netzlink

Gold Business Partner IBM

IBM Spectrum Sentinel für SAP HANA:

Schnelles Recovery nach einem Cyberangriff

Die Bedrohung im Cyber-Raum ist so hoch wie nie: Zu diesem Ergebnis kommt der aktuelle Lagebericht 2022 des Bundesamts für Sicherheit in der Informationstechnik. Ransomware ist dabei die Hauptbedrohung, besonders für Unternehmen und die öffentliche Verwaltung. Allein in Deutschland verursachten Ransomware Attacken– laut dem TV-Magazin WISO – im letzten Jahr einen Schaden von 24 Milliarden Euro.

Bisherige Policys reichen nicht aus

Ein alarmierender Trend ist, dass viele Organisationen eine „30-60-90"-Policy für Ihr Daten-Backup einsetzen. Snap-Shots werden alle paar Stunden erzeugt und komplette Backups alle 30, 60 und 90 Tage. Die Antwort der Hacker: Sie installieren Malware und lassen sie 100 Tage lang oder länger inaktiv, bevor die Falle zuschnappt. Dann hat der böswillige Code nicht nur die Produktionsdaten, die Systeme und Snap-Shots infiziert, sondern auch jede einzelne Backup-Kopie. Oft bleibt dann nur die erpresserische Bezahlung.

Sollten Kunden die Daten in einer Cloud sichern, hilft das auch nicht weiter. Denn Hacker trennen inzwischen gezielt die Cloud-Verbindungen, weil sie wissen, dass Kunden versuchen, Daten in der Cloud als Backup zu speichern. Diese „Hintertür" bleibt damit auch verschlossen.

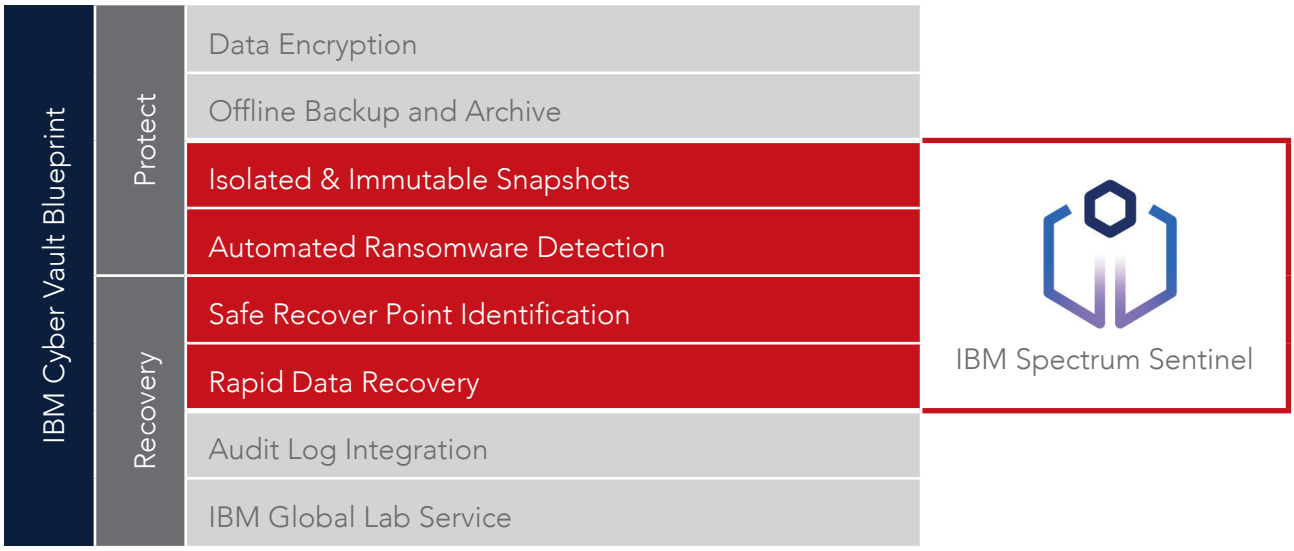
Die Antwort heißt automatisiertes, schnelles Recovery

IBM Spectrum Sentinel stellt die Daten nach einem Cyberangriff mit nachweislich sauberen Kopien wieder her. Die Recovery-Lösung bietet einen End-to-End-Cyber-Resiliency-Workflow mit automatisierter Anomalie- und Ransomware-Erkennung. **Sie ist für die IBM FlashSystem-Familie und für den IBM San Volume Controller SVC verfügbar.**

IBM Spectrum Sentinel basiert auf dem IBM Cyber Vault-Blueprint. Dieses Framework beinhaltet Maßnahmen und Aktionen einerseits zum Schutz der Daten und andererseits für eine Wiederherstellung der Primärdaten. Ziel ist es, nach einem Angriff möglichst schnell wieder produktiv zu sein. Die wichtigsten Maßnahmen von Protect und Recover sind in der folgenden Grafik dargestellt:

IBM Spectrum Sentinel für SAP HANA:

Schnelles Recovery nach einem Cyberangriff



IBM Spectrum Sentinel …

- … bietet eine automatisierte Ransomware-Erkennung.
- … verwendet MLM (Machine Learning Model) Algorithmen zur Anomalie-Erkennung, um potenzielle Bedrohungen zu identifizieren.
- … erstellt unveränderlich anwendungsspezifische primäre Speicher-Snapshots (Safeguarded Copies).
- … orchestriert das Recovery mit verifizierten und validierten Sicherungskopien.
- … unterstützt SAP HANA mit x86 und Power Linux.

Leistungsstarke Scan-Engine

IBM Spectrum Sentinel verwendet die IBM Spectrum Copy Data Management Software. Diese kümmert sich um die Erstellung und Verwaltung von anwendungsbezogenen IBM Safeguarded Copy-Sicherungen, die während der kontinuierlich vollzogenen Anomalie- und Ransomware-Scans als „sauber“ und nicht kompromittiert erkannt wurden.

Eine spezielle Scan-Engine analysiert die Datenkopien der Applikation fortlaufend auf zerstörerische Programmcodes. Für diese Aufgabe nutzt der Scanner ein Machine Learning Modell (MLM), das mit realen zerstörerischen Codes trainiert wurde. Auf diese Weise sind potenzielle Angriffe schnell identifizierbar.

IBM Spectrum Sentinel für SAP HANA:
Schnelles Recovery nach einem Cyberangriff

Pre-attack | **Scanning** | **Determine Good Snapshot** | **Attack Occurs** | **Review Integrity** | **Restore**

Im Scanprozess wird auch die Integrität von Datenbanken überprüft, um Beschädigungen der internen Datenbankdaten zu erkennen. Der Scanner untersucht Datenbankseiten, Zuordnungstabellen, Hilfsfelder und Signaturen. Zusätzlich führt er Cyclic Redundancy Checks (CRC) und vieles mehr durch, immer mit dem Ziel, Anomalien zu entdecken.

Forensische Berichte informieren über mögliche Unregelmäßigkeiten. So lässt sich die Quelle eines Angriffs schnell diagnostizieren und identifizieren. Das System wird ständig mit neuen Updates versorgt. Damit ist sicher gestellt, dass auch neuere Bedrohungen erkannt werden.

Die fortlaufenden Scans helfen die guten, nicht infizierten Safeguarded Copies als verwendbare Backup-Kopien mit einem konsistenten Datenbestand herauszufiltern und schaffen damit die Grundlage für ein sehr schnelles Recovery der Primärdaten. Der Systemadministrator kann dabei einen integrierten Datenkatalog nutzen, in dem sofort die Scan-Ergebnisse angezeigt werden. Mit wenigen Klicks ist dann der Recocery-Prozess eingeleitet.

Aus der Praxis für die Praxis

IBM Spectrum Sentinel basiert auf Erfahrungen von Unternehmen, die einen Ransomware-Angriff oder eine andere Cyberbedrohung erfolgreich überstanden haben. Die sichere und schnelle Wiederherstellung der Daten nimmt einen besonders hohen Stellenwert ein. IBM Spectrum Sentinel ersetzt nicht existierende Real-Time Security-Anwendungen, bietet aber im Korruptionsfall eine „letzte Verteidigungslinie“ für ein schnelles Recovery.

IBM plant in 2023, weitere Workloads und Datenbank-Applikationen mit IBM Spectrum Sentinel zu unterstützen.

Ihr Ansprechpartner:

Jörg Fricke
Vertriebsleitung

Telefon: +49 (0) 511-51529-441
E-Mail: fricke@netzlink.com

Netzlink Informationstechnik GmbH
IT-Campus Westbahnhof
Hollerithallee 17
30419 Hannover