



Descripción general de la seguridad cibernética de CathexisVision 2019

Contenidos

1	Introducción	2
2	Seguridad de Cathexis	3
2.1	Comunicación entre los componentes de CathexisVision.....	3
2.2	Archivo de datos	3
2.3	Protección de Información Personal (POPI)	3
3	Equipos periféricos.....	4
3.1	Configuración de la cámara	4
3.2	Control de la cámara	4
3.3	Transmisión de vídeo.....	4
4	I.T. Consideraciones	5
4.1	Acceso a la red.....	5
4.2	Bloqueo del sistema operativo.....	5
5	Conclusiones.....	6

1 Introducción

Cathexis lleva más de 20 años desarrollando y suministrando soluciones de gestión de vídeo al mercado global. La seguridad que implica tanto el acceso a los datos como la integridad de los mismos siempre ha sido una alta prioridad teniendo en cuenta el entorno seguro 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 la medida empleada 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

2 Seguridad de Cathexis

En este capítulo se describen las diferentes 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 Gateways de Gestión de Alarmas.

Se garantizará una comunicación segura entre los componentes anteriores mediante:

- i. Todas las conexiones de sitios externos soportan encriptación de diferentes niveles:
 - a. Discapacitado,
 - b. Mínimo (sólo conexiones críticas cifradas),
 - c. Seguro (la opción predeterminada que encripta todas las conexiones excepto las de vídeo de alto volumen),
 - d. Todas (todas las conexiones cifradas, incluidos los enlaces de vídeo de alto volumen).
- ii. Las contraseñas nunca se almacenan como texto plano y en su lugar se envían en hash utilizando SHA512 (de CathexisVision 2017).
- iii. Las credenciales de inicio de sesión se negocian utilizando RSA1024,
- iv. Los canales de comunicación sensibles se cifran mediante AES128/CBC,
- v. HMAC se utiliza para la verificación de la integridad.
- vi. La Infraestructura de Clave Pública (PKI) es administrada internamente por Cathexis para mayor seguridad.

2.2 Archivo de datos

- i. La integridad de los vídeos está asegurada mediante llaves duales RSA1024 (para firmar),
- ii. El cifrado opcional se realiza mediante el cifrado de bloques AES128 con una IV aleatoria por bloque y una frase de paso generada por el usuario.
- iii. El vídeo puede ser marcado para indicar la fuente de la información (es decir, la información del usuario).
- iv. El material de vídeo y los metadatos sólo pueden reproducirse a través de un reproductor de vídeo Cathexis Archive propietario.
- v. El vídeo exportado/archivado puede estar restringido a la reproducción controlada por contraseña.

2.3 Protección de Información Personal (POPI)

Con el fin de ayudar a garantizar que las imágenes de vídeo no lleguen al dominio público, hemos añadido la capacidad de:

- i. Archivar vídeo que sólo puede reproducirse bajo control de contraseña.
- ii. Superponer una filigrana en el vídeo para representar la fuente de la información (por ejemplo, información del usuario).

3 Equipos periféricos

La variedad de productos y protocolos a los que CathexisVision se conecta determina la seguridad de los equipos periféricos (por ejemplo, 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 encriptados,
- iii. Soportado por CURL (biblioteca de transferencia de URL del lado del cliente).

3.2 Control de la cámara

- i. RTSP - protocolo de streaming en tiempo real.
- ii. Control de conexión de cámara encriptada HTTPS (donde sea compatible con el fabricante).

3.3 Transmisión de vídeo

- i. RTP - Protocolo de transporte en tiempo real.
- ii. Transmisión de vídeo encriptada (si es compatible con el fabricante).

4 I.T. Consideraciones

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

4.1 Acceso a la red

El primer paso en cualquier sistema es garantizar que el acceso a la red se controle adecuadamente. Hay varias técnicas para esto que están bien documentadas y que deberían ser conocidas y adoptadas por cualquier empresa de redes competente. Estos incluyen:

- i. Firewall,
- ii. Conmutadores de red inteligentes,
- iii. Redes Gestionadas,
- iv. Controla del acceso "físico" a la red.

4.2 Bloqueo del sistema operativo

Para atacar el software, el acceso debe obtenerse 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, incluyendo:

- i. Impidiendo la apertura de puertos no autorizados permitiendo el uso de elementos como ftp, telnet, correo electrónico. Si es necesario que se produzca alguna comunicación a través de estos medios, hay que asegurarse de que se utilizan protocolos de seguridad como SSH/SFTP,
- ii. Desactivando el acceso "root" al sistema operativo,
- iii. Asegurando de niveles de contraseña seguros,
- iv. Añadiendo software antivirus y anti-malware, que se actualiza continuamente,
- v. Acceso restringido a Internet.

5 Conclusiones

Para más información consulte la página web de CathexisVision (www.cathexisvideo.com) o contacte con support@cathexisvideo.com