Visión general de la ciberseguridad de CathexisVision 2020

Contenido

1 Introducción[1]

Cathexis lleva más de 20 años desarrollando y suministrando soluciones de gestión de vídeo al mercado mundial. La seguridad, tanto en el acceso a los datos como en la integridad de los mismos, siempre ha sido una alta prioridad teniendo en cuenta el entorno de seguridad en el que se han utilizado los productos de Cathexis.

En los últimos tiempos, el término "ciberseguridad" se ha convertido en un tema candente en el espacio de los sistemas de seguridad física y es algo que Cathexis se toma muy en serio.

Este documento describe las medidas empleadas para reducir la posibilidad de riesgo de acceso a la información y manipulación de datos, y ofrece algunas sugerencias para aumentar la seguridad en áreas de los sistemas que Cathexis no puede controlar, como los equipos periféricos y de terceros.

[1] Aunque Cathexis ha hecho todo lo posible para asegurar la exactitud de este documento, no hay garantía de su exactitud, ni explícita, ni implícita. Las especificaciones están sujetas a cambios sin previo aviso.

2 Seguridad de Cathexis

Este capítulo describe las diversas medidas de seguridad adoptadas por Cathexis.

2.1 Comunicación entre los componentes de CathexisVision

CathexisVision garantizará la seguridad de las comunicaciones entre sus componentes, incluyendo:

i. Servidores de grabación a clientes,
ii. Servidores de grabación a otros servidores de grabación,
iii. Servidores de grabación a Video Walls,
iv. Servidores de grabación a portales de gestión de alarmas.

La comunicación segura entre los componentes anteriores se garantizará mediante:

i. Todas las conexiones externas del sitio soportan encriptación de varios niveles:
    a. Desactivado,
    b. Mínimo (sólo se encriptan las conexiones críticas),
    c. Segura (la opción por defecto que encripta todas las conexiones excepto las de alto volumen de vídeo),
    d. Todas (todas las conexiones encriptadas, incluidas las de alto volumen de vídeo).
ii. Las contraseñas nunca se almacenan como texto sin formato y, en su lugar, se hace un hash con SHA512 (de CathexisVision 2017).
iii. Las credenciales de inicio de sesión se negocian mediante el intercambio de claves Diffie-Hellmann y se firman con una clave privada RSA (admite claves RSA de 1024 y 2048).
iv. El cifrado en los canales de red se realiza mediante AES128/GCM con claves de cifrado únicas negociadas por conexión.
v. Se utiliza HMAC para la verificación de la integridad.
vi. La infraestructura de clave pública (PKI) es gestionada internamente por Cathexis para mayor seguridad.

2.2 Archivo de datos

i. La integridad de los vídeos se asegura utilizando claves dobles RSA1024 (para la firma),
ii. El cifrado opcional se realiza mediante un cifrado de bloques AES128 con un IV aleatorio por bloque y una frase de paso generada por el usuario.
iii. El vídeo puede llevar una marca de agua para indicar la fuente de la información (es decir, la información del usuario).
iv. Las secuencias de vídeo y los metadatos sólo pueden reproducirse a través de un reproductor de vídeo propio de Cathexis Archive.
v. El vídeo exportado/archivado puede estar restringido a una reproducción controlada por contraseña.

2.3 Protección de la información personal (POPI por sus siglas en inglés)

Para ayudar a garantizar que las secuencias de vídeo no sean de dominio público, hemos añadido la posibilidad de:

i. Archivar vídeos que sólo pueden ser reproducidos bajo control de contraseña.
ii. Superponer una marca de agua en el vídeo para mostrar la fuente de la información (por ejemplo, información del usuario).

3 Equipos periféricos

La variedad de productos y protocolos a los que se conecta CathexisVision determina la seguridad de los equipos periféricos (por ejemplo, las cámaras IP). Por esta razón, Cathexis está trabajando con socios tecnológicos y otros actores de la industria para aumentar la seguridad de esta interfaz.
En general, la conexión con cámaras IP incluye lo siguiente:

3.1 Configuración de la cámara

i. HTTP: protocolo de hipertexto,
ii. Ssl/tls encriptado,
iii. Soportado por CURL (biblioteca de transferencia de URL del lado del cliente).

3.2 Control de la cámara

i. RTSP - protocolo de transmisión en tiempo real.
ii. Control de la conexión de la cámara encriptada por HTTPS (cuando el fabricante lo admita).

3.3 Transmisión de vídeo

i. RTP - Protocolo de transporte en tiempo real.
ii. Transmisión de vídeo encriptado (si el fabricante lo admite).

4 Consideraciones informáticas.

Esta sección cubre las consideraciones de seguridad en torno al sistema informático más allá del control de Cathexis.

4.1 Acceso a la red

El primer paso en cualquier sistema es asegurar que el acceso a la red esté debidamente controlado. Existen varias técnicas para ello que están bien documentadas y que deberían ser conocidas y adoptadas por cualquier empresa de redes competente. Entre ellas se encuentran:

i. Los Firewalls (cortafuegos),
ii. Conmutadores de red inteligentes,
iii. Redes gestionadas,
iv. Controlar el acceso "físico" a la red.

4.2 Bloqueo del sistema operativo

Para atacar el software, el acceso debe realizarse a través del sistema operativo del sistema en el que se ejecuta el software. Por lo tanto, es importante asegurarse de que el sistema operativo esté "bloqueado" para evitar el acceso no autorizado. Esto se puede hacer de varias maneras, tal y como indicamos a continuación:

i. Impidiendo la apertura de puertos no autorizados que permitan el uso de elementos como ftp, telnet, correo electrónico. Si hay que comunicarse por estos medios, hay que asegurarse de que se utilizan protocolos de seguridad como SSH/SFTP,
ii. Desactivando el acceso "root" al sistema operativo,
iii. Garantizando niveles de contraseña fuertes,
iv. Añadiendo un software antivirus y antimalware, que se actualice continuamente,
v. Restringiendo el acceso a Internet.

5 Conclusión

Para más información, consulte el sitio web de CathexisVision (www.cathexisvideo.com) o póngase en contacto con support@cat.co.za.