Cybersecurity reference guide

Manual del usuario

Índice

Cybersecurity reference guide

Introducción

Introducción

El objetivo de esta guía es ofrecer una base común y servir de referencia para los materiales relacionados con la ciberseguridad producidos por Axis. Se trata de descripciones, modelos y estructuras simplificados basados en NIST, SANS, ISO y CONI, así como materiales de distintas organizaciones dentro de la comunidad de la ciberseguridad.

Enlaces a otros materiales de Axis:

- *axis.com/about-axis/cybersecurity*
- *help.axis.com/cybersecurity-qna*
- *axis.com/support/cybersecurity/resources*
- *help.axis.com/axis-security-development-model*
- *axis.com/support/cybersecurity/vulnerability-management*

Definición de ciberseguridad

En parte, a partir de la definición procedente de NIST:

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.

Tipos de organización

Diferentes organizaciones tienen diferentes activos, recursos, exposición y madurez cibernética. Al seguir las prácticas recomendadas, *los controles CIS (denominados "controles de seguridad críticos")* definen tres perfiles de organización.

- **Grupo de implementación SANS 1 (IG1)**

  En la mayoría de los casos, una empresa IG1 suele ser pequeña o mediana, con experiencia en TI y ciberseguridad limitadas para dedicar su tiempo a proteger activos de TI y al personal.

- **Grupo de implementación SANS 2 (IG2)**

  Una empresa IG2 emplea personas responsables de gestionar y proteger la infraestructura de TI. Por lo general, estas empresas cuentan con distintos departamentos con distintos perfiles de riesgo en función de la función laboral y de la misión. Las unidades empresariales de pequeño tamaño pueden tener que cumplir con los requisitos normativos.

- **Grupo de implementación SANS 3 (IG3)**

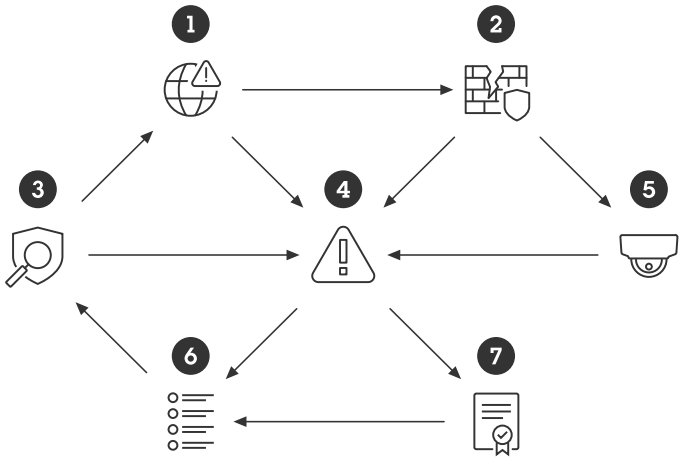
  Una empresa IG3 emplea habitualmente expertos en seguridad que se especializan en los distintos aspectos de la ciberseguridad (por ejemplo, gestión de riesgos, pruebas de riesgos, pruebas de penetración, seguridad de aplicaciones). Los activos y datos de IG3 contienen información confidencial o funciones sujetas a procedimientos normativos y de conformidad.

Terminología

Terminología

Terminología

El mapa de terminología muestra las relaciones de términos clave de la ciberseguridad concretos que se debaten en este documento.



- **(1) Amenazas** explotar **(2) vulnerabilidades** exposición **(5) activos** y aumentando **(4) riesgos**
- **(4) Riesgos** influencia **(7) política** e indica **(6) requisitos**
- **(6) Requisitos** se abordan en **(3) controles de seguridad**, que constantemente enfrentan **(1) amenazas** mientras reducen **(4) los riesgos**

Riesgo

La ciberseguridad es la gestión de los riesgos a lo largo del tiempo. Los riesgos nunca pueden eliminarse, solo mitigarse. A veces, las personas pueden confundir los términos: riesgo, activo, amenaza, vulnerabilidad o impacto negativo

El glosario de seguridad en internet RFC 4949 define los riesgos como una expectativa de pérdida expresada como la probabilidad de que una amenaza concreta aproveche una vulnerabilidad concreta con un resultado perjudicial particular.

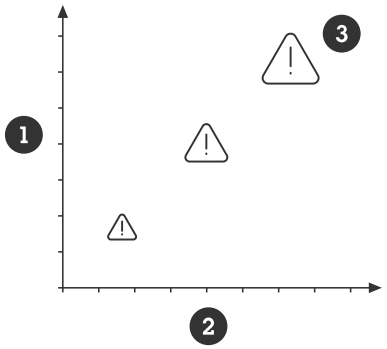
Una versión breve que se usa habitualmente es **Riesgo = Probabilidad x Impacto**

Esta fórmula se utiliza para priorizar los riesgos. La definición de RFC incluye el término "particular" para amenazas, vulnerabilidades y resultados perjudiciales. Cada amenaza debe considerarse individualmente, empezando por la más plausible y con el mayor impacto negativo.

Un problema a la hora de hablar de riesgo es el factor de probabilidad. Las cosas pueden suceder o no. La probabilidad de que un adversario haga uso de una vulnerabilidad a menudo está determinada por la facilidad con la que la vulnerabilidad se puede aprovechar (exposición) y el beneficio potencial para el adversario para aprovecharla.

Con estas dos dimensiones, es posible crear un gráfico de riesgos: utilice la probabilidad de que se produzca un riesgo como un eje y el impacto del riesgo, si se produce, en el otro. Esto da una visión clara del impacto y la prioridad potenciales que debe dar a cada riesgo.

Terminología



1 ***Probabilidad*** *de menor a mayor*
2 ***Impacto negativo*** *de menor a mayor*
3 ***Niveles de riesgo*** *de menor a mayor*

Valor de ataque = Ventajas de ataque – Coste de ataque

Añadir protección aumentará el coste del ataque y, por lo tanto, reducirá las posibilidades. El coste del ataque tiene en cuenta el tiempo, los recursos, las habilidades y la sofisticación necesarios para que el ataque tenga éxito. El riesgo de que lo pillen u otras consecuencias negativas también forma parte del coste del ataque.

La evaluación de riesgos, que es el proceso para analizar los riesgos en el ciberespacio, es la misma que para la protección física. Las preguntas que deben tenerse en cuenta son las siguientes:

1. ¿Qué desea proteger?
2. ¿De quién quiere protegerse?
3. ¿Cuál es la probabilidad de un impacto negativo?
4. ¿Cómo de graves serán las consecuencias si falla?
5. ¿Qué estrategias debería implementar para mitigar los riesgos?

La implementación de cualquier tipo de medida de protección o control de seguridad implica algún tipo de coste. Todas las organizaciones disponen de recursos fiscales limitados. Si no sabe cuáles son los riesgos, es difícil estimar el presupuesto para su protección. Siempre tendrá que aceptar riesgos, pero esa decisión debe ser una decisión deliberada basada en el riesgo.

El cálculo del impacto negativo potencial en cada tipo de activo es duro y complejo. En muchos casos, las estimaciones son subjetivas y, a menudo, el análisis del impacto se infravalora. El uso del modelo de impacto y los tipos de designación (es decir, limitados, serios, graves o catastróficos) de la norma ISO 27000 pueden ayudarle a obtener una visión general rápida para ayudarle a priorizar. Ofrece una manera sencilla de establecer un valor más preciso a partir de la estimación del tiempo que se tardaría en recuperarse de un impacto negativo, a saber:

- **Limitado** = de horas a días
- **Serio** = de días a semanas
- **Grave** = de semanas a meses
- **Catastrófico** = de meses a años, si se recupera

Activos

Aunque la protección física se centra en la protección de personas y objetos físicos, la protección de la ciberseguridad se centra en la protección de activos de datos y recursos informáticos. Existen tres áreas principales:

- **Confidencialidad**: revelación de información o recurso

- **Integridad**: destrucción o modificación de la información o recurso
- **Availability (Disponibilidad)**: acceso a información y recursos

Estas áreas también se conocen como tríada CIA. Con frecuencia, la tecnología de operación (OT) dará prioridad a la usabilidad, mientras que los que trabajan con tecnología de la información (IT) suelen priorizar la seguridad. Encontrar el equilibrio adecuado entre confidencialidad, integridad y disponibilidad es a menudo un desafío.

Los activos y recursos deben clasificarse para determinar los niveles de protección adecuados. No todos los activos de datos y los recursos informáticos son iguales en términos de impacto negativo. A menudo, se clasifican de la siguiente forma:

- **Público**: el activo está destinado a un consumidor público. O bien, el impacto negativo se limitará si se difunde al público.
- **Privado**: el activo puede ser de interés para un grupo específico/seleccionado. Normalmente, el impacto negativo se limita a una organización específica, como una empresa o familia.
- **Restringido**: el activo es una ventaja importante para las personas seleccionadas dentro de una organización.

El vídeo en directo de un sistema de vídeo puede clasificarse como público, lo que hace referencia tanto al público en general como al público de una organización. Sin embargo, en la mayoría de los casos, el vídeo en directo se clasifica como privado, lo que significa que solo puede acceder a él una unidad concreta de la organización. Mientras, el vídeo grabado, en la mayoría de los casos, está clasificado como restringido, ya que puede haber escenas que podrían ser muy sensibles. Las credenciales y configuraciones son también datos que deben clasificarse como restringidos.

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 no se producen por que sí. Siempre hay alguna motivación para comprometer el sistema y sus activos. Los ataques pueden clasificarse como oportunistas u objetivos. En ciberseguridad, a los atacantes también se les conoce como adversarios que pueden tener intenciones maliciosas.

En la actualidad, la mayoría de ataques son oportunistas: ataques que se producen simplemente porque hay una ventana de oportunidad. En muchos casos, un atacante oportunista externo ni siquiera sabe quién es la víctima. Estos atacantes utilizarán vectores de ataque a un precio reducido, como el fraude electrónico y rastreos. En estos casos, no tienen la información suficiente para dedicar tiempo y recursos a un ataque fallido. se desplazan rápidamente a su siguiente intento. 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.

Adversarios habituales (actores de amenazas)

- **Cercano y querido**: personas que quieran entrar en su vida personal
- **Empleados**: o personas que han accedido legalmente al sistema, ya sea por accidente o por uso incorrecto deliberado
- **Bromistas** : personas que disfrutan tratando de interferir en sistemas informáticos.
- **Hacktivistas**: personas que desean atacar a organizaciones por motivos políticos o ideológicos
- **Ciberdelincuentes**: personas interesados en ganar dinero a través de fraude o de la venta de información valiosa
- **Competidores industriales**: entidades interesadas en obtener una ventaja económica para sus empresas u organizaciones
- **Ciberterroristas**: personas o entidades que realizan un ataque diseñado para causar alarma o pánico, a menudo por motivos políticos o ideológicos
- **Estados**: agentes del servicio de inteligencia extranjero que actúan para obtener beneficios económicos y políticos o para causar daños en los sistemas de información críticos

- **Particulares**: una persona o grupo específicos que actúa por su cuenta en los que la motivación puede ser distinta de las enumeradas anteriormente. Puede ser un investigador, un periodista, un hacker de sombrero blanco o similar. Los hackers de sombrero blanco (también conocidos como hackers éticos) pueden representar una amenaza si da prioridad a ocultar los defectos en lugar de solucionarlos.

Vulnerabilidad

Todos los sistemas tienen vulnerabilidades. Las vulnerabilidades ofrecen oportunidades a los adversarios para atacar o acceder a un sistema. Pueden ser resultado de defectos, exposición, 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 o 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.

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 compensatorias. Por otra parte, si un atacante detecta un nuevo defecto desconocido, el riesgo de éxito de aprovechamiento de dicha vulnerabilidad desde el día cero aumenta porque la víctima no ha tenido tiempo de proteger el sistema.

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.

Directiva

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.

Controles de seguridad

Los controles de seguridad son protecciones o contramedidas que se implementan para evitar, detectar, combatir o minimizar los riesgos de seguridad para la propiedad física, la información, los sistemas informáticos y demás activos. Los procesos de implementación de controles de seguridad se suelen denominar protección.

La compensación de controles de seguridad son protecciones alternativas que pueden utilizarse cuando no es posible aplicar el control de seguridad preferido, o cuando el control preferido puede no estar disponible o puede resultar demasiado costoso.

Los controles de seguridad deben vigilarse y actualizarse continuamente a medida que las amenazas, el valor, las vulnerabilidades y los cambios de exposición cambian a lo largo del tiempo. Para ello es necesario definir y seguir las políticas y los procesos.

SANS Institute ha publicado una *lista de controles CIS*, que es un conjunto de recomendaciones de ciberdefensa prioritarias. Aquí está la lista completa de los controles de seguridad.

- Control CIS 1: Inventario y control de activos empresariales
- Control CIS 2: Inventario y control de activos de software
- Control CIS 3: Protección de datos
- Control CIS 4: Configuración segura de activos y software empresariales
- Control CIS 5: Administración de cuentas
- Control CIS 6: Gestión del control de acceso

Terminología

- Control CIS 7: Gestión continua de vulnerabilidades
- Control CIS 8: Gestión de registros de auditoría
- Control CIS 9: Protección de correo electrónico y navegador web
- Control CIS 10: Defensas de malware
- Control CIS 11: Recuperación de datos
- Control CIS 12: Gestión de infraestructuras de red
- Control CIS 13: Supervisión y defensa de redes
- Control CIS 14: Conocimiento de seguridad y formación de habilidades
- Control CIS 15: Gestión de proveedores de servicios
- Control CIS 16: Seguridad del software de aplicaciones
- Control CIS 17: Gestión de respuesta a incidentes
- Control CIS 18: Pruebas de penetración

La *Guía de seguridad de sistemas de AXIS OS* se basa en CIS.

Medidas de protección ante amenazas comunes

Comprender y contrarrestar las amenazas comunes permite mitigar la mayoría de los riesgos.

Uso incorrecto intencionado o accidental de un sistema

El balance entre la usabilidad y la seguridad de un sistema es difícil. Muchos sistemas se protegen desde una perspectiva de comodidad, no desde la seguridad. Esto ofrece oportunidades de uso incorrecto deliberado o accidental. Las personas que tienen acceso autorizado a un sistema es una de las amenazas más comunes a cualquier sistema.

Ejemplos de amenazas comunes:

- Las personas pueden acceder a servicios (por ejemplo, vídeo en vivo o grabado) para los que no están autorizados
- Las personas cometen errores
- Las personas pueden tratar de solucionar los problemas que resultan en una reducción del rendimiento del sistema
- Personas descontentas pueden provocar daños intencionadamente en el sistema
- Las personas son susceptibles a la ingeniería social
- Las personas roban
- Las personas pueden perder o desplazar componentes críticos (tarjetas de acceso, teléfonos, portátiles, documentación, etc)
- Los ordenadores de las personas pueden verse comprometidos e infectar de forma no intencionada un sistema con malware

Las medidas de protección recomendadas más habituales son:

- Política y proceso de cuenta de usuario definidos
- Esquema de autenticación de acceso suficiente
- Herramientas para gestionar cuentas de usuario y privilegios a lo largo del tiempo
- Reducir exposición
- Formación sobre conocimiento cibernético

Cómo ayuda Axis a contrarrestar esta amenaza:

- La *Guía de protección de sistemas de AXIS OS* describe los controles de seguridad más habituales para las amenazas comunes para un dispositivo
- La *Guía de protección de AXIS Camera Station* describe los controles de seguridad más habituales para los sistemas de vídeo
- *AXIS Device Manager* y *AXIS Device Manager Extend* ayudan a gestionar los controles de seguridad más habituales

Manipulación y sabotaje físico

La protección física de los sistemas de TI es muy importante desde una perspectiva de ciberseguridad.

Ejemplos de amenazas comunes:

- Equipo físicamente expuesto que puede manipularse
- Equipo físicamente expuesto que puede ser robado
- Cables físicamente expuestos que pueden desconectarse, redirigirse o cortarse

Medidas de protección ante amenazas comunes

Las medidas de protección recomendadas más habituales son:

- Coloque el equipo de red (por ejemplo, servidores y switches) en áreas cerradas
- Monte las cámaras de manera que sean difíciles de alcanzar
- Utilice una carcasa protectora cuando esté físicamente expuesta
- Proteja los cables en paredes o conductos

Cómo ayuda Axis a contrarrestar esta amenaza:

- Tarjeta SD cifrada para evitar la reproducción de vídeo si un usuario no autorizado puede expulsar la tarjeta SD
- Detección de manipulación de la vista de la cámara
- Detección de apertura de carcasa

Explotación de vulnerabilidades de software conocidas

Todos los productos basados en software tienen vulnerabilidades que pueden aprovecharse. Pueden clasificarse como conocidas y desconocidas. Con el tiempo, todas las vulnerabilidades desconocidas se conocerán. es cuestión de tiempo. La mayoría de las vulnerabilidades tienen un riesgo bajo, lo que significa que son muy difíciles de aprovechar, o que 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 and Exposures) para ayudar a otras personas a mitigar los riesgos.

Las medidas de protección recomendadas más habituales son:

- Un proceso de parches continuo ayuda a minimizar el número de vulnerabilidades conocidas en un sistema.
- Minimice la exposición a la red para dificultar la investigación y aprovechar las vulnerabilidades conocidas.
- Trabaje con subcontratistas de confianza que trabajen según políticas y procesos que minimicen los defectos, tengan procesos para proporcionar parches y le notifiquen cuando se descubran vulnerabilidades críticas.

Cómo ayuda Axis:

- *El modelo de desarrollo de seguridad de Axis* es un marco que define los procesos y herramientas que Axis utiliza para reducir el riesgo de comercializar productos con vulnerabilidades de software.
- *La política de gestión de vulnerabilidades de Axis* implica la identificación, la corrección y la revelación de vulnerabilidades que los clientes deben conocer para tomar las acciones adecuadas. Desde abril de 2021, Axis es una autoridad de numeración (CNA) de vulnerabilidades y exposiciones comunes (CVE) para los productos Axis, lo que nos permite adaptar nuestros procesos al proceso estándar del sector de MITRE Corporation. Esto, a su vez, nos ayuda a ayudar a nuestros clientes de una mejor manera.
- *Las guías de protección de Axis*, como la *Guía de seguridad de sistemas de Axis OS*, ofrecen recomendaciones sobre cómo reducir la exposición y agregar controles compensatorios para reducir el riesgo de fallos del software.
- Las versiones de firmware LTS (soporte a largo plazo) permiten a los clientes aplicar parches al sistema operativo de los dispositivos Axis al tiempo que minimizan los riesgos de problemas de incompatibilidad con sistemas de gestión de vídeo de terceros.

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. Se utiliza sobre todo cuando otros vectores de ataque (por ejemplo, ingeniería social, ataques de phising o sondeo de interfaces) fallan debido a los elevados niveles de protección del sistema. El ataque se logra al poner en peligro el software/firmware/productos y asegurar a un administrador que lo instale en su sistema. Un producto puede verse comprometido durante la entrega al propietario del sistema. Para poder hacer un ataque en la cadena de suministro se necesitan habilidades, tiempo y recursos.

Medidas de protección ante amenazas comunes

Las medidas de protección recomendadas más habituales son:

- Tenga una política para instalar solo software de fuentes de confianza y verificadas.
- Verifique la integridad del software comparando la suma de verificación del software (digest) con la suma de verificación del proveedor antes de la instalación.
- Al entregar el producto, compruebe si se ha manipulado el producto o el paquete.

Cómo ayuda Axis a contrarrestar esta amenaza:

- Axis publica un software con una suma de verificación para que los administradores puedan validar la integridad del software antes de instalarlo.
- El firmware firmado de un dispositivo Axis garantiza tanto que el sistema operativo instalado (AXIS OS) sea realmente de Axis como que Axis firmará también cualquier firmware nuevo que deba descargar e instalar en el dispositivo.
- El inicio seguro en un dispositivo Axis permite al dispositivo comprobar si el firmware tiene la firma de Axis. Si el firmware no se ha autorizado o se ha modificado, se cancelará el proceso de arranque.
- El ID de dispositivo Axis compatible con IEEE 802.1AR es un certificado de proveedor de Axis exclusivo para dispositivos que proporciona un modo para que el sistema compruebe que el hardware de la carcasa procede de Axis.
- El cifrado de tarjetas SD y el cifrado del sistema de archivos evitan la extracción de datos almacenados cuando la tarjeta o el dispositivo se roba.

Manual del usuario
Cybersecurity reference guide

Ver. M3.2
Fecha: Noviembre 2023
N.º de pieza T10201166