Ciberseguridad industrial: el diseño integral es la base

Phoenix Contact
www.phoenixcontact.com

Vivimos en una época en la que el desarrollo de las tecnologías de comunicación permite que millones de equipos intercambien información en todo el mundo. Por eso, es necesaria una estrategia para garantizar la seguridad de red y la disponibilidad de la planta. En este contexto, *Phoenix Contact* desarrolla soluciones para proteger los sistemas, los conocimientos técnicos y todos los datos confidenciales que dan forma a los procesos comerciales y de producción de las empresas.

El tema de la ciberseguridad incumbe a todos, tanto fabricantes como empresas explotadoras, la industria o la infraestructura crítica.

Relevancia de la ciberseguridad en todas las industrias

La lista de incidentes de seguridad en la industria es cada vez más larga: *Stuxnet*, un programa dañino especial para sistemas SCADA, los virus *Industroyer* (2016) y *Triton* (2017), un ataque selectivo a los controles de seguridad y el software de extorsión *WannaCry* (2017), que ha atacado a más de 230.000 sistemas en todo el mundo.

El tema de la ciberseguridad incumbe a todos, tanto fabricantes como empresas explotadoras, la industria o la infraestructura crítica. La creciente interconexión y conexión de sistemas de control y automatización industriales (ICS) a Internet también hace que estos cada vez estén más expuestos

a ataques cibernéticos y cambios no deseados. Por este motivo, la ICS Security cada vez adquiere más relevancia.

Para los fabricantes de maquinaria, la seguridad aumenta la fiabilidad y disponibilidad de sus máquinas. Para el mantenimiento remoto de cara al cliente se precisa, además, una conexión remota segura.

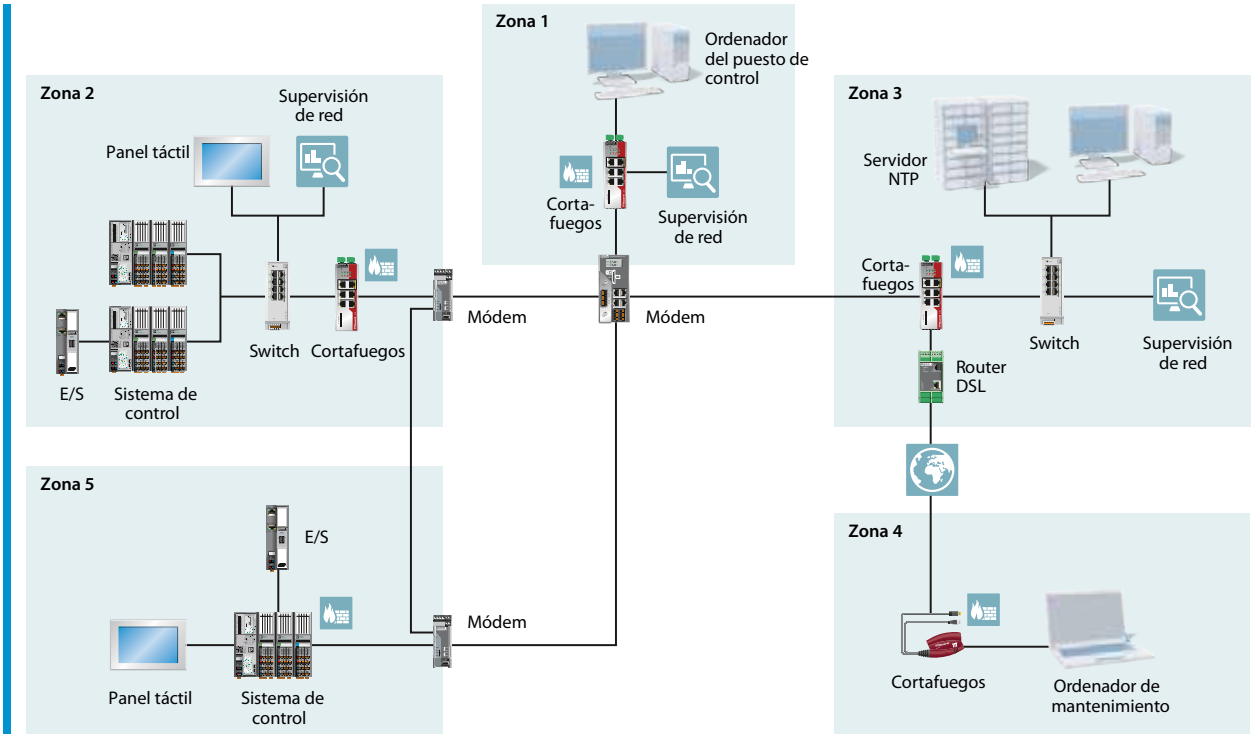
Para el explotador de la instalación, la seguridad, no solo garantiza la disponibilidad y el desarrollo fiable de sus instalaciones y procesos, sino que protege, además, sus conocimientos técnicos sobre producción.

En la industria automovilística, la disponibilidad de sus instalaciones es su activo más preciado. Los mecanismos de seguridad garantizan la disponibilidad de las líneas de producción y pueden incluso aumentarla.

En el sector energético, las empresas juegan un papel importante en el suministro básico a las personas. Por este motivo, los legisladores de muchos países obligaron a los explotadores a proteger la infraestructuras de importancia crítica de sus instalaciones para evitar un acceso no autorizado.

En el caso de tratamiento de aguas y aguas residuales, su tarea más importante es garantizar el suministro continuo de agua potable y la limpieza de las aguas residuales. La seguridad garantizará el acceso remoto a las estaciones remotas de bombeo y elevación y protegerá los sistemas de automatización frente al creciente número de ciberataques por Internet.

Respecto de petróleo y gas, la seguridad debe considerarse un requisito en el ámbito de la protección (safety), en particular en entornos explosivos o ligeramente inflamables. No en vano, una instalación hackeada, no solo puede suponer un riesgo financiero, sino también un riesgo para la seguridad de sus empleados.

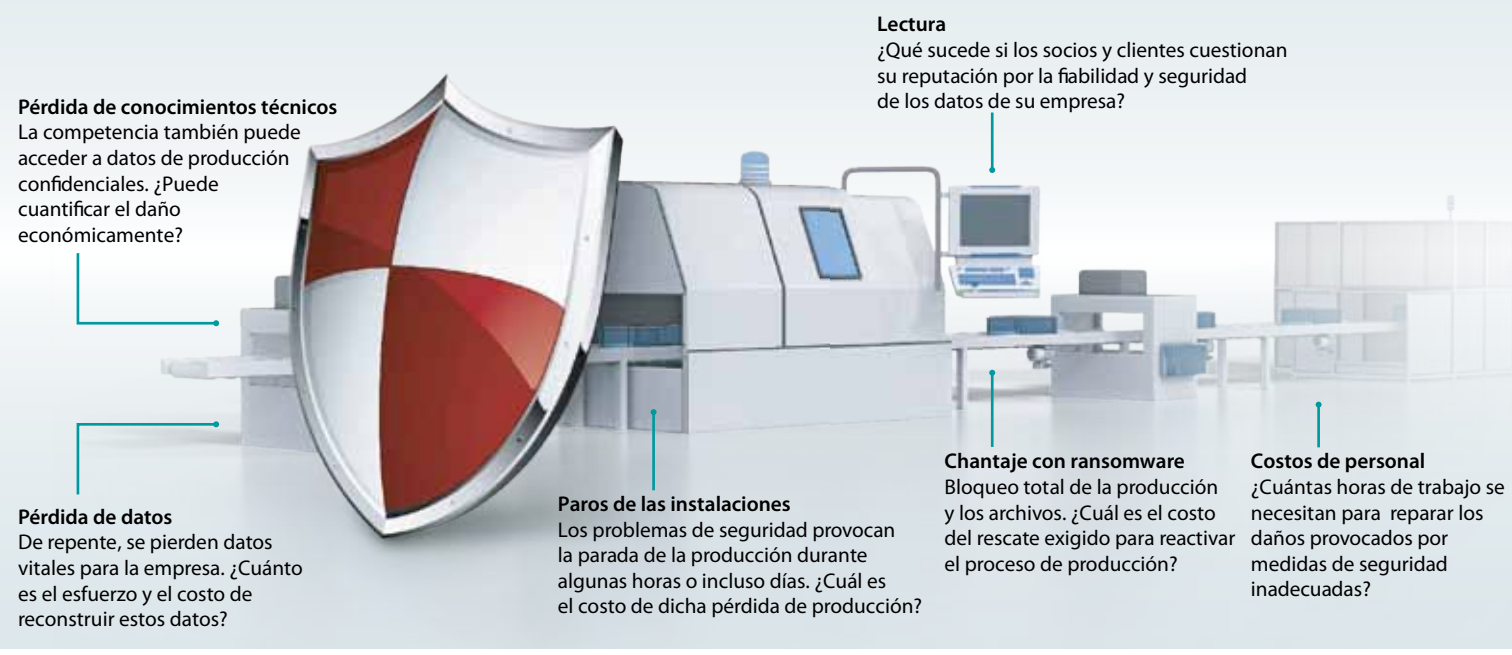


Posibles consecuencias de un incidente de seguridad

Las empresas solo tienen éxito si sus plantas de producción funcionan de forma segura y sin fallos. Los fallos, los sabotajes o las pérdidas de datos pueden causar un alto daño económico. Y es que las paradas no solo implican pérdidas financieras, sino que también ponen en peligro los plazos de entrega y, como consecuencia, la imagen y la reputación de la empresa. En un análisis de sitios y procesos, se pueden evaluar los riesgos relativos de un sistema industrial y su interacción con el sistema de información de la instalación.

Los cuestionamientos que vale la pena hacerse son los siguientes:

- Pérdida de conocimientos técnicos. La competencia también puede acceder a datos de producción confidenciales. ¿Se puede cuantificar el daño económicamente?
- Pérdida de datos. De repente, se pierden datos vitales para la empresa. ¿Cuánto es el esfuerzo y el costo de reconstruir estos datos?
- Paros de las instalaciones. Los problemas de seguridad provocan la parada de la producción durante algunas horas o incluso días. ¿Cuál es el costo de dicha pérdida de producción?
- Lectura. ¿Qué sucede si los socios y clientes cuestionan la reputación por la fiabilidad y seguridad de los datos de la empresa?
- Chantaje con *ransomware*. Bloqueo total de la producción y los archivos. ¿Cuál es el costo del rescate exigido para reactivar el proceso de producción?
- Costos de personal. ¿Cuántas horas de trabajo se necesitan para reparar los daños provocados por medidas de seguridad inadecuadas?



Riesgos de seguridad habituales y soluciones

Los fallos y virus provenientes de Office se pueden contagiar directamente al entorno de producción. La solución a esto es la división de grandes redes en pequeños segmentos, se puede controlar el intercambio de datos entre las diferentes zonas, por ejemplo, entre la producción y Office, o entre diferentes partes de la instalación. Los segmentos individuales se pueden separar con ayuda de VLAN o cortafuegos. Para la comunicación entre los segmentos de red individuales deben emplearse routers o switches de capa 3. Estos equipos captan los errores de red, de manera que no se puedan expandir al resto de la red.

Las paradas no solo implican pérdidas financieras, sino que también ponen en peligro los plazos de entrega y, como consecuencia, la imagen y la reputación de la empresa.

Otro riesgo es la infección por software dañino. Con frecuencia, el software dañino está concebido de forma que intenta expandirse a los sistemas vecinos para dañarlos. Un ejemplo es el software dañino *WannaCry*, que infecta los sistemas Windows no actualizados.

La solución al software dañino es la limitación de la comunicación. El uso de cortafuegos puede limitar o impedir la propagación del software dañino. Si se bloquean todas las posibilidades de comunicación que no son técnicamente necesarias, se pueden evitar muchos ataques. Además, el monitoreo integral apto para la industria ayuda a detectar y contener en una fase temprana cambios y manipulaciones en sistemas basados en Windows, como sistemas de control, unidades de operación o PC.

El ataque de hackers, por su lado, implica un riesgo en tanto que los delincuentes pueden usar una conexión abierta a Internet para copiar datos o realizar cambios en el sistema. La solución es la transmisión de datos codificada. Se debe impedir el acceso a los sistemas de automatización a través de Internet. Esto se puede lograr mediante un cortafuegos, que limita todo el tráfico entrante y saliente a las conexiones necesarias y permitidas. Todas las conexiones de amplio alcance deben estar cifradas, por ejemplo, a través de VPN con Ipsec.

Para el acceso no autorizado a las instalaciones, la solución consiste en un acceso remoto seguro a una o más máquinas, y quizá con diferentes soluciones tecnológicas. Por un lado, la comunicación externa está codificada, por ejemplo, a través de IPsec u OpenVPN. Por el otro, se puede iniciar el mantenimiento remoto en la máquina a través de un conmutador de llave. De esta forma, se garantiza que solo se realicen los cambios en la máquina en la que está previsto. Al mismo tiempo, el conmutador de llave se puede utilizar para bloquear las reglas de comunicación en la red durante el tiempo del mantenimiento remoto.

Un gran amigo de los ciberataques es la administración insuficiente de usuarios. on frecuencia, se utilizan contraseñas colectivas para el acceso. Cuando los empleados dejan la empresa, estas contraseñas no se modifican ni se desactivan. El resultado es que demasiados empleados conocen la contraseña colectiva y pueden provocar usos inadecuados. La solución es una administración de usuarios centralizada, en donde se concede acceso individual a cada empleado.

Otro riesgo lo presentan los equipos y terminales móviles no autorizados que se comunican a través de la interfaz WLAN. Para este caso, se puede asignar una contraseña WLAN segura, con contraseñas individuales. Si se conocen las contraseñas WLAN y no se cambian durante un largo periodo de tiempo, se puede producir un acceso incontrolado a la red de maquinaria. Además, se puede proteger

la comunicación WLAN con una zona desmilitarizada y aislarla del resto de la red.

Por último, vale destacar el riesgo por configuración incorrecta o insegura de los equipos. Las configuraciones estándar se han diseñado para garantizar que los componentes funcionen correctamente y que sean fáciles de poner en funcionamiento y, en este contexto, los mecanismos de seguridad juegan con frecuencia un papel secundario. Como respuesta a esto, se pueden implementar gestión de dispositivos y parches.

Al gestionar varios equipos, una gestión de dispositivos y parches inteligente y eficiente puede automatizar procesos que requieren mucho tiempo y reducir, además, los riesgos de una configuración incorrecta. Ayuda a configurar, desplegar y gestionar los equipos y reduce los riesgos de seguridad y cumplimiento acortando los ciclos de parches y actualizaciones. La gestión de dispositivos y parches permite la creación y gestión centralizadas de todos los ajustes de los equipos relevantes para la seguridad, además de facilitar las actualizaciones de firmware

Las medidas organizativas y técnicas sostenibles, ajustadas al ciclo de vida de una instalación, minimizan el riesgo de posibles ataques.

Una respuesta posible

Phoenix Contact ofrece seguridad normalizada en productos, soluciones industriales y servicios para lograr un funcionamiento seguro en el futuro de máquinas, instalaciones e infraestructuras. La seguridad está anclada en todo el ciclo de vida de los productos y soluciones.

Las medidas organizativas y técnicas sostenibles, ajustadas al ciclo de vida de una instalación, minimizan el riesgo de posibles ataques. Para lograr la máxima estabilidad y transparencia, la empresa ayuda a seleccionar el hardware adecuado, a desarrollar conceptos de protección personalizados y a impartir cursos de formación práctica.

Su idea de "Security by Design" (seguridad bajo diseño), conforme a la norma internacional IEC 62443-2-4, significa:

- Determinación de los requisitos de protección
- Realización de un análisis de riesgos y amenazas
- Desarrollo de un concepto de red segura, con zonas y conductos, teniendo en cuenta la norma IEC 62443
- Selección de productos de automatización seguros
- Documentación y puesta en marcha de la instalación
- Servicios complementarios para la instalación (por ejemplo, gestión de parches) a lo largo del ciclo de vida ❖