Texto
R. Contreras

LOS DATOS CRÍTICOS NECESITAN LA MÁXIMA PROTECCIÓN

La nueva joya de la corona

<< ¿Cuáles son los retos a los que se enfrentan las organizaciones alrededor de la protección del dato? ¿Qué modelos TI están aplicando al respecto? ¿Qué se recomienda a las compañías para definir una estrategia exitosa a largo plazo? Estas cuestiones fueron abordadas durante el encuentro que organizó Computing de la mano de IBM y Capgemini. Con la digitalización, el panorama en torno a los datos se ha revolucionado, dado el viaje masivo a la nube y a la movilización de los empleados. Las organizaciones ya no se hallan tranquilas en un feudo cerrado con siete llaves.

Adrián López Jareño, Manager-Digital Advisor de Penteo, fue el encargado de pintar este nuevo panorama sobre el valor de los datos para las empresas dentro de los procesos de transformación digital. "Lo que vemos es que nuestros activos a proteger ya no son físicos. Se viene apreciando esta tendencia en los últimos años y, agravada con la pandemia, a medida que disminuye la inversión en infraestructura tradicional va aumentando la inversión en el cloud".

En consecuencia, la nube es el marco donde concentrar los esfuerzos de la salvaguarda de la información. La complejidad crece porque se diluye el concepto de seguridad del dato dentro del perímetro de red clásico. Además, el nivel de conocimiento de los responsables de seguridad de las compañías es mejorable y la componente multicloud es una tendencia imparable que añade más incertidumbre. "Los diferentes entornos cloud se contratan con distintos proveedores, por lo que la correcta orquestación es otro reto añadido", puntualiza el experto de Penteo.

Y a este cóctel explosivo hay que añadir la pervivencia de los sistemas legacy, todavía hay mucha reticencia para subirlos a la nube, como es el caso de los sistemas industriales. "Vamos a tener una miscelánea de escenarios donde convivirán entornos on premise con la nube. Dentro del cloud, habrá entornos multicloud donde se habilitará la creación de multiplataformas digitales, que son las que nos permitirán crear ecosistemas abiertos para la integración e interconexión de nuestros aplicativos y nuestros datos del exterior. Esto genera una gran dispersión sobre dónde están nuestros datos y se agrava con la seguridad delegada en terceras partes, donde la responsabilidad de la protección recae en el cliente y no en estos proveedores", retrata el analista completando el círculo vicioso.

Desde su punto de vista, las medidas que deben aplicar las compañías pasan por la concienciación en materia de ciberseguridad, un término muy repetido como un mantra, pero es importante recalcarlo: "Una concienciación que debe ir de arriba hacia abajo. Desde los Comités de Dirección hasta los arquitectos y desarrolladores que deben embeber la seguridad en el diseño de los modelos de datos de la compañía, hasta el último empleado que debe estar entrenado para evitar malas praxis en esta materia". Adrián López considera crucial el compromiso de la Dirección para que salga adelante esta estrategia y permita el éxito de los negocios. Hay que diseñar modelos formales de gestión del gobierno del dato y en materia de ciberseguridad. Un estudio de Penteo señala que existe un bajo nivel en España de estos marcos normativos formalizados, basadas en mejores prácticas, como puede ser la ISO 27001.

En tercer lugar, la inversión es una piedra angular, "algo que históricamente se consideraba como un coste añadido; se construían los productos y luego había que securizarlos. La entrada en vigor de normativas como GDPR incentivó que, a partir de mayo de 2018, se hayan abordado muchos proyectos de ciberseguridad y protección del dato. Fue positivo porque la ciberseguridad pasó a ocupar un lugar en los Comités de Dirección, ya que la aplicación de este reglamento recaía sobre ellos".

Como resultado de todos estos factores, el rol del CISO tiene que acaparar mayor protagonismo, algo que se aprecia en las grandes compañías, y no así en las pequeñas, donde no existe un responsable de ciberseguridad. "El CISO debe verse como un facilitador, como un partner para TI y para negocio, propiciando que los sistemas sean seguros, pero sin convertirse en un stopper, lo cual a veces puede degenerar en el shadow IT", opina el experto.

> **"GDPR incentivó que se hayan abordado muchos proyectos de ciberseguridad y protección del dato"**

En último término, el analista de Penteo muestra su optimismo, pues se observa una tendencia favorable, dado que la mayoría de las compañías que han aumentado sus presupuesto lo han hecho en un 38%, mostrando un grado de concienciación mayor.

La visión de las empresas

En el caso de Dragados Offshore, no cuenta con un CISO como tal, según explica Luis Enrique Fiteni, IT Manager, "tenemos que valernos de técnicos y contratar con terceros para contar con especialistas que nos den su punto de vista de fuera de la empresa. Hace unos años apostamos por un sistema de recuperación de desastres robusto, replicando los datos en un sistema de backup, lo cual nos ha servido para salvaguardar información".

Como explica el CIO, Dragados Offshore se ha decantado por la tecnología de Sophos,

ISABEL TRISTÁN, IBM SECURITY SOFTWARE MARKET LEADER SPGI (SPAIN, PORTUGAL, GREECE & ISRAEL)

"UNA BRECHA DE DATOS CUESTA 3,86 MILLONES DE DÓLARES A LAS EMPRESAS"

Un estudio de Ponemon Institute indica que el coste medio a nivel global de una brecha de datos en 2020 fue de 3,86 millones de dólares y, por tanto, los retos son muchos y variados. Por un lado, esa protección resulta más complicada en la actualidad dado que el volumen de los datos es cada vez mayor y están distribuidos en múltiples repositorios de muy diversas tecnologías y fabricantes. Estos entornos tan heterogéneos suponen un reto para los CISOs para llevar a cabo una protección de la información efectiva, ya que el perímetro ya no existe. Otro de los retos es conocer los datos críticos de la empresa. En el caso de una fuga de información, cuáles tendrían un mayor impacto en el negocio y una vez que tenemos claro cuáles son las joyas de la corona realizar las medidas de monitorización y protección pertinentes. El cumplimiento regulatorio exige a las empresas cumplir diferentes normativas según el tipo de datos que manejan, así como los países en los que operan. Se requieren unas medidas de protección y mantener una auditoría de quién accedió a qué datos para informar al regulador. En este contexto, IBM aporta tecnología para ayudar a los clientes alrededor de su seguridad 'data centric'. Con IBM Guardium cubrimos todo el ciclo de vida de la protección de la información, una solución abierta enfocada a monitorizar y auditar los repositorios de bases de datos, sistemas big data, data warehouse o ficheros de diversos fabricantes, así como las distintas nubes del mercado.

ANDRÉS DE BENITO, DIRECTOR DE CIBERSEGURIDAD DE CAPGEMINI ESPAÑA

"DAR UN PASO ATRÁS ES CLAVE PARA UNA ADECUADA ESTRATEGIA DE PROTECCIÓN DE DATOS"

Hay tres aspectos clave a día de hoy que afectan a las organizaciones: el aumento exponencial de la información de la que hacen uso, que dificulta la identificación de los datos críticos, los realmente relevantes para la marcha de tu empresa y a los que hay que prestar mayor atención; la descentralización del dato en diferentes repositorios y de los servicios en la nube; y el aumento de la presión regulatoria, que obliga a las compañías a tomar medidas muchas veces incómodas y difíciles de cubrir.

Desde Capgemini recomendamos a las empresas que den un paso atrás, e intenten verlo todo en perspectiva para saber exactamente qué es lo que tienen que hacer, porque estos proyectos son muy complejos si no se abordan de la manera adecuada. Primero, hay que analizar qué datos tienes y cuáles son los más importantes para tu negocio, las joyas de la corona.

Una vez identificados, analizar cuál es su ubicación, todo el flujo de datos existente, por dónde van a pasar… y en cada uno de esos lugares, cuáles son las mejores medidas para protegerlos; es ahí donde entran en juego las tecnologías a utilizar.

Esta es la última pregunta que se deben hacer las organizaciones, no al revés, y la clave de que el proyecto termine con éxito.

"tenemos un UTM que, además de las funciones de firewall, te aporta un punto más de seguridad en el control y la conexión a Internet. También tenemos otros endpoints de McAfee a nivel de equipos personales".

¿Existe una mayor proactividad de la empresa privada en este ámbito en comparación con la Administración Pública? A esta pregunta responde Miguel Ángel Martínez Gómez, responsable asesor de Seguridad Infor-

ASISTENTES

1 Andrés de Benito, Capgemini | **2** Luis Enrique Fiteni, Dragados Offshore | **3** Iñaki Zabala, Grupo Sepro | **4** Isabel Tristán, IBM | **5** Miguel Ángel Martínez, Ministerio de Agricultura y Pesca, Alimentación y Medio Ambiente | **6** Adrián López, Penteo | **7** Rafael Pastor, UNED

mática del Ministerio de Agricultura y Pesca, Alimentación y Medio Ambiente: "Depende del organismo en cuestión, en nuestro ministerio se puede llevar un ritmo de empresa privada, se puede trabajar a buen ritmo sin cortapisas burocráticas". En este punto ayuda mucho que la persona responsable del Ministerio "está por la labor" y cuenta con el apoyo de la Dirección General. "En mi caso, trabajo en análisis de riesgos y lo hacemos con las herramientas del Centro Nacional de Inteligencia como CLARA (analiza las características de seguridad técnicas definidas a través del Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica)".

Estrategias de seguridad del dato

En principio, su ministerio no tiene una estrategia definida de ciberseguridad y de protección del dato, "nos encontramos en un impasse de búsqueda de aplicativos. Lo que tenemos nos sirve hoy en día, e iremos avanzando poco a poco. Tenemos que renovar 5.000 ordenadores y vamos a ir realizando pequeñas adquisiciones".

En este punto, Isabel Tristán, IBM Security Software Market Leader SPGI (Spain, Portugal, Greece & Israel), comenta que los clientes están preocupados porque cuentan con repositorios de diferentes proveedores, algo que complica la gestión. Y como dato para tener en cuenta, una encuesta de Ponemon Institute señala que desde que se produce una fuga de información hasta que se termina de contener pasan de media 280 días, "por eso resulta muy crítico cómo podemos detectar de forma rápida que la información de tu compañía se está filtrando. Las soluciones tradicionales no son suficientes y hay que dar un paso adicional introduciendo inteligencia artificial para poder detectar de forma más dinámica".

Por su parte, Andrés de Benito, director de Ciberseguridad de Capgemini, aduce que "el problema de las compañía no es tanto cómo proteger los datos, sino saber qué datos tiene que proteger, la criticidad de los mismos y su importancia para la organización; así como las normativas y regulaciones que inciden sobre ellos". Unos proyectos que pueden resultar muy complejos si no se tienen claros los objetivos y a los que hay que aproximarse de forma escalonada.

Fuga de información

La UNED tiene bien claro cuáles son sus datos más críticos, los de sus estudiantes. Este centro dispone de sistemas de información muy descentralizados por lo que, según explica Rafael Pastor, director de la Escuela de Informática, "contamos con una fórmula de trabajo, con herramientas de data analytics para la toma de decisiones. Hay datos especialmente sensibles, como son los vídeos y audios que recogen las cámaras online durante los exámenes, una información muy protegida por GDPR. Tenemos bien separada la parte de gestión del dato y la protección de los activos de información". La UNED también trabaja con herramientas del CCN-CERT como EMMA (desarrollada para agilizar la visualización de activos en una red, su autenticación y segregación, así como la automatización de auditorías de seguridad de la infraestructura). Coincidiendo con la opinión general, Pastor Vargas considera la persona como el "eslabón débil". Se muestra partidario de la motivación y la concienciación, campañas que echa de menos que no sean más frecuentes dentro de la Administración.

Iñaki Zabala, responsable IT de Grupo Sepro, se suma al hilo general del debate: "Estamos subiendo cada vez más cosas en la nube. Tenemos un proyecto muy bonito de SharePoint a la hora de compartir recursos. En cualquier caso, on premise cubre la mayor parte de nuestros sistemas, cabinas de almacenamiento que seguiremos dedicando a backups. La fuga de información siempre ha sido una asignatura pendiente y por fin vamos a cambiar el antivirus a una versión cloud que lleva incluidas muchas herramientas, una de las cuales implica el control de la fuga de información desde las plataformas de intercambio del estilo de OneDrive o WeTransfer". ■

"En nuestro ministerio se puede llevar un ritmo de empresa privada, se puede trabajar a buen ritmo sin cortapisas burocráticas"