SOPHOS

Ransomware-Report 2024

Ergebnisse einer unabhängigen Befragung von 5.000 IT-/Cybersecurity-Entscheidern aus 14 Ländern. Durchgeführt im Zeitraum Januar und Februar 2024.

Sophos-Whitepaper, April 2024

Einführung

Die fünfte jährliche Studie von Sophos zu den Erfahrungen mit Ransomware von Unternehmen und Organisationen in aller Welt untersucht den gesamten Angriffsprozess – von der Ursache über den Schweregrad bis hin zu den finanziellen Auswirkungen und den Ausfallzeiten. Neue Erkenntnisse in Kombination mit den Ergebnissen unserer früheren Studien zeigen die aktuellen Herausforderungen, mit denen Unternehmen heute konfrontiert sind. Darüber hinaus erfahren Sie mehr über die Folgen von Ransomware im Verlauf der letzten fünf Jahre.

Der diesjährige Report nimmt auch völlig neue Aspekte unter die Lupe, wie etwa Lösegeldforderungen im Vergleich zu Lösegeldzahlungen, und beschäftigt sich eingehend mit dem Zusammenhang zwischen Umsatz eines Unternehmens und den Auswirkungen eines Ransomware-Angriffs. Außerdem wird zum ersten Mal die Rolle der Strafverfolgungsbehörden bei der Bereinigung von Ransomware beleuchtet.

Hinweis zu den Datumsangaben im Report

Um einen einfachen Vergleich der Daten unserer jährlichen Umfragen zu ermöglichen, benennen wir den Report nach dem Jahr, in dem die Studie durchgeführt wurde, in diesem Fall 2024. Da sich die Antworten der Befragten auf ihre Erfahrungen im vergangenen Jahr beziehen, fanden viele der erwähnten Angriffe bereits im Jahr 2023 statt.

Über die Studie

Der Report basiert auf den Ergebnissen einer von Sophos in Auftrag gegebenen unabhängigen Befragung von 5.000 IT-/Cybersecurity-Entscheidern aus 14 Ländern in Nord- und Südamerika, EMEA und Asien-Pazifik. An der Umfrage nahmen Unternehmen und Organisationen mit 100 bis 5.000 Mitarbeitern teil. Die Befragung wurde vom Marktforschungsinstitut Vanson Bourne im Januar und Februar 2024 durchgeführt. 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 in zwei Unterbereiche unterteilt:
1. Grund- und weiterführende Schulen
2. Hochschulen.

Häufigkeit von Ransomware-Angriffen

59 % der Unternehmen waren im vergangenen Jahr von Ransomware betroffen, ein geringfügiger, aber erfreulicher Rückgang ggü. den 66 %, die in den beiden vorangegangenen Jahren gemeldet worden waren. Zwar stimmen diese Zahlen durchaus positiv. Da jedoch nach wie vor mehr als die Hälfte der Unternehmen Opfer eines Angriffs war, ist weiterhin Vorsicht geboten.

2020	2021	2022	2023	2024
51 %	37 %	66 %	66 %	59 %

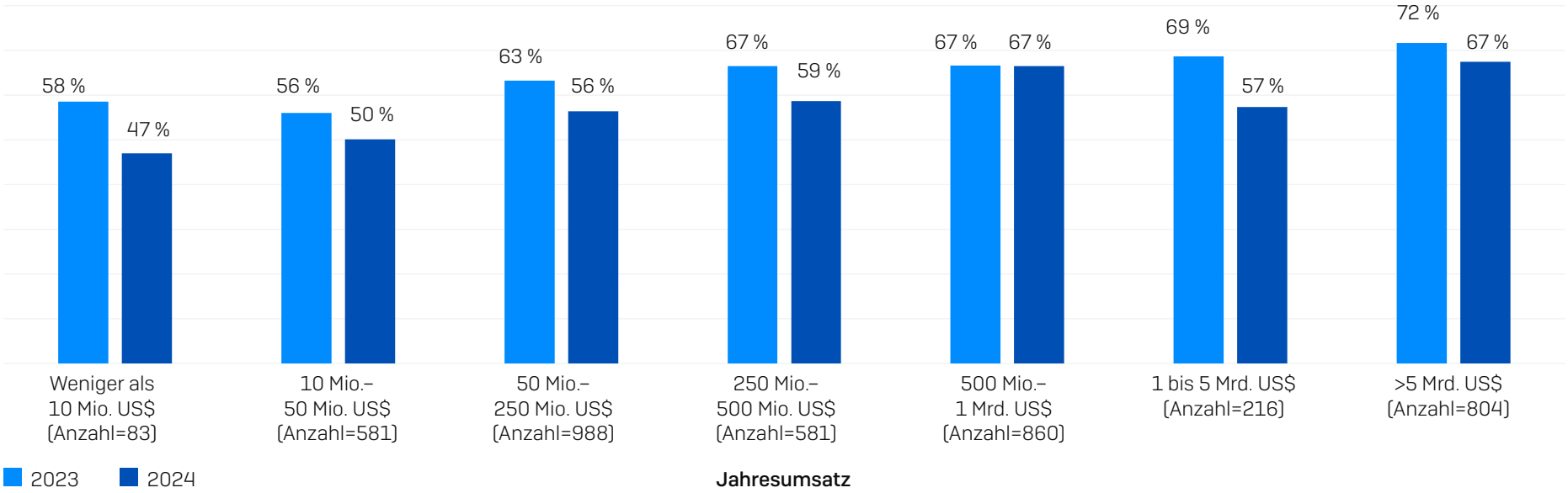
War Ihr Unternehmen/Ihre Organisation im letzten Jahr von Ransomware betroffen?
Ja. Anzahl=5.000 (2024), 3.000 (2023), 5.600 (2022), 5.400 (2021), 5.000 (2020).

Angriffe nach Umsatz

Erfreulicherweise verzeichneten alle Umsatzsegmente im letzten Jahr rückläufige Ransomware-Angriffsraten (bei Unternehmen mit einem Umsatz von 500 Mio. bis 1 Mrd. US$ belief sich der Rückgang jedoch auf weniger als 1 Prozent).

Die Angriffswahrscheinlichkeit stieg im Allgemeinen mit dem Umsatz, wobei Unternehmen mit einem Umsatz von mehr als 5 Mrd. US$ die höchste Angriffsrate (67 %) meldeten. Aber auch kleine Unternehmen und Organisationen (mit Umsätzen unter 10 Mio. US$) blieben nicht verschont: Knapp die Hälfte (47 %) war im letzten Jahr von Ransomware betroffen. Während zahlreiche Ransomware-Angriffe von professionell agierenden, gut finanzierten Banden ausgeführt werden, nimmt die Verwendung von einfacher, billiger Ransomware durch weniger versierte Bedrohungsakteure zu.

Prozentsatz der Unternehmen, die im letzten Jahr von Ransomware betroffen waren



Wurde Ihr Unternehmen/Ihre Organisation im letzten Jahr von Ransomware getroffen? Ja. Anzahl=5.000 (2024), 3.000 (2023). Anzahl der in 2024 erhaltenen Antworten nach Segment jeweils in Klammer.

Angriffe nach Branche

Mit einigen wenigen Ausnahmen bewegte sich das Angriffsaufkommen im Branchenvergleich im Wesentlichen auf dem gleichen Niveau: In 11 der 15 untersuchten Branchen waren zwischen 60 und 68 % der Unternehmen betroffen. Die klaren Gewinner der diesjährigen Umfrage sind *Behörden auf Landes- und Kommunalebene* (34 %) und der *Einzelhandel* (45 %): In beiden Bereichen verzeichneten weniger als die Hälfte der befragten Unternehmen und Organisationen Angriffe.

Interessanterweise ließen sich signifikante Unterschiede beim Angriffsaufkommen in *Bundesbehörden* (höchste Angriffsrate aller Branchen/Bereiche mit 68 %) und *Behörden auf Landes- und Kommunalebene* (34 %) feststellen. Dennoch lag die Angriffsrate bei *Bundesbehörden* in Einklang mit dem allgemeinen Rückgang der Angriffe unter den 70 % von 2023.

Die Diskrepanz in diesem Bereich lässt sich auf mehrere mögliche Gründe zurückführen. Das vergangene Jahr war vielerorts von politischen Konflikten geprägt. Möglicherweise wurden Regierungen daher häufiger Opfer politisch motivierter Angriffe. Womöglich spiegeln die Zahlen auch die Bemühungen von Behörden auf Landes- und Kommunalebene im letzten Jahr wider, ihre Cyberabwehr zu stärken. Vielleicht passten Cyberkriminelle ihre Strategien jedoch auch an und reagierten damit auf die begrenzten Mittel zur Finanzierung des Lösegelds in Behörden auf Landes- und Kommunalebene.

Außerdem zeichneten sich im Branchenvergleich im letzten Jahr unter anderem folgende Änderungen ab:

- Rückgang der höchsten individuellen Angriffsrate von 80 % (*Grund- und weiterführende Schulen*) auf 69 % (*Bundesbehörden*)
- Der Bildungssektor meldete nicht mehr die beiden höchsten Angriffsraten. 66 % der Umfrageteilnehmer aus dem *Hochschulbereich* und 63 % aus *Grund- und weiterführenden Schulen* waren Opfer von Angriffen. Letztes Jahr lag der prozentuale Anteil noch bei 79 % bzw. 80 %
- Das *Gesundheitswesen* zählte zu den fünf Bereichen mit einem rückläufigen Angriffsaufkommen und verzeichnete einen Rückgang von 60 % auf 67 %
- Der Bereich *IT, Technologie und Telekommunikation* meldete mit 55 % nicht mehr das niedrigste Angriffsaufkommen. 2023 lag die Zahl noch bei 50 %

Im Anhang finden Sie eine detaillierte Aufschlüsselung der Ransomware-Angriffsrate nach Branche.

Angriffe nach Land

Frankreich meldete 2024 die höchste Rate an Ransomware-Angriffen. 74 % der Befragten gaben an, dass sie im letzten Jahr betroffen waren, gefolgt von Südafrika (69 %) und Italien (68 %). Die niedrigsten Angriffsraten verzeichneten hingegen Brasilien (44 %), Japan (51 %) und Australien (54 %).

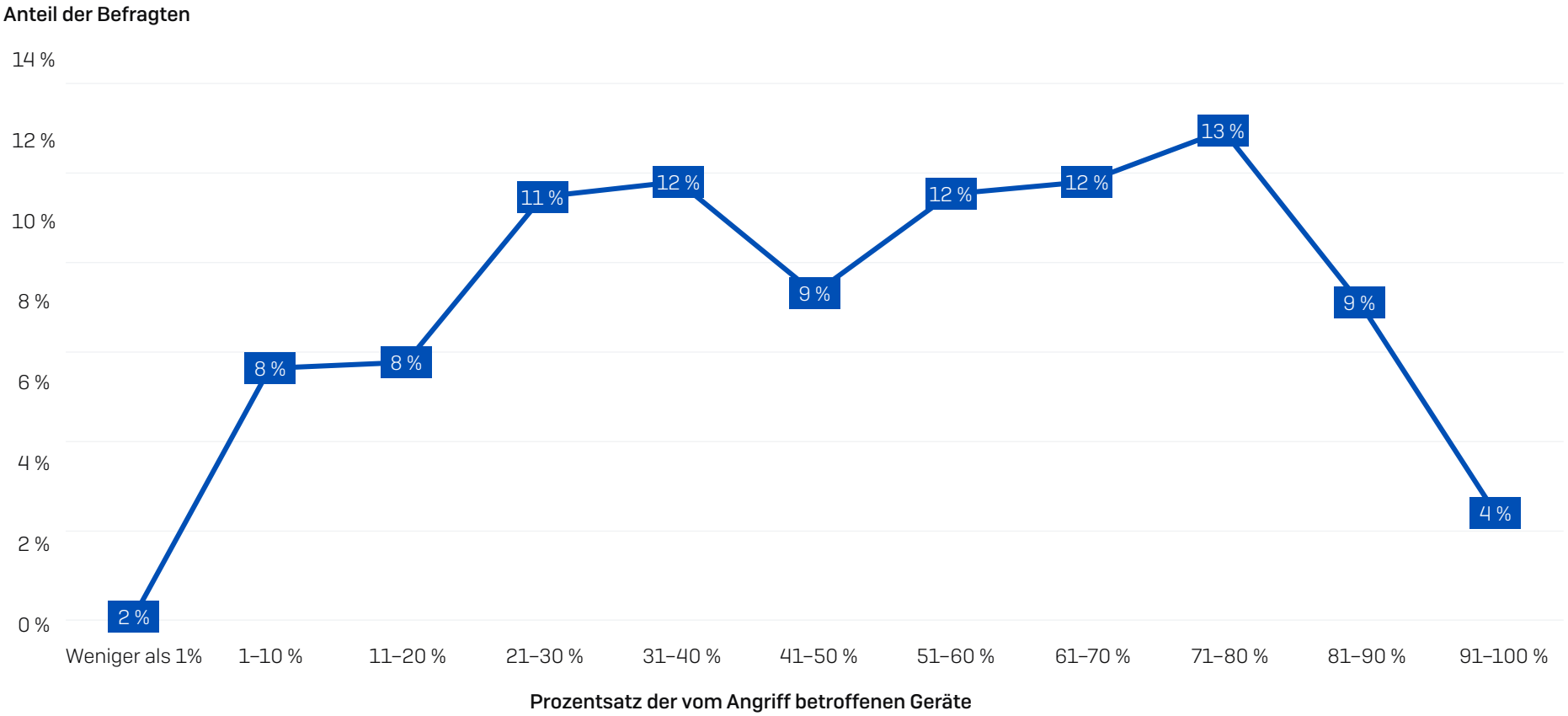
Insgesamt meldeten neun Länder eine niedrigere Angriffsrate als im Jahr 2023. Die fünf Länder, die eine höhere Angriffsrate als im Jahr 2023 angaben, liegen alle in Europa: Österreich, Frankreich, Deutschland, Italien und Großbritannien (der Anstieg in Deutschland betrug weniger als 1 %). Möglicherweise wurden europäische Unternehmen und Organisationen im vergangenen Jahr verstärkt ins Visier genommen. Vielleicht konnten sie auch weniger gut mit dem sich verändernden Verhalten der Angreifer Schritt halten.

Im Anhang finden Sie eine detaillierte Aufschlüsselung der Ransomware-Angriffsrate nach Ländern.

Prozentsatz der betroffenen Computer

Im Durchschnitt war nur knapp die Hälfte (49 %) der Computer eines Unternehmens oder einer Organisation von einem Ransomware-Angriff betroffen. Nur in äußerst seltenen Fällen wurde die gesamte Umgebung verschlüsselt. Lediglich 4 % der Unternehmen/Organisationen gaben an, dass 91 % oder mehr ihrer Geräte kompromittiert waren. Zwar betrafen auch vereinzelte Angriffe lediglich eine Handvoll Geräte, doch auch dies war eine absolute Ausnahme: Nur 2 % der betroffenen Unternehmen/Organisationen gaben an, dass weniger als 1 % ihrer Geräte kompromittiert wurden.

Prozentsatz der vom Angriff betroffenen Geräte



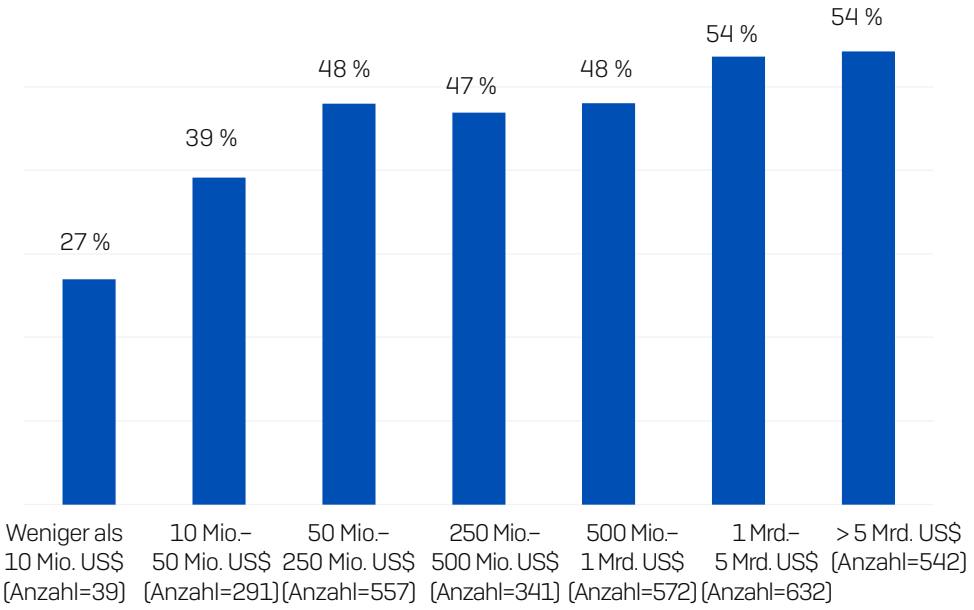
Wie viel Prozent der Computer in Ihrem Unternehmen waren im letzten Jahr von Ransomware betroffen? Anzahl=2.974 Unternehmen, die Opfer von Ransomware waren.

Prozentsatz der betroffenen Computer nach Umsatz

Während die Verteilung über alle Befragten hinweg breit gefächert war, ließen sich bei den betroffenen Geräten erhebliche Unterschiede sowohl nach Unternehmensgröße als auch nach Branche feststellen.

Mit zunehmendem Umsatz stieg auch der Anteil der kompromittierten Computer. Die kleinsten Unternehmen und Organisationen (Umsätze von weniger als 10 Mio. US$) meldeten nur halb so viele betroffene Geräte wie Unternehmen mit einem Umsatz von 1 Mrd. US$ oder mehr (27 % ggü. 54 %).

Dieses Ergebnis lässt sich wahrscheinlich auf mehrere Faktoren zurückführen. Kleinere Unternehmen verwalten alle Geräte seltener zentral, sodass sich Angriffe nicht so leicht über den gesamten Bestand ausbreiten können. Außerdem nutzen die meisten kleinen Unternehmen und Startups SaaS-Plattformen, die mit einem geringeren Risiko eines Geschäftsausfalls durch Bedrohungen wie Ransomware einhergehen.



Jahresumsatz

Wie viel Prozent der Computer in Ihrem Unternehmen waren im letzten Jahr von Ransomware betroffen?
Anzahl=2.974 Unternehmen, die Opfer von Ransomware waren.

Prozentsatz der betroffenen Computer nach Branche

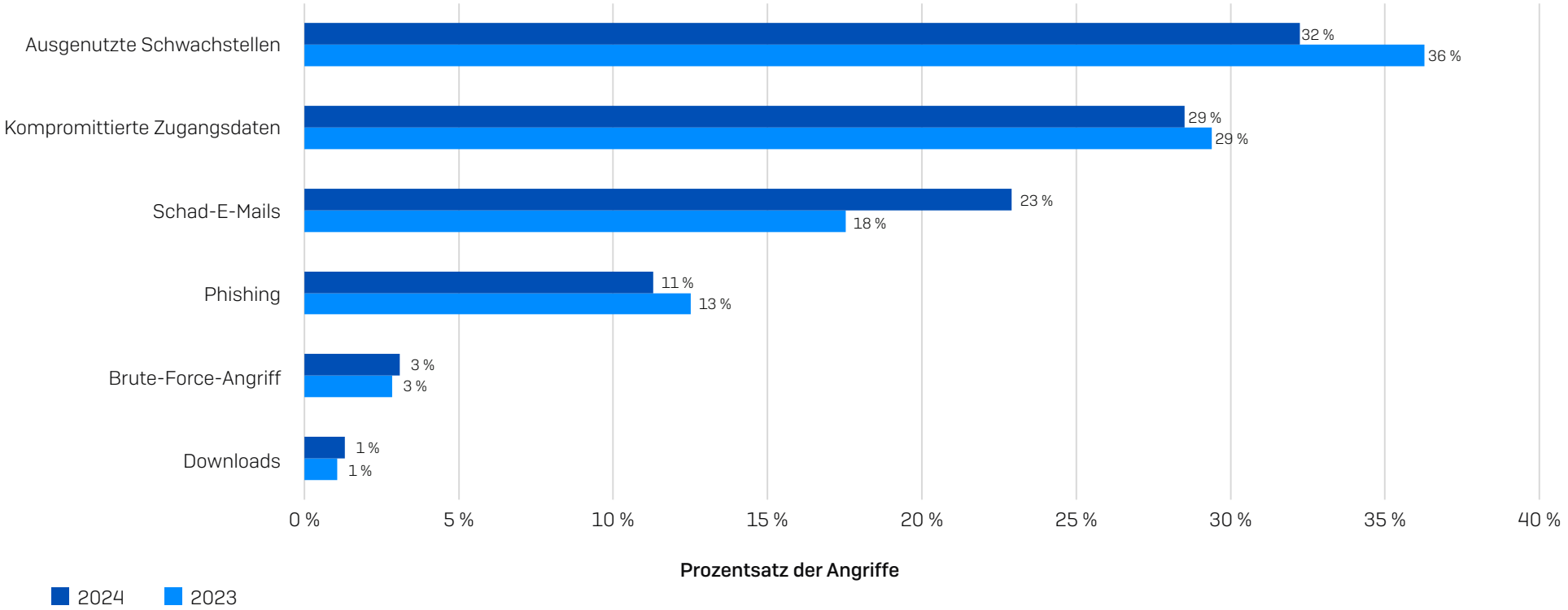
Prozentual verzeichnete der Bereich *IT, Technologie und Telekommunikation* (33 %) die wenigsten betroffenen Geräte. Dies spiegelt die in dieser Branche üblicherweise sehr starke Cyberabwehr wider. Mit 62 % waren die Auswirkungen des Angriffs in *Energie, Öl/Gas und Versorgungsunternehmen* in weiten Teilen der Organisation zu spüren, gefolgt vom *Gesundheitswesen* (58 %). Beide Branchen nutzen mehr veraltete Technologien und Infrastrukturkontrollen als die meisten anderen Bereiche. So ist es für Unternehmen in diesen Bereichen wahrscheinlich schwerer, Geräte zu sichern, laterale Bewegungen einzuschränken und die Ausbreitung von Angriffen zu verhindern.

Im Anhang finden Sie eine detaillierte Aufschlüsselung der betroffenen Computer nach Branche.

Ursachen von Ransomware-Angriffen

99 % der von Ransomware betroffenen Unternehmen und Organisationen konnten die Angriffsursache ermitteln: Im zweiten Jahr in Folge waren ausgenutzte Schwachstellen der Hauptangriffsvektor. Insgesamt änderte sich die Reihenfolge im Vergleich zu unserer Studie aus dem Jahr 2023 kaum.

34 % der Befragten führten E-Mail-basierte Angriffsvektoren als Hauptursache an, wobei etwa doppelt so viele von einer Schad-E-Mail (d. h. einer Nachricht mit einem bösartigen Link oder Anhang, der Malware herunterlädt) wie von Phishing (d. h. einer Nachricht, die den Leser zur Preisgabe von Informationen verleiten soll) ausgingen. Phishing dient in der Regel dem Zweck, Zugangsdaten zu stehlen. Somit ist es gewissermaßen der erste Schritt eines Angriffs mit kompromittierten Zugangsdaten.



Kennen Sie die Ursache des Ransomware-Angriffs auf Ihr Unternehmen im vergangenen Jahr? Ja. Anzahl=2.974 Unternehmen/Organisationen, die von Ransomware betroffen waren.

Von ausgenutzten Schwachstellen ausgehende Angriffe

Ransomware-Angriffe haben immer negative Auswirkungen auf die Opfer. Manche Angriffe sind jedoch besonders verheerend. Betroffene Unternehmen, bei denen ungepatchte Schwachstellen als Einfallstor genutzt wurden, meldeten erheblich schwerwiegendere Folgen als solche, bei denen der Angriff durch kompromittierte Zugangsdaten ausgelöst wurde. Zudem zeichneten sich folgende Tendenzen ab:

- Backups wurden kompromittiert (Erfolgsquote 75 % ggü. 54 % bei kompromittierten Zugangsdaten)
- Daten wurden verschlüsselt (Verschlüsselungsrate 67 % ggü. 43 % bei kompromittierten Zugangsdaten)
- Unternehmen zahlten das Lösegeld (71 % Zahlungsrate ggü. 45 % bei kompromittierten Zugangsdaten)
- Unternehmen trugen die Lösegeldkosten selbst (31 % ggü. 2 % bei kompromittierten Zugangsdaten)

Sie berichteten auch über:

- 4 Mal höhere Bereinigungskosten nach einem Angriff (3 Mio. US$ ggü. 750.000 US$ bei kompromittierten Zugangsdaten)
- Längere Ausfallzeiten (45 % benötigen mehr als einen Monat für die Wiederherstellung ggü. 37 % bei kompromittierten Zugangsdaten)

Umfassende Informationen zu diesem Thema erhalten Sie unter Ungepatchte Sicherheitslücken: Der gefährlichste Angriffsvektor für Ransomware.

Ursache nach Branche

Lücken in der Cyberabwehr sind in einigen Branchen stärker ausgeprägt als in anderen – Angreifer nutzen dies aus. Daher variiert die Ursache für Ransomware-Angriffe je nach Branche erheblich:

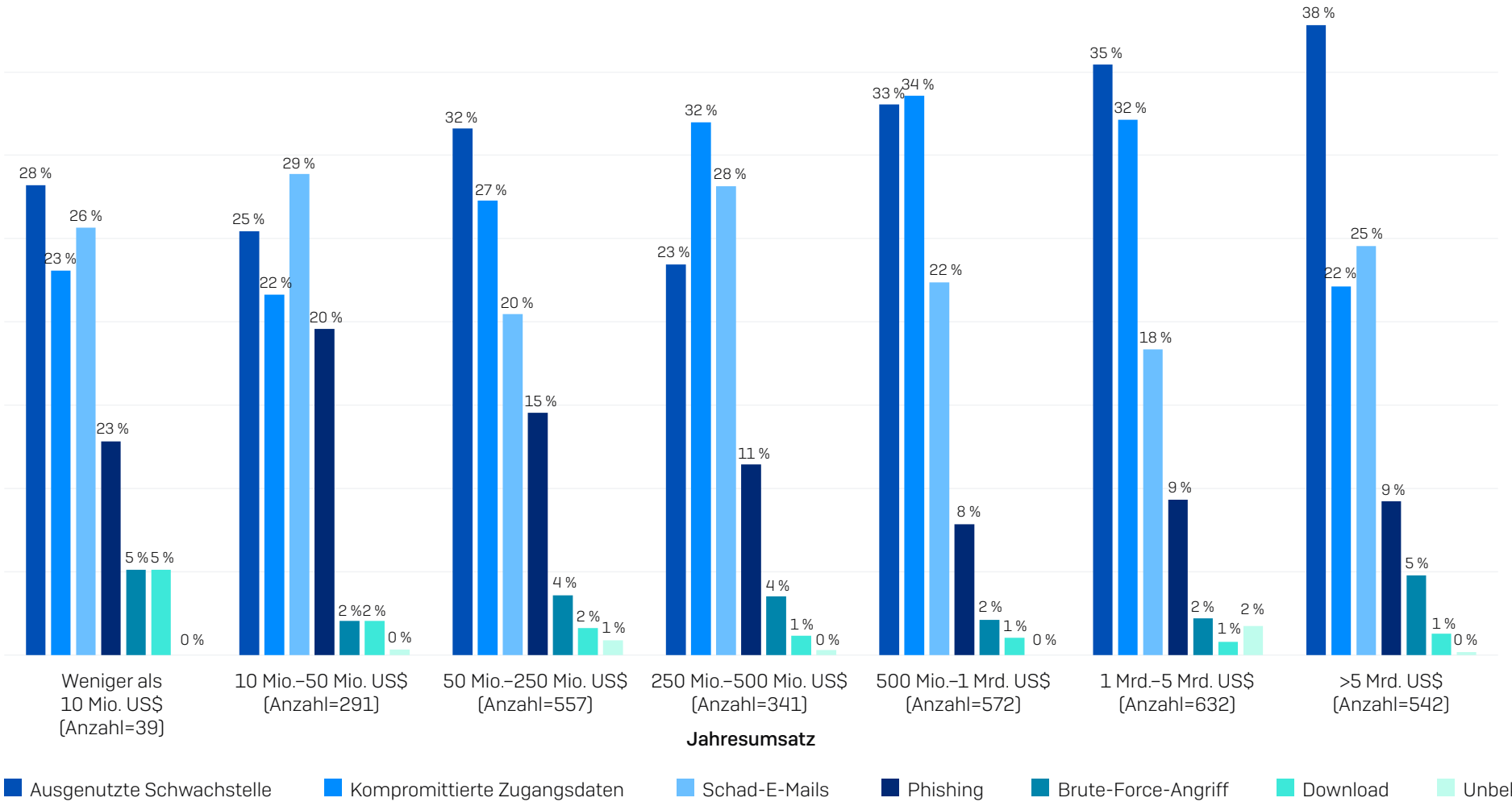
- *Energie, Öl/Gas und Versorgungsunternehmen* fielen am ehesten der Ausnutzung ungepatchter Schwachstellen zum Opfer: Fast die Hälfte (49 %) der Angriffe gingen von diesem Angriffsvektor aus. Unternehmen dieser Branche nutzen in der Regel häufiger ältere Technologien, die anfälliger für Schwachstellen sind. Zudem sind für veraltete und nicht mehr unterstützte Lösungen möglicherweise keine Patches verfügbar
- Regierungsbehörden sind besonders anfällig für Angriffe, die mit dem Missbrauch kompromittierter Zugangsdaten beginnen: 49 % (*Behörden auf Landes- und Kommunalebene*) und 47 % (*Bundesbehörden*) der Angriffe ließen sich auf gestohlene Zugangsdaten zurückführen
- 7 % der Ransomware-Vorfälle in der *IT, Technologie und Telekommunikation* und im *Einzelhandel* begannen mit einem Brute-Force-Angriff. Womöglich zwingt die geringere Gefährdung durch ungepatchte Schwachstellen und kompromittierte Zugangsdaten die Angreifer dazu, auf andere Methoden zurückzugreifen

Im Anhang finden Sie eine detaillierte Aufschlüsselung der Angriffsursache nach Branche.

Ursache nach Umsatz

Im Allgemeinen waren größere Unternehmen häufiger von Angriffen betroffen, die von ungepatchten Schwachstellen ausgingen, wobei das Umsatzsegment über 5 Mrd. US$ den höchsten prozentualen Anteil an Angriffen dieser Art meldete (38 %). Unternehmenswachstum ist meistens auch mit größeren und komplexeren IT-Infrastrukturen verbunden. Dies erschwert es IT-Teams, alle Schwachstellen zu erkennen und zu beheben, bevor sie ausgenutzt werden.

Kompromittierte Zugangsdaten waren insbesondere in den mittleren/hohen Umsatzsegmenten ein weit verbreiteter Angriffsvektor. In Unternehmen mit einem Jahresumsatz von 250 Mio. bis 500 Mio. US$ und von 500 Mio. bis 1 Mrd. US$ waren sie die Hauptangriffsursache. Während Schwachstellen und kompromittierte Zugangsdaten zu Recht viel Aufmerksamkeit erhalten, sind schädliche E-Mails die am häufigsten gemeldete Ursache in Unternehmen mit einem Jahresumsatz von 10 bis 50 Mio. US$. Insgesamt machten E-Mail-basierte Bedrohungen knapp die Hälfte (49 %) der Angriffe in diesem Bereich aus.



Kennen Sie die Ursache des Ransomware-Angriffs auf Ihr Unternehmen im vergangenen Jahr? Anzahl=2.974 von Ransomware betroffene Unternehmen.

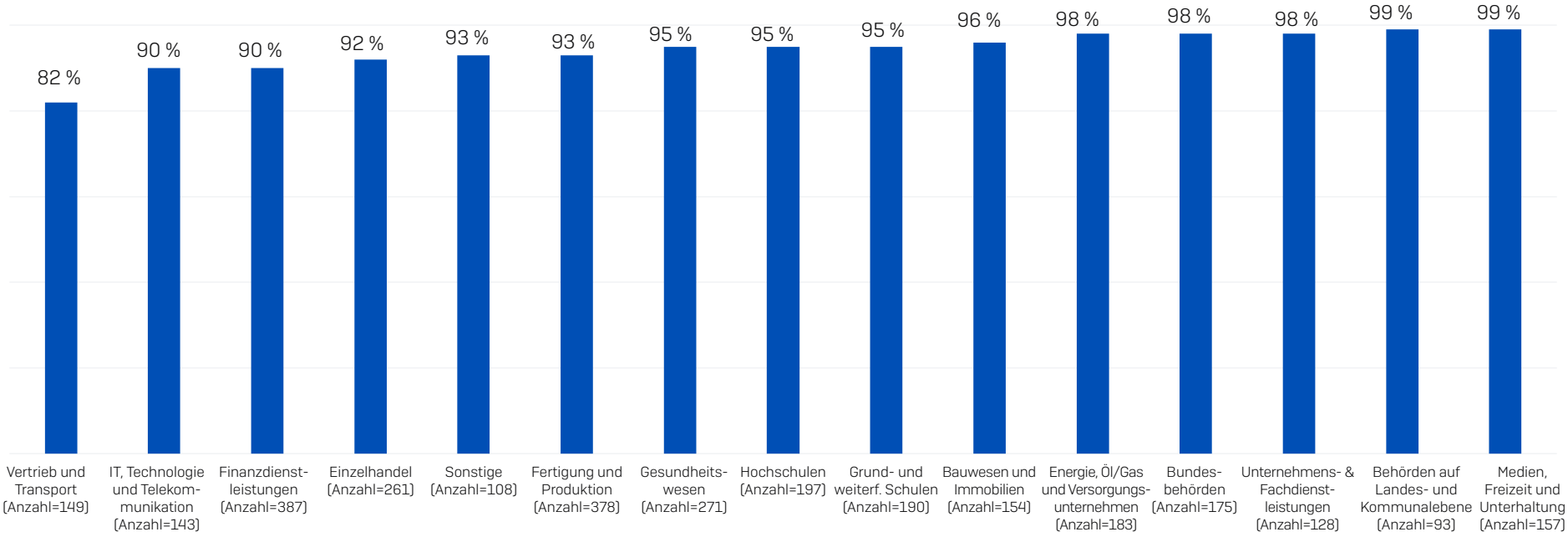
Kompromittierung von Backups

Bei einem Ransomware-Angriff gibt es im Wesentlichen zwei Optionen zur Wiederherstellung verschlüsselter Daten: Datenwiederherstellung aus Backups und Zahlung des Lösegelds. Indem Ransomware-Akteure die Backups ihrer Opfer kompromittieren, vereiteln sie die Wiederherstellung verschlüsselter Daten aus Backups und erhöhen so den Druck, das Lösegeld zu zahlen.

Versuchte Kompromittierung von Backups

94 % der Befragten, die im vergangenen Jahr von Ransomware betroffen waren, gaben an, dass Cyberkriminelle im Rahmen des Angriffs versuchten, Backups zu schädigen. Bei Behörden auf *Landes- und Kommunalebene* sowie im *Medien-, Freizeit- und Unterhaltungssektor* lag der prozentuale Anteil sogar bei 99 %. Im Bereich *Vertrieb und Transport* wurden die wenigsten Kompromittierungsversuche gemeldet. Doch selbst in dieser Branche bestätigten mehr als acht von zehn (82 %) der von Ransomware betroffenen Unternehmen und Organisationen, dass die Angreifer versucht hatten, auf ihre Backups zuzugreifen.

Prozentualer Anteil der Angriffe, bei denen die Angreifer versuchten, Backups zu kompromittieren



Versuchten Cyberkriminelle Ihre Backups zu kompromittieren? Ja. Anzahl der erhaltenen Antworten jeweils in Klammer;

Erfolgsquote von Versuchen, Backups zu kompromittieren

Über alle Branchen hinweg waren 57 % der Versuche, Backups zu kompromittieren, erfolgreich. Somit konnten Cyberkriminelle die Wiederherstellung nach einem Ransomware-Angriff bei mehr als der Hälfte ihrer Opfer beinträchtigen. Im Branchenvergleich zeichneten sich signifikante Unterschiede bei der Erfolgsquote der Angreifer ab:

- In den Sektoren *Energie, Öl/Gas und Versorgungsunternehmen* (Erfolgsquote: 79 %) und *Bildung* (Erfolgsquote: 71 %) gelang es Angreifern am häufigsten, die Backups ihrer Opfer zu schädigen
- In der *IT, Technologie und Telekommunikation* (Erfolgsquote: 30 %) sowie im *Einzelhandel* (Erfolgsquote: 47 %) wurden Backups dagegen am seltensten kompromittiert

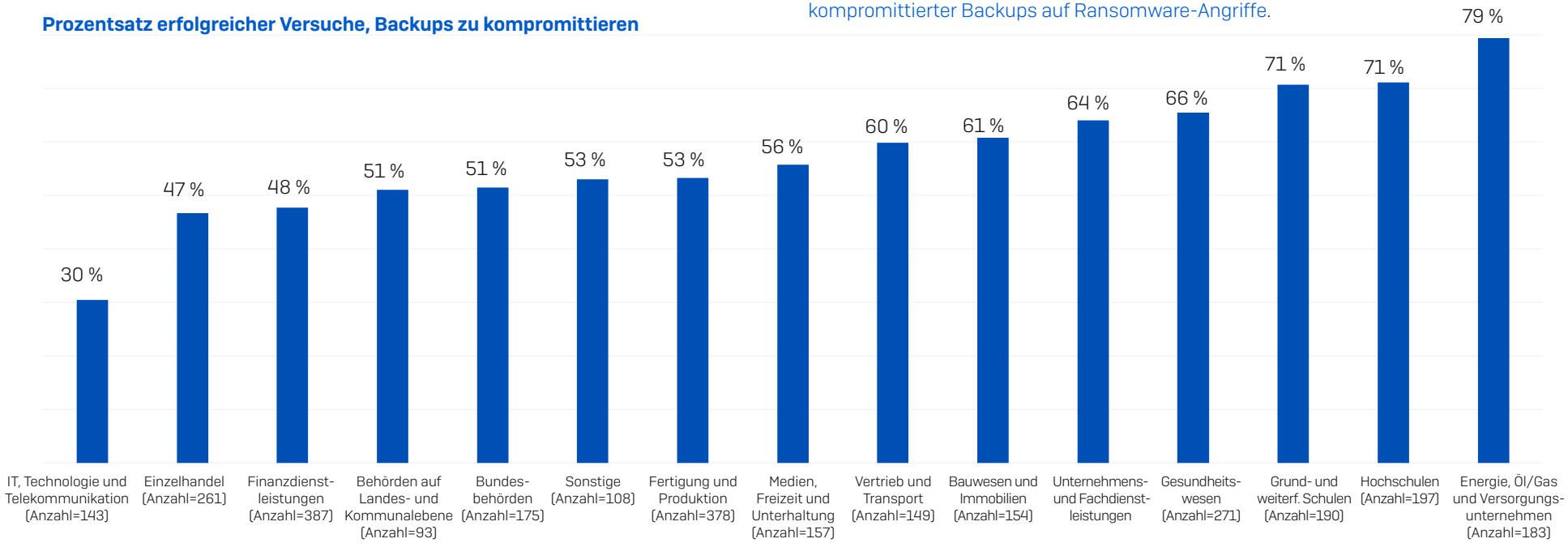
Die unterschiedlichen Erfolgsquoten lassen sich auf mehrere mögliche Gründe zurückführen. Vermutlich verfügten Unternehmen und Organisationen aus den Bereichen *IT, Telekommunikation und Technologie* über einen stärkeren Backup-Schutz und waren so besser gegen die Angriffe gewappnet als andere Branchen. Möglicherweise waren sie auch besser in der Lage, Kompromittierungsversuche rechtzeitig zu erkennen und zu stoppen.

Vom Angriffsvektor einmal abgesehen: Wenn Backups im Zuge eines Angriffs kompromittiert wurden, meldeten betroffene Unternehmen erheblich schwerwiegendere Folgen:

- Die Lösegeldforderungen waren im Durchschnitt mehr als doppelt so hoch wie bei Unternehmen, deren Backups nicht betroffen waren (mittlere erste Lösegeldforderungen in Höhe von 2,3 Mio. US$ ggü. 1 Mio. US$)
- Unternehmen und Organisationen, deren Backups beeinträchtigt wurden, zahlten fast doppelt so häufig Lösegeld, um ihre verschlüsselten Daten wiederherstellen zu können (67 % ggü. 36 %)
- Die mittleren Gesamtbereinigungskosten fielen achtmal höher aus (3 Mio. US$ ggü. 375.000 US$) als in Unternehmen mit intakten Backups

Eine ausführliche Analyse zu diesem Thema bietet unser Report Die Auswirkungen kompromittierter Backups auf Ransomware-Angriffe.

Prozentsatz erfolgreicher Versuche, Backups zu kompromittieren



Versuchten Cyberkriminelle Ihre Backups zu kompromittieren? Ja, Anzahl der erhaltenen Antworten jeweils in Klammer.

Datenverschlüsselungsrate

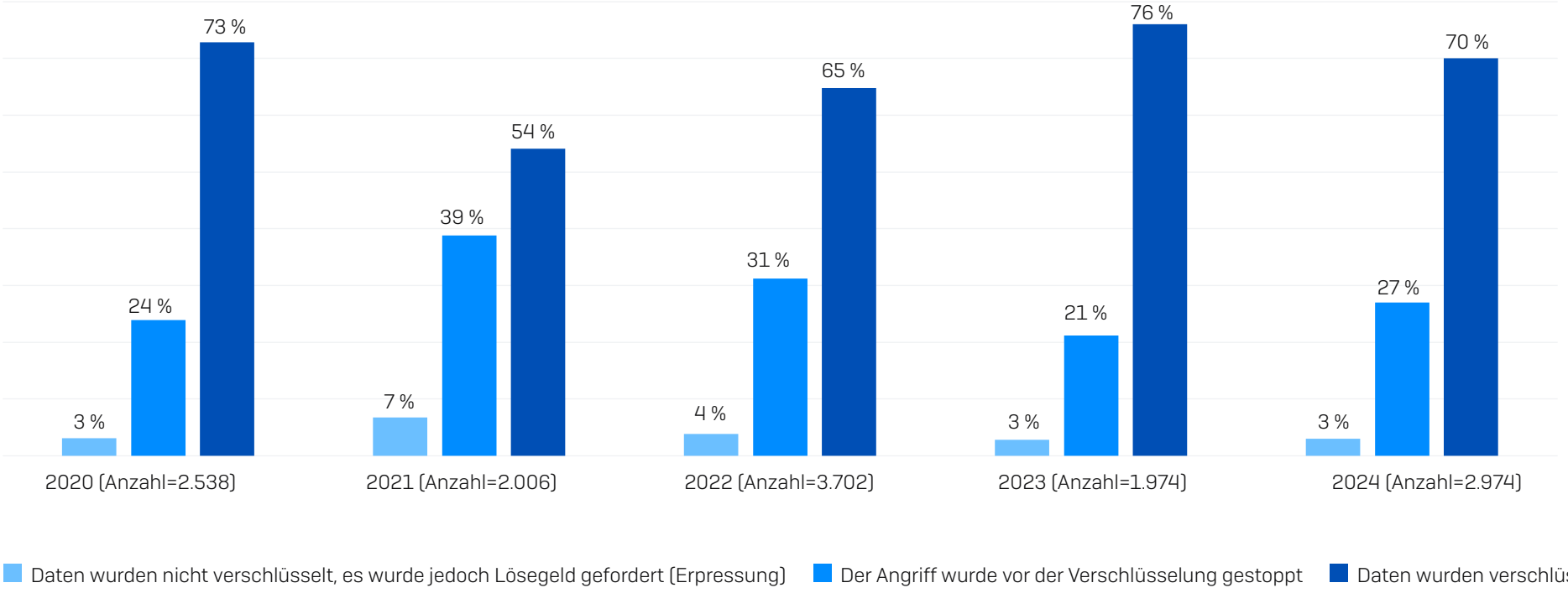
Sieben von zehn (70 %) Ransomware-Angriffen gingen im letzten Jahr mit Datenverschlüsselungen einher. Obwohl dieser Prozentsatz hoch ist, liegt er doch leicht unter den 76 % der Angriffe, bei denen die Angreifer im Vorjahr Daten verschlüsseln konnten.

Datenverschlüsselungsrate nach Branche

Der diesjährige Report zeigt erhebliche Diskrepanzen bei den Verschlüsselungsraten im Branchenvergleich.

- *Behörden auf Landes- und Kommunalebene* verzeichneten in diesem Jahr das niedrigste Angriffsaufkommen (34 %). Gleichzeitig meldete der Sektor jedoch auch die **höchste Datenverschlüsselungsrate**: Bei 98 % der Angriffe wurden Daten verschlüsselt
- *Finanzdienstleister* (49 %), gefolgt vom Einzelhandel (56 %) meldeten die **niedrigsten Datenverschlüsselungsraten**
- Der Bereich *Vertrieb und Transport* war am häufigsten von **Extortion-Angriffen** betroffen. 17 % der Befragten – fast dreimal so viele wie in allen anderen Branchen – gaben an, dass ihre Daten nicht verschlüsselt wurden, sie jedoch erpresst wurden

Im Anhang finden Sie eine detaillierte Aufschlüsselung der Datenverschlüsselungsrate nach Branche.



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

Sophos-Whitepaper, April 2024

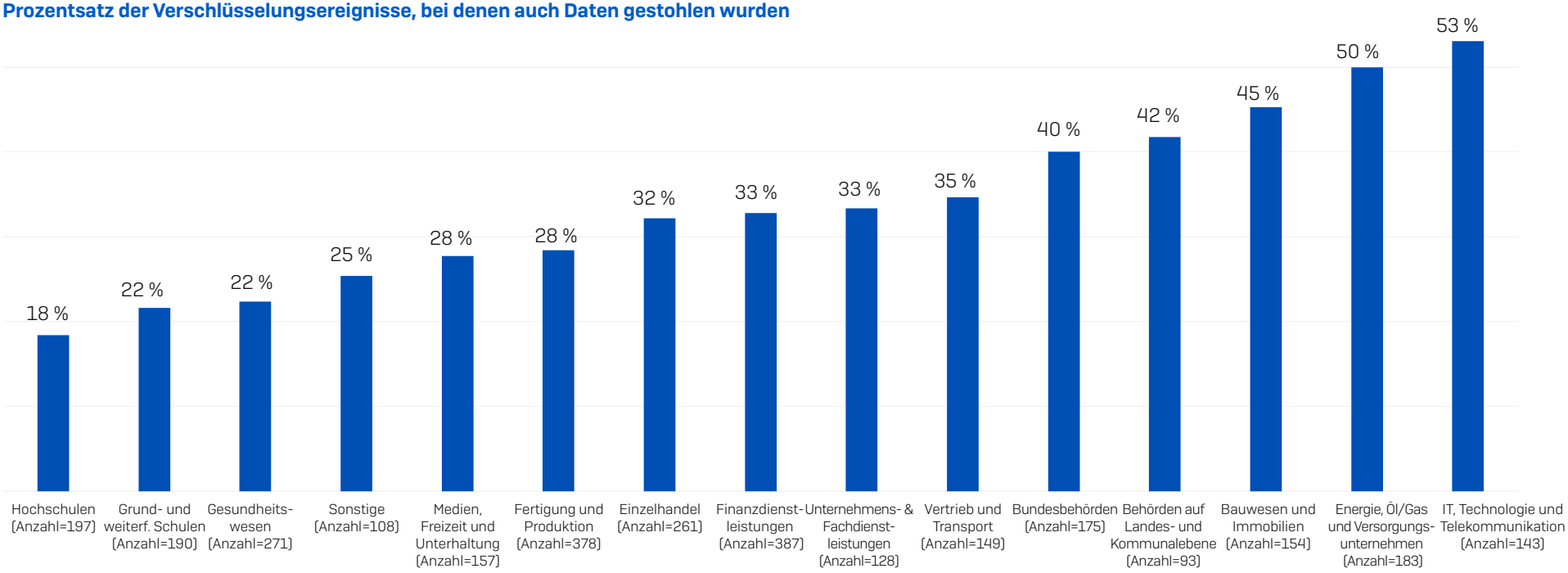
Datendiebstahl

Cyberkriminelle verschlüsseln nicht nur Daten – sie stehlen sie auch. Bei 32 % der Vorfälle, bei denen Daten verschlüsselt wurden, wurden Daten zudem gestohlen – etwas häufiger als im Vorjahr (30 %). Datendiebstahl erleichtert es den Angreifern, Geld von ihren Opfern zu erpressen. Außerdem können Cyberkriminelle die gestohlenen Daten im Dark Web zum Verkauf anbieten und so noch mehr Profit aus dem Angriff schlagen.

Auch hier zeigen sich im Branchenvergleich erhebliche Unterschiede. So schnitt der Bereich IT, Technologie und Telekommunikation am schlechtesten ab: Bei 53 % der Angriffe wurden Daten nicht nur verschlüsselt, sondern auch gestohlen. An zweiter Stelle stehen *Energie, Öl/Gas und Versorgungsunternehmen*: 50 % der Verschlüsselungsereignisse gingen mit Datendiebstahl einher. Das Bildungswesen verzeichnete die niedrigste Datendiebstahlsrate bei Angriffen. In *Hochschulen* wurden Daten am seltensten verschlüsselt und gestohlen (18 %), gefolgt von *Grund- und weiterführenden Schulen*, die sich den zweiten Platz mit dem Gesundheitswesen teilen (jeweils 22 %).

Diese Ergebnisse spiegeln möglicherweise unterschiedliche Analysekapazitäten und Prioritäten im Branchenvergleich wider. Die Feststellung, ob Daten exfiltriert wurden, erfordert ein höheres Maß an forensischen Kapazitäten und stützt sich häufig auf Protokolle von EDR/XDR-Tools. Womöglich sind Unternehmen aus dem Bereich *IT, Technologie und Telekommunikation* eher in der Lage, Datendiebstahl zu erkennen, als andere Branchen. Vielleicht erleichtern die relativ einfach gestalteten IT-Umgebungen vieler *Energie, Öl/Gas und Versorgungsunternehmen* Angreifern zudem den Diebstahl von Daten. Umgekehrt verfügen Bildungseinrichtungen oft nicht über die nötigen Fähigkeiten und Tools, um festzustellen, ob Daten gestohlen wurden. Gleichzeitig möchten Unternehmen mitunter nicht wissen, ob Daten exfiltriert wurden, da die Offenlegung einer Datenpanne mit hohen Kosten verbunden sein kann.

Prozentsatz der Verschlüsselungsereignisse, bei denen auch Daten gestohlen wurden



Konnten Cyberkriminelle bei dem Ransomware-Angriff Ihre Unternehmensdaten verschlüsseln? Ja. Ja und Daten wurden gestohlen. Anzahl der erhaltenen Antworten jeweils in Klammer.

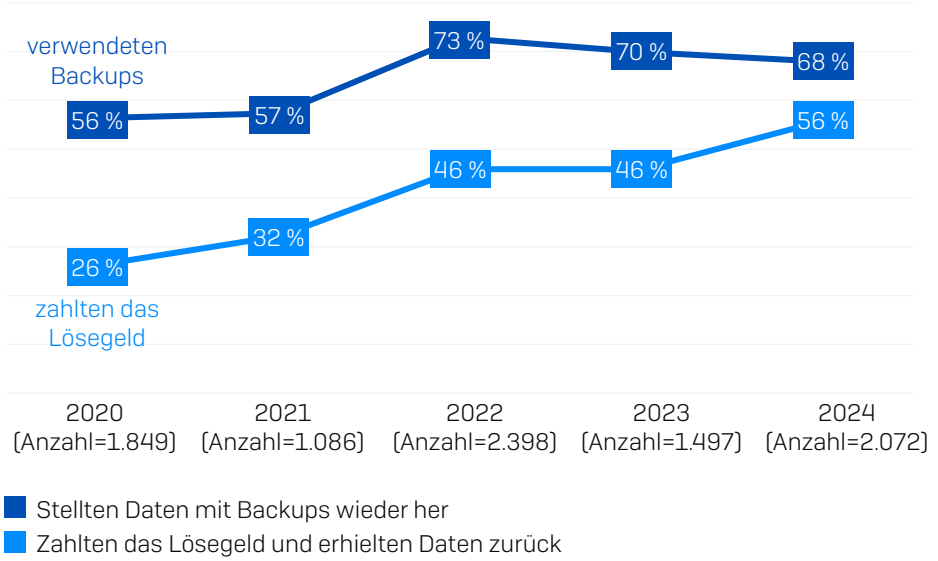
Datenwiederherstellung

98 % der Unternehmen, deren Daten verschlüsselt wurden, bekamen Daten zurück. Die gängigsten Methoden zur Datenwiederherstellung waren Backups (68 %) sowie die Zahlung von Lösegeld, um den Entschlüsselungsschlüssel zu erhalten (56 %). 26 % der Unternehmen, deren Daten verschlüsselt wurden, gaben an, dass sie ihre Daten über „andere Mittel" zurückbekamen. Zwar wurden diese Mittel im Rahmen der Umfrage nicht weiter untersucht, denkbar sind jedoch beispielsweise die Zusammenarbeit mit Strafverfolgungsbehörden oder die Verwendung bereits veröffentlichter Entschlüsselungsschlüssel.

Stellten Daten mit Backups wieder her	Zahlten das Lösegeld und erhielten Daten zurück	Stellten Daten mit anderen Mitteln wieder her
68 %	**56 %**	**26 %**

Eine nennenswerte Änderung ggü. dem Vorjahr besteht darin, dass Opfer von Ransomware zunehmend mehrere Methoden zur Wiederherstellung verschlüsselter Daten anwenden (z. B. Zahlung des Lösegelds und Verwendung von Backups). Fast die Hälfte der Unternehmen, deren Daten verschlüsselt wurden, verwendeten mehr als eine Methode (47 %) – mehr als doppelt so viel wie im Jahr 2023 (21 %).

Die Fünfjahresbetrachtung zeigt, dass die Diskrepanz zwischen der Nutzung von Backups und der Zahlung des Lösegelds weiter abnimmt. Die Nutzung von Backups ist im zweiten Jahr in Folge leicht zurückgegangen. Gleichzeitig ist die Zahl der Lösegeldzahlungen seit der Umfrage von 2023 um 10 Prozent gestiegen. Die Bereitschaft, Lösegeld zu zahlen, hängt von vielen Faktoren ab, unter anderem von der Verfügbarkeit von Backups. Dies ist jedoch ein beunruhigender Trend: Mehr als die Hälfte der Opfer zahlen für den Entschlüsselungsschlüssel.



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 Umsatz

Die Bereitschaft, Lösegeld für die Wiederherstellung von Daten zu zahlen, stieg im Allgemeinen mit dem Umsatz. Unternehmen mit den geringsten Umsätzen (weniger als 10 Mio. US$) wiesen die bei weitem niedrigste Lösegeldzahlungsrate auf (25 %). Unternehmen mit den höchsten Umsätzen (über 5 Mrd. US$) zahlten am häufigsten das Lösegeld (61 %). Die Verfügbarkeit von Mitteln zur Deckung des Lösegelds spielte hier wahrscheinlich eine entscheidende Rolle – viele sehr kleine Unternehmen sind einfach nicht in der Lage, das Lösegeld aufzubringen.

Wie wir bereits gesehen haben, ist die Datenrettung jedoch nicht nur eine Frage von Backups oder Lösegeld. Die Nuancen in puncto Datenwiederherstellungsmethoden werden deutlich, wenn wir die Daten genauer betrachten und die Zahlen für 2024 mit denen des letzten Jahres vergleichen.

Mit Ausnahme der Unternehmen mit einem Umsatz von weniger als 10 Mio. US$ meldeten alle Umsatzsegmente eine Zunahme der Lösegeldzahlungsquote. Gleichzeitig wurden Daten auch häufiger über Backups wiederhergestellt. Das niedrigste Umsatzsegment wies die höchste Backup-Nutzungsquote auf (88 %), dicht gefolgt von Unternehmen mit einem Jahresumsatz von 250 bis 500 Mio. US$ (85 %).

Datenwiederherstellung nach Branche

Es überrascht vielleicht kaum, dass *Bundesbehörden* am seltensten das Lösegeld für die Wiederbeschaffung von Daten zahlen. Einerseits sind Zahlungen in diesem Sektor streng reglementiert. Andererseits nutzen Bundesbehörden am häufigsten Backups zur Wiederherstellung von Daten (39 % bzw. 81 %).

Insgesamt ließ sich kein eindeutiger Zusammenhang zwischen der Nutzung von Backups und Lösegeldzahlungen herleiten:

- Unternehmen aus dem Bereich *Medien, Freizeit und Unterhaltung* zahlten am häufigsten das Lösegeld, um ihre Daten wiederherzustellen (69 %). Auch bei der Backup-Nutzung lagen sie relativ weit vorn (74 %)
- *Energie, Öl/Gas und Versorgungsunternehmen* wiesen die niedrigste Backup-Nutzung (51 %) auf. Mit 61 % lag zudem ihre Lösegeldzahlungsquote unter vier weiteren Bereichen

Im Anhang finden Sie eine detaillierte Aufschlüsselung der Datenwiederherstellungsmethode nach Branche.

	JAHRESUMSATZ													
	Weniger als 10 Mio. US$ (Anzahl=39)		**10 Mio.–50 Mio. US$ (Anzahl=291)**		**50 Mio.–250 Mio. US$ (Anzahl=557)**		**250 Mio.–500 Mio. US$ (Anzahl=341)**		**500 Mio.–1 Mrd. US$ (Anzahl=572)**		**1 Mrd. –5 Mrd. US$ (Anzahl=632)**		**>5 Mrd. (Anzahl=542)**	
Methoden zur Datenwiederherstellung	2023	2024	2023	2024	2023	2024	2023	2024	2023	2024	2023	2024	2023	2024
Stellten Daten mit Backups wieder her	80 %	88 % ▲	72 %	68 % ▼	77 %	60 % ▼	75 %	85 % ▲	68 %	70 % ▲	66 %	65 % ▼	63 %	66 % ▲
Zahlten das Lösegeld und erhielten Daten zurück	36 %	25 % ▼	41 %	49 % ▲	42 %	57 % ▲	33 %	50 % ▲	51 %	59 % ▲	52 %	56 % ▲	55 %	61 % ▲

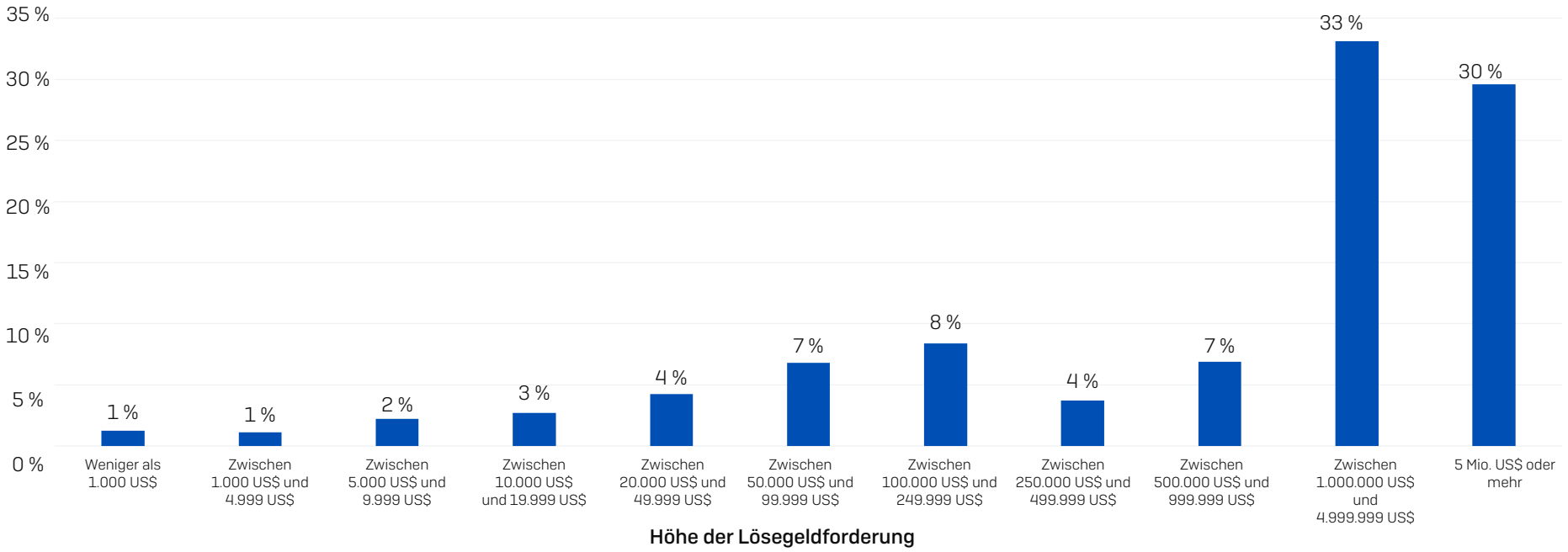
Erhielt Ihr Unternehmen Daten wieder zurück? Ja, wir haben das Lösegeld gezahlt und unsere Daten zurückerhalten; Ja, wir haben Backups genutzt, um die Daten wiederherzustellen. Anzahl der 2024 erhaltenen Antworten jeweils in Klammer. Pfeil zeigt Anstieg/Rückgang im Vergleich zu 2023 an.

Lösegeldforderungen

Der diesjährige Report berücksichtigt zum ersten Mal sowohl Lösegeldforderungen als auch -zahlungen. Bei den 1.701 Unternehmen, deren Daten verschlüsselt wurden und die die ursprüngliche Lösegeldforderung der Angreifer angeben konnten, betrug die durchschnittliche Forderung 4.321.880 US$ (Durchschnitt) und 2 Mio. US$ (Mittelwert).

Eines der bemerkenswertesten Ergebnisse der diesjährigen Studie ist, dass 63 % der Lösegeldforderungen mindestens 1 Million US$ und 30 % der Forderungen sogar 5 Mio. US$ oder mehr betrugen. Lediglich eine kleine Minderheit der Befragten meldete vierstellige Lösegeldforderungen.

Prozentualer Anteil der Lösegeldforderungen am Gesamtbetrag



Wie viel Lösegeld forderten die Angreifer? Anzahl=1.701

Lösegeldforderungen nach Umsatz

Betrachtet man sowohl den Durchschnitt als auch den Mittelwert der Daten, so zeigt sich, dass die Lösegeldforderungen mit dem Umsatz steigen. Dies lässt darauf schließen, dass Bedrohungsakteure ihre Lösegeldforderungen – zumindest teilweise – an die wahrscheinliche Zahlungsfähigkeit anpassen.

Hohe Lösegeldforderungen sind nicht mehr nur den umsatzstärksten Unternehmen vorbehalten. So sind Forderungen in Höhe von 1 Million US$ oder mehr mittlerweile in allen Umsatzsegmenten üblich: 47 % der Unternehmen mit einem Umsatz von 10 Mio. bis 50 Mio. US$ erhielten im letzten Jahr siebenstellige Lösegeldforderungen.

Lösegeldforderungen nach Branche

Hier gibt es keine Gewinner, denn alle genannten Branchen (außer „Sonstige“) meldeten durchschnittliche Lösegeldforderungen von 1 Mio. US$ oder mehr.

- Der *Einzelhandel* und die *IT, Technologie und Telekommunikation* erhielten im Mittel die niedrigsten Lösegeldforderungen (1 Mio. US$), gefolgt vom *Bauwesen* (1,1 Mio. US$)
- Besonders horrende Summen forderten Cyberkriminelle von *Bundesbehörden.* Hier beliefen sich Lösegeldzahlungen im Mittel auf 7,7 Mio. US$ und im Durchschnitt auf 9,9 Mio. US$

Im Anhang finden Sie eine detaillierte Aufschlüsselung der Lösegeldforderungen nach Branche.

	JAHRESUMSATZ					
Lösegeldforderung	**10 Mio.–50 Mio. US$ (Anzahl=207)**	**50 Mio.–250 Mio. US$ (Anzahl=288)**	**250 Mio.–500 Mio. US$ (Anzahl=158)**	**500 Mio.–1 Mrd. US$ (Anzahl=268)**	**1 Mrd. –5 Mrd. US$ (Anzahl=366)**	**>5 Mrd. (Anzahl=398)**
Durchschnitt	1.774.941 US$	1.704.853 US$	3.407.796 US$	5.184.024 US$	4.281.258 US$	7.467.294 US$
Mittelwert	330.000 US$	220.000 US$	840.000 US$	2.000.000 US$	3.000.000 US$	6.600.000 US$

Wie viel Lösegeld forderten die Angreifer? Anzahl der erhaltenen Antworten jeweils in Klammer. Hinweis: Das Umsatzsegment „Weniger als 10 Mio. US$“ ist aufgrund der geringen Antwortanzahl nicht in der Tabelle enthalten.

Lösegeldzahlungen

1.097 Unternehmen, die der Lösegeldforderung nachkamen, gaben die tatsächlich gezahlte Summe an. Bei den mittleren und durchschnittlichen Lösegeldzahlungen lässt sich ein erheblicher Anstieg im letzten Jahr feststellen:

- Mittlere Lösegeldzahlung: 2.000.000 US$ (ein 5-facher Anstieg ggü. den für 2023 gemeldeten 400.000 US$)
- Durchschnittliche Lösegeldzahlung: 3.960.917 US$ (2,6 Mal mehr als 2023 (1.542.330 US$))

Wie aus der folgenden Grafik hervorgeht, ist der Anteil der niedrigeren Lösegeldzahlungen in den letzten drei Jahren stetig gesunken. Der Anteil der sehr hohen Zahlungen ist dagegen in die Höhe geschnellt. Lösegeldzahlungen in siebenstelliger Höhe oder mehr sind inzwischen die Regel.

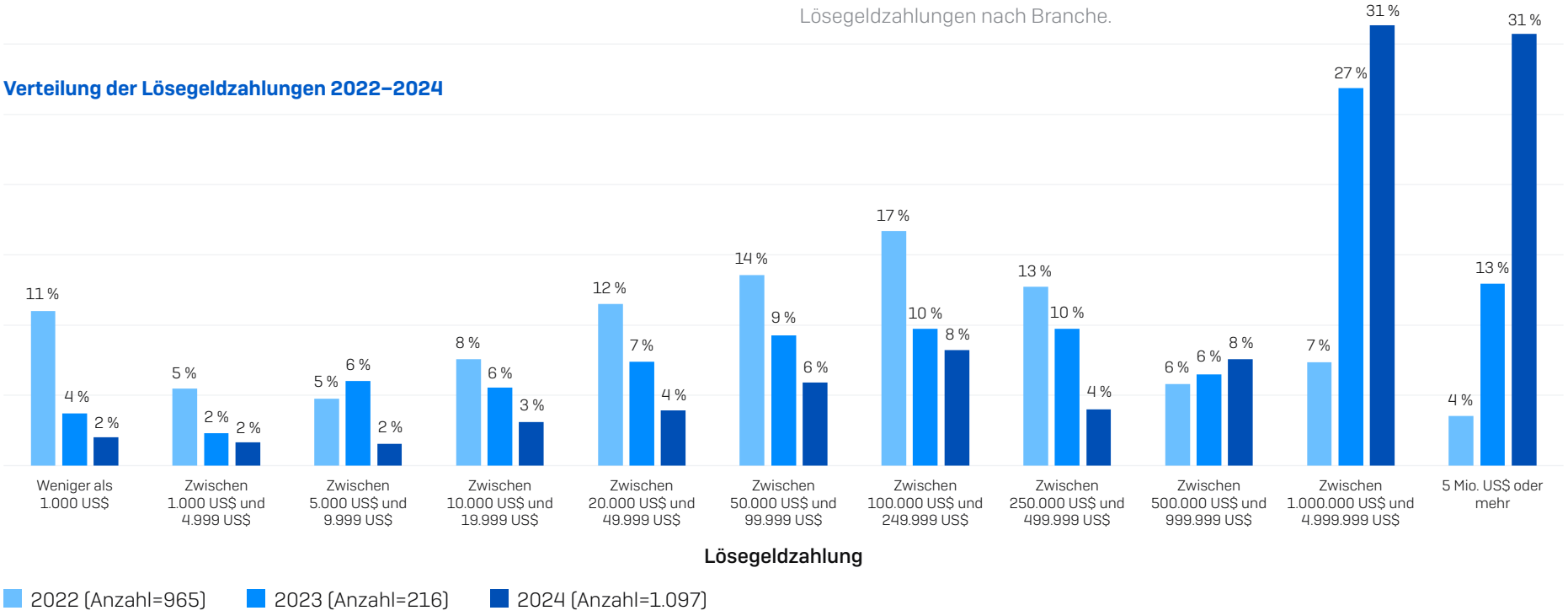
Lösegeldzahlungen nach Branche

Doch nicht nur bei den durchschnittlichen Lösegeldforderungen, sondern auch bei den durchschnittlichen Lösegeldzahlungen zeigen sich signifikante Unterschiede im Branchenvergleich. Der Bereich *IT, Technologie und Telekommunikation* meldete die niedrigsten mittleren Lösegeldzahlungen (300.000 US$), gefolgt von *Vertrieb und Transport* (440.000 US$). Am anderen Ende der Skala zahlten Ransomware-Opfer aus *Grund- und weiterführenden Schulen* und *Bundesbehörden* mittlere Lösegeldsummen in Höhe von 6,6 Mio. US$.

Im Großen und Ganzen lässt sich ein Zusammenhang zwischen niedrigeren Forderungen und niedrigeren Zahlungen (und umgekehrt) herleiten. Doch Ausnahmen bestätigen bekanntlich die Regel: Im Bereich *Vertrieb und Transport* beliefen sich die mittleren Lösegeldforderungen auf über 2,8 Mio. US$, die durchschnittlichen Zahlungen jedoch auf 440.000 US$.

Im Anhang finden Sie eine detaillierte Aufschlüsselung der durchschnittlichen Lösegeldzahlungen nach Branche.

Verteilung der Lösegeldzahlungen 2022–2024



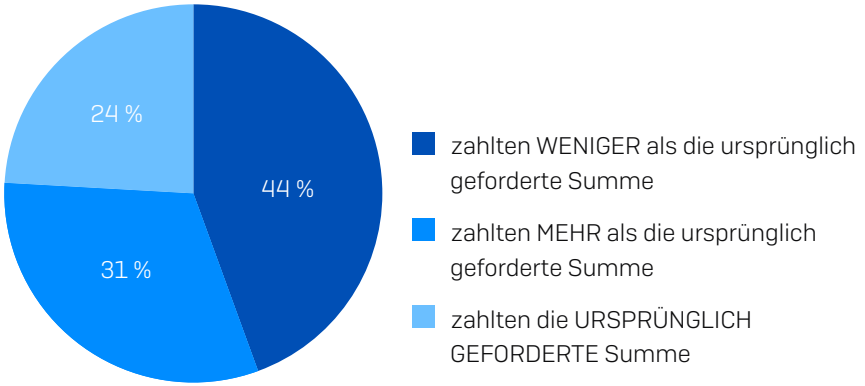
Wie viel Lösegeld wurde den Angreifern gezahlt? Anzahl der erhaltenen Antworten jeweils in Klammer.

Lösegeldforderung vs. Lösegeldzahlung

Wenn Daten verschlüsselt werden, stehen alle Beteiligten unter enormem Druck und beide Seiten möchten ihre Ergebnisse optimieren. Unternehmen, deren Daten verschlüsselt wurden, möchten die finanziellen Auswirkungen so gering wie möglich halten. Gleichzeitig versuchen Cyberkriminelle, in kürzester Zeit so viel Geld wie möglich herauszuschlagen. So drohen sie häufig mit höheren Lösegeldforderungen, sollte die Zahlung nicht bis zu einem bestimmten Termin erfolgen, und verstärken damit den Druck auf ihre Opfer.

Bereitschaft zur Verhandlung über die Lösegeldsumme

Unsere Studie hat ergeben, dass die betroffenen Unternehmen nur selten die ursprünglich von den Angreifern geforderte Summe zahlen: Lediglich 24 % der Befragten gaben an, dass ihre Zahlung der ursprünglichen Forderung entsprach. 44 % zahlten weniger als die ursprüngliche Forderung, 31 % mehr.



Wie viel Lösegeld forderten die Angreifer? Wie viel Lösegeld wurde den Angreifern gezahlt? Anzahl=1.097.

Im Branchenvergleich zeigt sich, dass die beiden Dienstleistungsbereiche – *Unternehmens- und Fachdienstleistungen* und *Finanzdienstleistungen* – am häufigsten versuchten, die Lösegeldsumme herunterzuhandeln: 67 % gaben an, weniger als die ursprüngliche Forderung gezahlt zu haben. *Fertigung und Produktion* folgen dicht dahinter: Bei 65 % der Unternehmen lag die gezahlte Summe unter der ursprünglichen Forderung.

Umgekehrt zahlten Bereiche mit einem hohen Anteil an öffentlichen Einrichtungen am ehesten mehr als die ursprüngliche Forderung:

- Von Ransomware betroffene *Hochschulen* zahlten am häufigsten mehr als die ursprüngliche Forderung (67 % zahlten mehr) und am seltensten weniger (20 % zahlten weniger)
- Im *Gesundheitswesen* lag die gezahlte Summe am zweithäufigsten über der ursprünglichen Forderung (57 %), gefolgt von *Grund- und weiterführenden Schulen* (55 %)

Möglicherweise sind Einrichtungen in diesen Bereichen weniger in der Lage, ihre Kosten mit Hilfe professioneller Lösegeldvermittler zu senken. Möglicherweise müssen Daten aufgrund des öffentlichen Auftrags dieser Einrichtungen eher „um jeden Preis" wiederhergestellt werden. In jedem Fall ist klar, dass zwischen der ursprünglichen Forderung und der letztendlichen Zahlung Handlungsspielraum besteht.

Im Anhang finden Sie eine detaillierte Aufschlüsselung der Lösegeldforderungen und Lösegeldzahlungen nach Branche.

Gezahlter prozentualer Anteil der Lösegeldforderung

Obwohl in den meisten Fällen über die Höhe des Lösegelds verhandelt wurde, wich die letztendlich gezahlte Summe nur geringfügig vom geforderten Betrag ab: Befragten aller Branchen gaben an, dass sie im Durchschnitt 94 % der ursprünglichen Forderung zahlten.

Bei näherer Betrachtung zeigt sich, dass alle Umsatzgruppen mit Ausnahme der Unternehmen mit den höchsten Umsätzen in der Lage waren, die Lösegeldzahlung herunterzuhandeln. Unternehmen mit einem Umsatz von 50 Mio. bis 250 Mio. US$ zahlten den niedrigsten Anteil der ursprünglichen Forderung (84 %). Nur Unternehmen mit mehr als 5 Mrd. US$ Jahresumsatz zahlten im Durchschnitt 115 % des geforderten Lösegelds.

	JAHRESUMSATZ					
Gruppe	**10 Mio.–50 Mio. US$ (Anzahl=100)**	**50 Mio.–250 Mio. US$ (Anzahl=206)**	**250 Mio.–500 Mio. US$ (Anzahl=104)**	**500 Mio.–1 Mrd. US$ (Anzahl=175)**	**1 Mrd. – 5 Mrd. US$ (Anzahl=233)**	**>5 Mrd. (Anzahl=275)**
Gezahlter prozentualer Anteil der Lösegeld-forderung	93 %	84 %	90 %	88 %	85 %	115 %

Wie viel Lösegeld forderten die Angreifer? Wie viel Lösegeld wurde den Angreifern gezahlt? Anzahl=1.097. Hinweis: Das Umsatzsegment „Weniger als 10 Mio. US$" ist aufgrund der geringen Antwortanzahl nicht in der Aufschlüsselung der Jahresumsätze enthalten.

Gezahlter Anteil der Lösegeldforderung nach Branche

Im Branchenvergleich zeigt sich, dass Branchen, die am häufigsten versuchten, das Lösegeld herunterzuhandeln, auch den niedrigsten Prozentsatz der ursprünglichen Forderung zahlten – und umgekehrt.

WENIGER ALS 100 %	MEHR ALS 100 %
Fertigung und Produktion (70 %)	Hochschulwesen (122 %)
Unternehmens- & Fachdienstleistungen (74 %)	Grund- und weiterführende Schulen (115 %)
Finanzdienstleistungen (75 %)	Gesundheitswesen (111 %)
Sonstige 79 %	Behörden auf Landes- und Kommunalebene (104 %)
IT, Telekommunikation und Technologie (82 %)	Bundesbehörden (103 %)
Einzelhandel (84 %)	Energie, Öl/Gas und Versorgungsunternehmen (101 %)
Bauwesen und Immobilien (95 %)	
Vertrieb und Transport (95 %)	
Medien, Freizeit und Unterhaltung (95 %)	

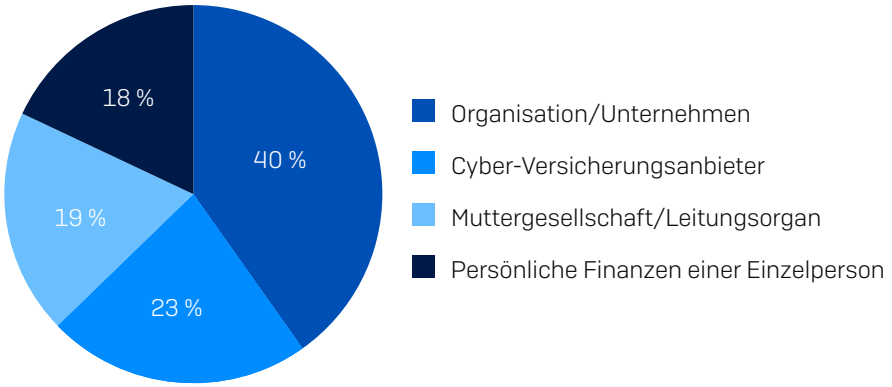
Wie viel Lösegeld forderten die Angreifer? Wie viel Lösegeld wurde den Angreifern gezahlt? Anzahl=1.097.

Quellen zur Finanzierung des Lösegelds

Besonders interessant ist auch, wie das Lösegeld finanziert wird. Hierzu gibt unsere Studie interessante Einblicke:

- Das Lösegeld aufzubringen, ist eine gemeinsame Anstrengung. So führten mehr als vier Fünftel der Befragten (82 %) mehrere Finanzierungsquellen an
- Die Hauptquelle für die Finanzierung des Lösegelds war das Unternehmen selbst, das im Durchschnitt 40 % der Zahlung übernahm. Die Muttergesellschaft und/oder das Leitungsorgan brachte in der Regel 19 % auf
- Versicherungsanbieter waren in hohem Maße an Lösegeldzahlungen beteiligt
  - 23 % aller Lösegeldzahlungen wurden von Versicherungsunternehmen finanziert
  - Bei 83 % der Angriffe beteiligten sich Versicherer an der Lösegeldzahlung
  - Allerdings übernahmen Versicherer nur äußerst selten (1 %) den vollen Betrag: Bei 79 % der Fälle finanzierte die Versicherung weniger als die Hälfte der Gesamtsumme

Finanzierungsquelle des Lösegelds



Aus welchen der folgenden Quellen wurde das Lösegeld finanziert? Anzahl=1.168.

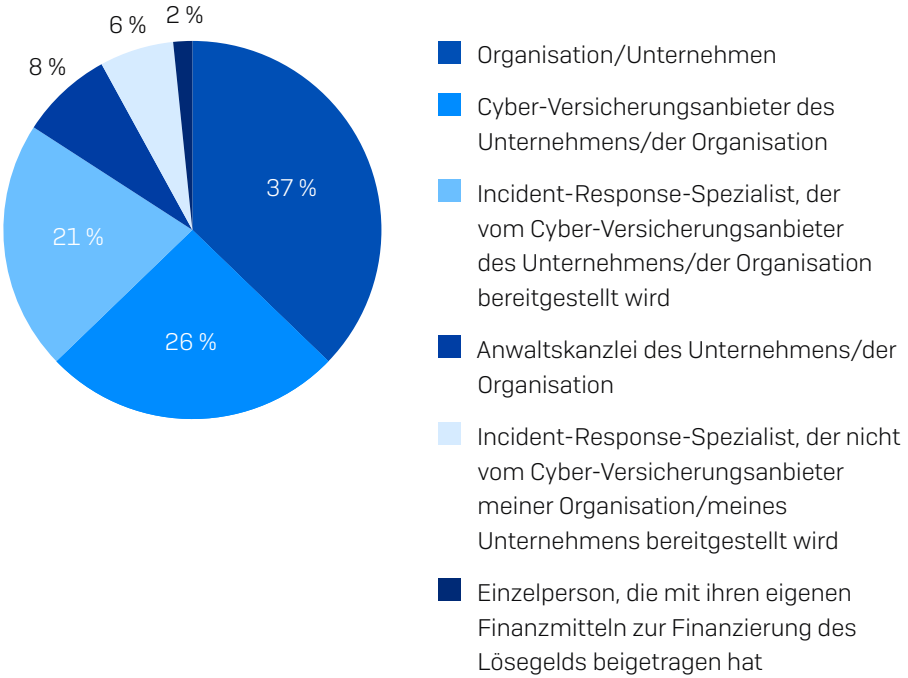
Lösegeldtransaktion

Obwohl das Lösegeld zum Teil aus mehreren Quellen zusammengetragen wurde, wurden die Mittel in der Regel in einer einzigen Transaktion von einer Partei überwiesen.

Insgesamt überwiesen Versicherungsanbieter die Mittel für fast die Hälfte der Lösegeldzahlungen entweder direkt (26 %) oder über den von ihnen beauftragten Incident-Response-Spezialisten (21 %). 37 % der Zahlungen wurden von den betroffenen Unternehmen selbst geleistet, 8 % von ihrer Anwaltskanzlei.

Insgesamt wurden 28 % (gerundet) der Überweisungen von Incident-Response-Spezialisten getätigt, die entweder vom Versicherungsanbieter (21 %) oder einer anderen Partei – in der Regel dem Opfer (6 %) – beauftragt wurden.

Lösegeldüberweisung



Wer hat die Lösegeldzahlung vorgenommen, d. h. wer hat das Geld auf das Konto des Angreifers überwiesen? Anzahl=1.168.

Bereinigungskosten

Lösegeldzahlungen sind nur eine Komponente der Bereinigungskosten bei Ransomware-Vorfällen. Ohne Berücksichtigung des gezahlten Lösegelds beliefen sich die mittleren Bereinigungskosten nach einem Ransomware-Angriff im Jahr 2024 auf 2,73 Mio. US$. Dies entspricht einem Anstieg von fast 1 Mio. US$ ggü. den 1,82 Mio. US$ aus dem Jahr 2023.

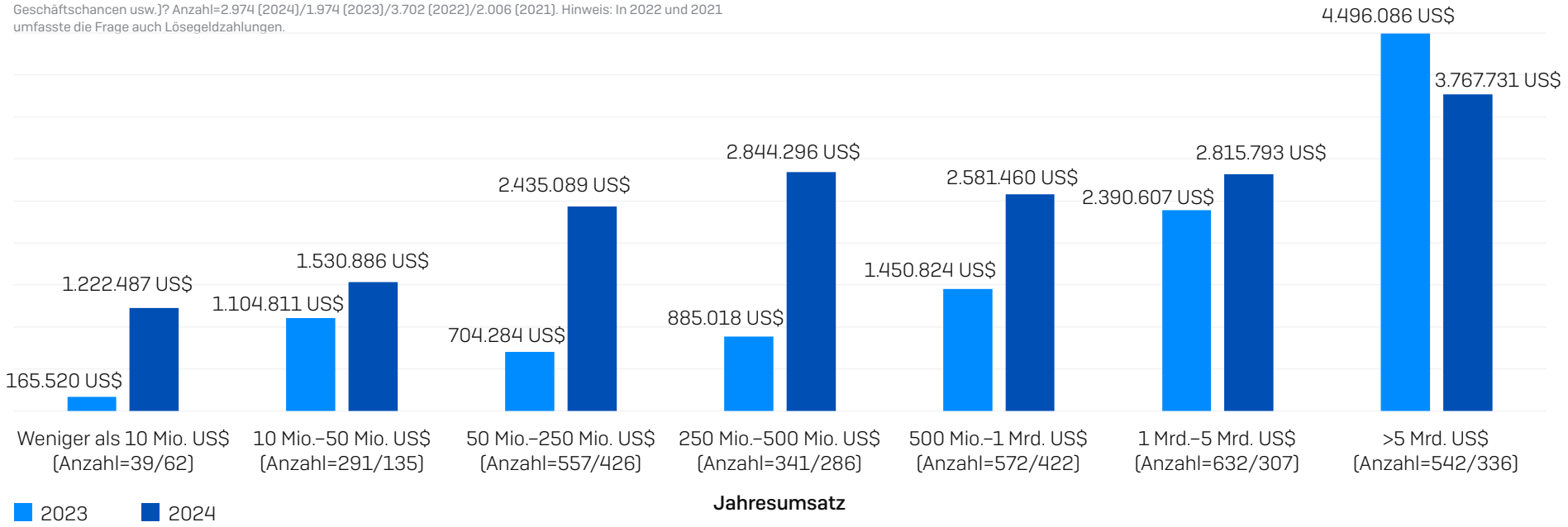
2021	2022	2023	2024
1,85 Mio. US$	1,4 Mio. US$	1,82 Mio. US$	2,73 Mio. US$

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=2.974 (2024)/1.974 (2023)/3.702 (2022)/2.006 (2021). Hinweis: In 2022 und 2021 umfasste die Frage auch Lösegeldzahlungen.

Der größte Anstieg der gesamten Bereinigungskosten ließ sich in den unteren und mittleren Umsatzsegmenten feststellen. Unternehmen mit einem Umsatz von 250 bis 500 Mio. US$ verzeichneten den größten individuellen Anstieg um 2 Mio. US$ (von 885.018 US$ auf 2.885.296 US$).

Auch in Unternehmen mit einem Umsatz von 1 bis 5 Mrd. US$ stiegen die Zahlen (vergleichsweise weniger) um knapp über 400.000 US$ an. Lediglich in großen Unternehmen mit einem Jahresumsatz von mehr als 5 Mrd. US$ waren die Bereinigungskosten rückläufig (4.496.096 US$ ggü. 3.767.731 US$).

Ein Blick auf die mittleren Bereinigungskosten bestätigt diese Entwicklung. Insgesamt verdoppelten sich die mittleren Bereinigungskosten im letzten Jahr von 375.000 US$ auf 750.000 US$. Der Anstieg war vor allem bei den fünf unteren Umsatzsegmenten zu verzeichnen, die durchgehend einen erheblichen Kostenanstieg meldeten. In den beiden Unternehmensgruppen mit den höchsten Umsätzen bewegten sich die Kosten ungefähr auf dem gleichen Niveau wie im Vorjahr.



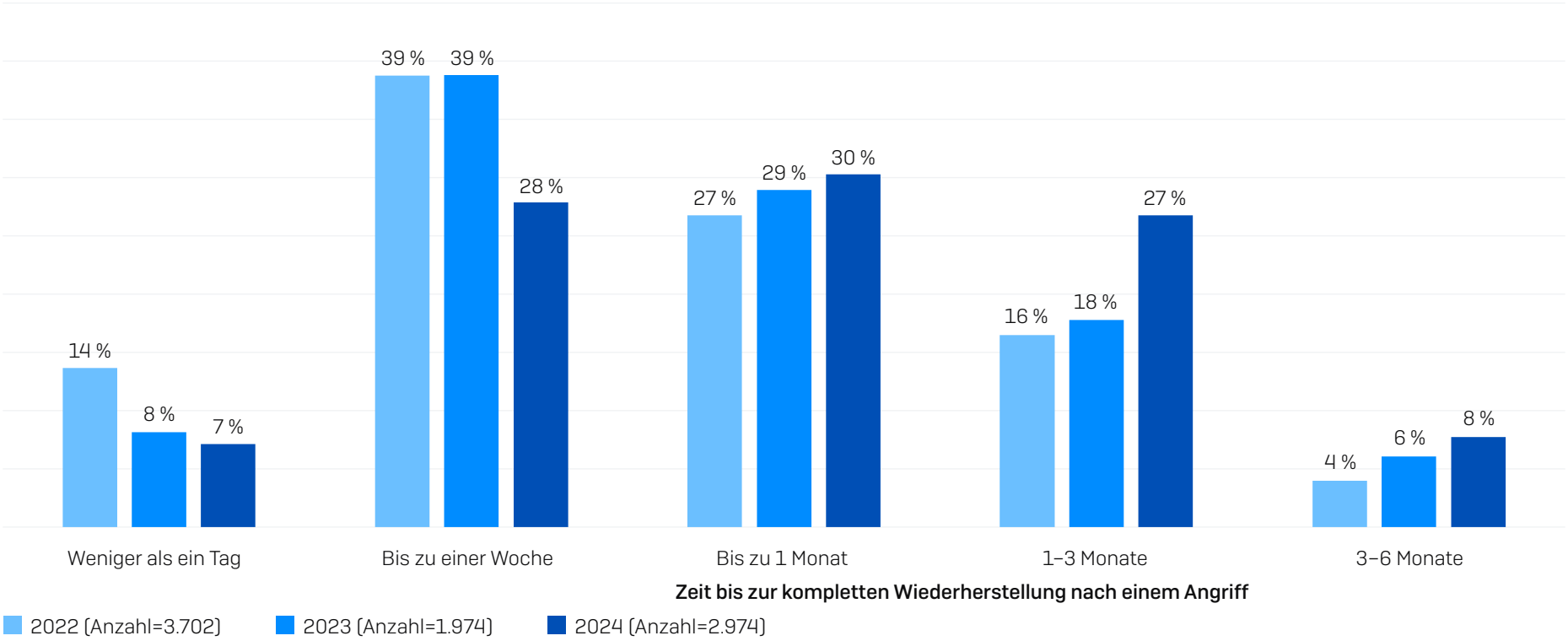
Wie hoch waren die ungefähren Kosten, die Ihrem Unternehmen durch den schwerwiegendsten Ransomware-Angriff entstanden sind (unter Berücksichtigung von Ausfallzeiten, Arbeitsstunden, Geräte- und Netzwerkkosten, entgangenen Geschäftschancen, Lösegeld usw.)? Anzahl=2.974 (2024), 1.974 (2023). Anzahl der 2024/2023 erhaltenen Antworten nach Umsatz jeweils in Klammer

Ausfallzeiten

Die Ausfallzeiten nach einem Ransomware-Angriff nehmen stetig zu. Unsere diesjährige Studie zeigt:

- Bei 35 % der Ransomware-Opfer nahm die Wiederherstellung eine Woche oder weniger in Anspruch, ggü. 47 % im Jahr 2023 und 52 % im Jahr 2022
- Bei einem Drittel (34 %) erstreckte sich die Wiederherstellung über mehr als einen Monat und war damit langwieriger als in 2023 (24 %) und 2022 (20 %)

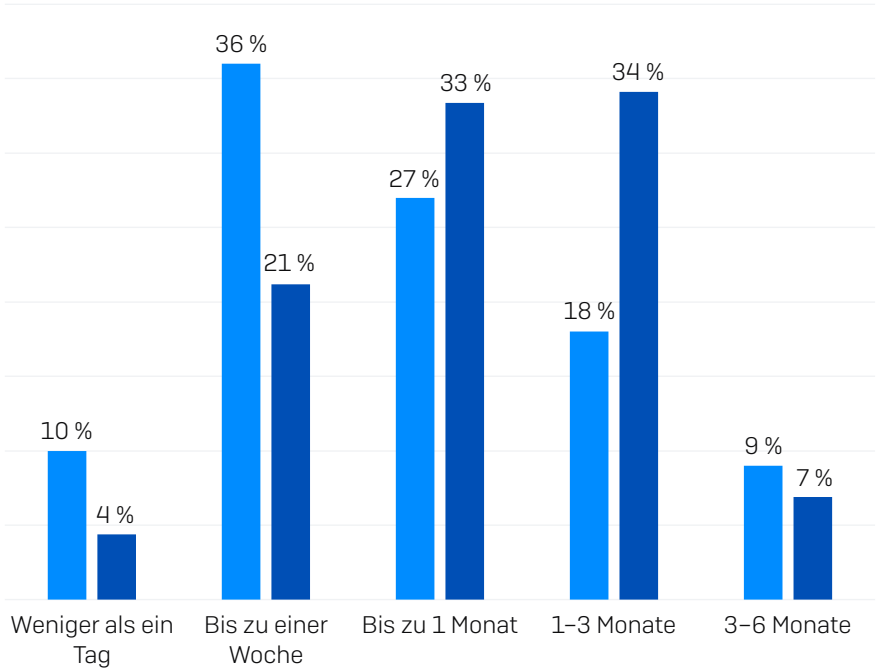
Diese Verlangsamung könnte die zunehmende Komplexität und den Schweregrad der Angriffe widerspiegeln, die einen entsprechend größeren Wiederherstellungsaufwand bedingt haben könnten. Womöglich sind Unternehmen auch immer weniger auf die Wiederherstellung nach einem Vorfall vorbereitet.



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

Ausfallzeiten: Auswirkungen der Kompromittierung von Backups

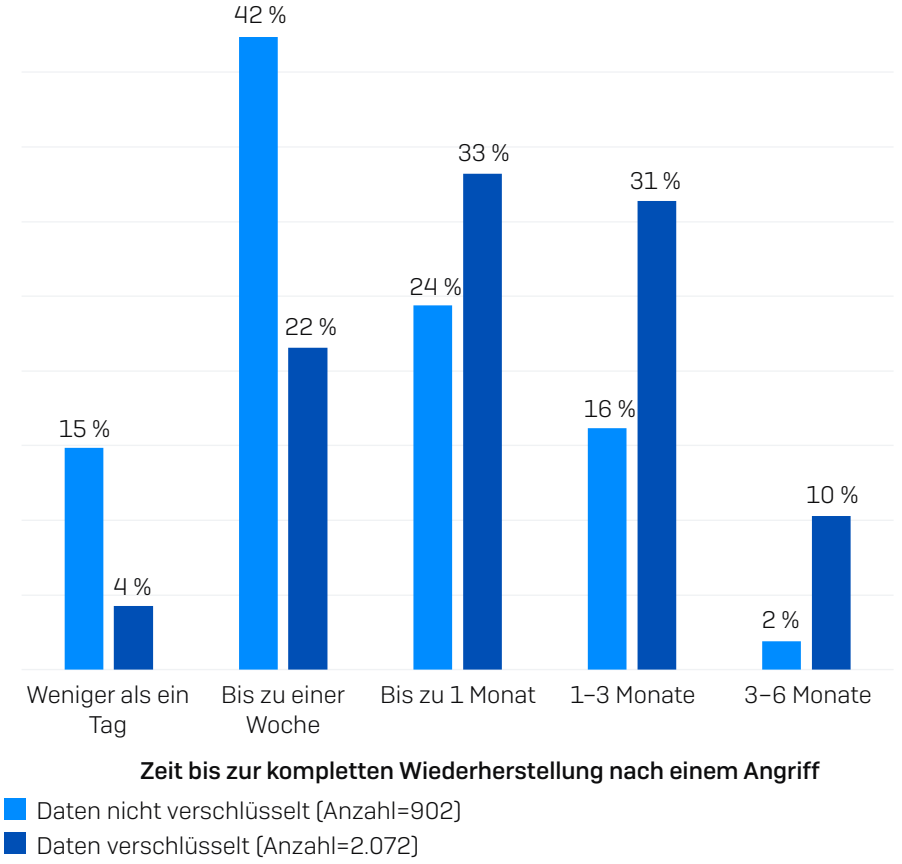
Die Beeinträchtigung Ihrer Backups hat erhebliche Auswirkungen auf die Gesamtausfallzeiten. Fast die Hälfte der Unternehmen, deren Backups intakt blieben, stellten ihre Daten innerhalb einer Woche oder weniger wieder her (46 %), verglichen mit einem Viertel (25 %) der Unternehmen, deren Backups kompromittiert wurden. Wenn Ihre Backups kompromittiert werden, gestaltet sich die Wiederherstellung verschlüsselter Daten wesentlich komplexer. Außerdem ist mit der Erstellung und Sicherung neuer, intakter Backups ein zusätzlicher Aufwand verbunden.



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

Ausfallzeiten: Auswirkungen von Datenverschlüsselung

Es überrascht wahrscheinlich kaum, dass bei einem Angriff, bei dem Daten verschlüsselt werden, die Ausfallzeiten erheblich länger sind. 57 % der Unternehmen, deren Daten nicht verschlüsselt waren, konnten den Angriff innerhalb einer Woche komplett bereinigen. Bei Unternehmen, deren Daten verschlüsselt wurden, lag der prozentuale Anteil bei lediglich 25 %.

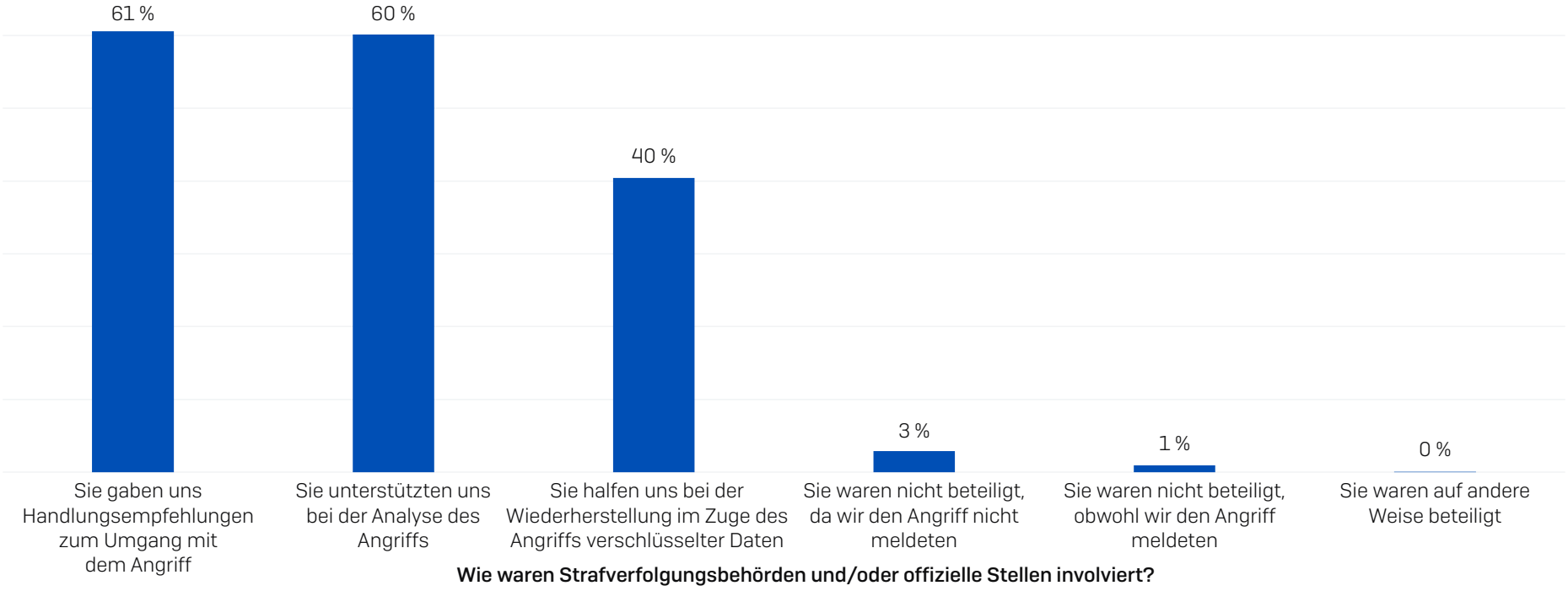


Wie lange hat es gedauert, bis sich Ihr Unternehmen vollständig von dem Ransomware-Angriff erholt hat? Anzahl der erhaltenen Antworten jeweils in Klammer.

Einbindung der Strafverfolgungsbehörden

Die Art und Verfügbarkeit von Unterstützung durch die Strafverfolgungsbehörden bei der Bewältigung eines Ransomware-Angriffs variierten von Land zu Land, ebenso wie die Instrumente zur Meldung eines Cyberangriffs. Beispielsweise können sich betroffene Unternehmen in den USA an die Cybersecurity and Infrastructure Security Agency (CISA), Unternehmen in Großbritannien an das National Cyber Security Centre (NCSC) und australische Unternehmen an das Australian Cyber Security Center (ACSC) wenden. In Europa ist das European Cybercrime Centre (EC3) eine mögliche Anlaufstelle für betroffene Unternehmen.

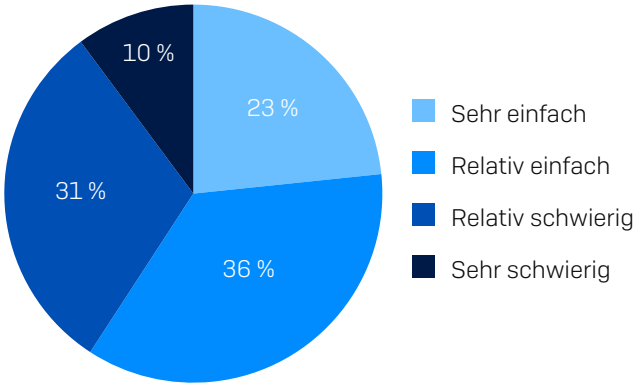
Die Normalisierung von Ransomware spiegelt sich auch darin wider, dass weltweit 97 % der von Ransomware betroffenen Unternehmen sich bei einem Angriff mit den Strafverfolgungsbehörden und/oder offiziellen Regierungsstellen in Verbindung setzten. 61 % gaben an, dass sie Handlungsempfehlungen zum Umgang mit dem Angriff erhielten, 60 % bekamen Hilfe bei der Analyse des Angriffs und 40 % wurden bei der Wiederherstellung nach dem Angriff unterstützt.



Wenn Ihre Organisation/Ihr Unternehmen den Angriff den Strafverfolgungsbehörden und/oder einer offiziellen Regierungsstelle gemeldet hat, wie waren diese dann beteiligt? Anzahl=2.974.

Komplexität der Zusammenarbeit

Ermutigend ist, dass mehr als die Hälfte (59 %) der Befragten, die sich mit Strafverfolgungsbehörden und/oder offiziellen Stellen in Verbindung gesetzt hatten, das Vorgehen als „einfach" einstuften (23 % „sehr einfach", 36 % „relativ einfach"). Lediglich 10 % empfanden den Prozess als „sehr schwierig". 31 % bezeichneten ihn als „relativ schwierig".



Wie einfach oder schwierig war die Zusammenarbeit mit den Strafverfolgungsbehörden und/oder offiziellen Stellen im Zusammenhang mit dem Angriff für Ihr Unternehmen? Anzahl=2.874 (Ohne „Weiß nicht"-Angaben).

Ohne Mitwirkung öffentlicher Stellen

3 % (86 Befragte) meldeten den Angriff aus diversen Gründen nicht. Am häufigsten wurde die Sorge angeführt, dass dies negative Auswirkungen auf ihr Unternehmen haben würde, z. B. Geldstrafen, Kosten oder zusätzliche Arbeit (27 %). Andere wiederum glaubten nicht, dass es ihnen weiterhelfen würde (ebenfalls 27 %). Mehrere Unternehmen schalteten keine offiziellen Stellen ein, da sie das Problem intern beheben konnten.

Wir waren besorgt, dass es negative Auswirkungen auf unsere Organisation haben würde, z. B. Geldstrafen, Kosten, zusätzliche Arbeit	27 %
Wir glaubten nicht, dass es für unsere Organisation von Nutzen wäre, den Angriff zu melden	27 %
Wir waren nicht der Meinung, dass sich offizielle Stellen für den Angriff interessieren würden	22 %
Wir waren zu sehr mit dem Angriff beschäftigt, als dass wir daran gedacht hätten, offizielle Stellen einzubeziehen	21 %
Die Angreifer warnten uns davor, offizielle Stellen einzuschalten	19 %
Wir wussten nicht, welche Strafverfolgungsbehörden oder offiziellen Stellen wir einschalten sollten	10 %
Wir waren nicht gesetzlich verpflichtet, den Angriff zu melden	9 %
Sonstiges (bitte angeben)	3 %
Unsicher	1 %

Warum haben Sie den Angriff nicht den Strafverfolgungsbehörden und/oder offiziellen Stellen gemeldet? (Anzahl=86).

Fazit

Ransomware bleibt eine der größten Bedrohungen für die Sicherheit sämtlicher Unternehmen/Organisationen weltweit. Während die Gesamtangriffsrate in den letzten zwei Jahren zurückging, waren die Auswirkungen der Angriffe schwerwiegender. Da Angreifer ihre Angriffe ständig verbessern und weiterentwickeln, muss die Cyberabwehr der Unternehmen und Organisationen damit Schritt halten.

Prävention. Der beste Ransomware-Angriff ist ein abgewehrter Angriff, bei dem die Angreifer sich keinen Zugang zu Ihrem Unternehmen oder Ihrer Organisation verschaffen konnten. Da ein Drittel der Angriffe mit der Ausnutzung ungepatchter Schwachstellen beginnt, müssen Sie Ihre Angriffsfläche kontrollieren und Patches risikobasiert priorisieren. Alle Unternehmen und Organisationen sollten sich mit Multi-Faktor-Authentifizierung (MFA) vor dem Missbrauch von Zugangsdaten schützen. Regelmäßige Benutzertrainings zur Erkennung von Phishing und bösartigen E-Mails sind weiterhin unerlässlich.

Schutz. Ein starkes Sicherheitsfundament ist ein Muss, einschließlich Endpoint-, E-Mail- und Firewall-Technologien. Endpoints (einschließlich Server) sind das Hauptziel von Ransomware-Akteuren. Stellen Sie daher sicher, dass diese umfassend geschützt sind, unter anderem mit speziellem Anti-Ransomware-Schutz, um bösartige Verschlüsselungen zu stoppen und rückgängig zu machen. Sicherheitstools müssen richtig konfiguriert und eingesetzt werden, um optimalen Schutz zu bieten. Setzen Sie daher auf sofort einsetzbare Lösungen mit einfachen Mechanismen zur Kontrolle Ihrer Sicherheitslage. Komplizierte und schwer zu implementierende Schutzlösungen können das Risiko schnell erhöhen, anstatt es zu reduzieren.

Detection and Response. Je eher Sie einen Angriff stoppen, desto besser. Wenn Sie Angreifer in Ihrer Umgebung erkennen und stoppen, bevor sie Ihre Backups kompromittieren oder Ihre Daten verschlüsseln, können Sie die Auswirkungen des Angriffs erheblich abmildern.

Planung und Vorbereitung. Mit einem Incident-Response-Plan, den sie zur Reaktion auf Vorfälle gezielt anwenden können, reduzieren Sie erheblich die Auswirkungen eines schwerwiegenden Vorfalls. Üben Sie die Wiederherstellung von Daten aus Backups regelmäßig, damit Sie im Falle eines Angriffs schnell reagieren können.

Sie möchten mehr darüber erfahren, wie Sophos Sie bei der Optimierung Ihrer Ransomware-Abwehr unterstützen kann? Sprechen Sie mit einem unserer Ansprechpartner oder besuchen Sie unsere Website unter www.sophos.de

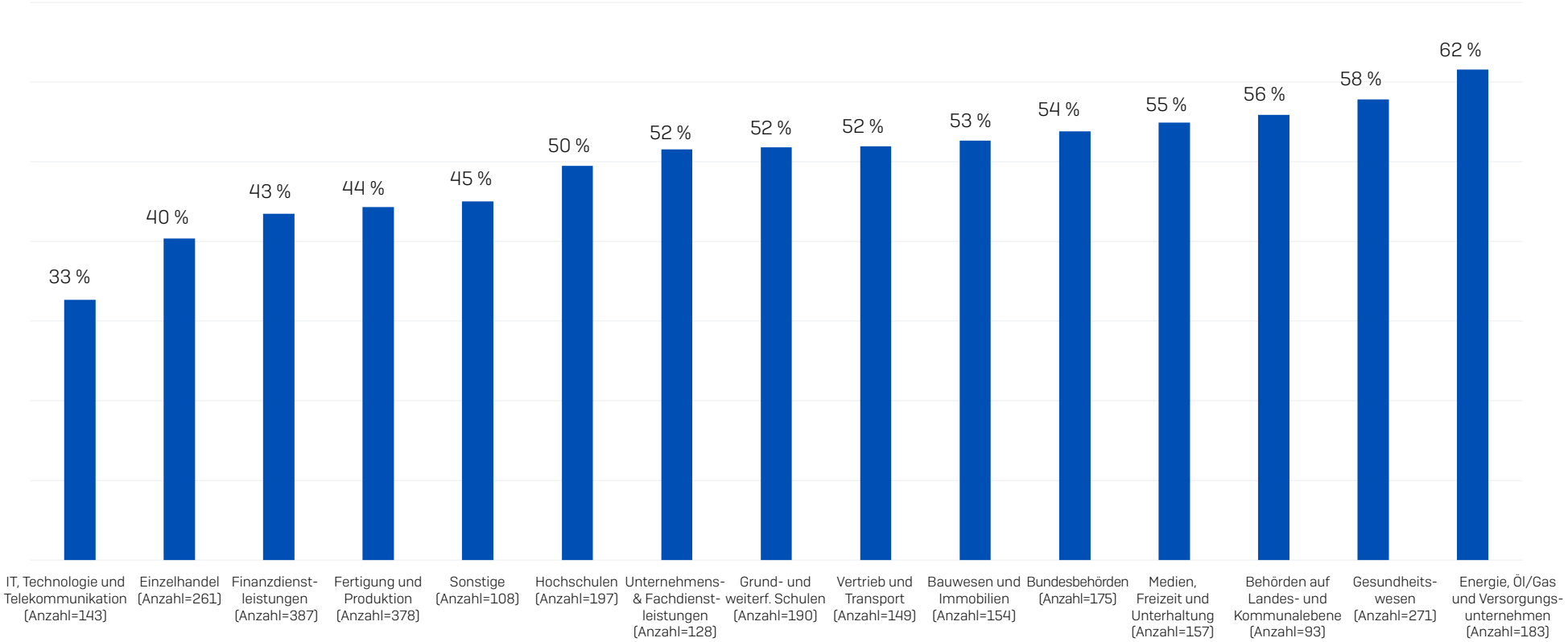
Über Vanson Bourne

Vanson Bourne ist ein unabhängiger Spezialist für Marktforschung in der Technologiebranche. Den Ruf, solide und vertrauenswürdige forschungsbasierte Analysen zu verfassen, verdankt das Unternehmen seinen strengen Forschungsgrundsätzen sowie der Fähigkeit, die Meinungen von Entscheidungsträgern in allen technischen und nicht-technischen Unternehmensbereichen, Branchen und bedeutenden Märkten einzuholen. Nähere Informationen finden Sie unter www.vansonbourne.com

Anhang

Prozentsatz der betroffenen Computer nach Branche

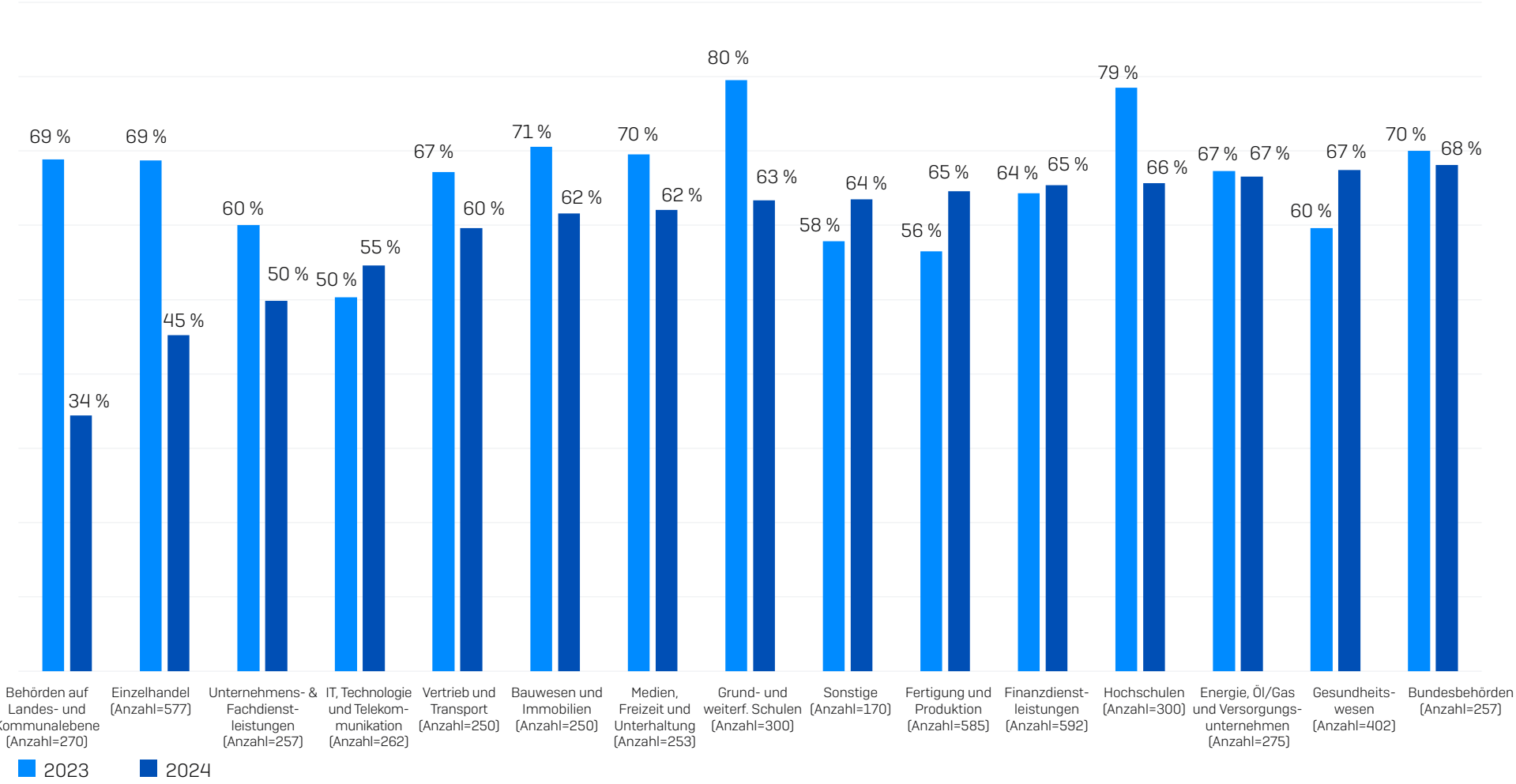
Prozentsatz der betroffenen Geräte



Wie viel Prozent der Computer in Ihrem Unternehmen waren im letzten Jahr von Ransomware betroffen? Anzahl=2.974 Unternehmen, die Opfer von Ransomware waren. Anzahl der erhaltenen Antworten nach Branche jeweils in Klammer.

Häufigkeit von Ransomware-Vorfällen nach Branche

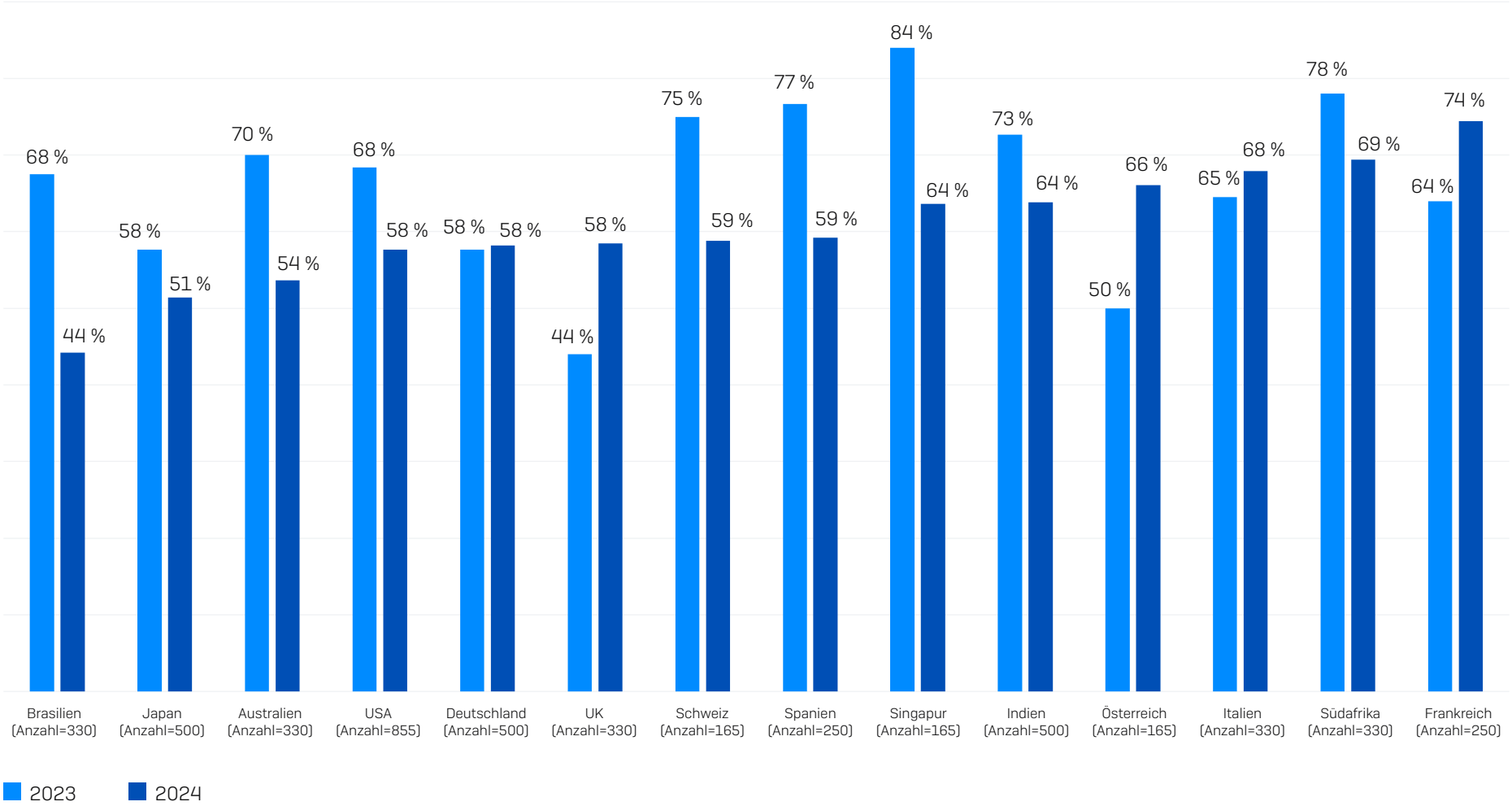
Prozentsatz der Unternehmen, die im letzten Jahr von Ransomware betroffen waren



War Ihr Unternehmen/Ihre Organisation im letzten Jahr von Ransomware betroffen? Ja. Anzahl=5.000 (2024), 3.000 (2023), 5.600 (2022). Anzahl der in 2024 erhaltenen Antworten nach Branche jeweils in Klammer.

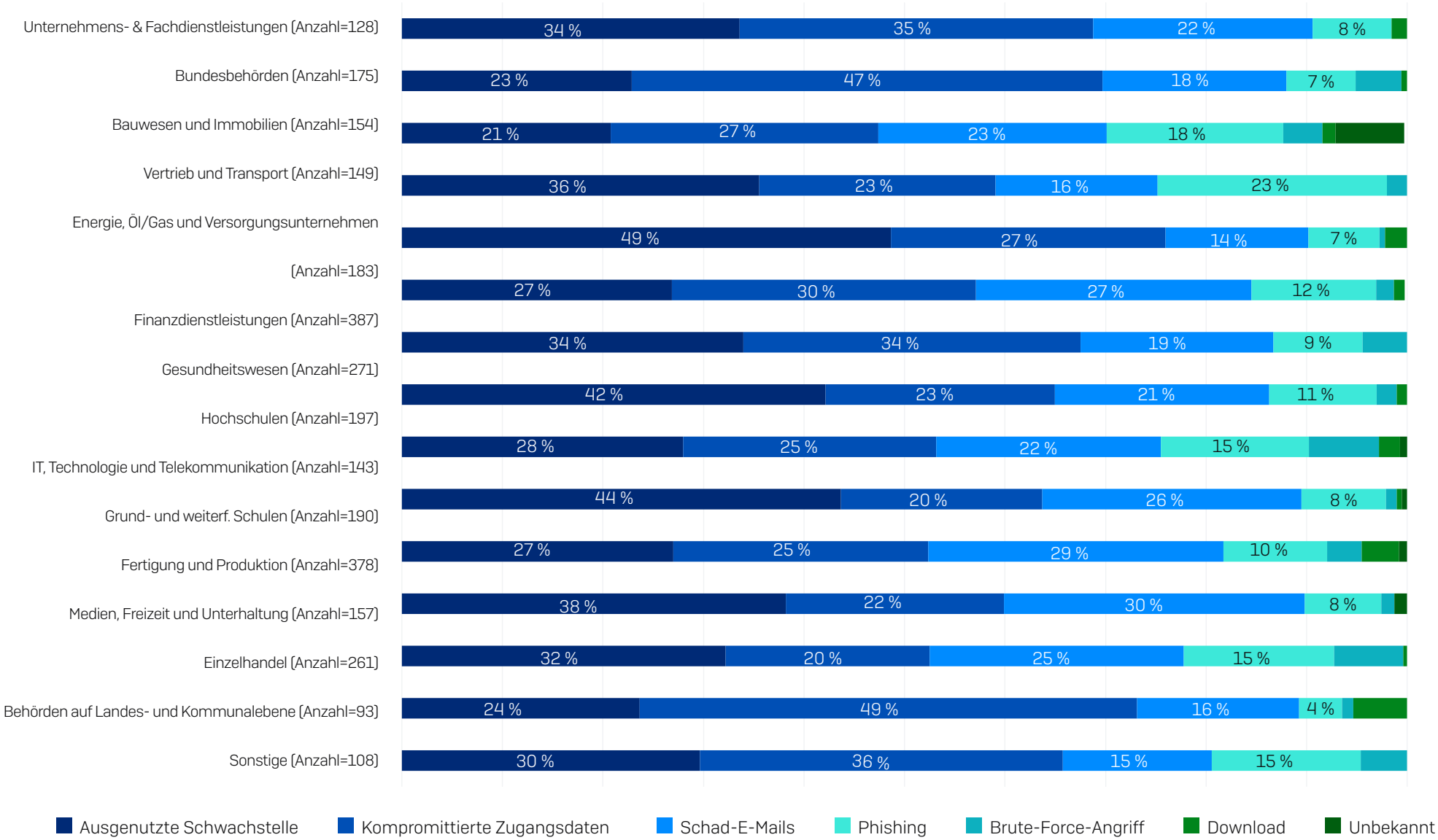
Häufigkeit von Ransomware-Vorfällen nach Land

Prozentsatz der Unternehmen, die im letzten Jahr von Ransomware betroffen waren



Wurde Ihr Unternehmen/Ihre Organisation im letzten Jahr von Ransomware getroffen? Ja. Anzahl=5.000 (2024), 3.000 (2023). Anzahl der in 2024 erhaltenen Antworten nach Land jeweils in Klammer.

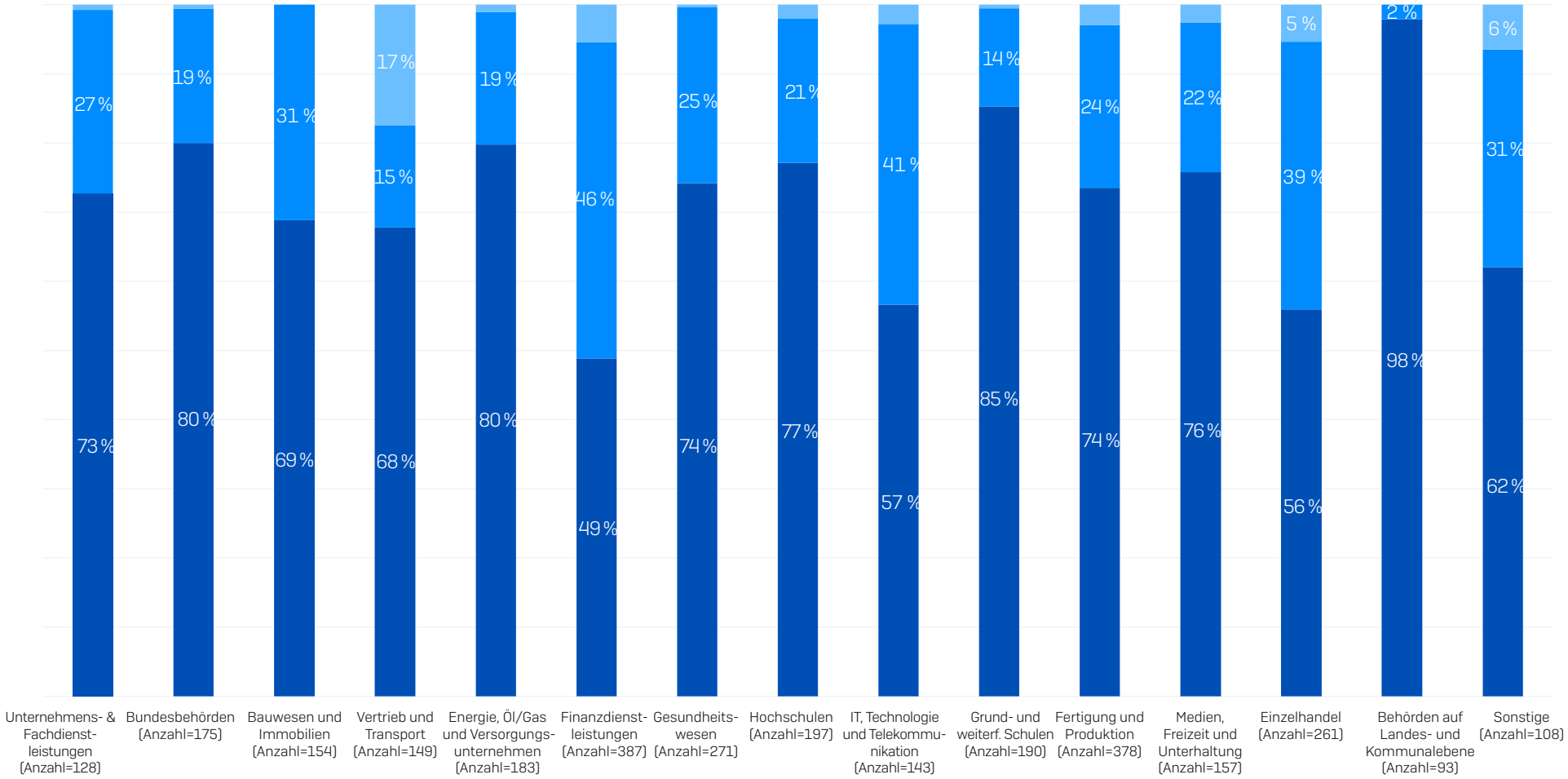
Angriffsursache nach Branche



Kennen Sie die Ursache des Ransomware-Angriffs auf Ihr Unternehmen im vergangenen Jahr? Anzahl=2.974 von Ransomware betroffene Unternehmen.

Datenverschlüsselungsrate nach Branche

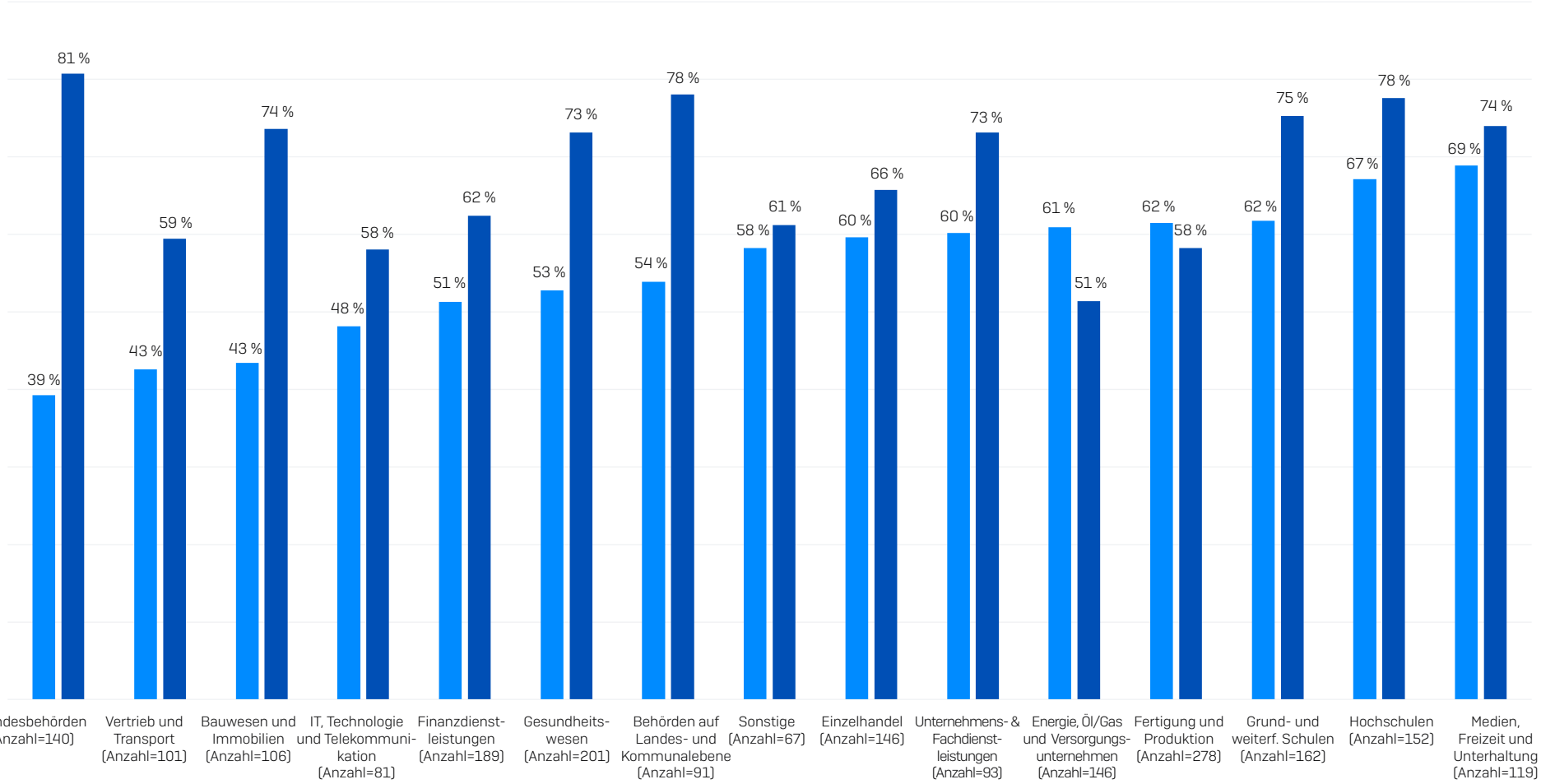
Wahrscheinlichkeit, dass Daten im Zuge eines Angriffs verschlüsselt wurden



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

Methode zur Datenwiederherstellung nach Branche

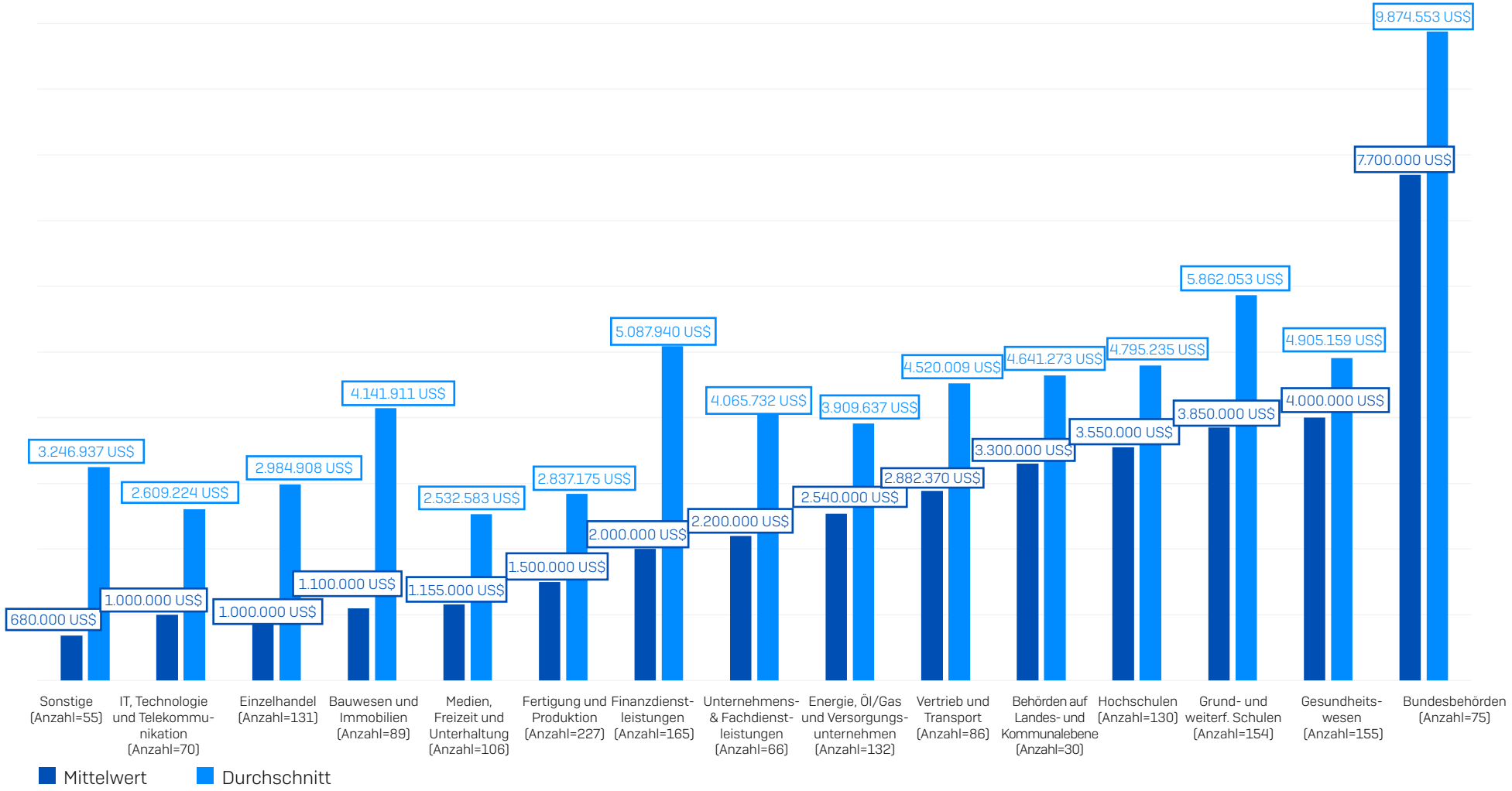
Wie häufig werden Daten über Backups und Zahlung des Lösegelds wiederhergestellt?



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. Angeordnet nach der Bereitschaft, das Lösegeld zu zahlen.

Lösegeldforderungen nach Branche

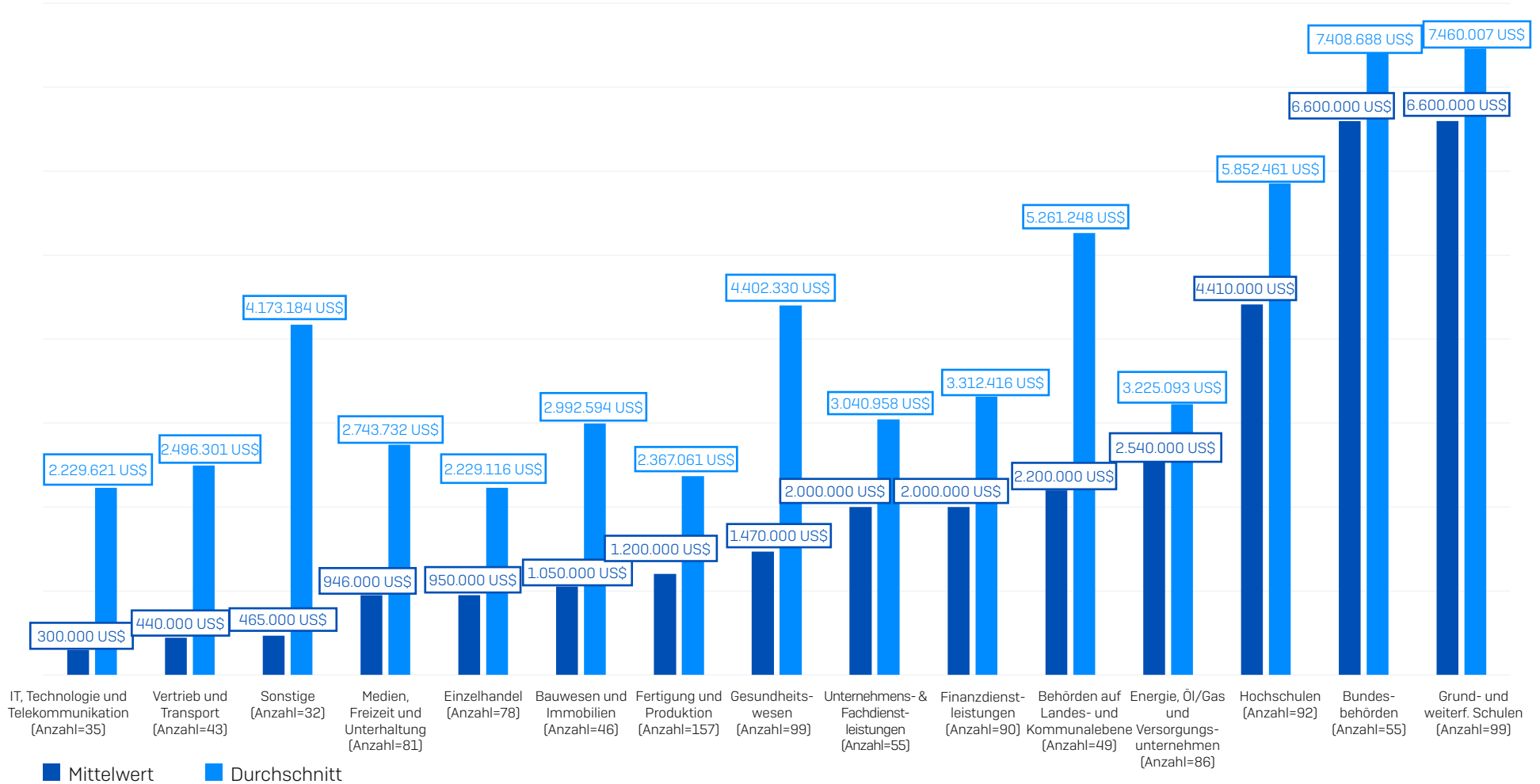
Lösegeldforderungen



Wie viel Lösegeld forderten die Angreifer? Anzahl der erhaltenen Antworten jeweils in Klammer. Angeordnet nach der mittleren Forderung.

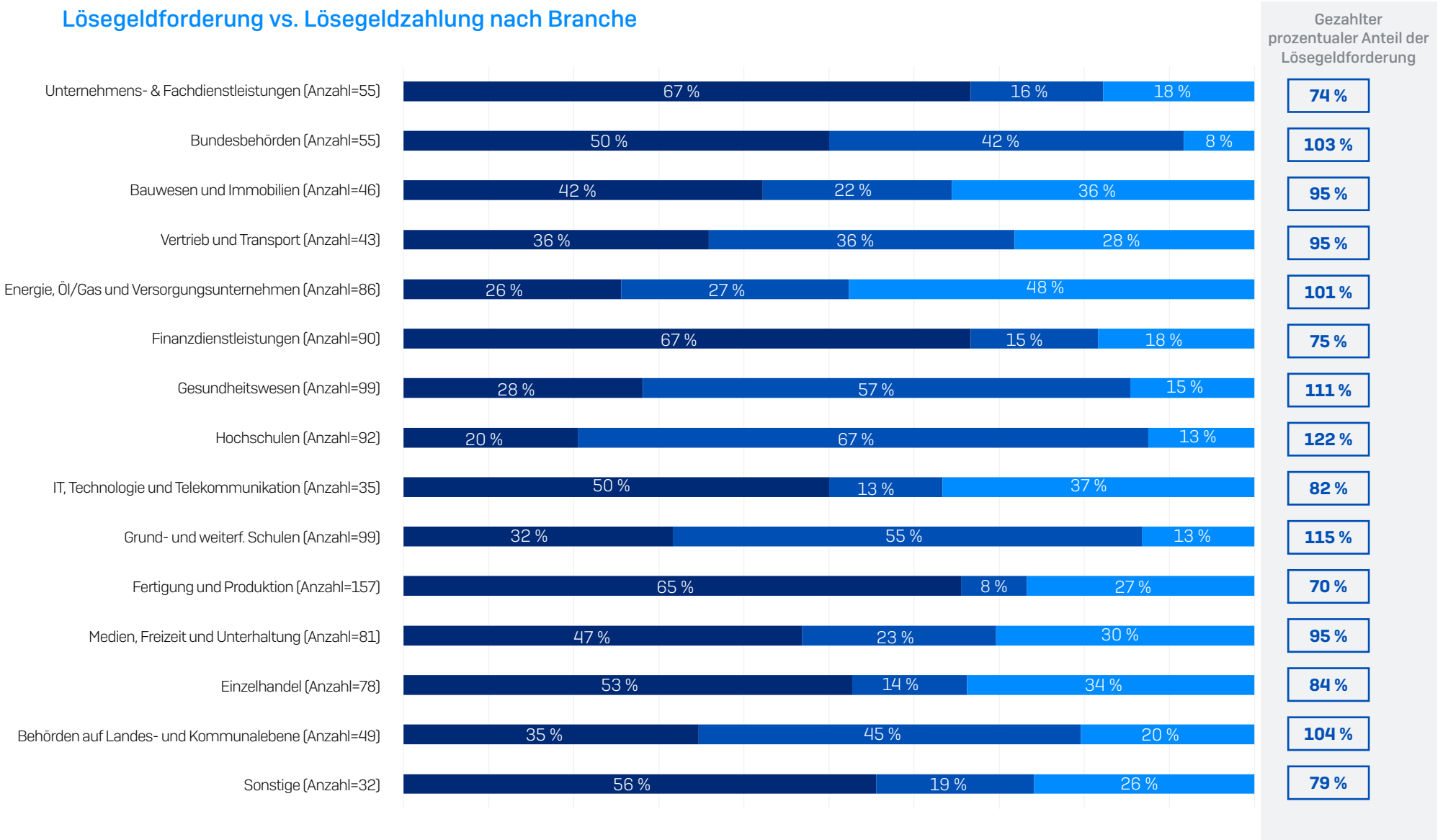
Lösegeldzahlung nach Branche

Lösegeldzahlung



Wie viel Lösegeld wurde den Angreifern gezahlt? Anzahl der erhaltenen Antworten jeweils in Klammer. Angeordnet nach der mittleren Zahlung.

Lösegeldforderung vs. Lösegeldzahlung nach Branche



Wie viel Lösegeld forderten die Angreifer? Wie viel Lösegeld wurde den Angreifern gezahlt? Anzahl der erhaltenen Antworten jeweils in Klammer.

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.

2024-04-16 (WP-PC)

SOPHOS