Combinación de software de monitoreo y firewall industrial: el sistema inmune para las redes de producción

Hernán López
Phoenix Contact
hlopez@phoenixcontact.com
www.phoenixcontact.com

El nivel de seguridad de las redes de producción se puede incrementar rápida y sencillamente combinando software para monitoreo de la red y dispositivos de seguridad industrial. Esta combinación crea un nuevo estándar de seguridad en aplicaciones industriales e infraestructuras de redes críticas

La seguridad de acceso es un tema de creciente importancia en tiempos de Industria 4.0. Por eso, *Security Matters* y *Phoenix Contact* han reunido su experiencia en una sociedad tecnológica. El nivel de seguridad en las redes de producción puede mejorar de forma significativa y sencilla combinando software para monitorear la red con aplicaciones de seguridad industrial. La solución mancomunada configura nuevos estándares, tanto para la fabricación, como para infraestructuras críticas.

Hoy en día, más y más máquinas y sistemas intercambian información entre sí local y globalmente. La cantidad creciente de comunicaciones conduce a que se incrementen los requisitos de seguridad en la red. Los operadores deben, entonces, preguntarse a sí mismos qué información debe transmitirse, a qué máquina y cuándo. Sobre todo cuando se trata de sistemas de producción que se han expandido, o se han integrado completamente en la red tras cierta cantidad

de años. La respuesta a esta pregunta resulta ser difícil y consume demasiado tiempo. *Security Matters* y *Phoenix Contact* han conformado una sociedad tecnológica para proveer a los usuarios un soporte eficiente, integrado y profesional.

Por una parte, *Security Matters* fue fundada en la ciudad alemana de Eindhoven en 2009, es una compañía innovadora, activa en el campo de seguridad TI y está especializada en la detección de anomalías en las redes industriales. *Silent Defense* es un componente esencial de su portafolio de productos. Esta plataforma para monitoreo de red está disponible en el mercado desde 2013.

Por otra parte, como una de las líderes e innovadoras en el mercado en ingeniería eléctrica, electrónica y automatización, *Phoenix Contact* opera, entre otras cosas, su propio centro de excelencia para ciberseguridad localizado en Berlín. Respaldada por su experiencia en la temática, la empresa provee productos a medida y soluciones de red que satisfacen requisitos industriales específicos. Los routers del rango de productos *FL mGuard* son el núcleo de la línea de producto de protección (ver figura 1).

Figura 1. Los dispositivos de protección FL mGuard se utilizan también en entornos de producción

Identificación simultánea de errores y diagnóstico de ataques

En 2016, *Security Matters* y *Phoenix Contact* decidieron combinar sus productos de protección, generando así un valor añadido para los usuarios. Para proveer una solución para monitorear la red, *Silent Defense* da soporte a los usuarios con análisis y fortalecimiento de su red. La capacidad de visualizar la red en tiempo real, llevar a cabo tests definidos por el usuario y monitorear de forma automática la comunicación de red son solo algunas de las funciones que distinguen este sistema de monitoreo. *Silent Defense* se puede usar para diagnosticar ciberataques y también para identificar errores operacionales (ver figura 2).

Los routers industriales *FL mGuard* de *Phoenix Contact* están diseñados para operar sin ventiladores y brindar protección y rendimiento confiables en una carcasa metálica compacta que se puede montar en riel DIN. Además de proveer un

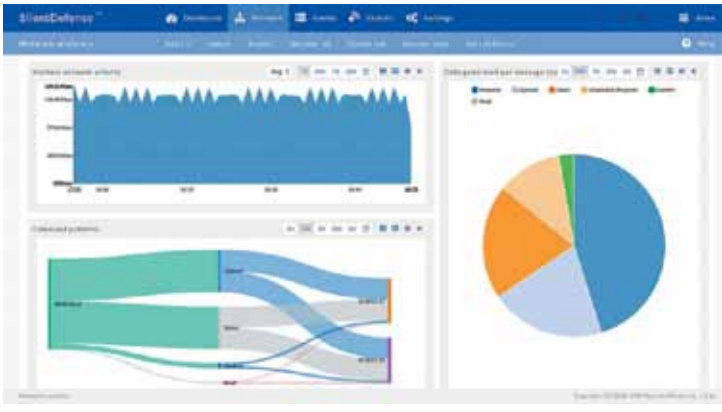

Figura 2. La visualización en tiempo real de la comunicación de red en el tablero de análisis de la red

túnelVPN seguro, los dispositivos son capaces de varias funciones firewall específicas de la industria. Esto incluye un firewall de usuario, un firewall condicional para activar reglas de firewalls específicas, así como inspección para la investigación a fondo de cualquier paquete de datos transmitido a través de OPC clásico o Modbus/TCP.

Esto habilita que el concepto de defensa-en-profundidad, basado en los estándares internacionales ISA 99 e IEC 62443, se pueda implementar profesionalmente en las aplicaciones. Gracias al concepto de seguridad descentralizada, las plantas productivas quedan protegidas de forma segura contra el sabotaje y los malos funcionamientos asociados en un proceso de producción (ver figura 3).

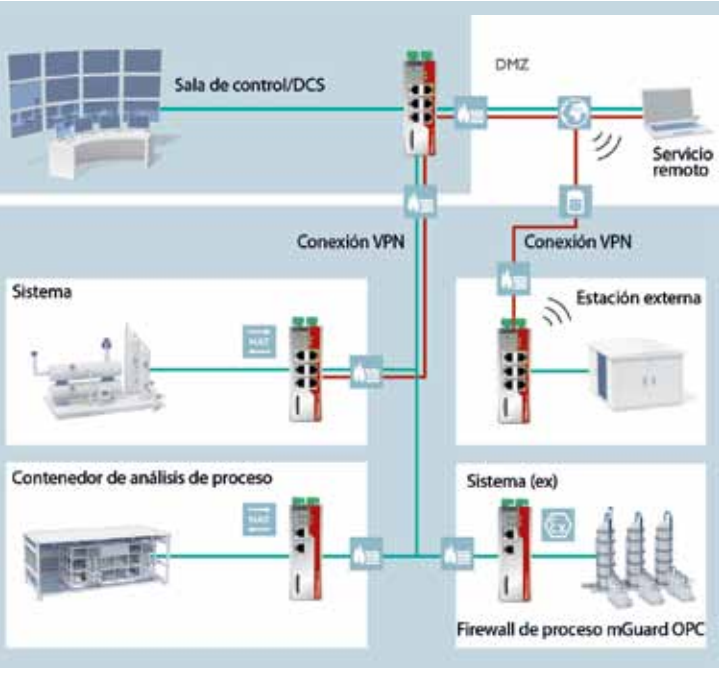

Figura 3. Las plantas de producción se pueden proteger con routers de seguridad de forma descentralizada

Detección inmediata de cambios menores en la red

Cuando se combinan en la práctica *Silent Defense* y *FL mGuard*, hay un beneficio adicional para los usuarios. Por ejemplo, *Security Consulting* de *Phoenix Contact* utiliza el software para monitorear la red a fin de analizar en detalle el intercambio de datos en redes industriales complejas. El operador del sistema tiene de esta forma un panorama exacto sobre qué participantes en la red de producción están enviando qué contenido a qué otros participantes, así como cuándo y cómo se envía. La comunicación no autorizada es visible y puede ser apagada. Un ciberataque espectacular no representa el mayor riesgo para muchas compañías, sino los innumerables pequeños cambios autoinducidos en el sistema que se van agregando a lo largo del tiempo e implican un riesgo mayor para la disponibilidad de la red de fabricación.

Los ejemplos abundan. Un controlador, por ejemplo, se intercambia por un dispositivo de reemplazo que está programado de alguna forma diferente al PLC original. Durante una actualización del sistema, el proveedor del producto utiliza un protocolo para tiempo de sincronización más débil que el que se usaba antes. Los nuevos dispositivos agregados intentan alcanzar un servidor externo utilizando puertos TCP desconocidos. Establecer la conexión con un servidor no disponible inunda la red de producción con datos. La lista de ejemplos es interminable.

Transmisión directa de datos de configuración registrados en el firewall

Después de que *Silent Defense* analiza las relaciones comunicacionales en la red de producción y se apagan las conexiones no deseadas, el segundo paso importante que sigue es proteger la red utilizando firewalls de la gama *Fl mGuard*. El aspecto

innovador de esta solución es la interacción de hardware y software insitu para el usuario. Las relaciones comunicacionales que fueron identificadas como correctas se transmiten directamente como registros de datos de configuración de firewall en el dispositivo de protección instalado en un sistema descentralizado. Esto hace que definir las reglas de firewall sea mucho más fácil y evita reglas de firewall descuidadamente mantenidas o defectuosas. Los empleados responsables en particular prefieren dejar que los paquetes de datos no identificados o desconocidos pasen por el firewall en las redes de producción que son complejas y han crecido a lo largo de los años, antes que correr el riesgo de que el sistema quizá no fabrique más. Esta práctica, sin embargo, implica un riesgo de protección grande e innecesario. Con la solución descripta en esta nota, los requisitos de usuario se implementan ahora de forma profesional, garantizando una elevada disponibilidad del sistema y a la vez, alta protección de la red de producción contra acceso no autorizado y acciones dañinas.

Ajuste dinámico de mediciones de seguridad

Los proyectos piloto iniciales están dando el próximo paso innovador. Si *Silent Defense* se instala de forma permanente en el lugar del usuario, este tiene la opción de ajustar de forma dinámica las medidas de protección. Si, por ejemplo, los hackers están utilizando un link de comunicación ya existente para un ataque, el firewall *FL mGuard* puede cambiar la configuración esencialmente en tiempo real siguiendo la aprobación de un empleado responsable o *Silent Defense* puede ser usado para hacer esto automáticamente. De esta manera, las conexiones no deseadas se pueden detener rápida y fácilmente, a la vez que una transmisión de datos deseada va a permitirse específicamente después.

La sociedad tecnológica entre *Security Matters* y *Phoenix Contact*, por lo tanto, ha conducido a un salto innovador en la protección industrial y está configurando nuevos estándares en el área de calidad. El software *Silent Defense* y el router

Familia de productos de Ethernet industrial, de *Phoenix Contact*

FL mGuard forman una simbiosis y crean un claro beneficio para el usuario. Por lo tanto, es irrelevante si se utiliza en una aplicación de infraestructura crítica o en una aplicación en uno de los muchos sectores industriales.

Funciones para equipos de seguridad

El nuevo firmware 8.4 para dispositivos de protección en la gama de productos de *FL mGuard* expande el rango de utilidades de estos dispositivos, entre otras cosas, con el Inspector Modbus TCP y el firewall basado en nombres DNS. El Inspector Modbus TCP, una inspección de paquete profunda para Modbus/TCP, se puede usar para proveer protección detallada para conexiones que usan el estándar industrial ampliamente adoptado. Los derechos de acceso se pueden configurar tanto a nivel de puertos y direcciones IP como para códigos de función y registros utilizados dentro del protocolo Modbus. Por ejemplo, el usuario puede definir qué participantes Modbus están habilitados para solo leer valores y cuáles para sobreescribirlos. Más aún, los derechos de acceso se pueden definir de forma precisa de acuerdo con el registro.

El firewall basado en nombres DNS permite crear derechos de acceso a firewall que incluso estén basados en direcciones IP y nombres DNS. Esto hace que las creaciones de configuraciones sean más sencillas en escenarios en donde las direcciones IP frecuentemente cambian. La nueva versión de firmware 8.4 está lista para descargar en el área de descarga de su respectiva página de producto. ❖