SONICWALL

RESUMEN EJECUTIVO

Los desafíos de la gestión de la seguridad de red

Examen de los obstáculos en la gestión de los riesgos, las operaciones y los recursos

Resumen

La rápida implementación de los firewalls y otros servicios de seguridad a través de redes hiperdistribuidas y la necesidad de movilidad en la «nueva normalidad» subrayan la necesidad de una gestión de la seguridad unificada en las empresas de todos los tamaños. Este informe explora las tendencias emergentes y examina los desafíos de la seguridad de red en las áreas de gestión de riesgos, operaciones de seguridad y asignación de recursos.

Introducción

El trabajo desde casa, las redes distribuidas, la migración a la nube y la proliferación de aplicaciones y dispositivos han provocado un aumento de los puntos de exposición. Ya se trate de una pequeña empresa, una empresa distribuida o un proveedor de servicios gestionados de seguridad, la necesidad de proteger un «negocio en cualquier momento y en cualquier lugar» constituye la nueva normalidad.

Al mismo tiempo, las amenazas son cada vez más evasivas. Dado que el incremento interanual de las amenazas no detectadas es de un 145 por ciento,[1] las organizaciones pueden no ser conscientes de qué amenazas se están pasando por alto.

Además, las organizaciones de TI se enfrentan a un aumento de los costes, a la reducción de los presupuestos y a un grupo más escaso de personal cualificado.

En conjunto, estas fuerzas crean importantes desafíos de seguridad de red para que TI pueda contener el riesgo, gestionar las operaciones y asignar los recursos.

Diferentes necesidades

Todas las organizaciones deben comprender e identificar las amenazas en constante evolución. Es necesario que todas conozcan las actividades, el uso y los riesgos de la red. Asimismo, deben supervisar, solucionar y resolver los desafíos operativos y de seguridad. Y todas deben cumplir estrictas directrices internas de seguridad.

Sin embargo, las pequeñas empresas pueden tener recursos técnicos propios limitados. Gestionar la seguridad y optimizar el rendimiento puede resultar abrumador. Si bien las empresas más grandes y los proveedores de servicios pueden contar con su propio personal de seguridad de las operaciones (SecOps), pueden enfrentarse a inquietudes aún más amplias y difíciles. Es posible que necesiten escalar la implementación y la gestión de la seguridad en complejas redes distribuidas. Les preocupa la automatización de la seguridad y la gestión del cambio, los informes de auditoría y la continuidad de las políticas.

Gestión de riesgos

Las organizaciones hoy en día entienden que las cosas pueden pasar de ser normales un día a ser caóticas en cuestión de segundos. El riesgo de ser víctimas de ataques selectivos persiste para muchas organizaciones a medida que las noticias sobre violaciones de red y la exposición masiva de datos siguen ocupando los titulares.

¿Cómo puede saber en qué medida corre riesgo su organización? ¿Existen brechas de seguridad en sus operaciones internas? ¿Qué sucede con los usuarios de su red y los activos, los sitios web y las aplicaciones SaaS que utilizan? ¿Y cómo decide priorizar y abordar estos riesgos?

El tráfico de datos y aplicaciones recorre Internet, los campus remotos, las oficinas remotas e incluso los proveedores externos. Las organizaciones pueden tener una visibilidad y un control insuficientes sobre las actividades de red inseguras, las irregularidades en el tráfico, el acceso y los movimientos inusuales de datos, el *firmware* sin parches, los eventos de seguridad y el estado del sistema.

Los riesgos que no se gestionan pueden dar lugar a algo peor. Una infracción ralentizará el impulso y el crecimiento de una

empresa. Las operaciones se interrumpen porque el personal clave desvía su atención de las prioridades comerciales fundamentales. Los ejecutivos se ven obligados a dedicar todo su tiempo al control de los daños y las relaciones públicas. La imposibilidad de reconocer los riesgos de seguridad obstaculiza la planificación de la seguridad, las decisiones sobre políticas y las medidas decisivas.

Operaciones de seguridad

Los propios firewalls también son puntos de exposición. Una investigación de Gartner[2] sugiere que el 99 por ciento de las brechas de seguridad en los firewalls son causadas por errores en su configuración. A medida que se crean, copian y modifican las reglas del firewall, pueden confrontarse entre sí y provocar consecuencias de seguridad y rendimiento no deseadas. Las configuraciones erróneas y las reglas contradictorias pueden hacer que la red sea vulnerable ante amenazas sofisticadas, accesos no autorizados o intrusiones.

En lugar de rastrear las brechas de seguridad y las vulnerabilidades, podría dedicarse más tiempo a garantizar que las configuraciones de los firewalls no sean excesivamente permisivas y no dejen puertas traseras abiertas a sus infraestructuras. Las organizaciones deben validar y auditar las políticas y configuraciones antes de implementarlas y revertirlas rápidamente si es necesario.

La transición a unas redes multinube más grandes y complejas que admitan más aplicaciones y usuarios constituye un nuevo espacio de trabajo digital. A medida que crecen las redes, gestionar las operaciones de seguridad, optimizar el rendimiento, resolver los problemas operativos y garantizar las medidas de seguridad y controlar el acceso para los usuarios, los dispositivos y las aplicaciones siguen siendo desafíos complejos.

Las organizaciones se esfuerzan por establecer operaciones de seguridad interna adecuadas para cumplir las políticas de nivel de servicio internas. Estas políticas están diseñadas para proteger a las empresas y a sus empleados, reducir los riesgos de seguridad y limitar las responsabilidades financieras y jurídicas.

Al gestionar dispositivos de firewall dispares de forma individual y manual, las organizaciones suelen experimentar incoherencias en las políticas y los procedimientos. No suele haber o son escasos los procesos de análisis, prueba, auditoría y homologación para garantizar que la empresa está aplicando las reglas de firewall correctas, en el momento correcto y de conformidad con los requisitos de cumplimiento internos.

Asignación de recursos

La escasez de talento capacitado en el sector de la seguridad ha hecho que la dotación de personal sea un serio problema. Muchas organizaciones, especialmente las pymes, no disponen de los talentos ni de las habilidades pertinentes en materia de seguridad para mantener los firewalls de manera experta y resolver los problemas graves de seguridad a medida que surgen.

Incluso un solo firewall requiere un mantenimiento planificado periódico, supervisión diaria, revisiones y administraciones de políticas y actualizaciones de firmware. A medida que las redes se expanden y crecen en las empresas distribuidas y las redes de proveedores de múltiples usuarios, la carga que recae sobre el personal de seguridad se multiplica exponencialmente.

Para colmo de males, el personal de operaciones de seguridad puede tener que encargarse de gestionar y operar silos de firewall complejos y fragmentados. Las administraciones suelen ser complejas, engorrosas y laboriosas. Las tareas y los procesos generalmente no se comprueban, no se corroboran y no cumplen los requisitos. Esto desemboca en una situación en la que las redes pequeñas pueden acumular decenas de reglas de firewall a lo largo de muchos años, mientras que las redes más grandes pueden tener miles.

Conclusión

Se necesita una mejor manera de avanzar. Se requieren herramientas de gestión más inteligentes para que los equipos de seguridad hagan su trabajo con eficacia.

La solución Network Security Manager (NSM) de SonicWall le ofrece todo lo que necesita para la gestión integral de los firewalls. Proporciona una visibilidad completa, un control granular y la capacidad para gestionar todas las operaciones de seguridad de red de SonicWall con mayor claridad, precisión y velocidad. Todo esto lo hace desde una única interfaz repleta de funciones a la que se puede acceder desde cualquier lugar utilizando cualquier dispositivo con navegador web.

Más información. Contacte con su representante de SonicWall, o visite www.sonicwall.com/nsm.

Acerca de SonicWall

SonicWall ofrece Boundless Cybersecurity (Ciberseguridad sin límites, sin perímetro) para la era hiperdistribuida y una realidad laboral en la que todo el mundo usa tecnología móvil, a distancia y poco segura. Al conocer lo desconocido, proporcionar visibilidad en tiempo real y posibilitar una economía revolucionaria, SonicWall cierra la brecha comercial en materia de ciberseguridad para empresas, gobiernos y pymes de todo el mundo. Para obtener más información, visite www.sonicwall.com.

[1] Informe sobre ciberamenazas de 2020 de SonicWall
[2] Info Security

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035 (Estados Unidos)
Encontrará más información en nuestro sitio web.
www.sonicwall.com

ExecutiveBrief-TheChallengeOfNSM-US-VG-1965