

Cada brecha de seguridad costó de media al sector sanitario 7,13 millones de dólares en 2020, el mayor coste sectorial

- Según el último estudio Data Breach Report de IBM
- IBM destaca tecnologías como la computación confidencial para lograr un nivel más alto de seguridad en la protección de datos críticos en sectores como el sanitario
- Los entornos cloud mal configurados provocaron un 19% de las brechas de seguridad intencionadas

Madrid, 28 de enero de 2021. La pandemia y la adopción masiva del teletrabajo ha puesto el foco más que nunca en la ciberseguridad y la protección de los datos de las personas y organizaciones. En 2020 la COVID-19 fue una temática recurrente utilizada por los ciberdelincuentes para la obtención de información sensible de las empresas, a través de técnicas de phishing, ransomware, o suplantación de identidad. Con motivo del día internacional de la privacidad de la información, IBM desvela algunos avances en materia de ciberseguridad.

Según el último [Data Breach Report](#) de IBM, el sector sanitario ha sido uno de los más afectados durante la pandemia, registrando el coste medio por brecha de datos más alto en comparación con otros sectores, valorado en 7,13 millones de dólares, un incremento del 10% respecto al mismo estudio de 2019. En ese aspecto, para dar un nivel más alto de protección a los datos críticos de las organizaciones, IBM apuesta por la tecnología de **computación confidencial** para garantizar la seguridad al más alto nivel en entornos cloud.

La información confidencial que maneja el sector sanitario es un área de gran interés para la ciberdelincuencia. Con la pandemia, al extenderse el teletrabajo y las consultas médicas virtuales, los atacantes encontraron nuevos puntos de acceso para lograr acceder a la información confidencial de los hospitales y pacientes. El ataque más extendido consistía en chantajear pidiendo rescates económicos a cambio de volver a hacer accesibles los datos clínicos. El estudio señala que la mitad de las causas de las brechas producidas en este sector corresponden a ataques malintencionados, frente a un 23% de fallos técnicos y un 27% de errores humanos. Asimismo, el sector sanitario tardó de media 329 días en identificar y contener una brecha de datos, el mayor tiempo promedio en comparación con otras industrias.

El pasado mes de diciembre, además, IBM anunció un [ciberataque a la cadena de frío de las vacunas](#) del coronavirus a nivel global, lo que destaca la importancia de mantener unos niveles altos de seguridad para la información más confidencial de las organizaciones e instituciones. El último informe de Data Breach Report de IBM también destaca que las credenciales comprometidas y los entornos cloud mal configurados fueron la causa de un 19% de las brechas de seguridad intencionadas, por lo que mejorar la seguridad en entornos cloud es crucial en el escenario tecnológico actual.

Confidential Computing, máxima seguridad mientras se utilizan los datos

En los últimos meses, a medida que las empresas dependen cada vez más de los servicios de nube pública e híbrida, la privacidad de los datos se vuelve un factor vital. De esta forma, IBM pone el foco en la tecnología de computación confidencial que se caracteriza por proteger los datos en la nube en el momento de su uso o ejecución, evitando vulnerabilidades cuando están descifrados.

¿Qué es y cómo funciona la computación confidencial?

La computación confidencial es una tecnología de computación en la nube que aísla los datos confidenciales en un enclave dentro de un CPU protegido durante el procesamiento. El contenido del enclave -los datos que se procesan y las técnicas utilizadas para procesarlos- son accesibles solo para el código de programación autorizado, y son invisibles e incomprensibles para cualquier otra persona, incluido el proveedor de la nube.

A medida que las empresas dependen cada vez más de los servicios de nube pública e híbrida, la privacidad de los datos se hace más y más imperativa. El objetivo principal de la informática confidencial es brindar una mayor seguridad de que los datos en la nube estén protegidos y sean confidenciales y alentar a las empresas a que trasladen más datos confidenciales y cargas de trabajo informáticas a los servicios de nube pública.

Durante años, los proveedores de la nube han ofrecido servicios de cifrado para proteger los datos en reposo (cuando están almacenados en bases de datos) y los datos en tránsito (moviéndose a través de una conexión de red). La informática confidencial elimina la vulnerabilidad de seguridad restante al proteger los datos en uso, es decir, durante el procesamiento o el tiempo de ejecución.

Antes de que una aplicación pueda procesarlos, los datos deben descifrarse en la memoria. Esto hace que los datos sean vulnerables justo antes, durante y justo después del procesamiento.

La informática confidencial resuelve este problema al aprovechar un entorno de ejecución confiable basado en hardware, o TEE, que es un enclave seguro dentro de una CPU. El TEE está protegido mediante claves de cifrado integradas y mecanismos de certificación integrados que garantizan que las claves sean accesibles únicamente para el código de aplicación autorizado. Si un malware u otro código no autorizado intenta acceder a las claves, o si el código autorizado es pirateado o alterado de alguna manera, el TEE niega el acceso a las claves y cancela el cálculo.

De esta forma, los datos sensibles pueden permanecer protegidos en la memoria hasta que la aplicación le indique al TEE que los descifre para procesarlos. Mientras se descifran y durante todo el proceso de cálculo, los datos son invisibles para el sistema operativo (o el monitor en una máquina virtual), para otros recursos de la pila de cómputo y para el proveedor de la nube y sus empleados.

Este enfoque para proteger los datos críticos de las empresas es compartido por diversos proveedores de hardware, nube y desarrolladores, a través del [Consortio de Computación Confidencial](#) del que IBM forma parte. El objetivo de esta comunidad de proyectos es definir y acelerar la adopción de la informática confidencial, en un momento en el que las empresas se trasladan cada vez más a los entornos en la nube.

For further information: Patricia Núñez IBM Comunicación patricia.nunez@es.ibm.com
