SOPHOS
Cybersecurity delivered.

Ransomware-Report 2022

Ergebnisse einer unabhängigen Befragung von 5.600 IT-Entscheidern in mittelständischen Unternehmen aus 31 Ländern.

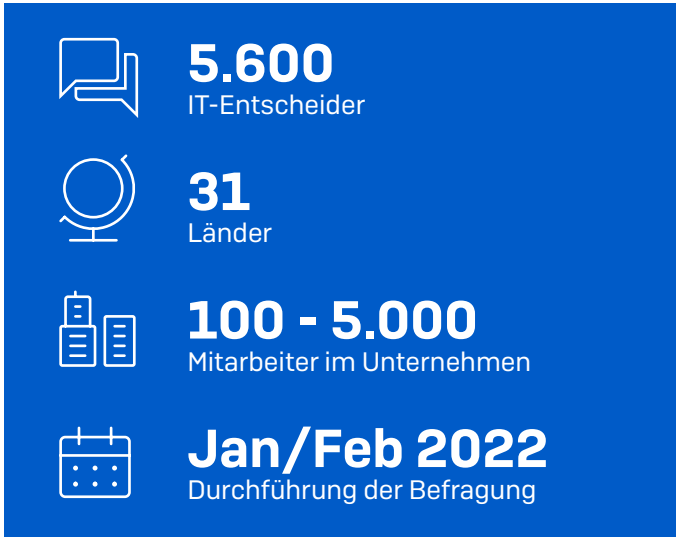
Sophos-Whitepaper. April 2022

Einleitung

Jedes Jahr befragt Sophos im Rahmen einer Studie IT-Experten aus aller Welt zu ihren Erfahrungen mit Ransomware. Die diesjährigen Ergebnisse zeigen, dass die Bedrohungslandschaft immer komplexer wird. Auch die finanziellen und betrieblichen Belastungen, mit denen die Betroffenen zu kämpfen haben, nehmen zu. Darüber hinaus beleuchtet die Studie das Thema Cyberversicherung und Ransomware sowie die Rolle der Versicherer, wenn es darum geht, dass Unternehmen ihre Cybersicherheit ausbauen.

Über die Studie

Sophos beauftragte das Marktforschungsunternehmen Vanson Bourne mit der Durchführung einer unabhängigen Befragung von 5.600 IT-Fachleuten in mittelständischen Unternehmen (100 – 5.000 Mitarbeiter) aus 31 Ländern. Die Befragung fand im Januar und Februar 2022 statt. Die Umfrageteilnehmer wurden gebeten, sich bei der Beantwortung der Fragen auf ihre Erfahrungen innerhalb des vergangenen Jahres zu beziehen.

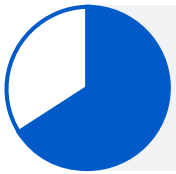


Angriffe nehmen zu, werden komplexer und folgenschwerer

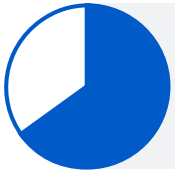
Im letzten Jahr waren 66 % der Unternehmen von Ransomware betroffen, im Vergleich zu 37 % in 2020. Innerhalb eines Jahres ist dies ein Anstieg von 78 %. Ein Indiz dafür, dass Cyberkriminelle immer besser in der Lage sind, großangelegte Angriffe auszuführen. Darin spiegelt sich vermutlich auch der wachsende Erfolg des Ransomware-as-a-Service-Modells wider, das die Reichweite von Ransomware deutlich vergrößert. Denn es sind weniger Kenntnisse erforderlich, um einen Angriff zu lancieren. [Anmerkung: „von Ransomware betroffen" bedeutet hier, dass der Angriff auf ein oder mehrere Geräte erfolgte, es dabei aber nicht unbedingt zu einer Verschlüsselung kam.]

Auch die Verschlüsselung von Daten gelingt den Angreifern immer häufiger. Im Jahr 2021 wurden bei 65 % der Angriffe Daten verschlüsselt – im Jahr zuvor lag die Rate noch bei 54 %. Allerdings gab es weniger sogenannte Extortion-Angriffe, bei denen Daten nicht verschlüsselt werden, sondern die Angreifer damit drohen, Daten zu veröffentlichen. Diese Zahl sank von 7 % auf 4 %.

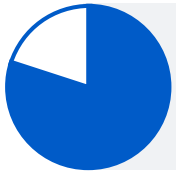
Die Erfolgsquote der Angreifer steigt. Dieser Trend geht einher mit einem immer komplexeren Bedrohungsumfeld: Im letzten Jahr verzeichneten 57 % der Befragten eine Zunahme an Angriffen, 59 % bestätigten eine zunehmende Komplexität und 53 % schwerwiegendere Folgen. 72 % verzeichneten einen Anstieg bei mindestens einem dieser Punkte.



66 %
wurden Opfer eines Ransomware-Angriffs



65 %
der Angriffe führten zur Datenverschlüsselung



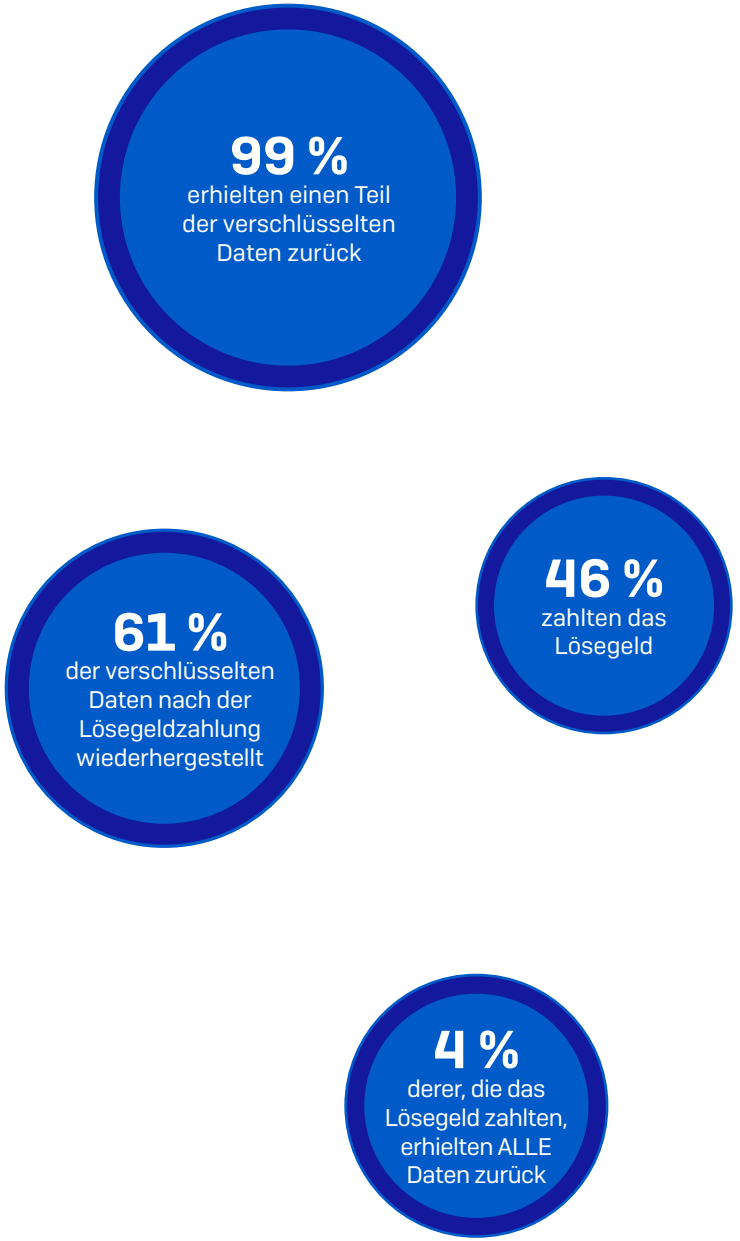
72 %
verzeichneten eine Zunahme bei der Zahl/Komplexität/Schwere der Angriffe

Mehr Erfolg beim Wiederherstellen der Daten nach einem Angriff

Mit der zunehmenden Verbreitung von Ransomware gelingt es Unternehmen mittlerweile offenbar besser, mit den Folgen eines Angriffs umzugehen. Fast alle Unternehmen, die im letzten Jahr von Ransomware betroffen waren (99 %), erhielten ihre verschlüsselten Daten teilweise zurück; ein leichter Anstieg zum Jahr davor, damals waren es noch 96 %.

73 % der Unternehmen, deren Daten verschlüsselt wurden, nutzten Backups – die am häufigsten verwendete Methode zur Wiederherstellung von Daten. Gleichzeitig gaben 46 % der Befragten an, dass sie Lösegeld gezahlt haben, um ihre Daten wiederherzustellen. Diese Zahlen zeigen, dass viele Unternehmen mehrere Ansätze verfolgen, um schneller und effizienter den Betrieb wieder aufnehmen zu können. Insgesamt nutzte fast die Hälfte (44 %) der Befragten, deren Unternehmensdaten verschlüsselt wurden, mehrere Methoden zur Wiederherstellung der Daten.

Mit der Zahlung des Lösegelds erhalten die Unternehmen fast immer einen Teil ihrer Daten zurück. Doch der Prozentsatz der wiederhergestellten Daten nach erfolgter Lösegeldzahlung ist zurückgegangen. Im Durchschnitt erhielten Unternehmen, die das Lösegeld zahlten, nur 61 % ihrer Daten zurück, gegenüber 65 % im Jahr 2020. Und nur 4 % der Unternehmen, die der Lösegeldforderung nachkamen, erhielten ALLE Daten zurück. Im Vorjahr waren es noch 8 %.



Höhere Lösegeldsummen werden gezahlt

965 der Befragten, deren Unternehmen von Ransomware betroffen war und das Lösegeld gezahlt hatte, nannten die genauen Lösegeldsummen. Dadurch wurde ersichtlich, dass die durchschnittlich gezahlten Lösegeldsummen deutlich höher geworden sind.

So hat sich der Anteil der Opfer, die Lösegeld in Höhe von 1 Million US-Dollar oder mehr zahlten, fast verdreifacht: von 4 % im Jahr 2020 auf 11 % im Jahr 2021. Parallel dazu sank der Prozentsatz der Unternehmen, die weniger als 10.000 US-Dollar zahlten, von jedem dritten Unternehmen (34 %) im Jahr 2020 auf jedes fünfte (21 %) im Jahr 2021.

Insgesamt belief sich die durchschnittliche Lösegeldzahlung auf 812.360 US-Dollar, ein 4,8-facher Anstieg gegenüber dem Durchschnitt von 170.000 US-Dollar im Jahr 2020 (laut Angaben von 282 Befragten). Zwar sind für diese Gesamtsumme 15 achtstellige Beträge mit verantwortlich, doch es ist generell ein klarer Aufwärtstrend bei den Lösegeldforderungen zu erkennen. Je nach Branche gibt es enorme Unterschiede. Die Cyberkriminellen verlangten die höchsten Summen von denjenigen, die sie als am zahlungsfähigsten erachten:

- Die **höchsten** Lösegeldsummen wurden im Bereich Fertigung und Produktion gezahlt, im Schnitt 2,04 Mio. US-Dollar (Anzahl=38), sowie im Bereich Energie, Öl/Gas und Versorgungsunternehmen, im Schnitt 2,03 Mio. US-Dollar (Anzahl=91)
- Am **niedrigsten** waren die Lösegeldzahlungen im Gesundheitswesen (Anzahl=83) mit durchschnittlich 197.000 US-Dollar sowie bei Behörden auf Landes- und Kommunalebene (Anzahl=20) mit 214.000 US-Dollar

In Italien, wo Lösegeldzahlungen bei Cyberangriffen gesetzlich verboten sind, bekannten 43 % der Unternehmen, deren Daten verschlüsselt wurden, sie hätten Lösegeld gezahlt (Anzahl=6). So zeigt die Studie, dass gesetzliche Schranken allein nicht ausreichen, um Lösegeldzahlungen zu verhindern.

3x
Anstieg des Anteils der Unternehmen/Behörden, die Lösegeld in Höhe von 1 Mio. US-Dollar oder mehr zahlten

21 %
zahlten ein Lösegeld, das niedriger war als 10.000 US-Dollar

812.360 $
durchschnittliche Lösegeldzahlung (ohne Extremwerte)

Fertigung, Versorgung
höchste durchschnittliche Lösegeldzahlung (2 Mio. US-Dollar)

Gesundheitswesen
niedrigste durchschnittliche Lösegeldzahlung (197.000 US-Dollar)

Ransomware hat gravierende Auswirkungen auf Geschäft und Betrieb

Die Lösegeldsummen sind nur ein Teil des Problems. So führen Ransomware-Angriffe nicht nur zu verschlüsselten Datenbanken und Geräten. 90 % der Unternehmen, die im letzten Jahr von Ransomware betroffen waren, gaben an, dass der schwerste Angriff ihre Betriebsfähigkeit beeinträchtigt habe. Darüber hinaus gaben 86 % der privatwirtschaftlichen Unternehmen an, dass sie dadurch Geschäftseinbußen oder Umsatzverluste hinnehmen mussten.

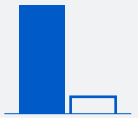
Insgesamt zahlten Unternehmen im Jahr 2021 durchschnittlich 1,4 Millionen US-Dolllar, um die Auswirkungen des letzten Ransomware-Angriffs zu beheben. Im Jahr 2020 waren es noch 1,85 Mio. US-Dollar. Dieser erfreuliche Rückgang spiegelt vermutlich wider, dass mit der zunehmenden Verbreitung von Ransomware auch der Reputationsschaden durch einen Angriff geringer geworden ist. Gleichzeitig sind die Versicherungsanbieter besser in der Lage, den Betroffenen schnell und effektiv zu helfen und somit die Kosten zur Bedrohungsbeseitigung zu senken.

Auch erwähnenswert: Wenn Lösegeld gezahlt wird, übernimmt dies häufig das Versicherungsunternehmen. Darauf gehen wir im Folgenden noch näher ein.

Im Schnitt erholten sich Unternehmen, die im letzten Jahr Opfer von Angriffen wurden, erst nach einem Monat vom schwersten Angriff – eine lange Zeit für die meisten Unternehmen. Im Hochschulwesen und bei Bundesbehörden waren es sogar 2 von 5 Befragten, die eine Wiederherstellungszeit von über einem Monat angaben. Am schnellsten erholten sich die Unternehmen aus den Bereichen Fertigung und Produktion (10 % benötigten mehr als einen Monat) und Finanzdienstleistungen (12 % benötigten mehr als einen Monat). Dies ist wahrscheinlich auf eine umfangreiche Planung und Vorbereitung der Wiederherstellungsmaßnahmen zurückzuführen.

Zudem setzen einige Unternehmen weiterhin auf unwirksame Abwehrmaßnahmen. Von den Befragten, deren Unternehmen im letzten Jahr nicht von Ransomware betroffen waren und auch künftig nicht damit rechnen, begründeten 72 % dies mit Methoden, die nicht vor Angriffen schützen: 57 % nannten Backups und 37 % eine Cyberversicherung als Grund, warum sie nicht mit einem Angriff rechnen, wobei einige beide Optionen wählten. Diese Ansätze helfen den Unternehmen zwar dabei, sich von einem Angriff zu erholen, aber sie verhindern ihn nicht im Voraus.

90 %
wurden durch den Angriff in ihrer Betriebsfähigkeit beeinträchtigt



86 %
verzeichneten Geschäftseinbußen/ Umsatzverluste

1,4 Mio. $
durchschnittliche Kosten für die Behebung der Angriffs-Folgen

1 Monat
durchschnittlich benötigte Zeit bis zur kompletten Wiederherstellung nach einem Angriff

72 %
verlassen sich auf Methoden, die einen Angriff nicht verhindern

Budgets und Ressourcen zur Abwehr von Ransomware werden nicht effektiv genutzt

Die Studie macht deutlich, dass das Problem nicht einfach nur mit mehr Personal und Geld zu lösen ist. Vielmehr gilt es, in die richtigen Technologien zu investieren. und zu wissen, wie man diese effektiv einsetzt.

64 % der Unternehmen, die im letzten Jahr von Ransomware betroffen waren, gaben an, dass ihr Budget für Cybersicherheit über dem Bedarf läge, während weitere 24 % meinten, dass ihr Budget angemessen sei. Ebenso erklärten 65 % der Unternehmen, die Ransomware zum Opfer gefallen waren, dass sie mehr Mitarbeiter für die Cybersicherheit hätten, als sie benötigten, und 23 % waren der Ansicht, dass ihre Personaldecke stimme. Diese Ergebnisse deuten darauf hin, dass es für viele Unternehmen schwierig ist, ihre Ressourcen angesichts des zunehmenden Umfangs und der Komplexität der Angriffe effektiv einzusetzen.

Die Studie lässt auch darauf schließen, dass Unternehmen sich möglicherweise nicht bewusst sind, dass sie nicht über die erforderlichen Kenntnisse verfügen, um auf die neuesten Angriffsmethoden reagieren zu können: 58 % der Unternehmen, die von Ransomware betroffen waren, gaben an, dass sie ihre Protokolle fast immer vollständig/vollständig überprüfen würden, um verdächtige Signale oder Aktivitäten zu erkennen, und 56 % sagten, dass sie fast immer vollständig/vollständig über die neuesten Angriffs-Tools/-Methoden informiert seien.

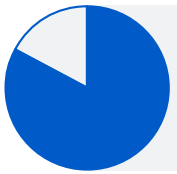
Umgekehrt beruht die Zuversicht von Unternehmen, die im vergangenen Jahr nicht von Ransomware betroffen waren und nicht mit einem künftigen Angriff rechnen, insbesondere darauf, dass sie über geschulte IT-Sicherheitsexperten oder ein internes Security Operations Center (SOC) verfügen, um Angriffe zu stoppen.

Ransomware steigert Nachfrage nach Cyberversicherungen

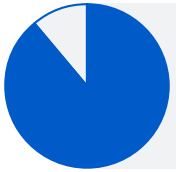
Vier von fünf mittelständischen Unternehmen haben eine Cyberversicherung gegen Ransomware. Während jedoch 83 % der Befragten sagen, ihr Unternehmen habe eine Cyberversicherung, die bei einem Ransomware-Angriff die Kosten übernehme, sagen 34 %, es gebe in ihrer Police Ausnahmen/Ausschlüsse. Unternehmen im Bereich Energie, Öl/Gas und Versorgung sind am ehesten versichert (89 %), dicht gefolgt vom Einzelhandel (88 %). Die Akzeptanz von Cyberversicherungen steigt mit der Größe des Unternehmens: 88 % der Unternehmen mit 3.001 bis 5.000 Mitarbeitern haben eine Cyberversicherung, im Vergleich zu 73 % der Unternehmen mit 100 bis 250 Mitarbeitern.

Unternehmen, die im letzten Jahr von Ransomware betroffen waren, haben mit sehr viel höherer Wahrscheinlichkeit eine Cyberversicherung als solche, die nicht Opfer eines Angriffs wurden. Von den betroffenen Unternehmen haben 89 % eine Cyberversicherung, bei den nicht betroffenen Unternehmen sind es 70 %. Ursache und Wirkung sind hier nicht eindeutig zuzuordnen. Möglicherweise hat ein Ransomware-Vorfall viele Unternehmen dazu veranlasst, eine Versicherung abzuschließen, um die Folgen künftiger Angriffe abzufedern. Oder die Angreifer nehmen Unternehmen und Einrichtungen ins Visier, von denen sie wissen, dass diese versichert sind, um so ihre Chancen auf eine Lösegeldzahlung zu erhöhen. Möglich ist auch, dass einige Unternehmen eine Versicherung abgeschlossen haben, um bekannte Schwachstellen in ihrer Abwehr auszugleichen. Wahrscheinlich handelt es sich um eine Kombination aller drei Optionen.

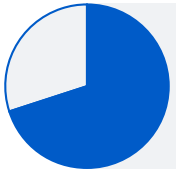
Bei den Unternehmen, die nicht betroffen waren und auch nicht mit einem Angriff rechnen, haben nur 61 % einen Versicherungsschutz. Da viele dieser Unternehmen auf Ansätze vertrauen, die Ransomware nicht stoppen, müssen sie bei einem Vorfall für alle Folgekosten aufkommen.



83 %
haben eine Cyberversicherung gegen Ransomware



89 %
der von Ransomware Betroffenen haben eine Cyberversicherung



70 %
der nicht von Ransomware Betroffenen haben eine Cyberversicherung

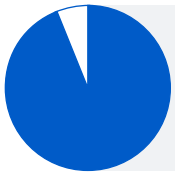
Unternehmen stärken ihre Cyberabwehr für bessere Versicherungsbedingungen

94 % der Unternehmen, die eine Cyberversicherung abgeschlossen haben, gaben an, dass sich die Konditionen beim Versicherungsschutz im letzten Jahr verändert hätten.

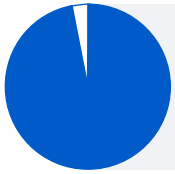
- 54 % gaben an, dass sie jetzt ein höheres Maß an Cybersicherheit nachweisen müssten, um eine Versicherung abschließen zu können
- 47 % meinten, dass die Policen jetzt komplexer seien
- 40 % meinten, dass weniger Versicherer eine Cyberversicherung anbieten
- 37 % gaben an, dass der Bearbeitungsprozess länger dauere
- 34 % gaben an, dass der Versicherungsschutz teurer geworden sei

Da die Preise bei den Cyberversicherungen erst im zweiten und dritten Quartal 2021 anstiegen, waren die Auswirkungen für viele der Befragten zum Zeitpunkt der Umfrage vermutlich noch nicht spürbar.

Der Markt für Cyberversicherungen verhärtet sich und es wird schwieriger, Schäden abzusichern. Daher haben 97 % der Unternehmen mit Cyberversicherungsschutz ihre Cyberabwehr verbessert, um dadurch einen besseren Versicherungsstatus zu erhalten. 64 % haben neue Technologien/Dienstleistungen eingeführt, 56 % bieten mehr Aus- und Weiterbildungsmaßnahmen für ihre Mitarbeiter an und 52 % haben ihre Prozesse/Verhaltensweisen geändert.



94 %
fanden es schwieriger, eine Cyberversicherung abzuschließen



97 %
derjenigen mit einer Cyberversicherung haben ihre Abwehr optimiert, um ihren Versicherungsstatus zu verbessern

Cyberversicherung übernimmt fast alle Ransomware-Schadenfälle

Beruhigend für alle, die eine Cyberversicherung haben: Bei 98 % der Unternehmen, die von Ransomware betroffen waren und eine Cyberversicherung gegen Ransomware hatten, kamen die Versicherungsunternehmen beim schwersten Angriff für den Schaden auf – gegenüber 95 % im Jahr 2019.* In einigen Ländern stieg die Erstattungsrate auf 100 %: Schweiz (Anzahl=52), Mexiko (Anzahl=131), Schweden (Anzahl=68), Belgien (Anzahl=66), Polen (Anzahl=75), Türkei (Anzahl=51), UAE (Anzahl=49), Indien (Anzahl=218) und Singapur (Anzahl=91).

Darüber hinaus zeigt die Studie, dass Versicherer vermehrt für die Bereinigungskosten und weniger für Lösegeldzahlungen aufkommen. 77 % der Befragten gaben an, dass ihr Versicherer die Bereinigungskosten übernommen habe. Dabei handelt es sich um die Kosten, die entstanden sind, um das Unternehmen wieder betriebsfähig zu machen – 2019 lag die Zahl noch bei 67 %. Umgekehrt gaben 40 % an, ihr Versicherer habe das Lösegeld gezahlt; 2019 waren es noch 44 %.

Die Bereitschaft, das Lösegeld zu erstatten, ist jedoch branchenabhängig. Die höchste Erstattungsrate wurde im Bildungswesen (primärer und sekundärer Bildungsbereich) (53 %), bei Behörden (49 %) und im Gesundheitswesen (47 %) gemeldet, die niedrigste im Bereich Fertigung und Produktion (30 %) sowie bei Finanzdienstleistungen (32 %). Interessanterweise sind die Branchen mit der niedrigsten Erstattungsrate beim Lösegeld diejenigen, die sich am schnellsten von einem Vorfall erholen – was die Bedeutung eines Notfallplans zur Wiederherstellung der Daten und Systeme unterstreicht.

Wichtig an dieser Stelle: Eine Cyberversicherung hilft Unternehmen zwar dabei, den Zustand vor dem Angriff wiederherzustellen, sie kommt aber nicht für „Verbesserungsmaßnahmen" auf, z.B. für notwendige Investitionen in bessere Technologien und Dienste, um Schwachstellen zu beheben, die den Angriff möglich machten.

98 %
Erstattungsrate bei Ransomware-Schadenfällen

△ Übernahme der Bereinigungskosten △

67 % 2019

77 % 2021

▽ Übernahme der Lösegeldzahlung ▽

44 % 2019

40 % 2021

** Fragen zum Thema Cyberversicherung wurden für das Jahr 2020 nicht gestellt, deshalb werden hier als Vergleichswerte die Antworten zum Jahr 2019 herangezogen.*

Fazit

Die Bedrohung durch Ransomware-Angriffe wächst. Der Anteil der Unternehmen, die direkt von Ransomware betroffen waren, hat sich innerhalb von zwölf Monaten fast verdoppelt: von etwas mehr als einem Drittel im Jahr 2020 auf zwei Drittel im Jahr 2021.

Da Ransomware-Angriffe damit fast zu einer „normalen" Bedrohung geworden sind, können Unternehmen jetzt besser mit den Folgen eines Angriffs umgehen: Fast alle Unternehmen erhalten mittlerweile einen Teil der verschlüsselten Daten zurück, und fast drei Viertel nutzen Backups zur Wiederherstellung ihrer Daten.

Der Anteil der verschlüsselten Daten, die nach Zahlung des Lösegelds wiederhergestellt wurden, ist auf durchschnittlich 61 % gesunken. Dennoch hat sich der Prozentsatz der Opfer, die Lösegeld in Höhe von 1 Million US-Dollar oder mehr zahlten, fast verdreifacht.

Die Studie zeigt, dass sich das Problem nicht einfach nur mit mehr Personal und Geld lösen lässt. Vielmehr gilt es, in die richtigen Technologien zu investieren. Unternehmen sollten Experten mit an Bord holen, die sie darin unterstützen, die Rentabilität ihrer Cyberinvestitionen zu erhöhen und ihren Schutz zu verstärken.

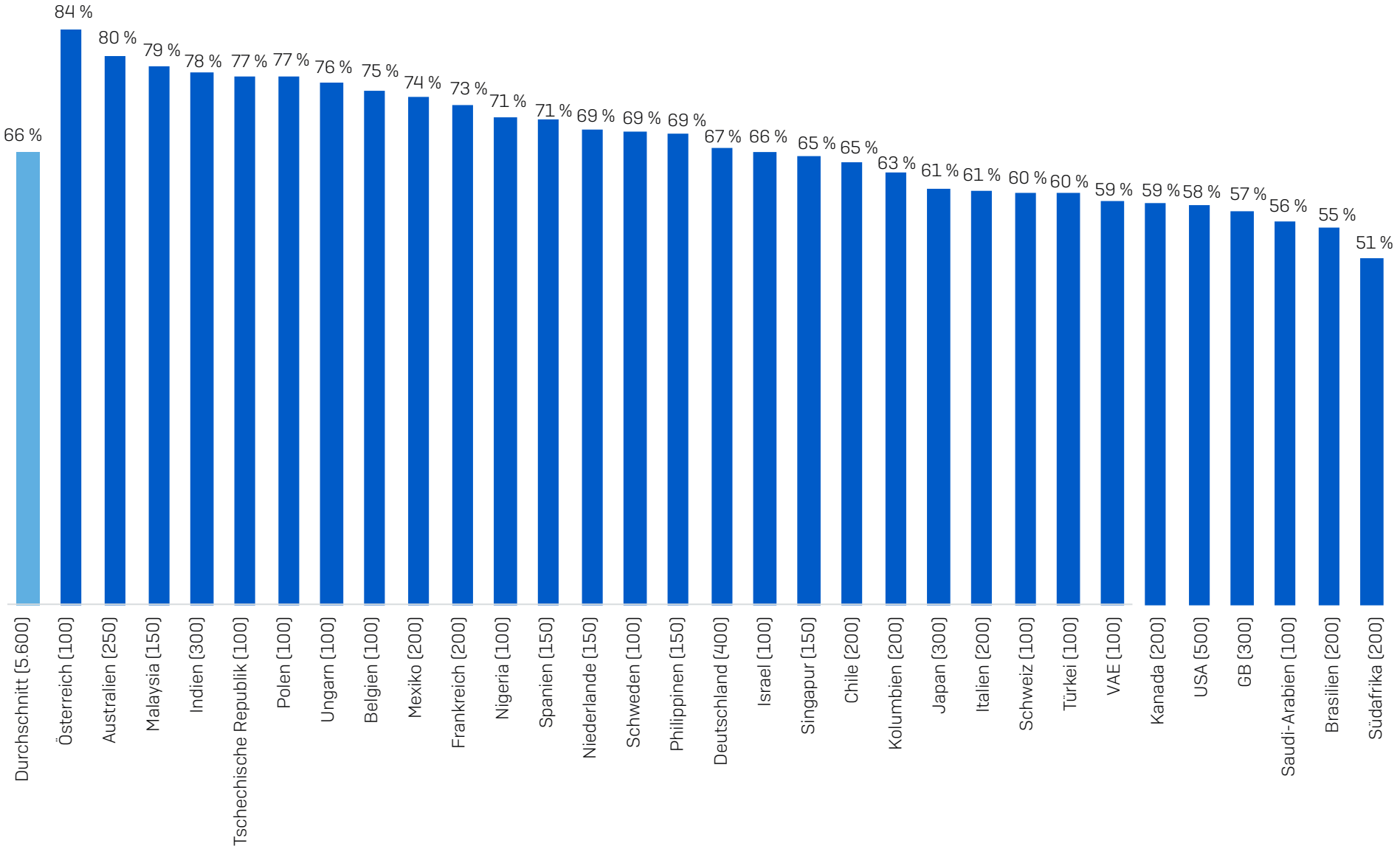
Die meisten Unternehmen schließen eine Cyberversicherung ab, um finanzielle Verluste nach einem Angriff abzufedern. Für sie ist es beruhigend zu wissen, dass die Versicherer in fast allen Schadenfällen einen Teil der Kosten übernehmen. Allerdings wird es für Unternehmen immer schwieriger, einen Versicherungsschutz zu erhalten. Daher sorgen sie für eine effektivere Cyberabwehr, um ihren Versicherungsstatus zu verbessern.

Ob Sie eine Versicherung abschließen möchten oder nicht – optimale Cybersecurity ist für alle Unternehmen unerlässlich. Unsere fünf wichtigsten Tipps für Sie:

- Sorgen Sie an allen Stellen in Ihrer gesamten Umgebung für einen hochwertigen Schutz. Überprüfen Sie Ihre Sicherheitskontrollen und stellen Sie sicher, dass sie weiterhin Ihren Anforderungen entsprechen.
- Gehen Sie proaktiv auf die Suche nach Bedrohungen, damit Sie Angreifer stoppen können, bevor diese ihren Angriff ausführen können – wenn Sie nicht über entsprechende Ressourcen verfügen, beauftragen Sie einen MDR-Spezialisten.
- Härten Sie Ihre Umgebung, indem Sie nach Sicherheitslücken suchen und diese schließen. Dazu gehören z. B. ungepatchte Geräte, ungeschützte Rechner, offene RDP-Ports usw. Extended Detection and Response (XDR) ist für diesen Zweck optimal geeignet.
- Planen Sie im Vorfeld für den Ernstfall. Sie sollten wissen, was bei einem Cybervorfall zu tun ist und wen Sie kontaktieren müssen.
- Erstellen Sie Backups und üben Sie, damit Ihre Daten wiederherzustellen. Ihr Ziel ist es, den Betrieb schnell wieder aufzunehmen.

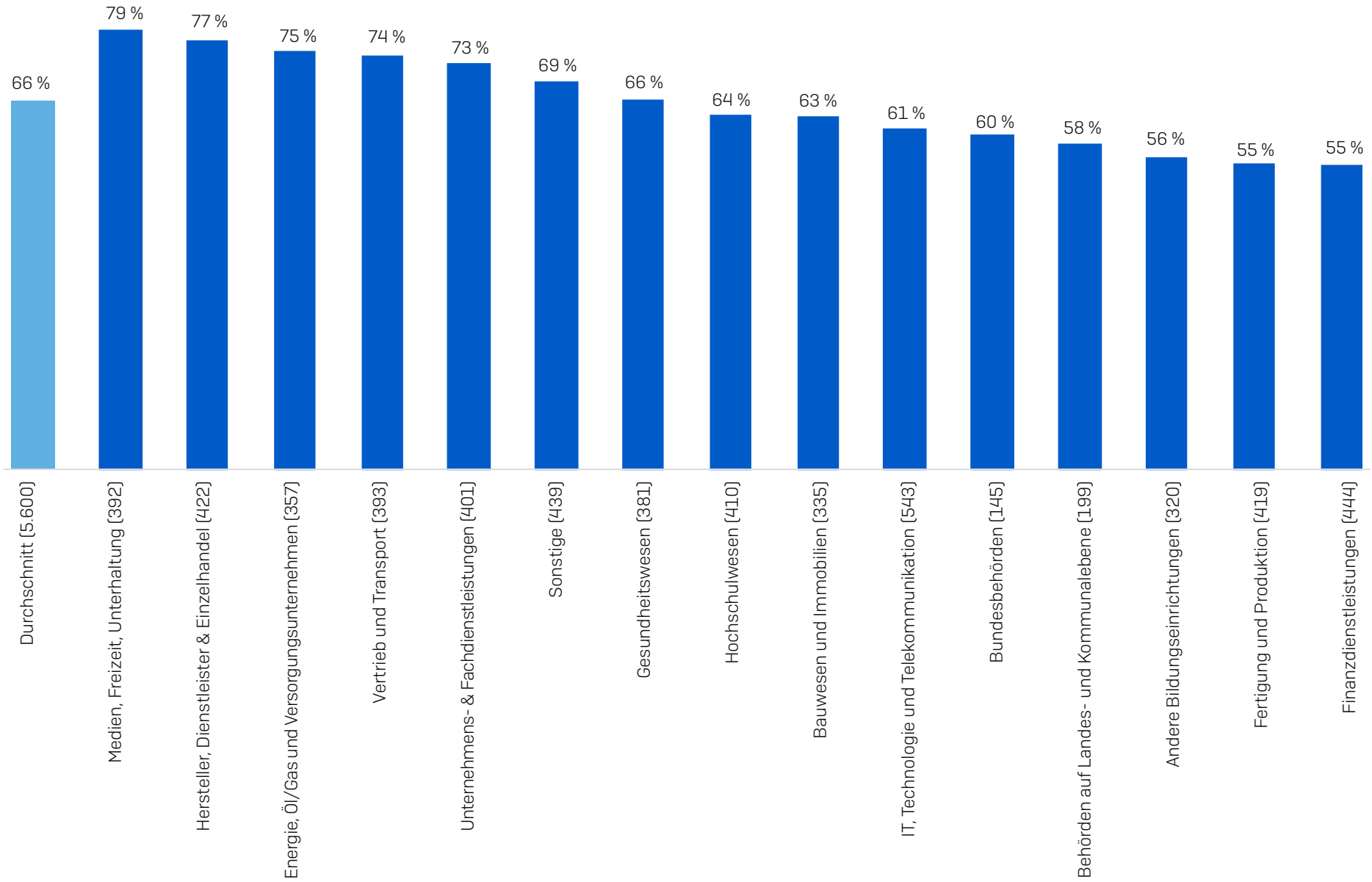
Ausführliche Informationen zu einzelnen Ransomware-Gruppen finden Sie im Sophos Ransomware Threat Intelligence Center.

Ländervergleich: Unternehmen, die im letzten Jahr von Ransomware betroffen waren



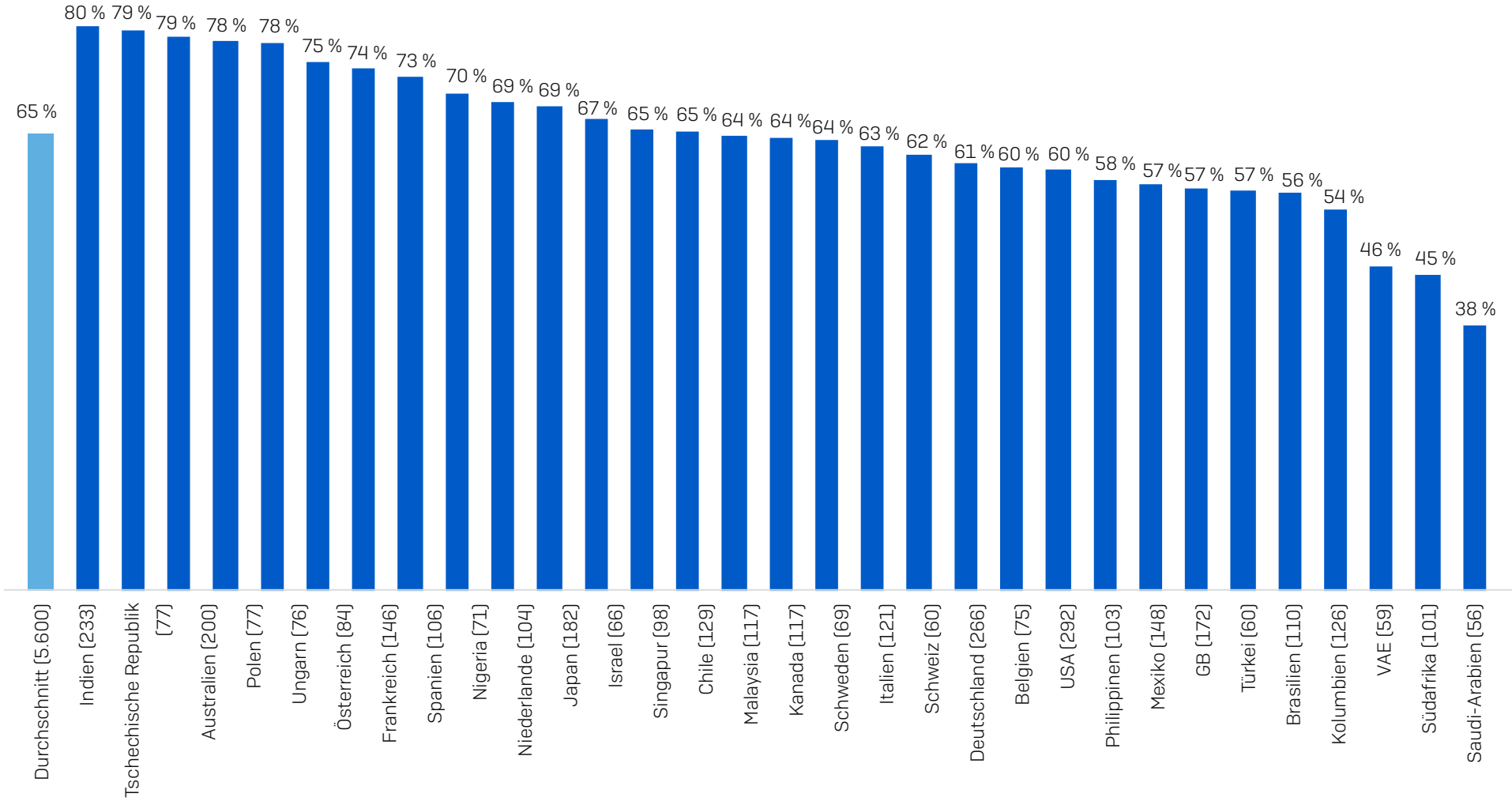
War Ihr Unternehmen im letzten Jahr von Ransomware betroffen? (Anzahl=5.600): Ja

Branchenvergleich: Unternehmen, die im letzten Jahr von Ransomware betroffen waren



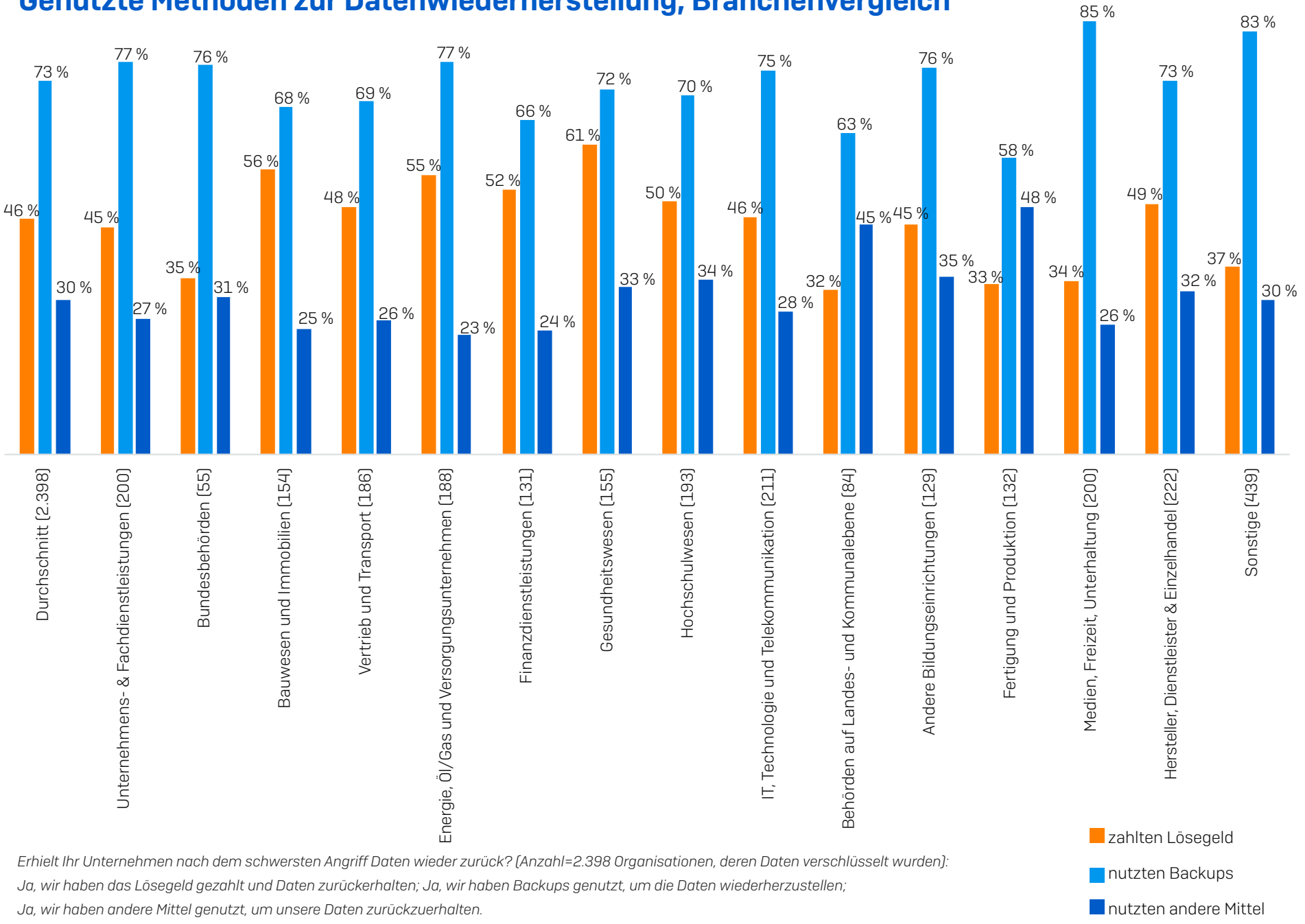
War Ihr Unternehmen im letzten Jahr von Ransomware betroffen? (Anzahl=5.600): Ja

Verschlüsselungsrate bei Ransomware-Angriffen, Ländervergleich



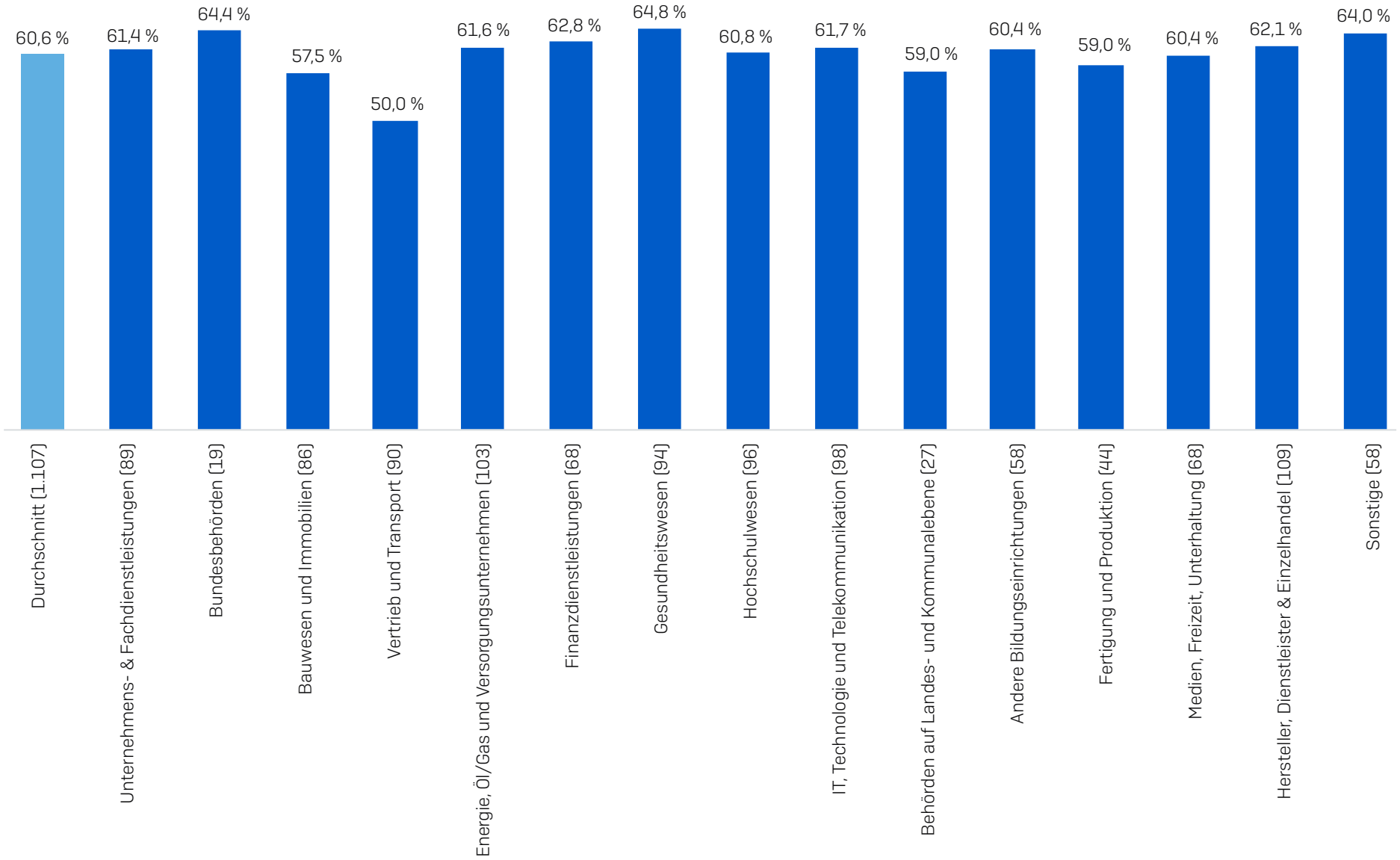
Konnten die Cyberkriminellen beim schwersten Ransomware-Angriff Ihre Unternehmensdaten verschlüsseln? (Anzahl=3.702 Unternehmen, die im letzten Jahr von Ransomware-Angriffen betroffen waren): Ja

Genutzte Methoden zur Datenwiederherstellung, Branchenvergleich



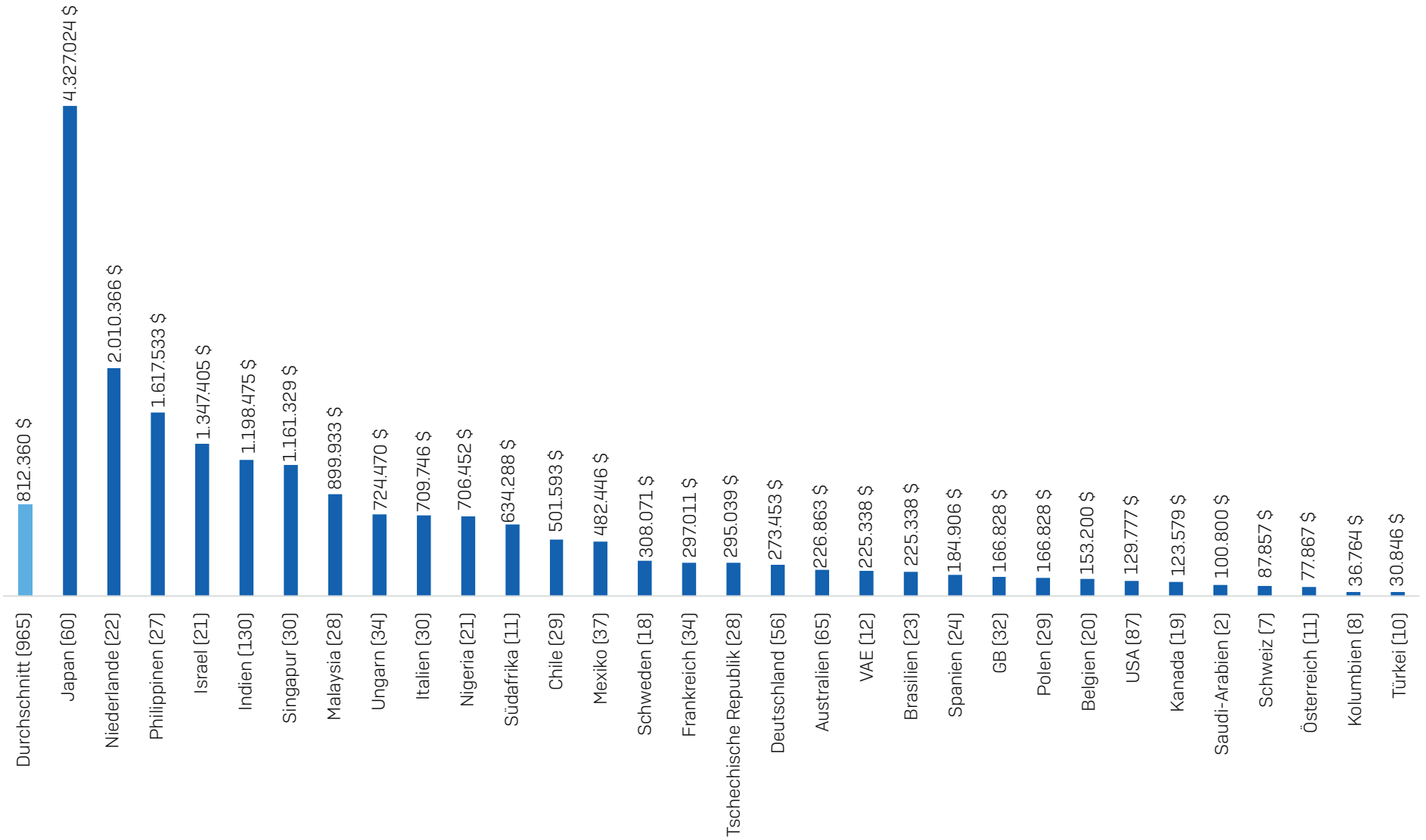
Erhielt Ihr Unternehmen nach dem schwersten Angriff Daten wieder zurück? (Anzahl=2.398 Organisationen, deren Daten verschlüsselt wurden): Ja, wir haben das Lösegeld gezahlt und Daten zurückerhalten; Ja, wir haben Backups genutzt, um die Daten wiederherzustellen; Ja, wir haben andere Mittel genutzt, um unsere Daten zurückzuerhalten.

Wiederhergestellte Daten nach Lösegeldzahlung, Branchenvergleich



Wie viele Daten Ihres Unternehmens haben Sie nach dem schwersten Ransomware-Angriff zurückerhalten?
(Anzahl=1.107 Unternehmen, die das Lösegeld gezahlt und Daten zurückerhalten haben)

Durchschnittliche Lösegeldzahlungen, Ländervergleich



Wie hoch war die Lösegeldzahlung, die Ihr Unternehmen beim schwersten Ransomware-Angriff geleistet hat? Angaben in US-Dollar; Anzahl der erhaltenen Antworten jeweils in Klammer; ohne "weiß nicht"-Angaben und Extremwerte; Bei Ländern mit niedrigen Antwort-Zahlen sind die Ergebnisse nicht repräsentativ, können jedoch als Indikator dienen.

Durchschnittliche Kosten zur Behebung der Angriffsschäden (in Millionen US-Dollar)

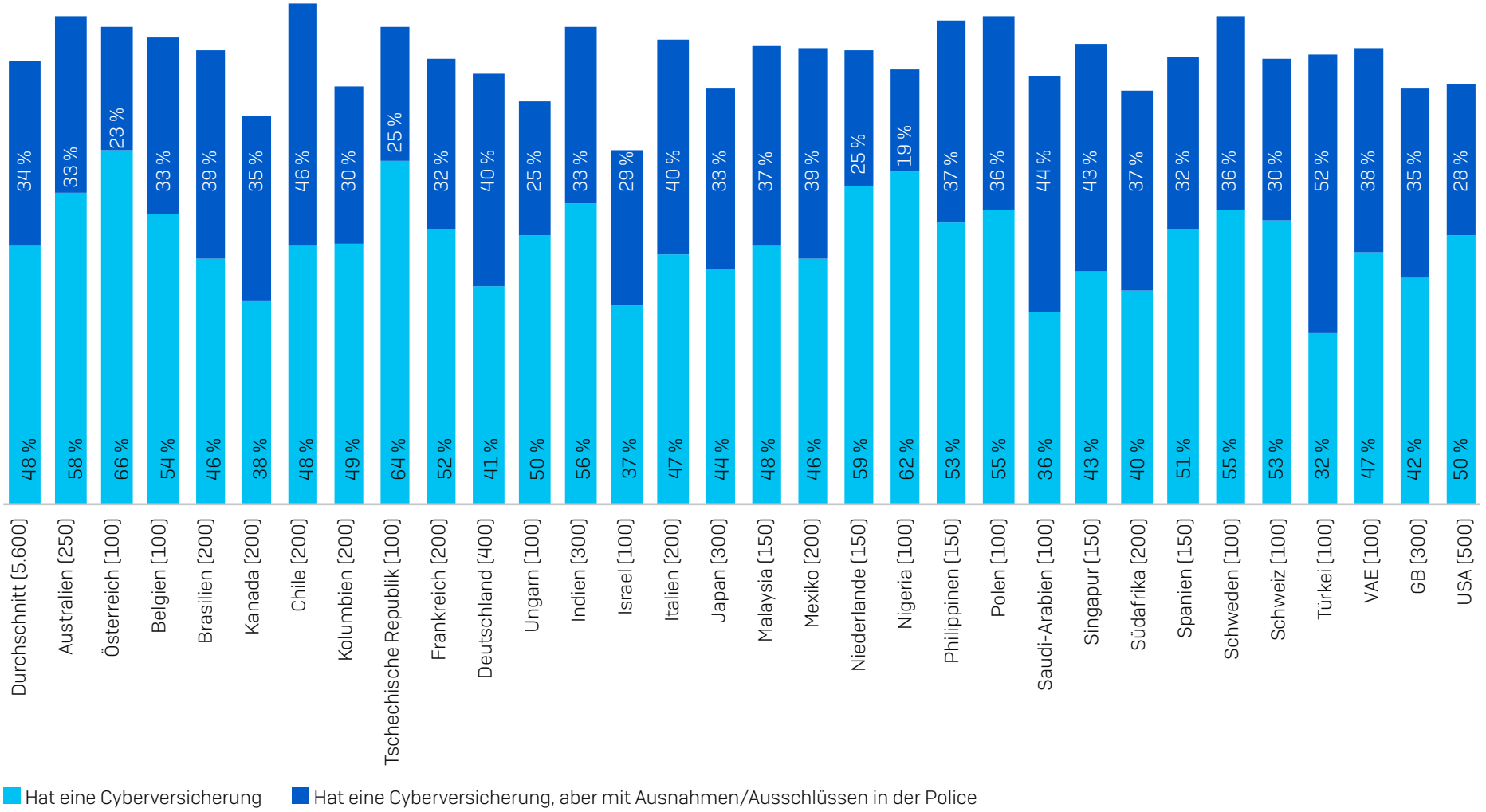
Land	2021	2020	Veränderung gegenüber dem Vorjahr
Durchschnitt (3.702)	1,40 $	1,85 $	-24 %
Australien (200)	1,01 $	1,84 $	-45 %
Österreich (84)	0,81 $	7,75 $	-90 %
Belgien (75)	3,71 $	4,75 $	-22 %
Brasilien (110)	0,69 $	0,82 $	-16 %
Kanada (117)	0,65 $	1,92 $	-66 %
Chile (129)	1,58 $	0,73 $	116 %
Kolumbien (126)	0,50 $	1,26 $	-60 %
Tschechische Republik (77)	2,58 $	0,37 $	589 %
Frankreich (146)	2,03 $	1,11 $	83 %
Deutschland (266)	1,73 $	1,17 $	48 %
Ungarn (76)	1,51 $	--	--
Indien (233)	2,81 $	3,38 $	-17 %
Israel (66)	1,41 $	0,57 $	148 %
Italien (121)	1,65 $	0,68 $	141 %
Japan (182)	0,96 $	1,61 $	-40 %
Malaysia (118)	1,22 $	0,77 $	58 %

Land	2021	2020	Veränderung gegenüber dem Vorjahr
Mexiko (148)	0,88 $	2,03 $	-57 %
Niederlande (104)	0,98 $	2,71 $	-64 %
Nigeria (71)	3,43 $	0,46 $	644 %
Philippinen (103)	1,34 $	0,82 $	63 %
Polen (77)	1,78 $	--	--
Saudi-Arabien (56)	0,65 $	0,21 $	212 %
Singapur (98)	1,91 $	3,46 $	-45 %
Südafrika (101)	0,71 $	--	--
Spanien (106)	0,75 $	0,60 $	25 %
Schweden (69)	0,75 $	1,40 $	-46 %
Schweiz (60)	1,64 $	1,43 $	15 %
Türkei (60)	0,37 $	0,58 $	-36 %
VAE (59)	1,26 $	0,52 $	144 %
GB (172)	1,08 $	1,96 $	-45 %
USA (292)	1,08 $	2,09 $	-49 %

Die in Klammern angegebenen Zahlen der erhaltenen Antworten gelten nur für die Daten von 2021.
Die Werte sind in Millionen US-Dollar angegeben.

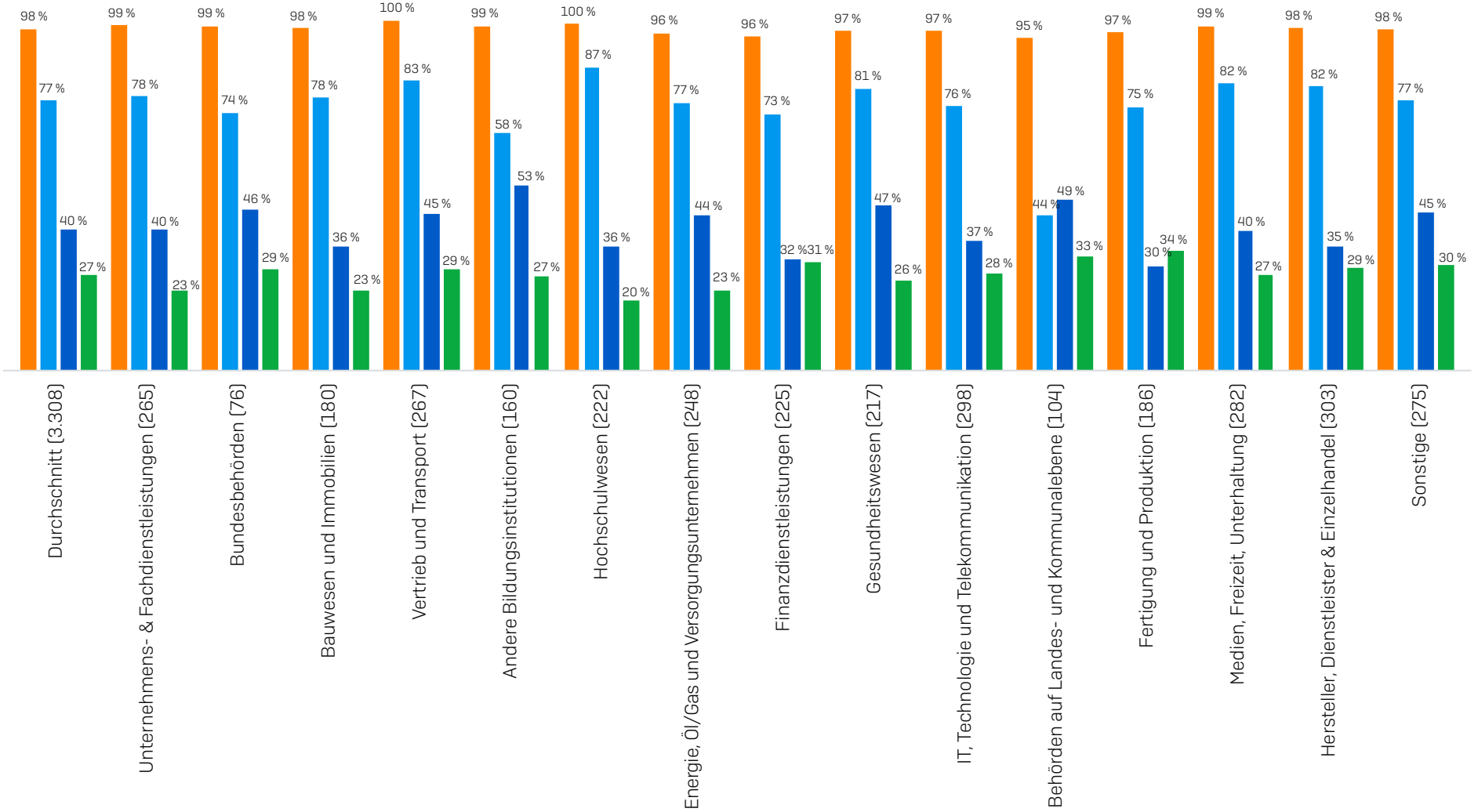
Wie hoch waren die ungefähren Kosten, die Ihrem Unternehmen durch den letzten Ransomware-Angriff entstanden sind (unter Berücksichtigung von Ausfallzeiten, Arbeitsstunden, Geräte- und Netzwerkkosten, entgangenen Geschäftschancen, Lösegeld usw.)? (Anzahl=3.702 Unternehmen, die im letzten Jahr von Ransomware-Angriffen betroffen waren)

Unternehmen mit Cyber-Versicherungsschutz, Ländervergleich



Hat Ihr Unternehmen eine Cyberversicherung, die bei einem Ransomware-Angriff für den Schaden aufkommt? (Anzahl=5.600). Ja; Ja, aber es gibt Ausnahmen/Ausschlüsse in unserer Police

Auszahlungsrate bei Cyberversicherungen, Branchenvergleich



Hat die Cyber-Versicherung die Kosten für den schwersten Ransomware-Angriff übernommen? (Anzahl=3.308 Unternehmen, die im vergangenen Jahr von Ransomware betroffen waren und eine Cyberversicherung gegen Ransomware abgeschlossen hatten). Ja, Bereinigungskosten wurden übernommen (z. B. Kosten für die Wiederherstellung des Betriebs); Ja, das Lösegeld wurde gezahlt; Ja, sonstige Kosten wurden übernommen (z. B. Kosten für Ausfallzeiten, entgangene Umsatzchancen usw.)

Erfahren Sie mehr über Ransomware und darüber, wie Sophos Sie und Ihr Unternehmen davor schützen kann.

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.

2022-04-04 (WP-NP)

SOPHOS