CIBERSEGURIDAD

Gestión del ciclo de vida de los dispositivos

Los riesgos vinculados a la ciberseguridad están presentes en todos los pasos del ciclo de vida de un dispositivo de red, desde la producción hasta la desinstalación. Si no se tienen en cuenta, el resultado pueden ser alteraciones en las actividades y problemas con la confidencialidad, la integridad y la disponibilidad de los datos. Por tanto, es fundamental que todos los actores implicados, desde proveedores hasta clientes finales, asuman su responsabilidad en la gestión de los riesgos.

En este sentido, las consideraciones relativas al ciclo de vida de seguridad de los dispositivos son importantes en el terreno de las compras. Un fabricante debe aplicar medidas para reducir los riesgos de ciberseguridad antes de que el producto llegue al cliente, mientras el producto está en servicio y cuando se desinstala.

Las siguientes páginas presentan las tecnologías, las herramientas y consejos, así como los modelos y procesos aplicados por Axis para mitigar los riesgos en el ciclo de vida de un dispositivo Axis.

Modelo de seguridad: Axis Edge Vault, AXIS OS, Axis Security Development Model


PRODUCCIÓN


DISTRIBUCIÓN


IMPLEMENTACIÓN


EN SERVICIO


DESINSTALACIÓN

Modelo de seguridad: hardware, software y planteamiento

Protección de la integridad del producto y reducción del riesgo de vulnerabilidades desde el primer minuto

Plataforma de ciberseguridad Axis Edge Vault
Esta plataforma de hardware integra prestaciones que protegen la identidad y la integridad del dispositivo frente a accesos no autorizados, para que pueda iniciar el dispositivo de forma segura, integrarlo y mantener protegidos los datos confidenciales, como las claves.

Sistema operativo AXIS OS
AXIS OS es el motor de numerosos dispositivos Axis. Actualizado con las últimas recomendaciones del sector en materia de gestión de vulnerabilidades, AXIS OS es una plataforma ideal para introducir de forma rápida y práctica funciones y parches de seguridad de software en un gran número de productos.

Modelo de desarrollo de la seguridad de Axis (ASDM)
Es la metodología aplicada por Axis para reducir el riesgo de lanzar al mercado productos con vulnerabilidades de software. El modelo ASDM garantiza que se tiene en cuenta la seguridad en el desarrollo del software y utiliza, entre otros recursos, evaluaciones de riesgos, modelado de amenazas, análisis de código, pruebas de penetración, programas de recompensas por errores y análisis y gestión de vulnerabilidades.

Transparencia
Este aspecto es clave en Axis para generar confianza. Axis es una autoridad numeradora de vulnerabilidades y exposiciones comunes (CVE). Por este motivo, publicamos las vulnerabilidades y avisamos a los implicados para que los clientes puedan adoptar las medidas adecuadas. También publicamos una lista de materiales de software (SBOM) para AXIS OS.

PRODUCCIÓN Y DISTRIBUCIÓN

Reducción de la presencia de componentes de riesgo

- **Cadena de suministro:** los componentes esenciales se compran directamente a proveedores estratégicos. Axis trabaja en estrecha colaboración con sus socios de fabricación. Los procesos de producción se controlan y los datos se comparten con Axis de forma permanente, lo que permite un análisis en tiempo real y garantiza una gran transparencia.
- **Axis Edge Vault:** instalado en los dispositivos Axis en la fase de producción, Axis Edge Vault incluye las siguientes prestaciones:
  - **Almacén de claves seguro,** con módulos de computación criptográficos (como elementos seguros, módulo de plataforma segura, entorno de ejecución de confianza, etc.) para proteger las claves almacenadas contra manipulaciones.
  - **Firmware firmado,** que garantiza que el AXIS OS instalado es realmente de Axis. Además, también garantiza que cualquier nuevo firmware que tenga que descargarse e instalarse en el dispositivo esté también firmado por Axis.
  - **Arranque seguro,** una tecnología que permite al dispositivo comprobar que el firmware tenga una firma de Axis. Si el firmware no tiene autorización o se ha modificado, se cancela el proceso de arranque y el dispositivo deja de funcionar. La combinación del firmware firmado, el arranque seguro y la configuración predeterminada de fábrica del dispositivo ofrece una gran protección contra modificaciones maliciosas durante el envío de un dispositivo.
  - **ID de dispositivo Axis,** un certificado específico de cada dispositivo con sus correspondientes claves, que demuestran la autenticidad de un dispositivo Axis. Basado en la norma IEEE 802.1AR, el ID de dispositivo Axis permite la identificación de un dispositivo y su incorporación segura a una red.
  - Un **sistema de archivos cifrado**, que impide la extracción o la manipulación de configuraciones específicas de clientes o información almacenada en el sistema de archivos mientras el dispositivo no se utiliza, por ejemplo durante su transporte de un integrador de sistemas al cliente final.

IMPLEMENTACIÓN

Control del riesgo de incorporar a la red productos en riesgo o sin suficiente protección, que puedan abrir la puerta a accesos no autorizados, la extracción de datos confidenciales o la transferencia de datos modificados entre terminales de red

- **Configuración predeterminada de fábrica:** aplicación de una configuración predeterminada de fábrica al dispositivo antes de configurarlo. De este modo se garantiza que el dispositivo no incluye software o configuraciones no deseados, ya que el único software en su interior será AXIS OS, con sus ajustes predeterminados.
- **Consulta del firmware más reciente para el dispositivo:** si ya ha pasado un tiempo entre la producción y la instalación, merece la pena consultar el sitio web de Axis para ver si hay firmware nuevo, que puede incluir correcciones de errores para un dispositivo en concreto.
- **ID de dispositivo Axis:** para garantizar que en la red solo se instalan dispositivos Axis auténticos, el ID de dispositivo Axis puede verificarse mediante autenticación IEEE 802.1X o al establecer una conexión de red segura a través del protocolo HTTPS. En una red IEEE 802.1X, el ID de dispositivo Axis puede utilizarse para reforzar la seguridad y reducir el tiempo de implantación.
- **Almacén de claves seguro:** el almacén de claves seguro, basado en módulos de computación criptográficos, almacena información confidencial, como el ID de dispositivo Axis y las claves cargadas por clientes, lo que impide el acceso no autorizado y la extracción maliciosa de información confidencial, aunque el dispositivo esté en riesgo.
- **Sistema de archivos cifrado:** este mecanismo impide la extracción o la manipulación de datos almacenados en el sistema de archivos cuando no se utiliza el dispositivo.
- **Guías de seguridad:** la Guía de seguridad de AXIS OS, disponible en el apartado de AXIS OS del sitio web de Axis, define una configuración de referencia para abordar las amenazas más habituales, además de incluir recomendaciones y asesoramiento técnico. También hay disponible una guía de seguridad del software de gestión de vídeo AXIS Camera Station y para los switches de red Axis.
- **Guía de análisis de seguridad de AXIS OS:** Axis recomienda realizar análisis de seguridad en los dispositivos Axis para comprobar si han estado expuestos a vulnerabilidades o presentan configuraciones poco seguras. La Guía de análisis de seguridad de AXIS OS incluye recomendaciones para resolver algunos de los avisos de los análisis y presenta los falsos positivos más habituales.
- **AXIS Device Manager:** esta herramienta facilita la configuración y la gestión de dispositivos Axis de forma local. Permite procesar por lotes tareas de instalación y seguridad, como gestionar credenciales de los dispositivos, implantar certificados, desactivar servicios no utilizados y actualizar AXIS OS.

EN SERVICIO

Gestión de riesgos asociados al uso de firmware con vulnerabilidades conocidas, la actualización de dispositivos con firmware no autenticado o el vencimiento de configuraciones de seguridad

> **Actualización de firmware:** para garantizar la ciberseguridad de un dispositivo Axis es fundamental mantener actualizado el firmware, a través del modelo activo de actualización de AXIS OS o bien con el modelo de soporte a largo plazo (LTS). Sea cual sea el modelo elegido, las actualizaciones de firmware siempre serán gratuitas e incluirán parches de seguridad. El firmware firmado garantiza que solo puede instalarse firmware auténtico de Axis.

> **AXIS Device Manager Extend:** este complemento de AXIS Device Manager permite la gestión remota de dispositivos Axis y simplifica la aplicación a escala de tareas de mantenimiento, como la actualización del firmware de los dispositivos.

> **Gestión de vulnerabilidades:** Axis ofrece un servicio de notificaciones de seguridad al que puede suscribirse para recibir información sobre vulnerabilidades y otros aspectos vinculados a la seguridad.

> **Guía forense de AXIS OS:** esta guía incluye recomendaciones técnicas para quien quiera realizar análisis forenses de dispositivos Axis en caso de ciberataque en la red y la infraestructura de TI en las que está instalado un dispositivo Axis.

> **Vídeo firmado:** con esta función activada en una cámara compatible, se añaden firmas criptográficas a la transmisión de vídeo antes de que salga del dispositivo, lo que permite a quienes lo visualizan saber si ha sido manipulado o no. Esta prestación resulta especialmente útil en investigaciones o en procesos judiciales.

DESINSTALACIÓN

Gestión del riesgo de dispositivos para los que ya no se ofrece soporte y que tienen vulnerabilidades conocidas y sin parches, así como el riesgo asociado a los datos confidenciales que quedan en los dispositivos después de su eliminación

> **Fecha de fin de soporte de firmware:** la página de soporte de muchos de los productos en Axis.com indica la fecha de fin de soporte del firmware del producto en concreto, lo que permite a los clientes planificar la desinstalación y la sustitución del producto con suficiente antelación.

> **AXIS Device Manager Extend:** permite comprobar el estado de la garantía de todos los dispositivos del sistema y muestra información sobre la descatalogación y el fin de soporte de los productos. Con esta información podrá preparar un dispositivo para su desinstalación y ahorrarse los riesgos de usar un dispositivo sin soporte.

> **Asesoramiento:** la página de AXIS OS del sitio web de Axis incluye recomendaciones para la desinstalación de un dispositivo Axis. Recuperando la configuración predeterminada de fábrica de un dispositivo se eliminan todas las configuraciones y datos.

Para obtener más información, visite: **www.axis.com/es-es/about-axis/cybersecurity**