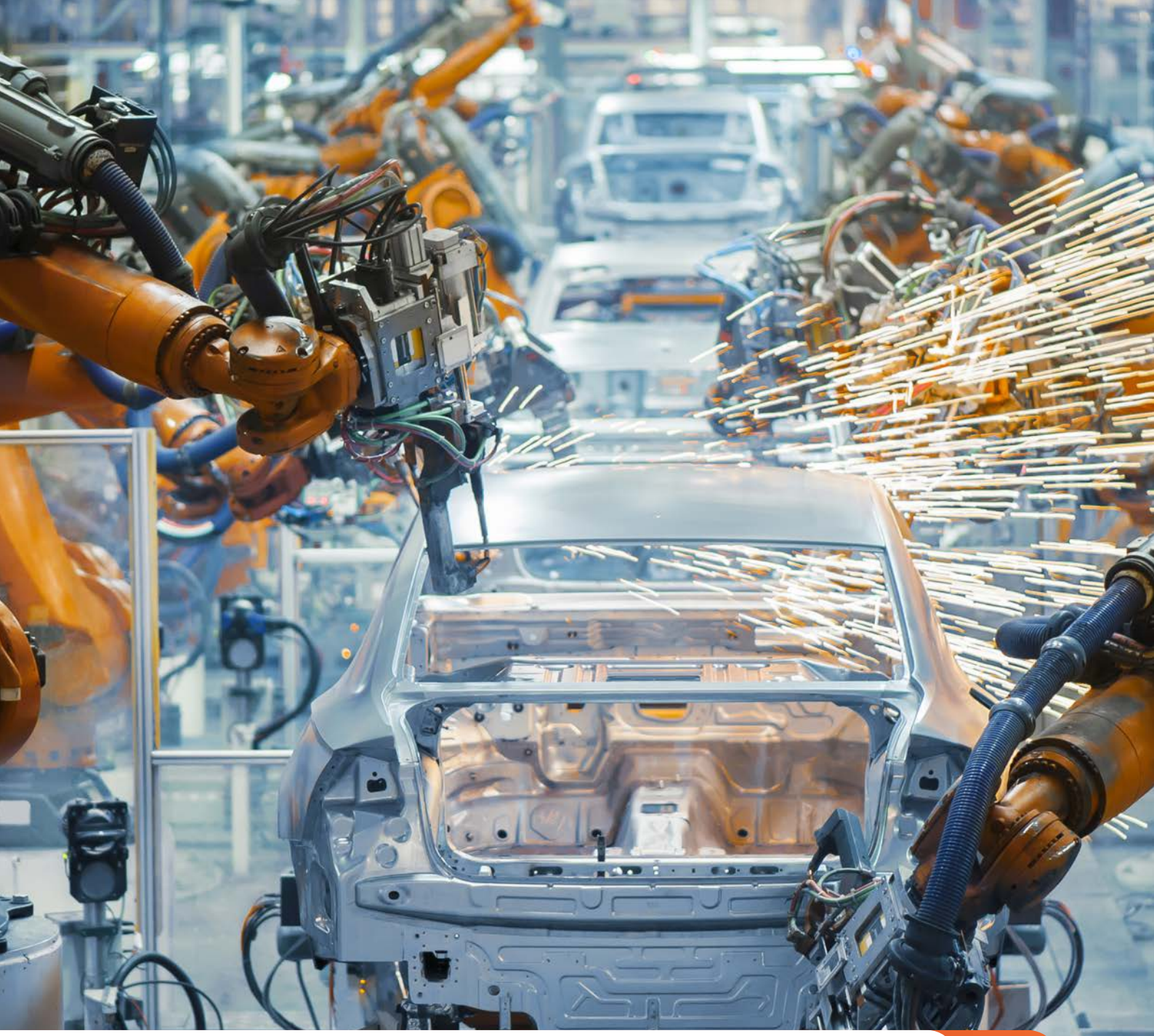


Rockwell Automation

O Inteligente da Próxima Geração Fabricação automotiva Exige cibersegurança proativa

Sumário

Introdução

Desde a adoção de carros sem motorista até o incentivo para veículos movidos a bateria, a indústria automotiva está passando por mudanças mais rápidas e abrangentes do que em qualquer outro momento de sua história. Os líderes da indústria estão inovando para tornar os carros totalmente elétricos e híbridos mais divertidos de dirigir, enquanto as mudanças nos projetos dos motores de combustão interna estão diminuindo as emissões e aumentando o desempenho. Ao mesmo tempo, as montadoras têm uma oportunidade sem precedentes de introduzir novas eficiências em suas operações, aumentando a automação, a digitalização e a conectividade no chão de fábrica.

Esse ritmo acelerado de transformação digital – juntamente com o alto perfil da indústria automobilística – está tornando a fabricação automotiva um alvo cada vez mais atraente para o cibercrime. Os hackers mal-intencionados estão bem cientes do alto custo do tempo de parada não programada nas fábricas de automóveis e sabem que esses custos podem levar as vítimas do ransomware a considerar fazerem grandes pagamentos para retomar a produção rapidamente.

Os cibercriminosos também sabem que a base instalada de equipamentos de montagem automotiva, incluindo sistemas de controle industrial (ICS) e sistemas de execução de manufatura (MES), tende a ter um longo ciclo de vida e que o gerenciamento de vulnerabilidade é um desafio perpétuo em tecnologia operacional (TO).

No mundo de hoje, os riscos cibernéticos enfrentados pelas montadoras são grandes e significativos. O cenário de ameaças continua desafiador, com previsão de que os prejuízos do crime cibernético custarão ao mundo mais de US$ 10,5 trilhões anualmente até 2025, com custos crescendo 15% ano a ano.[1] Enquanto isso, os hackers mal-intencionados mais sofisticados e mais bem financiados, aqueles patrocinados por Estados-nação, estão se tornando mais capazes e mais ousados. Pesquisadores estimam que ataques cibernéticos "significativos" patrocinados por estados dobraram de frequência entre 2017 e 2021.[2] Entre os fabricantes industriais, pelo menos 53% sofreram uma violação de cibersegurança em uma de suas instalações nos últimos dois anos.[3]

[1] *Cybersecurity Ventures*, [2] *States, Cyberconflict and the Web of Profit*, [3] *LNS Research*

Por que os fabricantes de automóveis são suscetíveis a ataques cibernéticos

Os fabricantes automotivos são um dos principais alvos dos cibercriminosos, em parte porque compartilham muitas características com outros fabricantes, incluindo infraestruturas legadas que muitas vezes permanecem sem correção, juntamente com a falta de recursos qualificados para gerenciar riscos. Estudos recentes mostram que entre as 100 principais montadoras, 49% são "altamente suscetíveis" a ataques de ransomware. Senhas vazadas ou credenciais roubadas de 91% dessas empresas foram encontradas rapidamente disponíveis na Dark Web, enquanto 79% das montadoras e fornecedores diretos receberam classificações ruins para gestão de patches. 90% foram classificados como "altamente suscetíveis" a ataques de phishing.[4]

As montadoras também são um alvo principal porque enfrentam riscos específicos únicos do setor. As cadeias de suprimentos automotivos são inerentemente complexas, com OEMs automotivos dependendo de redes de fabricantes terceirizados distribuídas globalmente para uma vasta gama de peças, incluindo software e componentes eletrônicos de hardware. Como os veículos de hoje incluem um número crescente de sistemas controlados por software e conectados à Internet, garantir a integridade das cadeias de fornecimento é fundamental para manter a segurança funcional dos veículos – e proteger a vida de seus ocupantes.

Segurança durante a rápida transformação digital

A transformação digital está ocorrendo em todo o cenário industrial. O setor automotivo está entre os que mais se movimenta. A digitalização dos processos de fabricação de automóveis está gerando maior produtividade, melhorando a qualidade e a consistência do produto e otimizando os fluxos de trabalho que aumentam a segurança e a eficiência da fábrica. A capacidade de compartilhar dados entre os sistemas de TI e TO está permitindo análises que estão melhorando as operações, criando melhores resultados de negócios para as montadoras.

Esses avanços também podem aumentar o risco cibernético, especialmente quando as montadoras não desenvolveram um programa abrangente de cibersegurança industrial corporativa. Adotar uma abordagem de defesa em profundidade alinhada com o Estrutura de cibersegurança NIST é essencial para proteger redes e dispositivos individuais para defender sistemas contra ataques externos.

Os fabricantes de automóveis também devem desenvolver capacidades contínuas e rápidas de detecção e resposta, identificando atividades anômalas e bloqueando ataques antes que causem tempos de parada sérios ou perdas financeiras e de equipamentos. E eles devem se tornar capazes de se recuperar rapidamente de incidentes cibernéticos. Isso exige uma abordagem multicamadas com as pessoas, processos e tecnologias certas, incluindo produtos ICS seguros desde o projeto e soluções de segurança robustas desenvolvidas especificamente para ambientes industriais.

[4] Black Kite

FOCO FUTURO:

Proteger veículos conectados é essencial para conquistar a confiança dos consumidores de hoje

Veículos conectados são aqueles que compartilham dados com sistemas baseados em nuvem, aplicativos veiculares e outros sistemas, incluindo infraestrutura rodoviária, outros veículos, dispositivos móveis ou serviços telemáticos. Desde que a GM introduziu o primeiro sistema automático de chamada de emergência no carro em 1996, a conectividade de veículos de passageiros cresceu aos trancos e barrancos. **Estima-se que os veículos conectados representarão mais de 25% do mercado automotivo global até o final de 2023 e mais de 75% até 2025.**[5]

Os veículos tecnologicamente mais sofisticados de hoje que incorporam sistemas avançados de assistência ao motorista (ADAS) contêm mais de 150 unidades de controle eletrônico (ECUs) baseadas em microprocessador e mais de 150 milhões de linhas de código.[6] A Deloitte estima que até 40% do custo de um carro novo pode ser atribuído a sistemas eletrônicos baseados em semicondutores,[7] e o bom funcionamento do software costuma ser um fator determinante do desempenho e da eficiência do veículo – e, portanto, das preferências do consumidor por um determinado modelo de carro ou marca automotiva.

Estima-se que os veículos conectados representarão mais de 25% do mercado automotivo global até o final de 2023 e mais de 75% até 2025.

Automóveis agora ‘nascem ouvindo’

Muitos motoristas agora esperam que seus carros funcionem com um software e se comportem como velozes centros de dados móveis. Eles também estão prestando mais atenção à cibersegurança no veículo. Quando os pesquisadores de segurança demonstraram que podiam assumir remotamente o controle de um jipe em uma via de alta velocidade, sequestrando seus sistemas de bordo pela Internet, o incidente levou a Chrysler a fazer um recall de 1,4 milhão de veículos. Os principais meios de comunicação também tomaram conhecimento.[8]

Em outra demonstração de prova de conceito, os hackers conseguiram abrir as portas de um veículo elétrico popular usando um drone carregando um dongle WiFi e até invadir o servidor central de Comando e Controle (C2) usado para se comunicar com toda a frota do cliente da mesma fabricante.[9]

Mais do que nunca, a cibersegurança rigorosa de veículos conectados é imperativa para as marcas automotivas que desejam conquistar e manter a confiança do consumidor. De acordo com uma pesquisa recente, 80% dos compradores de carros nunca comprariam um veículo de uma montadora se essa marca tivesse sofrido com um veículo hackeado.[10] E outra pesquisa descobriu que 84% dos consumidores não comprariam um carro novamente em uma concessionária onde eles compraram um veículo anteriormente se descobrissem que seus dados foram comprometidos em uma violação.[11]

[5]Capgemini, [6]IEEE Future Directions, [7]Deloitte, [8]Wired, [9]Electrek, [10]After Market News, [11]Total Dealer Compliance

As maiores ameaças de cibersegurança da indústria automotiva

A transformação digital está ocorrendo em todo o cenário industrial. O setor automotivo está entre os que mais se movimenta. A digitalização dos processos de fabricação de automóveis está gerando maior produtividade, melhorando a qualidade e a consistência do produto e otimizando os fluxos de trabalho que aumentam a segurança e a eficiência da fábrica. A capacidade de compartilhar dados entre os sistemas de TI e TO está permitindo análises que estão melhorando as operações, criando melhores resultados de negócios para as montadoras.

Esses avanços também podem aumentar o risco cibernético, especialmente quando as montadoras não desenvolveram um programa abrangente de cibersegurança industrial corporativa. Adotar uma abordagem de defesa em profundidade alinhada com o Estrutura de cibersegurança NIST é essencial para proteger redes e dispositivos individuais para defender sistemas contra ataques externos.

Os fabricantes de automóveis também devem desenvolver capacidades contínuas e rápidas de detecção e resposta, identificando atividades anômalas e bloqueando ataques antes que causem tempos de parada sérios ou perdas financeiras e de equipamentos. E eles devem se tornar capazes de se recuperar rapidamente de incidentes cibernéticos. Isso exige uma abordagem multicamadas com as pessoas, processos e tecnologias certas, incluindo produtos ICS seguros desde o projeto e soluções de segurança robustas desenvolvidas especificamente para ambientes industriais.

Ataques comuns de cibersegurança às Montadoras automotivas

Os três cenários de ataque mais prevalentes atualmente incluem ataques de ransomware, ataques de phishing (resultando em roubo de credenciais) e a exploração de vulnerabilidades não corrigidas em dispositivos de chão de fábrica.

A AMEAÇA DO RANSOMWARE

Os ataques de ransomware são o tipo de crime cibernético que mais cresce no mundo, com danos globais causados por ransomware estimados atualmente em mais de US$ 20 bilhões. Pesquisadores estimam que hoje em dia uma empresa é afetada por um ataque de ransomware a cada 11 segundos.[12]

A manufatura está entre os setores com maior probabilidade de serem visados por operadores de ransomware, com organizações industriais recebendo quase o dobro do tráfego de rede relacionado a ransomware do que o segundo setor mais visado.[13] E entre os fabricantes, as montadoras são um alvo especialmente atraente porque os custos associados com produção parada são muito altos. Na verdade, o mesmo fenômeno que torna as montadoras mais propensas a considerar o pagamento de resgates – intolerância ao tempo de parada não programada – também torna muitas delas lentas para corrigir vulnerabilidades.

Os ataques de ransomware geralmente começam com tentativas bem-sucedidas de phishing. Os operadores de ransomware também exploram com frequência portas críticas publicamente visíveis para carregar um malware no ambiente ou se aproveitar de credenciais roubadas para obter acesso remoto a sistemas. A **segmentação** adequada de redes industriais e corporativas é essencial para impedir que o ransomware se espalhe desde o ponto inicial da infecção. Garantir que DMZs (zonas desmilitarizadas) industriais e zonas de segurança críticas sejam logicamente isoladas das redes corporativas de TI pode bloquear tentativas de movimentação lateral em ambientes de TO, se o acesso for obtido pela TI ou TO.

[12] *Cybersecurity Ventures*, [13] *Cisco*

ATAQUES DE PHISHING VISAM MONTADORAS

Os ataques baseados em e-mail direcionados especificamente às montadoras são generalizados. Pesquisadores de ameaças avaliando a exposição ao risco de phishing da indústria automotiva descobriram mais de 18.000 domínios falsos ou de phishing que foram criados explicitamente para atingir as 100 principais montadoras e OEMs.[14] Phishing é uma tática altamente eficiente para os cibercriminosos usarem, pois pode resultar em privilégios internos de TI ou ICS, incluindo credenciais administrativas.

Depois que uma tentativa de phishing é bem-sucedida, pode ser difícil para os defensores detectarem os estágios subsequentes do ataque, pois as atividades do atacante se parecerão com as de um usuário interno. Sua capacidade de causar danos imediatos será limitada apenas por seu conhecimento de como operar os sistemas da planta e manipular os componentes do ICS para atingir objetivos específicos. Proteger-se contra esses tipos de ameaças requer controles de nível de rede, aplicativo e dispositivo, bem como monitoramento contínuo de segurança de TI/TO para detectar rapidamente anomalias comportamentais ou tentativas incomuns de login.

Um programa abrangente de **treinamento de conscientização de segurança** que ensine os funcionários a identificar e evitar tentativas de phishing pode reduzir esses riscos, assim como a implementação de políticas apropriadas que controlam o acesso administrativo a sistemas operacionais industriais e de fabricação. Também é fundamental investir na educação e no treinamento que manterão os funcionários atualizados sobre as ameaças à segurança e as melhores práticas atuais.

VULNERABILIDADES NÃO CORRIGIDAS NA BASE INSTALADA

A gestão de patches da base instalada é muito desafiadora para as empresas automotivas, mas aquelas que continuarem incapazes de reduzir vulnerabilidades nos sistemas do chão de fábrica rapidamente se depararão com riscos inaceitáveis.

Em um relatório de pesquisa recente, descobriu-se que até 91% dos fabricantes de automóveis têm pelo menos uma vulnerabilidade severa em seu software de TO ou ICS.[15] Algumas foram expostas na Internet aberta e muitas não puderam ser corrigidas porque as atualizações para o hardware após o fim da vida útil dele não eram mais fornecidas pelos fabricantes.

É essencial desenvolver um processo eficaz e bem compreendido para lidar com vulnerabilidades na base instalada e atender aos requisitos de aplicação de patches. **Identificar e inventariar todos os ativos de rede** em todo o ambiente de TO, incluindo hardware, equipamentos, servidores, sensores e dispositivos móveis e realizar **monitoramento contínuo de ativos** para detectar ativos ou usuários não autorizados nas redes – é uma etapa vital.

Testes de penetração regulares também são cruciais. Os especialistas tentam violar sistemas e podem fornecer uma avaliação verdadeira das fraquezas e vulnerabilidades, permitindo sua correção.

[14] *Intsights*, [15] *Black Kite*

A natureza mutável do que deve ser protegido

No passado, as redes de TI das montadoras precisavam ser protegidas e defendidas, assim como os controladores lógicos programáveis (CLPs) e ICSs no chão de fábrica.

Hoje, esses sistemas ainda devem ser protegidos, mas também devem ser protegidos os ecossistemas de TI/IoT/IIoT cada vez mais complexos e interconectados, juntamente com veículos conectados que dependem de software. Isso levanta um novo conjunto de questões para as montadoras:

- Como um fabricante pode corrigir o software em um veículo que já está na estrada?
- As montadoras precisam construir novos centros de operações de segurança (SOCs) apenas para poder monitorar a frota de veículos que já produziram?
- Que tipo de nova vigilância regulatória a indústria automobilística enfrentará nos próximos anos?
- Como as montadoras podem obter melhor visibilidade das práticas de segurança de seus fornecedores terceirizados de ECU?

Construindo uma abordagem sólida para a cibersegurança automotiva

À medida que as montadoras adotam cada vez mais a conectividade de ponta a ponta em seus ecossistemas de instalações de produção e de computação empresarial, há uma necessidade crescente de adotar uma abordagem abrangente de cibersegurança para proteger pessoas, propriedade intelectual, produtividade e continuidade operacional.

As redes de TO são inerentemente complexas; não há bala de prata ou solução simples e única que possa garantir um ambiente permanentemente seguro.

Em vez disso, é essencial adotar uma abordagem contínua baseada em riscos, identificando os riscos únicos de pessoas, processos e tecnologias enfrentados pela empresa. Uma avaliação clara das vulnerabilidades e riscos associados pode ajudar a organização a alocar os recursos certos, implementar as políticas e procedimentos certos e implantar as tecnologias certas.

Os fabricantes automotivos devem começar entendendo a postura de segurança de sua base instalada, conduzindo um inventário completo de ativos e uma avaliação de risco abrangente.

Linha do tempo dos principais ataques direcionados aos fabricantes de automóveis

Março 2019

Em um ataque altamente direcionado, provavelmente conduzido por um grupo de ameaças persistentes avançadas (APT), os cibercriminosos obtiveram acesso a servidores contendo dados de clientes em uma violação que pode ter afetado até 3,1 milhões de pessoas.[16]

Dezembro de 2019

Um grupo APT suspeito de ter laços com o governo vietnamita, APT 32 (Ocean Lotus) teria violado redes em dois grandes fabricantes de automóveis.[17]

Fevereiro de 2020

Pesquisadores de segurança encontraram 19 vulnerabilidades em veículos, permitindo que eles se comuniquem com os servidores de back-end do fabricante para abrir as portas do carro e ligar os motores remotamente.[18]

Abril de 2020

Ao fazer engenharia reversa da unidade de controle telemático (TCU) de um veículo individual, os pesquisadores de segurança foram capazes de utilizar a conexão telemática para se infiltrar na rede corporativa do OEM e obter acesso com privilégios administrativos completos.[19]

Maio de 2020

O código-fonte dos componentes conectados instalados nas vans de uma montadora vazou depois que os repositórios Git contendo imagens, código, documentação detalhada e ambientes de desenvolvimento para as unidades lógicas de bordo (OLUs) das vans foram tornados públicos.[20]

Junho de 2020

Um ataque de ransomware direcionado a uma montadora japonesa infectou servidores internos e levou a empresa a suspender a produção em fábricas em todo o mundo.[21]

Agosto de 2020

Um pesquisador de segurança conseguiu obter o controle de toda a frota de veículos conectados da empresa de uma mesma marca, explorando uma vulnerabilidade do lado do servidor na rede do OEM.[22]

Agosto de 2020

Uma concessionária foi vítima do grupo que operava o ransomware Ryuk. Os invasores roubaram dados corporativos durante o incidente e os publicaram em seu portal de vazamentos dedicado.[23]

Fevereiro de 2021

A montadora sofreu um suposto ataque de ransomware DoppelPaymer que afetou os sistemas internos e voltados para o cliente e levou a uma interrupção prolongada.[24]

Maio de 2021

Uma subsidiária de fabricação de peças deste grande fabricante de automóveis sofreu um ataque direcionado de ransomware. Dados financeiros e de clientes foram exfiltrados e expostos enquanto a empresa controladora da organização lutava contra paralisações de produção devido a problemas na cadeia de fornecimento.[25]

[16] CPO Magazine, [17] ZD Net, [18] Upstream, [19] Pen Test Partners, [20] ZDNet,
[21] Dark Reading, [22] Electrek, [23] TechNadu, [24] CPO Magazine, [25] The Register

A Estrutura de cibersegurança NIST

A Estrutura de cibersegurança do Instituto Nacional de Padrões e Tecnologia (National Institute of Standards and Technology – NIST) fornece um conjunto de diretrizes e práticas recomendadas que foram adotadas como padrão em uma ampla variedade de setores e indústrias. A Estrutura de cibersegurança NIST oferece orientação sobre como as organizações podem gerenciar e reduzir o risco de cibersegurança e inclui um conjunto de recomendações sobre como prevenir, detectar e responder a eventos de cibersegurança para permitir uma recuperação rápida. É amplamente entendido como a base padrão ouro sobre a qual uma organização pode construir um programa de segurança sólido.

A estrutura inclui cinco funções principais: **Identificar, Proteger, Detectar, Responder e Recuperar.** Juntas, elas abrangem todo o contínuo de ataque e o ciclo de vida do gerenciamento de segurança. As cinco Funções organizam áreas-chave que os fabricantes de automóveis podem abordar para melhorar sua postura geral de segurança, reduzir o número de vulnerabilidades de ataque exploráveis e minimizar os danos que um evento de cibersegurança de TO pode causar.

Exploraremos cada uma dessas áreas com mais profundidade abaixo, fornecendo um roteiro das etapas envolvidas na construção de uma estratégia de segurança de defesa em profundidade alinhada com o Estrutura de cibersegurança NIST.

IDENTIFICAR

Na primeira das funções da Estrutura NIST, as organizações são aconselhadas a descobrir processos e ativos críticos para os negócios, bem como inventariar os sistemas e softwares em seus ambientes de TI e TO. Isso possibilita entender melhor as fontes de risco de cibersegurança, mapeando-as em sistemas, ativos, dados e recursos. Com esse entendimento, uma organização pode focar e priorizar seus esforços de forma consistente com os objetivos do negócio e a estratégia de gestão de riscos.

Como a taxa de novos dispositivos conectados ficando on-line é rápida nas instalações de fabricação de hoje, pode se tornar cada vez mais desafiador para as equipes de segurança entender qual hardware TO está em rede. É quase impossível proteger o que você não pode ver.

Manter um inventário de ativos atual e preciso (incluindo informações sobre dispositivos específicos, como conectividade e riscos ou vulnerabilidades presentes nos ativos) é essencial. Quando as equipes de segurança entendem o que está na rede, elas podem documentar arquiteturas de sistema e fluxos de dados usando representações padrão que permitirão que equipes globais comparem topologias de hardware – e riscos – em vários locais.

Um inventário abrangente de ativos fornece uma avaliação inicial para identificar deficiências e projetar e implementar um programa de segurança para resolvê-las. Depois de concluir um inventário inicial de ativos, as montadoras devem planejar avaliações de segurança contínuas que possam gae os objetivos de segurança continuemrantir qu sendo atendidos e que a conformidade com os padrões do setor seja mantida. Os inventários de ativos também ajudam a revelar ativos não autorizados ou que estão sendo usados de maneira não autorizada.

Avaliações de segurança também são essenciais para identificar vulnerabilidades de software (CVEs). Eles fornecem uma base para reduzir as vulnerabilidades existentes agora, enquanto permitem que as organizações criem uma abordagem proativa para descobrir e corrigir vulnerabilidades futuras.

PROTEGER

A função Proteger inclui atividades que melhoram a higiene cibernética e permitem a defesa em profundidade. Isso fornece um conjunto de proteções que diminuem o risco cibernético e protegem a integridade e a confidencialidade de dados de alto valor, juntamente com a disponibilidade de sistemas críticos para os negócios. Essas proteções incluem controles de gerenciamento de identidade e acesso, segmentação de rede, CIP Security, arquitetura CPwE, programas de gerenciamento de vulnerabilidades, soluções de backup, treinamento de conscientização de segurança para funcionários e controles de configuração baseados em dispositivos.

A segmentação de rede é uma consideração importante para montadoras e outros fabricantes industriais. Os projetos de rede de TO legados tendiam a ser simples, mas as redes de TI e TO segmentadas incorretamente possibilitam que os invasores que obtêm acesso aos sistemas de TI se movam lateralmente e rapidamente pelos ambientes da fábrica, potencialmente disseminando ransomware, obtendo acesso a informações proprietárias ou comprometendo a produção.

O projeto de rede adequado e a segmentação eficaz de DMZs industriais e zonas de segurança permitem que as equipes de segurança isolem rapidamente os sistemas afetados no caso de um ataque. Isso permite que a produção normal continue em outras partes da instalação.

Os fabricantes que implantam novas soluções automatizadas ou conectadas podem se aproveitar de uma arquitetura de referência validada para garantir que estejam projetando uma rede pronta para o futuro, segmentada adequadamente e testada quanto a desempenho, disponibilidade e segurança. O uso de uma arquitetura composta por designs previamente validados, com documentação sobre as melhores práticas e ajustes de configuração, permite que as organizações implementem uma rede convergente de TI/TO robusta que atenda a todos os requisitos de desempenho, escalabilidade e segurança.

DETECTAR

As atividades dentro da função Detectar permitem que as equipes de cibersegurança identifiquem rapidamente os comportamentos da rede ou fluxos de dados anômalos podem sinalizar a ocorrência de um ataque. Essas atividades incluem coleta e monitoramento de registros e monitoramento contínuo da segurança lógica e física dos ambientes de TI e TO. Um centro de operações de segurança (SOC) 24 horas por dia, 7 dias por semana fornecerá os recursos necessários de alerta e investigação de eventos e resposta.

Os serviços de detecção de ameaças de terceiros podem fornecer acesso a tecnologias de detecção de anomalias e violações. Seu uso permite que os defensores estabeleçam uma avaliação inicial das operações normais e identifiquem e investiguem situações que não estejam de acordo com esses padrões esperados.

Para determinar o impacto que um evento de segurança pode ter nas operações da planta, é vital ter uma documentação consistente e completa para todos os sistemas da planta, redes TO e dispositivos IoT/IIoT, incluindo aqueles que são potencialmente inseguros. Em muitos ambientes de fabricação, uma compreensão das arquiteturas do sistema de TO – e quais sistemas estão expostos a redes externas – foi mantida como "conhecimento hereditário" entre o pessoal da fábrica. A documentação formal permite uma colaboração mais forte e produtiva entre engenheiros de fábrica e equipes de operações de segurança.

RESPONDER

Quando um incidente de cibersegurança é detectado, as organizações que realizaram as atividades dentro da função Responder poderão agir rapidamente para conter o incidente e reduzir seu impacto. A função Responder incorpora tanto capacidades técnicas quanto processos e fluxos de comunicação. As organizações devem identificar proativamente as funções e responsabilidades das principais partes interessadas que seriam acionadas no caso de um incidente cibernético de TO.

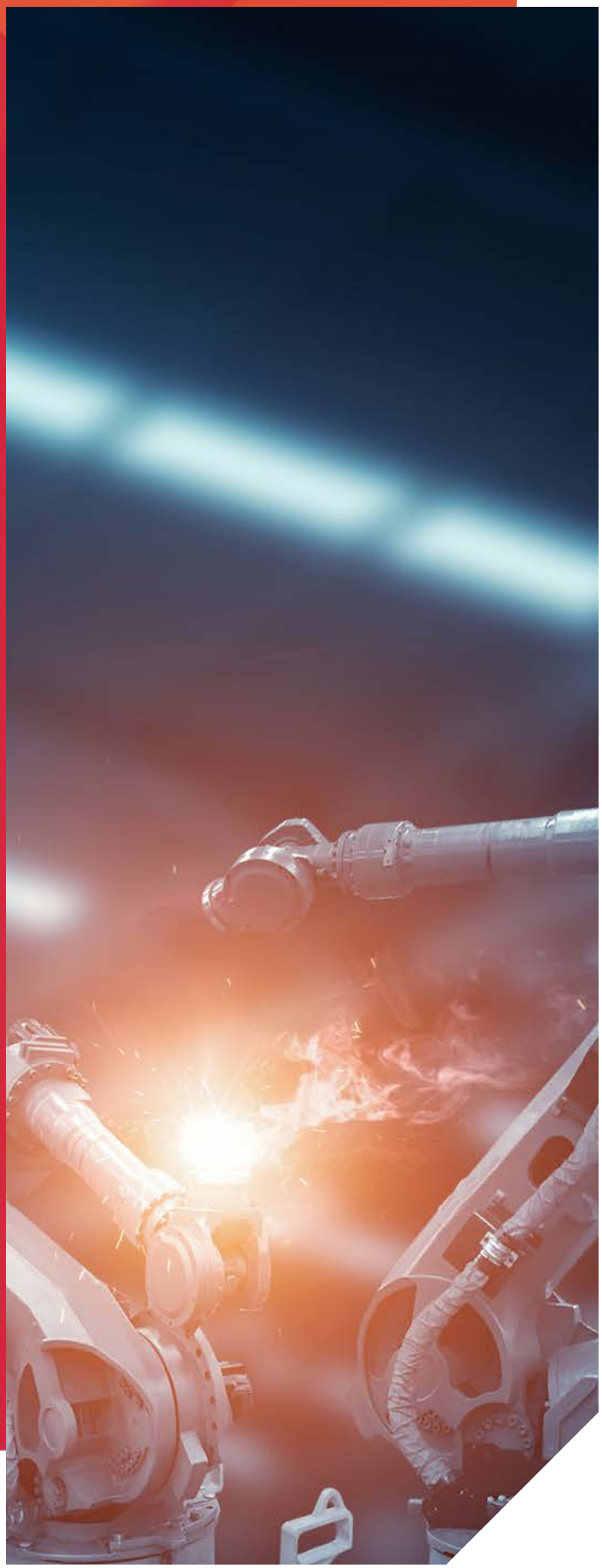
As equipes SOC e os engenheiros da planta precisarão compartilhar as responsabilidades pela investigação do evento. Todo o pessoal interno e externo se beneficiará de exercícios regulares de bancada em diferentes cenários para revisar os procedimentos em vigor e garantir que estejam prontos para tomar decisões rápidas e precisas caso ocorra uma crise.

RECUPERAR

A função Recuperar vai além das atividades de resposta imediata e de curto prazo. As organizações devem desenvolver planos que lhes permitam restaurar rapidamente recursos ou serviços afetados por incidentes de cibersegurança. Isso aumenta a resiliência e protege a continuidade operacional.

Todos os fabricantes industriais devem não apenas manter backups abrangentes, mas também garantir que uma restauração completa possa ser concluída em um prazo curto o suficiente para que não haja impactos operacionais graves. Testar os recursos de backup é essencial, assim como realizar exercícios de bancada regularmente para identificar e corrigir lacunas na resiliência do processo de negócios.

A recuperação do ICS requer habilidades e capacidades especializadas. As equipes de segurança não precisam apenas concluir a análise forense e a avaliação de danos e garantir que todo o software malicioso tenha sido removido, mas também precisam comissionar novamente as unidades e restabelecer os processos do CLP para que estejam totalmente operacionais. As equipes devem ter experiência em recuperar os processos e executá-los rapidamente.



O conceito central do Zero Trust é "nunca confie, sempre verifique".

Zero Trust para Montadoras

Zero Trust é uma abordagem para segurança de rede que foi descrita pela primeira vez por John Kindervag na Forrester Research há mais de uma década. Desde então, ganhou força entre os profissionais de segurança de TI, em grande parte porque é ideal para proteger ambientes modernos de TI remotos e baseados em nuvem. Hoje também está começando a ter uma adoção mais ampla entre os profissionais de segurança de TO.

O conceito central do Zero Trust é "nunca confie, sempre verifique". A consequência decorrente é que nenhum usuário, identidade de máquina, fluxo de tráfego ou aplicativo deve ser inerentemente confiável. Em vez disso, as identidades e os níveis de risco devem ser verificados continuamente, com aplicação contínua de políticas para cada conexão.

No mundo de hoje, onde os ataques são incessantes, a adoção de uma abordagem de confiança zero reduzirá os riscos e diminuirá as chances de sucesso de qualquer ataque. Zero Trust pode beneficiar os fabricantes automotivos:

- Reduzindo o tamanho da superfície de ataque por meio do estabelecimento de controles de acesso granulares para ativos críticos.
- Reduzindo consideravelmente o número de intrusões maliciosas na rede, tornando os requisitos de autenticação e validação de identidade mais rigorosos
- Removendo a confiança excessiva dos projetos de arquitetura de rede para tornar o trabalho dos invasores muito mais difícil

As estratégias de Zero Trust de hoje são melhor projetadas por meio de outra metodologia fornecida por Kindervag, com foco na identificação das superfícies de proteção da organização – os elementos de Dados, Ativos, Aplicativos e Serviços (DAAS) mais críticos para as operações e protegendo-os com controles de Zero Trust em ordem de prioridade.

Como a Rockwell Automation pode ajudar

A Rockwell Automation é líder mundial em automação industrial, com mais de cem anos de experiência projetando e construindo sistemas de TO.

A empresa aproveita essa profunda experiência para proteger as fábricas, ativos e redes essenciais do mundo. Tendo atendido a milhares de clientes de ICS e automação em todo o mundo, a Rockwell Automation sabe o que é necessário para proteger infraestruturas, evitar o tempo de parada não programada e reduzir danos causados por ataques cibernéticos. A Rockwell fornece serviços de cibersegurança de nível industrial que protegem as operações de produção nas quais você e seus clientes dependem diariamente – do chão de fábrica à nuvem.

A Rockwell fornece serviços gerenciados que abrangem as atividades dentro de todas as cinco funções dentro da Estrutura de cibersegurança NIST, incluindo identificação de ativos, teste e avaliação de penetração, monitoramento e correção de vulnerabilidades, projeto e implementação de programas de segurança, backup e detecção de ameaças e serviços de resposta e recuperação de incidentes.

Além disso, a Rockwell oferece um complemento de serviços baseados em projetos completo para permitir que os clientes acelerem sua maturidade de segurança de TO. A Rockwell também mantém parcerias estreitas com líderes do setor em TI e segurança, como Cisco, Claroty, Microsoft, Dragos e Crowdstrike. Eles co-desenvolveram a arquitetura Ethernet convergida em toda a fábrica (Converged Plantwide Ethernet – CPwE) com a Cisco para oferecer aos clientes um conjunto de planos arquitetônicos pré-validados e documentados, juntamente com orientações práticas para implementá-los e configurá-los.

O portfólio de produtos da Rockwell Automation inclui soluções de controle industrial seguras desde o projeto, bem como tecnologias de segurança que foram criadas especialmente para adicionar camadas adicionais de proteção aos produtos da Rockwell. Essas soluções de segurança específicas fornecem proteção de perímetro, segmentação de rede, comunicações seguras entre elementos de controle e proteção de dados para usuários de seus dispositivos.

Para saber mais sobre como os fabricantes automotivos podem dar o próximo passo em direção à construção de instalações de produção cibernéticas resilientes, entre em contato hoje mesmo com um especialista da 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-BR004A-PT-P-maio 2022