IBM Italy News Room

IBM offre nuove funzionalità di data resilience, potenziate grazie all'AI, per combattere i ransomware e altri tipi di minacce informatiche con soluzioni di Storage avanzate

Milano, 13 marzo 2024 - Oggi, le organizzazioni devono affrontare rischi diversi per proteggere i propri dati, come attacchi informatici, minacce interne, esfiltrazione dei dati, malfunzionamenti hardware, oltreché disastri naturali, ormai diventati un pericolo da non sottovalutare. Inoltre, come evidenziato nel recente report 2024 IBM X-Force Threat Intelligence, con il consolidarsi del mercato dell'intelligenza artificiale generativa, l'AI potrebbe arrivare ad un momento di maturità tale da divenire una potenziale superficie di attacco, inducendo i criminali informatici alla ricerca di nuovi strumenti.

Per aiutare i clienti a contrastare le minacce alla sicurezza dei propri dati, IBM ha sviluppato nuove funzionalità avanzate di Ransonware Threat Detection (RTD) integrandole nei nuovi **FlashCore Module (FCM4)** disponibili nei sistemi storage FlashSystem.

Completa l'offerta la soluzione **IBM Storage Defender** in grado di fornire strumenti idonei ad affrontare il tema della resilienza dei dati end-to-end sui carichi di lavoro sia primari che secondari. Storage Defender integra le funzionalità software sviluppate per contrastare minacce come ransomware, esfiltrazioni e attacchi interni, coordinando le azioni di difesa migliorando le capacità di rilevamento di tentativi di intrusione.

La quarta generazione della tecnologia **FlashCore Module (FCM)** abilita funzionalità di intelligenza artificiale all'interno della gamma prodotti IBM Storage FlashSystem. FCM lavora con Storage Defender per fornire una *data resilience* end-to-end con sensori basati sull'intelligenza artificiale progettati per rilevare in anticipo le minacce informatiche e aiutare le aziende a ripristinare i loro sistemi più velocemente.

Click here to experience IBM FlashSystem in a virtual demo

Click here for IBM Storage Defender information

Rilevamento precoce delle minacce nel *Data Stream*

Le soluzioni IBM FlashSystem eseguono la scansione di tutti i dati senza alcun impatto sulle prestazioni durante la scrittura, utilizzando il software di rilevamento della corruzione dei dati in linea e l'intelligenza artificiale cloud-based per identificare le anomalie che potrebbero indicare l'inizio di un attacco informatico. Il sistema è così in grado di rilevare, rispondere ed effettuare rapidamente il ripristino grazie a copie immutabili. La nuova tecnologia di FCM4 è stata progettata per monitorare continuamente le statistiche raccolte da ogni singolo I/O utilizzando modelli di machine learning per rilevare anomalie come i ransomware in meno di un minuto.[1]

"Le minacce informatiche si evolvono rapidamente, rendendo il rilevamento precoce un passo fondamentale nell'aiutare i clienti a rispondere agli attacchi", ha dichiarato **Daneyand "DJ" Singley, Executive Director di MAPSYS**. *"Con IBM FlashSystem e FCM3 favoriamo il rapido ripristino delle attività dei clienti mentre, la nuova tecnologia FCM4 nei nuovi array FlashSystem ci permette di contrastare tempestivamente gli attacchi"*.

I prodotti della gamma IBM FlashSystem già misurano parametri quali la comprimibilità e la casualità o l'entropia dei dati e trasmettono queste informazioni al software IBM Storage Insights in modo da poter segnalare il rilevamento di un'anomalia nel workload, come, ad esempio, quelle causate da un ransomware che inizia a codificare i dati di un'applicazione. La tecnologia FCM4 nei nuovi array FlashSystem è progettata per raccogliere e riassumere in tempo reale statistiche dettagliate su ogni I/O. FlashSystem utilizza i modelli di machine learning per distinguere i ransomware e i malware dalle situazioni normali, consentendo alle organizzazioni di intervenire e allo stesso tempo continuare a operare in caso di attacco.

"Le organizzazioni devono adottare un approccio di 'difesa in profondità' contro i ransomware e altri attacchi informatici, soprattutto perché i malware diventano sempre più sofisticati", ha dichiarato **Dave Pearson, Research VP, Infrastructure, IDC**. *"L'infrastruttura di storage è un altro livello in cui la cyber resilience può essere migliorata e IBM ha sviluppato il nuovo FlashCore Module 4 con funzionalità basate sull'AI, progettate per*

velocizzare il rilevamento dei ransomware, ridurne la diffusione e l'impatto e accelerare il ripristino".

Migliorare l'identificazione delle minacce

Il software IBM Storage Defender offre una *data resilience* end-to-end per i moderni ambienti IT ibridi multi-cloud che includono VM (Virtual Machine), database, applicazioni, file system, carichi di lavoro SaaS e container.

Inoltre, IBM Storage Defender include sensori basati sull'intelligenza artificiale sviluppati da IBM Research e progettati per rilevare rapidamente e con elevata precisione i ransomware e altre minacce avanzate. Defender invia segnalazioni di elevata attendibilità agli strumenti di sicurezza per ridurre il raggio d'azione delle violazioni alla sicurezza e aiutare le aziende nelle operazioni di ripristino in caso di attacco.

Inoltre, IBM include funzionalità di gestione dello storage e dei workload in IBM Storage Defender, progettate per aiutare le organizzazioni a valutare la portata delle proprie applicazioni e dei propri dati. Ciò consentirà di incorporare i propri asset in un piano di *business continuity* per recuperare il livello minimo di operatività dopo un attacco informatico. Defender prevede inoltre la possibilità di orchestrare e automatizzare il recupero delle applicazioni VMware.

Una importante caratteristica di Defender è la facilità con cui si integra con altre soluzioni IBM Storage e IBM Security, inclusi IBM QRadar, IBM Guardium**,** IBM FlashSystem, IBM Storage Scale, IBM Storage Ceph e IBM Fusion. Oltre alle soluzioni IBM, Defender si integra con Cohesity e con altre piattaforme di dati di terze parti per aumentare la *data resilience* end-to-end nell'infrastruttura aziendale.

Integrazione per garantire migliori risultati

Singolarmente, sia FlashSystem sia Defender dispongono di funzionalità che possono contribuire a rendere le organizzazioni ancora più *data resilient*, ma insieme raggiungono risultati ancora più efficaci. Ad esempio, gli storage administrators possono ora creare gruppi di protezione che includono volumi specifici e di cui viene automaticamente eseguito il backup in base ai criteri definiti dall'utente. Le copie immutabili dei dati, nella fase di recupero da un attacco informatico, possono ora essere ripristinate o recuperate in diverse ambienti. Inoltre,

le copie immutabili possono essere replicate su un altro cluster IBM Storage Defender per un ulteriore livello di protezione.

IBM ha anche definito impostazioni che consentono agli amministratori di automatizzare la creazione di snapshot di Safeguarded Copy, copie cyber-resilienti *point-in-time* di dati che non possono essere modificate o eliminate in seguito ad errori dell'utente, azioni dannose o attacchi informatici. L'isolamento di queste copie di backup dai dati di produzione è stato progettato per consentire alle aziende di recuperare i dati più rapidamente dopo la loro compromissione.

Il nuovo hardware FlashCore Module e il software Storage Defender sfruttano le funzionalità AI di IBM per aiutare le organizzazioni ad affrontare meglio gli attacchi informatici generati dall'intelligenza artificiale. Il portafoglio di prodotti IBM non solo aiuta a offrire una *data resilience* ai clienti, tra cui molte delle più grandi organizzazioni finanziarie e sanitarie del mondo, per aiutarli a fronteggiare le minacce, ma anche ad accelerare il processo di ripristino dei sistemi nel caso in cui i cybercriminali siano stati in grado di violarli.

IBM

IBM è un'azienda leader a livello mondiale nel settore del cloud ibrido, dell'AI e dei servizi alle imprese e opera con le imprese di oltre 175 Paesi aiutandole a capitalizzare sugli insight dei loro dati, a semplificare i processi aziendali, a ridurre i costi e a ottenere un vantaggio competitivo nei loro settori d'industria. Quasi 4.000 enti governativi e aziende in aree infrastrutturali critiche come quelle dei servizi finanziari, delle telecomunicazioni e sanità si basano sulla piattaforma cloud ibrida di IBM e su Red Hat OpenShift per realizzare la loro trasformazione digitale in modo rapido, efficiente e sicuro. Le innovazioni di IBM nell'ambito dell'AI, del quantum computing, delle soluzioni cloud specifiche per settore d'industria e nei servizi sono offerte con opzioni open e flessibili. Tutto questo è supportato dal ben noto impegno di IBM per la trasparenza, la responsabilità, l'inclusività e il servizio. Per maggiori informazioni, visitate il sito https://www.ibm.com/it-it.

LinkedIn: IBM

Contatti
Morgana Stell - *External Relations Leader, IBM Italia*
email: morgana.stell@it.ibm.com
mobile: 335 7693528

[1] *Avvertenza: la sperimentazione interna di IBM Research ha dimostrato il rilevamento del ransomware entro 1 minuto dall'inizio del suo processo di crittografia. Questo esperimento è stato eseguito su FlashSystem 5200 con 6 FCM con il caricamento del firmware 4.1. Il 5200 eseguiva il software di livello GA 8.6.3. L'host collegato alla 5200 eseguiva Linux su un file system XFS. In questo caso particolare, è stato utilizzato il simulatore ransomware IBM denominato WannaLaugh. Il sistema sottostante deve essere compatibile con FCM4.1 e deve eseguire il software con versione 8.6.3 di livello GA per poter riprodurre i risultati ottenuti.*

---

https://it.newsroom.ibm.com/storagedefender