Abril 2019 / n.º 510 Automática e Instrumentación

Completo dispositivo para la seguridad industrial

La ciberseguridad con groov

Existe una preocupación creciente acerca de la ciberseguridad industrial en la automatización y el intercambio de datos. Tenemos que asegurarnos que sólo el software y los usuarios autorizados pueden realmente acceder a la red y al sistema de control. Opto22 ha diseñado groov, un poderoso y completo dispositivo para conseguirlo.

Los sistemas y las arquitecturas actuales son complejos, caros y difíciles de mantener, lo que hace todavía más interesante ir a soluciones sencillas, seguras y con mayor rendimiento.

Otra preocupación añadida es la dependencia del sistema operativo Microsoft Windows que actualmente presenta tres problemas importantes: mantenimiento del propio sistema operativo y las aplicaciones; fallos de seguridad y los riesgos asociados con la ciberseguridad y un futuro inquietante del producto según la propia visión de Microsoft. Por eso, hace cinco años, Opto22 apostó fuerte por el uso de Linux, pero añadiendo una capa protectora de software que evita la posibilidad o necesidad de llegar al sistema operativo o de requerir un "administrador/gurú" de Linux. Toda la funcionalidad de groov, sea configurable o programable, se hace desde cualquier navegador web, mediante una conexión segura https (web port 443).

En el producto groov, simplemente no existe "puerta de atrás" o "acceso desde línea de comandos", ni la posibilidad de enviarle archivos, actualizaciones, programas instalables o código web, que son las maneras más habituales de introducir virus, gusanos y troyanos con el fin de tomar el control o destruir un sistema informático.

Regla #1: Separación física entre la red corporativa (I.T.) y la red de producción (O.T)

Aunque algunas empresas siguen confiando en mantener una red única y una programación compleja de VLANs, switches y routers en su infraestructura de red, aquellos que han sufrido algún ataque informático (externo o interno) ya han aprendido a separar y aislar completamente su red de control de producción de su red corporativa informática, la cual sigue bajo control de sus especialistas de seguridad informática.

■ Groov Box es un servidor industrial conectable a tres redes independientes separadas.

Pero con la solución aparece otro problema: lógicamente los administradores de la red informática se resisten a la conexión de equipos industriales en su red, pues saben perfectamente que éstos carecen generalmente de seguridad informática. Entonces, ¿cómo se resuelve el rompecabezas de mover datos entre los dos entornos?, una necesidad cada vez más común.

Datos como órdenes de producción, códigos, recetas, etc., que existen en bases de datos en la red corporativa, son necesarios en autómatas y dispositivos industriales en la red de producción. Similarmente, datos de producción, históricos, archivos y cualquier dato necesario para un análisis avanzado de negocio en la red industrial, tiene que estar accesible por la red I.T. y las aplicaciones informáticas.

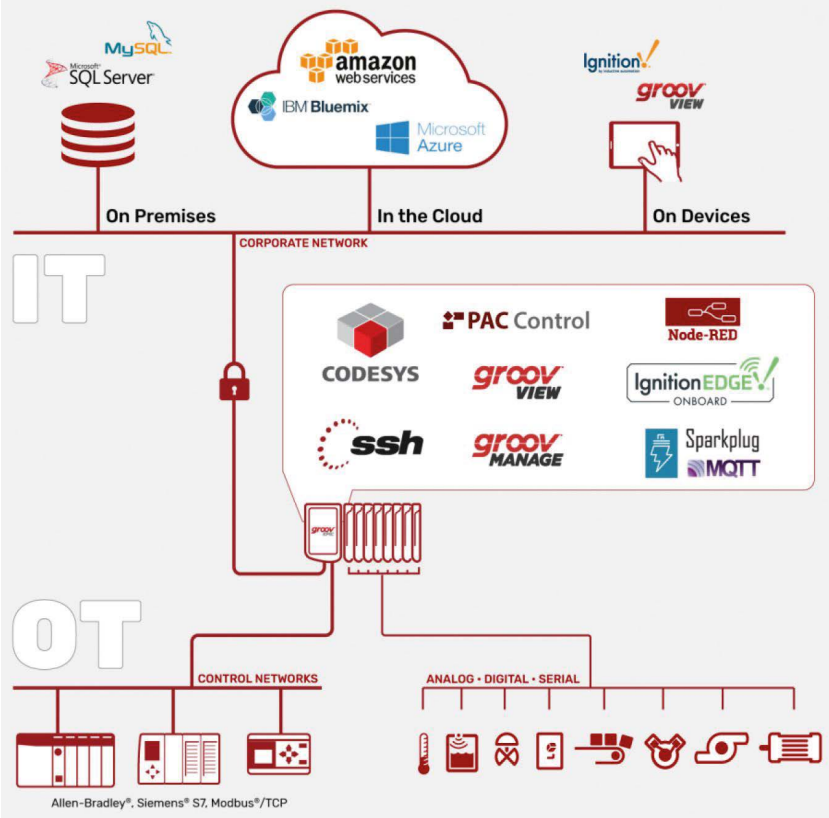
Hay fábricas que solamente permite mover datos mediante una memoria USB, sin ser consciente de que es la fuente más común de transferir virus. Pero lo habitual es tener un ordenador con dos tarjetas de red actuando como un "bridge" casero, basado en Microsoft Windows y en productos y software "middleware" cada vez más difícil y costosos de mantener.

Como alternativa, Opto22 ofrece el producto groov. ¿Pero qué es groov?

Es un sistema industrial, sencillo y compacto para aplicaciones Edge, con conectividad con PLCs y con Internet, Node RED, visualización móvil y Control Industrial. Groov Box es un servidor industrial conectable a tres redes independientes separadas, no utiliza MS-Windows y está diseñado para instalaciones industriales (temperatura, humedad, polvo, etc.)

Hay diversas maneras en las que groov nos ayuda a mantener los sistemas seguros:

- Encriptación: Los productos groov utilizan la misma capa de protocolo de seguridad que los bancos. Veremos los "https" cuando iniciamos sesión. Todas las comunicaciones entre un cliente y groov están cifradas mediante RSA, claves simétricas/asimétricas y claves de sesión.
- Autenticación: Controla el acceso al software a través de la autenticación del usuario. Los certificados SSL pueden ser de formato PEM, PKCS12 o CSR y ser auto generados, autofirmados o firmados públicamente (CA).
- Sistemas separados: Las interfases de red independientes mantienen la red de control separada de la red del PC. Groov incorpora dos interfases de red Ethernet que nunca pueden comunicarse entre ellas.
- Cortafuegos integrado, configurable para varios grados de complejidad y alcance.
- Contenidos del HMI: Podemos determinar lo que cada usuario puede ver y hacer en Groov View. Construimos páginas separadas y asignamos usuarios a grupos de usuarios.
- Webserver integrado: Con las herramientas necesarias incluidas, cualquier ingeniero puede crear páginas webs seguras para la monitorización o el control. Por motivos de seguridad, no se permite el uso de herramientas externas de diseño web.
- Acceso vía Restful API segura: groov genera un repositorio seguro de los datos accesibles desde la red industrial. Las aplicaciones y herramientas informáticas nunca pueden llegar a la red industrial, pero sí pueden acceder a los datos en el repositorio de groov mediante comandos GET / POST y llamadas REST, usando la interfaz segura https y con certificados SSL.



■ Groov actúa como servidor OPC-UA en la red industrial. Incluye todas las tecnologías, protocolos y herramientas para garantizar la conectividad con cualquier dispositivo o sistema actual.

Cómo groov lo simplifica todo-groov: Actúa como servidor OPC-UA en la red industrial. Incluye todas las tecnologías, protocolos y herramientas para garantizar la conectividad con cualquier dispositivo o sistema actual. Groov tiene preinstalados drivers de comunicación directa para autómatas Allen-Bradley, Opto22, Schneider (Modbus) y Siemens, así como para la conexión a cualquier otro servidor OPC-UA.

- groov: Actúa como cliente en la red informática. Incluye todas las tecnologías y herramientas para garantizar la seguridad y conectividad en el entorno I.T.
- groov: Aísla totalmente ambas redes y no permite tráfico entre ellas. Los datos se mantienen en un espejo común entre ambos "mundos".
- groov: Revoluciona la arquitectura de comunicaciones industriales. Incluye todas las tecnologías y herramientas para sustituir el modelo "polling" por "publicación/suscripción".
- groov: Elimina completamente la dependencia de Microsoft Windows, software adicional y licencias.
- groov: Garantía total de un solo fabricante: Hardware, sistema operativo, software, herramientas, integración de software de terceros, e interoperabilidad en un dispositivo industrial único.

José Bielza (Automática e Instrumentación)