Crear una red de confianza cero rentable

Maximizar la seguridad de la red y minimizar los costes

Resumen de la solución

Alcatel·Lucent Enterprise

Ciberseguridad y confianza cero

La ciberseguridad preocupa cada vez más a medida que avanza la tecnología y aumenta el número y la complejidad de las ciberamenazas. Las amenazas evolucionan con rapidez, lo que dificulta que las organizaciones puedan predecirlas y defenderse. Ello exige que los expertos en ciberseguridad estén a la última en cuanto a tendencias y puntos de vulnerabilidad más recientes.

Existen muchas fuentes y vectores de ataque diferentes, como correos electrónicos de suplantación de identidad, ingeniería social y vulnerabilidades de los programas informáticos. Defenderse de las ciberamenazas requiere una estrategia única para cada tipo de ataque.

Puede resultar difícil identificar y proteger todos los posibles puntos de vulnerabilidad de un sistema complejo, por lo que es crucial que los expertos en ciberseguridad comprendan cómo funcionan conjuntamente los distintos sistemas y redes para desarrollar medidas de seguridad eficaces.

El error humano es una causa común de las violaciones de la ciberseguridad y, para 2025, se estima que la falta de talento o los fallos humanos serán responsables de más de la mitad de los incidentes cibernéticos de gran importancia.[1]

Otro de los retos que requiere experiencia y conocimientos especializados es el cumplimiento de las complejas reglamentaciones y normas de ciberseguridad, como el Reglamento general de protección de datos (RGPD) y la Ley de portabilidad de los seguros de enfermedad y de responsabilidad respecto de estos en los Estados Unidos (Health Insurance Portability and Accountability Act).

1 Gartner® Predicts 2023: Cybersecurity Industry Focuses on the Human Deal | Bitsight, enero de 2023.

Proceso de violación de la ciberseguridad

La siguiente figura muestra las fases que sigue un ciberatacante para penetrar en una red y robar datos importantes. Comienza con el reconocimiento, en el que los atacantes investigan, identifican y seleccionan objetivos, y buscan puntos vulnerables en la red.

La siguiente etapa es la militarización, en la que los atacantes determinan cómo comprometer un punto final objetivo y entregar una carga útil militarizada.

Después de eso viene la explotación, donde el atacante activa la carga útil armada y escala privilegios en el endpoint comprometido para moverse lateralmente a través de la red.

La siguiente fase es la instalación, en la que los atacantes establecen un acceso de shell remoto e instalan malware para establecer persistencia.

En la fase de mando y control, los atacantes establecen canales de comunicación cifrados con los servidores de mando y control para dirigir el ataque y ejecutar los objetivos a distancia.

La última etapa es el movimiento lateral y la exfiltración, en la que los atacantes pueden tener múltiples objetivos, entre ellos el robo de datos, la destrucción o modificación de sistemas críticos y la denegación de servicio.

La clave para detener a los atacantes es detectar a tiempo las distintas fases del ciclo de vida del ataque e interrumpir su avance.

Para evitar el ataque, es necesario adoptar una serie de medidas como la gestión de vulnerabilidades y parches, la detección y prevención de malware, el bloqueo de aplicaciones y servicios de riesgo, y el registro y supervisión de toda la actividad de la red, los puntos finales y, por supuesto, la nube.

En cuanto a la red, es necesario implementar tecnologías que proporcionen un control granular de las aplicaciones y supervisen el tráfico entre zonas o segmentos en un modelo de confianza cero. La confianza cero se basa en el principio de que todo debe considerarse no fiable por defecto.

El concepto de confianza cero se desarrolló en respuesta al creciente número de sofisticados ciberataques a las redes informáticas. Para proteger sus redes, tradicionalmente las organizaciones han utilizado soluciones de seguridad basadas en el perímetro, como cortafuegos y software antivirus. Sin embargo, a medida que los ciberataques son más avanzados y complejos, tales soluciones han demostrado ser insuficientes y, en su lugar, cada solicitud de acceso debe ser verificada y autenticada antes de conceder el acceso a los recursos.

Fuente: XDR for Dummies, Palo Alto Networks Special Edition, 2022

Presentar una mejor estrategia de confianza cero

Alcatel-Lucent Enterprise ayuda a los clientes a ser más seguros y a avanzar hacia un entorno de confianza cero con sencillez y rentabilidad. En ALE somos conscientes de la importancia de implementar un modelo de confianza cero para garantizar la seguridad de la red y los datos de nuestros clientes. Ofrecemos una gama de soluciones diseñadas para ayudar a las organizaciones a implementar una red de confianza cero y hacer frente a los retos que plantean las ciberamenazas.

Refuerzo de la red

Ofrecemos una **red reforzada, tanto dentro como fuera**. Comienza con una infraestructura segura y la garantía de que el propio dispositivo no se verá afectado. Nuestra familia de productos Alcatel-Lucent OmniSwitch® funciona con el sistema operativo seguro Alcatel-Lucent Operating System (AOS), que utiliza código diversificado seguro para proteger las redes de posibles vulnerabilidades y ataques. El código se actualiza continuamente para hacer frente a las amenazas actuales y futuras, con la diversificación del software mediante la aleatoriedad en la disposición del espacio de direcciones (ASLR) utilizada para protegerse de los ataques de desbordamiento de búfer. La verificación y validación independientes (IVV) también sirve para analizar y probar el código fuente del AOS en busca de posibles puntos vulnerables, puertas traseras, malware y vulnerabilidades de seguridad del sistema. Expertos en ciberseguridad externos realizan estas pruebas, que se ejecutan en imágenes de software de disponibilidad general para garantizar la integridad del software.

Aplicamos la macrosegmentación y la microsegmentación para garantizar el acceso a la red de confianza cero. Ambos componentes son esenciales para una estrategia de seguridad de confianza cero. **Macrosegmentación** se refiere a la partición de la red en zonas o dominios separados por función, aplicación o grupo de usuarios. Esto proporciona un alto nivel de segmentación de la red, lo que permite a las organizaciones aislar los activos y recursos críticos del resto de la red. La **microsegmentación**, por su parte, se centra en segmentar la red a un nivel más granular, hasta llegar al usuario o dispositivo en concreto. Este enfoque proporciona un control más detallado del acceso a la red, lo que permite a las organizaciones aplicar directivas de seguridad en el usuario o dispositivo en concreto.

La conexión de ruta más corta (SPB) y **los perfiles de red universal** (UNP) ofrecen una potente solución para ayudar con la macrosegmentación y microsegmentación de redes, lo que mejora la seguridad y el rendimiento al limitar el alcance de posibles ataques.

SPB es un protocolo de red de capa 2 que posibilita el enrutamiento de múltiples rutas en redes grandes, al tiempo que simplifica la configuración y gestión de la infraestructura de red. Funciones como la segmentación virtual de la red ofrecen mayor protección contra accesos no autorizados y ciberataques. Al utilizar SPB en su infraestructura de red, las organizaciones disfrutarán de una mayor eficacia y seguridad de la red, ayudándolas a cumplir sus objetivos empresariales con confianza.

ALE UNP es un control de acceso basado en perfiles, una potente función del switch Alcatel-Lucent Enterprise que permite a los administradores de red crear y gestionar perfiles de usuario para el acceso a la red en función de la identidad, la ubicación y el dispositivo. Pueden implementar una gestión centralizada de las directivas de la red, simplificando su configuración y aplicación. Al implementar UNP de ALE, las organizaciones podrán mejorar la visibilidad, seguridad y control de su red, así como mejorar el rendimiento de la red, proteger los activos y reducir las interrupciones.

Juntos, SPB y UNP permiten a los administradores de red gestionar y proteger eficazmente su infraestructura de red para:

- Aplicar sistemáticamente directivas en toda la red
- Segmentar y aislar los dispositivos IoT de otros dispositivos
- Minimizar la superficie de ataque de la red

Autenticación sólida

ALE proporciona una autenticación sólida a través de un gestor de autenticación de directivas unificada (UPAM).

Un componente clave de la ciberseguridad es la autenticación, que es el proceso de verificar la identidad de un usuario, dispositivo o sistema. Consiste en confirmar que un usuario o dispositivo es quien dice ser, normalmente proporcionando algún tipo de identificación, como un nombre de usuario y una contraseña.

La solución ALE da soporte a varios métodos de autenticación de usuarios.

- **802.1X**, un protocolo de autenticación de red, permite a los dispositivos conectarse a una red segura proporcionando credenciales, como un nombre de usuario y una contraseña. Cuando un dispositivo intenta conectarse a una red mediante 802.1X, primero se autentica antes de permitirle acceder a la red. En un mundo ideal, el dispositivo se autentica a través de 802.1x. La autenticación genera un registro que puede compartirse con un cortafuegos.
- Si el dispositivo no es compatible con 802.1x, la autenticación de la **dirección MAC** ofrece una alternativa. Una dirección MAC es una tarjeta de identificación digital para cada dispositivo de una red. Es única, identifica cada dispositivo y permite la comunicación entre ellos, de forma parecida a la etiqueta identificativa de un ordenador o teléfono.
- ALE es compatible con **la identificación de dispositivos y sistemas mediante huella digital**. Si la autenticación 802.1X o MAC no devuelve ningún perfil, lo intentaremos con la huella digital. La toma de huellas dactilares en seguridad informática es el proceso de recopilación de información sobre un dispositivo o sistema, como su sistema operativo, software y puertos abiertos, para identificarlo y categorizarlo y evaluar posibles riesgos y vulnerabilidades. También se puede utilizar para asignarla a un perfil de un dispositivo registrado en la base de datos del inventario de IoT.
- ALE también proporciona un valor «capturar todo» predeterminado en caso de que no se devuelva un perfil. La regla «capturar todo» predeterminada puede permitir un acceso limitado o denegar completamente el acceso si falla la autenticación primaria.

Para ejecutar estos diferentes tipos de autenticaciones se necesita un lugar donde crear y gestionar las credenciales de usuarios y dispositivos. Se requiere UPAM, un componente de la solución de acceso unificado de ALE. Proporciona servicios centralizados de autenticación, autorización y contabilidad (AAA) para la red. Permite a los administradores de red crear y gestionar perfiles de usuario para acceder a la red, sobre la base de la identidad y la ubicación, entre otros datos. UPAM puede configurarse y gestionarse a través del sistema de gestión de red Alcatel-Lucent OmniVista® Network Management System, lo que permite a los administradores de red definir y aplicar directivas de acceso a la red.

Capacidad de respuesta ante incidentes

Responder con rapidez a los incidentes de red es un factor clave para minimizar los daños a sistemas y redes, así como para reducir las interrupciones, causados por ataques a la seguridad, como el ataque de denegación de servicio distribuido (DDoS).

Minimice los riesgos, maximice la calidad de la experiencia (QoE) y mejore la seguridad con Alcatel-Lucent OmniVista Network Advisor. **OmniVista Network Advisor** es un sistema inteligente y autónomo basado en IA que proporciona supervisión de la red en tiempo real, emitiendo alertas cuando surgen problemas y recomendando soluciones para diversas cuestiones relacionadas con la red y la seguridad, incluidos los ataques DDoS. Realiza continuamente auditorías de configuración y análisis del rendimiento de la red para poder **identificar** rápidamente los posibles problemas, **mitigarlos** y **optimizar** la red con una intervención mínima o nula de TI.

Asociaciones e integraciones

Un aspecto importante de la autenticación es la integración con los cortafuegos. Por ejemplo, mediante la integración con Fortinet, los usuarios o dispositivos autenticados en las redes LAN y/o WLAN también pueden autenticarse simultáneamente y sin problemas en el cortafuegos Fortinet.

Con la integración del cortafuegos de nueva generación de Palo Alto Networks (PAN), los usuarios o dispositivos autenticados en las redes LAN y/o WLAN también pueden autenticarse simultáneamente y sin problemas en el cortafuegos PAN.

Nuestra asociación con Versa Networks permite el acceso seguro a recursos críticos, independientemente de la ubicación de los usuarios, datos, aplicaciones o dispositivos. Esto da muy buen resultado en especial a las empresas con oficinas regionales o sucursales alejadas de la sede central o el centro de datos. A diferencia de las redes de área extensa (WAN) tradicionales, que requieren múltiples saltos de red y pueden conllevar costes adicionales, SASE y SD-WAN son soluciones rentables y seguras para la era del cliente a la nube. Combinando estas dos soluciones, las empresas pueden simplificar la gestión de la infraestructura de TI y permitir un acceso seguro a Internet y a aplicaciones empresariales en situaciones de trabajo desde cualquier lugar, como empresa/centro de datos, oficinas regionales/sucursales y trabajadores en casa/móviles.

La oferta ALE-Versa Titan es una solución integral que combina los servicios Secure Access Service Edge (SASE) y SD-WAN desde la nube. Esto incluye Versa Titan SD-WAN, que proporciona SD-WAN en la nube para conseguir una TI ágil, así como Versa Secure Access (VSA), que presenta funciones de cortafuegos de última generación y bloqueo geográfico, junto con Zero Trust Network Access (ZTNA) para situaciones de trabajo desde cualquier lugar. Además, la pasarela web segura (SWG) de Versa proporciona seguridad en la navegación web y en el acceso a aplicaciones de Internet (SaaS) para una conectividad segura remota/de oficina en casa. El portal web y la app de Versa Titan ofrecen servicios integrados de red y seguridad en una única plataforma, con todos los componentes SASE proporcionados por el mismo proveedor. Con un único repositorio de directivas que abarca las de red y seguridad, las empresas pueden simplificar la gestión de TI y garantizar un acceso seguro a los recursos críticos.

La metodología de confianza cero

Para implementar un modelo de confianza cero, las organizaciones deben abordar primero los problemas de su infraestructura de seguridad actual, como las directivas contradictorias, la confianza implícita y los dispositivos IoT vulnerables. Para combatir estos problemas, el objetivo es establecer capacidades de acceso a la red y de control de acceso basado en funciones, segmentación y supervisión, con una segmentación adecuada que permita dividir los recursos sensibles y limitar el acceso solo a quienes lo requieran. Las funciones de supervisión y cuarentena permiten a los clientes identificar y aislar posibles amenazas.

Una metodología sencilla pero potente para crear una red de confianza cero con soluciones ALE se compone varias etapas.

- **Supervisar**: Debe llevarse a cabo una supervisión que incluya el tráfico e inventario de dispositivos
- **Validar y evaluar**: La validación y evaluación implica analizar las necesidades empresariales, los requisitos de conformidad, las capacidades y los flujos
- **Planear**: Debe crearse un plan de corrección basado en los resultados de la evaluación. La planificación incluye seleccionar las directivas y tecnologías de segmentación adecuadas, así como considerar la autenticación frente a la clasificación, además de las integraciones.
- **Simular**: En la fase de simulación, las directivas están abiertas por defecto y en modo de registro. También se probarán otras funciones.
- **Aplicar**: La fase de aplicación consiste en implementar directivas restrictivas, registrar, supervisar y realizar acciones de cuarentena.

Coste total de propiedad

El coste total de propiedad (CTP) abarca todos los gastos asociados a la propiedad y el funcionamiento de un producto o servicio durante toda su vida útil. Estos gastos son, entre otros, el precio de compra, el mantenimiento, la asistencia técnica y las actualizaciones. Es importante elegir soluciones rentables que ofrezcan valor a largo plazo, lo que puede mitigar los excesos presupuestarios y proporcionar un retorno de la inversión (ROI) más preciso.

Hay que distinguir entre la inversión de capital inicial y los gastos corrientes necesarios para mantener el sistema autorizado y operativo. Mientras que algunos componentes, como los cortafuegos, se centran puramente en la seguridad, otros también son cruciales para construir una estrategia de seguridad más profunda. Entre estos destacan la gestión de directivas, la tecnología de separación eficiente de redes de ruta (macrosegmentación y microsegmentación avanzadas y automatizadas), la asignación automática de redes virtuales (VLAN), el protocolo de cifrado de red, la visibilidad de las aplicaciones y la validación y atestación independientes del código del sistema operativo.

La estrategia de ciberseguridad de la red de ALE aborda los elementos esenciales de la seguridad de la red mencionados anteriormente sin coste alguno, mientras que las alternativas de otros proveedores exigen conocimientos específicos y numerosos elementos y licencias costosos para su funcionamiento y mantenimiento. El planteamiento de ALE reporta a los clientes importantes beneficios económicos y garantiza una ciberseguridad de la red sólida y eficiente.

Conclusión

Es evidente que la implementación de una red de confianza cero para lograr una seguridad sólida puede presentar algunas dificultades, como la complejidad y el coste en términos de creación y mantenimiento. Sin embargo, ALE ofrece un enfoque único y rentable para abordar estas cuestiones. Las tecnologías avanzadas de macrosegmentación y microsegmentación, aparte de los demás componentes presentados en este documento, proporcionan un medio sencillo y asequible de implementar una red de confianza cero que responda a los requisitos de la ciberseguridad moderna. Nos comprometemos a ayudar a nuestros clientes a resolver sus problemas de ciberseguridad y consideramos que nuestro enfoque puede ayudar a lograr este objetivo.

Las soluciones ALE incluyen nuestra tecnología resistente y segura intelligent Fabric (iFab) y, UNP, así como el control sólido de acceso a la red (NAC) con UPAM, que proporciona un control de acceso basado en perfiles. Nuestra innovadora solución OmniVista Network Advisor garantiza un funcionamiento fluido y una rápida recuperación y prevención de ataques. Además, nos asociamos con proveedores de SASE como Versa Networks y nos integramos con proveedores de cortafuegos como Palo Alto Networks para ofrecer a los clientes soluciones de seguridad más completas e integradas.

Alcatel·Lucent Enterprise