

ESG WHITEPAPER

Die Rolle der Datenspeicherung für die Herstellung echter Cyberresilienz

Von Scott Sinclair, ESG Practice Director und Senior Analyst
und Monya Keane, ESG Senior Research Analyst

Januar 2022

Dieses ESG Whitepaper wurde im Auftrag von IBM erstellt
und unter der Lizenz von TechTarget, Inc. herausgegeben.

Inhalt

Kurzfassung.....	3
Einleitung	3
Wachsende Bedrohung durch Cyberattacken und Ransomware.....	3
Die Rolle der Datenspeicherung für die Cyberresilienz	5
Datenspeicherung und Datensicherung: Ansatzpunkte für die Minimierung von Ransomware-Risiken	6
Von Cybersicherheit zu Cyberresilienz mit IBM	6
Cyberresilienz mit IBM Cyber Vault	7
The Bigger Truth	8

Kurzfassung

Daten spielen bei der Transformation von Unternehmen eine immer wichtigere Rolle. Steigende Investitionen in die Anwendungsentwicklung, moderne DevOps-Praktiken und gestiegene Anforderungen an Business Intelligence, Analytik und maschinelles Lernen – nahezu alle Unternehmen setzen verstärkt auf die Erstellung und Nutzung von Datenbeständen. Darüber hinaus erhöht sich die Zahl der Standorte, an denen die Daten genutzt werden. Wachsende Datenmengen in Verbindung mit dem zunehmenden Druck, den Betrieb zu beschleunigen, haben die Komplexität sowohl der IT-Infrastruktur als auch des IT-Betriebs erhöht.

Dadurch steigt für Unternehmen und ihre Infrastrukturen das Risiko von bösartigen Angriffen, menschlichen Fehlern und fahrlässigem Verhalten. Leider lässt sich mit herkömmlichen Strategien nicht hinreichend sicherstellen, dass der Geschäftsbetrieb während und nach solchen Ereignissen weiterläuft. Unternehmen können versuchen, Funktionen miteinander zu verknüpfen, um Angriffe und andere Verstöße zu verhindern, jedoch ist die Erfüllung von Sicherheitszielen aufgrund von funktionalen Lücken, schlechter Integration und komplexer Verwaltung zeitaufwändig und schwierig.

Eine Abkehr von reiner Prävention hin zur aktiven Vorbereitung auf den Ernstfall – z. B. in Form von Speicherlösungen mit integrierter Cyberresilienz – ist der Schlüssel zum Schutz kritischer Datenbestände und zur schnellen Reaktion und Wiederherstellung nach Angriffen mit Ransomware oder anderen Cyberattacken.

Einleitung

Der IT-Bereich steht vor neuen Herausforderungen. Fast die Hälfte (46 %) der Befragten der ESG-Umfrage gaben an, dass ihre IT heute komplexer als noch vor zwei Jahren ist. Ursachen für den höheren Komplexitätsgrad können laufende digitale Transformationsinitiativen (29 %), höhere Datenmengen (35 %), die rasche Weiterentwicklung der Cybersicherheitslandschaft (37 %) und/oder Bemühungen um die Einhaltung neuer Datensicherheits- und Datenschutzbestimmungen (32 %) sein.¹

Gleichzeitig haben Unternehmen mit einem problematischen Mangel an qualifizierten IT-Fachkräften zu kämpfen. Tatsächlich geben 48 % der befragten Unternehmen an, dass sie nicht genügend Cybersicherheitspezialisten haben. Dies war der am häufigsten genannte Mangelbereich. Darüber hinaus müssen sich Unternehmen für eine zunehmenden Zahl von Anwendungen, Geräten und mobilen Mitarbeitern rüsten, also für eine deutliche Ausweitung des Sicherheitsbereichs, den die IT-Abteilung schützen muss.²

Angesichts der Komplexität der modernen IT, der wachsenden Datenmenge und der zunehmenden Bedrohung durch Cyberangriffe haben IT-Teams oft Mühe, Schritt zu halten. Wer versucht, Komplexität allein mit internem Personal zu bewältigen, kämpft auf verlorenem Posten. Um erfolgreich zu sein, bedarf es einer Modernisierung der zugrundeliegenden Infrastruktur. IT-Entscheidungsträger müssen Technologien ins Auge fassen, die nicht nur die Anwendungsanforderungen erfüllen und den Betrieb vereinfachen. Echten Erfolg bringen nur Ansätze, die neben diesen Zielen auch die Cyberresilienz der Anwendungsumgebung verbessern.

Wachsende Bedrohung durch Cyberattacken und Ransomware

Unternehmen sind mit zunehmenden Bedrohungen ihrer IT-Systeme konfrontiert – ein lukratives Betätigungsfeld für Cyberkriminelle. So sind die Meldungen aus der amerikanischen Öffentlichkeit an das Internet Crime Complaint Center (IC3) des FBI im Jahr 2020 gegenüber 2019 um 69% gestiegen, wobei die gemeldeten Verluste über 4,1 Milliarden Dollar

¹ Quelle: Vollständige Umfrageergebnisse ESG, [2022 Technology Spending Intentions Survey](#), November 2021.

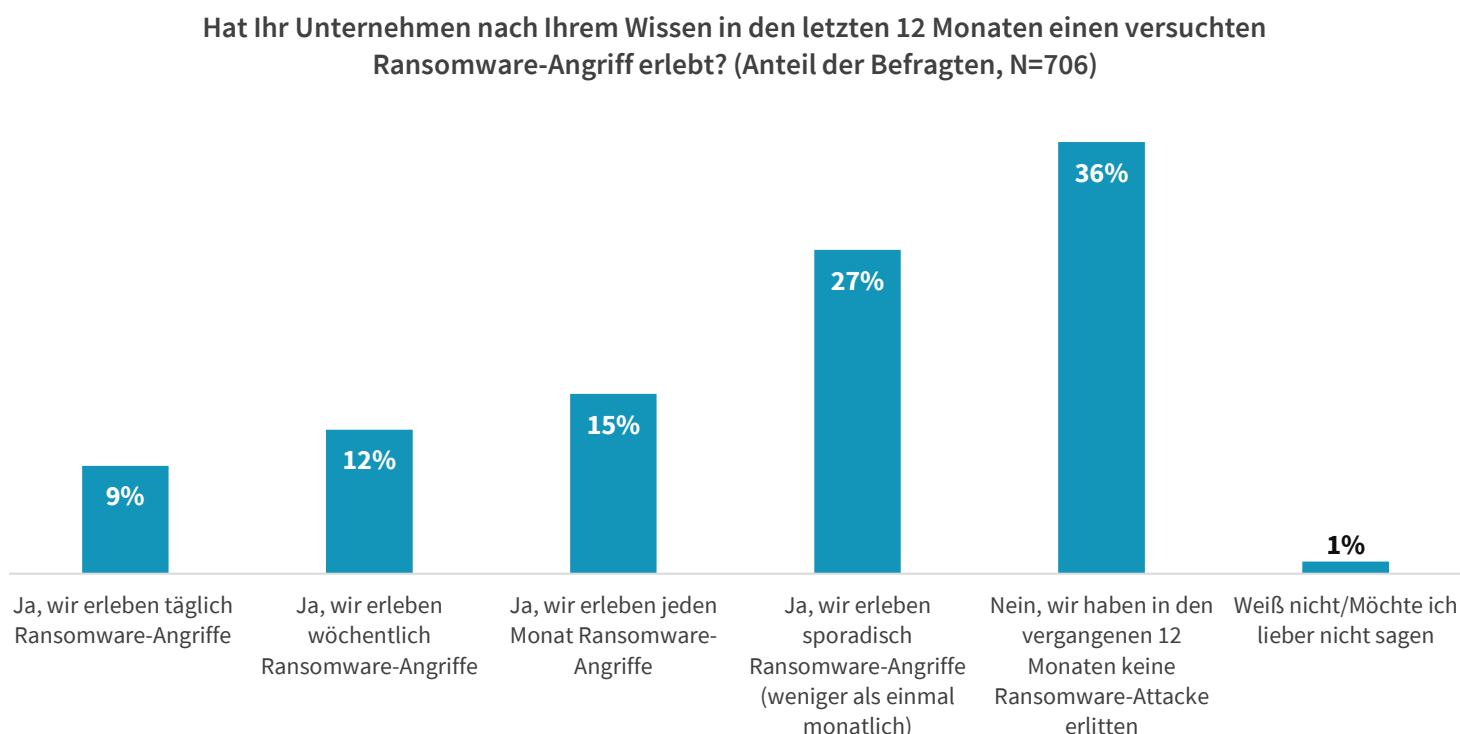
² Ebd.

betrogen.³ Für die letzten fünf Jahre beziffert das IC3 die Verluste auf insgesamt 13,3 Milliarden Dollar.⁴ Im vierten Quartal 2020 betrug die durchschnittliche Dauer der Unterbrechung nach einem Ransomware-Angriff in den USA 21 Tage.⁵ Die negativen Auswirkungen von Ransomware auf den Geschäftsbetrieb sind zweifellos erheblich.

Es besteht eine starke Korrelation zwischen der Komplexität der IT und der Anfälligkeit für Cyberangriffe. Da die IT immer komplexer wird, treten Cyberangriffe immer häufiger auf und werden immer verlustreicher.

Ransomware ist eine verbreitete Bedrohung, die das wertvollste Gut eines Unternehmens angreift – seine Daten. Das IC3 registrierte 2.474 gemeldete Ransomware-Vorfälle im Jahr 2020. ESG stellte in einer Umfrage fest, dass 63 % der befragten

Abbildung 1. 63 % Prozent der Befragten waren in den letzten 12 Monaten von Ransomware-Angriffen betroffen



Quelle: ESG, ein Geschäftsbereich von TechTarget, Inc.

Unternehmen im vergangenen Jahr von Ransomware-Angriffen betroffen waren. Tatsächlich erlebten 9 % der Befragten sogar täglich Ransomware-Angriffe (siehe Abbildung 1).⁶

Der Schutz vor Ransomware erfordert eine Technologiestrategie, die über den die traditionelle Cybersicherheit hinausgeht und sich neuere Fortschritte bei Datenspeicherung und Datenschutz zunutze macht.

³ Quelle: Federal Bureau of Investigation Internet Crime Complaint Center, [Internet Crime Report 2020](#).

⁴ Ebd.

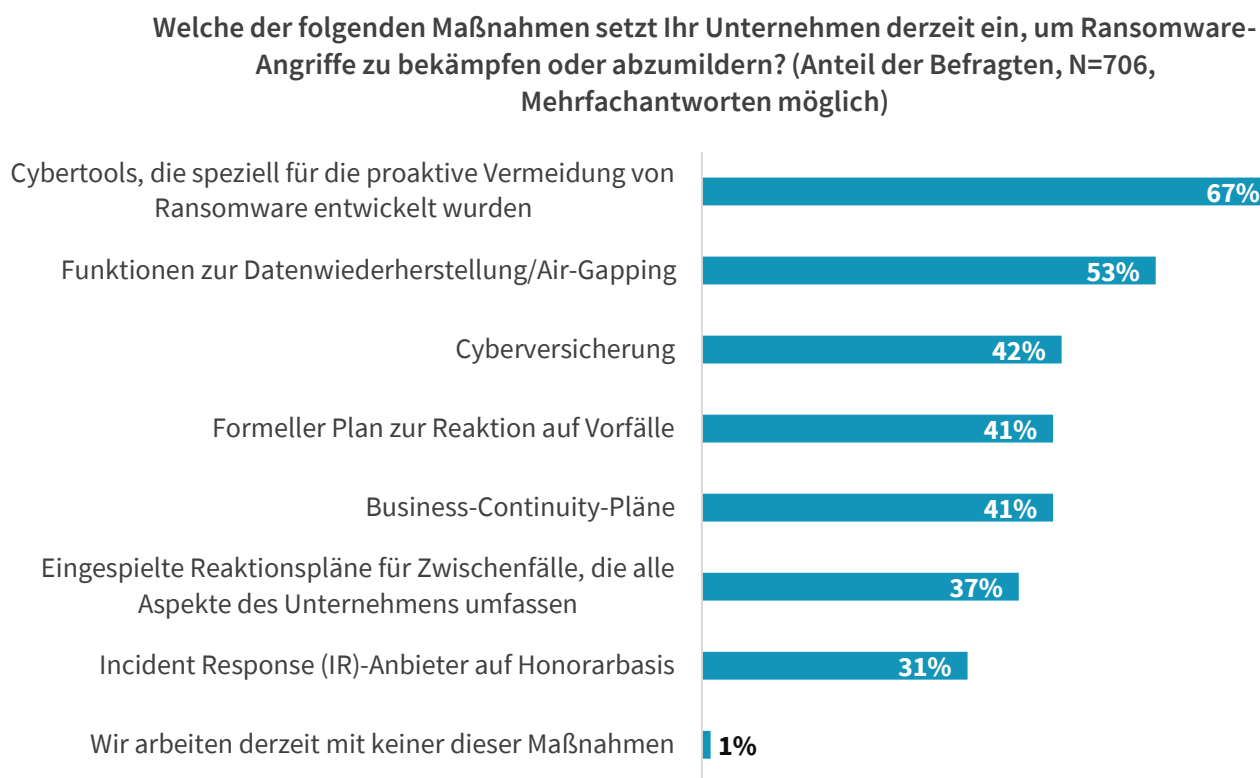
⁵ Quelle: Coveware Blog, [Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands](#), Februar 2021.

⁶ Quelle: Vollständige Umfrageergebnisse ESG, [2022 Technology Spending Intentions Survey](#), November 2021.

Die Rolle der Datenspeicherung für die Cyberresilienz

Beim Schutz vor Ransomware spielen sowohl die Speichersysteme als auch die Speicheradministratoren eine wichtige Rolle. ESG befragte IT-Entscheider, welche Maßnahmen ihre Unternehmen zur Bekämpfung oder Eindämmung von Ransomware-Angriffen ergriffen haben. 67 % der Befragten gaben an, dass sie Cybertools zur proaktiven Vermeidung von Ransomware einsetzen, und 53 % nannten Ansätze zur Datenwiederherstellung wie Air-Gapping (siehe Abbildung 2).⁷ Diese beiden häufig gegebenen Antworten machen deutlich, wie wichtig es ist, nicht nur Maßnahmen zur Vermeidung eines Angriffs zu ergreifen, sondern auch in Lösungen zu investieren, die sicherstellen, dass sich das Unternehmen nach einem unabwendbaren Angriff wieder erholt. Es reicht nicht, lediglich Richtlinien zur Bekämpfung oder Eindämmung von Ransomware einzurichten. Dieser „partielle“ Ansatz schafft ein falsches Gefühl der Sicherheit, da zwar Anstrengungen unternommen werden, um Angriffe abzuschwächen, aber wenig oder gar keine Bemühungen, um einen effektiven Datenwiederherstellungsplan zu erstellen, *bevor* er benötigt wird.

Abbildung 2. Gängige Maßnahmen zur Bekämpfung oder Eindämmung von Ransomware-Attacken



Quelle: ESG, ein Geschäftsbereich von TechTarget, Inc.

Es ist wichtig, nicht aus dem Blick zu verlieren, dass die Bekämpfung eines Angriffs etwas ganz anderes ist als eine herkömmliche Datenwiederherstellung. Normalerweise wollen Unternehmen ihre Daten fast immer mit der aktuellsten Kopie wiederherstellen. Aber bei Ransomware weiß die IT-Abteilung in der Regel nicht, welche Kopie sicher und am besten geeignet ist. Daher ist die Wiederherstellung oft riskanter und kann viel länger dauern. Einige Ransomware-Angriffe zielen nicht nur auf Daten ab, sondern auch auf die Backup-Infrastruktur. Aus diesem Grund sind fortschrittliche Speicherfunktionen die Grundlage für eine effektive Ransomware-Wiederherstellung.

⁷ Ebd.

Auch wenn die in Abbildung 2 genannten Maßnahmen sicherlich klug sind und weiter ausgebaut werden sollten, dürfen Unternehmen nicht vergessen, dass eine einzelne Abwehrmaßnahme niemals zu 100 % wirksam sein und eine vollständige Wiederherstellung nach Ransomware gewährleisten kann. Es ist zwar wichtig, Tools in Betracht zu ziehen, die auf die Erkennung und Abwehr von Ransomware sowie die Wiederherstellung von Daten spezialisiert sind, aber das ist nur ein Teil der Bemühungen. Selbst die beste Verteidigung kann bei einem Angriff durchbrochen werden. Unternehmen müssen sich auf diese Eventualität vorbereiten und prüfen, wie sie die Auswirkungen auf das Geschäft durch schnellstmögliche Wiederherstellung minimieren können. Um die Gefährdung durch Ransomware insgesamt zu minimieren, sollten Unternehmen nach Möglichkeiten suchen, wie sie Angriffe schneller erkennen, schnell eventuelle Schäden abmildern und ihre Bestände anhand einer sicheren und brauchbaren Kopie wiederherstellen können.

Hier kommen starke Cyberresilienz-Strategien ins Spiel, die *alle Komponenten des Datenmanagements* berücksichtigen, also die Hardware, die Software, den Menschen und die Prozesse. Bei der Entwicklung einer Cyberresilienz sollten sich Unternehmen nicht mehr fragen: „Wie schützen wir uns?“, sondern „Wie schnell können wir unsere Abläufe nach einem Ransomware-Angriff wiederherstellen? Wie schnell kann unser Geschäft zur Normalität zurückkehren?“

Datenspeicherung und Datensicherung: Ansatzpunkte für die Minimierung von Ransomware-Risiken

Die Wiederherstellung nach Ransomware ist eine Form der Notfallwiederherstellung. Allerdings sind die Auswirkungen von Ransomware ganz anders als beispielsweise die eines Feuers oder einer Überschwemmung. Bei einem Feuer kann man erkennen, wenn es vollständig gelöscht und die Gefahr gebannt ist. Ransomware hingegen hinterlässt versteckte Funken, die jederzeit wieder aufflammen können. Speicheradministratoren müssen sich auf bestimmte Bereiche konzentrieren, um die mit Ransomware verbundenen Risiken zu verringern. Da Schnelligkeit entscheidend ist, müssen sie wissen, wie schnell ihr Unternehmen:

- ein Risiko aufdecken kann;
- einen erlittenen Schaden beziffern kann;
- einen Schaden mindern kann, indem es eine sichere und brauchbare Kopie identifiziert, die Wiederherstellung mit dieser Kopie durchführt und schließlich den Betrieb wiederherstellt.

Eine „Uns passiert das schon nicht“-Haltung ist bestenfalls riskant. Unternehmen müssen proaktiv handeln und eine effektive Lösung zur Datenspeicherung und zum Schutz ihrer Daten einrichten – bevor sie sie tatsächlich benötigen.

Von Cybersicherheit zu Cyberresilienz mit IBM

Mit seiner umfangreichen Erfahrung in den Bereichen Cybersicherheit und Risikomanagement ist IBM ein anerkannter Marktführer im Bereich der Cyberresilienz und bietet eine umfassende Palette an fortschrittlichen Speicher- und Datenschutzlösungen, darunter:

- **IBM FlashSystem, IBM Cloud Object Storage und IBM Spectrum Scale**, Primärspeicherlösungen, die Daten in unveränderbarer Form speichern und über Verschlüsselungsfunktionen verfügen.
- **IBM Tape Storage**, eine Lösung, die die Unveränderbarkeit und Verschlüsselung von Daten unterstützt und Schutz durch Air-Gapping bietet.
- **IBM Spectrum Copy Data Management**, eine Software für Datenmanagement und Schutz von Datenkopien.

- **IBM Spectrum Protect Suite** für zusätzlichen Schutz. Spectrum Protect Software-definierter Storage kann Daten auf Flash, Festplatte, Objekt-Storage und physisches oder virtuelles Tape speichern. Es erkennt dann Malware- und Ransomware-Aktivitäten, indem es größere Abweichungen von normalen Zugriffsmustern identifiziert.
- **QRadar und Storage Insights** beschleunigen die Erkennung potenzieller Bedrohungen durch KI-gestützte Funktionen.

Cyberresilienz mit IBM Cyber Vault

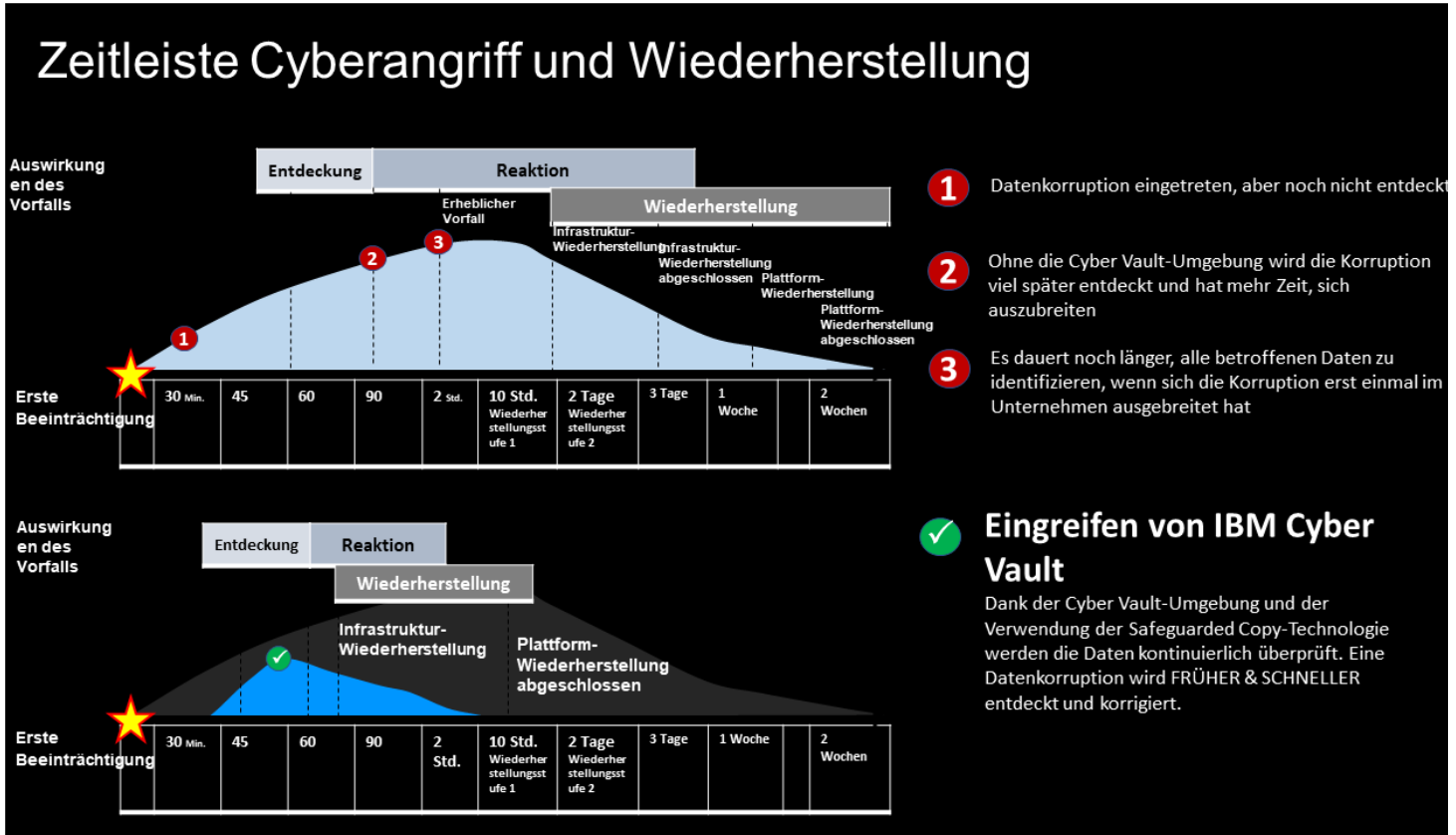
Die Rolle des Speichers beim Schutz vor Ransomware kann gar nicht hoch genug eingeschätzt werden. Die Speichersoftware sieht die Änderungen, die an den Primärdaten vorgenommen werden, und ist dadurch in der Lage zu erkennen, wenn ein Angriff beginnt. Sie beinhaltet die Technologie, die Sekundärkopien erstellt und schützt – und damit einen wichtigen Beitrag zur Wiederherstellung leistet. In Anbetracht all dieser Tatsachen ist IBM Cyber Vault wohl eines der nützlichsten Tools im IBM Werkzeugkasten für Cyberresilienz.

IBM Cyber Vault ist eine Sicherheitslösung zur schnellen Wiederherstellung nach einer Cyberattacke. Sie basiert auf IBM Safeguarded Copy, einer Technologie zur regelmäßigen Erstellung isolierter, unveränderlicher Snapshots. Cyber Vault analysiert diese Snapshots auf potenziell bösartige Änderungen, die auf Ransomware hinweisen könnten. IBM Cyber Vault lässt sich auch mit IBM QRadar und IBM Storage Insights integrieren, um eine noch schnellere Erkennung zu ermöglichen. Die Validierung unveränderbarer Kopien ermöglicht es Administratoren, schnell eine brauchbare Kopie zu identifizieren, sie zu überprüfen und dann den Datenbestand aus ihr wiederherzustellen.

IBM Cyber Vault hilft Speicheradministratoren insbesondere bei der Beschleunigung folgender Vorgänge:

- **Identifikation** – Die Integration von QRadar und Storage Insights bietet eine verbesserte Erkennung und Überwachung.
- **Minderung und Quantifizierung des Schadens** – Dies geschieht im Rahmen eines automatisierten Prozesses. Die frühzeitige, automatische Erkennung von Angriffen ermöglicht logischerweise eine schnellere Wiederherstellung.
- **Identifizierung einer sicheren und brauchbaren Kopie** – Die automatische Identifizierung unveränderlicher Datenkopien erfolgt, wenn eine Bedrohung erkannt wird.
- **Wiederherstellung des Betriebs** – Eine schnelle Wiederherstellung innerhalb von Stunden statt Tagen oder Wochen ist möglich (siehe Abbildung 3).

Abbildung 3. Wie IBM Cyber Vault die Cyberwiederherstellung beschleunigt



Quelle: IBM

The Bigger Truth

IT-Infrastrukturen werden immer komplexer, was das Risiko für menschliche Fehler, Systemausfälle oder Nachlässigkeit erhöht. Gleichzeitig sind böswillige Akteure – sowohl innerhalb als auch außerhalb des Unternehmens – unermüdlich auf der Suche nach Schwachstellen und nutzen diese aus.

Sicherheitsvorfälle sind zweifelsohne unvermeidbar. Daher sollten Unternehmen von reaktiv zu proaktiv umdenken, von reiner Prävention hin zur Vorbereitung auf Sicherheitsprobleme und deren Handhabung *im Moment ihres Auftretens*. Dies ist der Wandel, den Unternehmen vollziehen müssen, um von Cybersicherheit zu echter Cyberresilienz zu gelangen.

Viele Unternehmen orientieren sich bei der Entwicklung ihrer Cyberresilienz-Strategien an den Vorgaben des NIST Cybersecurity Framework, in dem empfohlen wird, kritische Ressourcen zu identifizieren, diese Ressourcen zu schützen, Ausfälle und Verstöße zu erkennen und die Reaktion und Wiederherstellung auf Cybervorfälle zu planen. Führende Unternehmen setzen insbesondere auf IT-Infrastrukturfunktionen, die ihre Cyberresilienz durch Funktionen wie Datenermittlung, Kopienverwaltung, Verschlüsselung, Zugriffskontrolle und unveränderliche Speicherung verbessern und gleichzeitig mehrere Optionen zur Datenwiederherstellung bereitstellen können.

Für die IT- und Unternehmensleitung geht es bei der Cyberresilienz darum, die richtigen technologischen und geschäftlichen Entscheidungen zu treffen, um den Geschäftsbetrieb aufrechtzuerhalten.

Alle Produktnamen, Logos, Marken und Warenzeichen sind Eigentum ihrer jeweiligen Inhaber. Die Informationen in dieser Publikation stammen aus Quellen, die TechTarget, Inc. als zuverlässig erachtet, ohne jedoch Gewähr für deren Richtigkeit zu unternehmen. Diese Publikation kann Ansichten von TechTarget, Inc. enthalten, die sich jederzeit ändern können. Sie kann ferner Prognosen, Hochrechnungen und andere vorausschauende Aussagen enthalten, die Annahmen und Erwartungen von TechTarget, Inc. vor dem Hintergrund der derzeit verfügbaren Informationen darstellen. Diese Prognosen beruhen auf Branchentrends und beinhalten Variablen und Unsicherheiten. Folglich übernimmt TechTarget, Inc. keine Garantie für die Richtigkeit von Prognosen, Hochrechnungen oder vorausschauender Aussagen, die hierin enthalten sind.


Diese Veröffentlichung ist urheberrechtlich geschützt durch TechTarget, Inc. Jegliche Vervielfältigung oder Weitergabe, ob ganz oder teilweise, ob in Papierform, elektronisch oder auf andere Weise an Personen, die nicht zum Erhalt der Publikation berechtigt sind, verstößt ohne die ausdrückliche Zustimmung von TechTarget, Inc. gegen das US-Urheberrecht und wird zivilrechtlich und gegebenenfalls strafrechtlich verfolgt. Weitere Fragen beantwortet unsere Kundenberatung unter cr@esg-global.com.



Die Enterprise Strategy Group ist ein integriertes Unternehmen für Technologieanalyse, Recherche und Strategiearbeit, das der weltweiten Tech-Community Marktdaten, relevante Informationen und Content-Services für Produkteinführungen bietet.

 www.esg-global.com

 contact@esg-global.com

 508.482.0188