Ciberseguridad empresarial de Alcatel-Lucent Enterprise para empresas

Folleto

Alcatel·Lucent Enterprise

Información general

Hace tiempo que la ciberseguridad se convirtió en una prioridad clave para las empresas. Sin embargo, las necesidades de ciberseguridad están cambiando debido a la transformación digital que se está produciendo. La transformación digital significa que las organizaciones utilizan más dispositivos conectados y móviles en sus redes mientras los empleados acceden cada vez más a aplicaciones y datos desde fuera del perímetro de la red.

A medida que el cambio se acelera, los antiguos métodos de seguridad de la red se están quedando obsoletos. Este documento comparte ideas sobre las fuerzas que están cambiando los requisitos actuales de la ciberseguridad en la empresa y recomienda estrategias que las empresas pueden adoptar y tecnologías que pueden implementar para mantener los datos y sistemas seguros en la era de la transformación digital.

La solución de ciberseguridad de Alcatel-Lucent Enterprise responde a las exigencias de una empresa transformada digitalmente. Con un enfoque multifacético de la ciberseguridad, las empresas puede proporcionar un acceso basado en políticas a los dispositivos conectados, datos seguros y aplicaciones de software en todo el ecosistema empresarial.

Nuevos retos

La naturaleza de las amenazas a la ciberseguridad está cambiando. Los hackers están utilizando la inteligencia artificial (IA) y el aprendizaje automático (ML, Machine Learning) para crear ataques más sofisticados y automatizados. Las nuevas técnicas de ingeniería social permiten a los delincuentes conectar restos de información encontrados en las redes sociales para crear perfiles de las personas o de los datos que poseen las organizaciones.

La transformación digital de la empresa también está afectando a los requisitos en materia de ciberseguridad, lo que resulta en una mayor complejidad, un mayor uso de dispositivos conectados y un perímetro que está desapareciendo, y todo ello a un ritmo acelerado.

Más dispositivos, más complejidad

Las empresas están adoptando nuevas tecnologías, como la nube, el móvil, el IoT, el Big Data y el análisis avanzado. Estas nuevas soluciones aportan un nuevo nivel de complejidad que requiere una nueva forma de ver la seguridad. Además, a medida que aumenta el número de dispositivos conectados, también lo hacen las vulnerabilidades y las oportunidades para que se produzcan infracciones.

Por ejemplo, en muchos casos la primera generación de dispositivos conectados no requería contraseñas. Como estos dispositivos estaban conectados a la red, los piratas informáticos podían utilizarlos como puerta de entrada a la red. Hoy en día, las funciones de seguridad, como las contraseñas codificadas, suelen ser obligatorias en los dispositivos; sin embargo, las infracciones siguen siendo inevitables y, cuando se producen, los piratas informáticos pueden seguir accediendo a la red.

La desaparición del perímetro

Durante mucho tiempo, la mayoría de las organizaciones han delimitado claramente tanto los usuarios como los recursos dentro y fuera de la red. Sin embargo, a medida que las organizaciones adoptan la transformación digital, estas se abren más a los intercambios con el ecosistema en su conjunto, incluidos otros partners y proveedores en un entorno de colaboración integrado. Los usuarios ya no acceden simplemente a los recursos desde el interior del perímetro de la red, sino que lo pueden hacer desde cualquier lugar. Se puede intercambiar información con contactos de otra red. Además, los recursos de TI ya no se limitan al interior del perímetro de la empresa. Pueden estar en las instalaciones y en la nube, así como conectados a través de las API. Las empresas necesitan formas modernas de proteger los recursos cuando el perímetro deja de existir.

Macrosegmentación y microsegmentación en un mundo de confianza cero

Hay dos tipos de segmentación, la macro y la micro. En la macrosegmentación, la red física se divide en diferentes segmentos lógicos. Todas las empresas utilizan la segmentación, pero no siempre por razones de seguridad. A menudo, la macrosegmentación se utiliza con fines de escalabilidad, administrativos u organizativos. Estos segmentos pueden ser una VLAN, una combinación de VLAN + VRF, una VPN cuando hablamos de la conexión de ruta más corta, MPLS, o incluso VXLAN o túneles GRE. El tráfico entre usuarios o dispositivos en diferentes segmentos está controlado por un cortafuegos físico. Si dos dispositivos están asignados a diferentes VLAN y pueden comunicarse sin pasar por un cortafuegos, significa que están en el mismo macrosegmento. Por ejemplo, las cámaras y las cerraduras de las puertas estarían bajo el control del grupo de seguridad de acceso, mientras que los termostatos podrían ser controlados por el grupo de mantenimiento del edificio.

La microsegmentación va un paso más allá. No todos los usuarios son iguales y no todos tienen una necesidad legítima de acceder a todos los recursos. El mismo perfil que asigna a los usuarios a un segmento también incluye un conjunto de políticas que agregan control granular sobre los privilegios de los usuarios/dispositivos que son diferentes según las funciones, como RRHH o finanzas. Esto se conoce como «acceso basado en funciones» y está directamente relacionado con el «principio de mínimo privilegio». Por eso, aunque las cámaras y las cerraduras de las puertas estén en el mismo segmento, no tienen por qué utilizar los mismos recursos.

La cámara necesita comunicarse con el grabador de vídeo, mientras que la cerradura con su servidor. No es necesario que una cámara se comunique con una cerradura de puerta, al igual que no es necesario que una cerradura de puerta se comunique con otra. Estos permisos granulares se implementan a través de políticas que forman parte del perfil y que se aplican de forma dinámica al dispositivo después de la autenticación.

La pregunta es si realmente necesitamos ambas cosas El reto de tener un enfoque basado únicamente en la macrosegmentación se da cuando el cortafuegos se convierte en un cuello de botella, ya que todas las VLAN tienen que terminar en el cortafuegos, momento en el que surgen problemas de rendimiento. Como alternativa, se pueden desplegar más cortafuegos en la capa de distribución; sin embargo, esto sería bastante costoso y aún no recomendable desde el punto de vista del rendimiento. Además, un mayor número de cortafuegos significa que habrá varios puntos de aplicación de políticas y varios lugares para mantenerlas actualizadas.

La microsegmentación por sí sola también puede ser problemática. Si la única aplicación de políticas se realiza a través de las políticas de control de acceso a la red (NAC), las listas de políticas se vuelven más largas y complejas, pudiendo agotar los límites de capacidad del dispositivo. Un equilibrio entre estos dos tipos de segmentación permite que el cortafuegos controle el tráfico entre diferentes segmentos (vertical) y que las políticas de NAC controlen el tráfico dentro de un determinado segmento (lateral). Al combinar la macrosegmentación y la microsegmentación, se puede hacer frente a las amenazas a la seguridad que se extienden de un segmento de seguridad a otro, así como a las que se desplazan lateralmente por el mismo segmento.

En cuanto a un enfoque de confianza cero en la seguridad de la red, el principio rector es «actuar como si los atacantes ya estuvieran presentes». Esto significa autenticar todas las conexiones. Ningún activo ni usuario es inherentemente fiable. Ya sea en las instalaciones o fuera de ellas, pasan los mismos controles. No se puede confiar en los usuarios internos. Se autentican todos los accesos.

Si consideramos un enfoque tradicional de la seguridad en el que la red se percibía como una fortaleza construida alrededor de la empresa, la fortaleza representa el cortafuegos, de modo que todo lo que está fuera no es de confianza y se examina, mientras que todo lo que está dentro es implícitamente fiable y está permitido. Sin embargo, la microsegmentación, concretamente la microsegmentación definida por software, va un paso más allá. Además de la fortaleza, y de la seguridad que rodea al edificio, también hay guardias de seguridad que requieren la autenticación. Este límite de confianza es difuso, está distribuido y es móvil. No está vinculado a una ubicación, puerto de conmutador o VLAN en particular. Depende de la identidad, el dispositivo, la situación y la hora del día. Está definido por software y se ajusta sobre la marcha. La clave de este enfoque es que los componentes se gestionan y deben ser capaces de reaccionar y reconfigurarse según sea necesario para responder a las amenazas o a los cambios en el flujo de trabajo.

Una solución para la empresa en evolución

Alcatel-Lucent Enterprise ofrece un enfoque polifacético de la ciberseguridad de la empresa, que proporciona seguridad exhaustiva a los dispositivos y aplicaciones conectados a través de múltiples capas de seguridad.

Conectividad flexible

Nuestro planteamiento comienza con una red autónoma flexible que agiliza y facilita la configuración de las políticas de red y de ciberseguridad para el gran número de usuarios, dispositivos y aplicaciones conectados que alimentan la transformación digital.

En el pasado, la TI ha sido una operación de romper y arreglar. El departamento de TI instalaba nuevos equipos, los ponía en marcha y gestionaba la red mediante tediosos procesos manuales. Digital Age Networking de Alcatel-Lucent Enterprise ofrece una red inteligente y automatizada que facilita la conexión de los usuarios y los dispositivos a sus aplicaciones específicas de manera segura. Creada con la tecnología ALE Intelligent Fabric (iFab), Digital Age Networking combina iFab con el estándar del sector, la conexión de ruta más corta (SPB). En combinación, estas tecnologías simplifican la creación y la configuración de las redes, al tiempo que agilizan el enrutamiento multirruta y la agregación de enlaces para combinar varias conexiones de red en paralelo para aumentar el rendimiento y proporcionar redundancia.

Con la estrategia de ALE, los equipos de TI definen los servicios de red, la arquitectura, las políticas de acceso y los contenedores de IoT, y la red se construye automáticamente. Una vez diseñada la red, si se mueve, cambia o añade algo, entonces la red realiza los ajustes necesarios de forma automática e indetectable. Por ejemplo, si un conmutador está fuera de servicio, la red se redirige automáticamente alrededor de ese conmutador.

Al utilizar una red autónoma, las empresas obtienen una automatización que reduce los errores de configuración manual y les ayuda a seguir el ritmo acelerado de los cambios que se dan en sus organizaciones. Dado que la automatización elimina el trabajo manual, las TI se convierten en un motor del negocio.

Control de acceso mediante políticas inteligentes y automatizadas

Las empresas pueden utilizar Digital Age Networking para definir las normas y políticas de acceso de los usuarios que rigen las aplicaciones y los dispositivos que los usuarios pueden utilizar y a los que pueden acceder; asimismo, la empresa puede utilizar esta solución para seguir a los usuarios dondequiera que vayan. Por ejemplo, pueden establecer políticas que permitan el acceso a:

- Sistemas específicos
- Servicios de Internet
- Política basada en los contratistas de aplicación a otros partners

Alcatel-Lucent Enterprise también ofrece servicios basados en la ubicación, como la orientación en interiores y el seguimiento de bienes y personas, que permiten a las organizaciones establecer políticas que tengan en cuenta la ubicación del usuario.

Las funciones de gestión de autenticación de políticas unificada (UPAM) aplican las políticas automáticamente cada vez que un usuario se conecta, garantizando que los usuarios tengan solamente los privilegios de acceso permitidos. Una vez que los usuarios se conectan a la red con un dispositivo y se validan sus credenciales, no necesitan seguir autenticándose. Permanecen conectados si el dispositivo está encendido y el sistema aplica automáticamente la política para ese usuario.

Las políticas garantizan que todos los usuarios, dentro o fuera de la organización, tengan acceso exclusivamente a las áreas permitidas y que los controles de acceso se apliquen de manera sistemática. También simplifican los flujos de trabajo de las empresas al tiempo que garantizan la ciberseguridad. Los usuarios pueden acceder rápidamente a los sistemas y a la información que necesitan sin necesidad de realizar costosos procedimientos de acceso a la seguridad.

Reducir la vulnerabilidad de los dispositivos

Las empresas se conectan a muchos dispositivos IoT. La solución Digital Age Networking de Alcatel-Lucent Enterprise permite a las organizaciones contenerizar cada dispositivo, creando un segmento de red virtual con el fin de evitar que cualquier dispositivo se convierta en un punto de ataque. La contenerización dentro de Digital Age Networking hace que haya múltiples redes virtuales a partir de una única red física, es fácil de implementar para los equipos de TI y es administrada por un único sistema de gestión. Esta solución detecta de manera automática cada dispositivo de la red. Cuando un dispositivo se conecta a la red, el sistema de gestión de red Alcatel-Lucent OmniVista® Network Management System, disponible en las instalaciones o en la nube, intenta identificar ese dispositivo. Si el sistema de gestión no tiene el dispositivo en su base de datos, consultará una base de datos en la nube con más de 29 millones de dispositivos.

Una vez identificado el dispositivo, el sistema lo clasificará, por ejemplo, como una cámara de seguridad. Si ese dispositivo está en la lista de proveedores aprobados para cámaras de seguridad, se conectará a la red. De lo contrario, no se conectará. A continuación, la solución se instala en un contenedor virtual para el dispositivo, segmentándolo del resto de la red. Si alguien ataca cualquier dispositivo conectado a la red, ese atacante no podrá utilizar ese dispositivo para acceder al resto de la red.

Inteligencia artificial para un entorno de confianza

Una vez que los dispositivos están conectados, deben ser supervisados continuamente para identificar cualquier amenaza y mantener la confianza. La visibilidad de análisis y aplicación de Alcatel-Lucent Enterprise permiten que los administradores de la red vean lo que está pasando en la red para cada dispositivo. El análisis identifica patrones de comportamiento normales y esperados de la red, así como cualquier patrón atípico cuando surge. El comportamiento de las aplicaciones en el extremo de la red se puede supervisar para decidir si nos conectamos a la aplicación, así como para detectar un comportamiento inusual en las aplicaciones permitidas, como una cámara de vídeo que esté generando más datos de los que debería.

Si se produce una anomalía o un comportamiento inusual en el dispositivo, los análisis lo mostrarán para que el gestor de seguridad de la red pueda intervenir. Actualmente, la investigación debe realizarse de forma manual, pero ALE está trabajando en la automatización de la respuesta utilizando la inteligencia artificial y el aprendizaje automático.

Proteger la red

Aunque las organizaciones actuales son conscientes de la necesidad de proteger los dispositivos IoT en la red, es posible que no tengan en cuenta los dispositivos que forman la base de la red, como los conmutadores y los puntos de acceso. Alcatel-Lucent Enterprise emplea muchas tecnologías para reducir la amenaza procedente de estos dispositivos. Soluciones de Alcatel-Lucent Enterprise:

- Reforzar el software del sistema operativo para proporcionar un código seguro y diversificado
- Enviar el software del sistema operativo para la verificación y validación de terceros para corroborar que no tiene puntos de entrada o puertas traseras sencillos
- Asegurar que cada vez que se arranca un conmutador, la memoria se compila y se actualiza de una manera diferente. Aunque los conmutadores funcionan de forma idéntica, no hay dos que tengan la misma configuración de memoria internamente. Si alguien violara un conmutador ALE, no podría acceder a otro conmutador de la misma manera.
- Proporcionar protección integrada de Denegación de servicio (DoS). La CPU puede detectar cantidades inusuales de tráfico de red y apagar automáticamente la CPU si es necesario.
- Múltiples certificados de seguridad, como JDIC y FIPS
- Realizar actualizaciones continuas del software

Conexiones seguras para el tráfico entrante y saliente

Para el tráfico entrante, las funciones VPN de ALE proporcionan una conexión cifrada a la red local, mientras que el tráfico de extremo a extremo está protegido mediante el cifrado MACsec (también conocido como IEEE 802.1AE) para proteger la información a medida que recorre la red; además la capacidad de volver a cargar los servicios, como TKS y HTTPS, sin necesidad de reinicio garantiza que no se interrumpe la red.

Presentación de informes

La presentación de informes de ALE permite que diferentes personas accedan a información sobre el estado, la situación y el rendimiento de la red, el funcionamiento de las aplicaciones y la satisfacción de los usuarios. Por ejemplo, el equipo de TI puede ver datos sobre el rendimiento y las operaciones de la red.

Las unidades de negocio pueden garantizar que los equipos, como los sensores o los sistemas de telemetría, transmiten datos a los servidores y las tabletas sin ningún problema. El departamento de TI puede determinar si la red está prestando servicios que permiten a los empleados pasar más tiempo realizando su trabajo y si están sacando el máximo provecho de la red.

La ciberseguridad en los distintos sectores

Educación

A medida que los centros de enseñanza adoptan estrategias de campus inteligente, se añadirán más dispositivos móviles y conectados a sus redes, mientras que los dispositivos del Internet de las Cosas (IoT) accederán cada vez más a aplicaciones y datos desde fuera del perímetro de la red.

A medida que la conectividad y la innovación se implantan en las infraestructuras de los grandes campus, se vuelven inmediatamente vulnerables a las ciberamenazas. La solución Digital Age Networking para campus inteligentes de Alcatel-Lucent Enterprise mantiene la seguridad de los datos y activos de TI de los en la actual era de la transformación digital. Con esta solución, los centros pueden controlar estrictamente el acceso de los usuarios, reducir las vulnerabilidades creadas por los dispositivos móviles, de IoT y de red, e impedir que la inevitable infracción proporcione un punto de ataque, a la vez que se habilitan para los alumnos y el personal los servicios y aplicaciones que estos requieren.

Transporte

Los avances en los sistemas de transporte resultantes de las innovaciones tecnológicas requerirán la transformación de la base actual sobre la que se crearon. La integración de los dispositivos y sistemas que permiten el funcionamiento de cualquier ecosistema de transporte exige conexiones rápidas, fiables y seguras. Las redes de datos de transporte deben ser conscientes del IoT para conectar sin problemas y de forma conjunta sensores, cámaras, señalización y sistemas de control del tráfico. La seguridad de la red también es de vital importancia para proteger los datos y la integridad de la red.

ALE utiliza un código diversificado seguro para mejorar la integridad de la red y proporcionar una mayor seguridad contra los ciberataques a la red. Este código protege las redes frente a vulnerabilidades intrínsecas, uso indebido de códigos, malware y posibles puertas traseras que podrían poner en peligro las operaciones fundamentales. ALE también ofrece la impresión digital para que IoT identifique cada dispositivo, incluidos los vehículos, los sensores y las cámaras, para garantizar que no suponen una amenaza para la seguridad de la red. La estrategia de seguridad exhaustiva de ALE ha recibido los más altos niveles de certificación por parte de organismos gubernamentales, como Common Criteria (EAL2 y NDcPP), JITC, FIPS 140-2 y NIST.

Sanidad

La sanidad ha sido, y sigue siendo, uno de los sectores más atacados por los hackers. Y el problema sigue creciendo. En 2018, el sector de la asistencia sanitaria vio comprometidos 15 millones de historiales clínicos de pacientes en 503 infracciones, tres veces más que en 2017, según el barómetro de infracciones de Protenus.[1]

Las filtraciones se producen porque los datos sanitarios son extremadamente valiosos. Los expedientes individuales de los pacientes contienen todo, incluido el nombre, las direcciones actuales y anteriores, el historial laboral, los nombres y las edades de los familiares de la persona y la información financiera, como las tarjetas de crédito y los números bancarios.[2]

Con un enfoque multifacético de la ciberseguridad, Digital Age Networking de ALE mantiene la confianza con un acceso seguro y basado en políticas a los dispositivos médicos conectados, los datos de los pacientes y las aplicaciones de software en todo el ecosistema sanitario.

Administración pública

La ampliación de la función de lo digital tanto en la administración pública central como en la local ha difuminado la línea que protege los activos digitales que se emplean para el transporte, el mantenimiento de las infraestructuras y la supervisión del entorno. Es necesario revisar las políticas de ciberseguridad de la administración pública dirigidas a la seguridad de los datos, la vulnerabilidad y la gestión de la confianza.

El planteamiento de ALE acerca de la ciberseguridad proporciona una estrategia de seguridad de extremo a extremo, centrada en el servicio, para proteger todas las capas del servicio, desde la red hasta el software. En cuanto a los dispositivos, las organizaciones del sector público pueden utilizar la contenerización para crear un segmento de red virtual que evite que los dispositivos se conviertan en un punto de ataque.

Sector hotelero

El crecimiento del IoT en el sector hotelero conlleva una explosión de amenazas de ciberseguridad, ya que la proliferación de sensores y dispositivos conectados amplía enormemente la superficie de ataque de la red. El IoT es especialmente susceptible, ya que muchos dispositivos de IoT se fabrican sin tener en cuenta la seguridad o son creados por empresas que no entienden los requisitos de seguridad actuales. En consecuencia, los sistemas de IoT son cada vez más el eslabón débil de la seguridad de la red para las empresas del sector hotelero.

Proteger el tráfico y los dispositivos de IoT requiere un enfoque estratégico que aproveche las múltiples garantías de seguridad. Para ayudar a los hoteles, casinos, resorts y otras empresas de este sector a que aprovechen las ventajas y mitigar los riesgos de la implementación del IoT, ALE ofrece una estrategia de seguridad multinivel que proporciona protección en cada capa de la infraestructura, desde el usuario y el dispositivo a nivel individual hasta la capa de red. También ofrece una estrategia de contención del IoT para simplificar y asegurar la incorporación de dispositivos y proporcionar los recursos de red adecuados para que el sistema funcione de forma correcta y eficiente, todo ello en un entorno seguro con el fin de proteger a las empresas del sector hotelero frente a los ciberataques.

1 https://healthitsecurity.com/news/the-10-biggesthealthcare-data-breaches-of-2019-so-far

2 https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000tohackers/#2bb1f96b50cf

Resumen

La transformación digital ha cambiando profundamente las necesidades en ciberseguridad de las empresas a medida que el número de dispositivos conectados aumenta, el perímetro de la red desaparece y los cambios se siguen produciendo de manera acelerada. Digital Age Networking de Alcatel-Lucent Enterprise mantiene la seguridad de los datos y activos de TI en la actual era de la transformación digital. Con esta solución, puede controlar estrictamente el acceso de los usuarios, reducir las vulnerabilidades creadas por los dispositivos móviles, de IoT y de red, impedir que la inevitable infracción genere un punto de ataque y proporcionar un ecosistema empresarial de confianza.