Cuestiones técnicas a la hora de diseñar un sistema de vídeo IP

Nueve aspectos informáticos fundamentales
a la hora de diseñar un sistema de vídeo IP

sourceSecurity.com
making the world a safer place

Alcatel·Lucent
Enterprise

Índice

Alcatel-Lucent Enterprise encargó a SourceSecurity.com la elaboración de este documento.

Introducción

Un sistema de videovigilancia tiene necesidades especializadas en lo que respecta a la tecnología de la información (TI). Aunque un sistema de vídeo digital puede utilizar las mismas tecnologías que otros sistemas informáticos, se configuran de forma diferente y teniendo en cuenta las necesidades específicas de la videovigilancia.

El vídeo es un entorno más exigente y supone una mayor carga de trabajo para todos los componentes de un sistema informático. Dada la tensión, y especialmente en el caso de un sistema empresarial más grande, las cosas pueden empezar a romperse. Elegir el equipo adecuado para el trabajo garantiza una mayor fiabilidad con el tiempo.

Alcatel-Lucent Enterprise colaboró con los expertos del sector SourceSecurity.com y Stone Security para identificar los nueve aspectos informáticos fundamentales a la hora de diseñar un sistema de vídeo IP. En este documento técnico, analizamos de qué manera influirán las necesidades especializadas de un sistema de videovigilancia en las tecnologías informáticas que se implementen y en el uso que se haga de ellas.

1. El papel de los conocimientos informáticos en los sistemas de vídeo

Diseñar y crear un sistema de videovigilancia basado en el protocolo de internet (IP) requiere un alto nivel de conocimientos informáticos en la comunidad de integradores.

Algunos integradores tienen habilidades suficientes para poner en marcha de forma experta un sistema de vídeo IP, mientras que otros pueden tener dificultades.

La formación y certificados adicionales conocidos por la mayoría en el mundo de las TI pueden permitir a los integradores ofrecer el alto nivel de servicio requerido. Para empezar, los instaladores deben tener la aptitud adecuada y unos conocimientos básicos de redes y resolución de problemas.

Los integradores pueden garantizar una plantilla competente limitando su abanico de opciones tecnológicas y asegurándose de que cada empleado esté bien formado en el menor número de tecnologías. Elegir las mejores soluciones y asegurarse de que los empleados son expertos en esos productos permite al integrador ofrecer a sus clientes un sistema de mayor calidad.

Limitar la combinación de productos también permite al integrador comprender mejor la amplitud de funciones que ofrece un producto determinado. Con demasiada frecuencia, un cliente adquiere un sistema que ofrece una serie de funciones y luego solo utiliza un número limitado de ellas en el día a día, lo que resta valor al sistema por el que ha pagado.

Los integradores pueden ayudar a los clientes formándolos para que saquen el máximo partido del sistema que compren.

Los integradores también pueden depender de los servicios de consultoría previa de los fabricantes de equipos para orientarse. En algunos casos, los fabricantes de equipos tienen conocimientos específicos sobre diversos mercados verticales, acumulados a lo largo de una historia de servicio a esos mercados.

Los fabricantes que se toman en serio un mercado vertical específico contratarán a expertos del sector para garantizar un soporte específico para las necesidades de cada cliente. Su orientación puede ayudar a los integradores a triunfar en nuevos mercados y/o a racionalizar las mejores prácticas de los mercados en los que operan.

Los fabricantes también ofrecen formación y certificados para garantizar que los integradores estén bien equipados para instalar sus sistemas. Se debe impartir una formación eficaz y práctica en sesiones más cortas que respeten el valor del tiempo de cada asistente.

2. Reestructuración de los equipos para satisfacer las necesidades de videovigilancia

Cuestiones como los requisitos de ancho de banda y Power Over Ethernet (PoE) son variables importantes en un sistema de vídeo. Además, el servidor de vídeo tiene una carga mayor, sobre todo cuando se trata de vídeo de una transmisión en directo. Todos los datos llegan al servidor, incluso los que no se registran.

El vídeo se almacena, lo que garantiza que hay al menos un par de segundos de vídeo que se pueden conservar antes de una grabación de vídeo real activada por alarma. En el caso de identificar una imagen que se aproxima desde una distancia mayor, pueden ser necesarios períodos de almacenamiento más largos. Todas las entradas y salidas pasan por el servidor, aunque un volumen limitado de datos se escribirá en el almacenamiento a largo plazo.

Existe una diferencia fundamental entre cómo ven el tamaño del sistema los integradores de sistemas de seguridad y cómo lo ven los profesionales de TI. Los integradores de sistemas suelen hablar más en términos de número de cámaras, mientras que los profesionales de TI suelen hacerlo más en términos de gestión de datos desde el sistema. Ambos están intrínsecamente relacionados, por supuesto, pero la relación no es lineal. En general, un mayor número de cámaras equivale a más datos que debe gestionar el departamento informático. Sin embargo, hay otros factores que influyen en las necesidades de datos, como el número de fotogramas, los requisitos de calidad de la imagen, las necesidades de almacenamiento, las aplicaciones diurnas/nocturnas y el uso de análisis de vídeo.

Una competencia clave a la hora de especificar un sistema de seguridad IP es traducir los requisitos de equipamiento y funcionalidad del sistema en los datos necesarios para satisfacer esas necesidades. Para un sistema local, esto equivale a la necesidad de especificar un servidor informático que maximice el rendimiento del sistema al tiempo que reduce los costes. Cuestiones como la virtualización y los sistemas en nube pueden complicar la ecuación y, al mismo tiempo, ofrecer una nueva flexibilidad.

Otra variable relacionada con el diseño del sistema es el uso de cámaras en el perímetro de la red para grabar vídeo mediante tarjetas SD. Hoy en día existen incluso sistemas "sin servidor"; por ejemplo, toda la grabación tiene lugar en el perímetro. Este planteamiento, en efecto, desplaza la carga computacional del servidor a la periferia, con la consiguiente reducción de la necesidad de capacidad del servidor. Las cámaras actuales proporcionan datos más allá del flujo de vídeo, como metadatos y audio, que también influyen en el diseño del sistema.

Los profesionales de TI deben tener una visión completa del sistema en su conjunto, como lo que se va a conectar, las velocidades de fotogramas, la resolución y los códecs de vídeo de las cámaras. Con esta información, pueden calcular los requisitos de la red, la potencia, los servidores, la capacidad de disco, la memoria, el almacenamiento y la posibilidad de utilizar sistemas en la nube o en las instalaciones. Esto garantiza un planteamiento exhaustivo y reflexivo del diseño y la implementación.

Los fabricantes ofrecen "calculadoras" de software para ayudar a los integradores a diseñar sistemas traduciendo los requisitos del sistema en especificaciones de equipos específicos. Tenga en cuenta que los cálculos deben cumplir o superar las expectativas y permitir el crecimiento futuro.

La implementación de sistemas en la nube es otra variable a la hora de diseñar sistemas de videovigilancia. La tendencia clara es hacia el uso de más sistemas en la nube para la videovigilancia. Sin embargo, la elección de la nube frente a las soluciones locales debe hacerse en función de cada caso. Los diseñadores de sistemas y los usuarios finales deben resistirse a la aparente inevitabilidad de la nube y, más bien, tomar decisiones basadas en las necesidades del cliente.

Muchos fabricantes se ven presionados para trasladar sus sistemas a la nube, pero lo ideal sería que ofrecieran a sus clientes la posibilidad de elegir entre varios sistemas y no una solución universal.

Los fabricantes están en una buena posición para asesorar a los clientes sobre la conveniencia de una configuración en la nube frente a un diseño local. Los integradores también deben conocer bien las ventajas de uno u otro enfoque o facilitar al cliente la decisión en uno u otro sentido. El mercado no debería estar enviando las aplicaciones a la nube a menos que ese sea el enfoque óptimo para cada cliente concreto.

3. El papel fundamental de las redes

Un sistema de vídeo es tan fuerte como su eslabón más débil. Puede que los conmutadores de red no sean tan visibles como las cámaras y los VMS, pero no por ello son menos críticos.

Sin embargo, lo que suele ocurrir es que los clientes dan por sentado el funcionamiento de una red, prestando poca atención a cómo funciona o a cómo maximizar su utilidad. De hecho, algunos clientes quieren instalar un sistema de vídeo utilizando una infraestructura de red existente. Esto se puede hacer, pero la capacidad de optimizar la parte de red de un sistema de vídeo puede ser limitada.

Lo ideal es que el cliente opte por los mejores conmutadores para la videovigilancia, que garantizarán que un sistema funcione de forma eficaz y fiable.

Cada sistema de vídeo es diferente, por lo que prestar especial atención a sus requisitos individualizados garantiza que cumpla su misión única. A la hora de poner en marcha un sistema, la red no debe considerarse un elemento secundario. Por el contrario, debe ensamblarse cuidadosamente utilizando los mejores componentes para permitir y mejorar las operaciones en todo el sistema.

Los conmutadores que funcionan a "velocidad de cable", es decir, que tienen suficiente capacidad de procesamiento para gestionar la velocidad Ethernet completa con tamaños de paquete mínimos, son ahora la norma en el sector. Un nuevo punto de diferenciación entre los conmutadores es la capacidad de comprender y gestionar su tráfico.

En el mercado existen conmutadores no gestionados, pero no suelen utilizarse para aplicaciones comerciales y/o empresariales. Están diseñados para su uso en redes pequeñas con necesidades básicas; no hay ajustes que configurar.

Por el contrario, los conmutadores gestionados permiten detectar y diagnosticar problemas de rendimiento y garantizan un rendimiento fiable de los sistemas de videovigilancia. Permiten a los usuarios ver de forma granular qué puede estar causando problemas en el sistema y dan una idea de cómo es esa información.

El valor de los conmutadores gestionados, que son totalmente configurables, personalizables y proporcionan una serie de datos sobre el rendimiento, se manifestará a lo largo de la vida útil del sistema, ya que proporcionan información importante sobre el funcionamiento del sistema y permiten una resolución de problemas más sencilla para identificar los problemas.

Los conmutadores deben diseñarse para responder a las necesidades de los sistemas de vídeo IP. Un ejemplo, en el caso de un conmutador de 16 puertos, es un balance de potencia suficiente para hacer funcionar todas las cámaras de vídeo conectadas al conmutador. Las cámaras PoE actuales consumen más energía que las generaciones anteriores. Los integradores tienen que saber que un conmutador proporciona la suficiente potencia para gestionar el número de cámaras y el crecimiento futuro.

"A la hora de seleccionar el hardware, queremos que todos los conmutadores tengan la capacidad de ancho de banda y el balance de potencia necesarios, y que sean conmutadores gestionados que nos ahorren mucho tiempo en la resolución de problemas. Nos ahorran dinero y ahorran dinero al cliente. Es una inversión inicial mayor, pero se amortizará a largo plazo al crear un sistema más útil."

Aaron H. Simpson, presidente y director de tecnología, Stone Security

4. Dar más importancia al valor que al precio

La fiabilidad es fundamental en la videovigilancia y comienza con la elección de los equipos.

Optar por componentes de menor calidad puede responder a una necesidad económica en el momento. Sin embargo, a largo plazo, el funcionamiento del sistema sufrirá. El coste de elegir un funcionamiento que no sea el óptimo puede no ser obvio al diseñar un sistema, pero quedará perfectamente claro con el tiempo.

Por otro lado, elegir un equipo mejor –aunque sea más caro– saldrá rentable.

Es fundamental sopesar los costes (como el precio de un equipo mejor) frente a los riesgos de un sistema inadecuado o defectuoso. Adoptar un enfoque de coste total de propiedad (TCO) al evaluar costes y riesgos es la mejor estrategia. Otro elemento de coste a largo plazo a tener en cuenta es el valor de los sistemas abiertos, que pueden garantizar flexibilidad a la hora de ampliar o cambiar un sistema en el futuro.

Siempre es mejor trabajar con un proveedor que ofrezca un producto en el que confíe y al que pueda prestar soporte durante mucho tiempo.

5. Amenazas a la ciberseguridad y soluciones

Históricamente, una ironía del sector de la seguridad física ha sido la falta de atención a la ciberseguridad de los sistemas IP.

Afortunadamente, las partes interesadas en la seguridad física prestan ahora más atención a los problemas de ciberseguridad a todos los niveles y en toda la cadena de suministro de la seguridad física. De hecho, la ciberseguridad se ha convertido en uno de los pilares fundamentales del proceso decisorio para los grandes sistemas de videoseguridad.

Un paso mínimo hacia la protección frente a las ciberamenazas y la restricción del acceso a un sistema es evitar el uso de contraseñas predeterminadas. Estas son menos seguras y pueden ser más fácilmente adivinables por un pirata informático o un bot. De hecho, las contraseñas predeterminadas se han prohibido en California.

Los riesgos de ciberseguridad comienzan en la cadena de suministro, donde los ataques pueden comprometer un producto antes incluso de que se entregue. Analizar un producto en busca de posibles ataques de "puerta trasera" o "desbordamiento de búfer" antes de su entrega puede mitigar la amenaza. Los clientes también pueden optar por instalar virtualmente un "código bueno" tras la entrega de los productos de hardware, garantizando así la ciberseguridad y sobrescribiendo cualquier código malicioso que pudiera haberse instalado durante el envío.

También hay una serie de medidas de ciberseguridad que deben abordarse durante la instalación y en las distintas fases de implementación del sistema. Por ejemplo, la "seguridad de puerto aprendida" garantiza que a un puerto solo acceda un dispositivo autorizado. Si un dispositivo no autorizado intenta conectarse al sistema —por ejemplo, para conectar una nueva cámara—, se activa una alerta y se deniega el acceso al puerto hasta que lo autorice una persona.

La tecnología de conexión de ruta más corta (SPB) puede evitar que las actividades maliciosas salten de un sistema a otro. Se establecen reglas para que una cámara solo pueda transmitir al grabador, y se instala otra potente tecnología de segmentación en redes multi-IoT.

Los sistemas deben desactivar protocolos inseguros como FTP y Telnet, que facilitan la comunicación a través de una red, pero pueden ofrecer más oportunidades a los piratas informáticos. Estas capacidades deben ser "seguras por defecto" para no permitir una conexión a la red a menos que sea intencionada.

Una ciberseguridad eficaz también requiere restringir el acceso físico a un sistema. Si un conmutador se instala en el armario de un conserje, donde el acceso físico está abierto a todo el mundo, no está bien protegido. Permitir el acceso físico a un sistema facilita que cualquiera —incluido un empleado que represente una amenaza interna— conecte un portátil y acceda a todo el sistema.

Las cámaras deben grabar el acceso a los equipos de red como un enfoque de "defensa a fondo".

6. Limitaciones de un planteamiento de "aislamiento físico"

Cuando se trata de proteger los sistemas de vídeo de los ataques de ciberseguridad a través de internet, un método común históricamente ha sido crear sistemas físicamente aislados.

Un sistema físicamente aislado consiste en aislar un ordenador o una red e impedir que establezca una conexión externa. Dado que un ordenador físicamente aislado está físicamente separado y es incapaz de conectarse de forma inalámbrica o física con otros ordenadores o dispositivos de red, este método se considera la panacea para garantizar la ciberseguridad de los sistemas de vídeo.

Sin embargo, es arriesgado depender de este aislamiento como única protección de ciberseguridad. Hay una gran variedad de situaciones en las que un sistema físicamente aislado puede estar expuesto a internet, incluso durante un breve período de tiempo. Cuando eso ocurre, el sistema depende de otras medidas de ciberseguridad —si es que existen— para protegerse del desastre.

Asumir que un sistema estará aislado físicamente para siempre no es una solución para la ciberseguridad. Al contrario, es la crónica de una muerte anunciada.

Los sistemas físicamente aislados tampoco pueden aprovechar la inteligencia artificial (IA) y otras funciones que dependen del acceso a muchos usuarios y del análisis de experiencias compartidas. Los datos de un solo cliente no son tan útiles como los de cientos de clientes, disponibles en la nube. Los sistemas físicamente aislados no permiten a los clientes aprovechar el valor adicional de un análisis más inteligente. Ceder algunos datos (que implica cuestiones de privacidad) es un precio que los clientes pagan para aprovechar un mayor valor.

Dadas las necesidades de los clientes actuales para conectarse a sus sistemas y tener acceso continuo a ellos, los casos prácticos de sistemas físicamente aislados son cada vez más limitados.

Las organizaciones también tienden a retroceder ante la posibilidad de crear una infraestructura de red totalmente independiente para la videovigilancia. No existe una red "separada y segura".

7. Garantizar que no se pierdan datos de vídeo

La pérdida de datos es un problema para cualquier sistema informático, pero mucho más para los sistemas informáticos que proporcionan videovigilancia. Un sistema de videovigilancia es de misión crítica y debe funcionar 24 horas al día, 7 días a la semana. No hay tiempo de inactividad que permita a los administradores diagnosticar y resolver cualquier problema de pérdida de datos; más bien, los problemas deben abordarse continuamente y en tiempo real.

Aquí es donde los conmutadores gestionados pueden ayudar. Los conmutadores gestionados permiten a los administradores de sistemas diagnosticar y solucionar rápidamente cualquier problema de pérdida de datos. También pueden identificar fácilmente la(s) fuente(s) de la pérdida de datos. No hay que "acusar" a ningún componente del sistema.

Los paquetes pueden perderse debido a la conversión de datos de transmisión por fibra a cobre y Ethernet. Los transceptores eléctricos se utilizan para traducir los datos de transmisión por fibra a transmisión eléctrica, y los dispositivos pueden ser una fuente de pérdida de paquetes de datos.

En la videovigilancia, la pérdida de un paquete de datos equivale a poner en peligro una imagen de vídeo, perdiéndose para siempre. No hay forma de restaurar las imágenes de vídeo que se pierden durante las interrupciones por inactividad. Pensemos, por ejemplo, en un casino, donde la consecuencia de que falle un sistema de vídeo es la pérdida de cobertura de una mesa de juego, lo que, a su vez, puede significar también una pérdida de ingresos.

En la amplia variedad de aplicaciones de videovigilancia, la redundancia es necesaria para garantizar un funcionamiento continuo las 24 horas del día, los 7 días de la semana.

La necesidad de fiabilidad debe sopesarse en el contexto del riesgo frente al beneficio. Un sistema puede ser menos costoso, menos complejo y/o menos tolerante a fallos, pero puede que no funcione como estaba previsto, lo cual conlleva sus propios costes.

Otra variable que puede causar problemas de rendimiento en los sistemas de vídeo gira en torno a la distinción entre unidifusión y multidifusión, que son dos métodos para enviar datos a través de una red. La unidifusión proporciona una comunicación individual en la que un único emisor entrega datos a un único receptor. La multidifusión es un modelo "de uno a muchos" en el que un único emisor proporciona datos a varios destinatarios.

Muchas aplicaciones de videovigilancia funcionan en modo unidifusión. Esto significa que una cámara es supervisada en tiempo real por una persona: interviene un único flujo de vídeo.

Sin embargo, algunas aplicaciones requieren multidifusión, en la que un único flujo de vídeo es visto por varios usuarios. Los problemas surgen cuando un sistema pasa de unidifusión a multidifusión. Hacer la transición implica algo más que "pulsar un interruptor", y los matices y detalles del paso pueden causar problemas en el rendimiento del sistema. Pueden surgir problemas si partes de un sistema están configuradas para la unidifusión cuando deberían ser de multidifusión, o al revés. Es fundamental configurar correctamente este punto en todo el sistema.

Las funciones de asesor de red inteligente permiten al usuario final comprender lo que es normal en términos de rendimiento de la red y detectar cuando algo es anormal o se sale de las expectativas habituales. Cualquier desviación se notifica automáticamente, y las personas pueden intervenir cuando sea necesario para resolver los problemas.

8. Gestión de los ciclos de vida en los sistemas de vigilancia IP

En el mundo de las TI, los ciclos de vida de los productos pueden ser de tres a diez años, según el sector y el producto. Existen protocolos para abordar cuestiones como el tiempo medio entre fallos (MTBF), el firmware y los parches de seguridad.

En el ámbito de la videovigilancia, los ciclos de vida de los productos han sido históricamente más largos: hay cámaras de vídeo con décadas de antigüedad que siguen funcionando sobre el terreno. Adaptar las estrategias de gestión de TI a los sistemas de vídeo IP puede revelar una desconexión.

El soporte informático proporcionado por un fabricante aporta un inmenso valor al integrador y al usuario final. Históricamente, los ciclos de vida más largos en seguridad física han dado lugar a sistemas que siguen funcionando más allá del período previsto y en un entorno sin soporte.

Existen riesgos inherentes a seguir utilizando equipos que no cuentan con el respaldo del fabricante. Por ejemplo, no actualizar el firmware puede abrir la puerta a amenazas de ciberseguridad.

La mayoría de los equipos actuales tienen una garantía de cinco años y, siendo realistas, podrían seguir funcionando otros cinco años más. Sin embargo, con el panorama tecnológico en rápida evolución, la mayoría de los clientes querrán aprovechar las capacidades más actuales. En efecto, la aceleración tecnológica equivale a ciclos de vida más cortos en seguridad, al igual que ocurre en el entorno general de las TI y las redes.

9. El ecosistema informático en los sistemas de vídeo

Un ecosistema informático unificado es el mejor enfoque para garantizar el éxito de un sistema de vídeo IP. El éxito de cualquier nueva tecnología depende de un ecosistema informático que la respalde. Cuestiones como la interoperabilidad de hardware y software garantizan el buen funcionamiento del sistema.

Las normas abiertas garantizan a los clientes la máxima flexibilidad en el presente y en el futuro. También son útiles las ofertas simplificadas. Por ejemplo, Alcatel-Lucent Enterprise tiene un único sistema operativo que funciona con todos los conmutadores Ethernet que vende la empresa.

Para garanizar el éxito, mantenga una estrategia de adopción de productos que "funcionen bien" en su entorno y con otros productos del ecosistema.

Un ecosistema informático de éxito no surge de la nada. Más bien se nutre de socios del sector que trabajan juntos para garantizar el éxito. Principios como la apertura y la interoperabilidad contribuyen al ecosistema informático. El éxito aumenta el rendimiento de cada componente de un sistema y del sistema en su conjunto.

Más información sobre las soluciones de videovigilancia de Alcatel-Lucent Enterprise.

Alcatel·Lucent Enterprise