Rockwell Automation

Casos prácticos de ciberseguridad industrial

Retos, soluciones y resultados en todas las industrias

Tabla de contenido

COMPARTIENDO LAS LECCIONES APRENDIDAS 01

Un mensaje de Rockwell Automation

BREVE RESUMEN DEL MERCADO 02

Amenazas de ciberseguridad en las industrias de OT: el ransomware sigue causando interrupciones

PRODUCTOS FARMACÉUTICOS 06

Una empresa farmacéutica global obtiene visibilidad de amenazas de ICS en tiempo real además de información diaria sobre el inventario de activos en 64 sitios globales

CIENCIAS BIOLÓGICAS 08

Un fabricante de dispositivos médicos moderniza su infraestructura de red para mejorar la ciberseguridad de OT y apoyar el crecimiento empresarial

EMPRESA DE ENERGÍA 10

Una empresa de energía aumenta la ciberseguridad en 62 estaciones y terminales de compresores con la detección de amenazas y el inventario de activos en tiempo real

PETRÓLEO Y GAS 12

Una empresa de petróleo y gas disminuye el riesgo de tiempo improductivo cibernético en tan solo un mes con la detección de amenazas y la identificación del inventario de activos de red en tiempo real

INDUSTRIA AUTOMOTRIZ 14

Cómo un fabricante de automóviles evaluó su seguridad de OT para identificar mejoras en dos días

PRODUCTOS DE CONSUMO ENVASADOS 16

Un fabricante de alimentos implementa la gestión unificada de amenazas en 46 sitios globales para alinear la ciberseguridad entre docenas de empresas de adquisición

ALIMENTOS Y BEBIDAS 18

Un fabricante de alimentos y bebidas aumenta la ciberseguridad y la respuesta a incidentes, y mejora su puntuación de eficacia del equipo (OEE) en un 5%

ALIMENTOS Y BEBIDAS 20

Una empresa de alimentos y bebidas agiliza y simplifica la ciberseguridad de OT con servicios de asistencia técnica administrados 24/7

PRODUCTOS DE CONSUMO ENVASADOS 22

Una empresa de CPG implementa una transformación digital segura y reduce su tiempo de respuesta de red promedio a 3.5 minutos, lo que representa una mejora de un 90%

PRODUCTOS QUÍMICOS 24

Una empresa de productos químicos proporciona a sus empleados acceso remoto seguro para controlar el manejo del sistema en 8,000 puntos de E/S durante la pandemia

COMPARTIENDO LAS LECCIONES APRENDIDAS

Un mensaje de Rockwell Automation

Estimados lectores:

Sabemos que estos son tiempos difíciles para los proveedores de infraestructura crítica. Debido a los ciberataques ininterrumpidos, complejas iniciativas de transformación digital y una pandemia que parece interminable, muchas organizaciones están esforzándose por proteger sus sistemas de tecnología de operaciones (OT).

La seguridad de OT se ha hecho cada vez más importante a medida que los actores de amenazas han demostrado su capacidad y voluntad de filtrarse en los sistemas de IT como un paso intermedio hacia la infiltración de la OT y los sistemas de control industrial (ICS). Como será evidente, este tipo de brecha puede detener los sistemas de IT, así como la infraestructura crítica.

Si existe una amenaza específica que inquiete a los ejecutivos empresariales, es el vertiginoso aumento global de los ataques de ransomware. Por ejemplo, puesto que la tensión sigue aumentando tras la invasión rusa a Ucrania, la Agencia de Ciberseguridad y Seguridad de Infraestructuras de EE. UU. (CISA) ha avisado a las entidades gubernamentales estatales y locales estadounidenses, y a las redes del sector de aviación y energía, sobre un elevado riesgo de ataques de ransomware provenientes de Rusia.

Como circunstancia agravante, a muchas organizaciones de infraestructura crítica les faltan las capacidades automatizadas de detección y respuesta de amenazas como el monitoreo continuo de redes y sistemas. Otros problemas comunes incluyen los riesgos asociados con la transformación digital, sistemas y aplicaciones anticuados, activos digitales desconectados y una falta de gestión centralizada de redes y amenazas.

Por otra parte, la COVID-19 ha dado lugar a sus propios desafíos que incluyen la necesidad de capacidades seguras de trabajo remoto, así como interrupciones operativas periódicas y los impactos en la cadena de suministro.

¿Se ha preguntado alguna vez cómo los negocios lidian con estos innumerables riesgos? En esta recopilación de casos prácticos de clientes de Rockwell Automation, exploramos qué ha ayudado a otras organizaciones en una gama de industrias, entre ellas los sectores de productos farmacéuticos, de ciencias biológicas, de energía, de petróleo y gas, de fabricación automotriz, de alimentos y bebidas, de productos de consumo envasados y de fabricación.

Si le preocupan las amenazas a su infraestructura de OT e ICS, lea los relatos de éxito siguientes. Nuestros equipos expertos han ayudado a empresas en varias industrias a implementar operaciones industriales más seguras. Si bien no se puede garantizar que un programa de infraestructura crítica sea 100% seguro contra riesgos, sí existen soluciones probadas que pueden reducir en gran medida los riesgos de seguridad de infraestructura crítica de forma eficaz y eficiente.

Kamil Karmali

Gerente global, servicios de consultoría de ciberseguridad

Rockwell Automation

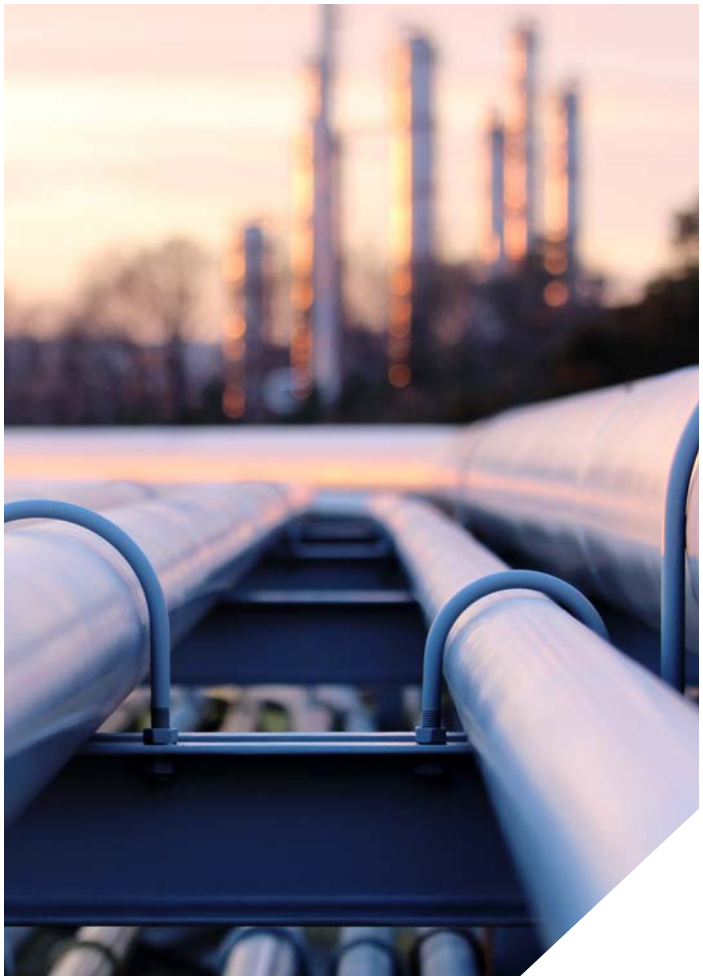
BREVE RESUMEN DEL MERCADO

Amenazas de ciberseguridad en las industrias de OT

EL RANSOMWARE SIGUE CAUSANDO INTERRUPCIONES

Si la experiencia es el mejor maestro, la segunda mejor opción podría ser las lecciones aprendidas de sus homólogos en la industria. Las organizaciones que han sufrido brechas perpetradas por actores de amenazas internos o externos normalmente aprenden valiosas lecciones sobre la ciberseguridad, entre ellas cómo identificar y corregir vulnerabilidades, y cómo defenderse frente a ataques en el futuro.

En el grupo de casos prácticos del presente informe, examinaremos cómo 10 proveedores de infraestructura crítica mejoraron las defensas de seguridad antes de que los ciberdelincuentes pudieran robar contraseñas e infiltrarse en redes y aplicaciones. Pero primero presentaremos una vista preliminar de la situación actual de ciberataques y seguridad en 16 industrias de infraestructura crítica identificadas por la Agencia de Ciberseguridad y Seguridad de Infraestructuras de EE. UU. (CISA).



PRODUCTOS FARMACÉUTICOS Y DE CIENCIAS BIOLÓGICAS

Llegar al corazón de una respuesta ante la COVID-19

Las empresas farmacéuticas y de ciencias biológicas se sitúan en el centro de la respuesta ante la COVID-19.

Los ciberdelincuentes siguen aprovechándose de la pandemia para obtener una ganancia comercial mediante la implementación de malware, ransomware, phishing y estafas de URL con el uso frecuente de temas de la COVID-19 y coronavirus como señuelos. A igual que en otras industrias, los actores de amenazas intentan además obtener acceso a la nueva infraestructura de acceso remoto para los empleados que trabajan desde sus casas.

Además, los ataques de estados nación procedentes de países como Corea del Norte, Rusia y China –concebidos para invadir las empresas que desarrollan vacunas contra la COVID-19, productos terapéuticos y dispositivos médicos– están en aumento y se hacen cada vez más sofisticados. Las metas de los ataques incluyen, por ejemplo, el espionaje industrial, el robo de propiedad intelectual y el acceso a información protegida sobre la salud de los pacientes.

Los fabricantes de dispositivos médicos también son el objetivo de los actores de amenazas que intentan penetrar a los equipos médicos portables e implantables. Algunos de estos dispositivos como los marcapasos y monitores de glucosa conectados se vinculan a redes hospitalarias por Internet. Muchos ejecutivos del sector sanitario temen que los dispositivos médicos conectados abran las puertas a ciberatques a hospitales e instalaciones médicas con repercusiones que pueden ser mortales.

En vista de la importancia de lo que está en juego, la Administración de Alimentos y Medicamentos de EE. UU. (FDA), que regula estos dispositivos, ha priorizado la necesidad de actualizaciones para protegerlos debidamente.

EL 85% DE LAS ORGANIZACIONES AFIRMAN QUE TIENEN POCA O NINGUNA VISIBILIDAD DEL ENTORNO DE ICS.

FUENTE: DRAGOS

PETRÓLEO y GAS

La seguridad de los sistema de transporte por tubería y el disparo que se oyó en todo el mundo

Comprensiblemente los ejecutivos del sector de petróleo y gas se preocupan por los ataques de ransomware tras la brecha sufrida por Colonial Pipeline, el sistema de transporte de combustible por tubería más grande de EE. UU. Su preocupación está justificada. El ataque paralizó algunos sistemas empresariales y provocó una escasez de combustible en la región oriental de EE. UU.

Según Bloomberg, los jáquers obtuvieron acceso a las redes el 29 de abril de 2021 mediante una cuenta VPN que ya no se usaba cuando ocurrió el ataque, pero que todavía podía usarse para acceder a la red de Colonial. Por otra parte, un informe reciente descubrió que el 77% de las empresas de energía grandes en EE. UU. reportan la filtración de por lo menos una contraseña para acceso en línea.

Además, los incidentes de seguridad entre las empresas de petróleo y gas están en aumento a medida que digitalizan y conectan los sistemas de tecnología de operaciones (OT) con sistemas de control industrial (ICS) para gestionar las operaciones desde un punto central. En EE. UU., la industria de petróleo y gas constituye el tercer sector más atacado, después de los servicios financieros y la fabricación.

El ataque a Colonial Pipeline pone en relieve la capacidad de los actores de amenazas de irrumpir los sistemas de OT, así como el impacto posiblemente catastrófico de los ataques a los proveedores de infraestructura crítica y, por consiguiente, a la vida cotidiana de los consumidores.

INDUSTRIA AUTOMOTRIZ

El aumento de la conectividad causa nuevas preocupaciones con respecto a la ciberseguridad

En el sector automotriz, los fabricantes de automóviles y de piezas enfrentan un notable incremento en los ataques de ransomware que pueden poner en peligro la seguridad de los sistemas de IT y OT convergentes. Un estudio descubrió que un 49% de los principales fabricantes de automóviles son muy vulnerables a los ataques de ransomware. En muchos casos, estos ataques comienzan con intrusiones en los sistemas de IT que se propagan después a los activos de OT conectados.

Por ejemplo, en un reciente ataque a un fabricante de automóviles global, los ciberdelincuentes llevaron a cabo una campaña de phishing que sembró ransomware en el sistema de IT de la empresa, el cual se propagó a sus activos de OT. El ataque paralizó las plantas de producción en todo el mundo e interrumpió los sistemas de IT y correo electrónico de la empresa.

El ransomware no es la única amenaza que mantiene desvelados a los ejecutivos. Las interrupciones causadas por los ciberataques a proveedores automotrices han dado lugar a problemas en la cadena de suministro que se han extendido a otras industrias y regiones limitando las operaciones y, en algunos casos, cerrando plantas enteras.

PRODUCTOS DE CONSUMO ENVASADOS (CPG)

La frecuencia y los costos de los ciberataques están en aumento

Los incidentes de ciberseguridad a las empresas de CPG están en aumento. Más de un 40% de los fabricantes de CPG sufrieron ciberataques en 2020. Y sus repercusiones financieras son altas y siguen aumentano. El costo promedio de las brechas de datos en el sector de CPG subió a US$3.7 millones en 2021, lo cual representa un aumento de un 42.9% en comparación con el año anterior.

Las tendencias que se espera impulsen un incremento de los requisitos de ciberseguridad incluyen un uso más frecuente de los sensores y dispositivos de la Internet de las cosas (IoT), la creciente disponibilidad de 5G y la convergencia de las redes de IT y OT. Más dispositivos y sistemas operativos conectarán y transmitirán datos a través de las redes, lo cual amplía considerablemente las superficies de ataque.

Para enfrentar los ataques a la cadena de suministro los fabricantes de CPG se han visto obligados a rediseñar la adquisición, ajustar el espacio del almacén y reconsiderar los modelos de entrega, así como reexaminar la viabilidad de sus proveedores.

ALIMENTOS Y BEBIDAS

Los ataques de ransomware se tornan cada vez más destructivos

La industria estaba navegando a través de cambios gigantescos en las preferencias de los clientes en torno a alimentos más saludables y experiencias atrayentes de compra. Por ejemplo, los consumidores más jóvenes tienden a preferir alimentos nutritivos con base vegetal de origen local y distribuidos en envases ecológicos. Simultáneamente, los ciberataques a las empresas de alimentos y bebidas se estaban tornando cada vez más perjudiciales en cuanto a costos y tiempo improductivo.

Y en medio de todo eso, apareció la COVID-19. Las empresas de alimentos y bebidas implementaron rápidamente plataformas de teletrabajo para satisfacer los nuevos requisitos de seguridad, protección y privacidad de los trabajadores. Las empresas descubrieron que sus sistemas y aplicaciones anticuadas eran a menudo incompatibles con las soluciones de ciberseguridad modernas. La necesidad de programas de seguridad actualizados basados en riesgos se hizo más evidente, sobre todo por el aumento de los ataques.

Por ejemplo, el ataque de ransomware a JBS, un procesador de productos cárnicos brasileño, afectó a sus plantas en EE. UU., Canadá y Australia. Los actores de amenazas encriptaron los sistemas y datos de la empresa y exigieron un rescate de millones de dólares para restaurar el acceso. JBS pagó US$11 mil millones. Por otra parte, en los 12 meses previos al ataque a JBS ocurrieron alrededor de 40 ataques adicionales a productores de alimentos, según el diario Chicago Tribune.

Este tipo de campaña de malware resalta la tendencia a atacar específicamente las empresas de alimentos y bebidas que usan los sistemas de IT y OT convergentes para gestionar mejor la producción. Sin la planificación y los controles de ciberseguridad adecuados, esta convergencia puede exponer los sistemas de OT a una gama de ciberamenazas sofisticadas.

Aprenda del éxito de otros

Los siguientes casos prácticos muestran la amplia gama de desafíos experimentados por los clientes de Rockwell Automation. Pero todos comparten elementos en común.

Las mejores soluciones de ciberseguridad de OT –en términos de calidad de la protección, velocidad de implementación y servicio continuo que minimiza el tiempo improductivo y defiende contra los ciberataques– requieren experiencia en operaciones industriales.

Preste atención a desafíos similares a los suyos en estos casos. Sabemos que las perspectivas compartidas en esta recopilación de casos prácticos son intrínsecamente valiosas para conocer los tipos de soluciones que pueden desplegarse para superar las amenazas de OT en varias industrias.

PRODUCTOS FARMACÉUTICOS

Una empresa farmacéutica global obtiene visibilidad en tiempo real en torno a las amenazas del ICS y a los inventarios diarios de activos en 64 sitios globales

Las empresas farmacéuticas han sido desde hace mucho tiempo un objetivo preferido de los ciberdelincuentes sofisticados. Pero la pandemia de COVID-19 ha agudizado la rápida necesidad de un programa de ciberseguridad basado en riesgos.

Un fabricante farmacéutico global necesitaba ayuda para desarrollar un programa de ciberseguridad para sus sistemas de IT y OT. Los activos de OT sin parches estaban aumentando los riesgos de seguridad para las plantas de fabricación y la falta de visibilidad en tiempo real de las amenazas a los controladores hacía casi imposible la detección de malware de OT.

Como agravante de los riesgos, la empresa farmacéutica thText Boxe no había separado mediante segmentación sus redes empresariales de sus redes de la planta industrial, ni había limitado el tráfico y las rutas entre los sistemas de fabricación críticos.

Con miras al futuro, la empresa se dio cuenta de que necesitaba educar a sus equipos en torno a una buena higiene de ciberseguridad a fin de crear mejoras duraderas en la cultura de seguridad.

UN 88% DE LOS LÍDERES DE TECNOLOGÍA MÉDICA DE EE. UU. NO CREEN QUE SUS EMPRSAS ESTÉN PREPARADAS PARA ENCARAR UN INCIDENTE DE CIBERSEGURIDAD.

FUENTE: IRDETO

QUÉ SE IMPLEMENTÓ

Después de evaluar los riesgos, esta gigantesca empresa farmacéutica acudió a Rockwell Automation para dar pasos importantes hacia la madurez de sus protecciones de ciberseguridad mediante la segmentación de redes y el fortalecimiento de la seguridad de punto final y perimetral.

Para empezar, se diseñó y se implementó rápidamente un programa de ciberseguridad de tres fases.

La primera prioridad supuso la separación de las redes lógicas y físicas en 64 sitios globales para ayudar a contener la propagación de amenazas a medida que los ataques alcanzan las redes y sistemas. Además, la empresa aumentó la seguridad de los dispositivos perimetrales para frenar a los actores de amenazas y desplegó una "lista de autorización" de aplicaciones a fin de permitir el uso de aplicaciones solamente si estas habían sido preaprobadas, a fin de proteger los puntos finales.

A continuación, la empresa implementó una suite de servicios de detección de amenazas y llevó a cabo una limpieza de USB para gestionar y monitorear desde un punto central los medios físicos de USB en la red de OT a fin de protegerse contra amenazas o ataques, lanzados ya fuera desde dentro o desde fuera de la red. Los servicios de detección de amenazas también determinan el comportamiento normal de la red que puede usarse como una línea base, y emplear capacidades de monitoreo de amenazas 24/7 a fin de emitir una señal de alerta si se detectan actividades anómalas. Esto ayuda a la empresa a identificar actividades que puedan plantear un riesgo a sus sistemas más rápidamente, o antes de ocurrir los ataques.

RESULTADOS

Rockwell Automation ayudó a la empresa farmacéutica a diseñar e implementar una estrategia de seguridad ampliada a través de los 64 sitios globales en tan solo unos nueve meses. Esto ha mejorado la capacidad de la empresa para defender sus activos de OT e ICS contra las cada vez más sofisticadas ciberamenazas. Ahora la empresa cuenta con una visibilidad uniforme en tiempo real de las amenazas de ICS en toda la empresa global.

LAS CIFRAS HABLAN POR SÍ MISMAS

El rápido desarrollo de defensas sofisticadas contra las ciberamenazas

ALCANCE

- 9 meses de despliegue
- 64 sitios globales

SOLUCIONES

- Plan de ciberseguridad
- Segmentación de la red
- Seguridad de punto final y perimetral
- Detección de amenazas
- Gestión de medios físicos de USB

CIENCIAS BIOLÓGICAS

Un fabricante de dispositivos médicos moderniza su infraestructura de red para mejorar la ciberseguridad de OT y fomentar el crecimiento

Un fabricante de dispositivos médicos estadounidense tenía grandes planes para aumentar sus capacidades de producción global.

Sus previsiones de crecimiento condujeron al requisito de contar con un plan de infraestructura normalizado que pudiera facilitar la expansión de sus esfuerzos de transformación digital y modernizar su infraestructura de OT. La empresa también necesitaba aumentar la ciberseguridad mediante la segmentación de sus redes de IT y OT.

A lo largo de los años, las inversiones en la OT no se habían mantenido al ritmo de la IT y la empresa necesitaba rediseñar los sistemas de IT y OT para fortalecer la protección de ciberseguridad de una empresa digital en evolución y expansión.

La velocidad era esencial. El fabricante de dispositivos necesitaba desarrollar e implementar con rapidez una estrategia centralizada de ciberseguridad y modernización para ayudar a proteger sus redes expandidas y activos digitales. Pero la empresa carecía de los recursos para implementar nuevas capacidades lo suficientemente rápido como para satisfacer los cronogramas de la empresa.

EL 80% DE LOS LÍDERES DE SEGURIDAD GLOBALES OPINAN QUE EL RANSOMWARE ES PELIGROSO Y REPRESENTA UNA CRECIENTE AMENAZA A LA SEGURIDAD PÚBLICA.

FUENTE: WORLD ECONOMIC FORUM

QUÉ SE IMPLEMENTÓ

Rockwell Automation colaboró con el fabricante de dispositivos médicos para desarrollar un amplio plan a fin de evaluar y rediseñar redes, y añadir una zona desmilitarizada industrial (IDMZ) a siete sitios en cuatro regiones globales.

Posteriormente se desarrolló un plan de diseño estándar para la infraestructura virtual de la organización. Primero la empresa segmentó sus redes de IT y OT para proteger mejor los datos que fluyen entre los ambientes. Otra iniciativa clave supuso la creación de una frontera de seguridad digital conocida como IDMZ entre las redes de IT y OT. Esta tecnología emplea controles de seguridad de redes y aplicaciones para gestionar y proteger el flujo de datos entre las zonas.

A lo largo de la iniciativa que duró 12 meses, la empresa necesitaba una perspectiva de los requisitos y costos exactos de la automatización, así como la implementación de redes e IDMZ y normas de diseño de redes uniformes. La empresa colaboró con diversos socios del ecosistema de Rockwell Automation para obtener esta vista y facilitar la implementación, incluyendo Panduit para la instalación y cableado físicos, y nuestros servicios LifecycleIQ para el despliegue global de los sistemas de control supervisorio y adquisición de datos (SCADA).

La empresa implementó asimismo un programa de servicios administrados para monitorear y gestionar sus redes, centros de datos y aplicaciones.

RESULTADOS

La solución logró la meta de la empresa de establecer un plan estándar de infraestructura de redes e IDMZ para facilitar un crecimiento rápido y seguro además de aumentar la capacidad de producción. El plan dio cabida a la estructura adecuada para la implementación por fases de sitios totalmente nuevos, y puede usarse también para modernizar la infraestructura de red de sitios existentes y gestionar de forma remota la expansión de requisitos de red.

El fabricante de dispositivos médicos ahora disfruta de una vista directa de sus gastos de capital (CapEx) para estos requisitos, lo cual permite la planificación y toma de decisiones estratégicas mejoradas y garantiza que se aborde la ciberseguridad a medida que crezca la empresa.

LAS CIFRAS HABLAN POR SÍ MISMAS

Escalado seguro con una infraestructura de red moderna

ALCANCE

- 12 meses de despliegue
- 7 sitios globales

SOLUCIONES

- Diseño y plano de redes
- IDMZ
- Servicios de ciberseguridad administrados

EMPRESA DE ENERGÍA

Una empresa de almacenamiento y transporte por tubería de gas natural refuerza la ciberseguridad en 62 estaciones y terminales de compresores con la detección de amenazas y monitoreo del inventario de activos en tiempo real

A medida que las empresas de petróleo y gas se esfuerzan por evitar el aumento de ciberataques, muchas comprenden la necesidad de implementar un programa de ciberseguridad exhaustivo para proteger sus redes de IT y OT.

Este es el caso con un proveedor estadounidense importante de gasoducto interestatal. La falta de un programa de ciberseguridad unificado dejó a los líderes de la empresa y de IT con una comprensión mínima de las amenazas actuales y futuras al equipo, a las redes y al tiempo productivo de producción. En un momento dado, un actor de amenazas podría filtrar inadvertidamente los activos digitales de la empresa, lo cual podía interrumpir las operaciones, e incluso perjudicar o cerrar la planta y las instalaciones.

Mientras la empresa conectaba los sistemas de IT y OT como parte de su transformación digital, los líderes de la empresa reconocieron la necesidad de centrarse en la implementación de un programa de ciberseguridad basado en riesgo que permitiera a la empresa detectar y responder rápidamente a las ciberamenazas en las redes.

UN 77% DE LAS EMPRESAS DE ENERGÍA ESTADOUNIDENSES IMPORTANTES EXPERIMENTAN POR LO MENOS UNA CONTRASEÑA FILTRADA EN LÍNEA, LO CUAL LAS HACE VULNERABLES FRENTE A LOS ATAQUES.

FUENTE: THE HOUSTON CHRONICLE

QUÉ SE IMPLEMENTÓ

Rockwell Automation ayudó a la empresa de gasoductos de gas natural a diseñar e implementar la base de una protección de amenazas unificada en 62 estaciones y terminales de compresores en Norteamérica.

En colaboración con Claroty, un socio del ecosistema, Rockwell Automation diseñó servicios administrados de detección de amenazas con el monitoreo del inventario de activos para identificar todos los activos de IT y OT en la red de la empresa. Realizar un inventario de activos de la base instalada constituye un paso crítico para exponer las vulnerabilidades de seguridad y desarrollar un plan para bloquear las amenazas internas y externas, lo cual permite una respuesta y una contención más rápidas de los ciberataques. El proveedor de gasoductos también colaboró con Claroty para implementar su solución de monitoreo de amenazas en tiempo real y definir flujos de trabajo para la respuesta a incidentes.

Gracias a las capacidades modernas de detección de amenazas, el proveedor de gasoductos ahora está listo para identificar y responder con rapidez a las amenazas de ciberseguridad tanto en el campo como en los locales de la empresa. Además, desarrolló prácticas recomendadas para el personal a fin de facilitar una clara perspectiva en torno a los requisitos en evolución.

RESULTADOS

Rockwell Automation ayudó a la empresa a completar la creación de una base para una iniciativa de seguridad moderna en aproximadamente 11 meses, lo que representa un lapso muy corto para una misión tan compleja y apremiante. Actualmente, con una visibilidad total de todos los activos digitales en las redes de IT y OT, la empresa ha mejorado su postura de seguridad y puede identificar de manera continua las amenazas de seguridad en tiempo real, y responder rápidamente a los incidentes para disminuir el impacto de las brechas de seguridad.

LAS CIFRAS HABLAN POR SÍ MISMAS

Incorporación de la seguridad en el sistema de transporte por tubería

ALCANCE

- 11 meses de despliegue
- 62 sitios en Norteamérica

SOLUCIONES

- Detección de amenazas administrada
- Monitoreo de amenazas
- Inventario de activos
- Planificación de respuesta a incidentes

PETRÓLEO y GAS

Un proveedor de petróleo y gas disminuyó el riesgo de tiempo improductivo cibernético en un solo mes mediante el uso de la detección de amenazas y la identificación de inventario de activos de red en tiempo real

Las ciberamenazas a los sistemas de petróleo y gas están en aumento a medida que los actores de amenazas asechan al sector de energía con ransomware y otro malware. El ataque a Colonial Pipeline demostró que las brechas pueden interrumpir gravemente los servicios y suministros de infraestructura crítica, y afectar a millones de personas y ocasionar pérdidas financieras considerables.

En paralelo, la COVID-19 ha acelerado el ritmo de la digitalización y la capacidad de teletrabajo de sus empleados, lo cual aumenta aun más los riesgos de seguridad.

Para reducir riesgos, una empresa de energía multinacional necesitaba fortalecer su estrategia corporativa de gestión de riesgos. Un elemento clave incluía la actualización de los sistemas de OT para minimizar los riesgos en caso de un ciberataque.

Además, la empresa sabía que era necesario defender de forma proactiva sus activos digitales mediante la implementación de una plataforma escalable de detección de amenazas que pudiera identificar rápidamente las vulnerabilidades y amenazas potenciales, además de generar perspectivas operativas impulsadas por datos a fin de mejorar la toma de decisiones.

La empresa también necesitaba ayuda con la gestión de costos relacionados con la obsolescencia y modernización, así como la corrección de soluciones incompatibles para diseñar una infraestructura más unificada.

EL 79% DE LAS EMPRESAS DE PETRÓLEO Y GAS HAN REPORTADO UN AUMENTO DE LOS ATAQUES DISRUPTIVOS EN LOS ÚLTIMOS 12 MESES.

FUENTE: EY GLOBAL STATE OF SECURITY SURVEY 2021

QUÉ SE IMPLEMENTÓ

En colaboración con Rockwell Automation, se diseñó y se desplegó un programa completo de detección de amenazas. La solución identifica una línea base de comportamiento de redes normal y proporciona inventarios de activos de redes en tiempo real. Posteriormente, la solución monitorea continuamente actividad para detectar y comunicar comportamiento inusual antes de que las amenazas se conviertan en brechas. La solución de detección de amenazas también proporcionó una profunda comprensión de los sistemas de OT y de la actividad de redes para una mejor toma de decisiones.

Rockwell Automation colaboró con la empresa de energía y con Claroty, su socio del ecosistema, para implementar soluciones de gestión de amenazas en un total de 12 refinerías, 3 instalaciones de midstream (transporte, procesos y almacenamiento), 1 sistema SCADA y 1 consola de gestión empresarial centralizada.

EL 49% DE LAS PRINCIPALES EMPRESAS DE ENERGÍA ESTADOUNIDENSES SUFREN UNA VULNERABILIDAD CRÍTICA DEBIDO A SISTEMAS ANTICUADOS.

FUENTE: BLACK KITE RESEARCH

RESULTADOS

Esta empresa de petróleo y gas tiene ahora una estrategia unificada para proteger las redes de OT e IT contra brechas, incluidos servicios de detección de amenazas y capacidades de inventario de activos, lo cual permite a la empresa detectar, responder y mitigar las amenazas de ciberseguridad a la vez que se reduce la probabilidad de tiempo improductivo a causa de incidentes de ciberseguridad, lo cual minimiza el riesgo de interrupción de la continuidad comercial.

La solución mejoró las capacidades de seguridad en el mes siguiente al despliegue piloto. Actualmente ayuda a los líderes de la empresa a comprender mejor el rendimiento operacional y de personal, reduce la sobrecarga del equipo de seguridad y facilita la toma de decisiones basadas en datos.

LAS CIFRAS HABLAN POR SÍ MISMAS

Minimización de riesgos de interrupción de la continuidad comercial con la detección de amenazas mejorada

ALCANCE

- Piloto de 1 mes
- 17 sitios
- Socio de ecosistema: Claroty

SOLUCIONES

- Detección de amenazas
- Inventario de activos en tiempo real

INDUSTRIA AUTOMOTRIZ

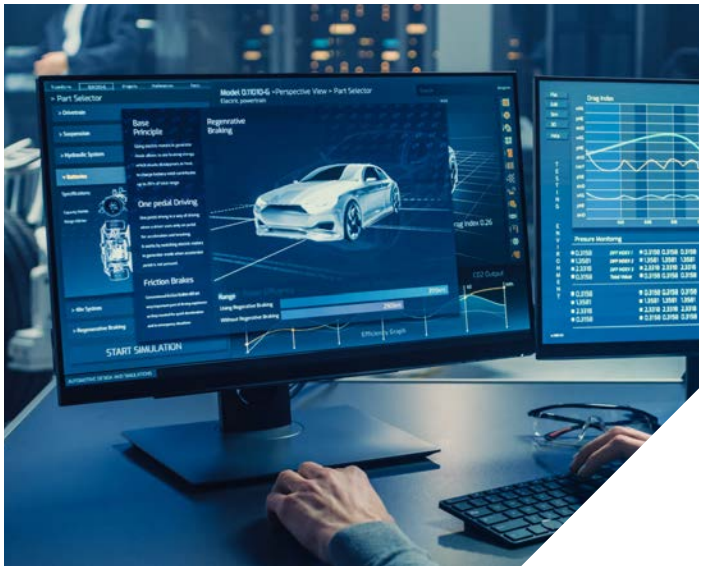
Cómo un fabricante de automóviles evaluó la seguridad de OT para identificar mejoras en tiempo récord

Los fabricantes de automóviles están lidiando con múltiples desafíos a medida que enfrentan la demanda de productos en rápida evolución y un ecosistema cambiante. En medio de unas condiciones caóticas, un fabricante de automóviles global se preocupó de su ciberseguridad insuficiente.

Específicamente, a la empresa le preocupaba que las vulnerabilidades de OT pudieran permitir a los ciberdelincuentes entrar en las redes de IT y OT para robar información sensible e interrumpir las operaciones y las líneas de producción. Aun cuando la empresa había invertido recientemente en la protección de su entorno de fabricación crítico, los líderes de la empresa creían que las redes todavía eran vulnerables a brechas. Y puesto que una gran cantidad de ataques de phishing y ransomware han acosado a empleados individuales, la empresa sabía que la concientización de los empleados en torno a las amenazas ayudaría a reducir los riesgos de ciberseguridad a las infraestructuras de IT y OT de la empresa.

EL 48% DE LOS FABRICANTES DE AUTOMÓVILES SON MUY VULNERABLES A UN ATAQUE DE RANSOMWARE.

FUENTE: BLACK KITE, RANSOMWARE RISK: AUTOMOTIVE MANUFACTURING IN 2021, JUNIO DE 2021



QUÉ SE IMPLEMENTÓ

Rockwell Automation ayudó a la empresa automotriz a evaluar sus capacidades de ciberseguridad mediante el uso de una prueba de penetración, que es un ciberataque simulado a los sistemas, realizado por expertos, para identificar brechas de seguridad.

En este caso, la empresa automotriz quería determinar si los actores de amenazas externos podían infiltrar y tomar control de los ambientes de IT y OT. Gracias a los conocimientos profundos de ciberseguridad de OT del equipo de Rockwell Automation, los servicios de pruebas necesarios se completaron seis meses antes del tiempo que habría tardado un proveedor tercero promedio en completar dichas pruebas.

De hecho, en dos días el equipo descubrió que se había instalado software de control remoto en varias áreas de la planta para permitir a los encargados de seguridad conectarse rápidamente. Nuestros expertos de ciberseguridad colaboraron con el CIO y CISO de la empresa para probar la aplicación y descubrieron la capacidad de establecer una conexión directa procedente de la Internet pública a cada entorno de producción, burlando los perímetros reforzados con cortafuegos.

Dicho de otra forma, durante una prueba de penetración de dos días, Rockwell Automation descubrió que los ciberdelincuentes podían tomar control total de las redes de IT y OT, y obtener acceso a activos digitales, incluidos servidores de interface operador-máquina (HMI) y sistemas de control, planes de fabricación confidenciales, datos de clientes, cámaras de seguridad y hasta contraseñas de usuarios de cuentas de correo electrónico de Microsoft Office 365, incluyendo la del director general.

RESULTADOS

Las pruebas de penetración y evaluación ayudaron a identificar rápidamente varias vulnerabilidades críticas, exponiendo acceso a rutas que podrían permitir a los actores de amenazas controlar los activos y los entornos de producción del fabricante. Ahora los líderes ejecutivos entienden las vulnerabilidades del mundo real y cómo proteger mejor sus infraestructuras de IT y OT. La evaluación condujo a Rockwell Automation a desarrollar un plan de protección completo a la medida de las necesidades del fabricante de automóviles con base en las vulnerabilidades reveladas durante la prueba de penetración. La empresa automotriz tenía previsto ampliar las evaluaciones de seguridad y la corrección de brechas, y ayudar a los empleados a entender la importancia de la buena higiene de ciberseguridad.

LAS CIFRAS HABLAN POR SÍ MISMAS

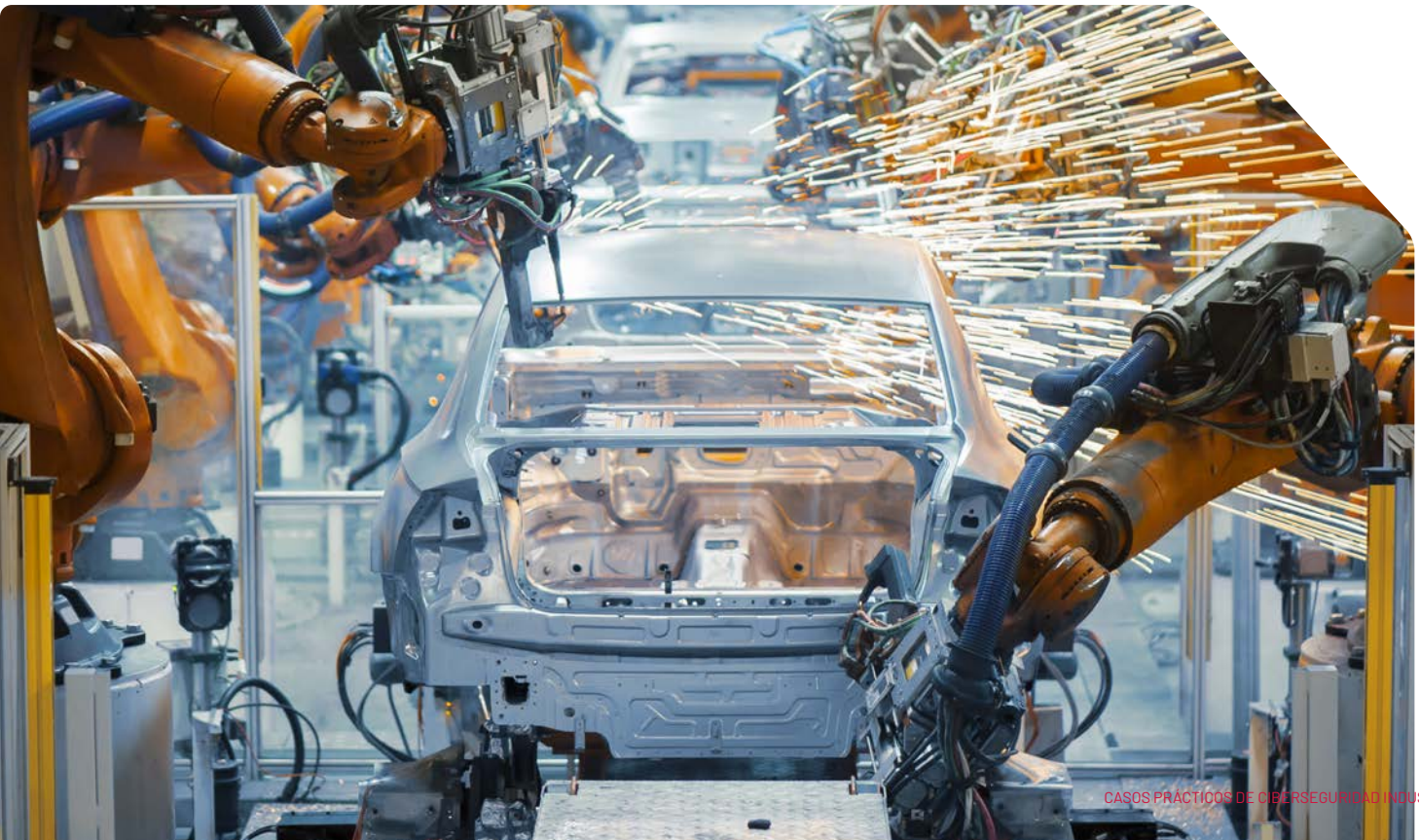
Las pruebas de penetración identifican vulnerabilidades críticas

ALCANCE

- 2 semanas
- 6 sitios

SOLUCIONES

- Pruebas de penetración



PRODUCTOS DE CONSUMO ENVASADOS

Un fabricante de alimentos implementa la gestión unificada de amenazas en 46 sitios globales para alinear la ciberseguridad entre docenas de empresas adquiridas

Aunque algunas empresas de productos de consumo envasados (CPG) han prosperado durante la COVID-19 (por ej., los proveedores de comestibles, alimentos y productos de salud), otras han luchado por mantenerse a flote. Pero las dos enfrentan retos abrumadores. Los ciberataques son cada vez más frecuentes y costosos, los sistemas de OT e IT interconectados pueden poner en peligro los sistemas de control industrial y los requisitos de seguridad pública en evolución exigen agilidad.

Para superar estos obstáculos, un fabricante de alimentos de consumo de Fortune 500 necesitaba una clara comprensión de las vulnerabilidades de ciberseguridad de sus redes de OT e IT. Para complicar las cosas, la empresa había adquirido docenas de empresas de productos alimenticios durante las últimas dos décadas con sus propias tecnologías y ecosistemas de seguridad disímiles.

Como resultado, al fabricante le faltaba una vista centralizada en tiempo real de la seguridad de sistemas en sus 46 sitios de fabricación globales. Lograr la transparencia requeriría una estrategia de seguridad estándar basada en riesgos y capacidades de gestión unificada de amenazas.

EL 43% DEL COSTO PROMEDIO DE UNA BRECHA DE DATOS ENTRE LAS EMPRESAS DE CPG SUBIÓ A US$3.7 MILLONES EN 2021, ES DECIR, UN 42.9% MÁS QUE EN EL AÑO 2020

FUENTE: IBM SECURITY, COST OF A DATABREACH REPORT 2021, JULIO DE 2021

QUÉ SE IMPLEMENTÓ

En colaboración con el director de ciberseguridad de la empresa y con el socio de ecosistema Claroty, Rockwell Automation diseñó e implementó servicios centralizados de detección de amenazas en 46 sitios de fabricación globales. Esto contribuyó a determinar una línea base de actividad de redes y permitió el monitoreo continuo de amenazas en busca de actividad inusual que pudiera indicar ciberataques sin interrumpir las operaciones.

Ahora, si surge una brecha, un flujo de trabajo personalizado ayuda a recuperar los sistemas y redes comprometidos. Además, puesto que la capacitación de empleados es esencial para una seguridad eficaz, se implementó un programa para promover una cultura de higiene de ciberseguridad en toda la planta.

RESULTADOS

Actualmente este fabricante de alimentos ha establecido sistemas de gestión de amenazas centralizados y unificados para ayudar a reducir al mínimo los riesgos de ciberseguridad mediante la ampliación de la visibilidad desde la IT al entorno de OT para detectar y reaccionar ante ciberamenazas antes de que se conviertan en brechas. Los empleados han adquirido una nueva concientización en torno a la ciberseguridad como consecuencia del programa de capacitación a nivel de toda la empresa.

En lo sucesivo, la empresa está posicionada para implementar programas de ciberseguridad uniformes a medida que sigue creciendo mediante adquisiciones futuras.

LAS CIFRAS HABLAN POR SÍ MISMAS

Centralización de la detección de amenazas y minimización de los riesgos de las redes globales de OT e IT

ALCANCE

- 46 sitios globales
- Socio de ecosistema: Claroty

SOLUCIONES

- Servicios de detección de amenazas

ALIMENTOS Y BEBIDAS

Un fabricante de alimentos y bebidas aumenta la ciberseguridad y la respuesta a incidentes, y mejora su puntuación de eficacia del equipo (OEE) en un 5%

Tras un ataque de malware que interrumpió los sistemas de computación y líneas de producción, una empresa de bocadillos necesitaba fortalecer las defensas de ciberseguridad y modernizar su infraestructura de red en 80 sitios en todo el mundo. Previamente había intentado implementar una plataforma de Eficacia Total del Equipo (OEE) para ayudar a medir y mitigar los riesgos de seguridad y mejorar el rendimiento de las aplicaciones existentes. Pero la iniciativa fracasó debido a incompatibilidades entre el software de OEE y los requisitos de redes y de la capa de control de la empresa.

La empresa solicitó la ayuda de Rockwell Automation para crear un inventario global de sus activos digitales y modernizar su respuesta a incidentes y capacidades generales de ciberseguridad.

UN 43% DE AUMENTO DEL COSTO PROMEDIO TOTAL DE UNA BRECHA DE DATOS EN 2021 ENTRE LAS EMPRESAS DE CPG.

IBM SECURITY, COST OF A DATA BREACH REPORT 2021, JUNIO DE 2021

DESAFÍOS

Los tiempos han sido difíciles en el sector de productos de consumo envasados (CPG). Todos están conscientes de los cambios notables de las preferencias de productos y compra, cadenas de suministro globales golpeadas, políticas pandémicas que limitan el tamaño de los grupos de personas y la escasez de trabajadores calificados que se produjeron durante la última década.

Ahora se suma a estos problemas una frecuencia de ciberataques en alza.

QUÉ SE IMPLEMENTÓ

Rockwell Automation colaboró con el director de ingeniería global de la empresa para evaluar sus redes y ayudar a garantizar que los datos necesarios para medir la OEE fueran compatibles con redes y aplicaciones empresariales.

Posteriormente, Rockwell Automation efectuó evaluaciones exhaustivas de la red en todas las instalaciones globales de la empresa e implementó centros de datos industriales (IDC) de interoperación para el monitoreo y gestión remotos de activos digitales. Tras una profunda evaluación, nuestro equipo desarrolló un plan para mitigar los conflictos de redes en la aplicación de OEE e implementar el monitoreo y administración remotos 24/7/365 suministrados por el equipo de asistencia técnica de Rockwell Automation.

RESULTADOS

Una vez implementada la nueva infraestructura de red, este fabricante de bocadillos experimentó en poco tiempo mejoras en la exactitud de datos y la generación de informes global normalizada. Una infraestructura unificada, apareada con nuestros servicios administrados, ayudó a la empresa a reducir el tiempo improductivo, mejorar la exactitud de los datos y responder más rápido a los incidentes de ciberseguridad mediante el uso de contratos de nivel de servicio (SLA).

Todos estos factores ayudaron a la empresa de alimentos y bebidas a incrementar su puntuación de OEE general en un 5%. Incluso una mejora de 1% de OEE puede representar ahorros considerables en una línea de producción grande y puede fomentar además la justificación comercial para fortalecer las defensas de ciberseguridad de OT de la empresa.

LAS CIFRAS HABLAN POR SÍ MISMAS

Mejora de la ciberseguridad y aumento de OEE

ALCANCE

- 80% de sitios globales
- Mejora de un 5% en la eficacia total del equipo (OEE)
- Socio de ecosistema: World Wide Technology

SOLUCIONES

- Soluciones
- Evaluación de la red
- Inventario de activos global
- Despliegue de IDC para montireo y gestión remotos 24/7
- Respuesta a incidentes

ALIMENTOS Y BEBIDAS

Una empresa de alimentos y bebidas agiliza y simplifica la ciberseguridad de OT con servicios de asistencia técnica administrados 24/7

DESAFÍOS

Muchos fabricantes no logran actualizar sus sistemas y software anticuados con el paso del tiempo. Esto puede incrementar el riesgo de ciberataques, ocasionar ineficiencias operacionales que afectan los resultados, y complicar los esfuerzos para lograr una transformación digital.

Esta fue la situación que encaraba un fabricante de alimentos y bebidas global cuando empezó a planificar un proyecto de modernización de varios años. Fue necesario abordar tres retos principales. Una meta clave: agilizar la gestión de sus sistemas de OT críticos e integrar nuevos activos que no se habían implementado de forma uniforme con las anticuadas tecnologías todavía en uso. Sin esta integración, al personal de la empresa le faltaban las destrezas para gestionar de manera coherente los sistemas de OT.

Para complicar las cosas, la demanda de productos alimenticios aumentó con la COVID-19. A los líderes comerciales de la empresa les preocupaba que su infraestructura de tecnología no pudiera resistir al aumento de tráfico, y terminara ocasionando tiempo improductivo y una pérdida de ingresos.

Además, la empresa necesitaba ayuda con la implementación del acceso remoto seguro para protegerse del aumento de incidentes de ciberseguridad a medida que más empleados y terceros empezaban a trabajar desde sus casas. En conjunto, estos factores crearon un ecosistema de tecnología inestable y poco confiable que provocó pérdidas financieras imprevistas. El fabricante necesitaba ayuda para desplegar una gestión uniforme y confiable de sus activos digitales de OT para contribuir a garantizar un tiempo productivo confiable a pesar de los desafíos.

QUÉ SE IMPLEMENTÓ

La empresa de alimentos y bebidas solicitó a Rockwell Automation ayuda para implementar servicios administrados a fin de protegerse mejor contra ciberataques, y crear un entorno operacional estable y eficiente.

Rockwell Automation colaboró con la empresa para diseñar un programa de servicios de asistencia técnica administrados de OT empresarial que admite todos los equipos de infraestructura digital. Se implementaron soluciones adicionales para permitir el despliegue y asistencia técnica coherentes de aplicaciones, software e infraestructura críticos, así como monitoreo remoto 24/7.

Además, Rockwell Automation ayudó a la empresa a desplegar 19 centros de datos industriales (IDC) de OT con una plataforma de detección de amenazas continua para enfrentar los riesgos de ciberseguridad Y para proteger a empleados que trabajaban desde sus casas, diseñamos e implementamos el acceso remoto seguro en 40 sitios en Norteamérica.

RESULTADOS

La infraestructura modernizada y los servicios administrados compatibles permiten a este fabricante reducir las amenazas de ciberseguridad a sus redes corporativas y de OT mediante el monitoreo de amenazas 24/7, lo cual les permite minimizar a la vez los riesgos de tiempo improductivo. El despliegue e integración uniformes de los activos de tecnología han contribuido a incrementar la confiabilidad y mejorar la gestión de aplicaciones y el tiempo productivo de la planta. El despliegue de capacidades de acceso remoto seguro protege a empleados, a terceros socios y a la infraestructura operacional de la empresa frente a ciberriesgos.

Combinadas, estas iniciativas han permitido a la empresa mejorar las eficiencias operacionales y a la vez reducir los costos.

LAS CIFRAS HABLAN POR SÍ MISMAS

Actualizar sistemas anticuados y obtener poderosas protecciones de ciberseguridad

ALCANCE

- 40 sitios
- 19 centros de datos industriales de OT

SOLUCIONES

- Asistencia técnica administrada para todos los equipos de infraestructura digital
- Centros de datos industriales de OT
- Acceso remoto seguro
- Detección de amenazas 24/7

PRODUCTOS DE CONSUMO ENVASADOS

Una empresa de CPG adopta una transformación digital segura y reduce el tiempo de respuesta promedio de la red en un 90%

La COVID-19 aparentemente interminable ha perturbado las operaciones del lugar de trabajo, transformado los hábitos de compra de los consumidores y paralizado las cadenas de suministro globales. Un elemento agravante es un alza precipitada de la frecuencia, gravedad y costo de los ciberataques. Por ejemplo, del 61% de los fabricantes que comunicaron un ciberataque en 2021 según un estudio, un 75% de ellos sufrió interrupciones en sus sistemas.

Un efecto secundario de los retos de la pandemia ha sido la aceleración de los esfuerzos en torno a la transformación digital para superar nuevos desafíos como el teletrabajo y el requisito paralelo de ciberseguridad industrial para proteger nuevas operaciones y redes conectadas.

Como descubrió un fabricante de alimentos y bebidas multinacional, la transformación digital y la ciberseguridad ya no pueden considerarse como dos iniciativas independientes, sino que deben implementarse de forma holística. La empresa creó un plan para lanzar una iniciativa de digitalización centrada en la seguridad para aprovechar los datos en tiempo real generados por sus sistemas empresariales cada vez más digitales. No obstante, primero necesitaba abordar las deficiencias técnicas que se habían acumulado con el paso de los años.

Los sistemas y aplicaciones anticuados del fabricante de alimentos, por ejemplo, eran incompatibles con las plataformas modernas de computación en la nube y de ciberseguridad. Sus redes e infraestructura virtual dispersas no pudieron admitir las tecnologías de analítica de datos críticos e inteligencia artificial. Y una concientización en el área de ciberseguridad y programas de capacitación inadecuados para los empleados contribuyeron a una cultura de mala higiene de seguridad.

EL 61% DE LAS PLANTAS EXPERIMENTARON UN INCIDENTE DE SEGURIDAD EN 2021.

FUENTE: TRENDMICRO, THE STATE OF INDUSTRIAL CYBERSECURITY, MAYO DE 2021

QUÉ SE IMPLEMENTÓ

El fabricante de CPG pidió ayuda a Rockwell Automation para modernizar y unificar sus sistemas de IT y OT, implementar el monitoreo y gestión automatizados de la nueva red, y actualizar las capacidades de ciberseguridad en 44 sitios en Norteamérica. Sin embargo, el fabricante no quería reflejar estos esfuerzos como inversiones en bienes de capital (CapEx).

Rockwell Automation creó e implementó una solución moderna basada en la nube usando nuestra oferta de infraestructura como servicio (IaaS). Nuestro equipo colaboró con la empresa de CPG para diseñar la red de IaaS e implementar capacidades de ciberseguridad, entre ellas la segmentación de redes, gestión de parches de sistemas operativos y soluciones antivirus. Un socio de ecosistema de Rockwell Automation, World Wide Technology, administró la entrega de hardware para la iniciativa. Seguidamente, toda la infraestructura de red y computación fue migrada a un servicio administrado en la OT.

Por otro lado, la empresa desplegó los servicios de asistencia técnica para aplicaciones y asistencia técnica TechConnectSM de Rockwell Automation para poder ofrecer una mejor asistencia 24/7 para aplicaciones e infraestructura, y enviar personal de campo a las plantas para proporcionar asistencia práctica a través del teclado. Si bien los contratos de nivel de servicio (SLA) establecían una respuesta a alertas de IaaS dentro de un lapso de 10 minutos o menos, el promedio del tiempo de respuesta en la práctica era de tan solo 3.5 minutos.

RESULTADOS

Esta solución de transformación digital segura cubrió grandes brechas de ciberriesgos mediante la implementación de una infraestructura de red moderna usando la oferta de infraestructura como servicio, así como una gestión de parches de OT eficaz –un requisito de seguridad notablemente complejo de resolver– y protección antivirus.

Gracias al uso de los servicios de asistencia técnica para aplicaciones de Rockwell Automation, la empresa mejoró el tiempo de respuesta de alarmas y alertas críticas en un 90%, lo que redujo a su vez el tiempo improductivo. el financiamiento de la iniciativa provino de los gastos operativos de la empresa, lo cual le permitió financiar la transformación digital sin tener que echar mano a las reservas de CapEx. El modelo de asistencia técnica global con servicios listos ayudó a abordar la escasez de profesionales de IT y ciberseguridad en sus nuevas operaciones digitales, y preparó a la empresa para el escalado futuro.

LAS CIFRAS HABLAN POR SÍ MISMAS

Transformación digital segura, y tiempo de respuesta mejorado en un 90%

ALCANCE

- 44 sitios en Norteamérica
- El tiempo de IaaS según el SLA de 10 minutos se redujo a un promedio de 3.5 minutos
- Socio de ecosistema: World Wide Technology

SOLUCIONES

- Infraestructura como servicio (IaaS)
- Gestión de parches de OT
- Antivirus
- Asistencia técnica para aplicaciones y asistencia técnica TechConnectSM

PRODUCTOS QUÍMICOS

Una empresa química proporciona a sus empleados acceso remoto seguro para controlar el manejo del sistema de 8000 puntos de E/S durante la pandemia

DESAFÍOS

Mientras la COVID-19 persiste, un número considerable de empleados siguen trabajando desde sus casas. Las empresas de biocombustibles no son una excepción.

Un productor sudamericano de etanol, bioenergía y alimento para ganado necesitaba implementar acceso remoto seguro a las redes de IT y OT de la empresa. Una de las principales prioridades era la implementación de acceso seguro para una iniciativa totalmente nueva con proveedores remotos. Además, la empresa de biocombustibles necesitaba acatar restricciones relativas a la reducción de viajes y facilitar simultáneamente auditorías de todas las interacciones remotas con el sistema de control industrial (ICS).

QUÉ SE IMPLEMENTÓ

La empresa de biocombustibles se asoció con Rockwell Automation para diseñar y desplegar soluciones de seguridad con opciones de fuentes de alimentación eléctrica complejas.

La primera prioridad fue el proyecto totalmente nuevo. Rockwell Automation proporcionó servicios de consultoría para ayudar a la empresa a comprender la compleja gama de opciones de fuentes de alimentación eléctrica que serían apropiadas para lograr las metas del proyecto. Una opción elegida fue Intelligent Packaged Power (IPP) con equipos de alimentación eléctrica de mediano y bajo voltaje integrado en el sistema de control distribuido (DCS) de la empresa.

SE PREVÉ QUE LA DEMANDA GLOBAL DE 28% DE BIOCOMBUSTIBLE CRECERÁ EN UN 28% ENTRE 2021 Y 2026.

INTERNATIONAL EMERGENCY AGENCY, RENEWABLES 2021 ANALYSIS AND FORECAST TO 2026, DICIEMBRE DE 2021

Posteriormente, Rockwell Automation ayudó a la empresa a mejorar el monitoreo centralizado de la información de seguridad mediante la implementación de una solución de un centro de datos industrial (IDC) y capacidades de monitoreo y administración remotos 24/7 para el entorno virtual. Nuestro equipo también diseñó e implementó una zona desmilitarizada industrial (IDMZ) para aislar de manera segura las redes empresariales y los sistemas de control industrial de la empresa.

Las capacidades de acceso remoto y configuración seguros eran también críticas dadas las restricciones de viaje y de distanciamiento social debido a la COVID-19. Esto permitió que la empresa de biocombustibles monitoreara las interacciones de los operadores remotos con el CIS y realizara una auditoría de todas las interacciones remotas con un proveedor clave ubicado a 1,243 millas del sitio. Este enfoque se implementará también con sitios totalmente nuevos en el futuro.

RESULTADOS

Gracias al uso de los servicios del ciclo de vida útil ofrecidos por Rockwell Automation en conjunto con el despliegue de una IDMZ y acceso remoto seguro, la empresa logró satisfacer sus requisitos del proyecto nuevo y redujo a la vez los riesgos de ciberseguridad de las redes corporativas y de OT. Además, la iniciativa simplificó el control y monitoreo de sesiones de acceso remoto de OT e ICS, aumentó la confiabilidad del sistema, mejoró la eficiencia del personal y optimizó la cobertura de asistencia técnica del sistema con monitoreo remoto 24/7.

El equipo de Rockwell Automation también ayudó a la empresa de biocombustibles a mejorar los protocolos de seguridad de los empleados para pandemias actuales y futuras.

LAS CIFRAS HABLAN POR SÍ MISMAS

Despliegue de acceso remoto seguro durante la pandemia

ALCANCE

- 2 sitios
- Socio de ecosistema: Claroty

SOLUCIONES

- Servicios de detección de amenazas

Rockwell Automation: Protegemos las cosas en que confía el mundo

Rockwell Automation ofrece una gama de soluciones y servicios de seguridad industrial para ayudarlo a gestionar las amenazas y aumentar la resiliencia de sus operaciones de OT e IT. Nuestros expertos pueden diseñar una infraestructura de red robusta y segura a la vez que defienden frente a las amenazas y responden rápidamente a los incidentes con monitoreo 24/7. Además de conocimientos profundos y experiencia en las mejores prácticas más recientes, contribuimos con nuestra experiencia en operaciones de fabricación producto de más de 100 años en la automatización industrial.

Nuestras ubicaciones a nivel mundial permiten a los clientes implementar una protección de ciberseguridad coherente a escala global en múltiples sitios con la logística debidamente ajustada que se esperaría del líder de la industria de la automatización industrial.

Recursos que lo ayudarán a dar el primer paso

- Obtenga más información sobre los ataques de ciberseguridad de OT comunes. Vea la presentación de la sesión de la conferencia Automation Fair®: Los principales 10 ataques de ciberseguridad en la OT
- Realice nuestra evaluación de preparación de ciberseguridad y reciba un informe personalizado con una comparación con los encuestados originales. Entérese de cómo se compara su organización según la industria, el tamaño de la empresa y la región.
- Comuníquese con un experto de Rockwell Automation y conozca cómo podemos ayudarlo a seleccionar el programa adecuado de ciberseguridad de OT para proteger mejor sus operaciones industriales.

Conéctese con nosotros.

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

AMÉRICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel.: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPA/MEDIO ORIENTE/ÁFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Bélgica, Tel.: (32) 2 663 0600, Fax: (32) 2 663 0640
ASIA-PACÍFICO: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel.: (852) 2887 4788, Fax: (852) 2508 1846
ARGENTINA: Rockwell Automation S.A., Av. Leandro N. Alem 1050, Piso 5, Ciudad Autónoma de Buenos Aires, Tel.: (54) 11.5554.4040, www.rockwellautomation.com.ar
CHILE: Rockwell Automation Chile S.A., Av. Presidente Riesco 5435, Piso 15, Las Condes, Santiago, Tel.: (56) 2.290.0700, www.rockwellautomation.com.cl
COLOMBIA: Rockwell Automation S.A., Edf. North Point, Carrera 7 N 156-78 Piso 19, PBX: (57) 1.649.9600, www.rockwellautomation.com.co
ESPAÑA: Rockwell Automation S.A., C/ Josep Plà, 101-105, Barcelona, España 08019, Tel.: 34 902 309 330, www.rockwellautomation.es
MÉXICO: Rockwell Automation de S.A. de C.V., Av. Santa Fe 481, Piso 3 Col. Cruz Manca, Deleg, Cuajimalpa, Ciudad de México C.P. 05349, Tel.: 52 (55) 5246-2000, www.rockwellautomation.com.mx
PERÚ: Rockwell Automation S.A., Av. Victor Andrés Belaunde N 147, Torre 12, Of.102, San Isidro Lima, Perú, Tel.: (511) 211-4900, www.rockwellautomation.com.pe
PUERTO RICO: Rockwell Automation, Inc., Calle 1, Metro Office #6, Suite 304, Metro Office Park, Guaynabo, Puerto Rico 00968, Tel.: (1) 787.300.6200, www.rockwellautomation.com.pr
VENEZUELA: Rockwell Automation S.A., Edf. Allen-Bradley, Av. González Rincones, Zona Industrial La Trinidad, Caracas 1080, Tel.: (58) 212.949.0611, www.rockwellautomation.com.ve

Allen-Bradley y expanding human possibility son marcas comerciales de Rockwell Automation, Inc.
Las marcas comerciales que no pertenecen a Rockwell Automation son propiedad de sus respectivas empresas.

Publicación GMSN-AP001A-ES-P-Mayo de 2022

Copyright © 2022 Rockwell Automation, Inc. Todos los derechos reservados. Impreso en EE. UU.