Priorizar la resistencia y la seguridad

Soluciones de Alcatel-Lucent Enterprise para la administración pública

Alcatel·Lucent Enterprise

Libro electrónico

Índice

Descripción general

Ante los crecientes retos mundiales y el aumento de los riesgos cibernéticos y físicos, las administraciones públicas deben dar prioridad a la gestión de riesgos, salvaguardar las infraestructuras fundamentales y proteger a los ciudadanos. Según CloudSek, los ciberataques contra la administración pública aumentaron un 95 % en 2022.[1] Se prevé que la actividad de la administración continúe sea cual sea la situación y que los ciudadanos se mantengan a salvo. En el clima global actual, es más importante que nunca mantener la seguridad de los datos, proteger su soberanía y garantizar la disponibilidad del servicio.

El sector público y por qué las TIC son más importantes que nunca

En los últimos años, la transformación digital en el sector público ha avanzado rápidamente, con un número cada vez mayor de ciudadanos que acceden a servicios digitales. La transformación digital también ha permitido a los funcionarios adoptar un estilo de trabajo desde cualquier lugar. Existe una presión creciente sobre las administraciones públicas para que sigan acelerando la transformación digital. Según un artículo de Deloitte, el setenta y siete por ciento de los organismos gubernamentales afirman que las iniciativas de transformación digital impulsadas durante la pandemia ya están teniendo un impacto positivo en su organización.[2]

Alcatel-Lucent Enterprise trabaja con administraciones públicas de todo el mundo y reconoce la importancia de proteger a los ciudadanos, las operaciones y los edificios frente a los riesgos cibernéticos y físicos. Nuestras soluciones tienen en cuenta la seguridad y la privacidad de los datos en todas las fases del proceso de diseño y se construyen con opciones resistentes que se adaptan a todo tipo de organización. Este libro electrónico ofrece información detallada sobre la resistencia y la seguridad de sus soluciones de comunicaciones, nube y red de ALE.

1 Los ciberataques contra la administración pública incrementaron un 95 % en el segundo semestre de 2022, según CloudSek. CSO United States, enero de 2023.

2 https://www2.deloitte.com/uk/en/insights/industry/public-sector/government-digital-transformation-strategy.html.

Por qué es fundamental la colaboración TI/TO

Antes de analizar cómo puede mejorar la resistencia y la seguridad con las soluciones de Alcatel-Lucent Enterprise, es importante reconocer la cambiante relación entre la tecnología de la información y la tecnología de operaciones. En el pasado, los equipos de TI y operaciones no colaboraban estrechamente; cada uno tenía sus propias funciones y responsabilidades. Estos dos mundos convergen ahora y deben trabajar como uno solo. Los equipos de TI y operaciones que no son conscientes de las actividades de los demás, o que no se coordinan y colaboran, ponen en peligro a toda la organización.

Pensemos, por ejemplo, en el gran número de dispositivos de Internet de las cosas (IoT) que se están desplegando rápidamente en muchos organismos públicos y ciudades inteligentes. Si el departamento de TI no conoce los nuevos dispositivos IoT implementados por el equipo de operaciones, no puede garantizar que los dispositivos cumplan las políticas de seguridad de la organización. Los dispositivos IoT tienen niveles muy variables en cuando a las características de ciberseguridad y pueden no estar equipados con los últimos mecanismos de protección, o sus capacidades pueden no haberse implementado completamente. Estos dispositivos de "TI en la sombra" no autorizados podrían ejecutar cualquier software y estar ya infectados con virus y malware. Si no se controlan, pueden introducir fácilmente nuevas vulnerabilidades y vectores de ataque en la red. Asistimos actualmente a la aparición de la colaboración TI/TO necesaria para garantizar la seguridad y resistencia de la red.

Soluciones de red resistentes y seguras

La infraestructura de red forma parte integrante del funcionamiento de las organizaciones gubernamentales, así como de la prestación de servicios a los ciudadanos. Debido a la naturaleza sensible de la información contenida en las redes de la administración publica y a los servicios esenciales gestionados por la administración pública, el tiempo de inactividad o las interrupciones en los servicios de red pueden tener graves consecuencias, por lo que la resistencia y la seguridad se convierten en la prioridad. Es fundamental contar con redes fiables y seguras para que las administraciones públicas presten servicios públicos eficaces, protejan la información confidencial y garanticen un funcionamiento fluido.

Las redes Digital Age Networks de ALE son resistentes y van más allá de lo que ofrecen muchos otros proveedores de tecnología. Integramos la seguridad en nuestra red y soluciones desde las primeras fases del diseño, sin costos adicionales de licencias.

Seis prácticas recomendadas para elegir soluciones de red

1. Adopte una estrategia de seguridad de confianza cero. La macrosegmentación y microsegmentación de su red es fundamental para mantener una infraestructura resistente. Un enfoque por fases para la microsegmentación garantiza la correcta implantación y ayuda a evitar interrupciones.
2. Plantéese adoptar una solución de conexión de ruta más corta (SPB) para la redundancia y la seguridad, ya que esta estrategia redirige dinámicamente el tráfico a través de múltiples rutas en caso de fallo, a la vez que crea una red eficiente y en contenedores. SPB mejora la seguridad con la encapsulación MAC-in-MAC, eliminando las direcciones IP para evitar la suplantación de IP y los ataques de análisis de paquetes.
3. Tantee la posibilidad de aprovechar las capacidades de chasis virtual para mejorar la fiabilidad en áreas críticas, ya que esto dota de redundancia y resistencia a la red, siendo compatible con las actualizaciones de software en servicio (ISSU) y posibilitando interconexiones específicas en malla o en anillo. El chasis virtual presenta una solución rentable para simplificar la gestión de la red a la vez que garantiza una alta disponibilidad.
4. Plantéese implementar el protocolo de redundancia de router virtual (VRRP) VRRP mejora la resistencia de la red proporcionando un router virtual de reserva que puede tomar el relevo sin problemas si falla el router primario.
5. Implemente una solución que garantice que dispone de todas las copias de seguridad de configuración de los conmutadores de red y que puede restaurarlas en el peor de los casos o cuando sea necesario.
6. Un paso hacia la seguridad reforzada es tener un código diversificado seguro que aleatoriza la ubicación de diferentes segmentos de código en sus conmutadores, lo que aumenta considerablemente la seguridad. Esto se puede combinar con un proceso de verificación y validación independientes (IVV) dirigido por un experto en ciberseguridad externo, que analiza y prueba el sistema operativo para identificar y eliminar cualquier posible punto vulnerable, puerta trasera, malware o vulnerabilidad de seguridad del sistema.

Invertir en soluciones de red resistentes y seguras

Invertir para garantizar la resistencia y seguridad de la red siempre tiene sentido. Sin embargo, saber dónde invertir mejor puede ser complejo y llevar tiempo: la planificación es clave. Antes de empezar, aquí tiene algunas áreas clave que debe tener en cuenta para garantizar la seguridad y resistencia que necesita su organización:

- Revise y actualice el diseño de su red para asegurarse de que los requisitos de su organización se ven reflejados en la red, incluido el nivel adecuado de resistencia para las áreas sensibles y críticas que afectan a los servicios públicos fundamentales. Para las áreas críticas, considere la posibilidad de añadir servidores de reserva y conexiones múltiples siempre que sea posible y aplicable.
- Tenga en cuenta la importancia cada vez mayor del tiempo de respuesta a incidentes: por ejemplo, utilizamos funciones de inteligencia artificial (IA) y aprendizaje automático (AA) para que nuestro Alcatel-Lucent OmniVista Network Advisor identifique y resuelva los problemas con mayor rapidez. Esta herramienta garantiza que los problemas se resuelvan antes de que afecten a los usuarios finales, identificando y abordando de forma proactiva los problemas de red o de seguridad. Agiliza la resolución de problemas y mejora la seguridad de la red mediante auditorías de configuración y la administración de alertas en tiempo real sobre cualquier cambio repentino en el comportamiento de la red.
- Considere el uso de conmutadores reforzados para entornos adversos. La familia Alcatel-Lucent Enterprise de conmutadores Ethernet robustos está diseñada específicamente para destacar en entornos difíciles y temperaturas extremas. Estos conmutadores están fabricados con componentes resistentes y alojados en robustas carcasas, lo que garantiza su durabilidad y fiabilidad, y cuentan con el mismo sistema operativo que el resto de los conmutadores ALE. Para aumentar la seguridad y proteger la información sensible, algunos modelos de conmutadores están equipados con alertas de intrusión y relés de alarma que permiten la conexión de sistemas de alarma externos. Algunos modelos incluso son compatibles con MACsec, con lo que se logran comunicaciones de datos seguras entre los dos extremos. La capacidad de chasis virtual en los conmutadores robustos ofrece redundancia, resistencia y escalabilidad mejoradas.

Soluciones de comunicaciones resistentes y seguras

Las comunicaciones son fundamentales para que las administraciones públicas interactúen con los ciudadanos, los grupos de interés y otros organismos gubernamentales, así como para la difusión de información importante. Los sistemas de comunicaciones deben estar disponibles en tiempos de crisis, cuando los ciudadanos más necesitan la ayuda de las instituciones públicas. La resistencia y la seguridad evolucionan, y las revisiones periódicas ayudarán a mantener su solución de comunicaciones de Alcatel-Lucent Enterprise segura y disponible.

Las soluciones de comunicaciones de ALE son de diseño seguro. Esto significa que tenemos en cuenta la seguridad en cada paso de la definición, el desarrollo y la entrega del producto. Todo el hardware y los sistemas operativos están reforzados, y la protección contra la denegación de servicio (DoS) está integrada. Cumplimos las certificaciones y acreditaciones reconocidas de las normas globales de seguridad y privacidad (ISO 27001, ISO 27017 e ISO 27018). Además, cumplimos las normas de seguridad y privacidad específicas del sector, como la ley Health Insurance Portability and Accountability Act (HIPAA) en EE. UU. y Hébergeurs de Données de Santé (HDS) relativa al alojamiento de datos sanitarios en Francia, así como las normas regionales de seguridad y privacidad, como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea.

Seis prácticas recomendadas para sus soluciones de comunicaciones

A continuación se detallan seis prácticas recomendadas que ayudarán a optimizar al máximo la resistencia y la seguridad integradas en sus soluciones de comunicaciones de ALE.

1. Asegúrese de tener la última versión del software o los parches adecuados para disponer de las últimas mejoras de seguridad para una mejor protección.
2. Considere la posibilidad de adoptar una solución que incluya supervisión de alarmas y recuerde realizar actualizaciones periódicas con los umbrales adecuados. Verifique que las notificaciones por fallos del sistema de comunicación o las alertas de calidad se envían a las personas adecuadas.
3. Revise y aplique una directiva de contraseñas segura, preferiblemente utilizando autenticación externa con un servidor RADIUS. Implemente recordatorios a los usuarios para ayudar a prevenir las estafas telefónicas, que siguen siendo una amenaza en muchos países.
4. Ofrezca formación a los empleados en concienciación sobre la seguridad y consiga que conozcan los riesgos y las medidas de prevención.
5. Asegúrese de realizar copias de seguridad remotas automatizadas del sistema para ayudar a evitar la pérdida de datos de configuración.
6. Tantee la posibilidad de instalar una VLAN para voz específica. Separar la voz del resto del tráfico reduce la posibilidad de contaminación, que podría interrumpir las operaciones e incluso los servicios públicos.

Invertir en soluciones de comunicaciones resistentes y seguras

En los últimos años, el panorama mundial ha puesto de relieve la importancia de las comunicaciones entre la administración pública y los ciudadanos. A continuación se indican algunas áreas clave que deben tener en cuenta los organismos públicos que tengan previsto invertir en una solución de comunicaciones para mejorar la resistencia y la seguridad.

- Arquitectura redundante y resistente. Su arquitectura debe ser completamente redundante y resistente. Duplicar los servidores de llamadas en las áreas críticas, implementar la redundancia de sitios remotos y duplicar los servidores de aplicaciones críticas puede proporcionar una protección adicional.
- Cree un flujo de trabajo con Rainbow y/o el asistente de notificación visual Alcatel-Lucent Visual Notification Assistant (VNA) con desencadenadores automáticos (ya sean humanos, de IoT o de sistema) para notificar a las personas clave de los problemas del sistema para que actúen rápidamente y aceleren el proceso de recuperación
- Implemente un cifrado sólido. El cifrado se basa en estándares del sector diseñados nativamente en la solución, sin que afecten a la calidad y rendimiento de la voz

- Implemente Rainbow™ by Alcatel-Lucent Enterprise, la herramienta de colaboración ideal para complementar las soluciones de comunicaciones de ALE. Rainbow ofrece un conjunto completo de funciones, como voz, video y mensajería instantánea, que facilitan unas comunicaciones fluidas y una colaboración eficaz. Con Rainbow, puede intercambiar imágenes, videos y señales de videovigilancia, lo que mejorará el reconocimiento contextual y permitirá una mejor toma de decisiones. Rainbow también proporciona comunicaciones híbridas con conectividad segura entre las instalaciones y la nube. Garantiza unas comunicaciones resistentes, que lo mantendrán conectado con compañeros de trabajo y clientes mediante Rainbow, proporcionando una conectividad ininterrumpida incluso en situaciones difíciles. Las comunicaciones híbridas también tienen la ventaja de que las operaciones en la nube y en las instalaciones se ejecutan desde diferentes ubicaciones para lograr la máxima resistencia y mantener las comunicaciones abiertas.
- Para los organismos con requisitos de seguridad más estrictos, Rainbow Edge ofrece una alternativa in situ con una instancia de nube privada. La instancia puede alojarse en cualquier centro de datos, lo que proporciona un control total sobre los servidores, el almacenamiento y las redes, permitiendo a las agencias personalizar y configurar la infraestructura de acuerdo con sus necesidades. Se pueden aplicar políticas de seguridad personalizadas y gestionar los recursos de forma autónoma. Este nivel de control proporciona visibilidad y autoridad completas sobre la infraestructura, lo que permite a los organismos tomar decisiones con conocimiento de causa y optimizar el rendimiento en consonancia con sus objetivos.
- Defina una estrategia de comunicación segura del personal distribuido. ALE ofrece múltiples opciones de comunicaciones y colaboración para los empleados distribuidos, móviles y que trabajan desde casa, entre las que se incluyen las siguientes:
  - Rainbow
  - IP Desktop softphone
  - ALE Softphone
  - Teléfono de escritorio con VPN incorporada de implementación masiva con seguridad integrada (VPN)

Protección de personas y activos

ALE ofrece sistemas de notificación y comunicaciones en tiempo real, flexibles, seguros y de alta disponibilidad. Estas soluciones pueden integrarse en las operaciones de los centros de control de seguridad pública o de ciudades inteligentes, agilizando la distribución y la priorización de llamadas, facilitando el intercambio de información contextual con datos de IoT y reforzando los esfuerzos de colaboración entre el personal de primera intervención y diversos grupos de interés, lo que permite mejorar la toma de decisiones y la coordinación.

La capacidad de interconectar dispositivos IoT dentro de edificios, recintos y ciudades, combinada con el análisis y la IA, está transformando de raíz el panorama de las comunicaciones. Mediante la integración de sensores, videovigilancia, flujo de trabajo Rainbow e IA, es posible pasar de un enfoque reactivo a uno proactivo, lo cual mejorará la eficiencia de los procesos en términos de tiempo y costes. Esta integración facilita una comprensión global del contexto, respalda los procesos de toma de decisiones y, en consecuencia, reduce los tiempos de respuesta en caso de emergencia. Además, funcionalidades como el seguimiento de activos y el control de cerraduras y luces inteligentes agilizan las operaciones. Asimismo, la posibilidad de grabar las comunicaciones y registrar las acciones simplifica el análisis posterior al suceso, mejorando los procesos de seguridad y mitigando posibles responsabilidades. Para lograr estos avances, es fundamental contar con un entorno conectado con acceso Wi-Fi ubicuo y una incorporación sencilla del IoT.

En el caso de las plataformas de comunicaciones en tiempo real urgentes, seguras y de alta disponibilidad, una infraestructura sólida se hace vital para garantizar un funcionamiento fluido. Su infraestructura tecnológica debe incluir el software adecuado, protocolos de red de alta disponibilidad y la flexibilidad para incorporar conmutadores de red resistentes que puedan integrarse perfectamente en su ecosistema y soportar condiciones ambientales adversas, como flujo de aire limitado, golpes y temperaturas climáticas extremas. Optar por equipos industriales de uso rudo garantiza la longevidad en lugares tan difíciles, donde los equipos no robustos serían menos duraderos.

En el campo de los sistemas de seguridad física, hay mucho en juego. Cada minuto y cada secuencia de video puede ser crucial para que las autoridades identifiquen irregularidades, localicen el origen de un incidente o comprendan la causa de una catástrofe. Una sólida infraestructura de videovigilancia es fundamental.
La infraestructura de red no solo debe proporcionar suficiente ancho de banda y Power over Ethernet (PoE) para las cámaras de vigilancia, sino que también debe integrarse perfectamente con los sistemas de gestión de videovigilancia. Esta integración garantiza una red de vigilancia eficaz y fiable con un funcionamiento fluido y una fácil resolución de problemas. El equipo de operaciones debe ser capaz de resolver rápidamente cualquier problema de vídeo, especialmente en entornos en los que cada fotograma de vídeo es de suma importancia. Las integraciones de la solución Alcatel-Lucent OmniSwitch®, logradas a través de complementos con los principales sistemas de gestión de vídeo, le permiten alcanzar este objetivo vital.

Además, hay situaciones en las que se hace necesario el seguimiento de activos o la localización de personas o equipos dentro de su organización. La eficacia de la solución de seguimiento de activos depende de su capacidad para localizar personas y activos de manera fácil y precisa. Este sistema también mejora la seguridad y la protección al permitir el envío rápido de ayuda cuando se conoce la ubicación de las personas. La solución de seguimiento de activos Alcatel-Lucent OmniAccess® Asset Tracking localiza rápidamente a personal y equipos y los muestra en un mapa de planta. El seguimiento de activos también proporciona información sobre los patrones de uso; saber si los activos se utilizan en exceso o se infrautilizan puede proporcionar información valiosa.

Soberanía y seguridad de los datos

Alcatel-Lucent Enterprise sobrepasa a otros proveedores de tecnología a la hora de implementar las prácticas recomendadas necesarias para la ciberseguridad de extremo a extremo. En ALE:

- Seguimos las prácticas recomendadas y otras recomendaciones del Instituto Nacional de Ciencia y Tecnología (NIST) a la hora de realizar evaluaciones de riesgos sobre nuevas funciones y de implantar funciones de ciberseguridad, como el cifrado nativo, en nuestras soluciones.
- Contamos con el Certificado Common Criteria EAL2
- Aplicamos las normas ISO 27001 a todas nuestras soluciones basadas en la nube
- Admitimos ZTNA, segmentación granular de la red y políticas de seguridad muy específicas para reducir el riesgo de actividades no autorizadas
- Ejecutamos pruebas específicas de seguridad altamente especializadas, como pruebas de penetración, en nuestros productos
- Garantizamos que nuestros productos obtienen las certificaciones clave del sector, como HDS, HIPAA y la Ley de Derechos Educativos y Privacidad Familia (FERPA)
- ALE International cumple la Directiva sobre seguridad de las redes y de la información (Directiva SRI 2) de la Unión Europea.

Como expertos reconocidos en ciberseguridad, contribuimos a las propuestas de directivas sobre ciberseguridad de la Unión Europea. También aprovechamos nuestra experiencia en ciberseguridad para ayudar a nuestros clientes a elegir e implantar la combinación adecuada de soluciones de colaboración y comunicaciones unificadas seguras para satisfacer sus necesidades y formar a sus empleados en las prácticas de ciberseguridad recomendadas.

Alcatel·Lucent Enterprise