Cisco busca provocar nuevas estrategias con su Reporte Anual de Ciberseguridad 2017

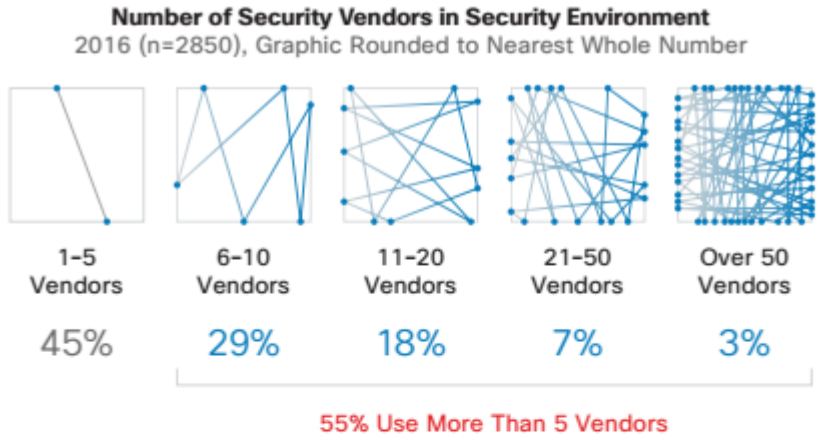
Cisco presentó la décima edición de su Reporte Anual de Ciberseguridad, según el cual 4 de cada 10 alertas levantadas por las soluciones no son atendidas, la mitad de las alertas investigadas resultan legítimas pero apenas el 46% de ellas son remediadas, lo que pone sobre la mesa la necesidad de soluciones inteligentes y automatizadas que puedan disminuir el riesgo de ataques a que las empresas son sometidas.

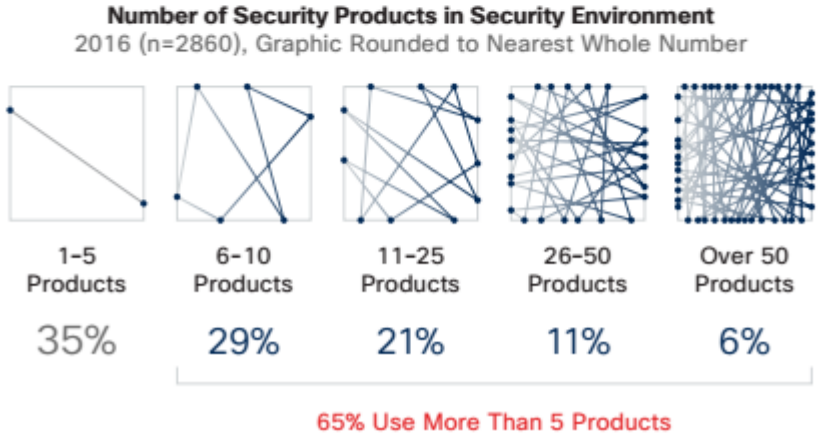
“Hay que provocar una nueva estrategia de seguridad para el negocio, hay dos veredas: cómo defenderse o cómo habilitar el negocio con seguridad. En el mundo de la digitalización las empresas que mejor estén en capacidad de tomar provecho son las que entienden que la seguridad es un habilitador y no un mal necesario o una herramienta sólo de control”, explica Juan Merino, Gerente de Desarrollo de negocios en Seguridad para Cisco Argentina.

El reporte está basado en una encuesta que la compañía levantó entre 3 mil Directores de Seguridad (COS’s) y se complementa de datos obtenidos de la infraestructura de seguridad de la compañía.

De entre los datos relevantes del estudio, destaca que 36% de los encuestados dijeron haber sufrido impactos en la seguridad de sus áreas de operaciones, 30% en las financieras, y 26% tanto en la reputación de marca como en retención de clientes, lo que indica que cada vez más las compañías están notando los efectos de ataques en el potencial de negocio, no sólo en términos más concretos como los recursos desperdiciados por la paralización del sistema o multas por no alcanzar los términos de servicio, sino incluyendo en los impactos la pérdida de oportunidades nuevas o la baja en la calidad del servicio que puede llevar a un cliente a no renovar.

Entre los obstáculos para tener una enfoque de seguridad avanzada, la compañía encontró el presupuesto, temas de compatibilidad, falta de personal entrenado, y la necesidad de certificaciones. Otro obstáculo está representado por la complejidad de los entornos pues 55% de las organizaciones reportaron tener más de 6 e incluso más de 50 distintos proveedores de seguridad, y 65% utiliza más de 6 y hasta más de 50 diferentes productos.





Más de dos tercios de los respondentes, identificaron sus herramientas de seguridad como muy efectivas o extremadamente efectivas, y un 58% siente que su su infraestructura de seguridad está muy actualizada, lo que expertos de Cisco consideran como un exceso de confianza.

Cisco propone un enfoque para minimizar los riesgos de ataques que va desde la adopción de una cultura basada en liderazgo, inversión y transferencia de conocimiento sobre el tema, la actualización, dimensionamiento y auditoría de los sistemas de seguridad, así como la integración de infraestructura pensada en ciberseguridad que incluya la automatización de procesos con el fin de reducir el tiempo de respuesta.

“Lo que más nos llama la atención es la necesidad de los clientes de entender bien la adopción correcta de las soluciones de seguridad, porque aunque la inversión en seguridad es cada vez más fuerte el tema de seguridad sigue con issues básicos de hace muchos años”, comparte Ghassan Dreibi, Gerente de Planeación y Estrategia para Desarrollo de Negocios en Seguridad para Cisco en Latinoamérica.