SOPHOS
Cybersecurity delivered.

Ransomware-Report 2022: Gesundheitswesen

Ergebnisse einer unabhängigen Befragung von 5.600 IT-Entscheidern – darunter 381 aus dem Gesundheitswesen – in Unternehmen und Einrichtungen mittlerer Größe aus 31 Ländern.

Sophos-Whitepaper. Mai 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 Organisationen ihre Cybersicherheit ausbauen.

Über die Studie

Sophos beauftragte das Marktforschungsunternehmen Vanson Bourne mit der Durchführung einer unabhängigen Befragung von 5.600 IT-Fachleuten (darunter 381 aus dem Gesundheitswesen) 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

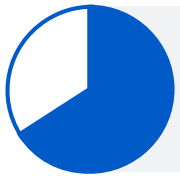
Im letzten Jahr waren 66 % der Gesundheitseinrichtungen von Ransomware betroffen, im Vergleich zu 34 % in 2020. Innerhalb eines Jahres ist dies ein Anstieg von 94 %. Ein Indiz dafür, dass Cyberkriminelle immer besser in der Lage sind, großangelegte Angriffe auszuführen. Darin spiegelt sich vermutlich 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.]

Vergleicht man die Häufigkeit von Ransomware-Angriffen in allen befragten Branchen, entsprach die Anzahl von Angriffen im Gesundheitswesen dem globalen Durchschnitt von 66 %.

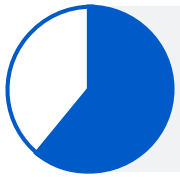
Bei der Datenverschlüsselung schnitt das Gesundheitswesen mit einer Verschlüsselungsrate von 61 % besser ab als der globale Durchschnitt von 65 %. Dies deutet darauf hin, dass das Gesundheitswesen besser in der Lage war, Datenverschlüsselungen im Rahmen von Ransomware-Angriffen zu stoppen. Außerdem sank die Verschlüsselungsrate im Gesundheitswesen gegenüber dem Vorjahr (65 % im Jahr 2020).

Der Prozentsatz der Opfer, die nur von Extortion-Angriffen betroffen waren, d. h. bei denen keine Daten verschlüsselt wurden, sondern eine Erpressung mit der Drohung erfolgte, Daten offenzulegen, sank von 7 % im Jahr 2020 auf 4 % im Jahr 2021. Ein Grund für diese positive Entwicklung könnte sein, dass Gesundheitseinrichtungen vermehrt Cyberversicherungen abschließen, die im Gegenzug strengere Cybersecurity-Maßnahmen voraussetzen. Wir werden diese Entwicklung im weiteren Verlauf dieses Reports noch näher beleuchten.

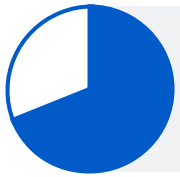
Die Erfolgsquote der Angreifer steigt. Dies geht einher mit einem immer komplexeren Bedrohungsumfeld, von dem das Gesundheitswesen stärker beeinträchtigt ist als jede andere Branche. Das Gesundheitswesen verzeichnete den höchsten Anstieg bei der Anzahl von Cyberangriffen (69 %) sowie bei der Komplexität von Cyberangriffen (67 %) im Vergleich zum branchenübergreifenden Durchschnitt von 57 % bzw. 59 %. Bei den Folgen dieser Cyberangriffe war das Gesundheitswesen die am zweitstärksten betroffene Branche (59 %), im Vergleich zum globalen Durchschnitt von 53 %.



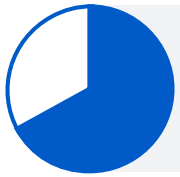
66 %
wurden Opfer eines Ransomware-Angriffs



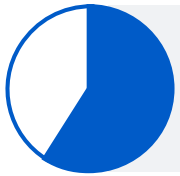
61 %
der Angriffe führten zur Datenverschlüsselung



69 %
Zunahme bei der Zahl der Cyberangriffe, der höchste Wert im Branchenvergleich



67 %
Zunahme bei der Komplexität von Cyberangriffen, der höchste Wert im Branchenvergleich



59 %
Zunahme bei den Auswirkungen von Cyberangriffen, der zweithöchste Wert im Branchenvergleich

Mehr Erfolg beim Wiederherstellen der Daten nach einem Angriff

Mit der zunehmenden Verbreitung von Ransomware gelingt es Unternehmen und Einrichtungen mittlerweile offenbar besser, mit den Folgen eines Angriffs umzugehen. 99 % der Gesundheitseinrichtungen, die im letzten Jahr von Ransomware betroffen waren, erhielten einen Teil ihrer verschlüsselten Daten zurück; ein deutlicher Anstieg zum Jahr davor, damals waren es noch 93 %.

72 % der Gesundheitseinrichtungen, deren Daten verschlüsselt wurden, nutzten Backups – die am häufigsten verwendete Methode zur Wiederherstellung von Daten. Gleichzeitig gaben 61 % der Befragten an, dass sie Lösegeld gezahlt hätten, um ihre Daten wiederherzustellen. 33 % nutzen andere Methoden zur Wiederherstellung von Daten. Diese Zahlen zeigen, dass viele Gesundheitseinrichtungen mehrere Ansätze verfolgen, um schneller und effizienter den Betrieb wieder aufnehmen zu können. Insgesamt nutzte etwas mehr als die Hälfte (52 %) der Befragten, deren Daten verschlüsselt wurden, mehrere Methoden zur Wiederherstellung der Daten.

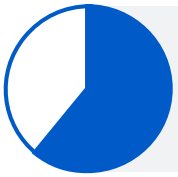
Das Gesundheitswesen führt die Liste an, wenn es um die parallele Verwendung aller drei Methoden zur Wiederherstellung verschlüsselter Daten geht: Backups, Lösegeldzahlung und andere Mittel. Dies war im Gesundheitsweisen bei 14 % der Befragten der Fall, im Vergleich zum globalen Durchschnitt von 7 %. Um die Kontinuität der Betriebsabläufe zu gewährleisten, ist das Gesundheitswesen im hohen Maße von der Datenverfügbarkeit abhängig. Denn fehlende zeitnahe Daten können die Patientenversorgung verzögern, was katastrophale Folgen haben kann. Die Bemühungen im Gesundheitswesen, Daten mit allen verfügbaren Mitteln wiederherzustellen, ist daher nur allzu verständlich.

Mit der Zahlung des Lösegelds erhalten betroffene Einrichtungen fast immer einen Teil ihrer Daten zurück. Doch der Prozentsatz der wiederhergestellten Daten nach erfolgter Lösegeldzahlung ist zurückgegangen. Im Durchschnitt erhielten Gesundheitseinrichtungen, die das Lösegeld zahlten, im Jahr 2021 nur 65 % ihrer Daten zurück, gegenüber 69 % im Jahr 2020. Und nur 2 % derjenigen, die der Lösegeldforderung nachkamen, erhielten in 2021 ALLE Daten zurück. Im Vorjahr waren es noch 8 %.

Die Bereitschaft, Lösegeld zu zahlen, ist im Gesundheitswesen am höchsten

Einrichtungen im Gesundheitswesen sind am ehesten bereit, Lösegeld zu zahlen: 61 % der Befragten, deren Daten verschlüsselt wurden, bekannten, sie hätten Lösegeld gezahlt. Der branchenübergreifende Durchschnitt lag bei 46 %. Im Vergleich zum Jahr 2020, in dem 34 % der Lösegeldforderung nachkamen, hat sich die Zahl somit fast verdoppelt. Das Gesundheitswesen verzeichnete bei der Anzahl und Komplexität von Angriffen im Vergleich zu allen anderen Branchen den höchsten Anstieg. Wahrscheinlich ist dies ein Grund dafür, warum im Gesundheitswesen so häufig Lösegeld gezahlt wird, um eine Bereinigung zu vermeiden, für die im Vorfeld keine ausreichenden Vorkehrungen getroffen wurden.

Weitere Gründe, wie wir später in diesem Report noch sehen werden, könnten die Auswirkungen von Ransomware sein, die sich nicht auf verschlüsselte Datenbanken und Geräte beschränken. Ransomware kann den gesamten Betrieb und die Geschäftseinnahmen von Gesundheitseinrichtungen beeinträchtigen, sodass extreme Eile geboten ist, den alten Status quo wiederherzustellen. Und schließlich sind die hohen Kosten für die Bereinigung von Angriffen im Gesundheitswesen – mit 1,85 Mio. US-Dollar die zweithöchsten Kosten im Branchenvergleich – vielleicht der Grund, warum Gesundheitsorganisationen lieber den Lösegeldforderungen nachkommen als die Bereinigungskosten zu zahlen.



61 %
der Befragten im Gesundheitswesen zahlten Lösegeld

△ Lösegeldzahlung △

61 %	34 %
2021	2020

Das Gesundheitswesen zahlte die niedrigsten Lösegeldsummen

Bei der Häufigkeit der Zahlungen führt das Gesundheitswesen die Liste zwar an, doch bei der Höhe der gezahlten Beträge belegt es im Branchenvergleich den letzten Platz. Insgesamt leistete das Gesundheitswesen mit ca. 197.000 US-Dollar die niedrigste durchschnittliche Lösegeldzahlung aller genannten Branchen. Obwohl Gesundheitseinrichtungen Lösegeldforderungen also häufig nachkommen, sind die gezahlten Beträge relativ gering. Die niedrigen Lösegeldsummen sind wahrscheinlich auf die finanziell angespannte Lage vieler und insbesondere öffentlicher Gesundheitseinrichtungen zurückzuführen. Die finanziellen Mittel dieser Einrichtungen sind schlichtweg begrenzt und sie können höheren Forderungen von Angreifern einfach nicht nachkommen – selbst wenn sie wollten.

Interessant ist, dass im Gesundheitswesen zwar die niedrigsten Lösegeldzahlungen geleistet wurden, der Gesamtbetrag des im Jahr 2021 gezahlten Lösegelds im Vergleich zu 2020 jedoch um 33 % stieg.

60 % der Lösegeldbeträge lagen im Gesundheitswesen unter 50.000 US-Dollar. Nur drei Befragte gaben an, dass ihre Einrichtung 1 Mio. US-Dollar oder mehr gezahlt habe. Diese Entwicklung läuft entgegen dem in anderen Branchen beobachteten Trend, wo sich der Anteil der Opfer, die Lösegeld in Höhe von 1 Mio. US-Dollar oder mehr zahlten, fast verdreifacht hat: 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.

197.000 $
durchschnittliche Lösegeldzahlung im Gesundheitswesen, der niedrigste Betrag im Branchenvergleich

33 %
Anstieg der Lösegeldzahlungen im Gesundheitswesen im Vergleich zum Vorjahr

60 %
der Lösegeldbeträge im Gesundheitswesen lagen unter 50.000 US-Dollar

Ransomware hat gravierende geschäftliche und betriebliche Auswirkungen im Gesundheitswesen

Die Lösegeldsummen sind nur ein Teil des Problems. So führen Ransomware-Angriffe nicht nur zu verschlüsselten Datenbanken und Geräten. 94 % der Gesundheitseinrichtungen, die im letzten Jahr von Ransomware betroffen waren, gaben an, dass der schwerste Angriff ihre Betriebsfähigkeit beeinträchtigt habe. Darüber hinaus gaben 90 % der privatwirtschaftlichen Gesundheitseinrichtungen an, dass sie dadurch Geschäftseinbußen oder Umsatzverluste hinnehmen mussten.

Branchenübergreifend zahlten Unternehmen und Einrichtungen im Jahr 2021 durchschnittlich 1,4 Mio. US-Dollar, um die Auswirkungen des letzten Ransomware-Angriffs zu beheben. Im Jahr 2020 waren es noch 1,85 Mio. US-Dollar. Dieser Rückgang ist vermutlich auf die zunehmende Verbreitung von Cyberversicherungen und deren Unterstützung zurückzuführen. Denn Versicherungsanbieter sind besser in der Lage, den Betroffenen schnell und effektiv unter die Arme zu greifen und somit die Bereinigunskosten zu senken.

Im Gesundheitswesen stiegen die durchschnittlichen Bereinigungskosten jedoch von 1,27 Mio. US-Dollar im Jahr 2020 auf 1,85 Mio. US-Dollar im Jahr 2021. Im Vergleich zum branchenübergreifenden Durchschnitt (1,85 Mio. US-Dollar vs. 1,4 Mio. US-Dollar) lag das Gesundheitswesen sogar an zweiter Stelle bei den durchschnittlichen Kosten, die für die Bereinigung eines Ransomware-Angriffs anfielen. Wie bereits erwähnt, haben sich Ransomware-Angriffe auf das Gesundheitswesen im letzten Jahr fast verdoppelt (66 % im Jahr 2021 gegenüber 34 % im Jahr 2020). Dies könnte ein Grund dafür sein, dass es für Gesundheitseinrichtungen deutlich schwieriger ist, eine Cyberversicherung abzuschließen als für andere Branchen – wir gehen auf diesen Punkt später noch genauer ein. Der Mangel an Cybersecurity-Expertise, die zunehmende Verbreitung medizinischer IoT-Geräte, anfällige Altsysteme und der 24/7-Betrieb (was schnelle Korrekturmaßnahmen auf anfälligen Systemen praktisch unmöglich macht) sind in der Gesundheitsbranche nach wie vor ein Problem und erhöhen die Gesamtkosten für die Bereinigung nach einem Angriff.

44 % der Gesundheitseinrichtungen, die im letzten Jahr Opfer eines Angriffs wurden, brauchten bis zu eine Woche, um sich von dem schwersten Angriff zu erholen, 25 % sogar bis zu einem Monat – für die meisten Einrichtungen ein langer Zeitraum. Im Hochschulwesen und bei den Bundesbehörden waren es sogar zwei von fünf Befragten, die eine Wiederherstellungszeit von über einem Monat angaben. Zudem setzen einige Unternehmen weiterhin auf unwirksame Abwehrmaßnahmen. Von den Befragten, deren Gesundheitseinrichtungen im letzten Jahr nicht von Ransomware betroffen waren und auch künftig nicht damit rechnen, begründeten 77 % dies mit Methoden, die nicht vor Angriffen schützen: 50 % nannten Backups und 43 % eine Cyberversicherung als Grund, warum sie nicht mit einem Angriff rechnen, wobei einige beide Optionen wählten. Diese Ansätze helfen den Einrichtungen zwar dabei, sich von einem Angriff zu erholen, aber sie verhindern ihn nicht im Voraus.

94 %
wurden durch den Ransomware-Angriff in ihrer Betriebsfähigkeit beeinträchtigt

90 %
verzeichneten Geschäftseinbußen/Umsatzverluste

1,85 Mio. US-Dollar
durchschnittliche Bereinigungskosten im Gesundheitswesen, der zweithöchste Wert im Branchenvergleich

EINE WOCHE
durchschnittlich benötigte Zeit bis zur kompletten Wiederherstellung nach einem Angriff

77 %
verlassen sich auf Methoden, die einen Angriff nicht verhindern

Für Gesundheitseinrichtungen ist es schwieriger, eine Cyberversicherung abzuschließen

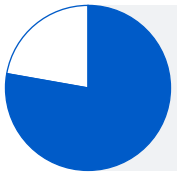
Branchenübergreifend haben 83 % der Unternehmen und Einrichtungen eine Cyberversicherung gegen Ransomware. Im Vergleich dazu haben nur 78 % der Gesundheitseinrichtungen einen solchen Versicherungsschutz und 46 % davon sagen, es gebe in ihrer Police Ausnahmen/Ausschlüsse. Angesichts der Häufigkeit von Ransomware-Vorfällen im Gesundheitswesen laufen viele Einrichtungen Gefahr, durch diese Versicherungs-Lücke die Kosten eines Angriffs komplett alleine tragen zu müssen.

Unternehmen im Bereich Energie, Öl/Gas und Versorgung sind am ehesten versichert – (89 %), dicht gefolgt vom Einzelhandel (88 %). Fertigung und Produktion belegen den letzten Platz: Hier sind nur 75 % versichert.

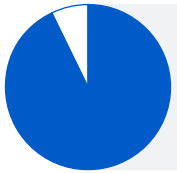
93 % der Gesundheitseinrichtungen, die eine Cyberversicherung abgeschlossen haben, gaben an, dass sich die Konditionen beim Versicherungsschutz im letzten Jahr verändert hätten und es schwieriger geworden sei, einen Versicherungsschutz zu erhalten. 51 % berichteten, dass sie jetzt ein höheres Maß an Cybersicherheit nachweisen müssten, um eine Versicherung abschließen zu können. 45 % meinten, dass die Policen jetzt komplexer seien, 48 % gaben an, dass weniger Versicherer eine Cyberversicherung anböten, und 46 % schilderten, dass der Bearbeitungsprozess länger dauere. 34 % sagten, der Versicherungsschutz sei teurer geworden.

Diese Entwicklungen stehen in engem Zusammenhang mit Ransomware, die den größten Treiber für Cyberversicherungs-Ansprüche darstellt. In den letzten Jahren haben Ransomware-Angriffe zugenommen, und die Kosten für Lösegeld und Auszahlungen sind in die Höhe geschnellt. Infolgedessen haben einige Versicherungsunternehmen den Markt verlassen, da er für sie einfach unrentabel geworden ist. Die verbleibenden Anbieter versuchen, ihr Risiko so gut wie möglich zu reduzieren, und diktieren die Preise.

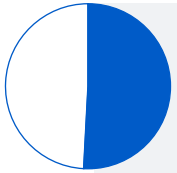
In einem solchen Verkäufermarkt haben die Versicherer die Zügel in der Hand und können sich ihre Kunden aussuchen. Durch eine starke Cyberabwehr können Unternehmen und Einrichtungen ihre Chancen auf den Abschluss einer geeigneten Cyberversicherung entscheidend verbessern.



78 %
der Gesundheitseinrichtungen haben eine Cyberversicherung gegen Ransomware



93 %
geben an, dass sich die Konditionen beim Versicherungsschutz im letzten Jahr verändert haben

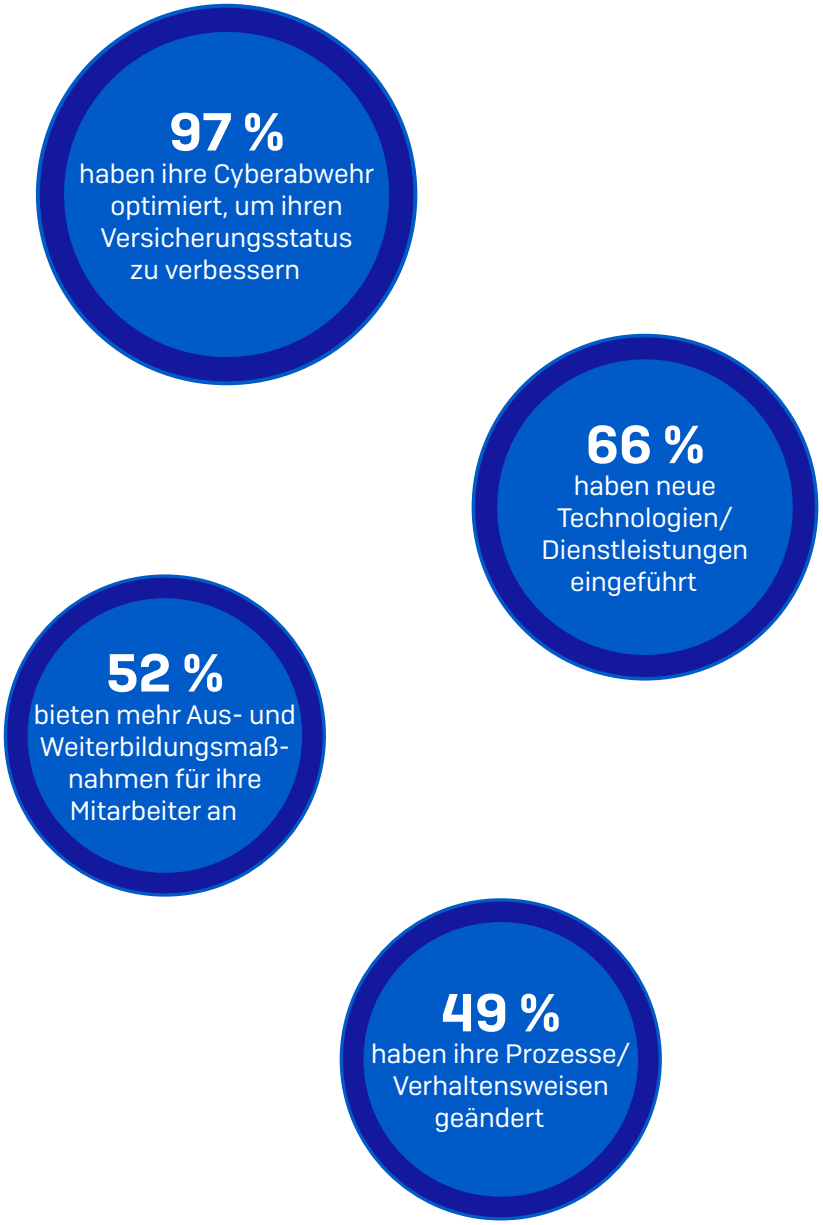


51 %
berichten, dass sie ein höheres Maß an Cybersicherheit nachweisen müssen, um eine Versicherung abschließen zu können

Gesundheitseinrichtungen stärken ihre Cyberabwehr für bessere Versicherungsbedingungen

Der Markt für Cyberversicherungen verhärtet sich und es wird schwieriger, Schäden abzusichern. Daher haben 97 % der Gesundheitseinrichtungen mit Cyberversicherungs-Schutz ihre Cyberabwehr verbessert, um dadurch einen besseren Versicherungsstatus zu erhalten. 66 % haben neue Technologien und Dienstleistungen eingeführt, 52 % bieten mehr Aus- und Weiterbildungsmaßnahmen für ihre Mitarbeiter und 49 % haben ihre Prozesse und Verhaltensweisen geändert.

Die Verhärtung des Cyberversicherungs-Marktes wird zu einem Großteil durch die zunehmende Erstattung von Lösegeldzahlungen befeuert. Zugleich ist diese Entwicklung auch treibende Kraft für Verbesserungsmaßnahmen bei der Cyberabwehr.

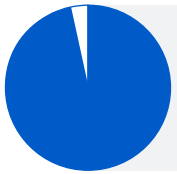


Cyberversicherung übernimmt fast alle Ransomware-Schadenfälle

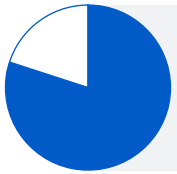
Beruhigend für alle, die eine Cyberversicherung haben: Bei 97 % der Gesundheitseinrichtungen, die von Ransomware betroffen waren und eine Cyberversicherung gegen Ransomware hatten, kamen die Versicherungsunternehmen beim schwersten Angriff für den Schaden auf. 81 % der Befragten gaben an, dass ihr Versicherer die Bereinigungskosten übernommen habe. Dabei handelt es sich um die Kosten, die entstanden sind, um das Unternehmen wieder betriebsfähig zu machen. Umgekehrt gaben 47 % an, ihr Versicherer habe das Lösegeld gezahlt. Darüber hinaus zeigt die Studie, dass Versicherer in allen Branchen im Vergleich zu 2020 vermehrt für die Bereinigungskosten und weniger für Lösegeldzahlungen aufkommen.

Die Bereitschaft, das Lösegeld zu erstatten, ist dagegen stark branchenabhängig. Die höchste Erstattungsrate wurde mit 53 % im Bildungswesen (primärer und sekundärer Bildungsbereich), bei Behörden mit 49 % und im Gesundheitswesen mit 47 % gemeldet, die niedrigste mit 30 % im Bereich Fertigung und Produktion sowie mit 32 % Finanzdienstleistungen. 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.

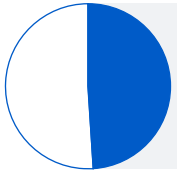
Wichtig an dieser Stelle: Eine Cyberversicherung hilft zwar dabei, den Zustand vor dem Angriff wiederherzustellen, sie kommt aber nicht für „Verbesserungsmaßnahmen" auf, z. B. für notwendige Investitionen in bessere Technologien und Dienste, um Schwachstellen zu beheben, die den Angriff möglich machten.



97 %
Auszahlungsrate bei Cyberversicherungen im Gesundheitswesen



81 %
Übernahme der Bereinigungskosten durch den Versicherer im Gesundheitswesen



47 %
Übernahme der Lösegeldzahlung durch den Versicherer im Gesundheitswesen

Fazit

Die Bedrohung durch Ransomware-Angriffe wächst. Der Anteil der Gesundheitseinrichtungen, 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 Gesundheitseinrichtungen jetzt besser mit den Folgen eines Angriffs umgehen: Fast alle erhalten mittlerweile einen Teil der verschlüsselten Daten zurück, und fast drei Viertel nutzen Backups zur Wiederherstellung ihrer Daten.

Gleichzeitig ist der Anteil der verschlüsselten Gesundheitsdaten, die nach Zahlung des Lösegelds wiederhergestellt wurden, auf durchschnittlich 65 % gesunken.

Das Gesundheitswesen zahlte die niedrigste durchschnittliche Lösegeldsumme (197.000 US-Dollar).

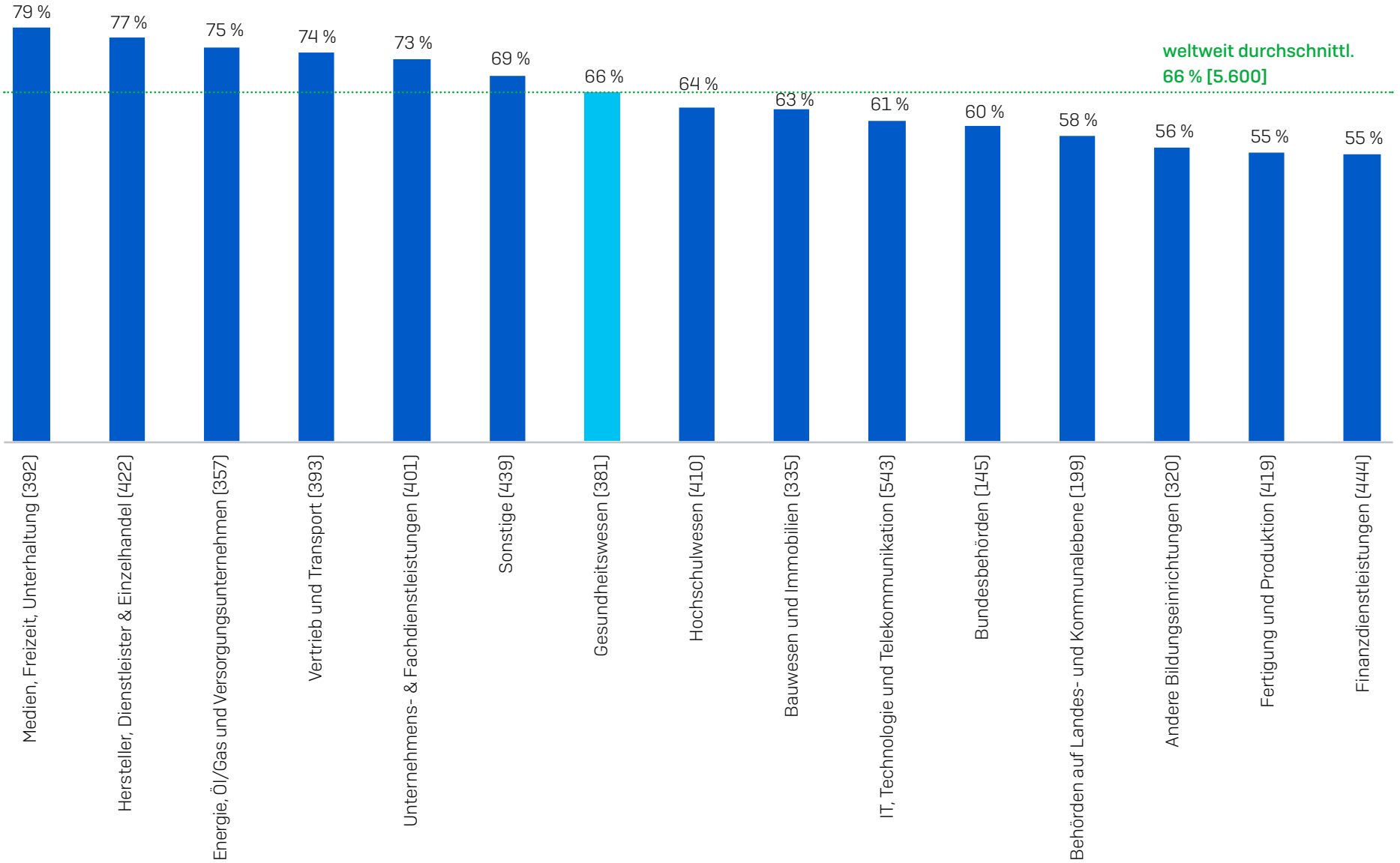
Ransomware wirkt sich auf den Betrieb, Geschäftsabläufe und Einnahmen im Gesundheitswesen aus. Die meisten Gesundheitseinrichtungen schließen eine Cyberversicherung ab, um finanzielle Verluste nach einem Angriff abzufedern. Für sie ist es beruhigend zu wissen, dass die Versicherer in fast allen Schadenfällen einen Teil der Kosten übernehmen. Allerdings wird es für Einrichtungen immer schwieriger, einen Versicherungsschutz zu erhalten. Dies hat fast alle Gesundheitseinrichtungen dazu veranlasst, ihre Cyberabwehr zu optimieren, um ihren Versicherungsstatus zu verbessern.

Ob Sie eine Versicherung abschließen möchten oder nicht – optimale Cybersecurity ist heute 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, nehmen Sie die Cybersecurity-Dienstleistungen eines MDR-Spezialisten in Anspruch.
- 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.

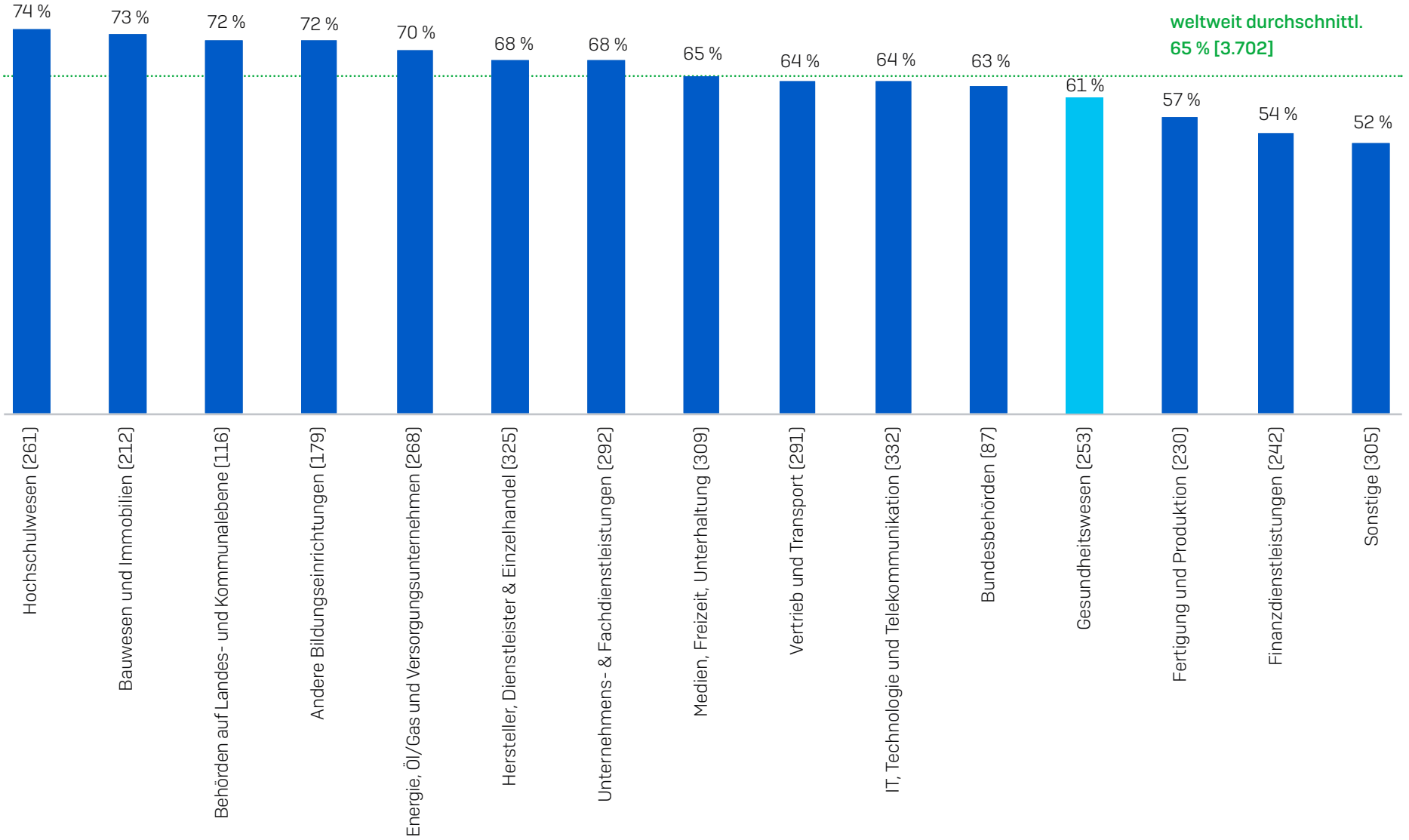
Ausführliche Informationen zu einzelnen Ransomware-Gruppen finden Sie im Sophos Ransomware Threat Intelligence Center.

Gesundheitswesen im Vergleich: Ransomware-Angriffe nach Branche



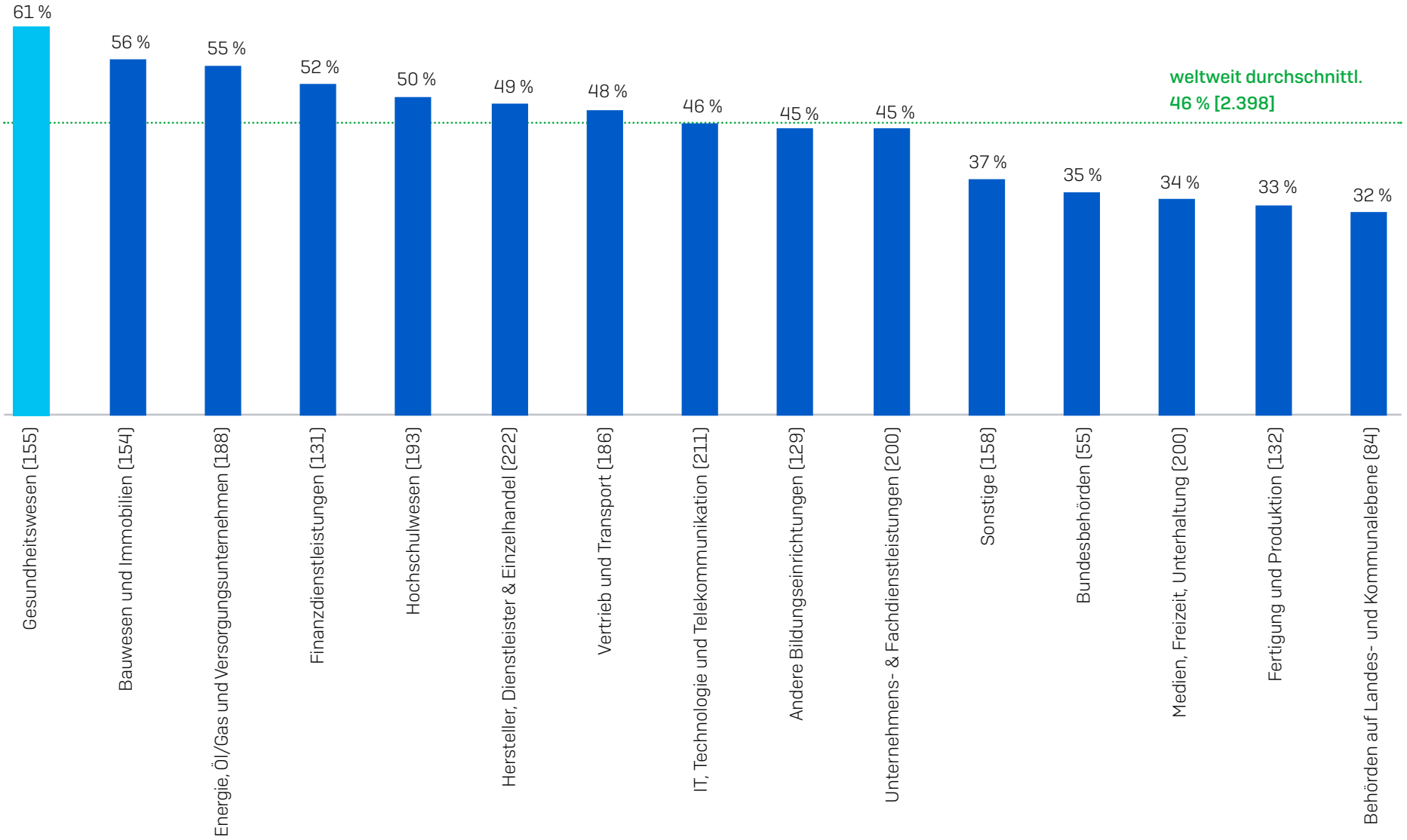
War Ihr Unternehmen im letzten Jahr von Ransomware betroffen? [Anzahl=5.600]

Gesundheitswesen im Vergleich: Datenverschlüsselungsrate nach Branche



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

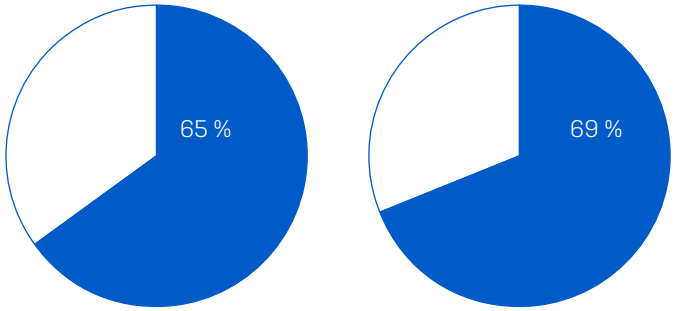
Im Gesundheitswesen ist die Bereitschaft, Lösegeld zu zahlen, am höchsten



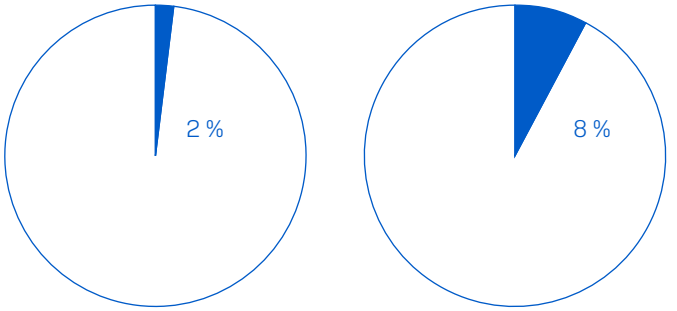
Erhielt Ihr Unternehmen nach dem schwersten Angriff Daten wieder zurück?
(Anzahl=2.398 Organisationen, deren Daten verschlüsselt wurden): Ja, wir haben das Lösegeld gezahlt und Daten zurückerhalten

Nach Zahlung von Lösegeld konnten im Gesundheitswesen weniger Daten wiederhergestellt als im Vorjahr

Prozentsatz der Daten, die nach der Lösegeldzahlung wiederhergestellt wurden

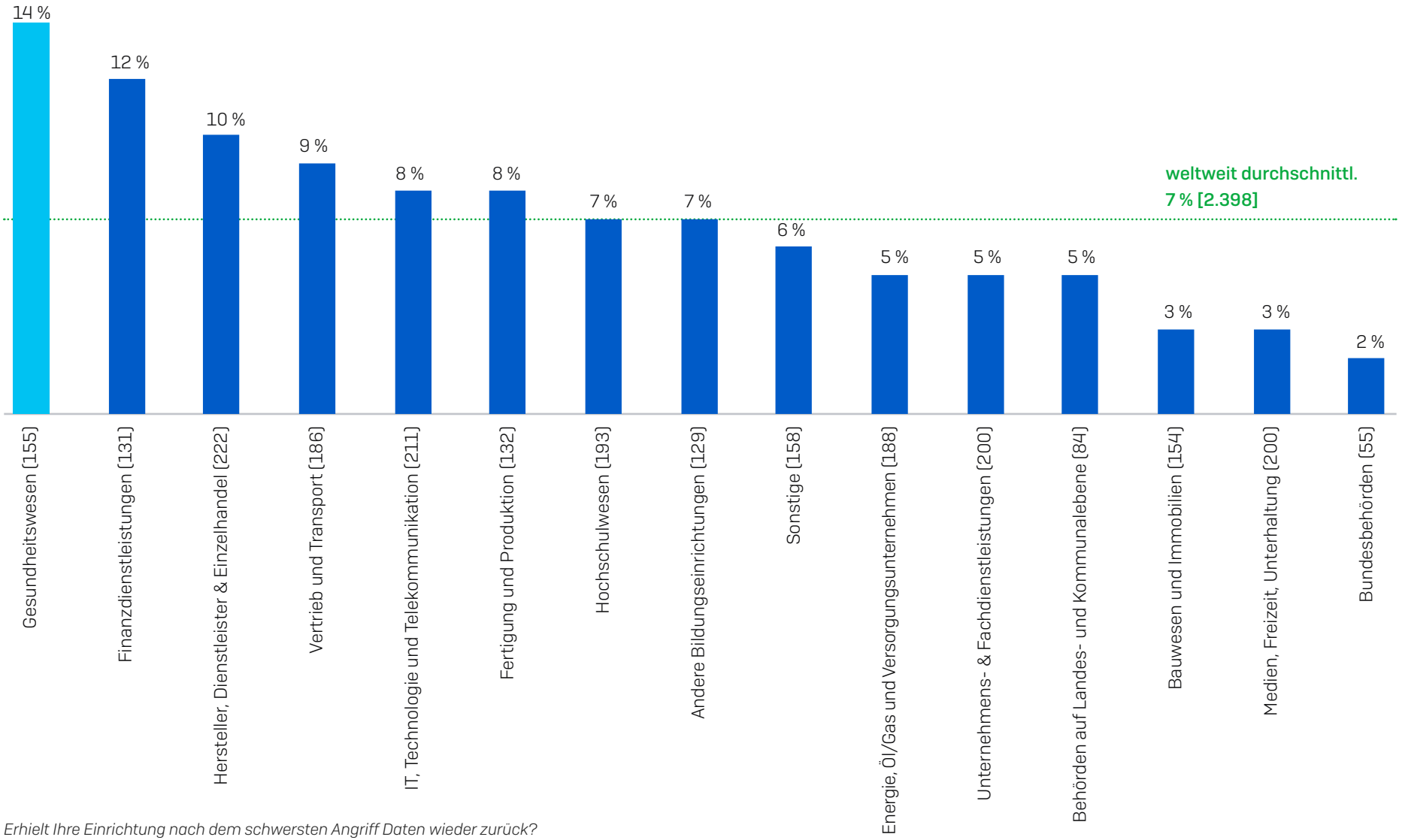


Prozentsatz, der nach der Lösegeldzahlung ALLE DATEN zurückerhalten hat



Wie viele Daten Ihrer Einrichtung haben Sie nach dem schwersten Ransomware-Angriff zurückerhalten?
(94/25 Gesundheitseinrichtungen, die das Lösegeld zahlten und Daten zurückerhalten haben)

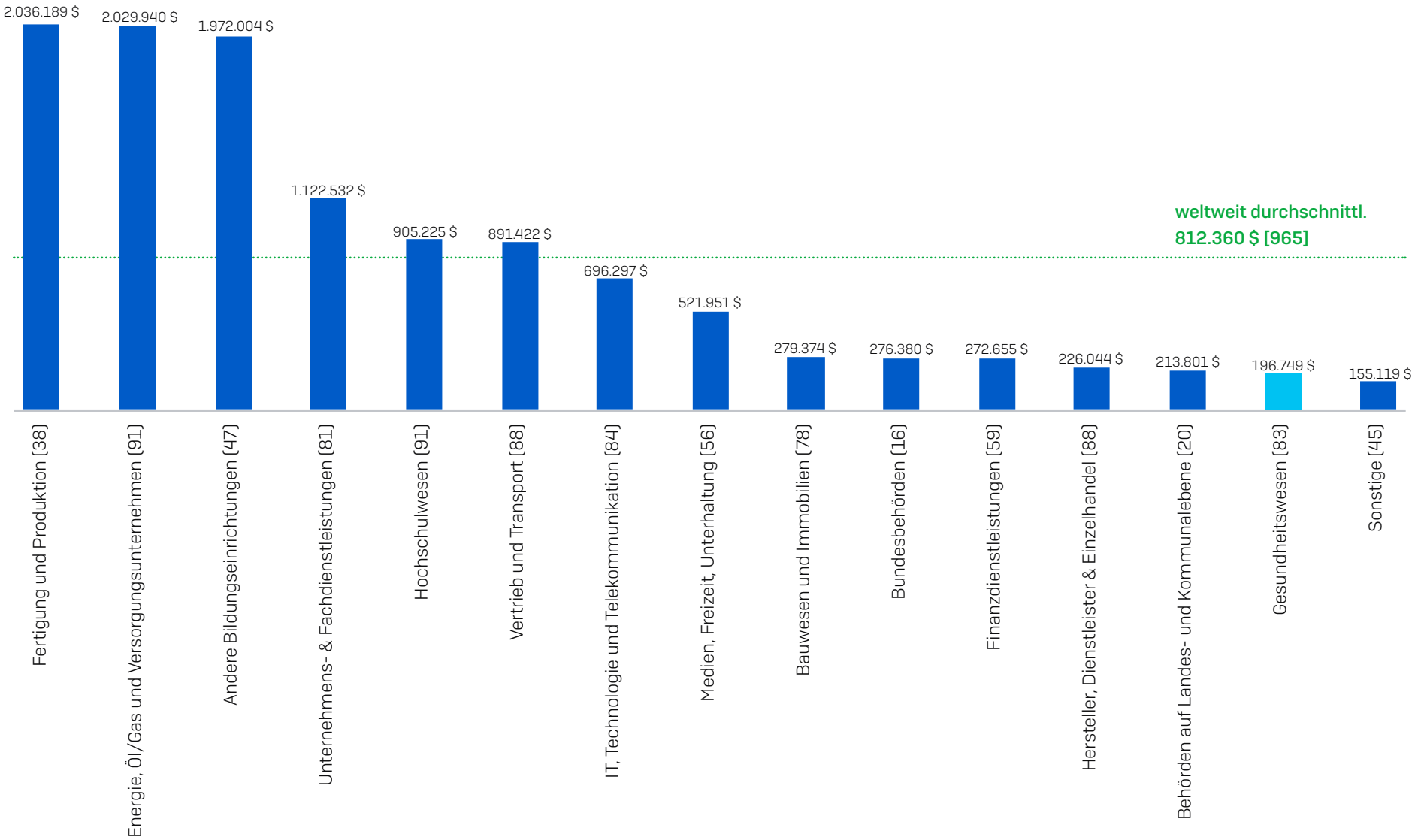
Im Gesundheitswesen werden am ehesten alle drei Methoden zur Wiederherstellung von Daten genutzt



Erhielt Ihre Einrichtung nach dem schwersten Angriff Daten wieder zurück?

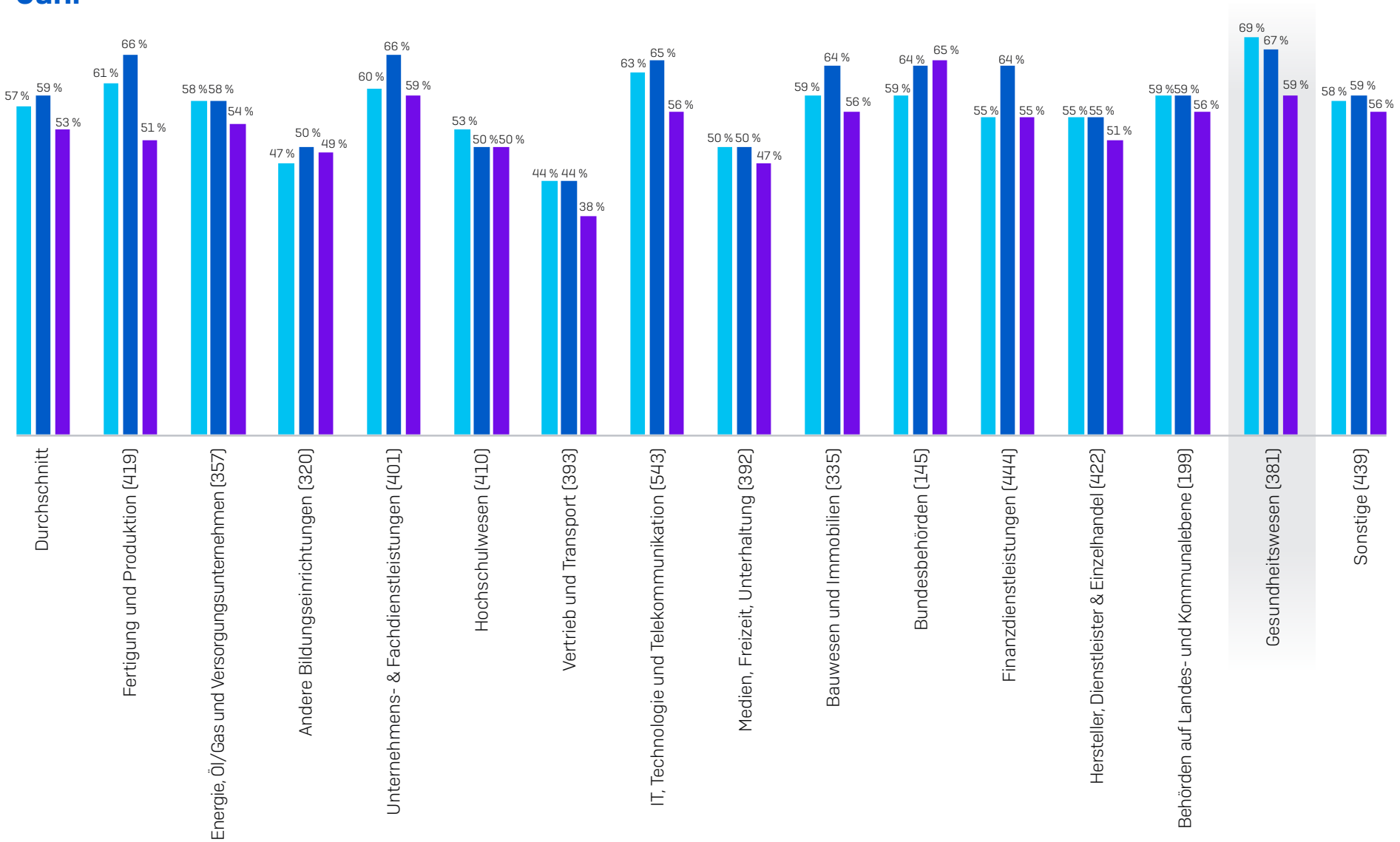
(2.398 Einrichtungen, deren Daten verschlüsselt wurden): Ja, wir haben alle drei Methoden (Backups, Lösegeldzahlung und andere Mittel) genutzt, um die Daten zurückzuerhalten

Das Gesundheitswesen zahlte die niedrigsten Lösegeldsummen



Wie hoch war die Lösegeldsumme, die Ihre Einrichtung beim schwersten Ransomware-Angriff gezahlt hat? Angaben in US-Dollar Anzahl der erhaltenen Antworten jeweils in Klammer; Ohne „Weiß nicht"-Angaben. Bei Branchen mit niedrigen Antwort-Zahlen sind die Ergebnisse nicht repräsentativ, können jedoch als Indikator dienen.

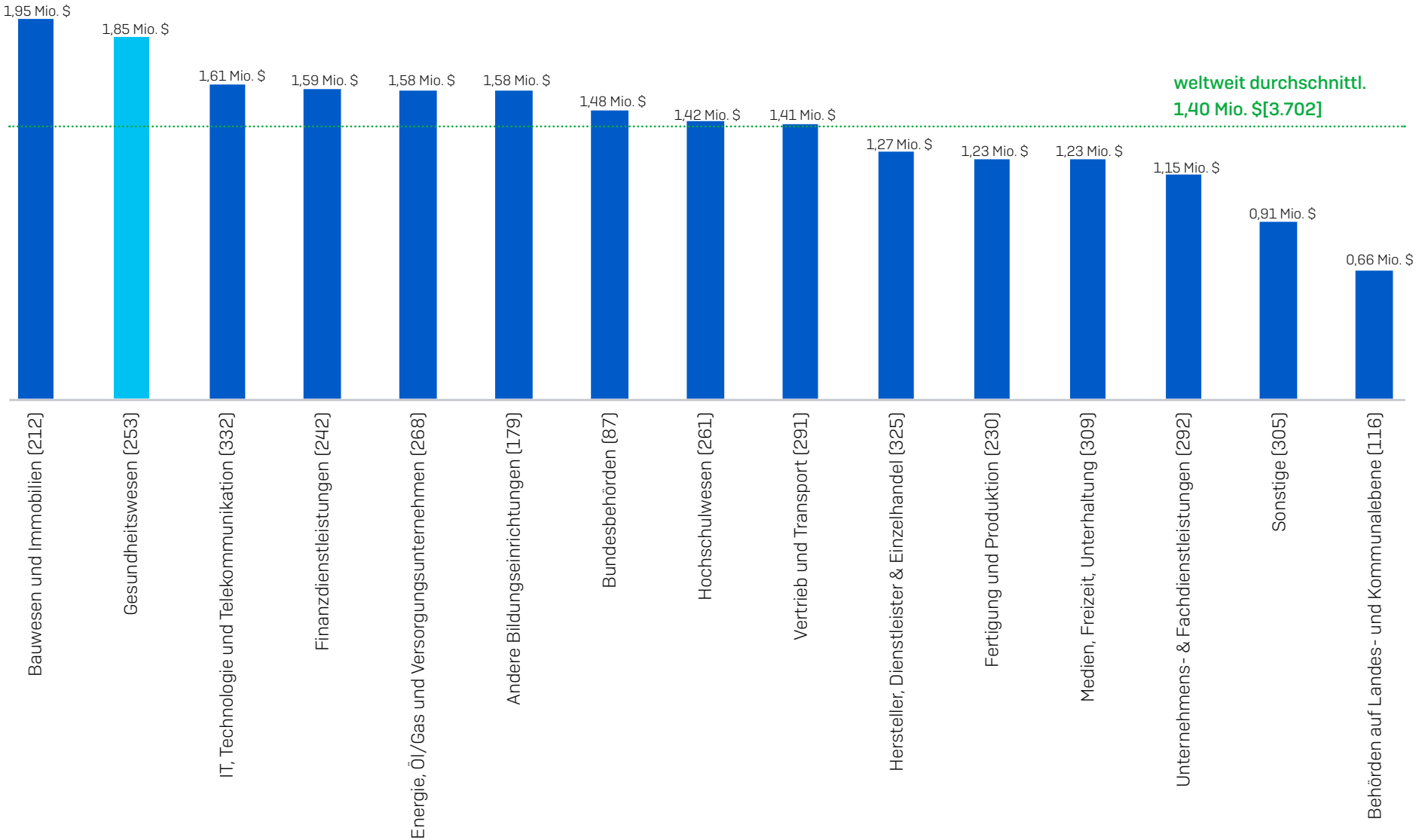
Gesundheitswesen im Vergleich: Veränderung der Erfahrungen mit Cyberangriffen im letzten Jahr



Wie haben sich die Erfahrungen Ihrer Einrichtung mit Cyberangriffen im letzten Jahr in Bezug auf Anzahl, Komplexität und Folgen verändert? (Anzahl=5.600): Hat erheblich zugenommen, hat leicht zugenommen

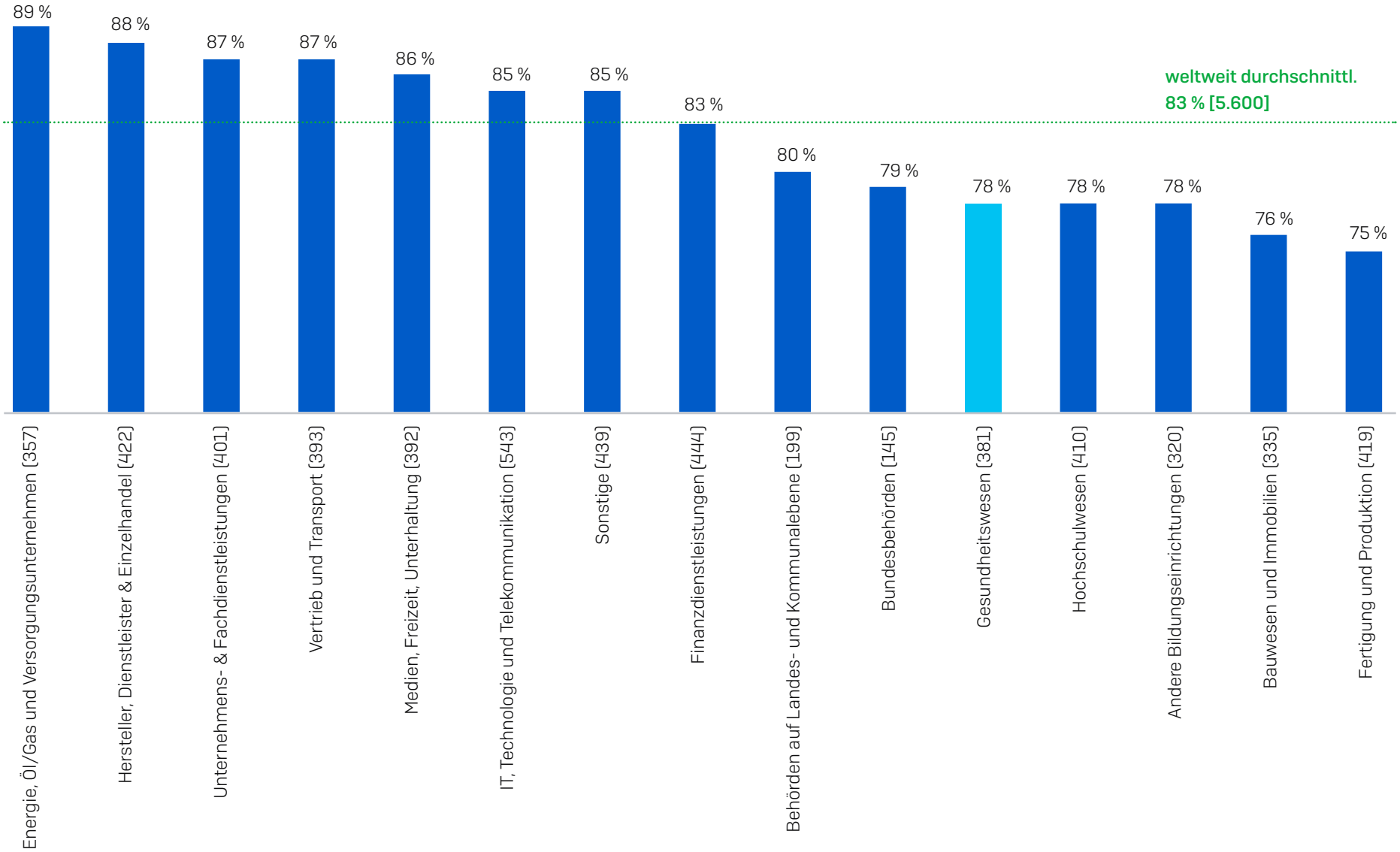
- Zunahme bei der Anzahl von Cyberangriffen
- Zunahme bei der Komplexität von Cyberangriffen
- Zunahme bei den Auswirkungen von Cyberangriffen

Im Gesundheitswesen liegen die Bereinigungskosten nach einem Ransomware-Angriff über dem weltweiten Durchschnitt



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.)? (3.702 Unternehmen/Einrichtungen, die von Ransomware betroffen waren)

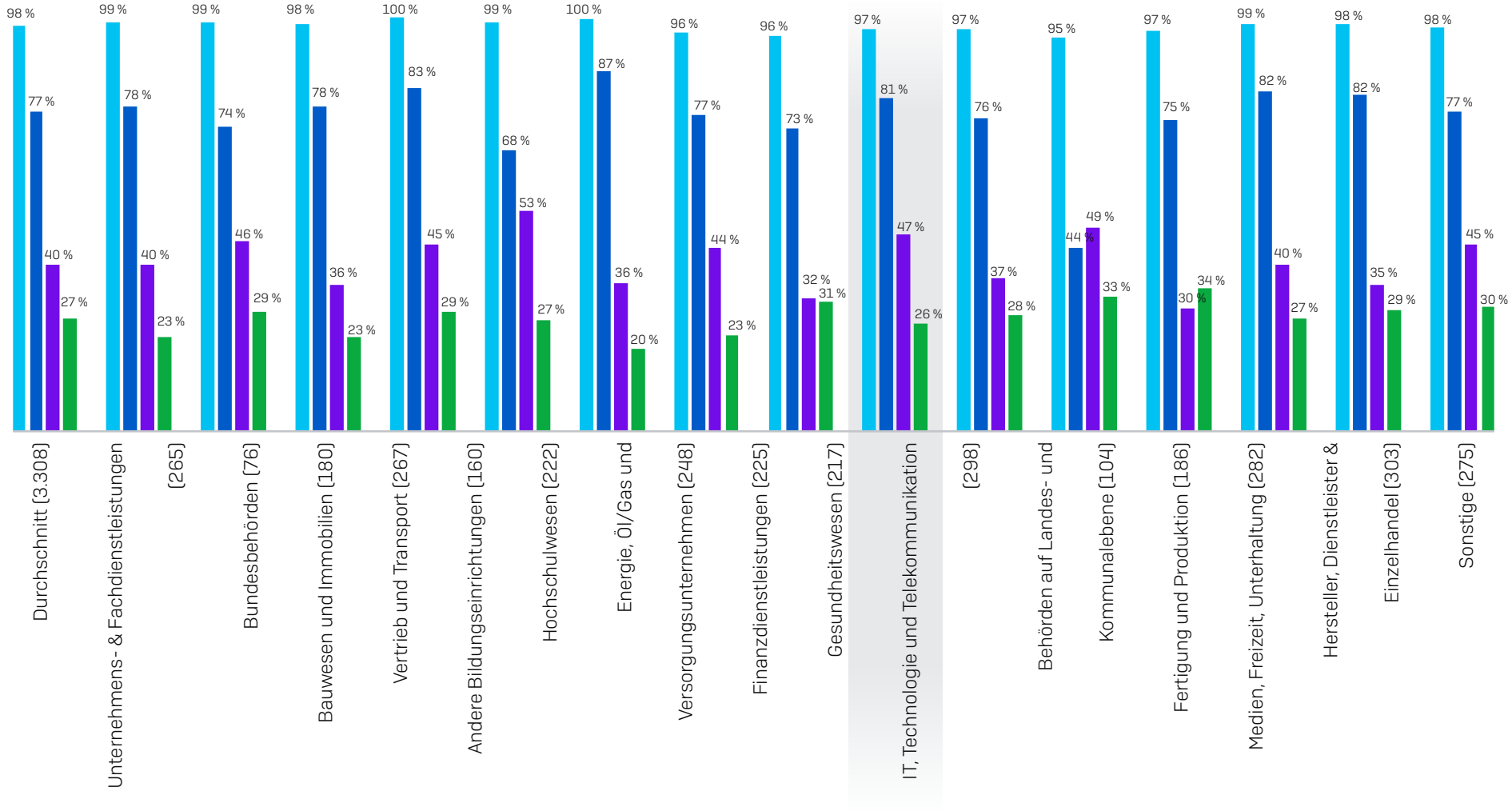
Gesundheitseinrichtungen sind unterdurchschnittlich gegen Cyberangriffe versichert



Hat Ihr Unternehmen eine Cyberversicherung, die für den Schaden aufkommt? (Anzahl der erhaltenen Antworten jeweils in Klammer).

Ja; Ja, aber es gibt Ausnahmen/Ausschlüsse in unserer Police

Gesundheitswesen im Vergleich: Auszahlungsrate von Cyberversicherungen nach Branche



Hat die Cyberversicherung 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.

2022-05-31 (WP-NP)

SOPHOS