Rockwell Automation

Assegurando a Quarta Revolução Industrial

A abordagem de Zero Trust para proteger a transformação digital na TO

Introdução

A Transformação Digital é um grande impulsionador de progresso e eficiência e uma mudança econômica que pode impactar profundamente os ritmos de inovação e desenvolvimento das organizações.

Adotar a tecnologia digital para transformar produtos, serviços e negócios envolve obter maior percepção e controle para melhorar a eficiência, geralmente aproveitando novos fluxos de dados. Esses esforços geralmente redefinem as experiências, como a experiência do cliente, e podem incluir mudanças nos modelos operacionais que afetam a segurança dos ativos digitais.

Na Tecnologia Operacional (TO), a Transformação Digital está impulsionando duas grandes mudanças:

- Os sistemas TO estão sendo conectados a redes às quais não estavam conectados antes, a fim de extrair novos dados sobre as operações. Por definição, esses sistemas vivem na "borda" da infraestrutura e, portanto, devem ser implantados, protegidos e gerenciados como endpoints.
- Aplicativos de software ricos em dados estão sendo implantados em ambientes de produção com TO, onde esses novos dados podem ser melhor usados. Podem ocorrer restrições de latência no processamento dos dados, devido ao seu alto volume e largura de banda. Para resolver esse problema, os aplicativos também estão sendo implantados, protegidos e gerenciados no endpoint.

Além disso, as organizações de TO enfrentam vários outros desafios comuns que afetam a segurança e devem ser enfrentados no caminho para a modernização.

1. Os sensores de processo, mesmo os modelos mais novos, não possuem segurança integrada nem senhas. Em um exemplo recente, um fornecedor líder acabou de enviar 3.000 novos sensores para os Emirados Árabes Unidos sem senhas.
2. Os fornecedores de segurança de rede de TI geralmente abordam a segurança nos níveis 2 a 7. Isso funciona para a maioria das redes de TI. Mas as ameaças de TO frequentemente chegam pelo caminho de nível 0 a 1, onde a telemetria não é monitorada e, portanto, as ameaças não são detectadas.
3. A propriedade final da segurança da TO permanece incerta. No papel, os CISOs podem ser os responsáveis, e muitas organizações industriais estão se movendo para atribuir essa responsabilidade aos CISOs. No entanto, os líderes do chão de fábrica são dominam o espaço e normalmente não liberam facilmente o controle para os CISOs, visto que os CISOs geralmente têm uma compreensão limitada das operações do chão de fábrica.
4. As diretrizes de cibersegurança da Transportation Security Administration (Administração para a Segurança dos Transportes – TSA) não abordam sistemas de controle, incluindo sensores. No entanto, sob a Agência de Cibersegurança e Infraestrutura (CISA), a TSA é proprietária de toda a rede de energia.
5. O padrão 1164 do American Petroleum Institute, cibersegurança dos sistemas de controle de tubulação (agosto de 2021) excluiu efetivamente os sensores de processo (cláusula 6.6.5.4 (b) ao declarar: "O inventário não deve incluir instrumentos individuais que não estejam conectados à rede".

Apesar do valor de ferramentas como a ferramenta MITRE ATT&CK e a metodologia CVE, mais trabalho é necessário. Por exemplo, a ferramenta MITRE ATT&CK não aborda sensores de processo e outros dispositivos de campo do sistema de controle, e a metodologia CVE para vulnerabilidades de software não tem contrapartida para hardware do sistema de controle.

Compreender os padrões de hoje – e abordar as lacunas nos padrões que estão evoluindo mais lentamente do que as ameaças à TO – não é para os que possuem coração fraco.

Além disso, para que a Transformação Digital segura seja bem-sucedida, TI e TO devem se comprometer a trabalhar juntos na implantação, segurança e gerenciamento de mudanças de processo. Isso garante que as melhorias de produtividade desejadas sejam realizadas e também sejam seguras, confiáveis e compatíveis.

Obstáculos comuns da transformação digital

Existem razões comuns pelas quais as empresas ficam aquém de suas metas de Transformação Digital. Esses problemas podem ser amplificados ao transformar a TO.

Os sistemas de TO em obsolescência devem se mover da ilha para o continente.

As 'Ilhas de Automação' na infraestrutura de TO tradicional carecem das bases necessárias para permitir o acesso aos dados. Além disso, os ambientes industriais são pouco inventariados, levando a uma falta de noção sobre o que está conectado no ambiente.

Sensores de processo, que são onipresentes como entradas para sistemas de controle e segurança, bem como para decisões do operador, não são inerentemente seguros. Falhas catastróficas podem ocorrer. Muitas vezes, isso significa que a atenção à proteção, que é bem compreendida pelas organizações de engenharia, ultrapassou a atenção à segurança, que é algo que as organizações de engenharia tendem a ver como responsabilidade da organização de TI.

Por sua vez, as organizações de TI tendem a ignorar a segurança do sensor de processo, vendo-a como uma responsabilidade de engenharia fora de seu próprio escopo.

No nível do sensor de processo, no entanto, segurança e proteção são realmente o mesmo problema.

Estratégia desalinhada ou indefinida.

A estratégia de Transformação Digital deve incluir esforços coordenados para definir resultados definidos e mensuráveis para as principais metas de negócios, mantendo a segurança dos ativos digitais críticos usados e garantindo a conformidade com os padrões do setor.

Roteiro não cria valor inicial.

Desenvolver um roteiro de curto e longo prazo para agregar valor a partir da Transformação Digital, guiado por resultados de negócios e não apenas por tecnologia, é uma base essencial para um projeto de sucesso.

Principais partes interessadas dirigindo-se para diferentes objetivos.

A Transformação Digital requer uma mudança na cultura da organização. Deve haver alinhamento entre as mentalidades dos líderes de TI e TO para que os dois grupos das partes interessadas conduzam com sucesso os objetivos de negócios do projeto.

O primeiro passo é identificar e priorizar o que precisa ser protegido na organização – Dados, Ativos, Aplicativos e Serviços (DAAS).

Uma olhada mais de perto nos sensores de processo

Os sistemas em obsolescência que operam há mais de 20 anos geralmente não são projetados para operar em um ambiente IoT com milhares de sensores de processo, o que causa vulnerabilidades de segurança. Sem planejamento e controles adequados, os esforços de modernização podem multiplicar os riscos de cibersegurança.

Por que proteger os sensores de processo é tão importante?

De acordo com um relatório recente: "As ameaças de cibersegurança estão aumentando e, como resultado, a transmissão de dados do sensor pode ser invadida. Como os dados do sensor hackeado afetam [desenvolver] o desempenho do controle deve ser entendido. Uma situação típica pode incluir dados do sensor sendo modificados por hackers e enviados para as malhas de controle, resultando em ações de controle extremas."

Alguns incidentes cibernéticos envolvendo sensores de processo incluem:

- Barragem com defeito, colapso devido a leituras errôneas de baixo nível
- Sensor resultando na liberação de 38 milhões de litros de esgoto não tratado
- A válvula de segurança de alívio em uma usina nuclear não levantou porque o sensor de pressão nunca atingiu seu ponto de referência
- A falha de um sensor de tensão em uma usina de ciclo combinado na Flórida causou uma oscilação de carga de 200 MW na usina que resultou em uma oscilação de carga de 50 MW em New England
- Explosões de tank farm devido a leituras incorretas do sensor de nível
- Avião cai devido a leituras erradas do sensor
- Explosão da refinaria devido a leituras incorretas do sensor.

Sensores de processo sem cibersegurança, autenticação ou registro cibernético tornam impossível saber se incidentes como esses foram atos maliciosos, feitos para parecerem não intencionais.

Três perguntas de segurança importantes precisam ser feitas para entender as vulnerabilidades inerentes aos sensores de processo:

1. Você precisa de uma presença física para comprometer o sensor?
   Não, pode ser feito remotamente.
2. Quanto dano os impactos aos sensores cibernéticos podem causar?
   O calibrador de campo calibra um sensor por vez, mas se conecta de forma insegura à Internet. Os sistemas de gerenciamento de ativos (AMS) têm acesso a milhares de sensores. Enquanto isso, o AMS pode ter conexões inseguras com a Internet e muitas vezes está conectado aos sistemas corporativos Planejamento de recursos da empresa (ERP). Um exemplo real de uma falha catastrófica decorrente de problemas de sensor: Colonial Pipeline.
3. O que acontece quando os dados comprometidos do sensor são enviados para a nuvem para análises de big data, IoT ou aplicativos da Indústria 4.0?
   Presume-se que os dados do sensor não estejam comprometidos.

As organizações de TO precisam lidar com as deficiências do sensor de processo à medida que realizam programas de Transformação Digital seguros, entendendo como os atacantes podem interromper, degradar ou possivelmente danificar e destruir a infraestrutura; quais são os riscos e custos; e quais medidas podem ser tomadas para encerrar as vulnerabilidades.

Zero Trust é uma estratégia disponível para remover o excesso de confiança e risco em torno dos sensores de processo. O Zero Trust fornece visibilidade total e validação contínua da confiabilidade de cada 'entidade' em uma empresa, sejam dados, aplicativos, serviços ou dispositivos, incluindo sensores de processo, começando por assumir um nível de confiança zero.

Planejando a transformação digital segura

Com todos os desafios da Transformação Digital segura que são ampliados em ambientes de TO, não é de admirar que as organizações industriais fiquem para trás de indústrias mais centradas em TI em relação à modernização.

A boa notícia: existem caminhos comprovados para o sucesso.

Alcançar a transformação digital segura em TO envolve algumas estratégias-chave:

- Uma abordagem Zero Trust
- As soluções digitais modernas certas
- Mudança da responsabilidade de propriedade dentro das organizações
- Melhorar os padrões de conformidade em torno de tais ativos comuns e vulneráveis, como sensores de processo. E, em vez dessas melhorias, abordar diretamente as lacunas

Embora cada um desses pontos seja importante, a abordagem Zero Trust é agora o foco desta discussão.

A abordagem Zero Trust

Zero Trust é uma excelente estratégia para implantar tecnologias seguras de Transformação Digital em ambientes industriais. Ele oferece suporte a novas populações de usuários, modelos de envolvimento do cliente, adoções rápidas e novos dispositivos e sensores de IoT e TO à medida que a transformação amadurece – tudo com proteção de cibersegurança.

O Zero Trust é baseado em cinco princípios de projeto que podem ser integrados com as cinco etapas essenciais a seguir, necessárias para conduzir a Transformação Digital segura em uma empresa:

1. Definir ativos e proteger superfícies
2. Mapear fluxos de transação
3. Projeto de arquitetura
4. Aplicar política
5. Realizar monitoramento e manutenção contínuos

Definir ativos e proteger superfícies. Como afirma John Kindervag, criador do Zero Trust: "Zero Trust é uma estratégia para alinhar a estratégia de negócios com as práticas de cibersegurança". Ao focar nos resultados de negócios, a segurança pode ser vista como um facilitador em vez de um inibidor.

O primeiro passo é identificar e priorizar o que precisa ser protegido na organização – elementos de dados, ativos, aplicativos e serviços (DAAS). Os elementos DAAS são altamente críticos para os negócios e cada um é priorizado. Dessa forma, eles são considerados superfícies de proteção, por ex. Controles ICS, redes de TI, bancos de dados de informações de clientes, dados de propriedade intelectual (IP) e assim por diante.

- **Dados**: classifique os dados com base na importância deles para sua organização, no quão valiosos seriam para os hackers e se estão sujeitos a regulamentações. Documentar um plano em torno da governança de dados – em geral e especialmente dentro de uma superfície protegida – significa que a organização pode identificar, classificar, transmitir, reter e descartar dados com controles de segurança eficazes.
- **Aplicativos**: entenda quais aplicativos usam dados confidenciais ou código proprietário que podem ser valiosos para um atacante. O projeto deve ser feito de dentro para fora. Mapeie como os sistemas devem funcionar e como vários componentes do elemento DAAS interagem com outros recursos da rede. Compreender a maneira como o tráfego se move pela rede, específico para os dados na superfície de proteção, ajudará no desenvolvimento de políticas para proteger os dados dentro e entre os aplicativos.
- **Ativos**: crie um inventário detalhado de todos os seus dispositivos – laptops, telefones celulares, equipamentos de fabricação, CLPs, dispositivos IoT como sensores de processo e outros ativos conectados à rede – para que você saiba o que incluir em sua superfície de proteção.
- **Serviços**: Identifique todos os serviços de rede críticos para os negócios que precisam ser protegidos, como Active Directory, DHCP e e-mail. As contas de serviço em geral devem ter comportamentos conhecidos e privilégios de conexão limitados. Eles nunca devem tentar acessar diretamente um controlador de domínio ou sistema de autenticação, e quaisquer anomalias de comportamento devem ser rapidamente identificadas e informadas aos superiores à medida que ocorrem.

Ao focar as defesas de cibersegurança em cada superfície protegida, priorizadas por sua importância para a organização, podem ser criados perímetros defensáveis que são ordens de grandeza menores e mais gerenciáveis do que a superfície de ataque empresarial usual, que pode ser considerada como toda a Internet.

Cada organização encontrará vários projetos de transformação digital e as superfícies de proteção que os acompanham. Começar com uma iniciativa de transformação inicialmente menor, mas estratégica, impactante e mensurável pode dar à organização experiência na implementação de cibersegurança Zero Trust e uma estrutura para o sucesso de projetos posteriores.

Mapear fluxos de transação. Ambientes industriais geralmente são mal inventariados em termos de ativos de rede, levando a vulnerabilidades em relação ao que deveria estar – e o que realmente está – conectado no ambiente. Esses sistemas muitas vezes cresceram organicamente, produzindo lacunas frequentes no conhecimento de projeto; ou ocorre de dispositivos que se presume que são seguros poderem fornecer pontos não protegidos de entrada de internet para as redes.

Para projetar adequadamente uma rede, você deve projetá-la de dentro para fora. É fundamental entender como os sistemas devem funcionar e como vários componentes DAAS interagem com outros recursos na rede. Ao mapear fluxos de tráfego e interdependências, documentar como recursos específicos interagem uns com os outros e trabalhar essas interdependências em políticas e controles de segurança, você pode determinar os tipos e níveis de proteção necessários.

O mapeamento de fluxos de transações e interdependências DAAS, especificamente em relação a qualquer coisa que se cruze com suas superfícies de proteção, permite melhores proteções sem interromper acidentalmente quaisquer aplicativos, serviços ou fluxos de trabalho relacionados. Também fornece maior compreensão e informações necessárias para decisões mais informadas na próxima etapa.

Projeto de arquitetura. Com a superfície de proteção definida e os fluxos mapeados, a arquitetura Zero Trust necessária normalmente se apresentará.

As melhores práticas de Zero Trust exigem que os controles de segurança sejam colocados o mais próximo possível dos elementos DAAS que estão sendo protegidos. Caso contrário, a arquitetura Zero Trust não é baseada em algum modelo universal. Em vez disso, ela utiliza vários tipos de ferramentas e políticas de cibersegurança, específicas para cada superfície de proteção, para atingir seus objetivos. As organizações devem implantar e integrar uma combinação de recursos que aprimoram o gerenciamento de identidade e acesso, controles de acesso, segmentação de rede, microperímetros e muito mais, conforme exigido pelo elemento DAAS em cada superfície protegida.

O design da rede Zero Trust deve, portanto, ser baseado em como as transações fluem através de uma rede, de e para os elementos DAAS da superfície de proteção e levar em consideração como os usuários e aplicativos acessam os dados de superfície. Com um fluxo otimizado em mente, é possível tomar decisões sobre onde a segmentação e os microperímetros devem ser colocados, usando dispositivos físicos e/ou virtuais.

Aplicar política. Nesta quarta etapa, as regras de política são escritas para o gateway de segmentação com base no comportamento esperado dos dados e no usuário ou aplicativos que interagem com esses dados.

Uma vez que a equipe de projeto tenha determinado o fluxo de tráfego ideal, a próxima etapa é determinar como aplicar o controle de acesso e as políticas de inspeção no gateway de segmentação. A política deve começar com uma abordagem mais geral e tornar-se

mais específica à medida que surge uma maior compreensão das necessidades do usuário e dos requisitos de negócios, à medida que a Transformação Digital amadurece e a visão de negócios se desenvolve.

Um princípio-chave do Zero Trust é limitar o acesso a uma base de conhecimento essencial – o princípio do menor privilégio – e a aplicação estrita desse controle de acesso. Para definir essas regras, a equipe de projeto deve ter uma compreensão detalhada de quais usuários têm acesso a quais dados, juntamente com as informações contextuais.

Não é mais suficiente saber o endereço de origem, o endereço de destino, a porta e o protocolo. As equipes de segurança precisam entender a identidade declarada do usuário, bem como o aplicativo, que geralmente servirá como um proxy para o tipo de dados no gateway de segmentação moderno.

Para que um recurso converse com outro, uma regra específica deve permitir esse tráfego. O desenvolvimento dessa regra implica responder ao seguinte:

- Quem deve ter acesso? Isso define a "identidade declarada".
- Qual aplicação para qual recurso? Qual aplicativo a identidade declarada está usando para acessar um recurso dentro da superfície de proteção?
- Quando o usuário deve ter acesso? Quando é feita a tentativa de acesso ao recurso?
- De onde eles devem ter acesso? Onde está o destino do pacote de dados?
- "Por que estamos fazendo isso?" Por que este pacote está tentando acessar este recurso dentro da superfície protegida? Isso está relacionado à classificação de dados, em que os metadados absorvidos automaticamente das ferramentas de classificação de dados ajudam a tornar sua política mais específica.
- Como devemos protegê-lo? Para protegê-lo, você deve entender como a identidade declarada de um pacote está acessando a superfície de proteção por meio de um aplicativo específico.

Realizar monitoramento e manutenção contínuos. Este é o quinto passo na implementação da abordagem Zero Trust.

Esse processo iterativo significa examinar continuamente todos os logs internos e externos por meio da Camada 7, com foco nos aspectos operacionais do Zero Trust. Ao enviar o máximo de telemetria possível sobre o ambiente, novos insights serão obtidos sobre como melhorar a segurança e a eficiência ao longo do tempo, bem como desenvolver insights úteis para transformar novas áreas.

Os ambientes de tecnologia estão sujeitos a inúmeras ameaças. As empresas devem manter uma capacidade de monitoramento contínuo para garantir que estejam cientes do que está ocorrendo em seus ambientes. Então, quanto mais uma rede for atacada, mais forte ela se tornará, pois irá tornar as políticas mais seguras e informar projetos iterativos com ajustes arquitetônicos que aumentam ainda mais a segurança.

Normas de Segurança Industrial

As indústrias de TO são guiadas por quatro padrões de segurança primários.

- IES 62443 – Segurança de Sistemas de automação e controle industriais (IAC)
- Departamento de Segurança Interna/Equipe de Resposta de Ciberemergência de Sistemas de Controle Industrial (ICS-CERT)
- NIST 800-82 Industrial – Instituto Nacional de Padrões e Tecnologia
- Departamento de Segurança Interna/Laboratório Nacional de Idaho

Cada um é baseado em uma arquitetura de segurança de defesa em profundidade que, por si só, possui vulnerabilidades. Além do mais, esses padrões não são realmente uma estratégia, são mais uma implantação de táticas para lidar com vulnerabilidades pontuais específicas por meio de um controle ou solução de produto, com base no conceito de Zona Industrial Desmilitarizada (IDMZ) – um limite, buffer ou rede isolada ("air gap") dentro uma instalação de fabricação ou processo entre os sistemas de negócios da organização e os sistemas de controle industrial com diferentes requisitos de segurança e sem compartilhar confiança inerente um no outro.

A Transformação Digital altera o fator de confiança para ambos os sistemas. A confiança, hoje, deve ser observadora, contextual e adaptativa para que a interação dos novos modelos de negócios desenvolvidos por meio da Transformação Digital seja bem-sucedida e forneça os resultados positivos esperados.

A Rockwell Automation se alinha ao padrão de segurança IEC 62443 Industrial Automation and Control Systems (IACS – Automação industrial e Sistemas de Controle), bem como à abordagem Zero Trust. Os princípios de projeto Zero Trust mapeiam bem os requisitos da IEC 62443, simplificando a conformidade e fortalecendo as defesas contra um ambiente de ameaças em constante evolução.

Resumo

A transformação digital segura da TO pode alavancar o Zero Trust como uma estrutura fundamental para garantir que os projetos de transformação sejam lançados com a proteção de cibersegurança adequada.

Tanto a Zero Trust quanto a Transformação Digital Segura são jornadas que devem ser implementadas de forma incremental. Como a Transformação Digital altera o fator de confiança entre os sistemas de controle industrial e os sistemas de negócios, um plano para alcançar uma Transformação Digital segura deve ser executado usando estratégias complementares para alcançar uma melhor eficiência e maior produtividade, com total visibilidade e aplicação da cibersegurança que se estende por todos os pontos da conexão na rede.

O planejamento de um projeto inicial de Transformação Digital Segura e a identificação, priorização e proteção dos elementos DAAS em cada superfície de proteção do projeto ajudará a organização a obter valor inicial de seus esforços e estabelecer um padrão de proteções de cibersegurança para proteger a organização durante a transformação.

Reúna tudo

A Rockwell Automation é altamente qualificada em Transformação Digital Segura em ambientes de TO complexos. Conte com nossa experiência para ajudá-lo a projetar, implementar e monitorar os projetos de sua organização para obter maiores recompensas operacionais, garantindo que as proteções corretas de cibersegurança estejam em vigor desde o planejamento até a produção.

Tome providências

Saiba mais sobre transformação digital CPG.

Saiba mais sobre Zero Trust em cibersegurança de TO.

Fale com um especialista sobre como começar.

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-WP003A-PT-P – maio de 2022