Redes de próxima generación: seguridad para hoy y mañana

La protección contra las amenazas del presente en redes diseñadas para satisfacer las necesidades del pasado hace vulnerables a las empresas.

El entorno informático empresarial evoluciona rápidamente como respuesta a la consumerización de la TI, la movilidad y la Cloud Computing. Estas tendencias implican nuevas oportunidades empresariales estratégicas, así como nuevos riesgos y vulnerabilidades. Las organizaciones de TI deben encontrar una forma de proteger los activos empresariales y a su vez permitir a la empresa aprovechar el valor de dichas tendencias. Esto puede complicarse más de lo necesario cuando la organización de TI cuenta con una red "suficientemente buena". Este informe técnico analiza las implicaciones que comporta proteger una red con gasto de capital (CAPEX) bajo frente a los riesgos actuales y cómo las redes de próxima generación contribuyen a un entorno de TI más seguro.

Modelo de seguridad de red de ayer

No hace tanto tiempo, la seguridad del entorno de TI era más sencilla de lo que es hoy. La información básica como las ubicaciones de los usuarios, las aplicaciones que se estaban ejecutando y los tipos de dispositivo que se estaban usando eran variables conocidas. Además, esta información resultaba ser bastante estática, por lo que las políticas de seguridad podían ampliarse fácilmente. Las aplicaciones se ejecutaban en servidores dedicados en el Data Center y la organización de TI controlaba el acceso a estas aplicaciones y establecía límites para aplicar políticas de seguridad. Las aplicaciones y puntos terminales estaban protegidos y se restringía el acceso a la red. El objetivo de la red era el de conectar a los usuarios con los recursos de TI en una arquitectura de cliente/servidor y, en casi todo, la red cumplía con los patrones de tráfico previsibles.

Hoy en día, las tendencias informáticas de rápida evolución están afectando a la seguridad de la red de dos formas fundamentales. La primera es que están cambiando la arquitectura de red. El perímetro de red ha evolucionado a medida que diversos dispositivos móviles se conectan a la red empresarial desde distintas ubicaciones. También se han producido cambios en las aplicaciones: se han virtualizado y pueden desplazarse entre servidores e incluso entre los Data Center. Al mismo tiempo, los usuarios están ampliando la red empresarial, ya que acuden a la nube para utilizar aplicaciones colaborativas como Dropbox o Google Docs. La TI ya no sabe qué dispositivos se conectan a la red o su ubicación y las aplicaciones en uso ya no están limitadas a las que proporciona la TI. Los datos no permanecen en los Data Center; recorren el país en smartphones y tablet PC, y van más allá del alcance de la TI, gracias a la nube.

La segunda tendencia que está afectando a la seguridad de red es la aparición de amenazas cada vez más complejas y sofisticadas. Las redes de ayer se veían afectadas por ataques de tipo masivo. Los hackers enviaban, por ejemplo, dos millones de correos electrónicos no deseados que se aprovechaban de vulnerabilidades o riesgos conocidos, y dependían en cierto modo de que los remitentes abrieran el correo y sucumbieran al ataque.

PUBLICACIÓN PERSONALIZADA DE
CSO Custom Solutions Group

PATROCINADO POR
CISCO

El ahorro inicial en costes se pierde rápidamente debido a que las redes suficientemente buenas carecen de seguridad integrada. Por esto, la TI debe solventar los riesgos con varias soluciones específicas.

Ahora el modelo de ataque ha cambiado completamente. Los hackers ya no se dirigen a un grupo amplio de personas. Ni siquiera buscan grandes vulnerabilidades. En lugar de ello, llevan a cabo ataques más complejos y dirigidos. Los hackers pueden usar la ingeniería social para conseguir información acerca del destinatario y, a continuación, hacer uso de la confianza que los usuarios tienen en la aplicación o en otro usuario para instalar software malicioso o robar datos. Es más probable que no se detecten estos ataques dirigidos, si los comparamos con los ataques de tipo masivo, hasta mucho después de que el hacker haya provocado algún daño.

Protección de la red "suficientemente buena"

Desafortunadamente, existe otro punto que complica aún más los esfuerzos en seguridad de las organizaciones de TI. Algunos analistas y proveedores están animando a las organizaciones de TI a considerar la red como un simple producto; es decir, cualquier red puede ofrecer los mismos servicios, y las organizaciones de TI solo necesitan implementar una red suficientemente buena al coste de adquisición más bajo. El ahorro inicial en costes se pierde rápidamente debido a que las redes suficientemente buenas carecen de seguridad integrada. Como resultado, la TI debe solventar los riesgos con varias soluciones específicas y dedicar más tiempo y esfuerzo a la implementación, configuración y gestión de las soluciones. La seguridad de la TI no puede mantener el ritmo y mucho menos anticipar los riesgos de seguridad. Puesto que las soluciones específicas individuales no están integradas, puede ser difícil aplicar políticas de seguridad coherentes en todo el entorno de TI. Desde el punto de vista defensivo, conforme más contexto tenga la TI, más preparada estará para detener un ataque a la red. Sin embargo, tener que establecer una correlación entre la información de distintos sistemas con el fin de conseguir ese contexto tan importante resulta contraproducente para conseguir el objetivo.

Una red suficientemente buena con varias soluciones específicas es una red inestable que crea un mayor riesgo de tiempo de inactividad. Este tiempo de inactividad puede estar provocado por una infracción de seguridad o por un error en uno de los muchos sistemas. Cuando la red deja de funcionar, afecta a todo, incluidos los ingresos.

Enfoque moderno para la seguridad de la red

Sin embargo, una red suficientemente buena y todo lo que ello conlleva en cuanto a seguridad no son la única opción. Las innovaciones en la seguridad de red han seguido el ritmo de las tendencias informáticas que evolucionan rápidamente. Una red de próxima generación tiene en cuenta las tecnologías del futuro y se crea con capacidades de seguridad integradas para conseguir una protección proactiva contra amenazas complejas y dirigidas. Es esta protección la que permite a la organización de TI mantener la confianza cuando se buscan oportunidades empresariales estratégicas como la movilidad o la Cloud Computing.

Una red de próxima generación ofrece un control y una visibilidad generalizados que tiene en cuenta todo el contexto para ofrecer una seguridad en toda la red, desde la sede central hasta las filiales, para empleados internos y trabajadores que utilizan dispositivos VPN, alámbricos o inalámbricos. Una arquitectura de política en toda la red puede crear, distribuir y supervisar reglas de seguridad basadas en un lenguaje contextual, como quién, qué, dónde, cuándo y cómo. La aplicación de dicha política puede incluir acciones como el bloqueo de acceso a datos o dispositivos, o la inicialización del cifrado de datos. Por ejemplo, cuando un empleado se conecta a la red empresarial desde un smartphone, la red identifica el dispositivo y el usuario, así como los privilegios concedidos. El motor de políticas no solo establece políticas para el dispositivo y el usuario, sino que también comparte estas políticas con todos los puntos de la red y actualiza la información de forma instantánea cuando aparece un nuevo dispositivo en la red.

Las políticas integradas en toda la red facilitan obviamente la adopción segura de las políticas de tipo BYOD (Bring Your Own Device, traiga su propio dispositivo)[1], pero las redes de próxima generación también pueden solucionar los problemas de seguridad relacionados con la Cloud Computing. Con solo pulsar un botón en

[1] "Bring your own device" (traiga su propio dispositivo) hace referencia a una nueva tendencia en la que los empleados usan sus dispositivos personales, como smartphones o tablets, para acceder a recursos empresariales.

Al implementar una red con un gasto de capital (CAPEX) bajo, las organizaciones de TI se arriesgan a tener que decir "no" a las nuevas tecnologías u operaciones empresariales debido a que la red no es compatible con ellas.

una red totalmente distribuida, las empresas pueden redirigir de forma inteligente el tráfico web para aplicar políticas de control y seguridad granular.

La red suficientemente buena frente a la red de próxima generación

La red de próxima generación ofrece mucho más que seguridad integrada. Esta red de próxima generación está diseñada estratégicamente para conseguir una optimización de los requisitos actuales y cuenta con una arquitectura que permite adaptarse a las alteraciones tecnológicas futuras a la vez que ofrece protección de la inversión. En otras palabras, una red de próxima generación es una red dinámica compatible con las tendencias de movilidad, de la Cloud Computing y del panorama de amenazas en constante evolución. También transforma la red en un mecanismo de prestación de servicios que permite a los directores de seguridad decir "sí" a los futuros esfuerzos empresariales estratégicos.

Cuando se calcule el coste total de la propiedad (TCO), el director de seguridad debe tener cuidado de no subestimar el valor empresarial que puede obtenerse gracias a las oportunidades estratégicas. Al implementar una red con un gasto de capital (CAPEX) bajo, las organizaciones de TI se arriesgan a tener que decir "no" a las nuevas tecnologías u operaciones empresariales debido a que la red no es compatible con ellas. Eso conlleva decir "no" a políticas BYOD (Bring Your Own Device, traiga su propio dispositivo), a la ampliación de los esfuerzos de virtualización de aplicaciones empresariales críticas, a los servicios de la nube y a la tecnología multimedia. Todos estos beneficios de agilidad, productividad, ventaja competitiva y ahorro en costes se pierden solo por ahorrar una ínfima cantidad de dinero en una red. Estos mismos beneficios pueden compensar el coste total de una red empresarial de próxima generación.

Echemos un vistazo en mayor profundidad y contrastemos en qué se distingue una red de bajo coste o suficientemente buena de una red empresarial de próxima generación.

- **Objetivo de la red:** una red suficientemente buena tiene un único objetivo: conectar un usuario a los recursos de TI. Esto era aceptable en 2005, cuando los usuarios se sentaban frente a equipos de sobremesa que se conectaban a puertos Ethernet. Una red empresarial de próxima generación es una red unificada que consta de clientes remotos, conectados por cable y conectados de forma inalámbrica. Dicha red engloba muchos dispositivos, así como los controles de consumo energético y de acceso al edificio. Además, puede servir para distintos propósitos, incluida la conectividad máquina a máquina, ya que puede utilizarse para nuevas redes de sensores o aplicaciones de copia de seguridad del Data Center.
- **Seguridad:** en una red suficientemente buena, la seguridad se va agregando paulatinamente. Dicho de otro modo, la seguridad consta de productos específicos que no tienen por qué integrarse bien. Una red de próxima generación integra funciones de seguridad de la instalación fija a la nube. La integración implica menos gastos generales administrativos y una reducción de los vacíos de seguridad.
- **Distinción de aplicaciones:** una red suficientemente buena no distingue entre aplicaciones y puntos terminales. Funciona bajo la premisa de que los datos son simplemente datos. Sin embargo, una red de próxima generación tiene en cuenta el punto terminal y la aplicación, y se adapta a la aplicación utilizada y al dispositivo de terminal en el que aparece.
- **Calidad de servicio:** las redes suficientemente buenas de hoy en día se sustentan en estándares de calidad de servicio básicos, que pueden resultar insuficientes para el tráfico de vídeo y escritorios virtualizados. Una red de próxima generación ofrece controles que tienen en cuenta el contenido multimedia para ofrecer integración de voz y vídeo.
- **Estándares:** una red suficientemente buena se basa en estándares sin preocuparse por el futuro. Una red de próxima generación no solo es compatible con estándares actuales, sino que también impulsa innovaciones que conducen a futuros estándares.
- **Garantía:** las redes suficientemente buenas ofrecen una forma de asistencia técnica limitada que incluye mantenimiento y una declaración de garantía. Los proveedores

La protección de las redes de ayer para las tecnologías de hoy es una dura batalla. Para anticiparse a los riesgos y las amenazas complejas que provoca la consumerización de la TI, la movilidad y la Cloud Computing, la TI necesita tener a las redes de próxima generación de su parte.

PATROCINADO POR

CISCO

de redes de próxima generación ofrecen una garantía, además de servicios inteligentes con gestión integrada.

- **Coste de adquisición:** el ahorro de dinero en los gastos de capital (CAPEX) puede verse contrarrestado por el aumento de los gastos de explotación (OPEX) si los costes de integración son más elevados y se producen más tiempos de inactividad o infracciones de seguridad graves. Mientras que los proveedores de redes suficientemente buenas minimizan estos costes, los proveedores de redes de próxima generación promueven un enfoque para los sistemas en el que, no solamente se reducen los costes de redes relacionados con el OPEX, sino que también se impulsan mejoras en los servicios de TI y nuevas oportunidades comerciales, por lo que se aumenta el rendimiento de la inversión.

La arquitectura Borderless Network

Cisco ha establecido un marco para las redes de próxima generación conocido como arquitectura Borderless Networks. En ella se define la planificación de la visión a largo plazo de Cisco para ofrecer un nuevo conjunto de servicios de redes, con el fin de satisfacer las demandas de la empresa y los usuarios finales. Estos servicios mejoran la capacidad que tiene la organización para satisfacer los requisitos nuevos y en constante cambio de los usuarios y de la TI. Los servicios de red inteligentes son fundamentales para reducir el coste total de la propiedad (TCO) y aumentar la habilidad que tiene la TI para ofrecer nuevas capacidades empresariales.

El objetivo de Cisco es el de crear sistemas y permitir a la TI dedicar menos tiempo a la realización de tareas de integración de red básica mediante la prestación de un conjunto de servicios de red que mejoren la capacidad de la red para satisfacer las necesidades de la empresa y de los usuarios.

Una de las claves del éxito de Cisco Borderless Network es Cisco SecureX Framework, un sistema de seguridad que se extiende desde el terminal hasta la nube y que ofrece política y control en cada salto de la red, así como gestión centralizada y herramientas integradas para la planificación previa, configuración, distribución de políticas en toda la red y solución de problemas.

Cisco SecureX Framework

Cisco SecureX combina el poder de la red de Cisco con la seguridad contextual para proteger las organizaciones actuales independientemente de cuándo, dónde o cómo usen la red las personas. Cisco SecureX Framework se ha creado teniendo en cuenta tres principios fundamentales:

- **Política sensible al contexto:** usa un lenguaje empresarial descriptivo simplificado para definir las políticas de seguridad basadas en cinco parámetros: la identidad de la persona, la aplicación en uso, el dispositivo de acceso, la ubicación y la hora. Estas políticas de seguridad ayudan a las empresas a ofrecer una seguridad más efectiva y a cumplir los objetivos de cumplimiento con el mayor control y la mayor eficiencia operativa.
- **Aplicación de seguridad contextual:** usa la inteligencia global y de red para tomar decisiones de aplicación en toda la red y para proporcionar una seguridad coherente y generalizada en cualquier lugar de la organización. Las opciones de implementación flexibles, como los servicios de seguridad integrados, los dispositivos independientes o los servicios de seguridad en nube, ofrecen una protección más cercana al usuario, por lo que se reduce la carga de red y aumenta la protección.
- **Inteligencia global y de red:** ofrece una visión profunda de la actividad de red y del panorama global de las amenazas para conseguir una protección segura y rápida, y una aplicación de las políticas:
  - > La inteligencia global de la infraestructura de red de Cisco recoge datos contextuales, tales como la identidad, el dispositivo, el estado, la ubicación y el comportamiento, con el fin de aplicar políticas de acceso y de integridad de datos.
  - > La inteligencia global de las actividades de seguridad global de Cisco (Cisco Security Intelligence Operations–SIO) proporciona datos completos y actualizados sobre el comportamiento y contexto de las amenazas, con lo que se consigue una protección segura y en tiempo real.

Cisco SecureX permite a las organizaciones optar por la movilidad y la nube a la vez que se protegen los activos empresariales importantes. Ofrece un control y una visibilidad granulares, a nivel de usuario y dispositivo, en toda la organización. Para las organizaciones de seguridad de TI, esto proporciona una protección más rápida y precisa de las amenazas mediante una inteligencia global integrada, siempre basada en la seguridad y de punta a punta. La organización de TI se beneficia de una mayor eficiencia operativa a través de políticas simplificadas, opciones de seguridad integradas y una aplicación de seguridad automática.

Conclusión

La protección de las redes de ayer para las tecnologías de hoy es una dura batalla. Para anticipar los riesgos y las amenazas complejas que provoca la consumerización de la TI, la movilidad y la Cloud Computing, la TI necesita tener a las redes de próxima generación de su parte. Las redes de próxima generación, que se han creado con una seguridad integrada y generalizada, hacen que sea más sencillo desarrollar la actividad empresarial a la vez que se mantiene el estado adecuado de seguridad que requiere la naturaleza crítica de los sistemas de TI de hoy en día.

Puede obtener más información en www.cisco.com/go/security.