No abras tu puerta al cibercrimen

LA RESPONSABILIDAD DE LA SEGURIDAD RECAE EN LA EMPRESA, NO EN EL PROVEEDOR

Texto R. Contreras
Fotografía Santiago Ojeda
Vídeo Jorge Pariente

La ciberseguridad consiste en una carrera sin freno ni respiro para los buenos, en sus intentos de minimizar el acoso de los malos. Una carrera marcada por una evolución tecnológica frenética y con un horizonte que da vértigo si se mira hacia la computación cuántica. De la misma manera, la inteligencia artificial ha venido a reforzar las defensas de las organizaciones, por su capacidad de aplicación holística, pero a cambio también está a disposición de los ciberdelincuentes, que son los que marcan el ritmo de este juego 'perverso'. De ahí que el reto de fabricantes y CISO es tratar de ser cada vez más innovadores e intentar anticiparse a los dictados del mundo del malware. En este escenario converge el mundo del cloud, como una masa gigantesca transversal plagada de servicios que también son codiciados por el mundo oscuro. Para los expertos reunidos en la tertulia organizada por Computing en colaboración con Sophos en torno a los nuevos paisajes de la ciberseguridad, se convino que "la nube es una oportunidad, si bien todavía tiene muchos aspectos por depurar". Surgen varios interrogantes: ¿qué tipo de nube usar?, ¿qué servicios?, ¿cómo compaginar la regulación bancaria? ¿continuidad de negocio?... Pero queda claro que la tendencia del consumo es ir a un 'modelo Netflix', con aplicaciones en cascada, donde la nube reina.

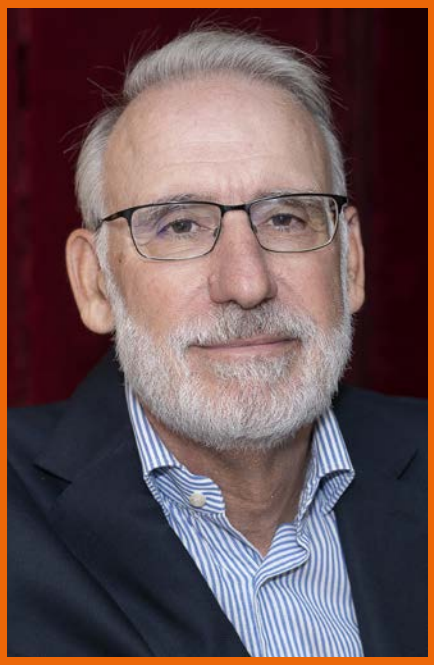
Una entidad como Rural Servicios Informáticos está subiendo su correo al cloud y está definiendo su estrategia para ver qué tipo de aplicación aloja en la nube. Aparentemente, el cloud aparece revestido de una mayor solidez, pero como se dejó caer en la mesa: "Los servicios en la nube son como tener una caja fuerte robusta pero con las llaves puestas". Se pueden tener los mejores servidores, pero ser vulnerables. Se puede definir la seguridad por defecto y por diseño en los productos, pero cuando un servicio se migra a la nube hay que repensarlo todo. Otro contertulio habló más de "necesidad que de oportunidad". Traer nuevas tecnologías no supone que sean más seguras, "hay que parametrizarlas, personalizarlas y ajustarlas al servicio requerido". Es el caso del correo en la nube que puede contratarlo cualquiera por poco dinero, pero el hecho de que los usuarios puedan acceder al mismo desde cualquier sitio multiplica los posibles vectores de ataque. La nube no es una opción, hay que ir hacia ella, pero hacerlo en buenas condiciones. Por otro lado, la nube permite resarcirnos de ataques y vulnerabilidades anteriores, frente al mundo on premise que es más estático.

Las empresas del encuentro están convencidas de la necesidad de usar Software as a Service por su disponibilidad y escalabilidad, pero reconocen que "falta conocimiento de la nube". Es preciso recurrir a expertos para evolucionar adecuadamente en el mundo cloud.

"Y como siempre el dedo acusador recae en el usuario, ese tan manido débil eslabón de la cadena, que por desconocimiento, bisoñez o mala fe nos abre las puertas de la caja fuerte"

RICARDO MATÉ SALGADO, COUNTRY MANAGER DE SOPHOS IBERIA

"NUESTRO MODELO DE SEGURIDAD SINCRONIZADA PERMITE EVITAR CUALQUIER ATAQUE"



"En los dos últimos años hemos visto que se está produciendo un incremento de los ataques dirigidos hacia todo tipo de empresas, desde pequeñas, medianas, grandes corporaciones, AAPP… y estos ciberataques son muy sofisticados. Por ejemplo, desde Sophos Labs estamos viendo un repunte del malware Emotet, puerta de entrada del ransomware Ryuk. En España en concreto, varios ayuntamientos han sido víctima de este ransomware. Muchos de estos ataques se producen los viernes por la tarde cuando los organismos son más vulnerables y disponen de menor capacidad de respuesta".

Desde Sophos recomendamos cubrir las buenas prácticas habituales, no clicar en cualquier correo desconocido, formar a los usuarios, pero además montar soluciones de protección más avanzadas como es el caso de Sophos Intercept X.

Si nos vamos hacia la nube pública, vemos que hay cada vez más servicios y estos grupos de delincuentes están escaneando todos ellos, y si no están protegidos tales servicios, en cuestión de pocos segundos se producen los ciberataques. Montamos un experimento con una serie de bots y comprobamos que en 54 segundos estos web services ya habían sido atacados. En este caso recomendamos herramientas como nuestra Cloud Optix para proteger todos los datos y aplicaciones que residen en cloud computing. Un mensaje de tranquilidad a los CISO: Hay soluciones para evitar los ciberataques, desde Sophos ofrecemos seguridad end to end gracias a nuestro concepto de seguridad sincronizada, por el que todo ataque que localizamos, ya sea en un móvil, CPD, perímetro, etc., somos capaces de detectarlo y tomar medidas predictivas.

"Todo este tipo de problemas complican la agenda del CISO, que mira con esperanza la inteligencia artificial como futuro gran aliado"

En este punto, empresas como Sophos pueden ayudar a las compañías identificando todos los activos que tiene en la nube pública, "el Shadow IT es una plaga y no puedes proteger algo que no conoces". La herramienta Cloud Optix se conecta a Azure, Google Cloud o AWS y clasifica los activos y vulnerabilidades en tiempo real.

Cambio de paradigma

Trabajar en la nube implica "cambiar de paradigma", sostienen estos expertos, "hay que aprender a monitorizar y madurar en la gestión de las aplicaciones". Tampoco estar en la nube garantiza la 'inmunidad', no te otorga la seguridad por defecto; "si tu política de contraseñas es nimia y no parcheas estás abriendo tus defensas".

Otro aspecto clave es que, en la cadena de responsabilidades en caso de un siniestro, es el CISO el que está por delante: "Los proveedores de cloud prestan un servicio que no tiene por qué ser seguro. Cuándo subes algo a la nube, ¿de quién depende la seguridad?, una cuestión que no todo el mundo tiene clara. El proveedor de nube pública, que se dirige a un mercado masivo, ofrece su catálogo a las compañías y estas son las que deciden lo que contratan. El usuario particular suele anteponer la usabilidad a la seguridad, pero las empresas no pueden dar por válido este comportamiento, hay que tratar de ir hacia factores de protección más sofisticados como el doble factor de autentificación o los sistemas de acceso condicionales.

En cualquier circunstancia, la responsabilidad es coto exclusivo de la empresa que contrata. En el caso de las entidades financieras, el Banco de España exige análisis de riesgos antes de poner un servicio en la nube. Fueron los proveedores de nube pública los que vendieron la idea de que "la nube es segura", y al mismo tiempo compartieron el mensaje de la seguridad compartida: "Nosotros somos responsables de que la infraestructura esté respaldada y dar continuidad de servicio, pero lo que el usuario aloje en la nube está en su esfera de responsabilidad". Y es que una configuración errónea puede dar pábulo a ataques fulminantes por parte de los hackers a la sombra.

Estas carencias demuestran la necesidad de implantar una estrategia para definir qué tipo de información o no debe situarse en la nube. En el caso de las ingenierías, perder un proyecto puede traducirse en el drama de echar por el desagüe muchos millones de euros. "La nube está muy bien para ahorrar costes, transferir riesgos y mejorar la seguridad, pero esa infor-

ASISTENTES

1 Bergé, Antonio Antúnez **|** **2** Fintonic, Javier Tobal **|** **3** División Industrial de Técnicas Reunidas, Carlos Asún **|** **4** Comar Madrid, Alberto López **|** **5** Prisa, Julio Collado **|** **6** Rural Servicios Informáticos (RSI), Pedro Pablo López **|** **7** Solvia, Manuel Barrios **|** **8** Sophos, Álvaro Fernández **|** **9** Wizink, Luis Ballesteros

"El proveedor de nube pública, que se dirige a un mercado masivo, ofrece su catálogo a las compañías y estas son las que deciden lo que contratan"

mación muy crítica para el negocio yo nunca la subiría a la nube, la tendría en casa bastante aislada", argumentó uno de los intervinientes, para matizar: "Nuestro departamento comercial es un búnker". Muy distinto es el caso del correo electrónico y de las aplicaciones, que en este tipo de negocios no suponen un riesgo, sino todo lo contrario. Pero esta visión no la compartieron otros tertulianos, para quienes la nube tiene más cosas positivas que negativas. Si bien el concepto de seguridad dinámica se impone más que nunca en este entorno.

Caja fuerte

Durante el encuentro la imagen de la caja fuerte con las llaves puestas sirvió de hilo conductor, porque el nivel de seguridad está en función de cómo se parametrice y de los giros de llave que se den. Y como siempre, el dedo acusador recae en el usuario, ese tan manido débil eslabón de la cadena, que por desconocimiento, bisoñez o mala fe nos abre las puertas de la caja de par para regodeo de los atracadores. En la nube se agudiza esta situación porque provisionar un servicio a veces se hace mediante un par de clics.

La movilidad de las aplicaciones en cloud también es otro aspecto que ocupa y preocupa a las empresas: "Cuando subes una app a la nube tienes que preocuparte de que sean movibles a otro proveedor, especialmente en empresas con miles de empleados". Otro axioma que quedó reflejado es el hecho de que "subir a la nube es muy fácil, pero bajarse no". Algo que es achacable a la falta de estándares en el mercado y de la falta de madurez propia del smartphone, que ha acelerado sustancialmente los procesos de portabilidad.

Todo este tipo de problemas complican la agenda del CISO, que mira con esperanza la inteligencia artificial como futuro gran aliado, pero también estamos en la prehistoria con soluciones incompletas y algoritmos todavía insuficientes. Dado que el usuario es el talón de Aquiles de la seguridad, la IA tiene que ir encaminada a ayudarle en este cometido, sin olvidar campañas de concienciación y cursos personalizados. Una queja que surgió como corolario de la reunión fue la "falta de soluciones en el mercado concebidas para proteger al usuario". Alguien sugirió la idea de crear "un carné de identidad para Internet". Sea como fuere, en la carrera de los buenos contra los malos, lo más aconsejable es no dejar nunca las puertas abiertas. ■