COHESITY

WHITEPAPER

Effiziente Recovery: Leitfaden für CISOs zum Einsatz von Backup-Daten für verbesserte Cyber-Resilienz

INHALTSVERZEICHNIS

Einleitung

Angesichts der zunehmenden Häufigkeit und Schwere von Cyberangriffen müssen Chief Information Security Officers (CISOs) ihren Fokus von der reinen Prävention auf die Resilienz gegenüber Cyberangriffen verlagern. Das bedeutet, dass Unternehmen sicherstellen müssen, dass sie Angriffen durch eine schnelle Reaktion standhalten, eine sichere Recovery bewerkstelligen und die Wiederholung ähnlicher Angriffe in Zukunft verhindern können.

Dieses Whitepaper hinterfragt traditionelle Vorstellungen von fortschrittlichen Backup-Systemen und positioniert sie als wichtige Komponenten einer Risikomanagementstrategie für Cybersicherheit. Es wird untersucht, wie moderne, sichere Backups nicht nur als Wiederherstellungstools, sondern als wertvolle Assets für die Bedrohungssuche, die frühzeitige Abwehr von Angreifern und die beschleunigte Reaktion auf Zwischenfälle zum Einsatz kommen können. Insbesondere bei Szenarien, in denen primäre Sicherheitsmaßnahmen umgangen oder isoliert werden, können Backups die entscheidende Transparenz und Kontrolle bieten, die zur Aufrechterhaltung der Betriebsintegrität erforderlich sind. Durch die Nutzung von umfangreichen historischen Informationen in Backup-Systemen können Unternehmen tiefere Einblicke in potenzielle Bedrohungen gewinnen, die Vorfallsreaktion und sichere Wiederherstellung beschleunigen sowie eine widerstandsfähigere Cybersicherheitspraxis aufbauen.

1. Verbessertes Threat Hunting

Die Bedrohungssuche (engl. Threat Hunting) ist eine proaktive Cybersicherheitsmaßnahme, bei der aktiv nach Hinweisen auf versteckte Bedrohungen im Netzwerk eines Unternehmens gesucht wird, um Angreifer so früh wie möglich in der Angriffskette zu stoppen. Herkömmliche Methoden zum Threat Hunting basieren häufig auf Endpunkt-Agenten und Systemprotokollen.

Nahezu alle RaaS-Plattformen (Ransomware as a Service) verfügen mittlerweile über eine gängige Umgehungstechnik: Bring Your Own Vulnerable Device Driver (BYOVD). Doch wie funktioniert sie? Bei diesem Ansatz setzen Angreifer einen signierten Gerätetreiber ein, der unterhalb der Betriebssystemebene ausgeführt wird, wodurch die Endpunktsicherheitslösung und die Protokollierung für Angriffe unwirksam werden. Hier werden Backup-Daten zu einem unschätzbaren Asset für das Threat Hunting.

Zu den wichtigsten Vorteilen von Backup-Daten für die Bedrohungssuche gehören:

- **Passives Threat Hunting**: Da Backup-Kopien von der primären Umgebung isoliert sind, können sie nicht manipuliert oder von Angreifern umgangen werden – insbesondere nicht von Ransomware-Banden, die Umgehungstechniken in ihre RaaS-Plattform einbetten, um gängige Sicherheitskontrollen wie Endpoint Detection and Response (EDR) und Extended Detection and Response (XDR) zu umgehen. Diese Isolation ermöglicht effektives und unauffälliges Threat Hunting.
- **Historischer Kontext**: Backup-Daten ermöglichen es Analysten, Systemzustände und Datenänderungen im Laufe der Zeit zu überprüfen und so subtile, langfristige Muster bösartiger Aktivitäten zu erkennen.
- **Umfassende Abdeckung**: Backups enthalten oft Daten aus dem gesamten Unternehmen und bieten einen holistischen Überblick, der Verbindungen zwischen scheinbar unabhängigen Ereignissen aufzeigen kann.
- **Offline-Analyse**: Bei der Bedrohungssuche können Backup-Daten offline analysiert werden. Dadurch wird das Risiko verringert, dass aktive Angreifer auf die Erkennungsmaßnahmen aufmerksam werden.
- **Wiederherstellung von gelöschten oder geänderten Daten**: Backups können Beweise aufdecken, die möglicherweise auf aktiven Systemen gelöscht oder geändert wurden, was für die Aufdeckung ausgeklügelter Angriffe entscheidend ist.

2. Einhaltung von Datenvorschriften

Mit dem Aufkommen von Sicherheitslösungen, die durch künstliche Intelligenz (KI) unterstützt werden, bilden Tools für das Data Security Posture Management (DSPM) zusammen mit Backup-Systemen ein leistungsstarkes Doppel. DSPM-Tools gehen über das Scannen von IT-Systemen, Netzwerken und Datenspeichern nach sensiblen Informationen wie Gesundheits- oder Finanzdaten hinaus. Durch sie kann auch in Erfahrung gebracht werden, wo sich diese Daten befinden, wie oft darauf zugegriffen wurde und von wem. In Verbindung mit fortschrittlichen Backup-Systemen können Compliance-Verantwortliche das Risiko einer Offenlegung sensibler Daten erheblich reduzieren.

Hier führen wir einige Vorteile auf, die sich aus der Integration Ihrer DSPM-Lösung in ein fortschrittliches Backup-System ergeben:

- **Schnelle Identifizierung von Systemen, die nicht gesichert sind**: DSPM-Lösungen erkennen und klassifizieren automatisch Daten-Assets in unterschiedlichen Umgebungen, einschließlich Schatten-Daten und vergessener Datenbanken. Einige dieser Daten sind wahrscheinlich bereits durch bestehende Backup-Richtlinien abgedeckt. Es ist jedoch auch möglich, dass erhebliche Mengen sensibler Daten nicht erfasst werden. In Verbindung mit fortschrittlichen Backup-Systemen über API-Integration können Sicherheitsteams Lücken in der Backup-Abdeckung leicht erkennen und dann Maßnahmen ergreifen, um diese Datenquellen in die Backup-Richtlinien Ihres Unternehmens aufzunehmen. Das Endergebnis: verbesserte Resilienz der Sicherheit und geringere Risiken.
- **Optimierte Häufigkeit von Backups und Aufbewahrungsfristen basierend auf der Kritikalität der Daten in den von Cohesity gesicherten Datenspeichern.**
- **Priorisierte Wiederherstellung von Daten basierend auf der geschäftlichen Kritikalität der Daten.**
- **„Just-in-Time"-Analyse datenbezogener Beweise für Zwischenfälle, wodurch der Prozess der Vorfallsreaktion optimiert wird (und somit die Reaktionszeiten bei Zwischenfällen verbessert werden)**. Gesicherte Kopien von Daten bieten eine reichhaltige Umgebung für DSPM-Aktivitäten, um zuvor „dunkle" Daten aufzudecken und zu schützen.
- **Verbesserte Einhaltung gesetzlicher Vorschriften wie DSGVO und SEC 8-K, die eine zeitnahe Benachrichtigung der Aufsichtsbehörden oder betroffenen Personen vorschreiben.**

3. Umfassende Vorfallsreaktion und Wiederherstellung

Eine solide Strategie für die Vorfallsreaktion und Wiederherstellung ist ausschlaggebend, um die Auswirkungen von Sicherheitsvorfällen auf ein Unternehmen zu minimieren. Sehen wir uns nun genauer an, wie die Verwendung von Backup-Daten die Reaktion auf Zwischenfälle verbessert und eine sichere Wiederherstellung gewährleistet.

Erkennung von Ransomware, Wiper-Angriffen und böswilligen Insidern

Ungewöhnliche Datenmuster und Benutzeraktivitäten bei Backup- und Wiederherstellungsvorgängen können frühzeitige Warnsignale für einen potenziellen Angriff sein. Diese Anomalien können Warnmeldungen auslösen, die die Triage und Untersuchung beschleunigen und Teams dabei unterstützen, schneller zu reagieren.

Reaktion auf Ransomware

Die für die Vorfallsreaktion verantwortlichen Mitarbeiter (Incident Responder) können unveränderliche Backup-Daten als Ressource mit einer starken Kontrollkette nutzen. Dadurch sind sie in der Lage, Dateisystemforensik durchzuführen, Artefakte aufzudecken und böswillige Änderungen an Konfigurationen und anderen Dateien zu identifizieren, die durch Ransomware- und Wiper-Angriffe verursacht wurden. Mithilfe eines fortschrittlichen Backup-Systems kann diese Analyse anhand einer Reihe von Snapshots durchgeführt werden, die über einen bestimmten Zeitraum hinweg gespeichert werden. Dies ermöglicht einen tieferen Einblick in den zeitlichen Ablauf des Angriffs.

Die Responder können auch passiv in Backup-Kopien in einer sicheren und isolierten Umgebung nach IOCs suchen, ohne dass sie dabei von Angreifern, die möglicherweise noch im Netzwerk aktiv sind, gestört oder gewarnt werden. Darüber hinaus können Backup-Daten historische Schwachstellen aufdecken, die während des Angriffs ausgenutzt wurden, und so wertvolle Informationen liefern, um die Angriffsfläche zu reduzieren und erneute Angriffe zu verhindern. Da die Ausnutzung von Schwachstellen mittlerweile die bevorzugte Methode von Ransomware-Betreibern für den ersten Zugriff ist und Exploits innerhalb weniger Tage in RaaS-Plattformen integriert werden, sind Sie ohne Patches vor der Wiederherstellung Ihrer Systeme nicht nur erneuten Angriffen des ursprünglichen Angreifers ausgesetzt, sondern auch Tausenden anderen Partnern, die die RaaS-Plattform nutzen.

Unveränderliche Backups sind Kopien von Daten, die nicht geändert oder gelöscht werden können. Diese Unveränderlichkeit stellt sicher, dass die Backup-Daten unangetastet bleiben und wiederhergestellt werden können, selbst wenn die Primärdaten durch Ransomware kompromittiert werden.

Eindämmung von Ransomware

Ransomware-Angriffe stellen eine wachsende Bedrohung für Unternehmen aller Größenordnungen dar. Im Fall eines solchen Angriffs können sichere und zuverlässige Backups den Unterschied zwischen einer geringfügigen Störung und einem katastrophalen Ereignis ausmachen. Auch wenn dies offensichtlich erscheinen mag, ist es aufgrund der Vielzahl von Unternehmen, die keine grundlegenden Sicherheitsmaßnahmen ergreifen, wichtig, diesen Punkt

erneut anzusprechen. Diese Vorkehrungen umfassen:

- **Unveränderliche Backups und Systemhärtung**: Unveränderliche Backup-Snapshots in Kombination mit WORM (Write Once, Read Many) und Zero Trust-basierten Prinzipien wie Zugriff mit geringsten Rechten, Multifaktor-Authentifizierung, Datenverschlüsselung und Aufgabentrennung verhindern, dass Ihre Backup-Daten zum Ziel von Angriffen werden.
- **Backups mit Air Gapping**: Air-Gapped-Backups sind physisch vom Netzwerk isoliert und bieten somit eine zusätzliche Sicherheitsebene. Selbst wenn das Netzwerk angegriffen wird, bleiben die Backups vor Ransomware-Angriffen geschützt.
- **Regelmäßige Backup-Zeitpläne**: Die Einführung regelmäßiger Backup-Zeitpläne gewährleistet, dass Daten ständig aktualisiert und geschützt werden. Je häufiger die Backups durchgeführt werden, desto geringer ist der Datenverlust, den das Unternehmen im Falle eines Angriffs erleiden wird.
- **Klon-Systeme**: Damit lassen sich Penetrationstests durchführen, ohne die Produktion zu beeinträchtigen.
- **Realistisches End-to-End-Training**: Gehen Sie über theoretische Übungen hinaus und führen Sie umfassende Simulationen durch, die eine durchgängige Prüfung und kontinuierliche Verbesserung von Mitarbeitern, Prozessen und Technologien ermöglichen. Durch das Klonen von Produktionssystemen und die Durchführung von Szenarien mit Verschlüsselung oder Zerstörung für das gesamte Team stellen Sie sicher, dass alle Aspekte der Reaktion und Wiederherstellung geprüft werden. Das bedeutet, dass Ihre Teams bereits Erfahrung haben, wenn Ihr Unternehmen zum ersten Mal mit einem destruktiven Cyberangriff konfrontiert wird.

Tests und Training

Regelmäßige Tests und Training sind unerlässlich, um zu gewährleisten, dass die Datensicherung und -wiederherstellung effektiv verläuft und alle Beteiligten mit ihren Aufgaben während eines Vorfalls vertraut sind.

- **Training zur Notfallwiederherstellung**: In regelmäßigen Disaster Recovery-Trainings werden reale Szenarien simuliert. Dies hilft dem Team, seine Reaktionsverfahren zu üben und zu verfeinern. Außerdem tragen solche Übungen dazu bei, potenzielle Schwachstellen und verbesserungswürdige Bereiche zu ermitteln.
- **Automatisierte Tests**: Durch automatisierte Tests von Backup-Daten kann die Integrität und Wiederherstellbarkeit von Backups ohne manuelle Eingriffe überprüft werden. Diese Automatisierung sorgt dafür, dass die Backups zuverlässig sind und bei Bedarf schnell wiederhergestellt werden können.
- **Dokumentation und Ablaufpläne**: Detaillierte Dokumentation und Recovery-Ablaufpläne stellen sicher, dass jeder seine Aufgaben kennt und weiß, welche Schritte bei einem Vorfall zu unternehmen sind. Diese Playbooks sollten regelmäßig auf der Grundlage der Ergebnisse von Tests und Trainings aktualisiert werden.

Detaillierte Überwachung und genaues Reporting

Eine effektive Reaktion auf Vorfälle und eine wirksame Wiederherstellung erfordern eine detaillierte Überwachung und genaues Reporting, um zu bestätigen, dass die Backup-Vorgänge reibungslos verlaufen und alle Probleme umgehend behoben werden.

- **Echtzeitüberwachung**: Die Echtzeitüberwachung von Backup-Prozessen stellt sicher, dass etwaige Fehler oder Probleme sofort erkannt und behoben werden, um einen möglichen Datenverlust zu verhindern.
- **Automatisierte Warnungen**: Automatisierte Warnungen benachrichtigen das IT-Team bei Unregelmäßigkeiten oder Fehlern im Backup-Prozess und ermöglichen ein schnelles Eingreifen und eine Korrektur.
- **Umfassendes Reporting**: Detaillierte Berichte über Backup-Status, Erfolgsraten und Wiederherstellungszeiten geben Aufschluss über die Effektivität der Backup-Strategie und zeigen Bereiche mit Verbesserungspotenzial auf. Durch die Implementierung dieser erweiterten Backup-Strategien können CISOs sicherstellen, dass ihre Unternehmen gut vorbereitet sind, um schnell und effektiv auf Vorfälle zu reagieren und die betroffenen Daten wiederherzustellen. Dieser umfassende Ansatz minimiert nicht nur Ausfallzeiten und Datenverluste, sondern stärkt auch die allgemeine Resilienz des Unternehmens gegenüber künftigen Bedrohungen.

4. Datenintegrität und Compliance

Die Aufrechterhaltung der Datenintegrität und die Einhaltung gesetzlicher Vorschriften ist für jedes Unternehmen von entscheidender Bedeutung, insbesondere im Bereich der Cybersicherheit. Backup-Daten spielen hierbei eine zentrale Rolle, da sie eine zuverlässige, überprüfbare Single Source of Truth (SSOT) bieten, die zur Überprüfung, Verifizierung und Wiederherstellung der Datenintegrität nutzbar ist. Im Folgenden erfahren Sie detailliert, wie Backup-Daten mehr Datenintegrität und die Einhaltung gesetzlicher Vorschriften ermöglichen können.

Einhaltung gesetzlicher Vorschriften

Unternehmen unterliegen zahlreichen regulatorischen Vorschriften, die strenge Anforderungen an den Datenschutz und die Datenintegrität stellen. Backup-Daten helfen dabei, die Einhaltung dieser Vorschriften zu erreichen und nachzuweisen, indem sie einen Audit-Pfad bieten und die Datenhaltung fördern.

- **Audit-Pfade**: Backup-Lösungen können umfassende Protokolle aller Datensicherungs- und Wiederherstellungsaktivitäten führen. Diese Protokolle sind von unschätzbarem Wert bei Compliance-Audits, da sie detaillierte Aufzeichnungen darüber liefern, wer zu welchem Zeitpunkt auf die Daten zugegriffen hat und welche Maßnahmen ergriffen wurden.
- **Daten-Aufbewahrungsrichtlinien**: Die Einhaltung regulatorischer Vorschriften (wie DSGVO, HIPAA oder SOX) erfordert häufig die Umsetzung strenger Richtlinien für die Datenhaltung. Automatisierte Backup-Lösungen können diese Richtlinien durchsetzen, indem sie sicherstellen, dass die Daten für die erforderliche Dauer aufbewahrt und sicher gelöscht werden, wenn sie nicht mehr benötigt werden.

Sichere Datenspeicherung und Zugriffskontrolle

Der Schutz von Backup-Daten vor unbefugtem Zugriff und ihre sichere Speicherung sind grundlegende Aspekte der Datenintegrität und der Einhaltung gesetzlicher Vorschriften.

- **Verschlüsselung**: Die Verschlüsselung von Backup-Daten sowohl im Ruhezustand als auch bei der Übertragung schützt sie vor unbefugtem Zugriff. Starke Verschlüsselungsprotokolle gewährleisten den Schutz vertraulicher Informationen und machen sie für jeden unlesbar, der nicht über die entsprechenden Entschlüsselungsschlüssel verfügt.
- **Rollenbasierte Zugriffskontrolle (RBAC)**: Durch die Implementierung von RBAC kann sichergestellt werden, dass nur befugtes Personal Zugriff auf die Backup-Daten hat. Anhand dieser Kontrolle wird die Gefährdung begrenzt und das Risiko von Datenschutzverletzungen oder Datenmissbrauch verringert.
- **Multifaktor-Authentifizierung (MFA)**: Die Erzwingung von MFA für den Zugriff auf Backup-Systeme stellt eine zusätzliche Sicherheitsebene dar, sodass selbst im Falle einer Kompromittierung der Anmeldedaten ein unbefugter Zugriff verhindert wird.

Geschäftskontinuität und Disaster Recovery

Eine wirksame Planung der Notfallwiederherstellung und Geschäftskontinuität ist ein wesentlicher Bestandteil einer umfassenden Compliance-Strategie. Mithilfe von Backup-Daten können sich Unternehmen schnell von Unterbrechungen erholen und den Betrieb mit minimalen Auswirkungen fortsetzen.

- **Analyse der Auswirkungen auf das Unternehmen (Business Impact Analysis, BIA)**: Die Durchführung einer BIA hilft Unternehmen, die potenziellen Auswirkungen von Datenverlusten oder -beschädigungen auf ihren Geschäftsbetrieb zu verstehen. Backup-Daten spielen bei dieser Analyse eine wichtige Rolle, da sie ein zuverlässiges Mittel zur Wiederherstellung kritischer Systeme und Daten sind.
- **Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO)**: Mit klaren RTO- und RPO-Vorgaben können Unternehmen Daten innerhalb eines akzeptablen Zeitrahmens und mit minimalem Datenverlust wiederherstellen. Backup-Lösungen müssen so konzipiert sein, dass sie diese Ziele erfüllen.
- **Kontinuitätsplanung**: Backup-Daten sind ein wesentlicher Bestandteil der Kontinuitätsplanung, damit Unternehmen ihren Geschäftsbetrieb während und nach einem Notfall aufrechterhalten können. Regelmäßige Tests von Notfallwiederherstellungsplänen anhand von Backup-Daten führen zu effektiveren und zuverlässigeren Recovery-Prozessen.

Datenintegrität und Compliance sind entscheidend für die Aufrechterhaltung des Vertrauens und der betrieblichen Zuverlässigkeit im komplexen regulatorischen Umfeld von heute. Durch die effektive Nutzung von Backup-Daten können Unternehmen die regulatorischen Anforderungen erfüllen, die Integrität ihrer Daten schützen und robuste Sicherheitsmaßnahmen aufrechterhalten. Mit der Implementierung erweiterter Datensicherungslösungen, die umfassende Audit-Pfade liefern, Datenhaltungsrichtlinien durchsetzen und sichere Speicher- und Zugriffskontrollen bieten, können Unternehmen diese Ziele erreichen und so eine solide Grundlage für kontinuierliches Wachstum und Resilienz schaffen.

5. Verbesserte Transparenz und Kontrolle

Für einen Chief Information Security Officer (CISO) sind eine höhere Transparenz und eine erweiterte Kontrolle über die Daten und Backup-Prozesse eines Unternehmens ausschlaggebend, um robuste Sicherheit und effizientes Datenmanagement zu gewährleisten. Durch den Einsatz erweiterter Datensicherungslösungen können CISOs umfassende Einblicke in ihre Datenumgebung gewinnen, Managementprozesse rationalisieren und wichtige Informationen besser schützen. Im Folgenden wird erörtert, wie die effektive Nutzung von Backup-Daten sowohl die Transparenz als auch die Kontrolle verbessert.

Zentralisiertes Management

Ein zentralisierter Managementansatz konsolidiert alle Backup-Aktivitäten und bietet so eine zentrale Kontrollstelle zur Backup-Überwachung über das gesamte Unternehmen hinweg. Diese Zentralisierung vereinfacht den Managementprozess und gewährleistet einen einheitlichen Datenschutzansatz.

- **Vereinheitlichtes Dashboard**: Ein vereinheitlichtes Dashboard bietet einen ganzheitlichen Überblick über die gesamte Backup-Umgebung, einschließlich des Status von Backup-Aufträgen, der Speichernutzung und möglicher Probleme. Diese Echtzeit-Transparenz ermöglicht es CISOs, den Zustand und die Leistung von Backups effektiv zu überwachen.
- **Vereinfachtes Management**: Zentralisierte Managementtools vereinfachen die Verwaltung mehrerer Backup-Systeme und -Standorte. Das vereinfachte Management ermöglicht operative Effizienz und verringert das Risiko von falschen Konfigurationen oder Fehlern.
- **Durchsetzung von Richtlinien**: Die zentrale Kontrolle sichert eine einheitliche Durchsetzung von Datenschutzrichtlinien im gesamten Unternehmen. Richtlinien für die Datenhaltung, Verschlüsselung und Zugriffskontrollen können einheitlich angewendet werden und so die Einhaltung von Vorschriften und die Sicherheit verbessern.

Umfassende Berichte und Analytik

Detailliertes Reporting und umfassende Analytik liefern wertvolle Einblicke in die Backup-Prozesse. Sie helfen CISOs, fundierte Entscheidungen zu treffen und ihre Datenschutzstrategien zu optimieren.

- **Audit-Protokolle**: Ausführliche Audit-Protokolle verfolgen alle Zugriffe und Aktivitäten im Zusammenhang mit den Backup-Daten. Aus diesen Protokollen geht klar hervor, wer auf die Daten zugegriffen hat, welche Maßnahmen ergriffen wurden und wann sie stattgefunden haben. Dies ist sowohl bei der Sicherheitsüberwachung als auch bei Compliance-Audits hilfreich.
- **Anpassbare Berichte**: Anpassbare Reporting-Tools ermöglichen es CISOs, Berichte zu erstellen, die auf spezifische Anforderungen zugeschnitten sind, wie z. B. in Bezug auf die Compliance, die betriebliche Leistung oder Sicherheitsaudits. Diese Berichte bieten einen klaren und umfassenden Überblick über die Backup-Aktivitäten.
- **Trendanalyse**: Mithilfe der Analyse von Trends bei Backup-Daten, z. B. Datenwachstumsmuster, Speichernutzung und Wiederherstellungszeiten, lassen sich langfristige Trends und potenzielle Problembereiche erkennen. Diese Analyse unterstützt die strategische Planung und die Zuweisung von Ressourcen.
- **Datenbasierte Einblicke**: Erweiterte Analytiktools können detailliertere Einblicke in die Backup-Daten geben. So lässt sich beispielsweise feststellen, welche Systeme oder Abteilungen die meisten Daten generieren, welche Daten am kritischsten sind und welche potenziellen Schwachstellen es gibt. Diese Erkenntnisse ermöglichen gezieltere und wirksamere Datenschutzmaßnahmen.

Durch den Einsatz erweiterter Datensicherungslösungen, die ein zentralisiertes Management, verbesserte Zugriffskontrolle, Echtzeitüberwachung, umfassendes Reporting und Automatisierung umfassen, können CISOs sicherstellen, dass die Daten ihres Unternehmens geschützt sind, den Vorschriften entsprechen und für die Wiederherstellung sofort zur Verfügung stehen. Diese Fähigkeiten stärken nicht nur die allgemeine Sicherheitslage, sondern bieten auch den nötigen Einblick und die Kontrolle, um Datensicherungsstrategien zu optimieren und den langfristigen Erfolg des Unternehmens zu unterstützen.

6. Strategische Erkenntnisse und Entscheidungsfindung

Im Bereich der Cybersicherheit ist eine strategische Entscheidungsfindung für das effektive Management von Ressourcen, die Antizipation künftiger Herausforderungen und die Aufrechterhaltung einer soliden Sicherheitslage unerlässlich. Backup-Daten, die oft nicht ausreichend genutzt werden, können wertvolle Einblicke liefern, die eine fundierte Entscheidungsfindung ermöglichen und die allgemeine Sicherheitsstrategie eines Unternehmens unterstützen. In den vorangegangenen Abschnitten haben wir Bereiche erörtert, in denen ein historischer Kontext eine Trendanalyse ermöglicht, um Bedrohungen aufzuspüren oder einen Einblick in das Grundverhalten für die Datennutzung zu erhalten. Dieser Abschnitt geht näher darauf ein, wie Backup-Daten dabei helfen können, strategische Einblicke in den Zustand des Unternehmens zu gewinnen.

Optimierte Ressourcenzuordnung

Eine effiziente Ressourcenzuordnung ist entscheidend für die Maximierung der Wirksamkeit von Sicherheitsinvestitionen. Backup-Daten bieten detaillierte Einblicke in die kritischsten Systeme und Daten, sodass Unternehmen ihre Sicherheitsanstrengungen nach Prioritäten ordnen und Ressourcen dort einsetzen können, wo sie am dringendsten benötigt werden.

- **Identifizierung kritischer Daten**: Mithilfe von Backup-Daten lässt sich feststellen, welche Daten und Systeme für den Geschäftsbetrieb wichtig sind. Durch das Verständnis der Kritikalität verschiedener Datensätze können Unternehmen Prioritäten bei der Datensicherung und Recovery setzen.
- **Kostenmanagement**: Die Analyse der Speicher- und Nutzungsmuster von Backup-Daten kann Möglichkeiten zur Kosteneinsparung aufzeigen. Dadurch können Unternehmen ihre Speicherlösungen optimieren, redundante Daten beseitigen und ihre Speicherkosten insgesamt senken, während sie gleichzeitig ihre Daten schützen.
- **Priorisierung von Ressourcen**: Einblicke in Backup-Daten ermöglichen es Unternehmen, ihre Ressourcen auf die anfälligsten oder wertvollsten Bereiche zu konzentrieren. Bei diesem zielgerichteten Ansatz erhalten die kritischsten Datenbestände das höchste Schutzniveau.

Strategische Geschäftseinblicke

Neben den Sicherheits- und Compliance-Aspekten können Backup-Daten auch strategische Geschäftseinblicke liefern, die weiter gefasste Unternehmensziele unterstützen.

- **Betriebliche Effizienz**: Die Analyse von Backup-Daten kann Ineffizienzen beim Datenmanagement und den betrieblichen Abläufen aufdecken. Unternehmen können diese Erkenntnisse nutzen, um Abläufe zu rationalisieren, Redundanzen zu verringern und die Gesamteffizienz zu verbessern.
- **Datennutzung**: Das Verständnis der Datennutzung innerhalb des gesamten Unternehmens hilft dabei, entsprechende Optimierungsmöglichkeiten zu finden und das Datenmanagement effektiver zu gestalten. Die Erkenntnisse aus den Backup-Daten können als Grundlage für Entscheidungen über die Datenarchivierung, das Lifecycle-Management und die Zugriffsrichtlinien dienen.
- **Innovation und Wachstum**: Dank Backup-Daten können Trends und Muster ermittelt werden, die Innovation und Unternehmenswachstum fördern. Mithilfe von Verlaufsanalysen sind Unternehmen in der Lage, neue Möglichkeiten zu erkennen, Prozesse zu optimieren und strategische Initiativen voranzutreiben.

Die Nutzung von Backup-Daten für strategische Einblicke und Entscheidungen verbessert die Fähigkeit eines Unternehmens, Ressourcen effektiv zu verwalten, Bedrohungen vorherzusehen und auf sie zu reagieren sowie gesetzliche Bestimmungen einzuhalten. Durch die Integration von Backup-Daten in breiter gefasste Betriebsstrategien können CISOs kontinuierliche Verbesserungen vorantreiben, die Ressourcenzuordnung optimieren und den langfristigen Erfolg des Unternehmens unterstützen. Erweiterte Datensicherungslösungen, die robuste Analytik-, Reporting- und Automatisierungsfunktionen bieten, helfen Unternehmen, das volle Potenzial ihrer Daten zu erschließen und sie in ein wertvolles Wirtschaftsgut für die strategische Planung und Entscheidungsfindung zu verwandeln.

Fazit

Weltweit stehen CISOs vor der großen Herausforderung, die Daten ihrer Unternehmen vor raffinierten Bedrohungen zu schützen und gleichzeitig strenge Vorschriften einzuhalten. Erstklassige Backup-Lösungen bieten weit mehr als nur Unterstützung bei der Notfallwiederherstellung – sie reduzieren Risiken in Bezug auf Compliance und Sicherheit. Heutzutage sind sie ein unverzichtbarer Bestandteil einer hochwertigen Cyberversicherung.

Fortschrittliche Backup-Systeme sind ein wesentlicher Bestandteil einer „tiefgreifenden Verteidigung“ und faktisch die letzte Verteidigungslinie bei einem Cyber-Zwischenfall. Die effiziente und sichere Übertragung großer Mengen sensibler Daten in kostengünstige Speicherlösungen, sei es in der Cloud oder lokal, sowie die Gewährleistung von Recovery Time Objectives verringern das Risiko von Datenverlusten, Betriebsausfällen und Reputationsschäden. Durch die Optimierung und Nutzung dieser Technologie können CISOs die Resilienz, Agilität und den langfristigen Geschäftswert in einer zunehmend komplexen digitalen Welt stärken.

Erfahren Sie mehr unter Cohesity.com

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

2000053-002-DE 4-2025