Ciberseguridad en la cadena de suministro

Riesgos y estrategias de protección en dispositivos electrónicos y sistemas de seguridad física

La creciente digitalización de infraestructuras y sistemas de seguridad ha ampliado significativamente la superficie de ataque de las organizaciones. En particular, la seguridad de la cadena de suministro tecnológica se ha convertido en un factor crítico para garantizar la integridad de dispositivos electrónicos utilizados en videovigilancia, control de accesos o sensores inteligentes. Analizamos los principales riesgos asociados al hardware y firmware de estos dispositivos, así como las estrategias técnicas y regulatorias necesarias para mitigarlos en el contexto europeo actual.

Claves del análisis

- La cadena de suministro tecnológica se ha convertido en un vector de ataque prioritario, especialmente en entornos donde dispositivos electrónicos y sistemas de seguridad física están conectados a redes corporativas.
- El hardware, el firmware y los componentes de terceros introducen riesgos específicos, desde manipulación de circuitos hasta vulnerabilidades en software embebido.
- El marco regulatorio europeo refuerza la gestión del riesgo en proveedores, especialmente mediante la Directiva NIS2 y su alineación con marcos regulatorios nacionales como el Esquema Nacional de Seguridad.
- La adopción de principios de seguridad desde el diseño y la trazabilidad de componentes es fundamental para garantizar la resiliencia de sistemas de videovigilancia, control de accesos y otros dispositivos de seguridad física.

La cadena de suministro como nuevo vector de ataque

La transformación digital de infraestructuras críticas y entornos corporativos ha impulsado una adopción masiva de dispositivos electrónicos conectados. Cámaras IP, sistemas de control de acceso, sensores inteligentes o plataformas de monitorización forman parte de ecosistemas tecnológicos cada vez más complejos y distribuidos.

En este contexto, la ciberseguridad ya no puede limitarse a la protección de redes o aplicaciones. Las amenazas pueden originarse en cualquier punto de la cadena de suministro: desde el diseño de componentes electrónicos hasta el desarrollo de firmware, la distribución de equipos o su mantenimiento operativo.

Este cambio responde a la creciente interdependencia entre fabricantes de hardware, desarrolladores de software, integradores tecnológicos y operadores finales. Cada uno de estos actores introduce dependencias tecnológicas que pueden convertirse en vectores de riesgo si no se gestionan adecuadamente.

Los ataques a la cadena de suministro tienen además un impacto especialmente amplio. Cuando un proveedor es comprometido, el efecto puede propagarse simultáneamente a múltiples organizaciones que utilizan sus productos o servicios. Entre los escenarios que ilustran estos riesgos se encuentran, de forma no exhaustiva:

- Inserción de hardware o firmware malicioso en componentes críticos durante la fabricación (casos reportados en la industria de telecomunicaciones y satélites).
- Manipulación de dispositivos durante transporte o distribución, incluyendo modificaciones físicas o instalación de software no autorizado (incidentes detectados en dispositivos de red globales).
- Vulnerabilidades en bibliotecas de terceros o firmware embebido, propagadas a múltiples dispositivos conectados (por ejemplo, Apache Log4j y SolarWinds).
- Actualizaciones remotas comprometidas, que permiten introducir código malicioso en dispositivos desplegados en entornos corporativos o críticos.

  -Explotación de credenciales por defecto o configuraciones inseguras, utilizadas para acceder a sistemas de control de acceso, cámaras o sensores inteligentes (incidentes frecuentes en dispositivos IoT y cámaras conectadas a Internet).

Riesgos en el hardware y los componentes electrónicos

Los dispositivos electrónicos utilizados en sistemas de seguridad física dependen de múltiples componentes hardware: microcontroladores, chips de comunicación, módulos de almacenamiento o sensores especializados. Estos componentes suelen fabricarse en cadenas de producción distribuidas globalmente, lo que dificulta la trazabilidad completa del proceso.

Uno de los riesgos más analizados es la introducción de hardware troyano, modificaciones maliciosas en circuitos integrados que alteran el comportamiento del dispositivo. Estas alteraciones pueden permitir acceso remoto oculto, filtrado de información o activación de funciones no documentadas.

Otro riesgo relevante es la manipulación de dispositivos durante las fases de transporte o distribución. Equipos interceptados antes de su instalación pueden ser modificados para incorporar firmware malicioso o mecanismos de acceso persistente.

Para mitigar estos riesgos, los fabricantes están incorporando tecnologías de protección como:

- raíces de confianza hardware (Root of Trust)

- mecanismos de arranque seguro (Secure Boot)
- almacenamiento seguro de claves criptográficas (TPM o similar)
- verificación de integridad del firmware

Firmware: un punto crítico de seguridad

El firmware constituye uno de los componentes más críticos desde el punto de vista de la seguridad. A diferencia del software convencional, el firmware opera con privilegios elevados y tiene acceso directo al hardware.

Muchos dispositivos desplegados en entornos de seguridad física presentan debilidades en este ámbito, como mecanismos de actualización insuficientemente protegidos, uso de bibliotecas obsoletas o ausencia de auditorías de seguridad del código.

Estas vulnerabilidades pueden permitir a un atacante comprometer completamente el dispositivo. En sistemas de videovigilancia, por ejemplo, un firmware comprometido podría manipular grabaciones, desactivar sensores o utilizar el dispositivo como punto de acceso a redes corporativas.

La mitigación de estos riesgos requiere incorporar prácticas de desarrollo seguro de firmware, incluyendo:

- firma criptográfica del firmware
- verificación de integridad durante el arranque
- actualización remota autenticada
- gestión segura de claves
- auditorías periódicas de seguridad

Seguridad física conectada: una superficie de ataque creciente

La convergencia entre seguridad física y tecnologías de la información ha transformado profundamente el sector. Sistemas tradicionalmente aislados, como la videovigilancia o el control de accesos, se integran hoy en redes IP corporativas y plataformas cloud.

Entre los dispositivos más habituales en estos entornos se encuentran cámaras IP, grabadores de vídeo en red, lectores de control de acceso o sensores de intrusión. Estos sistemas presentan características que incrementan su exposición a riesgos de ciberseguridad.

En primer lugar, suelen desplegarse a gran escala en instalaciones complejas. Además, tienen ciclos de vida prolongados —recuentemente diez años o más—lo que dificulta mantenerlos actualizados frente a nuevas vulnerabilidades.

La vulneración de estos dispositivos puede permitir a un atacante acceder a información sensible, manipular registros de seguridad o utilizar la infraestructura como punto de entrada a otros sistemas corporativos (como botnet).

Marco regulatorio: NIS2 y Esquema Nacional de Seguridad

El marco regulatorio europeo ha reforzado notablemente los requisitos de ciberseguridad aplicables a organizaciones públicas y privadas.

La Directiva NIS2 amplía el alcance de la normativa anterior e introduce obligaciones más estrictas para las entidades consideradas esenciales o importantes. Entre sus principales objetivos se encuentra mejorar la resiliencia de las organizaciones frente a incidentes de ciberseguridad y reforzar la cooperación entre Estados miembros.

Uno de los aspectos clave de NIS2 es la gestión del riesgo en la cadena de suministro. La directiva exige que las organizaciones evalúen los riesgos asociados a proveedores y adopten medidas para garantizar que los productos y servicios tecnológicos utilizados cumplen niveles adecuados de seguridad.

En el ámbito nacional, el Esquema Nacional de Seguridad establece el marco de referencia para garantizar la seguridad de la información en el sector público español y en las entidades que prestan servicios tecnológicos para la Administración.

El ENS incorpora controles específicos relacionados con la gestión de proveedores y la adquisición segura de productos TIC, estableciendo requisitos para evaluar la seguridad de los sistemas utilizados, gestionar vulnerabilidades y proteger el ciclo de vida completo de los sistemas.

El modelo de adquisición segura promovido por el ENS se apoya en el uso de productos y componentes certificados, así como en la utilización de recursos como el catálogo de CPSTIC (Catálogo de Productos y Servicios TIC), gestionado por el Centro Criptológico Nacional. Este catálogo facilita a las organizaciones públicas la identificación de soluciones tecnológicas evaluadas o certificadas conforme a criterios de seguridad reconocidos.

Recomendaciones prácticas para evaluar la seguridad de los proveedores

Evaluar la seguridad de proveedores tecnológicos:

Analizar las prácticas de seguridad de fabricantes e integradores antes de adquirir dispositivos electrónicos o soluciones de seguridad física. Se trata de analizar no solo los productos y servicios a adquirir, sino también la fiabilidad de quien los suministra desde el origen.

Evaluar proveedores de seguridad electrónica dentro de la cadena de suministro exige combinar criterios de ciberseguridad, continuidad operativa, cumplimiento normativo y resiliencia física. El objetivo no es solo verificar si “umplen” sino determinar si el proveedor puede convertirse en un punto de vulnerabilidad para toda la organización.

Una práctica efectiva es combinar:

- Evaluación inicial
- Clasificación de criticidad del proveedor (en función del acceso a datos y sistemas y el impacto posible)
- Evaluación técnica
- Requisitos contractuales (notificaciones, tiempos de respuesta, cumplimiento normativo)
- Monitorización continua (la evaluación no debe ser estática)

Principales aspectos que revisar en una evaluación inicial sobre un proveedor de dispositivos de seguridad electrónica

Gobierno y políticas:

- Política de seguridad de la información
- Responsable de ciberseguridad identificado
- Transparencia en la información
- Gestión de riesgos formal

Certificaciones y cumplimientos relevantes, las más aplicables suelen ser:

- ISO 27001
- IEC 62443
- ETSI 303 645
- SOC 2 Type II
- CRA (Cyber Resilience Act)
- ENS (si opera con sector público)
- NIST Cybersecurity Framework (alineado)

Gestión de vulnerabilidades:

- Frecuencia de actualizaciones
- Pen tests, escaneos periódicos y proactividad en la detección de vulnerabilidades
- Procedimiento de respuesta ante CVEs (vulnerabilidades publicadas)
- Tiempo medio de remediación (tiempo en facilitar un parche o actualización para afrontar las vulnerabilidades encontradas desde su publicación)

Desarrollo seguro:

Especialmente importante si el proveedor fabrica software o dispositivos:

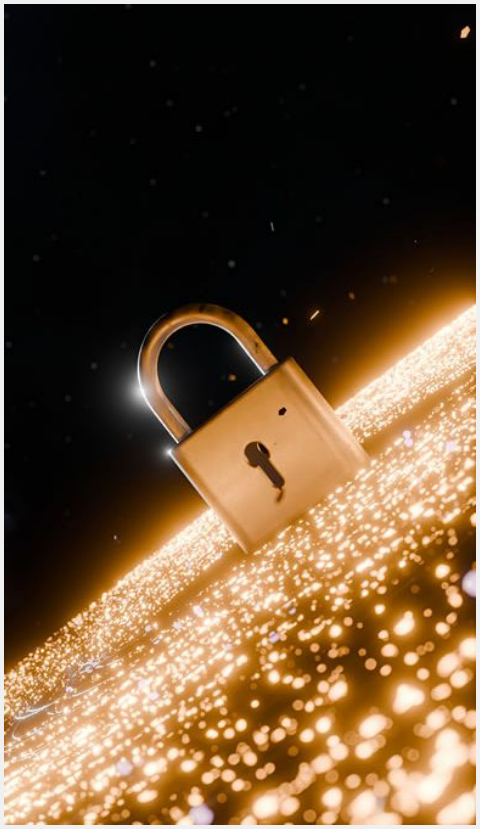
- Marco de desarrollo basado en Secure Software Development Life Cycle (SSDLC)
- Pruebas de penetración
- Revisión de código fuente (preferiblemente firmware no cifrado para garantizar la ausencia de “uertas traseras”y contraseñas hardcoded)
- Firmware firmado digitalmente

Indicadores prácticos de alerta (“Red flags”)

Se debe desconfiar cuando:

- No se permiten auditorías
- No están documentadas las actualizaciones
- Se utilizan contraseñas por defecto
- No existe soporte de firmware o no se especifican los términos y fechas
- El soporte remoto es opaco
- No se informa sobre subprocesadores o software de terceros incluído (SBOM)
- No se demuestran controles

Conclusión



La seguridad de la cadena de suministro se ha convertido en uno de los principales desafíos de la ciberseguridad actual. La creciente integración de dispositivos electrónicos en sistemas de seguridad física amplía la superficie de ataque y exige nuevas estrategias de protección.

Los riesgos pueden originarse en cualquier fase del ciclo de vida del dispositivo, desde la fabricación de componentes hasta la distribución de firmware o la gestión de proveedores tecnológicos. Por ello, las organizaciones deben adoptar enfoques integrales que combinen medidas técnicas, gestión de riesgos y cumplimiento normativo.

En un entorno cada vez más interconectado y dependiente de proveedores externos, garantizar la seguridad de cada eslabón de la cadena de suministro no es solo una cuestión técnica, sino una condición estratégica para preservar la resiliencia y confianza de las infraestructuras críticas y de los sistemas de seguridad física.

Alberto Alonso

Miembro del área de ciberseguridad de AES