El *backup*: tecnología "tradicional" para liderar la protección del dato

Señalada, hace años, como una tecnología de escasa innovación y poco valor, el *backup* ha sabido reivindicar su función esencial en las estrategias de seguridad de las empresas. En los dos últimos ejercicios, el despliegue masivo del teletrabajo y el aumento del consumo de aplicaciones y servicios en la nube provocaron que la protección del dato fuera la prioridad número uno. Con ella, el *backup* se convirtió en pieza imprescindible en los despliegues de seguridad de las empresas. Una reivindicación a la que han contribuido fabricantes como Cohesity, que ha hecho del *backup* bandera de negocio.

Marilés de Pedro

El *backup*, con una larga trayectoria en el mercado, se ha consolidado como una tecnología que protege eficazmente el dato. Las empresas deben tener en cuenta que en cualquier momento sus datos pueden estar en peligro ante diferentes amenazas, por lo que deben contar con un plan respaldado por las soluciones tecnológicas, los conocimientos y los procesos adecuados, algo que garantizará que, en caso de crisis, se puedan recuperar los datos rápidamente, evitando la discontinuidad de negocio. Un plan en el que el *backup* se torna en un elemento esencial. "El respaldo es un elemento importante en la continuidad de la producción de una empresa", señala Luis Gil, *brand manager* de Cohesity en Arrow.

"Hoy en día es imposible que una empresa no tenga una copia de seguridad con una política de recuperación rápida", valora. Una copia de seguridad plus que "debe ser inmutable, a prueba de manipulaciones, ya que los atacantes 3.0 atacan primero la copia de seguridad para evitar el retroceso".

Complejo panorama

Uno de los principales problemas es que las compañías carecen, en muchos casos, de una verdadera estrategia de gestión y protección a lo largo del ciclo de vida del dato. Otras cuentan con políticas de *backup* incompletas, que no incluyen una copia externalizada; y muchas otras restrigen la protección únicamente a la información de los servidores. En definitiva, no solo se trata de optar por la solución adecuada, sino de entender la problemática del *backup* y planificar una estrategia que defina la manera de llevar a cabo esta tarea. "Las empresas no valoran, en toda su dimensión, el uso de soluciones más completas, que no tienen por qué ser más complejas", puntualiza Luis Gil. Se trata, explica, de soluciones que permitan un RTO (*Recovery Time Objective*) y un RPO (*Recovery Point Objective*) más óptimos para la continuidad de negocio.

> "El *backup* es la última línea de defensa"

Algunas compañías siguen haciendo *backup* de los distintos silos de almacenamiento. La explosión del teletrabajo ha dejado en evidencia las carencias que existen en la protección de los puestos de trabajo. Aunque los datos críticos deberían de estar en un repositorio corporativo y usarse escritorios virtuales, la realidad es que muchos empleados trabajan en local y guardan datos críticos para la organización en sus propios dispositivos, lo que resulta muy peligroso ante un ataque de *ransomware*. "Ante el in-

"Hoy en día es imposible que una empresa no tenga una copia de seguridad con una política de recuperación rápida"

cremento de este tipo de ataques, las compañías deberían tener soluciones solventes para recuperar la operatividad en el menor tiempo y con el menor impacto posible", insiste Gil. "El *backup* es la última línea de defensa".

Algunas empresas cuentan con políticas de *backup* incompletas, que no incluyen una copia externalizada. No pueden acceder físicamente a su copia en local. Unas carencias que se hacen mucho más visibles en la actualidad, por el riesgo que supone el aumento del teletrabajo con conexiones poco o nada seguras, y porque los ataques de *ransomware* siguen creciendo cada día. "Cada vez hay más conexiones al sitio principal con datos críticos que hay que proteger", analiza. "La copia de seguridad debe ser confiable, rápida (también en la restauración) y protegida con características específicas, como MFA, RBAC, etc.".

Los ciberdelincuentes siguen haciendo uso del "tradicional" *phishing* como el método preferido para lanzar sus ataques de *ramsonware*. Si lo hacen a través del correo electrónico, resulta más "sencillo" para el usuario comprobar la dirección antes de abrir un enlace, sin embargo, en los servicios de mensajería instantánea no se espera una intervención maliciosa y, como consecuencia, es más fácil que un *hacker* se haga pasar por alguien que no es. Un clic equivocado puede costarle a una compañía miles e, incluso, millones de euros. "Los datos son el oro negro de una empresa", recuerda. "Si un correo electrónico puede representar un proyecto de varios millones de dólares, entonces, ¿qué hacemos cuando perdemos este correo electrónico y no podemos recuperarlo?", pregunta, con tino, el responsable de Cohesity en Arrow.

Creciente concienciación

A pesar de este complejo panorama, según Luis Gil cada vez hay más empresas que se han dado cuenta de que la copia de seguridad es imprescindible. "Las instantáneas no son copias de seguridad con restauración granular", recuerda. Los ataques que han sufrido han provocado que las empresas revisen su copia. "Debe ser un *backup* fácil de implementar y usar, con una interfaz única HTML5", relata. "Capaz de llevar a cabo restauraciones potentes, simples, automáticas y PIT (*Point in time*)". Las empresas deben entender, como paso básico, la problemática del *backup* y planificar una estrategia que defina la manera de

llevar a cabo esta tarea. La pregunta clave que debe hacerse la empresa es qué plan de contingencia tiene para proteger su *backup*. Tan importante es la metodología del *backup* como la tecnología. Una filosofía que debe incluir un análisis del *backup* y de las necesidades del cliente. "No disponer de buenas estrategias para desplegar un eficaz plan de recuperación ante desastres es otro grave error", completa.

Propuesta de Cohesity

Nacida en 2013, Cohesity disfruta de un variado plantel de clientes de todos los tamaños. Su fundador es Mohit Aron, uno de los fundadores de Nutanix, que trabajó, como ingeniero en Google, siendo el creador del Sistema de Archivos de la compañía.

El proveedor cuenta con el respaldo de Google Ventures, Qualcomm Ventures, Sequoia Capital y Softbank Vision Fund. Su llegada a España se produjo en 2019.

La propuesta de Cohesity se orquesta a través de una solución de *backup* y almacenamiento secundario, inmutable a ataques de *ransomware*, *cloud* nativa y fácilmente escalable. Se trata de una solución muy sencilla de implementar y de gestionar, creada en el siglo XXI para los nuevos desafíos generados por la explosión de la información actual.

La compañía basa su propuesta en la gestión del almacenamiento secundario desde una única plataforma, que se vio fortalecida con la compra de Imanis Data, en 2019, un proveedor de software de respaldo de base de datos que protege entornos NoSQL, como MongoDB, y de tipo Hadoop.

Los datos secundarios juegan un papel importante en las operaciones de una empresa. Resulta fundamental su gestión y almacenamiento, aunque los usuarios no acceden, de manera regular, a los mismos. Cohesity consolida silos de almacenamiento secundario en una plataforma de datos hiperconvergente y *web scale*, que permite a las empresas aplicar la máxima de pagar en función de sus necesidades; y abarca tanto nubes privadas como públicas. "Cohesity consolida la infraestructura del cliente", explica Gil. "En una sola plataforma de BU de carga de trabajo, con multiprotocolo NAS (*SMB*, NFS, S3) para volcados de registro del directorio principal de intercambio de archivos". La copia de seguridad, especifica, no es

solo un seguro. "También los datos ingeridos pueden ser utilizados por aplicaciones implementadas a través de *marketplace*, como es el caso de antivirus, enmascaramiento de datos, Tenable, Varonis, etc.". La marca cuenta con alianzas con HPE, Cisco, Dell, Lenovo y Fujitsu.

La marca divide su oferta en Dataprotect (BU software) y Smartfiles (con funcionalidad NAS), lo que la habilita para realizar copias de seguridad y restauraciones masivas y rápidas (DATAPROTECT), NAS Smartfiles y detección de anomalías.

Alcanza a todo tipo de empresas (*SMB*, *mid-market* y *enterprise*) y entornos (multisitio, híbrido y multinube).

Además de ofertar la fórmula de *backup* tradicional, Cohesity cuenta con una propuesta de BaaS (*Backup* como servicio), desplegada en AWS. Su solucion DMaaS (Data Management as a Service), ademas de incluir el *backup* como servicio incluye otras funcionalidades adicionales bajo esta misma fórmula. "A través de una única consola, Helios, se aplica una sencilla gestión y gobernanza del dato".

Política de canal

La estrategia de Cohesity transcurre en su totalidad a través del canal. Una estrategia en la que Arrow juega un papel esencial y que cuenta con un red de distribución conformada por 15 compañías que cuentan con un perfil de integradores y profundos conocimientos en el entorno de la proteccion del dato. "A través de Arrow garantizamos una extension del equipo de Cohesity en España", explica Luis Gil. "Desplegamos los conocimientos necesarios para entender y responder a las necesidades planteadas por los clientes".

Gil está convencido de que la oferta de Cohesity responde a la perfección a los retos que se abren en la protección y gestión del dato. Destaca, sobre todo, la versatilidad y la sencillez en su despliegue, "pudiéndose desplegar tanto en un formato *onpremise* como en un entorno de *cloud* nativa".

Los *partners* gestionan la totalidad del proyecto, desde la preventa hasta la implementacion de las soluciones y siempre cuentan con el apoyo del fabricante y de Arrow. "Se trata de una solucion rompedora y muy diferencial frente a los tradicionales fabricantes *legacy* de *backup*".

El *ransomware*, el peligro que no cesa

El ascenso del *ransomware* no es ningún secreto. Un panorama que sitúa al *backup* en primer plano. Datos como los recogidos en el "Informe sobre el estado global del *ransomware* 2021", publicado por Fortinet, lo dejan claro. El estudio muestra que dos de cada tres organizaciones han sido objeto de, al menos, un ataque de este tipo. Asimismo, el 85 % de las compañías encuestadas por el fabricante está más preocupada por un ataque de *ransomware* que por otras ciberamenazas.

La pérdida de datos lidera el ranking de preocupaciones en relación con un ataque de *ransomware*. Le sigue, de cerca, la pérdida de productividad y la interrupción de las operaciones. Además, el 84 % de las organizaciones declaró tener un plan de respuesta a incidentes y el seguro de ciberseguridad formaba parte del 57 % de esos planes. Ante la pregunta sobre pagar o no el rescate, el 49 % reconoció que pagaría directamente, mientras que un 25 % afirmó que su decisión dependería del valor de dicho rescate.

Un riesgo que se percibe, a nivel mundial, como el principal problema de un ataque de este tipo. Y es que actualmente el *ransomware* quita el sueño a las compañías de todo el mundo. Pero el estudio de Fortinet desvela algunas diferencias en el nivel de preocupación entre algunas regiones. Por ejemplo, Asia Pacífico Japón y Latinoamérica son las más preocupadas por esta ciberamenaza (98 %), le sigue EMEA (95 %) y después Norteamérica (92 %).

El pago de los rescates es otro elemento digno de estudio. Según un informe de Kaspersky sobre el *ransomware* en España, el 32 % de las víctimas de este tipo de ataque pagaron el rescate para recuperar el acceso a sus datos. A pesar de pagar por sus datos, el 13 % no recuperaron los datos robados.

El informe señala que, a pesar de estos datos, los consumidores españoles están más concienciados que la media porque en términos globales el 56 % cedió a la extorsión.

En el caso de las víctimas españolas, tanto si pagaron como si no, solo el 11 % pudo recuperar los archivos cifrados o bloqueados tras un ataque. El 47 % perdió al menos algún archivo, el 40 % una cantidad significativa y el 32 % un número pequeño; mientras que el 1 % de los que sufrieron un incidente perdió casi todos sus datos.