DO CAOS AO CONTROLE:

O ARTIGO TÉCNICO DE CIBERSEGURANÇA DEFINITIVO PARA OPERAÇÕES RESILIENTES

Descubra segredos de cibersegurança industrial com nosso guia definitivo. Aprenda estratégias baseadas em NIST para construir sistemas de TO resilientes, reduzir o tempo de parada não programada e proteger suas operações.

RA SecureOT

Introdução

Operações industriais – como o chão de fábrica, centrais elétricas, refinarias e instalações de tratamento de água em expansão – mantêm nosso mundo moderno funcionando 24 horas por dia. Nos últimos dez anos, muitos desses locais começaram a mesclar sua tecnologia operacional (TO) com redes empresariais, plataformas de nuvem e soluções de acesso remoto. A recompensa é enorme: monitoração de dados em tempo real, supervisão centralizada e cronogramas de manutenção mais precisos. No entanto, essa integração mais rígida também multiplica os riscos. Grupos de ransomware, invasores afiliados a Estados e cibercriminosos comuns agora estão se concentrando em sistemas industriais recém-conectados à rede.

Um gigante global de papel e embalagem descobriu isso da maneira mais difícil. Mesmo com 30 usinas e 300 fábricas de caixas em todo o mundo, eles não investiram na segmentação de suas redes de TO, então, quando o ransomware achou uma brecha, ele bloqueou as principais máquinas. A produção parou por dias, as perdas financeiras aumentaram e mais de 85.000 toneladas de produtos nunca chegaram aos clientes, um golpe constrangedor para compartilhar com os principais clientes.

Sob pressão, a empresa fez mudanças abrangentes em sua postura geral de segurança, retrabalhando tudo, desde a arquitetura de rede até as operações diárias, para garantir que qualquer ataque futuro não os atingiria de forma tão impactante. A produção logo retornou ao normal, e a liderança respirou aliviada, sabendo que havia reforçado as principais defesas.

Infelizmente, esse cenário não é único. O Global State of Industrial Cybersecurity (2023) da Claroty relata que 61% dos operadores pesquisados encontraram pelo menos uma invasão de ransomware de TO no ano passado. Outro número preocupante do estado de ransomware da Sophos (2023) coloca o custo médio de violação em torno de US$ 1,85 milhão, levando em consideração os pagamentos de resgate e o tempo de parada não programada. Números como esses muitas vezes mantêm supervisores de fábrica e a segurança acordados à noite, porque ignorar lacunas conhecidas de TO em um mundo hiperconectado é como ficar de pé em um barril de pólvora, apenas esperando para explodir.

Então, como as organizações podem se proteger contra essas ameaças? Este artigo propõe uma abordagem voltada para o futuro para proteger a TO e reduzir o tempo de parada não programada. Fundamentado pelos seis pilares principais do framework de cibersegurança NIST – Identificar, Proteger, Detectar, Responder, Recuperar e Governar – ele combina exemplos do mundo real, conselhos práticos e melhores práticas comprovadas.

O objetivo é direto: ajudar os profissionais de TO e os gerentes de segurança a sair da perpétua resposta a crises para uma postura de segurança mais confiante e resiliente, defendendo os sistemas industriais que alimentam nossas vidas diárias.

Tempo de parada não programada e crescentes ameaças de TO

O tempo de parada não programada é uma grande preocupação para os gerentes industriais e, é completamente compreensível. Até mesmo uma única hora ociosa pode custar centenas de milhares, ou às vezes milhões, de dólares. De acordo com a Deloitte & MAPI (2021), alguns fabricantes da Fortune 500 podem perder mais de US$ 50 milhões por hora em condições extremas se a produção parar. Enquanto isso, na montagem automotiva, uma pequena parada pode custar cerca de US$ 22.000 por minuto — cerca de US$ 1,32 milhão por hora (ARC Advisory Group, 2022). Os fornecedores de energia enfrentam seus próprios problemas: se a rede falhar, eles podem perder US$ 2,48 milhões por hora (Pingdom, "Custo do tempo de parada", 2023), além de quaisquer multas que possam ocorrer quando os reguladores intervirem.

Mas esses valores em dólares são apenas parte da história. Quando a produção para, as cadeias de fornecimento deixam de funcionar e os clientes insatisfeitos começam a procurar outro fornecedor. Uma única oscilação em uma grande empresa com vários locais pode bagunçar cronogramas cuidadosamente planejados, enquanto empresas menores podem ter que correr atrás de um financiamento de emergência, ou arriscar perder clientes-chave, se não puderem se recuperar rápido o suficiente.

TO sob ataque

No passado, os cibercriminosos estavam visando principalmente os sistemas corporativos de TI, coletando informações pessoais, registros financeiros ou outros dados confidenciais. Mas, com a fusão de TO e TI, eles têm se voltado para algo ainda maior: máquinas físicas reais. Se um agente de ataque sequestrar um controlador lógico programável (CLP) ou uma interface homem-máquina (IHM), ele pode causar interrupção nas linhas de produção ou bagunçar a qualidade do produto. Os grupos de ransomware aproveitam essa vantagem criptografando o software de controle principal ou bloqueando os operadores totalmente até que sejam pagos.

O phishing (apropriação de identidade) é geralmente a porta de entrada. O Relatório de Investigações de Violações de Dados da Verizon (2023) revela que a engenharia social está envolvida em 90% das violações. Um único engenheiro ou terceirizado com privilégios remotos pode abrir um arquivo mal-intencionado, dando aos invasores acesso a redes que nunca foram destinadas aos olhos externos. A partir daí, a segmentação limitada e os protocolos antigos permitem que as ameaças se movam lateralmente pelos ambientes de produção, assumindo o controle de um sistema após o outro.

Posturas de segurança reativas

Embora essas ameaças não sejam secretas, muitas organizações ainda operam em um modo reativo quando se trata de segurança de TO. De acordo com a IDC Manufacturing Insights (2024–2025), os orçamentos para cibersegurança industrial geralmente crescem apenas após uma grande crise ocorrer. Esse padrão leva a um ciclo de correções apressadas e guiadas pelo pânico. As lacunas críticas passam despercebidas até que uma violação real force todos a agir. Nesse momento, as consequências financeiras e de reputação podem ser enormes.

O cenário da TO: por que ela possui uma vulnerabilidade diferente

A tecnologia operacional moderna abrange todo o hardware e software que alimentam os processos do mundo real — pense em CLPs, sistemas de controle distribuído (SDCD), plataformas SCADA, sensores, atuadores e muito mais. No passado, essas montagens geralmente permaneciam isoladas, raramente ligadas à empresa como um todo. Agora, graças às demandas por dados em tempo real, diagnósticos remotos e conectividade da cadeia de fornecimento, as redes de TO estão se misturando com as infraestruturas de TI. Essa mudança combina protocolos Fieldbus mais antigos com protocolos baseados em IP, conectando efetivamente máquinas com décadas de idade em ambientes modernos e orientados por nuvem que não foram projetados para isso.

Dispositivos em obsolescência

Muitos controladores industriais foram construídos há 20 ou 30 anos, quando a segurança simplesmente não era uma prioridade. As atualizações de firmware podem ser esparsas ou totalmente indisponíveis. Algumas unidades dependem de protocolos proprietários sem criptografia ou autenticação, deixando-as abertas a comandos não autorizados. Enquanto isso, a aplicação de patches pode ser arriscada se não houver laboratório de teste ou se os fabricantes não fornecerem mais suporte. Essas vulnerabilidades são um imã para os invasores: um controlador sem correção, ou mesmo um que esteja uma senha padrão que não foi alterada, pode causar uma interrupção importante antes que qualquer pessoa perceba que ela está acontecendo.

Altos riscos de segurança e regulamentação

Diferente das violações típicas de TI, onde o pior resultado pode ser roubo de dados ou um site off-line, um comprometimento na TO pode levar a riscos reais. Imagine uma fábrica química obtendo leituras incorretas do sensor de temperatura, o que pode provocar uma explosão ou liberar substâncias tóxicas. Os fornecedores de energia enfrentam supervisão igualmente séria de agências como a North American Electric Reliability Corporation (NERC CIP) ou a diretriz NIS2 da UE. A não conformidade ou interrupções prolongadas podem desencadear grandes multas e reações públicas negativas. Como resultado, os operadores industriais devem proteger mais do que apenas seus dados – eles têm o dever de proteger as pessoas que trabalham lá e as comunidades ao seu redor.

Pontos de entrada comuns para ataques de TO

Phishing (apropriação de identidade)

Engenheiros ou técnicos podem verificar e-mails nos mesmos sistemas que configuram ou monitoram o hardware de controle. Um link infectado pode abrir uma porta oculta para as redes de produção.

Acesso remoto inseguro

Alguns portais de fornecedores ou modems de discagem antigos permanecem ativos, sem criptografia ou autenticação adequadas. Os invasores que encontram esses pontos de entrada podem passar por firewalls normais com pouca resistência.

Adulteração da cadeia de fornecimento

A incorporação de malware em atualizações de firmware genuínas ou software de terceiros surgiu como uma tática poderosa. Se o software se originar de um fornecedor "confiável", ele pode evitar verificações padrão e se espalhar sem verificação.

Firewalls mal configurados

Quando as fábricas criam links diretos ou de hospedagem dupla entre TO e TI, elas às vezes não conseguem definir políticas rígidas de firewall. Como resultado, os invasores podem se mover lateralmente pelo ambiente com poucos obstáculos.

Consequências: financeiras, de segurança e além

Erro econômico

Um dos maiores golpes financeiros de uma violação de TO aparece imediatamente: as linhas de produção são interrompidas, as margens de lucro diminuem e as equipes tem que fazer hora extra para atender o backlog. No entanto, essa é apenas uma peça do quebra-cabeça. Se clientes e fornecedores começarem a perceber atrasos consistentes, eles podem procurar outro lugar e os executivos podem enfrentar perguntas difíceis dos investidores, especialmente se a violação for manchete dos jornais. Em alguns setores, a revalidação obrigatória de processos ou a recertificação de equipamentos pode aumentar ainda mais os custos.

Danos à reputação

Na fabricação e na infraestrutura, a confiança é tudo. Quando uma instalação passa dias bloqueada por ransomware, os parceiros de negócios podem repentinamente duvidar de sua capacidade de entregar pedidos futuros no prazo. Enquanto isso, a mídia geralmente se aproveita de histórias dramáticas sobre "hackers assumindo o controle de uma fábrica", deixando uma nuvem de desconfiança duradoura na imagem pública da empresa. Mesmo que as operações voltem ao normal rapidamente, o problema de reputação pode permanecer por muito tempo após o término da crise.

Riscos de segurança

Diferente das violações de TI padrão, um ataque de TO pode causar danos no mundo real. Se os invasores ajustarem as configurações de temperatura ou pressão em uma fábrica química, por exemplo, os acidentes podem variar de explosões a vazamentos tóxicos. Os sistemas com instrumentos de segurança automatizados (SIS) são projetados para limitar esses perigos, mas também podem ser comprometidos se não estiverem bem isolados. Os agentes reguladores de campos como energia, produtos farmacêuticos e energia nuclear estão atentos a incidentes como este, e qualquer sinal de negligência pode causar graves consequências legais ou regulatórias.

A Estrutura de cibersegurança NIST:

Uma abordagem estratégica

Para combater os riscos crescentes, inúmeras organizações recorrem à Estrutura de cibersegurança NIST, que se baseia em seis funções inter-relacionadas: Identificar, Proteger, Detectar, Responder, Recuperar e Governar.

IDENTIFICAR

Você não pode proteger o que você não pode ver. Os ambientes de TO geralmente possuem de tudo, desde máquinas em obsolescência até sensores com tecnologia de ponta, cada um com suas próprias vulnerabilidades. A realização de auditorias regulares e a montagem de um inventário completo de ativos iluminam possíveis pontos cegos. Depois de saber o que está por aí, você pode se concentrar nos ativos mais vulneráveis a ameaças.

PROTEGER

Pense na proteção como fortificar uma fortaleza. A autenticação multifator, por exemplo, adiciona uma parede extra em torno de sistemas sensíveis. Os controles de acesso rígidos limitam quem pode acessar as engrenagens do sistema, e a segmentação de redes reduz o raio de ação de qualquer violação bem-sucedida. Investir nessas medidas antecipadamente é quase sempre mais barato, e muito menos caótico, do que lutar para conter um incidente cibernético não controlado.

DETECTAR

Não importa o quão seguro seja seu perímetro, invasores determinados podem encontrar um caminho. É aqui que a monitoração contínua e os alertas em tempo real se tornam fundamentais. As ferramentas que sinalizam tráfego incomum ou comportamento de usuário desconhecido dão às equipes de segurança a vantagem que precisam para investigar. O tempo é tudo: quanto mais rápido você notar um problema, mais rápido você pode impedir que ele saia do controle.

RESPONDER

Às vezes, apesar dos seus melhores esforços, os cibercriminosos ainda acham uma fresta. Um plano de resposta a incidentes serve como seu projeto de contenção de crise. Ele descreve quem toma decisões, como as equipes coordenam e como você se comunica com as partes interessadas, incluindo funcionários, clientes e parceiros, para que a confusão não amplie os danos. Uma resposta bem coreografada pode ser a diferença entre uma interrupção curta e uma catástrofe prolongada.

RECUPERAR

Voltar ao caminho certo significa mais do que reinicializar algumas máquinas. Um plano de recuperação bem elaborado vai além: ele identifica como e por que um ataque foi bem-sucedido, corrige lacunas de segurança e traduz as lições aprendidas em procedimentos atualizados. Essa introspecção fortalece os sistemas contra o próximo ataque cibernético e ajuda a restaurar a confiança dentro da organização.

GOVERNAR

Uma governança forte atua como a base da segurança de TO. Pergunte a si mesmo: Quem elabora as políticas e quem garante que elas não sejam apenas palavras soltas no papel? Ao estabelecer uma supervisão formal e atribuir funções claras, como um diretor de segurança da informação ou uma equipe dedicada, a liderança ganha visibilidade total das operações diárias. Essa clareza ajuda a integrar os objetivos de cibersegurança em metas estratégicas mais amplas.

Construir uma postura de segurança de TO resiliente não se trata apenas de proteger hardware ou dados. Trata-se de proteger as pessoas que mantêm as instalações funcionando e preservar a confiança que as partes interessadas depositam em suas operações. Ao aplicar os princípios fundamentais do framework NIST nos fluxos de trabalho diários, as organizações deixam de atuar na defesa após uma violação para impedir proativamente as ameaças antes que elas se criem raízes.

Categoria 1 do NIST: IDENTIFICAR

Estabelecendo as bases para a defesa proativa

Em contextos industriais, muitos lapsos de segurança derivam da mesma questão fundamental de supervisão: não manter uma visão precisa e atualizada do cenário de TO. "Identificar" no framework de cibersegurança NIST enfatiza a importância de entender o que você está defendendo: máquinas, sensores, controladores, caminhos de rede e os fluxos de dados que mantêm tudo funcionando.

Por que a visibilidade é fundamental

Uma fábrica de papel pode hospedar milhares de sensores, CLPs, inversores e dispositivos de campo. Alguns desses componentes podem ter décadas e se comunicar por meio de protocolos que as ferramentas modernas de varredura de TI não compreendem bem, como Modbus RTU ou Profibus. Se esses ativos passarem despercebidos, eles podem estar perdendo patches essenciais ou ainda usar credenciais padrão, deixando a porta aberta para os invasores.

A falta de visibilidade também complica a resposta a incidentes. Quando algo dá errado, é desperdiçado um tempo precioso descobrindo qual equipamento está com falha. A detecção antecipada só é possível se os operadores e as equipes de segurança souberem como é o comportamento "normal" da rede e do dispositivo.

Desafios comuns para obter visibilidade em ambientes de TO

- Idade e diversidade de sistemas: SDCD (sistemas digitais de controle distribuído) em obsolescência, hardware ICS proprietário e soluções de Internet das coisas industrial totalmente novas podem coexistir. Esse mosaico requer ferramentas especializadas de descoberta e monitoração.
- Complexidade do protocolo: protocolos industriais proprietários ou incomuns não aparecem claramente em uma varredura TCP/IP padrão. Ferramentas como Wireshark podem decodificá-las, mas a monitoração consistente requer plataformas com reconhecimento de ICS, como Dragos, Nozomi Networks ou Claroty.
- Restrições de recursos: alguns sistemas de produção não podem suportar impactos no seu desempenho decorrente de varreduras ativas. As técnicas devem ser cuidadosamente projetadas para evitar o acionamento de encerramentos do processo.

Quatro pilares de um programa de identificação maduro

Inventário abrangente de ativos

Planilhas e monitoração passiva só podem levá-lo até certo ponto. Se você deseja segurança real em ambientes industriais, precisa de visibilidade total, não apenas de vislumbres do tráfego da rede. É aí que entra a descoberta de ativos baseada em endpoint. Ao interagir diretamente com controladores, IHMs e dispositivos de campo, esse método descobre ativos que, de outra forma, passariam despercebidos. Mesmo dispositivos que não estão se comunicando ativamente na rede podem representar riscos, portanto, identificá-los é fundamental. Mas não se trata apenas de saber quais ativos existem, mas sim de entender todo o contexto.

A coleta de dados contextuais mais profundos, como configurações de dispositivos, comportamentos de comunicação, padrões de acesso do usuário e dependências operacionais, permite às equipes de segurança irem além das listas básicas de inventário. Um CLP com firmware desatualizado pode parecer um ativo de alto risco no papel, mas se estiver em uma área isolada de baixo impacto, pode não exigir reparação imediata. Por outro lado, uma vulnerabilidade aparentemente pequena em um dispositivo que controla diretamente uma linha de produção de alta velocidade pode ter graves consequências financeiras ou de segurança. Ao sobrepor a inteligência de ativos ao contexto operacional do mundo real, as organizações podem identificar vulnerabilidades mais cedo, priorizar riscos de forma mais eficaz e aplicar controles de segurança onde eles mais importam.

Topologia de rede e mapeamento do fluxo de dados

Diagramas visuais e mapas em tempo real de fluxos de dados criam um projeto de interdependências. Se um agente de ataque comprometer uma IHM (interface homem-máquina), você quer ter uma noção imediata de quais CLPs podem ser afetados. O mapeamento também ajuda a planejar estratégias de segmentação.

Acompanhamento de vulnerabilidade

Vulnerabilidades específicas do sistema de controle industrial, como as encontradas em determinadas versões de firmware para CLPs da Siemens ou controladores da Rockwell Automation, podem permanecer por anos se não forem catalogadas adequadamente. A avaliação automatizada de vulnerabilidade vinculada ao inventário de ativos sinaliza fraquezas conhecidas. Mas sem contexto mais profundo, como exploração, criticidade do dispositivo e exposição da rede, as organizações correm o risco de perder tempo com correções de baixo impacto e perder as ameaças reais. As etapas de reparação ou redução devem ser priorizadas com base em uma combinação de gravidade da vulnerabilidade e impacto operacional.

Classificação de criticidade operacional

Classifique cada sistema ou dispositivo de acordo com sua importância para a segurança, produção ou conformidade. Se um defeito do sensor em uma linha química puder causar um perigo ambiental, esse sensor se move em direção ao topo de sua lista de verificação de segurança. Essa priorização deve ir além de apenas rotular os dispositivos como "críticos" ou "não críticos". Compreender o papel operacional de cada ativo, como ele se conecta a processos mais amplos, quais dados eles geram e o que a falha significaria para a produção, garante que as equipes de segurança se concentrem nas ameaças que representam o maior risco do mundo real.

Além dos inventários "criado e esquecido"

É tentador fazer um inventário detalhado de ativos uma vez, colocar os dados em uma prateleira e esquecer deles até o próximo grande projeto. No entanto, as fábricas modernas possuem um fluxo constante, em que novas linhas de produtos são adicionadas, as linhas existentes são reconfiguradas e os sensores são substituídos. Um dispositivo adicionado por um prestador de serviços para um teste piloto pode permanecer conectado indefinidamente se ninguém estiver monitorando. A verificação contínua ou programada e a documentação detalhada do processo são essenciais para manter uma visão precisa e informada sobre o risco.

Começar com o elemento Identificar cria uma base sólida para todos os outros elementos da Estrutura NIST. Você não pode proteger, detectar ou responder de forma eficaz ao operar parcialmente cego. A conscientização detalhada do seu ambiente de TO é a bússola pela qual você navega pelas ameaças emergentes. Toda vez que um ativo é descoberto ou uma vulnerabilidade é sinalizada, o restante do seu aparato de segurança ganha muito mais clareza. Em última análise, o estágio Identificar é sua política de seguro contra ser pego de surpresa, que é uma situação perigosa em qualquer sistema de produção em tempo real.

Categoria 2 do NIST: PROTEGER

Garantia de operações ininterruptas com defesas preventivas

Depois que o cenário industrial é mapeado e catalogado, a próxima pergunta se torna: como você cria proteções robustas em torno de seus ativos mais críticos? Muitas organizações procuram apenas firewalls de perímetro ou ferramentas antivírus. Em configurações complexas de TO, uma camada mais holística de medidas de segurança é fundamental. Os invasores podem chegar por meio de serviços de acesso remoto, um laptop de manutenção, um enlace de dados de TI-TO convergido ou uma atualização de software de um fornecedor que esteja comprometida. Uma única linha de defesa simplesmente não consegue lidar com as inúmeras maneiras pelas quais um agente de ataque pode entrar ou se mover lateralmente.

Profundidade defensiva em sistemas industriais

A categoria "Proteger" lida com etapas práticas para manter os invasores fora das camadas críticas de produção ou, pelo menos, limitar gravemente sua capacidade de causar danos generalizados se eles conseguirem invadir. As tentativas de intrusão podem se concentrar em desabilitar uma IHM, corromper o firmware de um controlador lógico ou adulterar o banco de dados do histórico que registra as corridas da produção. Cada alvo em potencial exige análise de risco cuidadosa e controles relevantes.

Exemplos de medidas de proteção

- Proteções de perímetro de rede: firewalls de perímetro clássicos, sistemas de prevenção de intrusão (IPS) e filtros de conteúdo gerenciam dados de entrada e saída.
- Segmentação e microssegmentação: os modelos tradicionais de zona e eletroduto (com base no Modelo Purdue para ICS) podem separar os sistemas de nível gerencial dos controles. A microssegmentação refina isso ainda mais isolando subconjuntos menores de dispositivos ou processos em seus próprios enclaves de segurança.
- Proteção e reforço de endpoint: lista de permissões leve ou soluções antivírus de próxima geração para consoles de operador. Restrinja os privilégios do usuário para reduzir o risco de um ataque mudar de uma única estação de trabalho para toda a rede.
- Gestão da configuração segura: imponha listas de controle de acesso (ACLs) rigorosas, desabilite portas e serviços não utilizados e remova credenciais padrão. Automatize as verificações de configuração para obter referências de segurança consistentes.

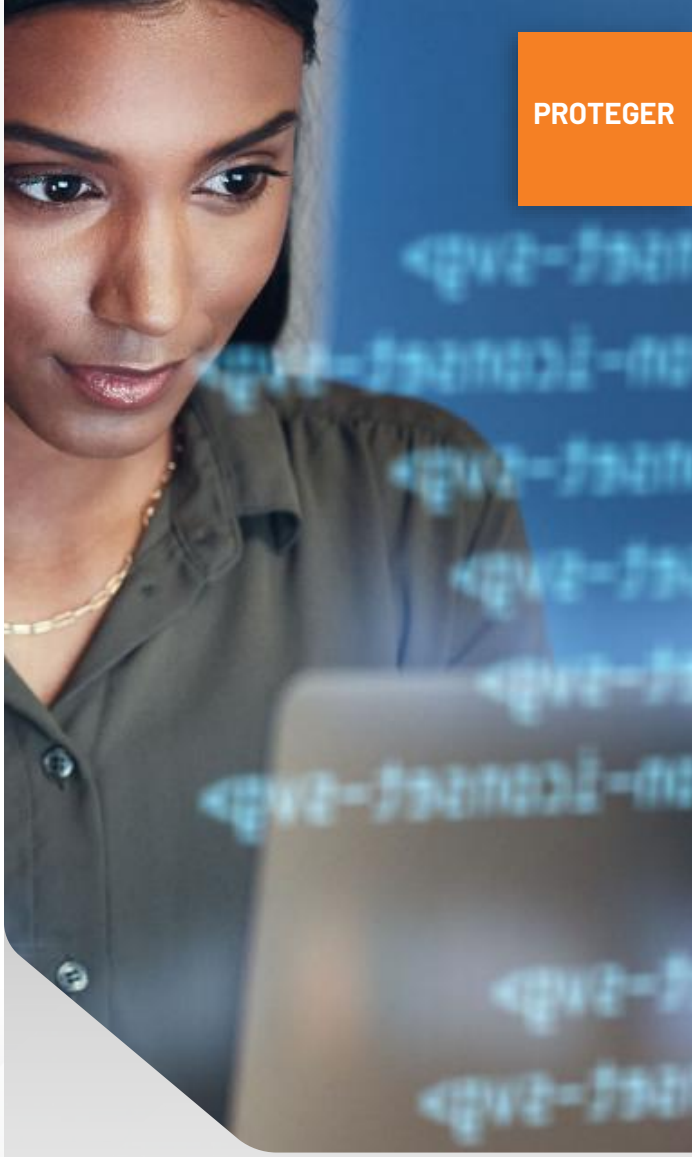
Por que a segmentação é fundamental para a TO

A segmentação, muitas vezes misturada com a abordagem mais simples de "espaço livre", é mais sutil do que apenas bloquear o tráfego de uma rede corporativa. A segmentação verdadeira requer um planejamento arquitetônico deliberado. Você cria camadas distintas (por exemplo, nível 2: controladores locais, nível 3: operações locais, nível 4: TI empresarial) com eletrodutos monitorados entre eles. Cada camada é regida por firewalls ou zonas industriais desmilitarizadas (IDMZ), limitando o movimento não autorizado.

Benefícios da microssegmentação

- Contenção de danos: se um agente de ataque comprometer uma estação de trabalho em uma célula, ele não poderá se mover lateralmente para sabotar outras células críticas.
- Personalização de políticas: zonas diferentes podem ter regras exclusivas. Por exemplo, uma zona de sistema com instrumentos de segurança (SIS) pode impor os parâmetros de comunicação mais rígidos, enquanto uma zona de manutenção pode ser mais flexível.
- Alinhamento de modelo Zero Trust: a microssegmentação complementa uma mentalidade Zero Trust: nunca confie, sempre verifique. É especialmente relevante para redes ICS, que historicamente concedem ampla confiança quando você está dentro do perímetro.

PROTEGER



Gestão de mudanças em tempo real

As fábricas são dinâmicas. O tempo de parada não programada ou programada ocorre para reparos ou atualizações. Com o tempo, os funcionários podem conectar novos dispositivos ou abrir caminhos de comunicação temporários para localização de falhas. Essas alterações alteram o ambiente de segurança. Uma estratégia robusta de "Proteger" integra a gestão de mudanças em tempo real, verificando cada adição ou modificação em relação às políticas de segurança estabelecidas. Se um prestador de serviços tentar ignorar o firewall para manutenção remota, alertas automatizados ou aprovações manuais devem ser acionados antes que esse canal seja aberto.

Aplicação contínua de patches e reforço de configuração

Os sistemas de TO geralmente ficam longos períodos sem serem corrigidos para evitar qualquer interrupção nos processos em andamento. Infelizmente, os invasores exploram essa lacuna previsível. Um ciclo de gestão de patches em camadas, normalmente feito em coordenação com engenheiros de processo e janelas de manutenção, permanece sendo essencial. Soluções como testes de patches off-line podem verificar se as atualizações não interromperão a produção. Além disso, as práticas de configuração segura devem garantir que vulnerabilidades bem conhecidas (por exemplo, senhas de administrador padrão em CLPs) sejam corrigidas rapidamente. As soluções especializadas de gestão de patches do sistema de controle industrial podem agendar e distribuir atualizações de forma a minimizar o risco operacional.

A mudança voltada para o Zero Trust na TO

O Zero Trust na fabricação não é mais hipotético. Algumas organizações avançadas implantam frameworks do modelo Zero Trust (ZTA) especificamente adaptados às redes ICS. Eles integram autenticação contínua e microautorização para confirmar cada dispositivo ou solicitação do usuário. Como protocolos ICS como Modbus ou EtherNet/IP raramente incorporam autenticação forte, envolver esses sistemas com uma camada de sobreposição Zero Trust pode reduzir significativamente os riscos de movimento lateral.

Resumo da camada protetora

Proteger as infraestruturas de TO requer uma combinação estratégica de segmentação, defesa de endpoint, configuração segura e alinhamento com padrões reconhecidos, como ISA/IEC 62443. Ao tecer essas práticas em conjunto, as instalações estão mais bem equipadas para manter a continuidade operacional e evitar catástrofes. Em vez de focar apenas nas fortificações de perímetro, a segurança avançada do sistema de controle industrial exige uma arquitetura multicamadas. Essa arquitetura pode resistir mesmo que um componente defensivo falhe, mantendo os processos essenciais em operação e em boas condições.

Categoria 3 do NIST: DETECTAR

Pare as ameaças antecipadamente — antes que causem falhas em cascata

Os atacantes sofisticados podem não ser detectados em um ambiente de TO por períodos prolongados, testando lentamente quais válvulas ou CLPs eles podem controlar. As soluções tradicionais de detecção de intrusão de TI geralmente deixam passar sinais específicos do sistema de controle industrial, especialmente quando se concentram em registros do Windows ou Linux sem um ponto de vista que reconhece o sistema de controle industrial. A função "Detectar" garante que as anomalias sejam notadas com rapidez suficiente para evitar danos reais.

Monitoração 24 horas por dia, 7 dias por semana, em um mundo que não para nunca

A maioria das fábricas opera 24 horas por dia. Os invasores exploram horários fora de pico — noites, fins de semana, feriados — quando a equipe é reduzida. Uma solução robusta de monitoração de TO não pode descansar. Ele precisa rastrear continuamente o tráfego da rede, os dados operacionais e a atividade do usuário, gerando alertas a qualquer sinal de intenção maliciosa.

Análise de tráfego de rede

Monitorar ambientes de TO requer mais do que apenas observar o tráfego da rede. Embora as ferramentas especializadas de monitoração de TO observem passivamente os fluxos de dados em busca de padrões suspeitos, essa abordagem por si só deixa lacunas, especialmente quando os invasores se movem lateralmente ou visam dispositivos que não se comunicam frequentemente pela rede. Uma estratégia mais eficaz combina análise de tráfego de rede com monitoração de endpoint para fornecer uma visão completa de ameaças potenciais.

Uma abordagem combinada detecta ameaças analisando a atividade da rede e as interações diretas com endpoints, identificando anomalias como:

- Comandos incomuns: um CLP recebe repentinamente instruções para alterar a pressão em uma sequência anormal, detectada no nível da rede e do dispositivo.
- Alterações não programadas: alterações de configuração aplicadas a um dispositivo de chão de fábrica fora do horário de manutenção padrão, visíveis por meio de registro de endpoint e políticas de segurança.
- Violações de protocolo: pacotes Modbus ou Profinet malformados indicam que um agente de ataque está testando cargas úteis de exploração — detectadas por meio de varredura de rede e registros de eventos de endpoint.

Ao integrar as operações de segurança de endpoint, as equipes obtêm informações mais profundas sobre ataques que podem não gerar tráfego de rede óbvio. Em vez de depender exclusivamente da detecção baseada em assinatura (correspondendo padrões ruins conhecidos), as plataformas de segurança avançadas usam heurística e aprendizado de máquina para estabelecer uma avaliação inicial do comportamento "normal" para tráfego de rede e atividade no nível do dispositivo. Ao longo de semanas ou meses, eles podem sinalizar rapidamente picos inesperados, alterações de configuração não autorizadas ou execuções de processos incomuns, reduzindo o tempo de resposta e melhorando a postura geral de segurança.

Monitoração de endpoint e correlação de registros

Camadas de detecção adicionais incluem monitoração de IHMs industriais, estações de trabalho de engenharia e servidores SCADA especializados. A correlação de registros entre esses endpoints pode detectar sinais sutis de infiltração:

- Tentativas de login com falha em um servidor SCADA, repetidas em vários operadores, podem sugerir um ataque de força bruta.
- O serviço reinicia em momentos incomuns, possivelmente indicando malware conectado aos processos do sistema.
- Registros de data e hora sobrepostos entre uma tentativa de intrusão no controlador de domínio corporativo e anomalias no ambiente de TO.

A integração com soluções de gestão de eventos e informações de segurança (SIEM) ou detecção e resposta estendidas (XDR) pode ajudar a unificar esses alertas. No entanto, as soluções SIEM padrão podem não analisar registros do sistema de controle industrial adequadamente, a menos que sejam personalizadas com feeds de inteligência de ameaças do sistema de controle industrial e regras de análise de eventos.

Alertas e resposta em tempo real

A detecção precoce é mais valiosa quando se traduz diretamente em intervenção imediata. Fluxos de trabalho automatizados podem isolar endpoints suspeitos ou bloquear dados para IPs suspeitos no momento em que uma anomalia é confirmada. Essas ações de cerceamento não devem ser tomadas de forma leviana – falsos positivos em um ambiente de sistema de controle industrial podem interromper a produção. Mas com a lógica de detecção bem ajustada, os benefícios (parar ameaças reais) superam e muito os riscos.

Principais resultados da detecção robusta

1. Tempo de permanência reduzido

Quanto mais rápido uma fábrica detectar um invasor, menos tempo os invasores terão para alternar entre diferentes controladores, sabotarem processos ou roubar propriedade intelectual.

2. Menos danos colaterais

O isolamento rápido de zonas comprometidas minimiza a necessidade de desligar toda uma instalação.

3. Análise forense proativa

Como os registros são agregados e correlacionados, os pesquisadores podem reunir a cadeia de ataque rapidamente, identificar as causas e melhorar as proteções futuras.

Criação de uma cultura de detecção colaborativa

As pessoas continuam sendo componentes cruciais de qualquer estratégia de detecção. Operadores de sala de controle, engenheiros de processo e analistas de segurança devem compartilhar percepções. Uma leitura suspeita em um sensor pode ter uma explicação mecânica ou pode sinalizar sabotagem. Canais de comunicação abertos e treinamento cruzado ajudam a equipe a diferenciar entre flutuações de processo normais e eventos maliciosos. Com o tempo, essa sinergia entre sistemas de detecção técnica e experiência humana forma uma linha de defesa poderosa.

Categoria 4 do NIST: RESPONDER

Ação rápida para conter e neutralizar ameaças

Até mesmo defesas bem reforçadas podem ser penetradas por um agente de ataque furtivo ou persistente. A questão então se torna: a organização sabe como responder de forma eficaz? Muitas empresas industriais adiam o planejamento de resposta a incidentes (IR). Quando ocorre uma violação, eles lutam para descobrir quais equipes ou parceiros externos chamar e os processos são improvisados em meio ao pânico.

O preço da falta de preparação

Em indústrias regulamentadas, farmacêuticas, de energia nuclear ou de processamento químico, uma violação de segurança pode ter ramificações imediatas de conformidade. Deixar de responder adequadamente pode expor uma empresa a penalidades legais, riscos ambientais ou incidentes de saúde e segurança. O custo operacional e financeiro pode aumentar se a resposta for atrasada ou desorganizada, porque o agente de ataque terá um tempo precioso para aumentar seus privilégios, vazar dados ou sabotar componentes do sistema de controle industrial.

Componentes fundamentais de um plano de resposta a incidentes focado em TO

1. Funções e responsabilidades claras: identificar quem lidera o processo de resposta a incidentes (IR). Mapeie as responsabilidades dos engenheiros de produção, da equipe da sala de controle, dos executivos de nível C e das equipes de segurança de TI/TO. Funções diferentes precisam de manuais de conduta distintos que detalhem protocolos exatos.
2. Protocolos de comunicação: durante um incidente, as interrupções do sistema podem afetar e-mail ou telefones VoiP. Canais alternativos, como aplicativos de mensagens criptografados ou comunicação por rádio, devem ser estabelecidos com antecedência. As partes interessadas externas – órgãos reguladores, parceiros da cadeia de fornecimento, autoridades locais – também podem precisar ser notificadas em determinadas circunstâncias.
3. Manuais pré-escritos: fluxos de trabalho estruturados para diferentes tipos de incidentes (por exemplo, ransomware, ameaça interna, DDoS em servidores de sistema de controle industrial) orientam os primeiros a responder. Esses manuais incluem etapas técnicas (como isolar máquinas infectadas) e processos de negócios (como notificar fornecedores ou acionistas críticos).
4. Exercícios e ensaios de bancada: os planos elaborados perdem valor se não forem testados em cenários quase reais. Exercícios de simulação usando sistemas de controle industrial reais em um ambiente controlado podem revelar lacunas ocultas: falta de detalhes de contato, servidores de failover sem correção ou confusão da equipe sobre os procedimentos de escalonamento.

Estratégias de contenção rápida

Uma vez que um incidente é confirmado, é vital ter uma contenção rápida. Isso pode envolver:

- Ajustes de segmentação de rede: bloquear temporariamente o tráfego para determinadas sub-redes ou restringir conexões de endpoints suspeitos.
- Revogação de acesso: retirar privilégios de contas comprometidas para interromper infiltrações adicionais.
- Bloqueio da zona desmilitarizada industrial: se a ameaça parecer passar de TI para TO, corte rapidamente ou limite drasticamente a comunicação entre essas zonas até que a ameaça seja neutralizada.

O desafio está em equilibrar a contenção com a continuidade operacional. Parar um processo crítico abruptamente pode causar perdas financeiras ou preocupações de segurança. Equipes qualificadas coordenam-se com equipes de controle de processo para evitar a criação de novos perigos e, ao mesmo tempo, reduzir a propagação do ataque.

Experiência externa e parcerias

Algumas organizações industriais mantêm recursos internos de resposta a incidentes, completos com especialistas em segurança do sistema de controle industrial. Outras dependem de fornecedores especializados ou consultorias. Acordos de serviço pré-arranjados, conhecidos como retentores de IR, são comuns. Um parceiro externo com experiência em investigações de ICS/TO pode intervir imediatamente com ferramentas forenses e melhores práticas aprimoradas a partir de vários engajamentos. O segredo é não esperar até que você esteja no modo de crise para avaliar possíveis provedores de serviço.

Aprendendo com as consequências

As revisões pós-incidente servem como catalisadores para melhoria. Cada detalhe, do vetor de comprometimento inicial à resolução final, produz lições. Talvez um engenheiro tenha usado uma senha VPN fraca ou um determinado processo de atualização fornecido pelo fornecedor estava vulnerável. A documentação desses insights orienta aprimoramentos nas fases Identificar, Proteger e Detectar, fechando o ciclo de vida do NIST.
Uma mentalidade de resposta robusta transforma incidentes dolorosos em oportunidades de resiliência.

Categoria 5 do NIST: RECUPERAR

Restaurando a normalidade e fortalecendo para o futuro

Depois que uma resposta a incidentes faz seu trabalho, a última parte do quebra-cabeça é a recuperação, colocando tudo de volta em operação, verificando se os sistemas permanecem sem comprometimento e garantindo que o mesmo caminho de ataque não possa ser usado novamente. Em ambientes de TO, a recuperação apressada ou o manuseio incorreto pode levar a novos danos ou, pior, perigos físicos reais.

Desafios únicos da recuperação de TO

- Sistemas em obsolescência e dependências de OEM: alguns componentes ICS exigem que o firmware específico do fornecedor ou software proprietário seja totalmente restaurado. Sem backups abrangentes ou suporte do fabricante, recuperar o hardware antigo se torna muito mais complicado.
- Coordenação de versões de software e configurações: reverter um sistema para um backup mais antigo pode provocar incompatibilidades se outros componentes vinculados permanecerem atualizados. Em muitas configurações de TO, os níveis de patches precisam corresponder em toda a cadeia de produção, para que não haja falhas quando os processos forem reiniciados.
- Validação de segurança e conformidade: simplesmente ligar o equipamento pode não ser suficiente. Pode ser necessário verificar novamente os recursos críticos de segurança, recalibrar os sensores ou verificar a consistência do lote para atender a referências regulatórias rigorosas.

Melhores práticas para uma estrutura robusta de recuperação de TO

1. Backups abrangentes e testados: as estratégias de backup devem incluir configurações, firmware, arquivos de interface do operador e quaisquer dados de aplicação ICS especializados. O simples backup de imagens do sistema operacional Windows em uma IHM é insuficiente se os arquivos reais do projeto de controle não forem salvos. Verifique periodicamente a integridade do backup realizando restaurações em um laboratório de teste isolado.
2. Equipes de recuperação multifuncionais: o processo de recuperação não pode ser conduzido apenas pela TI. Os engenheiros de TO, o pessoal de segurança, a garantia da qualidade e até mesmo os representantes do fornecedor devem colaborar para garantir que cada componente restaurado seja seguro e operacional. Um coordenador principal garante que as tarefas sejam sequenciadas em uma ordem lógica.
3. Restauração incremental: ligar tudo de uma vez pode criar conflitos ou reativar vulnerabilidades antigas. Uma abordagem mais cautelosa é colocar os sistemas on-line em etapas, testando-os primeiro em um ambiente de área de segurança ou carga parcial. Dessa forma, se algum malware oculto ou erro de configuração permanecer, você os identificará antes que eles possam se espalhar por toda a operação.
4. Teste de validação e pós-recuperação: quando tudo estiver funcionando novamente, é o momento dos testes de aceitação que reflitam a produção real. Verifique se os fluxos de dados correspondem às expectativas da avaliação inicial, certifique-se de que os sistemas com instrumentos de segurança (SIS) ainda estão intactos e confirme que quaisquer patches recém-aplicados não introduziram novas falhas.

Ransomware: um caso de recuperação especial

O ransomware geralmente criptografa arquivos em várias máquinas. Em um ambiente de TO, a infiltração pode causar bloqueios de IHM ou código lógico manipulado. A restauração de backups geralmente é o único caminho a seguir, presumindo que seus backups estejam intactos e não possam ser acessados ou corrompidos pelos invasores. Algumas organizações mantêm backups "frios" off-line, explicitamente para esses cenários, armazenados em instalações fisicamente separadas. Pode salvar vidas ter um registro off-line recente de seu ambiente ICS para reinstalar tudo do zero, se necessário.

Resiliência além do modo de crise

Quando uma resposta a incidentes é concluída, é aconselhável revisitar as fases anteriores da Estrutura do NIST. Suas ferramentas de monitoração detectaram a violação a tempo? A segmentação realmente limitou seu impacto? Os patches mais antigos ou senhas padrão facilitaram muito a vida dos invasores? Incorporar essas conclusões no ciclo contínuo Identificar–Proteger–Detectar–Responder–Recuperar mantém sua postura de segurança evoluindo em vez de ficar imóvel.

Em campos como ciências da vida ou petroquímica, uma interrupção prolongada pode prejudicar mais do que o resultado final. Se a produção parar, a escassez de medicamentos ou interrupções de energia podem afetar comunidades inteiras. Um plano de recuperação bem organizado não apenas faz com que as operações voltem a funcionar rapidamente, mas também preserva a confiança do público, evitando que pequenas oscilações evoluam para grandes crises.

Categoria 6 do NIST: GOVERNAR

Para operações industriais, uma governança forte não é opcional, é essencial. Nem todas as organizações seguem o mesmo roteiro; algumas usam a Estrutura de cibersegurança NIST (CSF),enquanto outras se baseiam na IEC 62443, ISO 27001ou em uma combinação personalizada de melhores práticas. O segredo é escolher uma estrutura que se encaixe em seu cenário de risco e necessidades operacionais. Não importa a estrutura, a governança garante a responsabilidade, define funções claras e alinha os esforços de segurança com as metas de negócios.

A boa governança responde às principais perguntas: quem é o proprietário das políticas de segurança? Como os riscos são avaliados? Qual é o plano de resposta para um incidente? Ela também ajuda a priorizar os investimentos em segurança com base no impacto do mundo real, garantindo que a TI, a TO e a liderança permaneçam alinhadas.

Selecionar a estrutura certa não se trata de marcar caixas de seleção, mas sim de construir uma estrutura expansível e adaptável que cresça com sua organização. Um modelo de governança bem implementado facilita o gerenciamento de riscos, atende aos requisitos de conformidade e melhora continuamente a resiliência da segurança.

Alinhando liderança e operações

Muitos ambientes industriais envolvem equipes separadas de TI e TO, além de fornecedores externos para hardware ou software crítico. Uma estrutura de governança sólida garante que executivos, gerentes de fábrica e profissionais de segurança sigam uma visão comum. Isso geralmente inclui orientações oficiais sobre quem possui quais ativos do sistema de controle industrial, como os ciclos de patches devem ser executados ou quais sinais de alerta exigem uma resposta a incidentes. A responsabilidade clara explica as responsabilidades da liderança – talvez do CISO ou do diretor de TO – para um grande panorama do investimento em segurança, relatórios de incidentes ou conformidade.

Orçamento e alocação de recursos

A governança também lida com o fluxo de dinheiro e mão de obra. Cada função do NIST precisa de financiamento adequado para que as medidas de segurança não sejam interrompidas durante a implementação. Se uma instalação exigir segmentação de rede especializada ou reconhecimento do protocolo ICS, por exemplo, os órgãos de governança podem sinalizar o orçamento necessário. Eles também podem aprovar programas de treinamento para que o pessoal de TO possa dominar novas ferramentas ou processos.

Análises de políticas e mecanismos de auditoria

As políticas e os procedimentos de segurança precisam de verificações periódicas, muitas vezes vinculadas a padrões reconhecidos como ISA/IEC 62443 ou ISO/IEC 27001. Auditorias internas ou externas verificam se a abordagem da organização para Identificar, Proteger, Detectar, Responder, Recuperar e Governar permanece atualizada. Se essas auditorias identificarem lacunas, como inventários de ativos desatualizados ou falta de backups, a governança entra em ação para guiar as correções.

Preenchendo as lacunas de comunicação

Um modelo de governança bem pensado também fecha o circuito entre executivos e engenheiros locais. Isso pode significar atualizações de segurança regulares em reuniões de liderança, simulações de bancada entre departamentos ou uma linguagem compartilhada para discutir metas de segurança. A governança eficaz corta os silos de informação, garantindo que os investimentos em uma fase do NIST (como a detecção avançada) sejam combinados com o treinamento da equipe ou com um planejamento robusto de resposta a incidentes de outra.

Resultados da governança eficaz

Quando a governança está afiada, cada função do NIST se beneficia:

- Identificar: os líderes mantêm listas precisas de ativos e garantem que as verificações de vulnerabilidade aconteçam regularmente.
- Proteger: a adesão organizacional e os orçamentos aprovados preparam o caminho para iniciativas de microssegmentação, gestão de patches e confiança zero.
- Detectar: a gestão investe em monitoração de ameaças incluindo o sistema de controle industrial (ICS) e sistemas de alerta em tempo real.
- Responder: estruturas de autoridade claras significam que manuais de incidentes são seguidos, com suporte de alto nível para contenção decisiva.
- Recuperar: etapas de recuperação documentadas, funções atribuídas e financiamento adequado permitem um retorno rápido às operações normais, além de uma chance de aprender com o que deu errado.

Resumindo, a governança é a cola que mantém a Estrutura NIST unida em contextos de TO. Ao esclarecer a responsabilidade, proteger recursos e simplificar a comunicação, ela garante que a segurança não seja abordada apenas de última hora, mas que esteja incorporada nas operações diárias, protegendo processos críticos, promovendo uma cultura de conscientização e mantendo os objetivos de negócios à vista.

Invista agora para criar resiliência e reduzir interrupções

As operações industriais prosperam com fluxos de trabalho simplificados. Se esses fluxos de trabalho são interrompidos, não são apenas os lucros que estão em jogo, mas a segurança do trabalhador e a reputação da marca também podem ser afetadas. Proteger a TO requer mais do que correções rápidas; exige comprometimento significativo e alinhamento com estruturas comprovadas como o NIST. Cada função – Identificar, Proteger, Detectar, Responder, Recuperar – ajuda sua organização a ficar um passo à frente de um cenário de ameaças em constante evolução. Ao adotar uma estratégia completa, você pode lidar com ataques de forma mais tranquila e manter os processos essenciais funcionando.

Por que medidas holísticas são importantes

As pessoas fazem parte do perímetro

Firewalls e ferramentas de detecção podem fazer muito, mas tem um limite. Se funcionários e contratados não reconhecerem e-mails de phishing (apropriação de identidade) ou entenderem a necessidade de senhas fortes, os invasores podem entrar. Uma cultura proativa, que recompensa o relato rápido de comportamentos estranhos, geralmente captura ameaças antes que a tecnologia o faça.

Tecnologias exigem integração cuidadosa

Em configurações de TO, protocolos mais antigos e demandas em tempo real tornam arriscado simplesmente implantar soluções padrão de segurança de TI. Qualquer nova ferramenta deve ser testada quanto à compatibilidade do sistema de controle industrial e implantada de forma que não interrompa a produção.

Auditorias e treinamentos contínuos

Os invasores nunca descansam, logo as equipes de segurança também não podem se dar ao luxo. Exercícios de bancada, engajamentos de equipes de emergência e avaliações de rede regulares mantêm as organizações um passo à frente. Essas táticas proativas extraem os conceitos do NIST da teoria para as rotinas diárias.

Interconexão global

Um link vulnerável em um subcontratado ou distribuidor pode ser transmitido por meio de conexões de dados, portais de fornecedores ou plataformas compartilhadas, atingindo todos os envolvidos. Um plano de segurança ICS eficaz se estende a todos os fornecedores e parceiros remotos, exigindo esforços conjuntos em vários locais.

Preenchendo lacunas com orientação de especialistas

Muitas empresas se beneficiam de profissionais de segurança de TO externos que realmente entendem CLPs em obsolescência, arquiteturas de modelo Zero Trust e implantações de interrupção mínima. Eles também podem reforçar a prontidão para incidentes elaborando manuais de IR, liderando exercícios de bancada e mantendo um plantonista 24 horas por dia, 7 dias por semana.

Cultura: o verdadeiro pilar da segurança de TO

Mesmo as melhores ferramentas e processos não garantirão a segurança se a cultura não os apoiar. Em um local de trabalho que trata a cibersegurança tão seriamente quanto a segurança física, um comportamento de rede suspeito ou uma unidade USB não autorizada são relatados imediatamente. No entanto, se os funcionários temem uma retaliação, eles podem permanecer quietos, dando aos invasores uma passagem livre. Por outro lado, uma cultura que incentiva alertas proativos gera relatos imediatos, promove a colaboração e investe nas habilidades de segurança do pessoal.

Os líderes definem o tom atribuindo orçamentos sérios de cibersegurança, garantindo que os funcionários recebam treinamento atualizado e enquadrando o tempo de parada não programada de uma violação não como um "problema de TI", mas como uma ameaça ao resultado final. Atualizações executivas frequentes sobre a postura de segurança – e incentivos para identificar ou prevenir problemas – mudam a atmosfera de mera conformidade para engajamento genuíno.

Contando as vantagens a longo prazo

Disponibilidade sustentada

Uma linha de produção com operação estável protege a receita, fortalece a imagem da marca e consolida parcerias.

Conformidade com a regulamentação

Uma segurança forte pode satisfazer os auditores, minimizar a exposição legal e agilizar as certificações, especialmente em setores altamente regulamentados.

Capacitação para a inovação

À medida que IoT, IA e robótica avançada se tornam padrão nas fábricas, uma base de segurança robusta garante que elas operem com segurança e eficiência

Vantagem competitiva

Em uma cadeia de fornecimento repleta de vulnerabilidades, um ambiente de sistema de controle industrial reforçado pode posicioná-lo como um parceiro confiável em mercados cautelosos.

Implementar a Estrutura NIST não significa assinalar caixas de seleção. É uma abordagem prática que reconhece riscos reais em ambientes industriais. Ao aplicar sistematicamente Identificar, Proteger, Detectar, Responder, Recuperar e Governar, as organizações cultivam uma cultura de segurança que acompanha as mudanças nas ameaças e se alinha às metas operacionais.

Como seguir em frente

Alcançar esse nível de resiliência exige tempo, recursos e adesão genuína da liderança, mas os retornos são importantes. Em vez de ser interrompida pela próxima violação, sua organização pode manter as operações funcionando 24 horas por dia, proteger sua reputação e atender clientes e parceiros de forma confiável.

Se você estiver pronto para ir além das correções de patches, considere fazer parceria com especialistas em cibersegurança que entendem TI e TO. Eles podem projetar abordagens que atendam às suas necessidades operacionais, gerenciar riscos e manter tudo flexível e seguro. Nunca é cedo demais, ou tarde demais, para investir em um futuro em que as ameaças cibernéticas sejam um golpe gerenciável em vez de uma crise completa.

Dê o próximo passo

Transforme insights em ação

Você explorou estratégias baseadas em NIST, exemplos do mundo real e melhores práticas para resiliência industrial. Pronto para colocá-los em prática? Nossa equipe é especializada em fazer a ponte entre as preocupações de TI e TO para ajudar a criar defesas duráveis sem sacrificar a disponibilidade.

Vamos transformar os insights do artigo técnico *Do caos ao controle* em um plano personalizado para sua organização.

Rok.auto/secureot

Publicação GMSN-WP012B-EN-P Dezembro de 2025 | Precede a publicação GMSN-WP012A-EN-P-Março de 2025

SecureOT

Sobre o conjunto de soluções SecureOT™

A Rockwell Automation capacita as organizações industriais a defender seus ambientes de TO com uma abordagem completa e gerenciada para a cibersegurança. Ao alinhar nossa abordagem com a Estrutura de Cibersegurança NIST, ajudamos você a identificar, proteger, detectar, responder e se recuperar de ameaças em evolução, sem sacrificar a disponibilidade da produção.

Estrutura comprovada alinhada ao NIST

Integramos soluções de avaliação de risco e gestão de vulnerabilidade que atendem às normas reconhecidas globalmente, como NIST, NIS2 e IEC 62443. Isso garante que sua estratégia atenda tanto aos requisitos regulatórios como às necessidades operacionais do mundo real.

Segurança holística de TO

Nossos serviços de ponta a ponta abordam todas as facetas da segurança industrial, desde a avaliação de sistemas de controle em obsolescência até a implantação de estratégias de detecção e reparação de ameaças. Oferecemos avaliação abrangente, visibilidade, monitoração, resposta a incidentes e redução automatizada de riscos, tudo personalizado para os desafios exclusivos dos ambientes de TO.

Experiência no setor

Com mais de um século de experiência em automação industrial, a Rockwell Automation conhece os prós e contras de suas linhas de produção. Entendemos a interação repleta de nuances entre TI e TO e projetamos nossas soluções para proteger processos críticos sem interrompê-los.

Inovação no centro

Nossas equipes de P&D ultrapassam os limites da cibersegurança, desenvolvendo as melhores tecnologias que permitem que você fique à frente de ameaças avançadas. Quer você esteja modernizando a infraestrutura antiga ou implementando novas iniciativas digitais, nossas soluções oferecem segurança que evolui com você.

Com a confiança dos líderes da indústria

As organizações globais contam com a Rockwell Automation para uma experiência de domínio profunda e propriedade intelectual robusta e proprietária. Nosso histórico inclui implantações bem-sucedidas em diversos setores, ajudando os clientes a manter suas operações sem interrupção, a proteger reputações e a atender as metas de conformidade.