Anuncios

Nuevo mainframe de IBM para la nube híbrida segura

• IBM z13s es el servidor más seguro del mundo, creado para cloud híbrida y disponible también para medianas empresas (1)

• El sistema encripta la información el doble de rápido que las generaciones anteriores y la nueva solución de analítica z Systems Cyber Security identifica los comportamientos maliciosos basándose en comportamientos aprendidos (2)

Madrid - 18 feb 2016: IBM (NYSE: IBM) presenta un nuevo mainframe que acerca a las medianas empresas las ventajas de la encriptación de la información sin impactar negativamente en el rendimiento del sistema. El nuevo sistema, IBM z13s, está optimizado para los entornos de nube híbrida y es capaz de proteger mejor que sus predecesores la información y las transacciones críticas. La Compañía también ha dado a conocer nuevos avances y colaboraciones en materia de seguridad:

• **Seguridad integrada en el hardware** – el nuevo IBM z13s dispone de funcionalidades de cifrado avanzadas que se han incorporado al hardware y que le permiten encriptar y descifrar información al doble de velocidad que las generaciones anteriores, y sin que ello suponga sacrificar el rendimiento.

• **Capacidades de seguridad inteligente** – IBM integra la tecnología del mainframe con las soluciones de software de IBM Security para tener una base segura en una infraestructura de nube híbrida. La Compañía también ofrece un nuevo servicio de *Cyber Security Analytics* a los clientes de z Systems que puede ayudar a identificar la actividad maliciosa gracias al aprendizaje del comportamiento del usuario a lo largo del tiempo.

• **Un ecosistema de socios ampliado** – IBM colabora con líderes del sector de la ciberseguridad a través del programa "*Ready for IBM Security Intelligence*" para ofrecer soluciones y productos a medida de sus clientes. Los nuevos socios para z Systems son BlackRidge Technology, Forcepoint (una empresa conjunta entre socios de Raytheon y Vista Equity Partners) y RSM Partners.

A medida que la empresa digital se va generalizando y aumentan las transacciones, la necesidad de una seguridad más robusta es primordial. Cada año, una empresa media puede llegar a enfrentarse a unos 81 millones de incidentes de seguridad3. Además, IDC predice una adopción de la nube híbrida empresarial del 80% para 20174. Los ciberdelincuentes actuales más que robar información, la manipulan, poniendo en peligro la fiabilidad de una compañía. El nuevo z13s permite acceder a las APIs y los microservicios en un entorno de nube híbrida, a la vez que mantiene la información segura y su integridad intacta.

La familia mainframe aumenta sus capacidades de seguridad

IBM z13s es el modelo de entrada del portfolio de z Systems para empresas de todos los tamaños e incorpora muchas novedades en materia de seguridad.

z Systems es capaz de encriptar información confidencial sin perjudicar el rendimiento transaccional ni afectar

al tiempo de respuesta, eliminando así lo que hasta ahora era una barrera para los departamentos de TI a la hora de implementar la encriptación. z13s incluye una tarjeta de coprocesador criptográfico actualizada de aceleración por hardware resistente a las manipulaciones con procesadores más rápidos y más memoria, que hace posible una encriptación el doble de rápida que los sistemas anteriores de gama media. Significa que los clientes ahora pueden procesar el doble de transacciones de gran volumen protegidas criptográficamente sin comprometer el rendimiento. Esto supone por ejemplo, poder procesar el doble de compras online y móviles con un coste por transacción inferior.

Los clientes de z Systems pueden aprovechar *z Systems Cyber Security Analytics*, que ofrece un nivel avanzado de monitorización de las amenazas basado en el análisis del comportamiento. La solución, desarrollada por IBM Research, aprende del comportamiento de los usuarios y con ello es capaz de detectar patrones anómalos en la plataforma, alertando a los administradores de una posible actividad maliciosa. La oferta de seguridad inteligente incluida en z Systems se completa con *IBM® Security QRadar®*, que puede correlacionar información de más de 500 fuentes para ayudar a las organizaciones a determinar si los eventos relacionados con la seguridad son simples anomalías o amenazas potenciales. El servicio *z Systems Cyber Security Analytics* estará disponible de forma gratuita como beta para los clientes de z13 y de z13s.

Por otra parte, *IBM Multi-factor Authentication for z/OS (MFA)* ya está disponible en z/OS. La solución añade otra capa de seguridad al solicitar a los usuarios con acceso privilegiado que introduzcan una segunda forma de identificación como un PIN o un identificador generado aleatoriamente para acceder al sistema. Esta es la primera vez que MFA se ha integrado estrechamente en el sistema operativo, en lugar de mediante una solución de software adicional. Se espera que este nivel de integración aporte una configuración más óptima y un mejor rendimiento y estabilidad.

Seguridad mejorada para la nube híbrida

La infraestructura de la nube híbrida ofrece ventajas en términos de flexibilidad pero también puede suponer nuevas vulnerabilidades. Más de la mitad de los atacantes se hallan dentro de las organizaciones, por lo que las empresas deben automatizar la monitorización, eliminando el error humano. Para ello, IBM incorpora en el mainframe las soluciones de IBM Security que abordan la gestión de identidades en accesos privilegiados y la protección de la información confidencial. Al combinarse con z Systems, con estas soluciones los clientes pueden establecer una seguridad completa en sus entornos de nube híbrida.

IBM Security Identity Governance and Intelligence ayuda a prevenir las pérdidas de información involuntarias o maliciosas, mediante la gestión y verificación del acceso según las políticas reconocidas, a la vez que permite acceder los usuarios autorizados. Por otro lado, *IBM® Security Guardium* emplea la analítica para ayudar a garantizar la integridad de la información mediante la monitorización inteligente al rastrear qué usuarios están accediendo a qué datos concretos. Finalmente, *IBM Security zSecure and QRadar* utilizan alertas en tiempo real para centrarse en las amenazas de seguridad críticas identificadas que pueden ser más importantes para la empresa.

El ecosistema se seguridad se expande a la plataforma mainframe

La seguridad de un sistema exige un profundo conocimiento de amenazas y de sectores concretos. Por ello, IBM está colaborando con otros líderes en esta área para potenciar sus propias soluciones. Ahora, el programa de colaboraciones estratégicas de IBM para la seguridad, "*Ready for IBM Security Intelligence*," incluye más

aplicaciones de software procedentes de ISVs (desarrolladores de software independientes) clave que integran sus soluciones para z Systems. Al ampliarse el programa a z Systems, ofrecerá una capa adicional de protección y gestión del acceso a las aplicaciones, los recursos y la información crítica que reside en el mainframe.

Algunos ejemplos son BlackRidge Technology, que ofrece seguridad de red basada en la identidad que opera antes de que se creen las conexiones de red, de modo que la protección se activa en la capa de las aplicaciones; Forcepoint's Trusted Thin Client®, que protege la información confidencial y de misión crítica en el terminal; y RSM Partners, con amplia experiencia en disponibilidad de las aplicaciones.

El nuevo z13s estará disponible en marzo de este año. IBM y sus *Business Partners* disponen de arrendamientos y planes de pago de *IBM Global Financing* con unos términos y condiciones flexibles que se pueden adaptar a las necesidades de cada cliente para actualizar los modelos antiguos a z13s, pasar de tener en propiedad un z System a una solución de arrendamiento al renovar el sistema o adquirir un z13s nuevo. Incluye 90 días de carencia para los clientes con crédito cualificado.

Para más información sobre IBM Security, puede visitar http://www.ibm.com/security, seguir @IBMSecurity en Twitter o visitar el blog de IBM Security Intelligence.

Más información acerca de la cartera IBM z Systems en http://www.ibm.com/systems/z/ o el blog de IBM Systems.

[1] *Basado en la clasificación de la seguridad de EAL5+ de Common Criteria para el mainframe z Systems; May the Cyber Security Force be with You, un estudio de Solitaire Interglobal Ltd; y 2015 Global Server Hardware and Server OS Reliability Survey, un estudio conjunto de ITIC y Strategy Analytics.*

[2] *Basado en pruebas de IBM del rendimiento de z/OS y del hardware donde la tarjeta CryptoExpress5S ha realizado más de 21.000 operaciones SSL de negociación o handshake completas por segundo, por cada tarjeta que usa System SSL; y mediciones llevadas a cabo en el laboratorio que revelan que el Central Processor Assist for Cryptographic Function (CPACF) se ha optimizado para ofrecer funciones de encriptación hasta 2,3 veces más rápidas en z13s al compararlo con zBC12.*

[3] *Basado en el índice* "IBM 2015 Cyber Security Intelligence Index"

[4] IDC, "IDC FutureScape – Worldwide Cloud 2015 Predictions – Mastering the Raw Material of Digital Transformation", Documento # 259840, noviembre de 2015.

[5] De acuerdo con el testimonio de National Security Administration, septiembre de 2015.

[6] Según el índice IBM 2015 Cyber Security Intelligence Index