Priorizar la resiliencia y la seguridad

Soluciones Alcatel-Lucent Enterprise para el sector educativo

Alcatel·Lucent Enterprise

Libro electrónico

Índice

Descripción general

Ante los crecientes retos mundiales y el aumento de los riesgos cibernéticos y físicos, los campus deben dar prioridad a la gestión de riesgos, salvaguardar las infraestructuras fundamentales y proteger al alumnado y el profesorado. Según EdTech Magazine, los ciberataques contra universidades se dispararon un 70 % en 2023.[1] Se espera que la actividad del sector educativo continúe, sea cual sea la situación y que los estudiantes y el personal 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 educativo y por qué las TIC son más importantes que nunca

En los últimos años, la transformación digital en el sector educativo ha avanzado rápidamente, con un número cada vez mayor de estudiantes y personal que acceden a servicios digitales. La transformación digital también ha permitido a determinados empleados de los centros educativos adoptar un estilo de trabajo desde cualquier lugar. Existe una presión creciente sobre los campus para que sigan acelerando la transformación digital. Según Educause, «la enseñanza universitaria ya no es inmune a las altas expectativas y preferencias de los estudiantes por el servicio digital».[2]

Alcatel-Lucent Enterprise trabaja con centros educativos de todo el mundo y reconoce la importancia de proteger a los alumnos, el personal, 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 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 (TI/TO). En el pasado, los equipos de TI y de 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 de 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 implementan rápidamente en muchos campus. 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 cuanto 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: tecnología no autorizada 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 los campus, así como de la prestación de servicios a los estudiantes y el personal. Debido a la naturaleza sensible de la información contenida en las redes de los campus y a los servicios esenciales gestionados por los centros educativos, 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 los campus presten servicios estudiantiles 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 costes adicionales de licencias.

Siete mejores prácticas para las soluciones de red

A continuación se describen siete mejores prácticas para garantizar la máxima optimización de la resistencia y la seguridad integradas en su solución de red de Alcatel-Lucent Enterprise.

1. Revise periódicamente su solución con su Business Partner para asegurarse de que tiene instalada la última versión del software, los parches y las mejoras de seguridad. Una herramienta de gestión del ciclo de vida como ALE PALM, que proporciona información sobre la obsolescencia y el final de la vida útil, es también es ventaja. Los campus pueden planificar con antelación la sustitución del hardware y anticipar la implantación.
2. El código diversificado seguro de ALE aleatoriza la ubicación de diferentes segmentos de código en sus conmutadores, lo que aumenta considerablemente la seguridad. Además, este código está sujeto a un proceso de verificación y validación independientes (IVV) dirigido por un experto en ciberseguridad externo que analiza y prueba el sistema operativo de ALE para identificar y eliminar cualquier posible punto vulnerable, puerta trasera, malware o vulnerabilidad de seguridad del sistema en todas las nuevas versiones.
3. Adopte una estrategia de seguridad de confianza cero e implante un acceso a la red de confianza cero. La macrosegmentación y microsegmentación de su red es crucial para mantener una infraestructura resistente. Siga el enfoque por fases de ALE para la microsegmentación a fin de garantizar la correcta implementación y no provocar consecuencias destructivas. Supervise, valide, planifique, simule y haga cumplir.
4. Use la conexión de ruta más corta (SPB) para lograr redundancia mediante la capacidad de redirigir dinámicamente el tráfico utilizando varias rutas en caso de que falle una. También crea una red eficiente y contenerizada automáticamente.
5. Considere 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 su red, siendo compatible con las actualizaciones de software en servicio (ISSU) y posibilitando interconexiones en anillo. El chasis virtual presenta una solución rentable para simplificar la gestión de la red a la vez que garantiza una alta disponibilidad.
6. Utilice las capacidades del sistema de gestión de red Alcatel-Lucent OmniVista® Network Management System. El gestor de red OmniVista Resource Manager garantiza que dispone de todas las copias de seguridad de configuración de los conmutadores de red y podrá restaurarlas en el peor de los casos o cuando sea necesario. Esta potente herramienta gestiona el ciclo de vida completo del proceso de copia de seguridad y restauración.
7. Implemente 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.

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 laborioso: 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:

- Junto con su Business Partner, 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 de campus fundamentales. Para las áreas críticas, considere la posibilidad de añadir servidores de reserva y conexiones múltiples siempre que sea posible y aplicable.
- Mejore la respuesta a incidentes, utilizando las capacidades de inteligencia artificial (IA) y aprendizaje automático (AA) con el Alcatel-Lucent OmniVista Network Advisor. 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 otros conmutadores ALE. Para aumentar la seguridad y proteger la información sensible, algunos modelos están equipados con alertas de intrusión y relés de alarma que permiten la conexión de sistemas de alarma externos. Algunos modelos incluso admiten MACsec (control de acceso de medios y seguridad) para comunicaciones de datos seguras. La capacidad de chasis virtual en los conmutadores robustos ofrece redundancia, resistencia y escalabilidad mejoradas.
- Imparta formación técnica sobre ALE al equipo de operaciones de red para ayudarlos a detectar problemas y reaccionar con rapidez ante ellos

Soluciones de comunicaciones resistentes y seguras

Las comunicaciones son fundamentales para que los centros educativos interactúen con los estudiantes, el personal y otros centros, así como para la difusión de información importante. Los sistemas de comunicaciones deben estar disponibles en tiempos de crisis, cuando los estudiantes y el personal más necesitan la ayuda de los campus. 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). También 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 UE.

Siete mejores prácticas para sus soluciones de comunicaciones

A continuación se detallan siete prácticas recomendadas para garantizar la máxima optimización de la resistencia y la seguridad de sus soluciones de comunicaciones de ALE.

1. Revise periódicamente el estado del sistema con su Business Partner para asegurarse de que se ha instalado la última versión del software, los parches y las mejoras de seguridad, y de que su contrato SPS está al día.
2. Revise periódicamente los componentes de seguridad y continuidad del servicio de su sistema de gestión de red Alcatel-Lucent OmniVista 8770 Network Management System, que incluye valiosa información y funciones de resistencia y seguridad para su solución de comunicaciones
    - Considere la posibilidad de realizar copias de seguridad remotas automatizadas del sistema para evitar la pérdida de datos de configuración.
    - Configure la supervisión de alarmas y asegúrese de que se actualiza periódicamente con los umbrales adecuados. Además, verifique que las notificaciones por fallos del sistema de comunicación o las alertas de calidad se envían a las personas adecuadas.
3. Revise y haga cumplir una política estricta de contraseñas, preferiblemente mediante autenticación externa (servidor RADIUS), y ponga en marcha recordatorios para los usuarios a fin de evitar el fraude telefónico, que sigue siendo una amenaza en muchos países.
4. Capacite a los empleados y asegúrese de que conozcan los riesgos y las medidas de prevención
5. Revise el estado, la idoneidad y la capacidad de servicio de los servidores de aplicaciones empresariales fundamentales.
6. Tantee la posibilidad de instalar una VLAN específica para voz. Separar los datos de voz del resto del tráfico reduce la posibilidad de contaminación, la cual podría interrumpir las operaciones y, posiblemente, los servicios del campus.
7. Asegúrese de que sus controladores de límites de sesión están configurados correctamente. Los requisitos pueden haber cambiado con el tiempo.

Invertir en soluciones de comunicaciones resistentes y seguras

En los últimos años, el entorno educativo ha puesto el focos sobre la importancia de la comunicación con los estudiantes, el profesorado y el resto del personal. A continuación se indican algunas áreas clave que deben tener en cuenta los campus que tengan previsto invertir en una solución de comunicaciones para mejorar la resistencia y la seguridad.

- Arquitectura 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.
- Los clientes que utilicen TDM DECT deben considerar la posibilidad de ampliar la cobertura a las áreas críticas para proporcionar resistencia en caso de fallo del sistema IP
- 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, de modo que puedan actuar rápidamente y acelerar 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™ de 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, vídeo y mensajería instantánea, que facilitan unas comunicaciones fluidas y una colaboración eficaz. Con Rainbow, puede intercambiar imágenes, vídeos 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 y le proporcionarán 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 ofrecer lo último en resistencia y comunicaciones abiertas.
- Para los campus 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 los centros educativos 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 su infraestructura, lo que permite a los campus 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 los campus 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 los diversos grupos de interés, lo que permite mejorar la toma de decisiones y la coordinación.

La capacidad de interconectar dispositivos IoT dentro de edificios, combinada con el análisis y la IA, está transformando de raíz el panorama de las comunicaciones. Mediante la integración de sensores, videovigilancia, Rainbow e IA, el paso de un enfoque reactivo a uno proactivo mejora la eficiencia en términos de tiempo y costes. Esta integración facilita una comprensión contextual completa, respalda los procesos de toma de decisiones y, en consecuencia, reduce los tiempos de respuesta a las solicitudes.

Funcionalidades como el seguimiento de activos y el control de cerraduras y luces inteligentes agilizan las operaciones. Además, 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 con su ecosistema y soportar condiciones ambientales adversas, como flujo de aire limitado, golpes y temperaturas climáticas extremas. Los equipos robustos garantizan la longevidad en lugares tan difíciles.

En lo que respecta a los sistemas de seguridad física, hay mucho en juego. Cada minuto y cada secuencia de vídeo puede ser crucial para identificar irregularidades, localizar el origen de un incidente o comprender la causa de alteraciones en el campus. Una sólida infraestructura de videovigilancia es fundamental.

La infraestructura de red no solo debe proporcionar suficiente ancho de banda y alimentación a través de 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. Esto permite al equipo de operaciones resolver rápidamente cualquier problema de vídeo, especialmente en entornos o situaciones 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, lo ayudan a alcanzar este objetivo vital.

Para los momentos en los que se hace necesario el seguimiento de activos o la localización de personas o equipos dentro de su organización, una solución eficaz de seguimiento de activos puede localizar con facilidad y precisión a personas y activos. 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 plano de planta. El seguimiento de activos también proporciona información sobre los patrones de uso, lo que ayuda a los campus a evaluar si los activos están sobreutilizados o infrautilizados.

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, nosotros:

- 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 o HIPAA, así como que cumplen la Ley de Derechos Educativos y Privacidad Familiar (FERPA)

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