

# Bericht über die Kosten einer Datenschutzverletzung 2023

# Inhaltsverzeichnis

## 01 →

### Zusammenfassung

- Neuerungen im Bericht 2023
- Wesentliche Feststellungen

## 02 →

### Vollständige Ergebnisse

- Globale Highlights
- Primäre Angriffsvektoren
- Angriffe erkennen
- Dauer der Datenschutzverletzungen
- Wesentliche Kostenfaktoren
- Ransomware und destruktive Angriffe
- Angriffe auf die Lieferkette von Geschäftspartnern
- Angriffe auf die Software-Lieferkette
- Rechtliche Rahmenbedingungen
- Datenschutzverletzungen in der Cloud
- Mega-Datenschutzverletzungen
- Sicherheitsinvestitionen
- KI und Automatisierung für die IT-Sicherheit
- Reaktion auf Vorfälle
- Bedrohungsdaten
- Sicherheitslücken- und Risikomanagement
- Angriffsflächenmanagement
- Anbieter von verwalteten Sicherheitsdiensten (MSSPs)

## 03 →

### Empfehlungen zur Reduzierung der Kosten einer Datenschutzverletzung

## 04 →

### Demografie der Unternehmen

- Geographische Demografie
- Branchendemografie
- Branchendefinitionen

## 05 →

### Forschungsmethoden

- Berechnung der Kosten von Datenschutzverletzungen
- FAQ zu Datenschutzverletzungen
- Grenzen der Forschung

## 06 →

### Informationen über das Ponemon Institute und IBM Security

- Nächste Schritte

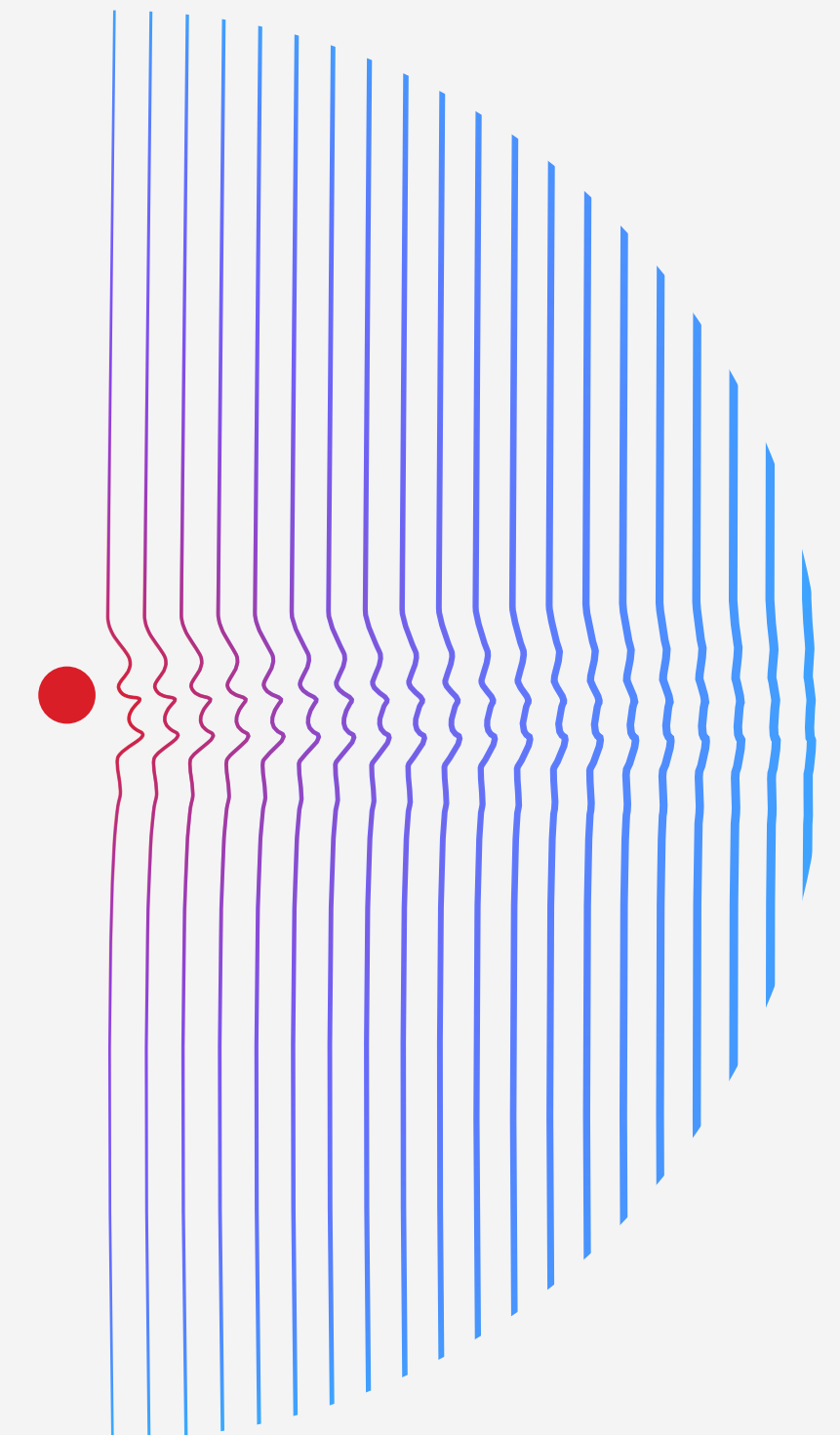
# Zusammenfassung

Der Bericht über die Kosten einer Datenschutzverletzung vermittelt Führungskräften in den Bereichen IT, Risikomanagement und Sicherheit quantifizierbare Daten für eine effizientere Steuerung ihrer Wertpapieranlagen, Risikoprofile und strategischen Entscheidungsfindungsprozesse. Die Ausgabe 2023 stellt die 18. aufeinanderfolgende Ausgabe dieses Berichts dar.

Die diesjährige Studie, die vom Ponemon Institute unabhängig durchgeführt und von IBM Security® gesponsert, analysiert und veröffentlicht wurde, untersuchte 553 Unternehmen, die zwischen März 2022 und März 2023 von Datenschutzverletzungen betroffen waren.

Die in diesem Bericht genannten Jahreszahlen beziehen sich auf das Erscheinungsjahr des Berichts, nicht unbedingt auf das Jahr des Verstoßes. Die untersuchten Verstöße fanden in 16 Ländern und Regionen und in 17 verschiedene Branchen statt.

In diesem Bericht untersuchen wir die Ursachen sowie die kurz- und langfristigen Folgen von Datenschutzverletzungen. Wir untersuchen auch die Faktoren und Technologien, die es den Unternehmen ermöglicht haben, die Verluste zu begrenzen – und die, die zu höheren Kosten geführt haben.





## Neuerungen im Bericht 2023

Jedes Jahr entwickeln wir den Bericht über die Kosten einer Datenschutzverletzung weiter, um ihn an neue Technologien, neue Taktiken und aktuelle Ereignisse anzupassen. Zum ersten Mal, erforscht die diesjährige Studie:

- Wie werden Sicherheitsverletzungen erkannt: durch die Sicherheitsteams eines Unternehmens, durch Dritte oder durch den Angreifer
- Die Auswirkungen der Einbeziehung von Strafverfolgungsbehörden in einem Ransomware-Angriff
- Die Auswirkungen von Ransomware-Playbooks und -Workflows
- Spezifische Kosten im Zusammenhang mit behördlichen Bußgeldern
- Ob und wie Firmen planen, ihre Sicherheitsinvestitionen aufgrund einer Verletzung zu erhöhen
- Die Auswirkungen der folgenden Strategien zur Schadensbegrenzung:
  - Bedrohungsinformationen
  - Sicherheitslücken- und Risikomanagement
  - Angriffsflächenmanagement (ASM)
  - Anbieter von verwalteten Sicherheitsdiensten (MSSPs)

Da die Kosten einer Sicherheitsverletzung weiter steigen, liefert dieser Bericht wichtige Erkenntnisse, die Sicherheits- und IT-Teams dabei helfen, Risiken besser zu managen und potenzielle Schäden und Verluste zu begrenzen. Der Bericht ist in fünf Hauptabschnitte unterteilt:

- Zusammenfassung mit den wichtigsten Ergebnissen und den Neuerungen der Ausgabe 2023
- Gründliche Analyse der vollständigen Ergebnisse, inklusive der Kosten für Sicherheitsverletzungen nach Region und Branche
- Sicherheitsempfehlungen der Experten von IBM Security basierend auf den Ergebnissen dieses Berichts
- Demografie der Unternehmen und Definition der Branchen
- Methodik der Studie mit Berechnungsweise der Kosten



4,45 Mio.  
US-Dollar

## Wesentliche Feststellungen

Die im Folgenden erläuterten Ergebnisse basieren auf der Analyse von Forschungsdaten des Ponemon Institute durch IBM Security. Alle Kostenbeträge in diesem Bericht sind in US-Dollar (USD) ausgewiesen.

51 %

### Durchschnittliche Gesamtkosten einer Verletzung

Die durchschnittlichen Kosten einer Datenschutzverletzung erreichten im Jahr 2023 mit 4,45 Millionen US-Dollar ein Allzeithoch. Dies entspricht einem Anstieg von 2,3 % gegenüber den Kosten von 4,35 Mio. US-Dollar im Jahr 2022. Langfristig betrachtet sind die durchschnittlichen Kosten von 3,86 Mio. US-Dollar im Bericht für 2020 um 15,3 % gestiegen.

### Prozentsatz der Unternehmen, die als Folge eines Sicherheitsverstoßes eine Erhöhung der Sicherheitsinvestitionen planen

Während die Kosten für Datenschutzverletzungen weiter steigen, waren die Teilnehmer des Berichts fast gleichmäßig darüber gespalten, ob sie aufgrund einer Datenschutzverletzung höhere Sicherheitsinvestitionen planen. Zu den wichtigsten Bereichen, in die zusätzliche Investitionen getätigt werden sollten, gehören die Planung und das Testen von Incident Response (IR), die Schulung von Mitarbeitern sowie Technologien zur Erkennung von und Reaktion auf Bedrohungen.

1,76 Mio.  
US-Dollar

### Die Auswirkung von umfangreicher Sicherheits-KI und Automatisierung auf die finanziellen Auswirkungen einer Sicherheitsverletzung

KI und Automatisierung im Sicherheitsbereich haben sich als wichtige Investitionen erwiesen, um die Kosten zu senken und die Zeit zur Identifizierung und Eindämmung von Sicherheitsverletzungen zu minimieren. Unternehmen, die diese Funktionen umfassend in ihr Konzept einbezogen haben, konnten die Zeit bis zur Erkennung und Eindämmung der Sicherheitsverletzung im Durchschnitt um 108 Tage verkürzen. Außerdem meldeten sie einen Rückgang der Kosten für Datenschutzverletzungen um 1,76 Millionen US-Dollar im Vergleich zu Unternehmen, die keine KI- und Automatisierungsfunktionen für die Sicherheit nutzen.

## 1 von 3

### Anzahl der Verstöße, die von den eigenen Sicherheitsteams oder -tools einer Organisation festgestellt wurden

Nur ein Drittel der Unternehmen entdeckte die Datenschutzverletzung durch ihre eigenen Sicherheitsteams, was die Notwendigkeit einer besseren Erkennung von Bedrohungen verdeutlicht. 67 % der Datenschutzverletzungen wurden von einer gutartigen dritten Partei oder von den Angreifern selbst gemeldet. Wenn Angreifer eine Sicherheitsverletzung meldeten, kostete dies die Unternehmen im Vergleich zur internen Erkennung fast 1 Million US-Dollar mehr.

## 470.000 US-Dollar

### Zusätzliche Kosten für Unternehmen, die bei einem Ransomware-Angriff die Strafverfolgungsbehörden nicht eingeschaltet haben

Die diesjährige Studie zeigt, dass der Ausschluss der Strafverfolgungsbehörden von Ransomware-Vorfällen zu höheren Kosten führt. Während 63 % der Befragten angaben, die Strafverfolgungsbehörden eingeschaltet zu haben, zahlten die 37 %, die dies nicht taten, 9,6 % mehr und erlebten einen 33 Tage längeren Lebenszyklus der Sicherheitsverletzung.

## 53,3 %

### Seit 2020 sind die Kosten für Datenschutzverletzungen im Gesundheitswesen um 53,3 % gestiegen

In der stark regulierten Gesundheitsbranche sind die Kosten für Datenschutzverletzungen seit 2020 erheblich gestiegen. Im 13. Jahr in Folge meldete die Gesundheitsbranche mit durchschnittlichen Kosten von 10,93 Millionen US-Dollar die teuersten Datenschutzverletzungen.

## 82 %

### Der Prozentsatz der Sicherheitsverletzungen, die in der Cloud gespeicherte Daten betrafen – öffentlich, privat oder umgebungsübergreifend

Cloudumgebungen waren im Jahr 2023 häufige Ziele von Cyberangreifern. Angreifer verschafften sich häufig Zugriff auf mehrere Umgebungen. 39 % der Einbrüche erstreckten sich auf mehrere Umgebungen und verursachten mit 4,75 Millionen US-Dollar überdurchschnittlich hohe Kosten.



## 1,68 Mio. US-Dollar

### **Kosteneinsparungen durch eine hohe Akzeptanz von DevSecOps**

Integrierte Sicherheitstests im Softwareentwicklungsprozess (DevSecOps) haben 2023 einen beträchtlichen ROI unter Beweis gestellt. Unternehmen mit einer hohen DevSecOps-Akzeptanz sparten 1,68 Millionen US-Dollar im Vergleich zu Unternehmen mit einer geringen oder gar keiner Akzeptanz. Im Vergleich zu anderen kostensenkenden Faktoren wies DevSecOps die größten Kosteneinsparungen auf.

## 1,49 Mio. US-Dollar

### **Kosteneinsparungen, die Unternehmen mit einem hohen Maß an IR-Planung und -Tests erzielen**

IR-Planung und -Tests sind nicht nur eine vorrangige Investition für Unternehmen, sondern haben sich auch als äußerst wirksame Taktik zur Eindämmung der Kosten einer Datenschutzverletzung erwiesen. Unternehmen mit einem hohen Maß an IR-Planung und -Tests sparten 1,49 Millionen US-Dollar im Vergleich zu Unternehmen mit einem geringeren Maß.

## 1,44 Mio. US-Dollar

### **Anstieg der Kosten für Datenschutzverletzungen bei Unternehmen mit einem hohen Grad an Komplexität der Sicherheitssysteme**

Unternehmen mit einem niedrigen oder gar keinem Komplexitätsgrad ihres Sicherheitssystems verzeichneten im Jahr 2023 durchschnittliche Kosten für Datenschutzverletzungen in Höhe von 3,84 Millionen US-Dollar. Diejenigen mit einem hohen Grad an Komplexität des Sicherheitssystems meldeten durchschnittliche Kosten von 5,28 Mio. US-Dollar, was einem Anstieg von 31,6 % entspricht.

## 1,02 Mio. US-Dollar

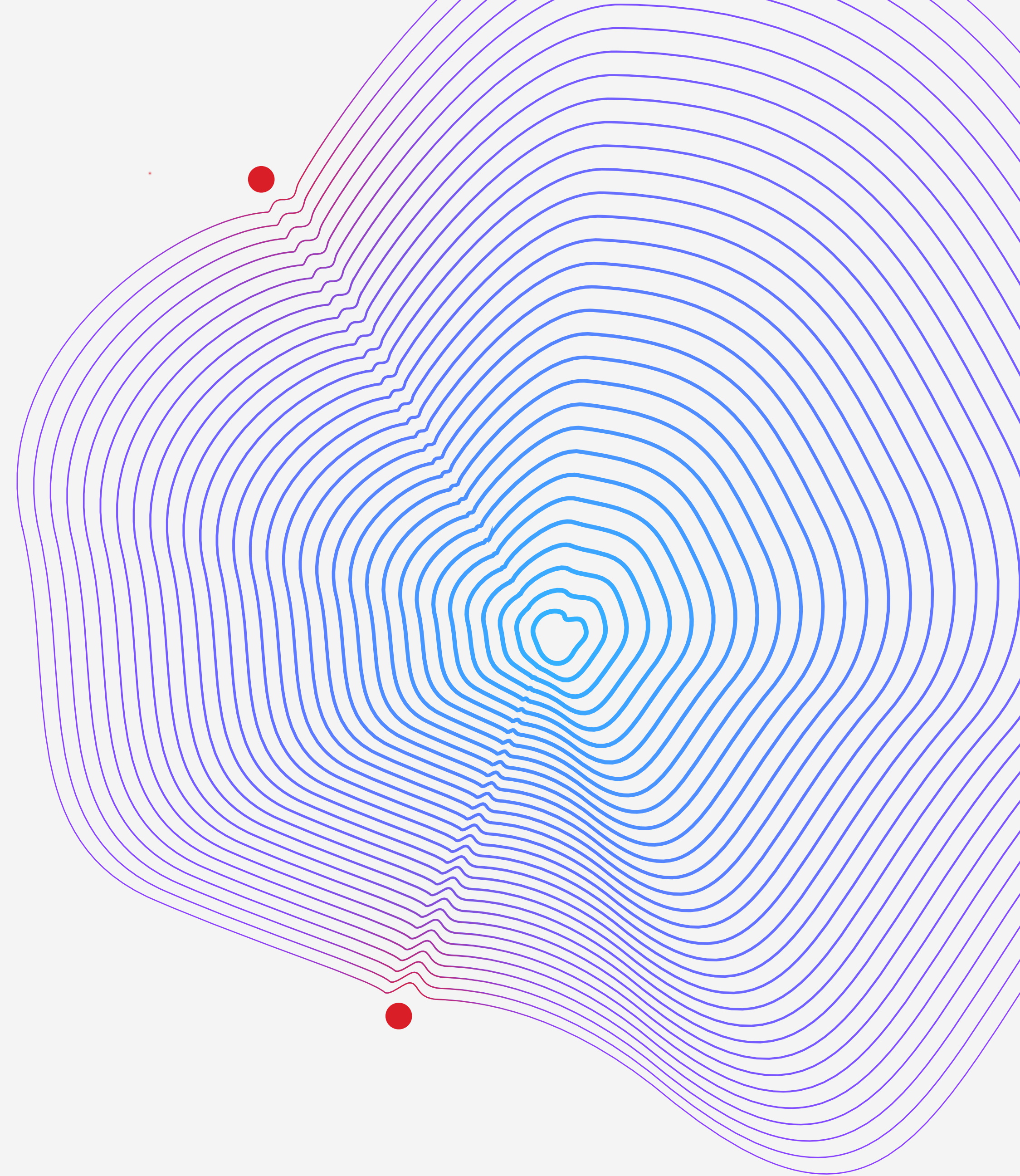
### **Durchschnittliche Kostendifferenz zwischen Sicherheitsverletzungen, deren Erkennung und Behebung mehr als 200 Tage dauerte, und jenen, die in weniger als 200 Tagen behoben wurden**

Die Zeit zur Identifizierung und Eindämmung von Sicherheitsverletzungen – auch als „Lebenszyklus“ bezeichnet – ist nach wie vor ein wesentlicher Bestandteil des finanziellen Gesamtschadens. Verletzungen mit einer Feststellungs- und Eindämmungszeit von weniger als 200 Tagen kosteten die Unternehmen 3,93 Millionen US-Dollar. Verletzungen, die mehr als 200 Tage dauerten, kosteten 4,95 Millionen US-Dollar – ein Unterschied von 23 %.

# Vollständige Ergebnisse

Dieser Abschnitt enthält die detaillierten Ergebnisse des Berichts, gegliedert in 18 Themenbereiche. Die Reihenfolge der Themen ist wie folgt

- Die wichtigsten globalen Ergebnisse
- Primäre Angriffsvektoren
- Angriffe erkennen
- Dauer der Datenschutzverletzungen
- Wesentliche Kostenfaktoren
- Ransomware und destruktive Angriffe
- Angriffe auf die Lieferkette von Geschäftspartnern
- Angriffe auf die Software-Lieferkette
- Regulatorische Rahmenbedingungen
- Cloud-Verstöße
- Mega-Datenschutzverletzungen
- Sicherheitsinvestitionen
- KI und Automatisierung für die IT-Sicherheit
- Reaktion auf Vorfälle
- Bedrohungsinformationen
- Sicherheitslücken- und Risikomanagement
- Angriffsflächenmanagement
- Anbieter von verwalteten Sicherheitsdiensten





## Die wichtigsten globalen Ergebnisse

Der Bericht über die Kosten einer Datenschutzverletzung bietet ein globales Bild der Kosten von Datenschutzverletzungen, das auf der Grundlage von Daten aus über 553 Datenschutzverletzungen in 16 verschiedenen Ländern und unter Berücksichtigung von Hunderten von Kostenfaktoren erstellt wurde. In diesem Abschnitt werden kritische Metriken auf der Ebene des globalen Durchschnitts untersucht. Wir untersuchen auch die durchschnittlichen Vergleichskosten pro Datensatz zwischen Ländern und Branchen.

# 4,45 Mio. US-Dollar

Durchschnittliche weltweite Gesamtkosten einer Datenschutzverletzung

**Abbildung 1. Die Kosten einer Datenschutzverletzungen stiegen auf einen neuen Höchststand.**  
Weltweit stiegen die durchschnittlichen Kosten einer Datenschutzverletzung auf 4,45 Mio. US-Dollar, was einem Anstieg von 100.000 US-Dollar gegenüber 2022 entspricht. Dies entspricht einem Anstieg von 2,3 % gegenüber den durchschnittlichen Kosten von 4,35 Mio. US-Dollar im Jahr 2022. Seit 2020, als die durchschnittlichen Gesamtkosten einer Datenschutzverletzung 3,86 Mio. US-Dollar betrugen, sind die durchschnittlichen Gesamtkosten um 15,3 % gestiegen.

**Abbildung 2. Die Kosten pro Datensatz für einen Datenschutzverstoß haben ebenfalls einen neuen Höchststand erreicht.**  
Im Jahr 2023 betrugen die durchschnittlichen Kosten pro Datensatz, der von einer Datenschutzverletzung betroffen war, 165 US-Dollar, was einem leichten Anstieg gegenüber dem Durchschnitt von 164 US-Dollar im Jahr 2022 entspricht und dem relativ geringen Anstieg zwischen 2021 und 2022 entspricht, als die Kosten nur um 3 US-Dollar stiegen. In den letzten sieben Jahren war der größte Anstieg der durchschnittlichen Kosten pro Datensatz zwischen 2020 und 2021 zu verzeichnen, als die durchschnittlichen Kosten von 146 US-Dollar auf 161 US-Dollar bzw. um 10,3 % stiegen. In der Studie wurden Verstöße mit einem Umfang von 2.200 bis 102.000 Datensätzen untersucht.<sup>1</sup>

Gesamtkosten eines Datenschutzverstoßes

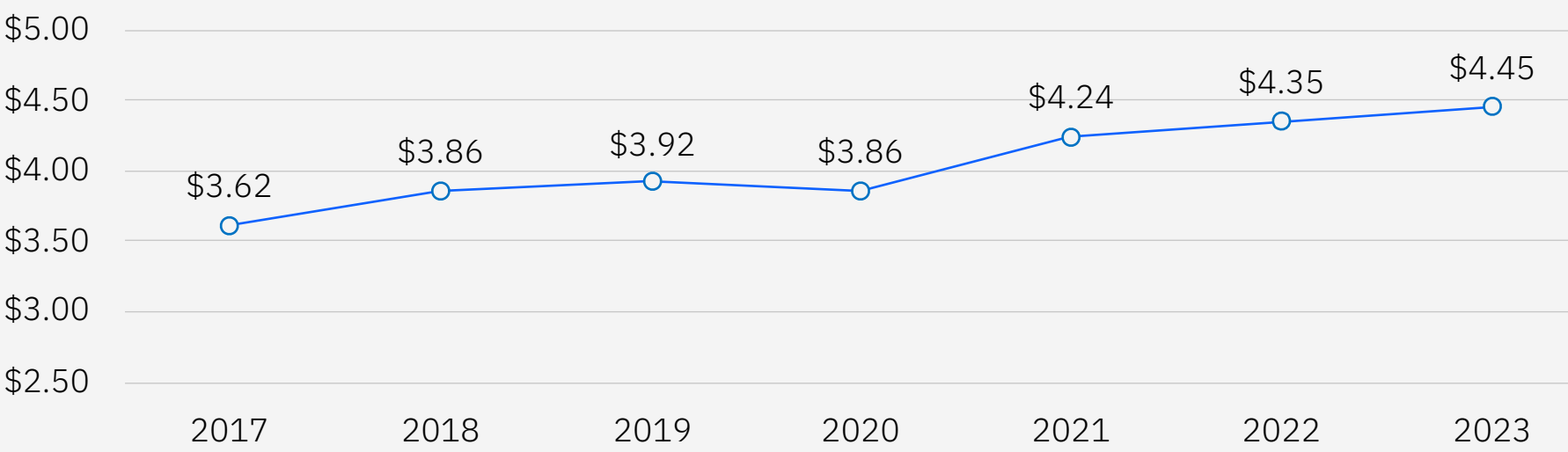


Abbildung 1. Angaben in°Mio.°US-Dollar

Kosten eines Datenschutzverstoßes pro Datensatz

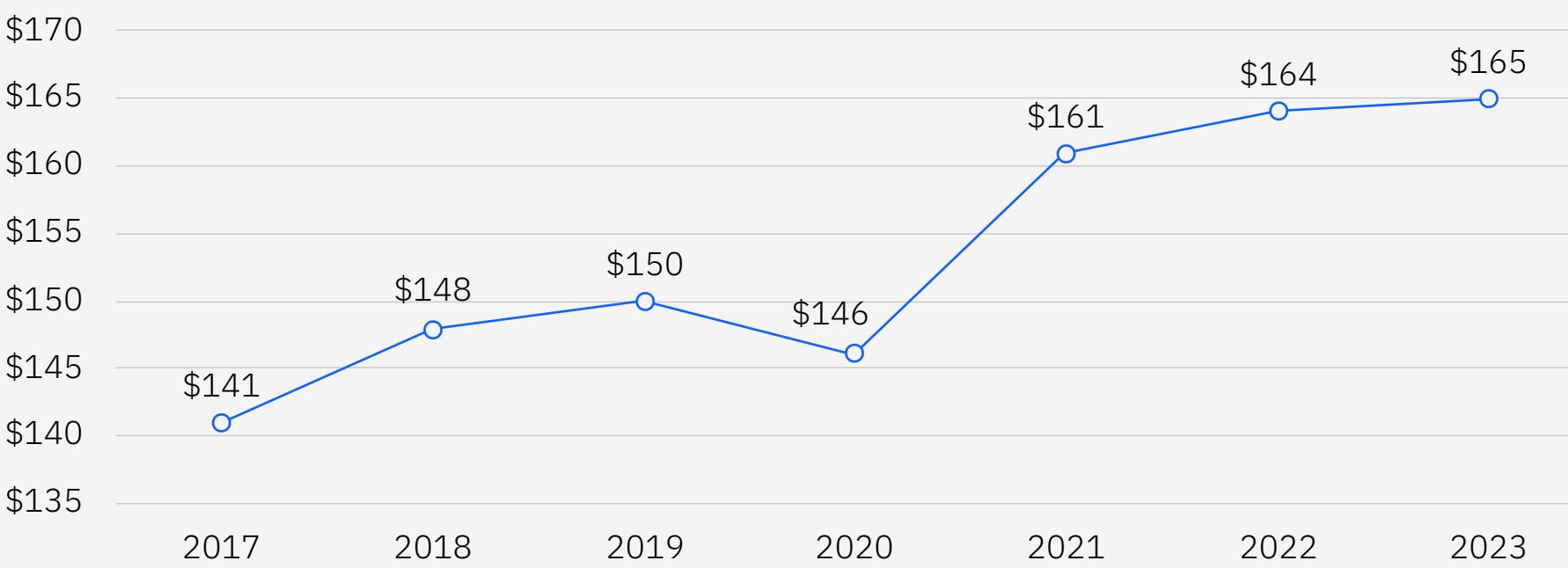


Abbildung 2. Angaben in US-Dollar

**Abbildung 3. Zum 13. Mal in Folge waren die USA das Land mit den höchsten Kosten für Datenschutzverletzungen.**  
Bei den fünf Ländern bzw. Regionen mit den höchsten durchschnittlichen Kosten einer Datenschutzverletzung gab es im Vergleich zu 2022 erhebliche Veränderungen.

		2023	2022
1	↑	<b>USA</b> 9,48 Mio. US-Dollar	<b>USA</b> 9,44 Mio. US-Dollar
2	↑	<b>Nahe Osten</b> 8,07 Mio. US-Dollar	<b>Nahe Osten</b> 7,46 Mio. US-Dollar
3	↓	<b>Kanada</b> 5,13 Mio. US-Dollar	<b>Kanada</b> 5,64 Mio. US-Dollar
4	↓	<b>Deutschland</b> 4,67 Mio. US-Dollar	<b>Vereinigtes Königreich</b> 5,05 Mio. US-Dollar
5	↓	<b>Japan</b> 4,52 Mio. US-Dollar	<b>Deutschland</b> 4,85 Mio. US-Dollar

Von den diesjährigen Top Fünf ist Japan das einzige Land, das 2022 nicht mehr unter den Top Fünf zu finden sein wird, nachdem es im letzten Jahr noch auf Platz 6 der teuersten Länder lag. Auf der Top-5-Liste des letzten Jahres war auch das Vereinigte Königreich (UK) mit durchschnittlichen Kosten von 5,05 Mio. US-Dollar für Datenschutzverstöße vertreten. In diesem Jahr sind die Durchschnittskosten im Vereinigten Königreich im Vergleich zum Vorjahr um 16,6 % auf 4,21 Mio. US-Dollar gesunken, was zu einer Platzierung knapp außerhalb der Top Fünf führt.

Die Vereinigten Staaten wiesen mit 9,48 Mio. US-Dollar erneut die höchsten durchschnittlichen Gesamtkosten einer Datenschutzverletzung auf, was einem

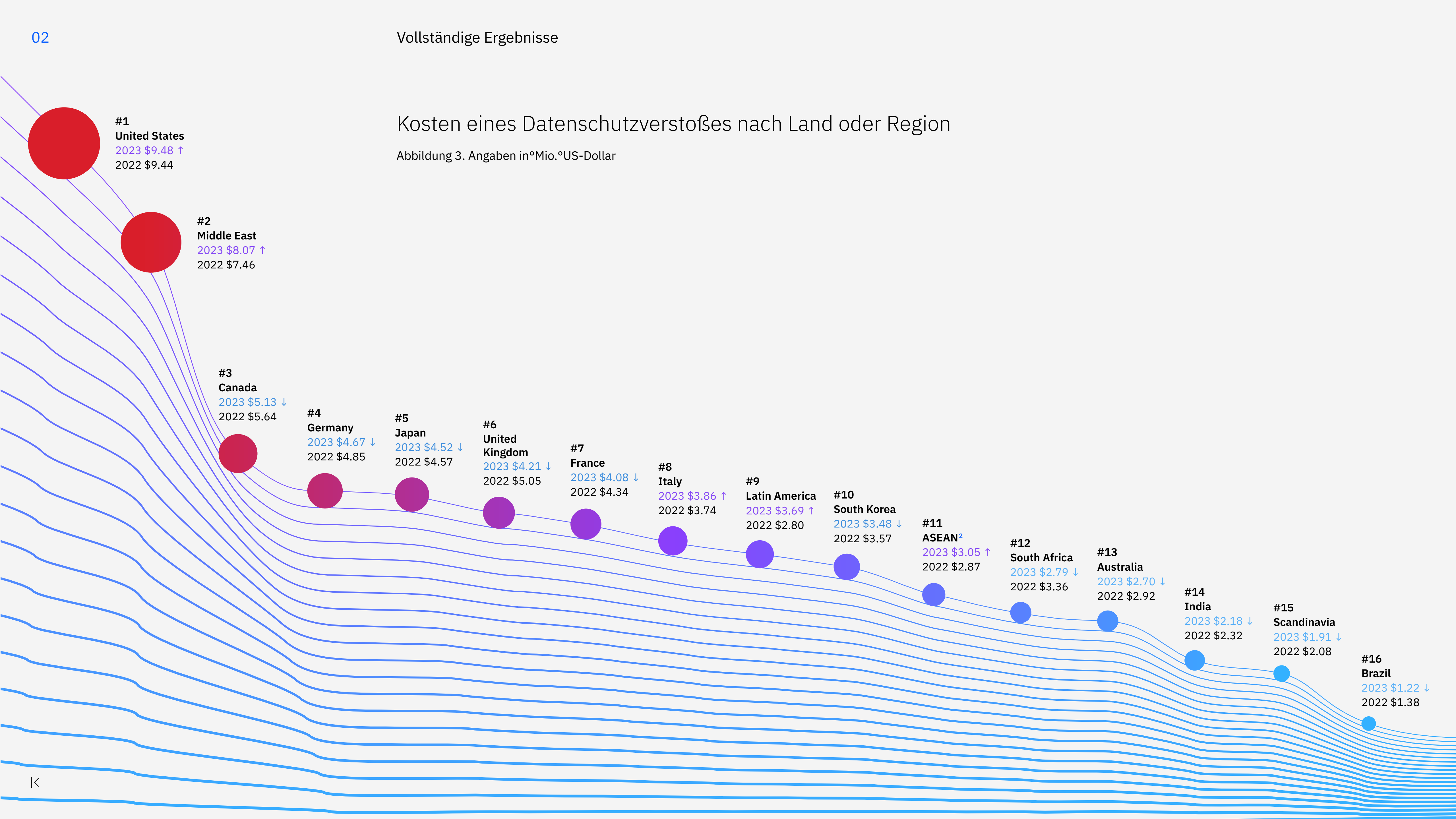
Anstieg von 0,4 % gegenüber dem Vorjahr (9,44 Mio. US-Dollar) entspricht. Wie im Vorjahr verzeichnete der Nahe Osten mit 8,07 Mio. US-Dollar die zweithöchsten durchschnittlichen Gesamtkosten einer Datenschutzverletzung, ein Anstieg um 8,2 % von 7,46 Mio. US-Dollar.

In Kanada sanken die durchschnittlichen Gesamtkosten einer Datenschutzverletzung von 5,64 Mio. US-Dollar auf 5,13 Mio. US-Dollar oder 9 %. Auch in Deutschland sanken die durchschnittlichen Kosten von 4,85 Mio. US-Dollar auf 4,67 Mio. US-Dollar bzw. 3,7 %. Japan verzeichnete einen leichten Rückgang von 4,57 Mio. US-Dollar auf 4,52 Mio. US-Dollar bzw. 1,1 %.



# Kosten eines Datenschutzverstoßes nach Land oder Region

Abbildung 3. Angaben in°Mio.°US-Dollar



**Abbildung 4. Branchenübergreifend verzeichnete das Gesundheitswesen das 13. Jahr in Folge die höchsten Kosten.** Das Gesundheitswesen verzeichnet nach wie vor die höchsten Kosten für Datenschutzverletzungen aller Branchen, mit einem Anstieg von 10,10 Mio. US-Dollar im Jahr 2022 auf 10,93 Mio. US-Dollar im Jahr 2023 – ein Plus von 8,2 %. In den letzten drei Jahren sind die durchschnittlichen Kosten einer Datenschutzverletzung im Gesundheitswesen um 53,3 % gestiegen, was einem Anstieg von mehr als 3 Mio. US-Dollar entspricht, verglichen mit durchschnittlichen Kosten von 7,13 Millionen US-Dollar im Jahr 2020. Das Gesundheitswesen ist stark reguliert und wird von der US-Regierung als kritische Infrastruktur eingestuft. Seit Beginn der COVID-19-Pandemie sind die durchschnittlichen Kosten für Datenschutzverletzungen in der Branche deutlich gestiegen.

Die fünf teuersten Branchen haben sich gegenüber dem Vorjahr verändert. Der Technologiesektor fiel aus den Top Fünf heraus, während der Industriesektor neu hinzukam und mit einem Zuwachs von 5,8 % vom siebten auf den fünften Platz vorrückte. Laut IBM Threat Intelligence ist die Fertigungsindustrie die am häufigsten von Cyberkriminellen angegriffene Branche.

		2023	2022
1	↑	<b>Gesundheitswesen</b> 10,93 Mio. US-Dollar	<b>Gesundheitswesen</b> 10,10 Mio. US-Dollar
2	↓	<b>Finanzwesen</b> 5,90 Mio. US-Dollar	<b>Finanzwesen</b> 5,97 Mio. US-Dollar
3	↓	<b>Pharma</b> 4,82 Mio. US-Dollar	<b>Pharma</b> 5,01 Mio. US-Dollar
4	↑	<b>Energie</b> 4,78 Mio. US-Dollar	<b>Technologie</b> 4,97 Mio. US-Dollar
5	↑	<b>Industrie</b> 4,73 Mio. US-Dollar	<b>Energie</b> 4,72 Mio. US-Dollar

Kosten eines Datenschutzverstoßes nach Branche

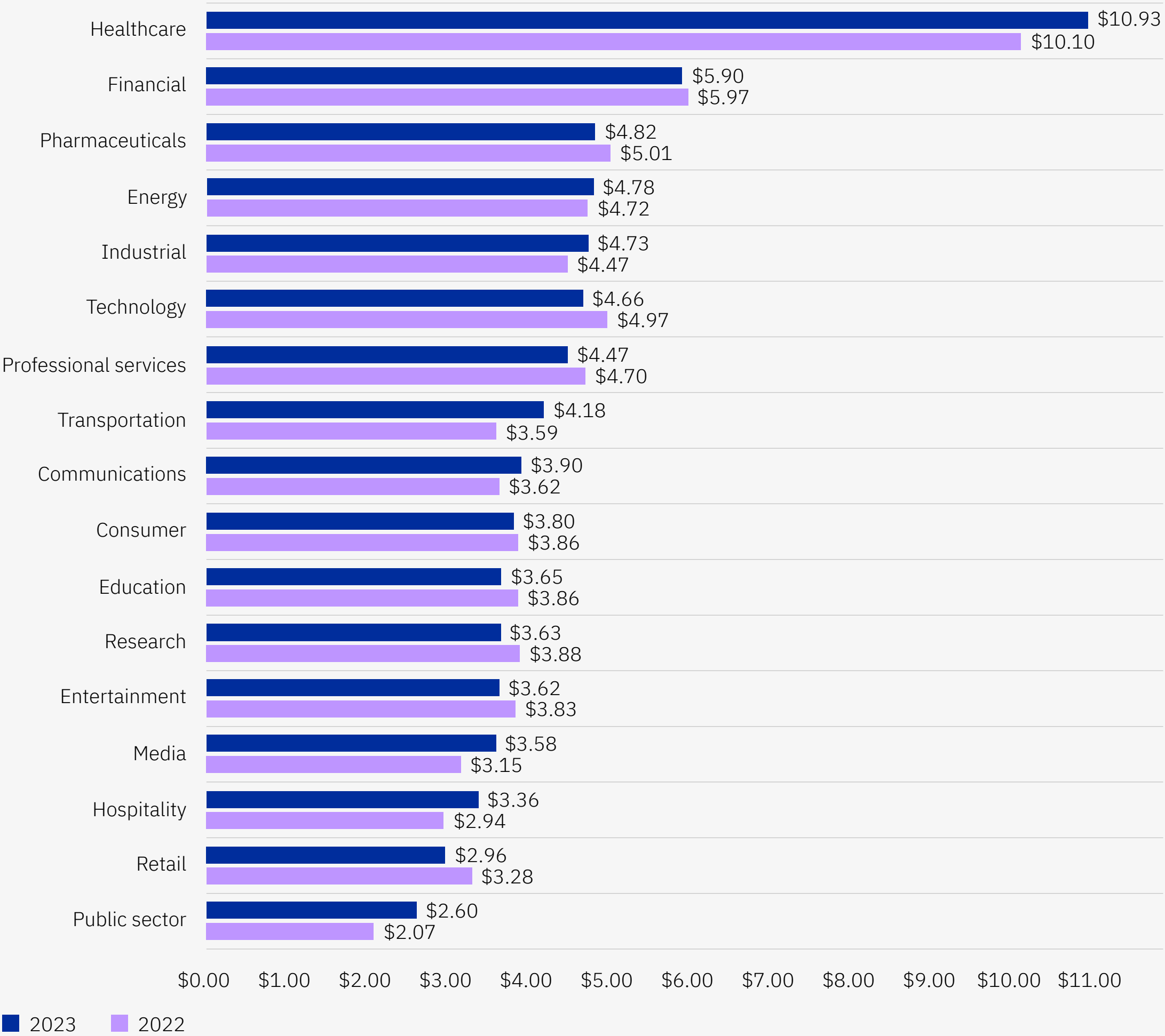


Abbildung 4. Angaben in°Mio.°US-Dollar

**Abbildung 5. Die durchschnittliche Zeit für die Ermittlung und Eindämmung von Sicherheitsverletzungen ist in etwa gleich geblieben.**

Im Vergleich zu 2022 haben sich sowohl die mittlere Zeit bis zur Entdeckung (MTTI) als auch die mittlere Zeit bis zur Eindämmung (MTTC) von Verstößen nur geringfügig verändert. Mittlere Zeit bis zur Erkennung bezieht sich auf die Zeit, die ein Unternehmen benötigt, um eine Sicherheitsverletzung aufzudecken. Die mittlere Eindämmungszeit bezieht sich auf die Zeit, die benötigt wird, um eine Sicherheitsverletzung zu beheben, nachdem sie erkannt wurde.

Im Jahr 2022 dauerte es durchschnittlich 207 Tage, bis eine Datenschutzverletzung erkannt wurde. Im Jahr 2023 dauerte es nur 204 Tage. Andererseits benötigten Unternehmen im Jahr 2023 durchschnittlich 73 Tage, um Verstöße einzudämmen, verglichen mit durchschnittlich 70 Tagen im Jahr 2022. Die längsten durchschnittlichen Zeiten, um Verstöße einzudämmen bzw. zu erkennen, gab es im Jahr 2021 mit 212 bzw. 75 Tagen.

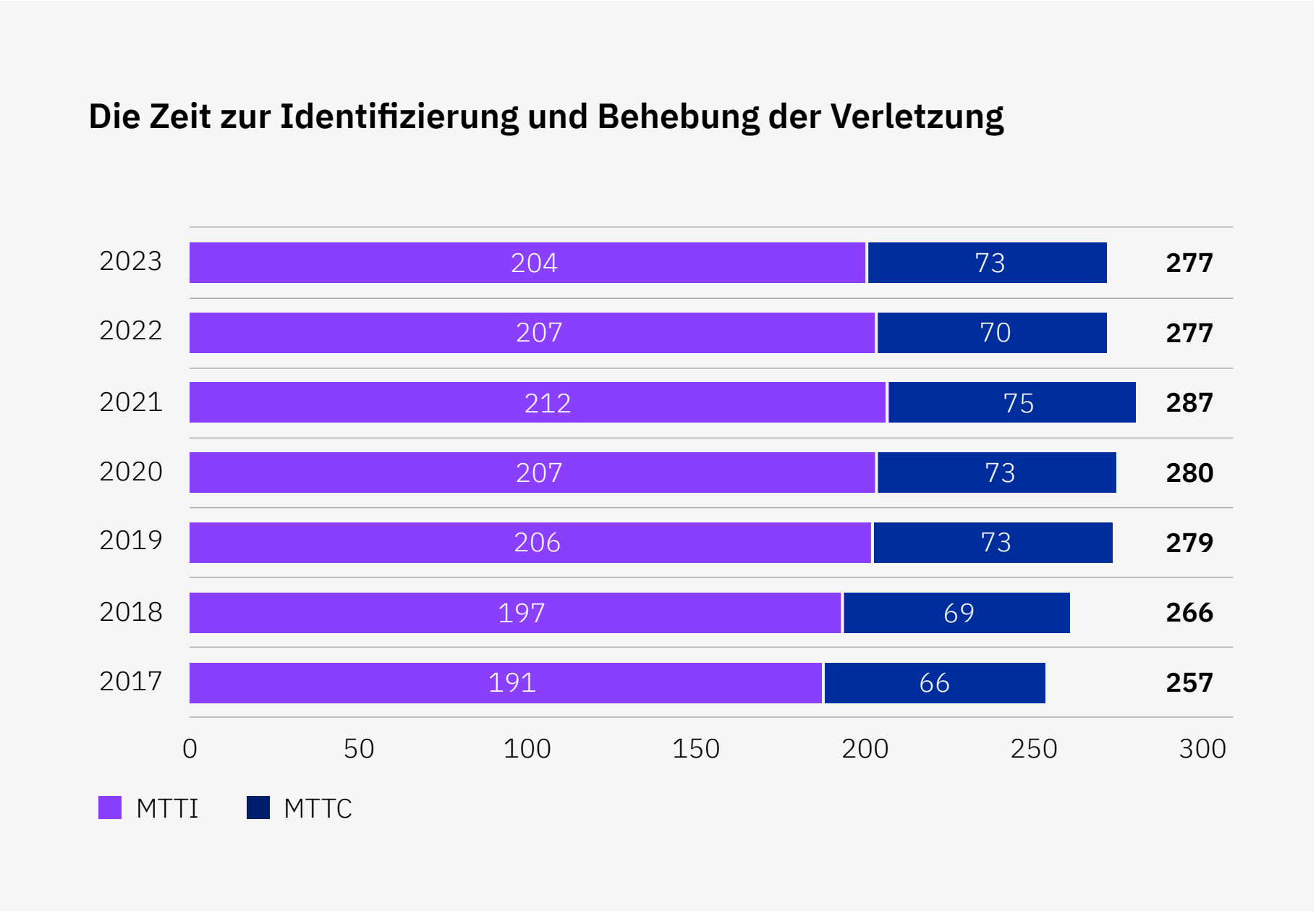


Abbildung 5. Angaben in Tagen



**Abbildung 6. Die Geschäftsausfallkosten erreichten ein Fünfjahrestief.**

Im Vorjahresbericht wurde festgestellt, dass die Aufdeckungs- und Eskalationskosten zur teuersten Ausgabenkategorie für Datenschutzverletzungen geworden sind, was auf eine Verlagerung hin zu längeren und komplexeren Untersuchungen von Datenschutzverletzungen hindeutet. Dieser Trend setzte sich auch in diesem Jahr fort, wobei die Kosten für Erkennung und Eskalation an erster Stelle blieben und von 1,44 Mio. US-Dollar auf 1,58 Mio. US-Dollar anstiegen, was einer Veränderung von 140.000 US-Dollar bzw. 9,7 % entspricht. Erkennungs- und Eskalationskosten umfassen Aktivitäten, die es einem Unternehmen ermöglichen, einen Verstoß angemessen zu erkennen. Dazu können forensische und investigative Tätigkeiten, Bewertungs- und Prüfungsdienste, Krisenmanagement und die Kommunikation mit Führungskräften und Vorständen gehören.

Auch in den anderen wichtigen Kostensegmenten einer Datenschutzverletzung – Geschäftsausfallkosten, Reaktion auf eine Sicherheitsverletzung und Benachrichtigung – gab es im Vergleich zu 2022 Veränderungen. Die Geschäftsausfallkosten sanken um 8,5 %, von 1,42 Mio. US-Dollar im Jahr 2022 auf 1,30 Mio. US-Dollar im Jahr 2023. Geschäftsausfallkosten umfassen Aktivitäten wie Betriebsunterbrechungen und Umsatzeinbußen aufgrund von Systemausfällen, Kosten für verlorene Kunden und für die Gewinnung neuer Kunden sowie Reputationsverluste und verminderten Goodwill.

Insbesondere die Benachrichtigungskosten stiegen von 310.000 US-Dollar im Jahr 2022 auf 370.000 US-Dollar im Jahr 2023, was einem Anstieg von 19,4 % entspricht. Die Kosten für die Reaktion nach dem Verstoß stiegen um nur 20.000 US-Dollar. Benachrichtigungskosten umfassen Aktivitäten, die es dem Unternehmen ermöglichen, betroffene Personen, Datenschutzbehörden und andere Dritte zu benachrichtigen.

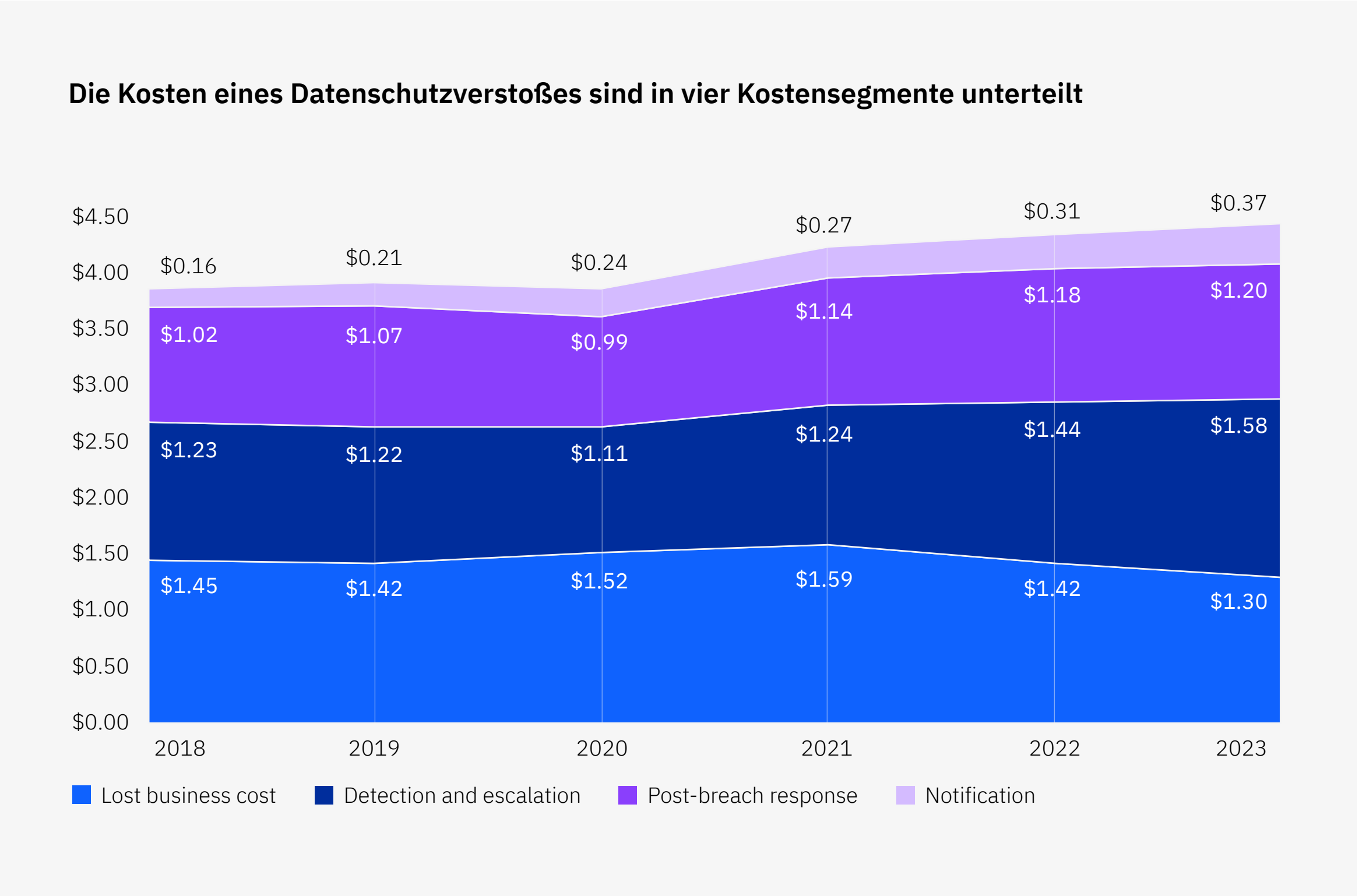


Abbildung 6. Angaben in°Mio.°US-Dollar

**Abbildung 7. Kleinere Unternehmen waren mit erheblich höheren Kosten für Datenschutzverstöße konfrontiert als im letzten Jahr.**

Für Unternehmen mit mehr als 5.000 Mitarbeitern sind die durchschnittlichen Kosten einer Datenschutzverletzung im Jahr 2023 im Vergleich zu 2022 gesunken. Auf der anderen Seite sind die durchschnittlichen Kosten einer Datenschutzverletzung bei Unternehmen mit bis zu 5.000 Mitarbeitern deutlich angestiegen.

Unternehmen mit weniger als 500 Beschäftigten gaben an, dass die durchschnittlichen Auswirkungen einer Datenschutzverletzung von 2,92 Mio. US-Dollar auf 3,31 Mio. US-Dollar gestiegen sind, d.h. um 13,4 %. Unternehmen mit 500 bis 1.000 Beschäftigten verzeichneten einen Anstieg um

21,4 %, von 2,71 Mio. US-Dollar auf 3,29 Mio. US-Dollar. Im Bereich von 1.001 bis 5.000 Beschäftigten stiegen die durchschnittlichen Kosten einer Datenschutzverletzung von 4,06 Mio. US-Dollar auf 4,87 Mio. US-Dollar, d. h. um fast 20 %.

Im Bereich von 10.001 bis 25.000 Beschäftigten gaben die Befragten durchschnittliche Kosten von 5,46 Mio. US-Dollar an, was einem Rückgang von 1,8 % gegenüber dem Wert von 5,56 Mio. US-Dollar im Jahr 2022 entspricht. Bei Unternehmen mit mehr als 25.000 Beschäftigten sanken die durchschnittlichen Kosten von 5,56 Mio. US-Dollar im Jahr 2022 auf 5,42 Mio. US-Dollar im Jahr 2023, was einem Rückgang von 140.000 US-Dollar bzw. 2,5 % entspricht.

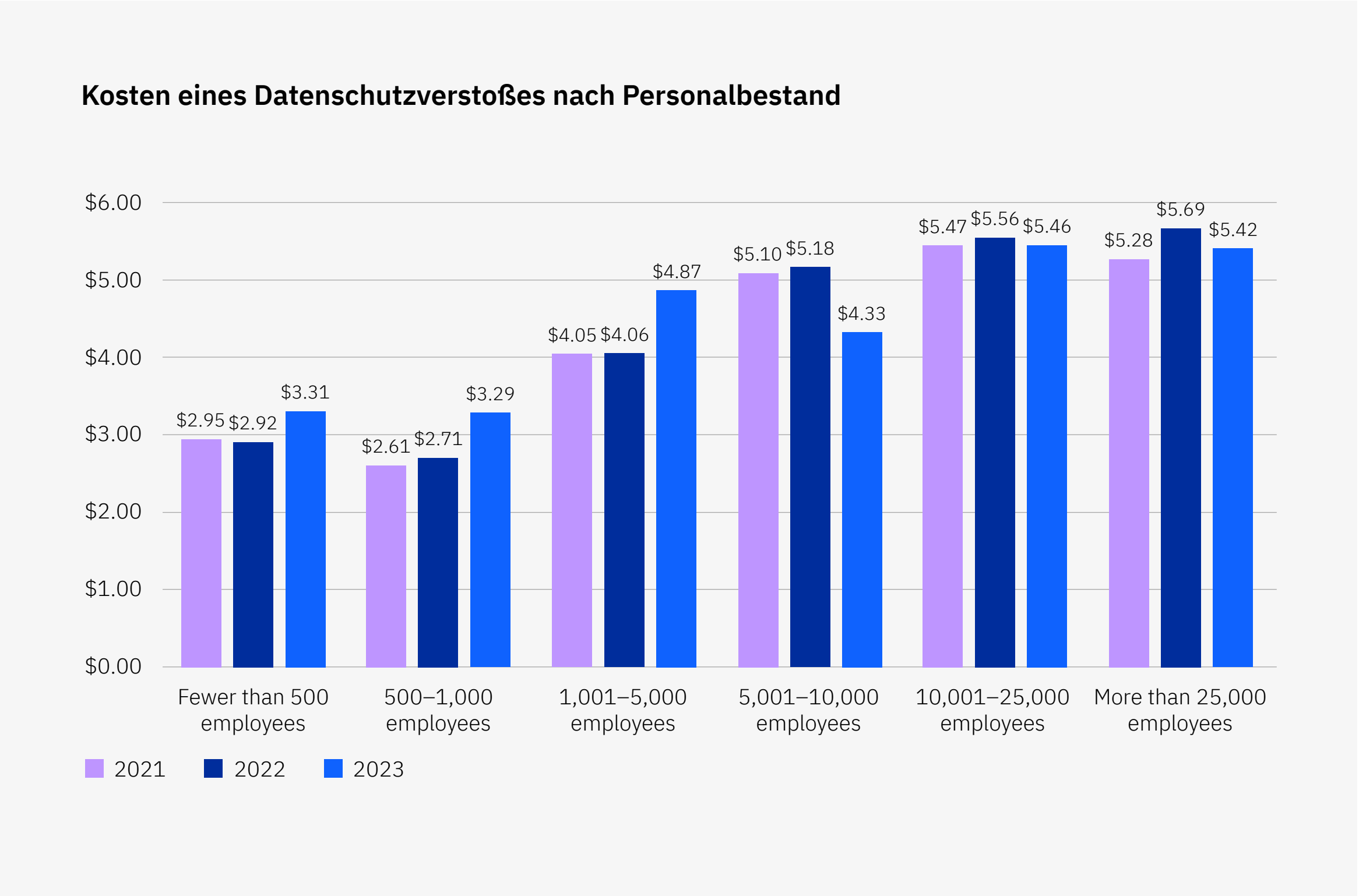
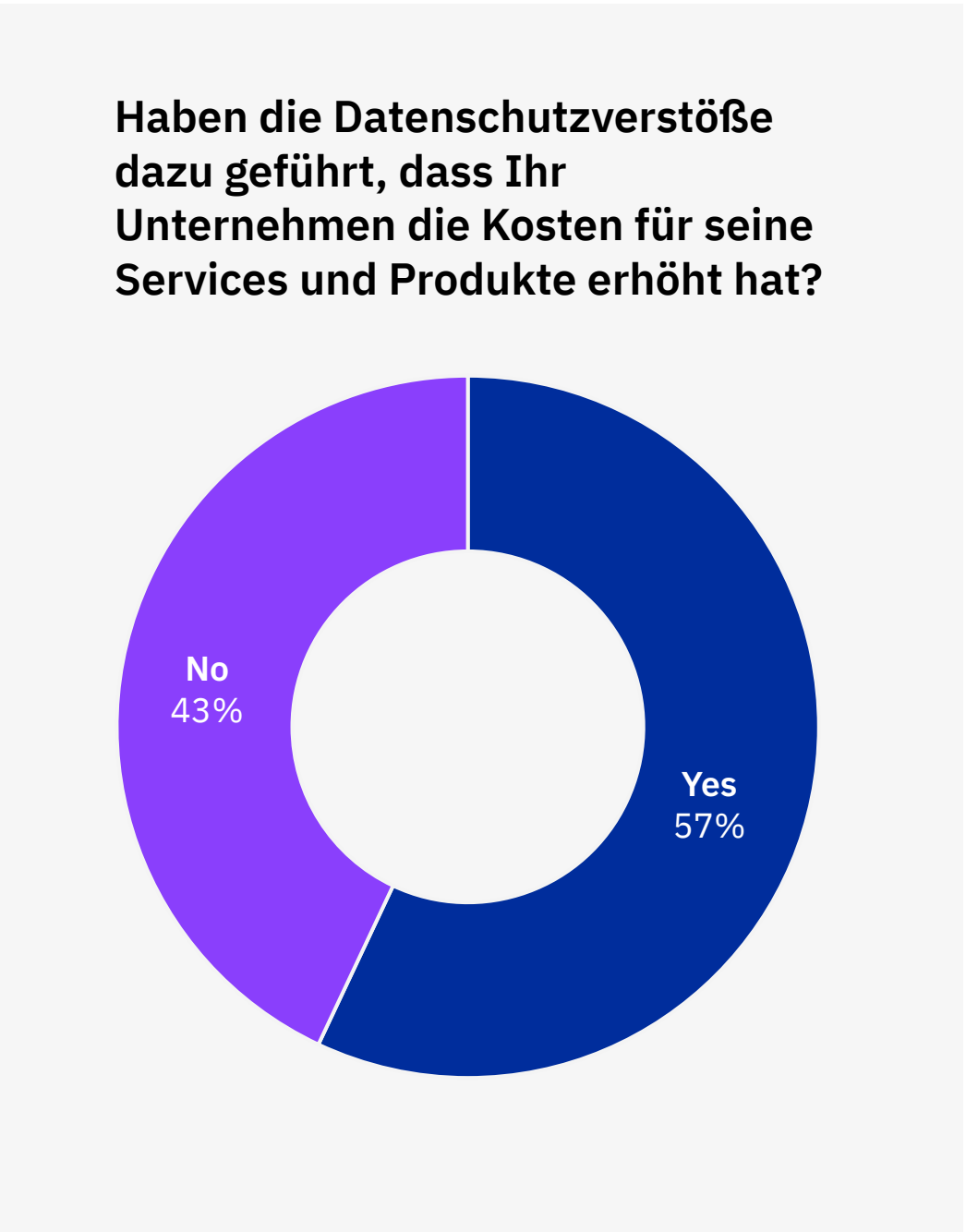


Abbildung 7. Angaben in°Mio.°US-Dollar





**Abbildung 8. Als Folge einer Datenschutzverletzung erhöhen die meisten Unternehmen die Preise für ihre Dienstleistungen und Produkte.**  
Die Mehrheit (57 %) der Befragten gab an, dass die Datenschutzverletzungen zu Preiserhöhungen bei ihren Geschäftsangeboten geführt haben, wodurch die Kosten an die Verbraucher weitergegeben wurden. Dieses Ergebnis ähnelt unserem Bericht aus dem Jahr 2022, in dem 60 % der Befragten angaben, die Preise erhöht zu haben.



Abbildung 8. Anteil an der Gesamtstichprobe der betroffenen Unternehmen



**Abbildungen 9a und 9b.**  
**Personenbezogene Daten von Kunden waren die kostspieligsten – und am häufigsten kompromittierten – Datensätze.**  
Von allen Datensatztypen war die Kompromittierung personenbezogener Daten von Kunden und Mitarbeitern am kostspieligsten. Im Jahr 2023 kosten personenbezogene Daten von Kunden wie Namen und Sozialversicherungsnummern Unternehmen 183 US-Dollar pro Datensatz, dicht gefolgt von personenbezogenen Mitarbeiterdaten mit 181 US-Dollar pro Datensatz. Anonymisierte Kundendaten sind mit 138 US-Dollar pro Datensatz im Jahr 2023 die kostengünstigste Datensatzkategorie.

Wie bereits 2022 und 2021 waren auch 2023 personenbezogene Kundendaten die am häufigsten von Verstößen betroffene Datensatzkategorie. 52 % aller Verstöße betrafen personenbezogene Kundendaten. Dies ist ein Anstieg um fünf Prozentpunkte gegenüber 2022, als 47 % aller kompromittierten Daten auf personenbezogene Kundendaten waren. Die zweithäufigste Datenkategorie waren personenbezogene Mitarbeiterdaten mit 40 %. Kompromittierte personenbezogene Daten von Mitarbeitern haben seit 2021, als sie nur 26 % aller kompromittierten Datensätze ausmachten, erheblich zugenommen.

Der Anteil des kompromittierten geistigen Eigentums ist seit 2022 um drei Prozentpunkte gestiegen, während der Anteil der anonymisierten Daten (Nicht-personenbezogene Daten) seit 2022 um sieben Prozentpunkte gesunken ist – von 33 % auf 26 %. Andere Unternehmensdaten, wie Finanzdaten und Kundenverzeichnisse, stiegen von 15 % der gefährdeten Daten im Jahr 2022 auf 21 % im Jahr 2023.

Typ der kompromittierten Daten

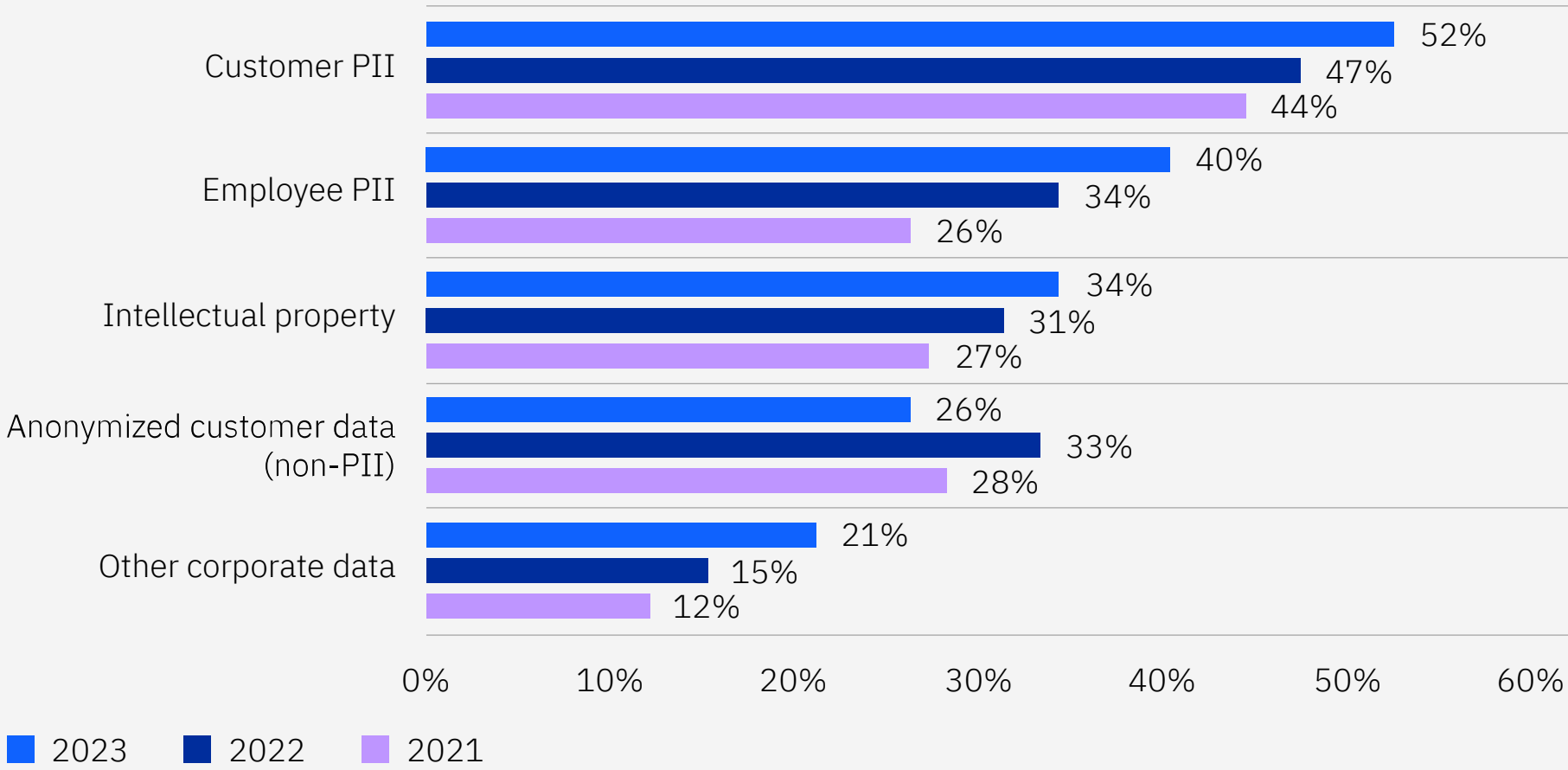


Abbildung 9a. Mehr als eine Antwort zulässig

Kosten pro Datensatz für einen Datenschutzverstoß nach Typ des kompromittierten Datensatzes



Abbildung 9b. Angaben in USD

## Primäre Angriffsvektoren

In diesem Abschnitt wird der ursprüngliche Angriffsvektor untersucht, der in der Studie für Datenschutzverstöße identifiziert wurde, und seine Auswirkungen auf die Kosten und den Zeitrahmen des Verstoßes. Der Bericht identifiziert die häufigsten Ursachen für Datenschutzverstöße und vergleicht die durchschnittlichen Kosten von Datenschutzverstößen für jede Kategorie sowie die durchschnittliche Zeit, die bis zur Erkennung und Eindämmung dieser Verstöße vergeht. Phishing und gestohlene oder kompromittierte Zugangsdaten waren die beiden häufigsten Angriffsvektoren im diesjährigen Bericht, und gehörten auch zu den vier kostspieligsten Arten von Sicherheitsvorfällen.

# 16 %

Prozentsatz der Sicherheitsverstöße, bei denen Phishing der ursprüngliche Angriffsvektor war

# 4,90 Mio. US-Dollar

Durchschnittliche Kosten eines Datenschutzverstoßes mit einem böswilligen Insider als ursprünglichem Angriffsvektor

**Abbildung 10. Phishing und gestohlene oder kompromittierte Zugangsdaten waren die beiden häufigsten ursprünglichen Angriffsvektoren.** Phishing und gestohlene oder kompromittierte Zugangsdaten waren für 16 % bzw. 15 % der Sicherheitsverletzungen verantwortlich, wobei Phishing mit knappem Vorsprung vor gestohlenen Zugangsdaten, die im Bericht 2022 der häufigste Vektor waren, an erster Stelle stand. Die fehlerhafte Konfiguration der Cloud wurde bei 11 % der Angriffe als Ausgangsvektor identifiziert, gefolgt von der Kompromittierung von Geschäfts-E-Mails mit 9 %. In diesem Jahr hat der Bericht zum ersten Mal sowohl Zero-Day-Sicherheitslücken (unbekannte Sicherheitslücken) als auch bekannte, nicht gepatchte Sicherheitslücken als Ursache

für Datenschutzverletzungen untersucht und festgestellt, dass mehr als 5 % der untersuchten Sicherheitsverletzungen auf bekannte Sicherheitslücken zurückzuführen sind, die noch nicht gepatcht wurden.

Obwohl sie mit 6 % relativ selten waren, verursachten Angriffe durch böswillige Insider mit durchschnittlich 4,90 Mio. US-Dollar die höchsten Kosten. Das sind 9,6 % mehr als die durchschnittlichen Kosten von 4,45 Mio. USD pro Datenschutzverletzung weltweit. Phishing war der am weitesten verbreitete Angriffsvektor und mit 4,76 Mio. US-Dollar der zweitteuerste. Sicherheitsverletzungen aufgrund von Systemfehlern waren mit durchschnittlich 3,96 Mio. US-Dollar am wenigsten kostspielig und mit 5 % der Verstöße auch am wenigsten verbreitet.

Kosten und Häufigkeit eines Datenschutzverstoßes nach ursprünglichem Angriffsvektor

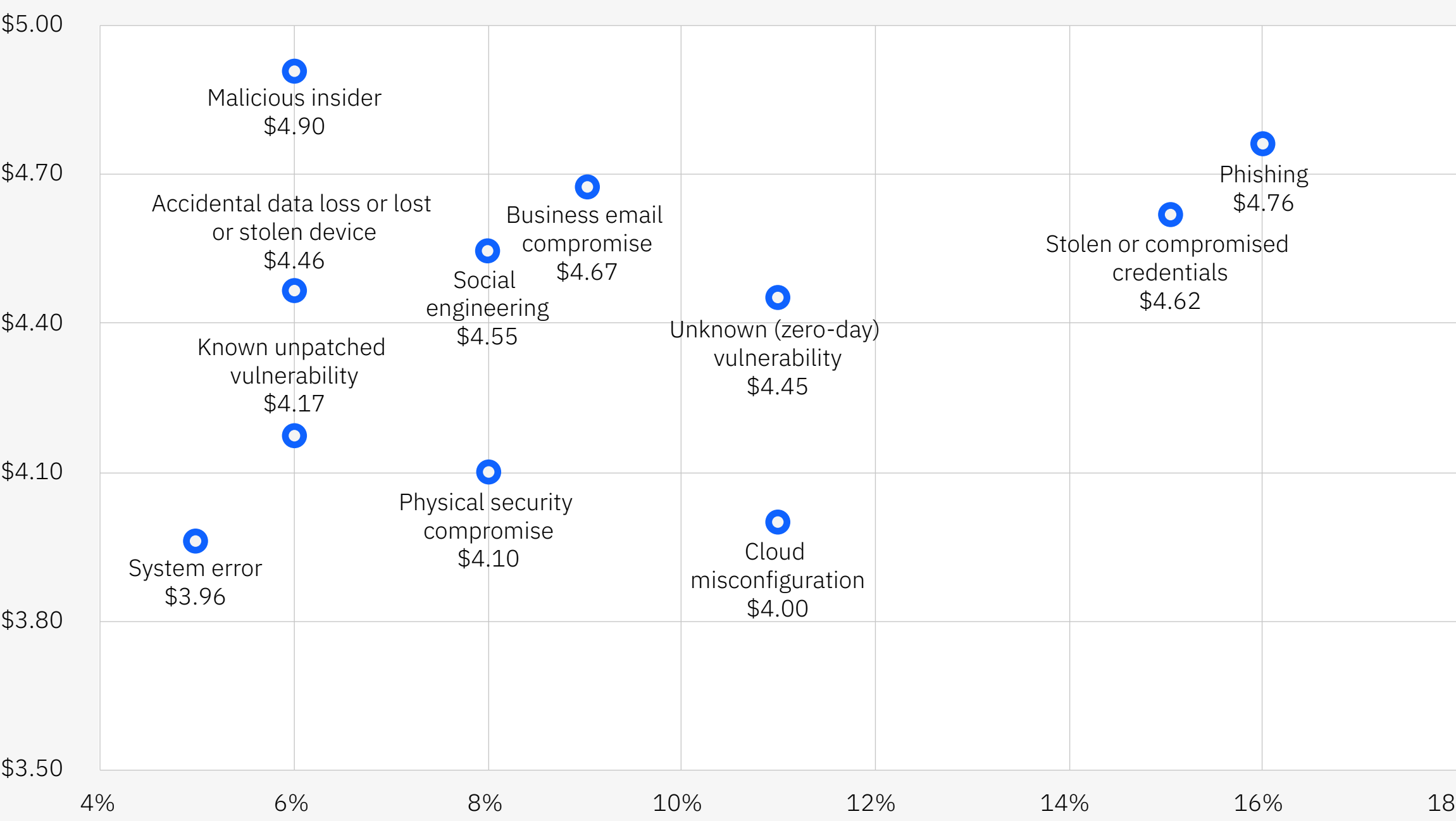


Abbildung 10. Angaben in°Mio.°US-Dollar



**Abbildung 11. Verstöße, die durch gestohlene oder kompromittierte Zugangsdaten und böswillige Insider eingeleitet wurden, dauerten am längsten.**

In diesem Jahr dauerte es durchschnittlich fast 11 Monate (328 Tage), um Datenschutzverletzungen zu erkennen und einzudämmen, die durch gestohlene oder kompromittierte Zugangsdaten verursacht wurden, und etwa 10 Monate (308 Tage), um Verstöße zu beheben, die durch böswillige Insider verursacht wurden. Diese beiden Vektoren, zusammen mit Phishing und der Kompromittierung von Geschäfts-E-Mails, waren auch für die teuersten Sicherheitsverletzungen verantwortlich.

Zum Vergleich: Die durchschnittliche Zeit, um einen Datenschutzverstoß zu erkennen und einzudämmen, betrug 277 Tage oder etwas mehr als neun Monate. Diese Zahl blieb in den letzten Berichtsjahren relativ konstant.

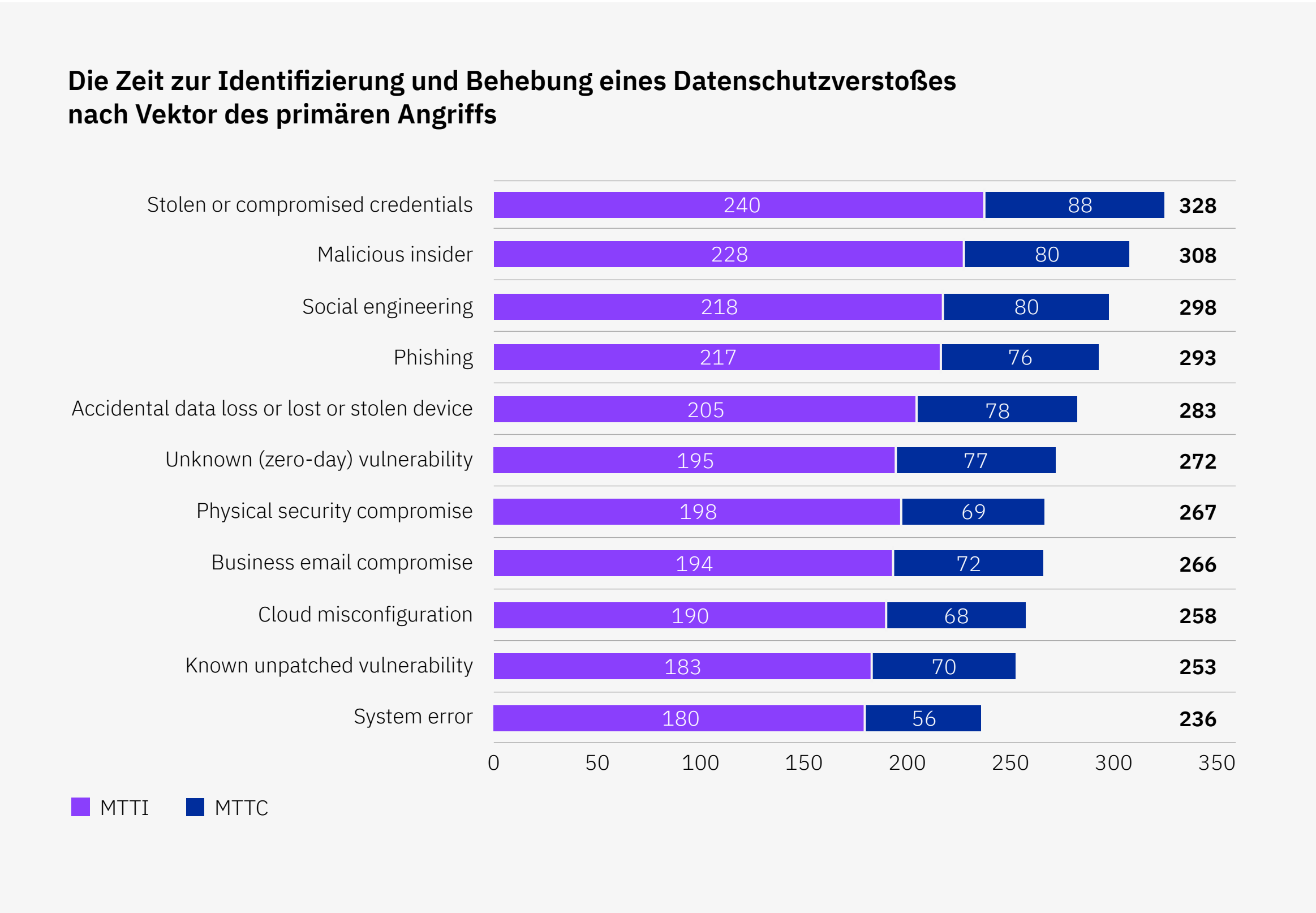
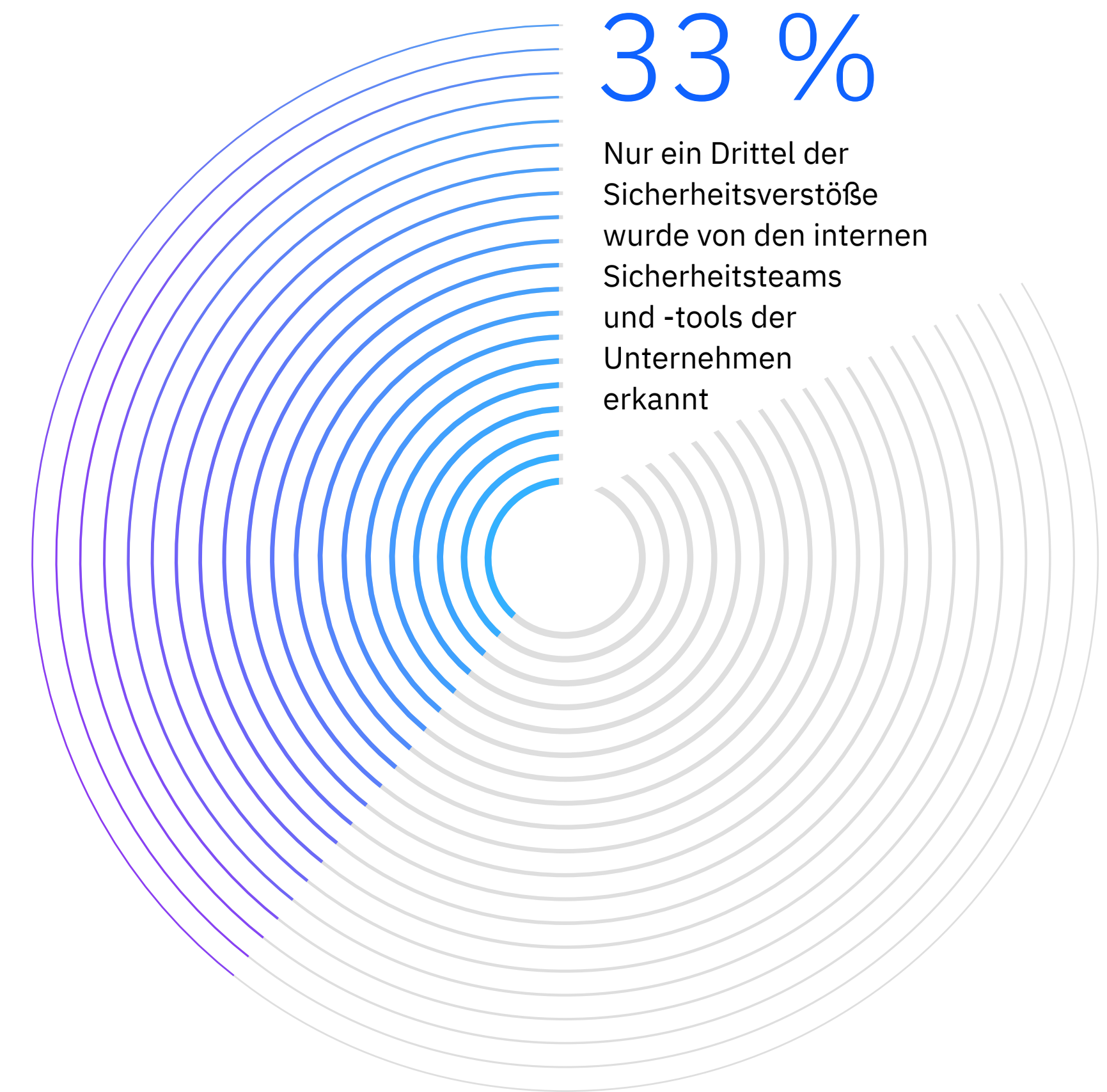


Abbildung 11. Angaben in Tagen

## Angriffe erkennen

Dieser Abschnitt befasst sich mit der Art und Weise, wie Verstöße aufgedeckt wurden, sowie mit den Unterschieden bei den Kosten und der Eindämmungszeit je nach Aufdeckungsmethode. Diese Analysen werden in diesem Jahr zum ersten Mal veröffentlicht. Es gibt drei Kategorien, die definieren, wie Sicherheitsverletzungen aufgedeckt werden: durch die internen Sicherheitsteams und -tools eines Unternehmens, einschließlich Managed Security Service Provider (MSSP); durch einen harmlosen Dritten, wie einen Sicherheitsforscher oder die Strafverfolgungsbehörden; und durch die Offenlegung durch den Angreifer, wie im Fall von Ransomware.



**Abbildung 12. Verstöße wurden am häufigsten von einer gutartigen dritten Partei festgestellt.**  
40 % der Sicherheitsverletzungen wurden von einem wohlwollenden Dritten oder einer externen Person aufgedeckt während 33 % der Verstöße von internen Teams und Tools identifiziert wurden. Mehr als ein Viertel oder 27 % der Sicherheitsverletzungen wurden vom Angreifer im Rahmen eines Ransomware-Angriffs aufgedeckt.

**Abbildung 13. Datenschutzverstöße, die vom Angreifer offengelegt werden, z. B. bei Ransomware, kosten deutlich mehr.**  
Angriffe, die von Angreifern aufgedeckt wurden, verursachten durchschnittliche Kosten in Höhe von 5,23 Mio. US-Dollar. Das ist ein Unterschied von 19,5 % oder 930.000 US-Dollar gegenüber den durchschnittlichen Kosten für Verstöße, die von internen Sicherheitsteams oder -werkzeugen aufgedeckt wurden (4,30 Mio. US-Dollar). Darüber hinaus kosten die von Angreifern aufgedeckten Verstöße 16,1 % oder 780.000 US-Dollar mehr als die durchschnittlichen Kosten von 4,45 Millionen US-Dollar für einen Datenschutzverstoß im Jahr 2023. Datenschutzverletzungen, die von den eigenen Sicherheitsteams und -tools eines Unternehmens aufgedeckt wurden, waren deutlich weniger kostspielig und kosteten fast 1 Mio. US-Dollar weniger als die vom Angreifer aufgedeckten Verstöße.

Wie wurde der Sicherheitsverstoß identifiziert?

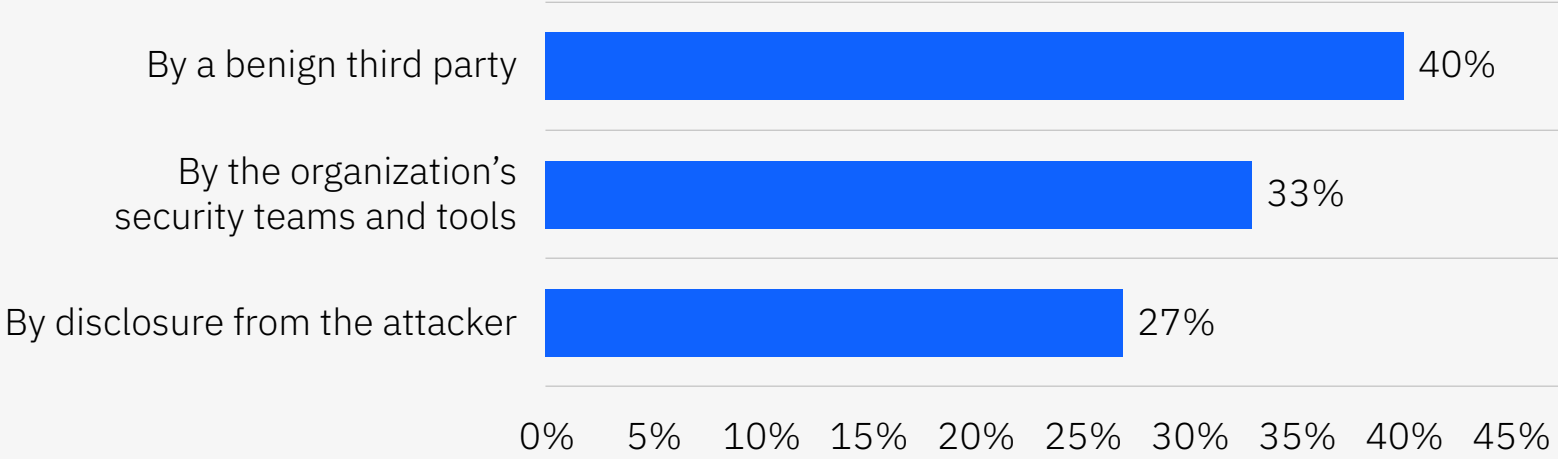


Abbildung 12. Nur eine Antwort ist zulässig

Kosten eines Datenschutzverstoßes, abhängig davon, wie der Verstoß festgestellt wurde

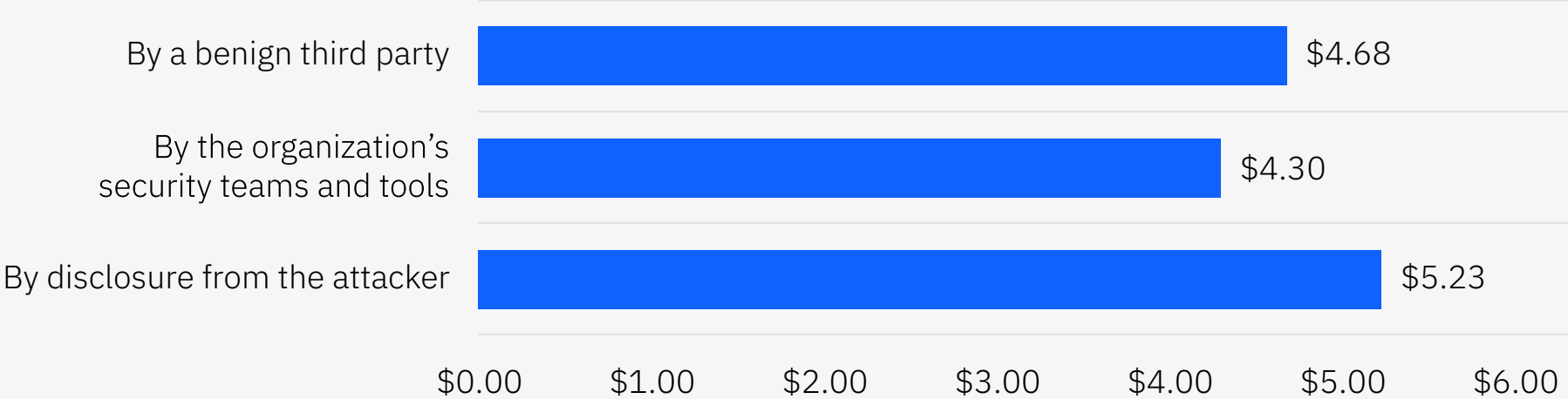


Abbildung 13. Angaben in°Mio.°US-Dollar





**Abbildung 14. Am längsten dauerte auch die Erkennung und Eindämmung von Datenschutzverletzungen.**  
Die Befragten benötigten durchschnittlich 320 Tage, um die vom Angreifer aufgedeckten Verstöße zu erkennen und einzudämmen. Dies sind 80 Tage oder 28,2 % mehr als bei den intern festgestellten Verstößen, bei denen es im Durchschnitt 241 Tage dauerte, bis sie erkannt und eingedämmt wurden. Im Durchschnitt dauerte es 47 Tage oder 15,9 % länger, eine von einem Angreifer entdeckte Sicherheitsverletzung zu erkennen und einzudämmen, als eine von einem harmlosen Dritten entdeckte Sicherheitsverletzung.

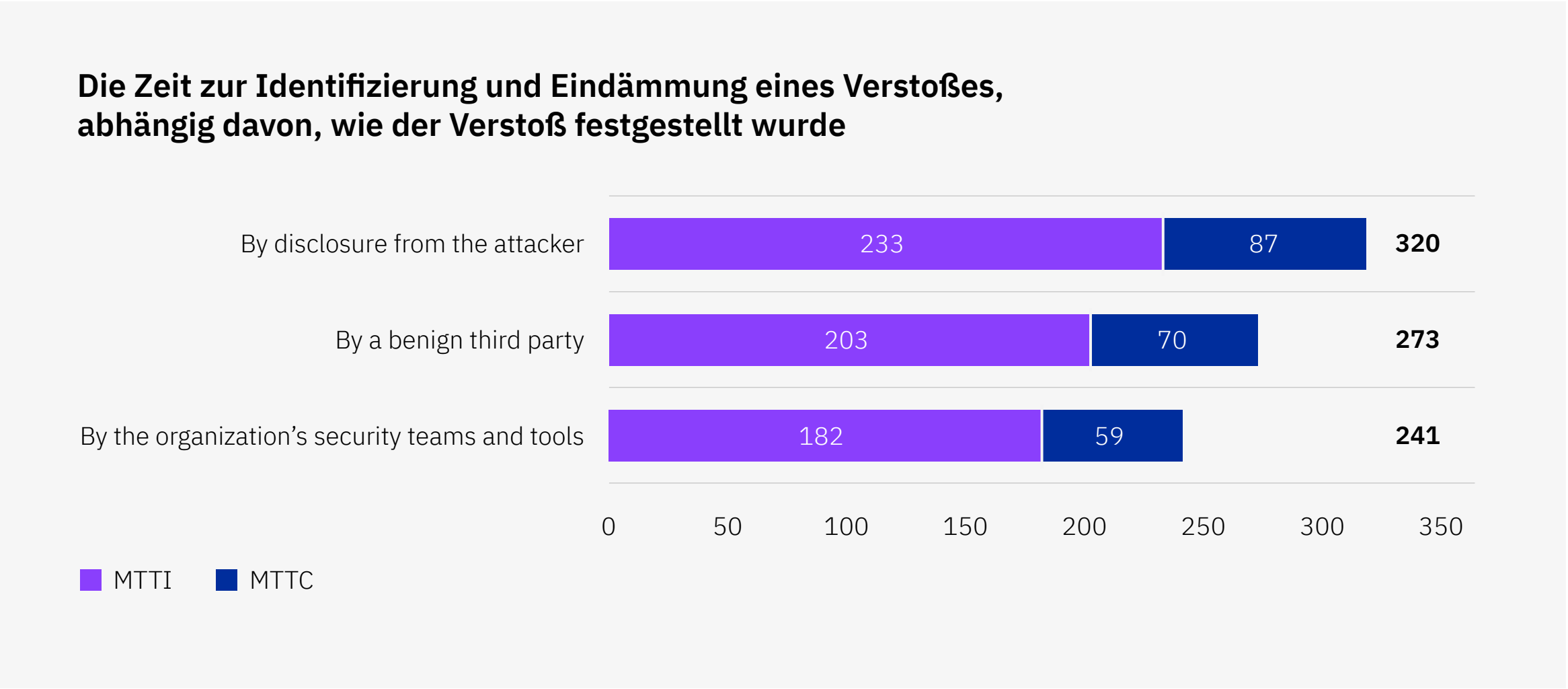


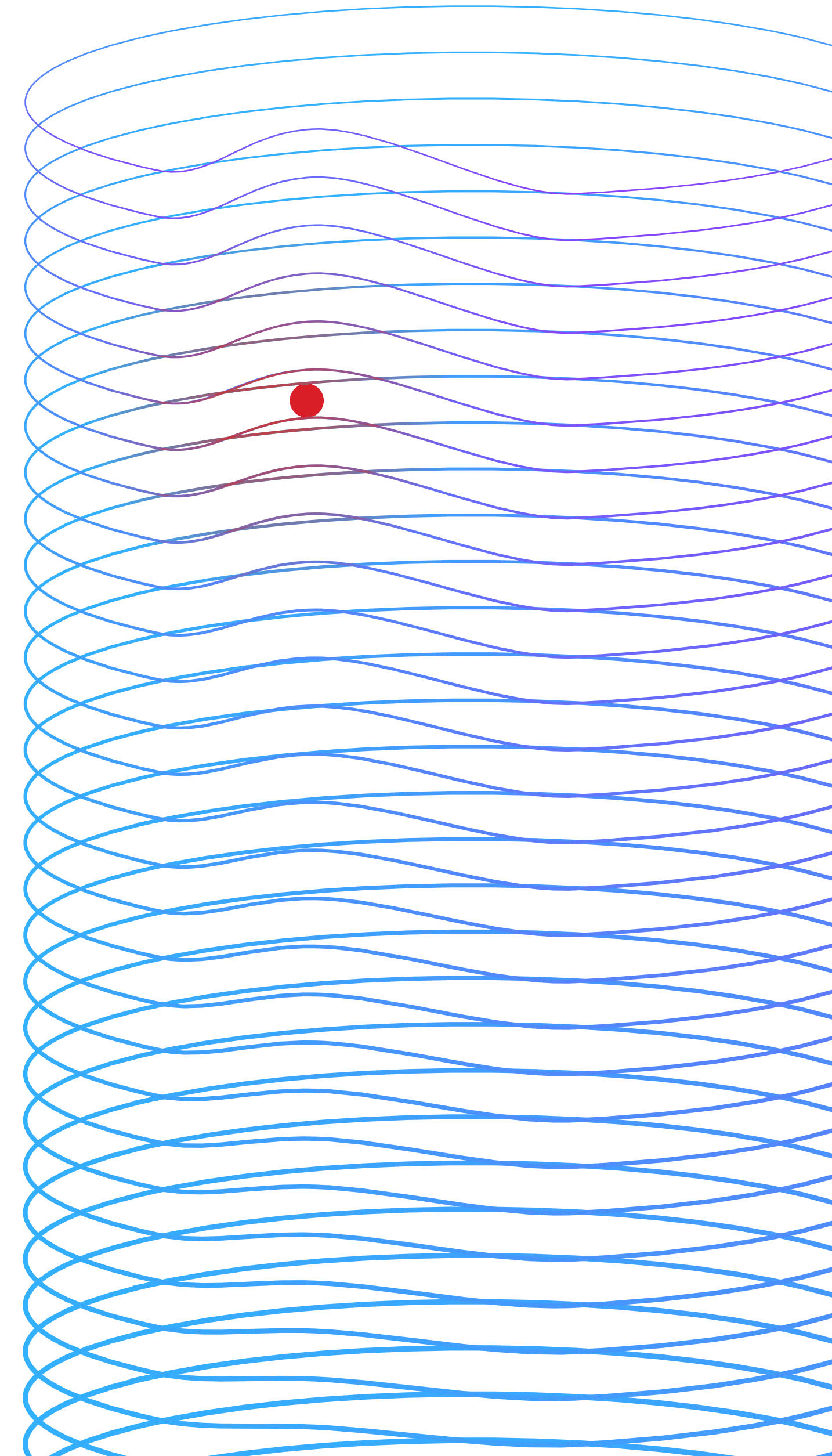
Abbildung 14. Angaben in Tagen

## Dauer der Datenschutzverletzungen

Der Lebenszyklus von Datenschutzverletzungen ist definiert als die Zeit, die zwischen der ersten Erkennung der Verletzung und ihrer Eindämmung verstreicht. Die „Zeit bis zur Erkennung“ beschreibt die Zeit in Tagen, die benötigt wird, um einen Vorfall zu entdecken. Die „Zeit bis zur Eindämmung“ bezieht sich auf die Zeit in Tagen, die ein Unternehmen benötigt, um die Situation zu lösen und den Service wiederherzustellen, nachdem die Verletzung entdeckt wurde. Diese beiden Metriken helfen dabei, die Effektivität der Reaktions- und Eindämmungsprozesse eines Unternehmens zu bestimmen.

# 277 Tage

Die Zeit zur Identifizierung und Behebung eines Datenschutzverstoßes



**Abbildung 15. Eine kürzere Dauer der Datenschutzverletzung wird weiterhin mit geringeren Kosten für Datenschutzverletzungen in Verbindung gebracht.**

Ein kürzerer Lebenszyklus einer Datenschutzverletzung von weniger als 200 Tagen war mit durchschnittlichen Kosten von 3,93 Mio. US-Dollar verbunden. Ein längerer Zyklus von mehr als 200 Tagen ist hingegen mit durchschnittlichen Kosten von 4,95 Mio. US-Dollar verbunden. Dies entspricht einer Differenz von 23 % und einer Kostenersparnis von 1,02 Mio. US-Dollar für den kürzeren Lebenszyklus.

In den vergangenen Jahren lagen die durchschnittlichen Kosten von Datenschutzverletzungen auf der Grundlage eines 200-Tage-Lebenszyklus relativ konstant, auch wenn sie sich schrittweise verändert haben. Bei einem Lebenszyklus einer Datenschutzverletzung von weniger als 200 Tagen stieg der Wert um 5,1 % auf 3,93 Mio. US-Dollar für 2023, gegenüber den Durchschnittskosten im Vorjahr von 3,74 Mio. US-Dollar. Bei einem Lebenszyklus einer Datenschutzverletzung von mehr als 200 Tagen stieg der Wert im Jahr 2023 um 1,9 % auf 4,95 Mio. US-Dollar gegenüber den durchschnittlichen Kosten im Vorjahr von 4,86 Mio. US-Dollar. Die im Jahr 2023 gemeldeten durchschnittlichen Kosteneinsparungen von 1,02 Mio. US-Dollar bedeuten einen Rückgang um 8,9 % gegenüber den Kosteneinsparungen von 1,12 Mio. US-Dollar im Jahr 2022.

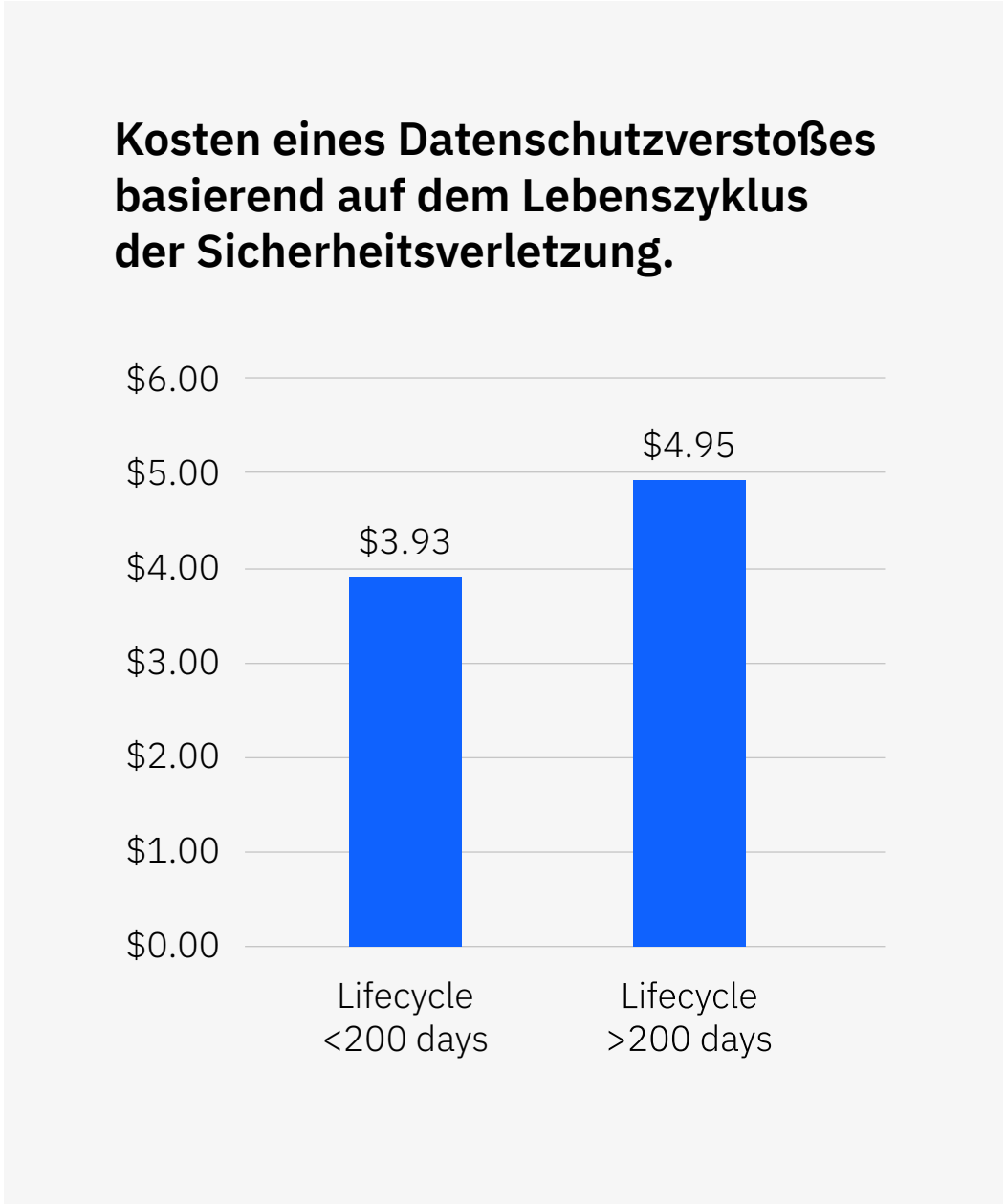


Abbildung 15. Angaben in Mio. US-Dollar



## Wesentliche Kostenfaktoren

Einer der vielen Faktoren, die die durchschnittlichen Kosten einer Datenschutzverletzung beeinflussen, sind die Sicherheitstechnologien und -praktiken, die in einem Unternehmen eingesetzt werden. In diesem Abschnitt werden 27 Kostenfaktoren quantifiziert, um Entscheidungsträgern in den Bereichen Sicherheit und Risiko zu helfen, das Ausmaß zu verstehen, in dem diese Faktoren die Kosten erhöhen oder reduzieren. Diese Faktoren sind nicht additiv. Es entspricht also nicht der Forschungsmethodik, mehrere Kostenfaktoren zu addieren, um die potenziellen Kosten einer Verletzung zu berechnen.

In diesem Jahr berücksichtigt der Bericht über die Kosten einer Datenschutzverletzung mehrere neue Faktoren, darunter Verletzungen in der Lieferkette, ASM-Tools, Software für Datensicherheit und -schutz, EDR-Tools, Bedrohungsdaten, proaktives Thread-Hunting, Reaktionsteams und SOAR-Tools (Security Orchestration, Automation and Response).

# 5,36 Mio. US-Dollar

Durchschnittliche Kosten einer Sicherheitsverletzung für Unternehmen mit einem hohen Mangel an Sicherheitskompetenzen

**Abbildung 16. Der Einfluss von 27 Faktoren auf die durchschnittlichen Kosten einer Datenschutzverletzung.** Das Diagramm zeigt den durchschnittlichen Kostenunterschied von Sicherheitsverletzungen bei Unternehmen mit diesen Kostenfaktoren im Vergleich zu den durchschnittlichen Gesamtkosten für Datenschutzverletzungen von 4,45 Mio. US-Dollar. Kostenmindernde Faktoren beschreiben jene Aspekte von Sicherheitsverletzungen, die mit unterdurchschnittlichen Kosten verbunden sind. Kostensteigernde Faktoren sind hingegen mit überdurchschnittlichen Kosten verbunden.

Die drei Faktoren, die am effektivsten zur Kostenreduzierung beitragen und mit den höchsten Kostenreduzierungen verbunden sind, sind die Einführung eines DevSecOps-Ansatzes, Mitarbeiterschulungen sowie IR-Planung

und -Tests. So lagen die durchschnittlichen Kosten für Datenschutzverletzungen in Unternehmen mit einem DevSecOps-Ansatz rund 249.000 US-Dollar unter den durchschnittlichen Kosten für Datenschutzverletzungen im Jahr 2023 in Höhe von 4,45 Mio. US-Dollar – also etwa bei 4,20 Mio. US-Dollar.

Die größten kostensteigernden Faktoren waren die Komplexität der Sicherheitssysteme, der Mangel an Sicherheitskräften und die Nichtkonformität mit Vorschriften. So lagen die durchschnittlichen Kosten von Sicherheitsverletzungen in Unternehmen mit komplexen Sicherheitssystemen rund 241.000 US-Dollar über den durchschnittlichen Kosten einer Datenschutzverletzung im Jahr 2023 in Höhe von 4,45 Mio. US-Dollar – also bei rund 4,69 Mio. US-Dollar.

Auswirkungen wichtiger Faktoren auf die Gesamtkosten einer Datenschutzverletzung

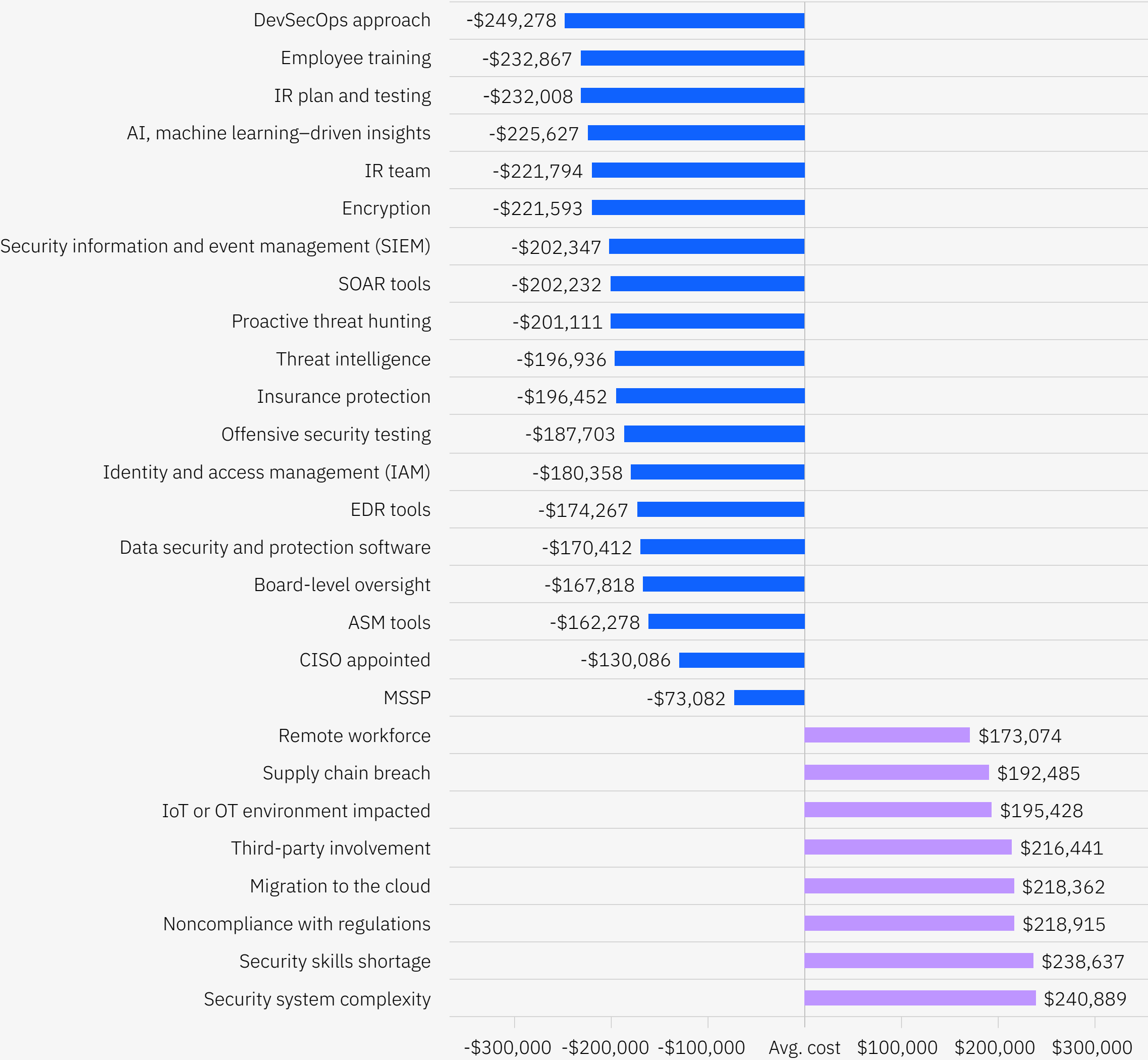


Abbildung 16. Angaben in USD

**Abbildung 17. Die drei wirkungsvollsten Kostenverstärker aus 27 Faktoren.**

Dieses Diagramm vergleicht Unternehmen mit der höchsten Ausprägung eines der wichtigsten Kostensteigerungsfaktoren mit denen mit der niedrigsten Ausprägung, was in einigen Fällen bedeuten kann, dass derselbe Faktor nicht vorkommt. Dieser Vergleich unterscheidet sich von der vorherigen Analyse (Abbildung 16), bei der eine hohe Präsenz dieser Faktoren mit dem Mittelwert verglichen wird. Es konnte eine Differenz von 1,58 Mio. US-Dollar oder 34,6 % zwischen Unternehmen mit einem hohen und einem geringen Mangel an Sicherheitskompetenzen beobachtet werden. Das entspricht einer Differenz von 1,44 Mio. US-Dollar oder 31,6 %, die zwischen Unternehmen mit hoher bzw. niedriger Komplexität des Sicherheitssystems besteht. Außerdem gab es eine Differenz von 1,04 Mio. US-Dollar oder 23 % zwischen einem hohen und einem niedrigen Niveau der Nichtkonformität mit Vorschriften.

Unternehmen mit einem starken Mangel an Sicherheitskompetenzen hatten durchschnittliche Kosten in Höhe von 5,36 Mio. US-Dollar und damit 910.000 US-Dollar mehr als die durchschnittlichen Kosten einer Datenschutzverletzung. Das entspricht einer Differenz von 18,6 %. Unternehmen mit einer hohen Komplexität des Sicherheitssystems hatten durchschnittliche Kosten in Höhe von 5,28 Mio. US-Dollar. Dies entspricht einer Differenz von 830.000 US-Dollar oder 17,1 % im Vergleich zu den durchschnittlichen Kosten einer Datenschutzverletzung. Unternehmen mit einem hohen Grad an Nichtkonformität mit Vorschriften wiesen durchschnittliche Kosten von 5,05 Mio. US-Dollar auf und übertrafen damit die durchschnittlichen Kosten einer Datenschutzverletzung um 560.000 US-Dollar, was einer Differenz von 12,6 % entspricht.

**Kosten einer Datenschutzverletzung für Unternehmen mit einem hohen bzw. niedrigen Niveau der drei kostensteigernden Faktoren**

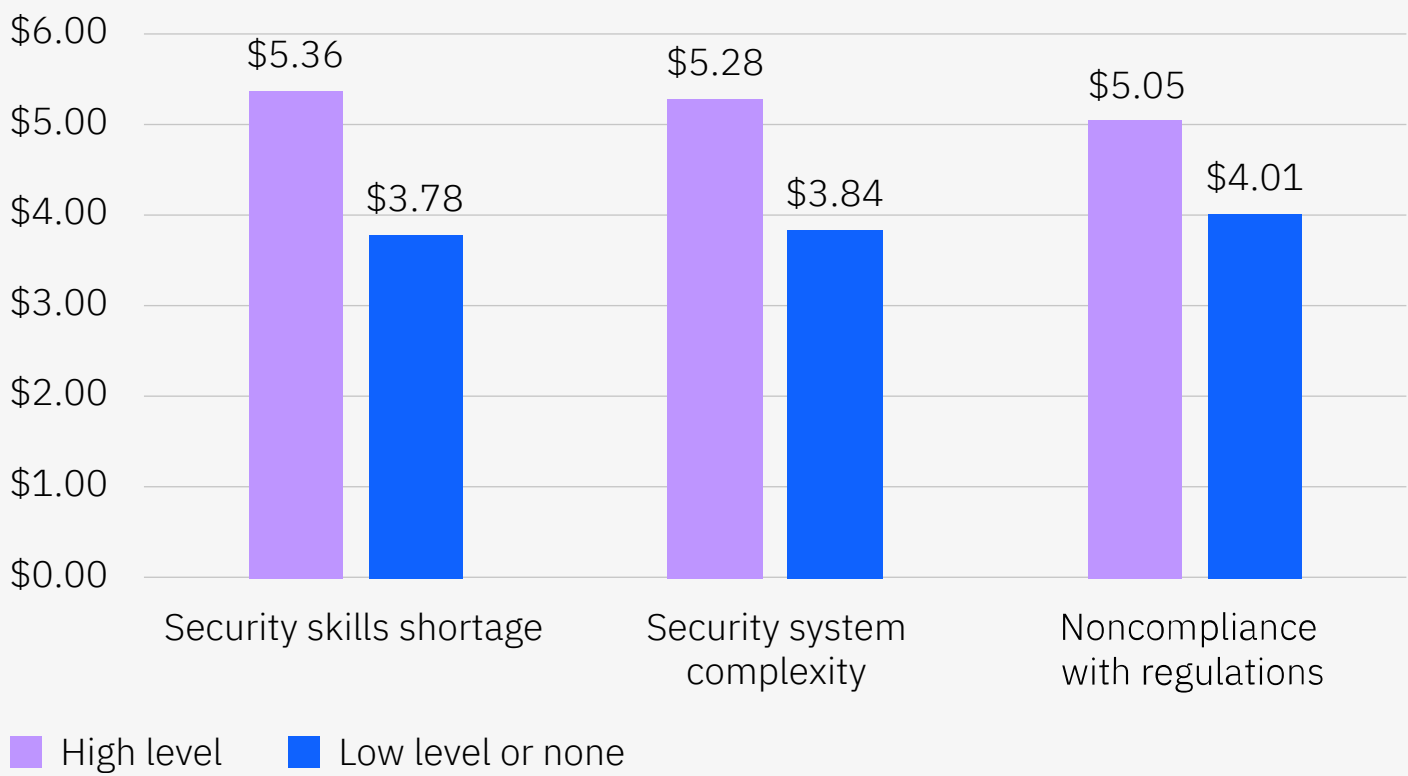


Abbildung 17. Angaben in Mio. US-Dollar



**Abbildung 18. Die drei wirksamsten Kostenreduzierer von insgesamt 27 Faktoren.**  
Das Diagramm vergleicht Unternehmen mit der höchsten Ausprägung eines der wichtigsten Kostenminderungsfaktoren mit denen mit der niedrigsten Ausprägung, was in einigen Fällen bedeuten kann, dass derselbe Faktor nicht vorkommt. Die durchschnittlichen Kosten einer Sicherheitsverletzung wiesen eine Differenz von 1,68 Mio. US-Dollar oder 38,4 % zwischen Unternehmen mit einem hohen und einem niedrigen Niveau an DevSecOps auf. Es lag eine Differenz von 1,49 Mio. US-Dollar oder 34,1 % zwischen hohen Niveaus und wenig bis gar keinen IR-Planungen und -Tests vor. Und schließlich gab es eine Differenz von 1,5 Mio. US-Dollar oder 33,9 % zwischen einem hohen und einem niedrigen Niveau der Mitarbeiterschulung.

Unternehmen mit einem hohen Maß an diesen Kostenminderungsfaktoren hatten deutlich geringere Kosten für eine Datenschutzverletzung als der Durchschnitt. Bei denjenigen Nutzern, die gut entwickelte DevSecOps einsetzen, beliefen sich die durchschnittlichen Kosten auf 3,54 Mio. US-Dollar – ein Unterschied von 910.000 US-Dollar oder 22,8 % im Vergleich zu den durchschnittlichen Gesamtkosten einer Datenschutzverletzung. Unternehmen mit einem gering entwickelten DevSecOps-Ansatz hatten im Durchschnitt Kosten in Höhe von 5,22 Mio. US-Dollar, was eine deutliche Differenz von 770.000 US-Dollar oder 15,9 % zu den durchschnittlichen Kosten einer Datenschutzverletzung darstellt.

**Kosten einer Datenschutzverletzung für Unternehmen mit einem hohen bzw. niedrigen Niveau der drei Kostenminderungsfaktoren**

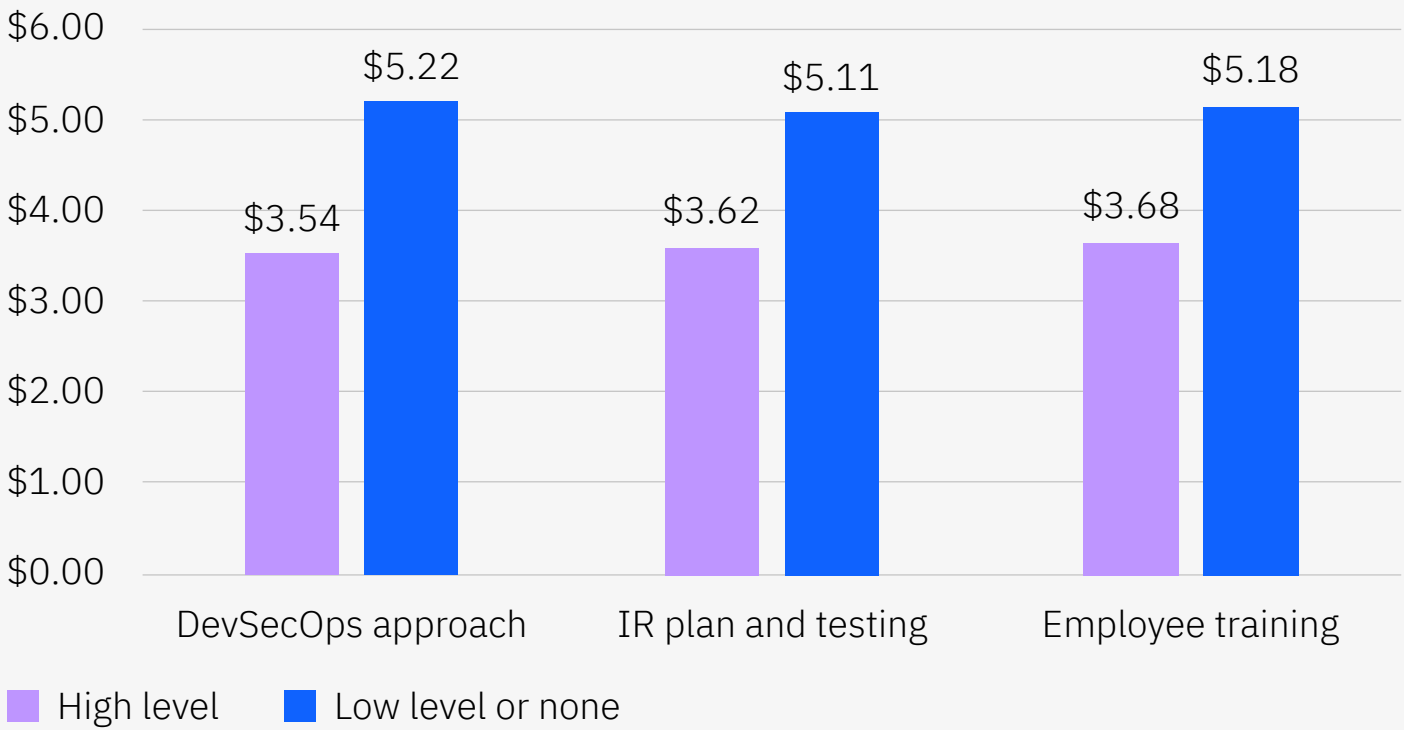
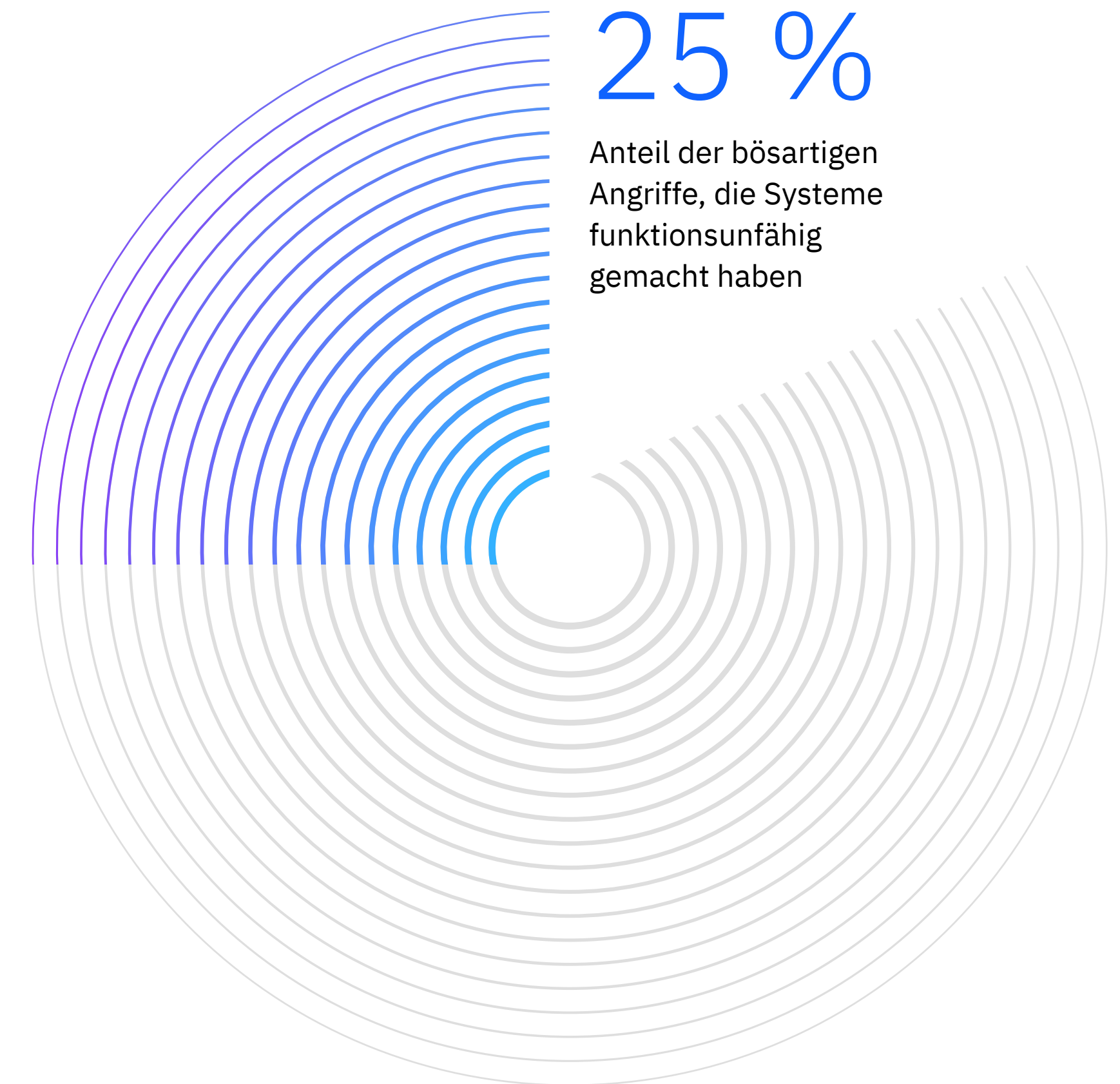


Abbildung 18. Angaben in Mio. US-Dollar

## Ransomware und destruktive Angriffe

In diesem Jahr machten Ransomware und destruktive Angriffe<sup>3</sup> 24 % bzw. 25 % der böswilligen Angriffe aus.

Wie im Bericht von 2022 haben wir den Lebenszyklus solcher Sicherheitsverletzungen und die Auswirkungen der Zahlung eines Lösegelds im Vergleich zur Nichtzahlung untersucht. In dieser Studie werden die Kosten des Lösegelds bei der Berechnung der Gesamtkosten der Verletzung nicht berücksichtigt. Im Bericht 2023 haben wir zum ersten Mal untersucht, welchen Einfluss das Einschalten der Strafverfolgungsbehörden bei der Eindämmung eines Ransomware-Angriffs hat.



**Abbildung 19. Bei fast einem Viertel der Angriffe handelte es sich um Ransomware.**  
Zu den destruktiven Angriffen, die Systeme funktionsunfähig machen, zählte einer von vier Angriffen. Bei weiteren 24 % handelte es sich um Ransomware. Angriffe auf Geschäftspartner und die Software-Lieferkette machten 15 % bzw. 12 % der Angriffe aus.

**Abbildung 20. Die Kosten für Ransomware-Angriffe sind erheblich gestiegen.**  
Die durchschnittlichen Kosten eines Ransomware-Angriffs stiegen im Bericht 2023 mit 5,13 Mio. US-Dollar um 13 % gegenüber den durchschnittlichen Kosten von 4,54 Mio. US-Dollar im Bericht 2022. Mit 5,24 Mio. US-Dollar stiegen die durchschnittlichen Kosten eines destruktiven Angriffs im Bericht 2023 ebenfalls um 2,3 % gegenüber den durchschnittlichen Kosten von 5,12 Mio. US-Dollar im Bericht 2022.

Anteil der gesamten Verstöße nach Typ des böswilligen Angriffs

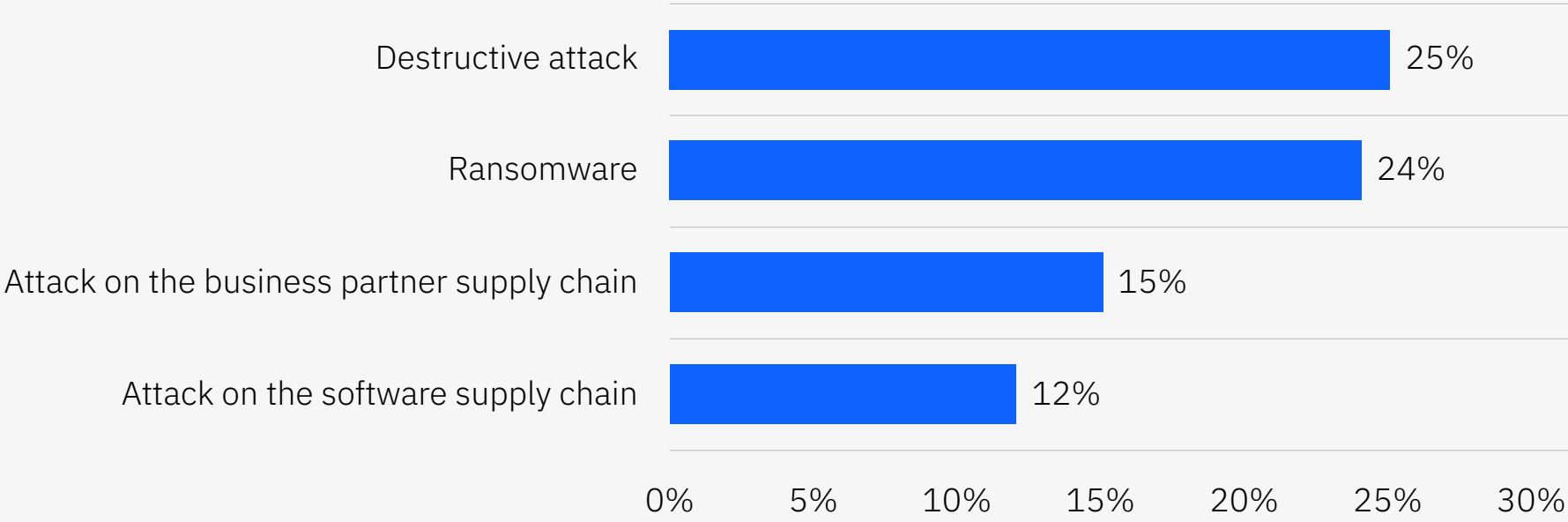


Abbildung 19. Die prozentualen Anteile der einzelnen Angriffstypen an der Gesamtzahl der Verletzungen; die Summe der Balken ergibt nicht 100 %.

Kosten eines Ransomware- oder destruktiven Angriffs

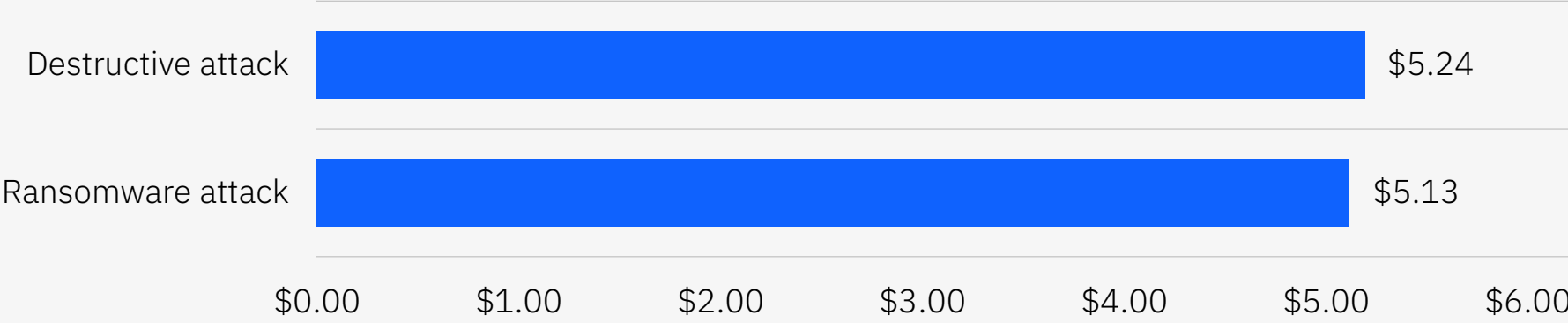


Abbildung 20. Angaben in Mio. US-Dollar



**Abbildungen 21 und 22. Unternehmen, die Strafverfolgungsbehörden einbezogen, konnten erhebliche Zeit- und Kosteneinsparungen erzielen.** 37 % der Ransomware-Opfer entschieden sich dafür, die Strafverfolgungsbehörden nicht einzuschalten, um einen Ransomware-Angriff einzudämmen. Bei denjenigen, die die Strafverfolgungsbehörden einschalteten, waren die Ransomware-Verletzungen insgesamt weniger kostspielig. Die durchschnittlichen Kosten eines Ransomware-Verstoßes betrugen 5,11 Mio. US-Dollar, wenn die Strafverfolgungsbehörden nicht involviert waren, und 4,64 Mio. US-Dollar, wenn die Strafverfolgungsbehörden involviert waren. Das entspricht einer Differenz von 9,6 % oder 470.000 US-Dollar.

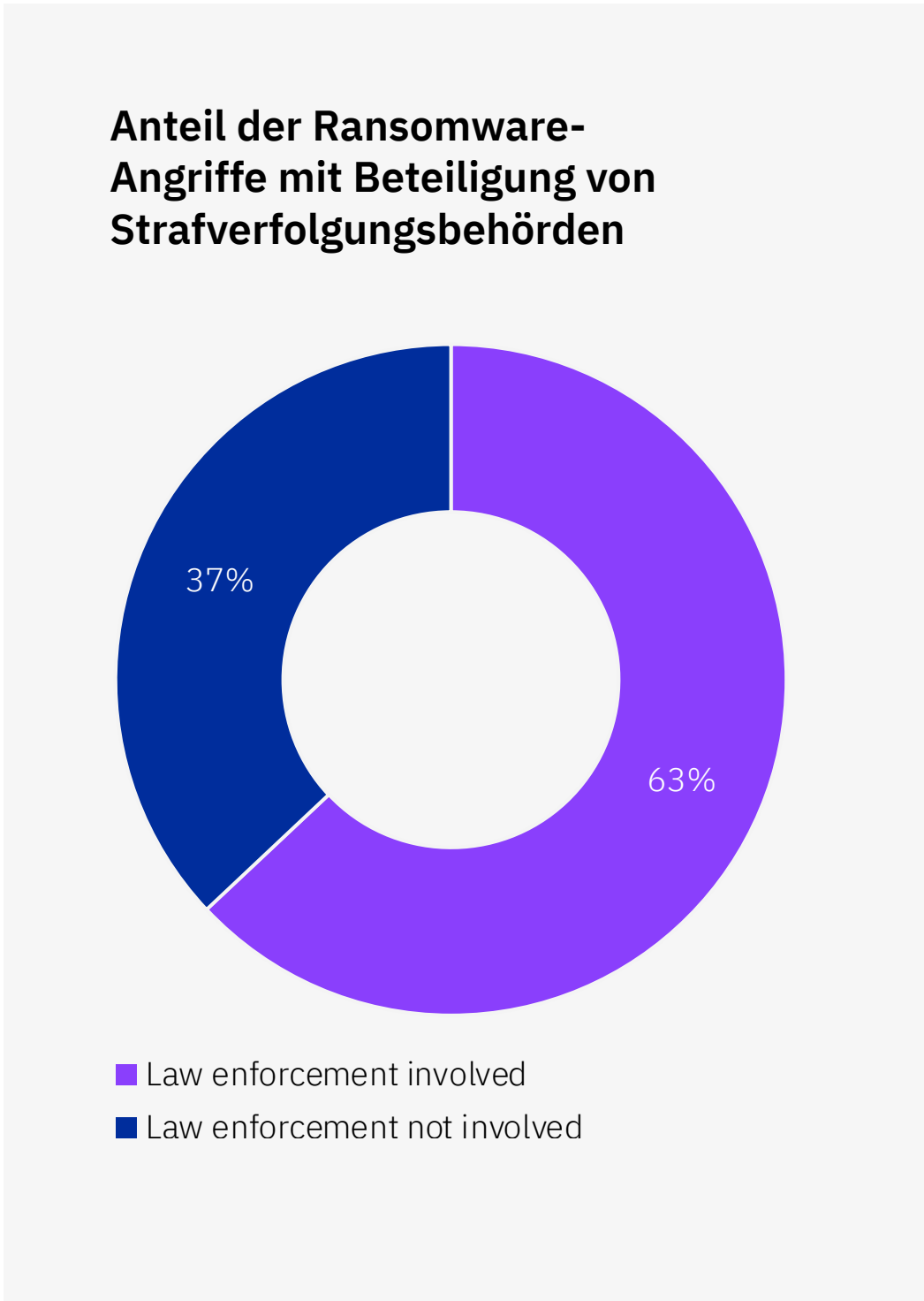


Abbildung 21. Anteil aller Ransomware-Angriffe

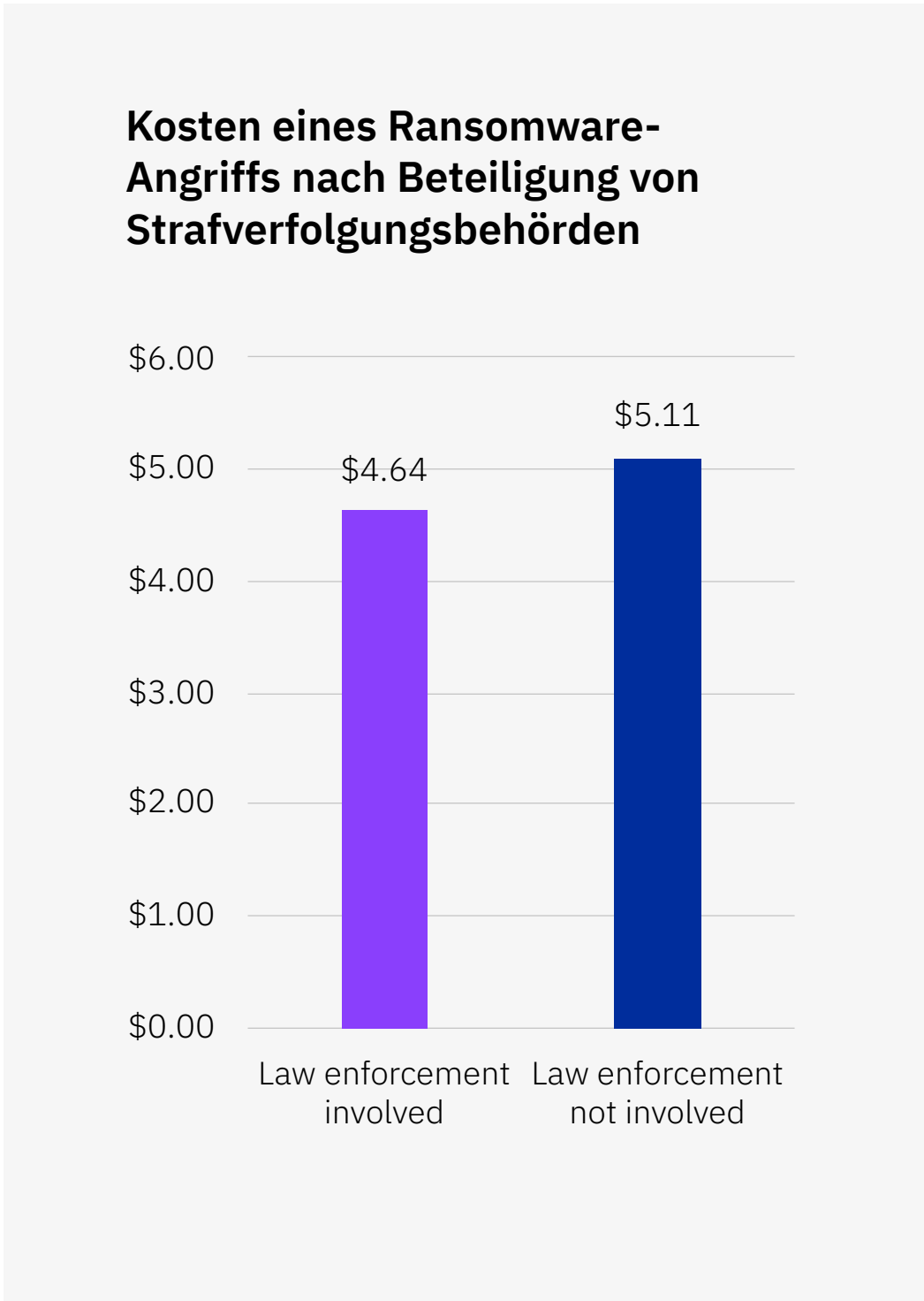


Abbildung 22. Angaben in°Mio.°US-Dollar

# Die Zeit zur Identifizierung und Eindämmung eines Ransomware-Angriffs mit Beteiligung der Strafverfolgungsbehörden

Abbildung 23. Angaben in Tagen

**Abbildung 23. Strafverfolgungsbehörden haben dazu beigetragen, die Zeit zur Erkennung und Eindämmung von Ransomware-Verletzungen zu verkürzen.**  
Die Gesamtzeit für die Erkennung und Eindämmung einer Ransomware-Verletzung war um 11,4 % bzw. 33 Tage kürzer, wenn die Strafverfolgungsbehörden involviert waren, mit insgesamt 273 Tagen im Vergleich zu 306 Tagen.  
Die durchschnittliche Zeit zur Eindämmung eines Ransomware-Verstoßes betrug 63 Tage bzw. 23,8 % weniger, wenn die Strafverfolgungsbehörden beteiligt waren, verglichen mit 80 Tagen ohne Beteiligung.  
Es zeigt sich, dass das Einschalten von Strafverfolgungsbehörden dazu beitragen kann, die Kosten und die Dauer einer Ransomware-Verletzung zu reduzieren.

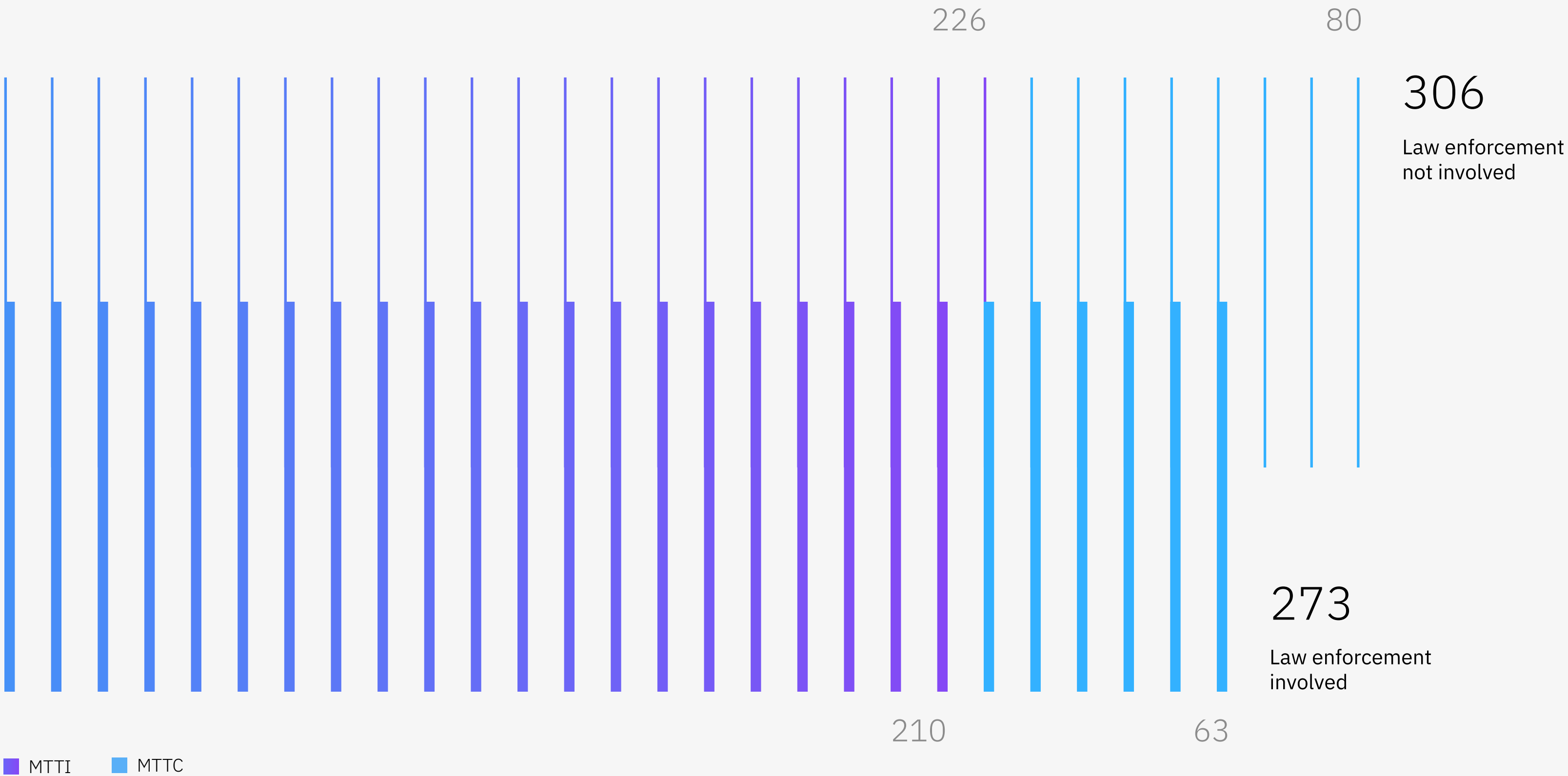


Abbildung 24. Automatisierte Antwort-Playbooks oder -Workflows verkürzen die Zeit bis zur Eindämmung eines Ransomware-Angriffs.

Von den Unternehmen, die Opfer eines Ransomware-Angriffs wurden, waren diejenigen, die über automatisierte Antwort-Playbooks oder -Workflows speziell für Ransomware-Angriffe verfügten, in der Lage, diese in 68 Tagen, also um 16 % schneller einzudämmen, verglichen mit dem Durchschnitt von 80 Tagen für Unternehmen ohne Antwort-Playbooks oder -Workflows.

Abbildung 25. Die Zahlung des Lösegelds führte zu minimalen Kosteneinsparungen.

Unternehmen, die während eines Ransomware-Angriffs Lösegeld gezahlt haben, erzielten nur einen geringen Unterschied bei den Gesamtkosten,

nämlich 5,06 Mio. US-Dollar im Vergleich zu 5,17 Mio. US-Dollar, ein Kostenunterschied von 110.000 US-Dollar oder 2,2 %. Diese Berechnung beinhaltet jedoch nicht die Lösegeldkosten selbst. Angesichts der hohen Kosten der meisten Ransomware-Forderungen haben Unternehmen, die das Lösegeld gezahlt haben, wahrscheinlich insgesamt mehr ausgegeben als Unternehmen, die das Lösegeld nicht gezahlt haben. Im Bericht für das Jahr 2022 beliefen sich die Kosteneinsparungen auf insgesamt 630.000 US-Dollar, was einer Kostendifferenz von 13,1 % entspricht, wobei auch hier die Kosten für das Lösegeld selbst nicht berücksichtigt sind. Die Daten zeigen, dass die Zahlung von Lösegeld zunehmend unvorteilhafter geworden ist, mit einem Rückgang der Einsparungen um 82,5 % im Vorjahresvergleich.

Auswirkungen von automatisierten Reaktionsplänen oder Workflows für Ransomware auf die Zeit bis zur Eindämmung eines Ransomware-Angriffs

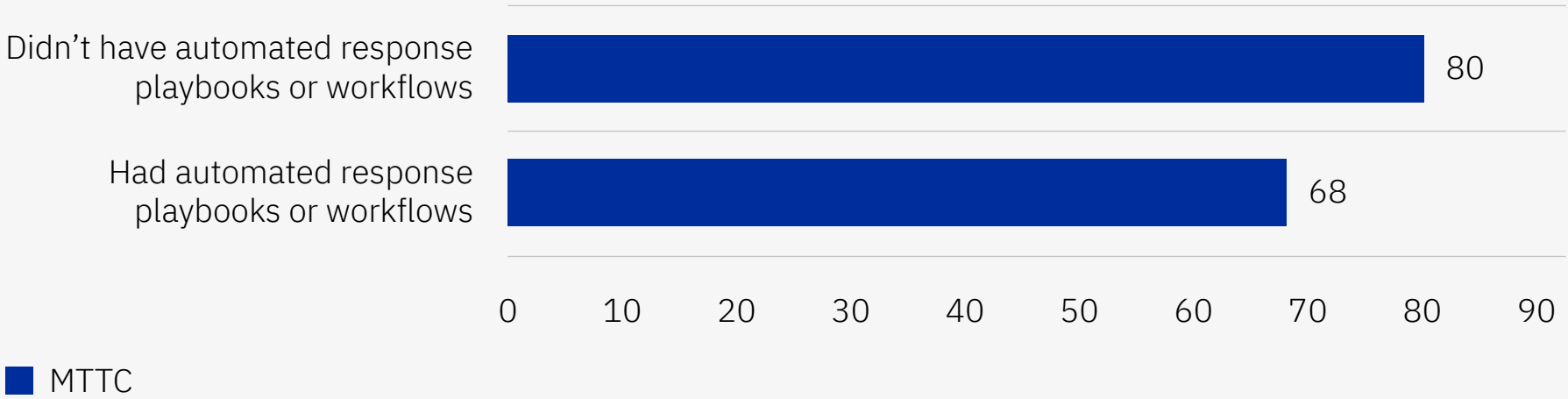


Abbildung 24. Angaben in Tagen

Kosten eines Ransomware-Angriffs basierend darauf, ob Lösegeld bezahlt wurde

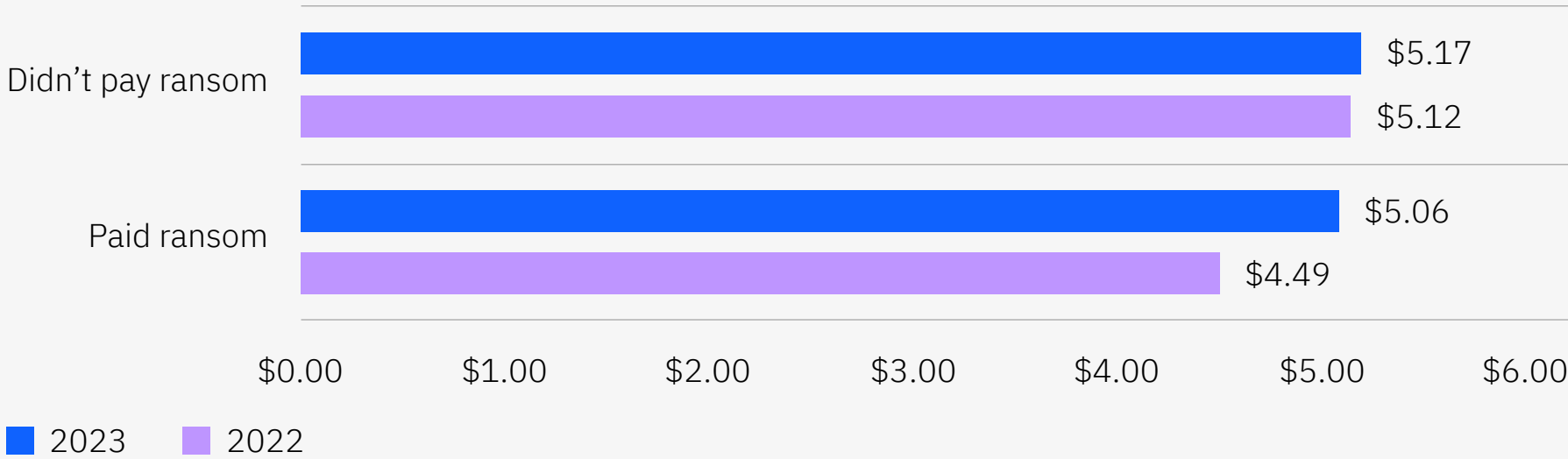


Abbildung 25. Gemessen in Mio. US-Dollar (Lösegeldkosten nicht inbegriffen)



## Angriffe auf die Lieferkette von Geschäftspartnern

Eine Kompromittierung der Lieferkette eines Geschäftspartners ist eine Datenverletzung, die auf einen Angriff auf einen Geschäftspartner zurückgeht. In der diesjährigen Studie gaben 15 % der Unternehmen an, dass eine Kompromittierung der Lieferkette die Ursache für eine Datenschutzverletzung war.

**Abbildungen 26 und 27. Die Kompromittierung der Lieferkette eines Geschäftspartners verursachte 11,8 % höhere Kosten und erforderte 12,8 % mehr Zeit für die Erkennung und Eindämmung als andere Arten von Sicherheitsverletzungen.**

Die Kosten einer Datenschutzverletzung, die auf die Kompromittierung der Lieferkette eines Geschäftspartners zurückzuführen ist, betrugen durchschnittlich 4,76 Mio. US-Dollar und waren damit 530.000 US-Dollar oder 11,8 % höher als die durchschnittlichen Kosten von 4,23 Mio. US-Dollar für Datenschutzverletzungen, die auf eine andere Ursache zurückzuführen waren.

Die Unternehmen benötigten durchschnittlich 233 Tage, um eine Kompromittierung der Lieferkette des Geschäftspartners zu erkennen, und 74 Tage, um sie zu beheben, was einer Gesamtdauer von 307 Tagen entspricht. Diese Durchschnittsdauer war 37 Tage oder 12,8 % länger als die durchschnittliche Dauer von 270 Tagen bei Datenschutzverletzungen, die auf eine andere Ursache zurückzuführen waren.

**Kosten einer Datenschutzverletzung aufgrund einer Kompromittierung der Lieferkette eines Geschäftspartners**



Abbildung 26. Angaben in°Mio.°US-Dollar

**Zeit zur Erkennung und Eindämmung einer Datenschutzverletzung, basierend auf der Kompromittierung der Lieferkette eines Geschäftspartners**

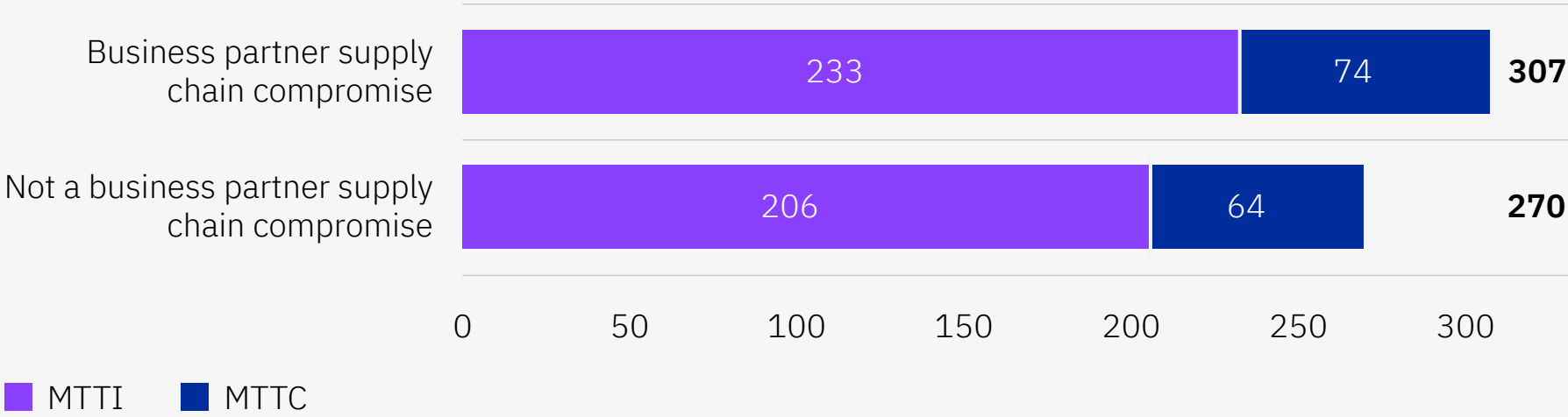
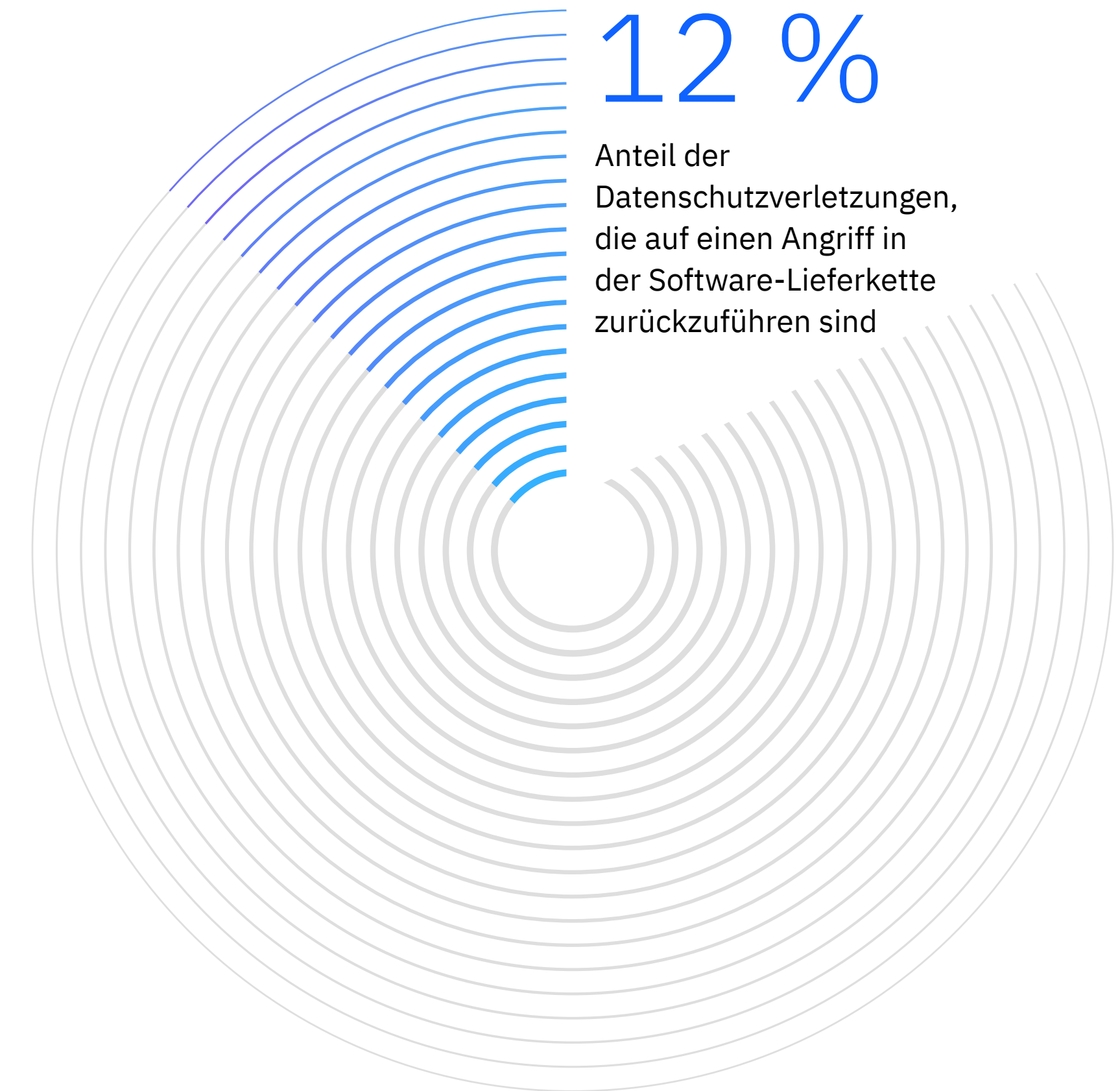


Abbildung 27. Angaben in Tagen

## Angriffe auf die Software-Lieferkette

Im Rahmen der Studie wurden in diesem Jahr erstmals auch Angriffe untersucht, die ihren Ursprung in der Software-Lieferkette haben. Dabei dringt ein Angreifer in das Netz eines Softwareanbieters ein und setzt schädlichen Programmcode ein, um die Software zu kompromittieren, bevor der Anbieter sie an seine Kunden weitergibt. Die kompromittierte Software greift dann die Daten oder das System des Kunden an. In der diesjährigen Studie gaben 12 % der Unternehmen an, dass ein Angriff auf die Software-Lieferkette die Ursache für eine Datenverletzung war.



**Abbildungen 28 und 29.**  
**Kompromittierungen der Software-Lieferkette kosteten 8,3 % mehr als andere Arten von Sicherheitsverletzungen, und zudem dauerte es 8,9 % länger, sie zu erkennen und einzudämmen.**  
Die Kosten einer Datenschutzverletzung, die auf die Kompromittierung der Software-Lieferkette zurückzuführen ist, betrugen durchschnittlich 4,63 Mio. US-Dollar und waren damit 370.000 US-Dollar oder 8,3 % höher als die durchschnittlichen Kosten von 4,26 Mio. US-Dollar für

Datenschutzverletzungen, die auf eine andere Ursache zurückzuführen waren. Eine Datenschutzverletzung aufgrund einer Kompromittierung der Software-Lieferkette dauerte 8,9 % länger (294 Tage im Vergleich zu 269) als Datenverletzungen aufgrund anderer Ursachen.  
  
Obwohl eine Kompromittierung innerhalb der Software-Lieferkette weniger kostspielig ist als eine, die von einem Geschäftspartner ausgeht, sind beide dennoch teurer und dauern länger als die durchschnittliche Datenschutzverletzung.

**Kosten einer Datenschutzverletzung basierend auf dem Auftreten einer Kompromittierung der Software-Lieferkette**

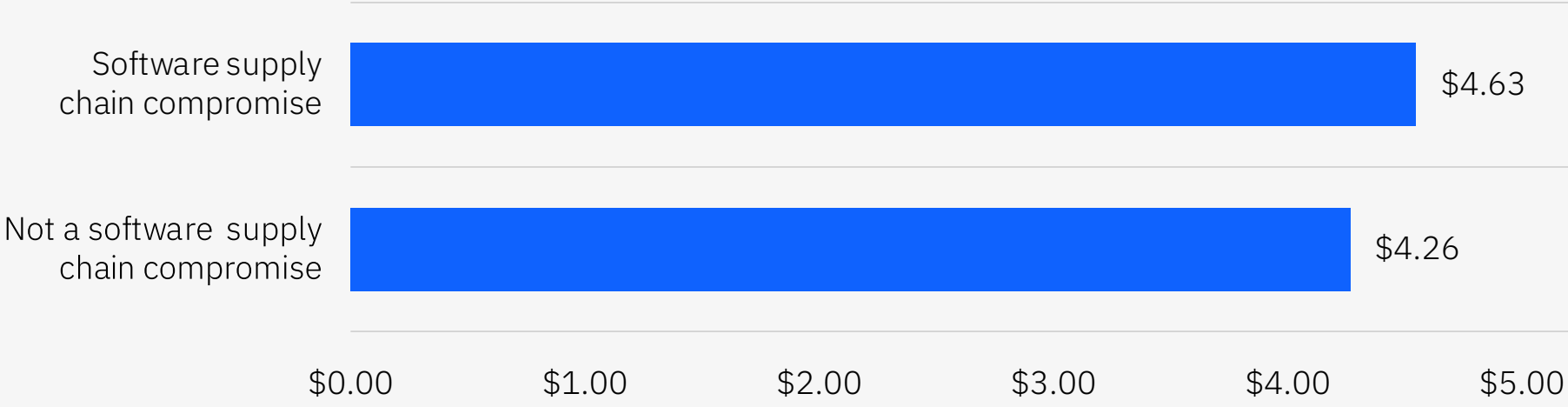


Abbildung 28. Angaben in°Mio.°US-Dollar

**Zeit zur Erkennung und Eindämmung einer Datenschutzverletzung basierend auf der Kompromittierung einer Software-Lieferkette**

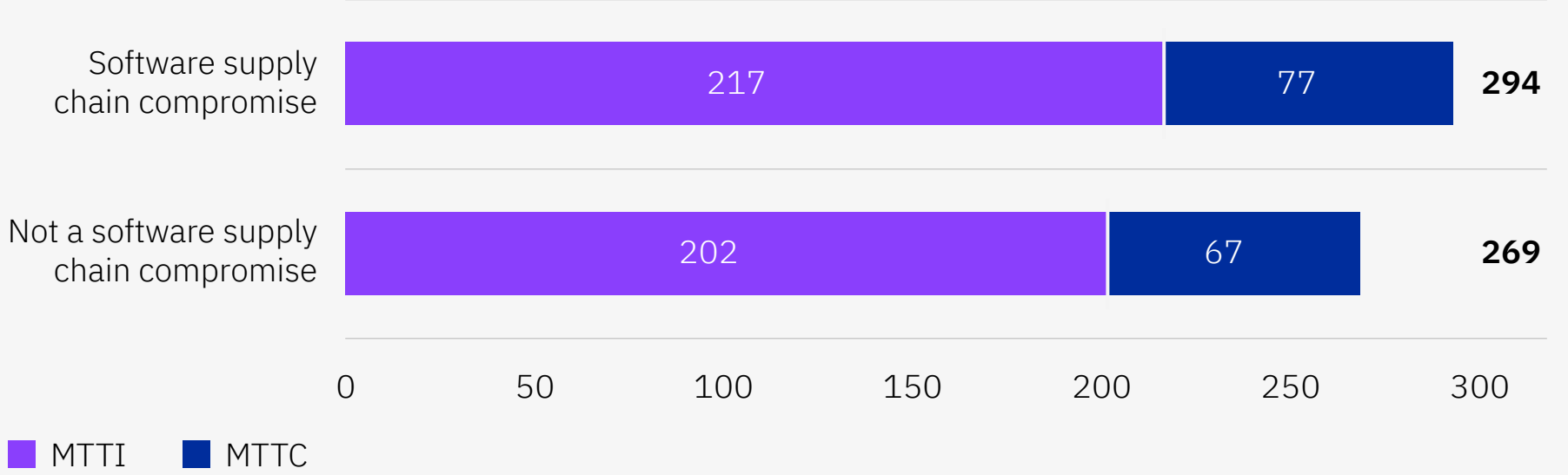


Abbildung 29. Angaben in Tagen



## Regulatorische Rahmenbedingungen

Die Studie untersuchte, wie der Grad der Datenregulierung die Kosten einer Datenschutzverletzung beeinflusst. In Umgebungen mit einem hohen Maß an Datenregulierung fielen 58 % der Kosten auch nach dem ersten Jahr weiter an. In Umgebungen mit geringer Regulierung war es wahrscheinlicher, dass 64 % der mit einem Verstoß verbundenen Kosten innerhalb des ersten Jahres behoben wurden.

Je nachdem, wie viel Zeit seit der Datenschutzverletzung verstrichen ist, ändern sich auch die entsprechenden Kosten. Mit jeder Phase der Sicherheitsverletzung können unterschiedliche Kosten verbunden sein, wenn diese erkannt und eingedämmt wird und wenn die kompromittierten Daten wiederhergestellt oder repariert werden.

# 250.000 US-Dollar

20 % der Unternehmen, die von einer Datenschutzverletzung betroffen waren, zahlten so viel oder mehr an Bußgeldern

**Abbildungen 30a und 30b.**  
**In Umgebungen mit starker Datenregulierung fielen die Spitzenkosten mehr als zwei Jahre nach Aufdeckung einer Datenschutzverletzung an.**  
Unternehmen in Umgebungen mit geringer Regulierung mussten fast zwei Drittel ihrer Kosten für Datenschutzverletzungen im ersten Jahr tragen, während die Kosten für Unternehmen in Umgebungen mit starker Regulierung weniger als die Hälfte betrugen. In Umgebungen mit geringer Regulierung erreichten die Kosten für Datenschutzverletzungen im Zeitraum von 6-9 Monaten einen Höchstwert von 21 % der Gesamtkosten. In stark regulierten Umgebungen erreichten die Kosten für Datenschutzverletzungen nach zwei Jahren mit 21 % der Gesamtkosten ihren Höhepunkt. Der Großteil der Kosten für Datenschutzverletzungen in einer gering regulierten Umgebung stieg anfangs stark an und nahm mit der Zeit ab. In einer Umgebung mit starker Regulierung schwankten die Kosten und stiegen zwei Jahre nach der Erkennung der Datenschutzverletzung weiter an.

Zeitliche Verteilung der Kosten für Datenschutzverletzungen in Umgebungen mit geringer Regulierung im Vergleich zu Umgebungen mit starker Regulierung im Bereich der Datenverarbeitung

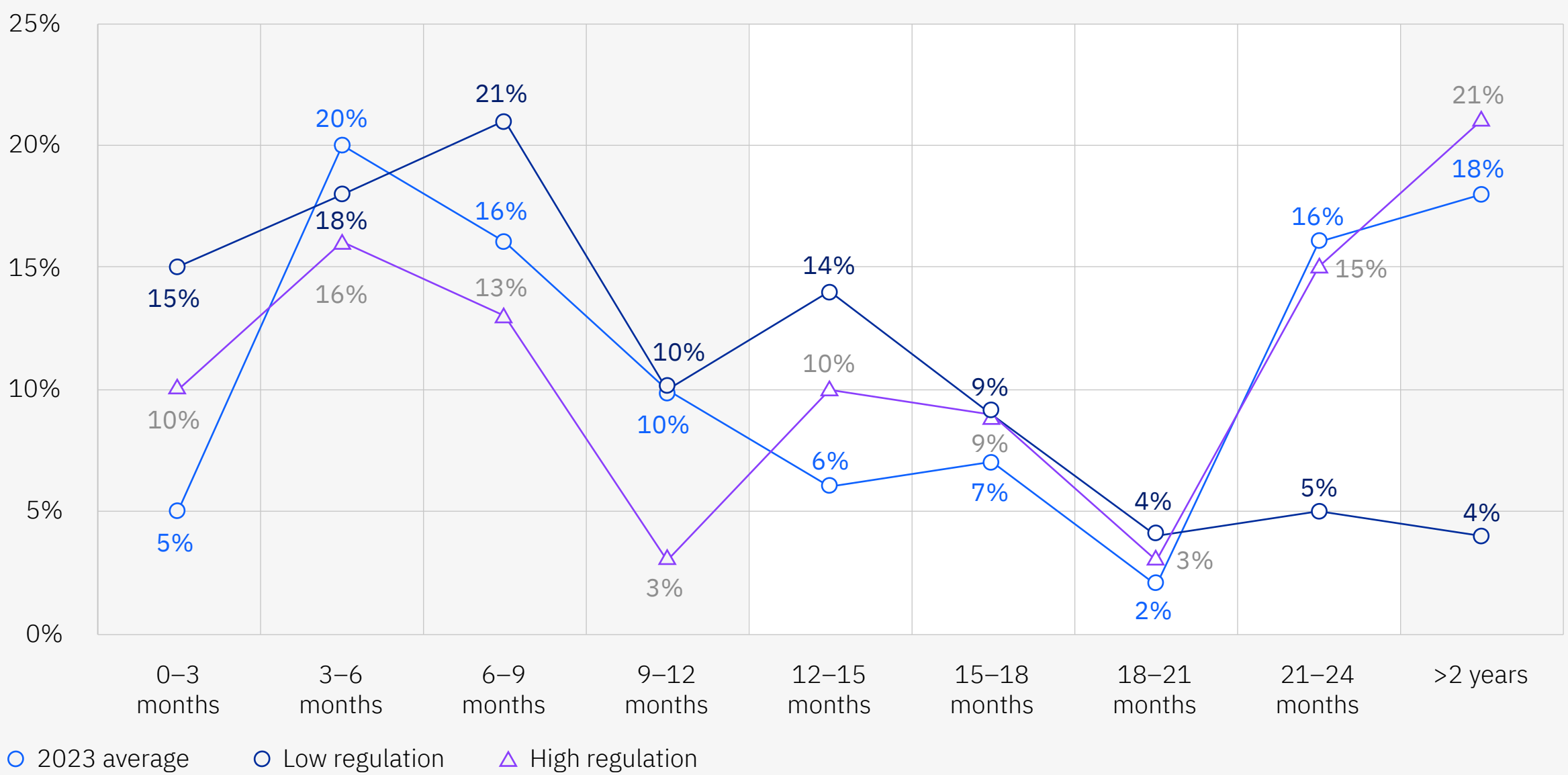


Abbildung 30a. Anteil an angefallenen Gesamtkosten in 3-Monatsintervallen

Verteilung der Kosten für Datenschutzverletzungen nach Jahr in Umgebungen mit geringer Regulierung im Vergleich zu Umgebungen mit starker Regulierung im Bereich der Datenverarbeitung

Verstrichene Zeit seit dem Verstoß	Anteil an den Gesamtkosten		
	Durchschnitt 2023	Geringe Regulierung	Starke Regulierung
Erstes Jahr	51 %	64 %	42 %
Zweites Jahr	31 %	32 %	37 %
Zwei und mehr Jahre	18 %	4 %	21 %

Abbildung 30b. Prozentsatz der Gesamtkosten über die Jahre

# Kosten einer Datenschutzverletzung in Branchen mit kritischer Infrastruktur im Vergleich zu anderen Branchen

Abbildung 31. Angaben in°Mio.°US-Dollar

**Abbildung 31. Die Kosten für Datenschutzverletzungen in Branchen mit kritischer Infrastruktur belaufen sich auf über 5 Mio. US-Dollar.**

Zu den Organisationen und Einrichtungen mit kritischer Infrastruktur zählen solche aus den Bereichen Finanzdienstleistungen, Industrie, Technologie, Energie, Transport, Kommunikation, Gesundheitswesen, Bildung und öffentliche Hand. Bei diesen Organisationen lagen die Kosten für Datenschutzverletzungen um 1,26 Mio. US-Dollar höher als die durchschnittlichen Kosten von 3,78 Mio. US-Dollar für Organisationen in anderen Branchen, was einer Differenz von 28,6 % entspricht. Dieser Wert von 5,04 Mio. US-Dollar spiegelt auch einen Anstieg von 4,6 % (4,82 Mio. US-Dollar) gegenüber den für 2022 gemeldeten durchschnittlichen Kosten einer Datenschutzverletzung für Branchen mit kritischer Infrastruktur wider.





**Abbildungen 32 und 33. Weniger als ein Drittel der Organisationen musste aufgrund von Datenschutzverletzungen Bußgelder zahlen, und 80 % der Bußgelder beliefen sich auf 250.000 US-Dollar oder weniger.** Von den untersuchten Unternehmen mussten 31 % aufgrund einer Datenschutzverletzung Bußgelder zahlen, und nur 20 % dieser Bußgelder überstiegen 250.000 US-Dollar. Eine Geldbuße von 250.000 US-Dollar entsprach 5,6 % der durchschnittlichen Gesamtkosten einer Datenschutzverletzung im Bericht von 2023.

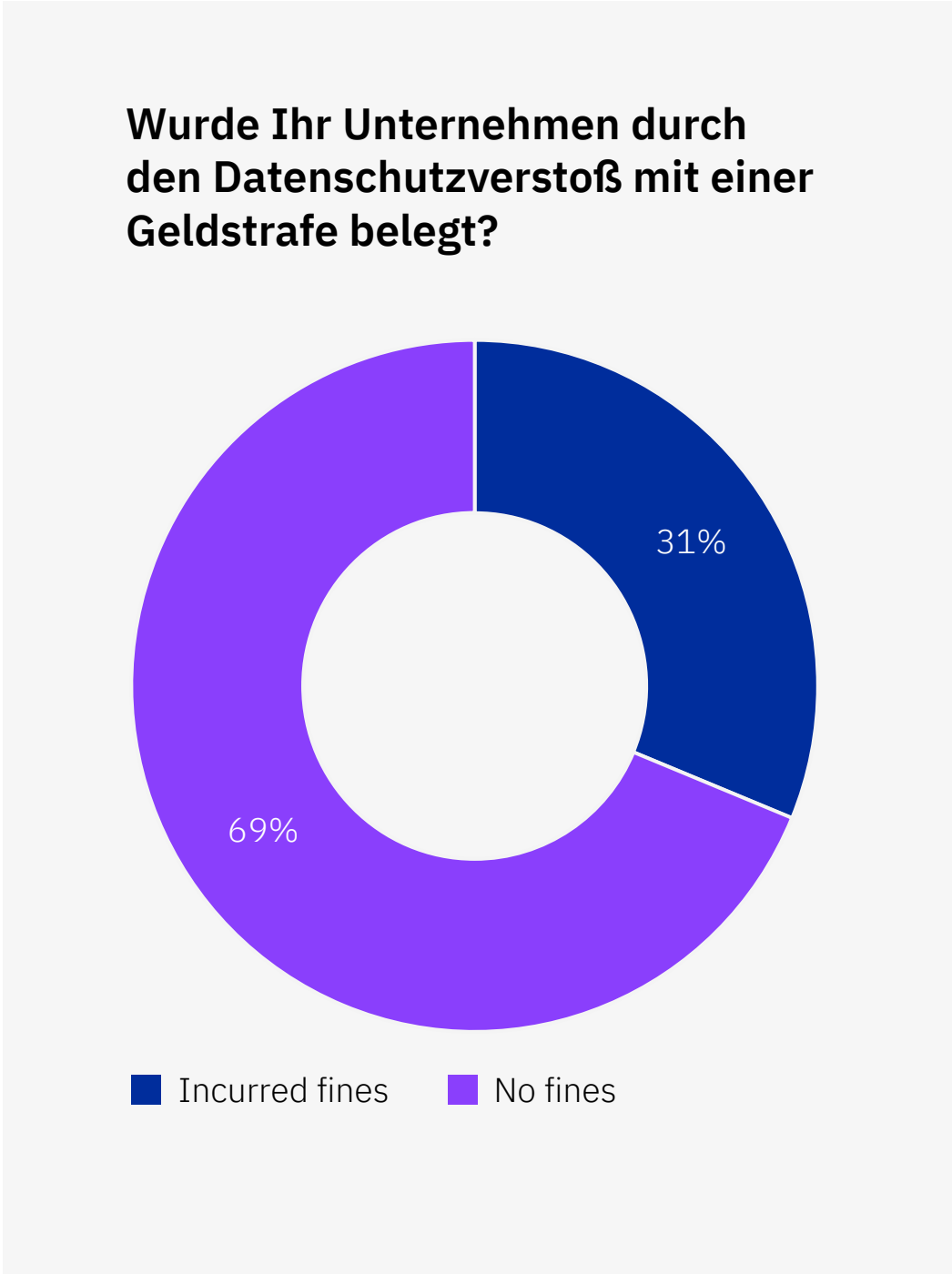


Abbildung 32. Anteil aller Unternehmen

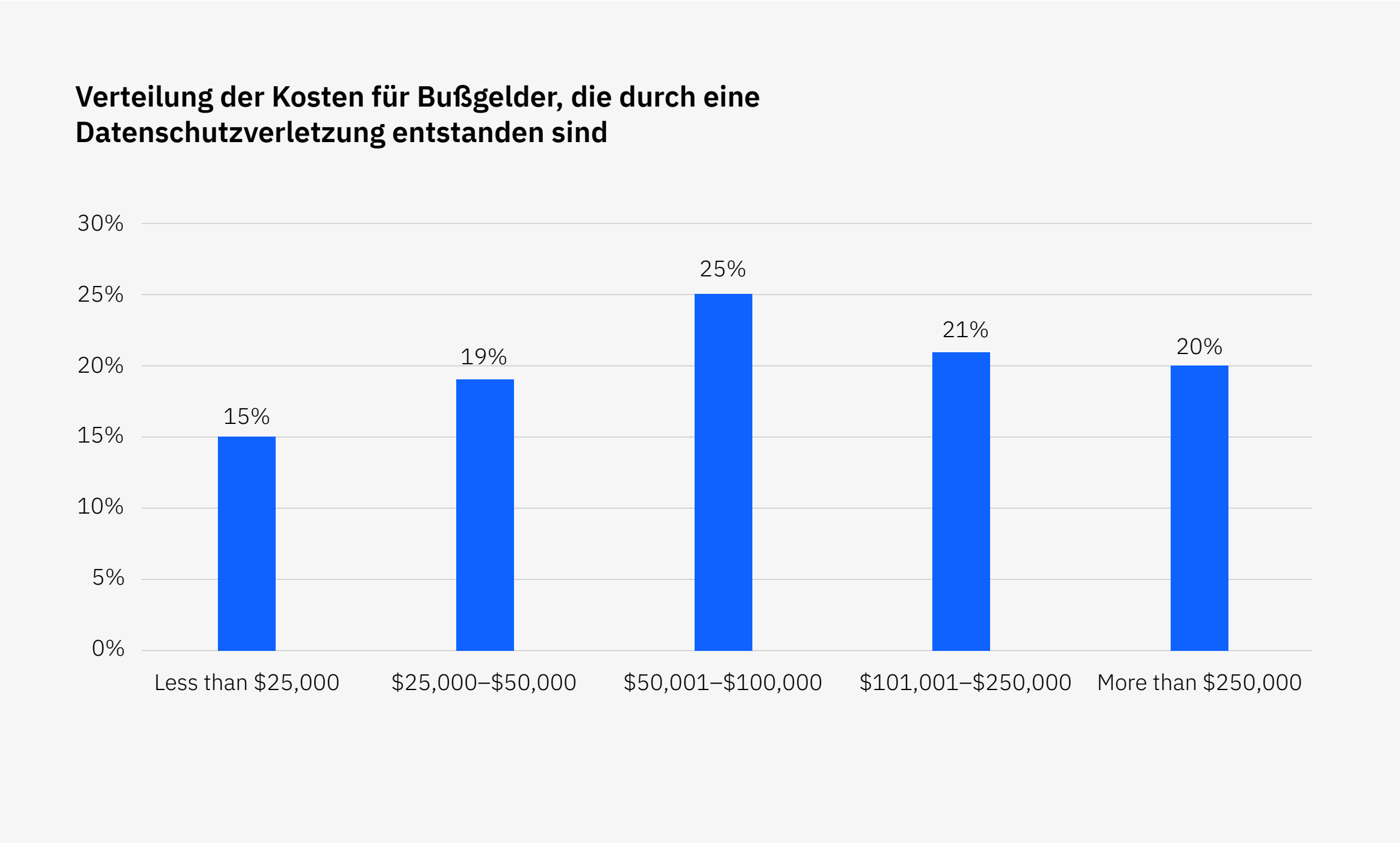
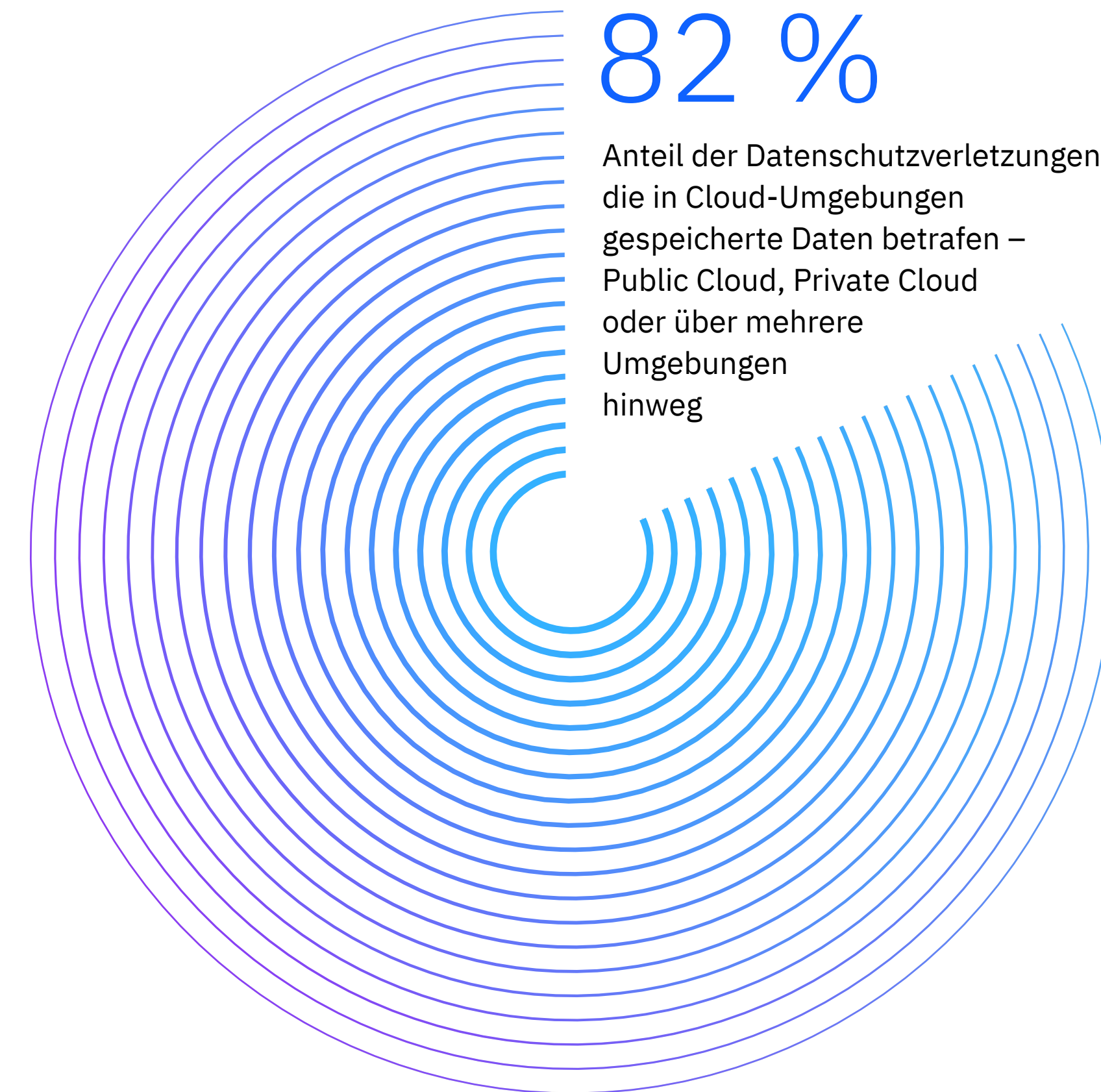


Abbildung 33. Von denjenigen, die Geldstrafen erhielten, gemessen in US-Dollar

## Cloud-Verstöße

Die Kosten und die Dauer einer Sicherheitsverletzung variierten je nachdem, wo die Daten gespeichert waren. Die meisten der untersuchten Vorfälle betrafen Daten, die sich über mehrere Umgebungen erstreckten – einschließlich Cloud und On-Premise – und solche Sicherheitsverletzungen trugen auch zu höheren Kosten und einem längeren Zeitraum für die Erkennung und Eindämmung einer Datenschutzverletzung bei.



**Abbildung 34. Verstöße betrafen am häufigsten Daten, die in mehreren Umgebungen gespeichert waren.**  
Der größte Prozentsatz der Sicherheitsverletzungen, nämlich 39 %, betraf Daten, die in verschiedenen Umgebungen gespeichert waren, gefolgt von 27 % der Sicherheitsverletzungen, die Daten in der öffentlichen Cloud betrafen. Die Anzahl der Sicherheitsverletzungen, die in mehreren Umgebungen auftraten, übertraf die kombinierten 34 % der Verstöße, die nur in privaten Cloud- oder On-Premises-Umgebungen stattfanden.

**Abbildung 35. Datenschutzverletzungen in Public Clouds und mehreren Umgebungen verursachten höhere Kosten.**  
Im Bericht 2023 erreichten die Kosten für Datenschutzverletzungen in mehreren Umgebungen 4,75 Mio. US-Dollar. Dies sind die höchsten Kosten der analysierten Umgebungen und 17,6 % höher als die Kosten von 3,98 Mio. US-Dollar für Datenschutzverletzungen in einer Private-Cloud-Umgebung, die die niedrigsten Kosten der analysierten Umgebungen darstellte. Die Kosten von Datenschutzverletzungen in mehreren Umgebungen überstiegen die durchschnittlichen Kosten einer Datenschutzverletzung von 4,45 Mio. US-Dollar um 6,5 %.

Wo wurden die kompromittierten Daten gespeichert?

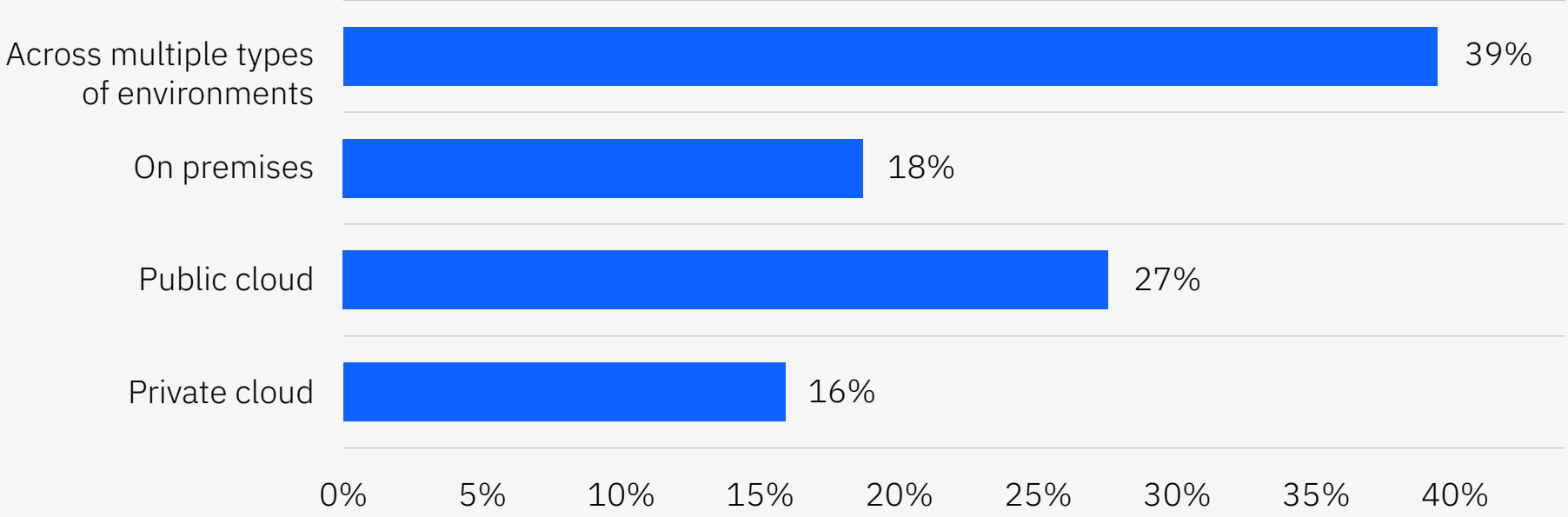


Abbildung 34. Anteil aller Verletzungen

Kosten einer Datenschutzverletzung nach Speicherort der verletzten Daten



Abbildung 35. Angaben in Mio. US-Dollar



**Abbildung 36. Die Nutzung von öffentlichen Clouds und mehreren Umgebungen trägt ebenfalls zu längeren Lebenszyklen von Datenverletzungen bei.**  
Die längste Zeit, um eine Sicherheitsverletzung zu identifizieren und einzudämmen, betraf Daten, die in mehreren Umgebungen gespeichert waren, und dauerte 291 Tage. Dieses Intervall übertraf die kürzeste Zeit zur Identifizierung und Eindämmung einer Sicherheitsverletzung – die in einer Private-Cloud-Umgebung 235 Tage betrug – um 56 Tage oder 21,3 %. Es ist auch erwähnenswert, dass die Verwendung mehrerer Umgebungen das einzige Modell ist, das die für 2023 gemeldete durchschnittliche Zeit zur Erkennung und Eindämmung einer Datenschutzverletzung von 277 Tagen um 14 Tage oder 4,9 % übertrifft.

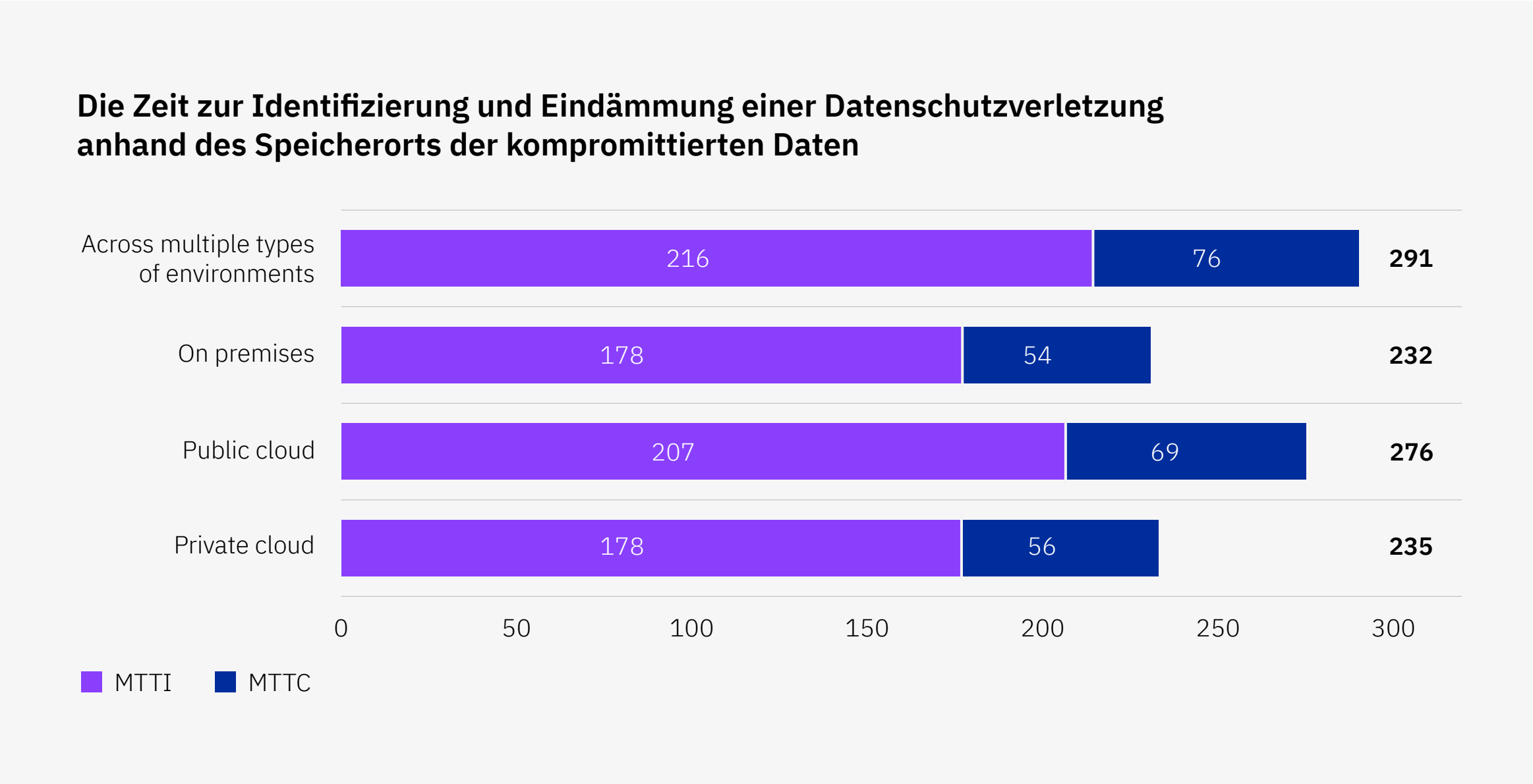
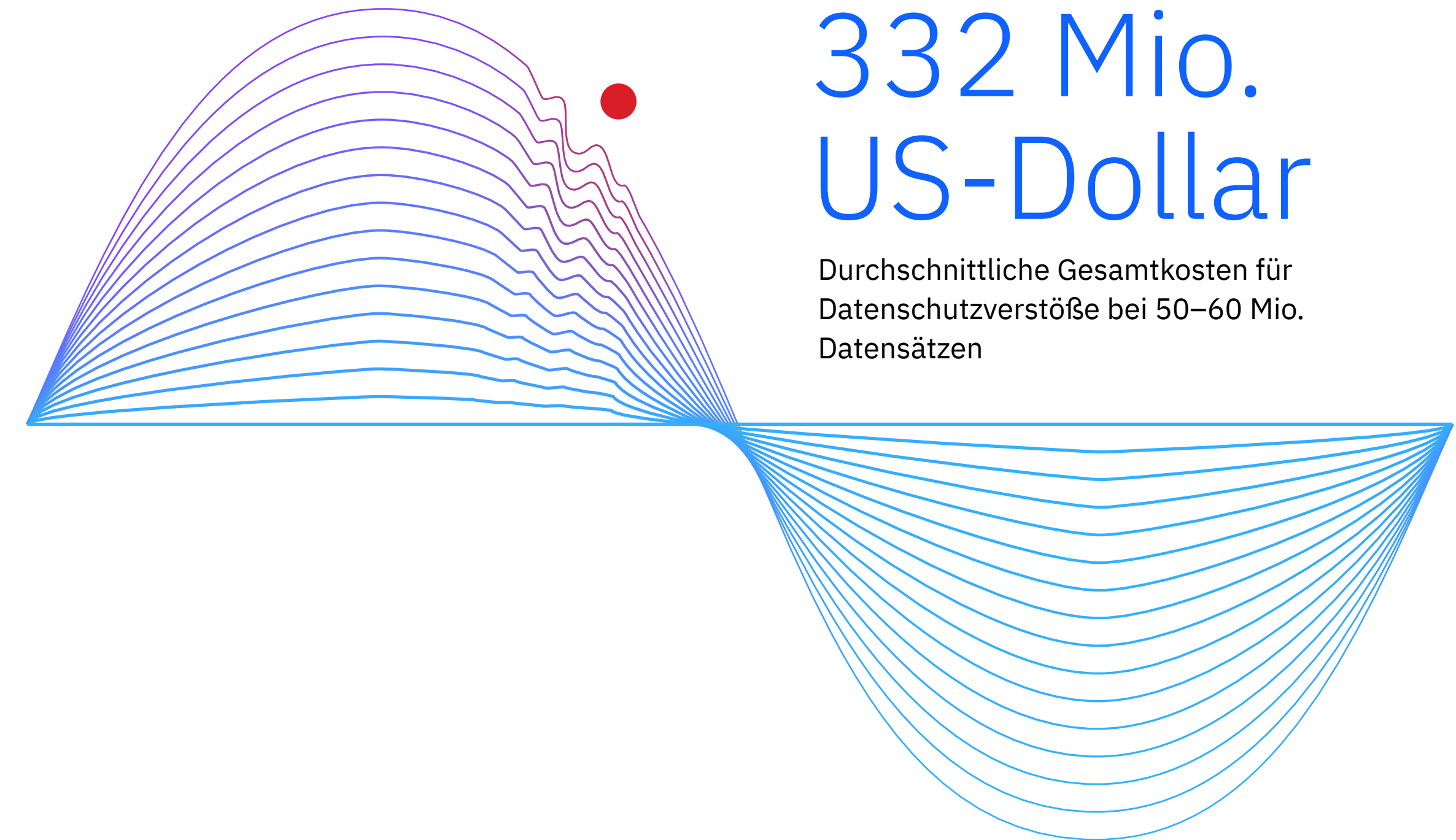


Abbildung 36. Angaben in Tagen

## Mega-Datenschutzverletzungen

Große Datenschutzverletzungen, bei denen mehr als eine Million Datensätze betroffen sind, sind relativ selten, aber sie haben aufgrund ihres enormen Ausmaßes eine starke Wirkung.

Die diesjährige Studie umfasste 20 Unternehmen, die durch Datenschutzverletzungen den Verlust oder Diebstahl von 1 Million bis 60 Millionen Datensätzen erlitten haben. In der Studie wurde eine besondere Methodik zur Untersuchung dieser Mega-Datenschutzverletzungen angewandt. Sie wurden gesondert von den anderen 553 Verstößen der Studie betrachtet, die jeweils nicht mehr als 101.200 verlorene oder kompromittierte Datensätze umfassten. Eine vollständige Erläuterung der Forschungsmethodik finden Sie in den [Fragen zu Datenschutzverletzungen](#) am Ende dieses Berichts.



**Abbildung 37. Die Kosten von Mega-Datenschutzverletzungen sind im Bericht 2023 gesunken.**

Die durchschnittlichen Kosten eines Mega-Verstoßes sind in den unterschiedlichen Größenordnungen unterschiedlich stark gesunken. Der höchste prozentuale Rückgang fand in der Kohorte zwischen 1 Million bis 10 Millionen statt, mit einem Rückgang von 26,5 % von 49 Mio. US-Dollar im Bericht für das Jahr 2022 und auf 36 Mio. US-Dollar im Bericht für das Jahr 2023. Der geringste prozentuale Rückgang fand in der Kohorte zwischen 30 und 40 Millionen statt, mit einem Rückgang um 3,8 % von 316 Mio. US-Dollar im Bericht für das Jahr 2022 und auf 304 Mio. US-Dollar im Bericht für das Jahr 2023. In der Kohorte zwischen 50 und 60 Millionen sanken die für 2022 gemeldeten Kosten von 387 Mio. US-Dollar um 55 Mio. US-Dollar oder 14,2 % auf 332 Mio. US-Dollar im Bericht für 2023.

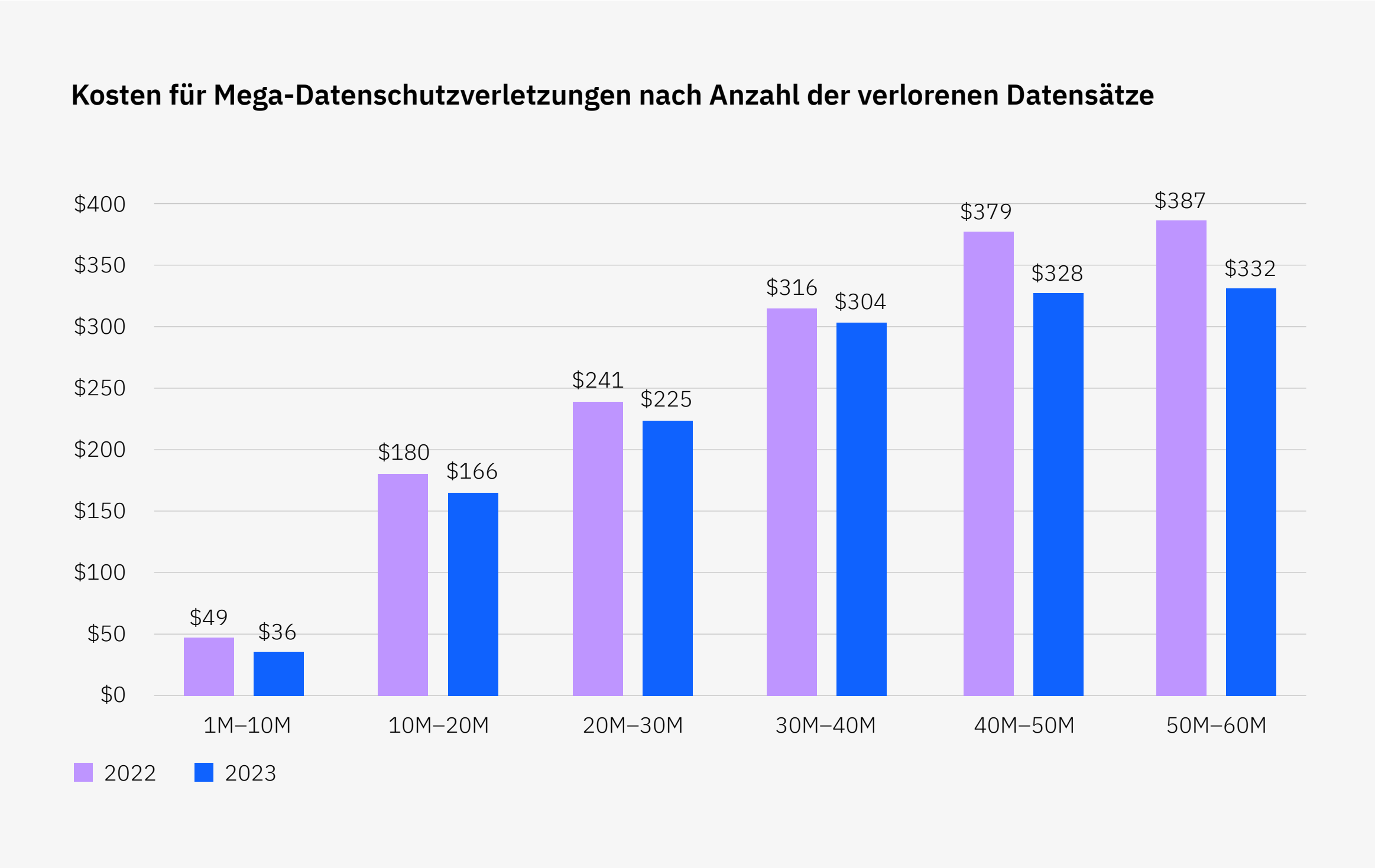
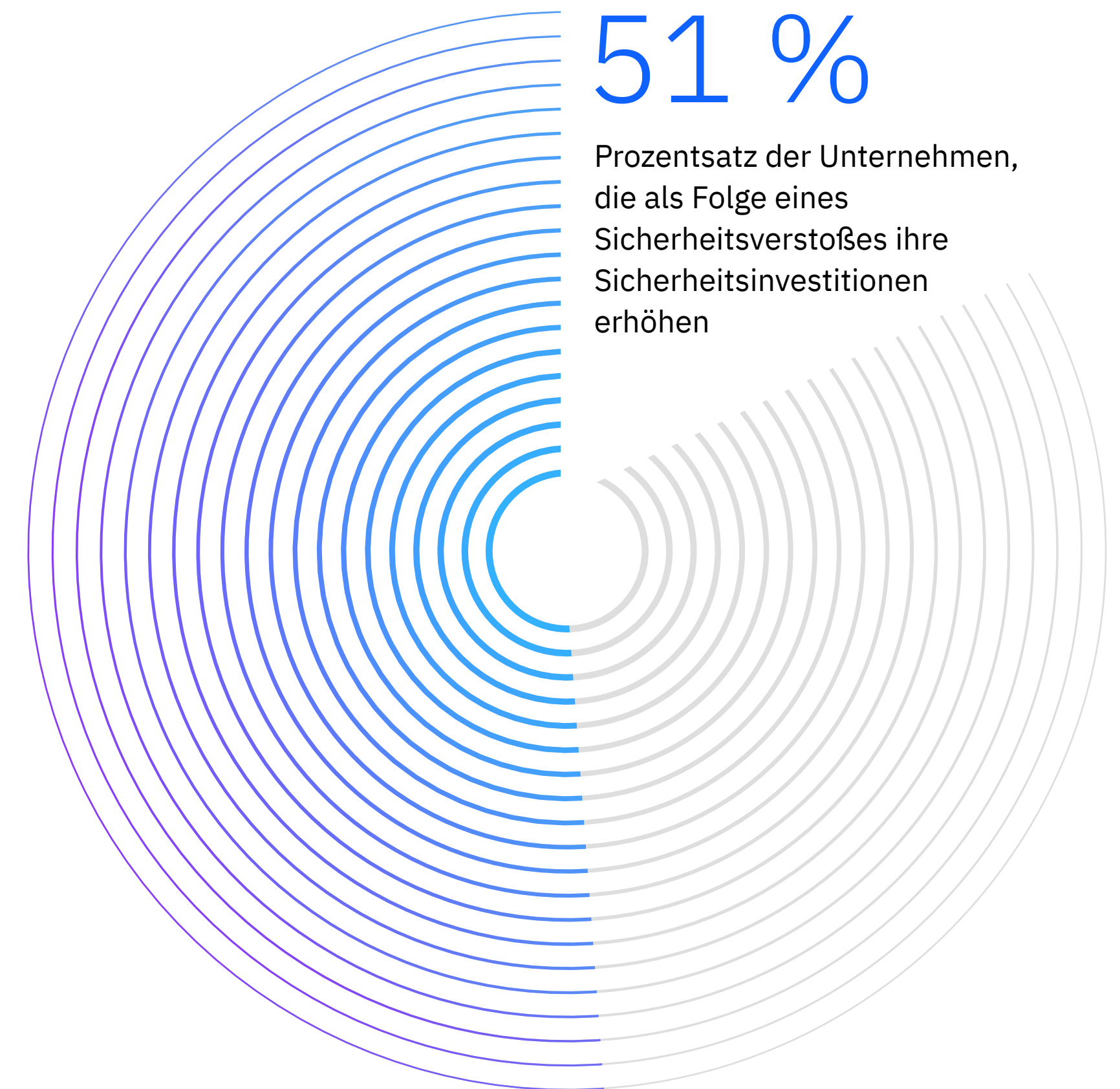


Abbildung 37. Angaben in°Mio.°US-Dollars



## Sicherheitsinvestitionen

In diesem Abschnitt werden die Strategien für Sicherheitsinvestitionen untersucht, die Unternehmen nach einer Datenschutzverletzung gewählt haben. Wir untersuchen, wie oft Unternehmen ihre Ausgaben nach einem Sicherheitsverstoß erhöht haben und wie sie die Mittel eingesetzt haben.



**Abbildung 38. Die Befragten waren geteilter Meinung, was die Erhöhung der Sicherheitsinvestitionen nach einer Sicherheitsverletzung angeht.** Selbst als die Globalkosten einer Datenschutzverletzung stiegen, berichteten die Studienteilnehmer über geteilte Ansichten zur Erhöhung der Sicherheitsinvestitionen nach einem Sicherheitsvorfall. 51 % der Befragten gaben an, dass sie nach dem Verstoß zusätzliche Sicherheitsausgaben planen.

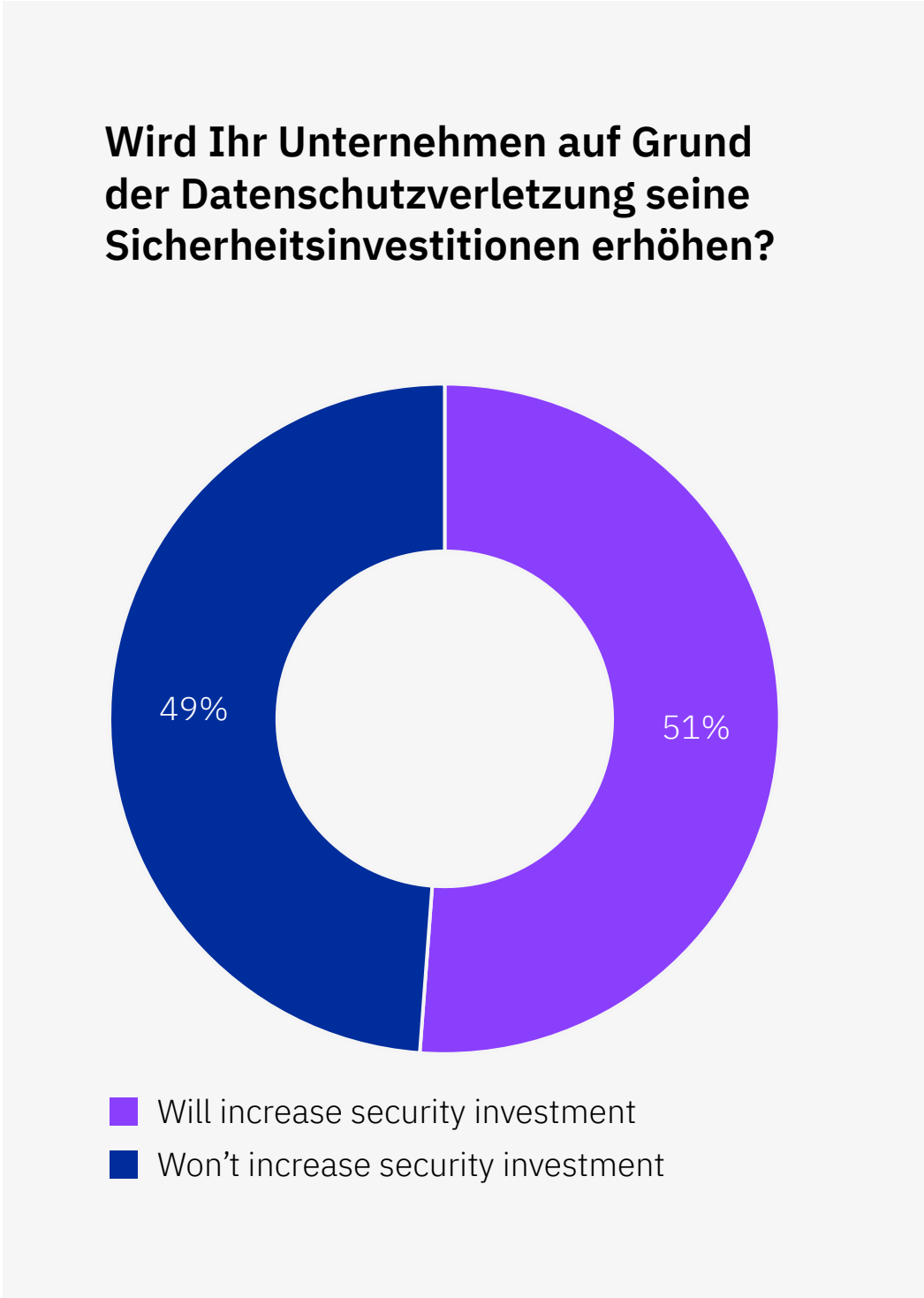


Abbildung 38. Anteil aller Unternehmen



**Abbildung 39. Nach dem Verstoß wurde erheblich in die IR-Planung und -Tests sowie die Schulung der Mitarbeiter investiert.**

Von den 51 % der Befragten, die ihre Ausgaben nach einer Sicherheitsverletzung erhöht haben, investierten 50 % in die Planung und Durchführung von IR-Tests, dicht gefolgt von Schulungen für Mitarbeiter mit 46 %. Technologien zur Erkennung von und Reaktion auf Bedrohungen rangieren mit 38% an dritter Stelle und sind damit die meistgenannten Technologien oder Tools, die in diesem Abschnitt berücksichtigt werden. Bemerkenswert ist, dass diese drei Investitionen eng mit den wichtigsten Faktoren in Verbindung mit geringeren Kosten für Datenschutzverletzungen zusammenhängen, die in diesem Jahr im Abschnitt über die wichtigsten Kostenfaktoren untersucht werden. Nur 18 % der Befragten investierten nach einer Sicherheitsverletzung in Versicherungsschutz, die am wenigsten verbreitete Maßnahme.

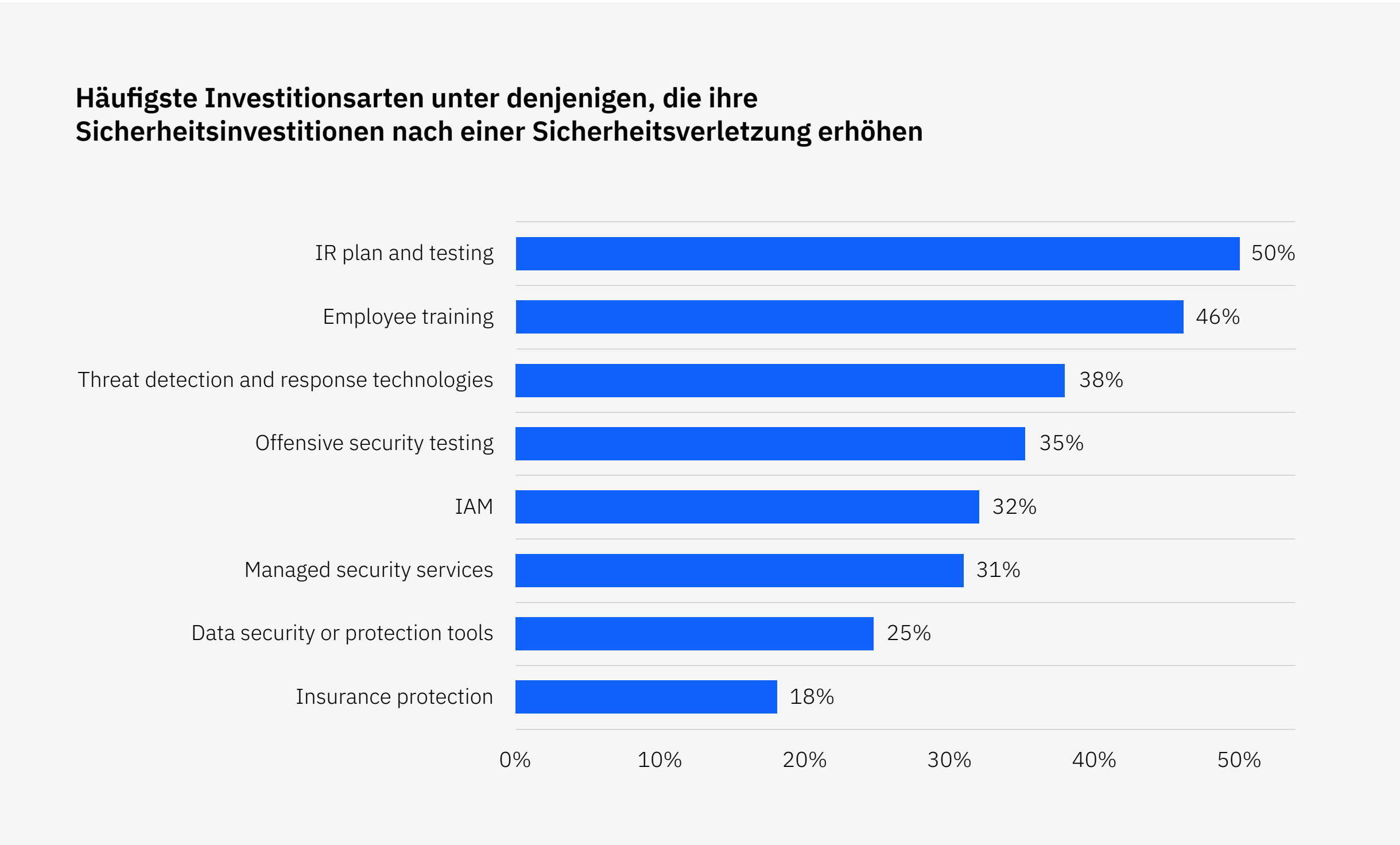


Abbildung 39. Anteil der Unternehmen, die ihre Investitionen erhöhen; mehr als eine Antwort zulässig



## KI und Automatisierung für die IT-Sicherheit

Angesichts der fortschreitenden Anwendungsfälle für Sicherheits-KI und Automatisierung in der Sicherheitsbranche untersucht dieser Bericht die Auswirkungen dieser Technologien auf die Kosten und den Zeitplan von Datenschutzverletzungen. Beispiele hierfür sind der Einsatz von KI, maschinellem Lernen, Automatisierung und Orchestrierung, um manuelle Eingriffe bei der Erkennung und Untersuchung von Bedrohungen sowie bei der Reaktion und Eindämmung zu ergänzen oder zu ersetzen. Am anderen Ende des Spektrums stehen Prozesse, die über manuelle Eingaben gesteuert werden, oft über Dutzende von Tools und komplexe, nicht integrierte Systeme, ohne dass Daten zwischen ihnen ausgetauscht werden.

Obwohl wir bereits zum sechsten Mal die Auswirkungen von KI und Automatisierung auf die Cybersicherheit untersuchen, führen wir in diesem Jahr neue

Kriterien ein, die die Durchdringung der Sicherheitsprozesse eines Unternehmens mit KI berücksichtigen, anstatt wie in den Vorjahren den Grad der Bereitstellung – von nicht bereitgestellt bis teilweise oder vollständig bereitgestellt.

- „Umfangreicher Gebrauch“ bezieht sich auf die Integration von Sicherheits-KI und Automatisierung im gesamten Betrieb, einschließlich mehrerer verschiedener Tools und Funktionen.
- „Eingeschränkter Gebrauch“ bezieht sich auf die Anwendung von KI auf nur einen oder zwei Anwendungsfälle innerhalb der Sicherheitsoperationen.
- „Nicht in Gebrauch“ bezieht sich auf Sicherheitsprozesse, die ausschließlich durch manuelle Eingaben gesteuert werden.

# 108 Tage

Unternehmen, die KI und Automatisierung im Sicherheitsbereich umfassend einsetzen, erkannten und verhinderten eine Datenschutzverletzung 108 Tage schneller als Unternehmen, die dies nicht taten.

**Abbildung 40. Eine Mehrheit von 61 % der Unternehmen setzt ein gewisses Maß an Sicherheit, KI und Automatisierung ein.** Nur 28 % der Unternehmen setzten KI und Automatisierungstools für die Sicherheit in ihren Cybersecurity-Prozessen umfassend ein, während 33 % sie nur in begrenztem Umfang nutzten. Das bedeutet, dass sich fast 4 von 10 Unternehmen bei ihren Sicherheitsmaßnahmen ausschließlich auf manuelle Eingaben verlassen.

**Abbildung 41. Der umfassende Einsatz von Sicherheits-KI und Automatisierung führte zu Kosteneinsparungen von fast 1,8 Mio. US-Dollar.** Unternehmen, die KI und Automatisierung im Sicherheitsbereich ausgiebig nutzen, erzielten im Vergleich die höchsten Kosteneinsparungen. Die durchschnittlichen Kosten einer Datenschutzverletzung lagen bei 3,60 Mio.

US-Dollar, was 1,76 Mio. US-Dollar weniger und einen Unterschied von 39,3 % im Vergleich zu Unternehmen ohne Nutzung von KI und Automatisierung bedeutet. Selbst Unternehmen, die KI und Automatisierung im Sicherheitsbereich nur in begrenztem Umfang einsetzen, verzeichneten durchschnittliche Kosten für eine Datenschutzverletzung in Höhe von 4,04 Mio. US-Dollar, also 1,32 Mio. US-Dollar oder 28,1 % weniger als Unternehmen, die keine KI oder Automatisierung einsetzen. Bei Unternehmen, die keine KI und Automatisierung im Sicherheitsbereich einsetzen, beliefen sich die durchschnittlichen Kosten einer Datenschutzverletzung auf 5,36 Mio. US-Dollar. Das sind 18,6 % mehr als die durchschnittlichen Kosten einer Datenschutzverletzung im Jahr 2023 in Höhe von 4,45 Mio. US-Dollar.

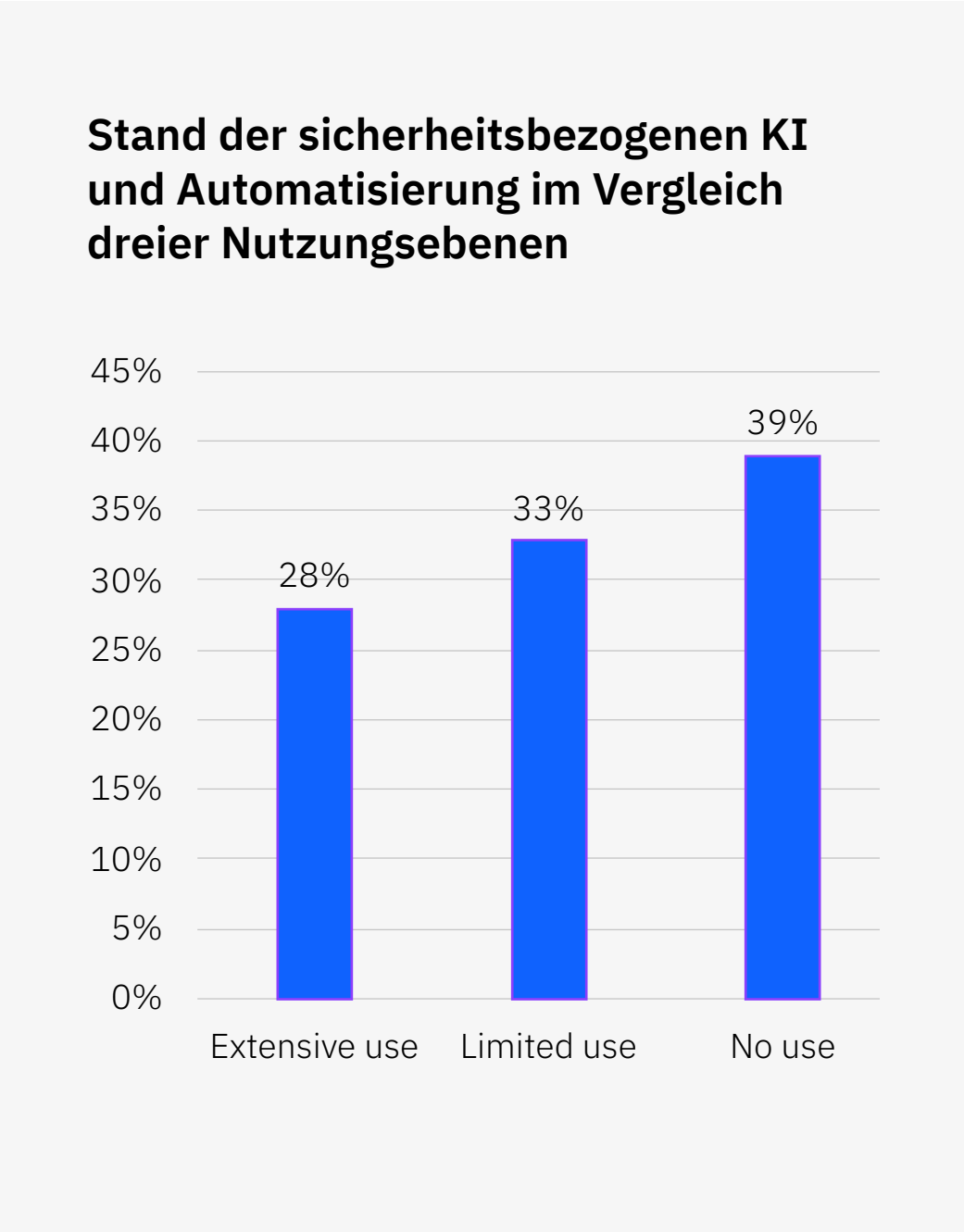


Abbildung 40. Prozentsatz der Unternehmen pro Nutzungsstufe

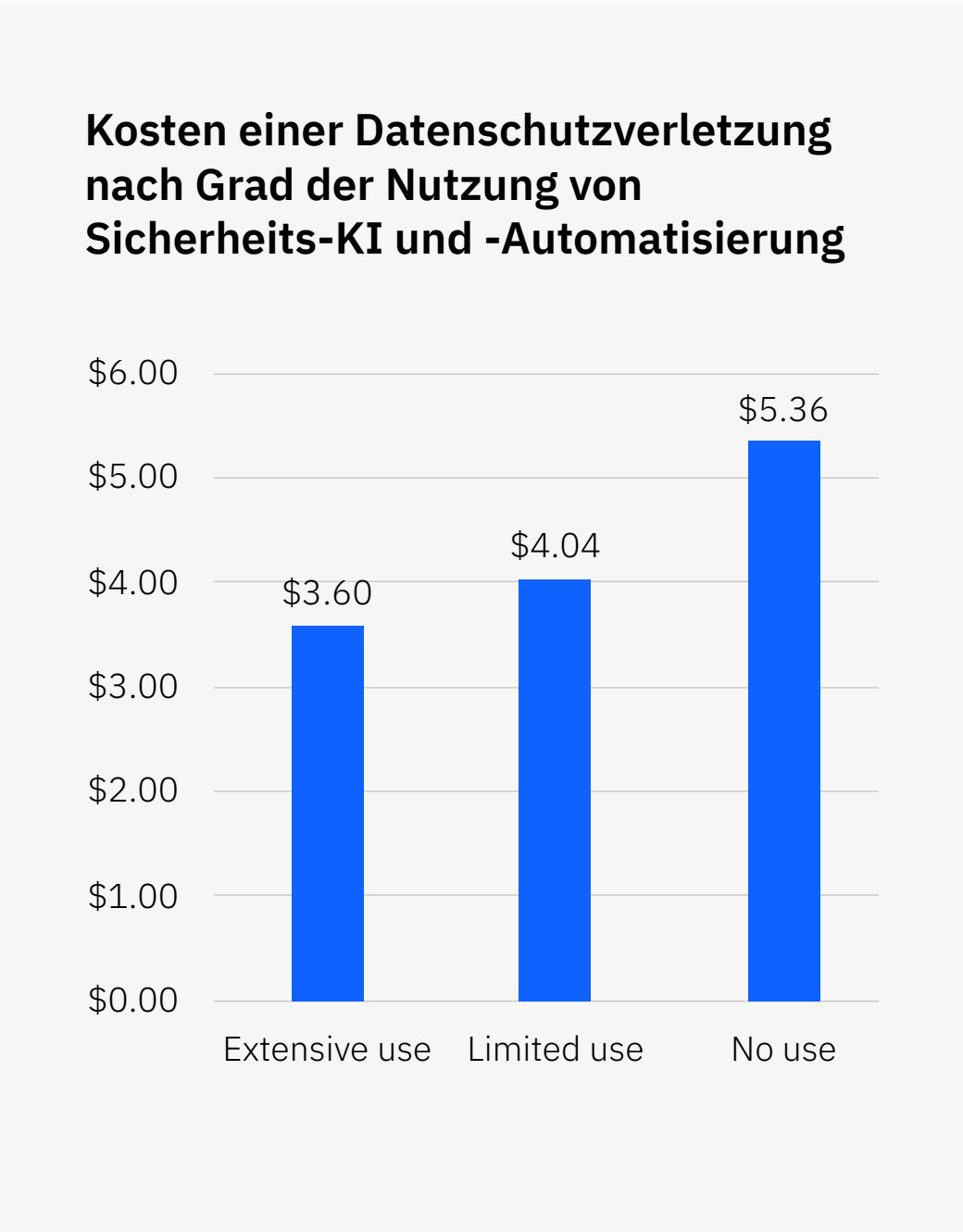


Abbildung 41. Angaben in°Mio.°USD

**Abbildung 42. Umfassende Sicherheits-KI und Automatisierung verkürzten die Zeit zur Erkennung und Eindämmung einer Sicherheitsverletzung um mehr als 100 Tage.**

Befragte aus Unternehmen, die KI und Automatisierung im Sicherheitsbereich umfassend einsetzen, waren in der Lage, eine Sicherheitsverletzung innerhalb von 214 Tagen zu erkennen und einzudämmen, d. h. 108 Tage schneller als Unternehmen, die keine KI einsetzen. Dies bedeutet, dass die Erkennung und Eindämmung einer Sicherheitsverletzung bei umfassender Nutzung von KI und Automatisierung nur 66 % der Zeit in Anspruch nahm,

die Unternehmen ohne den Einsatz dieser Technologien benötigten. Auch eine eingeschränkte Nutzung von KI hatte einen signifikanten Einfluss: Die durchschnittliche Zeit für die Erkennung und Eindämmung einer Sicherheitsverletzung betrug 234 Tage und war damit 88 Tage kürzer als bei Unternehmen, die keine KI und Automatisierung einsetzten. Es ist deutlich, dass selbst begrenzte Anstrengungen zur Integration von KI und Automatisierung in Sicherheitsabläufe die Zeit für die Identifizierung und Eindämmung von Sicherheitsverletzungen erheblich verkürzen und die Kosten deutlich senken können.

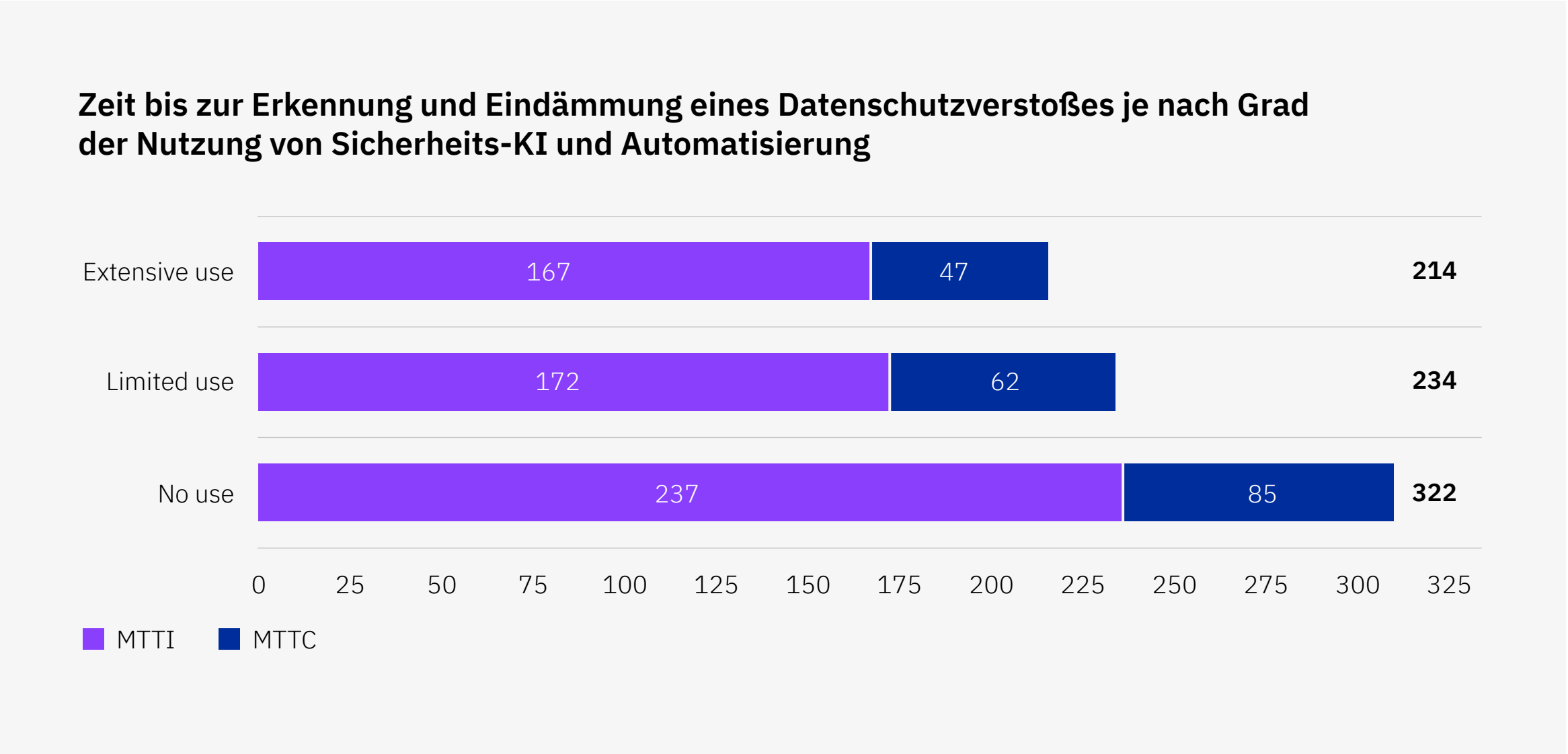


Abbildung 42. Angaben in Tagen

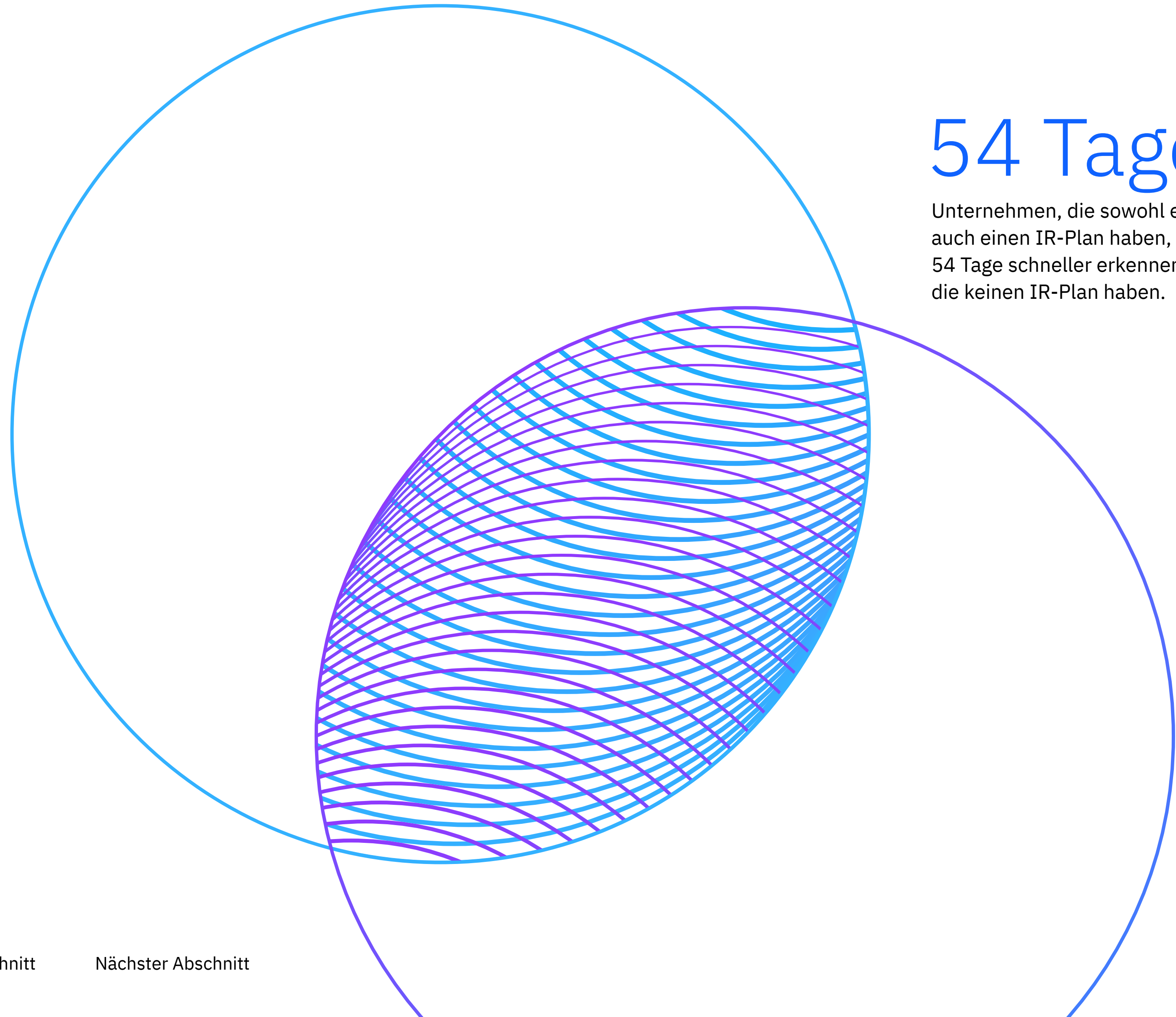


## Reaktion auf Vorfälle

IR-Strategien und -Taktiken haben dazu beigetragen, die Auswirkungen von Datenschutzverletzungen zu verringern. Die wirksamste IR-Strategie zur Verkürzung der Dauer einer Datenschutzverletzung war die Kombination der Bildung eines IR-Teams mit dem Testen des IR-Plans. Einige Unternehmen verfolgten jedoch nur eine der beiden Strategien. Als eigenständige Maßnahme war das Testen des IR-Plans wirksamer als die Bildung eines IR-Teams, um die Gesamtzeit bis zur Erkennung und Eindämmung des Verstoßes zu verkürzen.

# 54 Tage

Unternehmen, die sowohl ein IR-Team als auch einen IR-Plan haben, konnten Verstöße 54 Tage schneller erkennen als Unternehmen, die keinen IR-Plan haben.



**Abbildung 43. Mit der kombinierten IR-Strategie konnten 54 Tage für die Erkennung und Eindämmung einer Sicherheitsverletzung eingespart werden.**

Eine duale Strategie, bei der ein Reaktionsteam gebildet und ein Reaktionsplan getestet wird, führte zu einer kürzeren Zeit (252 Tage) für die Erkennung und Eindämmung einer Datenschutzverletzung im Vergleich zu 306 Tagen, wenn keiner der beiden Ansätze verfolgt wird. Dies entspricht einem Unterschied von 54 Tagen oder 19,4 %. Das Testen eines Reaktionsplans ohne Teambildung war mit einem Unterschied von 48 Tagen oder 17 % fast genauso effektiv.

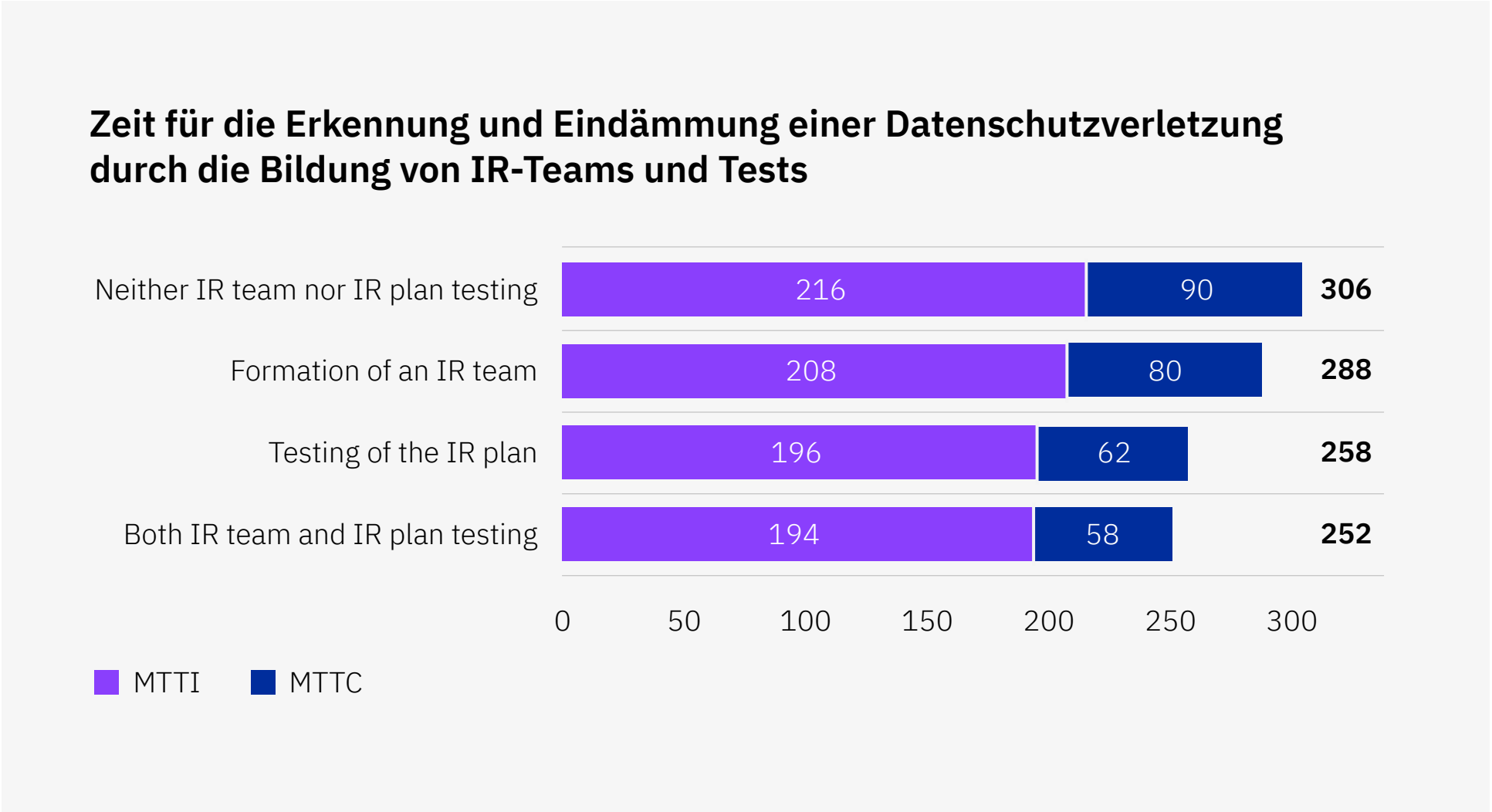


Abbildung 43. Angaben in Tagen

## Bedrohungsinformationen

Im diesjährigen Bericht wurde die Auswirkung von Bedrohungsdaten-Services auf die durchschnittliche Zeit bis zur Erkennung einer Sicherheitsverletzung erneut untersucht. Bedrohungsdaten-Services liefern Sicherheitsverantwortlichen Informationen und Erkenntnisse über Cyberbedrohungen und Schwachstellen, damit sie die Sicherheitslage in ihrem Unternehmen verbessern können.

# 28 Tage

Unternehmen, die Bedrohungsdaten verwenden, sind 28 Tage schneller bei der Erkennung von Sicherheitsverletzungen.

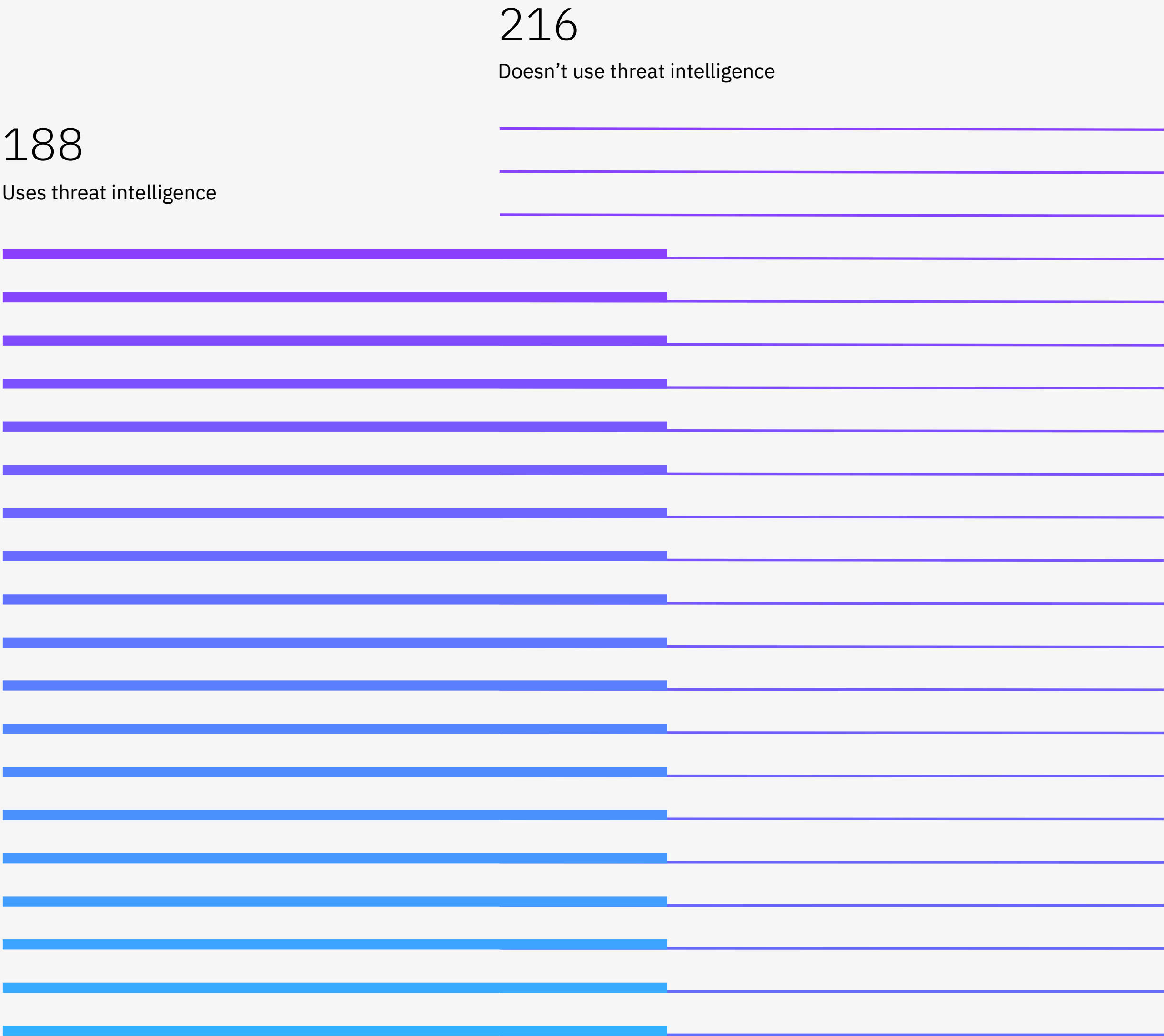


**Abbildung 44. Bedrohungsdaten verkürzen die Zeit zur Identifizierung von Verstößen.**

Die diesjährige Studie ergab, dass Nutzer von Bedrohungsdaten 13,9 % weniger Zeit für die Aufdeckung von Sicherheitsverletzungen benötigten als Unternehmen, die nicht in Bedrohungsdaten investierten – eine Differenz von 28 Tagen. Verglichen mit der diesjährigen globalen MTTI von 204 Tagen konnten Unternehmen, die Bedrohungsdaten-Services nutzten, Verstöße um 8,2 % bzw. um 16 Tage schneller erkennen. Befragte, die keine Bedrohungsdaten nutzten, brauchten 5,7 % bzw. 12 Tage länger als der weltweite Durchschnitt, um Verstöße zu erkennen.

Zeit für die Erkennung einer Datenschutzverletzung mithilfe von Bedrohungsdaten

Abbildung 44. MTTI, Angaben in Tagen



## Sicherheitslücken- und Risikomanagement

Erstmals wurde in diesem Jahr untersucht, wie Unternehmen Risiken und Sicherheitslücken priorisieren und wie sich dies auf die Kosten einer Datenschutzverletzung auswirkt. Unternehmen mit einem proaktiveren und risikobasierten Sicherheitsmanagement – z. B. mit Schwachstellen- und Penetrationstests oder Red Teaming – verzeichneten unterdurchschnittliche Kosten für Datenschutzverletzungen im Vergleich zu Unternehmen, die sich ausschließlich auf das branchenübliche CVE-Glossar (Common Vulnerabilities and Exposures) und das CVSS (Common Vulnerability Scoring System) stützten. Beim proaktiven Risikomanagement nimmt das IT-Sicherheitsteam des Unternehmens in der Regel die Perspektive eines potenziellen Angreifers ein, um zu ermitteln, welche Schwachstellen ausnutzbar sind und den größten Schaden anrichten können.

# 3,98 Mio. USD

Kosten einer Datenschutzverletzung für Unternehmen,  
die eine solide risikobasierte Analyse durchgeführt haben

**Abbildungen 45 und 46. Unternehmen, die Aktivitäten über die CVE-Bewertung hinaus priorisieren, erleben weniger kostspielige Sicherheitsverletzungen.** Mehr als ein Drittel der Unternehmen oder 36 % verließ sich bei der Priorisierung von Sicherheitslücken ausschließlich auf das CVE-Scoring, während die Mehrheit der Unternehmen oder 64 % eine umfassendere risikobasierte Analyse verwendete. Die Studie für 2023 zeigt einen signifikanten Unterschied in den Kosten von Datenschutzverletzungen zwischen diesen beiden Gruppen. Unternehmen, die eine intensivere, risikobasierte Analyse einsetzten, hatten im Durchschnitt Kosten in Höhe von 3,98 Mio. US-Dollar, was einem Unterschied von 18,3 % entspricht, verglichen mit 4,78 Mio. US-Dollar für Unternehmen, die sich nur auf CVE-Scores verließen.

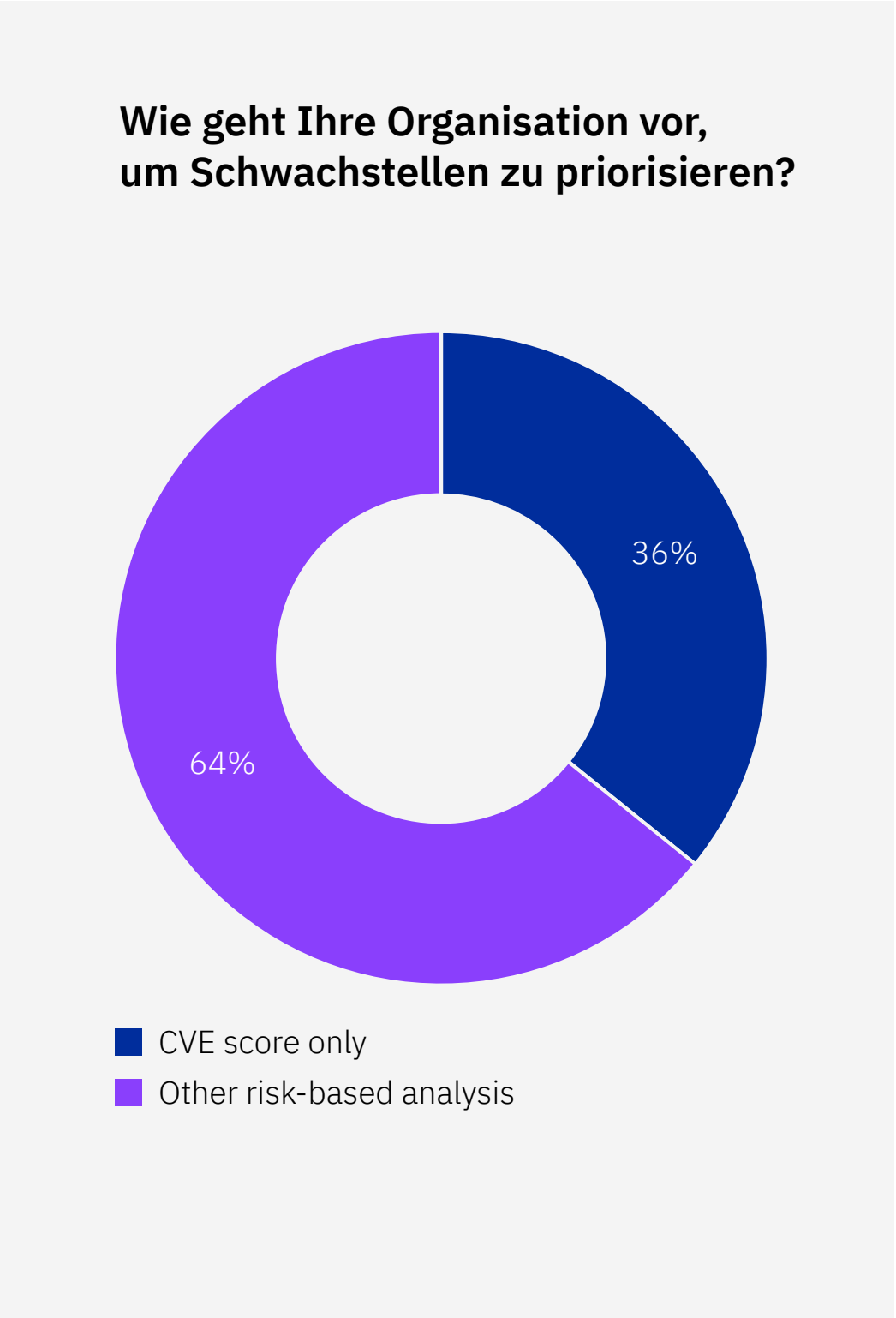


Abbildung 45. Anteil aller Unternehmen

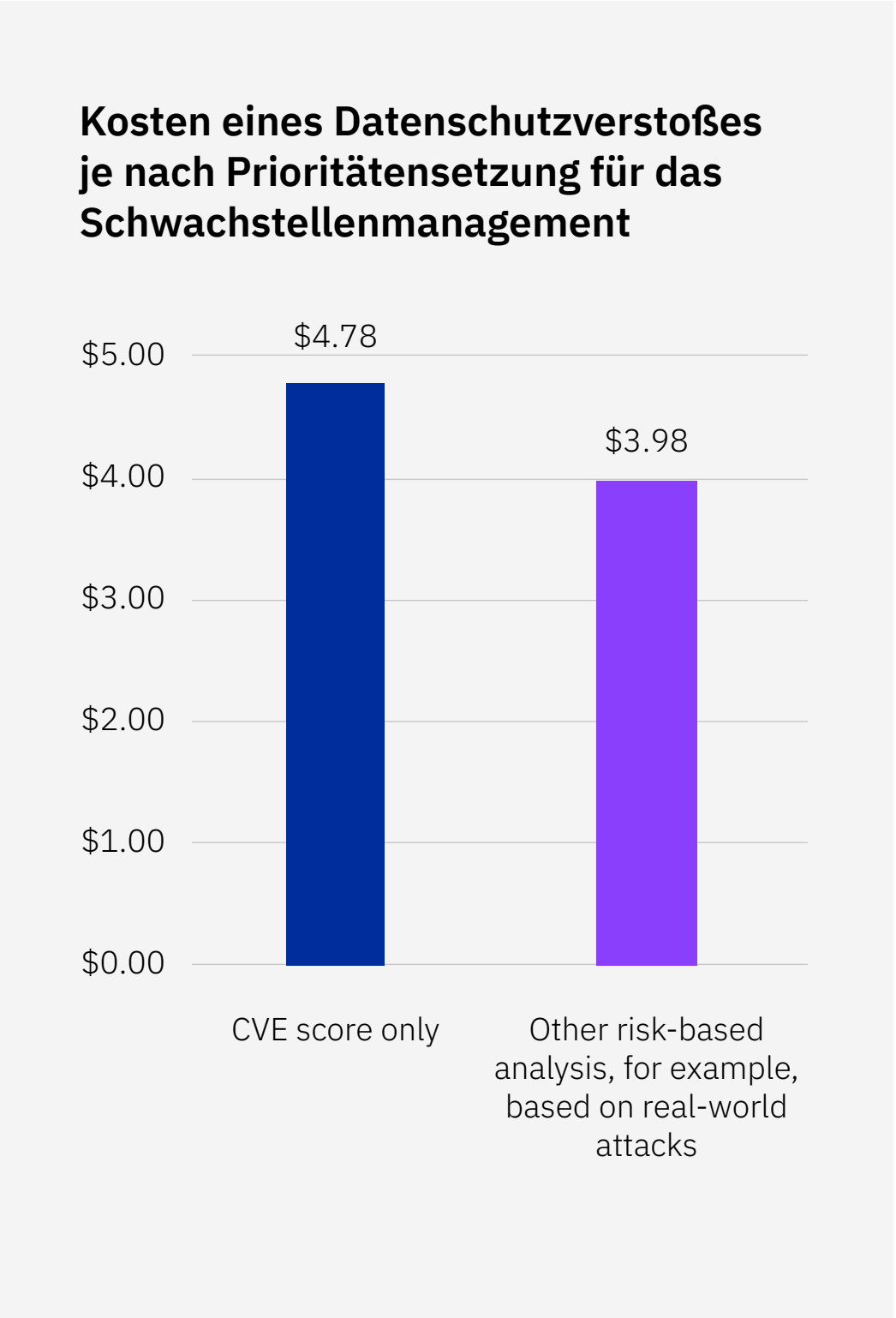


Abbildung 46. Angaben in°Mio.°USD



## Angriffsflächenmanagement

ASM bezeichnet eine Reihe von Prozessen, die bei der Erkennung, Analyse, Behebung und Überwachung potenzieller Angriffsflächen oder Schwachstellen eines Unternehmens helfen. Unternehmen mit ASM waren in der Lage, Datenschutzverletzungen in 75 % der Zeit zu erkennen und einzudämmen, die Unternehmen ohne ASM benötigten.

**Abbildung 47. ASM hat dazu beigetragen, die Gesamtzeit für die Erkennung und Eindämmung einer Datenschutzverletzung um fast 12 Wochen zu verkürzen.** Ohne eine ASM-Lösung dauerte es 260 Tage, bis eine Datenschutzverletzung erkannt wurde, und weitere 77 Tage, bis sie eingedämmt war – insgesamt also 337 Tage oder rund 11 Monate. Unternehmen mit einer ASM-Lösung konnten Verstöße in 193 Tagen erkennen und in 61 Tagen eindämmen. Die Gesamtdauer von 254 Tagen für die Erkennung und Eindämmung einer Sicherheitsverletzung entspricht einer Verkürzung um 83 Tage oder rund 12 Wochen. Die Datenschutzverletzungen wurden also in 75 % der Zeit erkannt und eingedämmt, die für Datenschutzverletzungen in Unternehmen ohne ASM-Lösungen benötigt wurde.

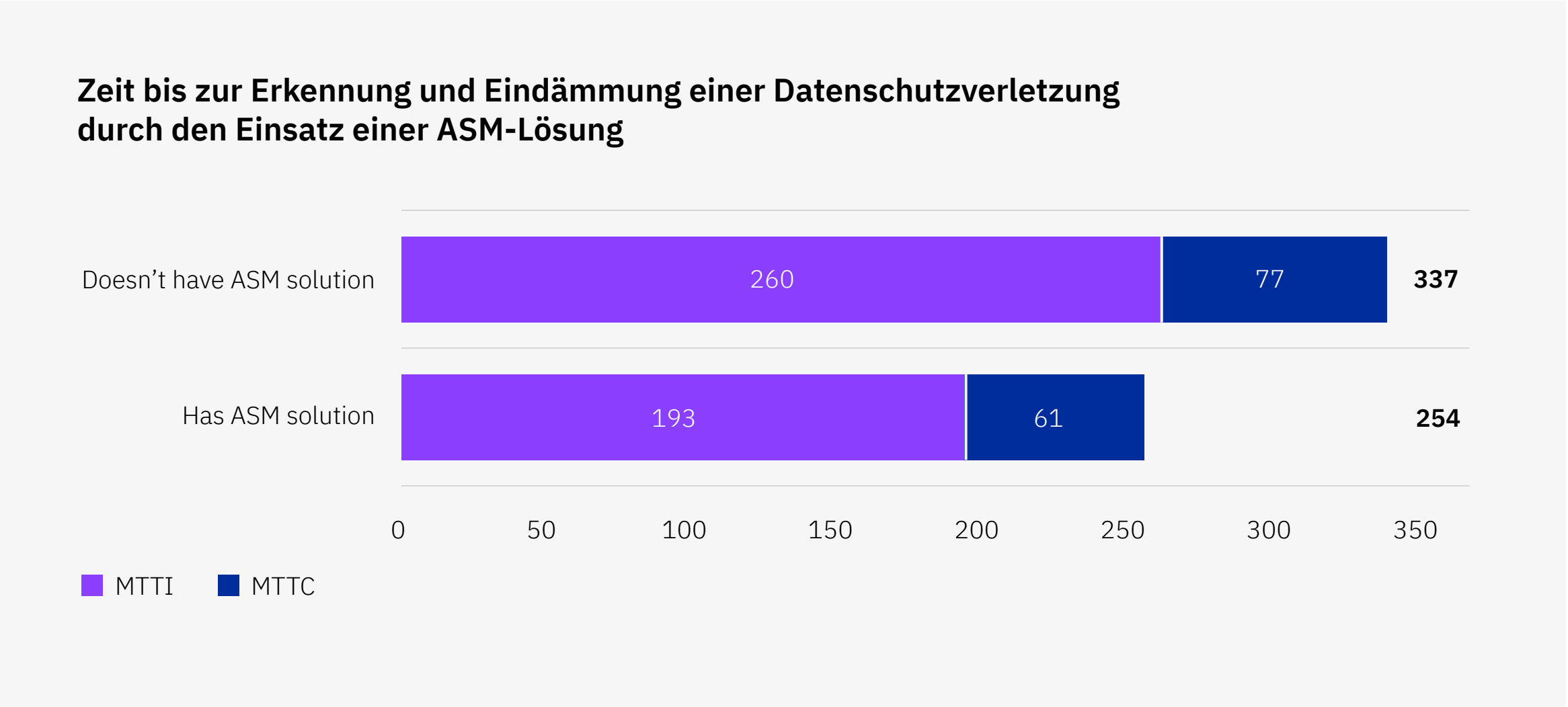


Abbildung 47. Angaben in Tagen

# Anbieter von verwalteten Sicherheitsdiensten

Zum ersten Mal haben wir untersucht, wie sich die Zusammenarbeit mit einem MSSP auf die Zeit auswirkt, die für die Erkennung und Eindämmung einer Sicherheitsverletzung benötigt wird. MSSPs bieten Unternehmen die Möglichkeit, die Sicherheitsüberwachung und -verwaltung auszulagern. Dabei werden häufig hochverfügbare Sicherheitszentren eingesetzt, die rund um die Uhr ihre Services anbieten. MSSPs können Unternehmen dabei helfen, ihre Sicherheitslage zu verbessern, ohne die Zahl der Mitarbeiter zu erhöhen oder in die Ausbildung interner Ressourcen investieren zu müssen.

**Abbildung 48. Unternehmen mit MSSPs verzeichneten einen um 21 % kürzeren Lebenszyklus von Sicherheitsverletzungen.**  
Im Bericht von 2023 konnten Unternehmen mit MSSP, Sicherheitsverletzungen in 80 % der Zeit erkennen und eindämmen, die Unternehmen ohne MSSP benötigten. Unternehmen mit MSSP konnten Sicherheitsverletzungen um 16 Tage bzw. 8,2 % schneller erkennen als der 2023 ermittelte weltweite Durchschnitt von 204 Tagen. Diejenigen ohne MSSP benötigten 28 Tage bzw. 12,8 % länger. Die Eindämmungszeiten ohne MSSP waren 5 Tage bzw. 6,6 % länger als der globale Durchschnitt von 73 Tagen im Jahr 2023. Mit MSSP-Unterstützung wurde die Eindämmungszeit um 10 Tage oder 14,7 % verkürzt.

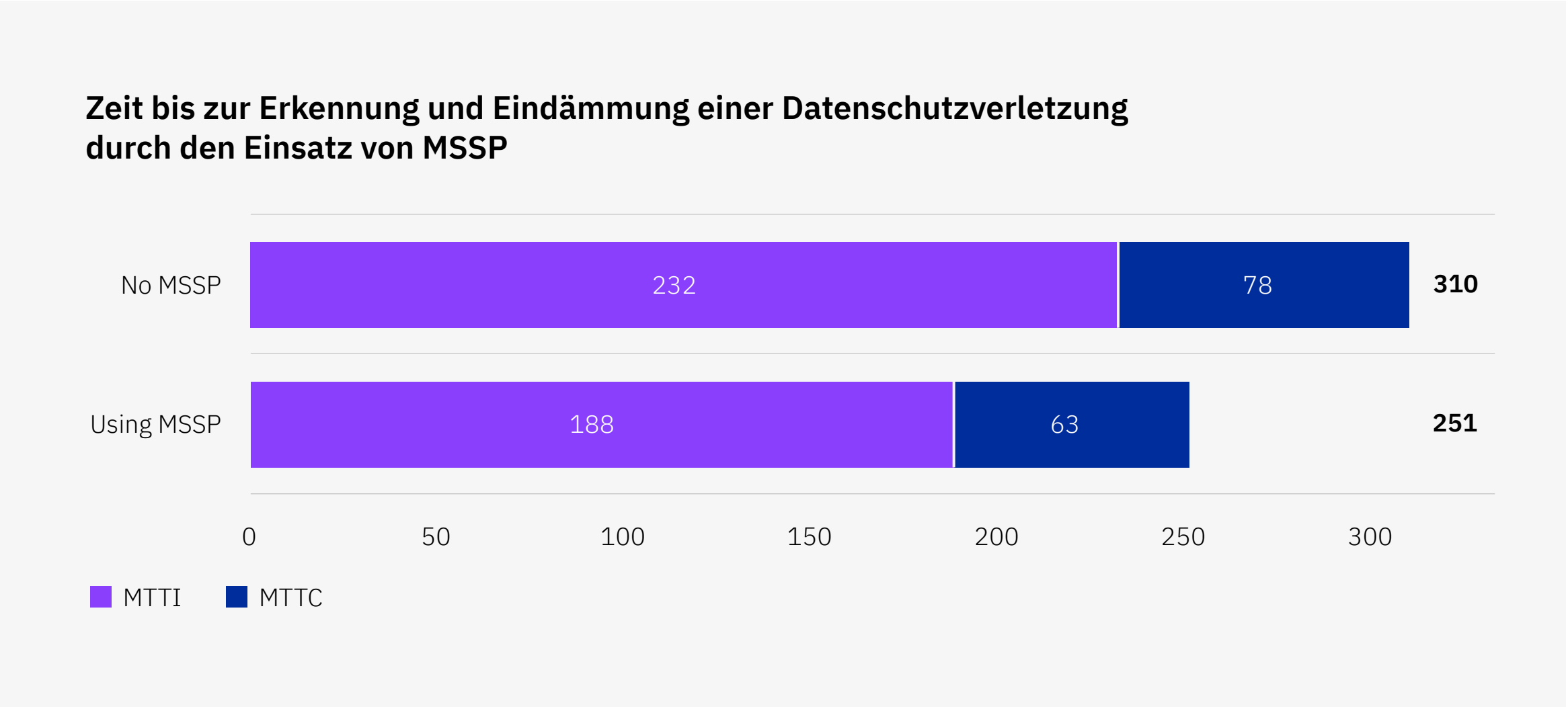
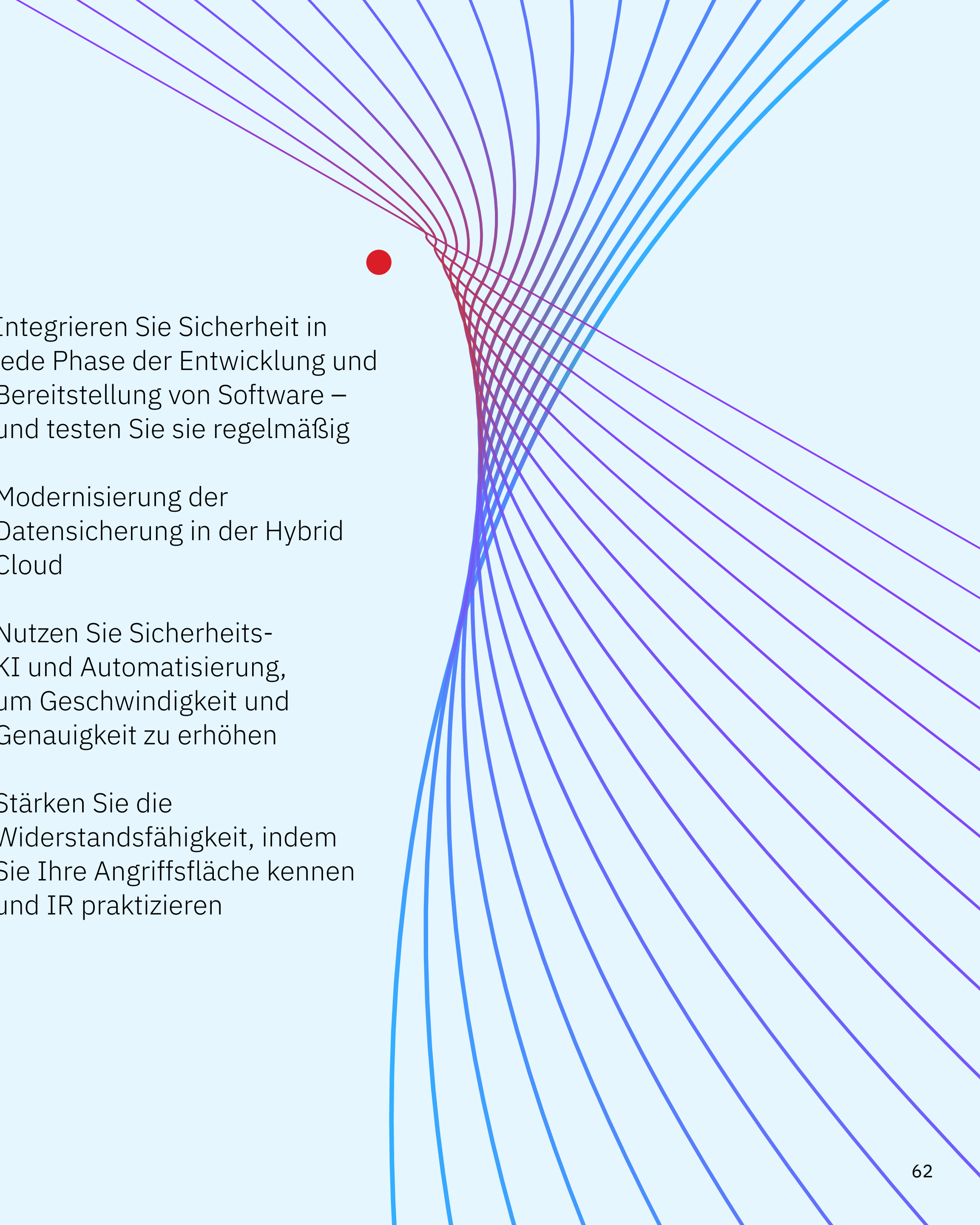


Abbildung 48. Angaben in Tagen

## Empfehlungen zur Reduzierung der Kosten einer Datenschutzverletzung

In diesem Abschnitt beschreibt IBM Security die Schritte, die Unternehmen befolgen können, um die finanziellen und reputationsbezogenen Auswirkungen einer Datenschutzverletzung zu reduzieren. Unsere Empfehlungen umfassen erfolgreiche Sicherheitsansätze, die mit geringeren Kosten und kürzeren Zeiten für die Erkennung und Eindämmung von Sicherheitsverletzungen verbunden sind.

- 
- 1 Integrieren Sie Sicherheit in jede Phase der Entwicklung und Bereitstellung von Software – und testen Sie sie regelmäßig
  - 2 Modernisierung der Datensicherung in der Hybrid Cloud
  - 3 Nutzen Sie Sicherheits-KI und Automatisierung, um Geschwindigkeit und Genauigkeit zu erhöhen
  - 4 Stärken Sie die Widerstandsfähigkeit, indem Sie Ihre Angriffsfläche kennen und IR praktizieren



# 1

## **Integrieren Sie Sicherheit in jede Phase der Entwicklung und Bereitstellung von Software – und testen Sie sie regelmäßig**

Die gesetzlichen Anforderungen werden immer komplizierter, vor allem, weil neue Technologien immer stärker mit dem Alltag verwoben sind und die Software immer mehr Funktionen und Komplexität aufweist. Ein [DevSecOps-Ansatz](#) – der wichtigste Kostenfaktor in einer speziellen Analyse von 27 Faktoren im Bericht 2023 – ist entscheidend, um Sicherheit in alle Tools oder Plattformen zu integrieren, die Unternehmen nutzen, um ihre Mitarbeiter oder Kunden einzubinden.

Unternehmen aller Art sollten dafür sorgen, dass Sicherheit der Kernaspekt der Software ist, die sie entwickeln, bzw. die sie als kommerzielle Standardsoftware einsetzen. Anwendungsentwickler müssen die Einführung der Prinzipien „[Secure by Design](#)“ und „[Secure by Default](#)“ weiter vorantreiben, um sicherzustellen, dass Sicherheit eine Kernanforderung ist, die bereits in der ersten Entwicklungsphase von Projekten zur [digitalen Transformation](#) einbezogen und nicht erst im Nachhinein berücksichtigt wird. Die gleichen Prinzipien werden auf [Cloudumgebungen](#) angewandt, um die Entwicklung von cloudnativen Anwendungen zu unterstützen, die sich ernsthaft um den Schutz der Benutzerdaten und die Minimierung von Angriffsflächen bemühen.

## [Anwendungstests oder Penetrationstests](#)

aus der Angreiferperspektive bieten Unternehmen auch die Möglichkeit, Schwachstellen zu erkennen und zu beheben, bevor sie zu Sicherheitsverletzungen führen. Keine Technologie oder Anwendung wird jemals vollständig sicher sein, und neue Funktionen bergen stets neue Risiken. Laufende Anwendungstests können Unternehmen helfen, neue Sicherheitslücken zu finden.

## 2

### **Modernisierung der Datensicherung in der Hybrid Cloud**

Daten werden in beispiellosem Umfang in Multi-Cloud-Umgebungen erstellt, geteilt und abgerufen. Die rasche Einführung neuer Cloudanwendungen und Cloud-Services erhöht das Risiko von „Shadow Data“, d. h. von sensiblen Daten, die nicht nachverfolgt oder verwaltet werden. Damit steigen auch die Risiken für Sicherheit und Compliance. Die Mehrheit (82 %) der Datenschutzverletzungen in diesem Bericht betraf Daten, die in Cloud-Umgebungen gespeichert waren, und 39 % der Datenschutzverletzungen betrafen Daten, die über mehrere verschiedene Umgebungen verteilt waren. Die Kosten und das Risiko solcher Datenschutzverletzungen werden dadurch

erhöht, dass die Matrix der geltenden Gesetze und die Strafen für Nichteinhaltung sich immer weiterentwickeln.

Angesichts dieser Herausforderungen sollte die Transparenz und Kontrolle von Daten, die in einer hybriden Cloud verteilt sind, für Unternehmen aller Art oberste Priorität haben und ein Schwerpunkt auf starke Verschlüsselung, Datensicherheit und Datenzugriffsrichtlinien gelegt werden. Unternehmen sollten sich um [Datensicherheits- und Konformitäts-Technologien](#) bemühen, die auf allen Plattformen funktionieren und es ihnen ermöglichen, Daten zu schützen, während sie sich zwischen Datenbanken, Anwendungen und Diensten bewegen, die in hybriden Cloud-Umgebungen eingesetzt

werden. Lösungen zur Überwachung der Datenaktivität können dazu beitragen, dass angemessene Kontrollen vorhanden sind und diese Richtlinien aktiv durchgesetzt werden, z. B. durch die frühzeitige Erkennung verdächtiger Aktivitäten und die Blockung von Echtzeitbedrohungen für kritische Datenspeicher.

Darüber hinaus können neuere Technologien wie das Management der Datensicherheitslage dabei helfen, unbekannte und sensible Daten in der gesamten Cloud aufzuspüren – einschließlich strukturierter und unstrukturierter Daten bei Cloud-Service-Anbietern, Software-as-a-Service (SaaS) und Data Lakes. Auf diese Weise lassen sich Sicherheitslücken

in den zugrundeliegenden Datenspeicherkonfigurationen, Berechtigungen und Datenflüssen identifizieren und entschärfen. Da Unternehmen zunehmend auf den hybriden Multicloud-Betrieb umsteigen, ist es unerlässlich, solide Strategien für das Identitäts- und Zugriffsmanagement (IAM) einzusetzen. Das umfasst auch Technologien wie die Multifaktorauthentifizierung (MFA), wobei der Schwerpunkt auf der Verwaltung privilegierter Benutzerkonten mit erhöhter Zugriffsebene liegt.

## 3

**Nutzen Sie Sicherheits-KI und Automatisierung, um Geschwindigkeit und Genauigkeit zu erhöhen**

Im Bericht 2023 gaben nur 28 % der Unternehmen an, dass sie KI und Automatisierung im Sicherheitsbereich intensiv nutzen. Das bedeutet, dass viele Unternehmen die Möglichkeit haben, ihre Geschwindigkeit, Genauigkeit und Effizienz zu verbessern. Der umfassende Einsatz von KI und Automatisierung im Sicherheitsbereich führte zu Kosteneinsparungen in Höhe von fast 1,8 Mio. US-Dollar bei Datenschutzverletzungen und verkürzte die Zeit zur Identifizierung und Eindämmung um mehr als 100 Tage im Vergleich zu Unternehmen, die keine KI einsetzen.

Sicherheitsteams können davon profitieren, wenn sie KI und Automatisierung in ihre Tools integrieren. Der Einsatz von KI und Automatisierung in allen [Tools zur Erkennung von und Reaktion auf Bedrohungen](#) kann Analysten beispielsweise dabei helfen, neue Bedrohungen genauer zu erkennen und Sicherheitswarnungen effektiver zu kontextualisieren und zuzuordnen. Diese Technologien können auch Teile des Untersuchungsprozesses von Bedrohungen automatisieren oder Maßnahmen empfehlen, um die Reaktion zu beschleunigen. Darüber hinaus können KI-gesteuerte Datensicherheits- und Identitätslösungen zu einer proaktiven Sicherheitshaltung beitragen, indem sie

risikoreiche Transaktionen identifizieren, sie mit minimaler Benutzerbelastung schützen und verdächtige Verhaltensweisen effektiver miteinander verknüpfen.

Beim Einsatz von KI in Ihren Sicherheitsabläufen, sollten Sie nach Technologien Ausschau halten, die bewährte und ausgereifte Anwendungsfälle mit nachgewiesener Genauigkeit, Effektivität und Transparenz bieten, um mögliche systematische Fehler, blinde Flecken oder Abweichungen zu vermeiden. Unternehmen sollten ein Betriebsmodell für die Einführung von KI planen, das kontinuierliches Lernen unterstützt, da sich sowohl die Sicherheitsbedrohungen als auch die technologischen Möglichkeiten weiterentwickeln.

Unternehmen können außerdem von einem Ansatz profitieren, der die wichtigsten Sicherheitstechnologien für reibungslosere Arbeitsabläufe und den Austausch von Erkenntnissen über gemeinsame Datenpools eng integriert. Chief Information Security Officers (CISOs) und Leiter der Sicherheitsabteilung (SecOps) können außerdem die [Bedrohungsdaten-Ermittlung](#) nutzen, um Muster zu erkennen und neu entstehende Bedrohungen zu erkennen.



## 4

### **Stärken Sie die Widerstandsfähigkeit, indem Sie Ihre Angriffsfläche kennen und IR praktizieren**

Verstehen Sie, welchen Angriffen Ihre Branche und Ihr Unternehmen am stärksten ausgesetzt sind, und ordnen Sie Ihrer Sicherheitsstrategie entsprechende Prioritäten zu. Tools wie [ASM](#) oder Techniken wie die [Angreifersimulation](#) können Unternehmen dabei helfen, einen Einblick in ihr individuelles Risikoprofil und ihre Sicherheitslücken zu erhalten, einschließlich der Sicherheitslücken, die leicht ausgenutzt werden können.

Darüber hinaus hat sich gezeigt, dass ein Team, das bereits mit den richtigen Protokollen und Tools für die Reaktion auf einen Vorfall vertraut ist, die Kosten und die Zeit für die Identifizierung und Eindämmung des Vorfalls erheblich reduziert.

Die IR-Planung und -Tests gehörten nicht nur zu den Top 3 der Kostenreduzierung im Bericht von 2023. Die Daten zeigen auch, dass Unternehmen, die diese Gegenmaßnahmen in hohem Maße einsetzen, 1,49 Millionen US-Dollar weniger Kosten für Datenschutzverletzungen aufwenden müssen als Unternehmen, die keine oder nur geringe Maßnahmen ergreifen, und dass sie Vorfälle 54 Tage schneller aufklären. Bilden Sie ein spezielles [IR-Team](#), erstellen Sie IR-Playbooks und testen Sie regelmäßig IR-Pläne in Tabletop-Übungen oder simulierten Umgebungen wie einem [Cyber-Bereich](#). Die Beauftragung eines IR-Anbieters kann ebenfalls dazu beitragen, die Zeit bis zur Reaktion auf einen Sicherheitsverstoß zu verkürzen.

Darüber hinaus sollten Unternehmen darauf achten, Netzwerksegmentierungspraktiken zu implementieren, um die Ausbreitung von Angriffen und das Ausmaß der von ihnen verursachten Schäden zu begrenzen, die allgemeine Widerstandsfähigkeit zu stärken und den Wiederherstellungsaufwand zu verringern.

*Empfehlungen für Sicherheitsverfahren dienen allein Informationszwecken und können keine Ergebnisse garantieren.*

# Demografie der Unternehmen

Die diesjährige Studie untersuchte 553 Unternehmen unterschiedlicher Größe aus 16 Ländern und geografischen Regionen und 17 Branchen. In diesem Abschnitt wird die Aufschlüsselung der untersuchten Unternehmen nach geografischen Regionen und Branchen erläutert und die Klassifizierung der Branchen definiert.

## 18 Jahre

Die USA nehmen seit 18 Jahren am Bericht über die Kosten einer Datenschutzverletzung teil und sind damit das am längsten teilnehmende Land bzw. die am längsten teilnehmende Region.

### Geografische Gliederung

Die Studie für das Jahr 2023 wurde in 16 verschiedenen Ländern und Regionen durchgeführt.

Globale Studie auf einen Blick

Länder	2023 Stichprobe	Prozentsatz	Währung	2023 USD Umrechnungskurs <sup>7</sup>	Untersucht seit (Jahren)
ASEAN	23	4 %	SGD	1,3294	7
Australien	24	4 %	AUD	1,4916	14
Brasilien	43	8 %	BRL	5,0702	11
Kanada	26	5 %	CAD	1,3525	9
Frankreich	34	6 %	EUR	0,9198	14
Deutschland	45	8 %	EUR	0,9198	15
Indien	51	9 %	INR	82,19	12
Italien	24	4 %	EUR	0,9198	12
Japan	42	8 %	JPY	132,75	12
Lateinamerika <sup>4</sup>	23	4 %	MXN	18,025	4
Naher und Mittlerer Osten <sup>5</sup>	36	7 %	SAR	3,7037	10
Skandinavien <sup>6</sup>	22	4 %	NOK	10,4445	5
Südafrika	21	4 %	ZAR	17,73	8
Südkorea	23	4 %	ZRW	1303,8	6
Vereinigtes Königreich	49	9 %	GBP	0,8085	16
USA	67	12 %	USD	1,00	18
Gesamt	553	100 %			

Abbildung 49. Tabelle mit allen untersuchten Ländern



### Untersuchte Branchen

Die Auswahl von 17 Branchen wurde über mehrere Jahre in die Studie einbezogen.

Insgesamt machen fünf Branchen 55 % der in der diesjährigen Studie untersuchten Unternehmen aus.

- 14 % Finanzwesen
- 12 % Dienstleistungen
- 11 % Technologie
- 10 % Industrie
- 8 % Energie

Verteilung der Stichprobe nach Branchen

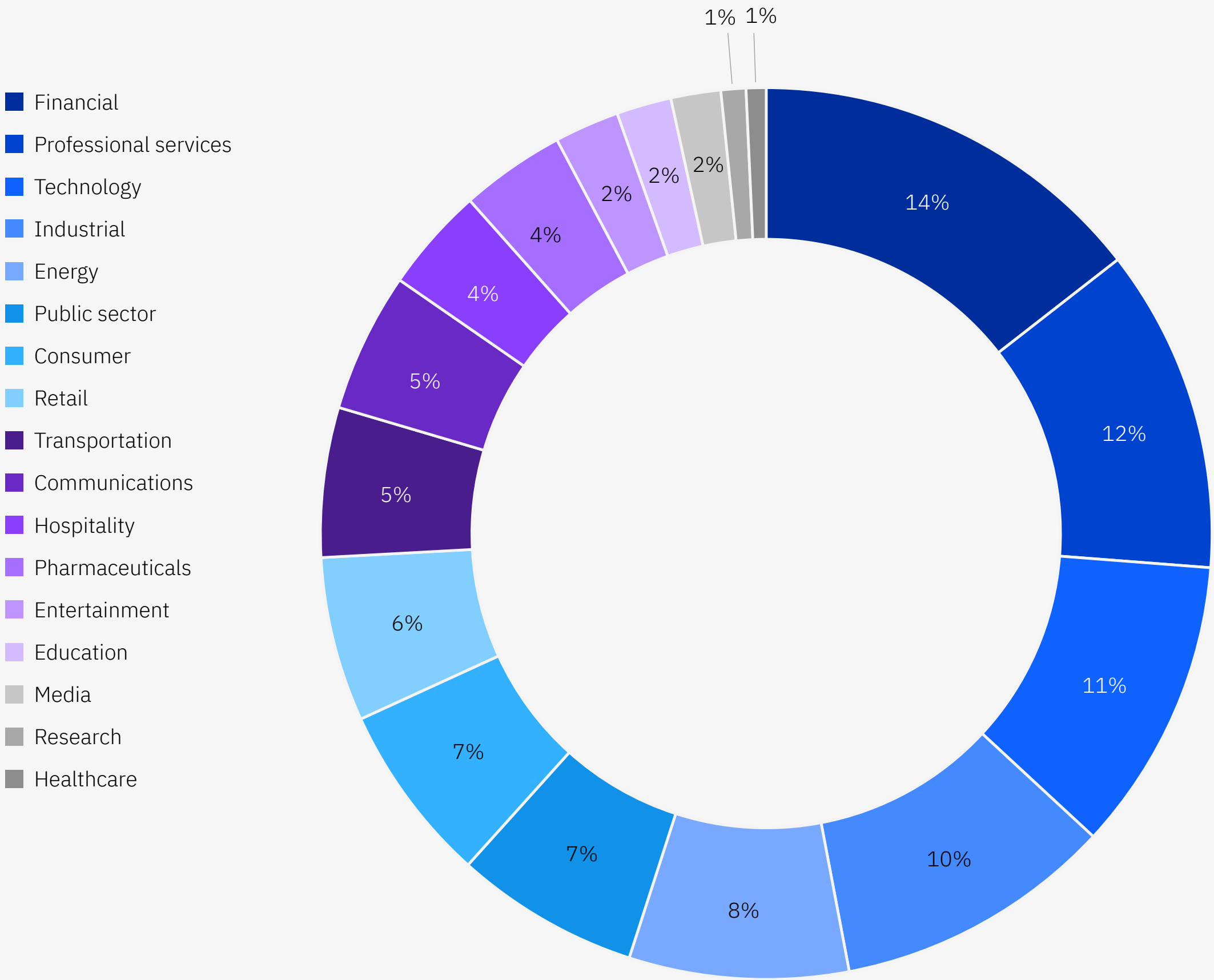


Abbildung 50. Prozentualer Anteil der Branchen

Definition der Branchen

- Gesundheitswesen**  
Krankenhäuser und Kliniken
- Finanzwesen**  
Banken, Versicherungen,  
Investmentgesellschaften
- Energie**  
Öl- und Gasunternehmen,  
Versorgungsunternehmen, Produzenten  
und Lieferanten alternativer Energien
- Pharma**  
Pharmazeutische Unternehmen, inklusive  
biomedizinische Lebenswissenschaften
- Industrie**  
Chemie-, Maschinenbau-  
und Fertigungsunternehmen
- Technologie**  
Hard- und Softwareunternehmen

- Schulung**  
Öffentliche und private Universitäten  
und Fachhochschulen, Aus- und  
Weiterbildungsunternehmen
- Services**  
Professionelle Dienstleistungen wie  
Rechts-, Steuer- und Beratungsfirmen
- Unterhaltung**  
Filmproduktion, Sport, Gaming  
und Kasinos
- Transport**  
Fluggesellschaften, Eisenbahnen,  
Speditionen und Lieferunternehmen
- Kommunikation**  
Zeitungen, Verleger und Werbeagenturen

- Konsumgüter**  
Hersteller und Vertreiber  
von Konsumgütern
- Medien**  
Fernsehen, Satelliten, soziale Medien  
und Internet
- Hotel- und Gastgewerbe**  
Hotels, Restaurantketten  
und Kreuzfahrtgesellschaften
- Einzelhandel**  
Ladengeschäfte und Online-Handel
- Forschung**  
Marktforschung, Thinktanks, Forschung  
und Entwicklung (F&E)
- Öffentlicher Sektor**  
Bundes-, Landes- und Kommunalbehörden  
sowie Nichtregierungsorganisationen  
(NGOs)

# Forschungsmethoden

Um die Vertraulichkeit zu wahren, wurden mit dem Benchmark-Instrument keine unternehmensspezifischen Informationen erhoben. Die Datenerhebungsmethoden berücksichtigten keine tatsächlichen Buchhaltungsdaten, sondern basierten auf der Schätzung der direkten Kosten durch die Teilnehmer, indem sie eine Spanne auf einer Zahlenreihe markierten. Die Teilnehmer sollten die Zahlenreihe an einer Stelle zwischen der Unter- und Obergrenze eines Bereichs für jede Kostenkategorie markieren.

Der aus der Zahlenreihe abgeleitete numerische Wert – anstelle einer Punktschätzung für jede dargestellte Kostenkategorie – gewährleistete die Wahrung der Vertraulichkeit und eine höhere Rücklaufquote. Im Rahmen des Benchmark-Instruments wurden die Befragten auch gesondert um eine zweite Schätzung der indirekten Kosten und der Opportunitätskosten gebeten.

Um einen überschaubaren Datensatz für das Benchmarking zu erhalten, wurden nur die Kostenstellen berücksichtigt, die einen entscheidenden Einfluss auf die Kosten von Datenschutzverletzungen haben. Nach Gesprächen mit Experten wurde eine feste Anzahl von Kostenbereichen ausgewählt. Nach der Erfassung der Benchmark-Informationen wurde jedes Instrument sorgfältig auf Konsistenz und Vollständigkeit geprüft.

Der Umfang der Kosten von Datenschutzverletzungen wurde auf bekannte Kostenkategorien beschränkt, die sich auf ein breites Spektrum von Geschäftsvorgängen im Zusammenhang mit personenbezogenen Daten beziehen. Wir haben uns dafür entschieden, uns auf die Geschäftsprozesse zu konzentrieren und nicht auf die Aktivitäten zur Einhaltung des Datenschutzes oder der Privatsphäre, weil wir glaubten, dass die Prozessstudie qualitativ bessere Ergebnisse liefern würde.



## Berechnung der Kosten von Datenschutzverletzungen

Zur Berechnung der durchschnittlichen Kosten einer Datenschutzverletzung wurden sehr kleine und sehr große Verstöße nicht mit einbezogen. Die im Bericht 2023 untersuchten Datenschutzverletzungen bewegten sich in einer Größenordnung zwischen 2.160 und 101.200 kompromittierten Datensätzen. Zur Untersuchung der Kosten sehr großer Datenschutzverletzungen führten wir eine separate Analyse durch, die im Abschnitt „Fragen zu Datenschutzverletzungen“ des Berichts näher erläutert wird.

Bei dieser Untersuchung wurde die Prozesskostenrechnung verwendet, bei der Prozesse identifiziert und die Kosten entsprechend der tatsächlichen Nutzung zugewiesen werden. Vier prozessbezogene Aktivitäten führen zu einer Reihe von Ausgaben im Zusammenhang mit einer Datenschutzverletzung in einem Unternehmen: Erkennung und Eskalation, Benachrichtigung, Reaktion nach dem Verstoß und entgangenes Geschäft.

**Erkennung und Eskalation**  
Aktivitäten, die es einem Unternehmen ermöglichen, den Verstoß zu erkennen, einschließlich:

- Forensische und investigative Maßnahmen
- Bewertungs- und Auditdienste
- Krisenmanagement
- Kommunikation mit Führungskräften und Vorstand

**Benachrichtigung**  
Maßnahmen zur Benachrichtigung betroffener Personen, Datenschutzbehörden und sonstiger Dritter:

- E-Mails, Briefe, ausgehende Anrufe oder allgemeine Mitteilungen an die Betroffenen
- Feststellung der gesetzlichen Bestimmungen
- Kommunikation mit den Behörden
- Beauftragung externer Experten

**Reaktion auf Vorfall**  
Maßnahmen zur Unterstützung der Opfer von Sicherheitsverletzungen bei der Kommunikation mit dem Unternehmen und bei der Durchführung von Wiedergutmachungsmaßnahmen für Opfer und Aufsichtsbehörden, einschließlich:

- Help Desk und eingehende Kommunikation
- Kreditüberwachung und Identitätsschutzdienste
- Einrichtung neuer Konten oder Ausgabe neuer Kreditkarten
- Rechtskosten
- Produktrabatte
- Ordnungsrechtliche Geldbußen

**Entgangenes Geschäft**  
Maßnahmen zur Minimierung von Kundenverlusten, Geschäftsunterbrechungen und Umsatzeinbußen:

- Betriebsunterbrechung und Einnahmeverluste aufgrund von Systemausfallzeiten
- Kosten durch Kundenabgang und Neukundenakquise
- Reputationsschäden und geschmälerter Goodwill

## Häufig gestellte Fragen zum Datenschutz

### Was ist eine Datenschutzverletzung?

Eine Sicherheitsverletzung ist definiert als ein Ereignis, bei dem Datensätze, die personenbezogene Daten, finanzielle oder medizinische Kontodaten oder andere geheime, vertrauliche oder geschützte Daten enthalten, potenziell kompromittiert werden. Diese Daten können in elektronischer Form oder in Papierform vorliegen. Im Rahmen dieser Studie wurden Verstöße zwischen 2.200 und 102.000 kompromittierten Datensätzen berücksichtigt.

### Was ist ein kompromittierter Datensatz?

Ein Datensatz ist eine Information, die vertrauliche oder urheberrechtlich geschützte Unternehmens-, Regierungs- oder Finanzdaten enthüllt oder eine Person identifiziert, deren Daten durch eine Datenschutzverletzung verloren gegangen sind oder gestohlen wurden. Beispiele hierfür sind eine

Datenbank mit dem Namen einer Person, Kreditkarteninformationen und anderen personenbezogenen Daten oder eine Patientenakte mit dem Namen des Versicherungsnehmers und Zahlungsinformationen.

### Wie erhalten Sie diese Daten?

Unsere Forscher erfassten detaillierte qualitative Daten in über 3.475 Einzelgesprächen mit Personen in 553 Unternehmen, die zwischen März 2022 und März 2023 von einer Datenschutzverletzung betroffen waren. Die Befragten waren IT-, Compliance- und Informationssicherheitsexperten, die mit der Datenschutzverletzung in ihrem Unternehmen und den damit verbundenen Kosten vertraut waren. Aus Gründen des Datenschutzes haben wir keine unternehmensspezifischen Informationen erhoben.

### Wie werden die durchschnittlichen Kosten einer Datenschutzverletzung berechnet?

Es wurden sowohl die direkten als auch die indirekten Kosten, die dem Unternehmen entstanden sind, erfasst. Die direkten Kosten umfassten die Beauftragung forensischer Experten, die Auslagerung des Hotline-Supports und die Bereitstellung kostenloser Abonnements für die Kreditüberwachung sowie Rabatte für künftige Produkte und Dienstleistungen. Indirekte Kosten umfassten interne Untersuchungen und Kommunikation sowie den hochgerechneten Wert des Kundenverlusts aufgrund von Fluktuation oder verringerten Kundengewinnungsraten.

Bei dieser Untersuchung wurden nur Ereignisse mit direktem Bezug zur Datenschutzverletzung berücksichtigt. Vorschriften wie die Allgemeine Datenschutzverordnung (DSGVO) und das kalifornische Gesetz zum Schutz der Privatsphäre von Verbrauchern (CCPA) können Unternehmen veranlassen, verstärkt in ihre Technologien für die Cybersicherheit zu investieren. Solche Maßnahmen wirkten sich in dieser Untersuchung jedoch nicht direkt auf die Kosten einer Datenschutzverletzung aus.

Um die Vergleichbarkeit mit den Vorjahren zu gewährleisten, haben wir die gleiche Währungsumrechnungsmethode angewandt, anstatt die Bilanzierungskosten anzupassen.



### Was ist der Unterschied zwischen Benchmarkforschung und Umfrageforschung?

Die Analyseeinheit im Bericht über die Kosten einer Datenschutzverletzung war das Unternehmen. Bei der Umfrageforschung ist die Analyseeinheit die Einzelperson. Wir haben 553 Organisationen für die Teilnahme an dieser Studie gewonnen.

### Können die durchschnittlichen Kosten pro Datensatz zur Berechnung der Kosten von Sicherheitsverletzungen mit Millionen verlorener oder gestohlener Datensätze verwendet werden?

Es ist mit dieser Untersuchung nicht vereinbar, die Gesamtkosten pro Datensatz als Grundlage für die Berechnung der Kosten einzelner oder mehrerer Sicherheitsverletzungen mit insgesamt Millionen von Datensätzen heranzuziehen. Die Kosten pro Datensatz wurden aus unserer Studie von Hunderten von Datenschutzverletzungen abgeleitet,

bei denen jeweils 101.200 oder weniger Datensätze kompromittiert wurden. Um die Auswirkungen von Mega-Datenschutzverletzungen, die eine Million oder mehr Datensätze betreffen, zu messen, verwendet die Studie stattdessen ein Simulation-Framework, das auf einer Stichprobe von 20 Ereignissen dieser Größenordnung basiert.

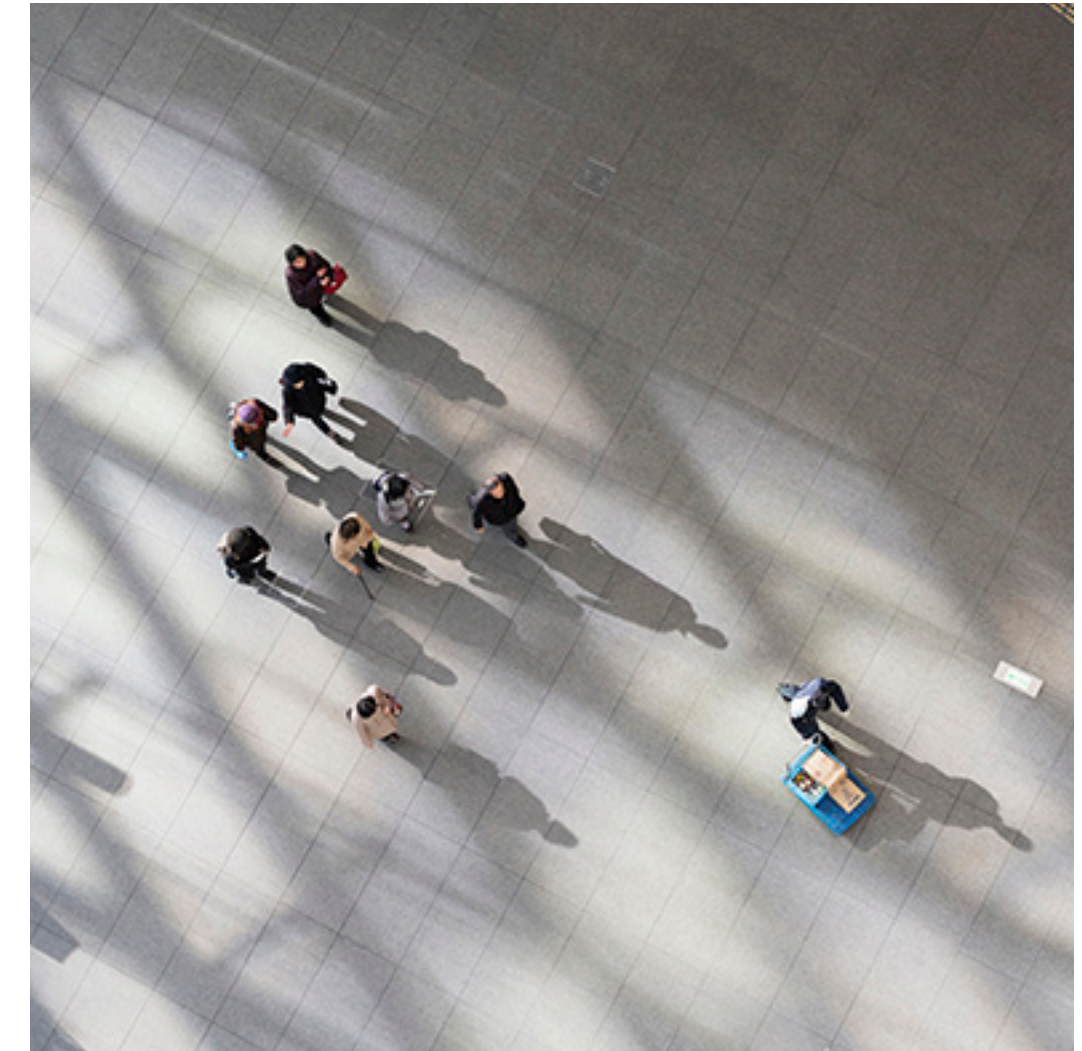
### Warum wurden Simulationsverfahren zur Schätzung der Kosten einer Mega-Datenschutzverletzung eingesetzt?

Die Stichprobengröße von 20 Unternehmen, bei denen eine Mega-Datenschutzverletzung auftrat, war nicht groß genug, um eine statistisch signifikante Analyse mit den in der Studie verwendeten tätigkeitsbezogenen Kostenmethoden durchzuführen. Deshalb haben wir Monte-Carlo-Simulationen verwendet, um durch wiederholte Versuche eine Reihe möglicher, d. h. zufälliger, Ergebnisse zu ermitteln.

Wir haben insgesamt über 250.000 Versuche durchgeführt. Der Gesamtmittelwert aller Stichprobenmittelwerte ergab das wahrscheinlichste Ergebnis für jede Größe der Datenschutzverletzung im Bereich von 1–60 Mio. kompromittierter Datensätze.

### Beobachten Sie jedes Jahr die gleichen Unternehmen?

Für jede jährliche Studie wird eine andere Auswahl an Unternehmen herangezogen. Um die Vergleichbarkeit mit früheren Berichten zu gewährleisten, werden jedes Jahr Unternehmen mit ähnlichen Merkmalen rekrutiert und abgeglichen, wie z. B. Branche, Beschäftigtenzahl, geografische Ausdehnung und Umfang der Datenschutzverletzung. Seit Beginn dieser Untersuchung im Jahr 2005 haben wir die Erfahrungen mit Datenschutzverletzungen von 5.580 Unternehmen untersucht.





## Grenzen der Forschung

In unserer Studie wurde eine vertrauliche und geschützte Benchmark-Methode verwendet, die bereits in früheren Untersuchungen erfolgreich eingesetzt wurde. Die mit dieser Benchmark-Studie verbundenen Einschränkungen müssen jedoch sorgfältig berücksichtigt werden, bevor Schlussfolgerungen aus den Ergebnissen gezogen werden.

### **Nichtstatistische Ergebnisse**

Unsere Studie stützt sich auf eine repräsentative, nichtstatistische Stichprobe weltweiter Unternehmen. Statistische Schlussfolgerungen, Fehlermargen und Konfidenzintervalle können auf diese Daten nicht angewendet werden, da unsere Stichprobenverfahren nicht wissenschaftlich waren.

### **Fehlende Beobachtungen**

Eine Verzerrung durch fehlende Beobachtungen wurde nicht untersucht. Es ist deshalb möglich, dass sich die

Unternehmen, die nicht teilgenommen haben, in Bezug auf die zugrundeliegenden Kosten der Datenschutzverletzungen wesentlich unterscheiden.

### **Verzerrung des Stichprobenrahmens**

Da es sich bei unserem Stichprobenrahmen um ein wertendes Verfahren handelte, ist die Qualität der Ergebnisse davon abhängig, inwieweit der Rahmen repräsentativ für die untersuchte Unternehmenspopulation war. Wir sind der Meinung, dass der derzeitige Stichprobenrahmen Unternehmen mit ausgereifteren Datenschutz- oder Informationssicherheitsprogrammen begünstigt hat.

### **Unternehmensinformationen**

Im Rahmen der Untersuchung wurden keine unternehmensbezogenen Informationen erfasst. Einzelpersonen konnten kategoriale Antwortvariablen verwenden, um demografische Informationen über das Unternehmen und die Branchenkategorie offenzulegen.

### **Unberücksichtigte Faktoren**

Bei unseren Analysen wurden Variablen wie führende Trends und organisatorische Merkmale nicht berücksichtigt. Inwieweit die nicht berücksichtigten Variablen die Benchmark-Ergebnisse erklären können, lässt sich nicht feststellen.

### **Extrapolierte Kostenwerte**

Trotz bestimmter Kontrollmechanismen, die in den Benchmark-Prozess integriert werden können, besteht immer die Möglichkeit, dass die Befragten keine genauen oder wahrheitsgemäßen Angaben gemacht haben. Zudem kann die Verwendung von Kostenextrapolationsmethoden anstelle von tatsächlichen Kostendaten unbeabsichtigt zu Verzerrungen und Ungenauigkeiten führen.

### **Währungsumrechnung**

Durch die Umrechnung von lokalen Währungen in USD wurden die durchschnittlichen Gesamtkostenschätzungen für andere Länder deflationiert. Aus Gründen der Vergleichbarkeit mit den Vorjahren haben wir uns entschlossen, die gleiche Bilanzierungsmethode beizubehalten und die Kosten nicht anzupassen. Es ist zu beachten, dass sich dieses Problem nur auf die globale Analyse auswirken kann, da alle Ergebnisse auf Länderebene in lokaler Währung dargestellt werden. Die aktuellen realen Wechselkurse, die in diesem Forschungsbericht verwendet werden, wurden von der US-Notenbank am 31. März 2023 veröffentlicht.

# Informationen über das Ponemon Institute und IBM Security

## Ponemon Institute

Das 2002 gegründete Ponemon Institute widmet sich der unabhängigen Forschung und Aufklärung zur Förderung verantwortungsvoller Praktiken im Umgang mit Daten und Datenschutz in Unternehmen und Behörden. Unsere Aufgabe ist es, hochwertige empirische Studien zu wesentlichen Themen durchzuführen, die die Verwaltung und Sicherheit sensibler Daten zu Personen und Unternehmen betreffen.

Das Ponemon Institute hält im Hinblick auf Vertraulichkeit, Datenschutz und Forschungsethik strenge Standards ein und sammelt im Rahmen seiner geschäftlichen Forschung keinerlei personenbezogene Daten von Einzelpersonen oder identifizierbare Unternehmensdaten. Darüber hinaus stellen strenge Qualitätsstandards sicher, dass Befragten keine sachfremden, irrelevanten oder unangemessenen Fragen vorgelegt werden.

## IBM Security

IBM Security unterstützt die größten Unternehmen und Regierungen der Welt mit einem integrierten Portfolio von Sicherheitsprodukten und -services, die mit dynamischer KI und Automatisierungsfunktionen ausgestattet sind. Das Portfolio, das von der weltweit anerkannten IBM Security X-Force® Forschung unterstützt wird, ermöglicht es Unternehmen, Bedrohungen vorherzusehen, Daten zu schützen, während sie bewegt werden, und schnell und präzise zu reagieren, ohne geschäftliche Innovationen zu behindern. Tausende von Unternehmen vertrauen IBM als ihrem Partner bei der Bewertung, Strategieentwicklung, Implementierung und Verwaltung von Sicherheitstransformationen.

IBM betreibt eine der weltweit größten Organisationen für Sicherheitsforschung, -entwicklung und -bereitstellung, überwacht täglich mehr als 150 Milliarden Sicherheitsereignisse in mehr als 130 Ländern und hat weltweit mehr als 10.000 Sicherheitspatente erhalten.

Bei Fragen oder Anmerkungen zu diesem Forschungsbericht, inklusive Anfragen zur Genehmigung einer Zitierung oder Vervielfältigung des Berichts, wenden Sie sich bitte per Post, Telefon oder E-Mail an:

Ponemon Institute LLC  
Attn: Forschungsabteilung  
2308 US 31 North  
Traverse City  
Michigan 49686 USA  
1.800.887.3118  
[research@ponemon.org](mailto:research@ponemon.org)

Erfahren Sie mehr über die Verbesserung Ihres Sicherheitsniveaus

Besuchen Sie [ibm.com/de-de/security](https://ibm.com/de-de/security).

Nehmen Sie am fachlichen Austausch der [IBM Security Community](#) teil.

Nächste Schritte

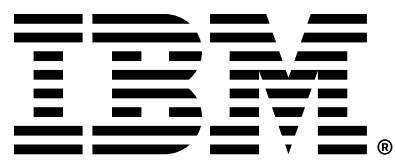
- KI-Lösungen für Cybersicherheit**  
Beschleunigen Sie die Reaktionszeiten der Sicherheit und steigern Sie die Produktivität.  
[Mehr erfahren](#)
- Lösungen für die Bedrohungserkennung und -reaktion**  
Ermächtigen Sie Sicherheitsteams, Bedrohungen mit Schnelligkeit, Genauigkeit und Effizienz zu überlisten.  
[Mehr erfahren](#)
- Cloud-Sicherheitslösungen**  
Sicherheit in den Weg zur hybriden Multi-Cloud-Umgebung integrieren.  
[Mehr erfahren](#)
- Lösungen für Ransomware**  
Verwalten Sie Cybersicherheitsrisiken und -schwachstellen, um die Auswirkungen von Ransomware zu minimieren.  
[Mehr erfahren](#)

- Lösungen für Identitäts- und Zugriffsmanagement**  
Sichere Verbindungen für alle Benutzer, APIs und Geräte mit jeder App.  
[Mehr erfahren](#)
- Services zur Reaktion auf Vorfälle und Erkennung von Bedrohungen**  
Proaktiv auf Sicherheitsbedrohungen antworten und auf sie reagieren.  
[Mehr erfahren](#)
- Datensicherheits- und Datenschutzlösungen**  
Datenschutz und Konformität über hybride Clouds hinweg vereinfachen.  
[Mehr erfahren](#)

- Angriffsflächenmanagement**  
Verwalten Sie die Erweiterung Ihres digitalen Fußabdrucks und verbessern Sie die Cyberresilienz Ihrer Organisation schnell.  
[Mehr erfahren](#)
- Lösungen für Unified Endpoint Management**  
Skalieren Sie Ihre mobilen Mitarbeiter, indem Sie jedes Gerät schützen und verwalten.  
[Mehr erfahren](#)
- Governance, Risiko- und Konformitäts-Services**  
Erhöhen Sie die Cybersicherheitsfähigkeit mit einem integrierten Governance-, Risiko- und Konformitäts-Ansatz.  
[Mehr erfahren](#)

- Persönliches Beratungsgespräch vereinbaren**  
Treffen Sie sich mit einem Experten bei IBM Security X-Force, um Ihre Anforderungen zu besprechen.  
[Mehr erfahren](#)
- Workshop zu IBM Sicherheit und Framing-Erkennung anfordern**  
Holen Sie sich Unterstützung bei der Modernisierung Ihres Sicherheitsprogramms.  
[Mehr erfahren](#)





1. Es ist mit dieser Untersuchung nicht vereinbar, die Kosten pro Datensatz zu verwenden, um die Kosten einzelner oder mehrerer Sicherheitsverletzungen mit mehr als 102.000 Datensätzen zu berechnen. Weitere Informationen finden Sie im Abschnitt „Forschungsmethode“.
2. ASEAN ist eine Cluster-Stichprobe von Unternehmen in Singapur, Indonesien, Malaysia, Thailand, Vietnam und auf den Philippinen.
3. Destruktive Angriffe sind definiert als Angriffe, die Systeme funktionsunfähig machen und eine Wiederherstellung in Frage stellen. Sie können auch ein Lösegeld beinhalten, müssen es aber nicht.
4. Lateinamerika ist eine Cluster-Stichprobe von Unternehmen in Mexiko, Argentinien, Chile und Kolumbien.
5. Naher Osten ist eine Cluster-Stichprobe von Unternehmen in Saudi-Arabien und den Vereinigten Arabischen Emiraten.
6. Skandinavien ist eine Cluster-Stichprobe für Unternehmen in Dänemark, Schweden, Norwegen und Finnland.
7. Devisenkurse – H.10, 31. März 2023.

© Copyright IBM Corporation 2023

IBM Deutschland GmbH  
IBM-Allee 1  
71139 Ehningen  
[ibm.com/de](http://ibm.com/de)  
IBM Österreich  
Obere Donaustraße 95  
1020 Wien  
[ibm.com/at](http://ibm.com/at)  
IBM Schweiz  
Vulkanstrasse 106  
8010 Zürich  
[ibm.com/ch](http://ibm.com/ch)  
IBM Corporation  
New Orchard Road  
Armonk, NY 10504

Hergestellt in den  
Vereinigten Staaten von Amerika  
Juli 2023

IBM, das IBM Logo, IBM Security und X-Force sind Marken oder eingetragene Marken der International Business Machines Corporation in den Vereinigten Staaten und/oder anderen Ländern. Weitere Produkt- und Servicenamen sind möglicherweise Marken von IBM oder anderen Unternehmen. Eine aktuelle Liste der Marken von IBM finden Sie unter [ibm.com/de-de/trademark](http://ibm.com/de-de/trademark).

Das vorliegende Dokument ist ab dem Datum der Erstveröffentlichung aktuell und kann jederzeit von IBM geändert werden. Nicht alle Angebote sind in allen Ländern, in denen IBM tätig ist, verfügbar.

Alle angeführten oder beschriebenen Beispiele illustrieren lediglich, wie einige Kunden IBM Produkte verwendet haben und welche Ergebnisse sie dabei erzielt haben. Die tatsächlichen Umgebungskosten und Leistungsmerkmale variieren in Abhängigkeit von den Konfigurationen und Bedingungen des jeweiligen Kunden. Es können keine generell zu erwartenden Ergebnisse bereitgestellt werden, da die Ergebnisse jedes Kunden allein von seinen Systemen und bestellten Services abhängt. DIE INFORMATIONEN IN DIESEM DOKUMENT WERDEN OHNE JEGliche AUSDRÜCKliche ODER STILLSCHWEIGENDE GEWÄHRLEISTUNG ZUR VERFÜGUNG GESTELLT, EINSCHLIESSLICH DER GEWÄHRLEISTUNG DER HANDELSÜBLICHKEIT, DER TAUGLICHKEIT FÜR EINEN BESTIMMTEN ZWECK UND DER GEWÄHRLEISTUNG ODER BEDINGUNG DER NICHTVERLETZUNG VON RECHTEN. Die Gewährleistung für Produkte von IBM richtet sich nach den Vertragsbedingungen der Vereinbarungen, unter denen sie bereitgestellt werden.

Erklärung zu guten Sicherheitsverfahren:  
IT-Systemsicherheit umfasst den Schutz von Systemen und Informationen durch Prävention, Erkennung und Reaktion auf unzulässigen Zugriff innerhalb und außerhalb Ihres Unternehmens. Unbefugter Zugriff kann dazu führen,

dass Informationen verändert, vernichtet, veruntreut oder unsachgemäß gebraucht werden. Er kann auch zu Schäden an Ihrem System oder zum Missbrauch davon, u. a. im Rahmen von Angriffen gegen Dritte, führen. Kein IT-System oder -Produkt darf als vollkommen sicher betrachtet werden und es gibt kein Produkt, keine Dienstleistung und keine Sicherheitsmaßnahme, das bzw. die alleine vollständig vor einer unsachgemäßen Verwendung oder unbefugtem Zugriff schützen kann. Die Systeme, Produkte und Dienstleistungen von IBM werden als Teil eines rechtmäßigen, umfassenden Sicherheitsansatzes konzipiert. Daran sind notwendigerweise weitere Betriebsverfahren beteiligt und es können weitere Systeme, Produkte oder Dienstleistungen erforderlich sein, um eine möglichst hohe Effektivität zu erzielen. IBM GEWÄHRLEISTET NICHT, DASS SYSTEME, PRODUKTE ODER DIENSTLEISTUNGEN GEGEN SCHÄDLICHES ODER RECHTSWIDRIGES VERHALTEN JEDLICHER PARTEIEN IMMUN SIND ODER IHR UNTERNEHMEN DAGEGEN IMMUN MACHEN.

Die Einhaltung der Datenschutzgesetze und -richtlinien liegt in der Verantwortung des Kunden. IBM bietet keine Rechtsberatung an und gewährleistet nicht, dass die Dienstleistungen oder Produkte von IBM die Einhaltung von Gesetzen oder Vorschriften durch den Kunden sicherstellen. Aussagen über die zukünftige Ausrichtung und Vorhaben von IBM vorbehalten, da sie lediglich Ziele und Absichten darstellen.