Texto
Laura del Río

LA CLOUD ABRE PUERTAS EN TODOS LOS ÁMBITOS, TAMBIÉN EN SEGURIDAD

¿Están los CISO en la nube?

<< Los responsables de ciberseguridad llevan tiempo predicando sobre la importancia de incorporar por defecto la seguridad a todas las áreas de la empresa, pero ¿han tenido en cuenta los CISO los entornos complejos creados en la nube?

VÍCTOR MOLINA, CHANNEL & TELCO SE TEAM LEADER DE CHECK POINT ESPAÑA

SOLUCIONES COMPLETAS PARA ENTORNOS CLOUD COMPLEJOS

Los entornos creados en cloud son marcos con nuevas capacidades, dinámicos, donde prima la operatividad, el time to market y el despliegue rápido. Este crecimiento, muchas veces, compromete la seguridad, no porque no exista la tecnología para securizar estos entornos, sino porque nos olvidamos de aplicarla de la misma manera que en los ecosistemas on premise.

En Check Point contamos con las tecnologías y el talento necesarios para implementar de manera flexible la seguridad, tanto en la cloud pública y en las micronubes que se pueden crear dentro de esta, como en on premise y en entornos serverless o de contenedores.

Check Point ofrece una configuración avanzada para blindar las cargas de trabajo, la seguridad en red, las aplicaciones web y todo tipo de entornos complejos manteniendo una visibilidad total y una postura de seguridad continua.

JULIO GARCÍA, ENTERPRISE SECURITY EXECUTIVE DE MICROSOFT

CLOUD, DE ACTIVO A PROTEGER A FACILITADOR DE LA CIBERSEGURIDAD

Microsoft enmarca la seguridad en la nube dentro del contexto de la digitalización. Avanzamos hacia un modelo híbrido multicloud que, igual que TI y Negocio, precisa de una transformación del área de Ciberseguridad.

La cloud está pasando de ser una extensión del modelo on premise a tener mayor peso dentro de las organizaciones. Es importante cambiar de perspectiva y dejar de ver la nube no solo como un activo a proteger, sino como una potente herramienta que ayuda a securizar los demás entornos empresariales.

La cloud nos permite manejar grandes volúmenes de datos, aplicar machine learning y automatización a los procesos de forma que se reduzcan los tiempos de respuesta a los ataques y, por tanto, el riesgo de estos; aplicar un modelo Zero Trust basado en identidad y securizar nuevos servicios con la agilidad que el negocio requiere.

La nube también favorece un uso eficiente del presupuesto de seguridad, reduciendo los costes de integración, despliegue y operación.

Las capacidades de Azure posibilitan la consolidación en una plataforma de seguridad cloud que aumenta la agilidad y reduce los riesgos y los costes.

La cloud aporta una agilidad, escalabilidad y accesibilidad excepcional a los negocios, pero esto también influye en la creación de ecosistemas complejos, de rápido crecimiento y con un perímetro abierto difíciles de securizar. Los CISO de compañías de diversos sectores hablan sobre cómo afrontan la seguridad en los nuevos laberintos cloud en el encuentro de Computing, organizado junto a Check Point, Microsoft y T-Systems.

La migración a la nube avanza sin prisa pero sin pausa. La accesibilidad a los sistemas deslocalizados de las compañías con sedes en otros países ha aumentado exponencialmente gracias a la cloud. Este aumento "ha evitado la generación de cuellos de botella en los servicios centrales", afirma Alberto López, IT & Cybersecurity Manager de Solaria Energía. "El entorno on premise está pasando a ser una extensión de la cloud. Estamos realizando despliegues en Azure, pero vamos muy despacio ya que a cada paso extendemos la seguridad de extremo a extremo". La compañía cuenta con un CyberSoc, "cuyos sistemas están conectados a la red 24/7 y tenemos muy controlado el perímetro y los equipos que poseen cada uno de nuestros 135 empleados".

Existen empresas que no tienen oficinas internacionales, pero sí clientes que manejan

ÁNGEL OTERMIN, HEAD OF CYBER SECURITY BUSINESS DE T-SYSTEMS IBERIA

TECNOLOGÍA Y PARTNERSHIPS PARA UNA VISIÓN HOLÍSTICA DE LA SEGURIDAD

T-Systems es una compañía integradora que, mediante la implementación de tecnología clave y el establecimiento de sólidos partnerships con hiperescalares, acompaña a los clientes en su viaje hacia la nube aportando una visión holística e integral del proceso. Desde la compañía certificamos a nuestros equipos en la gestión de tecnologías como la de Check Point y aprovechando las capacidades de seguridad de los hiperescalares y su arquitectura en la nube, como ocurre con nuestra alianza con Microsoft.

En T-Systems realizamos una adecuada monitorización de los sistemas, tanto en la nube como on premise, para dar respuesta a las incidencias en tiempo real; somos proactivos en el cumplimiento de las políticas de seguridad, contando con las certificaciones de partners y terceras empresas, lo que nos permite dar servicio a entidades públicas; y aplicamos un enfoque Zero Trust que permite al usuario acceder a las aplicaciones en cualquier momento, lugar y dispositivo, eliminando el uso de VPN pero implantando una conexión intermedia entre usuario e infraestructura que protege el aplicativo.

sistemas de muy distinta naturaleza. "En Haya Real Estates nuestros principales clientes son entidades bancarias que poseen datos sensibles, diversos sistemas y aplicaciones y, además, están muy sujetas a la regulación, lo que nos obliga a actuar siempre acorde a la normativa", cuenta Javier Sánchez, CISO de la compañía. "Los servicios de caja negra en cloud -de los que hay que tener muy controladas las entradas y salidas, es decir, su interfaz- los gestionamos nosotros. Sin embargo, otro tipo de servicios de los que hay que controlar más su funcionamiento interno y no tanto su forma de interactuar con los demás sistemas, los gestiona, en muchas ocasiones, un tercero", explica el CISO. En Haya Real Estates no poseen sistemas heredados, "todo lo nuevo que vamos implantando lo hacemos mediante soluciones modernas en la nube con la seguridad por diseño y aplicando monitorización y regulación".

> **"El despliegue en la cloud es tan ágil que a veces aplicamos la seguridad de manera liviana"**

El paso de on premise a la nube conlleva la convivencia de ambos modelos durante un periodo de tiempo, la mayoría de las veces indefinido, que los CISO han tenido que aprender a gestionar. "Durante los últimos seis años, en Roche hemos combinado las soluciones locales con las de la nube siguiendo los estándares de seguridad. Esto ha sido posible gracias al entrenamiento en esta nueva tecnología y la concienciación de todos los equipos de la compañía", dice Jairo Serrano, IT Security Manager de Roche – Diabetes Care. Al igual que el sector financiero, el de Pharma está muy regulado, "un factor que obliga a someter las cajas negras creadas en la cloud a unos controles de seguridad muy específicos y que, muchas veces, retrasan la adopción de esta tecnología".

La ventaja de los sectores más regulados es que también son los más concienciados en materia de ciberseguridad. "En WiZink Bank somos nativos digitales, no tenemos sucursales, por lo que nube siempre ha jugado un papel fundamental en nuestra estrategia", afirma Luis Ballesteros, CISO del banco. Para Ballesteros, "la pregunta ya no es ¿subo a la nube o no?, sino ¿cuándo subo a la nube?". La cloud brinda la oportunidad de gestionar la seguridad de manera más eficiente. "En WiZink tenemos un CyberSoc y soluciones de monitorización en la nube que también aplicamos al entorno on premise".

Precisamente, la monitorización es considerada el punto débil de la estrategia de ciberseguridad por algunos expertos. Francisco García, CISO de Palladium Hotel Group, habla del extenso perímetro de sus sistemas -"cada complejo hotelero es como una miniciudad"-, que dificulta la monitorización, por no hablar

ASISTENTES

1 José Fernández, Autoridad Portuaria de Valencia | **2** Javier Sánchez, Haya Real Estate | **3** Martín de Riquer, Médicos Sin Fronteras | **4** Jesús Lizarraga, Mondragon Unibertsitatea | **5** Francisco García, Palladium Hotel Group | **6** Jairo Serrano, Roche – Diabetes Care | **7** Alberto López, Solaria Energía | **8** Luis Ballesteros, WiZink Bank

de los problemas de acceso a Internet existentes en algunos países. "Crear un entorno híbrido y multicloud nos ha permitido unificar aplicaciones para monitorizarlas más fácilmente". No obstante, el CISO advierte de los problemas que puede crear relajar las medidas de seguridad en la nube: "El despliegue en la cloud es tan ágil que a veces aplicamos la seguridad de manera liviana".

La alineación clave: cloud, CISO y organización

El equipo de seguridad debe encargarse de que un proyecto cumpla todos los protocolos antes de pasar a producción, pero, en ocasiones, esto hace que las compañías consideren a los responsables de ciberseguridad stoppers de los proyectos en la nube. "La seguridad debe verse como una oportunidad de entregar más funcionalidades en menos tiempo", indica Jesús Lizarraga, CISO de Mondragon Unibertsitatea. El desarrollo de múltiples proyectos en los que intervienen distintas personas "requiere de una visión holística de la gestión de estos". Otro obstáculo importante a la seguridad en la cloud es la creencia de que la responsabilidad de esta recae 100% en el proveedor: "La responsabilidad es compartida entre empresa y proveedor, y hay que dejar muy claro hasta dónde llega cada una".

Los CISO tienen que alinear su estrategia con los objetivos de la organización. "Hacer que el negocio se desarrolle bajo unos estándares de seguridad sin ser un stopper para este", es como define Martín de Riquer, Head of Information Security de Médicos Sin Fronteras, los malabarismos que tienen que hacer los expertos en ciberseguridad. "Para una organización que nunca ha tenido a más del 5% de los empleados dentro de un perímetro acotado, la gestión de identidades, la seguridad Zero Trust y la convergencia de redes ha sido como poder hacer magia", celebra el CISO. "Actualmente estamos trabajando en la seguridad predictiva, esencial cuando actuamos en emergencias, y en diseñar una política de seguridad común para nuestros modelos SaaS, PaaS e IaaS".

La estrategia de seguridad de una empresa tiene que incluir los requerimientos aplicados a los productos adquiridos a terceros. "Para el sector público es crítico escoger un proveedor de referencia certificado según el Esquema Nacional de Seguridad. Proveedor que, a su vez, tiene que trabajar con partners que también cumplan estas medidas, y así se cierra el ciclo", señala José Fernández, CISO de Autoridad Portuaria de Valencia. La parte colaborativa y ofimática es la más fácil de subir a la nube; sin embargo, "la Dirección aún no ve la necesidad de migrar ciertos sistemas core de negocio, pero cuando maduremos en esta tecnología, será un paso inevitable". "La seguridad la establecen los CISO y la agilidad, la Dirección", matizan en el encuentro. La agilidad es un elemento crítico que no puede ir en contra de la seguridad, pero por mucho que intentes avanzar rápido, la seguridad en los procesos lleva su tiempo.

Pasar de una nube a otra es una cuestión que también preocupa a los CISO. "Cada nube tiene diferentes métodos de configuración y esto dificulta el mantenimiento de los estándares de seguridad cuando se desea cambiar de proveedor cloud". Por este motivo, los proveedores ofrecen cada vez más herramientas que contienen plantillas de medidas y procedimientos de seguridad para seguirlos sin perder agilidad.

Para adelantarse a las demandas de agilidad del negocio y la Junta Directiva, el equipo de ciberseguridad necesita cambiar ciertas maneras de hacer las cosas. Igual que el área de Negocio ha experimentado una transformación cultural y metodológica en los últimos años, los CISO deben empezar a incluir la seguridad by desing, creando modelos dinámicos y haciendo análisis de código automáticos aplicables a las fases previas del desarrollo de productos, entre otras acciones. Así se ahorra tiempo, esfuerzo y recursos.

La seguridad está alcanzando la velocidad del negocio. Ser considerada como un factor integrado en cualquier actividad empresarial fomenta que pierda rigidez y gane eficacia, marcando el camino más que los límites. ■

"La seguridad la establecen los CISO y la agilidad, la Dirección"