SOPHOS
Cybersecurity evolved.

Ransomware-Report 2021

Die von Sophos weltweit angelegte Studie „The State of Ransomware 2021" liefert neue Einblicke in die Erfahrungen mittelständischer Unternehmen mit Erpressungssoftware. Unser Status-Report geht sowohl auf die Häufigkeit von Ransomware-Angriffen als auch auf deren Auswirkungen auf die Opfer ein und beleuchtet Trends im Vergleich zum Vorjahr. In diesem Jahr veröffentlichen wir zum ersten Mal auch die tatsächlichen Lösegeldzahlungen der Opfer sowie die Datenmenge, die sich retten ließ.

Sophos-Whitepaper. April 2021

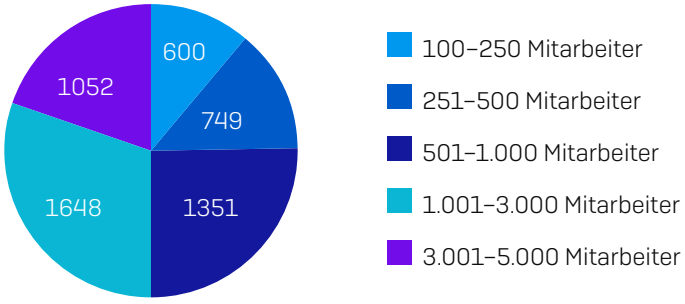
Über die Studie

Sophos hat eine unabhängige Befragung zum Thema Ransomware in Auftrag gegeben, die vom Marktforschungsinstitut Vanson Bourne zwischen Januar und Februar 2021 durchgeführt wurde. Im Rahmen dieser Studie wurden 5.400 IT-Manager in 30 Ländern zu ihren Erfahrungen mit Ransomware befragt.

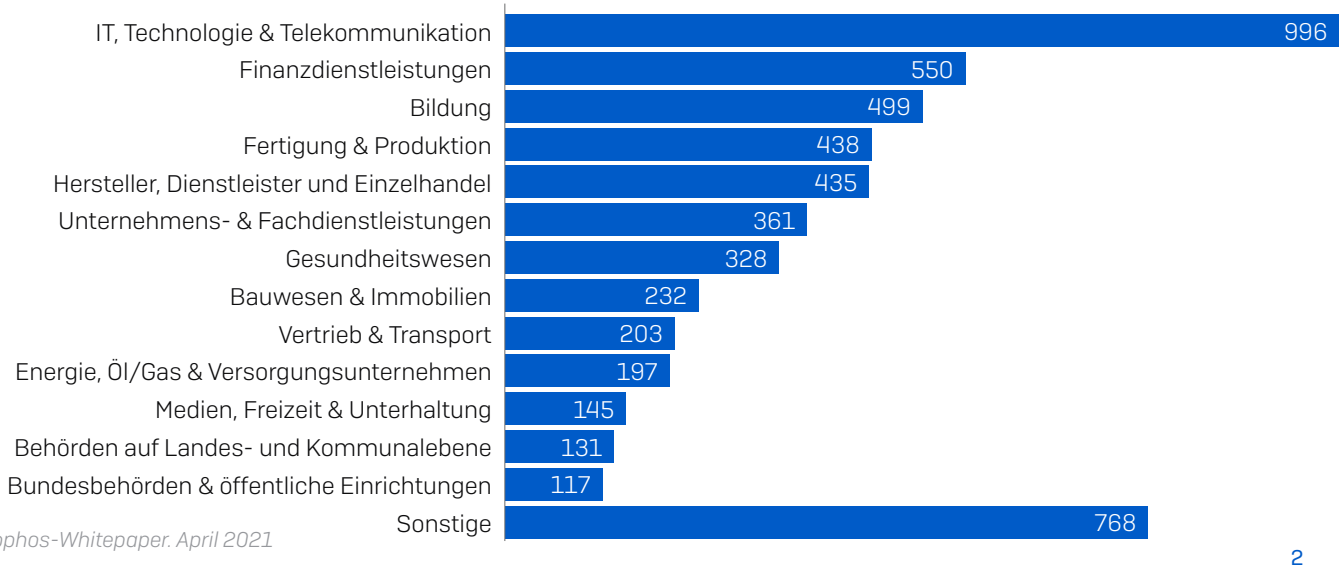
LAND	# UMFRAGETEILNEHMER	LAND	# UMFRAGETEILNEHMER	LAND	# UMFRAGETEILNEHMER
Australien	250	Indien	300	Saudi-Arabien	100
Österreich	100	Israel	100	Singapur	150
Belgien	100	Italien	200	Südafrika	200
Brasilien	200	Japan	300	Spanien	150
Kanada	200	Malaysia	150	Schweden	100
Chile	200	Mexiko	200	Schweiz	100
Kolumbien	200	Niederlande	150	Türkei	100
Tschechische Republik	100	Nigeria	100	VAE	100
Frankreich	200	Philippinen	150	Vereinigtes Königreich	300
Deutschland	300	Polen	100	USA	500

Wie in den vergangenen Jahren stammten die Umfrageteilnehmer zu 50 % aus Unternehmen mit 100 bis 1.000 Mitarbeitern und zu 50 % aus Unternehmen mit 1.001 bis 5.000 Mitarbeitern. Zudem repräsentieren die befragten Unternehmen einen breiten Querschnitt unterschiedlicher Branchen.

Wie viele Mitarbeiter beschäftigt Ihr Unternehmen weltweit?



In welcher Branche sind Sie tätig?



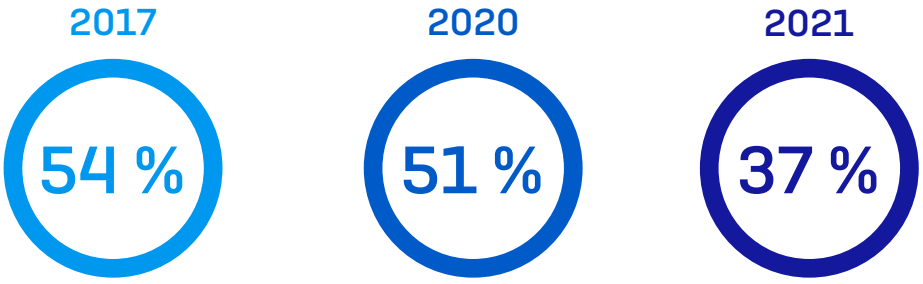
Wichtigste Erkenntnisse

- **37 %** der **Umfrageteilnehmer waren im letzten Jahr Opfer von Ransomware**
- Bei **54 %** der betroffenen Unternehmen gelang es **Cyberkriminellen im Zuge des schwerwiegendsten Angriffs, Daten zu verschlüsseln**
- **96 %** der Betroffenen, deren Daten verschlüsselt wurden, **bekamen ihre Daten** nach dem schwerwiegendsten Ransomware-Vorfall wieder zurück
- Bei Unternehmen mittlerer Größe belief sich das **Lösegeld** durchschnittlich auf **170.404 USD**
- Im Schnitt konnten nach der Lösegeldzahlung jedoch lediglich **65 % der verschlüsselten Daten** wiederhergestellt werden
- Die durchschnittlichen Kosten für die **Bereinigung nach einem Ransomware-Angriff** (Ausfallzeiten, Personal-, Hardware- und Netzwerkkosten sowie entgangene Geschäfte usw.) betrugen **1,85 Millionen USD**
- Sogenannte **Extortion-Angriffe**, bei denen Daten zwar nicht verschlüsselt, aber dennoch Lösegeldforderungen gestellt werden, haben sich im vergangenen Jahr **mehr als verdoppelt** (von 3 % auf 7 %)
- **Geschultes IT-Personal, das Angriffe abwehren kann,** wurde als Hauptgrund dafür angeführt, dass Unternehmen in Zukunft keine Ransomware-Angriffe befürchten

Die Verbreitung von Ransomware

Ransomware stellt nach wie vor eine signifikante Bedrohung dar

Mehr als ein Drittel (37 %) der 5.400 Umfrageteilnehmer fielen im vergangenen Jahr Ransomware-Angriffen zum Opfer, d. h. **mehrere Computer waren von Ransomware betroffen, es wurden jedoch nicht in allen Fällen Daten verschlüsselt**. Zwar bewegt sich der prozentuale Anteil nach wie vor auf einem hohen Niveau, liegt jedoch deutlich unter dem Vorjahr (51 %).

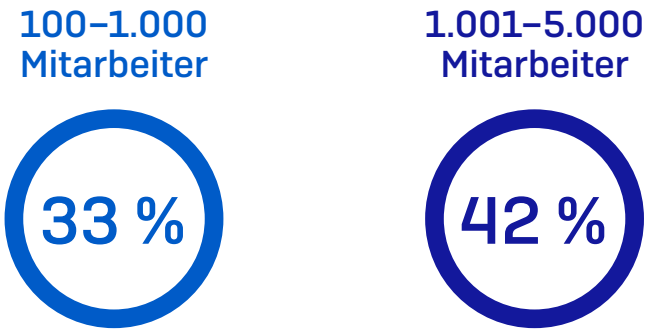


War Ihr Unternehmen im letzten Jahr von Ransomware betroffen? Ja [2021=5.400; 2020=5.000; 2017=2.700], wobei einige Antwortmöglichkeiten übersprungen wurden, im Jahresvergleich

Von den SophosLabs und den „Sophos Managed Threat Response"-Experten beobachtete Änderungen im Angriffsverhalten lassen darauf schließen, dass die rückläufigen Angriffszahlen teilweise auch auf die zunehmende Raffinesse der Cyberkriminellen zurückzuführen sind. So konzentriert sich eine Vielzahl der Angreifer mittlerweile etwa nicht mehr auf groß angelegte, automatisierte Angriffe, sondern geht vielmehr gezielt und manuell vor. Zwar liegt die Gesamtanzahl der Angriffe unter dem Vorjahresniveau, solche gezielten Angriffe besitzen unserer Erfahrung nach jedoch ein weitaus größeres Schadenspotenzial.

Je größer das Unternehmen, desto höher die Angriffswahrscheinlichkeit

Wenn wir die Anzahl der Ransomware-Vorfälle nach Unternehmensgröße betrachten, zeigt sich, dass größere Unternehmen mehr Angriffe verzeichneten: 42 % der befragten Unternehmen mit 1.001 bis 5.000 Mitarbeitern waren Opfer von Ransomware. Bei kleineren Unternehmen lag der prozentuale Anteil bei 33 %.

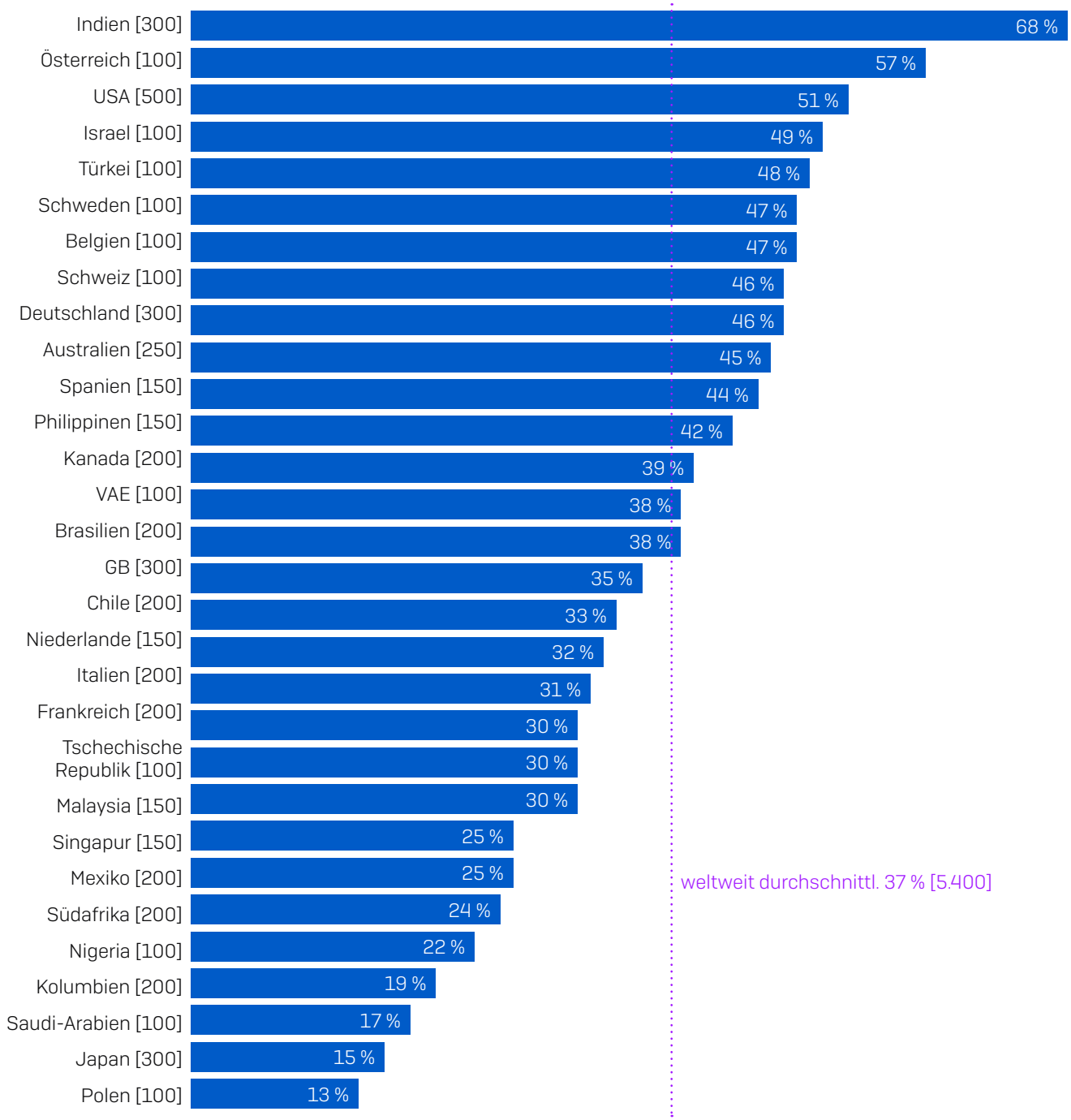


War Ihr Unternehmen im letzten Jahr von Ransomware betroffen? Ja [5.400], wobei einige Antwortmöglichkeiten übersprungen wurden, aufgeschlüsselt nach Unternehmensgröße

Auch der Abstand zwischen kleineren und größeren Unternehmen vergrößerte sich im vergangenen Jahr von 7 % in 2020 auf 9 %. Größere Unternehmen gelten als lukrativere Ziele. Die Konzentration der Angreifer auf diese Gruppe überrascht also kaum. Dennoch verzeichnete immerhin ein Drittel der befragten kleineren Unternehmen im letzten Jahr Ransomware – ein klarer Beleg dafür, dass die Angreifer auch diese Unternehmen nach wie vor durchaus ins Visier nehmen. Es gibt schlichtweg keine Gewinner.

Das Angriffsaufkommen ist standortabhängig

Eine Analyse der Daten nach Land, in dem die befragten Unternehmen ansässig sind, liefert interessante Ergebnisse.



War Ihr Unternehmen im letzten Jahr von Ransomware betroffen? Ja [Basiszahlen im Diagramm], wobei einige Antwortmöglichkeiten übersprungen wurden, im Ländervergleich

Indien führt die Liste an – 68 % der Befragten verzeichneten im letzten Jahr Ransomware-Angriffe. Obgleich meist Ransomware-Akteure aus China, Nordkorea, Russland oder anderen ehemaligen Ostblockstaaten in die Schlagzeilen geraten, beobachten die SophosLabs auch zahlreiche Ransomware-Angriffe von indischen Cyberkriminellen auf indische Unternehmen.

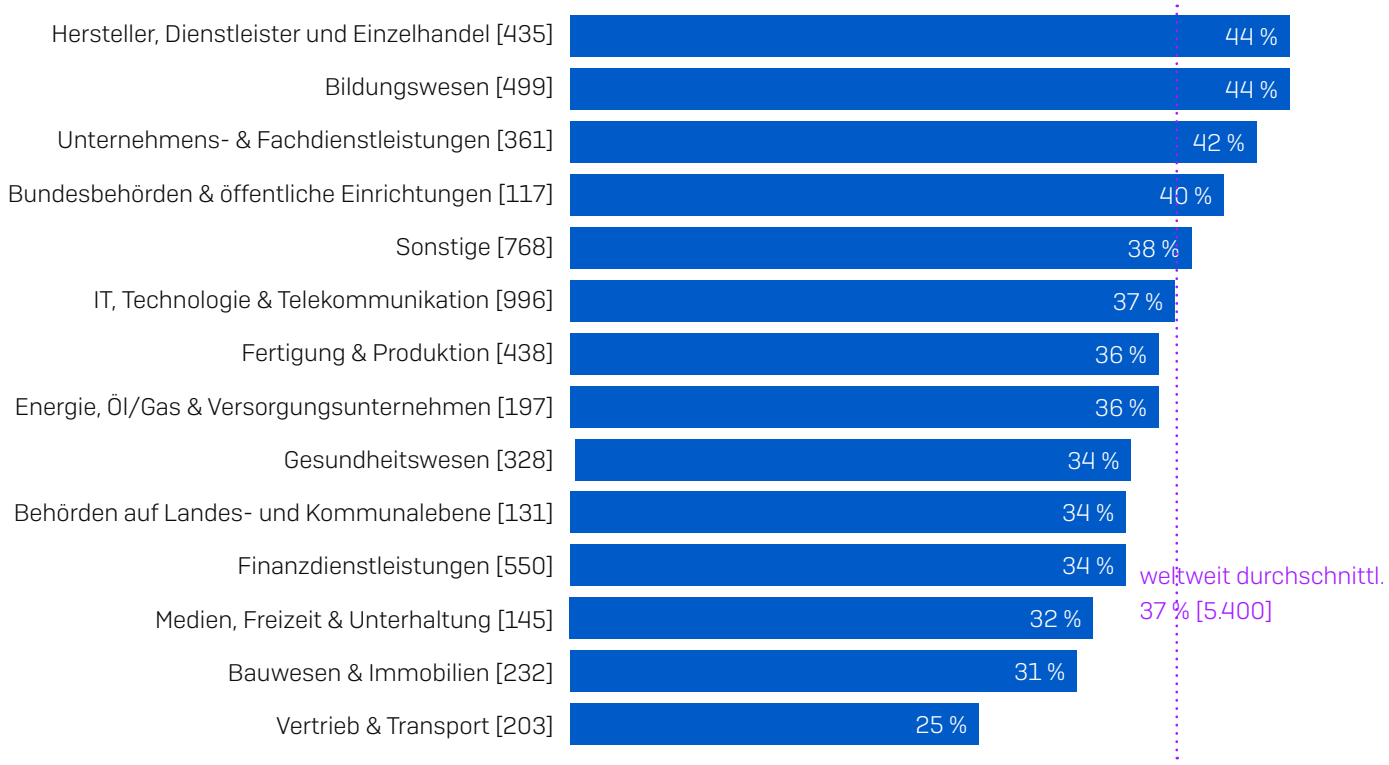
Da sich Hacker hohe Lösegeldsummen von US-amerikanischen Unternehmen versprechen, sind die **USA** ein beliebtes Ziel – 51 % der Umfrageteilnehmer aus den USA meldeten Ransomware-Angriffe.

In **Polen, Kolumbien, Nigeria, Südafrika** und **Mexiko** werden die wenigsten Angriffe verzeichnet, was aller Wahrscheinlichkeit nach auf das vergleichsweise niedrigere BIP und die damit verbundenen geringen Lösegelderwartungen zurückzuführen ist.

Japan sticht als Industrieland mit einem äußerst geringen Ransomware-Aufkommen hervor – lediglich 15 % der befragten Unternehmen waren im vergangenen Jahr betroffen. Japanische Unternehmen melden in unseren Umfragen regelmäßig ein sehr geringes Ransomware-Aufkommen. Dies kann daran liegen, dass japanische Unternehmen massiv in Anti-Ransomware-Technologien investieren oder dass die japanische Sprache aufgrund ihrer Einzigartigkeit Angriffe erschwert.

Hersteller, Dienstleister, Einzelhandel und Bildungswesen verzeichnen die meisten Ransomware-Vorfälle

Die Angriffswahrscheinlichkeit variiert stark je nach Branche.



War Ihr Unternehmen im letzten Jahr von Ransomware betroffen? Ja [Basiszahlen im Diagramm], wobei einige Antwortmöglichkeiten übersprungen wurden, im Branchenvergleich

Im Bereich **Hersteller, Dienstleister und Einzelhandel** und im **Bildungswesen** wurden die meisten Angriffe gemeldet – 44 % der befragten Branchenvertreter waren Opfer von Ransomware.

Obwohl Ransomware-Angriffe auf Einrichtungen des **Gesundheitswesens** immer wieder in die Schlagzeilen geraten, lagen die gemeldeten Angriffe mit 34 % knapp unter dem Durchschnitt. Die Überrepräsentation dieser Branche in den Medien ist vermutlich auf regulatorische Auflagen zurückzuführen, aufgrund derer Gesundheitseinrichtungen im Gegensatz zu vielen Wirtschaftsunternehmen Angriffe offenlegen müssen.

Die Folgen von Ransomware

Verschlüsselung ist rückläufig. Extortion-Angriffe sind auf dem Vormarsch.

Wir haben von Ransomware betroffene Unternehmen gefragt, ob es den Angreifern gelungen ist, Daten zu verschlüsseln. 54 % bejahten dies. 39 % der befragten Unternehmen konnten den Angriff stoppen, bevor ihre Daten verschlüsselt wurden. Bei 7 % wurden zwar keine Daten verschlüsselt, aber dennoch Lösegeldforderungen gestellt.

Wenn wir diese Zahlen mit dem Vorjahr vergleichen, zeichnet sich ein interessanter Trend ab.

2020	2021	
73 %	54 %	Cyberkriminelle konnten Daten verschlüsseln
24 %	39 %	Der Angriff wurde gestoppt, bevor Daten verschlüsselt werden konnten
3 %	7 %	Lösegeld wurde gefordert, obwohl keine Daten verschlüsselt wurden

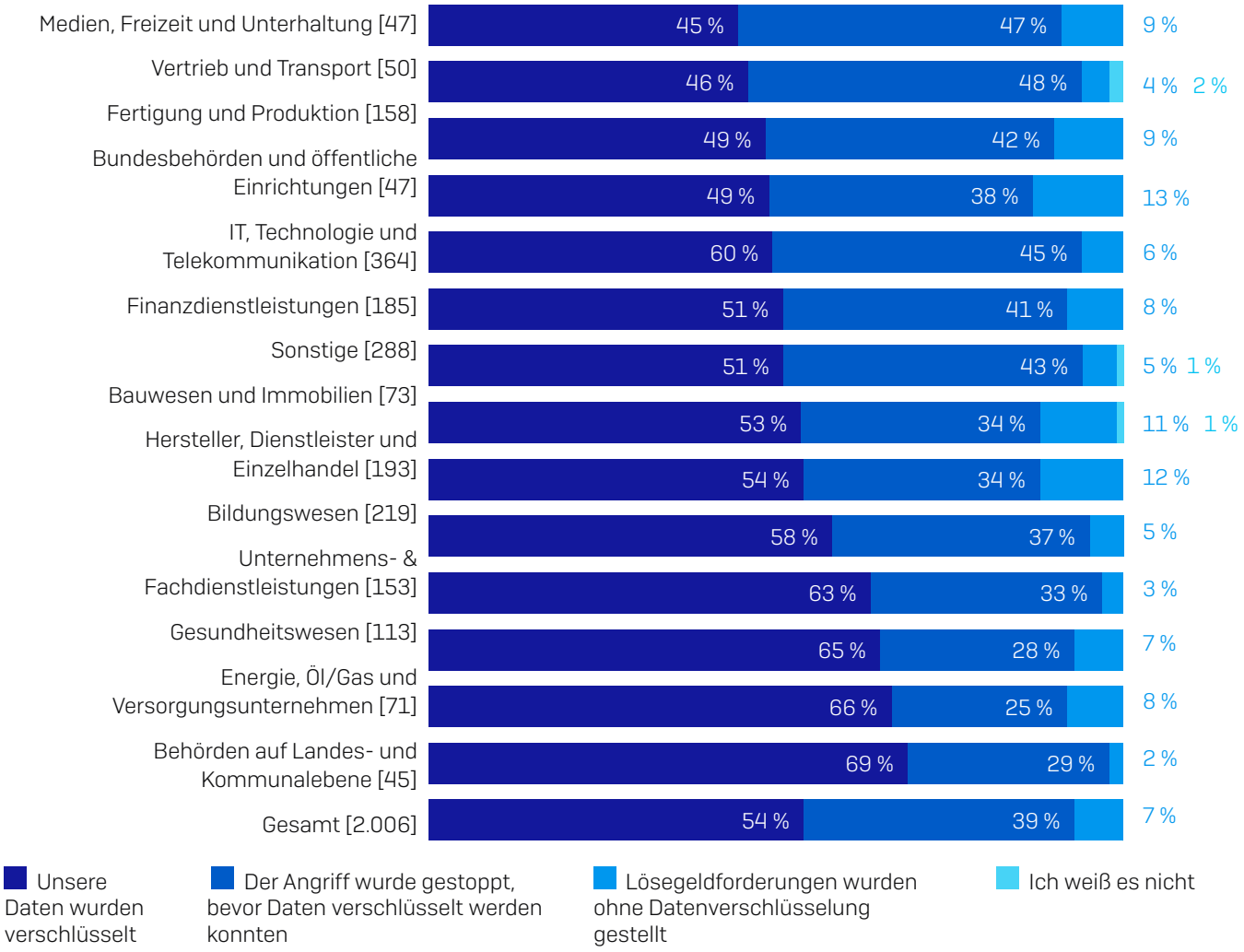
Konnten Cyberkriminelle im Verlauf des schwerwiegendsten Angriffs Ihre Unternehmensdaten verschlüsseln? [2021=2.006, 2020=2.538]
Unternehmen, die im vergangenen Jahr von Ransomware betroffen waren

Im Verlauf des letzten Jahres sank der prozentuale Anteil der Angriffe, bei denen Cyberkriminelle Daten verschlüsselten, drastisch von 73 % auf 54 %. Dies ist darauf zurückzuführen, dass wesentlich mehr Unternehmen Angriffe stoppen konnten, bevor es zur Verschlüsselung ihrer Daten kam. Ein eindeutiges Indiz dafür, dass sich Investitionen in Anti-Ransomware-Technologie bezahlt machen.

Angriffe, bei denen Daten zwar nicht verschlüsselt wurden, es aber dennoch zu Lösegeldforderungen kam, haben sich jedoch mehr als verdoppelt. Es kommt nun vermehrt zu Extortion-Angriffen. Dabei verschlüsseln Angreifer keine Daten, sondern drohen mit der Veröffentlichung von Daten, wenn kein Lösegeld gezahlt wird. Extortion-Angriffe sind weniger aufwendig, da keine Ver- bzw. Entschlüsselung erforderlich ist. Dabei treiben Cyberkriminelle ihre Forderungen in die Höhe, indem sie auf die drastischen Geldstrafen hinweisen, die bei einer Verletzung des Schutzes personenbezogener Daten verhängt werden können.

Eine Verhinderung der Verschlüsselung ist branchenabhängig

Inwieweit Unternehmen die Verschlüsselung ihrer Daten erfolgreich abwehren, variiert stark von Branche zu Branche.



Konnten Cyberkriminelle im Verlauf des schwerwiegendsten Angriffs Ihre Unternehmensdaten verschlüsseln? [Basiszahlen im Diagramm]
Unternehmen, die im vergangenen Jahr von Ransomware betroffen waren

Am erfolgreichsten bei der Abwehr der Verschlüsselung von Daten sind Unternehmen im Bereich **Vertrieb und Transport** (48 %), gefolgt von **Medien, Freizeit und Unterhaltung** (47 %).

Die größte Wahrscheinlichkeit für eine Datenverschlüsselung im Zuge eines Ransomware-Angriffs besteht bei **Behörden auf Landes- und Kommunalebene** (69 %). Dies hat vermutlich die beiden folgenden Gründe:

- Schwächere Abwehrmechanismen: In der Regel haben Behörden auf Landes- und Kommunalebene mit niedrigen IT-Budgets und überlastetem bzw. mangelndem IT-Personal zu kämpfen.
- Gezielte Angriffe: Aufgrund ihrer Größe sowie ihrem Zugang zu öffentlichen Mitteln gelten Regierungsbehörden nicht selten als lukrative Ziele und werden Opfer gezielter, komplexer Angriffe. Außerdem ist die Bereitschaft, Lösegeldforderungen nachzukommen, bei Regierungsbehörden besonders hoch, wie wir später noch sehen werden.

Bundesbehörden sowie öffentliche Einrichtungen sind besonders anfällig für Extortion-Angriffe (13 %).

Im **Gesundheitswesen** liegt die Zahl der Angriffe wie bereits erwähnt unter dem Durchschnitt. Allerdings gelingt es Angreifern in fast zwei Dritteln der Fälle (65 %), Dateien zu verschlüsseln, was deutlich über dem Durchschnitt liegt.

Mehr Opfer zahlen Lösegeld

Wir haben Unternehmen, deren Daten verschlüsselt wurden (1.086), gefragt, ob sie ihre Daten wieder zurückerhalten haben und wenn ja, wie.

2020	2021	
26 %	32 %	zahlten Lösegeld, um Daten wieder zurückzubekommen
56 %	57 %	stellten Daten über Backups wieder her
12 %	8 %	stellten Daten mit anderen Mitteln wieder her
94 %	96 %	konnten Daten zumindest teilweise wiederherstellen

Hinweis: Aufgrund der Rundung entsprechen einige Gesamtsummen nicht der Summe der einzelnen Zahlen

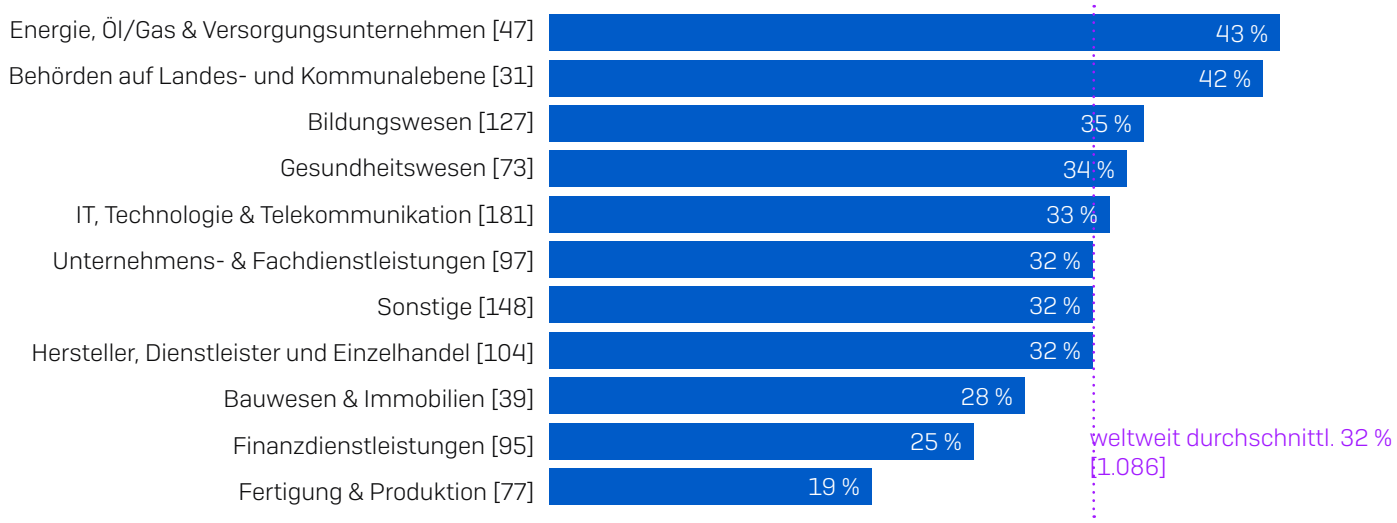
Erhielt Ihr Unternehmen die Daten nach dem schwerwiegendsten Ransomware-Angriff wieder zurück?

[2021=1.086, 2020=1.849] Unternehmen, deren Daten verschlüsselt wurden

Wie aus der obigen Grafik hervorgeht, zahlten 32 % das Lösegeld, um ihre Daten zurückzubekommen, was einem Anstieg um 26 % gegenüber der Umfrage des Vorjahres entspricht. 57 % konnten ihre Daten mit Hilfe von Backups wiederherstellen. Dieser Prozentsatz bewegt sich in etwa auf dem gleichen Niveau wie im vergangenen Jahr. Insgesamt bekamen beinahe alle Unternehmen (96 %) zumindest einen Teil ihrer Daten zurück.

Die Zahlungsbereitschaft ist branchenabhängig

Die Bereitschaft, Lösegeldforderungen nachzukommen, variiert enorm je nach Branche.



Erhielt Ihr Unternehmen die Daten nach dem schwerwiegendsten Ransomware-Angriff wieder zurück? Ja, wir haben das Lösegeld bezahlt [Basiszahlen im Diagramm] Unternehmen, deren Daten im Zuge des schwerwiegendsten Ransomware-Angriffs verschlüsselt wurden, wobei einige Antwortmöglichkeiten übersprungen wurden, im Branchenvergleich

Im Bereich **Energie, Öl/Gas und Versorgung** ist die Bereitschaft, Lösegeldforderungen zu zahlen, am höchsten. 43 % der befragten Unternehmen aus diesem Bereich gaben der Lösegeldforderung nach. Da die Infrastruktur in Unternehmen dieser Branche häufig veraltet ist und sich nicht einfach erneuern lässt, sehen sich Ransomware-Opfer oft zur Zahlung gezwungen, um die fortlaufende Bereitstellung der Dienste zu gewährleisten.

In **Behörden auf Landes- und Kommunalebene** ist die Bereitschaft zur Zahlung von Lösegeld mit 42 % am zweithöchsten. Interessanterweise entspricht dies der bereits erwähnten Erkenntnis, dass dieser Bereich am ehesten von einer Datenverschlüsselung betroffen ist. Vermutlich zielen Cyberkriminelle aufgrund der hohen Zahlungsbereitschaft von Behörden auf Landes- und Kommunalebene auch vermehrt auf diese ab.

Allem Anschein nach besteht ein Zusammenhang zwischen der Fähigkeit eines Unternehmens, Daten mit Hilfe von Backups wiederherzustellen, und seiner Bereitschaft, Lösegeldforderungen nachzukommen. In der **Fertigung und Produktion** tätige Unternehmen zahlen am seltensten Lösegeld und sind gleichzeitig am ehesten in der Lage, Daten mit Hilfe von Backups wiederherzustellen (68 %). Auch im Bereich **Bauwesen und Immobilien** sowie bei **Finanzdienstleistern** finden unterdurchschnittlich oft Lösegeldzahlungen statt. Beiden gelingt es überdurchschnittlich oft, ihre Daten aus Backups wiederherzustellen.

Bundesbehörden und öffentliche Einrichtungen werden in der Grafik nicht aufgeführt, da keine hinreichenden Daten vorliegen. Aus den Angaben der Befragten geht jedoch hervor, dass von den 23 Behörden, deren Daten verschlüsselt wurden, 61 % ihre Daten mit Hilfe von Backups wiederherstellen konnten und lediglich 26 % das Lösegeld zahlten. Eine mögliche Erklärung dafür, warum dieser Bereich so anfällig für Extortion-Angriffe ist.

Keine Garantie auf vollständige Datenfreigabe trotz Lösegeldzahlung

65 %

der Daten wurden nach der Lösegeldzahlung wiederhergestellt

Durchschnittlicher prozentualer Anteil der Daten, den Unternehmen nach dem schwerwiegendsten Ransomware-Angriff [344] nach der Lösegeldzahlung wieder zurückbekamen

Was bei Lösegeldforderungen nicht erwähnt wird: Auch wenn Opfer das Lösegeld bezahlen, ist die Wahrscheinlichkeit, dass sie sämtliche Daten zurückbekommen, verschwindend gering. Im Schnitt erhielten Unternehmen, die das Lösegeld gezahlt hatten, nur 65 % der verschlüsselten Dateien zurück – mehr als ein Drittel der Daten war also nicht mehr zugänglich. 29 % der Befragten gaben an, dass 50 % oder weniger Daten wiederhergestellt wurden und lediglich 8 % bekamen sämtliche Daten wieder zurück.

Die Kosten von Ransomware

Lösegeldforderungen variieren enorm

Von den 357 Umfrageteilnehmern, die Lösegeldforderungen nachgekommen waren, teilten uns 282 Unternehmen die genaue Lösegeldsumme mit. Im Durchschnitt beliefen sich die Zahlungen in dieser Gruppe auf **170.404 USD**. Die Summen variierten jedoch sehr stark von Unternehmen zu Unternehmen. Am häufigsten wurde eine Lösegeldsumme von 10.000 USD bezahlt (laut Angabe von 20 Befragten), die höchste Summe lag bei schwindelerregenden 3,2 Millionen USD (laut Angabe von zwei Befragten).

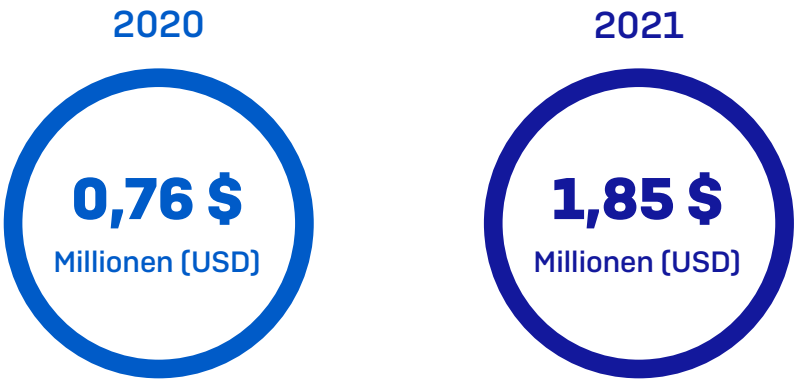
Aus diversen Gründen weichen diese Zahlen stark von den achtstelligen Lösegeldsummen ab, die häufig in den Schlagzeilen zu finden sind.

1. **Unternehmensgröße.** Da sich unsere Umfrageteilnehmer aus kleinen und mittelständischen Unternehmen mit 100 bis 5.000 Mitarbeiten zusammensetzen, sind die finanziellen Mittel im Vergleich zu größeren Unternehmen meist begrenzt. Ransomware-Akteure passen ihre Lösegeldforderungen an die Zahlungsfähigkeit ihrer Opfer an, d. h. kleinere Unternehmen müssen entsprechend weniger bezahlen. Unsere Umfrageergebnisse belegen dies: Die durchschnittlich gezahlte Lösegeldsumme in Unternehmen mit 100 bis 1.000 Mitarbeitern beläuft sich auf 107.694 USD, in Unternehmen mit 1.000 bis 5.000 Mitarbeitern auf 225.588 USD.
2. **Art des Angriffs.** Cyberkriminelle gehen auf unterschiedliche Art und Weise vor: von hochkomplexen Angreifern, die mit ausgefeilten Taktiken, Techniken und Prozessen (TTPs) auf einzelne Unternehmen abzielen, bis hin zu weniger versierten Hackern, die vorgefertigte Ransomware-Kits für generische Spray-and-Pray-Angriffe nutzen. Ransomware-Akteure, die intensiv in gezielte Angriffe investieren, versprechen sich ein entsprechend hohes Lösegeld. Die Gewinnerwartungen bei generischen Angriffen sind hingegen meist niedriger.
3. **Standort.** Die höchsten Lösegeldforderungen erhalten Unternehmen in westlichen Industriestaaten, da deren Zahlungsfähigkeit als am höchsten eingeschätzt wird. Die beiden Höchstsummen wurden von italienischen Unternehmen bezahlt. Ferner beliefen sich Lösegeldzahlungen in den USA, Kanada, Großbritannien, Deutschland und Australien im Schnitt auf 214.096 USD. Sie liegen somit 26 % über dem Durchschnitt (Basis: 101 Befragte). In Indien betrugen Lösegeldforderungen im Mittel dagegen 76.619 USD – weniger als die Hälfte des weltweiten Durchschnitts. (Basis: 86 Befragte).

Die Kosten zur Bereinigung nach einem Ransomware-Angriff haben sich im letzten Jahr mehr als verdoppelt

Neben der Begleichung des Lösegelds kommen viele zusätzliche Kosten auf die Opfer zu. Zwar waren sowohl die Gesamtanzahl der Ransomware-Angriffe als auch die Angriffe, bei der Cyberkriminelle Daten verschlüsseln konnten, im vergangenen Jahr rückläufig, doch die für die Bereinigung des Angriffs anfallenden Gesamtkosten sind deutlich gestiegen.

Aus unserer Studie geht hervor, dass sich der mit dem Ransomware-Angriff einhergehende finanzielle Aufwand im Schnitt auf 1,85 Millionen USD belief (unter Berücksichtigung von Ausfallzeiten, Arbeitsstunden, Geräte- und Netzwerkkosten, entgangenen Umsatzchancen, Lösegeld usw.). Dies ist eine Verdopplung im Vergleich zum Vorjahr (761.106 USD).

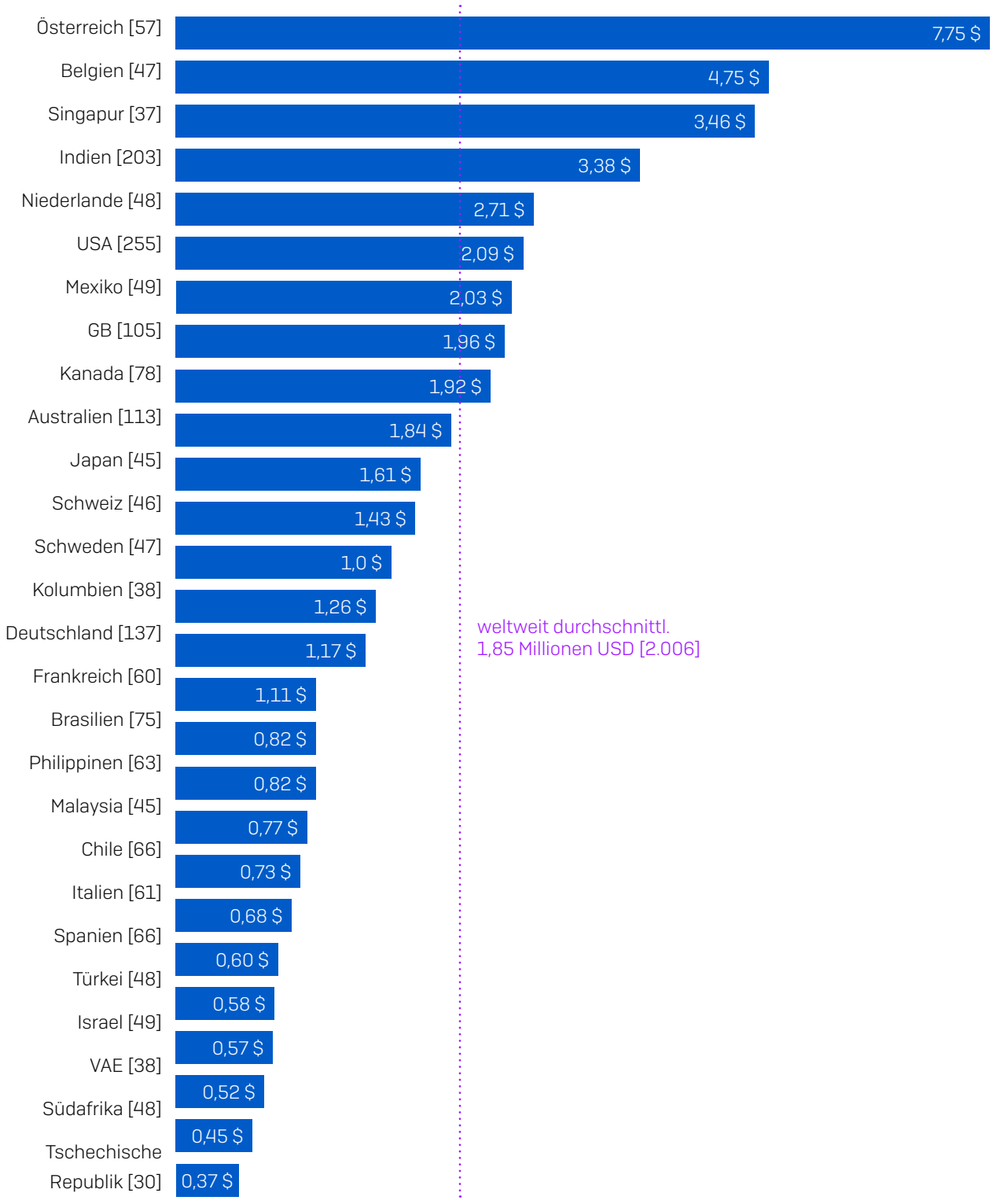


Finanzieller Aufwand, der Unternehmen im Schnitt durch Ransomware-Angriffe entstand (unter Berücksichtigung von Ausfallzeiten, Arbeitsstunden, Geräte- und Netzwerkkosten, entgangenen Umsatzchancen, Lösegeld usw.) [2021=2.006, 2020=2.538] Unternehmen, die im vergangenen Jahr von Ransomware betroffen waren, im Jahresvergleich

Im vergangenen Jahr verzeichneten unsere Experten einen signifikanten Anstieg an komplexen Ransomware-Angriffen, bei denen verstärkt auf eine Kombination aus Automatisierung und manuellem Hacking gesetzt wird. Ebenso komplex gestaltet sich die Wiederherstellung bei solchen Angriffen. Dies dürfte auch der Grund für die steigenden Bereinigungskosten sein.

Bereinigungskosten variieren je nach Standort

Der mit der Bereinigung einhergehende finanzielle Aufwand variiert stark je nach Standort der betroffenen Unternehmen.



Finanzieller Aufwand, der Unternehmen im Schnitt durch Ransomware-Angriffe entstand (unter Berücksichtigung von Ausfallzeiten, Arbeitsstunden, Geräte- und Netzwerkkosten, entgangenen Umsatzchancen, Lösegeld usw.) [Basiszahlen im Diagramm] Unternehmen, die im vergangenen Jahr von Ransomware betroffen waren, im Ländervergleich, in Mio. USD

Österreich sticht als das Land mit den höchsten Bereinigungskosten hervor, die durch Ransomware verursacht wurden. Österreichische Unternehmen waren im vergangenen Jahr von mehreren spektakulären Cyberangriffen betroffen. So fiel Meldungen zufolge etwa das österreichische Außenministerium einem staatlich finanzierten Akteur zum Opfer, und die Cyberkriminellen der Ransomware-Gruppe Netwalker behaupteten auf Twitter, das städtische IT-Netzwerk der österreichischen Stadt Weiz infiltriert zu haben. Doch selbst wenn wir Österreich aus der Statistik herausnehmen, liegen die durchschnittlichen Bereinigungskosten bei 1,68 Millionen USD und sind somit immer noch mehr als doppelt so hoch wie im Vorjahr.

Im Allgemeinen melden Länder mit einem höheren Lohnniveau wie Belgien, Singapur, die Niederlande und die USA die höchsten Gesamtkosten. Länder mit einem niedrigeren Lohnniveau wie die Tschechische Republik und Südafrika verzeichnen wiederum auch die niedrigsten Gesamtkosten. Diese Zahlen belegen den enormen finanziellen und manuellen Aufwand, der mit der Bereinigung nach einem Angriff einhergeht. Tatsächlich belaufen sich die Gesamtkosten zur Bereinigung nach einem Ransomware-Angriff auf das Zehnfache des durchschnittlichen Lösegelds.

Israel zählt zu den Industrieländern mit den geringsten Gesamtkosten für die Bereinigung nach einem Ransomware-Angriff. Aus geopolitischen Gründen ist Israel ein Hauptangriffsziel für Cyberkriminelle (nicht nur Ransomware-Akteure). Demzufolge sind Cyberabwehr-Maßnahmen sowie die Expertise zur Bereinigung nach Angriffen im gesamten Land besonders ausgeprägt. So erklären sich die verhältnismäßig geringen finanziellen Auswirkungen von Ransomware-Angriffen.

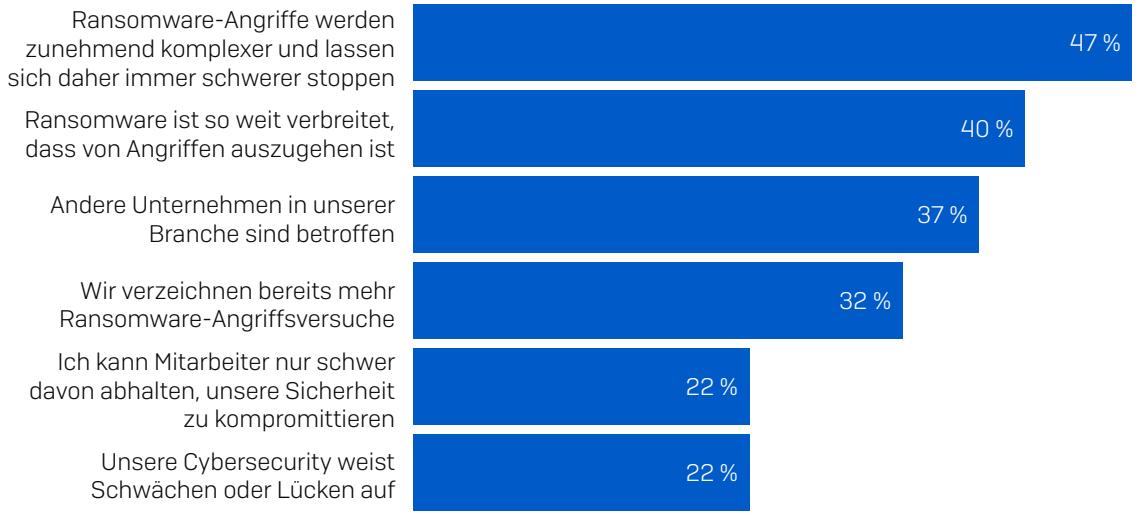
Die Zukunft

Nicht alle Unternehmen sehen sich von Ransomware bedroht

62 % der Umfrageteilnehmer (3.353) gaben an, dass sie im vergangenen Jahr nicht von Ransomware betroffen waren. In dieser Gruppe lassen sich starke Diskrepanzen hinsichtlich der Einstellung zum Umgang mit Ransomware feststellen. 65 % gehen davon aus, dass sie in Zukunft Opfer von Ransomware werden könnten, 35 % rechnen nicht mit Angriffen.

Warum rechnen Unternehmen mit Ransomware-Angriffen?

Die meisten (47 %) der 2.187 Unternehmen, die im letzten Jahr zwar nicht von Ransomware-Angriffen betroffen waren, jedoch künftig mit Angriffen rechnen, gaben an, dass „Ransomware-Angriffe zunehmend komplexer werden und sich daher immer schwerer stoppen lassen".



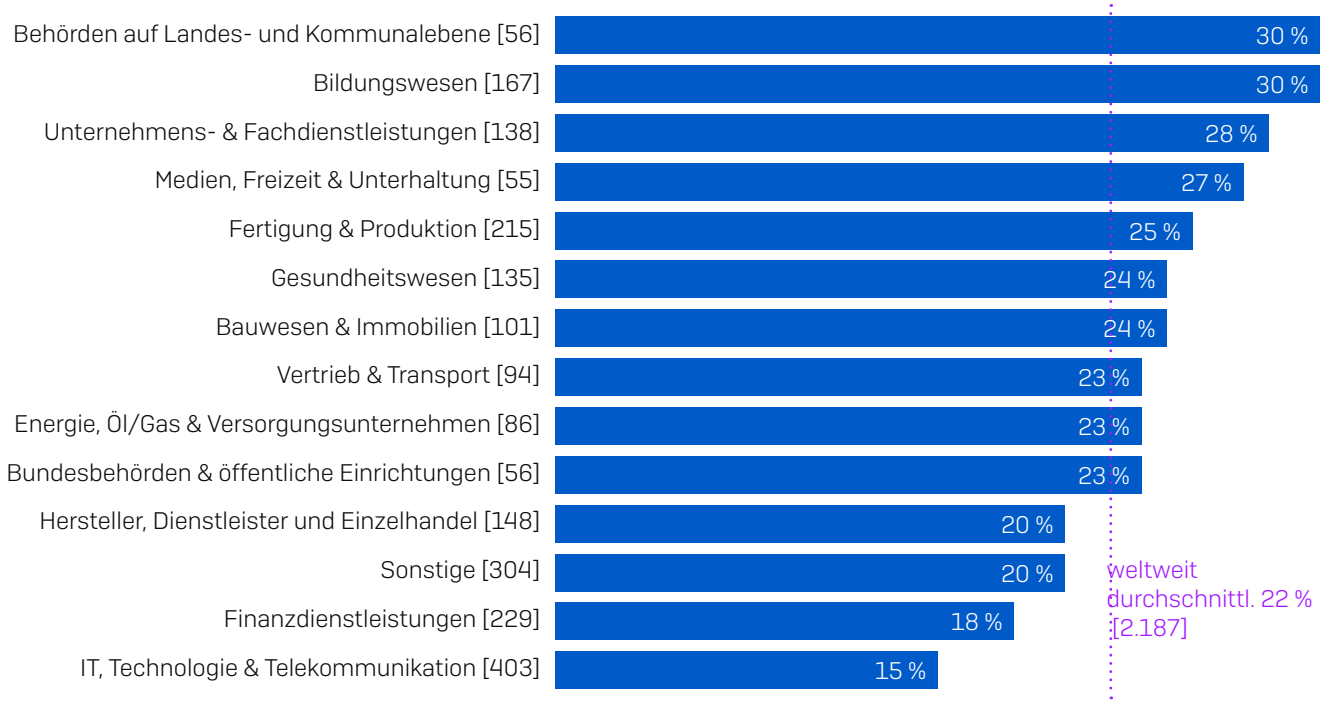
Warum gehen Sie davon aus, dass Ihr Unternehmen in Zukunft von Ransomware betroffen sein könnte? [2.187] Unternehmen, die im letzten Jahr nicht von Ransomware betroffen waren, jedoch in Zukunft mit Angriffen rechnen, wobei einige Antwortmöglichkeiten übersprungen wurden

So hoch diese Zahl auch klingen mag: Die Tatsache, dass sich diese Unternehmen der zunehmenden Komplexität von Ransomware bewusst sind, ist in jedem Fall positiv. Dieses Bewusstsein könnte auch erklären, warum diese Unternehmen in der Lage waren, Angriffe im vergangenen Jahr abzuwehren.

22 % betrachten Benutzer als wichtigen Risiko-Faktor für mögliche Ransomware-Angriffe in der Zukunft. An dieser Zahl ist erfreulicherweise zu sehen, dass die meisten IT-Abteilungen die Schuld nicht nur den Mitarbeitern zuschieben.

So gaben auch 22 % der Befragten an, dass ihre Cybersecurity Schwächen oder Lücken aufweise. Sicherheitslücken sind natürlich problematisch, doch schon allein das Bewusstsein darüber, dass hier Probleme bestehen, ist ein erster wichtiger Schritt in der Stärkung der Abwehrmechanismen.

Zu den Branchen, die sich am ehesten Sicherheitslücken eingestehen, gehören Behörden auf Landes- und Kommunalebene sowie das Bildungswesen (jeweils 30 %).



Warum gehen Sie davon aus, dass Ihr Unternehmen in Zukunft von Ransomware betroffen sein könnte? Unsere Cybersecurity weist Schwächen oder Lücken auf [Basiszahlen im Diagramm] Unternehmen, die im letzten Jahr nicht von Ransomware betroffen waren, jedoch in Zukunft mit Angriffen rechnen, wobei einige Antwortmöglichkeiten übersprungen wurden, im Branchenvergleich

Zwar fielen die Umfrageteilnehmer, die diese Frage beantworteten, nicht selbst Ransomware zum Opfer, aller Wahrscheinlichkeit nach wurden sie jedoch von den Ransomware-Vorfällen in ihrer Branche beeinflusst:

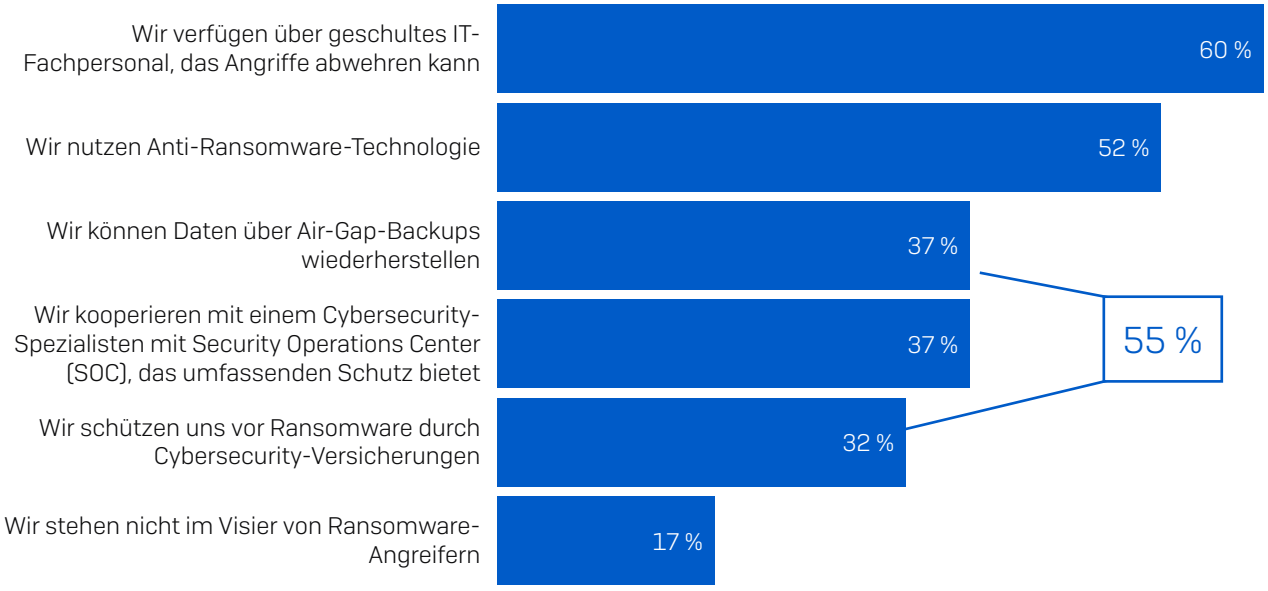
- Bei **Behörden auf Landes- und Kommunalebene** ist die Wahrscheinlichkeit am größten, dass es zur Verschlüsselung der Daten kommt
- Die meisten Unternehmen, die im vergangenen Jahr Opfer von Ransomware waren, sind im **Bildungswesen** und im Bereich **„Hersteller, Dienstleister und Einzelhandel“** tätig

In beiden Branchen mangelt es in der Regel an den nötigen finanziellen Mitteln für Technologie und IT, was wiederum zu Lücken in der Cybersecurity führt.

Von den Umfrageteilnehmern aus den Bereichen **IT, Technologie und Telekommunikation** (15 %) und **Finanzdienstleistungen** (18 %) gaben die wenigsten Unternehmen an, dass ihre Cybersecurity Lücken aufweise. Da beide Branchen neue Technologien relativ schnell einführen und ihnen meist auch mehr finanzielle Mittel zur Verfügung stehen, können sie Schwachstellen besser ausgleichen.

IT-Fachpersonal gibt Unternehmen Sicherheit beim Umgang mit Ransomware

1.166 der befragten Unternehmen, die im vergangenen Jahr keine Ransomware-Angriffe verzeichnet hatten, rechnen nicht mit Angriffen in der Zukunft. Als Hauptgrund für diese Zuversicht führten sie ihr geschultes IT-Fachpersonal an, das in der Lage ist, Angriffe abzuwehren.



Warum gehen Sie nicht davon aus, dass Ihr Unternehmen in Zukunft von Ransomware betroffen sein könnte? [1.166] Unternehmen, die im letzten Jahr nicht von Ransomware betroffen waren und in Zukunft nicht mit Angriffen rechnen, wobei einige Antwortmöglichkeiten übersprungen wurden

Moderne, automatisierte Technologien stellen zwar durchaus wesentliche Komponenten einer effektiven Anti-Ransomware-Abwehr dar, manuell agierende Hacker lassen sich jedoch nur stoppen, wenn geschultes Fachpersonal die Technologie überwacht und bei Bedarf eingreift. Egal ob interne IT-Teams oder externe Experten diese Aufgabe übernehmen: Geschultes Personal erkennt Anzeichen dafür, dass Ransomware-Akteure Ihr Unternehmen ins Visier nehmen.

37 % der befragten Unternehmen, die nicht mit Ransomware rechnen, arbeiten mit auf Cybersecurity spezialisierten Partnern mit einem umfassenden Security Operations Center (SOC) zusammen. Noch vor wenigen Jahren waren SOCs Großkonzernen vorbehalten, doch mittlerweile haben auch mittelständische Unternehmen die Notwendigkeit eines effektiven Cypersecurity-Konzepts erkannt.

Doch es gibt nicht nur gute Nachrichten. Teilweise geben die Ergebnisse Anlass zur Besorgnis:

- 55 % der Umfrageteilnehmer, die nicht von Angriffen ausgehen, vertrauen auf einen Ansatz, der keinerlei Schutz vor Ransomware bietet:
  - 37 % der befragten Unternehmen führten Air-Gap-Backups als Grund dafür an, dass sie keine Angriffe befürchten. Wie wir bereits gesehen haben, sind Backups zwar durchaus ein probates

Mittel zur Datenwiederherstellung nach einem Angriff, sie schützen jedoch nicht davor.

- 32 % der Befragten erklärten, dass Cybersecurity-Versicherungen sie vor Ransomware bewahren. Auch Versicherungen erleichtern die Schadensbegrenzung zwar durchaus, können Angriffe jedoch nicht verhindern.

Manche Umfrageteilnehmer wählten beide Optionen, 55 % mindestens eine Option aus.

- Darüber hinaus gehen 17 % der Befragten nicht davon aus, dass Ransomware-Akteure sie ins Visier nehmen. Das entspricht jedoch leider nicht der Realität. Kein Unternehmen ist vor diesen Angriffen sicher.

IT-Wiederherstellungspläne sind Standard

Auf einen kritischen Cybersecurity-Vorfall reagieren zu müssen, setzt viele Sicherheitsteams unter enormen Stress. Sich von der erzeugten Drucksituation komplett zu befreien, ist leider ein Ding der Unmöglichkeit. Mit einer effektiven Incident-Response-Strategie lassen sich mögliche Schäden jedoch auf ein Minimum reduzieren.

Es stimmt also sehr positiv, dass 90 % der befragten Unternehmen über einen Wiederherstellungsplan nach einem Angriff verfügen. Bei knapp über der Hälfte (51 %) liegt ein vollständig ausgearbeiteter Plan vor, 39 % der befragten Unternehmen haben diesen teilweise erstellt.

In vielerlei Hinsicht lässt sich die Wiederherstellung nach einem Malware-Angriff mit dem Wiederaufbau nach einer Naturkatastrophe vergleichen. In beiden Fällen müssen Sie darauf vorbereitet sein, dass Sie ganz von vorne anfangen müssen. Unternehmen in den Philippinen, einem Land das häufig von Fluten und Erdbeben heimgesucht wird, sind am besten für Malware-Vorfälle gerüstet: 83 % der befragten Unternehmen verfügen über vollständig ausgearbeitete, detaillierte Wiederherstellungspläne.

Regierungsbehörden sind am wenigsten auf Malware-Angriffe vorbereitet

Viele Branchen sind in der Lage, ihre Daten nach einem Malware-Angriff wiederherzustellen. Wie aus unserer Umfrage hervorgeht, sind Regierungsbehörden jedoch am wenigsten für die Abwehr von Malware-Angriffen gerüstet: Lediglich 73 % der **Behörden auf Landes- und Kommunalebene** und 81 % der **Bundesbehörden und öffentlichen Einrichtungen** besitzen einen Wiederherstellungsplan.

Die Tatsache, dass Ransomware-Akteure sehr häufig auf diese Branchen abzielen, gibt Anlass zur Besorgnis. Insbesondere bei Behörden auf Landes- und Kommunalebene ist die Wahrscheinlichkeit, dass Daten im Zuge eines Angriffs verschlüsselt werden, am größten. Bundesbehörden und öffentliche Einrichtungen sind hingegen besonders anfällig für Extortion-Angriffe.

Der Mangel an Wiederherstellungsplänen nach Malware-Angriffen trägt möglicherweise dazu bei, dass Behörden auf Landes- und Kommunalebene am zweithäufigsten Lösegeldforderungen nachkommen.

Empfehlungen

In Anbetracht der Ergebnisse unserer Studie empfehlen wir folgende Best Practices:

1. **Gehen Sie davon aus, dass Sie einem Angriff zum Opfer fallen werden.** Ransomware befindet sich nach wie vor auf dem Vormarsch. Keine Branche, kein Land und kein Unternehmen sind vor Angriffen gefeit. Vorsicht ist besser als Nachsicht.

2. **Sichern Sie Ihre Daten.** Backups sind die gängigste Methode zur Datenwiederherstellung nach einem Angriff. Wie bereits erwähnt, lassen sich auch trotz Lösegeldzahlung in der Regel nicht alle Daten wiederherstellen. Back-ups sind also ohnehin unerlässlich.

3. **Setzen Sie auf mehrschichtige Abwehrmaßnahmen.** Angesichts des signifikanten Anstiegs von Extortion-Angriffen ist es wichtiger denn je, Cyberkriminelle schon im Vorfeld abzuwehren, bevor sie Ihr Unternehmensnetzwerk kompromittieren können. Setzen Sie in der gesamten Umgebung auf mehrschichtigen Schutz.

4. **Kombinieren Sie das Know-how von IT-Experten mit Anti-Ransomware-Technologie.** Ein zentraler Aspekt bei der Abwehr von Ransomware besteht in der Kombination von dedizierter Anti-Ransomware-Technologie mit Threat Hunting durch hochqualifizierte Bedrohungsexperten. Während die Technologie für das erforderliche Maß an Automatisierung und Skalierbarkeit sorgt, erkennen Cybersecurity-Experten Taktiken, Techniken und Prozesse, die auf Angriffsversuche hindeuten. Wenn Ihr Unternehmen nicht über entsprechende interne Experten verfügt, empfiehlt sich die Zusammenarbeit mit auf Cybersecurity spezialisierten Partnern – SOCs sind mittlerweile eine realistische Option für Unternehmen jeder Größe.

5. **Zahlen Sie kein Lösegeld.** Das sagt sich natürlich leicht, wenn Ihr Unternehmen aufgrund eines Ransomware-Angriffs stillsteht. Von moralischen Aspekten ganz abgesehen, bekommen Sie die Daten durch die Zahlung von Lösegeld nicht immer vollständig zurück. Wenn Sie sich dennoch dazu entschließen, Lösegeldforderungen nachzukommen, sollten Sie bei Ihrer Kosten-Nutzen-Analyse bedenken, dass Cyberkriminelle im Schnitt lediglich zwei Drittel Ihrer Daten wiederherstellen.

6. **Erarbeiten Sie einen Wiederherstellungsplan.** Vorbereitung ist die beste Strategie, um zu verhindern, dass sich ein Cyberangriff zu einer weitreichenden Sicherheitspanne entwickelt. Nach einem Angriff stellen Unternehmen oft fest, dass ihnen ein Incident-Response-Plan für Cybersecurity-Vorfälle viel Kosten, Probleme und Betriebsunterbrechungen erspart hätte.

Mehr erfahren

Unser Sophos Incident Response Guide unterstützt Sie bei der Aufstellung Ihres eigenen Incident-Response-Plans und geht auf zehn wichtige Punkte ein, die Sie beim Erstellen Ihrer Strategie berücksichtigen sollten.

Wichtige Einblicke in die Abwehr von Cybersecurity-Vorfällen liefern Ihnen außerdem unsere vier Insider-Tipps von Incident-Response-Experten.

Beide Guides basieren auf den realen Erfahrungen der Response-Experten von Sophos, die bereits auf Tausende von Cybersecurity-Vorfällen reagiert und diese erfolgreich neutralisiert haben.

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.

19.04.2021 (SB-NP)

SOPHOS