



Documento blanco

Sistemas de Seguridad Todo en uno versus Sistemas Distribuidos (Convencionales)

Al seleccionar aparatos electrónicos, electrodomésticos y equipos para el hogar, muchos consumidores se dejan convencer por la simplicidad de los dispositivos que combinan varias funciones en una. Los equipos de oficina multi funcionales son un ejemplo perfecto. En lugar de comprar una fotocopiadora, un fax, un escáner y una impresora separados, eligen un dispositivo todo en uno que los combina en un solo equipo. En el mercado de la seguridad, este sistema está representado por la seguridad todo en uno o los sistemas auto contenidos, que combinan el panel, el teclado numérico y la sirena en una sola unidad. Estos tipos de sistemas pueden ofrecer beneficios evidentes; sin embargo, existen también algunos inconvenientes distintos. En este documento blanco, comparamos los sistemas todo en uno con el tradicional sistema de seguridad distribuido con múltiples componentes por separado.

Sección I. Ataques Físicos

La capacidad del sistema de soportar ataques físicos es posiblemente la diferencia más importante entre los sistemas todo en uno y los distribuidos. “Es posible que intrusos completamente inexpertos retiren físicamente de la pared estos sistemas y los vuelvan añicos”, según Daniel McKimm, fundador y propietario de ProTech Security en North Canton, Ohio. Antes del lanzamiento de ProTech hace 30 años, McKimm estaba en la policía, lo cual le dio experiencia práctica en la respuesta a alarmas en casos de robos e intrusión.

Con todos los elementos en un paquete, dice que los ataques de fuerza bruta son demasiado fáciles de perpetrar. Estos tipos de ataques se facilitan porque un intruso es atraído a él por el ruido de la sirena o conoce la ubicación aproximada del sistema. Los intrusos, capaces de reconocer el tipo de sistema de seguridad, podrán identificarlo como un todo en uno fácil de atacar.

Al menos un fabricante ha compensado esa falla con un poco de programación. Cuando se detona una alarma, hay por lo general un retraso de ingreso antes de que se envíe la señal de alarma a la Estación Central. En algunos sistemas, se transmite una señal de alarma tentativa inmediatamente a la Estación Central y allí se deja. Cuando el usuario ingresa el código para desarmar el sistema, este envía una cancelación a la Estación Central. Si se ataca y deshabilita el sistema durante la demora del ingreso, no se envía señal de cancelación, y se activa la señal de alarma tentativa. La mayoría de los sistemas todo en uno carecen de dicha función.

Los sistemas distribuidos son de por sí más resistentes a los ataques físicos. Los componentes periféricos visibles y de fácil acceso podrían ser atacados todos, pero el panel está por lo general oculto y protegido. Si se detona el sistema o si se ataca alguno de los elementos periféricos, el panel conserva la capacidad de transmitir la señal de alarma a la Estación Central.

Sección II. Facilidad de Instalación y Operación

La programación de los sistemas todo en uno solía ser la opción más simple para el instalador durante la configuración inicial, debido a la ausencia de numerosos dispositivos para interconectar (panel a sensores, sirenas, etc), que permitían "conectar y usar". Los instaladores apreciaban esta característica, porque les permitía hacer más instalaciones durante el día. Esta no es la gran ventaja que solía ser. El creciente predominio de sistemas inalámbricos, como el XTL™ de DMP permiten una instalación muy rápida. Un sistema inalámbrico distribuido puede instalarse en menos de una hora, debido a características que ahorran tiempo, como Walk Test y Survey LED, que permiten a un solo instalador colocar y configurar con rapidez los componentes del sistema. La simplicidad que ofrece un sistema XTL es igual o mejor que la mayoría de los sistemas todo en uno.

Una vez instalado, la operación básica es comparable para ambos tipos de sistemas. Actividades rutinarias, como el armado y el desarmado son muy similares. Los sistemas distribuidos tienen algunas opciones adicionales de programación para el consumidor, y por ende, el potencial añadido de ajustar el sistema para acomodarse a las necesidades del usuario final. Sin embargo, estas pueden limitarse por la compañía de alarmas para crear un sistema en extremo fácil de vender e instalar.

Al igual que con el dispositivo de oficina multifuncional, el sistema de seguridad todo en uno implica que hay un solo dispositivo. Puede haber menos cosas que fallen. Pero, cuando algo va mal, por lo general requiere el reemplazo del sistema **completo**.

Con un sistema distribuido, si llegara a fallar un componente individual, puede reemplazarse con facilidad y costo efectivo. No es necesario asumir el mayor gasto asociado a la compra de un sistema completamente nuevo. La alternativa distribuida ofrece también la oportunidad a los consumidores de actualizar los componentes en forma selectiva o de añadir nuevos dispositivos y funciones a su sistema.

Sección III. Costo

El precio siempre es un factor de peso para los consumidores. En el caso de los todo en uno, se esperaría que la simplicidad del diseño y el reducido número de componentes los haría más económicos. De hecho, la ventaja es poca o ninguna al comprar estos sistemas.

Para los distribuidores de sistemas, los todo en uno los ponen en posible desventaja en términos de ganancias. La incapacidad de modificar o expandir estos sistemas hace imposible incorporar complementos o actualizaciones que el consumidor pueda querer. Además, estas actualizaciones ofrecen oportunidades adicionales de generación de ingresos para el distribuidor.

Las expansiones, actualizaciones y complementos fácilmente incorporables en sistemas convencionales distribuidos, como servicios móviles y monitoreo de video, crean muchas oportunidades potenciales de generación de ingresos mensuales recurrentes (RMR).

Sección IV. Resumen

Los sistemas todo en uno son una forma simple y de bajo costo a la seguridad y un buen ejemplo de recibir aquello por lo que se paga. Su simplicidad los limita para personalizarse o actualizarse. Son lo que son. Los sistemas distribuidos son a la vez personalizables y actualizables. A medida que nuevas características y funciones entran al mercado, pueden añadirseles. Las actualizaciones de software pueden aplicarse también para añadir prestaciones y mejorar la operación. Lo más importante, la vulnerabilidad a los ataques de los sistemas todo en uno implica que no son capaces de ofrecer el mismo grado de protección de un sistema distribuido.

La decisión es en última instancia de los consumidores, pero distribuidores como Dan McKimm, que desean dotar a sus clientes de sistemas de seguridad sólidos y confiables, recomiendan los sistemas distribuidos en forma consistente.

	800-641-4282	INTRUSION • FIRE • ACCESS • NETWORKS
	www.dmp.com	2500 North Partnership Boulevard
	Designed, Engineered and Assembled in U.S.A.	Springfield, Missouri 65803-8877

