COHESITY

Bericht zum Stand von Datensicherheit und -management 2023

Juli 2023

Auf einen Blick

Der zum zweiten Mal jährlich erscheinende State of Data Security and Management Report basiert auf einer Umfrage aus dem Jahr 2023, die von Cohesity, Tenable und BigID in Auftrag gegeben und von Censuswide durchgeführt wurde. Die Teilnehmer waren über 3.400 IT- und Security Operations (SecOps)-Entscheidungsträger (die Anzahl der Befragten in beiden Gruppen war etwa gleich groß). Im Rahmen der Umfrage wurden im April 2023 Unternehmen und Organisationen in Australien, Frankreich, Deutschland, Japan, Neuseeland, Großbritannien und den USA befragt.[1]

In einer Zeit, in der Cyberangriffe immer aggressiver und häufiger werden, waren drei Ergebnisse besonders auffällig:

- **Die meisten Unternehmen verfügen nicht über die notwendigen Cyber-Resilienz-Strategien oder Datensicherheitsfunktionen, um Bedrohungen zu bekämpfen und die Geschäftskontinuität aufrechtzuerhalten.**
- **Im Vergleich zu 2022 sind weniger Befragte zuversichtlich, dass ihre Organisation ihre Daten nach einem Angriff schnell wiederherstellen kann.**
- **Es wird immer schwieriger, eine Cyberversicherung abzuschließen.**

Zunehmende Cyberangriffe geben Anlass zu anhaltender Sorge in Bezug auf Ransomware

Als wir 2022 den ersten State of Data Security and Management Report veröffentlichten, standen Ransomware-Bedrohungen ganz oben auf der Liste. Tatsächlich gaben 74 % der Umfrageteilnehmer an, das Gefühl zu haben, dass die Bedrohung durch Ransomware-Angriffe in ihrer Branche im letzten Jahr zugenommen habe.

Wir haben den diesjährigen Umfrageteilnehmern die gleiche Frage gestellt und der Prozentsatz ist deutlich gestiegen. Ganze 93 % der Befragten gaben an, dass die Bedrohung durch Ransomware-Angriffe in diesem Jahr im Vergleich zum Vorjahreszeitraum zugenommen habe.

Und es sind nicht nur Bedrohungen, die Anlass zur Sorge geben. Es sind die tatsächlich erfolgten Angriffe. Zwei Jahre in Folge gab fast die Hälfte der Befragten an, dass ihr Unternehmen in den letzten sechs Monaten Opfer eines Ransomware-Angriffs geworden sei.

1. Censuswide befolgt die Vorgaben der Market Research Society und beschäftigt Mitglieder der Organisation, die sich auf die ESOMAR-Grundsätze stützt.

Wenn Sie sich fragen, ob Ransomware und andere Cyberangriffe immer noch eine echte Bedrohung für Ihr Unternehmen und die weltweite Wirtschaft darstellen, lautet die Antwort dieser globalen Umfrage eindeutig „Ja“.

Gaben an, das Gefühl zu haben, dass die Bedrohung durch Ransomware-Angriffe für ihre Branche im Jahr 2023 zugenommen habe.

Gaben an, Ihre Organisation sei in den vergangenen sechs Monaten Opfer eines Ransomware-Angriffs geworden.

Problem 1

Den meisten Unternehmen fehlen solide Cyber-Resilienz-Strategien oder Datensicherheitsfunktionen, um Bedrohungen zu bekämpfen und die Geschäftskontinuität aufrechtzuerhalten.

Trotz der Bedrohungszunahme und des hohen Prozentsatzes an Befragten, deren Unternehmen kürzlich Angriffen ausgesetzt waren, gab es keinen entsprechenden Anstieg der strategischen Maßnahmen zur Stärkung der Cyber-Resilienz. Tatsächlich sind fast vier von fünf Umfrageteilnehmern nicht vollständig davon überzeugt, dass ihr Unternehmen über eine Cyber-Resilienz-Strategie verfügt, die darauf ausgelegt ist, den zunehmenden Cyber-Herausforderungen und -Bedrohungen von heute zu begegnen.

Und es ist nicht nur eine Frage der Überzeugung. Unternehmen benötigen außerdem Cyber-Resilienz- und Datensicherheitsfunktionen, um ihre Daten und den Geschäftsbetrieb wiederherstellen zu können, und zwar so schnell wie möglich.

Das NIST Cyber Security Framework wird von Organisationen häufig als Referenzrahmen für Cybersicherheit und Cyber-Wiederherstellung angeführt. Durch seine Funktionen zum Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen vereinfacht das Framework die Priorisierung von Investitionen, basierend auf Risiken und Betriebsprioritäten. Und die Ausrichtung auf Standards bietet mehrere Vorteile: Die Frameworks geben Anleitung zur Bereitstellung geeigneter Kontrollen und Prozesse und bieten Unternehmen einen gemeinsamen Bezugspunkt, um Sicherheit, IT und Geschäft aufeinander abzustimmen.

80 % äußerten Bedenken hinsichtlich der Cyber-Resilienz-Strategie ihres Unternehmens und dessen Fähigkeit, die heutigen Cyber-Herausforderungen und -Bedrohungen zu bewältigen.

(Zu Beginn der Umfrage wurde den Befragten diese NIST-Definition von Cyber-Resilienz vorgelegt.)

„Cyber-Resilienz beginnt damit, die richtigen Grundlagen zu schaffen, insbesondere im Hinblick auf Ihre Daten. Es gilt zu verstehen, wo Ihre sensiblen Daten gespeichert sind, was sie beinhalten, wer Zugriff darauf hat und welche Risiken damit verbunden sind. Als Sicherheitsgemeinschaft müssen wir Daten in den Mittelpunkt unserer Sicherheitsstrategie stellen.“

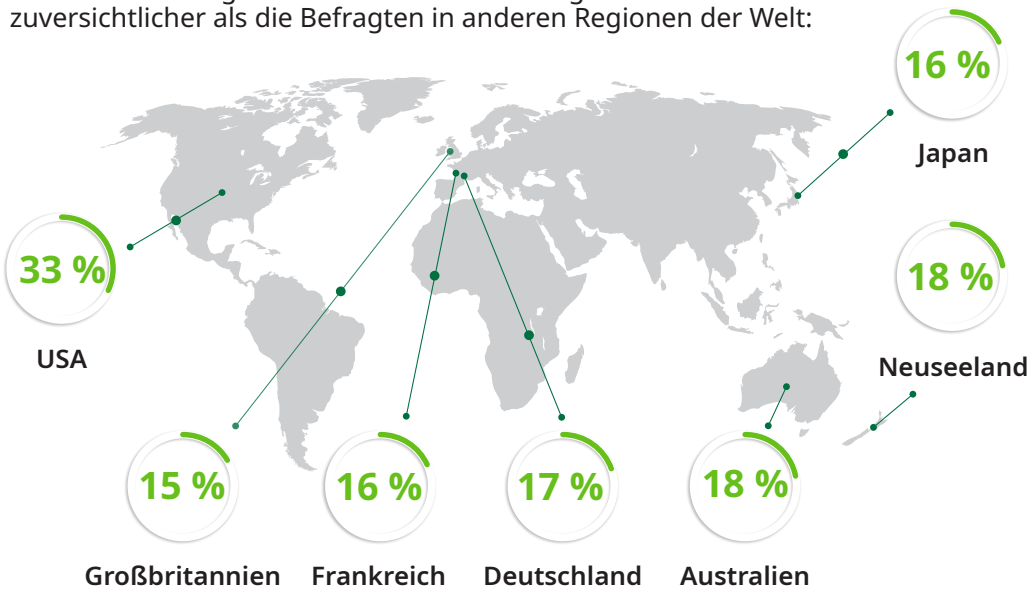
TYLER YOUNG, CHIEF INFORMATION SECURITY OFFICE, BIGID

Problem 2

Die Befragten befürchten, dass in ihren Organisationen Wiederherstellungen nach Angriffen nicht möglich seien.

Auf die Frage nach der Bedrohung durch Ransomware gaben im letzten Jahr 40 % der Befragten an, dass ihnen „Fehler bei der Datenwiederherstellung“ Sorgen bereiteten – selbst wenn ihre Daten gesichert waren. In diesem Jahr sind 67 % nicht vollständig davon überzeugt, dass ihr Unternehmen im Falle eines systemweiten Cyberangriffs Daten und kritische Geschäftsprozesse wiederherstellen kann.

Von dem kleinen Prozentsatz weltweit (21 %), der antwortete, er sei „absolut zuversichtlich“, dass ihre Unternehmensdaten nach einem Cyberangriff ohne das Risiko einer erneuten Infektion mit Malware wiederhergestellt werden können, waren die Umfrageteilnehmer in den Vereinigten Staaten weitaus zuversichtlicher als die Befragten in anderen Regionen der Welt:



Welche Hürden erschweren die Wiederaufnahme der Geschäftstätigkeit? Zu den drei größten Herausforderungen gehören laut der Umfrage:

34 % Mangelnde Integration von IT- und Sicherheitssystemen

Mangelnde Koordination zwischen IT- und Sicherheitsexperten **33 %**

32 % Veraltete Backup- und Recovery-Systeme

… und wenn eine Wiederherstellung möglich ist, erfolgt sie nicht unbedingt schnell.

Eine langsame Wiederherstellung führt zu Unvorhersehbarkeit und schadet dem Unternehmen. Darüber hinaus werfen Verzögerungen zahlreiche Fragen auf.

Wann sind Ihre virtuellen Maschinen, Datenbanken und NAS-Daten wieder online und zugänglich? Werden die Daten sauber sein oder wird erneut Malware eingeschleust, die Ihre Systeme infiziert? Können Sie aufgabenkritische Daten im großen Maßstab zu jedem Zeitpunkt und an jedem Ort wiederherstellen? Wenn ja, wann? Wenn nicht, was passiert dann?

Auf die Frage, wie lange es im Unternehmen im Falle eines Cyberangriffs durchschnittlich dauern würde, Daten und Geschäftsprozesse wiederherzustellen, antworteten:

Es würde über 24 Stunden dauern

Es würde über 4 Tage dauern

Es würde über eine Woche dauern

Und bei einem Ransomware-Angriff zählt jede Minute. Je länger ein Unternehmen ausfällt und seine Daten nicht zugänglich sind, desto größer ist das Risiko schwerwiegender und oft unmittelbarer nachgelagerter Folgen.

„Organisationen können es sich nicht leisten, offline zu sein und ihren Betrieb zu unterbrechen, insbesondere nicht länger als einen Tag. Die bittere Realität ist jedoch, dass viele Unternehmen anfällig für Cyber-Attacken sind, weil sie nicht in der Lage sind, ihre Daten und Geschäftsprozesse bei Bedarf schnell wiederherzustellen.“

BRIAN SPANSWICK, CHIEF INFORMATION SECURITY OFFICER UND HEAD OF IT, COHESITY

Da 95 % der Befragten ihre Daten und Geschäftsprozesse nicht innerhalb von 24 Stunden wiederherstellen können, sind Unternehmen nicht nur anfällig. Sie sind auch eher bereit, Entscheidungen zu treffen, die Anreize für künftige Branchenangriffe bieten können. Entscheidungen, die Lösegeldzahlungen einschließen.

Die meisten würden erwägen, ein Lösegeld zu zahlen

Obwohl die Zahlung eines Lösegelds im Allgemeinen als letztes Mittel angesehen wird, gaben weltweit 90 % der Umfrageteilnehmer an, dass ihr Unternehmen – teils in jedem Fall, teils abhängig vom Betrag – die Zahlung eines Lösegelds in Betracht ziehen würde, wenn es so seine Daten und Geschäftsprozesse wiederherstellen oder ihre Wiederherstellung beschleunigen könnte. Zu den Ländern, die dazu am ehesten bereit wären, gehören:

- **Australien und Neuseeland (95 %)**
- **USA (94 %)**
- **Frankreich (93 %)**
- **Großbritannien (91 %)**

Deutschland **(87 %)** und Japan **(78 %)** wären weiterhin zu Zahlungen bereit, wenn auch insgesamt in geringerem Umfang.

Natürlich hat man es im Umgang mit Cyberkriminellen nicht mit gutwilligen Akteuren zu tun. Denken Sie immer daran, dass es keine Garantie gibt, dass bei Zahlung eines Lösegelds auch Ihre Daten freigegeben werden – oder dass diese im Falle einer Wiederherstellung sauber und frei von Malware sind.

Problem 3

Es wird immer schwieriger, eine Cyberversicherung abzuschließen.

Da Cyberkriminalität die Welt voraussichtlich jährlich 8 Billionen USD kosten wird (10,5 Billionen USD bis 2025), versuchen immer mehr Unternehmen, sich finanziell gegen Verluste durch Cyberangriffe, Datenschutzverletzungen und andere Cyber-Vorfälle abzusichern. Sie nutzen Cyberversicherungen als eine ihrer Schutzstrategien.

In diesem Jahr gaben 74 % der Umfrageteilnehmer an, dass ihr Unternehmen derzeit über eine Cyberversicherung verfügt. (In Japan hingegen waren es nur 61 %.) Aber der Abschluss einer Versicherungspolice ist nicht einfach – und wird immer schwieriger, wie fast die Hälfte (46 %) der Umfrageteilnehmer erklärten. Sie gaben an, dass es heute schwieriger sei als noch vor drei Jahren, eine Cyberversicherung abzuschließen.

Die Liste der Technologien und Fähigkeiten, die von den Befragten für entscheidend gehalten werden, wenn Unternehmen versuchen, eine Cyberversicherung abzuschließen, ist lang. Die Lösung umfasst:

- 40 % – Starke Verschlüsselung
- 38 % – Möglichkeit zum Überprüfen der Integrität von Backups
- 37 % – Multifaktor-Authentifizierung (MFA)
- 34 % – Erkennung von Anomalien
- 33 % – Datenisolation/ Air Gapping
- 29 % – Unveränderlichkeit

Die Erfüllung kritischer Funktionen kann nicht nur dazu beitragen, schwer erhältliche Cyberversicherungspolicen abzuschließen, sondern auch dazu, die Prämien zu senken.

Die Cyberversicherung bietet eine weitere Schutzebene in einem mehrschichtigen Sicherheitsansatz zur Bekämpfung von Ransomware und Cyberangriffen im weiteren Sinne.

Probleme gibt es im Überfluss. Aber das gilt auch für ihre Lösungen.

Es *ist* möglich, die Cyber-Resilienz zu stärken.

Trotz der gravierenden Probleme, die dieser Bericht behandelt, können Unternehmen ihre Cyber-Resilienz angesichts eskalierender Bedrohungen stärken, sei es gegen Ransomware und andere Cyber-Vorfälle (wie hier behandelt), Katastrophen wie Erdbeben oder Überschwemmungen, Systemausfälle oder auch menschliches Versagen.

Zwei konkrete Möglichkeiten zur Förderung der Cyber-Resilienz sind eine stärkere Zusammenarbeit und detailliertere Einblicke.

Intensivere Zusammenarbeit

87 % der Befragten meinen, dass Daten- und Cybersicherheitsanbieter zusammenarbeiten müssen, um vollständige und integrierte Anti-Ransomware-Lösungen bereitzustellen.[2] Wenn Anbieter auf das gemeinsame Ziel hinarbeiten, Ransomware zu bezwingen und integrierte Lösungen zu entwickeln, die saubere Wiederherstellungsmethoden unterstützen, profitieren Unternehmen davon. Eine stärkere Cyber-Resilienz hilft den Unternehmen selbst und ist besser für ihre Kunden ebenso wie für ihre Branchen. Da immer häufiger staatliche Akteure in Cyberkriminalität involviert sind, ist es auch für die Welt besser, diese Angriffe zu vereiteln und ausfallsicher zu werden.

Detailliertere Einblicke

Zusätzlich zu den Vorteilen der Zusammenarbeit zwischen Anbietern sind 90 % der Befragten der Meinung, dass ihr Unternehmen von einer Plattform für Data Security and Data Management profitieren würde, die Einblicke in ihre allgemeine Sicherheitslage und Cyber-Resilienz bietet. Mit diesen Einblicken können Unternehmen das Risiko von Betriebsunterbrechungen senken und ihre Widerstandsfähigkeit gegen Cyberangriffe verbessern. Darüber hinaus können diese Einblicke dazu beitragen, Prüfungen zur Einhaltung von Branchen- und Datenschutzvorschriften zu beschleunigen und zu vereinfachen.

2. Diese Statistik kombiniert die Ergebnisse der Befragten, die entweder „extrem wichtig“ oder „einigermaßen wichtig“ ausgewählt haben.

„In der heutigen hochentwickelten Cyber-Bedrohungslandschaft auf herkömmliche Datensicherung und -wiederherstellungssysteme zu vertrauen, denen es an modernen Datensicherheitsfunktionen mangelt, ist ein Weg in die Katastrophe. Stattdessen sollten Unternehmen nach Plattformen für Data Security and Data Management suchen, die sich in ihre bestehenden Cybersicherheitslösungen integrieren lassen, Einblick in ihre Sicherheitslage bieten und ihre Cyber-Resilienz verbessern.“

BRIAN SPANSWICK, CHIEF INFORMATION SECURITY OFFICER AND HEAD OF IT, COHESITY

„Die einzige Möglichkeit, Cyber-Resilienz zu erreichen, besteht darin, proaktive Sicherheitsmaßnahmen zu priorisieren, die Cyberangriffe von vornherein verhindern. Dieser Ansatz sollte sich auch auf die Datensicherung und -wiederherstellungsmaßnahmen erstrecken, um die Geschäftskontinuität auch im Falle eines Cybersicherheitsvorfalls zu gewährleisten. Unternehmen müssen daher nicht nur ihr Cyber-Risiko verwalten, sondern auch ihre Gefährdung besser verstehen, indem sie Schwachstellen- und Gefährdungsdaten nutzen, um fundierte Entscheidungen über Abhilfemaßnahmen zu treffen.“

RAY KOMAR, VICE PRESIDENT OF TECHNOLOGY AND CLOUD ALLIANCES, TENABLE

Bericht zum Stand von Datensicherheit und -management 2023

Fazit

Wenn ein Unternehmen von Ransomware betroffen ist und Daten gestohlen, gelöscht, infiziert oder auf andere Weise kompromittiert werden, kann es erst wieder ordnungsgemäß funktionieren, wenn seine Daten, Prozesse, Abläufe und Anwendungen wiederhergestellt wurden. Für die Widerstandsfähigkeit des Unternehmens ist es von entscheidender Bedeutung, sicherzustellen, dass diese Wiederherstellung sauber und schnell erfolgt.

Angesichts dieser Realität ist ein umfassender Data Security and Management-Ansatz die beste Verteidigung gegen anhaltende weltweite Bedrohungen.

Die diesjährige globale Umfrage zeigt Folgendes:

1. **Die meisten Unternehmen verfügen immer noch nicht über die notwendigen Cyber-Resilienz-Strategien oder Datensicherheitsfunktionen, um diesen Bedrohungen zu begegnen und die Geschäftskontinuität aufrechtzuerhalten.**
2. **Weniger IT- und SecOps-Experten sind zuversichtlich, dass sich ihr eigenes Unternehmen nach einem Cyberangriff effektiv und schnell erholen kann.**
3. **Cyberversicherungen sind zwar verfügbar, aber immer schwieriger abzuschließen. Die Liste der Technologien und kritischen Fähigkeiten, die für die Qualifizierung erforderlich sind, ist lang.**

Letztendlich werden Unternehmen, die mit Anbietern zusammenarbeiten, und ihre Lösungen für Cybersicherheit, Datensicherheit und -management gemeinsam mit Partnern integrieren, besser in der Lage sein, Cybervorfällen zu widerstehen, sich davon zu erholen und ihre Gesamtbetriebsrisiken zu senken. Darüber hinaus sind Unternehmen mit Datensicherheit und -management-Plattformen, die Einblicke in ihre allgemeine Sicherheitslage bieten, besser in der Lage, Bedrohungen zu widerstehen und sich sicher zu erholen.

Heutige Unternehmen können es sich nicht leisten, unvorbereitet zu sein.

COHESITY