Ransomware – wenn jede Sekunde zählt!

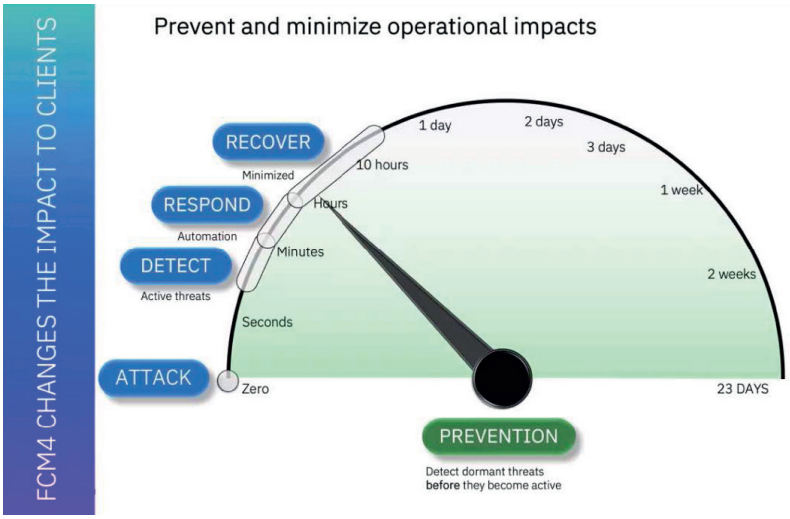
In der heutigen digitalen Landschaft ist die Bedrohung durch Ransomware immens und hat verheerende Folgen für Unternehmen weltweit. Laut IBM Threat Intelligence Index 2024 steht Europa im Zentrum der Angriffe – mit 32 % aller im Jahr 2023 verzeichneten Angriffe ist es inzwischen das Hauptziel aller Attacken.

Was passiert, wenn Hacker die unternehmensweiten Sicherheitsbarrieren durchbrechen?

Ein Ransomware-Angriff kann bis zu 1,7 TB Daten pro Minute verschlüsseln – innerhalb von nur 24 Stunden werden damit 2,5 PB an Daten unzugänglich.* Die durchschnittliche Zeit bis zur Erkennung eines solchen Angriffs liegt im Bereich von vier Tagen bis zu mehreren Wochen, wodurch sich der Wiederherstellungsprozess im Durchschnitt auf über 23 Tage verlängert. Dies führt zu erheblichen Betriebsstörungen und finanziellen Verlusten. Laut Cost of a Data Breach Report kostete ein Datenleck deutsche Unternehmen im Jahr 2023 durchschnittlich 4,3 Millionen Euro. Zudem sind viele Unternehmen nicht mehr in der Lage, ihren kompletten Datenbestand wiederherzustellen.

Damit Unternehmen trotz eines Angriffs weiterarbeiten können, sind drei Schritte notwendig:

- **Schnelle Erkennung von Schadsoftware,** bevor sich Ransomware weiterverbreiten kann und größere Datenbestände verschlüsselt werden
- Das Anfertigen **unveränderlicher, unternehmenskritischer Datenkopien** (SGC = Safeguarded Copy). Die Wiederherstellung dieser Datenbestände sollte dadurch in Minuten oder Stunden statt Wochen möglich sein
- **Automatisierte Routinen** für Datenscanning, Prüfung, Isolation und schnelle Wiederherstellung, da im Falle- des- Falles auf „Knopfdruck" schnell geprüft und wiederhergestellt werden muss



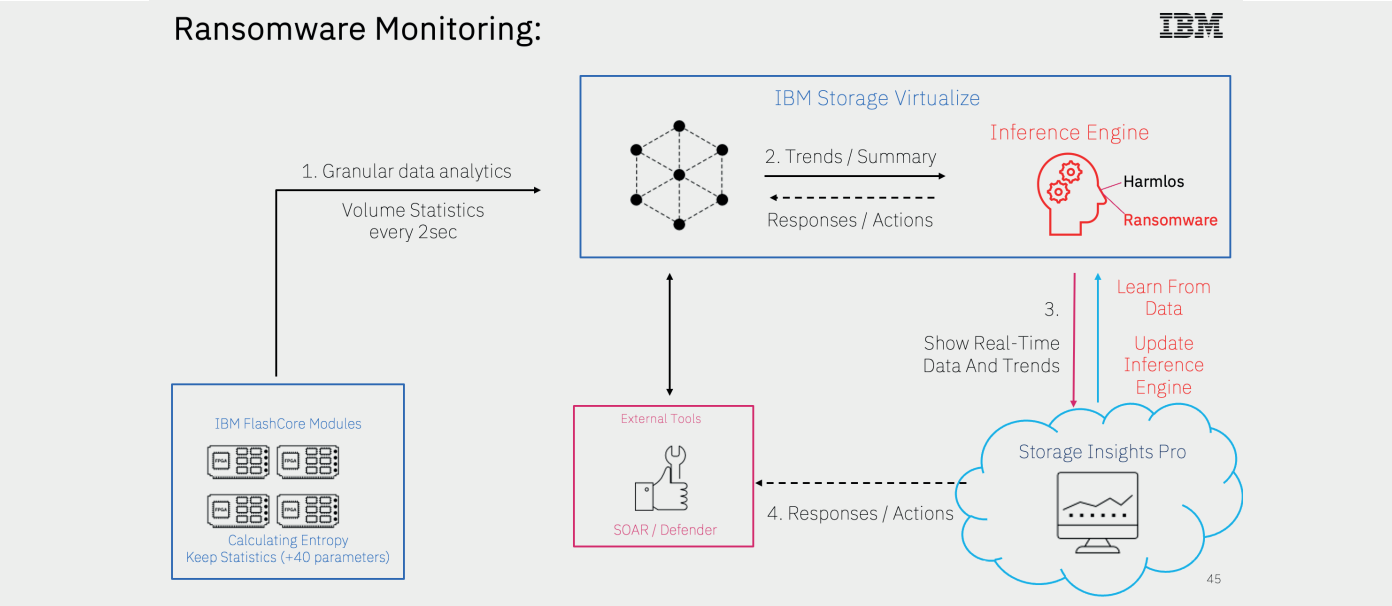
Ihr starker IT-Partner.
Heute und morgen.

Integrierte Ransomware-Erkennung.

Um die Erkennung eines Cyber-Angriffs in Sekunden zu realisieren, nutzt IBM erstmals in der Industrie Computational Storage und KI in Form von IBM FlashCore-Modulen 4 (FCM4). Diese Speichermodule analysieren geschriebene Daten-Inputs und -Outputs anhand von etwa 40 Parametern (z. B. Compression Change Rate, Input/Output Transfer Size). Eine speziell trainierte KI im Speichersystem erkennt mit diesen Daten potenzielle Angriffe in Realtime (siehe Abb. 2). Diese integrierte Ransomware-Erkennung (RTD – Ransomware Threat Detection) arbeitet ohne Performance-Verluste für das Speichersystem. Durch frühe Erkennung von Schadsoftware können deutlich schnellere Gegenmaßnahmen zum Schutz der Daten eingeleitet werden (zum Beispiel die Erstellung weiterer Kopien oder die Isolation der Workloads).

IBM FCM4 können mehr.

IBM FCM4 geht über die bloße Erkennung von Ransomware hinaus und bietet ein Komprimierungsverhältnis von bis zu 3:1 sowie Datenverschlüsselung und maximale Speichereffizienz, ohne die Leistung zu beeinträchtigen. Die Speichermodule stehen dabei mit bis zu 115 TB effektiver Kapazität zur Verfügung – das bedeutet, es können bis zu 1 PB an Flash auf einer Rack-Höheneinheit (1RU) gespeichert werden. Dies ist die höchste Speicher-Packungsdichte in der Industrie, sie hilft bei Platzproblemen und der Energieversorgung im Rechenzentrum!



Erkennen, prüfen, wiederherstellen, orchestrieren – Data Resiliency mit IBM Storage Defender.

In Kombination mit IBM Storage Defender, der umfassenden Data-Resilience-Plattform für den Schutz von Primär- und Sekundärdaten, bietet IBM FCM4 den perfekten Schutz für kritische Produktionsdaten in Unternehmen.

Von der Sicherung von Anwendungen und Dateisystemen bis zur proaktiven Untersuchung ruhender Daten automatisiert IBM Storage Defender die Bedrohungserkennung, führt Wiederherstellungstests durch und ermöglicht eine nahtlose Wiederherstellung innerhalb von Minuten nach einem Angriff. Durch die Zusammenarbeit von IBM FCM4 und IBM Storage Defender können Unternehmen ihre Abwehr-maßnahmen stärken, Risiken mindern und die Geschäftskontinuität zuverlässig gewährleisten.

Darüber hinaus lässt sich die Lösung nahtlos in bestehende SIEM/SOAR-Systeme integrieren, optimiert Sicherheitsabläufe und ermöglicht eine Reaktion auf Bedrohungen in Echtzeit. Durch erweiterte Automatisierungsfunktionen ermöglicht IBM FCM4 Unternehmen, Cyber-Bedrohungen einen Schritt voraus zu sein und ihre wertvollsten Vermögenswerte mit beispielloser Effizienz und Effektivität zu schützen.

Weitere Informationen: www.ibm.com/flashsystem

* Von IBM UK gemessener Kundenfall, Ransomware-Angriff auf ein Flash-Array