CIO CSO COMPUTERWOCHE VOICE OF DIGITAL

STUDIE

IT-SECURITY-TRENDS 2024

FORTINET SPIRIT/21 IT that works.

Ein aktuelles Studienprojekt von CIO, CSO und COMPUTERWOCHE

Partner

FORTINET

SPIRIT/21
IT that works.

Security und KI: Miteinander, gegeneinander – oder beides?

Simon Hülsbömer,
Senior Research Manager, CIO, CSO & COMPUTERWOCHE

Man kann nur schützen, was man kennt – mit diesem Satz zieht unser Analyst Oliver Schonschek sein zusammenfassendes Fazit zu dieser Studie (siehe Seite 38). Und bezieht sich damit auf die Absicherung von KI-Tools und -Systemen, die die Unternehmen bereits heute im Einsatz haben. Denn diese sind oft nur unzureichend geschützt – unter anderem deshalb, weil eine umfassende KI-Strategie fehlt, die auch Sicherheitsaspekte berücksichtigt. Nicht einmal sechs von zehn Unternehmen haben bisher eine KI-Strategie entwickelt.

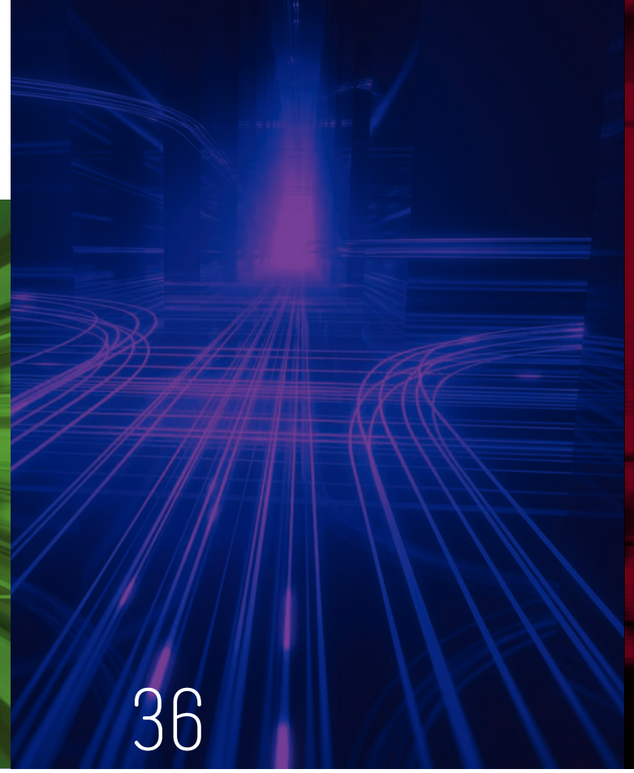
Somit entsteht schnell der Eindruck einer Unkenntnis des Themas KI-Sicherheit – trotz der (hohen) Relevanz, die 90 Prozent der Unternehmen ihm beimessen. Es gilt also, die eingesetzten KI-Systeme (noch) besser kennenzulernen und geeignete Sicherheitsmechanismen zu deren Schutz zu etablieren, beispielsweise mit speziellen KI-Firewalls, die sich mehr als 40 Prozent der Unternehmen für den Eigengebrauch wünschen.

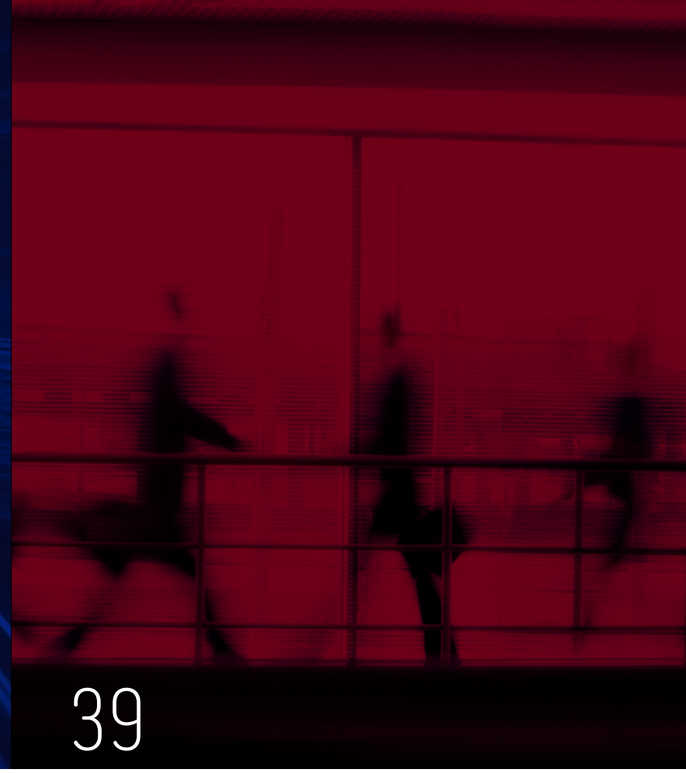
Die Sicherheit von KI-Systemen ist aber nur die eine Seite der Medaille. Auf der anderen Seite stehen die Angriffe, die überhaupt erst durch künstliche Intelligenz möglich werden. Der Schutz vor solchen KI-Attacken ist für 86 Prozent der Unternehmen (sehr) relevant – und damit für die Befragten fast genauso wichtig wie das Thema Security für KI. Es überrascht etwas, dass sowohl der Aufbau personeller Ressourcen im IT-Security-Bereich als auch eine bessere Ransomware-Resilienz, beides Dauerbrenner im Bereich Security, im „Relevanz-Ranking“ erst knapp dahinter liegen (mit jeweils etwas mehr als 80 Prozent der Nennungen).

Eine wichtige Frage wird sein, ob KI heute und vor allem in Zukunft für mehr Sicherheit oder doch eher für mehr Gefahren in den Unternehmen sorgen wird. Hier steht, wie die Studie zeigt, eine allgemein akzeptierte Antwort noch aus: Rund 31 Prozent der Befragten stimmen der These zu, dass KI-basierte Copilot-Systeme ihrem Unternehmen dabei helfen, die Sicherheit zu verbessern – rund 26 Prozent indes halten dagegen.

Es ist aber egal, ob nun „Security für KI“, „Security mit KI” oder „Security trotz KI“ gilt. Kein Unternehmen wird IT-Security in Zukunft mehr denken, planen oder gar praktisch umsetzen können, ohne das Thema künstliche Intelligenz mit einzupreisen – sei es in die eine oder in die andere Richtung.

Seien Sie gespannt, welche Erkenntnisse – auch abseits von künstlicher Intelligenz – die vorliegende Studie „IT-Security-Trends 2024“ bereithält. Ich wünsche Ihnen eine spannende Lektüre!





Inhalt

10 20 36 39

Die wichtigsten Ergebnisse

Weitere Studienergebnisse

Blick in die Zukunft

CIO-Agenda 2024

Management Summary

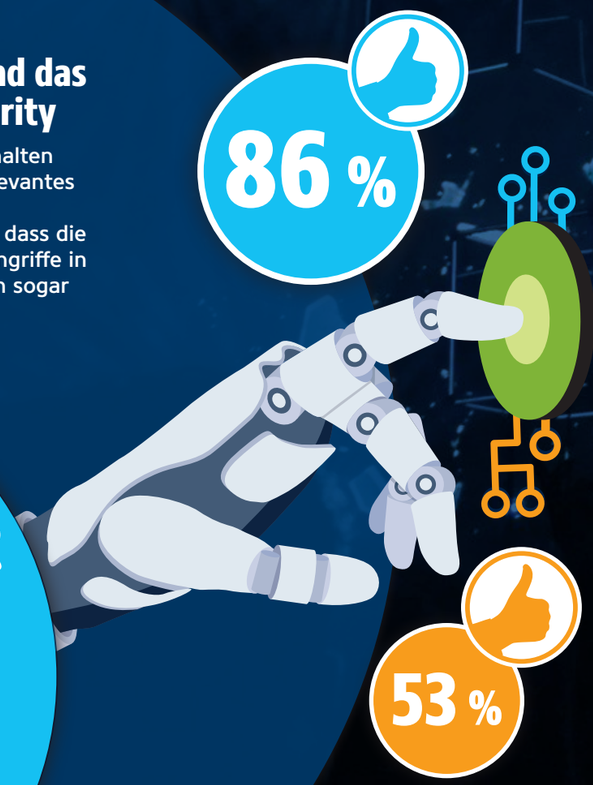
Die Key Findings im Überblick

Mehr Schutz für KI-Systeme ist den meisten Unternehmen wichtig

Für 15 Prozent der Unternehmen ist der Bedarf an speziellen Security-Maßnahmen zum Schutz von KI-Systemen „essenziell“. 35 Prozent halten ihn für „sehr hoch“, 26 Prozent für „hoch“, 14 Prozent für immer noch „eher hoch“. Insgesamt sind damit **neun von zehn Befragten** der Auffassung, dass dies ein relevantes Thema ist.

KI-basierte Angriffe sind das Trendthema der Security

86 Prozent der Unternehmen halten KI-gesteuerte Attacken für ein relevantes Thema in der IT-Security.
53 Prozent der Befragten meinen, dass die Bedeutung solcher KI-gestützter Angriffe in den nächsten zwei bis drei Jahren sogar noch zunehmen wird.

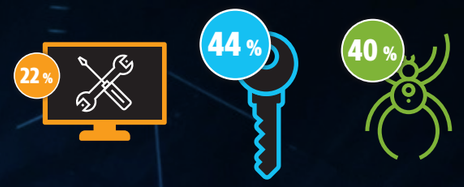


Mangel an Personal und Know-how sind die größten Security-Hemmnisse

Fehlendes Personal ist für 41 Prozent der befragten Unternehmen ein Hindernis für ihren IT-Sicherheitsbereich, das damit einhergehende **fehlende Know-how** für 28 Prozent, fehlendes Budget für 25 Prozent. Immerhin acht Prozent der Befragten sehen für sich indes **keinerlei Security-Hindernisse**.

Unternehmen investieren eher in IAM als in Ransomware-Schutz

Nur 22 Prozent der Unternehmen investieren in einen spezialisierten **Schutz vor Ransomware-Attacken**, doppelt so viele (44 Prozent) in **Identity and Access Management (IAM)**. Sicherheitsarchitekturen wie **Zero Trust** stehen in 40 Prozent der Unternehmen auf der Investitionsliste.



NIS2-Umsetzung läuft für die meisten Unternehmen nach Plan

Mehr als **neun von zehn der von der europäischen NIS2-Richtlinie betroffenen Unternehmen** geben an, dass sie die neuen Vorgaben bereits umgesetzt haben oder dies bis Jahresende 2024 schaffen werden.

Security Automation ist immer noch eine Insellösung

Geht es um die Automatisierung von Security-Funktionen, kommt diese vor allem bereits bei der **Erkennung** (62 Prozent) und **Meldung** (59 Prozent) von Angriffen zum Einsatz. Bereiche wie **Forensik** (24 Prozent) oder **Awareness-Trainings** (23 Prozent) sind indes deutlich weniger automatisiert.

Security-Tools und -Anbieter werden konsolidiert

Der größte Teil der befragten Unternehmen achtet im Zuge der technischen Investitionen bereits auf eine **Konsolidierung** der eingesetzten **Security-Tools** (96 Prozent) und **-Hersteller** (93 Prozent) oder plant dies künftig zu tun.

Die Security-Community ist im Zwiespalt

Trotz bekräftigtem Fachkräftemangel stimmen nur **26 Prozent** der Unternehmen **(voll und ganz)** der Aussage **zu**, dass sie ihre **offenen Security-Stellen nicht besetzt** bekommen – **28 Prozent stimmen** der Aussage indes **(überhaupt) nicht zu**.
Ein ähnlich kontroverses Bild ergibt sich bei der Frage der Notwendigkeit von Security-Dienstleistern.

Das zentrale Ergebnis

Schutz vor KI-gesteuerten Angriffen relevanter als der Fachkräftemangel

Zur Relevanz bestimmter IT-Security-Themen befragt, nennen 86 Prozent der Unternehmen den Schutz vor KI-gesteuerten Angriffen. Damit liegt dieses Thema unter anderem knapp vor den Themen Aufbau personeller Ressourcen im IT-Security-Bereich (83 Prozent) und Ransomware-Resilienz (82 Prozent).

Auch andere Themen mit KI-Bezug stehen in der Liste der Themen mit Relevanz für die IT-Security weit oben. Eine spezielle Security für KI-Systeme, um diese vor Angriffen und Missbrauch zu nutzen, sind für 82 Prozent der Befragten relevant, KI-basierte Security und Security-Automatisierung immerhin noch für 74 Prozent.

Trotz der laufenden NIS2-Umsetzung *(vgl. Weiteres Key Finding 2, Seite 12 f.)* haben dagegen Angriffe auf und aus der Supply Chain eine geringere Wahrnehmung bei den befragten Unternehmen: Den Schutz der Lieferkette betrachten 78 Prozent als relevant – einen vergleichbaren Wert erreicht die Zero Trust Security, die gerade bei der zunehmend mobilen Arbeit und im Homeoffice so wichtig wäre.

Nach Auffassung von 53 Prozent der befragten Unternehmen wird die Bedeutung des Schutzes vor KI-gesteuerten Cyberangriffen in den nächsten zwei bis drei Jahren noch steigen. Bei KI-basierter Security sehen immer noch 42 Prozent der Befragten eine zunehmende Bedeutung in den nächsten Jahren, bei Ransomware-Resilienz dagegen nur 32 Prozent. Ebenfalls 32 Prozent der Unternehmen meinen, Security für KI-Systeme würde an Bedeutung zulegen.

Künstliche Intelligenz (KI) ist damit gleich mehrfach ein zentraler Trend der IT-Security – als Mittel der Angreifenden, als Unterstützung einer verbesserten Verteidigung sowie als schutzbedürftige Technologie.

Welche dieser IT-Security-Themen werden für Ihr Unternehmen in den nächsten 2 bis 3 Jahren an Relevanz (deutlich) zunehmen?

Angaben in Prozent. Mehrfachnennungen möglich. Basis: n = 339

Schutz vor KI-gesteuerten Angriffen	52,5
KI-basierte Security / Security Automation	41,6
Ransomware-Resilienz	32,2
Security für KI-Systeme (Daten, ggf. Anwendungen / Modelle)	31,6
Zero Trust Security	28,0
Schutz der Supply Chain (z.B. durch Einsatz einer Digital Twin Supply Chain)	26,0
Extended Security & Response (XDR)	23,3
IoT-Security (Internet of Things)	22,1
Infrastrukturelle Resilienz	18,9
Aufbau personeller Ressourcen im Bereich IT-Security	18,6
Unternehmensübergreifende Cybersecurity-Allianzen	18,0
Secure Access Service Edge (SASE)	14,2
Quantenkryptografie	12,4
Allgemeine Verbesserung der Security Awareness der Beschäftigten	12,4
DevSecOps / SecDevOps	12,1
Dezentrale Identitätslösungen (DID)	10,3

Wie relevant sind die aufgeführten IT-Security-Themen für Ihr Unternehmen?

Angaben in Prozent. Dargestellt sind jeweils die kumulierten Werte für „sehr relevant“ und „relevant“ sowie „weniger relevant“ und „gar nicht relevant“. Basis: n = 314-331

Die weiteren Key Findings

Zahlen und Analysen, die aus Sicht des Marktforschungsteams besonders wichtig sind

IT-Security-Trends 2024

Der Schutzbedarf bei KI-Systemen wird als hoch angesehen

15 Prozent der befragten Unternehmen stufen spezielle IT-Sicherheitsmaßnahmen zum Schutz von KI-Systemen als „essenziell“ ein, für weitere 75 Prozent ist der Bedarf für einen solchen Schutz „eher hoch“ bis „sehr hoch“. Besonders wichtig erscheint 43 Prozent der Unternehmen eine spezielle Firewall für KI.

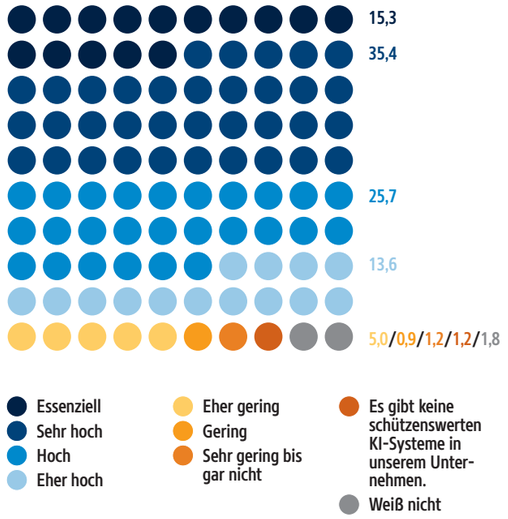
Selbst für kleinere Betriebe mit weniger als 500 Beschäftigten hat der Schutz für KI-Systeme gegen Attacken, Missbrauch und Manipulation der Lernmodelle und Daten einen hohen oder sogar zentralen Stellenwert – insgesamt 83 Prozent in dieser Befragtengruppe geben eine entsprechende Einschätzung ab. Bei den großen Unternehmen mit mehr als 1.000 Beschäftigten erhöht sich dieser Anteil auf 94 Prozent.

Unter den CISOs sind beachtliche 97 Prozent von einem entsprechenden Schutzbedarf der KI-Systeme überzeugt, in den Fachbereichen sind es 75 Prozent der Befragten. Auch die Höhe des jährlichen IT-Budgets des Unternehmens hat einen Einfluss auf die wahrgenommene Bedeutung für einen Schutz von KI-Systemen. 87 Prozent der Unternehmen mit einem jährlichen IT-Budget von unter zehn Millionen Euro sehen einen hohen Schutzbedarf für KI – bei den Betrieben mit einem noch höheren Budget sind es 96 Prozent.

Die Firmen, die einen hohen oder essenziellen KI-Schutzbedarf sehen, wünschen sich als Security-Funktionen in diesem Bereich in erster Linie eine spezielle KI-Firewall (43 Prozent), die Unterstützung von Zero Trust (38 Prozent) – dies übrigens besonders stark seitens der CISOs eingefordert – und Data Loss Prevention (37 Prozent).

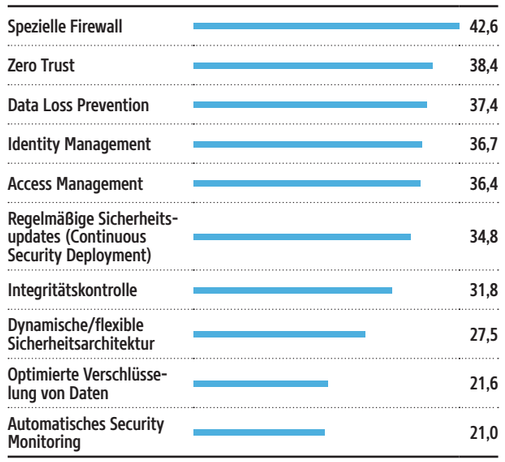
Wie hoch ist Ihrer Meinung nach der Bedarf an dedizierten IT-Security-Maßnahmen/-Tools zum Schutz von KI-Systemen in Ihrem Unternehmen?

Angaben in Prozent. Basis: n = 339



Sie sehen für Ihr Unternehmen gesteigerten Bedarf an dedizierten IT-Security-Maßnahmen/-Tools zum Schutz von KI-Systemen: Welche Funktionen wünschen Sie sich dabei am meisten?

Angaben in Prozent. Mehrfachnennungen möglich. Filter: Unternehmen, die einen eher hohen bis essenziellen Bedarf an dedizierten IT-Security-Maßnahmen zum Schutz von KI-Systemen sehen. Basis: n = 305



2

Keine Probleme mit NIS2-Vorbereitungen

Obwohl das deutsche NIS2-Umsetzungsgesetz zum Zeitpunkt der Befragung noch nicht in trockenen Tüchern ist, geben 94 Prozent der befragten Unternehmen an, dass ihre Vorbereitungen auf NIS2 bereits abgeschlossen seien oder bis Ende des Jahres 2024 beendet sein werden.

Die neue EU-Richtlinie zur Cybersicherheit NIS2 betrifft nach deren eigenen Angaben 62 Prozent der Unternehmen, die an der Studie teilnehmen. 31 Prozent erklären indes, nicht von NIS2 betroffen zu sein, die restlichen sieben Prozent sind sich noch unsicher. Selbst unter den kleineren Unternehmen mit weniger als 500 Beschäftigten sind es immer noch 48 Prozent, die meinen, unter NIS2 reguliert zu werden – ebenso viele geben an, nicht von der neuen Cybersicherheitsrichtlinie betroffen zu sein.

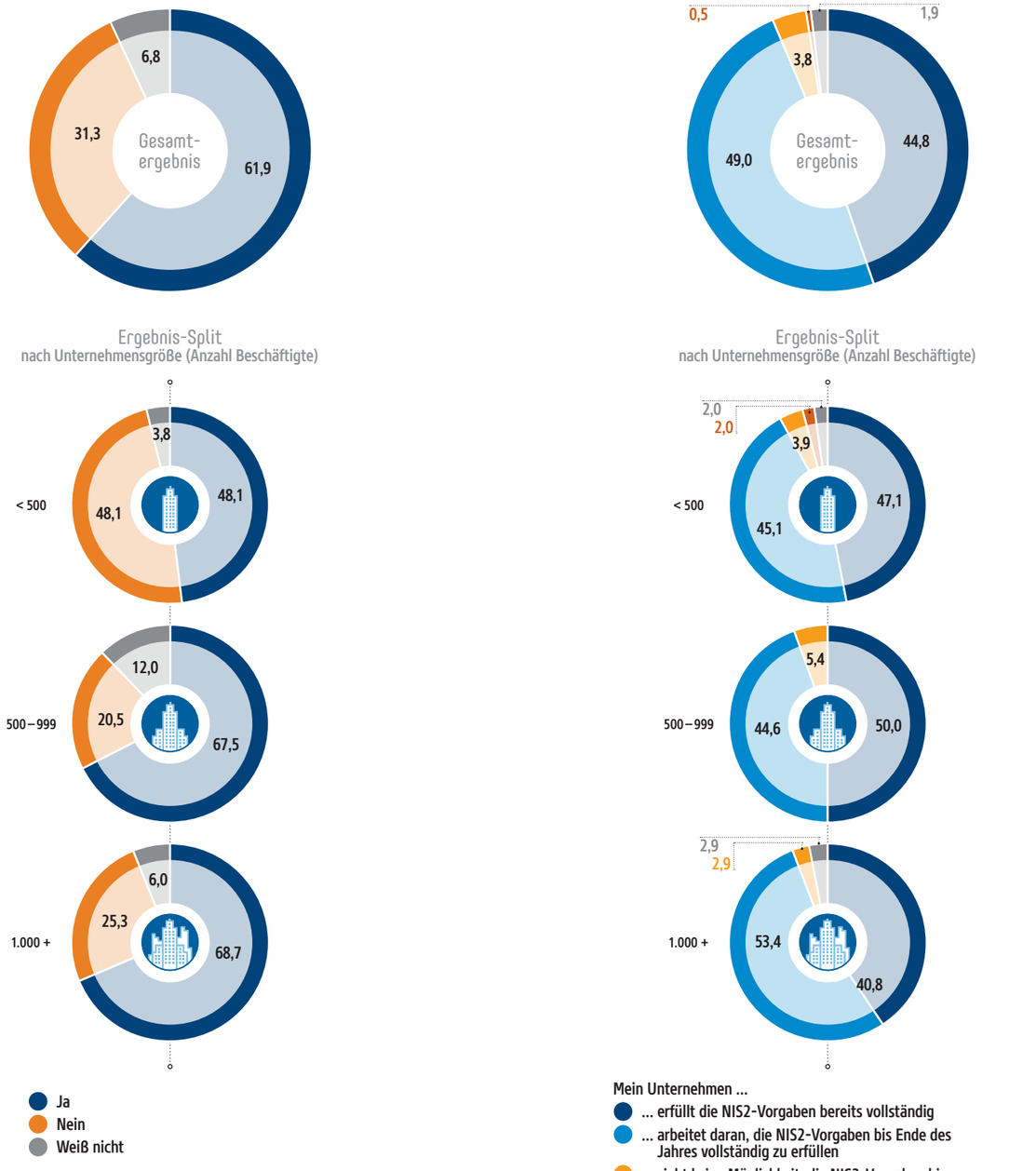
Mit steigender Beschäftigtenzahl erhöht sich auch der Anteil der von NIS2 betroffenen Unternehmen. Bei 500 bis 999 Beschäftigten liegt der Anteil der unter NIS2 regulierten Unternehmen bei 68 Prozent, ab 1.000 Beschäftigten sind es dann 69 Prozent der befragten Unternehmen, die sich von NIS2 betroffen sehen.

Interessant ist, dass immerhin zwölf Prozent der mittelgroßen Unternehmen mit 500 bis 999 Beschäftigten noch nicht sicher sind, ob NIS2 sie betrifft oder nicht. Bedenklich ist, dass unter den – zugegeben sehr wenigen – befragten CISOs ganze elf Prozent nicht sagen können, ob NIS2 sie betrifft oder nicht. In den etwas stärker in der Befragung vertretenen Fachbereichen sind es sogar 14 Prozent.

Unter den von NIS2 betroffenen Unternehmen finden sich den eigenen Angaben zufolge 45 Prozent, die bereits alle Vorgaben von

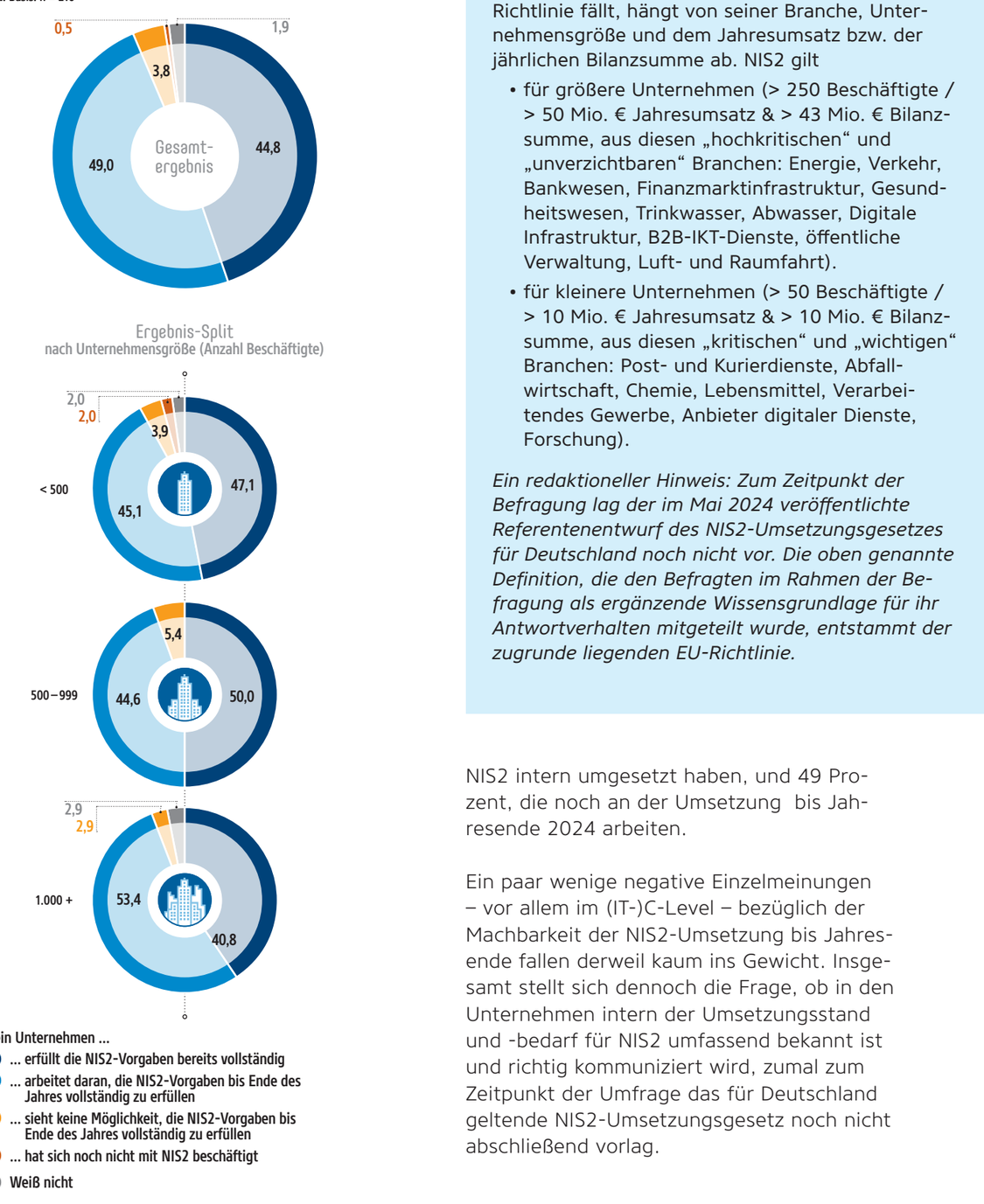
Ist Ihr Unternehmen von der NIS2-Richtlinie betroffen?

Angaben in Prozent. Basis: n = 339



Wie gut ist Ihr Unternehmen bereits auf NIS2 vorbereitet?

Angaben in Prozent. Filter: Unternehmen, die von der NIS2-Richtlinie betroffen sind. Basis: n = 210



NIS2-Richtlinie

Die NIS2-Richtlinie (Network and Information Systems Directive 2) ist eine europäische Rechtsvorschrift, die auf die Verbesserung der Cybersecurity und des Schutzes kritischer Infrastrukturen abzielt. Sie muss bis Oktober 2024 von allen EU-Staaten in nationales Recht überführt werden.

Ob ein Unternehmen unter die Vorgaben der NIS2-Richtlinie fällt, hängt von seiner Branche, Unternehmensgröße und dem Jahresumsatz bzw. der jährlichen Bilanzsumme ab. NIS2 gilt

- für größere Unternehmen (> 250 Beschäftigte / > 50 Mio. € Jahresumsatz & > 43 Mio. € Bilanzsumme, aus diesen „hochkritischen“ und „unverzichtbaren“ Branchen: Energie, Verkehr, Bankwesen, Finanzmarktinfrastruktur, Gesundheitswesen, Trinkwasser, Abwasser, Digitale Infrastruktur, B2B-IKT-Dienste, öffentliche Verwaltung, Luft- und Raumfahrt).
- für kleinere Unternehmen (> 50 Beschäftigte / > 10 Mio. € Jahresumsatz & > 10 Mio. € Bilanzsumme, aus diesen „kritischen“ und „wichtigen“ Branchen: Post- und Kurierdienste, Abfallwirtschaft, Chemie, Lebensmittel, Verarbeitendes Gewerbe, Anbieter digitaler Dienste, Forschung).

Ein redaktioneller Hinweis: Zum Zeitpunkt der Befragung lag der im Mai 2024 veröffentlichte Referentenentwurf des NIS2-Umsetzungsgesetzes für Deutschland noch nicht vor. Die oben genannte Definition, die den Befragten im Rahmen der Befragung als ergänzende Wissensgrundlage für ihr Antwortverhalten mitgeteilt wurde, entstammt der zugrunde liegenden EU-Richtlinie.

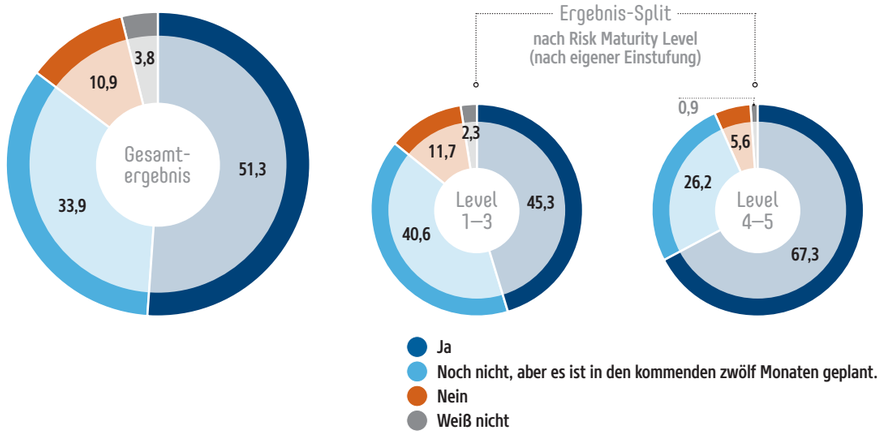
NIS2 intern umgesetzt haben, und 49 Prozent, die noch an der Umsetzung bis Jahresende 2024 arbeiten.

Ein paar wenige negative Einzelmeinungen – vor allem im (IT-)C-Level – bezüglich der Machbarkeit der NIS2-Umsetzung bis Jahresende fallen derweil kaum ins Gewicht. Insgesamt stellt sich dennoch die Frage, ob in den Unternehmen intern der Umsetzungsstand und -bedarf für NIS2 umfassend bekannt ist und richtig kommuniziert wird, zumal zum Zeitpunkt der Umfrage das für Deutschland geltende NIS2-Umsetzungsgesetz noch nicht abschließend vorlag.

3

Setzt Ihr Unternehmen Security Automation ein?

Angaben in Prozent. Basis: n = 339



Das Potenzial von Security Automation bleibt teils noch ungenutzt

Erst etwas mehr als die Hälfte der befragten Unternehmen (51 Prozent) nutzt die Möglichkeit, Security-Funktionen zu automatisieren, weitere 34 Prozent befinden sich dazu in der Planungsphase. Der Fokus der (geplanten) Automatisierung liegt auf der Angriffserkennung.

Elf Prozent der befragten Unternehmen setzen noch keine Security Automation ein und planen dies auch nicht. Bei kleineren Unternehmen mit weniger als 500 Beschäftigten sind es hier mit zwölf Prozent nur wenig mehr. Diese Unternehmen setzen Security Automation derzeit aber auch noch deutlich seltener ein (30 Prozent) als der genannte Durchschnitt über alle Unternehmensgrößen hinweg und befinden sich dementsprechend wesentlich häufiger noch in der Planungsphase (52 Prozent).

Ob Automatisierung in der Security bereits genutzt wird oder nicht, hängt auch mit dem Risikomanagement-Reifegrad des jeweiligen Unternehmens nach dem „Risk Maturity Model“ *(vgl. Weiteres Ergebnis 7, Seite 28 f.)* zusammen: Von den Unternehmen, die auf Level 1, 2 oder 3 stehen, nutzen 45 Prozent Security Automation, von den Unternehmen auf Level 4 oder 5 indes 67 Prozent.

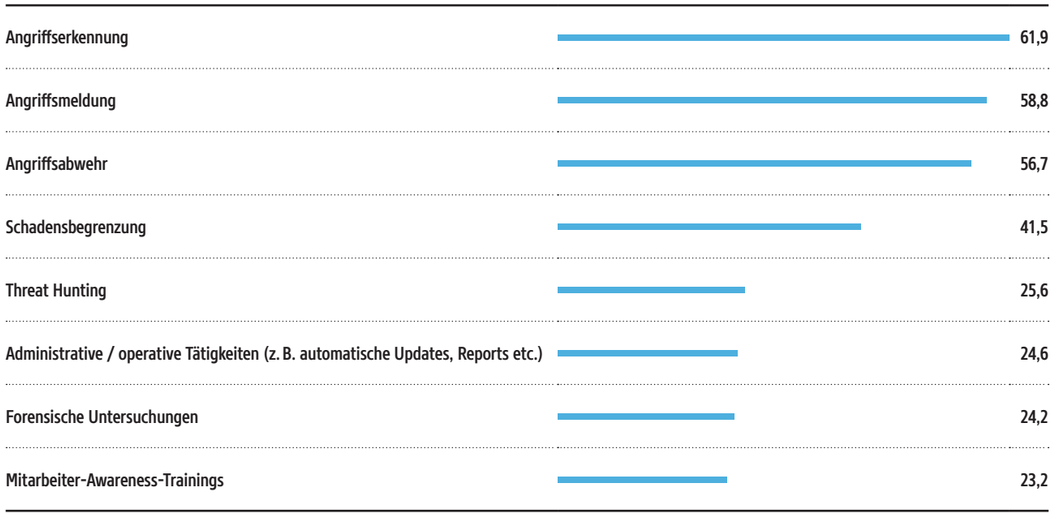
Die meisten Unternehmen, die Security Automation bereits einsetzen oder deren Einsatz planen, haben die Angriffserkennung automatisiert (62 Prozent). Es folgen die Angriffsmeldungen (59 Prozent) und die Angriffsabwehr (57 Prozent), in welcher die Unternehmen auch den größten Nutzen der Security-Automatisierung allgemein sehen. Zur Reduktion von administrativen Aufgaben in der Security greift nur noch jedes vierte Unternehmen zur Automatisierung (25 Prozent), den Bereich Security Awareness haben 23 Prozent der Befragten automatisiert.

Dass Security Automation helfen kann, die meist knappen personellen Security-Ressourcen zu entlasten, sehen nur 17 Prozent als ihren größten Nutzen.

Insgesamt scheinen die befragten Unternehmen die Potenziale einer Automatisierung noch nicht auszuschöpfen, denn Security Automation kann dann am meisten leisten, wenn möglichst viele Security-Funktionen eingebunden sind, die zusammenwirken – andernfalls beschränkt man sich auf Insellösungen.

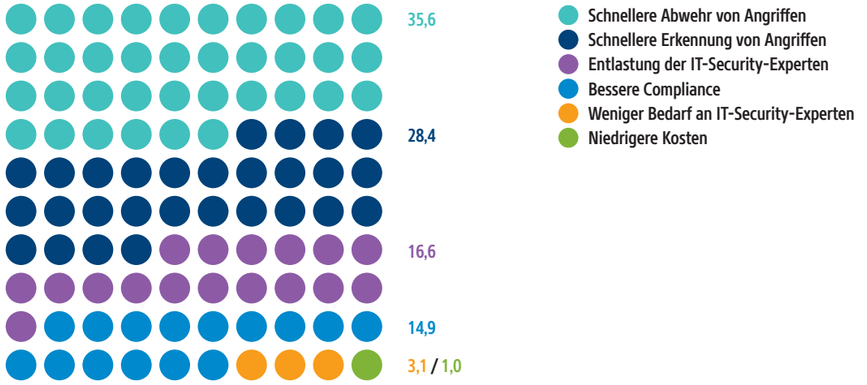
Welcher Teil Ihrer IT-Security ist automatisiert oder soll automatisiert werden?

Angaben in Prozent. Mehrfachnennungen möglich. Filter: Unternehmen, die Security Automation bereits einsetzen oder dies in den kommenden zwölf Monaten planen.
Basis: n = 289



Was ist in Ihren Augen der größte Nutzen von Security Automation?

Angaben in Prozent. Filter: Unternehmen, die Security Automation bereits einsetzen oder dies in den kommenden zwölf Monaten planen.
Basis: n = 289 (zu 100 fehlende Prozent: „Weiß nicht“)



4

Unternehmen investieren besonders in IAM und in Zero Trust

Nur drei Prozent der befragten Unternehmen investieren gegenwärtig nicht in technische Systeme für die Cybersicherheit. Am häufigsten fließt das Geld in das Identity and Access Management (44 Prozent) und in IT-Sicherheitsarchitekturen wie Zero Trust (40 Prozent). Nur halb so häufig wird in Ransomware-Schutz investiert (22 Prozent).

Besonders häufig investieren kleinere Unternehmen mit weniger als 500 Beschäftigten in **→ IAM *** (49 Prozent in dieser Befragtengruppe), Unternehmen mit 500 bis 999 Beschäftigten präferieren indes Investitionen in Lösungen für **→ Penetrationstests** (41 Prozent in dieser Befragtengruppe). Große Firmen mit mindestens 1.000 Beschäftigen kümmern sich zuerst um das Thema IT-Sicherheitsarchitektur wie beispielsweise **→ Zero Trust** (47 Prozent in dieser Befragtengruppe).

Die Höhe der jährlichen IT-Aufwendungen spielt im Investitionsverhalten ebenfalls eine Rolle. Unternehmen, die weniger als zehn Millionen Euro IT-Budget im Jahr zur Verfügung haben, investieren gegenwärtig häufiger in IT-Sicherheitsarchitekturen als die Unternehmen mit höheren Budgets (45 zu 37 Prozent). Beim Thema IAM ist es genau umgekehrt: Hier investieren Unternehmen mit mindestens zehn Millionen Euro jährlichem IT-Budget häufiger als diejenigen mit geringeren finanziellen IT-Mitteln (47 zu 44 Prozent).

Interessant ist auch, dass der Risk Maturity Level, den sich die Unternehmen selbst vergeben (vgl. Weiteres Ergebnis 7, Seite 28 f.), ebenfalls eine Rolle bezüglich der Frage spielt, in welchen Bereichen investiert wird. 52 Prozent der Unternehmen im Level 1 bis 3 investieren in IAM, aber nur 45 Prozent derer im Level 4 und 5. Letztere stecken das Geld noch lieber in die Security-Automatisierung (49 Prozent).

***Mit → markierte Begriffe werden im Glossar auf Seite 45 erläutert.**

In welche der folgenden technischen Systeme / Prozesse investiert Ihr Unternehmen?
Angaben in Prozent. Mehrfachnennungen möglich. Basis: n = 339

	Gesamtergebnis	Ergebnis-Split nach IT-Budget (jährliche Aufwendungen in IT-Systeme sowie Anwendungen/Applikationen) in Euro: < 10 Millionen	≥ 10 Millionen
Identitäts- und Berechtigungsmanagement (IAM)	44,0	44,0	47,0
Sicherheitsarchitektur (z.B. Zero-Trust-Ansatz)	39,8	44,7	37,2
Security Automation	37,8	44,0	32,3
Penetration-Testing / externe Security-Überprüfung	32,7	27,7	41,5
Firewall / SD-WAN	30,1	36,2	24,4
Ransomware-Schutz	22,4	28,4	18,3
Patchmanagement	22,1	17,0	28,7
Backup & Restore	22,1	27,0	17,7
API Security	21,8	20,6	23,2
Data Leakage Prevention	17,1	17,7	16,5
Vulnerability Management	15,0	16,3	15,2
XDR-Plattformen	10,3	7,1	13,4
Wir investieren in keine der genannten technischen Systeme / Prozesse.	2,9	0,7	3,0
Weiß nicht	3,8	1,4	1,2

5

Konsolidierung von Tools und Herstellern ist ein besonders wichtiges Ziel

Nicht nur die Zahl der genutzten Security-Tools, sondern auch die der in Anspruch genommenen Security-Anbieter ist vielen Unternehmen zu hoch – 96 beziehungsweise 93 Prozent der Befragten wollen für eine entsprechende Konsolidierung sorgen. Die Security-Fachkräfte sind im Bereich der Tool-Konsolidierung besonders deutlich: Hier gibt es niemanden, der oder die sich nicht dafür ausspricht.

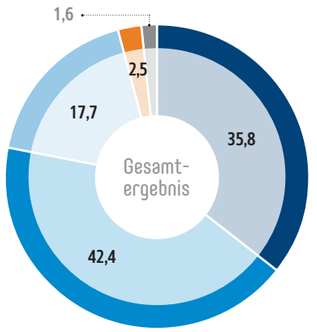
Mit steigender Beschäftigtenzahl erhöht sich auch der Wunsch nach Verringerung der eingesetzten Tools für Security. Während 93 Prozent der Unternehmen mit weniger als 500 Beschäftigten ihre Security-Tools bereits aktiv konsolidieren oder dies zumindest planen, sind es 98 Prozent der Unternehmen ab 1.000 Beschäftigten.

Auch die Höhe der jährlichen IT-Aufwendungen wirkt sich auf den Wunsch nach Konsolidierung aus: 95 Prozent der Befragten mit einem IT-Budget von unter zehn Millionen Euro pro Jahr achten im Zuge technischer Security-Investitionen auf eine Konsolidierung der eingesetzten Tools oder planen dies zumindest in Zukunft zu tun. Bei den Unternehmen mit einem höheren IT-Budget sind es sogar 98 Prozent.

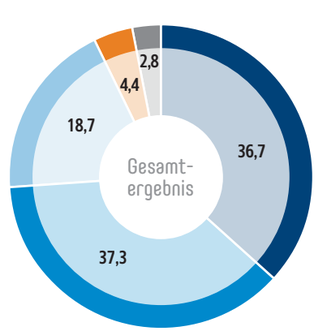
Eine Reduktion ist auch bei der Zahl der genutzten Security-Hersteller erwünscht. 37 Prozent der befragten Unternehmen haben diese bereits konsolidiert, weitere 37 Prozent planen dies konkret, und 19 Prozent haben dies zumindest angedacht.

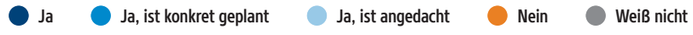
Offensichtlich besteht der deutliche Wunsch, die Komplexität in der Administration der Security-Tools und in der Zusammenarbeit mit den Security-Herstellern zu verringern.

Achten Sie im Zuge technischer IT-Security-Investitionen auch auf eine Konsolidierung bei den Tools, die im Unternehmen zur Anwendung kommen?
Angaben in Prozent. Filter: Unternehmen, die in zuvor abgefragte technische Systeme / Prozesse investieren – *vgl. Weiteres Key Finding 4.*
Basis: n = 316



Achten Sie im Zuge technischer IT-Security-Investitionen auch auf eine Konsolidierung bei den Herstellern, mit denen Ihr Unternehmen zusammenarbeitet?
Angaben in Prozent. Filter: Unternehmen, die in zuvor abgefragte technische Systeme / Prozesse investieren – *vgl. Weiteres Key Finding 4.*
Basis: n = 316





Der IT-Security-Bereich braucht mehr Personal und Know-how

Gefragt nach den Hindernissen, auf die sie im IT-Sicherheitsbereich stoßen, nennen 41 Prozent der Unternehmen das fehlende Personal, 28 Prozent den Know-how-Mangel und 25 Prozent die zu knappen Budgets. Steigende Compliance-Anforderungen sind nur für 18 Prozent der Befragten ein Problem, und immerhin acht Prozent haben keinerlei Hürden zu überwinden.

Personal, Know-how und Budget sind die Eckpfeiler eines jeden Projekts. Trotzdem krankt die Security weiterhin vor allem an diesen drei Bereichen. Gerade die kleineren Unternehmen mit weniger als 500 Beschäftigten leiden unter dem Personalmangel – 46 Prozent der Unternehmen dieser Größe bezeichnen das fehlende Personal als Security-Hemmnis.

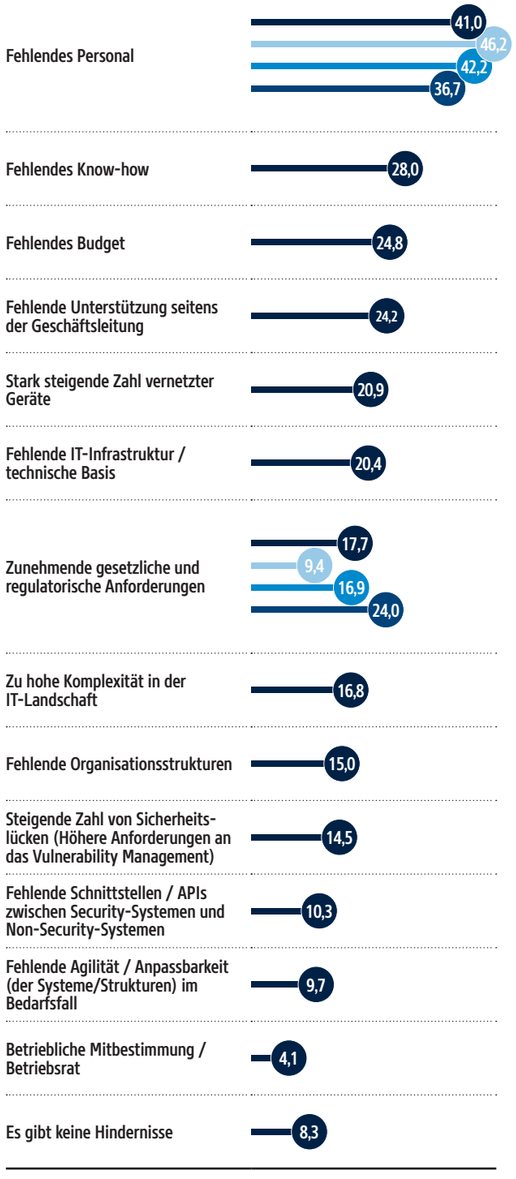
Über alle Unternehmensgrößen hinweg sind es vor allem die Befragten aus den Fachbereichen und dem IT-C-Level, die das Problem des fehlenden Security-Personals als größtes Hindernis des IT-Security-Bereichs nennen (47 beziehungsweise 43 Prozent).

Interessant ist auch, dass viele der Themen, die in der Security gegenwärtig stark diskutiert werden, nicht so häufig zu den Hindernissen gerechnet werden, wie man glauben könnte. So nennen nur 17 Prozent der Unternehmen die IT-Komplexität, 15 Prozent die vielen Schwachstellen der IT und sogar nur vier Prozent die betriebliche Mitbestimmung.

Die regulatorischen Anforderungen werden je nach Unternehmensgröße unterschiedlich häufig als Hindernis für die Security genannt. Während kleinere Unternehmen mit weniger als 500 Beschäftigten nur zu neun Prozent die Regulierung als Hemmnis werten, sind es bei den großen Unternehmen mit mindestens 1.000 Beschäftigten 24 Prozent.

Auf welche Hindernisse / Widerstände stößt Ihr Unternehmen im IT-Security-Bereich?

Angaben in Prozent. Mehrfachnennungen möglich. Basis: n = 339



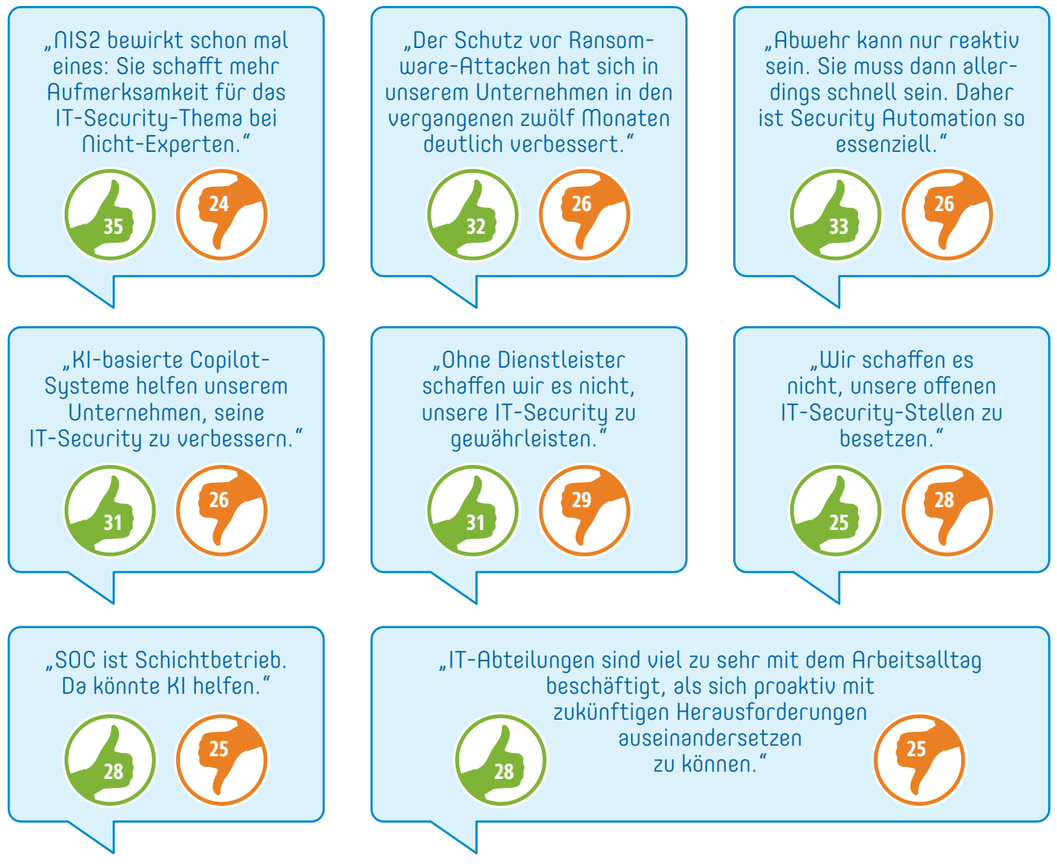
Die Security steht bei vielen Fragen zwischen den Stühlen

Im Rahmen der Befragung für diese Studie wurden die Unternehmen mit einigen Thesen konfrontiert, zu denen sie die Frage gestellt bekamen, inwieweit sie ihnen zustimmen können.

Was die Haltung zu bestimmten Aussagen aus dem IT-Security-Bereich angeht, bewegen sich die befragten Unternehmen meist ziemlich ausgeglichen zwischen Zustimmung und Ablehnung. Wenn es aber etwa gleich viele Befürworter wie Gegner für bestimmte Security-Themen gibt, kann es der Security-Community schwerfallen, einen festen Kurs zu finden und zu verfolgen. Offensichtlich muss in vielen Fragen noch mehr Aufklärungsarbeit geleistet werden – intern wie extern.

Nachfolgend sind nun einige Statements aufgeführt. Sagen Sie uns bitte jeweils, inwieweit Sie diesen Aussagen zustimmen können.

Angaben in Prozent. Abgefragt wurde auf einer Skala von 1 („Stimme voll und ganz zu“) bis 6 („Stimme ganz und gar nicht zu“). Dargestellt sind jeweils die kumulierten, kaufmännisch gerundeten Werte 1 und 2 (grüne Daumen) sowie 5 und 6 (orange Daumen). Basis: n = 334–338



Weitere Studienergebnisse

Zahlen und Analysen, die aus Sicht des Marktforschungsteams ebenfalls wichtig sind

IT-Security-Trends 2024

Vier von zehn Unternehmen haben noch keine KI-Strategie

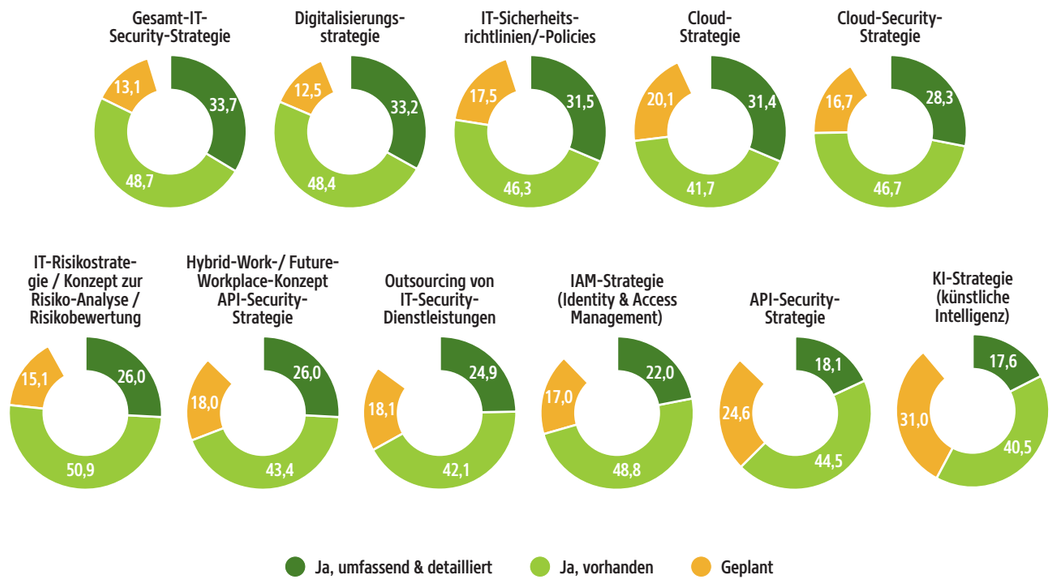
Obwohl die meisten Unternehmen einen hohen Schutzbedarf für ihre KI-Systeme sehen *(vgl. Weiteres Key Finding 1, Seite 11)*, haben erst 58 Prozent von ihnen bereits eine KI-Strategie, während 31 Prozent diese noch planen. Eine IAM-Strategie ist hingegen in 71 Prozent der Unternehmen vorhanden.

Ohne die richtigen Strategien kann eine gezielte und fundierte Absicherung nicht gelingen. So ist es entscheidend, dass 82 Prozent der befragten Unternehmen bereits eine Digitalisierungsstrategie haben. Aber auch für spezielle Security-Bereiche sollte eine zugehörige Strategie nicht fehlen.

Im Bereich der Cloud-Sicherheit können 75 Prozent der Befragten auf eine Cloud-Security-Strategie verweisen, wohingegen nur 73 Prozent auch eine Cloud-Strategie haben. Der ebenfalls zunehmend wichtige Bereich Hybrid Work wird von 69 Prozent der Befragten mit einer eigenen Strategie bedacht.

Bezieht man weitere Ergebnisse dieser Studie mit ein, ist es aber besonders kritisch, dass es im Bereich KI nur in rund sechs von zehn Unternehmen eine passende Strategie gibt. Dabei soll KI in der Cybersicherheit nicht nur unterstützen, sondern wird gleichzeitig selbst als schutzbedürftiger Bereich angesehen. Entsprechend sollten Unternehmen eine KI-Strategie nicht vernachlässigen und hier alsbald nachziehen.

Welche der folgenden Strategien und Konzepte gibt es in Ihrem Unternehmen?
Angaben in Prozent. Basis: n = 335–339 (zu 100 fehlende Prozent: „Nicht vorhanden“ und „Weiß nicht“)

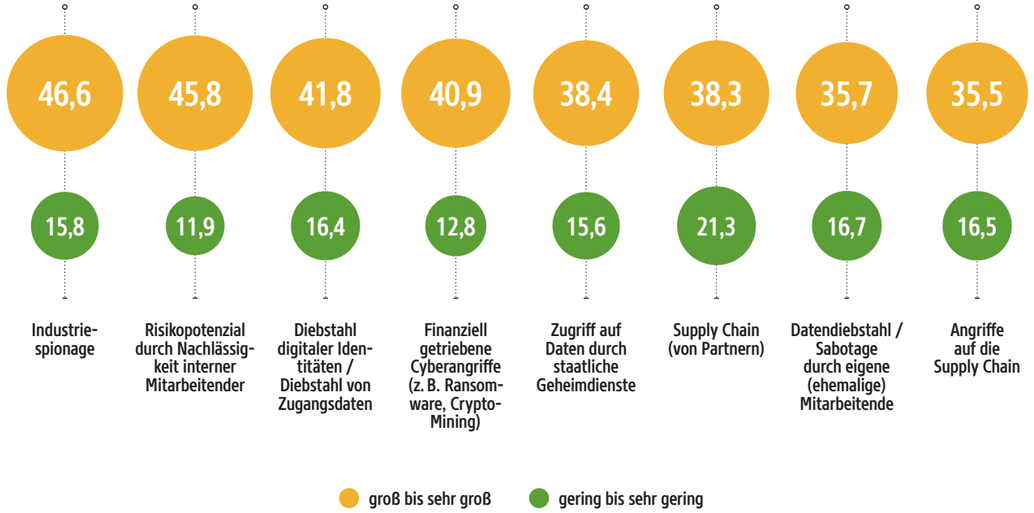


2

Industriespione mehr gefürchtet als Ransomware-Gruppen

Die Gefahr, Opfer einer finanziell getriebenen Cyberattacke wie beispielsweise Ransomware zu werden, schätzen 41 Prozente der Befragten für sich als (sehr) groß ein. Opfer von Industriespionage zu werden ist sogar für 47 Prozent eine große Gefahr. Bedrohungen rund um die eigene Supply Chain sind indes nicht ganz so stark gefürchtet.

Wie groß schätzen Sie die Gefahr für Ihr Unternehmen ein, Opfer der aufgeführten Cybervorfälle zu werden?
Angaben in Prozent. Dargestellt sind jeweils die kumulierten Werte für „sehr groß" / „groß" sowie „gering" /„sehr gering". Basis: n = 327–336



Am häufigsten nennen die kleineren Unternehmen mit weniger als 500 Beschäftigten die Industriespionage als „große" oder „sehr große" Gefahr (52 Prozent in dieser Befragtengruppe). Betrachtet man die Unternehmensrollen, dann sind es vor allem die Befragten aus dem C-Level, die die Industriespionage stark fürchten (56 Prozent in dieser Befragtengruppe).

Trotz der genannten und als groß empfundenen Cyberbedrohungen fühlen sich 35 Prozent der Befragten als „sehr gut" bis „erstklassig" vor den Gefahren der Cyberkriminalität geschützt. Besonders die Unternehmen, die ihren Risk Maturity Level mit 4 oder 5 als besonders hoch einstufen *(vgl. Weiteres Ergebnis 7, Seite 28 f.)*, sind von ihrem Schutz entsprechend überzeugt (50 Prozent in dieser Befragtengruppe). Ein weniger gutes Gefühl haben indes die Befragten aus den Fachbereichen – nur 14 Prozent von ihnen fühlen sich „sehr gut" oder gar „erstklassig" geschützt.

Auch wenn die finanziell getriebenen Attacken wie die Ransomware-Angriffe aktuell nicht die am häufigsten genannte große IT-Sicherheitsgefahr sind, gehen doch 54 Prozent der Unternehmen davon aus, dass diese Angriffe in den nächsten ein bis zwei Jahren deutlich an Relevanz gewinnen werden.

Und wie gut fühlen Sie sich als Unternehmen insgesamt vor den Gefahren der Cyberkriminalität geschützt?
Angaben in Prozent. Abgefragt wurde auf einer Skala von 0 (völlig unzureichend geschützt) bis 10 (erstklassig geschützt).
Basis: n = 330

Welche dieser Gefahren werden für Ihr Unternehmen in den kommenden ein bis zwei Jahren an Relevanz deutlich zunehmen?
Angaben in Prozent. Mehrfachnennungen möglich. Basis: n = 339

Finanziell getriebene Cyberangriffe (z.B. Ransomware, Crypto-Mining)	54,3
Risikopotenzial durch Nachlässigkeit interner Mitarbeitender	43,1
Diebstahl digitaler Identitäten / Diebstahl von Zugangsdaten	41,3
Zugriff auf Daten durch staatliche Geheimdienste	37,5
Industriespionage	36,9
Datendiebstahl / Sabotage durch eigene (ehemalige) Mitarbeitende	34,5
Angriffe auf die Supply Chain	23,0
Angriffe aus der Supply Chain (von Partnern)	15,9

3

Unternehmen sorgen sich wegen staatlich organisierter Cyberkriminalität

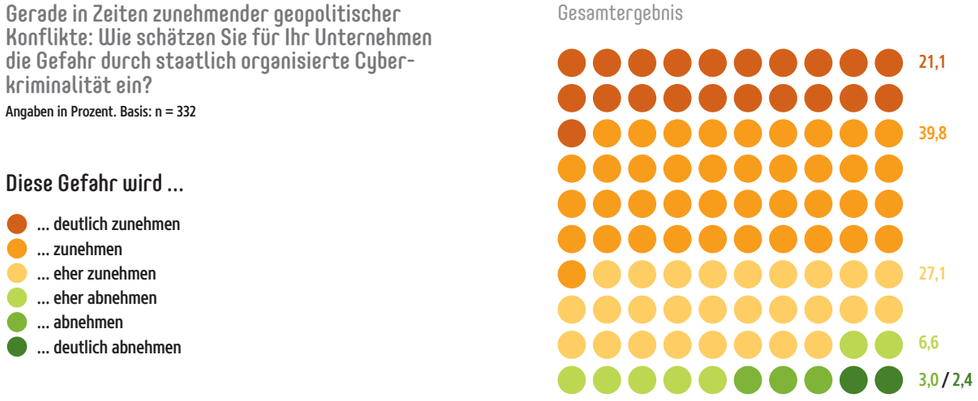
Neben finanziell motivierten Cyberangriffen sind es die staatlich organisierten Cyberattacken, die Unternehmen als steigende Bedrohung sehen. So geben insgesamt 61 Prozent der Befragten an, dass die Gefahr durch diese Art von Angriffen (deutlich) zunehmen wird. Nur fünf Prozent der Unternehmen gehen von einer abnehmenden Gefahr aus.

Etwas weniger besorgt scheinen die größeren Unternehmen mit mehr als 1.000 Beschäftigten zu sein – hier sagen nur 56 Prozent der Befragten, dass sie von einer (deutlich) zunehmenden Gefahr durch staatlich organisiertes Cybercrime ausgehen.

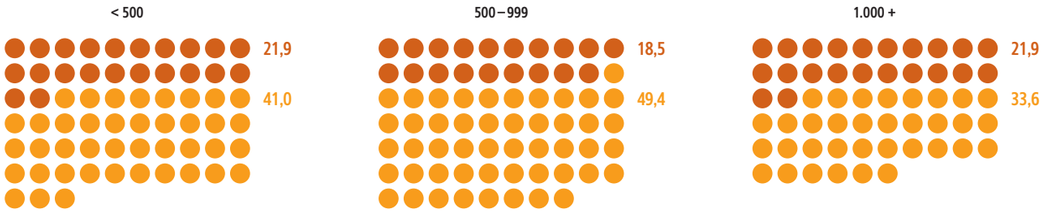
Im C-Level ist die Sorge vor staatlich organisierter Internetkriminalität besonders hoch – 68 Prozent aus dieser Befragtengruppe erwarten eine (deutlich) zunehmende Bedrohung. In den Fachbereichen denken nur 52 Prozent so, unter den CISOs sind es 61 Prozent der Befragten.

Der Risk Maturity Level der Unternehmen *(vgl. Weiteres Ergebnis 7, Seite 28 f.)* hat indes keinen Einfluss auf die Umfrageergebnisse an dieser Stelle: Unternehmen der Level 1 bis 3 sowie der Level 4 bis 5 erwarten gleichermaßen stark eine Zunahme der Gefahr durch staatlich organisierte Cyberkriminalität (64 beziehungsweise 65 Prozent).

Gerade in Zeiten zunehmender geopolitischer Konflikte: Wie schätzen Sie für Ihr Unternehmen die Gefahr durch staatlich organisierte Cyberkriminalität ein?
Angaben in Prozent. Basis: n = 332



Teil-Ergebnis-Split
nach Unternehmensgröße (Anzahl Beschäftigte)



4

CISOs sind oft nicht die Verantwortlichen

Die federführende Verantwortung für Security liegt nur in elf Prozent der Unternehmen in den Händen der CISOs / CSOs und (IT-)Security-Vorstände. Bei den großen Unternehmen mit mindestens 1.000 Beschäftigten steigt der Anteil der CISOs unter den Security-Verantwortlichen auf zumindest 15 Prozent.

Selbst die Unternehmen, die ihren Risk Maturity Level auf hohe 4 oder 5 schätzen *(vgl. Weiteres Ergebnis 7, Seite 28 f.)*, geben nur zu 15 Prozent an, dass die CISOs für „ihr" Thema IT-Security auch hauptverantwortlich zeichnen.

In deutlich mehr Fällen sind es die CIOs, CDOs und IT-Vorstände, die die Security federführend verantworten (23 Prozent) – selbst die IT-Leitungen sind deutlich häufiger verantwortlich (21 Prozent) als die CISOs. In drei Prozent der Unternehmen wird gar der oder die betriebliche Datenschutzbeauftragte mit der Security-Verantwortung betraut, obwohl dies rechtlich gesehen einen Interessenskonflikt (nach Datenschutz-Grundverordnung) darstellt.

Selbst unter den Stellen, die im Unternehmen zumindest beratend bei Security-Entscheidungen einbezogen werden, liegen die CISOs nicht vorn. Vielmehr haben in 35 Prozent der Unternehmen die IT-Leitungsebenen eine beratende Rolle in der Security, die CISOs hingegen werden nur in 22 Prozent der Unternehmen beratend miteinbezogen.

Einen etwas höheren Anteil an der Security-Beratung im Unternehmen haben die CISOs dort, wo die Beschäftigtenzahl mindestens 1.000 beträgt. Das mag auch damit zusammenhängen, dass das Jobprofil und der CISO-Titel meist überhaupt erst in Unternehmen dieser Größenordnung existieren.

Es bleibt dennoch festzuhalten, dass die deutliche Mehrheit der Unternehmen trotz der Komplexität von Security und trotz des Wunsches, die Security durch Konsolidierung zu vereinfachen, die interne Expertise für Security nicht ausreichend nutzen.

Wer ist in Ihrem Unternehmen federführend verantwortlich für das Thema IT-Security?
Angaben in Prozent. Basis: n = 339

CIO / CDO / IT-Vorstand	22,7
IT-Leitung / EDV-Leitung / Leitung Rechenzentrum	20,9
CEO / Geschäftsführung / Vorstand	16,2
CISO / CSO / (IT-)Security-Vorstand	10,9
CTO / Chief Technology Officer / Technik-Vorstand	8,8
Security (Operations) Manager(in)	6,8
COO / CFO / Kaufmännische Leitung	4,4
Betriebliche(r) Datenschutzbeauftragte(r)	3,2
Risk Manager(in)	2,1
Administrator(in)	1,2
Compliance Officer	0,6

Und wer ist außerdem noch an den Entscheidungsprozessen zu IT-Security beteiligt, zumindest in beratender Weise?
Angaben in Prozent. Mehrfachnennungen möglich. Basis: n = 339

IT-Leitung / EDV-Leitung / Leitung Rechenzentrum	35,1
CEO / Geschäftsführung / Vorstand	32,2
CIO / CDO / IT-Vorstand	31,9
CTO / Chief Technology Officer / Technik-Vorstand	28,9
CISO / CSO / (IT-)Security-Vorstand	22,4
Security (Operations) Manager(in)	14,5
COO / CFO / Kaufmännische Leitung	11,2
Betriebliche(r) Datenschutzbeauftragte(r)	10,3
Risk Manager(in)	9,1
Administrator(in)	8,0
Compliance Officer	4,7

5

Jedes zweite Unternehmen mit verpflichtenden Security-Zertifizierungskursen

Obwohl der Mangel an Personal und Know-how als größtes Hindernis in der Security gilt *(vgl. Weiteres Key Finding 6, Seite 18)*, sehen nur 50 Prozent der Unternehmen eine interne Zertifizierung für die Verantwortlichen in der IT-Sicherheit als verpflichtende Maßnahme vor.

Verpflichtende Schulungen zu aktuellen Bedrohungen gibt es in 56 Prozent der Unternehmen, zu Themen aus dem Bereich Datenschutz und Compliance bei 51 Prozent. Noch geringer ist der Anteil der Pflichtschulungen im Bereich Cloud-Sicherheit (48 Prozent) – und das trotz der allgemein hohen Cloud-Nutzungsraten.

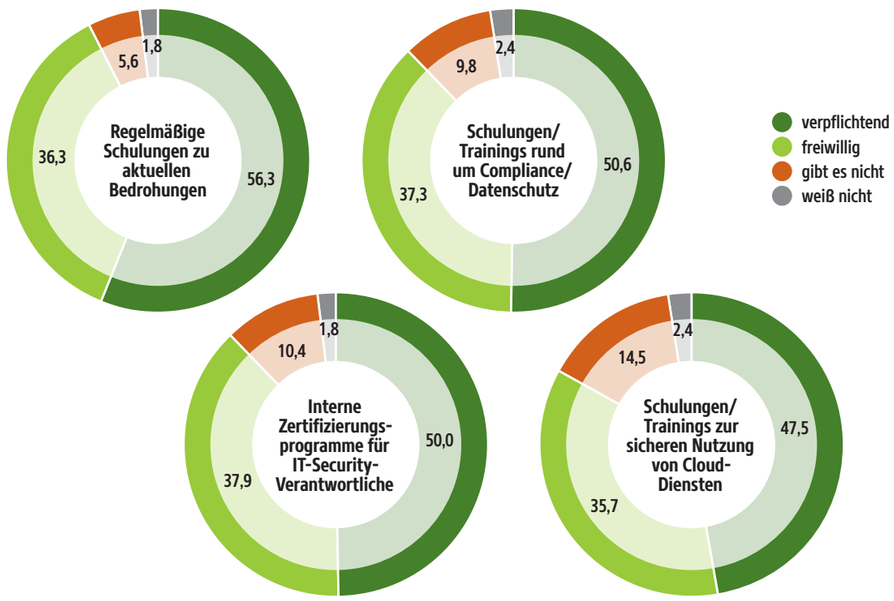
Selbst die Unternehmen, die ihren Risk Maturity Level mit 4 oder 5 als hoch einstufen *(vgl. Weiteres Ergebnis 7, Seite 28 f.)*, haben nicht deutlich mehr Schulungsangebote im Pflichtprogramm: Zertifizierungen für Security-Verantwortliche findet man nur bei 52 Prozent der entsprechenden Unternehmen.

Bei großen Unternehmen mit mehr als 1.000 Beschäftigten ist der Anteil der Pflichtzertifizierungen für Verantwortliche der Security mit 54 Prozent auch nicht spürbar höher.

Mit Blick auf die NIS2-Richtlinie und die dort vorhandenen Schulungspflichten *(vgl. Weiteres Key Finding 2, Seite 12 f.)* besteht damit generell ein hoher Nachholbedarf für Schulungen, gerade im Bereich der Führungskräfte und (Security-)Verantwortlichen.

Welche Schulungen, Weiterbildungen oder Trainings bietet Ihr Unternehmen seinen Beschäftigten im Bereich IT-Security an?

Angaben in Prozent. Basis: n = 338–339



6

Cyberversicherung wird zum betrieblichen Standard

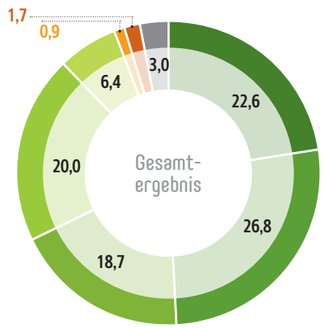
Nur zwei Prozent der befragten Unternehmen haben sich noch nicht mit dem Thema Cyberversicherung auseinandergesetzt. 68 Prozent haben eine solche Versicherung bereits abgeschlossen, 23 Prozent davon sogar bereits seit vielen Jahren.

Jedes zweite Unternehmen (51 Prozent) mit mehr als 500 Beschäftigten hat bereits seit vielen Jahren eine Cyberversicherung, kleinere Unternehmen mit weniger Mitarbeitenden immer noch zu 15 Prozent. Was die konkret geplanten Neuabschlüsse angeht, lässt sich Folgendes feststellen: Die Unternehmen, die ein jährliches IT-Budget von über zehn Millionen Euro zur Verfügung, aber bislang noch keine solche Versicherung abgeschlossen haben, planen den Neuabschluss etwas häufiger als diejenigen mit einem niedrigeren Budget (22 zu 19 Prozent).

Doch Cyberversicherung ist nicht gleich Cyberversicherung, es kommt auf den genauen Versicherungsgegenstand und den gewünschten Umfang an. Unternehmen, die bereits eine Cyberversicherung ihr Eigen nennen, haben zu zwei Dritteln (67 Prozent) eine Cyberhaftpflicht gewählt. Eine Cybererpressungs-Versicherung beziehungsweise Ransomware-Versicherung wurde von 58 Prozent abgeschlossen, eine Cyberdiebstahlversicherung von 55 Prozent. Nur 23 Prozent der Befragten wählten andere Formen der Cyberversicherung oder haben sich individuell gegen Cyberrisiken versichern lassen. Es ist damit ersichtlich, dass in vielen Unternehmen mehrere verschiedene Cyberversicherungspolicen gleichzeitig aktiv sind.

Hat Ihr Unternehmen eine Cyberversicherung abgeschlossen?

Angaben in Prozent. Filter: Nur C-Level, IT-Leitung, IT-Security- und Risk-Management-Verantwortliche in Unternehmen, in denen nach eigener Einschätzung ein (initialer) Reifegrad nach dem Risk Maturity Model vorhanden ist. Basis: n = 235



- Seit vielen Jahren
- Seit zwei oder drei Jahren
- Seit Kurzem
- Der Abschluss einer Cyberversicherung ist (konkret) geplant.
- Der Abschluss einer Cyberversicherung ist angedacht.
- Der Abschluss einer Cyberversicherung ist nicht zustande gekommen.
- Wir haben uns mit dem Thema einer Cyberversicherung noch gar nicht auseinandergesetzt.
- Weiß nicht

Welche Cyberversicherung hat ihr Unternehmen abgeschlossen oder plant es (möglicherweise) abzuschließen?

Angaben in Prozent. Mehrfachnennungen möglich. Filter: Nur C-Level, IT-Leitung, IT-Security- und Risk-Management-Verantwortliche in Unternehmen, in denen ihrer eigenen Einschätzung nach ein (initialer) Reifegrad nach dem Risk Maturity Model vorhanden ist und die bereits eine Cyberversicherung abgeschlossen haben, es konkret planen oder zumindest angedacht haben. Basis: n = 222

Cyberhaftpflichtversicherung	66,7
Cybererpressungsversicherung (Ransomware-Versicherung)	58,1
Cyberdiebstahlversicherung	55,0
Andere bzw. individuell auf uns zugeschnittene Cyberversicherung	23,4
Das ist noch nicht entschieden	4,5
Weiß nicht	0,5

CISOs sind vom betrieblichen Risikomanagement besonders überzeugt

45 Prozent der befragten Unternehmen stufen ihr Risikomanagement im „Risk Maturity Model" in die höchsten Level 4 und 5 ein. Auf der anderen Seite finden 14 Prozent der Befragten bei sich nur ein initiales Risikomanagement im Sinne einer einfachen Risikobuchhaltung vor. Aus Sicht der CISOs erscheint das betriebliche Management der Risiken indes deutlich besser.

Fragt man die CISOs und Verantwortlichen für Risk Management nach der Reife des internen Risikomanagements, geben 64 Prozent von ihnen an, dass die Risiken nach Level 4 (controlled) oder Level 5 (optimizing) gemanagt würden. Das Level 5 sehen ganze 36 Prozent der befragten CISOs / Risk Manager und -Managerinnen bei ihren Unternehmen. Offensichtlich sind diese CISOs und Risk-Verantwortlichen nicht wirklich selbstkritisch – zumindest dann nicht, wenn sie selbst für das Risikomanagement (mit)verantwortlich sind (was überwiegend der Fall sein dürfte). Schließlich geben von den Befragten aus dem C-Level im Gegensatz dazu nur elf Prozent zu Protokoll, dass ihr Unternehmen eine Level-5-Bewertung verdiene.

Interessant ist auch, dass die beste Bewertung für das eigene Risikomanagement gerade bei großen Unternehmen mit mindestens 1.000 Beschäftigten zu finden ist (27 Prozent dieser Befragtengruppe). Ein weiterer Einflussfaktor für eine positive Selbsteinschätzung scheint das jährliche IT-Budget zu sein: Unternehmen mit mehr als zehn Millionen Euro sehen sich ebenfalls entsprechend oft auf Level 5 im „Risk Maturity Model" (27 Prozent in dieser Befragtengruppe).

Wie schätzen Sie den Reifegrad des Risikomanagements in Ihrem Unternehmen ein (nach dem „Risk Maturity Model")?

Angaben in Prozent. Filter: Nur C-Level, IT-Leitung, IT-Security- und Risk-Management-Verantwortliche. Basis: n = 238 (zu 100 fehlende Prozent: „Weiß nicht")

Das Risk Maturity Model

Level 1 „initial":
Lediglich Großrisiken werden erfasst (zumindest qualifiziert) und einzeln dargestellt („Risikobuchhaltung").

Level 2 „defined":
Risiken und Chancen werden vollständig erfasst (zumindest qualifiziert) und in zyklischen Intervallen an das Management reportet.

Level 3 „managed":
Der Risikomanagement-Prozess folgt einer nachvollziehbar dokumentierten Methode. Die Risiken werden qualifiziert und aggregiert, die Maßnahmen in ihrer Gesamtheit bewertet.

Level 4 „controlled":
Chancen und Risiken werden als Korridor der Unternehmensplanung bewertet und aggregiert. Abhängigkeiten zwischen Risiken werden berücksichtigt. Maßnahmen werden sowohl mit ihrem Nutzen als auch ihren Kosten miteinbezogen.

Level 5 „optimizing":
Der risikoorientierte Planungsprozess ist integraler Bestandteil der strategischen Unternehmensführung. Das RM-System ist direkt an die Steuerungssysteme des Unternehmens angebunden. Eine Risikokultur ist verankert.

8

Knapp die Hälfte der Unternehmen bewertet die IT-Risiken nicht explizit

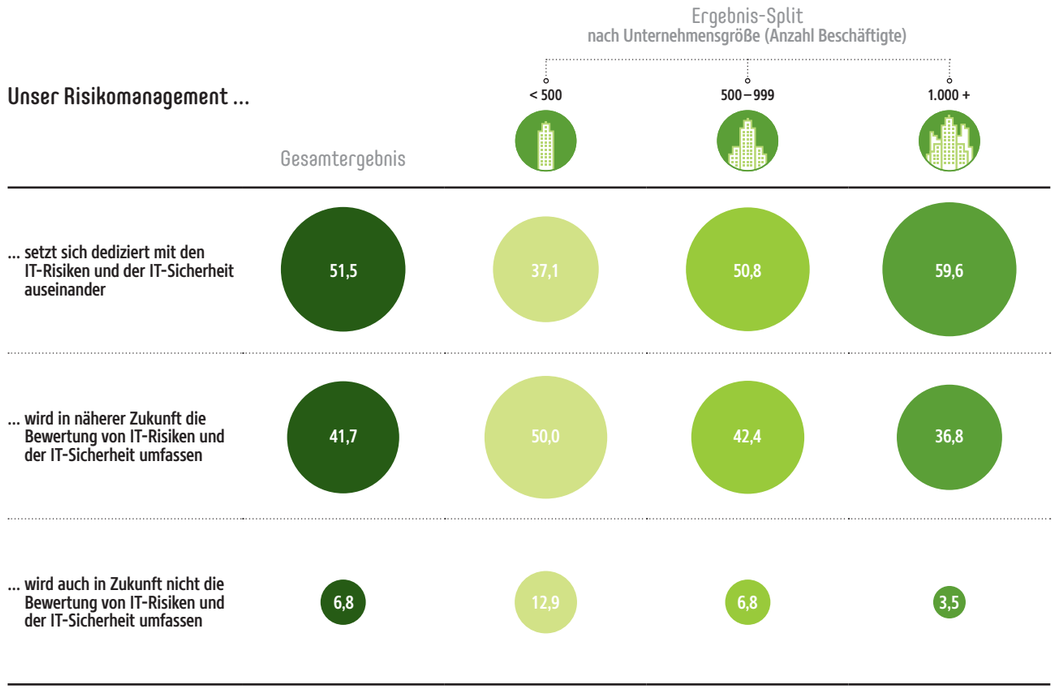
Nur 52 Prozent der Unternehmen geben an, dass sich ihr Risikomanagement bereits dediziert mit den IT-Risiken und der IT-Sicherheit auseinandersetzt. 42 Prozent der Befragten planen ein solches Vorgehen für die Zukunft, sieben Prozent haben dies aber auch später nicht vor. Doch nicht immer ist auch der IT-Bereich involviert, wenn die IT-Risiken bewertet werden.

In großen Unternehmen mit mindestens 1.000 Beschäftigten werden IT-Risiken und IT-Sicherheit zwar häufiger im betrieblichen Risikomanagement berücksichtigt als in kleineren Firmen mit weniger als 500 Beschäftigten – dennoch sind die Werte insgesamt auch hier recht niedrig (60 zu 37 Prozent).

Selbst von den Unternehmen, die laut Selbsteinstufung im Risk Maturity Model die höchsten Level 4 oder 5 erreichen *(vgl. Weiteres Ergebnis 7, Seite 28 f.)*, managen nur 59 Prozent die IT-Sicherheit und die IT-Risiken mit den anderen Unternehmensrisiken zusammen. In den Leveln 1 bis 3 sind es 45 Prozent.

Ist die IT eigener Bestandteil des Risikomanagements Ihres Unternehmens?

Angaben in Prozent. Filter: Nur C-Level, IT-Leitung, IT-Security- und Risk-Management-Verantwortliche in Unternehmen, in denen ihrer eigenen Einschätzung nach ein (initialer) Reifegrad nach dem Risk Maturity Model vorhanden ist. Basis: n = 235



Doch selbst dann, wenn die IT-Risiken dediziert im Risikomanagement des Unternehmens Berücksichtigung finden, bedeutet dies nicht automatisch, dass auch der IT-Bereich wirklich einbezogen wird. Stark involviert im IT-Risikomanagement ist der IT-Bereich nur in 42 Prozent der entsprechend agierenden Unternehmen. Bei elf Prozent der Befragten wird der IT-Bereich „eher nicht“ oder „gar nicht“ miteinbezogen, wenn es um das Management der IT-Risiken geht.

Offensichtlich sollte sich dies ändern, wenn man bedenkt, dass viele Unternehmen über die Komplexität der IT und die steigenden IT-Bedrohungen klagen. IT-Expertise sollte im IT-Risikomanagement nicht fehlen.

Wie stark ist der IT-Bereich in das IT-Risikomanagement Ihres Unternehmens involviert?

Angaben in Prozent. Filter: Nur C-Level, IT-Leitung, IT-Security- und Risk-Management-Verantwortliche in Unternehmen, in denen ihrer eigenen Einschätzung nach ein (initialer) Reifegrad nach dem Risk Maturity Model vorhanden ist. Basis: n = 235

9

Security-Outsourcing – nicht nur für kleine Unternehmen

Jedes zweite befragte Unternehmen lagert Aufgaben der IT-Security an externe Dienstleister aus. Dabei unterscheiden sich kleinere Unternehmen mit weniger als 500 Beschäftigten, die zu 53 Prozent Security-Outsourcing nutzen, nicht stark von den großen Unternehmen mit mindestens 1.000 Beschäftigten. Diese lagern IT-Sicherheitsaufgaben zu 47 Prozent aus.

Wenn IT-Security ausgelagert wird, geschieht dies bei 49 Prozent der entsprechenden Unternehmen zur Implementierung von sicherheitsfördernden Prozessen in einzelnen Abteilungen, also nicht unternehmensweit.

Nur zwölf Prozent der Unternehmen nutzen externe Dienstleister für solch komplexe Themen wie die Analyse von Bedrohungen, wobei hier „externes Wissen" besonders wichtig und hilfreich wäre. 19 Prozent der Befragten setzen bei der Untersuchung von Angriffen und forensischen Aufgaben auf externe Unterstützung. Dies ist ebenfalls eine relativ kleine Zahl, da für diese Aufgaben viel Erfahrung notwendig ist, die Security-Dienstleister eher sammeln können als interne Security-Abteilungen, deren Sicht vornehmlich auf das eigene Unternehmen konzentriert ist.

Unter den technischen Systemen sind es insbesondere Lösungen für Zero Trust, die als externer Dienst bezogen werden: 48 Prozent der Unternehmen entscheiden sich hier für das Outsourcing. Jedes dritte Unternehmen hat technische Aufgaben für IAM (Identity and Access Management) an Externe ausgelagert. Penetrationstests und die externe Überprüfung der internen Security werden jeweils von 29 Prozent der Unternehmen als Service bezogen.

Welche der folgenden IT-Bereiche hat Ihr Unternehmen an externe Dienstleister / Services Provider ausgelagert?

Angaben in Prozent. Mehrfachnennungen möglich. Basis: n = 339

	Gesamtergebnis	Ergebnis-Split nach Unternehmensgröße (Anzahl Beschäftigte) < 500	500 – 999	1.000 +
IT-Security	50,1	52,8	51,8	47,3
IT-Schulungen	49,9	45,3	45,8	55,3
Service Desk / IT-Hotline / technischer Support	32,7	33,0	26,5	36,0
IT-Infrastruktur	29,5	33,0	30,1	26,7
Software-, Datenbank, Web-Entwicklung	29,2	28,3	31,3	28,7
Wir haben andere IT-Bereiche ausgelagert.	11,2	8,5	10,8	13,3
Wir haben keine IT-Bereiche ausgelagert.	10,0	10,4	10,8	9,3
Weiß nicht	2,1	3,8	1,2	1,3

Welche IT-Security-Themen hat Ihr Unternehmen an einen oder mehrere Dienstleister / Services Provider ausgelagert?

Angaben in Prozent. Mehrfachnennungen möglich. Basis: Filter: Unternehmen, die den Bereich IT-Security ausgelagert haben. Basis: n = 170

	Gesamtergebnis	Ergebnis-Split nach Unternehmensgröße (Anzahl Beschäftigte) < 500	500 – 999	1.000 +
Implementierung von sicherheitsfördernden Prozessen in einzelnen Abteilungen	48,8	46,4	39,5	56,3
Überwachung von Security-Policies	42,9	37,5	44,2	46,5
Implementierung von technischen Systemen / Software	38,2	33,9	34,9	43,7
IT-Sicherheitstrainings / -schulungen	32,9	28,6	32,6	36,6
Evaluation von Security-Lösungen	25,9	32,1	23,3	22,5
Network Security	23,5	19,6	25,6	25,4
Analyse von Angriffen / forensische Maßnahmen	18,8	19,6	16,3	19,7
Maßnahmen zur Schärfung der Security Awareness unter Beschäftigten	16,5	12,5	16,3	19,7
Analyse von Bedrohungen	12,4	8,9	9,3	16,9
Data Leakage Prevention	11,2	10,7	9,3	12,7
Erstellung von Security-Policies	4,7	0,0	7,0	7,0

Welche technischen IT-Security-Systeme / -Prozesse hat Ihr Unternehmen an einen oder mehrere Dienstleister / Services Provider ausgelagert?

Angaben in Prozent. Mehrfachnennungen möglich. Filter: Unternehmen, die den Bereich IT-Security ausgelagert haben. Basis: n = 170

	Gesamtergebnis	Ergebnis-Split nach Unternehmensgröße (Anzahl Beschäftigte) < 500	500 – 999	1.000 +
Sicherheitsarchitektur (z.B. Zero-Trust-Ansatz, Absicherung von Microservices)	47,6	44,6	44,2	52,1
Identitäts- und Berechtigungsmanagement (IAM)	32,9	28,6	27,9	39,4
Penetration-Testing / externe Security-Überprüfung	28,8	23,2	23,3	36,6
Threat Intelligence / (KI-basierte) Bedrohungsanalysen	27,1	23,2	25,6	31,0
Security-Operation-Center-(SOC)-Operationen	23,5	19,6	18,6	29,6
API Security	19,4	16,1	25,6	18,3
Cloud Security	18,8	17,9	18,6	19,7
Firewall / SD-WAN	18,2	16,1	9,3	25,4
Security Automation	17,6	23,2	11,6	16,9
Mobile Device Management	15,9	21,4	11,6	14,1
Ransomware-Schutz	14,7	12,5	11,6	18,3
Patchmanagement	14,1	14,3	9,3	16,9
Web Application Security	13,5	10,7	11,6	16,9
Vulnerability Management	12,9	19,6	2,3	14,1
Backup & Restore	11,8	8,9	2,3	19,7
Data Leakage Prevention	10,6	10,7	4,7	14,1
Endpoint Security	7,1	3,6	4,7	11,3

10

XDR mit geringerer Verbreitung als Zero Trust oder SASE

Neue Technologien und Konzepte setzen sich in der Security unterschiedlich schnell durch. Während 71 Prozent der Befragten angeben, Zero Trust mindestens seit einigen Monaten im Einsatz zu haben, sind es im Fall von SASE (Secure Access Service Edge) 68 Prozent, und bei XDR (Extended Detection and Response) nur noch 43 Prozent.

Nur jeweils sechs Prozent der Unternehmen haben kein Interesse an →**Zero Trust*** oder aber an →**SASE**. Bei →**XDR** sind es sogar nur drei Prozent. Dennoch ist die Nutzung dieser Security-relevanten Technologien oder Konzepte gegenwärtig unterschiedlich stark ausgeprägt.

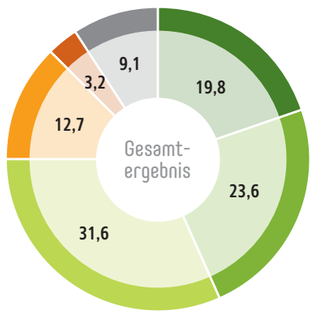
Gerade der Einsatz von XDR liegt im Vergleich zu den beiden anderen Konzepten SASE und Zero Trust deutlich zurück. 32 Prozent der befragten Unternehmen evaluieren derzeit konkret den XDR-Einsatz, weitere 13 Prozent planen diesen zumindest nicht mehr binnen Jahresfrist.

Unternehmen mit 500 bis 999 respektive mindestens 1.000 Beschäftigten setzen XDR häufiger ein als die kleineren Unternehmen mit weniger als 500 Mitarbeiterinnen und Mitarbeitern (48 bzw. 47 Prozent zu 34 Prozent).

Was den Vergleich des XDR-Einsatzes bezogen auf das jährliche IT-Budget angeht, lässt sich feststellen, dass die Unternehmen mit einem IT-Budget von über zehn Millionen Euro XDR deutlich häufiger im Einsatz haben (59 Prozent) als die Firmen mit weniger IT-Budget (34 Prozent).

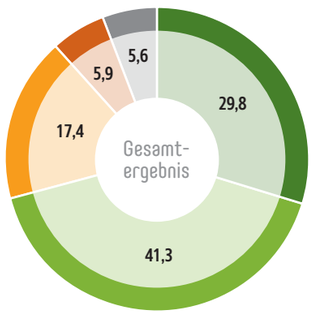
*** Mit → markierte Begriffe werden im Glossar auf Seite 45 erläutert.**

Hat Ihr Unternehmen XDR-Tools oder -Plattformen im Einsatz?
Angaben in Prozent. Basis: n = 339



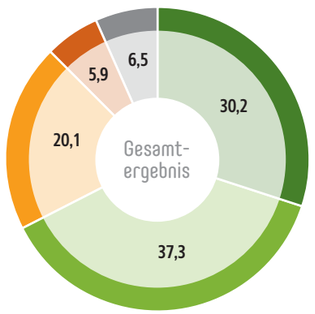
- XDR-Nutzung seit mehr als einem Jahr
- XDR-Nutzung seit einigen Monaten
- Derzeit Evaluierung von XDR-Lösungen
- Kein Einsatz von XDR binnen Jahresfrist geplant
- Kein Bedarf/Interesse an XDR
- Weiß nicht

Setzt Ihr Unternehmen ein Zero-Trust-Konzept ein?
Angaben in Prozent. Basis: n = 339



- Ja, schon seit mindestens einem Jahr
- Ja, seit einigen Monaten
- Nein, es ist aber geplant
- Nein, wir haben keinen Bedarf/Interesse an Zero Trust
- Weiß nicht

Hat Ihr Unternehmen ein SASE-Konzept im Einsatz?
Angaben in Prozent. Basis: n = 338



- Ja, schon seit mindestens einem Jahr
- Ja, seit einigen Monaten
- Nein, es ist aber geplant
- Nein, wir haben keinen Bedarf/Interesse an SASE
- Weiß nicht

Thorsten Henning
Regional Systems Engineering Director DACH, Fortinet

„Es ist wichtig, **kontinuierlich auf dem neuesten Stand zu bleiben und proaktiv neue Trends für sich und sein Unternehmen nach Relevanz und Kritikalität zu bewerten.** Die Bedrohungslandschaft entwickelt sich ständig weiter, und nur durch ständige Weiterbildung und Anpassung können Unternehmen effektiv geschützt bleiben. Der Threat Landscape Report der FortiGuard Labs ist ein Beispiel einer regelmäßig erscheinenden Informationsquelle.“

„Künstliche Intelligenz hat 2024 nicht nur die gesamte Gesellschaft durchdrungen, sondern beeinflusst auch die IT-Sicherheit nachhaltig. Dabei entdecken sowohl nicht-professionelle als auch professionelle Angreifer immer raffiniertere Angriffsvektoren. (IT-)Führungskräfte und Sicherheitsexperten sind deshalb heute mehr denn je gefordert, nicht nur die technischen, sondern vor allem auch die zwischenmenschlichen Faktoren in ihren Security-Konzepten zu berücksichtigen.“

Timo Hagenlocher,
Head of IT-Strategy, SPIRIT/21

IT-Security-Trends 2024

Die IT-Security zwischen alten Problemen und neuen Bedrohungen

Es ist nicht die Umsetzung von neuen Regulierungen wie NIS2, die den Unternehmen Kopfzerbrechen bereitet. Altbekannte Herausforderungen wie der Mangel an Personal und Know-how scheinen sich nicht lösen zu lassen. Zusätzlich kommen mit künstlicher Intelligenz (KI) neue Gefahren, die die Unternehmen sehen, aber noch nicht richtig adressiert haben.

Von Oliver Schonschek

Nur weil viel und ausführlich über die neuen Anforderungen durch die EU-Richtlinie NIS2 und die anstehende Umsetzung in Deutschland diskutiert und berichtet wird, bedeutet das nicht, dass die Unternehmen wirklich Schwierigkeiten damit haben. Zumindest denken die meisten Unternehmen, sie hätten die Vorgaben von NIS2 bereits erfüllt oder würden dies bis Jahresende in den Griff bekommen.

Ohne eine finale deutsche Gesetzgebung zur NIS2-Umsetzung sind aber die genauen Vorgaben gar nicht bekannt, denn die nationalen Umsetzungen dürfen die NIS2-Forderungen verschärfen. Doch es scheint so, als hätten die befragten Unternehmen zu viele andere „Security-Baustellen“, um sich gegenwärtig mit diesen „Details“ befassen zu können.

Zum einen sind es die Klassiker unter den Security-Hindernissen, die auch 2024 zu den klaren Trends der IT-Security gezählt werden müssen. So sind für die befragten Unternehmen (weiterhin) der Mangel an Personal und Know-how die größten Security-Hemmnisse.

Doch es kommen auch neue Bedrohungen auf die Betriebe in Deutschland zu. So geben mehr als acht von zehn Unternehmen an, dass KI-gesteuerte Attacken ein relevantes Thema für die IT-Security seien, und sehen deren Bedeutung noch höher als den vorherrschenden Fachkräftemangel – mit steigender Tendenz für die nächsten Jahre.

Offensichtlich hat KI einen mehrfachen Einfluss auf die Security. Die Stärkung der Angreiferseite durch KI-Unterstützung wird allerdings bewusster wahrgenommen als die Möglichkeiten, die KI und andere Verfahren zur Automatisierung der Security haben können. Auch im Jahr 2024 wird Security Automation noch nicht so genutzt, wie es für einen erfolgreichen Einsatz sein sollte, nämlich umfassend und integriert.

Stattdessen begrenzen die befragten Unternehmen Automatisierung in der Security auf einige Bereiche wie die Erkennung der Angriffe. Aber nur wenn die Security Automation wirklich von der Vorwarnung über die Entdeckung bis hin zur Reaktion und Aufklärung genutzt wird, lässt sich das knappe Security-Personal auch wirklich erfolgreich unterstützen.

Andererseits ist den meisten Betrieben sehr bewusst, dass KI in ihrem Unternehmen geschäftskritisch und schützenswert ist. Neun von zehn Firmen sehen für spezielle Security-Maßnahmen zum Schutz von KI-Systemen einen (eher/sehr) hohen bis essenziellen

Bedarf. Nur ein Prozent der Befragten meinen, keine schützenswerten KI-Lösungen im Unternehmen zu haben.

Wer bisher das vielfach beschriebene Ransomware-Risiko unter den IT-Security-Trends 2024 vermisst hat, wird auch jetzt enttäuscht werden. So gehört Ransomware-Schutz im Gegensatz zu Lösungen für IAM (Identity and Access Management) und Zero Trust nicht zu den Schwerpunkten bei den Security-Investitionen. Natürlich helfen IAM-Funktionen wie die Beschränkung von Berechtigungen und Zero Trust auch bei der Minderung der Ransomware-Risiken, diese stehen aber bei den Investitionen in Security im Jahr 2024 nicht wirklich im Fokus.

Überhaupt möchten die Unternehmen nur ungern viele weitere Security-Lösungen und Security-Anbieter in ihrem „Portfolio“, das sie managen müssen. Stattdessen geben fast alle Unternehmen an, dass die Zahl der Security-Tools kleiner werden müsse. Gleiches gilt für die Zahl der Security-Hersteller, mit denen man zusammenarbeitet.

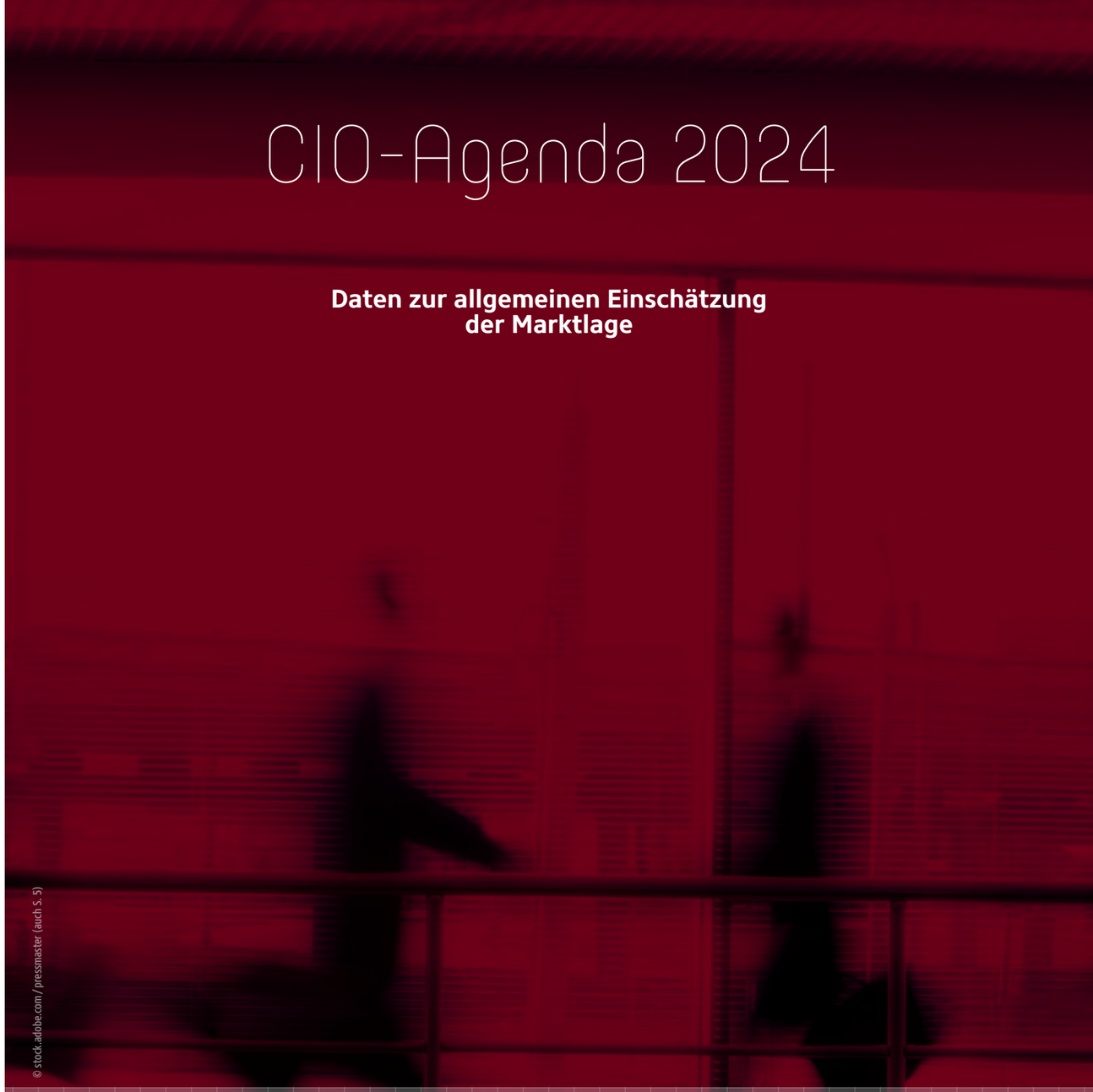
Während sich die Befragten in diesen Punkten sehr einig sind, sind sie es bei vielen anderen drängenden Security-Fragen gegenwärtig nicht. So erklären trotz Fachkräftemangel mehr Unternehmen, dass sie ihre offenen Security-Stellen eher besetzen können, als es Unternehmen gibt, die über offene Stellen klagen, die unbesetzt bleiben.

Dabei ist es gerade bei so vielen Aufgaben und Herausforderungen für die Security extrem wichtig, klare Richtungen und Perspektiven einzunehmen. Nur wenn zum Beispiel der Fachkräftemangel von möglichst vielen Unternehmen richtig erkannt und adressiert wird, kann es Bewegung bei diesem „alten“ Problem geben. Ebenso muss die Sicht auf neue Bedrohungen wie KI geschärft werden. Wenn viele Unternehmen keine Strategie für KI haben, werden auch die gewünschten Lösungen zum Schutz von KI nicht wirklich greifen können. Bekanntlich kann man nur schützen, was man richtig kennt.

Das aber verweist auf ein weiteres, schon lange bestehendes Problem der Security, das endlich angegangen werden muss: Viele CISOs erhalten auch im Jahr 2024 noch keine Verantwortung für die Security. Dabei erfordern Security-Entscheidungen sehr viel Expertise, von der es viel zu wenig gibt. Deshalb sollte man die Expertise, die dank CISOs verfügbar ist, auch wirklich nutzen.

CIO-Agenda 2024

Daten zur allgemeinen Einschätzung der Marktlage



Exklusive Einblicke: Wie IT-Verantwortliche das Business in Gegenwart und Zukunft gestalten

IT-Security-Trends 2024

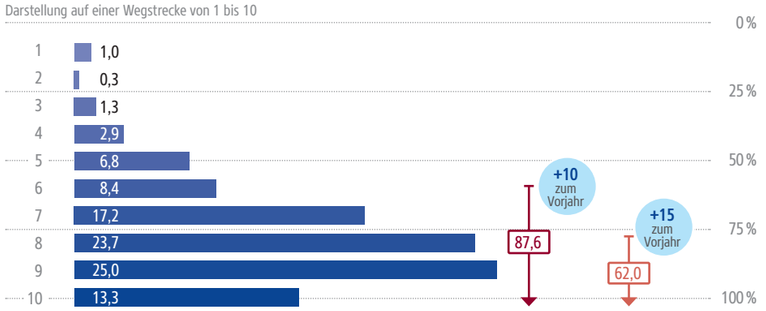
CIO-Agenda 2024

Alle Angaben in Prozent

Ein Studienprojekt des Custom Research Teams von CIO, CSO und COMPUTERWOCHE in Kooperation mit Bechtle, Lufthansa Industry Solutions sowie der WHU – Otto Beisheim School of Management.

Digitaler Wandel – es geht schnellen Schrittes voran

Mehr als 87 Prozent der befragten IT-Verantwortlichen sehen sich und ihre Unternehmen auf der zweiten Hälfte des Weges der digitalen Transformation, **62 Prozent** davon bereits gut im letzten Viertel. Beide Werte liegen deutlich über denen des Vorjahrs (+10 bzw. +15 Prozentpunkte).

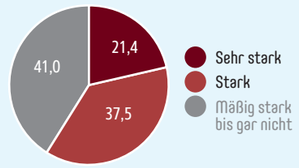


Generative KI ist eine Wucht

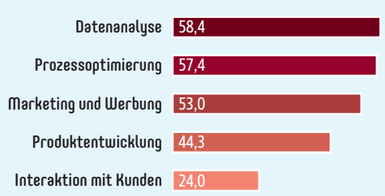
In **59 Prozent** der Unternehmen kommt generative künstliche Intelligenz stark oder sehr stark zum Einsatz – meist zur **Datenanalyse, Prozessoptimierung oder in Marketing und Vertrieb**.

Ein Drittel der Nutzenden hat die Technologie bereits vollständig in ihre täglichen Arbeitsabläufe integriert. **68 Prozent** der Unternehmen planen in den kommenden zwei bis drei Jahren, die GenAI-Nutzung weiter auszubauen.

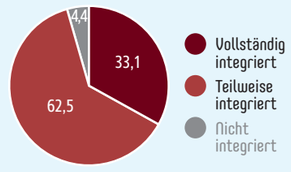
Wie stark wird generative KI in Ihrem Unternehmen genutzt?



In welchen Bereichen wird generative KI in Ihrem Unternehmen genutzt?



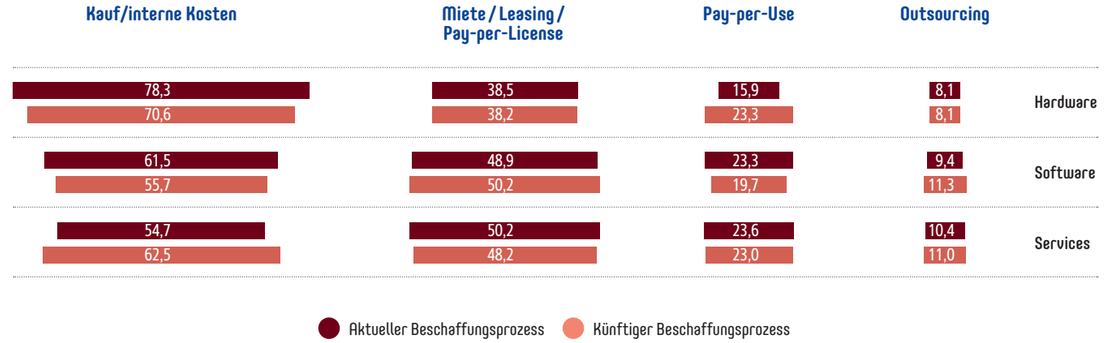
In welchem Maß ist die generative KI in die täglichen Arbeitsabläufe Ihres Unternehmens integriert?



Welche Pläne hat Ihr Unternehmen bezüglich der Nutzung generativer KI in den kommenden 2 bis 3 Jahren?

Sich verändernde Beschaffungsprozesse

Besonders **Hard- und Software** werden noch eher physisch eingekauft respektive selbst entwickelt als beispielsweise nach dem „Pay-per-Use"-Modell aus der Cloud bezogen. Gerade im Hardware-Bereich könnte sich das künftig aber wandeln.



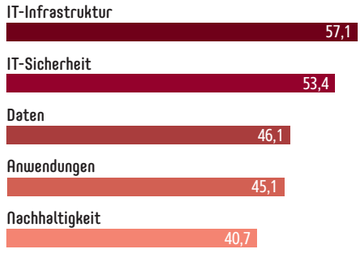
Mut zur Pionierarbeit

Jede/r dritte CIO **(33 Prozent)** sieht sich als Vorreiter/in für Digitalisierungsinitiativen – satte 21 Prozentpunkte mehr als im Vorjahr. Als „Fast Follower" bezeichnen sich **51 Prozent** (-3 Prozentpunkte).

Welche der folgenden Beschreibungen charakterisiert Ihr Unternehmen am besten?

Viel Geld für IT-Infrastruktur

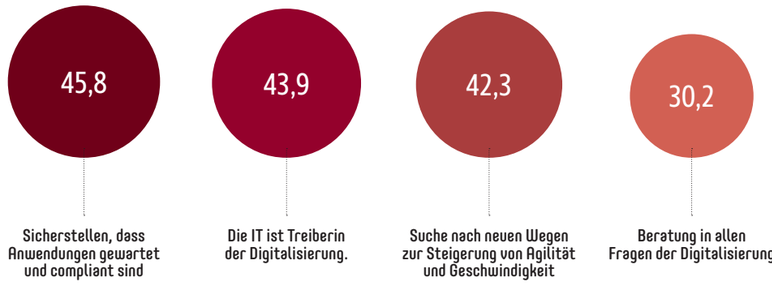
Substanzielle IT-Investments wollen die CIOs in den kommenden drei Jahren am häufigsten im Bereich **Infrastruktur** tätigen. Auch in **IT-Sicherheit** – das Topthema des Vorjahrs – und **Daten** wird weiter (stark) investiert.
Die Aufsteiger in die Top 5: **Anwendungen** und **Nachhaltigkeit**.



Gestalten anstatt „nur" beraten

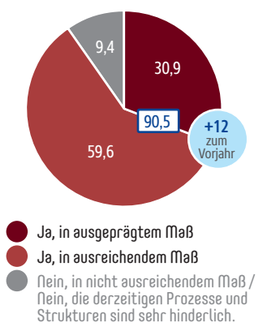
Die meisten CIOs/IT-Leitenden sehen ihren eigenen Fokus und den des gesamten IT-Bereichs mittelfristig verstärkt darin, sicherzustellen, dass Anwendungen gewartet und compliant sind. Zudem geht es um das Treiben der Digitalisierung und die Suche nach neuen Wegen zur Steigerung von Agilität und Geschwindigkeit. In einer „reinen" Beraterrolle sehen sich die CIOs eher weniger.

Verstärkter Fokus in fünf Jahren:



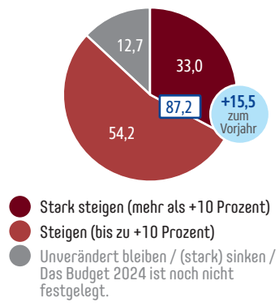
Entwicklung neuer digitaler Geschäftsmodelle

Mehr als **90 Prozent** der Unternehmen verfügen über grundlegende Prozesse und Strukturen dafür. Der Wert liegt deutlich über dem des Vorjahrs (+12 Prozentpunkte).



Hohe Energiepreise beeinflussen IT-Budgets

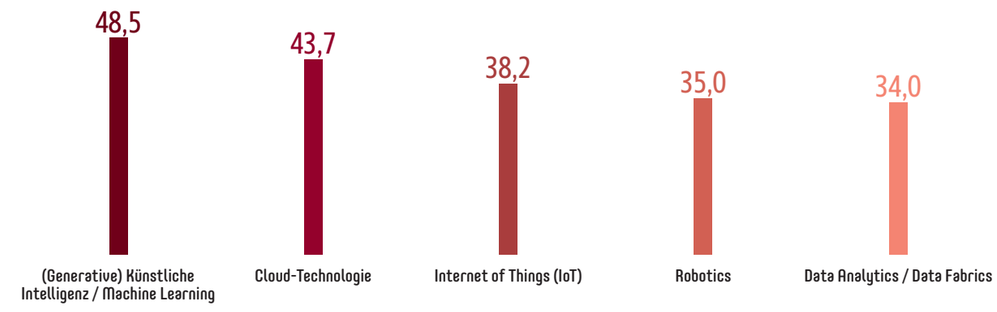
Das Gesamt-IT-Budget wird bei **87 Prozent** der Befragten steigen – bei **33 Prozent** davon sogar stark. Dass diese Entwicklung (auch) unmittelbar mit den hohen Energiepreisen zusammenhängt, bestätigen 73 Prozent der Unternehmen.



Umwälzende Technologien

Fast jede/r zweite Befragte **(49 Prozent)** erwartet, dass (generative) künstliche Intelligenz und Machine Learning die Technologien sind, die das Geschäftsmodell des Unternehmens in den kommenden drei Jahren am stärksten verändern werden. Cloud-Technologie, IoT, Robotics und Analytics folgen mit etwas Abstand.

Was meinen Sie: Welche der genannten Technologien / IT-Themen werden Geschäftsmodell und Geschäftsprozesse Ihres Unternehmens in den kommenden drei Jahren am stärksten verändern?



Grundgesamtheit:
Oberste (IT-)Verantwortliche von Unternehmen in der DACH-Region: Beteiligte an strategischen (IT-) Entscheidungsprozessen im C-Level-Bereich, Tech-C-Level (CIOs, CTOs CDOs etc.) und in den Fachbereichen (LoBs), Entscheidungsbefugte sowie Expertinnen & Experten aus dem IT-Bereich

Gesamtstichprobe:
309 abgeschlossene und qualifizierte Interviews

Untersuchungszeitraum:
14. bis 29. November 2023

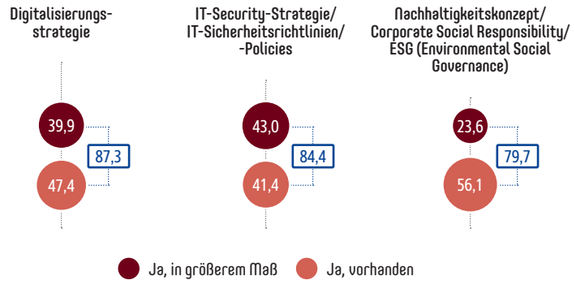
Methode:
Online-Umfrage (CAWI)

CIO-Agenda 2024

Alle Angaben in Prozent

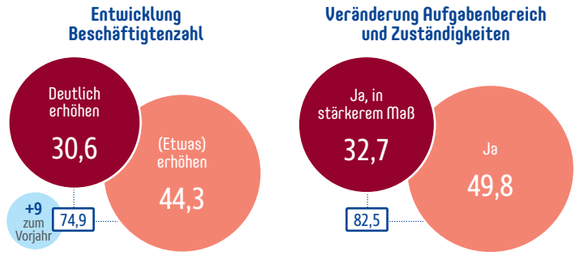
Digitalisiert, abgesichert, nachhaltig

87 Prozent der Unternehmen haben eine Digitalisierungsstrategie, **84 Prozent** eine IT-Security-Strategie oder zumindest IT-Sicherheitsrichtlinien. Mit einem Konzept zu Nachhaltigkeit / CSR / ESG warten **80 Prozent** auf.



IT-Bereich – mehr Personal, neue Aufgaben

Die Zahl der IT-Beschäftigten soll in **75 Prozent** der Unternehmen (zum Teil deutlich) erhöht werden. Dieser Anteil steigt im Vergleich zum Vorjahr um knapp neun Prozentpunkte. Gleichzeitig erwarten **83 Prozent** der IT-Verantwortlichen eine Veränderung von Aufgaben und Zuständigkeiten des IT-Bereichs, 33 Prozent davon sogar in stärkerem Maß.

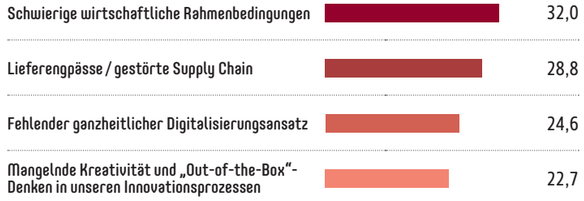


Kooperation mit Wettbewerbern und Behörden

Um besser für die Herausforderungen der Zukunft gewappnet zu sein, arbeiten **39 Prozent** der Unternehmen punktuell mit Wettbewerbern zusammen. **42 Prozent** planen das (+7 Prozentpunkte zum Vorjahr). Mit dem Public Sector kooperieren **45 Prozent** der Befragten (+8), **39 Prozent** planen dies (+1).

Widerstände

Besonders die **hohen Energiepreise**, die **schwierigen wirtschaftlichen Rahmenbedingungen** und **gestörte Lieferketten** begrenzen die digitalen Ambitionen vieler Unternehmen.



Executive Summary

Der Mut ist zurück: Sah sich im Zuge unserer letztjährigen Erhebung zur „CIO-Agenda" gerade einmal etwas mehr als jede/r zehnte befragte IT-Verantwortliche als Vorreiter/in für Digitalisierungsinitiativen, ist es nunmehr jede/r dritte. Dass sich die meisten CIOs und IT-Leitenden daraus folgend in Zukunft eher in der Gestaltungsrolle für den digitalen Wandel sehen als „nur" beratend zur Seite zu stehen oder bestehende Systeme und Prozesse zu verwalten, ist ebenfalls ein untrügliches Zeichen neugewonnener Stärke. Es soll und darf investiert werden – in IT-Personal, Strategie und Technik. Der gesamte IT-Bereich darf und muss aber auch selbstbewusst auftreten – denn es ist seitens der meisten Vorstände und Geschäftsführungen unbestritten, dass nur eine agile und flexible IT-Organisation dem Business Geschwindigkeit und Stärke verleiht.
In unsicheren wirtschaftlichen Zeiten wie diesen ist diese Erkenntnis nicht die schlechteste.
Fast jedes neunte Unternehmen hat mittlerweile den eigenen Weg der digitalen Transformation zu mehr als der Hälfte zurückgelegt – mehr als jedes sechste sieht sich sogar schon (fast) auf der selbstgesteckten Zielgeraden. Im Vergleich zum Vorjahr sind das allesamt erhebliche Steigerungen und beachtliche Zahlen.
Daraus folgt konsequenterweise, dass die meisten Organisationen mittlerweile über grundlegende Prozesse und Strukturen für die Entwicklung neuer digitaler Geschäftsmodelle verfügen. Neben den strategischen und organisatorischen Vorkehrungen braucht es dafür innerhalb und außerhalb des IT-Bereichs die richtige technologische Grundlage – und hier kristallisiert sich besonders der Einsatz von generativer KI zunehmend als „Gamechanger" heraus – sei es für die Analyse von Daten, die Optimierung von Arbeitsabläufen oder ein besseres Kundenerlebnis. Es verwundert also nicht, dass die IT-Verantwortlichen – sicherlich auch angesichts des Fachkräftemangels – zunehmend auf diese Karte setzen.

Die stille Revolution der generativen KI

Vielerorts als größter technologischer Fortschritt dieser Tage gefeiert, hängen Einsatztiefe und Business-Nutzen der generativen künstlichen Intelligenz stark vom digitalen Reifegrad eines Unternehmens ab.

Prof. Dr. Dries Faems
ist Inhaber des Lehrstuhls für Entrepreneurship, Innovation und Technologische Transformation an der WHU – Otto Beisheim School of Management.

Von Prof. Dr. Dries Faems

In weniger als einem Jahr hat die generative KI, die für ihre Fähigkeit bekannt ist, neue Texte, Bilder und Sprachen zu erzeugen, einen enormen Popularitätsschub erfahren. Während Studierende damit ihre Hausarbeiten erledigen sowie Influencerinnen und Influencer ihre Präsenz in den sozialen Medien steigern, war bisher eher noch unbekannt, in welchem Ausmaß die Technologie seitens der Unternehmen angenommen und eingesetzt wird.

Die Ergebnisse der Studie „CIO-Agenda 2024", die von der CIO-Marktforschung in Zusammenarbeit mit der WHU – Otto Beisheim School of Management, Bechtle und Lufthansa Industry Solutions durchgeführt wurde, geben nun aber Aufschluss darüber, wie Unternehmen in der DACH-Region generative KI einsetzen und in ihren Betrieb integrieren.

Signifikante Durchdringung

Befragt wurden 309 CIOs, CEOs, Vorstände, C-Führungskräfte und Abteilungsleitungen aus allen Bereichen und Branchen. Es zeigt sich eine signifikante Durchdringung der generativen KI in der DACH-Unternehmenslandschaft. Auffallend viele, nämlich 21 Prozent der Befragten, berichten von einer „sehr starken Nutzung", während 37 Prozent diese Technologie „stark" und 29 Prozent „eher stark" nutzen. Es verbleiben lediglich 13 Prozent der Befragten, die generative KI selten oder nie nutzen, was eine weit verbreitete Akzeptanz und Annahme unter den Unternehmen unterstreicht. Mit anderen Worten: Die Mehrheit der Unternehmen in unserer Umfrage scheint im Stillen damit begonnen zu haben, mit generativer KI für ihre Geschäftsaktivitäten zu experimentieren.

Interessanterweise konzentriert sich der Einsatz in diesen Unternehmen überwiegend auf interne Prozesse. Produktentwicklung (44 Prozent), Marketing (53 Prozent), Prozessoptimierung (57 Prozent) und Datenanalyse (58 Prozent) sind die wichtigsten Anwendungsbereiche. Diesem internen Fokus steht eine relativ bescheidene Anwendung nach außen gegenüber: Nur 24 Prozent der Unternehmen setzen generative KI in der Kundeninteraktion ein. Diese Zweiteilung deutet auf eine vorsichtige Herangehensweise an externe Anwendungen hin – möglicherweise aufgrund von Bedenken hinsichtlich des Datenschutzes und der Datensicherheit.

Digitale Pionierarbeit auch im KI-Umfeld

Im Zuge der Befragung haben wir – mithilfe von vorgegebenen Eigenbeschreibungen – die Unternehmen ihren digitalen Reifegrad einschätzen lassen. Dadurch ließen sich die folgenden vier Kategorien clustern: digitale Pioniere („Unser Unternehmen ist ein Vorreiter der digitalen Transformation"), digitale

Mitläufer („Unserem Unternehmen fällt es eher leicht, vom Wettbewerb gestartete Digitalisierungsinitiativen zu übernehmen bzw. sich diesen anzupassen“), digitale Nachzügler („Unserem Unternehmen fällt es eher schwer, vom Wettbewerb gestartete Digitalisierungsinitiativen zu übernehmen bzw. sich diesen anzupassen“) und digitale Verlierer („Unser Unternehmen hat den Digitalisierungsinitiativen des Wettbewerbs nichts entgegenzusetzen“).

Bei der Anwendung dieser Kategorisierung konnten wir einen deutlichen Unterschied in der Nutzungsintensität zwischen den verschiedenen Gruppen feststellen. Die digitalen Pioniere sind führend in der Nutzung generativer KI – 41 Prozent von ihnen nutzen sie „sehr stark“. Im Vergleich dazu berichten nur zwölf Prozent der digitalen Mitläufer, sieben Prozent der digitalen Nachzügler und weitere sieben Prozent der digitalen Verlierer über die gleiche Nutzungsintensität. Diese Diskrepanz verdeutlicht eine digitale Kluft, bei der die digital versierteren Unternehmen eher dazu neigen, generative KI vollständig zu nutzen.

Noch deutlicher wird diese Kluft durch den Grad der Integration generativer KI in die täglichen Aktivitäten. Auch hier sind die digitalen Pioniere führend: 48 Prozent von ihnen haben generative KI vollständig integriert, gefolgt von 29 Prozent der digitalen Nachzügler, 23 Prozent der digitalen Mitläufer und 20 Prozent der digitalen Verlierer. Dieses Ergebnis zeigt, dass digitale Marktführer generative KI nutzen, um Abläufe zu optimieren, Innovationen zu fördern und einen Wettbewerbsvorteil zu erzielen.

Fazit

Insgesamt vermittelt die „CIO-Agenda 2024“ ein erstes Bild von der stillen Revolution der generativen KI in DACH-Unternehmen. Obwohl sie als reine Technologie bereits auf breiter Front eingeführt wurde, ist dennoch klar erkennbar, dass ihre Einsatztiefe vom digitalen Reifegrad eines Unternehmens abhängt. Digitale Vorreiter sind nicht nur begeisterte Anwender, sondern auch geschickter bei der Integration dieser Technologien in ihre Kernprozesse. Dieser Trend deutet darauf hin, dass die generative KI die Kluft zwischen den digitalen Marktführern und den Verlierern potenziell vergrößern und die Wettbewerbslandschaft in der DACH-Region weiter prägen könnte.

Hintergrund zur Studie

Die Studie „CIO-Agenda 2024“ wurde vom 14. bis 29. November 2023 vom Custom Research Team von CIO, CSO und COMPUTERWOCHE in Zusammenarbeit mit der WHU, Bechtle und Lufthansa Industry Solutions durchgeführt. Es nahmen 309 CIOs, Geschäftsführungs- und Vorstandsmitglieder, C-Führungskräfte, Abteilungsleiter und -leiterinnen aus verschiedenen Unternehmensbereichen aller Branchen in Deutschland, Österreich und der Schweiz an der Onlinebefragung teil.

IAM (Identity and Access Management)
Oberbegriff für die Gesamtheit der Technologien, Strategien und Prozesse, die verwendet werden, um digitale Identitäten und deren Zugriff auf Ressourcen innerhalb eines Unternehmens zu verwalten. Entscheidend für die Sicherheit und Effizienz von IT-Infrastrukturen, da es sicherstellt, dass nur autorisierte Benutzer Zugriff auf sensible Daten und Systeme haben und dass diese Zugriffe überwacht und protokolliert werden können.

Penetrationstest / Penetration Testing
Umfassender Sicherheitstest einzelner Rechner oder Netzwerke jeglicher Größe. Prüft die Sicherheit von Systembestandteilen und Anwendungen eines Netzwerks oder Softwaresystems mit aus zahlreichen bekannten Angriffsmustern abgeleiteten Mitteln und Methoden, die deshalb tauglich sind, unautorisiert in das System einzudringen. Kann somit Sicherheitslücken aufdecken, aber nicht ausschließen.

SASE (Secure Access Service Edge)
IT-Security-Konzept, das im Wesentlichen mehrere Netzwerk- und Sicherheitsfunktionen in einer einzigen cloudbasierten Architektur kombiniert. Integriert traditionelle Netzwerkfunktionen wie SD-WAN (Software-defined Wide Area Networking) mit Sicherheitsfunktionen wie Firewall, Secure Web Gateway (SWG), CASB (Cloud Access Security Broker), Zero Trust Network Access (ZTNA), Data Loss Prevention (DLP) und mehr.

XDR (Extended Detection and Response)
Die erweiterte Erkennung und Reaktion auf Cyberbedrohungen im gesamten Netzwerk. Erhöht im Vergleich zu bisherigen Endpoint-Protection-Lösungen (u.a. EDR) die Sichtbarkeit im Netzwerk durch die breitere Analyse von Daten aus der IT-Umgebung und fördert dadurch auch die schnellere Erkennung von Bedrohungen bei abweichendem Verhalten.

Zero Trust
Sicherheitskonzept, bei dem keinem Gerät, keinem Nutzer und keinem Dienst – weder innerhalb noch außerhalb des Unternehmensnetzes – per se vertraut wird. Sämtliche Anwender und Dienste müssen einzeln authentifiziert werden.

Studiendesign

Alle wissenswerten Informationen
zu Aufbau, Methodik
und Stichprobe der Studie

IT-Security-Trends 2024

Studienpartner

Basis-Partner:

Fortinet GmbH
Feldbergstraße 35
60323 Frankfurt am Main
Telefon: +49 69 310192–0
E-Mail: sales-germany@fortinet.com
Web: www.fortinet.com/de

SPIRIT/21 GmbH
Otto-Lilienthal-Straße 36
71034 Böblingen
Telefon: +49 7031 2093333
E-Mail: info@spirit21.com
Web: www.spirit21.com

Gesamtstudienleitung

Matthias Teichmann
Director Research
Custom Research Team
Telefon: +49 89 36086 131
matthias.teichmann@foundryco.com

Projektmanagement

Simon Hülsbömer
Senior Research Manager
Custom Research Team
Telefon: +49 89 36086 177
simon.huelsboemer@foundryco.com

Armin Rozsa
Research Manager
Custom Research Team
Telefon: +49 89 36086 184
armin.rozsa@foundryco.com

Sales-Team

Julia Depaoli
Director SDR, Research & Commercial
Telefon: +49 89 36086 125
julia.depaoli@foundryco.com

Impressum

Studienkonzept / Fragebogenentwicklung:
Simon Hülsbömer,
Matthias Teichmann

Endredaktion / CvD Studienberichtsband:
Simon Hülsbömer

Analysen / Kommentierungen:
Oliver Schonschek, Bad Ems

Kommentierungen CIO-Agenda 2024:
Simon Hülsbömer

Hosting / Koordination Feldarbeit:
Armin Rozsa

Artdirector & Grafik:
Daniela Petrini, Reutte

Umschlaggestaltung unter
Verwendung eines Farbfotos
von © freepik.com / Flat data privacy
day illustration

Lektorat:
Elke Reinhold, München

Ansprechpartner:
Matthias Teichmann
matthias.teichmann@foundryco.com

Herausgeber:

Foundry
(formerly IDG Communications)

Anschrift:
IDG Tech Media GmbH
Georg-Brauchle-Ring 23
80992 München
Telefon: +49 89 36086–0
Fax: +49 89 36086 118
E-Mail: info@idg.de

Vertretungsberechtigter:
Jonas Triebel, Geschäftsführer

Registergericht:
Amtsgericht München, HRB 99110

Umsatzsteueridentifikationsnummer:
DE 811 257 834

Weitere Informationen unter:
www.foundryco.com

Studiensteckbrief

Herausgeber	CIO, CSO und COMPUTERWOCHE
Studienpartner	Fortinet GmbH SPIRIT/21 GmbH
Grundgesamtheiten	Oberste (IT-)Verantwortliche in Unternehmen der DACH-Region: Beteiligte an strategischen (IT-)Entscheidungsprozessen im C-Level-Bereich und in den Fachbereichen (LoBs); Entscheidungsbefugte sowie Experten und Expertinnen aus dem IT(Security)-Bereich
Teilnehmergenerierung	Persönliche E-Mail-Einladung über die exklusive Unternehmensdatenbank von CIO, CSO und COMPUTERWOCHE sowie – zur Erfüllung von Quotenvorgaben – über externe Online-Access-Panels
Gesamtstichprobe	339 abgeschlossene und qualifizierte Interviews
Untersuchungszeitraum	06. bis 13. Mai 2024
Methode	Online-Umfrage (CAWI)
Fragebogenentwicklung und Durchführung	Custom Research Team von CIO, CSO und COMPUTERWOCHE in Abstimmung mit den Studienpartnern

Stichprobenstatistik

Branchenverteilung*	Land- und Forstwirtschaft, Fischerei, Bergbau	6,8 %
	Energie- und Wasserversorgung	13,6 %
	Chemisch-pharmazeutische Industrie, Life Science	15,0 %
	Medizin- und Labortechnik	10,3 %
	Metallerzeugende und -verarbeitende Industrie	14,2 %
	Maschinen- und Anlagenbau	9,1 %
	Automobilindustrie und Zulieferer	10,6 %
	Herstellung von elektrotechnischen Gütern, IT-Industrie	21,2 %
	Konsumgüter-, Nahrungs- und Genussmittelindustrie	5,3 %
	Medien, Papier- und Druckgewerbe	5,3 %
	Baugewerbe, Handwerk	3,2 %
	Groß- und Einzelhandel (inkl. Online-Handel)	10,3 %
	Banken und Versicherungen	10,6 %
	Transport, Logistik und Verkehr	9,7 %
	Dienstleistungen für Unternehmen	10,6 %
	Hotel- und Gastgewerbe, Tourismus	5,6 %
	Öffentliche Verwaltung, Gebietskörperschaften, Sozialversicherung	7,1 %
	Schule, Universität, Hochschule	3,5 %
	Gesundheits- und Sozialwesen	6,2 %
	Andere Branchengruppe	3,8 %
Unternehmensgröße deutschlandweit	Weniger als 100 Beschäftigte	5,6 %
	100 bis 249 Beschäftigte	13,3 %
	250 bis 499 Beschäftigte	12,4 %
	500 bis 999 Beschäftigte	24,5 %
	1.000 bis 9.999 Beschäftigte	31,9 %
	10.000 Beschäftigte und mehr	12,4 %
Umsatzklasse deutschlandweit	Weniger als 20 Millionen Euro	8,3 %
	20 bis unter 50 Millionen Euro	15,0 %
	50 bis unter 100 Millionen Euro	16,5 %
	100 Millionen bis unter 1 Milliarde Euro	28,0 %
	1 bis unter 5 Milliarden Euro	15,3 %
	5 Milliarden Euro und mehr	11,8 %
	Weiß ich nicht / keine Angabe	5,0 %
Jährliche Aufwendungen in IT-Systeme	Weniger als 1 Million Euro	12,7 %
	1 bis unter 10 Millionen Euro	28,9 %
	10 bis unter 100 Millionen Euro	29,8 %
	100 Millionen Euro und mehr	18,6 %
	Weiß ich nicht / keine Angabe	10,0 %

* Mehrfachnennungen möglich

Das Studienkonzept

Die Multi-Client-Studien von CIO, CSO und COMPUTERWOCHE sind mehr als nur Befragungen von C-Level-Verantwortlichen und IT-Fachleuten. Hinter den Marktforschungsprojekten steht ein nachhaltiges Studienkonzept, das auf eine Laufzeit von mindestens sechs Monaten ausgelegt ist.

Die Veranstaltung der initialen redaktionellen Round Tables, moderiert von leitenden Redakteuren und Redakteurinnen von CIO, CSO und COMPUTERWOCHE, steht immer zu Beginn eines jeden Studienprojekts.

Über den Verlauf der Round-Table-Veranstaltungen wird ausführlich berichtet, und die Themen, die den Branchenfachleuten besonders „auf den Nägeln brennen“, werden auch bei der Entwicklung des Studienfragebogens mitberücksichtigt. Die Unternehmen, die das Projekt als Partner begleiten, können eigene Ideen und Fragestellungen einbringen.

Etwa drei Monate nach der methodischen und inhaltlichen Ausgestaltung der Studie liegen die zentralen Ergebnisse in Form eines hochwertigen Survey Reports vor. Die Studienergebnisse werden auf Messen und Events, wie der Hannover Messe, dmexco oder it-sa, präsentiert, zum Teil in Form von Podiumsdiskussionen, bei denen sich die Studienpartner einem interessierten Fachpublikum stellen können.

Begleitet wird das gesamte Studienprojekt durch kontinuierliche Berichterstattung von CIO, CSO und COMPUTERWOCHE, zum Thema im Allgemeinen und zur Studie im Speziellen. Fachwissen und Kompetenz unserer Autoren und Autorinnen sowie unseres redaktionellen Teams tragen maßgeblich dazu bei, dass die Ergebnisse der Multi-Client-Studien richtig eingeordnet werden können. Berichtet und kommentiert wird auf allen modernen Medienkanälen; Infografiken, Bildergalerien und Video-Interviews tragen dazu bei, dass die Studien auf großes Interesse stoßen.

Round-Table-Moderation

Julia Mutzbauer:
Redakteurin

Julia Mutzbauer ist für die Medienmarke CSO zuständig, dort vor allem für die inhaltliche Ausrichtung des Onlinemagazins. Für die tägliche Berichterstattung beschäftigt sie sich mit allen Themen rund um Cybersicherheit. Zudem pflegt sie das CSO-LinkedIn-Netzwerk.

Protokoll

Richard Ruf, München

Der Autor dieser Studie

Oliver Schonschek

Oliver Schonschek ist freier Analyst und Fachjournalist und schreibt für führende Fachmedien über IT, Sicherheit und Datenschutz, darunter COMPUTERWOCHE und CIO. Er ist Herausgeber und Autor mehrerer Fachbücher und wurde in den USA mehrfach als Influencer und Media Leader für Technologien wie Blockchain, KI, VR/AR und Mobile Computing ausgezeichnet.

Unsere Studienreihe

Laufende Studienberichterstattung auf
computerwoche.de/p/research,3557

Folgen Sie uns auf LinkedIn:
https://www.linkedin.com/showcase/research-services-germany

FORTINET

SPIRIT/21

IT that works.