# Los riesgos del desconocimiento

Seguridad informática aplicada a la seguridad electrónica

*La constante evolución e integración de las tecnologías llevan a una necesaria pregunta: la seguridad electrónica y la seguridad informática, ¿son dos disciplinas separadas? La respuesta es "no" y aquí se explican algunas de la razones.*

**Lic. Damián Colaneri**
Gerente Técnico
CTO/CIO/CISO - ISSI MBB S.A.

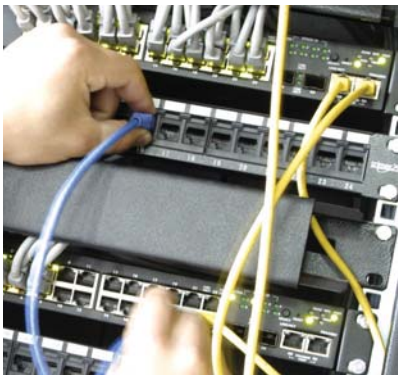
A lo largo del tiempo, las ramas de seguridad electrónica y seguridad informática han llevado caminos paralelos sin que uno afecte al otro. En la actualidad, las nuevas tecnologías en seguridad electrónica, la integración de sistemas y el IdC (Internet de las Cosas) hacen que todos los sistemas, por un medio u otro, estén conectados a una red y, en la mayoría de los casos, a internet. Esto hace que los caminos de la seguridad electrónica y la seguridad informática se crucen: si los sistemas de seguridad no son implementados por técnicos idóneos, se corren riesgos muy importantes y lo que debería ser una inversión en seguridad se transforma en una trampa para el propietario.

Podemos encontrar fallas de seguridad informática en dos grupos:

- Fallas de instalación del técnico: es la falla más común. El técnico no idóneo suele instalar los sistemas dejando, por desconocimiento, valores por defecto. Esto incluye errores básicos, como no cambiar la clave por defecto del "admin" o dejar la clave por defecto para el usuario "superuser" (muy utilizado por varias marcas de CCTV, que no puede ser eliminado pero sí es necesario cambiar su clave por defecto). Con solo un barrido de direcciones IP, o incluso búsquedas avanzadas de Google, se pueden encontrar cientos de DVR o NVR con claves por defecto e ingresar con privilegios totales al equipo. Si tomamos dimensión de esto, nos damos cuenta de que una invasión al sistema de CCTV puede transformarse en una invasión a su privacidad e incluso usarse para cometer un ilícito al saber cuándo se encuentran los dueños de casa. Este problema se potencia cuando se trata de fábricas, empresas, etc.
- Fallas del producto o su firmware: hay varias DVR o NVR, generalmente las más económicas, que no cumplen con el estándar de seguridad, lo cual hace que se pueda ingresar a ellas incluso cuando se hayan cambiado todas claves por defecto. Esto se debe principalmente a fallos en el código de acceso web y es algo que los fabricantes deben tener en cuenta a la hora de lanzar un producto.

## PROBLEMAS COMUNES

El CCTV no es el único afectado por problemas en seguridad informática: las alarmas domiciliarias presentan situaciones aún más complejas. Estos sistemas, muy usados incluso en bancos, poseen una función de configuración remota, a través de la cual, si el panel cuenta con módulo GSM, la propia central de alarma generara una conexión si se envía un SMS con nuestra IP y puerto. Esto es lo que se conoce como "conexión inversa": en lugar de ser el usuario el que realiza la conexión al panel, es el panel el que se conecta con el usuario. Las conexiones inversas pasan los firewall, los cuales por defecto controlan las conexiones entrantes pero no las salientes. En este caso, con una laptop desde la puerta de una sucursal bancaria es posible desactivar la alarma en cuestión de minutos.



Imaginemos una locación con una mala implementación de CCTV y alarma de intrusión: un delincuente podría cometer un ilícito con total impunidad. Podría ver desde el exterior si hay personas en la propiedad para luego apagar la DVR, desactivar la alarma e ingresar al lugar sin que quede registro alguno. Esto puede parecer complejo pero es en realidad muy simple, y no es necesario ningún experto en seguridad para lograrlo, por lo que si no se atiende a esta complicación, el riesgo puede ser muy alto.

No escapan a esta problemática los controles de acceso, tanto los centralizados como los del tipo standalone. Por ejemplo, en los hoteles modernos, donde para abrir la habitación se usa una tarjeta, con solo un pendrive puede abrirse cualquier habitación sin que el hotel reciba un alerta.

## HACIA UNA INTEGRACIÓN

Por medio de este resumen queremos significar que los tiempos y tecnologías cambian día a día, lo cual obliga a que los implementadores tengan más conocimientos sobre el trabajo que desarrollan y a que se actualicen constantemente. Es por esto que los cursos de certificación como el ofrecido por CASEL son muy importantes y deberían ser tratados como proyecto de ley, donde los técnicos tengan una matrícula para poder ejercer la profesión. Según mi criterio como profesional de la seguridad de la información, la mejor forma de saber cómo proteger un sistema es saber ingresar en él.

En próximos artículos, trataremos punto por punto cada falla, cómo explotarla y, por ende, cómo solucionarla para realizar implementaciones seguras. Explicaremos varios conceptos de seguridad informática para que los integradores tomen conciencia de que una mala instalación, según la nueva ley de delitos informáticos, será responsabilidad de ellos. ■