El futuro de los sistemas de seguridad

El avance de IdC en la integración

Los sistemas de seguridad tienden a dejar de lado su funcionamiento estanco para comportarse como parte de un todo. Y en ese sentido mucho tiene que ver el cada vez más frecuente uso de Internet de las Cosas. Esto, sin embargo, requiere de capacitación para evitar sistemas vulnerables.

Matías Guasco
Docente en Instituto CETIA
matias.guasco@gmail.com

Cuando nos referimos a un sistema de seguridad, primero debemos entender que un sistema es un conjunto de dispositivos que, unidos, integran una solución acorde a una necesidad planteada.

Quiero remarcar la frase "necesidad planteada" porque ésta no siempre será igual, sino que suele ser una variable en constante cambio. Esto se debe a que lo que se espera hoy de un sistema de seguridad no es lo mismo que se esperaba hace unos años atrás, haciendo que las necesidades sean distintas y cada vez más exigentes.

Desde hace varios años los sistemas de seguridad evolucionan cada vez más rápidamente. Hasta hace poco teníamos cámaras analógicas que no llegaban a ser HD y cada vez que un cliente las quería visualizar, debíamos hacer malabares con cada router para habilitar puertos, hablar con empresas proveedoras de internet, etc.

En la actualidad, existen cámaras que superaron ampliamente el espectro del HD y solo con una aplicación celular, automáticamente estamos viendo las cámaras desde cualquier lugar.

Los sistemas de intrusión, por su parte, solo podían reportar por línea telefónica y los controles de acceso estaban destinados al único fin de controlar puertas.

¿Qué pasó?: surgió la necesidad de integrar los sistemas haciéndonos la pregunta de por qué un sistema de seguridad debía componerse de partes separadas, incomunicadas entre sí, cuando todo apuntaba al mismo fin.

Luego empezamos a ver que los clientes no solo se preocupaban por la seguridad, sino que ponían el confort en la balanza. Esto derivó en que el celular sea el mando controlador de todo sistema. Hoy vemos que basta con "loguearse" a una aplicación o escanear un código QR para tener conexión directa con cualquier dispositivo, sumando la posibilidad de configurarlo y controlarlo desde cualquier parte del mundo.

Esto se logra gracias a lo que conocemos como "Cloud Computing" o, en español, "computación en la nube", que permite a las empresas ofrecer a sus clientes servidores o espacios en la nube para almacenar información y administrar productos.

La gran pregunta es: ¿hacia dónde creemos que evolucionarán los sistemas de seguridad? Difícil poder decirlo con exactitud, ya que es imposible saber si en 5 o 10 años no aparecerá una nueva tecnología que revolucionará todo. Basándonos en un análisis global, el camino lleva a la integración con dispositivos de uso comunes, a través de una tecnología que está empezando a masificarse, denominada IdC (Internet de las Cosas) o en inglés, Internet of Things (IoT).

¿QUÉ ES IDC?

Sencillamente son las mismas cosas que utilizamos día a día como luces, electrodomésticos o cámaras, pero que tienen identidad virtual propia, son más inteligentes y pueden "hablar" en la red con otro individuo, ya sea una máquina (M2M), un humano o, inclusive, con un cerebro o nube central.

Esta interconexión es posible a través de sensores, actuadores, controladores y concentradores de red que integran un sistema de estas características.

Debemos tener en cuenta que IdC representa la próxima evolución de internet, que será un enorme salto en su capacidad para reunir, analizar y distribuir datos que podemos convertir en información.

En este contexto, IdC se vuelve inmensamente importante. Los datos individuales por sí mismos no son muy útiles, pero en grandes volúmenes permiten identificar tendencias y patrones.

¿Por qué IdC es la evolución de la seguridad electrónica?: simplemente porque los sistemas de seguridad ya son parte de Internet de las Cosas, aunque no se utilizan con tal fin.

¿A qué me refiero con esto? Todo profesional del sector instaló alguna vez cámaras de CCTV, detectores de alarma o lectoras de puertas como parte de un sistema de seguridad electrónica. Al mismo tiempo, estaban también instalando sensores que recopilan información.

Todo sistema de seguridad posee entradas (cámaras, detectores, lectoras, etc.), procesamiento de datos (placa de alarma, NVR, VMS, etc.) y salidas (sirena, etc.). Ahora bien, la sirena en este caso es solo una parte de esa salida, que en IdC conocemos como "Actuadores".

La realidad es que con solo decirle al sistema que en lugar de hacer sonar una sirena encienda una luz o active un motor, ya estoy integrando ese sistema a una red de datos más grandes. Y si además aprovechamos el gran volumen de información que estos dispositivos nos bridan y podemos almacenarla (Big Data) para luego analizarla o hacer que los sistemas aprendan de ella (Machine Learning, Deep Learning), podemos entonces decir que evolucionamos a un nuevo nivel.

Ejemplo: una provincia o municipio anuncia que se instalaron 200 cámaras de seguridad, cuyo fin es vigilar el tránsito y detectar eventos de inseguridad. Viéndolo desde el lado evolutivo, también nos están diciendo que acaban de instalar 200 nuevos sensores que reportan a un procesador central y su salida está siendo utilizada para dar un aviso local a un operador. ¿Qué pasa si además de eso, podemos adicionar un actuador que utilice el sensor de movimiento de la cámara para encender o apagar las luces de la vía pública? Estaríamos ahorrando una gran cantidad de energía con una poca inversión. Y hago hincapié en poca in-

versión porque las cámaras no fueron aprobadas con ese fin, pero igual pudimos encontrarle un nuevo uso y volver el sistema más eficiente.

NUEVOS USOS

¿Qué pasaría si tomara en cuenta las cámaras instaladas en una cadena de supermercados y le adicionara, a través de analíticas de video, la recopilación de datos para que me diga en qué góndolas la gente se concentra más o qué productos son los más buscados a principio y fin de mes y así poder incluso darle a mi cliente datos precisos sobre sus ventas?

También podemos ver el mismo ejemplo en otras áreas, como oficinas, utilizando los detectores de un sistema de alarma para detectar cuando alguien se encuentra o no en el ambiente y de no estarlo poder apagar las luces o el aire acondicionado. Esto permitiría el ahorro energético optimizado.

Por otro lado, el control de acceso nos podría indicar cuando alguien ingresa a un lugar y según qué persona sea (ID), cargar un escenario de iluminación, climatización, etc., predefinido según cada gusto o necesidad.

Como vimos, los sistemas de seguridad tienen sensores que recaudan información y, a través de la tecnología conocida como Deep Learning, podemos hacer que el mismo dispositivo aprenda y tome decisiones en base a su conocimiento, como confirmar mediante analíticas inteligentes de video si existe o no un evento de incendio reportado previamente por el panel, sin la necesidad de dejarlo a consideración del operador.

De hecho, las posibilidades son casi infinitas. Teniendo en cuenta que la industria de la seguridad electrónica se está viendo afectada por la presencia masiva de productos de bajo precio, que reducen drásticamente los márgenes para los fabricantes, distribuidores e integradores, encontrar soluciones que añadan valor a una vena o instalación permiten desarrollar nuevas oportunidades de negocio.

El sector de la seguridad deberá prepararse para aprovechar la creciente demanda de dispositivos conectados a internet. No hacerlo significará marginarse del mercado y seguir batallando contra los bajos márgenes de los productos que se han "comodotizado", como los sistemas de alarma de intrusión y de videovigilancia.

RETOS

Ahora bien, no todas pueden ser buenas noticias. La realidad es que, aunque IdC y los dispositivos interconectados entre sí son el futuro del mercado de la seguridad electrónica, también conllevan grandes riesgos que, de no tomarlos en cuenta, pueden perjudicar nuestro negocio o a nuestro cliente final.

La seguridad de los dispositivos es un punto preocupante, debido a que tener dispositivos conectados a internet puede ser un riesgo si no se toman las medidas de seguridad suficientes, como autenticación de usuarios, filtrado de acceso, encriptación de datos, detección de intrusión en tiempo real, protección de dispositivos y aplicaciones, etc.

Otros de los riesgos que debemos entender es que, una vez que el dispositivo está utilizando un servidor basado en la nube, la información recolectada es tanto del usuario final como del fabricante. Esto se debe a que el usuario está utilizando los servidores del fabricante para la recolección de datos.

Un ejemplo del riesgo, de no tomar los recaudos necesarios, es el hecho de que nuestros hábitos y datos de uso de estos dispositivos conectados estén viajando por internet y puedan ser colectados por personas que, sabiendo esta importante cantidad de información, pueden conocer nuestra rutina diaria y saber cuándo estamos fuera de casa o incluso engañar a estos sistemas interfiriendo en sus comunicaciones o robando datos personales, así como también como encontrar información en patrones en respecto a cantidad de gente que asiste al lugar.

Un punto importante para minimizar los riesgos, más allá de las medidas necesarias, es la capacitación y concientización de los integradores y el usuario final que administra el sistema, evitando contraseñas fácilmente descifrables y puertos liberados al azar.

La realidad es que muchos fabricantes de seguridad electrónica están trabajando en esto y poseen ya datos encriptados y de securización de sus sistemas para llegar al futuro de los sistemas de seguridad en condiciones que no perjudiquen a nuestros clientes.

Día a día los sistemas de seguridad están más cerca de ser un sistema informático, lo cual hace que la rama de conocimiento y experiencia de un instalador debe ampliarse a cada momento, pudiendo entender hacia qué dirección ir. De no lograrlo, correrán el riesgo de no tener los conocimientos necesarios para trabajar con la próxima generación de dispositivos y sus interconexiones con el mundo actual. ■