rubrik

Langs Building Supplies stoppt Ransomware Angriff mit Backup-Lösung der nächsten Generation

ERGEBNISSE

- 25 Minuten zum Schreiben eines Scripts zur Dateiwiederherstellung auf der VM vom letzten Snapshot
- 1 Stunde bis zur Beseitigung der Gefahr und Betriebsaufnahme
- kein Datenverlust

DIE HERAUSFORDERUNG

- Ransomware-Angriff auf das System über E-Mail-Link
- ein Produktionsdateiserver infiziert mit CryptoLocker
- 15.000 verschlüsselte Dateien

DIE LÖSUNG

- API-First-Architektur
- globale Dateisuche in Echtzeit
- konvergentes Datenmanagement für Backup und Wiederherstellung

„Mit einer erstklassigen Datenmanagementlösung kann ich meine tägliche Arbeit verrichten, ohne mir Gedanken über Datenverlust zu machen. Ich weiß, dass wir gut vorbereitet sind“, so Matthew Day, ICT und Support Manager bei Langs Building Supplies, einem führenden Hersteller und Lieferanten von Gütern für die Bauindustrie mit Standort in Stapylton, Queensland, Australien. Das Unternehmen war kürzlich von einem Ransomware-Angriff betroffen. Aufgrund der effektiven Backup-Struktur konnte das Unternehmen die Gefahr abwenden und die Daten ohne Bezahlung von Lösegeld wiederherstellen.

DIE ZUNEHMENDE RANSOMWARE-BEDROHUNG

Ransomware ist eine spezielle Art der Malware, bei der der Angreifer die Daten des Benutzers „gefangenhält“, bis ein Lösegeld gezahlt wird. Viele Formen der Ransomware verwenden eine starke Kryptographie zum Verschlüsseln der Daten des Opfers und nur der Angreifer kennt den Entschlüsselungscode. Nach einer angegebenen Zeit löscht der Angreifer den Entschlüsselungscode und die Daten des Opfers sind für immer verloren. Selbst wenn das Opfer den Angreifer vor der Frist bezahlt, kann der Angreifer dem Opfer den erforderlichen Entschlüsselungscode bereitstellen oder auch nicht. Ransomware-Angriffe nehmen exponentiell zu. Es wurden durchschnittlich 4.000 Ransomware-Angriffe pro Tag seit dem 1. Januar gemeldet. Eine Zunahme von 300 Prozent im Vergleich zu den 1.000 Angriffen pro Tag in 2015.[1] Die üblichen Opfer stammen aus Branchen, in denen der Zugriff auf einen Computer für kritische Aktivitäten erforderlich ist. In der Regel sind nicht überall moderne Technologien vorhanden und das Lösegeld wird gezahlt, um wieder Zugriff auf die Daten zu erhalten. In der Vergangenheit gab es keine effektive Möglichkeit, diese Angriffe zu umgehen, und die Häufigkeit der Ransomware-Angriffsversuche nimmt zu.

PRAXISFALL: LANGS BUILDING SUPPLIES

Anfang Juni wurde ein Produktionsdateiserver bei Langs Building Supplies durch CryptoLocker über einen E-Mail-Link infiziert, den ein Mitarbeiter angeklickt hatte. Das IT-Team wurde innerhalb von 10 Minuten vom Überwachungs-Tool, das hohe Änderungsraten in den Datenstrukturen überwacht, über den Angriff benachrichtigt. So wurde nur an 15.000 von Millionen Dateien die Endung .encrypted hinzugefügt. Die Dateiendung verhindert den Dateizugriff ohne Kennwort des Angreifers.

RANSOMWARE-ANGRIFF DANK DATENMANAGEMENTLÖSUNG DER NÄCHSTEN GENERATION VERHINDERT

Nach Empfang einer Warnmeldung vom Überwachungssystem konnte Day den betroffenen VDI-Desktop isolieren und verhindern, dass sich der Angriff auf die restliche Infrastruktur der Firma ausweitete. „Dank unseres Backups konnten wir einen Script schreiben, um unsere Dateien anhand der letzten Dateiversion auf der VM wiederherzustellen. In etwa einer Stunde waren alle Dateien wieder auf dem Dateiserver. Ohne jeglichen Schaden“, so Day.

[1] Quelle: Symantec Internet Security Threat Report, 2016

Es gab ein paar Aspekte bei der Datenmanagementlösung von Lang Building Supplies, die es ermöglicht haben, einen potenziellen Schadensfall zu entschärfen:

1. **Moderne Technologie:** „Moderne Technologie bedeutet nicht unbedingt weniger manuellen Aufwand, sondern dass sie bei Bedarf so funktioniert, wie sie soll. Unsere konvergente Backup-Appliance hilft wirklich, unsere Daten zu verwalten. Sie kann unsere VMs mit Leichtigkeit verwalten und schützen, unsere Schutzrichtlinien so allgemein oder detailliert festlegen wie gewollt und in unseren geschützten Daten nach bestimmten VMs, Objekten oder bestimmten Dateien suchen, die wiederhergestellt werden sollen."

2. **Programmierbare Schnittstelle und API-basiert:** „Beim üblichen Anwendungsfall ist es einfach, ab und zu eine Datei über die Benutzeroberfläche zu finden, das Finden von Tausenden von Dateien wäre jedoch zeitaufwendig gewesen. Da wir über eine programmierbare Schnittstelle verfügen, die angepasste Workflows für Drittanbieter ermöglicht, kann das Management unserer Umgebung noch weiter automatisiert und orchestriert werden. Da Rubrik über RESTful APIs verfügt, konnten wir einen Script zur Suche nach unseren betroffenen Dateien und zu ihrer Wiederherstellung schreiben und mussten so keinen aufwendigen manuellen Such- und Wiederherstellungsprozess durchlaufen.

3. **Inkrementeller Ansatz:** „Wir können öfter Snapshots erstellen, da weniger Daten auf unseren Backup-Speicherort verschoben werden müssen – zu jederzeit und mit einem inkrementellen Ansatz. Dies hat es uns ermöglicht, den genauen Zeitpunkt zu ermitteln, zu dem unsere Dateien umbenannt wurden, und die Dateien vom Zeitpunkt kurz vor dem Angriff wiederherzustellen."

4. **Schnelle Wiederherstellung:** VMs und Anwendungen können durch direktes Mounten in Rubrik schnell wiederhergestellt werden. Day sagte: „In einer Stunde waren unsere Produktionsserver normalisiert und in Betrieb."

„Da wir mit Rubrik arbeiten, waren keine längerfristigen finanziellen Schäden möglich. Wir verfügen über Systeme, die diese Eventualitäten abdecken. Schulungen der Endnutzer und Gruppenrichtlinien allein reichen nicht aus. Es sind auch getrennte Backups nötig, die von einem System verwaltet werden, das absolut unabhängig von der Produktionsumgebung ist, damit kein Angriff Auswirkungen darauf hat. Hier kommt Rubrik ins Spiel", so Day.

Die beste Möglichkeit Ransomware-Angriffe abzuschwächen, ist ein tief greifender Schutzmechanismus, bei dem Sicherheit mit Datenschutz integriert wird. Day erklärte: „Schwachstellen wird es immer geben. Deshalb ist ein hundertprozentig zuverlässiges Datenmanagement erforderlich. Man muss immer weitermachen und nicht zurückblicken. Da wir uns auf diese Fehler vorbereiten, konnte diese Bedrohung auf ein kleines Ärgernis reduziert werden. Am nächsten Tag war es, als ob nie etwas passiert wäre."

LANGS BUILDING SUPPLIES

„Mit einer erstklassigen Datenmanagementlösung kann ich meine tägliche Arbeit verrichten, ohne mir Gedanken über Datenverlust zu machen. Ich weiß, dass wir gut vorbereitet sind,"

so Matthew Day, ICT Manager bei Langs Building Supplies

rubrik

Hauptsitz
299 South California Ave. #250
Palo Alto, CA 94306
USA

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

Rubrik stellt die branchenführende Cloud-Datenmanagement-Plattform zur Verfügung, und beschleunigt die Art und Weise, wie Unternehmen überall Daten schützen, verwalten und sichern. Fortune 500-Unternehmen setzen auf die Single-Plattform von Rubrik, denn sie verfügt über Funktionen für Datenschutz, Suche und Analysen, Archivierung und Compliance sowie Copy Data Management für sofortigen Datenzugriff. Außerdem können die Gesamtbetriebskosten halbiert und der tägliche Verwaltungsaufwand auf Minuten reduziert werden.