“La microsegmentación es el futuro de la protección del centro de datos”

En Data Center Market hablamos con Carlos Moliner, responsable de desarrollo de Negocio para Iberia en Guardicore, compañía israelí cuya misión es entregar formas más precisas y efectivas de detener las amenazas avanzadas a través de la detección y respuesta de amenazas en tiempo real.

Lucía Bonilla

¿Cuál es la propuesta de Guardicore para el mercado de centros de datos?
Guardicore se dedica a proteger el centro de datos extendido, es decir, tanto la infraestructura on premise como en la nube con todas sus variantes. Guardicore protege el interior de toda la infraestructura. Y es que Guardicore, desde su creación, fue consciente de que desde el interior de las compañías es muy difícil tener una visibilidad de las conexiones que se están generando, lo cual puede suponer un terreno abonado para los atacantes, y es que se suele desconocer con exactitud lo que se tiene. La premisa de Guardicore es dar luz a aquello que permanece oculto, construyendo un mapa en el que se reflejen con claridad todas esas conexiones que se están produciendo, tanto en el centro de datos físico, como el centro de datos en la nube. Sobre ese mapa se establecen áreas aisladas entre sí, para intentar evitar que los atacantes puedan desplazarse entre ellas y expandir cualquier tipo de malware. Llevando este ejemplo al extremo de hacer esos segmentos de red cada vez más pequeños, llegamos al concepto de microsegmentación.

¿Puede detallar el concepto?
Consiste en ir aislando progresivamente los distintos elementos, aplicaciones, sistemas y demás componentes del centro de datos. Tradicionalmente, esto se venía haciendo con herramientas típicas tipo firewalls o WLAN, pero hoy en día lo que es muy útil es la segmentación definida por software, es decir, definir esto que acabo de contar a través de herramientas de software. Una vez que has segmentado, el siguiente paso es controlar cómo se está

> *Casi siempre el objetivo principal es, al margen de la motivación económica, obtener algún tipo de información y destrucción de infraestructuras a gran escala.*

produciendo esa comunicación entre los elementos. Muchas compañías han intentado hacer segmentos de red, separando, pero con poco éxito.

La gran diferencia entre la segmentación definida por software y la segmentación tradicional es que la primera es mucho más rápida y eficiente. Los proyectos de microsegmentación han sido tradicionalmente muy complejos, pero con la microsegmentación definida por software eso se acabó. Lo interesante es que desde un único punto puedes ver y conocer todo el entorno, y desde una única plataforma puedes decidir lo que tiene que suceder y qué conexiones se tienen que producir y cuáles no.

¿En qué consisten las fases del proceso de microsegmentación?

En primer lugar, se despliegan una serie de aplicaciones que se instalan en cada uno de los servidores, y monitorizan la actividad. Pasado ese tiempo, llega el momento en el que se conocen cuáles son todas las dependencias entre las máquinas; es decir, se ve qué máquinas se interrelacionan con otras para saber quién hace qué. Después hay una fase de consultoría y en la última fase se determina cuáles de esas conexiones son legítimas y cuáles no, para emitir una alerta. Es un proceso en el que se recoge información de la infraestructura, después se procesa y finalmente se actúa implementando una serie de reglas.

¿Para qué tipo de amenazas o ataques puede ser útil?

Aparte de la microsegmentación, también tenemos otra serie de funcionalidades que van por encima, y que sirven para detectar ataques. Cuando algún atacante intenta entrar por alguno de los segmentos que hemos creado, las herramientas lo detectan, como puede ser el caso de un ransomware, por ejemplo. Cualquier conexión sospechosa que ocurra en el CPD la vamos a detectar. Lo más interesante es que, además de detectar, somos capaces de prevenir. Y ahí está la clave. Es posible prevenir cualquier extensión de cualquier ataque que penetre en las defensas del perímetro del centro de dato. Por supuesto es complementario a firewalls y demás soluciones de seguridad. Cualquier ataque que consiga penetrar en las defensas y que infecte los sistemas, lo vamos a detectar y cortar, porque vamos a evitar que una primera vez infectado ese primer equipo, el atacante salte a otros equipos.

¿Cuáles son los principales riesgos que puede haber en un centro de datos?

Desde nuestra experiencia, lo más grave son los ataques endógenos. No me refiero necesariamente a un empleado, que también sucede, pero me refiero a que muchas veces un atacante consigue infectar una máquina y a partir de ahí se extiende. El tipo de ataque puede ser muy variopinto y por distintas motivaciones, pero casi siempre el objetivo principal es, al margen de la motivación económica, obtener algún tipo de información y destrucción de infraestructuras a gran escala. De cara al futuro, los ataques con el objetivo de destruir y sobre todo a gran escala de Naciones-Estado se van a incrementar.

¿La nube complica o facilita la gestión de la seguridad de los sistemas?

Lo complicado no es la nube en sí, sino la heterogeneidad de entornos, porque muchas veces lo complicado es saber qué pasa entre ellos. El multicloud genera heterogeneidad y complica. Y es imposible contar con una única herramienta para monitorizar la actividad de cada aplicación y nube. Por eso es necesario desplegar una única herramienta que te facilite una visibilidad de todo el conjunto.