Ciberseguridad y gestión remota de infraestructura, pilares de la resiliencia de redes

Asegurar la infraestructura de red consiste en velar por la seguridad de todo negocio, una prioridad indudable. Ingenieros de redes y CIO están de acuerdo en que los problemas de ciberseguridad representan el mayor riesgo para las organizaciones que no logran poner las redes en el centro de sus planes de transformación digital. Según una investigación encargada por Opengear, una compañía de Digi International, **53% de los ingenieros de redes y 52% de los CIO encuestados clasifican la ciberseguridad entre la lista de sus mayores riesgos.**

Por otro lado, de acuerdo con Positive Technologies, en 93% de los casos un atacante externo puede violar el perímetro de la red empresarial y obtener todos los accesos locales, ya que **en casi 81% de las organizaciones los permisos se encuentran en la red principal,** por lo que cualquier intruso que ingrese a la red puede hacerse administrador de la infraestructura en tan solo dos días.

Una empresa que dependa de un centro de datos para todas –o parte de sus operaciones– debe contar con medidas de seguridad que protejan la información que circula en su infraestructura de red: Gateways, routers, conmutadores, servidores, firewalls, sistemas de almacenamiento y controladores de aplicaciones que gestionan y almacenan la información proveniente de los usuarios, data que es **materia prima para la empresa a fin de obtener insights de valor y crecimiento y mayor negocio.**

Las preocupaciones son alimentadas por un número creciente de ciberataques. El **61% de los CIO informa de un aumento en ataques y brechas de ciberseguridad en 2020 y 2021** en comparación con los dos años anteriores. En cuanto a la transformación digital, **70% de los ingenieros de redes dice que la seguridad es el área de enfoque más importante, y 31% dice que es su mayor prioridad.**

Opengear | Bárbara Gaxiola- Ronin PR | 555 438 4389 | barbara@roninpr.co
www.roninpr.co

La industria financiera es el área de enfoque crítica en temas de ciberseguridad. Muchas instituciones financieras participan en asociaciones y subcontratan servicios para reducir costos. Al hacerlo, permiten que estas entidades de terceros accedan a datos y sistemas internos, lo que aumenta el riesgo de vulnerabilidades y puede causar una interrupción: **Un minuto de tiempo de inactividad cuesta en promedio 5,500 dólares,** esto es algo que ninguna organización quiere que suceda, por lo que la mayoría gestionan de forma centralizada a terceros, lo que incluye un seguimiento continuo y la creación de protocolos para reducir estos riesgos.

En un mundo hiperconectado, la seguridad de la red presenta un reto mayor a medida que más aplicaciones empresariales operan en las nubes privadas y públicas. Además, los centros de datos tienden a estar distribuidos en muchas ubicaciones, muchas veces fuera del campo de control físico de los sistemas de seguridad.

Durante 2021 se desplegaron más de 600 de estos centros con infraestructuras de híper escala en todo el mundo, según Statista; **México es, cabe mencionar, una de las Top 10 naciones que cuenta con más centros de datos, al sumar 163 de ellos**.

Los CIO tienen muy clara la importancia de todos estos desafíos. Más de la mitad (51%) de los ingenieros de redes dicen que sus CIO les han consultado sobre inversiones en planes de transformación digital, la máxima prioridad en la encuesta. Asimismo, **41% de los responsables de tecnología clasifica la ciberseguridad entre las prioridades de inversión más importantes de su organización** durante el próximo año, y 35% afirma que se encuentra entre las prioridades más grandes en los próximos cinco años. En ambos casos, la ciberseguridad ocupa el lugar más alto que cualquier otro factor.

Más aún, se consideraba que **los costos de daños por ciberdelincuencia alcanzarían los 6 billones anuales para 2021-2022,** según la última investigación realizada por Cybersecurity Ventures.

Según Gartner, el riesgo primario de ciberseguridad es la ampliación de la zona de acceso, que se debe a que 60% de los trabajadores operan de forma remota, lo que lleva a:

- Un mayor uso de la red pública;
- Que las cadenas de suministro tengan que estar muy conectadas;
- Que los centros de datos estén expuestos a nuevas posibilidades de intermitencia o fallo.

Dado que el número de ataques a las empresas es cada vez mayor, la protección del tráfico y la infraestructura de la red es fundamental.

Seguridad de la Infraestructura de red

La seguridad de la infraestructura de red requiere un enfoque holístico de procesos y prácticas que garanticen que la infraestructura no solo permanezca protegida, sino que tenga la capacidad de reanudar sus operaciones incluso ante cualquier fallo, es decir, ser resiliente. **La gestión de la red fuera de banda (OOB) implementa rutas de administración alternas a la red principal**, para manejar los dispositivos de red de forma remota. Sin embargo, aun con ello, es necesario ir un paso más allá, y controlar los accesos OOB a los dispositivos críticos. Para ello, se requiere de un portal de gestión que supervise y monitoree sin problemas todos los dispositivos críticos desde un solo panel de mando.

Centralización de la administración remota

Se ha vuelto, pues, imprescindible la implementación de más restricciones de acceso y la gestión de entradas y salidas remotas del personal a la red, entre otros aspectos. **Las empresas necesitan visibilidad y control completo de su infraestructura crítica.**

“Cada vez son más las empresas que requieren herramientas diseñadas para la administración remota. Una plataforma que proporcione a los administradores un eficiente monitoreo de toda la infraestructura, sin tener que estar en el lugar físico y que actúe como centro de control unificado, es una de las mejores formas de asegurar la red", compartió Miranda Hernández Landavazo, Channel Marketing Manager de Opengear para Latinoamérica. "Paneles de administración de la red como el Lighthouse permiten tener un control en tiempo real de los dispositivos de red a través de servidores de consola conectados a los equipos que conforman cada centro de datos, por lo que ante una irregularidad, los administradores pueden ser notificados en el momento y solucionar problemas sin perder tiempo ni dinero en el traslado o en reparaciones diversificadas”.

La resiliencia y la seguridad de la red de hoy en día consisten en la gestión centralizada de sitios descentralizados o remotos, empoderando a los administradores con un control exhaustivo que les permita tener un acceso alternativo a la red en caso de interrupción, mientras que al mismo tiempo, monitorean todos los aspectos de su infraestructura a través de un tablero central que les promueva la seguridad, estabilidad y resiliencia del negocio.