Estrategias para atender la ciberseguridad

Siemens
www.siemens.com.ar

Internet se presenta como un gran acelerador de procesos de negocio y ha revolucionado las operaciones en todo el mundo.

Los cambios resultantes en la industria de producción también se pueden describir como "revolución": algunos se animan a hablar de "cuarta revolución industrial". La Industria 4.0 afecta todos los aspectos de la cadena de valor industrial, incluyendo comunicación industrial y seguridad.

Más todavía, ahora la seguridad se regula con leyes que atienden infraestructuras críticas particulares. Como ejemplos, se puede mencionar el IT Security Act, en Alemania; la certificación ANSSI, en Francia, y NERC CIP, en Estados Unidos. Después de todo, la comunicación abierta y el crecimiento de la red en los sistemas de producción involucran no solo grandes oportunidades, también grandes riesgos. Para proveer una planta industrial de seguridad integral contra posibles ataques, se deben tomar medidas apropiadas. La empresa *Siemens* tiene herramientas para realizar la tarea.

Después de todo, la comunicación abierta y el crecimiento de la red en los sistemas de producción involucran no solo grandes oportunidades, también grandes riesgos.

Defensa en profundidad

Con la defensa en profundidad, la empresa *Siemens* busca ofrecer un concepto multifacético que otorgue protección al sistema. El concepto está

basado en la seguridad de planta, la seguridad de red y la integridad del sistema, de acuerdo a las recomendaciones de ISA 99/IEC 62443, la normativa de seguridad más importante en la automatización industrial.

Seguridad de planta

La seguridad de planta se vale de una cantidad de métodos diferentes para prevenir que personas no autorizadas ganen acceso físico a componentes críticos. Esto comienza con un acceso convencional y se extiende a la construcción de áreas sensibles a las que se accede solamente por medio de tarjetas de ingreso.

Los servicios de seguridad de planta incluyen servicios de consultoría, paquetes de

Nro.	Amenaza	Explicación
1	Infección de malware a través de Internet o de la intranet	Los componentes IT estándar, tales como los sistemas operativos, servidores de aplicación y bases de datos en general contienen desperfectos y puntos débiles que los atacantes pueden aprovechar.
2	Introducción de malware a través de hardware externo o medio removible	Los medios removibles como los pendrives son objeto de introducción de infección de malware. El uso de notebooks con data externa y software de mantenimiento que podría haber sido usada en otras compañías implica un gran peligro.
3	Ingeniería social	La ingeniería social es un método para ganar acceso no autorizado a información o sistemas IT casi sin llevar a cabo procedimientos técnicos, puesto que se puede aprovechar de actitudes humanas como la colaboración, la confianza, el miedo o el respecto a la autoridad. Un ejemplo de esto son los sitios de Internet que infectan el sistema de la víctima con malware.
4	Error humano y sabotaje	El personal que trabaja en ICS ocupa un lugar especial cuando se trata de seguridad. Esto se aplica tanto a personal propio como externo involucrado en tareas de mantenimiento o construcción. La seguridad nunca puede estar garantizada solamente por medidas técnicas; también se requieren regulaciones organizacionales.
5	Intrusión a través de acceso por mantenimiento remoto	El acceso desde el exterior al ICS por mantenimiento es una práctica muy extendida. Y cuando se puede ingresar a un sistema por mantenimiento, otros quedan más accesibles. A menudo, la falta de autentificación o autorización, o jerarquías de red planas, son las causas de los incidentes de ciberseguridad.
6	Componentes de control conectados a Internet	Los componentes inseguros de ICS tales como PLC a menudo se conectan directamente a Internet, en contra de las recomendaciones del fabricante, sin las medidas de seguridad correspondientes.
7	Malfuncionamientos técnicos y de fuerza mayor	Siempre son posibles las fallas a causa de influencias ambientales extremas o defectos técnicos. Aquí, el riesgo potencial de daño solo se puede minimizar.
8	Comprometer teléfonos inteligentes en el entorno de producción	La posibilidad de ver y modificar parámentros de producción y operación en un teléfono inteligente o una táblet es una característica que se promociona y utiliza cada vez más en los componentes ICS. Esto significa un caso especial de acceso remoto por mantenimiento, por lo que el uso de teléfonos inteligentes implica un punto de ataque adicional.
9	Introducción de componentes extra net o en la nube	La tendencia generalizada de externalizar los componentes IT está llegando a los ICS. Por ejemplo, los proveedores de soluciones de mantenimiento remoto colocan los sistemas del cliente en la nube, pero esto lleva a que los dueños del sistema solo tengan control limitado sobre la seguridad de los componentes.
10	Ataques (D)DoS	Los ataques de denegación de servicio (distribuido) (DDoS) se pueden usar para interrumpir conexiones de red y recursos requeridos y causar el colapso en los sistemas, por ejemplo, para quebrantar la funcionalidad de un ICS.

Fuente. Industrial Control System Security: Top 10 Threats and Countermeasures v1.1
Publication date: March 26, 2014
Nota. Esta lista de amenazas fue elaborada junto con BSI (Oficina Federal Alemana para Seguridad de la Información)

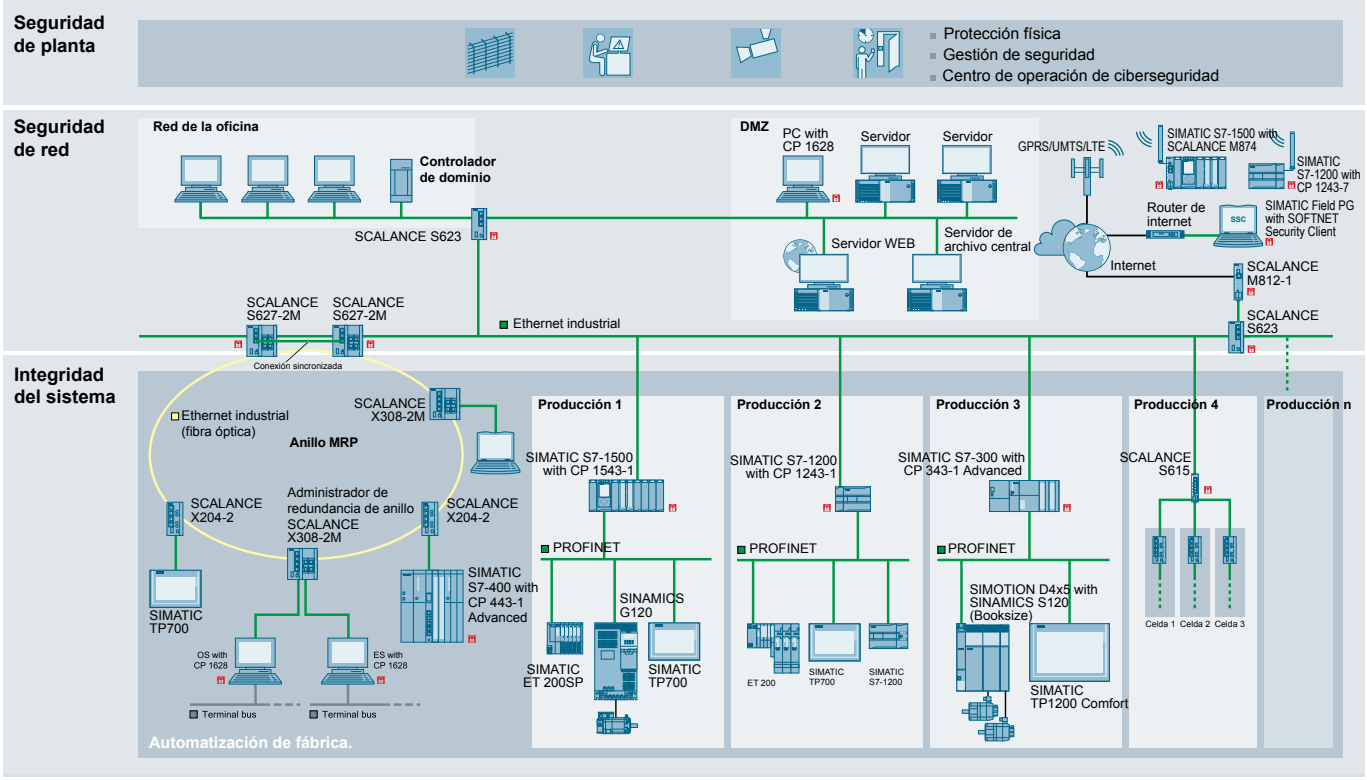
implementación y servicios de seguridad administrada, para lograr una protección holística de la planta y a largo plazo.

Atender la seguridad implica analizar y atender el estado de la planta respecto de la tecnología, la arquitectura de red y el personal.

Las instalaciones productivas están constantemente a merced de las amenazas. Dispositivos infectados, personal no autorizado, acceso no autorizado a través de red y la Internet, requieren tomar medidas.

Atender la seguridad implica analizar y atender el estado de la planta respecto de la tecnología, la arquitectura de red y el personal. Los paquetes de implementación van desde brindar apoyo para la planificación de red y la instalación de sistemas de detección de ataques hasta la integración de medidas de fortalecimiento del sistema.

Con actualizaciones continuas y un monitoreo comprehensivo, los servicios de seguridad pueden asegurar que se ajustarán rápidamente a las amenazas, que son cambiantes; y que serán transparentes a la hora de mostrar el estado de seguridad de la planta, gracias al monitoreo en todo el mundo y alertas en tiempo real.



Defensa en profundidad de *Siemens*

La clave: seguridad de red

La seguridad de red significa proteger las redes de automatización de accesos no autorizados. Esto incluye monitorear todas las interfaces entre las redes de oficina y planta, o el acceso a Internet por mantenimiento remoto.

La segmentación de la red de planta en celdas de automatización protegidas individualmente minimiza los riesgos e incrementa la seguridad.

Se puede atender a través de firewalls y, si aplica, estableciendo una zona desmilitarizada (DMZ) segura y protegida. La DMZ se usa para hacer que pueda haber data disponible a otras redes pero sin otorgar acceso directo a la red de automatización en sí misma.

La segmentación asegurada de la red de planta en celdas de automatización protegidas individualmente minimiza los riesgos e incrementa la seguridad.

La división por celdas y la asignación de dispositivos se basan en los requisitos de protección y comunicación.

La transmisión de datos se puede encriptar con un VPN, y así queda protegida contra el espionaje y la manipulación. Las estaciones de comunicación se están autentificadas de forma segura. Las redes de automatización, los sistemas de automatización y la comunicación industrial se pueden asegurar con componentes *Scalance* de "seguridad integrada", tales como los módulos de seguridad *Scalance S*, *Scalance M*, routers inalámbricos móviles y PC de seguridad para *Simatic*.

La integridad del sistema también implica autentificación de usuarios, autorizaciones de acceso o para realizar cambios, y fortalecimiento del sistema; en otras palabras, la robustez de los componentes en contra de los ataques.

Integridad del sistema

El tercer pilar de la defensa en profundidad es el resguardo de la integridad del sistema. Aquí, el énfasis está puesto en la protección de los sistemas de automatización y componentes de control tales como *Simatic S7-1200* y *S7-1500*, así como sistemas SCADA y HMI contra acceso no autorizado; también, es satisfacer requisitos especiales como protección del saber-hacer.

Además, la integridad del sistema también implica autentificación de usuarios, autorizaciones de acceso o de realizar cambios, y fortalecimiento del sistema; en otras palabras, la robustez de los componentes en contra de los ataques. ❖