Cómo mitigar ciberataques contra los elementos de automatización de la fábrica

PLC, HMI y demás sistemas se han convertido en blancos fáciles del cibercrímen. En este artículo, algunos consejos prácticos sobre cómo estar preparado y un detalle sobre algunas características de la ciberseguridad integrada del PLC.

Recomendación de lectura de Enrique Larrieu Let
elarrieulet@gmail.com

Históricamente, los sistemas de fabricación han estado protegidos, ya sea por estar aislados del mundo exterior, ya sea por estar conectados a redes IT ya protegidas con firewalls o softwares antivirus. Sin embargo, a medida que la fabricación se adentra en la era digital, también se hace más susceptible a los ataques. Afortunadamente, durante la última década, los fabricantes han evidenciado sus esfuerzos para proteger sus PLC, HMI, y demás sistemas, contra hackers o softwares maliciosos.

La ciberresiliencia es la capacidad que tiene una organización de atender, recuperarse y adaptarse a los ciberataques.

Entender la ciberamenaza en la fabricación

Los sistemas de fabricación modernos son una combinación sofisticada de sistemas de control PLC, tecnología de la información (IT) y tecnología operacional (OT). Cada uno juega su rol a favor de la eficiencia y la productividad, y el ataque a cualquiera de estos componentes puede ser devastador. La tendencia de interconectar sistemas con tecnologías modernas abre nuevas puertas a cibercriminales potenciales. Dado que estos componentes suelen contar con medidas de seguridad inadecuadas de las que se pueden aprovechar los ciberatacantes, se deben emplear otras capas de seguridad.

De cara a tales amenazas, emergió la ciberresiliencia como punto central en una estrategia de ciberseguridad. La ciberresiliencia es la capacidad que tiene una organización de atender, recuperarse y adaptarse a los ciberataques. Esta resiliencia es una combinación de muchas estrategias que previenen o minimizan el impacto de un ingreso no deseado, mantienen operaciones críticas y aseguran una pronta recuperación.

Fuente: *https://www.engineering.com/story/mitigating-cyber-attacks-on-manufacturing-automation-assets*

Implica hacer de la ciberseguridad un factor clave de la cultura de la empresa, con comunicación clara y consistente acerca de su importancia.

El factor humano en la ciberseguridad

A la vez que las medidas técnicas conforman el núcleo de cualquier estrategia de ciberseguridad, la cuestión humana es igualmente crucial. Los ataques de ingeniería social —en donde los atacantes engañan a la gente para obtener información confidencial— son una forma común de ciberataque y, a menudo, exitosa. Entrenar a los empleados en ciberseguridad los ayuda a entender las amenazas que enfrentan y cómo sus acciones impactan en la ciberseguridad de la empresa.

Esto implica hacer de la ciberseguridad un factor clave de la cultura de la empresa, con comunicación clara y consistente acerca de su importancia.

Estrategias para mitigar los ciberataques

Evaluación y gestión de riesgos

Más allá del sistema, uno de los primeros pasos hacia un entorno de fabricación ciberresiliente es llevar adelante una evaluación exhaustiva del riesgo. Identificar y evaluar los riesgos potenciales, es decir, ranqueados desde contraseñas débiles o softwares desactualizados hasta conexiones de red o controles de acceso físico inseguros. Tales riesgos se pueden reducir con un buen conjunto de prácticas de trabajo en red tales como implementar encriptado, autenticación de dos factores, actualizaciones periódicas de software y monitoreo constante.

Es esencial un entrenamiento en ciberseguridad regular y efectivo para todos los empleados.

Entrenamiento a empleados

Es esencial un entrenamiento en ciberseguridad regular y efectivo para todos los empleados. Podría cubrir tópicos que van desde saber identificar y evitar intentos de phishing o practicar buena higiene de contraseñas, hasta entender la

importancia y procedimientos de actualización de un software.

Defensa en capas

Los fabricantes deberían adoptar una defensa en capas, también conocida como "defensa en profundidad". Este acercamiento implica el despliegue de una serie de mecanismos defensivos tales como firewalls; prevención y detección de la intrusión; protocolos de encriptado, y auditorías periódicas del sistema. Contar con múltiples capas de medidas de seguridad minimiza enormemente la posibilidad de éxito de cualquier intento de vulneración. Dividir el PLC y las redes en subredes o segmentos mejora la seguridad y rendimiento de la red. Si un atacante compromete un grupo, no sufrirá daños la red completa.

Los fabricantes deberían adoptar una defensa en capas, también conocida como "defensa en profundidad".

Sistemas heredados

El equipamiento más viejo quizá necesite capas extras de seguridad que podrían incluir límites físicos de acceso a los puertos de conexión. También se podrían explorar métodos alternativos de recolección de la información, por ejemplo, usar un PLC intermedio. En un entorno de fabricación, la seguridad física y la ciberseguridad no se deberían entender como entidades separadas, sino que se deberían atender de manera integrada. Los sistemas de vigilancia se podrían usar para disuadir y, a la vez, proveer información valiosa en caso de ataque efectivo.

Planificar la respuesta ante incidentes

Contar con un plan de respuestas bien estructurado y practicado puede reducir drásticamente el daño y el tiempo de recuperación de un ataque. Un plan semejante debería incluir roles y responsabilidades bien definidos, protocolos de comunicación y pasos a seguir para aislar los sistemas y procesos afectados, a fin de recuperar el sistema y llevar a cabo un análisis luego del incidente. Esto incluye conservar copias de seguridad a las que se puede recurrir en caso de vulneración.

El equipamiento más viejo quizá necesite capas extras de seguridad que podrían incluir límites físicos de acceso a los puertos de conexión.

Monitoreo y mejora

Las ciberamenazas evolucionan constantemente, lo que significa que las medidas de seguridad estáticas son inadecuadas. El que debe tomar lugar es un sistema de monitoreo y actualización constante de medidas de seguridad. Esto implica estar al día con las últimas novedades en ciberseguridad, inteligencia de las amenazas y avances tecnológicos. Los programas de PLC se pueden auditar automáticamente en modificaciones no autorizadas en comparación con copias de seguridad. Cualquier anomalía puede generar una alerta que facilite y agilice una respuesta.

Seguridad en la cadena de suministro

A fin de mitigar los ataques a la cadena de suministro, los fabricantes necesitan extender sus esfuerzos de ciberseguridad hasta sus proveedores. Esto incluye gestionar auditorías de ciberseguridad, colaborar con las mejores prácticas de seguridad y redactar medidas contractuales sobre ciberseguridad. Recordar que la mejor estrategia de seguridad, en general, incluye una combinación de herramientas y técnicas adaptadas a las necesidades y riesgos específicos de un entorno de fabricación específico.

Seguridad de PLC

El concepto de ciberseguridad integrada en el PLC es nuevo y evoluciona, aunque algunas empresas ya habían comenzado a incorporar características básicas de seguridad en sus PLC a fin de atender la cuestión. A continuación, algunos ejemplos. (Nótese que, aunque estos PLC cuentan con ciberseguridad integrada, no son inmunes a todas las ciberamenazas. Medidas de seguridad en niveles, siguiendo las mejores prácticas y con actualizaciones periódicas son esenciales para mantener un entorno seguro. También es importante trabajar cerca de los proveedores de PLC y expertos en ciberseguridad a fin de comprender de manera más acabada las características, limitaciones y mejores usos de cada PLC).

- S7-1500, de Siemens. La ciberseguridad del PLC S7-1500 incluye dispositivos de programación y paneles HMI que requieren autorizaciones específicas del usuario para conectarse; integridad de la comunicación, donde los datos se protegen de la manipulación durante la transmisión mediante cifrado y códigos de autenticación de mensajes. Incluso la comunicación de PLC a PLC y de PLC a HMI requiere que los dispositivos se conecten entre sí para cerrar una ruta de acceso que, de otro modo, estaría abierta.
- ControlLogix 5580, de Rockwell. Estos controladores incluyen un conjunto de características tales como control de acceso basado en roles; firmware encriptado y firmado digitalmente; detección de cambios y accesos, y auditoría de seguridad, así como protección de direcciones IP y MAC.
- Schneider Electric Modicon M580, de Schneider Electric. Características tales como ciberseguridad integrada, encriptado ethernet, y certificación Achilles Nivel, una certificación reconocida que indica un alto nivel de protección contra amenazas conocidas.
- ControlEdge PLC, de Honeywell. Evita cargas de firmware no autorizadas y favorece controles de usuario sólidos para gestionar el acceso.
- AC500-S, de ABB. Incluyen gestión de usuario, control de acceso basado en roles y un firewall. Está diseñado de acuerdo a IEC 62443, un estándar internacional de ciberseguridad referido a sistemas de control y automatización industrial. ❖