DOCUMENTO TÉCNICO

La digitalización y la ciberseguridad del control de acceso físico

Un análisis de los sistemas y protocolos que permiten a las empresas aprovechar al máximo el potencial del control de acceso y crear un mundo más inteligente y seguro

Julio 2021

AXIS COMMUNICATIONS

Índice

1 Resumen

El desarrollo de las tecnologías en la nube está transformando el sector de la seguridad física y obliga a los instaladores a adaptarse para no perder su lugar. El control de los sistemas de acceso se está convirtiendo en territorio de las empresas tecnológicas internacionales, coincidiendo con el crecimiento de las expectativas sobre los sistemas, que son cada vez más inteligentes, escalables y basados en el extremo.

Esta evolución, combinada con el potencial de integración en otros sistemas empresariales, implica también que la ciberseguridad debe tener un protagonismo cada vez mayor en el desarrollo y la implementación de los sistemas, sobre todo en aquellos casos en que se utilice la infraestructura existente. Superar barreras técnicas, como la arquitectura en serie o la ausencia de direcciones MAC, es crucial en esta transición a los sistemas de control de acceso digitales para dar respuesta a las necesidades actuales y de futuro.

Cuando implementamos y protegemos un sistema digital utilizado para el control de acceso, tenemos que aplicar las prácticas recomendadas para garantizar el máximo nivel de seguridad. Tenemos que evaluar y probar todos los componentes del sistema, ya sean dispositivos, distribuidores o protocolos. Todos tienen que ser fiables. También debemos estar pendientes en todo momento de las amenazas y saber cómo responder ante los riesgos que plantean nuevas vulnerabilidades y errores.

Los proveedores merecen un capítulo aparte, puesto que son sus dispositivos los que se conectarán a su red. Un proveedor con garantías debe diseñar y comunicar procesos para proteger sus productos y servicios, por ejemplo, mediante la publicación de una guía de reforzamiento o la creación de herramientas específicas para gestionar y proteger los dispositivos de la red de forma más sencilla, etc. Además, es recomendable que se muestre dispuesto a divulgar su estrategia para gestionar las vulnerabilidades y errores descubiertos.

2 Introducción: El futuro del control de acceso

La conectividad en la nube ha mostrado al sector de la seguridad física un camino completamente nuevo para la implementación y la utilización de sus sistemas. Los usuarios finales y los compradores piden soluciones más inteligentes, integradas y adaptadas a las necesidades de su empresa, con unas opciones de vigilancia y control de acceso que van mucho más allá de las que ofrecían las tecnologías tradicionales.

Muchos proveedores han levantado un sólido modelo de negocio basado en sus conocimientos y experiencia en el ámbito de la seguridad física. Sin embargo, con las redes y el IoT este mundo está en constante evolución y a los proveedores e instaladores tradicionales de soluciones de seguridad física no les queda otra opción que aprender el lenguaje de las TI (plataformas abiertas, conectividad IP e integración de software) para poder adaptarse a los cambios y mantener su relevancia.

Parece que el control está dejando de ser territorio exclusivo de los proveedores de sistemas de acceso electrónicos: están ganando protagonismo rápidamente las empresas tecnológicas internacionales, capaces de dibujar un nuevo horizonte para la seguridad y revolucionar el paradigma clásico. Las ciudades y los edificios inteligentes presentan grandes oportunidades y muchos apuntan a un rápido crecimiento del mercado del control de acceso moderno gracias a la facilidad de implementación y la sofisticación de las tecnologías actuales, que aportan numerosas ventajas en los entornos inteligentes.

No es extraño constatar el auge del control de acceso alojado, sobre todo en un momento en que los grandes gigantes tecnológicos han demostrado el éxito de las tecnologías en la nube, convertidas en una pieza clave durante la pandemia de la COVID-19. Estas compañías tienen la capacidad, la envergadura y la imaginación necesarias para impulsar un cambio radical y, en esta transición, la seguridad física también cambiará porque las empresas son cada vez más conscientes del valor de la nube y prefieren las soluciones alojadas para todas sus necesidades de seguridad y gestión.

Sin embargo, la realidad es que en estos momentos muchos fabricantes no están preparados para este mercado en pleno proceso de transformación y siguen con sus modelos de negocio basados en diseños rígidos y de uso privado. La transición hacia las soluciones inteligentes de seguridad física convive con este enfoque tradicional, al que le esperan no pocos desafíos. Aunque el cambio no se producirá de la noche a la mañana y las nuevas soluciones de alojamiento en la nube no son todavía la opción mayoritaria, este nuevo mundo es el feudo de los ingenieros que aterrizan ahora en nuestro sector.

El futuro del control de acceso, y de la seguridad física en su conjunto, estará marcada por la expectativa de obtener más valor. Los sistemas de control de acceso se convertirán en puntos de recopilación de datos y los controladores de puerta pasarán a ser dispositivos de E/S inteligentes. Los códigos QR para la gestión de visitantes y el reconocimiento facial biométrico para un control de acceso más ágil se gestionarán cada vez más desde el extremo, a través de analítica integrada en una cámara o sensor. El futuro del control de acceso llega cargado de oportunidades y desafíos para aquellos dispuestos a aceptarlos y contribuir a la transformación del sector, una oportunidad inmejorable de innovar para un mundo más inteligente y seguro.

En este documento técnico, analizamos los aspectos que son especialmente relevantes para el control de acceso, como muchas de las funciones esenciales de estos sistemas. Repasaremos también las prácticas recomendadas para los proveedores. Asimismo, daremos información y sugerencias a los usuarios finales para que puedan plantear sus inquietudes a los proveedores con más conocimiento de causa y tomar decisiones de compra más acertadas.

3 Desafíos de un mercado de control de acceso en plena transformación

En el terreno de los sistemas de control de acceso físico (PACS), la tendencia es abordar los factores de riesgo en términos de concesión o bloqueo de la entrada física. No obstante, es importante adoptar un enfoque neutro al diseñar un sistema de este tipo y tener en cuenta las amenazas potenciales.

Hoy en día, cada vez son más los edificios protegidos por soluciones de control de acceso electrónico con un gran nivel de sofisticación. Estos sistemas son una opción rápida y eficiente para gestionar el acceso en el conjunto de la empresa y dejan una huella digital que puede analizarse y supervisarse si es necesario, además de estar totalmente integrados en otros sistemas, como soluciones de recursos humanos y gestión de visitantes.

Con la unificación de los sistemas, se genera información de gran utilidad para tomar decisiones empresariales, de seguridad y también de control de acceso. Y, en este contexto, es crucial evaluar a conciencia la madurez del sistema en el ámbito de la ciberseguridad. Sabemos que los delincuentes utilizan estrategias cada vez más sofisticadas y que las amenazas no dejan de evolucionar, por lo que ahora el reto es reducir riesgos como credenciales de acceso clonadas, amenazas internas y ciberataques remotos.

No obstante, la propia arquitectura es problemática. Muchos sistemas tradicionales de control de acceso se basan en infraestructuras desfasadas. Como son varias las tecnologías de seguridad que utilizan esta infraestructura, los proveedores se encuentran con un doble desafío: por un lado, adaptar su hardware para que pueda conectarse a estas redes corporativas y, por el otro, tomar conciencia de la importancia de la seguridad informática y de los cambios en el mundo de la seguridad, que impulsan la necesidad de analizar los numerosos riesgos a los que se expone una empresa y también buscar protección.

La ciberseguridad debe ocupar un lugar prioritario en el desarrollo de nuevos sistemas de seguridad. Las tecnologías de control de acceso son una parte esencial de cualquier solución de seguridad física y, por lo tanto, su proceso de fabricación debe respetar principios reconocidos en materia de ciberseguridad y prácticas recomendadas, además de incluir herramientas para generar informes en caso de incidentes. Es importante ser muy consciente de que la integridad de un sistema es igual a la seguridad del eslabón más

débil. **Un sistema que no esté preparado para asumirlo** presenta un riesgo potencial de exposición. Si no demuestra su capacidad para asumirlo, informar de lo ocurrido y aplicar planes de recuperación contrastados, disminuirá su eficiencia a la hora de ofrecer los niveles de seguridad física que motivaron su implementación.

3.1 Credenciales de ciberseguridad (madurez del sistema)

La creciente presencia del sector de las TI está empezando a cambiar los procedimientos de evaluación, implantación y mantenimiento de las tecnologías. Para los responsables de TI, es fundamental evaluar las credenciales de ciberseguridad de una empresa, prestando una especial atención a los conocimientos de los proveedores en este terreno. Es lo que suele conocerse como madurez en ciberseguridad e implica que el proveedor está familiarizado con las amenazas y con las estrategias para combatir los riesgos. La exhaustiva documentación y pautas sobre ciberseguridad desarrolladas para las cámaras de red pueden aplicarse también al control de acceso físico, puesto que los desafíos, evaluaciones y explicaciones de los ciberriesgos y los posibles ataques son igual de relevantes para estos productos.

3.2 El futuro de la arquitectura de los sistemas de seguridad

Los dispositivos de control de acceso modernos están conectados por cables de red y conectores RJ45. Las redes proporcionan alimentación a los controladores de acceso y también posibilitan la comunicación entre los dispositivos y con los sistemas de gestión centrales. En el control de acceso, el motor del cambio es la transición a los sistemas basados en TCP/IP. Desde el lanzamiento del primer controlador de puerta IP (AXIS A1001) en 2013, los PACS han continuado evolucionando y ahora ofrecen un amplio abanico de funciones de última generación, que nunca hubieran visto la luz con la tecnología anterior.

Algunos ejemplos de estas innovaciones son los lectores de códigos QR para facilitar el control de acceso sin contacto, el reconocimiento facial mediante la integración con cámaras de red y la lectura de matrículas. En todos estos casos, los sistemas interactúan con bases de datos de PACS para permitir o rechazar la entrada usando un sistema de toma de decisiones en el extremo. Entre las principales ventajas de los sistemas IP, encontramos los reducidos costes de instalación, combinados con un procedimiento sencillo de configuración y gestión de los dispositivos. La integración sin fisuras con otros dispositivos prepara la solución para el futuro: garantiza que se podrán incorporar nuevas tecnologías y mejoras sin complicaciones.

3.3 Ventajas de la tecnología IP frente al control de acceso tradicional

Las ventajas de la tecnología IP se traducirán en nuevos diseños de control de acceso más modernos, sobre todo sistemas sin contacto, que son los que esperan los usuarios finales. Los usuarios quieren también que el control de acceso se adapte al uso que hacen de sus smartphones y tablets, lo que implica ir un paso más allá de las credenciales móviles. ¿Cómo conseguirá el sector crear sistemas de control de acceso más potentes, útiles y con una mejor relación tiempo/coste? ¿Logrará seguir el ritmo de los ciclos de innovación con los que trabajan las grandes empresas tecnológicas? Estos son los desafíos a los que se enfrentan los proveedores del sector.

Hasta ahora no se han explotado estas oportunidades, seguramente porque los sistemas de control de acceso existentes dependen de controladores de puerta instalados en una arquitectura en serie y conectados por cables RS-485 a una unidad o servidor central. Además, en la mayoría de los sistemas el controlador de puerta puede gestionarse únicamente con el software definido por el proveedor. Por lo tanto, el usuario final está atado a un único proveedor de hardware y software. Y no solo eso: la complejidad de estos sistemas obliga a contar con profesionales expertos para su instalación y configuración en la mayoría de los casos.

El proceso de ampliación de sistemas de acceso tradicionales es complicado: un controlador central suele estar diseñado para un número determinado de puertas y las configuraciones que se salen de la norma implican costes elevados a causa de la limitada flexibilidad del sistema. A veces, añadir una sola puerta puede representar una gran inversión y, por lo tanto, un gasto difícilmente justificable.

Las redes IP han abierto la puerta a una arquitectura de los PACS mucho más sencilla y más fácil de instalar, con unos niveles incomparables de flexibilidad y personalización. Los profesionales de TI lo tienen claro: prefieren usar dispositivos IP auténticos e integrarlos en sistemas de control de acceso basados en redes. Incluir a estos expertos en el proceso de diseño es fundamental, porque será la mejor forma de garantizar el uso de estos dispositivos IP, que serán clave para reducir el coste de futuras ampliaciones y también serán piezas imprescindibles en los sistemas de control de acceso del futuro.

3.4 Protocolos abiertos

El futuro del control de acceso dependerá en gran medida de la voluntad de los fabricantes de compartir sus conocimientos en un foro de protocolos abiertos. La resistencia a este nuevo paradigma es evidente: muchos desarrolladores de sistemas de acceso prefieren procesos que aten los usuarios finales a sus soluciones para asegurarse unos ingresos. Sin embargo, este enfoque no genera valor a largo plazo. Los usuarios piden más a sus soluciones y no tienen inconveniente en compartir la información para conseguirlo.

Los diseñadores de sistemas y los proveedores de hardware de acceso raras veces tienen los recursos y los conocimientos tecnológicos necesarios para ofrecer todas las soluciones que los usuarios quieren en su sistema de seguridad física. Muchos parecen no darse cuenta de que su oferta está quedando rápidamente eclipsada por soluciones innovadoras que amenazan su modelo de negocio y también su posición en el mercado del control de acceso. Es tal la velocidad de la innovación y la sofisticación de los sistemas de última generación que estamos muy cerca de no necesitar para nada un controlador de acceso; las unidades de E/S inteligentes se están convirtiendo en su relevo natural.

El uso de protocolos abiertos permite a los proveedores crear dispositivos adecuados para sistemas de acceso de pequeña escala, proyectos en los que se valora especialmente la simplicidad y que requieren unos costes de compra e instalación competitivos. Luego, estos mismos dispositivos pueden adaptarse para instalaciones más grandes y con una mayor complejidad técnica. Esta flexibilidad es el factor diferencial de la seguridad moderna y garantiza la relevancia en el futuro de los sistemas comprados hoy, aunque el negocio crezca y las necesidades cambien.

Encontrará más información sobre la tecnología abierta y esta filosofía en el sitio web de ONVIF *www.onvif.org*, un organismo creado para impulsar la adopción de estándares abiertos en el sector.

4 Barreras técnicas a la adopción

El control de acceso digital es posible gracias a numerosas conexiones técnicas, interfaces y dispositivos. Pueden existir ramificaciones como consecuencia de la sustitución de sistemas tradicionales por sistemas en la nube. En los apartados siguientes repasaremos los aspectos que debemos tener en cuenta para evitar que la tecnología existente y los procesos relacionados se conviertan en una barrera para la adopción de nuevas soluciones.

4.1 Controladores RS-485

Un aspecto que debe tenerse en cuenta es la implantación del controlador RS-485 y los riesgos potenciales de instalar dispositivos semiinteligentes, que raras veces tienen una dirección de control de acceso al medio (MAC), lo que dificulta su identificación. El estándar RS-485, también conocido como TIA-485(-A)

o EIA-485, define las características eléctricas y los controladores y receptores usados en sistemas de comunicaciones en serie. Las señales eléctricas están balanceadas y pueden utilizarse sistemas multipunto. Sin embargo, el estándar RS-485 especifica únicamente la capa física: el generador y el receptor. No incide en la importante capa de comunicaciones.

La ausencia de una dirección MAC o la adopción de una arquitectura en serie no son necesariamente sinónimo de problemas de fiabilidad ni de efectos negativos sobre el funcionamiento del sistema de control de acceso: durante más de 30 años estos diseños han sido la norma en el sector. No obstante, difícilmente pueden percibirse mejoras en los niveles de seguridad a menos que todos y cada uno de los dispositivos de control de un sistema de control de acceso sean inteligentes y puedan gestionarse individualmente. En nuestra opinión, solo los sistemas totalmente inteligentes y los dispositivos completamente accesibles pueden ofrecer el valor esperado. Y cuando hablamos de "completamente accesibles" no nos referimos a dispositivos con una ciberseguridad deficiente, más bien todo lo contrario.

4.1.1 Open Supervised Device Protocol (OSDP)

El Open Supervised Device Protocol (OSDP) es un nuevo método de comunicación aceptado por el IEC con un gran potencial para reforzar la seguridad en las comunicaciones relacionadas con el acceso. Se trata de un estándar de comunicaciones para el control de acceso desarrollado por la Security Industry Association (SIA) con el objetivo de mejorar la interoperabilidad entre los productos de control de acceso y seguridad. El protocolo OSDP utiliza cifrado de 128 bits, permite las instalaciones multipunto y supervisa las conexiones para informar de problemas de lectura. Otro dato interesante es que el OSDP es compatible con lectores de tarjetas, mecanismos de apertura de puertas, contactos de alarma y funciones de petición para salir usando solo 2 cables, en lugar de las múltiples conexiones que antes eran necesarias en cada puerta. En el sitio web de SIA se refieren así a este protocolo: "El OSDP fue aprobado como un estándar internacional por la International Electrotechnical Commission en mayo de 2020 y se publicará como IEC 60839-11-5 en julio de 2020. El OSDP de SIA es objeto de mejoras constantes para mantener su liderazgo en el sector".

4.2 El valor de los dispositivos con una dirección MAC

La dirección MAC es la dirección de hardware única de un dispositivo o adaptador de red. En el contexto de las redes informáticas, la dirección MAC es igual de importante que una dirección IP. Las direcciones MAC identifican cada ordenador de la LAN y son necesarias para el funcionamiento de protocolos como TCP/IP. La dirección MAC está asociada al dispositivo y, aunque es posible manipularla a través del sistema operativo, esta práctica no es recomendable. Es importante que su solución de seguridad la proteja.

Las arquitecturas TCP/IP y otras arquitecturas de redes comunes suelen adoptar un modelo Open Systems Interconnection (OSI), en el que la funcionalidad de la red se subdivide en capas. Las direcciones MAC funcionan en la capa de enlace de datos (capa 2 en el modelo OSI) y permiten a los ordenadores identificarse de forma unívoca en la red. El filtrado de direcciones MAC aporta una capa extra de seguridad. Antes de permitir el acceso de un dispositivo a la red, el router comprueba si su dirección MAC aparece en una lista de direcciones autorizadas. Si la dirección del cliente figura en la lista del router, se le permite el acceso; si no está, no puede acceder.

4.2.1 Alimentación a través de Ethernet (PoE)

PoE presenta dos ventajas que se mantienen invariables independientemente del tipo de aplicación: ahorro económico y flexibilidad en la colocación de los dispositivos. Con la alimentación a través de Ethernet, un mismo cable transporta la alimentación y los datos, lo que permite simplificar la arquitectura de los dispositivos en comparación con los diseños tradicionales. En este punto, vale la pena aclarar que muchos sistemas de control de acceso se promocionan como sistemas IP.

5 Las buenas prácticas imprescindibles

La gestión del control de acceso es importante para controlar el flujo de personas y supervisar el acceso. Para las empresas, no es suficiente con cerrar una puerta o levantar una barrera; necesitan opciones de control avanzadas que les permitan ofrecer una mejor atención a los clientes y garantizar altos niveles de seguridad en todo momento. Cuando hablamos de aplicar buenas prácticas al control de acceso, no nos referimos solo a elegir las herramientas adecuadas. Se trata de contar con la arquitectura correcta, incorporar tecnologías de calidad, aplicar procedimientos y protocolos apropiados, y ayudar a los empleados y colaboradores a adoptar las actitudes y comportamientos esperados.

5.1 La gestión de las partes interesadas y el enfoque de la seguridad convergente

Según vamos observando que el panorama tecnológico converge en las mismas infraestructuras para ofrecer las tecnologías necesarias para que estos sitios funcionen sin problemas, también necesitamos un proceso de toma de decisiones convergente. Hemos visto casos de éxito en los que un enfoque de seguridad convergente ha derribado muros y ha facilitado la colaboración entre equipos en una empresa. Esta convergencia nunca ha sido tan importante como hoy, cuando en las redes corporativas conviven los modelos tradicionales de seguridad electrónica y física.

Es fundamental que los equipos de seguridad física puedan contar con tecnologías capaces de dar respuesta a sus necesidades y de abordar los riesgos asociados, y que al mismo tiempo cumplan las políticas de seguridad informática y garanticen que los dispositivos físicos no se conviertan en una puerta trasera para acceder a la red corporativa. Si todas las partes colaboran, es posible crear un entorno digital y físico seguro.

5.2 Qué esperar de socios, proveedores y distribuidores

Es importante que los colaboradores entiendan la importancia de aplicar las prácticas de seguridad recomendadas en todo lo que hacen y que sean capaces de dar respuesta a necesidades específicas. Las relaciones con terceros son fundamentales para crear una cadena de suministro sólida y para forjar un vínculo fuerte y basado en la confianza.

Principales consideraciones al evaluar a terceros y su impacto en la cadena de suministro: Entienden y reconocen los riesgos asociados a la ciberseguridad > Demuestran una estrategia de ciberseguridad madura con los procesos y las herramientas a su alcance > Entienden el impacto de las regulaciones y la legislación en su oferta > Son capaces de explicar cómo ayudarán a un usuario a cumplir los requisitos normativos > La ciberseguridad es un proceso, no solo una tecnología: pueden demostrar cómo gestionarán el ciclo de vida de la ciberseguridad para proteger la empresa de un usuario.

5.3 Gestión de la seguridad: Gobernanza y procesos de los proveedores

Como ocurre con cualquier sistema de seguridad eficaz, la ciberseguridad depende de lo profundo que sea el nivel de defensa. Se trata de proteger correctamente la red de cámaras IP en todos los niveles, desde los productos y socios elegidos hasta los requisitos definidos.

5.3.1 Normas y directivas

ISO 27001 –Gestión de la seguridad de la información ISO/IEC 27001 es un sistema de gestión de la seguridad que exige:

- El análisis sistemático de los riesgos para la seguridad de la información de una organización, teniendo en cuenta las amenazas, las vulnerabilidades y los impactos

- El diseño y la implementación de un conjunto coherente y completo de controles de seguridad de la información u otras formas de gestión de los riesgos (como evitar o transferir riesgos) para hacer frente a los riesgos considerados inaceptables
- La adopción de un proceso de gestión global para garantizar que los controles de seguridad de la información se ajusten continuamente para dar respuesta a las necesidades de la organización en este ámbito

5.3.2 Cyber Essentials Plus

Cyber Essentials es un programa que cuenta con el apoyo del gobierno y la industria para ayudar a las organizaciones a protegerse contra las amenazas online más habituales. Se trata de un indicador muy útil para las empresas que entienden los desafíos que plantea la ciberseguridad. Su función es evaluar las políticas y los procesos de una compañía. Se centra en concreto en los siguientes aspectos:

- Configuraciones seguras
- Control de acceso y administración
- Protección frente a malware
- Gestión de parches de seguridad
- Cortafuegos y pasarelas de Internet

Para los fabricantes de tecnología, la primera línea de defensa debe consistir en atenuar el riesgo asociado a sus propios sistemas. A partir del 1 de octubre de 2014, el gobierno exige a todos los proveedores que licitan para la obtención de contratos que implican la gestión de determinados datos personales delicados una certificación basada en el programa Cyber Essentials.

5.3.3 Secure by Design, Secure by Default

La iniciativa **Secure by Design, Secure by Default**, presentada en 2019 por el Surveillance Camera Commissioner británico, establece unos requisitos mínimos para los fabricantes de sistemas y componentes de cámaras. La idea es adoptar un enfoque integral para resolver los problemas de seguridad de raíz, en lugar de tratar los síntomas; actuar a escala para reducir el daño global en un sistema o tipo de componente.

Secure by Design, Secure by Default hace referencia al esfuerzo técnico de largo recorrido dirigido a garantizar que se incorporen los principios de seguridad adecuados en el software y el hardware. También abarca la tarea, igualmente exigente, de garantizar que esas primitivas estén disponibles y sean utilizables de manera que el mercado pueda adoptarlas fácilmente.

Para respaldar nuestras tecnologías, Axis ha adaptado Secure by Design, Secure by Default al código de conducta de la National Cybersecurity Strategy:

- Solicitud de contraseña
- Indicador de seguridad de la contraseña
- Cifrado HTTPS
- 802.1x
- Acceso remoto DESHABILITADO (NAT traversal)

6 Guías y herramientas (procesos de proveedores)

Para proteger una red, las organizaciones suelen implantar varios controles técnicos con el objetivo de crear una "defensa por capas", que les ayude a limitar los puntos directos de error y exposición. Sin embargo, un proceso importante que a menudo se olvida es el "endurecimiento del sistema", que incluye la realización de cambios de configuración en los ajustes predeterminados del sistema para que este último sea más seguro ante las amenazas a la seguridad de la información. Además, este proceso contribuye a reducir el número de vulnerabilidades inherentes que existen en todos los sistemas.

6.1 Guía de reforzamiento en los procesos de fabricación

Todos los dispositivos vinculados a una red deberían contar con un proceso de reforzamiento del sistema. Esto incluye estaciones de trabajo, servidores y otros dispositivos de red. Puesto que cada fabricante conoce la configuración de su sistema mejor que nadie, debería ser su responsabilidad facilitar a los socios y usuarios la información necesaria para proteger la integridad de los dispositivos y la instalación del usuario final. Una guía de reforzamiento debería proporcionar asesoramiento técnico a cualquier persona que participe en el despliegue de soluciones de videovigilancia. Asimismo, debería establecer una configuración de referencia, así como información completa para hacer frente a los cambios constantes en las amenazas.

Todos los proveedores deberían esforzarse por mantener una apuesta decidida por la aplicación de las prácticas de ciberseguridad recomendadas en el diseño, el desarrollo y las pruebas de los dispositivos, para minimizar el riesgo de fallos que puedan abrir la puerta a posibles ataques. Sin embargo, la seguridad de una red, sus dispositivos y los servicios a los que presta apoyo exige la participación activa de toda la cadena de suministro del proveedor, así como de la organización del usuario final. La seguridad de un entorno depende de sus usuarios, los procesos y la tecnología. Una buena guía de reforzamiento debe seguir principios de referencia, como los Controles de CIS - Versión 6.1. Estos controles antes eran conocidos como SANS Top 20 Critical Security Controls.

6.2 Gestión de dispositivos

Un gestor de dispositivos es una herramienta utilizada en local que permite gestionar los dispositivos conectados de una forma sencilla, segura y económica. Ofrece a los instaladores de soluciones de seguridad y administradores de sistemas una herramienta muy eficaz para gestionar todas las tareas principales de instalación, seguridad y mantenimiento.

Inventario de dispositivos / Sistema de gestión de activos:

- Política sobre cuentas y contraseñas
- Instalación eficiente de actualizaciones de firmware y aplicaciones
- Aplicación de controles de ciberseguridad: gestione HTTPS y cargue certificados IEEE 802.1x, gestione cuentas y contraseñas
- Gestión del ciclo de vida de los certificados: gestione las principales tareas de instalación, seguridad y funcionamiento
- Configuración rápida y sencilla de dispositivos nuevos: ajustes de copia de seguridad y restauración
- Adecuado para emplazamientos de cualquier tamaño: instalaciones sencillas o múltiples

6.3 Los desafíos vinculados a los OEM/ODM

Los fabricantes de equipos originales (OEM) son fabricantes que revenden el producto de otra empresa con su propio nombre y marca. Un fabricante de diseños originales (ODM) es una empresa que diseña y fabrica un producto con las especificaciones y, en su caso, con la marca de otra empresa, que luego lo comercializa. Estas empresas permiten a la compañía que pone la marca realizar una producción sin tener que montar o gestionar una fábrica.

Son muchas las ventajas para un fabricante que quiera ser OEM u ODM de un producto de otro distribuidor. La primera es que elimina los riesgos y costes de fabricación, y permite a la organización centrarse en los procesos de venta y marketing. Esta es una de las principales razones por las que muchos fabricantes de cámaras del sector de la seguridad recurren a la figura del OEM u ODM para los productos de su marca. Está documentado que hasta 96 proveedores venden cámaras fabricadas por otra empresa a través del modelo OEM u ODM.

Esto plantea varios retos y uno de los más evidentes es el de la ciberseguridad. Si un fabricante tiene una vulnerabilidad en sus productos, este problema puede afectar a todos los redistribuidores y socios de la cadena de suministro. También puede hacer muy difícil la visibilidad completa de la cadena de suministro. Con el elevado número de OEM y ODM, un usuario final que haya seguido el proceso de diligencia debida y haya rechazado las tecnologías de un determinado fabricante podría acabar utilizando de manera involuntaria esas tecnologías bajo otra marca, aunque sin ser consciente de ello.

6.4 Chips de microprocesadores de CPU

Se ha constatado que los chips de procesamiento de CPU genéricos que se instalan en los dispositivos están en el punto de mira de los hackers, y se han identificado numerosas vulnerabilidades. Una de las principales razones es la escalabilidad que generan a partir de una única vulnerabilidad identificada. Algunos ejemplos recientes son los fallos "Meltdown" y "Spectre", dos ataques relacionados, de canal lateral, contra los microprocesadores de CPU modernos que tienen la capacidad de acceder de manera ilícita a los datos utilizando código sin privilegios.

La mayoría de los dispositivos, desde los smartphones hasta el hardware de los centros de datos, pueden ser vulnerables en mayor o menor medida. Los principales proveedores de sistemas operativos han desarrollado parches que mitigan los problemas, aunque algunas partes de los parches se tienen que instalar a través del fabricante del equipo (OEM), ya que contienen elementos específicos de la plataforma. El National Cybersecurity Centre (NCSC) británico aconseja aplicar los parches de seguridad a los dispositivos lo antes posible.

6.5 Estrategia de firmware

El firmware firmado es importante para los usuarios finales y combate algunos de los posibles riesgos de manipulación de los dispositivos durante el proceso de logística y/o distribución. La firma, denominada a veces "hash", se adjunta al firmware en el momento de distribuirlo. Un procesador calcula su propio hash y solo carga una imagen de firmware con un hash que coincida con uno firmado por un certificado de confianza.

6.6 Gestión de las vulnerabilidades

El continuo crecimiento de la ciberdelincuencia y los riesgos asociados están obligando a muchas organizaciones a prestar más atención a la seguridad de la información. Un proceso de gestión de las vulnerabilidades debería formar parte de los esfuerzos de una organización por controlar los riesgos

para la seguridad de la información. Este proceso permite a una organización tener una visión de las vulnerabilidades de su entorno informático en todo momento y de los riesgos asociados a las mismas. Solo identificando y combatiendo las vulnerabilidades del entorno informático, es posible evitar que los atacantes penetren en las redes y roben información.

Es crucial que los distribuidores se aseguren de que la gestión de las vulnerabilidades está integrada en sus operaciones, incluidos los procesos para detectar y reparar las vulnerabilidades en todos los sistemas, y para evitar que se introduzcan nuevas vulnerabilidades durante los procesos de cambio y la implantación de nuevos sistemas. Todos los incidentes relacionados con el riesgo que el distribuidor acepte deben comunicarse al usuario final y consensuarse. Si no se aplica este principio, los atacantes podrían explotar vulnerabilidades del sistema para llevar a cabo ataques contra la empresa y sus distribuidores.

Los parches de seguridad informática y las actualizaciones de las vulnerabilidades de seguridad deben instalarse a través de un proceso aprobado de manera oportuna para evitar cualquier violación de la seguridad. Los sistemas de los distribuidores que, por el motivo que sea, no se puedan actualizar deberán implementar medidas para proteger el sistema vulnerable. Todos los cambios deben realizarse según el proceso de gestión de cambios del distribuidor.

6.7 Notificaciones de avisos de seguridad

Los avisos de seguridad ayudan a reducir los riesgos vinculados a vulnerabilidades conocidas. Estos avisos pueden tener relación con informes CVE (vulnerabilidades y exposiciones comunes) oficiales o con otros informes e incluyen una descripción de la vulnerabilidad, una evaluación del riesgo, recomendaciones e información sobre la fecha prevista para el lanzamiento del parche. La mayoría de los proveedores implantan un modelo de venta indirecta y cuentan con un programa de socios.

Las notificaciones de avisos de seguridad permiten a los clientes que no están inscritos en un programa de socios del fabricante recibir notificaciones de ciberseguridad pertinentes a la primera oportunidad y en cuanto se comunican al distribuidor. Se trata de una herramienta fundamental para los usuarios finales que cuentan con equipos instalados pero que tal vez no tengan un contrato con la empresa que realizó la instalación en su momento.

6.8 Building Security in Maturity Model (BSIMM)

BSIMM es un entorno para analizar el nivel de seguridad del software. Se creó con el objetivo de ayudar a las empresas a comparar la seguridad de su software con otras iniciativas y descubrir cómo quedan en esta comparación. BSIMM permite evaluar procesos, actividades, funciones y responsabilidades en las siguientes áreas:

- Revisiones de diseño y arquitectura
- Revisiones de código
- Prueba de vulnerabilidades conocidas
- Ejecución de una herramienta estándar de análisis de vulnerabilidades que permita detectar vulnerabilidades CVE en paquetes de código abierto

6.9 Soporte a largo plazo (LTS)

El soporte a largo plazo (LTS, por sus siglas en inglés) es una política de gestión del ciclo de vida del producto en la que una versión estable del software se mantiene durante un período de tiempo superior al

de la edición estándar. El firmware del soporte a largo plazo debe incluir únicamente parches de estabilidad, rendimiento y seguridad. Los proveedores ofrecen firmware LTS durante un máximo de diez años desde el inicio de la comercialización de un dispositivo.

Se espera que el LTS exista en paralelo pero de forma independiente al soporte activo. Una de las principales ventajas del soporte LTS es que mantendrá la integración con terceros relacionados con la versión original del firmware.

6.10 Formación y colaboración

Uno de los aspectos esenciales que hay que tener en cuenta a la hora de seleccionar cualquier proveedor de tecnología es la formación y la asistencia que ofrece. A medida que evolucionan los retos a los que se enfrentan los distribuidores y la industria, especialmente en lo que respecta a la ciberseguridad, los fabricantes deberían abordar el tema de forma proactiva y proporcionar documentos y contenidos para el mercado. Algunos ejemplos posibles son los siguientes:

- Cursos presenciales gratuitos sobre ciberseguridad
- Formación sobre ciberseguridad online
- Prueba rápida de ciberseguridad online
- Guía de reforzamiento
- Políticas de vulnerabilidad
- Prácticas recomendadas sobre ciberseguridad
- Conceptos y terminología de ciberseguridad

7 Promover la ciberhigene: próximos pasos y consideraciones

Una buena ciberhigene pasa por identificar, priorizar y responder a los riesgos que amenazan los productos y servicios clave de una organización. La aplicación de las prácticas recomendadas para reforzar la seguridad en este terreno le ayudará a prevenir robos de datos y configuraciones incorrectas del sistema, además de minimizar los riesgos derivados para su empresa. Además, es importante consensuar con las demás partes implicadas cuáles son las principales amenazas para tener claro dónde centrar los esfuerzos en gestión del riesgo.

Aunque esta lista no es exhaustiva, los puntos siguientes le ayudarán a ser más eficiente en todo lo relacionado con la gestión de las ciberamenazas.

7.1 Distribuidores

Compruebe los registros y las certificaciones

Revise los registros y certificaciones pertinentes, por ejemplo, solicite documentos que acrediten los registros de la norma ISO9000 y otras certificaciones de calidad. Analice si los productos del distribuidor están diseñados para su uso en una red corporativa.

Busque pruebas de buenas prácticas

Asegúrese de que el proveedor elegido puede demostrar la aplicación de buenas prácticas en materia de ciberseguridad. Debería contar con una guía de reforzamiento detallando las medidas para reforzar la seguridad física y digital, además de prácticas recomendadas para proteger la red.

Realice una auditoría al proveedor

Someta al proveedor a una auditoría exhaustiva antes de cerrar ningún compromiso de compra. Revise las condiciones para asegurarse de que son claras y transparentes. Desde una perspectiva financiera, es importante preguntar qué sucedería con el producto y la asistencia si la empresa tuviera problemas.

Estudie si los recursos del proveedor serán suficientes en el futuro

Valore si el proveedor cuenta con los recursos necesarios para crear las soluciones que probablemente necesite en un futuro. Analice si su tamaño, alcance y especialización le ofrecen garantías en este sentido.

Define las necesidades de futuro de su empresa

Piense en sus necesidades de futuro. Los dispositivos y soluciones inteligentes aportan un plus a su negocio hoy y le sitúan en una situación inmejorable para encarar el futuro. Debe tener la confianza de que su proveedor cumplirá o superará sus expectativas, con contratos de mantenimiento y asistencia continua.

Busque pruebas de prácticas éticas

Encuentre pruebas que demuestren prácticas éticas y sostenibles. Una alianza basada en la confianza y los objetivos comunes es la mejor inversión a largo plazo. ¿El proveedor cuenta con sistemas de gestión medioambiental, un programa de responsabilidad social corporativa (RSC) o una política de abastecimiento ético?

7.2 Productos y sistemas

Aplique el procedimiento de diligencia debida

Analice el sistema y sus principales componentes según el procedimiento de diligencia debida para comprobar que ofrece el valor previsto y que no hay factores que impidan su funcionamiento. Verifique que existe información clara sobre evaluación y reducción de riesgos.

Estudie el contrato de mantenimiento

Analice qué incluye el contrato, por ejemplo si el contrato de servicio y mantenimiento incluye actualizaciones de software del fabricante y actualizaciones de firmware.

Proteja los dispositivos conectados

Realice comprobaciones para tener la certeza de que el sistema de seguridad física conectado a la red es seguro. En la implementación de los sistemas de seguridad, la ciberseguridad debe ocupar un lugar central: cambie el nombre de usuario y la contraseña asignados por defecto, instale la última versión del firmware, utilice cifrado (idealmente HTTPS) y desactive el acceso remoto.

Solicite un certificado de seguridad del diseño

Su distribuidor debería poder facilitarle un certificado de seguridad del diseño que avale la ciberseguridad de los dispositivos conectados a la red.

Analice la inteligencia del sistema

Los dispositivos conectados realmente inteligentes son los que están conectados a una red con una dirección MAC y forman parte de la arquitectura del sistema. Los dispositivos sin dirección MAC no son inteligentes y es imposible su identificación, gestión y protección individual.

Evalúe el cumplimiento del RGPD/ley de protección de datos

El RGPD entró en vigor en 2018, junto con la Ley de Protección de Datos de 1998 actualizada. Asegúrese de que los productos y sistemas incluyen los mecanismos necesarios para cumplir la Ley de Protección de Datos de 2018 y el RGPD.

T10168631/ES/M1.7/2107

Acerca de Axis Communications

Axis contribuye a crear un mundo más inteligente y seguro a través de soluciones en red que mejoran la seguridad y suponen una nueva manera de hacer negocios. Como líder de la industria del vídeo en red, Axis pone a su disposición productos y servicios de videovigilancia y analítica, control de accesos y sistemas de audio e intercomunicación. Axis cuenta con más de 3800 empleados especializados en más de 50 países, y proporciona soluciones a sus clientes en colaboración con empresas asociadas de todo el mundo. Fundada en 1984, su sede central se encuentra en Lund, Suecia.

Para más información sobre Axis, visite nuestro sitio web *axis.com*.