KPMG

Protegendo as redes de *Operational Technology* (OT)

Implementação da arquitetura *zero trust* e gerenciamento de riscos da cadeia de suprimentos para prevenir ataques cibernéticos na infraestrutura crítica

KPMG em Singapura
Novembro de 2021

Sumário

Prefácio

As redes de *Operational Technology* (OT, ou Tecnologia Operacional, em português) são sistemas computadorizados utilizados para controlar operações industriais físicas e são encontradas em uma ampla variedade de setores *asset intensive* (ativos intensivos). Elas executam diversas tarefas, desde o monitoramento da infraestrutura crítica até o controle de robôs em uma planta industrial.

Conforme os esforços para modernizar a infraestrutura crítica são intensificados, os riscos de ataques cibernéticos nas redes de OT aumentam. Tradicionalmente, os sistemas de OT eram separados da Internet, mas o aumento da digitalização levou a uma maior integração entre TI e OT. Infelizmente, isso também significa que centenas de milhões de dispositivos de OT e da Internet das Coisas (IoT), tais como equipamentos médicos e de energia, estão hoje vulneráveis a ataques.

O número de vulnerabilidades de OT identificadas e reportadas anualmente pela Equipe de Resposta a Emergências Cibernéticas de Sistemas de Controle Industriais dos EUA (ICS-CERT) aumentou a uma taxa estimada de 16% ano após ano de 2017 a 2020, de acordo com o relatório Cenário Cibernético de Singapura de 2020, elaborado pela Agência de Segurança Cibernética de Singapura.

"Os ataques cibernéticos em sistemas de OT podem ter consequências sérias e muito prejudiciais, pois os invasores podem incapacitar a infraestrutura crítica, como estações de tratamento de água, oleodutos e redes de energia. Isso explica porque os líderes de negócios identificaram o risco de segurança cibernética como a maior ameaça ao crescimento de suas organizações".

A pandemia da covid-19 obscureceu ainda mais os limites entre os mundos físico e digital, expondo falhas na infraestrutura de segurança cibernética e revelando uma série de novos desafios.

No contexto pós-pandemia, a escassez de mão de obra no local de trabalho é um desses desafios. Um dos principais motivos para a falta de pessoal é que as empresas estão adotando arranjos de trabalho híbridos e dividindo as equipes em meio às restrições relacionadas à covid-19. Isso geralmente leva a ciclos de manutenção prolongados e soluções alternativas, como suporte por serviço remoto para os empregadores. Consequentemente, os riscos da cadeia de suprimentos também aumentaram.

Em muitos casos, as empresas começaram a implementar redes privadas virtuais *(Virtual Private Networks,* ou VPNs em sua sigla em inglês) para possibilitar o acesso remoto. No entanto, isso pode ser uma faca de dois gumes, uma vez que as VPNs são alvos potenciais para invasores obterem acesso não autorizado à rede de TI e OT da empresa.

Os ataques cibernéticos em sistemas de OT podem ter consequências sérias e muito prejudiciais, pois os invasores podem incapacitar a infraestrutura crítica, como em estações de tratamento de água, oleodutos e redes de energia.

Isso explica porque os líderes de negócios identificaram o risco de segurança cibernética como a maior ameaça ao crescimento de suas organizações nos próximos três anos, de acordo com a pesquisa *KPMG CEO Outlook Pulse Survey 2021*.

Portanto, torna-se importante entender a natureza e as rotas de ataque aos sistemas de operação para construir defesas robustas. As empresas precisam entender como os invasores estão reunindo informações sobre sistemas específicos. Isso ocorre por meio da inteligência de código aberto (*open-source intelligence*, ou OSINT em sua sigla em inglês) ou outros métodos de detecção de informações? Eles estão usando protocolos de engenharia reversa ou desenvolvendo ferramentas personalizadas? Eles testaram as ações em um ambiente simulado antes de realizar os ataques?

Este relatório examina os principais desafios que os profissionais enfrentam e busca traçar um roteiro claro para proteger os sistemas de OT em um cenário de ameaças em rápido crescimento.

Eddie Toh
Sócio-líder de Tecnologia Forense da KPMG na região Ásia-Pacífico

Três tipos de ataques nas redes de OT

Um ataque do tipo *watering hole* ocorre quando os invasores espalham *malwares* pela rede de uma organização, infectando sites que os membros do grupo costumam visitar. O ataque Havex foi um bom exemplo. Os invasores podem usar ferramentas de rastreamento da Internet para identificar os sites visitados frequentemente pelo alvo e, em seguida, pesquisar as vulnerabilidades desses sites. Isso é explorado para criar códigos maliciosos que redirecionam o usuário para outro site que hospeda o *malware*.

De maneira geral, as organizações enfrentam três tipos de ataques atualmente: diretos, indiretos e de reconhecimento. Todos eles podem expor vulnerabilidades em cadeias de suprimentos cruciais, capazes de paralisar as operações normais de uma organização. Em situações extremas, esses ataques podem encerrar as operações de um setor crítico do qual muitas pessoas dependem.

- Ataques diretos são realizados para causar danos a um sistema de OT específico. Entre os exemplos de *hackers* que usam conexões remotas para lançar esses ataques, estão os incidentes recentes em uma rede elétrica na Europa e em uma estação de tratamento de água nos Estados Unidos.

  Uma vez que os sistemas são violados, os invasores podem inserir neles códigos maliciosos, causando seu mau funcionamento e modificando sua lógica de controle. Foi o que aconteceu quando um *malware* batizado de *Triton* assumiu o controle remoto de uma estação de trabalho de controle de segurança em uma usina de energia. Os investigadores descobriram que uma estação de trabalho de engenharia (*engineering workstation*, EWS) de um Sistema de Instrumentação de Segurança (*Safety Instrumentation Systems*, SIS) foi a primeira a ser comprometida. Em seguida, a EWS interagiu diretamente com os controladores do SIS usando o protocolo *User Datagram Protocol* (UDP).

Quatro arquivos binários foram carregados para os controladores — dois embutidos em um s*cript Python* compilado com dois outros arquivos direcionados a um controlador SIS específico. Foi assim que o SIS acionou o desligamento do sistema neste ataque.

- Ataques indiretos também estão crescendo. Eles não afetam diretamente os sistemas de OT, mas ainda podem levar a consequências graves, como interrupção dos serviços e danos ao meio ambiente, ameaças à segurança de processos e a vidas humanas. Entre os exemplos recentes, estão os ataques de *ransomware* a um oleoduto de combustível nos Estados Unidos e a um hospital universitário na Europa.

  Em ambos os casos, os *hackers* buscavam atingir originalmente os sistemas de TI, em vez das redes de OT, mas as operações ainda assim foram paralisadas, causando danos substanciais. O ataque ao oleoduto estava vinculado a um grupo criminoso especializado em criar *ransomware*s e vendê-los a afiliados, conhecido como *Ransomware-as-a-Service* (RaaS). Ele violava o sistema de TI da organização por meio de credenciais coletadas e *ransomware*s implementados que, segundo informações, afetou os sistemas de faturamento da empresa, bloqueando terminais e extraindo *terabytes* de dados confidenciais.

  Consequentemente, a empresa precisou fechar quase nove mil quilômetros de oleodutos enquanto investigava a profundidade da invasão dos seus sistemas. A interrupção pode ser comparada às consequências de desastres naturais, como furacões, que muitas vezes forçam o fechamento de trechos de oleodutos e refinarias por dias ou semanas.

  O ataque a um hospital universitário na Europa mostrou como as vidas humanas também estão em jogo. Nesse caso, um *malware* apelidado de *Doppel-Paymer* obteve acesso ao sistema por meio de uma vulnerabilidade de *software*. Uma paciente que buscava tratamento de emergência perdeu a vida. Seu atendimento foi recusado depois que o *malware* infectou mais de 30 terminais do hospital, paralisando as operações normais. Esses exemplos revelam como somos vulneráveis a consequências indiretas de ataques a sistemas de TI.

- Ataques de reconhecimento não levam a interrupções imediatas. Os invasores podem se esconder em um ambiente para coletar informações, extrair dados confidenciais e realizar ciberespionagem.

  Um dos exemplos mais conhecidos é o ataque Havex, realizado por um grupo de ameaça de persistência avançada (*advanced persistence threat*, APT). Esse caso envolveu um Cavalo de Troia (*trojan*) de acesso remoto (*remote access trojan*, RAT) baixado de sites de fornecedores de OT.

  O RAT então usou a *Open Platform Communication* (OPC) para procurar dispositivos em portas comumente utilizadas por mecanismos de OT. As informações coletadas foram enviadas de volta ao servidor de controle e comando (C2) do invasor.

Ataques às cadeias de suprimentos por meio de sistemas de OT representam grandes riscos

Entender como a arquitetura de segurança em redes de OT é configurada pode ajudar a identificar as lacunas que precisam ser preenchidas e proteger as cadeias de suprimentos de ataques cibernéticos.

Conforme destacado na seção anterior, as vulnerabilidades da cadeia de suprimentos podem ser expostas aos três tipos de ataques. Para interrompê-las, os invasores podem escolher focar diferentes fases do ciclo de vida do sistema, do projeto, passando pelo desenvolvimento e distribuição até a manutenção e descarte.

As cadeias de suprimentos costumam ser visadas por meio de conteúdos maliciosos disfarçados de produtos conhecidos ou confiáveis. Esse método oferece uma rota aos invasores para atingir muitos alvos. Em um dos exemplos mais conhecidos, o código-fonte foi infectado com um código malicioso pouco antes da compilação final do *patch* de *software*.

Os *patches* infectados atingiram mais de 20 mil usuários finais, incluindo agências governamentais e organizações privadas. Ao sequestrar atualizações, minar a assinatura do código e comprometer o código-fonte aberto, os invasores podem destruir a confiança nos *softwares e hardwares* adquiridos.

Mais recentemente, um fornecedor de plataforma de *managed security provider* (MSP) foi atingido por um ataque que afetou mais de mil empresas, incluindo uma grande rede de supermercados escandinava.

Segmentação das redes de OT

À medida que as ameaças cibernéticas aumentam durante a pandemia da covid-19, as organizações estão reconhecendo a necessidade de segmentar suas redes para proteger os sistemas de OT. Embora a maioria dos sistemas de OT tenham perímetros reforçados com *gateways, firewalls* e diodos, muitos sistemas de OT legados ainda são redes planas e não segmentadas internamente.

Isso permite que os invasores se movam lateralmente para outros sistemas na rede após violar os pontos de entrada iniciais. Portanto, a abordagem tradicional para resolver esse problema é a segmentação da rede. O Modelo Purdue e os Padrões IEC 62443, descritos abaixo, foram desenvolvidos para abordar questões de segurança em sistemas de automação e controle industriais (*industrial automation and control systems*, IACS) e OT.

O Modelo Purdue

Este modelo define os IACS em vários níveis: nível 0 — dispositivos de campo; nível 1 — controladores de campo; nível 2 — controle de sistema e aquisição de dados (*system control and data acqusition*, SCADA); nível 3 — rede local da planta industrial (LAN); nível 3,5 — zona desmilitarizada (*de-militarisede zone*, DMZ) da planta; nível 4 — zona empresarial; nível 5 — DMZ empresarial. Cada nível deve ter sua própria defesa em camadas ou em profundidade.

IEC 62443

Cinco níveis de segurança

Sete requisitos fundamentais (*foundational requirements*, FRs)

Definida pela Comissão Eletrotécnica Internacional, esta série de padrões cobre as orientações gerais sobre a proteção de sistemas de OT, política e procedimentos, tecnologia e desenho de sistemas, além dos requisitos de componentes. O IEC 62443 recomenda que as redes de OT sejam segmentadas em zonas e conduítes e define cinco Níveis de Segurança (*Security Levels*, SL), de 0 a 4, com sete requisitos fundamentais (FRs), mostrados na figura acima. Os SLs são atribuídos pela avaliação dos FRs implementados em cada zona e com que eficiência os pontos de estrangulamento interzonas estão protegidos.

Migração para *zero trust* em OT

Embora o Modelo Purdue e o IEC 62443 sejam estruturas bem estabelecidas, o conceito de *zero trust* (confiança zero, em português) está ganhando popularidade. E por um bom motivo: o número crescente de incidentes em que os invasores desestabilizaram a confiança das vítimas nos *softwares* e *hardwares* adquiridos.

Uma arquitetura de segurança *zero trust* é um modelo relativamente novo que assume que as identidades autenticadas ou mesmo a própria rede já podem estar comprometidas — mesmo que não estejam. Essa abordagem trata cada usuário, dispositivo e interação como uma ameaça potencial e, dessa forma, cada conexão ou condição precisa ser validada continuamente para garantir que seja legítima. O modelo *zero trust* baseia-se amplamente nos seguintes princípios:

- A distinção entre zonas confiáveis e não confiáveis foi removida, uma vez que todas as zonas são consideradas como não confiáveis.
- Todas as fontes de dados e serviços de computação são considerados recursos.
- Qualquer usuário humano, aplicativo ou dispositivo que acesse os recursos deve ser autenticado e autorizado.
- As decisões de acesso são independentes da localidade na rede. Em outras palavras, os *hosts* que estão na mesma zona não confiam inerentemente uns nos outros.
- Não há zonas e conduítes, apenas um plano de controle, que processa solicitações de acesso a recursos protegidos, e um plano de dados, onde todo o resto reside.
- Não há confiança: a verificação é sempre necessária.

Os princípios de *zero trust* foram originalmente concebidos para empresas. À medida que a OT evolui para ser mais interconectada e digital, alguns elementos deste modelo também devem ser adotados na OT.

O modelo *zero trust* elimina o fardo de proteger as senhas. A autenticação multifator ("o que você tem" e "quem você é") é utilizada, em vez de credenciais do tipo "o que você sabe".

O que você precisa saber

Em uma estrutura *zero trust*, o controle de acesso baseado em funções é praticado e matrizes de controle de acesso são criadas seguindo o princípio do menor privilégio, ou seja, um usuário só tem direitos suficientes para realizar a sua função. Além disso, o gerenciamento rígido da sessão é implementado para que todas as sessões sejam encerradas imediatamente assim que o usuário conclua a função necessária. Caso uma sessão fique ociosa por muito tempo, ela também será encerrada.

A criptografia é uma consideração importante para o modelo *zero trust* em OT. Mas a comunicação da OT é tradicionalmente não autenticada e os protocolos não são criptografados em trânsito. Há um grande potencial para utilizar criptografia em protocolos de OT como *Secure Modbus, Open Platform Communication Unified Architecture* (OPC UA) *e Generic Object-Oriented Substation Event* (GOOSE). Eles estão descritos no IEC 62351 (itens Gerenciamento de Sistemas de Energia e Intercâmbio de Informações Associadas — Segurança de Dados e Comunicações).

O modelo *zero trust* evita políticas e configurações padrão. Portanto, os dados históricos de comportamento do usuário e as suas ações atuais são enviados para análise em um mecanismo no plano de controle.

As pontuações de confiança são fornecidas em relação a uma linha de base e as políticas são desenvolvidas, implementadas e aplicadas posteriormente. Este método é descrito na publicação *Zero Trust Reference Architecture* do Departamento de Defesa dos EUA.

Embora as defesas perimetrais, como *gateways*, ainda sejam importantes, há menos ênfase em tecnologias como VPNs, que costumam ser o alvo dos invasores. Como parte da abordagem *zero trust*, toda a rede é microssegmentada no nível do aplicativo. Um mecanismo da lista de permissões é implementado, por meio do qual algumas entidades identificadas têm permissão para acessar um privilégio, serviço, mobilidade ou reconhecimento específico. Enquanto isso, os *firewalls* de última geração (*next generation firewalls,* NGFWs) realizam a inspeção profunda de pacotes (*deep packe inspection*, DPI) do tráfego Norte-Sul, enquanto o tráfego Leste-Oeste é monitorado com alta granularidade.

Superando os desafios de migrar sistemas de OT para *zero trust*

Conforme o modelo *zero trust* é adotado em sistemas de OT, a implementação manual é vista como impraticável, porque é cara e demorada. Recursos como poder de computação e capacidade de armazenamento de *logs* precisam ser projetados para que o monitoramento, análise, criptografia, gerenciamento de chaves e auditoria possam ser automatizados para reduzir as despesas gerais.

Alguns profissionais de OT consideram que a migração para a arquitetura *zero trust* é muito onerosa, pois exige que as organizações destruam e reconstruam a infraestrutura legada. Mas há uma visão diferente — esse processo não precisa ser caro. A publicação especial 800-207 on *Zero Trust Architecture, do National Institute of Standards and Technology* (NIST), dos Estados Unidos, traça um roteiro para implementar o modelo *zero trust* em um sistema de OT como um caminho com várias etapas, em vez de uma substituição total da infraestrutura. Os seguintes passos são propostos:

1 Identificar quem são os participantes, como usuários e administradores do sistema.

2 Identificar objetos no sistema, como ativos, dispositivos, serviços, etc.

3 Identificar os principais processos e avaliar os riscos associados à execução deles.

4 Identificar um processo candidato para implementação da arquitetura *zero trust*.

5. Formular políticas para o processo de candidatura.

6. Implementar, monitorar e gerar *feedback*.

7. Ampliar o uso da arquitetura *zero trust*.

Fortalecimento do gerenciamento de riscos da cadeia de suprimentos

O que pode ser feito

Conforme apresentado nas seções anteriores, o aumento dos ataques a sistemas de OT expôs vulnerabilidades globais nas cadeias de suprimentos. Esses ataques também intensificaram o foco sobre a necessidade da arquitetura *zero trust* no gerenciamento de riscos cibernéticos da cadeia de suprimentos (C-SCRM) para OT. Em Singapura, por exemplo, a CSA deve publicar o seu Programa de Cadeia de Suprimentos de Infraestrutura de Informações Críticas (CII). Na base deste programa, estão três princípios norteadores para gerenciar os riscos de segurança cibernética das cadeias de suprimentos: asseguração, transparência e responsabilidade.

Ao mesmo tempo, é importante entender os diferentes tipos de riscos em jogo. As ameaças à cadeia de suprimentos podem ser amplamente categorizadas em riscos de *hardware*, *software* e de fornecedores. Os principais controles de segurança para mitigá-los incluem:

1 Entender bem o seu inventário. Isso envolve a criação de uma lista de materiais para *hardware* e *software*, o conhecimento da função e origem de cada item e a verificação de sua integridade.
2 Praticar o conceito de *security by design*. Assim como o ciclo de vida do projeto de *software*, isso exige a avaliação de vulnerabilidades e riscos, testes de penetração e revisão completa do código pré-produção.
3 Especificar os requisitos de segurança cibernética para fornecedores e produtos que serão atendidos como parte do contrato. As organizações devem verificar isso analisando os certificados e garantindo o direito de auditoria.

Um maior foco no gerenciamento de ameaças à segurança cibernética da cadeia de suprimentos em redes de OT culminou no desenvolvimento de algumas estruturas bem conhecidas que visam enfrentar esses riscos.

Publicações do NIST sobre C-SCRM

O NIST dos EUA comissionou o Projeto NIST C-SCRM em 2008 para melhorar o gerenciamento de riscos das cadeias de suprimentos no setor. Entre seus principais relatórios, está a Publicação Especial (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations* (Controles de Segurança e Privacidade para Sistemas de Informação e Organizações).

A NIST SP 800-53 lista as 20 famílias de controle recomendadas, incluindo controle de acesso, conscientização e treinamento, gerenciamento de configurações e de riscos das cadeias de suprimentos. Na família de controles de gerenciamento de riscos das cadeias de suprimentos, há 12 controles com suas melhorias. Isso serve como uma excelente referência para estabelecer uma estrutura para C-SCRM organizacional. O que é ainda melhor é que os controles relacionados estão vinculados a cada controle da cadeia de suprimentos. Por exemplo, o Controle 10 da Cadeia de Suprimentos (SR) — Inspeção de Sistemas ou Componentes, está vinculado ao Controle 3 de Conscientização e Treinamento (AT) — Treinamento Baseado em Funções, que garante a competência durante a inspeção.

Relatório Técnico do MITRE

Além do NIST, as organizações também podem considerar a abordagem descrita no relatório técnico do MITRE *Supply Chain Attack Framework* (Estrutura e Padrões de Ataque à Cadeia de Suprimentos) para abordar e se proteger contra vulnerabilidades da cadeia de suprimentos.

O diagrama a seguir explica como os usuários podem se concentrar em tipos específicos de ataques à cadeia de suprimentos que podem danificar seus sistemas.

Ataque nos locais

De acordo com este relatório técnico, há quatro tipos de ataques à cadeia de suprimentos que podem ocorrer — *hardware*, *software*, *patch*/*firmware* e dados/informações do sistema.

Segundo o relatório, os pontos onde os ataques podem ocorrer são mapeados para cada local vulnerável — produção principal (*hardware*/*software*), integração de *hardware*/*software*; subempregador; empregador principal; escritório do programa.

Ataques aos elos

Depois que os ataques a locais estiverem mapeados, os pontos onde em que eles podem ocorrer também são mapeados para cada elo vulnerável — logística (fluxo físico via processamento, embalagem e distribuição), informações e fluxo de dados (via redes e conectividade de Internet).

Ataques na fase do ciclo de vida do produto

Além disso, há cinco fases do ciclo de vida de um produto que podem ser atacadas — análise de soluções de material, desenvolvimento da tecnologia (*technology development*, TD), desenvolvimento de engenharia e manufatura (*engineering and manufacturing development*, EMD), produção e implementação (*production and deployment*, P&D) e operações e suporte (*operations and support*, O&S). Os ataques são mapeados para a fase em que é provável que haja comprometimento.

Catalogação de possíveis ataques

1. ID de ataque (número de ID exclusivo), por exemplo, A1, A2, A3 etc.
2. Ponto de ataque (localização ou elo da cadeia de suprimentos).
3. Fase alvo (fase do ciclo de vida de aquisição).
4. Tipo de ataque (inserção maliciosa de SW, HW, FW ou informações/dados do sistema).
5. Ato do ataque (o "o quê").
6. Vetor do ataque (o "como").
7. Origem do ataque (o "quem").
8. Objetivo do ataque (o "porquê").
9. Impacto do ataque (consequência caso bem- sucedido).
10. Referências (fontes de informação).
11. Ameaça (evento adverso dirigido à cadeia de suprimentos).
12. Vulnerabilidades (pontos fracos exploráveis).

Análise de ataques potenciais

O mapeamento de cada ataque contra locais vulneráveis e fases do ciclo de vida permite que controles sejam implementados visando reduzir os riscos da cadeia de suprimentos.

Estudo de caso de ataques de cenário para consideração

Componente crítico focado para inserção maliciosa	Fase focada	Número de ataques aplicáveis	Ataques específicos																		
Hardware	TTD	5	**A2**		**A6**		**A8**								**A29**				**A36**		
	EMD	13	**A2**	**A5**	**A6**	**A7**		**A9**	**A10**		**A15**	**A22**		**A24**			**A29**	**A31**	**A33**		**A36**	
	P & D	12	**A2**	**A5**	**A6**	**A7**				**A11**	**A15**	**A22**		**A24**	**A25**		**A29**	**A31**	**A33**			
	O & S	10		**A5**	**A6**	**A7**			**A10**		**A15**		**A23**	**A24**		**A28**				**A34**	**A36**	
Software	TTD	5					**A13**	**A18**				**A27**			**A36**	**A38**						
	EMD	15	**A1**	**A3**	**A4**	**A5**	**A13**	**A18**	**A19**		**A26**	**A27**	**A32**		**A36**	**A38**	**A39**	**A40**	**A41**			
	P & D	9		**A3**	**A4**	**A5**			**A19**		**A26**	**A27**	**A32**			**A38**	**A39**		**A41**			
	O & S	11		**A3**	**A4**	**A5**	**A13**			**A21**				**A35**	**A36**	**A38**	**A39**	**A40**	**A41**			
Firmware	TTD	1							**A29**													
	EMD	8	**A4**	**A7**	**A10**		**A15**	**A20**	**A29**	**A33**	**A41**											
	P & D	8	**A4**	**A7**		**A12**	**A15**	**A20**	**A29**	**A33**	**A41**											
	O & S	8		**A7**	**A10**						**A41**											
	MSA	4			**A16**	**A17**																
	TTD	4				**A17**	**A18**															
Sys Info/Data	EMD	3	**A14**			**A18**		**A31**														
	P & D	3					**A30**	**A31**	**A37**													
	O & S	2					**A30**		**A37**													

Examplo: O Foco do componente

Revisar esses ataques à cadeia de suprimentos por meio de inserção maliciosa para aplicabilidade

Exemplo de estudo de caso: considerar ataque A3

Fonte: MILLER, John F. *Technical Report on Supply Chain Attack Framework and Attack Patterns*. MITRE, 2013.

O futuro da segurança de OT

Espera-se que as ameaças de OT aumentem em intensidade e complexidade à medida que as organizações adotam novas tecnologias. Alguns exemplos incluem a análise de dados e *machine learning* (aprendizado de máquina, em português), virtualização de sistemas de controle distribuído (*distributed control systems*, DCS) e SCADA *as a Service* (hospedado na nuvem). Essas máquinas virtuais e modelos em nuvem representam cargas de trabalho que também exigem segurança *zero trust*.

Enquanto isso, a computação quântica surge como um benefício, mas que pode gerar riscos para os sistemas de OT. Se por um lado ela melhora o desempenho e a velocidade do sistema, por outro, ela permite que os adversários quebrem a criptografia tradicional com maior facilidade.

Finalmente, a tecnologia de *blockchain* também representa uma nova fronteira, oferecendo aos profissionais de OT muitas reflexões. Embora o *blockchain* ainda esteja nas fases iniciais de adoção em sistemas de OT, provavelmente haverá vários novos casos de uso no futuro. Por exemplo, a capacidade de um livro-razão do *blockchain* de permanecer inalterado é uma promessa de autenticação de transações *host-to-host* em sistemas de OT. Só o tempo dirá como a segurança de OT evoluirá, mas o que está claro é que as empresas devem estar preparadas para se adaptar rapidamente para permanecer à frente de adversários mal-intencionados.

Não importa onde a empresa esteja em sua jornada de segurança cibernética, a KPMG pode ajudar a chegar ao seu destino: um local de confiança no qual é possível atuar sem interrupções devastadoras decorrentes de um evento de segurança cibernética — e com um orçamento viável. A KPMG também está preparada para trabalhar com estratégia e governança, transformação organizacional, defesa e resposta cibernética, entre outras áreas.

De testes de invasão e estratégia de privacidade ao gerenciamento de acesso e mudança cultural, a KPMG adota uma abordagem prática para ajudar as organizações em cada etapa do caminho.

Fale com nosso time

Eddie Toh
Sócio-líder de Tecnologia Forense
KPMG na Ásia Pacífico
eddietoh@kpmg.com.sg
+65 6213 3028

Rodrigo Milo
Sócio de Cyber Security da KPMG no Brasil
rodrigomilo@kpmg.com.br

Luis Lima
Sócio-diretor de Cyber Security em OT/IIoT da KPMG no Brasil
luislima@kpmg.com.br

Baixe o
nosso APP

kpmg.com.br

/kpmgbrasil

Este material foi traduzido da língua inglesa, baseado na publicação original "Securing Operational Technology (OT) networks".