AXIS Camera Station 5

Guía de seguridad del sistema

AXIS Camera Station 5

Introducción

Introducción

Una función única e infalible que podría hacer que cualquier sistema de seguridad y cualquier sitio fueran 100% ciberseguros. Por muy atractivas que suenen esas palabras, no existe tal característica - ni es probable que exista pronto. En su lugar, hay que examinar el riesgo que plantean las amenazas y vulnerabilidades propias de su organización y, cuando el riesgo se considere inaceptable, implantar controles para mitigarlo. Unas políticas y procedimientos bien definidos garantizan una comunicación y aplicación coherentes de esos controles en toda la organización y constituyen la base de un programa de ciberseguridad maduro.

Un enfoque recomendado es trabajar de acuerdo con marcos estandarizados de gestión de riesgos de seguridad informática como ISO 27001, NIST CSF u otros. Aunque esta tarea puede resultar desalentadora para las organizaciones más pequeñas, definir un conjunto básico de políticas de seguridad de la información y procesos de apoyo es mucho mejor que no tener nada en absoluto. Si su organización se está iniciando en el camino hacia la madurez cibernética y dispone de recursos limitados, le recomendamos investigar el *Centro para la Seguridad en Internet (CIS) Controles críticos de seguridad Versión 8*. El CIS proporciona una lista de 18 actividades de control de la seguridad organizadas en tres grupos de aplicación para ayudar a las organizaciones a desarrollar y madurar su programa de ciberseguridad.

Las brechas de seguridad se producen en muchas organizaciones porque la empresa no ha establecido políticas, reglas y procedimientos claros que rijan el uso y los derechos de acceso de sus propios empleados.© ¿Su organización trabaja con políticas y procesos para las operaciones de gestión de vídeo? Si no es así, es el momento de empezar a definirlas.

Propósito

En este documento se describen varias políticas y procedimientos de ciberseguridad útiles para la implementación y el mantenimiento seguros de los sistemas de AXIS Camera Station 5. Aunque no se asigna directamente a un marco de ciberseguridad, nos basamos principalmente en cis security controls v8 con un enfoque particular en las siguientes actividades de control:

- *Control 1: Inventario y control de activos empresariales*
- *Control 2: Inventario y control de activos de software*
- *Control 3: Protección de datos*
- *Control 4: Configuración segura de activos y software empresariales*
- *Control 5: Administración de cuentas*
- *Control 6: Gestión del control de acceso*
- *Control 7: Gestión continua de vulnerabilidades*
- *Control 10: Defensas de malware*

Nuestras recomendaciones se centran en ayudar a instaladores, integradores y usuarios finales a mitigar los riesgos comunes al implementar y gestionar los sistemas de AXIS Camera Station 5 .

Requisitos previos

Se asume que las recomendaciones y procedimientos definidos y descritos en la *Guía de seguridad del sistema operativo AXIS* se comprenderán y seguirán. Además, este documento hace referencia a varias funciones de usuario comunes que interactúen con un sistema de vídeo. Asigne estas funciones de usuario para que coincidan con sus propias clasificaciones de usuario y función. Un usuario individual puede tener varias funciones, dependiendo de la organización.

Roles definidos:

- **Instalador del sistema**: Instala, instala, repara, actualiza y degrada sistemas
- **Administrador de red**: Mantiene la infraestructura de red, la conectividad de los nodos finales, los servidores y recursos de red, así como la protección de la red

Introducción

- **Administrador del sistema de vídeo**: Define y gestiona el sistema de vídeo para proteger su uso, rendimiento y privilegios de usuario
- **Mantenedor de sistemas de vídeo**: Supervisa, ajusta y soluciona problemas de componentes para garantizar el rendimiento del sistema en nombre del administrador del sistema de vídeo
- **Usuarios**: Personas que utilizan el cliente de AXIS Camera Station 5 para acceder al vídeo en directo y grabado y suelen ser responsables de la protección física de una organización.

Políticas de seguridad del sistema

Seguridad física

Política de protección física

Servidores, dispositivos, equipos de red y cables son objetos físicos que pueden interferir, eliminarse o obtener información. El host en el que se ejecuta el software de servidor AXIS Camera Station 5 y equipos de red importantes (enrutadores, conmutadores, etc.) debe ubicarse en un entorno con acceso restringido tanto física como lógicamente. Las cámaras y otros dispositivos conectados deben montarse en lugares de difícil acceso y cuentan con modelos o carcasas a prueba de agonía. Debe prestarse atención a la protección de los cables en paredes o conductos, ya que estos aumentan el riesgo de manipulación y desatención.

Políticas y procedimientos recomendados
Defina una unidad individual o de empresa responsable de auditar visualmente la protección física de los servidores VMS, el hardware de red, los dispositivos conectados y el cableado a intervalos definidos. Es fundamental mantener un inventario preciso de todos los servidores y dispositivos, incluida su ubicación.

Software de gestión

Política de software de aplicaciones de terceros

Como AXIS Camera Station 5 se instala en un entorno de Windows estándar, puede ser tentador utilizar ese entorno para aplicaciones de software no relacionadas con la gestión de vídeo. La instalación de otras aplicaciones de otros proveedores abre la posibilidad de introducir en el entorno productos de "megá", lo que podría provocar un tiempo de inactividad del sistema o una puerta trasera para que un atacante entre en la red de la organización.

Políticas y procedimientos recomendados
No ejecute nada que no sea el software del servidor de AXIS Camera Station 5 e integraciones de terceros de confianza en el hardware host. Si el hardware físico debe utilizarse para otros fines, se recomienda utilizar varias instancias de servidores virtuales y ejecutar el software del servidor de AXIS Camera Station 5 en una máquina virtual y el software de terceros no relacionado con VMS en otra máquina virtual. Encontrará información sobre la ejecución de AXIS Camera Station 5 en un entorno virtual *aquí*.

Se recomienda implementar software antivirus en todos los servidores y ordenadores que se conecten al servidor de AXIS Camera Station 5. Si se implementan dispositivos móviles, esto incluye asegurarse de que los dispositivos tienen instalados los últimos sistemas operativos y correcciones (aunque no directamente antivirus). Cuando realice el barrido de virus, no escanee los directorios y subdirectorios que contienen bases de datos de grabación. El barrido de virus en estos directorios puede afectar al rendimiento del sistema.

Administración de cuentas

Política general de cuentas

En ocasiones, se conceden derechos de nivel de administrador a los usuarios normales por su comodidad. En muchas organizaciones, no es el responsable de revisar los privilegios de la cuenta y supervisar el acceso de los empleados a los sistemas.

Políticas y procedimientos recomendados
Recomendamos que las organizaciones sigan el principio de mínimo privilegio al definir cuentas del sistema. Esto significa que los privilegios de acceso del usuario se limitan únicamente a los recursos que necesita para realizar sus tareas de trabajo específicas. También es aconsejable auditar periódicamente los privilegios de cuenta de los usuarios del sistema para protegerse de "privilegios".

AXIS Camera Station 5 política de cuentas de administrador

Un error común al implementar AXIS Camera Station 5 en un entorno windows es que se define una sola cuenta de administrador para el host de Windows. Con el tiempo, la contraseña puede compartirse dentro de la organización con el riesgo de que personas no autorizadas obtengan privilegios de administrador del entorno Windows. Esto puede resultar fácilmente en numerosas aplicaciones de usuario no deseadas o en la instalación de Euros en ese servidor.

Políticas y procedimientos recomendados
La máquina Windows que aloja el servidor de AXIS Camera Station 5 debe tener al menos una cuenta privilegiada de administrador y otra de usuario. Ninguna de estas cuentas debe ser la misma que la cuenta de administrador predeterminada para Windows. La cuenta de administrador predeterminada debe desactivarse después de crear las cuentas de usuario y de administrador. Tras la implantación, la contraseña de la cuenta de administrador solo debe ser conocida y utilizada por **administrador(es) de red**. La cuenta privilegiada del usuario debe ser utilizada por el **administrador del sistema de vídeo** si/cuando necesiten iniciar sesión en el servidor de AXIS Camera Station 5. Debe tenerse en cuenta que, incluso si las dos funciones anteriores son desempeñadas por la misma persona, se recomienda tener cuentas separadas de administrador de red y de administrador del sistema de vídeo a efectos de auditoría.© Para dar soporte a otros roles definidos anteriormente, deben crearse más cuentas de usuario sin privilegios para cada **usuario** individual que se conectará al sistema.

Si el host que ejecuta AXIS Camera Station 5 se sitúa en un entorno de dominio de Active Directory de Windows, se pueden crear cuentas de administrador y de usuario en el contexto del dominio o se puede utilizar la cuenta de dominio existente de un empleado para autenticarse en el host de AXIS Camera Station 5. Esto puede simplificar la gestión de cuentas, ya que no es necesario crear ni mantener cuentas adicionales. Esto también abre la posibilidad de utilizar la gestión de directivas de grupo para imponer la complejidad de las contraseñas, la implantación de certificados y otras funciones de seguridad disponibles en los entornos de dominio.

AXIS Camera Station 5 política de cuenta de usuario

Las cuentas de usuario se asignan a funciones específicas en AXIS Camera Station 5, que, a su vez, determina los derechos específicos que cada usuario tiene en el sistema, como a qué vistas y vídeos tiene privilegio de acceder. Si varias personas comparten una sola cuenta de usuario, existe un mayor riesgo de que una contraseña se comparta con otras personas de la organización. Compartir cuentas también permitirá realizar una auditoría de quién ha accedido a qué cámara/vídeo en ese momento prácticamente imposible.

Políticas y procedimientos recomendados

Si es posible, utilice Microsoft Active Directory para facilitar la gestión de usuarios y grupos. También se recomienda comprobar que se han definido los grupos de seguridad relevantes para todos los roles de usuario antes de configurar el sistema.

Active Directory también proporcionará:

- Una política de contraseñas que requiere que los usuarios cambien su contraseña con regularidad
- Protección contra fuerza bruta, para que la cuenta de Windows AD se bloquee tras varios intentos fallidos de autenticación, de acuerdo con la política de contraseñas de la organización.
- Permisos basados en roles, para que los controles de acceso puedan aplicarse en todo el dominio

Si hay que utilizar cuentas locales de Windows, se recomienda crear una cuenta única para cada usuario del sistema y darles acceso sólo a las entidades del sistema necesarias para llevar a cabo sus responsabilidades. Utilizar grupos para los usuarios puede ayudar a simplificar la asignación de permisos si hay varios usuarios con permisos idénticos.

Política de cuenta del dispositivo

Las cuentas de los dispositivos Axis son principalmente cuentas de ordenador/cliente. **Los usuarios** nunca debe permitirse el acceso directo al dispositivo. El único cliente que debería acceder a los dispositivos durante el funcionamiento normal es el servidor de AXIS Camera Station 5. Una estrategia habitual es que todos los dispositivos tengan la misma contraseña. Esto introduce riesgos adicionales, pero también puede simplificar la gestión de contraseñas, por lo que hay que evaluar su propia tolerancia a riesgos. AXIS Camera Station 5 permite asignar contraseñas únicas a cada dispositivo a través de su interfaz de gestión.

Un error común es que los dispositivos se agregan a AXIS Camera Station 5 con una sola cuenta compartida por varias funciones. En algún momento, cuando un **Mantenedor de sistemas de vídeo** necesita utilizar un navegador para ajustar algo, se utiliza la contraseña de la cuenta maestra (root) del dispositivo. En cuestión de meses, la mayoría de las personas de la organización conocerán la contraseña para todos los dispositivos y tendrán privilegios de administrador para el sistema.

Políticas y procedimientos recomendados
El dispositivo debe tener al menos dos cuentas de administrador: Una única creada para los administradores de dispositivos y la cuenta de root predeterminada para agregar dispositivos al servidor de AXIS Camera Station 5. El acceso temporal, por ejemplo, cuando **mantenedor de sistemas de vídeo** accede a un dispositivo mediante un navegador web, debe gestionarse mediante el uso de cuentas temporales.

AXIS Device Manager debe utilizarse como la herramienta principal para gestionar cuentas y contraseñas de dispositivos. Una versión de AXIS Device Manager se ha integrado directamente en AXIS Camera Station 5 y está disponible en la pestaña Gestión. La

contraseña raíz del dispositivo solo debe ser utilizada por AXIS Device Manager y AXIS Camera Station 5 y solo debe ser conocido por aquellos que utilicen AXIS Device Manager o AXIS Camera Station 5 como herramienta de gestión de dispositivos.

Utilice AXIS Camera Station 5 para proporcionar una cuenta temporal cuando alguien en una función de manutención tiene que utilizar un navegador web para acceder a dispositivos para solucionar problemas o realizar tareas de mantenimiento. Seleccione los dispositivos y cree una cuenta nueva, preferiblemente con privilegios de operador, que el mantenedor puede utilizar. Una vez que haya completado la tarea, elimine la cuenta temporal.

Mantenimiento del sistema

AXIS Camera Station 5 Política de parches de host de Windows

AXIS Camera Station 5 servidor y clientes que se ejecutan en la parte superior de un entorno de Windows. Es importante que estos sistemas estén actualizados para garantizar que los sistemas de alojamiento de software de AXIS Camera Station 5 no tienen vulnerabilidades abiertas que puedan aprovecharse para acceder sin autorización al sistema de gestión de vídeo.

Políticas y procedimientos recomendados
Para todos los sistemas de AXIS Camera Station 5 ya sea que se ejecuten en NVR de Axis o en hardware personalizado, se recomienda desactivar la actualización automática. En el pasado, las actualizaciones de Windows no se han integrado en el sos windows existente, por lo que se recomienda probar las actualizaciones disponibles en algunos equipos para garantizar la estabilidad del sistema antes de enviarse a todos los sistemas de alojamiento que ejecutan AXIS Camera Station 5. Sin embargo, es necesario lograr un equilibrio entre seguridad y estabilidad, ya que dejar el sistema de Windows sin parches durante demasiado tiempo puede introducir riesgo en el entorno global. En función del nivel de exposición del sistema del cliente a amenazas externas, en la política de correcciones se describen los plazos para garantizar que los sistemas reciban las actualizaciones más recientes.

AXIS Camera Station 5 política de actualización de software

En la mayoría de los casos, utilizar la última versión de software para AXIS Camera Station 5 se asegurará de que utiliza los parches de seguridad para todas las vulnerabilidades recién descubiertas. Dejar el sistema sin parches durante un periodo más largo aumentará el riesgo de que un adversario explote las vulnerabilidades y pueda comprometer el sistema.

Políticas y procedimientos recomendados
Es importante definir una política de parches con evaluaciones periódicas de las versiones de software para asegurarnos de que AXIS Camera Station 5 esté actualizada. La política de parches también debe identificar quién es el responsable de gestionar el trabajo asociado a la actualización tanto del software del servidor como del cliente. Para AXIS Camera Station 5, la versión más reciente se puede encontrar en *www.axis.com*. AXIS Camera Station 5 requiere las bibliotecas .NET más recientes, por lo que se debe tener cuidado de alinear la política de parches de Windows con la política de AXIS Camera Station 5.

Política de actualización del firmware del dispositivo

Utilizar dispositivos con versiones de firmware actualizadas mitiga la mayoría de los riesgos comunes, ya que las últimas versiones de firmware incluirán parches para vulnerabilidades conocidas que los atacantes podrían intentar explotar. Axis ofrece una versión a largo plazo del firmware del dispositivo (LTS) que incluye correcciones de errores y correcciones de errores de seguridad, pero las características adicionales se limitan a garantizar la estabilidad a largo plazo de la plataforma. Para obtener más información sobre la estrategia de Axis en cuanto al desarrollo del firmware, consulte el documento técnico *sobre gestión de firmware* de Axis.

Políticas y procedimientos recomendados
Para dispositivos de hardware, la política debe estado que todo el firmware esté actualizado. Los procesos pueden aprovechar la función de actualización de firmware en AXIS Camera Station 5 o AXIS Device Manager Extend, para identificar si hay nuevas versiones de firmware disponibles para los dispositivos Axis. Debe definirse una hora programada,normalmente fuera del horario laboral, para implementar todas las actualizaciones de firmware para todas las cámaras. AXIS Camera Station 5 / AXIS Device Manager Extend también puede verificar si se aceptaron las actualizaciones de firmware. Si el sistema tiene integraciones específicas que podrían verse afectadas por la actualización, considere la posibilidad de estandarizar en un seguimiento del firmware LTS.

Seguridad de red

Política de acceso remoto

Los dispositivos y servicios expuestos a Internet aumentan el riesgo de que los adversarios externos resalten o aprovechen las vulnerabilidades conocidas. Las cámaras expuestas a Internet, por ejemplo en organizaciones pequeñas que necesitan acceso remoto a vídeo, se convierten en fáciles víctima si se utilizan contraseñas débiles o se descubre una nueva vulnerabilidad crítica. El acceso remoto al entorno de Windows debe controlarse o evitarse estrictamente, si es posible. Aunque el entorno de Windows puede tener conectividad a Internet como una cuestión de comodidad para actualizar sistemas, el uso de servicios de escritorio remoto como Windows Remote Desktop, TeamDesk y AnyDesk introducen rutas para acceder al sistema si no se gestiona correctamente.

Políticas y procedimientos recomendados
Nunca exponga la dirección IP/puerto de una cámara de modo que sea accesible directamente desde Internet. Si es necesario acceder a vídeo remoto, utilice Axis Secure Remote Access. AXIS Camera Station 5 utiliza un servidor de acceso remoto basado en la nube para facilitar el acceso remoto al sistema a través del clientes de AXIS Camera Station 5 o la aplicación móvil AXIS Camera Station. Además de ser responsable de la gestión de conexiones para usuarios remotos y móviles, el servidor de acceso remoto juega un papel importante a la hora de proteger la integridad cuando lo utilizan los usuarios remotos. Para obtener más información sobre Axis Secure Remote Access, consulte *esta información*. Axis suministra aplicaciones móviles de marca oficial para Android y Apple iOS. La aplicación móvil AXIS Camera Station solo debe descargarse de fuentes oficiales, Google Play Store y Apple App Store respectivamente.

En lo que respecta al acceso de escritorio remoto al entorno de Windows, no se recomienda proporcionar este tipo de acceso a un sistema que ejecuta AXIS Camera Station 5. No obstante, si es necesario, debe adoptarse la máxima cuidado para garantizar que la aplicación de escritorio remoto que elija es segura y que solo se proporciona acceso a las personas que lo requieren. Se recomienda la implementación de capas de controles adicionales, como la autenticación multifactor (KERBEROS). Se recomienda realizar un registro y una auditoría posterior de los intentos de conexión remota para realizar un seguimiento de quién y en qué momento se está accediendo de forma remota al entorno Windows.

Política de exposición a la red local

La reducción de la exposición en red local puede ayudar a mitigar muchas amenazas comunes mediante la reducción de la superficie de ataque. Existen muchas maneras de reducir la exposición a la red, como la segmentación física de la red (hardware y cables de red independientes), la segmentación de la red lógica mediante LAN virtuales (VLAN) y el filtro IP. Las cámaras Axis admiten un filtro IP (tablas IP) de manera que el dispositivo solo responde a solicitudes de conexión realizadas desde direcciones IP permitidas explícitamente.

Políticas y procedimientos recomendados
AXIS Camera Station S22 NVR son servidores de hardware con puertos de red duales. Uno de los puertos crea una red segmentada para las cámaras y el otro se conecta a la red principal (dominio) para servir a los clientes de vídeo. El servidor actúa como puente y cortafuegos de la red de cámaras, evitando que los clientes accedan directamente a las cámaras. De esta forma, se reduce el riesgo de amenazas de los adversarios en la red principal.

Si el servidor de AXIS Camera Station 5 y las cámaras están todos ubicados en la red principal, se recomienda configurar el filtro IP de la cámara, lo que limita el acceso a solo los servidores que alojan AXIS Camera Station 5, AXIS Device Manager y clientes de mantenimiento adicionales.

Política de cifrado de red

El tráfico de red transferido a través de redes inseguras debe cifrarse siempre. Internet está clasificado como una red insegura. Una red local también puede clasificarse como insegura y, por lo tanto, el tráfico de red también debe cifrarse. La política que se aplicará al tráfico de vídeo en la red depende de la clasificación del vídeo y del riesgo de que los adversarios tengan acceso a la red al sistema de vídeo. Se recomienda suponer que la red ya se ha visto comprometida. Normalmente, las organizaciones de mayor tamaño tendrán una política que defina cómo se clasifica la red.

Políticas y procedimientos recomendados

El tráfico entre el cliente de vídeo y el servidor de AXIS Camera Station 5 debe utilizar encriptación. El tráfico entre el servidor de AXIS Camera Station 5 y las cámaras debe cifrarse en función de la infraestructura. Las cámaras Axis incluyen un certificado con firma propia y HTTPS activado de forma predeterminada. Si existe riesgo de suplantación de red, como cuando un ordenador malintencionado intenta hacerse pasar por una cámara, debe utilizarse una infraestructura de clave privada (PKI) con certificados firmados por una CA. AXIS Camera Station 5 dispone de una autoridad de certificación (CA) local integrada que puede gestionar de forma rentable la firma y distribución de certificados de servidor para los dispositivos Axis.

Versiones de TLS

Recomendamos desactivar las versiones 1.1 y 1.0 de TLS. El instalador de AXIS Camera Station ofrece asistencia durante la instalación o actualización.

Codificadores HTTPS

AXIS Camera Station 5 admite y utiliza conjuntos de cifrado TLS para cifrar las conexiones HTTPS de forma segura. El conjunto de cifrado específico depende del cliente que se conecte a AXIS Camera Station 5 o el servicio contactado, y AXIS Camera Station 5 lo negocia según el protocolo TLS. Recomendamos configurar Windows para que no utilice los conjuntos de cifrado TLS 1.2 enumerados *en RFC 7540*. La posibilidad de desactivar un conjunto de cifrado depende de los dispositivos y cámaras utilizados junto con AXIS Camera Station 5. Si un dispositivo o cámara requiere un conjunto de cifrado específico, puede que no sea posible desactivar el conjunto de cifrado débil.

Gestión de datos

Clasificación en vídeo

El vídeo en directo y grabado debe clasificarse. El vídeo puede clasificarse como público, privado, restringido o cualquier otra clase definida por políticas de publicidad. En muchos casos, el vídeo está regulada por la ley y la normativa regional, así como por políticas internas de IT, por lo que es responsabilidad del propietario del sistema ser consciente de las leyes y normativas aplicables a sus datos de vídeo.

Políticas y procedimientos recomendados
Clasifique el vídeo en directo, el vídeo grabado y el audio de acuerdo con las políticas de clasificación de datos de la organización. Configure los privilegios de acceso del usuario y la protección del sistema según la sensibilidad de los datos de vídeo y audio. Si no es necesario, el audio puede desactivarse en un nivel de dispositivo.

Controles de seguridad adicionales

En función del nivel de madurez y de la tolerancia a riesgos de su organización, hay varios controles de seguridad adicionales de CIS Controls v8 que recomendamos implementar para ayudar a reducir los riesgos de ciberseguridad en las operaciones diarias.

Controles CIS adicionales:

Control 8: Gestión de registros de auditoría
Recopile, alerte, revise y conserve los registros de auditoría de los eventos que podrían ayudar a detectar, comprender o recuperarse de un ataque.

Control 14: Implemente un programa de concienciación y formación en materia de seguridad
Comprenda las habilidades y los comportamientos de los miembros de su plantilla. Forme al personal sobre cómo identificar distintas formas de ataques.

Control 17: Respuesta y gestión de incidentes
Utilice planes escritos de respuesta a incidentes con fases claramente definidas de gestión/manejo de incidentes y roles del personal, así como la forma de informar de un incidente de seguridad a las autoridades pertinentes y a terceros.

Guía de seguridad del sistema
AXIS Camera Station 5

Ver. M3.2
Fecha: 2024
N.º de pieza T10179095