Rockwell Automation

COMPREENDENDO A CIBERSEGURANÇA AUTOMOTIVA:

Ameaças comuns, prevenção proativa

Resumo executivo

Hackers mal intencionados estão mirando empresas automotivas com ataques cibernéticos bem-sucedidos. Incidentes recentes de alto nível indicam que as atuais proteções de cibersegurança da indústria automotiva claramente não são robustas o suficiente:

- Fevereiro de 2021. Um dos principais fabricantes de automóveis da Coreia do Sul sofreu um ataque de ransomware que resultou em interrupções nos serviços de pagamento, em seus aplicativos móveis e nos sistemas internos das concessionárias.
- Junho de 2020. A principal fabricante automotiva do Japão foi vítima de um ataque cibernético que levou a interrupções operacionais em fábricas no Reino Unido, América do Norte e Itália.
- Abril de 2020 Uma investigação de uma publicação automotiva encontrou sérias falhas de segurança em dois modelos de carros mais vendidos.

Vários fatores contribuem para uma superfície de ataque expandida em empresas automotivas, incluindo:

- Aumento do fluxo de dados, comunicação, conectividade e integração da infraestrutura de tecnologia operacional e tecnologia da informação (TO/TI).
- Falta de recursos qualificados para gerenciar riscos envolvendo Sistemas de Controle Industrial (ICS), Controle de Supervisão e Aquisição de Dados (SCADA) e outros sistemas TO.
- Baixa visibilidade do número e tipos de ativos conectados a redes automotivas.
- A pandemia em andamento sobrecarregou as operações da cadeia de fornecimento, aumentando ainda mais o risco e o custo do tempo de parada não programada da fabricação, em um momento em que o estoque está fortemente restrito. Infelizmente, é improvável que essa situação diminua num futuro próximo.
- O advento da infraestrutura de veículos elétricos gera novas ameaças aos veículos conectados, estações de recarga públicas e até mesmo à rede elétrica. E a falta de padrões de segurança para proteger as estações de carregamento apenas complica ainda mais sua proteção.

Os inimigos visam vulnerabilidades na base instalada de ativos instalados na rede, incluindo máquinas e dispositivos no chão de fábrica. Como quase metade dos 100 principais fabricantes automotivos de hoje são considerados altamente suscetíveis a incidentes de ransomware[1], fica claro: a gestão de riscos na indústria automotiva ainda é muito reativa para lidar com a crescente velocidade e sofisticação dos ataques.

[1] Black Kite

Custos e Consequências

Vulnerabilidades exploradas por hackers mal-intencionados podem levar a vários resultados operacionais negativos que incluem as preocupações típicas centradas em TI, como violações de dados, e vão além.

PARADA DE PRODUÇÃO

O tempo de parada não planejado é um dos maiores riscos para as empresas automotivas porque o tempo de parada não programada da fábrica é muito caro. Uma estimativa mostrou um custo de US$ 22.000 por minuto ou US$ 1,3 milhão por hora de inatividade. Algumas estimativas mostram um custo de US$ 50.000 por minuto.[2] Muitas vezes, os ataques cibernéticos causam tempo de parada não programada em ambientes TO e os inimigos entendem que as interrupções na produção de veículos vêm com esses altos custos, tornando a indústria automotiva um alvo principal.

Separados dos custos de tempo de parada não programada, estão as despesas com danos físicos e operacionais, com os custos de resposta, remediação e recuperação de ataques cibernéticos, que normalmente são estimados entre mais de US$ 1 milhão a US$ 13 milhões ou mais por incidente.

COMPROMETIMENTO DE DADOS CONFIDENCIAIS

O potencial de comprometimento de dados confidenciais se estende da TI à TO. No entanto, dados confidenciais no chão de fábrica assumem uma forma diferente. Segredos comerciais, incluindo fórmulas, técnicas, software ou dados de máquinas e receitas, são propriedade intelectual extremamente valiosa e ativos comerciais altamente competitivos. Os fabricantes automotivos valorizam essas informações porque podem fornecer uma vantagem competitiva em eficiência operacional ou recursos do produto, especialmente em relação à mudança para veículos elétricos e estações de recarga.

Os invasores que conseguem se infiltrar em ambientes de TO/ICS podem comprometer e vazar informações vitais e/ou dados confidenciais de clientes.

ESCASSEZ NA CADEIA DE FORNECIMENTO

As montadoras não são as únicas em que os atacantes se concentram. Os riscos se estendem aos fornecedores que fornecem componentes críticos de fabricação às empresas automotivas, como sistemas de ar-condicionado e aquecimento. Ataques cibernéticos graves a fornecedores podem causar um efeito cascata que pode levar a uma escassez prolongada da cadeia de fornecimento.

Os cibercriminosos visam vulnerabilidades em todos os níveis da cadeia de fornecimento automotiva. Em outubro de 2021, por exemplo, o fornecedor alemão de peças automotivas Eberspächer Group[3], que opera 50 fábricas, sofreu um ataque de ransomware em suas redes e servidores globais que criptografou dados. A empresa desligou os sistemas de TI como medida de precaução, mas foi forçada a lidar com interrupções significativas, mandando trabalhadores para casa em licença remunerada e gerando outras perdas.

AMEAÇAS À SEGURANÇA FÍSICA

Os ataques cibernéticos que se infiltram em ambientes de TO automotivos também podem se transformar em potenciais ameaças à segurança física. Malware, worms e vírus podem sabotar dispositivos industriais, como controladores lógicos programáveis (CLPs) e dar aos inimigos controle sobre as máquinas da linha de montagem. Ajustes inesperados nos processos da linha de montagem ou no comportamento do equipamento também podem representar ameaças à segurança dos trabalhadores do chão de fábrica. Além disso, danos intencionais à TO podem prejudicar a integridade do produto e colocar em risco a segurança do cliente.

[2] TPC, [3] Eberspaecher

Atacantes do setor automotivo e ciberataques comuns

Para obter uma visão clara do cenário de cibersegurança automotiva, é importante entender mais sobre os atacantes da ameaça maliciosa direcionados às empresas automotivas e os métodos comumente usados em ataques. Também é importante observar que, embora a sofisticação dos ataques esteja crescendo exponencialmente, os ataques cibernéticos mais bem-sucedidos exploram vulnerabilidades conhecidas que podem ser corrigidas com as ferramentas e práticas recomendadas que estão disponíveis.

ATACANTES

Operadores de cibersegurança mal-intencionados, como gangues de ransomware, procuram se infiltrar nas redes para receber recompensas financeiras. Outros atacantes podem atacar empresas automotivas com a intenção de causar danos físicos ou roubar propriedade intelectual valiosa, informações pessoais identificáveis ou outros ativos de informação valiosos.

Além disso, a indústria automotiva faz parte do setor de Manufatura Crítica identificado pela Agência de Cibersegurança e Infraestrutura (CISA)[4] como crucial para a prosperidade e continuidade econômica dos EUA. A natureza econômica crítica da fabricação automotiva também torna as empresas desse setor suscetíveis a ataques cibernéticos de estado-nação. Na tentativa de promover seus próprios interesses nacionais, os países podem contratar atacantes para coletar informações ou sabotar os principais alvos industriais.

Os pesquisadores de segurança também descobrem e divulgam vulnerabilidades nas posturas de cibersegurança das empresas automotivas. Um incidente recente[5] viu pesquisadores de segurança analisarem os sistemas de computador de um modelo popular de um grande fabricante de automóveis dos EUA e descobrirem um conjunto de credenciais Wi-Fi para uma montadora.

Embora os pesquisadores de segurança normalmente não se proponham a explorar vulnerabilidades de forma maliciosa, eles podem descobrir lacunas que criam pesadelos de relações públicas, impactando a credibilidade entre os clientes.

Agora vamos nos voltar para os ataques comuns que os fabricantes de automóveis e seus fornecedores enfrentam com frequência.

RANSOMWARE.

O ransomware é um tipo de ataque em rápido crescimento, criando problemas em todos os setores industriais. O relatório de violação de terceiros de 2021 da Black Kite[6] descobriu que o ransomware é agora a origem número um de violações de dados de terceiros, respondendo por 27% dos ataques em 2021 e 53% dos CISOs disseram que foram atingidos por ransomware pelo menos uma vez no ano passado.

Em um ataque típico de ransomware, os adversários se infiltram na rede e fornecem uma carga maliciosa que criptografa vários arquivos e dispositivos. Muitos incidentes de ransomware envolvem exfiltração e criptografia de dados porque os atacantes acreditam que a extorsão tem mais chances de sucesso se puderem ameaçar divulgar informações confidenciais roubadas. À medida que as linhas divisórias entre TI e TO se confundem, os ataques de ransomware podem levar a temidas interrupções na produção do chão de fábrica.

[4] CISA, [5] Which.co, [6] Black Kite

ATAQUES ICS

A conectividade integrada e as comunicações cada vez mais abertas entre dispositivos de TI, TO e Internet das Coisas (IoT) também expandiram a superfície de ataque em ambientes ICS, expondo pela primeira vez à Internet e a aplicativos baseados em nuvem tecnologias com décadas de idade. As organizações que se consideram suficientemente isoladas estão descobrindo que na verdade é o oposto.

Ataques frequentes incluem a exploração de protocolos de comunicação inseguros; software não corrigido; segurança IoT fraca; e ataques de malware na cadeia de fornecimento que afetam os dispositivos de fabricação. E os ataques de ICS estão aumentando, como evidenciado pela divulgação de 41% mais vulnerabilidades de ICS[7] no primeiro semestre de 2021 do que no mesmo período de 2020.

INVASÃO DE VEÍCULOS CONECTADOS

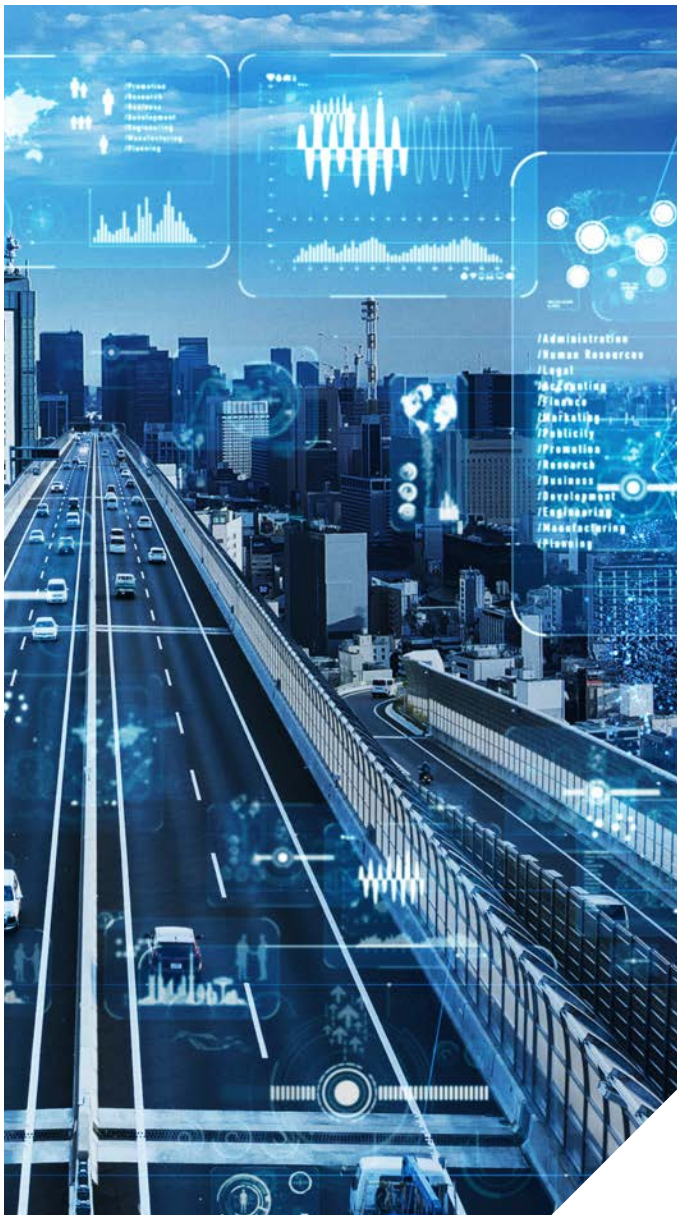
Veículos motorizados conectados modernos têm vários sistemas de computador de bordo que os atacantes podem atingir com ataques físicos e remotos. Os veículos de hoje 'acordam' e se conectam antes de saírem da linha de montagem, equipados com sistemas potencialmente exploráveis.

- A Unidade de Controle Telemático (TCU) pode ser suscetível a hacks. Em um incidente[8], os pesquisadores pegaram uma unidade telemática de um veículo, retiraram o cartão do módulo de identidade do assinante (SIM) e conseguiram usar o acesso do SIM para obter controle total da rede corporativa do fabricante do equipamento original (OEM) usando credenciais de administrador.
- O barramento Controller Area Network (CAN) permite a comunicação entre diferentes microcontroladores e sensores em veículos motorizados. A pesquisa[9] mostra que um barramento CAN típico é altamente suscetível a ataques que exploram vulnerabilidades, como falta de autenticação ou criptografia, o que pode levar à tomada de controle de veículos ou violações de dados confidenciais.

APLICATIVO MÓVEL

Em nosso mundo cada vez mais móvel, muitos OEMs oferecem aplicativos móveis que permitem que os clientes se conectem a seus veículos. Alguns desses aplicativos permitem que os usuários localizem seu veículo, abram as portas e liguem o motor. Os hackers podem explorar vulnerabilidades na programação dos aplicativos, como o aplicativo se comunica ou como ele armazena dados.

As consequências dos ataques aos aplicativos móveis variam desde a violação de informações confidenciais até possíveis ameaças à segurança. Em 2018, por exemplo, uma montadora[10] inadvertidamente expôs os detalhes pessoais de mais de 50.000 usuários de aplicativos em uma unidade de armazenamento em nuvem não segura.



[7] CPO Magazine, [8] Pen Test Partners, [9] University of Washington, [10] Bleeping Computer

Cibersegurança proativa na fabricação de automóveis

As empresas automotivas precisam de uma abordagem mais proativa para lidar com o dilúvio de ameaças que enfrentam agora. Nossas recomendações abrangem aspectos críticos da defesa em profundidade e se alinham com a Estrutura de cibersegurança (CSF) do NIST.

INVENTÁRIO DE ATIVOS E AVALIAÇÃO DE RISCO

A segurança proativa começa com a superação das lacunas de visibilidade. Quais ativos do chão de fábrica estão conectados à rede? Qual software é usado em ambientes de TO e quais são os riscos específicos para esses ativos e softwares? As empresas automotivas não podem proteger o que não conhecem.

Um inventário completo e uma avaliação de risco podem ajudar a orientá-lo para as correções mais importantes antes que hackers mal-intencionados possam explorar quaisquer pontos fracos evidentes.

As etapas iniciais que você pode seguir se alinham com a categoria Identificar do CSF do NIST, projetada para ajudar a focar e priorizar as proteções de segurança nas vulnerabilidades de prioridade mais alta. O objetivo é proteger os ativos de maior valor no negócio primeiro, com base em ameaças reconhecidas e riscos impostos à organização.

GESTÃO DE PATCHES

A gestão de patches em TO é desafiadora porque qualquer nível de tempo de parada não programada é caro e é evitado, e a correção de software desatualizado geralmente exige a retirada da máquina de operação.

Na maioria dos casos, fazer um inventário de ativos e conduzir uma avaliação de risco marcará vários dispositivos de chão de fábrica executando sistemas operacionais desatualizados. Essas etapas também revelarão ativos não autorizados escondidos na rede, expondo a organização a vulnerabilidades críticas.

Uma abordagem de segurança proativa deve incluir uma metódica gestão de patches para abordar vulnerabilidades de acordo com a função Proteger do CSF do NIST. As empresas automotivas precisam de processos para lidar com instalação de patches com interrupção operacional mínima. Algumas empresas optam por uma abordagem de infraestrutura como serviço, que simplifica bastante a aplicação de patches e outros processos operacionais e de gerenciamento de cibersegurança.

As equipes de segurança devem considerar estes fatores ao determinar a priorização de patches:

- O risco potencial para os ativos se uma vulnerabilidade for explorada
- A importância de qualquer dispositivo ou sistema vulnerável para o processo geral de fabricação
- As proteções de segurança fornecidas por cada patch.

ZONEAMENTO DE REDE LÓGICA E CPWE

A arquitetura de rede desempenha um papel vital na segurança de ambientes conectados de TI e TO. Os ataques podem se propagar de máquinas individuais, em switches e outros componentes do chão de fábrica para a rede de TI, bem como vice-versa – de TI para redes TO. Isso geralmente leva à decisão de colocar os sistemas de produção off-line durante incidentes de segurança de TI.

No exemplo de exploit anterior da violação do TCU de um veículo, o OEM não tinha segmentação de rede adequada. O zoneamento de rede lógica ajuda a melhorar a criação das estratégias de zoneamento corretas para uma segurança mais holística em toda a planta, protegendo as operações contra uma variedade de ataques.

Uma arquitetura de referência comprovada, como Converged Plantwide Ethernet (Ethernet convergentes em toda a fábrica – CPwE), também fornece uma base sólida para segmentação de rede adequada, para que os atacantes não possam explorar vulnerabilidades e se mover entre ambientes de TI e TO.

Frequentemente, as arquiteturas de TO surgem de projetos de produção funcionais e eficientes, em vez de terem segurança incorporada desde o início. Os sistemas de TO são criados para serem implantados e executados sem problemas. Muitas vezes, há pouco ou nenhum foco em como uma decisão de design específica pode afetar a segurança de rede.

O que as montadoras precisam são sistemas de TO fluidos com as proteções de cibersegurança corretas para protegê-los. Mesmo com o aumento do número e da gravidade dos ataques, ainda é importante manter um fluxo de informações tranquilo e seguro para maximizar o tempo de disponibilidade confiável.

A CPwE usa uma Zona Desmilitarizada Industrial (IDMZ) para compartilhar informações com segurança entre sistemas de TI e TO, ao mesmo tempo em que protege os sistemas de produção do tráfego malicioso proveniente de sistemas corporativos de TI ou da Internet. Os firewalls de perímetro e interno fornecem forte proteção e aplicação de políticas de segurança, fornecendo inspeção de tráfego em todas as redes.

DETECÇÃO E RESPOSTA CONTÍNUAS A AMEAÇAS

A detecção e resposta a ameaças fornece armamentos críticos nas defesas de segurança de qualquer organização.

Embora uma abordagem proativa à cibersegurança automotiva comece com etapas de prevenção que melhoram a resiliência cibernética, a implementação de controles de detecção de ameaças e de resposta a incidentes pode ajudar as empresas a detectar ataques rapidamente, responder a ameaças e ajudar a prevenir a propagação, e recuperar os sistemas afetados mais rapidamente em caso de violação.

As soluções de detecção de ameaças devem identificar continuamente assinaturas de ameaças, como dispositivos anômalos e atividades na rede. A avaliação inicial da atividade normal do usuário e dos fluxos de tráfego podem ser úteis na análise e podem reduzir o tempo de detecção de incidentes, especialmente em redes complexas com altos níveis de convergência de TI/TO.

A detecção de ataques em tempo real também permite uma resposta rápida a incidentes, como colocar dispositivos em quarentena ou remover o acesso, ajudando os fabricantes automotivos a evitar a escalada de danos.

Experiência em cibersegurança da Rockwell Automation para a indústria automotiva

Na Rockwell Automation, nossos serviços de cibersegurança de força industrial protegem os processos de fabricação automotiva nos quais você e seus clientes dependem diariamente. Nossa abordagem proativa abrange todo o ciclo de vida da cibersegurança, desde a avaliação até a recuperação – para que sua organização possa estar preparada antes, durante e depois de um ataque.

Oferecemos uma compreensão profunda das operações de produção, aproveitando insights de mais de 100 anos de automação industrial. Começando com um inventário completo e uma avaliação de risco, podemos ajudá-lo a obter visibilidade clara da arquitetura instalada,

da infraestrutura de rede e das vulnerabilidades presentes em seu ambiente.

Nossa experiência com Converged Plantwide Ethernet (CPwE) garante uma defesa em profundidade holística para ajudar a impedir que as ameaças se propaguem entre as operações de TI e TO. E a detecção e resposta de força industrial usando um Centro de Operações de Segurança (SOC) de TO ativo 24 horas por dia, 7 dias por semana, pode ajudar a interromper ataques antes que agentes mal-intencionados interrompam as operações.

Para saber mais sobre como as estratégias proativas de segurança automotiva podem proteger contra criminosos cibernéticos, entre em contato conosco hoje mesmo.

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-WP004A-PT-P – maio 2022