EY
Cybersicherheit II

Befragungsergebnisse

Juli 2025

Building a better working world

Befragungsdesign | Beschreibung der Untersuchung

Auftraggeber

EY Ernst & Young ServicegmbH

Zielgruppe

Österreichische Unternehmen ab 20 Mitarbeitenden

Stichprobe

n = 200 Interviews, davon:
n=80 20-49 MA
n=49 50-99 MA
n=71 100+ MA

Methode

Telefonische Befragung, Quotenstichprobe (Unternehmensgröße, Branche, Bundesland)

Technische Details

Maximale Schwankungsbreite: +/- 6,9%

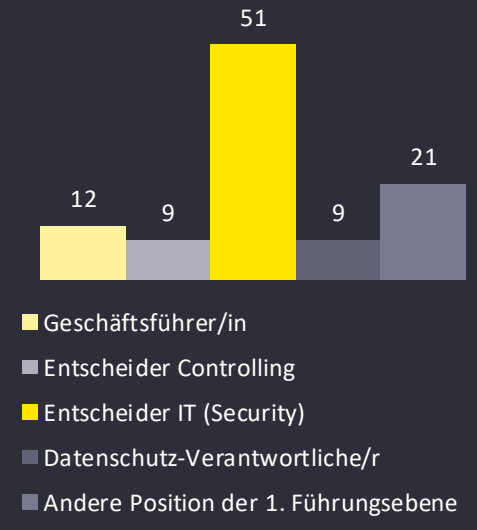
Ø Interviewdauer: 8 Min.

Erhebungszeitraum

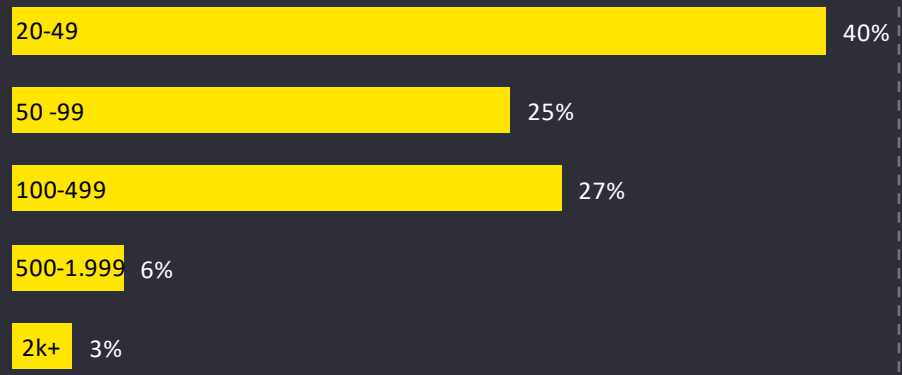
03. Juni – 02. Juli 2025

Befragungs- und Stichprobendesign

Beschreibung der Stichprobe



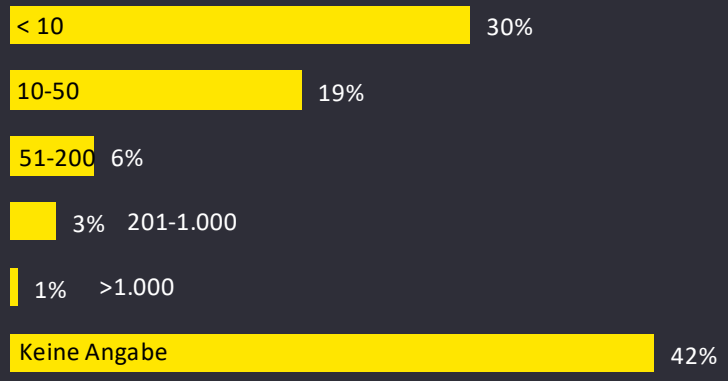
Unternehmensgröße nach MA-Anzahl



Branche

19% Wien
21% Niederösterreich
4% Burgenland
14% Steiermark
7% Kärnten
19% Oberösterreich
4% Salzburg
10% Tirol
4% Vorarlberg

Unternehmensgröße nach Umsatz (in Mio. EUR)

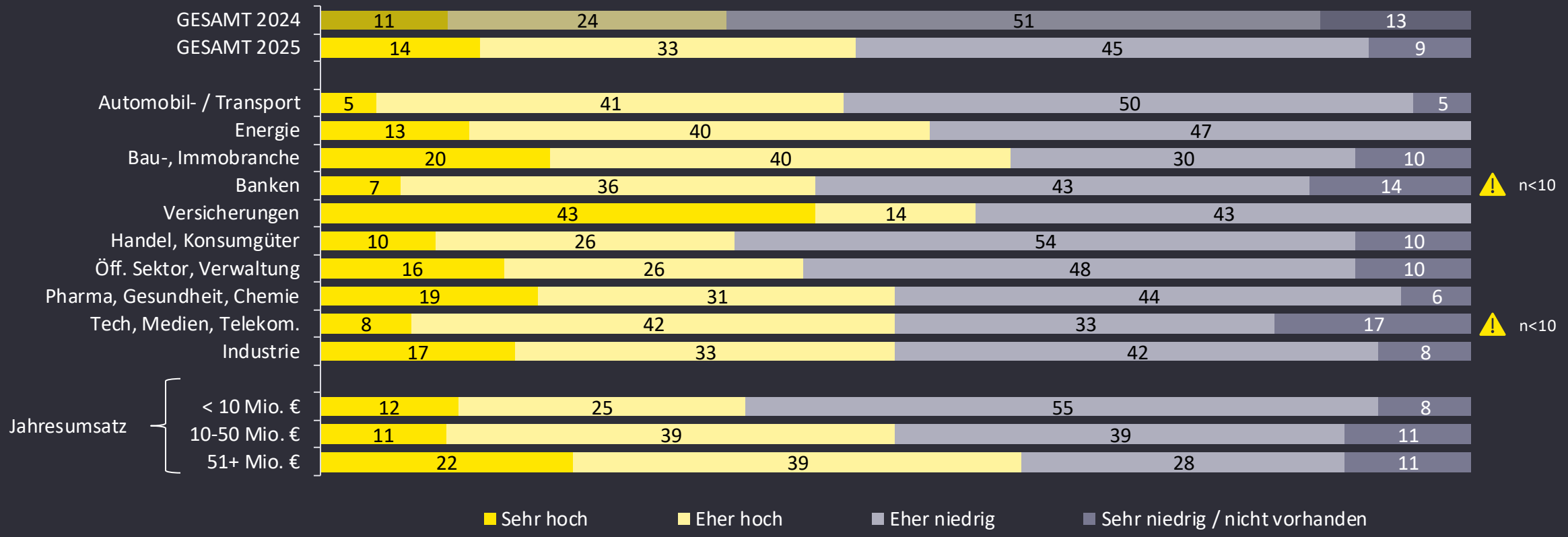


Detailergebnisse

Einschätzung des Risikos von Cyberangriffen

100% (n=200)

Frage 1: Wie hoch schätzen Sie das Risiko für Ihr Unternehmen ein, Opfer von Cyberangriffen/Datendiebstahl zu werden? (Einfachantwort)
Werte in %

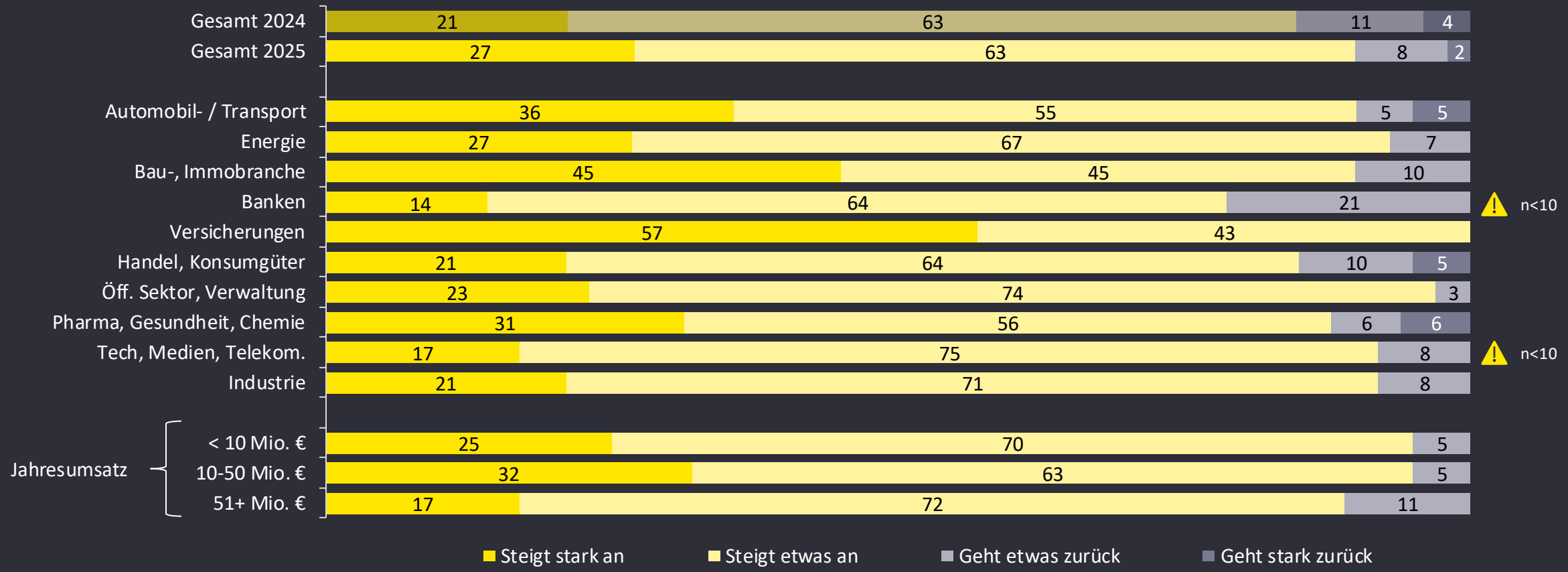


- Im Jahresvergleich hat die subjektive Einschätzung des Risikos von Cyberangriffen deutlich zugenommen: 47% halten das Risiko für sehr oder eher hoch (2024: 35%).
- Unternehmen mit Jahresumsatz über 51 Mio. Euro liegen wie auch 2024 deutlich über dem Schnitt, außerdem zeigen sich Branchenunterschiede.

Einschätzung über die Entwicklung von Cyberangriffen und Datenklau

100% (n=200)

Frage 2: Wie wird sich die Bedeutung des Problems „Cyberangriffe/Datenklau“ künftig für Ihr Unternehmen entwickeln? (Einfachantwort)
Werte in %



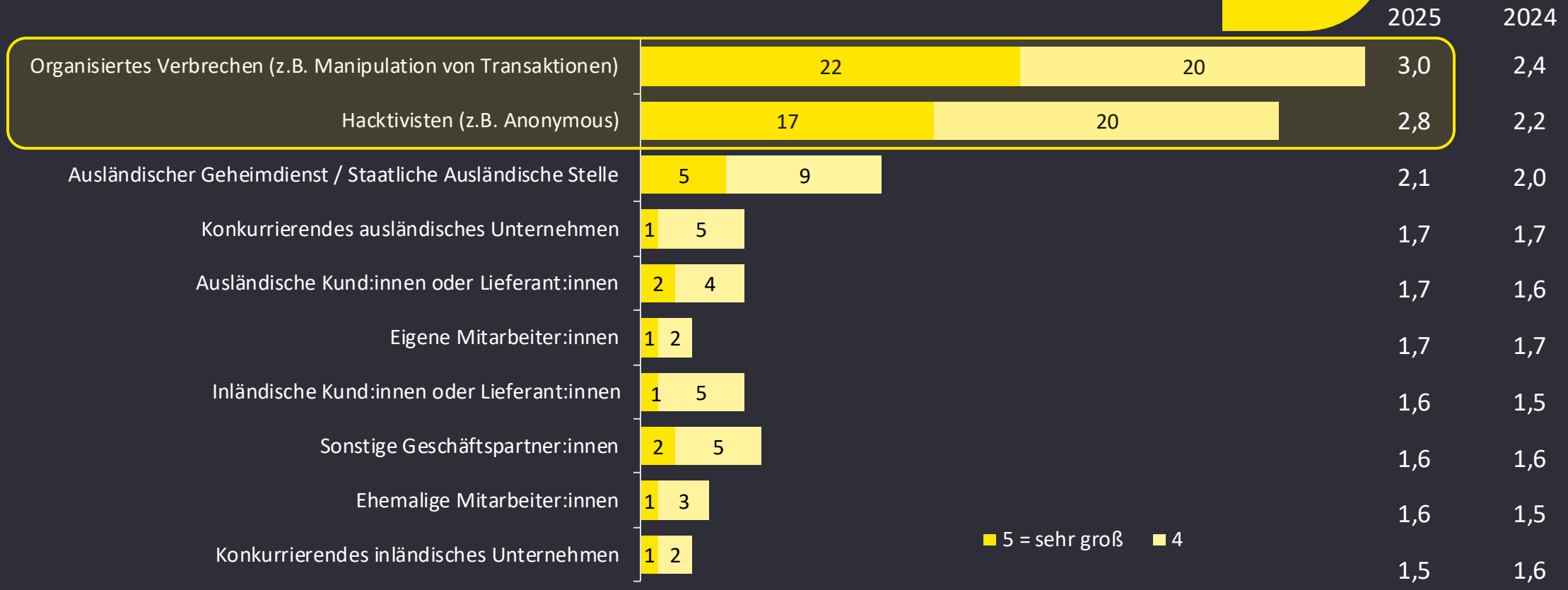
- Wie auch im Vorjahr erwartet der Großteil der Befragten, dass Cyberangriffe künftig noch problematischer werden.
- Ein gutes Viertel spricht von einem sehr starken Anstieg, weitere 63% von einem moderaten.

Risikoeinschätzung unterschiedlicher Tätergruppen

Frage 3: Wie bewerten Sie das Risiko für Ihr Unternehmen, von folgenden „Tätergruppen“ geschädigt zu werden?
(Skalenfrage: 1 = sehr gering; 5 =sehr groß)
Werte in %

MA-Anzahl
2,8 bis 49 MA
3,0 50-99 MA
3,3 100+ MA

100% (n=200)

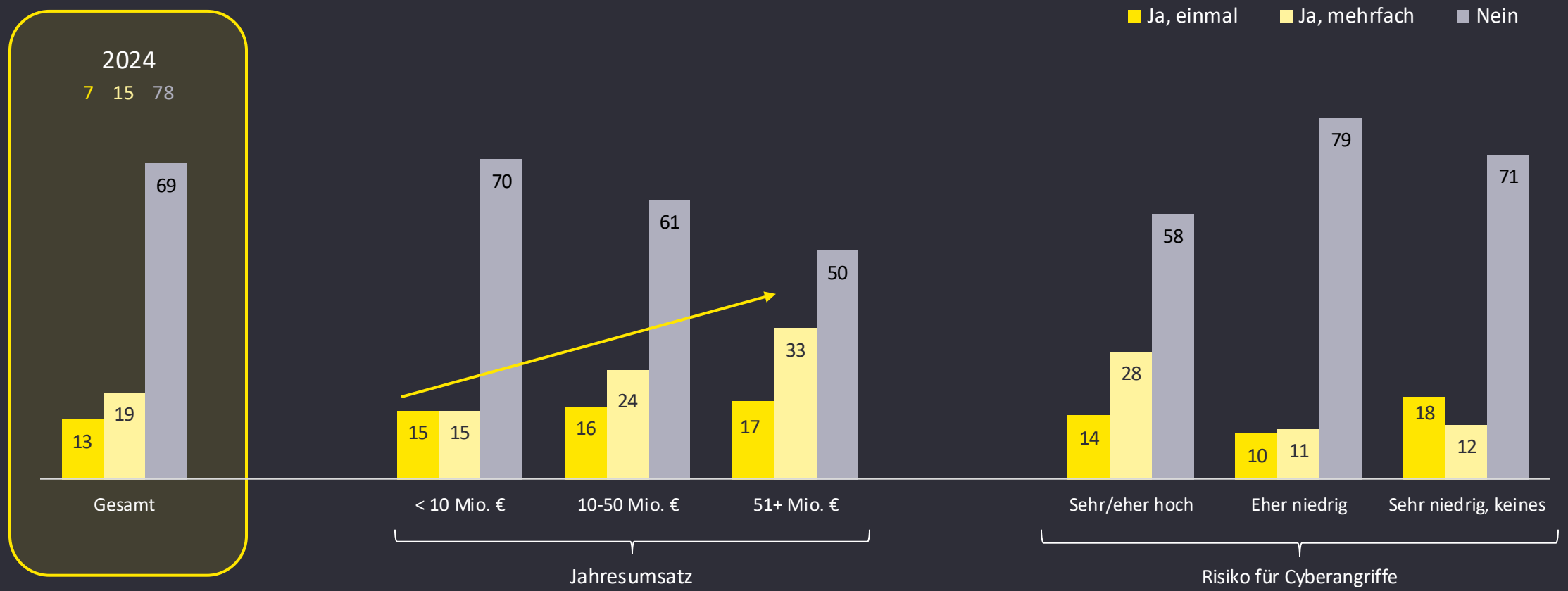


- Die Gefahr, einem organisierten Verbrechen zum Opfer zu fallen, wird von den Befragten erneut am höchsten eingeschätzt, gefolgt von Hacker-Angriffen.
- Diese beiden Gefahren haben im Zeitvergleich auch sehr deutlich zugenommen.

Konkrete Hinweise auf Netzwerk- / Datenangriffe innerhalb der letzten 5 Jahre

100% (n=200)

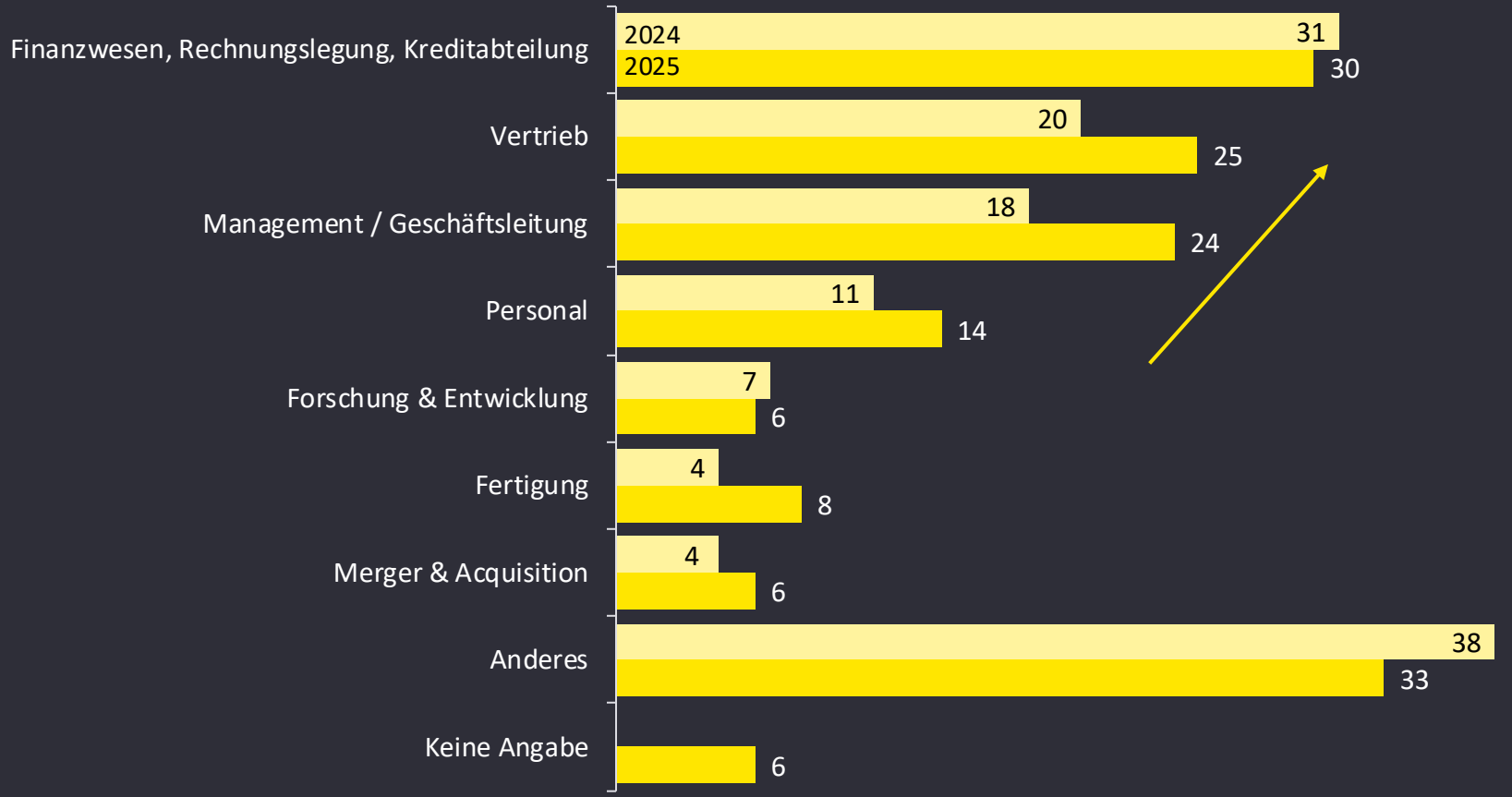
Frage 4: Gab es in Ihrem Unternehmen innerhalb der vergangenen 5 Jahre bereits konkrete Hinweise auf Angriffe auf Ihre Netzwerke und Daten? (Einfachantwort)
Werte in %

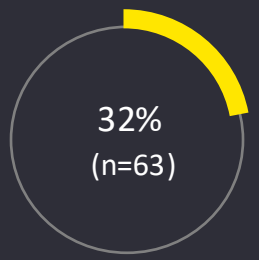


- Rund 70% der befragten Unternehmen hatte in den vergangenen 5 Jahren nicht mit Datenangriffen zu tun, 32% schon, ein Plus von 10 %-Punkten im Vergleich zu 2024.
- Mit dem Umsatz steigt die Wahrscheinlichkeit: ein Drittel der Unternehmen ab 51 Mio. Euro Umsatz haben sogar mehrfach Angriffe erlebt. Dieser Unterschied wurde bereits 2024 deutlich.

Bereiche, die von Datenklau bzw. Verdacht auf Datenklau betroffen waren

Frage 5: Welcher Bereich/welche Bereiche war/en von dem Datenklau betroffen bzw. wo ergab sich dieser Verdacht? (Mehrfachantwort)
Werte in %
Werte 2024
Werte 2025

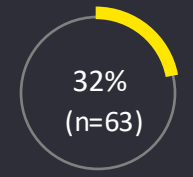




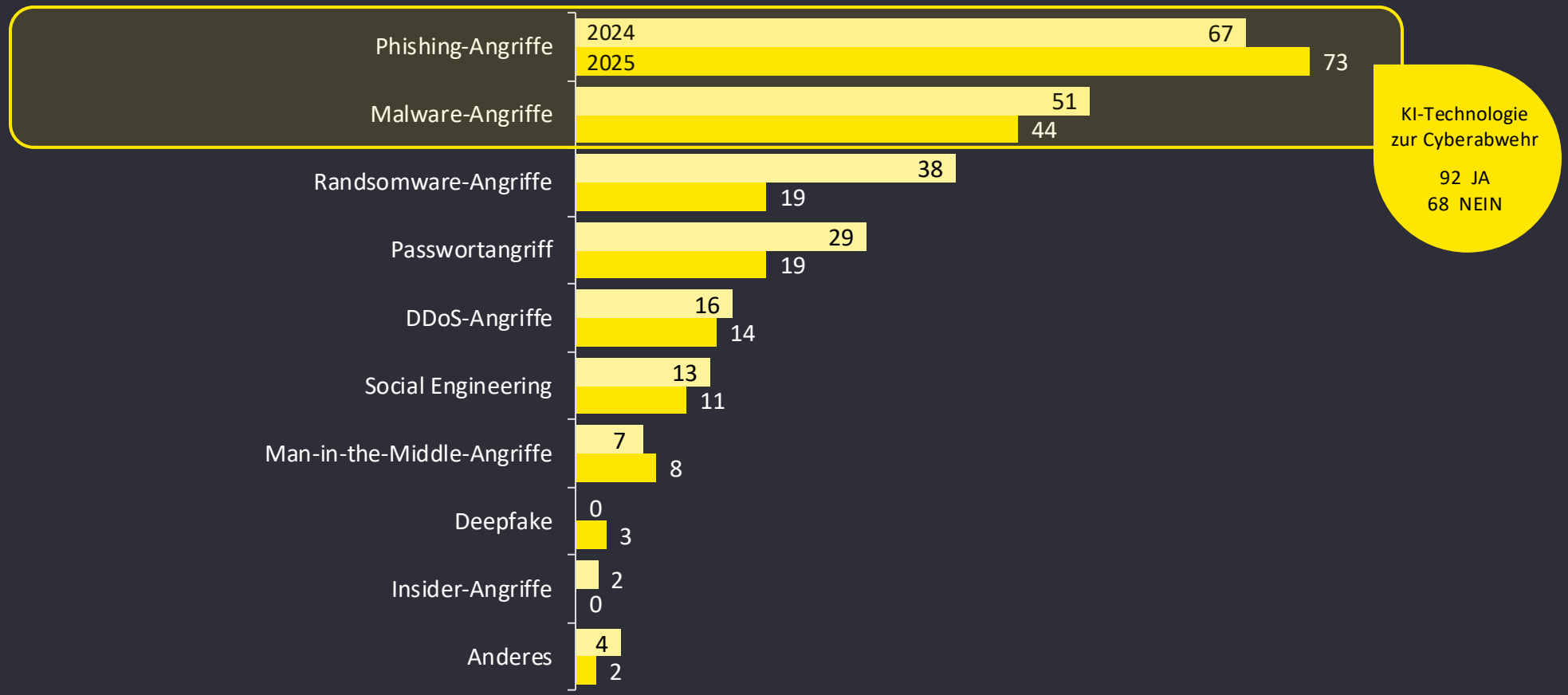
Befragte, deren Unternehmen von Netzwerk-/Datenangriffen betroffen war

➢ Während Angriffe und Datenklau in Finanz- und Kreditabteilungen stabil bleiben, nehmen jene im Vertrieb, auf höherer Managementebene und im Personalbereich zu.

Art der Angriffe

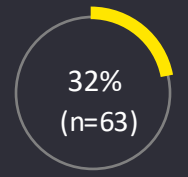


Frage 6: Von welchen Cyberangriffen war Ihr Unternehmen in der Vergangenheit betroffen? (Mehrfachantwort)
Werte in %
Werte 2024
Werte 2025

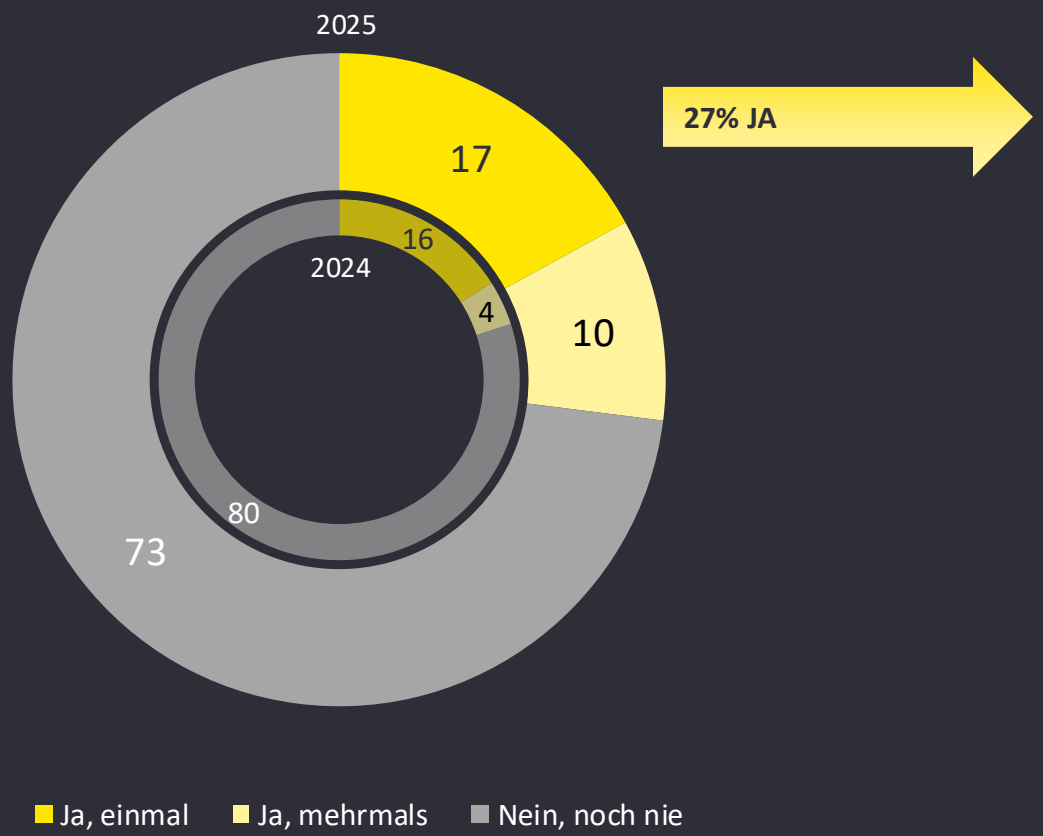


- Rund 3 von 4 Cyberangriffen, von denen die Befragten berichten, sind Phishing-Angriffe, Tendenz steigend.
- Randsomewareangriffe sind im Vergleich zum Vorjahr deutlich zurückgegangen, Malware- und Passwortangriffe ebenso, aber weniger stark.

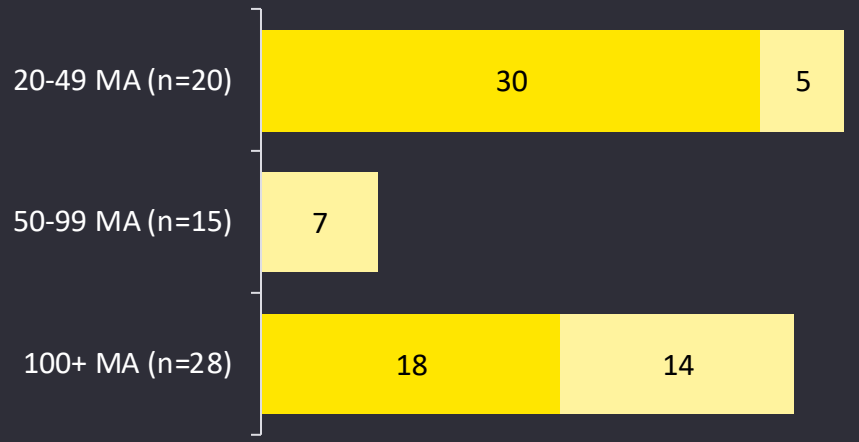
Erpressungsversuche, bei denen Geld gefordert wurde



Frage 7: Gab es jemals Erpressungsversuche gegenüber Ihrem Unternehmen im Zusammenhang mit Angriffen, bei denen Geld gefordert wurde? (Einfachantwort)
Werte in %



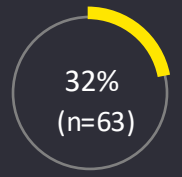
27% JA



Frage 8: Haben Sie gezahlt und wieviel? (Einfachantwort)
n=17 Befragte, von deren Unternehmen Geld gefordert wurde

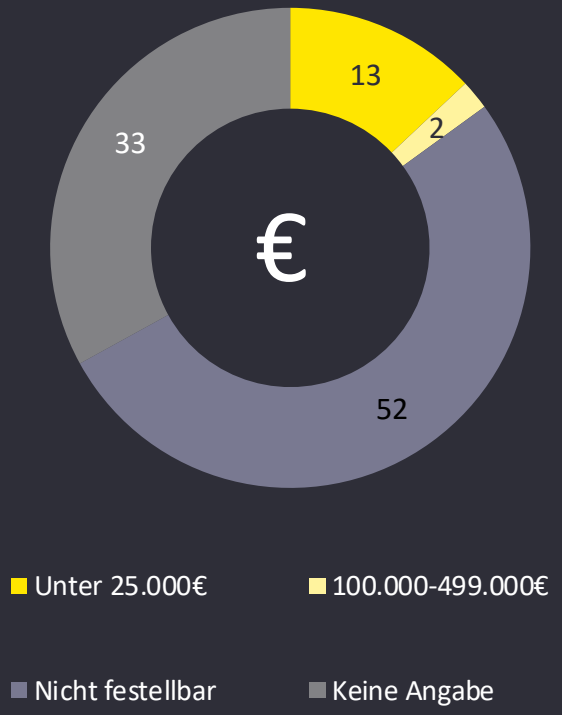
Keines der 17 Unternehmen, die von Erpressungsversuchen betroffen waren, hat gezahlt. 2024 wurde ebenfalls nie gezahlt.

Schadenshöhe und Aufdeckung der kriminellen Handlung

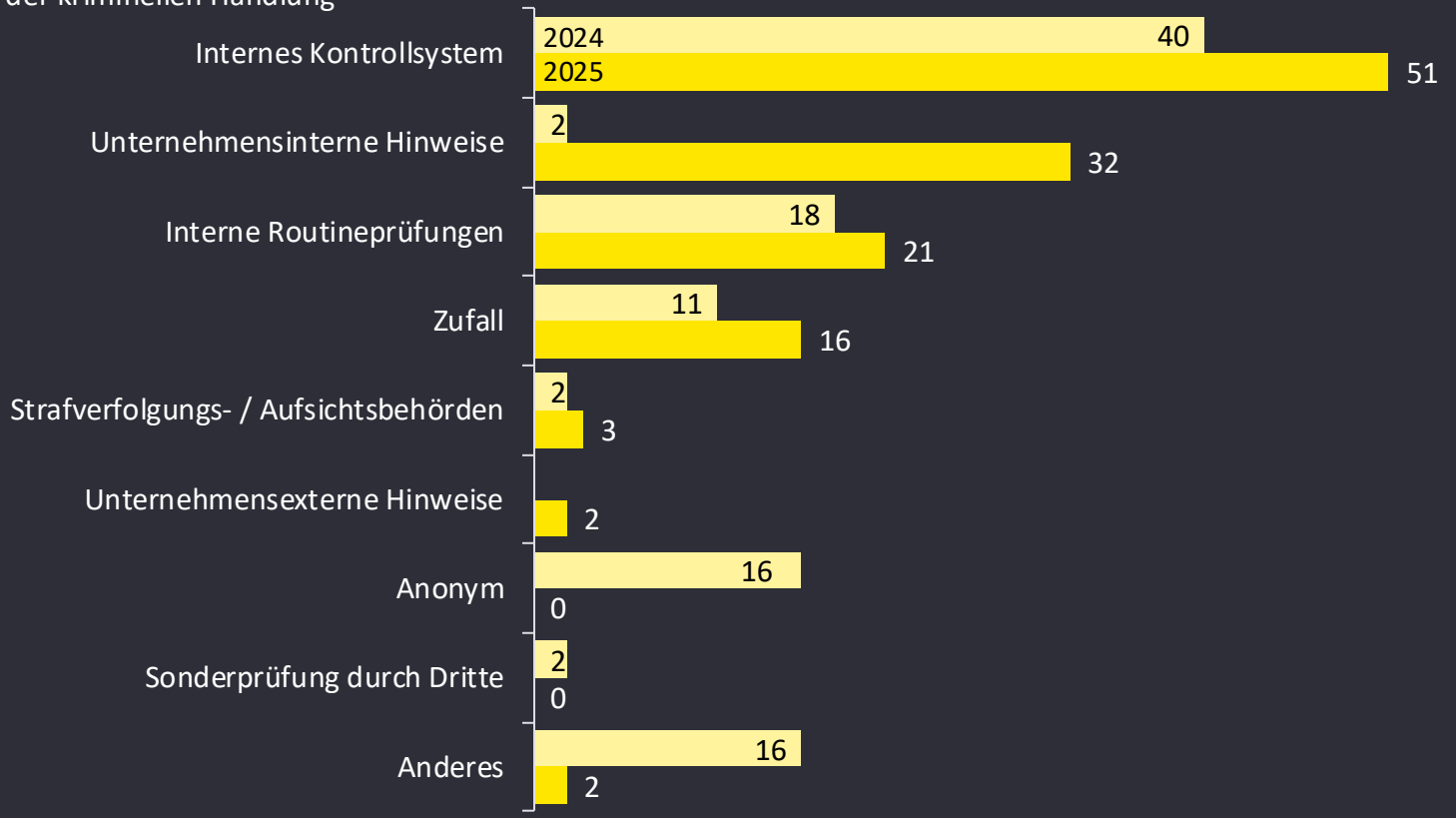


Frage 9: Wie hoch war ungefähr der durchschnittliche Schaden pro Datendiebstahl? (Einfachantwort)
Frage 10: Wie wurden die kriminellen Handlungen aufgedeckt? (Mehrfachantwort)
Werte in %

Schadenshöhe

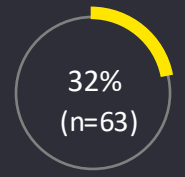


Aufdeckung der kriminellen Handlung

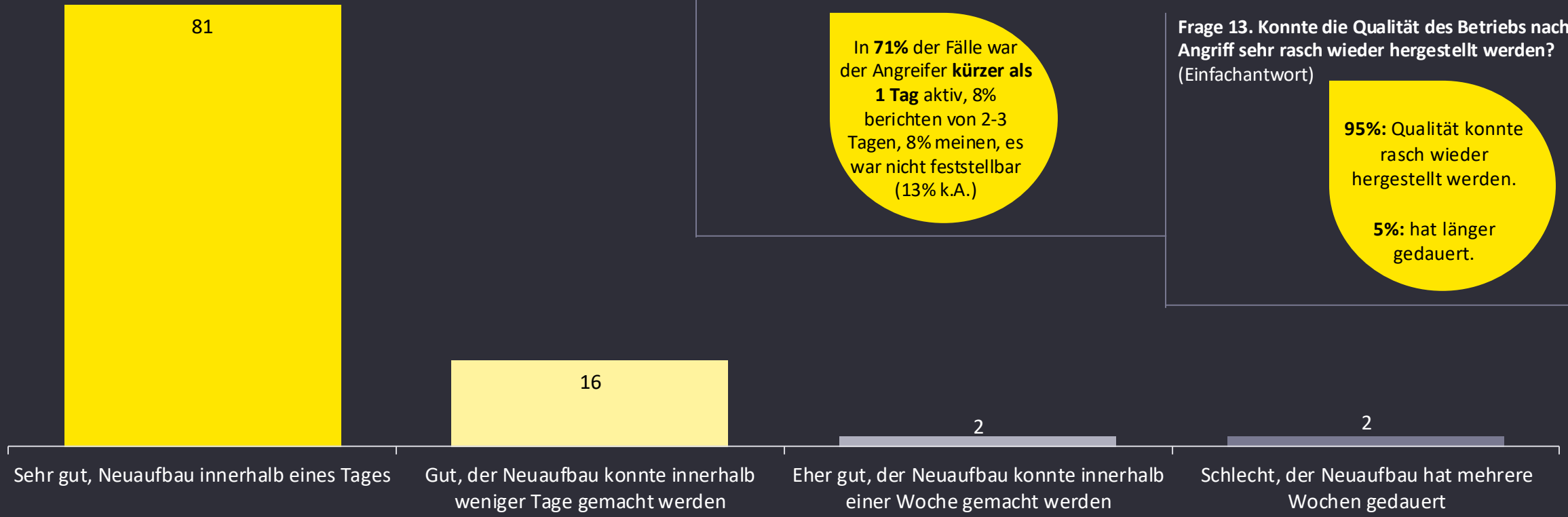


- In 13% der Fälle belief sich der Schaden auf unter 25.000 Euro, bei 2% der Datendiebstähle auf einen höheren Betrag.
- Die Hälfte der Angriffe konnten von unternehmensinternen Kontrollsystemen aufgedeckt werden, ein Drittel dank unternehmensinterner Hinweise.
- Aufgrund der geringen Fallzahl ist ein Vergleich mit 2024 nicht sinnvoll.

Verlauf der Wiederherstellung & Dauer des Angriffs



Frage 12: Wie ist die Wiederherstellung des Betriebs und der Sicherheit nach dem Angriff gelaufen? (Einfachantwort)
Werte in %



Frage 11: Wie lange war der Angreifer aktiv, bevor der Angriff erkannt wurde? (Einfachantwort)

In **71%** der Fälle war der Angreifer **kürzer als 1 Tag** aktiv, 8% berichten von 2-3 Tagen, 8% meinen, es war nicht feststellbar (13% k.A.)

Frage 13. Konnte die Qualität des Betriebs nach dem Angriff sehr rasch wieder hergestellt werden? (Einfachantwort)

95%: Qualität konnte rasch wieder hergestellt werden.

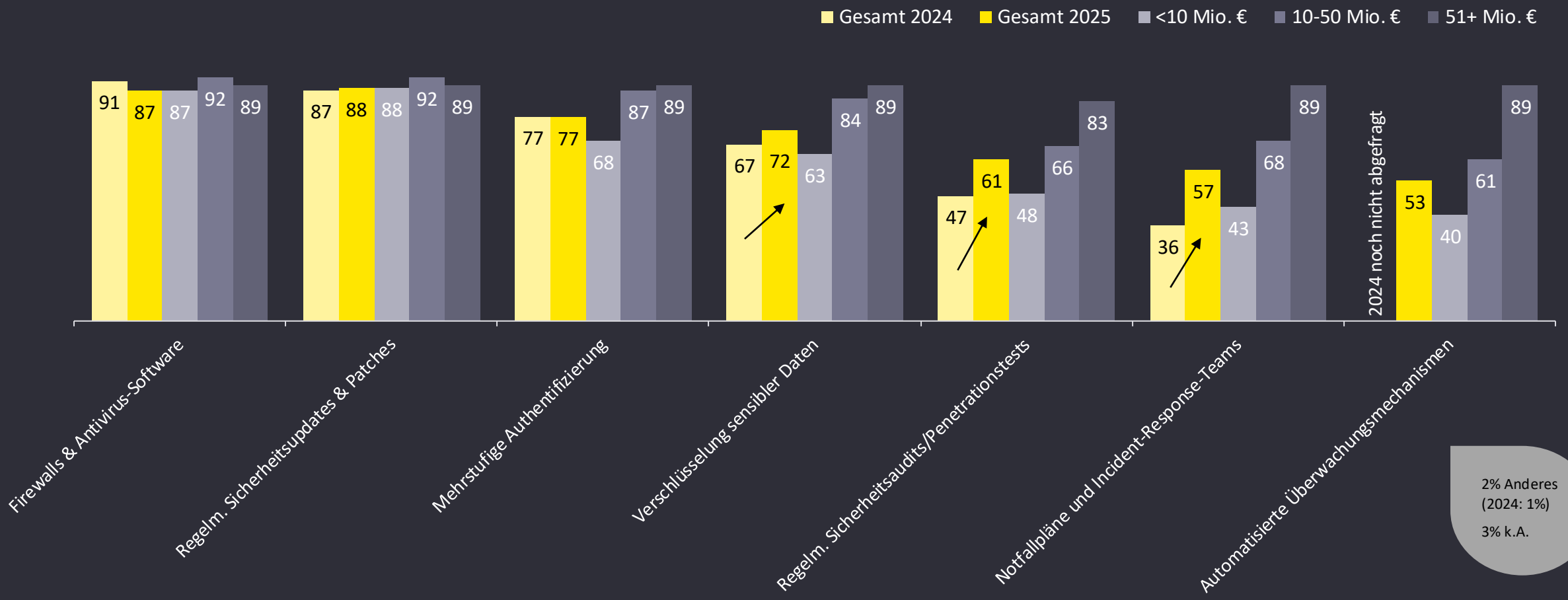
5%: hat länger gedauert.

- In 8 von 10 Fällen verlief die Wiederherstellung nach dem Cyberangriff sehr gut, der Neuaufbau konnte innerhalb eines Tages abgeschlossen werden.
- Auch die Wiederherstellung der Qualität lief in 95% der Fälle rasch und unkompliziert.
- Rund 70% geben an, dass der Angriff kürzer als einen Tag aktiv war.

Sicherheitsmaßnahmen gegen Cyberangriffe

100% (n=200)

Frage 14: Welche Sicherheitsmaßnahmen setzt Ihr Unternehmen ein, um sich vor Cyberangriffen zu schützen? (Mehrfachantwort)
Werte in %



2% Anderes (2024: 1%)

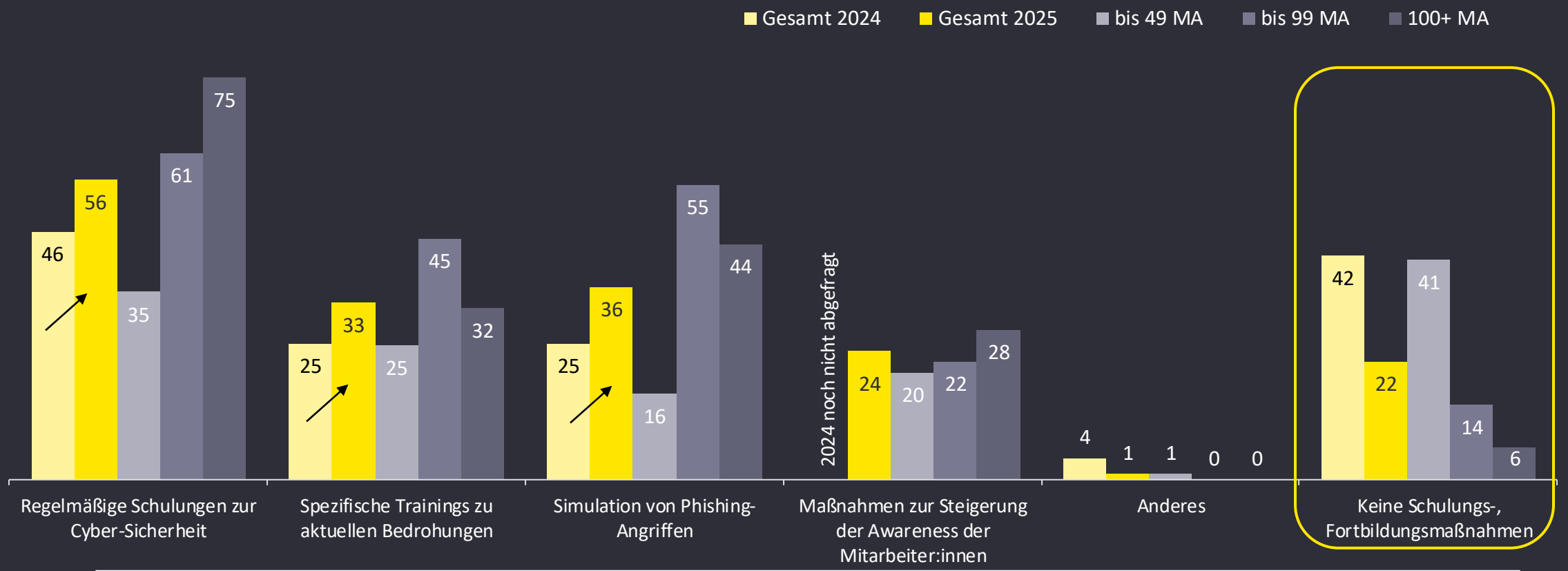
3% k.A.

- Der Einsatz der Verschlüsselung sensibler Daten, regelmäßige Sicherheitsaudits und Notfallpläne hat im Vorjahresvergleich etwas bzw. deutlich zugenommen, mit Umsatzstärke der Unternehmen nimmt der Einsatz dieser Sicherheitsmaßnahmen deutlich zu.
- Am prominentesten bleiben Firewalls & Antivirus-Software, regelmäßige Sicherheitsupdates und die Verwendung mehrstufiger Authentifizierung.

Schulungs- und Fortbildungsmaßnahmen für Mitarbeitende

100% (n=200)

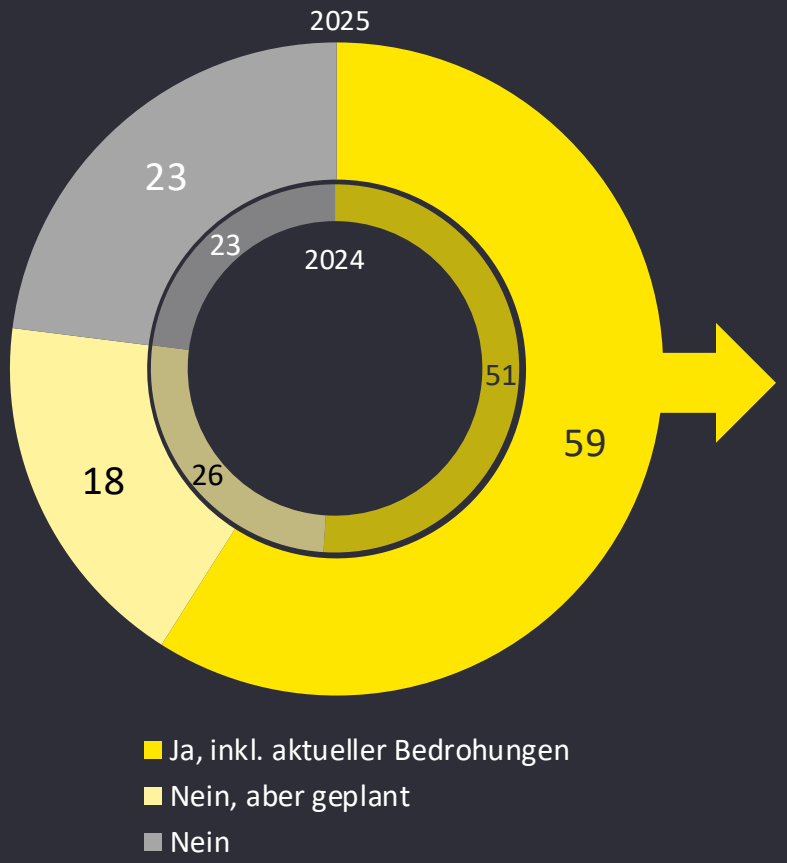
Frage 15: Welche Schulungs- und Fortbildungsmaßnahmen hinsichtlich der Awareness/Aufmerksamkeit und Achtsamkeit für Cybersecurity bieten Sie Ihren Mitarbeiter:innen an (egal, ob extern oder intern)? (Mehrfachantwort)
Werte in %

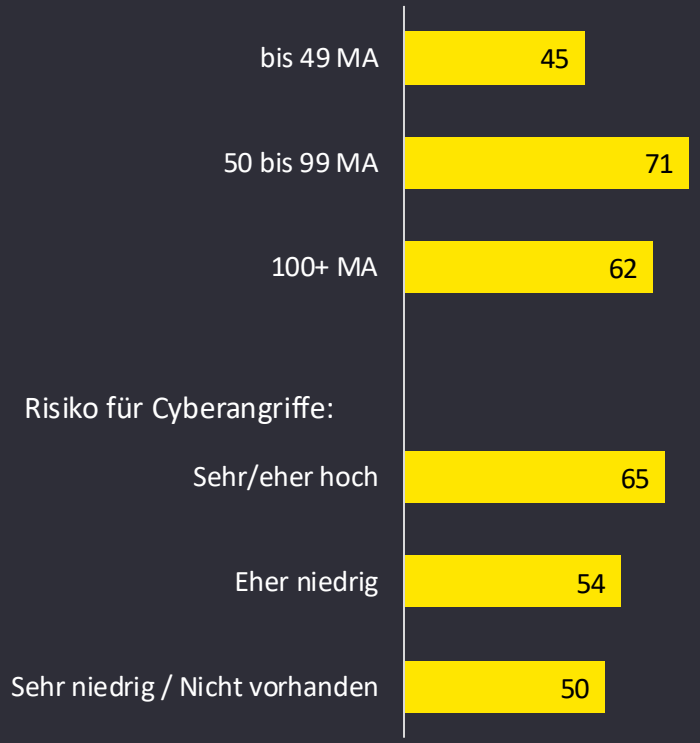


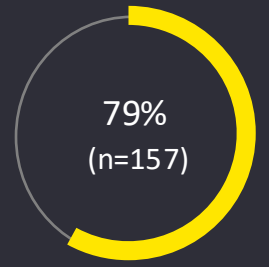
- Während 2024 noch 42% keine Schulungs- bzw. Fortbildungsmaßnahmen angeboten haben, sind es heute nur noch 22% der Unternehmen.
- Hauptsächlich werden allgemeine Schulungen zum Thema Cybersicherheit angeboten (56%), ein Drittel berichtet auch von spezifischen Trainings, 36% von Simulationen von Phishing-Angriffen.

Aktuelle Bedrohungen als Inhalt von Cybersecurity-Schulungen

Frage 16: Beinhalten diese Schulungen auch aktuelle Bedrohungen wie zum Beispiel Deep-Fakes, Umgang mit KI-Bedrohungen oder ähnliches? (Einfachantwort)
Werte in %







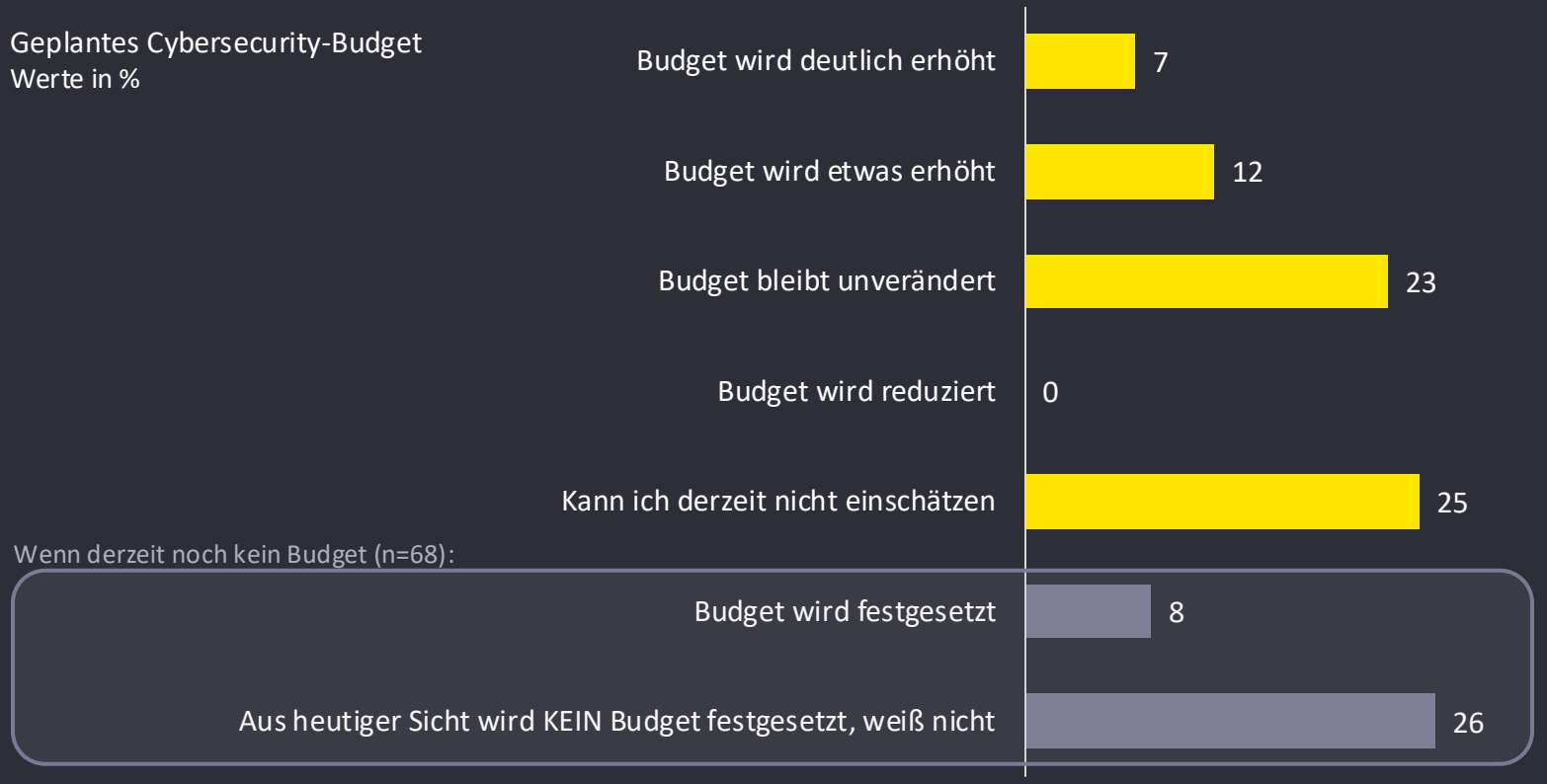
Befragte, die ihren MA Fortbildungsmaßnahmen hinsichtlich der Awareness/ Aufmerksamkeit/ Achtsamkeit anbieten

- In 6 von 10 Unternehmen, die Fortbildungsmaßnahmen im Bereich Cybersecurity für Mitarbeitende anbieten, werden (auch) aktuelle Bedrohungen im Rahmen der Schulungen behandelt.
- Unternehmen mit 50 bis 99 Mitarbeitenden liegen über dem Schnitt, außerdem jene, die das Risiko von Cyberangriffen höher einschätzen.

Budget für Cybersecurity und Budget-Planung

100% (n=200)

Frage 17: Wie viel Budget hat Ihr Unternehmen für Cybersecurity pro Jahr? (Einfachantwort)
Frage 19: Planen Sie Ihr Budget (…) in den nächsten 2 Jahren zu erhöhen bzw. ein Cybersecurity-Budget festzusetzen? (Einfachantwort)



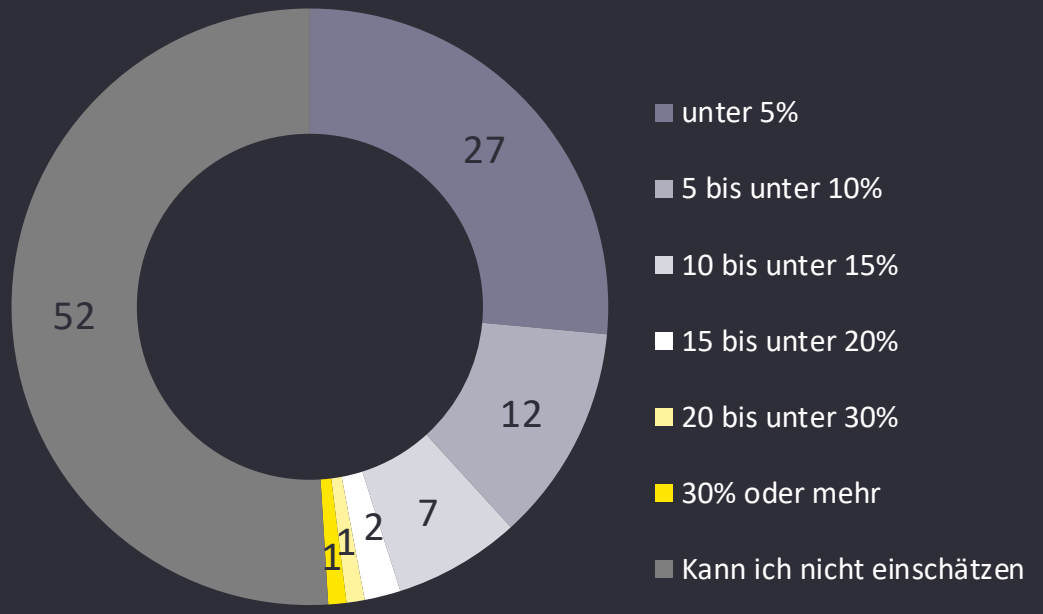
- Das Budget für Cybersecurity fällt im Vergleich zum Vorjahr deutlich geringer aus: ein Drittel gibt an, KEIN Budget zu haben. Das Vorjahres-Ergebnis, nach dem nur 1% der Unternehmen KEIN Budget haben, scheint rückblickend fragwürdig. Diese dürften „unter 25Tsd“ angegeben haben. Es scheint nun das Wissen und die Fähigkeit, dies abzuschätzen, gestiegen zu sein.
- 9% haben ein Budget von über 25.000 Euro (14% 2024), 16% unter 25.000 Euro (36% 2024).
- Ein Fünftel gibt an, das Budget werde in den nächsten 2 Jahren erhöht, in 23% der Unternehmen soll es unverändert bleiben.

Anteil IT-Budget am Gesamtbudget & Häufigkeit der Tests auf Schwachstellen

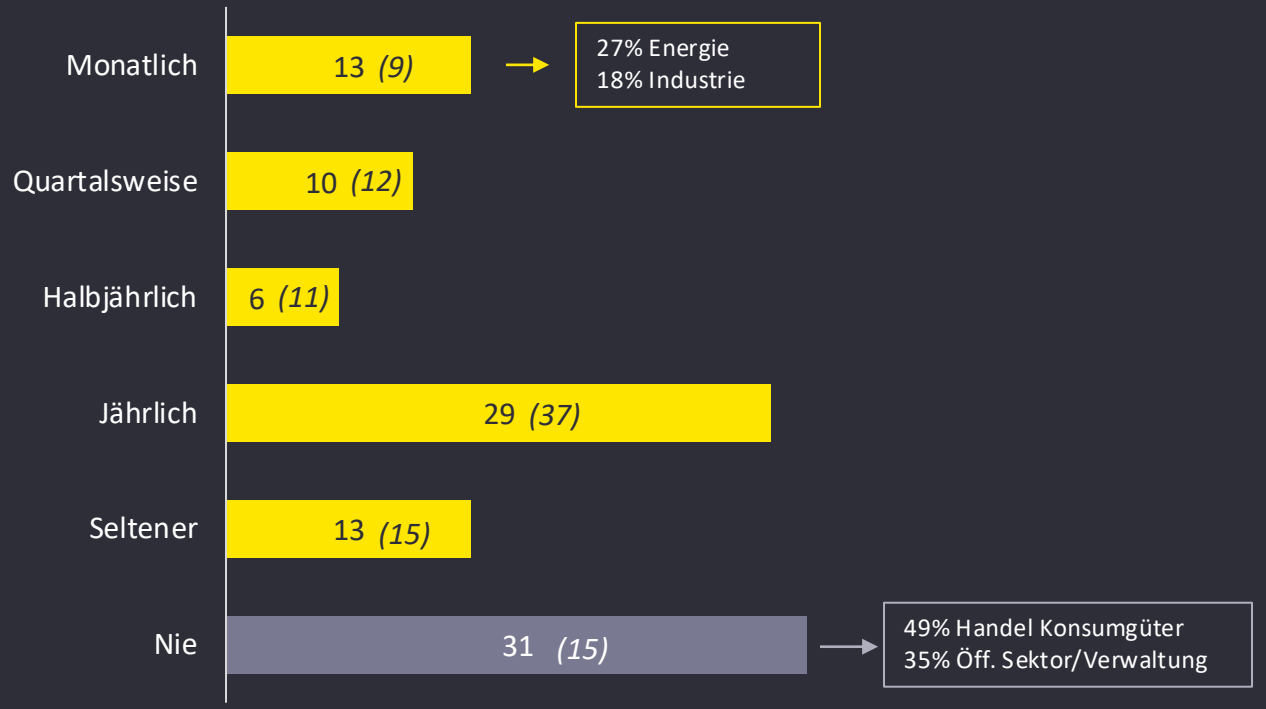
100% (n=200)

Frage 18. Können Sie ungefähr einschätzen, welcher Anteil am Gesamtbudgets Ihres Unternehmens auf den gesamten IT-Bereich (Hardware, Software, externe Dienstleister) entfällt? (Einfachantwort)
Frage 20: Lässt sich Ihr Unternehmen regelmäßig (extern und/oder intern) auf Schwachstellen im Hinblick auf Cyberangriffe/Datendiebstahl testen? (Einfachantwort)
Werte in %

Anteil IT-Budget am Gesamtbudget



Häufigkeit der Schwachstellen-Tests
Werte in Klammer = 2024



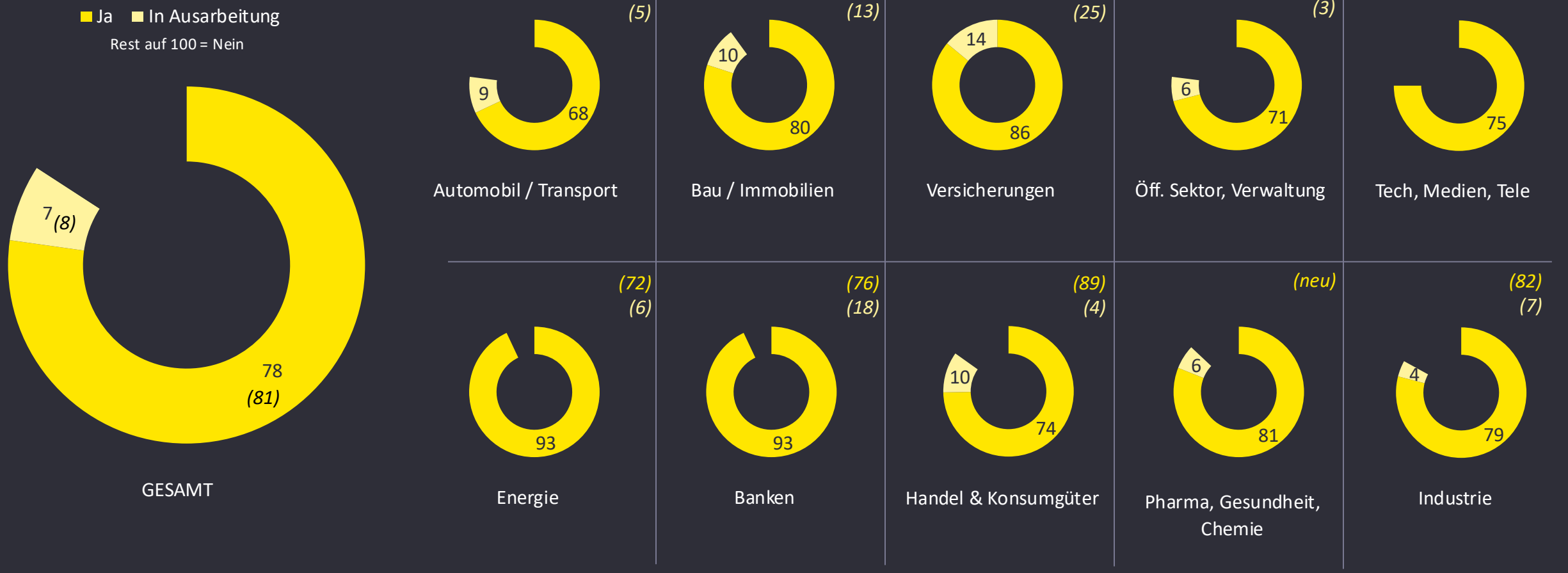
- 3 von 10 Befragten schätzen den Anteil des IT-Budgets vom Gesamtbudget auf unter 10%. Etwas mehr als die Hälfte gibt keine Schätzung ab.
- Monatliche Schwachstellentest sind unter den Befragten etwas verbreiteter als letztes Jahr, ABER: doppelt so viele Unternehmen geben an, nie Schwachstellen-Tests durchzuführen!

Pläne für Wiederherstellung der Infrastruktur nach einem Cyberangriff

– unverändert wie 2024 in 8 von 10 Unternehmen vorhanden

100% (n=200)

Frage 21: Gibt es in Ihrem Unternehmen Pläne für die Wiederherstellung der Infrastruktur nach einem Cyberangriff? (Einfachantwort)
Werte in %
Werte in Klammer = 2024

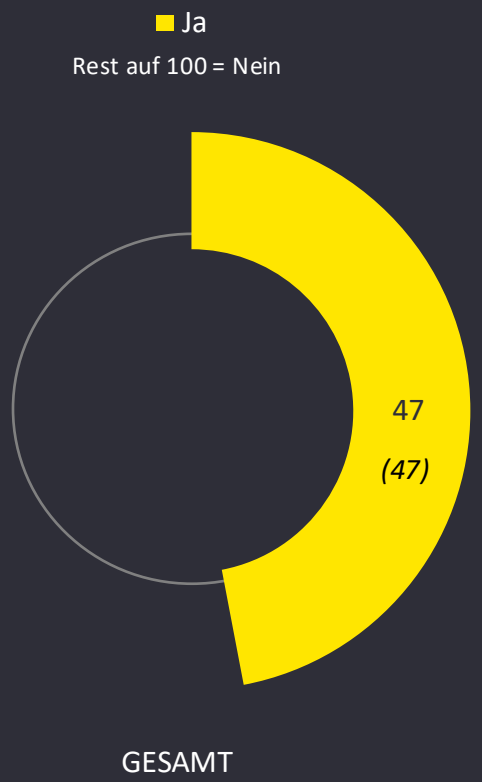


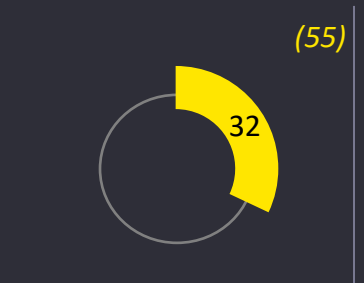
Versicherung gegen digitale Risiken

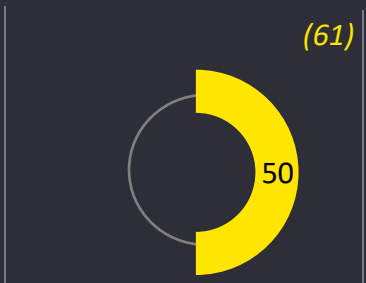
- ebenfalls unverändert wie 2024 in knapp jedem 2. Unternehmen

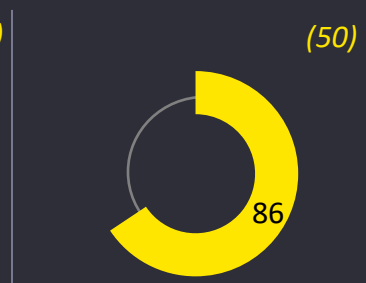
100% (n=200)

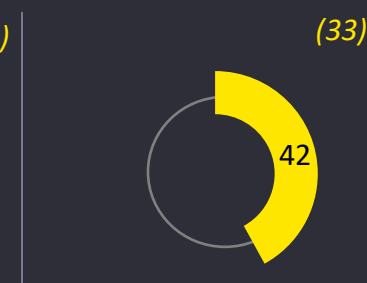
Frage 22: Hat Ihr Unternehmen eine Versicherung gegen digitale Risiken (=Hackerangriffe etc.) abgeschlossen? (Einfachantwort)
Werte in %
Werte in Klammer = 2024

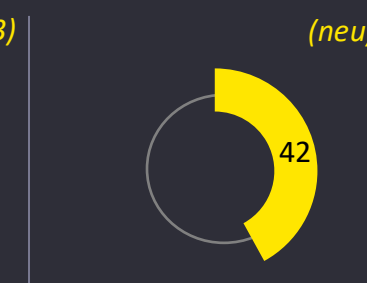


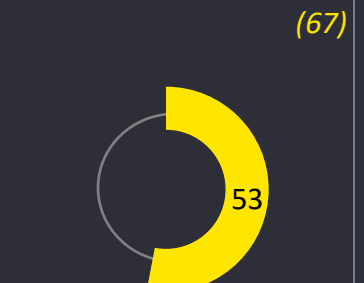


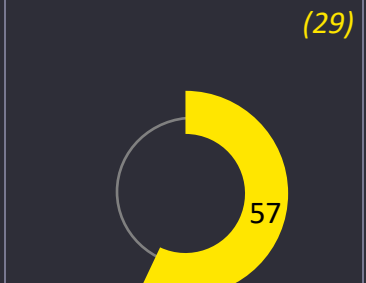


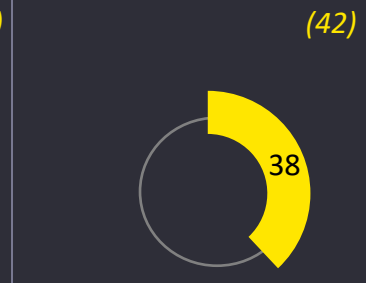


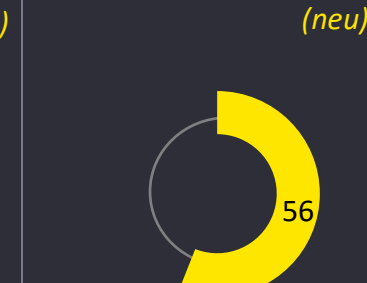


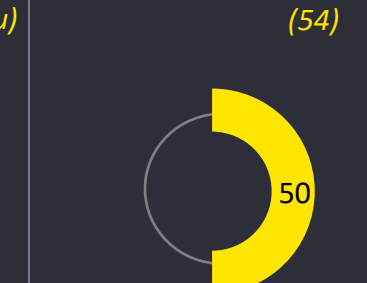








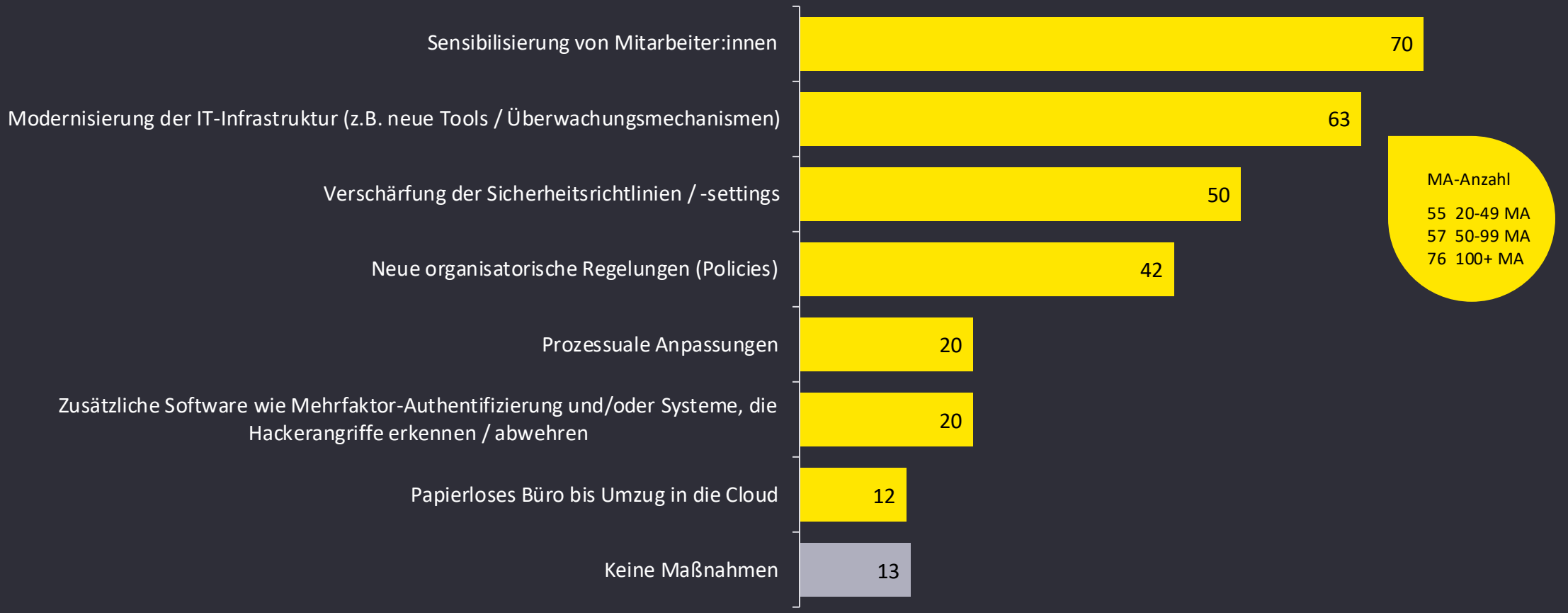




Maßnahmen, die im letzten Jahr umgesetzt wurden

100% (n=200)

Frage 23. Welche der folgenden Maßnahmen wurden in Ihrem Unternehmen im letzten Jahr umgesetzt? (Mehrfachantwort)
Werte in %

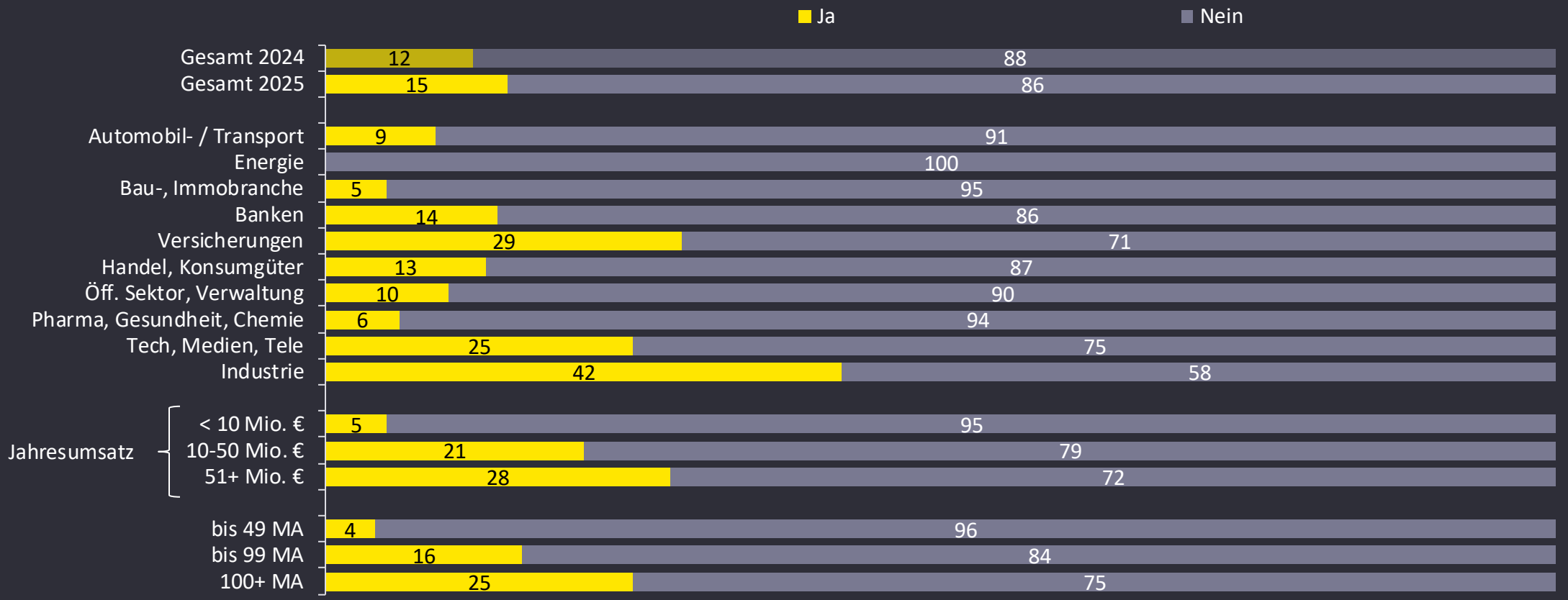


- 7 von 10 Befragten geben an, im letzten Jahr an der Sensibilisierung von Mitarbeiter:innen gearbeitet zu haben.
- 63% haben die IT-Infrastruktur generell modernisiert.
- Nur 13% der Unternehmen haben im letzten Jahr keine Maßnahmen gesetzt.

Einsatz von KI-Technologien im Bereich Cybersicherheit

100% (n=200)

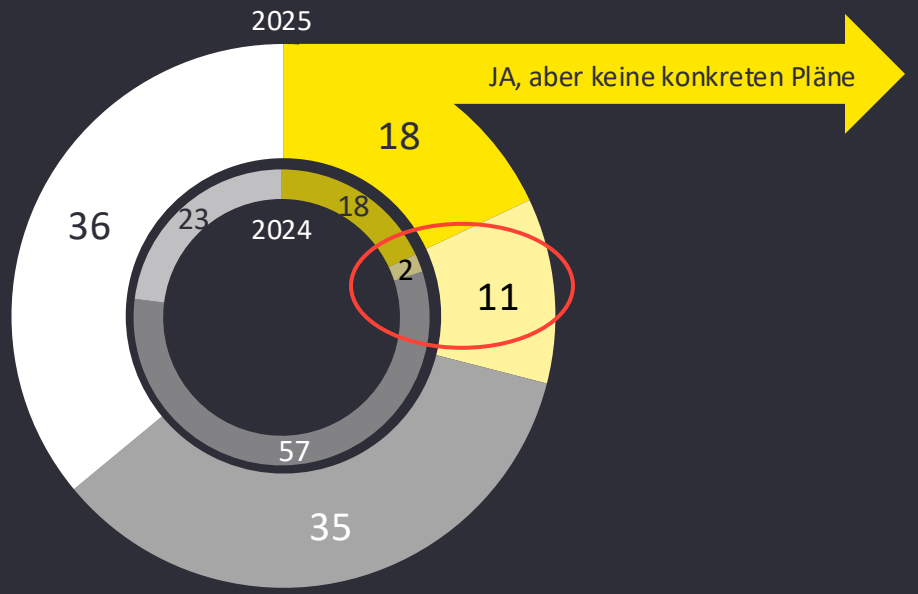
Frage 24: Setzen Sie derzeit KI-Technologien im Bereich Cybersecurity ein? (Einfachantwort)
Werte in %

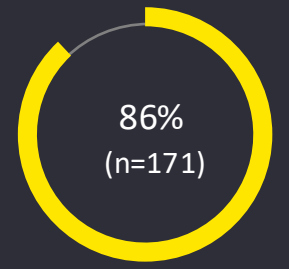


- 15% setzen derzeit KI-Technologien im Cybersicherheitsbereich ein, etwas mehr als im Vorjahr.
- Industrie-Unternehmen, Versicherungen und Unternehmen der Tech-, Medien oder Telekommunikationsbranche eher.
- Größere Unternehmen (in Hinblick auf beides, Umsatz und MA-Anzahl) sind Vorreiter.

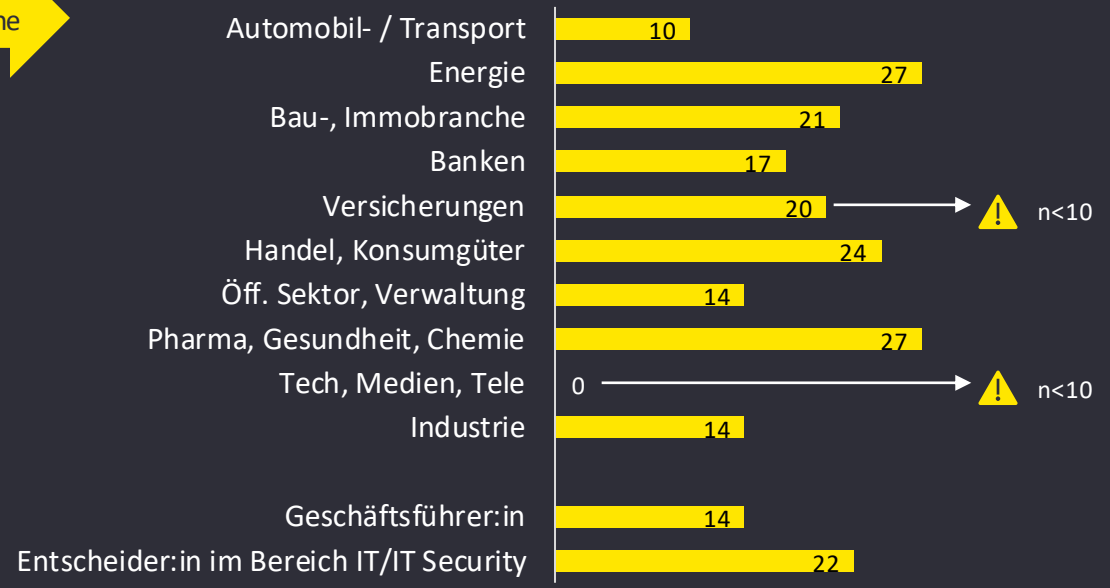
Geplanter Einsatz von KI-Technologien für Cyberabwehr

Frage 25. Planen Sie zukünftig, KI-Technologien für die Cyberabwehr einzusetzen? (Einfachantwort)
Werte in %



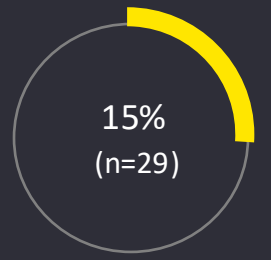


Befragte, die derzeit keine KI für Cyberabwehr einsetzen



- Im Vergleich zum Vorjahr ist die Anzahl an Unternehmen, die bereits konkrete Pläne zum Einsatz von KI-Technologien zur Cyberabwehr haben, um 9%-Punkte gestiegen.
- Interessiert, aber noch planlos, sind weiterhin 18% der Unternehmen, vor allem Jene der Energiebranche, des Handels sowie der Pharma- und Gesundheitsbranche.

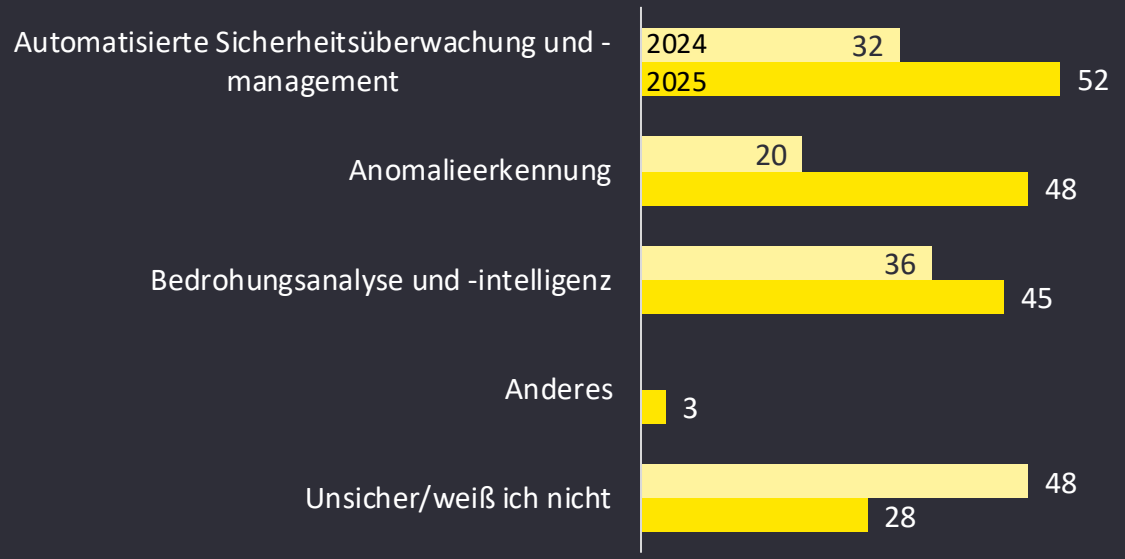
Methoden & Prozesse im Bereich Cybersicherheit, die durch KI-Technologie unterstützt werden und geleisteter Beitrag



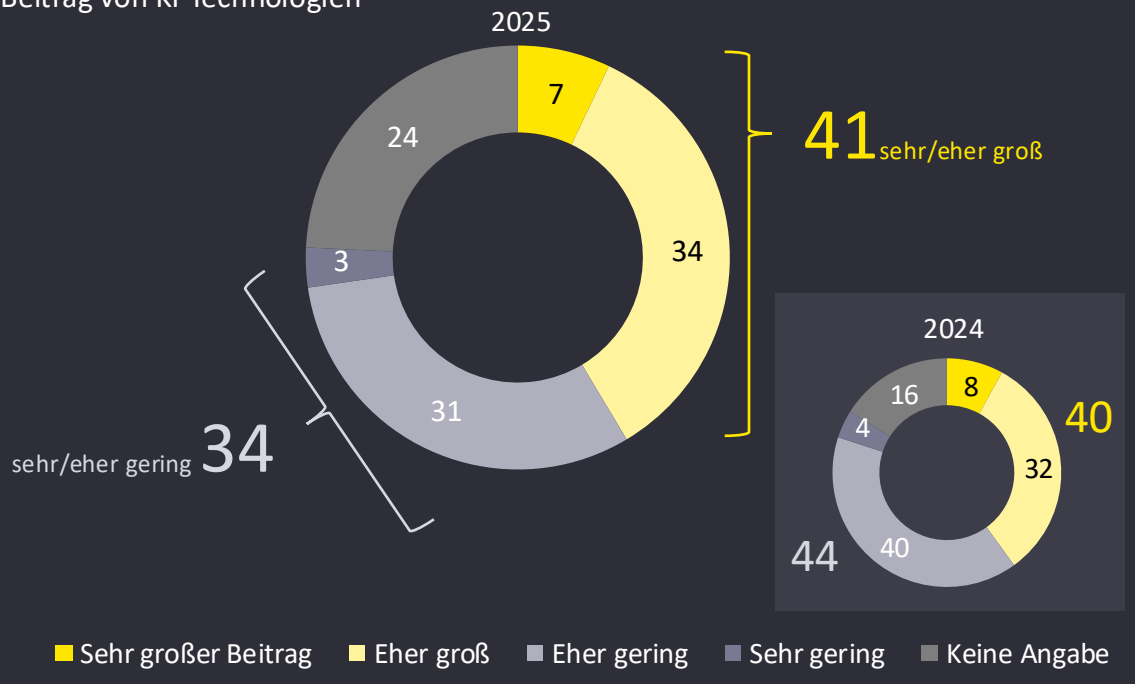
Befragte, die derzeit KI im Bereich Cyberabwehr einsetzen

Frage 26. Welche Methoden oder Prozesse im Bereich Cybersecurity in Ihrem Unternehmen werden durch KI-Technologien unterstützt? (Mehrfachantwort)
Frage 27: Welchen Beitrag leisten KI-Technologien für die Cybersicherheit in Ihrem Unternehmen? (Einfachantwort)
Werte in %
Werte 2024
Werte 2025

Eingesetzte Methoden/Prozesse

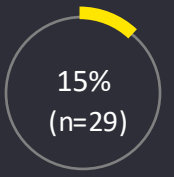


Beitrag von KI-Technologien

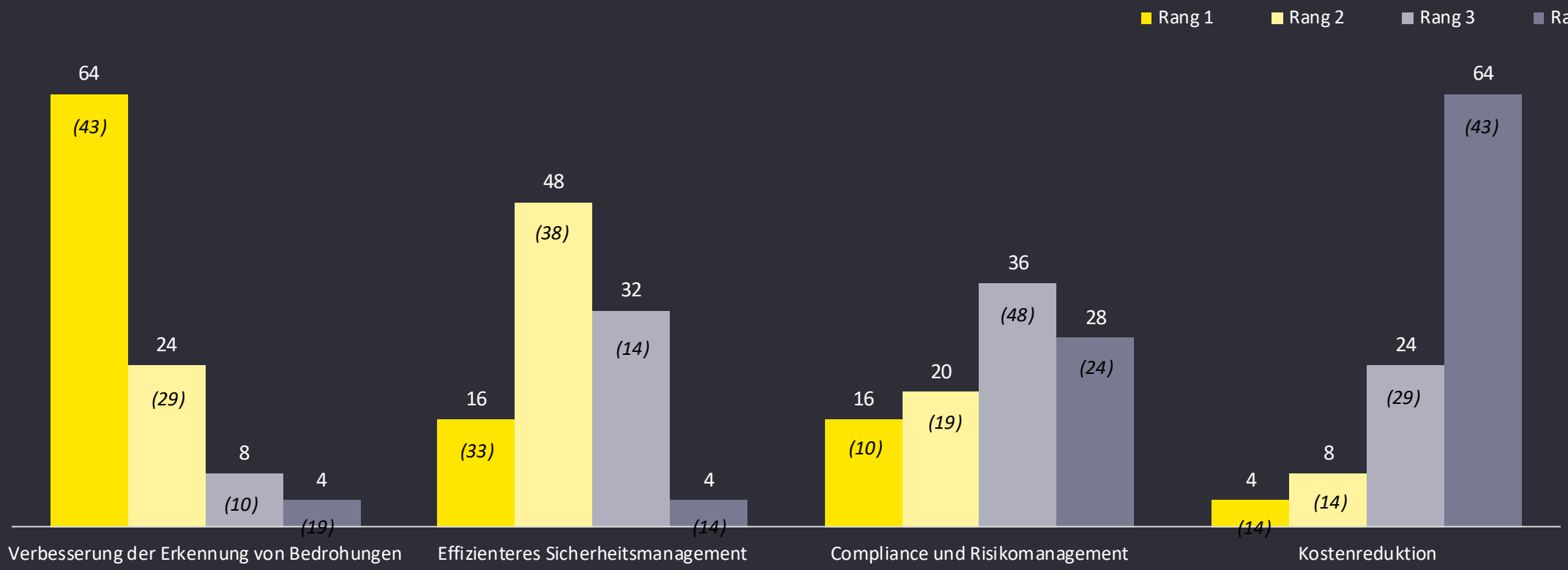


- Jedes zweite Unternehmen, das derzeit bereits KI zur Cyberabwehr einsetzt, tut dies zur automatisierten Sicherheitsüberwachung, Tendenz stark steigend. Auch KI-gestützte Anomalieerkennung und Bedrohungsanalyse und –intelligenz sind dieses Jahr weiter verbreitet.
- Der Einsatz von KI-Technologien zahlt sich laut 41% der Befragten jedenfalls aus.

Ziele, die durch Einsatz von KI verfolgt werden

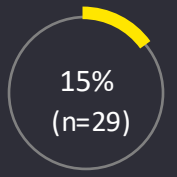


Frage 28: Welche Ziele verfolgen Sie mit dem Einsatz von KI in Ihrer Cybersecurity-Strategie? (Rangreihung)
Werte in %
Werte in Klammer = 2024



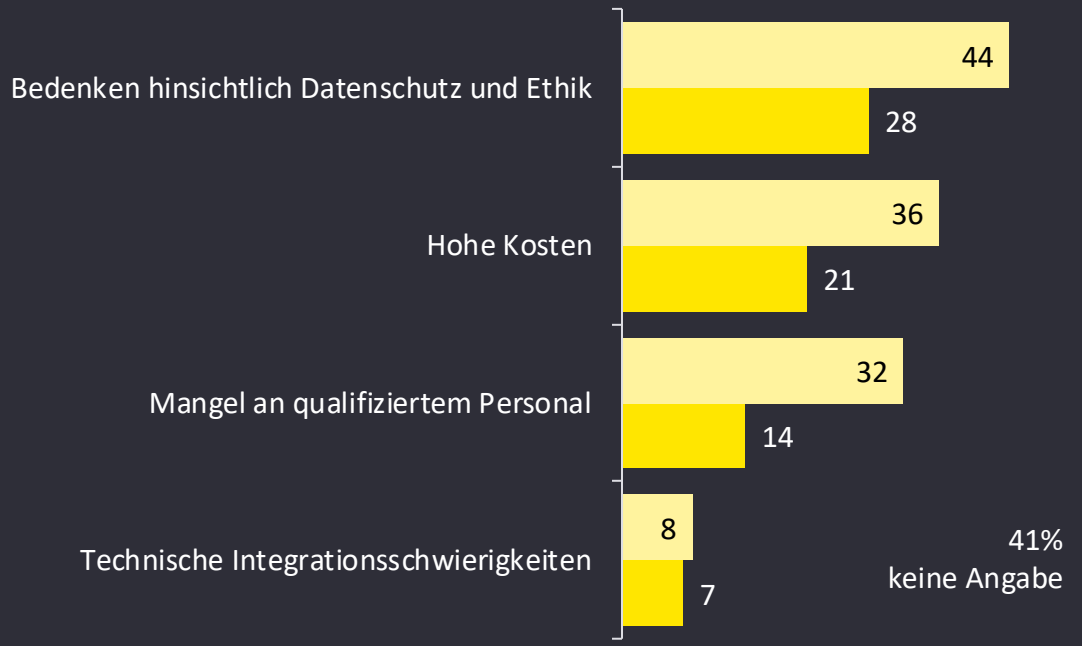
- Bedrohungen besser und schneller zu erkennen, wird von knapp zwei Drittel der Befragten als wichtigsten Ziel genannt und wird heuer deutlich wichtiger eingestuft als die Effizienz im Sicherheitsmanagement.
- Die Reduktion der Kosten durch den Einsatz von KI wird im Vorjahresvergleich weniger wichtig eingestuft und landet auf Platz 4.
- Achtung auf geringe Antwortbasis und daher nur bedingte Vergleichbarkeit der Ergebnisse!

Herausforderungen der Implementierung & Veränderung des KI-Einsatzes

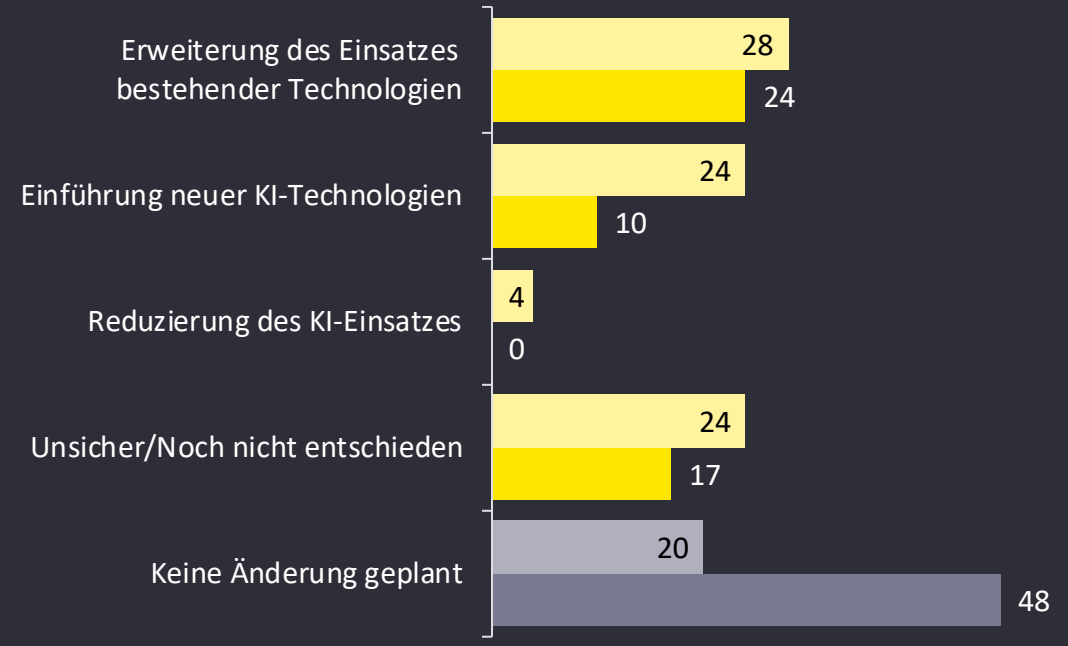


Frage 29: Welche Herausforderungen sind Ihnen bei der Implementierung von KI in der Cybersecurity aufgefallen? (Mehrfachantwort)
Frage 30: Wie planen Sie, Ihren Einsatz von KI in der Cybersecurity in den nächsten 12 Monaten zu verändern? (Mehrfachantwort)
Werte in %
Werte 2024
Werte 2025

Herausforderungen der Implementierung



Geplante Veränderung

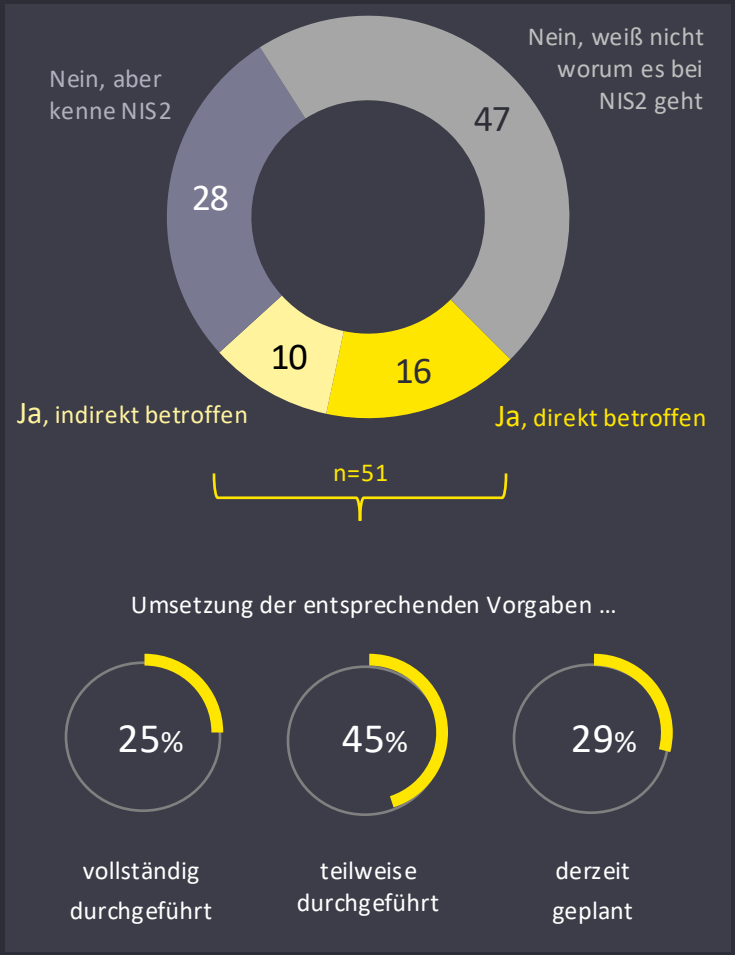


- Bedenken über hohe Kosten fallen geringer aus als jene bezüglich Datenschutz und Ethik, über die technische Integration machen sich die Befragten die wenigsten Sorgen. Insgesamt liegen die Werte deutlich unter den Vorjahresergebnissen.
- Fast die Hälfte hat derzeit keine Änderungen geplant, ein Viertel wird bestehende Technologien erweitern.

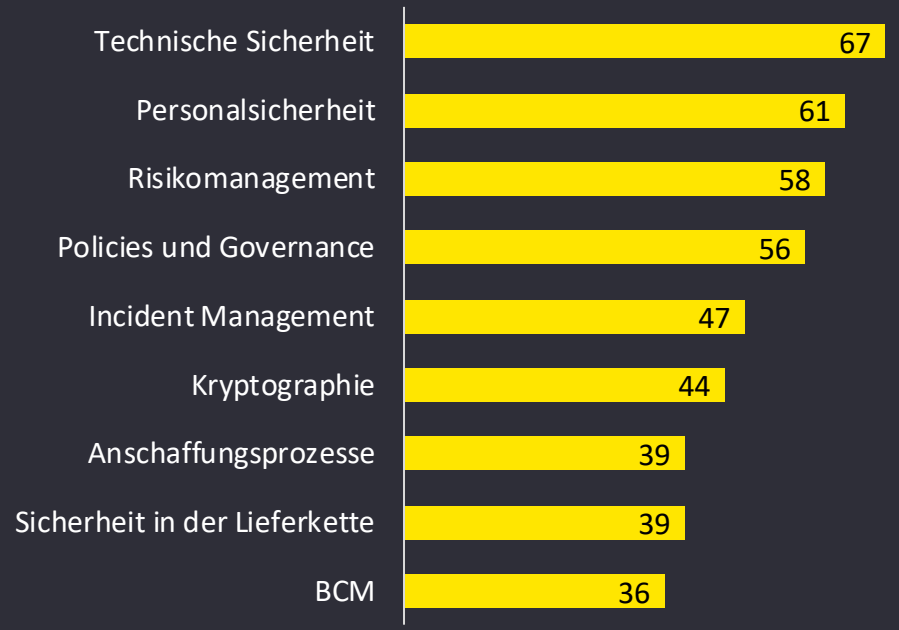
NIS2

100%
(n=200)

Frage 31. Noch kurz 3 Fragen zur Regulatorik im Bereich Cybersicherheit. Ist Ihr Unternehmen von NIS2 betroffen? (Einfachantwort)
Frage 32. Wie weit sind Sie in der Umsetzung der entsprechenden Vorgaben? (Einfachantwort)
Werte in %



Frage 33. Wenn Umsetzung zumindest teilweise durchgeführt:
In welchen Bereichen wurde die Umsetzung bereits abgeschlossen? (Mehrfachnennung)
n=36 Befragte, deren Unternehmen die Vorgaben zumindest teilweise durchgeführt haben
Werte in %



- Ein Viertel der Unternehmen ist von NIS2 betroffen, unter ihnen führen 7 von 10 bereits (teilweise) die entsprechenden Vorgaben durch. Bei den übrigen 3 von 10 Unternehmen ist die Umsetzung noch in Planung.
- 2 von 3 Unternehmen haben die Umsetzung im Bereich „Technische Sicherheit“ bereits abgeschlossen.

EY | Building a better working world

EY setzt sich für eine besser funktionierende Welt ein, indem wir neuen Wert für Kund:innen, Mitarbeitende, die Gesellschaft und den Planeten schaffen und gleichzeitig das Vertrauen in die Kapitalmärkte stärken.

Mithilfe von Daten, KI und fortschrittlicher Technologie helfen wir unseren Kund:innen, die Zukunft mit Zuversicht zu gestalten und Lösungen für die drängendsten Herausforderungen von heute und morgen zu entwickeln.

Unsere EY-Teams betreuen das volle Spektrum an Services in der Wirtschaftsprüfung, Unternehmensberatung, Steuerberatung sowie Strategie- und Transaktionsberatung. Angetrieben von branchenspezifischen Erkenntnissen, einem global vernetzten, multidisziplinären Netzwerk und vielfältigen Ökosystempartner:innen, erbringen wir Dienstleistungen in mehr als 150 Ländern und Gebieten.

Das internationale Netzwerk von EY Law, in Österreich vertreten durch die Pelzmann Gall Größ Rechtsanwälte GmbH, komplettiert mit umfassender Rechtsberatung das ganzheitliche Serviceportfolio von EY.

All in to shape the future with confidence.

EY bezieht sich auf die globale Organisation oder ein oder mehrere Mitgliedsunternehmen von Ernst & Young Global Limited, von denen jedes eine eigene juristische Person ist. Ernst & Young Global Limited ist eine Gesellschaft mit beschränkter Haftung nach englischem Recht und erbringt keine Leistungen für Kund:innen. Informationen darüber, wie EY personenbezogene Daten erhebt und verarbeitet, sowie eine Beschreibung der Rechte, die Einzelpersonen gemäß der Datenschutzgesetzgebung haben, sind unter ey.com/at/datenschutz verfügbar. Weitere Informationen über unsere Organisation finden Sie unter ey.com/at.

© 2025 Ernst & Young Wirtschaftsprüfungsgesellschaft m.b.H.
All Rights Reserved. | ED None

Diese Präsentation ist lediglich als allgemeine, unverbindliche Information gedacht und kann daher nicht als Ersatz für eine detaillierte Recherche oder eine fachkundige Beratung oder Auskunft dienen. Es besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität. Jegliche Haftung seitens der Ernst & Young Wirtschaftsprüfungsgesellschaft m.b.H. und/oder anderer Mitgliedsunternehmen der globalen EY-Organisation wird ausgeschlossen.

ey.com/at