SOPHOS

Ransomware-Report 2023

Ergebnisse einer unabhängigen Befragung von 3.000 IT-/Cybersecurity-Entscheidern aus 14 Ländern. Durchgeführt im Zeitraum Januar bis März 2023.

Sophos-Whitepaper, Mai 2023

Einführung

Jedes Jahr befragt Sophos im Rahmen einer Studie IT-/Cybersecurity-Experten aus aller Welt zu ihren Erfahrungen mit Ransomware. Die Studie geht auf die gängigsten Angriffsursachen ein und gibt Aufschluss darüber, wie sich die Erfahrungen mit Ransomware je nach Unternehmensumsatz unterscheiden. Außerdem zeigt sie, welche Auswirkungen auf Geschäft und Betrieb es hat, wenn Unternehmen Und Organisationen nach einem Ransomware-Angriff Lösegeld zahlen, um die Daten zurück zu erhalten, statt Backups zum Wiederherstellen ihrer Daten zu nutzen.

Über die Studie

Sophos hat eine unabhängige Befragung von 3.000 IT-/Cybersecurity-Entscheidern in Unternehmen und Organisationen mit 100 bis 5.000 Mitarbeitern aus 14 Ländern in Nord- und Südamerika, EMEA und Asien-Pazifik in Auftrag gegeben. Die Befragung fand von Januar bis März 2023 statt. Die Umfrageteilnehmer wurden gebeten, sich bei der Beantwortung der Fragen auf ihre Erfahrungen innerhalb des vergangenen Jahres zu beziehen.

Im Bildungsbereich wurde die Gruppe der Befragten unterteilt in zwei Unterbereiche:

1. Grund- und weiterführende Schulen

2. Hochschulen

Inhaltsverzeichnis

Häufigkeit von Ransomware-Angriffen

Die Studie ergab, dass das Ransomware-Aufkommen relativ stabil geblieben ist. Genau wie im Vorjahr waren 66 % der Befragten im vergangenen Jahr von Ransomware betroffen. Da Bedrohungsakteure heute in der Lage sind, großangelegte Angriffe auszuführen, ist Ransomware das aktuell wohl größte Risiko für Unternehmen.

Cyberkriminelle haben das Ransomware-as-a-Service-Modell über mehrere Jahre hinweg weiterentwickelt und optimiert. Ransomware-as-a-Service erleichtert den Einstieg in die Cyberkriminalität und sorgt für zunehmend komplexe Angriffe, da Angreifern so ermöglicht wird, sich auf verschiedene Phasen eines Angriffs zu spezialisieren. Mehr Informationen zu Ransomware-as-a-Service finden Sie im Sophos Threat Report 2023.

2020	2021	2022	2023
51 %	37 %	66 %	66 %

War Ihr Unternehmen im letzten Jahr von Ransomware betroffen?
Ja. Anzahl=3.000 (2023), 5.600 (2022), 5.400 (2021), 5.000 (2020)

Angriffe nach Land

Trotz des relativ unveränderten Ransomware-Aufkommens im Vergleich zum Vorjahr zeigen sich Unterschiede auf Länderebene. Mit 84 % meldete Singapur das höchste Aufkommen an Ransomware-Angriffen. Großbritannien verzeichnete dagegen die wenigsten Ransomware-Angriffe (44 %).

In Österreich ging die Angriffsrate am stärksten zurück – von 84 % auf 50 %. Südafrika beobachtete den größten Anstieg des Angriffsaufkommens von 51 % in 2022 auf 78 % in 2023.

Weitere Informationen finden Sie im Abschnitt „Häufigkeit von Ransomware-Vorfällen nach Land: 2022 ggü. 2023“ auf Seite 20.

Angriffe nach Branche

Mit 80 % (Grund-und weiterführende Schulen) und 79 % (Hochschulen) war das Bildungswesen am häufigsten von Ransomware-Angriffen betroffen. Im Bildungsbereich mangelt es oft an den nötigen personellen, finanziellen und technologischen Ressourcen. Die Daten zeigen eindeutig, dass Cyberkriminelle diesen Umstand ausnutzen.

Die IT, Technologie und Telekommunikation meldete das geringste Angriffsaufkommen (50 %), ein klares Indiz für eine effektivere Cyberabwehr.

Weitere Informationen finden Sie im Abschnitt „Häufigkeit von Ransomware-Vorfällen nach Branche“ auf Seite 21.

66 % von Ransomware betroffen

Singapur höchstes Angriffsaufkommen (Land)

UK niedrigste Angriffsrate (Land)

Bildungswesen höchstes Angriffsaufkommen (Branche)

IT, Technologie und Telekommunikation
niedrigste Angriffsrate (Branche)

Angriffe nach Unternehmensgröße: Umsatz vs. Zahl der Mitarbeiter

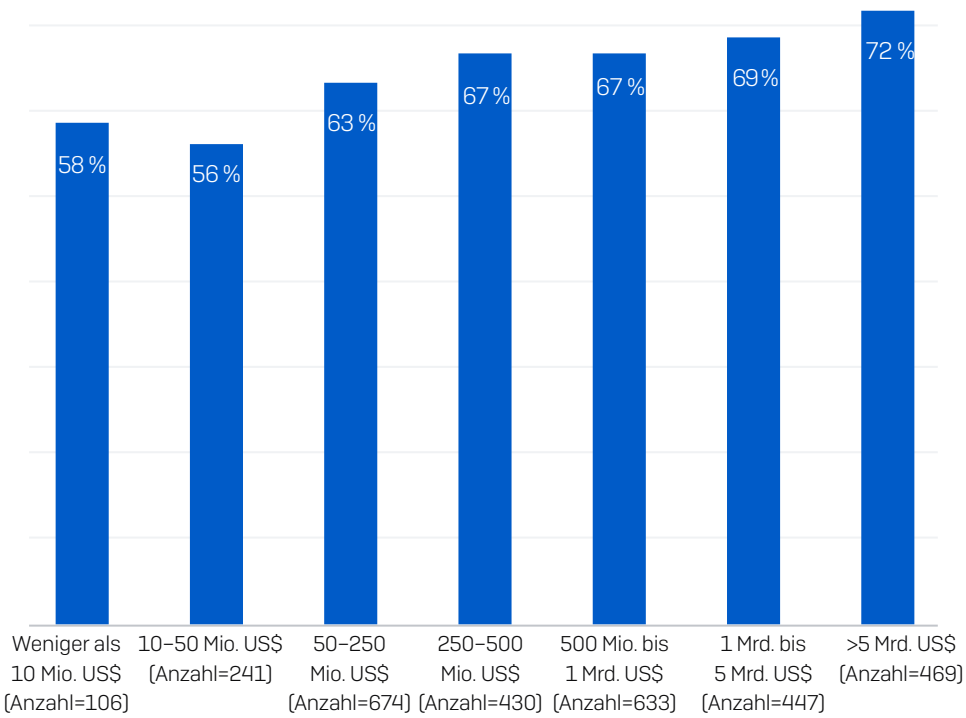
Die Studie offenbart einen direkten Zusammenhang zwischen dem Jahresumsatz und der Wahrscheinlichkeit eines Ransomware-Angriffs: Je höher der Jahresumsatz, desto höher das Angriffsaufkommen. So waren im vergangenen Jahr 56 % der Unternehmen mit einem Jahresumsatz von 10 bis 50 Mio. US$ Opfer von Ransomware. Bei Unternehmen mit einem Jahresumsatz von 5 Mrd. US$ steigt der Anteil der Betroffenen auf 72 %.

Dagegen ließ sich kein klarer Zusammenhang zwischen der Mitarbeiterzahl und der Angriffswahrscheinlichkeit feststellen. Mit Ausnahme der Unternehmen mit 1.001 bis 3.000 Mitarbeitern war das Angriffsaufkommen relativ einheitlich:

- 100–250 Mitarbeiter 62 %
- 251–500 Mitarbeiter 62 %
- 501–1.000 Mitarbeiter 62 %
- 1.001–3.000 Mitarbeiter 73 %
- 3.001–5.000 Mitarbeiter 63%

Die Daten verdeutlichen, dass der Jahresumsatz in Zusammenhang mit der Unternehmensgröße ein weitaus aussagekräftigerer Indikator für die Angriffswahrscheinlichkeit ist als die Mitarbeiterzahl.

Prozentsatz der Unternehmen, die von Ransomware betroffen waren, nach Umsatz



War Ihr Unternehmen im letzten Jahr von Ransomware betroffen? Ja. Anzahl der erhaltenen Antworten jeweils in Klammer

Ursachen von Ransomware-Angriffen

Wie aus der Studie hervorgeht, waren ausgenutzte Schwachstellen die häufigste Ursache von Ransomware-Angriffen (36 %), gefolgt von kompromittierten Anmeldedaten (29 %). Diese Zahlen entsprechen im Wesentlichen den Ergebnissen unserer aktuellen retrospektiven Analyse von 152 Vorfällen, die von unseren Incident Respondern und MDR-Experten bearbeitet wurden. Dabei gingen 37 % der Vorfälle von ausgenutzten Sicherheitslücken aus und 30 % von kompromittierten Anmeldedaten.

30 % der Angriffe (gerundet) wurden durch E-Mails verursacht: 18 % der Angriffe waren auf Schad-E-Mails, 13 % auf Phishing zurückzuführen. 3 % gingen von einem Brute-Force-Angriff aus und lediglich 1 % von einem Download.

36 %	29 %	18 %
Ausgenutzte Schwachstelle	Kompromittierte Anmeldedaten	Schad-E-Mails
13 %	**3 %**	**1 %**
Phishing	Brute-Force-Angriff	Downloads

Kennen Sie die Ursache des Ransomware-Angriffs auf Ihr Unternehmen im vergangenen Jahr? Wenn Ihr Unternehmen von mehreren Angriffen betroffen war, denken Sie bei Ihrer Antwort an den schwersten Angriff. (Anzahl=1.974 Unternehmen, die im letzten Jahr von Ransomware-Angriffen betroffen waren)

Ursachen nach Branche

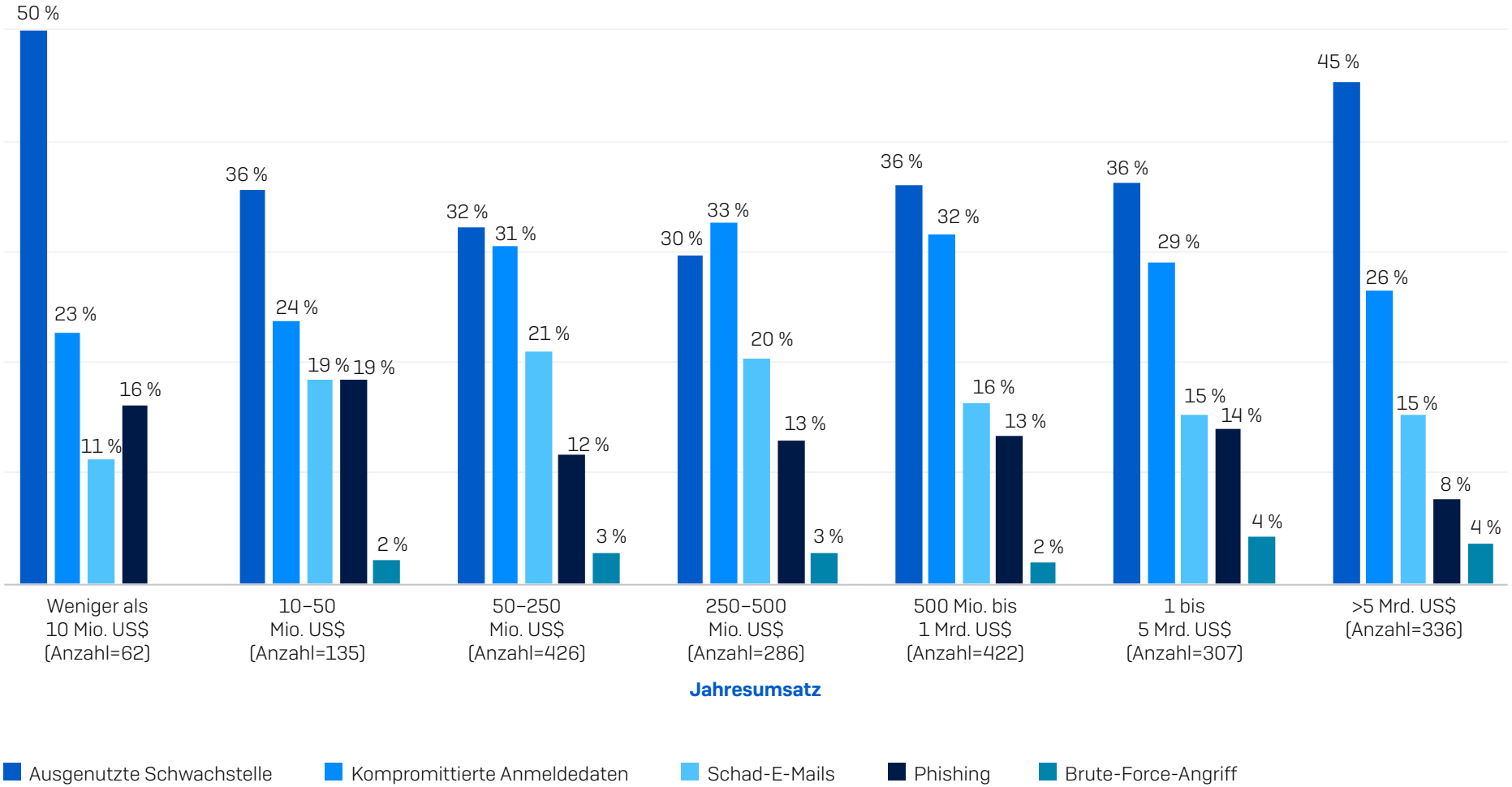
Der Medien-, Freizeit- und Unterhaltungssektor meldete die meisten Angriffe aufgrund ausgenutzter Schwachstellen (55 %). Dies lässt darauf schließen, dass Sicherheitslücken in dieser Branche weit verbreitet sind. Die Mehrheit der Vorfälle aufgrund kompromittierter Anmeldedaten verzeichneten Bundesbehörden mit 41 %. Womöglich ist dies darauf zurückzuführen, dass der öffentliche Sektor besonders häufig Opfer von Zugangsdatendiebstahl ist und die Ausnutzung gestohlener Anmeldedaten nur bedingt verhindern kann.

Unternehmen im Bereich IT, Technologie und Telekommunikation meldeten die niedrigsten Raten ausgenutzter Schwachstellen (22 %) und kompromittierter Anmeldedaten (22 %). Aller Wahrscheinlichkeit nach liegt dies an der effektiven Cyberabwehr in diesem Bereich. Allerdings meldete diese Branche die meisten E-Mail-basierten Angriffe. So gingen mehr als die Hälfte der Angriffe (51 %) von den Posteingängen der Mitarbeiter aus.

Weitere Informationen finden Sie im Abschnitt „Angriffsursache nach Branche“ auf Seite 22.

Ursachen nach Umsatz

Betrachten wir die Angriffsursache nach Jahresumsatz, so zeigt sich bei ausgenutzten Schwachstellen und kompromittierten Anmeldedaten eine gegenläufige Tendenz. Der höchste prozentuale Anteil von Angriffen durch ausgenutzte Schwachstellen entfiel auf Unternehmen mit dem niedrigsten (<10 Mio.US$: 50 %) und dem höchsten (>5 Mrd. US$: 45 %) Umsatz. In der Gruppe dazwischen (250–500 Mio. US$) wurden lediglich 30 % Angriffe durch ausgenutzte Schwachstellen verursacht. Unternehmen in der mittleren Umsatzgruppe verzeichneten die meisten Angriffe aufgrund kompromittierter Anmeldedaten (33 %), Unternehmen mit dem höchsten (23 %) und niedrigsten (26 %) Jahresumsatz die wenigsten.

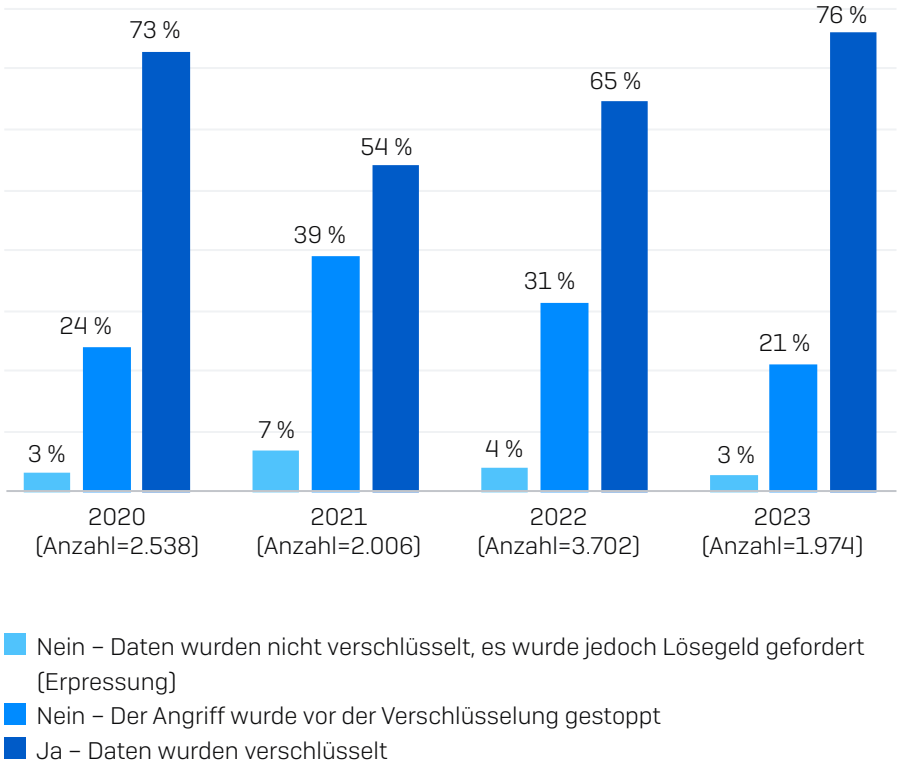


Kennen Sie die Ursache des Ransom-Angriffs auf Ihr Unternehmen im vergangenen Jahr? Ausgewählte Antwortoptionen. Anzahl der erhaltenen Antworten jeweils in Klammer

Datenverschlüsselungsrate

Die Verschlüsselung von Daten nahm weiter zu: Bei mehr als drei Vierteln (76 %) der Ransomware-Angriffe verschlüsselten die Angreifer Daten ihrer Opfer. Derzeit befindet sich die Verschlüsselungsrate sogar auf dem höchsten Stand der letzten vier Jahre. Dies ist vermutlich darauf zurückzuführen, dass Bedrohungsakteure zunehmend professionell vorgehen und ihre Angriffsmethoden kontinuierlich optimieren.

Konnten Cyberkriminelle bei dem Ransomware-Angriff Ihre Unternehmensdaten verschlüsseln?



Datenverschlüsselung nach Branche

Den meisten Branchen fällt es schwer, Angriffe vor der Datenverschlüsselung zu stoppen: Mit nur einer Ausnahme kam es in allen Branchen bei mehr als zwei Dritteln der Angriffe zu einer Verschlüsselung von Daten. Am häufigsten (92%) wurden Daten im Bereich „Unternehmens- und Fachdienstleistungen" verschlüsselt.

Der Bereich IT, Technologie und Telekommunikation bildet die Ausnahme: Hier konnten Cyberkriminelle bei weniger als der Hälfte der Angriffe (47 %) Daten verschlüsseln. Auch hier zeigt sich, dass diese Branche über eine effektive Cyberabwehr verfügt und gut auf Angriffe vorbereitet ist.

Weitere Informationen finden Sie im Abschnitt „Datenverschlüsselung nach Branche" auf Seite 23.

Datendiebstahl

30 % der Angriffe, bei denen Daten verschlüsselt wurden, gingen zudem mit Datendiebstahl einher. Immer häufiger verfolgen Bedrohungsakteure diese duale Strategie, um möglichst viel Profit aus ihren Angriffen zu schlagen. So können sie mit der Drohung, gestohlene Daten zu veröffentlichen, sowohl Lösegeld erpressen als auch die Daten verkaufen. Angesichts der Häufigkeit von Datendiebstählen ist es umso wichtiger, Angriffe so früh wie möglich zu stoppen, bevor Daten exfiltriert werden können.

30 %
der Angriffe, bei denen Daten verschlüsselt wurden, gingen zudem mit Datendiebstahl einher

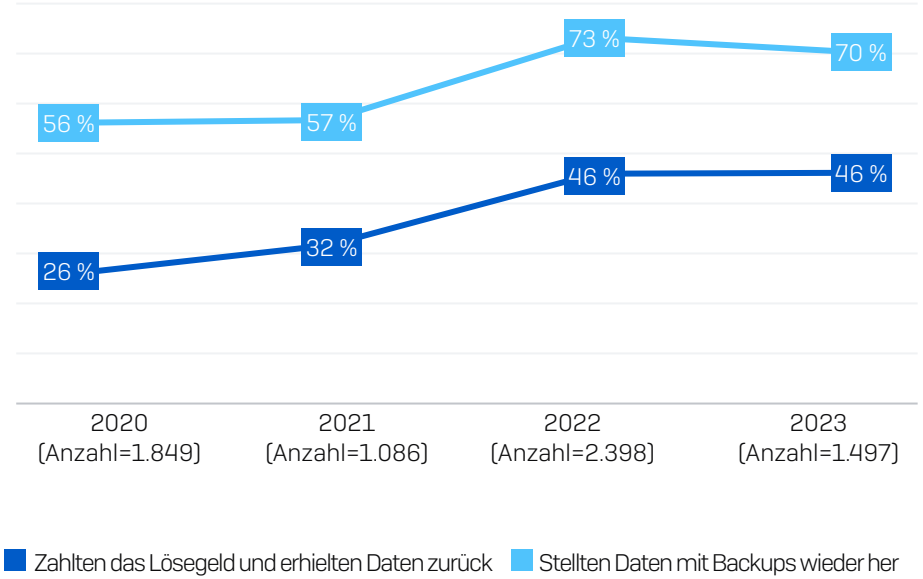
Konnten Cyberkriminelle bei dem Ransomware-Angriff Ihre Unternehmensdaten verschlüsseln? Ja; Ja und Daten wurden gestohlen. Anzahl=1.497

Datenwiederherstellung

97 % der Unternehmen, deren Daten verschlüsselt wurden, bekamen Daten zurück. Am häufigsten wurden Daten mit Backups wiederhergestellt (70 % der Vorfälle). 46 % zahlten das Lösegeld und erhielten ihre Daten zurück und 2 % setzten andere Methoden ein. Insgesamt nutzte ein Fünftel (21 %) der Befragten mehrere Methoden zur Wiederherstellung der Daten. 1 % der Unternehmen, deren Daten verschlüsselt wurden, zahlten zwar das Lösegeld, erhielten jedoch keine Daten wieder.

Stellen Daten mit Backups wieder her	Zahlten das Lösegeld und erhielten Daten zurück	Stellen Daten mit anderen Mitteln wieder her
70 %	**46 %**	**2 %**

Anlass zur Besorgnis gibt, dass im Vergleich zum Vorjahr (73 %) weniger Unternehmen Daten mit Backups wiederherstellen. Der prozentuale Anteil der Lösegeldzahlungen ist im Vergleich zum Vorjahr stabil geblieben.



Erhielt Ihr Unternehmen Daten wieder zurück? Ja, wir haben das Lösegeld gezahlt und unsere Daten zurückerhalten; Ja, wir haben Backups genutzt, um die Daten wiederherzustellen. Anzahl der erhaltenen Antworten jeweils in Klammer

Datenwiederherstellung nach Land

Insgesamt meldeten Umfrageteilnehmer in der Region EMEA eine höhere Backup-Nutzung (75 %) und weniger Lösegeldzahlungen (40 %) als Unternehmen in Nord- und Südamerika (65 %/55 %) und im asiatisch-pazifischen Raum (67 %/49 %). Auf Länderebene ist die Nutzung von Backups in Frankreich am weitesten verbreitet (87 %), dicht gefolgt von der Schweiz (84 %).

Wie wichtig Backups sind, zeigt sich dadurch, dass die beiden Länder, die am wenigsten in der Lage sind, Daten mit Backups wiederherzustellen – Italien (55 %) und Singapur (57 %) – auch die niedrigsten Datenwiederherstellungs-Raten insgesamt aufweisen (93 % bzw. 90 %). Italien meldete außerdem die höchste Bereitschaft, Lösegeld zu zahlen (56 %), gefolgt von den USA und Brasilien (jeweils 55 %).

In den meisten Fällen konnten Unternehmen, die das Lösegeld zahlten, Daten wiederherstellen. In Frankreich und Großbritannien erhielt jedoch rund eines von zehn Unternehmen, die das Lösegeld zahlten, keine Daten zurück.

Weitere Informationen finden Sie im Abschnitt „Datenwiederherstellung nach Land“ auf Seite 24.

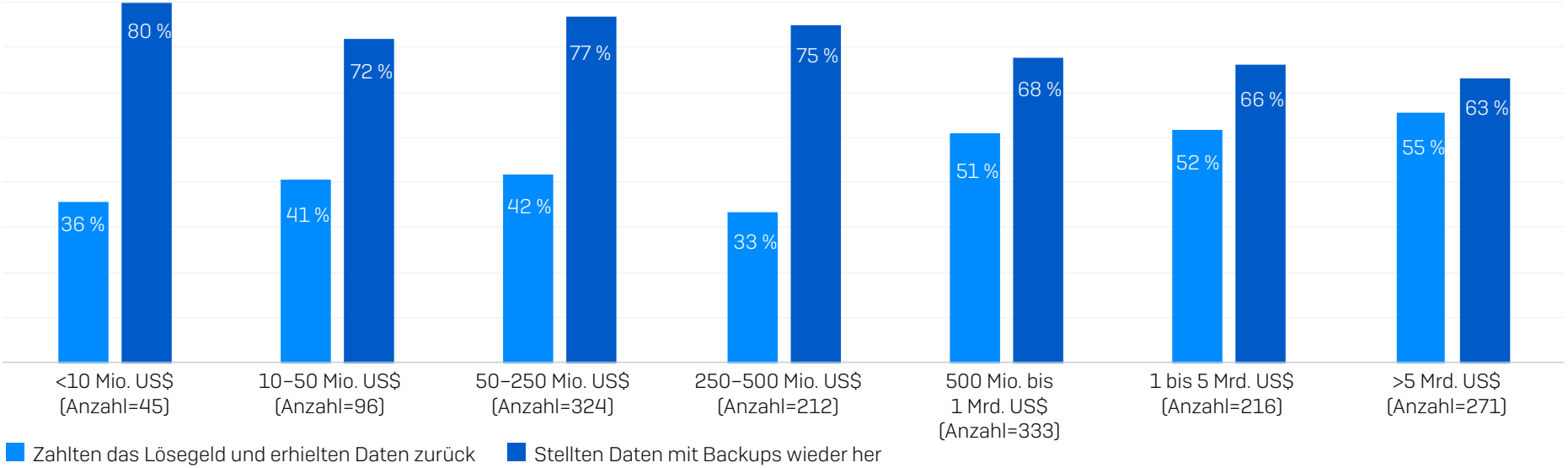
Lösegeldzahlungen und Backup-Nutzung nach Umsatz

Generell gilt: Je höher der Jahresumsatz, desto höher ist die Bereitschaft der Unternehmen, das Lösegeld zu zahlen, um ihre Daten wiederherzustellen. Gleichzeitig nimmt die Backup-Nutzung ab.

55 % der Unternehmen mit einem Jahresumsatz von mehr als 5 Mrd. US$ erhielten Daten nach Zahlung des Lösegelds zurück, 63 % verwendeten Backups. Gleichzeitig stellten 36 % der Unternehmen mit Umsätzen unter 10 Mio. US$ ihre Daten durch Zahlung des Lösegelds wieder her, während 80 % auf Backups zurückgriffen – mehr als alle anderen Umsatzgruppen.

Unternehmen im unteren Umsatzbereich verfügen nicht über die nötigen finanziellen Mittel für Lösegeldzahlungen und müssen sich daher auf die Datenwiederherstellung konzentrieren. Größere Unternehmen mit hohen Umsätzen arbeiten in der Regel mit komplexen IT-Infrastrukturen, die die zeitnahe Wiederherstellung von Daten mit Hilfe von Backups erschweren können. Außerdem sind diese Unternehmen eher in der Lage, sich „freizukaufen“.

Lösegeldzahlungen und Backup-Nutzung nach Umsatz



Erhielt Ihr Unternehmen Daten wieder zurück? Ja, wir haben das Lösegeld gezahlt und unsere Daten zurückerhalten; Ja, wir haben Backups genutzt, um die Daten wiederherzustellen. Anzahl der erhaltenen Antworten jeweils in Klammer

Auswirkung von Cyber-Versicherungen auf die Datenwiederherstellung

Bei Unternehmen mit Cyber-Versicherungsschutz war die Wahrscheinlichkeit, dass verschlüsselte Daten wiederhergestellt werden konnten, wesentlich höher als bei Unternehmen ohne entsprechende Versicherung. Dabei war die Art der Cyber-Versicherung jedoch kaum ausschlaggebend: 98 % der Unternehmen mit einer gesonderten Cyber-Versicherung und 97 % der Unternehmen mit einer Versicherung, die Cyber-Vorfälle miteinschließt, erhielten ihre Daten zurück. Im Vergleich: 84 % der Unternehmen ohne Cyber-Versicherung konnten verschlüsselte Daten wiederherstellen.

Prozentsatz der Ransomware-Opfer, die verschlüsselte Daten wiederherstellen konnten

Erhielt Ihr Unternehmen Daten wieder zurück? Anzahl=1.497 Unternehmen, die im letzten Jahr von Ransomware betroffen waren, wobei Daten verschlüsselt wurden

Diese Diskrepanz ist aller Wahrscheinlichkeit nach auf mehrere Faktoren zurückzuführen. Zum einen erhalten Unternehmen in der Regel nur dann eine Cyber-Versicherung, wenn sie über Backups und Wiederherstellungspläne verfügen. Darüber hinaus können Versicherer von Ransomware-Angriffen betroffene Unternehmen durch den Wiederherstellungsprozess führen, um die Ergebnisse zu optimieren. Außerdem sind Unternehmen mit einer Cyber-Versicherung eher bereit, das Lösegeld zu zahlen, um Daten wiederherzustellen, als Unternehmen ohne Versicherungsschutz.

Auswirkung von Versicherungen auf Lösegeldzahlungen

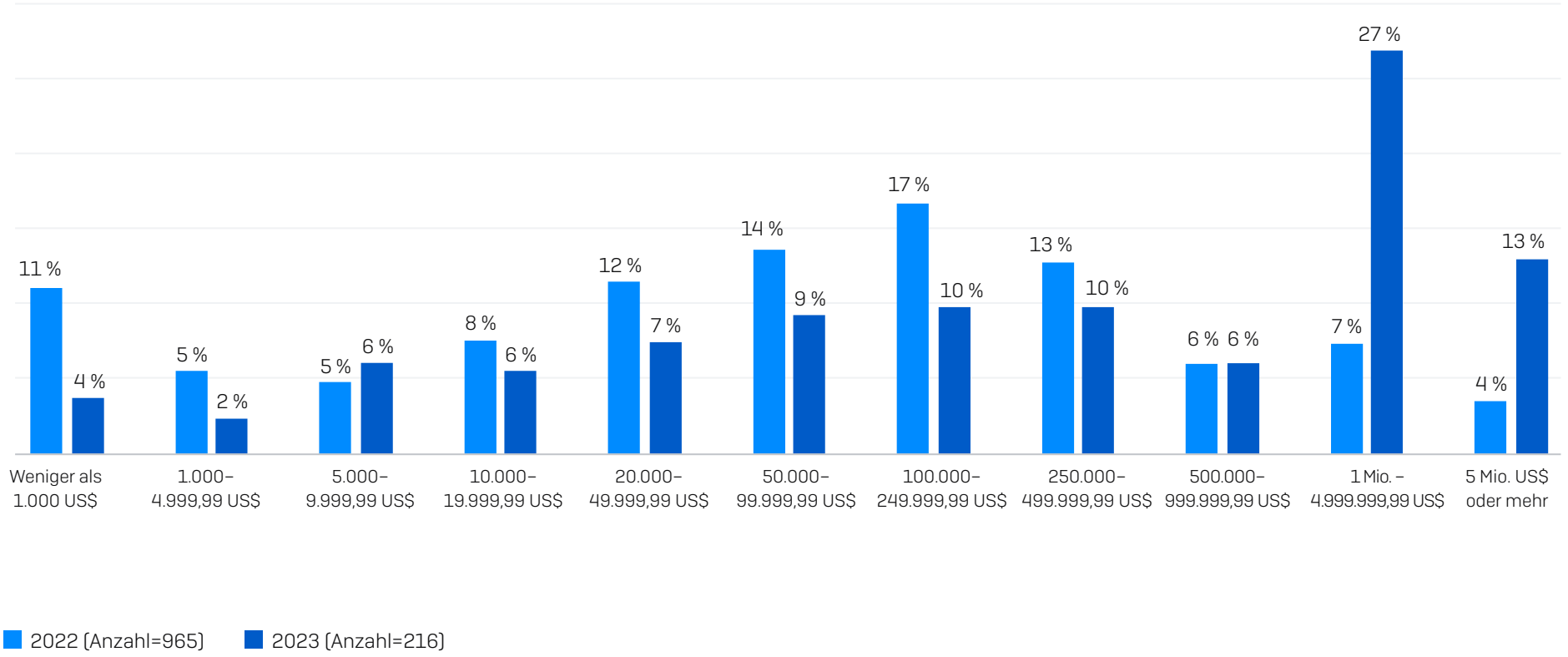
Erhielt Ihr Unternehmen Daten wieder zurück? Ja, wir haben das Lösegeld gezahlt und Daten zurückerhalten. Anzahl=1.497 Unternehmen, die im letzten Jahr von Ransomware betroffen waren, wobei Daten verschlüsselt wurden (771 gesonderte Versicherung, 658 Versicherung, die Cyber-Vorfälle miteinschließt, 67 keine Cyber-Versicherung)

Lösegeldzahlungen

Im Vergleich zum Vorjahr ist die Bereitschaft, Lösegeld zu zahlen, zwar relativ konstant geblieben, die durchschnittlich gezahlten Lösegeldsummen haben sich hingegen fast verdoppelt – von 812.380 US$ in 2022 auf 1.542.333 US$ in 2023. Im Durchschnitt zahlten die Umfrageteilnehmer im vergangenen Jahr 400.000 US$ Lösegeld.

Lösegeldsummen variierten im letzten Jahr stark. Im Vergleich zum Vorjahr zahlten jedoch mehr Unternehmen höhere Lösegelder. So meldeten 40 % der Unternehmen Zahlungen in Höhe von 1 Mio. US$ oder mehr, verglichen mit 11 % in 2022. Lediglich 34 % zahlten wiederum weniger als 100.000 US$, gegenüber 54 % im Vorjahr.

Lösegeldzahlungen: 2023 ggü. 2022



Wie viel Lösegeld wurde den Angreifern gezahlt? Ohne „Unsicher"-Angaben.

Lösegeldzahlungen nach Unternehmensumsatz

Es überrascht wohl kaum, dass die einkommensstärksten Unternehmen am häufigsten die höchsten Lösegelder zahlen, denn Cyberkriminelle passen ihre Forderungen an die Zahlungsfähigkeit ihrer Opfer an. Im Rahmen der Umfrage wurde nicht zwischen Zahlungen durch Versicherer oder das Unternehmen selbst unterschieden.

Interessanterweise ließen sich nur minimale Unterschiede zwischen den durchschnittlichen und mittleren Lösegeldzahlungen bei der Umsatzgruppe von 250 bis 500 Mio. US$ und der Gruppe von 500 Mio. bis 1 Mrd. US$ feststellen.

	50–250 MIO. US$ (ANZAHL=37)	250–500 MIO. US$ (ANZAHL=33)	500 MIO. BIS 1 MRD. US$ (ANZAHL=72)	1 – 5 MRD. US$ (ANZAHL=45)	>5 MRD. US$ (ANZAHL=21)
Durchschnittliche Lösegeldzahlung	690.996 US$	1.523.652 US$	1.466.240 US$	2.049.817 US$	2.464.339 US$
Mittlere Lösegeldzahlung	145.000 US$	428.000 US$	425.000 US$	1.000.000 US$	3.000.000 US$

Wie viel Lösegeld wurde den Angreifern gezahlt? Ohne „Unsicher"-Angaben. Aufgrund der niedrigen Antwort-Zahlen werden Unternehmen und Einrichtungen mit einem Jahresumsatz unter 50 Mio. US$ ausgeschlossen. Anzahl der erhaltenen Antworten jeweils in Klammer. Bei weniger als 30 erhaltenen Antworten sind die Daten nicht repräsentativ, können jedoch als Richtwerte dienen.

Bereinigungskosten

Lösegeldzahlungen sind nur eine Komponente der Bereinigungskosten bei Ransomware-Vorfällen. Ohne Berücksichtigung von Lösegeldzahlen beliefen sich die durchschnittlichen Bereinigungskosten bei Ransomware-Angriffen auf 1,82 Mio. US$. Damit fielen sie höher aus als im Vorjahr (1,4 Mio. US$), bewegten sich jedoch im gleichen Bereich wie in 2021 (1,85 Mio. US$).

Hinweis: In der Umfrage der Jahre 2021 und 2022 wurden bei den geschätzten Kosten auch Lösegeldzahlungen berücksichtigt, in der aktuellen Umfrage ist dies nicht der Fall. Dementsprechend ist der Vergleich zum Vorjahr nur als Indikator zu verstehen.

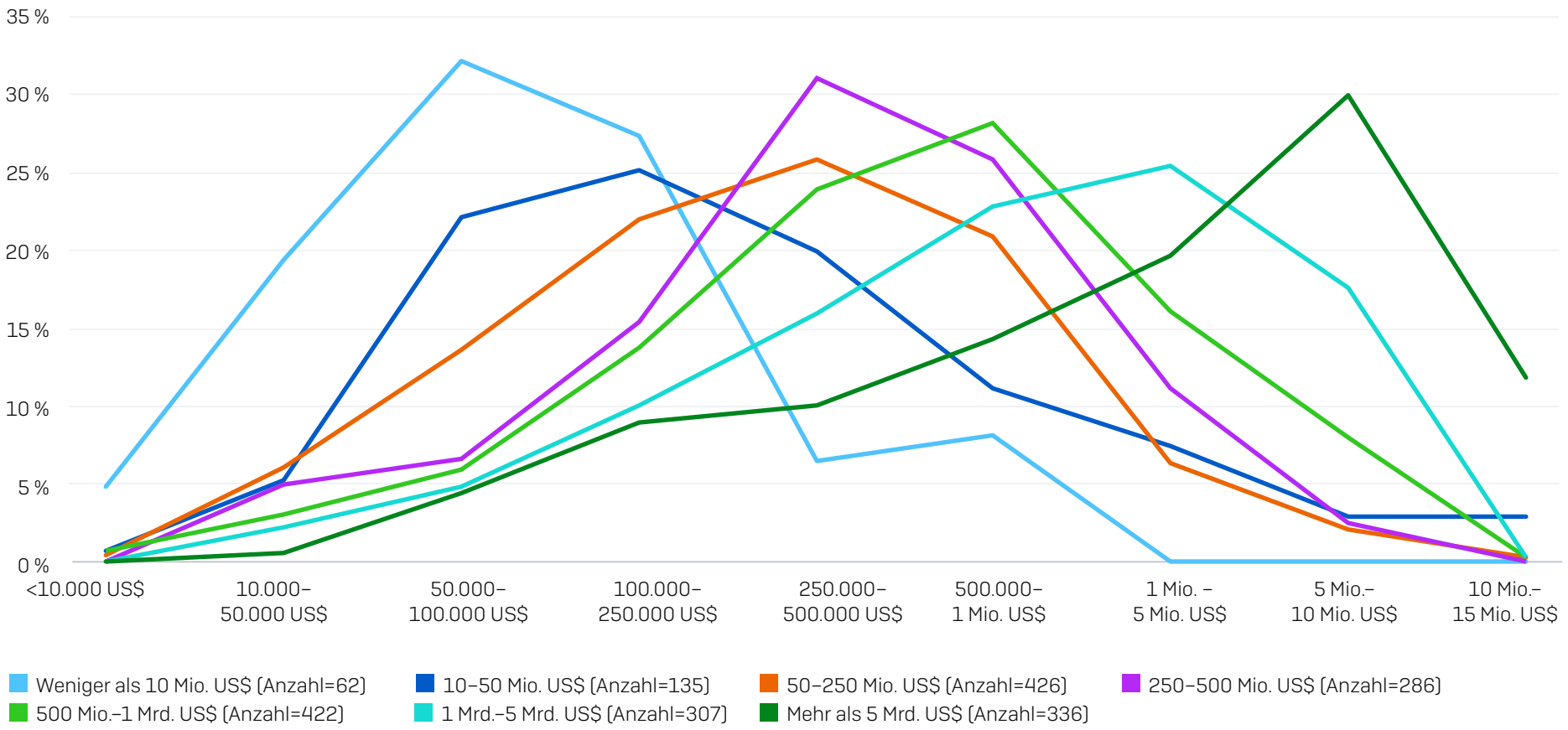
Durchschnittliche Bereinigungskosten

2021	2022	2023
1,85 Mio. US$	1,4 Mio. US$	1,82 Mio. US$

Wie hoch waren die ungefähren Kosten, die Ihrem Unternehmen durch den schwersten Ransomware-Angriff entstanden sind (unter Berücksichtigung von Ausfallzeiten, Arbeitsstunden, Geräte- und Netzwerkkosten, entgangenen Geschäftschancen usw.)? Anzahl=1.974 (2023)/3.702 (2022)/2.006 (2021). Hinweis: In 2022 und 2021 umfasste die Frage auch Lösegeldzahlungen.

Die durchschnittlichen Wiederherstellungskosten beliefen sich bei Unternehmen mit einem Jahresumsatz von weniger als 10 Mio. US$ auf 165.520 US$, bei Unternehmen mit einem Jahresumsatz von mindestens 5 Mrd. US$ auf 4.496.086 US$. Trotz der relativ weiten Spanne der Wiederherstellungskosten lässt sich ein klares Muster erkennen: Je höher der Jahresumsatz, desto höher die Wiederherstellungskosten. Dies geht auch aus dem Diagramm auf der nächsten Seite hervor.

Bereinigungskosten nach Umsatz



Wie hoch waren die ungefähren Kosten, die Ihrem Unternehmen durch den schwersten Ransomware-Angriff entstanden sind (unter Berücksichtigung von Ausfallzeiten, Arbeitsstunden, Geräte- und Netzwerkkosten, entgangenen Geschäftschancen usw.)? Anzahl der erhaltenen Antworten jeweils in Klammer

Bereinigungskosten nach Methode der Datenwiederherstellung

In jedem Fall sind Backups für die Wiederherstellung nach einem Ransomware-Angriff wesentlich kostengünstiger als Lösegeldzahlungen. Die mittleren Wiederherstellungskosten in Unternehmen, die Backups nutzten, betrugen mit 375.000 US$ nur knapp die Hälfte der Kosten in Unternehmen, die das Lösegeld zahlten (750.000 US$). Außerdem fallen die durchschnittlichen Bereinigungskosten in Unternehmen, die Backups nutzen, um fast 1 Mio. US$ niedriger aus. Die Zahlen zeigen ganz klar, dass sich eine fundierte Backup-Strategie immer auszahlt.

Zahlten das Lösegeld und erhielten Daten zurück	Stellen Daten mit Backups wieder her
750.000 US$	**375.000 US$**
Mittelwert	Mittelwert
2,6 Mio. US$	**1,62 Mio. US$**
Durchschnitt	Durchschnitt

Wie hoch waren die ungefähren Kosten, die Ihrem Unternehmen durch den schwersten Ransomware-Angriff entstanden sind (unter Berücksichtigung von Ausfallzeiten, Arbeitsstunden, Geräte- und Netzwerkkosten, entgangenen Geschäftschancen usw.)? Anzahl=694, die das Lösegeld zahlten und Daten zurückerhielten, und 1.053, die Daten mit Backups wieder herstellten.

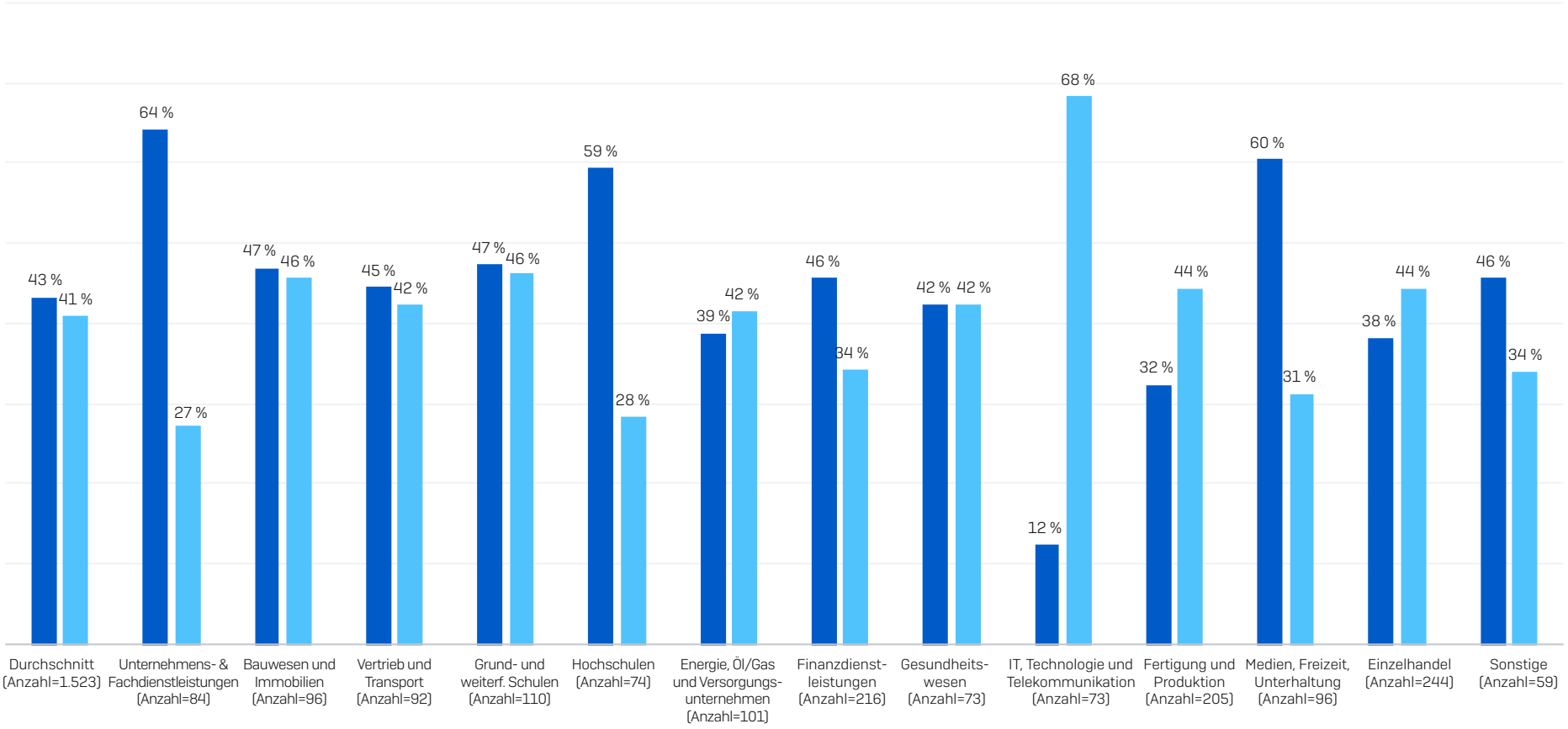
Business Impact

84 % der privatwirtschaftlichen Unternehmen, die von Ransomware betroffen waren, gaben an, dass sie dadurch Geschäftseinbußen oder Umsatzverluste verzeichneten. Der Jahresumsatz hatte einen relativ geringen Einfluss auf die Geschäftseinbußen. So meldeten Unternehmen mit Umsätzen zwischen 250 und 500 Mio. US$ die niedrigsten (79 %), Unternehmen mit Umsätzen unter 10 Mio. US$ und über 5 Mrd. US$ (88 %) die höchsten Einbußen.

Eine wesentlich größere Rolle spielte die Branchenzugehörigkeit. Grund- und weiterführende Schulen (94 %) und das Bauwesen und Immobiliengewerbe (93 %) verzeichneten am häufigsten Geschäftseinbußen bzw. Umsatzverluste, die Fertigungs- und Produktionsbranche war hiervon am wenigsten betroffen (77 %).

Die Wahrscheinlichkeit „signifikanter" Geschäftseinbußen und Umsatzverluste war in hohem Maße branchenabhängig. Unternehmens- und Fachdienstleister waren hiervon fünfmal häufiger (64 %) betroffen als die IT-, Technologie- und Telekommunikationsbranche (12 %).

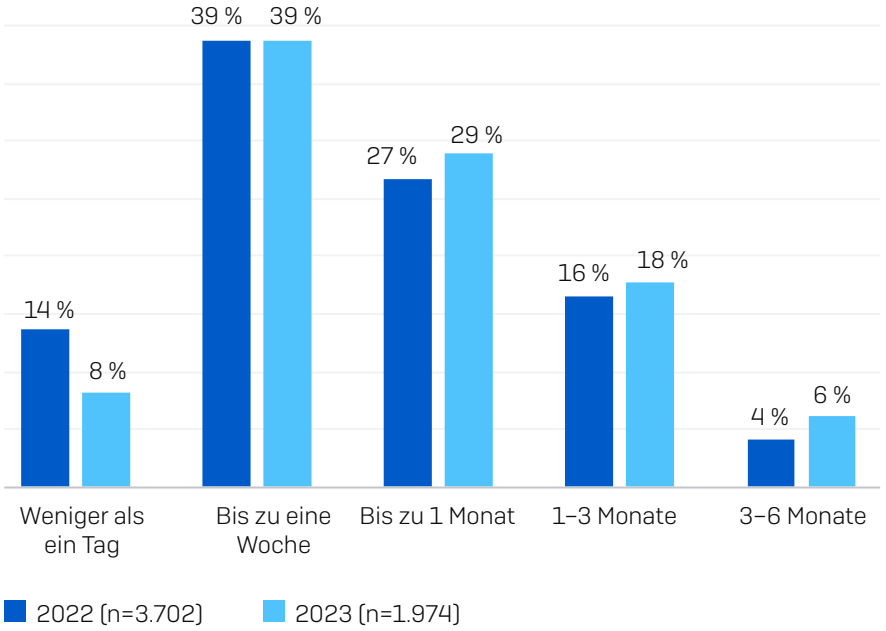
Geschäftsausfälle/Umsatzverluste nach Branche



Musste Ihr Unternehmen durch den Ransomware-Angriff Geschäftseinbußen oder Umsatzverluste hinnehmen? Ja, wir mussten signifikante Geschäftseinbußen/Umsatzverluste hinnehmen; Ja, wir mussten geringe Geschäftseinbußen/Umsatzverluste hinnehmen. Von Ransomware betroffene privatwirtschaftliche Unternehmen, Anzahl der erhaltenen Antworten jeweils in Klammer

Ausfallzeiten

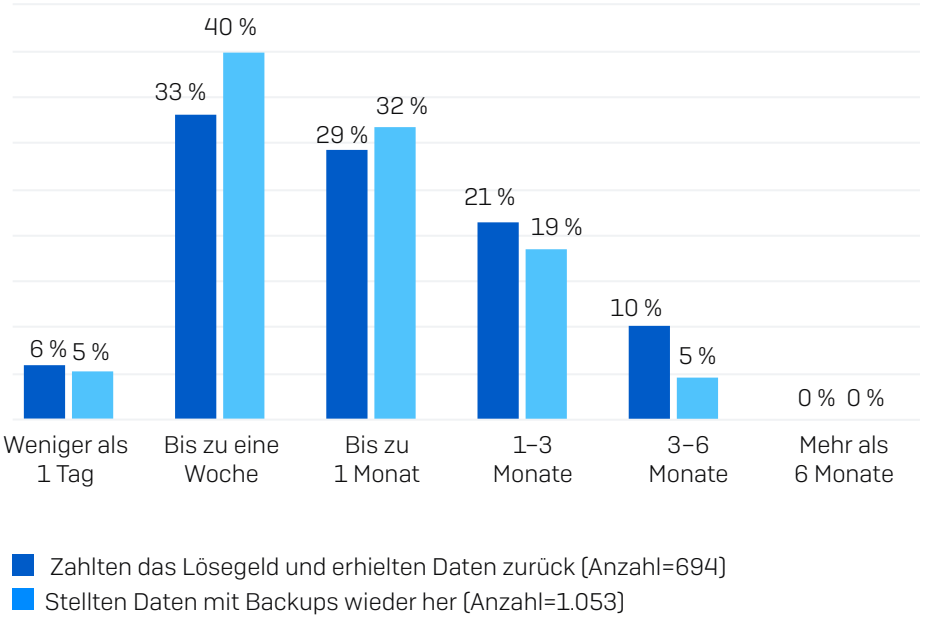
Zwar blieb die benötigte Zeit bis zur Wiederherstellung nach einem Ransomware-Angriff relativ konstant, jedoch konnten lediglich 8 % der Unternehmen die Wiederherstellung in weniger als einem Tag abschließen – ggü. 14 % in 2022.



Wie lange hat es gedauert, bis sich Ihr Unternehmen vollständig von dem Ransomware-Angriff erholt hat? Anzahl der erhaltenen Antworten jeweils in Klammer

Ausfallzeiten nach Methode der Datenwiederherstellung

Die Studie ergibt ganz klar: Unternehmen, die ihre Daten mit Backups wiederherstellen, erholen sich schneller von Angriffen als Unternehmen, die das Lösegeld zahlen. 45 % der Unternehmen, die Backups nutzten, konnten die Wiederherstellung innerhalb einer Woche abschließen. Bei Unternehmen, die das Lösegeld zahlten, waren es 39 %. Fast ein Drittel (32 %) der Umfrageteilnehmer, die das Lösegeld zahlten, benötigten mehr als einen Monat für die Wiederherstellung. In Unternehmen, die Backups nutzten, betrug der prozentuale Anteil 23 % (gerundet). Auch wenn sich die beiden Antwortoptionen nicht gegenseitig ausschließen und manche Unternehmen das Lösegeld zahlten und Backups nutzten, sind die Vorteile von Backups für die Wiederherstellung von Daten offensichtlich.



Wie lange hat es gedauert, bis sich Ihr Unternehmen vollständig von dem Ransomware-Angriff erholt hat? Unternehmen, die das Lösegeld zahlten und/oder Daten mit Backups wiederherstellten. Anzahl der erhaltenen Antworten jeweils in Klammer

Fazit

Ransomware ist für Unternehmen und Organisationen – unabhängig von Umsatz, geografischer Lage oder Branche – weiterhin eine signifikante Bedrohung. Unternehmen und Organisationen tun sich schwer, mit Cyberkriminellen mitzuhalten, die sich immer neuer Taktiken, Techniken und Prozesse bedienen. Höhere Verschlüsselungsraten sind die Folge.

Die rückläufige Nutzung von Backups zur Wiederherstellung verschlüsselter Daten gibt Anlass zur Besorgnis. Die Ergebnisse der Studie zeigen ganz klar: Eine fundierte Backup-Strategie zahlt sich immer aus, sowohl in finanzieller als auch in betrieblicher Hinsicht.

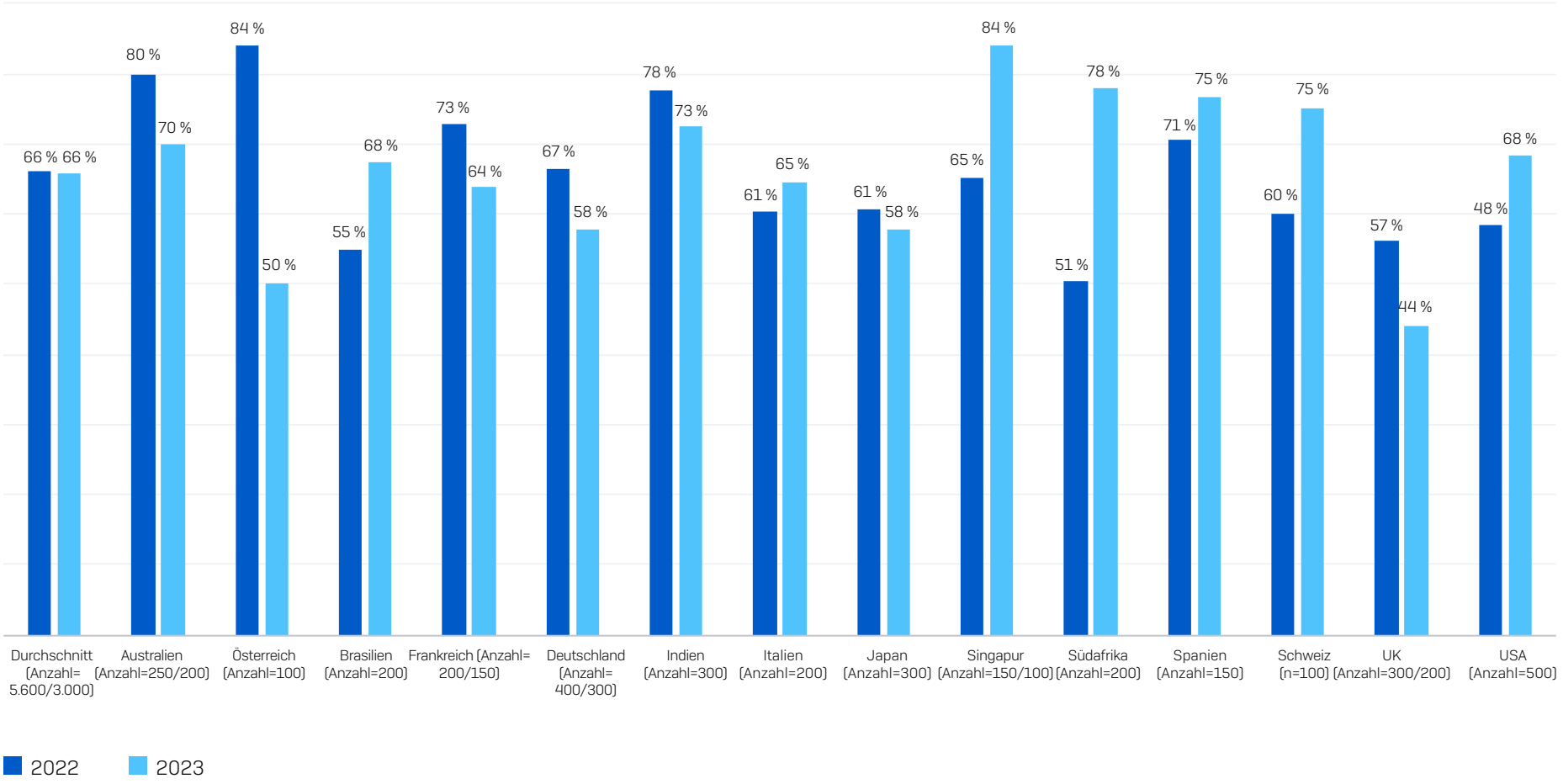
Da Ransomware-as-a-Service weiterhin auf dem Vormarsch ist, gehen wir nicht davon aus, dass das Angriffsaufkommen im kommenden Jahr zurückgehen wird. Unternehmen sollten sich auf folgende Bereiche konzentrieren:

- Verstärkung der Abwehrmaßnahmen mit:
  - Sicherheitstools, die vor den gängigsten Angriffsvektoren schützen. Hierzu zählen unter anderem Endpoint Protection mit leistungsstarken Anti-Exploit-Funktionen, die das Ausnutzen von Sicherheitslücken verhindern, sowie Zero Trust Network Access (ZTNA) zum Schutz vor kompromittierten Anmeldedaten
  - Adaptiven Technologien, die automatisch auf Angriffe reagieren. Dies verschafft IT-Teams wertvolle Zeit für die Vorfallsreaktion
  - 24/7 Bedrohungserkennung, -analyse und -reaktion durch die interne IT oder einen spezialisierten MDR-Service (Managed Detection and Response)
- Bessere Vorbereitung auf Angriffe durch regelmäßige Backups, Durchspielen der Datenwiederherstellung von Backups und kontinuierliche Aktualisierung des Incident-Response-Plans
- Diszipliniertes Einhalten von Cybersecurity-Maßnahmen, einschließlich zeitnahem Patching und einer regelmäßigen Überprüfung der Konfiguration von Sicherheitstools

Weitere Diagramme

Häufigkeit von Ransomware-Vorfällen nach Land: 2022 ggü. 2023

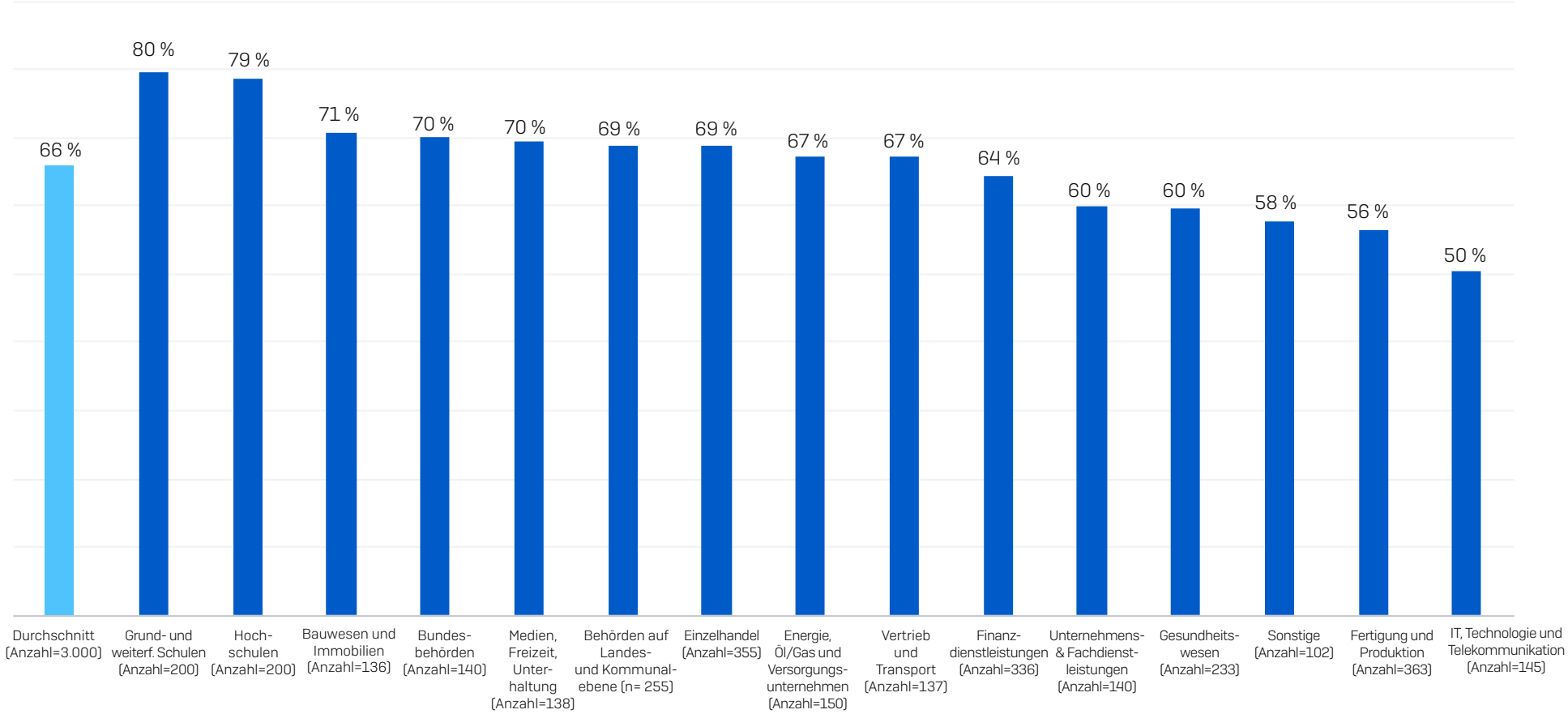
Prozentsatz der von Ransomware betroffenen Unternehmen



War Ihr Unternehmen im letzten Jahr von Ransomware betroffen? Anzahl der erhaltenen Antworten jeweils in Klammer

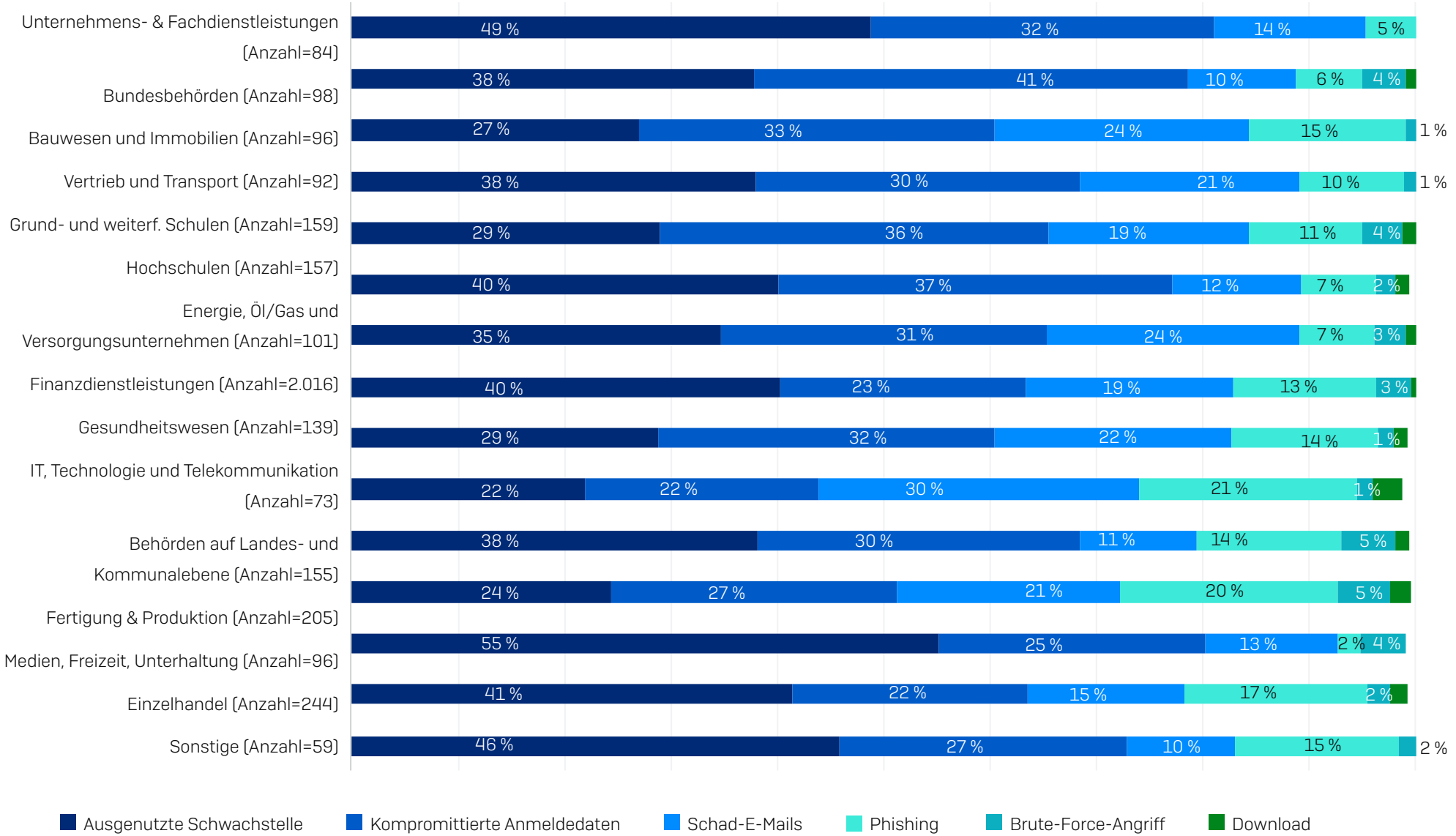
Häufigkeit von Ransomware-Vorfällen nach Branche

Prozentsatz der von Ransomware betroffenen Unternehmen



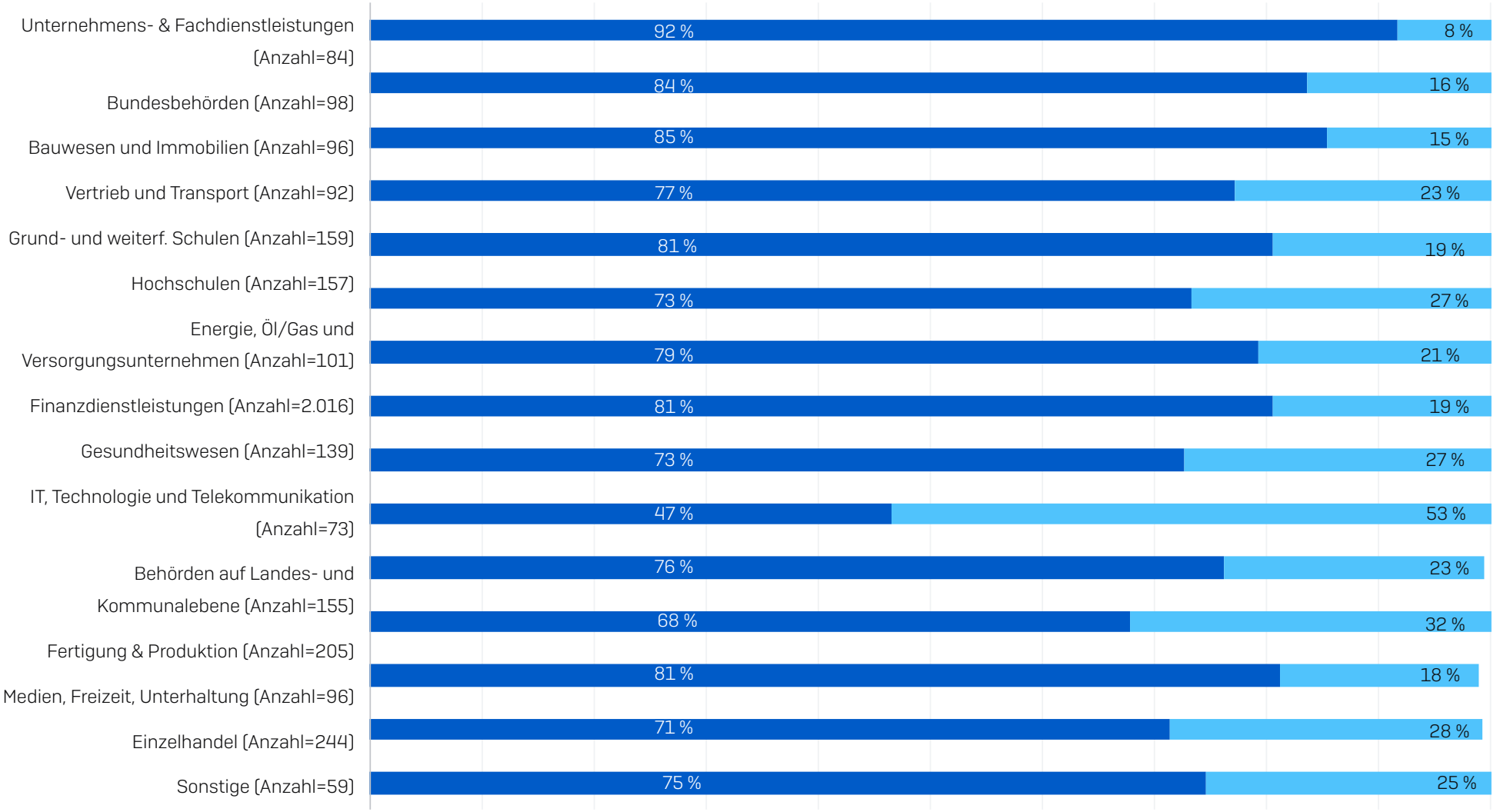
War Ihr Unternehmen im letzten Jahr von Ransomware betroffen? Anzahl der erhaltenen Antworten jeweils in Klammer

Angriffsursache nach Branche



Kennen Sie die Ursache des Ransom-Angriffs auf Ihr Unternehmen im vergangenen Jahr? Ausgewählte Antwortoptionen. Anzahl der erhaltenen Antworten jeweils in Klammer

Datenverschlüsselung nach Branche



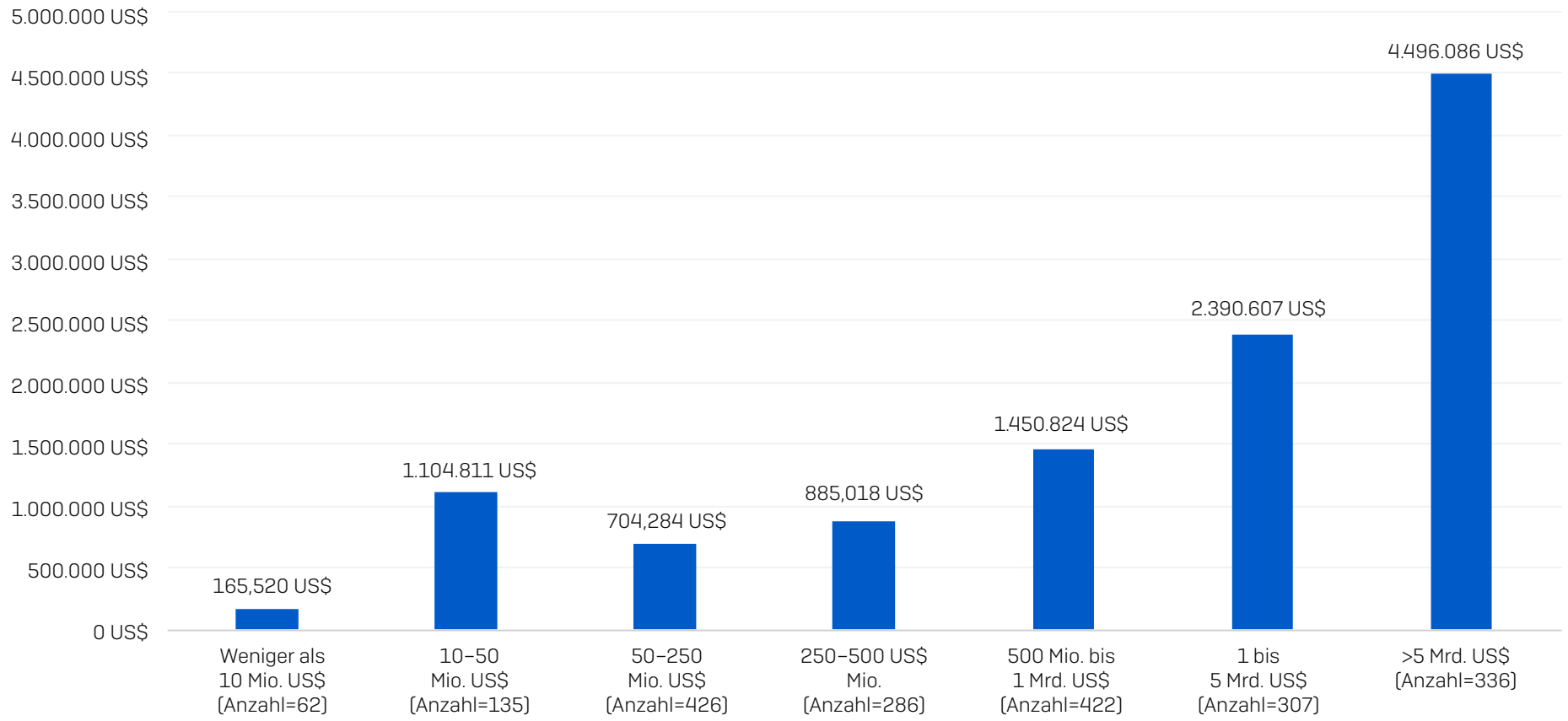
Konnten Cyberkriminelle bei dem Ransomware-Angriff Ihre Unternehmensdaten verschlüsseln? Konsolidierte Antwortoptionen. Anzahl der erhaltenen Antworten jeweils in Klammer

Datenwiederherstellung nach Land

Erhielt Ihr Unternehmen Daten wieder zurück?

	USA (ANZAHL=274)	BRASILIEN (ANZAHL=98)	DEUTSCHLAND (ANZAHL=122)	ÖSTERREICH (ANZAHL=48)	SCHWEIZ (ANZAHL=68)	UK (ANZAHL=66)	ITALIEN (ANZAHL=82)	SPANIEN (ANZAHL=93)	FRANKREICH (ANZAHL=68)	SÜDAFRIKA (ANZAHL=139)	INDIEN (ANZAHL=167)	AUSTRALIEN (ANZAHL=96)	JAPAN (ANZAHL=125)	SINGAPUR (ANZAHL=51)
Ja, wir haben das Lösegeld gezahlt und Daten zurückerhalten	54 %	55 %	44 %	42 %	38 %	44 %	54 %	29 %	22 %	45 %	43 %	53 %	52 %	53 %
Ja, wir haben die Daten mit Backups wiederhergestellt	66 %	61 %	78 %	73 %	84 %	68 %	55 %	81 %	87 %	76 %	73 %	73 %	60 %	57 %
Ja, wir haben die Daten mit anderen Mitteln wiederhergestellt	1 %	4 %	1 %	0 %	3 %	0 %	0 %	0 %	3 %	3 %	3 %	3 %	6 %	0 %
Nein, obwohl wir das Lösegeld gezahlt haben	1 %	0 %	0 %	0 %	0 %	5 %	2 %	0 %	3 %	0 %	1 %	0 %	0 %	0 %
Nein, wir haben das Lösegeld nicht gezahlt	0 %	1 %	2 %	2 %	1 %	2 %	5 %	2 %	0 %	0 %	1 %	1 %	5 %	10 %
Unsicher	0 %	0 %	2 %	0 %	0 %	0 %	0 %	0 %	0 %	0 %	0 %	0 %	0 %	0 %
Erhielten Daten über eine beliebige Methode zurück	99 %	99 %	95 %	98 %	99 %	94 %	93 %	98 %	97 %	100 %	98 %	99 %	95 %	90 %
Nutzen mehrere Methoden zur Datenwiederherstellung	22 %	21 %	27 %	17 %	26 %	18 %	16 %	12 %	12 %	24 %	20 %	29 %	22 %	20 %
Zahlten das Lösegeld	55 %	55 %	44 %	42 %	38 %	48 %	56 %	29 %	25 %	45 %	44 %	53 %	52 %	53 %
Prozentsatz der Unternehmen, die das Lösegeld zahlten und keine Daten zurückerhielten	1 %	0 %	0 %	0 %	0 %	9 %	4 %	0 %	12 %	0 %	3 %	0 %	0 %	0 %

Durchschnittliche Bereinigungskosten nach Umsatz



Wie hoch waren die ungefähren Kosten, die Ihrem Unternehmen durch den schwersten Ransomware-Angriff entstanden sind (unter Berücksichtigung von Ausfallzeiten, Arbeitsstunden, Geräte- und Netzwerkkosten, entgangenen Geschäftschancen usw.)? Anzahl der erhaltenen Antworten jeweils in Klammer.

Untersuchungsmethode

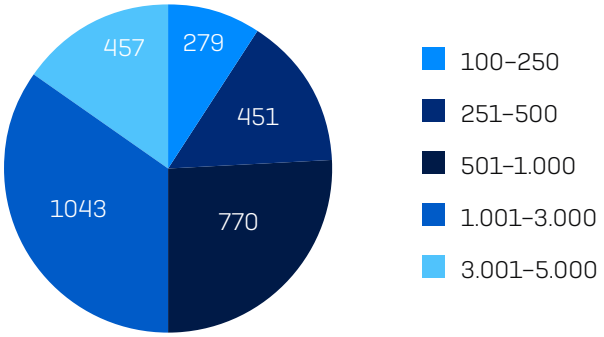
Sophos hat eine unabhängige Befragung von 3.000 IT-/Cybersecurity-Entscheidern in Auftrag gegeben, die von Januar bis März 2023 durchgeführt wurde. Die Umfrageteilnehmer stammten aus 14 Ländern in Nord- und Südamerika, EMEA und Asien-Pazifik.

An der Umfrage nahmen Unternehmen und Einrichtungen mit 100 bis 5.000 Mitarbeitern teil (50 % mit 100–1.000 und 50 % mit 1.001–5.000 Mitarbeitern). An der Studie nahmen Unternehmen mit einem Jahresumsatz von weniger als 10 Mio. US$ bis zu mehr als 5 Mrd. US$ teil.

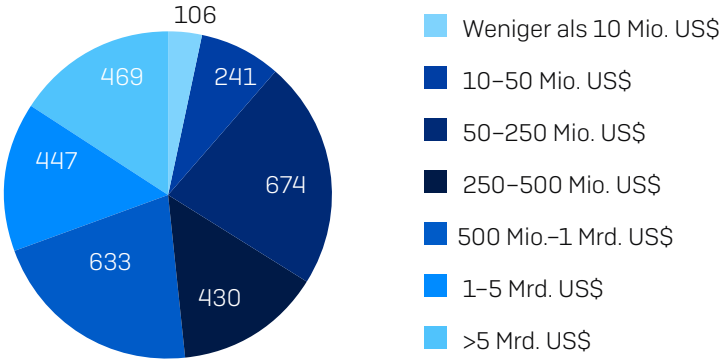
Befragte nach Land

LAND	ANZAHL DER BEFRAGTEN	LAND	ANZAHL DER BEFRAGTEN
Vereinigte Staaten	500	Vereinigtes Königreich	200
Deutschland	300	Südafrika	200
Indien	300	Frankreich	150
Japan	300	Spanien	150
Australien	200	Österreich	100
Brasilien	200	Singapur	100
Italien	200	Schweiz	100

Befragte nach Unternehmensgröße (Mitarbeiterzahl)



Befragte nach Unternehmensgröße (Jahresumsatz)



Sophos bietet branchenführende Cybersecurity-Lösungen für Unternehmen jeder Größe und schützt Kunden in Echtzeit vor komplexen Bedrohungen wie Malware, Ransomware und Phishing. Bewährte Next-Gen-Funktionen mit der Power von Machine Learning und künstlicher Intelligenz sichern Unternehmensdaten effektiv.

2023-05-05 (WP-DD)

SOPHOS