Preguntas y respuestas sobre ciberseguridad

Manual del usuario

Preguntas y respuestas sobre ciberseguridad

Para conocer otras preguntas y respuestas, visite la *Base de datos de preguntas frecuentes* de Axis.

Preguntas y respuestas sobre ciberseguridad

Preguntas generales

Preguntas generales

¿Qué es la ciberseguridad?

La ciberseguridad es la protección de los sistemas y servicios informáticos frente a ciberseguridades. Las prácticas de ciberseguridad incluyen procesos de prevención de daños y restauración de ordenadores, sistemas y servicios de comunicaciones electrónicas, comunicaciones electrónicas y cable, y almacenamiento de información para garantizar su disponibilidad, integridad, seguridad, autenticidad, confidencialidad y no rechazo.

La ciberseguridad es la gestión de los riesgos durante más tiempo. Los riesgos nunca pueden eliminarse, solo mitigarse.

¿Qué se suele implicar en la gestión de la ciberseguridad?

La ciberseguridad implica los productos, las personas, la tecnología y los procesos.

Por lo tanto, implicará **identificar** y evaluar varios aspectos de su organización, como hacer un inventario de dispositivos, sistemas, software y firmware; establecer objetivos críticos, documentar procedimientos y políticas de seguridad; aplicar una estrategia de gestión de riesgos y realizar continuamente evaluaciones de riesgos relacionadas con sus activos.

Supondrá la implementación de controles y medidas de seguridad para **proteger** los datos, dispositivos, sistemas e instalaciones que haya definido como prioridades frente a ciberataques.

También implicará el desarrollo e implementación de actividades que le ayudarán a **detectar** ciberataques para que pueda tomar acciones a tiempo. Esto podría implicar, por ejemplo, un Sistema de información de seguridad y gestión de eventos (SIEM) o un sistema de Información, automatización y respuesta de seguridad (SOAR) que gestione los datos de los dispositivos de red y el software de gestión, comente datos sobre comportamientos anómalos o posibles ciberataques y los analiza para proporcionar alertas en tiempo real. Los dispositivos Axis son compatibles con los registros SYS y los registros SYS remotos que son la fuente principal de datos para su sistema SIEM o SOAR.

La gestión de la ciberseguridad implica también el desarrollo e implementación de procedimientos para **responder** a un incidente de ciberseguridad una vez detectado. Debe tener en cuenta la normativa local y las políticas internas, así como los requisitos para la revelación de incidentes de ciberseguridad. Axis ofrece una *Guía AXIS OS Forensic* que le ayudará a comprender si un dispositivo Axis se ha visto comprometida durante un ataque de ciberseguridad.

También será importante desarrollar e implementar actividades para mantener los planes de seguridad de los usuarios para **recuperar** o restaurar las prestaciones o servicios dañados a causa de un incidente de ciberseguridad. *AXIS Device Manager*, por ejemplo, facilita la restauración de dispositivos Axis mediante la compatibilidad con puntos de restauración, que se guardan "instantáneas" de la configuración del sistema en un momento dado. En caso de que el punto de restauración sea relevante, la herramienta puede ayudar a devolver todos los dispositivos a sus estados predeterminados y enviar las plantillas de configuración guardadas a través de la red.

¿Cuáles son los riesgos de ciberseguridad?

Los riesgos de ciberseguridad (definidos por RFC 4949 Internet Security) *son una expectativa de pérdida expresada como la probabilidad de que una amenaza concreta aproveche una vulnerabilidad concreta con un resultado perjudicial particular.*

Es importante definir políticas y procesos del sistema claros para lograr una reducción de riesgos adecuada a largo plazo. Uno de los métodos recomendados es trabajar en un marco de protección de IT bien definido, como ISO 27001, NIST o similar. A pesar de que esta tarea puede resultar abrumadora para organizaciones más pequeñas, disponer de una política y una documentación mínimas de los procesos es mucho mejor que nada.

Para obtener información sobre cómo evaluar los riesgos y darles prioridad, consulte la *Guía de referencia de ciberseguridad*.

¿Cuáles son las amenazas?

Una amenaza se puede definir como cualquier cosa que pueda poner en peligro o causar daños en sus activos o recursos. En general, las personas tienden a asociar las ciberamenazas con hackers maliciosos y malware. En realidad, el impacto negativo a menudo se produce debido a accidentes, el uso incorrecto no intencionado o el fallo del hardware. Los ataques pueden clasificarse como oportunistas u objetivos. En la actualidad, la mayoría de ataques son oportunistas: ataques que se producen simplemente porque hay

Preguntas generales

una ventana de oportunidad. Estos ataques utilizarán vectores de ataque a un precio reducido, como el fraude electrónico y rastreos. La aplicación de un nivel de protección estándar mitigará la mayoría de los riesgos relacionados con ataques oportunistas.

Es más difícil protegerse de los atacantes que se dirigen a un sistema específico con un objetivo específico. Los ataques específicos utilizan los mismos vectores de ataque bajos que los atacantes oportunistas. Sin embargo, si los ataques iniciales fallan, están más decididos y dispuestos a dedicar tiempo y recursos a utilizar métodos más sofisticados para lograr sus objetivos. Para ellos, se trata en gran medida de cuánto valor se valora.

¿Cuáles son las amenazas más comunes y cómo se pueden resolver?

Uso incorrecto intencionado o accidental de un sistema

Las personas que tienen acceso autorizado a un sistema es una de las amenazas más comunes a cualquier sistema. Pueden acceder a servicios a los que no están autorizados. Pueden provocar daños intencionadamente en el sistema. Las personas también pueden cometer errores. Al tratar de solucionar las cosas, pueden reducir el rendimiento del sistema de manera inadvertida. Las personas son también susceptibles a la ingeniería social; es decir, una información que permite a los usuarios autorizados proporcionar información confidencial. Las personas pueden perder o desplazar componentes críticos (tarjetas de acceso, teléfonos, portátiles, documentación, etc). Los ordenadores de las personas pueden verse comprometidas y, sin que se presente "un sistema con problemas".

Las protecciones recomendadas incluyen disponer de una política y un proceso de cuenta de usuario definidos, disponer de un esquema de autenticación de acceso suficiente, disponer de herramientas para gestionar cuentas de usuario y privilegios a lo largo del tiempo, reducir la exposición y formación sobre ciberseguridad.

Axis ayuda a contrarrestar esta amenaza con *guías de protección* y herramientas como *AXIS Device Manager* y *AXIS Device Manager Extend*.

Manipulación y sabotaje físico

Los equipos físicamente expuestos se pueden manipular, robar, desconectar, redirigir o cortar.

Las protecciones recomendadas incluyen la colocación de engranajes de red (por ejemplo, servidores y conmutadores) en áreas cerradas, montaje de cámaras de difícil acceso, uso de carcasa protegida cuando se expone físicamente y protección de cables en paredes o conductos.

Axis ayuda a contrarrestar esta amenaza con *una carcasa protectora* para dispositivos, tornillos a prueba de manipulaciones, cámaras con capacidad para cifrar tarjetas SD, detección de manipulación de la vista de la cámara y detección de carcasa abierta.

Explotación sobre vulnerabilidades de software

Todos los productos basados en software tienen vulnerabilidades, conocidas o desconocidas, que pueden aprovecharse. La mayoría de las vulnerabilidades tienen un riesgo bajo, lo que significa que es muy difícil de aprovechar, o el impacto negativo está limitado. En ocasiones, pueden descubrirse vulnerabilidades que se pueden aprovechar y que tienen un impacto negativo significativo. MITRE aloja una gran base de datos de CVE (Common Vulnerabilities & Exposures) para ayudar a otras personas a mitigar los riesgos.

Las protecciones recomendadas incluyen disponer de un proceso de parches continuo que ayude a minimizar el número de vulnerabilidades conocidas en un sistema, minimizar la exposición a la red para dificultar la investigación y aprovechar vulnerabilidades conocidas y trabajar con subproveedores de confianza que trabajen según políticas y procesos que minimicen los defectos, y que proporcionen parches y sean transparentes acerca de las vulnerabilidades críticas detectadas.

Axis responde a la amenaza con el *modelo de desarrollo de seguridad de Axis*, que tiene como objetivo minimizar las vulnerabilidades aprovechables en el software de Axis; y con la *política de gestión de vulnerabilidades de Axis*, que identifica, soluciona y anuncia vulnerabilidades que los clientes deben ser conscientes para tomar las acciones adecuadas. (A partir de abril de 2021, *Axis es una autoridad de numeración de vulnerabilidades y exposiciones comunes* para los productos Axis, lo que nos permite adaptar nuestros procesos al proceso estándar del sector de MITRE Corporation). Axis también ofrece *guías de protección* con recomendaciones sobre cómo reducir la exposición y la adición de controles para reducir el riesgo de explotación. Axis ofrece a los usuarios *dos seguimientos diferentes del software del dispositivo* para mantener actualizado el sistema operativo de un dispositivo Axis:

1. El seguimiento activo proporciona actualizaciones de software del dispositivo compatibles con nuevas funciones y características, así como correcciones de errores y parches de seguridad.

2. El seguimiento a largo plazo del soporte (LTS) proporciona actualizaciones de software del dispositivo compatibles con correcciones de errores y parches de seguridad al tiempo que minimiza los riesgos de problemas de incompatibilidad con sistemas de terceros.

Preguntas y respuestas sobre ciberseguridad

Preguntas generales

Ataque a la cadena de suministro

Un ataque a la cadena de suministro es un ciberataque que intenta dañar a una organización al atacar elementos menos seguros de la cadena de suministro. El ataque se logra al poner en peligro el software/el sistema operativo/los productos y engañar a un administrador para que lo instale en el sistema. Un producto puede verse comprometido durante la entrega al propietario del sistema.

Entre las protecciones recomendadas, se recomienda disponer de una política de instalación únicamente de software de fuentes de confianza y verificadas, verificar la integridad del software al comparar la suma de verificación (digest) del software con la suma de verificación del proveedor antes de la instalación, al verificar las entregas del producto para comprobar si se trata de una manipulación.

Axis hace frente a esta amenaza de varias maneras. Axis publica un software con una suma de verificación para que los administradores puedan validar la integridad antes de instalarlo. Cuando va a cargarse el sistema operativo (SO) de un nuevo dispositivo, los dispositivos de red de Axis solo admiten software de dispositivo con la firma de Axis. *El arranque seguro* en dispositivos de red de Axis también garantiza que solo se ejecute el SO firmado por Axis en los dispositivos. Además, cada dispositivo cuenta con un ID de dispositivo Axis exclusivo, que proporciona una manera para que el sistema compruebe que el dispositivo es un producto de Axis muy importante. Los detalles sobre estas características de ciberseguridad se encuentran en el documento técnico *Axis Edge Vault* (pdf).

Para obtener más información sobre amenazas, consulte la *guía de referencia de ciberseguridad*.

¿Qué son las vulnerabilidades?

Las vulnerabilidades ofrecen oportunidades a los adversarios para atacar o acceder a un sistema. Pueden ser resultado de defectos, características o errores humanos. Los atacantes maliciosos pueden buscar aprovechar cualquier vulnerabilidad conocida, a menudo combinando uno o más. La mayoría de los fallos exitosos se deben a errores humanos, a sistemas mal configurados y a sistemas que se mantienen deficientemente; a menudo, a causa de la falta de políticas adecuadas, de responsabilidades indefinidos y de una falta de sensibilidad.

¿Cuáles son las vulnerabilidades de software?

Una API (interfaz de programación de aplicaciones) de dispositivo y los servicios de software pueden tener defectos o características que pueden aprovecharse para un ataque. Ningún proveedor puede garantizar nunca que los productos no tengan defectos. Si se conocen los defectos, los riesgos pueden mitigarse mediante medidas de control de seguridad. Por otra parte, si un atacante detecta un nuevo defecto desconocido, el riesgo aumenta porque la víctima no ha tenido tiempo de proteger el sistema.

¿Cuál es el sistema de sobresalía de vulnerabilidades común (CVSS)?

El *sistema de valor de vulnerabilidad común* (CVSS) es una forma de clasificar la gravedad de la vulnerabilidad del software. Es una fórmula que analiza lo fácil que es aprovechar y cuál puede ser el impacto negativo. La puntuación es un valor entre 0 y 10, con 10 que representa la mayor gravedad. A menudo encontrará el número CVSS en los informes de exposición y vulnerabilidades comunes (CVE) publicados.

Axis utiliza CVSS como una de las medidas para determinar la importancia de una vulnerabilidad identificada en el software/producto.

Preguntas y respuestas sobre ciberseguridad

Preguntas específicas para Axis

Preguntas específicas para Axis

¿Qué formación y guías disponibles me ayudan a comprender más sobre ciberseguridad y qué puedo hacer para proteger mejor los productos y servicios frente a ciberataques?

La página web de *Recursos* le proporciona acceso a guías de seguridad (por ejemplo, *guía de seguridad de sistemas AXIS OS*, *guía de seguridad de sistemas AXIS Camera Station* y *guía de seguridad de botones de red de Axis*), documentos de políticas, etc. Axis ofrece también cursos de *formación electrónica* sobre ciberseguridad.

¿Dónde puedo ir para encontrar el sistema operativo más reciente para mi dispositivo?

Vaya a *device software (software del dispositivo)* y busque su producto.

¿Cómo puedo actualizar fácilmente el sistema operativo de mi dispositivo?

Para actualizar el software de su dispositivo, puede utilizar un software de gestión de vídeo Axis, como *AXIS Companion* o *AXIS Camera Station* o herramientas como *AXIS Device Manager* y *AXIS Device Manager Extend*.

Si hay interrupciones en los servicios de Axis, ¿cómo puede informarse?

Visite *status.axis.com*.

¿Cómo se puede notificar que se ha descubierto una vulnerabilidad?

Puede suscribirse al *Servicio de notificación de seguridad de Axis*.

¿Cómo gestiona Axis las vulnerabilidades?

Consulte la *Política de gestión de vulnerabilidades de Axis*.

¿Cómo minimiza Axis las vulnerabilidades de software?

Lea el artículo *Hacer de la ciberseguridad un elemento integral del desarrollo de software de Axis*.

¿Cómo admite Axis la ciberseguridad durante todo el ciclo de vida de un dispositivo?

Visite *Una aproximación a la ciberseguridad según el ciclo de vida*.

¿Cuáles son las características de ciberseguridad integradas en los productos Axis?

Leer más:

- *Axis Edge Vault*
- *SO AXIS*
- *Compatibilidad con la ciberseguridad a lo largo del ciclo de vida del dispositivo*

¿Cuenta con la certificación ISO de Axis y con qué otras normativas cumple Axis?

Visite la página web de *Conformidad*.

Preguntas y respuestas sobre ciberseguridad

Preguntas específicas para Axis

¿Cómo ayuda Axis a mi empresa a cumplir con NIS 2?

Consulte el artículo sobre *NIS 2* (pdf).

Manual del usuario
Preguntas y respuestas sobre ciberseguridad

Ver. M4.2
Fecha: Julio 2024
N.º de pieza T10189380