Cisco identifica las mejores prácticas de seguridad

Cisco publicó su más reciente informe sobre ciberseguridad, Estudio de Resultados de Seguridad Volumen 2 Cisco Security Outcomes Study), en el que encuestó a más de 5,100 profesionales de la seguridad y la privacidad de 27 países, para comprobar las medidas más impactantes que pueden tomar los equipos para defender a sus empresas contra el cambiante panorama de las amenazas.

Los participantes compartieron sus enfoques sobre la actualización e integración de su arquitectura de seguridad, la detección y respuesta a las amenazas y la capacidad de recuperación cuando ocurre un desastre.

El estudio del año pasado reveló que hay cinco prácticas que tienen una gran influencia en la fortaleza general del programa de seguridad de una organización. Entre ellas se encuentran la renovación proactiva de la tecnología obsoleta, la buena integración de las tecnologías de seguridad, la respuesta oportuna a los incidentes, la recuperación rápida de los desastres y la inversión en capacidades precisas de detección de amenazas. El estudio de este año ha analizado con más detalle estas cinco principales prácticas para identificar los factores de éxito. Entre las conclusiones más destacadas se encuentran las siguientes:

Actualización e integración de la arquitectura

- En promedio, el 39% de las tecnologías de seguridad utilizadas por las empresas se consideran obsoletas, por lo que en estos momentos invertir en una estrategia de actualización tecnológica proactiva es más importante que nunca. No es de extrañar que las organizaciones con arquitecturas basadas en la nube tengan más del doble de probabilidades de renovarse que las que tienen tecnologías locales más anticuadas.
- Las empresas con tecnologías integradas tienen siete veces más probabilidades de alcanzar altos niveles de automatización de procesos. Además, estas organizaciones cuentan con una capacidad de detección de amenazas más fuerte en más de un 40%.
- Más del 75% de los programas de operaciones de seguridad que no cuentan con grandes recursos de personal son capaces de lograr capacidades sólidas mediante altos niveles de automatización. La automatización duplica con creces el rendimiento del personal menos experimentado, lo que ayuda a las empresas a superar la escasez de habilidades y de mano de obra.

Detección y respuesta a las amenazas

- No se puede subestimar el valor de las arquitecturas de seguridad basadas en la nube. Las empresas que afirman tener implementaciones maduras de arquitecturas Zero Trust o Secure Access Service Edge (SASE) tienen un 35% más de probabilidades de informar sobre operaciones de seguridad sólidas que aquellas con implementaciones incipientes.

- Las compañías que aprovechan la inteligencia sobre amenazas se mueven dos veces más rápido para reparar los daños causados por las amenazas a la seguridad, que las empresas que no utilizan la inteligencia sobre amenazas.

Mantener la resiliencia en caso de catástrofe

- A medida que el panorama de las amenazas sigue evolucionando, probar la continuidad del negocio y las capacidades de recuperación de desastres de forma regular y de múltiples maneras es más importante que nunca, con empresas proactivas que tienen 2.5 veces más probabilidades de mantener la resiliencia del negocio.
- Las organizaciones con supervisión a nivel de la junta directiva de los esfuerzos de continuidad del negocio y recuperación de desastres que tienen operaciones que residen en los equipos de ciberseguridad son las que obtienen mejores resultados.

“Con el giro hacia el trabajo híbrido, las empresas están lidiando con la creciente complejidad de asegurar una fuerza de trabajo distribuida”, dijo Shailaja Shankar, vicepresidente senior y gerente general del Grupo de Negocios de Seguridad de Cisco. “Al mismo tiempo, también se enfrentan a contar con personal limitado y restricciones presupuestarias, por lo que es fundamental que las organizaciones inviertan en tecnologías y prácticas de seguridad innovadoras. El Security Outcomes Study Volumen 2 de Cisco elimina las conjeturas a la hora de priorizar las estrategias y tecnologías de seguridad. Al invertir en arquitecturas de seguridad integradas y basadas en la nube con un alto grado de automatización, los profesionales pueden responder a las amenazas con mayor rapidez, de modo que pueden centrarse en habilitar el negocio y mantener a los usuarios seguros”.