Ciberseguridad de los sistemas de seguridad físicos: un flanco abierto

Enrique Bilbao / Director técnico de Cuevavaliente Inerco

Los sistemas de seguridad están compuestos por el conjunto de dispositivos, infraestructuras y aplicaciones que permiten gestionar información relativa a la seguridad, detectar incidentes, analizarlos, tomar decisiones y actuar en consecuencia. Esto incluye desde el visionado de una cámara y la identificación de una tarjeta hasta la consecuente apertura de una puerta, pasando por la detección de intrusos y por muchas otras funciones fundamentales para la seguridad de cualquier instalación.

Los sistemas de seguridad de una cierta dimensión están gobernados por lo que se pueden denominar Centros de Control de Seguridad (CCS). Antiguamente (hace algunas decenas de años), estos CCS recibían y enviaban información a elementos distribuidos: cámaras de CCTV, controladores de lectoras de control de accesos y centrales de detección de intrusión y alarma a través de medios diversos (primeros dos niveles OSI [*Open System Interconnection*]: las capas físicas y de enlace), con cableados RG11 o RG59 de las cámaras, buses diversos (a veces propietarios) de control de accesos e intrusión, etc.

Reubicar un CCS era un drama técnico, fundamentalmente por la complejidad que implicaba desplazar/empalmar físicamente los cableados que llegaban hasta la antigua ubicación.

Además, las aplicaciones de control de estos subsistemas apenas empezaban a permitir la interacción entre ellos, como por ejemplo las alarmas que conmutan cámaras.

Actualmente, la capacidad y el alcance de los CCS son muy superiores, siendo muy parecidos a los sistemas de control industriales:

- Se basan en redes IP de datos, por lo que la arquitectura de los sistemas ha cambiado drásticamente.
- Las aplicaciones de control suelen estar superpuestas a sistemas operativos estándares: Windows Server, Linux, Unix, etc.
- Utilizan bases de datos estándares: Oracle, SQL…
- Tienen comunicaciones con el exterior para llevar a cabo un telemantenimiento, compartir operadores remotos, importar datos de altas y bajas de personal, etc.
- Siguen una estructura de servidor-cliente.
- Son multidispositivo y pueden operarse desde navegadores.

Es urgente auditar los CCS, analizar sus riesgos de ciberseguridad y estudiar el 'gap' entre las medidas existentes y las necesarias

Amenazas

En definitiva, los CCS son unos sistemas de control convencionales desde un punto de vista técnico, pero su función principal es la protección física de los activos y las personas mediante los subsistemas que gobierna.

Las amenazas que afectan a la **disponibilidad** del sistema presentan consecuencias muy graves, como por ejemplo seguridad totalmente inoperativa, la no detección de incendios o intrusiones, la no disponibilidad de

imágenes de TV y el caos en los accesos de un edificio en la hora punta.

Por su parte, las correspondientes a la **integridad** no son menores: borrado de imágenes grabadas, generación de tarjetas de control de acceso a personas ajenas, desconexión de alarmas a determinadas horas e indisponibilidad de la información relativa a las actuaciones del equipo de seguridad (vigilantes, operadores) sobre el propio sistema de seguridad.

Finalmente, la **confidencialidad**, teniendo en cuenta que en los CCS se almacenan imágenes grabadas, datos de personal y de visitas, etc., también es una consecuencia muy grave en caso de que las amenazas consigan su objetivo, como por ejemplo conocimiento por parte de terceros del sistema de seguridad, acceso a imágenes o información a personas que no deben conocerlas, incumplimiento de obligaciones relativas a protección de datos de carácter personal u otros incumplimientos.

Situación actual

En España hay algún millar de CCS. Algunos de ellos son de tamaño muy reducido, con decenas de cámaras de TV, de detectores de intrusión y algunas lectoras. Otros, sin embargo, llegan a

Actualmente, la capacidad y el alcance de los CCS son muy superiores, siendo muy parecidos a los sistemas de control industriales

Por otro lado, cabe destacar que, lógicamente, las amenazas son externas e internas:

- **Amenazas externas**: debidas a que la conectividad exterior descrita permite "puertas" por las que acceder al sistema desde el exterior.
- **Amenazas internas**: no solo de operadores (vigilantes u operadores del sistema), sino también porque en muchos casos la misma red de datos que comunican las cámaras de TV, las interfaces, las centrales de detección de incendios e intrusión, etc., es la misma que la red corporativa por la que circulan los correos electrónicos y diversas aplicaciones de la empresa.

controlar centenares de cámaras de TV (o millares, como por ejemplo en aeropuertos), centenares de lectoras de control de accesos y millares de detectores de incendio y de intrusión, amén de centenares de interfonos, etc.

Finalmente, se deben considerar también las centrales receptoras de alarmas, con decenas y a veces centenares de miles de conexiones mediante redes dedicadas o utilizando Internet directamente.

Desde nuestra experiencia en auditorías a CCS, aunque no pueda asumirse la muestra como totalmente representativa, el panorama es muy preocupante. Como ejemplos frecuentes podrían citarse los siguientes:

- No suele haber una política de contraseñas establecida para los operadores de seguridad, los mantenedores de los equipos o los responsables de seguridad que acceden a la información.
- Para los equipos informáticos de los sistemas de seguridad no se mantienen los criterios estandarizados a nivel corporativo para cualquier equipo conectado a la Intranet: sistemas operativos, antivirus, parches, actualizaciones, etc.
- No se realizan auditorías internas o externas de seguridad de la información sobre los sistemas de seguridad.
- No existen criterios de seguridad de la información a la hora de acordar servicios con terceros, SLA (*Service Level Agreement*) o al seleccionar a proveedores de servicios.

Finalmente, como conclusión cabe destacar que las amenazas han cambiado en todos los ámbitos, también el de los CCS. Si antiguamente proteger un CCS consistía en blindajes, esclusas y sistemas de control de acceso físico, ahora esas medidas no tienen nada que ver con las amenazas reales, cuyos actos pueden incluso pasar desapercibidos.

Es urgente auditar los CCS, analizar sus riesgos de ciberseguridad y estudiar el *gap* entre las medidas existentes y las necesarias. Pero, sobre todo, una vez más, es fundamental abrir los ojos de los responsables de seguridad física al nuevo escenario. Estas amenazas han llegado para quedarse… y para evolucionar a peor. Los ciberriesgos de los sistemas de seguridad físicos son un flanco abierto. S