Comunicados

IBM anuncia nuevos recursos de resiliencia de datos mejorados con IA para ayudar a combatir el ransomware y otras amenazas con soluciones de almacenamiento avanzadas

Lima, 27 de febrero de 2024 - Los ciberataques son un riesgo existencial, con el 89% de las organizaciones clasificando el ransomware como una de las cinco principales amenazas a su viabilidad, según un informe de noviembre de 2023 del Enterprise Strategy Group de TechTarget, firma de líder de analistas [1]. Y este es sólo uno de los muchos riesgos para los datos corporativos: las amenazas internas, las filtraciones de datos, las fallas de hardware y los desastres naturales también representan peligros importantes. Además, como lo demuestran el recientemente anunciado IBM X-Force Threat Intelligence Index 2024, a medida que el mercado de la IA generativa se consolide, podría desencadenar la madurez de la IA como una superficie de ataque, movilizando aún más la inversión de los cibercriminales en nuevas herramientas. El informe revela que las empresas también deben ser conscientes que su infraestructura existente es una puerta de entrada a sus modelos de IA y que los atacantes no requieren nuevas tácticas para alcanzar sus objetivos [2].

Para ayudar a los clientes a contrarrestar estas amenazas con una detección más precisa y temprana, IBM presenta nuevas versiones de la tecnología IBM FlashCore Module mejorada con IA, disponible dentro de los nuevos productos de IBM Storage FlashSystem y la nueva versión del software IBM Storage Defender para ayudar a las organizaciones a mejorar su capacidad para detectar y responder ante ransomware y otros ciberataques que amenacen sus datos.

La cuarta generación recientemente disponible de la tecnología FlashCore Module (FCM) habilita capacidades de inteligencia artificial en la familia IBM Storage FlashSystem. FCM trabaja con IBM Storage Defender para brindar resiliencia de datos de punta a punta en todas las cargas de trabajo primarias y secundarias con sensores impulsados por IA y diseñados para notificar anticipadamente el surgimiento de ciberamenazas para ayudar a las empresas a recuperarse más rápido.

Detección temprana de amenazas en el flujo de datos

Los productos existentes de IBM FlashSystem escanean todos los datos entrantes hasta una granularidad a nivel de bloque sin afectar el rendimiento a medida que se escriben, utilizando software secuencial de detección de corrupción de datos e inteligencia artificial basada en la nube para ayudar a identificar anomalías que

pueden indicar el inicio de un ciberataque, permitiendo al sistema detectar, responder y recuperarse rápidamente con copias inalterables. La nueva tecnología habilitada por FCM4 está diseñada para monitorear continuamente las estadísticas recopiladas de cada E/S utilizando modelos de aprendizaje automático para detectar anomalías, como ransomware, en menos de un minuto [3].

"Las ciberamenazas evolucionan rápidamente, haciendo que la detección temprana sea un paso crítico para ayudar a los clientes a responder a los ataques", dijo Daneyand "DJ" Singley, Director Ejecutivo de MAPSYS. "Elegimos a IBM FlashSystem y FCM3 para ayudar a nuestros clientes a recuperarse rápidamente. Con la nueva tecnología FCM4 en los nuevos arrays de FlashSystem, anticipamos la capacidad de tomar medidas inmediatas para detener los ataques".

Los productos IBM FlashSystem ya miden parámetros como la compresibilidad y aleatoriedad, o la entropía de los datos, y transfieren esta información al software IBM Storage Insights para que pueda alertar a los operadores cuando se detecta una anomalía en la carga de trabajo, por ejemplo, cuando el ransomware comienza a cifrar los datos de una aplicación. La tecnología FCM4 en los nuevos arrays de FlashSystem está diseñada para capturar y resumir estadísticas detalladas sobre cada E/S en tiempo real. FlashSystem usa modelos de aprendizaje automático para distinguir el ransomware y el malware del comportamiento normal, permitiéndole a las organizaciones actuar y continuar operando en caso de un ataque.

"Las organizaciones deben adoptar un enfoque de 'defensa en profundidad' contra el ransomware y otros ciberataques, especialmente a medida que el malware se vuelve cada vez más sofisticado", afirmó Dave Pearson, Vicepresidente de Investigación de Infraestructura de IDC. "La infraestructura de almacenamiento es otra capa para mejorar la ciberresiliencia, e IBM ha creado su nuevo FlashCore Module 4 con capacidades basadas en IA diseñadas para acelerar la detección de ransomware, reducir su propagación e impacto, y acelerar la recuperación".

Ser más inteligente en la identificación de amenazas en las cargas de trabajo

El software IBM Storage Defender ofrece resiliencia completa de los datos en entornos de TI híbridos multinube modernos que incluyen máquinas virtuales (VM), bases de datos, aplicaciones, sistemas de archivos, cargas de trabajo SaaS y contenedores. La nueva versión de IBM Storage Defender amplía sus capacidades de detección de amenazas para ayudar a aumentar la confiabilidad de la copia como base para que los equipos comiencen a recuperarse de los ciberataques. Además, IBM Storage Defender incluye sensores impulsados por IA, desarrollados por IBM Research, que están diseñados para detectar rápidamente ransomware y otras amenazas avanzadas con alta precisión. Defender genera alertas de alta fidelidad para que las herramientas de seguridad limiten el impacto de las violaciones de seguridad y ayuden a las empresas a recuperarse de los ataques.

IBM también incluyó en IBM Storage Defender, capacidades para la gestión de cargas de trabajo e inventario de almacenamiento, diseñadas para ayudar a las organizaciones a evaluar el alcance de sus aplicaciones y datos. Esto ayudar a incorporar sus activos en un plan de continuidad del negocio para recuperar una empresa mínima viable después de un ciberataque. Además, Defender tiene la capacidad de organizar y automatizar la recuperación de aplicaciones VMware.

Uno de los principales atractivos de Defender es la facilidad con que se integra a otras soluciones de IBM Storage e IBM Security, como IBM QRadar, IBM Guardium, IBM FlashSystem, IBM Storage Scale, IBM Storage Ceph e IBM Fusion. Además de las soluciones de IBM, Defender se integra con Cohesity y se integrará con otras

plataformas de datos de terceros para proporcionar resiliencia de datos de extremo a extremo en todo el tejido de datos empresarial.

Mejor juntos

Individualmente, tanto FlashSystem como Defender tienen características que pueden ayudar a aumentar la resiliencia de los datos de las organizaciones, pero son aún mejores juntos. Por ejemplo, los administradores de almacenamiento ahora pueden crear grupos de protección que incluyan volúmenes específicos de los que se realice una copia de seguridad automáticamente de acuerdo con las políticas definidas por el usuario. Se pueden restaurar o recuperar copias inmutables de datos en múltiples destinos o ubicaciones durante la recuperación de un ciberataque. Además, las copias inmutables se pueden replicar en otro clúster de IBM Storage Defender para obtener una capa adicional de protección.

IBM también ha diseñado configuraciones que permiten a los administradores automatizar la creación de instantáneas de Safeguarded Copy, copias de datos que son ciber resilientes y no se pueden alterar ni eliminar mediante errores del usuario, acciones maliciosas o ciberataques. El aislamiento estas copias de seguridad de los datos de producción está diseñado para permitir a las organizaciones recuperar datos rápidamente después de un evento de pérdida de datos.

Las noticias muestran que los actores de amenazas ahora están implementando ciberataques impulsados por IA y debemos combatir el fuego con fuego. El nuevo hardware FlashCore Module y el software Storage Defender aprovechan las capacidades de inteligencia artificial de IBM para ayudar a las organizaciones a enfrentar mejor ese desafío. El portafolio de productos de IBM no solo proporciona resiliencia integral de datos a los clientes, incluyendo a muchas de las organizaciones financieras y sanitarias más grandes del mundo, ayudándolos a prevenir amenazas en primer lugar, sino que también, permite a estas empresas acelerar el proceso de recuperación en caso de ataques exitosos.

Para ver una demostración virtual del IBM FlashSystem visite: https://www.ibm.com/demos/it-infrastructure/IBM_Storage_Virtualize/index.html

Para más información sobre IBM Storage Defender, visite: https://www.ibm.com/products/storage-defender

Lea la versión completa de este blog aquí: https://ibm.biz/AI_data_resilience

---

[1] *Preparación para ransomware 2023: el camino hacia la preparación y la mitigación, publicado por Enterprise Strategy Group/TechTarget, en noviembre de 2023*

[2] *Informe publicado por IBM Security en febrero de 2024: https://www.ibm.com/reports/threat-intelligence*

[3] *Disclaimer: la experimentación interna de IBM Research demostró la detección de ransomware 1 minuto después de que el ransomware comenzara su proceso de cifrado. Este experimento se realizó en un*

FlashSystem 5200 con 6 FCM con carga de firmware 4.1. El 5200 tenía cargado el software GA nivel 8.6.3. El host conectado al 5200 ejecutaba Linux con el sistema de archivos XFS. En este caso concreto se utilizó el simulador de ransomware de IBM llamado WannaLaugh. El sistema subyacente debe ser compatible con el software de nivel FCM4.1 y versión 8.6.3 GA cargado para lograr los resultados obtenidos.
