
HDI
HDI Cyberstudie 2023

Vorwort

Die Cyber-Risikolage bleibt weiterhin dynamisch. Immer wieder erfolgen neue Wellen von Cyberangriffen auch auf deutsche Unternehmen. Zum Beispiel gerieten im Februar 2023 durch eine publik gewordene Sicherheitslücke in der Software VMware mehrere hundert deutsche kleine und mittlere Unternehmen (kurz KMU) in das Fadenkreuz von Cyberkriminellen. Dabei ist dies nur eines von inzwischen zahlreichen Beispielen rund um das Thema Cyberbedrohung und Cyberangriffe. Wie gehen deutsche KMU mit diesen Herausforderungen um? Wie erfahren diese Unternehmen von Schwachstellen? Und wie sehr beschäftigt sich ein so wesentlicher Teil der deutschen Wirtschaft mit dem Thema Cyber? Und was ist den Unternehmen dabei wichtig? Diese Fragen haben auch wir erneut gestellt und greifen diese in der zweiten Auflage der HDI Cyberstudie auf. Damit möchten auch wir einen Beitrag zur Aufklärung und Verbesserung des Wissens rund um aktuelle Cybergefahren leisten. Diese Studie gibt daher einen Überblick über die aktuelle Risikolage und Entwicklungen im Vergleich zum Vorjahr.

Kumul-Ereignisse wie die bereits beschriebene VMware-Sicherheitslücke, Angriffe auf Microsoft Exchange oder auf Log4shell sind nur die bekanntesten Beispiele und offenbaren das Gefahrenpotenzial von Cyberattacken auf Unternehmen. Gleichzeitig haben wir im Rahmen der HDI Cyberstudie eine rückläufige Beschäftigung mit Cyberrisiken festgestellt. Dies ist eine bedenkliche Entwicklung, denn weniger Aufmerksamkeit bedeutet leider nicht, dass weniger passiert ist. Wir haben im Rahmen unserer Studie vor allem eine Zunahme der Gefahr für kleinere Unternehmen festgestellt, die immer häufiger in den Fokus der Angreifer rücken. Für bekannte Probleme existieren jedoch bereits heute viele bewährte Lösungen. Sei es z. B. die Schulung der Mitarbeitenden, die dadurch auch privat einen Mehrwert erhalten, oder die Implementierung technischer und organisatorischer Sicherheitsmaßnahmen. Geeignete Werkzeuge stehen bereit. Die Unternehmen müssen hier nur zugreifen und beginnen, ihren Cybersicherheitsraum auszubauen. Wir sind überzeugt, mit dieser Studie einen Anstoß hierfür zu geben, und engagieren uns mit Nachdruck dafür, den deutschen Mittelstand ein wenig sicherer zu machen. Ich wünsche Ihnen viel Spaß beim Studium der spannenden Ergebnisse.

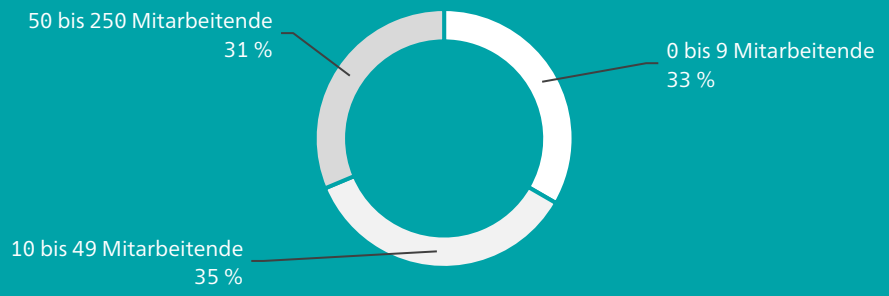
Ihr
Christian Kussmann
Bereichsvorstand Ressort Firmen & Freie Berufe

Methodik

Die Studie wurde Ende des Jahres 2022 zum bereits zweiten Mal durch das Marktforschungsinstitut Sirius Campus GmbH im Auftrag der HDI Versicherung AG durchgeführt. Hierfür wurden Entscheider und Mitentscheider in IT- sowie Versicherungsfragen aus insgesamt 702 verschiedenen kleinen und mittleren Unternehmen (kurz KMU) in Deutschland befragt. Die Stichprobe wurde nach Unternehmensgröße (Kleinstunternehmen, kleine und mittlere Unternehmen), Freiberuflern sowie anderen Branchen quotiert. Ende vergangenen Jahres (2022) wurden dafür 582 Online- und 120 Telefon-Interviews getätigt.
Die Daten wurden für die Auswertung repräsentativ anhand von Branche und Unternehmensgröße gewichtet. Alle Erwartungswerte stammen von Destatis und anderen Sirius Campus Versicherungsmarkt-Untersuchungen. Die Berufe Arzt, Steuerberater und Ingenieur (Kammerberufe) wurden mit je einem Drittel innerhalb dieser Gruppe gewichtet.
Die gewichtete Stichprobe setzt sich zu je einem Drittel aus den drei Gruppen der gängigen Klassifizierung nach Mitarbeitenden zusammen, die für KMU verwendet werden. Hierbei wurde unterteilt nach Kleinstunternehmen mit 0 bis 9 Mitarbeitenden, Kleinunternehmen mit 10 bis 49 Mitarbeitenden sowie mittleren Unternehmen mit 50 bis 250 Mitarbeitenden.
Zudem gaben 248 der Unternehmen an, bereits eine Cyberversicherung zu besitzen, und 230 befragte Unternehmen kündigten an, den Abschluss einer Cyberversicherung in den nächsten 12 Monaten zu forcieren. 185 der befragten Unternehmen besaßen allerdings keinerlei Cyberpolice und planen dies auch nicht.

Insgesamt lässt die Studie eine Hochrechnung der Ergebnisse auf die Gesamtheit der KMU in Deutschland zu.

Die Referenzstudie wurde Ende des Jahres 2021 ebenfalls durch das von der HDI Versicherung AG beauftragte Marktforschungsinstitut Sirius Campus GmbH durchgeführt. Hierbei wurden 518 Selbständige, Entscheider und Mitentscheider bei KMU befragt.



Inhaltsverzeichnis


Die Risikowahrnehmung sinkt.

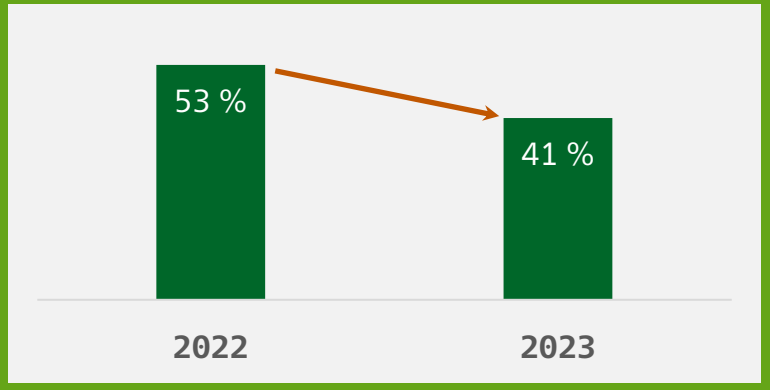
Die Risikowahrnehmung sinkt.

Seit Jahren gibt es zwei Trends hinsichtlich der Risikowahrnehmung des Cyberrisikos bei Unternehmen. Zum einen wird das Cyberrisiko inzwischen als Top-Risiko für Unternehmen angesehen. Zum anderen aber wird das mögliche eigene Risiko immer wieder unterschätzt. Das konnten wir bereits mit unserer Studie aus 2022 zeigen.

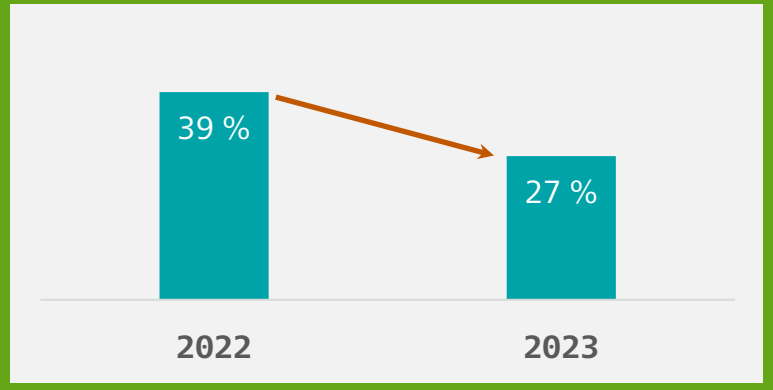
Im letzten Jahr bewerteten noch 53 % der Befragten das Risiko für KMU in Deutschland als hoch oder eher hoch, in den nächsten zwei Jahren Ziel einer Cyberattacke zu werden. 2023 waren es nur noch 41 %.

Das eigene Risiko wird als immer geringer eingeschätzt.

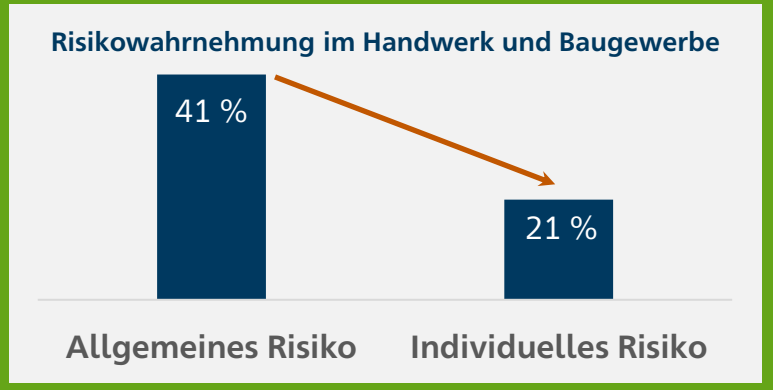
Entsprechend der allgemeinen Markterfahrung haben auch unsere Studien 2022 und 2023 bestätigt, dass Unternehmen trotz einer grundsätzlichen Wahrnehmung der Bedrohung häufig meinen, nicht selbst betroffen zu werden. Und auch diese Gefahrenwahrnehmung ist weiter zurückgegangen. 2022 sind noch 39 % der Befragten davon ausgegangen, innerhalb der nächsten zwei Jahre wahrscheinlich Opfer einer Cyberattacke werden zu können. 2023 lag dieser Wert nur noch bei 27 %. Von den befragten Entscheidern der IT- oder Software-Branche sehen jedoch in der neuen Befragung 40 % einen Cyberangriff auf das eigene Unternehmen als wahrscheinlich an. Handwerksunternehmen und Betriebe des Baugewerbes schätzen dabei von allen Befragten nicht nur das individuelle Risiko am geringsten ein (21 %), sondern zeigen auch die größte Differenz zur allgemeinen Risikowahrnehmung (41 %).



Die Risikowahrnehmung sinkt …



… auch für das eigene Risiko.

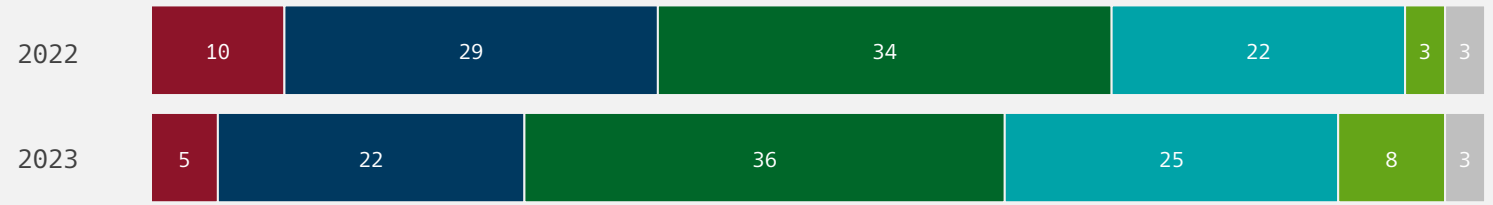


Im Handwerk und Baugewerbe herrscht die größte Differenz.

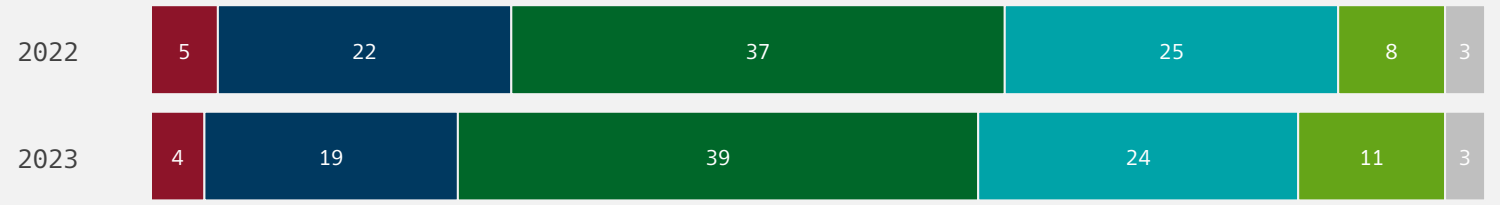
Zielverhalten: Risikowahrnehmung auf Gesamtebene

Allgemeine Risikowahrnehmung

Individuelle Risikowahrnehmung



Wahrnehmung Schadenrisiko



Hohes Risiko (100) | Eher hohes Risiko (75) | Eher geringeres Risiko (50) | Geringeres Risiko (25) | Kein Risiko (0) | Weiß nicht

Alle Angaben in Prozent.

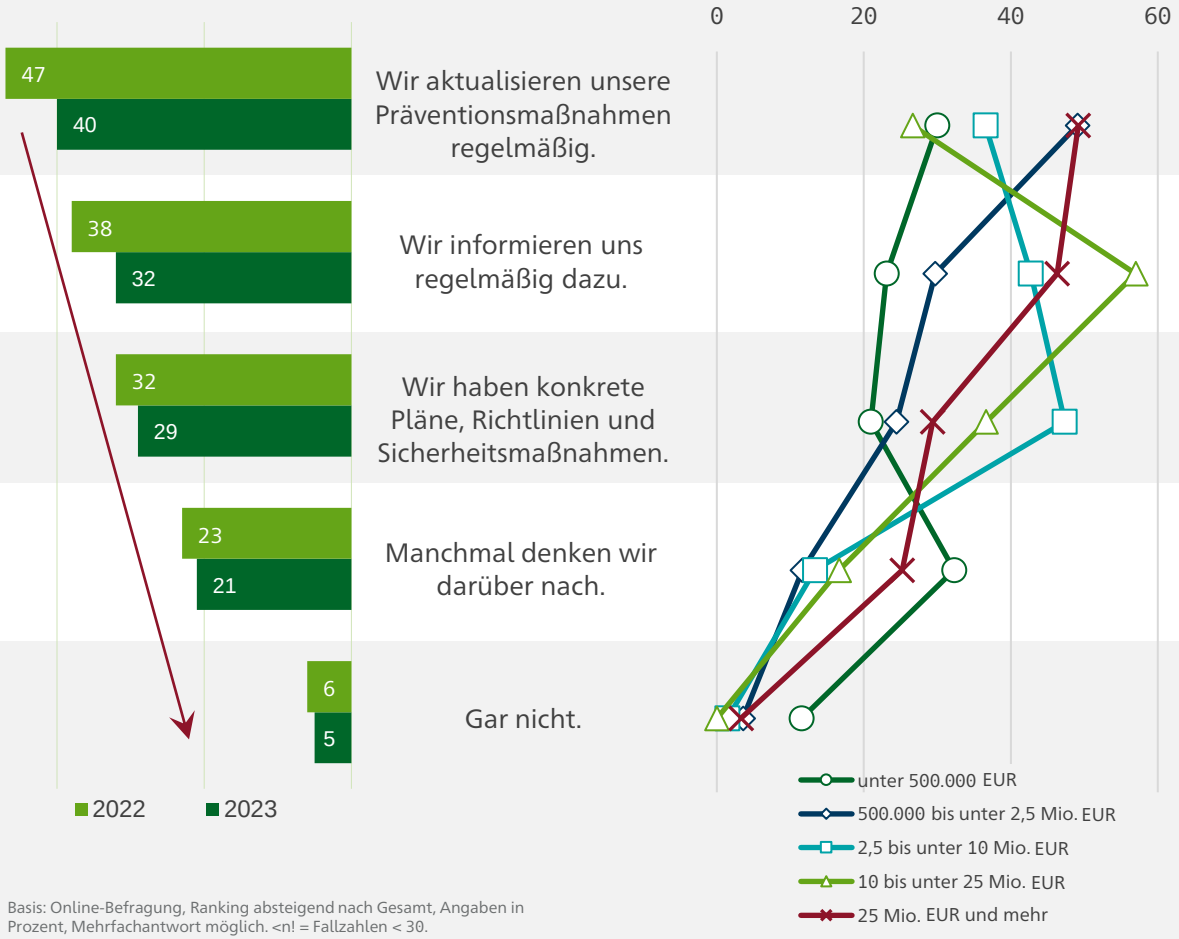
Wahrnehmung des allgemeinen und individuellen Risikos sinkt, aber bleibt beim potenziellen Schaden-risiko konstant.

Unabhängig von der Branche lässt sich die sinkende Tendenz mit einem Blick auf die Themen erklären, die die Wirtschaft im vergangenen Jahr bewegt haben. So haben 2022 unter anderem der Krieg in der Ukraine und die Inflation viele Unternehmen stark geprägt und gefordert – cyberrelevante Themen nicht so sehr.

In unserer Studie konnten wir in der Konsequenz auch feststellen, dass die Beschäftigungsquote mit den Themen IT-Sicherheit und Cybersicherheit im Jahresvergleich zurückgegangen ist (siehe Grafik, Seite 8). Aus unserer Schadenpraxis und den weiteren Ergebnissen der HDI Cyberstudie wissen wir jedoch, dass die gesunkene Aufmerksamkeit erhebliche Gefahren für die Unter-nehmen mit sich bringt. Die Schadenaufwände in der Cyberversicherung verharren weiterhin auf einem sehr hohen Niveau.

Beschäftigungsquote mit IT- und Cybersicherheit ist im Jahresvergleich zurückgegangen.

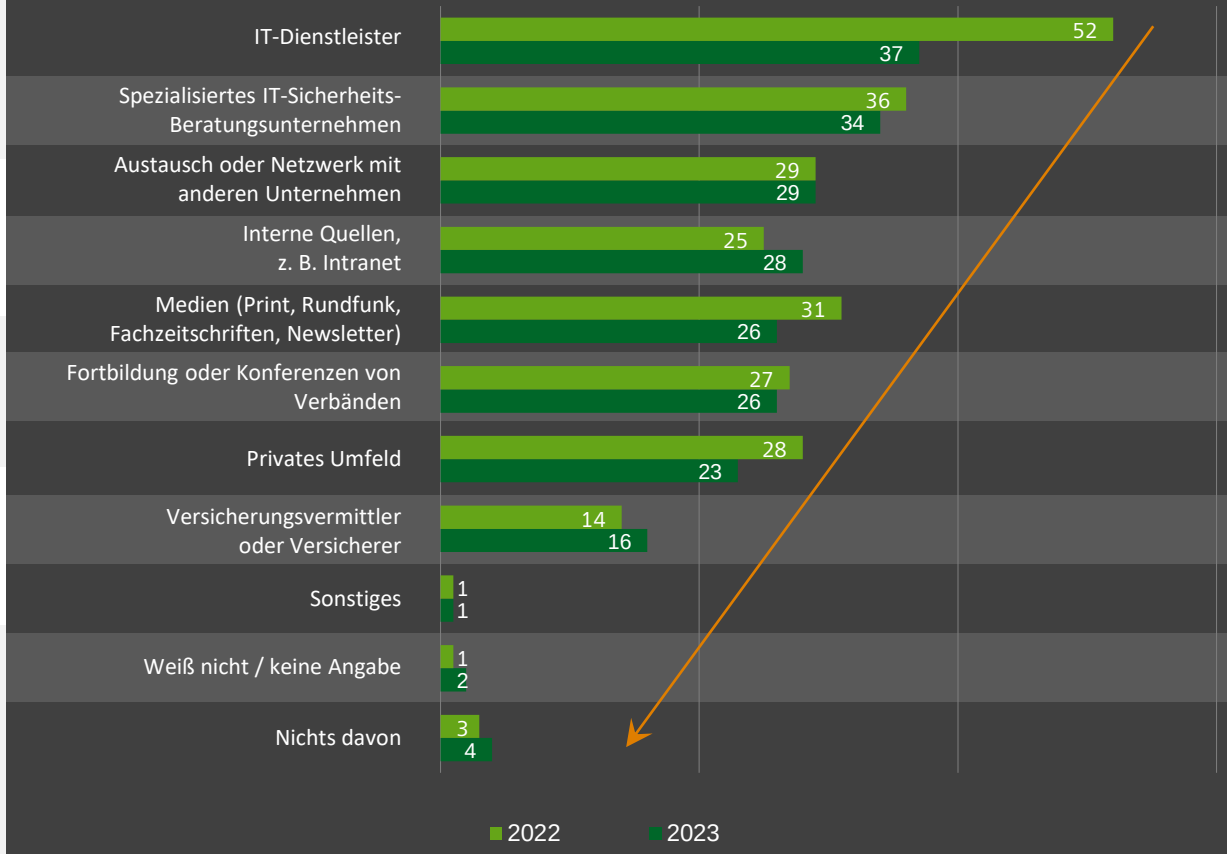
Wissensstand und Informationsverhalten
Wie sehr beschäftigt sich Ihr Unternehmen mit dem Thema IT- und Cybersicherheit?



Basis: Online-Befragung, Ranking absteigend nach Gesamt, Angaben in Prozent, Mehrfachantwort möglich. <n! = Fallzahlen < 30.

KMU setzen sich etwas seltener mit dem Thema IT-Sicherheit auseinander.

Wissensstand und Informationsverhalten: Informationsquellen
Welche Informationsquellen nutzt Ihr Unternehmen, um sich zu IT- und Cybersicherheit zu informieren?



Alle Angaben in Prozent.

Kleinere KMU im Fokus.

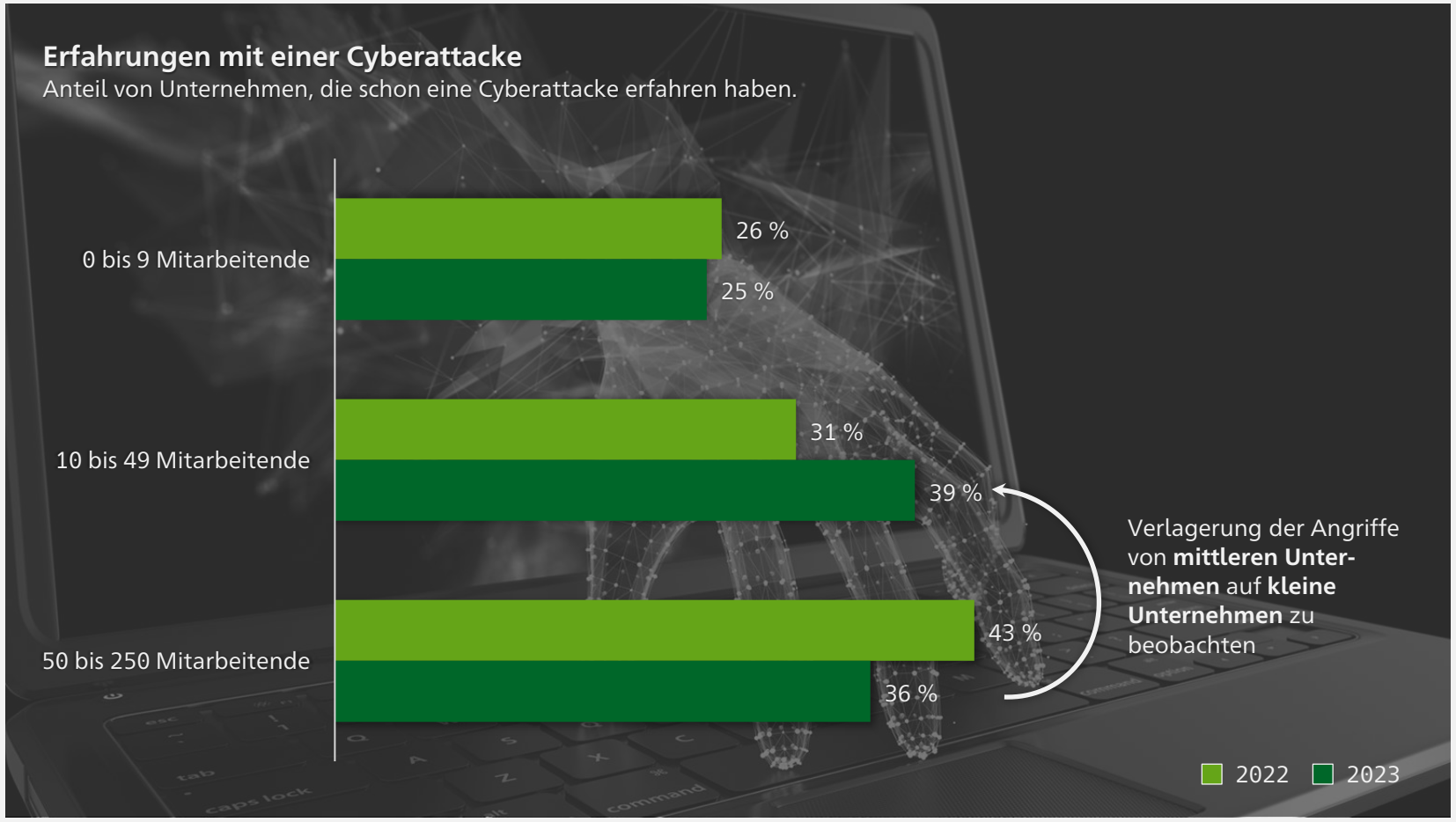
Kleinere KMU im Fokus.

Ähnlich zum Vorjahr, in dem 41 % der befragten Unternehmen Cyberattacken registrierten, haben in diesem Jahr 40 % der befragten Unternehmen von einer Cyberattacke berichtet. Am auffälligsten ist dabei, dass vor allem kleinere Unternehmen mit einer Größe von weniger als 50 Mitarbeitenden häufiger angegriffen wurden als Unternehmen mit mehr als 50 Mitarbeitenden.

KMU mit 10 bis 49 Mitarbeitenden am stärksten betroffen.

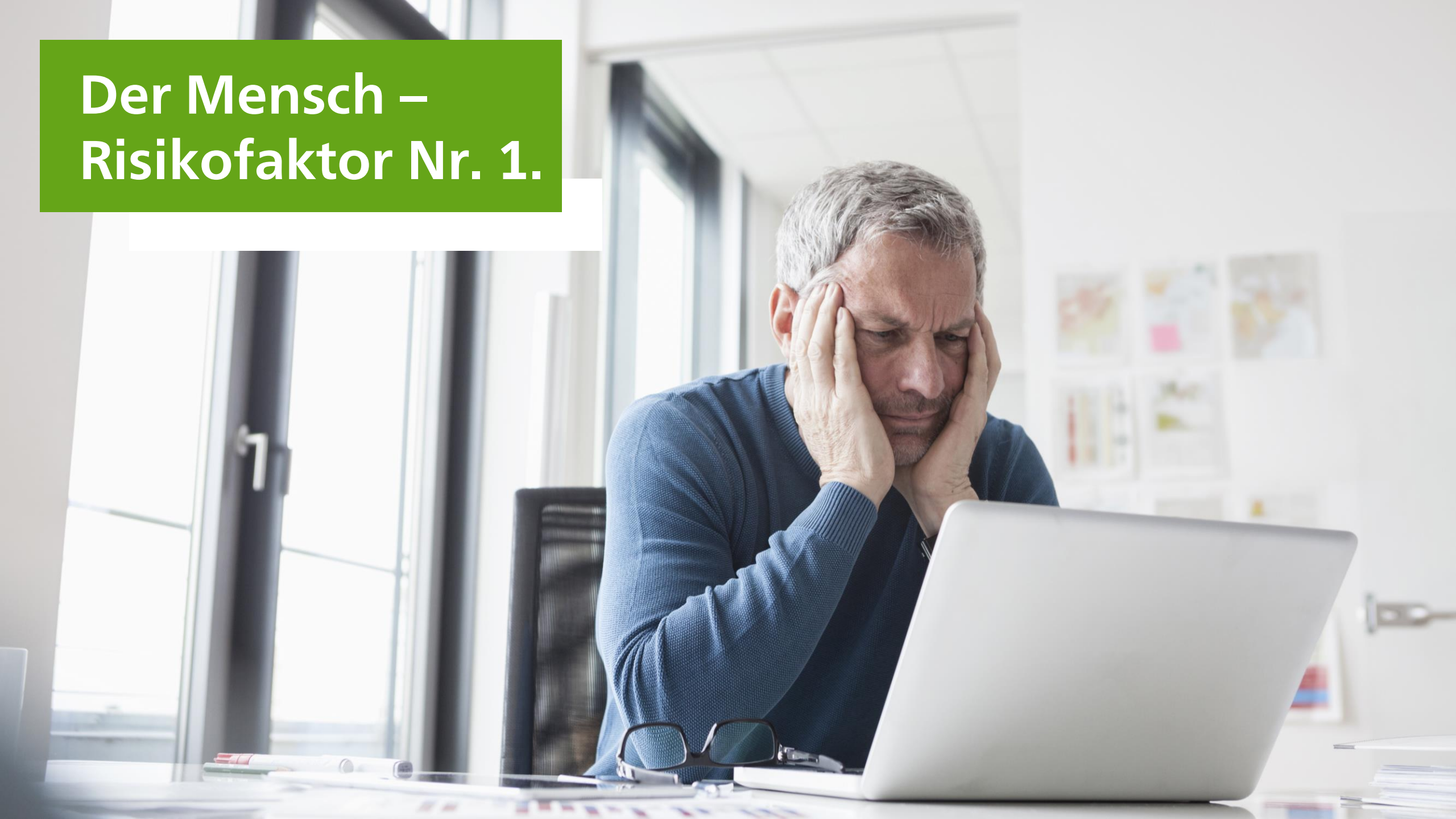
Vergleicht man den Trend zwischen den mittelgroßen KMU mit 10 bis 49 Mitarbeitenden und den größeren KMU mit 50 bis 250 Mitarbeitenden, zeigt sich im Jahresvergleich der beiden HDI Cyberstudien ein interessantes Ergebnis: War in der HDI Cyberstudie 2022 noch ein linearer Anstieg der Cyberangriffe im Verhältnis zur Unternehmensgröße festzustellen, hat sich der Fokus von Cyberkriminellen im vergangenen Jahr offenbar in Richtung kleinerer Unternehmen verschoben. So waren Unternehmen mit 10 bis 49 Mitarbeitenden mit 39 % (im Vorjahr noch 31 %) die Gruppe, die am häufigsten von einer Cyberattacke betroffen war. Erst an zweiter Stelle folgen mit 36 % nun die Unternehmen mit 50 bis 250 Mitarbeitenden. Im Jahr zuvor standen diese Unternehmen mit 43 % noch am stärksten im Fokus der Cyberkriminellen.

Dies zeigt insbesondere, dass die fehlende individuelle Risiko-Awareness gerade bei kleineren Unternehmen auf einem Trugschluss basiert. Kein Unternehmen kann sich mehr wegducken.



Der Anteil der betroffenen Unternehmen bleibt nahezu konstant.

Der Mensch – Risikofaktor Nr. 1.

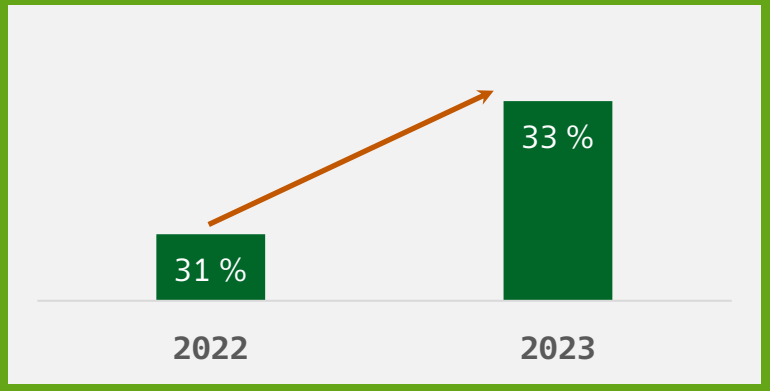


Der Mensch – Risikofaktor Nr. 1.

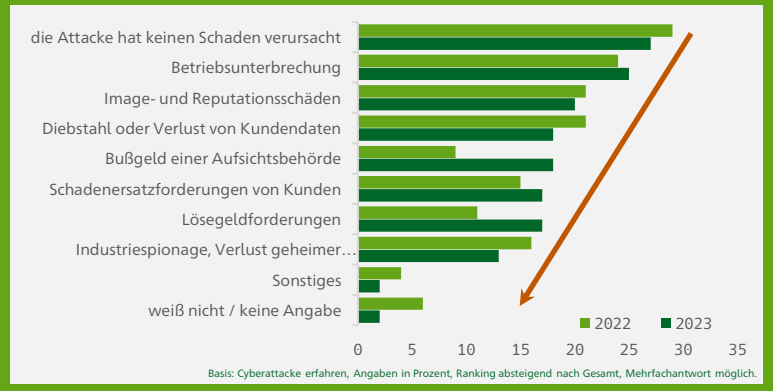
Das Vertrauen der Unternehmen in die von ihnen eingesetzten Präventionsmaßnahmen ist leicht gestiegen.

So sind 2023 33 % der Unternehmen der Meinung, dass die von ihnen durchgeführten präventiven Maßnahmen eine hohe Wirksamkeit gegen Cyberangriffe haben. 2022 waren 31 % der Befragten dieser Ansicht.

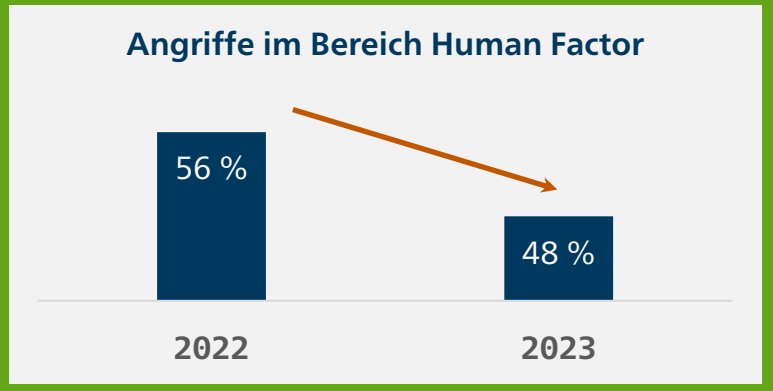
Eine erhöhte Sensibilisierung der Unternehmen zum Thema Informationssicherheit scheint sich auch in der Anzahl der 2023 erfolgreich durchgeführten Angriffe niederzuschlagen. So sind die erfolgreichen Angriffe im Jahresvergleich gesunken. Es muss sich allerdings noch zeigen, ob es sich hierbei um eine Momentaufnahme handelt oder um eine langfristige Tendenz. Vor allem beim „Risikofaktor Mensch" sind die erfolgreichen Angriffe zurückgegangen. Hier sind erfolgreiche Angriffe über das „Vortäuschen falscher Identitäten, Spam- oder Phishing-Mails" (von 20 % auf 15 %) und das Infizieren des Netzwerks über „Schadsoftware über Anhänge in E-Mails" (von 19 % auf 13 %) am deutlichsten gesunken. Dies kann der zunehmenden Etablierung und Umsetzung von Mitarbeitenden-Awareness-Maßnahmen geschuldet sein, wie sie durch diverse Richtlinien gefordert werden. Viele Cyberversicherungen am Markt bieten solche Maßnahmen als Zusatzleistung an.



Das Vertrauen in Präventionsmaßnahmen steigt langsam.



Erfolgreiche Angriffe werden weniger.



Der Risikofaktor Mensch wird kleiner.

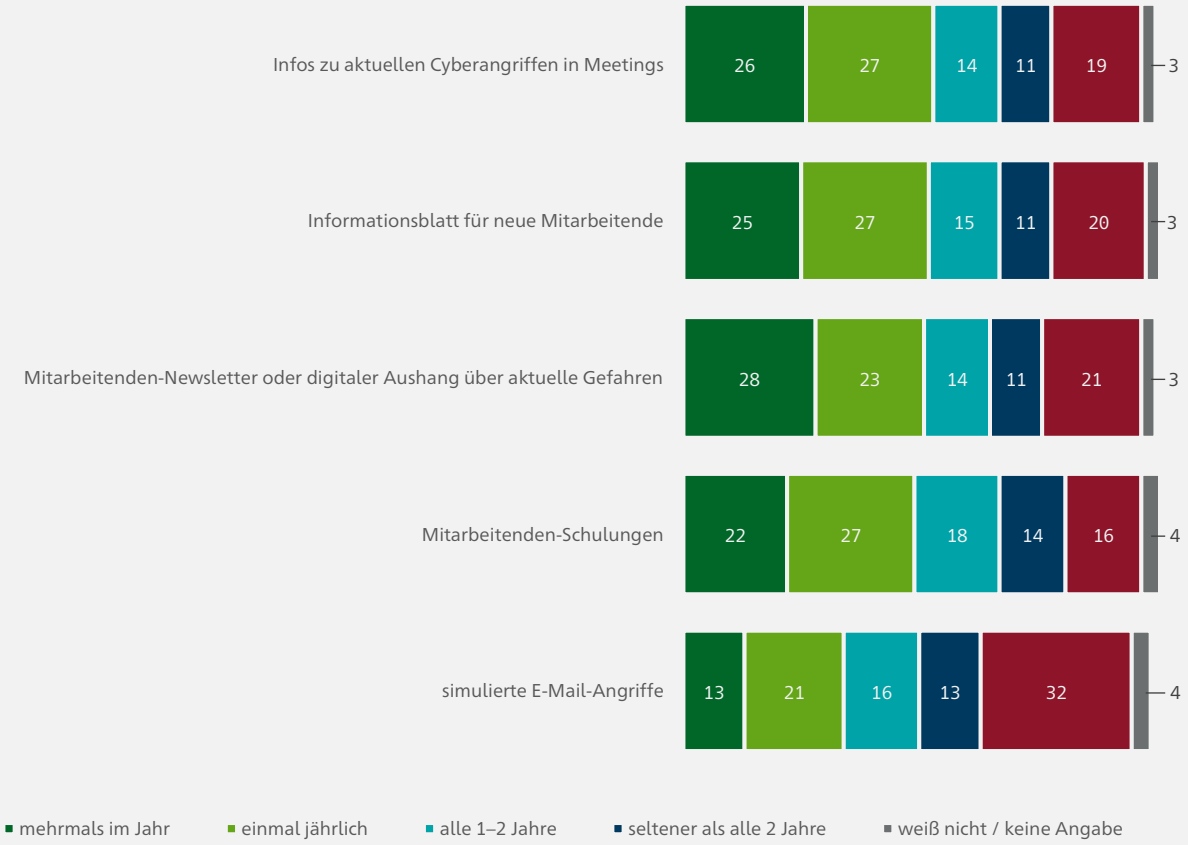
Mitarbeitenden-Sensibilisierung wichtig wie nie.

Trotz dieser positiven Entwicklungen bleibt der Mensch der Risikofaktor Nr. 1 für Cyberkriminalität. Technische Maßnahmen zur Cybersicherheit können das Risiko des menschlichen „Versehens" nicht komplett verhindern. Deshalb sind Präventionsmaßnahmen weiterhin essenziell – und werden auch zunehmend umgesetzt.

KMU führen im Jahresvergleich regelmäßige Präventionsmaßnahmen im Bereich Mitarbeitenden-Verhalten durch.

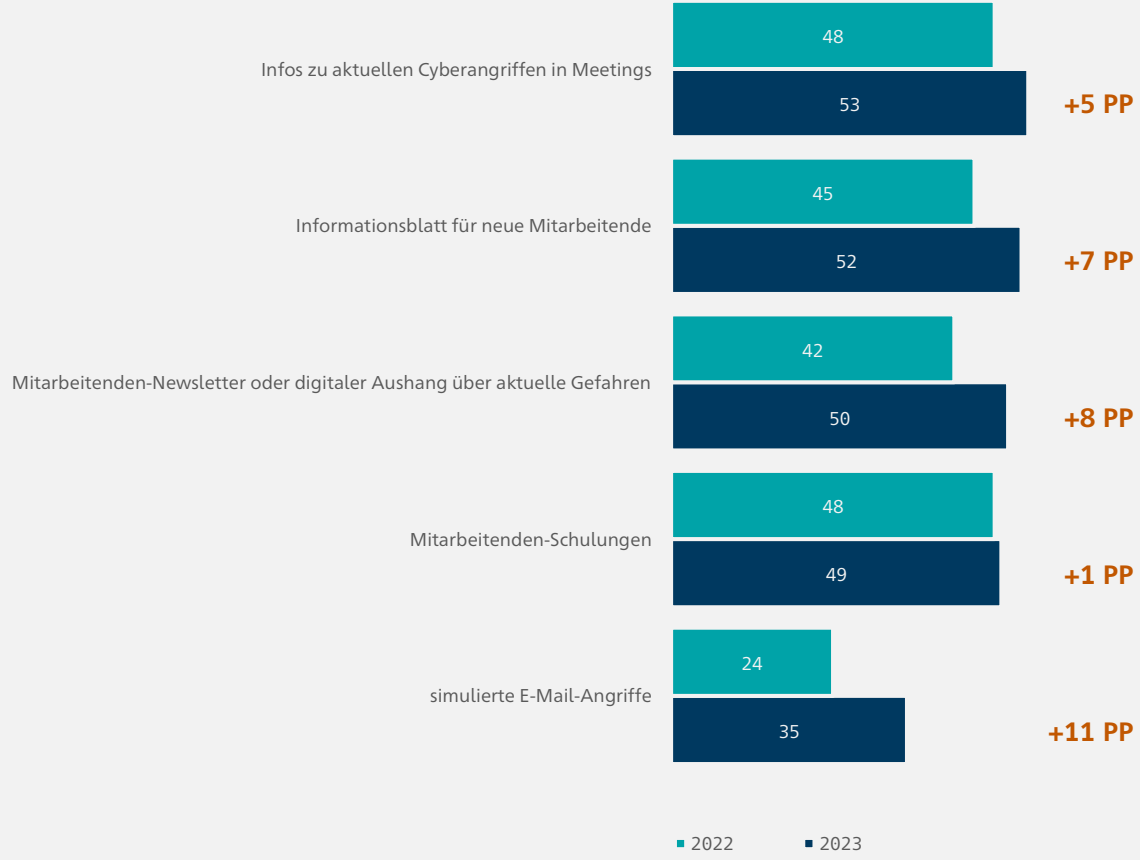
Prävention: Mitarbeitenden-Verhalten

Wie regelmäßig werden diese Präventionsmaßnahmen für Cybersicherheit im Bereich Mitarbeitenden-Verhalten in Ihrem Unternehmen umgesetzt?



Prävention: Maßnahmen zur Sensibilisierung im Jahresvergleich

Maßnahmen, die mindestens einmal jährlich durchgeführt wurden



Alle Angaben in Prozent.

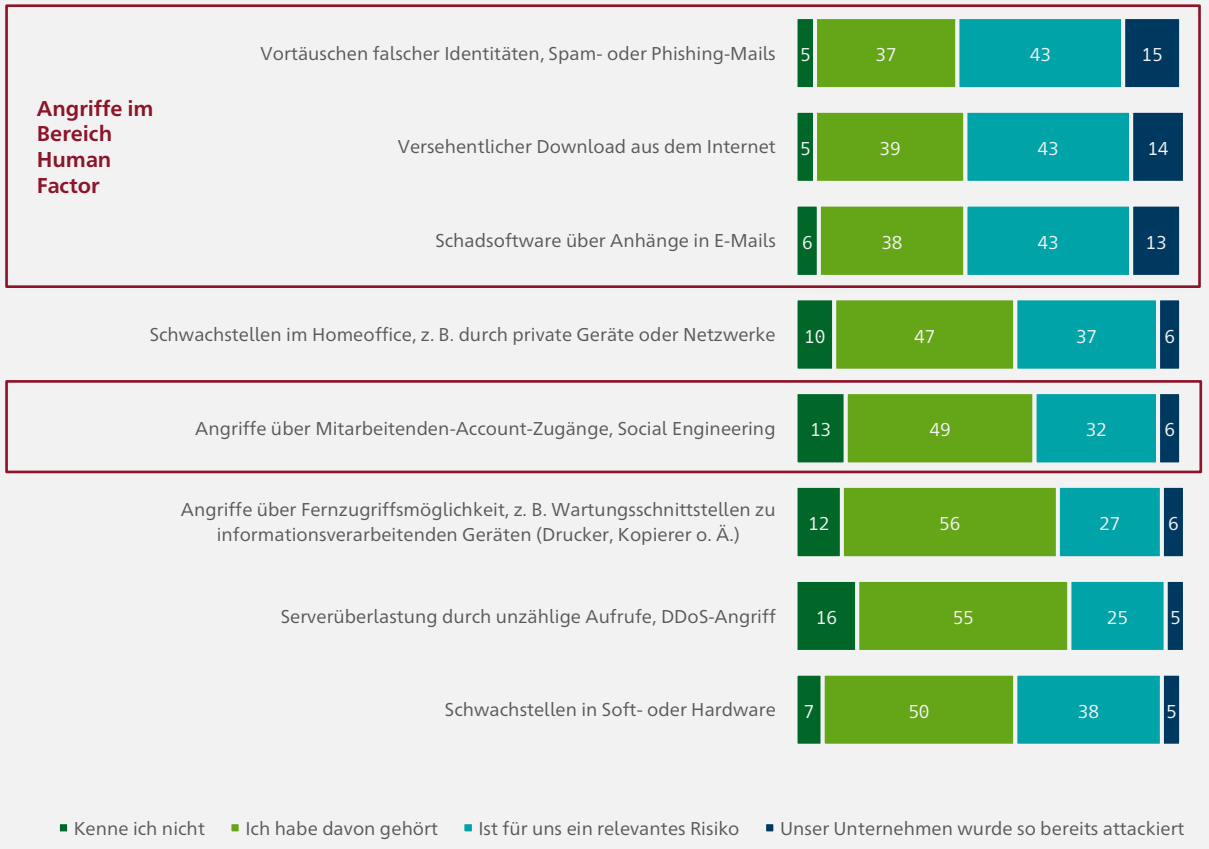
Mitarbeitenden-Sensibilisierung wichtig wie nie.

Trotz der Kombination aus Mitarbeitenden-Prävention und technischen sowie organisatorischen Maßnahmen gilt: Das Risiko von menschlichem „Versehen“ kann nicht komplett verhindert werden. So ist der „versehentliche Download einer Schadsoftware aus dem Internet“ von 10 % auf 14 % als auslösendes Ereignis für Cyberangriffe gestiegen.

KMU erleben im Jahresvergleich seltener Cyberangriffe, der Bereich Human Factor bleibt aber weiterhin Einfallstor Nr. 1.

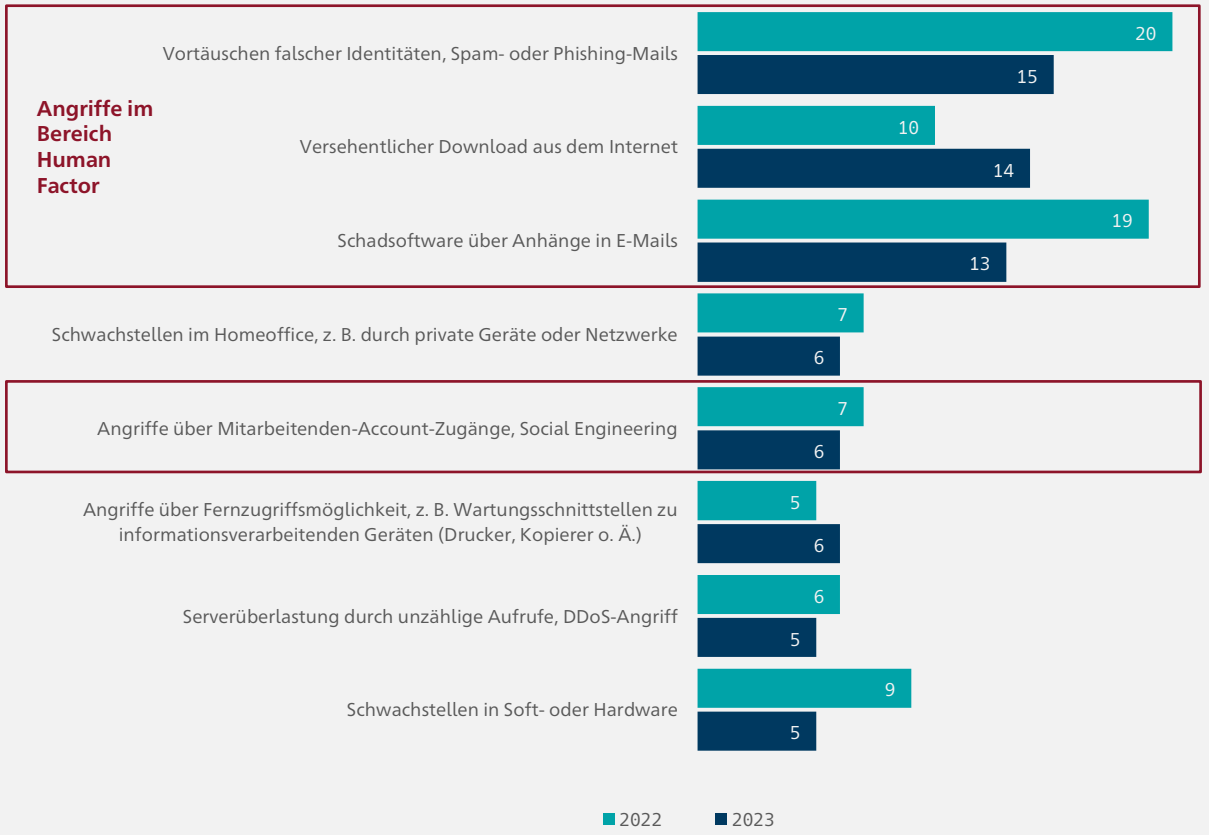
Risikowahrnehmung: Kenntnisse Cyberattacken

Kennen Sie die folgenden Formen von Cyberattacken?



Risikowahrnehmung: Kenntnisse Cyberattacken

„Unser Unternehmen wurde so bereits attackiert“ (Vergleich zum Vorjahr)



Basis: Alle Angaben in Prozent, Ranking nach Top-1-Box („unser Unternehmen wurde so bereits attackiert“).

Prävention ist besser als Reaktion.

Prävention ist besser als Reaktion.

Prävention ist besser als Reaktion: Daran hat sich auch laut der Cyberstudie 2023 nichts geändert. Die sinnvolle Zusammenstellung von organisatorischen, technischen und Awareness-Maßnahmen ist ein wesentliches Element der Informationssicherheits-strategie für die Unternehmen. Aus der Perspektive des Angegriffenen hat die Umsetzung von präventiven Maßnahmen signifikante positive Auswirkungen auf Schadenhöhe und -dauer.

Spezifische Präventionsmaßnahmen vermehrt im Fokus.

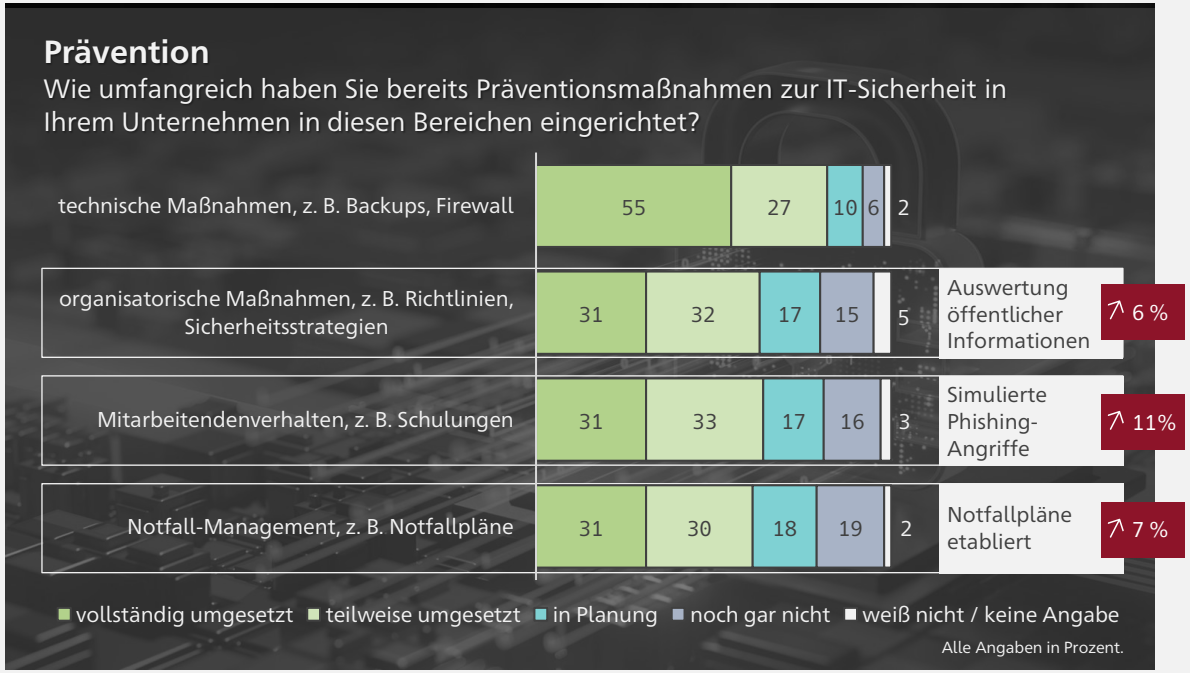
Diese wurden im Jahresvergleich in unterschiedlichem Maße von den Unternehmen umgesetzt. Während die technischen präventiven Maßnahmen, wie zum Beispiel Firewalls oder automatische Datensicherungen, von nahezu gleich vielen Unter-nehmen ergriffen wurden (2023: 82 %; 2022: 84 %), wurden organisatorische Maßnahmen eher vernachlässigt. So verließen sich in diesem Jahr nur noch 63 % der Unternehmen auf präventive organisatorische Maßnahmen, wie z. B. Passwortricht-linien. In der 2022er-Studie gaben noch 74 % der Befragten an, solche Maßnahmen durchzuführen. Erfreulich bei den organisatorischen Maßnahmen ist allerdings, dass laut der neuen Studie ein vermehrtes Augenmerk auf die Auswertung öffentlicher Schwachstellen sowie die Durchführung von Sicherheits-Checks gelegt wird.

Firmen setzen mehr auf Sensibilisierung der Mitarbeitenden.

Besonders erfreulich ist, dass Unternehmen verstärkt ihre Mitarbeitenden schulen. So geben 64 % der befragten Unternehmen an, Maßnahmen zur Mitarbeitenden-Sensibilisierung etabliert zu haben (2022: 60 %). Hervorzuheben ist hier insbesondere der verstärkte Einsatz von Phishing-Simulationen, welcher im Jahresvergleich um 11 Prozentpunkte gestiegen ist.

Die Wirksamkeit von Präventionsmaßnahmen belegt die Dauer von Betriebsunter-brechungen und Schadenhöhen nach einem erfolgreichen Cyberangriff.

Denn die Fakten zeigen: Prävention wirkt.



Geringere und kürzere Schäden dank Prävention.

Organisatorische Präventionsmaßnahmen (z. B. Passwortrichtlinien) werden weniger.

Technische Präventionsmaßnahmen bleiben beliebt.

Mitarbeitende werden stärker sensibilisiert.

Prävention wirkt!

Ein Unternehmen mit einem hohen Umsetzungsgrad von Präventionsmaßnahmen ist nach einem Cyberangriff und damit einhergehender Betriebsunterbrechung bereits nach durchschnittlich 3,8 Tagen wieder komplett arbeitsfähig. Wohingegen Unternehmen mit einem geringen Umsetzungsgrad von Präventionsmaßnahmen erst nach durchschnittlich 4,7 Tagen wieder ihrer täglichen Arbeit nachgehen können. Zudem zeigt sich eine signifikante Auswirkung auf die durchschnittliche Schadenhöhe. Der finanzielle Durchschnittsschaden einer Cyberattacke beträgt nach dem Ergebnis der HDI Cyberstudie 66.812 Euro.

Ein hoher Umsetzungsgrad der Präventionsmaßnahmen reduziert den Durchschnittsschaden um 25,7 % auf 49.645 Euro.

Auffällig, aber wenig überraschend ist ebenfalls, dass ein Unternehmen mit weniger umgesetzten Präventionsmaßnahmen einen im Durchschnitt höheren Cyberschaden erleidet. Dieser liegt gegenüber dem Durchschnittsschaden um 16,2 % höher bei 77.606 Euro.

Unternehmen sollten somit vermehrt auf Präventionsmaßnahmen setzen, um ihre Mitarbeitenden zu sensibilisieren und um auf den Notfall vorbereitet zu sein. Denn rechtzeitig ergriffene Präventionsmaßnahmen können Schäden durch erfolgreiche Cyberangriffe erheblich mindern.

Abgerundet wird eine vollumfängliche Informationssicherheitsstrategie mit einer Cyberversicherung. Dies belegen auch die Zahlen der Studie. So korreliert der Besitz einer Cyberversicherung mit dem Umsetzungsgrad von präventiven Maßnahmen. Das zeigt, dass eine vollumfängliche Informationssicherheitsstrategie ein Zusammenspiel mehrerer Faktoren ist, von denen die Cyberpolice einen wichtigen Teil ausmacht.

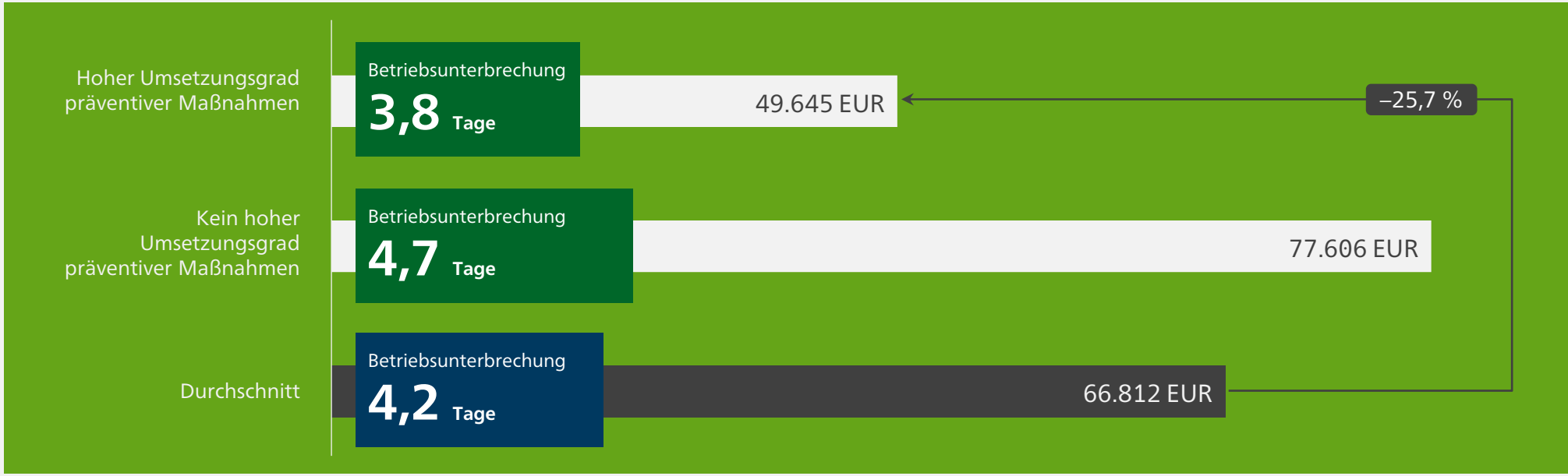
Mehr Prävention = weniger Schaden!

Prävention reduziert den finanziellen Schaden um durchschnittl. mehr als 25 %.

Eine Cyberattacke kostet im Durchschnitt 66.812 EUR.

Die Wahrscheinlichkeit, dass ein Cyberangriff auf ein Unternehmen mit genutztem Notfallplan zu einem Schaden führt, ist um 13 % niedriger.

Das Gleiche gilt für Unternehmen, die ihre Mitarbeitenden mindestens einmal im Jahr sensibilisieren.



Die Angst vor der Betriebsunterbrechung.

Die Angst vor der Betriebsunterbrechung.

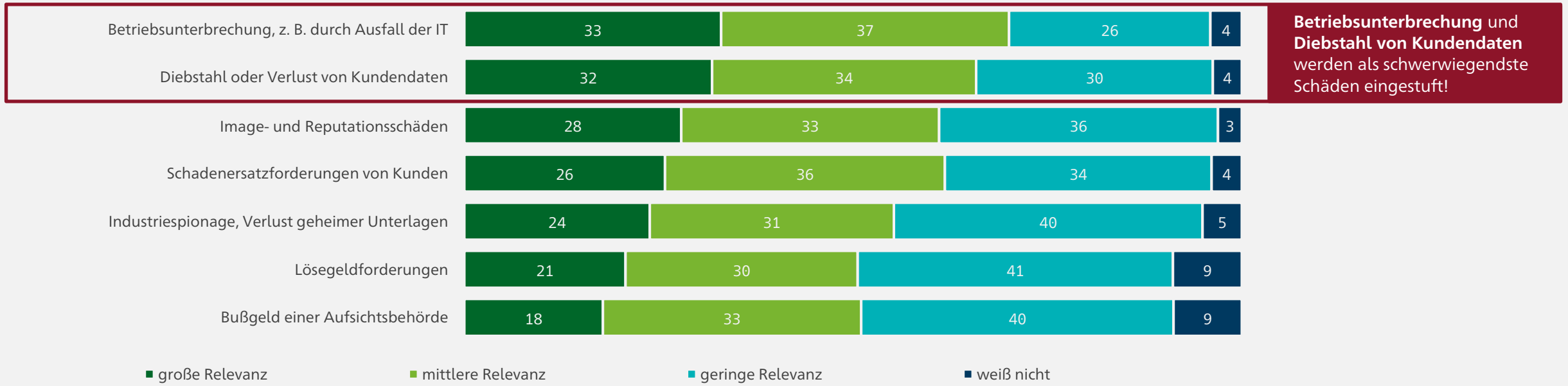
Zunehmende Schäden und damit einhergehende Erfahrungen von Unternehmen aller Größen sowie erhöhte mediale Präsenz machen klar: Betriebsunterbrechungen aufgrund von Cyberattacken können schwerwiegende Auswirkungen haben. Neben der finanziellen Stabilität ist auch das Image schnell gefährdet. Darüber hinaus drohen hohe Haftungsrisiken.

Cyberattacken bedrohen Image und Existenz.

Betriebsunterbrechungen haben die größte Relevanz für KMU.

Risikowahrnehmung: Schadenrelevanz

Welche Relevanz hätten oder hatten diese Schäden einer Cyberattacke für Ihr Unternehmen?



Betriebsunterbrechung und **Diebstahl von Kundendaten** werden als schwerwiegendste Schäden eingestuft!

Basis: Online-Befragung, alle Angaben in Prozent, Ranking nach Top-2-Box („große und mittlere Relevanz").

Angst vor Betriebsunterbrechung am größten und häufigsten.

Betriebsunterbrechung verursacht den größten Schaden und die größte Angst.

Arten der Schäden sind in den Branchen unterschiedlich relevant.

73 % der Cyberattacken verursachen tatsächlich einen Schaden.

Die HDI Cyberstudie 2023 belegt die Angst vor Betriebsunterbrechungen. Bei der Frage, wie relevant verschiedene Schäden durch Cyberattacken für Unternehmen sind, nimmt diese Gefahr mit 33 % (große Relevanz) den ersten Platz ein. Der Diebstahl oder Verlust von Kundendaten liegt mit 32 % auf Platz zwei. In der HDI Cyberstudie 2022 hatte dieser Schaden noch die größte Relevanz. Auf den weiteren Plätzen folgen Image- und Reputationsschäden (28 %) sowie Schadenersatzforderungen von Kunden (26 %).

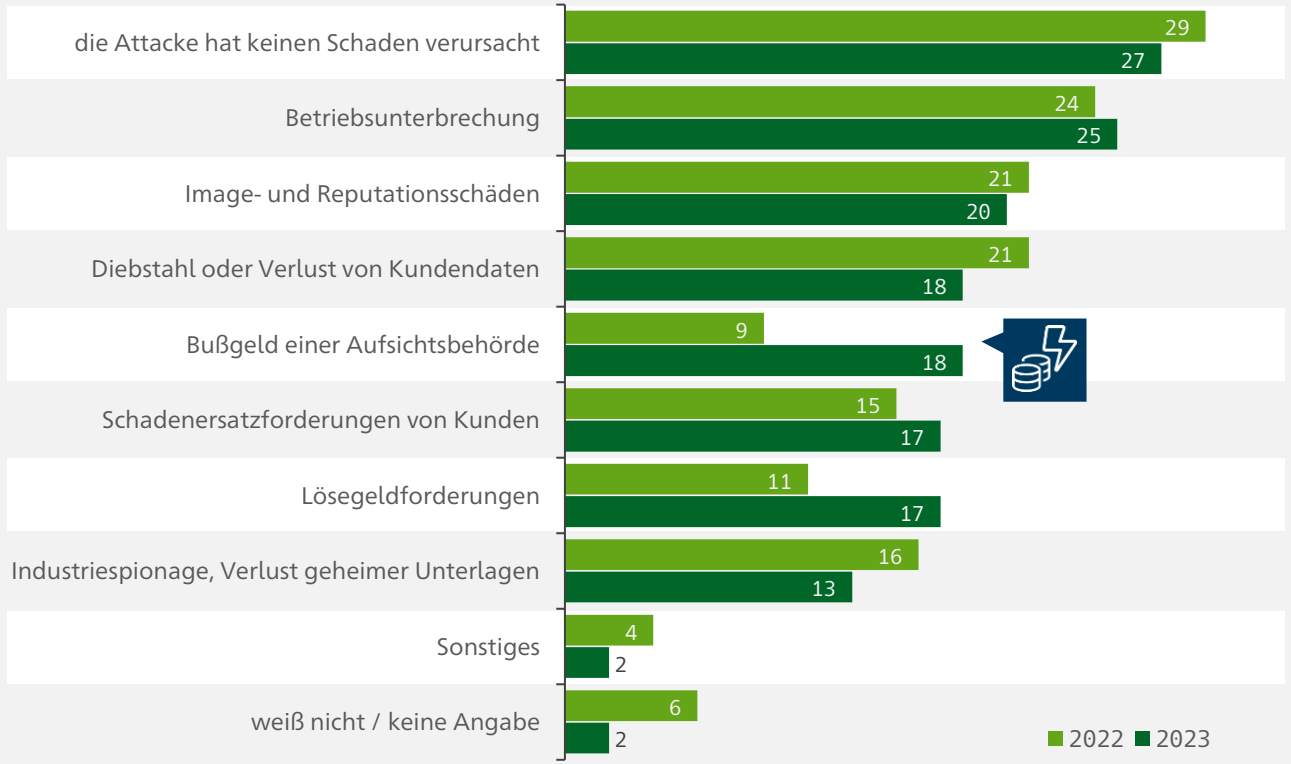
Auswirkungen je nach Branche unterschiedlich relevant.

Je nach Betriebsart unterscheiden sich die Ergebnisse in einigen Bereichen enorm. Handwerksbetriebe und Unternehmen des Baugewerbes messen dem Image- und Reputationsschaden eine niedrige Relevanz bei (61 %). Demgegenüber betonen Freiberufler (Steuerberater, Wirtschaftsprüfer, Rechtsanwälte, Notare, Architekten und Ingenieure) eine große Relevanz (34 %). Und nur 46 % attestieren eine geringe Relevanz.

Betriebsunterbrechung schadet am meisten.

Dass dieses Ergebnis in der Befragung nicht dem Bauchgefühl entspricht, zeigt die HDI Cyberstudie 2023 ebenso. Erfragt wurde, welche Erfahrungen mit Cyberattacken Unternehmen gemacht haben und welche Schäden dabei entstanden sind. Während 2022 noch 29 % der Attacken keinen Schaden verursachten, lag dieser Wert 2023 nur noch bei 27 %. Darauf folgen die Schadenarten mit der größten Relevanz. Betriebsunterbrechung ist auch in 2023 mit 25 % an erster Stelle (2022: 24 %). An zweiter Stelle stehen im Jahr 2023 Image- und Reputationsschäden mit 20 % und darauf folgend der Diebstahl oder der Verlust von Kundendaten mit 18 %.

Erfahrungen mit einer Cyberattacke: Schäden
Welche Schäden sind bei der Cyberattacke entstanden?



Basis: Online-Befragung, Alle Angaben in Prozent, Ranking nach Top-1-Box gesamt („große Relevanz“).

Behörden verhängen mehr Bußgelder.

Ein besonderes Augenmerk verdient auch das Bußgeld. Während 2022 nur 9 % der Unternehmen, die durch einen Cyberangriff attackiert worden waren, ein Bußgeld zahlen mussten, liegt der Wert 2023 schon bei 18 %. Hier zeigt sich ein deutlich verändertes Verhalten der Behörden. Unternehmen schätzen die Relevanz eines solchen Vorfalls jedoch noch gering ein im Vergleich zur Betriebsunterbrechung.

Viele Unternehmen wissen nicht, was ein Cyberschaden kosten kann.

Anhand der Schadenerfahrungen von HDI Deutschland können wir den Unternehmen ein gutes Gefühl für die Relevanz der Risiken bestätigen. Nur fällt es ihnen offenbar schwer, die Risiken monetär adäquat einzuschätzen. 49 % der befragten Unternehmen können keine Aussage zum potenziellen Schaden treffen. Verschärfend zeigt sich, dass der Wert auf 71 % ansteigt bei Unternehmen, die keine Cyberversicherung haben. Unternehmen mit Cyberversicherung können ihr Risiko besser beziffern. Gleichlautend schätzen sie es erwartungsgemäß höher ein.

Unternehmen ohne Cyberversicherung unterschätzen potenzielle Kosten.

Der Durchschnitt des zu erwartenden Schadens liegt bei 84.688 Euro und ist damit gegenüber 2022 leicht gesunken (88.817 Euro). Damit bestätigt sich der Trend, dass die eigene Risikowahrnehmung leicht gesunken ist. Auch hier wird klar, dass Unternehmen mit Cyberversicherung das Risiko höher einschätzen (85.329 Euro) gegenüber Unternehmen ohne Cyberversicherung (41.305 Euro). Interessanterweise lässt sich daraus nicht ableiten, dass Unternehmen mit Cyberversicherung bereits Schadenerfahrungen haben. Vergleicht man die Gruppe der Unternehmen, die schon Opfer einer Cyberattacke waren, mit Unternehmen, die noch nicht attackiert wurden, so liegen die Werte ungefähr gleich auf. (84.202 Euro ohne Cyberattacke vs. 85.244 Euro mit Cyberattacke). Somit bleibt ungewiss, ob die realistischere Gefahreneinschätzung oder die größere Sorge zum Abschluss geführt hat.

Der Anteil der mit Bußgeld bestraften Unternehmen verdoppelt sich.

Knapp die Hälfte der Unternehmen kann das finanzielle Risiko einer Cyberattacke nicht einschätzen.

Nicht versicherte Unternehmen unterschätzen das finanzielle Risiko.

Erklärungsbedarf: Schäden durch eine Cyberattacke.

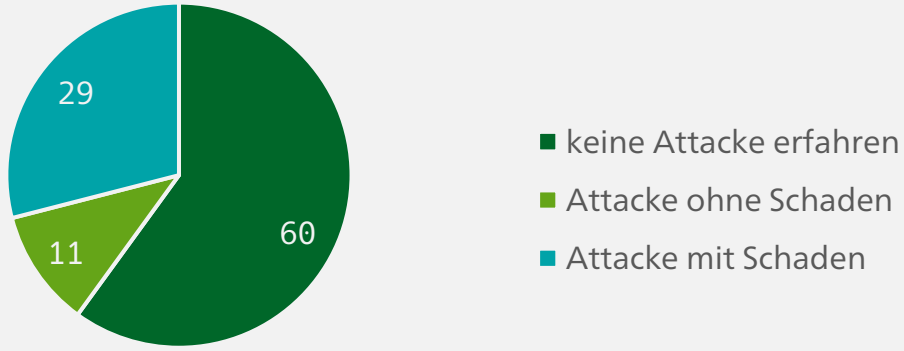
Risikowahrnehmung: Schadenhöhe
Was glauben Sie, welche maximale Schadenhöhe kann für Ihr Unternehmen durch eine Cyberattacke entstehen?

Alle Angaben in Prozent.

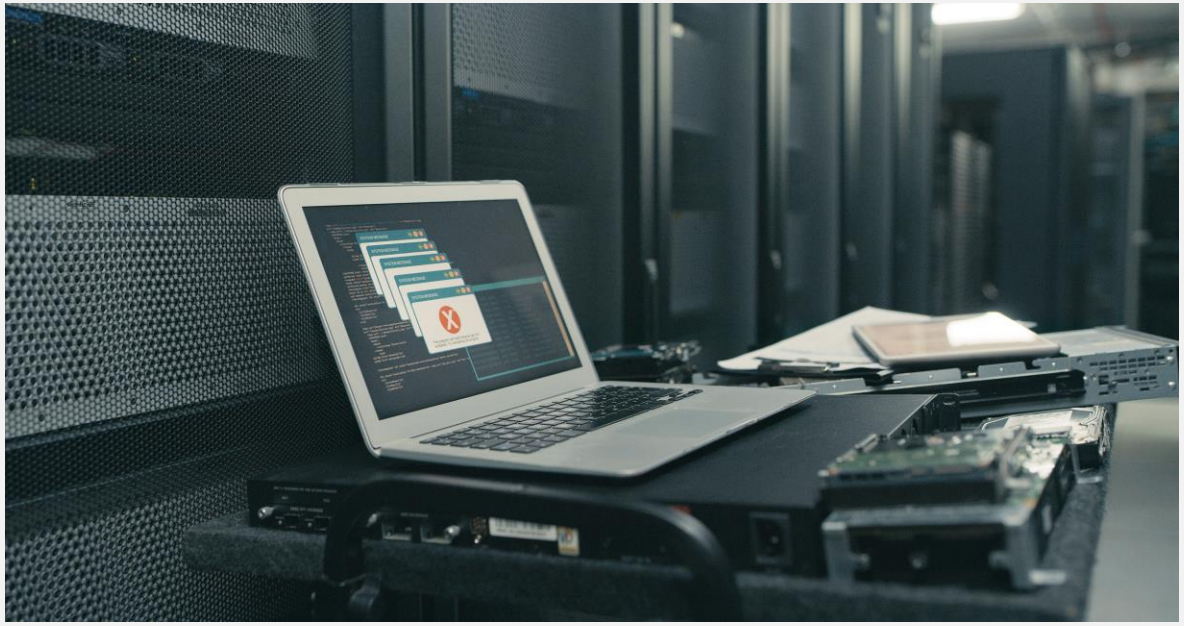
Die **Hälfte der KMU** kann die **Höhe** des potenziellen **Schadens** durch eine Cyberattacke **nicht beziffern.**

Aus Sicht von HDI Deutschland zeigt sich: Weitere Aufklärung zur realistischen Gefahreneinschätzung ist notwendig. Denn Unternehmen, die eine maximale Schadenhöhe nicht beziffern können, tun sich auch bei sinnvollen Präventionsmaßnahmen schwer.
Das gilt umso mehr mit Blick darauf, wie viele Unternehmen inzwischen Schäden erleiden:

Erfahrungen mit einer Cyberattacke



Alle Angaben in Prozent.

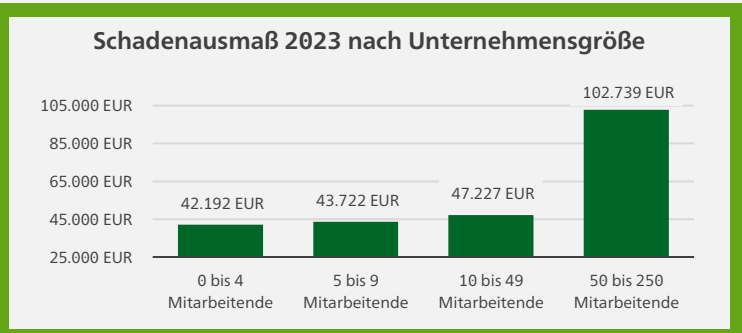



Cyberschäden sind
existenzbedrohend.

Cyberschäden sind existenzbedrohend.

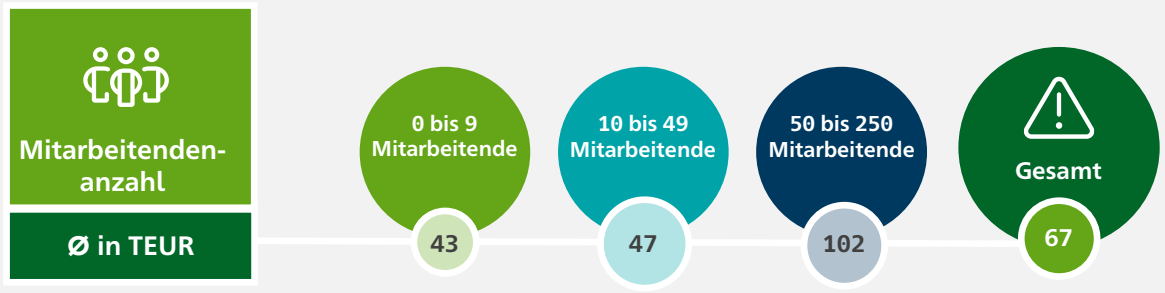
Die befragten Verantwortlichen in den Unternehmen schätzen die potenzielle Schadenhöhe realistisch ein. Mit 84.688 Euro ist der erwartete maximale Schaden einer möglichen Cyberattacke enorm hoch. Und es bestätigt sich: Cyberattacken können existenzbedrohend sein. Die durchschnittliche Schadenhöhe nach einer erfolgreichen Cyberattacke liegt bei 66.812 Euro. Sowohl 2022 als auch 2023 war bei 1 % der Fälle der Schaden größer als 500.000 Euro.

Das Schadenausmaß kann schneller existenzbedrohend sein, als häufig vermutet wird. Damit bestätigt sich auch die Notwendigkeit der Aufklärung. 49 % der Befragten können das Schadenausmaß nicht abschätzen. Fakt ist: Mit der Unternehmensgröße steigt auch das Schadenausmaß. Allerdings bleibt der Wert bei Unternehmen bis 49 Mitarbeitende relativ konstant.



Ab 50 Mitarbeitenden verdoppelt sich der durchschnittliche Schaden einer Cyberattacke.

Bei Unternehmen mit 50 bis 250 Mitarbeitenden steigt die Höhe sprunghaft an. Diese beziffern den Schaden auf durchschnittlich 102.739 Euro. Gerade für sehr kleine Unternehmen und größere Unternehmen zeigt sich die Brisanz einer Cyberattacke: Unternehmen mit einem Umsatz bis 2,5 Mio. Euro geben den Schadenaufwand im Schnitt mit 55.727 Euro an.



Die durchschnittliche Betriebsunterbrechung dauert 4,2 Tage.

KMU erleiden dabei im Durchschnitt eine Betriebsunterbrechung von 4,2 Tagen. Das mag zunächst wenig erscheinen. Aber: Nur 10 % der Unternehmen regeln die Probleme in weniger als einem Tag. Demgegenüber stehen 2 %, die länger als einen Monat mit Einschränkungen durch den Cyberangriff zu kämpfen haben. 7 % geben an, zwischen 1 und 4 Wochen beeinträchtigt gewesen zu sein.

Nur 10 % der Unternehmen sind einen Tag nach einer Attacke wieder voll arbeitsfähig.

KMU erleben im Durchschnitt 4,2 Tage Betriebsunterbrechung als Folge eines Cyberangriffs.

Erfahrungen mit einer Cyberattacke: Betriebsunterbrechung
Nach wie vielen Tagen hatte Ihr Unternehmen keinerlei Einschränkungen durch den Cyberangriff mehr im Betrieb, Vertrieb oder in der Produktion?

Alle Angaben in Prozent.

Betriebsunterbrechungen im verarbeitenden Gewerbe am längsten

Das verarbeitende Gewerbe ist dabei am stärksten von längeren Betriebsunterbrechungen betroffen. Der Durchschnittswert liegt bei 10 Tagen.
15 % der Unternehmen dieser Branche geben an, länger als einen Monat betroffen gewesen zu sein. 20 % mussten 1 bis 4 Wochen mit den Einschränkungen kämpfen.

Umfassende Systembereinigung dauert länger – lohnt sich aber.

Bei der Dauer der Betriebsunterbrechung zeigt sich die Wirksamkeit der Cyberversicherung. Unternehmen, die keine solche besitzen, sind im Schnitt 3,1 Tage durch eine Betriebsunterbrechung eingeschränkt. Unternehmen mit Cyberversicherung dagegen 4,4 Tage. Denselben Wert geben Unternehmen an, die planen, eine Cyberversicherung abzuschließen. Spricht das gegen die Cyberversicherung? Im Gegenteil. Das wird deutlich, wenn man sich die Details anschaut.

Während kein Unternehmen mit Cyberversicherung länger als einen Monat mit Einschränkungen zu kämpfen hatte, geben **6,8 % der Unternehmen ohne Cyberversicherung an, über einen Monat betroffen gewesen zu sein.** Außerdem können 5,8 % der Unternehmen die Dauer der Betriebsunterbrechung nicht angeben. Unternehmen mit Cyberversicherung können dies in allen Fällen. 3 % der Unternehmen mit Cyberversicherung geben keine Einschränkungen der Abläufe an. Der Wert bei Unternehmen ohne Cyberversicherung liegt mit 37 % deutlich höher. Aus der Praxis der Schadenregulierung bietet sich die Erklärung an, dass die Forensik und Bereinigung der Systeme einige Zeit in Anspruch nimmt. Bei Kostenübernahme durch die Versicherung wird dieser Schritt deutlich häufiger gemacht. Aus Sicht von HDI ist dies sinnvoll. Denn es zeigt sich immer wieder, dass die Wahrscheinlichkeit einer erneuten Cyberattacke insbesondere dann deutlich steigt, wenn keine adäquate Bereinigung der Systeme vorgenommen wird.

Versicherte Unternehmen sind nie länger als 1 Monat eingeschränkt.

Wird nicht adäquat bereinigt, sind einmal attackierte Systeme anfälliger für erneute Angriffe.

Ein Notfallplan ist unverzichtbar.

Ein Notfallplan ist unverzichtbar.

Nichts mehr dem Zufall überlassen: Nur wer Erstreaktionen, Abläufe, Ansprechpartner und einzuleitende Maßnahmen kennt, kann effektiv und effizient auf einen Cybervorfall reagieren. So ist die Wahrscheinlichkeit, dass ein Angriff zu einem Schaden führt, bei Unternehmen mit Cyber-Notfallplan bzw. organisiertem Notfallmanagement um 13 % niedriger als bei Unternehmen ohne Notfallplan.

Folgerichtig ist auch der Anteil der Unternehmen gestiegen, die planen, einen Notfallplan in ihrem Unternehmen umzusetzen. Waren es 2022 nur 16 % der Befragten, spielen 2023 bereits 21 % mit dem Gedanken, ein solches Instrument einzusetzen. Auch die Anzahl der Unternehmen mit bereits eingeführtem Notfallplan ist im Jahresvergleich gestiegen: von 19 % auf 24 %. Die Cyberversicherung nimmt hier durch Zusatzleistungen Einfluss: Besitzt ein Unternehmen eine Cyberversicherung, so wird bei 37 % der Unternehmen ein Notfallplan regelmäßig genutzt. Bei Unternehmen ohne Cyberversicherung sind es lediglich 16 %.

Unternehmen können Cyberrisiken zunehmend aktiv managen.

Eine weitere Erkenntnis aus der Studie: Unternehmen werden mehr und mehr gezielt auf Cyber-Incidents aufmerksam. So lässt sich entsprechend reagieren und ggf. größerer Schaden abwenden. Auch hier hilft der Notfallplan. Waren es 2022 noch 27 % der Unternehmen, die eine Cyberattacke per Zufall entdeckt haben, so ist dieser Wert 2023 auf 15 % gesunken. Vermehrt werden systemische, wiederkehrende Verfahren und Abläufe wie Screening oder Überprüfung veröffentlichter Schwachstellen zur Detektion eingesetzt. So treten die Unternehmen aus ihrer passiven Lage und haben die Möglichkeit, das Cyberrisiko aktiv zu managen. Allerdings werden trotz dieser positiven Entwicklungen immer noch 33 % aller Schäden lediglich durch Zufall entdeckt.

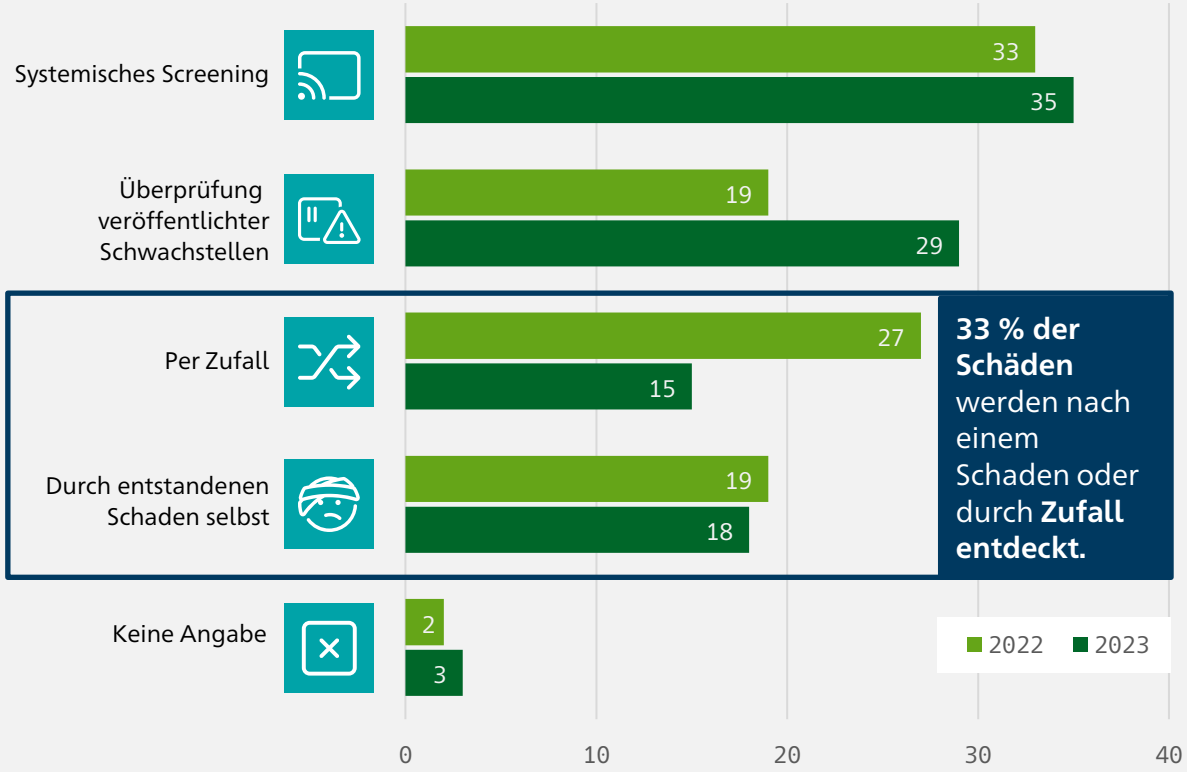
Mit Notfallplan 13 % niedrigere Erfolgsquote von Cyberattacken

Immer mehr Unternehmen haben einen Notfallplan bzw. wollen einen umsetzen.

Durch gezielte Screenings werden zufällig entdeckte Cyberattacken weniger.

Detektion von Cybervorfällen.

Durch systematische Überprüfungen werden immer mehr Cybervorfälle entdeckt und die Schäden behoben. Doch auch hier gibt es noch viel zu tun.



Alle Angaben in Prozent.

Sicherheitsberatung und Krisenunterstützung –

der größte Mehrwert der Cyberversicherung.

Sicherheitsberatung und Krisenunterstützung – der größte Mehrwert der Cyberversicherung.

Im Allgemeinen geht es beim Versicherungsschutz um den Risikotransfer bzw. die Kostenübernahme für versicherte Positionen. Bei der Cyberversicherung lässt sich dies in den Drittschadenbereich, also einem Haftpflichtansatz bei Schädigung eines Dritten (durch z. B. einen Datenschutzverstoß), und dem Eigenschadenbereich untergliedern. Im Eigenschadenbereich sind die direkt entstanden Kosten wie Forensikleistungen, Datenwiederherstellung, PR-Kosten oder auch die Betriebsunterbrechung erfasst, um nur einige zu nennen. Die operativen Mehrwerte von Cyberversicherungen liegen allerdings vor allem in den häufig in Versicherungspaketen integrierten abgestimmten Assistanceleistungen. Aufgrund der Komplexität des Cyberthemas wird dieser Ansatz auch von den Unternehmen mehr und mehr gefordert. Und viele sind bereit, für diese Zusatzleistungen auch höhere Versicherungsbeiträge in Kauf zu nehmen. Das daraus resultierende Leistungsversprechen, das sich sonst meist nur im Schadenfall manifestiert, ist somit bei einer Cyberversicherung deutlich weiter gefasst. Ein zentraler Bestandteil dieser Leistungen ist zum Beispiel ein umfassendes spezialisiertes Krisenmanagement.

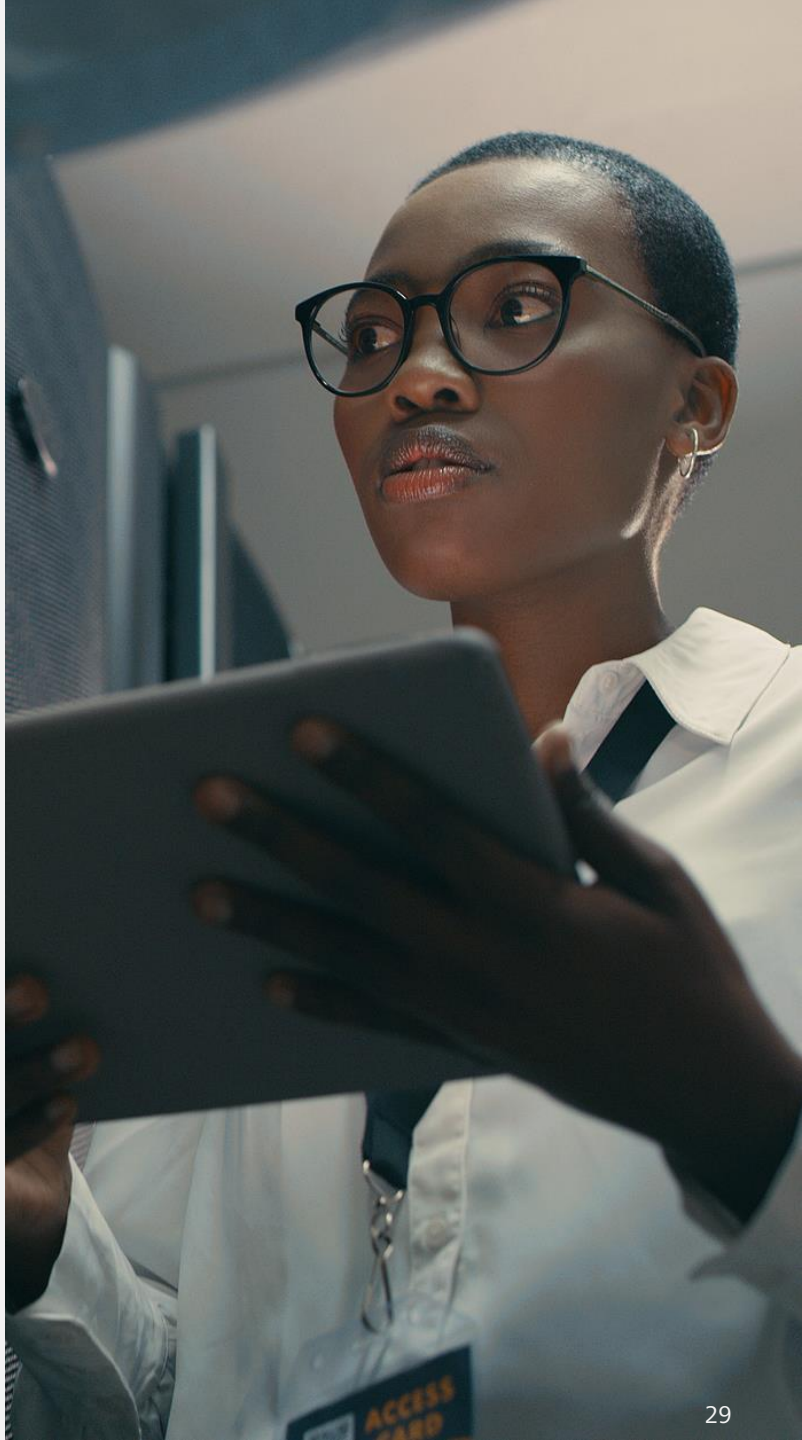
Hilfe und Beratung durch Spezialisten und 24/7-Schadenhotline sind besonders gefragt.

So ist für 43 % der befragten Unternehmen eine permanent erreichbare Schadenhotline mit Soforthilfe besonders wichtig und sollte ohne Zusatzkosten als Leistungsmerkmal integriert sein. Bei der Cyberversicherung können Versicherer über ein Schadennetzwerk oftmals mehr spezifische Leistungen zur Verfügung stellen, als ein Unternehmen im Sinne des Krisenmanagements in Eigenregie bereitstellen könnte. Daraus folgend sind für 35 % die Kostenübernahme für Daten- und Systemwiederherstellung durch Spezialisten wichtig. Hier zeigt sich, dass spezifisches Fachwissen für Cybersicherheit als essenziell angesehen wird und im Rahmen eines Netzwerks den höchsten Nutzen für ein Unternehmen bietet. 26 % sehen ergänzend eine Rechtsberatung bei Datenschutzverletzungen als wesentliches weiteres Leistungsmerkmal. Mit steigender Größe des Unternehmens wächst auch der Bedarf an externer Beratung zu Präventionsmaßnahmen oder externen Audits. Im Bereich der Unternehmen von 50 bis 250 Mitarbeitenden sind 20 % bereit, einen Mehrbeitrag für diese Zusatzleistungen zu bezahlen. Insgesamt ist der Wert von 12 % auf 16 % in 2023 angestiegen.

Umfassendes, spezialisiertes Krisenmanagement ist in der Cyberversicherung zentraler Bestandteil.

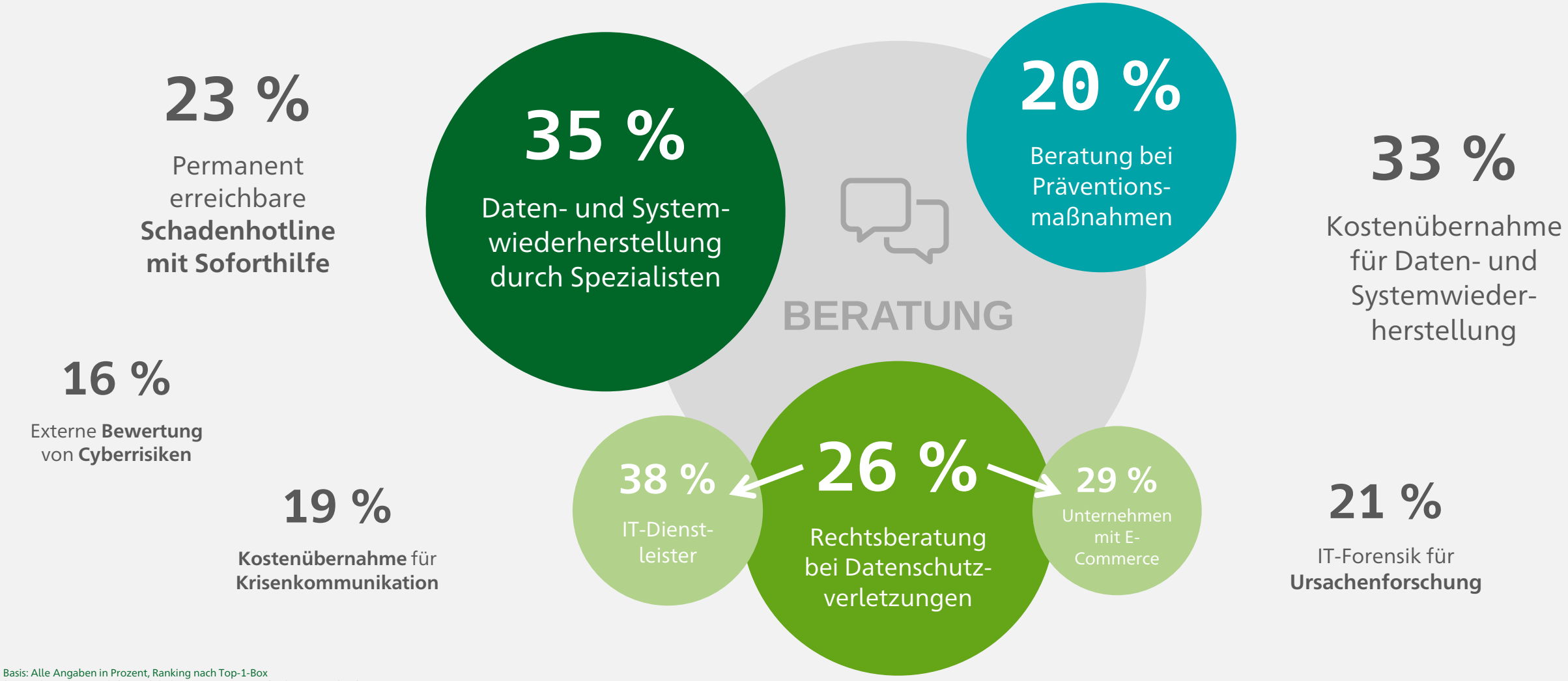
Wichtigste Leistung für Kunden: Kostenübernahme für Daten- und Systemwieder-herstellung durch Spezialisten.

Größere Unternehmen brauchen zunehmend auch Beratung zu Präventionsmaßnahmen.



Viele KMU akzeptieren einen höheren Versicherungsbeitrag für Zusatzleistungen. Beratungsleistungen sind dabei besonders gefragt.

Zielverhalten: Abschluss / Planung Cyberversicherung, Zusatzleistungen



Basis: Alle Angaben in Prozent, Ranking nach Top-1-Box
(„so wichtig, dass wir dafür auch höhere Beiträge in Kauf nehmen würden").

Die Bereitschaft, sich von Versicherern über IT-Sicherheit informieren zu lassen, steigt im Jahresvergleich deutlich an.

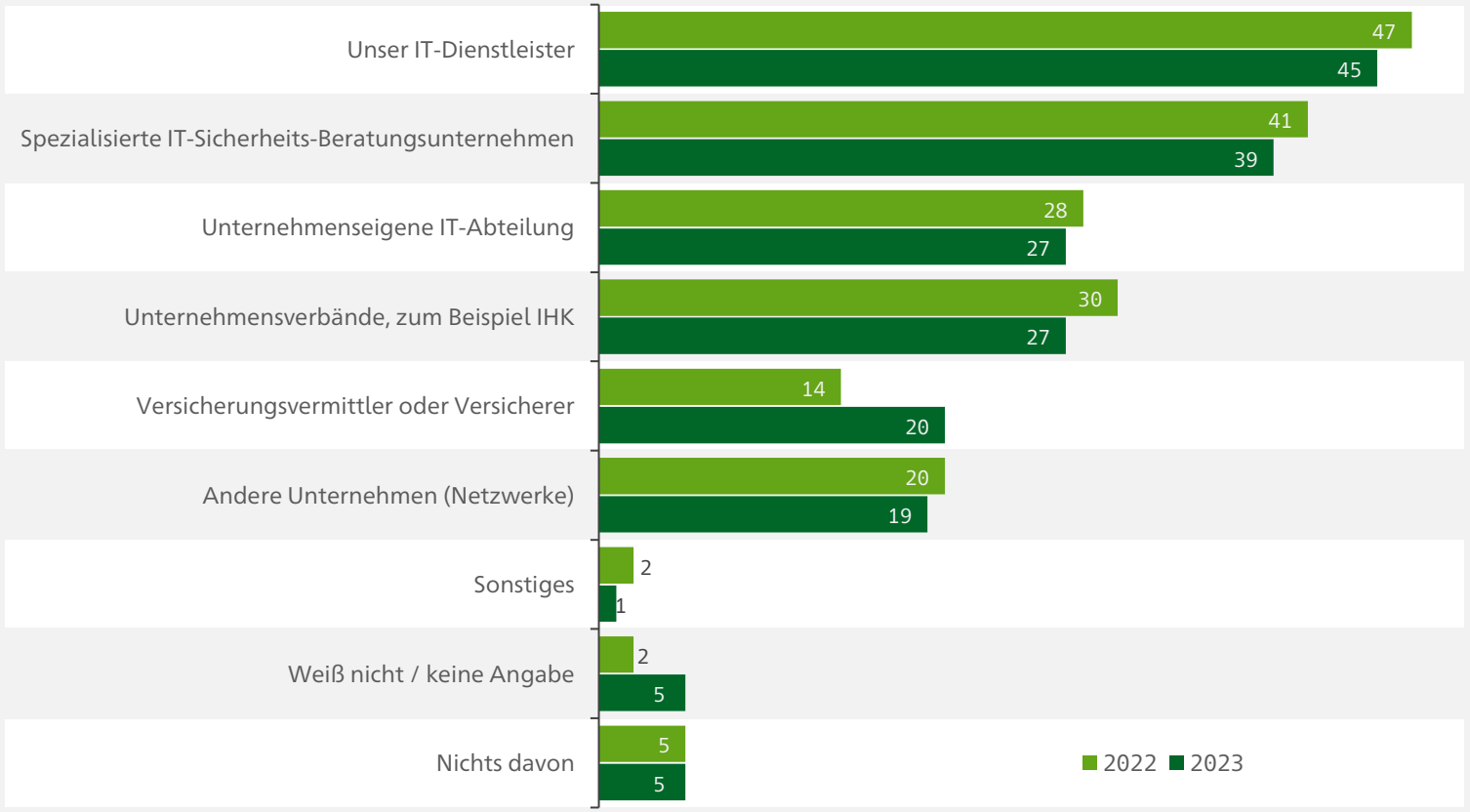
Chance für Versicherer: Entwicklung zum Ansprechpartner des Vertrauens für Unternehmen.

Ein eher unerwarteter Trend ist die Bereitschaft, sich durch Versicherungsvermittler oder Versicherer über Aktuelles in der IT-Sicherheit informieren zu lassen. Hier ist ein Anstieg auf 20 % zu verzeichnen (14 % in 2022). Eine Bereitschaft, die es von den Versicherern und Vermittlern zu nutzen gilt. Hier kommt es darauf an, skalierbare Hilfestellungen für die Unternehmen zu bieten, um diese Rolle langfristig einzunehmen und das Vertrauen zu bedienen. Die altgedienten Informationsmuster „IT-Dienstleister“, „IT-Beratung“, „eigene IT-Abteilung“ und „Unternehmensverbände“ haben hingegen einen leichten Rückgang zu verzeichnen. Der Empfehlung von IT-Diensteistern wird weiterhin grundsätzlich hohes Vertrauen entgegengebracht. Denn immer noch 45 % der eingeführten Präventionsmaßnahmen werden aufgrund der Empfehlung des eigenen IT-Dienstleisters umgesetzt.

IT-Dienstleister und andere IT-Spezialisten sind für KMU noch immer DER Ansprechpartner des Vertrauens.

Immer mehr Unternehmen würden sich auch von Versicherern über Aktuelles in der IT-Sicherheit informieren lassen.

Wissensstand und Informationsverhalten: gewünschter Ansprechpartner
Von wem möchten Sie über Aktuelles rund um die IT-Sicherheit informiert werden?



Basis: Alle Angaben in Prozent, Ranking absteigend nach Gesamt, Mehrfachantwort möglich. <n! = Fallzahlen < 30.

Sie haben Fragen zum Thema Cyberversicherung?

Wir helfen Ihnen gerne!
Bitte wenden Sie sich an:

cyberversicherung@hdi.de

7003001321-202306