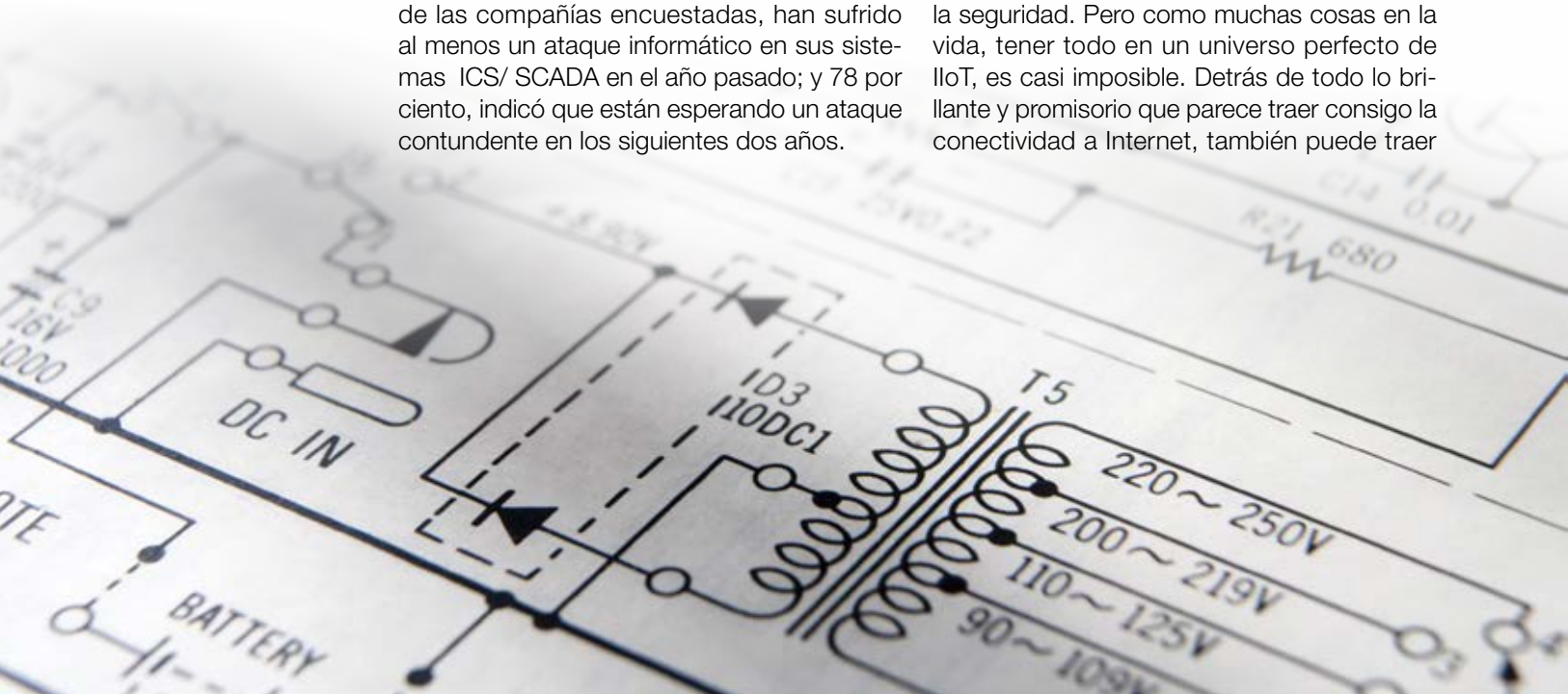
Fuente: Johnnie Konstantas, Director, Security Solutions
Marketing & Business Development de Gigamon.

Los Crecientes Riesgos en Ambientes ICS y SCADA

La conectividad a Internet no sólo puede traer beneficios sino vulnerabilidades para las empresas del sector industrial

De acuerdo con el reporte 2015 Dell Security Annual Threat Report, a nivel mundial, los ataques a sistemas SCADA se han incrementado de 91 mil 676 incidentes en enero de 2012, a 163 mil 228 en enero de 2013, llegando en 2014 a la cifra de 675 mil 186. Como lo menciona el estudio del Instituto Ponemon en su trabajo Critical Infrastructure: Security Preparedness and Maturity, el 67 por ciento de las compañías encuestadas, han sufrido al menos un ataque informático en sus sistemas ICS/ SCADA en el año pasado; y 78 por ciento, indicó que están esperando un ataque contundente en los siguientes dos años.

Entonces, ¿qué es lo que está causando este incremento?, situaciones como mayores sistemas de control conectados a Internet. Para las compañías que buscan hacer más con menos y ser más competitivas, sería difícil ignorar todo lo que promete el Internet de las cosas Industrial (IIoT): mejorar la eficiencia, incrementar la productividad, bajar los costos, mejorar la automatización e inclusive, mejorar la seguridad. Pero como muchas cosas en la vida, tener todo en un universo perfecto de IIoT, es casi imposible. Detrás de todo lo brillante y promisorio que parece traer consigo la conectividad a Internet, también puede traer



Una administración centralizada puede ser difícil cuando los sistemas de monitoreo designados son obsoletos y además, están aislados.

consigo vulnerabilidades a un mundo cada vez más conectado entre sí.

Viejos sistemas, nuevas amenazas

En un sentido, los ambientes de control industrial son como un auto viejo: frágiles, lentos y poco adaptables a cambios o actualizaciones. El tráfico de red en este tipo de sistemas es mucho más lento en comparación con una red IT estándar y sobre todo, la tecnología que los compone tiene más de 10 años y no fue desarrollada pensada para conectarse a Internet. Estos sistemas están físicamente aislados y las medidas de seguridad giraban alrededor de políticas de acceso, tratamiento y aislamiento del aire, y la prevención de la exposición al exterior. Al igual que el auto viejo, la introducción de algo nuevo y diferente tiene el potencial de causar estragos rápidamente.

Por definición, un sistema de aire industrial de este tipo no está conectado a Internet o a otro tipo de red sin seguridad. Sin duda, expertos en cibercrimen recomendarán mantener a dichos sistemas fuera de cualquier conexión a Internet, pero existe un debate considerablemente importante si esto es posible en una era como la actual. En serio, ¿los negocios y sus sistemas de control de redes, deben permanecer separados?

Inclusive los sistemas de aire son vulnerables a ser infectados con un simple dispositivo USB, ya sea infectado por descuido o por un miembro malicioso que así lo planeó. Los hackers utilizaron lo que se conoce como spear-phishing para infiltrarse en una acerera alemana, previniendo que un alto horno se apagara. Google dorking permitió a presun-

El sector industrial está repleto de instalaciones geográficamente dispersas y en muchas ocasiones a grandes distancias unas de otras, de la cual, la mayoría carecen de recursos IT/OT dedicados

Los ambientes de control industrial son como un auto viejo: frágiles, lentos y poco adaptables a cambios o actualizaciones

tos piratas informáticos iraníes entrar al sistema de control de la presa de Nueva York y afectar una válvula de una exclusa, y que ésta no fuera desconectada para su mantenimiento, lo que podría haber significado la apertura de compuertas y una inundación.

Sistemas de aire o no, es un tema el considerar que los perímetros pueden ser penetrados y establecer así defensas adicionales basadas en estos hechos cada vez más recurrentes.

El sector industrial está repleto de instalaciones geográficamente dispersas y en muchas ocasiones a grandes distancias unas de otras, de la cual, la mayoría carecen de recursos IT/OT dedicados, así como de experiencia en seguridad o peor aún, sin instalaciones eléctricas adecuadas, con accesos bloqueados y sin un alma a kilómetros a la redonda. Lo que dibuja una crisis de enorme magnitud si no hay personal durante una emergencia.

Desafortunadamente, una administración centralizada puede ser difícil cuando los sistemas de monitoreo designados son obsoletos y además, están aislados. Las compañías pueden armar a cada subestación ya sea que hablemos de agua o electricidad, de herramientas de detección dedicadas, lo que puede sonar costoso si se tienen 50, 100 o 1,000 instalaciones remotas que monitorear. Y, realmente desde un punto de vista de costos y tráfico de red, si sólo se tienen 10 megas de tráfico, no hay necesidad de contar con sistemas con capacidad de procesar Gigabytes enteros. No es rentable.

La solución es redirigir el tráfico de regreso a una central de procesamiento para su inspección.

NERC CIP proporciona un marco de controles de seguridad que está abierto a interpretación y a la aplicación de diversas metodologías. Como ejemplo, una empresa puede satisfacer su necesidad de un control mediante la supervisión de paquetes de datos, otra a través de la correlación de los datos de registro, y otra por simple reducción de la exposición a través de espacios de aire y la segmentación.

Para empresas interesadas en ampliar las capacidades de sus herramientas de seguridad informática en ambientes centralizados de producción para sus subestaciones, implementar un transporte de red de tipo out-of-band para ganar visibilidad tanto en paquetes de datos y tráfico syslog, puede ser benéfico. Una forma de lograr esto mientras se mantiene la segmentación de la red ICS es insertar un TAP de red pasivo entre un servidor syslog local y reportes en los endpoints, aislando el tráfico syslog vía un filtro IP y llevándolo en un túnel de regreso vía una red out-of-band a una ubicación central de monitoreo – Como lo dijo el Chief Hacker Rob Joyce de la NSA, TAPS en una red out-of-band son una pesadilla para hackear.

La centralización es una forma de mantener “sin aire” mientras se habilita un monitoreo en una vía que no pueda ser usado como una ruta para atacar y sea en sí, una forma para ganar inteligencia en como un sistema puede ser identificado, así como detectar y responder a una serie de ataques, de manera inmediata y remota.

Para las compañías que buscan hacer más con menos y ser más competitivas, sería difícil ignorar todo lo que promete el Internet de las cosas Industrial (IIoT).