“La ciberseguridad ha de ser un facilitador del proceso de transformación digital”

Miguel Ángel Martos, regional sales director para Iberia e Italia de Zscaler.

Lucía Bonilla

Zscaler adquirió recientemente a Edgewise Networks. ¿Cómo se están materializando los resultados de esta compra? Igualmente, la compañía anunció en abril su intención de adquirir Cloudneeti para reforzar la seguridad en la nube pública. ¿En qué posición está ahora mismo Zscaler? ¿Continuará este intenso ritmo de compras?

Zscaler nació hace 12 años como solución para proteger nuestro tráfico desde y hacia Internet, con una solución basada en cloud. Esto es la línea de negocio llamada Zscaler Internet Access, una plataforma completa de seguridad web que va desde el proxy de navegación, a DLP o CASB, pasando por Next Generation Firewall. Una vez protegido el tráfico desde y hacia Internet, nuestros clientes nos pidieron proteger el tráfico hacia aplicaciones privadas, estén dentro o fuera de su red corporativa, dando lugar a una segunda línea de negocio llamada “Zscaler Private Access”. Y fue un paso natural el de proteger el tráfico de aplicación a aplicación (Este-Oeste), o servidor a servidor, de nuevo, estén estos en entornos físicos o cloud. Esto ha dado lugar a una tercera línea de negocio que hemos llamado Zscaler Secure Apps and Workloads protection. Y dentro de la protección de cargas de trabajo aplicamos técnicas de microsegmentación, aplicamos técnicas de Cloud Posture Management, de acceso restringido de apliaciones y otras muchas más.

La compra de Cloudneeti y de Edgewise, ambas juntas están perfectamente integradas dentro de nuestra oferta y, junto con otros elementos, forman nuestra plataforma de protección de cargas de trabajo, que básicamente es de aplicación a aplicación.

Para terminar la foto, recordemos que primero los clientes nos pidieron proteger usuarios a Internet, después usuarios a aplicaciones, seguido

por aplicaciones a aplicaciones, que es lo que hemos hecho con estas adquisiciones. Pero hay un cuarto paso, una cuarta línea de negocio que hemos lanzado, tiene que ver no con la protección, sino con medir la experiencia de usuario cuando se conecta a cualquier aplicación. Ya no es puramente seguridad, sino experiencia. Si hay retrasos, etc, buscando dónde está el problema.

¿Qué tan segura puede ser la nube?
La nube es tan segura como las medidas que adoptes. La nube en sí no es una única, son muchas, y además hay muchas maneras de acceder a las nubes. Los clientes pueden consumir la nube como una plataforma en la que depositan sus propios servidores, como una plataforma PaaS, pueden consumir aplicaciones desde la nube, pueden consumir la nube como un soporte elástico para desarrollos y que se pueden incrementar o reducir su capacidad en tiempo real, en fin, cada elemento de la nube es tan seguro como las medidas que adoptes para securizarlo.

Lo que sí es importante es que, además de los controles que apliques para securizar la nube, es que la arquitectura que implementes sea adecuada para securizar la nube. Por ejemplo, es muy difícil securizar la nube en un entorno on-premise, por razones obvias. Es muy importante por ello implementar los controles siempre (detección de malware, remediación temprana de brechas, etc.). Nada nuevo, los controles son siempre los mismos, pero además cobra especial relevancia la arquitectura que implementes para securizarla. De ahí que Zscaler tenga especial importancia de proteger la nube no solo con los controles adecuados, sino desde la nube misma, porque no vemos otra arquitectura adecuada para hacerlo.

Pero recordemos siempre que cualquier estrategia de seguridad ha de contar con tres elementos claves: tecnología, procesos y personas.

¿La pandemia ha comprometido aún más a la seguridad de las compañías? ¿Ha habido cambios sustanciales en los últimos meses?
Sin duda. Ha habido más inseguridad y además nos obliga a cambiar la forma en la que trabajamos la seguridad. La pandemia además ha permitido a los "malos" utilizarla como herramienta de distracción para acceder mejor a los sistemas de la empresa. Así hemos visto un importante incremento en ataques de phishing, el uso cada vez más frecuente de ingeniería social, etc.
Pero, además, tener que mandar a los empleados a casa ha aumentado el riesgo de brechas de seguridad, aumentando la superficie de exposición de cualquier empresa. En segundo lugar, la protección de estas formas de trabajar en forma de contingencia, que es lo que sucedió en primavera, ha destapado la realidad de que muchas soluciones que se tomaron no han sido válidas al pasar de un modo contingencia a un modo permanencia.

Ahora las empresas tienen que revisar y analizar si la decisión que se tomó era la adecuada, sostenible en el tiempo, o si deben ir hacia otro tipo de soluciones. En muchos casos la solución ha funcionado perfectamente en ese marco de contingencia, pero hay que analizar si la arquitectura es la adecuada para una solución permanente. Y no solo eso, muchas empresas han empezado a analizar si las decisiones que se tomaron iban en línea con su estrategia de transformación digital.

La ciberseguridad, tal y como la vemos en Zscaler, ha de ser un facilitador del proceso de transformación digital. Un proceso de transformación, simplificándolo mucho, tiene tres fases. Una primera de transformación de las aplicaciones, para llevar al cabo mis aplicaciones, mis servicios de desarrollo, etc. Una segunda que viene de la mano de la transformación de la red desde el momento que el punto final de acceso es Internet. Y el tercer elemento de la transformación es la ciberseguridad, que ha de adaptarse a los cambios de transformación digital. Si no tenemos una ciberseguridad bien definida y alineada con la estrategia de transformación digital de la empresa, y además hemos seguido con esa urgencia, vamos a tener un auténtico problema.

¿Qué novedades de producto puede destacar?
Las novedades más latentes son las que hemos comentado en la primera pregunta con la integración de las dos empresas: protección de cargas de trabajo. También quiero destacar Zscaler Digital Experience. ¿Qué está ocurriendo cuando vamos a la nube y aplicamos la ciberseguridad desde la nube, la capacidad de identificar un problema en la experiencia de usuario es muy baja, porque no sabemos si el problema se debe a la nube, algo típico como un retardo, va muy lenta, o si es un problema del servicio que ofrece el proveedor del cloud, si es un problema del rúter, de la Wi-Fi, si es un problema de Zscaler, que está en medio, etc. Dado que Zscaler tiene protección completa desde el usuario hasta la aplicación final, esto nos permite hacer una trazabilidad de todo el camino intermedio, y tener métricas para saber dónde está el problema que tiene el usuario. Esta es una herramienta tremendamente potente para adoptar un proceso de transformación digital seguro y poder prevenir problemas en la experiencia de uso.