TÜV®

Cybersecurity Studie

Eine repräsentative Untersuchung im Auftrag des TÜV-Verbands zur IT-Sicherheit von Unternehmen in Deutschland

Vorwort

Die digitale Vernetzung von Produkten und Anlagen stellt viele Unternehmen vor große Herausforderungen. Zum einen müssen sie mit den sich rasant entwickelnden technischen Innovationen Schritt halten, zum anderen sind sie ständig neuen Sicherheitsrisiken ausgesetzt. Die Abwehr von Cyberangriffen steht bei vielen Unternehmen daher zu Recht ganz oben auf der Agenda ihrer IT-Sicherheitsmaßnahmen. Bereits heute zirkulieren weltweit 800 Millionen Schadprogramme, täglich kommen 390.000 weitere hinzu. Entsprechend häufig finden Cyberangriffe statt, wobei nur die besonders spektakulären Ereignisse überhaupt öffentlich bekannt werden. Dabei haben es Cyberkriminelle längst nicht mehr nur auf große Unternehmen abgesehen.

Welche Maßnahmen ergreifen Unternehmen, um sich zu schützen? Welchen Stellenwert hat die IT-Sicherheit? Wo liegen Defizite und vor allem: Was schlagen die betroffenen Unternehmen vor, um die IT-Sicherheit in der Wirtschaft zu verbessern? Die vorliegende Studie kommt hier zu teilweise überraschenden Ergebnissen: Es sind die Unternehmen selbst, die eine stärkere Regulierung und eine Verschärfung des gesetzlichen Rahmens für ihre IT-Sicherheit fordern. So gehen etwa einem Drittel der Unternehmen die Maßnahmen des bestehenden IT-Sicherheitsgesetzes nicht weit genug.

Besonders hoch ist der Wunsch nach Transparenz, etwa bei den Anforderungen durch umfangreiche Normen und hohe Standards für IT-Sicherheit. Zwei Drittel der befragten Unternehmen halten sie für wichtig, um den Schutz vor Cyberangriffen stetig zu verbessern. Es verwundert daher nicht, dass sich vor allem die größeren Unternehmen unabhängige Institutionen wie den TÜV als Partner wünschen, um durch Prüfungen oder Zertifizierungen für ein höheres IT-Sicherheitsniveau zu sorgen.

Mit der Forderung nach stärkerer Regulierung und höheren gesetzlichen Anforderungen spielen die Unternehmen den Ball klar in Richtung Politik. Die Rahmenbedingungen für eine wirkungsvolle IT-Sicherheit können nur in Berlin und, besser noch, europaweit in Brüssel geschaffen werden. Im Rahmen der Novelle des deutschen IT-Sicherheitsgesetzes sollten der Anwendungsbereich des Regelwerks ausgedehnt, die Sicherheitsstandards erhöht und neue Instrumente wie ein Prüfzeichen für IT-Produkte eingeführt werden. In der EU steht mit dem Cybersecurity Act ebenfalls ein Rahmenwerk für die IT-Sicherheit von Produkten zur Verfügung. Jetzt gilt es, die Anforderungen in den europäischen Regelungen für die einzelnen Warengruppen fest zu verankern.

Die vorliegende „TÜV Cybersecurity Studie“ soll die Diskussion um die Sicht der betroffenen Unternehmen bereichern. Der TÜV-Verband und seine Mitglieder haben seit mehr als 150 Jahren jede Entwicklung der Technik begleitet, daher sind wir auch heute davon überzeugt: IT-Sicherheit ist eine der wichtigsten Voraussetzungen für Innovation und Wachstum in Deutschland!

Herzlich
Ihr Dr. Michael Fübi
Präsident des TÜV-Verbands (VdTÜV)

Inhaltsverzeichnis

58%

berichten, dass ihre Mitarbeiter häufig von Sicherheitsvorgaben genervt sind

1.0 Kernergebnisse im Überblick

60%

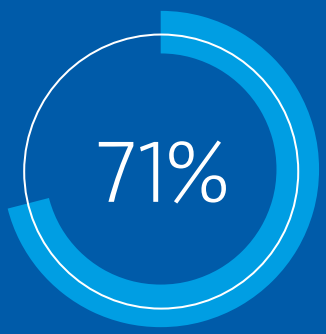
Prozent haben kein eigenes Budget für IT-Sicherheit

13%

hatten kürzlich einen schweren IT-Sicherheits-vorfall

38%

der großen Unternehmen nutzen Künstliche Intelligenz für ihre IT-Sicherheit



sagen, dass IT-Sicherheit für ihr Unternehmen eine große Rolle spielt

64%

sehen in Normen und Standards ein wichtiges Mittel, um ihren Schutz zu verbessern

92%

Prozent sehen in Cyberangriffen eine ernste Gefahr für Wirtschaft und Gesellschaft

22%

sehen die Gefahr eines schweren IT-Sicherheitsvorfalls

32%

nehmen bestimmte Risiken bei der Cybersecurity in Kauf

33%

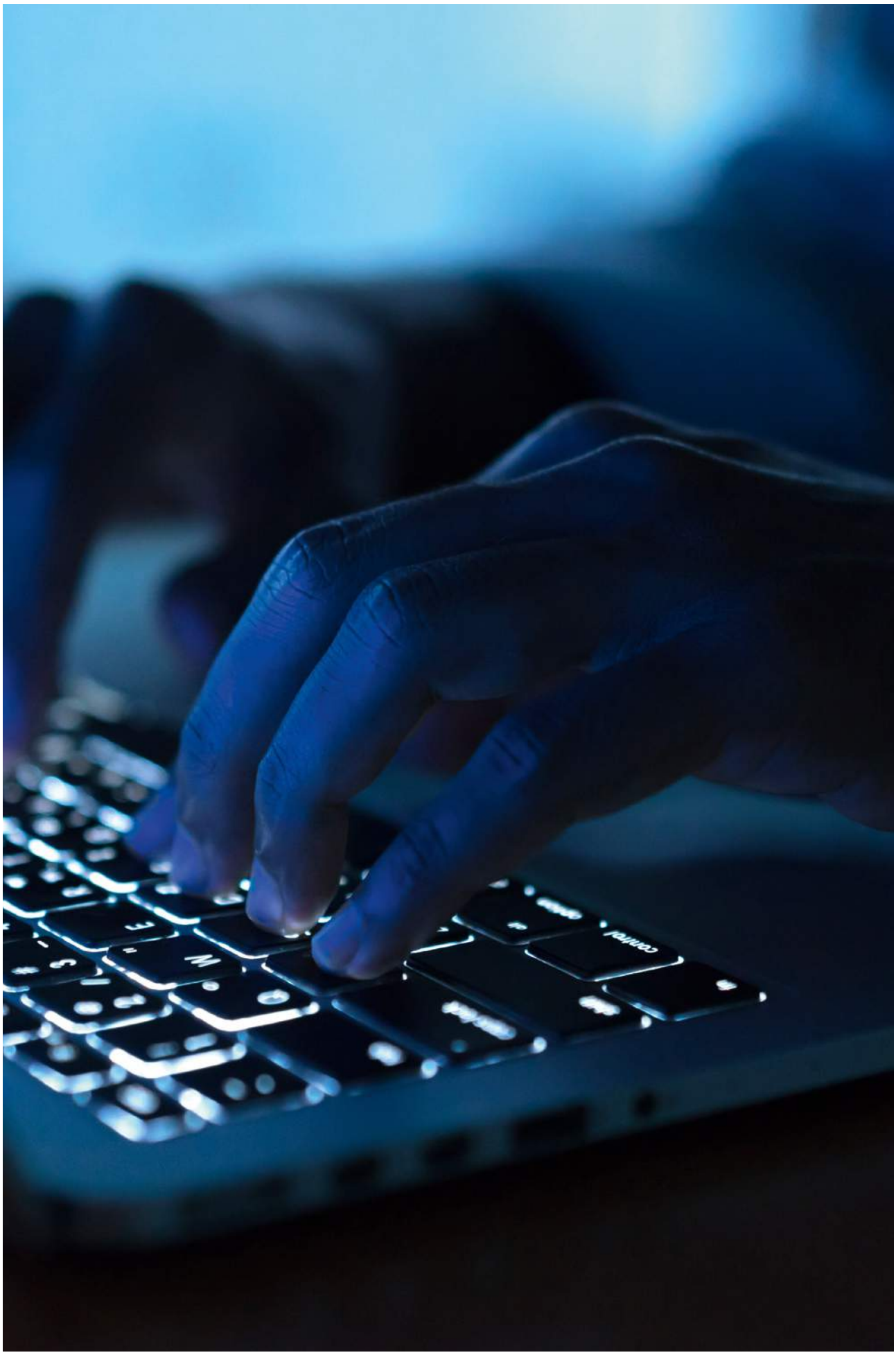
sagen, dass Cybersecurity ihre Geschäftsprozesse bremst

68%

setzen Normen und Standards für IT-Sicherheit um oder orientieren sich an diesen

47%

befürworten höhere gesetzliche Anforderungen für die IT-Sicherheit von Unternehmen


control

2.0

Cybersecurity: allgemeine Risikobewertung

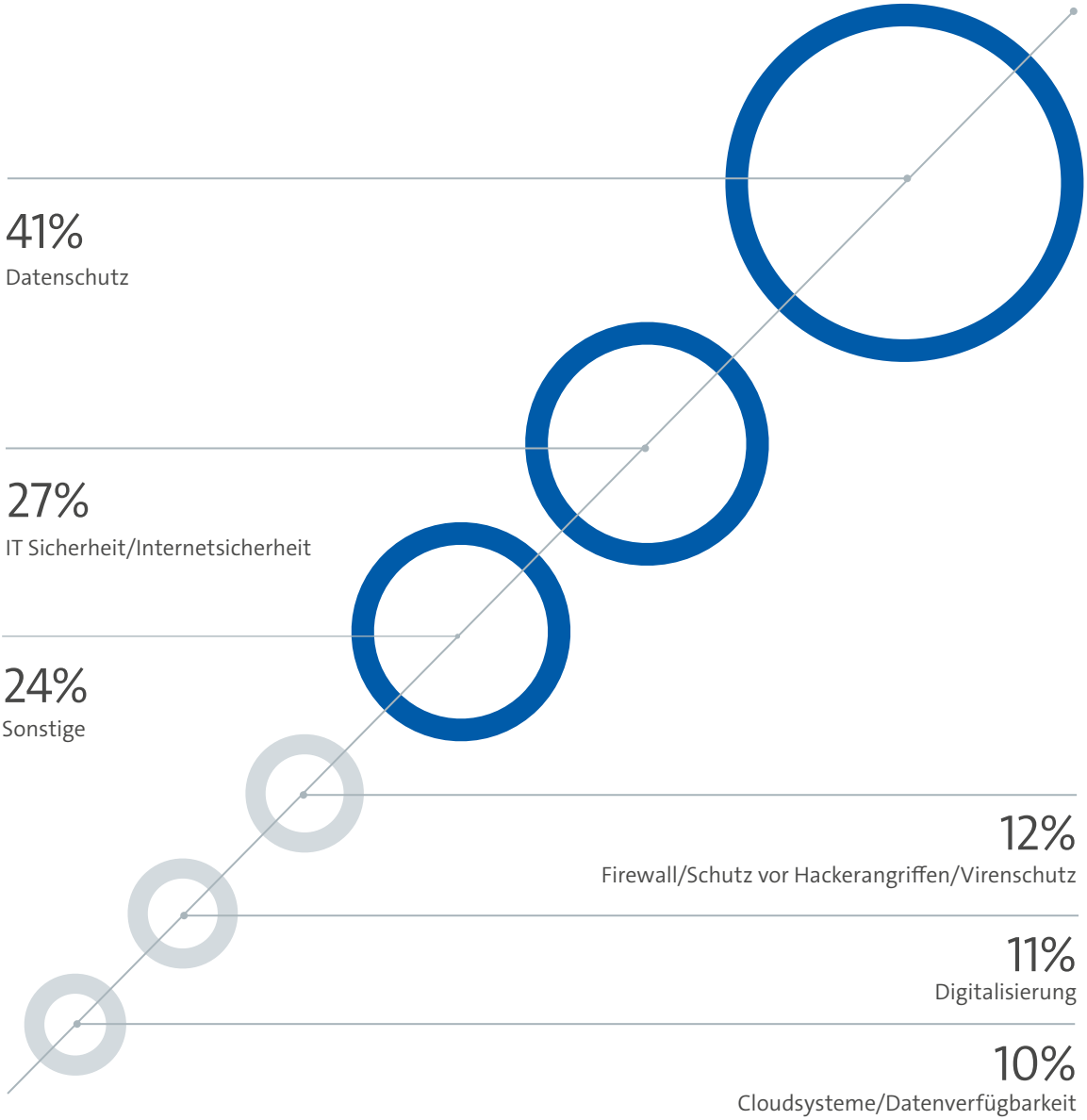
2.1

Datenschutz und IT-Sicherheit: Top-Themen der IT-Abteilungen

Was sind die wichtigsten Themen der IT-Abteilungen in der nahen Zukunft?

Diese Frage wurde den Teilnehmern der Befragung offen gestellt, also ohne vorformulierte Antwortoption. Datenschutz, IT-Sicherheit generell und einige spezielle Sicherheitsthemen wie Virenschutz oder Firewalls stehen in den IT-Abteilungen an der Spitze der aktuellen Herausforderungen.
Das Megathema „Digitalisierung“ folgt erst im Anschluss. Das deutet auf eine hohe Bedeutung von Cybersecurity in den Unternehmen hin.

Was sind die drei wichtigsten Themen für IT-Abteilungen in naher Zukunft?



Basis: Alle Befragten (n=503). Was sind Ihrer Einschätzung nach die drei wichtigsten Themen, mit denen sich IT-Abteilungen von deutschen Unternehmen wie Ihrem in naher Zukunft beschäftigen werden?

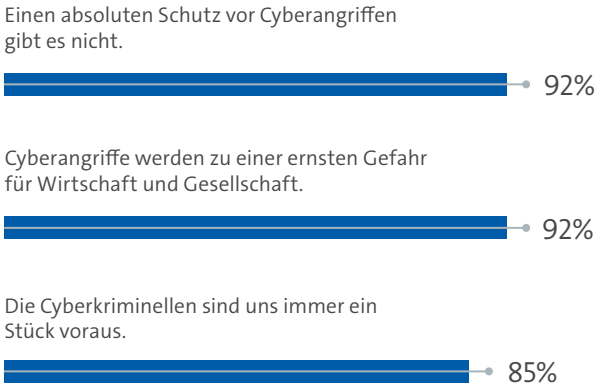
2.2

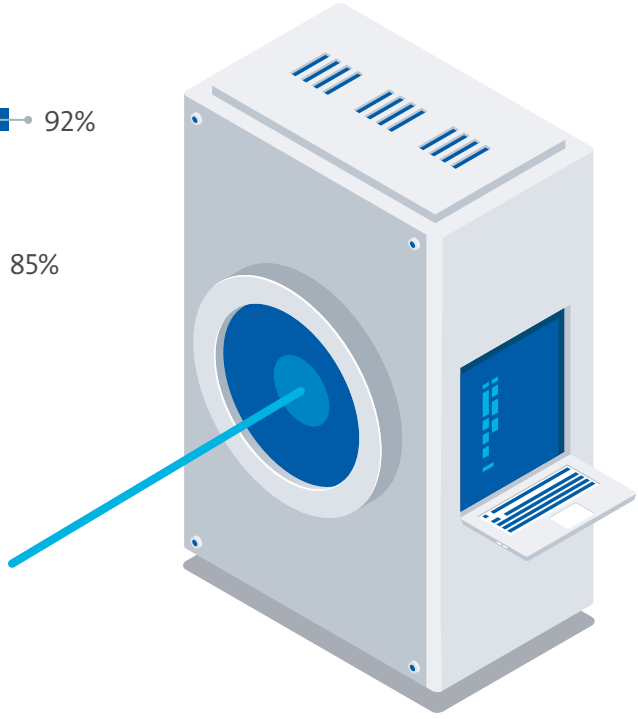
Absoluten Schutz vor Cyberangriffen gibt es nicht

Fast alle befragten Unternehmen (92 Prozent) sind sich einig, dass es einen absoluten Schutz vor Cyberangriffen nicht gibt.

Ebenso viele halten Cyberangriffe für eine ernste Gefahr für Wirtschaft und Gesellschaft. Dabei werden den Angreifern hohe kriminelle Energie und Fachkenntnis zugesprochen: 85 Prozent der befragten Unternehmen meinen, dass die Cyberkriminellen den Unternehmen immer ein Stück voraus sind.

Bedeutung Künstlicher Intelligenz für die IT-Sicherheit





Basis: Alle Befragten (n=503). Stimmen Sie den Aussagen voll/eher zu?

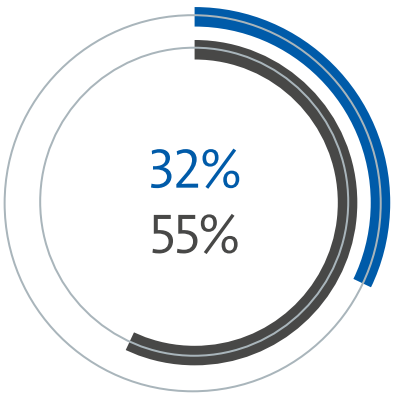
2.3

Viele nehmen bestimmte Risiken bei der IT-Sicherheit in Kauf

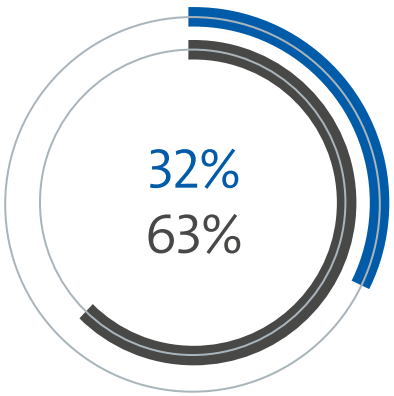
Den Unternehmen sind die Gefahren durch Cyberangriffe zwar bewusst, dennoch sind viele zu Abstrichen bei der IT-Sicherheit bereit.

Rund ein Drittel der Befragten gibt an, dass ihre Unternehmen bestimmte Risiken bei der IT-Sicherheit bewusst in Kauf nehmen. Ebenfalls ein Drittel machten die Feststellung, dass die für IT-Sicherheit eingesetzten Ressourcen in keinem Verhältnis zum Sicherheitsgewinn stünden. Die Risikobereitschaft variiert aber je nach Branche: So ist in Unternehmen aus dem produzierenden Gewerbe die Risikobereitschaft am höchsten. In den Bereichen Energie, Bau und Verkehr sowie im öffentlichen Bereich und dem Gesundheitswesen ist diese Bereitschaft zwar geringer, dennoch gibt rund ein Viertel der Unternehmen aus dem Sektor der kritischen Infrastrukturen an, bewusst Risiken bei der IT-Sicherheit in Kauf zu nehmen.

Wie bewerten sie die folgenden Aussagen zur IT-Sicherheit?



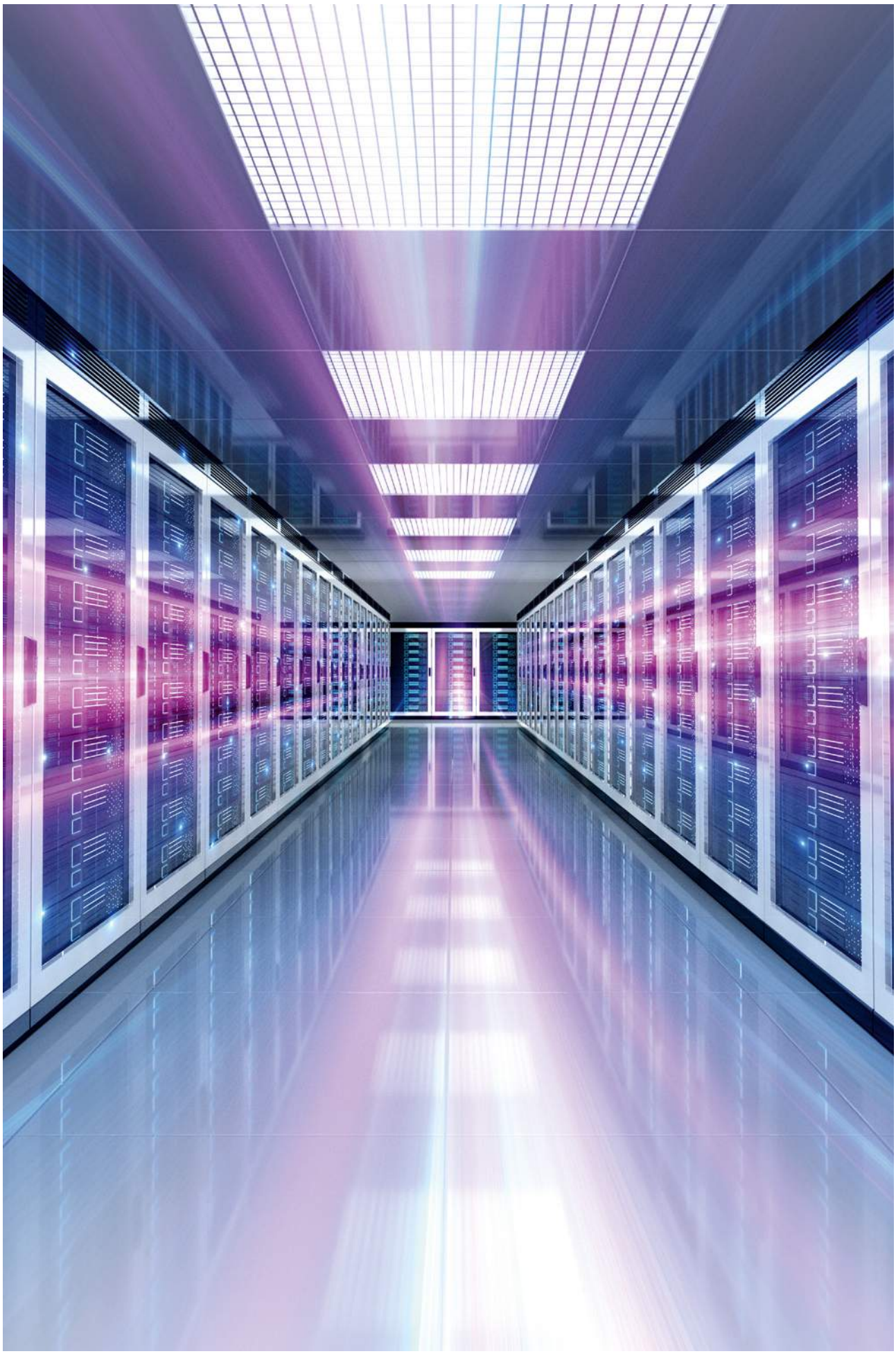
Die für IT-Sicherheit eingesetzten Ressourcen stehen bei uns in keinem Verhältnis zum Sicherheitsgewinn.



Unser Unternehmen nimmt bestimmte Risiken bei der IT-Sicherheit bewusst in Kauf.

Stimme voll/eher zu Stimme eher nicht/gar nicht zu

Basis: Alle Befragten (n=503). Stimmen Sie den Aussagen (voll/eher) zu oder (eher/gar) nicht? Differenz zu 100 Prozent: weiß nicht/keine Angabe



3.0

Bedeutung von IT-Sicherheit im Unternehmen

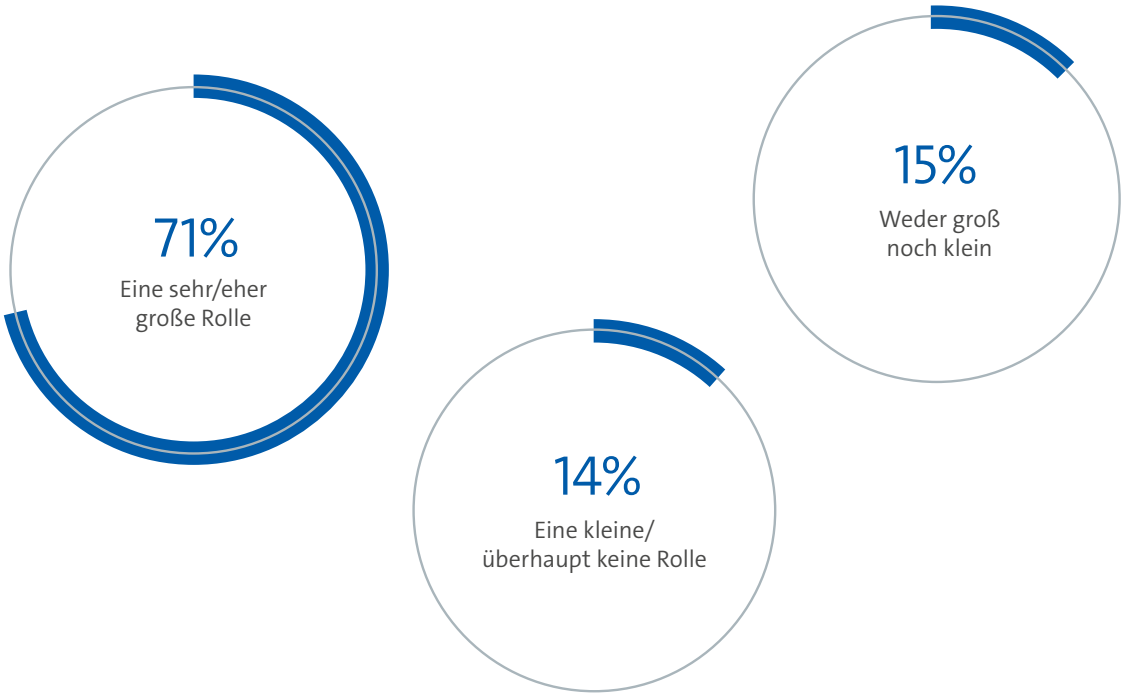
3.1

IT-Sicherheit ist für große Unternehmen besonders relevant

Die Relevanz von IT-Sicherheit ist für die befragten Unternehmen sehr hoch.

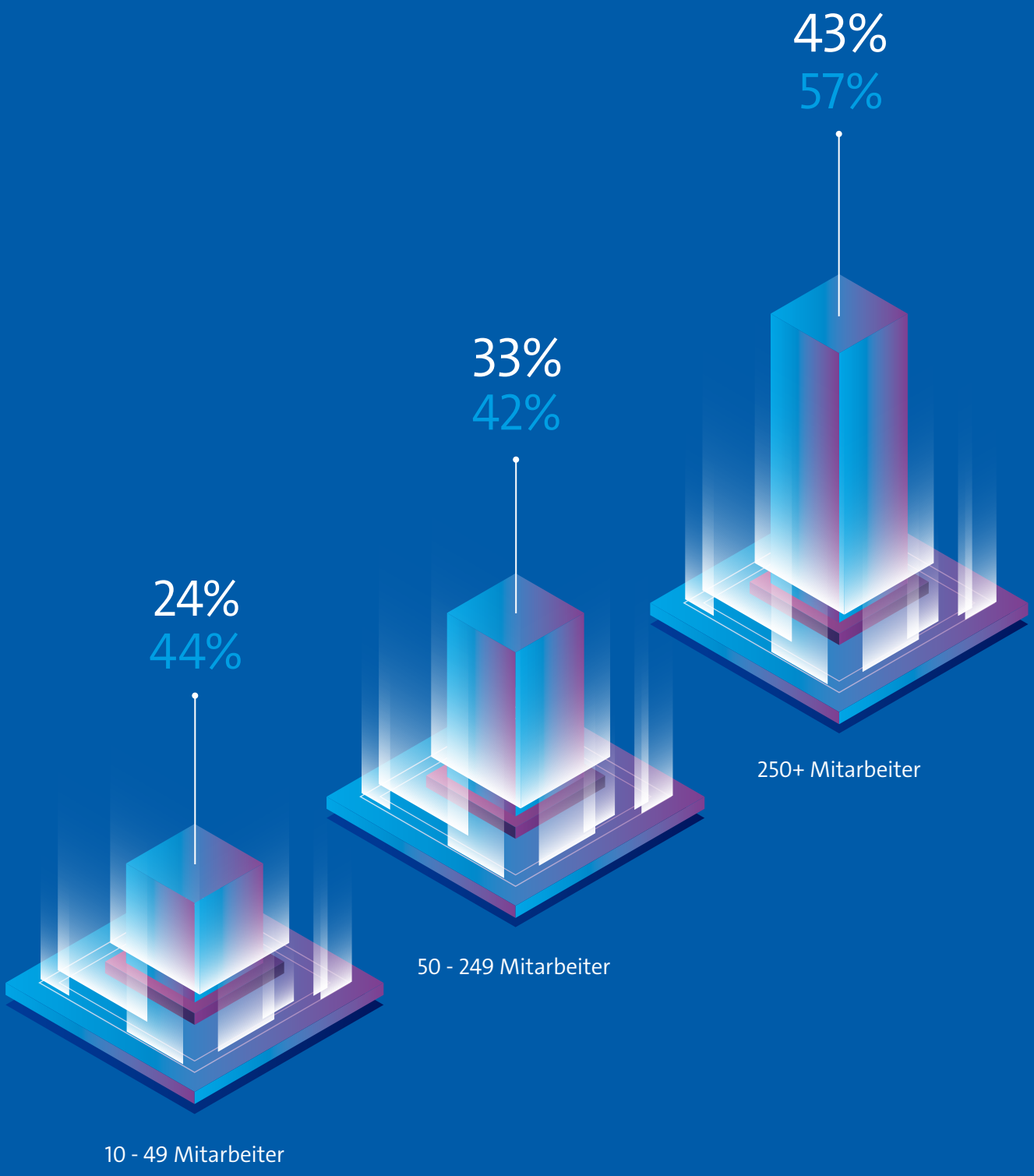
71 Prozent geben an, dass IT-Sicherheit aktuell für ihr Unternehmen eine „sehr große“ oder „eher große“ Rolle spiele. Hier gilt: Je größer das Unternehmen, umso höher ist die Relevanz der IT-Sicherheit. So spielt nur für zwei Drittel der kleinen Unternehmen unter 50 Mitarbeitern IT-Sicherheit eine große Rolle. Bei großen Unternehmen ab 250 Mitarbeitern sind es hingegen 100 Prozent. Unterschiede bestehen zwischen den einzelnen Branchen. So spielt im öffentlichen Bereich und im Gesundheitswesen die IT-Sicherheit die größte Rolle, eine geringere im Bereich Energie, Bau und Verkehr.

Welche Rolle spielt IT-Sicherheit aktuell für ihr Unternehmen?



Basis: Alle Befragten (n=503).

Welche Rolle spielt IT-Sicherheit aktuell für ihr Unternehmen?

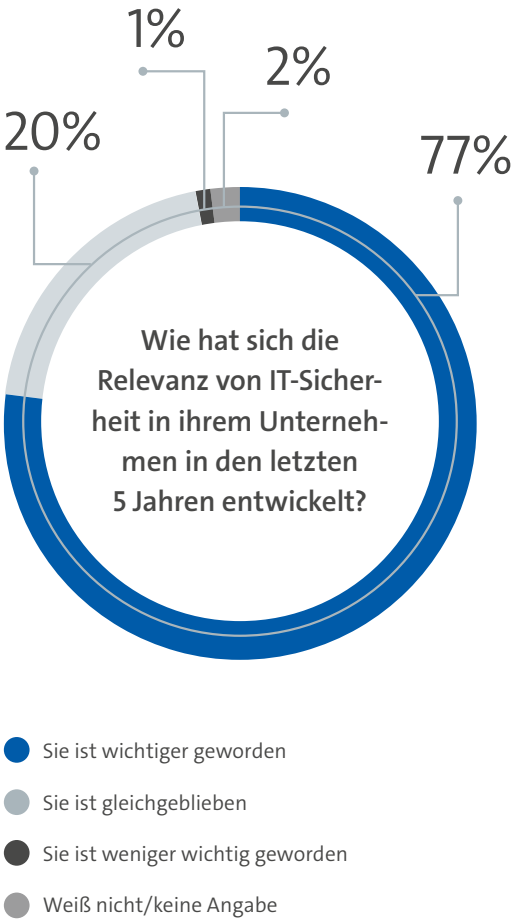


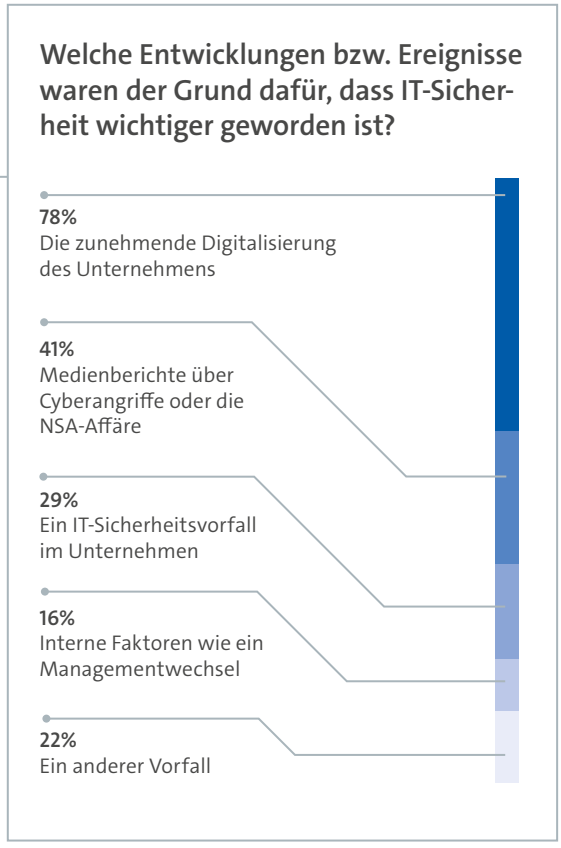
3.2

IT-Sicherheit hat stark an Bedeutung gewonnen

Wie hat sich die Relevanz der IT-Sicherheit entwickelt?

Gut drei Viertel (77 Prozent) der befragten Unternehmen geben an, dass IT-Sicherheit in den vergangenen fünf Jahren wichtiger geworden sei. Unter diesen Unternehmen spielt die zunehmende Digitalisierung der Organisation eine herausragende Rolle, fast acht von zehn Befragten geben dies als Grund für die gestiegene Relevanz an. Medienberichte über Cyberangriffe oder die NSA-Affäre waren für 41 Prozent der Unternehmen die Ursache für die gestiegene Bedeutung von IT-Sicherheit. Bei fast jedem dritten Unternehmen (29 Prozent) ist ein IT-Sicherheitsvorfall im eigenen Haus der Grund.





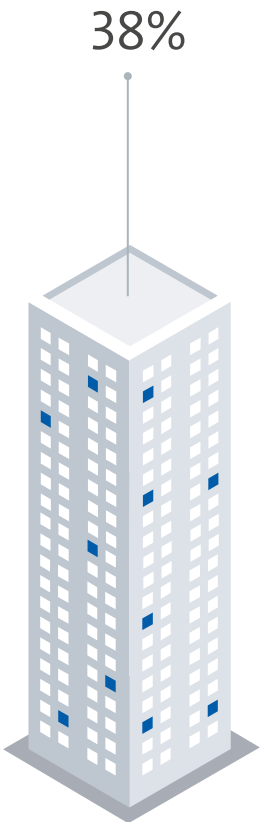
Basis: Alle Befragten (n=503). Wie würden Sie die Entwicklung der Relevanz von IT-Sicherheit in Ihrem Unternehmen in den vergangenen fünf Jahren einschätzen?
Basis: Alle Befragten, in deren Unternehmen die IT-Sicherheit in den vergangenen 5 Jahren wichtiger geworden ist (n=385). War einer der folgenden Vorfälle der Grund dafür, dass die IT-Sicherheit in den vergangenen 5 Jahren wichtiger geworden ist?

3.3

Viele sehen Gefahr eines schweren IT-Sicherheitsvorfalls

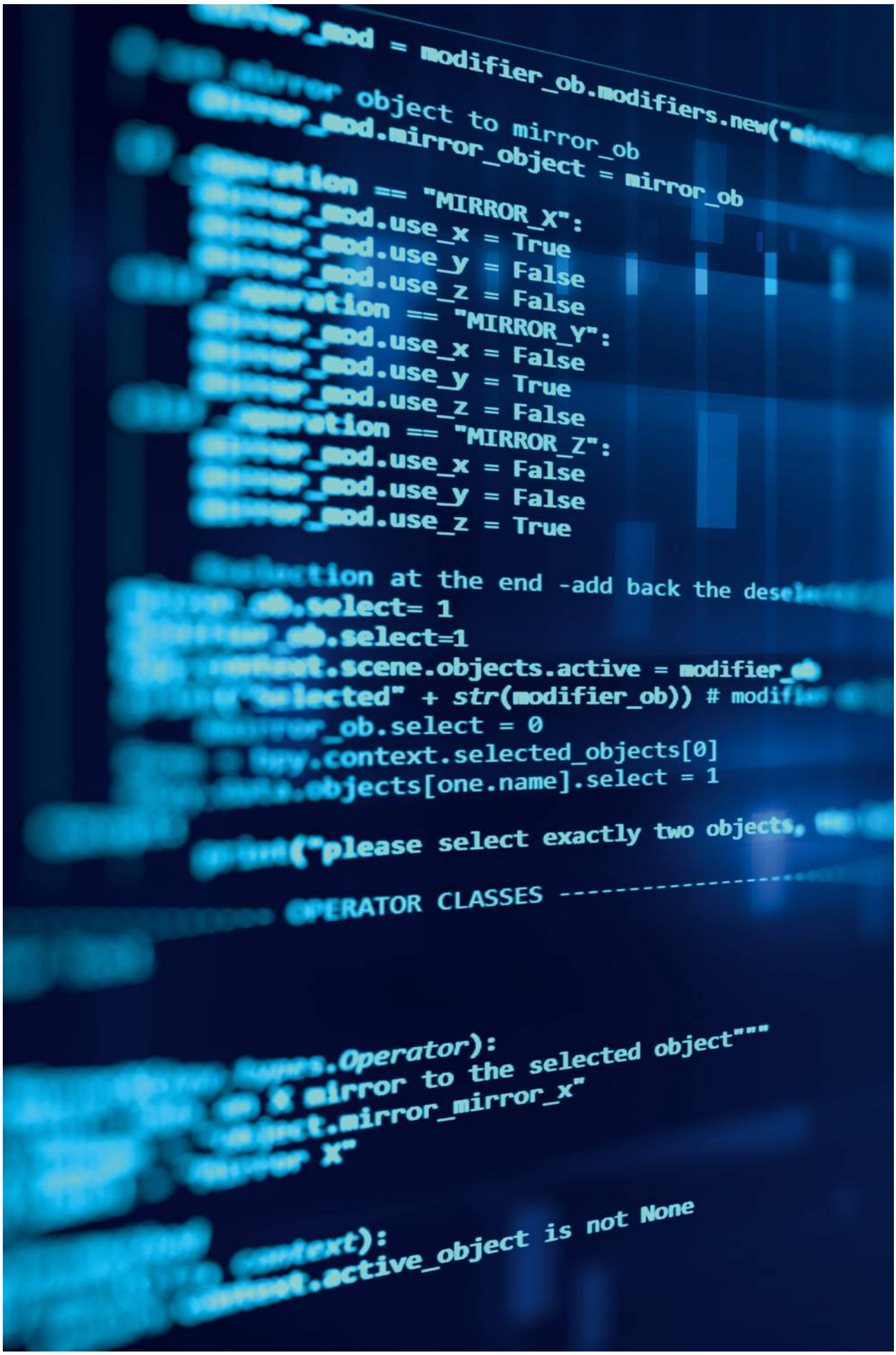
Gut ein Fünftel der befragten Unternehmen (22 Prozent) hält es für realistisch, dass es in den nächsten 12 Monaten zu einem schweren IT-Sicherheitsvorfall in ihrer Organisation kommt.

Drei Viertel der Unternehmen schätzen die Gefahr eher gering ein. Dabei hängt das Ergebnis von der Unternehmensgröße ab: Unter den Unternehmen ab 250 Mitarbeitern halten sogar 38 Prozent einen schweren Vorfall für realistisch.



der Unternehmen mit mehr als 250 Mitarbeitern halten einen Vorfall für sehr/eher realistisch

Basis: Alle Befragten (n=503). Für wie realistisch halten Sie die Gefahr, dass es in den kommenden 12 Monaten in Ihrem Unternehmen zu einem (weiteren) schweren IT-Sicherheitsvorfall kommt?


object to mirror_ob
mod.mirror_object = mirror_ob
== "MIRROR_X":
mod.use_x = True
mod.use_y = False
mod.use_z = False
== "MIRROR_Y":
mod.use_x = False
mod.use_y = True
mod.use_z = False
== "MIRROR_Z":
mod.use_x = False
mod.use_y = False
mod.use_z = True
at the end -add back the
.select= 1
.select=1
.scene.objects.active = modifier
" + str(modifier_ob)) # modifi
ob.select = 0
.context.selected_objects[0]
objects[one.name].select = 1
("please select exactly two objects,
OPERATOR CLASSES
.Operator):
mirror to the selected object"""
.mirror_mirror_x"
X"
ext):
.active_object is not None

4.0

Stand der IT-Sicherheit und aktuelle Vorfälle

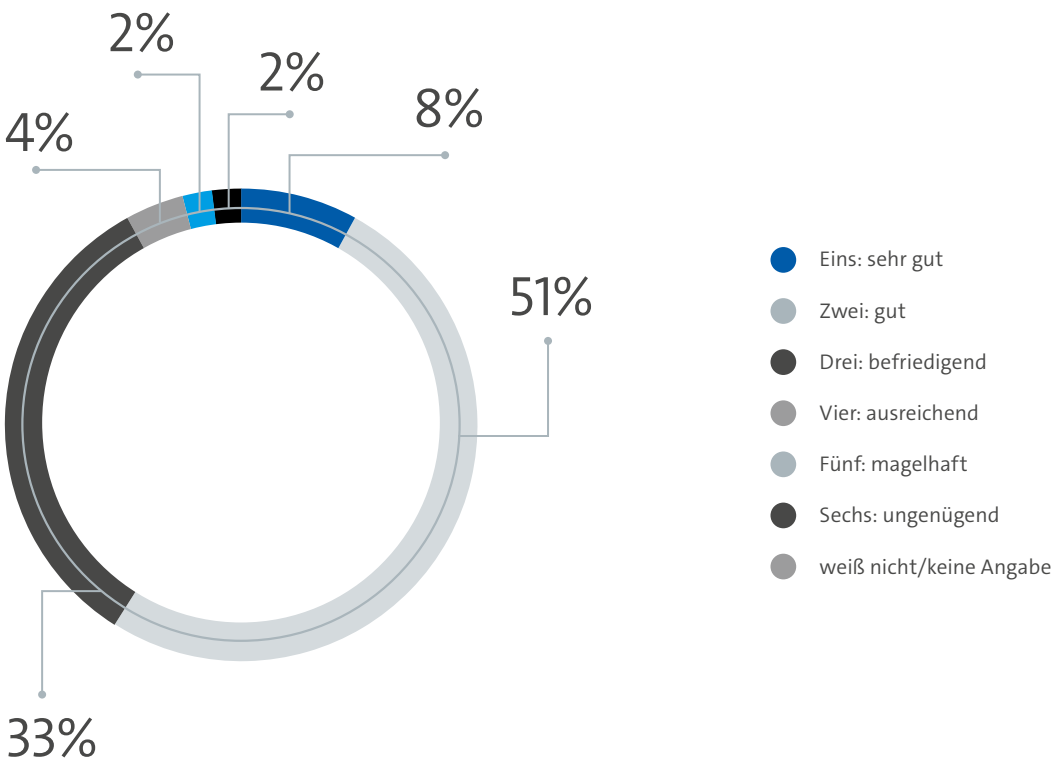
4.1

Die meisten würden ihrer IT-Sicherheit eine „Zwei“ geben

Wie benoten die Unternehmen ihre eigene IT-Sicherheit?

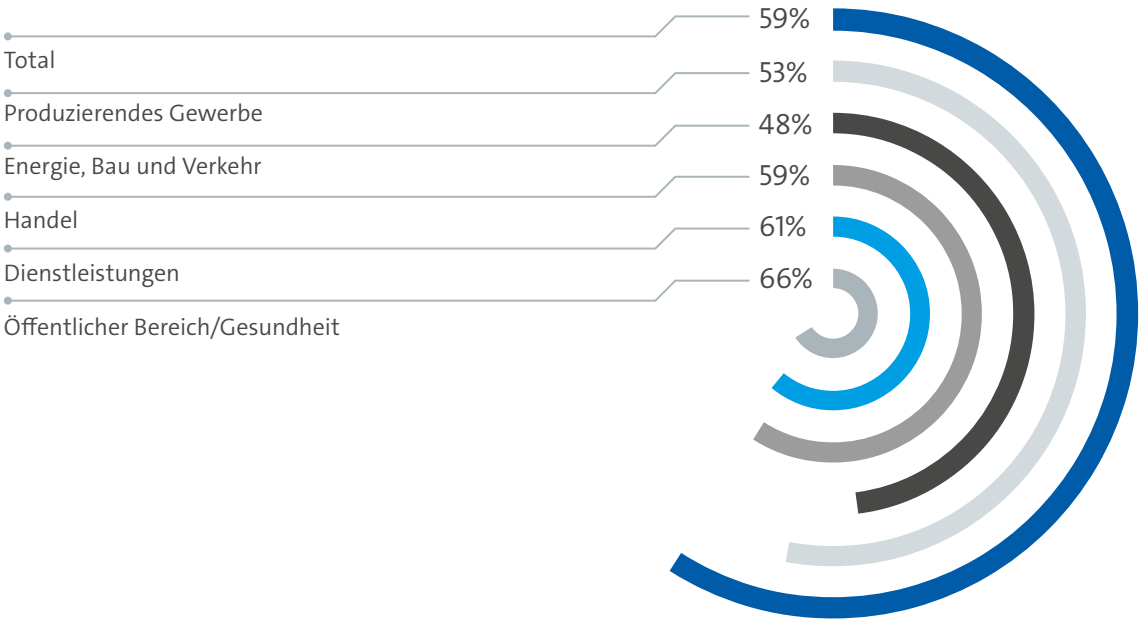
Eine deutliche Mehrheit der Befragten würde die IT-Sicherheit des eigenen Unternehmens mit „gut“ oder „befriedigend“ bewerten. Eine „Eins“ würden sogar 8 Prozent vergeben, eine „Vier“ oder schlechter nur 6 Prozent. Auch hier differieren die unterschiedlichen Branchen: Der öffentliche Bereich und das Gesundheitswesen sehen ihre eigene IT-Sicherheit mit zwei Dritteln „sehr gut“ oder „gut“ im oberen Bereich, hingegen werden in kritischen Infrastrukturbereichen wie Energie, Bau und Verkehr nur von knapp der Hälfte der befragten Unternehmen diese Spitzenwerte vergeben.

Selbsteinschätzung der IT-Sicherheit nach Schulnoten



Basis: Alle Befragten (n=503). Wie würden Sie persönlich das Niveau der IT-Sicherheit in Ihrem Unternehmen einschätzen?

Selbsteinschätzung nach Branchen (sehr gut/gut)



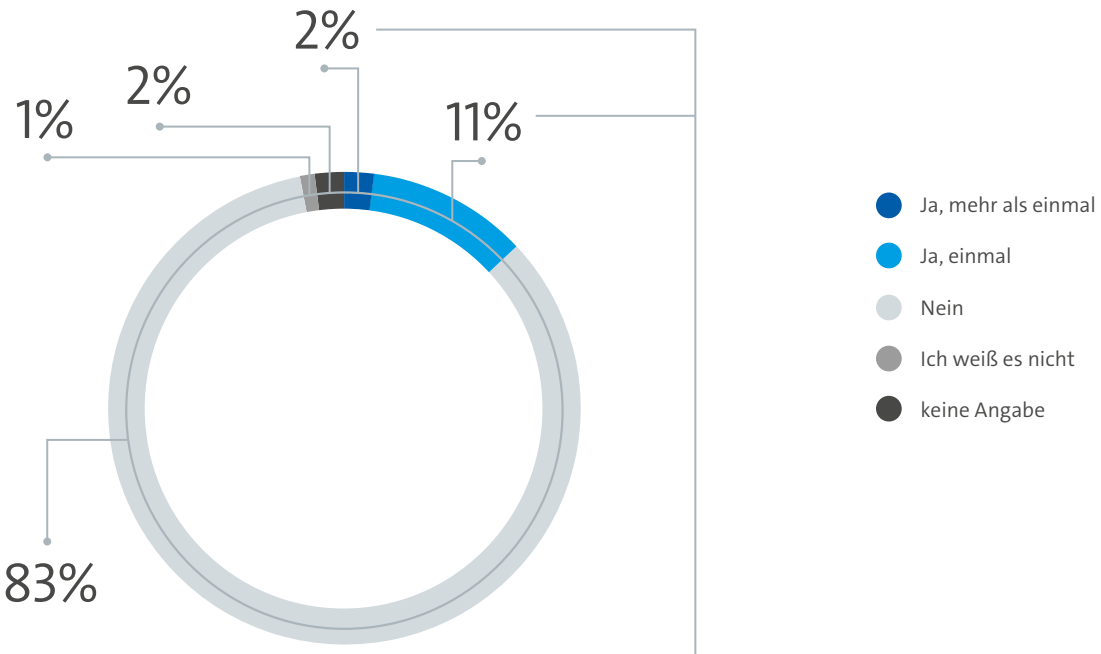
4.2

Jedes achte Unternehmen hatte kürzlich einen IT-Sicherheitsvorfall

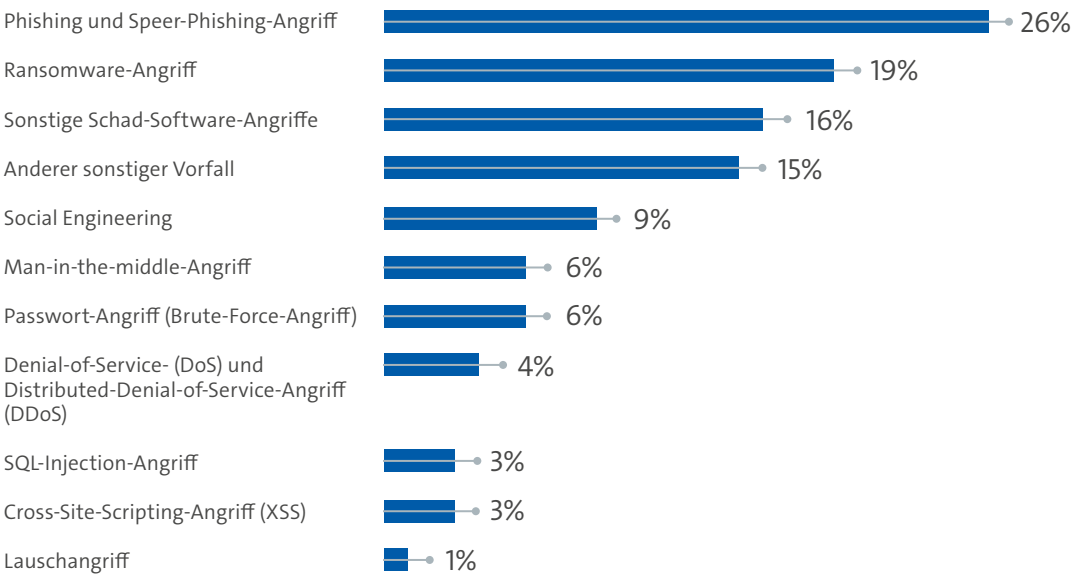
Gut jedes achte Unternehmen in Deutschland (13 Prozent) hatte in den vergangenen 12 Monaten vor der Befragung mindestens einen schweren IT-Sicherheitsvorfall.

Dabei ist die Art der Vorfälle sehr unterschiedlich. Die meisten betroffenen Unternehmen berichten von Phishing-Angriffen, bei denen in der Regel per E-Mail Schadsoftware in die Organisation eingeschleust wird. An zweiter Stelle steht Ransomware, mit deren Hilfe Cyberkriminelle die IT-Systeme einer Organisation lahmlegen und die Unternehmen dann erpressen. Ein weiteres weit verbreitetes Phänomen ist Social Engineering. Mitarbeiter werden gezielt manipuliert, um sich Zugang zu den IT-Systemen des Unternehmens zu verschaffen. Erfahrungen gibt es aber auch mit weiteren gefährlichen Angriffsszenarien, wie etwa durch Man-in-the-middle-, Passwort-, DoS- oder DDoS-Angriffe. Andere betroffene Unternehmen berichten über sonstige Schad-Software-Angriffe oder andere Angriffsvarianten, ohne sie näher zu spezifizieren.

Hat ihr Unternehmen in den letzten 12 Monaten einen IT-Sicherheitsvorfall gehabt?



Art des Vorfalls



Basis: Alle Befragten (n=503). Hat Ihr Unternehmen in den letzten 12 Monaten einen IT-Sicherheitsvorfall gehabt? Basis: Alle Befragten, in deren Unternehmen es in den letzten 12 Monaten mindestens einen IT-Sicherheitsvorfall gab (n=69). Bitte geben Sie an, ob es sich bei Ihrem Sicherheitsvorfall um einen der Vorfälle handelte.

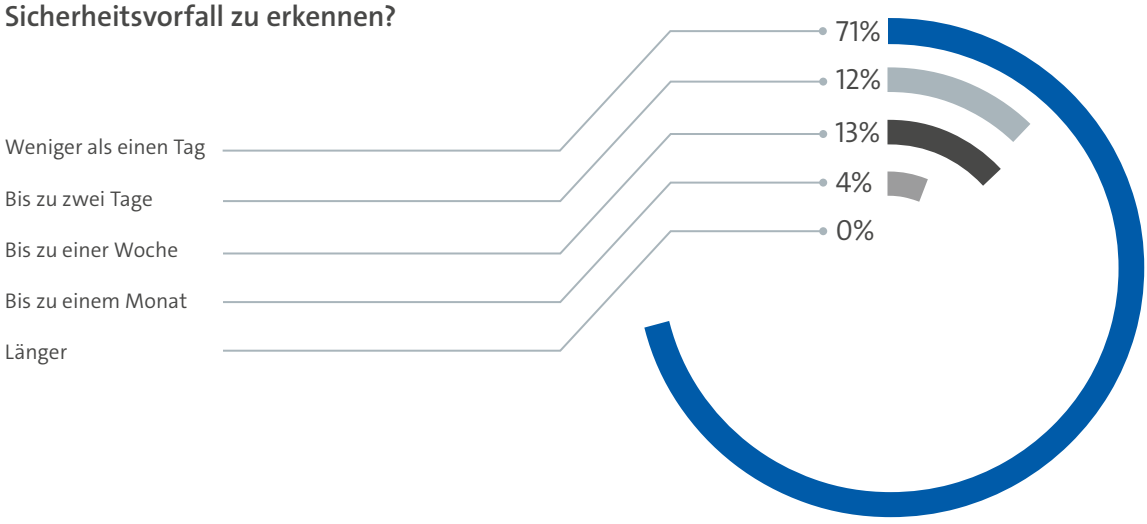
4.3

Sicherheitsvorfälle zügig erkannt und behoben

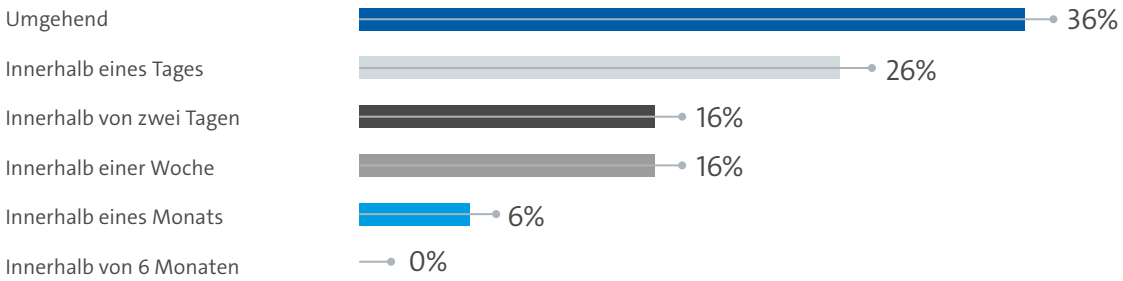
Kam es zu einem Sicherheitsvorfall, wurde er meistens schnell erkannt.

71 Prozent der Unternehmen geben an, sie hätten einen Tag für die Erkennung des Vorfalls gebraucht und weitere 12 Prozent zwei. Bei 13 Prozent hat es bis zu einer Woche gedauert und bei 4 Prozent bis zu einem Monat. Die Sicherheitsvorfälle konnten in der Regel zügig behoben werden. In jedem zweiten betroffenen Unternehmen (52 Prozent) gelang dies innerhalb eines Tages. Weitere 16 Prozent brauchten zwei Tage, weitere 16 Prozent bis zu einer Woche und nur 4 Prozent bis zu einem Monat.

Wie lange haben Sie gebraucht, um den Sicherheitsvorfall zu erkennen?



Wie schnell konnte der Vorfall behoben werden?



Basis: Alle Befragten, in deren Unternehmen es in den letzten 12 Monaten mindestens einen IT-Sicherheitsvorfall gab (n=69). Wie lange haben Sie gebraucht, um den Sicherheitsvorfall zu erkennen? Wie schnell konnte dieser Sicherheitsvorfall behoben werden?

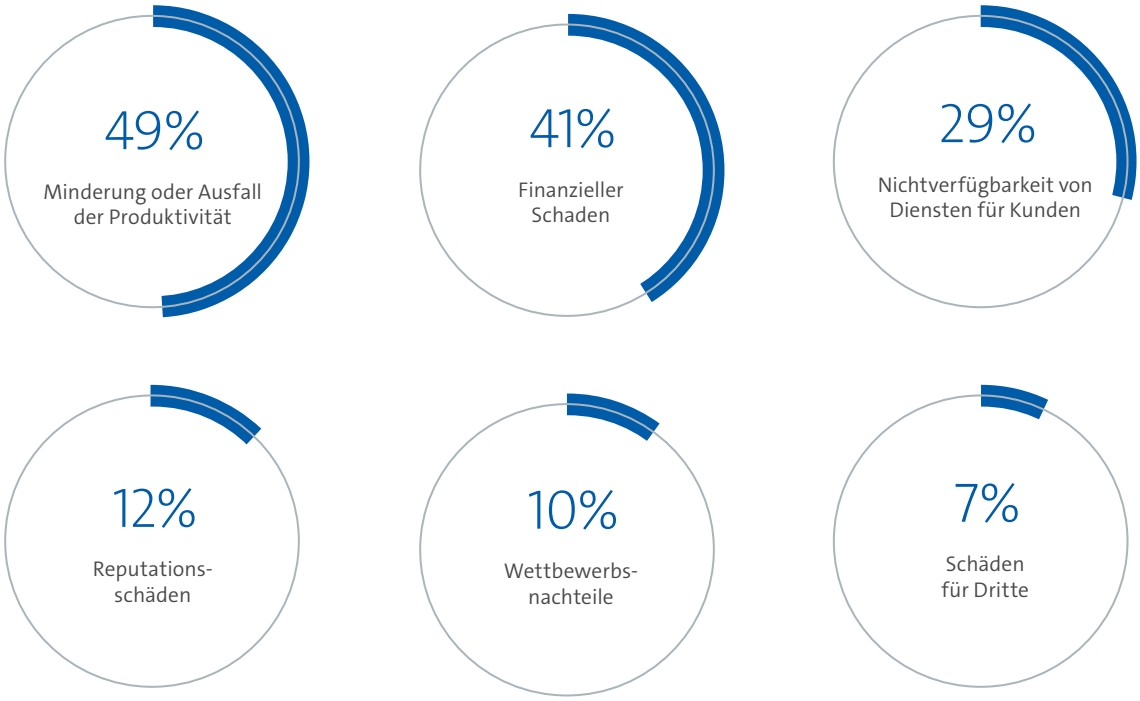
4.4

Arbeitsausfall und finanzielle Schäden sind die Folgen

Die Sicherheitsvorfälle zeigen, dass Cyberkriminalität enorme Schäden verursacht.

Fast die Hälfte der betroffenen Unternehmen berichtet von einer Minderung oder sogar einem kompletten Ausfall ihrer Produktivität. Rund vier von zehn Unternehmen beklagten einen finanziellen Schaden. Bei fast jedem dritten betroffenen Unternehmen waren Dienste für Kunden zeitweise nicht verfügbar. Aber auch alle weiteren genannten Beeinträchtigungen wie Reputationsschäden, Wettbewerbsnachteile oder auch Schäden für Dritte können für Unternehmen langfristig verheerende Folgen haben.

Was waren die Folgen des Sicherheitsvofalls?



Basis: Alle Befragten, in deren Unternehmen es in den letzten 12 Monaten mindestens einen IT-Sicherheitsvorfall gab (n=69).
Ich lese Ihnen nun mögliche Folgen eines Sicherheitsvorfalls vor. Bitte geben Sie an, ob diese auf Sie zutreffen.

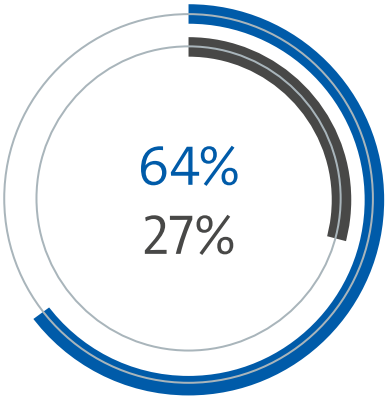
4.5

Fachkräftemangel schlägt auf Cybersecurity durch

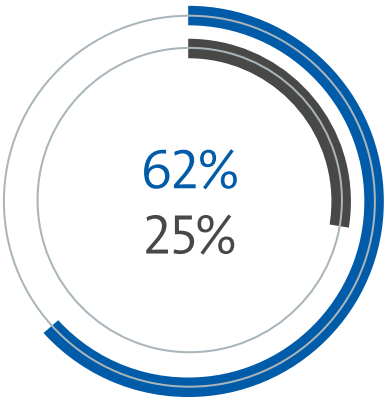
Der Mangel an Fachkräften ist ein beherrschendes Thema in der Diskussion um die Zukunft des Industriestandortes Deutschland.

Auch für die IT-Sicherheit spielt diese Frage eine wichtige Rolle. Ein Viertel der befragten Unternehmen gibt an, dass sich der Mangel an IT-Experten auf ihre IT-Sicherheit auswirkt. Bei 14 Prozent führt dies sogar dazu, dass die Cybersecurity schlechter ist als erforderlich. Es ist davon auszugehen, dass die Auswirkungen des Fachkräftemangels eher unterschätzt werden, da viele Unternehmen die IT-Sicherheit an externe Dienstleister auslagern und daher nicht direkt mit dem Problem konfrontiert sind.

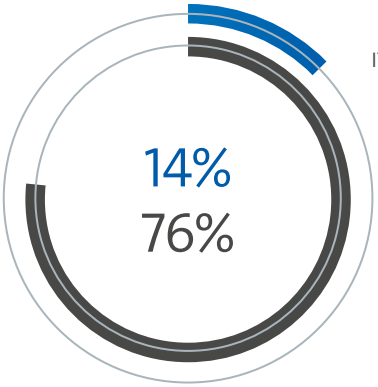
Wie bewerten Sie die Aussagen zum Fachkräftemangel?



Der Mangel an IT-Experten spielt für die IT-Sicherheit unseres Unternehmens keine Rolle



Wir spüren zwar auch Engpässe bei IT-Experten, das wirkt sich bei uns aber nicht auf die IT-Sicherheit aus.



Der Fachkräftemangel im IT-Bereich führt in unserem Unternehmen dazu, dass die IT-Sicherheit schlechter ist als erforderlich.

Stimme voll/eher zu Stimme eher nicht/gar nicht zu

Basis: Alle Befragten (n=503). Stimmen Sie den Aussagen (voll/eher) zu oder (eher/gar) nicht? Differenz zu 100 Prozent: weiß nicht/keine Angabe

5.0

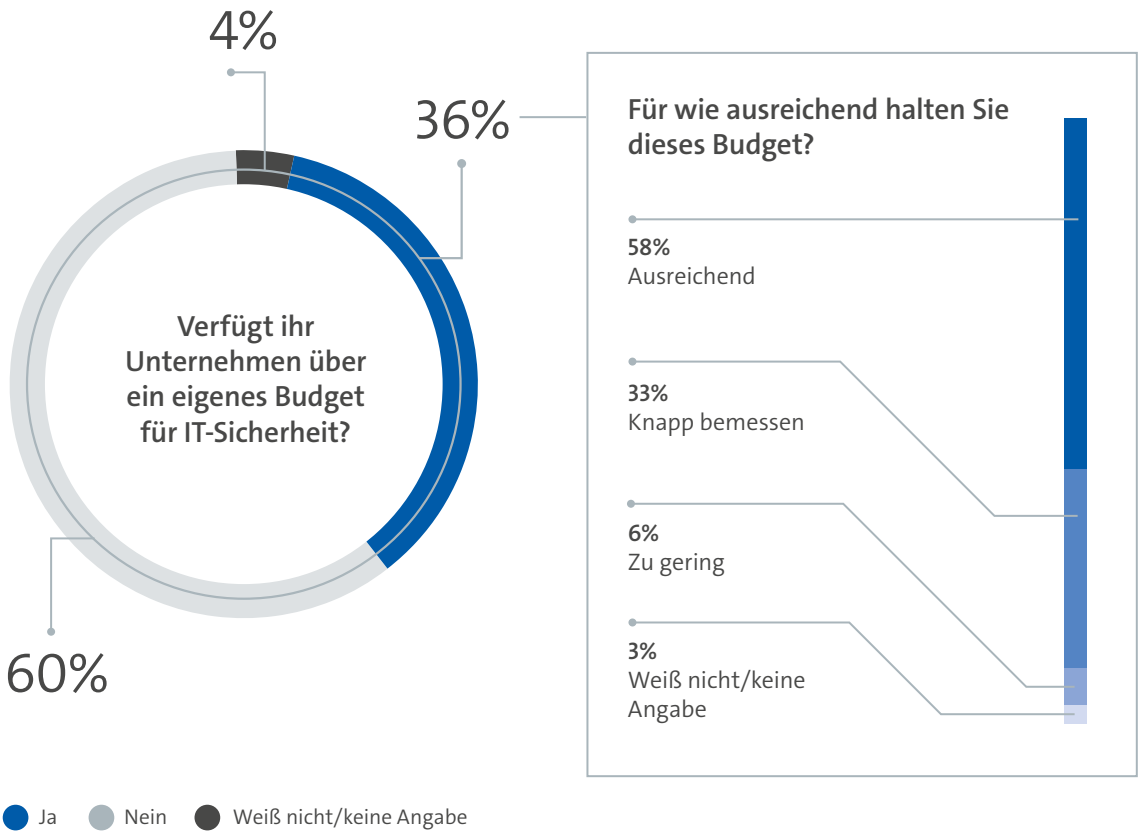
Aktuelle Maßnahmen für mehr IT-Sicherheit

5.1

Nur jedes dritte Unternehmen hat ein eigenes Budget für IT-Sicherheit

Der Anteil der befragten Unternehmen, der über ein eigenes Budget für IT-Sicherheit verfügt, beträgt nur 36 Prozent.

Je größer allerdings ein Unternehmen ist, umso häufiger ist auch ein eigenes Budget für IT-Sicherheit vorhanden. Allerdings ist auch hier der Anteil ohne IT-Budget sehr hoch: Bei einer Mitarbeiterzahl zwischen 50 und 249 fehlt es bei 55 Prozent – und jedes zweite Unternehmen mit mehr als 250 Mitarbeitern verfügt über kein eigenes IT-Budget. Unter allen Befragten halten 58 Prozent die bereitgestellten Mittel für ausreichend, ein Drittel hält das Budget für knapp bemessen.



Basis: Alle Befragten (n=503). Verfügt Ihr Unternehmen über ein eigenes Budget für Ausgaben im Bereich IT-Sicherheit?/Basis: Alle Befragten, deren Unternehmen über ein eigenes IT-Budget verfügt (n=181). Für wie ausreichend schätzen Sie dieses Unternehmensbudget für IT-Sicherheit ein?

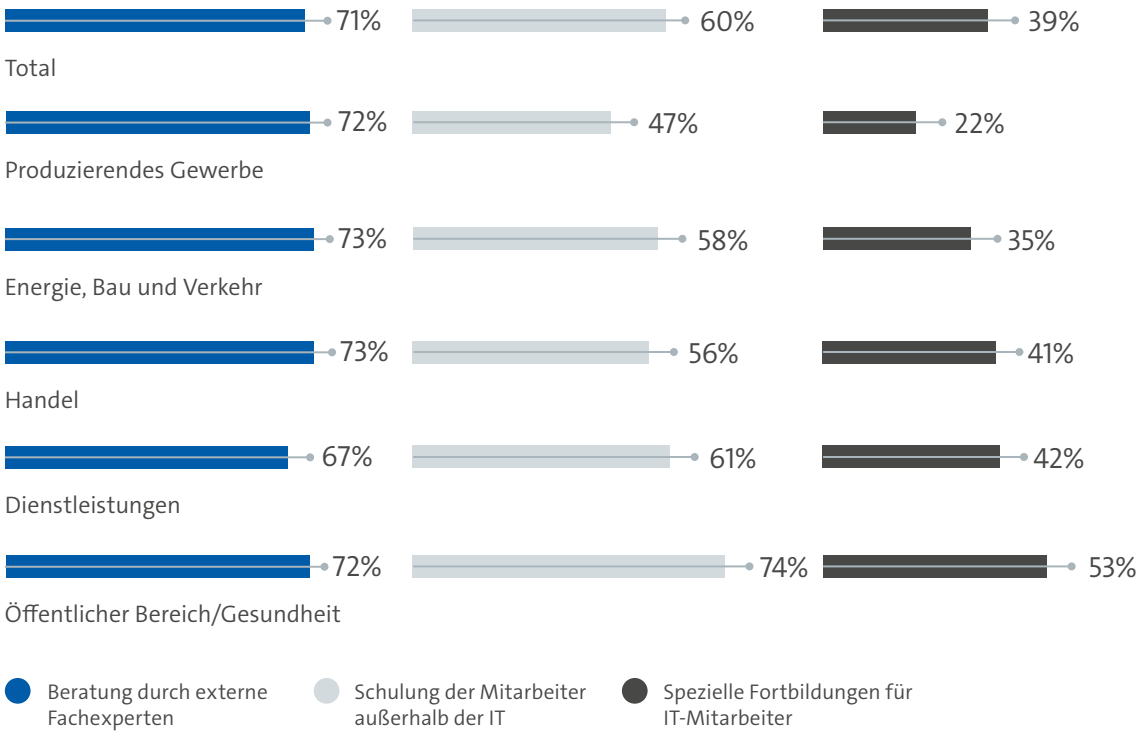
5.2

Beratung, Schulung, Software: aktuelle IT-Sicherheitsmaßnahmen

Wie werden die Mittel aktuell eingesetzt, um den Schutz vor Cyberangriffen zu verbessern?

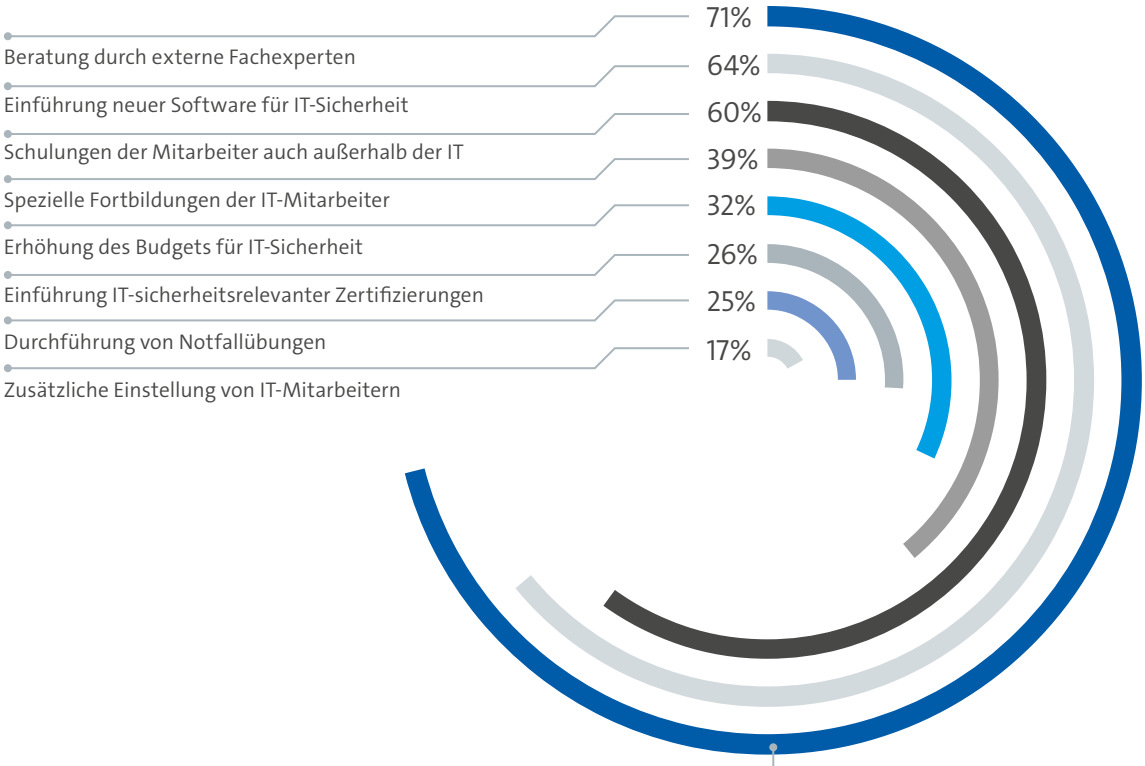
Sieben von zehn Unternehmen geben an, in den vergangenen 24 Monaten Beratung durch externe Fachexperten in Anspruch genommen zu haben. Je zwei Drittel haben neue Software für IT-Sicherheit eingeführt oder in die Schulung der Mitarbeiter außerhalb der IT-Abteilungen investiert. Immerhin fast jedes dritte Unternehmen (32 Prozent) hat das Budget für IT-Sicherheit erhöht, jedes vierte (26 Prozent) sicherheitsrelevante Zertifizierungen eingeführt und 17 Prozent zusätzliche IT-Spezialisten eingestellt. Mehr als die Hälfte der Unternehmen, die sich von Fachexperten beraten lassen, hat die IT-Sicherheit komplett an externe Dienstleister vergeben. In fast allen Branchen ist die Beratung durch externe Fachexperten die wichtigste Maßnahme zur IT-Sicherheit. Nur im öffentlichen Bereich und im Gesundheitswesen sind Schulungen für Mitarbeiter außerhalb der IT noch etwas wichtiger.

Unterschiedliche Schwerpunkte je nach Branche



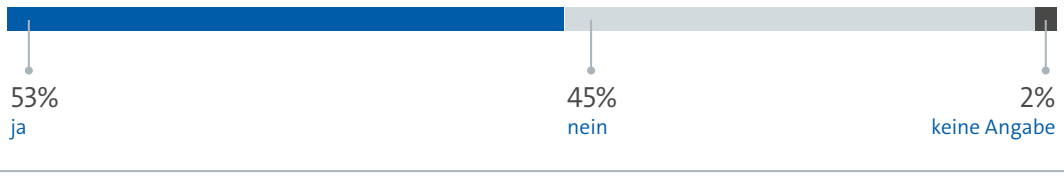
Basis: Alle Befragten (n=503). Geben Sie an, ob Ihr Unternehmen diese Maßnahmen in den vergangenen 24 Monaten ergriffen hat oder nicht. Sie sagten gerade, Ihr Unternehmen wird durch externe Fachexperten beraten. Haben Sie die IT-Sicherheit extern vergeben?

Hat ihr Unternehmen folgende Maßnahmen in den letzten 24 Monaten ergriffen?



Haben Sie die IT-Sicherheit extern vergeben?

Externe Prüfung/Zertifizierung durch unabhängige Stellen



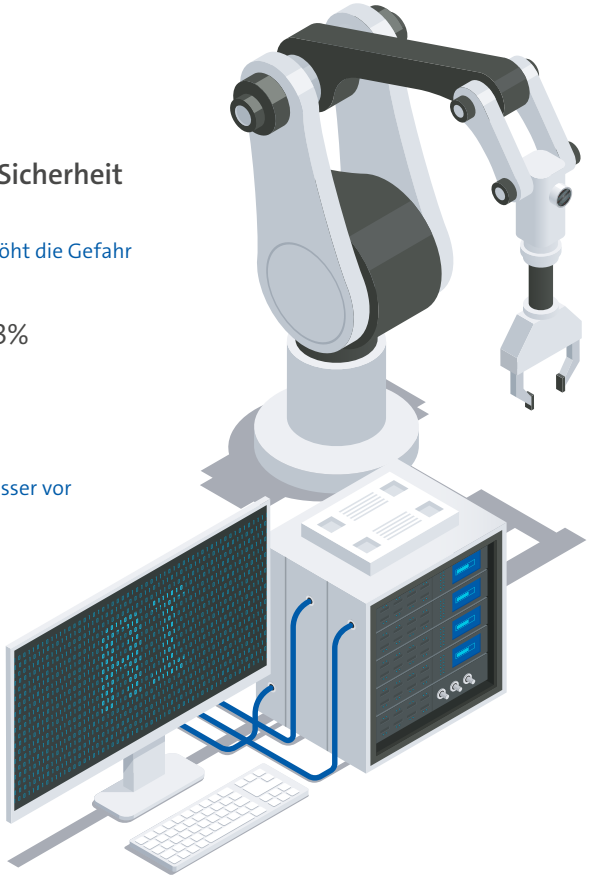
Basis: Alle Befragten (n=503). Ich lese Ihnen nun einige Maßnahmen zur IT Sicherheit vor. Bitte geben Sie an, ob Ihr Unternehmen diese in den vergangenen 24 Monaten ergriffen hat oder nicht. Mit * markierte Zahlen weisen auf Fallzahlen < 30 hin.

5.3

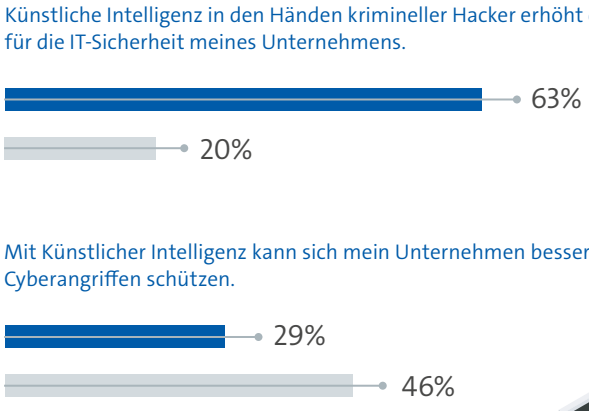
Künstliche Intelligenz: Fluch oder Segen für die Sicherheit?

Künstliche Intelligenz (KI) bedeutet, dass ein Computer oder eine Maschine eigenständig dazuzulernen und so komplexe Aufgaben lösen kann.

Unternehmen bietet diese Technologie ein enormes Potenzial für ihre Geschäftstätigkeit. Gerät sie allerdings in die falschen Hände, stellt KI ein hohes Risiko dar. So können Cyberkriminelle Künstliche Intelligenz nutzen, um Cyberangriffe zu automatisieren oder zu individualisieren. Knapp zwei Drittel der Befragten sind der Meinung, dass von Hackern eingesetzte KI die Gefahr für die IT-Sicherheit ihres Unternehmens erhöht. Dagegen sehen nur 29 Prozent die Möglichkeit, ihr Unternehmen mithilfe Künstlicher Intelligenz besser vor Cyberangriffen zu schützen.



Bedeutung künstlicher Intelligenz für die IT-Sicherheit



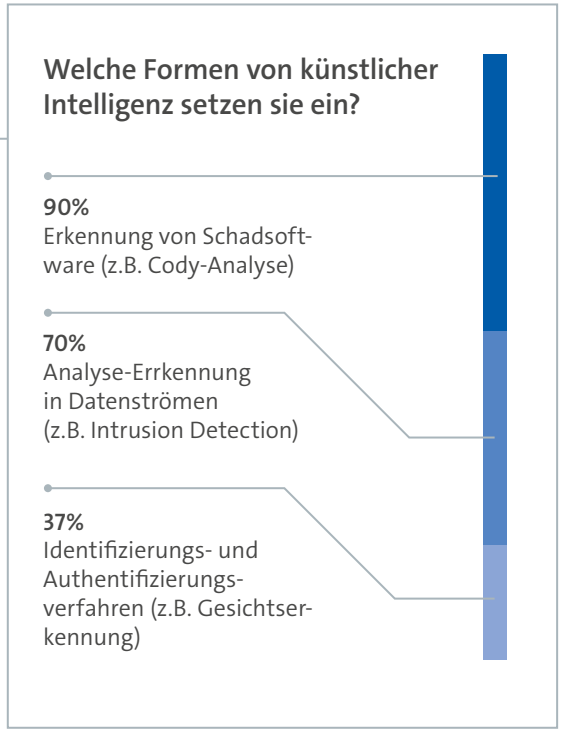
Basis: Basis: Alle Befragten (n=503). Stimmen Sie den Aussagen (voll/eher) zu oder (eher/gar) nicht? Differenz zu 100 Prozent: weiß nicht/keine Angabe

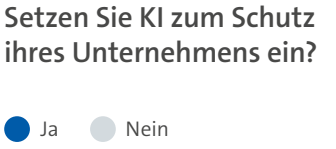
5.4

Vor allem große Unternehmen nutzen KI für IT-Sicherheit

Fast jedes achte Unternehmen (12 Prozent) setzt Künstliche Intelligenz bereits heute zu seinem eigenen Schutz vor Cyberangriffen ein.

Dabei hängt die KI-Nutzung stark von der Unternehmensgröße ab. Bei großen Unternehmen ab 250 Mitarbeitern sind es bereits 38 Prozent. Dabei stehen die Identifizierung von Schadsoftware und die Erkennung von Anomalien in Datenströmen im Vordergrund. Ein weiterer Anwendungsbereich im Bereich der IT-Sicherheit sind Identifizierungs- und Authentifizierungsverfahren.





	10 bis 49 Mitarbeiter	50 bis 249 Mitarbeiter	250+ Mitarbeiter
Ja	10%	16%	38%
Nein	84%	77%	48%

Basis: Basis: Alle Befragten (n=503). Setzen Sie Künstliche Intelligenz zum Schutz Ihres Unternehmens ein?/ Basis: Alle Befragten, die KI zum Schutz einsetzen (n=60). Welche Formen von Künstlicher Intelligenz setzen Sie zum Schutz Ihres Unternehmens ein?

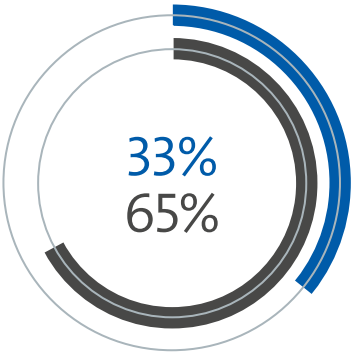
5.5

Genervt und ausgebremst: negative Folgen von Maßnahmen zur IT-Sicherheit

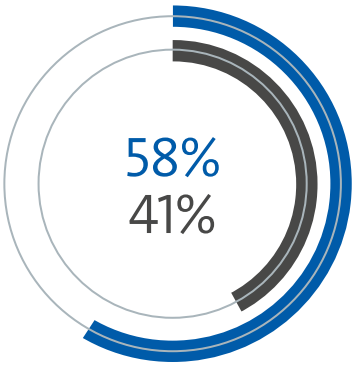
Viele Maßnahmen zur IT-Sicherheit haben Auswirkungen auf den Betriebsablauf und werden von den Mitarbeiterinnen und Mitarbeitern nicht immer positiv gesehen.

Jeder dritte Befragte gibt an, dass IT-Sicherheit die Geschäftsprozesse im Unternehmen bremst. Fast ein Viertel sieht durch IT-Sicherheit die Produktivität gemindert und für 19 Prozent bedeutet sie ein Innovationshemmnis. Vor allem stoßen Maßnahmen der IT-Sicherheit auf Widerstand bei den Beschäftigten: So reagieren in 58 Prozent der befragten Unternehmen die Mitarbeiter genervt, weil sie bestimmte Sicherheitsanforderungen erfüllen müssen, etwa komplizierte Authentifizierungsverfahren oder häufige Passwortwechsel. Ein Fünftel der Unternehmen gibt sogar an, dass Mitarbeiter bewusst die IT-Sicherheitsvorgaben umgehen.

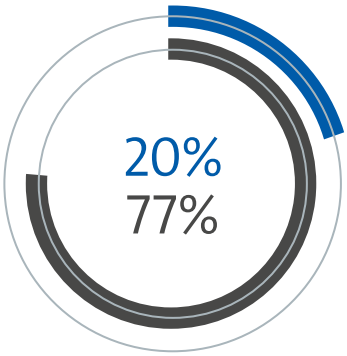
Wie bewerten Sie die Aussagen zur IT-Sicherheit in Ihrem Unternehmen?



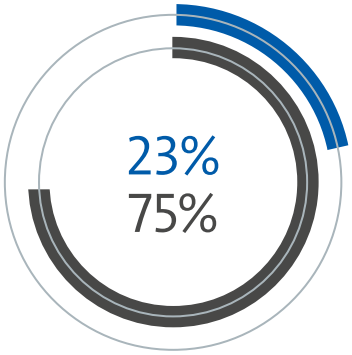
IT- Sicherheit bremst die Geschäftsprozesse in meinem Unternehmen.



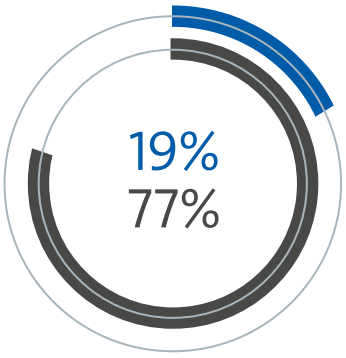
Die Mitarbeiter sind häufig genervt, weil sie bestimmte IT-Sicherheitsanforderungen erfüllen müssen (z.B. bei Authentifizierung, Passwortwechsel).



IT- Sicherheit bremst die Geschäftsprozesse in meinem Unternehmen.



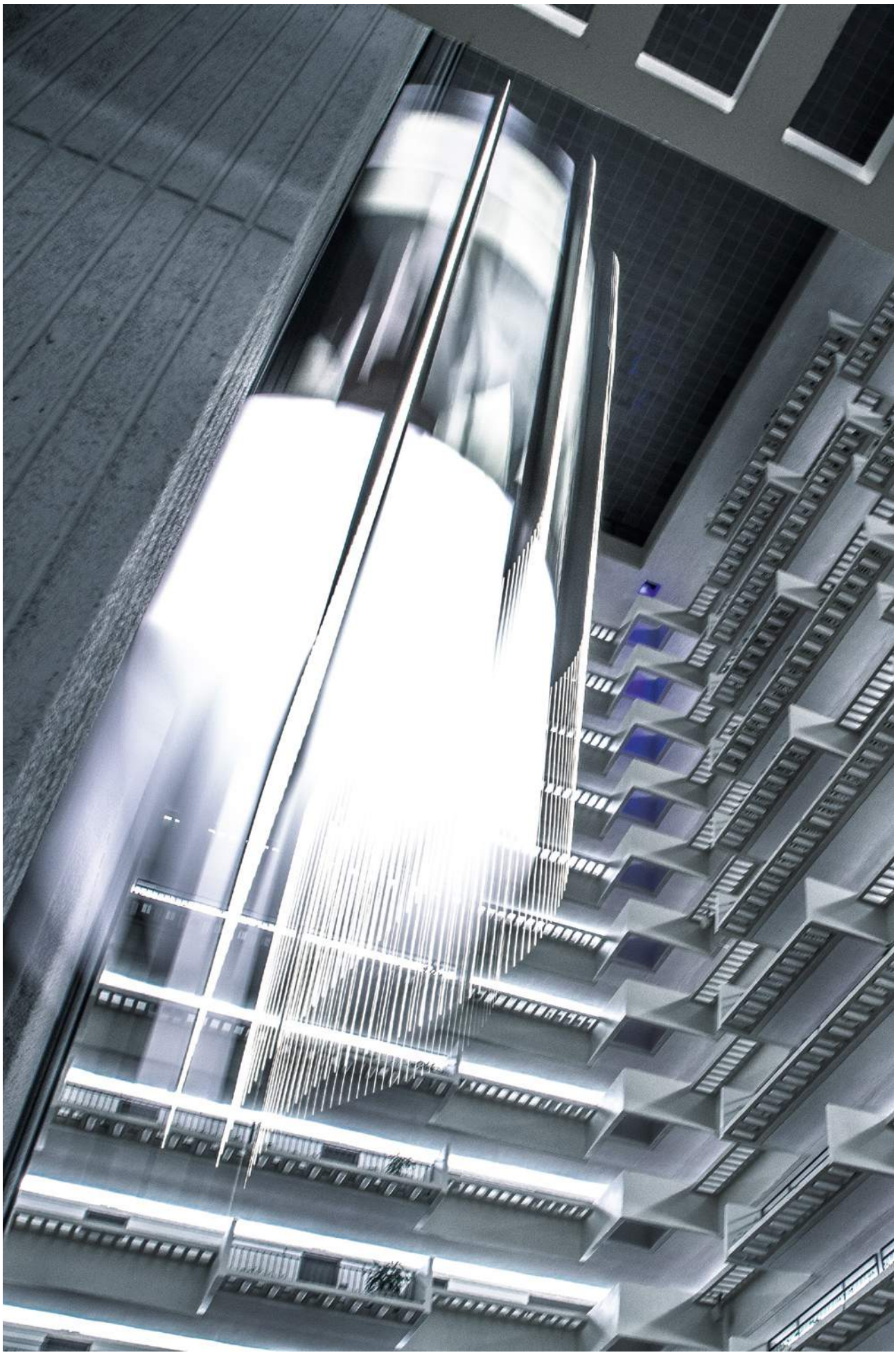
IT-Sicherheit verringert die Produktivität meines Unternehmens.



IT-Sicherheit ist in meinem Unternehmen häufig ein Innovationshemmnis.

Stimme voll/eher zu Stimme eher nicht/gar nicht zu

Basis: Alle Befragten, (n=503). Stimmen Sie den Aussagen (voll/eher) zu oder (eher/gar) nicht? Differenz zu 100 Prozent: weiß nicht/keine Angabe



6.0

Normen und Standards als IT-Sicherheitsfaktor

6.1

Technik, Ressourcen, Standards: Wie sich Unternehmen besser schützen können

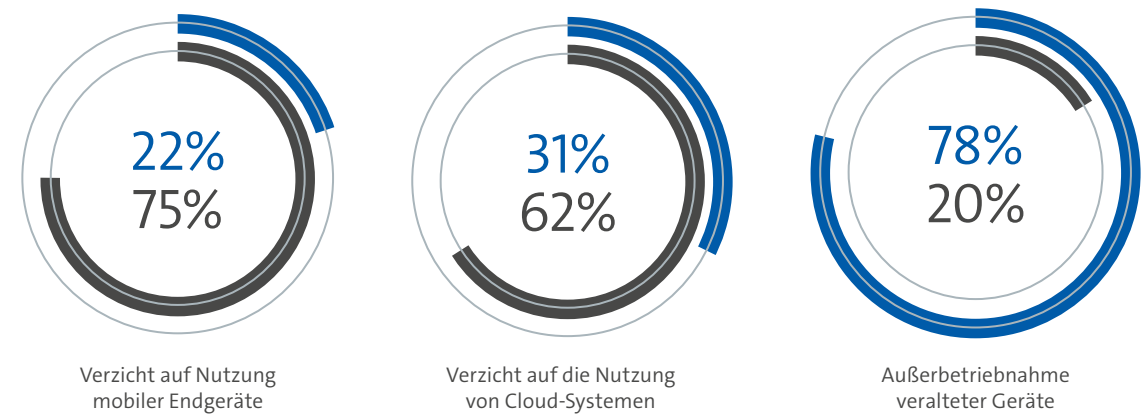
Die vorliegende Studie bildet nur einen Ausschnitt möglicher Maßnahmen ab, mit denen Unternehmen die eigene IT-Sicherheit aus Sicht der Befragten verbessern können.

Diese lassen sich in technische Maßnahmen, verfügbare Ressourcen und sonstige Rahmenbedingungen unterteilen. Technisch steht die Außerbetriebnahme veralteter Geräte und Systeme an erster Stelle. Immerhin ein Drittel der Befragten sieht im Verzicht auf Cloud-Computing und gut ein Fünftel im Verzicht auf mobile Endgeräte Lösungsansätze. In Bezug auf die Ressourcen wünscht sich jeweils gut die Hälfte der Befragten ein höheres Budget und mehr IT-Spezialisten in diesem Bereich. Voraussetzung dafür ist ein stärkeres Bewusstsein für das Thema IT-Sicherheit in der Geschäftsleitung. Das halten 72 Prozent der Befragten für notwendig.

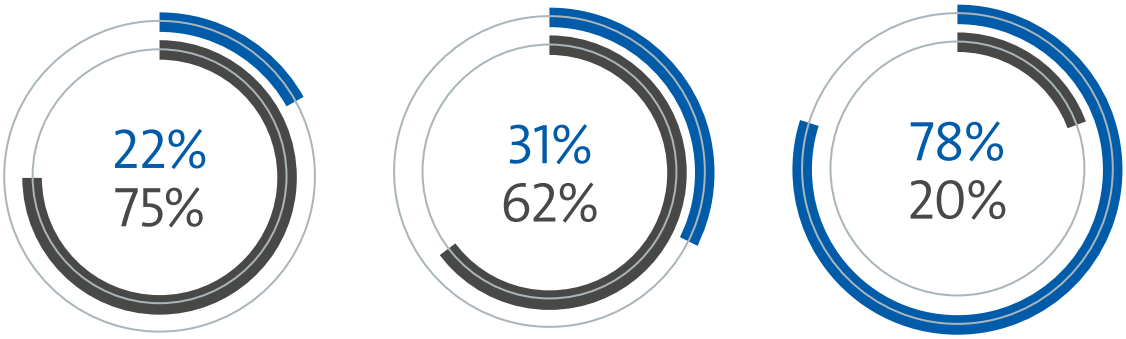
Die Hälfte der Befragten wünscht sich eine Zertifizierung von IT-Produkten und IT-Systemen durch unabhängige Prüforganisationen. Allerdings besteht im Bereich Normen und Standards ein Informationsdefizit. So wünschen sich sieben von zehn Unternehmen Orientierungshilfen zu bestehenden Regelwerken im Bereich der IT-Sicherheit. Über die Hälfte fordert die Entwicklung zusätzlicher Normen und Standards für die Umsetzung von IT-Sicherheitsmaßnahmen. Fast jeder zweite Befragte stimmt zudem der Aussage zu, dass Gesetze für die IT-Sicherheit in Unternehmen einen wichtigen Beitrag leisten können.

Halten Sie diese Maßnahmen für wichtig für die Verbesserung der IT-Sicherheit ihres Unternehmens?

Technische Maßnahmen

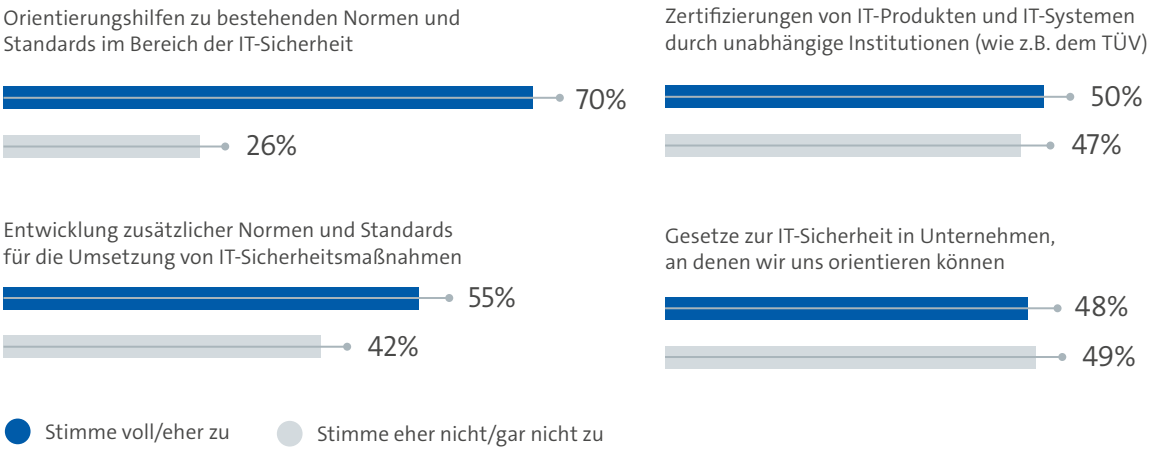


Ressourcen



Stimme voll/eher zu Stimme eher nicht/gar nicht zu

Normen



Stimme voll/eher zu Stimme eher nicht/gar nicht zu

Basis: Alle Befragten (n=503). Geben Sie bitte an, ob Sie diese Maßnahmen als wichtig für die Verbesserung der IT-Sicherheit in Ihrem Unternehmen halten. Stimmen Sie (voll/eher) zu oder (eher/gar) nicht? Differenz zu 100 Prozent: weiß nicht/keine Angabe

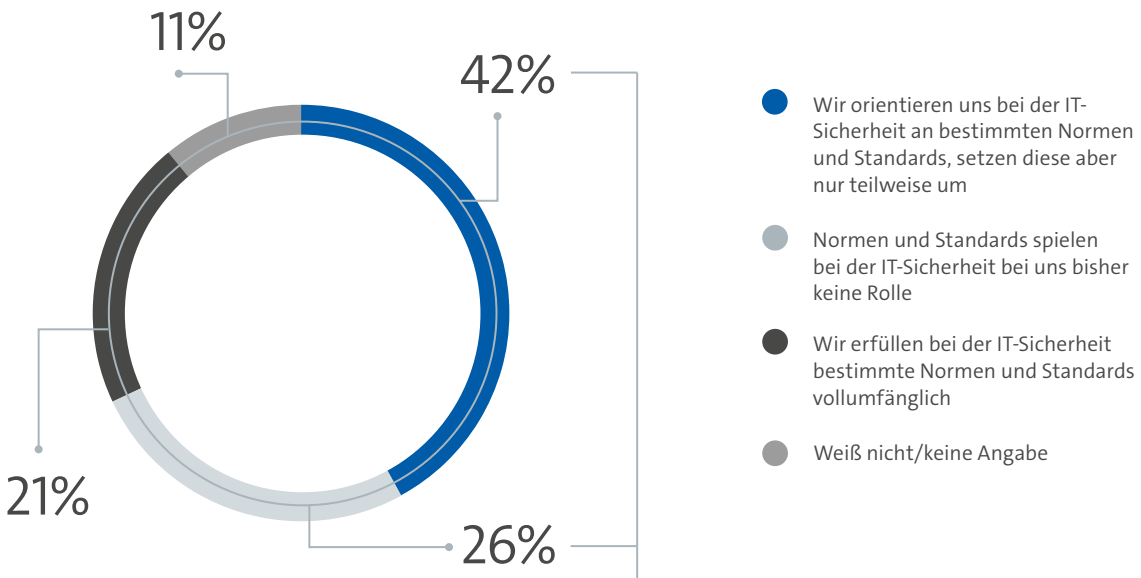
6.2

Normen und Standards geben Orientierung

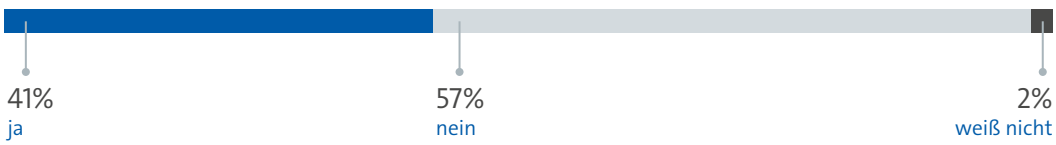
Normen und Standards zur IT-Sicherheit spielen in der Praxis bereits eine Rolle, ihre Anwendung wird aber nicht durchgängig als verbindlich betrachtet.

So gibt eine Mehrheit von 42 Prozent der befragten Unternehmen an, sie orientierten sich an bestimmten Normen und Standards, setzten diese aber nur teilweise um. Etwa ein Viertel erfüllt bei der IT-Sicherheit bestimmte Regelwerke vollumfänglich. Von solchen Unternehmen, die Normen und Standards zumindest teilweise anwenden, lassen sich dies 41 Prozent von externen unabhängigen Stellen zertifizieren.

Welche der Aussagen zu Normen und Standards für IT-Sicherheit trifft auf ihr Unternehmen zu?



Externe Prüfung/Zertifizierung der Einhaltung von Normen und Standards durch unabhängige Stellen

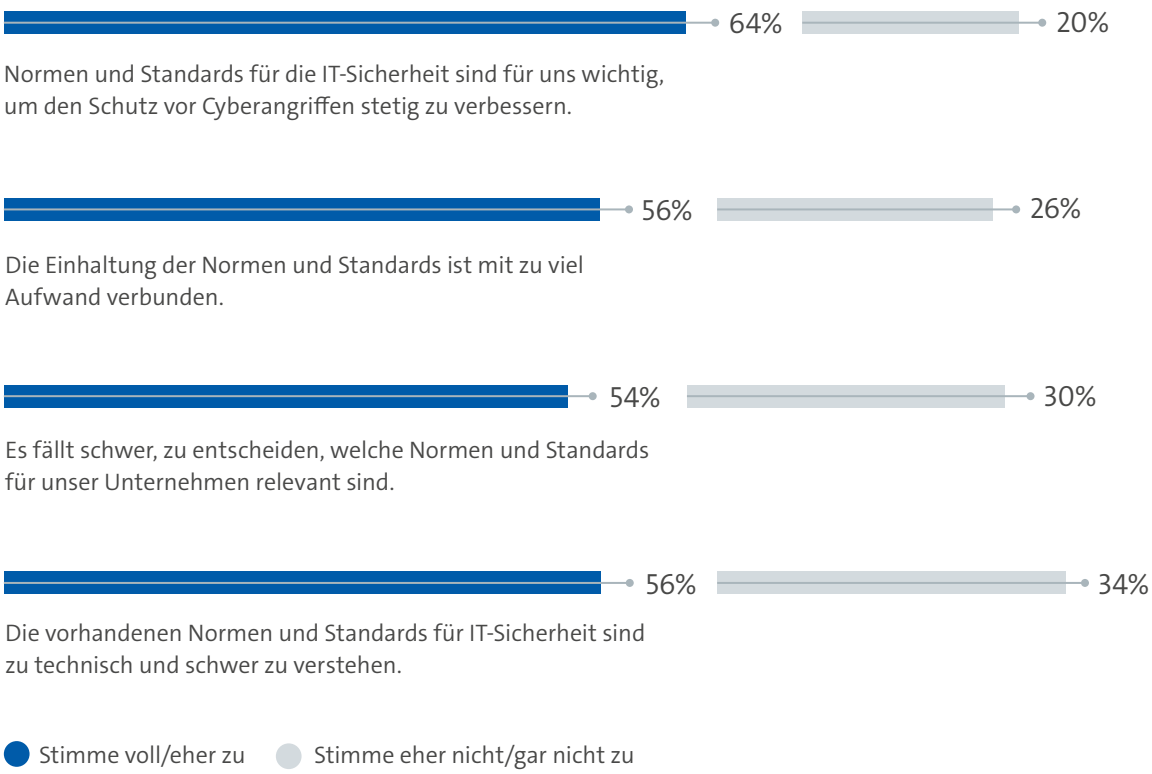


Basis: Alle Befragten (n=503). Nun lese ich Ihnen 3 Aussagen zu Normen und Standards für die IT-Sicherheit wie z.B. DIN ISO 27001 oder IT-Grundschutz vor. Bitte geben Sie an, welche der 3 Aussagen am ehesten auf Ihr Unternehmen zutrifft. Basis: Alle Befragten, deren Unternehmen Normen und Standards für IT-Sicherheit erfüllen (n=344): Lassen Sie die Einhaltung von Normen und Standards für IT-Sicherheit von unabhängigen, externen Stellen überprüfen bzw. zertifizieren?

6.3

Sinnvoll aber kompliziert: Normen und Standards

Wie bewerten Sie die Aussagen zu Normen und Standards für IT-Sicherheit?



Fast zwei Drittel der befragten Unternehmen geben an, dass Normen und Standards für sie wichtig sind, um den Schutz vor Cyberangriffen stetig zu verbessern.

Am häufigsten wird diese Ansicht von Unternehmen aus dem öffentlichen Bereich und dem Gesundheitswesen geäußert. Allerdings wird auch deutlich, dass es für die Unternehmen noch großen Informationsbedarf gibt. So fällt es über der Hälfte der befragten Unternehmen schwer, zu entscheiden, welche Normen und Standards für sie relevant sind – und 46 Prozent sind der Ansicht, dass die Regelwerke für IT-Sicherheit zu technisch und schwer verständlich sind. 56 Prozent geben zudem an, dass die Einhaltung von Normen und Standards aus ihrer Sicht mit zu viel Aufwand verbunden ist. Auffällig ist, dass bis zu einem Fünftel der Befragten zum Umgang mit Normen und Standards mit „weiß nicht“ antwortet. Das deutet darauf hin, dass sich viele Unternehmen mit diesen Themen bisher nur wenig beschäftigt haben.

Basis: Alle Befragten (n=503). Stimmen Sie den Aussagen (voll/eher) zu oder (eher/gar) nicht? Differenz zu 100 Prozent: weiß nicht/keine Angabe

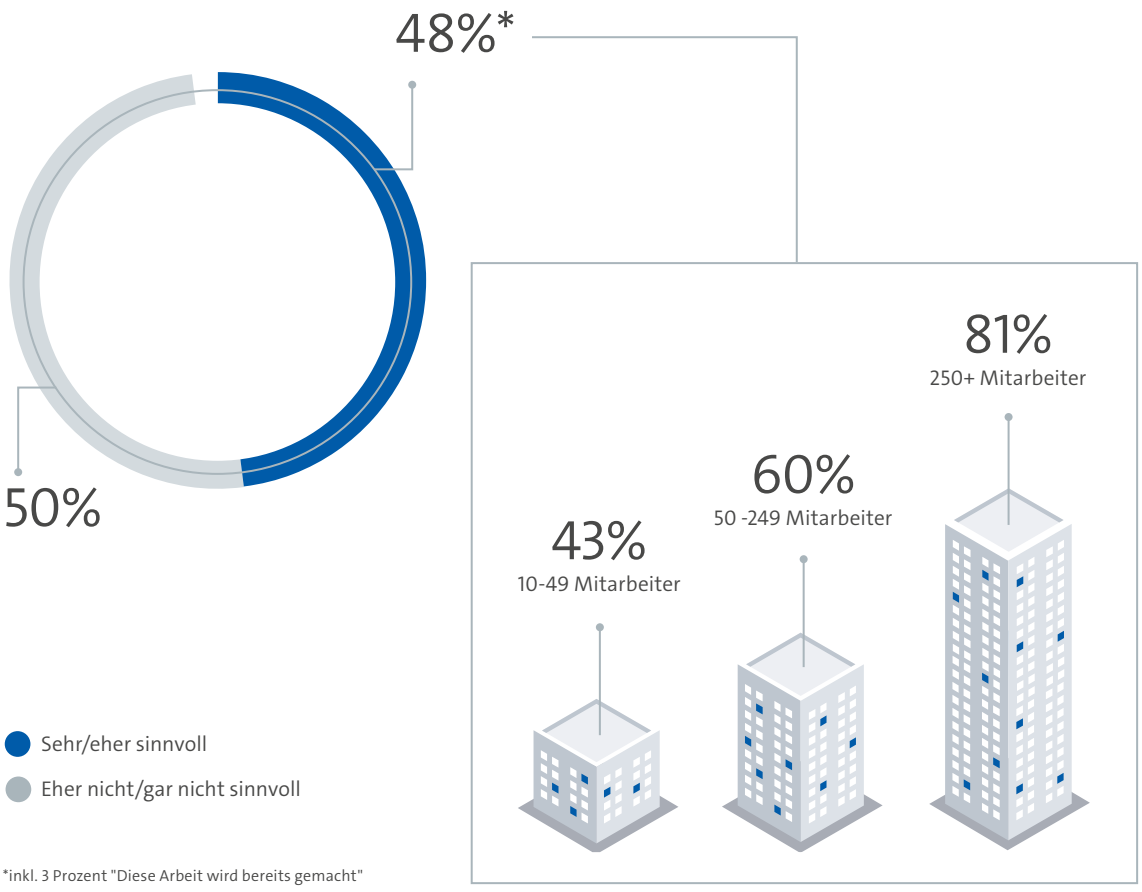
6.4

Externe Prüfungen sinnvoll für die IT-Sicherheit

Fast die Hälfte der befragten Unternehmen (48 Prozent) hält eine Zertifizierung oder Prüfung der IT-Sicherheit durch unabhängige Institutionen für sinnvoll oder lässt eine solche bereits durchführen.

Deutlich sind die Unterschiede bei der Unternehmensgröße: Besteht bei Unternehmen mit weniger als 50 Mitarbeitern nur bei 40 Prozent der Wunsch nach einer Zertifizierung ihrer IT-Sicherheit, ist es bei großen Unternehmen ab 250 Mitarbeitern mit 81 Prozent die deutliche Mehrheit.

Würden Sie eine Prüfung oder Zertifzierung durch eine unabhängige Institution sinnvoll finden, um die IT-Sicherheit zu erhöhen?



*inkl. 3 Prozent "Diese Arbeit wird bereits gemacht"

Basis: Alle Befragten (n=503). Stellen Sie sich vor, eine unabhängige Institution (z.B. der TÜV, Wirtschaftsprüfer oder das BSI) würde die IT-Sicherheit Ihres Unternehmens prüfen bzw. zertifizieren. Würden Sie das sinnvoll finden, um die IT-Sicherheit zu erhöhen?

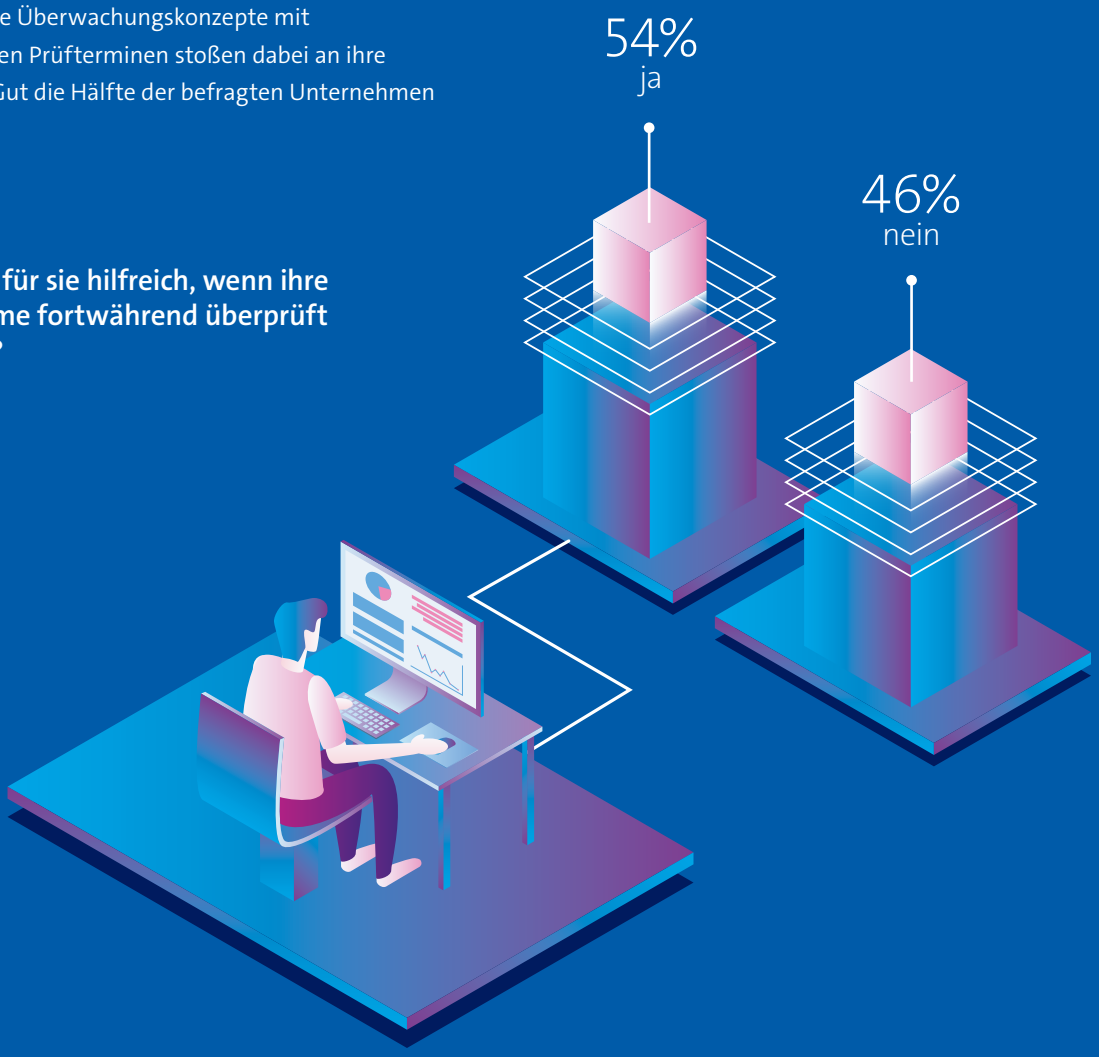
6.5

Die Hälfte befürwortet eine Echtzeitüberprüfung der IT-Systeme

Sicherheitsmaßnahmen im IT-Bereich müssen auch an die Dynamik technischer Entwicklungen, etwa durch kontinuierliche Softwareupdates, und an permanente Bedrohungsszenarien angepasst sein.

Periodische Überwachungskonzepte mit festgelegten Prüfterminen stoßen dabei an ihre Grenzen. Gut die Hälfte der befragten Unternehmen befürwortet daher einen Paradigmenwechsel in der Prüfpraxis. IT-Systeme sollen nach ihrer Auffassung fortlaufend und in Echtzeit überwacht und geprüft werden.

Wäre es für sie hilfreich, wenn ihre IT-Systeme fortwährend überprüft würden?



Basis: Alle Befragten (n=503). IT-Systeme verändern sich dauernd, zum Beispiel durch regelmäßige Updates. Wäre es für Sie hilfreich, wenn Ihre IT-Systeme nicht nur zu bestimmten Zeitpunkten, sondern fortwährend überprüft würden, um Aussagen zum Zustand der IT-Sicherheit machen zu können?

7.0

Einstellungen zu gesetzlicher Regulierung

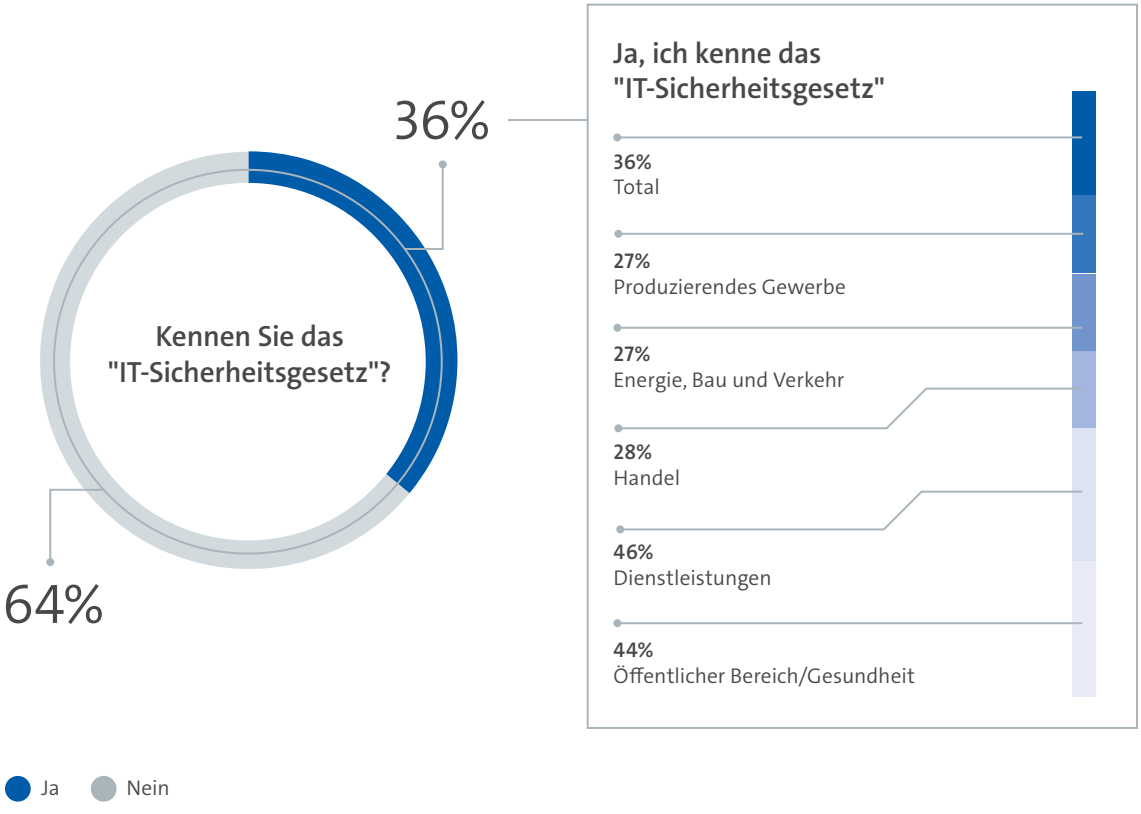
7.1

Nur wenige kennen das IT-Sicherheitsgesetz

Seit dem Jahr 2015 ist in Deutschland das „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ in Kraft.

Ziel des IT-Sicherheitsgesetzes ist es, den Schutz vor Cyberangriffen vor allem in den für unser Gemeinwesen besonders wichtigen Bereichen zu erhöhen. Zu den Kritischen Infrastrukturen (KRITIS) zählen zum Beispiel Krankenhäuser, Energieversorger, Telekommunikationsanbieter oder große Lebensmittelversorger (vgl. Kap. 8.2.). In der Umfrage gibt nur jedes dritte Unternehmen (36 Prozent) an, das IT-Sicherheitsgesetz zu kennen. Bei 64 Prozent ist das nicht der Fall. Am bekanntesten ist das IT-Sicherheitsgesetz in der Dienstleistungsbranche (46 Prozent) sowie im öffentlichen Bereich und dem Gesundheitswesen (44 Prozent).

Kennen Sie das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme?



Basis: Alle Befragten (n=503). Seit Juli 2015 gibt es das „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“, auch IT-Sicherheitsgesetz genannt. Kennen Sie dieses Gesetz? Mit * markierte Zahlen weisen auf Fallzahlen < 30 hin.

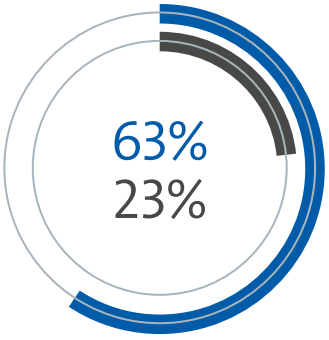
7.2

Regulierung unterstützt Unternehmen bei der IT-Sicherheit

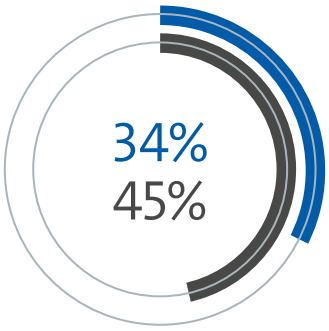
Fast zwei Drittel der Befragten sehen in regulatorischen Anforderungen eine Unterstützung, um IT-Sicherheitsmaßnahmen umzusetzen und gegenüber der Geschäftsleitung, Anteilseignern oder Mitarbeitern zu vertreten.

Mit 59 Prozent ist eine deutliche Mehrheit der Meinung, dass eine Regulierung durch den Gesetzgeber wichtig ist und zu einer höheren IT-Sicherheit in ihrem Unternehmen beiträgt. Jedes dritte Unternehmen vertritt sogar die Ansicht, das bestehende IT-Sicherheitsgesetz gehe nicht weit genug.

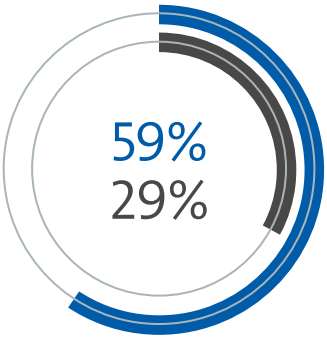
Wie bewerten Sie die Aussagen zum "IT-Sicherheitsgesetz"?



Regulatorische Anforderungen wie das IT-Sicherheitsgesetz unterstützen mich dabei, IT-Sicherheitsmaßnahmen zu vertreten und umzusetzen.



Das IT-Sicherheitsgesetz enthält sinnvolle Maßnahmen, geht aber nicht weit genug.



Die Regulierung durch den Gesetzgeber ist wichtig und trägt zu einer besseren IT-Sicherheit unseres Unternehmens bei.

Stimme voll/eher zu Stimme eher nicht/gar nicht zu

Basis: Alle Befragten (n=503). Stimmen Sie den Aussagen (voll/eher) zu oder (eher/gar) nicht? Differenz zu 100 Prozent: weiß nicht/keine Angabe

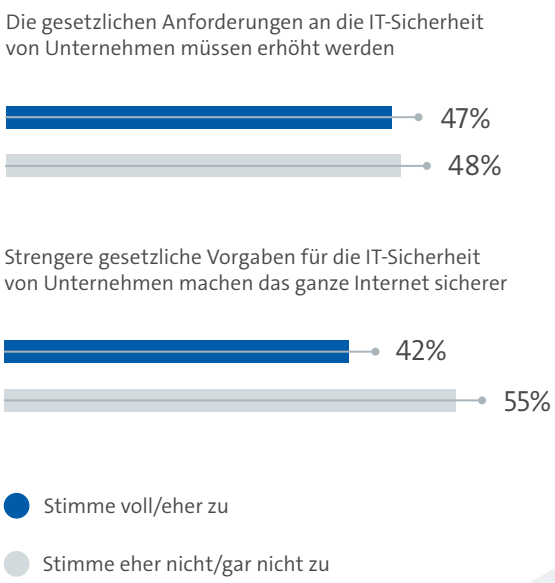
7.3

Starkes Votum für höhere gesetzliche Anforderungen

Erstaunlich viele Unternehmen geben in der Umfrage ein klares Votum für eine stärkere gesetzliche Regulierung der IT-Sicherheit in der deutschen Wirtschaft ab.

So vertritt fast die Hälfte der Befragten (48 Prozent) die Ansicht, dass die gesetzlichen Anforderungen an die IT-Sicherheit von Unternehmen erhöht werden müssen. Vier von zehn Befragten (42 Prozent) sind darüber hinaus der Überzeugung, dass strengere gesetzliche Vorgaben für die IT-Sicherheit von Unternehmen das Internet insgesamt sicherer machen würden.

Wie bewerten Sie die folgenden Aussagen zur IT-Sicherheit?



Basis: Alle Befragten (n=503). Stimmen Sie den Aussagen (voll/eher) zu oder (eher/gar) nicht? Differenz zu 100 Prozent: weiß nicht/keine Angabe

8.0

Fazit und politische Empfehlungen

8.1

Fazit

Die Ergebnisse der Studie zeigen: IT-Sicherheit hat sich in sehr vielen deutschen Unternehmen zu einem zentralen Thema ihrer Geschäftstätigkeit entwickelt. Ihre Bedeutung steigt aufgrund der fortschreitenden Digitalisierung und der zunehmenden Gefahr unterschiedlicher Angriffsszenarien. Viele Unternehmen haben bereits Erfahrungen mit schwerwiegenden Sicherheitsvorfällen oder befürchten einen Angriff. Über die möglichen Folgen ist man sich einig: Sie stellen eine schwerwiegende Gefahr für Wirtschaft und Gesellschaft dar.

Trotz eines erkennbaren Gefahrenbewusstseins werden aber auch Defizite deutlich. In vielen Unternehmen gibt es kein eigenes Budget für IT-Sicherheit. Die Umsetzung von Sicherheitsmaßnahmen wird in vielen Unternehmen als Bremse im Betriebsablauf betrachtet und kann auch am Widerstand der Belegschaft scheitern. Das ist bedenklich, weil viele Angriffsszenarien gerade solche Schwachstellen in den Sicherheitssystemen gezielt ausnutzen.

Zudem können viele Unternehmen zu Normen und Standards oder auch zum IT-Sicherheitsgesetz keine Angaben machen, obwohl es zahlreiche Best-Practice-Ansätze im Bereich der IT-Sicherheit gibt. Deutlich wird auch: IT-Sicherheit hängt auch davon ab, ob den Unternehmen dafür genügend Fachkräfte zur Verfügung stehen.

Um die IT-Sicherheit zu verbessern, gibt es von den Unternehmen ein klares Signal an die Politik: Regulierung und höhere gesetzliche Anforderungen leisten nach ihrer Ansicht einen wichtigen Beitrag, um die Sicherheit in der Wirtschaft zu erhöhen. Dabei wird insbesondere bei mittleren und größeren Unternehmen ab 50 Mitarbeitern die Prüfung und Zertifizierung durch unabhängige Institutionen als wichtiges Instrument gesehen.

8.2

Politische Empfehlungen

Wie in anderen Bereichen stellt sich auch bei der IT-Sicherheit die Frage nach der Notwendigkeit von mehr oder weniger gesetzlicher Regulierung. Für die TÜV-Organisationen ist klar: Die in alle Lebensbereiche vordringende Digitalisierung, Technologien wie Künstliche Intelligenz und die immer neuen Arten von Cyberbedrohungen machen einen grundlegenden Sinneswandel notwendig. Zum einen muss Cybersecurity fester Bestandteil der Produktsicherheit werden, um Verbraucher besser zu schützen. Und zum anderen müssen in kritischen Bereichen der Wirtschaft gesetzliche Regelungen Mindeststandards für die IT-Sicherheit vorgeben, an denen sich alle Unternehmen orientieren können. Für den TÜV-Verband ergeben sich daraus folgende Kernforderungen:

1. Anwendungsbereich des IT-Sicherheitsgesetzes erweitern – KRITIS-Fokus aufgeben

Das IT-Sicherheitsgesetz legt Sicherheitsstandards für die Betreiber kritischer Infrastrukturen (KRITIS) fest, zu denen Unternehmen bestimmter Größe aus den Bereichen Energie, Wasser, Gesundheit, Ernährung, IT und Telekommunikation, Transport und Verkehr sowie Finanz- und Versicherungswesen gehören. Bisher fallen wegen eng gefasster Kriterien nur rund 1.700 Unternehmen unter das Gesetz. Es gibt in Deutschland aber rund 400.000 Unternehmen ab 10 Mitarbeitern und weitere 3 Millionen Kleinunternehmen. Noch gar nicht erfasst sind unter anderem Entsorger, Unternehmen der Sicherheits- und Verteidigungsindustrie sowie Maschinen- und Fahrzeugbauer. Vor diesem Hintergrund wäre es konsequent, den Anwendungsbereich des IT-Sicherheitsgesetzes 2.0 auszudehnen und die Einschränkung auf KRITIS-Branchen aufzugeben.

2. Überprüfung der gesetzlichen IT-Sicherheitsstandards verbessern

Die Anforderungen des IT-Sicherheitsgesetzes sind in den branchenspezifischen Sicherheitsstandards definiert und von den Unternehmen nach „Stand der Technik“ umzusetzen. Aus Sicht des TÜV-Verbands reichen die bestehenden Vorgaben nicht aus. Die Erfahrungen der vergangenen Jahre haben gezeigt, dass es bei der Umsetzung in der Praxis häufig Defizite gibt. Es muss auf gesetzlicher Grundlage verifiziert werden können, dass die Maßnahmen in den Systemen, Prozessen und Produkten der Unternehmen erfolgreich umgesetzt worden sind.

3. Cybersecurity Act umsetzen: Produktsicherheit um IT-Sicherheit ergänzen

Der Cybersecurity Act ist seit Juli 2019 in Kraft und schafft einen allgemeinen Rechtsrahmen für die IT-Sicherheit von vernetzten Produkten und Dienstleistungen in der EU. Das macht den Weg frei, den Produktsicherheitsbegriff in Europa neu zu definieren: In Zukunft muss neben der funktionalen Sicherheit auch die digitale Sicherheit fester Bestandteil eines Produkts sein. Nur dann sollte ein Produkt in Europa auf den Markt gebracht werden dürfen. Das funktioniert aber nur, wenn die Anforderungen an die IT-Sicherheit in den Richtlinien der einzelnen Produktgruppen konsequent festgeschrieben werden – für Maschinen, Spielzeuge, Medizinprodukte, Fahrzeuge und viele andere Produkte. Der Cybersecurity Act ist dafür die Grundlage.

4. Künstliche Intelligenz nach Risikoklassen prüfen

Eine besondere Herausforderung für die IT-Sicherheit ist der Einsatz Künstlicher Intelligenz in Produkten und digitalen Anwendungen. Bei hoch automatisierten Fahrzeugen hängt die körperliche Unversehrtheit eines Menschen direkt von Systemen mit Künstlicher Intelligenz ab. In diesen Fällen müssen die Funktionen selbstlernender Algorithmen von externer Stelle überprüfbar sein. Dafür benötigen die Prüfer Zugang zur Software und den Daten der Systeme. Je nach Risikoklasse eines KI-Systems können unterschiedliche Anforderungen an die Sicherheit und die Prüfungen gestellt werden. Entsprechende Vorschläge hat auch die Datenethikkommission der Bundesregierung in ihrem Abschlussbericht aufgegriffen.

5. Geplantes IT-Sicherheitskennzeichen aufwerten

Das geplante IT-Sicherheitskennzeichen für vernetzte Produkte ist ein Schritt in die richtige Richtung, hat aber Schwächen. Es soll aus zwei Teilen bestehen: einer Herstellerselbsterklärung und einer Information des BSI. Kunden können über einen QR-Code recherchieren, ob das Produkt die „Versprechen“ des Herstellers aktuell hält. Das heißt, das Prüfzeichen allein sagt nicht viel über die Sicherheit des Produkts aus. Neben dem Produkt selbst sollten aus Sicht des TÜV-Verbands auch qualitäts- und sicherheitsrelevante Unternehmensprozesse bei den Herstellern überprüft werden. Hier könnten unabhängige Prüforganisationen Verantwortung übernehmen und das Prüfzeichen substanziell aufwerten.

6. Digitale Sicherheitsarchitektur schaffen

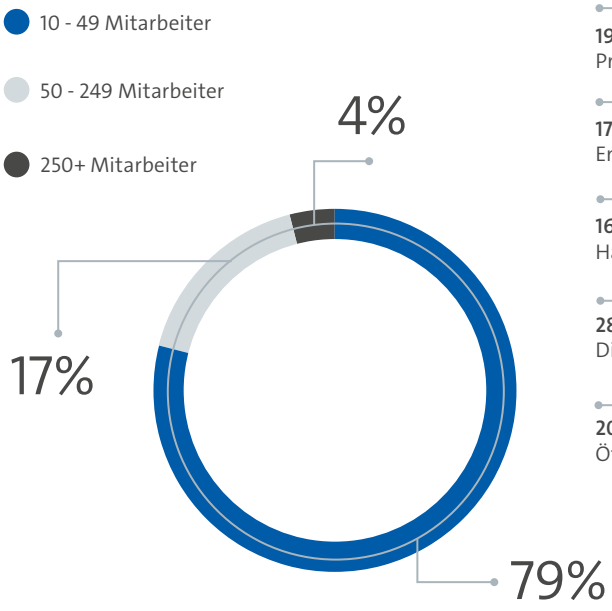
Die Cybersicherheitsstrategie der Bundesregierung muss zügig weiterentwickelt werden. Deutschland und die EU brauchen eine ganzheitliche „Digitale Sicherheitsarchitektur“. Diese muss auf mehreren Säulen stehen: Sie muss erstens einen geeigneten gesetzlichen Rahmen schaffen. Sie muss zweitens die handelnden Institutionen einbinden und drittens die Entwicklung technologischer Kompetenzen fördern. Fundament einer Digitalen Sicherheitsarchitektur muss das Know-how von Menschen und Organisationen sein: Dazu gehört die Aus- und Weiterbildung von Fachkräften, Technikkompetenz und eine enge Verzahnung von Wirtschaft, Wissenschaft und staatlichen Stellen wie dem BSI.

Methodik

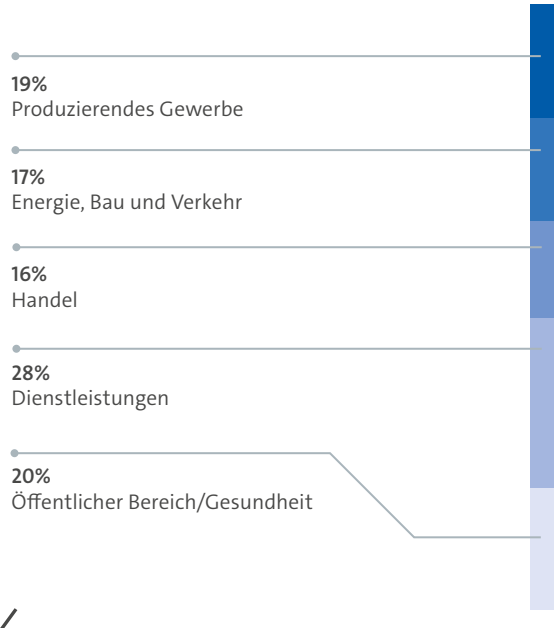
Im Auftrag des TÜV-Verbands führte die Ipsos GmbH eine Unternehmensbefragung zum Thema Cybersecurity durch. Im Rahmen der Befragung wurden deutsche Unternehmen unter anderem zum aktuellen Stand der IT-Sicherheit, zur Relevanz des Themas für ihr Unternehmen, zu den geltenden Normen und Standards der IT-Sicherheit sowie zu ihrer Einschätzung von unabhängigen Zertifizierungen von IT-Sicherheitsmaßnahmen und von IT-Produkten befragt.

Die Grundgesamtheit der Stichprobe bildeten Verantwortliche für IT-Sicherheit, IT-Leiter sowie die Geschäftsleitung deutscher Unternehmen ab einer Unternehmensgröße von zehn Mitarbeitern. Für die Befragung wurde eine repräsentative Unternehmensstichprobe von 503 Unternehmen aus öffentlich zugänglichen Registern gezogen. Die Stichprobe bildet ein repräsentatives Abbild nach den Merkmalen „Unternehmensgröße“, „Branche“ und „Nielsen-Region“. Die Befragung wurde mithilfe von computergestützten telefonischen Interviews (CATI) im August und September 2019 durchgeführt.

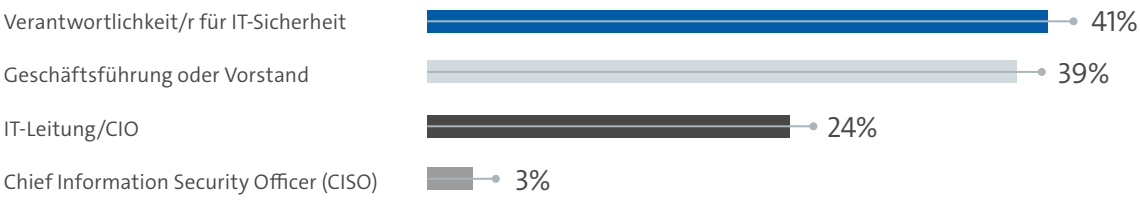
Unternehmensgröße



Branchen



Welche Tätigkeiten üben Sie im Unternehmen aus? (Mehrfachnennung)



Ansprechpartner und Kontakt

Über den TÜV-Verband

Der Verband der TÜV e.V. (VdTÜV) vertritt die politischen und fachlichen Interessen seiner Mitglieder gegenüber Politik, Verwaltung, Wirtschaft und Öffentlichkeit. Der Verband setzt sich für technische und digitale Sicherheit bei Produkten, Anlagen und Dienstleistungen durch unabhängige Prüfungen und qualifizierte Weiterbildung ein. Mit seinen Mitgliedern verfolgt der TÜV-Verband das Ziel, das hohe Niveau der technischen Sicherheit in unserer Gesellschaft zu wahren und Vertrauen für die digitale Welt zu schaffen.

Ansprechpartner

Dr. Joachim Bühler
Geschäftsführer
T +49 30 760095-350
joachim.buehler@vdtuev.de

Marc Fliehe
Leiter Digitales und IT-Sicherheit
T +49 30 760095-460
marc.fliehe@vdtuev.de

BILDNACHWEIS
Seite 03 TÜV Rheinland, Seite 08 shinnarhch / freepik.com, Seite 14 sebdeck / freepik.com, Seite 20 monsitj / iStock,
Seite 30 pressfoto / freepik.com, Seite 36 AzmanJaka / iStock, Seite 38 Upal Patel / unsplash, Seite 46 Massimo Virgilio / unsplash

KONZEPTION & DESIGN
Nordpunkt Designagentur GmbH

Herausgeber

Verband der TÜV e. V.
Friedrichstraße 136, 10117 Berlin
Tel.: +49 30 760095-400
Fax: +49 30 760095-401
E-Mail: berlin@vdtuev.de
www.vdtuev.de
www.twitter.com/vdtuev_news