Simplificar la seguridad

a través de una plataforma en la nube

Los profesionales de TI y de seguridad saben que el panorama de las amenazas es dinámico. Cada día, los atacantes se vuelven más listos e inventan nuevas técnicas para evitar que les detecten. Ahora que los ataques sin programa malicioso y en memoria constituyen el **72 por ciento** de las vulneraciones, los antivirus tradicionales ya no bastan para proteger los sistemas. De hecho, menos de un tercio de las organizaciones creen que los antivirus tradicionales puedan detener los ataques avanzados con programas de secuestro que son tan comunes hoy en día.[2] Para hacer frente a este mayor riesgo, muchas organizaciones han optado por añadir más productos a la pila de seguridad que ya tenían, aumentando así el coste y la complejidad de los entornos. Actualmente, el **60 por ciento** de las organizaciones empresariales usan por lo menos **25 herramientas** diferentes de ciberseguridad para gestionar, investigar y responder a las amenazas a la seguridad.[3] Lamentablemente, esta complejidad no guarda correlación con la eficacia por varios motivos.

1. Demasiados silos Contar con diversas soluciones no es suficiente si no pueden funcionar de forma conjunta. Las organizaciones trabajan con datos, sistemas y consolas que funcionan de forma aislada. En caso de tener que realizar una investigación, los profesionales tienen que trabajar con conjuntos de datos dispares de múltiples soluciones de seguridad. Esto lo convierte en una tarea complicada y dilatada que, en última instancia, no ofrece bastante información sobre el contexto en el que se ha producido el incidente. **2.** Gestión complicada Tener diversos sistemas y productos es una carga para los profesionales de TI y de seguridad. Supone una complejidad excesiva y mucha formación. De hecho, más de la mitad de las organizaciones que tienen implementadas más de 50 soluciones de seguridad definen su coordinación de la seguridad como «muy complicada» y, a causa de esto, casi la mitad (el 49 por ciento) de las alertas legítimas no se corrigen. **3.** Esto implica un riesgo considerable para la organización, ya que las personas dedican menos tiempo a lo importante. **4.** Efecto sobre el rendimiento de los terminales La ejecución de múltiples sistemas acaba sobrecargando a los terminales. Cuantos más agentes se añaden, más lentos se vuelven. Los análisis antivirus y otros modelos de protección requieren una potencia de procesamiento excesiva y, si se produce un problema, la visibilidad limitada que proporcionan estos sistemas supone una importante pérdida de productividad, sobre todo si se tienen que volver a crear imágenes de las máquinas. Algunos usuarios desactivarán por completo la seguridad de los terminales; una situación que, en el mejor de los casos, supone un incumplimiento y, en el peor, abre las puertas a una vulneración grave. La mayoría de los equipos de TI y de seguridad tienen dificultades para contratar suficiente personal de seguridad cualificado.

El 32 por ciento de los profesionales de la ciberseguridad creen que su organización está llevando a cabo las acciones necesarias para hacer frente a los efectos que tiene la falta continuada de conocimientos en ciberseguridad.

5. Además, los profesionales que ejecutan varias soluciones aisladas sobrecargan tanto a su reducido personal que no le permiten ser efectivo.

Con un mercado tan escaso, los recursos cualificados tienen que centrarse en las actividades de seguridad esenciales y no se les debe sobrecargar con la tarea de intentar descifrar la información procedente de varios sistemas dispares. Por si fuera poco tener que abordar estos desafíos en cuanto al personal, además los equipos de TI y de seguridad tienen diferentes exigencias. Sucede con demasiada frecuencia que estos profesionales se enredan en discusiones interminables sobre las concesiones que implica añadir una nueva herramienta de seguridad. Los profesionales de TI centran sus esfuerzos en el rendimiento de las máquinas y la productividad de los usuarios finales, mientras que a los profesionales de seguridad les preocupa tener la información adecuada y el control necesario para detener los ataques y proteger los datos.

Fuente de información:
Revista Byte