Ransomware-Prävention
CHECKLISTE

Unternehmen, die bei der Abwehr von Ransomware-Angriffen am erfolgreichsten sind, treffen insbesondere **fünf wichtige Schutzmaßnahmen, die auch Sie ergreifen sollten:**

1 | Schutz von Backup-Daten und -Systemen

- ☐ Planen Sie regelmäßige Backups, die Ihren Geschäfts- und Compliance-Anforderungen entsprechen und als Schutzrichtlinien automatisiert sind.
- ☐ Sichern Sie Ihre Workloads kontinuierlich, auch nach dem Ausfall einer Hardware- oder Softwarekomponente.
- ☐ Patchen Sie die Software regelmäßig und scannen Sie bestehende Systeme, um Schwachstellen zu verringern.
- ☐ Verschaffen Sie sich einen Überblick über Sicherheitslücken in Systemkonfigurationen und operativen Konzepten.
- ☐ Schaffen Sie ein Gleichgewicht zwischen mehr Sicherheit und schnelleren RTOs/RPOs, um Ihre SLAs im digitalen Geschäftsbetrieb zu erfüllen.
- ☐ Investieren Sie in eine bewährte und robuste Datensicherheits- und -managementlösung, die Ihre Informationen nachweislich vor Ransomware-Angriffen schützt.

WICHTIGE FUNKTIONEN:

Unveränderliche Snapshots

WORM

Datenverschlüsselung

Konfigurationsaudit und Scans

Fehlertoleranz

Moderne und flexible Datenisolation

2 | Verringern des Risikos unbefugter Zugriffe

- ☐ Informieren Sie Ihre Mitarbeiter über die Gefahren von Phishing-Angriffen und kompromittierten Anmeldedaten.
- ☐ Setzen Sie die Zero-Trust-Prinzipien, einschließlich Least Privilege und MFA, in Ihrer Datensicherheits- und -managementlösung durch.
- ☐ Richten Sie eine Multibenutzergenehmigung für kritische Vorgänge und Änderungen ein.
- ☐ Informieren Sie sich über verfügbare und neue Backup-Funktionen, die den unbefugten Zugriff auf Unternehmensdaten verhindern und sowohl vor Ransomware als auch vor Insider-Bedrohungen schützen.

WICHTIGE FUNKTIONEN:

Multifaktor-Authentifizierung (MFA)

Überwachte Veränderung

Granulare, rollenbasierte Zugriffskontrolle (RBAC)

COHESITY

3 | Erkennen und Aufspüren von Angriffen, um Übergriffe zu stoppen

- ☐ Klassifizieren Sie Daten und identifizieren Sie sensible Informationen, die möglicherweise gefährdet sind.
- ☐ Verschaffen Sie sich einen tiefgreifenden Einblick in Daten und Anwendungen, um Software- und Cyber-Schwachstellen zu identifizieren.
- ☐ Integrieren Sie KI/ML, um Anomalien zu erkennen, die auf eine Bedrohung oder einen Ransomware-Angriff hindeuten können.
- ☐ Erkennen Sie Kompromittierungsindikatoren (Indicators of Compromise, IOCs), indem Sie Backup-Daten routinemäßig auf Bedrohungen überprüfen.

WICHTIGE FUNKTIONEN:

KI/ML-gestützt

Anomalieerkennung nahezu in Echtzeit

Automatisierte Warnmeldungen

Ermittlung von Cyber-Schwachstellen

4 | Verbessern der Sicherheitslage mit erweiterbarer Plattform

- ☐ Stellen Sie sicher, dass Ihre vorhandene Backup- oder Datenmanagement-Lösung Sicherheitsintegrationen unterstützt, insbesondere für SOC-Lösungen, damit Ransomware schneller erkannt und behoben werden kann.
- ☐ Verbessern Sie die Zusammenarbeit, indem Sie Silos zwischen Menschen, Prozessen und der Datenplattform aufbrechen.
- ☐ Informieren Sie sich über die APIs der führenden Sicherheitsprodukte und -plattformen.
- ☐ Sorgen Sie für nahtlose Backup-Workflows, um Erkenntnisse zu gewinnen und gleichzeitig Ihre Daten zu schützen.

WICHTIGE FUNKTIONEN:

Vorgefertigte Integrationen

Anpassbare Integrationen

Interoperabilität mit wertsteigernden Anwendungen

5 | Gewährleistung einer schnellen Datenwiederherstellung in großem Maßstab

- ☐ Bestimmen Sie, ob Ihre vorhandene Backup- oder Datenmanagement-Lösung Daten schnell, sauber, vorhersehbar und skalierbar wiederherstellen kann.
- ☐ Berücksichtigen Sie länderspezifische Anforderungen an Datenschutz und Souveränität.
- ☐ Bewerten Sie die Fähigkeiten zur Unterstützung einer schnellen Wiederherstellung zu jedem Zeitpunkt und an jedem Ort.
- ☐ Verschaffen Sie sich einen Überblick über den Zustand eines Snapshots und stellen Sie unstrukturierte Daten ohne zusätzliche Investitionen wieder her.
- ☐ Ermitteln Sie, wie Sie unstrukturierte Daten vor Ort wiederherstellen können, um Ausfallzeiten zu reduzieren.

WICHTIGE FUNKTIONEN:

Sofortige, skalierbare Wiederherstellung

Saubere Wiederherstellung

Wiederherstellung vor Ort

Den vollständigen Leitfaden zur Ransomware-Bereitschaft herunterladen

COHESITY

© 2023 Cohesity, Inc. Alle Rechte vorbehalten.

Cohesity, das Cohesity Logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, das Helios Logo, DataGovern, SiteContinuity und andere Cohesity Marken sind Warenzeichen oder eingetragene Warenzeichen von Cohesity, Inc. in den USA und/oder international. Andere Unternehmens- oder Produktnamen können Warenzeichen der jeweiligen Unternehmen sein, mit denen sie verbunden sind. Dieses Material (a) soll Ihnen Informationen über Cohesity und unser Geschäft und unsere Produkte liefern, (b) wurde zum Zeitpunkt der Erstellung für wahrheitsgemäß und korrekt gehalten, unterliegt aber Änderungen ohne vorherige Ankündigung und (c) wird ohne Gewähr zur Verfügung gestellt. Cohesity lehnt alle ausdrücklichen oder impliziten Bedingungen, Zusagen und Gewährleistungen jeglicher Art ab.

Cohesity.com/de/ | 1-855-926-4374 | 300 Park Ave., Suite 1700, San Jose, CA 95110

9100074-002-DE 7-2023