opengear
A DIGI COMPANY

COMENTARIO DE LA INVESTIGACIÓN

Analizando el costo real de las interrupciones de red

La red y su operación eficiente son vitales para el éxito de casi todas las organizaciones que operan en la actualidad. Cuando no se encuentra disponible, la productividad disminuye, la empresa se ve afectada a nivel financiero y perjudica su reputación. Sin embargo, las tendencias como el trabajo remoto y la virtualización, si bien ayudan a impulsar la flexibilidad y la productividad del negocio, también pueden hacer que la red sea más vulnerable, tanto a fallas como a ataques.

A medida que la industria de TI se ha vuelto más virtualizada, con la migración constante a la nube, el aumento de la conectividad y la aparición de la Internet industrial de las cosas (IIoT), la red se vuelve más complicada y costosa de administrar. A medida que más personas trabajan desde casa (una tendencia que probablemente se acelerará por la actual crisis del coronavirus) o se conectan de forma remota, mientras están fuera del sitio, la dispersión es mayor. En conjunto, estos factores aumentan la importancia de que la red se mantenga en funcionamiento, pero también la probabilidad de que se produzcan interrupciones.

POR QUÉ OCURRE EL TIEMPO DE INACTIVIDAD

Las empresas están sumando capas de complejidad a las redes y esto, a menudo, se traduce en más vulnerabilidades. Hoy en día, vemos una serie de factores que pueden causar interrupciones en la red o el sistema, desde problemas con el proveedor de internet, cortes de fibra hasta un simple error humano. Sumado a esto, los dispositivos de red son cada vez más complejos. Eso puede dificultar el logro de una seguridad de red sólida.

Dado que los paquetes de software deben actualizarse con más frecuencia, se vuelven más vulnerables a errores y ciberataques. Por un lado, existe el riesgo de ataques externos por parte de ciberdelincuentes con la intención de explotar las debilidades de la red corporativa, o bots externos que buscan, de forma constante, vulnerabilidades que les permitan penetrar en las redes de la empresa. Por otro lado, existe una creciente amenaza por parte de los propios empleados de la empresa. Las causas son tan diversas como los riesgos, desde empleados descontentos que abren deliberadamente las puertas a los ciberdelincuentes, hasta usuarios inocentes que son víctimas de ataques de phishing.

Por último, la continua expansión de las redes para abarcar la computación de borde (edge computing) ha llevado a un aumento de la computación periférica, como por ejemplo, los servicios de última generación como Netflix, y a la instalación de equipos más complejos en lugares remotos, donde no hay personal de TI y donde la redundancia no es factible. En tales escenarios, ya no es suficiente solo diseñar un centro de datos sólido. La red es tan fuerte como su punto más débil y, por lo tanto, la proliferación de la computación de borde requiere una nueva forma de pensar acerca de la red.

En conjunto, todo esto aumenta el nivel de interrupciones de la red. En un estudio independiente reciente solicitado por Opengear y realizado por OnePoll, en el que participaron 500 altos tomadores de decisiones de TI, más de la mitad (51 %) de los encuestados dijeron que su organización había tenido cuatro o más interrupciones que duraron más de 30 minutos durante el último año. De hecho, casi uno de cada cinco (18 %) señaló que había experimentado siete o más interrupciones de este tipo en los últimos 12 meses. Sumado a esto, casi dos tercios (65 %) de los encuestados señalaron que la cantidad de interrupciones experimentadas por su organización había aumentado en los últimos cinco años.

La prevalencia y la duración del tiempo de inactividad también, en este momento, tienen un impacto financiero significativo en las empresas. Cerca de uno de cada tres (31 %) de los responsables sénior de la toma de decisiones de TI a nivel mundial indicó que las interrupciones de la red le habían costado a su negocio más de 1,2 millones de dólares en los últimos 12 meses, y uno de cada seis en total (17 %) señaló que les había costado 6 millones de dólares o más. Además, menos de uno de cada diez personas de la muestra (8 %) pudo afirmar que estos cortes no le había costado nada durante ese período de tiempo.

NECESIDAD DE UNA RESPUESTA RÁPIDA

Para agravar las dificultades que enfrentan, a menudo estas interrupciones son difíciles de resolver con rapidez. El 38 % de la muestra de la investigación indicó que a sus organizaciones les está tomando, en promedio, más de una jornada laboral, encontrar y resolver una interrupción de la red después de su detección.

La falta de planificación es un problema. Más de la mitad (59 %) de las empresas encuestadas no han implementado un programa de mantenimiento preventivo para minimizar los tiempos de inactividad. Con muchas redes dispersas que están en funcionamiento, no es de extrañar que para el 41 % de los encuestados en la lista "tiempo de desplazamiento para llevar ingenieros al sitio" se encuentre entre los dos principales desafíos que enfrentan para resolver un problema de red con rapidez. Dado el tiempo necesario para resolver las interrupciones de la red y los costos incurridos, encontrar una solución que aborde estos temas se ha convertido en prioridad absoluta.

POR QUÉ LA RESILIENCIA ES LA SOLUCIÓN

Dados todos los desafíos mencionados con anterioridad, hoy vemos un enfoque creciente en un concepto conocido como resiliencia de red. Pero, ¿qué queremos decir exactamente con esto, por qué es importante y cuál es la mejor manera de lograrlo? Existe una gran cantidad de definiciones distintas.

Según Joshua Sanders, Lending Tree: "Para mí, la resiliencia de la red es una iniciativa para minimizar el tiempo de inactividad. Si la red falla, hay que tener una forma de acceder a ella y no verse obligado a desplazarse al sitio real para repararla".

Chris Weindel, Eldorado Resorts, agregó: "La resiliencia de la red significa la rapidez con la que se puede volver a trabajar después de una interrupción. ¿Cierto? La red fuera de banda es nuestra última línea de defensa. Esperamos nunca tener que utilizarla, pero nos alegra tenerla cuando la necesitamos".

Desde el punto de vista de Opengear, la resiliencia de la red es la "capacidad de proporcionar y mantener un nivel de servicio aceptable frente a fallas y desafíos para un normal funcionamiento". Vemos esto como nuestra definición oficial, que luego también se traduce en nuestra "visión resumida": "la capacidad de resistir y recuperarse de una interrupción del servicio". Una forma de medirlo, es la rapidez con la que la empresa puede volver a funcionar a su capacidad normal, tras una interrupción.

Sea cual sea la definición exacta, la mayoría de la gente tiene claro que la verdadera resiliencia de la red no se puede lograr al dar resiliencia a una sola pieza de equipo, ya sea un conmutador central o un enrutador. En cambio, es importante que cualquier solución de resiliencia pueda conectarse a todos los equipos en un sitio periférico o centro de datos, mapear lo que está allí y establecer lo que está en línea y fuera de ella, en cualquier momento.

Una prioridad debe ser garantizar que la empresa tenga visibilidad y agilidad para revertir la situación cuando surjan problemas. Imagine una gran empresa financiera o de atención médica con un centro de operaciones de red (NOC, por sus siglas en inglés) que posiblemente requiera tiempo de actividad constante para las aplicaciones y el servicio al cliente. Es probable que tengan varias sucursales repartidas por todo el mundo con problemas de zona horaria presentes. Como resultado, pueden tener dificultades para saber que se ha producido una interrupción, porque no se les notifica de forma proactiva si ocurre una desconexión. Incluso cuando están al tanto, puede ser difícil saber en qué equipo y en qué ubicación se encuentra un problema, si no hay nadie en el lugar para inspeccionarlo físicamente.

ANÁLISIS DEL ROL DE OUT-OF-BAND Y NETOPS

Para solucionar las fallas, una organización puede tener que llevar a cabo un reinicio rápido del sistema, de forma remota. Si esto no funciona, posiblemente haya un problema con una actualización de software. Ahí es donde entra en juego el concepto Out-of-Band. La red tradicional en banda implica la gestión de dispositivos mediante protocolos comunes como telnet o SSH, con el uso de la propia red como medio. La gestión Out-of-Band (OOB) proporciona una capa completamente separada de la red, por lo que puede acceder y reparar de manera rápida cualquier equipo afectado si el sistema está bloqueado. Esto es de especial importancia, por ejemplo, en un ciberataque.

Por lo tanto, los problemas de red, como el problema de actualización de software destacado anteriormente, se pueden solucionar mediante los dispositivos más modernos de *Smart* Out-of-Band (OOB) puesto que es posible conservar una imagen del equipo básico y su configuración, ya sea un enrutador o un conmutador, por ejemplo. Además, el dispositivo se puede volver a configurar rápido, de manera remota, sin la necesidad de tener a nadie en el lugar. Este es un punto crucial a considerar, sobre todo tomando en cuenta las restricciones de viaje actuales debido al brote de coronavirus.

Si se produjo una interrupción, también es posible ofrecer resiliencia de red a través de Failover to Cellular™. Esto permitiría que los servicios críticos de la empresa se mantuvieran en funcionamiento mientras la falla original se soluciona de forma remota, incluso cuando la red principal no funcionara.

Aunque brindar resiliencia adicional a través del OOB cuesta dinero, el retorno de la inversión (ROI) puede superar el gasto, de manera significativa. Esta ruta de acceso alternativa a lo mejor la organización la utiliza solo de forma ocasional. Sin embargo, cuando se necesita, se convierte en un factor crítico para obtener el éxito. También vale la pena considerar que la resiliencia suele ser mucho menos costosa que tener que comprar grandes cantidades de equipos innecesarios. Esto es cada vez más cierto, a medida que crece la implementación de ubicaciones perimetrales. Aunque tal vez sea posible para una empresa comprar equipos innecesarios para un centro de datos principal, esos mismos aparatos innecesarios no se pueden instalar en todos y cada uno de los racks o armarios de datos en una ubicación remota y pequeña.

El estudio identificó el ahorro de tiempo (referenciado en un 45 %) y el ahorro de costos (41 %) como los dos principales beneficios para las organizaciones, al tener una solución que podría funcionar independiente de la red principal en banda; que podría detectar y solucionar problemas de red, de forma automática.

Para solucionar las fallas, una empresa puede tener que llevar a cabo un reinicio rápido del sistema, de forma remota. Si esto no funciona, posiblemente haya un problema con una actualización de software. Por fortuna, esto también se puede solucionar con los dispositivos más modernos de *Smart* OOB™, puesto que es posible conservar una imagen del equipo básico y su configuración, ya sea un enrutador o un conmutador por ejemplo; y el dispositivo se puede volver a configurar rápido, de forma remota, sin tener que enviar unas "manos inteligentes" al lugar.

Más allá de garantizar una solución de respaldo invulnerable con herramientas como la gestión de *Smart* OOB y Failover to Cellular, las empresas pueden brindar mayor protección y lograr un ahorro de costos, al agregar herramientas para la automatización de NetOps adicional a las soluciones para el aprovisionamiento seguro fuera del sitio. Esto puede acabar con muchas tareas repetitivas, eliminar la posibilidad de errores humanos y ahorrar tiempo. De acuerdo con esto, el 43 % de la muestra del estudio indicó que estaban "aumentando el nivel de automatización en toda la red", para impulsar la resiliencia de esta dentro de su organización. También es significativo que el 89 % de los encuestados que habían adoptado un enfoque de automatización NetOps, dijeran que habían hecho que la red de su organización fuera más confiable.

IR MÁS ALLÁ DE LA RED EN BANDA PARA ENFRENTAR EL DESAFÍO DEL TIEMPO DE INACTIVIDAD DE LA RED

El tiempo de inactividad de la red es un problema importante para la mayoría de las grandes empresas. Las interrupciones son frecuentes, cuestan tiempo y dinero, y provocan daños a la reputación de la empresa. Aún así, existe una falta de planificación preventiva y las empresas a menudo gastan sumas importantes para que la organización vuelva a funcionar, sobre todo en términos de llevar ingenieros a sitios remotos.

Una solución capaz de operar de forma independiente, de la red principal en banda y detectar y solucionar problemas en ella automáticamente, es de gran valor en este contexto. Una estrategia basada en la resiliencia de la red, respaldada por la gestión de *Smart* OOB y dentro del contexto de un enfoque de automatización de NetOps, debe representar la mejor forma de avanzar.

METODOLOGÍA DE LA ENCUESTA

Los datos se basan en una encuesta a 500 tomadores de decisiones sénior de TI ubicados en Norteamérica y Europa. Opengear solicitó la encuesta y OnePoll, miembro de AAPOR, la llevó a cabo, en enero de 2020.

opengear
A DIGI COMPANY

ANALIZANDO EL **COSTO REAL** DE

LAS INTERRUPCIONES DE LA RED

Una red sólida es vital para el éxito de casi todas las organizaciones. Cuando no se encuentra disponible, la productividad disminuye, la empresa se ve afectada a nivel financiero y perjudica su reputación. Las empresas están sumando capas de complejidad a las redes y esto, a menudo, se traduce en más vulnerabilidades.

En un estudio global reciente*, solicitado por Opengear y en el que participaron 500 altos tomadores de decisiones de TI, por encargo de Opengear, se descubrió que:

31%

ha **perdido más de USD 1 millón** en los últimos 12 meses a causa de las interrupciones de la red.

83% afirmó que la resiliencia de la red es su principal prioridad. **#1**

El 23 % informó un **aumento del 25 % o más** en interrupciones de la red, en los últimos 5 años.

El 39 % de las interrupciones de la red tardó más de un día en resolverse.

42% afirmó que **los traslados de los ingenieros** son el desafío más común en el proceso de reparación.

Empresas de todo el mundo reconocen que la capacidad de operar, de forma independiente de la red de producción, **para detectar y solucionar los problemas automáticamente, puede considerablemente:**

mejorar la seguridad en un **48%**

ahorrar tiempo en un **45%**

reducir los costos en un **41%**

Implementar una solución para la resiliencia de la red que aborde todo esto es prioridad absoluta.

Tome la decisión de tener una red resiliente: implemente *Smart* Out-of-Band de Opengear

opengear **ESTADOS UNIDOS:** +1 888 346 6853 | **APAC:** +61 7 3871 1800 | **REINO UNIDO:** +44 20 4539 0280 | sales@opengear.com | latam@opengear.com