cybereason

RANSOMWARE:
DIE WIRKLICHEN KOSTEN FÜR UNTERNEHMEN

PreventID

Globale Studie zu den Auswirkungen von Ransomware für Unternehmen

EINFÜHRUNG
EINBLICKE EINES CEO

Im Mai 2021 gab Colonial Pipeline bekannt, dass das Unternehmen Opfer eines verheerenden Ransomware-Angriffs geworden war. Der Angriff legte den Betrieb still und schnitt Millionen von Menschen von der Brennstoffversorgung ab, was zu massiven wirtschaftlichen Schäden im Osten der USA führte. Das FBI bestätigte, dass die Attacken von der DarkSide Ransomware-Gruppe ausgeführt wurden, einem relativ neuen Angreifer, den Cybereason schon seit August 2020 beobachtete.

Schätzungen zufolge erfolgt im Durchschnitt alle 11 Sekunden ein Ransomware-Angriff auf Unternehmen, wobei sich die weltweiten Ransomware-Schäden in diesem Jahr auf voraussichtlich 20 Milliarden US-Dollar belaufen werden. Das FBI berichtet von einem Anstieg der Gesamtverluste durch Ransomware um mehr als 225% im Jahr 2020 allein in den USA.

Die Bewältigung der Nachwirkungen eines Ransomware-Angriffs ist kompliziert und kostspielig. Die wichtigsten Erkenntnisse dieser neuen Studie zeigen, dass die überwiegende Mehrheit der Unternehmen aufgrund von Ransomware-Angriffen erhebliche geschäftliche Auswirkungen erfahren hat, darunter Umsatzeinbußen und Schädigung der Marke des Unternehmens, unplanmäßige Personalreduzierungen und sogar die Schließung des gesamten Unternehmens.

Diese Studie unterstreicht, dass Vorbeugung die beste Strategie zur Minimierung der Gefahr eines Ransomware-Angriffs und zur Sicherstellung ist, dass Ihr Unternehmen gar nicht erst Opfer einer Attacke wird.

LIOR DIV
CEO, CYBEREASON

Die Studie zeigt auch, dass die Mehrheit der Unternehmen, die sich in der Vergangenheit für die Zahlung von Ransomware-Forderungen entschieden, nicht vor weiteren Ransomware-Angriffen geschützt waren, die häufig von denselben Angreifern durchgeführt wurden. Darüber hinaus garantiert der Abschluss einer Cyber-Versicherung nicht, dass ein Unternehmen Verluste, die mit einem Ransomware-Angriff in Verbindung gebracht werden, ersetzt bekommt.

Ein wesentlicher Vorteil dieses Berichts ist, dass er Einblicke in die geschäftlichen Auswirkungen von Ransomware-Angriffen in den wichtigsten Branchen bietet und Daten offenlegt, die zur Entwicklung besserer Abwehrmaßnahmen gegen Ransomware genutzt werden können. Diese Studie unterstreicht, dass Vorbeugung die beste Strategie zur Minimierung der Gefahr eines Ransomware-Angriffs und zur Sicherstellung ist, dass Ihr Unternehmen gar nicht erst Opfer einer Attacke wird.

Cybereason hat es sich zur Aufgabe gemacht, neuartige Bedrohungen aufzudecken und verwertbare Informationen bereitzustellen, um Unternehmen besser gegen schädigende Ransomware-Angriffe zu schützen. Gemeinsam können wir den gegnerischen Vorteil umkehren und uns – den Verteidigern – das Feld zurück erobern.

WESENTLICHE GLOBALE ERGEBNISSE

Die Gefahr ist Realität

81%
sind bezüglich der Gefahr eines Ransomware-Angriffs höchst oder sehr besorgt

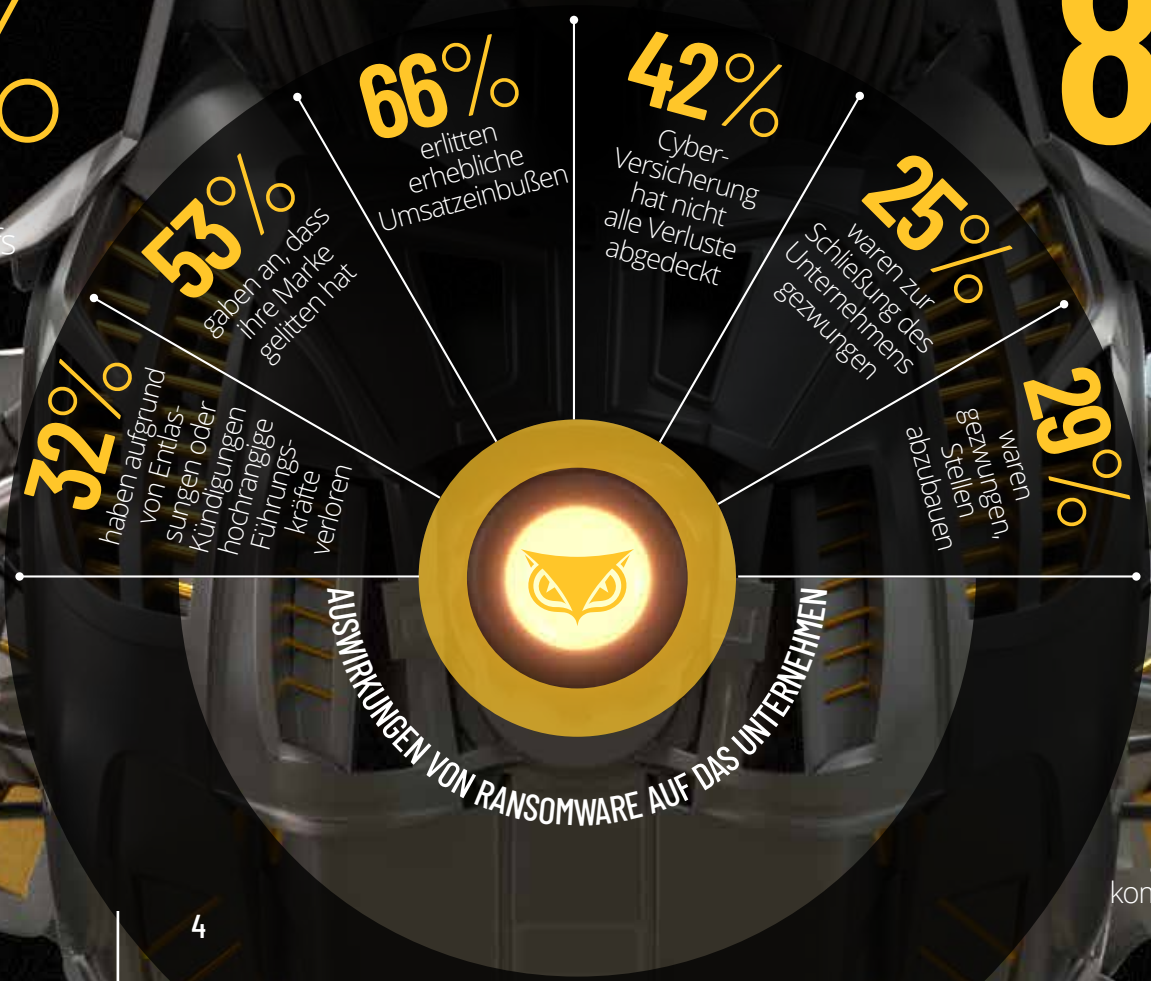
73%
haben einen konkreten Plan oder eine Richtlinie, um einen Ransomware-Angriff effektiv abzuwehren

42%
glauben, dass sie über kompetentes Personal für diese Abwehr verfügen

Bezahlen lohnt sich nicht

80%
derjenigen, die eine Ransomware-Forderung zahlten, erlitten einen weiteren Angriff

46%
erhielten nach einer Zahlung wieder Zugang zu ihren Daten, diese allerdings teilweise oder komplett beschädigt waren



RANSOMWARE

KAPITEL 1

AUSWIRKUNGEN VON RANSOMWARE AUF DAS UNTERNEHMEN

Ransomware-Angriffe können sich auf vielfältige Weise negativ auf ein Unternehmen auswirken, die möglichen Gesamtverluste können zehn bis sogar Hunderte Millionen US-Dollar umfassen. Kurzfristige Auswirkungen können unter anderem sein: Störungen entscheidender Geschäftsabläufe wegen unmöglichem Datenzugriff, Kosten für die Angriffsabwehr und Maßnahmen zur Schadensbegrenzung, Unterbrechung von Systemprozessen, Produktivitätsverluste sowie die Zahlung der Ransomware-Forderung selbst, wenn das Unternehmen sich dazu entscheidet, der Lösegeldforderung nachzugeben.

Zu den längerfristigen Auswirkungen zählen Ertragseinbußen, Schädigung der Marke, Verlust von wichtigen Führungskräften und Personalentlassungen, Verlust von Kunden und strategischen Partnern und – unter bestimmten Umständen – sogar eine Existenzbedrohung des gesamten Unternehmens.

Von den 1.263 Teilnehmern an der Umfrage erlitten

66%

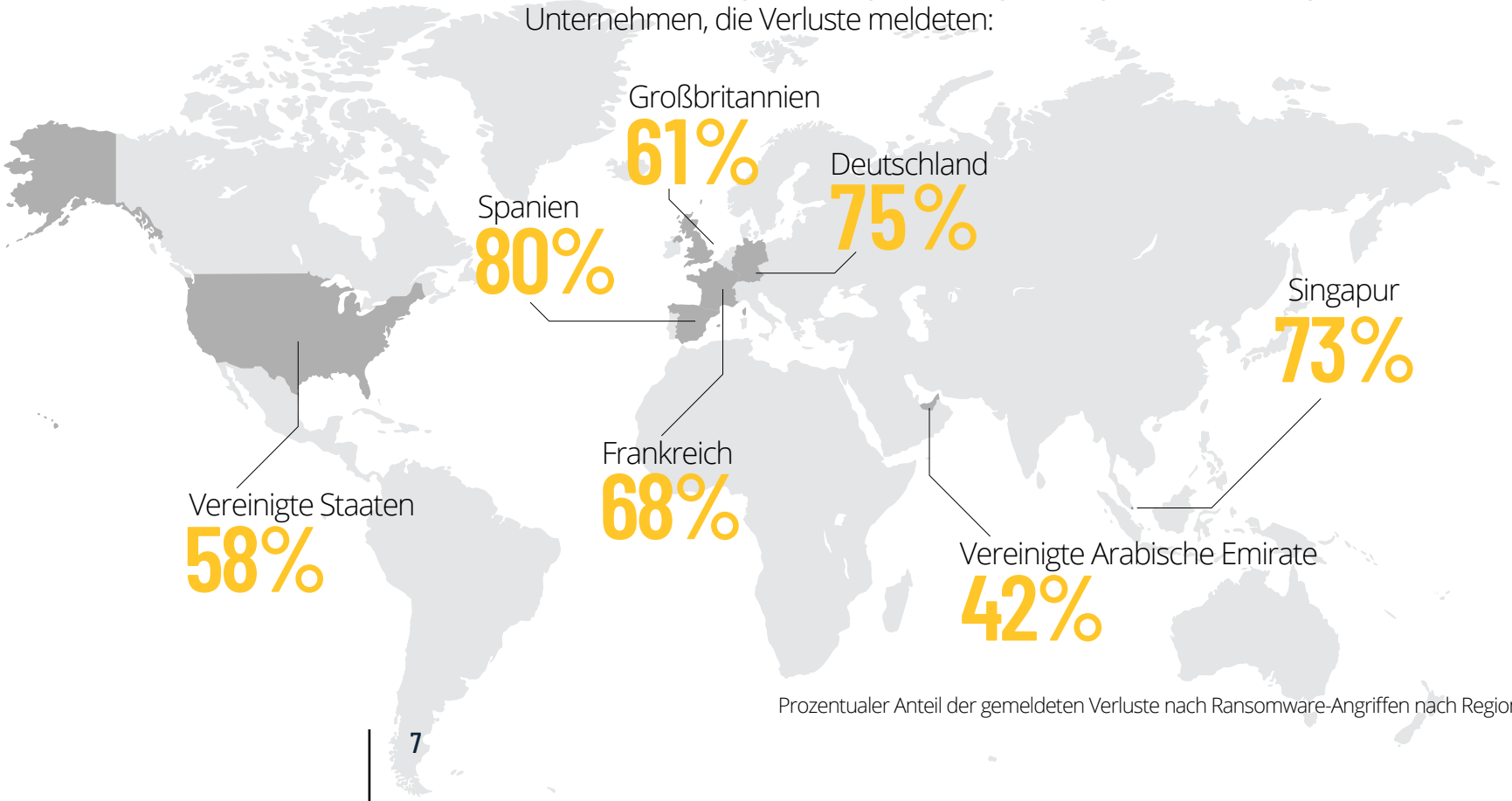
erhebliche Ertragsein-bußen

ERTRAGSVERLUSTE

FedEx meldete Verluste von rund 300 Millionen US-Dollar infolge der NotPetya-Ransomware-Angriffe im Jahr 2017, die Stadt Atlanta zahlte Berichten zufolge mehr als 2,6 Millionen US-Dollar, um sich aus einem SamSam-Ransomware-Angriff im Jahr 2018 zu retten. Die Stadt Baltimore hat Berichten zufolge mehr als 18 Millionen US-Dollar investieren müssen, um ihr gesamtes IT-Netzwerk neu aufzubauen, nachdem sie bei einem weiteren SamSam-Ransomware-Angriff die Zahlung verweigert hatte. Cognizant Technology Solutions meldete einen verringerten Gewinn im Jahr 2020, unter anderem wegen der Auswirkungen eines Maze-Ransomware-Angriffs.

ERTRAGSVERLUSTE NACH REGIONEN

Von den 1.263 Teilnehmern der Umfrage gaben zwei Drittel (66%) an, dass ihr Unternehmen durch einen Ransomware-Angriff erhebliche Gewinneinbußen erlitten hat. Den Umfrageergebnissen zufolge scheint die Unternehmensgröße nur einen geringen Einfluss auf den Ertragsverlust zu haben. Das folgende Diagramm zeigt die regionale Verteilung der Unternehmen, die Verluste meldeten:



Prozentualer Anteil der gemeldeten Verluste nach Ransomware-Angriffen nach Region

UNTERNEHMEN, DIE VERLUSTE MELDETEN, NACH BRANCHE:

75%
Regierung

Finanzdienstleistungen
73%

Einzelhandel
74%

Gesundheitswesen
64%

Technologie
64%

Automobilindustrie
58%

Diese Ergebnisse unterstreichen die Tatsache, dass jede Branche nach einem erfolgreichen Ransomware-Angriff mit einer statistisch signifikant hohen Wahrscheinlichkeit Ertragsverlusten ausgesetzt ist, unter anderem bedingt durch Unterbrechungen von Geschäftsprozessen, Systemausfallzeiten, Abzug von Ressourcen und Arbeitskräften für die Wiederherstellung und Markenbeschädigung.

Produktion
51%

Justiz
50%

Prozentualer Anteil der gemeldeten Ertragsverluste nach Ransomware-Angriffen nach Region

SCHADEN FÜR MARKE UND ANSEHEN

Kein Unternehmen möchte das nächste TJ Maxx, Target, Equifax oder Microsoft sein – nach der kürzlich passierten, umfassenden Gefährdung ihres Exchange-Server-Angebots. Aber diese berühmt-berüchtigten Angriffe verblassen im Vergleich zu SolarWinds, wo die Marke selbst zum Synonym für den Angriff auf das Unternehmen geworden ist.

Ransomware-Angriffe können Marken, die mit ihnen in Verbindung gebracht werden, beschädigen – und tun dies auch. Der britische National Health Service (NHS) beispielsweise leidet noch immer unter den massiven WannaCry-Ransomware-Angriffen im Jahr 2017, die das Unternehmen mehr als 100 Millionen US-Dollar an Gesamtverlusten kostete und zu mehr als 19.000 abgesagten Terminen führte. Die Vielzahl der Servicestörungen hatte zweifellos einen negativen Einfluss darauf, wie NHS-Kunden die Zuverlässigkeit ihres Gesundheitsdienstleisters bewerten.

In der Studie gaben mehr als die Hälfte (53%) der Teilnehmer an, dass die Marke ihres Unternehmens durch einen Ransomware-Angriff gelitten hat. Singapur (40%), Spanien (44%) und Frankreich (49%) meldeten die niedrigste Anzahl an Unternehmen, die nach einem Ransomware-Angriff einen Imageschaden erlitten haben. Mehr als die Hälfte der Befragten in Deutschland (51%), den V.A.E. (54%), den USA (56%) und Großbritannien (63%) berichteten, dass die Marke ihres Unternehmens Schaden genommen hatte.

Unternehmen denken, dass sie auf die Auswirkungen eines Ransomware-Angriffs umfassend vorbereitet sind, wenn sie eine Cyber-Versicherung abgeschlossen haben, Datensicherungen durchführen und in der Lage sind, die Datenwiederherstellung in kurzer Zeit durchzuführen. Realität ist jedoch: Egal, wie gut ein Unternehmen auf einen Ransomware-Angriff vorbereitet ist – die Marke wird dem Risiko eines erheblichen Schadens ausgesetzt, unabhängig von allen anderen Faktoren.

RANSOMWAREANGRIFFE SIND DARÜBER HINAUS EIN RISIKO FÜR DIE FÜHRUNGSSPITZE.

RÜCKTRITTE UND KÜNDIGUNGEN DER FÜHRUNGSSPITZE

Der Verantwortliche für die zentrale IT-Sicherheit (CISO) ist ein ständiges Opfer von Sicherheitsvorfällen. Die durchschnittliche Unternehmenszugehörigkeit eines CISO ist im Laufe der letzten Jahre kontinuierlich gesunken und liegt derzeit bei etwa 18 bis 26 Monaten. Trotz des großen C am Anfang des Titels besetzen die meisten CISO keine der üblichen Spitzenpositionen in ihren Unternehmen.

Bedeutet dies, dass die Führungsspitze nach einem großen Sicherheitsereignis immun ist gegenüber Konsequenzen? Ganz und gar nicht. Die CEO von Target, Home Depot, Sony und TalkTalk wurden nach großen Sicherheitsverletzungen entweder entlassen, traten zurück oder schieden aus dem Unternehmen aus.

Ransomware-Angriffe stellen auch ein Risiko für die Führungsspitze dar, wie sich im Jahr 2020 zeigte. Der CEO und Präsident von ERT, Jim Corrigan, wurde nach einem Ransomware-Angriff, der die COVID-19-Impfstoffstudien des Unternehmens verzögerte, vermutlich zum Rücktritt gedrängt. In diesem Punkt gab fast ein Drittel der Teilnehmer unserer Umfrage (32%) an, dass sie nach einem Ransomware-Angriff ihre Führungsspitze entweder durch Entlassung oder Rücktritt verloren haben.

Die richtigen Präventions-, Identifzierungs- und Reaktionskompetenzen, die sicherstellen, dass ein versuchter Ransomware-Angriff abgewehrt wird, haben demnach unmittelbaren Einfluss auf die Amtszeiten der Führungsspitze. Die Umfrageergebnisse machen deutlich, dass ein größerer Sicherheitsfall in Form eines erfolgreichen Ransomware-Angriffs zu einer Diskussion in der Vorstandsetage führt, da die Auswirkungen auf die betroffenen Unternehmen erheblich sind.

MITARBEITER- UND PERSONALABBAU

Nicht nur die Führungsspitze ist durch Ransomware gefährdet, auch Mitarbeiter können zu Opfern werden, wenn Unternehmen nach einem Angriff versuchen, die Stabilität wiederherzustellen. Im Jahr 2020 kündigte der Stahlproduzent Evraz nach einem Ransomware-Angriff, der den nordamerikanischen Geschäftsbetrieb des Unternehmens zerstörte, umfangreiche Entlassungen in der Produktion und im Rohrleitungsbau an.

Die neueste Studie belegt diese traurige Folge von Ransomware-Angriffen: Knapp ein Drittel (29%) der Befragten gab an, dass ihr Unternehmen nach einer Ransomware-Attacke dazu gezwungen war, Arbeitsplätze abzubauen. Teilnehmer in Singapur (13%), Deutschland (19%) und den V.A.E. (29%) gaben an, im oder unter dem Durchschnittswert zu liegen, während Großbritannien (31%), Spanien (31%) und die USA (33%) leicht über dem Durchschnittswert liegen. Frankreich als negativer Ausnahmefall meldete, dass 39% der Unternehmen nach einem Ransomware-Angriff gezwungen waren, Arbeitsplätze zu streichen.

Im Branchenüberblick meldeten Teilnehmer im Regierungssektor keine Arbeitsplatzverluste, während in der Automobilindustrie, im Einzelhandel und im Justizbereich deutlich mehr Arbeitsplatzverluste nach einem Ransomware-Angriff verzeichnet wurden. Daraus lässt sich ableiten, dass der öffentliche Sektor bis zu einem gewissen Grad vor Personalauswirkungen eines Ransomware-Angriffs geschützt ist, während für den privaten Sektor nach einem erfolgreichen Ransomware-Angriff das Risiko von Personalabbau besteht – unabhängig der Branche:

NACH BRANCHE	PROZENTUALER ANTEIL DER ENTLASSUNGEN
Justiz	50%
Einzelhandel	48%
Automobilindustrie	42%
Produktion	29%
Technologie	29%
Gesundheitswesen	24%
Finanzdienstleistungen	23%
Regierung	0%

Prozentualer Anteil der gemeldeten Entlassungen nach Ransomware-Angriffen nach Region

PROZENTSATZ DER GESCHÄFTSAUFGABEN

ZUR GESCHÄFTSAUFGABE GEZWUNGEN

Schließlich kommen wir zur endgültigen Konsequenz, die ein Unternehmen durch Ransomware-Angreifer erleiden kann: seine Auflösung. Die Telemarketing-Firma The Heritage Company teilte 300 Beschäftigten mit, dass sie nach einem Ransomware-Angriff den Betrieb einstelle und sich die Belegschaft eine neue Anstellung suchen solle, da die Produktionsserver infolge des Angriffs für lange Zeit nicht liefen. Die Ankündigung kam nur wenige Tage vor den Weihnachtsferien.

Der komplette Verlust eines Unternehmens aufgrund eines Ransomware-Angriffs mag wie der ultimative Ausnahmefall erscheinen, ist aber eine weitaus realere Gefahr, als die meisten Führungskräfte annehmen. Mehr als ein Viertel der befragten Teilnehmer (25%) gab an, dass ein Ransomware-Angriff die Aufgabe ihres Unternehmens erzwungen hat. Die folgende Grafik zeigt die Aufteilung nach Regionen:

REGION	PROZENTSATZ DER GESCHÄFTSAUFGABEN
Vereinigte Arabische Emirate	42%
Großbritannien	34%
Vereinigte Staaten	31%
Frankreich	22%
Deutschland	21%
Singapur	20%
Spanien	5%

DIE ERGEBNISSE ZEIGEN DEUTLICH, DASS KEINE BRANCHE VOR MÖGLICHERWEISE KATASTROPHALEN FOLGEN NACH EINEM ERFOLGREICHEN RANSOMWARE-ANGRIFF GESCHÜTZT IST.

Bei der Auswertung der Umfrageergebnisse nach Anzahl der Mitarbeiter waren die Ergebnisse gemischt. Insbesondere Unternehmen mit 250 bis 500 Mitarbeitern traf es mit fast einem Drittel (27%) am schlimmsten, während im Branchenvergleich die Automobilindustrie und der Einzelhandel mit 42 bzw. 33 Prozent am stärksten betroffen waren. Diese Ergebnisse zeigen deutlich, dass kein Unternehmen vor möglicherweise katastrophalen Folgen aufgrund eines erfolgreichen Ransomware-Angriffs geschützt ist.

DECKT DIE CYBER-VERSICHERUNG DIE KOSTEN?

Laut einer weiteren Studie, die von einem der größten nordamerikanischen Anbieter von Cyber-Versicherungen erhoben wurde, waren Ransomware-Angriffe die Ursache für fast die Hälfte aller Cyber-Versicherungsansprüche (41%), die in den ersten sechs Monaten des Jahres 2020 eingereicht wurden. Aber deckt eine Cyber-Versicherung nicht immer die vielfältigen Kosten ab, die mit einem erfolgreichen Ransomware-Angriff verbunden sind? Die Antwort lautet: nicht unbedingt.

Die Stadt New Orleans wurde Opfer eines erfolgreichen Ransomware-Angriffs, der Berichten zufolge zu einem geschätzten Schaden von über 7 Millionen US-Dollar führte. Trotz der Tatsache, dass ihre Versicherungspolice Verluste infolge von Ransomware-Angriffen abdeckt, konnte die Stadt letztlich nur etwa 3 Millionen US-Dollar der Verluste bei ihrem Versicherer geltend machen.

Dieses Szenario wurde auch von unseren Studienergebnissen bestätigt: 54% der Befragten gaben an, dass ihr Unternehmen in den letzten 24 Monaten eine Cyber-Versicherungspolice abgeschlossen hat, die Ransomware-Folgen abdeckt. 21% der Befragten gaben an, dass ihr Unternehmen zwar eine Cyber-Versicherungspolice abgeschlossen hat, diese aber nicht die durch Ransomware-Angriffe entstandenen Verluste abdeckt.

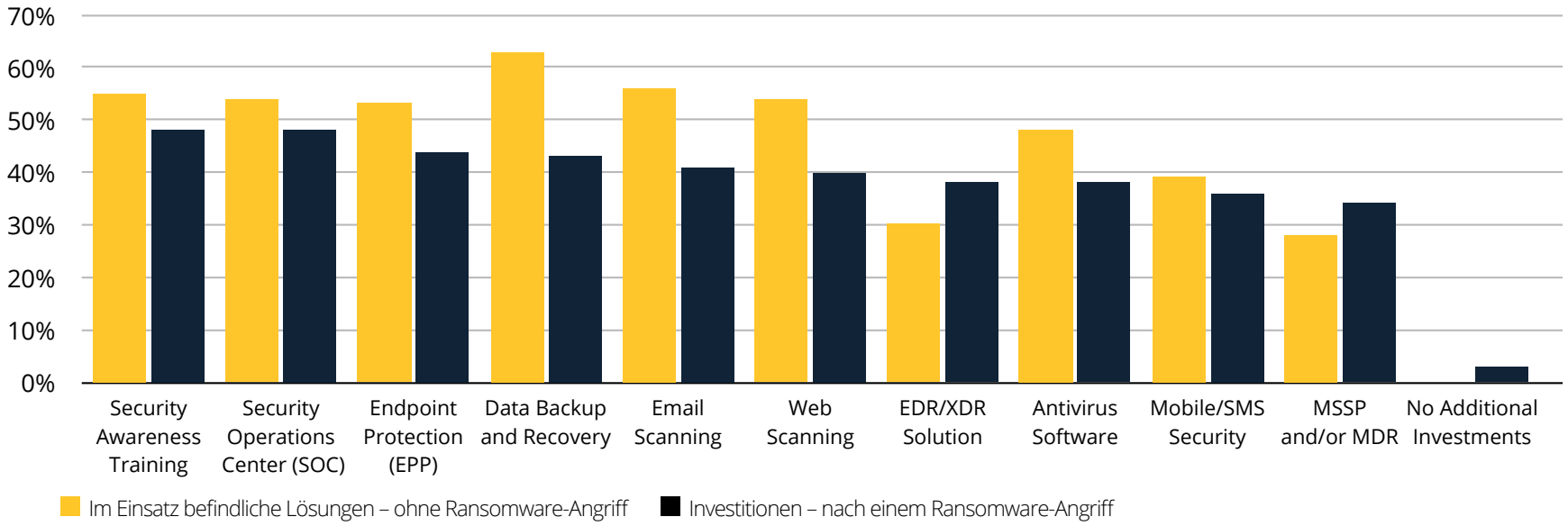
Von den Unternehmen, die eine Cyber-Versicherung abgeschlossen hatten und von einem Ransomware-Angriff betroffen waren, gab ein Großteil (42%) an, dass ihr Versicherer nur einen Teil der Verluste erstattet hat. Diese Ergebnisse lassen darauf schließen, dass diejenigen, die keine entsprechende Versicherung haben, mit schwerwiegenden Folgen für ihr Unternehmen rechnen müssen. Bei Unternehmen mit umfassenderem Versicherungsschutz besteht dennoch das Risiko erheblicher Folgeschäden. Zusammenfassend lässt sich sagen: Wenn Sie eine Cyber-Versicherung haben, prüfen Sie bitte gründlich, ob Sie hinreichend abgedeckt sind.

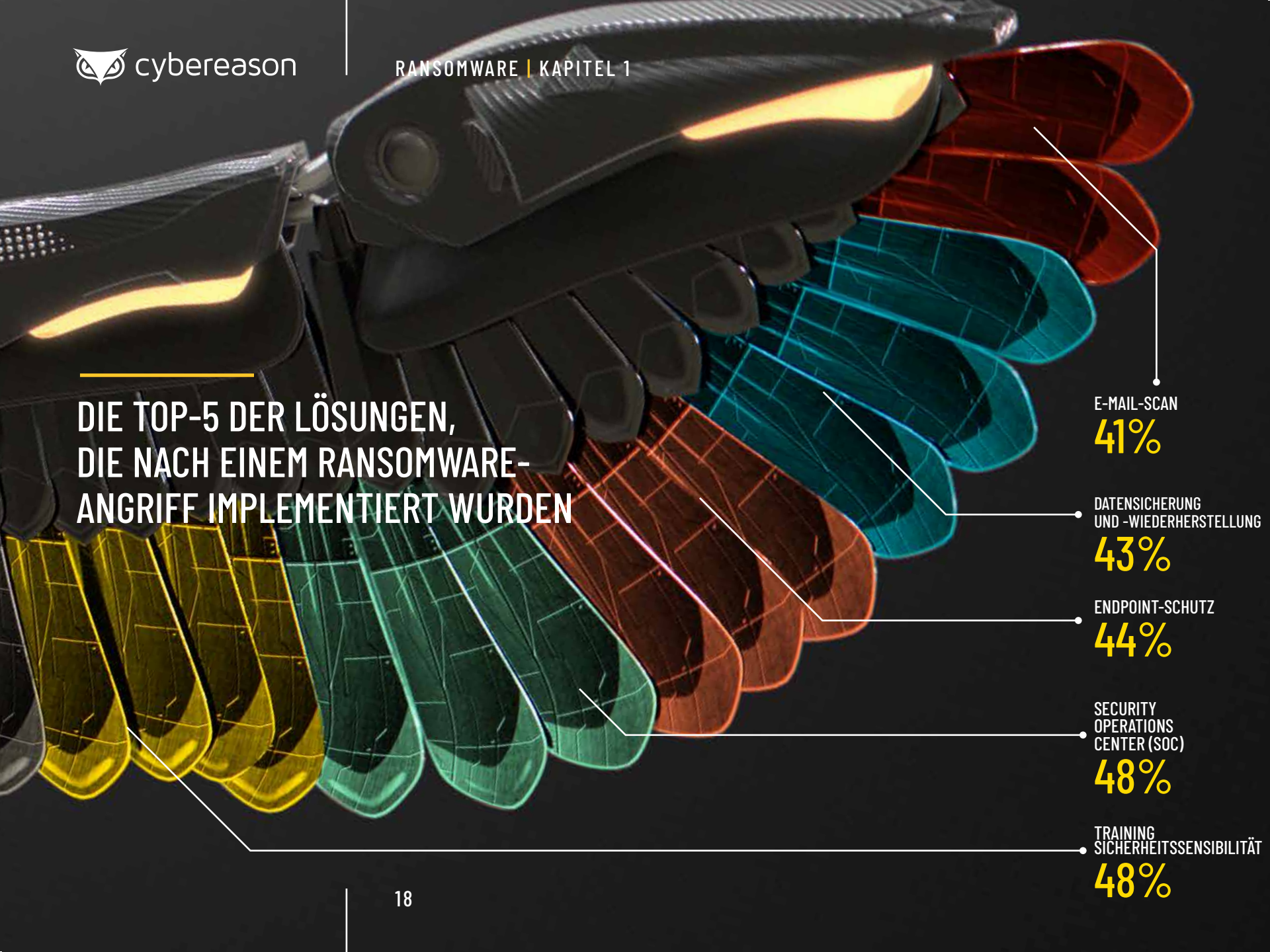
SICHERHEITSINVESTITIONEN NACH RANSOMWARE-ANGRIFFEN

Sicherheit ist seit jeher mit der Frage verbunden, warum die Kompetenz einer Software häufig mit dem Negativbeweis gestellt wird: Wenn keine größeren Sicherheitsvorfälle stattfinden – warum müssen wir dann weiter in einer solchen Größenordnung in Sicherheitslösungen und -abläufe investieren? Leider braucht es oft einen großen Sicherheitsvorfall, um zusätzliche Investitionen in das Sicherheitsprogramm, die Tools und das Personal zu beschleunigen.

Wir haben die Umfrageteilnehmer, die angaben, dass ihr Unternehmen in den letzten 24 Monaten von einem Ransomware-Angriff betroffen war, gebeten uns mitzuteilen, in welche Sicherheitslösungen sie nach dem Angriff investiert haben, um ihre Netzwerke vor zukünftigen Vorfällen zu schützen.

Die folgende Tabelle vergleicht diese Investitionen mit den Lösungen, die bereits in Unternehmen im Einsatz sind, die in den letzten 24 Monaten nicht von einem Ransomware-Angriff betroffen waren. Die Grafik zeigt eine Gegenüberstellung der bestehenden Lösungen, die Unternehmen potentiell vor einem Ransomware-Angriff schützen könnten, und der Investitionen, die Unternehmen nach einem Angriff getätigt haben:





DIE TOP-5 DER LÖSUNGEN, DIE NACH EINEM RANSOMWARE-ANGRIFF IMPLEMENTIERT WURDEN

E-MAIL-SCAN
41%

DATENSICHERUNG UND -WIEDERHERSTELLUNG
43%

ENDPOINT-SCHUTZ
44%

SECURITY OPERATIONS CENTER (SOC)
48%

TRAINING SICHERHEITSSENSIBILITÄT
48%

RANSOMWARE

KAPITEL 2

RANSOMWARE: WER IST BETROFFEN? JEDER

Eine der wichtigsten Erkenntnisse dieser Studie ist so alarmierend wie ermutigend. Auf die Frage „Wie besorgt sind Sie wegen der mit Ransomware verbundenen Risiken?“ antworteten mehr als vier von fünf Befragten (81%), dass sie bezüglich der Gefahr von Ransomware-Angriffen sehr oder höchst besorgt sind. Dieses Ergebnis ist aus zwei Gründen alarmierend. Es zeigt, dass die Bedrohung durch Ransomware allgegenwärtig ist und verdeutlicht die Dringlichkeit, die Ransomware-Krise anzugehen. Wenn Sie heute im Bereich Cybersicherheit arbeiten und nicht mindestens ein bisschen besorgt sind wegen Ransomware, richten Sie nicht genug Aufmerksamkeit auf dieses Thema.

Fast
75%
der Umfrageteil-nehmer gaben an, dass sie einen konkreten Plan oder eine Richtlinie haben, um einen Ransomware-Angriff effektiv abzuwehren.

In der Praxis erkennt die große Mehrheit, wie hoch das Risiko durch Ransomware ist. Allerdings zeigen unsere Daten, dass es eine gewisse Diskrepanz oder ein falsches Sicherheitsgefühl bei der Frage gibt, wie gut Unternehmen auf die Abwehr von Ransomware-Angriffen vorbereitet sind. Fast 75% der Umfrageteilnehmer gaben an, dass sie über einen spezifischen Plan oder eine Richtlinie verfügen, um einen Ransomware-Angriff effektiv zu bewältigen, und fast 60% glauben, dass sie über das richtige Personal dafür verfügen. Wenn Unternehmen einen Plan und die richtigen Mitarbeiter haben, warum sind die meisten dann noch besorgt?

Interessanterweise war in den USA die Zahl derer, die glauben, dass sie über die richtigen Mitarbeiter verfügen (69%), höher als die Zahl derer, die angaben, einen Plan oder eine Strategie zu haben (58%). Dies deutet darauf hin, dass einige Unternehmen in den USA so viel Vertrauen in ihr IT-Sicherheitsteam haben, dass sie glauben, dass dies auch ohne Implementierung von Ablaufprozessen für ihren Schutz ausreicht.

Dabei sind die USA weiterhin die Hauptbelasteten der größten Ransomware-Angriffe, daher sollen Studien wie diese dazu beitragen, die Lücke zu schließen und einen klareren Blick auf die potenziellen Auswirkungen von Ransomware auf Unternehmen zu bekommen. In Ländern wie Großbritannien, Deutschland, Spanien und Frankreich verfügen 73% bis 87% der Unternehmen über einen Plan oder eine Richtlinie, während der Prozentsatz, der angibt, über die richtigen Mitarbeiter zu verfügen, zwischen 45% und 66% liegt – im Gegensatz zu den Ergebnissen aus den USA.

BEI EINEM DOUBLE EXTORTION -ANGRIFF STEHLEN DIE ANGREIFER ZUNÄCHST SENSIBLE DATEN UND GEISTIGES EIGENTUM UND DROHEN ANSCHLIESSEND DAMIT, DIE GESTOHLENEN DATEN OFFENZULEGEN ODER ZU VERKAUFEN, FALLS DIE RANSOMWARE-FORDERUNG NICHT ERFÜLLT WIRD – DAVOR BIETEN DATENSICHERUNGEN KEINEN SCHUTZ.

Obwohl ein Großteil der Unternehmen angibt, dass sie über die nötigen Richtlinien und Mitarbeiter verfügen, um sich gegen Ransomware zu schützen, war das letzte Jahr eine außergewöhnliche Herausforderung. Cyberkriminelle erkannten die Gelegenheit, aus dem Chaos und der Verwirrung Kapital zu schlagen, als Unternehmen auf der ganzen Welt mit der COVID-19-Pandemie zu kämpfen hatten und viele von heute auf morgen auf ein komplett dezentrales Homeoffice-Modell umstellten. Dies stellte IT-Sicherheitsteams vor große Herausforderungen – die Angriffsfläche war größer und die Sichtbarkeit erschwert. Ransomware ermöglicht es Angreifern außerdem, in der Pandemie bequem und sicher Systeme zu kompromittieren und Ransomware-Zahlungen zu erhalten.

Das Gesamtvolumen der Ransomware-Angriffe scheint zu sinken, allerdings sind die laufenden Angriffe raffinierter und haben verheerendere Auswirkungen. Als Reaktion auf die Zunahme von Ransomware-Angriffen verbesserten Unternehmen ihre Backup-Prozesse und -Technologien. Im Falle eines Ransomware-Angriffs könnten sie die Lösegeld-Forderung einfach ignorieren, die Systeme aus dem Backup wiederherstellen und den normalen Betrieb wiederaufnehmen. Cyberkriminelle haben sich jedoch angepasst und so genannte Double-Extortion-Malware-Angriffe entwickelt. Bei einem Double-Extortion-Angriff werden nicht nur Daten verschlüsselt, sondern vorher sensible Daten und geistiges Eigentum herausgefiltert. Die Angreifer drohen dann damit, die gestohlenen Daten zu veröffentlichen oder zu verkaufen, wenn die Ransomware-Forderung nicht erfüllt wird – davor können Datensicherungen nicht schützen.

Gleichzeitig sind Ransomware-Forderungen sprunghaft angestiegen. Die durchschnittliche Ransomware-Forderung im Jahr 2018 lag Berichten zufolge bei 6.000 US-Dollar. Diese Zahl erhöhte sich 2019 um das 14-fache auf 84.000 US-Dollar und 2020 nochmals um mehr als das Doppelte auf 178.000 US-Dollar. Im Jahr 2021 waren wir Zeugen einer Reihe von Angriffen, die die die bisherigen Ransomware-Forderungen in den Schatten stellen. Colonial Pipeline zum Beispiel hat Berichten zufolge eine Ransomware-Forderung von 5 Millionen US-Dollar an DarkSide gezahlt, und sowohl Acer als auch Apple wurden mit Ransomware-Forderungen in Höhe von 50 Millionen US-Dollar konfrontiert.

Die Zusammenarbeit mit der öffentlichen Hand und der Privatwirtschaft ist ein Schritt zur Schließung der Lücke zwischen der Wahrnehmung, vorbereitet zu sein, und der Besorgnis. Die US-Regierung hat eine Ransomware-Task-Force gebildet, der Cybereason angehört. Sie setzt sich aus Vertretern verschiedener Regierungsbehörden, Unternehmen der öffentlichen Hand und der Privatwirtschaft zusammen, die gemeinsam an der Bewältigung der Ransomware-Krise arbeiten.

DIE BEMÜHUNGEN DER RANSOMWARE TASK-FORCE FALLEN IN DREI HAUPTKATEGORIEN: VORBEREITUNG, UNTERBINDUNG UND REAKTION. RANSOMWARE IST EIN GLOBALES PROBLEM UND BETRIFFT ALLE. DAHER IST ES WICHTIG FÜR UNS, DASS WIR ZUSAMMENARBEITEN, UM RANSOMWARE-ANGRIFFE ABZUWEHREN UND DEN GEGNERISCHEN VORTEIL UMZUKEHREN.

RANSOMWARE

KAPITEL 3

IN DEN MEISTEN FÄLLEN LOHNT ES SICH NICHT, ZU ZAHLEN.

Wenn Unternehmen von einem Ransomware-Angriff betroffen sind, ist für sie eine der wichtigsten Fragen, ob sie die Ransomware-Forderung zahlen sollen. Neben der Zweckmäßigkeit als wichtiger Faktor gibt es viele weitere Aspekte, die zu erwägen sind, und auch definitiv Risiken, die mit einer Entscheidung zur Zahlung verbunden sind.

Sollten Unternehmen einen Spezialisten mit der Aushandlung der Zahlungsbedingungen beauftragen? Werden die Angreifer ihren Teil der Abmachung einhalten und den Zugriff auf alle Daten zurückgeben? Was passiert, wenn die Daten dabei beschädigt werden? Was passiert, wenn sich der Angreifer in einem Land befindet, das Sanktionen unterliegt, sodass eine Zahlung eine strafrechtliche Handlung darstellt? Wird die Zahlung die Angreifer dazu ermutigen, einen weiteren Ransomware-Angriff zu starten? Welche Risiken bestehen für das Unternehmen, wenn die Lösegeld-Forderung nicht gezahlt wird?

Es ist eine schwierige Situation für jedes Unternehmen, und es gibt keine eindeutigen „Best Practices“, die als Beispiel dienen. Jedes Eindringen, jede Angriffsgruppe, jedes vom Angriff betroffene Unternehmen, jeder gefährdete Datensatz und jeder potenziell betroffene Dritte ist individuell verschieden. Bei der Überlegung, ob eine Zahlung geleistet werden soll oder nicht, gilt es zahlreiche Faktoren abzuwägen. Daher müssen die meisten Ransomware-Angriffe von Fall zu Fall neu bewertet werden.

DOUBLE EXTORTION

Bei der Double Extortion (doppelte Erpressung) filtern Angreifer zunächst sensible Daten heraus und drohen damit, diese zu veröffentlichen, wenn die Ransomware-Forderung nicht erfüllt wird. Das bedeutet, dass das Opfer weiter mit der Aussicht konfrontiert ist, die Ransomware-Forderung zahlen zu müssen – unabhängig davon, ob es als Vorsichtsmaßnahme Daten gesichert hat oder nicht.

In jüngster Zeit haben einige Ransomware-Angreifer neuartige Double-Extortion-Ansätze eingesetzt, um die Wahrscheinlichkeit zu erhöhen, dass sie ihre Ransomware-Forderung erhalten. Zum Beispiel wurde erst im April 2021 berichtet, dass die DarkSide-Ransomware-Gruppe zusätzlichen Druck auf ihre Opfer ausübte, indem sie damit drohte, Insider-Informationen, die auf den exfiltrierten Daten basierten, an Aktienhändler weiterzugeben. Diese hätten damit Short-Positionen gegen börsennotierte Unternehmen eingehen können, sollte das angegriffene Unternehmen sich weigern, die Ransomware-Forderung zu erfüllen.

NAHEZU
DIE HÄLFTE DER BEFRAGTEN (46%) GAB AN,
NACH DER ZAHLUNG WIEDER ZUGANG ZU IHREN DATEN ERHALTEN ZU HABEN, JEDOCH WAREN
DIESE ZUM TEIL ODER SOGAR ALLE
BESCHÄDIGT.

WAS PASSIERT, WENN WIR ZAHLEN MÖCHTEN?

Lohnt es sich bei so hohem Risiko, einfach zu zahlen? Von den Umfrageteilnehmern, die angaben, dass ihr Unternehmen nach einem Angriff die geforderte Ransomware-Forderung gezahlt hat, gab fast die Hälfte der Befragten (46%) an, dass sie nach der Zahlung wieder Zugriff auf ihre Daten hatten – einige oder sogar alle Daten aber beschädigt waren.

Andere Unternehmen hatten mehr Glück. Mehr als die Hälfte (51%) gab an, dass sie erfolgreich und ohne Datenverlust wieder Zugriff auf die verschlüsselten Daten erhielten. Nur 3% gaben an, dass sie keinen Zugriff auf die verschlüsselten Daten erhielten.

Macht die Zahlung der Lösegeld-Forderung das Unternehmen anfälliger für nachfolgende Ransomware-Angriffe? Das wird von den Maßnahmen abhängen, die sie ergreifen, um die Schwachstellen zu erkennen und auszumerzen, die den Erfolg des ersten Angriffs ermöglichten.

Ein unbenanntes Unternehmen, das Ziel eines erfolgreichen Ransomware-Angriffs war und eine Ransomware-Forderung in Millionenhöhe zahlte, war offenbar nur zwei Wochen später Opfer eines zweiten Ransomware-Angriffs von denselben Angreifern. Das Unternehmen hatte nicht die notwendigen Schritte unternommen, um zu verstehen, wie es zum ersten Angriff kam, und keine zusätzliche Maßnahmen implementierte, um sicherzustellen, dass die Angriffsmechanik ausgehebelt werden konnte.

Die Studie ergab, dass von den Unternehmen, die sich für die Zahlung einer Ransomware-Forderung entschieden, 80% einen weiteren Angriff erlitten. Von denjenigen, die erneut angegriffen wurden, gab fast die Hälfte (46%) an, dass es sich um dieselben Angreifer handelte, während nur 34% angaben, dass der zweite Angriff von anderen Cyberkriminellen verübt wurde.

ABWEHR VON RANSOMWARE

Hat ein Unternehmen erst einmal einen Ransomware-Angriff erlitten, gibt es nicht mehr viele Optionen. Wenn die Lösegeld-Forderung nicht gezahlt wird, kann der Geschäftsbetrieb für Tage – oder gar Wochen – zum Stillstand kommen, während Daten aus Backups und Systeme wiederhergestellt werden. Im Falle eines Double-Extortion-Angriffs bedeutet die Nichtzahlung der Forderung auch das Risiko zu akzeptieren, dass sensible Daten oder geistiges Eigentum öffentlich zugänglich gemacht oder im Dark Web an den Meistbietenden verkauft werden. Auch hier können die finanziellen Folgen des Geschäfts- und Produktivitätsverlusts in Kombination mit den Wiederherstellungskosten oft die Ransomware-Forderung übersteigen.

Die Alternative besteht darin, der Ransomware-Forderung nachzukommen, aber auch das birgt Probleme und Risiken. Wie bereits erwähnt, können viele Unternehmen, die die Ransomware-Forderung zahlen, den Zugriff auf ihre Daten wiedererlangen, müssen aber feststellen, dass einige oder alle Daten beschädigt wurden. Das von Ransomware-Angreifern zur Verfügung gestellte Entschlüsselungs-Tool ist oft fehlerhaft oder langsam, sodass Unternehmen gezwungen sind, Systeme mit ihren eigenen Backups wiederherzustellen, auch wenn sie der Ransomware-Forderung nachgekommen sind. Ferner gibt es keinerlei Garantie dafür, dass die Daten nicht doch noch online verkauft werden, nachdem die Ransomware-Forderung bezahlt wurde.

3 TIPPS ZUR ABWEHR

1 **Nutzen Sie die Best Practices zur „Security Hygiene“:** Rechtzeitiges Patch-Management, Offsite-Datensicherung und Mitarbeiter-Sicherheitstraining

2 **Einsatz von Multi-Layer-Präventions-Kapazitäten** auf allen Unternehmensendpunkten im gesamten Netzwerk

3 **Implementierung von erweiterten Erkennungs- und Reaktionslösungen** in der gesamten Umgebung für Transparenz, um fortgeschrittene Ransomware-Angriffe zu beenden, bevor sie ins Netzwerk eindringen können

Die einzige gute Option besteht darin, zu vermeiden, überhaupt mit Ransomware infiziert zu werden. Herkömmliche Cybersecurity-Tools und Endpunktlösungen der nächsten Generation (NGAV) sind unzureichend, da sie auf der Erkennung von zuvor identifizierten Attacken und Angriffsindikatoren beruhen.

Unternehmen benötigen Cybersicherheit mit umfassender Sichtbarkeit in der gesamten Umgebung und der Fähigkeit, neben den Indikatoren für einen Angriff auch Verhaltensindikatoren zu analysieren. Die Verhaltensindikatoren liefern Hinweise darauf, was gerade im gesamten System passiert oder was bald passieren könnte, im Gegensatz zu den Angriffsindikatoren, die sich auf die Reaktion auf einen bereits stattgefundenen Angriff konzentrieren.

Es ist wichtig, den gesamten schädigenden Vorfall – die so genannte Malop (malicious operation) – zu betrachten, um das Ausmaß des Angriffs zu verstehen und den Zusammenhang zwischen Aktionen und Verhaltensweisen, die für sich betrachtet harmlos erscheinen mögen, zu erkennen. Die Analyse der Malop bietet ein umfassenderes Verständnis darüber, was gerade passiert, und bietet die nötige Transparenz, den Kontext und die Informationen, um Ransomware-Angriffe zu erkennen und zu verhindern, bevor ein Schaden entsteht.

Fazit und Erkenntnisse

Die Lehre, die man aus dieser Studie ziehen kann, ist recht einfach: Die Auswirkungen eines erfolgreichen Ransomware-Angriffs auf den Umsatz und die Marke eines Unternehmens sind beträchtlich unabhängig von Region, Branche oder Unternehmensgröße. Ransomware-Angriffe können weitreichende Auswirkungen haben, die ein Unternehmen in seinen Grundfesten erschüttern können. Die häufigen Folgen sind Rufschädigung, Verlust von Arbeitsplätzen, Umsatzeinbußen und im schlimmsten Fall sogar der Verlust des gesamten Unternehmens.

Ein gutes Risikomanagement erfordert zwar, dass Unternehmen über Notfallpläne für den Umgang mit den Folgen eines Ransomware-Angriffs auf allen Ebenen verfügen. Die umsichtigste Strategie zur Vermeidung erheblicher Verluste für ein Unternehmen basiert jedoch immer auf Prävention. Trotz zuverlässiger Präventionsfunktionen, die die meisten Ransomware-Angriffe abwehren können, werden doch einige Angriffe unvermeidbar die Präventionsabwehr durchbrechen. Unternehmen müssen daher auch in umfassende Erkennungs- und Reaktionsfunktionen investieren.

Datensicherungslösungen sind ebenfalls sehr zu empfehlen, da sie die Wiederherstellungsversuche erleichtern können. Unternehmen müssen jedoch bedenken, dass Angreifer über Strategien verfügen, die Backups unter bestimmten Umständen nahezu unmöglich machen. Auch die Wahl der richtigen Schutzhöhe einer Cyber-Versicherung ist entscheidend: sie kann die Erstattung aller Verluste im Zusammenhang mit einem Ransomware-Angriff, der Erstattung nur eines Teils der Kosten oder überhaupt keine Erstattung bedeuten.

Unternehmen müssen sicherstellen, dass sie über das geeignete Personal mit den notwendigen Kompetenzen und die richtigen Sicherheitslösungen verfügen. Sie müssen gewährleisten, dass Ransomware-Angriffe mittels effektiver Sicherheitskontrollen entweder vollständig abgewehrt oder zumindest zum frühstmöglichen Zeitpunkt erkannt und verhindert werden, bevor der Angriff so weit eskalieren kann, dass dem Unternehmen beträchtlicher Schaden zugefügt wird.

UMFRAGEMETHODIK

Die Umfrage wurde im April 2021 von Censuswide im Auftrag von Cybereason durchgeführt. 1.263 Cybersecurity-Experten nahmen an der Umfrage teil – mit Teilnehmern aus den USA (24%), Großbritannien (24%), Spanien (12%), Deutschland (12%), Frankreich (12%), den Vereinigten Arabischen Emiraten (8%) und Singapur (8%). Die Umfrage bietet einen differenzierten Überblick, wie lange die Teilnehmer bereits in ihrem Unternehmen arbeiten und wie lange sie in ihrer aktuellen Position tätig sind.

Die Stichprobe der Umfrage umfasst Antworten aus einer Vielzahl von Branchen. Die Technologiebranche ist in der Umfrage mit 44% am stärksten vertreten, gefolgt von der Fertigungsindustrie (16%) und dem Finanzsektor (11%). Die restlichen Umfrageteilnehmer kamen aus dem Gesundheitswesen, der Automobilindustrie, dem Regierungssektor, der Justiz oder anderen Branchen.

Es sind Unternehmen unterschiedlicher Größen vertreten. Die größte Gruppe umfasst 500 oder mehr Mitarbeiter (30%), wir erhielten jedoch auch Rückmeldungen von Unternehmen mit 250 bis 500 Mitarbeitern (23%), 100 bis 249 Mitarbeitern (25%), 50 bis 99 Mitarbeitern (11%),10 bis 49 Mitarbeitern (10%) und weniger als 10 Mitarbeitern (1%).

ÜBER CYBEREASON

Cybereason ist der Branchenführer in modernster Cyber-Sicherheit. Unsere innovativen Abwehrmechanismen bieten zukunftsorienterten Schutz vor Angriffen für alle Endpunkte Ihres Unternehmens und darüber hinaus – überall dort, wo Bedrohungen stattfinden können. Die Cybereason Defense Platform kombiniert die branchenweit besten Erkennungs- und Abwehrmaßnahmen (EDR und XDR), Virenschutz der nächsten Generation (NGAV) und proaktive Bedrohungssuche, um eine kontextbezogene Analyse der Malops (malicious operation) zu ermöglichen. So können Verteidiger Cyberangriffe von Endgeräten aus und von überall beenden. Cybereason ist ein privates, internationales Unternehmen mit Hauptsitz in Boston, London und München sowie Kunden in mehr als 45 Ländern.

Erfahren Sie mehr unter **www.cybereason.com/de**