Estudos de caso em cibersegurança industrial

Desafios, soluções e resultados em todos os setores

Sumário

COMPARTILHANDO LIÇÕES APRENDIDAS

Uma mensagem da Rockwell Automation

Caros leitores

Reconhecemos que estes são tempos difíceis para provedores de infraestrutura crítica. Por meio de cibercriminosos implacáveis, iniciativas complexas de transformação digital e uma pandemia aparentemente imparável, muitas organizações estão lutando para proteger os sistemas de Tecnologia Operacional (TO).

A segurança de TO tornou-se cada vez mais importante, pois os atacantes provaram que podem e irão violar os sistemas de TI como um trampolim para a infiltração de TO e sistemas de controle industrial (ICS). Esse tipo de violação, como você verá, também pode derrubar sistemas de TI e infraestrutura crítica.

Se há uma ameaça específica que preocupa os executivos de negócios, é o aumento global de ataques de ransomware. À medida que as tensões aumentam após a invasão da Ucrânia pela Rússia, por exemplo, a Agência de Cibersegurança e Infraestrutura (CISA) alertou os governos estaduais e locais dos EUA e as redes do setor de aviação e energia sobre um risco aumentado de ataques de ransomware da Rússia.

Para agravar a situação, muitas organizações de infraestrutura crítica carecem de recursos automatizados de detecção e resposta a ameaças, como monitoramento contínuo de redes e sistemas. Outros problemas comuns incluem riscos associados à transformação digital, sistemas e aplicativos em obsolescência, ativos digitais desconectados e falta de rede centralizada e de gestão de ameaças.

Além disso, o COVID-19 gerou seus próprios desafios, que incluem a necessidade de recursos seguros de trabalho remoto, além de interrupções operacionais periódicas e colapsos da cadeia de fornecimento.

Você já se perguntou como as empresas lidam com essa imensidão de riscos? Neste resumo dos estudos de caso de clientes da Rockwell Automation, exploramos o que funcionou para outras organizações em vários setores, incluindo farmacêutico, ciências da vida, energia, petróleo e gás, fabricação automotiva, alimentos e bebidas, bens de consumo embalados e indústrias verticais.

Se você está preocupado com as ameaças à sua infraestrutura de TO e ICS, confira as histórias de sucesso a seguir. Nossas equipes experientes ajudaram empresas de vários setores a implementar operações industriais mais seguras. Embora nenhum programa de infraestrutura seja 100% isento de riscos, existem soluções comprovadas que podem reduzir substancialmente os riscos de segurança da infraestrutura crítica de forma eficaz e eficiente.

Kamil Karmali

Gerente Global, Serviços de Consultoria em Cibersegurança

Rockwell Automation

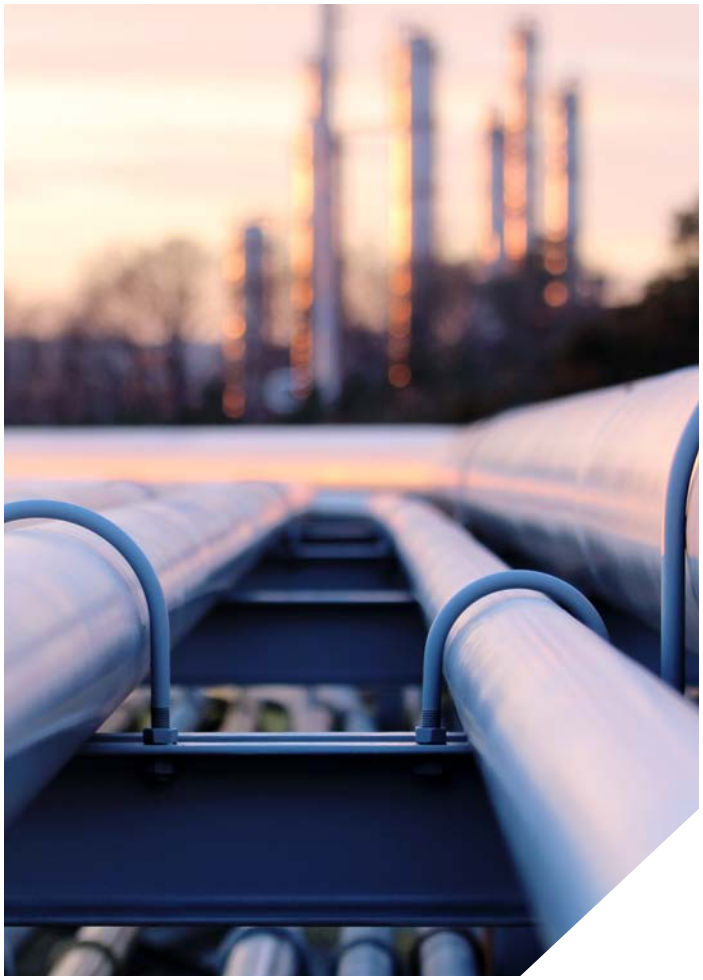
UM RESUMO DO MERCADO

Ameaças à cibersegurança nos setores de TO

O RANSOMWARE CONTINUA CAUSANDO INTERRUPÇÕES

Se a experiência é o melhor professor, o segundo melhor pode ser as lições aprendidas com outras pessoas em seu setor. As organizações violadas por atacantes internos ou externos geralmente aprendem lições valiosas sobre cibersegurança, incluindo como identificar e fechar vulnerabilidades e como se defender contra ataques futuros.

Na amostragem de estudos de caso deste relatório, examinaremos como 10 provedores de infraestrutura crítica melhoraram as defesas de segurança antes que os cibercriminosos pudessem roubar senhas e se infiltrar em redes e aplicativos. Mas, primeiro, veremos o estado atual dos ataques cibernéticos e da segurança em seis dos 16 setores de infraestrutura crítica identificados pela Agência de Cibersegurança e Infraestrutura (CISA).



CIÊNCIAS FARMACÊUTICAS E DA VIDA

Visando o coração de uma resposta ao COVID-19

As empresas farmacêuticas e de ciências da vida estão no epicentro da resposta ao COVID-19.

Os cibercriminosos continuam a explorar a pandemia para obter ganhos comerciais, implantando malware, ransomware, phishing e golpes de URL, geralmente usando temas como COVID-19 e coronavírus como iscas. Assim como em outros setores, os atacantes também tentam obter acesso a uma infraestrutura de acesso remoto nova para funcionários que trabalham em casa.

Além disso, os ataques de estados-nação de países como Coréia do Norte, Rússia e China – projetados para violar empresas que desenvolvem vacinas, remédios e dispositivos médicos contra COVID-19 – estão aumentando com sofisticação crescente. Os objetivos do ataque incluem espionagem industrial, roubo de propriedade intelectual e acesso a informações protegidas de saúde do paciente, por exemplo.

Os fabricantes de dispositivos médicos também são alvo de atacantes que tentam invadir equipamentos de saúde implantáveis e acessórios. Alguns desses dispositivos, como marca-passos e monitores de glicose conectados, conectam-se às redes hospitalares usando a Internet. Muitos executivos do setor de saúde temem que os dispositivos médicos conectados abram uma porta de entrada para ataques cibernéticos em hospitais e instalações médicas, com consequências potencialmente fatais.

Diante de riscos tão altos, a Food and Drug Administration, uma agência federal do Departamento de Saúde e Serviços Humanos dos Estados Unidos que regulamenta esses dispositivos, priorizou a necessidade de atualizações para protegê-los adequadamente.

86% DAS ORGANIZAÇÕES RELATAM POUCA OU NENHUMA VISIBILIDADE DO AMBIENTE ICS.

FONTE: DRAGOS

PETRÓLEO E GÁS

Segurança de oleodutos e o disparo ouvido em todo o mundo

Executivos de petróleo e gás estão compreensivelmente preocupados com ataques de ransomware após a violação do Colonial Pipeline, o maior oleoduto dos EUA. A preocupação é justificada. O ataque desligou alguns sistemas de negócios e causou escassez de gás no leste dos EUA.

Segundo a Bloomberg, os hackers conseguiram entrar nas redes em 29 de abril de 2021 por meio de uma conta VPN, que não estava mais em uso no momento do ataque, mas ainda poderia ser usada para acessar a rede da Colonial. E um relatório recente descobriu que 77% das grandes empresas de energia dos EUA têm pelo menos uma senha vazada online.

Os incidentes de segurança entre empresas de petróleo e gás também estão aumentando à medida que as empresas digitalizam e conectam sistemas de tecnologia operacional (TO) com sistemas de controle industrial (ICS) para gerenciar operações centralmente. Nos EUA, petróleo e gás são o terceiro setor visado com mais frequência, atrás de serviços financeiros e manufatura.

O ataque à Colonial Pipeline ressalta a capacidade dos atacantes de violar sistemas TO, bem como o impacto potencialmente catastrófico de ataques a provedores de infraestrutura crítica – e, por sua vez, na vida cotidiana dos consumidores.

AUTOMOTIVO

O aumento da conectividade gera novas preocupações de cibersegurança

No setor automotivo, montadoras e fabricantes de peças enfrentam crescentes ataques de ransomware que podem colocar em risco a segurança dos sistemas convergentes de TI e TO. Um estudo descobriu que 49% das principais montadoras são altamente suscetíveis a ataques de ransomware. Em muitos casos, esses ataques começam com invasões em sistemas de TI e depois se espalham para ativos de TO conectados.

Em um ataque recente a uma montadora global, por exemplo, cibercriminosos conduziram uma campanha de phishing que implantou um ransomware no sistema de TI da empresa, que se espalhou para seus ativos de TO. O ataque desativou plantas de produção em todo o mundo e interrompeu os sistemas de TI e de e-mail da empresa.

O ransomware não é a única ameaça que mantém os executivos acordados à noite. Interrupções decorrentes de ataques cibernéticos em fornecedores automotivos criaram obstáculos na cadeia de fornecimento que se espalharam por setores e regiões geográficas, restringindo operações e, em alguns casos, fechando fábricas inteiras.

BENS DE CONSUMO EMBALADOS (CPG)

Ataques cibernéticos estão aumentando em frequência e custo

Entre as empresas de CPG, os incidentes de cibersegurança estão aumentando. Mais de 40% dos fabricantes de CPG foram atingidos por um ataque cibernético em 2020. E as consequências financeiras desse comprometimento são altas e crescentes. O custo médio das violações de dados no setor de CPG subiu para US$ 3,7 milhões em 2021, um salto de 42,9% em relação ao ano anterior.

As tendências que devem impulsionar o aumento dos requisitos de cibersegurança incluem o maior uso de sensores e dispositivos da Internet das Coisas (IoT), a crescente disponibilidade de 5G e convergência de rede de TI/TO. Mais dispositivos e sistemas operacionais se conectarão e transmitirão dados pelas redes, expandindo significativamente as superfícies de ataque.

Lidar com os ataques à cadeia de fornecimento também estimulou os fabricantes de CPG a repensarem aquisições, ajustarem o espaço do armazém e reconsiderarem os modelos de entrega, bem como reavaliar a viabilidade de seus vendedores e fornecedores.

ALIMENTOS E BEBIDAS

Ataques de ransomware se tornam mais destrutivos

A indústria estava enfrentando mudanças enormes nas preferências dos clientes por alimentos mais saudáveis e experiências de compra envolventes. Os consumidores mais jovens, por exemplo, tendem a exigir alimentos nutritivos à base de plantas, de origem local e distribuídos em embalagens ecologicamente corretas. Ao mesmo tempo, os ataques cibernéticos aos negócios de alimentos e bebidas estavam se tornando cada vez mais prejudiciais em termos de custos e tempo de parada não programada.

Então veio o COVID-19. As empresas de alimentos e bebidas implementaram rapidamente plataformas de trabalho remoto para atender aos novos requisitos de segurança, proteção e privacidade do trabalhador. As empresas descobriram que seus sistemas e aplicativos em obsolescência eram frequentemente incompatíveis com as soluções modernas de cibersegurança. A necessidade de programas de segurança atualizados e baseados em riscos tornou-se mais óbvia, especialmente com o aumento dos ataques.

Por exemplo, o ataque de ransomware à JBS, uma grande processadora de carnes brasileira, atingiu fábricas nos EUA, Canadá e Austrália. Atacantes criptografaram os sistemas e dados da empresa e exigiram um resgate multimilionário para restaurar o acesso. A JBS pagou US$ 11 bilhões. Além disso, estima-se que 40 ataques adicionais a produtores de alimentos ocorreram nos 12 meses anteriores ao ataque à JBS, de acordo com o Chicago Tribune.

Esse tipo de campanha de malware ressalta a tendência de almejar empresas de alimentos e bebidas que usam sistemas convergentes de TI e TO para gerenciar melhor a produção. Sem planejamento e controles adequados de cibersegurança, essa convergência pode expor os sistemas de TO a uma variedade de ameaças cibernéticas sofisticadas.

Aprenda com o sucesso dos outros

Os estudos de caso a seguir mostram uma ampla gama de desafios enfrentados pelos clientes da Rockwell Automation. No entanto, todos têm elementos em comum.

As melhores soluções de cibersegurança de TO – em termos de qualidade de proteção, velocidade de implantação e serviço contínuo que minimiza o tempo de parada não programada e defende contra ataques cibernéticos – exigem experiência em operações industriais.

Procure desafios semelhantes aos seus nessas histórias. Reconhecemos que os insights compartilhados neste resumo são intrinsecamente valiosos para entender os tipos de soluções que podem ser implantados para superar as ameaças à TO em vários setores.

PRODUTOS FARMACÊUTICOS

Uma empresa farmacêutica global obtém visibilidade de ameaças de ICS em tempo real, além de insights diários de inventário de ativos em 64 locais de todo o mundo

As empresas farmacêuticas há muito são o alvo favorito de criminosos cibernéticos sofisticados. Mas a pandemia do COVID-19 intensificou a necessidade de um programa de cibersegurança baseado em risco, e o quanto antes.

Um fabricante farmacêutico global precisava de ajuda para criar um programa de cibersegurança para seus sistemas de TI e TO. Os ativos de TO sem correção estavam aumentando os riscos de segurança para as fábricas, e a falta de visibilidade em tempo real das ameaças aos controladores ICS tornava praticamente impossível detectar um malware de TO.

Para agravar os riscos, a empresa farmacêutica thText Boxe não havia segmentado suas redes corporativas de suas redes das plantas industriais, nem havia limitado o tráfego e os caminhos de e para sistemas críticos de fabricação.

Olhando para o futuro, a empresa sabia que precisava educar suas equipes sobre uma boa higiene de cibersegurança para criar melhorias culturais de segurança duradouras.

88% DOS LÍDERES DE TECNOLOGIA MÉDICA DOS EUA NÃO ACHAM QUE SUAS EMPRESAS ESTÃO PREPARADAS PARA UM INCIDENTE DE CIBERSEGURANÇA.

FONTE: IRDETO

O QUE FOI IMPLANTADO

Depois de avaliar os riscos, essa gigante farmacêutica fez parceria com a Rockwell Automation, dando passos significativos para o amadurecimento das proteções de cibersegurança por meio da segmentação de rede e fortalecendo a segurança de endpoint e de perímetro.

Para começar, um programa de cibersegurança em três fases foi rapidamente projetado e implementado.

A primeira prioridade envolvia a separação de redes lógicas e físicas em 64 sites globais para ajudar a conter a propagação de ameaças à medida que atingiam redes e sistemas. A empresa também aumentou a segurança dos dispositivos de perímetro para impedir os atacantes e implantou "listas de aplicativos permitidos" para permitir o uso de aplicativos apenas se eles fossem pré-aprovados, para proteger os endpoints.

Em seguida, a empresa implementou um conjunto de serviços de detecção de ameaças e um de limpeza de USB para gerenciar e monitorar de forma centralizada a mídia USB na rede de TO, para proteção contra ameaças ou ataques – de dentro e de fora da rede. Os serviços de detecção de ameaças também determinam o comportamento normal da rede que pode ser usado como avaliação inicial e empregam recursos de monitoramento de ameaças 24 horas por dia, 7 dias por semana, para detectar e levantar um aviso quando atividades anômalas são detectadas. Isso ajuda a empresa a identificar atividades que possam representar um risco para seus sistemas mais rapidamente ou antes dos ataques.

RESULTADOS

A Rockwell Automation ajudou a empresa farmacêutica a projetar e implementar uma estratégia de segurança expandida em 64 sites globais em aproximadamente nove meses. Isso melhorou a capacidade da empresa de defender seus ativos de TO e ICS contra ameaças cibernéticas cada vez mais sofisticadas. A empresa agora tem visibilidade consistente e em tempo real das ameaças de ICS globalmente

SEGUINDO O PLANEJADO

Construindo rapidamente defesas sofisticadas contra ameaças cibernéticas

ESCOPO

- Implantação de 9 meses
- 64 sites globais

SOLUÇÕES

- Plano de cibersegurança
- Segmentação de rede
- Segurança de endpoint e perímetro
- Detecção de ameaças
- Gerenciamento de mídia USB

CIÊNCIAS DA VIDA

Um fabricante de dispositivos médicos moderniza sua infraestrutura de rede para melhorar a cibersegurança de TO e melhorar o crescimento

Text BoxUm fabricante de dispositivos médicos com sede nos EUA tinha grandes planos para acelerar suas capacidades de produção global.

Suas previsões de crescimento levaram à necessidade de um plano de infraestrutura padronizado que pudesse apoiar a expansão de seus esforços de transformação digital e modernizar sua infraestrutura de TO. A empresa também precisava reforçar a cibersegurança segmentando suas redes de TI e TO.

Ao longo dos anos, os investimentos em TO não acompanharam o ritmo de TI, e a empresa precisou projetar novamente os sistemas de TI e TO para fortalecer a proteção de cibersegurança para uma empresa digital em evolução e expansão.

A velocidade era essencial. O fabricante de dispositivos precisava desenvolver e implantar rapidamente uma estratégia centralizada de cibersegurança e modernização para ajudar a proteger suas redes expandidas e ativos digitais. No entanto, a empresa carecia de recursos para implementar novas soluções com rapidez suficiente para atender aos cronogramas da empresa.

80% DOS LÍDERES GLOBAIS DE SEGURANÇA VEEM O RANSOMWARE COMO UMA AMEAÇA PERIGOSA E CRESCENTE À SEGURANÇA PÚBLICA.

FONTE: FÓRUM ECONÔMICO MUNDIAL

O QUE FOI IMPLANTADO

A Rockwell Automation colaborou com o fabricante de dispositivos médicos para desenvolver um plano abrangente para avaliar e projetar novamente as redes e adicionar uma Zona Desmilitarizada Industrial (IDMZ) para sete locais em quatro regiões globais.

Em seguida, foi desenvolvida uma planta de projeto padrão para a infraestrutura virtual da organização. A empresa começou segmentando suas redes de TI e TO para proteger melhor os dados que fluem entre os ambientes. Outra iniciativa importante envolveu a criação de um limite de segurança digital, conhecido como IDMZ entre as redes de TI e TO. Essa tecnologia usa controles de segurança de rede e de aplicativos para gerenciar e proteger o fluxo de dados entre as zonas.

Ao longo da iniciativa de 12 meses, a empresa precisava de uma linha de visão sobre os requisitos e custos precisos de automação, bem como a implementação de rede e IDMZ e padrões consistentes de projeto de rede. A empresa trabalhou com vários parceiros do ecossistema da Rockwell Automation para obter essa visão e dar suporte à implementação, incluindo a Panduit para instalação física e cabeamento e nosso negócio de Serviços LifecycleIQ para implantação global de sistemas de controle de supervisão e aquisição de dados (SCADA).

A empresa também implementou um programa de Serviços Gerenciados para monitorar e gerenciar suas redes, data centers e aplicativos.

RESULTADOS

A solução atingiu o objetivo da empresa de estabelecer uma rede padrão e um modelo de infraestrutura IDMZ para dar suporte a um crescimento rápido e seguro, além de aumentar a capacidade de produção. O projeto forneceu a estrutura certa para a implementação em fases de fábricas novas e também pode ser usado para modernizar a infraestrutura de rede em locais existentes e gerenciar remotamente a expansão dos requisitos de rede.

O fabricante de dispositivos médicos agora tem visão de sua despesa de capital (CapEx) para esses requisitos, permitindo um melhor planejamento estratégico e melhores decisões e garantindo que a cibersegurança seja abordada à medida que a empresa cresce.

SEGUINDO O PLANEJADO

Dimensionamento seguro com uma infraestrutura de rede moderna

ESCOPO

- implantação de 12 meses
- 7 sites globais

SOLUÇÕES

- Projeto e modelo de rede
- IDMZ
- Serviços de cibersegurança gerenciados

EMPRESA DE ENERGIA

Empresa de armazenamento e gasodutos de gás natural aumenta a cibersegurança em 62 estações de compressão e terminais com detecção de ameaças em tempo real e monitoramento de inventário de ativos

À medida que as empresas de petróleo e gás lutam para evitar ataques cibernéticos crescentes, muitas entendem a necessidade de implantar um programa abrangente de cibersegurança para protegerem suas redes de TI e TO.

Esse foi o caso de um grande fornecedor de gasoduto interestadual nos Estados Unidos. A falta de um programa unificado de cibersegurança deixou os líderes corporativos e de TI da empresa com, na melhor das hipóteses, uma compreensão mínima das ameaças atuais e futuras a equipamentos, redes e tempo de disponibilidade da produção. A qualquer momento, um invasor pode se infiltrar nos ativos digitais da empresa sem ser detectado, o que pode interromper as operações e até danificar ou fechar fábricas e instalações.

Como a empresa conectou os sistemas de TI e TO como parte de sua transformação digital, os líderes corporativos reconheceram a necessidade de levar a sério a implementação de um programa de cibersegurança centralizado e baseado em risco que permitiria à empresa detectar e responder rapidamente a ameaças cibernéticas nas redes.

77% DAS GRANDES EMPRESAS DE ENERGIA DOS EUA VAZARAM PELO MENOS UMA SENHA ON-LINE, DEIXANDO-AS VULNERÁVEIS A ATAQUES.

FONTE: THE HOUSTON CHRONICLE

O QUE FOI IMPLANTADO

A Rockwell Automation ajudou a empresa de gasodutos a projetar e implantar a base para proteção unificada contra ameaças em 62 estações de compressão e terminais norte-americanos.

Trabalhando com o parceiro de ecossistema Claroty, a Rockwell Automation projetou serviços gerenciados de detecção de ameaças com monitoramento de inventário de ativos para identificar todos os ativos de TI e TO na rede da empresa. O inventário de ativos da base instalada é uma etapa crítica para expor vulnerabilidades de segurança e desenvolver um plano para bloquear ameaças internas e externas, o que permite uma resposta mais rápida e contenção de ataques cibernéticos. O fornecedor de tubulação também colaborou com a Claroty para implementar sua solução de monitoramento de ameaças em tempo real e definir fluxos de trabalho para resposta a incidentes.

Com recursos modernos de detecção de ameaças, o fornecedor de tubulação agora está pronto para perceber e responder rapidamente às ameaças de cibersegurança no campo e nos locais de negócios. Também desenvolveu melhores práticas da força de trabalho, oferecendo uma visão clara sobre os requisitos em evolução.

RESULTADOS

A Rockwell Automation ajudou a empresa a concluir a base para uma iniciativa de segurança moderna em aproximadamente 11 meses – uma reviravolta rápida para uma missão complexa, mas urgente. Hoje, com visibilidade total de todos os ativos digitais nas redes de TI e TO, a empresa melhorou sua posição de segurança e pode identificar ameaças de segurança continuamente em tempo real e responder rapidamente a incidentes para ajudar a diminuir o impacto das violações.

SEGUINDO O PLANEJADO

Colocando a segurança no percurso

ESCOPO

- implantação de 11 meses
- 62 locais na América do Norte

SOLUÇÕES

- Detecção de ameaças gerenciadas
- Monitoramento de ameaças
- Inventário de ativos
- Planejamento de resposta a incidentes.

PETRÓLEO E GÁS

Uma empresa de petróleo e gás reduz o risco cibernético de tempo de parada não programada em um mês, com detecção de ameaças em tempo real e identificação de inventário de ativos em rede

As ameaças cibernéticas aos sistemas de petróleo e gás estão aumentando à medida que os atacantes visam o setor de energia com ransomware e outros malwares. O ataque à Colonial Pipeline provou que as violações podem interromper gravemente infraestruturas críticas de serviços e suprimentos, afetando milhões de pessoas e causando perdas financeiras significativas.

Paralelamente, a COVID-19 acelerou o ritmo da digitalização, juntamente com a necessidade de os funcionários trabalharem remotamente, aumentando ainda mais os riscos de segurança.

Para reduzir os riscos, uma empresa multinacional de energia precisava fortalecer sua estratégia de gerenciamento de riscos corporativos. Um elemento-chave incluiu a atualização dos sistemas de TO para minimizar os riscos no caso de um ataque cibernético.

A empresa também sabia que precisava defender proativamente seus ativos digitais implementando uma plataforma de detecção de ameaças expansível que pudesse identificar rapidamente vulnerabilidades e ameaças potenciais e gerar informações operacionais baseadas em dados para melhorar a tomada de decisões.

A empresa também precisava de ajuda para gerenciar os custos relacionados à obsolescência e modernização da tecnologia, bem como corrigir soluções inconsistentes de engenharia em uma infraestrutura mais unificada.

79% DAS EMPRESAS DE PETRÓLEO E GÁS RELATAM UM AUMENTO DE ATAQUES DE INTERRUPÇÃO NOS ÚLTIMOS 12 MESES.

FONTE: EY GLOBAL STATE OF SECURITY SURVEY 2.021

O QUE FOI IMPLANTADO

Trabalhando com a Rockwell Automation, um programa abrangente de detecção de ameaças foi projetado e implementado. A solução identifica uma avaliação inicial do comportamento normal da rede, bem como fornece inventários de ativos de rede em tempo real. A solução monitora continuamente a atividade para detectar e relatar comportamentos incomuns, antes que as ameaças se tornem violações. A solução de detecção de ameaças também forneceu uma compreensão profunda dos sistemas de TO e da atividade da rede para melhorar a tomada de decisões em geral.

Trabalhando com a empresa de energia, a Rockwell Automation e a parceira de ecossistema Claroty implementaram soluções de gerenciamento de ameaças para um total de 12 refinarias, 3 instalações intermediárias, 1 sistema SCADA e 1 console de gestão corporativa centralizado.

49% DAS PRINCIPAIS EMPRESAS DE ENERGIA DOS EUA TÊM UMA VULNERABILIDADE CRÍTICA DEVIDO A SISTEMAS DESATUALIZADOS.

FONTE: PESQUISA BLACK KITE

RESULTADOS

Esta empresa de petróleo e gás agora tem uma estratégia unificada para proteger as redes de TO e TI contra violações, incluindo serviços de detecção de ameaças e recursos de inventário de ativos em tempo real, permitindo que a empresa detecte, responda e reduza ameaças de cibersegurança, reduzindo a probabilidade de tempo de parada devido a incidentes de cibersegurança, o que minimiza o risco da continuidade dos negócios.

A solução forneceu recursos de segurança aprimorados no mês após a implantação do piloto. Atualmente, ele ajuda os líderes corporativos a entender melhor o desempenho operacional e da força de trabalho, reduz a sobrecarga da equipe de segurança e oferece suporte à tomada de decisões baseada em dados.

SEGUINDO O PLANEJADO

Minimizando os riscos da continuidade do negócio com detecção de ameaças aprimorada

ESCOPO

- Piloto de 1 mês
- 17 locais
- Parceiro do ecossistema: Claroty

SOLUÇÕES

- Detecção de ameaças
- Inventário de ativos em tempo real

AUTOMOTIVO

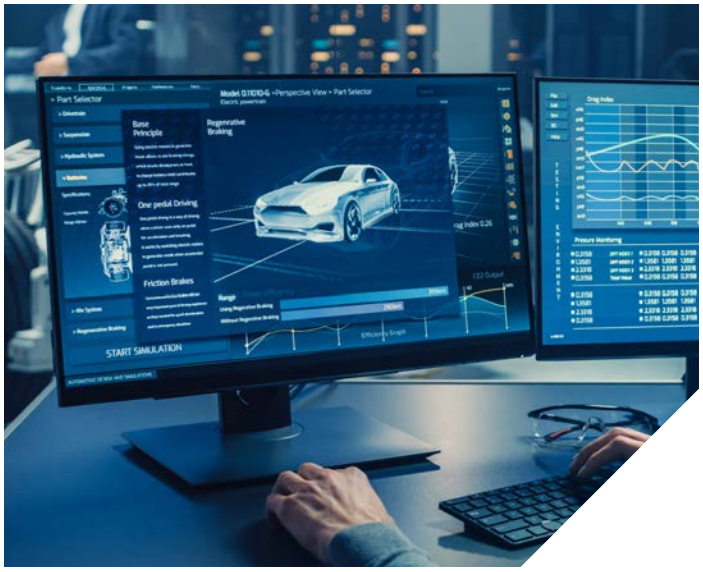
Como um fabricante automotivo avaliou sua segurança de TO para melhorias em tempo recorde

Os fabricantes automotivos estão enfrentando vários desafios à medida que navegam pelas demandas de produtos em rápida evolução e em um ecossistema em transformação. Em meio a condições caóticas, um fabricante automotivo global ficou preocupado com suas deficiências de cibersegurança.

Especificamente, a empresa estava preocupada com o fato de as vulnerabilidades de TO permitirem que cibercriminosos invadissem as redes de TI e TO para roubar informações confidenciais e interromper operações e linhas de produção. Embora a empresa tivesse investido recentemente na proteção de seu ambiente de fabricação crítico, os líderes ainda assim acreditavam que as redes permaneciam vulneráveis a violações. E como uma enxurrada de ataques de phishing e ransomware atingiu funcionários individualmente, a empresa sabia que uma maior conscientização entre os funcionários a respeito das ameaças ajudaria a reduzir os riscos de cibersegurança para as infraestruturas de TI e TO da empresa.

48% DOS FABRICANTES AUTOMOTIVOS CORREM ALTO RISCO DE ATAQUE DE RANSOMWARE.

FONTE: BLACK KITE, RANSOMWARE RISK: AUTOMOTIVE MANUFACTURING IN 2.021, JUNHO 2.021



O QUE FOI IMPLANTADO

A Rockwell Automation ajudou a empresa automotiva a avaliar os recursos de cibersegurança usando testes de penetração – um ataque cibernético simulado em sistemas, realizado por especialistas, para identificar falhas de segurança.

Nesse caso, a empresa automotiva queria determinar se agentes externos poderiam se infiltrar e obter controle dos ambientes de TI e TO. Graças à experiência em cibersegurança de TO da equipe da Rockwell Automation, os serviços de teste necessários foram executados seis semanas mais rápido do que um provedor terceirizado médio.

Na verdade, em dois dias, a equipe descobriu que um software de controle remoto havia sido instalado em várias áreas do chão de fábrica para permitir que os profissionais de segurança se conectassem rapidamente. Nossos especialistas em cibersegurança trabalharam com o CIO e o CISO da empresa para testar o aplicativo e descobriram que era possível se conectar diretamente da Internet pública a cada ambiente de produção, contornando perímetros protegidos por firewalls.

Em outras palavras, em um teste de penetração de dois dias, a Rockwell Automation descobriu que os cibercriminosos poderiam obter controle total das redes de TI e TO e acessar ativos e dispositivos digitais, incluindo servidores e sistemas de controle de interface homem-máquina (IHM), planos de fabricação confidenciais, dados de clientes, câmeras de segurança e até senhas de usuário para contas de e-mail do Microsoft Office 365, incluindo a do CEO.

RESULTADOS

O teste e a avaliação de penetração ajudaram a identificar rapidamente várias vulnerabilidades críticas, expondo caminhos de acesso que poderiam permitir que os atacantes controlassem os ativos e os ambientes de produção do fabricante. Os líderes executivos agora têm uma compreensão real das vulnerabilidades e como proteger melhor suas infraestruturas de TI e TO. A avaliação levou a Rockwell Automation a criar um plano de proteção completo adaptado às necessidades do fabricante automotivo, com base nas vulnerabilidades descobertas durante o teste de penetração. O setor automotivo planejava expandir as avaliações de segurança e a correção de lacunas e ajudar os funcionários a entender a importância de uma boa higiene de cibersegurança.

SEGUINDO O PLANEJADO

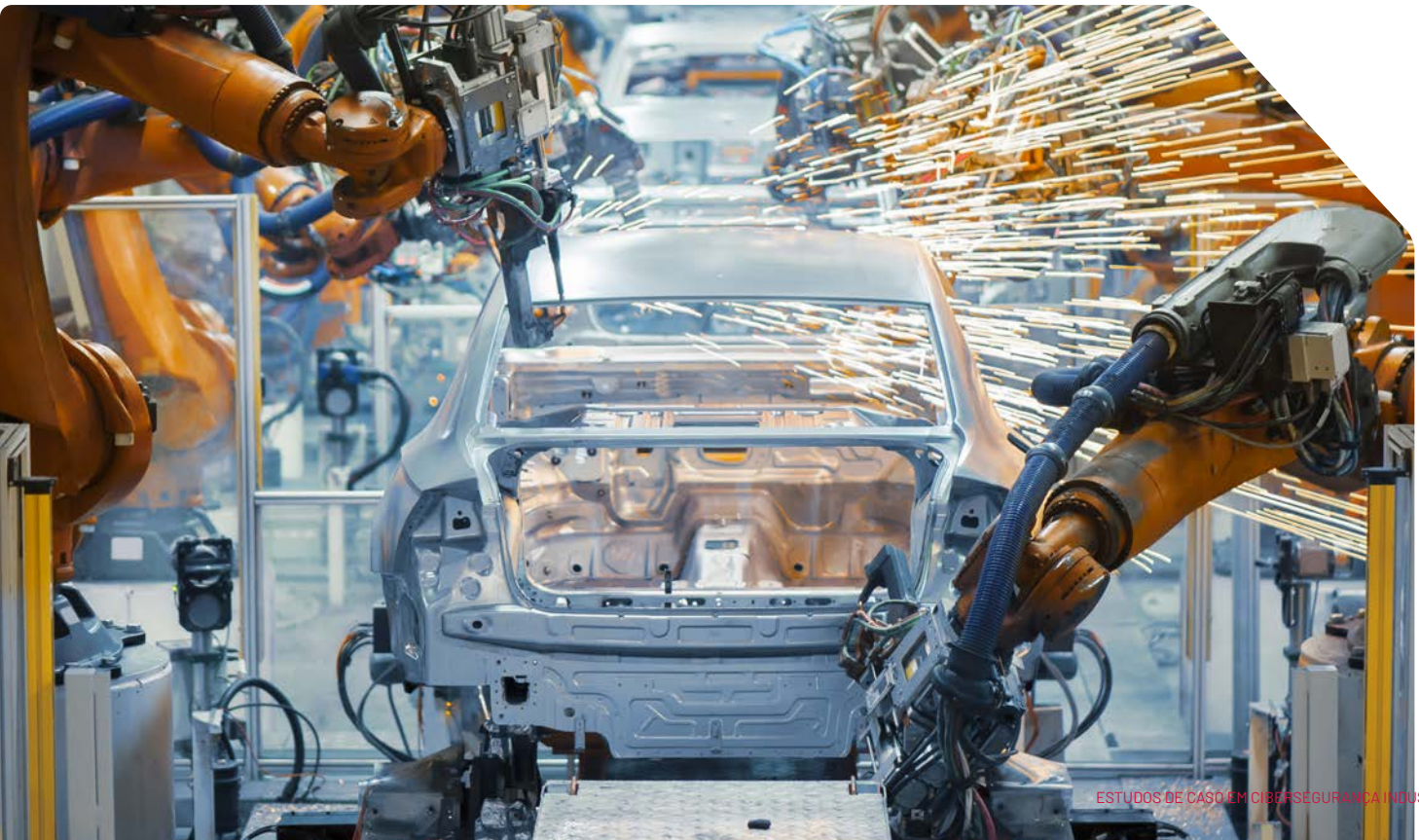
O teste de penetração identifica vulnerabilidades críticas

ESCOPO

- 2 semanas
- 6 locais

SOLUÇÕES

- Teste de penetração



BENS DE CONSUMO EMBALADOS

Um fabricante de alimentos implanta a gestão unificada de ameaças em 46 locais globais, alinhando a cibersegurança entre dezenas de empresas adquiridas

Enquanto algumas empresas de bens de consumo embalados (CPG) floresceram durante o COVID-19 – pense em fornecedores de produtos de mercearia, alimentos e saúde – outras fracassaram. No entanto, ambos enfrentam desafios assustadores. Os ataques cibernéticos são cada vez mais comuns e caros, os sistemas de TO e TI interconectados podem comprometer os sistemas de controle industrial e os requisitos de segurança pública em evolução exigem agilidade.

Para superar esses obstáculos, um fabricante de bens de consumo embalados da Fortune 500 precisava de um entendimento claro das vulnerabilidades de cibersegurança para suas redes de TO e TI. Para complicar as coisas, a empresa adquiriu dezenas de empresas de alimentos nas últimas duas décadas, cada uma com tecnologias e ecossistemas de segurança diferentes.

Como resultado, o fabricante carecia de uma visão centralizada e em tempo real da segurança dos sistemas em seus 46 locais de produção globais. Alcançar a transparência exigiria uma estratégia de segurança padrão baseada em riscos e recursos de gestão unificada de ameaças.

43% O CUSTO MÉDIO DE UMA VIOLAÇÃO DE DADOS ENTRE EMPRESAS DE CPG SUBIU PARA US$ 3,7 MILHÕES EM 2021, UM AUMENTO DE 42,9% EM RELAÇÃO A 2020

FONTE: SEGURANÇA IBM, RELATÓRIO DE CUSTO DE UM DE VIOLAÇÃO DE DADOS 2021, JULHO DE 2021

O QUE FOI IMPLANTADO

Colaborando com o chefe de cibersegurança da empresa e trabalhando com o parceiro de ecossistema Claroty, a Rockwell Automation projetou e implantou serviços centralizados de detecção de ameaças em 46 locais de produção globais. Isso ajudou a determinar uma referência inicial da atividade de rede e permitiu o monitoramento contínuo de ameaças para atividades incomuns que poderiam indicar ataques cibernéticos, sem interromper as operações.

Agora, se ocorrer uma violação, um fluxo de trabalho personalizado ajuda a recuperar redes e sistemas comprometidos. E como o treinamento de funcionários é fundamental para uma segurança eficaz, um programa foi implementado para promover uma cultura de higiene de cibersegurança de toda a empresa.

RESULTADOS

Atualmente, esse fabricante de alimentos possui sistemas de gerenciamento de ameaças centralizados e unificados para ajudar a minimizar os riscos de cibersegurança, expandindo a visibilidade da TI para o ambiente de TO, detectando e agindo sobre ameaças cibernéticas antes que se tornem violações. Os funcionários têm uma nova consciência de cibersegurança resultante do programa de treinamento de toda a empresa.

No futuro, a empresa está posicionada para implementar programas consistentes de cibersegurança à medida que continua a crescer por meio de aquisições futuras.

SEGUINDO O PLANEJADO

Centralizando a detecção de ameaças, minimizando o risco para redes globais de TO e TI

ESCOPO

- 46 sites globais
- Parceiro do ecossistema: Claroty

SOLUÇÕES

- Serviços de detecção de ameaças

ALIMENTOS E BEBIDAS

Um fabricante de alimentos e bebidas aumenta a cibersegurança e a resposta a incidentes, melhora a pontuação de eficiência do equipamento (OEE) em 5%

Após um ataque de malware que interrompeu os sistemas de computação e as linhas de produção, uma empresa global de salgadinhos precisava fortalecer as defesas de cibersegurança e modernizar sua infraestrutura de rede em 80 locais em todo o mundo. Anteriormente, havia tentado implantar uma plataforma de eficiência geral do equipamento (OEE) para ajudar a medir e reduzir os riscos de segurança e melhorar o desempenho dos aplicativos existentes. Mas a iniciativa fracassou devido a incompatibilidades entre o software OEE e a camada de controle empresarial da empresa e os requisitos de rede.

A empresa pediu à Rockwell Automation para ajudar a criar um inventário global de seus ativos digitais e modernizar sua resposta a incidentes e recursos abrangentes de cibersegurança.

AUMENTO DE 43% NO CUSTO MÉDIO TOTAL DE UMA VIOLAÇÃO DE DADOS EM 2021 ENTRE EMPRESAS DE CPG.

SEGURANÇA IBM, RELATÓRIO DE CUSTO DE UM DE VIOLAÇÃO DE DADOS 2021, JULHO DE 2021

DESAFIOS

Os tempos têm sido difíceis no segmento de bens de consumo embalados (CPG). As grandes mudanças da última década nas preferências de produtos e compras, cadeias de fornecimento globais desgastadas, políticas pandêmicas que limitam o tamanho das multidões e a escassez de trabalhadores qualificados não são novidade para ninguém.

Agora adicione a frequência crescente de ataques cibernéticos.

O QUE FOI IMPLANTADO

A Rockwell Automation colaborou com o diretor global de engenharia da empresa para avaliar suas redes e ajudar a garantir que os dados necessários para medir o OEE fossem compatíveis com as redes e aplicativos corporativos.

A Rockwell Automation realizou avaliações de rede abrangentes nas instalações globais da empresa e implementou Data centers industriais (IDCs) interoperáveis para monitoração remota e gerenciamento de ativos digitais. Após uma avaliação detalhada, nossa equipe desenvolveu um plano para reduzir os conflitos de rede com o aplicativo OEE e implementar administração e monitoração remota 24 horas por dia, 7 dias por semana, pela equipe de suporte da Rockwell Automation.

RESULTADOS

Com a nova infraestrutura de rede implantada, esse fabricante de salgadinhos percebeu rapidamente melhorias na precisão dos dados e nos relatórios globais padronizados. Uma infraestrutura unificada, combinada com nossos serviços gerenciados, ajudou a empresa a diminuir o tempo de parada não programada, aumentar a precisão dos dados e responder mais rapidamente a incidentes de cibersegurança usando acordos de nível de serviço (SLAs).

Juntos, esses fatores ajudaram a empresa de alimentos e bebidas a aumentar sua pontuação geral de OEE em 5%. Mesmo uma melhoria de 1% no OEE pode significar uma grande economia de custos em uma grande linha de produção e pode apoiar o plano de negócios para reforçar as defesas de cibersegurança de TO de uma empresa.

SEGUINDO O PLANEJADO

Melhorando a cibersegurança e obtendo maior OEE

ESCOPO

- 80% dos sites globais
- 5% de melhoria na eficiência geral do equipamento
- Parceiro do ecossistema: World Wide Technology

SOLUÇÕES

- Soluções
- Avaliações da rede
- Inventário global de ativos
- Implantação de IDC para monitoramento e gerenciamento remoto 24 horas por dia, 7 dias por semana
- Resposta a incidentes

ALIMENTOS E BEBIDAS

Uma empresa de alimentos e bebidas otimiza e simplifica a cibersegurança de TO com serviços de suporte gerenciados 24 horas por dia, 7 dias por semana

DESAFIOS

Muitos fabricantes falham em atualizar sistemas e software em obsolescência ao longo dos anos. Isso pode aumentar o risco de ataques cibernéticos, criar ineficiências operacionais que prejudicam os resultados e complicar os esforços de transformação digital.

Essa é a situação em que um fabricante global de alimentos e bebidas se encontrava quando começou a planejar um projeto de modernização plurianual. Três desafios principais precisavam ser enfrentados. Um objetivo principal: simplificar o gerenciamento de seus sistemas de TO críticos e integrar novos ativos que não foram implementados de forma consistente com as tecnologias antigas ainda em uso. Sem essa integração, a força de trabalho da empresa carecia de habilidades para gerenciar de forma consistente os sistemas de TO.

Para agravar a situação, a pandemia de COVID-19 estimulou a demanda por produtos alimentícios. Os líderes de negócios da empresa temiam que sua infraestrutura de tecnologia não pudesse suportar o aumento do tráfego, resultando potencialmente em tempo de parada não programada e perda de receita.

A empresa também precisava de ajuda para implementar o acesso remoto seguro para se proteger contra o aumento dos incidentes de cibersegurança à medida que mais funcionários e terceiros trabalhavam em casa. Combinados, esses fatores criaram um ecossistema de tecnologia instável e não confiável que causou perdas financeiras não planejadas. O fabricante precisava de ajuda para implementar um gerenciamento consistente e confiável de seus ativos digitais de TO para ajudar a garantir um tempo de disponibilidade confiável em meio aos desafios.

O QUE FOI IMPLANTADO

A empresa de alimentos e bebidas pediu à Rockwell Automation para ajudar a implantar serviços gerenciados para melhor proteção contra ataques cibernéticos, bem como criar um ambiente operacional estável e eficiente.

A Rockwell Automation trabalhou com a empresa para projetar um programa corporativo de Serviços de suporte gerenciado de TO que dá suporte a todos os equipamentos de infraestrutura digital. Soluções adicionais foram implementadas para permitir implantação e suporte consistentes para aplicativos, software e infraestrutura críticos, bem como monitoração remota 24 horas por dia, 7 dias por semana.

A Rockwell Automation também ajudou a empresa a implantar 19 Data centers industriais (IDCs) de TO com uma plataforma de detecção contínua de ameaças para lidar com os riscos de cibersegurança. E para proteger os trabalhadores em suas casas, projetamos e implementamos acesso remoto seguro em 40 locais na América do Norte.

RESULTADOS

A infraestrutura modernizada e os serviços gerenciados de suporte permitem que esse fabricante reduza as ameaças à cibersegurança em suas redes corporativas e TO por meio da monitoração de ameaças 24 horas por dia, 7 dias por semana, minimizando os riscos de tempo de parada. A implantação e a integração consistentes de ativos de tecnologia ajudaram a aumentar a confiabilidade do sistema e melhorar o gerenciamento de aplicativos e o tempo de disponibilidade da fábrica. A implantação de recursos seguros de acesso remoto protege funcionários, parceiros terceirizados e a infraestrutura operacional da empresa contra riscos cibernéticos.

Combinadas, essas iniciativas permitiram à empresa aumentar a eficiência operacional e, ao mesmo tempo, reduzir custos.

SEGUINDO O PLANEJADO

Atualizando sistema em obsolescência e obtendo poderosas proteções de cibersegurança

ESCOPO

- 40 locais
- 19 Data Centers industriais de TO

SOLUÇÕES

- Suporte gerenciado para todos os equipamentos de infraestrutura digital
- Data Center industrial de TO
- Acesso remoto seguro
- Detecção de ameaças 24 horas por dia, 7 dias por semana

BENS DE CONSUMO EMBALADOS

Empresa de CPG passa por transformação digital segura, reduzindo o tempo médio de resposta da rede em 90%

A aparentemente imparável pandemia de COVID-19 derrubou as operações no local de trabalho, transformou os hábitos de compra dos consumidores e prejudicou as cadeias de fornecimento globais. Para agravar a situação, há um aumento acentuado na frequência, gravidade e custo dos ataques cibernéticos. Considere, por exemplo, que entre os 61% dos fabricantes que relataram um ataque cibernético em 2021 em um estudo, 75% sofreram interrupções do sistema.

Um efeito colateral dos desafios da pandemia tem sido a aceleração dos esforços de transformação digital para enfrentar novos desafios, como trabalho remoto, e o requisito paralelo de cibersegurança industrial para proteger operações e redes recém-conectadas.

Como descobriu um fabricante multinacional de alimentos e bebidas, a transformação digital e a cibersegurança não podem mais ser vistas como duas iniciativas separadas, mas devem ser implementadas de forma holística. A empresa planejou lançar uma iniciativa de digitalização centrada na segurança para aproveitar os dados em tempo real gerados por seus sistemas de negócios cada vez mais digitais. Mas primeiro precisaria resolver as deficiências técnicas acumuladas ao longo dos anos.

Os sistemas e aplicativos em obsolescência do fabricante de alimentos, por exemplo, eram incompatíveis com a computação em nuvem moderna e as plataformas de cibersegurança. Suas redes e infraestrutura virtual distintas não podiam acomodar análise de dados críticos e tecnologias de inteligência artificial. E programas inadequados de conscientização e treinamento em cibersegurança para funcionários contribuíram para uma cultura de higiene de segurança precária.

61% DAS FÁBRICAS SOFRERAM UM INCIDENTE DE SEGURANÇA EM 2021.

FONTE: TRENDMICRO, O ESTADO DA CIBERSEGURANÇA INDUSTRIAL, MAIO DE 2021

O QUE FOI IMPLANTADO

O fabricante de CPG pediu à Rockwell Automation para ajudar a modernizar e unificar seus sistemas de TI e TO, implementar monitoramento e gerenciamento automatizados da nova rede e atualizar os recursos de cibersegurança em 44 locais na América do Norte. No entanto, não queria recorrer ao financiamento via despesas de capital (CapEx) para fazê-lo.

A Rockwell Automation criou e implantou uma solução moderna baseada em nuvem usando nossa oferta de infraestrutura como serviço (IaaS). Nossa equipe colaborou com a empresa de CPG para projetar a rede IaaS e implementar recursos de cibersegurança para incluir segmentação de rede, gestão de patches para sistemas operacionais e soluções antivírus. Um parceiro do ecossistema da Rockwell Automation, a World Wide Technology, gerenciou a entrega do hardware para a iniciativa. Toda a infraestrutura de rede e computação foi então migrada para um serviço gerenciado em TO.

A empresa também implementou os serviços TechConnectsm Support e Application Support da Rockwell Automation para melhorar o suporte de help desk 24 horas por dia, 7 dias por semana para aplicativos e infraestrutura, e para enviar a mão de obra no local para o suporte via computador. Enquanto os acordos de nível de serviço (SLAs) exigiam uma resposta aos alertas de IaaS em 10 minutos ou menos, os tempos de resposta reais eram em média de apenas 3,5 minutos.

RESULTADOS

Essa solução segura de transformação digital fechou grandes lacunas de risco cibernético implementando uma infraestrutura de rede moderna usando a oferta de infraestrutura como serviço, bem como a gestão eficaz de patches de TO – um requisito de segurança notoriamente complexo para resolver – e proteções antivírus.

Usando o serviço Application Support da Rockwell Automation, a empresa melhorou o tempo de resposta para alarmes e alertas críticos em 90%, o que, por sua vez, diminuiu o tempo de parada não programada. O financiamento para a iniciativa veio das despesas operacionais da empresa, o que permitiu financiar a transformação digital sem recorrer às reservas de CapEx. O modelo de suporte pronto para serviços e com suporte global ajudou a lidar com a escassez de profissionais qualificados de TI e cibersegurança em suas novas operações digitais e preparou a empresa para expansões futuras.

SEGUINDO O PLANEJADO

Transformação digital segura, tempo de resposta 90% melhor

ESCOPO

- 62 locais na América do Norte
- O SLA de IaaS de 10 minutos diminuiu para uma média de 3,5 minutos
- Parceiro do ecossistema: World Wide Technology

SOLUÇÕES

- Infraestrutura como serviço (IaaS)
- Gestão de atualizações (patches) de TO
- Antivírus
- Suporte TechConnectsm e suporte a aplicativos

QUÍMICO

Uma empresa química fornece aos funcionários acesso remoto seguro para controle do sistema de controle de 8.000 pontos de E/S durante a pandemia

DESAFIOS

À medida que o COVID-19 persiste, um número significativo de pessoas continua trabalhando em casa. As empresas de biocombustíveis não são exceção.

Um produtor sul-americano de etanol, bioenergia e ração animal precisava implementar acesso remoto seguro às redes de TI e TO da empresa. Uma das principais prioridades foi a implementação de acesso seguro para uma iniciativa totalmente nova com fornecedores remotos. A empresa de biocombustíveis também precisava contornar a ordem de redução nas viagens, ao mesmo tempo em que permitia auditorias de todas as interações remotas com o sistema de controle industrial (ICS).

O QUE FOI IMPLANTADO

A empresa de biocombustível fez parceria com a Rockwell Automation para projetar e implantar soluções de segurança com opções complexas de fonte de alimentação.

A primeira prioridade foi o projeto de fábrica nova. A Rockwell Automation forneceu consultoria para ajudar a empresa a entender a complexa gama de opções de fonte de alimentação que seriam apropriadas para atender aos objetivos do projeto. Uma opção selecionada foi o Intelligent Packaged Power (Energia Inteligente Armazenada – IPP) com equipamentos de energia de média e baixa tensão, integrados ao Sistema Digital de Controle Distribuído (DCS) da empresa.

28% PREVÊ-SE QUE A DEMANDA GLOBAL POR BIOCOMBUSTÍVEIS CRESÇA 28% ENTRE 2021 E 2026.

AGÊNCIA INTERNACIONAL DE EMERGÊNCIA, ANÁLISE E PREVISÃO DE RENOVÁVEIS DE 2021 PARA 2026, DEZEMBRO DE 2021

A Rockwell Automation ajudou a empresa a melhorar o monitoramento centralizado de informações de segurança, implementando uma solução de Data center Industrial (IDC) e monitoramento remoto 24 horas por dia, 7 dias por semana e recursos de administração para o ambiente virtual. Nossa equipe também projetou e implementou uma Zona Desmilitarizada Industrial (IDMZ) para isolar com segurança as redes de negócios e os sistemas de controle industrial da empresa.

O acesso remoto e os recursos de configuração seguros também foram críticos, dadas as restrições de viagens e distanciamento social da COVID-19. Isso permitiu que a empresa de biocombustíveis monitorasse as interações do operador remoto com o ICS, bem como auditasse todas as interações remotas com um fornecedor chave localizado a 2000 km de distância do local. Essa abordagem também será implantada em fábricas novas futuras.

RESULTADOS

Usando os serviços de ciclo de vida da Rockwell Automation, combinados com a implantação de um IDMZ e acesso remoto seguro, a empresa concluiu seus requisitos de projeto de fábrica nova enquanto reduzia os riscos de cibersegurança para redes corporativas e de TO. A iniciativa também simplificou o controle e o monitoramento das sessões de acesso remoto de TO e ICS, aumentou a confiabilidade do sistema, melhorou a eficiência da força de trabalho e melhorou a cobertura de suporte do sistema com monitoramento remoto 24 horas por dia, 7 dias por semana.

A equipe da Rockwell Automation também ajudou o negócio de biocombustíveis a aprimorar os protocolos de segurança dos funcionários para pandemias – presentes e futuras.

SEGUINDO O PLANEJADO

Implantando acesso remoto seguro durante a pandemia

ESCOPO

- 2 locais
- Parceiro do ecossistema: Claroty

SOLUÇÕES

- Serviços de detecção de ameaças

Rockwell Automation: Protegendo aquilo que o mundo depende

A Rockwell Automation oferece uma variedade de soluções e serviços de segurança industrial para ajudá-lo a gerenciar ameaças e aumentar a resiliência de suas operações de TO e TI. Nossos especialistas podem projetar uma infraestrutura de rede robusta e segura, defendendo-se contra ameaças e respondendo rapidamente a incidentes com monitoramento 24 horas por dia, 7 dias por semana. Além da profunda experiência e conhecimento das melhores práticas mais recentes, trazemos a sabedoria em operações de produção de mais de 100 anos em automação industrial.

Nossas localizações em todo o mundo permitem que os clientes apliquem proteções de cibersegurança consistentes em escala global em vários locais com logística tão bem ajustada quanto você esperaria do líder do setor em automação industrial.

Recursos para ajudar você a começar

- Saiba mais sobre ataques comuns de cibersegurança TO. Assista à apresentação da sessão da conferência Automation Fair®: Top 10 Cybersecurity Attacks in TO.
- Faça a Avaliação de preparação para cibersegurança e receba um relatório personalizado, comparado com os entrevistados originais da pesquisa. Veja como sua organização se compara por setor industrial, tamanho da empresa e região.
- Fale com um especialista da Rockwell Automation e saiba como podemos ajudá-lo com o programa certo de cibersegurança de TO para melhor proteger suas operações industriais.

Rockwell Automation

Conecte-se conosco.

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

AMÉRICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 EUA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPA/ORIENTE MÉDIO/ÁFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Bélgica, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
ÁSIA-PACÍFICO: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846
BRASIL: Rockwell Automation do Brasil Ltda., Rua Verbo Divino, 1488 – 1° andar, Chac. Sto Antonio, 04719-904, São Paulo, SP, Tel: (55 11) 5189-9500, www.rockwellautomation.com.br
PORTUGAL: Rockwell Automação, Lda., Av. Prof. Dr. Cavaco Silva, Edificio Ciência II, n.º 11 - 2ºC, Taguspark, Porto Salvo 2740-120, Tel.: (351) 214 225 500, www.rockwellautomation.com.pt

Publicação GMSN-AP001A-PT-P-maio 2022