zahl der Unternehmen, die entsprechende Maßnahmen umsetzen, im Jahr 2025 ihren bisherigen Höchststand. Gleichzeitig geben 2025 erstmals seit Jahren wieder mehr Unternehmen an, keine definierten Prozesse für den Notfall zu haben – auch wenn dieser Anteil mit knapp 7 Prozent weiterhin auf einem sehr niedrigen Niveau liegt. Während im Bereich der Mitarbeitersensibilisierung zahlreiche Produkte und Anbieter verfügbar sind, gestaltet sich die Entwicklung eines individuellen Notfallplans deutlich komplexer.

Um die Widerstandsfähigkeit gegenüber Cyberangriffen zu stärken, sind Investitionen in die IT-Sicherheit unerlässlich. Fast die Hälfte der befragten Unternehmen plant, das Budget für IT-Sicherheit zu erhöhen, bei rund einem Drittel bleibt es unverändert. Nur etwa 2 Prozent gehen von sinkenden Ausgaben aus.

Budget für IT-Sicherheit

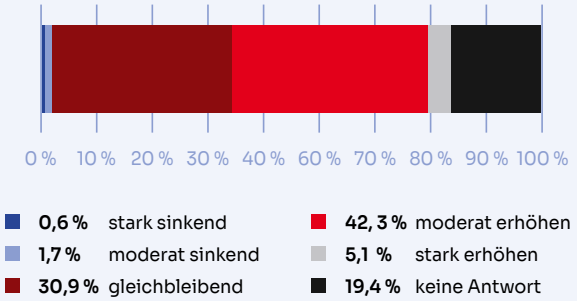


Abbildung 14: IT-Security-Budgets

Im Vergleich zu den Vorjahren zeigt sich ein kontinuierlicher Anstieg des Anteils an Unternehmen, die ihre Sicherheitsbudgets aufstocken. Zwar wird das durch die Corona-Pandemie und den Anstieg mobiler Arbeit bedingte Rekordniveau von 2022 noch nicht wieder erreicht, dennoch ist die anhaltende Zunahme der Investitionen – als Reaktion auf die wachsende Bedrohungslage – ein positives Signal.

Budget für IT-Sicherheit moderat oder stark wachsend im Jahresvergleich

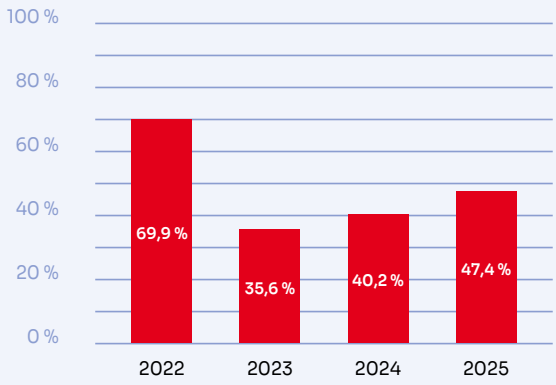


Abbildung 15: Budgets im Jahresvergleich

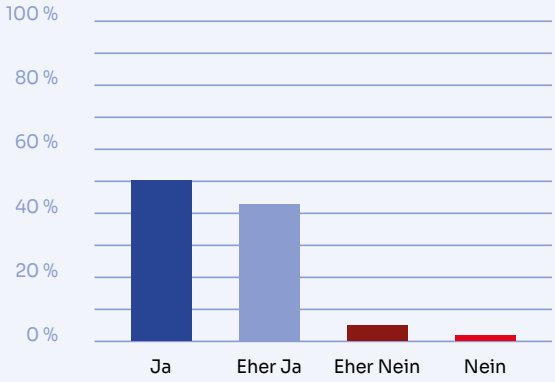
Aktuelle Themen

Die jährlich wiederholte Frage nach den wichtigsten Sicherheitsthemen für das kommende Jahr ermöglicht eine hohe Vergleichbarkeit der Ergebnisse über die Zeit. Gleichzeitig greifen die Studienautor*innen aktuelle Ereignisse auf, um den Fragenkatalog gezielt zu erweitern und so den sich wandelnden politischen und gesellschaftlichen Rahmenbedingungen Rechnung zu tragen.

Einer der derzeit bedeutendsten Trends mit direktem Einfluss auf die IT-Sicherheit ist der rasante Einsatz von Künstlicher Intelligenz (KI). Diese Technologie birgt das Potenzial, sowohl von Angreifenden als auch von Verteidigenden genutzt zu werden. Über 93 Prozent der befragten Unternehmen gehen davon aus, dass KI die Bedrohungslage weiter verschärfen wird. Zugleich setzen bereits rund 40 Prozent der Unternehmen KI aktiv für Aufgaben im Bereich der IT-Sicherheit ein.

Die Chance beim Einsatz von KI liegt vor allem in der schnelleren Erkennung und Reaktion auf Bedrohungen, etwa durch automatisierte Anomalieerkennung oder Unterstützung bei der Auswertung großer Datenmengen. Auf der anderen Seite besteht das Risiko, dass Angreifer KI nutzen, um gezieltere Phishing-Angriffe, Deepfakes oder automatisierte Schwachstellenscans durchzuführen – in einer Geschwindigkeit und Qualität, die klassische Schutzmechanismen herausfordert.

Wird Künstliche Intelligenz die Bedrohungslage verschärfen?



Setzen Sie KI in Ihrem Unternehmen für IT-Sicherheit ein?

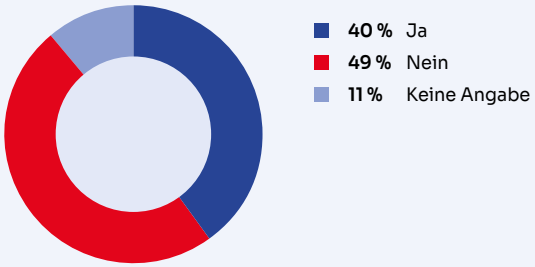


Abbildung 16: Einfluss von Künstlicher Intelligenz auf die Bedrohungslage

Sicherheitsthemen für 2025

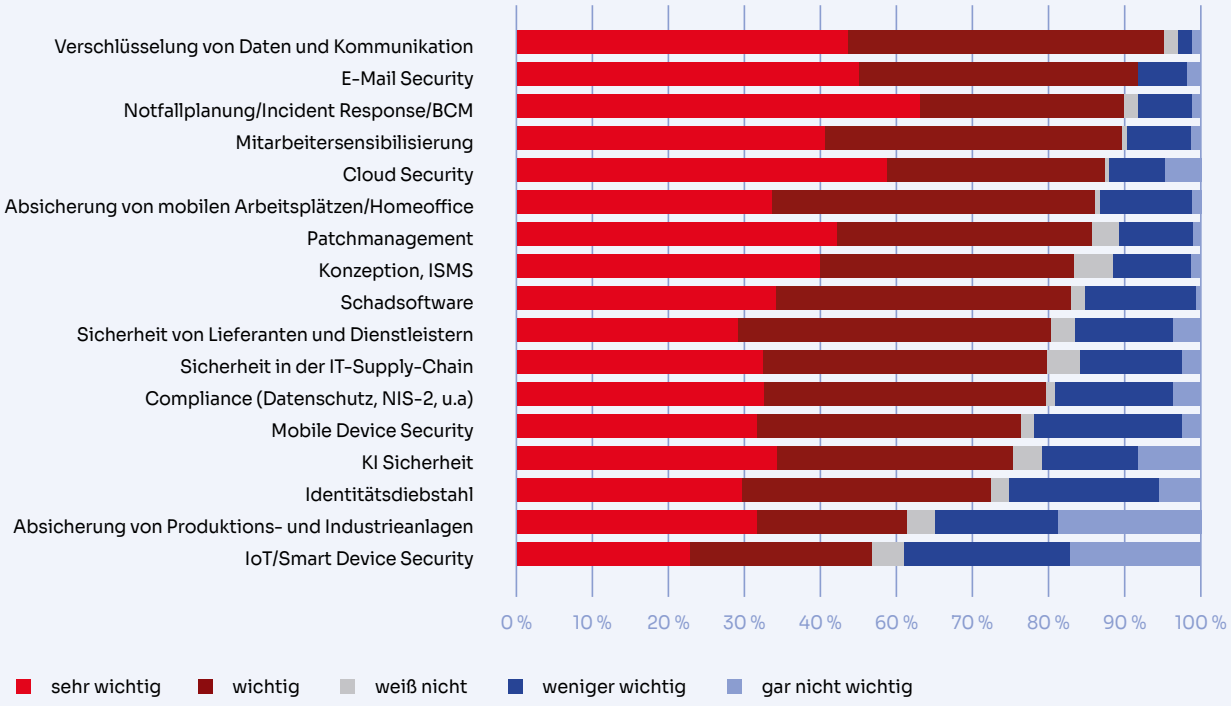


Abbildung 17: Sicherheitsthemen 2025

Verschlüsselung und E-Mail-Sicherheit belegen die Spitzenplätze unter den wichtigsten IT-Sicherheitsthemen der Umfrage 2025. Verschlüsselung steht in den letzten Jahren kontinuierlich im Vordergrund und ist angesichts zunehmender Cloud-Nutzung, internationaler Datenflüsse und wachsender regulatorischer Anforderungen – wie der EU-NIS2-Richtlinie – unverzichtbar.

E-Mail-Sicherheit hat einen großen Sprung nach vorn gemacht. Phishing-Angriffe werden durch den Einsatz von Künstlicher Intelligenz (KI) noch gezielter und glaubwürdiger. Täuschend echte Deepfake-Mails oder automatisiert erstellte Social-Engineering-Kampagnen machen es für Mitarbeitende immer schwieriger, legitime von betrügerischen Nachrichten zu unterscheiden. Dies unterstreicht auch den hohen Anteil von CEO Fraud-Angriffen.

Dicht dahinter folgen Notfallplanung und Mitarbeitersensibilisierung, beides war auch in den Vorjahren auf den vorderen Plätzen zu finden. Notfallpläne gewinnen durch die Zunahme von Ransomware-Angriffen und gezielten Attacken auf kritische Infrastrukturen weiter an Bedeutung. Unternehmen müssen in der Lage sein, auch im Falle einer erfolgreichen Kompromittierung handlungsfähig zu bleiben – nicht zuletzt, um regulatorischen Meldepflichten schnell und strukturiert nachkommen zu können. Mitarbeitersensibilisierung ist angesichts der weiterentwickelten Angriffsmethoden wichtiger denn je. KI-generierte Phishing-Mails, täuschend echte Fake-Identitäten und Social-Engineering-Tricks erfordern ein wachsendes Bewusstsein auf allen Ebenen im Unternehmen – vom Empfang bis zur Führungsetage.

Die Anforderungen an die IT-Sicherheit ändern sich. Was sind aus Ihrer Sicht die stärksten Treiber der Veränderung mit Sicht auf die kommenden 5 Jahre?

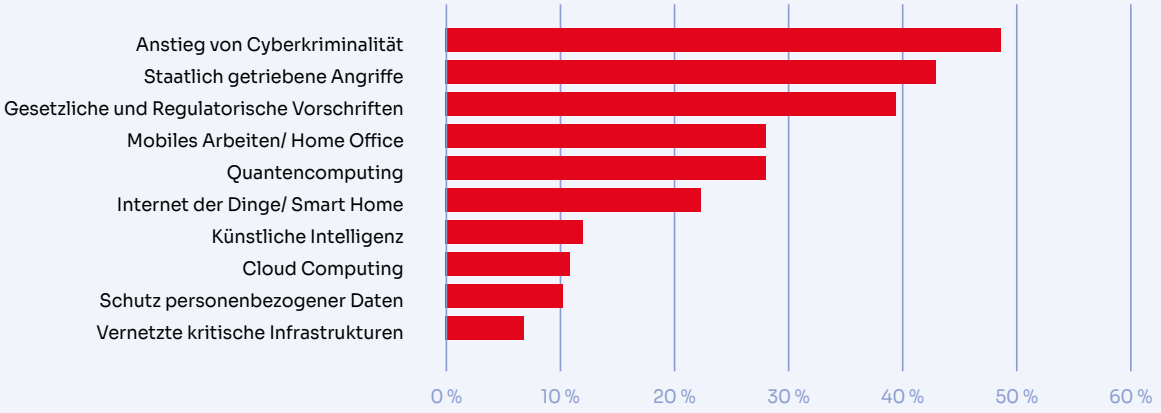


Abbildung 18: Treiber für Veränderungen im Bereich Cybersicherheit

Der Anstieg der Cyberkriminalität wird weiterhin als der stärkste Treiber für Veränderungen im Bereich der IT-Sicherheit in den kommenden Jahren angesehen.

Auch das Thema staatlich gesteuerte Angriffe hat – wie bereits im Vorjahr – einen deutlichen Sprung nach vorne gemacht. Immer klarer wird, dass internationale Konflikte nicht nur auf physischer, sondern zunehmend auch auf digitaler Ebene ausgetragen werden. Cyberangriffe als Mittel geopolitischer Auseinandersetzung betreffen dabei längst nicht mehr nur Regierungen, sondern auch kritische Infrastrukturen und Unternehmen.

Auf dem dritten Platz sehen die Befragten das Thema Regulierung. Angesichts aktueller Entwicklungen wie der NIS-2-Richtlinie, dem europäischen Cyber Resilience Act (CRA), der Digital Operational Resilience Act (DORA) für den Finanzsektor und weiteren nationalen Gesetzesinitiativen überrascht diese Einschätzung nicht. Unternehmen stehen zunehmend unter Druck, regulatorische Anforderungen frühzeitig umzusetzen und ihre Sicherheitsstrategien daran auszurichten.

Treiber für Veränderungen 2021–2025

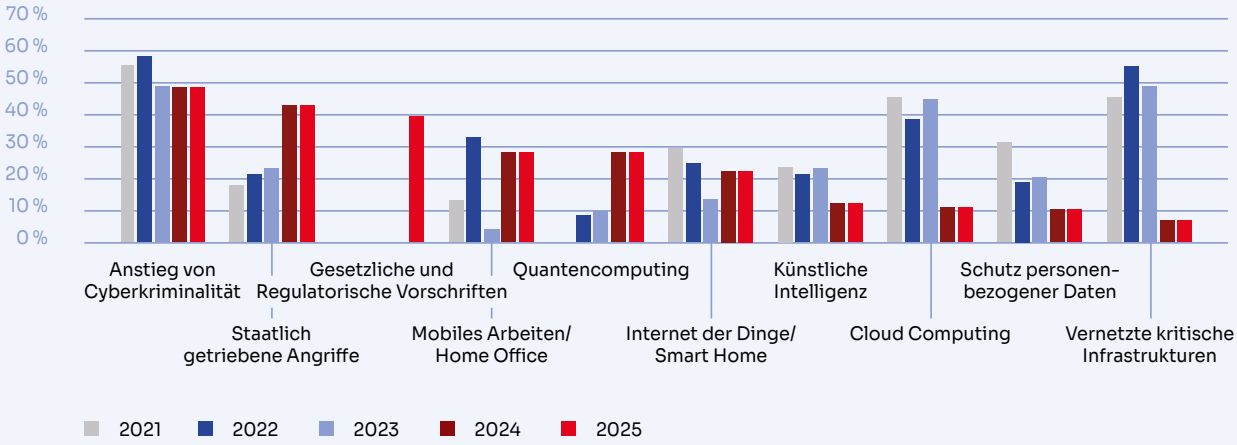


Abbildung 19: Teiber für Veränderungen im Jahresvergleich 2021 bis 2025

Fazit

Die Ergebnisse der Studie verdeutlichen: Die IT-Sicherheitslage bleibt angespannt. Organisierte Cyberkriminalität und staatlich gesteuerte Angriffe nehmen weiter zu und richten sich zunehmend gezielt gegen Unternehmen und öffentliche Infrastrukturen. Vor diesem Hintergrund wird klar: Cybersicherheit ist kein Randthema mehr – sie muss integraler Bestandteil jeder unternehmerischen Entscheidung sein. Sie gehört in die Verantwortung der Unternehmensleitung und darf nicht allein der IT-Abteilung überlassen werden.

Gleichzeitig zeigt die Studie aber auch: Unternehmen sind den wachsenden Bedrohungen nicht schutzlos ausgeliefert. Mit gezielten Investitionen in IT-Sicherheit, wirksamen Notfallplänen und der Sensibilisierung der Mitarbeitenden lassen sich Risiken minimieren und die Auswirkungen möglicher Angriffe deutlich begrenzen. Wer frühzeitig handelt, stärkt nicht nur die eigene Widerstandsfähigkeit, sondern auch das Vertrauen von Kunden, Partnern und Aufsichtsbehörden.

Ihre Ansprechpartner bei eco zum Thema Security:

Cornelia Schildt
Senior Projekt Managerin IT-Sicherheit
eco - Verband der Internetwirtschaft e.V.

Büro Köln
Lichtstraße 43h
50825 Köln

Telefon: +49 (221) 7000 48 – 175
E-Mail: sicherheit@eco.de

Michael Weirich
Projekt Manager IT-Sicherheit
eco - Verband der Internetwirtschaft e.V.

Büro Köln
Lichtstraße 43h
50825 Köln

Telefon: +49 (221) 7000 48 – 193
E-Mail: sicherheit@eco.de

eco –Büro Köln

Lichtstraße 43h
50825 Köln

+49(0)221/700048-0

sicherheit@eco.de
www.eco.de