Cybersicherheit in deutschen Unternehmen

Neue Bedrohungslage – besserer Schutz

TÜV VERBAND

Inhalt

Cyberbedrohungslage verschärft sich – Handlungsbedarf bei Politik und Wirtschaft

Seit der letzten TÜV Cybersecurity Studie vor zwei Jahren hat sich die internationale Sicherheitslage dramatisch verschärft. Durchtrennte Unterseekabel, Spionagedrohnen, Desinformation und Cyberangriffe auf staatliche Institutionen, Politiker und Parteien – Deutschland ist dauerhaft hybriden Angriffen ausgesetzt. Täglich kommt es zu Cyberattacken auf Unternehmen, besonders auf die Verteidigungsindustrie und Kritische Infrastrukturen wie Energieversorger, Kliniken oder Breitbandnetze. Auf diesem Feld agieren staatliche Hacker mit dem Ziel der Destabilisierung ebenso wie Kriminelle, die Geld erpressen oder Geschäftsgeheimnisse stehlen wollen. Für die aktuelle Studie wollten wir von den Verantwortlichen für IT-Sicherheit aus 500 Unternehmen wissen: Wie ist die aktuelle Bedrohungslage? Was ist neu? Was tun Unternehmen, um sich zu schützen? Welche Rolle spielen Normen, Standards und Gesetze bei der Verbesserung der Cybersicherheit?

In den zwölf Monaten vor der Befragung kam es in 15 Prozent der Unternehmen zu IT-Sicherheitsvorfällen – 4 Prozentpunkte mehr als vor zwei Jahren. Gut die Hälfte davon war mehrfach betroffen.
Die mit Abstand häufigste Angriffsmethode ist Phishing. In der Regel sind es E-Mails, die zu einer Schadsoftware führen. 84 Prozent der betroffenen Unternehmen berichten von Phishing-Angriffen – 12 Prozentpunkte mehr als noch vor zwei Jahren.
Die Studie zeigt ein Ungleichgewicht. Hacker setzen vermehrt KI-Systeme ein, um ihre Angriffe weiter zu professionalisieren. Doch nur jedes zehnte Unternehmen nutzt Künstliche Intelligenz für die Abwehr von Cyberattacken. Dabei könnte KI helfen, Anomalien zu erkennen, Schwachstellen zu analysieren und Angriffe automatisiert abzuwehren. Hier muss die Mehrheit der Unternehmen dringend aufholen.
Die gute Nachricht: Es lohnt sich, in Cybersicherheit zu investieren. Denn andere Angriffsmethoden sind rückläufig, insbesondere Ransomware. Bei den Angriffen werden sensible Daten verschlüsselt oder gestohlen und das Unternehmen dann erpresst. Ransomware bleibt eine Bedrohung, aber viele Unternehmen können sich heute besser schützen, unter anderem mit professionellen Backup-Systemen.

Eine weitere Gefahr sind Cyberangriffe über Zulieferer und Kunden. Gut ein Fünftel schätzt das Risiko als hoch oder sehr hoch ein. Und jedes zehnte Unternehmen hat bereits Angriffe festgestellt, die über diese Wege erfolgt sind. Ein Gegenmittel sind Sicherheitsanforderungen zwischen Geschäftspartnern in der Lieferkette. Jedes dritte Unternehmen macht entsprechende Vorgaben, aber nur sehr wenige überprüfen diese mit entsprechenden Audits.

Die Unternehmen tun einiges, um sich vor Cyberangriffen zu schützen. Investitionen in moderne Hard- und Software, Unterstützung von externen Experten oder Schulungen der Mitarbeitenden. Sehr wichtig aus unserer Sicht: Notfallübungen, um Abläufe für den Ernstfall einzuüben und Pentests, die technische Schwachstellen im eigenen Unternehmen aufdecken können.

Ein wichtiges Instrument sind Normen und Standards. Sie geben vor, was Unternehmen technisch und organisatorisch tun müssen, um ihre Cybersicherheit zu verbessern. Für 70 Prozent der Befragten sind Normen und Standards wichtig oder sehr wichtig, um den Schutz vor Cyberangriffen stetig zu verbessern.

Angesichts der technischen und geopolitischen Entwicklungen ist es aber auch notwendig, gesetzliche Vorgaben zu machen. Diese Ansicht teilt die Mehrheit der befragten Sicherheitsverantwortlichen: 56 Prozent fordern, dass jedes Unternehmen gesetzlich verpflichtet sein sollte, angemessene Maßnahmen für seine Cybersicherheit zu ergreifen. Die europäische NIS2-Richtlinie verfolgt genau dieses Ziel. Sie legt Mindestanforderungen für Unternehmen in 18 sicherheitskritischen Branchen wie Energie, Gesundheit, Transport oder digitalen Diensten fest. Allerdings hinkt Deutschland bei der Umsetzung hinterher. Die Bundesregierung muss jetzt handeln und das Gesetz zügig verabschieden. Fatal aus unserer Sicht: Nur die Hälfte der Unternehmen kennt die NIS2-Richtlinie. Hier ist noch viel Aufklärungsarbeit notwendig.

Die TÜV-Organisationen stehen bereit, insbesondere den Mittelstand bei der Umsetzung in der Praxis zu unterstützen. Dabei werden wir auch in Zukunft vertrauensvoll mit Partnern wie dem Bundesamt für Sicherheit in der Informationstechnik zusammenarbeiten. Denn uns eint das Ziel, die Cybersicherheit in der deutschen Wirtschaft kontinuierlich zu verbessern.

Ich wünsche Ihnen eine anregende Lektüre!

Quelle: Tobias Koch

Dr.-Ing. Michael Fübi
Präsident TÜV-Verband e.V. und
CEO TÜV Rheinland

Bei der Cybersicherheit „viel Luft nach oben“

Cybersicherheit ist für uns im Bundesamt für Sicherheit in der Informationstechnik (BSI) ein zentrales Element, um den wirtschaftlichen Erfolg Deutschlands zu bewahren und im Rahmen der Digitalisierung weiter zu fördern. Cyberangriffe mit Ransomware, bei denen Unmengen an wertvollen Daten gestohlen und ganze Netzwerke verschlüsselt werden, sind das drängendste Problem für die deutsche Wirtschaft. Dazu kommt eine geopolitische Lage, die seit Jahrzehnten nicht mehr so angespannt und komplex war wie heute. Mit ihr gehen Cyberspionage und Cybersabotage einher. Dies alles sind reale Bedrohungen, die wir im BSI Tag für Tag beobachten und aktiv in Deutschland abwehren.

Umso erstaunter war ich, als in der vorliegenden Umfrage über 90 Prozent der Unternehmen angegeben haben, sie seien gut oder sehr gut aufgestellt in Sachen Cybersicherheit. So sehr ich mir wünsche, dass dies den Tatsachen entspricht: Ich muss vor einem trügerischen Gefühl der Sicherheit warnen. Sowohl die Ergebnisse unserer Cyber-Risikos-Checks, die sich an kleinere Unternehmen richten als auch die deutlich komplexeren Nachweise, die wir von Betreibern Kritischer Infrastrukturen erhalten, zeigen ein anderes Bild: Wir haben in Deutschland in Sachen Cybersicherheit viel Luft nach oben! Wir müssen weiter konsequent unsere Digitalisierung schützen, nur so können wir auch unseren Wohlstand erhalten.

Ein Mittel dafür wird die Umsetzung der NIS-2-Richtlinie in deutsches Recht sein. Rund 29.000 Unternehmen werden künftig angemessene Cybersicherheitsmaßnahmen umsetzen und nachweisen müssen. Zudem wird eine Meldepflicht für IT-Sicherheitsvorfälle eingeführt. Zurecht weisen die Unternehmen in dieser Studie daraufhin, dass regulatorische Vorgaben herausfordernd sind, auch weil sie zu Bürokratie und damit zu Mehraufwand führen. Gleichzeitig können sie aber auch dabei helfen, dass IT-Sicherheitsmaßnahmen in Unternehmen auch umgesetzt werden. Uns ist dieser Spagat durchaus bewusst und daher verfahren wir im BSI nach dem Credo „Cybersicherheit vor Bürokratie“. Für uns ist entscheidend, dass Unternehmen Planungssicherheit haben und wissen, was auf sie zukommt. Wir stellen die uns mögliche maximale Transparenz zu NIS-2 her und bieten mit Webinaren, einer NIS-2-Betroffenheitsprüfung und vielen Informationen Orientierung. Seien Sie versichert: Wir arbeiten zusammen an einem gemeinsamen Ziel!

Ein Top-Thema für die befragten Unternehmen ist Künstliche Intelligenz. Und ja: für uns auch. Wir arbeiten intensiv an der Sicherheit von KI, an der Sicherheit durch KI und erforschen die Bedrohungen, die von KI ausgehen. Dieses Thema ist aktueller denn je und es ist gekommen um zu bleiben.

Auch aus diesem Grund bin ich überzeugt: Für die Cybernation Deutschland müssen Digitalisierung und Sicherheit in der Informationstechnik stets zusammen gedacht werden. Dafür brauchen wir starke Partner – dafür brauchen wir einander!

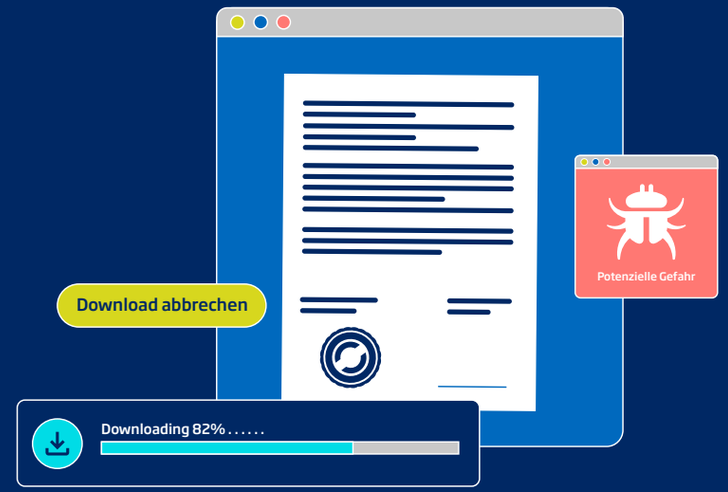
Gehen wir's an!

Quelle: BMI/ Henning Schacht

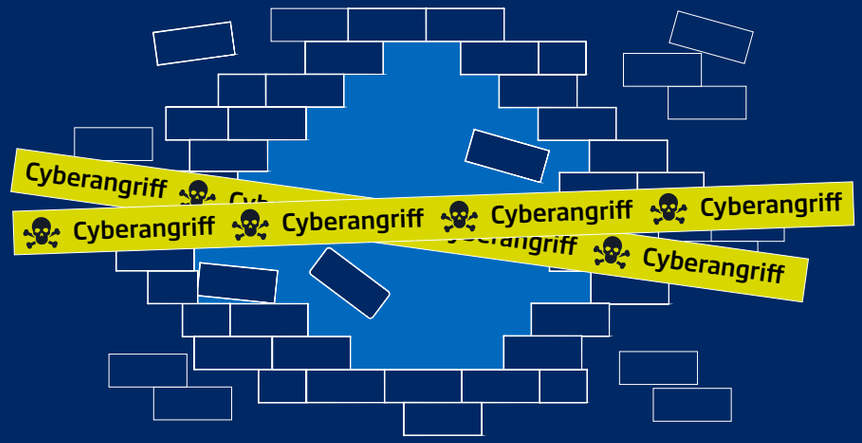
Claudia Plattner
Präsidentin des Bundesamtes für Sicherheit in der Informationstechnik

Kernergebnisse

73 %
schreiben Cybersicherheit eine wichtige Rolle zu



15 %
sind im vergangenen Jahr Opfer eines Cyberangriffs geworden



10 %
haben Cyberangriffe über Zulieferer oder Kunden festgestellt

55 %
fühlen sich von organisierten Cyberkriminellen bedroht

20 %
nutzen KI, um Cyberangriffe abzuwehren

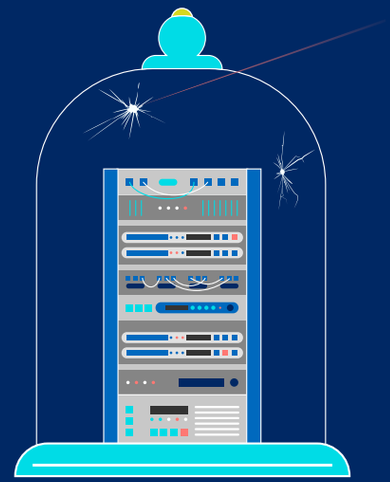
51 %
beobachten, dass Angreifer Künstliche Intelligenz einsetzen

65 %
überstehen Cyberangriffe weitgehend schadlos

32 %
lassen ihre Cybersicherheit von externen Stellen zertifizieren

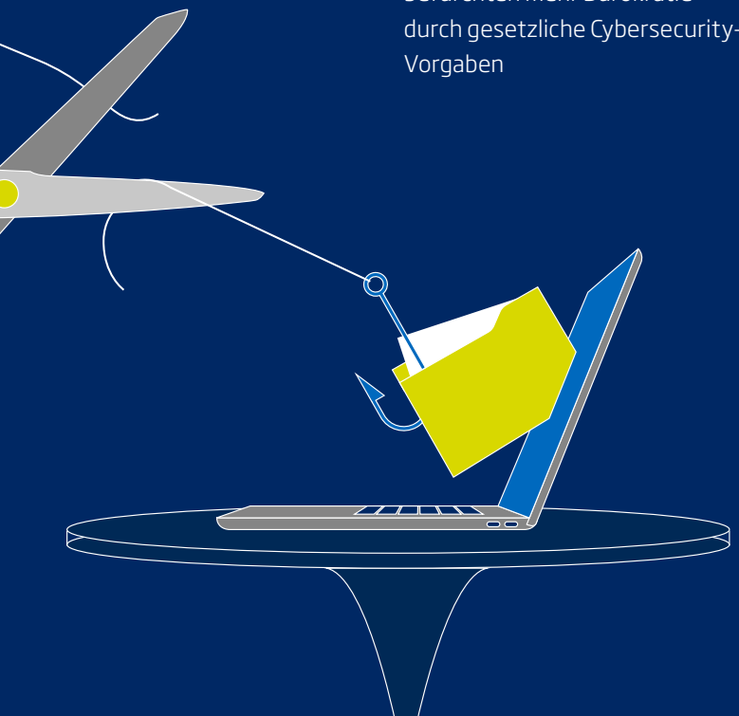
75 %
sind überzeugt, dass Normen und Standards ihre IT-Sicherheit verbessern

79 %
speichern ihre Daten ausschließlich in Rechenzentren in der EU



88 %
befürchten mehr Bürokratie durch gesetzliche Cybersecurity-Vorgaben

60 %
der mit der Richtlinie Vertrauten erwarten mehr Cybersicherheit durch NIS2



50 %
kennen die NIS2-Richtlinie der EU für Cybersicherheit nicht

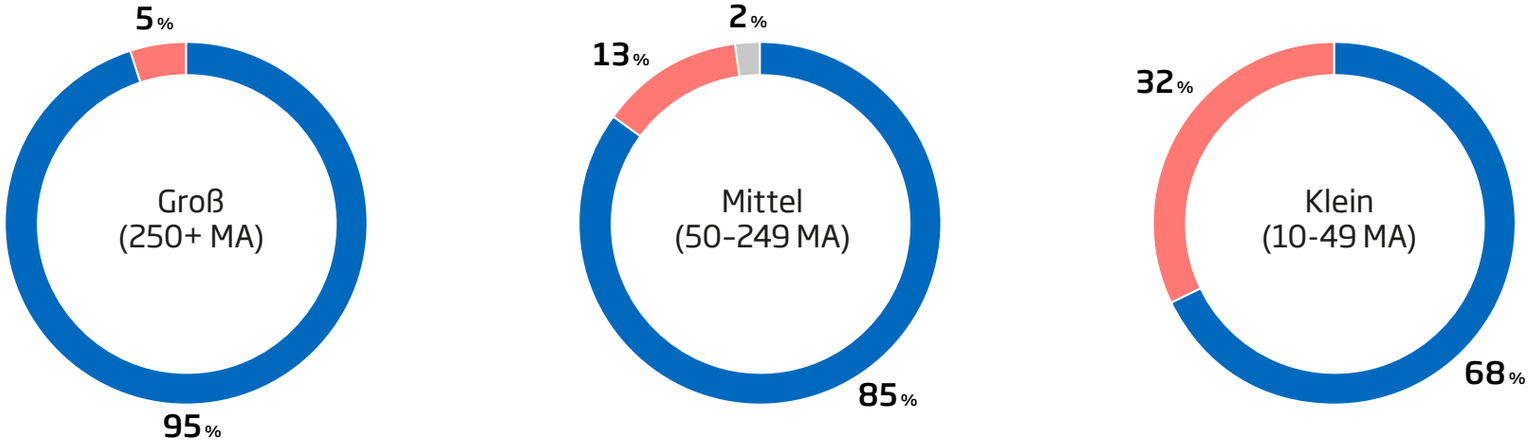
56 %
halten verpflichtende Cybersecurity-Vorgaben für richtig

Bedeutung von Cybersicherheit und aktuelle Bedrohungslage

1

Cybersicherheit hat in drei von vier Unternehmen eine hohe Relevanz

Welche Rolle spielt Cybersecurity in Ihrem Unternehmen?



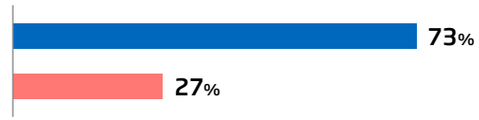
Sehr/eher große Rolle
Eher kleine/überhaupt keine Rolle
Weiß nicht/Keine Angabe

Frage: Welche Rolle spielt Cybersecurity aktuell für Ihr Unternehmen?
Basis: Alle befragten Unternehmen (n=506)

Der Schutz der firmeneigenen Informations- und Kommunikationstechnik ist einer breiten Mehrheit wichtig. Die Bedeutung steigt mit der Größe des Unternehmens.

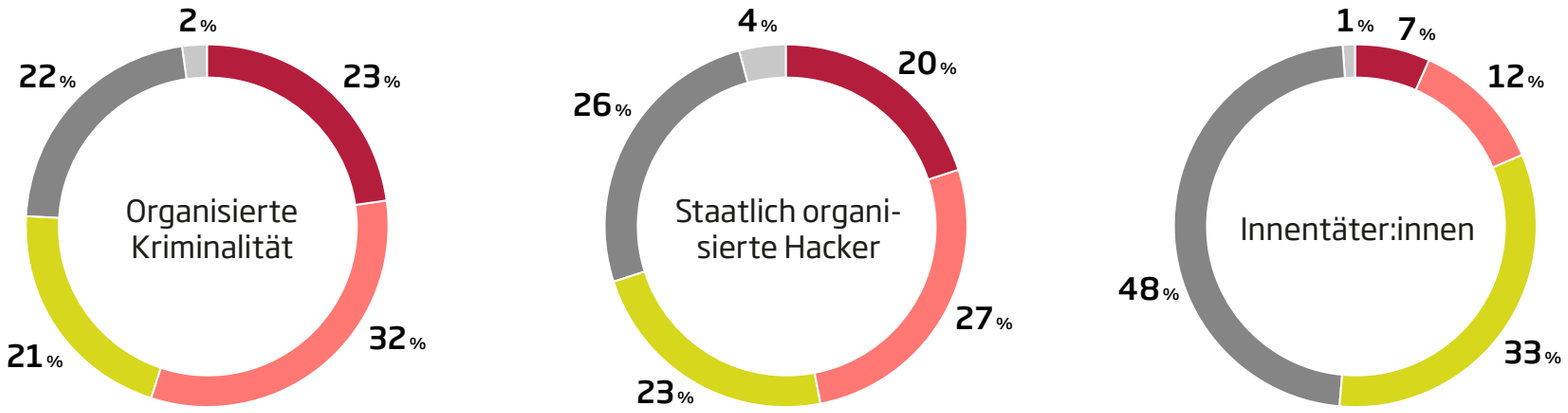
Große Unternehmen sind die Schrittmacher bei der Cybersicherheit. 95 Prozent der Unternehmen mit 250 und mehr Beschäftigten schreiben ihr eine hohe Bedeutung zu. Mit sinkender Firmengröße nimmt auch die Zustimmung ab. So sehen bei Unternehmen mit 50 bis 249 Beschäftigten 85 Prozent für die Cybersicherheit eine wichtige Rolle. Bei Firmen mit bis zu 49 Beschäftigten sind es 68 Prozent. Insgesamt sehen knapp drei Viertel (73 Prozent) der Unternehmen eine hohe Relevanz für den Schutz ihrer IT.

Gesamt



Unternehmen fürchten vor allem kriminelle Banden und staatliche Hacker

Inwiefern stellen diese Akteure eine Bedrohung für die Cybersicherheit Ihres Unternehmens dar?



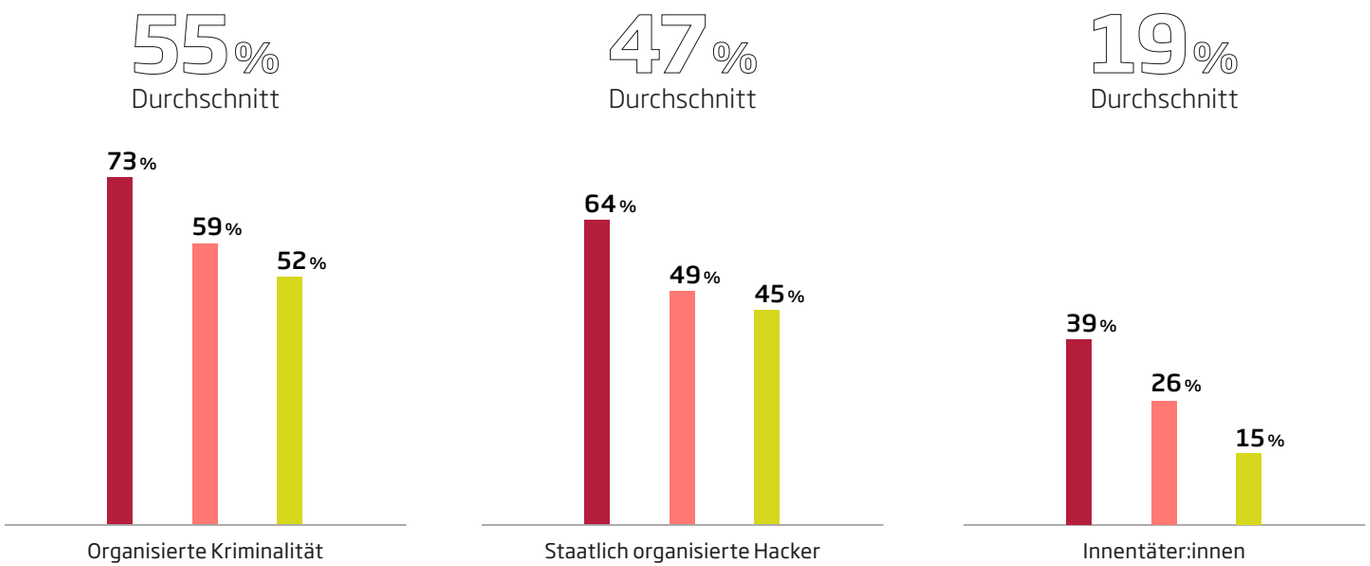
Frage: Ich lese Ihnen nun einige Akteure vor, die Cyberangriffe initiieren. Inwiefern stellen diese Akteure eine große, mittlere, kleine oder keine Bedrohung für die Cybersecurity Ihres Unternehmens dar? | Basis: Alle befragten Unternehmen (n=506)

Jeweils rund die Hälfte der Befragten sieht in der organisierten Kriminalität und in Cybergangstern, die im Auftrag von Staaten tätig sind, eine beträchtliche Bedrohung. Eigene Beschäftigte dagegen werden von einer Minderheit als Gefahr betrachtet.

Die Gefahr kommt meist von außen – so schätzen Unternehmen ihre Lage mit Blick auf Cyberattacken ein. Mehr als die Hälfte (55 Prozent) nimmt organisierte Kriminalität als große Bedrohung (23 Prozent) oder mittlere Bedrohung (32 Prozent) wahr. Nur knapp dahinter liegen staatlich organisierte Hacker, die von fast der Hälfte (47 Prozent) als beträchtliche Gefahr gesehen werden. Weniger kritisch fällt der Blick auf die eigenen Beschäftigten aus. Knapp jeder fünfte Befragte (19 Prozent) erkennt bei Innentäter:innen Potenzial für einen Cyberangriff.

Große Unternehmen fühlen sich besonders häufig bedroht

Inwiefern stellen diese Akteure eine große/mittlere Bedrohung für die Cybersecurity Ihres Unternehmens dar?



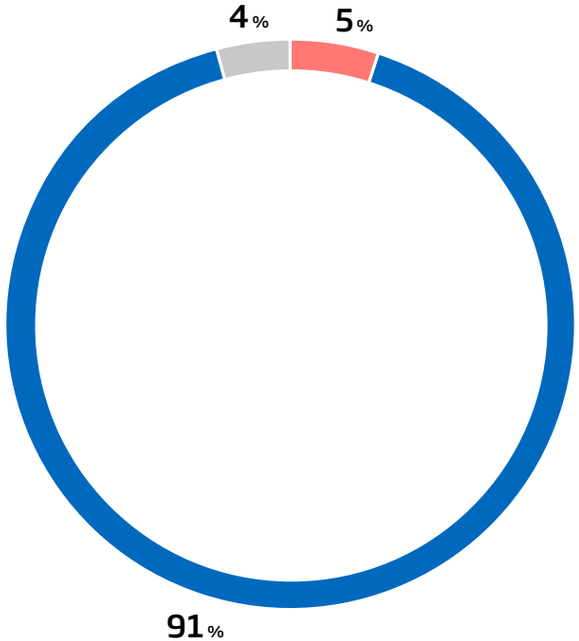
Frage: Ich lese Ihnen nun einige Akteure vor, die Cyberangriffe initiieren. Inwiefern stellen diese Akteure eine große, mittlere, kleine oder keine Bedrohung für die Cybersecurity Ihres Unternehmens dar? | Basis: Alle befragten Unternehmen (n=506) | Unterteilung nach Unternehmensgröße (Mitarbeiter:innen)

Ob organisierte Kriminalität, staatlich organisierte Hacker oder Innentäter:innen: In Unternehmen mit 250 und mehr Beschäftigten ist die Sorge vor Cyberangriffen besonders ausgeprägt.

Ein Angriff auf die firmeneigene IT durch organisierte Kriminelle – vor allem große Unternehmen empfinden dieses Szenario als realistisch. Fast drei Viertel von ihnen (73 Prozent) sehen dies als Bedrohung. Mit abnehmender Größe sinkt auch die Sorge, zum Opfer solcher Attacken zu werden. Bei mittleren Unternehmen fühlen sich knapp drei von fünf Befragten durch organisierte Kriminelle bedroht (59 Prozent), bei kleinen Betrieben ist es gut die Hälfte (52 Prozent). Ein ähnliches Gefälle zeigt sich auch bei der Einschätzung zu staatlich organisierten Hackern und Innentäter:innen – auf insgesamt niedrigerem Niveau. Besonders gering ist die Sorge vor Cyberattacken durch Mitarbeiter:innen bei kleinen Firmen (15 Prozent).

Begrenzte Auswirkungen von geopolitischen Konflikten

Haben geopolitische Konflikte innerhalb der letzten 12 Monate zu mehr Cyberangriffen in Ihrem Unternehmen geführt?



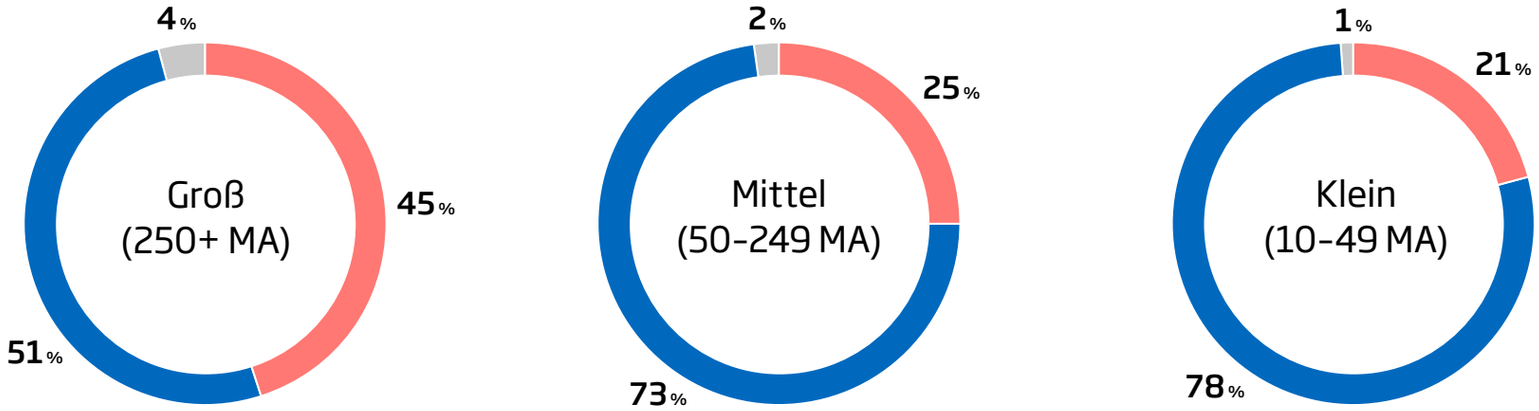
Frage: Haben geopolitische Konflikte innerhalb der letzten 12 Monate zu mehr Cyberangriffen in Ihrem Unternehmen geführt? Haben Sie in den letzten 12 Monaten Angriffe aus bestimmten Regionen identifiziert? | Basis: Alle befragten Unternehmen (n= 506)

Globale Konflikte bergen zwar ein beträchtliches Risiko für die Geschäftsentwicklung vor allem von international tätigen Unternehmen. Mit Blick auf Cyberangriffe sind die Auswirkungen laut Umfrage jedoch gering.

Der russische Angriffskrieg in der Ukraine oder die anhaltenden Spannungen zwischen China und den USA – geopolitische Konflikte haben nach Aussage der befragten Unternehmen nur geringe Auswirkungen auf ihre Cybersicherheitslage. Nur 5 Prozent haben binnen eines Jahres vermehrte Cyberattacken aufgrund dieser Konflikte festgestellt. Mehr als neun von zehn Befragten (91 Prozent) sehen sich davon nicht betroffen. Eine Minderheit (4 Prozent) kann dazu keine Angaben machen.

Cyberangriffe über Zulieferer und Kunden (1/2)

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

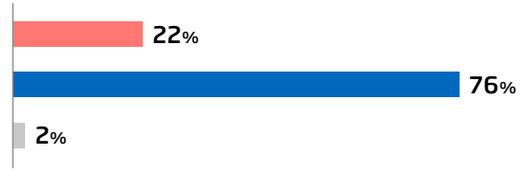


Frage: Wie hoch schätzen Sie das Risiko eines Cyberangriffs über einen Ihrer Zulieferer oder Kunden ein?
Basis: Alle befragten Unternehmen (n=506)

Können Cyberkriminelle einen Angriff starten, indem sie die IT-Systeme von Lieferanten oder Kunden nutzen? Weniger als ein Viertel der Befragten hält dies für realistisch.

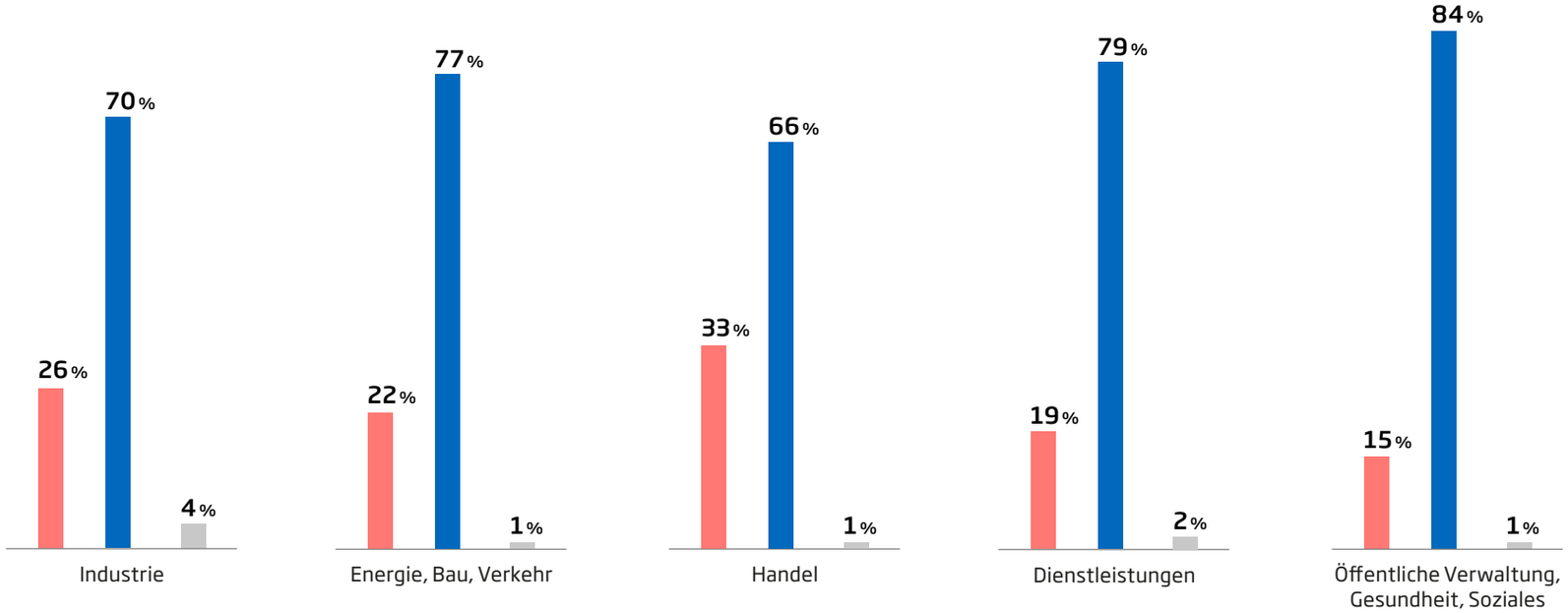
Viele Cyberattacken erfolgen nicht direkt, sondern nehmen einen Umweg über Zulieferer oder Kunden, deren IT von den Hackern zunächst ins Visier genommen worden ist. Etwas mehr als ein Fünftel der Befragten (22 Prozent) bewertet dieses Risiko als beträchtlich. Dabei zeigen sich abhängig von der Firmengröße deutliche Unterschiede. So erkennt fast die Hälfte der großen Unternehmen (45 Prozent) hier eine Gefahr. Generell weniger häufig bedroht sehen sich mittlere sowie kleinere Unternehmen (25 bzw. 21 Prozent).

Gesamt



Cyberangriffe über Zulieferer und Kunden (2/2)

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

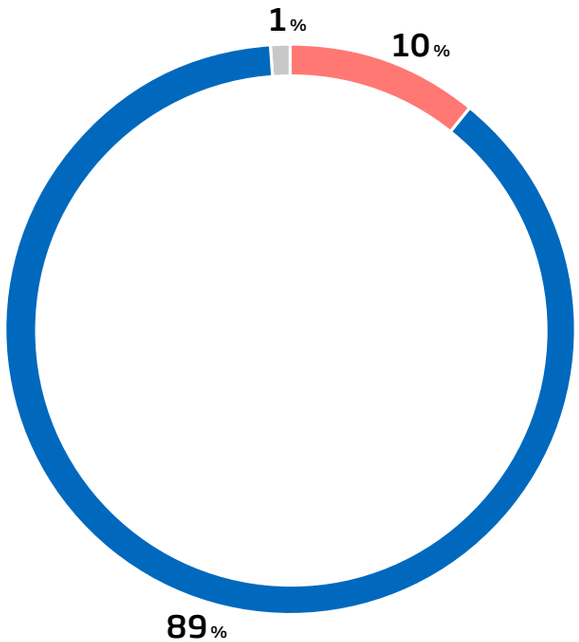


Frage: Wie hoch schätzen Sie das Risiko eines Cyberangriffs über einen Ihrer Zulieferer oder Kunden ein?
Basis: Alle befragten Unternehmen (n=506)

Zwischen den einzelnen Branchen zeigen sich teils deutliche Unterschiede in Bezug auf die Gefahreneinschätzung eines Cyberangriffs über Zulieferer und Kunden. Überdurchschnittlich hoch liegt der Wert insgesamt beim Handel (33 Prozent). Am wenigsten gefährdet durch Angriffe über Kunden oder Zulieferer sieht sich die Öffentliche Verwaltung (15 Prozent).

Zulieferer und Kunden als Einfallstor für IT-Angriffe

Haben Sie einen oder mehrere Cyberangriffe auf Ihr Unternehmen festgestellt, die über Zulieferer oder Kunden erfolgt sind?



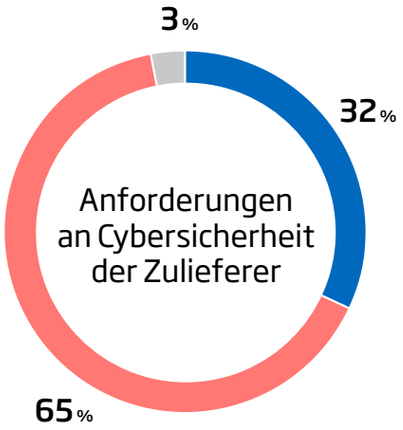
Frage: Haben Sie einen oder mehrere Cyberangriffe auf Ihr Unternehmen festgestellt, die über Zulieferer oder Kunden erfolgt sind?
Basis: Alle befragten Unternehmen (n=506)

Auch, wenn die Mehrheit der Ansicht ist, dass Cyberattacken über Zulieferer und Kunden für sie keine Gefahr darstellen: Tatsächlich ist dies schon bei jedem zehnten Unternehmen geschehen.

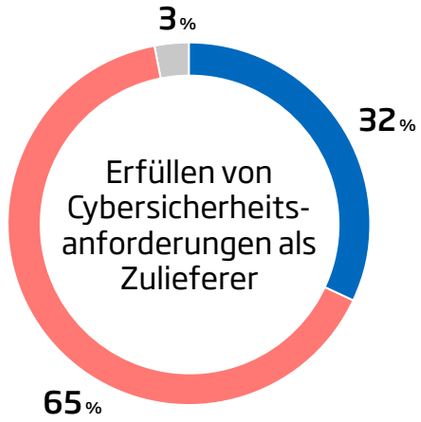
Die Mehrheit ist sicher: Über das Liefer- oder Vertriebsnetzwerk haben Hacker bislang keinen Angriff auf das eigene Unternehmen gestartet. Fast neun von zehn Befragten (89 Prozent) sind dieser Ansicht. Bei einem Zehntel (10 Prozent) allerdings gelang es Cyberkriminellen, die IT von Zulieferern oder Kunden als Einfallstor zu nutzen. Mit hoher Wahrscheinlichkeit ist das Dunkelfeld groß, da der Ursprung eines Angriffs nur schwer nachzuvollziehen ist.

Jeder Dritte stellt Sicherheitsanforderungen an seine Zulieferer

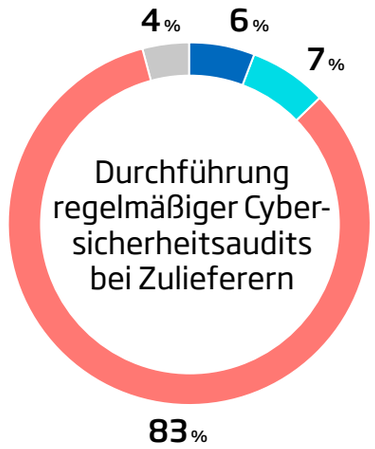
Stellt Ihr Unternehmen Anforderungen an die Cybersicherheit Ihrer Zulieferer?



Müssen Sie selbst als Zulieferer bestimmte Anforderungen bei der Cybersicherheit erfüllen, die an Ihr Unternehmen gestellt werden?



Führen Sie Cybersicherheitsaudits bei Ihren Zulieferern durch, um potenzielle Risiken zu identifizieren?



Ja
Nein
Weiß nicht/Keine Angabe

Fragen: Stellt Ihr Unternehmen Anforderungen an die Cybersicherheit Ihrer Zulieferer? Müssen Sie selbst als Zulieferer bestimmte Anforderungen bei der Cybersicherheit erfüllen, die an Ihr Unternehmen gestellt werden? | Basis: Alle befragten Unternehmen (n=506)

Ja, regelmäßig
Ja, aber nicht regelmäßig
Nein
Weiß nicht/Keine Angabe

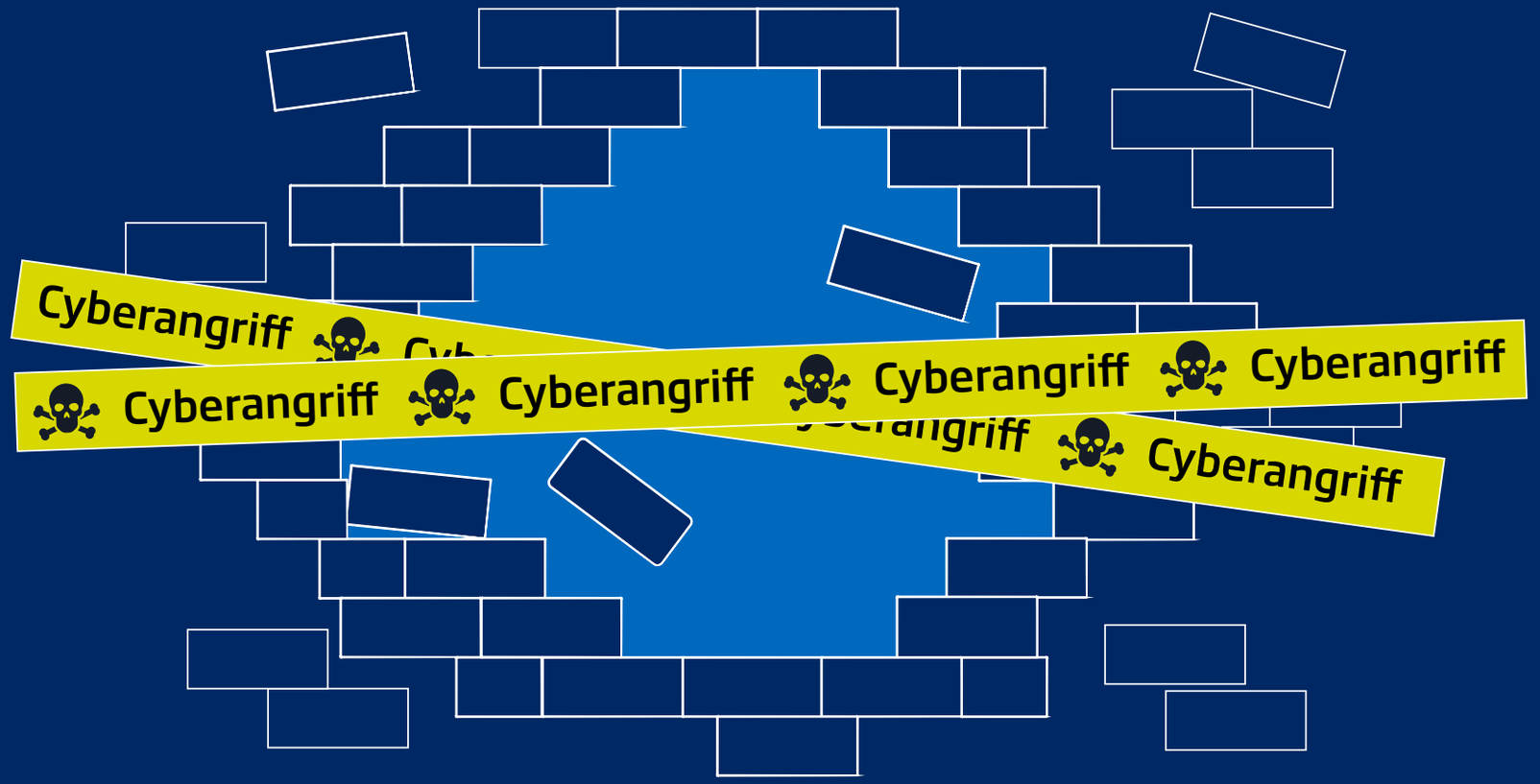
Frage: Führen Sie Cybersicherheitsaudits bei Ihren Zulieferern durch, um potenzielle Risiken zu identifizieren? | Angaben in Prozent | Basis: Alle befragten Unternehmen (n=506)

Anforderungen an die Cybersicherheit von Zulieferern stellt ein knappes Drittel der Befragten. Entsprechende Audits im Liefernetzwerk werden von noch weniger Unternehmen gemacht.

Wie lässt sich sicherstellen, dass von Zulieferern keine Gefahr für die eigenen IT-Systeme ausgeht? Knapp ein Drittel (32 Prozent) stellt dazu Anforderungen an die Cybersicherheit von Geschäftspartnern in ihrer Lieferkette. Auf Cybersicherheitsaudits setzt eine deutliche Minderheit regelmäßig (6 Prozent) oder nicht regelmäßig (7 Prozent). Wenn sie selbst in der Zuliefererrolle sind, müssen sich knapp ein Drittel (32 Prozent) der Firmen bestimmten Anforderungen ihrer Auftraggeber an die Cybersicherheit stellen.

Erfolgreiche Cyberangriffe – und der Umgang damit

2



Die Zahl erfolgreicher Cyberangriffe steigt

15 %

verzeichneten in den letzten 12 Monaten mindestens einen IT-Sicherheitsvorfall.

+4 %

im Vergleich zu 2023

Frage: Hat Ihr Unternehmen in den letzten 12 Monaten einen IT-Sicherheitsvorfall gehabt?
Basis: Alle befragten Unternehmen (n=506)

Eine wachsende Zahl von Unternehmen wird Opfer von Attacken auf ihre IT. Ein hoher Anteil von ihnen erlebt sogar mehr als einen Sicherheitsvorfall binnen eines Jahres.

Der Anstieg ist beträchtlich: Um vier Prozentpunkte und damit deutlich mehr als 30 Prozent ist die Zahl der Unternehmen gestiegen, die innerhalb von zwölf Monaten mindestens einen IT-Sicherheitsvorfall erlebt haben – also einen erfolgreichen Cyberangriff. Knapp eines von sieben Unternehmen (15 Prozent) ist damit jüngst Opfer von Cyberkriminellen geworden. Etwa die Hälfte von ihnen hat mehr als einen Sicherheitsvorfall erlebt.

Phishing ist die häufigste Angriffsmethode

Was sind die häufigsten IT-Sicherheitsvorfälle?

1. 84 % Phishing und Spear-Phishing-Angriff
2. 12 % Passwort-Angriff
3. 12 % Ransomware-Angriff
4. 6 % Denial-of-Service (DoS) und Distributed-Denial-of-Service (DDoS) Angriff
5. 6 % Social Engineerirng
6. 6 % Supply-Chain-Angriff
7. 5 % Drive-by-Angriff
8. 5 % Man-in-the-middle-Angriff

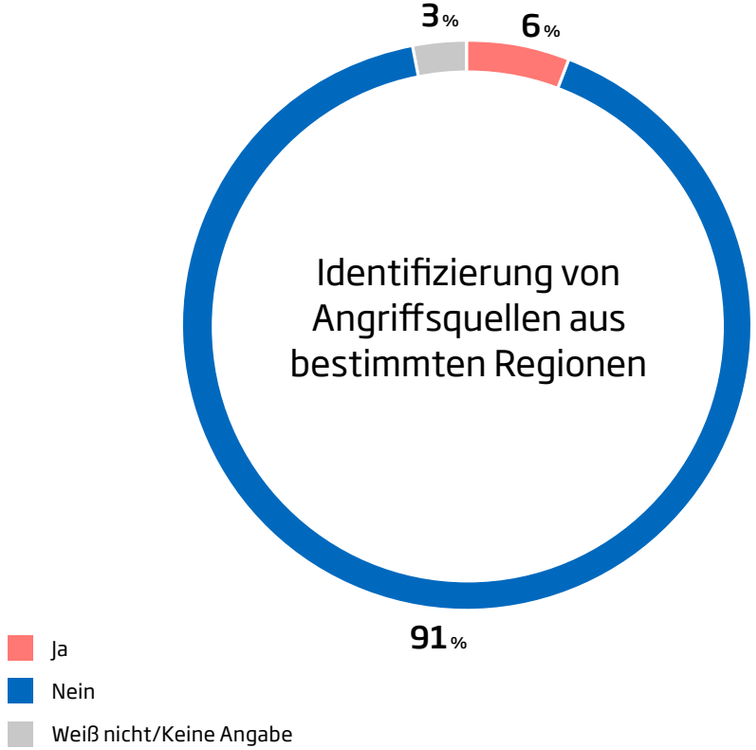
Frage: Um welche Art von IT-Sicherheitsvorfall bzw. Cyberangriffen handelte es sich? (Mehrfachnennungen) | Basis: Unternehmen, die in den letzten zwölf Monaten mindestens einen IT-Sicherheitsvorfall hatten (n=89)

Die Zahl der IT-Sicherheitsvorfälle durch Phishing-Angriffe steigt. Es ist die mit großem Abstand häufigste Form der Cyberattacke auf Unternehmen.

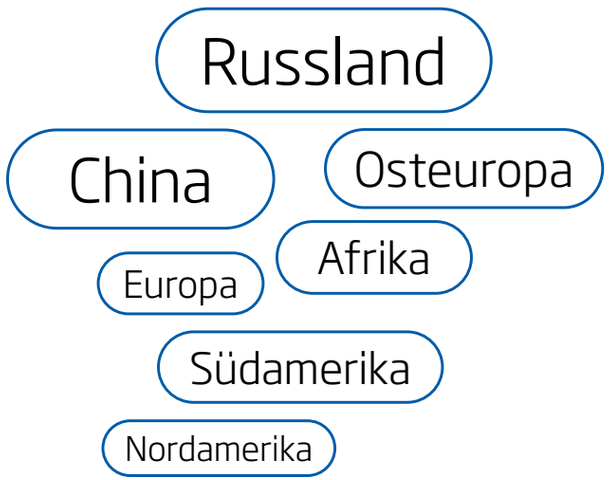
Eine vermeintliche Mail vom Kunden oder dem Kreditinstitut, mit dem das Unternehmen zusammenarbeitet – mit der Bitte, mit einem Klick auf einen Link Daten zu überprüfen: Spear-Phishing heißt die Methode, bei der Cyberkriminelle Wissen über Beschäftigte nutzen, um sie zu täuschen und gezielt Zugang zum Unternehmenskonto einer bestimmten Person zu erhalten. Gemeinsam mit weniger zielgerichteten Nachrichten etwa über vorgetäuschte Gewinnspiele ist dies die mit weitem Abstand häufigste Art des Angriffs. 84 Prozent nennen Phishing und Spear-Phishing als häufigsten Grund für einen IT-Sicherheitsvorfall – ein Anstieg von zwölf Prozent im Vergleich zum Jahr 2023. Auf je zwölf Prozent Nennung kommen Passwort- und Ransomware-Angriffe als nächsthäufige Ursachen. Möglicherweise ist diese Zunahme durch die Popularität von KI-basierten Textgeneratoren (wie zum Beispiel ChatGPT) begründet: Sie tragen in den Händen von Kriminellen zu einem höheren Grad an Automatisierung, Professionalisierung und Individualisierung von Phishing-Angriffen bei.

Herkunft der Cybergangriffe meist unklar

Haben Sie in den letzten 12 Monaten Cyberangriffe aus bestimmten Regionen identifiziert?



Offene Abfrage zur Identifikation von Angriffen



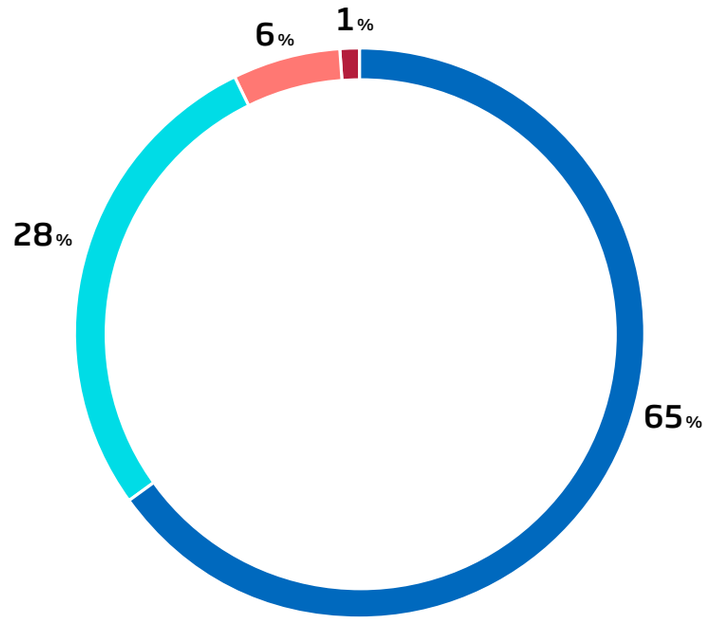
Eine Minderheit der Unternehmen ist in der Lage, die Angriffe bestimmten Regionen zuzuordnen. Wenn dies gelingt, sind die Täter:innen häufig in China und Russland ansässig.

Etwa neun von zehn Unternehmen (91 Prozent) können Cyberattacken nicht mit einem Land oder einer Region in Verbindung bringen, von der aus die Täter:innen operieren. Dies ist nur in sechs Prozent der Fälle möglich. In einer offenen Abfrage zur Identifikation von Angriffen entfallen die häufigsten Nennungen auf China und den asiatischen Raum sowie auf Russland und den osteuropäischen Raum. Westeuropa, Süd- und Nordamerika sowie Afrika wurden deutlich seltener genannt.

Frage: Haben Sie in den letzten 12 Monaten Angriffe aus bestimmten Regionen identifiziert? | Basis: Alle befragten Unternehmen (n= 506) und Unternehmen, die in den letzten 12 Monaten Angriffe aus bestimmten Regionen identifiziert haben (n= 37) | Die Größe der Wörter entspricht der Häufigkeit der Nennungen, d.h. je größer der Begriff, desto mehr Teilnehmende haben dies geäußert.

Zwei Drittel überstehen erfolgreiche Cyberangriffe schadlos

Wie würden Sie den materiellen und immateriellen Schaden für Ihr Unternehmen durch diese IT-Sicherheitsvorfälle bzw. Cyberangriffe bewerten?



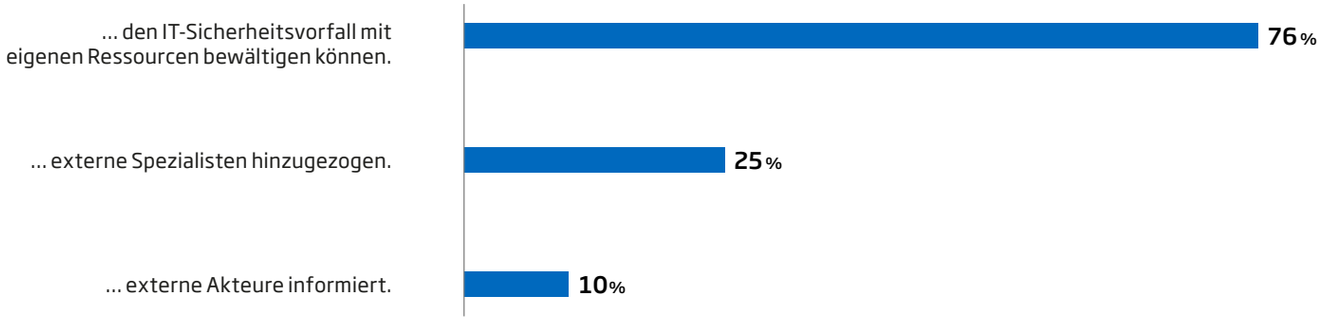
Frage: Wie würden Sie den materiellen und immateriellen Schaden für Ihr Unternehmen durch diese IT-Sicherheitsvorfälle bzw. Cyberangriffe bewerten? | Abweichungen zu 100 Prozent „Weiß nicht"
Basis: Unternehmen, die in den letzten zwölf Monaten mindestens einen IT-Sicherheitsvorfall hatten (n=89)

In einer Minderheit der Fälle gelangen Hacker bei einer erfolgreichen Attacke auch ans Ziel. Nur bei einer geringen Zahl von IT-Sicherheitsvorfällen sind schwere oder gar existenzbedrohende Schäden die Folge.

Der Schaden bei erfolgreichen Cyberangriffen hält sich für Unternehmen meist in Grenzen. Bei rund zwei Drittel (65 Prozent) haben sie gar keine Folgen. In etwas mehr als einem Viertel der Fälle (28 Prozent) ist das Ausmaß des Schadens gering. Jedoch führen sechs Prozent der Attacken zu schweren Schäden. Ein Prozent der Betroffenen nennt die Auswirkungen existenzbedrohend.

Unternehmen bewältigen IT-Sicherheitsfälle überwiegend allein

Inwieweit haben Sie externe Akteure eingebunden als Reaktion auf den IT-Sicherheitsvorfall bzw. Cyberangriff? Wir haben...



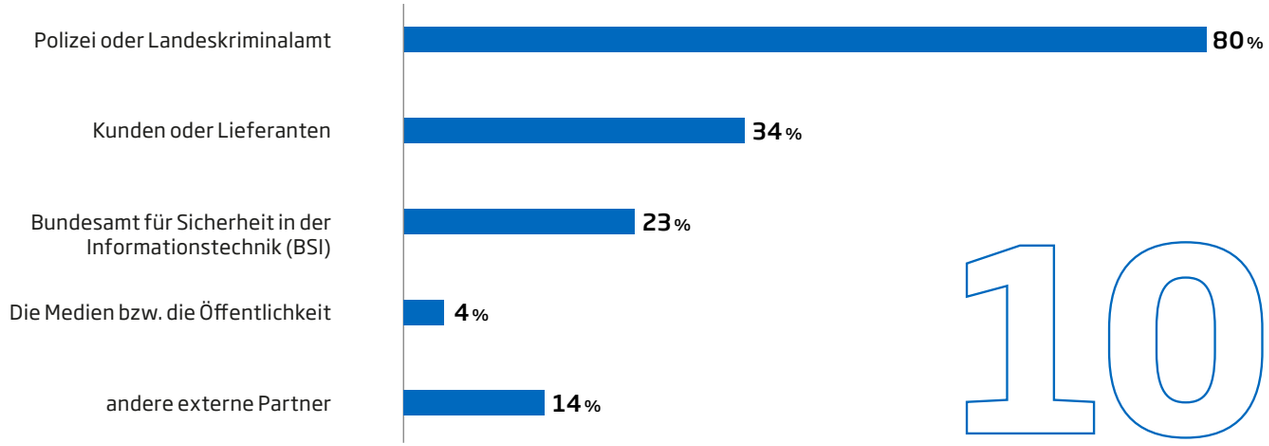
Frage: Inwieweit haben Sie externe Akteure eingebunden, als Reaktion auf den IT-Sicherheitsvorfall bzw. Cyberangriff? Wir haben... (Mehrfachnennungen)
Basis: Unternehmen, die in den letzten zwölf Monaten mindestens einen IT-Sicherheitsvorfall hatten (n=89)

Externe Expertise spielt für Unternehmen, die Opfer eines Cyberangriffs geworden sind, eine untergeordnete Rolle.

Wie reagieren, wenn Cyberkriminelle ans Ziel gekommen sind? Rund drei Viertel der Unternehmen (76 Prozent) zeigen sich in der Lage, den IT-Sicherheitsvorfall mit eigenen Ressourcen in den Griff zu bekommen. Externe Spezialisten haben ein Viertel hinzugezogen (25 Prozent). Benachrichtigt wurden externe Akteure von einem Zehntel der Unternehmen (10 Prozent).

An wen sich Unternehmen bei IT-Sicherheitsvorfällen wenden

Welche externen Akteure haben Sie im Zusammenhang mit dem Vorfall informiert?



10 %

der Unternehmen haben als Reaktion auf einen IT-Sicherheitsvorfall einen externen Akteur informiert.

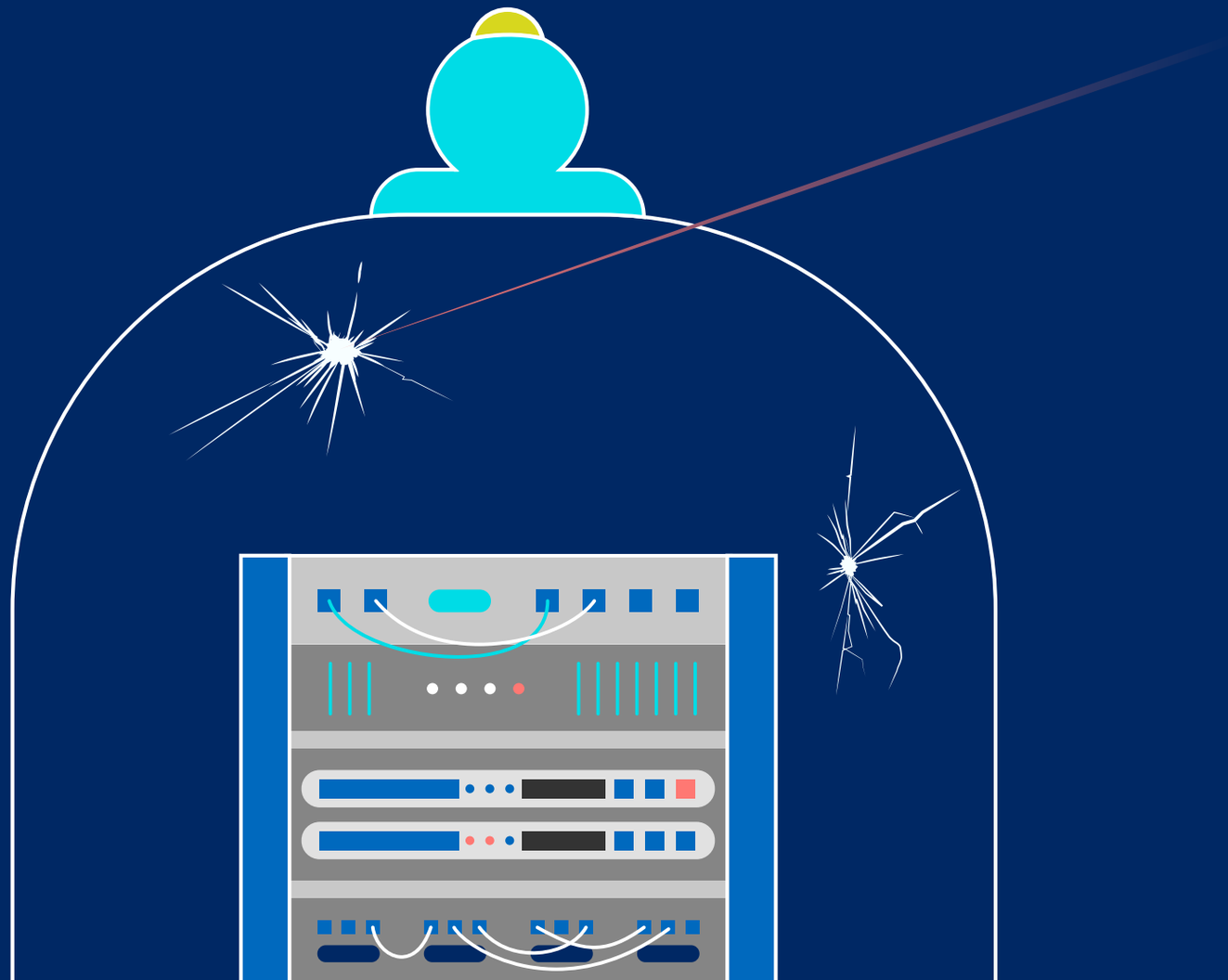
Häufigster Ansprechpartner für Unternehmen ist bei einer Cyberattacke das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Wen kontaktieren Unternehmen bei einem IT-Sicherheitsvorfall? Die breite Mehrheit (80 Prozent) der Unternehmen, die sich an externe Akteure wenden, nehmen Kontakt zur Polizei oder dem Landeskriminalamt auf. Rund ein Drittel der Firmen (34 Prozent) meldet den Cyberangriff. An ihren Kunden oder Lieferanten geht knapp ein Viertel (23 Prozent). Die Ausnahme ist, Medien oder die Öffentlichkeit in Kenntnis zu setzen – dies macht eines von 25 Unternehmen (4 Prozent).

Frage: Welche externen Akteure haben Sie im Zusammenhang mit dem Vorfall informiert? (Mehrfachnennungen) | Basis: Unternehmen, welche externe Akteure informiert haben, 2025 (n=8)

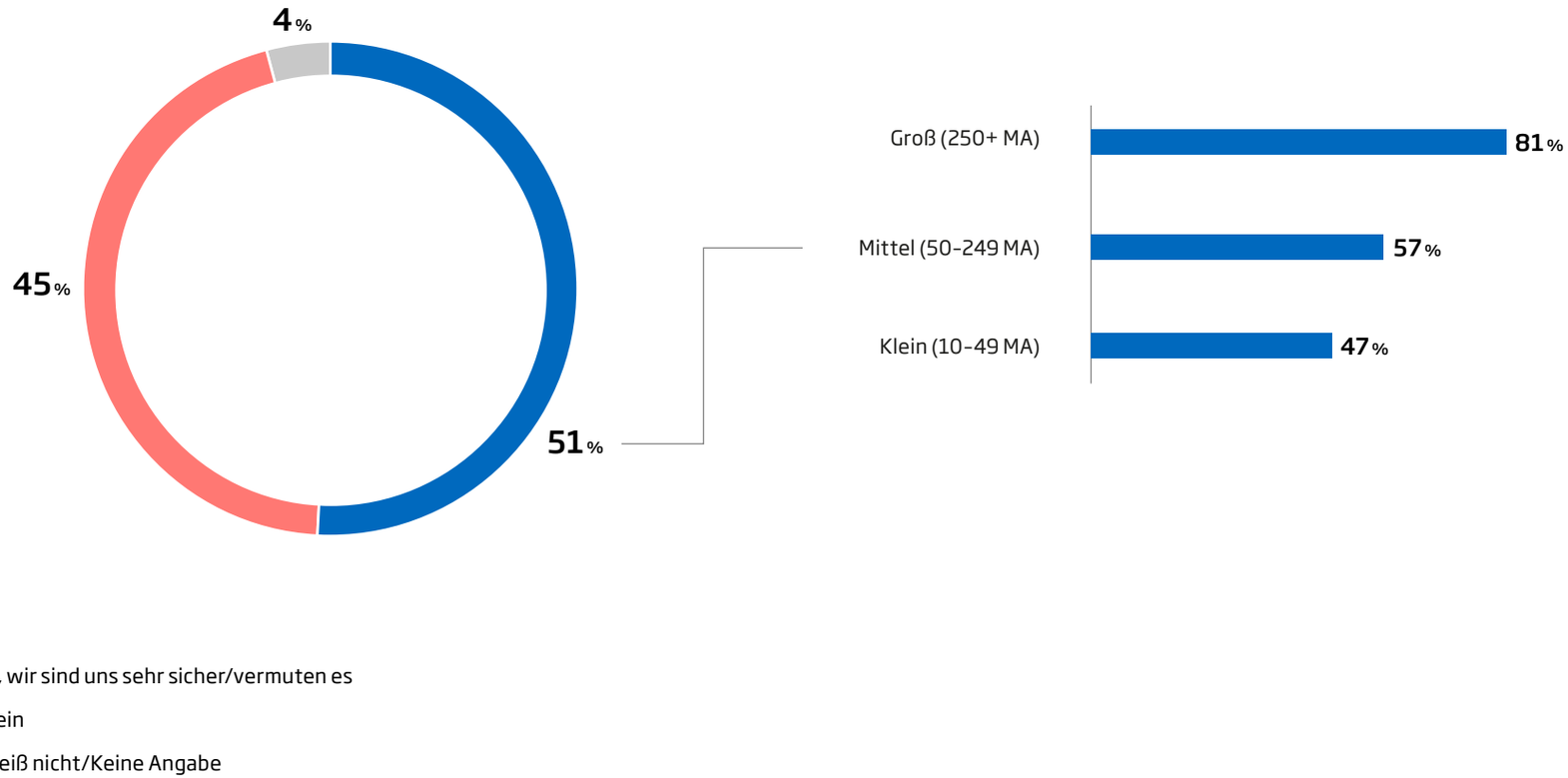
Künstliche Intelligenz: Besserer Schutz und höheres Risiko

3



Viele Unternehmen glauben: Bei Cyberangriffen ist KI im Einsatz

Nehmen Sie wahr, dass Angreifer Künstliche Intelligenz nutzen, um Cyberangriffe auf Ihr Unternehmen durchzuführen?



Frage: Nehmen Sie wahr, dass Angreifer Künstliche Intelligenz nutzen, um Cyberangriffe auf Ihr Unternehmen durchzuführen ?
Basis: Alle befragten Unternehmen (n=506)

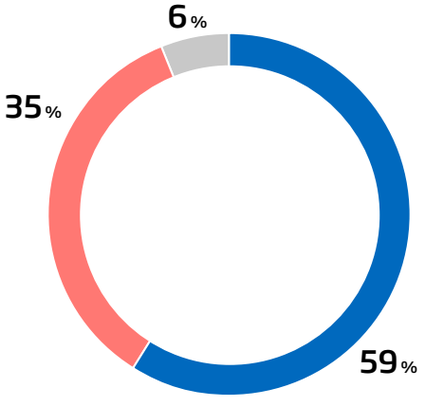
Vor allem große Unternehmen zeigen sich überzeugt oder vermuten, dass bei Attacken auf ihre IT-Systeme Künstliche Intelligenz genutzt wird.

Cyberkriminelle rüsten offenbar auf. Rund die Hälfte der Unternehmen (51 Prozent) ist sich sicher oder vermutet zumindest, dass Angreifer mit Künstlicher Intelligenz (KI) arbeiten. Besonders ausgeprägt ist diese Haltung bei großen Unternehmen mit 250 und mehr Beschäftigten (81 Prozent). Leicht unter dem Durchschnitt dagegen liegen bei dieser Frage kleine Firmen (47 Prozent). Sie vermuten seltener den Einsatz von KI bei einem Angriff.

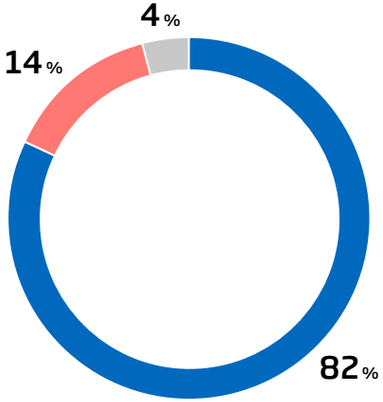
KI erhöht die Zielgenauigkeit von Angriffen

Inwiefern stimmen Sie diesen Aussagen zum Einsatz von KI bei Cyberangriffen zu?

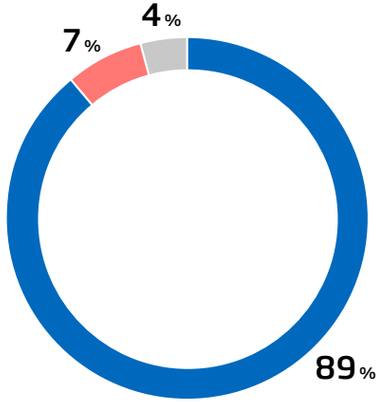
Durch den Einsatz von Künstlicher Intelligenz im Unternehmen erhöht sich die Gefahr von Cyberangriffen auf unser Unternehmen.



Künstliche Intelligenz ermöglicht es Angreifern, gezielt Schwachstellen in unseren Systemen auszunutzen.



Künstliche Intelligenz trägt dazu bei, dass Cyberangriffe effizienter und zielgerichteter durchgeführt werden können.



- Stimme voll/eher zu
- Stimme eher nicht/nicht zu
- Weiß nicht /Keine Angabe

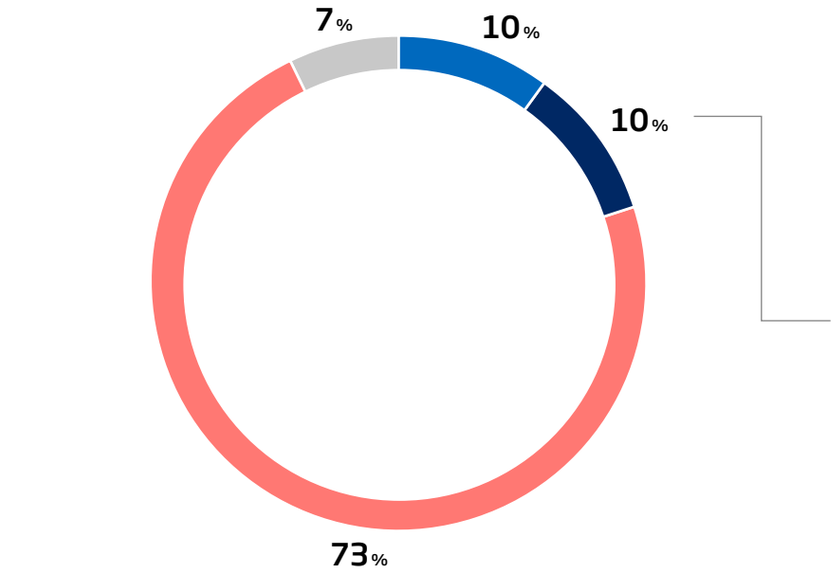
Frage: Ich werde Ihnen nun einige Aussagen zum Einsatz von KI bei Cyberangriffen vorlesen. Inwiefern stimmen Sie diesen zu oder nicht zu? | Basis: Alle befragten Unternehmen (n=506)

Eine breite Mehrheit der Unternehmen ist der Ansicht, dass Künstliche Intelligenz Cyberkriminelle in die Lage versetzt, Schwachstellen besser auszunutzen und gezielter anzugreifen.

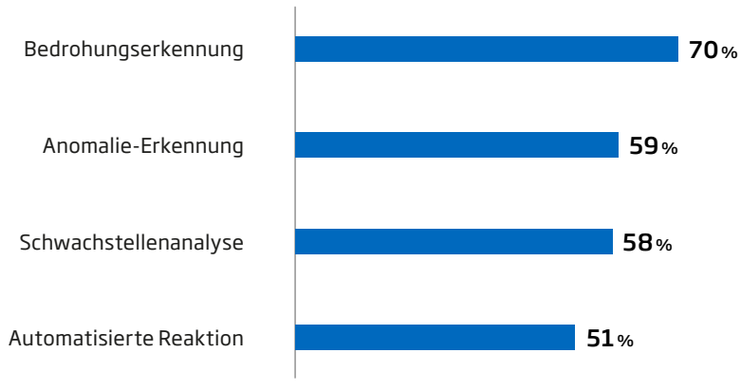
Die Gefahr von Cyberangriffen steigt, wenn ein Unternehmen Künstliche Intelligenz verwendet – diese Befürchtung äußern rund drei Fünftel der Befragten (59 Prozent). Noch einmal deutlich mehr Unternehmen sind der Ansicht, dass sich Schwachstellen der Firmen-IT gezielter aufspüren und ausnutzen lassen, wenn die Angreifer selbst KI nutzen – mehr als vier Fünftel (82 Prozent) stimmen zu. Fast neun von zehn Unternehmen (89 Prozent) gehen davon aus, dass die Attacken mit Unterstützung von KI effizienter und auch zielgerichteter werden.

Nur jedes zehnte Unternehmen nutzt KI für die Abwehr von Cyberangriffen

Setzt Ihr Unternehmen Künstliche Intelligenz (KI) bei der Abwehr von Cyberangriffen ein?



Einsatzbereich von Künstliche Intelligenz



Frage: Setzt Ihr Unternehmen Künstliche Intelligenz (KI) bei der Abwehr von Cyberangriffen ein? | Basis: Alle befragten Unternehmen (n=506)
Frage: In welchen Bereichen der Cybersicherheit setzen Sie KI-basierte Lösungen ein bzw. planen Sie diese einzusetzen? (Mehrfachnennungen) | Basis: Unternehmen, welche KI im Einsatz oder dessen Einsatz in Planung haben (n= 126)

Bedrohungen erkennen, Schwachstellen aufspüren, schnell reagieren: Unternehmen, die KI für den Schutz ihrer IT nutzen, verwenden diese für eine ganze Reihe von Sicherheitsmaßnahmen.

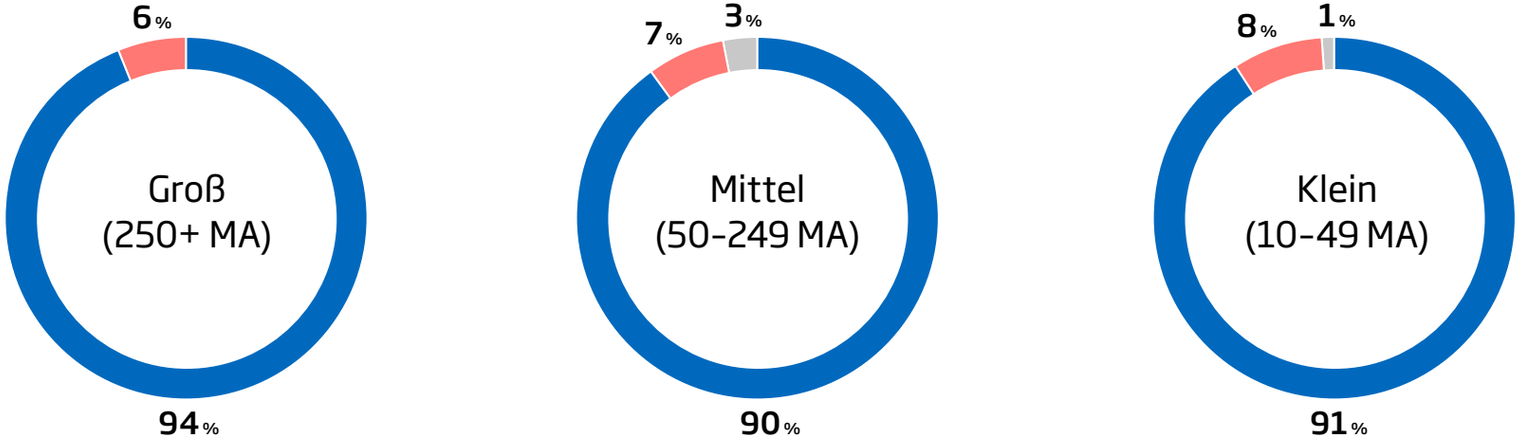
Um sich besser vor Cyberangriffen zu wappnen, setzt ein Fünftel der Unternehmen (20 Prozent) auf Künstliche Intelligenz – oder hat dies zumindest in Planung. Eine deutliche Mehrheit (73 Prozent) verzichtet darauf bislang. Bei den Bereichen, in denen KI-basierte Lösungen zum Einsatz kommen oder künftig genutzt werden sollen, liegt die Bedrohungserkennung an der Spitze (70 Prozent). Doch auch Anwendungen für die Erkennung von Anomalien (59 Prozent), der Analyse von Schwachstellen (58 Prozent) und für automatisierte Reaktionen (51 Prozent) sind bei den Unternehmen, die KI für die IT-Sicherheit verwenden, häufig zu finden.

Maßnahmen zur Verbesserung der Cybersicherheit

4

Unternehmen bewerten ihre Cybersicherheit als gut

Wie bewerten Sie die Cybersicherheit Ihres Unternehmens?



Frage: Wie bewerten Sie die Cybersicherheit Ihres Unternehmens insgesamt? | Basis: Alle befragten Unternehmen (n=506)

Die Wirtschaft betrachtet sich als gut gerüstet für Angriffe auf ihre IT-Systeme.

Sind genug Vorkehrungen gegen Attacken von Hackern getroffen worden? Gut neun von zehn Unternehmen (91 Prozent) bewerten ihre Cybersicherheit als gut. Dabei sind die Unterschiede bei Unternehmen verschiedener Größen und in den einzelnen Branchen gering. Blickt man auf die unterschiedlichen Verantwortungsbereiche überwiegt ebenfalls die positive Einschätzung der eigenen Cybersicherheit: 93 Prozent der IT-Leitungen, 92 Prozent der CISOs, 91 Prozent der IT-Sicherheitsverantwortlichen und 88 Prozent der CEOs halten ihr Unternehmen für gut geschützt. Die Gefahr ist hier, dass die Unternehmen die eigene Resilienz über und die Fähigkeiten der Angreifer unterschätzen.

Gesamt

Besserer Schutz durch zusätzliche Ressourcen

Hat Ihr Unternehmen in den letzten 24 Monaten eine dieser Maßnahmen zur Verbesserung der IT-Sicherheit ergriffen?

27 %

Erhöhung des Budgets für Cybersecurity

2023: 52%

14 %

Einstellung zusätzlicher IT-Experten

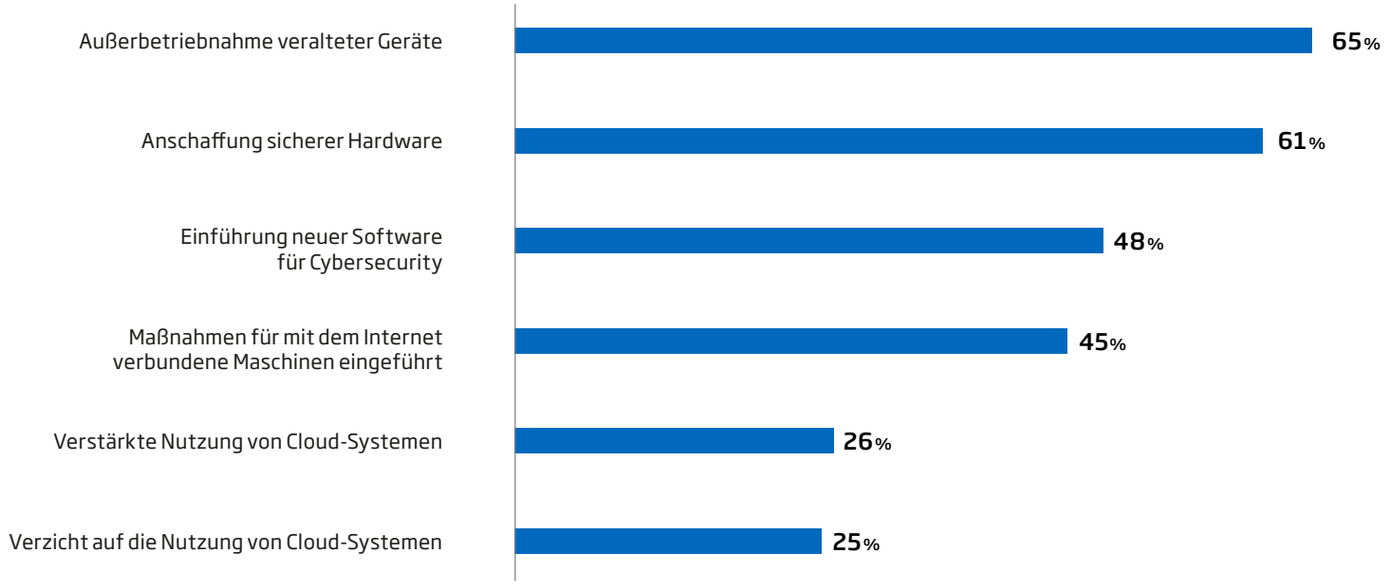
Mit einem höheren Budget und mehr eigenen Fachleuten stärkt ein Teil der Unternehmen die Cybersicherheit.

Eine höhere Resilienz gegen Cyberangriffe durch eine generelle Erhöhung des entsprechenden Budgets – darauf setzt ein gutes Viertel der Unternehmen (27 Prozent). Zusätzliche IT-Experten, die für mehr Sicherheit sorgen, hat rund jedes sechste Unternehmen (14 Prozent) binnen 24 Monaten eingestellt.

Frage: Nun geht es um Maßnahmen für die Verbesserung der IT-Sicherheit. Hat Ihr Unternehmen in den letzten 24 Monaten eine dieser Maßnahmen ergriffen? (Mehrfachnennungen) | Basis: Alle befragten Unternehmen (n=506)

Viele Schutzmaßnahmen betreffen Hard- und Software

Hat Ihr Unternehmen in den letzten 24 Monaten eine dieser Maßnahmen zur Verbesserung der IT-Sicherheit ergriffen?



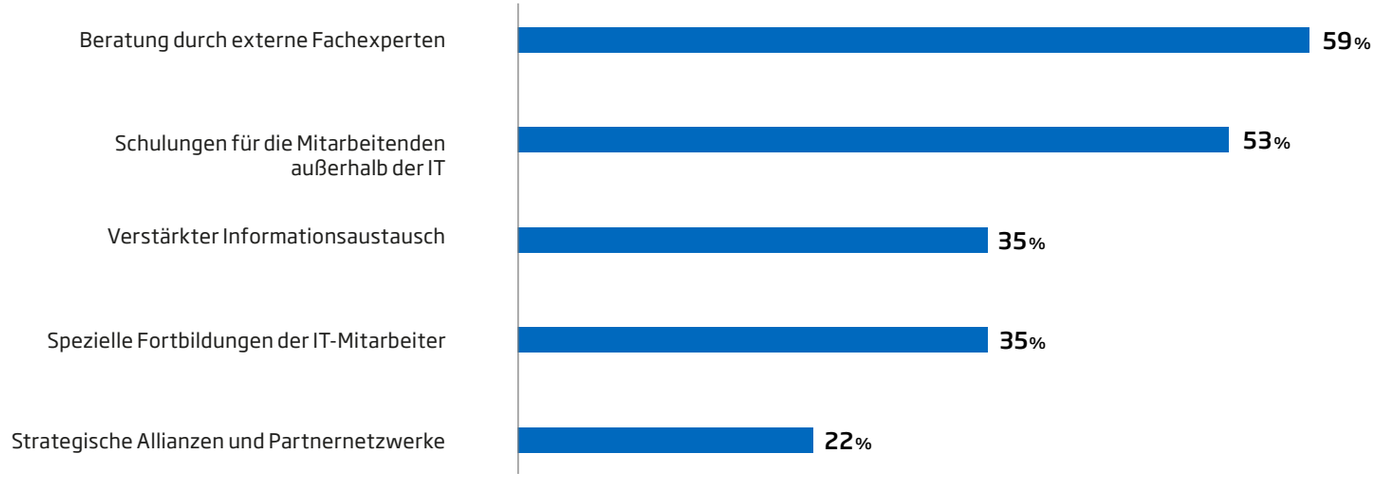
Investitionen in moderne Geräte und Programme sind für viele Unternehmen ein Baustein für die IT-Sicherheit. Bei der Cloud-Nutzung sind die Meinungen gespalten.

Wie können Einfallstore für Cybergangster geschlossen werden? Fast zwei Drittel der Unternehmen nehmen dazu veraltete Geräte außer Betrieb, rund sechs von zehn Unternehmen kaufen neue Hardware. Neue Software für Cybersecurity haben in den 24 Monaten vor der Befragung knapp die Hälfte angeschafft. Fast genauso viele Unternehmen (45 Prozent) schützen mit dem Internet verbundene Maschinen und Geräte besser. Im Umgang mit Cloud-Systemen zeigen sich zwei gegensätzliche Haltungen. Rund ein Viertel nutzt diese stärker, um den Schutz ihrer IT zu verbessern. Etwa dieselbe Zahl der Befragten verzichtet darauf aus Sicherheitsgründen.

Frage: Nun geht es um Maßnahmen für die Verbesserung der IT-Sicherheit. Hat Ihr Unternehmen in den letzten 24 Monaten eine dieser Maßnahmen ergriffen? (Mehrfachnennungen)
Basis: Alle befragten Unternehmen (n=506)

Umfassende Investitionen in das Know-how

Hat Ihr Unternehmen in den letzten 24 Monaten eine dieser Maßnahmen zur Verbesserung der IT-Sicherheit ergriffen?



Fortbildungen für die gesamte Belegschaft und gezielt für die eigenen IT-Spezialisten, dazu externe Beratung: Unternehmen investieren breit in ihr Sicherheits-Know-how.

Rat von außen ist gefragt, wenn sich Unternehmen auf Cyberangriffe vorbereiten. Rund drei von fünf Unternehmen (59 Prozent) haben dazu externe Fachleute konsultiert. Auch Schulungen der Beschäftigten stehen hoch im Kurs – gut die Hälfte der Befragten geben an, diese innerhalb der letzten 24 Monate durchgeführt zu haben. Die IT-Fachkräfte im Betrieb hat etwa ein Drittel (35 Prozent) weitergebildet. Den Informationsaustausch hat ebenfalls rund ein Drittel der Unternehmen intensiviert (35 Prozent). Strategische Allianzen und Partnernetzwerke haben knapp ein Viertel (22 Prozent) aufgebaut oder ausgeweitet.

Frage: Nun geht es um Maßnahmen für die Verbesserung der IT-Sicherheit. Hat Ihr Unternehmen in den letzten 24 Monaten eine dieser Maßnahmen ergriffen? (Mehrfachnennungen)
Basis: Alle befragten Unternehmen (n=506)

Eine Minderheit testet den Ernstfall

Hat Ihr Unternehmen in den letzten 24 Monaten eine dieser Maßnahmen zur Verbesserung der IT-Sicherheit ergriffen?

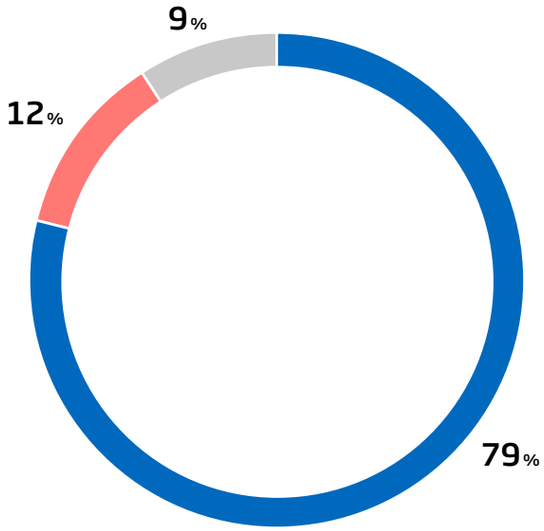
Knapp ein Viertel der Unternehmen bereitet sich mit Simulationen und Notfallübungen auf Cyberattacken vor. Dies gilt auch für Zertifizierungen für die IT-Sicherheit.

Schwachstellen selbst finden, bevor es Angreifer tun: Mit sogenannten Pentests können Unternehmen die Belastungsfähigkeit ihrer IT bei Cyberattacken prüfen. Gut jedes fünfte Unternehmen (22 Prozent) gibt an, diese in den zurückliegenden zwei Jahren genutzt zu haben. Genauso hoch ist die Zahl der Unternehmen, die Notfallübungen absolviert haben, um im Ernstfall schnell und adäquat reagieren zu können. Auf ähnlichem Niveau bewegt sich die Einführung sicherheitsrelevanter Zertifizierungen.

Frage: Nun geht es um Maßnahmen für die Verbesserung der IT-Sicherheit. Hat Ihr Unternehmen in den letzten 24 Monaten eine dieser Maßnahmen ergriffen? (Mehrfachnennungen)
Basis: Alle befragten Unternehmen (n=506)

Die Mehrheit speichert Daten ausschließlich innerhalb der EU

Werden Ihre Unternehmensdaten ausschließlich in Rechenzentren innerhalb der EU gespeichert und verarbeitet?



79%

speichern Unternehmensdaten ausschließlich auf Servern in Europa.

- Ja
- Nein
- Weiß nicht/Keine Angabe

Frage: Werden Ihre Unternehmensdaten ausschließlich in Rechenzentren innerhalb der EU gespeichert und verarbeitet? | Basis: Alle befragten Unternehmen (n=506)

Rechenzentren in der Europäischen Union sind für die meisten Unternehmen der bevorzugte Ort für die Speicherung und Verarbeitung ihrer Daten.

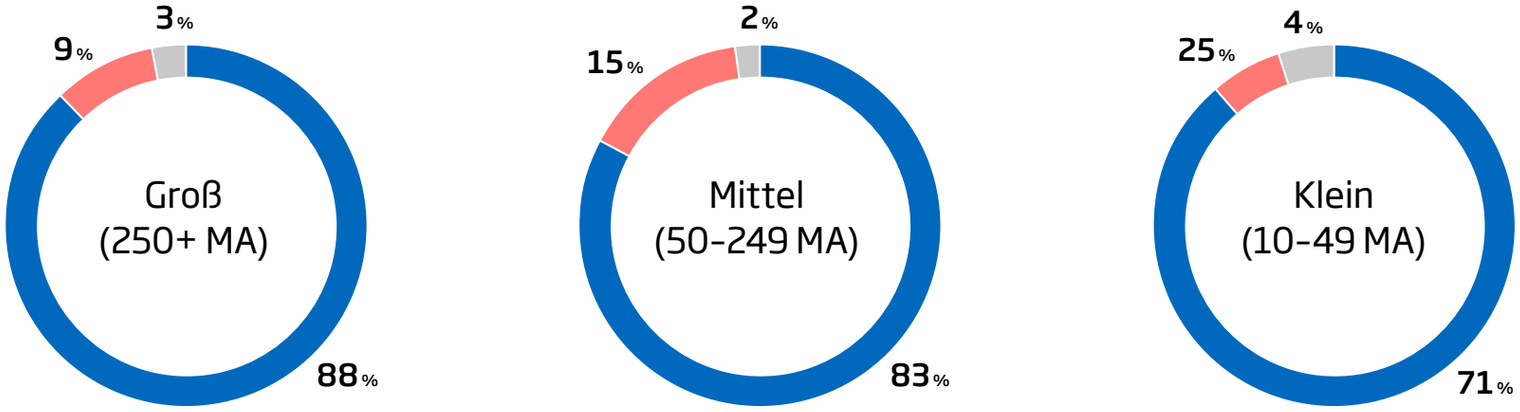
Wer bietet den höchsten Schutz der Daten, wenn diese gespeichert werden? Etwa vier von fünf Unternehmen (79 Prozent) vertrauen hier auf die Europäische Union. Die nötigen Server befinden sich bei ihnen allesamt in dieser Region. Etwa ein Achtel der Unternehmen (12 Prozent) setzt auch auf Rechenzentren außerhalb der EU. Knapp ein Zehntel der Befragten (9 Prozent) können nicht sagen, ob Daten allein hier gespeichert werden oder auch in anderen Regionen. Aufgrund von politischen Unsicherheiten ist die Frage des Datenstandorts sowie des dort geltenden Rechtssystems in den vergangenen Monaten und Jahren immer stärker von Bedeutung geworden.

Hardware-Sicherheit und Schatten-IT

5

Systematische Geräteerfassung in drei von vier Unternehmen (1/2)

Werden alle IT- und Kommunikationsgeräte systematisch erfasst?

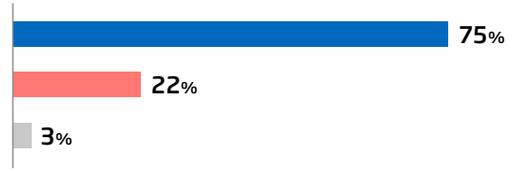


Frage: Werden alle IT- und Kommunikationsgeräte inklusive Smartphones in Ihrem Unternehmen systematisch erfasst? | Basis: Alle befragten Unternehmen (n=506)

Auch bei kleineren Betrieben weiß eine deutliche Mehrheit darüber Bescheid, welche IT- und Kommunikationsgeräte im Einsatz sind.

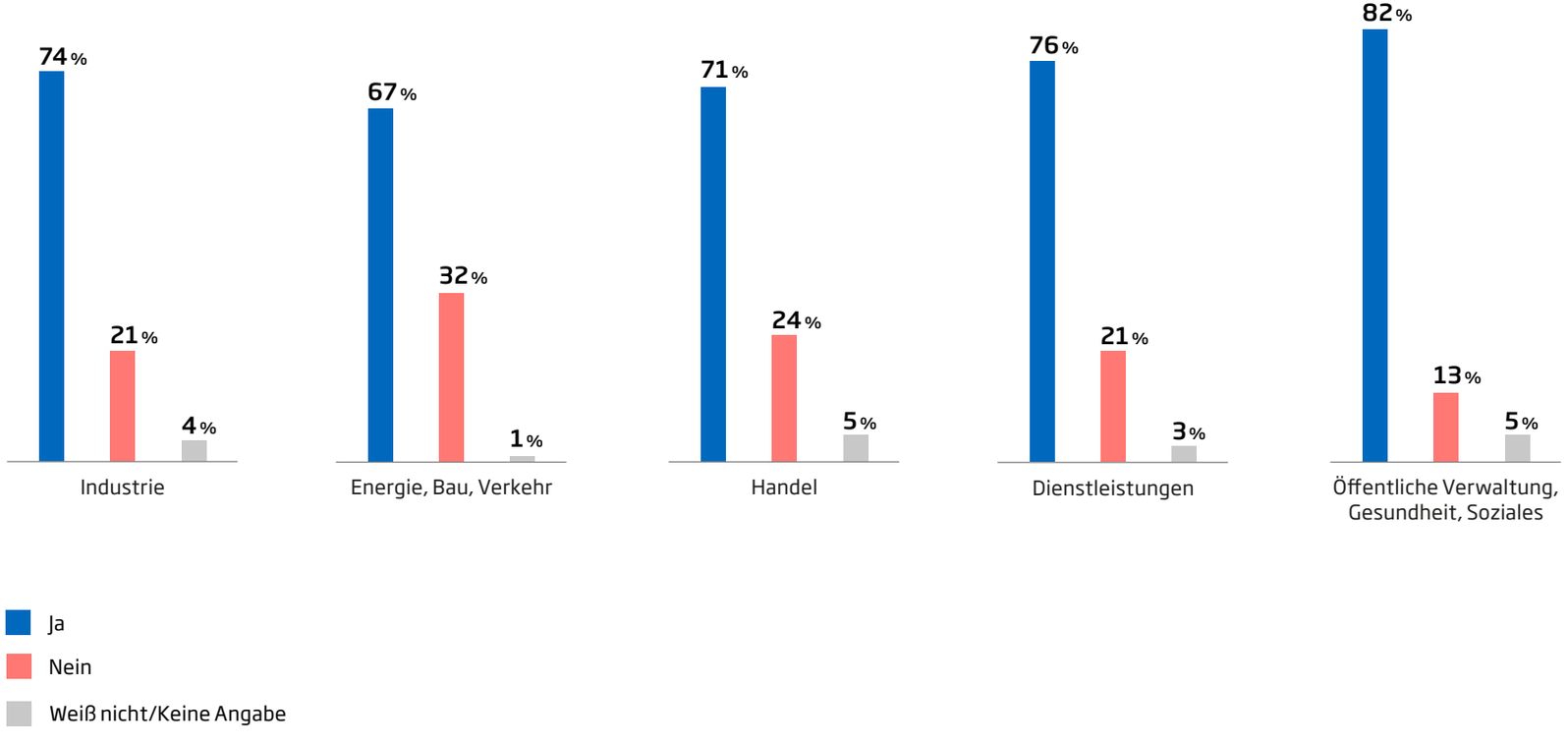
Ob Notebook, Smartphone oder Server – Cyberkriminelle nutzen unbekannte, vergessene oder veraltete IT-Geräte gerne als Einfallstor in die Unternehmensinfrastruktur. Eine systematische Erhebung, welche Geräte im Einsatz sind, leistet einen Beitrag für die Sicherheit. So können beispielsweise Geräte identifiziert werden, die veraltet sind. Im Schnitt gibt es eine solche Erfassung bei drei Viertel der Befragten. Kleinunternehmen liegen etwas unter dem Durchschnitt, Großunternehmen und mittlere Unternehmen deutlich darüber. Bei den Branchen haben Öffentliche Verwaltung sowie Gesundheits- und Sozialwesen eine Vorreiterrolle (82 Prozent). Weniger häufig ist die systematische Erfassung bei Energie, Bau und Verkehr (67 Prozent).

Gesamt



Systematische Geräteerfassung in drei von vier Unternehmen (2/2)

Werden alle IT- und Kommunikationsgeräte systematisch erfasst?



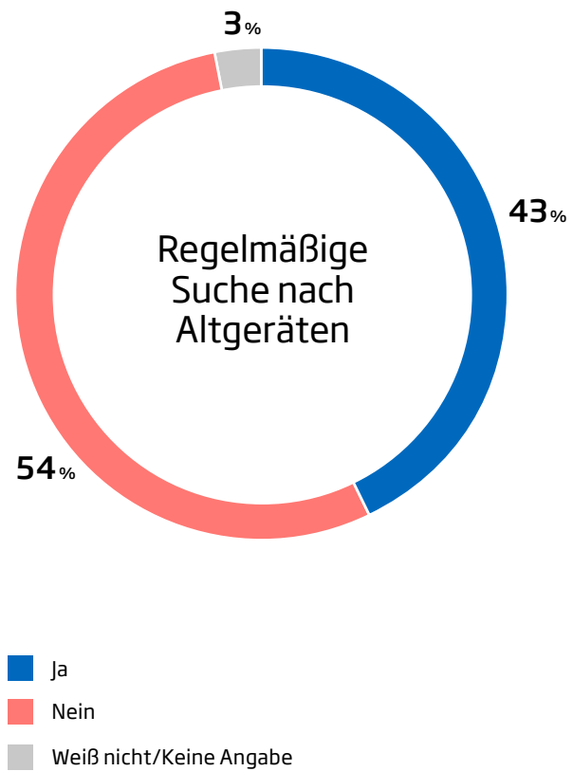
Frage: Werden alle IT- und Kommunikationsgeräte inklusive Smartphones in Ihrem Unternehmen systematisch erfasst? | Basis: Alle befragten Unternehmen (n=506)

Bei den Branchen haben Öffentliche Verwaltung sowie Gesundheits- und Sozialwesen eine Vorreiterrolle (82 Prozent). Weniger häufig ist die systematische Erfassung bei Energie, Bau und Verkehr (67 Prozent).

Die Angaben variieren je nach Funktion der Befragten im Unternehmen deutlich: 92 Prozent der CISOs, 78 Prozent der IT-Leitungen, 75 Prozent der IT-Sicherheitsverantwortlichen und 70 Prozent der CEOs berichten von einer systematischen Erfassung.

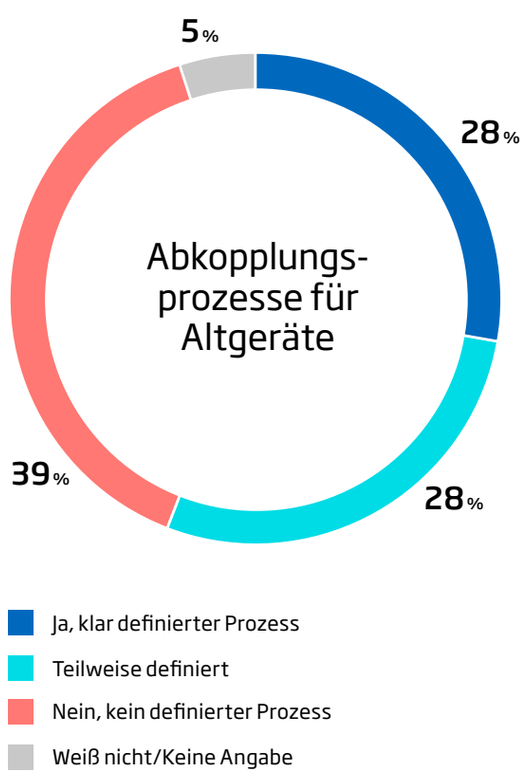
Umgang mit nicht registrierten und alten Geräten

Umgang mit Altgeräten



Fragen: Suchen Sie regelmäßig nach nicht registrierten IT-Geräten oder sogenannten Geräteleichen, also vergessenen bzw. versteckten Geräten?
Basis: Alle befragten Unternehmen (n=506)

Gibt es in Ihrem Unternehmen einen Prozess zur Abkoppelung alter Geräte und Systeme?



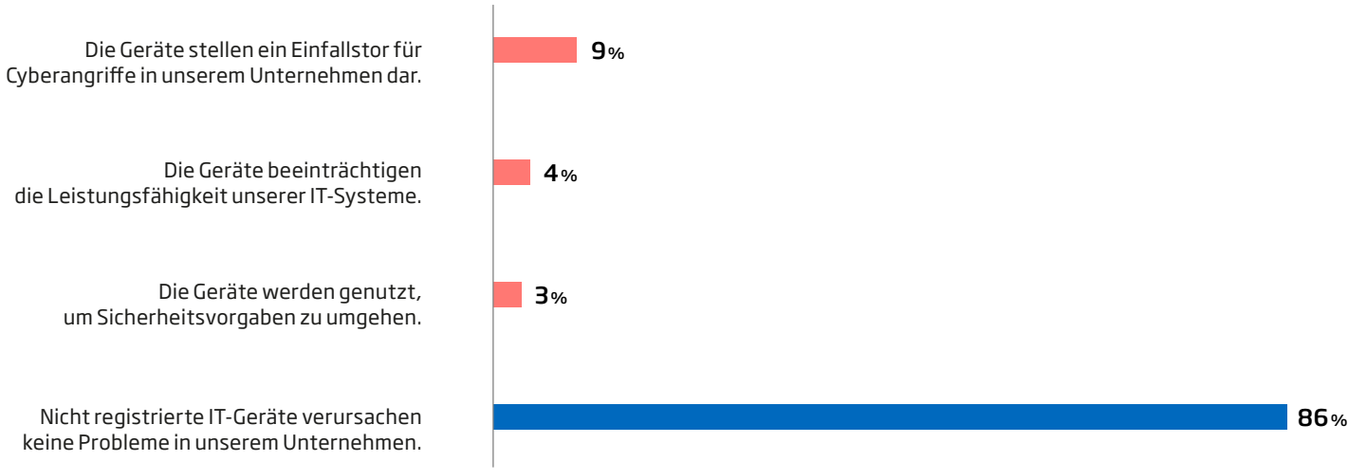
Gibt es in Ihrem Unternehmen einen Prozess zur Abkoppelung alter Geräte und Systeme?
Basis: Alle befragten Unternehmen (n=506)

Eine Minderheit sucht im Unternehmen regelmäßig nach Altgeräten, die nicht mehr genutzt werden. Ein klar definierter Prozess bildet dabei die Ausnahme.

Etwa zwei von fünf Unternehmen (43 Prozent) fahnden regelmäßig nach nicht registrierten Geräten oder nach Hardware, die nicht mehr genutzt wird oder sogar vergessen worden ist. Die Mehrheit (54 Prozent) tut dies nicht. Gut ein Viertel (28 Prozent) hat einen klar definierten Prozess für die Abkopplung alter Geräte und Systeme. Zumindest teilweise definierte Prozesse finden sich ebenfalls bei rund einem Viertel (28 Prozent). Auf einen definierten Prozess verzichten 39 Prozent der Unternehmen.

Einfallstor für Cyberangriffe – Gefahren durch Schatten-IT

Welche Probleme verursachen nicht registrierte IT-Geräte in Ihrem Unternehmen?



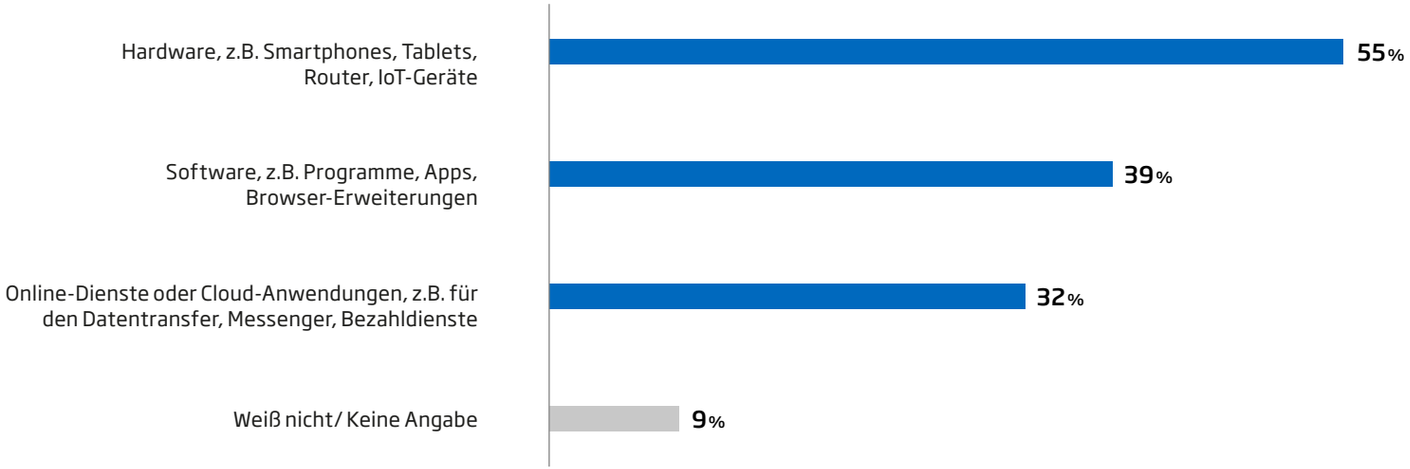
Frage: Welche Probleme verursachen nicht registrierte IT-Geräte in Ihrem Unternehmen? (Mehrfachnennungen) | Basis: Alle befragten Unternehmen (n=506)
Fehlende Angaben zu 100 Prozent Antworten für "Weiß nicht/Keine Angabe"

In vielen Unternehmen verursachen nicht registrierte IT-Geräte Sicherheitsprobleme. Die Mehrheit ist aber nicht betroffen.

Gibt es Risiken durch die Nutzung von privaten Smartphones, Notebooks oder Routern durch die Beschäftigten? Fast jedes achte Unternehmen (12 Prozent) hat Probleme mit nicht registrierten IT-Geräten. Knapp eines von zehn Unternehmen (9 Prozent) sieht in der Nutzung nicht registrierter IT-Geräte ein mögliches Einfallstor für Cyberangriffe. Immerhin 4 Prozent beobachten eine Beeinträchtigung der Leistungsfähigkeit ihrer IT-Systeme und 3 Prozent sagen, dass mit den Geräten Sicherheitsvorgaben umgangen werden. Weit überwiegend (86 Prozent) werden keine Probleme mit der Schatten-IT angenommen.

Hardware, Messenger, Apps – Herausforderung Schatten-IT

Welche nicht offiziell erfassten Geräte, Anwendungen oder Online-Services verursachen Probleme?



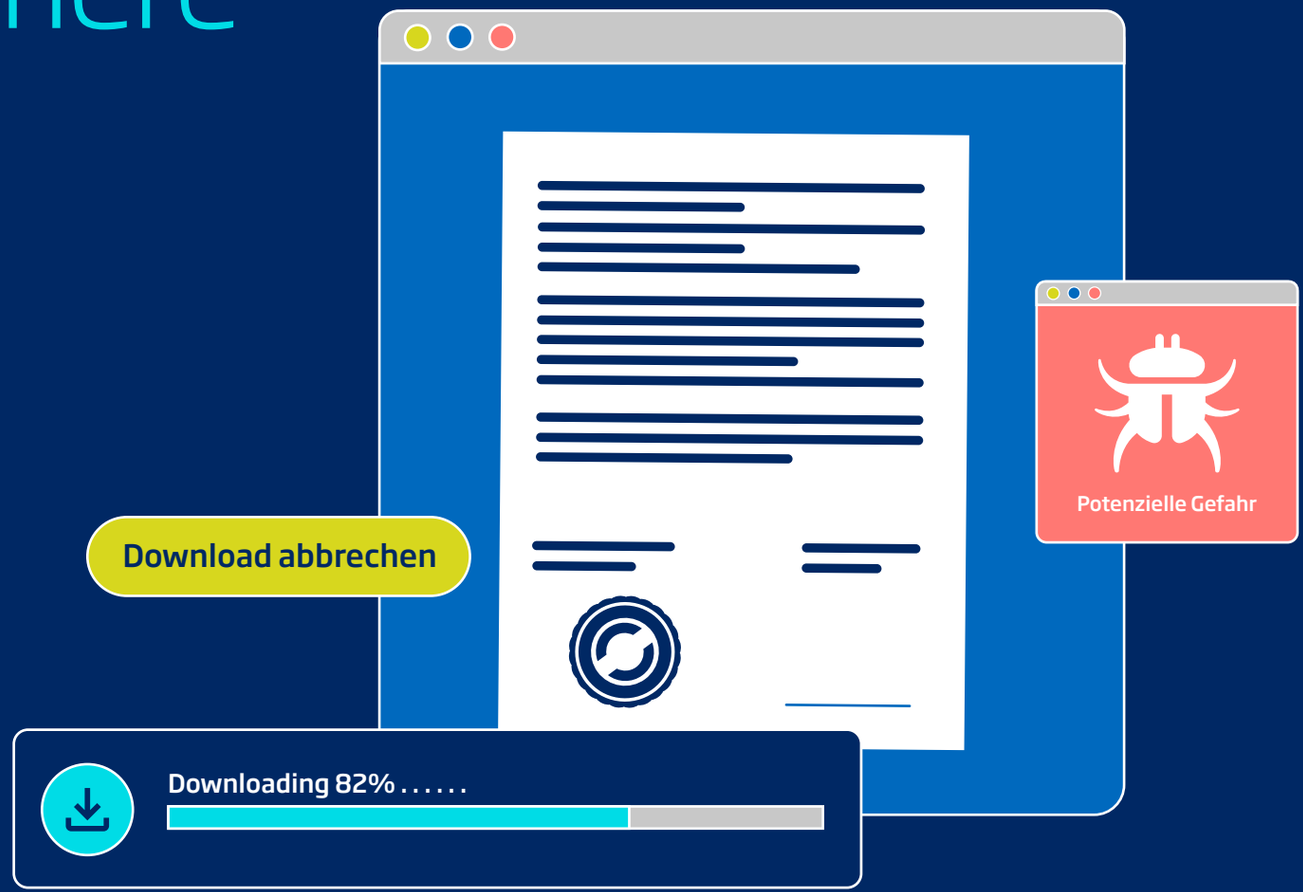
Frage: Welche nicht offiziell erfassten Geräte, Anwendungen oder Online-Services verursachen Probleme? (Mehrfachnennungen)
Basis: Unternehmen, die angaben Probleme mit Schatten-IT zu haben (n=36)

Eine Vielzahl von nicht erfassten Geräten und Anwendungen kann in Unternehmen IT-Probleme verursachen.

Smartphone, Tablet, Router: Bei Unternehmen, denen die Schatten-IT Probleme bereitet, ist überwiegend nicht erfasste Hardware der Auslöser (55 Prozent). In einer beträchtlichen Zahl der Fälle (39 Prozent) ist Software – etwa Apps oder Browser-Erweiterungen – die Ursache. Privat genutzte Online-Dienste oder im Unternehmen nicht zugelassene Cloud-Anwendungen etwa für den Datentransfer (z.B. DropBox, Google Drive) oder auch Messenger wie WhatsApp, Snapchat oder Viber sind Herausforderungen für knapp ein Drittel der Befragten (32 Prozent), die über die Schatten-IT klagen.

Normen und Standards: Grundlage für höhere Sicherheit

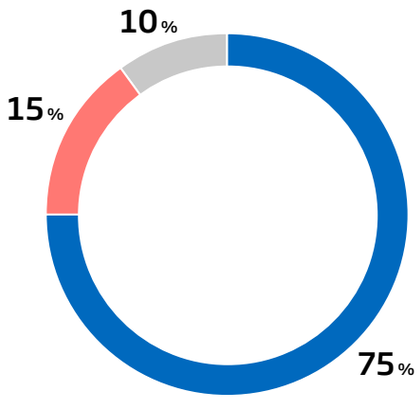
6



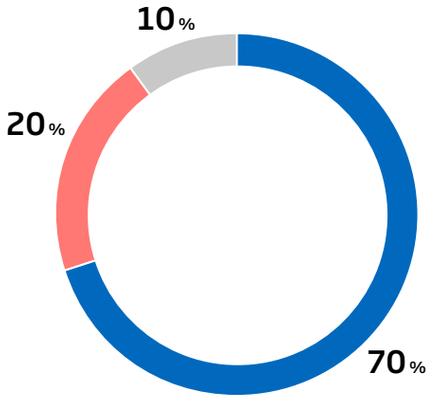
Was Normen und Standards für die Cybersicherheit leisten

Inwiefern stimmen Sie den Aussagen zu Normen und Standards für die Cybersecurity zu?

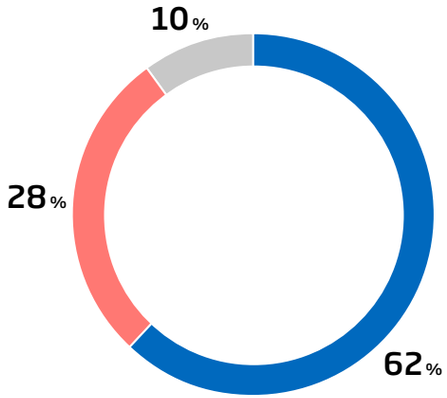
Normen und Standards geben uns Orientierung und helfen dabei Sicherheitsmaßnahmen effizient umzusetzen.



Normen und Standards für die Cybersecurity sind für uns wichtig, um den Schutz vor Cyberangriffen stetig zu verbessern.



Es fällt schwer, zu entscheiden, welche Normen und Standards für unser Unternehmen relevant sind.



Stimme voll/eher zu

Stimme eher nicht/nicht zu

Weiß nicht/Keine Angabe

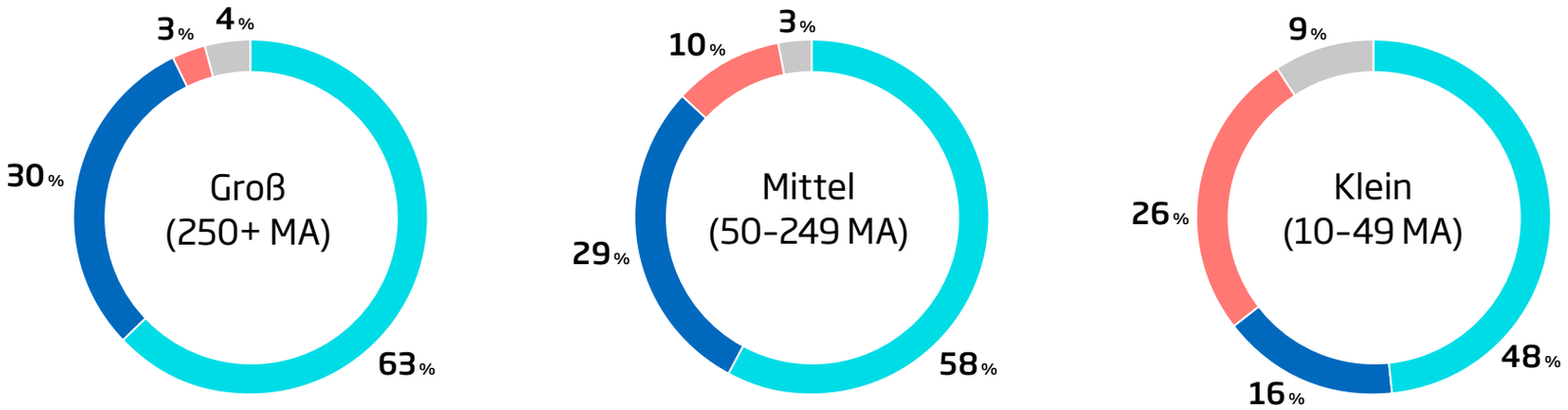
Frage: Inwiefern stimmen Sie folgenden Aussagen zu Normen und Standards für die Cybersecurity zu oder nicht zu? (Mehrfachnennungen) | Abweichungen zu 100% sind rundungsbedingt.
Basis: Alle befragten Unternehmen (n=506)

Die Mehrzahl der Unternehmen schreibt Normen und Standards einen Nutzen für die Cybersicherheit zu. Doch es fällt den meisten schwer zu entscheiden, welche davon relevant sind.

Orientierung gewinnen und Sicherheitsmaßnahmen effizient umsetzen – dazu erachten drei von vier Unternehmen Normen und Standards als hilfreich. Normen und Standards sind wichtig, um den Schutz vor Cyberangriffen stetig zu verbessern: Dieser Aussage stimmt eine deutliche Mehrheit der Unternehmen (70 Prozent) zu. Die Relevanz der einzelnen Vorgaben und Regelungen für das eigene Unternehmen zu erkennen – das fällt fast zwei von drei Befragten schwer.

Bedeutung von Normen und Standards steigt mit der Unternehmensgröße

Welche der Aussagen zu Normen und Standards für Cybersecurity trifft am ehesten auf Ihr Unternehmen zu?



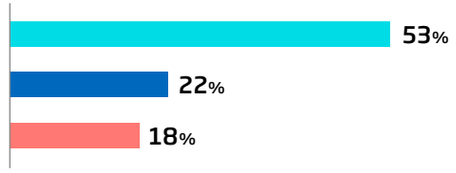
- Wir orientieren uns bei der Cybersecurity an bestimmten Normen und Standards, setzen diese aber nur teilweise um.
- Wir erfüllen bei der Cybersecurity bestimmte Normen und Standards vollumfänglich.
- Normen und Standards spielen bei der Cybersecurity bei uns bisher keine Rolle.
- Weiß nicht / Keine Angabe

Frage: Nun lese ich Ihnen drei Aussagen zu Normen und Standards für Cybersecurity im Unternehmen vor. Diese werden u.a. vom Bundesamt für Sicherheit in der Informationstechnik (BSI) oder dem Deutschen Institut für Normung (DIN) ausgearbeitet. Welche der drei Aussagen, trifft am ehesten auf Ihr Unternehmen zu? Basis: Alle befragten Unternehmen (n=506)

Besonders große und mittlere Unternehmen orientieren sich an Regelungen für die Cybersicherheit - setzen diese aber häufig nur teilweise um.

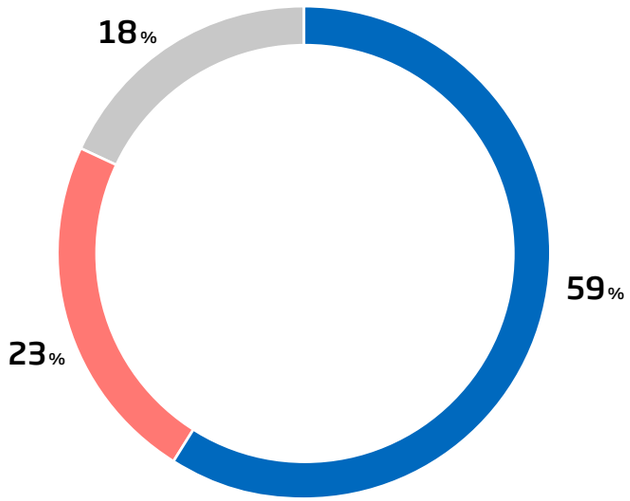
Normen und Standards für Cybersecurity in vollem Umfang erfüllen – dies geschieht vor allem bei großen und mittleren Unternehmen (30 bzw. 29 Prozent). Nur etwa halb so viele kleine Unternehmen gehen hier ähnliche konsequent vor (16 Prozent). Als Orientierung nutzen noch einmal fast zwei Drittel der großen Firmen die Regelungen (63 Prozent) – sie setzen diese aber nur teilweise um. Bei mittleren und kleinen Unternehmen liegt dieser Wert etwas niedriger (58 bzw. 48 Prozent). Keine Rolle spielen Standards und Normen für Cybersicherheit eher bei kleinen Unternehmen (26 Prozent).

Gesamt

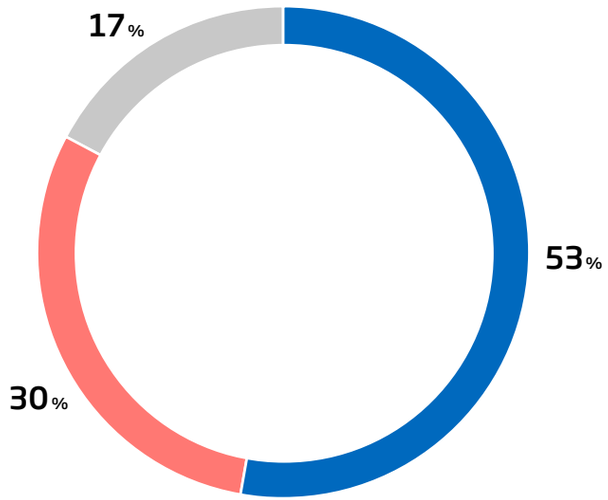


Kosten und Komplexität bremsen die Umsetzung von Standards

Inwiefern stimmen Sie folgenden Aussagen zu Normen und Standards für die Cybersecurity zu?



Die Einhaltung der Normen und Standards ist für uns mit zu hohen Kosten verbunden.



Die vorhandenen Normen und Standards für Cybersecurity sind zu technisch und schwer zu verstehen.

- Stimme voll/eher zu
- Stimme eher nicht/gar nicht zu
- Weiß nicht/Keine Angabe

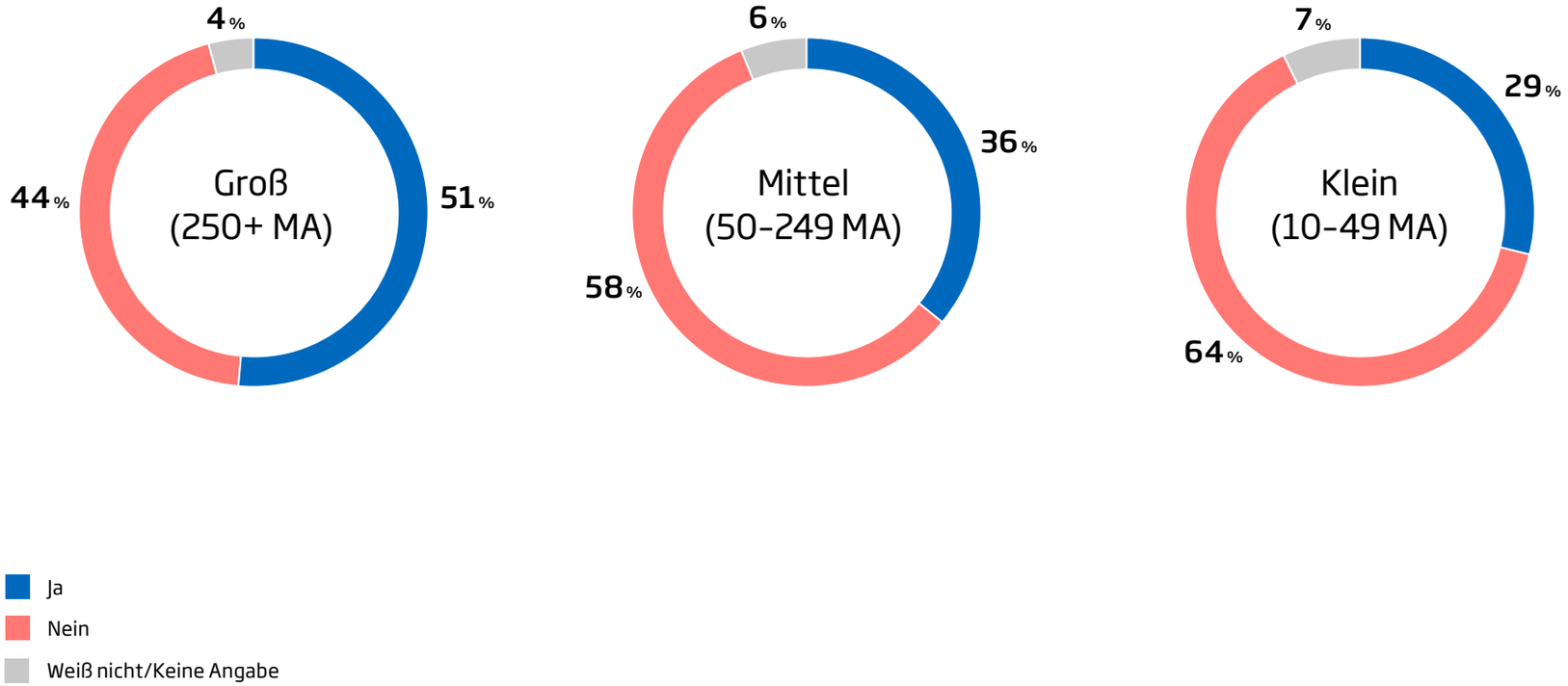
Frage: Inwiefern stimmen Sie folgenden Aussagen zu Normen und Standards für die Cybersecurity zu oder nicht zu? (Mehrfachnennungen) | Basis: Alle befragten Unternehmen (n=506)

Zu teuer, zu schwer verständlich – bei Normen und Standards fühlen sich viele Unternehmen überfordert.

Welche Cybersecurity-Normen und -Standards sind für das eigene Unternehmen relevant? Für eine beträchtliche Zahl von Unternehmen ist es schwierig, hier Antworten zu finden. Gut die Hälfte der Befragten (53 Prozent) bewertet die bestehenden Regelungen als zu technisch und schwer zu verstehen. Fast ein Drittel hat damit keine Probleme und fast ein Fünftel (17 Prozent) kann dazu keine Angaben machen. Als noch schwerwiegenderes Hindernis für die Umsetzung der Normen und Standards erweist sich der Kostendruck. Fast drei von fünf Unternehmen (59 Prozent) bewerten die Einhaltung der Regelungen als zu teuer, auch wenn die Umsetzung dieser gleichzeitig das Risiko eines kostenintensiven Cybersicherheitsvorfalls reduziert. Für fast jedes vierte Unternehmen (23 Prozent) sind die Kosten kein Hindernis.. Auch hier antworten 18 Prozent mit „Weiß nicht“, was auf eine geringe Kenntnis der entsprechenden Normen und Standards hindeutet.

Ein Drittel lässt Einhaltung von Cybersecurity-Standards prüfen

Lassen Sie die Einhaltung von Normen und Standards für Cybersecurity von unabhängigen Stellen überprüfen bzw. zertifizieren?

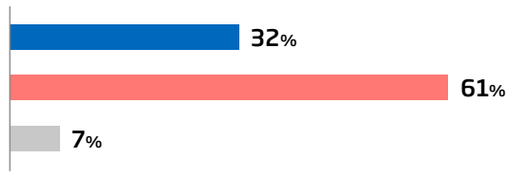


Frage: Lassen Sie die Einhaltung von Normen und Standards für Cybersecurity von unabhängigen, externen Stellen überprüfen bzw. zertifizieren?
Basis: Alle befragten Unternehmen (n=506)

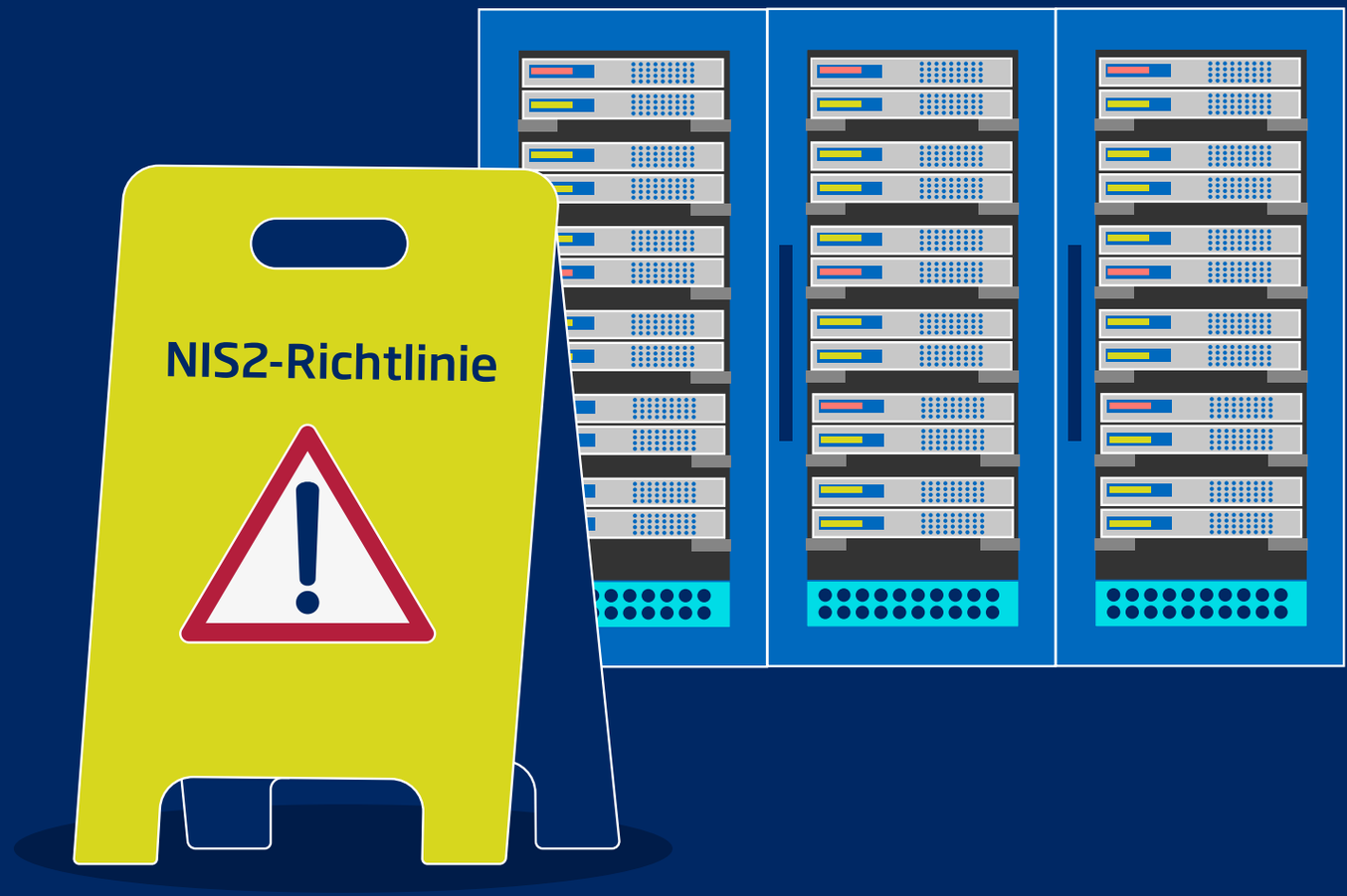
Die Mehrheit verzichtet auf die unabhängige Zertifizierung von Normen und Standards, die die IT-Sicherheit betreffen.

Wie wichtig ist Unternehmen die externe Beurteilung und Kontrolle ihrer IT-Sicherheit? Knapp ein Drittel (32 Prozent) legt Wert darauf, dass unabhängige Stellen die Einhaltung von cybersicherheitsrelevanten Normen und Standards bestätigen. Die Mehrheit (61 Prozent) verzichtet auf die externe Zertifizierung. Es sind vor allem Großunternehmen (51 Prozent), die sich zertifizieren lassen. Bei den mittelständischen Unternehmen sind es 39 Prozent und bei den Kleinunternehmen 29 Prozent.

Gesamt



Gesetzliche Vorgaben für mehr Cybersicherheit

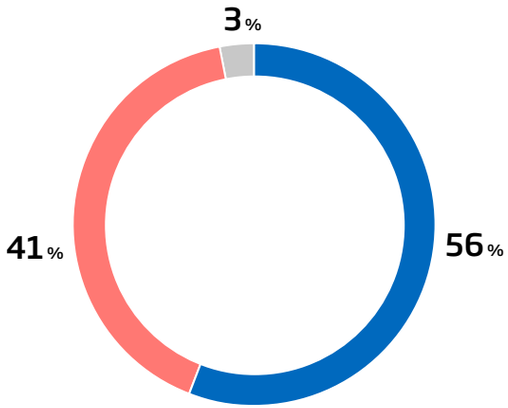


7

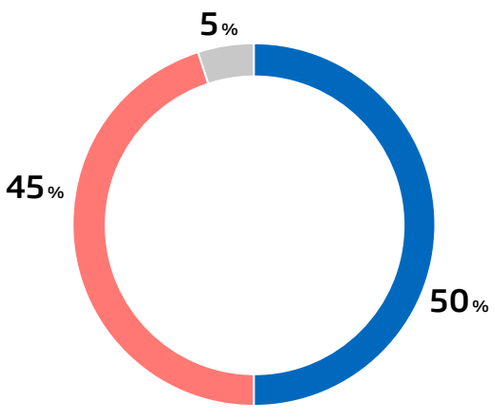
Mehrheit befürwortet gesetzliche Vorgaben für Cybersicherheit

Aussagen zur politischen Regulierung von Cybersecurity

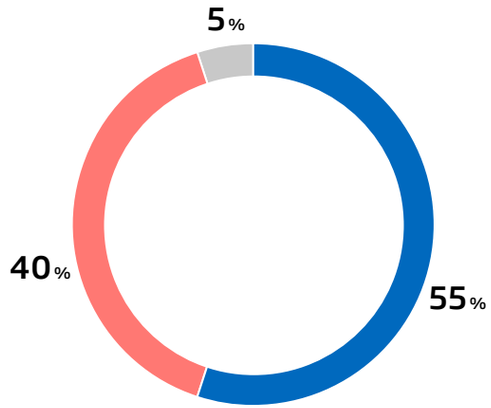
Jedes Unternehmen sollte gesetzlich verpflichtet sein, angemessene Maßnahmen für seine Cybersecurity zu ergreifen.



Die gesetzlichen Vorgaben für die Cybersecurity von Unternehmen müssen erhöht werden.



Strengere gesetzliche Vorgaben für die Cybersecurity von Unternehmen machen das ganze Internet sicherer.



- Stimme voll/eher zu
- Stimme eher nicht/nicht zu
- Weiß nicht/Keine Angabe

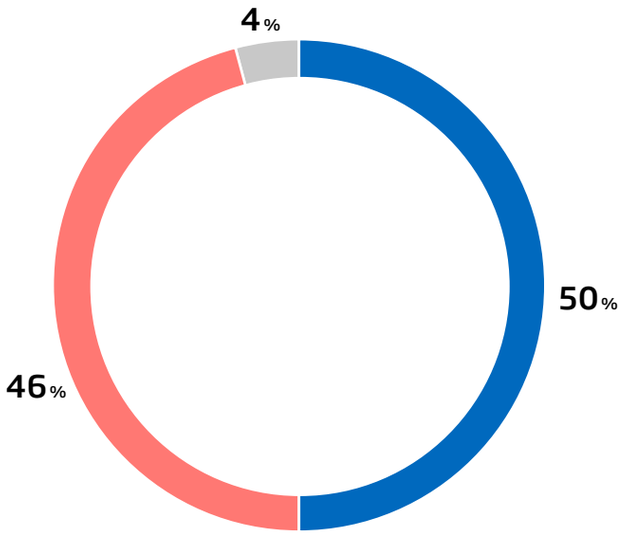
Frage: Ich lese Ihnen nun einige Aussagen zum Thema politische Regulierung von Cybersecurity vor. Inwiefern stimmen Sie diesen zu oder nicht zu? | Basis: Alle befragten Unternehmen (n=506)

Sollte der Staat stärker eingreifen, um die Wirtschaft zu einer höheren Cybersicherheit zu bewegen? Eine knappe Mehrheit der Unternehmen stimmen zu.

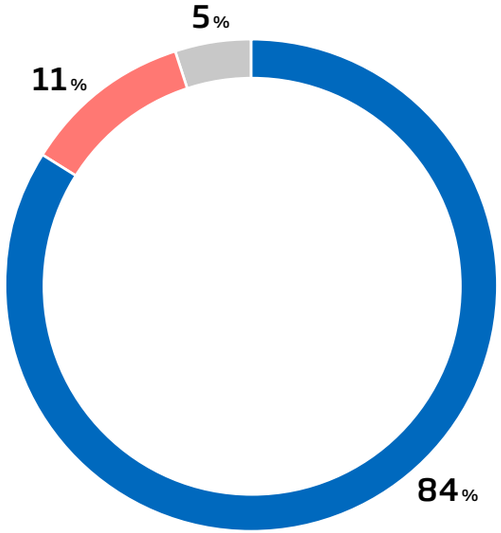
Mit einem Anteil von 56 Prozent spricht sich eine Mehrheit der Befragten dafür aus, dass jedes Unternehmen gesetzlich dazu verpflichtet sein sollte, angemessene Maßnahmen für seine Cybersicherheit zu ergreifen. 41 Prozent sind gegenteiliger Meinung. Große und mittlere Unternehmen liegen über dem Schnitt (59 Prozent und 63 Prozent), kleinere mit 10 bis 49 Mitarbeitenden etwas darunter (54 Prozent). Jedes zweite Unternehmen (50 Prozent) spricht sich sogar für strengere gesetzliche Vorgaben für Cybersecurity aus, 45 Prozent sind dagegen. Auch hier sind es mittlere und große Unternehmen, die sich mehrheitlich für strengere Anforderungen aussprechen (56 Prozent bzw. 54 Prozent). Kleinere Unternehmen liegen mit 47 Prozent unter dem Durchschnitt. Der Aussage, dass strengere gesetzlichen Vorgaben für Unternehmen das Internet insgesamt sicherer machen, stimmen 55 Prozent aller Befragten zu. 40 Prozent sind gegenteiliger Meinung.

Strengere Anforderungen führen zu mehr Sicherheit

Aussagen zur politischen Regulierung von Cybersecurity



Strengere gesetzliche Vorgaben helfen uns dabei, zusätzliche Maßnahmen für Cybersecurity umzusetzen.



IT-Sicherheitsvorfälle helfen dabei, das Thema Cybersicherheit bei der Unternehmensleitung zu priorisieren.

- Stimme voll/eher zu
- Stimme eher nicht/nicht zu
- Weiß nicht/Keine Angabe

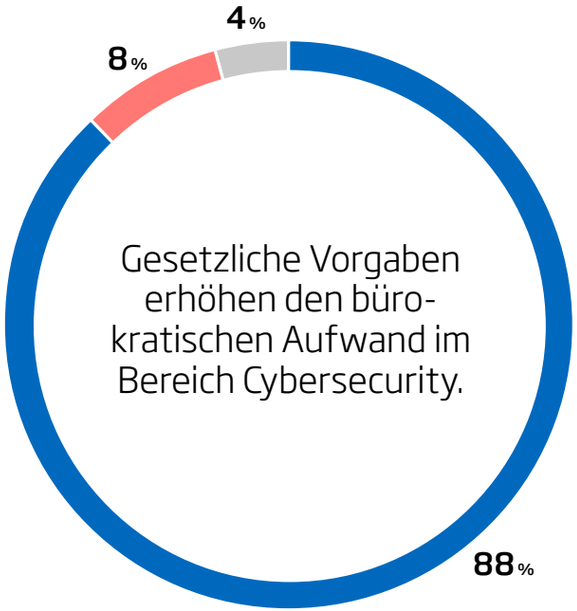
Ich lese Ihnen nun einige Aussagen zum Thema politische Regulierung von Cybersecurity vor. Inwiefern stimmen Sie diesen zu oder nicht zu?
Basis: Alle befragten Unternehmen (n=506)

Gesetzliche Vorgaben helfen vielen Unternehmen dabei, ihr Schutzniveau zu erhöhen. Häufig braucht es aber erst einen IT-Sicherheitsvorfall, um das Thema zu priorisieren.

Jeder zweite IT-Verantwortliche gibt an, dass strengere gesetzliche Vorgaben dabei helfen, zusätzliche Maßnahmen für die Cybersicherheit umzusetzen. Eine hohe Zustimmung gibt es bei der Frage, ob IT-Sicherheitsvorfälle dafür sorgen, dass das Management dem Thema Cybersicherheit eine höhere Priorität einräumt (84 Prozent).

Mehraufwand durch regulatorische Vorgaben

Aussagen zur politischen Regulierung von Cybersecurity



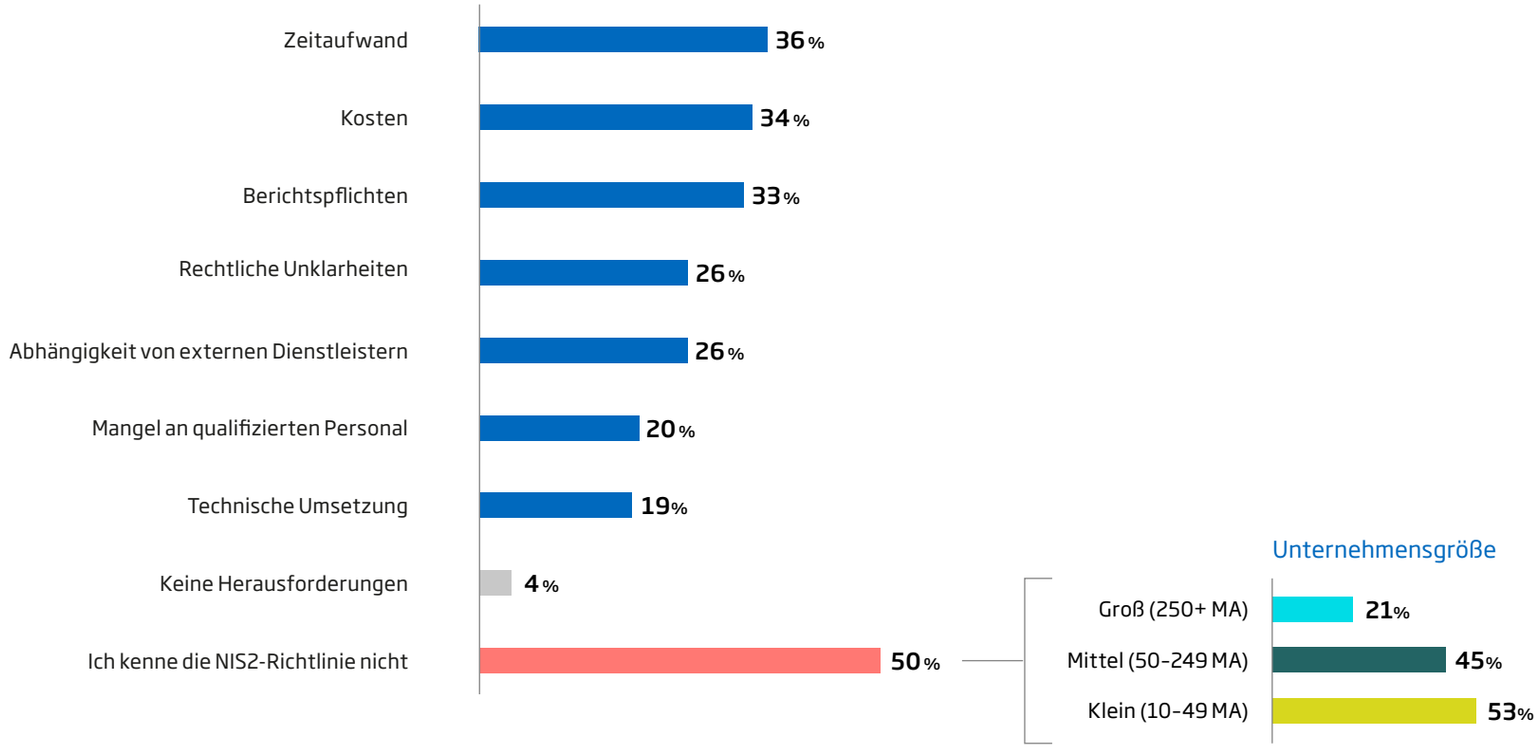
Frage: Ich lese Ihnen nun einige Aussagen zum Thema politische Regulierung von Cybersecurity vor. Inwiefern stimmen Sie diesen zu oder nicht zu?
Gesetzliche Vorgaben erhöhen den bürokratischen Aufwand im Bereich Cybersecurity. | Basis: Alle befragten Unternehmen (n=506)

Gesetzliche Vorgaben erhöhen den bürokratischen Aufwand – dennoch werden strengere Regelungen zumindest dann mehrheitlich befürwortet, wenn sie zu angemessenen Maßnahmen führen

Fast neun von zehn Befragten (88 Prozent) nehmen an, dass gesetzliche Vorgaben für IT-Sicherheit den bürokratischen Aufwand steigern. In der Praxis müssen Unternehmen ihre Maßnahmen für die IT-Sicherheit mit dem entsprechenden Regelwerk abgleichen. Im Fall eines Cyberangriffs greifen für viele Unternehmen bestimmte Informations- und Meldepflichten. Zumindest Letzteres lässt sich durch die Verhinderung von Cyberangriffen deutlich reduzieren. Das gilt auch für den hohen organisatorischen Aufwand, der nach einem erfolgreichen Cyberangriff entsteht.

EU-Regulierung bringt Herausforderungen mit sich

Welche Herausforderungen sehen Sie bei der Umsetzung der NIS2-Richtlinie in Ihrem Unternehmen?



Frage: Welche Herausforderungen sehen Sie bei der Umsetzung der NIS2-Richtlinie in Ihrem Unternehmen? (Mehrfachnennungen)
Basis: Alle befragten Unternehmen (n=506)

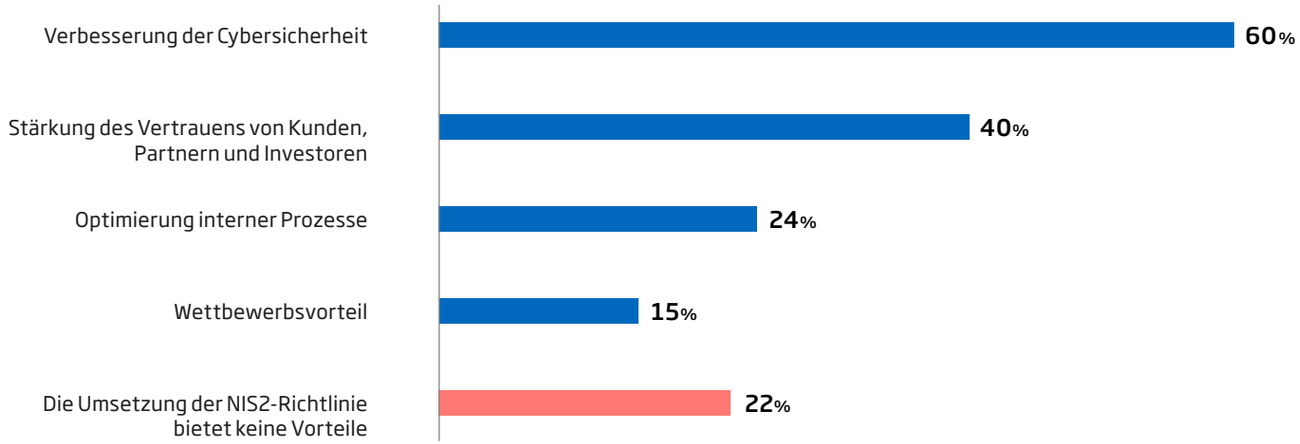
Eine Vielzahl von Faktoren erhöht aus Sicht der Unternehmen den Aufwand, der mit der NIS2-Richtlinie verbunden ist. Häufig fehlt aber noch Wissen über die EU-Regelung für mehr Cybersicherheit.

Wer ist betroffen? Welche Maßnahmen sind notwendig? Wie hoch ist der Aufwand? Mit Blick auf die europäischen NIS2-Richtlinie (Network and Information Security Directive), die auf eine Stärkung der Cybersicherheit der Wirtschaft zielt, fehlt in vielen Unternehmen das Wissen. Die Hälfte der Befragten (50 Prozent) kennt diese europäische Regulierung nicht. Vor allem kleinen (53 Prozent) und mittleren Unternehmen (45 Prozent) ist die Richtlinie unbekannt. Unter den großen Unternehmen sind es dagegen nur 21 Prozent. Je nach Rolle variiert der Kenntnisstand deutlich: 61 Prozent der CEOs geben an, NIS2 nicht zu kennen, bei IT-Leitungen sind es 38 Prozent, bei IT-Sicherheitsverantwortlichen 46 Prozent und bei CISOs nur 27 Prozent.

Bei der Umsetzung sehen die Befragten eine Reihe von Herausforderungen. Besonders häufig genannt werden der Zeitaufwand (36 Prozent), die Kosten (34 Prozent) und die Berichtspflichten (33 Prozent) – gefolgt von rechtlichen Unklarheiten und der Abhängigkeit von externen Dienstleistern (je 26 Prozent). Eine Minderheit (4 Prozent) sieht keine Herausforderungen.

Sicherheitsgewinn durch Network and Information Security Richtlinie NIS2

Welche Vorteile bietet die Umsetzung der NIS2-Richtlinie in Ihrem Unternehmen?



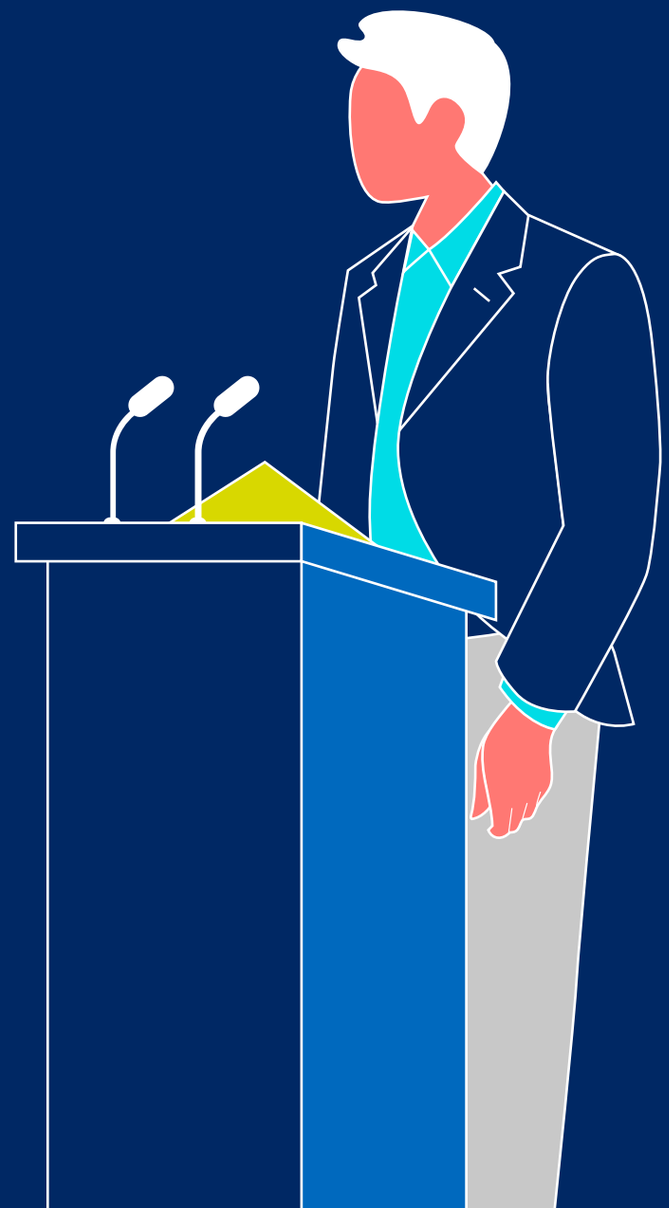
Frage: Welche Vorteile bietet die Umsetzung der NIS2-Richtlinie in Ihrem Unternehmen? (Mehrfachnennungen)
Basis: Unternehmen, welche von den NIS2-Richtlinien wissen (n= 281)

Die Mehrheit der Unternehmen, die mit der geplanten EU-Regelung vertraut sind, ist von deren Vorteilen überzeugt.

Das Kernziel Network and Information Security Richtlinie (NIS2) der Hälfte nicht bekannt wird nach Ansicht der Mehrheit erreicht – 60 Prozent der Befragten, die das Gesetzesvorhaben kennen, erwarten eine Verbesserung der Cybersicherheit. Darüber hinaus gehen 40 Prozent davon aus, dass die EU-Regelung das Vertrauen von Kunden oder Investoren stärkt. Einen Wettbewerbsvorteil durch die NIS2-Richtlinie erhofft sich knapp eines von sieben Unternehmen. Ein Viertel der Unternehmen geht davon aus, dass sich dank der Vorgabe interne Prozesse verbessern. Gut jeder fünfte Befragte geht davon aus, dass die NIS2-Richtlinie keine Vorteile bringen wird.

Fazit und politische Empfehlungen

8



Fazit

Die Gefahr durch Cyberangriffe ist der Mehrheit der Unternehmen bewusst – für drei von vier spielt IT-Sicherheit eine große Rolle. Mit steigender Unternehmensgröße nimmt die Bedeutung von Cybersicherheit zu. Die stärkste Bedrohung geht laut Umfrage von organisierten Kriminellen und staatlichen Hackern aus. Unterschätzt wird das Risiko, über die IT-Systeme von Zulieferern oder Kunden attackiert zu werden – hier erkennen gut drei Viertel keine oder eine geringe Gefahr. Dabei hat ein Zehntel solche Angriffe bereits erlebt.

Insgesamt ist die Zahl der erfolgreichen Cyberangriffe im Vergleich zur letzten Erhebung deutlich gestiegen. 15 Prozent der Unternehmen verzeichneten binnen eines Jahres mindestens einen IT-Sicherheitsvorfall – im Jahr 2023 lag dieser Wert noch bei 11 Prozent. Künstliche Intelligenz erhöht die Gefahr von IT-Angriffen – rund die Hälfte der Unternehmen ist der Ansicht, dass Cyberkriminelle diese nutzen, um gezielt Schwachstellen in ihren IT-Systemen auszuspüren oder täuschend echte Phishing-Mails zu formulieren. Auf der anderen Seite rüstet sich jedes fünfte Unternehmen mithilfe von KI, um Cyberangriffe besser abzuwehren. Dennoch besteht hier ein Ungleichgewicht. Während kriminelle Hacker nur eine Schwachstelle finden müssen, um einen erfolgreichen Angriff zu starten, müssen Unternehmen eine Vielzahl von potenziellen Einfallstoren im Blick haben.

Grundsätzlich bewertet die breite Mehrheit ihre Cybersicherheit als effektiv. Das steht in Kontrast zu den zahlreichen IT-Sicherheitsvorfällen, die mitunter schwere Schäden verursachen. Rund ein Viertel der Unternehmen hat das Budget für Cybersecurity in den vergangenen beiden Jahren erhöht – 2023 war das noch bei der Hälfte der Fall. Die Skepsis gegenüber der Cloud bleibt beträchtlich – etwa ein Viertel verzichtet darauf aus Sicherheitsgründen. Ebenfalls ein Viertel allerdings nutzt die Cloud gerade mit Blick auf einen besseren Schutz vor Cyberangriffen. Gespeichert werden Daten von einer breiten Mehrheit ausschließlich auf Servern innerhalb der EU.

Normen und Standards sehen drei Viertel als hilfreich an, um Sicherheitsmaßnahmen effizient umzusetzen – sie werden auch von einer deutlichen Mehrheit als wichtig für den Cyberschutz erachtet. Ein Drittel der Unternehmen lässt sich mit Blick auf die Vorgaben zertifizieren. Allerdings besteht Aufklärungsbedarf – vielen Unternehmen fällt es schwer zu entscheiden, welche Normen und Standards für sie relevant sind. Zudem sind Kosten und Verständnisprobleme der technischen Regelungen für viele ein Hindernis. Regulierung ist in der Wirtschaft in der Regel verpönt, weil sie Aufwand und Kosten verursacht. Allerdings erkennt die Mehrheit an, dass strengere Vorschriften das Schutzniveau erhöhen und das Internet insgesamt sicherer machen. Eine höhere Cybersicherheit verspricht die NIS2-Richtlinie der Europäischen Union. Auch hier erwarten die Unternehmen einen Mehraufwand. Beträchtlich ist aber der Anteil derjenigen, die eine Stärkung des Vertrauens zu Kunden, Partnern und Investoren oder einen Wettbewerbsvorteil durch die neue Richtlinie erwarten.

Politische Empfehlungen

Die Cyberbedrohungslage hat sich seit der TÜV-Cybersecurity-Studie 2023 weiter verschärft. Unternehmen und Betreiber kritischer Infrastrukturen in Deutschland und Europa sind zunehmend gezielten, hybriden Angriffen ausgesetzt – sowohl durch staatliche Akteure als auch durch hochprofessionelle Cyberkriminelle. Die Politik hat darauf mit wichtigen regulatorischen Maßnahmen reagiert: Auf EU-Ebene greifen der Cyber Resilience Act, die NIS-2-Richtlinie und der Cybersecurity Act ineinander. Doch die nationale Umsetzung – etwa beim NIS-2-Umsetzungsgesetz – verläuft bislang schleppend. Das führt zu Rechtsunsicherheit, unklaren Zuständigkeiten und fehlenden Ressourcen in den Unternehmen. Entscheidend ist jetzt, das Cybersicherheitsrecht zügig wirksam werden zu lassen und weitere Verzögerungen zu vermeiden.

Um die Cybersicherheit in den Unternehmen zu erhöhen, empfiehlt der TÜV-Verband:

›› Auftrag für die neue Bundesregierung: Cybersicherheit voranbringen!

Das neu geschaffene Bundesministerium für Digitales und Staatsmodernisierung (BMDS) und das Bundesinnenministerium müssen Cybersicherheit priorisieren und das Thema in die übergeordnete Sicherheitsstrategie der Bundesregierung eingebunden werden. Die Kompetenzen und Zuständigkeiten zwischen den Ministerien und dem BSI müssen klar geregelt, die Cybersicherheitsagenda aktualisiert und Förderprogramme neu ausgerichtet werden.

›› Schutzniveau erhöhen: Cybersecurity-Regulierung zügig umsetzen

Bei der Umsetzung der europäischen NIS2-Richtlinie ist Deutschland stark in Verzug. Die Bundesregierung muss das nationale Umsetzungsgesetz zügig auf den Weg bringen. Der Cyber Resilience Act (CRA) gilt als EU-Verordnung erst ab Dezember 2027 und muss wie geplant umgesetzt werden. Jetzt geht es darum, das Schutzniveau zu erhöhen und Staat, Wirtschaft und Zivilgesellschaft widerstandfähiger gegen kriminelle und staatliche Cyberangriffe zu machen. Richtig ist, die Qualität, Praxistauglichkeit und Effektivität gesetzlicher Anforderungen zu verbessern – ohne dabei das Schutzniveau zu gefährd

Empfehlungen für Unternehmen

Um die Cybersicherheit in den Unternehmen zu erhöhen, empfiehlt der TÜV-Verband:

» Cyberrisiken ernst nehmen!

Unternehmen sollten eine qualifizierte Risikoanalyse durchführen und diese angesichts des dynamischen technologischen und geopolitischen Umfelds regelmäßig aktualisieren. Was ist besonders zu schützen? Welche Bedrohungen gibt es? Was sind potenzielle Schwachstellen im Unternehmen? Diese und weitere Fragen gilt es zu beantworten. Je nach Größe, Branche und Tätigkeitsgebiet können Cyberrisiken sehr unterschiedlich bewertet werden.

» Cybersecurity-Strategie entwickeln

Übergeordnetes Ziel der Strategie ist es, ein angemessenes Sicherheitslevel für das jeweilige Unternehmen zu definieren. Bestandteil dessen sollte eine IT-Sicherheitsrichtlinie sein. In dieser werden messbare Ziele definiert, konkrete Sicherheitsanforderungen festgelegt und klare Verantwortlichkeiten geschaffen. Sie ist die Basis für die Maßnahmenplanung.

» Maßnahmenplan ausarbeiten

Auf Grundlage der Risikoanalyse und der strategischen Überlegungen können konkrete Maßnahmen festgelegt werden.
Der TÜV-Verband empfiehlt, aktuell folgende Punkte zu berücksichtigen:

- Vorsorge statt Nachsorge
  Präventiv eigene Schwachstellen identifizieren – zum Beispiel durch entsprechende Pentests.

- Unternehmen krisenfest machen
  Notfallübungen durchführen, um Abläufe für den Ernstfall einzuüben.

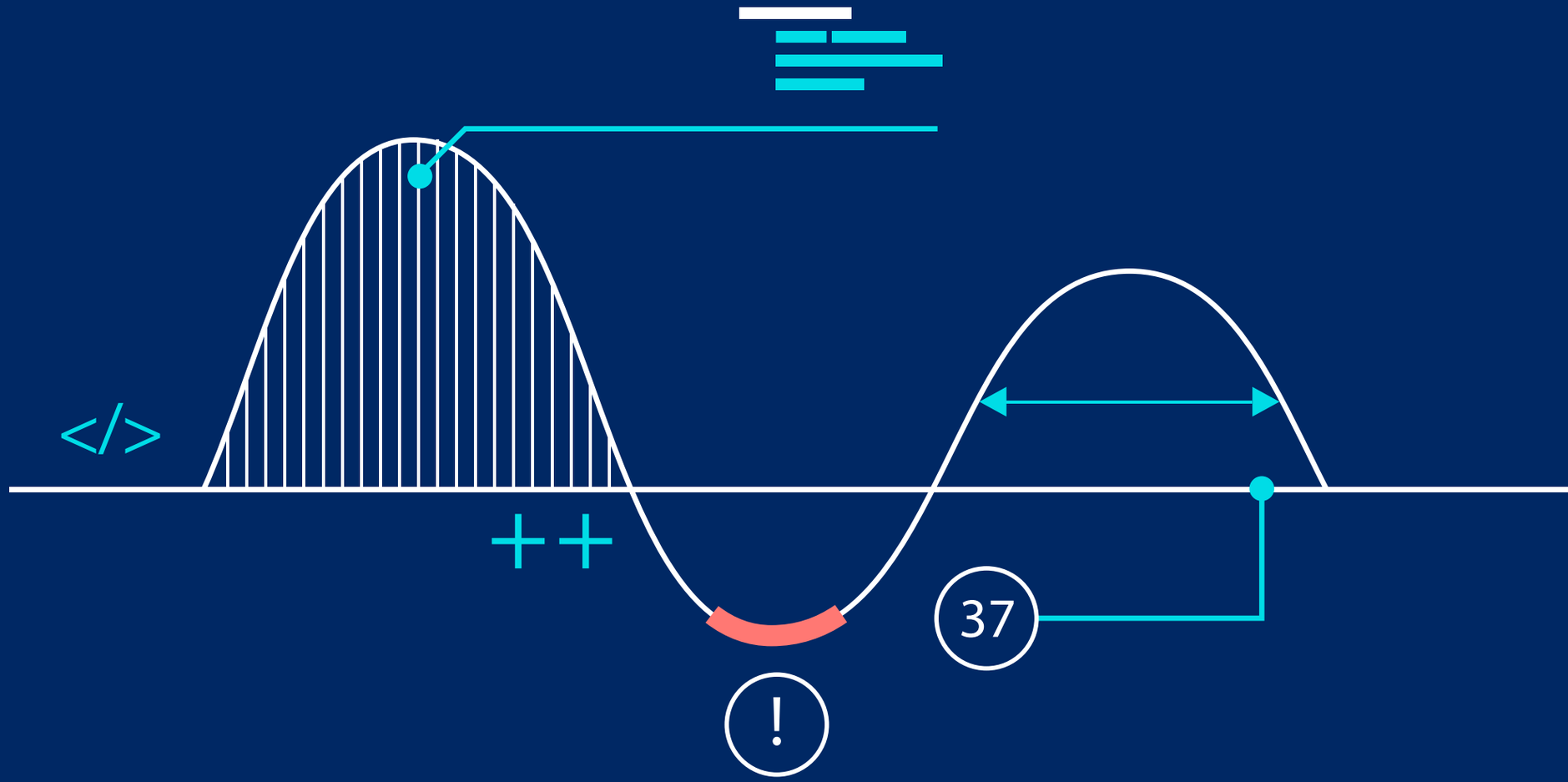
- Cybersicherheit mit Künstlicher Intelligenz stärken
  Konzept für den Einsatz von KI für die Cyberabwehr entwickeln, entsprechende Tools testen, externe Beratungsangebote nutzen.

- Know-how is key!
  Mitarbeitende qualifizieren, IT-Spezialisten einstellen und regelmäßig fortbilden, Mitarbeitende zu aktuellen Angriffsmethoden schulen.

- Normen und Standards nutzen
  Normen und Standards geben Orientierung und bringen die IT-Sicherheit auf ein höheres Level.

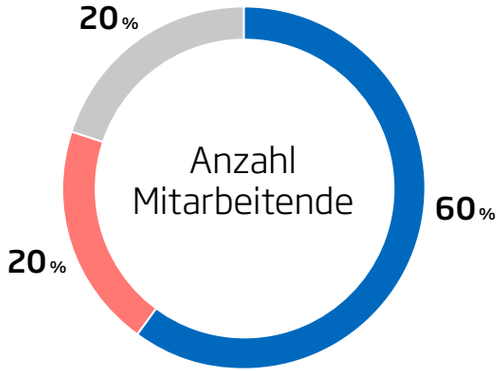
- Altgeräte und Altsysteme nicht vernachlässigen
  Altgeräte und Altsysteme sind häufig Einfallstor für Cyberangriffe. Prozesse für die Außerbetriebnahme und Entsorgung etablieren.

Methodik

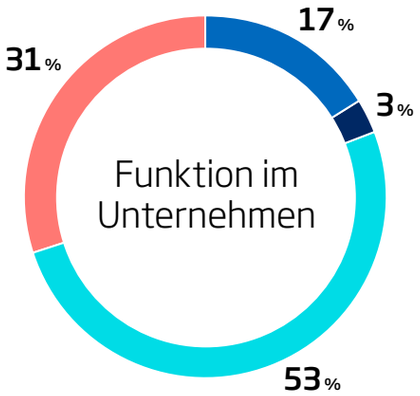


Methodik

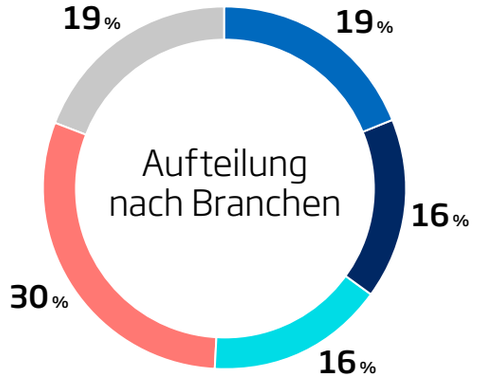
Die Umfrage wurde von der Ipsos GmbH im Auftrag des TÜV-Verbands durchgeführt. Die Interviews erfolgten mittels einer telefonischen CATI-Befragung zwischen 18. Februar und 14. März 2025. Basis: 506 befragte Unternehmen



- Zwischen 10 und 49 Mitarbeitern
- Zwischen 50 und 249 Mitarbeitern
- Mehr als 250 Mitarbeiter



- IT-Leitung / CIO
- Chief Information Security Officer (CISO)
- Verantwortliche/r für IT-Sicherheit
- Geschäftsführung oder Vorstand



- Industrie
- Energie, Bau und Verkehr
- Handel
- Dienstleistungen
- Öffentlicher Bereich / Gesundheit

Über den TÜV-Verband

Als TÜV-Verband e. V. vertreten wir die politischen Interessen der TÜV-Prüforganisationen und fördern den fachlichen Austausch unserer Mitglieder. Wir setzen uns für die technische und digitale Sicherheit sowie die Nachhaltigkeit von Fahrzeugen, Produkten, Anlagen und Dienstleistungen ein. Grundlage dafür sind allgemeingültige Standards, unabhängige Prüfungen und qualifizierte Weiterbildung. Unser Ziel ist es, das hohe Niveau der technischen Sicherheit zu wahren, Vertrauen in die digitale Welt zu schaffen und unsere Lebensgrundlagen zu erhalten. Dafür sind wir im regelmäßigen Austausch mit Politik, Behörden, Medien, Unternehmen und Verbraucher:innen.

TÜV VERBAND

Ansprechpartner:innen

Dr. Joachim Bühler
Geschäftsführer
Tel. +49 30 760095-400
joachim.buehler@tuev-verband.de

Marc Fliehe
Fachbereichsleiter Digitalisierung und Bildung
+49 30 760095-460
marc.fliehe@tuev-verband.de

Maurice Shahd
Leiter Kommunikation
Tel. +49 30 760095-320
maurice.shahd@tuev-verband.de

Linda Roy
Pressesprecherin
Tel. +49 30 760095-580
linda.roy@tuev-verband.de

TÜV-Verband e. V.
Friedrichstraße 136
10117 Berlin
Tel. +49 30 760095-400
berlin@tuev-verband.de
www.tuev-verband.de

Grafik & Design

Nordpunkt Designagentur GmbH