CYBER RESILIENCE HANDBUCH

Best Practices, um von einer minimalen Viabilität zur vollständigen Wiederherstellung nach einem Cyberangriff zu gelangen

Commvault®

ÜBERBLICK

Die Vorbereitung auf die Wiederherstellung nach einem Cyberangriff ist in der heutigen digitalen Ära entscheidend, in der Cyberdrohungen zunehmend komplex und weit verbreitet sind.

Effektive Strategien zur Wiederherstellung nach einem Cyberangriff sind entscheidend, um diese Bedrohungen zu bekämpfen und Ihr Unternehmen zu befähigen, in der Lage zu sein, nach einem Cyberangriff schnell kritische Systeme und Daten wiederherzustellen – die Ausfallzeiten zu minimieren und den Einfluss auf die Geschäftstätigkeit zu mildern.

Durch eine gute Vorbereitung auf Cyberangriffe zeigen Unternehmen Kunden, Stakeholdern und Aufsichtsbehörden, dass sie es ernst meinen, sensible Daten und die Systeme zu schützen, um ihre Verpflichtungen gegenüber ihren Kunden zu erfüllen.

Der erste Schritt zur Erstellung eines Plans zur Cyberbereitschaft besteht darin, die für die Mission kritischen Personen, Prozesse, Systeme und Daten zu identifizieren, die für den Betrieb notwendig sind – dies ist Ihre minimale Viabilität. Für die meisten Unternehmen umfasst dies die exekutive und operative Führung, ein Verständnis der Rollen und Verantwortlichkeiten während der Wiederherstellung sowie die technische Fähigkeit, kritische Systeme wie Unternehmensidentität (z. B. Active Directory), Kommunikationskanäle (z. B. E-Mail, Chat, Zusammenarbeitstools) wiederherzustellen und sicherzustellen, dass Daten, Anwendungen und Infrastruktur sauber und bereit sind, um aus dem Backup wiederhergestellt zu werden.

Neben den Compliance-Richtlinien (wie z. B. DSGVO, HIPAA, DORA oder SOCI), die detaillierte Cybersecurity-, Resilienz-, Notfallwiederherstellungs- und Geschäftskontinuitätspläne erfordern, verringert ein gut strukturierter Wiederherstellungsplan nach einem Cyberangriff das Risiko von Datenverlust und stellt sicher, dass kritische Informationen wie Kundendaten, proprietäre Daten und geistiges Eigentum geschützt bleiben [CF1]. Im Falle einer Datenkompromittierung hilft ein schnelles Wiederherstellungssystem dabei, die minimalen betriebsfähigen Operationen schnell wiederherzustellen und die Systeme schnell wieder online zu bringen.

DER COMMVAULT + GIGAOM BERICHT UNTERSTREICHT DIE KRITISCHE NOTWENDIGKEIT UMFASSENDER CYBERWIEDERHERSTELLUNGSSTRATEGIEN.

Lesen Sie weiter, um mehr über die wesentlichen Komponenten zu erfahren, die notwendig sind, um auf einen Cyberangriff vorbereitet zu sein – und sehen Sie, wie Commvault® Cloud die Werkzeuge liefert, die Ihnen zum Erfolg verhelfen.

STEP #01

IDENTIFIZIEREN

Ein wesentliches Prinzip jeder Strategie ist eine weitreichende Einsicht in die Umgebung und ein Verständnis dafür, welche Anwendungen, Systeme und Daten benötigt werden, um im Falle von Ausfällen und Cyberangriffen eine minimale Viabilität zu gewährleisten.

Mit Commvault Cloud umfasst dies die Fähigkeit, sensible Daten in allen Ihren Datenspeichern zu erfassen, zu klassifizieren und zu überwachen. Sobald Sie wissen, was geschützt werden muss, können Sie die Umgebung mit Bedrohungserkennung, Anomalieerkennung und Frühwarnmechanismen ausstatten, um Sicherheitsteams auf Bedrohungen in Ihren Netzwerken hinzuweisen, bevor sie Schaden anrichten. Sie benötigen auch einen mehrschichtigen Ansatz, um Malware, Ransomware und andere Vektoren für Datenkorruption zu finden und zu stoppen. Daten sollten an allen Punkten ihres Lebenszyklus überprüft werden, um korrupte Daten zu finden, damit Sie sie auf einen sauberen Zeitpunkt zurücksetzen können.

COMMVAULT CLOUD-PRODUKTE ZUR IDENTIFIZIERUNG VON BEDROHUNGEN:

- Risikoanalyse zur Erkennung und Kontrolle sensibler Daten
- Threatwise™ zur Erkennung von Bedrohungen und Anomalien sowie zur Frühwarnung
- Threat Scan zur Identifizierung von schädlichen oder korrupten Daten

COMMVAULT CLOUD PLATTFORM FÄHIGKEITEN:

- Cleanpoint-Validierung

STEP #02

SCHÜTZEN

Um auf einen unvermeidlichen Angriff vorbereitet zu sein, müssen Sie Ihre Daten vor den Aktionen von Angreifern, böswilligen Insidern und sogar Fehlkonfigurationen oder Ausfällen schützen. Dieser Schutz ist vielschichtig und muss die Daten selbst, die Identität und die Konfigurationen berücksichtigen.

Beginnend mit den Daten, empfiehlt es sich, dass Organisationen der 3-2-1-Regel folgen: drei Kopien der Daten, auf zwei Arten von Medien (oder auf zwei verschiedenen Plattformen) und eine Kopie, die nicht verändert werden kann. Das Duplizieren von Daten für die ersten beiden Schritte ist einfach, aber der dritte ist etwas herausfordernder. Sie benötigen einen Mechanismus, um die Daten unveränderlich und unlöschbar zu machen, um sie vor einseitigen Änderungen oder Löschungen zu schützen. Dies ist aus zwei Gründen besonders wichtig – die meisten Ransomware-Programme haben Mechanismen, um Backups zu manipulieren, und Insider-Bedrohungen sind real. Sie müssen sicherstellen, dass Ihre Infrastruktur (sowohl Cloud als auch Backup) nach den Prinzipien des Zero Trust konfiguriert ist. Es sollten Mechanismen vorhanden sein, die Konfigurationen überprüfen und Änderungen oder „Drifts“ melden und darauf hinweisen. Die Authentifizierung sollte ebenfalls den Prinzipien des Zero Trust folgen und je nach Zugriffsebenen und durchgeführten Aktionen eine Multi-Faktor- und Multi-Personen-Autorisierung umfassen. Darüber hinaus sollte jeder Mechanismus, den Sie zur Validierung der Identität verwenden, wie z.B. Active Directory oder Entra ID, ebenfalls konfiguriert, gesichert und auf Änderungen wie Hinzufügungen, Löschungen oder Privilegienanhebungen überwacht werden. Alle Daten, Konfigurationen oder Steuerungsebenen sollten gesichert werden, um eine Wiederherstellung im Falle eines Sicherheitsvorfalls zu ermöglichen, und die Backups sollten isoliert und air-gapped sein, um die Wahrscheinlichkeit zu verringern, dass Angreifer die Backups während der Aufklärung finden oder dass sie durch Malware oder Ransomware gelöscht oder verschlüsselt werden.

COMMVAULT CLOUD-PRODUKTE, DIE IHNEN HELFEN, IHRE DATEN ZU SCHÜTZEN:

- Backup und Wiederherstellung über Cloud-, On-Premises- und SaaS-Workloads
- Active Directory Backup und Wiederherstellung zum Schutz von Active Directory und Entra ID
- Air Gap Protect für unveränderlichen, unlöschbaren und getrennten Speicher
- Threat Scan zur Identifizierung und Quarantäne von schädlichen oder beschädigten Daten

COMMVAULT CLOUD PLATTFORM FÄHIGKEITEN:

- Security IQ für die Sicherheitslage-Verwaltung Ihrer Backup-Umgebung
- Rollenbasierte Zugriffskontrolle (RBAC) und MehrpersonenAutorisierung

STEP #03

ANTWORTEN

Keine Technologie wird Ihnen in einem Silo gut dienen. Deshalb integriert sich Commvault Cloud mit Security Information und Event Management (SIEM)-Software und Security Orchestration, Automation, und Remediation (SOAR)-Plattformen.

Dies ermöglicht den Austausch von Kontextinformationen zwischen Commvault Cloud und anderen Sicherheitswerkzeugen, um Sicherheitsvorfälle, Datenintegritätsprobleme und anomale Aktivitäten besser zu erkennen. Egal, ob Sie die Palo Alto Networks XSOAR-Plattform, Splunk SIEM, Microsoft Sentinel oder ein anderes Tool verwenden, die Bedrohungs- und Anomalieerkennung von Commvault Cloud ist ein Kraftverstärker beim Aufbau von Cyber-Resilienz und der Verbesserung der Vorfallreaktion. Wenn Commvault Cloud verdächtige Dateien findet oder eine Anomalie-Warnung von einer Integration erhält, kann diese Datei automatisch von Ihren Produktionsdaten isoliert und eine Kopie an einen Sandbox-Bereich zur Detonation und Analyse gesendet werden, um festzustellen, ob sie schädlich ist.

MIT FUNKTIONEN DER COMMVAULT CLOUD PLATTFORM KÖNNEN SIE SCHNELLER AUF BEDROHUNGEN REAGIEREN:

- Integrationen in das Sicherheitsökosystem mit SIEM- und SOAR-Technologien
- Integrationen von Bedrohungsinformationen für eine breitere Abdeckung von Bedrohungen
- Sandbox-Integrationen zur Ermöglichung der Inspektion und Detonation verdächtiger Dateien

STEP #04

WIEDERHERSTELLEN

Wenn es darum geht, Daten wiederherzustellen, sei es nach einer Katastrophe oder einem Cyberangriff, benötigen Sie einen Plan, der geübt und dokumentiert wurde; saubere, vollständige Daten; Flexibilität bei den Wiederherstellungszielen; die Fähigkeit, alles von den Daten bis zur Anwendung, die sie verwendet, wiederherzustellen; und Geschwindigkeit.

Der schlechteste Zeitpunkt, um festzustellen, dass Ihr Wiederherstellungsplan nicht funktioniert, ist, wenn Sie einem Angriff gegenüberstehen. Regelmäßige Tests sowohl der Mindestviabilität als auch der vollständigen Wiederherstellungspläne sind entscheidend, um sicherzustellen, dass eine Wiederherstellung im Bedarfsfall möglich ist, und helfen den Teams, welch die Wiederherstellung durchführen, zu verstehen, was von ihnen verlangt wird.

Portabilität ist für Tests und Wiederherstellung wichtig, da ein Angriff oder eine Ausfallzeit erfordern kann, dass gesamte Arbeitslasten in eine neue und unterschiedliche Umgebung verschoben werden. Dies könnte einfach das Wechseln von Konten bedeuten oder so drastisch sein, wie von lokal zu Cloud oder zu einer völlig anderen Cloud zu wechseln – daher muss Ihre Wiederherstellung hybrid und flexibel sein.

Wir haben bereits die Notwendigkeit des Scannens und Überwachens von Daten auf Anomalien, Malware und andere Defekte diskutiert. Wenn es an der Zeit ist, wiederherzustellen, ist es wichtig, eine letzte Überprüfung der Daten durchzuführen, um sicherzustellen, dass sie sauber, bereit zur Wiederherstellung und nicht einfach nur dazu da sind, Ihre Umgebung erneut zu infizieren.

Schließlich benötigen Sie nach einer Wiederherstellung eine Kopie der Daten und Systeme, die von dem Angriff betroffen waren, um sie an Drittanbieter für Untersuchungen und Incident-Response-Teams, Strafverfolgungsbehörden, Cyber-Versicherer oder andere interessierte Parteien weiterzugeben. Diese forensische Kopie sollte von Ihrer Produktionsumgebung getrennt und für Ihre Untersuchungen unverändert aufbewahrt werden. Dies kann bei der Rückentwicklung von Malware, der Identifizierung des Angreifers und der Identifizierung von Techniken und Verfahren, auf die man sich in Zukunft vorbereiten muss, helfen.

COMMVAULT CLOUDPRODUKTE, DIE IHNEN BEI DER WIEDERHERSTELLUNG HELFEN:

- Cleanroom-Wiederherstellung für Wiederherstellungstests, Validierung und Forensik
- Bedrohungsscan zur Validierung, dass wiederhergestellte Dateien sauber und frei von Malware, Ransomware und Beschädigungen sind
- Cloud Rewind zur Wiederherstellung von Anwendungen über verschiedene Clouds hinweg, von Code bis Daten
- Active Directory-Wiederherstellung zur Sicherstellung der Identitätskontinuität auch bei einem Cyberangriff

COMMVAULT CLOUD PLATTFORM FÄHIGKEITEN:

- Cloudburst-Wiederherstellung für schnelle, cloudbasierte Wiederherstellung, die bei Bedarf verfügbar ist
- Cleanpoint-Validierung zur Bereitstellung eines bekannten sauberen Zeitpunkts für die Wiederherstellung

STEP #05

ÜBERWACHEN

Alle Ihre Planungen und Vorbereitungen sind nur dann effektiv, wenn Sie Ihre Umgebung so eingerichtet haben, dass sie Securityund IT-Teams auf Anomalien oder Ereignisse in Ihrer Infrastruktur aufmerksam machen.

Die Überwachung von Bedrohungen, die in Ihre Organisation eingedrungen sind und versuchen, unentdeckt zu bleiben, ist entscheidend, um den Schaden zu minimieren, den sie verursachen können. Je früher Sie von ihnen erfahren, desto schneller können Sie sie entfernen und betroffene Daten wiederherstellen. Die Herausforderung bei der Überwachung besteht darin, dass viele Cyber-Tools Hunderte oder Tausende von Warnungen auslösen, was zu viel Lärm durch falsch-positive Meldungen führt. Dies führt Sicherheitsoperationsteams auf Ermittlungspfade ins Nichts, verursacht Burnout und Alarmmüdigkeit – und nimmt Zeit von der Untersuchung echter Bedrohungen weg. Das Einstellen von Systemen, um nur bei echten Angriffen zu warnen, ist entscheidend, um Teams zu helfen, sich zu konzentrieren und echte Bedrohungen aufzusüren. Produktions- und Backup-Daten sollten kontinuierlich auf Änderungen, Anomalien und Malware überwacht werden, um Bedrohungen früher zu erkennen, das Risiko zusätzlicher Infektionen zu minimieren und auf bekannte saubere Daten zurückzugreifen. Dies umfasst auch die Möglichkeit, das Verhalten von Dateien zu betrachten, nicht nur den Inhalt, sodass Sie bisher unbekannte Angriffe erkennen können. Sie profitieren auch davon, alle Überwachungen in einer einzigen Plattform zu konsolidieren – in den meisten Fällen ein SIEM- oder SOAR-Tool, das kontinuierlich von Sicherheitsoperationsteams überwacht wird und zur Koordination von Untersuchungen und Reaktionen verwendet wird.

COMMVAULT CLOUD-PRODUKTE, DIE KONTINUIERLICHE ÜBERWACHUNG ERMÖGLICHEN:

- Threatwise™ zur Entdeckung von Angreifern, und Stellen von Fallen, die hochgenaue Warnungen bei einem Einbruch bieten
- Threat Scan zur kontinuierlichen Überprüfung von Backup-Daten und Dateien auf Malware
- Threat Scan Predict zur Entdeckung von zero-dayoder KI-gesteuerten polymorphen Angriffen

COMMVAULT CLOUD PLATTFORM FÄHIGKEITEN:

- Sicherheitsökosystem-Integrationen zur Erweiterung der Bedrohungsintelligenz durch Drittanbieter

ZUSAMMENFASSUNG

Zusammenfassend müssen Sie sich der Risiken bewusst sein, die Ihre Daten für Ihre Organisation darstellen.

01

Identifizieren Sie, was Sie für die Mindestviabilität benötigen – die kritischen Systeme, Anwendungen und Daten, die für den Betrieb Ihres Unternehmens erforderlich sind.

02

Investieren Sie in fortschrittliche Schutz-, Erkennungs- und Überwachungstools, um die Fähigkeit Ihrer Organisation zu verbessern, Cyberbedrohungen schnell zu erkennen und darauf zu reagieren.

03

Entwickeln und pflegen Sie einen aktuellen Notfallplan, der klare Rollen, Verantwortlichkeiten und Verfahren im Falle eines Verstoßes umreißt.

04

Führen Sie vollständige Tests durch, um sicherzustellen, dass Sie mehrere Szenarien abgedeckt haben und sich vollständig erholen können.

05

Überwachen Sie Ihre Systeme und Backups, damit Sie sicher sind, dass sie sauber und einsatzbereit sind, wenn sie benötigt werden.

Um zu sehen, wie Commvault Cloud bei der technologischen Komponente des Cyber-Readiness-Puzzles helfen kann, fordern Sie eine Demo und eine Beratung mit unseren Readiness- und Recovery-Experten an.