Rockwell Automation

Reforzando la ciberseguridad en la fabricación inteligente

Cómo pueden las empresas de alimentos y bebidas conectar sus instalaciones y proteger sus datos

Umair Masud, gerente de cartera de servicios de consultoría y Sherman Joshua, director de marketing global de servicios de IIoT, Rockwell Automation

Introducción

Los productores de alimentos y bebidas están comenzando a disfrutar de las ventajas de la fabricación inteligente a un ritmo cada vez más mayor. Ellos reconocen el valor de la conectividad y las oportunidades de profundizar en el conocimiento de los procesos de producción, mejorar la visibilidad y las prácticas de seguridad de los alimentos, y solucionar o ayudar a prevenir problemas relacionados con la seguridad de los alimentos. Sin embargo, con esta importante tendencia viene otro asunto más preocupante: vulnerabilidades debidas a una ciberseguridad insuficiente.

Las amenazas de seguridad son hoy en día más cambiantes que nunca: pueden ser digitales o físicas, internas o externas, voluntarias o involuntarias. Y ninguna organización está exenta de incidentes de seguridad. Además, a medida que la conectividad de las operaciones es mayor, también lo son los riesgos de seguridad, particularmente, los de ciberseguridad.

Existe una amplia variedad de posibles adversarios en el mundo, todos con objetivos y métodos diferentes. En concreto, las empresas de alimentos y bebidas podrían ser objetivo de ataques que pretendan comprometer la seguridad de los alimentos o la integridad en el suministro alimentario del país. O podrían sufrir ataques destinados a probar métodos concebidos para otras organizaciones o industrias. Todas estas amenazas suponen un riesgo para las operaciones de las empresas del sector, para las marcas y también para los consumidores a los que sirven.

Las industrias con regulaciones más rigurosas se han visto forzadas a abordar las crecientes necesidades de seguridad mucho antes que otros sectores. Durante un tiempo, muchos de los productores de alimentos y bebidas se mantuvieron centrados en las medidas físicas asociadas con la calidad y la seguridad de los alimentos. Actualmente, muchas empresas están reconsiderando su estrategia de seguridad para hacerla más global y coherente en un ambiente conectado.

Enfoque basado en la evaluación de riesgos

La ciberseguridad es un mundo en constante evolución. No existe una solución completa que pueda ofrecer un ambiente completamente seguro. En consecuencia, los productores deben implementar una variedad de capacidades y controles diferentes que les permitan responder y adaptarse a estas amenazas emergentes y en constante evolución.

Un enfoque basado en la evaluación de riesgos permite identificar los riesgos únicos de una organización –relacionados con su personal, con sus procesos y con su tecnología– e implementar políticas y procedimientos para encararlos. De este modo, los productores disponen de flexibilidad para dimensionar correctamente sus esfuerzos y asignar los recursos adecuados a fin de reducir el riesgo hasta un nivel aceptable para toda la organización.

Cuando la estrategia está bien implementada, aporta valor más allá de las implicaciones de seguridad más obvias. También mejora la productividad y ayuda a evitar pérdidas innecesarias. Gracias a los programas de ciberseguridad, la visibilidad de los activos es mucho mayor, por lo que los productores pueden identificar y corregir los problemas de forma más efectiva. Por ejemplo, si los ingenieros pueden acceder de forma remota a un PLC del ambiente de producción, estarán aprovechando una ventaja que ayuda a la empresa a mantener los niveles de productividad. Sin embargo, si este acceso no se realiza con los controles adecuados, alguno de ellos podría acceder al PLC incorrecto y provocar interrupciones innecesarias y caídas de productividad.

La pregunta es ¿cómo pueden los productores evaluar su programa de seguridad actual y cambiar su estrategia por una más global basada en la evaluación de riesgos? Existen tres áreas clave que es necesario tener en cuenta: la higiene cibernética en la organización, la estrategia de defensa en profundidad y la planificación frente al ciclo continuo de los ataques.

Higiene cibernética

Para aquellos productores de alimentos y bebidas que hayan introducido recientemente la fabricación inteligente o que estén en las fases iniciales de actualización de sus prácticas de ciberseguridad, lo más natural es empezar por la higiene cibernética. Encarar cuatro áreas programáticas clave puede ayudar a las organizaciones a establecer un nivel básico de higiene cibernética.

En primer lugar, es necesario comenzar con un inventario en profundidad de los activos conectados en la planta, así como de sus vulnerabilidades conocidas, que, además, debe ser actualizado con regularidad. En segundo lugar, la organización debe crear programas que encaren las vulnerabilidades conocidas de los activos, con aplicación regular de parches y con procesos maduros que permitan realizar y hacer seguimiento a los cambios de configuración necesarios. En tercer lugar, es necesario emplear mecanismos para el respaldo y la recuperación de todos los activos críticos. Esto contribuye a asegurar que la empresa tiene de reserva un elemento de respaldo al que puede acceder con rapidez. Por último, la evaluación regular de riesgos permite a la organización medir y gestionar continuamente los riesgos. Esta evaluación proporciona un panorama actualizado del nivel de riesgo al que se ve expuesta la organización y los recursos necesarios para reducirlo.

Estos son pasos fundamentales que permiten construir una buena base de ciberseguridad a partir de la cual la organización puede seguir construyendo. Aun cuando es esencial mantener una buena higiene cibernética, una organización conectada debe ir más allá para desarrollar un programa de ciberseguridad más robusto que abarque todas sus operaciones.

Defensa en profundidad

Un enfoque de ocultamiento de activos ya no ofrece suficiente protección contra la gran variedad de actores maliciosos y amenazas actuales. Las organizaciones deben desarrollar su seguridad partiendo de una idea de que cualquier punto individual de protección probablemente podrá ser neutralizado por los atacantes. Una estrategia de defensa en profundidad crea varias capas de protección mediante barreras físicas, electrónicas y procedimentales. De esta manera, frente a una amenaza, la organización cuenta con más de una línea de defensa.

Existen seis componentes principales en una estrategia de defensa en profundidad: políticas y procedimientos, ambiente físico, redes, computadoras, aplicaciones y dispositivos. Aun cuando toda organización cuenta con una estrategia de seguridad única, cada uno de estos componentes tendrá un papel que jugar en la efectividad del enfoque general.

Las políticas y procedimientos abordan el lado humano de la seguridad, ya que ayudan a modelar el comportamiento de los empleados y a confirmar que estos siguen adecuadamente las prácticas de seguridad necesarias y que utilizan las tecnologías adecuadamente. La seguridad física limita el acceso del personal, tanto externo como interno, a las instalaciones. El acceso del personal debe estar fuertemente controlado, no solo en términos del acceso a ciertas áreas de la instalación, sino también en cuanto a los puntos de entrada a la infraestructura física de la red, es decir, a paneles de control, cableado y dispositivos.

La seguridad de la red debe ser desarrollada mediante una estrecha colaboración entre los departamentos de IT y de OT, cuyo trabajo conjunto permitirá identificar e implementar las políticas y tecnologías adecuadas. Estas tecnologías probablemente incluirán una zona desmilitarizada industrial (IDMZ) que separe el área de la empresa del área industrial, y que también ayude a gestionar el acceso y a monitorizar el tráfico.

El componente relacionado con la computadora es fundamental, ya que las vulnerabilidades de software representan el medio de entrada más frecuente a los sistemas de automatización. Entre las medidas concretas que pueden fortalecer las computadoras de la organización se encuentran la gestión de parches, el software antivirus, las listas de aplicaciones permitidas y los sistemas de detección de intrusiones.
Al nivel de aplicaciones de producción, se requieren dispositivos de seguridad para restringir tanto el acceso físico como el digital. El software de autentificación, autorización y registro (AAA, por sus siglas en inglés) ayuda a restringir y monitorear el acceso y los cambios a las aplicaciones.

Por último, los dispositivos representan la última área de defensa de la seguridad en profundidad. Las organizaciones deben considerar el despliegue de mecanismos de autentificación de dispositivos que permitan identificar los dispositivos no autorizados, además de modificar la configuración predeterminada de los dispositivos incorporados.

Gran parte de esta estrategia de defensa en profundidad está centrada en medidas defensivas proactivas que impiden que las amenazas se lleguen a manifestar completamente. Sin embargo, también es importante para las organizaciones investigar y prepararse para el ciclo de vida útil completo de las posibles amenazas, incluyendo aquellas que pueden convertirse en verdaderos incidentes de seguridad.

Ciclo continuo de los ataques

Los programas más robustos y efectivos de ciberseguridad tienen en cuenta todas las fases del ciclo continuo de los ataques: antes del ataque, durante el mismo y después de que se haya producido. Todos los pasos y actividades antes descritos están directamente relacionados con la fase previa al ataque, cuando la organización necesita enfocarse en la identificación y protección de los activos, tanto de IT como de OT. Contar con un plan de gestión de riesgos exhaustivo y actualizado frecuentemente y con un sólido programa de ciberseguridad permitirá a la organización minimizar la ocurrencia de los ataques.

Por supuesto, en un panorama tan complejo y cambiante en cuanto a amenazas, la vigilancia constante es fundamental. Por ese motivo, las organizaciones deben contar con sistemas que monitoreen y detecten todo comportamiento de la red que no se ajuste a la línea base o a los patrones esperados, y que puedan reaccionar, ajustar el sistema e impedir las posibles amenazas de los ataques.

Tras el ataque, la primera prioridad es ayudar a garantizar una producción segura y minimizar el tiempo improductivo resultante del ataque cibernético. Un plan de gestión de riesgos de la organización debe incluir los procesos necesarios para contener un ataque, para erradicar los efectos del mismo y para recuperar los sistemas lo más rápido posible. El plan también debe detallar los pasos que debe seguir la investigación posterior al ataque, cuyo objetivo es la identificación de las causas raíz y el fortalecimiento de los medios encargados de resistir dicho ataque.

Toma de medidas

Durante años, los productores de alimentos y bebidas han estado centrados en las medidas de seguridad física que mejoraban la calidad y la seguridad de los alimentos, que protegían a los consumidores y que vigilaban el suministro de alimentos del país. Sin embargo, en un ambiente conectado como el actual, la seguridad física y la ciberseguridad están unidas inexorablemente. Por eso ha llegado el momento de que las organizaciones de todo el sector confirmen que cuentan con un programa robusto de ciberseguridad para mitigar el mayor espectro de posibles riesgos y amenazas. La aplicación del mismo rigor a los programas de seguridad física y de ciberseguridad es la mejor manera que tienen las empresas de alimentos y bebidas de proteger su marca, su reputación y sus intereses financieros.

Obtenga más información en rok.auto/security

Umair Masud

Sherman Joshua

Masud manages the security services portfolio at Rockwell Automation. He has over 10 years of experience working to help customers manage cyber risk within their industrial control system environments. Reach him at utmasud@ra.rockwell.com.

Joshua leads global marketing for IIoT services at Rockwell Automation. These services include remote support services, network and cybersecurity consulting, remote monitoring, and data analytics. Reach him at sljoshua@ra.rockwell.com.

"How to Strengthen Cybersecurity in Smart Manufacturing"
Umair Masud and Sherman Joshua, Food Quality and Safety
March, Copyright © 2019

Connect with us.

rockwellautomation.com — expanding **human possibility**™

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication FOOD-SP028A-ES-P – November 2019