DOCUMENTO TÉCNICO

Los datos de vídeo como prueba

Asegurar la integridad de los datos de vídeo con AXIS Camera Station

Julio 2021

AXIS COMMUNICATIONS

Índice

1 Resumen

Los datos de vídeo de alta calidad, fiables y no manipulados pueden utilizarse como prueba. Las prácticas recomendadas para el manejo de los datos de vídeo como prueba mediante el uso de AXIS Camera Station son:

- Diseñar, configurar y validar el sistema adecuadamente para proporcionar la imagen, la grabación y la seguridad que desea
- Llevar a cabo un mantenimiento regular
- Manejar cualquier prueba según los procedimientos establecidos

2 Introducción

El vídeo de vigilancia está prácticamente hecho a medida para ser utilizado como prueba en los tribunales. Un suceso grabado, por así decirlo, no se puede negar, ¿o sí? Bueno, un juez probablemente aceptaría datos de vídeo de alta calidad, fiables y no manipulados.

Pero también hay casos en los que el valor probatorio del vídeo se reduce sin querer. Por ejemplo, las grabaciones de vigilancia con lagunas temporales, en las que las personas o los vehículos desaparecen repentinamente o "saltan" en la imagen, podrían no considerarse lo suficientemente fiables como para ser utilizadas como prueba. El vídeo también podría cuestionarse si los metadatos, como las marcas de tiempo o la dirección MAC de la cámara, no tienen sentido. Cualquier sospecha de que el vídeo pueda haber sido editado, borrado o manipulado puede reducir la credibilidad del propietario del vídeo.

En este documento técnico se ofrecen consejos sobre cómo gestionar el vídeo como prueba. Más concretamente, describe el papel del software de gestión de vídeo (VMS) AXIS Camera Station en la cadena de pruebas, así como el papel que desempeña el propietario del vídeo.

Figure 1. Si se configura y gestiona correctamente, la videovigilancia en lugares estratégicos puede proporcionar valiosas pruebas

3 Prácticas recomendadas para el manejo de datos de vídeo como prueba

Las empresas y organizaciones que utilizan la videovigilancia deben contar con procesos y procedimientos que determinen cómo manejar y almacenar los datos de vídeo. Para estar totalmente preparado cuando una de sus cámaras capte un incidente, debe asegurarse de que el vídeo esté protegido y que no pueda sobrescribirse, manipularse ni ser robado. También debe ser posible exportar las grabaciones a un almacenamiento seguro y entregarlas a las fuerzas del orden.

Pero la producción de pruebas de vídeo de alta calidad es un proceso que comienza con un diseño claro del sistema de vídeo. También es de suma importancia mantener el sistema actualizado y hacer un seguimiento de cualquier irregularidad. Este capítulo presenta los pasos de este proceso y cómo pueden seguirse con la ayuda de AXIS Camera Station y su paquete de integración.

Si produce un vídeo de vigilancia de acuerdo con estos principios sobre el diseño del sistema, el mantenimiento del sistema y la gestión de incidentes, cumplirá los requisitos actuales de ciberseguridad y, muy probablemente, podrá proporcionar pruebas válidas, en caso de que sea necesario.

Figure 2. El software AXIS Camera Station facilita tanto la configuración, como el funcionamiento diario y la gestión estratégica de un sistema de videovigilancia

3.1 Diseñar el sistema adecuadamente...

Un sistema de videovigilancia debe diseñarse con cuidado. Debe seleccionar el equipo en función de sus necesidades y configurarlo para que proporcione la imagen que desea, el tipo de grabación que quiere y la seguridad que busca conseguir. AXIS Site Designer es una excelente ayuda a este respecto.

3.1.1 Proporcionar la imagen que desea

La calidad de la imagen depende de la cámara y de su colocación. La resolución de la imagen, o más concretamente, la densidad de píxeles en la escena de los hechos, puede calcularse si se conoce el modelo de cámara, el objetivo y la distancia y el ángulo de la cámara con respecto a la escena. Para obtener una densidad de píxeles adecuada en la cara de una persona en la escena, es posible que tenga que desplegar más cámaras o utilizar cámaras con mayor resolución. Debe analizar el campo de visión, los requisitos de iluminación y otros parámetros para cámaras específicas en su instalación concreta. Todo esto se puede diseñar sin problemas en AXIS Site Designer.

3.1.2 Proporcionar las grabaciones que desea

Para la grabación de su vídeo, debe utilizar un hardware de alto rendimiento, validado y con redundancia. Para aumentar la fiabilidad del sistema, AXIS Camera Station admite la grabación en caso de fallo almacenando temporalmente las imágenes en la tarjeta SD de la cámara de red. Si utiliza el análisis

VMD (detección de movimiento por vídeo), asegúrese de que las grabaciones sean lo suficientemente largas como para aportar valor en la verificación de todo el incidente. Las grabaciones con detección de movimiento que no estén calibradas de forma óptima pueden presentar lagunas de tiempo y secuencias inconexas. La grabación continua puede ser una mejor opción en muchos casos, pero requiere mucho más almacenamiento, así como una disponibilidad constante de suficiente ancho de banda.

3.1.3 Proporcionar la seguridad que desea

Debe dotar al sistema de la seguridad física necesaria para evitar el acceso no autorizado. Todos los elementos de hardware, incluidas las cámaras, los equipos y cables de red, los servidores, el almacenamiento de datos, los dispositivos de alimentación y los cables deben estar protegidos. Las medidas de seguridad podrían incluir el mantenimiento de la sala de servidores como un área de acceso restringido, cerrar el armario del servidor, colocar el servidor en bastidor dentro del armario, desactivar los puertos físicos en el servidor y evitar que los cables de red queden expuestos.

También debe esforzarse por dotar al sistema de la ciberseguridad necesaria para minimizar los riesgos de abuso de datos, intentos de manipulación de datos y ataques maliciosos. Este reforzamiento puede ser proporcionado en parte por las herramientas de software y la tecnología, que garantizan que el sistema cumple con las normas de seguridad actuales. Pero el reforzamiento también requiere que el propietario del sistema aplique una mentalidad de ciberseguridad y trabaje activamente para implantarla en toda la organización. Por ejemplo, todos los usuarios del sistema deben ser conscientes de la importancia de utilizar contraseñas seguras y difíciles de adivinar, y tener cuidado de no revelarlas. Los accesos de los usuarios también deben minimizarse, así como los permisos de los usuarios, por ejemplo, utilizando el enfoque de las cuentas de usuarios con menos privilegios. Es responsabilidad del propietario del sistema educar a su personal sobre las prácticas recomendadas y asegurarse de que éstas se apliquen correctamente. Un integrador autorizado puede reforzar el sistema, pero ciertas medidas de ciberseguridad solo pueden ser eficaces con la cooperación activa de las personas que utilizan el sistema.

Una forma importante de lograr una mayor ciberseguridad general es proteger el vídeo mediante el transporte de datos cifrados. Para el transporte de datos entre el cliente y el servidor, AXIS Camera Station utiliza el cifrado AES para el vídeo, el audio y los metadatos, y el cifrado TLS 1.2 para los demás datos. AXIS Camera Station puede configurarse para cifrar también, mediante HTTPS, los flujos de datos entre las cámaras y el servidor. Otras prácticas recomendadas para proteger el software incluyen la desactivación de cualquier servicio que no se utilice, el uso de filtrado de direcciones IP/MAC, la adaptación de IEEE 802.1X, la adaptación de la supervisión de SNMP, la configuración de la fecha y la hora correctas junto con un servidor NTP de confianza (para garantizar la precisión de las marcas de tiempo en los metadatos de vídeo) y el uso exclusivo de Axis Secure Remote Access para las conexiones remotas (en lugar de la redirección de puertos o el escritorio remoto). Para conocer las medidas y recomendaciones de ciberseguridad detalladas, consulte la guía de reforzamiento de ciberseguridad de Axis.

3.1.4 Configurar y validar el sistema

Es posible configurar partes fundamentales del sistema ya cuando se diseña con AXIS Site Designer, con nombres de cámaras, resoluciones y tiempos de retención específicos. Una vez diseñado e instalado el sistema, las configuraciones establecidas en AXIS Site Designer pueden importarse automáticamente a AXIS Camera Station, desde donde podrá seguir retocando y ajustando la configuración si lo desea.

Una vez completada la instalación real, puede validar el sistema con AXIS Installation Verifier, que forma parte del paquete de integración de AXIS Camera Station. El verificador de la instalación prueba el sistema en modo normal y en modo nocturno para verificar que hay suficiente ancho de banda durante el funcionamiento con poca luz, cuando los niveles de ruido son más altos y se necesita más ancho de banda. A continuación, AXIS Installation Verifier realiza una prueba de estrés aumentando constantemente el

volumen de datos generado en el sistema hasta que se encuentra el primer cuello de botella. Esto revelará la capacidad sobrante del sistema e indicará si es necesario mejorarlo.

3.2 Llevar a cabo un mantenimiento regular

Una vez que el sistema esté en funcionamiento, es necesario seguir supervisándolo y actualizándolo.

Asegúrese de que tanto el hardware como el software sigan funcionando como se espera. Inspeccione la calidad del vídeo, limpie los objetivos de las cámaras según el calendario previsto, compruebe que no ha habido ninguna manipulación física y que el campo de visión y la dirección de las cámaras no han cambiado. Estudie los registros del sistema con regularidad, ya que proporcionan información sobre los inicios de sesión, las conexiones y los problemas de los dispositivos. AXIS Camera Station proporciona notificaciones sobre muchas irregularidades detectadas y las guarda en los registros del sistema. Reenvíe los registros a un almacenamiento remoto de solo lectura, en particular después de cualquier incidente importante. Axis también proporciona una supervisión del estado del sistema en línea como parte del paquete de integración, que le permite supervisar todas las instalaciones y proporciona el estado del sistema para facilitar el servicio y el mantenimiento.

Tanto el hardware como el software (sistema operativo y VMS) deben actualizarse periódicamente. Al utilizar siempre las últimas versiones de software y firmware, su sistema se beneficiará de los últimos parches de seguridad y correcciones de errores. Lo idóneo es que el VMS encuentre todas las actualizaciones de software y firmware de forma automática y que solicite la instalación de la actualización o que simplemente se actualice de forma automática. Cualquier software que descargue debe proceder de fuentes de confianza.

3.3 Manejar cualquier prueba según los procedimientos establecidos

Si ha aplicado los principios sobre el diseño y el mantenimiento de su sistema de vigilancia correctamente, AXIS Camera Station debería ser capaz de proporcionar pruebas fiables de cualquier incidente captado por sus cámaras. A continuación, hay que disponer de procedimientos sobre cómo proceder.

Debe seguir cualquier consejo de las fuerzas del orden. En caso de un delito grave, la organización encargada de hacer cumplir la ley tiene derecho a decidir cómo deben protegerse las pruebas, y usted debe seguir sus instrucciones.

En otros casos, el proceso principal es la exportación segura de las pruebas. Esto significa poder proporcionarlas fuera de su sistema exactamente del mismo modo y con la misma credibilidad que dentro.

La exportación debe ser manejada por un operador designado, preferiblemente junto con un testigo. Este operador podría ser un profesional externo contratado únicamente con el fin de proporcionar y documentar una exportación fiable. El uso de una tercera parte independiente para la exportación podría minimizar el riesgo para el propietario del vídeo de ser sospechoso de manipular las pruebas. El operador debe asegurarse de exportar un vídeo que cubra el incidente real, pero que también proporcione suficiente información sobre los acontecimientos que lo han provocado, así como sobre las secuelas.

Los vídeos seleccionados pueden exportarse a discos de solo lectura, como CD-R, DVD-R o Blu-ray (-R), que pueden entregarse a las fuerzas del orden. Una alternativa es exportar los clips de vídeo a archivos zip con cifrado y protegidos con una contraseña. Los archivos pueden ser firmados digitalmente con una firma que contenga el hash con la contraseña del usuario. Para confirmar el hash y compararlo con el hash actual del archivo, la firma debe introducirse en el reproductor de archivos de AXIS. Si los hashes coinciden, significa que no se ha modificado ningún dato en ese archivo.

Axis también proporciona el informe de incidencias de AXIS Camera Station, que funciona como una herramienta de exportación avanzada para los operadores. La herramienta debe ser configurada de antemano por un administrador que proporcione datos como las etiquetas de los incidentes y la ubicación de la exportación. A continuación, el informe de incidentes automatiza la exportación, permitiendo exportar vídeos organizados en incidentes y usar etiquetas como nombres de carpetas. La ubicación puede establecerse en un recurso local, por ejemplo, el almacenamiento en red tipo NAS o en un recurso remoto, por ejemplo, el almacenamiento en la nube si es accesible a través del protocolo SMB. El informe constará de archivos de vídeo, instantáneas en formato .jpg (creadas en AXIS Camera Station manualmente por el operador al crear el informe), marcadores en formato .txt y toda la información recogida en un informe en formato .pdf.

4 Recursos de ciberseguridad

En Axis reforzamos la ciberseguridad en el diseño, el desarrollo y las pruebas de nuestros dispositivos para minimizar el riesgo de errores que podrían aprovecharse para un ataque. Seguimos las mejores prácticas del sector en materia de ciberseguridad, por ejemplo, en lo que respecta a la gestión de las vulnerabilidades de seguridad, los requisitos para la transmisión y el almacenamiento seguros de los datos y el cifrado. Nos esforzamos para que le resulte fácil y rentable aplicar los controles de seguridad adecuados, y nuestros dispositivos son compatibles con el cifrado y la gestión de la seguridad.

Aunque Axis, como fabricante y proveedor, se esfuerza por ofrecer el sistema o la solución más completa y segura, usted, como usuario final, tiene una gran responsabilidad: aplicar las mejores prácticas de seguridad por su parte. Axis proporciona varias herramientas, guías y tutoriales para ayudarle. Vaya a www.axis.com/cybersecurity, donde encontrará, por ejemplo, guías de reforzamiento, información sobre la gestión de la seguridad y entradas del blog sobre ciberseguridad.

T10169774/ES/M1.2/2107

Acerca de Axis Communications

Axis contribuye a crear un mundo más inteligente y seguro a través de soluciones para mejorar la seguridad y el rendimiento empresarial. Como empresa de tecnología de red y líder del sector, Axis ofrece soluciones de videovigilancia, control de acceso y sistemas de audio e intercomunicación. Se ven reforzadas por aplicaciones de análisis inteligentes y respaldadas por formación de alta calidad.

Axis tiene alrededor de 4000 empleados dedicados en más de 50 países y colabora con socios de integración de sistemas y tecnología en todo el mundo para ofrece soluciones personalizadas. Axis se fundó en 1984 y la sede está en Lund, Suecia