La colaboración entre OT e IT es fundamental para la industria 4.0

Los equipos de OT e IT también deben desarrollar una estrategia conjunta de ciberseguridad que aborde los riesgos y desafíos específicos de ambos sistemas.

Los sistemas OT en una fábrica suelen ser infraestructuras críticas que controlan y monitorean el proceso de producción.

Kimberly Cornwell
Cortesía de BigStock.com
Derechos de autor: Yuri Hoyda

Siemens
www.siemens.com.ar

Los sistemas de tecnología operativa (OT) y tecnología de la información (IT) en una fábrica siempre han sido entidades separadas con diferentes objetivos, sistemas y tecnologías.

Con la creciente tendencia de la digitalización y la Industria 4.0, la línea entre OT e IT se ha difuminado, lo que lleva a la convergencia de estos dos sistemas. Como resultado, cada vez es más común que haya vulnerabilidades de OT que afecten a los sistemas de IT o vulnerabilidades de IT que afecten a los sistemas de OT. Ambos equipos tienen que colaborar y aprender las prioridades y los puntos ciegos de sus departamentos hermanos.

Por ejemplo, mientras que los departamentos de IT se han convertido en expertos en la educación de los empleados a fin de que lleven a cabo prácticas informáticas seguras, los departamentos de OT pueden no tener la experiencia en la reeducación de las mejores prácticas generales de los empleados.

Por el contrario, los profesionales de IT pueden no comprender inherentemente los objetivos de OT de redundancia de sistemas y minimizar el tiempo de inactividad.

Acerca de la autora
Kimberly Cornwell es ingeniera de sistemas en la división de automatización de fábricas de la industria digital de Siemens y miembro del equipo técnico de ciberseguridad de automatización de fábricas. Graduada en Ingeniería Mecánica del MIT, se dedica a los controles industriales y a la identificación de vulnerabilidades en el panorama industrial de OT.

Comprender dónde chocan los mundos de IT y OT

Los sistemas OT en una fábrica suelen ser infraestructuras críticas que controlan y monitorean el proceso de producción. Esto los convierte en objetivos principales para los ataques cibernéticos que podrían causar interrupciones, lo que lleva a pérdidas financieras, daños a la reputación e incluso riesgos de seguridad.

Por ejemplo, un ataque cibernético a los sistemas OT de una fábrica podría llevar al cierre de la línea de producción, lo que resultaría en la pérdida de tiempo y recursos valiosos. Los sistemas OT en una fábrica a menudo están aislados de la red de IT, lo que los hace menos susceptibles a los ataques cibernéticos. Sin embargo, esto también las hace más difíciles de asegurar, ya que estas redes "aisladas" pueden no tener el mismo nivel de medidas de seguridad que las redes corporativas que mantiene IT. Incluso sin integración de OT y IT, las redes y sistemas de OT son conocidos por tener una seguridad decepcionante o inexistente, desde redes WiFi abiertas hasta puertos de datos no seguros en la fábrica.

Como resultado, la integración de sistemas OT y IT en una fábrica sin una estrecha colaboración aumentan la posibilidad de ataque y abre nuevos vectores de ataque que podrían comprometer la seguridad de todo el sistema. Por lo tanto, el equipo de ciberseguridad de OT debe trabajar estrechamente con el equipo de IT para garantizar que las medidas de seguridad implementadas para la red de IT también se apliquen a la red de OT.

Los sistemas OT en una fábrica suelen ser más antiguos y menos sofisticados que los sistemas de IT, lo que los hace más vulnerables a los ataques cibernéticos. La mayoría de los equipos y sistemas en las plantas existentes fueron diseñados y construidos antes del advenimiento de las medidas modernas de ciberseguridad, y no fueron diseñados para resistir los ciberataques modernos. Estos sistemas pueden utilizar protocolos heredados y métodos de comunicación que son menos seguros que los protocolos actuales, lo que los convierte en un objetivo más fácil para los ciberdelincuentes. Para abordar estas vulnerabilidades, el equipo de ciberseguridad de OT debe trabajar con el equipo de IT para implementar medidas de seguridad modernas como firewalls, sistemas de detección de intrusos y cifrado, para proteger los sistemas de OT, detectar infracciones e implementar defensas y respuestas automatizadas.

El equipo de ciberseguridad de OT debe trabajar estrechamente con el equipo de IT para garantizar que las medidas de seguridad implementadas para la red de IT también se apliquen a la red de OT

El camino pavimentado con buenas intenciones

Los equipos de OT e IT de una fábrica tienen diferentes perspectivas y objetivos, y es posible que no siempre vean la importancia de colaborar en temas de ciberseguridad. Por ejemplo, el equipo de OT se ocupa principalmente de garantizar el buen funcionamiento del proceso de producción. Por el contrario, el equipo de IT se centra en garantizar la seguridad de sus redes. Sin embargo, ambos equipos deben entender que la seguridad de un sistema depende de la seguridad del otro y que comprometer un sistema podría tener un efecto dominó en ambos. Como resultado, los equipos de OT y IT deben trabajar juntos para desarrollar una estrategia conjunta de ciberseguridad que aborde los riesgos y desafíos específicos de ambos sistemas. ❖