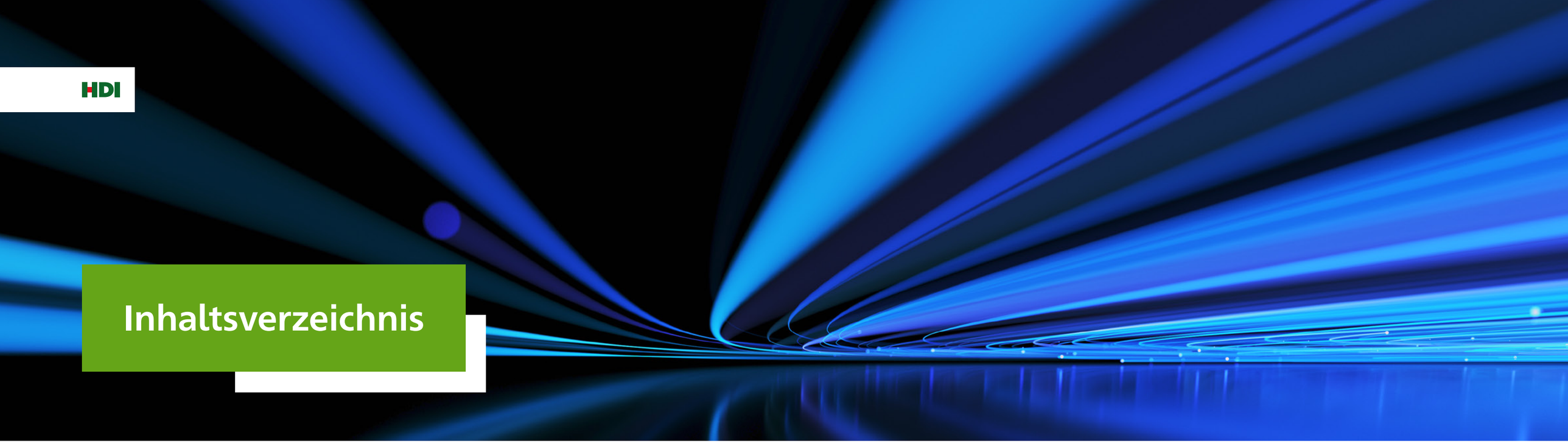
HDI Cyberstudie 2024

Effektives Cyberrisiko-Management in deutschen KMUs:
Die Herausforderungen verstehen und bewältigen.



Inhaltsverzeichnis

Vorwort

Sören Brokamp
Leiter Produktmanagement & Underwriting Cyber,
HDI Versicherung AG

Wir leben in einer Zeit, in der die Bedeutung der Cybersicherheit nicht mehr zu unterschätzen ist. Durch die zunehmende Vernetzung sind wir auf verschiedensten Ebenen von Cyberangriffen bedroht, sei es auf persönlicher, geschäftlicher oder gesellschaftlicher Ebene. Die finanziellen Schäden aufgrund von Cybervorfällen nehmen stetig zu. Es ist daher wichtiger denn je, sich mit den aktuellen Herausforderungen der Cyberlage auseinanderzusetzen und entsprechende Maßnahmen zu ergreifen.

Auch in der aktuellen HDI Cyberstudie 2024 stellen wir fest, dass eine effektive Prävention gegen Cyberangriffe ein maßgebliches Element zur Limitierung der entstehenden Kosten von Cyberschäden darstellt. Unternehmen, die proaktiv in ihre IT-Sicherheit investieren und wirksame Schutzmaßnahmen implementieren, können das Risiko von Cyberangriffen erheblich reduzieren. Dabei ist es wichtig, dass Unternehmen nicht nur auf technische Aspekte der Cybersicherheit achten, sondern auch ihre Mitarbeitenden sensibilisieren.

Leider sehen wir noch viel zu häufig eine gefährliche Nachlässigkeit bei Unternehmen. Viele nehmen die Gefahr von Cyberangriffen als etwas Abstraktes und nicht als eine reale Bedrohung wahr. Diese Einstellung kann verheerende Folgen haben, da sie Unternehmen anfällig für Angriffe macht. Um diesem Risiko entgegenzuwirken, ist es notwendig, ein Bewusstsein für die Risiken zu schaffen und die Implementierung von Sicherheitsmaßnahmen zur Priorität zu machen.

Eine sinnvolle Möglichkeit, das generelle Bedrohungsrisiko zu verstehen, zu verhindern und zu verringern, besteht in der Cyberversicherung. Diese Art von Versicherung bietet Unternehmen eine Absicherung im Falle eines Cyberangriffs, die mit einem wirksamen Schadenmanagement weit über die reine finanzielle Absicherung hinausgeht. Ferner unterstützt sie Unternehmen bei der Identifizierung und Bewertung vorhandener Schwachstellen sowie bei der Implementierung geeigneter Sicherheitsvorkehrungen.

Folglich ist für uns als Gesellschaft eine fortlaufende Auseinandersetzung mit der aktuellen Cyberlage ebenso unerlässlich wie die Implementierung effektiver Schutzmaßnahmen. Als Versicherer sehen wir uns in der Pflicht, unser Wissen mit Ihnen zu teilen. Wir verstehen unseren Einsatz auch als gesellschaftliche Verantwortung, um der Cybersicherheit in der Breite mehr Beachtung zu schenken und dem von uns gefundenen Effekt des „Cyber-Vergessens“ entgegenzuwirken. Ich wünsche Ihnen viel Spaß beim Lesen dieser spannenden Erkenntnisse aus unserer Studie.

Ihr **Sören Brokamp**
Leiter Produktmanagement & Underwriting Cyber,
HDI Versicherung AG

Methodik

Bereits zum dritten Mal wurde die HDI Cyberstudie durch das Marktforschungsinstitut Sirius Campus GmbH im Auftrag der HDI Versicherung AG durchgeführt*.

Dabei wurden Entscheider und Mitentscheider in IT- und Versicherungsfragen aus insgesamt **1.518 verschiedenen kleinen und mittelständischen Unternehmen** in Deutschland mittels Online-Interviews befragt. Die Stichprobe ist repräsentativ für deutsche KMUs. Um die Repräsentativität der Studie für die Zielgruppen der HDI zu gewährleisten, wurden pro Zielgruppe mindestens 100 Unternehmen befragt. Bei der Auswertung wurden die gewonnenen Daten nach Branche und Unternehmensgröße gewichtet.

Die gewichtete Stichprobe setzt sich in etwa zu je einem Drittel aus drei Klassifizierungen nach Mitarbeitenden zusammen, die für KMU verwendet werden. Dabei wurde unterschieden zwischen Kleinstunternehmen mit 0 bis 9 Beschäftigten, Kleinunternehmen mit 10 bis 49 Beschäftigten und mittleren Unternehmen mit 50 bis 250 Beschäftigten.

Insgesamt erlaubt die Studie eine **Hochrechnung der Ergebnisse auf die Gesamtheit der KMUs in Deutschland.**

Die Referenzstudien wurden in den Jahren 2021 und 2022 ebenfalls durch das Marktforschungsinstitut Sirius Campus GmbH im Auftrag der HDI Versicherung AG durchgeführt. Dabei wurden Ende 2021 518 und Ende 2022 702 Entscheider und Mitentscheider in KMUs befragt.

*Befragungszeitraum: Ende des Jahres 2023.

1.518 kleine und mittelständische Unternehmen mit Sitz in Deutschland
Basis: alle; Angaben in %

Risikowahrnehmung

Unternehmen zwischen hoher Aufmerksamkeit und Cyber-Vergessen.

Bereits ein Jahr nach einem Angriff setzt bei zwei Dritteln der KMUs „Cyber-Vergessen“ ein.

Die Wahrnehmung von Cyberrisiken bei KMUs steigt 2023 zwar leicht an, aber ein „Cyber-Vergessen” nach Angriffen offenbart eine gefährliche Diskrepanz zwischen Risikobewusstsein und tatsächlicher Bedrohung.

Die **allgemeine Risikowahrnehmung** bei KMUs ist im Vergleich zum Vorjahr wieder leicht angestiegen. Während im Jahr 2021 noch 53 % der Studienteilnehmer das **Risiko, Opfer eines Cyberangriffs** zu werden, für ihr Unternehmen als „hoch“ oder „eher hoch“ einschätzten, waren es im Folgejahr 2022 nur noch 41 %. Dies stützt die These, dass die Verantwortlichen von anderen Ereignissen wie der Energiekrise und der Inflation abgelenkt waren. So schätzen im Jahr 2023 49 % der Befragten das Risiko, Opfer eines Cyberangriffs zu werden, als „hoch“ oder „eher hoch“ ein. Das Thema **Cyber** ist jedoch nicht stärker in den Fokus gerückt als im Jahr 2021. Dies deutet auf eine Normalisierung der Risikowahrnehmung hin. Auffällig ist, dass die Befragten ihr eigenes Unternehmensrisiko tendenziell geringer einschätzen als das Risiko für andere KMU.

Auffallend ist, dass Studienteilnehmer von Unternehmen unmittelbar nach einem Angriff stark für das Thema Cyber sensibilisiert sind. Dies scheint jedoch nicht von Dauer zu sein, denn bereits nach kurzer Zeit ist die **Awareness** auf dem gleichen Niveau wie bei Unternehmen, die noch keinen Angriff erlebt haben. Dies zeigen die kombinierten Befragungsergebnisse der Studien 2023 und 2024. Hier zeigt sich, dass die Einschätzung der Befragten hinsichtlich des Angriffs- und Schadensrisikos für das eigene Unternehmen und für KMUs im Allgemeinen nach einem Angriff relativ schnell wieder abnimmt. So schätzen noch 57 % der Befragten, deren Unternehmen in den 12 Monaten vor der Befragung angegriffen wurde, das Angriffsrisiko für das eigene Unternehmen als „hoch“ oder „sehr hoch“ ein. Bereits ein Jahr nach dem Angriff sinkt dieser Wert auf 34 % und halbiert sich nach drei Jahren auf 27 %. Von einem „Cyber-Vergessen“ zu sprechen, ist demnach nicht übertrieben.

Die Ergebnisse zur Frage des **Schadensrisikos** verstärken dieses Bild. So schätzen 46 % derjenigen, deren Unternehmen, die in den 12 Monaten zuvor Opfer eines Cyberangriffs wurden, das Risiko, bei einem erneuten Angriff einen Schaden zu erleiden, als „hoch“ oder „eher hoch“ ein. Liegt der Angriff bereits ein bis zwei Jahre zurück, sind nur noch 39 % der Befragten dieser Meinung. Bei Unternehmen, die drei bis fünf Jahre keinen Cyberangriff erlitten haben, sind es nur noch 25 % der Befragten. Es wird deutlich, dass die Risikowahrnehmung bezüglich des Schadensrisikos abnimmt, je länger der Angriff zurückliegt.

Am deutlichsten sind die Ergebnisse bei der Einschätzung der Befragten zum **generellen Angriffsrisiko für KMUs durch Cyberangriffe.** Hier schätzen 67 % der Befragten, deren Unternehmen in den letzten 12 Monaten vor der Umfrage Opfer eines Cyberangriffs geworden sind, das Risiko eines Angriffs für KMUs als „hoch“ oder „sehr hoch“ ein. Bei Unternehmen, deren Cyberangriff ein bis zwei Jahre zurückliegt, sind es nur noch 36 %.

Risikowahrnehmung steigt – nachhaltige Awareness sinkt.

Zusammenfassend lässt sich anhand der Werte der Studie festhalten, dass die **allgemeine Risikowahrnehmung** im Vergleich zum Vorjahr wieder gestiegen ist. Der Fokus liegt nach Energiekrise, Inflation u. Ä. wieder stärker auf dem Thema Cyber. Auffällig ist, dass die Sensibilisierung für **Cyberangriffe** unmittelbar nach einem Angriff am höchsten ist und dann sukzessive abnimmt und in den Hintergrund tritt.

Nach dem Angriff ist vor der Vorsorge.

Cyberattacken auf den Mittelstand: mehr als die Hälfte betroffen.

Cyberattacken sind seit einigen Jahren nahezu allgegenwärtig. Dabei muss sich ein Cyberangriff nicht immer gezielt gegen ein bestimmtes Unternehmen richten, sondern kann eine IT-Infrastruktur auch zufällig treffen – Stichwort: Dynamite-Phishing. Auch der deutsche Mittelstand hat seine Erfahrungen damit gemacht. So gaben **51 % der befragten Unternehmen** an, in den letzten 5 Jahren Opfer eines solchen Angriffs geworden zu sein. Von diesen Unternehmen gaben 23 % an, zum Zeitpunkt des Angriffs nicht über eine **Cyberversicherung** verfügt zu haben.

Die häufigste Reaktion auf eine Attacke ist die Implementierung zusätzlicher **Präventivmaßnahmen.** Insgesamt ist die häufigste Maßnahme neben der grundsätzlichen Bereitstellung von zusätzlichem Budget für **IT-Ausgaben** (33 %) die Investition in neue Hard- und Software. Hier gaben 34 % der Studienteilnehmer an, in diesem Bereich aktiv geworden zu sein.

Cyberangriffe

Mensch weiterhin Risikofaktor Nr. 1, aber technische Angriffe holen auf.

Wie aber werden KMUs aktuell am häufigsten attackiert? Die Antwort darauf ist analog den Jahren zuvor noch immer die folgende: über den Faktor Mensch.

Die Mitarbeiter eines Unternehmens sind noch immer **das beliebteste Ziel von Cyberkriminellen.** Dabei attackieren die Angreifer vor allem via E-Mail. Aktuell gaben dementsprechend 27 % der Befragten an, dass ihr Unternehmen bereits via **Spam oder Phishing-Mail** attackiert worden sei. 41 % von diesen gaben an, dass die Attacke innerhalb der letzten zwölf Monate vor der Befragung eingetreten ist. Gleichzeitig gaben 98 % an, einen **Spam-Filter** zu nutzen. Dennoch stellt die Studie einen Anstieg dieser Angriffsmethode vom Vergleich zum Vorjahr fest. So hatten 2022 lediglich 15 % der Studienteilnehmer angegeben, auf diese Weise attackiert worden zu sein.

Die zweithäufigste Angriffsart, die Versendung von **Schadsoftware im E-Mail-Anhang,** betraf 25 % der Unternehmen. Hier ist die Quote der Unternehmen, die dabei innerhalb der letzten zwölf Monate betroffen waren, mit 45 % sogar noch etwas höher. Auch hier lässt sich im Vergleich zum Vorjahr eine deutliche Steigerung feststellen: Bei der Befragung 2022 hatten lediglich 13% dieser Unternehmen angegeben, auf diese Weise angegriffen worden zu sein.

Die dritthäufigste Schadenursache ist der **versehentliche Download von schädlichen Inhalten im Internet.** Hier wiesen 20 % der Unternehmen Erfahrungen mit dieser Art von Attacke auf. Auch hier fand eine Steigerung statt, denn 2022 hatten lediglich 14 % der Unternehmen angegeben, auf diese Art attackiert worden zu sein. Im Vergleich zu den noch häufigeren Angriffsarten ist die Quote der in den letzten zwölf Monaten vor der Befragung betroffenen Unternehmen mit 28 % etwas geringer.

Mensch bleibt Einfallstor Nummer 1, technische Angriffe nehmen zu.

Zusammenfassend lässt sich also sagen, dass wie auch im Vorjahr die Top-3-Arten, KMUs zu attackieren, alle den **Menschen als primäres Ziel** identifizieren. Insgesamt nehmen diese Cyberangriffe auch in der Häufigkeit zu, wie sich aus den Jahresvergleichen ablesen lässt.

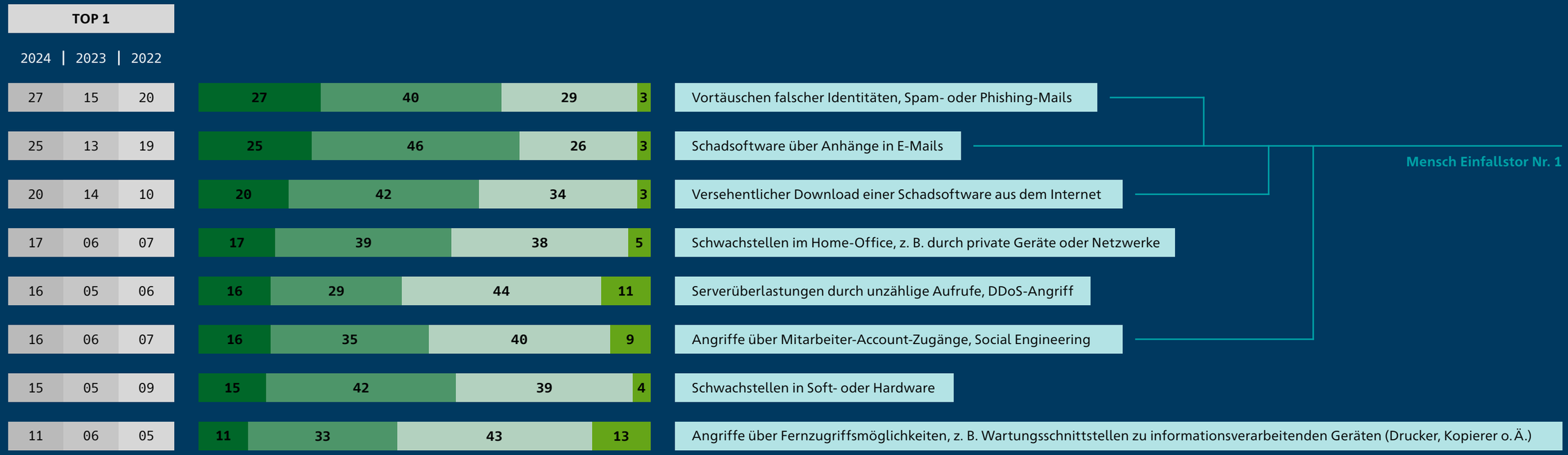
Gemessen an der Häufigkeit der Attacken folgen rein technisch basierte Angriffsarten, die sich vor allem auf Schwachstellen im Home-Office konzentrieren. Bei diesen werden vor allem Schwächen in Heimnetzwerken, bei Routern oder aber den privaten Geräten genutzt, um in den IT-Bereich von Unternehmen zu gelangen. 17 % der Studienteilnehmer gaben an, bereits Erfahrungen mit dieser Art der Attacke gemacht zu haben. Gemessen am Vorjahr, in dem dieser Wert bei 6 % lag, setzt sich auch hier der Trend der Steigerung signifikant fort.

Ähnlich verhält es sich mit der fünfthäufigsten Angriffsart, dem **Distributed Denial of Service (kurz DDoS).** Hier gaben 16 % der Befragten an, eine Attacke festgestellt zu haben, und auch hier ist im Vergleich zum Vorjahr (5 %) ein signifikanter Anstieg zu verzeichnen. Auf den weiteren Plätzen im Ranking folgen die Angriffsarten **Social Engineering,** worüber 16 % bereits attackiert wurden, das Ausnutzen von **Hard- und Softwareschwachstellen,** denen 15 % bereits zum Opfer fielen, und Angriffe über **Remote-Schnittstellen** wie Fernzugriffe oder Wartungsschnittstellen auf Geräte und Maschinen. Nach 6 % im Vorjahr mussten nun 11 % der Teilnehmer bereits eine solche Attacke auf ihr Unternehmen feststellen.

Zusammenfassend lassen sich also zwei Punkte herausstellen. Der Mensch bleibt weiterhin das Einfallstor Nr. 1 für Angreifer. Zeitgleich haben aber auch technische Angriffsszenarien an Bedeutung gewonnen und Unternehmen getroffen.

Erfahrung mit Cyberattacken

Sind Ihnen folgende Formen von Cyberattacken bekannt?



Die Jahresangaben der Grafik benennen die entsprechende Studie; die Datenerhebung erfolgte jeweils Ende des vorhergehenden Jahres.

Basis: KMUs mit einer Cyberattacke; Angaben in %
(Ranking nach Top 1: „Unser Unternehmen wurde so bereits attackiert")

- Unser Unternehmen wurde so bereits attackiert [100]
- Ist für uns ein relevantes Risiko [67]
- Ich habe davon gehört [33]
- Kenne ich nicht [0]

Cyberschäden

Steigende Kosten durch Cyberattacken.

Durch Cyberschäden verursachte Kosten steigen drastisch.

Präventive Maßnahmen können die finanziellen Schäden erheblich reduzieren.

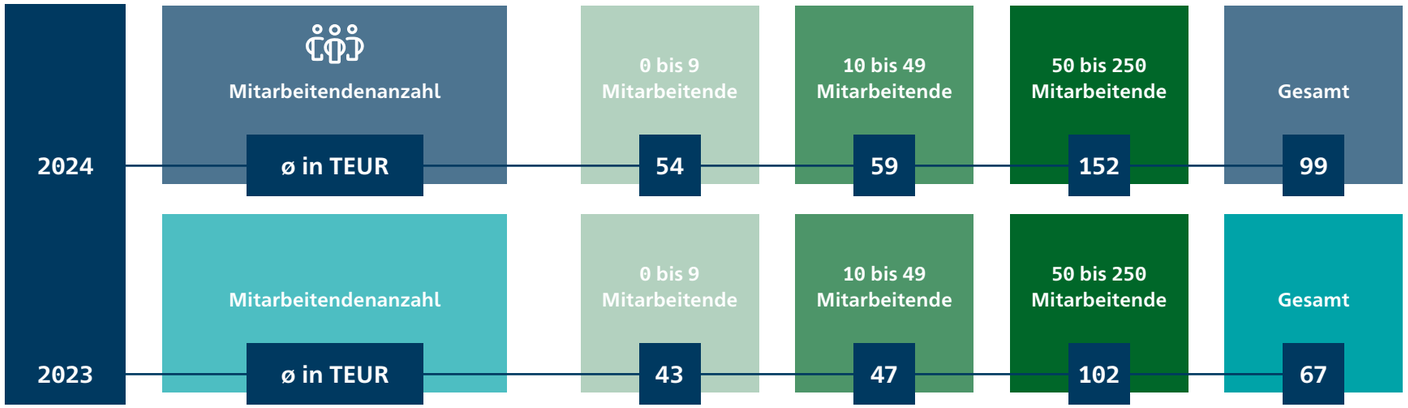
Cyberschäden werden für Unternehmen immer kostspieliger und können existenzbedrohende Ausmaße annehmen. So zeigen die Ergebnisse der HDI Cyberstudie 2024, dass die durchschnittlichen Kosten für einen Cyberschaden in diesem Jahr um circa 47 % – auf rund 99.000 € (98.643 €) – angestiegen sind. Im Jahr zuvor betrug der durchschnittliche Schaden noch knapp 67.000 €.

Eine nähere Betrachtung zeigt, dass die Höhe des finanziellen Schadens mit der Größe des Unternehmens zunimmt.

Insbesondere IT-Dienstleister und Software-Anbieter erleiden hohe finanzielle Schäden infolge einer Cyberattacke. Hier beträgt der Durchschnittsschaden circa 215.000 €. Aber auch das produzierende Gewerbe verzeichnete Verluste in Höhe von durchschnittlich circa 135.000 €.

Unternehmen können jedoch die finanziellen Schäden stark reduzieren, wenn präventive Maßnahmen eingesetzt werden.

Cyberschäden nach Unternehmensgröße



Die Jahresangaben der Grafik benennen die entsprechende Studie; die Datenerhebung erfolgte jeweils Ende des vorhergehenden Jahres.

Ein Cyberschaden ist, insbesondere für Kleinstunternehmen, existenzgefährdend.

Cyberkriminalität trifft Kleinstunternehmen härter: durch größere Schäden im Verhältnis zum Gesamtumsatz und längere Betriebsunterbrechungen.

Die Ergebnisse zeigen: Je größer ein Unternehmen ist, desto wahrscheinlicher ist es, dass es von **Cyberkriminellen** angegriffen wird. Bemerkenswert ist jedoch, dass ein Angriff bei kleinen Unternehmen mit 10 bis 49 Mitarbeitern am häufigsten zu einem Schaden führt (33 %). Bei mittleren Unternehmen ist dies nur bei 30 % der betroffenen Unternehmen der Fall.

Finanziell besonders **bedrohlich ist ein Cyberschaden für Kleinstunternehmen.** Das zeigt die aktuelle HDI Cyberstudie, wenn man die Schadenhöhen ins Verhältnis mit dem Umsatz der betroffenen Unternehmen setzt: Bei Unternehmen mit einem Umsatz von weniger als 500.000 € ist der finanzielle Schaden eines Cyberangriffs im Verhältnis zum Umsatz mit durchschnittlich 9 % am höchsten. Und bei Unternehmen mit einem Umsatz zwischen 500.000 € und 2,5 Mio. € macht der finanzielle Schaden im Durchschnitt noch 4% des Umsatzes aus. Unternehmen mit einem Umsatz von über 20 Mio. € haben dagegen nur knapp 1% ihres Umsatzes für einen Cyberschaden aufzuwenden.

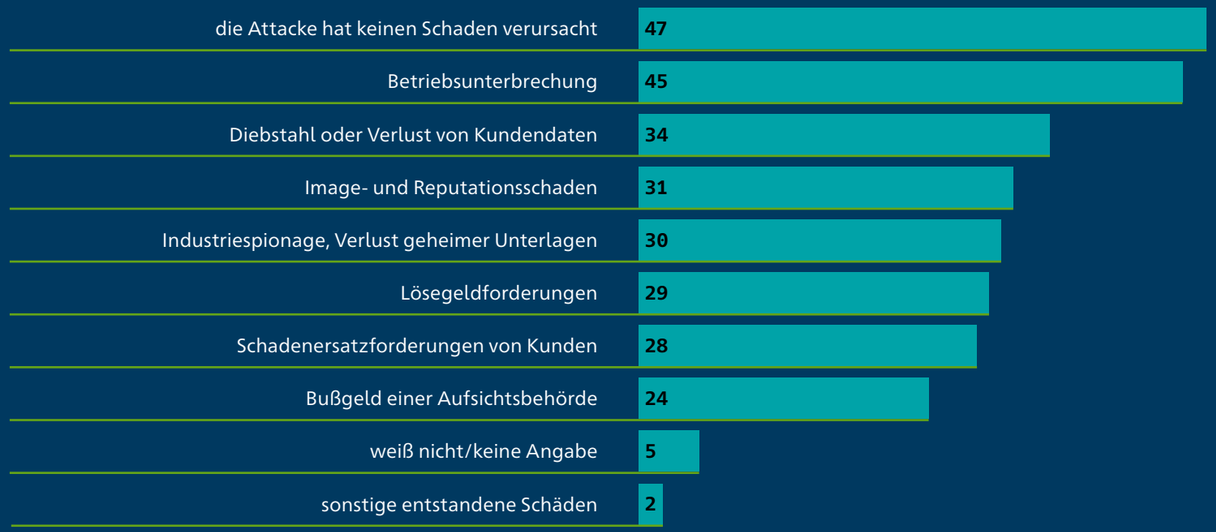
Längere Betriebsunterbrechungen und größere Datenverluste

Die durchschnittliche Betriebsunterbrechung aufgrund eines Cyberangriffs hat sich im Vergleich zum Vorjahr nicht geändert. Im Durchschnitt können die Unternehmen nach einem Cyberangriff erst nach 4,2 Tagen wieder auf ihre Systeme zugreifen. Auffällig ist, dass kleine Unternehmen mit einem Jahresumsatz zwischen 500.000 € und 2.500.000 € besonders gefährdet sind. Die Zahlen zeigen, dass sie erst nach **durchschnittlich 5,5 Tagen** wieder auf ihre Systeme zugreifen können. Im Vergleich zu mittleren Unternehmen (10 bis 25 Mio. €) sind das ganze zwei Tage mehr, die kleine Unternehmen nicht arbeiten können.

Übersicht Schäden

Welche Schäden sind bei der Cyberattacke entstanden? Bei mehreren Attacken: Was waren die Folgen der letzten?

Erlittene Schäden



Basis: KMUs mit einer Cyberattacke; Angaben in %

Cyberkriminelle zielen bei ihren Angriffen offenbar vor allem auf den Diebstahl von Kundendaten (34 %) und Betriebsunterbrechungen (45 %) der angegriffenen Unternehmen. Dies sind laut HDI Cyberstudie die häufigsten Schäden bei einem erfolgreichen Cyberangriff.

Erwähnenswert ist auch, dass der häufigste Grund für eine Betriebsunterbrechung auf die Mitarbeiter zurückzuführen ist. So haben 32 % der Unternehmen als Grund für die Betriebsunterbrechung den versehentlichen Download durch Mitarbeiter aus dem Internet genannt. Die folgenschwersten Angriffsmuster für eine Betriebsunterbrechung variieren allerdings je nach Unternehmensgröße. So wurde im vorangegangenen Kapitel bereits erwähnt, dass technische Angriffe auf dem Vormarsch sind. Dies zeigt sich insbesondere bei Kleinstunternehmen (0 bis 9 Mitarbeiter). Sie erwähnen besonders häufig technische Angriffe als Auslöser der Betriebsunterbrechung.

Zunehmende Zahl von Bußgeldern macht sich auch im Durchschnittsschaden bemerkbar.

Neben den Herausforderungen einer Betriebsunterbrechung hat sich die Anzahl der von Aufsichtsbehörden verhängten Bußgelder in den letzten drei Jahren um 266 % massiv erhöht. Im aktuellen Jahr gaben bereits 24 % der betroffenen Unternehmen an, aufgrund erfolgreicher Cyberattacken Bußgelder zu entrichten (2023: 18 %; 2022: 9 %). Dies spiegelt sich auch in dem gestiegenen Durchschnittsschaden wider.

Als Reaktion auf einen Cyberschaden investieren viele Unternehmen verstärkt in Cybersicherheit. Insbesondere wird in präventive Maßnahmen (35 %) sowie neue Soft- und Hardware (34 %) investiert.

Prävention

Prävention ist immer noch besser als Reaktion.

Prävention als Schlüssel gegen Cyberkriminalität

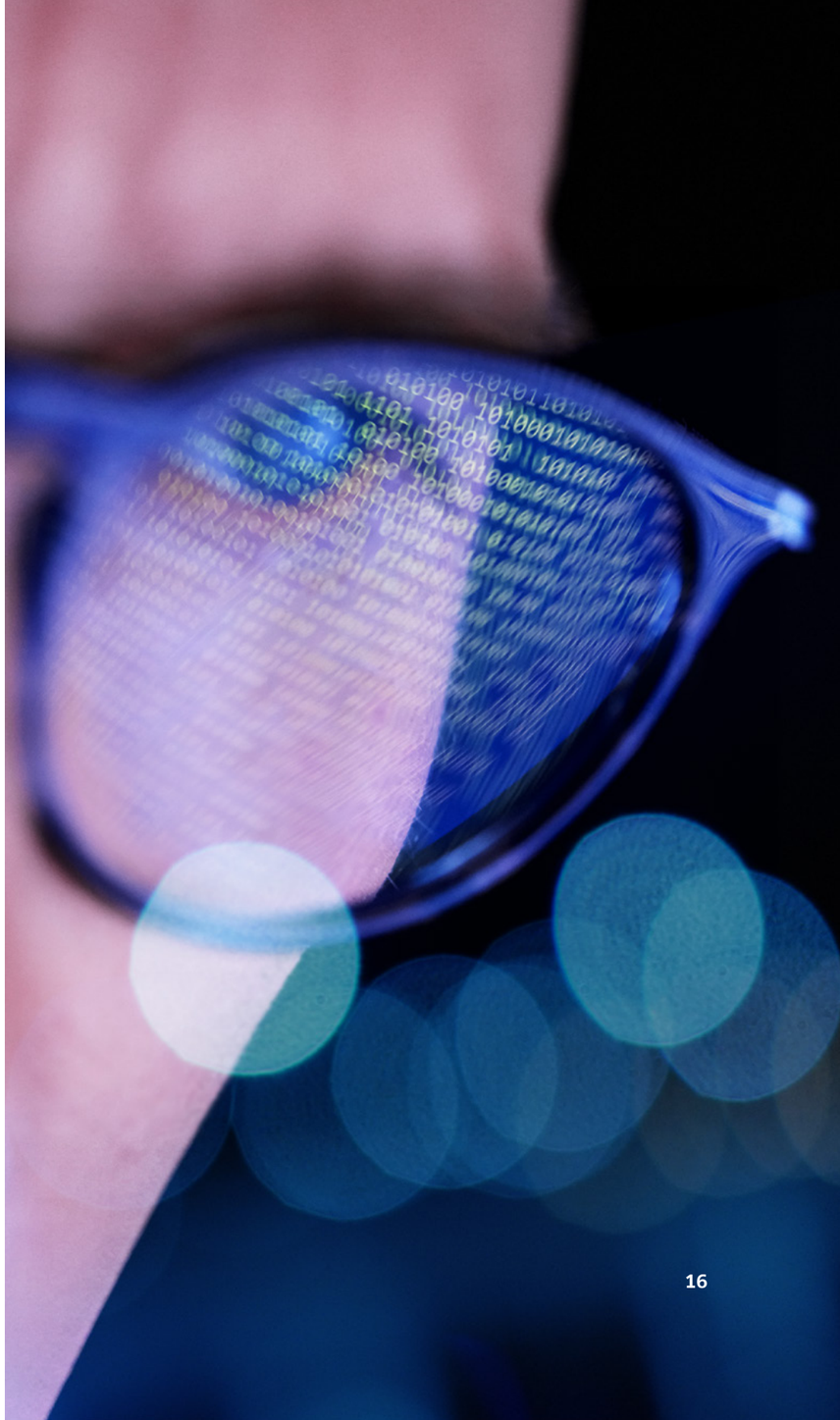
Zunehmender Fokus liegt auf proaktiven Strategien gegen Cyberbedrohungen.

Im digitalen Zeitalter, in dem Cyberkriminalität ein ständig wachsendes Problem darstellt, wird Prävention immer entscheidender. Nicht nur entscheidend bei der Vermeidung von Cyberschäden, sondern auch, um trotzdem eingetretene **Cyberschäden signifikant** zu reduzieren. Dies zeigen die Ergebnisse der HDI Cyberstudie. Wie bereits in den letzten Jahren sind Unternehmen mit einem hohen Umsetzungsgrad von präventiven Maßnahmen – ganz gleich ob technisch oder organisatorisch – im Hinblick auf die Cybersicherheit signifikant besser da als solche, die Präventionsmaßnahmen vernachlässigen. Nach wie vor sind vorbeugende Maßnahmen gegen Cyberangriffe von entscheidender Bedeutung , um Cyberschäden zu verhindern oder zumindest zu minimieren.

Mehr Vorbeugung und Mitarbeitersensibilisierung

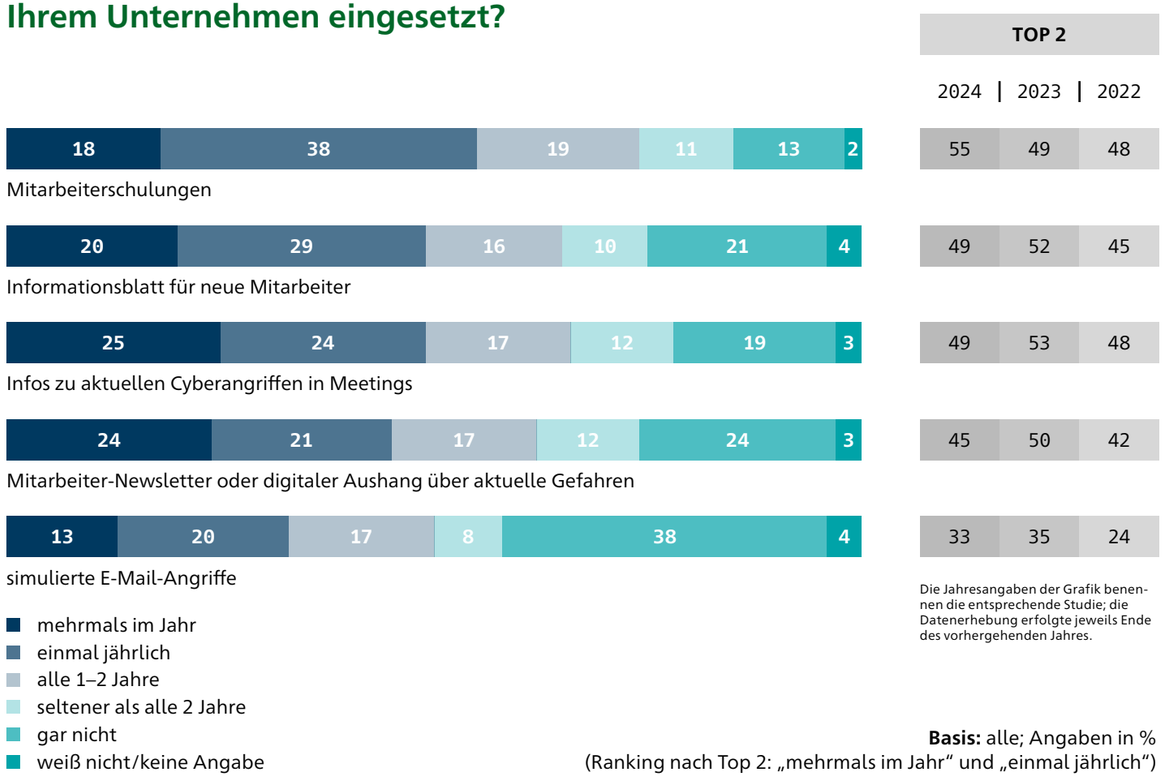
Immer mehr Unternehmen verankern präventive Maßnahmen in ihrer Informationssicherheitsstrategie. So ist insgesamt eine positive Entwicklung in allen Bereichen zu verzeichnen. Dies ist insbesondere bemerkenswert, da im letzten Jahr noch ein leichter Rückgang bei vereinzelten Präventionsmaßnahmen erkennbar war. So geben in der aktuellen Untersuchung 70 % der Befragten an, in ihrem Unternehmen **organisatorische Präventionsmaßnahmen** wie z. B. Passwortrichtlinien anzuwenden. Im letzten Jahr setzten nur 63 % der Unternehmen auf diese Maßnahmen.

Darüber hinaus legen die Verantwortlichen in Unternehmen vermehrtes Augenmerk auf die Qualifikation von Mitarbeitern. So ist im Jahresvergleich ein Anstieg von 7 Prozentpunkten zu verzeichnen. 71 % der befragten Unternehmen sensibilisieren ihre Mitarbeiter kontinuierlich (2023: 64 %). Besonders hervorzuheben ist hier die regelmäßige Mitarbeiterschulung im Hinblick auf aktuelle Cyberbedrohungen und die Förderung sicherer Verhaltensweisen, die um weitere 6 Prozentpunkte gestiegen ist (2024: 55 %; 2023: 49 %).



Prävention: Mitarbeiterverhalten

Wie regelmäßig werden diese Präventionsmaßnahmen für Cybersicherheit im Bereich Mitarbeiterverhalten in Ihrem Unternehmen eingesetzt?



Die Jahresangaben der Grafik benennen die entsprechende Studie; die Datenerhebung erfolgte jeweils Ende des vorhergehenden Jahres.

Basis: alle; Angaben in %
(Ranking nach Top 2: „mehrmals im Jahr“ und „einmal jährlich“)

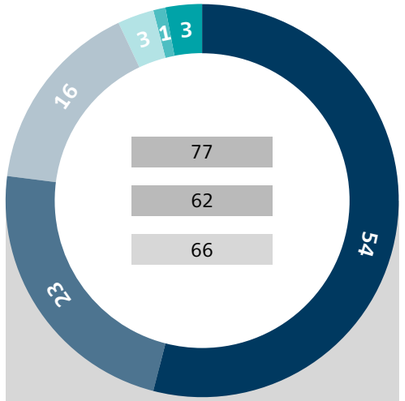
Technische Sicherheitsmaßnahmen auf dem Vormarsch

Im Bereich der technischen Maßnahmen wurden insbesondere die klassischen Maßnahmen wie **Spam-Schutz und Firewalls** von nahezu jedem Unternehmen eingesetzt (2024: 99 %; 2023: 77 %). Hervorzuheben sind aber auch weitere technische Maßnahmen, die an Verbreitung gewonnen haben. So setzen mittlerweile 3 von 4 Unternehmen (77 %) auf den **verschlüsselten Zugriff auf das Unternehmensnetzwerk –** z. B. über ein VPN –, um ihre Firmendaten vor Dritten zu schützen. Im letzten Jahr setzten nur 62 % der befragten Unternehmen auf diese Maßnahme.

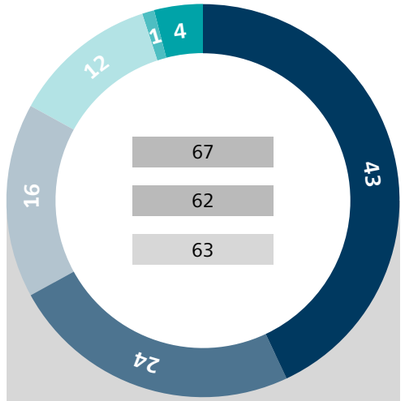
Auch die eigene Website des Unternehmens wird besser vor Angreifern geschützt. So setzten inzwischen 56 % (2023: 50 %) der befragten Unternehmen einen Schutz ihrer Homepage vor der Nichtverfügbarkeit (DDoS-Schutz) ein.

Maßnahmen zur Verhinderung unbefugter Zugriffe

Wie werden die folgenden technischen Maßnahmen zur Verhinderung unbefugter Zugriffe in Ihrem Unternehmen umgesetzt?



verschlüsselter Zugriff auf das Unternehmensnetzwerk, VPN

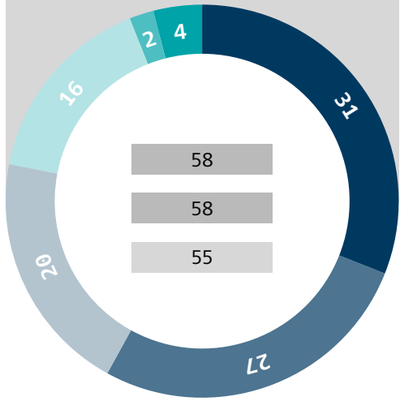


zentrale Verwaltung von Nutzer-rechten, Benutzermanagement

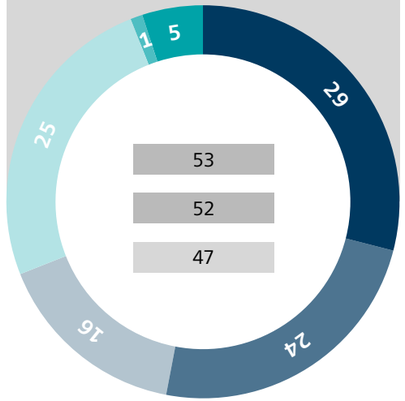
Verschlüsseln von Daten beim Speichern oder Versenden

TOP 2	
2024	77 / 67 / 61
2023	62 / 62 / 62
2022	66 / 63 / 51

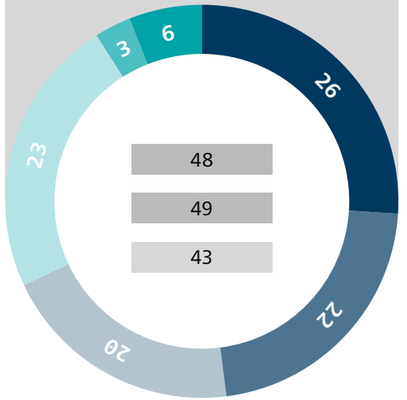
Multi-Faktor-Authentifizierung



zentrale Verwaltung mobiler Endgeräte



Aufteilung des Netzwerks in getrennte Subnetze, segmentierte Netzwerke



TOP 2	
2024	58 / 53 / 48
2023	58 / 52 / 49
2022	55 / 47 / 43

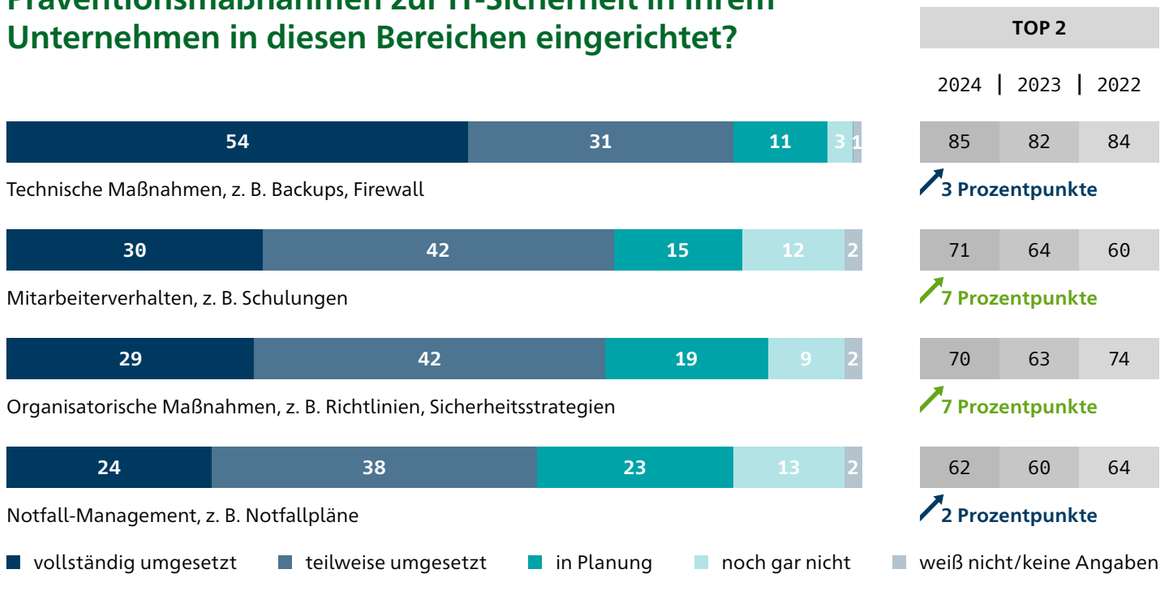
- dauerhafter/täglicher Einsatz
- Einsatz bei Bedarf
- in Planung
- bekannt, aber keine Nutzung
- kennen wir nicht
- weiß nicht/keine Angabe

Basis: alle; Angaben in %
(Top 2: „dauerhafter/täglicher Einsatz“ und „Einsatz bei Bedarf“)

Die Jahresangaben der Grafik benennen die entsprechende Studie; die Datenerhebung erfolgte jeweils Ende des vorhergehenden Jahres.

Gezielte Prävention

Wie umfangreich haben Sie bereits Präventionsmaßnahmen zur IT-Sicherheit in Ihrem Unternehmen in diesen Bereichen eingerichtet?



Basis: alle; Angaben in %
(Top 2: „vollständig umgesetzt“ und „teilweise umgesetzt“)

Die Jahresangaben der Grafik benennen die entsprechende Studie; die Datenerhebung erfolgte jeweils Ende des vorhergehenden Jahres.

Starker Fokus auf technischer Prävention.

Sensibilisierung von Mitarbeitenden nimmt weiter zu.

Organisatorische Präventionsmaßnahmen gewinnen wieder an Relevanz.

Investitionen ins Notfall-Management bleiben auf gleichem Niveau.

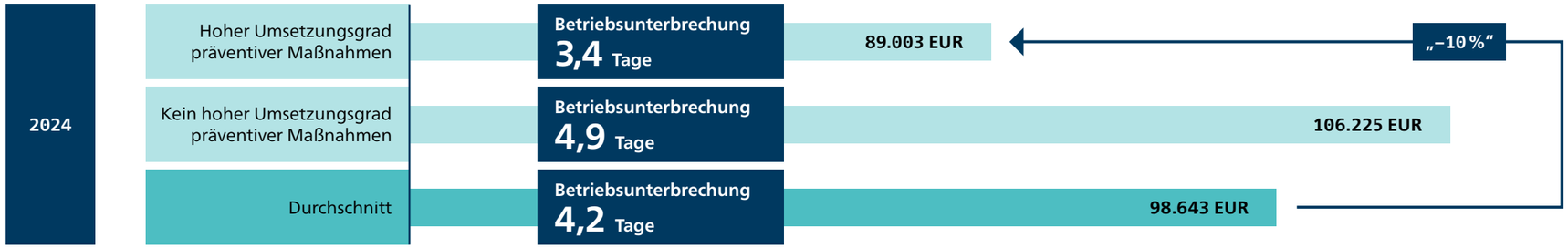
Unternehmen mit einem hohen Umsetzungsgrad von präventiven Maßnahmen: 36 Stunden schneller wieder einsatzbereit.

Je höher der Umsetzungsgrad der präventiven Maßnahmen, desto geringer die Kosten und Ausfallzeiten

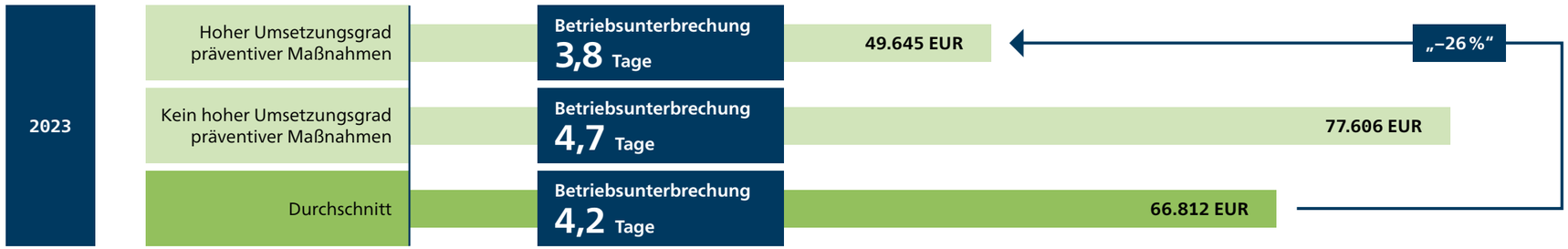
Eine hohe Umsetzungsquote von präventiven Maßnahmen kann erheblich dazu beitragen, die finanziellen Auswirkungen von Cyberschäden zu reduzieren. Die Ergebnisse der HDI Cyberstudie 2024 zeigen, dass Unternehmen, die vermehrt in ihre Cybersicherheit investieren und präventive Maßnahmen ergreifen, durchschnittlich 10 % weniger Kosten für die Bewältigung eines Cyberangriffes aufwenden als Unternehmen, die präventiven Maßnahmen einen weniger hohen Stellenwert beimessen. In Zahlen ausgedrückt, erleiden Unternehmen mit einem geringen Umsetzungsgrad von präventiven Maßnahmen einen **durchschnittlichen Schaden von circa 106.000 €,** während Unternehmen mit einem hohen Umsetzungsgrad einen deutlich geringeren **Durchschnittsschaden von circa 89.000 €** erfahren. Zur Erinnerung: Der durchschnittliche Cyberschaden über alle Unternehmen hinweg im Jahr 2024 beträgt laut der HDI Cyberstudie 98.643 €. Dabei gab es bei den befragten Unternehmen, auch solche die einen Cyberschaden von 500.000 € und mehr erlitten haben.

Dies verdeutlicht unter anderem den finanziellen Nutzen einer hohen Umsetzungsrate von präventiven Maßnahmen. Darüber hinaus zeigt sich, dass Unternehmen mit einer hohen Umsetzungsquote von präventiven Maßnahmen auch eine kürzere Betriebsunterbrechung nach einem Cyberangriff haben. Während Unternehmen mit einem weniger hohen Umsetzungsgrad im Durchschnitt knapp **fünf Tage (4,9)** benötigen, können Unternehmen mit einer hohen Umsetzungsquote den Schaden schneller beheben und nach etwas mehr als **drei Tagen (3,4)** ihre Geschäftsaktivitäten wieder aufnehmen. Dies bedeutet eine Verkürzung der Betriebsunterbrechung um **36 Stunden oder 44 %.** Der Durchschnitt über alle Unternehmen liegt hier bei **4,2 Tagen Betriebsunterbrechung.**

Betriebsunterbrechung 2024



Betriebsunterbrechung 2023



Die Jahresangaben der Grafik benennen die entsprechende Studie; die Datenerhebung erfolgte jeweils Ende des vorhergehenden Jahres.

Richtlinien und Patch-Management besonders effektiv zur Risikominimierung

Proaktive Sicherheitsmaßnahmen minimieren Cyberschäden und schützen Unternehmensreputation.

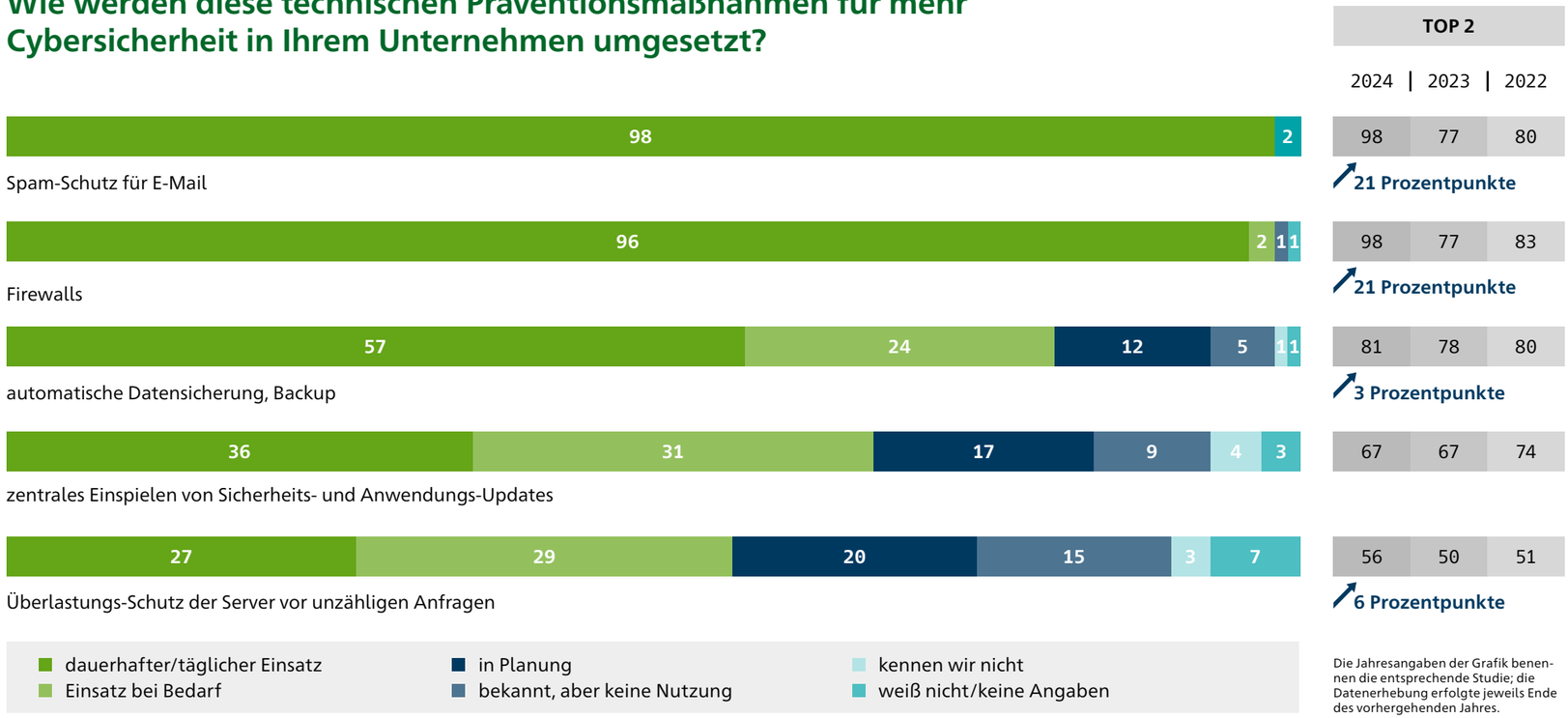
Angesichts der steigenden Zahl von Cyberangriffen ist es unerlässlich, dass die Vorbeugung Teil jeder Informationssicherheitsstrategie ist. Unternehmen sollten proaktiv Präventivmaßnahmen ergreifen, um ihre Systeme und Daten zu schützen.

Durch eine hohe Umsetzungsrate solcher Maßnahmen können die **finanziellen, betrieblichen und reputationsschädlichen Auswirkungen** von Cyberschäden minimiert oder sogar verhindert werden. Die Vorteile liegen auf der Hand – **Prävention ist besser als Reaktion.**

Als besonders wirksam haben sich ein funktionierendes Patch-Management sowie IT-Sicherheits- und Passwortrichtlinien erwiesen. Insbesondere die auf die Mitarbeiter ausgerichteten IT-Sicherheits- und Passwortrichtlinien **reduzieren die Eintrittswahrscheinlichkeit eines Schadens um 30 %.** Aber auch ein funktionierendes Patch-Management sollte in jedem Unternehmen implementiert sein. **Dieses reduziert die Schaden-Eintrittswahrscheinlichkeit um 23 %.**

Umsetzungsrate der technischen Präventionsmaßnahmen

Wie werden diese technischen Präventionsmaßnahmen für mehr Cybersicherheit in Ihrem Unternehmen umgesetzt?



TOP 2		
2024	2023	2022
98	77	80
↗ 21 Prozentpunkte		
98	77	83
↗ 21 Prozentpunkte		
81	78	80
↗ 3 Prozentpunkte		
67	67	74
56	50	51
↗ 6 Prozentpunkte		

Die Jahresangaben der Grafik benennen die entsprechende Studie; die Datenerhebung erfolgte jeweils Ende des vorhergehenden Jahres.

Basis: alle; Angaben in %
(Ranking nach Top 2: „dauerhafter/täglicher Einsatz“ und „Einsatz bei Bedarf“)

KI und KMUs

Risiken und Chancen für Unternehmen.

Auf dem Weg zur Künstlichen Intelligenz

2023 war das Jahr der Künstlichen Intelligenz (kurz: KI). Neben ChatGPT als wohl aktuell prominenteste KI-Lösung entstehen auch immer wieder **neue Lösungen für ein breiter werdendes Anwendungsgebiet.** Dem voran geht häufig jedoch die Frage, was eine Künstliche Intelligenz überhaupt charakterisiert. Das Fraunhofer Institut beschreibt die KI wie folgt: „Künstliche Intelligenz (KI) ist ein Teilgebiet der Informatik. Sie imitiert menschliche kognitive Fähigkeiten, indem sie Informationen aus Eingabedaten erkennt und sortiert. Diese Intelligenz kann auf programmierten Abläufen basieren oder durch maschinelles Lernen erzeugt werden."*

Eine KI besitzt also zunächst einmal die Fähigkeit, Informationen zu verarbeiten, und kann dabei sowohl einzelne Inhalte als auch große Mengen behandeln. Im Rahmen ihrer Funktionen werden anhand der eingegebenen Informationen Ergebnisse erzeugt, wobei Entscheidungskriterien vorab entweder programmiert werden oder sich aus der Komponente des maschinellen Lernens ergeben. Auch das maschinelle Lernen wird vom Fraunhofer Institut in der eigenen Studie **„Maschinelles Lernen. Eine Analyse zu Kompetenzen, Forschung und Anwendung" beschrieben. Hier lautet die Definition: „Maschinelles Lernen bezweckt die Generierung von ‚Wissen' aus ‚Erfahrung',** indem Lernalgorithmen aus Beispielen ein komplexes Modell entwickeln. Das Model und damit die automatisch erworbene Wissensrepräsentation, kann anschließend auf neue, potenziell unbekannte Daten derselben Art angewendet werden."**

Das maschinelle Lernen ist dementsprechend die Komponente, die kognitive Verhaltensweisen imitiert, da hier andere Gewichtungen oder gänzlich neue Entscheidungskriterien entstehen können. Die Menge der Daten, die zur Generierung und Änderung der Entscheidungskriterien führt, ist demnach mit der „Erfahrung" der KI gleichzusetzen.

*Quelle: https://www.iks.fraunhofer.de/de/themen/kuenstliche-intelligenz.html.
**Quelle: https://www.bigdata-ai.fraunhofer.de/content/dam/bigdata/de/documents/Publikationen/Fraunhofer_Studie_ML_201809.pdf.

Chancen > Risiken

Erstmals wurden im Rahmen der HDI Cyberstudie die Bedeutung und Anwendung von KI bei kleinen und mittelständischen Unternehmen untersucht. Die Ergebnisse sind dabei durchaus vielschichtig. Es werden zwar **vielfach Chancen** gesehen, aber es kann auch **eine gewisse Skepsis bis hin zu Ängsten** beobachtet werden.

Insgesamt überwiegt der Anteil der Studienteilnehmer, die durch KI eher Chancen als Risiken für das eigene Unternehmen sehen. So sieht knapp die Hälfte (49 %) große Chancen oder KI eher als Chance. Ein Drittel (33 %) hingegen sieht eher Risiken oder sogar große Risiken. 14 % der Unternehmen sehen keine Auswirkungen von KI auf das eigene Unternehmen und 5 % sehen sich nicht in der Lage, ein Urteil hierzu zu fällen.

Feststellbar ist dabei die unterschiedliche Wahrnehmung in Abhängigkeit von der Unternehmensgröße: 30 % der Teilnehmer von **kleinen Unternehmen** mit max. vier Mitarbeitern **sehen das Unternehmen gar nicht betroffen.** Bei **mittleren Unternehmen mit 50 bis 250** Mitarbeitenden sehen nur noch **7 % keine Auswirkungen** auf das eigene Unternehmen. Auffällig ist auch, dass viele der Befragten sich nicht eindeutig im Hinblick auf Chance oder Risiko festlegen. So sehen auf Gesamtebene nur **13 % große Chancen** und nur **6 % große Risiken.**

Auswirkungen der KI auf Unternehmen

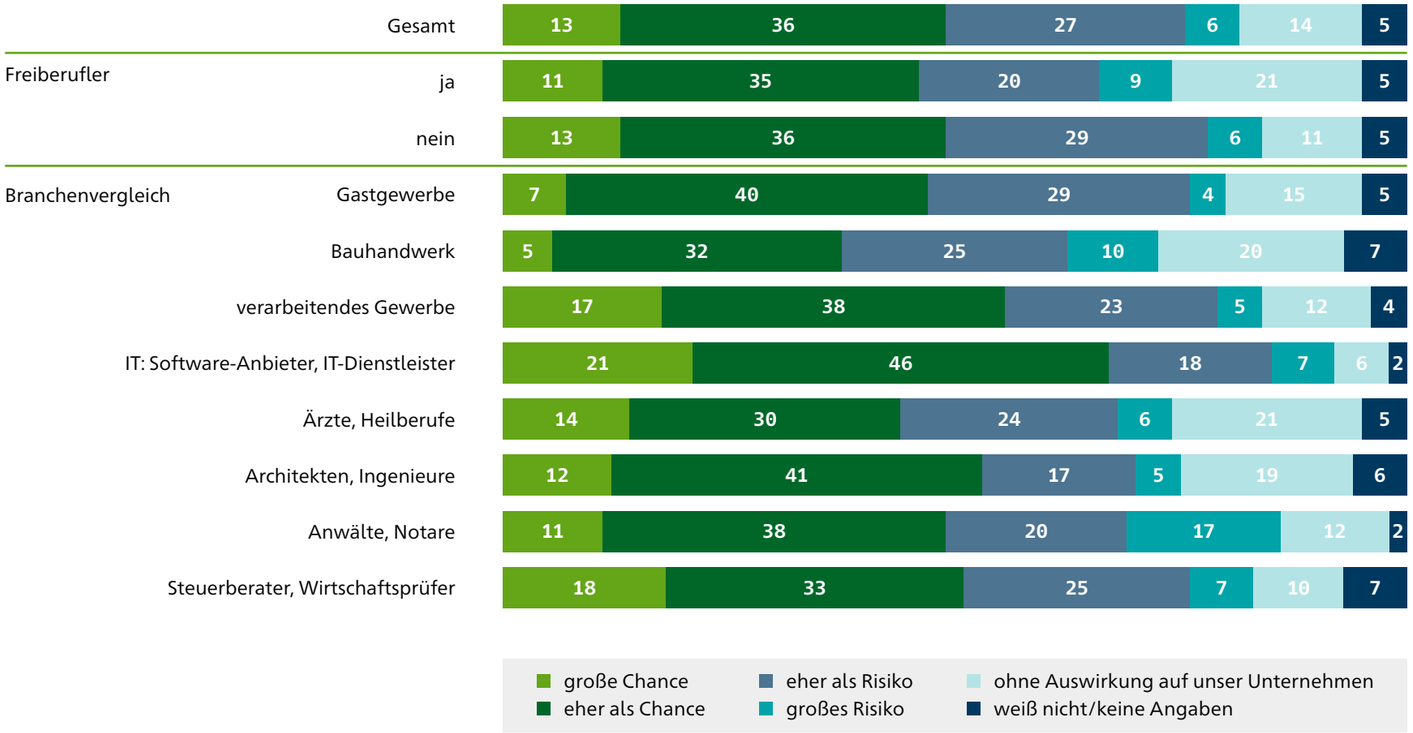
Wie bewerten Sie die Auswirkungen Künstlicher Intelligenz auf Ihre Unternehmensentwicklung insgesamt?

Basis: alle; Angaben in %

IT-Branche optimistisch – Bauhandwerk sieht sich nicht betroffen.

Branchenvergleich bei KI-Chancen

Im Branchenvergleich zeigen sich einige interessante Unterschiede: Besonders chancenorientiert sind die IT-Branche (67 % sehen eher Chancen oder große Chancen), das verarbeitende Gewerbe (55 %) und die Architekten/ Ingenieure (53 %). **Das Bauhandwerk sieht sich mit einem Anteil von 20 % besonders häufig gar nicht betroffen** und sieht gleichzeitig am seltensten Chancen für das eigene Unternehmen (37 %).



Basis: alle; Angaben in %

KI auf dem Vormarsch

KI-Anwendungen kommen bereits in zahlreichen Bereichen zum Einsatz.

In der HDI Cyberstudie wurde auch untersucht, in welchen Unternehmensbereichen bereits KI-Anwendungen zum Einsatz kommen.

Auffällig ist hierbei, dass es keine bestimmten Bereiche zu geben scheint, die eine Art Vorreiterrolle einnehmen oder prädestiniert für den Einsatz von KI erscheinen. So kommen alle elf abgefragten Bereiche auf eine **Nutzungsquote zwischen 10 und 12 %.**

KI-Implementierung

Wie intensiv beschäftigt sich Ihr Unternehmen bereits mit Künstlicher Intelligenz für die folgenden Unternehmensbereiche?

Basis: alle; Angaben in %
(Ranking nach Top 2: „bereits in der Nutzung“ und „in der Umsetzung“)

Die großen Player dominieren.

Bei der Frage, mit welchen Anbietern von KI schon zusammengearbeitet wird, werden vor allem drei genannt: am häufigsten **ChatGPT, gefolgt von Google und Microsoft.** Auch IBM wird häufiger genannt. Alle weiteren Anbieter wurden nur vereinzelt genannt, was nicht überrascht, da neben den großen Playern auch viele kleinere Unternehmen und Start-ups Lösungen anbieten.

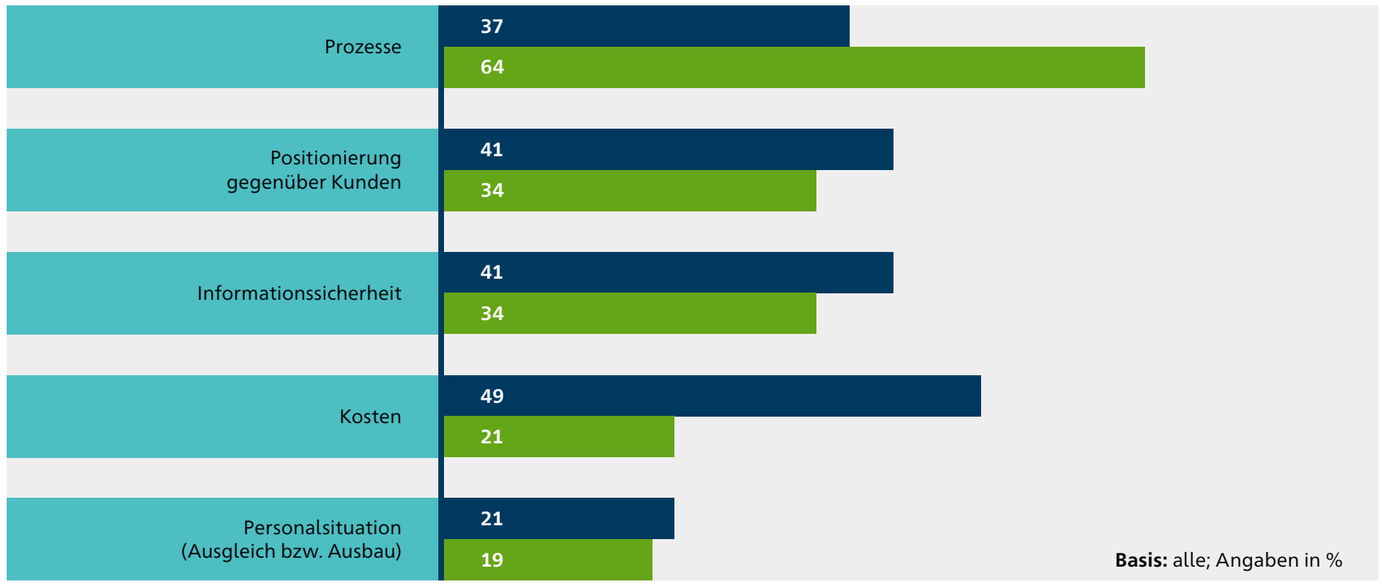
Chancen überwiegen, aber Bedenken bei Kosten und Kundenservice

Zu Beginn dieses Kapitels wurde festgestellt, dass aus Sicht der KMUs die Chancen für den Einsatz von KI in der Gesamtbetrachtung überwiegen. In der Detailbetrachtung wird jedoch deutlich, dass in Bezug auf konkrete Aspekte die Risiken durchaus deutlich schwerer wiegen können als die gesehenen Chancen. So wird KI in der allgemeinen Diskussion häufig mit großen Einsparpotenzialen in Verbindung gebracht. Etwa die Hälfte der in der Studie Befragten (49 %) sieht jedoch vor allem Risiken auf der Kostenseite. Nur etwa jedes fünfte Unternehmen (21 %) sieht den Einsatz von KI im Hinblick auf die Kostensituation als Chance.

Ein umgekehrtes Bild ergibt sich bei der Einschätzung der Auswirkungen von KI auf die Prozesse in den Unternehmen: So sehen knapp zwei Drittel (64 %) KI als Chance, Prozesse zu optimieren. Mehr als ein Drittel (37 %) befürchtet jedoch, dass sich Prozesse durch den Einsatz von KI auch verschlechtern können. Auffällig ist auch der hohe Anteil an Unternehmensvertretern, die befürchten, dass ihre Positionierung gegenüber den Kunden negativ beeinflusst wird. Dies ist vor allem auf die Sorge zurückzuführen, dass der Service im direkten Kundenkontakt leiden könnte.

Vor- und Nachteile von KI

Welche möglichen Chancen oder Vorteile sowie Risiken oder Nachteile sehen Sie für Ihr Unternehmen durch die Anwendung von Künstlicher Intelligenz?

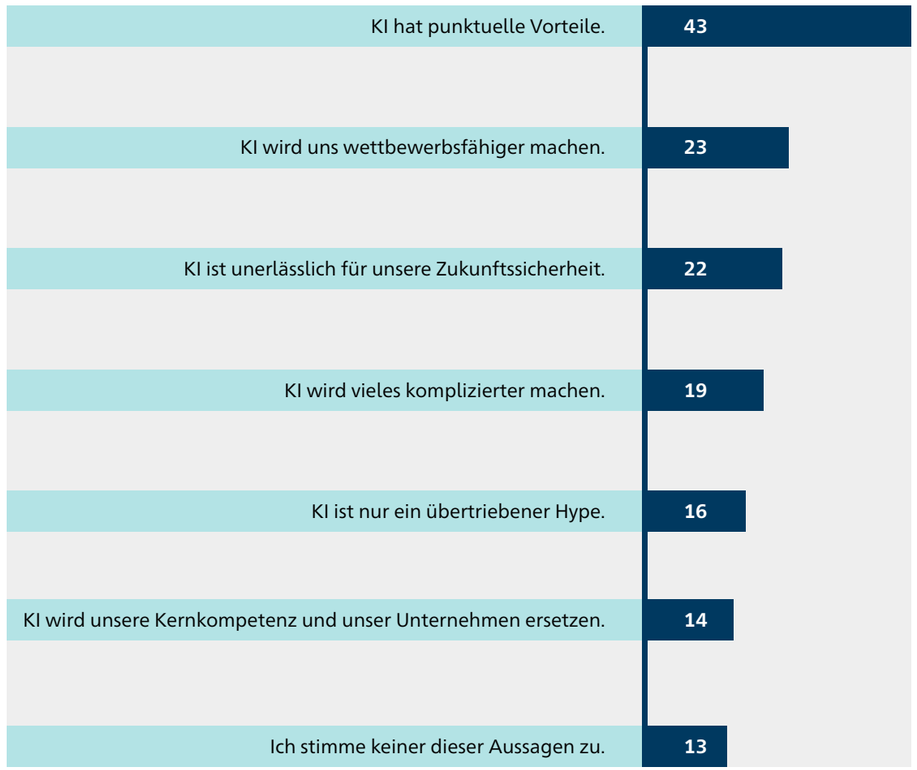


Eine gewisse Zurückhaltung beim Thema KI wird auch bei der abschließenden Beurteilung der befragten Unternehmen deutlich. Zwar überwiegen die Zustimmungsanteile zu den chancenorientierten Aussagen wie hinsichtlich der Wettbewerbsfähigkeit oder der Zukunftssicherheit. Mit Abstand am häufigsten wurde der Aussage „KI hat punktuelle Vorteile“ zugestimmt.

Die Umfrageteilnehmer sehen also Vorteile, aber eher im inkrementellen Bereich, und sehen KI weniger als „Game-Changer“ an.

Individuelle Einschätzung zum Thema

Welchen Aussagen über Künstliche Intelligenz stimmen Sie mit Blick auf Ihr Unternehmen zu?



Cyberversicherung

Mehr als nur Risikotransfer.

Die Magie der Cyberversicherung

„Better safe than sorry“ ist ein Leitsatz, der in vielen Bereichen angewendet werden kann: so auch beim Thema Cyberversicherung. Denn auch wenn sich ein Unternehmen schützt, **gibt es keine hundertprozentige Sicherheit gegen Cyberangriffe.** Eine Lösung für Unternehmen ist es, das Restrisiko weiterzugeben und **von den Leistungen einer Cyberversicherung zu profitieren.** Beim Versicherungsschutz geht es aber auch um das Thema Sensibilisierung. Laut den Ergebnissen der Studie sind KMUs, die eine Cyberversicherung abgeschlossen haben, im Durchschnitt auch besser gegen Cyberangriffe geschützt. So aktualisieren sie ihre Präventionsmaßnahmen regelmäßiger und verfügen deutlich öfter über konkrete Pläne, Richtlinien und Sicherheitsmaßnahmen als die KMUs ohne Cyberversicherung. Knapp über **60 % der Unternehmen** mit einer Cyberversicherung führen aktuell mindestens einmal im Jahr **Mitarbeiterschulungen und Phishing-Simulationen** durch, was erheblich zum Schutz vor möglichen Cyberangriffen beiträgt.

Bessere Schaden-Einschätzung bei Versicherten und bereits Angegriffenen

In den Unternehmen ist man sich der möglichen Schadenshöhe oft nicht bewusst. So können 56 % der Befragten aus Unternehmen ohne Cyberversicherung den maximalen Schaden nicht beziffern oder sie unterschätzen ihn. Bei den Unternehmen mit Cyberversicherung sind es immerhin noch 51 %. Ein ähnliches Bild ergibt sich beim Vergleich von Unternehmen, die bereits angegriffen wurden, mit Unternehmen, die noch keinen Cyberangriff erlebt haben. So können Umfrageteilnehmer aus Unternehmen, die bereits angegriffen wurden, den Schaden besser einschätzen als solche, die noch keinen Cyberangriff erlebt haben. Insgesamt ist die erwartete maximale Schadenshöhe für ihr Unternehmen nach Einschätzung der Befragten auf durchschnittlich 457.000 € gestiegen. Im Vorjahr lag die erwartete maximale Schadenshöhe noch bei 361.000 €. Teilnehmer aus Unternehmen mit einer Cyberversicherung schätzten den maximalen Schaden auf 495.000 €, und damit höher solche von Unternehmen ohne Cyberversicherung. Letztere schätzten den maximalen Schaden auf 402.000 €. Vertreter aus Unternehmen, die noch nicht angegriffen wurden, schätzten den maximalen Schaden sogar nur auf 435.000 €. Auffällig ist außerdem, dass die Einschätzung des erwarteten **Schadens umso höher ausfällt, je größer das Unternehmen in Bezug auf Umsatz und Mitarbeiterzahl ist.**

Bewusstsein für Relevanz von Cyberversicherungen steigt: Unternehmen erkennen Vorteile und reduzieren Vorbehalte

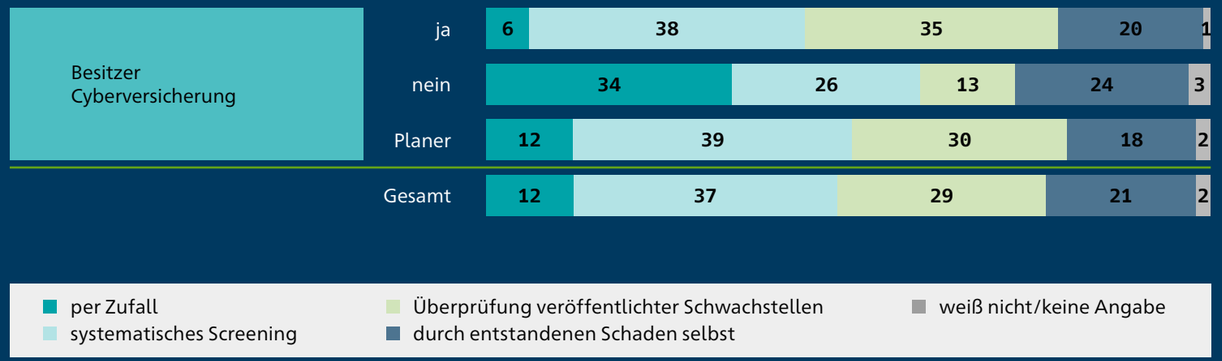
Mit zunehmender Sensibilisierung werden in den Unternehmen die Notwendigkeit und der Nutzen einer Cyberversicherung immer deutlicher. Die Studie zeigt auch, dass die Vorbehalte gegen eine Cyberversicherung abnehmen. Dies gilt vor allem für den Bereich Risikovorsorge. Im Jahr 2024 gaben nur noch **36 % der Befragten an, keine Cyberversicherung abschließen zu wollen,** weil das Risiko aus ihrer Sicht zu gering ist. Im Vorjahr waren es noch 54 %. Auch die Einschätzung, dass sich eine Cyberversicherung aus Kostengründen nicht lohnen würde, ist rückläufig. So gaben **im Jahr 2024 nur noch 38 % der Befragten an, keine Cyberversicherung** abschließen zu wollen, da diese zu „teuer“ sei. **Im Jahr 2023 waren es noch 43 %.**

Im Gegensatz zu den zuvor genannten Punkten hat die Unsicherheit, ob eine Versicherung im Schadenfall zahlt, leicht zugenommen. Im Vorjahr gaben dies noch **14 % der Umfrageteilnehmer** als Grund gegen eine Cyberversicherung an. **Im Jahr 2024 sind es nun 16 % der Unternehmen.**

Dass eine Cyberversicherung **nicht nur ein reiner Risikotransfer** ist, zeigt sich daran, dass Unternehmen **mit einer Cyberversicherung Cyberschäden deutlich früher erkennen.** So gaben 35 % der Unternehmen mit Cyberversicherung an, einen Cyberangriff durch die Überprüfung veröffentlichter Schwachstellen erkannt zu haben, 38 % der Befragten durch systematisches Screening. Nur 13 % der Unternehmen ohne Cyberversicherung entdeckten Cyberangriffe durch die Überprüfung veröffentlichter Schwachstellen und nur 26 % durch systematisches Screening. Insgesamt bedeutet dies, dass **in Unternehmen ohne Versicherungsschutz** mehr als die Hälfte der Cyberangriffe **zufällig oder durch den entstandenen Schaden** selbst bemerkt wurden. Dies ist als besonders kritisch einzustufen, da der Angreifer Zeit gewinnt, um sich in den Systemen des Unternehmens auszubreiten und wichtige Unternehmens- und Personendaten zu stehlen.

Erfahrung mit Cyberattacken

Wie wurde die Cyberattacke entdeckt?



Basis: KMUs mit Cyberattacken-Erfahrung, Angaben in %

Mehr als nur monetäre Absicherung – Unternehmen mit Versicherungsschutz sind besser auf Cyberangriffe vorbereitet.

Feststellbar ist auch eine **Korrelation zwischen einem geringen Umsetzungsgrad von Präventionsmaßnahmen und dem Entdecken eines Schadens durch Zufall oder durch den entstandenen Schaden selbst** zu bestehen. Unternehmen, die auf die zuvor genannte Art von einem Cyberangriff erfahren, setzen oft keine oder nur wenige Präventionsmaßnahmen um. Die **Signifikanz von Prävention** scheint den Unternehmen nach einem Angriff erst richtig bewusst zu werden. So investierten Unternehmen im Nachgang vermehrt in zusätzliche Präventionsmaßnahmen.
Eine positive Entwicklung ist immerhin im Hinblick auf die systematische Überwachung der Unternehmens-IT auf Cyberangriffe festzustellen.
So gaben 2024 nur noch 12% der Befragten an, dass eine Cyberattacke im Unternehmen nur per Zufall entdeckt wurde. 2022 lag diese Quote mit 27% noch signifikant höher. Dagegen stiegen die Entdeckungen durch systematisches Screening im selben Zeitraum von 33% auf 37% und durch die Überprüfung veröffentlichter Schwachstellen von 19% auf 29% Prozent.

Allerdings blieb die Entdeckung erst durch den bereits eingetretenen Schaden selbst stabil bei rund 20%. Christian Kussmann rät daher: „Die systematische Überwachung hat den großen Vorteil, dass Angriffe oft früher erkannt werden und die Schände für das Unternehmen eher in Grenzen gehalten werden können. Systematisches Screening und die Überprüfung bekannter Schwachstellen sollte daher in jedem Unternehmen fester Bestandteil der Cyberprävention sein."

Zusammenfassend lässt sich feststellen, dass eine **Cyberversicherung das Unternehmen nicht nur monetär absichert, sondern auch einen qualitativen Nutzen hat. So profitieren Unternehmen mit einer Cyberversicherung von einer besseren Vorbereitung und einer höheren Sensibilisierung für Cyberangriffe, was sich insbesondere positiv auf die Schadenshöhe sowie den Betriebsunterbrechungsschaden auswirkt.**

Sie haben Fragen zum Thema Cyberversicherung?

Wir helfen Ihnen gerne!
Bitte wenden Sie sich an:

cyberversicherung@hdi.de

HDI Versicherung AG
HDI-Platz 1
30659 Hannover
www.hdi.de/cyberversicherung

70030001332-202404